Configuring Cisco Networking Services

Last Updated: December 20, 2011

The Cisco Networking Services (CNS) feature is a collection of services that can provide remote event-driven configuring of Cisco IOS networking devices and remote execution of some command-line interface (CLI) commands.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco Networking Services

- Configure the remote router to support the Cisco Networking Services configuration agent and the Cisco Networking Services event agent.
- Configure a transport protocol on the remote router that is compatible with the remote router's external interface. The following table lists the supported transport protocols that can be used depending on the router interface.

- Create the configuration template in the Cisco Networking Services configuration-engine provisioning database. (This task is best done by a senior network designer.)

Table 1　　　　***Router Interface and Transport Protocols Required by Cisco Networking Services Services***

	Transport Protocol		
Router Interface	SLARP	ATM InARP	PPP (IPCP)
T1	Yes	Yes	Yes
ADSL	No	Yes	Yes
Serial	Yes	No	Yes

Cisco Networking Services Image Agent

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

Restrictions for Cisco Networking Services

Cisco Networking Services Configuration Engine

- The Cisco Networking Services configuration engine must be the Cisco Intelligence Engine 2100 (Cisco IE2100) series and must be running software version 1.3.
- The configuration engine must have access to an information database of attributes for building a configuration. This database can reside on the Cisco IE2100 itself.
- Configuration templates must be prepared on the Cisco Networking Services configuration engine before installation of the remote router.
- The user of Cisco Networking Services Flow-Through Provisioning and the Cisco Networking Services configuration engine must be familiar with designing network topologies, designing configuration templates, and using the Cisco Networking Services configuration engine.

Cisco Networking Services 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. For more details see the "Managing Configuration Files" module of the *Cisco IOS Configuration Fundamentals Configuration Guide* .

Cisco Networking Services Frame Relay Zero Touch

The Cisco Networking Services Frame Relay Zero Touch solution does not support switched virtual circuits (SVCs).

The Frame Relay zero touch solution does not support IP over PPP over Frame Relay because routing to an interface (or subinterface) that supports IP over PPP over Frame Relay is not possible.

Command Scheduler

The EXEC CLI specified in a Command Scheduler policy list must neither generate a prompt nor can it be terminated using keystrokes. Command Scheduler is designed as a fully automated facility, and no manual intervention is permitted.

Remote Router

- The remote router must run a Cisco IOS image that supports the Cisco Networking Services configuration agent and Cisco Networking Services event agent.
- Ports must be prepared on the remote router for connection to the network.
- You must ensure that the remote router is configured using Cisco Configuration Express.

Information About Cisco Networking Services

Cisco Networking Services

Cisco Networking Services is a foundation technology for linking users to networking services and provides the infrastructure for the automated configuration of large numbers of network devices. Many IP networks are complex with many devices, and each device must currently be configured individually. When standard configurations do not exist or have been modified, the time involved in initial installation and subsequent upgrading is considerable. The volume of smaller, more standardized, customer networks is also growing faster than the number of available network engineers. Internet service providers (ISPs) now need a method for sending out partial configurations to introduce new services. To address all these issues, Cisco Networking Services has been designed to provide "plug-and-play" network services using a central directory service and distributed agents. Cisco Networking Services features include Cisco Networking

Services configuration and event agents and a Flow-Through Provisioning structure. The configuration and event agents use a Cisco Networking Services configuration engine to provide methods for automating initial Cisco IOS device configurations, incremental configurations, and synchronized configuration updates, and the configuration engine reports the status of the configuration load as an event to which a network monitoring or workflow application can subscribe. The Cisco Networking Services Flow-Through Provisioning uses the Cisco Networking Services configuration and event agents to provide an automated workflow, eliminating the need for an on-site technician.

Cisco Networking Services Configuration Agent

The Cisco Networking Services configuration agent is involved in the initial configuration and subsequent partial configurations on a Cisco IOS device. To activate the Cisco Networking Services configuration agent, enter any of the **cns config** CLI commands.

Initial Cisco Networking Services Configuration

When a routing device first comes up, it connects to the configuration server component of the Cisco Networking Services configuration agent by establishing a TCP connection through the use of the **cns config initial**command, a standard CLI command. The device issues a request and identifies itself by providing a unique configuration ID to the configuration server.

When the Cisco Networking Services web server receives a request for a configuration file, it invokes the Java servlet and executes the corresponding embedded code. The embedded code directs the Cisco Networking Services web server to access the directory server and file system to read the configuration reference for this device (configuration ID) and template. The Configuration Agent prepares an instantiated configuration file by substituting all the parameter values specified in the template with valid values for this device. The configuration server forwards the configuration file to the Cisco Networking Services web server for transmission to the routing device.

The Cisco Networking Services configuration agent accepts the configuration file from the Cisco Networking Services web server, performs XML parsing, checks syntax (optional), and loads the configuration file. The routing device reports the status of the configuration load as an event to which a network monitoring or workflow application can subscribe.

For more details on using the Cisco Cisco Networking Services configuration engine to automatically install the initial Cisco Networking Services configuration, see the *Cisco Networking Services Configuration Engine Administrator's Guide* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns/ce/rel13/ag13/index.htm .

Incremental Cisco Networking Services Configuration

Once the network is up and running, new services can be added using the Cisco Networking Services configuration agent. Incremental (partial) configurations can be sent to routing devices. 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 routing device can check the syntax of the configuration before applying it. If the syntax is correct, the routing device applies the incremental configuration and publishes an event that signals success to the configuration server. If the device fails to apply the incremental configuration, it publishes an event that indicates an error.

Once the routing device has applied the incremental configuration, it can write the configuration to NVRAM or wait until signaled to do so.

Synchronized Configuration

When a routing device receives a configuration, the device has the option to defer application of the configuration upon receipt of a write-signal event. The Cisco Networking Services Configuration Agent feature allows the device configuration to be synchronized with other dependent network activities.

Cisco Networking Services Config Retrieve Enhancement with Retry and Interval

The Cisco Networking Services Config Retrieve Enhancement with Retry and Interval feature adds new functionality to the **cns config retrieve** command enabling you to specify the retry interval and an amount of time in seconds to wait before attempting to retrieve a configuration from a trusted server.

Cisco Networking Services EXEC Agent

The CNS EXEC agent allows a remote application to execute an EXEC mode CLI command on a Cisco IOS device by sending an event message that contains the command. A restricted set of EXEC **show** commands is supported.

Cisco Networking Services Event Agent

Although other Cisco Networking Services agents may be configured, no other Cisco Networking Services agents are operational until the **cns event**command is entered because the Cisco Networking Services event agent provides a transport connection to the Cisco Networking Services event bus for all other Cisco Networking Services agents. The other Cisco Networking Services agents use the connection to the Cisco Networking Services event bus to send and receive messages. The Cisco Networking Services event agent does not read or modify the messages.

Cisco Networking Services 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 or using Network Address Translation (NAT). The Cisco Networking Services image agent enables the managed device to initiate a network connection and request an image download allowing devices using NAT, or behind firewalls, to access the image server.

The Cisco Networking Services image agent can be configured to use the Cisco Networking Services Event Bus. To use the Cisco Networking Services Event Bus, the Cisco Networking Services event agent must be enabled and connected to the Cisco Networking Services event gateway in the Cisco Networking Services Configuration Engine. The Cisco Networking Services image agent can also use an HTTP server that understands the Cisco Networking Services image agent protocol. Deployment of Cisco Networking Services image agent operations can use both the Cisco Networking Services Event Bus and an HTTP server.

