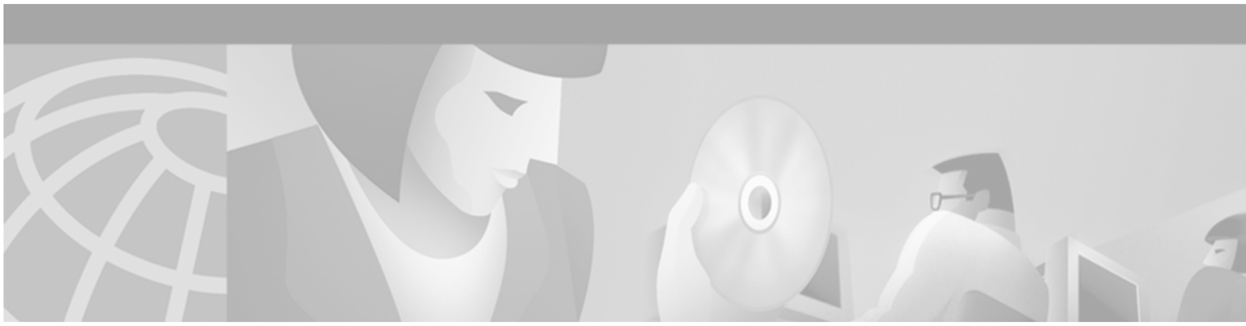

Release Notes for Cisco Internet CDN Software, Version 2.1.1

February 15, 2002

Contents

These release notes contain information about the Cisco Internet Content Delivery Network (CDN) Software, Version 2.1.1. It describes the following topics:

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

Introduction

The Cisco Internet CDN Software Version 2.1.1 contains the following modifications since the release of Version 2.1:

- New and expanded command-line interface (CLI) commands relating to system configuration properties, RealServer, file copying, and database troubleshooting
- A manifest file validator utility that validates the Extensible Markup Language (XML) syntax of a manifest file
- Ability to query database using Structured Query Language (SQL) queries and read-only database views
- Enhanced security for manifest file retrieval and for the Oracle database connection
- Load-based routing to Content Engines
- Various fixes since the previous software release

System Requirements

This section describes the devices and third-party applications that are supported on an Internet CDN, the media servers that are native to these devices, and the software and servers that are required for you to set up and manage an Internet CDN.

Cisco-Supported Hardware

Cisco Internet CDN Software Version 2.1.1 operates with the following Cisco hardware:

- Content Distribution Manager 4670 ICDN (model number CDM-4670-ICDN-K9)
- Content Router 4450 ICDN (model number CR-4450-ICDN-K9)
- AC and DC versions of the Content Engine 500 ICDN Series (model numbers CE-590-ICDN-K9 and CE-590-DC-ICDN-K9, respectively)
- AC and DC versions of the Content Engine 7320 ICDN Series (model numbers CE-7320-ICDN-K9 and CE-7320-DC-ICDN-K9, respectively)
- Content Services Switch 1115x and 1180x
- Cisco Catalyst switches (optional)
- AC and DC versions of the Storage Array 6 (model numbers SA6-SHF-6Disk-AC and SA6-SHF-6Disk-DC, respectively) for use with the Content Engine 590
- Storage Array 12 (model number SA12-SHF-12Disk-AC) for use with the Content Engine 7320

Refer to the Cisco documentation that came with each device for detailed, device-specific instructions on handling, installing, and configuring your Cisco CDN hardware.

Software Compatibility

For Version 2.1.1, the following upgrade sequences for the Cisco Internet CDN Software are supported:

- Version 2.0.1 —> Version 2.1.1

- Version 2.0 —> Version 2.1.1
- Version 2.1 (25) —> 2.1.1
- Version 2.1 (28) —> 2.1.1
- Version 1.0.2 —> Version 2.0.1 —> 2.1.1
- Version 1.0.1 —> Version 2.0.1—> Version 2.1 —> 2.1.1

The following downgrade sequences are supported:

- Version 2.1.1 —> 2.0.1
- Version 2.1.1 —> Version 2.1 (25)

Workstations That Access the Web-Based Interface

You interact with the Cisco Internet CDN Software using the web-based graphical user interface that is installed on the Content Distribution Manager. The following minimum hardware and software requirements apply to each machine that is used as a workstation for accessing the graphical user interface.

Network

- Ethernet connection
- Connection to the Internet

Platform and Operating System

- Windows 95/98 Pentium-class system, 266 MHz, 64 MB of RAM
- Windows NT/2000 Pentium-class system, 266 MHz, 64 MB of RAM

Software

- Microsoft Internet Explorer 4.x/5.0 (or later)
- Netscape 4.7 (or later)

Database Management System

The Cisco Internet CDN Software requires that the Oracle 8i database management system (DBMS) be installed on your host network. The Cisco Internet CDN Content Distribution Manager uses an Oracle database for persistent storage of system information and statistics.

The Cisco Internet CDN *does not* require a dedicated Oracle database. If you already have an Oracle database in use within your organization, that database can also be used with your Internet CDN.

If you have not already done so, you must purchase Oracle 8i from Oracle. The DBMS requirement is Oracle 8i Version 8.1.6 or later.

For information about setting up the Oracle 8i database, refer to the Oracle documentation, and the *Cisco Internet CDN Software Configuration Guide* for version 2.1, Chapter 2, in the section “Setting Up the Oracle 8i DBMS.”

Domain Name System

Cisco Internet CDN Software Version 2.1.1 uses the Domain Name System (DNS) to route requests to Content Engines. To serve content in your CDN, you must configure DNS. For information on how to do this, see the *Cisco Internet CDN Software Configuration Guide* for Version 2.1, Chapter 2, in the section "Configuring DNS."

RealServer, Darwin Streaming Server, and WMT Server

Content Engines that serve QuickTime media files using the Apple Computer Darwin Streaming Server, RealNetworks RealMedia files, or Windows Media files require that the server software be installed. Cisco Internet CDN Version 2.1.1 Content Engines ship with the Darwin Streaming Server Version 3.0, the RealNetworks RealServer Version 8.0, and the Starbak Windows Media Technologies (WMT) Server already installed.

If you wish to distribute RealMedia content over your CDN, you must also purchase a server license from RealNetworks in order to use the RealServer feature.

If you intend to serve live content using RealServer on Cisco Internet CDN Software Version 2.1.1, you must upgrade the RealServer software on your origin server to RealServer Version 8.0 if you have not already done so.

If you wish to distribute WMT content over your CDN, you must purchase a WMT server license from Cisco Systems for each Content Engine that will be serving WMT content.

File Transfer Protocol Server

You need a File Transfer Protocol (FTP) server configured to receive ACTIVE-mode transmissions if you want to enable remote logging. For information, refer to the Cisco Internet CDN Software online help or the *Cisco Internet CDN Software User Guide* for version 2.1.

SNMP Manager

You need a Simple Network Management Protocol (SNMP) manager if you want to monitor system statistics using SNMP. For information about creating and registering an SNMP manager with your CDN, refer to the *Cisco Internet CDN Software User Guide* for version 2.1, Chapter 4, in the section "Creating an SNMP Manager."

The Cisco Internet CDN Software Version 2.1.1 implements the HOST-RESOURCES MIB (IETF standard RFC 2790) and the CISCO-CONTENT-NETWORK-MIB. The CISCO-CONTENT-NETWORK-MIB monitors statistics related to the operation of the CDN. You can find the definition of the CISCO-CONTENT-NETWORK-MIB at ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CONTENT-NETWORK-MIB.my. For information on traps and variables in this MIB, refer to the *Cisco Internet CDN Software User Guide* for version 2.1.

Updating to a New Software Version

Review this entire section before beginning a software upgrade. It is important to have a clear view of the entire upgrade process before beginning.

To update your Internet CDN Software, you must follow this three-step procedure:

- Step 1—Determine the current software version
- Step 2—Add the software update file to your CDN
- Step 3—Update the software on your Internet CDN devices

In order to access and download your Cisco Internet CDN Software update, you need a registered username and password. If you are a Cisco customer and service contract owner, a Cisco reseller, Premier Certified Partner, the customer of a Cisco certified Partner Initiated Customer Access (PICA) partner, or a Cisco consultant, you can acquire a login directly from the Cisco.com website.

If you have questions or concerns about the upgrade, contact your designated Cisco Internet CDN Technical Support representative.

Step 1—Determine the Current Software Version

To determine the version of the Cisco Internet CDN Software that you are using:

Step 1 In your web browser, enter the secure IP address or DNS name of the Content Distribution Manager (CDM). For example:

```
https://10.0.0.0
```

Step 2 Log in to the Content Distribution Manager using the administrator username and password.

Step 3 From the Content Distribution Manager user interface, click **Tools**.

Step 4 From the System Tools drop-down list, choose **Software Update**.

Step 5 For each component (Content Distribution Manager, Content Engine, and Content Router), refer to the Version column. The current version of the software installed on that device is displayed.

Step 2—Adding a New Update File

Before you can update your Cisco Internet CDN Software, you must first acquire the appropriate software update file from Cisco.

In order to acquire the software update from Cisco, you must first:

- Access the Cisco.com website and locate the software update files.
- Download the software update files to a web server within your own organization or copy the location (URL) for the files (see the "Adding a New Update File Directly from Cisco.com" section on page 7,).
- Add the update to the CDN by copying the URL for the update files (pointing either to your web server or Cisco.com) to the Content Distribution Manager.
- Use the software update feature to import the update file pointed to by the link.

You must have a Cisco.com username and password before attempting to download a software update from Cisco.com. In order to acquire a Cisco.com login, go to http://www.cisco.com and click the **Register** link.

Note You need a service contract number, Cisco.com registration number and verification key, Partner Initiated Customer Access (PICA) registration number and verification key, or packaged service registration number in order to obtain a Cisco.com username and password.

To add an update file for the Cisco Internet CDN Software:

Step 1 Launch your preferred web browser and point it to:

```
http://www.cisco.com/cgi-bin/tablebuild.pl/cdn-sp
```

Step 2 When prompted, log in to Cisco.com using your designated Cisco.com username and password.

The Cisco Internet CDN Software download page appears, listing the available software updates for the Cisco Internet CDN Software product.

Note Each software update consists of two files: a binary-format update file (*.upg) and a smaller meta file (*.meta). Both files must be downloaded in order to successfully complete a Cisco Internet CDN Software update.

Step 3 Locate the files you wish to download by referring to the Release column for the proper release version of the software.

Step 4 Click the link for the software update file you wish to download. The order in which you download the update files does not matter. The download page appears.

Step 5 Click the Software License Agreement link. A new browser window will open displaying the license agreement.

Step 6 After you have read the license agreement, close the browser window displaying the agreement and return to the Software Download page.

Step 7 Click the filename link labeled Download.

Step 8 Click **Save to file** and then choose a location on your workstation to temporarily store the update file.

Step 9 Post the file you downloaded (*.meta or *.upg) to a designated area on your organization’s web server and make note of the URL required to access this file. You will need it later.

Note It is imperative that the upgrade (*.upg) file be placed in the same directory as its corresponding meta (*.meta) file.

Step 10 Repeat Step 3 through Step 9 for the other software update file.

Step 11 Launch the Cisco Internet CDN Software Version 2.1 Content Distribution Manager and log in using an administrative username and password.

Step 12 Click **tools**.

Step 13 From the drop-down list, choose **Software Update**.

The Software Update page appears listing available software updates. If there is currently no update available, a message appears.

Step 14 Click **Add New Update File**.

A page appears with a field for entering the URL of your software update.

Step 15 Paste the URL for the update meta file on your web server into the field provided. For example, a valid URL might look like this:

`http://internal.mysite.com/cdn/`*`internet-CDN-version`*`.meta`

where *internet-CDN-version* is the version number of the software update.

Note Do not attempt to link directly to the UPG file. The relative location of the update file is provided by the meta file.

Step 16 Click **OK**.

The version and URL for the update file appear, for example:

```
1.0.3 http://internal.mysite.com/cdnsw.upg
```

Adding a New Update File Directly from Cisco.com

It is also possible to add a software update to the CDN directly from Cisco.com, rather than posting it on a web server within your organization first.

To add the software update directly from Cisco.com:

Step 1 Launch your preferred web browser and point it to:

`http://www.cisco.com/cgi-bin/tablebuild.pl/cdn-sp`

Step 2 When prompted, log in to Cisco.com using your designated username and password.

The Cisco Internet CDN Software (Cisco CDN Service Provider Software) download page appears, listing the available software updates for the Cisco Internet CDN Software product. Note that each software update consists of two files: a binary-format upgrade file (*.upg) and a smaller meta file (*.meta).

