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

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.

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.

For more information about AAA authentication methods, see the "AAA Authentication Methods Configuration Task List" section in the "Configuring Authentication" chapter of the *Cisco IOS Security Configuration Guide,* Release 12.4.

Examples

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

```
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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

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

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

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-name* | *ip-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.

Defaults

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

Command Modes

Global configuration (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.

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.
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-name* | *ip-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.
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

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

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

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

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

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

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

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

Examples

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

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

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

```
[2005-09-08 14:30:44]: subject=cisco.mgmt.cns.config.results.dvlpr-7200-6, message=
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
<SOAP:Header>
```

```
<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true">
<wsse:UsernameToken>
<wsse:Username>user1</wsse:Username>
<wsse:Password>password1</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
<CNS:cnsHeader Version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope">
<CNS:Agent>CNS_CONFIG</CNS:Agent>
<CNS:Response>
<CNS:correlationID>SOAP_IDENTIFIER</CNS:correlationID>
</CNS:Response>
<CNS:Time>2005-09-13T08:34:36.523Z</CNS:Time>
</CNS:cnsHeader>
</SOAP:Header>
<SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
<configResults version="2.0" overall="Success">
<configId>AAA</configId>
</configResults>
</SOAP:Body>
</SOAP:Envelope>
```

Related Commands

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

cns config retrieve

To enable the 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-name* | *ip-address*} [**encrypt**] [*port-number*] [**page** *page*] [**overwrite-startup**] [**retry** *retries* **interval** *seconds*] [**syntax-check**] [**no-persist**] [**source** *interface name*] [**status** *url*] [**event**] [**inventory**]

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.

Defaults

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.3(1)	The **inventory** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	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.

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.

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 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 {*hostname* | *ip-address*} [**encrypt**] [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** {*ipv4-address* | *ipv6-address* | *interface-name*}] [**clock-timeout** *time*] [**reconnect-time** *time*]

no cns event [*hostname* | *ip-address*] [*port-number*] [**encrypt**] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**source** {*ipv4-address* | *ipv6-address* | *interface-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.
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 [*host-name* | *ip-address*] [**encrypt** [*enc-port-number*]] [*port-number*] [**source** *interface name*]

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

Syntax Description

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

Defaults

No CNS exec agent is configured.

Command Modes

Global configuration (config)

CommandHistory

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

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

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

Examples

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

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

Related Commands

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

cns id

To set the unique event ID, config ID, or image ID 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.
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.

Release	Modification
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.

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.

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.

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 a 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.

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.

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

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.

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

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.

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:

```
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.

Defaults

For XML encapsulation, a maximum size of 3072 bytes.

Command Modes

Global configuration

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.

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

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.

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.

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.

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.

Defaults

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 **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.

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 XML. For backwards compatibility, the configuration of a server string using the 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 the string 10.19.2.5 as a trusted server for the CNS event agent:

```
Router(config)# cns trusted-server event 10.19.2.5
```

The following example shows how to configure the string 10.2.2.8, which maps through DNS to host.somedomain.com as a trusted server for all CNS agents:

```
Router(config)# cns trusted-server all-agents 10.2.2.8
Router(config)# cns trusted-server all-agents host
Router(config)# 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(config)# cns trusted-server image 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.

comparison

To specify the type of Boolean comparison to perform, use the **comparison** command in event trigger test boolean configuration mode. To disable the specified comparison value, use the **no** form of this command.

comparison {**equal | greatOrEqual | greater | lessOrEqual | lesser | unequal**}

no comparison

Syntax Description

equal	Specifies the type of Boolean comparison as equal.
greatOrEqual	Specifies the type of Boolean comparison as equal to or greater.
greater	Specifies the type of Boolean comparison as greater.
lessOrEqual	Specifies the type of Boolean comparison as equal to or less.
lesser	Specifies the type of Boolean comparison as lesser.
unequal	Specifies the type of Boolean comparison as unequal.

Command Default

The default comparison value for Boolean test is unequal.

Command Modes

Event trigger test boolean configuration (config-event-trigger-boolean)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The specified value is used for Boolean comparison during trigger tests.

Examples

The following example shows how to specify a comparison value for Boolean test:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test boolean
Router(config-event-trigger-boolean)# comparison unequal
Router(config-event-trigger-boolean)#
```

Related Commands

Command	Description
test boolean	Configures parameters for the Boolean trigger test.

conditional object

To define a conditional object when evaluating an expression, use the **conditional object** command in expression object configuration mode. To disable the configured settings, use the **no** form of this command.

conditional object *conditional-object-id* [**wildcard**]

no conditional object

Syntax Description

conditional-object-id	Conditional object identifier for evaluating the expression. Conditional objects identifiers are specified as numerical value.
wildcard	(Optional) Enables the wildcarded search for conditional object identifiers.

Command Default

By default, the conditional object identifiers are not defined.

