

# CiscoWorks LAN Management Solution Deployment Guide

## 1. Device Setup

This section describes the minimum configuration tasks that should be performed on Cisco IOS® and Cisco Catalyst® devices before attempting to manage them using CiscoWorks. It should be noted that this is by no means an exhaustive configuration guide. Depending on the functionality required, further device configuration may be required. For comprehensive information, see “Performance and Fault Management” from Cisco Press as well as Cisco.com.

### 1.1. Network and Device Requirements Introduction

For CiscoWorks Campus Manager tools to function correctly, network services must first discover the devices in the network. The devices must be properly configured to complete the network discovery. To identify and discover devices and end stations on the network, the following requirements must be met:

- Devices must support the Cisco Discovery Protocol or Integrated Local Management Interface (ILMI) to be discovered, and the supported protocol (Cisco Discovery Protocol or ILMI) must be enabled on each interface that should be discovered. ILMI is required for ATM devices only.
- Enhanced LMI (ELMI) is also supported when dealing with a Cisco® WAN switching frame cloud.

- Simple Network Management Protocol (SNMP) read and write community strings must be configured on each device.
- To properly discover and identify all Cisco IOS Software-based devices on the network, the sysName variable must be unique on each Cisco IOS device. If two or more devices have the same sysName variable, it discovers only the first device.

The following additional requirements must also be met for specific features of the CiscoWorks Campus Manager application to work properly:

- Call detail records (CDRs) logging should be enabled on all Cisco CallManagers. CDR is a reporting option that logs IP address, phone number, and time of calls for Cisco IP phones. This information is needed to perform path analysis for any routes that involve Cisco CallManager devices.

### 1.2. Cisco IOS Devices

This section describes the steps that should be taken to set up Cisco IOS devices for network management. Note that not all steps may be required, and some steps can be expanded with more functionality. Do not forget to save the configuration to nonvolatile random-access memory (NVRAM) after performing these steps by using one of the two following commands:

write memory

or

copy running-config startup-config



### 1.2.1. Community Strings

CiscoWorks Resource Manager Essentials (RME) uses SNMP to retrieve and write information (configuration files, software images, etc.) to the devices. Therefore, all SNMP community strings must match on the devices and in the Essentials inventory.

To configure SNMP community strings on a Cisco IOS device, use the following global configuration commands:

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

### 1.2.2. System Reload

Some configuration and software management changes require reloading of a device before the changes will take effect. The device must be configured to allow an SNMP manager (in this case the CiscoWorks RME server) to reset the agent. This feature is available only for Cisco IOS devices.

To allow the Essentials server to reload a device, use the following global configuration command:

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

### 1.2.3. Syslog Message Logging

All devices must be configured to send syslog messages to the CiscoWorks RME server or a remote Syslog Analyzer Collector (SAC) in order to use the Syslog Analysis feature.

To configure message logging on a Cisco IOS device, use the following global configuration commands:

```
logging on
logging <server-ip-address>
logging trap <logging-level>
```

### 1.2.4. Remote Copy Protocol

The remote copy protocol (rcp) is one of the few protocols that can be used by configuration management and software management to transfer configuration files and software images between devices and the CiscoWorks RME server. To allow the Essentials server to read and write files to a device using rcp, this feature must be enabled on the device. The rcp feature is available only for Cisco IOS devices.

To enable rcp on a device, use the following global configuration commands:

```
ip rcmd rcp-enable
ip rcmd <remote-host> <remote-username> <server-ip-address> <local-username> enable
```

The server-ip-address parameter is the IP address or host name of the Essentials server.

Note: The remote-username and local-username parameters must match the value defined in the CiscoWorks RME server under Administration > System Configuration > RCP. The default value in Essentials is cwuser.

### 1.2.5. Command-Line Prompts

In order to use the NetConfig function to execute batch configuration commands on devices, all command-line prompts must meet certain requirements:

- The login prompt must end with angle bracket (>).
- The enable prompt must end with pound sign (#).



Examples:

- England\_router>
- England\_router#

If you have customized any prompts, they must meet these requirements.

### 1.2.6. Cisco Discovery Protocol

Cisco Discovery Protocol is a Cisco proprietary protocol that is used by devices to advertise their existence to other devices on the network. Each device that has Cisco Discovery Protocol enabled maintains a table of its neighbors. Network services uses Cisco Discovery Protocol to gather information on each device and its neighbors, in order to form a view of the network topology. If Cisco Discovery Protocol is not enabled on a device, network services will not be able to discover its neighbors and build a topology of the network. Cisco Discovery Protocol is enabled by default, so you need to enable it only if it has been disabled. You might also want to disable Cisco Discovery Protocol on devices that are on the borders of your management domain. That way, additional devices beyond those boundaries that you are not responsible for will not be discovered and displayed in CiscoWorks Campus Manager.

To enable Cisco Discovery Protocol on a Cisco IOS device, use the following commands:

```
cdp run (to enable on all interfaces)
cdp enable (to enable on specific interfaces only)
```

Use the **no** form of the Cisco IOS command to disable Cisco Discovery Protocol on a device or interface. For example:  
**no cdp enable.**

Tip: Where Not to Run Cisco Discovery Protocol

Do not run Cisco Discovery Protocol on links that you do not want discovered, such as Internet connections.

Note: Do not enable Cisco Discovery Protocol on links that do not go to Cisco devices. This protects you from Cisco Discovery Protocol denial-of-service (DoS) attacks.

### 1.2.7. SysName Variable

The system name must be unique on every Cisco IOS device for network services to discover all Cisco IOS devices on the network. Network services uses this variable to identify each device via Cisco Discovery Protocol. If this value is duplicated on any devices, network services discovers only one of the devices. On Cisco IOS Software, the domain name also affects the sysName.

To set the sysName variable on a Cisco IOS device, use the following global configuration command:

```
hostname <name>
```

### 1.2.8. Source Routing

Source routing is a function within IP that allows the source host to specify the route a packet should take through the network. If this option is specified in the IP header, then the packet is forwarded according to the path specified. This option must be enabled on Cisco IOS devices for the path-analysis function to be able to trace accurate paths from a source device to a destination. Source routing is enabled by default on Cisco IOS devices, so you need to enable it *only* if it has been disabled.



Verify that source routing has not been disabled by checking the device configuration for the following entry:

```
no ip source-route (this indicates source routing is currently disabled)
```

If source routing has been disabled on a device, use the following command to enable it:

```
ip source-route
```

Note: `ip source-route` can be a security hole. Allow it only if you are fully aware of all the security implications.

### 1.3. Cisco Catalyst Devices

This section describes the steps that should be taken to set up Cisco Catalyst devices for network management. Note that not all steps may be required, and some steps can be expanded with more functionality.

#### 1.3.1. Community Strings

Several important items must be configured correctly on every Cisco device that is going to be managed and monitored through CiscoWorks RME. Essentials uses SNMP to retrieve and write information (configuration files, software images, etc.) to the devices. Therefore, all SNMP community strings must match on the devices and in the Essentials inventory.

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

These commands ensure that the device can be identified and that inventory can be carried out.

#### 1.3.2. Syslog Message Logging

All devices must be configured to send syslog messages to the CiscoWorks RME server or a remote SAC in order to use the Syslog Analysis feature.

To configure message logging on a Cisco Catalyst device, use the following commands:

```
set logging server enable
set logging server <server-ip-address>
set logging level all <logging-level> default or
```

The `server-ip-address` parameter can be the address of the Essentials server or a remote SAC that has been configured to forward syslog messages to the Essentials server.

Note: Some of the Cisco Catalyst logging commands are found only on later releases of the Cisco Catalyst Operating System (CatOS).

#### 1.3.3. Telnet

Telnet must be enabled on Cisco IOS devices. This means that the VTY login has to be configured using the following commands:

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

This example references the minimal configuration. For better access control and logging facilities, consider using TACACS authentication and authorization.



#### 1.3.4. Command-Line Prompts

In order to use the NetConfig function to execute batch configuration commands on devices, all command-line prompts must meet certain requirements:

- The enable prompt must end with (enable).

Example:

- England\_cat(enable)

If you have customized any prompts, they must meet these requirements.

#### 1.3.5. Cisco Discovery Protocol

Cisco Discovery Protocol is a Cisco proprietary protocol that is used by devices to advertise their existence to other devices on the network. Each device that has Cisco Discovery Protocol enabled maintains a table of its neighbors. Network services uses Cisco Discovery Protocol to gather information on each device and its neighbors, in order to form a view of the network topology. If Cisco Discovery Protocol is not enabled on a device, network services is not able to discover its neighbors and build a topology of the network. Cisco Discovery Protocol is enabled by default, so you need to enable it only if it has been disabled. You might also want to disable Cisco Discovery Protocol on devices that are on the borders of your management domain. That way, additional devices beyond those boundaries that you are not responsible for will not be discovered and displayed in CiscoWorks Campus Manager.

To enable Cisco Discovery Protocol on a Cisco Catalyst device, use the following command:

```
set cdp enable <all | module/port>
```

Tip: All Parameter

Use the “all” parameter to enable Cisco Discovery Protocol on all ports on the device, or enter specific module and port numbers. A range of ports can also be entered. For example:

```
set cdp enable 2/1-10,3/5-10
```

To disable Cisco Discovery Protocol on a Cisco Catalyst device, use the set cdp disable command.

Tip: Where Not to Run Cisco Discovery Protocol

Do not run Cisco Discovery Protocol on links that you do not want discovered, such as Internet connections.

Note: Do not enable Cisco Discovery Protocol on links that do not go to Cisco devices. This protects you from Cisco Discovery Protocol DoS attacks.

#### 1.3.6. VLAN Trunk Protocol

Note: This protocol should be enabled and configured as part of the overall network design. This section is included for reference purposes only.

VLAN Trunk Protocol (VTP) is used to configure and communicate VLAN settings across multiple switches. VTP must be configured on all switches in order to manage VLANs via CiscoWorks Campus Manager. A VTP domain must be established and the VTP mode must be defined on each device. In addition, at least one switch in each VTP domain must be defined as a VTP server in order for Campus to create VLANs in that domain. Discovering VLANs established on a switch using VTP transparent mode is supported from CiscoWorks Campus Manager



Version 3.1. The old restriction of requiring at least one server in a VTP domain to identify virtual LANs (VLANs) has been removed. Then Campus can be used to view, create, modify, and delete VLANs via the topology services application instead of the command line.

To set a VTP domain and mode on a Cisco Catalyst switch, use the following commands:

```
set vtp domain <name>
set vtp mode <client | server | transparent>
set vtp v2 <enable | disable> (required for Token Ring networks)
```

Description of modes:

- *Server*—The switch maintains and communicates VLAN settings to all other switches in the VTP domain.
- *Client*—The switch synchronizes VLAN configuration with advertisements received from VTP servers, and forwards advertisements to neighbors.
- *Transparent*—The switch does not participate in VLANs advertised by the server, but forwards advertisements to neighbors. Any VLANs configured on a transparent switch are local to that switch only.

Note: Remember that each switch can be in only one VTP domain.

Note: VTP Version 2 must be used on Token Ring networks. VTP Versions 1 and 2 are not compatible, and they cannot both be run in the same domain.

The campus best-practice recommendations emphasize campus stability and predictability (especially for protocols such as Spanning-Tree Protocol [STP]). General suggestions for enterprises that prefer a cautious approach may include making use of VTP transparent or VTP off (CatOS 7.0) instead of the typical VTP server and client model. The major VTP benefit of uniform VLAN creation across multiple switches may be out-weighted by the drawbacks of the same thing it is supposed to simplify, which is the automatic extension of VLANs of all switches in a domain. Hence the risk of unnecessary unenforced STP and its issues across multiple switches. Spanning tree is not bad—it is the defaults that are bad.

Another major risk of the VTP client and server is the possibility that the new server versioning could override the existing VTP server and delete VLANs unknown to the new master server from all switches within that domain. Though some of these risks can be reduced by VTP authentication, trunk clearing, and VTP pruning, the added complexity of these functions is not really worth it.

CiscoWorks Campus Topology can still discover and depict VLANs on switches that make use of VTP transparent mode; see [http://www.cisco.com/en/US/products/sw/cscowork/ps563/products\\_user\\_guide\\_chapter09186a00800c9e72.html#35719](http://www.cisco.com/en/US/products/sw/cscowork/ps563/products_user_guide_chapter09186a00800c9e72.html#35719).

More details of this would go way beyond the scope of this document, but the following link—Best Practices for Cisco Catalyst 4000, 5000, and 6000 Series Switch Configuration and Management—[http://www.cisco.com/en/US/products/hw/switches/ps663/products\\_tech\\_note09186a0080094713.shtml](http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml)—can be referenced for quite a few campus switching best-practice suggestions, including more technical coverage on spanning tree, further Cisco Discovery Protocol details, channels, Point Aggregation Protocol (PAGP), trunks, trunk clearing, pruning, syslog levels, and unidirectional link detection (UDLD).



### 1.3.7. Trunking

Note: This protocol should be enabled and configured as part of the overall network design. This section is included for reference purposes only.

Trunking is a method of carrying traffic for multiple VLANs over the same link, between two switches or a switch and a router, thus extending the VLANs across the network. In order to perform trunking, ports on each side of the link must be set to trunk ports, and the Inter-Switch Link (ISL) or IEEE 802.1Q protocol must be enabled. ISL is a Cisco proprietary protocol used to combine traffic from multiple VLANs over one link. IEEE 802.1Q is the industry-standard protocol for performing the same function. IEEE 802.1Q must be used on Token Ring networks.

To enable trunking on a Cisco Catalyst Switch port, use the following command:

```
set trunk <module/port> on [vlans]
```

This command establishes the specified module or port as a trunk port and enables the ISL protocol.

You can use the optional “vlans” parameter to specify a specific range of VLANs to be allowed across the trunk. For example: set trunk 2/1 on 2-10 (valid ranges are from 1 to 1005).

## 2. Preinstallation Tasks

The following tasks should be carried out or reviewed before installing CiscoWorks.

### 2.1. Verify Locale Settings

CiscoWorks currently supports only the U.S. English and Japanese locales. Using other locales means that you are running on a nonsupported configuration. Further, CiscoWorks may display erratic behavior, such as JRunProxyServer services not starting automatically. Non-U.S. English keyboard layouts should work, though.

### 2.2. Verify DNS Settings

Make sure the CiscoWorks server has correct Domain Name System (DNS) settings. Verify connectivity to DNS, as well as forward and reverse lookup. CiscoWorks uses DNS for numerous operations, and waiting for DNS timeout will make it appear slow.

### 2.3. Check Browser Version

The recommended browser is Microsoft Internet Explorer 6.0 (JVM 5.0.0.3805). There are some issues with IE 6.0 Service Pack 1, so be sure to check them. Also, IE 5.5SP2 (JVM 5.0.0.3802) is supported in CiscoWorks Common Management Foundation (CMF) 2.1 and CiscoWorks RMEv3.4. Make sure the Microsoft VM (Java Virtual Machine) is installed.

CiscoWorks uses JRE Version 1.3.1 only.

Note: Java Plug-in 1.3.1 is the only supported version (that is, not versions 1.3.1\_01, 1.3.1\_02, 1.3.1\_03, 1.3.1\_04, 1.3.1\_05, or 1.4).

### 2.4. Register Devices and Interfaces in DNS

For the name lookup process to work, devices should be registered in DNS.



When the discovery process encounters a device, it performs a reverse lookup on the IP address where the device was encountered in order to get the host name for the device. CiscoWorks then performs a forward lookup on the host name to get the preferred management interface for the device. Hence, all interfaces should be registered in reverse DNS, but only the preferred management interface should be registered in the forward lookup. The loopback0 interface is an ideal candidate for this, because it is never down.

Also note that CiscoWorks Campus Manager from Version 3.3 onward lets you select the preferred management interface from the graphical user interface (GUI) after discovery has been performed.

## **2.5. Check Routing and Firewalls**

Make sure that any firewalls between the CiscoWorks server and the managed devices are configured to let management traffic through. Refer to Appendix C for information on which ports should be opened.

Also, make sure that there is connectivity between devices to be managed and the CiscoWorks server. Even if a route exists to a network behind a managed device, that does not mean that one exists to (and from) the device itself.

**Note:** Because of Common Object Request Broker Architecture (CORBA) limitations, any firewall between client and server needs to be not performing Network Address Translation (NAT) and it needs to allow all TCP ports > 1023. This effectively negates the usefulness of a firewall. NAT is not necessarily an issue for client connectivity. If NAT has been performed on the server, then you have problems.

**Note:** This CORBA limitation comes into play only for CiscoWorks Campus Manager, CiscoWorks ACL Manager, and Cisco Internetwork Performance Monitor (IPM). In other words, if you are just using CiscoWorks RME, you will not have this limitation.

## **2.6. Network Address Translation**

Normally, network management and NAT is not a very good combination. However, the following tips can help in managing networks that perform NAT:

- Create a management VLAN on each site on which NAT has been performed.
- Add all switched and router loopback interfaces to the VLAN.
- Set a trap source for SNMP and syslog to be the loopback interface.

As long as the IP addresses for the switches and loopback interfaces are unique throughout the network, the management process can use these IP addresses, even if the IP addresses for the networks on which NAT has been performed themselves are not unique. To make CiscoWorks discover the preferred management interface, see Section 2.4.

## **2.7. Check Device Configurations for “Odd” Letters**

CiscoWorks supports only the 7-bit ASCII character set. This means that device configurations that contain other letters such as Æ, Ø, and Å can cause problems. For example, configurations that contain these letters can cause the discovery process to hang, and thus never finish, or the device synchronization process can fail. Check the contact and location information, interface descriptions, host names, etc. for these letters before running discovery.





## 2.8. Network Time Protocol

To be able to correlate events across multiple devices, the devices need to have the same perception of the time. To achieve this, configure the Network Time Protocol (NTP) on the devices. For information on how to configure this functionality, refer to the Cisco device configuration documentation or <http://www.cisco.com/en/US/support/index.html>.

## 2.9. Server Sizing

Tables 1 through 4 give the recommended configurations for server sizing. These are approximate figures, and may not be applicable to every environment, even if the numbers of devices match. Also notice that the greater the number of modules (that is, CiscoWorks ACL Manager, Cisco IPM, etc.), the higher the requirements. Similarly, the number of simultaneous users will affect these requirements.

These figures assume that Asynchronous Network Interface (ANI) and CiscoWorks RME are installed. Windows disk sizing is for the Windows NTFS File System.

Table 1 Small-Scale Network (<200 devices)—System Recommendations

OS	CPU	RAM	SWAP	Disk
Windows	P3-1GHz SP	512 MB	1 GB	6 GB
Solaris	SunFire 280R 750MHz SP	512 MB	1 GB	36 GB

Table 2 Medium-Scale Network (200-500 devices)—System Recommendations

OS	CPU	RAM	SWAP	Disk
Windows	P3-1GHz SP	1 GB	1.5 GB	9 GB
Solaris	SunFire 280R 750MHz SP	1 GB	1.5 GB	36 GB

Table 3 Large-Scale Network (500-1000 devices)—System Recommendations

OS	CPU	RAM	SWAP	Disk
Windows	P3-1GHz MP	1.5 GB	2 GB	9 GB
Solaris	SunFire 280R 750MHz MP	1.5 GB	2 GB	36 GB

Table 4 Very Large-Scale Network (1000-2000 devices)—System Recommendations

OS	CPU	RAM	SWAP	Disk
Windows	P3-1.4GHz MP	2 GB	2.5-3 GB	15-20 GB
Solaris	SunFire 280R 900MHz MP	2 GB	2.5-3 GB	36 GB

The following parameters are assumed for the network:

- ANI discovery is configured.



- There are 1500 CiscoWorks Device Fault Manager (DFM) managed ports.
- One syslog message per second is received.
- Inventory information is collected weekly.
- Configurations are collected weekly.
- User Tracking keeps track of 20,000 end stations.
- HP OpenView daemons are running.

Variations in these parameters affect the performance of CiscoWorks, and the server should be sized accordingly. Also refer to the CiscoWorks documentation for information on client and server requirements.

In very large environments, the CiscoWorks applications may have to be spread on multiple servers. If this is the case, the following applications should be considered moved to separate servers:

- Real Time Monitor (recommended in any design)
- CiscoWorks Campus Manager
- CiscoWorks DFM and Voice Health Monitor

Note: CiscoWorks Campus Manager and Voice Health Monitor cannot reside on the same server.

