Cisco Configuration Engine Installation and Configuration Guide 3.5.3

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-17341-03

Cisco Configuration Engine Installation and Configuration Guide 3.5.3

CONTENTS

Preface

This preface describes the audience and conventions of the *Cisco Configuration Engine Installation and Configuration Guide 3.5.3*. It also describes the available product documentation and provides information on how to obtain documentation and technical assistance.

Audience

This guide is intended primarily for:

- System administrators familiar with installing high-end networking equipment
- System administrators responsible for installing and configuring internetworking equipment who are familiar with Cisco IOS software

Conventions

This guide uses the following conventions:

Item	Convention
Commands and keywords.	**boldface** font
Variables for which you supply values.	*italic* font
Optional command keywords. You do not have to select any options.	[enclosed in brackets]
Required command keyword to be selected from a set of options. You must choose one option.	{options enclosed in braces | separated by vertical bar}
Displayed session and system information.	`screen` font
Information you enter.	**`boldface screen`** font
Variables you enter.	*`italic screen`* font

Item	Convention
Menu items and button names.	**boldface** font
Choosing a menu item.	**Option > Network Preferences**

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

Table 1 describes the related documentation available for Cisco Configuration Engine.

Table 1 Cisco Configuration Engine 3.5.3 Documentation

Document Title	Available Formats
Cisco Configuration Engine Installation and Configuration Guide 3.5.3	This guide is available on Cisco.com.
Cisco Configuration Engine Administration Guide 3.5.3	This guide is available on Cisco.com.
Cisco Configuration Engine Software Development Kit API Reference and Programmer Guide 3.5.3	This guide is available on Cisco.com.
Troubleshooting Guide for Cisco Configuration Engine 3.5.3	This guide is available on Cisco.com.
Release Notes for Cisco Configuration Engine 3.5.3	This release notes is available on Cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS CONFIGURATION ENGINE MANAGEMENT SOFTWARE

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence. By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software. When used below, the term "server" refers to central processor unit.

---

1. **ADDITIONAL LICENSE RESTRICTIONS**

- **Software Upgrades, Major and Minor Releases**

Cisco may provide Cisco Configuration Engine Software 3.5.3 updates. The Software update and new version releases can be purchased through Cisco or a recognized partner or reseller. The Customer should purchase one Software update for each Configuration Engine installation. If the Customer is eligible to receive the Software update or new version release through a Cisco extended service program, the Customer should request to receive only one Software update or new version release per valid service contract.

- **Reproduction and Distribution.** Customer may not reproduce nor distribute software.

2. **DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS**

Please refer to the Cisco Systems, Inc. End User License Agreement.

CHAPTER 1

Installing the Product Software

The Cisco Configuration Engine is a network management software that acts as a configuration service for automating the deployment, management, and upgrading of network devices and services. Each Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Cisco Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

This chapter provides system requirements and procedures for installing, uninstalling, and ugrading the Cisco Configuration Engine software on the host system running on Solaris or Linux platforms. It contains the following sections:

Operating System Dependencies

Table 1-2 lists the supported Red Hat Enterprise Linux and Oracle Solaris OS versions for the Cisco Configuration Engine release 3.5.3.

Table 1-1 Operating System Dependencies

Operating System	Update Supported
Red Hat Enterprise Linux 4	Update 8 or above

Table 1-1 Operating System Dependencies

Operating System	Update Supported
Red Hat Enterprise Linux 5	Update 5 or above
Solaris version 10	Update 8/10 or above

System Requirements—Solaris

With the following system requirements, the device connections can scale up to 30,000 devices:

- Solaris 10
- 16 GB RAM
- 8 core 1.0 GHz UltraSPARC T1 processor
- 70 GB disk space (see Understanding Disk Space Calculation, page 1-2)

System Requirements—Linux

With the following system requirements, the device connections can scale up to 20,000 devices:

- Red Hat Enterprise Linux 4 and Linux 5(32-bit SMP, kernel 2.6 and SELinux disabled)
- 4 Intel(R) Xeon(R) CPUs 5140 at 2.33 GHz or equivalent and above
- 8 GB RAM
- 70 GB disk space (see Understanding Disk Space Calculation, page 1-2)

Understanding Disk Space Calculation

Note This disk space calculation is based on the Berkeley Database.

The /opt/ConfigEngine/openldap/var/openldap-data/id2entry.bdb file contains all the entries in the directory database. The size of this file provides a good approximation of the size of the directory database.

The following example shows that the size of the id2entry.bdb file is approximately 7 MB. Assume that the average size of an entry in the database is 1 KB and that the database contains approximately 7000 entries. The other *.bdb files are index files, which you must take into account. If you add the size of the id2entry.bdb file (approximately 7 MB) with the size of all of the index files (approximately 4.5 MB), the total database size would equal 11.5 MB.

In addition to the directory database, you must consider the disk space for database backups, Configuration Engine jobs, and log files. Because backups require as much storage as the active directory database, you must allocate space for backups also.

To view the size of the id2entry.bdb file, enter the **ls -alt** command.

Example

```
Average size of config job:

In-Progress/Stopped is 2K.
Completed is 2.5

Average size of Image job:

Stopped is 4K.
In-Progress is 2.5 K.

myCE(/opt/ConfigEngine/openldap/var/openldap-data)# ls -alt
total 31384
-rw------- 1 root other 16384 Sep 10 17:31 __db.001
-rw------- 1 root other 10485760 Sep 10 10:30 log.0000001452
-rw------- 1 root other 2371584 Sep 10 10:30 dn2id.bdb
-rw------- 1 root other 7012352 Sep 10 10:30 id2entry.bdb
-rw------- 1 root other 155648 Sep 10 10:30 objectClass.bdb
drwxr-xr-x 2 bin bin 2560 Sep 10 01:00 .
-rw------- 1 root other 176128 Sep 10 00:50 IOSConfigID.bdb
-rw------- 1 root other 180224 Sep 10 00:50 IOSEventID.bdb
-rw------- 1 root other 1499136 Sep 10 00:50 cn.bdb
-rw------- 1 root other 98304 Sep 8 18:07 __db.003
-rw------- 1 root other 270336 Sep 8 17:34 __db.002
-rw------- 1 root other 409600 Sep 8 17:31 __db.004
-rw------- 1 root other 24576 Sep 8 17:31 __db.005
drwxrwxr-x 5 bin bin 512 Aug 31 15:15 ..
myCE(/opt/ConfigEngine/openldap/var/openldap-data)#
```

Cisco IOS Dependencies

Table 1-2 lists Cisco IOS versions with corresponding versions of Cisco Configuration Engine 3.5.3 including feature limitations associated with each version.

Table 1-2 Cisco Configuration Engine 3.5.3 and Cisco IOS Dependencies

Cisco IOS	Cisco Configuration Engine	Limitations
12.3	1.3.2 or later	—
12.2(11)T	1.2 or later	—
12.2(2)T	1.2 or later with no authentication.	Applications are unable to use exec commands or point-to-point messaging.

Understanding Installation

The Cisco Configuration Engine 3.5.3 image is provided in a tar file format. You must untar the image in a directory, then go to that directory and run the installation script. You need root access to install Cisco Configuration Engine. For details about the installation procedure, see Installing the Software, page 1-4.

Cisco Configuration Engine 3.5.3 shares the web infrastructure-related software with bundled Cisco software. The installation script checks for shared and nonshared packages and takes appropriate action to install, abort, or prompt the user for package path.

To support different types of installations and setup, you are provided with the following installation script options:

./ce_install.sh—Default option. Installs all packages. Allows interactive installation that prompts the user for input.

./ce_install.sh-batch—Allows non-interactive installation. The installation script reads the default values from *installRule.solaris.xml* file or from the i*nstallRule.linux.xml* file as appropriate, and installs Cisco Configuration Engine 3.5.3 based on these settings without query for user input.

./ce_install.sh-demo—Installs the package without checking system resources except for minimum disk space, which is 650MB.

./ce_install.sh-force—Installs/uninstalls Cisco Configuration Engine 3.5.3 without installation or un-installation status check.

For details about the installation script, see Information About the Installation Script, page 1-8.

Installing the Software

The Cisco Configuration Engine 3.5.3 software is contained on a CD-ROM that is in the accessory kit.

Note You need root access to install the Cisco Configuration Engine software.

Step 1 Install the CD-ROM into the disk drive on the host system.

Step 2 Copy the tar file into a new folder where there is sufficient disk space (see Understanding Disk Space Calculation, page 1-2):

tar xvf <*tarfilename***>**

Note The tar file must be the only file in this new folder. You should use GNU tar for untarring the file.

Step 3 Check the system requirements for the installation .

./ce_check.sh—Checks the system software and the hardware requirements before installing the Cisco Configuration Engine software.

Step 4 Enter one of the following installation script commands as appropriate:

./ce_install.sh—Default option. Installs all packages. Allows interactive installation that prompts the user to provide input.

./ce_install.sh-batch—Allows non-interactive installation. The installation script reads the default values from *installRule.solaris.xml* file or from the i*nstallRule.linux.xml* file as appropriate, and installs Cisco Configuration Engine 3.5.3 based on these settings without query for user input.

./ce_install.sh-demo—Installs the package without checking system resources except for minimum disk space, which is 650MB.

./ce_install.sh-force—Installs/uninstalls Cisco Configuration Engine 3.5.3 without installation or un-installation status check.

Step 5 After installing the software, log out, then log back in again, or create a new window.

Step 6 Enter the following commands:

cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/bin/

./setup

Step 7 Go to Chapter 2, "Running the Setup Program" for a description of how to setup your system.

Upgrading from Release 2.0 or later to 3.5.3

The data migration feature allows you to upgrade your system from release 2.0 or later to 3.5.3. This feature populates the directory with the data you established for the prior release.

This is a four-step process:

1. Execute the Patch Script, page 1-5
2. Export Data to a Remote FTP Site, page 1-6.
3. Install Release 3.5.3 Software, page 1-6
4. Retrieve data from the FTP site, then setup the system (see Run datamigrate and Configure the System, page 1-7).

Note When you perform data migration on a box where the Cisco Configuration Engine 3.5.3 is not installed, then run the script *./reinitialize* from CISCO_CE_HOME/bin.

Execute the Patch Script

If you have custom attributes defined in Cisco Configuration Engine and planning to migrate to Cisco Configuration Engine 3.5.3, then you need to run this schema patch script. The patch script will be a part of Cisco Configuration Engine release 3.5.3 and the patch script file can be located in the RPMS/Patch directory when you untar the Cisco Configuration Engine 3.5.3 tar file. After applying this patch, you can run the search query based on your custom attributes.

To run the patch script, follow these steps:

1. Untar the Cisco Configuration Engine 3.5.3 tar file and go to the Patch folder.
2. Run the **./schema_patch.sh** file.

Example of dataexport Prompts

```
# ./schema_patch.sh
--------------------------------------------------
CE utility to patch schema of custom defined attributes.
--------------------------------------------------
Apply this patch if you are migrating from any CE release prior to CE 3.5.3 to CE 3.5.3 or
above release.
Do you want to apply the patch to update CE schema? (y/n) [n]y
Applying patch...
Patch SUCCESS!!!
Now you can run dataexport script for CE migration.
```

Export Data to a Remote FTP Site

Before exporting the data, it is assumed that your host has already been setup and is up and running.

Step 1 Enter the data export command from *cd $CISCO_CE_HOME/bin* directory:

./dataexport

Tip Make sure you type the period (**.**) prior to the command.

Step 2 Follow the sequence of prompts to enter information of the FTP site and storage location (absolute pathname including filename).

Example of dataexport Prompts

```
Entering Data Export
Type ctrl-c to exit

Enter FTP server (hostname.domainname or IP address): sername.cisco.com
Enter username used for FTP server: smith
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of data file on FTP server: /users/smith/migration.tar
```

Note To export data to a remote FTP site from the Cisco Configuration Engine release 2.0, follow the below steps.

Step 3 Insert the Release 3.5.3 CD-ROM into the CD drive of your host to be upgraded.

Step 4 To mount the CD-ROM, login as **root**, then enter the command:

mount /mnt/cdrom

Step 5 Copy the following image file from *RPMS/DataExport to cd $CISCO_CE_HOME/bin* directory.

- **cns_export_utils_1.6.sh**
- **cnsexport_1.6.sh**
- **cns_import_utils.pl**
- **dataexport**
- **setuputils.pm**

Step 6 After copying the image files, perform the Step 1 and 2.

Install Release 3.5.3 Software

Install the Cisco Configuration Engine 3.5.3 software on the target system. For the procedure, see Installing the Software, page 1-4.

Run *datamigrate* and Configure the System

Step 1 Log in as **root**.

Step 2 Start datamigrate by entering the following command:
$CISCO_CE_HOME/bin/datamigrate

The script proceeds in the following three stages:

a. Acquires information of the FTP server that stores the migration data and retrieves the data.

b. Starts Release 3.5.3 setup prompts and configures the system.

c. Populates internal directory storage with retrieved data.

Example of datamigrate Prompts

```
Enter FTP server (hostname.domainname or IP address): sername.cisco.com
Enter username used for FTP server: smith
Enter FTP password: *****
Re-enter FTP password: *****
Enter absolute pathname of data file on FTP server: /users/smith/migration.tar
```

Uninstalling the Software

To uninstall the software, use the uninstall script command, **ce_uninstall.sh**. The uninstall script is copied into */var/ciscoce/install* directory. This script reads the *installdata.xml* file to do package uninstallation. It proceeds in the following four stages:

1. Stops all running Cisco Configuration Engine 3.5.3 processes.
2. Removes all database data from BDB.
3. Removes installed database software if it is BDB.
4. Removes all presence of installed packages.

To uninstall Cisco Configuration Engine 3.5.3 packages without checking the installation status, use the **$ce_uninstall.sh {-force}** command. The option **-force** in the uninstallation script removes all Cisco Configuration Engine 3.5.3 packages except the preexisting shared packages on the target host.

Synchronizing Clocks

The clock (date and time) on your host and the clock on the PC that you use to access the Cisco Configuration Engine 3.5.3 user interface must be synchronized. This is particularly important when scheduling an update-image job for a future time (see the *Cisco Configuration Engine Administration Guide*).

If the host clock lags the PC clock, the user interface will not allow you to schedule the job and you will see an error message. For example, if your host clock reads 11:10 while the PC clock reads 12:10, the user interface will not allow a job to be scheduled before 12:10. You will see the following error message:

```
Please input a future time.
```

To verify that the clocks are correctly synchronized, make sure you have entered a valid time value on the client side. You can do this by using the clock on your PC with the browser used to access the Cisco Configuration Engine user interface.

Information About the Installation Script

The default behavior of the install script, *ce_install.sh,* is defined in the *installRule.solaris.xml* i*nstallRule.linux.xml, or* the i*nstallRule.linux5.xml* file as appropriate. This file is located in the same directory where the Cisco Configuration Engine 3.5.3 tar file is untarred. The *installRule* files contain the following information:

- Which package for which version should be installed.
- Can a package be shared.
- The behavior of the installation if the package exists or not.
- The methods to install and un-install the package.

The result of the installation is logged under */var/log/CNSCE/install.log.* This log file lists exactly what is being installed into the system. For a successful install, the contents of this log file should be the same as the contents of *installRule.solaris.xml* or the i*nstallRule.linux.xml* file as appropriate.

The *installError.xml* file is generated if there is an error during installation. Other files, such as those that contain all Cisco Configuration Engine 3.5.3 related environmental variables, are also generated during the installation stage including: *global.sh*, *global.csh*, *global.pm*, and *installdata.properties*.

Options for Setup Script

- Interactive Mode—This is the default option that prompts the user to provide inputs such as installation base directory, environment variables, and store them in a data file. The default value is read from *setupRule.xml* under: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/*.

  The result is stored in the log file: */var/log/CNSCE/appliance-setup.log*.

- Batch Mode—Reads all the information it requires for setup without user interaction from the data file: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/setupRule.xml*.

  The result is stored in the log file: */var/log/CNSCE/appliance-setup.log*.

Note Before running batch mode the first time, you must run the utility script **$CISCO_CE_HOME/bin/passwdEncryption.pl**. This creates encrypted passwords and loads them into the *setupRule.xml* file. The passwords in XML must be in encrypted text, not plain text.

Information About the Check Script

The default behavior of the Check script, *ce_check.sh* is defined in the *installRule.solaris.xml* i*nstallRule.linux.xml, or* the i*nstallRule.linux5.xml* file as appropriate. The script checks for the following:

- Root user
- OS

- CPU
- RAM
- Disk space for /var directory
- List of dependent packages and their versions. Reports errors and warnings when there is a mismatch in the requirement and package dependencies.

The result is stored in the checkError.log file in the same directory where the Cisco Configuration Engine 3.5.3 tar file is untarred.

Note The disk space requirement check for *${CISCO_CE_INSTALL_ROOT}* directory is done only during the installaiton.

Troubleshooting the Installation

For more information about the installation script, see *Cisco Configuration Engine Troubleshooting Guide*.

CHAPTER 2

Running the Setup Program

This chapter provides information about how to use the Setup program to configure your host system for Cisco Configuration Engine 3.5.3.

This chapter contains the following sections:

Tip The Encryption and Authentication settings in the Setup program allow you to enable security so that communication between the Cisco Configuration Engine and CNS Agents is secure. We strongly recommend that you enable security by answering **y** to the Encryption and Authentication setup prompts. For details, see Encryption Settings, page 2-7 and Authentication Settings, page 2-8. To enable security in the CNS agent devices, see Chapter 4, "Setting Up CNS Agent Devices for Secure Communication."

Running Setup

System configuration for Cisco Configuration Engine 3.5.3 is accomplished using the Setup program. You must run the Setup program when you start the system for the first time. Before running the Setup program, make sure you're in BASH shell mode. At the prompt, enter:
/bin/bash, SHELL=/bin/bash, export SHELL

Then, from the directory where Cisco Configuration Engine 3.5.3 software files are located, use the **./setup** command.

Limitations and Restrictions

- Once you have committed changes (`Commit changes (y/n): y`), it cannot be aborted by entering **Ctrl-c**.
- All password values in the Setup program must contain alphanumeric characters *only*. Special characters have different meanings in the UNIX shell and should *not* be used for passwords.
- Device Name values can contain the following characters only: period (.), underscore (_), hyphen (-), and alphanumeric characters.
- Group Name values can contain the following characters only: underscore (_) and alphanumeric characters.

Internal Directory Mode Setup Prompts

The following example shows the standard set of prompts for Internal Directory mode:

Notes

- Default values are shown within brackets: […]. To use a default value, simply press **Return**.
- Sample user inputs are shown in **bold** text.