Command Modes

Expression object configuration (config-expression-object)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The object identifier specifies the instance of the object to consider while evaluating an expression. If the object does not have an instance, the value specified for the object identifier will not be used. Conditional objects determine the use of the value specified for the object identifier.

Examples

The following example shows how to specify a conditional object:

```
Router(config)# snmp mib expression owner owner1 name Expression1
Router(config-expression)# object 32
Router(config-expression-object)# conditional object
mib-2.90.1.3.1.1.2.3.112.99.110.4.101.120.112.53
Router(config-expression-object)#
```

The following example shows how to enable wildcarded search for conditional object identifiers.

```
Router(config-expression-object)# conditional object mib-2.5 wildcard
Router(config-expression-object)#
```

Related Commands

Command	Description
snmp mib expression owner	Specifies the owner for an expression.

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

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.

context

Note Effective with Cisco IOS Release 15.0(1)M, the **context** command is replaced by the **snmp context** command. See the **snmp context** command for more information.

To associate a Simple Network Management Protocol (SNMP) context with a particular VPN routing and forwarding (VRF) instance, use the **context** command in VRF configuration mode. To disassociate an SNMP context from a VPN, use the **no** form of this command.

context *context-name*

no context

Syntax Description

context-name	Name of the SNMP VPN context. The name can be up to 32 alphanumeric characters.

Command Default

No SNMP contexts are associated with VPNs.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
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(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. Support for IPv6 was added.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.0(1)M	This command was replaced by the **snmp context** command.

Usage Guidelines

Before you use the **context** command to associate an SNMP context with a VPN, you must do the following:

- Issue the **snmp-server context** command to create an SNMP context.
- Associate a VPN with a context so that the specific MIB data for that VPN exists in the context.
- Associate a VPN group with the context of the VPN using the **context** *context-name* keyword argument pair of the **snmp-server group** command.

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, MIB data for that VPN exists in that context. Associating a VPN with a context helps service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about other VPN users on the same networking device.

A route distinguisher (RD) is required to configure an SNMP context. An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of an IPv4 prefix to make it globally unique. An RD is either an autonomous system number (ASN) relative, which means that it is composed of an autonomous system number and an arbitrary number, or an IP address relative and is composed of an IP address and an arbitrary number.

Examples

The following example shows how to create an SNMP context named context1 and associate the context with the VRF named vrf1:

```
Router(config)# snmp-server context context1
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:120
Router(config-vrf)# context context1
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode for the configuration of a VRF.
snmp mib community-map	Associates an SNMP community with an SNMP context, engine ID, or security name.
snmp mib target list	Creates a list of target VRFs and hosts to associate with an SNMP v1 or v2c community.
snmp-server context	Creates an SNMP context.
snmp-server group	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
snmp-server trap authentication vrf	Controls VRF-specific SNMP authentication failure notifications.
snmp-server user	Configures a new user to an SNMP group.

copy logging onboard module (Cat 6K)

To copy onboard failure logging (OBFL) data from the target OBFL-enabled module in Cisco Catalyst 6000 series switches to a local or remote file system, use the **copy logging onboard module** command in privileged EXEC mode.

copy logging onboard module *module-number destination-url*

Syntax Description

module-number	Module number.
destination-url	Destination URL of the copied file or directory. The destination can be either local or remote. • The exact format of the source and destination URL varies according to the file or directory location. • The default filename is “obfldump”.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SXI	This command was modified. “obfldump” was added as the default filename.

Usage Guidelines

The **copy logging onboard** command copies OBFL data from the target OBFL-enabled board to a local or remote file system. See the *Cisco IOS Configuration Fundamentals Command Reference* for more information about use of the **copy** command.

If you do not enter a filename after entering the destination URL, you will be prompted to enter a filename. If you do not enter a filename even after the prompt, “obfldump” is considered as the default filename.

```
Router# copy logging onboard module 5 bootflash:

Target filename [obfldump]?
OBFL feature copy bootflash:obfldump, Module 5
% File transfer succeeded
```

Examples

The following example shows the options for copying OBFL data:

```
Router# copy logging onboard module 2 ?

  bootflash:        Copy onboard logging to bootflash: file system
  const_nvram:      Copy onboard logging to const_nvram: file system
  dfc#2-bootflash:  Copy onboard logging to dfc#2-bootflash: file system
  dfc#4-bootflash:  Copy onboard logging to dfc#4-bootflash: file system
  disk0:            Copy onboard logging to disk0: file system
  disk1:            Copy onboard logging to disk1: file system
  ftp:              Copy onboard logging to ftp: file system
  http:             Copy onboard logging to http: file system
  https:            Copy onboard logging to https: file system
  null:             Copy onboard logging to null: file system
  nvram:            Copy onboard logging to nvram: file system
  rcp:              Copy onboard logging to rcp: file system
  scp:              Copy onboard logging to scp: file system
  sup-bootflash:    Copy onboard logging to sup-bootflash: file system
  sup-image:        Copy onboard logging to sup-image: file system
  syslog:           Copy onboard logging to syslog: file system
  system:           Copy onboard logging to system: file system
  tftp:             Copy onboard logging to tftp: file system
  tmpsys:           Copy onboard logging to tmpsys: file system
```

The following example shows how to transfer the OBFL data to a file on disk1:

```
Router# copy logging onboard module 2 disk1:tarmod2

OBFL feature copy disk1:tarmod2, Module 2
% File transfer succeeded
```

The following example shows how to transfer the OBFL data to a file on a remote server:

```
Router# copy logging onboard module 2 tftp://server1/user1/tars/tarmod2/mod2tar

OBFL feature copy tftp://server1/user1/tars/tarmod2/mod2tar 2
% File transfer succeeded
```

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
clear logging onboard (Cat 6K)	Clears onboard failure logs.
[**no**] **hw-module logging onboard (Cat 6K)**	Disables and enables OBFL.
show logging onboard (Cat 6K)	Displays onboard failure logs.

correlate

To build a single complex event, use the **correlate** command in trigger applet configuration mode. To disable the complex event, use the **no** form of this command.

correlate {**event** *event-tag* | **track** *track-object-number*} [**andnot** | **and** | **or**] {**event** *event-tag* | **track** *track-object-number*}

no correlate {**event** *event-tag* | **track** *track-object-number*} [**andnot** | **and** | **or**] {**event** *event-tag* | **track** *track-object-number*}

Syntax Description

event *event-tag*	Specifies the event that can be used with the **trigger** command to support multiple event statements within an applet. If the event associated with the *event-tag* argument occurs for the number of times specified by the **trigger** command, the result is true. If not, the result is false.
track *track-object-number*	Specifies the event object number for tracking. The range is from 1 to 500. If the tracked object is set, the result of the evaluation is true. If the tracked object is not set or is undefined, the result of the evaluation is false. This result is regardless of the state of the object.
andnot	(Optional) Specifies that if event 1 occurs the action is executed, and if event 2 and event 3 occur together the action is not executed.
and	(Optional) Specifies that if event 1 occurs the action is executed, and if event 2 and event 3 occur together the action is executed.
or	(Optional) Specifies that if event 1 occurs the action is executed, or else if event 2 and event 3 occur together the action is executed.

Command Default

The event detector counter is triggered when the specified counter crosses the threshold.

Command Modes

Trigger applet configuration (config-applet-trigger)

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.

Usage Guidelines

After you enter the trigger statement, the router enters trigger applet configuration mode. The correlate statement and up to eight attribute statements can be specified in trigger applet configuration mode. These statements are used to create a complex event correlation using the participating event statements to a maximum of eight statements. The correlate statement allows Boolean logic to be used to relate events and tracked objects. When the result of the correlate evaluation is true, the trigger criteria are applied. The correlation occurs from left to right taking into account the attribute statement conditions for the event.

Examples

The following example, shows how to configure a correlate statement after entering trigger applet configuration mode. This applet will run if the **write memory** or **copy run start** command occurs within 60 seconds of CRON specified time.

```
Router(config)# event manager applet trigger
Router(config-applet)# event tag e1 cli pattern "write mem.*" sync yes
Router(config-applet)# event tag e2 cli pattern "copy run start" sync yes
Router(config-applet)# trigger occurs 1 period-start 0-59/1 0-23/1 * * 0-7 period 60
Router(config-applet-trigger)# correlate event e1 or event e2
Router(config-applet-trigger)# attribute tag e1 occurs 1
Router(config-applet-trigger)# attribute tag e2 occurs 1
Router(config-applet-trigger)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet-trigger)# set 2.0 _exit_status 1
```

In the following example, the applet will run if either the **write memory** or **copy run start** command occurs and any syslog message that contains the string “hello” occurs within 60 seconds of any valid CRON specified time.

```
Router(config)# event manager applet trigger
Router(config-applet)# event tag e1 cli pattern "write mem.*" sync yes
Router(config-applet)# event tag e2 cli pattern "copy run start" sync yes
Router(config-applet)# event tag e3 syslog pattern "hello"
Router(config-applet)# trigger occurs 1 period-start 0-59/1 0-23/1 * * 0-7 period 60
Router(config-applet-trigger)# correlate event e1 or event e2 and event e3
Router(config-applet-trigger)# attribute tag e1 occurs 1
Router(config-applet-trigger)# attribute tag e2 occurs 1
Router(config-applet-trigger)# attribute tag e3 occurs 1
Router(config-applet-trigger)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet-trigger)# set 2.0 _exit_status 1
```

In the following example, the applet will run when the **write memory** command is entered and the tracked object 10 is set:

```
Router(config)# event manager applet trigger
Router(config)# event tag e1 cli pattern "write mem.*" sync yes
Router(config)# trigger occurs 1
Router(config-applet-trigger)# correlate event e1 and track 10
Router(config-applet-trigger)# attribute tag e1 occurs 1
Router(config-applet-trigger)# action 1.0 syslog msg "$_cli_msg Command Executed"
Router(config-applet-trigger)# set 2.0 _exit_status 1
```

Related Commands

Command	Description
action syslog	Specifies the action of writing a message to a syslog when an EEM applet is triggered.
attribute	Configures an attribute in a local service profile.
event manager applet	Registers an applet with the EEM and enters applet configuration mode.
trigger (EEM)	Enters the trigger applet configuration mode and specifies the multiple event configuration statements for an EEM applet.

cpu interrupt

To enter CPU owner configuration mode to set thresholds for interrupt level CPU utilization, use the **cpu interrupt** command in resource policy node configuration mode. To exit CPU owner configuration mode, use the **no** form of this command.

cpu interrupt

no cpu interrupt

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter CPU owner configuration mode to set rising and falling values for critical, major, and minor thresholds for interrupt level CPU utilization.

Examples

The following example shows how to enter CPU owner configuration mode to set thresholds for interrupt level CPU utilization:

```
Router(config-res-policy-node)# cpu interrupt
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

cpu process

To enter CPU owner configuration mode to set thresholds for process level CPU utilization, use the **cpu process** command in resource policy node configuration mode. To exit CPU owner configuration mode, use the **no** form of this command.

cpu process

no cpu process

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter CPU owner configuration mode to set rising and falling values for critical, major, and minor thresholds for process level CPU utilization.

Examples

The following example shows how to enter CPU owner configuration mode to set thresholds for process level CPU utilization:

```
Router(config-res-policy-node)# cpu process
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

cpu total

To enter CPU owner configuration mode to set thresholds for total CPU utilization, use the **cpu total** command in resource policy node configuration mode. To exit CPU owner configuration mode, use the **no** form of this command.

cpu total

no cpu total

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command allows you to enter CPU owner configuration mode to set rising and falling values for critical, major, and minor thresholds for total CPU utilization.

Examples

The following example shows how to enter CPU owner configuration mode to set thresholds for total CPU utilization:

```
Router(config-res-policy-node)# cpu total
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

critical rising

To set critical level threshold values for the buffer, CPU, and memory ROs, use the **critical rising** command in buffer owner configuration mode, CPU owner configuration mode, or memory owner configuration mode. To disable this function, use the **no** form of this command.

critical rising *rising-threshold-value* [**interval** *interval-value*] [**falling** *falling-threshold-value* [**interval** *interval-value*]] [**global**]

no critical rising

Syntax Description

rising-threshold-value	The rising threshold value as a percentage. Valid values are from 1 to 100.
interval	(Optional) Specifies the time, in seconds, during which the variation in rising or falling threshold values is not reported to the RU, resource groups, or resource user types. For example, if the buffer usage count remains above the configured threshold value for the configured interval, a notification is sent to the RU, resource group, or resource user types.
interval-value	The time, in seconds, during which the variation in rising or falling threshold values are not reported to the RU, resource groups, or resource user types. Valid values are from 0 to 86400. The default value is 0.
falling	(Optional) Specifies the falling threshold value as a percentage.
falling-threshold-value	(Optional) The falling threshold value as a percentage. Valid values are from 1 to 100.
global	(Optional) Configures a global threshold. The **global** keyword is optional when you set critical threshold values for public buffer, processor CPU, I/O memory, and processor memory. The **global** keyword is required when you set critical threshold values for interrupt CPU and total CPU.

Command Default

Disabled

Command Modes

Buffer owner configuration
CPU owner configuration
Memory owner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The interval is the dampening or observation interval time, in seconds, during which the variations in the rising and falling threshold values are not reported to the RUs. That is, the interval is the time the system waits to check whether the threshold value stabilizes. The interval is set to avoid unnecessary and unwanted threshold notifications. If not configured, the system defaults to 0 seconds.

This command allows you to configure three types of thresholding:

- System Global Thresholding
- User Local Thresholding
- Per User Global Thresholding

System Global Thresholding

System global thresholding is used when the entire resource reaches a specified value. That is, RUs are notified when the total resource utilization goes above or below a specified threshold value. The notification order is determined by the priority of the RU. The RUs with a lower priority are notified first and expected to reduce the resource utilization. This notification order prevents the sending of unwanted notifications to high-priority RUs.

You can set rising and falling threshold values. For example, if you set a total CPU utilization threshold value of 90% as the rising critical value and 20% as falling critical value, when the total CPU utilization crosses the 90% mark, a critical Up notification is sent to all the RUs and when the total CPU utilization falls below 20%, a critical Down notification is sent to all the RUs. The same criteria also apply to buffer ROs and memory ROs.

User Local Thresholding

User local thresholding is used when a specified RU exceeds the configured limits. The user local thresholding method prevents a single RU from monopolizing the resources. That is, the specified RU is notified when the resource utilization of the specified RU goes above or below a configured threshold value. For example, if you set a CPU utilization threshold value of 90% as the rising critical value and 20% as falling critical value, when the CPU utilization of the specified RU crosses the 90% mark, a critical Up notification is sent to that RU only and when the CPU utilization of the specified RU falls below 20%, a critical Down notification is sent to that RU only. The same method also applies to buffer and memory ROs.