Consult with your local Cisco office for the proper design before deploying CiscoWorks in very large-scale environments.

### 3. Setting Up CiscoWorks Security

After installing CiscoWorks, the first thing that you should do is to configure the security settings of the product.

#### 3.1. Select Login Module

First, you should verify that you are using the correct login module for CiscoWorks. You can do this by selecting the Server Configuration -> Setup -> Security -> Select Login Module menu item. Then you should be presented with a screen that shows which login module is being used, and gives you the option to select an alternative login module. Select the login module you want and click on the Next button to continue. The full procedure for modifying these settings is not described in this document.

Note: The login module is used only for authentication. This means that the user must be created in both the external and the internal (CiscoWorks) user databases, because this is checked for authorization.

#### 3.2. Modify Admin Password and Cisco.com Account

The default password for the CiscoWorks admin user is "admin." This should be changed as soon as possible by logging in as the admin user and then selecting the Server Configuration -> Setup -> Security -> Modify My Profile menu item. At the very least, the password should be changed. Add the Cisco.com and proxy information as needed. Next, click on the Modify button to confirm the changes.

#### 3.3. Add Users

Add further users into CiscoWorks as they are needed. Consider creating one user per operator for logging purposes. The menu item for this is Server Configuration -> Setup -> Security -> Add Users. Enter the information required. Make sure the proper roles are selected and click the Add button to confirm.



#### Tip: Permissions

For information on which operations can be carried out by which roles, select the Server Configuration -> Setup -> Security -> Permissions Report menu item.

Note: Never give a user Developer or Data Export privileges. Things will break. For example, users with these privileges might not show up in the Approvers list.

### 3.4. Schedule Backup

Schedule backup enables you to schedule automatic database backups. Backups can be scheduled on a daily, weekly, or monthly basis. In order to conserve disk space, select how many backup versions or generations should be retained (default is 0 or one retained version). Configure this by selecting Server Configuration -> Administration -> Database Management -> Schedule Backup.

Specify where you want the database dump to be stored, and the number of generations you want.

#### Tip: Where to Store

You should store the backups on a disk that is backed up to tape on a regular basis.

Note: Restore enables you to restore your database by running a script from the command line, not the desktop. The procedures for restoring your database are located in the online help.

Note: You cannot restore Windows NT data to a different drive than they were backed up from (that is, restoring D: data to C:). This is documented in bug ID (CSCds74983).

### 3.5. Create Self-Signed Certificates

CiscoWorks allows you to create self-signed security certificates, which can be used to enable Secure Sockets Layer (SSL) connections between your client browser and management server. This can be done using the Server Configuration -> Administration -> Security Management -> Create Self Signed Certificates menu option.

Note: Self-signed certificates are valid for one year 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 server.

Enter the values required for the fields described in Table 5.

Table 5 Information to be provided

Field	Description	Usage notes
Country name	Name of your country	Use the two-character country code (US = USA, UK = United Kingdom, NO = Norway, etc.).
State or province	Name of state or province	Use the two-character state or province code or the complete name of the state or province.
Locality	Name of your city or town	Use the two-character city or town code or the complete name of the city or town.
Organization name	Name of your organization	Use the complete name of your organization or an abbreviation.



Table 5 Information to be provided

Field	Description	Usage notes
Organization unit name	Name of your department in your organization	Use the complete name of your department or an abbreviation.
Host name	Name of the CiscoWorks server	Use the DNS name of the computer or the IP address of the computer. <b>Note:</b> Enter the HostName with a proper domain name. This is displayed on your certificate (whether self-signed or issued by third party)
E-mail address	Your e-mail address	

Either:

- Click Submit after entering the required values to create certificate.

or

- Click Restore to Default to clear all fields and reenter information.

The CiscoWorks server creates the security certificate. The process generates the files given in Table 6.

Table 6 Files Generated by Creating a Security Certificate

Filename	Description
<i>server.key</i>	Private key of the server
<i>server.crt</i>	Self- signed certificate of the server
<i>server.pk8</i>	Private key of the server in PKCS#8 format
<i>server.csr</i>	Certificate Signing Request (CSR) file; you can use this file to request a security certificate if you want to use third party-issued security certificates

### 3.6. Enable or Disable SSL

Select Server Configuration > Administration > Security Management > Enable/Disable SSL from the left pane of the window. The Configure SSL window appears in the right pane.

If SSL is enabled, CiscoWorks displays the Disable button. This will use CiscoWorks in the secure mode with Secure Hypertext Transfer Protocol (HTTPS),

If SSL is disabled, CiscoWorks displays the Enable button (refer to Table 7). This will use CiscoWorks in unsecure mode with Hypertext Transfer Protocol (HTTP).

Click the Enable button to enable SSL.



Note: If you have the required security certificates available on the server, CiscoWorks enables SSL. If you do not have the security certificates on the server, CiscoWorks prompts you to create your own self-signed certificate (as described in Section 3.5)

To complete the task of enabling SSL:

1. Log out from your CiscoWorks session and close all browser sessions.
2. Restart the daemon manager from the CiscoWorks server command-line interface (CLI):

On Windows 2000 enter:

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

On Solaris enter

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

3. Restart the browser and CiscoWorks session.

This can also be done on the command line using the following syntax:

On Solaris:

```
/opt/CSCOpX/objects/web/bin/ConfigSSL.pl -enable
/opt/CSCOpX/objects/web/bin/ConfigSSL.pl -disable
```

On Windows:

```
<INSTALLDIR>\bin\perl.exe <INSTALLDIR>\lib\web\ConfigSSL.pl -enable
<INSTALLDIR>\bin\perl.exe <INSTALLDIR>\lib\web\ConfigSSL.pl -disable
```

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with HTTPS instead of HTTP to indicate a secure connection.
- The port number succeeding the server name should be changed from 1741 to 1742.

Note: The port numbers mentioned previously are applicable for a CiscoWorks server running on Windows 2000. On Solaris, if the default port (1741) is used by another application, you can select a different port during CiscoWorks server installation.

Note: CiscoWorks Campus Manager and CiscoWorks DFM will not work on servers where SSL is enabled. This is mentioned in the release notes.

#### 4. Automatic Package Download

This section describes how to set up CiscoWorks to download new CiscoView packages as they become available. Furthermore, this section describes the procedure required to install these packages after download.

##### 4.1. Configure Cisco.com Account

The Automatic Package Updater requires Cisco.com access to work. This means that CiscoWorks must be configured with a Cisco.com account to use when downloading new and updated packages. This is configured using the Device Manager -> Administration -> Package Support Updater -> CCO Connection menu item. When this menu item is



selected, CiscoWorks should display a configuration page. At the very least you need to specify the Cisco.com login and password to use. If a proxy server is in use, configure the proxy parameters as well. Click on the Apply button to confirm the configuration.

#### **4.2. Schedule Package Downloads**

Next, configure the frequency with which CiscoWorks checks for new packages. This is done by using the Device Manager -> Administration -> Package Support Updater -> Schedule Downloads menu item. Here you select how often CiscoWorks should check for updates, what kind of packages to look for, etc., and then download the packages that meet the criteria selected. Configure this section as required. The configuration should be changed to reflect the customer's requirements. After the settings are configured press the Apply button to finalize the configuration.

#### **4.3. Import Downloaded Packages**

This point is not a one-time event that is performed right after installation. Rather, it is a recurring operation that is performed regularly. As the scheduled package download retrieves new and updated CiscoView packages, these need to be installed into CiscoView. This is done by selecting the Device Manager -> Administration -> Package Support Updater -> Staging Area Contents menu item. CiscoWorks displays a list of downloaded items. Check the items you want installed and click the Install button to continue the installation. Next, CiscoWorks displays a list of packages to be installed, and asks if you really want to install these packages. Click Yes to finalize the installation of these packages.

**Note:** If no integration with third-party network management tools such as HP OpenView has been performed, the installation of nmldb will fail, causing the whole package installation to fail. Thus, you need to deselect the nmldb item checkbox before attempting to install the packages.

After a little while you should get a message saying that the installation of the selected packages has finished, and that CiscoWorks is restarting the server.

### **5. Network Discovery**

One of the first tasks that should be carried out is discovering the network. This requires installation of the CiscoWorks Campus Manager component. Furthermore, CiscoWorks RME should also be installed to reap the full benefits of the procedures described within. This section describes a set of configuration tasks that should be performed.

#### **5.1. Device and Credential Synchronization**

The discovery process can send devices and device information to CiscoWorks RME when devices are discovered. To configure this functionality, select Server Configuration -> Setup -> ANI Server Admin -> Device Synchronization.

Add the host name of the server where CiscoWorks RME is installed. This is normally the same server on which CiscoWorks Campus Manager is installed.

**Note:** The host name or IP address of the CiscoWorks RME server should be used. Do not use localhost or 127.0.0.1, because these can confuse CiscoWorks in some cases.

The Port field contains the port number used to connect to CiscoWorks RME. This is normally the same port used to access the CiscoWorks GUI, that is, port 1741.



Next enter the admin user ID and password in the respective fields.

Tick each checkbox in the “Synchronize to Essentials” section, as well as “Synchronize from Essentials.” Because CiscoWorks by default runs a discovery every four hours, this ensures that new devices are added to CiscoWorks RME automatically, as well as sending information to CiscoWorks Campus Manager if something is changed from CiscoWorks RME. Click on the Apply button to save the configuration.

**Note:** Remember that a device that is imported from the CiscoWorks Campus Manager discovery is not managed in CiscoWorks RME until the device attributes are provided by the user. Refer to Section 6.4.3

**Note:** Only devices that are green in the topology map are synchronized to CiscoWorks RME. In other words, the device must be managed and must be reachable in CiscoWorks Campus Manager in order to be synchronized.

## 5.2. SNMP Settings

Use this section to configure the SNMP community strings that CiscoWorks Campus Manager is to use during the discovery process. These settings are configured under the Server Configuration -> Setup -> ANI Server Admin -> SNMP Settings menu item.

Add subnets or ranges with corresponding community strings as required.

**Tip:** Wildcards

You can use \* (asterisk) to indicate whole subnets such as 192.168.10.\* as well as ? (question mark) to indicate individual numbers, such as 1?, which will match any number from 10 to 19. You can also use ranges such as 192.168.10.[10-20], as long as they are enclosed in square brackets. Note that you can use \*.\*.\* to represent all networks. Note that multiple instances of \*.\*.\* can be specified, but the Multiple wildcards checkbox must be checked for this to take effect. You have to restart the ANI server after this checkbox has been selected.

**Note:** Multiple instances of \*.\*.\* are supported only in CiscoWorks Campus Manager 3.3. Do not try this in CiscoWorks Campus Manager 3.2.

When the settings are configured correctly, click the Save button to verify.

## 5.3. Discovery Schedule

This setting is used to change how often CiscoWorks should perform a network discovery to look for new and updated devices. By default this is done every 4 hours starting at midnight. Depending on the network topology and customer requirements, these settings may need to be changed. Furthermore, CiscoWorks checks device status every 5 minutes by default in CiscoWorks Campus Manager versions up to 3.2, and every 120 minutes by default in Campus Manager 3.3 onward. These settings can be changed by selecting the Server Configuration -> Setup -> ANI Server Admin -> Discovery Schedule menu item. Click the Apply button to store the changes made.

## 5.4. User and Host Acquisition

This setting changes how often CiscoWorks should poll edge switches to look for connected end-station devices such as PCs and printers. To change it, select the Server Configuration -> Setup -> ANI Server Admin -> User and Host Acquisition menu item.



The Major Acquisition setting determines how often CiscoWorks should scan edge switches for information, whereas the Minor Acquisition setting is used to select how often CiscoWorks should try to confirm that the device is still there.

To get the user ID when a user logs on, the UT.BAT file needs to be installed into the login script. Check the documentation for more information on this.

Click on the Apply button to save the changes made.

Note: To get UNIX usernames, rwhod must be running.

## 5.5. Discovery Settings

These settings must be changed for the discovery process to run. These settings are found under the Server Configuration -> Setup -> ANI Server Admin -> Discovery Settings menu item. At the very least one device must be added, and more than one device can be added. If more seed devices are required than there are lines for, additional lines can be added by right-clicking on the list and selecting Insert.

CiscoWorks topology discovery works by querying seed devices for information regarding the devices themselves. Next the discovery process queries the devices for Cisco Discovery Protocol neighbor tables to find neighboring devices. The process is then repeated for these devices. Thus, it is vital that SNMP and Cisco Discovery Protocol have been configured on the devices. Note that Cisco Discovery Protocol is a Layer 2 protocol, and as such is blocked by firewalls.

Cisco Discovery Protocol is also blocked by Layer 3 devices. This means that the discovery process stops when it reaches a router. However, this can be circumvented by selecting the Jump Router Boundaries checkbox. This causes CiscoWorks to check each interface on the router for Cisco Discovery Protocol neighbors, thus continuing the discovery process.

By default CiscoWorks tries to do a reverse lookup to find the hostname when it encounters a device. If you do not want this to happen, turn off the Use reverse DNS Lookup checkbox.

It is possible to filter which IP addresses or VTP domains CiscoWorks should or should not discover. This is done by adding them to the filter criteria at the bottom of the screen.

When all settings have been configured, click the Apply button to save them. CiscoWorks asks if you want the discovery process to start immediately. Click Yes or No to select the option you want.

### Tip: Monitoring the Discovery

You can monitor the progress of the discovery process by selecting the Server Configuration -> Diagnostics -> Discovery Metrics menu item. Click on the menu item again to update the information. When the discovery is done, click on the item listing the total number of devices discovered to see if there were any devices discovered that CiscoWorks was unable to manage for any reason.





## 5.6. Topology Group Administration

CiscoWorks Campus Manager can be used to display topology maps of your network. A recent feature addition is the ability to create topology groups, or containers. These are logical groupings of devices based on arbitrary hierarchical structures, such as geographical regions. For example, devices can be organized by country, within each country by state, within each state by city, etc. After the discovery has been performed, this can be configured using the Campus Manager -> Administration -> Topology Groups menu item.

## 5.7. Configure Path Analysis and User Tracking Scheduling

To configure scheduled jobs for path analysis and user tracking, select the Campus Manager -> Administration -> Job Schedule menu item.

### 5.7.1. Path Analysis

Included with CiscoWorks Campus Manager is a tool called Path Analysis, which can determine the Layer 2 and 3 path between a pair of devices (or end stations) in your network. To create a scheduled job to test a path between two devices on a regular basis, select the Campus Manager -> Administration -> Job Schedule menu item.

Next, click on the New Job button and enter the required parameters. The “No. of Archives” field specifies the number of versions of the result of this scan that you want to store for historical reasons.

### 5.7.2. User Tracking

CiscoWorks Campus Manager includes a utility called User Tracking. This tool keeps track of end-user equipment (PCs, printers, etc.), and where this equipment is connected to the network; that is, which switchport has which equipment connected to it. This information is updated regularly (as specified in Section 5.4). To store the User Tracking data to an external file on a regular basis for historical analysis, you need to schedule an export of this data. This is done using the menu item specified previously.

After selecting the menu item, click on the New Job button to create a new schedule. The “No. of Export Archives” field specifies the number of versions of the information that you want to store for historical reasons.

You should create a custom query and a custom layout in the User Tracking application before using this tool, because it requires the name of a predefined query and a predefined layout.

## 6. Setting Up CiscoWorks Resource Manager Essentials

This section describes how to set up CiscoWorks RME. This part of CiscoWorks is used for configuration management, software image management, and more. All the menu items for configuring CiscoWorks RME are found under the Resource Manager Essentials -> Administration folder.

Note that not every configuration setting is covered, because not all settings are required to make CiscoWorks manage the discovered network.

CiscoWorks can be configured to use the Secure Shell Protocol (SSH) instead of Telnet when talking to devices. However, note that the SSH implementation encrypts SSH packets that should not be encrypted. This can lead to unexpected results when using SSH, especially when the SSH session is closed. There is no workaround other than to not use SSH. However, a patch is available by calling the Cisco Technical Assistance Center (TAC), and referencing bug ID CSCdz03633.



Note: In CiscoWorks RME 3.4, SSH is supported only for configuration management. That is, CiscoWorks RME Software Image Manager (SWIM), for example, does not support SSH, nor does Check Device Attributes. Check bug IDs CSCdz20060 and CSCdz44557 for more information.

## 6.1. System Configuration

This menu item, found under Resource Manager Essentials -> Administration -> System Configuration, is used to change proxy, SNMP, Simple Mail Transfer Protocol (SMTP), and rcp settings. Change these settings as required, and click on the Apply button to save the new settings.

## 6.2. Job Approval

Both software-management and configuration-management tasks allow you to set up approval checkpoints before a job can be run that will change a configuration or update the software image on a device. This can help increase the security on your network by forcing these types of high-impact jobs to be “approved” before they can be executed. Additionally, other CiscoWorks applications can also take advantage of this feature (for example, CiscoWorks ACL Manager).

To set up job approval, you must first create an approver list, a list of CiscoWorks user accounts that must approve the job before it can be run. This is done by assigning one or more users the approver role when the users are created. Users must have the role of approver to even be considered for an approver list. After you have created at least one approver list, you can enable the job-approval feature for software management, configuration management, or both.

*To set up job approval, follow the steps in the next Sections 6.2.1 and 6.2.2.*

Note: The user must have the user role of system administrator or network administrator to perform this task.

### 6.2.1. Create an Approver List

Select Administration -> Job Approval -> Create Approver List from the Resource Manager Essentials drawer.

You must create at least one approver list before you can enable job approval. Only users who have been assigned the approver role will display in the list of valid user accounts for approval.

### 6.2.2. Enable Job Approval

Select the Resource Manager Essentials -> Administration -> Job Approval -> Edit Preferences menu item to enable job approval. You can select configuration-management or software-management jobs.

For software management, you can also be specific as to the types of jobs that require approval (new image distribution, undo image distribution, retry image distribution).

## 6.3. Inventory

Population of the inventory within the Essentials database must be completed before CiscoWorks RME can be used to manage your network. Devices can be neither monitored nor manipulated until they have been added to the inventory. Devices can be added to the inventory in four ways; the first three are directly associated with CiscoWorks RME tasks:

- Add each device manually.
- Import devices from a text file.



- Import devices from another network management system (local or remote).
- Synchronize with the Campus database (requires CiscoWorks Campus Manager 3.0, included with the CiscoWorks LAN Management Solution [LMS] bundle). The process for setting this up is described in Section 4.5.

For each request to enter a device into the inventory (by any of the methods described), the CiscoWorks Inventory Manager initiates an inventory data collection from the device via SNMP. If the device can be accessed and its Management Information Base (MIB) is recognized by Inventory Manager, data is uploaded from the device and placed in the Managed Devices table in the inventory along with the device and any device attributes received from the enter process. If the device does not respond to the SNMP query or the device type is not supported by the Inventory Manager function, it is placed in the Unmanaged Device table. Because the device is considered unmanaged by CiscoWorks RME, no further queries are directed toward it. The user can delete these devices or resubmit them for inclusion in the inventory.

CiscoWorks Inventory Manager cooperates with other CiscoWorks RME functions needed to perform an initial data collection (for example, CiscoWorks Configuration Manager), telling them that a new managed device exists.

If CiscoWorks Campus Manager has been installed, you can normally skip to Section 6.3.5.

**Note:** A device can be “managed” if it supports MIB-II. This means that CiscoWorks can gather basic inventory information, etc. MIB-II devices can be managed even if they are not Cisco devices.

**Note:** CiscoWorks RME “reads” deleted devices only when CiscoWorks Campus Manager finds them if the Campus Manager-to-CiscoWorks RME synchronization is enabled.

### 6.3.1. Manually Adding Devices

**Note:** This is normally not required when CiscoWorks Campus Manager has been installed.

Adding devices manually is a slow and time-consuming process, but it does allow the user to associate all possible device attributes with the device at inventory submission time. Adding devices to the inventory is an administration task, and hence it is found within the Resource Manager Essentials -> Administration -> Inventory -> Add Devices menu item. Selecting this menu item displays a set of three screens of attributes for a device. In the first screen you must enter (required) either the device IP address or host name in the first field. If you know the serial number under the maintenance contract for this device, you can enter it in the appropriate field. CiscoWorks Inventory Manager, however, attempts to populate this field when performing a MIB read of the device during inventory data collection.