Locate the software update you wish to install by consulting the Release column for the proper release version of the software.

Step 3 Click the link for the meta (*.meta) file. The download page appears.

Step 4 Click the Software License Agreement link. A new browser window will open displaying the license agreement.

Step 5 After you have read the license agreement, close the browser window displaying the agreement and return to the Software Download page.

Step 6 Right-mouse click the filename link labeled Download and choose the **Create Shortcut** option (Netscape) or the **Copy Shortcut** option (Internet Explorer). If you are using the Netscape browser, copy the contents of the URL field in the dialog that appears, then click **Cancel** to close the Create Shortcut dialog.

Step 7 Point your browser to the address of your Cisco Internet CDN Software Version 2.1 Content Distribution Manager and log in using an administrative username and password.

Step 8 Click **tools**.

Step 9 From the drop-down list, choose **Software Update**.

Step 10 The Software Update page appears, listing available software updates. If there is currently no update available, a message appears.

Step 11 Click **Add New Update File**.

A page appears for specifying the URL for the update location.

Step 12 Paste the shortcut you copied for the update meta file on Cisco.com into the field provided. The URL should begin with:

```
http://www.cisco.com/cgi-bin/Software/Tablebuild/download.cgi/...
```

Step 13 Click **OK**.

The version and URL for the update file appear, for example:

```
1.0.3 http://internal.mysite.com/cdnsw.upg
```

Step 3—Update the Software on Your Cisco Internet CDN Devices

The Content Distribution Manager will reboot at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the graphical user interface.

To update the Cisco Internet CDN Software on your devices, follow these steps:

Step 1 From the Content Distribution Manager user interface, click **tools**.

Step 2 From the drop-down list, choose **Software Update**.

Step 3 On the Software Update page, click the radio button next to the update file that you want to use.

Step 4 Click the tab corresponding to the type of device that you want to upgrade, for example, **Content Routers**. The window refreshes, listing the devices of the selected type on your CDN.

Note When updating the software on your Content Engines, you need to ensure that all Content Engines in a single supernode are updated at the same time.

Step 5 Refer to the column labeled Version to verify that the devices you are choosing are not already running the version to which you will be upgrading. Also verify that the current version has an upgrade path to the version to which you are upgrading.

Note If you have questions regarding upgrade paths, see the "Software Compatibility" section on page 2, or contact Cisco Technical Support.

Step 6 Check the check boxes next to the name of the device you will be upgrading, or check the box in the column header to select all devices.

Step 7 Click **OK**. The update process begins on the selected devices and they go offline temporarily.

Step 8 Repeat Step 4 through Step 7 for each device or group of devices that you wish to upgrade.

Step 9 Click the **Refresh** button to see the status of your upgrade.

You have completed the software update procedure.

Allow 15 to 30 minutes for the devices to come online on the CDM user interface after the upgrade has been completed. The CE-7320-CDN takes longer to come online than the CE-590-CDN because of the number of drives on the device.

Important Notes for Service Providers

This section describes issues related to Version 2.1.1 of the Cisco Internet CDN Software that may be of use or interest to service providers. The topics covered are:

- Accessing CDN Database Tables Using Read-Only Database Views
- Restoring a Deleted Content Distribution Manager to the CDN
- Deploying Cisco Internet CDN Behind a Firewall
- Implementing a Private Ethernet Link to the CDN Database
- Re-Synchronizing the Content Distribution Manager with an NTP Server
- Standby Content Distribution Manager Cannot Be Upgraded Through the User Interface
- Deployment of Standby Content Distribution Manager Requires Content Engines in Supernodes to Be Running Version 2.1 or Higher
- Using the RealServer RealSystem Media Commerce Suite
- Encoding Windows Media File Information in the Manifest File
- Limitations on Coverage Zones
- Large Content Engine Log Files May Be Transferred to FTP Host
- Some Features Are Unusable Unless All Devices Are Running the Same Software Version
- Configuration Script for the Content Services Switch Has Been Modified

Accessing CDN Database Tables Using Read-Only Database Views

Cisco has created a way for customers to gain programmatic access to data stored in the CDN Oracle database. Database views provide a look into data that is persisted by the CDM and can be accessed using SQL queries directly against the CDN database.

Information gathered through database views can be then be used to monitor the Content Distribution Network (CDN) for changes.

The following database views are now available:

- CE_VIEW (Detailed information for Content Engine)
- CR_VIEW (Detailed information for Content Router)
- REGION_VIEW
- LOCATION_VIEW
- SUPERNODE_VIEW
- CLUSTER_VIEW
- HOSTEDDOMAIN_VIEW (Hosted Domain information)
- SYS_MESSAGE_LOG_VIEW (System messages - these include liveness information)

- VIRTUAL_CDN_VIEW
- CDM_VIEW
- CUSTOMER_VIEW
- UPDATE_LOG_VIEW
- HOSTEDDOMAIN_TO_CLUSTER_VIEW
- VIRTUAL_CDN_TO_CLUSTER_VIEW
- CONFIG_PROPERTY_VIEW (System configuration properties - including specifications on third party services (applications) running on nodes.

For detailed information and technical documentation on accessing the Cisco Internet CDN database views, please contact your Cisco Account Representative.

Restoring a Deleted Content Distribution Manager to the CDN

Content Distribution Managers (CDMs) that are designated as "standby" CDMs can be deleted from the network. To add deleted CDMs back to the network, use the following procedure:

Step 1 Establish a Secure Shell (SSL) connection to the Content Distribution Manager and log on using your administrative login and password.

Step 2 Enter **register**. This causes the standby device to identify itself to the primary Content Distribution Manager.

Step 3 Point your web browser to the address of the primary Content Distribution Manager and log in to the graphic user interface.

Step 4 Activate the standby Content Distribution Manager through the user interface by following the instructions for "Changing the Warm Standby Content Distribution Manager Role" in Chapter 4: Maintaining Cisco Internet CDN Software of the *Cisco Internet CDN Software User Guide*.

Step 5 Wait for the standby CDM to come online, refreshing the CDM user interface periodically until you see the standby device status change.

When the user interface indicates online status, the CDM is back on the network and has synchronized its database with the other CDM.

Deploying Cisco Internet CDN Behind a Firewall

It is possible to deploy your Cisco Internet CDN behind a firewall. Technical documentation now exists with detailed information on supported and unsupported Internet CDN configurations if you will be deploying behind a firewall as well as port utilization for CDN devices.

For more information and for access to technical information on configuring your CDN behind a firewall, contact your Cisco Account Representative. (Issue CSCdv76716.)

Implementing a Private Ethernet Link to the CDN Database

Version 2.1.1 of the Cisco Internet CDN Software allows you to link your Content Distribution Manager to your designated CDN database server via a secondary, private network interface card (NIC). This allows your CDM to communicate with the CDN database without simultaneously exposing the database host to the larger CDN network.

For more information and for access to technical information on configuring a private ethernet connection to your CDN database, contact your Cisco Account Representative.

Re-Synchronizing the Content Distribution Manager with an NTP Server

The Content Distribution Manager (CDM) acts as the default network time protocol (NTP) server for the CDN. Content Engines and Content Routers synchronize their time with that of the CDM.

However, if the CDM is behind a firewall that blocks access to public NTP servers such as tick.usno.navy.mil, it may be prevented from synchronizing, thus preventing the Content Engines and Content Routers from synchronizing with it.

If this happens, the CDM must be synchronized with an NTP server that it can access—for example, an NTP server that is also located behind the firewall.

To re-synchronize your CDM with an NTP server, you must:

- Identify an NTP server that is accessible to your CDM
- Update the list of NTP servers used by the CDM to include the address of this NTP server, if that address is not already on the list
- Synchronize the CDM with the NTP server

See the sections that follow for detailed instructions on each of these steps.

Identifying an NTP Server for the CDM

To determine whether your CDM can communicate with a NTP server:

Step 1 Use Secure Shell (SSH) to connect to your CDM.

Step 2 Log on to the CDM using the "merlot" account and password. The bash shell will load.

Step 3 At the bash prompt, enter the following command:

```
0 # /etc/rc.d/init.d/xntpd stop
```

Step 4 Next, verify that the CDM is communicating with your recognized public or private NTP server using the following command:

```
0 # ntpdate <ntp_server_name>
```

Step 5 If you receive a message that no suitable server is found at the address you provided, repeat Step 4 until you receive a confirmation.

Update the NTP Server List

Step 1 Once you receive a confirmation, write down the address of the NTP server.

Step 2 Open a web browser and log in to the CDM graphical user interface.

Step 3 Use the System Configuration page to set the address of the NTP server.

Refer to the “Customizing the Network Time Protocol Server List” section in Chapter 4, Maintaining Cisco Internet CDN Software” of the *Cisco Internet CDN Software User Guide* for instructions on adding an NTP server to the list consulted by the CDM.

Synchronize the Content Distribution Manager

Step 1 Reboot the CDM. When the CDM reboots, it will synchronize its time with the NTP server you specified.

Step 2 Once your CDM has synchronized, you can reboot the other nodes in your CDN to force them to synchronize with your CDM.

Refer to Chapter 3: “Working with Cisco Internet CDN Software” in the *Cisco Internet CDN Software User Guide* for instructions on stopping and starting your CDN devices.

Refer to Chapter 4: “Maintaining Cisco Internet CDN Software” in the *Cisco Internet CDN Software User Guide* for instructions on adding an removing NTP servers from the list consulted by the CDM.

Standby Content Distribution Manager Cannot Be Upgraded Through the User Interface

To upgrade a standby Content Distribution Manager (CDM):

Step 1 Log in as **admin** to a Secure Shell (SSH) session with the CDM.

Step 2 Load the upgrade file onto the CDM by entering the following commands:

```
ftp
ftp> open ftp.cisco.com
ftp> username: CCO_user_account_name
ftp> password: CCO_account_password
ftp> passive
ftp> cd/cisco/content-delivery/cdn/sp
ftp> get upgrade_filename
ftp> bye
Host> enable
Host# upgrade swupgrade
```

When the upgrade is complete, the CDM will reboot itself.

Deployment of Standby Content Distribution Manager Requires Content Engines in Supernodes to Be Running Version 2.1 or Higher

While versions 2.1 or higher of the Cisco Internet CDN Software support CDNs in which some nodes are running earlier (2.0.x) CDN software releases, if you have deployed a failover Content Distribution Manager (CDM) and supernodes on the same CDN, it is necessary to update the software on *all* Content Engines and Content Routers in your supernodes to Version 2.1 or higher so that those supernodes can continue to communicate with the failover CDM.

Using the RealServer RealSystem Media Commerce Suite

The RealServer RealSystem Media Commerce Suite (RSMCS) has not been shipped with the software. (Caveat CSCdv66612). You must instead purchase the appropriate RealServer RSMCS plug-in from Real Networks and then install it on a Content Engine running Version 2.1 or later of the Cisco Internet CDN Software. For Version 2.1.1 a special command, **real rsmcs**, has been implemented to streamline deployment of the plug-in.

Note For RealMedia content that you want protected by RSMCS, specify the playserver property as “real” in the manifest. For example, if you have an RSMCS file named foo.rms, and want the cdn-url to be *cdn_foo.rms*, the item in the manifest file should read:

```
<item playserver="real" src="/foo.rms" cdn-url="/cdn_foo.rms">
```

Once you have obtained the plug-in, follow these steps to install it on your Content Engine:

Step 1 Verify that the plug-in file you have is rmffplin-linux.so.6.0, the Linux version that you need for the Cisco Internet CDN.

Step 2 Log in to the Content Engine on which you will be deploying the Commerce Suite.

Step 3 Transfer the plug-in to the cisco/merlot/state directory on the Content Engine using the **scp** or **ftp** commands.

Step 4 Enter enabled mode. For example:

```
Host>enable
Host#
```

Step 5 Enter the following command:

```
Host#real rsmcs
```

The RealSystem Media Commerce Suite (RSMCS) Plugin Administration menu appears.

Step 6 Choose option 1 to add your RSMCS license.

Step 7 Restart the Cisco Internet CDN Software by entering **control restart**.

Encoding Windows Media File Information in the Manifest File

In previous Cisco Internet CDN Software releases, if a HTTP URL was contained in a published ASX file, file information (like author and copyright) contained in the ASX file was not displayed on the player. The use of HTTP URLs is integral to the functioning of hybrid routing on the CDN.

In Version 2.1.1 an attribute, streamProperty, has been added to the <item/> and <item-group/> tags for use with Windows Media files (WMA, WMV, and ASF) only.

Note The streamProperty attribute only works with Windows Media Player Version 7.0 and later.

