Release Notes for CiscoWorks Network Compliance Manager, 1.2

January, 2007

These release notes include important information regarding CiscoWorks Network Compliance Manager (NCM), Release 1.2. NCM provides network configuration and change features, policy-based workflows, best of class compliance reporting capabilities, and APIs. NCM includes integration with CiscoWorks—initially launchable from the CiscoWorks home page and interoperability with other CiscoWorks applications such as the LMS bundle through the CommonServices Device Credential Repository (DCR).

Note All documentation, including this document and any or all of the parts of the NCM documentation set, *might* be upgraded over time. Therefore, we recommend you access the NCM documentation set using the Cisco.com URL: http://www.cisco.com/en/US/products/ps6923/tsd_products_support_series_home.html.

In addition, the **Docs** tab visible from within Network Compliance Manager *might* not include links to the latest documents.

Contents

This release note contains the following sections:

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

Features in This Release

This release includes the following features:

- Automated cisco.com product license registration, which enables:
  - Flexible licensing
  - Incremental node license registration
  - Incremental feature license registration for features such as high availability, satellite, and connectors
- Optional subscription to NCM Alert Center content packs, which can be downloaded from the cisco.com NCM Alert Center Web page into the NCM application. These content packs can keep you up to date with:
  - security compliance policies
  - product extensions
- Subscriber access to and ability to download content packs into NCM.
- New connector with third-party network management products such as Remedy AR.

System Requirements

This section includes the following:

Linux Server Requirements

The following tables provide the recommended requirements when installing NCM on a Linux platform. Keep in mind that the application server and the database server can be configured together or separately depending on the size of the network.

Note You must stop other network management applications, Web servers, databases, and Syslog/TFTP servers running on the same system before installing NCM. Applications include anti-virus (during Setup only) and WWW Publishing Server applications.

Table 1 Requirements for the Application Server on the Linux Platform

OS	RedHat Linux AS 3.0, Update 2 SUSE Linux Enterprise 9.0
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	14 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	Adobe Acrobat Reader 4.0 or higher (for viewing documentation) KDE Desktop Manager Mozilla Firefox 1.0+

Table 2 Requirements for the Database Server on the Linux Platform

Supported Databases	One of the following: • Microsoft SQL Server 2000 (SP 2) • Microsoft SQL Server 2005 • MySQL Max 3.23.55 (included with NCM) • Oracle 9.2 (32 bit) • Oracle 10.2
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	22 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Table 3 Requirements for the Application and Database on the Same Server on the Linux Platform

OS	One of the following: • RedHat Linux AS 3.0, Update 2 • SUSE Linux Enterprise 9.0
Database	MySQL Max 3.23 (included)
CPU	Dual Processor Intel Xeon or equivalent, 3.0+ GHz
Memory	4 GB RAM
Swap Space	8 GB Swap
Disk	36 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Note When installing NCM on a Linux platform, Nmap 3.81 is required for Nmap scanning when running the Detect Network Devices task.

Summary Reports

Summary reports are generated in the Microsoft Excel XLS format. Excel does not run on Linux. You can either run the Summary reports from a Windows client computer connected to your NCM server or you can use one of the following products that run on Linux and can open Excel files:

- Open Office (www.openoffice.org)
- GNUmeric (www.gnumeric.org)
- Star Office (wwws.sun.com/software/star/staroffice)

Solaris Server Requirements

The following tables provide the recommended requirements when installing NCM on a Solaris platform. Keep in mind that the application server and the database server can be configured together or separately depending on the size of the network.

Note You must stop other network management applications, Web servers, databases, and Syslog/TFTP servers running on the same system before installing NCM. Applications include anti-virus (during Setup only) and WWW Publishing Server applications.

Table 4 Requirements for the Application Server on the Solaris Platform

OS	Solaris 9 Solaris 10
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	14 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	Adobe Acrobat Reader 4.0 or higher (for viewing documentation) The X Window System, X11 (also known as OpenWindows) Mozilla Firefox 1.0+

Table 5 Requirements for the Database Server on the Solaris Platform

Supported Databases	One of the following: • Microsoft SQL Server 2000 (SP 2) • Microsoft SQL Server 2005 • MySQL Max 3.23.55 (included with NCM) • Oracle 9.2 (32 bit) • Oracle 10.2
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	2 GB RAM
Swap Space	4 GB Swap
Disk	22 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Table 6 Requirements for the Application and Database on the Same Server on the Solaris Platform

OS	Solaris 9
Database	MySQL Max 3.23 (included)
CPU	Dual UltraSPARC IIIi+, 1.3+ GHz (SunFire V240)
Memory	4 GB RAM
Swap Space	8 GB Swap
Disk	36 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Note When installing NCM on a Solaris platform, Nmap 3.81 is required for Nmap scanning when running the Detect Network Devices task.

Summary Reports

Summary reports are generated in the Microsoft Excel XLS format. Excel does not run on Solaris. You can either run the Summary reports from a Windows client computer connected to your NCM server or you can use one of the following products that run on Linux and can open Excel files:

- Open Office (www.openoffice.org)
- GNUmeric (www.gnumeric.org)
- Star Office (wwws.sun.com/software/star/staroffice)

Windows Server Requirements

The following tables provide the recommended requirements when installing NCM on a Windows platform. Keep in mind that the application server and the database server can be configured together or separately depending on the size of the network.

