CiscoWorks LAN Management Solution

Deployment Guide 3.0

Contents

1. Cisco LAN Management Solution 3.0 Deployment Guide

1.1. Introduction

Effective network management is critical in today's networks, helping enterprises deploy and manage solutions. With increasing reliance on networks to increase productivity, enterprises are confronted with an ever growing network size. Such increase in the number of network elements creates a challenge for network administrators. How does an enterprise effectively deploy and maintain their network devices?

CiscoWorks LAN Management Solution (LMS) provides the integrated management tools needed to simplify the configuration, administration, monitoring, and troubleshooting of Cisco networks. LMS provides IT organizations an integrated system for sharing device information across management applications, automation of device management tasks, visibility into the health and capability of the network, and identification and localization of network trouble. By using common centralized systems and network-inventory knowledge, CiscoWorks LMS delivers a unique platform of cross-functional management capabilities that reduces network administration overhead and provides upper-layer systems integration.

For detailed product info related to LMS, refer to http://www.cisco.com/go/lms.

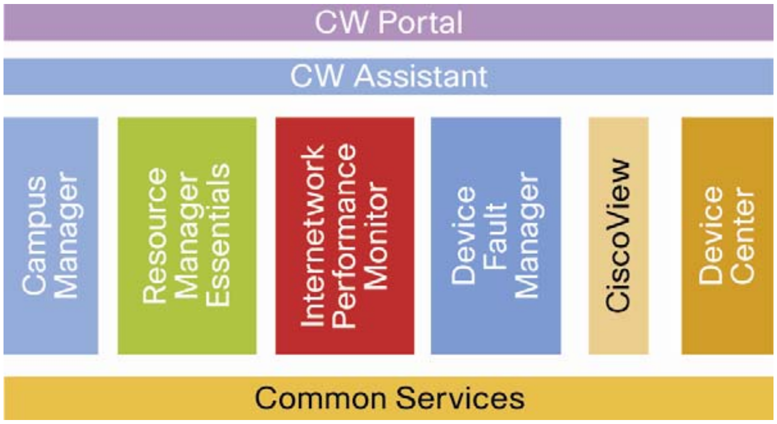
About the Deployment Guide:

This deployment guide considers scenarios where all applications reside on a single server and provides tips and suggestions on configuring the server and get the basic functions of applications running. Discussions related to multi-server deployment can be found in the white papers such as the LMS 3.0 Large Scale Deployment Guide, available at http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html.

1.2. LMS 3.0 Applications

LMS 3.0 is the latest version of LMS, released on June, 2007. Here is a list of all the applications in LMS 3.0.

Figure 1. LMS 3.0 Applications



- Common Services 3.1

  Common Services provides a set of shared application services that are used by all LMS applications. Common Services 3.1 includes CiscoView 6.16, Integration Utility 1.7, LMS Portal 1.0 and CiscoWorks Assistant (CWA) 1.0. Both LMS Portal 1.0 and CiscoWorks Assistant (CWA) 1.0 are have just been introduced as new features in LMS 3.0.

  - LMS Portal 1.0 gives the user ability to customize information regardless of applications and view frequently used information in a common place. With LMS Portal, users do not need to navigate through several pages to obtain the information they need—instead, users can display application-related information as portlets, and customize the homepage to have all information on a single screen from all applications.
  - CiscoView 6.16 provides a “front panel” graphical display of Cisco devices, allowing users to easily interact with device components to change configuration parameters and monitor statistics.
  - Integration Utility 1.7 is an integration module that supports third-party network management systems.
  - CiscoWorks Assistant (CWA) 1.0 has the following features:
  - Workflows to improve usability of LMS applications.
  - Help to solve real business problems and overcome network inconsistencies.

- Resource Manager Essentials (RME) 4.1

  To support life cycle management, RME provides the ability to manage device inventory and audit changes, configuration files, software images—as well as Syslog analysis.

- Campus Manager (CM) 5.0

  Campus Manager provides the ability to visualize network topology, manage VLANs, detect network discrepancies, and provide Layer 2 and Layer 3 data and voice traces and end-host user information.

- Device Fault Manager (DFM) 3.0

  Device Fault Manager provides the ability to monitor device faults in real-time and determine the root cause by correlating device-level fault conditions. DFM can issue notifications of critical network conditions via email or pager. Fault History lets the user store and access historical information about alerts and faults that are detected and processed by DFM.

- Internetwork Performance Monitor (IPM) 4.0

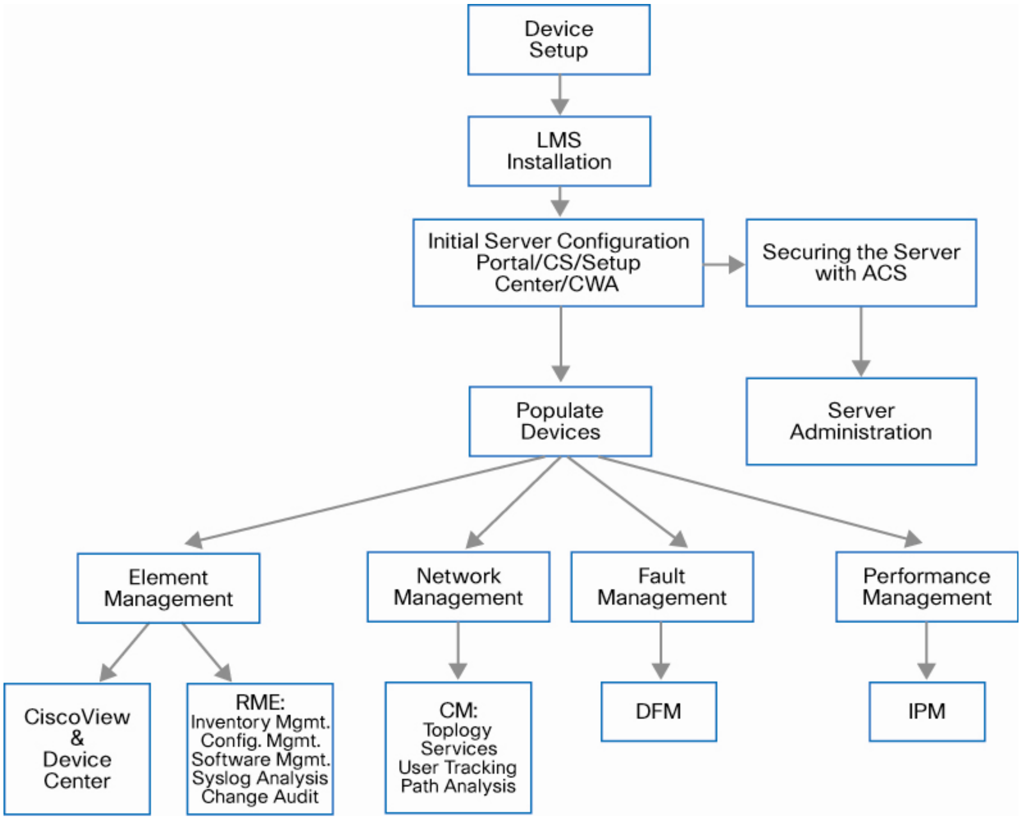
  Internetwork Performance Monitor measures network performance based on the synthetic traffic generation technology within the Cisco IOS® software, which is known as Cisco IOS IP SLA (Service Level Agreement). Using synthetic traffic by IPM gives the network manager a high degree of flexibility in selecting the end points in a network between which network performance will be measured. This flexibility makes IPM a highly effective performance-troubleshooting tool.

Compared to the previous version 2.6, LMS 3.0 added many new features to all existing applications, and two new applications, i.e. CiscoWorks Portal and CiscoWorks Assistant. The new features greatly improve the functions of LMS in performance, usability, scalability and reliability. See a list of the new features in the document “LMS30Win-readme.pdf” included with the LMS3.0 installation DVD.

1.3. LMS Workflow

Figure 1-2 summarizes the device and LMS setup workflow, which covers the whole lifecycle of LMS server from initial setup to ongoing operations. Subsequent chapters illustrate in details each of the steps mentioned in this workflow.

Figure 2. LMS Workflow



Step 1. The first step in the workflow is to turn on CDP, SNMP and credentials on the devices so that the devices can be discovered and managed.

Tools used: CLI tools such as console connection, Telnet, SSH and so on.

Step 2. The LMS server is installed and initial setup was done on the server. This includes setting up the dashboard for user interface, check/modify the default configurations for various applications, creating the user account with sufficient permissions to perform different tasks, and establish secure communication between the client and server and so on.

Tools used: LMS Portal, Common Services and Setup Center, CiscoWorks Assistant

For stronger security, Cisco recommends that you integrate LMS with the CiscoWorks Access Control Server (ACS). This will be discussed in details in chapter 4.

Step 3. After the devices and server are ready, we can populate the Device and Credential Repository (DCR) by either automatic discovery or manual import. During this process, all the access and credential information is stored into DCR so other applications can leverage the device information later. Some applications by default will automatically synchronize its own device repository with the DCR in Common Services. Others by default are set up to be manually populated.

Tools used: LMS Common Services, Campus Manage, Resource Management Essential, Device Fault Manager, Internetwork Performance Manager

Step 4. Once the Common Services DCR and the individual device database residing on different applications are populated, the administrator can start to perform his daily management tasks including:

- Element Management: Resource Management Essential (RME), Ciscoview, and Device Center
- Network Management: Campus Manager (CM)
- Fault Management: Device Fault Manager (DFM)
- Performance Management : Internetwork Performance Monitor (IPM)

Besides these steps, there is also ongoing work for the maintenance and administration of the LMS server. The administrator can backup and restore data on the LMS server. LMS also offers a rich set of command line tools to extract data from DCR and other individual application repositories.

2. Setting up Devices on the Network

The LAN Management Solution (LMS) 3.0 helps in managing Cisco devices on the network. However, before LMS 3.0 can function properly, the network devices that LMS interfaces with, must be set up correctly. The information provided in this chapter is a general description of the means and procedures recommended to ensure that the network devices are set up properly.

Note: This chapter provides a great deal of information on the device configuration procedures required to manage devices using CiscoWorks LAN Management Solution. Keep in mind that this document is not intended to be a comprehensive configuration guide for LMS 3.0. For additional LMS configuration details, please contact a Cisco Certified network engineer (if possible) and refer to pertinent documents that are posted on Cisco.com.

1) Prior to LMS deployment, in the case of Cisco IOS and CatOS devices all configuration changes must be saved to non-volatile memory (NVRAM) using the following commands:

```
write memory
```

or

```
copy running-config startup-config
```

Please note that the above command is provided to save pre-LMS deployment configuration changes. After LMS is deployed, configuration changes will be saved automatically where appropriate and no user intervention is required.

Also note newer versions of CatOS devices have separate running and startup configurations.

2.1. Device Setup Elements

This section describes each of the elements in the device setup, that correspondingly need to be addressed in LMS.

2.1.1. System Name

Each Cisco IOS device in the network must have a unique system name (sysname) in order to be managed. The system name is also populated in the Cisco Discovery Protocol (CDP) table. If there are duplicate system names on the network, LMS will discover only one device by that name on the network. On Cisco IOS devices, the domain name also affects the system name.

You can set up the system name using the following commands:

For Cisco IOS devices:

```
hostname <name>
```

For Cisco CatOS devices:

```
set system name <name>
```

2.1.2. Domain Name

You can set a domain name on a Cisco IOS or CatOS device. To set up the domain name, use the following commands.

For Cisco IOS devices:

```
ip domain-name <name>
```

For Cisco CatOS devices:

```
set system name <name with domain name>
```

2.1.3. SNMP Settings

LMS uses Simple Network Management Protocol (SNMP) Community strings to read and write information from and to the devices.

Note: LMS supports SNMP AuthNoPriv and AuthPriv mode of SNMP v3. AuthPriv is a new feature introduced in LMS 3.0.1.

Enabling SNMP v3 on Cisco IOS devices

To enable SNMP v3 on Cisco IOS devices, follow these steps:

- Create a View

```
snmp-server view campus oid-tree included
```

- Set the Security Model

```
snmp-server group cmtest v3 auth read campus write campus access access-list
```

- Create a user and authentication protocol to be used

```
snmp-server user cmtester campus v3 auth md5 password
```

- Create a group and associate the user with it

```
snmp-server user cmtester cmtest v3
```

Enabling SNMP v3 on Cat OS devices:

To enable SNMP v3 on Cat OS devices, follow these steps:

- Create a View

```
set snmp view campus 1.3.6.1 included nonvolatile
```

- Set the Security Model

```
set snmp access cmtest security-model v3 authentication read campus write campus
nonvolatile
```

- Create a user and authentication protocol to be used

```
set snmp user cmtester authentication md5 cisco123
```

- Create a group and associate the user with it

```
set snmp group cmtest user cmtester security-model v3 nonvolatile
```

Enabling SNMP v1/v2c on Cisco IOS devices:

To enable SNMP v1/v2c on Cisco IOS devices, follow these steps:

```
snmp-server community <read-community-string> ro
snmp-server community <write-community-string> rw
```

Enabling SNMP v1/v2c on Cisco CatOS devices:

To enable SNMP v1/v2c on Cisco IOS devices, follow these steps:

```
set snmp community read-only <read-community-string>
set snmp community read-write <write-community-string>
```

The community strings configured on the devices should match the community strings entered in DCR (Device Credential Repository) component in LMS.

Enabling traps in CatOS devices to be sent to a particular host

To enable traps in Catalyst OS devices to be sent to a particular host, enter this command:

set snmp trap 192.168.124.24 public

Enabling traps in IOS devices to be sent to a particular host using SNMP v2c version

To enable traps in IOS devices to be sent to a particular host using SNMP v2c, enter this command:

```
snmp-server host 192.168.124.24 traps version 2c public
```

In the above examples for enabling traps, the public community string is to help selective processing of traps on the trap receiving side.

Prerequisites for SNMPv3 Support on Spanning Tree Protocol:

For using various Spanning Tree features in devices running SNMPv3, you are required to make specific configurations on the devices for context name support. The additional command that needs to be configured for the three types of Spanning Tree Protocols are:

For type PVST:

```
set snmp access {group-name} security-model v3 authentication context vlan prefix
write {view-name} read {view-name} [volatile | nonvolatile]
```

For example:

```
set snmp access campusgroup security-model v3 authentication context vlan prefix
write campusview read campusview nonvolatile
```

For type MST:

```
set snmp access {group-name} security-model v3 authentication context mst prefix
write {view-name} read {view-name} [volatile | nonvolatile]
```

For example:

```
set snmp access campusgroup security-model v3 authentication context mst prefix
write campusview read campusview nonvolatile
```

For type MISTP:

```
set snmp access {group-name} security-model v3 authentication context mistp prefix
write {view-name} read {view-name} [volatile | nonvolatile]
```

For example:

```
set snmp access campusgroup security-model v3 authentication context mistp prefix
write campusview read campusview nonvolatile
```

Note: Context support is not available on XL series and 2950 switches, and Campus Manager will not fully work with them when they are configured to use SNMPv3.

For more information on SNMP settings, refer to:
http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml.

2.1.4. System Reload

After a software image distribution operation using Resource Manager Essentials (RME) is completed, RME will reload the device if specified in the Image Distribution job. RME will be able to reload any device (IOS or CatOS) only if an SNMP manager (in this case RME) is allowed to reset the agent.

The following command is needed on Cisco IOS devices only:

```
snmp-server system-shutdown
```

2.1.5. Command Line Prompts

To utilize the NetConfig capability to execute batch changes on devices, Cisco device command line prompts should meet the requirements described in this section.

Note: Customized prompts should also fulfill these requirements.

Cisco IOS devices:

- Login prompt should end with an angle bracket (>).

  For example: **Cisco>**

- Enable prompt should end with a pound sign (#).

  For example: **Cisco#**

Cisco CatOS devices:

- Enable prompt must end with (enable).

  For example: **Cisco(enable)**

2.1.6. Telnet/SSH

Telnet is one of the protocols that can be used by RME for configuration management. You can enable Telnet using the following commands.

Enable Telnet on Cisco IOS devices and CatOS devices, enter these commands:

```
line vty 0 4
password <password>
login
exec-timeout 0 0
```

Note: More than four VTY lines can be selected for login.

Different authentication on different VTY lines is not supported.

SSH provides for a secure communication with the device.

Cisco IOS

The following example configure SSH control parameters on a router running IOS:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

Catalyst OS

The following examples configure SSH in Cat OS:

```
(enable) set crypto key rsa 1024
(enable) set ip permit enable ssh
```

Note: For greater access control and logging facilities use TACACS. SSH configuration requires domain name to be configured.

2.1.7. Syslog Messages

Syslog messages can be enabled on Cisco devices to further use the capability of LMS, especially RME.

Cisco IOS Devices

```
Enable Syslog messages on IOS devices from global configuration mode:
logging on
logging <server-ip-address>
logging trap <logging-level>
```

Note: To limit the number of messages sent to the syslog servers, use the logging trap configuration command above.

Catalyst OS Devices

```
Enable Syslog messages on CatOS devices:
set logging server enable
set logging server <server-ip-address>
set logging level all <logging-level> default
```

2) The **`<server-ip-address>`** is the IP address of the LMS server. In case of multiple servers the server IP address entered here is the address of the RME server. In the case of remote Syslog Analyzer and Collector, this parameter is the IP address of the remote Syslog Analyzer and Collector.

2.2. Configuring Protocols

This section describes the basic configuration procedures for the following protocols:

- Cisco Discovery Protocol (CDP)
- Remote Copy Protocol (rcp)
- Secure Copy Protocol (scp)
- HTTP and HTTPS Protocols

2.2.1. Cisco Discovery Protocol

Cisco Campus Manager uses Cisco Discovery Protocol (CDP) to discover Cisco devices on the network. CDP is a Cisco proprietary layer 2 protocol that is media and protocol independent, and runs on all Cisco-manufactured equipment. A Cisco device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighbors. Since it is a layer 2 protocol, these packets (frames) are not routed. Campus Manager will use the following protocols in the respective technology—ILMI in LANE/ATM networks and ELMI on Stratacom FR Networks.

Enabling CDP on devices allows Campus Manager to learn information about neighboring devices, and to send SNMP queries to those devices. Campus Manager can discover the network topology only when CDP is enabled on devices.

Enable/Disable CDP on Cisco IOS devices:

CDP is enabled on Cisco IOS devices by default. To manually enable CDP capability on IOS devices use the following commands:

To enable CDP globally:

```
cdp run
```

To enable CDP on specific interfaces only:

```
cdp enable
```

Use the ***no*** command to disable CDP capability on Cisco IOS devices.

Enable/Disable CDP on Cisco CatOS devices:

CDP is enabled on Cisco CatOS devices by default. To enable CDP capability on CatOS devices use the following commands:

To enable CDP globally:

```
set cdp enable
```

To enable CDP on specific ports only:

```
set cdp enable [mod/port]
```

Use the **`set cdp disable`** command to disable cdp on CatOS devices.

3) Do not run CDP on links that don't need to be discovered by Campus Manager, for example, connection to the Internet, end host connection ports on access switches.

To protect from CDP DoS attacks, do not enable CDP on links that are connected to non Cisco devices.

`Note:` Certain non-Cisco devices support CDP. If you enable CDP on the Cisco devices connected to non-Cisco devices, they will appear on the Campus map.

For related information, please refer to the following URL, on configuring CDP on Catalyst 6500 Series switches: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00801a5b18.html.

2.2.2. Remote Copy Protocol (rcp)

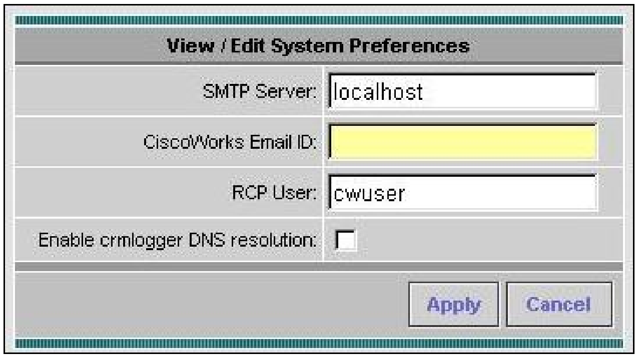
Remote Copy Protocol is one of the protocols that can be used by RME for configuration management and software image management. For LMS to be able to provide configuration and software management using rcp, it must be enabled on the devices.

rcp can be enabled only on devices running Cisco IOS using the following sample commands:

```
username cwuser password 7 000C1C0A05
ip rcmd rcp-enable
ip rcmd remote-host cwuser 172.17.246.221 cwuser enable
ip rcmd remote-username cwuser
```

`Note:` The value of `<remote-username>` and `<local-username>` entered in the device should match the "RCP User" value provided in the LMS server. The default value is cwuser. This value can be reset by traversing through the following user interface links in LMS server, **CWHP → Common Services → Server → Admin → System Preferences**.

Figure 3. System Preferences



2.2.3. Secure Copy Protocol (scp)

The Secure Copy feature was introduced in Cisco IOS 12.2(2)T.

To enable and configure a Cisco router for SCP server-side functionality, perform the following steps.

Table 1. SCRP Configuration

	Command	Purpose
Step 1	**enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**Router# configure terminal**	Enters global configuration mode.
Step 3	**Router (config)# aaa new-model**	Sets AAA authentication at login.
Step 4	**Router (config)# aaa authentication login default group tacacs+**	Enables the AAA access control system. Complete syntax: **aaa authentication login {default |** *list-name*} *method1* [*method2...*]
Step 5	**Router (config)# aaa authorization exec default group tacacs+**	Sets parameters that restrict user access to a network. The exec keyword runs authorization to determine if the user is allowed to run an EXEC shell; therefore, you must use it when you configure SCP. Syntax: **aaa authorization {network | exec | commands *level* | reverse-access | configuration} {default** | *list-name*} [*method1* [*method2...*]]
Step 6	**Router (config)# username superuser privilege 2 password 0 superpassword**	Establishes a username-based authentication system. You may skip this step if a network-based authentication mechanism—such as TACACS+ or RADIUS—has been configured. Syntax: **username** *name* **[privilege** *level*] {**password** *encryption-type encrypted-password*}
Step 7	**Router (config)# ip scp server enable**	Enables SCP server-side functionality.

2.2.4. HTTP and HTTPS

The Cisco IOS HTTP server provides authentication, but not encryption, for client connections. The data that the client and server transmit to each other is not encrypted. This leaves communication between clients and servers vulnerable to interception and attack.

Use the following command to enable HTTP mode.

```
ip http server
```

The Secure HTTP (HTTPS) feature provides the capability to connect to the Cisco IOS HTTPS server securely. It uses Secure Sockets Layer (SSL)[1] and Transport Layer Security (TLS) to provide device authentication and data encryption.

Note: As of LMS 2.5 release, HTTPS mode is supported only for VPN 3000 concentrators. To enable HTTPS mode in a VPN 3000 concentrator, access the following URL,

[1] This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more details please visit the following website: http://www.openssl.org/.

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a008015ce28.html#999607.

3. Cisco LAN Management Solution 3.0 Installation

Cisco LAN Management Solution installation is supported in both the Windows and Solaris operating systems.

3.1. Single Install Experience

In LMS 3.0, the installation framework is enhanced to support installation of multiple applications in the LMS bundle. You can install or upgrade the LMS applications from the single install image packaged in the LMS 3.0 DVD. Because everything is packaged in one bundle, customers do not need to worry about the sequencing order of installing the various components. When compared to the installation experience of previous LMS versions, the installation of LMS 3.0 on Windows and Solaris has been designed to be easier. The installation will finish in one coordinated effort, smoothly.

3.2. Checklist Before Installation

Before starting on the installation, we recommend that you:

- Back up your database if you have a previous version of LMS running. It is recommended to store backups on a separate partition or preferably on a separate disk. Backup partitions need to be large enough to store all application databases (for instance, RME, ANI, DFM and so on) as well as device configurations, software images and user accounts. The backup partition should allow for multiple revisions. It is recommended to verify all backups that may be needed in the future. Please refer to the document Data Migration Guide of LMS3.0 available on the installation DVD.
- Make sure your servers meet the hardware and software requirements (described in Sections 3.10 and 3.11 of this document).

We recommend that before installing the LMS 3.0 product, you register the product and receive a permanent license.

Note: The evaluation license only supports 100 devices and is for 90 days.

3.3. Licensing Process

To license your product, follow these steps:

Step 1. Register the LMS product with Cisco.com to get your license file. If you are a registered user of Cisco.com, get your license file from http://www.cisco.com/go/license.

Note: If you are not a registered user of Cisco.com, get your Cisco.com user ID from http://tools.cisco.com/RPF/register/register.do.

Once you have obtained your Cisco.com user ID, log on to http://www.cisco.com/go/license to get your license file.

Logging into Cisco.com allows your Cisco user profile information to auto-populate several product registration fields. Please note that the user authentication information is case sensitive.

Step 2. After you install LMS 3.0, copy the new license file to the CiscoWorks Common Services server into a directory with read permissions for the user name **`casuser`** or the user group **`casusers`**, such as **`.\NMSROOT`**.

Note: Do not save the license file on your desktop. **`casuser`** does not have read permission for the desktop folder. Even if you give **`casuser`** the read permission to the license file residing on your desktop, the **`casuser`** still can not access the file therefore license file can not be verified. You must give read permission to the folder in which the license file is located.

Step 3. Install the license file.

If you have obtained the LMS license before installation:

a. Select the first LMS application you wish to install (ideally Common Services 3.1), and when prompted:

- On Windows, select the first option button and click **Browse** and use the **File** browse window to locate the license file directory.
- On Solaris, select L for License File after you accept the Licensing Agreement and continue installing the application.

b. Click **Next** to install the license file.

If you have completed the LMS installation by entering the appropriate license number, or if you want to convert an evaluation copy to a licensed copy:

Go to the **CiscoWorks** Homepage and select **Common Services > Server > Admin > Licensing**. The License Administration page appears. Enter the path to the new license file in the License field, or click **Browse** to locate the license file that you copied to the server in Step 2.

The system verifies whether the license file is valid, and updates the license.

The updated licensing information appears in the License Information page.

If you encounter errors, repeat the steps to license your product.

Note: The License file obtained is platform independent and hence can be used in both Windows as well as Solaris operating systems.

3.4. SKUs of LMS 3.0

The licenses in LMS 3.0 are device-based for all applications. However, for Internetwork Performance Monitor (IPM) the license is based on the number of devices and the number of collectors.

You can select any one of the following four licenses of LMS 3.0:

- CW-LMS-3.0-100-K9

  Limits you to managing 100 devices in Resource Manager Essentials (RME), Campus Manager (CM) and Device Fault Manager (DFM) applications. IPM will support 300 collectors.

- CW-LMS-3.0-300-K9

  Limits you to managing 300 devices in Resource Manager Essentials (RME), Campus Manager (CM) and Device Fault Manager (DFM) applications. IPM will support 1000 collectors.

- CW-LMS-3.0-1.5k-K9

  Limits you to managing 300 devices in Resource Manager Essentials (RME), Campus Manager (CM) and Device Fault Manager (DFM) applications.

- CW-LMS-3.0-5K-K9

  Limits you to managing 5,000 devices in Resource Manager Essentials (RME) and Campus Manager (CM), and 1500 devices in Device Fault Manager (DFM) applications. IPM will support 2000 collectors.

- CW-LMS-3.0-10K-K9

  Limits you to managing 10,000 devices in Resource Manager Essentials (RME), 5K devices for Campus Manager (CM) and 1500 devices in Device Fault Manager (DFM) applications.

In IPM, the license details are:

- For every 100 devices IPM will allow 300 collectors

- For every 300 devices IPM will allow 1000 collectors
- Supports maximum of 5k devices and 2000 collectors

However, the number of devices that can be managed in a single server depends on your server configuration.

3.5. New Installation Instruction for LMS 3.0

Thanks to the single package installation design, the LMS 3.0 installation program on both Windows and Solaris is both user friendly and fail-proof. In Solaris, follow the interactive instructions once you execute setup.sh. For Windows-based installations, follow the interactive instructions on executing setup.exe.

For step-by-step installation instructions, please refer to the white paper ***"Installing and Getting Started with LMS 3.0"*** on the installation DVD.

3.6. Upgrade and Migration from Legacy LMS Versions

Direct upgrade from LMS 2.5.1 and LMS 2.6 are supported. Remote upgrade or migration to LMS 3.0 is supported from LMS 2.2, LMS 2.5, LMS 2.5.1 and LMS 2.6.

For more information on upgrade and migration, see ***Installing and Getting Started with CiscoWorks LAN Management Solution 3.0 (Maintenance Kit)*** and ***Data Migration Guide for CiscoWorks LAN Management Solution 3.0*** on the installation DVD.

Installation Log

The installation log exhaustively logs operations performed during the installation process. In case the installation is unsuccessful or problematic, you can review the installation log for error messages, if any.

- Solaris

  In Solaris, the installation log is located at /var/tmp/Ciscoworks_install_YYYYMMDD_hhmmss.log for LMS 3.0 installation, where YYYYMMDD denotes the year, month and date of installation and hhmmss denotes the hours, minutes and seconds of installation.

`For example:/var/tmp/Ciscoworks_install_20060721_182 205.log`

- Windows

  In Windows, the installation log is located in the root directory of the drive where the operating system is installed. Each installation creates a new log file.

  For LMS 3.0, the installation log file is C:\Ciscoworks_install_YYYYMMDD_hhmmss.log, where YYYYMMDD denotes the year, month and date of installation and hhmmss denotes the hours, minutes and seconds of installation.

`For example: C:\Ciscoworks_install_20060721_182205.log`

3.7. Verifying the LMS 3.0 Installation

After you install the CiscoWorks LMS 3.0 on Windows, you must verify the installation. To do this:

Step 4. Step 1: Launch CiscoWorks: http://server_name:port_number

where server_name is the name of the CiscoWorks Server and port_number is the TCP port used by the CiscoWorks Server.

In normal mode (HTTP), the default TCP port for CiscoWorks Server is 1741. When SSL (HHTPS) is enabled, the default TCP port for the CiscoWorks Server is 443.

You can change the HTTPS port number of CiscoWorks Server during the installation. See ***Installing and Getting Started with LAN Management Solution 3.0*** for more information.

Step 5. Select **Common Services > Software Center > Software Update**.

The Software Updates window appears. The following entries appear in the Products Installed table for each application that you have installed:

Figure 4. Installed Components

Products Installed

Showing 1-9 of 9 records

		Product Name	Version With Patch Level	Installed Date
1.		CiscoWorks Common Services	3.1.0	08 Mar 2007, 11:47:05 PST
2.		Campus Manager	5.0.0	08 Mar 2007, 11:47:06 PST
3.		CiscoView	6.1.6	08 Mar 2007, 11:47:07 PST
4.		CiscoWorks Assistant	1.0.0	08 Mar 2007, 11:47:07 PST
5.		Device Fault Manager	3.0.0	08 Mar 2007, 11:47:08 PST
6.		Internetwork Performance Monitor	4.0.0	08 Mar 2007, 11:47:09 PST
7.		Integration Utility	1.7.0	08 Mar 2007, 11:47:10 PST
8.		LMS Portal	1.0.0	08 Mar 2007, 11:47:11 PST
9.		Resource Manager Essentials	4.1.0	08 Mar 2007, 11:47:11 PST

3.8. Third Party Tools and Software Changes

Cisco supports HP OpenView 7.5.x and IBM NetView 7.1.x. On the client side, Firefox 2.0 and Internet Explorer 7.0 browsers are supported in this release.

3.9. Post-installation Tasks

The first step after installing the products is to check for any updates for service packs. Service packs can be downloaded from either Cisco.com or as a Software Update (accessed from **Common Services → Software Center → Software Update**).

Note: There is a link on LMS Portal for the latest announcements regarding software update and related topics.

3.10. System Requirements

Tables 1 and 2 list the CiscoWorks LMS 3.0 system requirements.

Table 2. System Requirements—Server

Part# (SKU)	Solaris	Microsoft Windows
CWLMS-3.0-100-K9	Not supported	Intel Pentium 4 at 2.6 GHz for 1 CPU with 2 GB RAM memory and 4 GB swap space
CWLMS-3.0-300-K9	SunFire v210 - 1 UltraSPARC IIIi CPU at 1.3 GHz with 2 GB RAM memory and 4 GB swap space on Solaris 9. SunFire v210 - 1 UltraSPARC IIIi CPU at 1.3 GHz with 4 GB RAM memory and 8 GB swap space on Solaris 10.	Intel Pentium 4 at 2.6 GHz for 1 CPU with 2 GB RAM memory 4 GB swap space.
CWLMS-3.0-1.5K-K9	SunFire v440 - 2 UltraSPARC IIIi CPU at 1.28 GHz with 4 GB RAM memory t and 8 GB swap space.	Windows 2003 Server Standard and Enterprise Editions with 2 Intel Xeon CPU at 3.66 GHz and 4 GB RAM memory and 8 GB swap space.
CWLMS-3.0-5K-K9	Dedicated Servers per product in LMS Suite : SunFire v440 - 4 UltraSPARC IV CPU at 1.03 GHz with 4 GB RAM memory and 8 GB swap space.*	Dedicated Servers per product in LMS Suite: Windows 2003 Server Standard and Enterprise Editions 4 Intel Xeon CPU at 3.66 GHz with 4 GB RAM memory and 8 GB swap space.*
CWLMS-3.0-10K-K9	Dedicated Servers per product in LMS Suite: SunFire v440 - 4 UltraSPARC IV CPU at 1.03 GHz with 4 GB RAM memory and 8 GB swap space.*	Dedicated Servers per product in LMS Suite:* Windows 2003 Server Standard and Enterprise Editions 4 Intel Xeon CPU at 3.66 GHz with 4 GB RAM memory and 8 GB of swap space.*
Minimum Disk	80GB Disk Space	80Gb Disk Space
Processor Support	• UltraSPARC III (280R, 480R) • UltraSPARC IIIi processor (V240, V250, V440) • UltraSPARC IV processor (V490, V890) • UltraSPARC IV+ processor (V490, V890) • UltraSPARC T1 processor (Sun Fire T1000 Server, Sun Fire T2000 Server)	Intel Processors • Intel Xeon processor (Dual Core) • Intel Core Duo processor T2600 - T2300 • Intel Pentium processor Extreme Edition 965 (Dual Core) • Intel Pentium D processor 960 (Dual Core) • Intel Pentium 4 processor with Hyper-Threading Technology AMD Processors • Dual-Core AMD Opteron Processor • AMD Opteron Processor • AMD Athlon 64 FX Processor • AMD Athlon 64 X2 Dual-Core

*Please note that for solution servers running all products of the LMS 3.0 suite, the maximum scalability limit is 3,000 devices with the indicated hardware requirements configured with 8 GB RAM memory and 16 GB swap space.

Table 3. System Requirements—Server

Disk space	Solaris: 1 GB swap space Windows: 1 GB virtual memory
Memory	512 MB
Hardware and software	IBM PC-compatible system with at least Intel Pentium IV processor running, • Windows 2000 Professional with Service Pack 4 • Windows 2000 Server with Service Pack 4 • Windows 2000 Advanced Server with Service Pack 4 • Windows Server 2003 Standard and Enterprise Edition with Service Pack 1 • Windows 2003 R2 Server Standard and Enterprise Editions • Windows XP with Service Pack 2 Solaris 8, Solaris 9 (English and Japanese only)
Browser	Internet Explorer 6.0. Service Pack 2—Windows 2000, Windows Server 2003 Internet Explorer 7.0 Firefox 2.0

3.11. Recommendations for Installation of LMS 3.0 Applications

Here are a few caveats for the installation:

- LMS Portal 1.0 and CiscoWorks Assistant 1.0 will be selected by default along with Common Sevices 3.1.
- Common Services 3.1, LMS Portal 1.0, and CiscoWorks Assistant 1.0 must be installed and uninstalled together.
- Integration Utility (NMIM) 1.7 can be installed independently without installing the default applications Common Services 3.1, LMS Portal 1.0, and CiscoWorks Assistant 1.0.
- Applications can be selected simultaneously for a reinstallation during new or upgrade install of LMS 3.0.