This attribute specifies one or more file properties that are displayed in the Windows Media Player when the file is played.

The supported attributes are:

- abstract
- title
- author
- copyright

For example, a manifest file might contain the following syntax:

```
<CdnManifest>
<server name=“origin-server”>
<host name=”www.name.com”
proto="http"
port="80" />
</server>
<item cdn-url= “q4results.asf”
server=”originserver”
src= “video/q4results.asf”
type=“live”
playserver=“wmt”
streamProperty = "author='paul roberts'
title='Cisco Q4 Results'  copyright='Cisco 02'"
ttl=300/>
</CdnManifest>
```

Limitations on Coverage Zones

For coverage zones to work, all Content Routers must be running Cisco Internet CDN Software Version 2.1 or higher. Coverage zones for a particular hosted domain work only if all Content Engines serving that hosted domain are running Internet CDN Software Version 2.1 or higher.

Large Content Engine Log Files May Be Transferred to FTP Host

If Content Engine log files exceed the size limit specified on the Tools > Remote Logging page on the Content Distribution Manager graphic user interface while still being generated, they are transferred to the FTP remote logging host. Existing log files are not affected in this way.

Some Features Are Unusable Unless All Devices Are Running the Same Software Version

A CDN comprised of devices using mixed versions of the Cisco Internet CDN Software is supported. However, some features are unusable in the CDN unless *all* devices are running the same version. These features are:

- Windows Media Technologies (WMT) support—If you want to serve WMT for a hosted domain, you must ensure that all Content Engines serving that hosted domain are running Version 2.1 or higher.
- Hybrid routing—To use the hybrid routing feature, all CDN devices need to be running version 2.1 or higher.
- Warm standby Content Distribution Manager (CDM)—CDN devices that are not running Version 2.1 or higher will not be aware of the standby CDM.

Configuration Script for the Content Services Switch Has Been Modified

The Content Services Switch (CSS) configuration script has been modified to allow you to add as many interfaces to a VLAN as are available on the CSS. In prior releases, a maximum of 32 interfaces was imposed for any single VLAN. After you assign a number to the VLAN, you are asked to assign interfaces in increments of ten. For example:

```
What is the number (1-4095) of this VLAN? [default = 1] 821
Configuring interfaces bridged to this VLAN...
How many interfaces are bridged to this VLAN? 56
Please input interfaces from 1 to 10: Separate them by space.
1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 2/1 2/2
Please input interfaces from 11 to 20: Separate them by space.
2/3 2/4 2/5 2/6 2/7 2/8 3/1 3/2 3/3 3/4
```

Do not input fewer than ten interfaces, unless there are no more to enter. The script asks you to input interfaces only as many times as it takes for you to enter all the bridged interfaces in increments of ten.

For example, if you entered 56 as the number of interfaces you would like bridged to the VLAN, the script will prompt you six times. The script does not check to ensure that you input as many interfaces as you initially asked for. If you fail to enter all the interfaces in this sequence of the script, you must run the script again until all interfaces are accounted for.

Important Notes for Content Providers

This section describes guidelines that content providers need to follow when modifying their web site to place content on their CDN. It also describes the behaviors that users accessing their CDN-enabled content can expect to see. The topics covered are:

- Windows Media Player Plug-In Required for a Netscape Browser
- Uppercase Tags Should Not Be Used in Content URLs
- Automating Manifest File Generation
- Using the Manifest Validator to Validate Manifest File Syntax

Windows Media Player Plug-In Required for a Netscape Browser

If the end user has Windows Media Player Version 7.1 installed and tries to open a Windows Media Technologies (WMT) file in a Netscape Version 4.76 browser, an error message may appear, saying “Invalid or corrupt data was encountered.” Content providers should inform end users that if they encounter this error message, they may need to install a Window Media Player plug-in for Netscape. To download the plugin, end users should:

Step 1 Go to http://www.microsoft.com/windows/windowsmedia/download/default.asp.

Step 2 In the Select Version field, choose **Player Plugin for Netscape** from the drop-down menu.

Step 3 Click the **Download Now** button to download the plug-in.

Uppercase Tags Should Not Be Used in Content URLs

Browsers display a “Page Not Found” message and fail to stream content if the CDN tag in the content URL has uppercase letters, for example:

```
http://hosted_domain/CDN-MEDIA/filename.xx.
```

Automating Manifest File Generation

This section contains information that you can use to automate the creation of manifest files for your website:

- Overview
- Installing PERL on Your Workstation
- Obtaining the Scripts
- Listing Website Content Using the Spider Script
- Spider Script Syntax Guidelines
- Combining Spider Data
- Customizing the Spider Script
- Selecting Live and Pre-Positioned Content Using the Manifest Script
- Manifest Script Syntax Guidelines
- Customizing the Manifest Script
- Creating a Rules File for the Spider and Manifest Scripts

Overview

Two sample scripts are provided to you:

- Spider—Crawls over the content of an origin server and outputs a database file containing a list of URLs for all *potentially* pre-positioned or live content objects on that origin server, regardless of whether that content will eventually be pre-positioned or streamed live from the hosted domain
- Manifest—Reads the database file output by the spider script and, using rules set out by the content provider, produces an XML-format manifest file containing the URLs of just those items or types of content that a Content Provider wants to make available to users through a hosted domain.

These scripts shipped with your CDN software and can serve as the basis for your own automation scripts.

Installing PERL on Your Workstation

You need to have PERL installed on your workstation before to working with or running the spider or manifest scripts. It may also be useful to have a PERL compiler available. PERL is open source software and can be downloaded for free from a variety of locations on the Internet. Refer to the Comprehensive PERL Archive Network (CPAN) at http://www.cpan.org, or http://www.perl.com.

Obtaining the Scripts

The spider and manifest scripts can be obtained from Cisco.com using the same procedure that is used to obtain updated versions of the Cisco Internet CDN Software.

To obtain the scripts from Cisco.com:

Step 1 See the "Step 2—Adding a New Update File" section on page 5, for instructions on locating the Internet CDN Software Download area of Cisco.com.

Step 2 When you are asked to locate the files you wish to download, look for the file named *manifest-tools.zip*. This is a ZIP archive containing both the manifest and spider PERL scripts.

Step 3 Follow the rest of the instructions to download the manifest-tools.zip file from Cisco.com.

Step 4 Use your preferred unzip program to unpack the scripts to a location on your workstation or your network.

Listing Website Content Using the Spider Script

This section contains information on the following topics:

- Spider Script Syntax Guidelines
- Combining Spider Data
- Customizing the Spider Script

In the simplest scenario, the spider script is pointed to the address of an origin server and given the name of a database (.db) file into which it will place any valid URLs it discovers on that site. For example, if you wanted to analyze the contents of www.cisco.com for content that might be pre-positioned, you would issue the following command:

```
spider --start=www.cisco.com --db=ciscocontent.db
```

Limiting Scope

But running the spider script on all of www.cisco.com might take too long and produce more information than you want. What if you want to limit your review of an origin server to just a particular part of that server? The spider script contains a variety of tools that enable you to limit as well as broaden the scope of the search action.

For example, to limit the search of www.cisco.com to just that part of the server containing product-related support information, you could enter the following command:

```
spider --start=www.cisco.com/public/support/ --db=ciscocontent.db
```

Broadening Scope

To ask the spider script to broaden its search and follow links from www.cisco.com to the Cisco networking professionals forum, you could enter the following spider command:

```
spider --start=www.cisco.com --allow=forums.cisco.com --db=ciscocontent.db
```

Running the Spider Script Against Servers More Than Once

In addition to searching new origin servers, the spider script can also be run on sites that have already been analyzed and that contain links to the CDN. When running the spider script on a server that has already been analyzed, you use the **--hd** keyword to specify the name of hosted domain on which content from the origin server will be hosted, and the **--map** keyword to provide mapping information between URLs on the origin server and on the Internet CDN.

For example, the following commands will trace the content mapped to the /support area on the hosted domain www.hosted.cisco.com back to its origins in the support area of www.cisco.com:

```
--start=http://www.cisco.com/public/support/tac/home.html
--hd=www.hosted.cisco.com
--map=http://www.cisco.com/public/support/tac/=/support
--db=ciscocontent.db
```

In each of the examples listed above, the spider script analyzes the URL of each piece of content on the origin server or in that area of the origin server that has been targeted and applies filters to the content that incorporate the parameters supplied when the spider script was run previously, identifying potential pre-positioning or live streaming candidates. If the URL matches the pattern provided by the spider script search, it is accepted and its URL is recorded in the database being created by the script. If the pattern does not match, the content is rejected and the spider script search moves on.

Spider Script Syntax Guidelines

The spider script uses the following syntax:

spider {**--start**=*origin_server_url*
[**--allow**=*allowed_url* | **--depth**=*number* | **--file**=*filename* |
{**--hd**=*hosted_domain_name* **--map**={*origin_server_url_prefix*=*cdn_prefix*} } |
--limit=*number* | **--prefix**=*url_prefix* | **--reject**=*disallowed_url* |]
--db=*database_name*.**db**}

Table 1describes the spider script keywords.

Table 1 Spider Script Keywords

Keyword	Description	Syntax
--start	Names the location (URL) of the origin server that will be analyzed.	`--start=www.cisco.com`
--allow (optional)	Names a location other than that specified using the **start** keyword that will be accepted when it is found in URLs.	`--allow=forums.cisco.com`
--db	Names the database file in which content URLs from the origin server and any allowed locations will be placed.	`--db=ciscocontent.db`
--depth (optional)	Causes the spider script to stop after following links a specified number of levels deep on the origin server.	`--depth=6`

Table 1 Spider Script Keywords

Keyword	Description	Syntax
--file (optional)	Causes the spider script to read its commands from a specified rules file, one line at a time.	`--file=cisco-rules.cfg`
--hd (optional)	Identifies a hosted domain on your CDN as the hosted domain for the content being searched by the spider script. Used with the **--map** keyword for mapping content from the CDN back to the origin server.	`--hd=www.hosted.cisco.com`
--limit (optional)	Causes the spider script to stop after retrieving a specified number of pages from the origin server. The default is 100. Specifying 0 sets no limit for the number of pages retrieved.	`--limit 1000`

--map (optional)	Causes the spider script to substitute the second URL prefix (appearing after the second =) for the first in any URLs from the origin server, or substitute the first prefix for the second when running the spider script a second time on origin server content.	`--map=http://www.cisco.com/`
		`public/support/tac/=/support`

--prefix (optional)	Specifies a URL prefix that will be accepted by the spider script when it is encountered.	`--prefix=http://www.cisco.co`
		`m/partners/CDN/`

--reject (optional)	Names a location that will be rejected when it is found in URLs.	`--reject=cgi-bin`

Combining Spider Data

You can run the Spider script on two separate locations on an origin server and then combine the content into one database from which a manifest file will be generated.

To combine spider script data:

Step 1 Open the *.db file containing the data you want to move, select that data and copy it.

Step 2 Open the *.db file you want to serve as the merged file.

Step 3 Locate the end of the file, and paste the data you copied into it.

The manifest script can now be run on the merged data. See the "Manifest Script Syntax Guidelines" section on page 20,.

Customizing the Spider Script

Because the Spider script anticipates certain platforms and scenarios that might not correspond to your own website configuration, Cisco provides you with the PERL source code for the spider script, which you can modify to suit your own needs.

See the "Obtaining the Scripts" section on page 17, for instructions on downloading the spider script from Cisco.com.

Selecting Live and Pre-Positioned Content Using the Manifest Script

Whereas the spider script is used to gather a list of potential hosted content from an origin server, it is in the manifest file that you analyze all the information gathered by the spider script and decide which content you will actually import to the CDN for placement on a hosted domain.

This section contains information on the following topics:

- Manifest Script Syntax Guidelines
- Customizing the Manifest Script

Pre-Positioned versus Live Content

The manifest script distinguishes between content that needs to be pre-positioned and live, streamed content that by definition cannot be pre-positioned.

Using the **prepos** command, you identify and pre-position all content which meets criteria that you specify. For example, to pre-position all image files from cisco.com larger than one megabyte, you would enter the following command:

```
manifest --prepos=’type(image/*) and size > 1000k’ --db=ciscocontent.db --xml=cisco.xml
```

Using the **live** command, you identify the URLs of live content. Unlike pre-positioned content, live content cannot be identified by information stored in the header, so you will need to devise a method of locating live content based solely on information contained in the URL of that content. For example, you might identify streamed content with the following command:

```
manifest --live=‘match(rtsp://*)’
```

Manifest Script Syntax Guidelines

The manifest script uses the following syntax:

manifest {[**--file**=*filename* | **--live**=’*keyword_comparison*’ | **--prepos**=‘*keyword_comparison*’ | **--set**=‘*attribute*=*value* : *keyword_comparison*’ | **--playservertable**=*filename* | **--map**={*origin_server_url_prefix*=*cdn_prefix*}] **--db**=*database_name*.**db** **--xml**=*manifest_file_name*.**xml**}

Table 2 describes the manifest script keywords.

