CNS

First Published: June 19, 2006
Last Updated: June 19, 2006

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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for CNS" section on page 64.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

CISCO SYSTEMS

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

Prerequisites for CNS

- Configure a transport protocol on the remote router that is compatible with the remote router's external interface. Table 1 lists the supported transport protocols that can be used depending on the router interface.
- Create the configuration template in the CNS configuration-engine provisioning database. (This task is best done by a senior network designer.)

Table 1 Router Interface and Transport Protocols Required by CNS Services

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

Restrictions for CNS

Remote Router

- The remote router must run a Cisco IOS Release 12.2(25)S or 12.2(33)SRA or later release image that supports the CNS configuration agent and CNS event agent. These include the following:
  - 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.

CNS Configuration Engine

- The CNS 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 CNS configuration engine before installation of the remote router.
- The user of CNS flow-through provisioning and the CNS configuration engine must be familiar with designing network topologies, designing configuration templates, and using the CNS configuration engine.

Information About CNS

To configure CNS, you should understand the following concepts:

- CNS, page 3
- CNS Configuration Agent, page 3
- CNS Exec Agent, page 3
- CNS Event Agent, page 3

CNS

CNS 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 quite 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, CNS has been designed to provide “plug-and-play” network services using a central directory service and distributed agents. CNS features include CNS configuration and event agents and a flow-through provisioning structure. The configuration and event agents use a CNS 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 CNS flow-through provisioning uses the CNS configuration and event agents to provide an automated workflow, eliminating the need for an on-site technician.

CNS Configuration Agent

The CNS configuration agent is involved in the initial configuration and subsequent partial configurations on a Cisco IOS device. To activate the CNS configuration agent, enter any of the **cns config** command-line interface (CLI) commands.

CNS 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 CLI commands—**show** commands—is supported.

CNS Event Agent

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

Initial CNS Configuration

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

When the CNS 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 CNS 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 CNS web server for transmission to the routing device.

The CNS configuration agent accepts the configuration file from the CNS 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.

Incremental CNS Configuration

Once the network is up and running, new services can be added using the CNS 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, it has the option to defer application of the configuration upon receipt of a write-signal event. The CNS Configuration Agent feature allows the device configuration to be synchronized with other dependent network activities.

CNS IDs

The CNS identifier (ID) is a text string that is used exclusively with a particular CNS agent. The CNS ID is used by the CNS agent to identify itself to the server application with which it communicates. For example, the CNS configuration agent will include the configuration ID when communicating between the networking device and the configuration server. The configuration server uses the CNS 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 CNS agent ID as defined on the routing device and the CNS 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 CNS agent ID is

always set to the host name. If the host name changes, the CNS agent ID also changes. If the CNS 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 CNS agent ID does not address security issues.

How to Configure CNS

This section contains the following tasks:

Deploying the CNS Router

Perform this task to manually install an initial CNS 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 CNS 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.

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

Initial CNS Configuration

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

CNS assigns the remote router a unique IP address or host name. After resolving the IP address (using SLARP, ATM InARP, or PPP protocols), the system optionally uses DNS reverse lookup to assign a host name to the router and invokes the CNS agent to download the initial configuration from the CNS configuration engine.

What to Do Next

If you do not need to configure CNS security features, proceed to the "Determining the CNS Agent ID" section on page 8.

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. **exit**
9. **cns config initial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [*inventory*]
10. **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 template connect** *name* **Example:** `Router(config)# cns template connect template 1`	Enters CNS template connect configuration mode and defines the name of a CNS 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 CNS template connect configuration mode and completes the configuration of a CNS connect template. **Note** Entering the **exit** command is required. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

	Command or Action	Purpose
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`	Specifies the interface for connecting to the CNS configuration engine and enters connect-interface configuration mode.
Step 8	**exit** **Example:** `Router(config-cns-conn-if)# exit`	Exits connect-interface configuration mode and returns to global configuration mode.
Step 9	**cns config initial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**event**] [*inventory*] **Example:** `Router(config)# cns config initial 10.1.1.1 no-persist`	Starts the CNS configuration agent, connects to the CNS 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 SSL. **Caution** If you write the new configuration to NVRAM by omitting the **no-persist** keyword, the original bootstrap configuration is overwritten.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring CNS Security Features

Perform this optional task to configure CNS trusted servers.

CNS Trusted Servers

The **cns trusted-server** command can be used to specify a trusted server for an individual CNS agent or for all the CNS agents. To avoid security violations, you can build a list of trusted servers from which CNS agents can receive messages. An attempt to connect to a server not on the list will result in an error message being displayed.

Configure a CNS trusted server when a CNS agent will redirect its response to a server address that is not explicitly configured on the command line for the specific CNS agent. For example, the CNS exec agent may have one server configured but receive a message from the CNS event bus that overrides the configured server. The new server address has not been explicitly configured, so the new server address is not a trusted server. An error will be generated when the CNS exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns trusted-server** {**all-agents** | **config** | **event** | **exec** | **image**} {*host-name* | *ip-address*}

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 trusted-server** {**all-agents** | **config** | **event** | **exec** | **image**} {*host-name* | *ip-address*} **Example:** `Router# cns trusted-server event 10.19.2.5`	Configures a CNS trusted server for the specified host name or IP address.

Determining the CNS Agent ID

Perform this task to determine the CNS agent IDs. CNS agent IDs can be configured for the CNS event agent or CNS configuration agent. By default, the value of **hostname** is set as the CNS agent ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns id cns id** *type number* {**ipaddress** | **mac-address**} [**event**] [**image**]
4. **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 id** *type number* {**ipaddress** | **mac-address**} [**event**] | [**image**] **Example:** `Router(config)# cns id fastethernet 0/1 ipaddress event`	Specifies a unique CNS ID and interface type and number from which to retrieve the unique ID. • Use the optional **event** keyword to specify an event agent ID.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns to privileged EXEC mode.

Enabling and Configuring the CNS Agents

Perform this task to enable and configure the various CNS agents.

CNS Event Agent Parameters

The CNS event agent command—**cns event**—has several parameters that can be configured. The **failover-time** keyword is useful if you have a backup CNS event gateway configured. If the CNS 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 CNS 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 CNS 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 CNS agents may be configured, no other CNS agents are operational until the **cns event** command is entered because the CNS event agent provides a transport connection to the CNS event bus for all other CNS agents.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *ip-address*] [**inventory**]
4. **cns exec** [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*] [**source** *ip-address*]
5. **cns event** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** i*p-address*] [**clock-timeout** *time*] [**reconnect** *time*]
6. **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 config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *ip-address*] [**inventory**] **Example:** `Router(config)# cns config partial 172.28.129.22 80`	(Optional) Starts the CNS configuration agent, which provides CNS 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 CNS configuration agent communications. • Use the optional **inventory** keyword to send an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request. **Note** The optional **encrypt** keyword is available only in images that support SSL.

