Cisco IOS Cisco Networking Services Command Reference

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

CONTENTS

A through E Commands

announce config

To specify that an unsolicited configuration inventory is sent out by the CNS inventory agent at bootup, use the **announce config** command in CNS inventory configuration mode. To disable the sending of the configuration inventory, use the **no** form of this command.

announce config
no announce config

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

CNS inventory configuration (cns_inv)

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to limit inventory requests by the CNS inventory agent. When configured, the routing device details will be announced on the CNS event bus, but the routing device will not respond to any queries from the CNS event bus.

Examples

The following example shows how to configure the CNS inventory agent to send out an unsolicited configuration inventory one time only at bootup:

```
Router(config)# cns inventory

Router(cns_inv)# announce config
```

Related Commands

Command	Description
cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.

clear cns config stats

To clear the statistics about the Cisco Networking Services (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.

Command Default

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 Cisco Networking Services (CNS) statistics, use the **clear cns counters** command in privileged EXEC mode.

clear cns counters

Syntax Description

This command has no arguments or keywords.

Command Default

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 Cisco Networking Services (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.

Command Default

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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.

clear cns image connections

To clear the Cisco Networking Services (CNS) image agent connections statistics, use the **clear cns image connections** command in privileged EXEC mode.

clear cns image connections

Syntax Description

This command has no arguments or keywords.

Command Default

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release XE 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

The **clear cns image connections** command clears all the statistics displayed by the **show cns image connections** command.

Examples

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

```
Router# clear cns image connections
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.

clear cns image status

To clear the Cisco Networking Services (CNS) image agent status statistics, use the **clear cns image status** command in privileged EXEC mode.

clear cns image status

Syntax Description

This command has no arguments or keywords.

Command Default

No statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

The **clear cns image status** command clears all the statistics displayed by the **show cns image status** command.

Examples

The following example shows how to clear all the status statistics for the CNS image agent:

```
Router# clear cns image status
```

Related Commands

Command	Description
show cns image status	Displays status information for the CNS image agent.

clear netconf

To clear network configuration protocol (NETCONF) statistics counters or NETCONF sessions and to free associated resources and locks, use the **clear netconf** command in privileged EXEC mode.

clear netconf {**counters**|**sessions**}

Syntax Description

counters	Clears the NETCONF statistics counters to zero.
sessions	Clears currently connected NETCONF sessions.

Command Default

NETCONF statistics counters are incremented and configured NETCONF sessions remain active.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to clear NETCONF statistics counters to zero, to clear all or specified NETCONF sessions and to disconnect and free associated resources and locks.

Examples

The following example shows how to clear all NETCONF counters:

```
Router# clear netconf counters
```

Related Commands

Command	Description
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

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 (config-templ-conn)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 the table below). 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 1: 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 aaa authentication

To enable Cisco Networking Services (CNS) Authentication, Authorization, and Accounting (AAA) options, use the **cns aaa authentication** command in global configuration mode. To explicitly disable CNS AAA options, use the **no** form of this command.

cns aaa authentication *authentication-method*
no cns aaa authentication *authentication-method*

Syntax Description

authentication-method	Specifies the AAA authentication method to be used.

Command Default

AAA is enabled when using CNS by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S

Usage Guidelines

Use the **cns aaa authentication** command to enable AAA when using CNS. When the **cns aaa authentication** command is configured, CNS notification messages sent to the device are rejected if they do not have sender credentials. By default, no authentication is enabled. This command must be enabled to configure AAA authentication for CNS messages. Use the **no cns aaa authentication** command to explicitly disable AAA support when using CNS.

Examples

The following example shows how to enable AAA authentication when using CNS:

```
Device(config)# cns aaa authentication method1
```

Related Commands

Command	Description
cns message format notification	Configures the message format for notification messages from a CNS device.

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.

Command Default

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.
show cns event connections	Displays the status of the CNS event agent connection.

cns config connect-intf

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

To specify the interface for connecting to the Cisco Networking Services (CNS) configuration engine, use the **cns config connect-intf** command in global configuration mode. To disable this interface for the connection, use the **no** form of this command.

cns config connect-intf *type number* [**ping-interval** *seconds*] [**retries** *number*]
no cns config connect-intf *type number*

Syntax Description

type	Type of connecting interface.
number	Number of the connecting interface.
ping-interval	(Optional) Specifies an interval between successive ping attempts.
seconds	(Optional) Interval between successive ping attempts, in seconds. Values are from 1 to 30. The default is 10.
retries	(Optional) Indicates that a ping will be retried a specified number of times.
number	(Optional) Number of times that a ping will be retried, in seconds. Values are from 1 to 30. The default is 5.

Command Default

Interfaces are not configured to connect to the CNS configuration engine.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(8)T	This command was replaced by the **cns connect** and **cns template connect** commands.
12.3(9)	This command was replaced by the **cns connect** and **cns template connect** commands.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration on the router finds the connecting interface, regardless of the slot in which the card resides or the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

Use this command to enter CSN Connect-interface configuration mode (config-cns-conn-if). Then use one of the following bootstrap-configuration commands to connect to the registrar for initial configuration:

- **config-cli** followed by commands that, used as is, configure the interface.
- **line-cli** followed by a command to configure modem lines to enable dialout and, after that, commands to configure the modem dialout line.

The **config-cli** command accepts the special directive character "**&**," which acts as a placeholder for the interface name. When the configuration is applied, the **&** is replaced with the interface name. Thus, for example, if we are able to connect using FastEthernet0/0, the **config-cli ip route 0.0.0.0 0.0.0.0 &** command generates the **ip route 0.0.0.0 0.0.0.0 FastEthernet0/0** command. Similarly, the **config-virtual terminal line (vty) cns id & ipaddress** command generates the **cns id FastEthernet0/0 ipaddress** command.

Examples

In the following example, the user connects to a configuration engine using the asynch interface and issues several commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotary-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli
 ...<other line commands>....
Router(config-cns-conn-if)# exit
```

These commands result in the following configuration being applied:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
cns config notify	Detects CNS configuration changes and sends an event containing the previous and current configuration.
cns config partial	Starts the CNS configuration agent, which provides CNS configuration services to Cisco IOS clients.

cns config initial

To enable the Cisco Networking Services (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-nameip-address*} **[encrypt]** [*port-number*] [**page** *page*] **[syntax-check] [no-persist]** [**source** *interface name*] [**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.
interface name	(Optional) Interface name 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.

Command Default

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 (config)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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(config)# 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.
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

Note Effective with Cisco IOS Release 15.1(1)T1, the **cns config notify** command is not available in Cisco IOS software.

To notify Cisco Networking Services (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]**

Cisco IOS Release 12.4(9)T or Later Releases
cns config notify diff [**interval** *minutes*] **[no_cns_events]** [**qlen** *number*]
no cns config notify diff [**interval** *minutes*] **[no_cns_events]** [**qlen** *number*]

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. **Note** This keyword is no longer available in Cisco IOS Release 12.4(9)T or later releases.
qlen *number*	(Optional) Specifies the number of configuration changes that must occur before the CNS agent is notified of the changes. The range is 1 to 1000. The default is 100.

Command Default

CNS agents do not receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.

Release	Modification
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.
12.4(9)T	The **old-format** and **all** keywords were removed. The **qlen** *number* keyword/attribute pair were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(1)T1	This command was removed.

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 configuration 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 configuration notify queue is full, subsequent events are dropped and a “lost” CNS configuration 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.

Use the **qlen** *number* keyword/argument pair to send configuration changes to the CNS agent only after the specified number of changes has occurred.

Examples

The following example shows how to configure the CNS agent to receive configuration change notifications for all configuration commands:

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

The following example shows how to configure the CNS agent to receive configuration change notifications only after 50 changes have been made:

```
Router(config)# cns config notify diff qlen 50
```

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-nameip-address*} [**encrypt**] [*port-number*] [**source** *interface name*] [**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.
interface name	(Optional) Interface name 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 (config)

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.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

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.

```
Device(config)# cns event 172.28.129.22
Device(config)# cns trusted-server config 172.28.129.40
Device(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 Cisco Networking Services (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-nameip-address*} **[encrypt]** [*port-number*] [**page** *page*] **[overwrite-startup]** [**retry** *retries* **interval** *seconds*] **[syntax-check] [no-persist]** [**source** *interface name*] [**status** *url*] **[event] [inventory]**

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.
overwrite-startup	(Optional) Replaces the startup configuration file. Does not apply to the running configuration file.
retry *retries*	(Optional) Specifies the retry interval. The range is 0 to 100. The default is 0.
interval *seconds*	(Optional) Specifies the time in seconds, before the next attempt to request the configuration of a device from a configuration server. The range is 1 to 3600.
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.
interface name	(Optional) Interface name of the source of the configuration.
status *url*	(Optional) Sends the configuration 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 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.

Command Default

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.
12.4(15)T	This command was modified. The **retry** *retries* and **interval** *seconds* keywords and arguments were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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.

You can use the optional **retry** and **interval** keywords to specify an amount of time in seconds to wait before attempting to retrieve a configuration from a trusted server. The number of retries is restricted to 100 to prevent the configuration agent from indefinitely attempting to reach an unreachable server. Use the keyboard combination **Ctrl-Shift-6** to abort this command.

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)# exit
Router# cns config retrieve 10.1.1.1
```

The following example shows how to request a configuration from a trusted server at 10.1.1.1 and to configure a CNS configuration retrieve interval:

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

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* [**retry-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 *interval-seconds*	(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.
retries *number-retries*	(Optional) Sets the number of times the CNS connect function will try to ping the CNS configuration engine. The default value is 3.
timeout *timeout-seconds*	(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.
sleep *sleep-seconds*	(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.