Note You must stop other network management applications, Web servers, databases, and Syslog/TFTP servers running on the same system before installing NCM. Applications include anti-virus (during Setup only) and WWW Publishing Server applications.

Table 7 Requirements for the Application Server on the Windows Platform

OS	Windows Server 2003 Enterprise Edition (recommended) Windows Server 2003 Standard Edition Windows 2000 Server with SP4 Windows 2000 Advanced Server with SP4
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	10 GB, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex
Applications	Adobe Acrobat Reader 4.0 or higher (for viewing documentation) Microsoft Excel 2000 or higher (for viewing Summary Reports) Microsoft Internet Explorer 5.5 or higher or Mozilla Firefox 1.0 or higher

Table 8 Requirements for the Database Server on the Windows Platform

Supported Databases	One of the following: • Microsoft SQL Server 2000 (SP 2) • Microsoft SQL Server 2005 • MySQL Max 3.23.55 (included with NCM) • Oracle 9.2 (32 bit) • Oracle 10.2
CPU	Intel Xeon or equivalent, 3.0+ GHz
Memory	2 GB RAM
Disk	18 GB, Single Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Table 9 Requirements for the Application and Database on the Same Server on the Windows Platform

OS	Windows Server 2003 Enterprise Edition (recommended) Windows Server 2003 Standard Edition Windows 2000 Server with SP4 Windows 2000 Advanced Server with SP4
Database	MySQL Max 3.23 (included)
CPU	Dual Processor Intel Xeon or equivalent, 3.0+ GHz
Memory	4 GB RAM
Disk	28 GB, Dual Channel RAID, Fast SCSI
Network	100 Mbps Fast Ethernet, full duplex

Note When installing NCM on a Windows platform, Nmap 3.81 and WinPcap (Windows Packet Capture Library) version 3.1 are required for Nmap scanning when running the Detect Network Devices task.

NCM and LMS Co-residency Requirements

The following are the recommended requirements when you are enabling co-residency of NCM and CiscoWorks LAN Management Solution (LMS):

- Operating System on the Application Server: Microsoft Windows 2003
- Server Hardware: At least a Xeon (or a Dual Core) Processor with 8 GB of RAM.

For detailed information on NCM and LMS co-residency, refer to the Configuration Guide for Network Compliance Manager and LMS Co-residency.

Installation Considerations

Note We sometimes release patches after the original release of a product. Therefore, you should review the the following site on Cisco.com for any updates.

http://www.cisco.com/cgi-bin/tablebuild.pl/cwncm-crypto

NCM Gateway Requirements

The Network Compliance Manager Gateway enables a NCM Core to manage servers that are behind one or more NAT devices or firewalls. The NCM Gateway is supported on the following platforms:

- RedHat Linux 3.0 AS
- RedHat Linux 4.0 AS

NCM High Availability System Requirements

The NCM High Availability Distributed System is a multi-master system where the data from each NCM Core is available to all other NCM Cores. This collection of NCM Cores is called an NCM mesh. This configuration helps provides a comprehensive view of your data and allows for redundant data and failover in the event of a problem with the NCM Core. Each NCM Core consists of an NCM Management Engine, its associated services (Syslog and TFTP), and a single database.

Note If you intend to install the NCM High Availability Distributed System, keep in mind that it only supports the Oracle 9.2 database server. If you are running Oracle 10.2 on the Core database server, you cannot upgrade to the NCM High Availability Distributed System.

Upgrading the OS

Before performing server maintenance or upgrades, take steps to ensure that in the case of application or OS corruption, you will be able to restore critical NCM data.

Step 1 Back up your database to a safe location before doing server maintenance.

Step 2 Save the contents of the following folders to a safe location:

<NCM directory>\client\scripts\

<NCM directory>\addins\

<NCM directory>\jre\

<NCM directory>\server\lib\drivers

<NCM directory>\docs

If upgrading the server causes NCM to malfunction, contact Technical Support.

Backing Up User Files

During an upgrade, the NCM Setup program automatically backs up user files, such as the Summary reports and NCM scripts, to the following directories:

For Windows:

\winnt\temp\rendition\addins

\winnt\temp\rendition\images

\winnt\temp\rendition\log

\winnt\temp\rendition\scripts

For Solaris:

/var/rendition/addins

/var/rendition/images

/var/rendition/log

/var/rendition/scripts

Note If you have changed directories, you can find your current Windows directory by opening a command prompt window and entering **set windir**. The Windows home directory is displayed. The installer restores all user files automatically, except log files. If you want to keep appending to saved log files, copy them to **\rendition\server\log**.

Installing the Enhanced PERL API

The following modules are provided on the NCM Distribution CD:

- Cisco::NCM::Util
- Cisco::NCM::Client
- Cisco::NCM::Connect

Installation Requirements

PERL version 5.8 or later is required.

If you are using the Auto Installer, skip to the "Auto Installer Method:" section on page 10.

Note NCM 1.2 does not currently support the system call to run the **install.pl** script. At this time, you will have to manually install the enhanced PERL API.