	Command or Action	Purpose
Step 4	**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 CNS exec agent, which provides CNS 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 CNS exec agent communications. **Note** The optional **encrypt keyword** is available only in images that support SSL.
Step 5	**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 CNS event gateway, which provides CNS 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 CNS event agent communications. • Use the optional **clock-timeout** keyword to specify the maximum time, in minutes, that the CNS 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 CNS event bus are made and therefore no other CNS agents are operational.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

What to Do Next

If you do not need to configure any advanced CNS features, proceed to the "Monitoring and Verifying the CNS Agents" section on page 13.

Configuring Advanced CNS Features

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

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

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 CNS 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.

Prerequisites

This task assumes that CNS is operational and that the required CNS agents are configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *ip-address*] [**inventory**]
4. **logging cns-events** [*severity-level*]
5. **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 config partial** {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *ip-address*] [**inventory**] **Example:** `Router(config)# cns config partial 172.28.129.22 80`	(Optional) Starts the CNS configuration agent, which provides CNS 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 CNS configuration agent communications. • Use the optional **inventory** keyword to send an inventory of the line cards and modules in the router to the CNS 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 CNS 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	**exit** **Example:** `Router# exit`	Exits global configuration mode.

Monitoring and Verifying the CNS Agents

Perform this optional task to display the status of the CNS event agent connection and to display a list of subjects about the CNS event agent connection.

SUMMARY STEPS

1. **enable**
2. **show cns event connections**
3. **show cns event subject** [*name*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show cns event connections**

Use this command to display the status of the CNS 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.

```
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.
```

Step 3 **show cns event subject** [*name*]

Use this command to display a list of subjects of the CNS 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 CNS

This section contains the following configuration examples:

Deploying the CNS Router: Example

The following example shows an initial configuration on a remote router. The host name of the remote router is the unique ID. The CNS configuration engine IP address is 172.28.129.22.

```
Router(config)# cns template connect template1
Router(config-templ-conn)# cli ip address negotiated
Router(config-templ-conn)# cli encapsulation ppp
Router(config-templ-conn)# cli ip directed-broadcast
Router(config-templ-conn)# cli no keepalive
Router(config-templ-conn)# cli no shutdown
Router(config-templ-conn)# exit
Router(config)# cns connect host1 retry-interval 30 retries 3
Router(config-cns-conn-if)# exit
Router(config)# hostname RemoteRouter
```

```
RemoteRouter(config)# ip route 172.28.129.22 255.255.255.0 10.11.11.1
RemoteRouter(config)# cns id Ethernet 0 ipaddress
RemoteRouter(config)# cns config initial 10.1.1.1 no-persist
Router(cns_inv)# 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 CNS 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 CNS configuration engine IP address is 172.28.129.22, and the port number is 80.

```
Router(config)# cns config partial 172.28.129.22 80
```

Enabling and Configuring CNS Agents: Example

The following example shows various CNS 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 CNS configuration engine IP address is 172.28.129.22, and the port number is 80. The CNS exec agent is enabled with an IP address of 172.28.129.23, and the CNS event agent is enabled with an IP address of 172.28.129.24. Until the CNS event agent is enabled, no other CNS agents are operational.

```
Router(config)# cns config partial 172.28.129.22 80
Router(config)# cns exec 172.28.129.23 source 172.22.2.2
Router(config)# cns event 172.28.129.24 source 172.22.2.1
Router(config)# exit
```

Additional References

The following sections provide references related to CNS agents.

Related Documents

Related Topic	Document Title
CNS Image Agent	CNS Configuration section of the *Cisco IOS Network Management Configuration Guide*, Release 12.4
CNS commands	*Cisco IOS Network Management Command Reference*, Release 12.4
CNS Configuration Engine	*Cisco Intelligence Engine 2100 Configuration Registrar Manual*, Release 1.1 or later *Cisco CNS Configuration Engine Administrator's Guide*
CNS Configuration Agent	CNS Configuration section of the *Cisco IOS Network Management Command Reference*, Release 12.4
CNS Event Agent	CNS Configuration section of the *Cisco IOS Network Management Command Reference*, Release 12.4
CNS Flow-Through Provisioning	CNS Configuration section of the *Cisco IOS Network Management Command Reference*, Release 12.4
CNS Frame Relay Zero Touch	CNS Configuration section of the *Cisco IOS Network Management Command Reference*, Release 12.4
Command Scheduler	CNS Configuration section of the *Cisco IOS Network Management Command Reference*, Release 12.4

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
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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 Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands only.

- **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

clear cns config stats

To clear the statistics about the CNS configuration agent, use the **clear cns config stats** command in privileged EXEC mode.

clear cns config stats

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **clear cns config stats** command clears all the statistics displayed by the **show cns config stats** command.

Examples

The following example shows how to clear all of the statistics for the CNS configuration agent:

```
Router# clear cns config stats
```

Related Commands

Command	Description
show cns config stats	Displays statistics about the CNS configuration agent.

clear cns counters

To clear all CNS statistics, use the **clear cns counters** command in privileged EXEC mode.

clear cns counters

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **clear cns counters** command clears all the statistics tracked and displayed by CNS agents.

Examples

The following example shows how to clear all of the statistics used by CNS:

```
Router# clear cns counters
```

Related Commands

Command	Description
show cns config stats	Displays statistics about the CNS configuration agent.
show cns event stats	Displays statistics about the CNS event agent.
show cns image stats	Displays statistics about the CNS image agent.

clear cns event stats

To clear the statistics about the CNS event agent, use the **clear cns event stats** command in privileged EXEC mode.

clear cns event stats

Syntax Description

This command has no arguments or keywords.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **clear cns event stats** command clears all the statistics displayed by the **show cns event stats** command.

Examples

The following example shows how to clear all of the statistics for the CNS event agent:

```
Router# clear cns event stats
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent.

cli (cns)

To specify the command lines of a Cisco Networking Services (CNS) connect template, use the **cli** command in CNS template connect configuration mode. To disable this configuration, use the **no** form of this command.

cli *config-text*

no cli *config-text*

Syntax Description

config-text	Command line to be included in a CNS connect template.

Command Default

No command lines are specified in the CNS connect template.

Command Modes

CNS template connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9). The CNS connect variable **${dlci}** is not supported in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

First use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), and 12.2(33)SRA the **config-cli** and **line-cli** commands are replaced by the **cli (cns)** command.

The command lines specified using the **cli** command can include CNS connect variables (see Table 2). These variables act as placeholders within the command lines of a CNS connect template. Each variable is defined by an associated **discover** command. Before a CNS connect template that contains these variables is applied to a router's configuration, the variables are replaced by the values defined by their associated **discover** command. For example, if the **discover interface serial** command was configured, and you were able to connect to the CNS configuration engine using Serial0/0, then the **cli ip route 0.0.0.0 0.0.0.0 ${interface}** command would generate the **cli ip route 0.0.0.0 0.0.0.0 serial0/0** command.