#### Tip: User Fields

The four User fields are definable by the user. These fields can be useful in creating device views. Example uses of User fields include Device Location, Device Type (core, access, distribution), and so on. After a value has been defined in a field, a dropdown list with potential values is displayed next to the appropriate User field. In CiscoWorks RME 3.5, users have the flexibility to change the User Name column heading to suit their own needs.

The second screen of attributes requires at least the entering of the device read community string. All other fields in the second and third screens are optional; however, entering password information is required for other CiscoWorks RME functions.



When you have finished entering the device attributes, click the Finish button on the third screen. At this time CiscoWorks Inventory Manager attempts to contact the device and place it into the appropriate table in the inventory. Meanwhile, a message is displayed asking if you wish to add more devices or view the status of the inventory submission. Click the corresponding button, depending on whether or not you want to add more devices. If you select to add more devices, you will be taken to the first screen to add another device.

**Tip: Changing Information**

Attributes can be changed or added any time after the device is in the inventory by using the Change Device Attributes task.

The user can also check device attributes during the add or import process by selecting the Check Device Attributes box. Any attribute (attributes) errors seen at this time are reported on the Add/Import Status Summary screen in the Device Attribute Errors field.

**Note:** The import from a network management system (NMS) or CiscoWorks Campus Manager process imports only community strings. Password attributes must be added after import has occurred.

### 6.3.2. Importing Devices from a File

**Note:** This is normally not required when CiscoWorks Campus Manager is installed.

Importing devices from a file can be useful if you do not have a NMS to import from or you do not want to add all your devices manually. Like the manual add of devices to the inventory, the file-import process allows you to associate all device attributes with a device at import time. CiscoWorks Inventory Manager uses two different files to import data from a file: a CSV and a DIF file. Examples of these two files can be found at <Install Directory>/CSCOpX/example/import.

**Note:** When creating these files, it is important to note that a required line IS embedded among the comment lines (comments preceded by a semicolon). The line starts with “cisco Systems NM data import, ....” This line is required; do not delete it.

After creating your import file, import it by selecting the task: Resource Manager Essentials -> Administration -> Inventory -> Import From File. Enter the location and name of the file and click on the Next button. Before proceeding with the import of devices, CiscoWorks Inventory Manager asks you for the Reconciliation Criteria in case any device being imported already exists in the inventory. In other words, which data should Inventory Manager use if conflicts exist—the data currently in the database or the data being imported? It also gives you the option of deciding after the file is imported on a device-by-device bases. We will look at the Reconciliation Criteria screens after first looking at the import from NMSs.

After selecting the reconciliation criteria, the CiscoWorks Inventory Manager starts contacting all the devices in the Import file and placing them in the appropriate table within the inventory. Meanwhile, the Add/Import Status screen is displayed (this screen is discussed in more detail later). First we look at the NMS import process.

**Tip: Exporting Inventory Information to a Text File**



You can also export the inventory database to a CSV or DIF text file by selecting Resource Manager Essentials > Administration > Inventory > Export to File. This data is exported to a directory with administrator and root privileges only because it contains password information in plaintext. You can take advantage of this feature by exporting the inventory, making changes to the device attributes, and then importing the file back to the inventory.

### 6.3.3. Importing from Local or Remote NMS

Note: This is normally not required when CiscoWorks Campus Manager is installed.

If your network is large and you have a third-party NMS that has already discovered the network devices, it may be best to import the devices. Check with the release notes or the online help for importing from a NMS to determine compatibility between versions.

To import devices from a supported third-party NMS, do the following:

1. Select Administration -> Inventory -> Import from Local NMS or Remote NMS from the Resource Manager Essentials drawer.

2. If you are importing from another NMS, select the NMS from the network management product pull-down menu. Only the products that are supported on your server platform are displayed in the list.

Note: If the NMS is installed in a nondefault location, you should select the Customize checkbox and enter the correct path information.

3. Select the desired Reconciliation Criteria.
4. You can also import third-party devices as well as Cisco devices by deselecting the Cisco devices only option. Remember, CiscoWorks RME is not optimized to read third-party device MIBs. Third-party device support within Essentials is extremely limited (MIB-II information mainly for use with CiscoWorks Availability Manager and lists of devices within CiscoWorks Inventory Manager).
5. After you have entered all the appropriate information, click Finish and the Add/Import Status Summary will appear.

### 6.3.4. Importing Devices from Proxy Server (Auto Update Server)

You can populate your CiscoWorks RME server with Cisco PIX<sup>®</sup> Firewall device data by importing the data from a supported proxy server such as Auto Update Server.

1. Select Resource Manager Essentials > Administration > Inventory > Proxy Management. The Import from Proxy Server dialog box appears.
2. In the Host Name field, enter the host name of the proxy server.
3. In the Port Number field, enter the port number of the proxy server.
4. In the User Name field, enter the username to be used to log into the proxy server.
5. In the Password field, enter the password and in the Verify field, reconfirm the password.
6. Click the Import button.
7. If there are suspended devices of a deleted proxy server, CiscoWorks RME displays a message asking you to confirm if the existing suspended devices of the earlier proxy server are now to be managed by the new proxy server.

If you click Yes, CiscoWorks RME manages the old devices through the new proxy server and the new devices are imported into the Essentials database. This may take a few minutes.



If you click No, CiscoWorks RME imports the devices of the new proxy server into its database. If some of the old devices appear in this import, they are moved to the managed state. The remaining devices continue to be suspended.

The Add/Import Status Summary dialog box displays the new information.

**Note:** Devices managed via AUS are not fully managed by CiscoWorks RME. Inventory features not supported are check device attributes, export to file, and inventory change filter. Basically, CiscoWorks RME handles configuration and software image management for only these devices.

### 6.3.5. Check Add/Import Summary

When devices are initially imported, they are added to the pending category until the CiscoWorks Inventory Manager has processed them. After devices are processed, they are added either to the Managed table or to one of the Unmanaged tables. You can check the progress on this by selecting the Resource Manager Essentials -> Administration -> Inventory -> Import Status menu item. Note that this screen does not automatically update. Continue to click Update until no devices are left pending. If the import was successful, all devices will be listed under Managed. You should resolve problems with any devices listed under the following unmanaged categories:

- **Alias**—Alias indicates that the same device has been reintroduced into inventory under a different host name or IP address. You must select the device that you want to become managed and placed in the inventory database.
- **Conflicting**—Conflicting indicates that two devices have the same name but different passwords or community strings (attributes). You must select which attributes are correct, that is, the attributes associated with the existing or the incoming device.
- **Not responding**—Not responding indicates that CiscoWorks Inventory Manager could not connect to the device via SNMP. Devices might not respond if there is an incorrect IP address or host name, no route to the device, or no SNMP agent enabled on the device. You should verify connectivity to the device, confirm that all information was entered correctly, and try to resubmit the device for import into the inventory database.
- **Suspended**—Any devices that you have suspended or deleted from the database are listed here. You can suspend any unmanaged devices that you might need to research, and resubmit or delete them later.

**Note:** CiscoWorks RME readds deleted devices only when CiscoWorks Campus Manager finds them if the Campus Manager-to-CiscoWorks RME synchronization is enabled.

### 6.3.6. Check Device Attributes

In order for all CiscoWorks RME functions to work properly, it is imperative that the attributes (community strings and passwords) of each device are placed in the inventory with the device. The Resource Manager Essentials -> Administration -> Inventory -> Check Device Attributes task uses all attributes to access the device. Any failures or lack of attribute data is reported in the View Check Attributes report.

**Note:** This report does not automatically update (click Update Status to update), nor does it give any indication when it is complete.

### 6.3.7. Change Device Attributes

Use the Resource Manager Essentials -> Administration -> Inventory -> Change Device Attributes task to change any device or group of devices attributes. You can also change a specific devices attribute directly from the View Device Attributes report.



Before continuing, make sure all device attributes are correct.

### 6.3.8. Removing Devices from the CiscoWorks RME Inventory

To remove a device from the CiscoWorks RME inventory database, do the following:

1. Select Resource Manager Essentials -> Administration -> Inventory -> Delete Devices. All data associated with the device will be removed, so make sure that you will not need any information before deleting the device.
2. When the device is selected, it is moved to a Suspended status. Click the Suspended link, select Delete Device, and click Finish to permanently remove the device from inventory.

Note that if CiscoWorks Campus Manager runs network discovery regularly, the deleted devices are added again if CiscoWorks Campus Manager finds them.

Note: There is also a CLI command to delete devices from CiscoWorks RME. Refer to the RME help file for more information on this.

### 6.3.9. Schedule Collection

The first way to perform automatic updates of the inventory is by scheduling a complete inventory collection for all managed devices and updating the inventory database if changes have occurred, at a specified time each day or week. This process collects all the latest MIB information for each managed device, including chassis details, hardware and software versions, Flash memory size, and power-supply information, even if the information has not changed on the device. If a change is detected on the device, a change record is also created.

Note: The time of the change is the time of the scheduled collection, and not the time that the change actually happened.

It is recommended that you run Schedule Collection at least once a week to ensure that information in the inventory database reflects up-to-date information about network devices. (Collecting all device inventory information can consume a lot of bandwidth.) You should also set the collection schedule to coincide with any reporting cycle. For example, if you produce inventory reports for management every Friday, you should schedule inventory collection to occur Thursday evening or early Friday morning.

To detect major changes to devices without significantly impacting the network, use Inventory Poller, which is discussed in more detail in the next section.

To set Schedule Collection, do the following:

1. Select Administration -> Inventory -> Schedule Collection from the Resource Manager Essentials drawer.
2. Select the appropriate options from the dialog box and click Finish. The default is once a week at 1:00 a.m.

### 6.3.10. Inventory Poller

The second method to automatically update the inventory for all managed devices is to schedule Inventory Poller, which periodically polls devices for any change. Instead of automatically collecting all information for each managed device, it polls devices to determine if a significant change has occurred, such as a chassis change or a reload. If this type of change is detected, the Inventory Poller then initiates a full inventory collection of all MIB information for that device only.





It is recommended that you use Inventory Poller more frequently to identify inventory changes on the network—as opposed to simply collecting all device information—because it uses fewer resources and will have less impact on the network and network devices. In addition, if it is run more frequently, changes will be detected closer to the time that they actually occur. Schedule Collection should be run less frequently, at night or when network activity is low, to pick up minor changes that are not detected by Inventory Poller.

To set Inventory Poller, do the following:

1. Select Administration -> Inventory -> Inventory Poller from the Resource Manager Essentials drawer.
2. Select Enable and the appropriate date and time options from the dialog box, and click Finish. By default, this function is disabled. It is recommended that you run Inventory Poller at least once a day to check for significant changes to the network. You should run Inventory Poller even more frequently during periods when you know that lots of changes are being made to the network.

#### 6.3.11. Update Inventory

You can update inventory information in the Essentials database immediately at any time by selecting Administration -> Inventory -> Update Inventory from the Resource Manager Essentials drawer. You can select individual devices or a group of devices to be updated. All inventory information is collected for the selected devices, and any noted changes are updated in the Essentials database.

This can be useful if major changes have been made to a few devices or if you need updated information for inventory reports before a scheduled inventory collection. It is important to update inventory information before running any inventory reports, to ensure that information in the reports is up-to-date.

**Note:** All inventory reports include a field with a time stamp indicating when the reported data was collected.

Because inventory information is collected when a device is added to the inventory, you should not need to perform this operation unless there is a specific change and you want to collect the new information.

### 6.4. Configuration Management

The Configuration Management function within CiscoWorks RME provides tools to make it easy to view, update, and track changes to device configurations on all managed devices in one central location.

**Note:** Certain configuration operations may fail in CiscoWorks RME 3.3 if the device is running Cisco IOS versions before Version 12.0 (bug ID CSCdu79886). This forces CiscoWorks RME to try Telnet to obtain the configuration (instead of the default Trivial File Transfer Protocol [TFTP]). The telnet and enable passwords are required for this. This bug has been fixed in Versions 3.3(5) and later.

CiscoWorks RME 3.5 supports job-based passwords, thus allowing CiscoWorks RME to support one-time passwords, for instance. This is supported in NetConfig, Config Editor, and Network Show Commands.

#### 6.4.1. General Setup

You can specify which actions will trigger the configuration archive to be updated, how long configuration files should be stored, and which protocol should be used to retrieve them. CiscoWorks RME then monitors the devices and archives new configuration files accordingly.

To set configuration archive preferences, do the following:





1. Select Administration -> Configuration Management -> General Setup from the Resource Manager Essentials drawer.
2. Using the Archive Setup tab, specify where you want the configuration files to be stored, and how long and how many you want to be stored. You can also ensure that certain configuration files are never purged from the archive (no matter what is set up for how long and how many) by labeling the desired configuration file. Use the Resource Manager Essentials -> Administration -> Configuration Management -> Label Configuration task to label desired configuration files.

Files older than the specified date are automatically deleted from the archive. In addition, if a maximum number of versions is specified, only that number of configuration files is stored for each device. The default is to purge files after 30 days or after 5 versions are stored in the archive. The archive always keeps a minimum of one configuration file for each managed device, regardless of these settings.

If you want to change the location of the configuration archive, you must first create the directory and stop the Change Audit process on the CiscoWorks server.

3. Use the Change Probe Setup tab to select the methods that you would like to use to identify changes to configuration files and update the archive. The following three options are available:
  - Listen to syslog messages—The archive retrieves new configuration files from Cisco IOS devices that forward a syslog message to the CiscoWorks RME server indicating a configuration change.
  - Config retrieval schedule—The archive retrieves configuration files from all managed devices according to the specified schedule.
  - SNMP poller schedule—The archive polls the configuration MIB variable on all managed Cisco IOS devices according to the specified schedule, and retrieves a new configuration file if the configuration has changed.

You can select one or all these methods to ensure that the configuration archive is kept up-to-date. Set the polling frequency and schedule collection based on how often you expect changes to occur on the network and how often you need information for troubleshooting.

Tip: Number of Configurations to Store

It may be a good idea to store a high number of configurations to be able to track changes over long periods of time. Hard-disk space is cheap—down-time is not.

4. Use the Transport Setup tab to select the order of transport protocols that should be used to retrieve configuration files from devices. Device configurations are downloaded to CiscoWorks RME Configuration Manager using TFTP, Telnet, SSH, or rcp. CiscoWorks RME attempts to use the first protocol specified in the list every time a configuration is retrieved. If this fails, it tries the next protocol in the list until retrieval is successful or all protocols have been attempted. Any protocols that are not supported by a device will fail. The default is TFTP, then Telnet, then SSH, then rcp (if rcp is enabled); rcp is disabled by default.

Tip: RCP

The rcp protocol is a connection-oriented protocol and is, therefore, more reliable, but is supported only on Cisco IOS devices.



#### 6.4.2. Config Editor Administration

You can set global job policy preferences so that the settings you use most often are automatically selected every time you create a Config Editor job to download files. You can also define how long Config Editor jobs should be stored in the Essentials database.

To set job preferences, do the following:

1. Start Config Editor by selecting the Resource Manager Essentials -> Configuration Management -> Config Editor menu item.
2. Select Edit -> Set Job Policies from the Config Editor main window.
3. Select the options that you will want to use for most jobs.

Make sure the User Configurable? box is checked if you want to allow users to override these preferences when a new job is created.

4. Select the Purge Policy Enabled box to have jobs automatically deleted after a certain number of days. This helps eliminate old data without requiring you to manually delete jobs. This option is not enabled by default, meaning that jobs will remain in the Config Editor job browser until they are manually removed.

#### 6.4.3. NetConfig Administration

You can set global job policy preferences so that the options you use most often are automatically selected every time you create a new job. You can also define how long NetConfig jobs should be stored in the Essentials database.

To set job preferences in NetConfig, do the following:

1. Start NetConfig by selecting the Resource Manager Essentials -> Configuration Management -> NetConfig menu item.
2. Select Admin -> Set Template Policies from the NetConfig main window.
3. Select the options that you will want to use for most jobs.

Make sure the User Configurable? box is checked if you want to allow users to override these preferences when a new job is created.

4. Select the Purge Policy Enabled box to have jobs automatically deleted after a certain number of days. This will help eliminate old data without requiring you to manually delete jobs. This option is not enabled by default, meaning that jobs will remain in the NetConfig job browser until they are manually removed.

Note: System administrators cannot be assigned NetConfig templates because they already have full access to all templates.

#### 6.4.4. Network show Commands

Network administrators are very familiar with the Cisco router and switch command called show. This command displays configuration or status information at the command line for a device. Now a CiscoWorks RME user can execute numerous show commands against numerous devices and view the results from CiscoWorks RME, using the Network Show Commands function.

This function can be used to display show command output for multiple devices in two modes:

- *Immediate execution*—Run the selected set of show commands for the selected devices immediately.
- *Batch mode*—Schedule a set of show commands to be run against a selected set of devices.



Use the Network Show tasks to organize and save one or more related show commands into logical groups, called command sets. These command sets can then be applied to devices whenever specific configuration or status information is needed.

By default, all users have access to the following six predefined command sets, which come with CiscoWorks RME. These include some of the most common show commands used in monitoring and troubleshooting a network:

- show interface info
- show IP routing info
- show protocol info
- show switch VLAN info
- show system info
- show system performance

In order to display output for other show commands within CiscoWorks RME, you must first define the command set, and then assign users to be able to access the command set.

**Note:** Configuring this functionality is not necessary to get CiscoWorks to perform management of the network. It is more of a “nice-to-have” feature.

#### 6.4.4.1. Creating Command Sets

You can create custom command sets to meet your specific network management needs. Command sets can be created to save any logical group of show commands for information-gathering and troubleshooting purposes. For example, you can create a command set to quickly display the software version running on all network devices. Command sets are stored in CiscoWorks RME and can be executed at any time by users with the appropriate access privileges.

To define a new command set, do the following. You must have either system administrator or network administrator privileges to perform these steps.

1. Select Administration -> Configuration Management -> Network Show -> Define Command Set from the Resource Manager Essentials drawer. A list of predefined command sets and their commands are listed.
2. Click Create to add a new command set. The Define Command Set dialog box will display. Enter the name (up to 12 characters) and description for the new command set.
3. Select the device category ([Cisco] FastSwitch [Device], [Cisco] Catalyst [Switch], or Cisco IOS [Software]) from the pull-down menu to display the available show commands for that device type in the window above. Then add the desired show commands from each category to the command set by selecting them and clicking Add after each selection.

More than one device category can be included in the same command set. For example, you can include show logging commands for both Cisco IOS and Cisco Catalyst devices. **Note:** Up to 6 commands can be added per device category, for a total of 18 show commands in a command set.

4. If you cannot find a show command in the list, enter it in the Custom Command field and click Add. You can include any valid show, ping, trace, where, or help command in a command set, even if it is not included in the list of available commands.
5. When you are done, click Finish.

#### 6.4.4.2. Assigning Users to Command Sets



The ability to use command sets and execute ad hoc show commands from CiscoWorks RME is restricted by user account. By default, all users have access to execute the six predefined command sets that come with CiscoWorks RME. However, users do not have access to execute ad hoc show commands or to use new command sets that are created unless they are explicitly assigned to them. To grant a user access to a newly defined command set, the user must be assigned to the command set. To allow a user to execute any ad hoc show command from the Network Show Command window, the user must be granted remote console access.

To assign a user to a command set or change a user's access privileges, do the following. The user must have either system-administrator or network-administrator privileges to perform these steps.

1. Select Administration -> Configuration Management -> Network Show -> Assign Users from the Resource Essentials Manager drawer. The Assign Users dialog box will display.
2. Select the user account and the command set to be assigned, and click Add.
3. The Enable Remote Console option allows CiscoWorks RME users to act like they are actually at the device command-line prompt. So, check the Enable Remote Console box to allow users to execute individual show commands when they are in the Essentials Network Show Commands screen.

If this option is selected, users will be allowed to execute any valid show, ping, trace, where, or help command from within CiscoWorks RME. If this option is not enabled, users will be able to display output only for the command sets that are assigned to them.

#### 6.4.4.3. Defining Network show Batch Commands

Batch Network Show Command reports allow the user to create a defined set of show and remote console commands to be run against selected devices in a scheduled manner. These reports can run once, daily, or weekly at any time. The command sets available to a user depend on what was assigned to that user. (Refer to "Assigning Users to Command Sets" presented earlier in this section.)

**Note:** Because the number of command sets, the number of devices to run them against, the execution time, and the number of times to be run against are unlimited, the network administrator must be cognizant of the potential load users could place on the network. Give network show command set access only to qualified users.

