CHAPTER 5

Cisco IOS Configuration Engine

This chapter describes how to use the Cisco Configuration Engine to configure the CGR 2010 ESM.

Note For complete configuration information for the Cisco Configuration Engine, go to http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

For complete syntax and usage information for the commands used in this chapter, go to the *Cisco IOS Network Management Command Reference, Release 12.4* at http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

This chapter consists of the following topics:

Understanding Cisco Configuration Engine Software

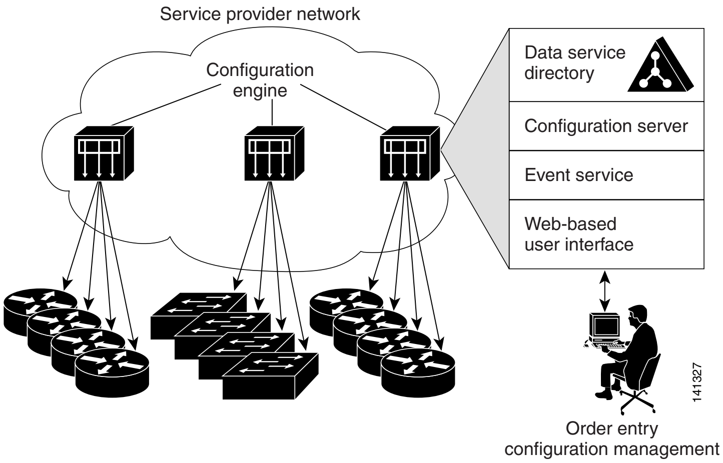
The Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services (see Figure 5-1). Each Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The 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.

The Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

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

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

Figure 5-1 Configuration Engine Architectural Overview



These sections contain the following conceptual information:

- Configuration Service, page 5-2
- Event Service, page 5-2
- About the CNS IDs and Device Hostnames, page 5-3

Configuration Service

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a configuration server that works with Cisco IOS CNS agents on the switch module. The Configuration Service delivers device and service configurations to the switch module for initial configuration and mass reconfiguration by logical groups. Switches receive their initial configuration from the Configuration Service when they start up on the network for the first time.

The Configuration Service uses the CNS Event Service to send and receive configuration change events and to send success and failure notifications.

The configuration server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server 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 a directory.

The Cisco IOS agent can perform a syntax check on received configuration files and publish events to show the success or failure of the syntax check. The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.

Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of configuration events. The event agent is on the switch module and facilitates the communication between the switch module and the event gateway on the Configuration Engine.

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

NameSpace Mapper

The Configuration Engine includes the NameSpace Mapper (NSM) that 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.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.

About the CNS IDs and Device Hostnames

The Configuration Engine assumes that a unique identifier is associated with each configured switch module and switch module. 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 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 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 switch module.

Within the scope of a single instance of the configuration server, no two configured switches can share the same value for ConfigID. Within the scope of a single instance of the event bus, no two configured switches can share the same value for DeviceID.

ConfigID

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

The ConfigID is fixed at startup time and cannot be changed until the device restarts, even if the switch module hostname is reconfigured.

DeviceID

Each configured switch module or switch module participating on the event bus has a unique DeviceID, which is analogous to the switch module source address so that the switch module can be targeted as a specific destination on the bus. All switches configured with the **cns config partial** global configuration command must access the event bus. The DeviceID, as originated on the switch module, must match the DeviceID of the corresponding switch module definition in the Configuration Engine.

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

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 switch module. The event gateway represents the switch module and its corresponding DeviceID to the event bus.

the switch module 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 switch module.

Hostname and DeviceID

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

When changing the switch module hostname on the switch module, the only way to refresh the DeviceID is to break the connection between the switch module and the event gateway. Enter the **no cns event** global configuration command followed by the **cns event** global configuration command.

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

Caution When using the Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch module acquires *after*–not *before*–you use the **cns config initial** global configuration command at the switch module. Otherwise, subsequent **cns config partial** global configuration command operations malfunction.

Using Hostname, DeviceID and ConfigID

In standalone mode, when a hostname value is set for a switch module, 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 switch module.

These and other associated attributes (tag value pairs) are set when you run **Setup** on the Configuration Engine.

Note For more information about running the setup program on the Configuration Engine, see the Configuration Engine setup and configuration guide at http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/prod_installation_guides_list.html

Understanding Cisco IOS Agents

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

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

Initial Configuration

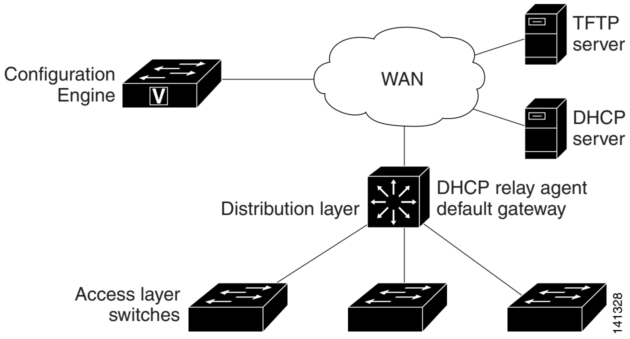
When the switch module first comes up, it attempts to get an IP address by broadcasting a DHCP request on the network. Assuming there is no DHCP server on the subnet, the distribution switch module acts as a DHCP relay agent and forwards the request to the DHCP server. On receiving the request, the DHCP server assigns an IP address to the new switch module 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 switch module.