3.12. Ports Used by LMS Applications

Table 4. LMS Application Port Usag

Protocol	Port	Service Name	Application(s)	Direction of Establishment of Connection
ICMP		Ping	RME, CM, and DFM	Server to Device
TCP	22	Secure Shell (SSH)	CiscoWorks Common Services and RME	Server to Device
TCP	23	Telnet	CiscoWorks Common Services,	Server to Device
TCP	49	TACACS+ and ACS	CiscoWorks Common Services, RME, CM, and DFM	Server to ACS, Device to ACS
TCP	80	HyperText Transfer Protocol (HTTP)	CiscoWorks Common Services, CiscoView	Client to Server
TCP	514	Remote Copy Protocol	CiscoWorks Common Services	Server to Device
TCP	514	rsh Daemon	RME	Server to Device
TCP	1683	Internet Inter-ORB Protocol (IIOP)	CiscoWorks Common Services, and CM	Client to Server
TCP	1684	IIOP	CiscoWorks Common Services, and CM	Server to Client
TCP	1741	CiscoWorks HTTP Protocol	CiscoWorks Common Services, CiscoView, and RME	Client to Server
TCP	443	CiscoWorks SSL Protocol	CiscoWorks Common Services	Client to server Server to server
TCP	1742	SSL/HTTP Port	CiscoWorks Common Services	Client to Server

TCP	1783	IIOP for IPM Gatekeeper	IPM	Client to Server
TCP	1784	IIOP for IPM Gatekeeper	IPM	Server to Client
TCP	8088	HIOP	CiscoWorks Common Services	Server to Client Client to Server
TCP	9002	DynamID authentication (DFM Broker)	DFM	Client to Server
TCP	9088	HIOP port for IPM gatekeeper	IPM	Server to Client Client to Server
TCP	42352	ESS HTTP (Alternate port is 44352/tcp)	CiscoWorks Common Services	Client to Server
TCP	44342	IPM Name Server (OSAGENT)	IPM	Client to Server
UDP	69	Trivial File Transfer Protocol (TFTP)	CiscoWorks Common Services and RME	Server to Device Device to Server
UDP	161	Simple Network Management Protocol (SNMP)	CiscoWorks Common Services, CiscoView, RME, CM, andDFM	Server to Device
UDP	162	SNMP Traps (Standard Port)	CiscoWorks Common Services, and DFM	Device to Server
UDP	514	Syslog	CiscoWorks Common Services and RME	Device to Server
UDP	9000	CSlistener (DFM server if port 162 is occupied)	DFM	Client to Server
UDP	16236	UT Host acquisition	CM	Device to Server

4. Initial Setup of the LMS 3.0 Server: Portal, Setup Center and Common Services

This chapter will guide you through the initial setup of the LAN Management Solution (LMS) server. This chapter provides setup information on the LMS Portal, LMS Setup Center and Common Services.

The tools we will use are LMS Portal, Setup Center and Common Services. LMS Portal is the dashboard of the server. LMS Setup Center is a brand new feature in LMS 3.0. It is the centralize location where the user can get done with most of the application settings including Common Services, Resource Management Essential, Campus Manager and Device Fault Manager. Common Services is the core of the LMS server and needs to be configured properly so other applications can run smoothly.

4.1. LAN Management Solution Portal

In previous version of LMS, users have had to go through multiple layers of user interface (UI), (sometimes through 3-4 mouse clicks), to reach status information or the desired data. Moreover there was no customization supported. Users could not customize the desktop for easy/quick access to frequently accessed data and/or functionality, which led to usability challenges.

Starting with LMS 3.0, the Cisco LMS Portal is introduced as the dashboard to provide Zero-Click Access to network data and management functionality, significantly improving the usability of LMS. Through this portal, you can easily launch all the functions offered by LMS and have direct access to the status of your LMS servers, network devices and network topologies.

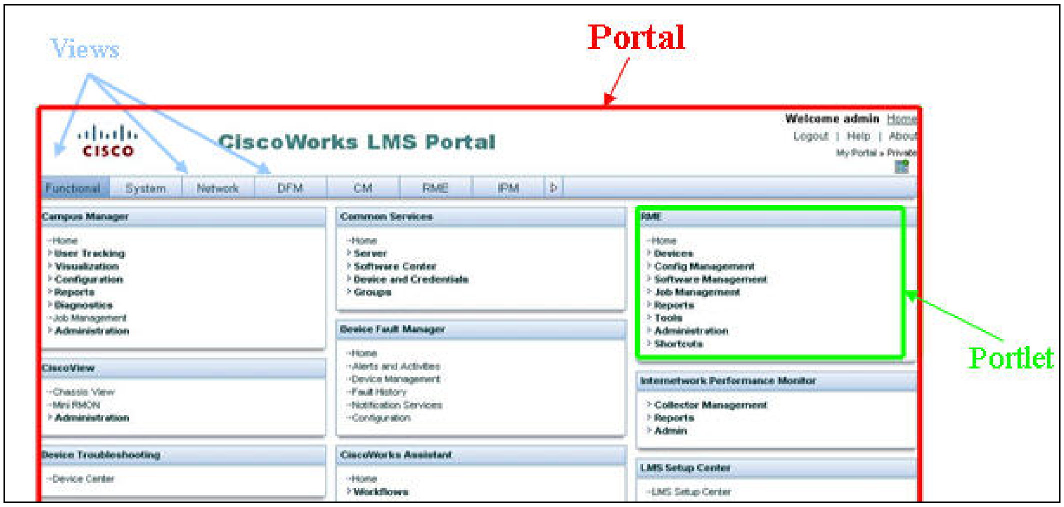
The primary benefits of CiscoWorks LMS Portal are:

- Customization: You can personalize the CiscoWorks Homepage using the drag-and-drop, add, edit, and remove features
- Information available in a single-click: Reduced number of mouse-clicks that provide for easy and quick access to the frequently viewed vital information, for the applications in the CiscoWorks LMS suite.
- Multi-server support: Lists all of the portlets based on the applications installed on remote servers.
- Lightweight GUI: Eliminates the need to install any plug-ins to launch the application.

4.1.1. Components of the LMS Portal

When the user logs into the LMS server first time, the fist thing the user views is the LMS Portal. The LMS Portal has three different components:

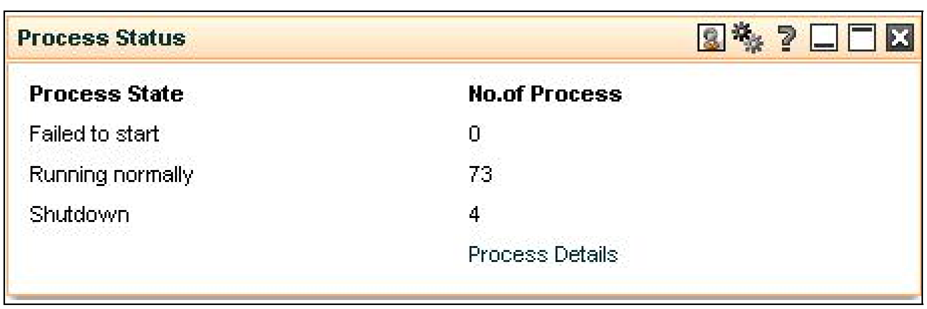
Figure 5. Portal Layout



- The Portal: The Portal serves as the overall container which contains a set of views. You can set up the Portal to manage a single server or multiple servers.
- Views: Views are organized tabs which contain a set of Portlets. LMS 3.0 comes out of the box with eight views, namely Function, System, Network, DFM, CM, RME, and IPM. You can add or delete Views except the Function View. You can set up public Views that everyone can see, or set up a private View only for yourself.
- Portlets: Portlets are individual pieces of data pointing to an application function or status report. You can add or remove portlets to customize the Views except the Function View. The Portlet list is based on the applications installed and registered. The visibility of Portlet contents is based on the user’s roles and privileges.

4) Each Portlet contains six icons on the top. These icons will be visible only when you move the mouse over the right corner of each Portlet.

Figure 6. Portlet



4.1.2. Customize the Portal

LMS 3.0 offers tremendous flexibility for the user to customize the look and feel of the Portal. You can,

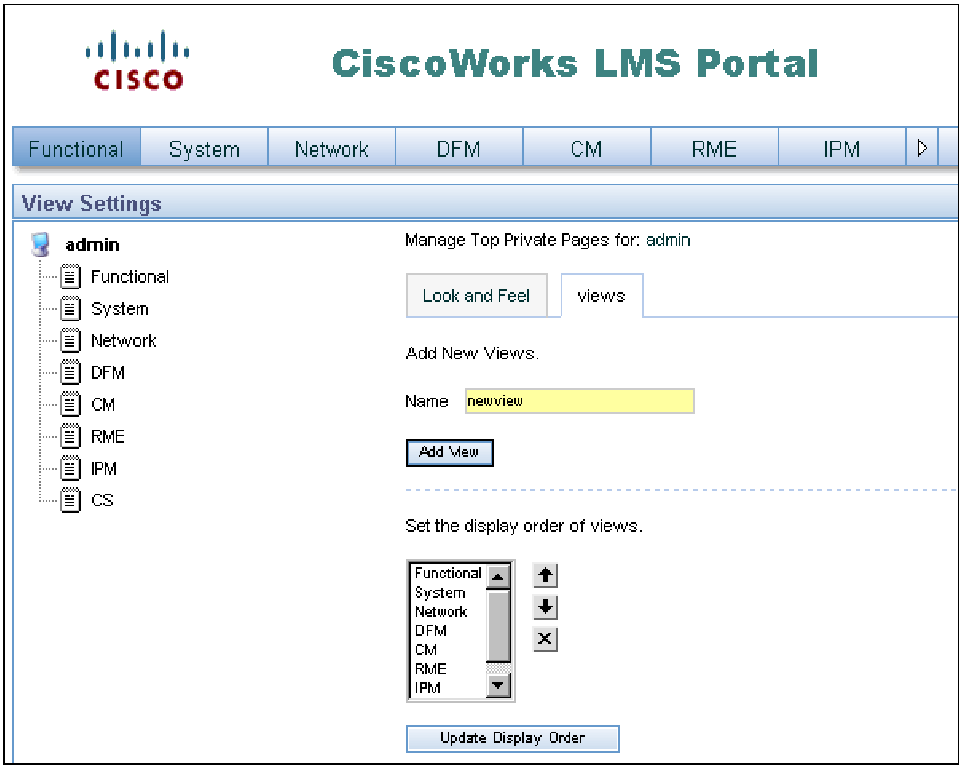
- Add a view

Adding a new view helps you to consolidate information specific to a particular function, such as troubleshooting. It also allows you to group data from different LMS applications on a single page.

To add a view:

Step 6. Go to the CiscoWorks LMS Portal home page and click Manage View in the upper right corner of the page . The View Settings Portlet appears.

Figure 7. Add View



Step 7. Click the root node icon in the tree structure on the left. In this case, it is **admin**..

Step 8. Click View.

Step 9. Enter the view name in the **Name** field

Step 10. Click **Add View**. The View name is added to the tree structure on the left and shows on the dashboard as a new tab.

On the same screen, you can update the display order if you want to move your View to more accessible location on the screen.

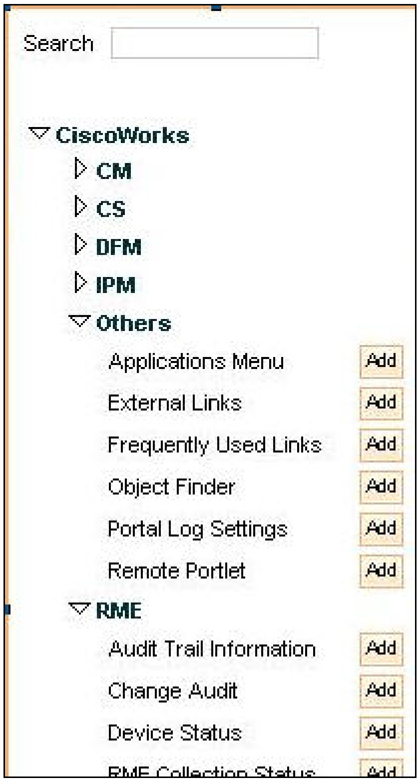
Note:

- After you add a View, you can customize it by either duplicating from an existing View as template or create it from afresh by adding your own Portlet.
- To duplicate from an existing View as template, click on your newly created View, and click on **View**, then choose the template and **Save**. Following this step, you can go to the View and choose to add or delete individual Portlets.

Customize a view

To start from a blank view, click on the tab for the new View, and click on the **Add Portlet** button, **.** The Portlet selector appears.

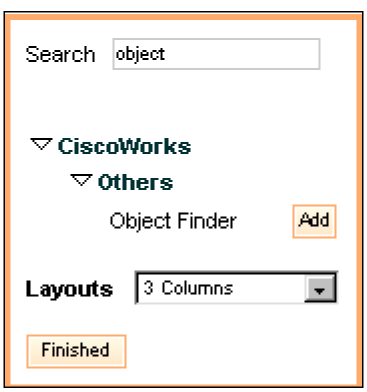
Figure 8. Add Portlet



From this selector, you can choose the Portlet you want to add to your View by browsing the available categories.

5) You can search a Portlet by using the search box on the top. For example, you can search for “Object Finder”.

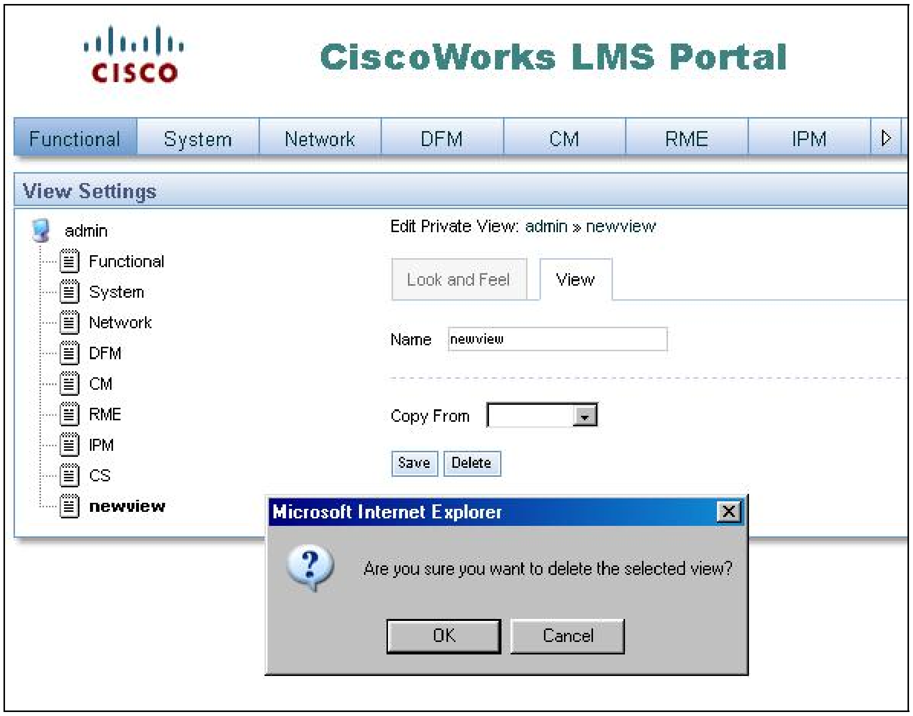
Figure 9. Search for Portlet



Deleting a View

To delete a view, Edit the view and choose the view to be deleted.

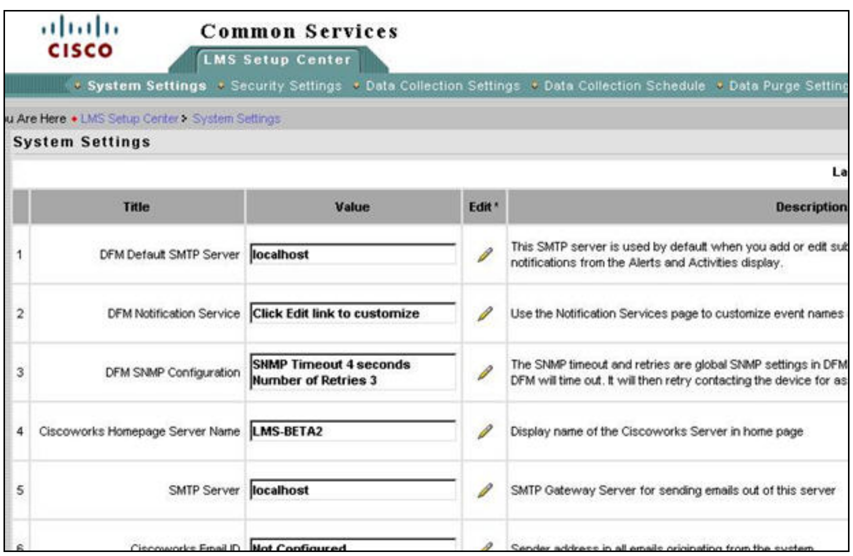
Figure 10. Delete a view



4.2. CiscoWorks LMS Setup Center

CiscoWorks LMS Setup Center is a centralized area that displays the CiscoWorks system configurations. One of the most common observations from new CiscoWorks users is that it is difficult to remember which application menu to navigate when changing a system setting. CiscoWorks LMS Setup Center was designed to provide shortcuts to those options that may be difficult to find. It allows you to configure the necessary server settings, immediately after installing the CiscoWorks LMS software. The Edit icon displayed for each setting takes you to the respective application page to configure the settings.

Figure 11. LMS Setup Center



The configurations in CiscoWorks LMS Setup Center are grouped into the following categories:

- **System Settings:** The configuration that the system needs to function effectively
- **Security Settings:** The security-related settings for the product
- **Data Collection Settings:** The settings necessary for collecting data from the devices
- **Data Collection Schedule:** The schedule settings for collecting the data from the server
- **Data Purge Schedule:** The configurations that are necessary for the device to purge data

The settings specific to all applications including CiscoWorks Common Services, CiscoWorks RME, CiscoWorks Campus Manager, and Device Fault Management are grouped within these five categories, and enables you to configure them in a common space.

Note: If an application is not installed, the corresponding entries are not available.

4.2.1. System Settings

This category lists the configurations that are necessary for the system to function.

The System Settings specific to all the applications are grouped under this category. If a CiscoWorks application is not installed, the corresponding entries are not displayed. To launch the System Settings page, click the **System Settings** tab from CiscoWorks Home Pages LMS Setup Center application. The **System Settings** page displays the name of the settings, their value and brief description. Each entry has an **Edit** icon. When you click the **Edit** icon for a specific **System Setting**, the corresponding **Settings** page appears.

4.2.2. Security Settings

The security related configurations of all CiscoWorks applications are grouped under this category. If a CiscoWorks application is not installed, then the corresponding entries are not displayed.

To launch the **Security Settings** page, click the **Security Settings** tab from the **LMS Setup Center** application. The **Security Settings** page displays the name of the settings, their value and brief description. Each entry has an **Edit** icon. When you click the **Edit** icon for a specific **Security** setting, the corresponding **Security Settings** page opens.

4.2.3. Data Collection Settings

This category lists the settings to collect the data from the devices. The **Data Collection** settings specific to all CiscoWorks applications are displayed here. If an application is not installed, the corresponding entries are not displayed.

To launch the **Data Collection Settings** page, click the **Data Collection Settings** tab from the **LMS Setup Center** application. The **Data Collection Settings** page displays the name of the settings, their value and brief description. Each entry has an **Edit** icon.

When you click the **Edit** icon for a specific **Data Collection** setting, the corresponding **Data Collection Settings** page appears.

4.2.4. Data Collection Schedule

This category lists the schedule settings for the server for data collection. The **Data Collection Schedule** settings for all CiscoWorks applications are under this category. If a CiscoWorks application is not installed, the corresponding entries are not displayed.

To launch the **Data Collection Schedule** page, click the **Data Collection Schedule** tab from the **LMS Setup Center** application. The **Data Collection Schedule** page displays the name of the settings, their value and brief description. Each entry has an **Edit** icon. When you click the **Edit** icon for a specific **Data Collection Schedule** setting, the corresponding configuration page opens.

4.2.5. Data Purge Schedule

This category lists the configurations for the device to purge data. The **Data Purge** settings specific to all CiscoWorks applications are under this category. If a CiscoWorks application is not installed, the corresponding entries are not displayed.

To launch the **Data Purge Schedule** page, click the **Data Purge Schedule** tab from the **LMS Setup Center** application. The **Data Purge Settings** page displays the name of the settings, their value and brief description. Each entry is accompanied by an **Edit** icon. When you click the **Edit** icon for a specific **Data Purge Schedule**, the corresponding configuration page opens.

4.2.6. RME Protocol Setup

One of the most important settings is the RME protocol setup. RME uses various protocols for configuration and software management. Network administrators can assign the protocols to be used in RME for Configuration Management and Software Management.

Configuration Management

You can set the protocols and order for Configuration Management applications such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations. The available protocols are: Telnet, TFTP (Trivial File Transport Protocol), RCP (remote copy protocol), SSH (Secure Shell), SCP (Secure Copy Protocol), HTTPS (Hyper Text Transfer Protocol Secured)

To setup protocol ordering for Configuration Management, go to **Resource Manager Essentials → Administration → Config Mgmt.**

Protocol ordering can be setup for different config applications (Archive Management, ConfigEditor and NetConfig) by selecting the application from the **Application Name** drop-down list. Select the protocol order by **Add** and **Remove** buttons on the screen and click **Apply**.

6) For secure communication between the server and device use SSH.

For Software Management protocol ordering, click on **Software Mgmt** and select **View/Edit Preferences** from the Table of Contents. Use **Add** and **Remove** buttons for selecting the protocol order.

Software Image Management

Software Management attempts downloading the software images based on the protocol order specified. While downloading the images, Software Management uses the first protocol in the list. If the first protocol in the list fails, these jobs use the second protocol and so on, until Software Management finds a transport protocol for downloading the images. The supported protocols are: RCP, TFTP, SCP and HTTP.

In the **View/Edit Preferences** dialog box (**Resource Manager Essentials → Administration → Software Mgmt → View/Edit Preferences**) you can define the protocol order that Software Management has to use for software image download. Use **Add** and **Remove** buttons for selecting the protocol order.

4.3. Common Services Setup

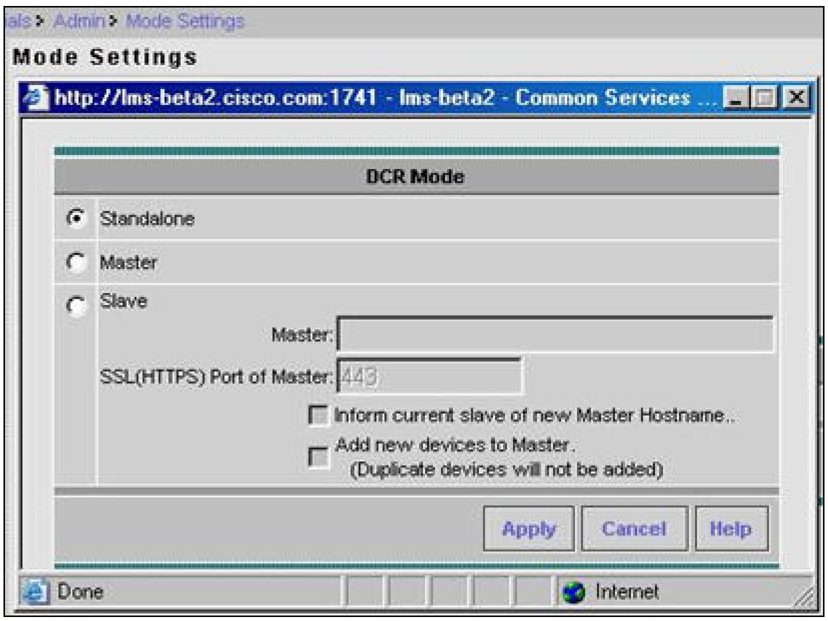
Common Services is the core component of the LMS applications relied by other applications to perform their tasks. Common Services maintain the database for Device Credential Repository which stores all the devices information to be managed.

4.3.1. General Server Setup

DCR Mode

This paper discusses LMS server as a standalone server. As you become more familiar with the LMS features, you can set up multiple LMS servers to work together in a Master/Slave scenario. To change the mode of the LMS server, go to **CS/Device** and **Credentials/Admin/Mode Settings.**

Figure 12. DCR Mode



Setting Up CiscoWorks Home Page

You can configure or change the CiscoWorks Home Page settings.

To modify CiscoWorks Home Page settings:

1. Select **Common Services/ Server/HomePage Admin/Settings**.
2. Enter a name for the CiscoWorks Server in the **Homepage Server Name** field.
3. Check the **Display Servername With Browser Title** checkbox to display the name of the CiscoWorks Server along with the browser title.
4. Select the **Hide External Resources** check box to hide the **Resources** and CiscoWorks Product Updates panels in the home page.
5. Enter the display name you want for **Third Party** tools in the **Custom Name for Third Party** field.
6. Enter the display name you want for **Custom tools/homegrown** tools in the **Custom Name for Custom Tools** field.

7. Select a value from the **Urgent Messages Polling Interval** drop-down list to set the polling interval for messages.

To disable this feature, select **Disable** from the drop-down list. The values are 1 Minute, 5 Minute, 10 Minutes and DISABLE.

The time you set here decides the polling interval for disk watcher messages and messages you want to broadcast using the Notify Users features. Disk watcher is a utility that monitors the file system. If the file system size goes above 90 percent, it displays an alert to the dashboard of logged-in CiscoWorks users. You can use this to monitor critical file systems.

Click **Update**. You can update any one of the above settings by clicking **Update**. If you have changed the homepage Server name, a popup window appears prompting you to confirm whether you want to use this name in Provider Group name.

- Click **OK** if you want the name to be suffixed to the Provider Group name.
- You need to restart Daemon Manager for the Provider Group name change to take effect.

Displaying CiscoWorks Server Name with Browser Title

Displaying CiscoWorks Server name with browser title helps you to identify the server from which the application window is launched especially in a multi-server setup and Single Sign-On based setup.

You can enable or disable the option of displaying the CiscoWorks Server name along with the browser title. When you choose to display the server name in the browser title, the browser window displays the title in the following format:

Hostname - ApplicationWindowTitle

Here *Hostname* is the name of the CiscoWorks Server and *ApplicationWindowTitle* is the title of application window launched from CiscoWorks Server.

For example, if the name of your CiscoWorks Server is **Imsdocultra**, then the title of the CiscoWorks Home Page would be displayed as **Imsdocultra - CiscoWorks**. If you launch **Common Services** from the CiscoWorks Home Page, the title of the Common Services Home window would be displayed as **Imsdocultra - Common Services Home**.

You can also enable or disable the display of server name with the browser title by changing the configurations in a properties file.

Configure the **uii-windows.properties** file located at ***NMSROOT*/lib/classpath** to:

- Enable or disable the option of displaying server name with browser title
- Change the format of display from *Hostname - ApplicationWindowTitle* to
- *ApplicationWindowTitle - Hostname* and vice versa
- Replace hyphen (-) with any other delimiter except empty spaces
- Trim the spaces between the Hostname, delimiter and Application window title

Registering Applications with CiscoWorks Home Page

Using this feature, you can register CiscoWorks applications on local or remote servers. You need to enter application instance attributes (host, port, and protocol). Other information such as AppName, URLs available are already defined by the application in a template.

During registration you are prompted to select an application template and then register with CiscoWorks Server. The registration enables the application to be integrated with other applications based on the template definition. It also helps application launch points to be displayed on CiscoWorks Home Page.

To view the registered applications:

1. Select **Common Services → Server → HomePage Admin → Application Registration**.
2. View the list of registered applications in the **Registered Applications** dialog box.

To register a new application:

1. Click Register in the **Registered Applications** dialog box. A wizard guides you through the process.
2. Choose the location for registration. You can select **Register from Templates** or **Import from Other servers**.

To register from Templates:

1. Select the **Register from Templates** radio button and click **Next**.
2. Select the radio button corresponding to the Template you require and click Next.
3. Enter the Server attributes in the Server attributes dialog box and click Next.
4. Click **Finish**.

Importing From Other Servers

You must perform the following tasks before importing application registrations from other servers. This is to ensure a secure environment for importing registrations.

- Create self signed certificates for the local and remote servers (if not already done).
- Add remote server's certificate to the local server. See Setting up Peer Server Certificate for details.
- Restart the local server.
- Create a Peer Server user on the remote server. Configure this user a System Identity user in the local server. See Setting up Peer Server Account and Setting up System Identity Account for details.

To import from other servers:

1. Select the Import from Others Servers radio button and click **Next**.
2. Enter the **Server Name, Server Display Name**, and the secure **Port Number** in the Import Server's **Attributes** dialog box. Click **Next**.
3. Select one or more applications from the list to import into the CiscoWorks Server. Click **Next**.
4. The **Import Registration Summary** window displays a summary of the information you entered. Click **Finish**.

When the browser-server security mode of the remote server is changed from non-SSL to SSL or from SSL to non-SSL, you should de-register the applications imported from that server and register them again.

Viewing Registered Application Information

The Application Registration screen shows the list of registered applications. You can view the application name, version, host name and description for each of the registered applications. This page shows the applications that are registered in the local server as well as any other applications whose templates are imported from other servers.

The version in this screen shows the major version of the applications. In order to know the version with patch level, go to **Software Center → Software Updates**. The **Software Updates** page shows the version with patch level information. The patch level information is only available for the applications installed in the local server.

Registering Links with CiscoWorks Home Page

You can add additional links to CiscoWorks Home Page for Custom tools and home grown tools, and third party applications such as HP OpenView. The links appear under the Third Party or Custom Tools on the LMS Portal as you have specified it.

To register links with CiscoWorks Home Page:

1. Select **Common Services → Server → HomePage Admin → Links Registration**. The Links Registration Status page appears.
2. Click **Register**. The **Enter Link Attributes** dialog box appears.
3. Enter the **Link Name** and the **URL**.
4. Select the radio button corresponding to **Third Party** or **Custom Tools** to set the display location.
5. Click **OK**.

4.3.2. Securing LMS Servers

Accessing LMS server securely via SSL

By default LMS server is accessed via http at http://server:1741. Common Services provides secure access between the client browser and management server by using SSL (Secure Socket Layer). SSL encrypts the transmission channel between the client, and server.

Note: SSL is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys.

To enable Browser-Server Security:

1. Go to the CiscoWorks Home Page, and select **Common Services → Server → Security → Browser-Server Security Mode Setup**.
2. Select the **Enable** option to enable SSL.
3. Click **Apply**.
4. Log out from your CiscoWorks session, and close all browser sessions.
5. Restart the Daemon Manager from the CiscoWorks Server CLI:

On Windows:

a. Enter net stop crmdmgtd

b. Enter net start crmdmgtd

On Solaris:

c. Enter /etc/init.d/dmgtd stop

d. Enter /etc/init.d/dmgtd start

6. Restart the browser, and the CiscoWorks session.

After this change has been implemented, you can log into the server securely via SSL by going to https://server:443. Note the port number has been changed from 1741 to 443.

Setup Local User

To create a local user, go to the CiscoWorks Home Page and select **Common Services → Server → Security → Local User Setup**. Click on **Add** to start the process. Fill in the form for user name, password, and chose the user role.

Note: By default, the minimum character limit for CiscoWorks local username is 5 characters. To add a local username with less than five characters, change the entry for "validateUser" to "false" in the **NMSROOT/lib/classpath/ss.properties** file.

7) You can only create one user at a time. To create local users in bulk, use the CLI tool. Refer to the help file and search on **Setting Up Local Users Through CLI**.

System administrators determine user security levels when users are granted access to CiscoWorks. When users are granted logins to the CiscoWorks application, they are assigned one or more roles.

Table 5. User Roles

Level	Description
0	Help Desk
1	Approver
2	Network Operator
4	Network Administrator
8	System Administrator
16	Export Data

A role is a collection of privileges that dictate the type of system access you have. A privilege is a task or operation defined within the application. The set of privileges assigned to you, defines your role and dictates how much and what type of system access you have.

The user role or combination of roles, dictates which tasks are presented to the users. The following table shows the security levels.

For information on tasks that can be performed with each role, you can generate a permissions report. To generate a permissions report:

1. Go to the CiscoWorks Home Page and select **Common Services → Server → Reports**.
2. Select **Permissions Report** from the **Available Reports** pane.
3. Click **Generate Report**.

Note: The permission report can only show the privilege details of the local users. If a user is created on ACS server, it will only show as Help Desk.

8) You can only add one user at a time for the GUI. To bulk create users, use CLI. For detailed info, search Setting up Local Users Through CLI from the online help that accompanies LMS.

Creating Self Signed Certificates

CiscoWorks allows you to create security certificates that enable SSL communication between your client browser and management server.

Self-signed certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed CiscoWorks.

Note: If you re-generate the certificate, when you are in multi-server mode, any existing peer relation might break. The peers need to re-import the certificate in this scenario.

To create a certificate:

1. Go to the CiscoWorks Home Page and select **Common Services → Server → Security → Certificate Setup**.
2. Enter the values required for the fields described in the following table:

Table 6. Security Certificate Setup

Field	Usage Notes
Country Name	Two character country code.
State or Province	Two character state or province code or the complete name of the state or province.
Locality	Two character city or town code or the complete name of the city or town.
Organization Name	Complete name of your organization or an abbreviation.
Organization Unit Name	Complete name of your department or an abbreviation.
Host Name	DNS name of the computer or the IP address of the computer. Enter the Host Name with a proper domain name. This is displayed on your certificate (whether self-signed or third party issued). Local host or 127.0.0.1 should not be given.
Email Address	E-mail address to which the mail has to be sent. You can also enter multiple e-mail addresses separated by comma.

3. Click Apply to create the certificate.

The process generates the following files:

- **server.key:** Server's private key.
- **server.crt:** Server's self- signed certificate.
- **server.pk8:** Server's private key in PKCS#8 format.
- **server.csr:** Certificate Signing Request (CSR) file.

You can use the CSR file to request a security certificate, if you want to use a third party security certificate.

Note: If the certificate is not a Self signed certificate, you cannot modify it.

Setting up the System Identity User

To view the System Identity User default settings or to change the default settings, traverse to **CWHP → Common Services → Server → Security → Multi-Server Trust Management → System Identity Setup** link and edit the necessary details.

Setting up a Peer Server Account:

Every CiscoWorks server needs to have a peer server account setup if it is has to exchange information (like device credentials and so on) with other CiscoWorks servers. A peer server account should have the System Identity user information of other CiscoWorks servers. After creating the System Identity user as described above, traverse to **CWHP → Common Services → Server → Security → Multi Server Trust Management → Peer Server Account Setup** link and ensure that the **System Identity** users of the other CiscoWorks servers are created.

Peer Server accounts can also be used for providing access to a third party application to access the CiscoWorks server and authenticate and authorize it. Create a Peer Server Account as described above and provide the third party user the credential information.

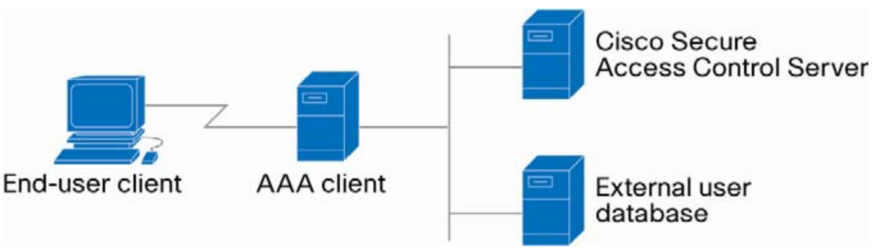
5. Securing LMS Server with Access Control Server

The LMS server has some built-in security features to authenticate users and assign them to some predefined roles to perform certain tasks. For maximum security protection, we recommend LMS server be integrated with Cisco Secure Access Control Server (ACS). This chapter will look at the steps required to configure the CiscoWorks server as an authentication, authorization and accounting (AAA) Client and use ACS for AAA services.

5.1. Introduction of ACS Server

ACS is a scalable, high-performance Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+) security server. As the centralized control point for managing enterprise network users, network administrators, and network infrastructure resources, ACS provides a comprehensive identity-based network-access control solution for Cisco intelligent information networks. ACS provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access server, PIXFirewall, or router, and even the CiscoWorks server.

Figure 13. AAA Client Model



CiscoWorks can be integrated with an ACS server to address the following tasks:

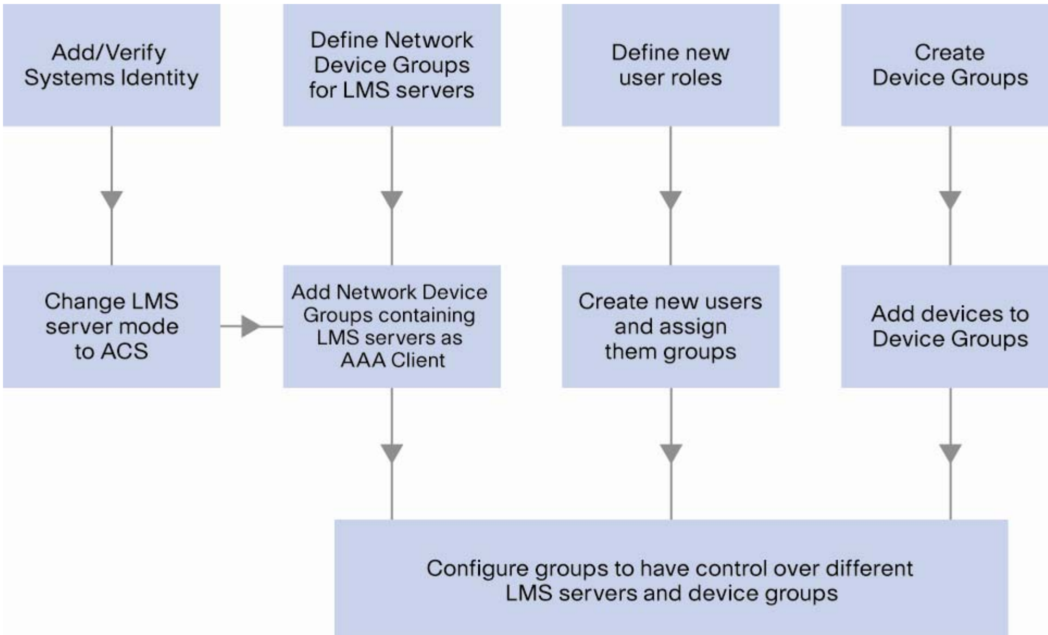
- Provide centralized user management for a group of CiscoWorks servers
- Provide device level authorization. Device level authorization restricts user access to perform certain tasks such as configuration updates and software image updates by authorizing the user for the task.
- Provide editable user roles. The user roles are mapped to tasks that the user is authorized to perform on the devices. ACS allows for the modification of the existing CiscoWorks user roles and for the creation of a new user role.
- Using ACS, groups of users can be assigned user roles per group of devices on a per application basis for the ultimate in authorization control.

