F through T Commands

format global

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

format global *location*:*local-filename*

no format global

Syntax Description

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

Command Default

The built-in spec file is used.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

kron occurrence

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

kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays* **:**] *numhours* **:**] *nummin*| **at** *hours* **:** *min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot**| **recurring**| **system-startup**}

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

Syntax Description

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

oneshot	Indicates that the occurrence is to run only one time. After the occurrence has run, the configuration is removed.
recurring	Indicates that the occurrence is to run on a recurring basis.
system-startup	Indicates that the occurrence is to run on system startup, in addition to the **recurring** or **oneshot** occurrences.

Command Default

No schedule parameters are specified.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

kron policy-list

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

kron policy-list *list-name*

no kron policy-list *list-name*

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

line-cli

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

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

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

Syntax Description

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

Command Default

No command lines are specified to configure modem lines.

Command Modes

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

Command History

Release	Modification
12.2(8)T	This command was introduced on Cisco 2600 series and Cisco 3600 series routers.
12.3(8)T	This command was replaced by the **cli (cns)** command.
12.3(9)	This command was replaced by the **cli (cns)** command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use this command to connect to the CNS configuration engine using a modem dialout line. The bootstrap configuration on the router finds the connecting interface, regardless of the slot in which the card resides or

the modem dialout line for the connection, by trying different candidate interfaces or lines until it successfully pings the registrar.

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

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

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

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

Examples

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

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

These commands apply the following configuration:

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

Related Commands

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

logging cns-events

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

logging cns-events [*severity-level*]

no logging cns-events

Syntax Description

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

Command Default

Level 7: debugging

Command Modes

Global configuration (config)

Command History

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

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

netconf beep initiator

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

netconf beep initiator {*hostname* | *ip-address*} *port-number* **user** *sasl-user* **password** *sasl-password* [**encrypt** *trustpoint*] [**reconnect-time** *seconds*]

no netconf beep initiator {*hostname* | *ip-address*} *port-number*

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

netconf beep listener

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

netconf beep listener [*port-number*] [**acl** *access-list-number*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*]

no netconf beep listener

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

netconf format

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

netconf format *location*:*local-filename*

no netconf format

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
netconf lock-time	Limits the amount of time NETCONF can lock a configuration.
netconf max-sessions	Limits the total number of NETCONF sessions.
netconf ssh	Enables NETCONF over SSHv2.

netconf lock-time

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

netconf lock-time *seconds*

no netconf lock-time

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf max-message

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

netconf max-message *size*

no netconf max-message

Syntax Description

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

Command Default

The maximum message size is set to infinite.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

netconf max-sessions

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

netconf max-sessions *session*

no netconf max-sessions

Syntax Description

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

Command Default

Four concurrent NETCONF sessions are allowed.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Extra NETCONF sessions beyond the maximum are not accepted.

Examples

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

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

Related Commands

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

netconf ssh

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

netconf ssh [**acl** *access-list-number*]

no netconf ssh

Syntax Description

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

Command Default

NETCONF over SSHv2 is not enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

NETCONF is supported only on SSHv2.

Examples

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

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

Related Commands

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

policy-list

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

policy-list *list-name*

no policy-list *list-name*

Syntax Description

list-name	Name of the policy list.

Command Default

No policy list is associated.

Command Modes

Kron-occurrence configuration (kron-config-occurrence)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

show cns config connections

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

show cns config connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced. This command replaces the **show cns config status** command.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **show cns config connections** command to determine whether the CNS event agent is connecting to the gateway, connected, or active, and to display the gateway used by the event agent and its IP address and port number.