To define batch reports, do the following:

1. Select Configuration Management -> Network Show Commands -> Batch Reports -> Define Reports from the Resource Manager Essentials drawer. The first of three definition screens will appear.
2. Select Create to define a new report. The second definition screen will be displayed.  
You can also edit or look at the Report Details of an existing report. If the existing report has executed, the number of outputs is indicated.
3. Provide a name for the report and select the devices to be used. There is no maximum number of devices. Click Next to display the final definition screen.
4. Select the command sets to run against the previously selected devices (again no limit.) Also enter any remote console commands to run (no limit—user must have been given access to the remote console). Click Finish to define the report.

#### 6.4.4.4. Scheduling a Network show Command Batch Report

The scheduling of batch reports is wizard driven. Batch reports can be scheduled to run once, daily, or weekly at a user-specified time.



To schedule a batch report, do the following:

1. Select Configuration Management -> Network Show Commands -> Batch Reports -> Schedule Reports from the Resource Manager Essentials drawer. The scheduling wizard will appear.
2. Select the report to schedule and click Next.
3. Provide a description for the scheduled report, and enter the amount and time to execute the report. Optionally, you can be notified by e-mail when the report finishes execution. Click Next.
4. The work order is displayed. Click Finish to schedule the report. The Network Show Job Browser is displayed.

The Network Show Job Browser lists all scheduled and completed batch reports (based on time to purge). From this screen you can view details of the job, edit the job, stop the job, make a copy of the job, or remove the job.

Tip: Launch Job Browser

To launch the Network Show Job Browser, select Resource Manager Essentials -> Configuration Manager -> Network Show Commands -> Batch Reports -> Job Browser.

#### 6.4.4.5. Setting Default Job Properties for Batch Reports

You can set global job policy preferences so that the options you use most often are automatically selected every time you schedule a new batch report. You can also define how long batch report jobs should be stored in the Essentials database.

To set job preferences for Network Show batch reports, do the following:

1. Select Resource Manager Essentials -> Configuration Manager -> Network Show Commands -> Batch Reports -> Set Job Policies. The Set Job Policies screen is displayed.
2. Select an e-mail address to which a job will send status notices about each job. Separate multiple addresses with a comma.

Check the User Configurable? box if you want to allow users to override these preferences when a new job is scheduled.

3. Select the Purge Policy Enabled box to have jobs automatically deleted after a certain number of days. This helps eliminate old data without requiring you to manually delete jobs. This option is not enabled by default, meaning that jobs will remain in the Network Show Job Browser until they are manually removed.

Note: This option is available only to users with either the system or network administrator user role.

### 6.5. Software Image Manager

The Software Management function within CiscoWorks RME provides tools to make it easy to store backup copies of all Cisco software images running on network devices, and to plan and execute a software upgrade to multiple devices on the network at the same time. It can analyze devices against software image requirements to determine device compatibility and make recommendations prior to performing a software upgrade. Software Management reports also allow you to track all software upgrades and monitor known bugs in the software versions running on your network.

Remote stage allows a user to have another Cisco IOS device act as a remote TFTP server from which other devices can upgrade. For instance, if you have a LAN across a slow WAN link, you can configure a Cisco IOS device in that LAN to act as a TFTP server to store images for all your Cisco Catalyst 6500 switches.



### 6.5.1. Establishing Software-Management Preferences

Before you begin using the Software-Management function to track and update software images on your network, you should set the general preferences that will be used for planning upgrades and executing software-management jobs. These options determine where images are stored, what protocol is used to transfer images, what actions are taken during and after a job, and what images are used when planning upgrades to devices.

To set software-management preferences, select Administration -> Software Management -> Edit Preferences from the Resource Manager Essentials drawer.

Following is a brief description of each of the fields and what they mean:

- *History Page Size*—This determines the number of records that are displayed on each page of a Software-Management report before you have to scroll to the next page. Software-Management reports include information on every software modification that is made to devices on the network.
- *Software Image Directory*—This is the location where software images from network devices are stored on the CiscoWorks RME server. It is important to make sure that you have enough space in this location for all software images that you intend to store. Allocate enough space for 2–8 MB per software image. It is a good idea to keep at least one previous version of each software image in case you have to roll back because of errors during an upgrade.

#### Tip: Changing Image Directory

The current software image directory must be empty if you want to change it. Therefore, it is best to change the location before you store any images in the software library. If you want to change the location of the directory after you have already stored images in the library, you must move them to a temporary location, delete the images from the current directory, enter the new directory in CiscoWorks RME, and then move the existing images to the new directory. Any new images added to the software library after that are stored in the new location.

- *User Script Name/Timeout*—These fields can be used to specify a user-defined script that runs before and after every software upgrade job. This can be used to check if the device is available and if anyone is connected to the device before a job is run. It can also be used to check the status of the upgrade after the job is run to determine whether or not to continue. Parameters within the script define whether actions in the script should be performed before or after the job. The timeout value specifies how long the user script is allowed to run before it will fail. The default is 90 seconds. Refer to Section 11, “References,” for more information about the specific parameters that can be used, and the location of a sample script.
- *Turn Debugging On*—This records all activity during a software upgrade or import in a file called `swim_debug.log`. A separate file is created for each job, and is stored within the Essentials directory under `/files/schedule` and the specific job number. This can help identify problems if an upgrade is unsuccessful, but does slow the upgrade process. It is recommended that you turn this option on before rerunning a failed job, or by TAC direction, to help troubleshoot the problem.
- *Use RCP for image transfer*—If this option is checked, Software Manager attempts to use rcp (if available) to copy software images to devices during upgrades. This protocol is connection oriented, and, therefore, more reliable, but it is supported only on Cisco IOS devices. If this option is not checked, TFTP is used.



- *Include CCO Images*—Select this option, if you have access to Cisco.com, to include the most current software images from Cisco when planning upgrades. You can also use the following filters to limit the images that will be included from Cisco.com:
  - Images newer than running image
  - Same image feature subset as running image
  - General deployment
  - Latest maintenance release

If this option is checked, performing a Cisco.com upgrade analysis or image distribution will list only the software images available for the selected device that match the filters selected. You can then download an image directly from Cisco.com into the Essentials software library and use it to upgrade the device.

### 6.5.2. Importing Baseline of Software Images

It is recommended that you first import a baseline of all software images currently 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 become corrupted and need a new software image loaded or if an error occurs during an upgrade.

To import a baseline of all software images on your network, do the following:

1. Select Software Management -> Library -> Add Images from the Resource Manager Essentials drawer.
2. Select Network, click Next, and then select the type of image—Cisco IOS [Software] or Catalyst [Switch]—to import images for all Cisco IOS or Cisco Catalyst devices on the network. Cisco IOS and Cisco Catalyst images must be imported separately.
3. Because the unique set of images is determined (from the information collected by CiscoWorks Inventory Manager), you can check the status by clicking Update until the baseline summary is complete. When completed, click Next to view, select, and confirm all images that will be imported from the network into the software library. For images running on multiple devices, you can select the device from which to pull the image. Click Next and verify the images selected.
4. In the Job Control window, enter job information and click Finish to schedule the job or to execute it immediately. This job first stores a copy of all retrieved software images in a temporary location.
5. To move the files from the temporary location to the software library, you must browse the job results by selecting either the Browse Job Status button for the screen displayed after the job has started or Software Management -> Job Management -> Browse Jobs. When the job status is Pending for Import, click on the job number to view the operational details of the job. Click on the image links within the Job Detail window to add image credentials and to move the images into the software library.

Note: The Job Status screen does not update automatically. Click the Update button to update the job status.

6. The remaining screens are used to verify the images you wish to put in the software library, confirming the features of the images and the ability to edit the image attributes (RAM, Flash memory, and BOOT ROM version requirements; information is used to verify requirements when downloading image to a device). Click Finish to complete the job—move images into the library. When the image is in the library, the job status indicates that the job is completed.





If you left any information blank during the import, such as minimum requirements, you can always go back and edit these later by browsing the images in the library. You can obtain accurate information on minimum requirements from Cisco.com. CiscoWorks Software Manager uses this information to make recommendations when planning upgrades, so it is important that it is accurate.

**Note:** Remember that each image is approximately 2–8 MB, so it is important to make sure that you have enough disk space in the software directory before importing images. It is recommended that you keep at least one previous version of all software images in the Essentials database as a backup.

### 6.5.3. Scheduling Synchronization Job

After you have imported a baseline of all software images into the software library, you can schedule a synchronization job to ensure that the library is up-to-date. This job can be run every day, week, or month, depending on how often you expect changes on your network. After you schedule the synchronization job, CiscoWorks Software Manager compares the software image version information collected by the CiscoWorks Inventory Manager for all managed devices against the software image versions in the library. Any images reported in use by the Inventory Manager that are not in the software library are listed in the Synchronization report. You can then import the images directly from the Synchronization report into the software library, ensuring that you always have a backup copy of all software images running on network devices.

To schedule a synchronization job, do the following:

1. Select Administration -> Software Management -> Schedule Synchronization Job from the Resource Manager Essentials drawer.
2. Select the Schedule radio button, enter the appropriate scheduling information, and click Finish. You can also enter an e-mail address to automatically notify someone of the job results. By default, the synchronization job is not scheduled.

To cancel the job at any time, select the Cancel radio button and click Finish.

3. To view the results of the job, select Resource Manager Essentials -> Software Management -> Library -> Synchronization Report. Use the buttons at the top of the report to import any outstanding images into the software image library.

#### Tip: Scheduling

Schedule the Synchronization Job to occur after an Inventory Scheduled Update to ensure that the inventory information is up-to-date.

### 6.5.4. Schedule Browse Bugs Job

You can also schedule a Browse Bugs job to identify any serious bugs related to software images running on your network. When the Browse Bugs job is scheduled, CiscoWorks Software Manager checks software images running on your network (using information collected by the CiscoWorks Inventory Manager) with software bugs logged on Cisco.com. Results of the job are posted in the Browse Bugs report.

**Note:** You must have access to Cisco.com to use this feature.

To schedule a Browse Bugs job, do the following:

1. Select Administration -> Software Management -> Schedule Browse Bugs Job from the Resource Manager Essentials drawer.





2. Click the Schedule radio button to activate the job, enter the appropriate scheduling information, and click Finish. You can also enter an e-mail address to automatically notify someone of the job results. By default, the job is not scheduled.

To cancel the job at any time, select the Cancel radio button and click Finish.

3. To view the results of the job, select Software Management -> Bug Report -> Browse Bugs from the Resource Manager Essentials drawer. The report shows only new bugs for software images running on your network that have been reported since the job was last run.

View this report periodically to determine if any serious bugs have been found that might impact your network. If so, you might need to plan a software upgrade to eliminate problems.

**Tip: Ad-Hoc Bug Reports**

You can also look up all the known bugs for a specific device or details for a specific bug ID at any time by selecting Software Management -> Bug Report -> Browse Bugs by Device or Locate Devices by Bugs. This retrieves the latest software image bug information for the selected device(s) or bug from Cisco.com and displays a summary report.

## **6.6. Change Audit**

The Change Audit Services (CAS) function within CiscoWorks RME provides tools to make it easy to quickly locate changes that have been made to a specific device, by a specific user, or during a specific time period. It provides a comprehensive record of who changed what, when, and how. This can help narrow down the source of problems when trying to troubleshoot a network error.

### **6.6.1. Configure Inventory Change Filter**

The CiscoWorks Inventory Change Filter lists all inventory attributes monitored for change. If any of the listed attributes changes between inventory updates (manual or automatic), then the inventory for that device is considered to have changed. This causes creation of a Change Audit Record.

After reviewing the inventory changes, you may not wish change in a certain attribute to cause the creation of a change audit record. To “filter” out this attribute and no longer monitor its changes, check the appropriate attribute in the Inventory Change Filter task. It can be launched by selecting Resource Manager Essentials -> Administration -> Inventory -> Inventory Change Filter.

**Note:** Place a checkbox next to the inventory information you do not want to monitor for changes. Normally this setting is not changed.

**Note:** These changes are still recorded in the inventory database and reflected on inventory reports. They just do not show up in Change Audit reports, to help simplify your monitoring of changes.

### **6.6.2. Defining Exception Periods**

Exception periods are defined as time periods in which you expect no changes to occur to devices on the network. Change Audit allows you to define exception periods for each day of the week. When these periods are defined, you can quickly determine if there has been unexpected activity by viewing the Exceptions Summary Report. The exception period defined acts as a filter on the change audit database, allowing for a quick method to search for change records during that defined time period.

**Tip: Alternative Use**



The Exceptions feature can be used more generally as a time filter to view what activity took place during specified times, not just what did not happen.

To define exception periods, do the following:

1. Select Administration -> Change Audit -> Define Exceptions Summary from the Resource Manager Essentials drawer.
2. Select the times and days of the week that you want to be included in the report, and click Finish (for example, from 8:00 a.m. to 6:00 p.m. on Monday through Friday, or all day Saturday and Sunday).

Tip: Exceptions Summary Report

To view the Exceptions Summary Report, select Change Audit -> Exceptions Summary from the Resource Manager Essentials drawer.

Note: The Exceptions Summary Report displays changes only for the past week.

### 6.6.3. Forwarding Traps

You can configure Change Audit Services to forward change records as SNMP traps to a remote server that has the ability to receive and display traps, allowing you to monitor change events from a remote enterprise NMS, such as HP OpenView. You can define up to two remote servers to receive the traps. Change Audit Services forwards the details of all change records for the selected functions in the form of SNMPv1 traps.

To establish the trap generator, do the following:

1. Select Administration -> Change Audit -> Administer Trap Generator from the Resource Manager Essentials drawer.
2. Select Start to begin using the trap-generator feature, and select the CiscoWorks RME functions for the traps that should be generated. You can select all functions or limit to any of the following: Config Archive, NetConfig, Config Editor, Software Management, or Inventory.

Note: Only functions that have previously seen changes are listed.

3. Enter the port number and IP address or host name of the remote server(s) that should receive the traps, and click Finish. The standard port for SNMP traps is 162. If you are forwarding traps to two servers, make sure you select the Dual Destinations option.

Tip: ChangeAudit MIBs

The ChangeAudit MIB files can be found at \$NMSROOT/objects/share/mibs.

### 6.7. Syslog Analysis

If devices on the network experience critical errors or faults, such as an unexpected reload or link failure, you want to know about it. Many Cisco devices log details about such events as syslog messages. These messages can be forwarded to the CiscoWorks RME syslog Analysis function to notify you of important errors, exceptions, and other activity on network devices. By having this information forwarded from devices and centrally stored in one location, you can identify and respond to problems on the network more quickly and minimize the impact to users.



The Syslog Analysis function within CiscoWorks RME provides an easy way to view, search, and filter syslog messages sent from devices in the network. It allows you to view syslog messages for a specific device, severity level, or date. You can filter out unwanted syslog messages and display only events that are important to your operation. In addition, Syslog Analysis reports include an explanation and recommended action for each event, a scenario that can help you determine what to do next.

### 6.7.1. Verifying Storage Options

Syslog messages are stored in the Essentials database for both managed and unmanaged devices. Managed devices are devices that have been successfully added to the Essentials inventory. Unmanaged devices are any devices on the network that have not been added to the Essentials inventory, either because they have not been identified or because the user chooses not to add it. The Syslog database contains messages from unmanaged devices if devices have been configured to log messages to the Essentials server but have not been added to the Essentials inventory. This can help you identify devices on the network that are missing from the Essentials inventory.

For managed devices, you can choose to keep messages in the syslog database for 1 to 14 days, depending on your network-troubleshooting needs. The default is 7 days. The maximum number of messages that will be stored for managed devices is 1 million. This option cannot be changed.

You can also specify how many messages to keep from unmanaged or unrecognized devices. The default is 50,000 messages.

**Note:** The device should use the management interface as the syslog source, otherwise CiscoWorks RME might get confused about whether the message comes from a device that it manages. To do this, use the logging trap source command in Cisco IOS Software.

To view and change storage options, do the following:

1. Select Administration -> Syslog Analysis -> Change Storage Options from the Resource Manager Essentials drawer.
2. Change the number of days or number of messages and click Finish. There is no limit to the number of messages that can be stored for unmanaged devices.

**Note:** When the threshold of messages or number of days has been reached, messages are purged from the syslog database. Messages are never purged from the syslog source file. However, if the syslog file becomes too large, you might need to manually clear or archive it. You can determine the location of the source file by looking at the path in the Message Source field at the bottom of the Change Storage Options window.

3. Enter the backup configuration information (refer to Table 7).

Table 7 Field Descriptions

Field	Description
Backup required	Check this to enable the backup process for syslog messages.
Backup directory	Enter the backup directory. When you start the backup process the syslog backup data gets stored in SyslogBackup.csv file. This SyslogBackup.csv file is in CSV format.



Table 7 Field Descriptions

Field	Description
Maximum size of the backup file (in MB)	Enter the maximum size that you want to set for the backup file.
E-mail addresses	Enter the e-mail ID for the notification to clean up the backup file. <b>Note:</b> On Windows, you must configure the SMTP server.

### 6.7.2. Defining Message Filters

You can create filters to exclude specific message types from being stored in the Syslog database. These filters will be applied to incoming syslog messages, and they can be used to eliminate unnecessary or low-priority messages from being saved in the Essentials Syslog message database. For example, if you use a firewall on your routers, you might not want to track all the audit trail messages that are generated every time someone goes through the firewall. You can enable a message filter to eliminate these messages from being stored in the Syslog database (or keep the firewall from sending them to you by configuring the device). Four predefined filters are included with CiscoWorks RME:

- Link up and down messages
- Cisco IOS Firewall audit trail messages
- Cisco PIX Firewall audit messages
- Severity 7 messages

By default, the last three are enabled. To include any of these messages in Syslog reports, the corresponding filter must be disabled. Message filter names preceded by a green icon in the Define Message Filter screen are currently active.

To create or enable a message filter, do the following:

1. Select Administration -> Syslog Analysis -> Define Message Filter from the Resource Manager Essentials drawer.
2. Select Add to create a new filter, or highlight an existing filter and click Change.
3. Select the specific messages that should be excluded from the Syslog database and click Add. Check the Enable Filter box to begin using the filter. Deselect the box to stop using a filter that has been enabled. Enabled filters are shown preceded by a green icon.

To make the message type selected more specific, highlight the message type and click Advanced. Change any of the wildcard fields (denoted by an asterisk) to make the message type more specific. Use this screen to add multiple instances of this message type with different specifics. These are the wildcard fields that can be changed to make the filters more specific:

- *Facility*—Enter the codes for the facilities you want reported. A facility is a hardware device, a protocol, or a module of the system software. See the Cisco IOS reference manual “System Error Messages” for a predefined list of system facility codes. Each code can consist of two or more uppercase letters. You can enter several facility codes, separated by commas; for example, SYS,ENV,LINK.



- **Severity**—Enter codes for the message severity levels you want reported. You can enter several severity codes, separated by commas. You must enter each severity level you want to report. For example, enter 0,1,2 to report all emergencies, alerts, and critical messages. Table 8 gives the codes that are allowed.

Table 8 Severity Codes

Code	Severity
0	Emergencies
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debug

- **Mnemonic**—Enter a code that uniquely identifies the error message.  
Note: To match for Cisco Catalyst 5000 Series devices, enter a hyphen (-) to indicate an empty mnemonic field. You can enter several mnemonics, separated by commas. An example is -, UPDOWN, RELOAD, CONFIG.
- **Pattern**—Enter a text string used to match substrings in the message’s “Description” field. You can use the asterisk character \* to represent a text string of zero or more characters. For example, enter \*router\* to include all messages that contain the word router in their description. Enter router\* to include all messages that begin with the word router.
- **Device names**—Enter the device names or corresponding IP addresses for which a filtering criteria has to be applied. To apply a criterion to a set of devices, you can use wildcards. For example, enter router\* to include all devices that begin with the word router. Wildcards cannot be used with IP addresses.

Click OK to close the Advanced message dialog and click Finish to finish adding and editing the message filter.

Note: The filters will be applied only to messages sent after the filter is enabled. Any messages that are already in the database from previous collections are not filtered out and are still displayed in reports.

### 6.7.3. Defining Automated Actions

Another feature of Syslog Analysis allows you to link a specific syslog message type to a command, so that any time that message type is received, the command is executed. For example, you can have CiscoWorks RME send an e-mail with the message text and device name to the system administrator any time a critical severity level 1 error message is received. This can help proactively notify you of faults on the network, so that you can respond to errors quickly before many users are impacted.