The CiscoWorks server will be defined as an AAA client, just like network devices are. Just like when a user tries to login to a network device, when a user tries to login to the CiscoWorks server, the CiscoWorks server (AAA client) sends a request to the ACS server (AAA server).

5.2. LMS/ACS Workflow

See the following diagram for the workflow to integrate LMS and ACS.

Figure 14. LMS/ACS Integration Workflow



The workflow starts on the LMS server side by setting up the System Identity, and change LMS mode to ACS. Then on the ACS server, we define the Network Device Groups for the LMS servers and register them as AAA clients. All the applications on LMS will also be registered on the ACS. This completes the LMS/ACS integration.

To use ACS for authentication and authorization, we define the user roles, create users based on the user roles and assign them to user groups. Then we define device groups and add devices into device groups based on their administrative region.

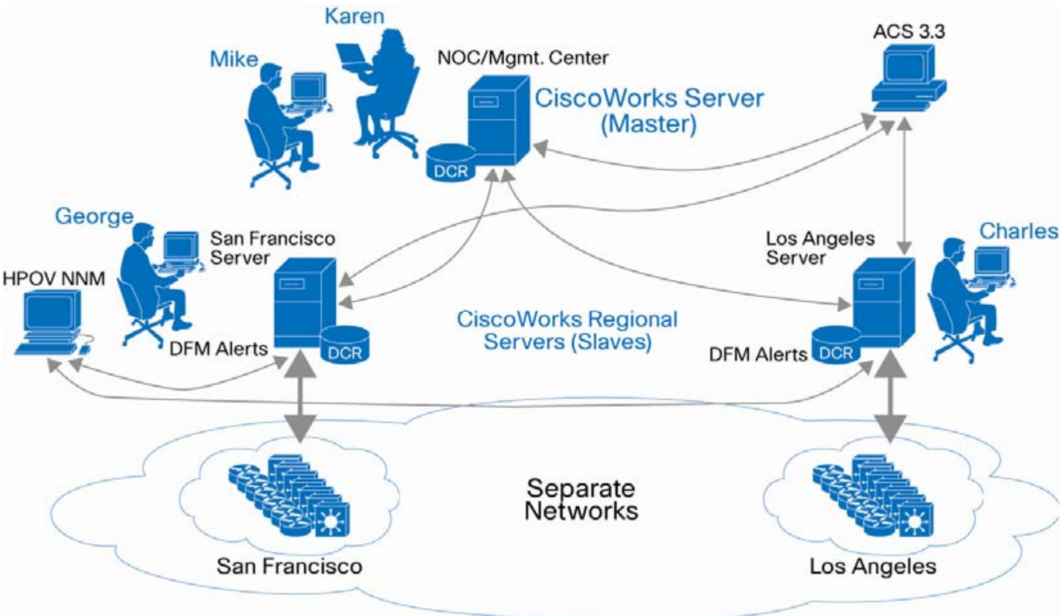
The last step is to tie all these together by configuring different user groups. Each group will have a set of users with different permissions on tasks/devices in the LMS servers. This will create secure views for the users to restrict their authentication and authorization rights.

In the following sections, we will illustrate this workflow with detailed step-by-step instructions by walking thru a business case.

5.3. Business Case

Here is a typical use case for LMS integration with ACS. In this scenario:

Figure 15. Scenario for LMS integration with ACS



- George is the network administrator in San Francisco. He will only manage the devices in the San Francisco network.
- Charles is the network administrator for Los Angeles. He will only manage the devices in the Los Angeles network.
- Karen and Mike both work in the NOC at the data center. They have the responsibility for all the network management servers and can manage all the devices, if needed.

To achieve this security requirement, we need to create secure views to restrict user's tasks on an AAA client, i.e. the LMS server. Secure Views are applicable only when CiscoWorks server is in ACS Login mode. Secure Views enable filtering of group membership based on the user and the application task context in which a request is made.

5.4. Detailed Examples

5.4.1. On the LMS Servers

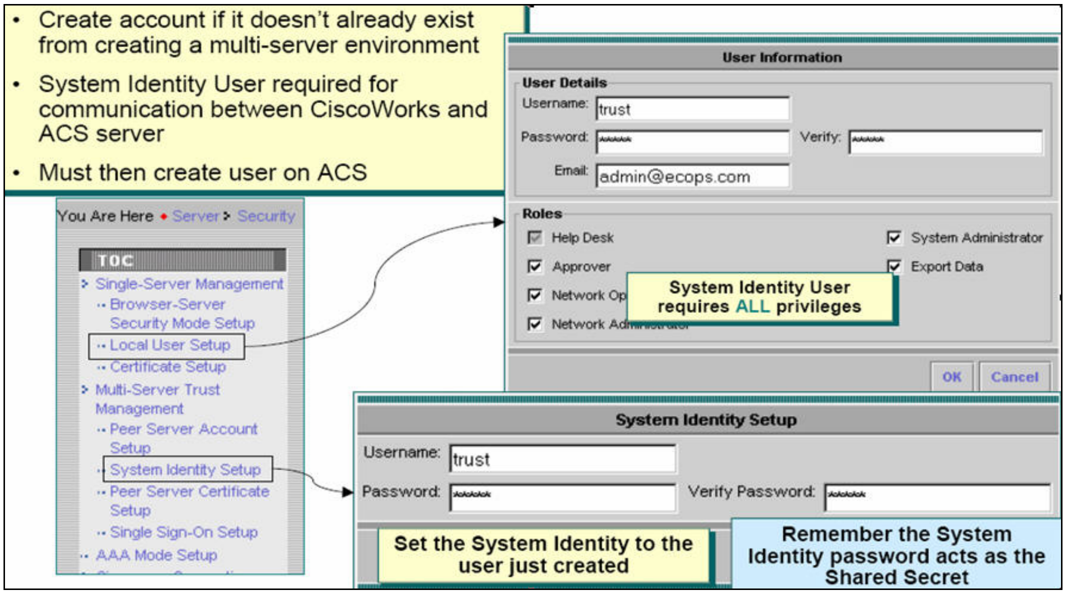
Add/verify the System Identity User

The System Identity user is needed for communication between the servers. It must be defined on both the CiscoWorks server and the ACS server, just like in the multi-server environment.

By default the "admin" user can be used as the System Identity user; it has all the user roles already assigned. In some environments, system administrators will create a separate local user with all the user roles and define this new user as the System Identity user.

Please note that when back on the ACS server, you need to create an identical user on ACS. The password acts as the shared secret key.

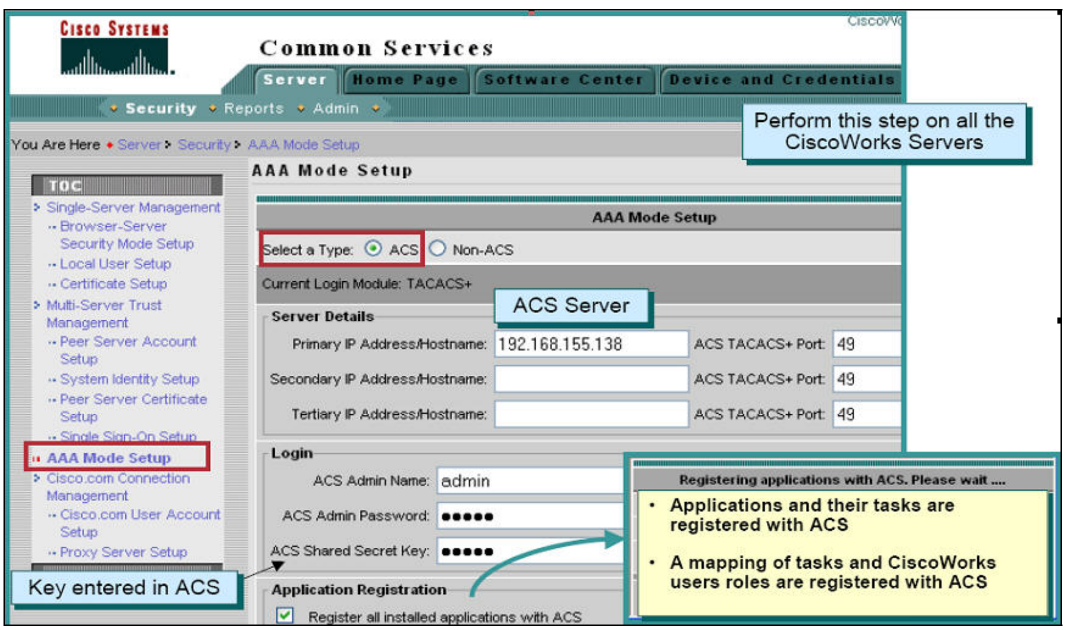
Figure 16. System Identity User



Change LMS to ACS Mode

To use an Access Control Server for AAA functions, select the AAA Mode Setup feature and change the AAA mode type to ACS. The system administrator will need to define the IP address, TACACS+ port and login information for the ACS in the network.

Figure 17. AAA Mode



When the Apply button is clicked, the following actions take place.

- A list of tasks in the CiscoWorks applications is registered with the ACS Server.
- A list of default user roles i.e. System Administrator, Network Administrator, Network Operator, Approver and Help Desk are registered with the ACS Server.

- A mapping of the tasks that the above user roles can execute is also registered with the ACS user.
- In the case of the LMS bundle, many tasks can be executed in the following products, i.e. Campus Manager, Resource Manager Essentials, Internetwork Performance Monitor, Device Fault Manager and Common Services. The mapping between user roles and these tasks are registered with the user. Note that this is a default mapping of user roles and tasks. This default mapping can be accessed in the LMS Server by traversing to **Common Services → Server → Reports → Permission Report** link and generating the report.

Note: The default mapping between tasks and the roles can be changed in the ACS Server and the changed mapping will not be reflected in the Permission Report.

After clicking **Apply** in the AAA Mode Setup Window, the above summary screen will be displayed. Verify that all the CiscoWorks applications successfully registered with the ACS server. Then restart the CiscoWorks Daemon Manager to make changes effective.

To restart the Daemon Manager:

From Windows command prompt:

```
net stop crmdmgtd
net start crmdmgtd
```

From the Solaris command prompt:

```
/etc/init.d/dmgtd stop
/etc/init.d/dmgtd start
```

Note:

- If planning to use ACS, configure it after all CiscoWorks applications have been installed and the trust relationships have been established.
- Multiple instances of same application on multiple CiscoWorks servers using the same ACS server will share settings. Any changes will affect all instances of that application.
- If an application is configured with ACS and then the application is reinstalled, the application will inherit the old settings.
- You can create new roles using ACS. The role you create is not shared across all the LMS applications. The role is shared across the same application in different CiscoWorks Servers registered to that particular ACS. You have to create new roles for each of the LMS applications that are running on the CiscoWorks Server. For example: Assume you have configured 10 CiscoWorks Servers with an ACS server and you have created a role in RME (say, RMESU). This role is shared for the RME application that runs on all 10 CiscoWorks Servers.
- System Identity User in ACS Mode: There can only be one System Identity User per machine. The System Identity User you configure has to be a Peer Server User. In the ACS mode, the System Identity user needs to be configured in ACS, with all the privileges the user has in CiscoWorks.

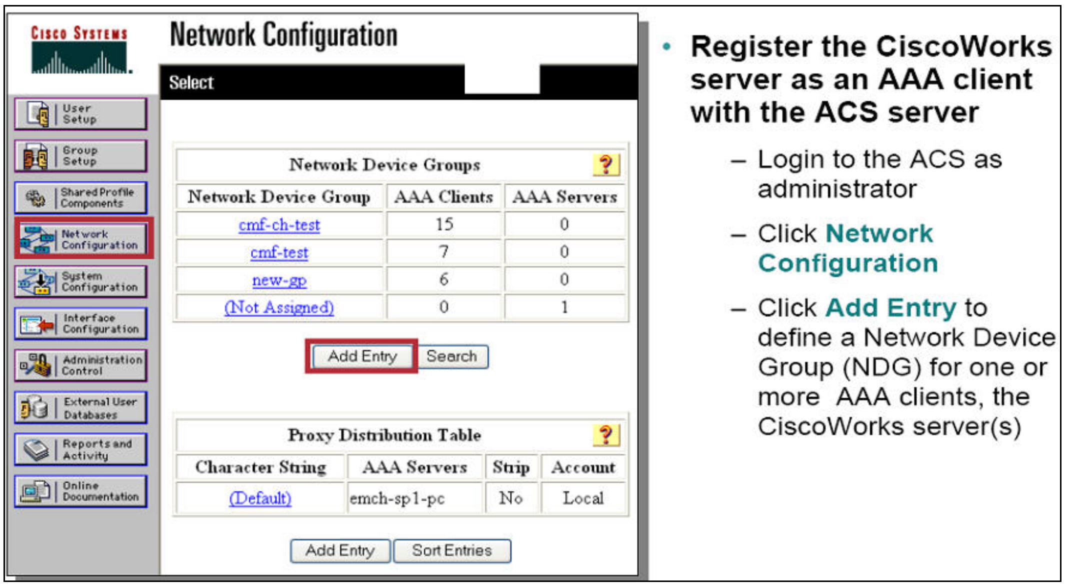
5.4.2. On the ACS Server

Defining NDGs for the CiscoWorks Servers

To define the CiscoWorks server as an AAA client within ACS, first we need to create Network Device Groups (NDG) for the LMS servers.

1. Login to the Cisco Secure ACS server.
2. From the ACS navigation menu, choose “Network Configuration”.
3. In order for the Network Device Groups table to be displayed in the ACS server, the Network Device Groups option must be enabled. To enable the Network Device Groups table, click **Advanced Options**. Select the **Network Device Groups**, check box. Click **Submit + Restart**. The **Network Device Groups** table will now be available.
4. In the **Network Device Group** (NDG) table, click **Add Entry**. This will allow you to create a NDG for containing one or more AAA clients, such as our CiscoWorks servers.

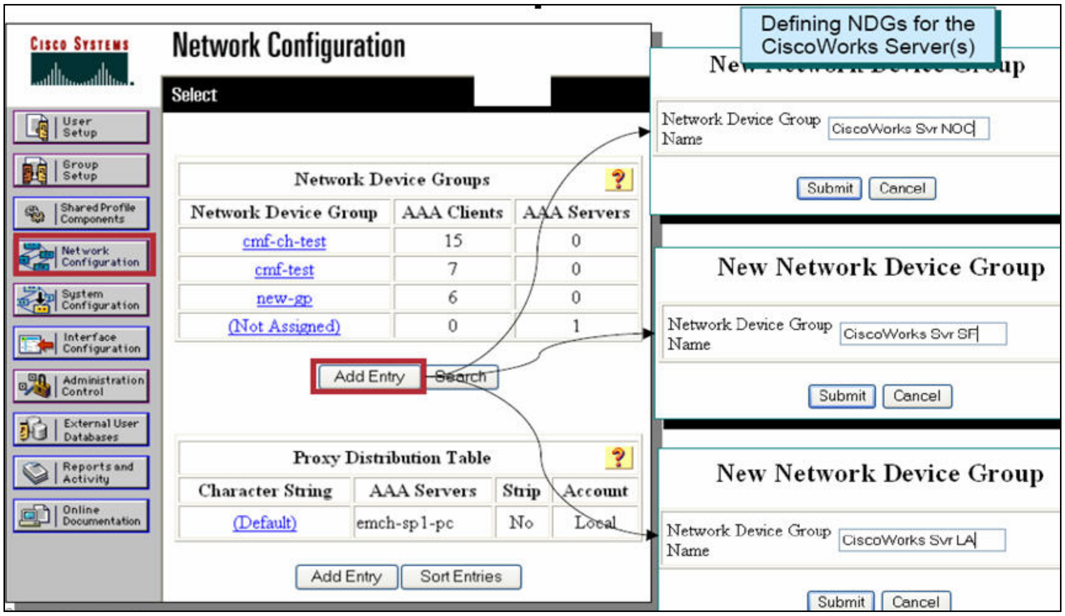
Figure 18. Register AAA Client



When **Add Entry** is selected in the Network Device Group (NDG) table, the New Network Device Group is displayed. If you have multiple CiscoWorks servers in a region that all users with the same privileges will access, they can be grouped together.

In this scenario, we want to separate the three servers into their own groups. Create three separate NDGs: CiscoWorks Server NOC, CiscoWorks Server SF, and CiscoWorks Server LA.

Figure 19. Define Network Device Groups

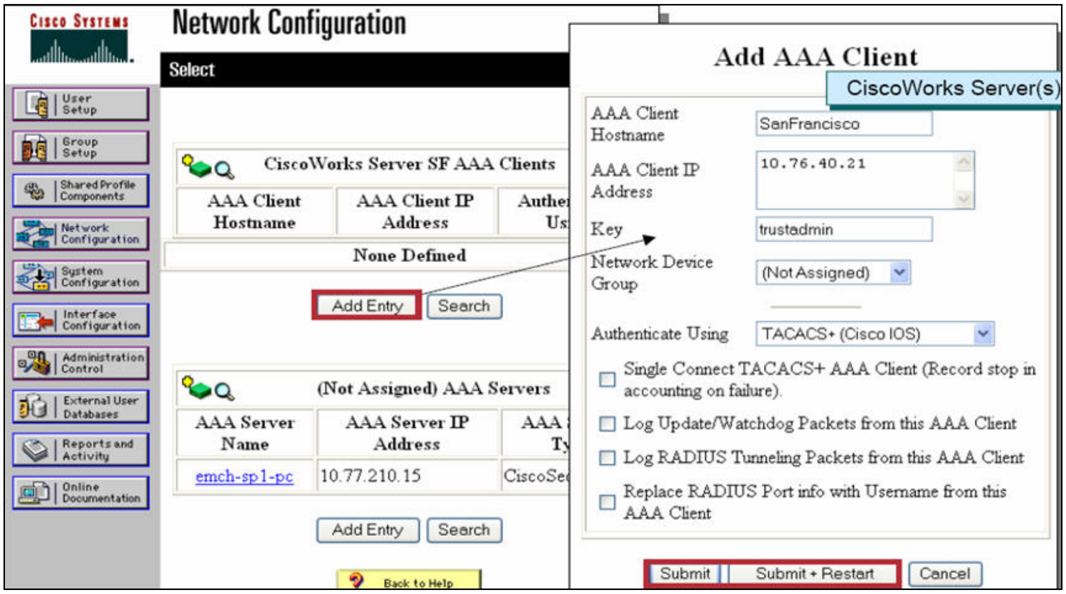


Define CiscoWorks as an AAA Client

Now you are ready to define each of the CiscoWorks servers as AAA Clients. Follow these steps to define the CiscoWorks server(s).

1. When the **Add AAA Client** dialog box appears, enter:
   - The host name of the CiscoWorks server.
   - The IP address of the CiscoWorks server.
   - The Key value. Be sure to give a value to the Key field so that the CiscoWorks server can contact the ACS server. You will need this key when changing the CiscoWorks AAA mode.
1. Leave the NDG as (Not Assigned).
2. Click **Submit** if you have more clients to enter or click **Submit +Restart** if all clients have been entered.
3. Repeat for all CiscoWorks server NDGs.

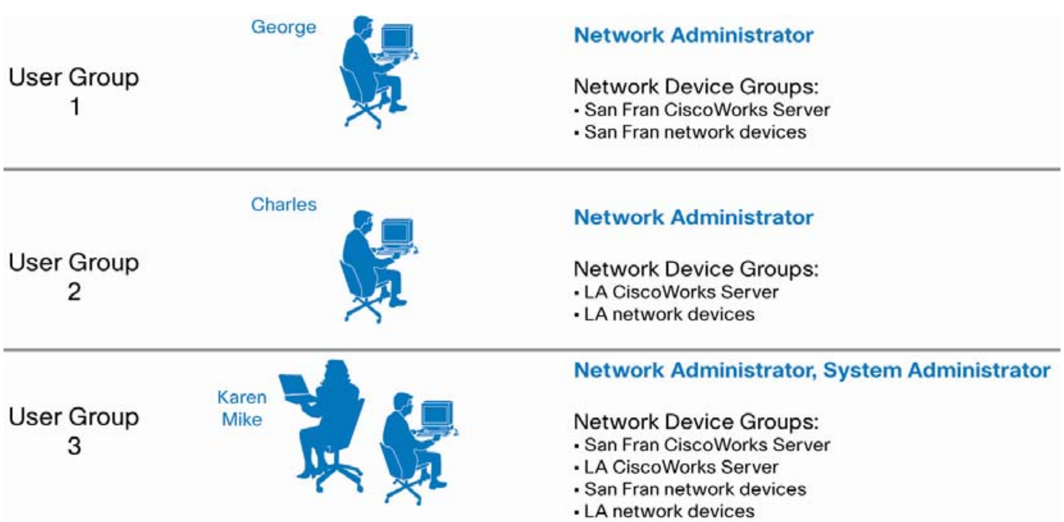
Figure 20. Add AAA Client



Defining the New Users

Now we define the users and groups within ACS.

Figure 21. Define New Users

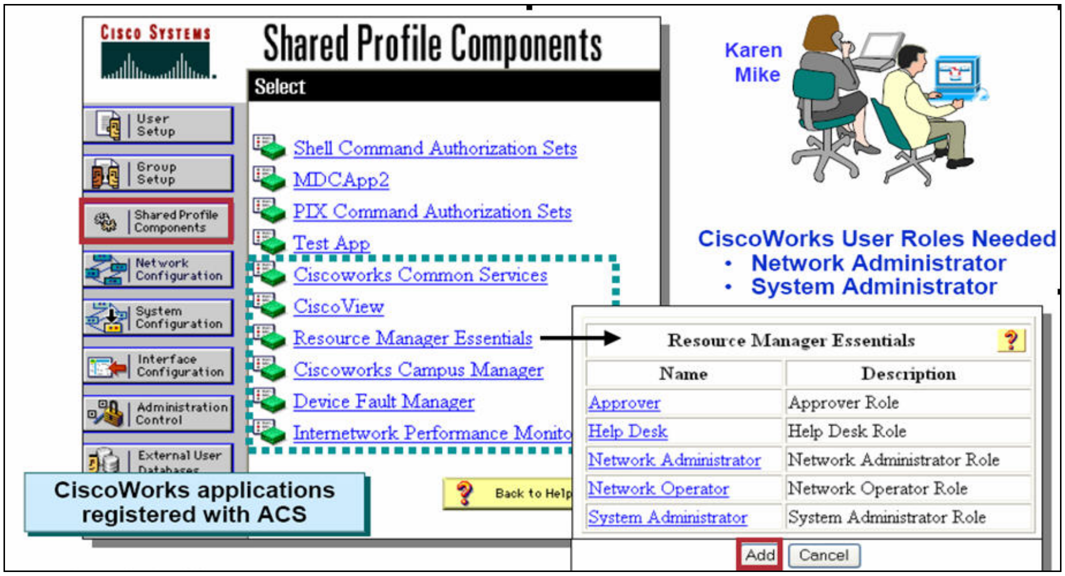


Remember that the CiscoWorks servers are AAA Clients, as well as the network devices themselves.

In the previous steps, we saw how the CiscoWorks applications were registered with the ACS. In addition, the CiscoWorks user roles are also registered. The default mapping between tasks and the roles can be changed in the ACS server, but note that the changed mapping will not be reflected in the Permission Report in CiscoWorks.

Defining New User Roles in ACS

Figure 22. Define New User Roles



In ACS, the administrator can assign only one role for a user on a Network Device Group. If a user requires privileges other than those associated with the current role, to operate on a Network Device Group, a custom role should be created. All necessary privileges to enable the user operate on the Network Device Group should be given to this custom role.

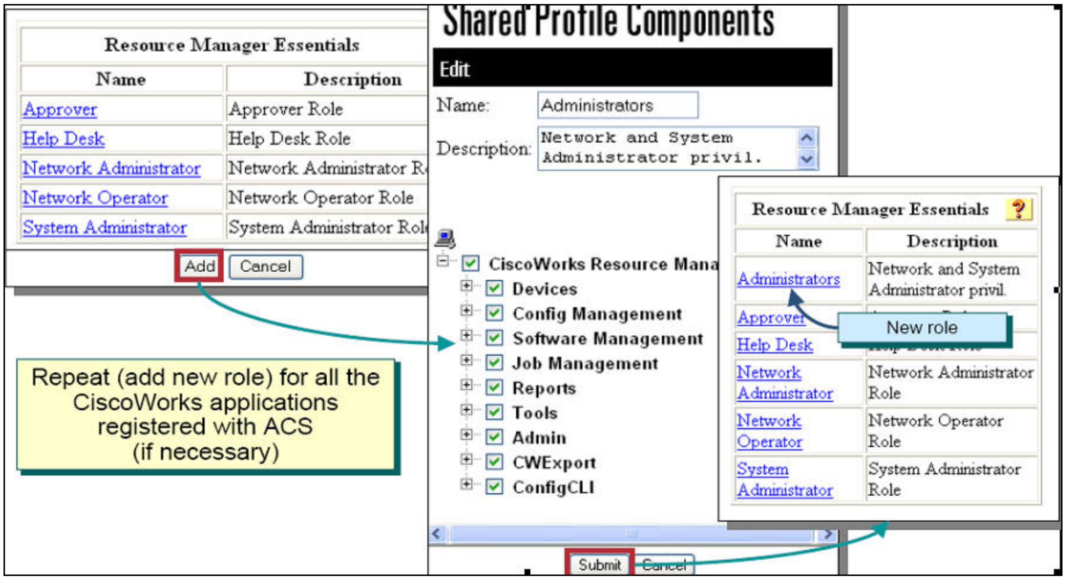
In this scenario, Karen and Mike need to have System Administrator and Network Administrator privileges to operate on the devices and CiscoWorks servers for San Francisco and Los Angeles. The next step would be to create a new role with Network Administrator and System Administrator privileges, Once created, assign this role to the users so that they can operate on the appropriate network device groups.

Cisco Secure ACS allows you to modify the privileges to these roles. You can also create custom roles and privileges that help you customize Common Services client applications to best suit your business workflow and needs.

If another instance of RME is registered with the same Cisco Secure ACS, your instance of RME will inherit those role settings. Furthermore, any changes you make to RME roles will be propagated to other instances of RME through Cisco Secure ACS. If you reinstall RME, your Cisco Secure ACS settings will automatically be applied upon RME restart.

To modify the CiscoWorks roles and privileges on Cisco Secure ACS:

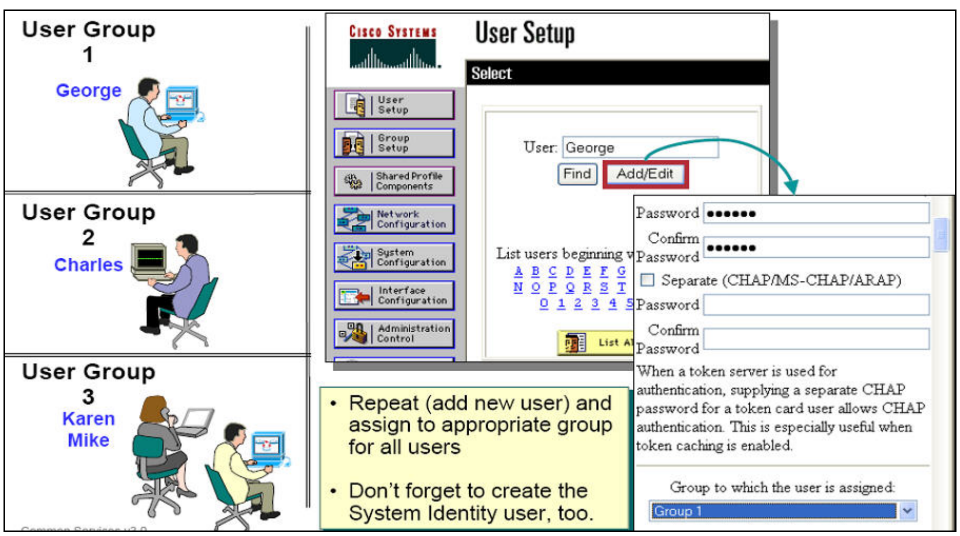
Figure 23. Modify User Roles



1. Select **Shared Profile Components → Resource Manager Essentials** and click on the RME roles that you want to modify.
2. Select or deselect any of the RME tasks that suit your business workflow and needs.
3. Click **Submit**.

Creating New Users in ACS

Figure 24. Create New Users



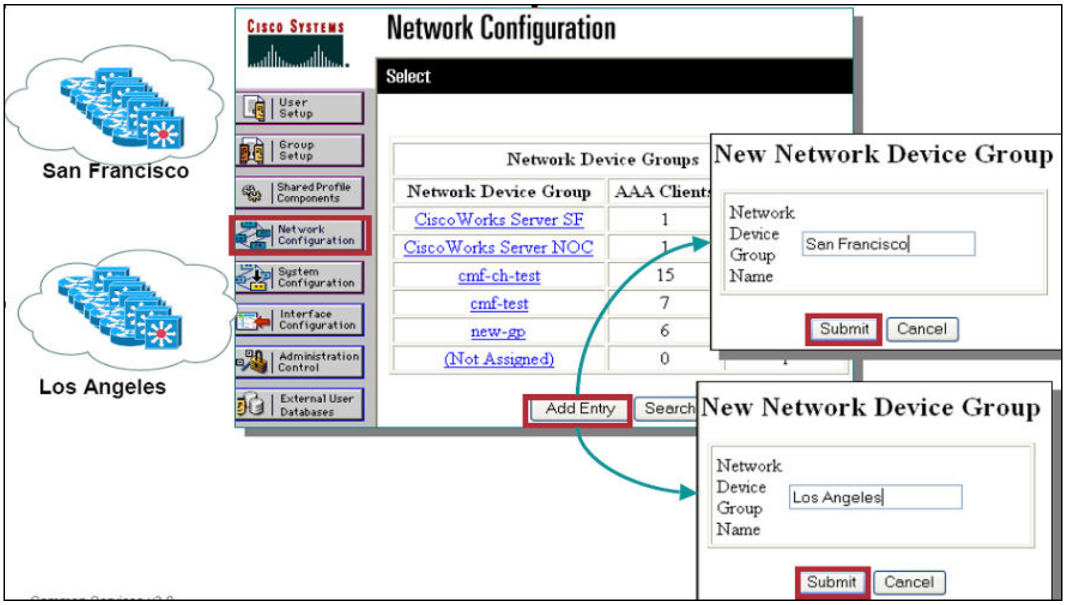
In the following procedure, the users George, Charles, Karen and Mike will be created in ACS:

1. From the main window of the ACS server, click **User Setup**. The **User Setup** dialog box appears.
2. Enter the following information:
   - Enter a username (in this example, **George**), then click **Add/Edit**.
   - Assign a password to the user **George**.
   - Assign **George** to group named Group1, then click **Submit**.

3. Similarly, create the other users by repeating these steps,
   - Create **Charles** and assign **Charles** to Group 2.
   - Create **Karen** and assign **Karen** to Group 3.
   - Create **Mike** and assign **Mike** to Group 3.
4. Finally, create the System Identity user. Use the same user information that was created on the CiscoWorks server. In ACS mode, the System Identity user needs to be configured in ACS, with all the privileges the user has in CiscoWorks.

Creating Device Groups in ACS

Figure 25. Create Device Groups

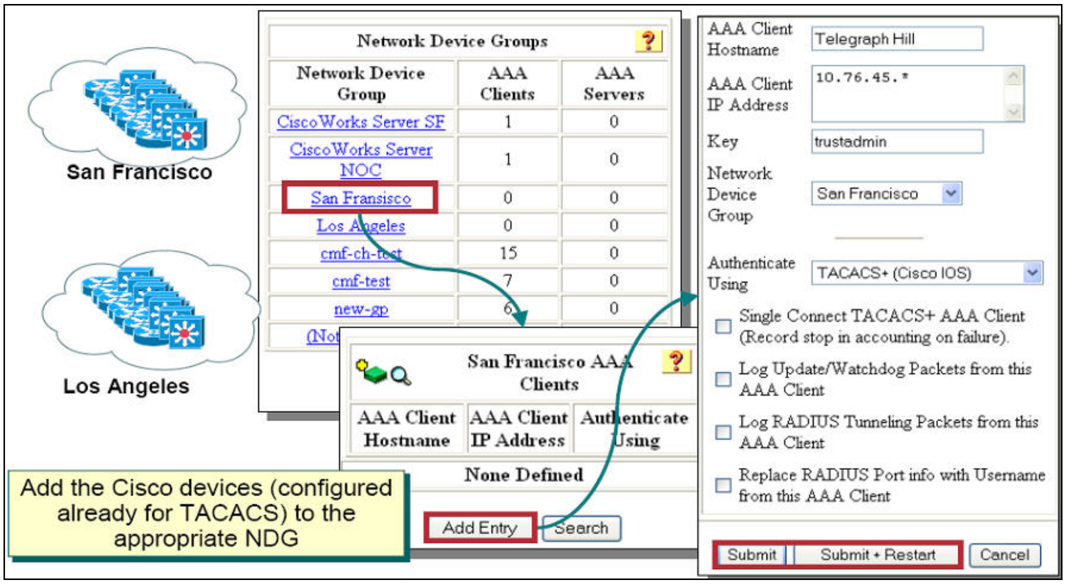


The next stage is to create two device groups for the Cisco devices located in San Francisco and the other Cisco devices located in Los Angeles. The following procedure details the steps:

1. From the main window in ACS, click **Network Configuration**. The **Network Device Groups** dialog is displayed.
2. Click **Add Entry**.
3. Create two **Network Device Groups—San Francisco** and **Los Angeles** as shown above. Click **Submit** after each entry.

Adding Devices to the Device Groups

Figure 26. Add Cisco Devices to Network Device Groups



Now let’s add devices into the two device groups just created for the Cisco devices located in San Francisco and the other Cisco devices located in Los Angeles.

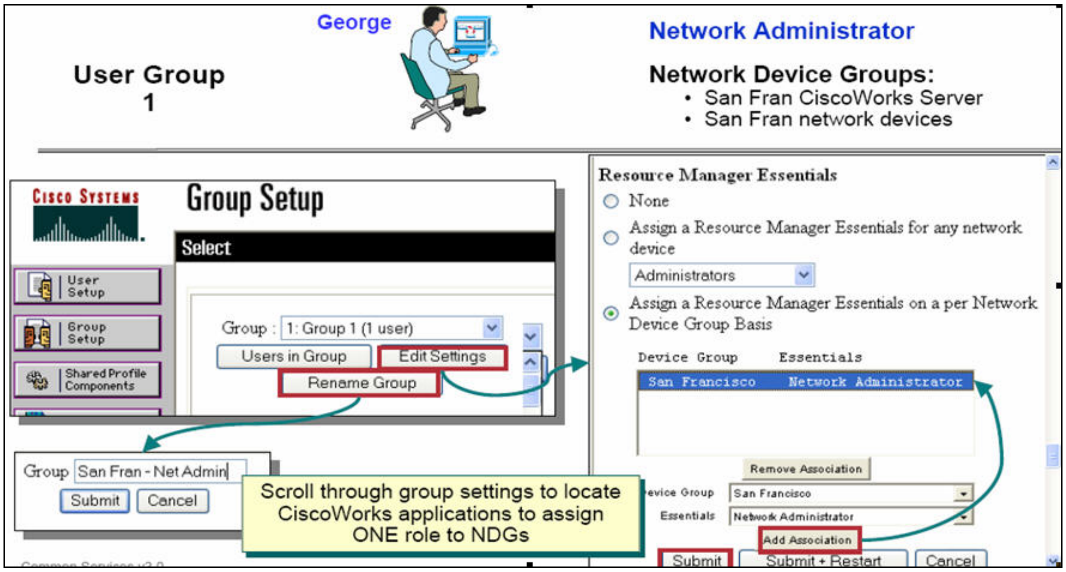
1. From the **Network Device Groups** dialog box, click the **San Francisco** link and in the **San Francisco AAA Client** dialog box, click **Add Entry** to add a single device that is located in San Francisco, a subnet, or a range of devices based on IP addresses.

Note: You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box. You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.

2. Enter the **Key** value. The **Key** is the shared secret pass-phrase that the TACACS+ or RADIUS AAA client and Cisco Secure ACS use to encrypt the data. The key must be configured in the AAA client and Cisco Secure ACS identically, including case sensitivity.
3. Click **Submit** if you have more devices or subnets to enter or click **Submit +Restart** if there are no other subnets or devices to add. .
4. Repeat for all devices that require AAA services.
5. Repeat steps for the **Los Angeles** NDG and its devices.