Table 2 Manifest Script Keywords

Keyword	Description	Syntax
--file	Causes the manifest script to read its commands from a specified rules file, one line at a time.	`--file=ciscocontent.cfg`
--live	Marks content URLs in the database file that match the terms of the keyword comparison as live (type=“live”) content in the manifest file.	`--live=‘match(rtsp://*)’`
--prepos	Marks content URLs in the database file that match the terms of the keyword comparison as pre-positioned content (type=‘prepos’) in the manifest file.	`--prepos=‘type(image/jpg) and size > 1000k’`

Table 2 Manifest Script Keywords

Keyword	Description	Syntax
--set	Sets the specified attribute to the value provided for all content items with URLs in the database file that match the keyword comparison.	`--set='ttl=10000 : match(*/urgent/*)'`
--playservertable	Adds the playserver table in the specified file to the manifest file. Playserver tables map MIME content types and filename extensions to specific server types to use (for example, "real" or "wmt") for the content in a specific hosted domain.	`--playservertable=info.txt`
--map	Causes the manifest script to substitute the second URL prefix (appearing after the second =) for the first in any URLs from the origin server.	`--map=http://www.cisco.com/ public/support/tac/=/support`
--db	Names the database file in which content URLs from the origin server and any allowed locations are located. This file provides the data that the manifest script analyzes.	`--db=ciscocontent.db`
--xml	Names the manifest file that is generated by the manifest script.	`--xml=ciscomanifest.xml`
match	Comparison keyword that locates text in content URLs that are identical to a value that is provided.	`--prepos='match (http://forums.cisco.com/*)'`
size	Comparison keyword that identifies content named in the database file according to the specified file size parameter (in kilobytes).	`--prepos='size >= 1000k'`
time	Comparison keyword that identifies content named in the database file according to the time since the content was last modified (in hours).	`--prepos= 'time < 72 hours'`
type	Comparison keyword that identifies content named in the database file according to its MIME type (text, application, image, and so on).	`--prepos='type(image/gif)'`

Customizing the Manifest Script

Because the manifest script anticipates certain platforms and scenarios that might not correspond to your own website configuration, Cisco provides you with the PERL source code for the manifest script, which you can modify to suit your own needs.

See the "Obtaining the Scripts" section on page 17, for instructions on downloading the manifest script from Cisco.com.

Creating a Rules File for the Spider and Manifest Scripts

When using the spider and manifest scripts on a large web server, the parameters and rules you set for your scripts may be numerous and complex. When this is the case, it may make more sense to create a file containing all your instructions to the scripts that you can then simply point to rather than having to type a long series of commands again and again.

Using a rules file makes it easy to rerun the spider and manifest scripts and be confident that the scripts are receiving identical commands each time. In addition, the same rules file can be read by both the manifest and the spider scripts without generating incorrect output; the spider script simply ignores commands for the manifest script, and vice versa.

To create a rules file for the spider and manifest scripts to use:

Step 1 Open your preferred text editor.

Step 2 Enter your commands one at a time, each on its own line. Each line of your rules file is sent to the scripts as a single argument.

For example, a rules file for the Cisco website might read:

```
--start=www.cisco.com
--allow=forums.cisco.com
--reject=cgi-bin
--limit=0
--db=ciscocontent.db
--prepos=‘match(image/gif) and size > 1000k’
--xml=ciscomanifest.xml
```

Step 3 Save your file in a location relative to the spider and manifest scripts.

Step 4 Use the **file** command to run each script using your rules file. For example:

```
spider --file=cisco-rules.cfg
manifest --file=cisco-rules.cfg
```

Using the Manifest Validator to Validate Manifest File Syntax

Because correct and accurate manifest file syntax is vital to the proper deployment of your website content on the CDN, Cisco makes a manifest file syntax checker available at no cost to its customers. This command-line-based utility can be used to proof the manifest files that you have created for your hosted domain.

When run, the manifest validator reviews each line of your manifest file, identifying syntax errors where they exist and determining whether or not the manifest is valid and ready for use in importing content to your hosted domain. The results of the manifest validator’s review of the manifest file are output to a text file in a location that you name.

The manifest validator is designed to run in the Windows (95/98, NT, 2000 and XP) and the Linux (RedHat 6.2) environments.

This section contains the following topics:

- Obtaining the Manifest File Validator
- Installing the Manifest File Validator
- Running the Manifest File Validator

- Understanding Manifest File Validator Output
- Repairing Manifest File Syntax

Obtaining the Manifest File Validator

The Manifest Validator utility can be obtained without cost from Cisco.com using the same procedure that is used to obtain updated versions of the Cisco Internet CDN Software.

To obtain the scripts from Cisco.com:

Step 1 See the "Step 2—Adding a New Update File" section on page 5, for instructions on locating the Internet CDN Software Download area of Cisco.com.

Step 2 When you are asked to "locate the files you wish to download," look for the file named *manifest-validator.zip*. This is a ZIP archive containing the validator utility.

Step 3 Follow the rest of the instructions to download the manifest-validator.zip file from Cisco.com.

Step 4 Use your preferred unzip program to unpack the utility to a location on your workstation or your network. Make sure all validator files are unzipped to the same location.

Installing the Manifest File Validator

Before installing the manifest validator, you must first install the Java (TM) 2 Runtime Environment, Version 1.2 or 1.3 on your workstation. The Java 2 Runtime Environment (JRE) contains the Java virtual machine, runtime class libraries, and Java application launcher. These components are necessary to run the Cisco manifest validator utility.

If you are using an earlier version of the JRE on your workstation, install either Version 1.2 or 1.3. You can download the latest version of the JRE along with instructions for installing it from the following web site:

```
http://java.sun.com
```

After you install the JRE, use the following instructions to install and run the Cisco manifest validator utility:

Step 1 Create a directory for the manifest validator on your local drive. For example:

```
c:\manifest
```

Step 2 Locate the manifest validator archive, *manifest-validator.zip*, that was provided to you by your service provider.

Step 3 Unzip the manifest validator files into the directory you created.

Step 4 Verify that all manifest validator files are present in the manifest directory you created. Table 3 contains a list of the sources files that constitute the manifest validator utility and their purpose.

Table 3 Manifest Validator Source Files

Validator File Name	Purpose
xerces.jar	Syntax parser
manval.zip	Standalone manifest validator
CdnManifest.dtd	Document type definitions for the CDN manifest file
PlayServerTable.dtd	Document type definitions for CDN PlayServerTables, used to define media servers (RealMedia, Windows Media) for the CDN
validate	Shell script used to run the validator
validate.bat	Batch file to run the validator

Running the Manifest File Validator

Once you have installed the Java 2 Runtime Environment and the Cisco manifest validator program files, you are ready to run the validator on a manifest file that you have created.

The manifest file validator can be run in one of two modes:

- Default mode—The manifest validator checks the syntax of your manifest file to make sure that source files are named for each content item in the manifest.
- Check size mode—The manifest validator checks the syntax of your manifest file to make sure that source files are named for each content item in the manifest. It then follows the URL for each content item to verify that the content is placed correctly and, if possible, to determine the size of the item. A special switch (-s) is used to run the validator in check size mode.

When running the manifest file validator, you are required to input the following information:

- Name and location of your manifest file, expressed either as a network file location <file> or a valid Internet URL <url>
- Name and location of the manifest validator's output file <output>.
- (Optional.) When the manifest file validator is used in check size mode, the length of time <seconds> that the manifest file validator should attempt to confirm the existence of content named in the manifest

To run the manifest validator utility:

Step 1 If you are running Windows, open a command prompt. Otherwise, proceed to Step 2.

Step 2 Change directories to the program directory for the manifest validator. For example, if you are running Windows, you would enter the following at the command prompt:

```
C:\>cd manifest
C:\manifest>
```

Step 3 Run the manifest validator as follows:

- If you are running Windows, enter the validate command and provide either a path and filename or URL pointing to your manifest file in the following format:

  ```
  validate -f [<file> | -u <url>] -o <output> [-s <seconds>]
  ```

- If you are running Linux, enter the following commands, providing either a path and filename or URL pointing to your manifest file in the following format:

  ```
  chmod u+x validate
  ```

```
validate -f [<file> | -u <url>] -o <output> [-s <seconds>]
```

Once you execute the validator, text output is displayed, indicating that the validator is running.

Step 4 Wait until the following message is displayed, indicating that the validator has completed processing the manifest file you pointed to:

```
Finish parsing /<manifest_file_name>.xml
```

Step 5 Locate the output file in the location that you specified and review it for errors.

The final lines of the manifest file validator's output will indicate whether or not the manifest is valid or not. For example, a valid manifest file output might read:

```
number of manifest warnings: 1
number of manifest errors: 0
manifest syntax is CORRECT
finish parsing
```

In this instance, one nonfatal syntax irregularity was located, but the manifest file was found to be syntactically correct. This file could be transferred to your service provider and used to deploy website content to your CDN.

The output file for an invalid manifest file will list the number of errors and warnings issued, for example:

```
number of manifest warnings: 1
number of manifest errors: 1
manifest syntax is INCORRECT
finish parsing
```

See the next section, "Understanding Manifest File Validator Output" for detailed information that will help you understand the manifest file validator results.

Understanding Manifest File Validator Output

Your manifest file validator output file will appear in the location you specified (using the -o option) when the validator was run.

Each output file has a similar structure and syntax and clearly identifies any errors or warning messages stemming from your manifest file syntax. Manifest files are judged by the validator either to be:

- CORRECT—Possibly containing syntax irregularities, but syntactically valid and ready for deployment on a CDN
- INCORRECT—Containing syntax errors and unsuitable for deployment on a CDN

Syntax Errors

The manifest file validator issues syntax errors only when the manifest file validator cannot identify a source file for a listed content item, either because it is not listed, or it is listed using improper syntax. All files containing syntax errors are marked INCORRECT.

Syntax errors are identified in the output with the ERROR label. In addition to the label, the line number containing the error is provided, as well as the manifest attribute for which the error was issued, valid options, and the default value for that attribute. For example, the following error appears in Example 1:

```
ERROR: japan.xml:13:Skip item because src is not defined.
```

In the preceding error message:

- *japan.xml* is the manifest file name
- *13* is the manifest file line number where the error occurs
- *src* is the manifest file attribute generating the warning

Example 1 Manifest File Validator Output Containing Errors and Warnings

```
start parsing file japan.xml
start options
 option clearlog: false
 option rd: null
 option prepos-tag: null
 option live-tag: null
 option notFoundUrl: null
 option noRedirectToOrigin: false
 option timezone: JST
 option manifest-id: null
end options
start server
 server name: WMTServer
start host
  host name: origin.cdn-japan.com
  host proto: http
  host port: 80
  host user: ceadmin
  host password: 3kDC
  creating new hash entry for WMTServer and origin.cdn-japan.com
 end host
end server
WARNING: japan.xml:13:Attribute "src" is required and must be specified for element type
"item".
start item
 item src: null
 ERROR: japan.xml:13:Skip item because src is not defined.
end item
end CdnManifest
number of items processed: 1
number of manifest warnings: 1
number of manifest errors: 1
manifest syntax is INCORRECT
finish parsing
```

The total number of errors encountered in the manifest file is provided at the end of the validator output file.

Syntax Warnings

The manifest file validator issues syntax warnings for a wide variety of irregularities in the manifest file syntax. Files containing syntax warnings may be marked CORRECT or INCORRECT, depending on whether or not syntax errors have also been issued.

Syntax warnings are identified in the output with the WARNING label. In addition to the label, the line number containing the warning is provided, as well as the manifest attribute for which the warning was issued, valid options, and the default value for that attribute. For example, the following warning might appear in the output for the japan.xml manifest file:

```
WARNING: /~content/manifest/japan.xml:12:Attribute “type” with value "vod" must have a value
from the list "(prepos|live)"
```

In the preceding warning message:

- *japan.xml* is the manifest file name

- *12* is the manifest file line number where the warning was issued
- *type* is the manifest file attribute generating the warning
- *vod* is the offending value
- (*prepos* | *live*) are the valid options for that attribute

The total number of warnings encountered in the manifest file is provided at the end of the validator output file.

Repairing Manifest File Syntax

Once you have identified syntax errors and warnings using the output from the manifest file validator, you can correct your manifest file syntax and then rerun the manifest file generator on the corrected file.