If you are manually installing the PERL API, confirm that certain versions of PERL and/or PERL modules (that are not part of some core PERL distributions) are installed before you begin. Refer to the **META.yml** file within each package/tarball for its requirements.

If your PERL distribution does not contain all of the required PERL modules, they are available at http://www.cpan.org and/or via PPM. If you are using ActivePerl, try PPM first.

PPM (ppm.exe) is part of the ActivePerl distribution. If you are using ActivePerl, it is recommended that you use the PPM method. You can also run PPM without arguments and then issue the install command. You may need to do this for some PERL modules that have multiple versions to choose from, followed by install # (where # is the item in the list returned by the install command). Keep in mind that PPM prefers to use the **-** as a namespace separator in place of the PERL **::** separator.

To install any of the required modules, use one of the following commands:

- **ppm install SOAP-Lite**
- **cpan install SOAP::Lite**

Note **NMAKE.EXE** is installed when installing NCM on a Windows platform. It is located in the **/client** directory. CPAN is simply a wrapper for the PERL -**MCPAN -e** shell command. The CPAN command **cpan.exe** is part of the core PERL install on all PERL versions since 5.8.0, including ActivePerl.

Installation Steps

There are two methods for installing the PERL API modules. The first and easiest method is to use the Auto Installer. You can only use the Auto Installer, however, if you have installed the PERL API distribution via the NCM installer. Otherwise, you must use the manual installation method.

Auto Installer Method:

The Auto Installer installs all of the Cisco::NCM modules as well as their dependencies.

Step 1 Open a shell.

- If you are on a Windows platform, open a command shell.
- If you are on a Linux or Solaris platform, you can either open a command shell or SSH into the NCM server.

Note You will need to have privileges to both create and modify files for NCM as well as PERL. As a result, you might need Administrator privileges on a Windows Platform and root privileges on Linux or Solaris platforms.

Step 2 Change to the directory where NCM is installed. This directory will have been set when you installed NCM.

Step 3 To run the install script, enter:

```
perl client/perl_api/har/install.pl
```

Note If PERL is not in your path or you have multiple PERL versions installed, use the full path to the PERL executable that you will be using. This should also match the value for the PERL interpreter set in the NCM server configuration.

All of the Cisco::NCM modules are installed, as well as their dependencies. However, only pure PERL dependencies are provided. For example, SOAP::Lite is provided, which includes a minimalist lightweight XML parser. For the best performance, we recommend that you have the XML::Parser module installed.

If you are using ActivePerl (with a PERL version of 5.8 or better), the XML::Parser module is included with the distribution. Otherwise, you will need to use PPM, CPAN, or manually download and install the module.

Manual Install Method:

Keep in mind that the installation could fail if your PERL installation does not meet certain requirements. Refer to the "Installation Requirements" section on page 9. In addition, the Cisco::NCM PERL modules are distributed as compressed tarballs, similar modules on CPAN. They are located in the following directory: **<NCM_ROOT>/client/perl_api/Cisco/**.

To untar and uncompress all of the modules at one time, you can use the **ptar** command. **ptar** is distributed as part of the popular PERL module Archive::Tar, which is included in the standard ActivePerl distributions. To view the contents of the directory and to extract the contents into your current directory, enter: **ptar -xzvf PATH/TO/whatever.tar.gz**.

For each of the following modules, uncompress and untar the module(s) and change to the directory that was created:

- Cisco::NCM::Util
- Cisco::NCM::Client
- Cisco::NCM::Connect

To install the PERL API on a Windows platform with ActivePerl, or any platform running a version of PERL that has the Module::Build module installed, enter:

- **perl Build.PL**
- **perl Build build**
- **perl Build test**
- **perl Build install**

You may also use the traditional CPAN method. Enter:

- **perl Makefile.PL**
- **make**
- **make test**
- **make install**

Note If you are using the CPAN method on a Windows platform, you will need to enter **nmake** rather than **make**.

PERL Documentation

After installing the PERL API, you can view the following PERL POD pages:

- perldoc Cisco::NCM::Client
- perldoc Cisco::NCM::Connect
- perldoc Cisco::NCM::Client::4_5_x
- perldoc Cisco::NCM::Client::6_0_x

Your PERL distribution can also build HTML files for the documentation.

Examples

There are PERL API examples in the demo directory. These examples illustrate how to use the PERL API. Keep in mind that it is possible to run the examples without installing the PERL modules by remaining in the demo directory and supplying the relative (or full) path to each example, as in:

- unix_box$ perl demo/list_users.pl
- C:\Windows\Box> perl demo\list_users.pl

Resolved Problems

Table 10 lists the problems that were resolved in CiscoWorks Network Compliance Manager, Release 1.1. Table 11 lists the problems that were resolved in CiscoWorks Network Compliance Manager, Release 1.2.

Table 10 Resolved Problems in Release 1.1

DDTS Number	Description
CSCsf03275	NCM Version 1.0 may pose a security threat to the NCM server database when installed together with MySQL on a Linux or Solaris platform. Installations of NCM and MySQL where MySQL is installed on a separate host from NCM are not vulnerable regardless of platform.
CSCse50595	Importing devices into NCM fails when NCM runs in ACS mode. In particular, when running NCM server with user authentication type to TACACS+ the import (**cwncm_import.bat**) script fails to connect to the NCM server (NCM authentication type is TACACS+). However, it works if NCM authentication type is set to **local**.