Configuring User Groups

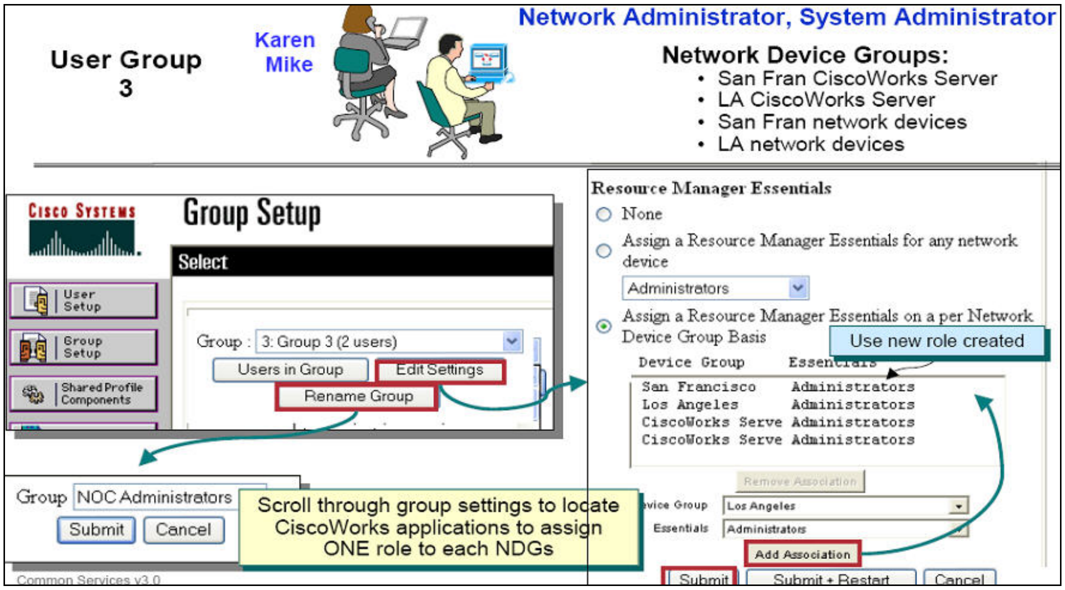
Figure 27. Configure User Groups



Now we need to tie these procedures together. The users were assigned to user groups when created. We can now rename these user groups. And now that the CiscoWorks applications have been registered with ACS, we can permit the users with a group to use the applications. Additionally, the flexibility of ACS will allow you to allow the users in the group to only have access to specific NDGs as well as specified task authorization on these devices, by assigning a user role to the NDG. Note that only one user role can be assigned per NDG. (For this reason, the ACS role of Administrators was created earlier. This role allows all tasks to be executed.)

1. From the main window in ACS, click **Group Setup**.
2. Select **Group 1** from the pull-down menu to define **George's** group and permissions.
3. Click **Rename Group**. Enter **San Fran – Net Admin** to define the group for the network administrators located in San Francisco.
4. Now define the NDG associations for the CiscoWorks applications in this group. Click **Edit Settings**.
5. Scroll through the settings and find the CiscoWorks applications.
6. The CiscoWorks Resource Manager Essentials application is illustrated. Click the **Assign Resource Manager Essentials on a per Network Device Group Basis** radio button.
7. Since **George** will only have network administrator privileges on the San Francisco devices, select San Francisco from the Device Group pull-down menu. Change the role for this NDG to be **Network Administrator**. Click **Add Association**.
8. Click **Submit** to make the changes. (You will need to click **Submit+Restart** when you are done making changes to the Groups.)

Figure 28. Configure User Groups



Now, to repeat this process for the NOC Data Center users, **Karen** and **Mike**, who are in **Group 3**:

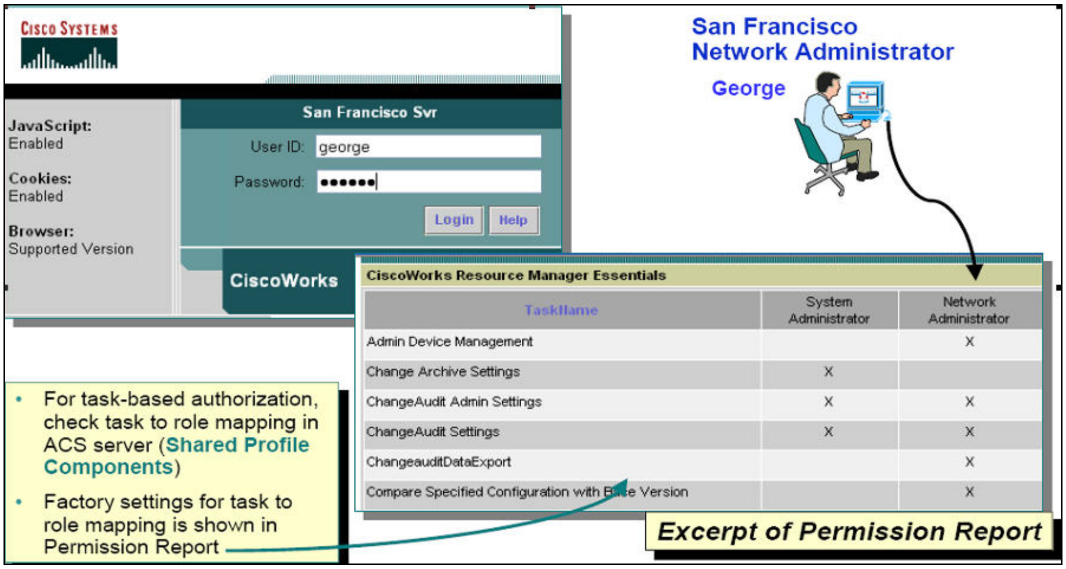
1. From the **Group Setup** window, select **Group 3** from the drop-down menu to define **Mike** and **Karen's** group and permissions.
2. Click **Rename Group**. Enter **NOC Administrators** to define the group.
3. Remember that Karen and Mike have permission for all tasks in CiscoWorks for all devices in San Francisco and Los Angeles. Therefore, the user role in ACS, **Administrators**, was created since NDGs can only have one role. The default roles imported from CiscoWorks limit the user to select tasks.
4. Now define the NDG associations for the CiscoWorks applications in this group. Click **Edit Settings**.
5. Scroll through the settings and find the CiscoWorks applications that the user needs access to. For example: Check the checkboxes next to **CWHP** if access to the CiscoWorks HomePage is needed.
6. The CiscoWorks Resource Manager Essentials application is illustrated. Click the “Assign Resource Manager Essentials on a per Network Device Group Basis” radio button.
7. **Karen** and **Mike** will have all privileges on the **San Francisco** and **Los Angeles** devices.
   - Select **San Francisco** from the Device Group pull-down menu. Change the role for this NDG to be **Administrators**. Click **Add Association**.
   - Secondly, select **Los Angeles** from the **Device Group** pull-down menu. Change the role for this NDG to be **Administrators**. Click **Add Association**.
8. Click **Submit+Restart** to make the changes and restart ACS.

Secure Views in CiscoWorks (Tasks Authorization)

With AAA services operational with ACS, **George** can now login to the San Francisco CiscoWorks server.

George's login is authenticated from the ACS server. **George** was assigned the role of Network Administrator in ACS. The **Network Administrator** role was imported from CiscoWorks when registered. Unless the **Network Administrator** role was modified in the Shared Profile components, the tasks will take on the factory settings as illustrated in the CiscoWorks Permissions Report.

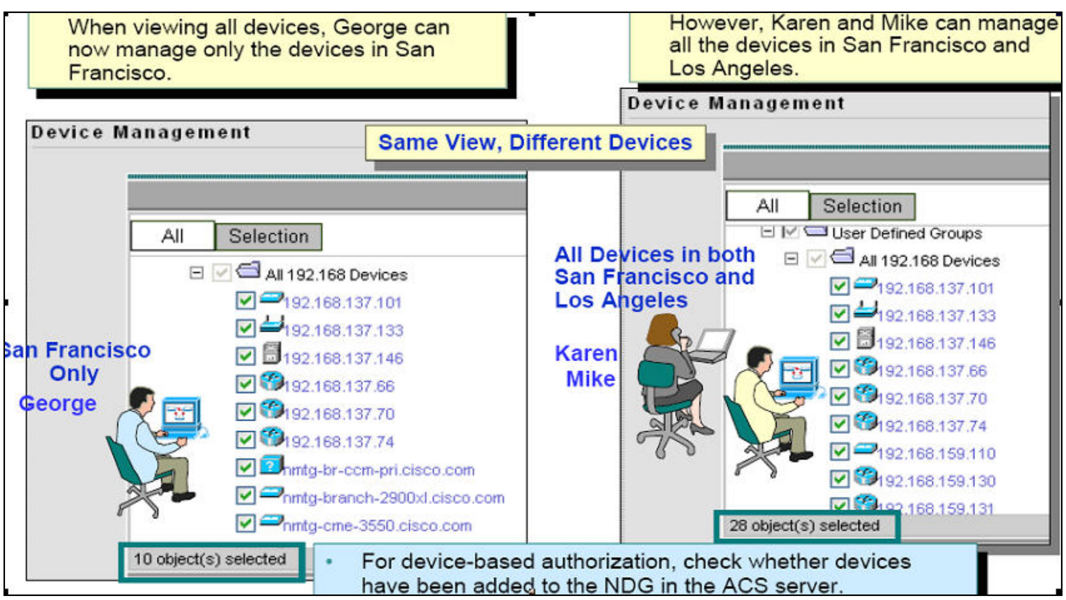
Figure 29. Secure Views in CiscoWorks



Secure Views in CiscoWorks (Device Authorization)

With AAA services operational with ACS, the same device views can restrict a user's view of devices to execute tasks on and run reports. As illustrated above, **George** can now only manage the devices in San Francisco. However, **Karen** and **Mike** can manage all the devices in San Francisco and Los Angeles.

Figure 30. Secure Views in CiscoWorks



6. Populating the DCR and Device Management for Individual Application Inventories

After the devices are setup with proper credentials and LMS server is installed and initially setup, we are ready to discover the devices to populate the Device and Credential Repository. After DCR is populated, we need to populate the individual inventories of LMS applications such as Campus Manager, RME, Campus Manager, DFM and IPM.

6.1. Device and Credential Repository

The Device and Credential Repository (DCR) is a common repository of devices, their attributes, and credentials that can be used by various network management applications. The Device and Credential Admin (DCA) provides an interface to administer DCR. DCR is part of Common Services and acts as a central secure repository for all the device and credential information. All applications within LMS request DCR for device credential information. Since there is a common device and credentials repository, devices populated in DCR can be automatically populated in different applications.

6.1.1. Configuring Default Credentials

The default credentials feature helps you to add or import devices into DCR with the default credentials and prevents the management applications from failing when the network management applications manage the devices added or imported in DCR.

To configure the default credentials:

1. Go to the CiscoWorks Home Page, select **Common Services → Device and Credentials → Admin**. Select **Default Credentials** from the TOC list.

Note: The **Default Credentials** list item is visible in the TOC only in DCR Master and DCR Standalone CiscoWorks Servers. You cannot see this list item in DCR Slave Server.

2. Select a credential type from the Default Credentials list panel and enter the respective credential information. You can select any of the credential types from the panel.
    - Standard Credentials
    - SNMP Credentials
    - HTTP Credentials
    - Auto Update Server Managed Device Credentials
    - Rx-Boot Mode Credential
3. Enter the following credentials as required:
    - Standard Credentials
        - Primary Credentials (Username, Password, Enable Password)
        - Secondary Credentials (Username, Password, Enable Password)
    - SNMP Credentials
        - SNMPv2c/SNMPv1 Credentials (Read-Only Community String, Read-Write Community String)
        - SNMPv3 Credentials (Username, Password, Authentication Algorithm)
    - HTTP Credentials
        - Primary Credentials (Username, Password)

  - Secondary Credentials (Username, Password)
  - Other Information (HTTP Port, HTTPS Port, Current Mode)
- Auto Update Server Managed Device Credentials (Username, Password)
- Rx-Boot Mode Credentials (Username, Password)

Note: Re-enter the value of password in the respective Verify fields.

4. Click **Apply** after you have entered all the values or click **Cancel** to cancel the changes.

To delete the default credentials configured:

1. Go to the CiscoWorks Home Page and select **Common Services → Device and Credentials → Admin.**
2. Select **Default Credentials** from the TOC list.

The Default Credentials page appears. You can also navigate to the Device Credentials page from the LMS Portal Home.

3. Click **Remove**. The default credentials you have configured are deleted. The devices added already to DCR with the default credentials will remain unaffected.

6.2. Populating the DCR

DCR can be populated in the LMS server through one of the three ways listed below:

1. **Campus Manager Device Discovery:** This is the easiest and more efficient way to populate the DCR. Campus Manager (CM) has the ability to discover Cisco devices present in the network using Cisco Discovery Protocol (CDP). Therefore, in order to discover devices using CM, CDP should be enabled on the network. If CDP is enabled on your network, you can enter a single or multiple **Seed Devices** in CM. A **Seed Device** is generally the core device(s). A core switch or switches will be the perfect seed device because this device will have a lot of CDP neighbors and this hastens the discovery process.

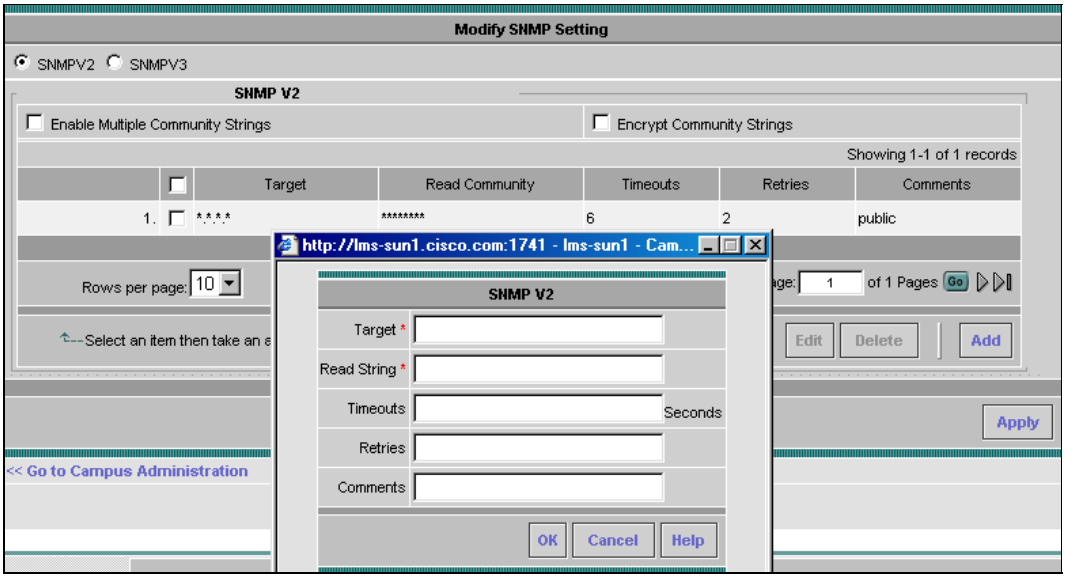
To configure Device Discovery:

Step 11. Go to the CiscoWorks Home Page and select **Campus Manager → Administration**.

Step 12. **Select Admin → Device Discovery → SNMP Settings**. Specify the community strings as required.

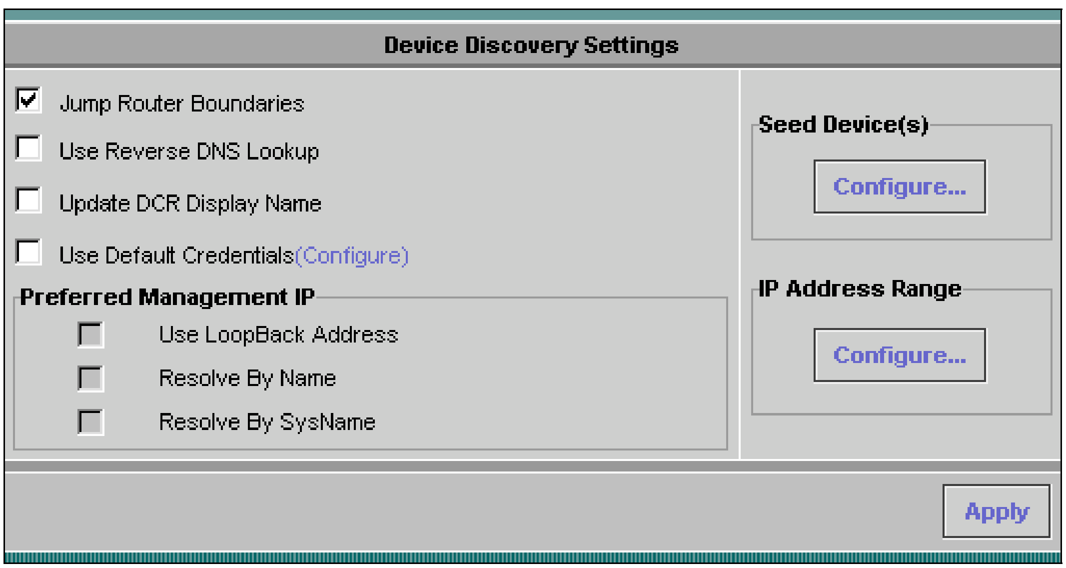
Note: Only the read community string needs to be entered in the **SNMP Settings** page. **Add** or **Edit** the read community strings depending on the number of community strings configured in the network. By default only the **SNMPv2** read string is populated. To populate SNMPv3, select the **SNMPV3** radio button.

Figure 31. Modify SNMP Setting



Step 13. **Select Admin → Device Discovery → Discovery Settings**. Specify the Discovery options such as Seed Device and IP address range. If IP Address Range is not specified, Device Discovery tries to discover as many devices as it can, based on the community strings and connectivity.

Figure 32. Device Discovery Settings



Selecting the **Jump router boundaries** checkbox will make the discovery beyond the seed device's neighbors.

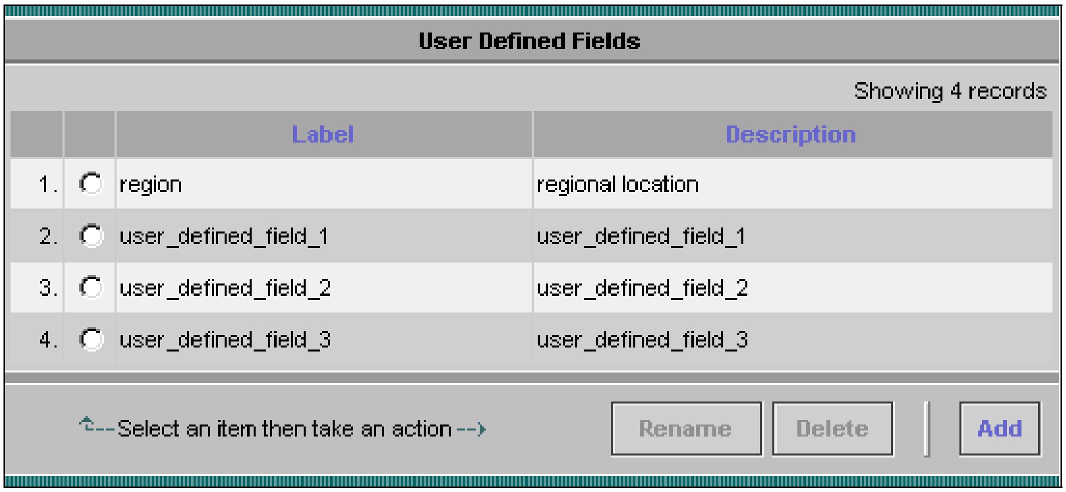
Step 14. Click **Apply** to start an immediate device discovery. Click on the **Home** link to verify the device discovery status. Refresh the page to update the device discovery status and verify the number of devices discovered when in **Idle** state.

All the devices discovered by CM should now be populated in DCR.

2. **Add Devices to DCR from Common Services:** LMS supports to add devices to DCR from Common Services. You can add devices one-by-one, or import them in bulk. To add individual devices, go to **Common Services → Device and Credentials → Device Management**, then choose **Add** to start.

Note: You can customize the DCR entries by using the **user_defined_field.** They are located under **Common Services → Device and Credentials → Admin → User Defined Fields**. By default there are four and you can add more.

Figure 33. User Defined Fields



LMS also supports bulk import into DCR. You can do bulk device import by traversing through **Common Services → Device and Credentials → Device Management → Bulk Import**.

Bulk Import into DCR can be done by one of the three formats listed below.

- File Import

  Select the "**File**" option to import devices from a CSV or XML file. The input file should have format as specified in the online help. In this case, all device credentials can be provided along with the device name/IP address. If the imported device does not have a device type associated with it then it will be a member of the group "/CS/System Defined Groups/Unknown Device Type". A device type can then be given to the device by selecting the device in Device Management screen and clicking on Edit button.

- Local NMS Import

  Select the "**Local NMS**" option to import devices from either HP OpenView Network Node Manager 6.x or IBM Tivoli NetView 7.x installed in the same machine as the CiscoWorks server. The install location of the HP OpenView NNM 6.x or IBM Tivoli NetView 7.x needs to be provided.

- Remote NMS Option

  Select the "**Remote NMS**" option to import devices from either HP OpenView Network Node Manager 6.x or IBM Tivoli NetView 7.x installed in a different machine from the CiscoWorks server.

Note: In LMS 3.0, the import of devices is allowed only from a remote Unix NMS server or a remote Windows NMS server that supports the rsh protocol.

Once the devices have been imported through the Local or Remote NMS option, the credentials for these devices can be edited by selecting the groups to which the devices belong and clicking on **Edit** button in Device Management screen.

Recommendation: If you have CDP enabled on your network, populating the Cisco devices through CM Device Discovery is recommended.

3. **Device Credentials Update:** To utilize the complete functionality of LMS, device credentials other than the SNMP read credentials need to be entered in DCR. Credential update in DCR can be done by going to **CWHP → Common Services → Device and Credentials → Device Management**. You can also specify default credentials as described in Section 6.1.1. Select all devices under the CS group by checking the CS group and click **Edit**, then follow the GUI to update the credentials.

Note: Do not select any device in the following screen.

Click on **Next** button which will by default select all the devices. Enter the device credentials and click **Finish**. If you need to enter **User Fields** for devices click on **Next** and enter up to four user-defined fields.

Note: If all the devices have the same credentials, use the above step to **Edit** credentials. However, if devices have different credentials, create groups of devices having the same credentials by going to **CWHP → Common Services → Groups** and creating groups underneath **CS/User Defined Groups** group.

6.3. Individual Inventories of LMS Applications

This section talks about how to populate the individual inventories for each of the LMS applications, Campus Manager, Resource Management Essential, Device Fault Manager and Internetwork Performance Monitor.

LMS applications have mode settings to help control the flow of device and credential information to the applications from the Device Credential Repository (DCR). The mode setting can be done only in each of the application user interface screen.

The two LMS application modes available to select are:

- manual mode
- auto synchronize mode

In manual mode the applications including Device Fault Manager, Resource Manager Essentials and Internetwork Performance Monitor will not automatically get device updates (device add, delete and credential updates) from DCR.

In auto synchronize mode the applications like Campus Manager, Device Fault Manager, Resource Manager Essentials and Internetwork Performance Monitor will automatically get device updates (device add, delete and credential updates) from DCR. In response to the device updates, the applications may do data collection, performance and fault monitoring on the modified devices.

6.3.1. Device Management in Campus Manager (CM)

Device Discovery vs. Device Data Collection

In the previous section, we used Campus Manager to discover the devices to populate the DCR. However the discovery only populate the DCR with the basic device information such as,

- Host name, Domain name, Management IP address, Display name, and sysObjectID
- SNMPv2 read-only community string (if SNMPv2 was used for communicating with the device)
- SNMPv3 user ID, password, engineID, authorization algorithm (if SNMPv3 was used for communicating with the device).

Note: Device Discovery does not update SNMPv2 write community string.

To manage the devices, Campus Manager has to perform Data Collection to collect more information about the devices for topology computation, reporting network discrepancies, and for various reports and device configurations.

Data Collection Server does Data Collection, at scheduled intervals, on the devices in DCR.

Data Collection involves the following steps:

1. Data Collection Server gets the list of devices and their credentials from DCR.
2. It polls these devices, fetches information that is required for topology computation, reporting network discrepancies, and for various reports and device configurations.

If the credentials in DCR are incorrect for any reason, the devices are reported as unreachable in Campus Manager.

It is not mandatory that Data Collection be done for all devices in DCR. You can set the Data Collection to be either manual mode or auto mode.

Managing Devices in Auto Mode

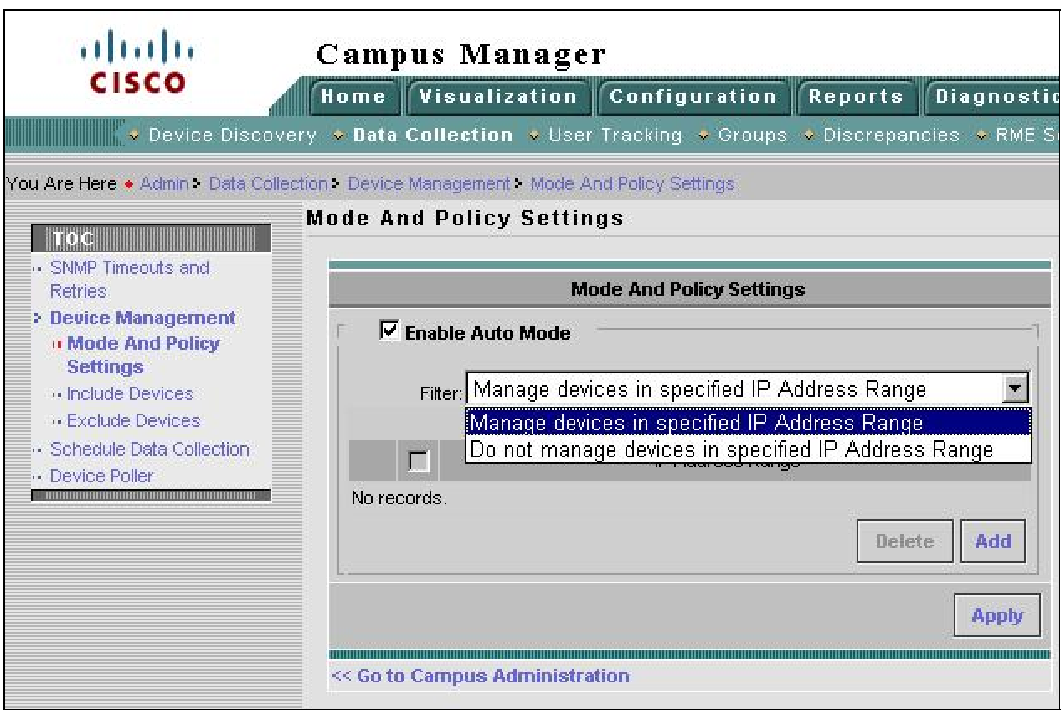
This is the default option, where devices in DCR are automatically managed in Campus Manager Data Collection. You can specify the filter policies based on IP addresses to exclude or include devices in data collection. You can also manually add or delete devices.

Managing Devices in Manual Mode

In this mode you have to manually add or delete devices and only those devices will be taken for data collection.

To change the mode setting, go to **Campus Manager → Admin → Data Collection → Device Management → Mode and Policy Settings**. See the following figure:

Figure 34. Enable Auto Mode



Data Collection can be run on a pre-determined schedule or on user action.

The following are some key facts about Campus Manager Data Collection

- A list of devices and corresponding credentials in Device Credential Repository are used for data collection
- Only devices in DCR are managed. If a device is not in DCR, then it will not be managed by Campus Manager.

- A filtering mechanism can be applied to manage a subset of devices found in Device and Credential Repository. The filtering is based on either IP address or VTP domain.

To optimize the data collection for the devices, the following steps can be taken.

- IP address or VTP domain filters can be set by traversing to **Campus Manager Administration → Admin → Campus Data Collection → Data Collection Filters**.
- When data collection is done for more than 5000 devices, the ANIServer process (Java based) reaches a threshold of 1024MB. If the data collection is done for a device count close to 5000 it is recommended to increase the heap size for ANIServer from –Xmx1024m to –Xmx1280m. This is done by editing the file NMSROOT/objects/dmgt/dmgtd.conf. In this file, there is an entry for starting the ANIServer process. This entry has a string "-Xmx1024m" which needs to be changed to "-Xmx1280m". Please note that any edits to dmgtd.conf file can be done only after the LMS Server is shutdown. LMS Server needs to be restarted after the edit to dmgtd.conf file is complete.

6.3.2. Device Management in Resource Manager Essentials (RME)

You can either:

- Add devices automatically
- Add devices manually

Mode setting for RME can be changed by going to **Resource Manager Essentials → Administration → Device Mgmt** and check/uncheck "**Automatically Manage Devices from Credential Repository**".

Figure 35. Device Management Settings

By default, RME is set to automatic synchronization with the DCR.

To manually add devices to RME selectively,

Step 15. Check if the Automatically Manage Devices from Credential Repository on Device Management Settings window (**Resource Manager Essentials → Admin → Device Mgmt**) is disabled.

Step 16. Select **Resource Manager Essentials → Devices → Device Management → RME Devices**.

Step 17. Click **Add Devices** without selecting any devices from the RME Device Selector.

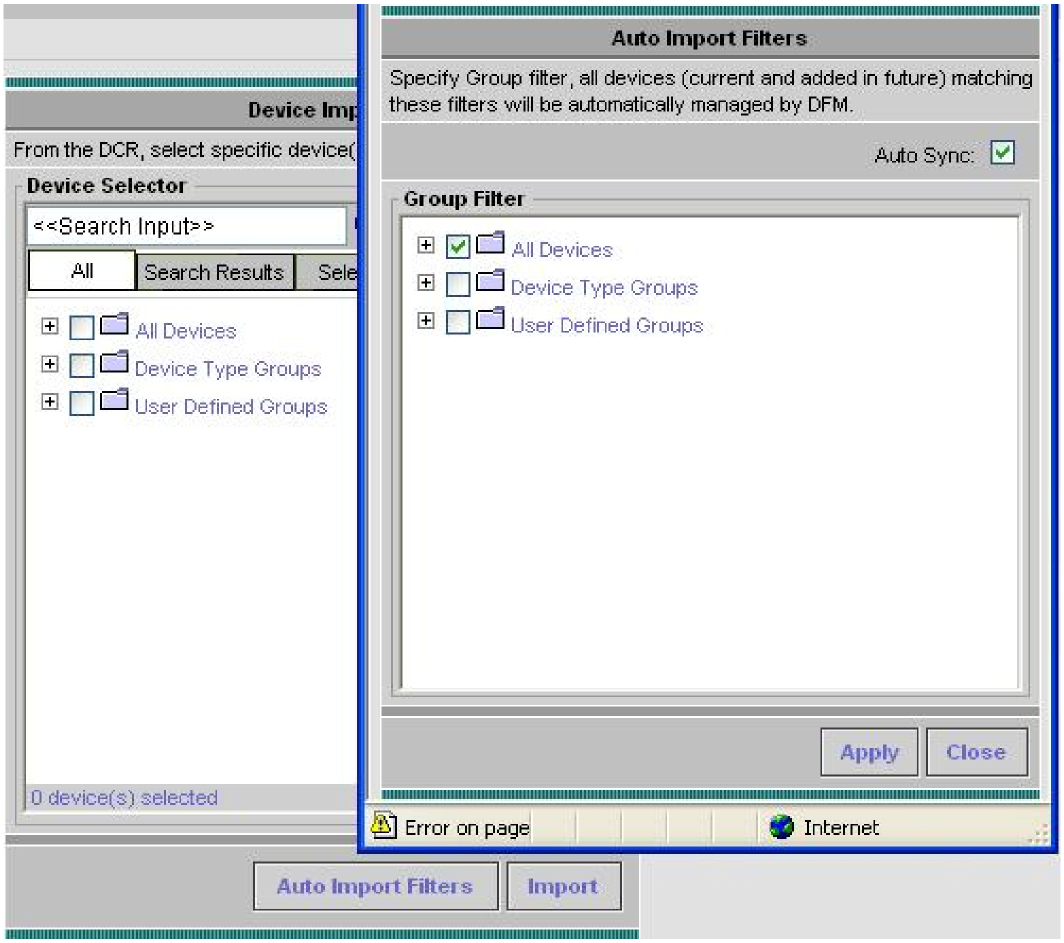
The **Devices in Device Credential Repository** dialog box appears. Follow the GUI to finish the device additions.

6.3.3. Device Fault Manager (DFM)

By default, DFM is setup in a manual manage mode. All devices added in DCR will need to be manually imported into DFM. Device import in DFM can be done by going to **Device Fault Manager → Device Management → Device Import**. By default, all devices are imported from DCR into DFM, unless Filter Selector is enabled at the same user interface.

To enable automatic device synchronization, click the **Auto Import Filter** button in the Device Import window to create a filter of the desired devices, then check the **Auto Sync** check box, then **Apply**. Default value for the filter IP address is *, which means all devices will be automatically imported from the DCR into the DFM inventory.

Figure 36. DFM Auto Sync Setting



6.3.4. Internetwork Performance Monitor (IPM)

Whenever you add devices to Common Services' Device and Credential Repository (DCR), the devices are added to IPM automatically if the **Internetwork Performance Monitor → Admin → System Preferences → Application Settings** option is enabled.

This option is enabled by default. Hence, the devices get added to IPM automatically after you have added the devices to DCR.

Figure 37. IPM Mode Setting

9) For easier management of devices across all applications, it is advisable to leave the auto-manage mode enabled.

The IPM application uses the following device credentials from the DCR:

- Device identity information such as IP address/host name/display name.
- Device access information such as SNMP v2/v3 credentials.

When a device is deleted from IPM, the DCR is not affected. You can add the devices back to IPM. However, if a device is deleted from DCR, it is also deleted from the IPM application.

When you import devices from Device and Credential Repository, if the devices already exist in IPM, they will be updated. IPM creates a separate log file for the Device and Credential Repository Import status. You can view the log file in: **IPMROOT/etc/source or IPMROOT/etc/target**.

You can view the results of importing devices from the CiscoWorks Homepage by clicking **View Import Source Log** or **View Import Target Log**.

To import DCR devices manually/selectively, deselect the Automatically Manage Devices from Credential Repository check box in the Application Settings page (**Internetwork Performance Monitor → Admin → Preferences → Application Settings**). You can add ad-hoc target devices from the IPM Devices page (**Internetwork Performance Monitor → Collector Management → Devices**).

6.4. Device Grouping

Device grouping in Common Services is used to create User Defined Groups based on User Defined field defined by DCR for the devices. These groups can then be used by RME, CM, DFM or IPM to launch tools pertinent to that application.

To create User Defined Groups based on User Defined field traverse to **CWHP → Common Services → Groups → Group Admin** link. In the **Group Administration** window,

- Select the **/CS/User Defined Groups** from the group selector and click on **Create** button.
- Give a group name and click on **Next** button. Select the **Variable** drop down box to have one of the four values “user_defined_field_0”, “user_defined_field_1”, “user_defined_field_2” and “user_defined_field_3”. Select an operator and value that matches the device value in DCR and click on **Add Rule Expression** button. Click **Next**.
- All the devices that match the criteria are shown in the right and click Next.
- Click **Finish** to create the new group under **/CS/User Defined Groups**. This newly created group can be accessed from any application screen in LMS.

7. Element Management: CiscoView, Resource Management Essentials, Device Center

7.1. Business Scenarios

As enterprise networks grow ever larger, it becomes a tedious job to manage hundreds even thousands of devices. With LMS applications discussed in this chapter, we can address problems like these:

1. How do I keep track of the inventory of devices on my network? How do I generate customized report digging out inventory information for just what I need?
2. How do I deploy configurations to multiple devices on my network without doing it one-by-one thru CLI? How do I keep track of the changes?
3. How do I automatically upgrade the software images on devices without spending too much time and impacting our business?
4. How do I monitor the Syslog messages and be automatically notified if something happens?
5. How do I keep track of the PSIRT alert and End of Sale/Service news from Cisco? What action shall I take?