Cisco Networking Services Message Formats

SOAP Message Format

Using the Service-Oriented Access Protocol (SOAP) protocol provides a way to format the layout of Cisco Networking Services messages in a consistent manner. SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. SOAP uses extensible markup language (XML) technologies to define an extensible messaging framework that provides a message format that can be exchanged over a variety of underlying protocols.

Within the SOAP message structure, there is a security header that enables Cisco Networking Services notification messages to authenticate user credentials.

Cisco Networking Services messages are classified into three message types: request, response and notification. The formats of these three message types are defined below.

Request Message

The following is the format of a Cisco Networking Services request message to the Cisco IOS device:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
  <SOAP:Header>
    <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="0">
      <wsse:usernameToken>
        <wsse:Username>john</wsse:Username>
        <wsse:Password>cisco</wsse:Password>
      </wsse:usernameToken>
    </wsse:Security>
    <cns:cnsHeader version="1.0" xmlns:cns="http://www.cisco.com/management/cns/envelope">
      <cns:Agent>CNS_CONFIG</cns:Agent>
      <cns:Request>
        <cns:correlationID>IDENTIFIER</cns:correlationID>
        <cns:ReplyTo>
          <cns:URL>http://10.1.36.9:80/cns/ResToServer</cns:URL>
        </cns:ReplyTo>
      </cns:Request>
      <cns:Time>2003-04-23T20:27:19.847Z</cns:Time>
    </cns:cnsHeader>
  </SOAP:Header>
  <SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
    <config-event config-action="read" no-syntax-check="TRUE">
      <config-data>
        <config-id>AAA</config-id>
        <cli>access-list 1 permit any</cli>
      </config-data>
    </config-event>
  </SOAP:Body>
</SOAP:Envelope>
```

Note   The ReplyTo field is optional. In the absence of the ReplyTo field, the response to the request will be sent to the destination where the request originated. The body portion of this message contains the payload and is processed by the Cisco Networking Services agent mentioned in the Agent field.

Response Message

The following is the format of a Cisco Networking Services response message from the Cisco IOS device as a response to a request:

```
?xml version="1.0" encoding="UTF-8"?
SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope"
SOAP:Header
wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true"
wsse:UsernameToken
wsse:Username infysj-7204-8 /wsse:Username
wsse:Password NTM3NTg2NzIzOTg2MTk2MjgzNQ==/wsse:Password
/wsse:UsernameToken /wsse:Security
CNS:cnsHeader Version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope"
CNS:Agent CNS_CONFIG /CNS:Agent
CNS:Response
CNS:correlationID IDENTIFIER /CNS:correlationID
/CNS:Response
CNS:Time 2005-06-23T16:27:36.185Z /CNS:Time
/CNS:cnsHeader
/SOAP:Header
SOAP:Body xmlns="http://www.cisco.com/management/cns/config"
config-success config-id AAA /config-id /config-success
/SOAP:Body
/SOAP:Envelope
```

Note   The value of CorrelationId is echoed from the corresponding request message.

The body portion of this message contains the response from the Cisco IOS device to a request. If the request is successfully processed, the body portion contains the value of the response put in by the agent that processed the request. If the request cannot be successfully processed, then the body portion will contain an error response.

Notification Message

The following is the format of a Cisco Networking Services notification message sent from the Cisco IOS device:

```
?xml version="1.0" encoding="UTF-8"?
SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope"
SOAP:Header
wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true"
wsse:UsernameToken
wsse:Username dvlpr-7200-2 /wsse:Username
wsse:Password /wsse:Password
/wsse:UsernameToken
/wsse:Security
CNS:cnsHeader version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope"
CNS:Agent CNS_CONFIG_CHANGE/CNS:Agent
CNS:Notify /CNS:Notify
CNS:Time 2006-01-09T18:57:08.441Z/CNS:Time
/CNS:cnsHeader
/SOAP:Header
SOAP:Body xmlns="http://www.cisco.com/management/cns/config-change"
configChanged version="1.1" sessionData="complete"
sequence lastReset="2005-12-11T20:18:39.673Z" 7 /sequence
changeInfo
user/user
async port con_0 /port /async
when
absoluteTime 2006-01-09T18:57:07.973Z /absoluteTime
/when
/changeInfo
changeData
```

```
changeItem
context /context
enteredCommand
cli access-list 2 permit any /cli
/enteredCommand
oldConfigState
cli access-list 1 permit any /cli
/oldConfigState
newConfigState
cli access-list 1 permit any /cli
cli access-list 2 permit any /cli
/newConfigState
/changeItem
/changeData
/configChanged
/SOAP:Body
/SOAP:Envelope
```

A notification message is sent from the Cisco IOS device without a corresponding request message when a configuration change is made. The body of the message contains the payload of the notification and it may also contain error information. If the request message sent to the Cisco IOS device fails in XML parsing and the CorrelationId field cannot be parsed, then an error notification message will be sent instead of an error response.

Error Reporting

Error is reported in the body of the response or a notification message in the SOAP Fault element. The following is the format for reporting errors.

```
?xml version="1.0" encoding="UTF-8"?
SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope"
SOAP:Header
wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true"
wsse:UsernameToken
wsse:Username dvlpr-7200-2 /wsse:Username
wsse:Password /wsse:Password
/wsse:UsernameToken
/wsse:Security
CNS:cnsHeader version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope"
CNS:Agent CNS_CONFIG /CNS:Agent
CNS:Response
CNS:correlationID SOAP_IDENTIFIER /CNS:correlationID
/CNS:Response
CNS:Time 2006-01-09T19:10:10.009Z /CNS:Time
/CNS:cnsHeader
/SOAP:Header
SOAP:Body xmlns="http://www.cisco.com/management/cns/config"
SOAP:Detail
config-failure
config-id AAA /config-id
error-info
line-number 1 /line-number
error-message CNS_INVALID_CLI_CMD /error-message
/error-info
/config-failure
/SOAP:Detail
/SOAP:Fault
/SOAP:Body
/SOAP:Envelope
```

Cisco Networking Services Interactive CLI

The Cisco Networking Services Interactive CLI feature provides a XML interface that allows you to send interactive commands to a router, such as commands that generate prompts for user input. A benefit of this feature is that interactive commands can be aborted before they have been fully processed. For example, for commands that generate a significant amount of output, the XML interface can be customized to limit the

size of the output or the length of time allowed for the output to accumulate. The capability to use a programmable interface to abort a command before its normal termination (similar to manually aborting a command) can greatly increase the efficiency of diagnostic applications that might use this functionality. The new XML interface also allows for multiple commands to be processed in a single session. The response for each command is packaged together and sent in a single response event.

Cisco Networking Services IDs

The Cisco Networking Services ID is a text string that is used exclusively with a particular Cisco Networking Services agent. The Cisco Networking Services ID is used by the Cisco Networking Services agent to identify itself to the server application with which it communicates. For example, the Cisco Networking Services configuration agent will include the configuration ID when communicating between the networking device and the configuration server. The configuration server uses the Cisco Networking Services configuration ID as a key to locate the attribute containing the Cisco IOS CLI configuration intended for the device that originated the configuration pull.

The network administrator must ensure a match between the Cisco Networking Services agent ID as defined on the routing device and the Cisco Networking Services agent ID contained in the directory attribute that corresponds to the configuration intended for the routing device. Within the routing device, the default value of the Cisco Networking Services agent ID is always set to the hostname. If the hostname changes, the Cisco Networking Services agent ID also changes. If the Cisco Networking Services agent ID is set using the CLI, any change will be followed by a message sent to syslog or an event message will be sent.

The Cisco Networking Services agent ID does not address security issues.

Cisco Networking Services Password

The Cisco Networking Services password is used to authenticate the Cisco Networking Services device. You must configure the Cisco Networking Services password the first time a router is deployed, and the Cisco Networking Services password must be the same as the bootstrap password set on the Configuration Engine (CE). If both the router and the CE bootstrap password use their default settings, a newly deployed router will be able to connect to the CE. Once connected, the CE manages the Cisco Networking Services password. Network administrators must ensure not to change the Cisco Networking Services password. If the Cisco Networking Services password is changed, connectivity to the CE will be lost.

Command Scheduler

The Command Scheduler (KRON) Policy for System Startup feature enables support for the Command Scheduler upon system startup.

The Command Scheduler allows customers to schedule fully-qualified EXEC mode CLI commands to run once, at specified intervals, at specified calendar dates and times, or upon system startup. Originally designed to work with Cisco Networking Services commands, Command Scheduler now has a broader application. Using the Cisco Networking Services image agent feature, remote routers residing outside a firewall or using Network Address Translation (NAT) addresses can use Command Scheduler to launch CLI at intervals, to update the image running in the router.

Command Scheduler has two basic processes. A policy list is configured containing lines of fully-qualified EXEC CLI commands to be run at the same time or same interval. One or more policy lists are then scheduled to run after a specified interval of time, at a specified calendar date and time, or upon system startup. Each scheduled occurrence can be set to run either once only or on a recurring basis.

Examples of Letter Code Mappings for Active Template

Example 1

In this example, in response to a DHCP IP address request sent by the DHCP client, the DHCP server sends an Option 43 message such as **3P2N;B10.10.10.1** to the DHCP client. The DHCP client forwards the Option 43 message to the Cisco Networking Service. The Cisco Networking Service verifies if the Option 43 message is allowed to process. Option 43 messages are allowed to process by the Cisco Networking Service if the cns dhcp command is enabled on the Cisco Networking Service.

The ASCII data shown in this Option 43 message consists of types and values as shown in the following table.

Table 2   *Types and Values for Sample Option 43 Command*

Type	Value
3	P2N;B10.10.10.1

This message is decoded into tokens using the above arguments list. The parameters mapped for the 3P2N;B10.10.10.1 message using the arguments list are as follows:

P--Active template code

2--Version number of the Active template

N--Debug option which is OFF

;--Delimiter before the arglist

B10.10.10.1--CE address parameter name value pair

The Cisco Networking Service constructs the following commands and sends to the remote management server to request the initial configuration file. A timer is set for five minutes.