Table 11 Resolved Problems in Release 1.2

DDTS Number	Description
CSCsf21998	When viewing NCM license information using **Admin** > **About CiscoWorks Network Compliance Manager** > **View License Information**, the screen displays NCM 1.0 when the release is 1.1.
CSCsf31103	When generating diagrams using **Reports** > **Diagramming** > **Output Format** and you select Viso 2003 with SP2 and it is not installed, NCM will report an error.
CSCsf24217	The CWNCM installer does not automatically update the server name, user name and password info in **adjustable_options.rcx** file.
CSCsg01118	NCM incorrectly identifies the changing user of a device configuration in the daily email digests that are sent to the administrative users.
CSCse09653	Inconsistent login access to NCM server when accessed over internet. From the NCM login screen, provide username and password. NCM continues to display the login screen. No message is displayed.

Table 11 Resolved Problems in Release 1.2 (continued)

DDTS Number	Description
CSCse10342	This is one flow during which the error is consistently seen. Select **Policies** > **Policy List** >**Added New rule** >**Test** > **Added Devices** from **Device Selector**. Click **Perform Tes**t. This launches a browser window to display the test results screen. Click **Back**. **Page cannot be displayed** screen appear.s
CSCse24150	If you install the Oracle database on the same server as NCM, an error condition occurs.

Known Limitations and Problems

This section contains information about the limitations and problems known to exist in the NCM 1.2 product.

CSCse09644—The **cwncm_import** script does not parse the hostname as present in the CSV file.

Description: When exporting some devices from DCR into the CSV file using **dclr_export.sh** or from Device Management UI of LMS, the **cwncm_import** script does not parse the hostname (present) in the CSV file; instead, it substitutes the IP Address as the hostname for all these imported devices.

Workaround: You can manually change the Hostname by looking up the corresponding name in the CSV file. This issue will be fixed in a future release.

CSCse09092—Clicking **Perform Test** does not launch a new window.

Description: From **Policies** > **Policy List** > **Add New rule** > **Test** > **Added Devices** from Device Selector, select **Perform Test**. A browser window does not launch to display the Test Results screen.

Workaround: The problem only happens when you select a UNIX driver for the UNIX end hosts. Selecting any other device type will resolve the issue.

CSCse11820— Installation hangs if you provide incorrect Database credentials.

Description: Oracle is installed successfully and you proceed with NCM installation. If you provide any incorrect database credentials (port number, DB name, or password) while configuring the NCM Database, then NCM hangs while trying to connect to the database.

Workaround: Stop the installation using the Windows task manager. Restart the installation and enter the correct credentials.

CSCse14518—When you attempt to delete a large number of devices from the NCM database, it fails.

Description: Devices are imported into NCM, which uses Oracle database. Go to the **Device > Inventory** window, select a large number of devices that you wish to delete, and select **Delete**. NCM prompts you confirm the deletion. Click **yes**. After sometime, only 200 devices are deleted.

Workaround: Delete a smaller number of devices at each attempt (< 500 devices).

CSCse16371—An error message **incomplete command** displays when you try to get hardware information for a CRS-8/S device.

> **Description:** From **Inventory**, select a CRS-8/S device. Go to **View > Diagnostics > Hardware Information**. No hardware info gets displayed, instead an error with the message **incomplete command** is displayed.
>
> **Workaround:** There is no known workaround for this issue. Please avoid using this feature for this device type.

CSCse16848—Duplicate entries are seen in the software updates report.

> **Description:** When adding more than one image set from **Devices > Device tools > Software Images**, the weekly report incorrectly reports two successful updates when this is not the case.
>
> **Workaround:** There is no known workaround for this issue.

CSCsg79893—License monitor results column updated only after browser manual refresh.

> **Workaround:** This is how all the System Monitors work. By default the monitor data is updated every 6 hours but this is configurable.

CSCsh28136—Installer fails to copy licenses from a directory whose name has spaces.

> **Workaround:** Make sure that the directory and directory path where the license files are being copied do not have spaces in their names. If you must use directory and directory path names containing spaces, make sure to quote the entire path.

Caveats

Please read the following usability issues before using NCM. These issues are listed in alphabetical order.

Administrative Settings - User Authentication Page Crypto Key Exception

It is possible that after upgrading to NCM 1.2, you will not be able to access any of the menu items under Administrative Settings. This is due to a corrupted encryption option in the **site_options.rcx** file.

Workaround:

Step 1 Go to the **$NCM_HOME/jre** directory.

Step 2 Backup the current **site_options.rcx** file.

Step 3 Open the **site_options.rcx** file and locate all encrypted text options by searching for **EncryptedText**.

Step 4 Remove the value for all encrypted text options if it is not empty. In the following example, you would delete the information between **</comment>** and **</option>**.