To repair your manifest file:

Step 1 Open your manifest file using your preferred XML editor.

Step 2 Referring to your manifest file validator output, use the line numbers provided by the manifest file validator to locate the syntax violations in your manifest file.

In general, it is a good idea to review each WARNING and ERROR tag in your manifest. Some warnings, although they still allow the manifest file validator to find your manifest file syntax correct, may still be the source of problems when you deploy your website content.

Step 3 After you have made all necessary corrections for syntax warnings and errors, save your manifest file.

Step 4 Run the manifest file through the manifest file validator again, and review the validator output for errors and warnings.

Step 5 Repeat Step 1 through Step 4 until all errors and warnings have been adequately resolved and until the manifest validator labels your manifest file CORRECT.

Caveats

Caveats describe unexpected behavior in Cisco Internet CDN Software.

- Severity 1 caveats are deemed critical.
- Severity 2 caveats are serious, but not critical.
- Severity 3 caveats are of moderate seriousness and are only selectively included in the release notes documentation.

This section describes the caveats--both resolved and unresolved--that are associated with Version 2.1.1 of Cisco Internet CDN Software.

Open Caveats

The following caveats are open (unresolved). Unresolved caveats are listed according to their tracking number.

- CSCdt96485

  The QuickTime server runs even if you disable it.

- CSCdu04445

  After you run netsetup on a Content Engine 7320, you see the following message:

  ```
  epro100: Device or resource busy rmmod: module acenic is not loaded
  ```

  You can ignore this message.

- CSCdu21113

  The Supernode page allows you to create multiple supernodes with one Content Services Switch (CSS), even though creation of multiple supernodes on a single CSS is not supported. If you erroneously create multiple supernodes on one CSS, you should delete all supernodes associated with that CSS, and then create only one supernode.

- CSCdu24791

  The sort indicator on the View Supernode page does not appear after you click the Refresh button.

- CSCdu38518

  To preserve security, FTP is disabled on the Content Services Switch (CSS) by default. To transfer upgrade files to a CSS, you need to enable FTP on the switch. After you have transferred the file, you should disable FTP again.

- CSCdu41069

  When an inactive Content Engine or Content Router is registered, the Modify Content Engine or Modify Content Router page initially displays the fully qualified domain name (for example, ce590-1.canada.org). Once the Content Engine or Content Router reboots for the first time and comes online, only the host name (for example, ce590-1) is displayed on the user interface. This does not impact the routing capability of the CDN.

- CSCdu42467

  The clock on a device is not updated if the Network Time Protocol (NTP) server is inaccessible while the device is booting. To avoid this, you should wait until the NTP server is available and then reboot the device.

- CSCdu44384

  When a RealServer license expires on a Content Engine, an error message indicating the expiration is not logged. An expired RealServer license prevents the Content Engine from serving content through the RealServer.

- CSCdu45008

  If you delete a supernode from the CDM and then create a new supernode that is identical to the deleted one, all Content Engines associated with the re-created supernode must be rebooted to function properly. If they are not rebooted, they fail to serve content.

- CSCdu50308

  In the command-line interface, if you run setup remotely through Secure Shell (SSH) using the Dynamic Host Configuration Protocol (DHCP) address, you are disconnected from the device when netsetup is completed. You can reconnect to the device by using the IP address you specified during setup.

- CSCdu53388

  In Netscape, if you try to assign Content Engines to a hosted domain and fail to select a root location, the user interface does not display a warning message; it accepts the change when you click the Save button. If you do this using Internet Explorer, the user interface tells you that you must specify a root location.

- CSCdu56255

The system allows you to surpass the limit on the number of content items you can assign to a Content Engine (CE). When you have reached the limit, the CE warns you that you have reached the limit but allows you to assign further items. By default, the limit is set to 500,000 items, but the CE-7320 can support up to 1 million.

- CSCdu57706

  The **dnslookup** command in the command-line interface does not function as documented; it fails to resolve the host name of an IP address that you enter.

- CSCdu57718

  If you enter the show logs command-line interface command during a period of high end user activity on the system, the log output gets stuck on the SQuID log (the SQuID log records HTTP requests for content). To break out of this command, press Ctrl-C. To view selected logs, use the **view** *path_of_log_file* privileged level EXEC command. The following log files are available:

  – /cisco/merlot/state/merlot.log

  – /cisco/merlot/state/apache/log/*_log

  – /cisco/merlot/state/squid/logs/*.log

  – /cisco/merlot/state/sysout/*.log

- CSCdu60211

  If you have assigned a Content Engine (CE) to a location, you must manually restart the CE if you later change it to a different location through the Content Engine Details page. Otherwise, your routing performance will not be optimal.

- CSCdu64147

  While you modify a supernode cluster, an extra row is added to the Content Engine table.

- CSCdu66216

  On the Software Update page, the file at the top of the list of upgrade metafiles is selected by default. When you choose a different file, this choice is not perpetuated to all the other device tabs. Under the other device tabs, the file at the top of the list remains as the default. You must choose the upgrade file for each device individually.

- CSCdu69371

  Content Engines fetch the manifest file from the origin server instead of the hosted domain leader Content Engine. This is by design.

- CSCdu70671

  When you attempt to update a CDN password, the ! icon appears next to the wrong field after an incorrect value is entered into the Old Password field.

- CSCdu71747

  Password verification is limited to the first eight characters of the password.

- CSCdv44831

  If you use a browser that does not have cookies or JavaScript enabled, you receive a session timeout message. For the user interface to function, you must have both cookies and JavaScript enabled in your browser options.

- CSCdv47796

Do not downgrade a Content Distribution Manager (CDM) from the user interface; doing so may corrupt your database's table structure. Instead, downgrade your CDM through the command-line interface using the **upgrade** command. For more information on using the command-line interface, refer to the *Cisco Internet CDN Software Command Reference* for Version 2.1.

- CSCdv52128

  In Internet Explorer, next-click failover does not work for Windows Media Technologies (WMT) 7.1 content requested through HTTP. If you send HTTP requests through an Internet Explorer browser after a Content Engine failure behind a supernode, you need to take one of the following actions:

  - Go back to the original HTTP URL and click it again.
  - Do a refresh for any URL you enter in the browser location field.
  - Publish the HTTP URL as a web link.

  If you are using Internet Explorer 6.0, you can also get next-click failover by closing the WMT player, entering the HTTP URL directly into the browser location field, and then pressing Enter.

- CSCdv62694

  The peekable interface is disabled by default on Content Engines and Content Routers. If you do not enable the peekable interface:

  - You receive a "Page not found" error when clicking on a Content Engine on the Hosted Domains > Replication Status page.
  - You cannot access the Java Monitor for RealServer.
  - You cannot view the Tools > System Tools > Simple Peek page for the device, which you use to enable or disable Telnet and debugging.
  - You cannot view manifest log files for hosted domains.

  To enable the peekable interface, enter the **node peekable** command in the command-line interface. For more information, refer to the *Cisco Internet CDN Software Command Reference* for Version 2.1.

- CSCdv62704

  In a single software upgrade transaction, you can upgrade only the devices on one page. When you choose the check-all check box on the Upgrade Software page, all of the devices on that web page are selected. If you then go to the next page and choose all the devices, the devices on the first page are deselected.

- CSCdv64154

  When you are running setup on a Content Distribution Manager (CDM), you are prompted to enter the Oracle database username that you specified during Oracle configuration. You should not use the username of the database account to which you assigned administrator privileges. Doing so causes problems during upgrades and downgrades. If you only created one user account during database setup and gave it administrator privileges, you have to run the **setup** command to create a second user without administrator privileges. Once you have done so, you can rerun dbsetup on the CDM.

- CSCdv65761

  If you have Content Engines with Version 2.0.1 and a Content Router that never rebooted after Version 2.0.1 was installed on it, you must reboot the Content Router before upgrading it to version 2.1. If you do not reboot prior to upgrading, Content Engines running Version 2.0.1 will lose contact with the Content Router until they are rebooted.

- CSCdv70049

  The **no** command that appears in the command-line interface configuration menu is nonfunctional.

- CSCdv80269

  Your Content Engine may stall during a Version 2.0.1 to Version 2.1 software upgrade. If this happens, you need to reboot the Content Engine and repeat the upgrade procedure.

- CSCdv84379

  When you change the status of a Content Distribution Manager from primary to standby, the change is not recorded in the system log.

- CSCdv88053

  If you enter a video on demand (VOD) quota setting on a Content Engine by using the **node diskadmin** command-line interface command, the change is not registered. Changes made through the Content Distribution Manager (CDM) user interface are registered. This may cause a discrepancy between the VOD quota value that the CDM user interface displays and the value that the command-line interface **show disk** command displays.

- CSCdw14298

  You are unable to use the command-line interface (CLI) following a CLI downgrade. Following reboot of the device, the CLI session disconnects and if you attempt to reestablish a CLI connection, you see an error message similar to the following:

  ```
  Last login: Wed Dec  5 19:39:09 2001 from
  dhcp-161-44-174-117.cisco.com/cisco/merlot/state/dump/home/script-4364: No such file
  or directory
  Command terminated on signal 15."
  ```

  Workaround:

  To downgrade from 2.1.0.0.27 to 2.0.1.0.6:

  - Login in to the box as "root" using the bash shell.
  - Type your device password.
  - At the :: prompt type the 867...password.
  - mkdir -p /cisco/merlot/state/dump/home
  - exit out of bash.

- CSCdw16838

  It is not possible to disable the peekable system configuration property on the Content Distribution Manager, regardless of the setting of the enablePeekable property. This is because both peekable and the Content Distribution Manager user interface use the same port so if you disable peekable, the Content Distribution Manager user interface is also disabled.

- CSCdw28253

  SMIL files do not play reliably if distributed licensing is enabled on RealServer. When the enduser requests a SMIL file, the RealPlayer stalls and there is an indefinite delay in playback.

  Workaround:

  Disable distributed licensing until a fix is available.

- CSCdw36766

  You can only access one Content Distribution Manager user interface from one host. Multiple CDNs cannot be accessed at the same time by the same client.

- CSCdw41627

  When playing Windows Media Technologies (WMT) files through a Netscape browser that has not had a start page defined, only the first content file for a hosted domain plays per Netscape session.

Workaround:

Select the Home Page option in Netscape's Preferences dialog and provide a unique URL for that page in the field provided. Do not choose either the Blank Page or Last page visited options.

- CSCdw54426

  Content Distribution Manager User Interface upgrade fails, with the following error, then corrects:

  ```
  Database upgrade failed. Use cli upgrade --rollback to repair. [runmode = 1]
  ```

  Workaround:

  - Log on to the Content Distribution Manager Cisco Command Line Interface.
  - Execute the **upgrade display** command to verify the error. You should see the error message listed above.
  - Execute the **upgrade rollback** command.
  - Execute the **upgrade display** command a second time. The error message should have been removed.
  - Execute the **upgrade backup** command.
  - Execute the **upgrade display** command a third time. You should see a record showing successful backup of the database.
  - Execute the **upgrade restore** command and choose the version you wish to restore.
  - Execute the upgrade display command a fourth time. You should see one restore and one upgrade record listed.
  - Execute the **node stop** command to shut down the Content Distribution Manager.
  - Execute the **node start** command to re-start the Content Distribution Manager with the correct database version loaded.

- CSCdw61220

  Need procedure to set date and time on Internet CDN node via the bash shell.

- CSCdw64452

  After a software upgrade, Windows Media Services settings are not retained for hosted domains.

  Workaround:

  - From the Content Distribution Manager, select **Tools** > **Windows Media Services Configuration**.
  - Click the **Read and Accept Windows Media Server License Agreement** option, then click **Save**. The Windows Media License Agreement appears in the browser window.
  - Read it and click the **Accept** button that appears at the bottom of the Agreement.
  - Click **Yes** in the dialog appears. You will be returned to the Windows Media Services Configuration page. Windows Media Services will now be re-enabled on all hosted domains on which it was enabled prior to the software upgrade.

- CSCdw64794

  WMA file not playing using mmsu protocol only.

  Workaround:

  - Open your Windows Media Player V.7.
  - Click the Tools menu then select Options. The Options dialog appears.
  - Click the Network tab.

  - In the area marked Protocols, uncheck the UDP and verify that the TCP option is checked.
  - The mmst protocol will be used for all files with a mms* URL.

- CSCdw65140

  Running dbsetup on a Content Engine destroys the device's setup.cfg file.

  Workaround: Do not attempt to run dbsetup on Content Engines.

- CSCsp00588

  If a Content Engine or Content Router is shut down, the event may not be logged in the System Event Log on the Content Distribution Manager.