Note When creating a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Table 2 Summary of the CNS Connect Variables

Variable	Description
${line}	The line type defined by the associated **discover line** *line-type* command.
${controller}	The controller type defined by the associated **discover controller** *controller-type* command.
${interface}	The interface type defined by the associated **discover interface** command.
${dlci}	The active DLCI defined by the associated **discover dlci** command.
${next-hop}	The next hop interface. This variable is identical to the **${interface}** variable unless the **discover dlci** command has been configured. In this case, the **${next-hop}** variable is identical to the **${interface}.{subinterface}** variable, where the **{subinterface}** variable is specified by the **discover dlci** command. The **${next-hop}** variable should only be used in the CNS connect templates after the last **discover** command has been entered. A typical use of this variable is to allow the default IP route to be configured to send traffic towards the CNS configuration engine. Note that the CNS configuration engine may not be on the same LAN as the router. Therefore, configuring a route to the CNS configuration engine may require deployment-specific knowledge. Common practice is to define a default route to the interface using the **ip route** command (for example, **cli ip route 0.0.0.0 0.0.0.0 ${next-hop}**).
$$	A literal substitution of the $ symbol.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **&** variable is replaced by the **${interface}** variable.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router(config)# cns template connect template-1
Router(config-templ-conn)# cli command-1
Router(config-templ-conn)# cli command-2
Router(config-templ-conn)# cli no command-3
Router(config-templ-conn)# exit
Router(config)#
```

When the template1 template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

cns config cancel

To remove a partial Cisco Networking Services (CNS) configuration from the list of outstanding partial configurations, use the **cns config cancel** command in privileged EXEC mode.

cns config cancel *queue-id*

Syntax Description

queue-id	Indicates which partial configuration in the list of outstanding partial configurations to remove from the list. This list can be displayed by issuing the **show cns config outstanding** command in user EXEC or privileged EXEC mode.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18) ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22) S.
12.2(8)T	This command was implemented on additional platforms.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Incremental (partial) configurations take place in two steps:

1. The configuration agent receives the partial configuration. It checks the configuration commands for syntax, publishes the success or failure of the read and syntax-check operation to the sync-status subject “cisco.cns.config.sync-status,” and stores the configuration.
2. The configuration agent receives a second event message directing it to either apply or cancel the stored configuration.

Use the **cns config cancel** command in error scenarios where the second event message is not received and you need to remove the configuration from the list of outstanding configurations. Currently the maximum number of outstanding configurations is one.

Examples

The following example shows the process of checking the existing outstanding CNS configurations and canceling the configuration with the *queue-id* of 1:

```
Router# show cns config outstanding

The outstanding configuration information:
queue id   identifier       config-id
1          identifierREAD   config_idREAD
```

```
Router# cns config cancel 1

Router# show cns config outstanding

The outstanding configuration information:
queue id   identifier       config-id
```

Related Commands

Command	Description
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.
cns event	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.
show cns event connections	Displays the status of the CNS event agent connection.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.

cns config initial

To enable the CNS configuration agent and initiate a download of the initial configuration, use the **cns config initial** command in global configuration mode. To remove an existing **cns config initial** command from the running configuration of the routing device, use the **no** form of this command.

cns config initial {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**status** *url*] [**event**] [**inventory**]

no cns config initial

Syntax Description

host-name	Hostname of the configuration server.
ip-address	IP address of the configuration server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
page	(Optional) Indicates that the configuration is located on a web page.
page	(Optional) Web page where the configuration is located. The default is /cns/config.asp.
syntax-check	(Optional) Turns on syntax checking.
no-persist	(Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the **cns config initial** command. If not present, issuing the **cns config initial** command causes the resultant configuration to be automatically written to NVRAM.
source	(Optional) Specifies the source of CNS communications.
ip-address	(Optional) IP address of the source of CNS communications.
status *url*	(Optional) Sends an event to the specified URL via HTTP, either notifying successful completion of the configuration or warning that the configuration contained errors.
event	(Optional) Sends an event to the Event Bus notifying successful completion of the configuration or warning that the configuration contained errors. If the CNS event agent is not configured, the event will be saved until the CNS event agent is enabled. If the **event** keyword is not specified, a log message is sent to the console of the device after the configuration is complete.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.
Default web page of the initial configuration is /cns/config.asp.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **source** and **encrypt** keywords were added.
12.3(1)	The **inventory** keyword was added.
12.3(8)T	The **status** *url* keyword/argument pair was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command when a basic configuration—called a bootstrap configuration—is added to multiple routers before being deployed. When a router is initially powered (or each time a router is reloaded when the **no-persist** keyword is used) the **cns config initial** command will cause a configuration file—called an initial configuration—for the router to be downloaded from the configuration server. The initial configuration can be unique for each router.

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will retry until it successfully completes. Once the configuration has successfully completed the **cns config initial** command will be removed from the running configuration. By default, NVRAM will be updated except when the **no-persist** keyword is configured.

When this command is used with the **event** keyword, a single message will be published on the event bus after the configuration is complete. The event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the initial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the initial configuration but encountered possible semantic errors.

When this command is used with the **status** keyword, a single message will be published to the URL specified after the configuration is complete.

Examples

The following example shows how to enable the CNS configuration agent and initiate an initial configuration:

```
Router# cns config initial 10.19.4.5 page /cns/config/first.asp
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
cns config notify	Detects CNS configuration changes and sends an event containing the previous and current configuration.

Command	Description
cns config retrieve	Enables the CNS configuration agent and initiates a download of the initial configuration.
cns event	Configures the CNS event gateway, which provides CNS event services to Cisco IOS clients.
show cns config status	Displays information about the status of the CNS configuration agent.

cns config notify

To notify CNS agents of configuration changes on Cisco IOS devices, use the **cns config notify** command in global configuration mode. To disable notifications, use the **no** form of this command.

cns config notify {**all** | **diff**} [**interval** *minutes*] [**no_cns_events**] [**old-format**]

no cns config notify {**all** | **diff**} [**interval** *minutes*] [**no_cns_events**] [**old-format**]

Syntax Description

all	Captures all configuration commands for the config-changed event output.
diff	Captures commands that change configuration for the config-changed event output.
interval *minutes*	(Optional) Specifies the amount of time after the last configuration change that the config-changed event is sent. The default is 5 minutes. The timer starts when you make a configuration change and you remain in configuration mode after the configuration change. If you enter the **end** command, the config-changed event is sent immediately.
no_cns_events	(Optional) Disables event notification for configurations changed through an XML file. If the configuration is changed using the command-line interface (CLI), the config-changed event will be sent.
old-format	(Optional) Provides the event notification in the old XML format for backwards compatibility.