Command Default

No CNS connect profiles are defined.

Command Modes

Global configuration (config)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRD	This command was modified to allow users to reenter CNS connect configuration mode after configuring the CNS connect profile.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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. Multiple **discover** and **template** commands configured in a CNS connect profile are processed in the order in which they are entered.

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 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
```

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 dhcp

To enable Cisco Networking Service (CNS) with permission to process incoming DHCP Option 43 messages, use the **cns dhcp** command in global configuration mode. To disable this permission, use the **no** form of this command.

cns dhcp
no cns dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

The permission to process the incoming DHCP Option 43 message is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S
Cisco IOS XE Release 3.3SE	This command was integrated into Cisco IOS XE Release 3.3SE

Usage Guidelines

If you need to pass CNS configuration commands to the router via the DHCP option 43 message, the **cns dhcp** command enables the DHCP option 43 message that the CNS processes.

Examples

The following example shows how to enable permissions to process the incoming DHCP Option 43 message:

```
Router(config)# cns dhcp
```

Related Commands

Command	Description
wsma dhcp	Permits a WSMA to process the incoming DHCP Option 43 message.

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 {*hostnameip-address*} **[encrypt]** [*port-number*] **[backup]** [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** {*ipv4-addressipv6-addressinterface-name*}] [**clock-timeout** *time*] [**reconnect-time** *time*]
no cns event [{*hostnameip-address*}] [*port-number*] **[encrypt] [backup]** [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** {*ipv4-addressipv6-addressinterface-name*}] [**clock-timeout** *time*] [**reconnect-time** *time*]

Syntax Description

hostname	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 range is from 0 to 65535. 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 range is from 0 to 65535. The default is 3.
keepalive *seconds retry-count*	(Optional) Specifies a keepalive timeout, in seconds, and retry count.
source *interface-name*	(Optional) Indicates the interface name or IP address of the source for CNS communications.
ipv4-address	(Optional) IPv4 address of the source device.
ipv6-address	(Optional) IPv6 address of the source device.
interface-name	(Optional) Interface name of the source.

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 *time*	(Optional) Specifies the configurable upper limit of the maximum retry timeout, in seconds. • The range is from 1 to 65535. The default is 3600.

Command Default

No CNS event gateway is configured.

Command Modes

Global configuration (config)

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 integrated into Cisco IOS Release 12.2(2)XB and implemented on Cisco IAD2420 series Integrated Access Devices (IADs).
12.2(8)T	This command was modified. The **encrypt**, **init-retry**, **source**, and **force-fmt1** keywords were added.
12.3	This command was modified. The **reconnect-time** keyword was added.
12.3(1)	This command was modified. 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *ipv4-address* and *ipv6-address* arguments were added.

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 the 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.

If you configure CNS passwords using the **cns password** command, existing event connections will be closed and reopened.

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, config ID, or image ID used by CNS services.
cns password	Configures a CNS password.
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 [encrypt] [*port-number*] [**source** {*ipv4-addressipv6-address*|*interface-type number*}]
no cns exec [encrypt] [*port-number*] [**source** {*ipv4-addressipv6-address*|*interface-type number*}]

Syntax Description

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.
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.
ipv4-address	(Optional) IPv4 address of the source device.
ipv6-address	(Optional) IPv6 address of the source device.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

No CNS exec agent is configured.

Command Modes

Global configuration (config)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *ipv4-address* and *ipv6-address* arguments were added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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—is 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 used by Cisco Networking Services (CNS), 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.

cns id {*type number* {**ipaddress**|**mac-address**}|**hardware-serial**|**hostname**|**string** *string*|**udi**} [{**event**|**image**}]
no cns id {*type number* {**ipaddress**|**mac-address**}|**hardware-serial**|**hostname**|**string** *string*|**udi**} [{**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.
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.
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.
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.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)XB	This command was introduced on Cisco IAD2420 series IADs.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. The **dns-reverse** keyword was removed.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to set the unique ID for 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.

An IP address can be assigned to an interface, and **cns id** global configuration command can use this IP address as the CNS ID string.

When CNS ID configuration fails, the system defaults to the hostname of the Cisco IOS device as the unique ID.

To set the CNS event ID to the hostname of the Cisco IOS device, use the **no** form of this command with the **event** keyword. To set the CNS config ID to the hostname of the Cisco IOS device, use the **no** form of this command without the **event** keyword. To set the CNS image ID to the hostname 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. Any spaces in PID, VID, and SN values will be removed. To view the UDI for this product, use the **show inventory** command.

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 ipaddress 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 image

To configure the CNS image agent services, use the **cns image** command in global configuration mode. To disable the use of CNS image agent services, use the **no** form of this command.

cns image [**server** *server-url* [**status** *status-url*]]
no cns image [**server** *server-url* [**status** *status-url*]]

Syntax Description

server	(Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded.
server-url	(Optional) URL used to contact an image distribution server. An IP address or domain name can be used.
status	(Optional) Specifies that any status messages generated by CNS image agent operations will be sent to the URL specified by the *status-url* argument.
status-url	(Optional) URL of a web server to which status messages are written.

Command Default

When configured, the CNS image agent always listens for image events on the CNS Event Bus server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **cns image** command to start the CNS image agent process and to listen for image-related events on the CNS Event Bus.

If the optional server details are specified, the CNS image agent uses the server URL to contact the image management server. If no server details are specified, the URL for the image server must be supplied using one of the following three methods. The first method is to specify the image server using the server options on the **cns image retrieve** command. The second method is to use the server configured by the CNS event agent and stored as an image server event that can be received from the CNS Event Bus. The third method does not require a server URL because it uses CNS Event Bus mode.

If the optional status details are not specified, the status messages are sent as events on the CNS Event Bus.

Examples

The following example shows how to enable the CNS image agent services and configure a path to the image distribution server and a status messages server:

```
Router(config)# cns image server https://10.20.2.3:8080/cns/imageserver/
status https://10.20.2.3:8080/cns/imageserver/messages
/
```

Related Commands

Command	Description
show cns image status	Displays information about the CNS image agent status.

cns image password

To configure a password to use with the Cisco Networking Services (CNS) image agent services, use the **cns image password** command in global configuration mode. To disable the use of a password, use the **no** form of this command.

cns image password *image-password*
no cns image password *image-password*

Syntax Description

image-password	Password to be used for CNS image agent services.

Command Default

No password is used with the CNS image agent services.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to create a password that is sent with the image ID in all CNS image agent messages. The recipient of these messages can use this information to authenticate the sending device. This password may be different from the username and password used for HTTP basic authentication configured with other CNS image agent commands.

Examples

The following example shows how to configure a password to be used for the CNS image agent services:

```
Router(config)# cns image password textabc
```

Related Commands

Command	Description
cns id	Sets the unique event ID, config ID, or image ID used by CNS services.

cns image retrieve

To contact a Cisco Networking Services (CNS) image distribution server and download a new image if a new image exists, use the **cns image retrieve** command in privileged EXEC mode.

cns image retrieve [**server** *server-url* [**status** *status-url*]]

Syntax Description

server	(Optional) Specifies an image distribution server to contact for information about an updated image to be downloaded.
server-url	(Optional) URL used to contact an image distribution server.
status	(Optional) Specifies that any status messages generated by this command will be sent to the URL specified by the *status-url* argument.
status-url	(Optional) URL of a web server to which status messages are written.

Command Default

An error occurs when CNS image server has not previously been configured in global configuration mode.

Usage Guidelines

When the **cns image retrieve** command is issued in privileged EXEC mode without the **server** keyword and *server-url* argument, an error occurs.

When a CNS image server has been configured and the **cns image retrieve** command is issued with no **server** keyword and *server-url* argument, the server path configured in the **cns image** command is used.

When the **cns image** command is issued in global configuration mode with the optional **server** keyword, no keywords are required and no error occurs when you issue the **cns image retrieve** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

You must enable the CNS image agent services using the **cns image** command before configuring this command.

Use this command to poll an image distribution server and download a new image to the Cisco IOS device if a new image exists.

Examples

The following example shows how to configure the CNS image agent to access the image distribution server at 10.19.2.3 and download a new image if a new image exists:

```
Router# cns image retrieve server https://10.20.2.3:8080
/cns/imageserver/ status
https://10.20.2.3:8080/cns/imageserver/messages
/
```

Related Commands

Command	Description
cns image	Enables CNS image agent services.
cns trusted-server	Specifies a trusted server for CNS agents.
show cns image status	Displays information about the CNS image agent status.

cns image retry

To set the Cisco Networking Services (CNS) image upgrade retry interval, use the **cns image retry** command in global configuration mode. To restore the default value, use the **no** form of this command.

cns image retry *seconds*
no cns image retry *seconds*

Syntax Description

seconds	Integer in the range from 0 to 65535 that specifies the number of seconds in the interval. The default is 60 seconds.

Command Default

The default retry interval is 60 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to set an interval after which the CNS image agent will retry an image upgrade operation if the original upgrade attempt failed.

Examples

The following example shows how to set the CNS image upgrade interval to 240 seconds:

```
Router(config)# cns image retry 240
```

Related Commands

Command	Description
cns image	Enables CNS image agent services.

cns inventory

To enable the CNS inventory agent--that is, to send an inventory of the router's line cards and modules to the CNS configuration engine—and enter CNS inventory mode, use the **cns inventory** command in global configuration mode. To disable the CNS inventory agent, use the **no** form of this command.

cns inventory
no cns inventory

Syntax Description

This command has no arguments or keywords.

Command Default

The CNS inventory agent is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(1)	The **config**, **event**, and **notify oir** keywords were removed.
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.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command with the **announce config** and **transport event** CNS inventory configuration mode commands to specify when to notify the CNS configuration engine of changes to the router's port-adaptor and interface inventory. A transport must be specified in CNS inventory configuration mode before any of the CNS inventory commands are executed.

Examples

The following example shows how to enable the CNS inventory agent and enter CNS inventory configuration mode:

```
Router(config)# cns inventory
Router(cns_inv)#
```

Related Commands

Command	Description
announce config	Species that an unsolicited configuration inventory is sent out by the CNS inventory agent at bootup.
cns config initial	Starts the CNS configuration agent and initiates an initial configuration.
transport event	Species that inventory events are sent out by the CNS inventory agent.

cns message format notification

To configure the message format for notification messages from a Cisco Networking Services (CNS) device, use the **cns message format notification** command in global configuration mode. To unconfigure a configured message format for notification messages from a CNS device, use the **no** form of this command.

cns message format notification {**version 1**|**version 2**}
no cns message format notification {**version 1**|**version 2**}

Syntax Description

version 1	Configures CNS notification messages to use the non Service-Oriented Access Protocol (SOAP) format.
version 2	Configures CNS notification messages to use the SOAP format.

Command Default

Non-SOAP notification messages are used by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to configure a CNS agent to use the SOAP format for CNS notification messages. SOAP message formats are supported by default. If the Cisco IOS device receives a request in the non-SOAP message format, the response will be sent in the non-SOAP format. If the Cisco IOS device receives a request in the SOAP format, the response will be sent in the SOAP format. By default, notification messages that are sent without any corresponding request messages will be sent in both SOAP and non-SOAP formats.

When this command is configured, received CNS notification messages that do not conform to the configured message format are rejected.

If the **cns aaa authentication notification** command is already configured, then the sender's credentials will be authenticated. If the **cns message format notification** command is configured, then the notification messages will be sent as per the configured version number. The default configuration is the legacy non-SOAP format.

Examples

The following example shows how to configure CNS notification messages to use the SOAP format:

```
Router(config)# cns message format notification version 2
```

Related Commands

Command	Description
cns aaa authentication	Enables CNS AAA options.

cns mib-access encapsulation

To specify whether Cisco Networking Services (CNS) should use nongranular (Simple Network Management Protocol [SNMP]) or granular (Extensible Markup Language [XML]) encapsulation to access MIBs, use the **cns mib-access encapsulation** command in global configuration mode. To disable the currently specified encapsulation, use the **no** form of this command.

cns mib-access encapsulation {**snmp**|**xml** [**size** *bytes*]}
no cns mib-access encapsulation {**snmp**|**xml**}

Syntax Description

snmp	Enables nongranular (SNMP) encapsulation for MIB access.
xml	Enables granular (XML) encapsulation for MIB access.
size *bytes*	(Optional) Maximum size in bytes for response events. The default is 3072.

Command Default

For XML encapsulation, a maximum size of 3072 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
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.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Examples

The following example specifies that XML be used to access MIBs:

```
Router(config)# cns mib-access encapsulation xml
```

Related Commands

Command	Description
cns notifications encapsulation	Specifies whether CNS notifications should be sent using nongranular (SNMP) or granular (XML) encapsulation.

cns notifications encapsulation

To specify whether Cisco Networking Services (CNS) notifications should be sent using nongranular (Simple Network Management Protocol [SNMP]) or granular (Extensible Markup Language [XML]) encapsulation, use the **cns notifications encapsulation** command in global configuration mode. To disable the currently specified encapsulation, use the **no** form of this command.

cns notifications encapsulation {**snmp**|**xml**}
no cns notifications encapsulation {**snmp**|**xml**}

Syntax Description

snmp	Uses nongranular (SNMP) encapsulation to send notifications.
xml	Uses granular (XML) encapsulation to send notifications.

Command Default

CNS notifications are not sent using encapsulation.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
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.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Examples

The following example shows how to specify that granular notifications should be sent:

```
Router(config)# cns notifications encapsulation xml
```

Related Commands

Command	Description
cns mib-access encapsulation	Specifies whether CNS should use granular (XML) or nongranular (SNMP) encapsulation to access MIBs.

cns password

To configure a Cisco Networking Services (CNS) password, use the **cns password** command in global configuration mode. To disable the CNS password, use the **no** form of this command.

cns password *password*
no cns password *password*

Syntax Description

password	Any character string that specifies the CNS password.

Command Default

A CNS password is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(8)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

You must configure the CNS password the first time a router is deployed, and the CNS password must be the same as the bootstrap password set on the Configuration Engine (CE). If both the router and the CE bootstrap password use their default settings, a newly deployed router will be able to connect to the CE.

Once connected, the CE will change the CNS password from the bootstrap password to a random password. Network administrators must ensure not to change the CNS password. If the CNS password is changed, connectivity to the CE will be lost.

Examples

The following example shows how to set a CNS password named password1:

```
Router(config)# cns password password1
```

Related Commands

Command	Description
cns id	Sets a unique event ID, config ID, or image ID used by CNS services.

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 (config)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRD	This command was modified to allow users to reenter the CNS connect configuration mode after configuring the CNS connect profile.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
```

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 Cisco Networking Services (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**} *name*
no cns trusted-server {**all-agents**|**config**|**event**|**exec**|**image**} *name*

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.
name	A string that specifies the hostname or IP address of the trusted server.

Command Default

By default, only the implicit server strings are trusted.

The configuration of the CNS event agent's server string through the command-line interface (CLI) results in an implicit trust by all CNS agents. For the other CNS agents, the configuration of a server string using the CLI results in an implicit trust of the server for the specified agent. For example, **cns exec 10.2.1.2** implies the string 10.2.1.2 is implicitly trusted by the exec agent, and specifying **cns event 10.4.2.2** implies the string 10.4.2.2 is implicitly trusted by all the CNS agents.

Command Modes

Global configuration (config)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 results in an error message being displayed and an authentication failure reply extensible markup language (XML). For backwards compatibility

the configuration of a server address using the configuration CLI for a CNS agent results in an implicit trust of the server for the specified agent.

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 string 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 string.

The **cns trusted-server** command does not use Domain Name System (DNS). Instead a string comparison is done between the configured and implicit trusted servers and requested redirected 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, which maps though DNS to host.somedomain.com as a trusted server for all CNS agents:

```
Router# cns trusted-server all-agents 10.2.2.8
Router# cns trusted-server all-agents host
Router# cns trusted-server all-agents host.somedomain.com
```

The following example shows how to configure the string 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.

config-cli

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **config-cli** command is replaced by the **cli (cns)** command. See the **cli (cns)** command for more information.

To connect to the Cisco Networking Services (CNS) configuration engine using a specific type of interface, use the **config-cli** command in CNS Connect-interface configuration mode.

config-cli *type* [*number*] *interface-config-cmd*

Syntax Description

type	Type of interface. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
number	(Optional) Interface number. Indicates from which interface the IP or MAC address should be retrieved in order to define the unique ID.
interface-config-cmd	Command that configures the interface. The *type* argument must be configured before other interface configuration commands.

Command Default

No command lines are specified to configure the interface.

Command Modes

CNS connect-interface configuration (config-cns-conn-if)

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.
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

Begin by using the **cns config connect-intf** command to enter CNS Connect-interface configuration (config-cns-conn-if) mode. Then use either this or its companion CNS bootstrap-configuration command to connect to the CNS configuration engine for initial configuration:

- **config-cli** connects to the registrar using a specific type of interface. You must specify the interface type but need not specify the interface number; the router's bootstrap configuration finds the connecting interface, regardless of the slot in which the card resides, by trying different candidate interfaces until it can ping the configuration engine.
- **line-cli** connects to the registrar using modem dialup lines.

Immediately after either of the commands, enter additional configuration commands as appropriate.