Note To understand the internal mode setup prompts, see Understanding the Internal Mode Setup Parameters, page 2-6.

```
Choose operational mode of system. 0=internal directory mode, 1=external
directory mode. [0]

Enter country code: us
Enter company code: cisco

Do you want to authenticate Configuration Engine GUI users externally?
(y/n) [n] y
Enter IP Address of external directory server: 17x.xx.xxx.xxx
Enter port number of external directory server: [389]
Enter prefix for user name in external directory server: [cn]
Enter suffix for user name in external directory server: o=myorg,c=us
Do you want to enable authorization? (y/n) [n] y
Enter UserDN for external directory server: cn=simpleuser,o=myorg,c=us
Enter password for the above user: *****
Re-enter password for the above user: *****
Enter role attribute name in user objectclass which defines the role:
[description]
Enter role attribute value which defines the role of an administrator:
[administrator]

        Configuration Engine user ID is used to log in to the web-based GUI
        and manage network device objects and templates. This account does
        NOT have shell access.

Enter Configuration Engine login name: admin
Enter Configuration Engine login password: *****
Re-enter Configuration Engine login password: *****
Enter internal LDAP server port number: [389]
Enter internal LDAP server password: *****
Re-enter internal LDAP server password: *****
```

```
Email service settings:
-----------------------

Enter SMTP server (hostname.domainname or IP address):

Encryption settings:
--------------------

Enable cryptographic (crypto) operation between Event Gateway(s)/Config
server and device(s) (y/n)? [n] y
Enter absolute pathname of server key file: [/user/server.key]
Enter absolute pathname of server certificate file: [/user/server.crt]

Enabling plaintext operation will increase security risk.

Enable plaintext operation between Config Server and devices/GUI
administration (y/n)? [y]
Enable plaintext operation between Event Gateway and devices (y/n)? [y]
Enter port number for http web access: [80]
Enter port number for https web access: [443]
Enter Tomcat internal port number: [8009]
Enter Tomcat shutdown port number: [8005]

Authentication settings:
------------------------

IOS Devices are normally authenticated before being allowed to connect to the Event
Gateway/Config Server. Disabling authentication will increase security risk.

Enable authentication (y/n)? [n] y

The default bootstrap password should be the same as the "cns password" specified in your
bootstrap file. If you are not sure what it is and would like to finish the setup now, you
could enter a default password of your choice and then change it by using "update" option
through the Security Manager bootstrap GUI.

Enter the default bootstrap password:*****
Re-enter the default bootstrap password: *****

Event services settings:
------------------------

Enter Event Gateway application parameter(s) for NSM: [config]
Enable Event Gateway debug log (y/n)? [n]
Enter log file rotation timer (minutes, 0 = no rotation): [15]
Enter max log file size (Kbytes): [3072]
Enable log backup (y/n)? [y]

The event gateway ports 11011 and 11012 are reserved for port
        automatic allocation. If you want to zero touch deploy your devices
        or have devices currently configured to use to these 2 ports, then
        you should enable this feature and enter the current "cns event"
        commands in the later part of this setup. For details please refer
        to the CE installation and configuration guide.

Enable Event Gateways port automatic allocation (y/n)? [y]

        Each Event Gateway process serves 500 devices. Maximum number of
        Event Gateways allowed is 10.

Enter number of Event Gateways that will be started with crypto operation:
[0] 10
Is this a primary CE (y/n)? [y]
```

```
The CNS Event command configures how the managed devices should connect to this particular
CE. The command entered in the following line should match what's configured on the
devices WITHOUT the "cns event imgw-test35" and port number portion of the CLI.

For example, if "cns event imgw-test35 11011 source Vlan1 keepalive 120 2 reconnect 10" is
configured on devices, then the command "source Vlan1 keepalive 120 2 reconnect 10" should
be entered in the following line.
If this is a backup CE and CLI  "cns event imgw-test35 11011 source Vlan1 backup" is
configured on devices, then the command "source Vlan1 backup" should be entered in the
following line.

Unable to enter a correct CLI could cause the managed devices not be able to connect to
this CE.

Enter CNS Event command: cns event imgw-test35 11011 source Vlan1 keepalive 120 2
reconnect 10
Enter Cisco-CE Event Bus Network Parameter: [imgw-test35]
Enter Cisco-CE Event Bus Service Parameter: [7500]
Enter Cisco-CE Event Bus Daemon Parameter: [7500]
Enable Cisco-CE Event Bus routing daemon logging (y/n)? [n]
Enter http port for Event Bus Web Administration GUI: [7580]

Event Bus Web Admin port should always be closed unless the Web
admin GUI is needed. Keeping web admin port open is a security
risk.

Would you like to open Event Bus Administration port (y/n)? [n]

Current settings of IMGW:
-------------------------
Gateway ID: imgw-test35
Run as daemon (y/n)? y
Timeout in seconds for a CLI command to complete: 180
Timeout in seconds to get the next prompt in Telnet session: 60
Concurrent Telnet session limit: 25
Hoptest success retry interval (sec): 0
Hoptest failure retry interval (sec): 0
Logging level (verbose, error, silent): error
Log file Prefix: IMGW-LOG
Log file size (bytes): 50331648
Log file rotation timer (seconds): 60
Logging mode (append, overwrite): append
Alternative username prompt for device using TACACS/RADIUS:
Alternative password prompt for device using TACACS/RADIUS:

Re-configure IMGW (y/n)? [n]

CE Monitor Settings:
------------------------

Enter CE Monitor timer (seconds): [1800]

Web Services settings:
----------------------

Enable CEConfigService web service (y/n)?  [y]
Enable CEImageService web service (y/n)?  [y]
Enable CEAdminService web service (y/n)?  [y]
Enable CEExecService web service (y/n)?  [y]
Enable CENSMService web service (y/n)?  [y]
```

```
Multi-Zone Settings:
--------------------

Your box has multiple IP Addresses assigned: 17x.xx.xxx.xx 17x.xx.xxx.xxx
You can create http zones so that http traffic can be limited on the IP Address
17x.xx.xxx.xx. Only selected URLs can be accessed using IP Address 17x.xx.xxx.xx. For
details, you can check the CE Installation and Configuration Guide.

Do you want to create zones to have limited access to CE from public
network (y/n)?  [n] y
Do you want to allow plain-text http access to CE from public network
(y/n)?  [y] y

Please review the following parameters:
country code: us
company code: cisco
Do you want to authenticate Configuration Engine GUI users externally? (y/n) y
IP Address of external directory server: 172.xx.xxx.1xx
port number of external directory server: 389
prefix for user name in external directory server: cn
suffix for user name in external directory server: o=myorg,c=us
Do you want to enable authorization? (y/n) y
UserDN for external directory server: cn=simpleuser,o=myorg,c=us
password for the above user: *****
role attribute name in user objectclass which defines the role: description
role attribute value which defines the role of an administrator: administrator
Configuration Engine login name: admin
Configuration Engine login password: *****
internal LDAP server port number: [389]
internal LDAP server password: *****
SMTP server (hostname.domainname or IP address):
Enable cryptographic (crypto) operation between Event Gateway(s)/Config server and
device(s) (y/n)? y
absolute pathname of server key file: [/user/server.key]
absolute pathname of server certificate file: [/user/server.crt]
Enable plaintext operation between Config Server and devices/GUI administration (y/n)? y
Enable plaintext operation between Event Gateway and devices (y/n)? y
port number for http web access: 80
port number for https web access: 443
Tomcat internal port number: 8009
Tomcat shutdown port number: 8005
Enable authentication (y/n)? y
the default bootstrap password: *****
Event Gateway application parameter(s) for NSM: config
Enable Event Gateway debug log (y/n)? n
log file rotation timer (minutes, 0 = no rotation): 15
max log file size (Kbytes): 3072
Enable log backup (y/n)? y
number of Event Gateways that will be started with crypto operation: 10
Is this a primary CE (y/n)? y
CNS Event command: cns event imgw-test35 11011 source Vlan1 keepalive 120 2 reconnect 10
Cisco-CE Event Bus Network Parameter: imgw-test35
Cisco-CE Event Bus Service Parameter: 7500
Cisco-CE Event Bus Daemon Parameter: 7500
Enable Cisco-CE Event Bus routing daemon logging (y/n)? n
http port for Event Bus Web Administration GUI: 7580
Would you like to open Event Bus Administration port (y/n)? n
Re-configure IMGW (y/n)? n
CE Monitor timer (seconds): 1800
Enable CEConfigService web service (y/n)? y
Enable CEImageService web service (y/n)? y
Enable CEAdminService web service (y/n)? y
Enable CEExecService web service (y/n)? y
Enable CENSMService web service (y/n)? y
```

```
Do you want to create zones to have limited access to CE from public network (y/n)? y
Do you want to allow plain-text http access to CE from public network (y/n)? y

Warning: setup cannot be aborted while committing changes.
```

Understanding the Internal Mode Setup Parameters

The following sections describe the setup parameters:

- Login Name, LDAP Password, LDAP Port Number Settings, page 2-6
- Email Service Setting, page 2-6
- Encryption Settings, page 2-7
- Authentication Settings, page 2-8
- Event Services Settings, page 2-9
- Web Services Settings, page 2-11

Login Name, LDAP Password, LDAP Port Number Settings

Configuration Engine login name/password: Define the administrator account and password for accessing Cisco Configuration Engine GUI.

Enter internal LDAP server port number: Define the port number that should be used by the Lightweight Directory Access Protocol (LDAP) server. Default value is 389.

Enter internal LDAP server password: Define internal-directory-account password for the two internal administrative users: **dcdadmin** and **cdauser1**.

Table 2-1 Valid Values for General Parameters

Parameter	Type	Length/Range
Configuration Engine login name	Alphanumeric	1 – 30
Configuration Engine login password	Password	1 – 12
Internal LDAP server port number	Port number	0 – 65535
Internal LDAP server password	Password	1 – 20

- Password type refers to ASCII characters that are between the octal values 040 (space) and 176 (~) inclusive.
- Alphanumeric type refers to alphabetic and numeric characters plus the underscore (_) symbol.

Email Service Setting

Enter SMTP server (hostname.domainname or IP address): Specifies the SMTP server hostname or IP address to enable email notification service. The SMTP server is used to send out email. This parameter is optional. If you do not wish to provide email service, leave it blank.

Encryption Settings

Note The Encryption and Authentication settings in the Setup program allow you to enable security so that communication between the Cisco Configuration Engine server and CNS agent devices is secure. We strongly recommend that you enable security by answering **y** to the Encryption and Authentication setup prompts. To enable security in the CNS agent devices, see Chapter 4, "Setting Up CNS Agent Devices for Secure Communication."

Note For scalability, we recommend that you distribute devices evenly among Event Gateway ports. See Chapter 6, "Scalability Among Event Gateway Ports."

Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s) (y/n): This option enables crypto Secure Socket Layer (SSL) operation. The web server listens on TCP port 443, and responds to https requests (for example, *https://machine/config/login.html*). The event gateway listens to ports 11012, 11014, and so on (depending on the number of gateways started). All data between your host and the far end is encrypted. The SSL protocol (combined with valid certificates) ensures that your host is authenticated by the far end. In order to complete SSL configuration, valid certificates need to be placed on your host. See "Configuring SSL Certificates" section on page 2-20 for details. For testing, after configuration open an SSL connection to each port (**openssl s_client –connect hostname:port**). This should be done for both enable and disable cases.

If disabling crypto operation, the rest of the prompts in this section are omitted.

Enable plaintext operation between Config Server and devices/GUI administration (y/n): This option enables plaintext config server operation. In addition to listening on TCP port 443 for crypto connections, the web server also listens on TCP port 80 for plaintext connections, responding to HTTP requests (for example, *http://machine/config/login.html*). **If crypto is disabled, plaintext between Config Server and devices/GUI administration is enabled.**

Enable plaintext operation between Event Gateway and devices (y/n): This prompt enables/disables the prompt: **number of Event Gateways that will be started with plaintext operation**, which is in Event service settings (see "Event Services Settings" section on page 2-9).

Port number for http web access: Specify the port number to be used for http web access. The default is 80.

Enter port number for https web access: Specify the port number to be used for secure http web access. The default is 443.

Enter Tomcat internal port number: Specify the port number for internal communication between Apache and Tomcat. The default is 8009.

Enter Tomcat shutdown port number: Specify the shutdown port number for Tomcat. The default is 8005.

Table 2-2 Valid Values for Encryption Parameters

Parameter	Type	Length/Range
Enable cryptography (crypto) between Event Gateway(s)/Config Server and device(s)	y, n	—
Absolute pathname of key file	Alphanumeric	1 – 255
Absolute pathname of certificate file	Alphanumeric	1 – 255

Table 2-2 Valid Values for Encryption Parameters (continued)

Parameter	Type	Length/Range
Enable plaintext between Config Server and devices/operators	y, n	—
Enable plaintext operation between Event Gateway and devices	y, n	—
port number for http web access	Port number	0 – 65535
port number for https web access	Port number	0 – 65535
Tomcat internal port number	Port number	0 – 65535
Tomcat shutdown port number	Port number	0 – 65535

Authentication Settings

Note The Encryption and Authentication settings in the Setup program allow you to enable security so that communication between the Cisco Configuration Engine server and CNS agent devices is secure. We strongly recommend that you enable security by answering **y** to the Encryption and Authentication setup prompts. To enable security in the CNS agent devices, see Chapter 4, "Setting Up CNS Agent Devices for Secure Communication."

Enable authentication (y/n): Enable IOS device authentication mechanism within your host. To test, attempt to connect an IOS device, with an incorrect password, to the Configuration Engine 1.6. The password can be changed on IOS with the hidden command **cns password newPassword**.

Enter the default bootsrap password: Define the default bootstrap password for accessing the Cisco Configuration Engine GUI. The password should be same as the **cns password** specified in your bootstrap file. If you are not sure what it is and would like to finish the setup now, you could enter a default password of your choice and then change it by using "update" option through the Security Manager bootstrap GUI.

Note If disabling device authentication, connection to devices with pre 12.2(10)T IOS is implicitly allowed.

Table 2-3 Valid Values for Authentication Parameters

Parameter	Type	Length
Enable authentication	y, n	—
Enter the default bootstarp password	Alphanumeric	—

External Authentication

The Cisco Configuration Engine can authenticate a user by using external authentication application. When a user logs into the Cisco Configuration Engine, instead of authenticating the user by using the Cisco Configuration Engine LDAP server, the Cisco Configuration Engine forwards the authentication request to an external authentication application. The Cisco Configuration Engine can support the LDAP based authentication and integrate with the MS Active Directory.

The Cisco Configuration Engine can authenticate the user both internally and externally based on the user selection during the Cisco Configuration Engine setup.

During the Cisco Configuration Engine setup, the administrator can select the authentication mode. The Cisco Configuration Engine prompts for IP address and user credentials for the remote LDAP server.

Choose the authentication mode of the system *0=internal mode, 1=external mode*.

This example shows how to set the external authentication settings.

```
Enter IP Address of external directory server: 10.1.2.3
Enter port number of external directory server: [389]
Enter prefix for user name in external directory server: [cn]
Enter suffix for user name in external directory server: o=myorg,c=us
```

Authorization

The Cisco Configuration Engine does not support task or resource-based authorization. However, the Cisco Configuration Engine GUI have Admin and Operator user levels. Depending on the role of the user, the appropriate GUI screens are shown to the user.

Backup Authentication-Authorization

To support the existing Cisco Configuration Engine users, backup authentication and authorization is supported for the external authentication mechanism. The Cisco Configuration Engine user who logs in is authenticated against the external application. If the external authentication fails, the user is authenticated against the Cisco Configuration Engine LDAP Server. The fall-back server will be the LDAP directory used by the Cisco Configuration Engine (internal or external). If the user chooses internal authentication, the Cisco Configuration Engine LDAP is used for authentication and there will be no fall-back authentication server used.

Event Services Settings

Event Gateway application parameter(s) for NSM: Specifies the application namespace to be used in NameSpace Mapper for resolving mapping. The default namespace used is **config**.

Event Gateway debug log: Send Event Gateway **debug** output to the log file: */var/log/CNSCE/evtgateway.*

Log file rotation timer (minutes, 0 = no rotation): The time period to check whether event gateway log files should be log-rotated in current working directory. If the value is **0** then the event log files are not log-rotated. The default value is 2 minutes if event gateway debug logging is turned on and 5 minutes if event gateway debug logging is turned off. Valid values are 0 to 1440.

Max log file size (Kbytes): The file size above which log-rotation starts. The default is 3072 Kbytes. Valid values are 1 to 2097152 (Kbytes).

Log backup (y/n)? Indicates whether the event gateway log-rotated file should be copied to the backup directory */var/log/CNSCE/evt_gateway/backup*. Default is **y**; log files in */var/log/CNS* are tarred, time stamped and moved into the backup directory.

Number of Event Gateways that will be started with crypto operation: Specify the number of Event Gateway processes that should be started in crypto mode; for example, the number of Event Gateways that communicate with devices using SSL.

Note If crypto operation is disabled, this prompt is also disabled.

Is this a primary CE(y/n)? Specify the Cisco Configuration Engine as primary Cisco Configuration Engine.

Number of Event Gateways that will be started with plaintext operation: Specify the number of Event Gateway processes that should be started in plaintext mode; for example, the number of Event Gateway that communicate with devices without using SSL.

Note For dual processor, 2GB RAM system, the number of Event Gateways should not exceed 20.

Event CNS Event Command: Specify the CNS event command to configure the network element to connect to this particular Cisco Configuration Engine. The command entered should match with what is configured on the network element without the event gateway port number. For example, if **cns event ce-host 11011 source Vlan1 keepalive 120 2 reconnect 10** is configured on the device, then the command **cns event <ce-host> source Vlan1 keepalive 120 2 reconnect 10** should be entered, where **<ce-host>** is the IP address or hostname of the Cisco Configuration Engine server.

Event CNS Bus Network Parameter: Specify the outbound network interface of host system for publishing events. It can be an IP address, the name of the local network interface, a hostname, or multicast address.

Event CNS Bus Service Parameter: Specify the UDP port used for publishing and listening to events among Event Bus daemons. Dedicating a port for communication between a host system and its managing devices can reduce traffic caused by listening to other unrelated events. The default is 7500.

Enter CNS Event Bus Daemon Parameter: Specify the TCP port that should be used for the TCP connections between Event Bus daemon and its client applications. The default is 7500.

Enable CNS Event Bus routing daemon logging (y/n)? Enable or disable Event Bus logging. The default is disable. Log file can be found at */var/log/CNSCE/rvrd/rvrd.log*.

Enter http port for Event Bus Web Administration GUI: Specify the http port for accessing Event Bus Web Administration interface. The default is 7580.

Would you like to open Event Bus Web Administration port (y/n)? Enable or disable the http port for Event Bus Web interface access.

Table 2-4 Valid Values for Event Service Parameters

Parameter	Type	Range
Event Gateway application parameter(s) for NSM	Alphanumeric, dash, space	1 – unlimited
Event Gateway debug log	y, n	—
Log file rotation timer (minutes, 0=no rotation)	Timer	0 – 1440
Max log file size	File size	1 – 2097152 (Kbytes
Log backup (y/n)?	y, n	—
Number of Event Gateways that will be started with crypto operation	Integer	1-11 1-20 for dual processor, 2GB RAM

Table 2-4 Valid Values for Event Service Parameters (continued)

Parameter	Type	Range
Number of Event Gateways that will be started with plaintext operation	Integer	**crypto enabled:** 0-11 0-20 for dual processor, 2GB RAM **crypto disabled:**1-11 1-20 for dual processor, 2GB RAM
Is this a primary CE (y/n)	y, n	—
Event CNS Even Command	Command	—
Event CNS bus network parameter	Network parameter	—
Event CNS bus service parameter	Port number	0 – 65535
Event CNS bus daemon parameter	Port number	0 – 65535
Event CNS bus routing daemon logging (y/n)	y, n	—
HTTP port for Event Bus Web Administration GUI	Port number	0 – 65535
Open Event Bus Web Administration port (y/n)	y, n	—

Web Services Settings

The following Web Service interfaces are provided:

- **Enable CEConfigService web service**: Enable web service to send/acquire configurations to/from devices.
- **Enable CEImageService web service**: Enable web service to delete files, obtain an inventory of the hardware, file system(s) & their content, distribute or activate image(s) on devices.
- **Enable CEExecService web service**: Enable web service to execute show commands or reboot on devices.
- **Enable CEAdminService web service**: Enable web service to create and manage the various system objects used by the Cisco Configuration Engine to manage devices (such as devices, line-cards, images, configurations (templates), users, conditions, groups, passwords).
- **Enable CENSMService web service**: Enable web service to create and manage namespace, subjects in namespace and subject mappings in Namespace. It also includes an operational application programming interface (API) to resolve subjects.

Reconfigure IMGW Parameters

This section shows the set of prompts required for reconfiguring the IMGW settings.

```
Re-configure IMGW (y/n)? [n] y
Enter Gateway ID: [mainstreet]
```

```
Run as daemon (y/n)? [y]
Enter timeout in seconds for a CLI command to complete: [180]
Enter timeout in seconds to get the next prompt in Telnet session: [60]
Enter concurrent Telnet session limit: [20]
Remove temporary logs of Telnet sessions into devices (y/n)? [y]
Enter location of temporary logs of Telnet sessions into devices: [/tmp]
Enter hoptest success retry interval (sec): [7200]
Enter hoptest failure retry interval (sec): [3600]
Enter logging level (verbose, error, silent): [error]
Enter log file prefix: [IMGW-LOG]
Enter log file size (bytes): [50331648]
Enter log file rotation timer (seconds): [60]
Enter logging mode (append, overwrite): [append]
Alternative username prompt for device using TACACS/RADIUS:
Alternative password prompt for device using TACACS/RADIUS:
```

IMGW Parameter

Reconfigure IMGW: This yes/no prompt determines whether setup should display the section of prompts for re-configuring IMGW related parameters. Regular user should always answer **n**.

Gateway ID: Unique identifier assigned to the IMGW process. It is always set to hostname by default.

Run as daemon: Set to **y** for normal use. **n** is only used for debugging purposes.

Timeout in seconds for a CLI command to complete: The maximum waiting time in seconds for a command-line interface (CLI) to complete.

Timeout in seconds to get the next prompt in Telnet session: The maximum waiting time in seconds to get the next prompt in Telnet session.

Concurrent Telnet session limit: The maximum simultaneous Telnet connections that IMGW supports.

Remove temporary logs of Telnet sessions into devices: The y/n value that determines if IMGW should remove the temporary files it creates for download/exec.

Location of temporary logs of Telnet sessions into devices: File system location where IMGW should create the temporary files.

Hoptest success retry interval: Time interval in minutes for IMGW to check device in the Success list (devices for which connectivity-check succeeded).

Hoptest failure retry interval: Time interval in minutes for IMGW to check device in the Failure list (devices for which connectivity-check failed).

Logging level: Verbose mode logs both error and debugging messages. Error mode logs only error messages. Silent mode does not log any message.

Log file prefix: A prefix used to construct the name of the log file. The resulting filename is made up of the prefix and the IMGW gateway ID.

Log file size: Log file size that triggers log rotation.

Log file rotation timer: Time in seconds after which to check log-file size for log rotation.

Logging mode: Select whether to append new log to the end of the log file or overwrite the previous log.

Alternative username/password prompts for device using TACACS/RADIUS: When a device is authenticated by TACACS+ or RADIUS servers, the username/password prompts which are returned to the Telnet users are configurable. The **alternative username/password prompts** allow you to choose your own set of username/password prompts. If no inputs are entered, the default username/password prompts **Username:** and **Password:** are assumed.

Table 2-5 Valid Values for IMGW Parameters

Parameter	Type	Length/Range
Gateway ID	Alphanumeric	1 – 32
Run as daemon	y, n	
Timeout in seconds for a CLI command to complete	Integer	30 – 7200 (sec)
Timeout in seconds to get the next prompt in Telnet session	Integer	30 – 7200 (sec)
Remove temporary logs of Telnet sessions into devices	y, n	—
Location of temporary logs of Telnet sessions into devices	Full pathname	—
Concurrent Telnet Session Limit	Integer	1 – 25
Hoptest success retry interval (sec)	Integer	0 – 2147483647 (sec)
Hoptest failure retry interval (sec)	Integer	0 – 2147483647 (sec)
Logging level	verbose, error, silent	—
Log file prefix	Alphanumeric	1 – 32
Log file size (bytes)	Integer	5242880 – 4294967295 (bytes)
Log file rotation timer (minutes)	Integer	0 – 2147483647 (sec)
Log file rotation timer (seconds)	Integer	0 – 2147483647 (sec)
Logging mode	append, overwrite	—
Username prompt for device using TACACS/RADIUS	Printable ASCII characters	—
Password prompt for device using TACACS/RADIUS	Printable ASCII characters	—

External Directory Mode Setup Prompts

Most of the prompts in External Directory mode are identical to those for the Internal Directory mode except for the introduction of the External Directory mode settings and sample schema.

In the External Directory mode, the system is configured to contact the external directory storage for device information. Certain information that makes up the schema of the external directory such as attribute names (in the device class) and container locations must be entered during Setup.

To simplify the inputs, you can choose to use the predefined sample schema and construct your external directory accordingly.

Note No prompts are issued to set up FTP and TFTP File Servers in External Directory Mode as these services are always disabled in this mode. If you had previously set up FTP and/or TFTP in Internal Directory Mode, after switching to External Directory Mode the services will have been disabled. You will need to rerun the Setup program in Internal Directory Mode again to enable them.