Command Default

The interval defaults to 5 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(11)T	The **diff** keyword was removed.
12.3(1)	The **diff** and **old-format** keywords were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When the **cns config notify** command is enabled, commands entered in configuration mode are detected. If the **all** keyword is specified, the command is stored for future notification. If the **diff** keyword is specified, the command is stored for future notification if the software determines that the command will cause a configuration change. The **diff** keyword also allows the software to store information about the command including previous configuration states, source of the change (for example, a telnet user), and the time of configuration.

The stored information is formatted in XML and sent as part of a CNS config agent change notification event. A CNS config agent change notification event is sent to the CNS event bus when configuration mode is exited or no activity from that source has occurred for the configured interval time.

You must enable the CNS event agent using the **cns event** command before configuring this command. If the CNS event agent is not configured, the notification event will be queued and sent when the CNS event agent is enabled. If the CNS config notify queue is full, subsequent events are dropped and a "lost" CNS config change notification is sent when the CNS event agent is enabled.

Use the **no_cns_events** for applications that already record configuration changes sent to the routing device through the CNS event bus.

Use the **old-format** keyword to generate XML output—only the entered command and previous configuration state—that is compatible with the versions of this commands when the **diff** keyword was removed.

Examples

The following example detects configuration changes for all configuration commands:

```
Router(config)# cns config notify all
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.
cns event	Enables and configures CNS event agent services.

cns config partial

To start the Cisco Networking Services (CNS) configuration agent and accept a partial configuration, use the **cns config partial** command in global configuration mode. To shut down the CNS partial configuration agent, use the **no** form of this command.

cns config partial {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**source** *ip-address*] [**inventory**]

no cns config partial

Syntax Description

host-name	Hostname of the configuration server.
ip-address	IP address of the configuration server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link between the router and the web server.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
source	(Optional) Specifies the source of this device.
ip-address	(Optional) IP address to use as the source of this device.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Command Default

The CNS configuration agent is not enabled to accept a partial configuration and the router does not request or receive updates.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **source** keyword and **encrypt** arguments were added.
12.3(1)	The **inventory** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	This command was modified to include enhanced CNS error messages.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to start the CNS partial configuration agent. You must enable the CNS event agent using the **cns event** command before configuring this command. The CNS event agent sends an event with the subject "cisco.mgmt.cns.config.load" to specify whether configuration data can be pushed to the CNS partial configuration agent or pulled from a configuration server by the CNS partial configuration agent.

In the push model, the event message delivers the configuration data to the partial configuration agent.

In the pull model, the event message triggers the partial configuration agent to pull the configuration data from the CNS configuration engine. The event message contains information about the CNS configuration engine, not the actual configuration data. The host name or IP address is the address of the CNS configuration engine from which the configuration is pulled. Use the **cns trusted-server** command to specify which CNS configuration engines can be used by the CNS partial configuration agent.

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will retry until the configuration successfully completes. In the pull mode, the command will not retry after an error. By default, NVRAM will be updated except when the **no-persist** keyword is configured.

A message will be published on the CNS event bus after the partial configuration is complete. The CNS event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the partial configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the partial configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure(CLI syntax)—CNS configuration agent encountered a command line interface (CLI) syntax error and was not able to apply the partial configuration.
- cisco.mgmt.cns.config.failure(CLI semantic)—CNS configuration agent encountered a CLI semantic error and was not able to apply the partial configuration.

In Cisco IOS Releases 12.4(4)T, 12.2 (33)SRA, and later releases, a second message is sent to the subject "cisco.cns.config.results" in addition to the appropriate message above. The second message contains both overall and line-by-line information about the configuration that was sent and the result of the action requested in the original message. If the action requested was to apply the configuration, then the information in the results message is semantic in nature. If the action requested was to check syntax only, then the information in the results message is syntactical in nature.

Examples

The following example shows how to configure the CNS partial configuration agent to accept events from the event gateway at 172.28.129.22. The CNS partial configuration agent will connect to the CNS configuration server at 172.28.129.22, port number 80. The CNS partial configuration agent requests are redirected to a configuration server at 172.28.129.40, port number 80.

```
Router(config)# cns event 172.28.129.22
Router(config)# cns trusted-server config 172.28.129.40
Router(config)# cns config partial 172.28.129.22
```

The following example shows an enhanced error message sent to the subject "cisco.mgmt.cns.config.results":

```
[2005-09-08 14:30:44]: subject=cisco.mgmt.cns.config.results.dvlpr-7200-6, message=
<?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>user1</wsse:Username>
<wsse:Password>password1</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>2005-09-13T08:34:36.523Z</CNS:Time>
</CNS:cnsHeader>
</SOAP:Header>
<SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
<configResults version="2.0" overall="Success">
<configId>AAA</configId>
</configResults>
</SOAP:Body>
</SOAP:Envelope>
```

Related Commands

Command	Description
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns event	Enables and configures CNS event agent services.
cns trusted-server	Specifies a trusted server for CNS agents.
show cns config outstanding	Displays information about incremental CNS configurations that have started but are not yet completed.

cns config retrieve

To enable the CNS configuration agent and initiate a download of the initial configuration, use the **cns config retrieve** command in privileged EXEC mode.

cns config retrieve {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**overwrite-startup**] [**syntax-check**] [**no-persist**] [**source** *ip-address*] [**event**] [**inventory**]

Syntax Description

host-name	Host name of the configuration server.
ip-address	IP address of the configuration server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway.
port-number	(Optional) Port number of the configuration service. The value is from 0 to 65535. The default is 80 with no encryption and 443 with encryption.
page	(Optional) Indicates that the configuration is located on a web page.
page	(Optional) Web page where the configuration is located. The default is /cns/config.asp.
overwrite-startup	(Optional) Replaces the startup configuration file. Does not apply to the running configuration file.
syntax-check	(Optional) Turns on syntax checking.
no-persist	(Optional) Suppresses the default automatic writing to NVRAM of the configuration pulled as a result of issuing the **cns config retrieve** command. If not present, issuing the **cns config retrieve** command causes the resultant configuration to be automatically written to NVRAM.
source	(Optional) Specifies the source of CNS communications.
ip-address	(Optional) IP address of the source of the configuration.
event	(Optional) Sends an event to the CNS Event Bus stating successful completion of the configuration, a warning that the configuration contained errors, or a message noting that the configuration failed. If the CNS event agent is not configured, the event will be saved until the CNS event agent is enabled. If the **event** keyword is not specified, a log message is sent to the console of the device after the configuration is complete.
inventory	(Optional) Sends an inventory of the line cards and modules in the router to the CNS configuration engine as part of the HTTP request.

Defaults

The port number defaults to 80 with no encryption and 443 with encryption.
Default web page of the initial configuration is /cns/config.asp.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(1)	The **inventory** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command 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).

When the configuration has been received by the router, each line of the configuration will be applied in the same order as it was received. If the Cisco IOS parser has an error with one of the lines of the configuration, then all the configuration up to this point will be applied to the router, but none of the configuration beyond the error will be applied. If an error occurs, the command will not retry.

A single message will be published on the event bus after the partial configuration is complete. The event bus will display one of the following status messages:

- cisco.mgmt.cns.config.complete—CNS configuration agent successfully applied the configuration.
- cisco.mgmt.cns.config.warning—CNS configuration agent fully applied the configuration, but encountered possible semantic errors.
- cisco.mgmt.cns.config.failure—CNS configuration agent encountered an error and was not able to apply the configuration.

The **cns config retrieve** command can be used with Command Scheduler commands (for example, **kron policy-list** and **cli** commands) in environments where it is not practical to use the CNS event agent and the **cns config partial** command. Configured within the **cli** command, the **cns config retrieve** command can be used to poll the configuration server to detect configuration changes.

Examples

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