The action to be executed must be defined by the user in a script. Two arguments are available in CiscoWorks RME that can be passed to the script:



- \$M = The entire syslog message
- \$D = The device name

A sample e-mail script, and directions for use, can be viewed by clicking on the Help button of the Define Automated Action screen and then clicking on the Example link.

To create an automated action, do the following:

1. Select Administration -> Syslog Analysis -> Define Automated Action from the Resource Manager Essentials drawer.
2. Click Add to create a new action.
3. Select the specific message types that should trigger the action and click Add. The command is executed if any of the selected messages types is received. (Like message filters, use the Advanced button to be more specific.)
4. Check the Enable Action box to begin using the action. Deselect the box to stop using an action that has been enabled. Enabled actions are shown preceded by a green icon.
5. Enter the command to be executed, or the path and filename of a script that contains a series of commands, in the Command-Line field, and click Finish.

Note: Only syslog messages from managed devices can be handled by automated action.

Note: Scripts cannot require X or console access, and must be CLI based throughout.

#### 6.7.4. Creating Custom Syslog Reports

Syslog Analysis provides 13 default custom reports for displaying common types of syslog messages such as configuration changes, reloads, and duplicate IP addresses. You can also create your own custom syslog reports to display specific syslog messages or groups of messages. Defined Custom Syslog reports can be added to the Syslog 24-Hour Report as a reminder to check them on a daily basis.

To create or modify a Custom Syslog report, do the following:

1. Select Administration -> Syslog Analysis -> Define Custom Report from the Resource Manager Essentials drawer.
2. To create a new report, click Add. To use a predefined report as a template or to modify an existing report, highlight the report and click Change.
3. Select the specific messages that should be included in the report and click Add. Check the 24-Hour Report box to include the report in the Syslog 24-Hour Report. Like Message Filter and Automated Actions, use the Advanced button to be more specific for a particular syslog message.
4. Click Finish to add the report to the list of Custom Reports.

Tip: Viewing Custom Reports

To view a Custom Report, select Syslog Analysis -> Custom Reports or Custom Reports Summary under the Resource Manager Essentials folder. Any reports that have the 24-Hour Report box checked are also displayed under 24-Hour Reports -> Syslog Messages.

Note: If you want to add or remove a report from the Syslog 24-Hour Report, you must edit the report and check or uncheck the 24-Hour Report box. Reports included under 24-hour reports are shown preceded by a green icon.



### 6.7.5. Specifying a User URL

**Note:** Configuring this parameter is not common, and should be left to expert users.

If you are familiar with Common Gateway Interface (CGI) programming, you can configure Syslog Analysis to display syslog reports on a customized Web page. This is an advanced option for those who want to customize message logging. You might use this option to customize descriptions of your error messages, or to create a script that generates specific procedures for resolving a particular system message.

To specify a URL for the Web page, do the following:

1. Select Administration -> Syslog Analysis -> Change User URL from the Resource Manager Essentials drawer.
2. Enter the name and location of the CGI script that defines the Web page, and click Finish.

**Tip:** Sample Script

A sample script is located in the cgi-bin\Sysloga folder of the CiscoWorks RME root directory. You can also view this example by clicking the User-URL icon in any detail syslog message reference.

## 6.8. Availability Manager

The Availability function within CiscoWorks RME provides reports to quickly assess the status of selected devices on the network. The reports can provide details on device reachability, interface status, and reloads for any managed device in the Essentials inventory. Information can be tracked for all devices on the network, or only critical devices to reduce the load on the network and NMS.

### 6.8.1. Establishing Polling Options

To begin using the Availability function within CiscoWorks RME, you must determine which devices will be polled and how often. This will determine what information is tracked and displayed in all Availability reports. It is important to poll critical devices frequently to ensure that errors are discovered quickly. However, you do not want to create too much additional traffic on the network by polling excessively, or polling noncritical devices. Also, remember that if you are using an enterprise NMS such as HP OpenView, it may already be providing you with the information you need on device availability. If so, you do not want to duplicate the polling.

To set polling options, do the following:

1. Select Administration -> Availability -> Change Polling Options from the Resource Manager Essentials drawer.
2. Select the device views you want to poll for availability, and click Add to include in availability polling. When all views desired have been selected, click Next. By default, no views are selected. Therefore, you must select at least one view, or no information will be displayed in Availability reports. You can choose to poll all devices, or select only certain classes of devices. Any custom or private views that you have created can also be used.
3. Next, select the frequency for polling, number of ping packets, and SNMP settings. Then click Finish.

**Note:** Remember that each device polled increases the amount of traffic on the network because of SNMP requests.

**Note:** The same polling options are used for all device views. You cannot set unique polling options for each view polled.



Note: It is also important to note that these SNMP settings are used only for Availability polling. SNMP requests for all other functions use the SNMP settings under Administration -> System Configuration -> SNMP Tab.

## 7. CiscoWorks Device Fault Manager

CiscoWorks DFM reports faults that occur on Cisco devices, often identifying fault conditions before users of network services realize that the condition exists. DFM analysis technology differs from the traditional rules-based approach to event analysis. CiscoWorks DFM analysis uses a top-down approach that starts by identifying the fault conditions that affect managed systems and are important to identify and analyze. Each fault condition causes a set of symptoms—a problem signature—that occur within the faulty element and in related elements. CiscoWorks DFM creates a causality mapping between the fault conditions and the symptoms. After the fault conditions and their symptoms are identified, this information is coded in the analysis model.

Because the event information necessary to diagnose fault conditions is present in the analysis model, CiscoWorks DFM monitors only the events necessary to diagnose the condition. CiscoWorks DFM simplifies event analysis: there are no rules to write, and the analysis model guarantees that critical fault conditions are always identified.

CiscoWorks DFM can operate as an independent management system or can integrate with existing management applications to add fault management to the functionality already in place.

Note: This document does not specify how to configure polling intervals or thresholds in CiscoWorks DFM.

### 7.1. Trap Receiving

CiscoWorks DFM can listen for traps that indicate faults and problems such as link down, etc. To configure which port will be monitored for SNMP traps CiscoWorks DFM receives from other NMSs:

1. Make sure the devices or NMSs that are forwarding traps to CiscoWorks DFM are configured to send them to the port defined in the adapter configuration file.
2. If another NMS is already listening for traps on the standard User Datagram Protocol (UDP) trap port (162), you must configure this adapter to use another port, such as port 9000.
3. Select Device Fault Manager -> Administration -> Trap Configuration -> Trap Receiving.
4. In the Listening Port field, enter the port number of the local host where the CiscoWorks DFM server is running.
5. Click OK.

Note: CiscoWorks DFM may fail to register at port 162 if other trap listeners (such as HP OpenView, CiscoWorks Real-Time Monitor [RTM], or Cisco TrafficDirector) are installed on the same server.

### 7.2. Trap Forwarding

CiscoWorks DFM can be configured to listen for traps from Cisco devices and forward these traps to other NMS platforms for further actions.

To have CiscoWorks DFM send received traps to other NMSs:

1. Select Device Fault Manager -> Administration -> Trap Configuration -> Trap Forwarding.
2. In the Forwarding field, select ON or OFF to enable or disable trap forwarding.
3. If you want to add a recipient, in the Add Recipient field, enter the host name and port number of the machine you want to forward traps to.





4. If you want to remove a recipient, select the recipient from the Remove Recipient field.
5. Click OK.
6. If you want to add or remove any other recipients, repeat the appropriate steps, and click OK. Repeat these steps until you have added or removed all recipients.
7. For your changes to take effect, you must stop and restart the CiscoWorks DFM server process using Server Configuration -> Administration -> Process Management.

Note: When forwarding traps, the trap gets the source IP address from the CiscoWorks DFM server, not the originating device.

### **7.3. Configure the File Notifier Adapter**

It may be that a line has gone down and come online again without your noticing. This does not show in the CiscoWorks DFM event log. In order to keep track of all history, you should enable the CiscoWorks DFM File Notifier. This logs all events to \$NMSROOT/objects/smarts/logs/sm\_file\_notifier.log.

To enable or disable logging and storing alarms detected by CiscoWorks DFM in a log file:

1. Select Device Fault Manager -> Administration -> Fault Notification -> File Notifier.
2. In the Adapter field, select ENABLED or DISABLED to start or stop event logging in the alarms file.
3. Click OK.

### **7.4. Configure the Mail Notifier Adapter**

CiscoWorks DFM can be configured to send mail when an event occurs. This is done using the CiscoWorks DFM Mail Notifier. To notify other users of DFM alarms:

1. Select Device Fault Manager -> Administration -> Fault Configuration -> Mail Notifier.
2. In the Adapter field, select ENABLED or DISABLED to start or stop trap notification.
3. If you want to add a recipient, in the Add Recipient field, enter the host name and port number of the machine you want to notify about alarms.
4. If you want to remove a recipient, select the recipient from the Remove Recipient field.
5. In the SenderID field, enter the address associated with the adapter.
6. In the MailServer field, enter the fully qualified domain name for the mail host.
7. Click OK.

Note: This can generate a lot of mail and should be used with caution. Check the CiscoWorks DFM Help file for information on which files to modify to lower the amount of mail generated.

### **7.5. Configure the Trap Notifier**

In addition to receiving and forwarding traps, CiscoWorks DFM also polls devices for information and compares the polled information with thresholds. If a threshold has been breached, CiscoWorks DFM can be configured to send a trap of its own to an external NMS system:

1. Select Device Fault Manager -> Administration -> Fault Notification -> Trap Notifier.
2. In the Adapter field, select ENABLED or DISABLED to start or stop trap notification.



3. If you want to add a recipient, in the Add Recipients field, enter the host name and port number of the machine you want to notify about events and alarms.
4. If you want to remove a recipient, select the recipient from the Remove Recipient field.
5. Click OK.

## 8. Best Practices

- Use TACACS+ or Remote Access Dial-In User Service (RADIUS) authentication when accessing network devices.
- Configure a separate CiscoWorks user for TACACS+ or RADIUS.
- Baseline your network with regard to both configuration and performance.

### 8.1. Network Documentation

Document the physical network, including the network equipment and the wiring. Know which devices are connected to which ports of each switch and router. Also be able to identify which cables actually connect those devices.

Document the logical network as well, including topology diagrams, network addressing schemes (for example, IP, Internetwork Packet Exchange [IPX]), VLANs, as well as a list of IP addresses for critical devices [for example, routers, switches, and servers])

Good documentation enables quicker problem resolution when troubleshooting; it also allows outside people (for example, Cisco TAC) to quickly learn the network topology and begin problem resolution.

### 8.2. Change Control

Whenever possible, define and adhere to move, add, or change policies in which all network modifications are documented and planned in advance. Physical maps and inventories should always reflect any changes. The source of many network problems can often be traced back to a set of changes—when documented.

Secure the wiring closets, and grant access in a controlled manner only. An unlocked closet is begging to be disturbed.

### 8.3. Out-of-Band Management

Build a single VLAN (that is, IP subnet) dedicated for network management traffic. Connect the NMS as well as all (or critical data center) network devices (if possible) to this VLAN. This VLAN may consist simply of a single 10/100 Ethernet switch with which all network devices are connected. In this way, if there are network problems (in band) the devices are still manageable and able to report SNMP and syslog information back to the NMS that is directly connected.

Dedicate a workstation to run the NMS applications. In this way, your management applications and management data are not adversely affected by other nonmanagement applications (in terms of CPU, memory, disk space, operating system conflicts, etc.) and users.

### 8.4. Fault Monitoring

Configure all network devices for SNMP access and SNMP trap generation. SNMP access and trap generation provide read and write access to the NMS as well as real-time fault and alarm detection.



Configure all network devices for syslog message generation with time stamps. Devices then send their console messages to a centralized syslog server for later reference and correlation.

Synchronize the system clocks (date and time) on all network devices and on the NMS with NTP, a step that greatly improves event correlation abilities.

Configure all Cisco IOS devices to log console messages to their internal log via the logging buffered command. This stores console messages for later review and retrieval.

### **8.5. Technical Support Tips**

Provide modem access to your network for remote technical support (that is, Cisco TAC). This allows the TAC engineers to dial in and begin troubleshooting your Cisco network first hand.

Always have the Cisco TAC phone number and your contract number readily available so as to avoid delays in your TAC case handling.

In case of network problems, do not reboot a device without first capturing its internal log file (stored console messages) via the show log command.

### **8.6. Collect Baseline Data**

After designing, deploying, and documenting the network, it is time to learn the true nature of the network by monitoring data over time and studying traffic flows.

Baselining is key to knowing whether the network is healthy and for future capacity expansion. Baselining should be done at least on a quarterly basis.

Example information to collect includes:

- CPU utilization for routers, switches, and servers
- Memory utilization
- Link and interface utilization (LAN and WAN)
- Error rate, particularly cyclic-redundancy-check (CRC) errors
- Broadcast traffic

Deploy Remote Monitoring (RMON) probes (that is, probes or Cisco Network Analysis Module [NAM]) on critical device ports to collect baseline data.

A critical port is one that is vital to the success of network operation. Examples of critical port connections include:

- File and application server ports
- Router ports
- Trunk ports
- “Mahogany Row” ports (those executives in which you never want the network to go down)

Cisco SwitchProbe™ devices can determine baselines at data link, network, and application layers of the Open System Interconnection (OSI) stack.

### **8.7. Test Lab and Equipment**

Test new switches, routers, protocols, software, Cisco IOS configurations, etc. before deploying in the network.



Lab testing enables you to verify correct operation of the device, Cisco IOS configurations, etc.; it also reveals if any custom tuning (for your environment and applications) is required.

The test lab also serves as a training facility for network staff. Staff can rehearse upgrades and cutovers before performing on the production network (avoiding costly mistakes).

The Portable Network General Sniffer is also valuable for troubleshooting network and application problems.

### **8.8. Training**

Target those courses that apply to your environment (for example, LAN switching, ATM LAN Emulation [LANE], Open Shortest Path First [OSPF]).

Training everyone may not be realistic. Formal procedures are then needed for the less trained to follow (during cutovers, outages, etc.). Procedures include, for example, the Cisco IOS commands that need to be issued, what data to collect, how to call and escalate within Cisco TAC, etc.

### **8.9. Network Operations Center**

Set up a real network operations center (NOC) (24 x 7 if applicable).

Convert any existing mainframe people into LAN or WAN NOC operators as well.

The NOC operators should either be trained or have formal procedures instructing them how to detect and respond to network events.

### **8.10. Sniffer**

A good network sniffer can be a very useful tool in troubleshooting your network faults. A good freeware sniffer is Ethereal (<http://www.ethereal.com>), which works on the most popular OS platforms. A CiscoWorks front end for this tool, called JET is available from <http://cosi-nms.sourceforge.net/decode-progs.html>.

### **8.11. Spanning-Tree Documentation**

Procedurally save a printout or Visio file of every VLAN topology using the Spanning-Tree Filter option (that is, 10 VLANs = 10 topology diagrams if per-VLAN spanning tree is used. [Remember that each VLAN has its own characteristics and, therefore, should be considered as a network by itself with distinct and differing connectivity. Validate that the diagram depicts all the switches that the VLAN is configured on. Include extra information on this Visio or printed-out diagram such as root costs, primary and secondary root bridges, as well as additional parameters such as VTP domain, VTP mode, trunk mode (802.1Q or Inter-Switch Link [ISL]), root port, designated port, port cost, tweaked timers (hello, diameter), trunk links, and also the expected operating states of each port and link that is in a blocking or forwarding state. In certain cases, provide these diagrams with indicated STP, that is, STP Single Instance (generally third-party switches such as 3Com switches), PVST+-to-Single STP mapping, PVSTP+, and Multi-instance STP.

These diagrams will remove countless hours from CiscoWorks Campus Manager fault-finding and troubleshooting complexities, add more preemptive control, and potentially alert on any STP design and configuration issues.

## **9. Postinstallation Checklist**

Following is a quick checklist of variables that should have been reviewed or configured in a typical CiscoWorks configuration. Note that not every configuration item mentioned earlier in this document is listed here; only the most important ones are shown.



## **9.1. Device Setup**

### **9.1.1. Cisco IOS Devices**

- [ ] Community strings
- [ ] System reload
- [ ] Syslog message logging
- [ ] Telnet
- [ ] Command-line prompts
- [ ] Cisco Discovery Protocol
- [ ] SysName variable

### **9.1.2. Cisco Catalyst Devices**

- [ ] Community strings
- [ ] Syslog message logging
- [ ] Telnet
- [ ] Command-line prompts
- [ ] Cisco Discovery Protocol

## **9.2. CiscoWorks Security**

- [ ] Select login module.

Menu item: Server Configuration -> Setup -> Security -> Select Login Module

- [ ] Change admin password and set up Cisco.com connection.

Menu item: Server Configuration -> Setup -> Security -> Modify My Profile

- [ ] Create additional users.

Menu item: Server Configuration -> Setup -> Security -> Add Users

- [ ] Schedule backup.

Menu item: Server Configuration -> Administration -> Database Management -> Schedule Backup

## **9.3. Automatic Package Download**

- [ ] Configure Cisco.com account.

Menu item: Device Manager -> Administration -> Package Support Updater -> CCO Connection

- [ ] Schedule downloads.

Menu item: Device Manager -> Administration -> Package Support Updater -> Schedule Downloads

- [ ] Import new packages.

Menu item: Device Manager -> Administration -> Package Support Updater -> Staging Area Contents

Note: This is a recurring task.



#### **9.4. Network Discovery**

- [ ] Configure device and credentials synchronization.

Menu item: Server Configuration -> Setup -> ANI Server Admin -> Device Synchronization

- [ ] Configure SNMP settings.

Menu item: Server Configuration -> Setup -> ANI Server Admin -> SNMP Settings

- [ ] Review or configure discovery schedule.

Menu item: Server Configuration -> Setup -> ANI Server Admin -> Discovery Schedule

- [ ] Review or configure user and host acquisition schedule.

Menu item: Server Configuration -> Setup -> ANI Server Admin -> User and Host Acquisition

- [ ] Configure discovery settings.

Menu item: Server Configuration -> Setup -> ANI Server Admin -> Discovery Settings

- [ ] Perform discovery.

- [ ] Create topology groups.

Menu item: Campus Manager -> Administration -> Topology Groups

- [ ] Configure path analysis and user tracking scheduling.

Menu item: Campus Manager -> Administration -> Job Schedule

#### **9.5. Resource Manager Essentials**

- [ ] System Settings

Menu item: Resource Manager Essentials -> Administration -> System Configuration

##### **9.5.1. Job Approval**

- [ ] Create approver list.

Menu item: Administration -> Job Approval -> Create Approver List

- [ ] Enable job approval if desired.

Menu item: Administration -> Job Approval -> Edit Preferences

##### **9.5.2. Inventory Management**

- [ ] Check Add / Import Summary.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Import Status

- [ ] Check device attributes.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Check Device Attributes

- [ ] Change device attributes.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Change Device Attributes

- [ ] Remove unwanted devices.



Menu item: Resource Manager Essentials -> Administration -> Inventory -> Delete Devices

- [ ] Schedule collection.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Schedule Collection

- [ ] Configure inventory poller.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Inventory Poller

- [ ] Manually update inventory.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Update Inventory

### 9.5.3. Configuration Management

- [ ] Check general setup.

Menu item: Resource Manager Essentials -> Administration -> Configuration Management -> General Setup

- [ ] Setup Config Editor.

Menu item: Resource Manager Essentials -> Configuration Management -> Config Editor

Menu item: Edit -> Set Job Policies

- [ ] Setup NetConfig.

Menu item: Resource Manager Essentials -> Configuration Management -> NetConfig

Menu item: Admin -> Set Template Policies

#### 9.5.3.1. Network show Commands

- [ ] Create command sets.

Menu item: Resource Manager Essentials -> Administration -> Configuration Management -> Network Show -> Define Command Set

- [ ] Assign users to command sets.

Menu item: Resource Manager Essentials -> Administration -> Configuration Management -> Network Show -> Assign Users

- [ ] Define network show batch commands.

Menu item: Resource Manager Essentials -> Configuration Management -> Network Show Commands -> Batch Reports -> Define Reports

- [ ] Schedule a Network show Command Batch Report.

Menu item: Resource Manager Essentials -> Configuration Management -> Network Show Commands -> Batch Reports -> Schedule Reports

- [ ] Set default job properties for Batch reports.