The example shows the prompts for External Directory mode where the sample schema is enabled.

Notes

- Default values are shown within brackets: […]. To use a default value, simply press **Return**.
- Sample user inputs are shown in **bold** text.

Note To understand the external mode setup prompts, see Understanding the External Mode Setup Parameters, page 2-16.

```
Choose operational mode of system. 0=internal directory mode, 1=external
directory mode. [0] 1

Email service settings:
-----------------------

Enter SMTP server (hostname.domainname or IP address): abc.cisco.com

Encryption settings:

Enable cryptographic (crypto) operation between Event Gateway(s)/Config
Server and device(s) (y/n)? [n] y
Enter absolute pathname of key file: /a/b/c
Enter absolute pathname of certificate file: /a/b/c

        Enabling plaintext operation will increase security risk.

Enable plaintext operation between Config Server and devices/GUI
administration (y/n)? [y]
Enable plaintext operation between Event Gateway and devices (y/n)? [y]
Enter port number for http web access: [80]
Enter port number for https web access: [443]
Enter Tomcat internal port number: [8009]
Enter Tomcat shutdown port number: [8005]

Authentication settings:
------------------------

        IOS Devices are normally authenticated before being allowed to
        connect to the Event Gateway/Config Server. Disabling
        authentication will increase security risk.

Enable authentication (y/n)? [n]

Event services settings:
------------------------
```

```
Enter Event Gateway application parameter(s) for NSM: [config]
Enable Event Gateway debug log (y/n)? [n]
Enter log file rotation timer (minutes, 0 = no rotation): [15]
Enter max log file size (Kbytes): [3072]
Enable log backup (y/n)? [y]

        Each Event Gateway process serves 500 devices. Maximum number of
        Event Gateways allowed is 20.
Enter number of Event Gateways that will be started with plaintext
operation: [5] 4
Enter Cisco-CE Event Bus Network Parameter: [imgw-test7]
Enter Cisco-CE Event Bus Service Parameter: [7500]
Enter Cisco-CE Event Bus Daemon Parameter: [7500]
Enable Cisco-CE Event Bus routing daemon logging (y/n)? [n]
Enter http port for Event Bus Web Administration GUI: [7580]

        Event Bus Web Admin port should always be closed unless the Web
        admin GUI is needed. Keeping web admin port open is a security
        risk.

Would you like to open Event Bus Administration port (y/n)? [n]

External directory settings:
----------------------------
Do you want to authenticate Configuration Engine GUI users using external
Server ? (y/n) [n] y
Enter IP Address of external directory server: 10.1.2.3
Enter port number of external directory server: [389]
Enter prefix for user name in external directory server: [cn]
Enter suffix for user name in external directory server: o=myorg,c=us
Do you want to enable authorization? (y/n) [n] y
Enter UserDN for external directory server: cn=simpleuser,o=myorg,c=us
Enter password for the above user: *****
Re-enter password for the above user: *****
Enter role attribute name in user objectclass which defines the role: description
Enter role attribute value which defines the role of an administrator: admin

Current settings of IMGW:
-------------------------
Gateway ID: imgw-test7
Run as daemon (y/n)? y
Timeout in seconds for a CLI command to complete: 180
Timeout in seconds to get the next prompt in Telnet session: 60
Concurrent Telnet session limit: 25
Hoptest success retry interval (sec): 0
Hoptest failure retry interval (sec): 0
Logging level (verbose, error, silent): error
Log file Prefix: IMGW-LOG
Log file size (bytes): 50331648
Log file rotation timer (seconds): 60
Logging mode (append, overwrite): append
Alternative username prompt for device using TACACS/RADIUS:
Alternative password prompt for device using TACACS/RADIUS:
Re-configure IMGW (y/n)? [n]
```

Understanding the External Mode Setup Parameters

These parameter descriptions are for those parameters unique to the External Directory mode. The general parameter descriptions for the sample above (common to both modes) are listed beginning with "Understanding the Internal Mode Setup Parameters" section on page 2-6.

IP address of directory server: The location of the external directory expressed as IP address.

Port number of directory server: The service port number of the external directory.

Directory server login name: Directory user that has the administrative privileges for all objects under Cisco-CE context; for example, **admin**.

Directory server password: Directory user password.

User DN: The complete distinguished name for the directory administrative user.

Cisco-CE context: Directory context (DN) under which all Cisco Configuration Engine objects are created. This includes device objects, group objects, application objects, and event objects. These objects can be created inside containers under Cisco-CE context.

Use sample schema: Choose **y** for enabling the predefined sample schema and **n** for otherwise. See "Sample Schema" for the definition and default values of sample schema.

Table 2-6 Valid Values for General External Directory Mode Parameters

Parameter	Type	Length/Range
IP address of the Directory Server	IP address	—
Port number of the Directory Server	Port number	0 – 65535
Directory server login name	Alphanumeric	1 – 32
Directory server password	Alphanumeric	1 – 20
User DN	Name-value pair with space	3 – unlimited
Cisco-CE context	Name-value pair with space	3 – unlimited

Sample Schema

If you answer the first prompt (Use sample schema (y/n):) with **y** indicating that you want to use the sample schema, the default values shown in brackets in the sample below are used for all sample schema attributes and they do not appear.

If you answer the first prompt with **n** indicating you do not want to use the sample schema as is, the attributes of the sample schema appear along with their default values in brackets. You can overwrite any of these default values to create your own schema:

```
Use sample schema (y/n): n
Enter container name under which device objects are stored: [ou=CNSDevices]
Enter container name under which generic device objects are stored:
[ou=GenericDevices]
Enter container name under which PIX device objects are stored:
[ou=PIXDevices]
Enter container name under which linecard objects are stored:
[ou=LinecardDevices]
Enter container name under which application objects are stored:
[ou=CNSApplications]
Enter container name under which IMGW objects are stored: [ou=imgw]
Enter container name under which CIS objects are stored: [ou=CISObjects]
```

```
Enter container name under which image objects are stored: [ou=Images]
Enter container name under which CIS device objects are stored:
[ou=CISDevices]
Enter container name under which distribution objects for Image are stored:
[ou=Distributions]
Enter container name under which Query objects are stored: [ou=Query]
Enter objectclass for device object: [IOSConfigClass]
Enter template attribute name in device objectclass: [IOSconfigtemplate]
Enter config ID attribute name in device objectclass: [IOSConfigID]
Enter event ID attribute name in device objectclass: [IOSEventID]
Enter device category attribute name in device objectclass: [AdminDevType]

        Enabling Modular Router feature allows you to configure linecards
        independently of the slot numbers.

Would you like to use Modular Router Feature (y/n)? [y] y
Enter IOS device type attribute name in device objectclass: [IOSlinecardtype]
Enter IOS sub devices attribute name in device objectclass: [IOSsubdevices]
Enter IOS main device attribute name in device objectclass: [IOSmaindevice]
Enter IOS slot attribute name in device objectclass: [IOSslot]
Enter interfaces info attribute name in device objectclass: [IOSinterfacesinfo]
Enter controllers info attribute name in device objectclass: [IOScontrollerinfo]
Enter voiceports info attribute name in device objectclass: [IOSvoiceportinfo]
Enter Cisco-CE group attribute name in device: [parent]
Enter Cisco-CE password attribute name in device object class: [AuthPassword]
Enter objectclass for bootstrap password object: [CNSBootstrapPwdClass]
Enter bootstrap password attribute name in bootstrap password objectclass:
[CNSBootPassword]
```

Definitions

Device objects container name: The container in the directory under which device objects are created.

Generic device objects container name: The container in the directory under which generic device objects are created.

Groups objects container name: The container in the directory under which group objects are created.

Application objects container name: The container in the directory under which application objects are created.

IMGW objects container name: The container in the directory under which IMGW objects are created.

Object class: The name of the user defined object class for device object.

Template attribute name: Attribute of the device class (as specified in the Object-class prompt) that specifies the template file for the device object. Note this is not the template file itself, just the name of the attribute that has the value of the template filename.

Config ID attribute name: Attribute of the device class that uniquely identifies the device in the config-server domain.

Event ID attribute name: Attribute of the device class that uniquely identifies a device within the Event Gateway server.

Would you like to use Modular Router Feature (y/n)?: Enable/Disable the next seven modular router related schema prompts from IOS-device-type attribute name to voiceports-info attribute name.

IOS device type attribute name: Single-value string attribute which will be used to store device type information in the directory.

IOS sub devices attribute name: Attribute that stores sub-device list associated with main device in the directory. Note this has to be a multi-valued attribute.

IOS main device attribute name: Attribute that stores the name of the main device of a sub-device in the directory.

IOS slot device attribute name: Attribute that stores the inventory details related to slot numbering.

Interfaces info attribute name: Attribute that stores the inventory details related to interfaces.

Controllers info attribute name: Attribute that stores the inventory details related to controllers.

Voiceports info attribute name: Attribute that stores the inventory details related to voice-ports.

Cisco-CE group attribute: The attribute of the device class that specifies the group(s) to which the device object belongs. Note that this is only an attribute name, but not the groups themselves. **In addition, it is only required when NSM directive is set to http mode**.

Cisco-CE password attribute name in device object class: The attribute of the device class that stores the value that the host system expects as the CNS password from the IOS device. **If bypass authentication is "y", this prompt is disabled.**

objectclass for bootstrap password object: The name of the user defined object class for the bootstrap password object. **If bypass authentication is "y", this prompt is disabled.**

Bootstrap password attribute name in bootstrap password object class: The attribute of the bootstrap password class that stores the value that the host system uses as the bootstrap password. **If bypass authentication is "y", this prompt is disabled.**

Table 2-7 Valid Values for Sample Schema Parameters

Parameter	Type	Length
Device object container name	Name-value pair with space	3 – unlimited
Generic device object container name	Name-value pair with space	3 – unlimited
Group object container name	Name-value pair with space	3 – unlimited
Application container name	Name-value pair with space	3 – unlimited
Object class	Alphanumeric	1 – 80
Template attribute name	Alphanumeric	1 – 80
Config ID attribute name	Alphanumeric	1 – 80
Device ID attribute name	Alphanumeric	1 – 80
Event ID attribute name	Alphanumeric	1 – 80
IOS device type attribute name	Alphanumeric	1 – 80
IOS sub device type attribute name	Alphanumeric	1 – 80
IOS main device type attribute name	Alphanumeric	1 – 80
IOS slot attribute name	Alphanumeric	1 – 80
Interfaces info attribute name	Alphanumeric	1 – 80
Controllers info attribute name	Alphanumeric	1 – 80
Voiceports info attribute name	Alphanumeric	1 – 80
Cisco-CE group attribute	Alphanumeric	1 – 80
Cisco-CE password attribute name	Alphanumeric	1 – 80
Objectclass for bootstrap password object	Alphanumeric	1 – 80
Bootstrap password attribute name	Alphanumeric	1 – 80

Command Line Support for Start/Stop Components

Cisco Configuration Engine 3.5.3 supports start/stop for the following components:

- http/tomcat (webserver): **/etc/init.d/httpd {start|stop}**
- IMGW: **/etc/init.d/Imgw {start|stop}**
- Event gateway: **/etc/init.d/EvtGateway {start|stop} [port number]**
- Event gateway crypto: **/etc/init.d/EvtGatewayCrypto {start|stop} [port number]**

Cisco Configuration Engine 3.5.3 includes two new scripts to handle start and stop components. Some servers have dependency to other servers, therefore the shutdown and startup script is not provided for these types of servers. For example, Tibco has to be up for http/tomcat, if Tibco is shutdown, and brought up again, the webservers, httpd and tomcat, that rely on Tibco will have connection problem, therefore Tibco restart is not supported.

- **ce_startup** – a script to combine all the start up scripts for different components

  This script is located in: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/*

  -all: default option that bring up all the services

  -http: includes Apache, Tomcat, config server, image server, web service

  -imgw: start imgw server

  -eventgw: event gateway including event gateway crypto. This script should read the setup data file, *varsetup.dat*, for the user input *enable_ssl*; if the answer is **y** (yes), this script should run EvtGatewayCrypto; otherwise, run EvetGateway.

  -monitor: Configuration Engine Monitor scripts.

- **ce_shutdown** – a script to combine all the stop scripts for different components

  This script is located in: *${CISCO_CE_INSTALL_ROOT}/CSCOcnsie/bin/*

  -all: default option that bring down all the services

  -http: includes Apache, Tomcat, config server, image server, webservice

  -imgw: imgw server

  -evtgw: event gateway including event gateway crypto

  -monitor: Configuration Engine Monitor scripts

Registering System in DNS

Register the system in DNS, using the system hostname as its DNS name.

Caution If you do not register the system in DNS using the system hostname as its DNS name, network connectivity problems can occur.

Events are sent to the router with the hostname as the identifier, not the IP address. Consequently, if your host system is not registered in DNS, the routers are not able to find it and cannot download configurations.

Configuring SSL Certificates

To configure SSL, you must generate a valid certificate:

Step 1 On any UNIX host that has OpenSSL installed, enter the following commands:

```
% openssl genrsa -out server.key 1024
% chown root:root server.key
% chmod 400 server.key
% openssl req -new -key server.key -out server.csr
```

Step 2 Ensure that the Common Name is the fully qualified name of your host, for example: www.company.com

Step 3 Send the file *server.csr* to the Certificate Authority (CA) for signing.

Note The files *server.key* and *server.crt* must be present on your host system.

Verifying Software Installation

Step 1 Go to a different computer and bring up a web browser.

The Cisco Configuration Engine supports:

- Java SE Development Kit 6 update 5 and above
- Internet Explorer 6.0 and above

Step 2 On the net-site window enter the URL for the Cisco Configuration Engine.

For example: **http://<***ip_address***>**

where: <*ip_address*> is the IP address you entered during host system configuration. You can use the hostname if the name has been defined and registered within your DNS domain.

Note If you have enabled encryption in the Setup program, you must use **https://<***ip_address***>.**

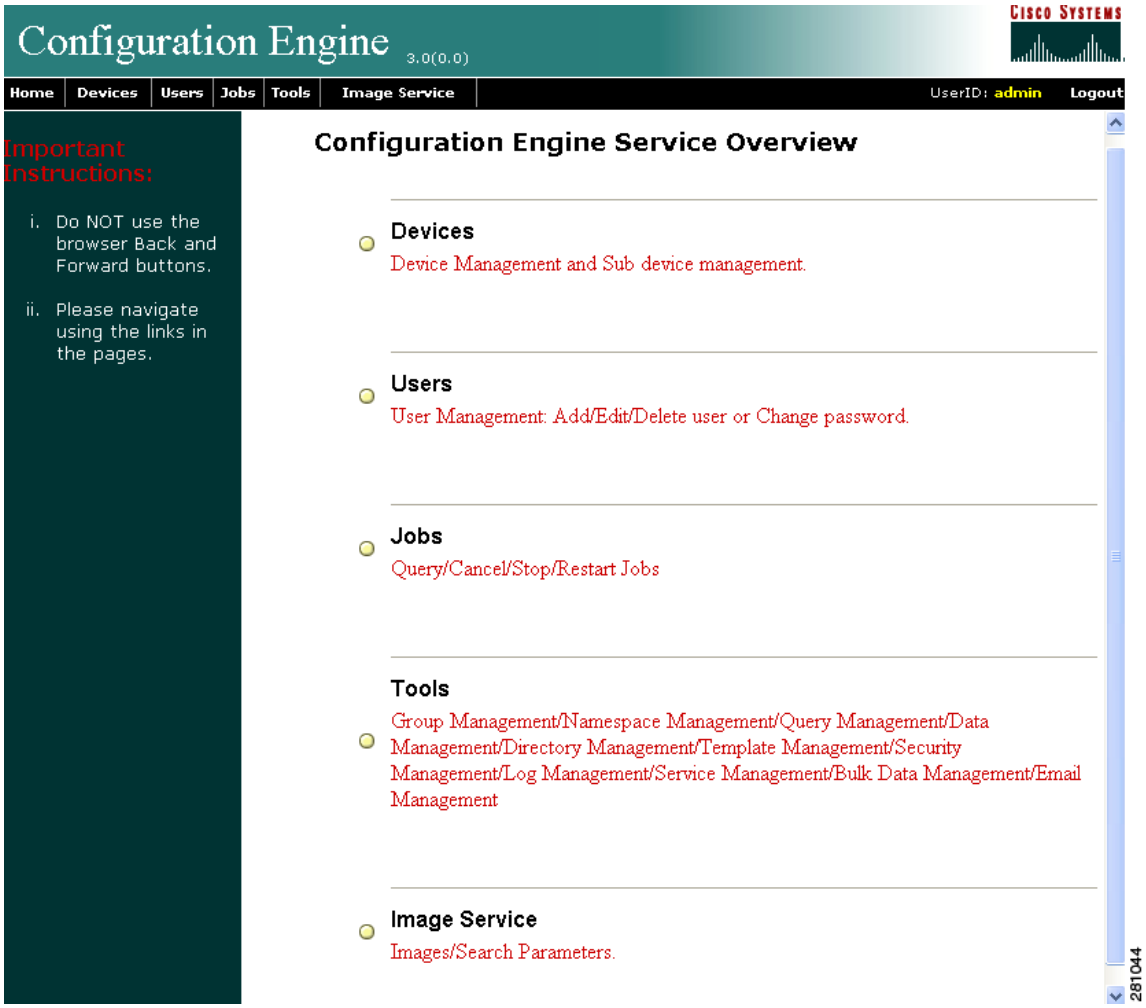
The Cisco Configuration Engine login page appears.

Step 3 Enter the ConfigService AdminID and Password that you entered during host system configuration.

The Home page appears.

If you have reached the Cisco Configuration Engine Home page (Figure 2-1), you have verified the successful installation on the Cisco Configuration Engine.

Figure 2-1 Internal Directory Mode Home Page



Reimaging System

If the image on your hard disk becomes corrupted, but the disk is operational (you can restart from the hard disk), you can reimage your system by uninstalling the Cisco Configuration Engine software, then reinstalling it.

CHAPTER 3

Configuring Cisco IOS CNS Agents

You must configure the Cisco Configuration Engine as well as the agent devices (routers and switches) connected to it. This chapter provides a brief overview of the Cisco Configuration Engine software and also provides information about configuring the Cisco IOS Cisco Networking Services (CNS) agents.

Note

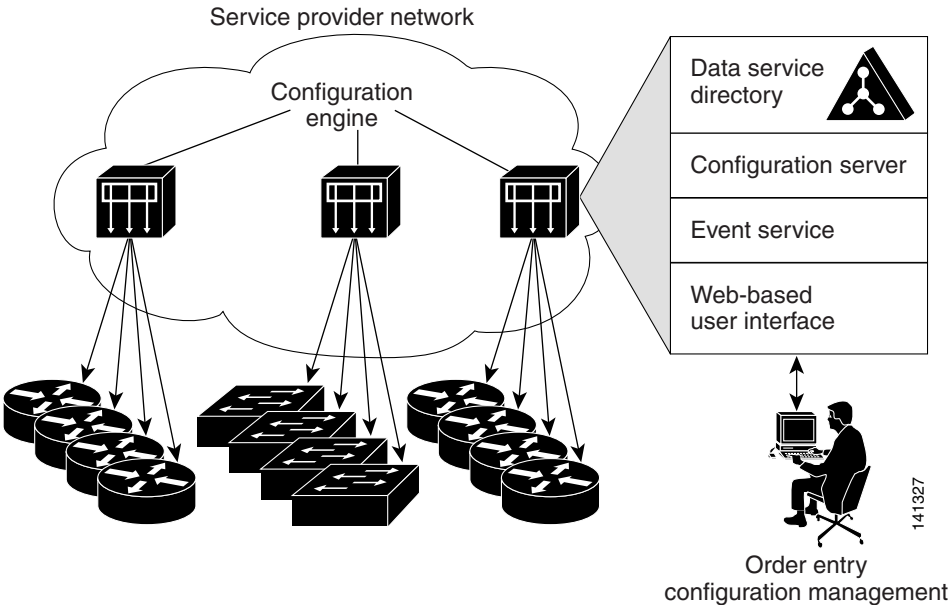
- For complete configuration information for the Cisco Configuration Engine, see the *Cisco Configuration Engine Administration Guide* at: http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/3.5.3/administration/guide/CE_ag.html
- For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Network Management Command Reference, Release 12.4* at: http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html

This chapter contains the following sections:

Understanding Cisco Configuration Engine Software

The Cisco Configuration Engine is a network management software that acts as a configuration service for automating the deployment, management, and upgrading of network devices and services (see Figure 3-1). Each Configuration Engine manages a group of Cisco devices (routers and switches) and the services that they deliver, storing their configurations and delivering them as needed. The Cisco Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

Figure 3-1 Cisco Configuration Engine Architectural Overview



The Cisco Configuration Engine supports standalone and server modes:

- In standalone mode, the Cisco Configuration Engine supports an embedded Directory Service. In this mode, no external directory or other data store is required.
- In server mode, the Cisco Configuration Engine supports the use of a user-defined external directory.

The Cisco Configuration Engine has the following CNS components:

- Configuration Service (web server, file manager, and namespace mapping server)
- Event Service (event gateway)
- Data Service Directory (data models and schema)

The following sections provide more information:

- Configuration Service, page 3-2
- Event Service, page 3-3
- CNS IDs and Device Hostnames, page 3-3

Configuration Service

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a configuration server that works in conjunction with configuration agents located at each router. The Configuration Service delivers device and service configurations to Cisco IOS devices for initial configuration and mass reconfiguration by logical groups. Routers receive their initial configuration from the Configuration Service when they start up on the network the first time.

The Configuration Service uses Event Service to send events required to apply configuration changes and receive success and failure notifications.

The configuration server consists of a web server that uses configuration templates and the device-specific configuration information stored in the embedded (Internal Directory mode) or remote (External Directory mode) directory.

Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in the directory.

The configuration server uses HTTP to communicate with the Configuration Agent running on the managed Cisco IOS device. The configuration server transfers data in eXtensible Markup Language (XML) format. The configuration agent in the router uses its own XML parser to interpret the configuration data and to remove the XML tags from the received configuration.

