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/3.5.4/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, page 3-33
- Understanding Cisco IOS Agents, page 3-37
- Configuring Cisco IOS Agents, page 3-38

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*
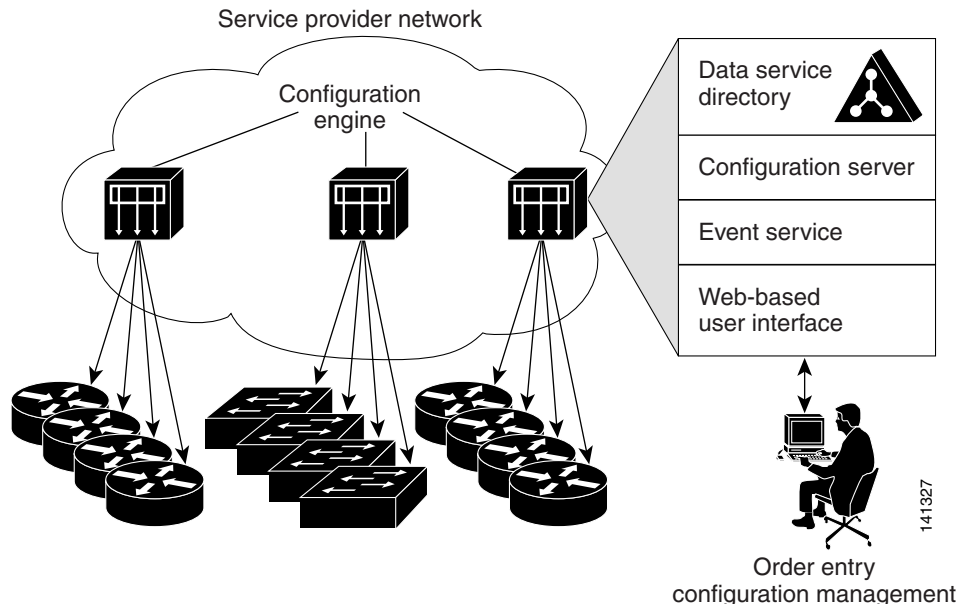
The Cisco Configuration Engine supports standalone and server modes:

- 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

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 3-37
- Incremental (Partial) Configuration, page 3-38
- Synchronized Configuration, page 3-38
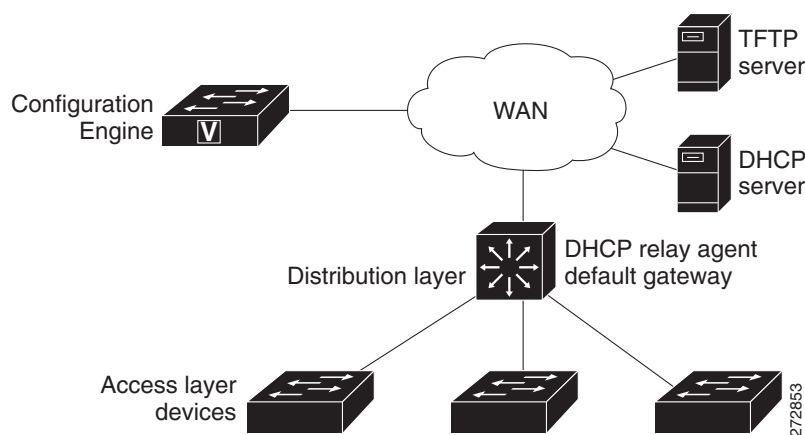
Initial Configuration

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.