- CSCsp01022

  There is no visual indication whether or not passwords have been overridden on a Content Delivery Network device.

- CSCsp01245

  A "Page not Found" error message is displayed in the Add Update File window when the Content Distribution Manager cannot reach the device hosting the upgrade file.

- CSCsp01249

  The web browser times out, displaying a "Page Not Found" error when the Content Distribution Manager attempts to locate upgrade files on an unreachable server.

- CSCsp01372

  It is possible to add the same upgrade files multiple times to the same Content Distribution Manager. This does not impact the upgrade in any way.

Resolved Caveats

The following caveats are fixed (resolved) in Cisco Internet CDN Software Version 2.1.1. Caveats are listed according to their tracking number.

- CSCdu03195

  The RealServer Java Monitor is not fully implemented.

- CSCdu16048

  Deployment of a standby Content Distribution Manager in the event of failover should be supported to allow for geographic diversity.

- CSCdu21104

  During setup, it should be possible to specify a VLAN name for a Content Services Switch.

- CSCdu23464

  The distributed licensing for RealServer feature does not work for live streams.

- CSCdu24818

  On the Content Router details page, under the Management Information heading, the Content Router IP address appears where you should see the Content Router host name. This resolves itself after some time.

- CSCdu26028

  The graphical user interface should display an error if the file named in the Manifest field does not exist.

- CSCdu32063

  Ability to configure the maximum number of manifest items allowed.
- CSCdu34339

  The status message on the Replication Progress page identifies live content files as “live items” but pre-positioned content files as “items.”
- CSCdu37494

  Manifest errors that appear in the logs are not displayed on the user interface.
- CSCdu39865

  By default, there is no inactivity timeout associated with the CDM user interface, which users can set through the Tools > System Configuration page. There is, however, a cdm.session.timeout property that can be set as a user interface logout interval. For instructions on how to modify this property, refer to the *Cisco Internet CDN Software User Guide* for version 2.1, Chapter 4, in the section “Modifying the System Timeout Value.”
- CSCdu45677

  The sorting button on the user interface first sorts uppercase items and then lowercase items.
- CSCdu48305

  There should be multiple levels of user access.
- CSCdu49531

  If you connect to a Content Engine with only the Gigabit Ethernet interface connected, the device fails to register with the Content Distribution Manager.
- CSCdu52703

  It should be possible to distribute configuration scripts from the Content Distribution Manager to the Content Services Switch through the user interface.
- CSCdu53202

  There should be a command-line interface command for creating optional static routes for a Content Router.
- CSCdu56623

  The **node restart** command in the command-line interface does not work.
- CSCdu57678

  The **contentmask** command in the configuration menu of the command-line interface is not implemented.
- CSCdu58508

  The **node update** command in the command-line interface does not work.
- CSCdu59102

  The prompt that is visible when you are logged in to a Content Services Switch (CSS) should be identical to the name of the supernode that the CSS is a member of.
- CSCdu62385

  The system allows you to add Content Engines with insufficient free disk space to hosted domains. This results in pre-positioned content being dropped from the Content Engine.
- CSCdu67146

When a Content Engine that is the last node in the root location changes its location, the assigned hosted domains using that root location must have their root location changed as well.

- CSCdu70447

  A supernode cannot come on line if the Content Distribution Manager is off line.
- CSCdu71733

  Server stop notifications are not issued to the SNMP manager if you run **node stop**, **exit**, and **reboot** commands on a device.
- CSCdu73919

  The configuration script for each device should enable users to use their company name as a signature on certificates.
- CSCdu74015

  If you delete the location leader Content Engine and add it back, two Content Engines will take on the role of location leader.
- CSCdu74880

  Access logs for Content Engines that are behind a Content Services Switch need to be labeled with the primary IP address, not the hidden IP address. This is because the same hidden IP address may be used on different supernodes.
- CSCdu76981

  SNMP times out while scanning ghost drives on Content Engine-590 devices.
- CSCdu80912

  When configuring Content Services Switches in a redundant configuration, administrators receive the following message: “The script is in use by another session.”
- CSCdu89261

  Content Engines report to Content Routers and their supernode leader while shutting down. This increases the period when Content Routers route requests to Content Engines that cannot serve them.
- CSCdu89276

  Content Engines and Content Routers report being on line even when they fail to serve content.
- CSCdv01319

  System time is not displayed on all pages of the user interface.
- CSCdv02380

  The IP address or location of the origin server should not be displayed in the error message you see when the origin server goes down while trying to retrieve content.
- CSCdv02431

  The gateway IP address that you assign to a Content Engine must be reverse-resolvable.
- CSCdv07620

  Generation of SNMP traps due to changes in run-mode level is not implemented.
- CSCdv12657

  Running the command-line interface command **node stop** may prevent the system from restarting.
- CSCdv13330

Running the **node status** command after your Content Distribution Manager (CDM) fails to come online after a reboot may instruct you to perform a database rollback. Before doing so, look at the CDM merlot log for the following message:

```
DBupgrade records contain incomplete operation ... run rollback.
```

If you see this message, running the **upgrade rollback** in the command-line interface will correct the booting problem.

If you do not see this message, the Content Distribution Manager may be experiencing a connectivity problem with the database. Remove the DBUPGRADE-FAILED file from the merlot-state directory and restart the Cisco Internet CDN Software by entering the **node restart** command in the command-line interface.

- CSCdv14297

  The Windows Media Technologies (WMT) server continues running on Content Engines even when Windows Media Server (WMS) is deactivated on the Tools > WMS Configuration page.

- CSCdv14346

  Origin Server failover does not work.

- CSCdv15182

  Content Engine statistics are not displayed correctly on a hosted-domain-by-hosted-domain basis.

- CSCdv15190

  To restore the default CLI or HTTP passwords on Cisco Internet CDN devices:

  – Reboot the device.

  – At the LILO prompt, enter:

  ```
  linux single
  ```

  – At the bash prompt, enter:

  ```
  /cisco/merlot/etc/reset-passwd
  ```

  – Reboot the device.

  You can now log in to the device using the default passwords. The passwords will remain reset until a new password is set using the Content Distribution Manager user interface.

- CSCdv17970

  Scroll bars are missing on the Routing Diagnostics > View Supernodes page.

- CSCdv19565

  The user interface does not always give a warning or require confirmation when an operation will result in a reboot or restart.

- CSCdv24460

  Telnet ports respond to probes even when they are disabled.

- CSCdv27477

  If you erroneously enter “http://” before the origin server name on the Hosted Domain Details page and click Save, the system rejects the whole transaction and requires you to start over. You also lose all information that you may have entered in the fields.

- CSCdv28773

  Sometimes you do not receive server stop traps because the SNMP agent shuts down early.

- CSCdv30542

The system does not keep track of used WMT licenses or require acknowledgment of an end user license agreement.

- CSCdv30840

  The **node status** command-line interface command does not give you information about the WMT server, as it does for the QuickTime Server and RealServer.

- CSCdv31624

  Content Engine performance drops briefly on an hourly basis because of usage log processing.

- CSCdv33683

  For RAM files, content providers must use a CDN tag in the manifest file. The syntax must use the cdn-http tag, for example: http://hosted_domain_name/cdn-http/path_to_file.ram.

- CSCdv33958

  Scroll bars are missing on the Content Router peek page.

- CSCdv34752

  You cannot log in to the command-line interface as admin after doing a manual upgrade. Instead, you have to log in to the bash shell and reboot the device.

- CSCdv34827

  The DNS statistics on the Content Engine Statistics page always show a value of 0. This is incorrect.

- CSCdv35138

  If the wildcard is removed from a manifest file and the file is fetched again, RealPlayer returns an error message stating that either the file cannot be found or “A General Error has occurred” when trying to access the live stream.

- CSCdv38305

  If you are upgrading from Version 2.0.1 to 2.1, subsequent to running setup on a device, you should immediately change the device password through the Content Distribution Manager user interface. If you do not change it, the security of your system is compromised because somebody can access the device using default information. The password that you set during setup only protects your device temporarily following reboot.

- CSCdv49216

  When you create or modify a routed domain or Secure Key Content Authentication (SKCA) or If-Modified-Since (IMS) settings, the newly created information may take up to 10 minutes to propagate to the Content Engines.

- CSCdv50154

  Upgrade scripts do not report that the upgrade file is invalid; they merely report “Script missing inside distribution.”

- CSCdv50195

  If you reset your Content Distribution Manager (CDM) password to the default using the reset-password script, you should change it immediately afterward through the CDM user interface.

- CSCdv58270

  A checkbox is missing on the Simple Peek Page when the UPG Metafile is not present.

- CSCdv62752

  Cancel button disappears from CDM interface when browser window is sized down.

- CSCdv66627

The Netscape browser doesn't support mmst URLs.Windows Media Player 6.4 doesn't work with http URLs in Merlot 2.1, therefore Windows Media files that are played on the Netscape browser using Windows Media Player Version 6.4 will not load.

Workaround:

Include the non-ASX files in an ASX file, then deploy the ASX file. For example, if the user has a foo.asf, and a hosted domain: www.foo.cisco.com, then in order to use Netscape and Windows Media Player 6.4, you would create an ASX file, foo.asx, which is something like:

```
<asx version = "3.0">
<entry>
<ref href="mms://www.foo.cisco.com/www.foo.cisco.com/cdn-wmt/cdnfoo.asf"/>
</entry>
</asx>
```

Note: cdnfoo.asf is the cdn url for foo.asf. You would preposition both foo.asf and foo.asx on the hosted domain, then use the following URL to link to them from your website:

```
http://www.foo.cisco.com/cdn-http/foo.asx
```

- CSCdv67951

  You should run Network Time Protocol (NTP) setup on a Content Services Switch (CSS) after you configure the IP address and default gateway. The reason is that the CSS configuration is clear before it starts, so the absence of an IP address or default gateway prevents the CSS from contacting the NTP server that you specify.

- CSCdv68918

  Executing the run-merlot command freezes devices if the core file is in the PID directory.

- CSCdv69513

  When you fetch the Coverage Zone file from a Content Router, you will see many warning messages in the merlot log file. These messages do not indicate disruption of hybrid routing.

- CSCdv70048

  Simple Peek feature renamed Debugging/Telnet Control.

- CSCdv70721

  You must reboot a Content Router after removing the URL for its coverage zone file from the Content Distribution Manager user interface.

- CSCdv71374

  You are not given a message warning that making either of the following modifications to Windows Media Technologies (WMT) settings causes the device to restart:

  - On the Tools > Windows Media Server Configuration page, setting the maximum number of concurrent streams or the maximum amount of bandwidth to serve concurrently
  - Checking the Enable WMT check box on a Hosted Domain page

- CSCdv71468

  On the Tools > Routing Properties page, if you change the setting for the minimum number of name server records to fewer than three, the new setting does not take effect until the Content Routers are rebooted.

- CSCdv71769

When you install a Content Engine and then attempt to activate it through the Content Distribution Manager user interface, the fully qualified domain name that you specified during setup is not propagated to the Content Engine page. Instead, the description that you specified for the Content Engine during setup appears in the Content Hostname field and you get an error message saying, “Transaction not completed! Content hostname must contain at least 1 dot.”

Workaround:

Enter the fully qualified content host name in the Content Hostname field and then click the Save button.

- CSCdv72380

  The **show build** command in the command-line interface returns inaccurate information. To verify which build is installed, enter the **show all** command, and check the “CDN SW Version” entry in the output.

- CSCdv74655

  The storeutil restore command in the command-line interface (CLI) does not work.

- CSCdv74702

  The storeutil PurgeSysLogs command in the command-line interface (CLI) does not work as expected.

- CSCdv76483

  Prompt feedback for devices required when using node debugon command in the command-line interface (CLI).

- CSCdv76484

  The node debugon and nodedebugoff commands should note that the node must be restartedto remove affected device from debug mode.

- CSCdv76716

  Customers would like to know how to configure a firewall in front of Content Enginess and Content Routers.

- CSCdv76733

  It should be possible to access and download manifest files securely, without the danger of exposing the HTTP password for the manifest file. In Version 2.1.1, you can use HTTPS URLs, and SSL is used anonymously to protect username and password information for the manifest file.

  Note The software does not authenticate origin servers. That is, there is no protection against server impersonation attack aimed at stealing the manifest file username and password.

- CSCdv76746

  API requested for access to CDN status and statistics.

- CSCdv76802

  Read-only database view for customer requested.

- CSCdv76994

  The device host name is no longer displayed at the command-line interface (CLI) prompt when in "config" mode.

- CSCdv77571

Next click failover does not work when both the root and non-root hosted domain leader Content Engines have failed.