```
Router(config)# cns trusted-server all 10.1.1.1
Router(config)# cns config retrieve 10.1.1.1
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns trusted-server	Specifies a trusted server for CNS agents.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
show cns config status	Displays information about the status of the CNS configuration agent.

cns connect

To enter Cisco Networking Services (CNS) connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine, use the **cns connect** command in global configuration mode. To disable the CNS connect profile, use the **no** form of this command.

cns connect *name* [**retry-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]

no cns connect *name* [**ping-interval** *interval-seconds*] [**retries** *number-retries*] [**timeout** *timeout-seconds*] [**sleep** *sleep-seconds*]

Syntax Description

name	Name of the CNS connect profile to be configured.
retry-interval	(Optional) Sets the interval (in seconds) between each successive attempt to ping the CNS configuration engine. The default value is 10 seconds. The valid range is 8 to 40 seconds.
interval-seconds	(Optional) Number of seconds between each successive attempt to ping the CNS configuration engine.
retries	(Optional) Sets the number of times the CNS connect function will try to ping the CNS configuration engine. The default value is 3.
number-retries	(Optional) Number of times the CNS connect function will try to ping the CNS configuration engine.
timeout	(Optional) Sets the amount of time (in seconds) after which an interface is no longer used for ping attempts. The default value is 120 seconds.
timeout-seconds	(Optional) Number of seconds after which an interface is no longer used for ping attempts.
sleep	(Optional) Sets the amount of time (in seconds) before the first ping is attempted for each interface. This option provides time for the far end of a link to stabilize. The default value is 0 seconds.
sleep-seconds	(Optional) Number of seconds before the first ping is attempted for each interface.

Command Default

No CNS connect profiles are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **ping-interval** keyword was replaced by the **retry-interval** keyword.

Usage Guidelines

Use the **cns connect** command to enter CNS connect configuration mode and define the parameters of a CNS connect profile for connecting to the CNS configuration engine. Then use the following CNS connect commands to create a CNS connect profile:

- **discover**
- **template**

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), and 12.2(33)SRA the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands.

Examples

The following example shows how to create a CNS connect profile named profile-1:

```
Router(config)# cns connect profile-1
Router(config-cns-conn)# discover interface Serial
Router(config-cns-conn)# template template-1
Router(config-cns-conn)# exit
Router(config)#
```

In this example, the following sequence of events occurs for each serial interface when the **cns connect profile-1** command is processed:

1. Enter interface configuration mode and apply all commands in the template-1 template to the router's configuration.
2. Try to ping the CNS configuration engine.
3. If the ping is successful, then download pertinent configuration information from the CNS configuration engine and exit. The **cns connect profile-1** command has completed its process.
4. If the ping is unsuccessful, enter interface configuration mode and remove all commands in the template-1 template from the router's configuration. The **cns connect profile-1** command has failed to retrieve any configuration information from the CNS configuration engine.

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

cns event

To configure the Cisco Networking Services (CNS) event gateway, which provides CNS event services to Cisco IOS clients, use the **cns event** command in global configuration mode. To remove the specified event gateway from the gateway list, use the **no** form of this command.

cns event {*host-name* | *ip-address*} [**encrypt**] [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** i*p-address*] [**clock-timeout** *time*] [**reconnect** *time*]

no cns event {*host-name* | *ip-address*} [*port-number*] [**encrypt**] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** *ip-address*] [**clock-timeout** *time*] [**reconnect** *time*]

Syntax Description

host-name	Hostname of the event gateway.
ip-address	IP address of the event gateway.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the event gateway. **Note** This keyword is available only in images that support SSL.
port-number	(Optional) Port number for the event gateway. The default is 11011 with no encryption or 11012 with encryption.
backup	(Optional) Indicates a backup gateway. If omitted, indicates the primary gateway. A primary gateway must be configured before you can configure a backup gateway. Optional keywords, if omitted, are set as for the primary gateway.
failover-time *seconds*	(Optional) Specifies a time interval, in seconds, to wait for the primary gateway route after the route to the backup gateway is established. The default is 3.
keepalive *seconds retry-count*	(Optional) Specifies a keepalive timeout, in seconds, and retry count.
source *ip-address*	(Optional) Indicates the IP address of the source for CNS communications.
clock-timeout *time*	(Optional) Specifies the maximum time, in minutes, that the CNS event agent will wait for the clock to be set for transports (such as SSL) that require an accurate clock. The default is 10.
reconnect *time*	(Optional) Specifies the configurable upper limit of the maximum retry timeout. The valid range is 1 through 65535. The default is 3600.

Command Default

No CNS event gateway is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into the Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(2)XB	This command was implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	The **encrypt**, **init-retry**, **source**, and **force-fmt1** keywords were added.
12.3	The **reconnect-time** keyword was added.
12.3(1)	The **init-retry** keyword was replaced with the **failover-time** keyword. The **force-fmt1** keyword was removed. The **clock-timeout** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The CNS event agent must be enabled before any of the other CNS agents are configured because the CNS event agent provides a transport connection to the CNS event bus for all other CNS agents. The other CNS agents use the connection to the CNS event bus to send and receive messages. The CNS event agent does not read or modify the messages.

The **failover-time** keyword is useful if you have a backup CNS event gateway configured. If the CNS event agent is trying to connect to the gateway and it discovers that the route to the backup is available before the route to the primary gateway, the *seconds* argument specifies how long the CNS 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 value of the *seconds* argument multiplied by the value of the *retry-count* argument determines the length of idle time before the CNS event agent will disconnect and attempt to reconnect to the gateway. We recommend a minimum *retry-count* of two.

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.

If network connectivity between the Cisco IOS router running the CNS event agent and the gateway is absent, the event agent goes into an exponential backoff retry mode and gets stuck at the maximum limit (which may be hours). The **reconnect-time** keyword allows a configurable upper limit of the maximum retry timeout.