Before:

```
<option name="twist/password"><title>Twist Password</title><section>Cisco Server
Automation System Authentication</section><size>30</size>
<type>EncryptedText</type><comment>Web Services Data Access Engine Password for
finding connected servers.</comment>encrypted:sQAHLgjGjdGIbvNB18NEoQ==</option>
```

After:

<option name="twist/password"><title>Twist Password</title><section>Cisco Server Automation System Authentication</section><size>30</size> <type>EncryptedText</type><comment Web Services Data Access Engine Password for finding connected servers.</comment></option>

Step 5 Save the file.

Step 6 Login to NCM.

Step 7 On the menu bar under Admin, select **Administrative Settings** and click **User Authentication**.

Step 8 Scroll down to the **TACACS+ / RADIUS Authentication** section.

Step 9 For the **TACACS+ or RADIUS Secret** option, enter the shared secret for the NCM host configured on the TACACS+ or RADIUS server.

Step 10 Scroll down to the **Cisco Server Automation System Authentication** section.

Step 11 For the Twist Password option, enter the SAS password to use when locating connected servers.

Step 12 Click **Save**.

Step 13 Click the **Device Access** tab.

Step 14 Scroll down to the **Bastion Host Settings** section.

Step 15 For the Default Bastion Host Password option, enter the password of the Bastion Host to use for Telnet and/or SSH access.

Step 16 Click **Save**.

Banner Handling Strings Require Device-specific Passwords

If you enter banner handling strings, **Devices > Inventory > Edit > Show Device Access Settings (device-specific settings) > Setting > Banner skip regex option** and enter common prompt strings, such as password or username, you cannot apply network-wide Password Rules to the device. If you do, the banner handling fails without generating any errors, and the device does not work with NCM device drivers. Tasks such as Snapshot and Driver Discovery do not work.

Workaround: Always use device-specific passwords on the Edit Device window.

Batch Insert ACL Line Option

When using the Batch Insert ACL Line option (**Devices > New Device Task > Batch Insert ACL Line**), the Task Options section on the New Task - Run Command Script window does not contain script content. While the Command Script to Run field correctly displays Cisco IOS **Insert (or Remove) Line into (or from) ACL by handle**, it does not present the script or script variables for execution until a device or device group for which the script supports is selected.

BayRS Device Can Lose Ability to Provide Snapshot

Occasionally, the BayRS device can enter a state in which it cannot provide a snapshot. Snapshot tasks fail with the following error message.

File retrieval error

Workaround: Rebooting the BayRS device restores the normal state on the device.

BayStack 450 Could Stop Responding to Telnet, SNMP, or ICMP

If you connect using a console to a BayStack 450, the allowed Telnet/SNMP Manager List is unexpectedly cleared out, indicating all management traffic is denied. This occurs when the device configuration file is downloaded repeatedly using TFTP. Nortel confirms this is an OS bug in some versions. The Nortel bug reference is CR 031215-85145.

Workaround: Do not snapshot more frequently than four times per day (the default). Be sure to turn off IGMP snooping if not in use. In case the BayStack 450 is unresponsive to Telnet, the switching function of the BayStack 450 is not affected. You should schedule a non-peak hour to reboot the device (or use terminal access to gain access).

Canceling or Deleting Tasks

Some NCM tasks will spawn external processes to run PERL or Expect scripts, or to run user-provided executables or shell scripts. Under certain circumstances, NCM may not be able to kill these external processes when the spawning task is cancelled or deleted. This could include scripts that spawn sub-processes or processes that are coded to catch kill signals.

Workaround: Manually stop the external process on the NCM server.

Cisco Banner Messages Special Characters

Cisco uses a superscript L (^{L}) special character to begin and end banner messages in its configuration files. This character is not typically supported by XML. Consequently, when you create a policy enforcement rule, incorporating the L special character, you are able to export the policy, but not import the policy using this rule.

Workaround: You can manually edit the XML before importing the policy by adding a delimiting character before and after the banner, as long as the delimiting character does not occur in the banner itself.

Cisco Catalyst Switches

Catalyst switches running CatOS 8.3(3) could crash when you connect to them using SSHv2 (for example from an SSH client, such as SecureCRT or Putty). By default, NCM uses SSHv2 as the primary access method to network devices. Therefore, there is a substantial risk that a Catalyst switch running 8.3(3) could be reset when managed by NCM.

Workaround: Upgrade your Cisco Catalyst to CatOS 8.3(4). If this is not possible, edit your Catalyst devices running 8.3(3) in NCM to use only SSHv1 or Telnet for device access.

Command Line Interface: connect Command

The **connect** command in the NCM Proxy now accepts a device ID. This is needed because device IP Addresses are no longer required to be unique. If you pass an invalid device ID, such as an ID that is not a number, with the **connect** command the NCM Proxy session is abruptly terminated.

Workaround: Reconnect to the NCM Proxy and enter a valid device ID.

Command Line Interface: Set Telnet or SSH Client Width to 500

The NCM CLI has very wide output. For maximum ease in viewing the data, set your client's buffer width to 500.

Console Server: SSH Access is not Supported

NCM does not support console server access using SSH. If you use a console server to access a device, you must use the Telnet connectivity. In other words, in the New Device window /Edit Device window, if **Use to access device** is checked in the Console Server Information section, you should make sure that the **Telnet** option in the Connection Information section is also checked.