The configuration agent can also perform a syntax check on received configuration files. The configuration agent can also publish events through the event gateway to indicate the success or failure of the syntax check.

Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of events. The Event Agent resides on Cisco IOS devices and facilitates communication between routers and the Event Gateway on the Cisco Configuration Engine.

The Event Service is a highly scalable publish-and-subscribe communication method. The Event Service uses subject-based addressing to help messages reach their destination. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.

NameSpace Mapper

The Cisco Configuration Engine includes the NameSpace Mapper (NSM), which provides a lookup service for managing logical groups of devices based on application, device or group ID, and event.

Cisco IOS devices recognize only event subject-names that match those configured in Cisco IOS software; for example, cisco.mgmt.cns.config.load. You can use the namespace mapping service to designate events by using any desired naming convention. When you have populated your data store with your subject names, NSM changes your event subject-name strings to those known by Cisco IOS.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

CNS IDs and Device Hostnames

The Cisco Configuration Engine assumes that a unique identifier is associated with each configured device. This unique identifier can take on multiple synonyms, where each synonym is unique within a particular namespace. The event service uses namespace content for subject-based addressing of messages.

The Cisco Configuration Engine intersects two namespaces, one for the event bus and the other for the configuration server. Within the scope of the configuration server namespace, the term *ConfigID* is the unique identifier for a device. Within the scope of the event bus namespace, the term *DeviceID* is the CNS unique identifier for a device.

Because the Cisco Configuration Engine uses both the event bus and the configuration server to provide configurations to devices, you must define both ConfigID and Device ID for each configured device.

Within the scope of a single instance of the configuration server, two configured devices cannot share the same value for ConfigID. Within the scope of a single instance of the event bus, two configured devices cannot share the same value for DeviceID.

ConfigID

Each configured device has a unique ConfigID, which serves as the key into the Cisco Configuration Engine directory for the corresponding set of device CLI attributes. The ConfigID defined on the device must match the ConfigID for the corresponding device definition on the Cisco Configuration Engine.

DeviceID

Each configured device participating on the event bus has a unique DeviceID, which is analogous to the device source address so that the device can be targeted as a specific destination on the bus. All devices configured with the **cns event ip port** global configuration command must access the event bus. Therefore, the DeviceID, as originated on the device, must match the DeviceID of the corresponding device definition in the Cisco Configuration Engine.

The origin of the DeviceID is defined by the Cisco IOS hostname of the device. However, the DeviceID variable and its usage reside within the event gateway adjacent to the device.

The logical Cisco IOS termination point on the event bus is embedded in the event gateway, which in turn functions as a proxy on behalf of the device. The event gateway represents the device and its corresponding DeviceID to the event bus.

The device declares its hostname to the event gateway immediately after the successful connection to the event gateway. The event gateway couples the DeviceID value to the Cisco IOS hostname each time this connection is established. The event gateway caches this DeviceID value for the duration of its connection to the device.

Hostname and DeviceID

The DeviceID is fixed at the time of the connection to the event gateway and does not change even when the device hostname is reconfigured.

When changing the hostname on the device, the only way to refresh the DeviceID is to break the connection between the device and the event gateway. Enter the **no cns event** global configuration command followed by the **cns event** global configuration command. You can change the DeviceID using the command **cns id event** without breaking the connection between the device and the event gateway.

When the connection is re-established, the device sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

Caution When using the Cisco Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the device acquires *after*—not *before*—you use the **cns config initial** global configuration command at the device. Otherwise, subsequent **cns event ip port** global configuration command operations malfunction.

Using Hostname, DeviceID, and ConfigID

In standalone mode, when a hostname value is set for a device, the configuration server uses the hostname as the DeviceID when an event is sent on hostname. If the hostname has not been set, the event is sent on the cn=<*value*> of the device.

In server mode, the hostname is not used. In this mode, the unique DeviceID attribute is always used for sending an event on the bus. If this attribute is not set, you cannot update the device.

These and other associated attributes (tag value pairs) are set when you run the Setup program on the Cisco Configuration Engine (see Chapter 2, "Running the Setup Program").

Understanding Cisco IOS Agents

The CNS event agent feature allows the device to publish and subscribe to events on the event bus and works with the Cisco IOS agent. The Cisco IOS agent feature supports the device by providing these features:

- Initial Configuration, page 3-5
- Incremental (Partial) Configuration, page 3-6
- Synchronized Configuration, page 3-6

Initial Configuration

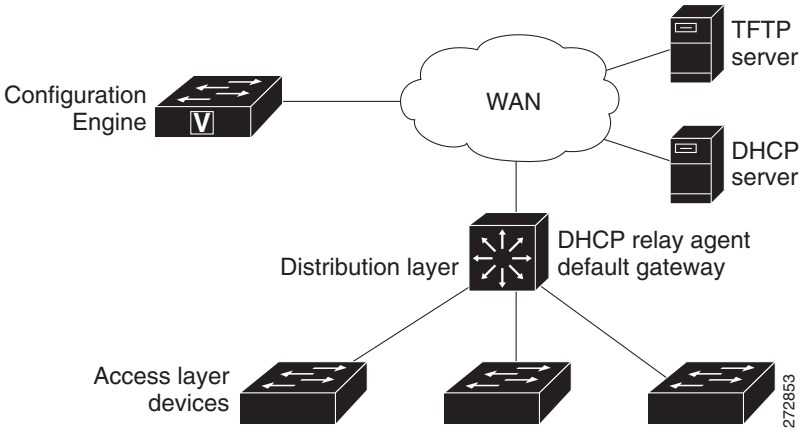
When the device first comes up, it attempts to get an IP address by broadcasting a DHCP request on the network. Assuming there is no DHCP server on the subnet, the distribution device acts as a DHCP relay agent and forwards the request to the DHCP server. Upon receiving the request, the DHCP server assigns an IP address to the new device and includes the TFTP server IP address, the path to the bootstrap configuration file, and the default gateway IP address in a unicast reply to the DHCP relay agent. The DHCP relay agent forwards the reply to the device.

The device automatically configures the assigned IP address on interface VLAN 1 (the default) and downloads the bootstrap configuration file from the TFTP server. Upon successful download of the bootstrap configuration file, the device loads the file in its running configuration.

The Cisco IOS agents initiate communication with the Cisco Configuration Engine by using the appropriate ConfigID and EventID. The Cisco Configuration Engine maps the Config ID to a template and downloads the full configuration file to the device.

Figure 3-2 shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

Figure 3-2 Initial Configuration Overview



Incremental (Partial) Configuration

After the network is running, new services can be added by using the Cisco IOS agent. Incremental (partial) configurations can be sent to the device. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the device to initiate a pull operation.

The device can check the syntax of the configuration before applying it. If the syntax is correct, the device applies the incremental configuration and publishes an event that signals success to the configuration server. If the device does not apply the incremental configuration, it publishes an event showing an error status. When the device has applied the incremental configuration, it can write it to NVRAM or wait until signaled to do so.

Synchronized Configuration

When the device receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the device not to save the updated configuration into its NVRAM. The device uses the updated configuration as its running configuration. This ensures that the device configuration is synchronized with other network activities before saving the configuration in NVRAM for use at the next reboot.

Configuring Cisco IOS Agents

The Cisco IOS agents embedded in the device Cisco IOS software allow the device to be connected and automatically configured. You could choose to change the configuration or install a custom configuration. Based on the device type (router or switch) and the Cisco IOS software supported on it, see the appropriate software configuration guide for instructions.

The following example provides a sample of the Cisco IOS commands on a Cisco 871 router.

Example of Cisco CNS commands on a Cisco 871 router

Note Substitute your CE hostname for myCE, your CE fdqn for myCE_domain, and the correct IP address for IP address 1.1.1.1.

- Example for plain text:

```
   ip host 1.1.1.1
   ip host myCE_domain 1.1.1.1
   cns trusted-server all-agents myCE
   cns trusted-server all-agents myCE_domain
   cns id mac-address
   cns id mac-address event

cns id mac-address image

   cns event myCE keepalive 60 3
   cns config partial myCE 80
   cns image server http://myCE:80/cns/HttpMsgDispatcher status
http://myCE:80/cns/HttpMsgDispatcher
cns exec
```

- Example for crypto SSL connections—assume that port 11012 is used:

```
ip host myCE 1.1.1.1
ip host myCE_domain 1.1.1.1
cns trusted-server all-agents myCE
cns trusted-server all-agents myCE_domain
```

```
cns id mac-address

    cns id mac-address event
    cns id mac-address image
    cns event myCE encrypt keepalive 60 3
    cns config partial myCE encrypt 443
    cns image server http://myCE:443/cns/HttpMsgDispatcher status
http://myCE:443/cns/HttpMsgDispatcher
cns exec encrypt 443
```

This section describes the usage guidelines for the CNS commands.

- **cns trusted-server**: The cns trusted-server command can be used to specify a trusted server for an individual CNS agent or for all the CNS agents. When you attempt to connect to a server not on the list, the system will display the message AUTHENTICATION FAILURE.
- **cns id**: Use this command to set the unique ID to the CNS configuration agent or configure the ID Cisco IOS device identifier used by the CNS services.
- **cns event**: Use this command to provide CNS event services to the Cisco IOS clients. This command allows to establish the connection between the device and the Cisco Configuration Engine. For example, when you turn off this command, the Agent Enable device on the GUI changes from green to red.
- **cns config partial**: Use this command to start the CNS partial configuration agent. For example, this command allows you to update the configuration feature on the Cisco Configuration Engine.
- **cns image**: Use this command to start the CNS image agent process and to listen image-related events on the CNS Event Bus.
- cns exec: The CNS exec agent allows a remote application to execute an EXEC mode command-line interface (CLI) command on a Cisco IOS device by sending an event message containing the command. For ex: this command is needed for Device Discovery and Query Device Inventory features on Config Engine.

CHAPTER 4

Setting Up a Multihomed System

By default, the installation of the Cisco Configuration Engine software offers a single-homed system setup. If you require a multihomed system setup, you must manually customize the network parameters of the Cisco Configuration Engine server. This chapter provides instructions for manually customizing these network parameters. It contains the following sections:

Setup Restrictions

Two network interfaces are installed in the Cisco Configuration Engine server: eth0 (Ethernet 0) and eth1 (Ethernet 1). Both interfaces can be configured and connected to networks. Cisco Configuration Engine setup has the following restrictions:

1. The hostname and domain name that are input at setup make up the identity for **eth0**.
2. There are no hostname and domain name assignments for eth1.
3. For both **eth0** and **eth1** interfaces, the default gateway must be configured on the same network as **eth0**.
4. Ethernet0 is used to connect to the management network. The customer premises equipment (CPE) resides in the management network.
5. There are no setup prompts that allow you to add additional routes into the routing table.
6. The Cisco Configuration Engine user interface does not allow you to manipulate the routing table.
7. The routing table changes are not automatically backed up and saved.

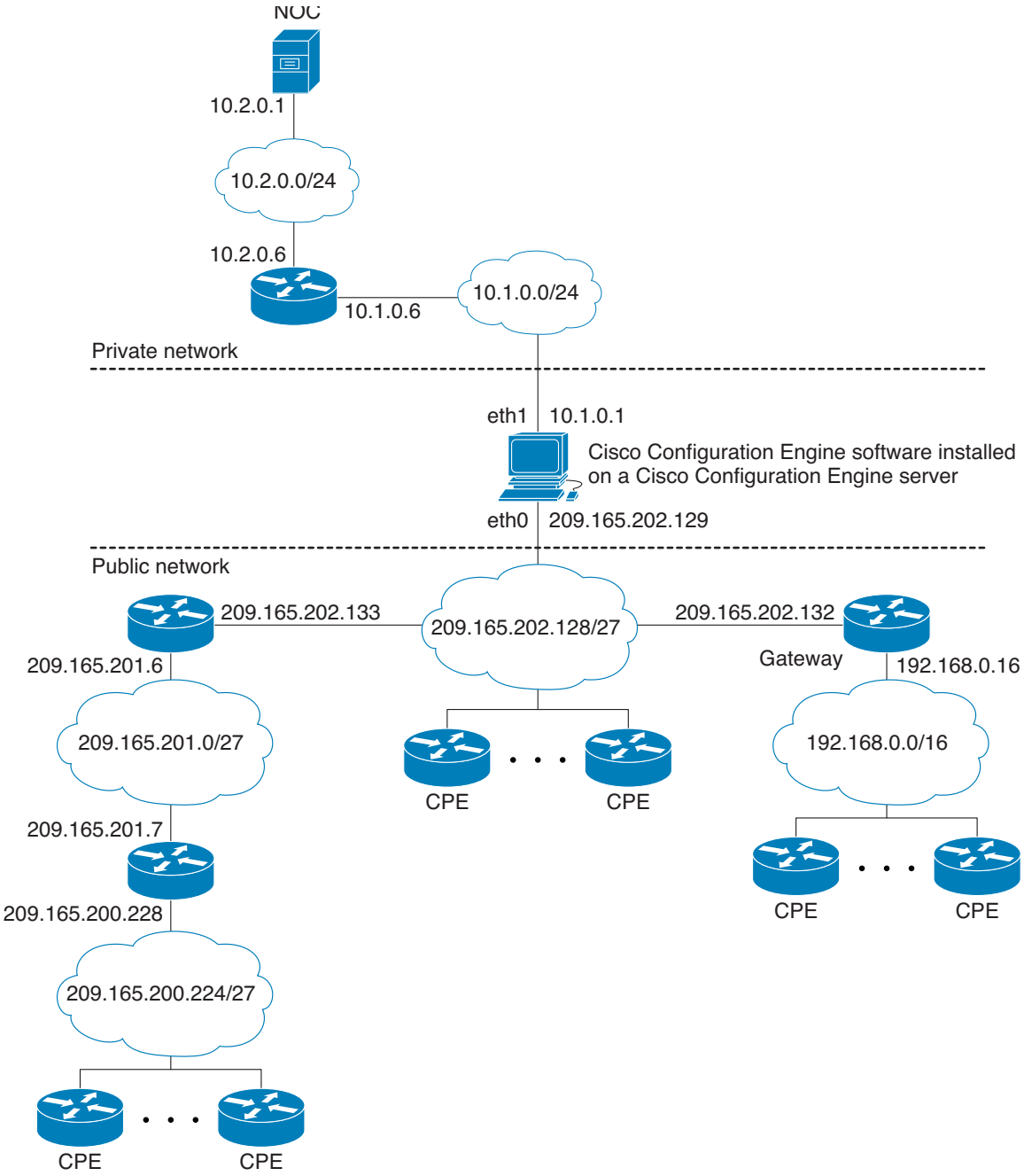
Typical Deployment of the Multihomed System

Figure 4-1 shows a typical deployment of Cisco Configuration Engine server with the Cisco Configuration Engine software in a two-network environment: private network and public network.

- Private Network—The private network contains the Network Operation Center (NOC), where the provisioning applications connect to the Cisco Configuration Engine through the CNS Event Bus.
- Public Network—The public network is the entry to the management network where CPE connects to the Cisco Configuration Engine through TCP connections.

This deployment provides security to network management because it physically isolates provisioning applications from external traffic.

Figure 4-1 Typical Deployment of a Multihomed System



See Figure 4-1 on page 4-3 and Setup Restrictions, page 4-1, and note the following:

- Ethernet0 is used for connecting to the CPE in the public (management) network (restriction 4) and eth1 is used for connecting to the provisioning applications in the private network.
- Gateway 209.165.202.132 is the default gateway because setup restricts the location of the default gateway (restriction 3). In effect, this restriction requires all routes going to the private network to be explicitly declared (or controlled) in the Cisco Configuration Engine server's routing table.

- The CNS Event Bus Network Parameter prompt in the Cisco Configuration Engine setup controls the location of the CNS Event Bus. By default, the CNS Event Bus is set to eth0, which means that the event bus is started on the public network. If you choose to start the event bus on the private network, you must set the CNS Event Bus Network Parameter to the eth1 IP address.
- By default, Cisco Configuration Engine setup automatically creates direct and default routes in the routing table. The network administrator must manually add the indirect routes to the routing table (restriction 5). For details, see Adding Indirect Routes to the Routing Table, page 4-6.

Note In the public network, the routes leading to networks 209.165.201.0/27, 192.168.0.0/16, and 209.165.200.224/27 could be defined either in the default gateway or in the Cisco Configuration Engine server. Defining the routes in the default gateway is preferable because it reduces management burden on the Cisco Configuration Engine server. In this chapter, however, we defined the routes in the Cisco Configuration Engine server to illustrate the routing table management tasks that you can perform on the server.

Understanding the Routing Table

The routing table in the Cisco Configuration Engine server plays a major role in maintaining the two network topologies. The Cisco Configuration Engine server is not a gateway for passing traffic between the public and private network, and it should be controlled and restrained from network access. Thus, the number of routes to be maintained in the routing table must be small. The current approach for maintaining the routing table is static routing.

Each route in the routing table describes a path from the network interface to the reachable network for directing outbound traffic. There are three types of routes required in the routing table: direct, indirect, and default.

Understanding Direct Routes

Direct routes specify the networks that are directly connected to the network interfaces. For example, the two directly connected networks in Figure 4-1 are networks 10.1.0.0/24 and 209.165.202.128/27. The two direct routes are:

- eth1 > 10.1.0.0/24
- eth0 > 209.165.202.128/27

Understanding Indirect Routes

Indirect routes describe the paths from the directly connected gateways to the indirectly connected networks. See Figure 4-1, and note the following information.

The indirectly connected networks in the public network are:

- 10.2.0.0/24
- 209.165.201.0/27
- 192.168.0.0/16
- 209.165.200.224/27

The indirect routes in the public network are:

- 209.165.202.133 > 209.165.201.0/27
- 209.165.202.132 > 192.168.0.0/16
- 209.165.202.133 > 209.165.200.224/27

Note A packet destined for network 209.165.200.224/27 is first forwarded to gateway 209.165.202.133, which sends it to gateway 209.165.201.7; therefore, the route 209.165.202.133 > 209.165.200.224/27 is required in the Cisco Configuration Engine server's routing table.

The indirect route in the private network is:

- 10.1.0.6 >10.2.0.0/24

Understanding Default Route

The default route specifies the default gateway for sending outgoing packets that have no matching routes. The default route in Figure 4-1 is 209.165.202.132 > 0.0.0.0/0.

Note Network 0.0.0.0/0 is a wildcard notation that matches any network address.

Manually Updating the Routing Table

By default, Cisco Configuration Engine setup automatically creates the direct and default routes in the routing table. The network administrator must manually add the indirect routes to the routing table. The following sections provide the steps for manually adding indirect routes and changing the default route:

- Indirect Routes, page 4-5
- Default Route, page 4-7
- Direct Routes, page 4-8

Note When modifying the routing table, we recommend that you log in through the serial port console connection.

Indirect Routes

Use variations of the **route** command to display, add, or delete routes from the routing table. The following sections provide more information:

- Displaying the Routing Table, page 4-6
- Adding Indirect Routes to the Routing Table, page 4-6
- Deleting a Route from the Routing Table, page 4-7
- Persistent Update—Indirect Routes, page 4-7

Displaying the Routing Table

Use the **route –n** command to display the routing table:

```
Router# route -n
```

Note The **–n** part of the command allows numerical addresses to be displayed instead of symbolic hostnames, thus avoiding DNS for hostname lookup. This prevents the command from hanging if the DNS is not ready or reachable.

Example of the Routing Table

```
Kernel IP routing table


Destination       Gateway           Genmask        Flags  Metric  Ref    Use Iface
209.165.202.128   0.0.0.0           255.0.0.0      U      0       0      0   eth0
10.1.0.0          0.0.0.0           255.255.255.0  U      0       0      0   eth1
172.16.0.0        0.0.0.0           255.0.0.0      U      0       0      0   lo
0.0.0.0           209.165.202.132   0.0.0.0        UG     0       0      0   eth0
```

Note The first two lines are direct routes (eth0 > 209.165.202.128 and eth1 > 10.1.0.0).

The last line is the default route (209.165.202.132 > 0.0.0.0). This default route was configured during Cisco Configuration Engine setup.

The third line is the route for using the loopback interface (lo > 172.16.0.0). This is the interface with a special IP address:172.16.0.1. This loopback interface is configured by default during setup.

Adding Indirect Routes to the Routing Table

Use the **route add** command to add indirect routes to the routing table. You must specify the network address, network mask, gateway address, and network interface identifier in the command:

```
route add -net 10.2.0.0        netmask 255.255.255.0 gw 10.1.0.6        dev eth1
route add -net 209.165.201.0   netmask 255.0.0.0     gw 209.165.202.133 dev eth0
route add -net 192.168.0.0     netmask 255.0.0.0     gw 209.165.202.132 dev eth0
route add -net 209.165.200.224 netmask 255.0.0.0     gw 209.165.202.133 dev eth0
```

Note In the example, the first line adds the indirect route for the private network: 10.1.0.6 > 10.2.0.0/24.

The next three lines add the indirect routes for the public network:

209.165.202.133 > 209.165.201.0/27

209.165.202.132 > 192.168.0.0/16

209.165.202.133 > 209.165.200.224/27

After you add the indirect routes, use the **route –n** command to display the updated routing table:

```
Router# route -n
```

Example of the Updated Routing Table

```
Kernel IP routing table

Destination   Gateway           Genmask      Flags Metric Ref    Use Iface
10.2.0.0        10.1.0.6          255.255.255.0   UG    0      0        0 eth1
10.1.0.0        0.0.0.0           255.255.255.0   U     0      0        0 eth1
192.168.0.0     209.165.202.132   255.0.0.0       UG    0      0        0 eth0
209.165.201.0   209.165.202.133   255.0.0.0       UG    0      0        0 eth0
127.0.0.0       0.0.0.0           255.0.0.0       U     0      0        0 lo
209.165.200.224 209.165.202.133   255.0.0.0       UG    0      0        0 eth0
209.165.202.128 0.0.0.0           255.0.0.0       U     0      0        0 eth0
0.0.0.0         209.165.202.132   0.0.0.0         UG    0      0        0 eth0
```

Deleting a Route from the Routing Table

Use the **route del** command to delete a route from the routing table. For example, to delete the route to network 209.165.200.224, enter the following command:

```
route del -net 209.165.200.224 netmask 255.0.0.0 gw 209.165.202.133 dev eth1
```

Persistent Update—Indirect Routes

Modifying the routing table with the route command provides only a temporary solution that is in effect until the machine reboots. For a persistent update, add the indirect routes into the file /etc/sysconfig/static-routes, in the following format:

```
any <type destination-address> netmask <netmask-address> gw <gateway-address> dev
<interface number>
```

Example

```
any net 10.2.0.0         netmask 255.255.255.0 gw 10.1.0.6        dev eth1
any net 209.165.201.0    netmask 255.0.0.0     gw 209.165.202.133 dev eth0
any net 192.168.0.0      netmask 255.0.0.0     gw 209.165.202.132 dev eth0
any net 209.165.200.224  netmask 255.0.0.0     gw 209.165.202.133 dev eth0
```

When the server reboots, the network startup script, /etc/rc.d/init.d/network, executes the following **route add** command for each line in the static routes table, beginning with the keyword **any** (as shown in the example above):

```
route add <type destination-address> netmask <netmask-address> gw <gateway-address> dev
<interface number>
```

Note If the routes are no longer required, you must physically remove them from the /etc/sysconfig/static-routes file.