- CSCdv77622

  Next click failover does not work when both Content Engines in the root location have failed.

- CSCdv80036

  If you reboot a Content Engine that has a missing hard drive, all cached content on that Content Engine becomes unavailable. If a hard drive fails, *always* replace the disk with a SCSI disk with the same SCSI ID as the failed drive before rebooting the Content Engine. Do not reboot the Content Engine with a drive missing, as this can potentially destroy data.

- CSCdv80529

  Device doesn't restart using node restart command.

- CSCdv81354

  Telnet cannot be enabled using the command-line interface (CLI) in privilege mode.

- CSCdv81401

  The **node restart** command-line interface command stops all processes, but does not start them again.

- CSCdv81645

  Using the enable command in the command-line interface (CLI) produces unexpected results.

- CSCdv82691

  Endusers may be unable to play the RealServer live stream that they select.

- CSCdv83519

  Subscriber should read publisher in instructions on "Configuring RealServer Distributed Licensing" in *Cisco Internet CDN Software User Guide*.

- CSCdv84723

  Do not use the cdn- tag in a hosted domain name or a filename; doing so will cause the RealServer, Darwin, and Windows Media Technologies (WMT) servers to have trouble verifying requests for content.

- CSCdv85458

  Logrotate is unable to rotate log files.

- CSCdv88138

  Content Routers that are not running reverse DNS and do not have the Content IP address set during netsetup generate ConstrainException errors when activated from the CDM interface.

- CSCdv89051

  Setup script is ambiguous when asking for DNS hostname of standby CDM.

- CSCdv90005

  The RealServer on Content Engines is unable to open a successful connection with the RealServer license publisher. This prevents end users who make requests for RealMedia content from obtaining a distributed license and viewing the content.

- CSCdv90595

  When the DNS server rejects a packet because of a format error, the error reply does not contain the serial number of the request.

- CSCdw00956

  The merlot-css-setup script is unable to configure more than 53 interfaces.
- CSCdw01712

  Incorrect wording on warnings when changing ConfigProperty.
- CSCdw02018

  When you import a very large file (1.5 GB or more), it may stall in an import state.
- CSCdw02308

  Able to specify duplicate Content Hostname/IP for two nodes.
- CSCdw02907

  Assignments of Content Engines to hosted domains and removal from hosted domains are not logged in the cdmAuditTrail log file.
- CSCdw03219

  Log file name should contain address of Content Engine.
- CSCdw03290

  It is unclear what username/password combination should be used when trying to access the "peek" pages for a node.
- CSCdw04930

  The number of Windows Media Services-enabled Content Engines does not have to correspond to the number of available Windows Media Technology licenses.
- CSCdw09872

  If you request a file using a Real-Time Streaming Protocol (RTSP) URL, directly or by reference in a SMIL file, the request may fail under either of the following conditions:

  - The requested file has been pre-positioned on some, but not all, Content Engines in the hosted domain before you make the request. The request is directed to one of the Content Engines that does not yet have the file.
  - You are using the hybrid routing feature, and the initial request is routed to a Content Engine that is not in a preferred location.

  You can work around the first problem by ensuring that the file is pre-positioned on all Content Engines before allowing the item to be served. You can accomplish this using the “serve” attribute in the manifest file. For more information on this attribute, refer to the “Manifest File Structure and Syntax” section in Chapter 2 of the *Cisco Internet CDN Software User Guide*, Version 2.1.

  Workaround:

  Use HTTP URLs for streams to be served using RealServer.
- CSCdw13893

  Activating a Content Engine generates a sysdb_bind failed error.
- CSCdw15201

  There is no command-line interface (CLI) command to specifically perform a software downgrade. However, you can use the **upgrade swupgrade** command to perform a downgrade as well.
- CSCdw16690

Upgrade files are removed from CDN device after the software upgrade initiated using the upgrade swupgrade command has completed.

- CSCdw16823

  The command-line interface (CLI) upgrade command will not execute if more than one upgrade file is present on the CDN device.

- CSCdw21322

  When adding a Content Engine to a hosted domain, receive transaction error referencing Cluster PublicIP.

- CSCdw23816

  Cisco CLI scp command needs to be documented.

- CSCdw24076

  You can now encode Windows Media Technologies (WMT) copyright information in the manifest file by specifying stream properties. For any content item or content group, you can encode this information through the *streamProperty* property name, for example, <src-url = "foo.asf" cdn-url= "foo.asf" streamProperty= "Author= 'foo author'" Title= 'foo title'"/>. The attributes supported within *streamProperty* can be one or more of the following:

  - Abstract
  - Title
  - Author
  - Copyright

- CSCdw25468

  Newly registered Content Engines may not receive the Content Engine certificate from the CDM and may not receive a proper initial update from the CDM.

- CSCdw26919

  Documentation of the Manifest DTD should not reference support of either the https or ftp protocols.

- CSCdw35615

  When Content Engines in the primary and secondary locations are overloaded, Content Engines in other locations are not selected as NS records, instead overloaded Content Engines in the primary location are selected.

- CSCdw38087

  command-line interface (CLI) node setprop command does not enable Peekable.

- CSCdw38121

  command-line interface (CLI) node setprop command does not enable Telnet.

- CSCdw42855

  Instructions for Telnet and peekable need to be changed.

- CSCdw61220

  Need procedure to set NTP server on a CDN device manually via bash shell.

- CSCdw63225

  Need an API to automate the Fetch Now command for the Manifest file.

- CSCsp01080

LogMover and LogRotate now both configured through the System Configuration page of the CDM graphical user interface.

Documentation Omissions

This section contains information that was not covered in the following documents:

- *Cisco Internet CDN Software User Guide, Version 2.1*
- *Cisco Internet CDN Software Command Reference, Version 2.1*

Cisco Internet CDN Software User Guide, Version 2.1

The following section describes information that has been added to the Cisco Internet CDN Software User Guide since the release of Version 2.1.

Consider Load for Routing Option added to Routing Properties

In Chapter 4, “Maintaining Cisco Internet CDN Software,” Table 4-1 in the section on “Modifying Dynamic Routing Properties” has been updated to include the Consider Load for Routing option.

When enabled, this option causes SuperNodes and standalone Content Engines to report their load to the Content Routers that for use in making routing decisions. Load is based on the response time of HTTP requests between SuperNode leader-Content Engines and SuperNode cluster addresses.

The Content Router then assigns a lower priority to overloaded SuperNodes or standalone Content Engines and a higher priority to unloaded nodes when routing content requests.

Cisco Internet CDN Software Command Reference, Version 2.1

The following commands either have been added to the command-line interface, or their syntax has been modified to include options that were not available in earlier versions of the software:

- **node**
- **real**
- **scp**
- **storeutil**

node

To control or monitor the status of Cisco Internet CDN devices, use the **node** command in privileged EXEC mode.

The syntax of the **node** command has been extended to include the following two options:

node {setprop [enableTelnet {1 | 0} | enablePeekable {1 | 0}] | secondnic}

Syntax Description

setprop	Sets a system property on a CDN device.
enableTelnet	Enables or disables the Telnet system property.
1	Enables the system property.
0	Disables the system property.
enablePeekable	Enables or disables the peekable system property. Enter 1 or 0 to enable or disable, respectively.
secondnic	Activates the second network interface card (NIC) which can be connected to your Oracle database server behind a firewall for added security.

Defaults

The enableTelnet and enablePeekable keywords are disabled by default.

Command Modes

Privileged EXEC

Usage Guidelines

After you successfully complete an **enableTelnet**, **enablePeekable**, or **secondnic** operation, you must reboot the device by entering the **reboot** command. Unless you reboot the device, the new settings will not take effect.

Before entering the **node secondnic** command, you must stop the Content Distribution Manager by entering the **node stop** command.

Examples

```
Host> enable
Host# node setprop enablePeekable 1

Host> enable
Host# node secondnic
Configuring eth1.

Enter the Secondary IP DNS Name: secondnic.cisco.com
Warning: Unable to resolve secondnic.cisco.com to an IP address.

Would you like to change this setting? [y/n]: n

Enter the Secondary IP Address: 192.168.0.0

WARNING
-------
secondnic.cisco.com does not currently resolve to 192.168.0.0
DNS must be setup to resolve this name before
the system will operate correctly.

Enter the Secondary IP Netmask: 255.255.255.0
Enable Secondary Nic now? [y/n]: y
Network validation succeeded.
```

Related Commands

enable

real

To add or remove RealServer licences or plug-ins from a Content Engine, use the **real** command in privileged EXEC mode.

real {license | rsmcs}

Syntax Description

license	Adds or removes RealServer licenses.
rsmcs	Deploys the RealServer Media Commerce Suite (RSMCS) plug-in.

Defaults

The default RealServer license on a Content Engine allows ten simultaneous users and no live streams. If distributed licensing is enabled, then these features are controlled by the license server.

Command Modes

User and privileged EXEC

Usage Guidelines

The RealServer Media Commerce Suite (RSMCS) plug-in allows Content Engines to decrypt the encrypted content received from content providers so that the content can be streamed to endusers.

Before you deploy the RSMCS plug-in, you must download the plug-in to your Content Engine's cisco/merlot/state directory by using the **ftp** or **scp** command.

Once the plugin is on the device, you can deploy it by entering the **real rsmcs** command. When the deployment is confirmed, enter the **node restart** command. This will briefly disrupt service from the Content Engine.

The LICENSE plugin allows you to add or remove a RealServer license file from your CDN device. Before you add the license using the LICENSE plugin, you must download it to your Content Engine's cisco/merlot/state directory by using the **ftp scp** command. Then deploy it by entering the **real license** command.

When the deployment is confirmed, enter the **node restart** command. This will briefly disrupt service from the Content Engine.

Examples

```
Host> enable
Host# real license
License Administration

1. Add License file
2. Remove License file
3. exit

Select [1-3]:1

Host> enable
Host# real rsmcs
RealSystem Media Commerce Suite (RSMCS) Plugin Administration

1. Add RSMCS license
2. Remove RSMCS license
```

```
3. exit

Select [1-3]:1
```

Related Commands

scp

To securely copy files from a CDN device you are logged on to, to another CDN device, use the **scp** command in user EXEC mode with the following syntax:

scp {[*source_path***] merlot@[***target_IP_address***]:/[***target_path***]}**

To securely copy files to a CDN device you are logged on to, from another CDN device, use the **scp** command in user EXEC mode with the following syntax:

scp {merlot@[*source_IP_address***]:/[***source_path***][***target_path***]}**

Syntax Description

merlot	BASH account name. You must use this account name in order to execute the scp command.
source_path	Relative directory path and file name on the source CDN device of the file that is being transferred.
target_path	Relative directory path on the target CDN device to which the file is being copied.
source_IP_address *or* *target_IP_address*	IP address of the source or target CDN device.

Defaults

No default behavior or values

Command Modes

User EXEC

Usage Guidelines

After logging in to the CLI for either the device from which or to which you will be copying, enter the **scp** command, following the syntax description provided above, then do the following:

- After you have entered the **scp** command, you will be prompted to confirm your decision to continue your connection. Enter ‘y’.
- You will be prompted to enter a password to access the remote device you are accessing (either to copy files to the device or from it). Enter the root password for that device. If you have not changed the root password before, that password is ‘default’.

Refer to Chapter 3: Working with the Cisco Internet CDN Software” in the Cisco Internet CDN Software User Guide for information on setting the root password for your CDN devices.

Examples

```
Host> scp /cisco/merlot/state/mycdmfile.log merlot@10.1.2.3:/cisco/merlot/state/dump/home

Host> scp merlot@10.0.0.0:/cisco/merlot/state/mycdmfile.log /cisco/merlot/state/dump/home
```

Related Commands

ftp

storeutil

To manage the Oracle database holding your CDN data, use the utilities accessible from the storeutil command.

storeutil {**dbcheck** [*username password IP_address servicename*]| **invalidate** | **purgesyslog** [**days** {*number*}| **count** {*number*}]| **relocate** | **report** | **restore** | **validate**}

Syntax Description

dbcheck	Tests whether or not the database connection is active.
username	Database administrator account name
password	Database administrator account password
IP_address	Database host IP address
servicename	Name of the CDN service
invalidate	Marks database records invalid.
purgesyslog	Clears syslog records up to a point specified either by a number of days or a record count.
days	Specifies that the syslog should be purged from the beginning of the log to a point some specified number of days before the end of the log.
number	The number of days before the end of the log for which syslog messages should not be purged.
count	Specifies that the syslog should be purged from the beginning of the log to a point some specified number of records before the final record in the log.
number	The number of records before the end of the log that should not be purged.
relocate	Launches a simple script that allows you to changes the IP address of the CDN Oracle database.
report	Saves a list of objects that have been marked invalid in the merlot/state/validation.log file.
restore	Launches a simple script that allows you to restore invalidated database records.
validate	Validates the current database store, outputting results to the screen.