Examples

The following example enters CNS Connect-interface configuration mode, connects to a configuration engine using an asynchronous interface, and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotary-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli
...<other line commands>....
Router(config-cns-conn-if)# exit
```

These commands apply the following configuration:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
line-cli	Connects to the CNS configuration engine using a modem dialup line.

discover (cns)

To define the interface parameters within a Cisco Networking Services (CNS) connect profile for connecting to the CNS configuration engine, use the **discover** command in CNS connect configuration mode. To disable this functionality, use the **no** form of this command.

discover {**line** *line-type*|**controller** *controller-type*|**interface** [*interface-type*]|**dlci** [**subinterface** *subinterface-number*]}
no discover {**line** *line-type*|**controller** *controller-type*|**interface** [*interface-type*]|**dlci** [**subinterface** *subinterface-number*]}

Syntax Description

line	Indicates that a line is used to connect to the CNS configuration engine. When the **line** *line-type* keyword and argument are specified, all the lines that create an interface that match the specified *line-type* argument are discovered. The CNS connect templates associated with the **discover line** *line-type* command are applied in line configuration mode.
line-type	Type of line used to connect to the CNS configuration engine.
controller	Indicates that a controller is used to connect to the CNS configuration engine. When the **controller** *controller-type* keyword and argument are specified, all the controllers that create an interface that match the specified *controller-type* argument are discovered. The CNS connect templates associated with the **discover controller** *controller-type* command are applied in controller configuration mode.
controller-type	Type of controller used to connect to the CNS configuration engine.
interface	Indicates that an interface is used to connect to the CNS configuration engine. If the **discover interface** *interface-type* command is the first **discover** command configured in a CNS connect profile, the interfaces that match the specified *interface-type* argument are discovered. If the **discover interface** *interface-type* command is configured after the **discover line** *line-type* or **discover controller** *controller-type* commands in a CNS connect profile, the specified *interface-type* argument is ignored. Instead, the CNS connect templates associated with the **discover interface** command are applied to all the interfaces associated with the preceding **discover line** *line-type* or **discover controller** *controller-type* commands. The CNS connect templates associated with the **discover interface** *interface-type* command are applied in interface configuration mode.
interface-type	(Optional) Type of interface used to connect to the CNS configuration engine.

dlci	Active DLCIs to be used for connecting to the CNS configuration engine. When this keyword is defined, all the active DLCIs are discovered on the interface specified by the preceding **discover interface** *interface-type* command. A Frame Relay LMI message will return a list of active DLCIs. Active DLCIs can only be discovered on interfaces configured with Frame Relay. Therefore, the location of the **discover dlci** command in a CNS connect profile is important. It must be entered after the interfaces have been configured with Frame Relay. The CNS connect templates associated with the **discover dlci** command are applied in subinterface (point-to-point) configuration mode. Defines the CNS connect variable **${dlci}** and **${next-hop}**. **Note** Any Cisco IOS command that requires knowledge of the active DLCIs must be configured after the **discover dlci** command.
subinterface	(Optional) Indicates that a point-to-point subinterface is used to perform a search for active DLCIs. If a number is not specified, the default value is 9999.
subinterface-number	(Optional) Number of the point-to-point subinterface used to perform a search for active DLCIs.

Command Default

No interface parameters within a CNS connect profile are defined.

Command Modes

CNS connect configuration (config-cns-conn)

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 **dlci subinterface** *subinterface-number* keywords and argument and the CNS connect variable **${dlci}** are not supported in this release.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

First 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 to apply to a router's configuration. The first **discover** command in a CNS connect profile defines the scope of interfaces

to be searched and used to perform the ping iterations for connecting to the CNS configuration engine. Subsequent **discover** commands limit this scope.

The search is based on discovering all the interfaces that match the specified line, controller, or interface type. The search is case-insensitive and allows for abbreviations. For example, the **discover interface Serial**, **discover interface Ser**, **discover interface serial**, and **discover interface ser** commands all match the serial interface.

Each **discover** command must have at least one unique CNS connect template associated with it. Specifically, the **template** command must be configured after configuring the **discover** command. The **discover** command specifies the configuration mode in which the CNS connect templates (specified by the **template** command that is associated with the **discover** command) are to be applied. When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

The table below provides a summary of the interface parameters that can be defined using the **discover** command.

Table 2: Summary of the discover Commands

discover Command	Description	Associated CNS Connect Variable	Configuration Mode in Which CNS Connect Templates Are Applied	Prerequisite discover Command	Required Subsequent discover Command
discover line *line-type*	Discovers all the lines that create an interface that match the specified *line-type* argument.	**${line}**	Line	—	**discover interface** *interface-type*
discover confgoller *controller-type*	Discovers all the controllers that create an interface that match the specified *controller-type* argument.	**${controller}**	Controller	—	**discover interface** *interface-type*

discover Command	Description	Associated CNS Connect Variable	Configuration Mode in Which CNS Connect Templates Are Applied	Prerequisite discover Command	Required Subsequent discover Command
discover interface[*interface-type*]	• If this is the first **discover** command configured, then all the interfaces that match the specified *interface-type* argument are discovered. • If configured after the **discover line** *line-type* or **discover controller** *controller-type* commands, then the specified *interface-type* argument is ignored.	**${interface}** **${next-hop}**	Interface	—	—
discover dlci [**subinterface** *subinterface-number*]	Discovers all active DLCIs on the interface specified by the preceding **discover interface** command.	**${dlci}** **${next-hop}**	Subinterface (point-to-point)	**discover interface** *interface-type*	—

CNS connect variables can be used as placeholders within a CNS connect template configuration. Each variable is defined by an associated **discover** command (see the table above and the table below). 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, 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.

Table 3: Summary of the CNS Connect Variables

Variable	Description
${line}	The line type defined by the associated **discoverline** *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.

Variable	Description
${next-hop}	The next hop interface. This variable is identical to the **${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 create a CNS connect profile named EG:

```
Router (config)# cns connect EG
Router (config-cns-conn)# discover controller T1
Router (config-cns-conn)# template timeslot-1
Router (config-cns-conn)# discover interface
Router (config-cns-conn)# template frame
Router (config-cns-conn)# exit
Router (config)#
```

In this example, the following sequence of events occur for each T1 controller when the **cns connect EG** command is processed:

1. Enter controller configuration mode and apply all commands in the timeslot-1 template to the router's configuration.
2. For each interface associated with each T1 controller:
    1. Enter interface configuration mode and apply all commands in the frame 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 EG** command has completed its process.
    4. If the ping is unsuccessful, enter interface configuration mode and remove all commands in the frame template from the router's configuration.
3. Enter controller configuration mode and remove all commands in the timeslot-1 template from the router's configuration. The **cns connect EG** 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 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.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

F through T Commands

format global

To specify a default Operational Data Model (ODM) specification file other than the built-in specification file for XML-formatted requests, use the **format global** command in global configuration mode. To remove the default file, use the **no** form of this command.

format global *location*:*local-filename*
no format global

Syntax Description

location:*local-filename*	Command ODM file location and filename. Valid locations are **bootflash:**, **flash:**, **nvram:**, and any valid disk or slot number (such as **disk0:** or **slot1:**). ODM spec files have a .odm suffix.

Command Default

The built-in spec file is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **format global** command to specify an ODM spec file as the default for all XML-formatted requests coming from NETCONF operations. The NETCONF file search precedence is to look first for the file associated by the **netconf format** command, then for the file defined by the **format global** command, and finally for the built-in spec file.

The ODM spec file must exist on the files ystem before NETCONF can be configured to use it. If the file does not exist, the **format global** command is rejected.

Examples

The following example shows how to define a default ODM file to be used for all requests, then associates that file with NETCONF for all XML-formatted requests. If no file is specified, the built-in spec file is used for all requests:

```
Router(config)# format global disk0:spec3.3.odm
Router(config)# netconf format disk2:spec3.3.odm
```

Related Commands

Command	Description
netconf format	Associates NETCONF with an ODM spec file for XML-formatted requests.
spec-file install built-in	Replaces the current spec file with the built-in spec file.
spec-file install file	Replaces a local spec file with a remote spec file.

kron occurrence

To specify schedule parameters for a Command Scheduler occurrence and enter kron-occurrence configuration mode, use the **kron occurrence** command in global configuration mode. To delete a Command Scheduler occurrence, use the **no** form of this command.

kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays* **:**] *numhours* **:**] *nummin*|**at** *hours* **:** *min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot**|**recurring**|**system-startup**}
no kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays* **:**] *numhours* **:**] *nummin*|**at** *hours* **:** *min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot**|**recurring**|**system-startup**}

Syntax Description

occurrence-name	Name of the occurrence. The length of *occurrence-name* is from 1 to 31 characters. If the *occurrence-name* is new, an occurrence structure will be created. If the *occurrence-name* is not new, the existing occurrence will be edited.
user	(Optional) Identifies a particular user.
username	(Optional) Name of the user.
in	Indicates that the occurrence is to run after a specified time interval. The timer starts when the occurrence is configured.
numdays **:**	(Optional) Number of days. If used, add a colon after the number.
numhours **:**	(Optional) Number of hours. If used, add a colon after the number.
nummin	Number of minutes.
at	Indicates that the occurrence is to run at a specified calendar date and time.
hours **:**	Hour as a number using the twenty-four hour clock. Add a colon after the number.
min	Minute as a number.
month	(Optional) Month name. If used, you must also specify *day-of-month*.
day-of-month	(Optional) Day of month as a number.
day-of-week	(Optional) Day of week name.
oneshot	Indicates that the occurrence is to run only one time. After the occurrence has run, the configuration is removed.
recurring	Indicates that the occurrence is to run on a recurring basis.
system-startup	Indicates that the occurrence is to run on system startup, in addition to the **recurring** or **oneshot** occurrences.

Command Default

No schedule parameters are specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified. The **system-startup** keyword was added. The **user** keyword and *username* argument were removed from this command in Cisco IOS Release 12.4(15)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Prior to Cisco IOS Release 12.4, when you configured a kron occurrence for a calendar time when the system clock was not set, you received a printf message stating that the clock was not set and the occurrence would not be scheduled until it was set.

Beginning in Cisco IOS Release 12.4, when you configure a kron occurrence for a calendar time when the system clock is not set, the occurrence is scheduled but a printf message appears stating that the clock is not set and that it currently reads <current clock time>.

If you set the clock, the schedule of the occurrence is affected in one of the following ways:

- A new clock time set for less than 3 hours after the occurrence is scheduled to happen causes the occurrence to happen immediately.
- A new clock time set for less than 3 hours before the occurrence is scheduled to happen causes the occurrence to happen as scheduled.
- A new clock time set for more than 3 hours after the occurrence is scheduled to happen causes the occurrence to be rescheduled for the next regular calendar time.
- A new clock time set for more than 3 hours before the occurrence is scheduled to happen causes the occurrence to be rescheduled for the previous regular calendar time.

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command-line interface (CLI) commands to be scheduled to run on the router at a specified time.

Use the **show kron schedule** command to display the name of each configured occurrence and when it will next run.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named info-three and schedule it to run every three days, 10 hours, and 50 minutes. The EXEC CLI in the policy named three-day-list is configured to run as part of occurrence info-three.

```
Router(config)# kron occurrence info-three user IT2 in 3:10:50 recurring
Router(config-kron-occurrence)# policy-list three-day-list
```

The following example shows how to create a Command Scheduler occurrence named auto-mkt and schedule it to run once on June 4 at 5:30 a.m. The EXEC CLI in the policies named mkt-list and mkt-list2 are configured to run as part of occurrence auto-mkt.

```
Router(config)# kron occurrence auto-mkt user marketing at 5:30 jun 4 oneshot
Router(config-kron-occurrence)# policy-list mkt-list
Router(config-kron-occurrence)# policy-list mkt-list2
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.
show kron schedule	Displays the status and schedule information for Command Scheduler occurrences.

kron policy-list

To specify a name for a Command Scheduler policy and enter kron-policy configuration mode, use the **kron policy-list** command in global configuration mode. To delete the policy list, use the **no** form of this command.

kron policy-list *list-name*
no kron policy-list *list-name*

Syntax Description

list-name	String from 1 to 31 characters that specifies the name of the policy.

Command Default

If the specified list name does not exist, a new policy list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command-line interface (CLI) commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

When the *list-name* is new, a policy list structure is created. When the *list-name* is not new, the existing policy list is edited.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a policy named sales-may and configure EXEC CLI commands to run the CNS command that retrieves an image from a server:

```
Router(config)# kron policy-list sales-may
Router(config-kron-policy)# cli cns image retrieve server
https://10.21.2.3/imgsvr/ status https://10.21.2.5/status/
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

line-cli

Note Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **line-cli** command is replaced by the **cli (cns)** command. See the **cli (cns)** command for more information.

To connect to the Cisco Networking Services (CNS) configuration engine using a modem dialup line, use the **line-cli** command in CNS Connect-interface configuration mode.

line-cli {*modem-cmdline-config-cmd*}

Syntax Description

modem-cmd	Modem line command that enables dialout. Indicates from which line or interface the IP or MAC address should be retrieved in order to define the unique ID.
line-config-cmd	Command that configures the line. The *modem-cmd* argument must be configured before other line configuration commands.

Command Default

No command lines are specified to configure modem lines.

Command Modes

CNS connect-interface configuration (config-cns-conn-if)

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.
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.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a modem dialout line. The bootstrap configuration on the router finds the connecting interface, regardless of the slot in which the card resides or the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

Enter this command to enter CNS Connect-interface configuration (config-cns-conn-if) mode. Then use one of the following bootstrap-configuration commands to connect to the registrar for initial configuration:

- **config-cli** followed by commands that, used as is, configure the interface.

- **line-cli** followed by a command to configure modem lines to enable dialout and, after that, commands to configure the modem dialout line.

The **config-cli** command accepts the special directive character "**&**," which acts as a placeholder for the interface name. When the configuration is applied, the **&** is replaced with the interface name. Thus, for example, if we are able to connect using FastEthernet0/0, the following is the case:

- The **config-cli ip route 0.0.0.0 0.0.0.0 &** command generates the **config ip route 0.0.0.0 0.0.0.0 FastEthernet0/0** command.
- The **cns id & ipaddress** command generates the **cns id FastEthernet0/0 ipaddress** command.

Examples

The following example enters CNS Connect-interface configuration mode, connects to a configuration engine using an asynchronous interface, and issues a number of commands:

```
Router(config)# cns config connect-intf Async
Router(config-cns-conn-if)# config-cli encapsulation ppp
Router(config-cns-conn-if)# config-cli ip unnumbered FastEthernet0/0
Router(config-cns-conn-if)# config-cli dialer rotart-group 0
Router(config-cns-conn-if)# line-cli modem InOut
Router(config-cns-conn-if)# line-cli
...<other line commands>...
Router(config-cns-conn-if)# exit
```

These commands apply the following configuration:

```
line 65
modem InOut
.
.
.
interface Async65
encapsulation ppp
dialer in-band
dialer rotary-group 0
```

Related Commands

Command	Description
cns config connect-intf	Specifies the interface for connecting to the CNS configuration engine.
config-cli	Connects to the CNS configuration engine using a specific type of interface.

logging cns-events

To enable extensible markup language (XML)-formatted system event message logging to be sent through the Cisco Networking Services (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

Command Default

Level 7: debugging

Command Modes

Global configuration (config)

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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.

netconf beep initiator

To configure Blocks Extensible Exchange Protocol (BEEP) as the transport protocol for Network Configuration Protocol (NETCONF) and to configure a peer as the BEEP initiator, use the **netconf beep initiator** command in global configuration mode. To disable the BEEP initiator, use the **no** form of this command.

netconf beep initiator {*hostname ip-address*} *port-number* **user** *sasl-user* **password** *sasl-password* [**encrypt** *trustpoint*] [**reconnect-time** *seconds*]
no netconf beep initiator {*hostname ip-address*} *port-number*

Syntax Description

hostname	Hostname of the remote device. Spaces and special characters cannot be used in hostnames. An error message is displayed if the syntax of the hostname is not appropriate.
ip-address	IP address of the remote device.
port-number	Specifies the BEEP port to use. The valid range is 1 to 65535.
user *sasl-user*	Specifies the Simple Authentication and Security Layer (SASL) user on the far end for this NETCONF session.
password *sasl-password*	Sets the password for the SASL user on the far end.
encrypt *trustpoint*	(Optional) Configures transport layer security (TLS) on this NETCONF session.
reconnect-time *seconds*	(Optional) Specifies the retry timeout, in seconds, for the NETCONF session. The range is from 3 to 3600.

Command Default

BEEP is not enabled as the transport protocol for NETCONF sessions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **netconf beep initiator** command to specify BEEP as the transport protocol for NETCONF sessions and to specify a peer as the BEEP initiator.

BEEP is a peer-to-peer client-server protocol. Each peer is labeled in the context of the role it plays at a given time. When a BEEP session is established, the peer that awaits new connections is the BEEP listener. The other peer, which establishes a connection to the listener, is the BEEP initiator. The BEEP peer that starts an

exchange is the client; similarly, the other BEEP peer is the server. Typically, a BEEP peer that acts in the server role also performs in the listening role. However, because BEEP is a peer-to-peer protocol, the BEEP peer that acts in the server role is not required to also perform in the listening role.

Use the optional **encrypt** keyword to configure BEEP to use TLS to provide simple security for NETCONF sessions.

If an invalid hostname is specified for the remote device, an error message is displayed.

Examples

The following example shows how to enable NETCONF over BEEP and to configure a BEEP peer as the BEEP initiator:

```
!
hostname myhost
ip domain-name mydomain.com
ntp server myntpserver.mydomain.com
!generate RSA key pair
crypto key generate rsa general-keys
!do this only once - 1024 bytes
!config a trust point
crypto pki trustpoint mytrustpoint
 enrollment url http://10.10.10.10
 subject-name CN=myhost.mydomain.com
 revocation-check none
!get self signed cert
 crypto pki authenticate mytrustpoint
!get own certificate
 crypto pki enroll mytrustpoint
 netconf beep initiator host1 23 user user1 password password1 encrypt mytrustpoint
reconnect-time 60
```

Related Commands

Command	Description
netconf beep listener	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP listener.

netconf beep listener

To configure Blocks Extensible Exchange Protocol (BEEP) as the transport protocol for Network Configuration Protocol (NETCONF) and to configure a peer as the BEEP listener, use the **netconf beep listener** command in global configuration mode. To disable the BEEP listener, use the **no** form of this command.

netconf beep listener [{*port-number*}] [**acl** *access-list-number*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*]
no netconf beep listener

Syntax Description

port-number	(Optional) Specifies which BEEP port on which to listen.
acl *access-list-number*	(Optional) Specifies the access control list to be applied to restrict incoming client connections.
sasl *sasl-profile*	(Optional) Configures a Simple Authentication and Security Layer (SASL) profile to use during session establishment.
encrypt *trustpoint*	(Optional) Configures transport layer security (TLS) on a NETCONF session.

Command Default

BEEP is not enabled as the transport protocol for NETCONF sessions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **netconf beep listener** command to specify BEEP as the transport protocol for NETCONF sessions and to specify a peer as the BEEP listener.

BEEP is a peer-to-peer client-server protocol. Each peer is labeled in the context of the role it plays at a given time. When a BEEP session is established, the peer that awaits new connections is the BEEP listener. The other peer, which establishes a connection to the listener, is the BEEP initiator. The BEEP peer that starts an exchange is the client; similarly, the other BEEP peer is the server. Typically, a BEEP peer that acts in the server role also performs in the listening role. However, because BEEP is a peer-to-peer protocol, the BEEP peer that acts in the server role is not required to also perform in the listening role.

You must configure an SASL profile before you can configure NETCONF over BEEP to use SASL during session establishment.

Examples

The following example shows how to configure NETCONF over BEEP and to specify a peer as the BEEP listener:

```
Router(config)# sasl profile beep
 mechanism digest-md5
 server user user1 password password1
 exit
Router(config)# netconf beep listener 23 acl 1 sasl beep encrypt 25
```

Related Commands

Command	Description
netconf beep initiator	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP initiator.

netconf detailed-error

To display helpful return codes if an invalid command is executed in a network configuration protocol (NETCONF) session, use the **netconf detailed-error** command in global configuration mode. To stop displaying the return codes, use the **no** form of this command.

netconf detailed-error
no netconf detailed-error

Command Default

NETCONF does not send return codes for invalid command execution.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **netconf detailed-error** command configures NETCONF to send a "NOT OK" return code if you attempt to execute an invalid command.

For **show** commands, the return code appears in this form:

```
<return-code>NOT OK</return-code>
```

For configuration commands, the return code includes the line number of the invalid command. This example includes the request and the response, to illustrate:

```
Request:-
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
<target>
<running/>
</target>
<config>
<cli-config-data>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>interface nve 1</cmd>
<cmd>member vni 5005</cmd>
<cmd>ingress-replication 1.1.1.1</cmd>
```

```
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
<cmd>hostname POLARIS-skaliath</cmd>
</cli-config-data>
</config>
</edit-config>
</rpc>]]>]]>

Response:-
<?xml version="1.0" encoding="UTF-8"?><rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><rpc-error>
<error-type>protocol</error-type><error-tag>operation-failed</error-tag>
<error-severity>error</error-severity><error-message>
**CLI Line # 20: % VNI 5005 already exists on other nve
interface</error-message></rpc-error></rpc-reply>]]>]]>
```

Note For a series of commands provided in an input XML:

- If NETCONF attempts to execute a series of **show** commands and it encounters an invalid command, NETCONF does not stop execution. It continues to execute any other commands in the input XML, and provides the error return code(s) for invalid commands in the output.
- If NETCONF attempts to execute a series of **configuration** commands and it encounters an invalid command, NETCONF stops execution. It provides the error return code for the invalid command, including line number, in the output.

Examples

Enabling detailed error reporting on a device:

```
Device(config)# netconf detailed-error
```

Related Commands

Command	Description
netconf beep initiator	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP initiator.
netconf beep listener	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP listener.
netconf format	Associates NETCONF with an ODM spec file for XML-formatted requests.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.

netconf format

To associate Network Configuration Protocol (NETCONF) with an Operational Data Model (ODM) specification file for XML-formatted requests, use the **netconf format** command in global configuration mode. To remove the association, use the **no** form of this command.

netconf format *location*:*local-filename*
no netconf format

Syntax Description

location:*local-filename*	Command ODM file location and filename. Valid locations are **bootflash:**, **flash:**, **nvram:**, and any valid disk or slot number (such as **disk0:** or **slot1:**). ODM spec files have a .odm suffix.

Command Default

The spec file defined by the **format global** command is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **netconf format** command to make an association with NETCONF to use the specified ODM spec file for all XML-formatted requests coming from NETCONF operations.

The ODM spec file must exist on the files ystem before NETCONF can be configured to use it. If the file does not exist, the **netconf format** command is rejected.

Examples

The following example shows how to associate a file named spec3.3.odm with NETCONF:

```
Router(config)# netconf format disk0:spec3.3.odm
```

Related Commands

Command	Description
netconf lock-time	Limits the amount of time NETCONF can lock a configuration.
netconf max-sessions	Limits the total number of NETCONF sessions.

Command	Description
netconf ssh	Enables NETCONF over SSHv2.

netconf lock-time

To specify the maximum time a network configuration protocol (NETCONF) configuration lock is in place without an intermediate operation, use the **netconf lock-time** command in global configuration mode. To set the NETCONF configuration lock time to the default value, use the **no** form of this command.

netconf lock-time *seconds*
no netconf lock-time

Syntax Description

seconds	Maximum NETCONF session time in seconds. The valid range is 1 to 300 seconds. The default is 10 seconds.

Command Default

The maximum lock time for a NETCONF session is 10 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

NETCONF enables you to set a configuration lock. Setting a configuration lock allows you to have exclusive rights to the configuration in order to apply configuration changes. Other users will not have access to the console during the lock time. If the user who has enabled the configuration lock is inactive, the lock timer expires and the session is ejected, preventing the configuration from being locked out if the user loses network connectivity while they have the configuration locked.

Examples

The following example shows how to limit a NETCONF configuration lock to 60 seconds:

```
Router(config)# netconf lock-time 60
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.

Command	Description
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf max-message

To specify the maximum size of messages received in a network configuration protocol (NETCONF) session, use the **netconf max-message** command in global configuration mode. To set an infinite message size for the messages received, use the **no** form of this command.

netconf max-message *size*
no netconf max-message

Syntax Description

size	Specifies the maximum message size, in kilobytes (kB), for the messages received. The valid range in is from 1 to 2147483.

Command Default

The maximum message size is set to infinite.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **netconf max-message** command specifies the maximum amount of memory required to be allocated to messages received in a NETCONF session. To protect the device against denial-of-service (DOS) attacks (that is, cases where the device runs out of memory for routing tasks) ensure the maximum size is not set to be very big. The **no netconf max-message** command sets the maximum message size to an infinite value.

Examples

The following example shows how to configure a maximum size of 37283 KB for messages received in a NETCONF session:

```
Router# configure terminal
Router(config)# netconf max-message 37283
```

Related Commands

Command	Description
netconf beep initiator	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP initiator.
netconf beep listener	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP listener.
netconf format	Associates NETCONF with an ODM spec file for XML-formatted requests.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.

Command	Description
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.

netconf max-sessions

To specify the maximum number of concurrent network configuration protocol (NETCONF) sessions allowed, use the **netconf max-sessions** command in global configuration mode. To reset the number of concurrent NETCONF sessions allowed to the default value of four sessions, use the **no** form of this command.

netconf max-sessions *session*
no netconf max-sessions

Syntax Description

session	Specifies the total number of concurrent NETCONF sessions allowed. The default is 4. The range is 4 to 16.

Command Default

Four concurrent NETCONF sessions are allowed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

You can have multiple NETCONF Network Managers concurrently connected. The **netconf max-sessions** command allows the maximum number of concurrent NETCONF sessions. The number of NETCONF sessions is also limited by the amount of available of vty line configured.

Note There must be at least as many vty lines configured as there are concurrent NETCONF sessions.

Extra NETCONF sessions beyond the maximum are not accepted.

Examples

The following example allows a maximum of five concurrent NETCONF sessions:

```
Router(config)# netconf max-sessions 5
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.

Command	Description
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf ssh

To enable Network Configuration Protocol (NETCONF) over Secure Shell Version 2 (SSHv2), use the **netconf ssh** command in global configuration mode. To disable NETCONF over SSHv2, use the **no** form of this command.

netconf ssh [**acl** *access-list-number*]
no netconf ssh

Syntax Description

acl	(Optional) Specifies an access list to use during NETCONF sessions.
access-list-number	Number of the access list to use during NETCONF sessions.

Command Default

NETCONF over SSHv2 is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

NETCONF is supported only on SSHv2.

Examples

The following example shows how to enable NETCONF over SSHv2 and apply access list 1 to NETCONF sessions:

```
Router(config)# netconf ssh acl 1
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.