Deploy to Startup Config and Reboot not Supported Using SNMP

NCM can deploy a configuration file to the startup configuration and reboot the device using the command line only. If the device is configured for SNMP access only (see the *Device Driver Reference for Network Compliance Manager* for Network Compliance Manager), deploy startup and reboot will fail.

Detect Network Devices Task

The NCM system prevents you from inadvertently running more than one Detect Network Devices task concurrently. Although the Detect Network Devices task generates only a minimal level of traffic, NCM provides this protection to help minimize additional traffic when running duplicate or additional Detect Network Devices tasks simultaneously. If a second or third Detect Network Devices task is scheduled while an earlier Detect Network Devices task is running, NCM will place the new task(s) in the **Waiting** state. The task(s) will run individually after the first Detect Network Devices task has completed.

Diagnostics: When to Run ICMP Tests

Use ICMP tests only to verify connectivity occasionally or after a change. They are not a replacement for monitoring software. You should schedule ICMP tests no more than once per 10 minutes.

Diagramming

NCM applies an absolute value for the **text height** attribute for interface and port labels shown in Visio diagrams. When the Visio VDX file is loaded, Visio assigns an incorrect formula to the **text height** attribute. As a result, when you have more than two lines of annotated text, such as a label, for an interface or port and you attempt to copy and paste, the label of the new interface or port is displayed improperly and could hide the interface or port icon.

Workaround: Click the **Text Tool** option on the Visio tool bar and move the label so as to expose the interface or port icon.

Displaying Diagnostics

Most NCM diagnostics are stored in text format. For a list of NCM diagnostics, from the **Reports** drop-down menu, select **Search For** and click **Diagnostics**. The following NCM diagnostics, however, are stored in binary format, and therefore are not searchable:

- NCM Module Status
- NCM Routing Table
- NCM OSPF Neighbors
- NCM Interfaces
- NCM Flash Storage Space

Workaround: Because the issue is that built-in diagnostics are not stored as clear text, you can create a custom diagnostic that performs the appropriate command (for instance, **Show Interfaces** for the equivalent of **Module Status**). As a result, the custom diagnostic will be searchable.

Distributed System Performance

When running a Distributed System, if you are deleting many objects simultaneously, the system may take a while to push transactions for large delete operations.

Duplicate IP Addresses with Multiple Sites

If your system is configured with multiple Sites in different Realms, you could see duplicate IP addresses if you select the **Multiple Devices/Groups** option on a **New Task** window when browsing the **Inventory Group** using the **Device Selector**.

Workaround: Using the **Device Selector**, browse to devices using the specific **Site Group**.

Extreme Devices: Configuration Comments Can Cause Misconfiguration

On Extreme devices, adding inline comments between multi-line commands, such as user account commands or set banner commands, can cause serious problems if the resulting configuration is deployed.

Workaround: Do not add inline comments between multi-line commands. Add comments on the line above the start of a command.

Installing NCM on Linux

When installing NCM on a Linux platform, the install might fail because there is no access to the MySQL database.

Workaround: When installing NCM on a Linux platform, perform the following steps prior to starting the installation.

Step 1 1. Open the **/etc/hosts** file.

Step 2 2. Change **127.0.0.1 localhost.localdomain localhost** to: **127.0.0.1 localhost**.

3. Save and close the **/etc/hosts** file.

If you have already started the installation, use the Linux command line to run the following commands:

```
#mysql -h <device ip - not 127.0.0.1> -u root mysql

mysql> GRANT ALL PRIVILEGES ON *.* TO root@localhost.localdomain IDENTIFIED
    BY '<password>' WITH GRANT OPTION

mysql> exit
```

Inventory: Data from Device Overwrites Manually Entered Values

Certain data on the Device Details window (and other windows) is auto-populated. If you manually change the data, NCM overwrites the values when the next snapshot occurs. The device-specific values are listed per device in the *Device Driver Reference for Network Compliance Manager.*

The automatically populated data includes:

- Domain Name
- Host Name
- Model
- Serial Number
- Location
- Vendor

JRE Versions

NCM uses JRE 1.4.2_08 to support I18N character sets. I18N (Internationalization) means modifying software or related technologies to potentially handle multiple languages, customs, and so on. Several NCM connectors, such as the HP OpenView Connector and SMARTS InCharge Connector, are installed with the NCM Client-only version, and must have the same JRE version as the NCM Server and the NCM Client for the API calls to work properly.

Note The AAA Log Reader and Solaris Syslog Reader are NCM clients and also need to have the same JRE version.

Juniper Devices with SCP Enabled do not Capture Running Configurations

If your Juniper device has SCP enabled, the copied configuration may not be the one running on the device.

Workaround: Always save the current configuration using the Save Configuration command.

NetScreen Devices

NetScreen devices could timeout during the discovery process. This does not occur on all platforms, however.

Workaround: Edit the NetScreen device information and set the **standard_timeou**t device variable to five seconds. This will enable the NetScreen device to complete the discovery process using the Command Line Interface (CLI).

When monitoring NetScreen devices, for NCM to detect that the device's interfaces are administratively down, the interface must be configured as down using the **set interface untrust ident-reset** command.