Per User Global Thresholding

Per user global thresholding is used when the entire resource reaches a specified value. This value is unique for each RU and notification is sent only to the specified RU. User global thresholding is similar to user local thresholding, except that the global resource usage is compared against the thresholds. That is, only the specified RU is notified when the total resource utilization goes above or below a configured threshold value. For example, if you have set a CPU utilization threshold value of 90% as the rising critical value and 20% as falling critical value, when the total CPU utilization crosses the 90% mark, a critical Up notification is sent to the specified RU only and when the total CPU utilization falls below 20%, a critical Down notification is sent to the specified RU only. The same method also applies to buffer and memory ROs.

Threshold Violations

The Cisco IOS device sends out error messages when a threshold is violated. The following examples help you understand the error message pattern when different threshold violations occur in buffer, CPU, and memory ROs:

System Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a system global threshold shows the following output:

```
System global threshold-Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical
threshold
configured <value> Current usage :<value>
```

For example:

```
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical
threshold
configured 144 Current usage :145

System global threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured <value> Current usage :<value>
```

For example:

```
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured 90 Current usage :89
```

Per User Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:24:04: %SYS-4-RESGLOBALBUFEXCEED: Buffer usage has gone above buffer Critical threshold
configured by resource user  <user-name>
configured 144 Current usage :145

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:25:08: %SYS-4-RESGLOBALBUFRECOVER: Buffer usage has gone below buffer Critical
threshold configured by resource user  <user-name>
configured 126 Current usage :125
```

User Local Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:31:15: %SYS-4-RESBUFEXCEED: Resource user  user_1 has exceeded the buffer Critical
threshold. configured 108 Current usage :109

User local threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:31:05: %SYS-5-RESBUFRECOVER: Resource user  user_1 has recovered after exceeding the
buffer Critical threshold. configured 90 Current usage :89
```

System Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a system global threshold shows the following output:

```
System global threshold- Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
================================================================================
00:19:36: %SYS-4-CPURESRISING: System is seeing global cpu util 19% at total level more
than the configured minor limit 11%

System global threshold - Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:20:56: %SYS-6-CPURESFALLING: System is no longer seeing global high cpu at total level
for the configured minor limit 10%, current value 4%
```

Per User Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a user global threshold shows the following output:

```
User global threshold - Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:14:21: %SYS-4-CPURESRISING: Resource user <user-name> is seeing global cpu util 11% at
total level more than the configured minor limit 6 %
```

For example:

```
00:14:21: %SYS-4-CPURESRISING: Resource user Test-proc-14:99s:1w:100n is seeing global cpu
util 11% at total level more than the configured minor limit 6%

User global threshold- Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:14:46: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing global high
cpu at total level for the configured critical limit 9%, current value 4%
```

For example:

```
00:14:46: %SYS-6-CPURESFALLING: Resource user Test-proc-14:99s:1w:100n is no longer seeing
global high cpu at total level for the configured critical limit 9%, current value 4%
```

User Local Threshold Violation in CPU RO

The threshold violation in CPU RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor will vary accordingly
- only process level)
================================================================================
00:12:11: %SYS-4-CPURESRISING: Resource user <user-name> is seeing local cpu util 15% at
process level more than the configured minor limit 6%
```

For example:

```
00:12:11: %SYS-4-CPURESRISING: Resource user Test-proc-9:85s:15w:100n is seeing local cpu
util 15% at process level more than the configured minor limit 6%

User local threshold- Recovery (keywords Critical, Major and Minor will vary accordingly
- only process level)
================================================================================
00:13:11: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing local high
cpu at process level for the configured critical limit 9%, current value 3%
```

System Global Threshold Violation in Memory RO

The threshold violation in memory RO for a system global threshold shows the following output:

```
System global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly )
(If violation happens in IO memory pool will be : I/O)
================================================================================
13:53:22: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
Pool: Processor  Used: 422703520  Threshold: 373885200
```

For example:

```
13:54:03: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Critical threshold
Pool: Processor  Used: 622701556  Threshold: 467356500

System global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
================================================================================
%SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Minor threshold
Pool: Processor  Used: 222473448  Threshold: 355190940
```

For example:

```
13:50:41: %SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Critical
threshold
Pool: Processor  Used: 222473152  Threshold: 443988675
```

Per User Global Threshold Violation in Memory RO

The threshold violation in memory RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
================================================================================
00:53:14: %SYS-4-RESGLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
configure by resource user <XYZ>
Pool: Processor  Used: 62273916  Threshold: 62246820

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
================================================================================
00:32:56: %SYS-4-RESGLOBALMEMRECOVER: Global Memory has recovered after exceeding the
Critical threshold configure by resource user <XYZ>
Pool: Processor  Used: 329999508  Threshold: 375865440
```