Default Route

Use the **route** command to change the default route on the routing table. The following sections provide more information:

- Changing the Default Route, page 4-8
- Persistent Update—Default Routes, page 4-8

Changing the Default Route

To change the default route, you must first delete the existing default route and then add the new default route to the routing table. For example, to change the default route in Figure 4-1 so that it points to the default gateway 10.1.0.6 that is connected to eth0 on the public network, follow these steps:

Step 1 Delete the default route. To delete the default route 209.165.202.132, enter the following command:

```
route del default gw 209.165.202.132
```

Step 2 Add the default route. To add the default route 10.1.0.6, enter the following command:

```
route add default gw 10.1.0.6
```

Example of the Routing Table with the Default Gateway 10.1.0.6

```
Kernel IP routing table

Destination     Gateway          Genmask         Flags Metric Ref    Use Iface
10.2.0.0        10.1.0.6         255.255.255.0   UG    0      0        0 eth1
10.1.0.0        0.0.0.0          255.255.255.0   U     0      0        0 eth1
192.168.0.0     209.165.202.132  255.0.0.0       UG    0      0        0 eth0
209.165.201.0   209.165.202.133  255.0.0.0       UG    0      0        0 eth0
127.0.0.0       0.0.0.0          255.0.0.0       U     0      0        0 lo
209.165.200.224 209.165.202.133  255.0.0.0       UG    0      0        0 eth0
209.165.202.128 0.0.0.0          255.0.0.0       U     0      0        0 eth0
0.0.0.0         10.1.0.6         0.0.0.0         UG    0      0        0 eth1
```

Note The last line displays the new default route.

Persistent Update—Default Routes

The /etc/sysconfig/network file stores the following network parameters:

```
NETWORKING=yes
HOSTNAME=rain106.cisco.com
DOMAINNAME=cisco.com
GATEWAY=209.165.202.132
GATEWAYDEV=eth0
```

For a persistent default route update, you must substitute the GATEWAY parameter and the GATEWAYDEV parameter with the new desired values; for example, 10.1.0.6 and eth1.

Note The Setup program updates the file with the gateway parameters, but your manual changes are lost when you rerun the Setup program.

Direct Routes

Because the direct routes are already defined at setup, you do not need to manually define them.

Persistent Update—Direct Routes

The files ifcfg-eth0 and ifcfg-eth1 in the /etc/sysconfig/network-scripts directory store the network parameters for eth0 and eth1. These files are used to configure the network interface and to create direct routes after each reboot.

Reloading the Routing Table

You can reload the routing table in one of the following ways:

- Use the **route** command to update temporary changes, modify the associated file, and then reboot the machine for persistent changes.
- Enter the following command directly at the command line: **/etc/rc.d/init.d/network restart**. This updates the routing table with all persistent changes without rebooting your machine.

Information About the /etc/hosts File

The hostname and domain name that you added during the Cisco Configuration Engine Setup program defined the identity of the system and of eth0. This information is stored in the /etc/hosts file. If a name is required for eth1, you can add it to the /etc/hosts file. However, the setup script removes eth0 and eth1 entries from the /etc/hosts file at setup and regenerates the eth0 entry only. Therefore, you must re-add the eth1 entry after each setup. Other entries are not affected.

CHAPTER 5

Setting Up a Multizone System

The installation of the Cisco Configuration Engine software does not offer the multizone system setup by default. If you require a multizone system setup, you must enable the multizone feature during the system setup. To setup multiple IP addresses on the Cisco Configuration Engine server, you must manually customize the network parameters of the server to have multiple IP addresses. You can configure multiple IP addresses by using IP aliasing on a network interface card or by using multiple network interface cards where each card should have an IP address. This chapter provides a brief overview of the Cisco Configuration Engine multizone setup. It contains the following sections:

Setup Restrictions

Two network interfaces are installed in the Cisco Configuration Engine server: **eth0** (Ethernet 0) and **eth1** (Ethernet 1). Both interfaces can be configured and connected to networks. The Cisco Configuration Engine setup has the following restrictions:

1. For both the **eth0** and **eth1** interfaces, the default gateway must be configured on the same network as **eth0**.
2. The primary IP address and hostname should be assinged to **eth0**.
3. The prompt CNS Event Bus Network parameter in the setup of CNS Configuration Engine controls the location of the CNS Event Bus. It should be set as **eth0** hostname.
4. Ethernet 0 is used to connect to the management network. The CPE resides in the management network.

Typical Deployment of the Multizone System

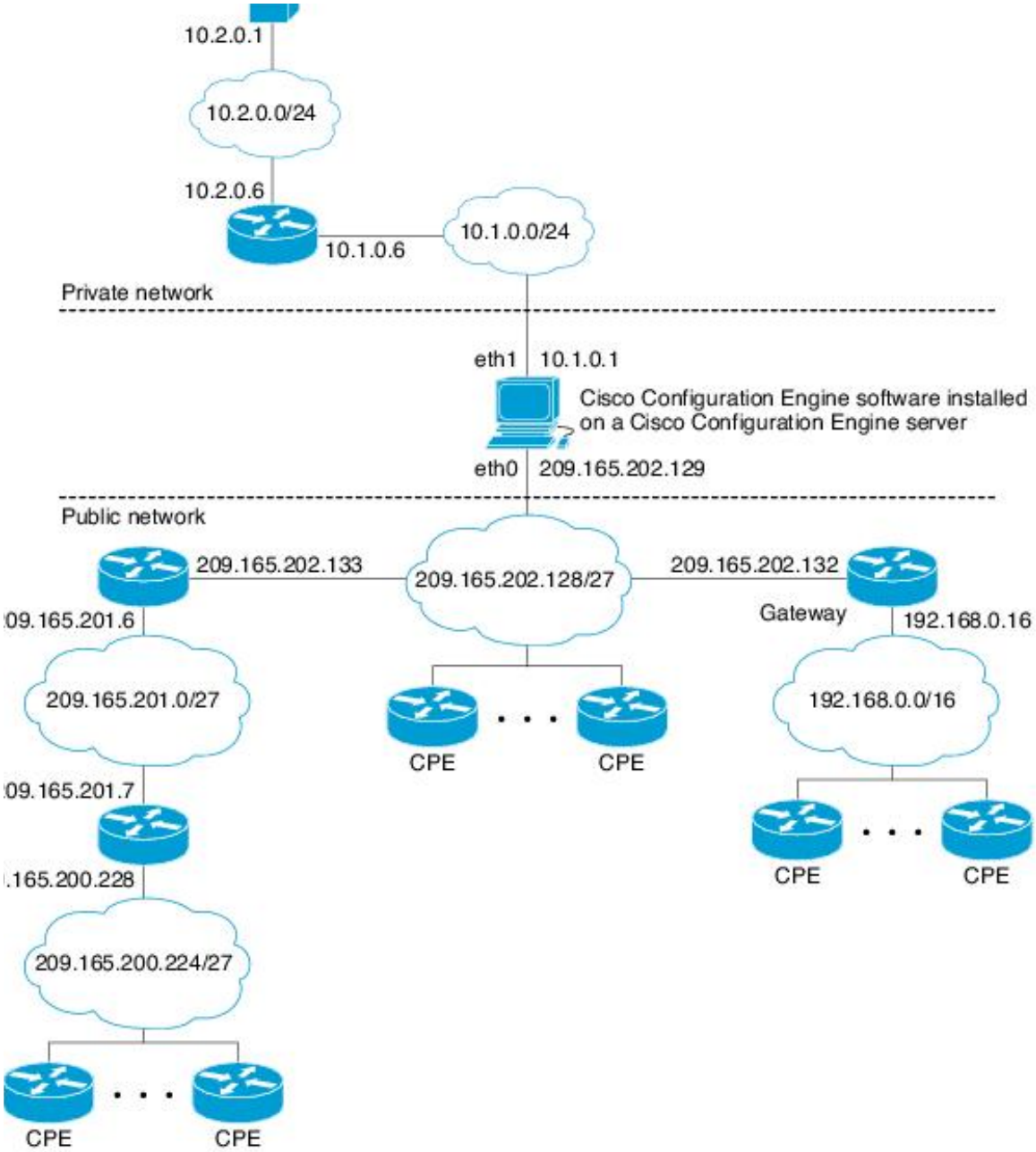
To deploy the Cisco Configuration Engine in a distributed architecture in different security zones, follow these steps:

- Zone 1: Deploy the Cisco Configuration Engine processes which communicate with the network elements through the public network.
- Zone 2: Deploy the Cisco Configuration Engine administrative interfaces, APIs, and the back-end services.
- Zone 3: Deploy the LDAP and the Network File System with the template files.

To deploy one instance of the Cisco Configuration Engine in a distributed architecture, the Cisco Configuration Engine should be in a Demilitarized Zone (DMZ). Figure 5-1 shows a typical deployment of Cisco Configuration Engine server with the Cisco Configuration Engine software in a multi-network environment: private network and public network.

- Private Network—The private network contains the Network Operations Center (NOC), where the provisioning applications connect to the Cisco Configuration Engine through the CNS Event Bus.
- Public Network—The public network is the entry to the management network where CPE connects to the Cisco Configuration Engine through TCP connections.

Figure 5-1 Multizone System



- In Figure 5-1, the public network represents **Zone 1**, private network represents **Zone 3** and the Cisco Configuration Engine resides in **Zone 2** of the DMZ.
- In Cisco Configuration Engine 3.5.3, the server can be configured to block all the administrative requests from the public network. This is done automatically during the setup. The setup program checks if multiple IP addresses are assigned to the Cisco Configuration Engine server. If so, it prompts the user to enable the multi-zone feature.

```
Your box has multiple IP Addresses assigned: 17x.xx.xxx.xx 17x.xx.xxx.xxx You can create
http zones so that http traffic can be limited on the IP Address 17x.xx.xxx.xx. Only
selected URLs can be accessed using IP Address 17x.xx.xxx.xx.
    Do you want to create zones to have limited access to CE from public
    network (y/n)?  [n] y
    Do you want to allow plain-text http access to CE from public network
    (y/n)?  [y] y
```

CHAPTER 6

Scalability Among Event Gateway Ports

Cisco Configuration Engine server can support up to 30,000 devices on Solaris and 20,000 devices on Linux server with the recommended hardware specification. Devices connect and communicate to Cisco Configuration Engine through Event Gateway.

Each Event Gateway process running on Cisco Configuration Engine listens to a server port. For better performance, we recommend that you distribute the devices evenly among Event Gateway ports. This chapter provides information about Event Gateway and Event Gateway port automatic assignment functions.

This chapter contains the following sections:

Understanding Cisco Event Gateway

Cisco Event Gateway enables network elements to publish and subscribe to events, which allows developers to write event-driven applications to communicate with Cisco network elements. The Event Gateway also acts as an interface to the Event Bus, enabling event-based communication. Each Event Gateway port can support up to a maximum of 500 devices. To support more than 500 devices, you must run multiple event gateway processes. You can configure a maximum of 60 event gateways on the Solaris platform and a maximum of 40 event gateways on the Linux platform.

Note Performance is not affected if you enter the maximum number of event gateways.

During the Cisco Configuration Engine setup, you can configure the number of concurrent gateway processes to start with either one or both of the following prompts, depending on how you set up the SSL (see Encryption Settings, page 2-7) communications:

```
Enter number of Event Gateways that will be started with crypto operation:X
Enter number of Event Gateways that will be started with plaintext operation:Y
```

Note The ports for Event Gateways with crypto operation are even numbers that start from 11014. The ports for Event Gateways with plaintext operation are odd numbers that start from 11013.

There will be X + 1 crypto event gateways started on the server in the above example, where X is the number you entered during setup. The additional one event gateway is reserved to perform port automatic assignment for devices which communicate to Cisco Configuration Engine through SSL. This additional event gateway is called as dispatcher event gateway. Similarly, Y + 1 plain-text event gateways will be started on the server in the above example for plain-text operation.

Note The Crypto dispatcher event gateway always listens to port 11012. The plain-text dispatcher event gateway always listens to port 11011. The port 11012 and 11011 are called the Cisco Configuration Engine well-known ports.

The dispatcher event gateway automatically reassigns an event gateway port to a network device as soon as the connection request is sent to port 11012 or 11011.

During Cisco Configuration Engine setup, you can enable the port automatic distribution feature if you choose to zero touch deploy your devices or if you already have the devices currently configured to use the Cisco Configuration Engine known ports. If you choose to enable the port automatic allocation during the setup, then you need to enter the correct **cns event** command in the later part of the Cisco Configuration Engine setup.

```
Enable Event Gateways port automatic allocation (y/n)? [y]
```

However, user also have the choice to turn off this feature. When the feature is turned off, the Dispatcher Event Gateways listening on port 11011 and 1102 are not started.

During the Cisco Configuration Engine setup, you can also configure the Cisco Configuration Engine to be the primary Cisco Configuration Engine or a backup Cisco Configuration Engine in a dual Cisco Configuration Engine deployment architecture. In this deployment architecture, network administrator configures a backup Cisco Configuration Engine. Upon the event gateway connection failure, the network element automatically fails over to the configured backup Cisco Configuration Engine. However, there is no load sharing of event gateway connections between the primary and backup Cisco Configuration Engine.

Note This is different from the Cisco's validated high availability deployment architecture, where multiple Cisco Configuration Engines, external LDAP and a load balancer are utilized in that architecture. There is load sharing of event gateway connections among all the participating Cisco Configuration Engines in that architecture.

```
Is this a primary CE (y/n)?
Enter CNS Event command:
```

The CNS event command configures how the network element should connect to this particular Cisco Configuration Engine. The command entered in the above line should match with what is configured on the network element without the event gateway port number. For example, if **cns event ce-host 11011 source Vlan1 keepalive 120 2 reconnect 10** is configured on the device, then the command **cns event <ce-host> source Vlan1 keepalive 120 2 reconnect 10** should be entered, where **<ce-host>** is the IP address or hostname of the Cisco Configuration Engine server. Another example is if this is a backup

Cisco Configuration Engine and the command **cns event ce-host 11011 source Vlan1 backup** is configured on the device, then the command **cns event ce-host source Vlan1 backup** should be entered in the above line.

Note When you enter the **cns event** command during the Cisco Configuration Engine setup, no port number should be given and the connect interface or the VLAN should be specified.

These commands are required for the network elements to establish connections with Cisco Configuration Engine server. The network devices cannot connect to Cisco Configuration Engine if you do not enter a correct command. The steps described above will enable the port auto-assignment feature. You can also change the configuration options on Cisco Configuration Engine to control how the port auto-assignment should work. These control options are stored in the *resource.properties* file located in *$CISCO_CE_HOME/conf* directory. The sample file and what each parameter means is demonstrated as below:

```
CNS_EVENT_CLI=cns event ce-host keepalive 120 2 reconnect 10
```

This line is configured during Cisco Configuration Engine setup when prompted *Enter CNS event* command. It is highly recommended to configured keepalive and reconnect as this is the only way for Cisco Configuration Engine server to detect whether a network element is still actively connected.

```
BACKUP_CE_ENABLED=0
```

This line is configured during Cisco Configuration Engine setup when prompted *Is this a primary Cisco Configuration Engine BACKUP_CE_ENABLED=0* means this is a primary *Cisco Configuration Engine, BACKUP_CE_ENABLED=1* means this is a backup Cisco Configuration Engine.

```
PERSIST_IN_NVRAM=1
```

PERSIST_IN_NVRAM=0 menas the config command specified in *CNS_EVENT_CLI* will be saved only in running config; PERSIST_IN_NVRAM=1 means the config command specified in CNS_EVENT_CLI will be saved in NVRAM. It is highly recommended to save the port information in the startup config. This is the default setting.

```
LoadBalance_Algorithm=0
```

LoadBalance_Algorithm=0 means the round robin algorithm is enabled and this is enabled by default; *LoadBalance_Algorithm=1* means the least connection algorithm is enabled.

Note The load sharing is between event gateways on the same Cisco Configuration Engine. A Cisco Configuration Engine level High Availability (HA) architecture is also available. If an event gateway is down, Cisco Configuration Engine automatically restarts it.

```
WAIT_AFTER_CONFIG=1
```

Time to wait for device to subscribe to the config load event in second. For slow network, this wait time might need to be increased. For example: 1.2, 1.5, 2, and so on.

```
DISPLAY_WIDTH=25
```

Display number of devices per line in port debugging page *http://ce-host/cns/ResourceInit?name=port*. After an event gateway configuration parameter is changed in *resource.properties*, Cisco Configuration Engine server need to be restarted by using the command **$CISCO_CE_HOME/bin/setup -r**.

When Cisco Configuration Engine is used to manage devices belong to different VLANs, only devices from one VLAN (configured during Cisco Configuration Engine setup) can use the event gateway port automatic allocation feature. After the devices in one VLAN are deployed, the deployment engineer can reconfigure the Cisco Configuration Engine and start to deploy the devices in the next VLAN.

Event Gateway Port Automatic Assignment

Each event gateway can support up to a maximum of 500 devices. During Zero Touch Deployment, this means the deployment engineer needs to update the bootstrap configuration file for every 500 devices. The event gateway port automatic assignment freed the deployment engineer from this manual process. When the Cisco Configuration Engine server is configured as the previous section, all the 30,000 devices can be deployed using the same bootstrap configuration file. The following is the sample bootstrap configuration file. The bolded lines are the required commands to support the port automatic assignment.

```
cns trusted-server all-agents ce-host
cns id hardware-serial
cns id hardware-serial event
cns config initial ce-host status http://ce-host/cns/PostStatus
cns event ce-host keepalive 120 1 reconnect 10
cns config partial ce-host
```

When a network element connects to Cisco Configuration Engine through dispatcher event gateway, Cisco Configuration Engine automatically assigns a port to the network element. The network element will save that information and connect to the designated Cisco Configuration Engine port. The Cisco Configuration Engine can manage a device after the device connects to a none Cisco Configuration Engine well-known port (ports other than 11011 and 11012).

Note The deployment engineer can also choose not to use the port automatic assignment feature. In this case, **cns event ce-host <port number>** command should be used in the bootstrap configuration file and the port number should be updated for every 500 devices.

Event Gateway Resource Monitor

The Cisco Configuration Engine has a resource health monitoring utility which periodically monitors the status of event gateways and Tibco event bus. If any of the monitored process is dead, resource monitor restarts that process automatically, and logs a message in */var/log/CNSCE/resource_monitor/resource_monitor.log*.

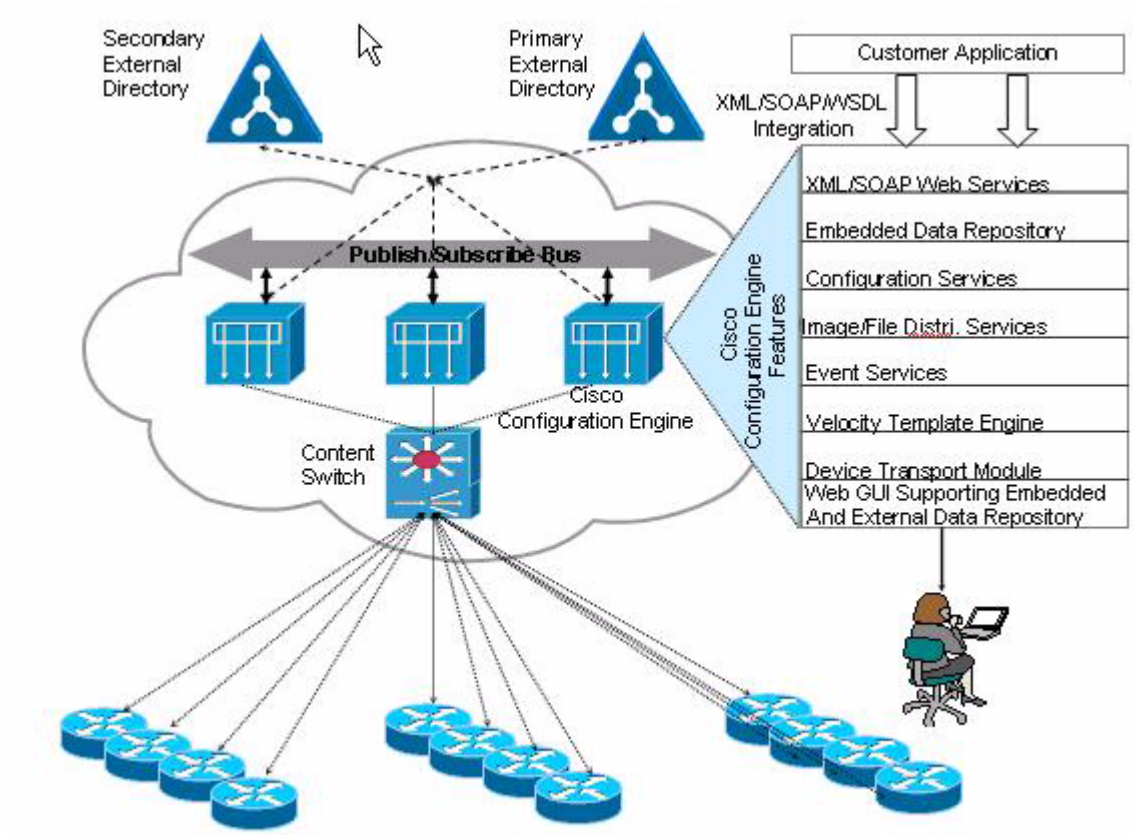
The health monitor is installed during Cisco Configuration Engine setup.