```
Router(config)# cns event 10.10.10.1
Router(config)# cns config partial 10.10.10.1 inventory
Router(config)# cns exec
Router(config)# cns trusted-server all-agents 10.10.10.1
```

The initial configuration file that is downloaded is checked. If the file download is successful, the process is complete.

Example 2

In this example, in response to a DHCP IP address request sent by the DHCP client, the DHCP server sends an Option 43 message such as **3P1N;A1881-ap;B10.10.10.1;J11024** to the DHCP client. The DHCP client forwards the Option 43 message to the Cisco Networking Service. The Cisco Networking Service verifies if the Option 43 message is allowed to process. Option 43 messages are allowed to process by the Cisco Networking Service if the **cns dhcp** command is enabled on the Cisco Networking Service.

The ASCII data shown in this Option 43 message consists of types and values shown in the following table.

Table 3   *Types and Values for Sample Option 43 Command*

Type	Value
3	P1N;A1881-ap;B10.10.10.1;J11024

This message is decoded into tokens using the above arguments list. The parameters mapped for the 3P1N;A1881-ap;B10.10.10.1;C11024 message using the arguments list are as follows:

P--Active template code

1--Version number of the Active template

N--Debug option which is OFF

;--Delimiter before the arglist

881-ap-Active template string values

B10.10.10.1--CE address parameter name value pair

J11024--Config server port value

How to Configure Cisco Networking Services

Deploying the Cisco Networking Services Router

Perform this task to manually install an initial Cisco Networking Services configuration.

Your remote router arrives from the factory with a bootstrap configuration. Upon initial power-on, the router automatically pulls a full initial configuration from the Cisco Networking Services configuration engine, although you can optionally arrange for this manually as well. After initial configuration, you can optionally arrange for periodic incremental (partial) configurations for synchronization purposes.

Initial Cisco Networking Services Configuration

Initial configuration of the remote router occurs automatically when the router is initialized on the network. Optionally, you can perform this configuration manually.

Cisco Networking Services assigns the remote router a unique IP address or hostname. After resolving the IP address (using Serial Line Address Resolution Protocol (SLARP), ATM Inverse ARP (ATM InARP), or PPP protocols), the system optionally uses Domain Name System (DNS) reverse lookup to assign a

hostname to the router and invokes the Cisco Networking Services agent to download the initial configuration from the Cisco Networking Services configuration engine.

Incremental Configuration

Incremental or partial configuration allows the remote router to be incrementally configured after its initial configuration. You must perform these configurations manually through the Cisco Networking Services configuration engine. The registrar allows you to change the configuration templates, edit parameters, and submit the new configuration to the router without a software or hardware restart.

Before you can configure an incremental configuration, Cisco Networking Services must be operational and the required Cisco Networking Services agents configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns template connect** *name*
4. **cli** *config-text*
5. Repeat Step 4 to add all required CLI commands.
6. **exit**
7. **cns connect** *name* [**retry-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]
8. Do one of the following:

    • **discover** {**line** *line-type* | **controller** *controller-type* | **interface** [*interface-type*]}
    •
    • **template** *name*
9. **exit**
10. **cns config initial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**]
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cns template connect** *name* **Example:** Router(config)# cns template connect template 1	Enters Cisco Networking Services template connect configuration mode and defines the name of a Cisco Networking Services connect template.
Step 4	**cli** *config-text* **Example:** Router(config-templ-conn)# cli encapsulation ppp	Specifies commands to configure the interface.
Step 5	Repeat Step 4 to add all required CLI commands. **Example:** Router(config-templ-conn)# cli ip directed-broadcast	Repeat Step 4 to add other CLI commands to configure the interface or to configure the modem lines.
Step 6	**exit** **Example:** Router(config-templ-conn)# exit	Exits Cisco Networking Services template connect configuration mode and completes the configuration of a Cisco Networking Services connect template. **Note** Entering the **exit** command is required. This requirement was implemented to prevent accidentally entering a command without the **cli** command.
Step 7	**cns connect** *name* [**retry-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*] **Example:** Router(config)# cns connect profile-1 retry-interval 15 timeout 90	Enters Cisco Networking Services connect configuration mode and defines the parameters of a Cisco Networking Services connect profile for connecting to the Cisco Networking Services configuration engine.

	Command or Action	Purpose
Step 8	Do one of the following: • **discover** {**line** *line-type* | **controller** *controller-type* | **interface** [*interface-type*]} • • **template** *name* **Example:** Router(config-cns-conn)# discover interface serial **Example:** **Example:** Router(config-cns-conn)# template template-1	(Optional) Configures a generic bootstrap configuration. • **discover** --Defines the interface parameters within a Cisco Networking Services connect profile for connecting to the Cisco Networking Services configuration engine. or • **template** --Specifies a list of Cisco Networking Services connect templates within a Cisco Networking Services connect profile to be applied to a router's configuration.
Step 9	**exit** **Example:** Router(config-cns-conn)# exit	Exits Cisco Networking Services connect configuration mode and returns to global configuration mode.
Step 10	**cns config initial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**] **Example:** Router(config)# cns config initial 10.1.1.1 no-persist	Starts the Cisco Networking Services configuration agent, connects to the Cisco Networking Services configuration engine, and initiates an initial configuration. You can use this command only before the system boots for the first time. **Note** The optional **encrypt** keyword is available only in images that support Secure Socket Layer (SSL). **Caution** If you write the new configuration to NVRAM by omitting the **no-persist**keyword, the original bootstrap configuration is overwritten.
Step 11	**exit** **Example:** Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Cisco Networking Services Event and EXEC Agents

Perform this task to enable and configure the Cisco Networking Services Event and EXEC agents.

Cisco Networking Services Event Agent Parameters

The Cisco Networking Services event agent command--**cns event**--has several parameters that can be configured. The **failover-time** keyword is useful if you have a backup Cisco Networking Services event gateway configured. If the Cisco Networking Services event agent is trying to connect to the gateway and it discovers that the route to the backup gateway is available before the route to the primary gateway, the *seconds* argument specifies how long the Cisco Networking Services event agent will continue to search for a route to the primary gateway before attempting to link to the backup gateway.

Unless you are using a bandwidth-constrained link, you should set a keepalive timeout and retry count. Doing so allows the management network to recover gracefully should a Cisco IE2100 configuration engine ever fail. Without the keepalive data, such a failure requires manual intervention on every device. The *seconds* value multiplied by the *retry-count* value determines the length of idle time before the Cisco Networking Services event agent will disconnect and attempt to reconnect to the gateway. We recommend a minimum *retry-count* value of 2.

If the optional **source** keyword is used, the source IP address might be a secondary IP address of a specific interface to allow a management network to run on top of a production network.

Note   Although other Cisco Networking Services agents may be configured, no other Cisco Networking Services agents are operational until the **cns event** command is entered because the Cisco Networking Services event agent provides a transport connection to the Cisco Networking Services event bus for all other Cisco Networking Services agents.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *interface name*] [**inventory**]
4. **logging cns-events** [*severity-level*]
5. **cns exec** [*host-name* | *ip-address*] [**encrypt**[enc-*port-number*]] [*port-number*] [**source** *ip-address*]
6. **cns event** {*hostname* | *ip-address*} [**encrypt**] [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *ip-address*][**clock-timeout** *time*] [**reconnect** *time*]
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router enable`	Enables privileged EXEC mode. - Enter your password if prompted.

Command or Action	Purpose
Step 2 **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3 **cns config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *interface name*] [**inventory**] **Example:** `Router(config)# cns config partial 172.28.129.22 80`	(Optional) Starts the Cisco Networking Services configuration agent, which provides Cisco Networking Services configuration services to Cisco IOS clients, and initiates an incremental (partial) configuration. • Use the optional *port-number* argument to specify the port number for the configuration server. The default is 80. • Use the optional **source** keyword and *ip-address* argument to specify the use of an IP address as the source for Cisco Networking Services configuration agent communications. • Use the optional **inventory** keyword to send an inventory of the line cards and modules in the router to the Cisco Networking Services configuration engine as part of the HTTP request. **Note** The optional **encrypt** keyword is available only in images that support SSL.
Step 4 **logging cns-events** [*severity-level*] **Example:** `Router(config)# logging cns-events 2`	(Optional) Enables XML-formatted system event message logging to be sent through the Cisco Networking Services event bus. • Use the optional *severity-level* argument to specify the number or name of the desired severity level at which messages should be logged. The default is level 7 (debugging).
Step 5 **cns exec** [*host-name* | *ip-address*] [**encrypt**[enc-*port-number*]] [*port-number*] [**source** *ip-address*] **Example:** `Router(config)# cns exec 10.1.2.3 93 source 172.17.2.2`	(Optional) Enables and configures the Cisco Networking Services EXEC agent, which provides Cisco Networking Services EXEC services to Cisco IOS clients. • Use the optional *port-number* argument to specify the port number for the EXEC server. The default is 80. • Use the optional **source** keyword and *ip-address* argument to specify the use of an IP address as the source for Cisco Networking Services EXEC agent communications. **Note** The optional **encrypt keyword** is available only in images that support SSL.

	Command or Action	Purpose
Step 6	**cns event** {*hostname* | *ip-address*} [**encrypt**] [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *ip-address*][**clock-timeout** *time*] [**reconnect** *time*] **Example:** Router(config)# cns event 172.28.129.22 source 172.22.2.1	Configures the Cisco Networking Services event gateway, which provides Cisco Networking Services event services to Cisco IOS clients. • The optional **encrypt**keyword is available only in images that support SSL. • Use the optional *port-number* argument to specify the port number for the event server. The default is 11011 with no encryption and 11012 with encryption. • Use the optional **backup** keyword to indicate that this is the backup gateway. Before configuring a backup gateway, ensure that a primary gateway is configured. • Use the optional **failover-time** keyword and *seconds* argument to specify a time interval in seconds to wait for the primary gateway route after the route to the backup gateway is established. • Use the optional **keepalive** keyword with the *seconds* and *retry-count* arguments to specify the keepalive timeout in seconds and the retry count. • Use the optional **source** keyword and *ip-address* argument to specify the use of an IP address as the source for Cisco Networking Services event agent communications. • Use the optional **clock-timeout** keyword to specify the maximum time, in minutes, that the Cisco Networking Services event agent will wait for the clock to be set for transports (such as SSL) that require an accurate clock. • Use the optional **reconnect** keyword to specify the configurable upper limit of the maximum retry timeout. **Note** Until the **cns event** command is entered, no transport connections to the Cisco Networking Services event bus are made and therefore no other Cisco Networking Services agents are operational.
Step 7	**exit** **Example:** Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

- Use the **show cns event connections**command to check that the Cisco Networking Services event agent is connected to the Cisco Networking Services event gateway.
- Use the **show cns event subject**command to check that the image agent subject names are registered. Subject names for the Cisco Networking Services image agent begin with cisco.mgmt.cns.image.