User Local Threshold Violation in Memory RO

The threshold violation in memory RO for a user local threshold shows the following output:

```
User local threshold- Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
01:05:42: %SYS-4-RESMEMEXCEED: Resource user <XYZ> has exceeded the Critical memory
threshold
Pool: Processor Used: 103754740 Threshold: 103744700

User local threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:44:43: %SYS-5-RESMEMRECOVER: Resource user <XYZ> has recovered after exceeding the
Critical memory threshold
Pool: Processor Used: 328892280 Threshold :375865440
```

Examples

Configuring Critical Rising Values for System Global Thresholding

The following example shows how to configure the critical threshold values for system global thresholding with a critical rising threshold of 90% at an interval of 12 seconds and a critical falling threshold of 20% at an interval of 10 seconds:

```
Router(config-owner-cpu)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-buffer)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-memory)# critical rising 90 interval 12 falling 20 interval 10 global
```

Configuring Critical Rising Values for User Local Thresholding

The following example shows how to configure the critical threshold values for user local thresholding with a critical rising threshold of 90% at an interval of 12 seconds and a critical falling threshold of 20% at an interval of 10 seconds:

```
Router(config-owner-cpu)# critical rising 90 interval 12 falling 20 interval 10
Router(config-owner-buffer)# critical rising 90 interval 12 falling 20 interval 10
Router(config-owner-memory)# critical rising 90 interval 12 falling 20 interval 10
```

Configuring Critical Rising Values for Per User Global Thresholding

The following example shows how to configure the critical threshold values for per user global thresholding with a critical rising threshold of 90% at an interval of 12 seconds and a critical falling threshold of 20% at an interval of 10 seconds:

```
Router(config-owner-cpu)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-buffer)# critical rising 90 interval 12 falling 20 interval 10 global
Router(config-owner-memory)# critical rising 90 interval 12 falling 20 interval 10 global
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets threshold values for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets threshold values for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets threshold values for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets threshold values for total CPU utilization.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

crypto mib topn

To configure TopN sampling parameters, use the **crypto mib topn** command in global configuration mode. To disable TopN sampling, use the **no** form of this command.

crypto mib topn [**interval** *seconds*] [**stop** *seconds*]

no crypto mib topn [**interval** *seconds*] [**stop** *seconds*]

Syntax Description

interval *seconds*	(Optional) Specifies the number of seconds between samples.The allowable range is from 60 to 86400 (60 seconds to 24 hours). The default is 300 (5 minutes). Defined in the MIB as TopnMinSampleInterval.
stop *seconds*	(Optional) Specifies the time, in seconds, from when this command is executed until sampling ceases. The allowable range is from 0 to 604800. A zero (0) indicates continuous sampling and is the default. For any value other than 0, the stop time value must be greater than or equal to the sampling interval value. Defined in the MIB as TopnStopTime.

Command Default

No TopN sampling parameters are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.

Usage Guidelines

Use this command to rank objects according to your chosen criteria. You will not see the stop parameter setting after enabling the **show running configuration** command if the stop parameter is set at a value greater than zero. Otherwise, the current sampling parameters are recorded in the active configuration (if sampling is enabled), and sampling occurs continuously (at the specified intervals) until, and after, the device is rebooted. This command should be disabled if your criteria queries performed by XSM clients (such as VPN Device Manager [VDM]) are not to be processed.

Crypto MIB commands apply to characteristics of the IP Security (IPSec) MIBs. TopN (**topn**) is a special subset of the IPSec MIB Export (IPSMX) interface that provides a set of queries that allows ranked reports of active Internet Key Exchange (IKE) or IPSec tunnels to be obtained depending on certain criteria. While the VPN Device Manager (VDM) application retrieves and presents the data elements defined in the IKE and IPSec MIBs, the application does not use the Simple Network Management Protocol (SNMP) interface.

Examples

The following example shows the **crypto mib topn** command being enabled with an interval frequency of 240 seconds and a designated stop time of 1200 seconds (20 minutes). At that time, the assigned sampling ceases.

```
crypto mib topn interval 240 stop 1200
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.

default-state

To set the default state for a stub object, use the **default-state** command in tracking configuration mode. To reset the default state to its internal default state, use the **no** form of this command.

default-state {**up** | **down**}

no default-state {**up** | **down**}

Syntax Description

up	Sets the current default state of a stub object to up.
down	Sets the current default state of a stub object to down.

Command Default

Internal default state is the default.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **default-state** command to set the default state of a stub object that has been created by the **track stub** command. The stub object can be tracked and manipulated by an external process, Embedded Event Manager (EEM).