The switch module 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 switch module loads the file in its running configuration.

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

Figure 5-2 shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

Figure 5-2 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 switch module. 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 switch module to initiate a pull operation.

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

Synchronized Configuration

When the switch module receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the switch module not to save the updated configuration into its NVRAM. The switch module uses the updated configuration as its running configuration. This ensures that the switch module 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 switch module Cisco IOS software allow the switch module to be connected and automatically configured as described in the "Enabling Automated CNS Configuration" section on page 5-6. If you want to change the configuration or install a custom configuration, see these sections for instructions:

- Enabling the CNS Event Agent, page 5-7
- Enabling the Cisco CNS Configuration Agent, page 5-9
- Upgrading Devices with Cisco CNS Image Agent, page 5-11

Enabling Automated CNS Configuration

To enable automated CNS configuration of the switch module, you must first complete the prerequisites in Table 5-1. When you complete them, power on the switch module. At the **setup** prompt, do nothing: The switch module begins the initial configuration as described in the "Initial Configuration" section on page 5-5. When the full configuration file is loaded on your switch module, you need to do nothing else.

Table 5-1 Prerequisites for Enabling Automatic Configuration

Device	Required Configuration
Access switch module	Factory default (no configuration file)
Distribution switch module	• IP helper address • Enable DHCP relay agent • IP routing (if used as default gateway)
DHCP server	• IP address assignment • TFTP server IP address • Path to bootstrap configuration file on the TFTP server • Default gateway IP address

Table 5-1 Prerequisites for Enabling Automatic Configuration (continued)

Device	Required Configuration
TFTP server	• A bootstrap configuration file that includes the CNS configuration commands that enable the switch module to communicate with the Configuration Engine • The switch module configured to use either the switch module MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID • The CNS event agent configured to push the configuration file to the switch module
CNS Configuration Engine	One or more templates for each type of device, with the ConfigID of the device mapped to the template.

Note For more information about running the setup program and creating templates on the Configuration Engine, see the *Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux* at http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

Enabling the CNS Event Agent

Note You must enable the CNS Event Agent on the switch module before you enable the CNS configuration agent.

Beginning in privileged EXEC mode, follow these steps to enable the CNS event agent on the switch module:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the event agent, and enter the gateway parameters. • For {*hostname* | *ip-address*}, enter either the hostname or the IP address of the event gateway. • (Optional) For *port number*, enter the port number for the event gateway. The default port number is 11011. • (Optional) Enter **backup** to show that this is the backup gateway. (If omitted, this is the primary gateway.) • (Optional) For **failover-time** *seconds*, enter how long the switch module waits for the primary gateway route after the route to the backup gateway is established. • (Optional) For **keepalive** *seconds*, enter how often the switch module sends keepalive messages. For *retry-count*, enter the number of unanswered keepalive messages that the switch module sends before the connection is terminated. The default for each is 0. • (Optional) For **reconnect** *time*, enter the maximum time interval that the switch module waits before trying to reconnect to the event gateway. • (Optional) For **source** *ip-address*, enter the source IP address of this device. • Though visible in the command-line help string, the **encrypt** and the **clock-timeout** *time* keywords are not supported.	**cns event** {*hostname* | *ip-address*} [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**reconnect** *time*] [**source** *ip-address*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify information about the event agent.	**show cns event connections**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable the CNS event agent, use the **no cns event** {*ip-address* | *hostname*} global configuration command.

This example shows how to enable the CNS event agent, set the IP address gateway to 10.180.1.27, set 120 seconds as the keepalive interval, and set 10 as the retry count.

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```

Enabling the Cisco CNS Configuration Agent

After enabling the CNS event agent, start the Cisco IOS CNS Configuration Agent on the switch module. You can enable the Cisco IOS agent with these commands:

- The **cns config initial** global configuration command enables the Cisco IOS agent and initiates an initial configuration on the switch module.
- The **cns config partial** global configuration command enables the Cisco IOS agent and initiates a partial configuration on the switch module. You can then use the Configuration Engine to remotely send incremental configurations to the switch module.

Enabling an Initial Configuration

Beginning in privileged EXEC mode, follow these steps to enable the IOS CNS configuration agent and initiate an initial configuration on the switch module:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter CNS template connect configuration mode, and specify the name of the CNS connect template.	**cns template connect** *name*
Step 3	Enter a command line for the CNS connect template. Repeat this step for each command line in the template.	**cli** *config-text*
Step 4	Repeat Steps 2 to 3 to configure another CNS connect template.	
Step 5	Return to global configuration mode.	**exit**

To disable the CNS Cisco IOS agent, use the **no cns config initial** {*ip-address* | *hostname*} global configuration command.