Configuring the Cisco Networking Services Image Agent

Perform this task to configure Cisco Networking Services image agent parameters using CLI commands.

Cisco Networking Services Image Agent ID

Cisco Networking Services uses a unique identifier to identify an image agent associated with that Cisco IOS device. Using the same process as Cisco Networking Services event and configuration agents, the configuration of the **cns id** command determines whether an IP address or MAC address of a specified interface, the hardware serial hardware number of the device, an arbitrary text string, or the hostname of the device is used as the image ID. By default, the system uses the hostname of the device.

The Cisco Networking Services image ID is sent in the content of the messages sent by the image agent and allows an application to know the unique image ID of the Cisco IOS device that generated the message. A password can be configured and associated with the image ID in the image agent messages.

- To configure the Cisco Networking Services image agent to use HTTP or HTTP over SSL (HTTPS) to communicate with an image server, you need to know the URL for the image server and the URL to which status messages can be sent.
- If you are using HTTPS to communicate with the image server, you must set up security certificates to allow the server to be authenticated by the image agent when the connection is established.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **cns id** *type number* {**ipaddress**| **mac-address**} [**event**| **image**]
   -
   - **cns id** {**hardware-serial**| **hostname**| **string** *text*} [**event**| **image**]
4. **cns password** *password*
5. **cns image** [**server** *server-url*[**status** *status-url*]]
6. **cns image password** *image-password*
7. **cns image retry** *seconds*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	Do one of the following:
	
	• **cns id** *type number* {**ipaddress**| **mac-address**} [**event**| **image**]
	
	•
	
	• **cns id** {**hardware-serial**| **hostname**| **string** *text*} [**event**| **image**]
	
	Example:
	
	`Router(config)# cns id fastethernet 0/1 ipaddress image`
	
	Example:
	
	Example:
	
	`Router(config)# cns id hardware-serial image`
		Specifies a unique Cisco Networking Services ID and interface type and number from which to retrieve the unique ID.
		or
		Specifies a unique Cisco Networking Services ID assigned from the hardware serial number, device hostname, or an arbitrary text string.
		
		The following information applies to either version of the syntax.
		
		• Use the **event** keyword to specify an event agent ID.
		• Use the **image** keyword to specify an image agent ID.
		• If no keywords are used, the configuration agent ID is configured.

Step 4	**cns password** *password* **Example:** `Router(config)# cns password password1`	Specifies a password for the Cisco Networking Services ID. You must configure the Cisco Networking Services password the first time a router is deployed, and the Cisco Networking Services password must be the same as the bootstrap password set on the Configuration Engine (CE).
Step 5	**cns image** [**server** *server-url*[**status** *status-url*]] **Example:** `Router(config)# cns image server https://10.21.2.3/cns/imgsvr status https://10.21.2.3/cns/status/`	Enables Cisco Networking Services image agent services and specifies the URL of the image distribution server. • Use the optional **status** keyword and *status-url* argument to specify the URL of a web server to which error messages are written. • If the **status** keyword and *status-url* argument are not specified, status messages are sent as events on the Cisco Networking Services Event Bus. To view the status messages on the Cisco Networking Services Event Bus, the Cisco Networking Services event agent must be configured.
Step 6	**cns image password** *image-password* **Example:** `Router(config)# cns image password abctext`	(Optional) Specifies a password for Cisco Networking Services image agent services. • If a password is configured, the password is included with the image ID in Cisco Networking Services image agent messages sent out by the image agent. The receiver of these messages can use this information to authenticate the sending device.

	Command or Action	Purpose
Step 7	**cns image retry** *seconds* **Example:** `Router(config)# cns image retry 240`	(Optional) Specifies an image upgrade retry interval in seconds. • The default interval is 60 seconds.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns the router to privileged EXEC mode.

What to Do Next

Proceed to the section to connect to the web server and download an image.

If any of the commands in the task fail, proceed to the section to try to determine the problem.

Retrieving a Cisco Networking Services Image from a Server

Perform this task to poll the image distribution server using HTTP or HTTPS.

This task assumes that you have already configured the Cisco Networking Services image agent using the tasks in the section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns image retrieve** [**server** *server-url*[**status** *status-url*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**cns image retrieve** [**server** *server-url*[**status** *status-url*]] **Example:** Router(config)# cns image retrieve server https://10.19.2.3/imgsvr/ status https://10.19.2.3/imgsvr/ status/	Contacts a Cisco Cisco Networking Services image distribution server and downloads a new image if a new image exists. • Use the optional **status** keyword and *status-url* argument to specify the URL of a web server to which status messages are written. • If the **server** and **status** keywords are not specified, the server and status URLs configured with the **cns image** command are used. **Note** We recommend using the **cns trusted-server** command to specify the host part of the server or status URL as a trusted server.

-

Troubleshooting Tips

- If the web server appears to be down, use the **ping** command to check connectivity.
- If using HTTP, use the **show ip http client all** command to display information about HTTP clients and connections.

Retrieving a Cisco Networking Services Configuration from a Server

Use this task to request the configuration of a device from a configuration server. Use the **cns trusted-server** command to specify which configuration server can be used (trusted).

This task assumes that you have specified a trusted server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns config retrieve** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**overwrite-startup**] [**retry** *retries* **interval** *seconds*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**cns config retrieve** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**overwrite-startup**] [**retry** *retries* **interval** *seconds*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**] **Example:** Router(config)# cns config retrieve server1 retry 5 interval 45	Allows the router to retrieve configuration data from a web server. • The **retry** keyword is a number in the range 1 to 100, and will prompt for an **interval** in the range 1 to 3600 seconds.

Troubleshooting Tips

If you need to stop the retrieval process, enter the Ctrl+Shift+6 key sequence.

Configuring Command Scheduler Policy Lists and Occurrences

Perform this task to set up Command Scheduler policy lists of EXEC Cisco Networking Services commands and configure a Command Scheduler occurrence to specify the time or interval after which the Cisco Networking Services commands will run.

Command Scheduler Policy Lists

Policy lists consist of one or more lines of fully-qualified EXEC CLI commands. All commands in a policy list are executed when the policy list is run by Command Scheduler using the **kron occurrence** command. Use separate policy lists for CLI commands that are run at different times. No editor function is available, and the policy list is run in the order in which it was configured. To delete an entry, use the **no** form of the

cli command followed by the appropriate EXEC command. If an existing policy list name is used, new entries are added to the end of the policy list. To view entries in a policy list, use the **show running-config** command. If a policy list is scheduled to run only once, it will not be displayed by the **show running-config** command after it has run.

Policy lists can be configured after the policy list has been scheduled, but each policy list must be configured before it is scheduled to run.

Command Scheduler Occurrences

An occurrence for Command Scheduler is defined as a scheduled event. Policy lists are configured to run after a specified interval of time, at a specified calendar date and time, or upon system startup. Policy lists can be run once, as a one-time event, or as recurring events over time.

Command Scheduler occurrences can be scheduled before the associated policy list has been configured, but a warning will advise you to configure the policy list before it is scheduled to run.

The clock time must be set on the routing device before a Command Scheduler occurrence is scheduled to run. If the clock time is not set, a warning message will appear on the console screen after the **kron occurrence** command has been entered. Use the **clock** command or Network Time Protocol (NTP) to set the clock time.

The EXEC CLI to be run by Command Scheduler must be tested on the routing device to determine if it will run without generating a prompt or allowing execution interruption by keystrokes. Initial testing is important because Command Scheduler will delete the entire policy list if any CLI syntax fails. Removing the policy list ensures that any CLI dependencies will not generate more errors.

If you use the **conditional** keyword with the **kron policy-list** command, execution of the commands will stop when an error is encountered.

Note

- No more than 31 policy lists can be scheduled to run at the same time.
- If a one-time occurrence is scheduled, the occurrence will not be displayed by the **show running-config** command after the occurrence has run.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **kron policy-list** *list-name* [**conditional**]
4. **cli** *command*
5. **exit**
6. **kron occurrence** *occurrence-name* [**user** *username*] {**in**[[*numdays:*]*numhours:*]*nummin*| **at** *hours:min*[[*month*] *day-of-month*] [*day-of-week*]} {**oneshot**| **recurring**| **system-startup**}
7. **policy-list** *list-name*
8. **exit**
9. **show kron schedule**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**kron policy-list** *list-name* [**conditional**] **Example:** `Router(config)# kron policy-list cns-weekly`	Specifies a name for a new or existing Command Scheduler policy list and enters kron-policy configuration mode. • If the *list-name* is new, a new policy list structure is created. • If the *list-name* exists, the existing policy list structure is accessed. The policy list is run in configured order with no editor function. • If the optional **conditional** keyword is used, execution of the commands stops when an error is encountered.
Step 4	**cli** *command* **Example:** `Router(config-kron-policy)# cli cns image retrieve server https://10.19.2.3/cnsweek/ status https://10.19.2.3/cnsstatus/week/`	Specifies the fully-qualified EXEC command and associated syntax to be added as an entry in the specified Command Scheduler policy list. • Each entry is added to the policy list in the order in which it is configured. • Repeat this step to add other EXEC CLI commands to a policy list to be executed at the same time or interval. **Note** EXEC commands that generate a prompt or can be terminated using keystrokes will cause an error.
Step 5	**exit** **Example:** `Router(config-kron-policy)# exit`	Exits kron-policy configuration mode and returns the router to global configuration mode.

	Command or Action	Purpose
Step 6	**kron occurrence** *occurrence-name* [**user** *username*] {**in**[[*numdays:*]*numhours:*]*nummin*| **at** *hours:min*[[*month*] *day-of-month*] [*day-of-week*]} {**oneshot**| **recurring**| **system-startup**} **Example:** Router(config)# kron occurrence may user sales at 6:30 may 20 oneshot	Specifies a name and schedule for a new or existing Command Scheduler occurrence and enters kron-occurrence configuration mode. • Use the **in** keyword to specify a delta time interval with a timer that starts when this command is configured. • Use the **at** keyword to specify a calendar date and time. • Choose either the **oneshot** or **recurring** keyword to schedule Command Scheduler occurrence once or repeatedly. Add the optional **system-startup** keyword for the occurrence to be at system startup.
Step 7	**policy-list** *list-name* **Example:** Router(config-kron-occurrence)# policy-list sales-may	Specifies a Command Scheduler policy list. • Each entry is added to the occurrence list in the order in which it is configured. **Note** If the CLI commands in a policy list generate a prompt or can be terminated using keystrokes, an error will be generated and the policy list will be deleted.
Step 8	**exit** **Example:** Router(config-kron-occurrence)# exit	Exits kron-occurrence configuration mode and returns the router to global configuration mode. • Repeat this step to exit global configuration mode.
Step 9	**show kron schedule** **Example:** Router# show kron schedule	(Optional) Displays the status and schedule information of Command Scheduler occurrences.

Examples

In the following example, output information is displayed about the status and schedule of all configured Command Scheduler occurrences:

```
Router# show kron schedule
Kron Occurrence Schedule
cns-weekly inactive, will run again in 7 days 01:02:33
may inactive, will run once in 32 days 20:43:31 at 6:30 on May 20
```

Troubleshooting Tips

Use the **debug kron** command in privileged EXEC mode to troubleshoot Command Scheduler command operations. Use any debugging command with caution because the volume of output generated can slow or stop the router operations.

Configuring Advanced Cisco Networking Services Features

Perform this task to configure more advanced Cisco Networking Services features. After the Cisco Networking Services agents are operational, you can configure some other features. You can enable the Cisco Networking Services inventory agent--that is, send an inventory of the router's line cards and modules to the Cisco Networking Services configuration engine--and enter Cisco Networking Services inventory mode.

Some other advanced features allow you to use the Software Developer's Toolkit (SDK) to specify how Cisco Networking Services notifications should be sent or how to access MIB information. Two encapsulation methods can be used: either nongranular (SNMP) encapsulation or granular (XML) encapsulation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns mib-access encapsulation** {**snmp** | **xml**[**size** *bytes*]}
4. **cns notifications encapsulation** {**snmp** | **xml**}
5. **cns inventory**
6. **transport event**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cns mib-access encapsulation** {**snmp** | **xml**[**size** *bytes*]} **Example:** `Router(config)# cns mib-access encapsulation snmp`	(Optional) Specifies the type of encapsulation to use when accessing MIB information. • Use the **snmp** keyword to specify that nongranular encapsulation is used to access MIB information. • Use the **xml** keyword to specify that granular encapsulation is used to access MIB information. The optional **size** keyword specifies the maximum size for response events, in bytes. The default byte value is 3072.

	Command or Action	Purpose
Step 4	**cns notifications encapsulation** {**snmp** | **xml**} **Example:** `Router(config)# cns notifications encapsulation xml`	(Optional) Specifies the type of encapsulation to use when sending Cisco Networking Services notifications. • Use the **snmp** keyword to specify that nongranular encapsulation is used when Cisco Networking Services notifications are sent. • Use the **xml** keyword to specify that granular encapsulation is used when Cisco Networking Services notifications are sent.
Step 5	**cns inventory** **Example:** `Router(config)# cns inventory`	Enables the Cisco Networking Services inventory agent and enters Cisco Networking Services inventory mode. • An inventory of the router's line cards and modules is sent to the Cisco Networking Services configuration engine.
Step 6	**transport event** **Example:** `Router(cns-inv)# transport event`	Specifies that inventory requests are sent out with each Cisco Networking Services inventory agent message.
Step 7	**exit** **Example:** `Router(cns-inv)# exit`	Exits Cisco Networking Services inventory mode and returns to global configuration mode. • Repeat this command to return to privileged EXEC mode.

Troubleshooting Cisco Networking Services Agents

This section explains how to troubleshoot Cisco Networking Services agent issues.

The **show** commands created for the Cisco Networking Services image agent display information that is reset to zero after a successful reload of the device. Depending on the configuration of the image distribution process, the new image may not reload immediately. When a reload is not immediate or has failed, use the Cisco Networking Services image agent **show** commands to determine whether the image agent has connected to the image distribution server over HTTP or whether the image agent is receiving events from an application over the Cisco Networking Services Event Bus.

SUMMARY STEPS

1. **enable**
2. **show cns image status**
3. **clear cns image status**
4. **show cns image connections**
5. **show cns image inventory**
6. **debug cns image** [**agent**| **all**| **connection**| **error**]
7. **show cns event connections**
8. **show cns event subject** [*name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cns image status** **Example:** Router# show cns image status	(Optional) Displays information about the Cisco Networking Services image agent status.
Step 3	**clear cns image status** **Example:** Router# clear cns image status	(Optional) Clears Cisco Networking Services image agent status statistics.
Step 4	**show cns image connections** **Example:** Router# show cns image connections	(Optional) Displays information about Cisco Networking Services image management server HTTP or HTTPS connections.
Step 5	**show cns image inventory** **Example:** Router# show cns image inventory	(Optional) Displays inventory information about the Cisco Networking Services image agent. • This command displays a dump of XML that would be sent out in response to an image agent inventory request message. The XML output can be used to determine the information requested by an application.

	Command or Action	Purpose
Step 6	**debug cns image** [**agent**| **all**| **connection**| **error**] **Example:** `Router# debug cns image all`	(Optional) Displays debugging messages for Cisco Networking Services image agent services.
Step 7	**show cns event connections** **Example:** `Router# show cns event connections`	(Optional) Displays the status of the Cisco Networking Services event agent connection--such as whether it is connecting to the gateway, connected, or active--and to display the gateway used by the event agent and its IP address and port number.
Step 8	**show cns event subject** [*name*] **Example:** `Router# show cns event subject subject1`	(Optional) Displays a list of subjects of the Cisco Networking Services event agent that are subscribed to by applications.

-

Examples

Sample Output for the show cns image status Command

In the following example, status information about the Cisco Networking Services image agent is displayed using the **show cns image status**privileged EXEC command:

```
Router# show cns image status
Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS
Last successful upgrade ended at 11:56:04.000 UTC Mon May 6 2003
Last failed upgrade ended at 06:32:15.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
 messages received: 12
 receive errors: 5
Transmit Status
  TX Attempts:4
    Successes:3         Failures 2
```

Sample Output for the show cns image connections Command

In the following example, information about the status of the Cisco Networking Services image management HTTP connections is displayed using the **show cns image connections**privileged EXEC command:

```
show cns image connections

CNS Image Agent:  HTTP connections
```

```
Connection attempts 1
never connected:0   Abrupt disconnect:0
Last successful connection at 11:45:02.000 UTC Mon May 6 2003
```

Sample Output for the show cns image inventory Command

In the following example, information about the Cisco Networking Services image agent inventory is displayed using the **show cns image inventory**privileged EXEC command:

```
show cns image inventory

Inventory Report
imageInventoryReport deviceName imageID Router /imageID hostName Router /ho
IOS (tm) C2600 Software (C2600-I-M), Experimental Version 12.3(20030414:081500)]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Apr-03 02:03 by engineer /versionString imageFile tftp://10.25.2.1.
```

Sample Output for the debug cns image Command

In the following example, debugging messages for all Cisco Networking Services image agent services are displayed using the **debug cns image**privileged EXEC command. The Cisco Networking Services image agent in this example is connecting to an image server over HTTP. After connecting, the image server asks for an inventory of the Cisco IOS device.