- To check the status of the resource monitor, use **/etc/init.d/ResourceMonitor status** command.
- To start the resource monitor, use **/etc/init.d/ResourceMonitor start** command.
- To stop the resource monitor, use **/etc/init.d/ResourceMonitor stop** command.

Event Gateway Scalability in Cisco Validated High Availability Architecture

The Cisco Configuration Engine can be deployed in the following Cisco validated HA architecture where multiple Cisco Configuration Engines, shared external LDAP server and an ACE load balancer is utilized. If a customer deploys this architecture, then the port automatic assignment feature shouldn't be used as the port auto-assignment overwrites the load sharing (among all the participating Cisco Configuration Engines) capability offered by the load balancer

Figure 6-1 High Availability Architecture.



To disable the port auto-assignment, simply do not use the port 11011 or 11012 for plain-text or crypto on network element during event agent configuration. For plain text, all devices can use the port 11013. For crypto, all devices can use the port 11014. The load balancer manages all the connections to event gateways on all the participating Cisco Configuration Engine servers.

Event Gateway Troubleshooting

Q. I setup my Cisco Configuration Engine correctly, but the device is shown as RED or could not be auto-discovered. Why my device is not connecting to Cisco Configuration Engine?

A. Make sure **cns trusted-server all-agents ce-host** and c**ns config partial ce-host** commands are configured on the device. Where **ce-hos**t is the IP address or the hostname of the Cisco Configuration Engine.

Q. I setup my Cisco Configuration Engine correctly and I could also see the new port is assigned to the device by using the *$CISCO_CE_HOME/tools/cns-listen* cisco.> debugging tool. But I could not see the device and it is in RED. The device shows up in the device discovery GUI. Seems that the connect event is never received by Cisco Configuration Engine.

A. Make sure **cns trusted-server all-agents ce-host** and **cns config partial ce-host** commands are configured on the device. Where **ce-host** is the ip address or the hostname of Cisco Configuration Engine. If this is a slow network, increase the *WAIT_AFTER_CONFIG* timer in *CISCO_CE_HOME/conf / resource.properties* and try the operation again. Increasing the wait timer will impact the overall performance. So make sure to find a shortest wait time that works in your network environment. The default wait time is one second.

Q. Can I configure my device to point to the same Cisco Configuration Engine but different ports as the primary and backup Cisco Configuration Engine?

A. No. A given Cisco Configuration Engine can only either be the primary or the backup Cisco Configuration Engine, but cannot be both.

Q. After I used the port auto-assignment, I could not get the status of my config initial?

A. Command **cns config initial ce-host** reports the config initial status through Event Gateway (by default). If you are using port auto-assignment function, you should post the status through HTTP. For example, *cns config initial ce-host* status *http://ce-host/cns/PostStatus* should be configured on the device.

Q. When I push a configuration job to a device, another device got the same config?

A. The device Id needs to be unique within Cisco Configuration Engine's namespace. Make sure the two devices do not have the same config Id, event Id, and image Id.

CHAPTER 7

Cisco CNS Configuration Engine SSL Security

This chapter discusses the setup and configuration of 128-Bit Secure Sockets Layer (SSL) Encrypted Communications between CNS Agent Enabled Cisco IOS Devices and the Cisco CNS Configuration Engine.

This chapter contains the following sections:

CNS Agent and Configuration Engine Security

Security in communication between the Cisco Configuration Engine server and the enabled CNS agent devices (routers) involves three basic functions:

- Identification—Unique CNS agent ID. At a minimum, the CNS agent IDs are required for a device to communicate with the Cisco Configuration Engine server.
- Authentication—Unique CNS password. The Authentication feature consists of a CNS password that the CNS agents present to the Cisco Configuration Engine server as part of any communication handshake.
- Encryption—128-Bit SSL / Shared PKI SSL Trust point Certificates. Secure Sockets Layer (SSL) protocol. The Encryption feature consists of the industry standard Secure Sockets Layer (SSL) protocol, which protects communications between the CNS agent devices and the Cisco Configuration Engine server.

While device identification is mandatory, authorization and encryption are optional features. Of the two optional features, you can enable either or both of them at any time. Encryption does not require authentication, and authentication does not require encryption.

Each security feature is configured and handled separately by both the Cisco Configuration Engine server and the CNS agent devices.

CNS ID, Password Authorization, SSL Encryption

The CNS Configuration Engine has settings for CPE Device Identification, Authorization, and Encryption. Each of these features is configured and handled separately by both the CNS Configuration Engine and the CNS CPE Devices communicating with the CNS Configuration Engine.

The CPE Device CNS Agent IDs are required for a CNS Agent enabled CPE device to communicate with the CNS Configuration Engine server. The Authorization feature consists of a CNS Password that the CNS Agent enabled devices present to the CNS Server. If you choose Encryption, CNS Agent to CNS Configuration Engine communication negotiations takes place as the first of the communication sequence. Only when the SSL Encryption is successful, the CNS Identification and CNS Authentication protocols are passed. When you enable all the options on the CNS Configuration Engine Server, the options should be successfully passed by the CNS Agent CPE Devices or the device is not allowed to connect to the server for any purpose and will be rejected.

The following sections provide more information:

- Identification, page 7-2
- Authentication, page 7-3
- Encryption, page 7-4

Identification

This is a mandatory setting. Each CNS Enabled CPE device (router) must have a unique ID assigned to it before it can start communication with the CNS Configuration Engine. You can configure several CNS agents on a single router. Each agent must have a unique ID assigned to it.

To configure CNS agent IDs on a CNS agent device, enter the following command, beginning in global configuration mode:

cns id string <*unique string*>

cns id string <*unique string for event agent*> **event**

cns id string <*unique string for image agent*> **image**

Example

```
Router#enable
Router#configure terminal
Router(config)#cns id string my-asset-tag1
Router(config)#cns id string my-asset-tag1 event
Router(config)#cns id string my-asset-tag1 image
Router(config)#end
```

On the Cisco Configuration Engine server, when setting up a new device object through the user interface, the administrator must specify these CNS agent IDs. The Cisco Configuration Engine server will not accept any agent connection unless the CNS agent device and the IDs are already configured on the server.

Authentication

The Authentication feature consists of a CNS password that the CNS agent device presents to the Cisco Configuration Engine server as part of any communication handshake. The CNS password is used in two ways:

- It is assigned at the CNS Configuration Engine Server as a global one-time-use password which is known to the CNS Configuration Engine administrator.
- This one-time-use password is then also placed in the CNS Agent Enabled device's configuration by the device administrator before the device attempts to connect to the CNS Configuration Engine Server.

On the CNS Configuration Engine web User Interface, the radio button under the Devices menu labeled Resync Device allows the administrator to reset any CPE Devices unique password as a global one-time-use password. Then, before the CNS agent device attempts to connect to the Cisco Configuration Engine server, the administrator must enter this one-time-use password in the CNS agent device configuration. If a device is out of sync with the server, it can be reset and the server will re-assign a new random value upon successful connection.

The following prompt in the CNS Configuration Engine Setup program sets the server to expect CNS Passwords from the CPE Devices:

```
Authentication settings:
------------------------
Cisco IOS Devices are normally authenticated before being allowed to connect to the Event
Gateway/Config Server. Disabling authentication will increase security risk.
Enable authentication (y/n)? [n] y
```

During setup of the Cisco Configuration Engine server, the administrator must assign this CNS password as a global one-time-use password. Then, before the CNS agent device attempts to connect to the Cisco Configuration Engine server, the administrator must enter this one-time-use password in the CNS agent device configuration.

In the Cisco Configuration Engine server Setup program, authentication is enabled when you answer y at the "Enable authentication" prompt (see Authentication Settings, page 2-8). This configures the Cisco Configuration Engine server to expect the password from the CNS agent device. After authentication is enabled, the administrator must use the Cisco Configuration Engine user interface to reconfigure the actual password. You can set the password by using the CNS Configuration Engine web UI under the menu **Tools** > **Security Mgr** > **BootStrap**.

This password can be used for the initial CPE Device connections to the CNS Configuration Engine Server. After each CPE device has been identified and authenticated, the CNS Configuration Engine server generates the password and automatically assigns a random password for the CPE device.

Note The random cns password command has been intentionally hidden for additional security. You can use the cns password command to set or reset the initial password, but you cannot view the password value after it has been set.

To configure the CNS password on the CPE device, enter the following command, beginning in global configuration mode:

cns password <password>

Example

```
Router(config)# cns password fgfg123
Router(config)# end
```

Encryption

The CNS communications between CNS Agent-enabled devices and the CNS Configuration Engine can be encrypted with 128-Bit SSL Protocol strong encryption. This brings all the benefits of the industry standard Secure Sockets Layer Encryption Protocol to the communications between CNS Agent enabled devices and the CNS Configuration Engine.

The CNS Configuration Engine Setup program prompts related to the SSL Encryption features are Shown below

```
...other prompts....
Encryption settings:
--------------------
Enable cryptographic (crypto) operation between Event Gateway(s)/Config
server and device(s) (y/n)? [n] y
Certificates already exist. Overwrite (y/n)? y
Enter certificate FTP server (hostname.domainname or IP address): cert-host.mydomain.com
Enter username used for FTP server: cnsie
Enter FTP password: ******
Re-enter FTP password: ******
Enter absolute pathname of remote key file: /tftpboot/server.key
Enter absolute pathname of remote certificate file: /tftpboot/server.cer
Enabling plaintext operation will increase security risk.
Enable plaintext operation between Config Server and devices/GUI
administration (y/n)? [y] n
Enable plaintext operation between Event Gateway and devices (y/n)? [y] n
Enter port number for https web access: [443]
...other prompts....
```

SSL Host Communication Basics

To take part in SSL based communications, the hosts system should have the following:

- A common PKI Certificate Server (CS) / Certificate Authority (CA) that is trusted to sign and issue Digital Certificates to use with SSL (Trustpoint).
- Hostname
- DNS Server IP Address (Name Resolution)
- DNS Domain Name(Name Resolution)
- Date and Time zone Settings
- NTP Date and Time Updates
- SSL Trust Point Signed SSL Certificates.

Every host that takes part in SSL Communications needs to have an accurate date and time, along with some fundamental Host Name Resolution capabilities. They should have a strong encryption based Operating Systems to enable 128-Bit SSL Export Grade Encrypted communications.

Four Steps to CNS SSL Communication

Using the CNS Agent and CNS Configuration Engine, you can establish a trusted and encrypted communication channel between Cisco IOS devices and the CNS Configuration Engine by using the CNS Agent SSL Encryption feature. You can encrypt the transmission of all IOS Syslog Messages including Firewall and IDS Sensor traffic, Configuration Updates, Statistics Gathering, and Device Inventory over a single 128-Bit SSL Connection.

There are four basic steps to set up the SSL Communications between the CNS Agents and CNS Configuration Engine:

Step 1 Obtain the Server Self-Signed (root) Certificate. In the first part of the deployment the Certificate Authority (CA) must be setup and you should have a Self-Signed Certificate.

Step 2 CNS Configuration Engine SSL Enrollment.

The CNS Configuration Engine needs to enroll and acquire its own unique SSL Certificate from the Cisco IOS CA Server. The CPE device checks the CNS Configuration Engine's SSL Certificate and the Root CA Signature against its own SSL Certificate in order to setup the SSL Connectivity. This enrollment is done over a File Copy or Terminal/Console cut and paste method.

Note In versions 1.3.2 and 1.4 of the CNS Configuration Engine there is no SCEP protocol enrollment client.

Step 3 Set the Cisco IOS Trustpoint.

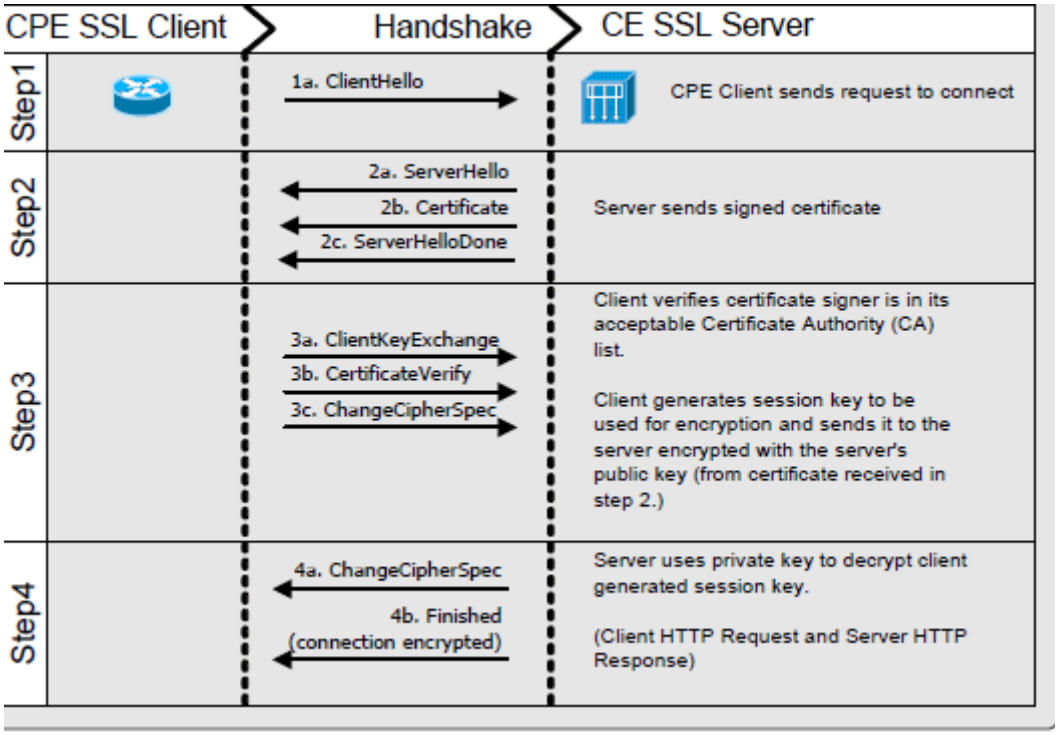
Cisco CNS Agent CPE Devices only need a copy of the Root CA's Certificate self-signed certificate. This is simply known as *Setting the Cisco IOS Trustpoint* as they are not required to enroll for their own individual certificate. You can use the same Root CA's Self-Signed certificate for CNS Configuration Engine Server Certificate validation. This is similar to how PC web browsers work today.

Cisco CPE Devices are designed to primarily utilize the Cisco SCEP Enrollment Protocol to set the SSL Trustpoints or enroll a CPE Device for its own Certificate. The use of the SSL Protocol in Cisco Devices was introduced into Cisco IOS in 1999-2000 and the SCEP Protocol for Certificate Enrollment and related functions was developed in a joint venture by Cisco Systems Inc. and Verisign Inc.

Step 4 Turn on the SSL.

On the CNS Configuration Engine re-run the Setup program to enable Encryption on the Server end. The CNS Agents in the CPE device(s) need to reconfigure the command to use the encrypt keyword.

Figure 7-1 CNS 128-Bit SSL Client & Server HandShake



Running SSL Encrypted Communication

After setting up the encryption on the server end, the Cisco IOS Device and the CNS Configuration Engine are prepared to begin the SSL Encrypted Communications. Any CNS Agent inbound service connection which attempts to initiate the connection with the keyword *encrypt* in its IOS command will be encrypted over SSL.

Cisco IOS v12.3(4)T Certificate Server

Before you configure the CNS Configuration Engine or an SSL Cisco IOS Device getting any certificates or setting the device SSL trustpoints, you should setup the SSL Certificate Server (Trustpoint).

The Cisco IOS Certificate Server supports Simple Certificate Enrollment Protocol (SCEP) over HTTP as its primary Certificate enrollment protocol.

Today, Cisco IOS SSL Client Devices use the SCEP as their primary Certificate Server enrollment protocol to set their SSL Cisco IOS Trustpoints. The CNS Configuration Engine uses a manual enrollment (terminal write) to enroll and obtain its SSL Certificate from the Certificate Server as it does not support the SCEP protocol or other automated enrollment protocols.

Engine Cert Enrollment IOS Command

For the CNS Configuration Engine Certificate Request, the following syntax on the Cisco IOS CS is required to have it accept the certificate request from a Terminal or Screen dump:

crypto pki server {cs-label} request pkcs10 terminal pem

Cisco IOS Cert Enrollment IOS Command

For the Cisco IOS CPE Device Certificate request by means of SCEP, use the following command:

crypto pki server {cs-label} request pkcs10 url {url}

The URL is the path that the Cisco IOS CPE Device uses to set its Trustpoint by means of SCEP.

Setting up the Cisco IOS Certificate Server

These are short version of IOS CS setup and configuration that you need to substitute with your own server name and issuer-name values. Further documentation covering the setup of the IOS Certificate Server in detail is available at Cisco.com.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip http server
Router(config)#crypto pki server IOS-CA-10090
Router(cs-server)#issuer-name CN=My Company,L=San Francisco CA,C=us
Router(cs-server)#grant auto
% This will cause all certificate requests to be automatically granted.

Are you sure you want to do this? [yes/no]: yes
Router(cs-server)#no shutdown
% Once you start the server, you can no longer change some of % the configuration.
Are you sure you want to do this? [yes/no]: yes
% Generating 1024 bit RSA keys ...[OK]

Mar 13 02:15:37.029: %SSH-5-ENABLED: SSH 1.99 has been enabled
% Certificate Server enabled.
Router(cs-server)#end
```

Viewing the IOS Certificate Server Self-Signed (root) Certificate

To view the Certificate Authorities own (self-signed) SSL Certificate on your IOS Certificate Server, use the command below. This is the Certificate that will be digitally signed and authenticate all of the SSL Certificates issued by this Certificate Authority.

Show Crypto CA Certificate

The following example shows how the **crypto ca certificate** command is used at the router prompt.

```
Router#show crypto ca certificates
CA Certificate
    Status: Available
    Certificate Serial Number: 01
    Certificate Usage: Signature
    Issuer:
        cn=My Company
        l=San Francisco CA
        c=us
    Subject:
        cn=My Company
        l=San Francisco CA
        c=us
    Validity Date:
        start date: 02:15:39 UTC Mar 13 2004
        end date: 02:15:39 UTC Mar 13 2007
    Associated Trustpoints: IOS-CA-10090
```

Show Crypto PKI Server

The following example shows how the **crypto pki server** command is used at the router prompt.

```
Router#show crypto pki server
Certificate Server IOS-CA-10090:
    Status: enabled, configured
    CA cert fingerprint: 7F1AEE23 9067BD38 97137AE7 24C80C37
    Granting mode is: auto
    Last certificate issued serial number: 0x1
    CA certificate expiration timer: 02:15:39 UTC Mar 13 2007
    CRL NextUpdate timer: 02:15:49 UTC Mar 20 2004
    Current storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

IOS Certificate Server Enrollment

This section describes the IOS certificate server enrollment procedure.