Defaults

No default behavior or values

Command Modes

User and privileged EXEC

Usage Guidelines

You must stop the Content Distribution Manager before running the **storeutil** command. Enter **node stop** to stop the Content Distribution Manager.

The **storeutil** command is a privileged level command, so you must enter **enable** before entering **storeutil**.

The **storeutil** set of commands lets you locate and debug invalid database records in which there are references from a store object to a nonexistent store object. The Content Distribution Manager may fail to start if there are invalid database references. If this happens, the user interface is not available and the Merlot log registers an error.

To send a test to your Oracle database to determine whether or not the database connection is active, use the **storeutil dbcheck** command. When issuing the command, you must provide the following connection information for the database in the command line:

- database administrator username
- database administrator password
- database host IP address
- database service name

To obtain a list of invalid references, use the **storeutil validate** command. The list appears in the merlot/state/validation.log file. To prevent invalid references from being loaded, use the **storeutil invalidate** command to mark the invalid references for exclusion. Run the **validate** and **invalidate** commands as many times as necessary to receive a “passed” message from the system.

To point the CDN to its Oracle database at a new IP address, use the **storeutil relocate** command. This will launch a script that allows you to input the new IP address for the database as well as the following information:

- database administrator username
- database administrator password
- database service name

To save a list of objects that have been marked invalid in the merlot/state/validation.log file, use the **storeutil report** command.

If you have corrected the invalid references through database intervention and want to validate them, use the **storeutil restore** command.

To free up some of the space in the database that is allocated to system messages, you need to periodically clear the system messages stored in it. To do this, use the **storeutil purgesyslog** command. When issuing this command, you will be prompted to enter

Examples

```
host# storeutil validate
Passed Validation.

host# storeutil relocate
Enter Database hostname [10.89.5.180]: 192.168.0.2
Enter Database username [cdmuser]]: cdmuser
Enter Database password [cdmpass]: cdmpass
Enter Database Service Name [service]: service

Operation Successful.
```

```
host# storeutil report
controller.storeAdmin[18225]: 1  ClusterConfig.RoutedDomains references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.SkcaConfigId references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.ImsConfigId references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.CmdPurgeRdId references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.RootLocation references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.CustomerId references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.DistTreeId references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
controller.storeAdmin[18225]: 4  RoutedDomain.ClusterConfigs references were found to be
invalid. [Tue Oct 30 20:42:08 GMT 2001]
```

Documentation Corrections

This section documents corrections to the following documents:

- Cisco Internet CDN Software Configuration Guide, Version 2.1
- Cisco Internet CDN Software User Guide, Version 2.1
- Cisco Internet CDN Software Command Reference, Version 2.1

Cisco Internet CDN Software Configuration Guide, Version 2.1

- In Chapter 1, “System Requirements” in the “Workstations for Accessing the Web-Based User Interface” section, the RealNetworks RealPlayer and Apple QuickTime player should not be listed as software required to access the Content Distribution Manager user interface.
- In Chapter 2, “Preparing to Configure CDN Devices,” in the following sections:
  - Configuring a Content Distribution Manager
  - Configuring a Content Router
  - Configuring a Standalone Content Engine
  - Configuring a Content Engine as Part of a Supernode

  The first three steps in each of these sections should be replaced with the following:

Step 1 Boot the device.

Step 2 Log in as **admin** with the password **default**.

Step 3 At the prompt, enter **enable**. Press **Enter**.

Step 4 At the prompt, enter **config**. Press **Enter**.

Step 5 At the config prompt, enter **setup**. Press **Enter**.

Continue with Step 4 in the appropriate section of the *Cisco Internet CDN Software Configuration Guide* for version 2.1.

- In Chapter 2, “Preparing to Configure CDN Devices,” the section on “Configuring DNS” should contain the following statement regarding support for BIND:

  We support versions 4, 8, and 9 of the Berkeley Internet Name Domain (BIND) implementation of DNS. Earlier versions of BIND may be incompatible with the Cisco Internet CDN Software.
- In Chapter 2, “Preparing to Configure CDN Devices,” Step 1 of the section on “Configuring the Oracle Database” should contain the following command syntax:

```
SQL> create tablespace cdn DATAFILE ‘datafile path on Oracle Server’ SIZE 250M REUSE;

SQL> create tablespace cdntemp DATAFILE ‘datafile path on Oracle Server’ SIZE 250M
REUSE;
```

Additional data files can be associated with the tablespace using the following command.

```
SQL> alter tablespace cdn add DATAFILE ‘datafile path on Oracle Server’ SIZE 250M
REUSE;
```

- In Chapter 3, “Configuring CDN Devices,” the section on “Configuring the Content Distribution Manager” should contain the following warning concerning the creation of an Oracle database user account:

  Note Do not use the database administrative account name as your user account.

  Supplying the database administrator account name as the database user account may affect your ability to upgrade or downgrade your Oracle database in the future.

Cisco Internet CDN Software User Guide, Version 2.1

- In Chapter 2, “Creating Content Delivery Networks,” the “<CdnManifest>” section contains the following statement:

  Any number of servers, hosts, and items can be defined, up to a limit of 10,000 items in the manifest file.

  As of Version 2.1.1 of the Cisco Internet CDN Software, the limit on the number of content items listed in a manifest file is a configureable variable that can be modified using the System Configuration feature on the CDM.
- In Chapter 3, “Working with Cisco Internet CDN Software,” the “Modify a Hosted Domain” section should indicate the default value for the manifest refresh rate in the description of the Refresh Time field (which identifies the frequency with which the Content Engines assigned to the hosted domain check for updates to the manifest file) in Step 6. The default refresh time is 30 minutes.
- In Chapter 4, “Maintaining Cisco Internet CDN Software,” the “Setting Up Remote Logging” section contains inaccurate log file formats for the different servers. The correct log file formats for each server are shown below. Note that the time stamp in each of the log filenames is not given in milliseconds.
  - SQuID cache log file format
    IPaddress~access.log.lognumber~timestamp.cdn.gz
  - QuickTime server log file format
    IPaddress~StreamingServer.lognumber.log~timestamp.cdn.gz
  - RealServer log file format
    IPaddress~rmaccess.log.lognumber~timestamp.cdn.gz
  - Windows Media Technologies log file format
    IPaddress~mms_export.xxxxx.log~timestamp.cdn.gz
- In Chapter 4, “Maintaining Cisco Internet CDN Software,” the “Configuring RealServer Distributing Licensing” section contains the following instruction:

  Under the Primary Publisher heading, enter the IP address of the subscriber RealServer in the IP field and the admin port number for the publisher RealServer in the Port field.

  This should instead read:

  Under the Primary Publisher heading, enter the IP address of the publisher RealServer in the IP field and the admin port number for the publisher RealServer in the Port field.
- In Chapter 4, “Maintaining Cisco Internet CDN Software,” the “Setting up Remote Logging” section contains the following instructions:

- In the Update Interval field, enter the frequency (in hours) that the system checks for log files on the selected device to be transferred to the remote FTP server. If log files are not available for transfer, no action is taken.
- In the Size Limit field, enter the maximum allowed size for log files transferred to the remote server. Log files that are larger than the maximum allowed size are not transported to the remote FTP server, so be sure to use a conservative estimate when supplying this ceiling.

These fields have been removed in Version 2.1.1 of the software. Instead, the default value for each option will be used.

- The default update interval is 600 seconds, or 10 minutes.
- The default size limit for noncompressed log files is 10 megabytes. Log files are compressed prior to being uploaded to the remote server.

The default values for each of these options can be changed using the System Configuration feature on the Content Distribution Manager graphical user interface. See the “Modifying System Properties” section in Chapter 4:” Maintaining Cisco Internet CDN Software” of the *Cisco Internet CDN Software User Guide, Version 2.1*.

Cisco Internet CDN Software Command Reference, Version 2.1

- Documentation of the dnslookup command on page 2-7 uses the following syntax example:

```
Host# dnslookup  172.16.0.0
official hostname: 172.16.0
address: 172.16.0
```

  This should read:

```
Host# dnslookup  172.16.0.0
official hostname: cisco.com
address: 172.16.0.0
```

- Documentation of the usage guidelines for the routerutil command on page 2-28 should read as follows:

  Consult Cisco Technical Support before using any **routerutil** command.

  The **routerutil** command is a privileged level command, so you must enter **enable** before entering a **routerutil** command.

  The routing table that is displayed when you enter the **routerutil supernodes** command shows all the hosted domains listed under the cluster containing the supernode leader. This is because the Content Router forwards all DNS requests to this lead cluster and has no knowledge of assignments to clusters within the supernode.

  If the **Consider Load for Routing** option has been enabled from the Content Distribution Manager graphic user interface, each hosted domain will also display a number corresponding to its current load as follows:

  - -1 = unloaded
  - 0 = loaded
  - 1 = overloaded

  Refer to the section on “Modifying Routing Properties” in the *Cisco Internet CDN Software User Guide* for information on enabling the Consider Load for Routing option.

The supernode list that is displayed after you enter the **routerutil supernodes** command may be very long. To display the entire list, press the **Spacebar** until you reach the end. The supernodes list is also saved to the cisco/merlot/state directory of your Content Router under the name "supernodes.html." To exit after the supernodes list is displayed, enter **q**.

- Documentation of the usage guidelines for the **shutdown** command on page 2-34 should read as follows:

  "After entering the **shutdown** command, you need to boot up the device manually. You need physical access to the device in order to perform a manual reboot.

  You will not be able to remotely access the device until you manually reboot."

- Documentation of usage guidelines for the **upgrade swupgrade** command on page 2-40 should note that:
  - The **upgrade swupgrade** command can also be used to perform a software downgrade.
  - The **upgrade swupgradeclr** command cannot be used after performing an upgrade using the **upgrade swupgrade** CLI command and should be used only when the upgrade has been initiated from the Content Distribution Manager user interface.

Product Documentation Set

Your Cisco Internet CDN product shipped with a minimal set of printed documentation, as well as a Documentation CD. The printed documentation provides enough information for you to install and initially configure your product. The CD contains additional product documentation (user guides, configuration manuals, and so forth), which you can access and print out.

The following is a list of the documentation that shipped with your product (you can access the URLs listed for each document on the Documentation CD and at www.cisco.com on the World Wide Web):

- *Release Notes for Cisco Internet CDN Software Version 2.1.1* (DOC-7814129=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/cdnsp/cdnsp21/index.htm

Related Product Documentation

The following is a list of related documentation for your product. These documents were not shipped with your product, but you can access them and order them by using the URLs listed below:

- *Cisco Internet CDN Documentation Roadmap* (DOC-7813922=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/cdnsp/cdnsp21/index.htm

- *Cisco Internet CDN Software Configuration Guide* (DOC-7813578=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/cdnsp/cdnsp21/icdn21cg/index.htm

- *Cisco Internet CDN Software User Guide* (DOC-7813576=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/cdnsp/cdnsp21/icdn21ug/index.htm

- *Cisco Internet CDN Software Command Reference* (DOC-7813577=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/cdnsp/cdnsp21/icdn21cr/index.htm

- *Cisco Content Engine 500 Series Hardware Installation Guide* (DOC-7811199=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/ce500/ce500hig/index.htm
- *Cisco Content Engine 500 Series Hardware Release Note* (DOC-7811338=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/ce500/index.htm
- *Hardware Installation Guide for the Seven-Rack Unit Chassis* (DOC-7811114=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/ce7300/ce7300hg/index.htm
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series* (DOC-7811564=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/safesite/11564rcs.htm
- *Release Notes for the Cisco Storage Array 6* (DOC-7810704=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/st_array/sa-6/rn_sa6.htm
- *Cisco Storage Array 6 Installation and Configuration Guide* (DOC-7810584=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/st_array/sa-6/sa6hig/index.htm
- *Cisco Storage Array 12 Installation and Configuration Guide* (DOC-7812102=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/st_array/sa-12/sa12_hig/index.htm
- *Cisco Content Distribution Manager 4670 Product Description Note* (DOC-7811568=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/cdm/11568pdn.htm
- *Cisco Content Router 4450 Product Description Note* (DOC-7811569=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/cr/cr4450/11569pdn.htm
- *Cisco Content Engine 7320 Product Description Note* (DOC-7811575=)

  http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/ce7300/11575pdn.htm

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Product Documentation Set" and "Related Product Documentation" sections.

This product contains copyrighted programs and license agreements that are used with permission and are the property of the following respective owners.