All these questions and more can be answered with three LMS applications for elements management:

- Resource Management Essential (RME)
- CiscoView
- Device Center

7.2. Managing Devices in RME

RME Overview

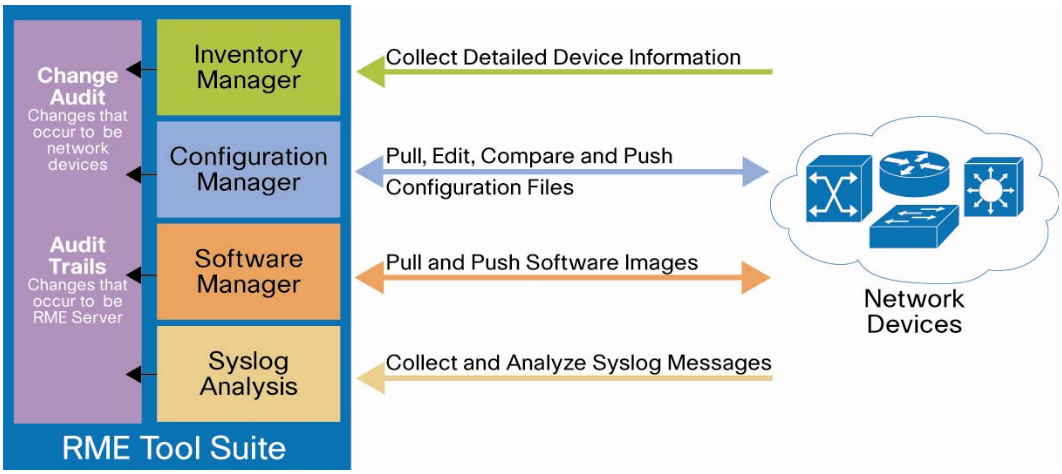
RME is the cornerstone application for the CiscoWorks LMS bundle of infrastructure management tools focusing primarily on configuration management tasks. It includes many automated features that simplify configuration management tasks, such as performing software image upgrades or changing configuration files on multiple devices. RME also includes some fault-management features, such as filtering of Syslog messages.

RME consists of the following major components:

- **Inventory Manager:** Builds and maintains an up-to-date hardware and software inventory providing reports on detailed inventory information. RME has many predefined reports right out of the box. You can also create custom report to dig out information for just what you need.
- **Configuration Manager:** Maintains an active archive of multiple iterations of configuration files for every managed device and simplifies the deployment of configuration changes. You can use ConfigEditor to change, compare, and deploy configuration to one device, or use NetConfig to deploy to multiple devices. You can design baseline template for different configuration needs. You can also specify which action to take after the configuration is deployed.

- **Software Manager:** Simplifies and speeds software image analysis and deployment. You can do an automatic upgrade analysis to help you select the right image. Then use the SWIM feature to import images, stage the image locally or remotely, then deploy to groups of devices.
- **Syslog Analysis:** Collects and analyzes Syslog messages to help isolate network error conditions. You can filter the Syslog messages and designate actions based on the messages.
- **Change Audit Services:** Continuously monitors incoming data versus stored data to provide comprehensive reports on software image, inventory, and configuration changes.
- **Audit Trails:** Continuously monitors and tracks changes made to the RME server by the system administrator.

Figure 38. RME Tool Suite



7.2.1. Inventory Management

Inventory Management provides comprehensive device information, including hardware and software details. This information is crucial for network maintenance, upgrades, administration, troubleshooting, and basic asset tracking. The inventory information can also be leveraged by other applications needing access to this same information without the need for additional device queries. Network administrators must often be able to quickly provide information to management on the number and types of devices being used on the network. The more information network administrators have in one central place about all the devices, the easier it is to locate necessary information, resolve problems quickly, and provide detailed information to upper management.

Inventory Management is also the starting point for many other management activities. For example, to upgrade the software image of a device, information about the amount of RAM, the modules installed, and the current software version is needed. All this data is collected by RME Inventory Management!

In chapter 4, we talked about how to populating the DCR and add devices to individual applications, such as RME's inventory. You can check out the RME devices under RME/Devices/Device Management/RME Devices.

Inventory Collection/Polling

At the time of RME installation, system jobs are created for both Inventory collection and polling, with their own default schedules.

Periodic inventory collection vs. Periodic inventory polling:

A periodic inventory collection job collects inventory data from all devices (devices in the “All Devices” group) and updates inventory database. The periodic polling polls all devices to check a certain MIB value to see whether the timestamp has changed. If there is a change in the timestamp, RME then goes ahead to retrieve inventory changes and collects and updates the inventory database.

Note: Inventory polling consumes much less bandwidth than inventory collection.

The default (out of the box) periodicity of the collector job is once a week and the default (out of the box) periodicity of the polling job is once a day.

10) The polling job detects most changes in all devices, with much less impact on your network and on the LMS server.

To change the default settings, traverse to **Resource Manager Essentials → Administration → Inventory → System Job Schedule**. The **System Job Schedule** dialog box displays the current collection or polling schedule, change the values and click **Apply**.

Reports Generator:

Once you add devices to RME from DCR, RME start retrieving inventory information based on the default schedule setting. RME has numerous predefined reports built-in for all the internal applications. These reports can be generated for view by going to RME/Reports/Report Generator. These applications include:

- Audit Trail
- BugToolkit
- Change Audit
- Contract Connection
- Device Credential
- Inventory
- Syslog

Under each application, you can generate different types of reports. For example, under **Inventory** you can generate these reports,

- 24-Hour Inventory Change Report
- Chassis Slot Details
- Chassis Slot Summary
- Detailed Device Report
- Hardware Report
- Software Report
- PSIRT Summary Report
- EoSale/EoL Report
- MultiService Port Details

- Hardware Summary Graph
- Software Version Graph
- Chassis Summary Graph

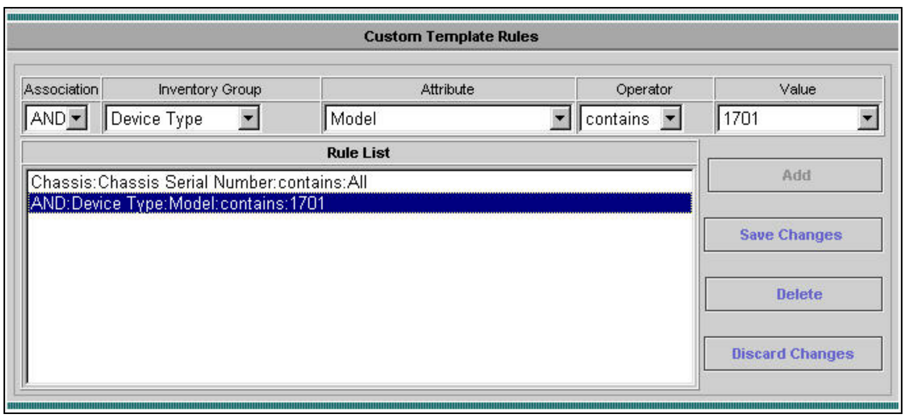
All these reports are generated with a set of pre-defined query variables. For example, Inventory/Software Report will list the software versions based on the categories of the devices. If you want to query a customized list of variables from the inventory, you can use **Custom Reports Template** for this as described below.

Custom Reports

To create a customized report with your interested query variables, such as “the serial number of all c1701 routers”, follow these steps,

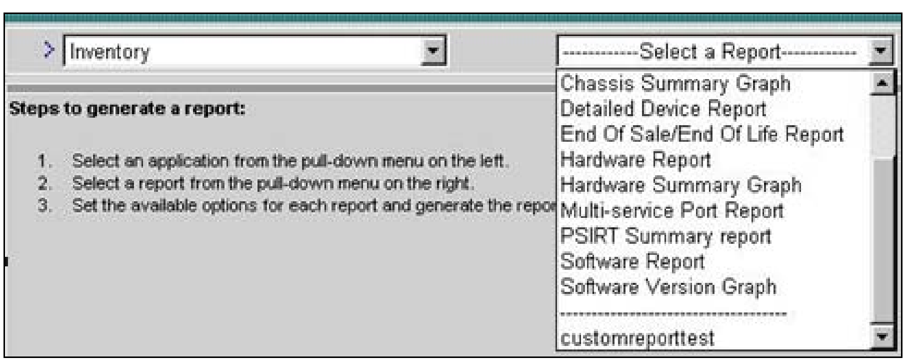
1. Create a custom report template. Go to **RME/Reports/Custom Reports Template**, choose application **Inventory**, give it a name such as **customreporttest**, make it public so everyone can see it, and define the rule as illustrated.

Figure 39. Custom Reports Template



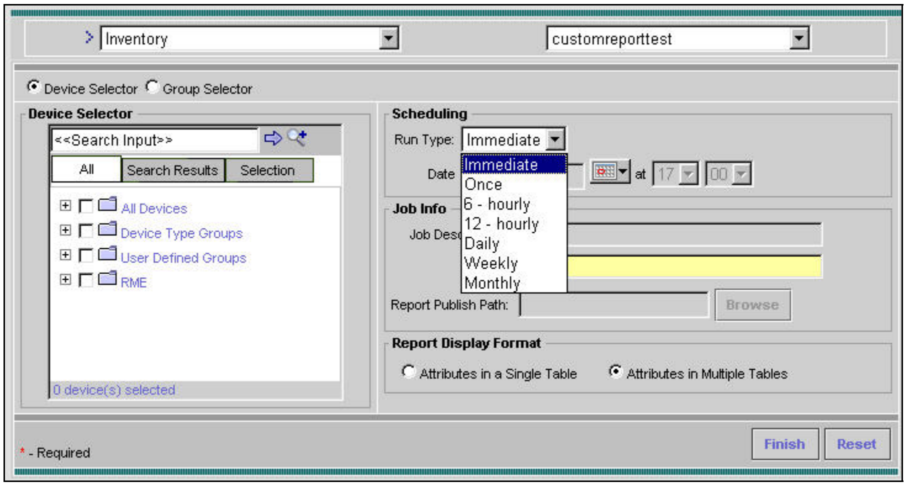
2. Go to **RME/Reports/Report Generator**, and choose **Inventory**. Notice the custom report template “**customreporttest**” shows up at the bottom of the dropdown list.

Figure 40. Custom Report



3. Choose your devices and generate the report. Here you can generate a one-time report, or schedule a job report to run daily, weekly, or monthly, and automatically sent to an email or publish to a central storage.

Figure 41. Generate Custom Reports



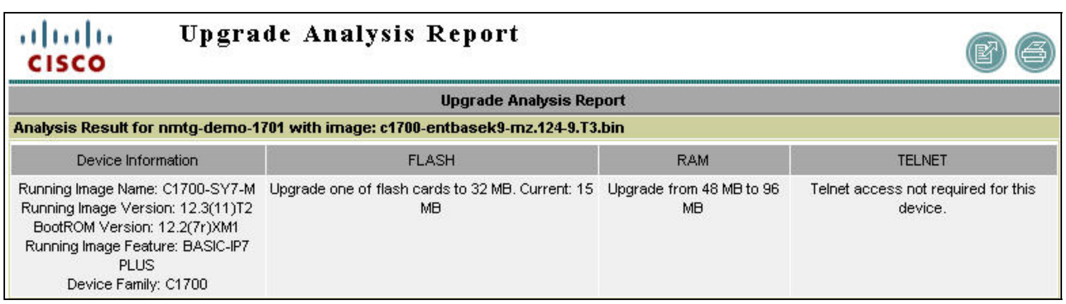
Note: Successfully generated reports are stored in the Archives. You can access the reports archives by selecting RME/Reports/Report Archives.

7.2.2. Software Image Management

RME greatly simplifies the work for software image management by building intelligence into the application to help the user pick and access device images from Cisco.com. Follow these steps to perform software upgrade to your devices.

Step 18. **Software Image Analysis.** RME helps the user to analyze the device and decide whether it has enough resources to run the new image. RME gives image recommendations for each selected device. Go to RME/Software Mgmt/Software Distribution/Upgrade Analysis, then log into Cisco.com. Once you log in, you can see all the available versions for this device. When you select a version, RME will give you suggestion what to do before upgrade.

Figure 42. Upgrade Analysis Report



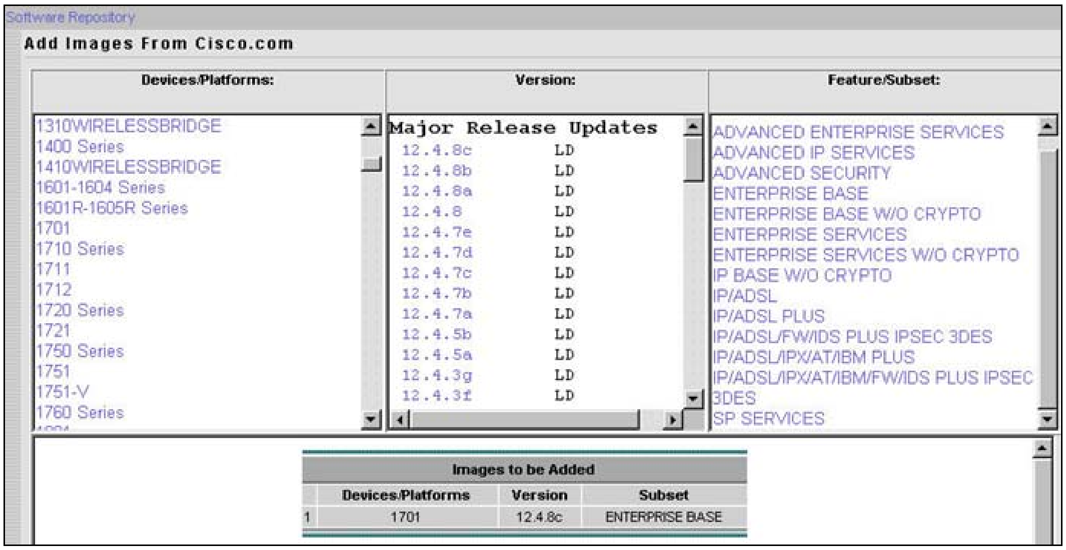
11) The criteria for image recommendation can be modified at **RME/Admin/Software Mgmt/View/Edit Preferences**.

Note: The number and type of variables analyzed depends on the device type and software version selected. The knowledge base used for analysis can be upgraded by going to **RME/Admin/Software Mgmt/Update Upgrade Analysis**.

Step 19. **Add image to Repository.** Instead of browsing around on Cisco.com trying to find the image file, RME helps the user to locate the image easily online and adds it into the local repository. You can schedule the download immediately or later.

Note: You can also export the image from the local repository to be used elsewhere.

Figure 43. Add Images from Cisco.com



Step 20. Create a job for image distribution. Instead of manually load the images one-by-one via CLI, the user can schedule a job to deploy images to a group of devices.

The methods of distribution include:

- **Basic:** This option enables you to select devices and then perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image for distribution.
- **By devices [Advanced]:** This option enables you to enter the software image and storage media for the device that you want to upgrade. The selected image and storage media is validated and verified for dependencies and requirements.
- **By images:** This option enables you to select a software image from the software image repository and then use it to perform an image upgrade on suitable devices in your network.
- **Use Remote Staging:** This option enables you to select a software image, store it temporarily on a device and then use this stored image to upgrade suitable devices in your network. This is helpful when the Resource Manager Essentials server and the devices (including the remote stage device) are distributed across a WAN.

Software Image Baseline Collection

It is recommended that you first import a baseline of all software images running on your network. The baseline imports a copy of each unique software image running on the network (the same image running on multiple devices is imported into the software library only once). The images act as a backup if any of your devices get corrupted and need a new software image or if an error occurs during an upgrade. If some devices are running software images not in the software repository then a synchronization report can be generated for these devices.

To schedule a Synchronization report:

a. Select **Resource Manager Essentials → Software Mgmt → Software Repository → Software Repository Synchronization**. Click **Schedule**. Enter the information and click **Submit**.
b. Import a baseline of all software images
c. Once Software Repository Synchronization job finished successfully you could create a job to import of all software images on your network by following steps
d. Select **Resource Manager Essentials → Software Mgmt → Software Repository**. Click **Add**. Select **Network and Use generated Out-of-sync Report** and click **Next**.
e. All running images that are not in the software repository will appear, click **Next**. Enter the **Job Control Information** and click **Next** and click **Finish**, when completed.

Note: If you have not selected the Use generated Out-of-sync Report option, it will take more time to show the software image selection dialog box.

Customize Software Management Settings

Software Management attempts downloading the software images based on the protocol order specified. While downloading the images, Software Management uses the first protocol in the list. If the first protocol in the list fails, these jobs use the second protocol and so on, until Software Management finds a transport protocol for downloading the images. The supported protocols are: RCP, TFTP, SCP and HTTP

In the **View/Edit Preferences** dialog box (**Resource Manager Essentials → Administration → Software Mgmt → View/Edit Preferences**) you can define the protocol order that Software Management has to use for software image download. Use **Add** and **Remove** buttons for selecting the protocol order.

Figure 44. Management Protocol Settings

7.2.3. Configuration Management

The Configuration Management tab in RME includes three applications:

1. **Archive Management:** The Archive Management application maintains an active archive of the configuration of devices managed by RME. It provides:,

- The ability to fetch, archive, and deploy the device configurations
- The ability to handle Syslog triggered config fetches, thereby ensuring that the archive is in sync with the device.
- The ability to search and generate reports on the archived data
- The ability to compare and label configurations, compare configurations with a baseline and check for compliance.

2. **Config Editor:** You can perform the following tasks using Config Editor:

Table 7. Config Editor Tasks

Task	Launch Point
Set or change your Config Editor preferences.	Select RME → Admin → Config Mgmt → Config Editor
View the list of previously opened files in private or public work area.	Select RME → Config Mgmt → Config Editor → Private Configs or Select RME → Config Mgmt → Config Editor → User Archive
Open a configuration file for editing in four ways: • **Device and Version** • **Pattern Search** • **Baseline** • **External Location**	Select RME → Config Mgmt → Config Editor → Config Files
View the status of all pending, running, and completed jobs. You can also create a new job or edit, copy, stop and delete a job that you have opened.	Select RME → Config Mgmt → Config Editor → Config Editor Jobs.

The RME Config Editor function can be used to edit a device configuration stored in the configuration archive and download it to the device. The Config Editor tool allows the user to make changes to any version of a configuration file, review changes, and then download the changes to the device.

When a configuration file is opened with Config Editor, the file is locked so that no one else will be able to make changes to it at the same time. While the file is locked, it is maintained in a “private” archive available only to the user who checked it out. If other users attempt to open the file to edit it, they will be notified that the file is already checked out and they can only open a “read-only” copy. The file will remain locked until it is downloaded to the device or manually unlocked within Config Editor by the user who checked it out or by a user that has network administrator and system administrator privileges.

3. **Netconfig:** You can perform the following tasks using NetConfig:

Table 8. NetConfig Tasks

Task	Launch Point
• **View and create NetConfig jobs using the NetConfig Job Browser.** • **View Job details (by clicking the Job ID hyperlink in the NetConfig Job Browser).** • **You can also:** **- Edit jobs** **- Copy jobs** **- Retry jobs** **- Stop jobs** **- Delete jobs**	Resource Manager Essentials → Config Mgmt → NetConfig or Resource Manager Essentials → Config Mgmt → NetConfig → NetConfig Jobs
Create and manage user-defined tasks.	Resource Manager Essentials → Config Mgmt → NetConfig → User-defined Tasks
Assign user-defined tasks to valid CiscoWorks users.	Resource Manager Essentials → Config Mgmt → NetConfig → Assigning Tasks

The NetConfig function provides a set of command templates that can be used to update the device configuration on multiple devices all at once. The NetConfig tool provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices. These templates can be used to execute one or more configuration commands on multiple devices at the same time. For example, to change SNMP community strings on a regular basis to increase security on devices, use the appropriate SNMP template to update community strings on all devices using the same job. A copy of all updated configurations will be automatically stored in the configuration archive. NetConfig comes with several predefined templates containing all necessary commands. The user simply supplies the parameters for the command and NetConfig takes care of the actual command syntax. These predefined templates include corresponding rollback commands; therefore, if a job fails on a device, the configuration will be returned to its original state.

Config Collection/Polling

The configuration archive can be updated with configuration changes by periodic configuration archival (with and without configuration polling). You can enable this using **Resource Manager Essentials → Administration → Config Mgmt → Archive Mgmt → Collection Settings**.

Note: A scheduled collection and polling are disabled by default as the customer's network may have sporadic bursts of traffic and the NMS should not take up the existing bandwidth. It is best for the customer to select the periodic collection and polling.

You can modify how and when the configuration archive retrieves configurations by selecting one or all of the following:

- Periodic Polling

  Configuration archive performs a SNMP query on the device, if there are no configuration changes detected in the devices, no configuration is fetched.

- Periodic Collection

  Configuration is fetched without checking for any changes in the configuration.

1. Select **Resource Manager Essentials → Administration → Config Mgmt → Archive Mgmt → Collection Settings**.
2. Select one or all the options.
   - Default Protocols used for Configuration Fetch and Deploy

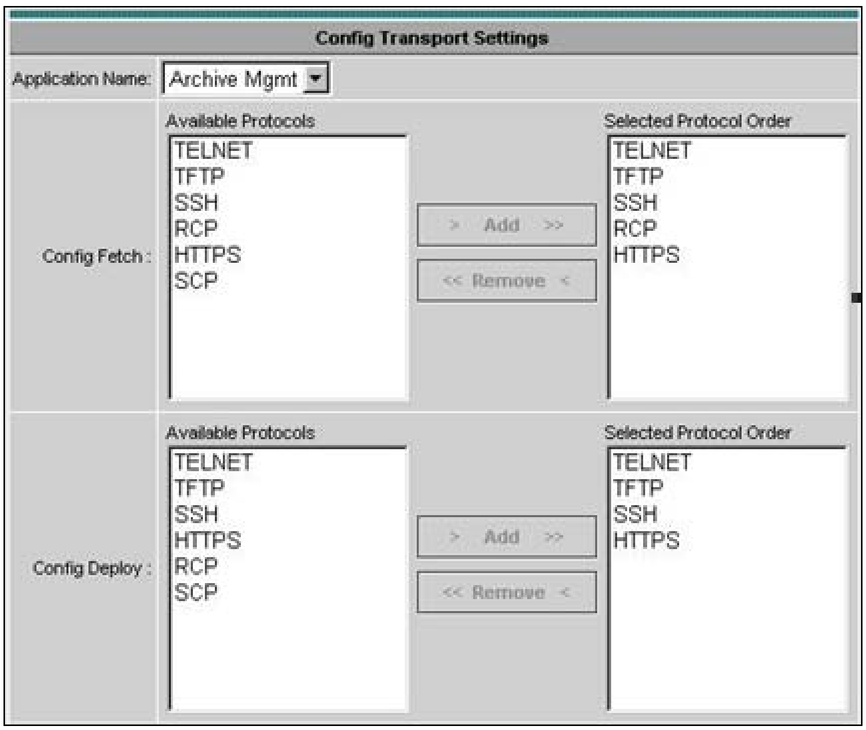
     Many protocols are used for performing a configuration fetch and deploy. The system provides a default order of protocols that will be used to fetch or deploy the configuration on the device. You can set the protocols and order for Configuration Management applications such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations.

The available protocols are:

- Telnet
- TFTP (Trivial File Transport Protocol)
- RCP (remote copy protocol)
- SSH (Secure Shell)
- SCP (Secure Copy Protocol)
- HTTPS (Hyper Text Transfer Protocol Secured)

To setup protocol ordering for Config Management, go to **Resource Manager Essentials → Administration → Config Mgmt → Transport Settings**.

Figure 45. RME Transport Settings



Protocol ordering can be setup for different config applications (Archive Mgmt, Config Editor and NetConfig) by selecting the application from the **Application Name** drop-down list. Select the protocol order by **Add** and **Remove** buttons on the screen and click **Apply**.

12) For secure communication between the server and device use SSH.

Change Management

All changes made on the network through LMS are recorded as part of the change audit. If syslogs are enabled on devices, any out of band changes made on the devices are also recorded as part of the change audit. Change Audit reports can be viewed by going to **Resource Manager Essentials → Reports → Report Generator**. Select Change Audit as the application and the report type could be either a 24 hour report, Standard Report or Exception Period Report. These reports help manage the changes on the network.

Resource Manager Essentials also provides the capability to have an **Audit Trail**. The **Audit Trail** provides a trail of all the changes that are being on the server i.e. addition or deletion of devices, credential change.

7.2.4. Syslog

LMS has the ability to collect and analyze syslogs received from devices in the network. The ability to collect syslogs helps manage the network more effectively. Enabling syslogs provides a multi fold advantage:

- LMS will collect and update any configuration and inventory changes on the network.
- Received syslogs can be analyzed and can also be used for further triggering automated actions.

Syslogs can be enabled on devices using NetConfig. A template for enabling Syslogs is built in NetConfig. You can access the template under **Resource Manager Essentials → Config Mgmt → NetConfig**. Create a NetConfig job by clicking NetConfig Jobs under the TOC.

Defining Message Filters

You can exclude messages from Syslog Analyzer by creating filters.

Select **Resource Manager Essentials → Tools → Syslog → Message Filters**.

A list of all message filters is displayed in a dialog box, along with the names, and the status of each filter—enabled, or disabled. Specify whether the filters are for dropping the Syslog messages or for keeping them, by selecting either Drop or Keep. If you select the Drop option, the Common Syslog Collector drops the syslogs that match any of the “Drop” filters from further processing. If you select the Keep option, Collector allows only the syslogs that match any of the “Keep” filters, for further processing.

Note: The Drop or Keep option applies to all message filters and is not on a per-filter basis.

7.2.5. Change Audit

Setting up Inventory Filters

Certain inventory attributes can change often and these changes can get logged whenever there is a collection. This may cause a lot of change audit messages to accumulate over a period of time. To prevent this inventory change filters can be enabled to not track change audits for these attributes. Inventory filters can be set by traversing **to Resource Manager Essentials → Administration → Inventory → Inventory Change Filter**.

Defining Exception Periods

An Exceptions period is a time you specify when no network changes should occur. Exception period can be set by traversing to **Resource Manager Essentials → Tools → Change Audit → Exception Period Definition**.

Select **Days of the week** from the **Day** drop-down list box. Start time and the end time from the **Start Time** and the **End Time** drop-down list box.

Click **Add**.

7.2.6. Job Management

Jobs need to be created for performing archive management, edit of configuration, download of configuration and device IOS/CatOS image management. There is a central location where all jobs created for various purposes in RME can be viewed. The central location can be accessed by traversing to CWHP → **Resource Manager Essentials** → **Job Mgmt** → **RME Jobs** link. All jobs can be searched on criteria like status of the jobs and type of job.

RME allows approval of jobs before they are executed. The following are the logical steps to configure job approval.

- Specify Approver Information. This can be done by traversing to **CWHP** → **Resource Manager Essentials** → **Administration** → **Approval** → **Approver Details** link. Note the user created here should have Approver role in the system (be it local security mode or ACS security mode).
- Specify Approver Lists. A list of approvers needs to be created. The list has to be named and assigned approvers. This can be done by traversing to **CWHP** → **Resource Manager Essentials** → **Administration** → **Approval** → **Create/Edit Approver Lists**. Provide an Approver name in the top left text field, click **Add**, select users from the list of available users field in the middle and click **Add** in the middle. Save the configuration of approval lists.
- Assign approval lists with the various functions like NetConfig, Config Editor, Archive Management and Software Management.
- Enable Approval policies on the various functions like NetConfig, Config Editor, Archive Management and Software Management.

The above steps will require all jobs created for NetConfig, Config Editor, Archive Management and Software Management to be approved before being executed.

All jobs pending approval can be viewed by traversing to the **CWHP** → **Resource Manager Essentials** → **Job Mgmt** → **Job Approval** link. The approver can either accept or reject the job. If a job is rejected then the status of the job is updated for the user who created the job.

7.2.7. Purge Policies

a. Configuration Management

You can specify when to purge archived configurations. This frees disk space and keeps your archive at a manageable size. You can purge configurations based on two criteria:

- Age. Configurations older than the number of days you specify are purged.
- The maximum number of versions of each configuration to keep.

  The oldest configuration is purged when the maximum number is reached. For example, if you set the maximum versions to keep to 10, when the eleventh version of a configuration is archived, the first is purged to keep the total number of archived versions at 10.

By default, the purging jobs are disabled.

1. Select **Resource Manager Essentials → Administration → Config Mgmt → Archive Mgmt → Purge Settings**.

The **Archive Purge Setup** dialog box appears.

2. Select **Enable**.
3. Click **Change** to schedule a purge job.
4. To specify when to purge configuration files from the archive, select one or both of the following options:
   - Click Maximum versions to retain and then enter the number of configurations to retain.
   - Click Purge versions older than and then enter a number and select days, weeks, or months.
   - Click Purge labeled files to delete the labeled configuration files.

The purged labeled files will be deleted only if it satisfies these conditions *Maximum versions to retain* and *Purge versions older than*.

5. Click Apply.

   b. Syslog

A default policy can be specified for the periodic purging of Syslog messages.

To specify the default purge policy:

Select **Resource Manager Essentials → Administration → Syslog → Set Purge Policy**. Specify the number of days in the Purge records older than field. Only the records older than the stated age (number of days that you specify here), will be purged. The default value is 7 days.

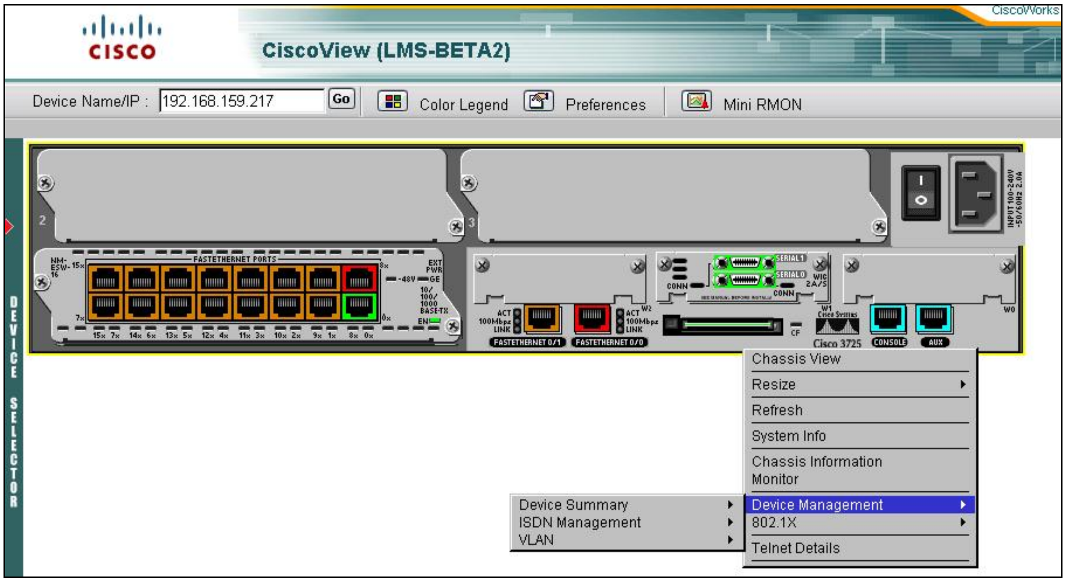
   c. Change Audit

A periodic purge or a forced purge of Change Audit data can be scheduled. This frees disk space and maintains the Change Audit data at a manageable size. Select **Resource Manager Essentials → Administration → ChangeAudit → Set Purge Policy**. Enter the values for each field and click Save, to save the purge policy that you have specified

7.3. Using CiscoView to Manage Devices

CiscoView is the primary Element Management System (EMS) to manage Cisco switches and routers. It is a graphical device management tool that uses SNMP v2/v3 to retrieve or set performance and configuration data from networked Cisco devices.

Figure 46. CiscoView



Using the performance data retrieved, CiscoView provides real-time views of Cisco devices. These views deliver a continuously updated physical/logical picture of device configuration and performance conditions. With the proper user authorization, the user can configure a Cisco device, and its cards and interfaces. The user can also monitor real-time statistics for interfaces, resource utilization, and device performance.

CiscoView simply uses SNMP to queries the configuration and performance of the device and displays the information graphically. Given the proper user authorization privileges, CiscoView can also be used to change or modify the configuration of the device using SNMP.

Therefore network managers can use CiscoView to:

- View a graphical representation of the device, including component (interface, card, power supply, LED) status.
- Configure parameters for devices, cards, and interfaces.
- Monitor real-time statistics for interfaces, resource utilization, and device performance.
- Set user preferences.
- Perform device-specific operations as defined in each device package.
- Manage groups of stackable devices.

To launch CiscoView:

- From LMS Portal, go to the **CiscoView Portlet**, and open **Chasis View**. Input device IP address or choose from **Device Selector** to open the chasis view.
- From LMS Portal, go to **Device Center Portlet**, open **Device Center**, input device IP address or choose from Device Selector, then click **CiscoView** under the Tools section of Device Center.

Mini-RMON Manager

CiscoView Mini-RMON manager is a real-time remote monitoring tool that provides option to enable RMON collection, display the collected ethernet statistics and lets you set thresholds against any of the collected statistics. An alarm is generated whenever the set thresholds are breached. This facilitates troubleshooting and improves network availability.

For more information about Mini-RMON manager, see http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/cs303/cv_ug/ug_app.htm.

For details about how to use the full features of CiscoView, see http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/cs303/cv_ug/index.htm.

7.4. Device Center

Device Center is a portal within the LMS bundle which provides the ability to gather and debug information about a particular device. The “Summary” in device center provides information about the device IP address, Device type, 24-hour Change Audit Summary, Last inventory and configuration collection times, Syslog summary, any fault related alerts for the device and the neighboring devices.

Device Center also provides a set of functions that help facilitate debugging, run reports on the device and any management tasks such as changing credentials.

Device Center is installed as part of the Common Services install and can be launched from **CWHP → Device Troubleshooting → Device Center**.

Figure 47. CiscoWorks Device Center

The procedure to launch debugging utilities on a particular device is given below.

- Browse through the group hierarchies to select a device or search for a particular device by typing in the name in the search utility provided above the group selector. Click on the link on the device name after you have selected it. This launches the summary and tools page for the device.
- You can look at the 24-hour reports on the device in the top half of the right frame and launch tools in the bottom half of the right frame.
- A suggested list of tools to be launched in a particular order as follows. The below list is not complete but helps to understand some of the tools available in Device Center.
  - Ping: Ping the device to see if it is reachable from the LMS server
  - Launch Credential Verification Report: Launch the Credential Verification Report to check for any missing credentials.
  - If the credentials are missing, launch the Edit Device Credentials tool to edit the credentials.
  - Launch Detailed Device Report on the device to view memory, flash, image, IP address information
  - Launch Fault History Report to view any faults that occurred in the last 24 hours or 31 days.
  - If some faults are found, go to CiscoView tool to view the chassis and make some changes on the interfaces or ports etc.
  - If the device is a switch, you can launch the switch port usage report for recently up, down or unused ports.

You can synch the archive or download a previous archive of the config or do image upgrade.

8. Network Management: Campus Manager

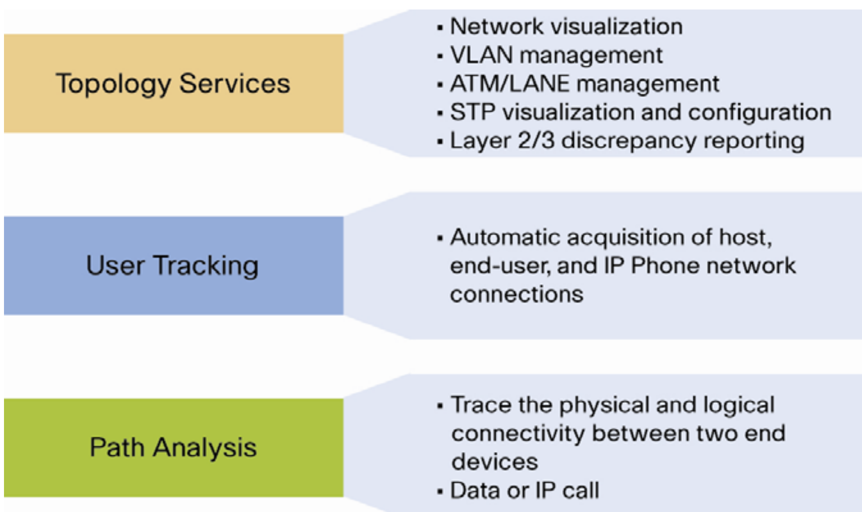
8.1. Business Scenario

Being a network management application, LMS Campus Manager addresses problems from the network administrators such as these following,

- How do I automatically discover the topology of my network which dynamically changes?
- How do I troubleshoot layer 2 problems such as VLAN, spanning tree without going thru CLI on switches one-by-one?
- How do I analyze the path between end stations without tracing the cables manually?
- How do I keep track of the users and end stations that move across campus and know which switch port they are connected to?
- How do I track down IP phones connected to which switch ports?

•Campus Manager has three major functions as in the figure as illustrated below:

Figure 48. Campus Manager



Topology Services

With topology services, you no longer have to trace cables from stack to stack through a wiring closet to determine which devices are connected through which ports. Topology Services auto discovers Cisco routers and switches on the network and displays the network layout in hierarchical topology maps. These maps make it easy to determine what types of devices are on the network, and how they are connected. In addition, topology services auto discovers ATM and VTP domains and VLAN memberships configured on the network, making it easy to view and track them. It also provides features to allow you to create and modify VLANs, LANE, and ATM services through an easy-to-use GUI. Automated discrepancy reports highlight physical and logical problems with the network configuration, making it easy to identify configuration errors such as line-speed mismatches on either end of a connection.