Certificate Enrollment using SCEP Protocol

SCEP is the recommended method of Certificate Enrollment for all Cisco IOS Devices. An example of IOS client configuration for SCEP enrollment is shown below:

```
crypto ca identity SSLrootCA
enrollment url http://myIOSCAserver.com
exit
```

Certificate Enrollment using Terminal Copy and Paste

The command line enrollment requires access to the IOS command. The certificate request and reply both will be issued on the console session screen and not saved to any file. The issued results can simply be copied to file as text and saved for use in the CNS Configuration Engine. To obtain a certificate, use the following command:

```
Router#crypto pki server iosca request pkcs10 terminal
<<paste request>>
<<copy certificate>>
```

Sample Terminal Enrollment

The following example shows how to use a certificate request for a CNS Configuration Engine:

Note Your certificate request can have PEM headers and footers.


```
Cisco-1711#crypto pki server IOS-CA-10090 request pkcs10 terminal
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE
REQUEST----MIIDQDCCAigCAQAwgawxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEbMBkGA1UEChMSQ2lzY28gU3lzdGVtcyBJbmMu
MSYwJAYDVQQLEx1OTVRHIENOUyBDb25maWd1cmF0aW9uIEVuZ2luZTENMAsGA1UE
AxMEb3B1czEhMB8GCSqGSIb3DQEJARYSZW1pa3VsaWNAY2lzY28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA84y2NE0C1GY5nnubkG6u2ZYAxK7h
Qy+9UPSfeVYHE3EWuQNuZljoXOd40+/FTfeOEdhh9fsertl+wNavHXwpngDfhx59
dbRduYekAmL7kPVute1BtVB6yJJ7yWRoGW3pG5PinMPXwNQhSRZHgBVBusWtdsD/
/clo7Mly4F2vqYmSVaE0SHLR1QiJKO+0iOx9iBzGxH8S2BpfdjwBKwO2MzRFgPhV
PgjtMvNDA47DgwfcuSiO6liW1Cv/g3GgzBT/G6sWzf6ah2+kTLQq9XXim5b9J2Hf
IIniAwohSq+kHo8f/cbq+WT/BwLaU163oZXiNKUxeYBYCuzZ7GGMkRHVwQIDAQAB
oE4wGAYJKoZIhvcNAQkHMQsTCWNyaW1zb241NTAyBgkqhkiG9w0BCQIxJRMjTmV0
d29yayBNYW5hZ2VtZW50IFRlY2hub2xvZ3kgR3JvdXAwDQYJKoZIhvcNAQEEBQAD
ggEBABtrhmhJYP3iD5iencZzQr4P8bwDjtYAS4B0EpFAfeymGV5ZSKMM3pLEbac8
iVL2EbLwB1G25O24PiFOmysw60+ehmR4TR1yI3pMZ7oTn71md4a3z04GAw6o9q4u
xPEWx07LckkGdmaZAd5t9+hLrBWTq+gZmZszVkenhBPIEdDh8gN0XKM5xd9IVtio
jZNJVeXPlVxWFT/nIz+BaVolJenuqrB6wgWjMoAfvknr2v9axIf8P6j80vPSX3wU
H+JUNCYTa4hXoX8sK9xeoHpqNyvVMz6ntAgHe+JjJyfRlLxq/hnbcem83lyr2Mix
% Granted certificate:
MIIDBzCCAnCgAwIBAgIBAjANBgkqhkiG9w0BAQQFADA9MQswCQYDVQQGEwJ1czEZ
MBcGA1UEBxMQU2FuIEZyYW5jaXNjbyBDQTETMBEGA1UEAxMKTXkgQ29tcGFueTAe
Fw0wNDAzMTMwMjIzNDRaFw0wNTAzMTMwMjIzNDRaMIGsMQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNVBAoT
EkNpc2NvIFN5c3RlbXMgSW5jLjEmMCQGA1UECxMdTk1URyBDTlMgQ29uZmlndXJh
dGlvbiBFbmdpbmUxDTALBgNVBAMTBG9wdXMxITAfBgkqhkiG9w0BCQEWEmVtaWt1
bGljQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPOM
tjRNAtRmOZ57m5BurtmWAMSu4UMvvVD0n3lWBxNxFrkDbmZY6FzneNPvxU33jhHY
YfX7Hq7ZfsDWrx18KZ4A34cefXW0XbmHpAJi+5D1brXtQbVQesiSe8lkaBlt6RuT
4pzD18DUIUkWR4AVQbrFrXbA//3JaOzJcuBdr6mJklWhNEhy0dUIiSjvtIjsfYgc
xsR/EtgaX3Y8ASsDtjM0RYD4VT4I7TLzQwOOw4MH3LkojupYltQr/4NxoMwU/xur
Fs3+modvpEy0KvV14puW/Sdh3yCJ4gMKIUqvpB6PH/3G6vlk/wcC2lNet6GV4jSl
MXmAWArs2exhjJER1cECAwEAAaMjMCEwHwYDVR0jBBgwFoAUUmc3z2kTZuJ3JJAW
BQGz2gYFGuQwDQYJKoZIhvcNAQEEBQADgYEAHOsmp3H2wii8NaoYV8uXsbIYyk5V
KDIpB3EX6G74b6MG0egzH+39HYJT7S7uevyPEbMg1xusJoeRmUGl0GricJcmlPUL
cqqSt+nueOpiZs0W1pwqunqYTkTy3DP1oyxSWA1Xe9sIJQXcPvppj+7KvpIvckCk
RqgVxWG1aPcBTYI=
```


Note if a PEM formated certificate is expected manually add the following PEM headers:

```
-----BEGIN CERTIFICATE-----
<<hex data>>
-----END CERTIFICATE-----

Hence the issued request would end up with headers above and below it's first and last
data lines:
-----BEGIN CERTIFICATE----MIIDBzCCAnCgAwIBAgIBAjANBgkqhkiG9w0BAQQFADA9MQswCQYDVQQGEwJ1czEZ
MBcGA1UEBxMQU2FuIEZyYW5jaXNjbyBDQTETMBEGA1UEAxMKTXkgQ29tcGFueTAe
Fw0wNDAzMTMwMjIzNDRaFw0wNTAzMTMwMjIzNDRaMIGsMQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNVBAoT
EkNpc2NvIFN5c3RlbXMgSW5jLjEmMCQGA1UECxMdTk1URyBDTlMgQ29uZmlndXJh
dGlvbiBFbmdpbmUxDTALBgNVBAMTBG9wdXMxITAfBgkqhkiG9w0BCQEWEmVtaWt1
bGljQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPOM
tjRNAtRmOZ57m5BurtmWAMSu4UMvvVD0n3lWBxNxFrkDbmZY6FzneNPvxU33jhHY
YfX7Hq7ZfsDWrx18KZ4A34cefXW0XbmHpAJi+5D1brXtQbVQesiSe8lkaBlt6RuT
4pzD18DUIUkWR4AVQbrFrXbA//3JaOzJcuBdr6mJklWhNEhy0dUIiSjvtIjsfYgc
xsR/EtgaX3Y8ASsDtjM0RYD4VT4I7TLzQwOOw4MH3LkojupYltQr/4NxoMwU/xur
Fs3+modvpEy0KvV14puW/Sdh3yCJ4gMKIUqvpB6PH/3G6vlk/wcC2lNet6GV4jSl
MXmAWArs2exhjJER1cECAwEAAaMjMCEwHwYDVR0jBBgwFoAUUmc3z2kTZuJ3JJAW
BQGz2gYFGuQwDQYJKoZIhvcNAQEEBQADgYEAHOsmp3H2wii8NaoYV8uXsbIYyk5V
KDIpB3EX6G74b6MG0egzH+39HYJT7S7uevyPEbMg1xusJoeRmUGl0GricJcmlPUL
cqqSt+nueOpiZs0W1pwqunqYTkTy3DP1oyxSWA1Xe9sIJQXcPvppj+7KvpIvckCk
RqgVxWG1aPcBTYI=
-----END CERTIFICATE----
```

Sample Commands and Output

The section provides the sample commands and the output.

Crypto Key and SSL Certificate Request Creation

The following steps will describe you the basics of RSA Key generation and SSL Certificate Request Generation on the CNS CE. The generated certificate is referred to as the *Certificate Signing Request* and is used to apply for a valid signed SSL Certificate from your Certificate Authority in return.

Logon to the Console or Terminal of your CNS Configuration Engine and enter the commands in the order they are presented here.

Note You have to substitute the sample filenames with your own actual filenames as required. The output listed here is actual OpenSSL output created in a test environment and your actual output data can vary slightly. In the following text, both the command input and any output generated is listed as captured on the screen. Make sure that the CNS Configuration Engine is installed and setup with the network TCP/IP connectivity.

Generating RSA Keys

Log into CNS Configuration Engine Console or Terminal, enter the following commands in order to generate an RSA Keypair and a Certificate Signing Request:

- **% openssl genrsa -out /root/server.key 1024**

```
Generating RSA private key, 1024 bit long modulus
................++++++
.....................................................++++++
e is 65537 (0x10001)
```

Changing the File Ownership rights of the RSA keys

To change the files ownership rights of the RSA keys, use the following command.

- **% chown -v root:root /root/server.key**

```
changed ownership of `/root/server.key' to root:root
```

- % chmod -v 400 /root/server.key

```
mode of `/root/server.key' changed to 0400 (r--------)
```

Generating an SSL Certificate Signing Request

To generate an SSL Certificate Signing request, use the following command.

- **% openssl req -new -key /root/server.key -out /root/server.csr**

```
Using configuration from /usr/share/ssl/openssl.cnfer.key -out /root/server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Cisco Systems Inc.
Organizational Unit Name (eg, section) []:Network Management Technology Group
Common Name (eg, your name or your server's hostname) []:opus
Email Address []:administrator@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:.
```

After you complete the above steps, create a v2.0 Privacy Enhanced Mail (PEM) formatted SSL Certificate Signing Request on the local CNS Configuration Engine file system. The SSL Certificate should be signed by your Certificate Server/Authority. The *server.csr* file can now be transferred to the certificate authority for signing.

The following example shows the unformatted file.

"-----BEGIN CERTIFICATE REQUEST-----" and "-----END

CERTIFICATE REQUEST-----" header and footer text on a line each by themselves.


```
[root@opus root]# more /root/server.csr
-----BEGIN CERTIFICATE
REQUEST----MIICETCCAXoCAQAwgbcxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEbMBkGA1UEChMSQ2lzY28gU3lzdGVtcyBJbmMu
MSwwKgYDVQQLEyNOZXR3b3JrIE1hbmFnZW1lbnQgVGVjaG5vbG9neSBHcm91cDEN
MAsGA1UEAxMEb3B1czEmMCQGCSqGSIb3DQEJARYXYWRtaW5pc3RyYXRvckBjaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALSbTB5cijXDFzGmGxDK
z5FpR1I8PfzJI/2lEfOUzKwffzbUmKESLOTTQ3g1Y7Qbh7lZBU1rVsc4I1pwHyKu
JOGNhG8wJCUau3ErmhExEM/OunD6zXU1VT/CSvMzG2e6l5JHEBIuZyL/LWEiaA+0
+7NiqI/xgsYPAUVdheEOqgkdAgMBAAGgGTAXBgkqhkiG9w0BCQcxChMIY2lzY28x
MjMwDQYJKoZIhvcNAQEEBQADgYEAQfwCg/fceFdy/xgpps6GSkRt8EB6gsMwNv2E
Cp+FQR0CK9NcpNwNezevbhqpNoaVhsmXgfbAw8mVxJWLJeLe1Bhf9GBXPwIttqLJ
IyfNZfagXMkW+S9z53MnPXg49RaT07itYkqe/1h6RV4TeHYjhPkHGuFeb9GsKM4X
B35lEeo=
-----END CERTIFICATE REQUEST----
```

Certificate Request Digitally Signed and Issued

Copy the SSL Certificate Request *server.csr* file to your Certificate Server and submit it for signing by the CS/CA. The CS/CA Administrator will verify the CNS Configuration Engine Certificate Request with the CS/CA's Root Certificate according to their policy and return the signed/valid SSL Certificate to you as a '*server.cer*' file in a Privacy Enhanced Mail (PEM) format. After you receive the certificate, copy or place the signed Certificate in you preferred directory location on the CNS Configuration Engine or on an external FTP Server that has IP FTP Client connectivity access.

Viewing the CNS Configuration Engine Certificate Contents

To view the CNS Configuration Engine Certificate contents, run the following command on the CNS Configuration Engine console (as root). In the output, you should look at the serial: number:

```
[root@nugi root]# openssl x509 -noout -text -in /etc/tibgate/server.crt
......other data.......
X509v3 Authority Key Identifier:
keyid:28:B6:86:CF:E5:52:C9:8C:23:BA:C2:A2:A0:22:F1:DA:5E:77:53:30
DirName:/Email=administrator@mycompany.com/C=US/ST=CA/L=San Jose/O=Company Co
Inc./OU=Dept/CN=Personnel
serial:4D:00:F1:83:1F:8D:56:AC:4F:63:BF:0A:CA:AB:4F:00
.....other data.......
```

Preview the Issued SSL Certificate

After you copy the CNS Configuration Engine Certificate onto the CNS Configuration Engine, to preview the signed contents of the CNS Configuration Engine Certificate, use the following OpenSSL command on the Certificate server.cer file.

root@opus root]# openssl x509 -noout -text -in /root/server.cer

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=us, L=San Francisco CA, CN=My Company
        Validity
            Not Before: Mar 13 02:23:44 2004 GMT
            Not After : Mar 13 02:23:44 2005 GMT
        Subject: C=US, ST=California, L=San Jose, O=My Company., OU=Personnel Dept,
    CN=myhostname/Email=administrator@company.com
    co.com
        Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:f3:8c:b6:34:4d:02:d4:66:39:9e:7b:9b:90:6e:
                ae:d9:96:00:c4:ae:e1:43:2f:bd:50:f4:9f:79:56:
                07:13:71:16:b9:03:6e:66:58:e8:5c:e7:78:d3:ef:
                c5:4d:f7:8e:11:d8:61:f5:fb:1e:ae:d9:7e:c0:d6:
                af:1d:7c:29:9e:00:df:87:1e:7d:75:b4:5d:b9:87:
                a4:02:62:fb:90:f5:6e:b5:ed:41:b5:50:7a:c8:92:
                7b:c9:64:68:19:6d:e9:1b:93:e2:9c:c3:d7:c0:d4:
                21:49:16:47:80:15:41:ba:c5:ad:76:c0:ff:fd:c9:
                68:ec:c9:72:e0:5d:af:a9:89:92:55:a1:34:48:72:
                1:d5:08:89:28:ef:b4:88:ec:7d:88:1c:c6:c4:7f:
                12:d8:1a:5f:76:3c:01:2b:03:b6:33:34:45:80:f8:
                55:3e:08:ed:32:f3:43:03:8e:c3:83:07:dc:b9:28:
                8e:ea:58:96:d4:2b:ff:83:71:a0:cc:14:ff:1b:ab:
            16:cd:fe:9a:87:6f:a4:4c:b4:2a:f5:75:e2:9b:96:
```

```
            fd:27:61:df:20:89:e2:03:0a:21:4a:af:a4:1e:8f:
            1f:fd:c6:ea:f9:64:ff:07:02:da:53:5e:b7:a1:95:
            e2:34:a5:31:79:80:58:0a:ec:d9:ec:61:8c:91:11:
            d5:c1
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
        keyid:52:67:37:CF:69:13:66:E2:77:24:90:16:05:01:B3:DA:06:05:1A:E4
Signature Algorithm: md5WithRSAEncryption
    1c:eb:26:a7:71:f6:c2:28:bc:35:aa:18:57:cb:97:b1:b2:18:
    ca:4e:55:28:32:29:07:71:17:e8:6e:f8:6f:a3:06:d1:e8:33:
    1f:ed:fd:1d:82:53:ed:2e:ee:7a:fc:8f:11:b3:20:d7:1b:ac:
    26:87:91:99:41:a5:d0:6a:e2:70:97:26:94:f5:0b:72:aa:92:
    b7:e9:ee:78:ea:62:66:cd:16:d6:9c:2a:ba:7a:98:4e:44:f2:
    dc:33:f5:a3:2c:52:58:0d:57:7b:db:08:25:05:dc:3e:fa:69:
    8f:ee:ca:be:92:2f:72:40:a4:46:a8:15:c5:61:b5:68:f7:01:
    4d:82
[root@opus root]#
```

CNS Configuration Engine Certificate Request

This is an example of keys and a certificate request on a test CNS Configuration Engine. You can create a certificate request on your CNS Configuration Engine (*.csr) and the CA signs the certificate and sends you back a valid certificate (*.cer).

```
[root@opus root]# openssl req -new -key /root/server.key -out /root/my-cnsce.csr
Using configuration from /usr/share/ssl/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:us
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Francisco
Organization Name (eg, company) [My Company Ltd]:Company Co Inc.
Organizational Unit Name (eg, section) []:Department
Common Name (eg, your name or your server's hostname) []:my-cnsce
Email Address []:administrator@company.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:2FCE2F9EF109E
An optional company name []:Company Co Inc.
[root@nugi root]#
```

Enabling SSL in the Configuration Engine

Log into the CNS Configuration Engine Console or Terminal as root, run the CNS Configuration Engine Setup program a nd entering the command Setup. This allows you to make changes to the CNS Configuration Engine Setup encryption settings, and only apply those changes you have made. In this case you will be enabling SSL on that host and identifying the key and certificate locations.

Sample CNS Configuration Engine Setup for SSL

The following example shows the screen from my SSL enabled CNS Configuration Engine Setup:

```
======CNS Configuration Engine SETUP======================

Please review the following parameters:
username for user-level shell account: admin
password for user-level shell account:
eth0 IP address: 10.1.2.8
eth0 network mask: 255.255.255.0
eth0 default gateway IP address: 10.1.2.7 eth1 IP address:
primary DNS server IP address: 10.1.2.3
secondary DNS server IP address (optional):
Configuration Engine login name: gui-admin
Configuration Engine login password: ******
internal LDAP server password: *********
Enable cryptographic (crypto) operation between Event Gateway(s)/Config server and
device(s) (y/n)? yes
Certificates already exist. Overwrite (y/n)? no
Enable plaintext operation between Config Server and devices/GUI administration (y/n)? no
Enable plaintext operation between Event Gateway and devices (y/n)? no
Enable authentication (y/n)? no
NSM directive (none, default, http): default
Enable Event Gateway debug log (y/n)?no
log file rotation timer (minutes, 0 = no rotation): 15
max log file size (Kbytes): 3072
the max versions of log file (0-99): 1
number of Event Gateways that will be started with crypto operation: 1
number of Event Gateways that will be started with plaintext operation: 1
CNS Event Bus Network Parameter: 10.1.25.18
CNS Event Bus Service Parameter: 7500
Re-configure IMGW (y/n)? no

 Warning: setup cannot be aborted while committing changes.

Commit changes (y/n):yes
```

Cisco IOS SSL

This section describes how to set the Cisco IOS SSL.

Setting the Cisco IOS SSL Trustpoint

In Cisco IOS you can set the trustpoint over a network by using the SCEP, or you can screen dump it by using the 'terminal' option. To paste it over a terminal, it needs to be in a specific format (encoded). It should be in Base-64 encoded format for the terminal entry method.

CPE SSL Trustpoint Using SCEP

The following example shows how to obtain the Trustpoint by using the SCEP Protocol method.

```
!
Router(config)#crypto ca trustpoint company.com
Router(config)#enrollment mode ra
Router(config)#enrollment url http://my-iosca:80/
Router(config)#usage ssl-client
Router(config)#revocation-check none
Router(config)#crypto ca authenticate att.com
```

```
Certificate has the following attributes:
Fingerprint: 1D74D54A 464207FD 817901A4D 67B5112B
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
!
crypto ca certificate chain company.com
certificate ca 4D69F1831F8D56AF4F63BF0F1B6B4F9B
308202F2 3082029C A0030201 0202104D 69F1821F 8D56AC4F 63BF0ACA AB4F9F30
0D06092A 864886F7 0D010105 05003081 97312139 1F06092A 864886F7 0D010901
1612656D 696B756C 69634063 6973636E 2E636F6D 310B3009 06035504 06130255
53310B30 09060355 04081302 43413111 300F0603 55040713 084D696C 70697461
73311B30 19060355 040A1312 43697365 6F205379 7374656D 7320496E 632E3113
30110603 55040B13 0A434E53 2D494E77 4D425531 13301106 03550403 130A494E
534D4255 2D434131 301E170D 30333035 32383232 34333533 5F970D30 35303532
38323235 3231325A 30819731 21301F06 092A8648 86F70D01 09011612 656D696B
756C6963 40636973 636F2E63 6F6D310B 30090603 55040613 02123331 0B300906
03550408 13024411 3111300F 06035504 0713084D 696C7069 74617331 1B301906
0355040A 13124369 73636F20 53797374 656D7320 496E632E 31133011 06035504
0B130A43 4E532D49 4E534D42 55311330 11060355 0403130A 494E534D 42552D43
4131305C 300D0609 2A864886 F70D0101 01050003 4B003048 02410097 2E2CED5E
B0F1194F 572E3275 F54F8C92 1A489BD4 CAD7701B 2275EA6B 3520DC29 7D17A1C4
AC6EB48C B03B1AF1 8CDAB68A A31FB15A 55325A45 032106E6 8214B902 03010001
A381C130 81BE300B 0603551D 0F040403 0201C630 0F060355 1D130101 FF040530
030101FF 301D0603 551D0E04 16041428 B686CFE5 52C98C23 BAC2A2A0 22F1DA5E
77533030 6D060355 1D1F0466 3064302F A02DA02B 86296874 74703A2F 2F67696C
6C696761 6E2F4365 7274456E 726F6C6C 2F494E53 4D42552D 4341312E 63726C30
31A02FA0 2D862B66 696C653A 2F2F5C5C 67696C6C 6967616E 5C436572 74456E72
6F6C6C5C 494E534D 42552D43 41312E63 726C3010 06092B06 01040182 37150104
03020100 300D0609 2A864886 F70D0101 05050003 41012C82 FA96ED42 329B01B7
83A48A06 4CEDFE36 2CF9706D 1ED1B7C8 882B0B4C 039A4E15 14B410FC 4258FFED
C8069002 76446090 CA22B642 B4207869 F495F8F2 BA51
quit
```

CPE SSL Trustpoint Using Terminal Copy/Paste

The following example shows how to set the trustpoint over the console by using a terminal session.

```
!
Router(config)#crypto ca trustpoint company.com
Router(config)#enrollment mode ra
Router(config)#enrollment terminal
Router(config)#usage ssl-client
Router(config)#revocation-check none
Router(config)#
!
Router(config)#crypto ca authenticate company.com
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE----MIIC8jCCApygAwIBAgIQTWnxgx+
NVqxPY78KyqtPnzANBgkqhkiG9w0BAQUFADCB
lzEhMB8GCSqGSIb3DQEJARYSZW1pa3VsaWNAY2lzY28uY29tMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCE1pbHBpdGFzMRswGQYDVQQKExJDaXNj
byBTeXN0ZW1zIEluYy4xEzARBgNVBAsTCkNOUy1JTlNNQlUxEzARBgNVBAMTCklO
U01CVS1DQTEwHhcNMDMwNTI4MjI0MzUzWhcNMDUwNTI4MjI1MjEyWjCBlzEhMB8G
CSqGSIb3DQEJARYSZW1pa3VsaWNAY2lzY28uY29tMQswCQYDVQQGEwJVUzELMAkG
A1UECBMCQ0ExETAPBgNVBAcTCE1pbHBpdGFzMRswGQYDVQQKExJDaXNjbyBTeXN0
ZW1zIEluYy4xEzARBgXMAAsTCkNOUy1JTlNNQlUxEzARBgNVBAMTCklOU01CVS1D
QTEwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAly4s7V6w8RlPVy4ydfVPjJIaSJvU
ytdwGyJ16ms1INwpfRehxKxutIywOxrxjNq2iqMfsVpVMlpFAyEG5oIUuQIDAQAB
o4HBMIG+MAsGA1UdDwQEAwIBxjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQo
tobP5VLJjCO6wqKgIvHaXndTMDBtBgNVHR8EZjBkMC+gLaArhilodHRwOi8vZ2ls
bGlnYW4vQ2VydEVucm9sbC9JTlNNQlUtQ0ExLmNybDAxoC+gLYYrZmlsZTovL1xc
```

```
Z2lsbGlnYW5cQ2VydEVucm9sbFxJTlNNQlUtQ0ExLmNybDAQBgkrBgEEAYI3FQEE
AwIBADANBgkqhkiG9w0BAQUFAANBACyC+pbtQjKbAbeDpIoGTO3+Niz5cG0e0bfI
iCsLTAOaThUUtBD8Qlj/7cgGkAJ2RGCQyiK2QrQgeGn0lfjyukE=
-----END CERTIFICATE----quit
Certificate has the following attributes:
Fingerprint: 1D74D54A B64207FD 81831A4D 1EDF56194
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Show Crypto CA Trustpoint IOS Command

The following example shows how to get the following output, and the key field in this example is the Serial Number.

```
Router#show crypto ca trustpoints
Trustpoint company-IOS-CA:
Subject Name: mytrustpoint
CN = Department
OU = Personnel
O = Company Co Inc.
L = San Francisco
ST = CA
C = US
EA = administrator@company.com
Serial Number: 4D69F1831F8Ef1344F63BF0ACAAB4F9F
Certificate configured.
CEP URL: <http://my-iosca>
```

OpenSSL Certificate Formats

This section describes the OpenSSL Certificate formats.