Nmap Requirements

Solaris and Linux Installations—When installing NCM on Solaris or Linux, the version of Nmap distributed with NCM (Nmap 3.81) is required for Nmap scanning when running the Detect Network Devices task. Refer to Chapter 1 of the *User Guide for Network Compliance Manager 1.2* for Nmap installation instructions.

Nmap Scanning

Careful consideration should be taken when identifying the network range you are going to scan. Some network topologies can result in very long scans. In addition, it is recommended that you do not scan Internet addresses. If you think your Nmap scan will take more than a few minutes, you can use several Nmap options, for example **--max_scan_delay <milliseconds>**, setting **<milliseconds>** to a value between 1 and 1000. Nmap will throttle up to 1000ms max as packets are dropped.

Keep in mind that Nmap settings can be changed using the **Administrative Settings** option under **Admin** on the menu bar, and selecting the **Device Access** option. Please refer to the Nmap documentation at www.insecure.org for detailed Nmap information.

RADIUS External Authentication

When setting up a user to authenticate using RADIUS, if the RADIUS server does not respond, NCM still authenticates the user against the NCM local password, even if you instruct NCM not to fail-over on external authentication.

Reports: Checkpointing Can Cause Reports to be Inflated

The **Make Snapshot a Checkpoint** option on the Snapshot Task window (**Task > New Task > Take Snapshot**), stores the configuration file regardless of whether it changed. However, even if there is no change, the snapshot still appears as a configuration change on the Home window, Summary reports, Configuration Change search results, and so on. As a result, the number of configuration changes includes the check-pointed configurations, and therefore these counts may not be accurate.

Scripts: Cannot Save Command Scripts with Quote Marks in the Name

Do not use quote marks when naming command scripts. If you do, you will not be able to select and run the command script.

Scripts: Cannot Save Template or Command Scripts with a Period in the Name

Command Scripts, Templates, and Custom Diagnostics cannot have a period in the name. Use underscores or dashes in place of a period.

Scripts: Command Scripts and Templates for Cisco Aironet VxWorks Devices

NCM supports command scripts and templates for Cisco Aironet wireless access points running VxWorks software (for example, OS versions 11.23T & 12.01T1). Because scripts and templates are deployed differently to Cisco Aironet devices, NCM uses TFTP to deploy a file containing the script to the device. Some OS versions on Cisco Aironet devices accept only a limited size file using TFTP. In these cases, any excess commands are ignored and will not be run on the device. However, the script will still report successful execution. Devices exhibiting this behavior will accept no more than approximately 130 lines of text and ignore the rest without reporting an error.

Workaround: Use scripts smaller than 100 lines, or use multiple scripts to deploy larger sets of configuration commands to the device. If possible, upgrade the device to a newer version of code, ideally a version of IOS (12.2).

Scripts: Output Results in HTML Format

When executing an advanced script or a Run External Application task, any text that the advanced script or external application writes to **stdout** is stored in NCM as the task result. Typically, this output is treated and displayed as plain text. Before NCM displays the task results, it will escape any characters that would affect the HTML rendering, for example converting < to **&lt;**.

However, you may want to create an advanced script that outputs its results in HTML format. In this case, none of the output characters would be escaped, so the results displayed would include any applicable HTML formatting. To indicate to NCM that your script outputs HTML results, the first item that your script writes to **stdout** must be **<html>**. If your script output begins with anything other than **<html>**, the script results will be treated as plain text.

SecurID Device Access

If you are using SSH to access devices, SSH connectivity will not work if a software token is in **Next Token** mode. Be sure to reset your software tokens to **Normal** mode before attempting SSH connectivity to devices.

SecurID Software Token Software, Version 3.0.5

If the NCM server is installed with the **3.0.5 SecurID** token software, turn off copy protection when exporting SecurID software token keys on the RSA server. Otherwise, NCM reports an error when accessing SecurID software tokens. A patched version of the SecurID software is available at RSA's website (http://www.rsasecurity.com).

Sending Reports to External Email Addresses

Even though you may have properly configured NCM to contact your SMTP server, for network security reasons your SMTP server could have been configured to reject messages from the NCM server address. In this case, you would see the following error message, and any NCM messages would not be delivered.

Error occurred when sending email. Please check the email address and/or your SMTP server settings.

If this occurs, you will need to configure the SMTP server to enable the NCM server to relay email messages through it.

Software Center: Cisco IOS 2500

A problem with the Cisco IOS 2500 can affect NCM's Software Update Center. With a Cisco IOS 2500, running Version 12.3(3) (distributed as c2500-i-l.123-3.bin), some file systems are inconsistently reported. The Software Update Center is not able to retrieve a list of files on devices running this software version. Additionally, the Software Update Center cannot deploy software to the Cisco IOS 2500 running Version 12.3(3) because the Software Update Center cannot query the device for the available locations (**dir ?** does not return **flash:** and **copy tftp ?** does not list **flash:**).

Workaround: Although the Software Update Center cannot execute a software upgrade to the Cisco IOS 2500 running Version 12.3(3) by specifying a single device (the missing flash: slot information prohibits it), you can perform a software upgrade by creating a device group that contains only the Cisco IOS 2500, and then execute a software upgrade to that group.