Examples

The following example shows how to set the address of the primary CNS event gateway to the configuration engine software running on IP address 10.1.2.3, port 11011, with a keepalive of 60 seconds and a retry count of 5:

```
Router(config)# cns event 10.1.2.3 11011 keepalive 60 5
```

Related Commands

Command	Description
cns id	Sets the unique event ID or config ID router identifier.
show cns event status	Displays status information about the CNS event agent.

cns exec

To enable and configure the Cisco Networking Services (CNS) exec agent, which provides CNS exec agent services to Cisco IOS clients, use the **cns exec** command in global configuration mode. To disable the use of CNS exec agent services, use the **no** form of this command.

cns exec [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*] [**source** *ip-address*]

no cns exec [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*] [**source** *ip-address*]

Syntax Description

host-name	(Optional) Hostname of the exec server.
ip-address	(Optional) IP address of the exec server.
encrypt	(Optional) Uses a Secure Sockets Layer (SSL) encrypted link to the exec agent server. **Note** This keyword is available only in images that support SSL.
enc-port-number	(Optional) Port number for the encrypted exec server. The default is 443.
port-number	(Optional) Port number for the exec server. The default is 80.
source	(Optional) Specifies the use of an IP address defined by the *ip-address* argument as the source for CNS exec agent communications.
ip-address	(Optional) IP address.

Defaults

No CNS exec agent is configured.

Command Modes

Global configuration

CommandHistory

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The CNS exec agent allows a remote application to execute an EXEC mode command-line interface (CLI) command on a Cisco IOS device by sending an event message containing the command. A restricted set of EXEC CLI commands—**show** commands—are supported.

In previous Cisco IOS releases, the CNS exec agent was enabled when the CNS configuration agent was enabled through the **cns config partial** command.

Examples

The following example shows how to enable the CNS exec agent with an IP address of 10.1.2.3 for the exec agent server, a port number of 93, and a source IP address of 172.17.2.2:

```
Router(config)# cns exec 10.1.2.3 93 source 172.17.2.2
```

Related Commands

Command	Description
cns event	Enables and configures CNS event agent services.
show cns event subject	Displays a list of CNS event agent subjects that are subscribed to by applications.

cns id

To set the unique event ID, config ID, or image ID Cisco IOS device identifier used by CNS services, use the **cns id** command in global configuration mode. To set the identifier to the hostname of the Cisco IOS device, use the **no** form of this command.

If ID Choice Is an IP Address or MAC Address

cns id *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]

no cns id *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]

If ID Choice Is Anything Else

cns id {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**]

no cns id {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**]

If Using Cisco IOS Release 12.2(33)SRA

cns id *type number* {**ipaddress** | **mac-address**} [**event**] [**image**]

Syntax Description

type number	Type of interface (for example, **ethernet**, **group-async**, **loopback**, or **virtual-template**) and the interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
dns-reverse	Uses DNS reverse lookup to retrieve the hostname of the Cisco IOS device and assign it as the unique ID.
ipaddress	Uses the IP address specified in the *type number* arguments as the unique ID.
mac-address	Uses the MAC address specified in the *type number* arguments as the unique ID.
event	(Optional) Sets this ID to be the event ID value, which is used to identify the Cisco IOS device for CNS event services. If both optional keywords are omitted, the event ID is set to the hostname of the Cisco IOS device.
image	(Optional) Sets this ID to be the image ID value, which is used to identify the Cisco IOS device for CNS image agent services. If both optional keywords are omitted, the image ID is set to the hostname of the Cisco IOS device.
hardware-serial	Uses the hardware serial number as the unique ID.
hostname	Uses the hostname as the unique ID. This is the system default.
string *string*	Uses an arbitrary text string—typically the hostname—as the unique ID.
udi	Uses the product Unique Device Identifier (UDI) as the unique ID.

Command Default

The system defaults to the hostname of the Cisco IOS device as the unique ID.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced on Cisco IAD2420 series IADs.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(1)	The optional **image** keyword was added to set an image ID.
12.3(14)T	The **udi** keyword was added to use the product UDI as the unique ID.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to set the unique ID to the CNS configuration agent, which then pulls the initial configuration template to the Cisco IOS device during bootup.

You can set one or all three IDs: the config ID value for CNS configuration services, the event ID value for CNS event services, and the image ID value for CNS image agent services. To set all values, use the command three times.

To set the CNS event ID to the host name of the Cisco IOS device, use the **no** form of this command with the **event** keyword. To set the CNS config ID to the host name of the Cisco IOS device, use the **no** form of this command without the **event** keyword. To set the CNS image ID to the host name of the Cisco IOS device, use the **no** form of this command with the **image** keyword.

Unique Device Identifier

Each identifiable Cisco product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a superentity, such as a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval. To use UDI retrieval, the Cisco product in use must be UDI-enabled.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which a product can be ordered; historically, it has been called the “Product Name” or “Part Number.” This identifier is the one to use to order an exact replacement part.

The VID is the version of the product. When a product is revised, the VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. The serial number is used to identify an individual, specific instance of a product.

Note The **udi** keyword will create an ID consisting of the PID, VID, and SN values without spaces but separated using commas. To view the UDI for this product, use the **show inventory** command. This keyword is not available in Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to pass the hostname of the Cisco IOS device as the config ID value:

```
Router(config)# cns id hostname
```

The following example shows how to pass the hardware serial number of the Cisco IOS device as the event ID value:

```
Router(config)# cns id hardware-serial event
```

The following example shows how to pass the UDI as the event ID value:

```
Router(config)# cns id udi event
```

The following example shows how to pass the IP address of Ethernet interface 0/1 as the image ID value:

```
Router(config)# cns id ethernet 0/1 image
```

Related Commands

Command	Description
cns event	Enables the CNS event gateway, which provides CNS event services to Cisco IOS clients.
cns image	Enables the CNS image agent services to Cisco IOS clients.
show inventory	Displays the product inventory listing for all Cisco products that are installed in a networking device.

cns template connect

To enter Cisco Networking Services (CNS) template connect configuration mode and define the name of a CNS connect template, use the **cns template connect** command in global configuration mode. To disable the CNS connect template, use the **no** form of this command.

cns template connect *name*

no cns template connect *name*

Syntax Description

name	Name of the CNS connect template to be configured.

Command Default

No CNS connect templates are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.