Command	Description
show netconf	Displays NETCONF statistics counters and session information.

policy-list

To associate a policy list with a Command Scheduler occurrence, use the **policy-list** command in kron-occurrence configuration mode. To delete a policy list from the Command Scheduler occurrence, use the **no** form of this command.

policy-list *list-name*
no policy-list *list-name*

Syntax Description

list-name	Name of the policy list.

Command Default

No policy list is associated.

Command Modes

Kron-occurrence configuration (kron-config-occurrence)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.

Usage Guidelines

Use the **policy-list** command with the **kron occurrence** command to schedule one or more policy lists to run at the same time or interval. Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy list containing EXEC command line interface (CLI) commands to be scheduled to run on the router at a specified time.

When the *list-name* is new, a policy list structure is created. When the *list-name* is not new, the existing policy list is edited.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and can it be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named may and associate a policy list named sales-may with the occurrence:

```
Router(config)# kron occurrence may at 6:30 may 20 oneshot
Router(config-kron-occurrence)# policy-list sales-may
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.

show cns config connections

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

show cns config 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. This command replaces the **show cns config status** command.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **show cns config connections** command to determine whether the CNS event agent 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 is sample output from the **show cns config connections** command:

```
Router# show cns config connections

The partial configuration agent is enabled.
Configuration server:  10.1.1.1
Port number:           80
Encryption:            disabled
Config id:             test1
Connection Status:     Connection not active.
```

Related Commands

Command	Description
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.
show cns config stats	Displays statistics about the CNS configuration agent.
show cns config status	Displays the status of the CNS Configuration Agent.

show cns config outstanding

To display information about incremental (partial) Cisco Networking Services (CNS) configurations that have started but not yet completed, use the **show cns config outstanding** command in privileged EXEC mode.

show cns config outstanding

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show cns config outstanding** command to display information about outstanding incremental (partial) configurations that have started but not yet completed, including the following:

- Queue ID (location of configuration in the config queue)
- Identifier (group ID)
- Config ID (identity of configuration within the group)

Examples

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

```
Router# show cns config outstanding

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

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
config-cli	Displays the status of the CNS event agent connection.
show cns config stats	Displays statistics about the CNS configuration agent.

show cns config stats

To display statistics about the Cisco Networking Services (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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 config status

Note Effective with Cisco IOS Release 12.2(8)T, the **show cns config status** command is replaced by the **show cns config connections** command. See the **show cns config connections** command for more information.

To display the status of the Cisco Networking Services (CNS) Configuration Agent, use the **show cns config status** command in EXEC mode.

show cns config status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was replaced by the **show cns config connections** command.
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(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command displays the status of the Configuration Agent. Use this option to display the following information about the Configuration Agent:

- Status of the Configuration Agent, for example, whether it has been configured properly.
- IP address and port number of the trusted server that the Configuration Agent is using.
- Config ID (identity of configuration within the configuration group).

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.
show cns config connections	Displays the status of the CNS event agent connection.

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

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.

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

show cns event gateway

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event gateway** command in EXEC mode.

show cns event gateway

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display the following information about CNS gateways:

- Primary gateway:
  - IP address
  - Port number
- Backup gateways:
  - IP address
  - Port number
- Currently connected gateway:
  - IP address
  - Port number

The following is sample output for the **show cns event gateway** command:

```
Router# show cns event gateway

The currently configured primary event gateway:
        ip address is 10.0.0.0.
        port number is 11011.
The currently configured backup event gateway:
        none.

The currently connected event gateway:
        ip address is 10.0.0.0.
        port number is 11011.
```

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event stats

To display statistics about the Cisco Networking Services (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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 status

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event status** command in EXEC mode.

show cns event status

Syntax Description

This command has no arguments or keywords.

Command Modes

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display the following information about the CNS Event Agent:

- Status of Event Agent:
  - Connected
  - Active
- Gateway used by the Event Agent:
  - IP address
  - Port number
- Device ID

The following is sample output for the **show cns event status** command:

```
Router# show cns event status

The event agent is configured.
The following gateway is used by event agent
   Event Gateway    10.00.00.00
   Port number      11011
```

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

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.

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

show cns image connections

To display the status of the Cisco Networking Services (CNS) image management server HTTP connections, use the **show cns image connections** command in privileged EXEC mode.

show cns image connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **show cns image connections** command when troubleshooting HTTP connection problems with the CNS image server. The output displays the following information:

- Number of connection attempts
- Number of connections that were never connected and those that were abruptly disconnected
- Date and time of last successful connection

Examples

The following is sample output from the **show cns image connections** command:

```
Router# show cns image connections

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

Related Commands

Command	Description
show cns image inventory	Displays inventory information about the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image inventory

To provide a dump of Cisco Networking Services (CNS) image inventory information in extensible markup language (XML) format, use the **show cns image inventory** command in privileged EXEC mode.

show cns image inventory

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

To view the XML output in a better format, paste the content into a text file and use an XML viewing tool.

Examples

The following is sample output from the **show cns image inventory** command:

```
Router# show cns image inventory

Inventory Report
<imageInventoryReport><deviceName><imageID>Router</imageID><hostName>Router</ho
IOS (tm) C2600 Software (C2600-I-M), Experimental Version 12.3(20030414:081500)]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Apr-03 02:03 by engineer</versionString><imageFile>tftp://10.25>
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image status

To display status information about the Cisco Networking Services (CNS) image agent, use the **show cns image status** command in privileged EXEC mode.

show cns image status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to display the following status information about the CNS image agent:

- Start date and time of last upgrade
- End date and time of last upgrade
- End date and time of last successful upgrade
- End date and time of last failed upgrade
- Number of failed upgrades
- Number of successful upgrades with number of received messages and errors
- Transmit status with number of attempts, successes, and failures

Examples

The following is sample output from the **show cns image status** command:

```
Router# show cns image status

Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS
Last successful upgrade ended at 00:00:00.000 UTC Mon May 6 2003
Last failed upgrade ended at 00:00:00.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
```

```
 messages received: 12
 receive errors: 5
Transmit Status
  TX Attempts:4
    Successes:3         Failures 2
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image inventory	Displays image inventory information in XML format.

show kron schedule

To display the status and schedule information of Command Scheduler occurrences, use the **show kron** schedule command in user EXEC or privileged EXEC mode.

show kron schedule

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Use the **show kron schedule** command to view all currently configured occurrences and when they are next scheduled to run.

Examples

The following sample output displays each configured policy name and the time interval before the policy is scheduled to run:

```
Router# show kron schedule

Kron Occurrence Schedule
week inactive, will run again in 7 days 01:02:33
may inactive, will run once in 32 days 20:43:31 at 6:30 on Jun 20
```

The table below describes the significant fields shown in the display.

Table 4: show kron schedule Field Descriptions

Field	Description
week inactive	The policy list named week is currently inactive.
run again in 7 days 01:02:33	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run on a recurring basis.

Field	Description
run once in 32 days 20:43:31	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run just once.

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

show netconf

To display network configuration protocol (NETCONF) information, use the **show netconf** command in privileged EXEC mode.

show netconf {**counters**|**session**|**schema**}

Syntax Description

counters	Displays NETCONF statistics and informational counters.
session	Displays the current state of all connected NETCONF sessions across all transports and any resources and locks in use by the session.
schema	Displays the NETCONF schema.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(20)T	This command was modified. The **schema** keyword was added.

Examples

The following is sample output from the **show netconf counters** command:

```
Router# show netconf counters

NETCONF Counters
Connection Attempts:0: rejected:0 no-hello:0 success:0
Transactions
        total:0, success:0, errors:0
detailed errors:
        in-use 0        invalid-value 0         too-big 0
        missing-attribute 0     bad-attribute 0         unknown-attribute 0
        missing-element 0       bad-element 0   unknown-element 0
        unknown-namespace 0     access-denied 0         lock-denied 0
        resource-denied 0       rollback-failed 0       data-exists 0
        data-missing 0  operation-not-supported 0       operation-failed 0
        partial-operation 0
```

The following is sample output from the **show netconf session** command:

```
Router# show netconf session
```

```
(Current | max) sessions:   3 | 4
Operations received: 100              Operation errors: 99
Connection Requests: 5                Authentication errors: 2   Connection Failures: 0
ACL dropped : 30
Notifications  Sent: 20
```

The output of the **show netconf schema** command describes the element structure for a NETCONF request and the resulting reply. This schema can be used to construct proper NETCONF requests and parse the resulting replies. The nodes in the schema are defined in RFC 4741. The following is sample output from the **show netconf schema** command:

```
Router# show netconf schema

New Name Space 'urn:ietf:params:xml:ns:netconf:base:1.0'
<VirtualRootTag> [0, 1] required
  <rpc-reply> [0, 1] required
    <ok> [0, 1] required
    <data> [0, 1] required
    <rpc-error> [0, 1] required
      <error-type> [0, 1] required
      <error-tag> [0, 1] required
      <error-severity> [0, 1] required
      <error-app-tag> [0, 1] required
      <error-path> [0, 1] required
      <error-message> [0, 1] required
      <error-info> [0, 1] required
        <bad-attribute> [0, 1] required
        <bad-element> [0, 1] required
        <ok-element> [0, 1] required
        <err-element> [0, 1] required
        <noop-element> [0, 1] required
        <bad-namespace> [0, 1] required
        <session-id> [0, 1] required
  <hello> [0, 1] required
    <capabilities> 1 required
      <capability> 1+ required
  <rpc> [0, 1] required
    <close-session> [0, 1] required
    <commit> [0, 1] required
      <confirmed> [0, 1] required
      <confirm-timeout> [0, 1] required
    <copy-config> [0, 1] required
      <source> 1 required
        <config> [0, 1] required
          <cli-config-data> [0, 1] required
            <cmd> 1+ required
          <cli-config-data-block> [0, 1] required
          <xml-config-data> [0, 1] required
            <Device-Configuration> [0, 1] required
              <> any subtree is allowed
        <candidate> [0, 1] required
        <running> [0, 1] required
        <startup> [0, 1] required
        <url> [0, 1] required
      <target> 1 required
        <candidate> [0, 1] required
        <running> [0, 1] required
        <startup> [0, 1] required
        <url> [0, 1] required
    <delete-config> [0, 1] required
      <target> 1 required
        <candidate> [0, 1] required
```

```
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
<discard-changes> [0, 1] required
<edit-config> [0, 1] required
  <target> 1 required
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
  <default-operation> [0, 1] required
  <test-option> [0, 1] required
  <error-option> [0, 1] required
  <config> 1 required
    <cli-config-data> [0, 1] required
      <cmd> 1+ required
    <cli-config-data-block> [0, 1] required
    <xml-config-data> [0, 1] required
      <Device-Configuration> [0, 1] required
        <> any subtree is allowed
<get> [0, 1] required
  <filter> [0, 1] required
    <config-format-text-cmd> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-text-block> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-xml> [0, 1] required
    <oper-data-format-text-block> [0, 1] required
      <show> 1+ required
    <oper-data-format-xml> [0, 1] required
      <show> 1+ required
<get-config> [0, 1] required
  <source> 1 required
    <config> [0, 1] required
      <cli-config-data> [0, 1] required
        <cmd> 1+ required
      <cli-config-data-block> [0, 1] required
      <xml-config-data> [0, 1] required
        <Device-Configuration> [0, 1] required
          <> any subtree is allowed
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
  <filter> [0, 1] required
    <config-format-text-cmd> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-text-block> [0, 1] required
      <text-filter-spec> [0, 1] required
    <config-format-xml> [0, 1] required
<kill-session> [0, 1] required
  <session-id> [0, 1] required
<lock> [0, 1] required
  <target> 1 required
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
<unlock> [0, 1] required
  <target> 1 required
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
```

```
<validate> [0, 1] required
  <source> 1 required
    <config> [0, 1] required
      <cli-config-data> [0, 1] required
        <cmd> 1+ required
      <cli-config-data-block> [0, 1] required
      <xml-config-data> [0, 1] required
        <Device-Configuration> [0, 1] required
          <> any subtree is allowed
    <candidate> [0, 1] required
    <running> [0, 1] required
    <startup> [0, 1] required
    <url> [0, 1] required
<notification-on> [0, 1] required
<notification-off> [0, 1] required
```

The table below describes the significant fields shown in the displays.

Table 5: show netconf Field Descriptions

Field	Description
Connection Attempts	Number of NETCONF connection attempts.
rejected	Number of rejected NETCONF sessions.
no-hello	Number of NETCONF sessions that were dropped because Hello messages were not received.
success	Number of successful NETCONF sessions.
in-use 0	The request requires a resource that is already in use.
invalid-value 0	The request specifies an invalid value for one or more parameters.
too-big 0	The request or response that would be generated would be too large for the implementation to handle.
missing-attribute 0	An expected attribute is missing.
bad-attribute 0	An attribute value is incorrect. An attribute that is the incorrect type, out of range, or contains a pattern mismatch will be displayed as a bad attribute.
unknown-attribute 0	An unexpected attribute is present.
missing-element 0	An expected element is missing.
bad-element 0	An element value is not correct. An element that is the incorrect type, out of range, or contains a pattern mismatch will be displayed as a bad element.
unknown-element 0	An unexpected element is present.
unknown-namespace 0	An unexpected name space is present.
access-denied 0	Access to a requested NETCONF session is denied because authorization failed.
lock-denied 0	Access to a requested lock is denied because the lock is currently in use.

Field	Description
resource-denied 0	A request could not be completed because of insufficient resources.
rollback-failed 0	A request to roll back a configuration change was not completed.
data-exists 0	A request could not be completed because the relevant content already exists.
data-missing 0	A request could not be completed because the relevant content does not exist.
operation-not-supported 0	A request could not be completed because the requested operation is not supported.
operation-failed 0	A request could not be completed because the requested operation failed for a reason not specified by another error notice.
partial-operation 0	Part of a requested operation failed or was not attempted.
(Current | max) sessions: 3 | 4	Number of current NETCONF sessions and the maximum number of concurrent NETCONF sessions allowed.
Operations received: 100	Number of NETCONF operations received.
Operation errors: 99	Number of NETCONF operation errors.
Connection Requests: 5	Number of NETCONF connection requests.
Authentication errors: 2	Number of NETCONF authentication errors.
Connection Failures: 0	Number of unsuccessful NETCONF session connections.
ACL dropped: 30	Number of NETCONF sessions dropped due to an access list.
Notifications Sent: 20	Number of NETCONF notifications sent.

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.

template (cns)

To specify a list of Cisco Networking Services (CNS) connect templates within a CNS connect profile to be applied to a router's configuration, use the **template** command in CNS connect configuration mode. To disable this CNS connect template, use the **no** form of this command.

template *name* [**. . .** *name*]
no template *name* [**. . .** *name*]

Syntax Description

name	Name of the CNS connect template to be applied to a router's configuration.
[*...name*]	Multiple *name* arguments, which are delimited by a single space. The ellipsis (...) in the command syntax indicates that the command input can include multiple names.

Command Default

No CNS connect templates are specified.

Command Modes

CNS connect configuration (config-cns-conn)

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).
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

First 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. The **template** command specifies the list of CNS connect templates that is to be applied to a router's configuration. The templates in the list are applied one at a time. That is, when the **template** command is processed, the first template in the list is applied to the router's configuration. The router then tries to ping the CNS configuration engine. If the ping fails, then the first template in the list is removed from the router's configuration and the second template in the list is applied and so on.

The configuration mode in which the CNS connect templates are applied is specified by the immediately preceding **discover** command. (If there are no preceding **discover** commands, the templates are applied in global configuration mode.) When multiple **discover** and **template** commands are configured in a CNS connect profile, they are processed in the order in which they are entered.

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 temp-A1 temp-A2
Router(config-cns-conn)# template temp-B1 temp-B2
Router(config-cns-conn)# exit
Router(config)#
```

In this example, the following sequence of events occur for all serial interfaces when the **cns connect profile-1** command is processed. Assume all ping attempts to the CNS configuration engine are unsuccessful.

1. Enter interface configuration mode and apply all commands in the temp-A1 template to the router's configuration.
2. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
3. Try to ping the CNS configuration engine.
4. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
5. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
6. Try to ping the CNS configuration engine.
7. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
8. Enter interface configuration mode and remove all commands in the temp-A1 template from the router's configuration.
9. Enter interface configuration mode and apply all commands in the temp-A2 template to the router's configuration.
10. Enter interface configuration mode and apply all commands in the temp-B1 template to the router's configuration.
11. Try to ping the CNS configuration engine.
12. Enter interface configuration mode and remove all commands in the temp-B1 template from the router's configuration.
13. Enter interface configuration mode and apply all commands in the temp-B2 template to the router's configuration.
14. Try to ping the CNS configuration engine.
15. Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.
16. Enter interface configuration mode and remove all commands in the temp-A2 template from the router's configuration.

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.
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.

transport event

To specify that inventory events are sent out by the CNS inventory agent, use the **transport event** command in CNS inventory configuration mode. To disable the transport of inventory events, use the **no** form of this command.

transport event
no transport event

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

CNS inventory configuration (cns_inv)

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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	The command was modified. The command default was changed to enabled in Cisco IOS Release 15.1(2)T and later releases.

Usage Guidelines

Use this command to send out inventory requests with each CNS inventory agent message. When configured, the routing device will respond to queries from the CNS event bus. Online insertion and removal (OIR) events on the routing device will be reported to the CNS event bus.

Examples

The following example shows how to enable the CNS inventory agent and configure it to send out inventory events:

```
Router> enable
Router# configure terminal
Router(config)# cns inventory
Router(cns_inv)# end
```

Related Commands

Command	Description
cns inventory	Enables the CNS inventory agent and enters CNS inventory configuration mode.