Software Center: Cisco IOS Devices

Software Center does not support 11.x drivers for Cisco IOS 11.x. Although it is possible to downgrade a Cisco device from 12.x to 11.x, it is not possible to upgrade from 11.x to 12.x. In addition, if you try to perform a software upgrade, the existing image on the device can be deleted, and the software update task will fail. Consequently, there is no way to upload an image to the device.

Workaround: Use a TFTP server to manually recover the lost image to the device.

Software Center: Deploying Software

When deploying software to a device, it is possible for the configuration file currently on the device to no longer be acceptable to the device. This is more likely during an OS downgrade. (OS upgrades are usually handled through upwards compatibility.) It is always a good idea to test the functionality of a given OS version before deploying it on a production network. When downgrading OS versions, the device configuration file may need to be manually updated. It is very important to make this change before rebooting the device, otherwise the device could attempt to use the invalid configuration file and become unresponsive.

For the Aironet 1100, if you deploy software with the Reboot option, the Aironet 1100 might not restart correctly. In fact, the Aironet 1100 might be left inaccessible and the Deploy Software task could continue running for up to an hour. This can also occur when manually deploying software.

Workaround: Turn the device off and back on to restore connectivity. Alternatively, you can avoid the problem by turning the radio off before deploying software.

NCM does not support BayRS software downgrades from 15.x to 14.x. Although the software update will function, the device configuration file after the reboot is not valid for the new software image. The device will need to be rebooted, and the configuration file saved with the new code using a console connection.

Workaround: You can pre-deploy a valid configuration file for a software update. The configuration file should be built by SiteManager for the particular version of code you are deploying.

Software Center: Downgrading Nortel OS and Rebooting Could Leave Device Inaccessible

When you deploy an earlier version of an OS to a Nortel device, you could experience unexpected results, including the device becoming inaccessible. This occurs because commands and configuration methods might have changed, and these might not work correctly for the earlier OS when downgrading.

Be sure to review the configuration file before downgrading and possibly test the procedure in a lab before migrating the change to your production network. You should also configure out-of-band access using a console port before downgrading a device OS.

Software Center: Image Set Name Requirements

Do not enter special characters, such as **$** or **&**, when naming an Image Set. In addition, do not include any characters outside of the alphabet or number scale in the Image Set name. These characters are mishandled in the URL and are not parsed correctly.

Software Center: Reboot Option

The Software Center reboot option is not supported when a BayRS device is configured to receive its configuration file from the network. The BayRS device returns an error message when NCM attempts to reload the device.

```
[1:TN]$ boot - 1:config
Configuration source is network - override allowed only when source is local.
```

Workaround: Configure the BayRS device to use the locally stored configuration file.

SQL Server 2005 Password Requirement

When installing NCM using a SQL Server 2005 database, you are prompted for the username and password NCM uses to connect to the database. If you enter a password that is not complicated enough for the existing Windows security policy, SQL Server 2005 discards the password and the NCM installation fails. A sample error message is: The password does not meet Windows policy requirements because it is too short.

Workaround: Enter a complex password that includes both lowercase and uppercase letters, several digits, and perhaps a special character. For example: PvyJ319?&

Syslog Messages

Certain Syslog messages (compliant with the Syslog RFC) sent from devices could have the same sender IP address as the IP address in the Syslog messages. In this case, NCM does not process the Syslog messages or schedules events. As a result, change detection will not work as expected on these devices.

Tasks: Running External Application Tasks Presents a Possible Security Risk

All Run External Application tasks run the application with root (UNIX) or system (Windows) privileges. This is a potential security risk that should be acknowledged by the System Administrator before using the Run External Application feature. Contact Technical Support to learn how to run NCM without root/system privileges.

Tasks: Task Scheduled for the 31st Might Run on the 1st

If you schedule a monthly recurring task for the 31st of every month and that task runs during a month that contains fewer than 31 days, NCM will run the task on the 1st, 2nd, or 3rd day of the next month depending on how many days less than 31 the previous month contains. For example, if you schedule a task in February (with 28 days) for the 30th, the task will actually run on March 2nd. If you want to run the task on the last day of the month, you must set the date correctly.

UNIX Host Commands

UNIX host commands, such as cursor and color commands, can result in unusual characters. As a result, the unusual characters are captured in NCM proxy sessions, configurations, diagnostics, or script results. For example, if your **ls** command is configured as an alias to **ls --color $@**, saved configurations could include the corresponding color commands which may cause the output to be difficult to read.

Workaround: Configure **ls** so that it is not an alias or utilize a command that does not use control characters to format the screen.

Unresponsive Script Warning Message in Mozilla Firefox 1.5 (or Higher)

When uploading a software image (New/Edit Software Image Set window) or any NCM window that requires file uploading, if you are using Mozilla Firefox 1.5 or higher and the file size is relatively large, you could see a warning message during uploading that indicates a script may be busy or has stopped responding.

Workaround: Click the **Continue** button.

If you want to avoid this warning message in the future, do the following.

Step 1 Enter **about:config** in Firefox's address bar.

Step 2 Scroll down to the **DOM.*** section.

Step 3 Locate the value for **dom.max_script_run_time**.

Step 4 Edit the default value **(5)** to something higher, for example **20**.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.