Certificate and Key Formats

The certificate and key formats are:

- PEM
- DER
- PKCS#12

PEM

This is the default format used by OpenSSL and the only format usable by CNS Configuration Engine v1.4 and earlier. This format can contain all the private keys (RSA and DSA), public keys (RSA and DSA) and (x509) certificates. PEM stores the data in Base64 encoded DER format, surrounded by ascii headers, so this format is suitable for text mode transfers between systems.

DER

DER format can contain all the private keys, public keys and certificates. DER stores according to the ASN1 DER format. It is the default format for most browsers.

PKCS#12

PKCS#12 is also known as PFX files. They can contain all the private keys, public keys and certificates.It stores the data in a binary format.

For more information see http://www.drh-consultancy.demon.co.uk/pkcs12faq.html/.

The format of a X509 PEM certificate is:

(Header Info)

```
------BEGIN (TRUSTED|X509) CERTIFICATE----(
Certificate Data)
------END (TRUSTED|X509) CERTIFICATE---
```

Converting Certificate Formats with OpenSSL

This section describes the procedure to convert the certificate formats with the OpenSSL tools. For more information refer the OpenSSL documentation.

OpenSSL To PKCS#12

The following example shows how to convert OpenSSL to PKCS#12.

```
openssl pkcs12 -export -in pem-certificate-and-key-file -out
pkcs-12-certificate-and-key-file
openssl pkcs12 -export -in pem-certificate-file -inkey pem-key-file -out
pkcs-12-certificate-and-key-file
```

OpenSSL From PKCS#12 to PEM

The following example shows how to convert OpenSSL from PKCS#12 to PEM.

```
openssl pkcs12 -in pkcs-12-certificate-file -out pem-certificate-file
openssl pkcs12 -in pkcs-12-certificate-and-key-file -out pem-certificate-and-key-file
```

OpenSSL From PEM/DER to DER/PEM

The following example shows how to convert OpenSSL from PEM/DER to DER/PEMPKCS#12.

```
openssl dsa -inform PEM|DER -outform DER|PEM -in pem-file|der-file -out der-file|pem-file
```

OpenSSL Certificate Formats

The following example shows the OpenSSL certificate formats.

```
OpenSSL From PEM/DER to DER/PEM - RSA Keys
openssl rsa -inform PEM|DER -outform DER|PEM -in pem-file|der-file -out der-file|pem-file
```

Troubleshooting CNS SSL Communications

To view the issued CNS Config Engine certificate contents n the CNS Configuration Engine, run the following OpenSSL command. This sample is taken from a real certificate issued by a IOS CS/CA in our lab. The key value to note here is the “Serial Number:” hex string, which denotes the serial number of the issued certificate.

Viewing the SSL Certificate

The following example shows how to view the SSL certificate.

```
openssl x509 -noout -text -in /etc/tibgate/server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            15:79:ce:3e:00:00:ef:00:00:04
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: Email=administrator@mycompany.com, C=US, ST=CA, L=San Francisco, O=Company
Co Inc., OU=Department, CN=Personnel
        Validity
            Not Before: May 30 01:52:27 2003 GMT
            Not After : May 30 02:02:27 2004 GMT
        Subject: Email=administrator@mycompany.com, C=us, ST=California, L=San Jose,
O=Company Inc., OU=Department, CN=config-engine
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:c8:5a:71:55:f8:30:21:da:ef:f1:6f:5c:e5:df:
                92:66:be:d2:7f:86:65:e7:e1:de:f4:c2:ac:1e:e1:
                e9:7a:a2:64:20:81:ed:a6:ff:f8:85:ab:fc:63:0f:
                d3:71:93:b1:6b:31:f5:0b:11:64:c1:dc:29:88:7f:
                ab:81:69:bf:f0:81:5c:af:1b:86:9d:14:30:47:fd:
                44:04:ea:3e:e6:e0:2b:7d:33:d4:37:ba:a9:ba:ee:
                29:2f:52:a9:f3:e2:26:60:5d:c7:6d:25:92:80:fe:
                16:07:f8:c9:2d:75:6f:29:4c:17:3c:85:70:ad:c1:
                65:aa:ea:c5:e0:09:47:24:e1
        Exponent: 65537 (0x10001)
    X509v3 extensions:
    X509v3 Subject Key Identifier:
        35:7E:67:7C:B9:AC:79:ED:34:CB:08:DF:AB:1E:C6:0D:FC:41:3B:71
    X509v3 Authority Key Identifier:
        keyid:28:B6:86:CF:E5:52:C9:8C:23:BA:C2:A2:A0:22:F1:DA:5E:77:53:30
        DirName:/Email=administrator@mycompany.com/C=US/ST=CA/L=San Jose/O=Company
Co Inc./OU=Department/CN=Marketing
        serial:4D:69:F1:1F:EF:8E:56:AC:4F:63:BF:0A:CA:AB:4F:9F
    X509v3 CRL Distribution Points:
        URI:http://my-iosca/
        URI:file://\\my-iosca
    Authority Information Access:
        CA Issuers - URI:http://my-iosca
        CA Issuers - URI:file://\\my-iosca
Signature Algorithm: sha1WithRSAEncryption
    24:d7:86:57:95:78:08:60:8d:88:ab:6b:46:76:bc:45:ce:59:
    6c:af:29:43:17:22:a1:78:d0:65:8a:11:79:ef:6b:15:84:8b:
    bf:40:de:9a:08:81:8c:da:ea:e1:0c:fb:bb:0c:8d:96:74:31:
    30:a0:12:de:19:ca:1b:24:60:0d
```

Debug Dump of SSL Transactions

To view the **debug** output of the SSL Transactions, use the following commands. The SSL Dump program is part of OpenSSL toolkit and can help in the process of SSL trustpoint setting and sharing.

```
/opt/CSCOcnsie/tools/ssldump -A -e -N -d -i eth0 port 443
..or more simply..
/opt/CSCOcnsie/tools/ssldump -i eth0 port 443
/opt/CSCOcnsie/tools/ssldump -i eth0 port 11012
..and the operator can easily pipe these to a file as such:
```

```
/opt/CSCOcnsie/tools/ssldump -i eth0 port 443 > ssl_http.log
/opt/CSCOcnsie/tools/ssldump -i eth0 port 11012 > ssl_event.log
```

IOS SSL Device Troubleshooting

The following debug and show commands are available on most of the IOS CPE's that support the SSL Security Layer. These commands can provided the operator all the information they may need to help debug a SSL Client trustpoint setup in the CPE device.

PKI Debug Commands

The following example shows the PKI debug commands.

```
debug crypto pki transactions
debug crypto pki messages
```

SSL Debug Commands

The following example shows the SSL debug commands.

```
debug ssl traffic
debug ssl error
debug ssh hdshake
```

Show Crypto Commands

The following example shows the crypto commands.

```
show crypto key pubkey-chain rsa
show crypto ca trustpoints
show crypto ca certificate
```

Show Crypto Key Pubkey-Chain RSA Command

The following example shows the output of what a Trustpoint certificate public key looks like in the IOS Device:

```
Router#show crypto key pubkey-chain rsa
Codes: M - Manually configured, C - Extracted from certificate

Code     Usage     IP-Address/VRF         Keyring            Name
C       Signing                           default            X.500 DN name:
                                CN = IOS-CA1
                                OU = Marketing
                                O = Company Co Inc.
                                L = San Jose
                                ST = CA
                                C = US
                                EA = administrator@company.com
```

Show Crytpo CA Trustpoint

The following example shows the output of a IOS SSL Trustpoint certificate contents and signature looks like in the IOS Device:

```
Router#show crypto ca trustpoints
Trustpoint cisco-ssl-home:
    Subject Name:
    CN = IOS-CA1
    OU = Marketing
    O = Company Co Inc.
    L = San Jose
    ST = CA
    C = US
    EA = administrator@company.com
        Serial Number: 4D69F1E1D5F8D6AC4F63BF0ACAAB4F9F
Certificate configured.
CEP URL: http://my-iosca
```

Show Crypto CA Certificate

The following example shows the output of the IOS “show crypto ca cert” contents look like in the IOS Device:

```
Router#show crypto ca cert
CA Certificate
    Status: Available
    Certificate Serial Number: 2D19F1841F8D56AC4F63BF0AC1DB4F9F
Certificate Usage: Signature
Issuer:
    CN = IOS-CA1
    OU = Marketing
    O = Company Co Inc.
    L = San Jose
    ST = CA
    C = US
    EA = administrator@company.com
Subject:
    CN = IOS-CA1
    OU = Marketing
    O = Company Co Inc.
    L = San Jose
    ST = CA
    C = US
    EA = administrator@company.com
CRL Distribution Point:
    http://my-iosca
Validity Date:
    start date: 22:43:53 UTC May 28 2003
    end date: 22:52:12 UTC May 28 2005
Associated Trustpoints: ssl-home
```

CNS ID Syntax

The following example shows the CNS ID Syntax.

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#cns id ?
    Async          Async interface
    BVI            Bridge-Group Virtual Interface
    CDMA-Ix        CDMA Ix interface
    CTunnel        CTunnel interface
    Dialer         Dialer interface
    Ethernet       IEEE 802.3
    FastEthernet   FastEthernet IEEE 802.3
    Group-Async    Async Group interface
    Lex            Lex interface
    Loopback       Loopback interface
    MFR            Multilink Frame Relay bundle interface
    Multilink      Multilink-group interface
    Tunnel         Tunnel interface
    Vif            PGM Multicast Host interface
    Virtual-PPP Virtual PPP interface
    Virtual-Template Virtual Template interface
    Virtual-TokenRing Virtual TokenRing
    Vlan Catalyst Vlans
    hardware-serial Use hardware serial number as unique ID
    hostname Use hostname as unique ID
    string Use an arbitrary string as the unique ID
```

CNS ID Network Interface Value Lookups

The following example shows the output of the CNS ID network interface value:

```
Router#enable
Router#configure terminal
Router#(config)#cns id FastEthernet 0 ?
ipaddress Use IP address as unique ID
mac-address Use MAC address as unique ID

Router(config)#cns id Async 1 ?
ipaddress Use IP address as unique ID
mac-address Use MAC address as unique ID
```

CNS ID Hardware Serial Number

The following example shows the output of the CNS ID hardware serial number:

```
Router(config)#cns id hardware-serial ?
event Set this ID as the event ID
image Set this ID as the image ID
<cr>
```

Viewing the Motherboard Hardware Serial Number

The following example shows the output of the motherboard hardware serial number:

```
Router#enable
Router#config terminal
Router(config)#do show version
Cisco IOS Software, C1700 Software (C1700-ADVENTERPRISEK9-M), Experimental Version 12.3
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Feb-04 20:04 by ntimms
ROM: System Bootstrap, Version 12.2(7r)XM4, RELEASE SOFTWARE (fc1)
cisco-1711 uptime is 2 days, 19 hours, 27 minutes
System returned to ROM by reload
System restarted at 07:51:21 UTC Thu Mar 4 2004
System image file is "flash:c1700-adventerprisek9-mz.24.Feb.2004"
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1711 (MPC862P) processor (revision 0x100) with 116939K/14133K bytes of memory.
Processor board ID FOC07271A6Q (2119579075), with hardware revision 0000
MPC862P processor: part number 7, mask 0
1 Ethernet interface
5 FastEthernet interfaces
1 Serial interface
1 terminal line
1 Virtual Private Network (VPN) Module
32K bytes of NVRAM.
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

View the CNS Image ID to Hardware-Serial

The following example shows the output of the CNS Image to hardware-serial:

```
Router#enable
Router#configure terminal
Router(config)#cns id hardware-serial image
Router(config)#do show cns image status
CNS Image Agent ID: FOC07271A6Q
Number of failed upgrades: 0
Number of successful upgrades: 0
Messages received: 8
Receive errors: 1
Bad XML format:1       Not Supported:0    Invalid Parameter:0
Memory exhausted:0     File too large:0   Operation failed:0
File Errors:0          Auth Errors: 0
Transmit Status
TX Attempts:7
Successes:6 Failures 3
Detailed Failures
Memory exhausted:0     queue error:0      external error:0
other error:3
```

CNS Config ID to Hardware-Serial

The following example shows the output of the CNS config id to hardware-serial:

```
Router#enable
Router#configure terminal
Router(config)#cns id hardware-serial
Router(config)#do show cns config connections
The partial configuration agent is enabled.
Configuration server: 10.1.25.94
Port number: 80
Encryption: disabled
Config id: FOC07271A6Q
Connection Status:
The initial configuration agent is not running.
```

Note The hardware-serial ID is what is listed in the 'show version' command and is retrieved internally by the CNS Agents from the device's motherboard. This may or may not be the same alpha-numeric string as the serial-number printed on the chassis of your particular Cisco IOS Device.

Additional Information Sources

You can refer the following documents for additional information.

Cisco IOS Certificate Server

For more information on Cisco IOS certificate server, see the document at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb0.html.

Certificate Server Data Sheet

For more information on certificate server data sheet, see the technical document at:

http://www.cisco.com/en/US/tech/tk583/tk372/tech_brief09186a00801e05dc.html.

Cisco IOS PKI

Cisco IOS Software Releases 12.3 T / Security Commands

For more information on Cisco IOS software releases and security commands, see the command reference document at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7f81.html.

SSL Public Key Infrastructure

For more information on SSL public key infrastructure, see the white paper at:

http://www.cisco.com/en/US/tech/tk583/tk618/technologies_white_paper09186a0080179739.shtml.

Certificate Security Attribute-Based Access Control

For more information on certificate security attribute-based access control, see the document at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541ce.html.

Cisco IOS Certificate Server Data Sheet

For more information on Cisco IOS certificate server data sheet, see the document at

http://www.cisco.com/en/US/tech/tk583/tk372/tech_brief09186a00801e05dc.html.

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/certs_ds.pdf.

Cisco IOS Certificate Server and Software Releases 12.3 T

For more information on Cisco IOS server and software releases 12.4, see the document at

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb0.html.

Trusted Root Certification Authority

For more information on trusted rooted certificate authority, see the document at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008007fecf.html.

Online Certificate Status Protocol

For more information on online certificate status protocol, see the document at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a755b.html.

Cisco's SCEP Home Page

For more information on SCEP home page, refer the document at:

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.html.

CISCO IOS Software Releases 12.3 T

For more information on Cisco IOS software releases 12.3 T and RSA Key pair, see the document at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb4.html.

Trustpoint Command

For more information on trustpoint commands, see the document at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm.

Certificate Enrollment Enhancements

For more information on certificate enrollment enhancements, see the document at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftenrol2.htm.

Configuring Crypto Maps

For more information on configuring crypto maps for DN-based access control, see the document at:

http://www.cisco.com/warp/public/471/vpn_dn.html - tools

Multiple RSA Key Pair Support

For more information on multiple RSA key pair support, see the document at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm -42193.

Simple Certificate Enrollment Protocol:

For more information on simple certificate enrollment protocol, see the document at:

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm.

Public Domain OpenSSL

For more information on OpenSSL, see *http://www.openssl.org.*

OpenSSL certificates

For more information on OpenSSL certificate, see *http://www.openssl.org/docs/HOWTO/certificates.txt.*

APPENDIX **A**

Installing the VMware

This appendix provides system requirements and procedures for installing the VMware software on the Windows or Linux platforms.

Installing the VMware

This section describes the installation process of VMware. The host operation system for VMware could be either Windows or Linux. The guest operating system for Cisco Configuration Engine is RHEL4 or RHEL5.

The Cisco Configuration Engine customers should refer to the formal VMware installation and setup guide from *VMware.com*. The steps captured in this document are used to setup the VMware environment and test the Cisco Configuration Engine in our test lab. It could be used as a reference document.

To install the VMware, follow these steps:

Step 1 Download the VMware software from the website *vmware.com*.

Step 2 Copy the VMware RPM file into a new folder where there is sufficient disk space (see Chapter 1, "Understanding Disk Space Calculation"):

Step 3 Run the **rpm -ivh** <*vmware rmp name*> command to install the VMware software.

Step 4 After the program is installed, from a new command prompt, enter the **/usr/bin/vmware-config.p**l installation script command, and press **Enter** to execute the configuration program. The console displays the following messages:

```
[root@ce-scale-1 /]# /usr/bin/vmware-config.pl
Making sure services for VMware Server are stopped.

Stopping VMware autostart virtual machines:
   Virtual machines                                        [FAILED]
Stopping VMware management services:
   VMware Virtual Infrastructure Web Access
   VMware Server Host Agent                                [FAILED]
Stopping VMware services:
   VMware Authentication Daemon                            [  OK  ]
   Virtual machine monitor                                 [  OK  ]
You must read and accept the End User License Agreement to continue.
Press enter to display it.
```

Note Ignore the error message [FAILED] in the VMware console display.

Step 5 At the system prompt, enter **yes** to accept the End User License Agreement.

Step 6 At the system prompt, enter **yes** to network the virtual machines. The system prompts you for configuring a bridged network for **vmnet0**.

Step 7 Enter a **name** for the bridge network, and press **Enter**. If the machine has two ethernet interfaces, the program displays the following message:

```
Your computer has multiple ethernet network interfaces available: eth0, eth1
Which one do you want to bridge to vmnet0? [eth0]
```

Step 8 At the system prompt, press **Enter**. The program displays the following message:

```
The following bridged networks have been defined:
. vmnet0 is bridged to eth0
Do you wish to configure another bridged network? (yes/no) [no] no
```

Step 9 Enter **yes** at the prompt to configure more virtual networks on this host machine. The system prompts you for configuring a bridged network for **vmnet2**.

Step 10 Enter a **name** for the bridge network and press **Enter**. The program displays the following message:

```
The following bridged networks have been defined:
. vmnet0 is bridged to eth0
. vmnet2 is bridged to eth1
```

Step 11 At the system prompt, enter **yes** to use the host-only networking in your virtual machines.

```
Configuring a host-only network for vmnet1.
Please specify a name for this network.
[HostOnly]
Do you want this program to probe for an unused private subnet? (yes/no/help)
[yes] no
What will be the IP address of your host on the private
network? 10.5.105.0
What will be the netmask of your private network? 255.255.255.0
The following host-only networks have been defined:

. vmnet1 is a host-only network on private subnet 10.5.105.0.

Do you wish to configure another host-only network? (yes/no) [no]
```

Step 12 At the system prompt, press **Enter** for the following prompts:

```
Please specify a port for remote connections to use [902]
Please specify a port for standard http connections to use [8222]
Please specify a port for secure http (https) connections to use [8333]
```

Step 13 Enter the name of the administrative user, and enter **yes**.

```
The current administrative user for VMware Server is 'xx'. Would you like to specify a
different administrator? [no] yes
Please specify the user whom you wish to be the VMware Server administrator root
Using root as the VMware Server administrator.
```

Step 14 At the system prompt, press **Enter** for the following prompts:

```
In which directory do you want to keep your virtual machine files?
[/var/lib/vmware/Virtual Machines]

The path "/var/lib/vmware/Virtual Machines" does not exist currently. This program is
going to create it, including needed parent directories.
```

```
Is this what you want? [yes]
```

Step 15 Enter your serial number in the xxxxx-xxxxx-xxxxx-xxxx format. The console displays the following messages:

```
Creating a new VMware VIX API installer database using the tar4 format.
Installing VMware VIX API.
In which directory do you want to install the VMware VIX API binary files?
[/usr/bin]
In which directory do you want to install the VMware VIX API library files?
[/usr/lib/vmware-vix/lib]
The path "/usr/lib/vmware-vix/lib" does not exist currently. This program is
going to create it, including needed parent directories. Is this what you want?
[yes]
In which directory do you want to install the VMware VIX API document pages?
[/usr/share/doc/vmware-vix]
The path "/usr/share/doc/vmware-vix" does not exist currently. This program is
going to create it, including needed parent directories. Is this what you want?
[yes]
The installation of VMware VIX API 1.6.0 build-122956 for Linux completed
successfully. You can decide to remove this software from your system at any
time by invoking the following command: "/usr/bin/vmware-uninstall-vix.pl.
```

Step 16 The program initializes the services of VMware and completes the installation.

```
Starting VMware services:
   Virtual machine monitor                                    [  OK  ]
   Virtual machine communication interface                    [  OK  ]
   VM communication interface socket family:                  [  OK  ]
   Virtual ethernet                                           [  OK  ]
   Bridged networking on /dev/vmnet0                          [  OK  ]
   Host-only networking on /dev/vmnet1 (background)           [  OK ]
   DHCP server on /dev/vmnet1                                 [  OK  ]
   Bridged networking on /dev/vmnet2                          [  OK  ]
   Host-only networking on /dev/vmnet8 (background)           [  OK  ]
   DHCP server on /dev/vmnet8                                 [  OK  ]
   NAT service on /dev/vmnet8                                 [  OK  ]
   VMware Server Authentication Daemon (background)           [  OK  ]
   Shared Memory Available                                    [  OK  ]
Starting VMware management services:
   VMware Server Host Agent (background)                      [  OK  ]
   VMware Virtual Infrastructure Web Access
Starting VMware autostart virtual machines:
   Virtual machines                                           [  OK  ]

The configuration of VMware Server 2.0.0 build-122956 for Linux for this
running kernel completed successfully.
```

Step 17 You can now login to the VMware server program by using the web browser on the host machine.

INDEX

A

C

D

E

H

I