Note When you create a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Note Effective with Cisco IOS Releases 12.3(8)T,12.3(9), and 12.2(33)SRA the **cns config connect-intf** command is replaced by the **cns connect** and **cns template connect** commands.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router(config)# cns template connect template1
Router(config-templ-conn)# cli command-1
Router(config-templ-conn)# cli command-2
Router(config-templ-conn)# cli no command-3
Router(config-templ-conn)# exit
Router(config)#
```

When the template1 template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cli (cns)	Specifies the command lines of a CNS connect template.
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

cns trusted-server

To specify a trusted server for CNS agents, use the **cns trusted-server** command in global configuration mode. To disable the use of a trusted server for a CNS agent, use the **no** form of this command.

cns trusted-server {**all-agents** | **config** | **event** | **exec** | **image**} {*host-name* | *ip-address*}

no cns trusted-server {**all-agents** | **config** | **event** | **exec** | **image**}

Syntax Description

all-agents	Specifies a trusted server for all CNS agents.
config	Specifies a trusted server for CNS config agent.
event	Specifies a trusted server for CNS event agent.
exec	Specifies a trusted server for CNS exec agent.
image	Specifies a trusted server for CNS image agent.
host-name	Hostname of the trusted server.
ip-address	IP address of the trusted server.

Defaults

all-agents

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **cns trusted-server** command to specify a trusted server for an individual CNS agent or all the CNS agents. In previous Cisco IOS Releases CNS agents could connect to any server and this could expose the system to security violations. An attempt to connect to a server not on the list will result in an error message being displayed. For backwards compatibility the configuration of a server address using the configuration command-line interface (CLI) for a CNS agent will result in an implicit trust of the server. The implicit trusted server commands apply only to commands in configuration mode, not EXEC mode commands.

Use this command when a CNS agent will redirect its response to a server address that is not explicitly configured on the command line for the specific CNS agent. For example, the CNS exec agent may have one server configured but receive a message from the CNS Event Bus that overrides the configured server. The new server address has not been explicitly configured so the new server address is not a trusted server. An error will be generated when the CNS exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address.

Examples

The following example shows how to configure server 10.19.2.5 as a trusted server for the CNS event agent:

```
Router# cns trusted-server event 10.19.2.5
```

The following example shows how to configure server 10.2.2.8 as an implicit trusted server for the CNS image agent:

```
Router# cns image server 10.2.2.8 status 10.2.2.8
```

Related Commands

Command	Description
cns config	Configures CNS configuration agent services.
cns event	Enables and configures CNS event agent services.
cns image	Configures CNS image agent services.

debug cns config

To turn on debugging messages related to the Cisco Networking Services (CNS) Configuration Agent, use the **debug cns config** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug cns config {**agent** | **all** | **connection** | **notify**}

no debug cns config {**agent** | **all** | **connection** | **notify**}

Syntax Description

agent	Displays debugging messages related to the CNS configuration agent.
all	Displays all debugging messages.
connection	Displays debugging messages related to configuration connections.
notify	Displays debugging messages related to CNS configurations.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.2(8)T	This command was implemented on the Cisco 2600 and Cisco 3600 series.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to turn on or turn off debugging messages related to the CNS Configuration Agent.

Examples

In the following example, debugging messages are enabled for CNS configuration processes:

```
Router# debug cns config all

00:04:09: config_id_get: entered
00:04:09: config_id_get: Invoking cns_id_mode_get()
00:04:09: config_id_get: cns_id_mode_get() returned INTERNAL
00:04:09: config_id_get: successful exit cns_config_id=minna1,cns_config_id_len=6
00:04:09: cns_establish_connect_intf(): The device is already connected with the config
server
00:04:09: cns_initial_config_agent(): connecting with port 80
00:04:09: pull_config() entered
00:04:09: cns_config_id(): returning config_id=minna1
00:04:09: Message finished 150 readend
00:04:09: %CNS-4-NOTE: SUCCESSFUL_COMPLETION
-Process= "CNS Initial Configuration Agent", ipl= 0, pid= 82
00:04:10: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

Command	Description
cns config cancel	Cancels a CNS configuration.
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.
cns config retrieve	Gets the configuration of a routing device using CNS.
debug cns event	Displays information on CNS events.
debug cns exec	Displays information on CNS management.
debug cns xml-parser	Displays information on the CNS XML parser.
show cns config	Displays information about the CNS Configuration Agent.

debug cns exec

To display debugging messages about CNS exec agent services, use the **debug cns exec** command in privileged EXEC mode. To disable debugging output, use the **no** or **undebug** form of this command.

debug cns exec {**agent** | **all** | **decode** | **messages**}

no debug cns exec {**agent** | **all** | **decode** | **messages**}

undebug cns exec {**agent** | **all** | **decode** | **messages**}

Syntax Description

agent	Displays debugging messages related to the exec agent.
all	Displays all debugging messages.
decode	Displays debugging messages related to image agent connections.
messages	Displays debugging output related to messages generated by exec agent services.

Defaults

Debugging output is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **debug cns exec** command to troubleshoot CNS exec agent services.

Examples

The following example shows a debugging message for the CNS exec agent when a response has been posted to HTTP:

```
Router# debug cns exec agent

4d20h: CNS exec agent: response posted
```

Related Commands

Command	Description
cns exec	Configures CNS Exec Agent services.

debug cns xml-parser

To turn on debugging messages related to the Cisco Networking Services (CNS) eXtensible Markup Language (XML) parser, use the **debug cns xml-parser** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug cns xml-parser

no debug cns xml-parser

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.2(8)T	This command was implemented on the Cisco 2600 and Cisco 3600 series.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example, debugging messages for the CNS XML parser are enabled:

```
Router# debug cns xml-parser

00:12:05: Registering tag <config-server>
00:12:05: Registering tag <server-info>
00:12:05: Registering tag <ip-address>
00:12:05: Registering tag <web-page>
00:12:05: Registering tag <config-event>
00:12:05: Registering tag <identifier>
00:12:05: Registering tag <config-id>
00:12:05: Registering tag <config-data>
00:12:05: Registering tag <cli>
00:12:05: Registering tag <error-info>
00:12:05: Registering tag <error-message>
00:12:05: Registering tag <line-number>
00:12:05: Registering tag <config-write>
00:12:05: Registering tag <exec-cmd-event>
00:12:05: Registering tag <identifier-exec>
00:12:05: Registering tag <event-response>
00:12:05: Registering tag <reply-subject>
00:12:05: Registering tag <server-response>
00:12:05: Registering tag <ip-address-exec>
00:12:05: Registering tag <port-number>
00:12:05: Registering tag <url>
00:12:05: Registering tag <cli-exec>
00:12:05: Registering tag <config-pwd>
```

```
00:12:06: Pushing tag <config-data> on to stack
00:12:06: open tag is <config-data>
00:12:06: Pushing tag <config-id> on to stack
00:12:06: open tag is <config-id>
00:12:06: Popping tag <config-id> off stack
00:12:06: close tag is </config-id>
00:12:06: Pushing tag <cli> on to stack
00:12:06: open tag is <cli>
00:12:06: Popping tag <cli> off stack
00:12:06: close tag is </cli>
00:12:06: Popping tag <config-data> off stack
00:12:06: close tag is </config-data>
00:12:06: %CNS-4-NOTE: SUCCESSFUL_COMPLETION
-Process= "CNS Initial Configuration Agent", ipl= 0, pid= 96
```