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

Examples

The following example shows how to create a stub object and configure a default state for the stub object:

```
track 2 stub
 default-state up
```

Related Commands

Command	Description
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

delta (test_threshold)

To specify a delta value for the threshold trigger test, use the **delta** command in event trigger threshold configuration mode. To disable the configured settings, use the no form of this command.

delta {**falling** | **rising**} {*threshold-value* | **event owner** *owner-name* **name** *event-name*}

no delta {**falling** | **rising**}

Syntax Description

falling	Specifies the delta value for falling threshold.
rising	Specifies the delta value for rising threshold.
threshold-value	Delta value for thresholds. The default value is 0.
event-owner	Name of the event owner.
name	Specifies the name of an event.
event-name	Name of the event.

Command Default

The delta threshold value is set to 0 and no event is invoked by default.

Command Modes

Event trigger threshold configuration (config-event-trigger-threshold)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **delta** command sets the delta falling or rising threshold to the specified value when the object sampling method is delta. The **delta rising event owner** command specifies the event to invoke when the delta rising threshold triggers. Similarly, the **delta falling event owner** specifies the event to invoke when the delta falling threshold triggers.

Examples

The following example shows how to specify a delta falling threshold:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# test threshold
Router(config-event-trigger-threshold)# delta falling 20
Router(config-event-trigger-threshold)#
```

Related Commands

Command	Description
test	Enables event trigger test.

delta interval

To specify an interval for the delta sampling of objects used while evaluating an expression, use the **delta interval** command in expression configuration mode. To disable the configured settings, use the **no** form of this command.

delta interval *seconds*

no delta interval

Syntax Description

seconds	Number of seconds for the delta sampling interval. The default is 0.

Command Default

The default delta sampling interval is 0.

Command Modes

Expression configuration (config-expression)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

If there are no objects configured for the delta sampling method, the **delta interval** command does not configure the interval.

Examples

The following example shows how to set the delta interval to 60 seconds:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# delta interval 60
Router(config-expression)#
```

Related Commands

Command	Description
snmp mib expression owner	Specifies owner for an expression.

description

To specify a description of the digital signal processor (DSP) interface, use the **description** command in voice-port or DSP farm interface configuration mode. To describe a MGCP profile that is being defined, use the **description** command in MGCP profile configuration mode. To specify the name or a brief description of a charging profile, use the **description** command in charging profile configuration mode. To delete a configured description, use the **no** form of the command in the appropriate configuration mode.

description *string*

no description

Syntax Description

string	Character string from 1 to 80 characters for DSP interfaces and MGCP profiles, or from 1 to 99 characters for charging profiles.

Command Default

Enabled with a null string.
The MGCP profile has no default description.
Charging profiles have no default description.

Command Modes

Voice-port configuration
DSP farm interface configuration
MGCP profile configuration
Charging profile configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series and Cisco 7200.
11.3(1)MA	This command in voice-port configuration mode was implemented on the Cisco MC3810.
12.0(5)XE	This command in DSP farm interface configuration mode was modified.
12.1(1)T	The DSP farm interface configuration mode modification was integrated into Cisco IOS Release 12.1(1)T.
12.2(2)XA	This command was implemented on the Cisco AS5300.
12.2(11)T	This command was implimented on the Cisco AS5850 and integrated into Cisco IOS Release 12.2(11)T.
12.3(8)XU	This command was introduced in charging profile configuration mode.
12.3(11)YJ	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command in charging profile configuration mode was integrated into Cisco IOS Release 12.3(14)YQ.
12.4(9)T	This was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SXH	This command was changed to allow the description to contain spaces.

Usage Guidelines

Use the **description** command to describe the DSP interface connection or a defined MGCP profile. The information is displayed when a **show** command is used, and it does not affect the operation of the interface in any way.

In Release 12.2(33)SXH and later releases, you can enter spaces in the description.

Examples

The following example identifies voice port 1/0/0 as being connected to the purchasing department:

```
voice-port 1/0/0
 description purchasing-dept
```

The following example identifies DSP farm interface 1/0 as being connected to the marketing department:

```
dspint dspfarm 1/0
 description marketing-dept
```

The following example shows a description for an MGCP profile:

```
mgcp profile newyork
 description This is the head sales office in New York.
 dot ...(socket=0)
 S:.
 R:250 NAA09092 Message accepted for delivery
 S:QUIT
 R:221 madeup@abc.com closing connection
 Freeing SMTP ctx at 0x6121D454
 returned from work-routine, context freed
```

Related Commands

Command	Description
category	Identifies the subscriber category to which a charging profile applies.
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies, as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies, as a trigger condition in a charging profile, that the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies, as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
gprs charging characteristics reject	Specifies that create PDP context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	

Command	Description
gprs charging profile	Creates a new charging profile (or modifies an existing one) and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of GGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
mgcp	Starts and allocates resources for the MGCP daemon.
mgcp profile	Initiates MGCP profile mode to create and configure a named MGCP profile associated with one or more endpoints or to configure the default profile.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

description (EEM)

To describe what an Embedded Event Manager (EEM) applet does, use the **description** (EEM) command in applet configuration mode. To remove the description of an applet, use the **no** form of this command.

description *line*

no description

Syntax Description

line	A brief description of a policy, upto 240 characters.