Menu item: Resource Manager Essentials -> Configuration Manager -> Network Show Commands -> Batch Reports -> Set Job Policies

### 9.5.4. Software Image Manager

- [ ] Establish software-management preferences.



Menu item: Resource Manager Essentials -> Administration -> Software Management -> Edit Preferences

- [ ] Import a baseline of software images.

Menu item: Resource Manager Essentials -> Software Management -> Library -> Add Images

- [ ] Schedule a synchronization job.

Menu item: Resource Manager Essentials -> Administration -> Software Management -> Schedule Synchronization Job

- [ ] Schedule a browse bugs job.

Menu item: Resource Manager Essentials -> Administration -> Software Management -> Schedule Browse Bugs Job

#### 9.5.5. Change Audit

- [ ] Configure the inventory change filter.

Menu item: Resource Manager Essentials -> Administration -> Inventory -> Inventory Change Filter

- [ ] Define exception periods.

Menu item: Resource Manager Essentials -> Administration -> Change Audit -> Define Exceptions Summary

- [ ] Configure trap forwarding.

Menu item: Resource Manager Essentials -> Administration -> Change Audit -> Administer Trap Generator

#### 9.5.6. Syslog Analysis

- [ ] Verify storage options.

Menu item: Resource Manager Essentials -> Administration -> Syslog Analysis -> Change Storage Options

- [ ] Define message filters.

Menu item: Resource Manager Essentials -> Administration -> Syslog Analysis -> Define Message Filter

- [ ] Define automated actions.

Menu item: Resource Manager Essentials -> Administration -> Syslog Analysis -> Define Automated Action

- [ ] Create custom Syslog reports.

Menu item: Resource Manager Essentials -> Administration -> Syslog Analysis -> Define Custom Report

#### 9.5.7. Availability Manager

- [ ] Establish polling options.

Menu item: Resource Manager Essentials -> Administration -> Availability -> Change Polling Options

### 9.6. CiscoWorks Device Fault Manager

- [ ] Configure trap reception.

Menu item: Device Fault Manager -> Administration -> Trap Configuration -> Trap Receiving

- [ ] Configure trap forwarding.

Menu item: Device Fault Manager -> Administration -> Trap Configuration -> Trap Forwarding





[ ] Configure the File Notifier Adapter.

Menu item: Device Fault Manager -> Administration -> Fault Notification -> File Notifier

[ ] Configure the Mail Notifier Adapter.

Menu item: Device Fault Manager -> Administration -> Fault Notification -> Mail Notifier

[ ] Configure the Trap Notifier.

Menu item: Device Fault Manager -> Administration -> Fault Notification -> Trap Notifier

## 10. Troubleshooting

This section contains descriptions of common problems and instructions on how to fix those problems.

### 10.1. General

#### 10.1.1. Known Problems

Known problems are unexpected behaviors or defects in CiscoWorks Software releases. You can search for known problems in the product release notes or on the Cisco bug tracking system tool, called Bug Navigator II.

To access Bug Navigator II, either:

- Enter <http://www.cisco.com/support/bugtools> in your Web browser and then select Bug Navigator II

or

- Log in to Cisco.com and select Services & Support -> Technical Assistance Center. Locate the Troubleshoot link and then locate the Software Bug Toolkit/Bug Watcher link. Select Bug Navigator II to enter the utility.

Locate CiscoWorks in the navigation window on the left side of the browser and then locate the product name.

Normally, the known problems at the time of release are also documented in the release notes.

### 10.2. CD-One

#### 10.2.1. Troubleshooting Login Authentication

CiscoWorks enables you to set debugging on your authentication module so that you have additional information in the log files to use for troubleshooting. Turn debugging on only when requested to do so by your customer service representative. Enabling debugging does not alter the behavior of the modules.

To turn debugging on, go to the Setup -> Security folder located in the CiscoWorks drawer. Click on Select Login Module. From the dialog window, click on Edit Options. The option to turn debugging on is available from the next dialog window.

Debugging information is not displayed in the CiscoWorks user interface, but is stored in the following locations:

UNIX Environment:

<install directory>/objects/jrun/jsm-cw2000/logs/stdout.log

Windows Environment:

C:\<install directory>\lib\jrun\jsm-cw2000\logs\stdout.log



Note: The stdout.log parameter can sometimes be incomplete when it comes to troubleshooting. The user should get the stderr, stdout, and event logs. These are all located in the logs directory mentioned previously.

Also, the Java PlugIn (JPI) console is useful for CiscoWorks CMF 2.1, and the native browser virtual machine console for CiscoWorks CMF 2.2.

### 10.2.2. Troubleshooting User Accounts

Although having unique and uncommon passwords is essential for securing the NMS, often a user forgets the password. If this happens, remember the following:

CiscoWorks cannot recover forgotten passwords for a user. Therefore, have the CiscoWorks system administrator (admin) change the password or delete it and then add the user again.

The user account admin is reserved and cannot be deleted. If the administrator has changed and forgotten the admin password, contact the Cisco TAC.

### 10.2.3. Collecting Self-Test Information

The Self-Test option, which is found in the Server Configuration -> Diagnostics folder as Self Test, provides a way for the system administrator to verify if the following functions are configured properly:

- The database backup facility is running and scheduled.
- The CMF database can be accessed.
- The platform has enough RAM and swap space allocated to run the CiscoWorks server.
- Name server lookup is working properly.

A self-test may take up to 5 minutes. To create a new self-test information report, click Create. To delete a self-test information report, check on the report box, and then click Delete. To display a self-test information report, click on the report name. To refresh this information, click Update.

#### Tip: Upgrading

When upgrading CD-One, the self-tests are saved and can still be viewed.

Note: For troubleshooting purposes, Cisco TAC is more interested in the information that can be obtained from the Collect Server Info menu item.

### 10.2.4. Collecting Information on the Server

A system administrator, network administrator, or network operator can gather troubleshooting information about the status of the server using this option, which is found under the Server Configuration -> Diagnostics -> Collect Server Info menu item.

To create a new report, click Create, then select the sections you want to report on (available from CiscoWorks CMF 2.2). The report may take up to 5 minutes to generate. Click Update to refresh the display and view any new reports created. The new report appears in the Reports history list.

To view a report, simply select a report from the Reports history list. The report shows information about the product database, the operating system, disk utilization statistics, etc.

A command-line script is also available at:

```
<install dir>/CSCOpX/bin/collect.info.
```



If you run the command through the CiscoWorks desktop, data is located at

`<install_directory>/CSCOpX/htdocs/collect.`

### 10.2.5. CiscoWorks Daemon Manager

Numerous runtime services are installed with CD One. One extremely important process is the Daemon Manager. The Daemon Manager, the master of all others, controls the starting and stopping of these processes.

To view a list of active services currently running on Windows, type `net start`.

To aid in troubleshooting or to stop all processes and have all processes release their resources, the system administrator needs to stop the main process controller, the Daemon Manager.

#### 10.2.5.1. Windows Environment

To stop the Daemon Manager, type `net stop crmdmgtd` at a DOS prompt.

To start the Daemon Manager, type `net start crmdmgtd` at a DOS prompt.

#### 10.2.5.2. UNIX Environment

To stop the UNIX Daemon Manager, type the command `/etc/init.d/dmgtd stop`.

To start the UNIX Daemon Manager, type the command `/etc/init.d/dmgtd start`.

### 10.2.6. Restoring the CiscoWorks Database

An important task for any system administrator is periodic backups so that if for some reason the database gets corrupted it can be restored.

**Note:** As part of the restoration process, the CiscoWorks processes are shut down and restarted. Make sure jobs are not running any critical tasks. Otherwise, the data might be lost.

Following are the restoration steps for both Windows and UNIX servers.

#### 10.2.6.1. Windows Environment

1. At the command line, make sure you have the correct permissions.
2. Stop all processes: `net stop crmdmgtd`.
3. Restore the database: `<install_directory>\bin\perl <install_directory>\bin\restorebackup.pl [-force] [-s suite][-gen generationNumber] -d backup_directory`

where:

- *suite* is the application to be restored (all by default)
- *force* forces the restore of an old schema
- *gen* allows the selection of backup version

4. Examine the log file in the following location to verify that the database was restored:

`<install_directory>\log\restorebackup.log`

5. Restart the system: `net start crmdmgtd`

**Note:** You cannot restore Windows NT data to a different drive from the drive it was backed up from (that is, restoring D: data to C:). This is documented in bug ID (CSCds74983).

#### 10.2.6.2. UNIX Environment



1. Log in as the supervisor and enter the root password.
2. Stop all processes: `/etc/init.d/dmgtd stop`.
3. Restore the database using the following script: `<install_directory>/bin/perl <install_directory>/bin/restorebackup.pl [-force] [-s suite][--generationNumber] -d backup_directory`  
where:
  - *suite* is the application to be restored (all by default)
  - *force* forces the restore of an old schema
  - *gen* allows the selection of backup version
4. Examine the log file in the following location to verify that the database was restored:  
`/var/adm/CSCOPx/log/restorebackup.log`.
5. Restart the system: `/etc/init.d/dmgtd start`.

#### 10.2.7. Viewing Process Failures

You can check for potential failures of processes running on the CiscoWorks server using this feature, which is found under the Server Configuration -> Diagnostics -> Process Failures menu item.

The Process Failures table provides you with two failure state options:

- *Failed to run*—The process has failed by exiting or sending a failed message.
- *Administrator has shut down the server*—The administrator or another program has shut down the process.

In the Core field, Not applicable means the program is running normally. CORE FILE CREATED means the program is not running normally and the operating system has created a file called a core file. The core file is used to store important data about processes.

The Information field describes what the process is doing. Not applicable means the program is not running normally.

Note: If a process fails, try stopping and restarting the process manually. Go to the Administration -> Process Management folder located in the CiscoWorks server drawer to start or stop processes and view their status.

Note: The stdout, stderr, and event logs (as well as error.log) are very useful here.

#### 10.2.8. ? on Cookies and No Login Screen

This is usually accompanied by a `java.lang.NullPointerException` error in the browser.

Check JRUN Proxy service. For some reason this does not start automatically on non-U.S. English localized systems.

Note: CiscoWorks is supported only on U.S. English and Japanese localized systems.

Note: The stdout, stderr, and event logs (as well as error.log) are very useful here.

#### 10.2.9. It Is Slow

Check DNS.

Recheck DNS.

Check RAM and CPU on the server.

Check browser version.



Check RAM and CPU on the client.

### 10.3. CiscoView

Problems within CiscoView usually stem from one of the following problems:

- No connectivity to the Cisco device
- Wrong or outdated device package
- Wrong SNMP community strings
- Short timeout values for a busy network

It is recommended that you review these areas, turn on CiscoView logging, and review Appendix A in the CiscoView User Guide prior to contacting Cisco. To turn on CiscoView logging, select the Administration -> CiscoView Server folder in the Device Manager drawer. Then select the function Debug Options and Display Log.

Note: Traces are stored in a file called cv.log. Refer to the display for the directory. You can click on View Trace to look at this file or clear this log file.

One of these methods should help resolve your problems in accessing a device using CiscoView.

### 10.4. CiscoWorks Campus Manager

#### 10.4.1. Analyzing the ANI Server

Network Services (commonly called ANI server) provides the discovery of network devices and their components.

The CiscoWorks server provides detailed diagnostic information about the ANI server. To view this information, select Server Configuration -> Diagnostics -> Analyze ANI Server. The diagnostic report includes the following three sections:

- *System Information*—Displays the host computer on which the ANI server is installed, memory available on the host computer, operating system, and Java version information.
- *Configuration Settings*—Displays contents of the ANIServer.properties file, which details the status of all ANI settings
- *Raw Analysis*—Displays details about the ANI service modules and their dependencies, supported devices, and contents of ANI database tables

You can check this report to verify that the ANI server is configured on the appropriate host computer and all properties are set correctly. This information can also help the Cisco TAC in resolving unusual ANI server-related errors. You can send this information directly to a Cisco TAC representative by using the File -> Send Page feature within your Web browser.

Note: The ANI server must be running to display the ANI Server Analysis report. The ANI server is enabled when CiscoWorks Campus Manager is installed.

#### 10.4.2. Enable Debugging Options

Another feature that can aid in troubleshooting problems with ANI processes is the debugging feature. This feature records detailed information about the discovery process and all interactions between ANI service modules and network devices. To enable debugging on the ANI server, select Setup -> ANI Server Admin -> Debugging Options from the Server Configuration drawer. You can enable debugging for a specific service or device module.



When you enable tracing for a specific service module (that is, SNMP, ATM, etc.), interactions between the network and that service module are logged. If you enable tracing for a device module (that is, devices.C5K, devices.Router, and so on), only interactions between ANI and those device types in your network are recorded. Refer to the online help for a complete description of each of the ANI service modules.

In addition, you can check the Show detailed messages while tracing the option to show messages from the code being invoked between the ANI service modules and their dependencies. This adds a much finer level of granularity to the trace.

**Note:** This option can create significantly more output to the log file, and it should be enabled only if requested by a Cisco representative.

Check the Record trace messages in the log file option and specify a path and filename in order to save and view all recorded trace messages in a file. When the number of logged messages reaches the maximum, the contents are moved and saved to a backup file called <yourfile>\_backup, where yourfile is the file name you assigned to the log file. The backup file is overwritten the next time the log file reaches its maximum. (There are never more than two log files in the directory, the backup and the current log file.)

**Note:** The debugging feature requires a detailed understanding of ANI service modules, and is usually used only with the assistance of a TAC representative.

#### 10.4.3. Global Discovery Checklist

If some devices are not initially discovered by the ANI server when you first install CiscoWorks Campus Manager, use the following checklist to confirm that all information and settings are correct:

- Verify that there is connectivity between the NMS and the device. Try performing pings on the device to confirm that it can be reached from the CiscoWork server.
- Confirm that Cisco Discovery Protocol is enabled on the device (ILMI for ATM devices). Check the Cisco Discovery Protocol neighbor table of the device and neighbor devices to ensure that Cisco Discovery Protocol is working properly.
- Confirm that each Cisco IOS device has a unique sysName variable assigned.
- Make sure that at least one valid seed device has been defined under Setup -> ANI Server Admin -> Discovery Settings from the Server Configuration drawer. If a particular device is not being discovered, confirm that no filters or router boundaries are excluding the device from being discovered.
- Verify that SNMP read and write community strings are defined on the device and that they match the values entered under Setup -> ANI Server Admin -> SNMP Settings from the Server Configuration drawer.
- If the ANI server times out when trying to access a device, increase the SNMP timeout values for that device under the ANI server SNMP settings.

#### 10.4.4. User and Host Discovery Checklist

If end stations or usernames are not initially discovered and displayed in the User Tracking table when you first install CiscoWorks Campus Manager, use the following checklist to confirm that all information and settings are correct:

- Verify that the end station is online and that there is connectivity between the NMS and the end station. Try performing pings to the end station to confirm that it can be reached from the CiscoWork server.



- Confirm that the ANI server has already discovered the network device to which the end station is attached. You can view the associated domain in topology services to see if the device has been discovered. If the device has not been discovered, refer to the Global Discovery Checklist on the previous page to help resolve the problem.
- If usernames are not being retrieved, verify that the User Name Collection options are correct under Setup -> ANI Server Admin -> User and Host Acquisition from the Server Configuration drawer. Also confirm that the necessary scripts have been installed on the server or hosts from which user-names should be retrieved (UTLite for NT and Novell servers, rusersd for UNIX hosts).

#### 10.4.5. Path-Analysis Trace Checklist

If you have trouble successfully tracing the path between two endpoints using the Path Analysis tool, use the following checklist to confirm that all information and settings are correct:

- Verify that both endpoints are online and accessible from the NMS. Try performing pings to each endpoint to confirm that it can be reached from the CiscoWorks server.
- Confirm that global discovery and user and host acquisition have occurred. You can view the associated domain in topology services to confirm that network devices have been discovered, and view entries in the User Tracking table to verify that users and hosts have been discovered (end stations must have been discovered within the past 48 hours). If network devices or end stations are missing, use the checklists on the previous two pages to help troubleshoot the problem.
- Check the entries in the Subnet Mapping table by selecting Edit -> Subnet Mapping. Verify that all VLAN and emulated LAN (ELAN)-to-subnet mappings are correct, and that there is a separate subnet entry for each standalone subnet.
- Make sure that source routing is enabled on all Cisco IOS devices along the specified path.
- Security issues might prevent CiscoWorks Campus Manager from retrieving information from devices along the specified route. To help minimize these issues, make the CiscoWorks server a trusted host in your Web browser.

#### 10.5. Discovery Never Stops

One cause for this in non-English speaking countries is the use of special characters such as —, ø, and å in configurations. Configurations should use only the letters defined in the 7-bit ASCII codeset for CiscoWorks. Thus you should check host names, interface descriptions, or any other parts of the configuration that may contain free text.

### 10.6. CiscoWorks Resource Manager Essentials

#### 10.6.1. Restarting the Server

CiscoWorks RME relies on the Daemon Manager to control all processes and the DbServer process to control the Essentials database. Occasionally, the Daemon Manager might stop running. If this happens, you can try restarting the server from the command line.

To restart the Daemon Manager on an NT server, enter the following commands from a CLI:

```
net stop crmdmgt  
net start crmdmgt
```

To restart the Daemon Manager on a UNIX server, enter the following commands from a CLI:



```
/etc/init.d/dmgttd stop
```

```
/etc/init.d/dmgttd start
```

### 10.6.2. Managing Processes

If the server is up but you are having problems running a specific function within CiscoWorks RME, you can use the tasks within the Server Configuration drawer to check for process failures. If there is a problem, you can stop and restart individual processes without having to restart the entire server.

To view process failures and stop and restart processes, do the following:

1. First, access the server from a client and select Diagnostics -> Process Failures from the Server Configuration drawer. If any processes have failed, a report displays the process name and the date and time that it failed.
2. If a process has stopped, select Administration -> Process Management -> Start Process. Select the process from the pull-down menu, and click “Start” to restart it.

If no processes have failed but you are still having problems with a particular function in CiscoWorks RME, try stopping and restarting the associated process. Refer to the online help for a detailed description of each Essentials process and its interdependencies with other processes.

### 10.6.3. Inventory Checklist

If devices are not initially detected by CiscoWorks RME when you try to add them manually or import them from another NMS, use the following checklist to confirm that all information is correct:

- To determine the status of all devices that have been manually added or imported, select Administration -> Inventory -> Import Status from the Resource Manager Essentials drawer. Click on the links to view details about which devices are not responding or have errors.
- Verify that SNMP read community strings are defined on the device and that they match the values entered in the Essentials inventory. Use Administration > Inventory > Check Device Attributes.
- Confirm that a valid IP address or host name is entered in the Essentials inventory for each device.
- If a host name is entered, make sure that a valid domain name is included (if necessary) and that the host name is entered correctly in DNS. If the host name fails, try using an IP address.
- Try performing a ping to the device to confirm that it can be reached from the Essentials server.
- If Essentials times out when trying to access a device, increase SNMP timeout values under Administration -> System Configuration -> SNMP Tab in the Resource Manager Essentials drawer.
- If importing from a remote NMS (UNIX only), confirm that the remote shell daemon is running on the remote host and that Essentials has access to remote databases.
- If importing from a local NMS, verify that the NMS is running.

### 10.6.4. Inventory Collection Status

If inventory reports do not appear to be up-to-date, you can use the Scan History Report to determine the last time that inventory information was updated in CiscoWorks RME.

- Select Inventory -> Scan History from the Resource Manager Essentials drawer. This shows the last date and time that inventory information was checked on devices, the number of devices scanned, and how long the scan took. If there is no scan history displayed, then inventory collection might not be scheduled.





- If the number of devices scanned does not equal the number of devices that should be in inventory, then Essentials might not be able to access some devices. Confirm that SNMP read community strings have not changed, and that they still match on the devices and in the Essentials inventory. You can also use Availability reports to determine if any devices are offline.
- Verify that Inventory Poller or Schedule Collection are enabled. Remember that it is recommended that you use Inventory Poller more frequently to detect changes in inventory.
- If you need up-to-date information for reports immediately, select Administration -> Inventory -> Update Inventory from the Resource Manager Essentials drawer.

#### 10.6.5. Syslog Collector Status

If no syslog messages are displaying for some or all devices in the Syslog Analysis reports, you can check the Syslog Collector status to confirm that the Syslog Analyzer Collector process is running periodically.