This example shows how to configure an initial configuration on a remote switch module when the switch module configuration is unknown (the CNS Zero Touch feature).

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```

This example shows how to configure an initial configuration on a remote switch module when the switch module IP address is known. The Configuration Engine IP address is 172.28.129.22.

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

Enabling a Partial Configuration

Beginning in privileged EXEC mode, follow these steps to enable the Cisco IOS agent and to initiate a partial configuration on the switch module:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the configuration agent, and initiate a partial configuration. • For {*ip-address* | *hostname*}, enter the IP address or the hostname of the configuration server. • (Optional) For *port-number*, enter the port number of the configuration server. The default port number is 80. • (Optional) Enter **source** *ip-address* to use for the source IP address. **Note** Though visible in the command-line help string, the **encrypt** keyword is not supported.	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify information about the configuration agent.	**show cns config stats** or **show cns config outstanding**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable the Cisco IOS agent, use the **no cns config partial** {*ip-address* | *hostname*} global configuration command. To cancel a partial configuration, use the **cns config cancel** privileged EXEC command.

Upgrading Devices with Cisco CNS Image Agent

Administrators maintaining large networks of Cisco IOS devices need an automated mechanism to load image files onto large numbers of remote devices. Existing network management applications are useful to determine which images to run and how to manage images received from the Cisco online software center. Other image distribution solutions do not scale to cover thousands of devices and cannot distribute images to devices behind a firewall. The Cisco CNS Image Agent enables the managed device to initiate a network connection and request an image download allowing devices behind firewalls to access the image server.

You can use the Image Agent to download one or more devices. The switch modulees must have the Image Agent running on them.

Prerequisites for the CNS Image Agent

Confirm these prerequisites before upgrading one or more devices with image agent:

- Determine where to store the Cisco IOS images on a file server to make the image available to the other networking devices. If the CNS Event Bus is to be used to store and distribute the images, the CNS event agent must be configured.
- Set up a file server to enable the networking devices to download the new images using the HTTPS protocol.
- Determine how to handle error messages generated by image agent operations. Error messages can be sent to the CNS Event Bus or an HTTP or HTTPS URL.

Restrictions for the CNS Image Agent

During automated image loading operations you must try to prevent the Cisco IOS device from losing connectivity with the file server that is providing the image. Image reloading is subject to memory issues and connection issues. Boot options must also be configured to allow the Cisco IOS device to boot another image if the first image reload fails.

These other restrictions apply to the image agent running on a the switch module:

- You can only download the tar image file. Downloading the bin image file is not supported.
- Only the immediate download option is supported. You cannot schedule a download to occur at a specified date and time.
- The Destination field in the Associate Image with Device window is not supported.

For more details, see your CNS IE2100 documentation and see the "File Management" section of the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2.*

Beginning in privileged EXEC mode, follow these steps to initiate the image agent to check for a new image and upgrade a device:

	Step	Command
Step 1	Enter global configuration mode	**configure terminal**
Step 2	Enter the IP address and the hostname of the event gateway.	**ip host** {*ip-address*} {*hostname*}
Step 3	Specify a trusted server for CNS agent.	**cns trusted-server all-agents** {*hostname*}

	Step	Command
Step 4	Disable AAA authentication on the event gateway.	**no cns aaa enable cns event** {*ip-address*} {*port number*}
Step 5	Specify the number of times to retry and download the image.	**cns image retry** {*number*}
Step 6	Download the image from the server to the switch module.	**cns image server** {*ip-address*} **status** {*ip-address*}
Step 7	Return to privileged EXEC mode.	**end**

Note This example shows how to upgrade a switch module from a server with the address of **172.20.249.20:**

```
Switch(config)> configure terminal
Switch(config)# ip host cns-dsbu.cisco.com 172.20.249.20
Switch(config)# cns trusted-server all-agents cns-dsbu.cisco.com
Switch(config)# no cns aaa enable cns event 172.20.249.20 22022
Switch(config)# cns image retry 1
Switch(config)# cns image server http://172.20.249.20:80/cns/HttpMsgDispatcher status
http://172.20.249.20:80/cns/HttpMsgDispatcher
Switch(config)# end
```

You can check the status of the image download by using the **show cns image** status user EXEC command.

Displaying CNS Configuration

You can use the privileged EXEC commands in Table 5-2 to display CNS configuration information.

Table 5-2 Displaying CNS Configuration

Command	Description
show cns config connections	Displays the status of the CNS Cisco IOS agent connections.
show cns config outstanding	Displays information about incremental (partial) CNS configurations that have started but are not yet completed.
show cns config stats	Displays statistics about the Cisco IOS agent.
show cns event connections	Displays the status of the CNS event agent connections.
show cns event stats	Displays statistics about the CNS event agent.
show cns event subject	Displays a list of event agent subjects that are subscribed to by applications.