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.
show cns event	Displays information about the CNS Event Agent.

logging cns-events

To enable XML-formatted system event message logging to be sent through the CNS event bus, use the **logging cns-events** command in global configuration mode. To disable the ability to send system logging event messages through the CNS event bus, use the **no** form of this command.

logging cns-events [*severity-level*]

no logging cns-events

Syntax Description

severity-level	(Optional) The number or name of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows (enter the number or the keyword): {**0** | **emergencies**}— System is unusable {**1** | **alerts**}—Immediate action needed {**2** | **critical**}—Critical conditions {**3** | **errors**}—Error conditions {**4** | **warnings**}—Warning conditions {**5** | **notifications**}—Normal but significant conditions {**6** | **informational**}—Informational messages {**7** | **debugging**}— Debugging messages

Defaults

Level 7: debugging

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you configure this command you must enable the CNS event agent with the **cns event** command because the CNS event agent sends out the CNS event logging messages. The generation of many CNS event logging messages can negatively impact the publishing time of standard CNS event messages that must be sent to the network.

If the **debug cns event** command is active when the **logging cns-events** command is configured, the logging of CNS events is disabled.

Examples

In the following example, the user enables XML-formatted CNS system error message logging to the CNS event bus for messages at levels 0 through 4:

```
Router(config)# logging cns-events 4
```

Related Commands

Command	Description
cns event	Configures CNS event gateway, which provides CNS event services to Cisco IOS clients.
debug cns event	Displays CNS event agent debugging messages.

show cns config stats

To display statistics about the CNS configuration agent, use the **show cns config stats** command in privileged EXEC mode.

show cns config stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.3(1)	Additional output fields were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command displays the following statistics on the CNS configuration agent:

- The number of configurations requests received
- The number of configurations completed
- The number of configurations failed
- The number of configurations pending
- The number of configurations cancelled
- The time stamp of the last configuration received
- The time stamp of the initial configuration received

Examples

The following is sample output from the **show cns config stats** command:

```
Router# show cns config stats

6 configuration requests received.
4 configurations completed.
1 configurations failed.
1 configurations pending.
0 configurations cancelled.
The time of last received configuration is *May 5 2003 10:42:15 UTC.
Initial Config received *May 5 2003 10:45:15 UTC.
```

Related Commands

Command	Description
clear cns config stats	Clears all the statistics about the CNS configuration agent.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.

show cns event connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns event connections** command in privileged EXEC mode.

show cns event connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show cns event connections** command to display the status of the 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.

Examples

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.
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event stats

To display statistics about the CNS event agent connection, use the **show cns event stats** command in privileged EXEC mode.

show cns event stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series routers.
12.3(1)	Output was changed to display statistics generated since last cleared.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to display the following statistics for the CNS event agent:

- Number of events received
- Number of events sent
- Number of events not processed successfully
- Number of events in the queue
- Time stamp showing when statistics were last cleared (time stamp is router time)
- Number of events received since the statistics were cleared
- Time stamp of latest event received (time stamp is router time)
- Time stamp of latest event sent
- Number of applications using the Event Agent
- Number of subjects subscribed

Examples

The following example displays statistics for the CNS event agent:

```
Router# show cns event stats

0 events received.
1 events sent.
0 events not processed.
```

```
0 events in the queue.
0 events sent to other IOS applications.
Event agent stats last cleared at Apr 4 2003 00:55:25 UTC
No events received since stats cleared
The time stamp of the last received event is *Mar 30 2003 11:04:08 UTC
The time stamp of the last sent event is *Apr 11 2003 22:21:23 UTC
3 applications are using the event agent.
0 subjects subscribed.
1 subjects produced.
0 subjects replied.
```

Related Commands

Command	Description
clear cns event stats	Clears all the statistics about the CNS event agent.
cns event	Enables and configures CNS event agent services.
show cns event connections	Displays the status of the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event subject

To display a list of subjects about the Cisco Networking Services (CNS) event agent connection, use the **show cns event subject** command in privileged EXEC mode.

show cns event subject [*name*]

Syntax Description

name	(Optional) Displays a list of applications that are subscribing to this specific subject name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show cns event subject** command to display a list of subjects of the event agent that are subscribed to by applications.

Examples

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

```
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
```

Related Commands

Command	Description
show cns event connections	Displays the status of the CNS event agent connection.
show cns event stats	Displays statistics about the CNS event agent connection.

Feature Information for CNS

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for CNS

Feature Name	Releases	Feature Information
CNS	12.2(25)S, 12.2(33) SRA	The 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. In 12.2(25)S, this feature was introduced. In 12.2(33)SRA, this feature was integrated into Cisco IOS Release 12.2(33)SRA.
CNS Configuration Agent	12.2(2)T, 12.0(18)ST, 12.0(22)S, 12.2(33)SRA	The CNS Configuration Agent feature supports routing devices by providing the following: • Initial configurations • Incremental (partial) configurations • Synchronized configuration updates
CNS Event Agent	12.2(2)T, 12.0(18)ST, 12.0(22)S, 12.2(33)SRA	The CNS Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications to publish and subscribe to events on a CNS Event Bus. CNS Event Agent works in conjunction with the CNS Configuration Agent feature.
CNS Flow-Through Provisioning	12.2(2)T, 12.2(2)XB, 12.2(8)T	Cisco Networking Services (CNS) Flow-Through Provisioning provides the infrastructure for automated configuration of large numbers of network devices. Based on CNS event and config agents, it eliminates the need for an onsite technician to initialize the device. The result is an automated workflow from initial subscriber-order entry through Cisco manufacturing and shipping to final device provisioning and subscriber billing. This focuses on a root problem of today's service-provider and other similar business models: use of human labor in activating service.

Table 3 Feature Information for CNS

Feature Name	Releases	Feature Information
CNS Zero Touch	12.3(9)	The CNS Zero Touch feature provides a zero touch deployment solution where the router contacts a CNS configuration engine to retrieve its full configuration automatically. As part of the CNS Zero Touch feature, the following commands have been replaced by new commands: • The **cns config connect-intf** command is replaced by the **cns connect** and cns template connect commands. • The **config-cli** and **line-cli** commands are replace by the **cli (cns)** command.
CNS Frame-Relay Zero Touch	12.3(2)XF, 12.3(8)T	The CNS Frame Relay Zero Touch feature provides a CNS zero touch deployment solution over Frame Relay where the CPE router discovers its DLCI and IP address dynamically, and then contacts a CNS engine to retrieve its full configuration automatically.
Command Scheduler	12.3(1), 12.2(33)SRA	The Command Scheduler feature provides the ability to schedule some EXEC command-line interface (CLI) commands to run at specific times or at specified intervals.