```
Router# debug cns image all

All cns image debug flags are on
Router# cns image retrieve

May  7 06:11:42.175: CNS Image Agent: set EXEC lock
May  7 06:11:42.175: CNS Image Agent: received message from EXEC
May  7 06:11:42.175: CNS Image Agent: set session lock 1
May  7 06:11:42.175: CNS Image Agent: attempting to send to destination(http://
10.1.36.8:8080/imgsrv/xgate):
?xml version="1.0" encoding="UTF-8"? cnsMessageversion="1.0" senderCredentials userName
dvlpr-7200-6 /userName /senderCredentials
messageID dvlpr-7200-6_2 /messageID sessionControl imageSessionStart version="1.0"
initiatorInfotrigger EXEC/trigger initiatorCredentials userName dvlpr-7200-6/userName
/initiatorCredentials /initiatorInfo /imageSessionStart /sessionControl /cnsMessage
May  7 06:11:42.175: CNS Image Agent: clear EXEC lock
May  7 06:11:42.175: CNS Image Agent: HTTP message sent url:http://10.1.36.8:8080/imgsrv/
xgate
May  7 06:11:42.191: CNS Image Agent: response data alloc 4096 bytes
May  7 06:11:42.191: CNS Image Agent: HTTP req data free
May  7 06:11:42.191: CNS Image Agent: response data freed
May  7 06:11:42.191: CNS Image Agent: receive message
?xml version="1.0" encoding="UTF-8"?
cnsMessage version="1.0"
senderCredentials
userName myImageServer.cisco.com/userName
passWord R0lGODlhcgGSALMAAAQCAEMmCZtuMFQxDS8b/passWord
/senderCredentials
messageID dvlpr-c2600-2-476456/messageID
request
replyTo
serverReply http://10.1.36.8:8080/imgsrv/xgate /serverReply
/replyTo
imageInventory
inventoryItemList
all/
/inventoryItemList
/imageInventory
/request
/cnsMessage
```

Sample Output for the show cns event Commands

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event connections

The currently configured primary event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
Event-Id is Internal test1
Keepalive setting:
        none.
Connection status:
        Connection Established.
The currently configured backup event gateway:
        none.
The currently connected event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
```

The following sample displays a list of subjects of the Cisco Networking Services event agent that are subscribed to by applications:

```
Router# show cns event subject

The list of subjects subscribed by applications.
   cisco.cns.mibaccess:request
   cisco.cns.config.load
   cisco.cns.config.reboot
   cisco.cns.exec.cmd
```

Configuration Examples for Cisco Networking Services

Deploying the Cisco Networking Services Router Example

The following example shows an initial configuration on a remote router. The hostname of the remote router is the unique ID. The Cisco Networking Services configuration engine IP address is 172.28.129.22.

```
cns template connect template1
 cli ip address negotiated
 cli encapsulation ppp
 cli ip directed-broadcast
 cli no keepalive
 cli no shutdown
 exit
cns connect host1 retry-interval 30 retries 3
exit
 hostname RemoteRouter
 ip route 172.28.129.22 255.255.255.0 10.11.11.1
 cns id Ethernet 0 ipaddress
 cns config initial 10.1.1.1 no-persist
 exit
```

Configuring a Partial Configuration Example

Incremental or partial configuration allows the remote router to be incrementally configured after its initial configuration. You must perform these configurations manually through the Cisco Networking Services configuration engine. The registrar allows you to change the configuration templates, edit parameters, and submit the new configuration to the router without a software or hardware restart.

The following example shows incremental (partial) configuration on a remote router. The Cisco Networking Services configuration engine IP address is 172.28.129.22, and the port number is 80.

```
cns config partial 172.28.129.22 80
```

Enabling and Configuring Cisco Networking Services Agents Example

The following example shows various Cisco Networking Services agents being enabled and configured starting with the configuration agent being enabled with the **cns config partial** command to configure an incremental (partial) configuration on a remote router. The Cisco Networking Services configuration engine IP address is 172.28.129.22, and the port number is 80. The Cisco Networking Services exec agent is enabled with an IP address of 172.28.129.23, and the Cisco Networking Services event agent is enabled with an IP address of 172.28.129.24. Until the Cisco Networking Services event agent is enabled, no other Cisco Networking Services agents are operational.

```
cns config partial 172.28.129.22 80
cns exec 172.28.129.23 source 172.22.2.2
cns event 172.28.129.24 source 172.22.2.1
exit
```

In the following example, the Cisco Networking Services image agent parameters are configured using the CLI. An image ID is specified to use the IP address of the FastEthernet interface 0/1, a password is configured for the Cisco Networking Services image agent services, the Cisco Networking Services image upgrade retry interval is set to four minutes, and image management and status servers are configured.

```
cns id FastEthernet0/1 ipaddress image
cns image retry 240
cns image password abctext
cns image server https://10.21.2.3/cns/imgsvr status https://10.21.2.3/cns/status/
```

In the following example, the Cisco Networking Services image agent is configured to use the Cisco Networking Services Event Bus. An image ID is specified as the hardware serial number of the networking device, the Cisco Networking Services event agent is enabled with a number of parameters, and the Cisco Networking Services image agent is enabled without any keywords or options. The Cisco Networking Services image agent will listen for events on the Cisco Networking Services Event Bus.

```
cns id hardware-serial image
cns event 10.21.9.7 11011 keepalive 240 120 failover-time 5
cns image
cns image password abctext
```

Command Scheduler Policy Lists and Occurrences Examples

In the following example, a Command Scheduler policy named cns-weekly is configured to run two sets of EXEC CLI involving Cisco Networking Services commands. The policy is then scheduled with two other policies to run every seven days, one hour and thirty minutes.

```
kron policy-list cns-weekly
```

```
cli cns image retrieve server http://10.19.2.3/week/ status http://10.19.2.5/status/week/
cli cns config retrieve page /testconfig/config.asp no-persist
exit
kron occurrence week in 7:1:30 recurring
policy-list cns-weekly
policy-list itd-weekly
policy-list mkt-weekly
```

In the following example, a Command Scheduler policy named sales-may is configured to run a Cisco Networking Services command to retrieve a specified image from a remote server. The policy is then scheduled to run only once on May 20, at 6:30 a.m.

```
kron policy-list sales-may
cli cns image retrieve server 10.19.2.3 status 10.19.2.3
exit
kron occurrence may at 6:30 May 20 oneshot
policy-list sales-may
```

In the following example, a Command Scheduler policy named image-sunday is configured to run a Cisco Networking Services command to retrieve a specified image from a remote server. The policy is then scheduled to run every Sunday at 7:30 a.m.

```
kron policy-list image-sunday
cli cns image retrieve server 10.19.2.3 status 10.19.2.3
exit
kron occurrence sunday user sales at 7:30 sunday recurring
policy-list image-sunday
```