Command Default

By default, no description is specified for an applet.

Command Modes

Applet configuration (config-applet)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to describe what an EEM applet does. It is valid to have applets without a description. The Description of an applet can be added in any order, before or after any other applet configuration. Configuring a new description for an applet that already has a description, overwrites the current description.

Examples

The following example shows how to add or modify the description for an EEM:

```
Router(config)# event manager applet one
Router(config-applet)# description "This applet looks for the word count in syslog
messages"
Router(config-applet)# event syslog pattern "count"
Router(config-applet)# action 1 syslog msg hi
```

Related Commands

Command	Description
show event manager policy active	Displays EEM policies that are executed.
show event manager policy available	Displays EEM policies that are available to be registered.

description (event)

To describe the function and use of an event, use the **description** command in event configuration mode. To remove the description, use the **no** form of this command.

description *event-description*

no description

Syntax Description

event-description	Description of the function and use of an event. The description text string can be up to 256 characters in length. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

By default, events are not described.

Command Modes

Event configuration (config-event)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **description** command configures a free-text description of the function and use of an event.

Examples

The following example shows how to describe an event:

```
Router(config)# snmp mib event owner owner1 name EventA
Router(config-event)# description "EventA is an RMON event"
Router(config-event)#
```

Related Commands

Command	Description
snmp mib event owner	Specifies an event owner for a management event.

description (expression)

To provide a description of the use of an expression, use the **description** command in expression configuration mode. To remove the description, use the **no** form of this command.

description *expression-description*

no description

Syntax Description

expression-description	Description of the function and use of an expression. The description text string can be up to 256 characters in length.

Command Default

By default, no expression is described.

Command Modes

Expression configuration (config-expression)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **description** command configures a free-text description of the function and use of an expression.

Examples

The following example shows how to describe an expression:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# description expressionA is created for the sysLocation MIB
object
Router(config-expression)#
```

Related Commands

Command	Description
snmp mib expression owner	Specifies the owner for an expression.

description (trigger)

To provide a description of the function and use of an event trigger, use the **description** command in the event trigger configuration mode. To remove the description, use the **no** form of this command.

description *trigger-description*

no description

Syntax Description

trigger-description	Description of the function and use of a trigger. The description text string can be up to 256 characters in length.

Command Default

By default, no trigger is described.

Command Modes

Event trigger configuration (config-event-trigger)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **description** command configures a free-text description of the function and use of an event trigger.

Examples

The following example shows how to describe an event trigger:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# description triggerA is configured for network management
events
Router(config-event-trigger)#
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies the event trigger owner while configuring management event trigger information.

discontinuity object (expression)

To define the discontinuity properties for an object, use the **discontinuity object** command in expression object configuration mode. To disable the configuration settings, use the **no** form of this command.

discontinuity object *discontinuity-object-id* [**wildcard**] [**type** {**timeticks** | **timestamp** | **date-and-time**}]

no discontinuity object

Syntax Description

discontinuity-object-id	Discontinuity object identifier to identify discontinuity in a counter. The default object identifier is sysUpTime.0.
wildcard	(Optional) Specifies whether an object identifier is to be wildcarded or fully specified. By default the object identifier is fully specified.
type	(Optional) Specifies the type of discontinuity in a counter. The default value for discontinuity type is timeticks.
timeticks	(Optional) Specifies timeticks for discontinuity in a counter.
timestamp	(Optional) Specifies the time stamp for discontinuity in a counter.
date-and-time	(Optional) Specifies the date and time of discontinuity in a counter.

Command Default

The default discontinuity object identifier is sysUpTime.0.

Command Modes

Expression object configuration (config-expression)

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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **discontinuity object** command configures discontinuity properties of an object when the object sampling type is delta or changed.

Examples

The following example shows how to configure discontinuity properties for an object:

```
Router(config)# snmp mib expression owner owner1 name ExpressionA
Router(config-expression)# object 43
Router(config-expression-object)# discontinuity object 0.7
```

The following example shows how to enable wildcarded search for discontinuity object identifiers:

```
Router(config-expression-object)# discontinuity object 0.7 wildcard
Router(config-expression-object)#
```

The following example shows how to specify the type for discontinuity in a counter:

```
Router(config-expression-object)# discontinuity object 0.7 type timeticks
Router(config-expression-object)#
```

Related Commands

Command	Description
snmp mib expression owner	Specifies the owner for an expression.

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

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.

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.

Table 25 provides a summary of the interface parameters that can be defined using the **discover** command.

Table 25 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.	**${line}**	Line	—	**discover interface** *interface-type*
discover controller *controller-type*	Discovers all the controllers that create an interface that match the specified *controller-type* argument.	**${controller}**	Controller	—	**discover interface** *interface-type*
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 Table 25 and Table 26). 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 26 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 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:
   a. Enter interface configuration mode and apply all commands in the frame template to the router's configuration.
   b. Try to ping the CNS configuration engine.
   c. 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.
   d. 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.