User Tracking

The User Tracking tool greatly simplifies the task of tracking user and end-station connections to the network. User Tracking automatically identifies all end stations connected to Cisco devices that have been discovered on the network, including printers, servers, and PCs. User Tracking also collects detailed information about each end-station, including MAC address, IP address, Domain Name System (DNS) hostname, port assignment, and VLAN memberships. In addition, User Tracking can be configured to collect usernames associated with end stations, from UNIX hosts, a Windows NT primary domain controller (PDC), or Novell Directory Services (NDS), making it easier to locate specific users on the network. User Tracking provides a means to track VLAN memberships, port assignments, and end-user host specifications.

From LMS 3.0, Campus Manager also supports dynamic user tracking. See details later in this chapter.

Path Analysis

Path analysis is a diagnostic tool for troubleshooting connectivity-related problems between end stations and Layer 2 and 3 devices. You can trace the Layer 2 or Layer 3 path between any two endpoints on the discovered network, making it much easier to narrow down where the problem might be when connectivity is lost. Path analysis provides more detailed information about each device than typical trace output, including interface type and speed and VLAN information. Output can be viewed in graphical, table, or trace output format.

8.2. How Campus Manager Works

In Chapter 5, we covered the device discovery and data collection. During the device discovery, Campus Manager uses SNMP to collect the Cisco Discovery Protocol (CDP) neighbor tables to build the current physical connectivity of the network. Then during data collection, Campus Manager collects (from each device) additional information such as interfaces, ports, Spanning Tree Protocol, VTP domains, VLAN configurations, Switch CAM tables and more.

These information is time stamped and stored in a database. Campus Manager can then be configured to automatically update this information at regular intervals. Any Campus Manager-collected information required by the network administrator is quickly retrieved from the Campus database and displayed in the many Campus Manager reports.

Because Campus Manager relies on Data Collection to maintain the latest knowledge about the network, we recommend data collection be scheduled at regular intervals to update the database with the most current knowledge. You can also do data collection on certain devices right before your operation.

8.3. Campus Manager Topology Service

Visualize the Network

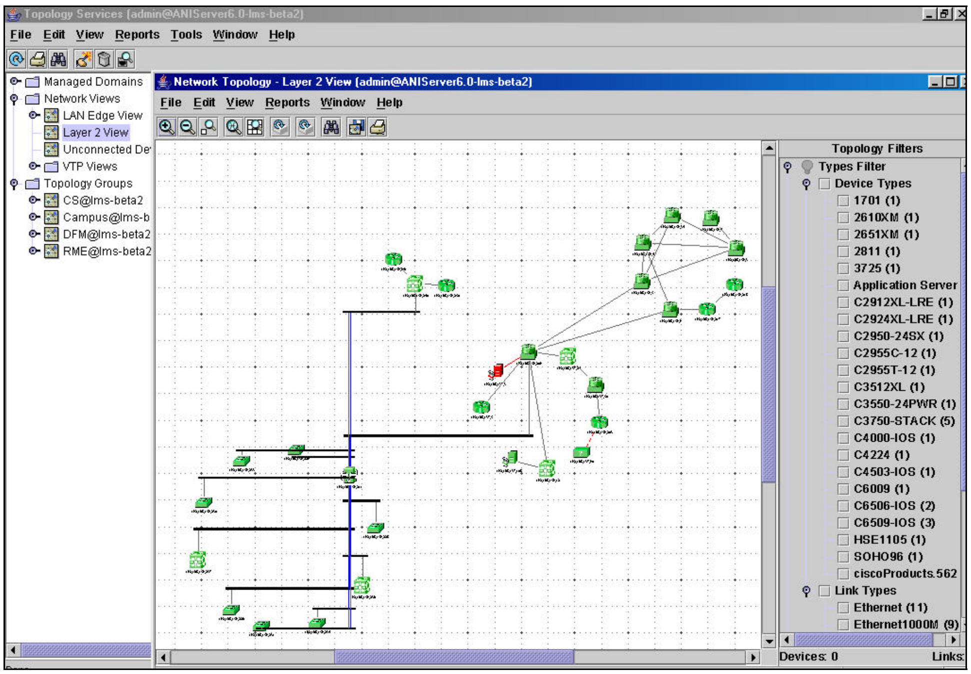
After Campus Manager gathered the device and network information from the data collection, the first thing to do is to verify the device discovery and data collection by visually creating the topology map,

1. From LMS Portal, go to the Campus Manager Portlet, and choose **Visualize**.
2. Choose **Topology Services**, and click on **Launch Topology Services**.

3. Once the **Topology Services** interface shows up, you can get a list and count of how many devices you have. Then click on **Network Services** and right click on a view such as **Layer 2 View**.
4. The **Layer 2 View** shows up. You can zoom in/out, drag and drop the icons to organize the view better, or go to **View** and choose **Relay out**, and choose **Circular** to organize the layout in better order. You can also show the IP addresses by turn on **Show IP** under **View/Show Labels**.

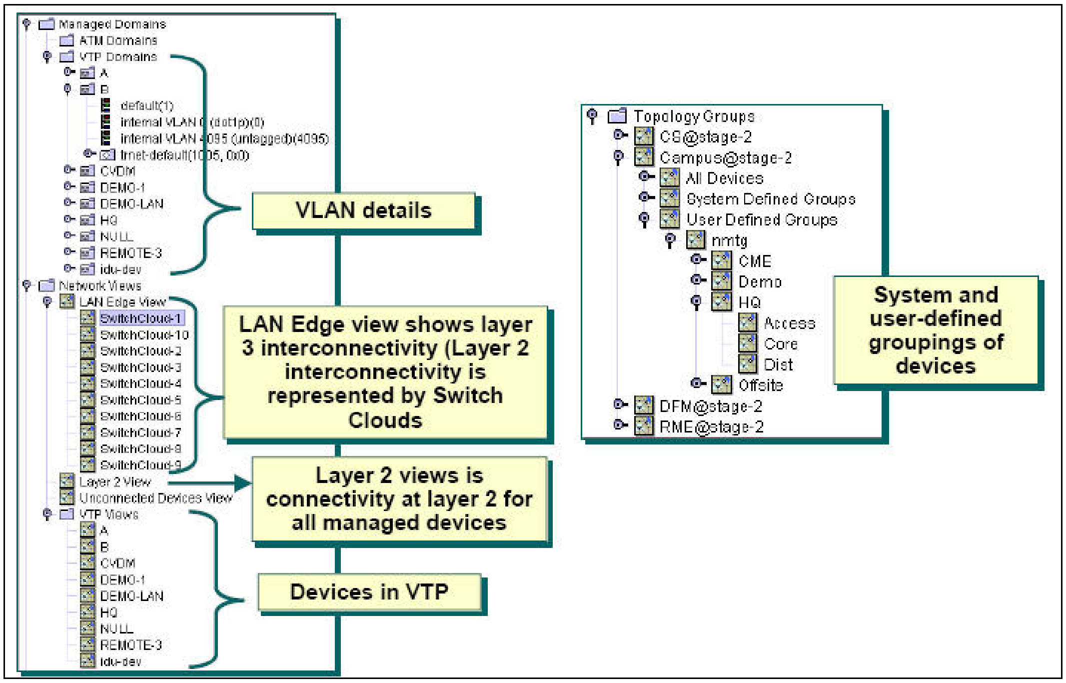
Note: From LMS 3.0, the topology services use Java Webstart technology which allows you launch the application directly from the Internet. Users do not need to install local Java plug-in and worry about version compatibility issues anymore.

Figure 49. Topology Services



Note: To see the list of map legends, check out the list at Help/Map Legend. On the left side of the Network Topology map, you have different network views.

Figure 50. VLAN Management



Here are the definitions of the different network views.

Table 9. Network Views in Campus Manager

Item	Description	Usage Notes
LAN Edge View	Shows network connectivity between Layer 3 devices that have routing characteristics. Devices without Layer 3 connectivity are placed in ATM Domain or Switch Cloud network views.	View: Device Attributes IPv6 Addresses Port Attributes Change Management IP Configure Inter-VLAN Routing Link Attributes Aggregate Link Attributes Delete Link(s)
Switch Cloud View	Displays the Layer 2 devices between two Layer 3 devices in your network.	View: Device Attributes IPv6 Addresses Port Attributes Service Attributes Change Management IP Configure Inter-VLAN Routing VLAN Report Link Attributes Configure EtherChannel Create Trunk Trunk Attributes TDR Report

Layer 2 View	Displays the Layer 2 information about your network, including ATM and LAN switches, routers, MLS devices, hubs, and switch probes.	View: Device Attributes IPv6 Addresses Port Attributes Service Attributes Change Management IP Configure Inter-VLAN Routing VLAN Report Link Attributes Configure EtherChannel Create Trunk Trunk Attributes TDR Report
Unconnected Devices View	Displays devices for which connectivity information could not be obtained, including devices not supported by Topology Services. This can include non-Cisco ATM devices discovered through Integrated Local Management Interface (ILMI), since it is an industry standard.	View: Device Attributes IPv6 Addresses Port Attributes VLAN Report Change Management IP Configure Inter-VLAN Routing Link Attributes
VTP Views	Shows the devices that are participating in VTP domains. VTP Views also shows the non-VTP devices and ATM domains connected directly to the VTP domain.	View: Device Attributes Port Attributes Service Attributes VLAN Report Change Management IP Configure Inter-VLAN Routing Link Attributes Configure EtherChannel Create Trunk Trunk Attributes TDR Report

Note: From menu **View**, select Panner to see the full view of the network. On the right side of the Layer 2 View, you can filter the devices on the map based on their device types, link types, PoE enabled and etc.

Customize the Map

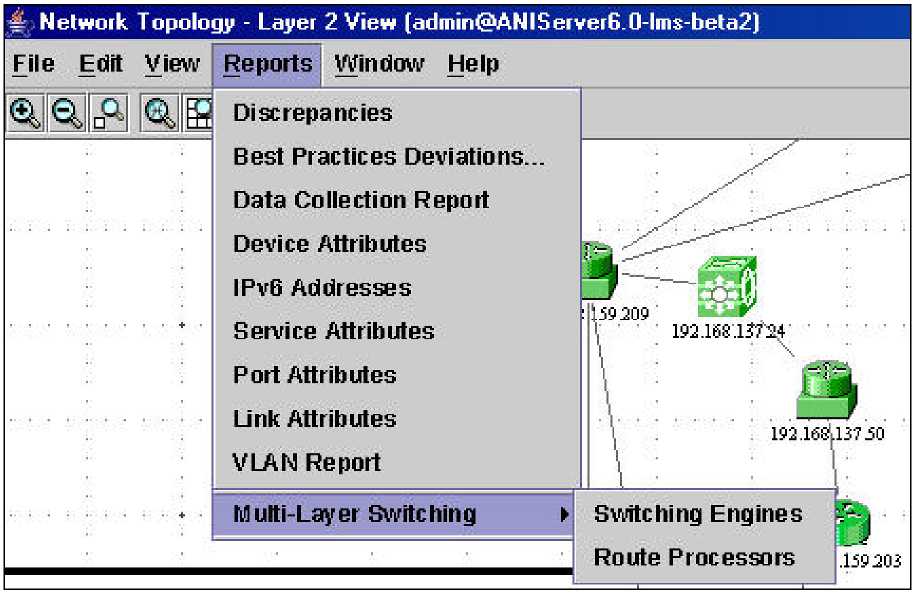
You can add a geographical map as background image to the map and position the network devices according to their locations. Do this by selecting **Edit/Map Preferences**, and choose background image.

If you have too many devices to put into one map, consider to organize them into Hierarchical Maps under the Topology Groups. For example, you can have one group for headquarter, and several groups for branch offices. Do this by going to **Campus Manager/Admin/Groups**, and create groups for different locations.

Launch the Reports

From the Network Topology, you can directly launch many reports. The variety of reports depend on which map you are launch from. For example, for “Layer 2 View” map, you can see these reports.

Figure 51. Campus Manager Layer 2 View



Note: Some of these reports can also be launched from Campus Manager/Reports. They are,

1. Best Practices Deviations Report
2. Device Attributes Report
3. Discrepancies Report
4. Port Attributes Report
5. VLAN Report

For detailed information about these reports, search for the latest Campus Manager User Guide at Cisco.com.

Network Configurations

From Topology Services, you can perform many network configurations on the GUI which is much easier than CLI commands. Under the Tools menu, configuration commands are listed as in the table below.

Figure 52. VLAN Management

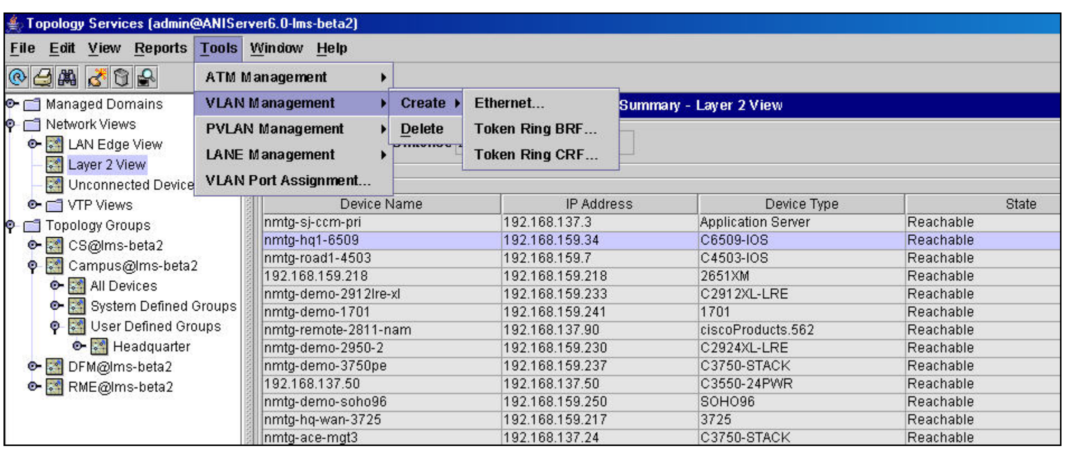


Table 10. Network Configuration Commands

ATM Management → Display VCs	Displays virtual connections per device, or between devices.

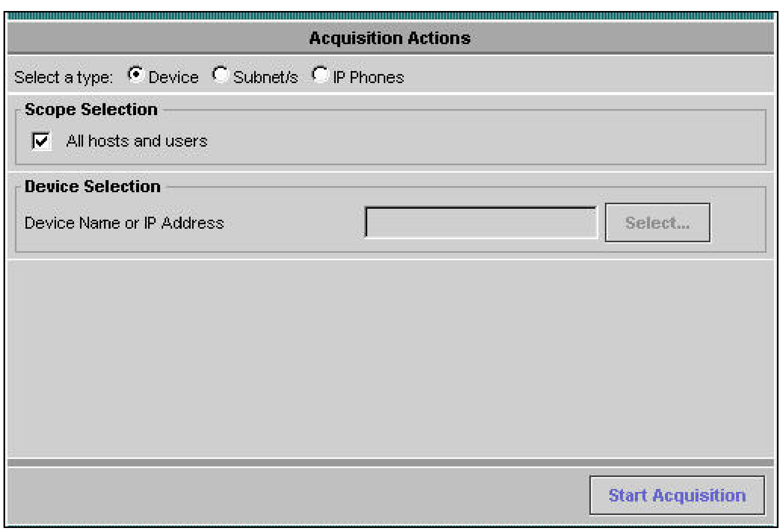
ATM Management → Create SPVC/SPVP	Creates a Soft Permanent Virtual Path or Connection. This function can only be performed by users logged in as Network Administrators or System Administrators.
ATM Management → OAM Ping	Performs an OAM ping to check VC connectivity.
ATM Management → Interface Configuration	Configures a new ATM interface configuration, or makes changes to the current interface configuration. This function can be performed only by users logged in as Network Administrators or System Administrators.
ATM Management → RMON Data Collection	Disables RMON Data Collection. This function can be performed only by users logged in as Network Administrators or System Administrators.
ATM Management → Template Manager	Creates, edits, or deletes traffic templates.
VLAN Management → Create	Creates an Ethernet, Token Ring BRF, or Token Ring CRF VLAN. This function can be performed only by users logged in as Network Administrators or System Administrators.
VLAN Management → Delete	Deletes the selected VLAN. This function can be performed only by users logged in as Network Administrators or System Administrators.
PVLAN Management → Create	Creates Private VLAN.
PVLAN Management → Delete	Deletes Private VLANs.
LANE Management → Add/Modify LANE Services	Adds or modifies LANE services for an Ethernet VLAN, a Token Ring CRF, or a standalone ATM-VLAN. This function can be performed only by users logged in as Network Administrators or System Administrators.
LANE Management → Configure Config Server	Configures the master and backup LE Config servers. This function can be performed only by users logged in as Network Administrators or System Administrators.
VLAN Port Assignment	Moves ports between VLANs in the same VTP domain.

8.4. User Tracking

User Tracking helps you to locate and track the end hosts in your network. Thus it provides you the information required to troubleshoot as well as to analyze any connectivity issues. The application identifies all end users connected to the discovered Cisco access layer switches on the network, including printers, servers, IP phones and PCs.

To start User Tracking, first start the acquiring process by accessing **Campus Manager/Admin/User Tracking/Acquisition**

Figure 53. Acquisition Actions



There are two major types of acquisition in User Tracking. They are

- Major Acquisition:

  Discovers all the end hosts that are connected to the devices managed by Campus Manager.
- Minor Acquisition:

Minor acquisition occurs on a device if any of the following changes take place:

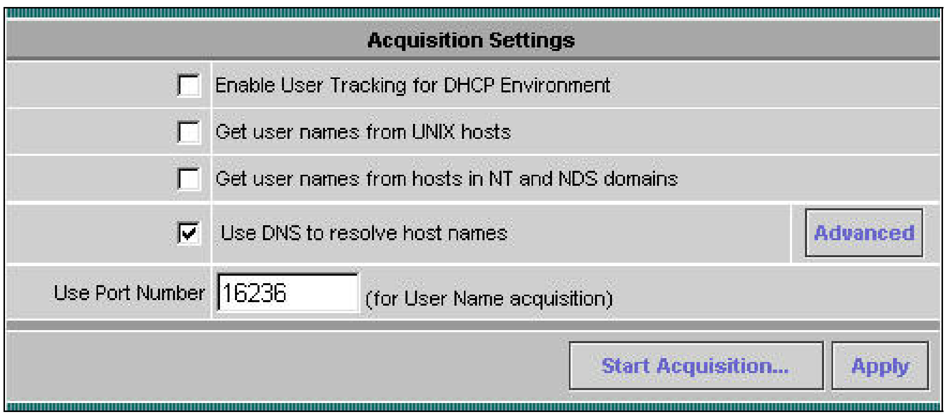
- A new device is added to the network.
- A port changes state. That is if it comes up or goes down.
- A new VLAN is added to the network.
- There is a change in the existing VLAN.

Minor acquisition updates the Campus database, only with the changes that have happened in the network. It is triggered at regular intervals. The default for these intervals is 60 minutes. You can configure the interval at which the acquisition takes place.

Traverse to Campus **Manager → Administration → User Tracking → Admin → Acquisition** and initiate a UT Major discovery. The following are the list of some important options that can be selected for a major acquisition.

- "Enable User Tracking for DHCP Environment" – This is an option for tracking the end hosts in case the IP address changes.
- "Use DNS to resolve host names" – This is an option for resolving the host names.

Figure 54. Campus Manager Acquisition Settings



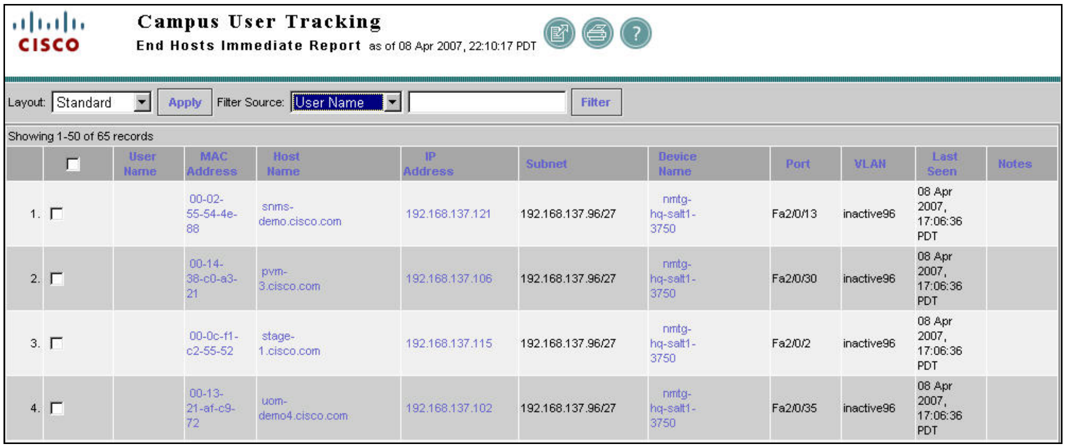
A schedule can be set for a major acquisition to happen. The schedule can be set by traversing to **Campus Manager → Administration → User Tracking → Admin → Acquisition → Schedule Acquisition** link.

A ping sweep can be enabled on all IP addresses in a subnet before starting a major acquisition. An option can be chosen to exclude certain subnets from the ping sweep.

Note: A Ping sweep operation is a very time consuming process.

After the acquisition is complete, you can generate a User Tracking report, which as illustrated in the following figure:

Figure 55. Campus User Tracking



		User Name	MAC Address	Host Name	IP Address	Subnet	Device Name	Port	VLAN	Last Seen	Notes
1.			00-02-55-54-4e-88	snms-demo.cisco.com	192.168.137.121	192.168.137.96/27	nmtg-hq-salt1-3750	Fa2/0/13	inactive96	08 Apr 2007, 17:06:36 PDT	
2.			00-14-38-c0-a3-21	pvm-3.cisco.com	192.168.137.106	192.168.137.96/27	nmtg-hq-salt1-3750	Fa2/0/30	inactive96	08 Apr 2007, 17:06:36 PDT	
3.			00-0c-f1-c2-55-52	stage-1.cisco.com	192.168.137.115	192.168.137.96/27	nmtg-hq-salt1-3750	Fa2/0/2	inactive96	08 Apr 2007, 17:06:36 PDT	
4.			00-13-21-af-c9-72	uom-demo4.cisco.com	192.168.137.102	192.168.137.96/27	nmtg-hq-salt1-3750	Fa2/0/35	inactive96	08 Apr 2007, 17:06:36 PDT	

User Tracking (UT) Reports

You can generate UT Reports by traversing to **CWHP → Campus Manager → Administration → User Tracking → Reports** link.

The following reports can be generated.

- UT provides the ability to quickly view reports on end hosts and IP Phones. A simple query can be input to view a subset of the end hosts or IP Phones present in UT.
- UT can run reports on switch port usage statistics of the switches. The switch port usage reports can be run for recently down, unused down and unused up ports.
- UT can list the jobs that are run periodically to generate reports. These jobs are for generating reports on end hosts, IP Phones, duplicate device entries and switch port usage. The report job listing can be found by traversing to **User Tracking → Reports → Report Jobs** link.
- You can generate Custom Reports for end hosts and IP Phones by selecting a group, evaluating a query on the group to subset the number of end hosts and IP Phones. You can generate Custom reports by traversing to **User Tracking → Reports → Custom Reports**. You can save these custom reports. These custom reports can be used while generating detailed reports on end hosts or IP Phones by going to **User Tracking → Reports → Report Generator**.

Note:

- The username in the User Tracking report is not filled unless UTLite is installed. UTLite is a utility that allows the network administration to collect user name from Primary domain controllers, Windows Active Directory and Novell directory servers. Combined with Campus Manager User Tracking, the administrator will not only know which end host is connected to which switch ports, but what is the UserID of the person logged into that end station.
- There is another tool, User Tracking Utility. It is a Windows toolbar to quickly query the User Tracking database outside the CiscoWorks user interface.

Purge Policies

End hosts and IP Phones can be deleted from User Tracking either on demand or on a specified interval after major acquisition by traversing to **CWHP → Campus Manager → Administration → User Tracking → Admin → Acquisition → Delete Interval**.

Archives or Jobs older than a particular date can also be purged by traversing to **CWHP → Campus Manager → Administration → User Tracking → Admin → Reports → User Tracking Purge Policy**.

Dynamic User Tracking

User Tracking generates reports on various functions and attributes of the end hosts and devices connected to your network that are managed by Campus Manager. These reports are generated by polling the network at intervals set by the network administrator.

In addition to polling the network at regular intervals, Campus Manager 5.0 tracks changes about the end hosts and users on the network to provide real-time updates.

Dynamic Updates are asynchronous updates that are based on SNMP MAC notifications traps.

When an endhost is connected to a switch managed by Campus Manager, an SNMP MAC notification trap is immediately sent from the switch to the Campus Manager Server, indicating an ADD event. This trap contains the MAC address of the end host connected to the switch.

Similarly if an end host is disconnected from a switch port, an SNMP MAC notification trap is sent from the switch to the Campus Manager indicating a DELETE event. Thus Campus Manager provides real time data about end hosts coming into/moving out of the network.

The difference between UT Major Acquisition and Dynamic UT process is:

- Campus Manager collects data from the network at regular intervals for UTMajor Acquisition.
- In Dynamic UT, the devices send traps to Campus Manager as and when changes happen in the network.

This implies that you need not wait till next UTMajor Acquisition cycle to see the changes that has happened in your network. This is an improvement over the earlier versions, where updates on endhost information happened based on polling cycle.

As a result of Dynamic updates, the following reports contain up-to-date information:

- End-Host Report

  Contains information from UT Major Acquisition **and** the recently added end-hosts.
- History Report

  Contains information from UT Major Acquisition **and** the recently disconnected end-hosts/end-hosts that have moved between ports or VLANs.
- Switch Port reports

  Contains information about the utilization of switch ports.

SNMP Traps are generated when a host is connected to the network, disconnected from the network or when it moves between VLANs or ports in the network.

To enable Dynamic Updates feature:

- Switches must be managed by Campus Manager.
- Configure Campus Manager as a primary or secondary receiver of the MAC notifications.
- Configure all devices to send traps to the Trap Listener port of the Campus Manager server (This is the port number that you would have configured on Campus Manager Administration screen).
- Configure DHCP snooping on the switches. Dynamic Host Configuration Protocol (DHCP) snooping is a security feature that filters untrusted DHCP message received from outside the network or Firewall, and builds and maintains a DHCP snooping binding table. Campus Manager queries the CISCO-DHCP-SNOOPING-MIB to get the IP address of the end-host connected. For details on configuring DHCP, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cddhcp.htm.
- User Tracking collects username and IP address through UTLite for Windows environment.

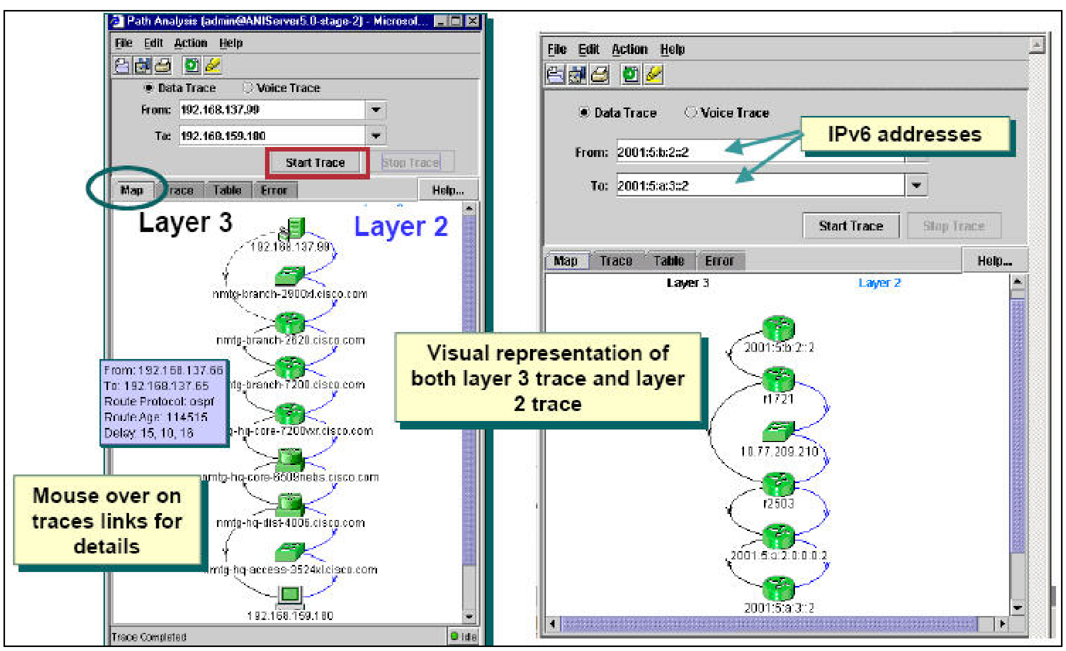
Note: In the Windows environment you can either install UTLite or configure DHCP snooping to get IP address of the end host. They can also co-exist. If you have neither installed UTLite nor enabled DHCP snooping, the IP address of the end-host connected will be updated only in the next UT Major Acquisition cycle.

8.5. Path Analysis

Path Analysis is the third application in Campus Manager. It is an operation and diagnostic tool that traces the connectivity between two specified devices on your network; not just the Layer 3 path like the “trace route” command, but also the physical path providing you with more detailed info about the path for troubleshooting. For extended troubleshooting efforts, Path Analysis can also be scheduled to occur at a specific time or recurring periodically.

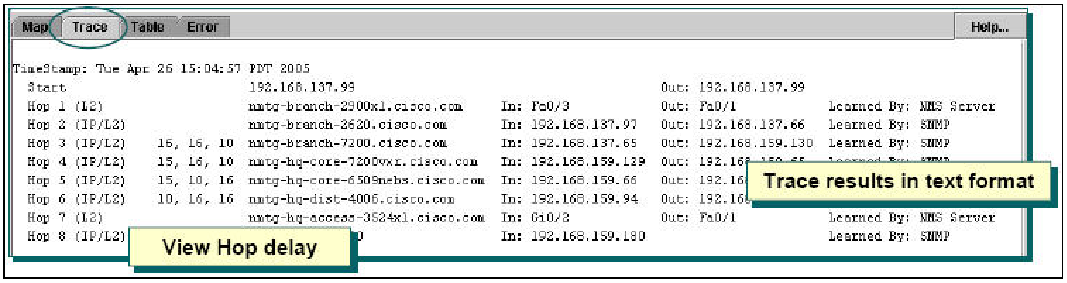
When you generate a path analysis between two end points, you can view the reports in three different options, Map, Trace, and Table. Here is the map view showing both the Layer 2 and Layer 3 path.

Figure 56. Path Analysis



Here is the trace view:

Figure 57. Trace View

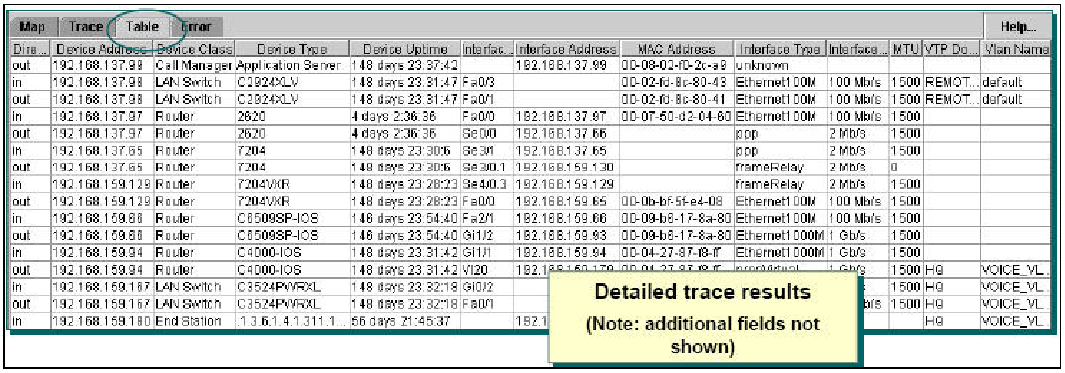


The Trace tab displays results of the trace in a format very similar to the common trace route command. Use this output to determine the delay between hops along the path, which can help identify slow response times and bottlenecks.

In addition to the information usually displayed from a trace route command, the Path Analysis trace output includes layer 2 hops and both incoming and outgoing interfaces. It also displays the method by which Path Analysis obtained the information, in the Learned By field. Path Analysis uses one of the following four methods to determine each hop on a traced route: SNMP requests, NMS server queries, trace route command, best guess. If “best guess” is listed in the Learned By column, this indicates that Path Analysis was not able to obtain the necessary information from one of the other three sources, or information from some of these sources was conflicting. Best-guess information might not be accurate, but it should not be considered very reliable.

Here is the table view:

Figure 58. Detailed Trace Results



Dire...	Device Address	Device Class	Device Type	Device Uptime	Interfac...	Interface Address	MAC Address	Interface Type	Interface...	MTU	VTP Do...	Vlan Name
out	192.168.137.99	Call Manager	Application Server	148 days 23:37:42		192.168.137.99	00-08-02-f0-2c-a9	unknown				
in	192.168.137.98	LAN Switch	C2924XLV	148 days 23:31:47	Fa0/3		00-02-fd-8c-80-43	Ethernet100M	100 Mb/s	1500	REMOT...	default
out	192.168.137.98	LAN Switch	C2924XLV	148 days 23:31:47	Fa0/1		00-02-fd-8c-80-41	Ethernet100M	100 Mb/s	1500	REMOT...	default
in	192.168.137.97	Router	2620	4 days 2:36:36	Fa0/0	192.168.137.97	00-07-50-d2-04-60	Ethernet100M	100 Mb/s	1500		
out	192.168.137.97	Router	2620	4 days 2:36:36	Se0/0	192.168.137.66		ppp	2 Mb/s	1500		
in	192.168.137.65	Router	7204	148 days 23:30:6	Se3/1	192.168.137.65		ppp	2 Mb/s	1500		
out	192.168.137.65	Router	7204	148 days 23:30:6	Se3/0.1	192.168.159.130		frameRelay	2 Mb/s	0		
in	192.168.159.129	Router	7204VXR	148 days 23:28:23	Se4/0.3	192.168.159.129		frameRelay	2 Mb/s	1500		
out	192.168.159.129	Router	7204VXR	148 days 23:28:23	Fa0/0	192.168.159.65	00-0b-bf-5f-e4-08	Ethernet100M	100 Mb/s	1500		
in	192.168.159.66	Router	C6509SP-IOS	146 days 23:54:40	Fa2/1	192.168.159.66	00-09-b6-17-8a-80	Ethernet100M	100 Mb/s	1500		
out	192.168.159.66	Router	C6509SP-IOS	146 days 23:54:40	Gi1/2	192.168.159.93	00-09-b6-17-8a-80	Ethernet1000M	1 Gb/s	1500		
in	192.168.159.94	Router	C4000-IOS	148 days 23:31:42	Gi1/1	192.168.159.94	00-04-27-87-f8-ff	Ethernet1000M	1 Gb/s	1500		
out	192.168.159.94	Router	C4000-IOS	148 days 23:31:42	Vl20	[illegible]	[illegible]	[illegible]	1 Gb/s	1500	HQ	VOICE_VL...
in	192.168.159.167	LAN Switch	C3524PWRXL	148 days 23:32:18	Gi0/2	[illegible]	[illegible]	[illegible]	[illegible]	1500	HQ	VOICE_VL...
out	192.168.159.167	LAN Switch	C3524PWRXL	148 days 23:32:18	Fa0/1	[illegible]	[illegible]	[illegible]	[illegible]	1500	HQ	VOICE_VL...
in	192.168.159.180	End Station	.1.3.6.1.4.1.311.1...	56 days 21:45:37		192.1[illegible]	[illegible]	[illegible]	[illegible]		HQ	VOICE_VL...

The Table tab provides additional information about the trace, if available. Details will be available only if Path Analysis can obtain the information from the server database or User Tracking table.