In the following example, a Command Scheduler policy named file-retrieval is configured to run a Cisco Networking Services command to retrieve a specific file from a remote server. The policy is then scheduled to run on system startup.

```
kron policy-list file-retrieval
cli cns image retrieve server 10.19.2.3 status 10.19.2.3
exit
kron occurrence system-startup
policy-list file-retrieval
```

Retrieving a Cisco Networking Services Image from a Server Example

In the following example, the Cisco Networking Services image agent polls a file server using the **cns image retrieve** command. Assuming that the Cisco Networking Services image agent is already enabled, the file server and status server paths specified here will overwrite any existing image agent server and status configuration. The new file server will be polled and a new image, if it exists, will be downloaded to the networking device.

```
cns image retrieve server https://10.19.2.3/cns/ status https://10.19.2.3/cnsstatus/
```

Retrieving a Cisco Networking Services Configuration from a Server Examples

Retrieving Configuration Data from the Cisco Networking Services Trusted Server

The following example shows how to request a configuration from a trusted server at 10.1.1.1:

```
cns trusted-server all 10.1.1.1
exit
cns config retrieve 10.1.1.1
```

The following example shows how to request a configuration from a trusted server at 10.1.1.1 and to configure a Cisco Networking Services configuration retrieve interval using the **cns config retrieve** command:

```
cns trusted-server all 10.1.1.1
exit
cns config retrieve 10.1.1.1 retry 50 interval 1500
CNS Config Retrieve Attempt 1 out of 50 is in progress
Next cns config retrieve retry is in 1499 seconds (Ctrl-Shft-6 to abort this command).
..
00:26:40: %CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED:10.1.1.1 -Process= "CNS config
retv", ipl= 0, pid= 43
```

00:26:40: %CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED -Process= "CNS config retv", ipl= 0, pid= 43......

```
cns config retrieve 10.1.1.1
```

Applying the Retrieved Data to the Running Configuration File

The following example shows how to check and apply configuration data retrieved from the server to running configuration file only. The Cisco Networking Services Configuration Agent will attempt to retrieve configuration data at 30-second intervals until the attempt is successful, or is unsuccessful five times in these attempts.

```
cns config retrieve 10.1.1.1 syntax-check no-persist retry 5 interval 30
```

Overwriting the Startup Configuration File with the Retrieved Data

The following example shows how to overwrite the startup configuration file with the configuration data retrieved from the server. The configuration data will not be applied to the running configuration.

```
cns config retrieve 10.1.1.1 syntax-check no-persist retry 5 interval 30
cns config retrieve 10.1.1.1 overwrite-startup
```

Additional References

The following sections provide references related to the Cisco Networking Services feature.

Related Documents

Related Topic	Document Title
Cisco Networking Services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*
Cisco Networking Services Configuration Engine	*Cisco Intelligence Engine 2100 Configuration Registrar Manual , Release 1.1 or later*
	Cisco Cisco Networking Services Configuration Engine Administrator's Guide

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
The CNS Flow-Through Provisioning feature provides two mechanisms for accessing MIBs: a nongranular mechanism using SNMP encapsulation and a granular mechanism using XML encapsulation. These mechanisms enable you to access the MIBS currently available in the remote router. The MIBS currently available depend on the router platform and Cisco IOS release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Networking Services

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4   *Feature Information for Cisco Networking Services*

Feature Name	Releases	Feature Information
Cisco Networking Services	12.2(25)S 12.2(33) SRA 12.2(33)SB 12.2(33)SXI	The Cisco Networking Services feature is a collection of services that can provide remote event-driven configuring of Cisco IOS networking devices and remote execution of some CLI commands. The following commands were introduced or modified by this feature: **clear cns config stats**, **clear cns counters**, **clear cns event stats**, **cli (cns)**, **cns config cancel**, **cns config initial**, **cns config notify**, **cns config partial**, **cns config retrieve**, **cns connect**, **cns event**, **cns exec**, **cns id**, **cns template connect**, **cns trusted-server**, **debug cns config**, **debug cns exec**, **debug cns xml-parser**, **logging cns-events**, **show cns config stats**, **show cns event connections**, **show cns event stats**, **show cns event subject**.

Feature Name	Releases	Feature Information
Cisco Networking Services Config Retrieve Enhancement with Retry and Interval	12.4(15)T 12.2(33)SRC 12.2(33)SB 12.2(50)SY	The Cisco Networking Services Config Retrieve Enhancement with Retry and Interval feature adds two options to the **cns config retrieve** command enabling you to specify an amount of time in seconds to wait before attempting to retrieve a configuration from a trusted server. The number of retries is restricted to 100 to prevent the configuration agent from indefinitely attempting to reach an unreachable server. Use the keyboard combination **Ctrl-Shift-6** to abort the **cns config retrieve** command. • CNS Config Retrieve Enhancement with Retry and Interval, page 4 • Retrieving a CNS Configuration from a Server, page 27 • Retrieving a CNS Configuration from a Server: Example, page 43 The following command was modified by this feature: **cns config retrieve**.
Cisco Networking Services Event Agent	12.0(18)ST 12.0(22)S 12.2(2)T 12.2(33)SRA 12.2(33)SB 12.2(33)SXI	The Cisco Networking Services Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications to publish and subscribe to events on a Cisco Networking Services Event Bus. Cisco Networking Services Event Agent works in conjunction with the Cisco Networking Services Configuration Agent feature. The following commands were introduced or modified by this feature: **cns event**, **show cns event connections**, **show cns event stats**, **show cns event subject**.

Feature Name	Releases	Feature Information
Cisco Networking Services Image Agent	12.2(33)SEE 12.3(1) 12.2(31)SB2 12.2(33)SRB 12.2(33)SB 12.2(33)SXI	The Cisco Networking Services Image Agent feature is an infrastructure in Cisco IOS software to enable automated installation and activation of Cisco IOS images on Cisco IOS networking devices. The following commands were introduced or modified by this feature: **clear cns image connections**, **clear cns image status**, **cns id**, **cns image**, **cns image password**, **cns image retrieve**, **cns image retry**, **debug cns image**, **show cns image connections**, **show cns image inventory**, **show cns image status**.
Cisco Networking Services Interactive CLI	12.0(28)S 12.2(18)SXE 12.2(18)SXF2 12.2(33)SRC 12.2(33)SXI	The Cisco Networking Services Interactive CLI feature introduces a new XML interface that allows you to send interactive commands to a router, such as commands that generate prompts for user input.
Command Scheduler	12.3(1) 12.2(33)SRA 12.2(33)SRC 12.2(33)SB 12.2(33)SXI 12.2(50)SY	The Command Scheduler feature provides the ability to schedule some EXEC CLI commands to run at specific times or at specified intervals. The following commands were introduced or modified by this feature: **cli**, **debug kron**, **kron occurrence**, **kron policy-list**, **policy-list**, **show kron schedule**.

Feature Name	Releases	Feature Information
CNS Configuration Agent	12.0(18)ST 12.0(22)S 12.2(2)T 12.2(8)T 12.2(33)SRA 12.2(33)SB 12.2(33)SXI	The Cisco Networking Services Configuration Agent feature supports routing devices by providing the following: • Initial configurations • Incremental (partial) configurations • Synchronized configuration updates The following commands were introduced or modified by this feature: **cns config cancel**, **cns config initial**, **cns config partial**, **cns config retrieve**, **cns password**, **debug cns config**, **debug cns xml-parser**, **show cns config outstanding, show cns config stats**, **show cns config status**.