- Select Administration -> Syslog Analysis -> Syslog Collector Status from the Resource Manager Essentials drawer. This displays the last date and time that information in the Syslog Analysis database was updated, and the number of messages processed. It should be updated every 5–10 minutes. If not, something is wrong with the Syslog Analyzer process or the configuration of a remote SAC. Refer to the RME online help for detailed procedures on how to correctly install a remote SAC.
- Check the status of the Syslog Analyzer process under Server Configuration -> Administration -> Process Management -> Process Status. If it has failed, stop and restart it.
- Verify that all devices are configured correctly to log syslog messages to the Essentials server or a remote SAC.
- Check the Syslog Analysis storage options to make sure that messages are not being purged immediately from the Essentials syslog database. If messages are being stored for only 1–2 days, there may not be any data in the database.

#### 10.6.6. Configuration Archive Status

If you know that there have been changes to device configurations but the files in the CiscoWorks RME configuration archive do not appear to be the most current, you can check the status of the Configuration Archive to determine when it was last updated.

- Select Administration -> Configuration Management -> Archive Status from the Resource Manager Essentials drawer.
- Click on the links under both the Running and Startup Configuration tabs to view details about any failures. An explanation is given for any devices that cannot be accessed or are not responding. Cisco Catalyst 5000 devices with sub-modules are listed under Partial Failure because Essentials can archive only the configuration file for the Supervisor Engine module.
- If any devices are listed under Failed, verify that the read and write community strings and Telnet and enable passwords are correct in the Essentials inventory. Essentials uses Telnet to gather module configurations for Cisco Catalyst and startup configurations from Cisco IOS devices.
- If TACACS authentication is configured on devices, make sure that the TACACS username and password are entered in the Essentials inventory for each device. Also, if you use custom TACACS login and password prompts, Configuration Management may not be able to perform a Telnet to the device. To resolve this, edit the TacacsPrompts.ini file to make your prompts recognizable. Refer to online help for the detailed procedure.



- Verify that preferences under Administration -> Configuration Management -> General Setup under the Resource Manager Essentials drawer are set to retrieve configuration files often enough for your network management needs. Remember that the syslog message and SNMP poller options work only for Cisco IOS devices. Also confirm that configuration files are being stored long enough to support troubleshooting.
- If you need updated configuration files immediately and do not want to wait for the next scheduled collection, select Configuration Management -> Update Archive under the Resource Manager Essentials drawer.

#### 10.6.7. Job Management Checklist

When executing a Software Management, NetConfig, or Config Editor job, it is very important to make sure that all device requirements are met and job properties are set correctly. It is very frustrating to schedule a job overnight and come back the next day to find out it has failed. Review the following guidelines to help avoid a job failure:

- Confirm that all community strings, Telnet and enable passwords, and TACACS usernames and passwords are correct in inventory. Both Software Management and Configuration Management require full access to the device in order to upload software images and configuration files.
- Verify that all devices are online prior to scheduling a job.
- Ensure that an appropriate device order is set if devices are dependant on one another for access. For example, if Device A is required to get to Device B, perform the update in the reverse order and update B first.
- If using Config Editor or a custom NetConfig template to edit configuration files, ensure that all entries are valid configuration commands. Essentials does not check ad hoc commands for validity.
- Always select job options to synchronize updates with the Essentials database to ensure that information in Essentials is up-to-date.
- Before scheduling software-management jobs, verify that settings under Administration -> Software Management -> Edit Preferences in the Resource Manager Essentials drawer are correct. Make sure that the Include CCO/ Cisco.comImages option is checked if you want the most current images available from CCO/ Cisco.com to be listed when performing an upgrade.
- If you are performing a software upgrade and the Reboot Immediately option is selected, make sure that all Cisco IOS devices are configured with the snmp-server system shutdown command.

Note: You can use the Administration -> Job Management screen under the Server Configuration drawer to forceably stop jobs as well as unlock resources.

#### 10.6.8. Availability Report Checklist

If no information is displaying in Availability reports or some devices are missing, use the following checklist to help determine the problem:

- Verify that devices are included in the view selected under Availability polling options.
- Confirm that SNMP timeouts are set high enough so that Essentials does not time out when trying to retrieve availability information.
- Make sure that no polling options are turned off, unless you do not want that information.



## 11. References

### 11.1. Books

#### 11.1.1. *Performance and Fault Management*—Cisco Press. ISBN: 1578701805

The key to efficiently running networks is proper management. Performance management measures the level of operation of a network, ensures that it maintains an acceptable level, and provides information for expanding the network. Fault management detects, logs, and notifies users of network problems and automatically fixes many problems to keep the network running effectively. These two management concepts go hand-in-hand by defining the capability of a network, and then identifying and repairing problems. This technology is complex, and even experienced networking professionals struggle with these concepts and look for quantity instruction on how to implement them. *Performance and Fault Management* is a comprehensive guide to designing and implementing effective solutions that will measure and report the effectiveness of Cisco networks.

#### 11.1.2. *Cisco Enterprise Management Solutions: Volume 1*—Cisco Press. ISBN 1587050064

CiscoWorks is the latest product family offering from Cisco® designed to increase user access to information on the performance of a network and ease management tasks. CiscoWorks (RME), upon which the bulk of *Cisco Enterprise Management Solutions, Volume I* is based, provides users with the tools they need to perform daily management tasks. As with any network management solution, users need to be well versed in the application of the features of each component in order to gain maximum performance benefits. To this end, Cisco offers the Cisco Enterprise Management Solutions (EMS) course that explains routed and switched network management solutions.

*Cisco Enterprise Management Solutions, Volume I* provides readers with an excellent self-study solution to help them master the intricacies of managing Cisco networks. It begins with an overview of network management as a concept, followed by how industry standards such as SNMP, MIBs, and RMON are implemented. Product installation and server requirements are also discussed. It then moves on to cover CiscoWorks RME and the included component applications in detail. Inventory, device configuration, and software image management are all discussed in depth, as well as change audit services, syslog analysis, and reporting with availability manager. book ends with coverage of Cisco management connection and CiscoWorks RME tools and a discussion about troubleshooting common problems associated with the use of CiscoWorks RME.

#### 11.1.3. *Hardening Cisco Routers*—O'Reilly & Associates. ISBN 0596001665

As a network administrator, auditor, or architect, you know the importance of securing your network and finding security solutions you can implement quickly. This succinct book departs from other security literature by focusing exclusively on ways to secure Cisco routers, rather than the entire network. The rationale is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. *Hardening Cisco Routers* is a reference for protecting the protectors. Included are the following topics:

- The importance of router security and where routers fit into an overall security plan
- Different router configurations for various versions of Cisco IOS Software
- Standard ways to access a Cisco router and the security implications of each

Password and privilege levels in Cisco routers

- Authentication, authorization, and accounting (AAA) control
- Router warning banner use (as recommended by the FBI)



- Unnecessary protocols and services commonly run on Cisco routers
- SNMP security
- Antispoofing
- Protocol security for Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), NTP, and Border Gateway Protocol (BGP)
- Logging violations
- Incident response
- Physical security

Written by Thomas Akin, an experienced Certified Information Systems Security Professional (CISSP) and Certified Cisco Academic Instructor (CCAI), the book is well organized, emphasizing practicality and a hands-on approach. At the end of each chapter, Akin includes a checklist that summarizes the hardening techniques discussed in the chapter. The checklists help you double-check the configurations you have been instructed to make, and serve as quick references for future security procedures.

Concise and to the point, *Hardening Cisco Routers* supplies you with all the tools necessary to turn a potential vulnerability into a strength. In an area that is otherwise poorly documented, this is the one book that will help you make your Cisco routers dependable.

## 11.2. Web Sites

### 11.2.1. Simple Network Management Protocol

[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/snmp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm)

### 11.2.2. SNMP Notifications

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800ca66b.html#1000906](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66b.html#1000906)

### 11.2.3. SNMP Examples

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800ca66b.html#1001599](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66b.html#1001599)

### 11.2.4. Supported MIBs and RFCs

Cisco's implementation of SNMP supports all MIB II variables (as described in RFC 1213) and SNMP traps (as described in RFC 1215). Cisco provides its own private MIB extensions with every system. One of the sets of MIB objects provided is the Cisco Chassis MIB that enables the SNMP manager to gather data on system card descriptions, serial numbers, hardware and software revision levels, and slot locations. Another set is the Entity MIB (RFC 2037), which describes the logical resources, physical resources, and logical-to-physical mappings of devices managed by a single SNMP agent. The Entity MIB also records the time of the last modification to any object in the Entity MIB and sends out a trap when any object is modified. There are other MIBs for ATM, ISDN, voice, etc.

For lists of supported MIBs by platform and downloadable MIB files, send an e-mail to: [mii@external.cisco.com](mailto:mii@external.cisco.com)

The MIBs In Images (MII) tool is on Cisco.com at <http://www.cisco.com/go/mibs>. However, the e-mail interface is more accurate.



### 11.2.5. Remote Monitoring

[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/rmon.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm)

### 11.2.13. Overview of CiscoWorks

#### 11.2.13.1. CiscoWorks Resource Manager Essentials

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/>

#### 11.2.13.2. CiscoWorks Campus Manager

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/camp\\_mgr/camp\\_3x/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/camp_mgr/camp_3x/index.htm)

#### 11.2.13.3. Service Level Manager Product Overview

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/slm/uslm/overview.htm>

#### 11.2.13.4. CiscoWorks ACL Manager Overview

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/fam\\_prod/acl\\_mgr/aclm\\_1\\_x/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/fam_prod/acl_mgr/aclm_1_x/index.htm)

#### 11.2.13.5. Introduction to CiscoWorks Device Fault Manager

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/>

#### 11.2.13.6. Overview of CiscoWorks Internetwork Performance Monitor

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ipmcw2k/>

#### 11.2.13.7. CD-One CiscoView

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_d/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/index.htm)

#### 11.2.13.8. Discovering Preferred Management Addresses for Routers

[http://www.cisco.com/warp/public/cc/pd/wr2k/cpmn/prodlit/wk2ke\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/wr2k/cpmn/prodlit/wk2ke_wp.htm)

### 11.2.15. A Good Router Monitoring Task List

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun\\_c/fcprt3/fcmonitr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcmonitr.htm)

## 12. Appendix A—The Network Discovery Process Explained

This section describes how the Asynchronous Network Interface (ANI) uses standard Management Information Bases (MIBs) to perform network discovery.



## 12.1. Neighbor Discovery

ANI network discovery begins with an initial seed device or devices provided by the user and proceeds to discover an entire network using neighbor discovery protocols. Most Cisco devices implement one or more of the standard neighbor discovery protocols: Cisco Discovery Protocol or Integrated Local Management Interface (ILMI). Cisco Discovery Protocol is used on Ethernet networks. ATM networks use a different protocol, ILMI, to report neighbors.

ANI sends Simple Network Management Protocol (SNMP) requests to a device to query its neighbor table. The resulting neighbor entries are processed to see if the neighbor is a known device or a new, undiscovered device. New neighbors are queued for later processing by an available discovery thread.

ANI discovery is designed to be fast and efficient. Discovery is highly multithreaded, and the number of independent threads can be configured with the property `ThreadPool.background` in the `ANIServer.conf` (note: case sensitive) file. If the number of threads is set to one, discovery is single threaded and serial.

### 12.1.1. Controlling Discovery

It is often desirable or necessary to limit discovery to a subset of the larger overall network. The desire may be to limit discovery to a geographical region, IP address boundary, or region of management responsibility.

One of the simplest ways to limit discovery is to disable Cisco Discovery Protocol on edge devices. This causes discovery to stop just before reaching the edge device. Because the edge device itself is not running Cisco Discovery Protocol, it too is excluded from the discovered network.

Discovery can also be limited by:

- IP address
- VTP domain

IP address and VTP domain boundaries are configured by application properties. Users can set up a list of addresses or domains to include or exclude. There are separate configurations for addresses and domains. They can be set to either include all listed items but no others, or to exclude only the listed items.

For example,

```
Discovery.domains.exclude=test
Discovery.subnets.include=172.20.[1-5].*
```

This allows discovery of all devices contained in the subnet `172.20.1-5.*` except for those in the VTP domain “test.”

**Note:** A device outside discovery boundaries will still be discovered but discovery will not continue onto its neighbors. Neighbor entries can sometimes be inconsistent because of device agent bugs, different aging periods for cache entries, or for other reasons. The property `Topology.conflictIntersect` has values on and off. This controls if topology should use the intersection or union of neighbor entries. By default, `conflictIntersect` is set to off and topology uses a permissive union algorithm. The union algorithm creates a topology link even if the Cisco Discovery Protocol or ILMI neighbor information is inconsistent between the devices. When `conflictIntersect` is set to on, the Cisco Discovery Protocol or ILMI neighbor entries must be symmetric for a topology link to be created. When entries are not symmetric, a warning message is generated that the Cisco Discovery Protocol information is inconsistent.



## 12.2. Cisco Discovery Protocol Neighbor Discovery

Cisco Discovery Protocol is a proprietary Cisco protocol and is not any sort of public standard. Certain of Cisco's partners have chosen to implement Cisco Discovery Protocol on their devices. For example, NetScout probes implement Cisco Discovery Protocol. To run Cisco Discovery Protocol, a device must have a SNMP-reachable IP address. Also, Cisco Discovery Protocol must be enabled and running on a device for discovery to work.

The Cisco Discovery Protocol is described in internal Cisco documentation and the corresponding management MIB is CISCO-CDP-MIB.

### 12.2.1. The Cisco Discovery Protocol MIB

ANI reads the CdpCacheEntry table from CISCO-CDP-MIB on a discovered device.

The columns of the table fetched by ANI are given in Table 9:

Table 9 Columns of the Table Fetched by ANI

Name	Type	Description
cdpCacheIfIndex	Integer	ifIndex of the local devices connected port
cdpCacheAddressType	Integer	Media type
cdpCacheAddress	IP address	Neighbors' IP address
cdpCacheDeviceId	String	Neighbors' device ID
cdpCacheDevicePort	String	Neighbors' port ifName or ifDescr
cdpCachePlatform	String	Neighbors' hardware platform name
cdpCacheCapabilities	String	An enumeration identifying the class of device (router, switch, etc.)

These variables provide the IP address and device ID of the neighbor, the name of neighbor's port the link is connected to, and the ifIndex of the link port on the local device. A physical network link exists between two devices for each Cisco Discovery Protocol cache entry.

### 12.2.2. Device ID

Cisco Discovery Protocol uses an identifier known as the device ID (cdpCacheDeviceId in the Cisco Discovery Protocol MIB) to uniquely identify each device. There is currently no standard format for the device ID, and various platforms implement it differently. Cisco IOS® devices always use just the device sysName MIB variable. Ethernet switches typically use a combination of Media Access Control (MAC) address and sysName.

A recent addition to the Cisco Discovery Protocol MIB and implemented by newer devices is the variable cdpGlobalDeviceId. This variable represents the device ID sent by a device to its neighbors in Cisco Discovery Protocol advertisements. For older devices that do not implement this variable, ANI computes the device ID using device-specific algorithms.



### 12.2.3. Device Port

The devicePort is the name of the remote port on the neighbor. The format of cdpCacheDevicePort has not been standardized. Typically, devices report either ifName or ifDescr for the port name.

### 12.2.4. Address

The address is a IP address of the neighbor. Any valid IP address for the device can be used, whether or not it is assigned to this interface. The IP address must be SNMP reachable.

Some devices report unnumbered interfaces (0.0.0.0) for the address field. Although this is not in conformance with the Cisco Discovery Protocol specification, ANI attempts to look up the neighbor by device ID.

### 12.2.5. Cisco Discovery Protocol Example

The following ANI log file shows an example of Cisco Discovery Protocol discovery. Each Cisco Discovery Protocol entry reports the neighbor's IP address, device ID, and link information. The port connections of a link are displayed in the log as remote port (cdpCacheDevicePort) to local ifIndex.

```
53:32 EvalTask-background-01 CoreSMFGetCDPCache: reading CDP cache on 10.29.2.55
53:33 EvalTask-background-01 CDPCacheEntry: 10.29.3.55 nms-2610a Ethernet0/0-to-45
53:33 EvalTask-background-01 CDPCacheEntry: 10.29.2.56 0074844072/1-2-to-127
53:33 EvalTask-background-01 CDPCacheEntry: 10.29.2.1 nms-7507a ATM4/ 0.2-to-127
53:33 EvalTask-background-01 CDPCacheEntry: 10.29.3.1 nms-7507a ATM4/ 0.3-to-127
53:33 EvalTask-background-01 CDPCacheEntry: 10.29.2.2 nms-5500a-rsm Vlan2-to-381
53:33 EvalTask-background-01 CDPCacheEntry: 10.29.8.1 nms-2515a TokenRing0-to-384
?
54:30 EvalTask-background-04 CoreVladSMFGetCDPCache: reading CDP cache on 10.29.3.55
54:31 EvalTask-background-04 CDPCacheEntry: 10.29.2.55 069031368 9/5-to-1
```

Because discovery is multithreaded, a log typically contains messages from interleaved tasks. To correctly read the log, you must follow the entries for a single EvalTask number.

#### 12.2.5.1. Computing Topology

Creating a topology based upon Cisco Discovery Protocol involves matching both sides of the Cisco Discovery Protocol link information and looking up the ports.

Things to check if Cisco Discovery Protocol neighbors are not being discovered or links are missing follow:

- Cisco Discovery Protocol is enabled on the device
- For Cisco IOS devices, that sysName has been configured to be unique

The Cisco Discovery Protocol information reported by the command-line interface (CLI) is not always identical to that reported via SNMP. There have been many agent bugs where not all Cisco Discovery Protocol neighbors are reported by the SNMP device agent. Always walk the Cisco Discovery Protocol MIB to make sure that the known neighbors appear.

The cdpCache table can be walked using most SNMP walk utilities.





### 12.3. ILMI Neighbor Discovery

Cisco ATM devices exchange information with neighboring ATM devices using the standard ILMI defined by the ATM Forum. This is the mechanism by which ATM devices discover their neighboring ATM devices. In order for this neighbor discovery to take place, ILMI must be enabled on the interfaces between which the ATM devices are connected.

Certain Cisco devices enable ILMI by default on all interfaces, whereas others require explicit configuration.

When a device discovers its ATM neighbors using ILMI, it makes that information available using the ATM interface configuration table in the ATM-MIB (often referred to as the “AtoM-MIB”). The ATM-MIB is a standard MIB defined in RFC 1695, and is accessible using SNMP. The ATM-MIB interface configuration table provides, for each local ATM interface, the SNMP reachable IP address of the neighboring ATM device (if any) and the name of the interface on the remote device to which the local interface is connected.

For User-Network Interface (UNI) ATM interfaces, ILMI also provides a way for the “user side” to report its ATM addresses to the “network side.” A select few Cisco devices (such as the Cisco LightStream® 1010) make this UNI address registration information available using the Cisco proprietary CISCO-ATM-ADDR-MIB, which is accessible on those devices using SNMP. This MIB provides, for each local UNI interface, the set of ATM addresses that have been registered on that interface.

In order for ANI to access ATM neighbor information from an ATM device, the device must have ILMI enabled on its ATM interfaces, its neighbors must also have ILMI enabled on their ATM interfaces, and the device must have an SNMP-reachable IP address.

#### 12.3.1. The ATM-MIB

ANI reads part of the ATM interface configuration table from the ATM-MIB on a discovered device. The columns of the table fetched by ANI are given in Table 10.

Table 10 Columns of the Table Fetched by ANI

Name	Type	Description
atmInterfaceMyNeighborIfName	String	The ifName of the interface on the neighboring device to which the local interface is connected
atmInterfaceMyNeighborIpAddress	String	IP address of the neighboring device to which the local interface is connected

The atmInterfaceMyNeighborIpAddress address is an IP address that can be used to communicate with the neighboring device using SNMP, or 0.0.0.0 if there is no such IP address on the neighboring device.

**Note:** If you get 0.0.0.0 for ILMI neighbor information, you will need to do a shut/no shut on the affected interface to get ILMI information to renegotiate.

Both of these columns are indexed by the ifIndex of the local interface to which the information applies.

These variables provide the IP address of the neighbor, the name of neighbor’s interface that the link is connected to, and the ifIndex of the link interface on the local device.



An entry in the table whose local ifIndex specifies a physical port indicates that there is a physical link between the device and its neighbor.

An entry in the table whose local ifIndex specifies a subinterface of type atmLogical indicates that there is a VP tunnel between the device and its neighbor.