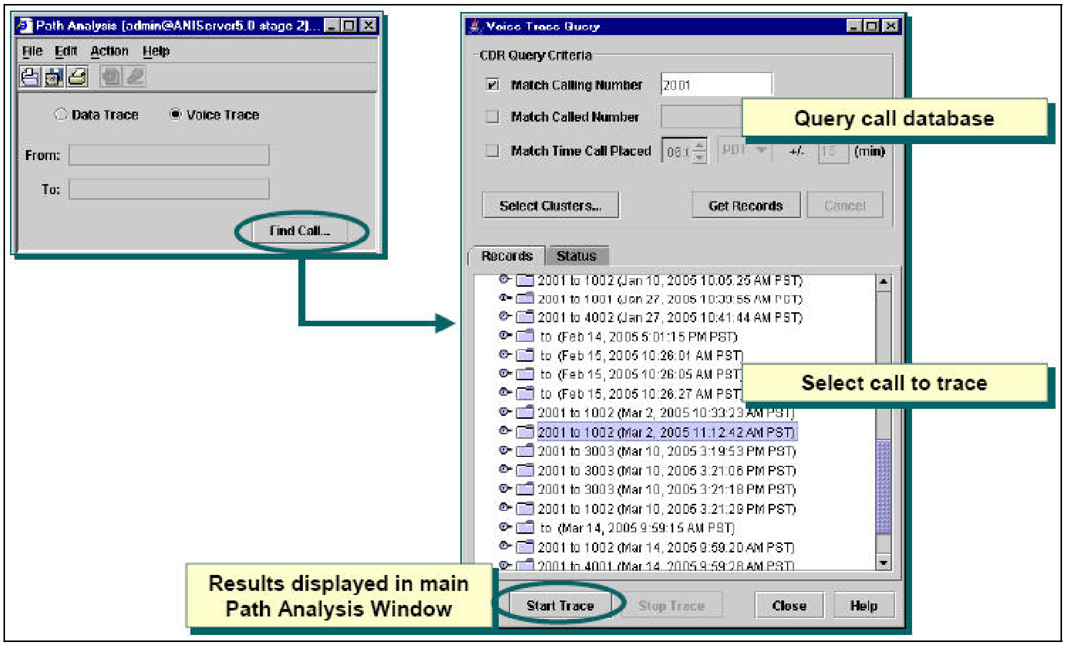
The following information is listed in a table format:

- Device IP address, alias, class, type, and uptime
- Connected interface name, address, mask, type, speed, MTU, and index number
- MAC address
- VTP domain and VLAN name
- ATM fabric, ELAN name, virtual path identifier (VPI), and virtual channel identifier (VCI)

In addition to data traces, Path Analysis can also be used to trace the path for IP calls. You can determine the data paths and troubleshoot the signaling paths that voice-over-IP (VoIP) traffic uses on the network by data tracing the path from the IP Phone to the Cisco Call Manager. Additionally, you can trace the flow of voice packets for three types of VoIP telephone calls on your data network: completed calls, calls in progress, potential calls (calls that did not occur, but may occur in the future). For calls in progress or potential calls, use the IP phones IP addresses garnered from the User Tracking data base and perform a Data Trace.

To trace a completed call, use the Voice Trace option. Performing a voice trace requires only slightly more effort when setting it up. From the Path Analysis window select Voice Trace. This will activate the button Find Call; select it. This will bring up the dialog to query the Call Details Record (CDR) database on any Cisco Call Manager known to Campus. Query the database to find the completed call to trace, highlight it, and select Start Trace.

Figure 59. Voice Call Tracing



9. Fault Management: Device Fault Manager

9.1. Business Scenarios

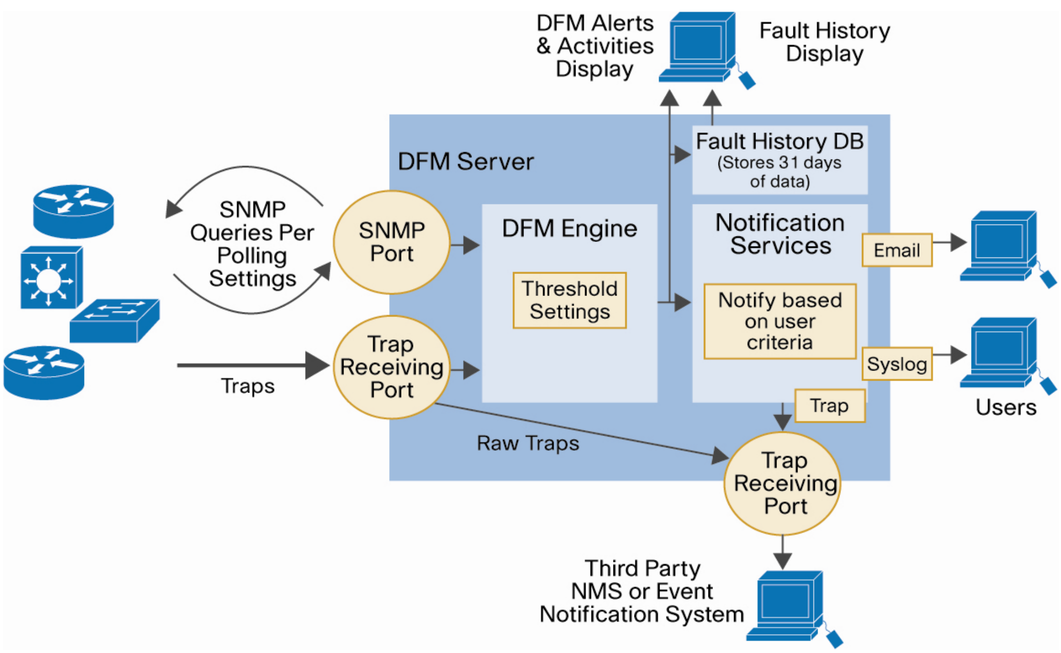
On a daily basis, Network Administrators face many challenges to maintain a healthy running network to support business needs. They constantly ask questions like:

- How do I quickly and easily detect, isolate, and correct network faults?
- How do I monitor not only up and down status, but also potential problems?
- How do I provide valuable insight into the relative health of a device and the network?
- How do I address problems before network service degradation impacts users?
- How do I minimize downtime and service degradation?

CiscoWorks Device Fault Manger proactively monitors the network for indicators of device or network faults, enabling the network administrator to know exactly where/what to fix, thus avoiding costly network service degradation. DFM has the built-in intelligence to determine what variables and events to look for to determine the health of a Cisco device, without user intervention, for true fault management.

9.2. DFM Architecture

Figure 60. DFM Architecture



As in Figure above, CiscoWorks DFM uses SNMP polling, and SNMP traps to discover and display real-time faults. DFM provides rules to analyze events that occur and help determine when a probable fault has occurred on Cisco devices. It allows you to configure immediate notifications on certain types of faults and stores events and alerts for 31 days in the fault history.

DFM already knows which MIB variables to poll for each different device to determine the status and health of the device. The necessary threshold values have also been predefined based on extensive testing. Therefore DFM can begin fault and performance monitoring right out of the box after the devices are added to the DFM inventory.

9.3. Device Management in DFM

The first thing to do in DFM is to pick which devices to import from DCR to be managed in DFM. By default, devices need to be manually imported into DFM. You can also set up automatic synchronization with DCR by enable the “Filter Selector”. See Chapter 5 for details on this topic.

Check the Device Status

After devices are imported into DFM, go to DFM/Device Management/Device Summary to see the list of devices and their states in the DFM inventory. The states of DFM devices are:

- **Known:** The device has been successfully imported, and is fully managed by DFM.
- **Learning:** DFM is discovering the device. This is the beginning state, when the device is first added or is being rediscovered. Some of the data collectors1 may still be gathering device information.
- **Questioned:** DFM cannot manage the device. For example, a Call Manager will show up as “questioned” if it’s included in the DFM inventory.
- **Pending:** The device is being deleted. (DFM is waiting for confirmation from all of its data collectors before purging the device and its details.)
- **Unknown:** The device is not supported by DFM.

To get more details of the devices, go to DFM/Device Management/Device Details tab.

13) Rediscover a Device: If a device is in stuck in “learning” state, you can rediscover the device by going to DFM/Device Management/ Rediscover.

9.4. Alerts and Activities

To monitor the alerts and activities on the devices, you need to create a view first.

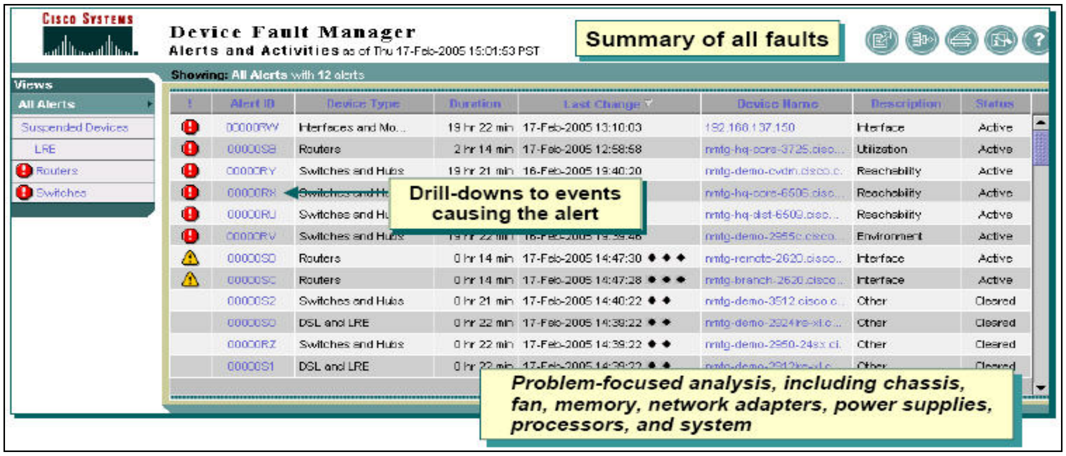
Create/Activate a View

Go to DFM/Configuration/Other Configuration/Alerts and Activities, click on **create** and include the devices for this view. You can create different views for different groups of devices.

After the view is created, select it to activate it. Then you can see the view by going DFM/Alerts and Activities. This will launch a browser window to show the alerts and activities on the devices.

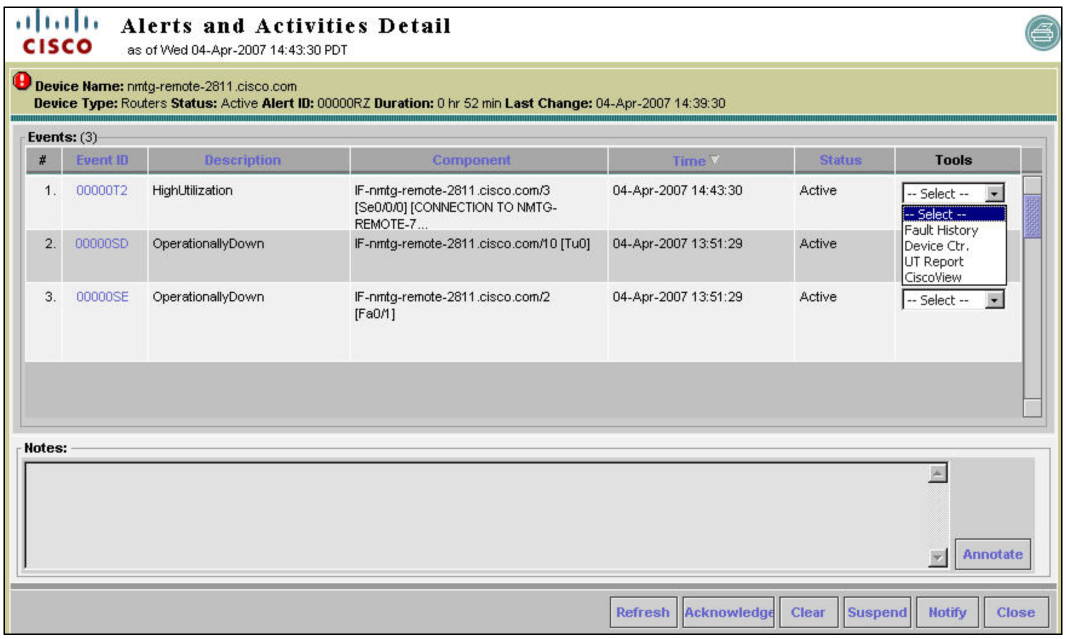
From this Alerts and Activities, you can monitor the faults going on in your network and start taking actions to correct it.

Figure 61. Summary of All Faults



Clicking on the Alert ID will open the Alert and Activities detail window:

Figure 62. Alerts and Activities Detail



From here, you can drill down to the event by clicking on the Event ID or taking actions to:

- **Acknowledge:** Changes the event status to Acknowledged.
- **Clear:** Clears and deletes alarms and events.
- **Suspend:** Suspends polling and trap processing on the device or device component by opening a Detailed Device View (DDV), from which you can perform the suspend command.
- **Notify:** Sends e-mail notification of the alert.

You can also launch the tools to help with the troubleshooting of the events,

- **Fault History:** Opens a 24-hour Fault History report on the component.
- **Device Ctr.:** Opens the CiscoWorks Device Center, which provides a centralized point for reports, tools, and tasks that you can perform on the selected device.

- **UT Report:** Opens a User Tracking End Host report that lists end-user hosts in the network. (This tool is available if Campus Manager is installed.)
- **CiscoView:** Opens the CiscoView chassis view for the device. (This tool is available if CiscoView is installed.)

9.5. Notification Services

The Alerts and Activities display requires constant visual contact to monitor what is going on with the network. To free the administrators from 24/7 visual contact with the Alerts and Activities display, DFM allows for alternate means to notify personnel, such as email, SNMP traps, and Syslog message. Each of these notification mechanisms would provide a summary of the alert/event. The receiver of the notification could then return to DFM for more details.

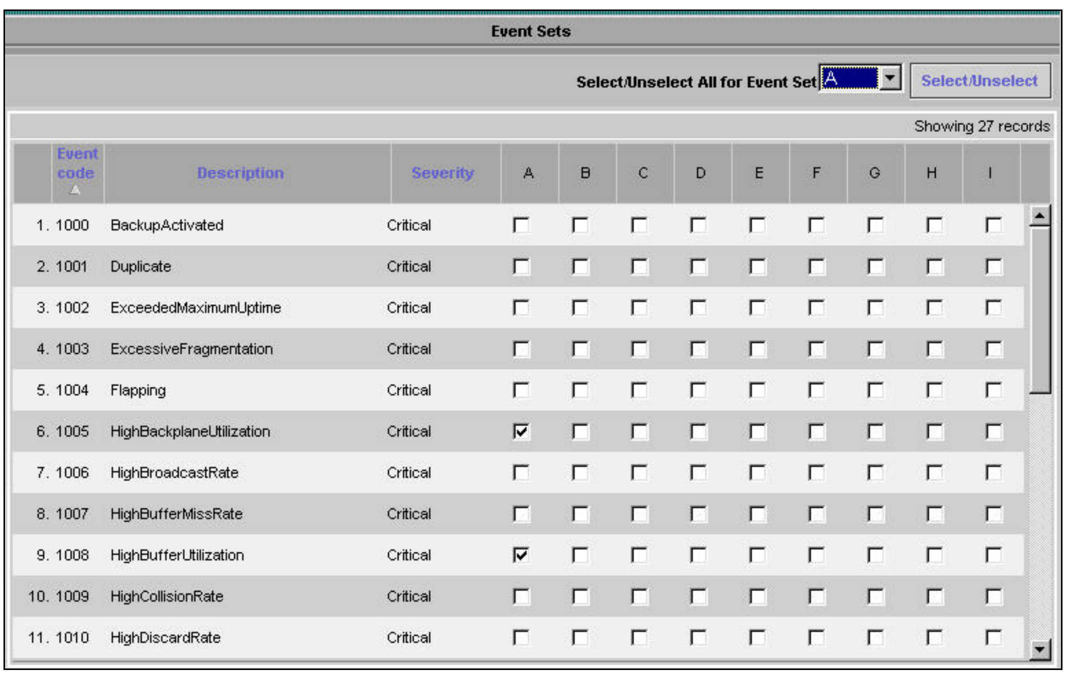
Notification Groups

Notifications are sent based on subscripts to notification groups. Basically a notification group is a set of events and alerts occurring on a set of devices. This allows for different recipients or notification mechanisms for different devices and alerts for ultimate notification flexibility.

Here are the setup steps for a typical application where the user receives email based on the notification group.

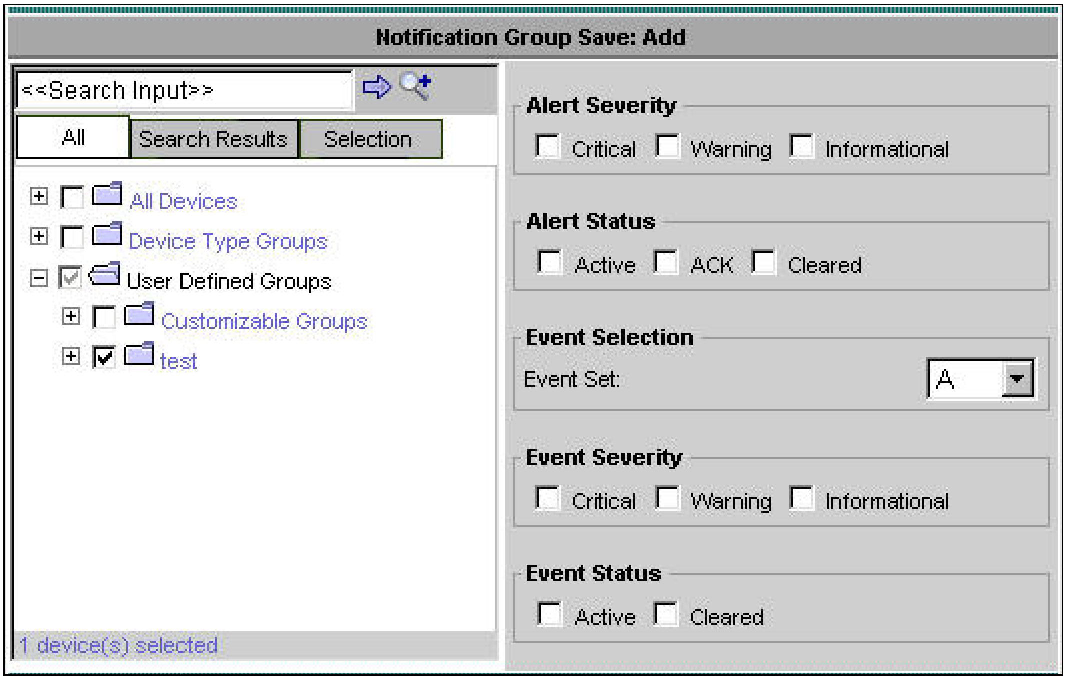
1. Set up the default email server. Go to DFM/Configuration/Other Configurations/SMTP Default server.
2. Create a custom group to select devices to be monitored on. See in this chapter, the section titled “Group Administration”.
3. Create event set to select the interesting events for the user. Go to DFM/Notification Services/Event Sets. Up to 9 event sets can be created.

Figure 63. Event Sets



4. Create notification group. Go to DFM/Notification Services/Notification Groups. Select the custom group created in step 2 and the event set created in steps 3.

Figure 64. Notification Group



5. Create email subscription. Go to DFM/Notification Services/ Email notification, and select the notification group, and then enter the email address as the destination.

Polling and Threshold Management

For the faults and events to show up in DFM, polling and threshold parameters need to be set. By default, DFM has built-in polling and threshold parameters based on device types and interface types. You can customize the polling and Threshold parameters can be set by traversing to **CWHP → Device Fault Manager → Configuration → Polling and Threshold link**.

Polling parameters are used to make DFM Server poll the devices in the various groups in specified intervals.

Threshold Parameters are used to determine the thresholds for various devices. When these thresholds are crossed for the various types of devices, alerts are raised in DFM Server.

9.6. Group Administration

System Defined Groups

When devices are imported from DCR to DFM, they are automatically grouped into system defined groups. These groups are:

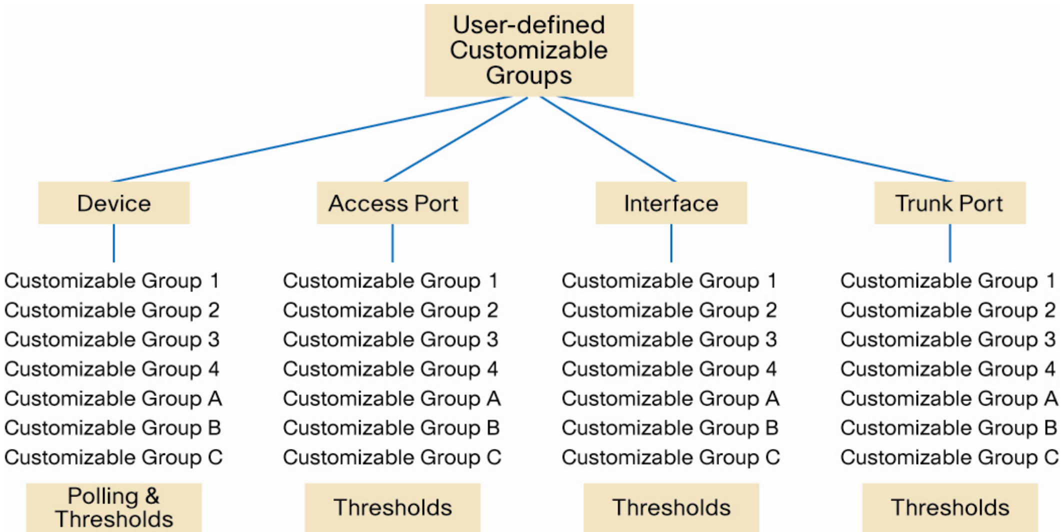
- Access Port Groups
- Interface Groups
- Trunk Port Groups

Note: DFM system defined groups cannot be added, modified or deleted.

Custom Groups

If you want to mange the device differently by setting customized polling and threshold parameters, you can create custom groups. DFM provides 28 customizable groups, which are divided into four categories.

Figure 65. Customizable Groups



To create DFM groups traverse to **Configuration → Other Configuration → Group Administration link**.

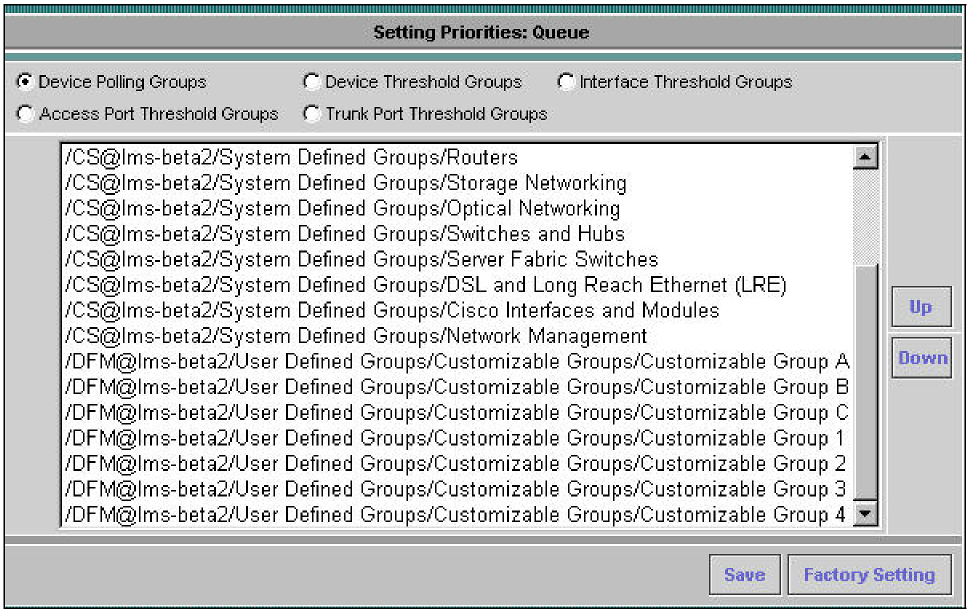
1. Select a customization group name.
2. Populate the group with devices and/or components.
3. Modify the polling and/or thresholds for the group.
4. Finally, change the priority of the customizable. See details next.

Priority Setting

When you create a custom group and add devices to it, the devices now belong to two groups, the system defined group or the default group, and the new custom group. You need to set the priority of the custom group to be higher than the system defined group.

To change the priority setting, go to DFM/Configurations/Polling and Thresholds/Setting Priorities.

Figure 66. Priority Setting



On this interface, you can move up/down the priorities for the groups.

9.7. Customizing DFM

DFM comes out of the box with the default settings ready to run. You can control and fine-tune these settings such as,

- Rediscovery Schedule
- Daily purge schedule
- SNMP Settings
- Trap Receiving
- Trap Forwarding
- Logging

Rediscovery Schedule

DFM discovers each device to determine the manageable components it contains. DFM can then assign appropriate polling and threshold parameters. In order to ensure DFM monitoring of a device is up to date, the device needs to be “re-discovered” on a periodic basis. The default is re-discover on a weekly basis. You can change this setting by going to DFM/Configuration/Other Configurations/ Rediscovery Schedule.

Daily Purging Schedule

A daily purging schedule needs to be setup for fault history information in the DFM. Traverse to DFM panel and click on **Configuration → Other Configuration → Daily Purging Schedule** to setup a purge schedule.

SNMP Settings

DFM gets the majority of its information used to determine a device's fault status using SNMP queries. Since SNMP is a UDP protocol, there is the opportunity for information to be "lost." To help alleviate this, servers can employs a series of timeouts and retries. DFM comes pre-configured to perform 3 retries using a timeout value of 4 seconds.

To change these variables, select **DFM → Device Management → SNMP Config** and make the changes.

SNMP Trap Receiving

This configuration is made for setting the global port for receiving traps in DFM. Traverse to DFM panel and click on **Configuration → Other Configuration → SNMP Trap Receiving** to set the port used for trap receiving.

SNMP Trap Forwarding

This configuration can be made to blindly forward traps that come into the trap receiver of the DFM. These are traps that are received from the devices in the network. Traverse to DFM panel and click on **Configuration → Other Configuration → SNMP Trap Forwarding** to setup trap forwarding.

Note: It is not north-bound trap generation for applications like HP Open View

Configure Logging

DFM writes application log files for all major functional modules. By default, DFM writes only error and fatal messages to these log files; DFM saves the previous three logs as backups. You cannot disable logging. However, you can:

- Collect more data when needed by increasing the logging level
- Return to the default logging level as the norm

Changing the logging setting by going to **DFM/Configurations/Other Configurations/Logging**.

10. Performance Management: Internetwork Performance Monitor

10.1. Business Scenarios

Managing mission-critical networks has become an integral component of today's businesses. Customers no longer see IP network as an unreliable infrastructure to build their business on. Internet service providers (ISPs) and even internal IT departments now have to offer a defined level of service—a service level agreement (SLA)—to provide their customers with a degree of predictability. How to measure network response time, determine device availability, resolve connectivity issues, analyze response time patterns and provide critical report, both real time and historical have taken on an even higher priority.

CiscoWorks Internetwork Performance Monitor (IPM) is a network management application that leverages the Cisco IOS IP SLA technology to monitor the end-to-end performance of multi-protocol networks. IPM measures performance from one end of the network to the other allows a broader reach and more accurate representation of the end-user experience. Using IP SLA, IPM measures and displays five key network performance statistics between a source and a target device. These five statistics include latency, availability, jitter, packet loss, and errors.

14) SLA was formerly known as RTR or SAA. For more information on Cisco IOS IP SLA, visit http://www.cisco.com/go/ipsla.

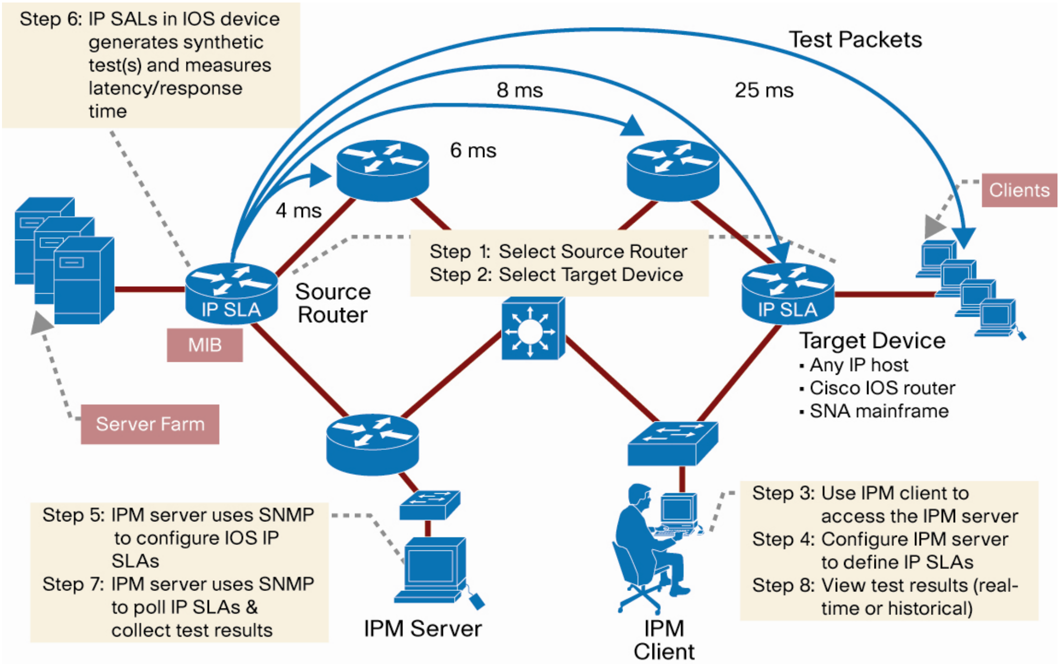
10.2. Workflow for IPM Application

To use IPM for performance management, users need to define collectors to gather the performance data. A collector is made of four components,

- **Source Router:** originating point from which IPM makes latency and availability measurements. This is where the IPM server uses SNMP to configure IOS IP SLAs. A source router must run Cisco IOS software with IP SLAs feature.
- **Target Router:** destination of source router operations (IP SLAs measurements) from which response data should be collected. A target can be an IP host, another IOS device with IP SLA, or an SNA host.
- **Test Operation:** the traffic test operations simulate actual network traffic for a specific protocol. For example, to measure the latency for a Voice over IP session, an Enhanced UDP test operation is created and defined to send a series of 60-byte UDP packets with a specified Type of Service (TOS) value and target port number.
- **Collection Schedule:** a collector can be scheduled to run at any point in time, or continuously over any time interval. This flexible scheduler makes IP SLAs suitable for both service-level monitoring and troubleshooting.

The workflow for IPM application is illustrated in the following figure:

Figure 67. IPM Workflow



As in this workflow diagram, we define the collector from step 1 to step 5. In the first and second step, source router and target device are defined. For IOS devices, we need to turn on IP SLAs in IOS.

In step 6, IP SLAs in the source router generates the synthetic tests and measure latency/response time. IPM server will then poll the collectors to collect test results and generate the results in real-time or historical reports.

The following sections will discuss each step in details.

10.3. Source Router and Target Device

The first thing for the user to do is to select the source router and target device. For example, to measure the response time between clients and an application server, the source router will be a Cisco IOS router running 11.2 or newer version on the same segment where the application server will be placed. The target device is placed on the same segment where many clients would access the application server.

The target device can be either of these,

- IP host – If the target is an IP host, it can be any IP-addressable device such as a network device, server, or workstation. Likely candidates for target devices are the actual servers providing application services, or devices such as routers that can provide protocol performance measurements for an intermediate network segment.
- SNA host – If the target is an SNA host (IBM MVS mainframe), it must run a Virtual Telecommunications Access Method (VTAM) program called NSPECHO, available in the IPM product, to measure SNA latency. Optionally, the SNA host can use an SCCP-LU Native Echo.

- Cisco IOS device with the IP SLA Responder enabled (12.0(3)T or later) – The Responder feature can improve the accuracy of the tests. The Responder can listen and respond to specified port number. Additionally, the Responder, based on the type of operation, might put timestamps on the return packets for accurate measurement times.

Configure the Source Router

Once the source of the test operation has been identified and the device has been selected, it will need to be configured.

First, check the IOS version of the source router. IOS release 11.2 is the earliest and first release that support the IP SLAs (formerly known as RTR or SAA).

Additionally, a few device configuration commands need to be set in order to configure IP SLAs using IPM and have IP SLA-related traps forwarded to a network management station (NMS). These commands are outlined in the figure above and discussed below.

- IPM uses SNMP to define the IOS IP SLA and to extract the data in the IP SLA MIB in the source router. Both the SNMP read-only (ro) and read-write (rw) community strings need to be configured on the source router.
- Optionally, to receive traps at a NMS when a test exceeds a specified latency threshold, verify that the source router is set up to send IP SLA-generated traps. The SNMP keyword rtr limits the traps sent to the specified address to IP SLA-related traps. If the keyword rtr is omitted, all default SNMP traps are sent to the named network management host including IP SLA-related traps.

Here is the configuration commands needed on the Source router:

```
router>enable
router#config t
router(config)#snmp-server community <string> ro
router(config)#snmp-server community <string> rw
router(config)#ip sla monitor
router(config)#snmp-server host <ip address> <trap community string> rtr
router(config)#snmp-server enable traps rtr --------------> still valid in 12.3
```

See more IP SLA commands at
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper0900aecd8022c2cc.shtml.

Configure the Target Device

Depending upon the type of target device selected, the target device may need to be configured.

- IP Host – The host must be reachable by the source device, but no other configuration is needed.
- SNA Host – It must run a VTAM program called NSPECHO, available in the IPM product, to measure SNA latency. Optionally, the SNA host can use an SCCP-LU Native Echo.
- Cisco IOS Device – The device must be reachable by the source device and the SNMP read community string must be configured.

- Cisco IOS Device with IP SLAs Responder – A target device that is running Cisco IOS software can be configured as a Responder, which processes measurement packets and provides detail timestamp information. The device must be reachable by the source device and the SNMP read community string must be configured. Additionally, the IP SLAs Responder feature must be enabled.

The responder has intimate knowledge of Cisco IOS software processing, so it can send information about the target router's processing delay back to the source IP SLA. This delay is removed during calculation to further improve accuracy.

Here is the list of commands on the target device if it is a Cisco router running IOS.

```
router>enable
router#config t
router(config)#snmp-server community <string> ro
router(config)#ip sla monitor responder
```

Device Management for Source Routes and Target Device

After the source and target routers are properly configured, they can be imported into IPM by three means,

- Automatic import from DCR
- Manually add the device one-by-one using IPM's configuration window
- Bulk import from a seed file such as a comma-separated value (CSV) file format.

Note: Auto sync with DCR is the most efficient and convenient way and has been discussed in Chapter 5.

When a new device is added to IPM, IPM first tries to access the device, and then verifies the SNMP community strings; and if successful and a Cisco device, IPM determines the device's IOS version and it's IP SLAs version, formerly known as SAA. If the information is valid, it adds the device to the IPM database.

For a device to be added to the list of source routers, the device must have valid SNMP read-only and readwrite community strings and a recent IOS version.

10.4. Define an Operation

IPM has a list of test operations built-in. You can also create your own test operations by going to IPM/Collector Management/Operation.

Here is a list of built-in test operations.

- Echo
- Path Echo
- UDP Echo
- ICMP Jitter
- UDP Jitter
- VoIP Post Dial Delay
- VoIP Gatekeeper Registration Delay
- RTP
- DNS
- DHCP
- HTTP
- FTP

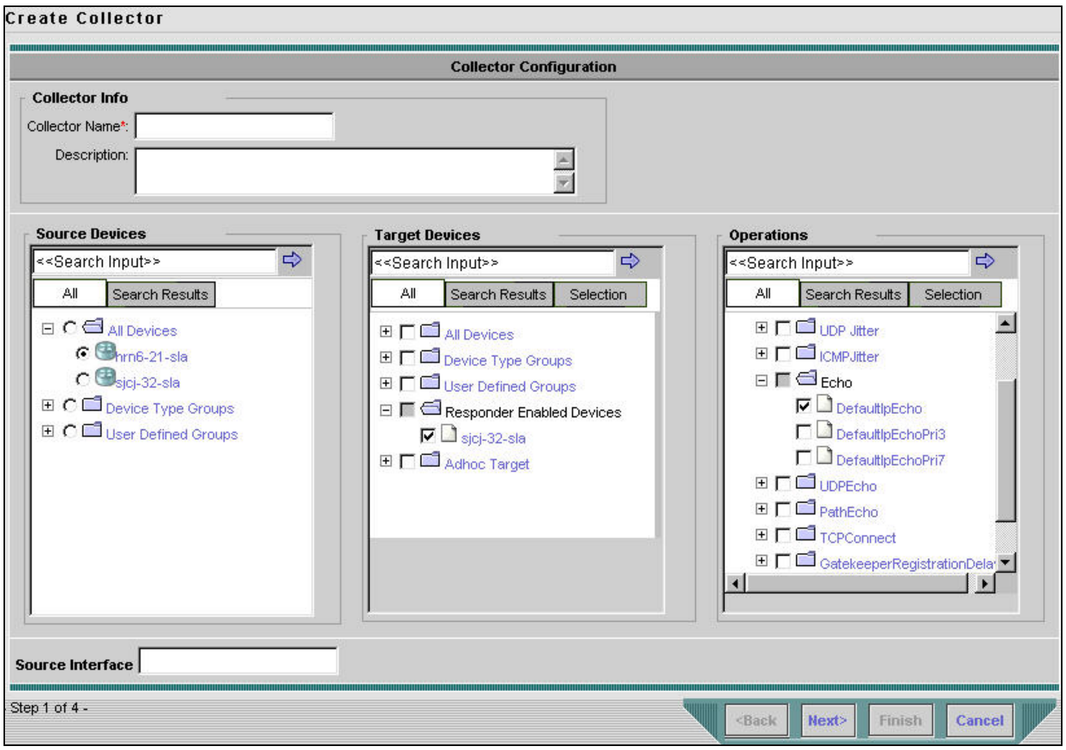
- DLSw
- TCP Connect

For definition of these test operations, please refer to http://www.cisco.com/en/US/products/ps6602/products_white_paper09186a00802d5efe.shtml.

10.5. Define a Collector

Finally we tie the four components of the Collector, that is, source and target devices, test operation and schedule by start creating a collector at IPM/Collector Management/Collector.

Figure 68. Create a Collector



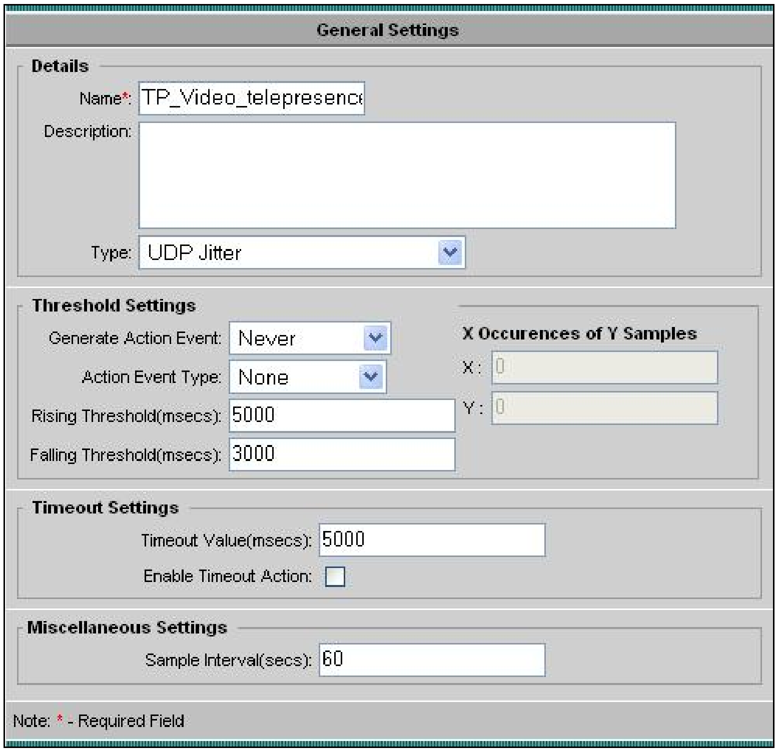
After the collector is created, we can monitor or generate reports based on the collector.

10.6. Sample Usage

Create a Report to Monitor the Video Jitter for Cisco TelePresence

Step 21. Define an operation “TP_Video_telepresence”. Choose type as “UDP jitter”.

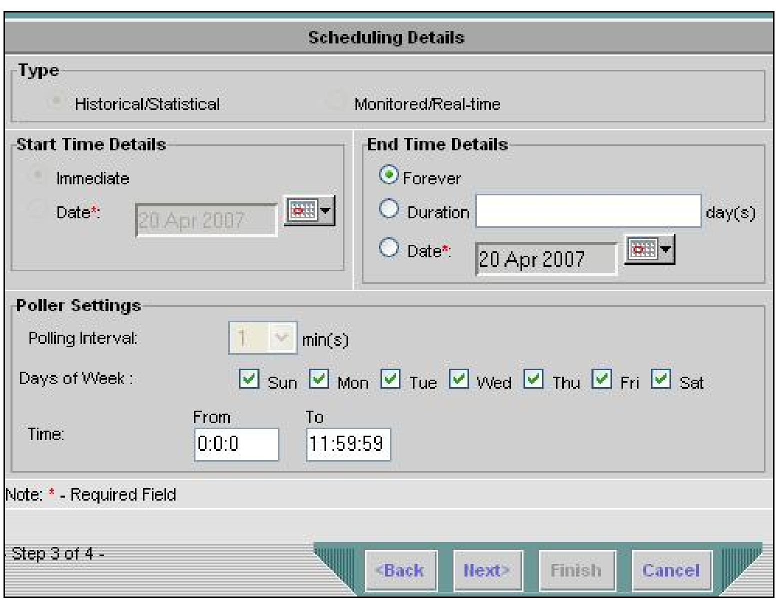
Figure 69. Define an Operation for TelePresence Video



Go to next screen, keep the default settings and finish the workflow for creating operation.

Step 22. Create a collector based on the operation just created. Set it to run forever, but ensure that it is deleted later.

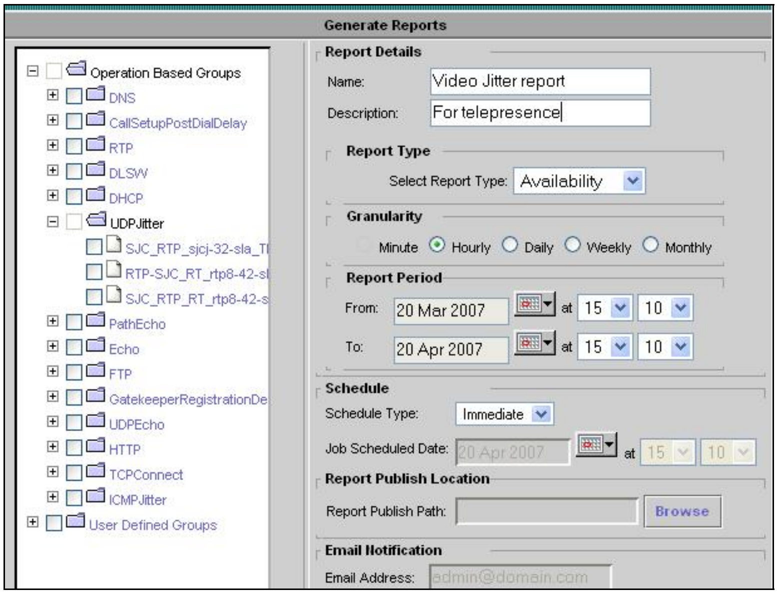
Figure 70. Schedule Setting



Step 23. Go to Collector Management to start the collector.

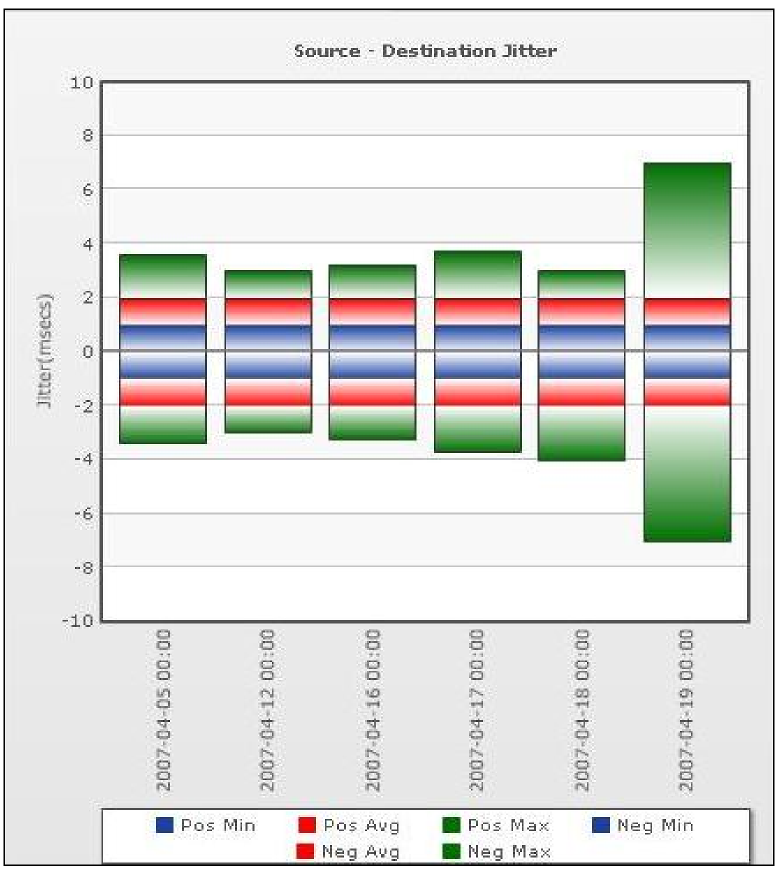
Step 24. After a few days of data collection, you can create a report under IPM/Reports.

Figure 71. IPM Report Generator



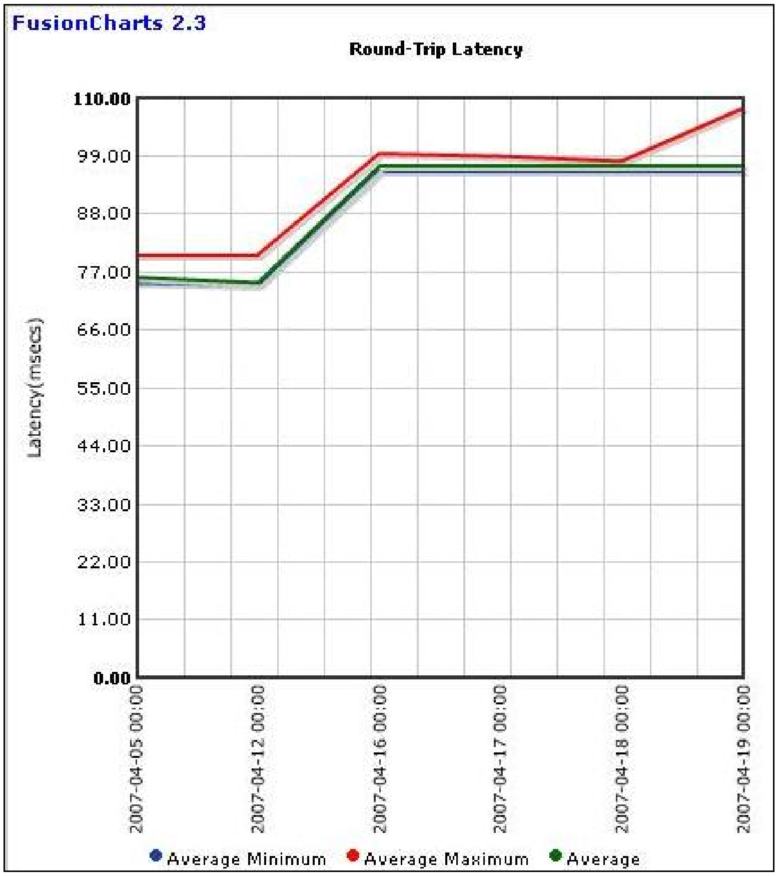
The jitter report will be illustrated in the figure:

Figure 72. Sample Report: Source-Destination Jitter



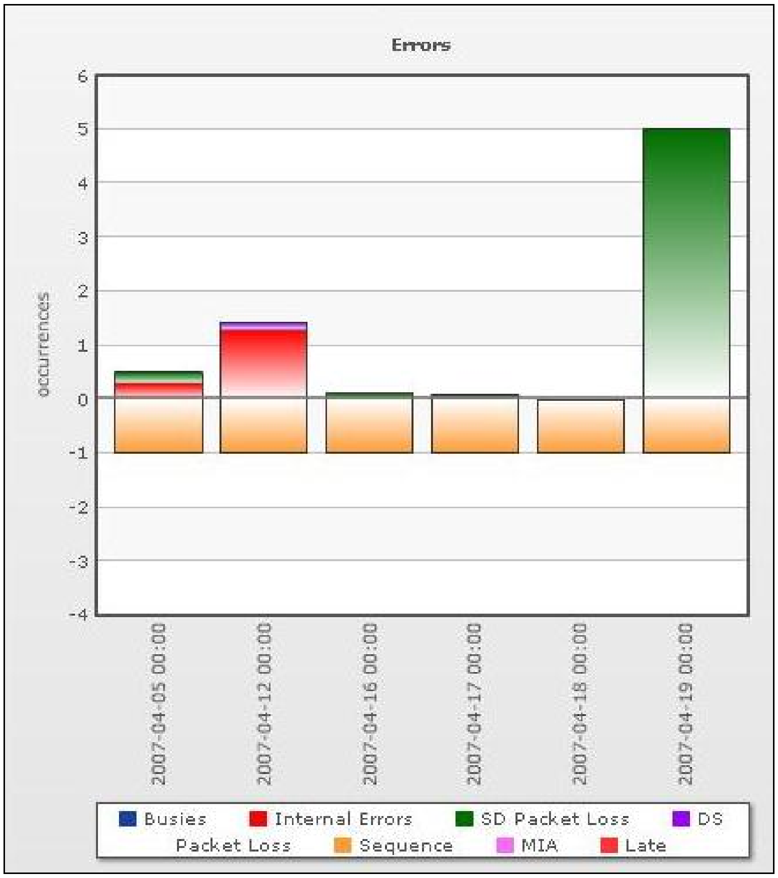
The latency report is illustrated below:

Figure 73. Round Trip Latency



The error report is illustrated below.

Figure 74. Errors Report



11. Server Administration

This section deals with server administration to optimally utilize the resources of the server while also maintaining a current status of the network topology.

11.1. Backup the Database

Backup of LMS data can be done via the GUI by traversing to **CWHP → Common Services → Server → Admin → Backup link, CWHP → LMS Setup Center → System settings**. A backup directory name can be provided and the backup job can either be run immediately or be scheduled. It is recommended that the backup data **not** be stored in a directory where the LMS is installed (that is, under the **NMSROOT** directory in Windows or Solaris).

The option **Generations** means the maximum number of versions of backups to be stored in the backup directory.

15) Enter multiple email addresses here by separating them with comma.

Note: Please note that the DCR Master/Slave mode is also backed up.

11.2. Restore the Database

Restoration of LMS data can be done only via CLI. You have to shut down and restart CiscoWorks while restoring data. Ensure that you do not run any critical tasks during data restoration—you may lose the data while performing such tasks.

The new restore framework supports restore across versions. This enables you to restore data from versions 2.1, 2.2, and 3.0, 3.0.5 in addition to Common Services 3.1. The restore framework checks the version of the archive.

- If the archive is of the current version, then the restore from current version is executed.
- If the backup archive is of an older version, the backup data is converted to Common Services 3.0.3 format, if needed, and applied to the machine.

Caution: Restoring the database from a backup permanently replaces your database with the backed-up version.

Restoring Data on UNIX

To restore the data on UNIX, log in as the superuser, and enter the root password. Stop all processes by entering:

```
/etc/init.d/dmgtd stop
```

Restore the database by entering:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl [-t temporary directory] [-
gen generationNumber] [-d backup directory] [-h]
```

[-t *temporary directory*]—The restore framework uses a temporary directory to extract the content of backup archive. By default the temporary directory is created under **NMSROOT as NMROOT/ tempBackupData**. You can customize this, by using the **-t** option, where you can specify your own temp directory. This is to avoid overloading **NMSROOT**.

[**-gen** *generationNumber*]—Optional. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest.

[**-d** *backup directory*]—Required. Which backup directory to use.

[-h]—Provides help. When used with **-d** <*backup directory*> syntax, shows correct syntax along with available suites and generations.

To restore the most recent version, enter:

```
/opt/CSCOpx/bin/perl /opt/CSCOpx/bin/restorebackup.pl -d backup directory
```

For example, `-d /var/backup`

Examine the log file in the following location to verify that the database was restored by entering:

```
/var/adm/CSCOpx/log/restorebackup.log
```

Restart the system:

```
/etc/init.d/dmgtd start
```

Restoring Data on Windows

To restore the data on Windows, make sure you have the correct permissions, and do the following:

Stop all processes by entering the following at the command line:

```
net stop crmdmgtd
```

Restore the database by entering:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl [-t temporary directory] [-gen
generationNumber] [-d backup directory] [-h]
```

where NMSROOT is the CiscoWorks installation directory. See the previous section for command option descriptions.

To restore the most recent version, enter the following command:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup directory
```

For example, `-d drive:\var\backup\`

When you restore the backup taken from a CS2.2 server, on a CS3.0 server, restore might fail if the backup archive has any file or folder with a long path name.

The following error message will be displayed:

```
ERROR: Restore cannot proceed. Seems you are hitting the bug CSCec01327
```

To workaround this problem, you have to install the patch cmf2.2-win-CSCec013271.tar on the CS2.2 server, before taking the backup.

The patch is available at http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-cd-one.

`Note:` You need not install this patch if you have installed Common Services2.2 Service Pack 3 on the CS2.2 server, before taking the backup.

Examine the log file in the following location to verify that the database was restored by entering:

```
NMSROOT\log\restorebackup.log
```

Restart the system by entering:

```
net start crmdmgtd
```

While restoring using a backup taken from a machine that is in ACS mode, the machine on which data is restored needs to be added as a client in ACS. Contact ACS administrator to add the restored machine as ACS client.

Data Restored from Common Services 3.0/3.0.3/3.0.5/CS 3.1 Backup Archive

The following data will be restored from a Common Services 3.0/3.0.3/CS 3.0.5/CS3.1 backup archive:

- CiscoWorks User information
- Single Sign-on configuration
- Device and Credential Repository (DCR) configuration
- Peer certificates
- Self Signed certificate (based on your confirmation)
- Peer Server Account information
- Login Module settings
- Software Center map files (Will not overwrite existing data)
- Application and Link registrations
- Log backup configuration
- License data (Will not be restored. But will compare and display a warning and ask for confirmation to continue, if licenses are different)
- ACS credentials
- System Identity Account configuration
- Cisco.com User configuration
- Proxy User configuration
- Database. Jobs data, DCR data, Groups data, and other data stored in the database

Data Restored from Common Services 2.2 Backup Archive

The following data will be restored from Common Services 2.2 backup archive:

- CiscoWorks user information
- Self Signed certificate (based on your confirmation)
- Login Module settings
- Management Connection data
- Log backup configuration
- Database. Jobs data, and other data stored in database

Though Common Services 2.2 supports ACS login module, restoring from a Common Services 2.2 backup archive will not restore the ACS login module. After restore, the login module of the machine will be non-ACS, TACACS+.

Data Restored from CD One 5th Edition Backup Archive

The following data will be restored from CiscoWorks2000 Server (CD One 5th edition) backup archive:

- CiscoWorks user information
- Self Signed certificate (based on your confirmation)
- Login Module settings
- Log backup configuration
- Database. Jobs data, and other data stored in the database

11.3. Reset the LMS Databases

In case you need to reset the LMS databases to factory default, follow this procedure, (Windows version, Solaris is similar)

```
cd CSCOpx\campus\bin
        perl reinitdb.pl –ut (User Tracking info only, LMS must be up)
        perl reinitdb.pl (Devices only, LMS must be up)
net stop crmdmgtd
        perl reinitdb.pl –restore (deletes all data, and reloads the tables)


cd CSCOpx/bin directory
        perl dbRestoreOrig.pl dsn=ani dmprefix=ANI    CM
        perl dbRestoreOrig.pl dsn=cmf dmprefix=Cmf    CS
        perl dbRestoreOrig.pl dsn=rmeng dmprefix=RME  RME

        perl dbRestoreOrig.pl dsn=dfmEpm dmprefix=EPM DFM Alerts
        perl dbRestoreOrig.pl dsn=dfmInv dmprefix=INV DFM inventory
        perl dbRestoreOrig.pl dsn=dfmFh dmprefix=FH   DFM Fault History
        del c:\progra~1\CSCOpx\objects\smarts\local\repos\icf\dfm.rps
net start crmdmgtd
```

11.4. Data Extraction from LMS Applications

This section covers the basic utilities available for data extraction from LMS applications. For complete information on this topic, search for the latest LMS user guides at Cisco.com.

11.4.1. DCR CLI

Using Command Line Interface, you can add, delete, view, modify devices and change DCR modes. You can import from local NMS, remote NMS or ACS server. You can also export the DCR content to a file or an ACS server.

The main command to launch is at

```
NMSROOT/bin/dcrcli.
```

The steps are:

Step 25. NMSROOT/bin/dcrcli –u username

Step 26. Enter the password corresponding to the username.

Step 27. Select one of the various top level commands

```
add – Adds a device
```

```
del – Deletes a device
mod – Modifies a device
lsattr – Lists the attributes stored in DCR
details – View Device details
lsmode – Lists the DCR mode as Master, Slave or Standalone
setmaster, setstand, setslave – Sets the DCR to Master, Standalone or Slave mode
impFile, impNms, impRNms, impACS – Imports device list from File, Local NMS, Remote
NMS and ACS ( AAA server ).
exp – Export to a file
expAcs – Export to an ACS server.
```

11.4.2. Campus Manager Data Extraction Engine

Campus Manager provides a data extraction engine to extract data about the following

- User Tracking Data
- Layer 2 Topology
- Discrepancies in the network configuration

Data Extraction can be done either through CLI or Servlet access.

The CLI tool **cmexport** can be accessed by going to NMSROOT/campus/bin directory.

The top level help provides the following output.

“

Usage: **cmexport <-h | -v | commands> <arguments>**

For command-specific help: cmexport <commands> -h

- h prints this help message
- v prints DEE version

commands can be one of the following:

```
ut            extracts user tracking data
l2topology    extracts layer 2 topology data
discrepancy   extracts discrepancy data
"
→ Core Commands
```

Table 11. Core Commands of Campus Manager DEE

Core Command	Description
ut	Generates User Tracking data in XML format.
l2topology	Generates layer 2 topology data in XML format
discrepancy	Generates discrepancy data in XML format

You must invoke the **cmexport** command with one of the core commands specified in the above table. If no core command is specified, **cmexport** can execute the **-v** or **-h** options only:

Option **-v** displays the version of the **cmexport** utility and

Option **-h** (or null option) lists the usage information of this utility.

Data generated through **cmexport** CLI is archived at the following locations by default.

For User Tracking:

```
PX_DATADIR/cmexport/ut/timestamput.xml
```

For Layer 2 Topology:

```
PX_DATADIR/cmexport/L2Topology/timestampL2Topology.xml
```

For Discrepancy:

```
PX_DATADIR/cmexport/Discrepancy/timestampDiscrepancy.xml
```

where

```
PX_DATADIR is %NMSROOT%\files folder (on Windows) or /var/adm/CSCOpx/files
directory (on Solaris).
```

NMSROOT is the directory where you installed Campus Manager; timestamp is the time at which the log was written in YearMonthDateHourOfDayMinuteSecond format.

You can also use the–f option to specify the file name and the directory for storing the DEE output. This utility does not inherently delete the files created in the archive. You should delete these files when necessary. However, using the same file name and directory twice would cause the previous file to be overwritten.

→ `Possible Combinations of cmexport commands`

User Tracking:

- **view** parameter specifies the format in which the user tracking XML data to be presented. It supports currently 2 options
  - *switch:* user tracking data is displayed based on the switch
  - *subnet*: user tracking data is displayed based on subnet in which they are present
- **query**: user tracking host data is exported in XML format for the query given in *queryname*. This parameter is applicable only when –host is chosen
- **layout**: user tracking host data is exported in XML format for the layout given in *layoutname*. The layout is a custom layout defined by the user in UT. This parameter is applicable only when –host is chosen
- **queryPhone**: user tracking phone data is exported in XML format for the query given in *phonequeryname*. This parameter is applicable only when –phone is chosen.
- **layoutPhone**: user tracking phone data is exported in XML format for the layout given in *layoutPhone*. This parameter is applicable only when –phone is chosen.

```
cmexport ut –u admin –p admin –host
cmexport ut –u admin –p admin –phone
cmexport ut –u admin –p admin –host  -query  dupMAC –layout all
cmexport ut –u admin –p admin –host  -query  dupMAC –layout <name>
cmexport ut –u admin –p admin –phone  -queryPhone  <name> –layoutPhone <name>
cmexport ut –u admin –p admin –host   -f  ut.xml
cmexport ut –u admin –view  switch –host
```

L2Topology or Discrepancy Commands:

```
cmexport L2Topology|Discrepancy –u admin –p admin
cmexport L2Topology|Discrepancy –u admin –p admin -f  013104L2.xml
```


The Servlet access to CM Data Extraction Engine is described below.

The Servlet accepts users request and authenticates the requesting user's identity using Common Services authentication mechanism. The command to export user tracking, topology, and discrepancy can be sent as HTTP or HTTPS requests. The Servlet requires a payload file that contains details about User's credentials, the command you want to execute and optional details such as log and debug options as inputs in XML format. The Servlet then parses the payload file encoded in XML, performs the operations, and returns the results in XML format. Typically, Servlet access is used to extract the data from a client system. While generating data through the Servlet, the output will be displayed at the client terminal.

The input XML file contains various tags for username, password, core command, and optional tags. The following outlines the steps to extract the export file from the Servlet.

1. Generate the necessary payload XML file with the required data.
2. Use a script to perform a POST operation to the Servlet with the payload file. The Servlet is http://Campus-Server:1741/CSCOnm/campus/servlet/CMExportServlet.
3. The HTTP response of the Servlet contains the XML file generated by executing the cmexport command on the server with the parameters provided in the payload file.
4. Extract the XML file from the content of the HTTP response and save it to a local file.

Sample Payload:

```
<payload>
<!—The following element specifies the username (valid CiscoWorks or ACS user ID)
of the person initiating this DEE call -->
<username>username</username>
<!— The following element specifies the valid password of the user ID -->
<password>password</password>
<!—The following element specifies the DEE command used for extracting UT host,
phone, discrepancy and l2 topology information -->
<command>ut_host</command>
<!—The following element specifies the logfile where all logs need to be output -->
<logfile>filename</logfile>
<!—The following element specifies the debug level at which the log is output. -->
<debug>1</debug>
<!—The following element specifies the custom report name created in the User
Tracking UI by traversing to CWHP → Campus Manager → User Tracking → Reports → Custom
Reports →
<view></view>
</payload>
```

Sample Perl Script to Access the Servlet:

```
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$| = 1;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
if ( -f $fname ) {
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{
$str .= $_ ;
```

```
}
close(FILE);
}
url_call($temp);

#-- Activate a CGI:
sub url_call {
my ($url) = @_;
my $ua = new LWP::UserAgent;
$ua->timeout(5000);
my $hdr = new HTTP::Headers ‘Content-Type’ => ‘text/html’;
my $req = new HTTP::Request (‘GET’, $url, $hdr);
$req->content($str);
my $res = $ua->request($req);
my $result;
if ($res->is_error)
       {
print “ERROR : “, $res->code, “ : “, $res->message, “\n”;
$result = “;
       }
else
       {
$result = $res->content;
if($result =~ /Authorization error/)
           {
print “Authorization error\n”;
           }
else
           {
print $result ;
           }


       }
}
```

Note: Sample scripts are available in the Campus Manager DEE online help.

The above Perl script will invoke the servlet with the use of payload xml file. The command will look similar to what is mentioned below.

In HTTP mode:

```
./perl script.pl http://server:1741/campus/servlet/CMExportServlet payload.xml
```

In HTTPS mode:

```
./perl script.pl https://server/campus/servlet/CMExportServlet  payload.xml
```

Any user using the data extraction engine is authenticated and authorized. The username and password are either provided as part of the CLI and Servlet call or the password is put in a password file for retrieval by Data extraction engine. The access permissions to the file can be set to prevent any unauthorized access. When using this option, the CMEXPORTFILE environment variable should be set so it points to the file containing the credentials and the command should be entered in the following format:

```
cmexport ut –u admin –host
```

The above syntax enables **cmexport** to find the relevant password associated with the username (in the above case, for the username admin).

11.4.3. RME Data Extraction Engine

Resource Manager Essentials provides a data extraction engine to extract data about the following

- Inventory
- Change Audit
- Config details of the device

Data extraction can be done by either through CLI or Servlet access.

The CLI tool **cwcli** can be accessed by going to NMSROOT/bin directory.

The top level help command "cwcli –help" provides the following output

"

`CiscoWorks command line.`

General syntax to run a command with arguments is `cwcli <application/command> <arguments>`

```
For detailed help on a command and it's arguments, run cwcli <application/command>
-help
 "
```

```
→ Core commands of "cwcli export" command
```

Table 12. Core Commands of RME DEE

Core Command	Description
inventory	CLI tool to create, delete and cancel a inventory collection job. It also helps in importing or exporting the data in inventory as XML files.
config	Provides a set of commands that are used to download and fetch configurations, compare two different configurations, delete the archived configuration files and reload the device.
export	Exports Inventory/Config/Change Audit data in XML
netconfig	CLI tool to create, delete and cancel a NetConfig job. It also helps in importing or exporting the User Defined Template XML files.
invreport	List all custom reports and generates CSV formatted inventory report(s) for given template(s).

You must invoke the **cwcli** command with one of the core commands specified in the above table. If no core command is specified, **cwcli** can execute the -v or -help options only:

Option **-v** displays the version of the **cwcli** utility and

Option **-help** (or null option) lists the usage information of this utility

The command line syntax of the application is in the following format:

cwcli export command GlobalArguments AppSpecificArguments

- cwcli export is the CiscoWorks command line interface for exporting inventory/config/changeaudit details into XML format.
- *Command* specifies which core operation is to be performed.
- *GlobalArguments* are the additional parameters required for each core command.
- *AppSpecificArguments* are the optional parameters, which modify the behavior of the specific **cwcli export** core command.

The order of the arguments and options are not important. However, you must enter the core command immediately after **cwcli export**.

On UNIX, you can view the **cwcli export** man pages by setting the MANPATH to /opt/CSCOpx/man/man1. The man pages to launch the **cwcli export** are man cwcli-export to launch the **cwcli export** command.

- man export-changeaudit to launch the **cwcli export changeaudit** command.
- man export-config to launch the **cwcli export config** command.
- man export-inventory to launch the **cwcli export inventory** command.

→ `Data Archiving Location`

Data generated through **cwcli export** CLI is archived at the following locations by default.

a. ChangeAudit

On Solaris: /var/adm/CSCOpx/files/rme/archive/YYYY-MM-DD-HH-MM-SS-changeaudit.xml

On Windows: NMSROOT\files\rme\archive\ YYYY-MM-DD-HH-MM-SS-changeaudit.xml

b. Config

On Solaris: /var/adm/CSCOpx/files/rme/cwconfig/YYYY-MM-DD-HH-MM-SS-MSMSMS-Device_Display_Name.xml

On Windows: NMSROOT\files\rme\cwconfig\ YYYY-MM-DD-HH-MM-SS- MSMSMS-Device_Display_Name.xml

c. Inventory

On Solaris: /var/adm/CSCOpx/files/rme/archive/YYYY-MM-DD-HH-MM-SS-inventory.xml

On Windows: NMSROOT\files\rme\archive\ YYYY-MM-DD-HH-MM-SS- inventory.xml

The details of Servlet access to RME Data Extraction Engine is given below.

The name of the Servlet is /rme/cwcli. The following is the Servlet to be invoked to execute any command:

For post request,

```
http://<rme-server>:<rme-port>/rme/cwcli <payload XML file>
```

For get request,

```
http://<rme-server>:<rme-port>/rme/cwcli?command=cwcli config <commandname>-u
<user> -p <BAse64 encoded pwd> -args1 <arg1value>...
```

Note: Use <arg> and <argval> tags when the argument is a file.

The contents of the payload xml file are as follows.

```
<payload>
<command>
cwcli config export -u admin -p <Base64Encoded pwd> -device 1.1.1.1 -xml
</command>
<arg>
</arg>
<arg-val>
</arg-val>
</payload>
```

For example to execute the import command payload.xml is as follows:

```
<payload>
<command>
cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106
<arg>
•  f
</arg>
<arg-val>
banner motd “welcome,Sir”
</arg-val>
</command>
</payload>
```

The Remote Access Servlet creates a temporary file with the contents specified between the arg-val tags for the import command. On the server the command is executed as “cwcli config import -u admin -p <Base64Encoded pwd> -device 10.77.240.106 -f tempfile”. Here the tempfile contains the line banner motd “welcome,Sir”.

For example:

```
perl samplescript.pl http(s)://<rme-server>:<rme-port>/rme/cwcli <payload XML file>
```

Note: For the secure mode (HTTPS) the port number is 443. The default port for CiscoWorks server in HTTP mode is 1741.

Sample Script to Invoke the Servlet

```
#!/opt/CSCOpx/bin/perl
use LWP::UserAgent;
$temp = $ARGV[0] ;
$fname = $ARGV[1] ;
open (FILE,"$fname") || die "File open Failed $!";
while ( <FILE> )
{       $str .= $_ ;
}
print $str ;
url_call($temp);
#-- Activate a CGI:
sub url_call
{
my ($url) = @_;
my $ua = new LWP::UserAgent;
$ua->timeout(1000);
# you can set timeout value depending on number of devices
my $hdr = new HTTP::Headers 'Content-Type' => 'text/html';
my $req = new HTTP::Request ('POST', $url, $hdr);
$req->content($str);
my $res = $ua->request ($req);
my $result;

if ($res->is_error)
{
print "ERROR : ", $res->code, " : ", $res->message, "\n";        $result = ";

}

else {
    $result = $res->content;
       if($result =~ /Authorization error/)
{           print "Authorization error\n";
          }

else {
print $result ;
         }

     }
}
```


11.4.4. IPM Export

There has been no change in the way the data can be exported in IPM from the previous version of the product. The **ipm export** cli is the command to do IPM export.

The following example shows the command syntax and help that is displayed when you use the **ipm export help** command:

Note: You must be logged in as the root user (Solaris) or administrator (Windows) to use export IPM data using the **ipm export** command.

Usage:

```
ipm export
   [-q] [[-k <letter>] | -w] [-h]
   [ ( -c | -s | -t | -o | -cs) [<CollectorName>] ]
  | [ (-dh | -dd | -dw | -dm)  <StartTime> <EndTime> [ <CollectorName> ] ]
  | [ (-jh | -jd | -jw | -jm)  <StartTime> <EndTime> [ <CollectorName> ] ]
  | [ (-ph | -pd | -pw | -pm)  <StartTime> <EndTime> [ <CollectorName> ] ]
  | [ -r [<WhichDay>] ]
  | [ -all [<StartDate>] [<EndDate>]]
```

General options:

```
ipmRoot] - Root location of IPM, such as /opt/CSCOipm

-q  Quiet output- display no column headings. Only applicable in plain text output
format

-k  Delimiter- set the field delimiter to <letter>.  By default, this
is set to a comma ‘,’. Only applicable in plain text output format.

-w  HTML output - A web page will be generated from the output of this command.

-h  Help - output this usage help
```

Format:

```
Time  - <StartTime> and <EndTime> need to be input as MM/DD/YYYY-hh:mm:ss
Date - <WhichDay> needs to be input as: MM/DD/YYYY
<StartDate> and <EndDate> need to be input as: MM/DD/YYYY
```

Appendix: List of Acronyms

Acronym	Meaning
AAA	Authentication, Authorization and Accounting
ACS	Access Control Server, a AAA server software from Cisco Systems, Inc.
CDP	Cisco Discovery Protocol. It is a Cisco proprietary protocol for discovering neighboring devices.
Certificate Setup	This feature allows the creation of self-signed security certificates, which can be used to enable SSL connections between the client browser and management server.
CWHP	CiscoWorks Home Page. A web page that a CiscoWorks user accesses after logging into a CiscoWorks Server.
DCR	DCR (Device and Credential Repository) is a common repository of devices, their attributes, and the credentials required to manage devices in a management domain. DCR will enable the sharing of device information among various network management applications.
ELMI	Enhanced Local Management Interface. It is a protocol used in Metro Ethernet.
FR	Frame Relay
ILMI	Integrated Local Management Interface. It is an ATM standard
IOS	Internetwork Operating System. It is an operating system that runs Cisco routers and switches.
LMS	LAN Management Solution
MISTP	Multiple Instances Spanning Tree Protocol. It is a Cisco proprietary Standard.
MST	Multiple Spanning Tree Protocol. It is a IEEE standard derived from MISTP.
NDG	Network Device Group. A term used in ACS to group devices.
NMIM	Network Management Integration Module
NMS	Network Management System
Peer Server Account Setup	This feature helps you create users who can programmatically login to CiscoWorks servers and perform certain tasks. These users should be set up to enable communication between multiple CiscoWorks servers.
Peer Server Certificate Setup	This feature allows you to add the certificate of another CiscoWorks server into a trusted store. This will allow one CiscoWorks server to talk to another, using SSL.
PVST	Per-VLAN Spanning Tree Protocol
RCP	Remote Copy Protocol
IP SLA	Cisco IOS® IP Service Level Agreement (SLA), a network performance measurement feature in Cisco IOS Software, provides a scalable, cost-effective solution for service level monitoring. It eliminates the deployment of dedicated monitoring devices by including the “operation” capabilities in the routers.
SCP	Secure Copy Protocol
Single Sign-On	A feature by which a single browser session is used to transparently navigate to multiple CiscoWorks servers without having to authenticate to each server.
SNMP	Simple Network Management Protocol
SSH	Secure Shell Protocol
SSL	Secure Socket Layer. It is an encryption protocol.
SSO	Single Sign On—The ability to login into multiple computers or servers with a single action and the entry of a single password. Especially useful where, for example, a user on a LAN or WAN requires access to a number of different servers.
STP	Spanning Tree Protocol. A protocol to avoid loops in a switched network.
System Identity Setup	Communication between multiple CiscoWorks servers is enabled by a trust model addressed by Certificates and shared secrets. System Identity setup should be used to create a “trust” user on slave / regular servers for communication to happen in multi-server scenarios.
TACACS+	Terminal Access Controller Access Control System Plus. It is an authentication protocol.
TLS	Transport Layer Security.
VLAN	Virtual Local Area Network
VTP	VLAN Trunk Protocol. A protocol used in a trunk link of two switches to maintain VLAN information in a switched network.

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.**

Printed in USA

C07-408046-02 07/10