Note: ANI ignores any entry in this table that does not contain a valid host IP address for the atmInterfaceMyNeighborIpAddress. This is because such entries are for links to devices that are not SNMP manageable, and as a result, ANI cannot resolve the links.

### 12.3.2. The CISCO-ATM-ADDR-MIB

ANI reads the ciscoAtmIfAdminAddrTable in the CISCO-ATM-ADDR-MIB on the devices that support that MIB. The columns of the table fetched by ANI are given in Table 11.

Table 11 Columns of the Table Fetched by ANI

Name	Type	Description
ciscoAtmIfAdminAddrAddress	String	A registered ATM address
ciscoAtmIfAdminAddrRowStatus	Integer	The SNMP RowStatus of the entry in the UNI registration table

Both of these columns are indexed by the ifIndex of the local interface to which the information applies.

These variables provide, for each local UNI interface, the set of ATM addresses that are registered on that interface.

#### 12.3.2.1. ILMI Neighbor Example:

The following ANI log file shows an example of ILMI neighbor discovery.

Each entry reports an ILMI neighbor acquired from the ATM-MIB of a device. For each entry, the local ifIndex is displayed along with the neighbor IP address and neighbor ifName. Each entry also contains the items “null” and “0.” These are dummy placeholders that are resolved later in the discovery, and can be ignored in these log entries.

The following log entries are for physical ATM links:

```
14:45:47 EvalTask-background-12 ani CoreSMFGetIlmiNeighbors: Adding new neighbor
(10,none,0,172.20.4.52,ATM1) on 172.10.126.118
14:45:47 EvalTask-background-12 ani CoreSMFGetIlmiNeighbors: Adding new neighbor
(11,none,0,172.20.4.88,ATM3/0) on 172.10.126.118
14:45:47 EvalTask-background-12 ani CoreSMFGetIlmiNeighbors: Adding new neighbor
(18,none,0,172.20.4.10,ATM4/0/0) on 172.10.126.118
```

The following log entries are for virtual-path tunnels. Note the subinterface numbers on the remote ifNames:

```
14:47:17 EvalTask3-05 ani CoreSMFGetIlmiNeighbors: Adding new neighbor
(19,none,0,172.20.4.11,ATM1/0/1.99) on 172.10.126.118
14:47:17 EvalTask3-05 ani CoreSMFGetIlmiNeighbors: Adding new neighbor
(28,none,0,172.20.4.11,ATM3/1/1.90) on 172.10.126.118
```



```
14:47:17 EvalTask3-05 ani CoreSMFGetIlmiNeighbors: Adding new neighbor  
(29,none,0,172.20.4.11,ATM3/1/1.91) on 172.10.126.118
```

The following entries are acquired from the CISCO-ATM-ADDR-MIB. Each entry contains the ifName of the local interface to which the entry applies and the registered ATM address on that interface. Note that several ATM addresses can be registered on a single interface.

```
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM9/0/ 3,4700790000000000000000000000a03e00000100)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM9/0/ 3,47009181000000000e0fe4b950100e01454c07901)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM9/0/ 3,47009181000000000e0fe4b950100e01454c07a01)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM9/0/ 3,47009181000000000e0fe4b950100e01454c07b00)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM11/0/ 2,47009181000000000e0fe4b950100e0fe4b912100)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM11/0/ 2,47009181000000000e0fe4b950100e0fe4b912200)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM13/0/ 0,4700790000000000000000000000a03e00000100)  
14:45:49 EvalTask-background-12 ani LS1010TopoSMFGetIlmiRegistrations: Adding new ILMI  
registration (ATM13/0/ 0,47009181000000000e0fe4b950100e0fe4b950500)
```

**Note:** Because discovery is multithreaded, a log typically contains a message from interleaved tasks. To correctly read the log, you must follow the entries for a single EvalTask number.

#### 12.3.2.2. Computing Topology

ILMI topology computation takes place in two parts.

The first part of the computation is to calculate the set of ATM links in the network using ILMI information. This set of links includes both physical ATM links and virtual-path tunnels.

The second part of the computation is to determine the set of ATM fabrics given the switches and ATM links in the network.

#### 12.3.2.3. Computing ATM Links

ANI can calculate three types of ATM links, depending on the information it has available.

- *Full*—A full ATM link is the best-case scenario where an entry in the ATM interface configuration table of a device indicates the ifIndex of a local interface, plus both the valid IP address of a discovered device and a known interface name on that device. This allows ANI to connect each end of the link to a discovered interface on a discovered device.
- *Partial*—A partial ATM link represents the case in which an entry in the ATM interface configuration table of a device indicates the ifIndex of a local interface, but the IP address of an unknown or unreachable device. Therefore, ANI does not know the remote interface name specified in the entry. This means that ANI can connect only one end of the link to a discovered interface—the local interface—while the remote side of the link dangles, associated with an IP address, but not with any particular remote interface.



- *Unknown UNI*—An unknown UNI link represents the case in which there are no ATM interface configuration table entries for a local interface, but the UNI address registration table shows registered ATM addresses on that interface. In this case, it can be inferred that there is an ATM link there, but probably one that is connected to a pure ATM device that has no IP addresses. In this case, ANI creates an “unknown UNI” link where one end is connected to a discovered interface—the local interface—while, instead of a remote side of the link, there is simply a set of registered ATM addresses.

**Note:** It is possible for an interface to have both ATM interface configuration table entries and UNI address registration table entries. In these cases, ANI constructs full or partial links as described previously, and then associates the registered ATM addresses with those links. ANI does not create unknown UNI links when there are valid ATM interface configuration table entries for a local interface.

ANI requires ILMI information from only one device, or one side of the link, in order to create an ATM link. If ANI discovers information about the same link from two different devices, one on each side of the link, it uses the information that seems to be more complete. Information that generates a full link always takes precedence over information that generates a partial link.

ANI does not create an ATM link if it is in conflict with another link computed on the same discovery. Two ATM links are in conflict if each is connected to the same port on one side but different ports on the other side.

ANI creates an ATM link if it is in conflict with another link that was computed on a previous discovery. In this case, the new link displaces the old link, and ANI deletes the old link.

#### 12.3.2.4. Computing ATM Links Examples

The following log entry indicates that ANI discovered a full ATM link. The link contains the IP addresses and interface names from both sides of the link. Both interfaces are discovered, known interfaces.

```
13:47:39 Discovery ani TopoSMFGenerateIlmiTopology: Found new link (full,(172.20.4.9,ATM0/0/0),(172.20.4.11,ATM1/0/1,))
```

The following log entries indicate that ANI discovered a partial ATM link. The link contains the IP addresses and interface names from both sides of the link. However, only the first interface name is known. The interface name on the remote device has not been discovered. This can be because the remote device is unreachable or unknown, or it could be because of SNMP timeouts.

**Note:** The link entry is preceded by a log entry that indicates that ANI does not know the interface indicated by the remote interface name.

```
13:47:40 Discovery ani TopoSMFGenerateIlmiTopology: Cannot find remote interface ATM4/0 on device 172.20.4.21
```

```
13:47:40 Discovery ani TopoSMFGenerateIlmiTopology: Found new link (partial,(172.20.4.8,ATM0/1/0),(172.20.4.21,ATM4/0,))
```

The following log entries indicate an unknown UNI link. The link contains the local IP address and interface name, plus one of the registered ATM addresses.

```
13:47:41 Discovery ani TopoSMFGenerateIlmiTopology: Creating dummy neighbor for ATM0/0/0
13:47:41 Discovery ani TopoSMFGenerateIlmiTopology: Correlating ILMI registration (ATM0/0/0,4700918100000000e01e50fd0100107b01422000) with ILMI neighbor (0,ATM0/0/0,0,none,none)
```



```
13:47:41 Discovery ani TopoSMFGenerateIlmiTopology: Found new link
(unknownAtm,(172.20.23.108,ATM0/0 / 0),4700918100000000e01e50fd0100107b01422000)
```

The following is an example of the discovery ignoring duplicate link information from one side of the link because it contains less information than was discovered from the other side of the link.

```
13:47:40 Discovery ani TopoSMFGenerateIlmiTopology: Found new link (full,(172.20.4.14,ATM10/
0),(172.20.4.15,ATM10/0/0,)) again with less information - ignoring
```

The following is an example of the discovery replacing link information from one side of a link with information from the other side because the newly discovered side contains more information.

```
13:47:40 Discovery ani TopoSMFGenerateIlmiTopology: Found new link
(full,(172.20.97.109,ATM0/1/3),(172.20.57.110,AT1/0/
0,47009181000000001029346b010009772b4d2001)) again with more information - replacing
```

The following is an example of conflicting links discovered on the same pass.

```
13:47:42 Discovery ani WARNING TopoSMFGenerateIlmiTopology: Inconsistent ILMI neighbor
tables: (unknownAtm,(172.20.4.89,ATM9/0/ 3),4700790000000000000000000000a03e00000100) will
be ignored because it conflicts with (full,(172.20.4.48,AT0),(172.20.4.89,ATM9/0/ 3,))
```

#### 12.3.2.5. Computing ATM Fabrics

When the set of ATM links is known, ANI then computes the ATM fabrics.

An ATM fabric is a set of ATM switches interconnected by ATM links such that any switch in the fabric can be reached from any other switch in the fabric by traversing one or more ATM links and optionally one or more ATM switches in the fabric. The fabric contains both ATM switches and all the ATM links that are connected to those ATM switches, including links-to-edge devices, but not including the edge devices themselves.

A fabric can consist of a single, disconnected ATM switch.

In theory, a fabric can consist of a single ATM link connecting two edge devices directly, although this will probably never happen in a real network.

**Note:** The CiscoWorks Campus Manager graphical user interface (GUI) displays edge devices in fabrics. However, technically, the edge devices are not part of any fabric. The ATM links to which the edge devices are connected are members of ATM fabrics, and AtmDirector displays the edge devices in the fabrics of the ATM links to which the edge devices are connected.

If a new link is discovered that connects switches in two different fabrics, then those fabrics merge to become one fabric. ANI creates a new fabric, it moves all the switches and links from the two old fabrics to the new fabric and destroys the two old fabrics. When ANI completes the merge, it then places the new link into the merged fabric.

If a link is removed that was connecting two switches, or if a switch is removed that had links to other switches, then ANI checks to see whether removing that link or switch partitions the fabric. If it does, then ANI separates the fabric into two or more new fabrics. Switches and links are moved from the old fabric into one of the new fabrics based on ATM reachability. When the old fabric is empty, ANI destroys it.

Whenever ANI creates a new fabric because of a merge or a separation, it generates a new, unique name for the new fabric. For a merge, the new name is a concatenation of the names of the two merged fabrics, plus a numeric suffix that guarantees uniqueness. For a separation, the new names of the new fabrics are equal to the name of the separated fabric, plus numeric suffixes that guarantee uniqueness. For entirely new fabrics, ANI uses the generic name "fabric," plus a numeric suffix that guarantees uniqueness.



During the initial ILMI topology computation, ANI places links and switches into fabrics based on the links and switches to which they are connected. If they are not connected to anything in a fabric, ANI creates a new fabric. Often, this new fabric is merged quickly into an existing fabric when additional links and switches are processed. This is why initial discovery can sometimes generate one fabric with the name “fabric-9” when there is no “fabric-1” through “fabric-8.” The other fabrics were probably temporary, and ANI destroyed them in merge operations before the ILMI topology calculation was finished.

#### 12.3.2.6. Computing ATM Fabrics Examples

The following example shows ANI placing new links into fabrics:

```
13:47:41 Discovery ani TopoSMFGenerateIlmiTopology: Created new fabric fabric-1
13:47:41 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.89,ATM12/0/0),(172.20.4.10,ATM4/0/0,)) to fabric fabric-1
13:47:41 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.11,ATM0/1/1),(172.20.4.10,ATM1/0/0,)) to fabric fabric-1
13:47:42 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.11,ATM3/1/0),(172.20.4.10,ATM3/0/1,)) to fabric fabric-1
13:47:42 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.9,ATM4/1/1.91),(172.20.4.11,ATM3/1/1.91,)) to fabric fabric-1
13:47:42 Discovery ani TopoSMFGenerateIlmiTopology: Created new fabric fabric-2
13:47:42 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.15,ATM12/1/0),(172.20.4.14,ATM3/0/ A,470079000000000000000000000000a03e00000100)) to fabric fabric-2
13:47:42 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.9,ATM0/0/0.99),(172.20.4.11,ATM1/0/1.99,)) to fabric fabric-1
13:47:42 Discovery ani TopoSMFGenerateIlmiTopology: Adding link (full,(172.20.4.15,ATM12/1/2),(172.20.4.66,ATM11/1/0,)) to fabric fabric-2
```

Following is an example of merging fabrics. Fabric-1 and fabric-4 are merged to produce fabric-7.

```
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Merging fabrics fabric-4 and fabric-1
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Created new fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving switch 172.20.126.66 from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving switch 172.20.126.67 from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving switch 172.20.126.68 from fabric fabric-1 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.70,ATM2/0/A),(172.20.126.66,ATM1/1/0,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.33,AT1/0),(172.20.126.66,ATM1/1/1,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.67,ATM0/0/1),(172.20.126.66,ATM0/0/3,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.67,ATM1/1/0),(172.20.126.66,ATM1/0/0,)) from fabric fabric-4 to fabric fabric-7
```



```
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.67,ATM0/0/0),(172.20.126.66,ATM0/0/2,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.5,AT2/0),(172.20.126.66,ATM1/1/3,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.69,ATM3/0/A),(172.20.126.66,ATM1/1/2,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link (full,(172.20.126.57,ATM5/0/A),(172.20.126.66,ATM0/0/1,)) from fabric fabric-4 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link
(unknownAtm,(172.20.126.68,LEC/ATM9/0 / 1),47009181000000009021565c01009021565c4800) from
fabric fabric-1 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving link
(unknownAtm,(172.20.126.68,ATM9/0/ 0),47009181000000009021565c01009021565c4700) from fabric
fabric-1 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Moving
link(unknownAtm,(172.20.126.68,LEC/ATM9/0/ 0),47009181000000009021565c01009021565c4700)
from fabric fabric-1 to fabric fabric-7
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Destroying fabric fabric-4
12:07:47 Discovery ani TopoSMFGenerateIlmiTopology: Destroying fabric fabric-1
```

### 13. Appendix B—rcp Explained

This section provides more background material of the remote copy protocol (rcp)—how it is configured and where and when it is used.

#### 13.1. Required Configuration to Support rcp for CiscoWorks RME Software Distribution

For CiscoWorks RME Software Image Manager (SWIM), the CiscoWorks Resource Manager Essentials (RME) server is the rcp server, and the Cisco IOS<sup>®</sup> device is the rcp client.

##### 13.1.1. Device

No configuration is required. Like the Trivial File Transfer Protocol (TFTP) client, the rcp client function is already enabled.

##### 13.1.2. CiscoWorks RME Server

1. Enable the use of rcp under the Administration section.

- 1.1. For Windows: No additional configuration is required.

CiscoWorks RME installs and enables an rcp service. During execution of the SWIM job, it dynamically creates ruser and rhost entries in the registry to match values it sends to itself via a Telnet session to the device. For example, if router rtr1 has an IP address of 10.1.1.1 and the CiscoWorks RME server rcp username is set to cwuser, then the RME server automatically adds these entries to the registry during execution of the job to authenticate the rcp client request from the router. The client request is initiated by the RME server through a Telnet session to the client. In the request, it automatically sets the remote-username to *cwuser*, or whatever value



was set in its configuration. For reference, this username is equivalent to the parameter in the Cisco IOS command `ip rcmd remote-username <value>`. Again, the RME server automatically sends the correct value in its rcp request, so this parameter does not need to be manually set on the device.)

Note: For rcp on Windows, you need to have the user SYSTEM allowed on the router for rcp to work.

#### 1.2. For UNIX:

1.2.1. Enable rcp services in UNIX, if not already enabled.

1.2.2. Create a UNIX user account to match the CiscoWorks RME server setting or change RME to match the existing UNIX account.

1.2.3. Create a `.rhosts` file and apply appropriate permissions to the file for RME access.

Like the Windows case, CiscoWorks RME automatically populates or removes the necessary authentication entries in the `.rhosts` file, that is, the device hostname, that is, `rtr1`, and its IP address or Domain Name System (DNS) name. The CiscoWorks RME server, through its Telnet session to the device, makes the rcp request to its rcp username setting, which happens to be a valid UNIX user account. The dynamic `.rhosts` entries match the hostname and address settings sent by the device and the rcp transfer can be completed.

Note: SWIM always uses TFTP for configuration file transfers, so rcp is not an option.

### 13.2. Required Configuration to Support rcp for CiscoWorks RME Configuration Management

For configuration management, the CiscoWorks RME server is the rcp client, and the Cisco IOS device is the rcp server.

#### 13.2.1. Device

1. Enable rcp server-side functions:

```
router(config)# ip rcmd rcp-enable
```

2. Create an authentication database entry to accept rcp requests from the CiscoWorks RME server:

```
router(config)# ip rcmd remote-host cwuser <RME server address> cwuser
```

Change `cwuser` to whatever value was set on the CiscoWorks RME server. Both values, `local-user-name` and `remote-username`, must be the same and they must match the CiscoWorks RME server setting. As the rcp client, the RME server sends these values to identify the local device account to use for authentication and the local name it assigns to itself.

#### 13.2.2. CiscoWorks RME Server

1. Change the preference of rcp, as desired, under Transport Options under RME Administration.
2. Verify that the CiscoWorks RME rcp username matches the device setting. If the device uses the default value of `cwuser`, then no change is required.

2.1. For Windows: No additional configuration is required.

CiscoWorks RME installs and enables an rcp service. During execution of the Configuration Management job, it sends an rcp request to the device using the rcp username value as both the remote username account on the device and the local name used to identify itself.





2.2. For UNIX: Enable rcp services to support the client-side function, if not already enabled.

During execution of the Configuration Management job, it sends an rcp request to the device using the rcp username value as both the remote username account on device and the local name used to identify itself.

Note: DNS must be functioning properly if DNS host names are used in CiscoWorks RME or on a Cisco IOS device. Verify configuration from both RME and the device using nslookup or testing domain-lookup. You may want to create reverse-lookup (PTR records) for each of the device interfaces to point to the same DNS name. You can also use the command ip rcmd source-interface to ensure that the same address is used by the device for rcp.

#### 14. Appendix C—CiscoWorks Port Usage

This section provides a list of TCP and User Datagram Protocol (UDP) ports used by the various CiscoWorks components.

Protocol	Port number	Service name	Application(s)	Direction (of establishment) of connection*
<b>Internet Control Message Protocol (ICMP)</b>	–	Ping	CiscoWorks Resource Manager Essentials (RME), Campus Manager, and Device Fault Manager (DFM)	Server–Device
<b>TCP</b>	22	Secure Shell Protocol (SSH)	CiscoWorks RME	Server–Device
	23	Telnet	CiscoWorks RME	Server–Device
	39	TACACS	CiscoWorks RME	Server–Device
	80	HTTP	CiscoWorks RME, CiscoWorks CiscoView (CV)	Server–Device
	514	rcp	CiscoWorks RME	Server–Device
	1741	CiscoWorks	Main CiscoWorks Web user interface	Client–Server
	1742	Secure Sockets Layer (SSL)	CiscoWorks RME	Server–Device
<b>UDP</b>	69	Trivial File Transfer Protocol (TFTP)	CiscoWorks RME, CiscoWorks ACL Manager	Device–Server
	161	Simple Network Management Protocol (SNMP)	CiscoWorks RME, CiscoWorks Campus Manager, CiscoWorks DFM, CiscoWorks RTM, CiscoWorks Internetwork Performance Monitor (IPM), CiscoWorks Voice Health Monitor (VHM), CiscoWorks CV	Server–Device
	162	SNMP traps	CiscoWorks DFM, CiscoWorks VHM, CiscoWorks RTM	Device–Server
	395	SNMP traps	CiscoWorks RTM	Device–Server
	514	Syslog	CiscoWorks RME	Device–Server

Please note that this list is not complete.

Note: UDP is a connectionless protocol. Thus, connections are not established as such. In this case, the direction indicates which party initiates the communication.

Refer to [http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products\\_quick\\_start09186a00800b7553.html#wp51666](http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_quick_start09186a00800b7553.html#wp51666) for a more complete list of ports in use.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0303R) 203080/ETMG\_05/03