Examples

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

```
Router# show cns config connections

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

Related Commands

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

show cns config outstanding

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

show cns config outstanding

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

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

Examples

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

```
Router# show cns config outstanding

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

Related Commands

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

show cns config stats

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

show cns config stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.3(1)	Additional output fields were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

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

Examples

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

```
Router# show cns config stats

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

Related Commands

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

show cns config status

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

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

show cns config status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was replaced by the **show cns config connections** command.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0 (22)S.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

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

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

Related Commands

Command	Description
cns config cancel	Cancels a CNS configuration.

Command	Description
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.
cns config retrieve	Gets the configuration of a routing device using CNS.
show cns config connections	Displays the status of the CNS event agent connection.

show cns event connections

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

show cns event connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **show cns event connections** command to display the status of the event agent connection—such as whether it is connecting to the gateway, connected, or active—and to display the gateway used by the event agent and its IP address and port number.

Examples

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

```
Router# show cns event connections

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

Related Commands

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

show cns event gateway

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

show cns event gateway

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

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

Examples

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

```
Router# show cns event gateway

The currently configured primary event gateway:
```

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

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

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event stats

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

show cns event stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series routers.
12.3(1)	Output was changed to display statistics generated since last cleared.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

- Number of events received
- Number of events sent
- Number of events not processed successfully
- Number of events in the queue
- Time stamp showing when statistics were last cleared (time stamp is router time)
- Number of events received since the statistics were cleared

- Time stamp of latest event received (time stamp is router time)
- Time stamp of latest event sent
- Number of applications using the Event Agent
- Number of subjects subscribed

Examples

The following example displays statistics for the CNS event agent:

```
Router# show cns event stats

0 events received.
1 events sent.
0 events not processed.
0 events in the queue.
0 events sent to other IOS applications.
Event agent stats last cleared at Apr 4 2003 00:55:25 UTC
No events received since stats cleared
The time stamp of the last received event is *Mar 30 2003 11:04:08 UTC
The time stamp of the last sent event is *Apr 11 2003 22:21:23 UTC
3 applications are using the event agent.
0 subjects subscribed.
1 subjects produced.
0 subjects replied.
```

Related Commands

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

show cns event status

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

show cns event status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

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

Examples

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

```
Router# show cns event status

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

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event subject

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

show cns event subject [*name*]

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

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

Examples

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

```
Router# show cns event subject

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

```
cisco.cns.config.reboot
cisco.cns.exec.cmd
```

Related Commands

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

show cns image connections

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

show cns image connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# show cns image connections

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

Related Commands

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

show cns image inventory

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

show cns image inventory

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show cns image inventory

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

Related Commands

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

show cns image status

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

show cns image status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# show cns image status

Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS
Last successful upgrade ended at 00:00:00.000 UTC Mon May 6 2003
```

```
Last failed upgrade ended at 00:00:00.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
 messages received: 12
 receive errors: 5
Transmit Status
  TX Attempts:4
    Successes:3         Failures 2
```

Related Commands

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

show kron schedule

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

show kron schedule

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show kron schedule

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

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

Table 1: show kron schedule Field Descriptions

Field	Description
week inactive	The policy list named week is currently inactive.

Field	Description
run again in 7 days 01:02:33	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run on a recurring basis.
run once in 32 days 20:43:31	Time in days, hours, minutes and seconds before the policy will run. This policy is scheduled to run just once.

Related Commands

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

show netconf

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

```
Router# show netconf counters

NETCONF Counters
Connection Attempts:0: rejected:0 no-hello:0 success:0
Transactions
        total:0, success:0, errors:0
detailed errors:
        in-use 0        invalid-value 0         too-big 0
        missing-attribute 0     bad-attribute 0         unknown-attribute 0
        missing-element 0       bad-element 0   unknown-element 0
        unknown-namespace 0     access-denied 0         lock-denied 0
        resource-denied 0       rollback-failed 0       data-exists 0
```

```
        data-missing 0  operation-not-supported 0       operation-failed 0
        partial-operation 0
```

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

```
Router# show netconf session

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

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

```
Router# show netconf schema

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

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

```
        <startup> [0, 1] required
        <url> [0, 1] required
    <notification-on> [0, 1] required
    <notification-off> [0, 1] required
```

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

Table 2: show netconf Field Descriptions

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

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

Related Commands

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

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

template (cns)

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

template *name* [*... name*]

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

Syntax Description

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

Command Default

No CNS connect templates are specified.

Command Modes

CNS connect configuration (config-cns-conn)

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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

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

A CNS connect profile specifies the **discover** commands and associated **template** commands that are to be applied to a router's configuration. The **template** command specifies the list of CNS connect templates that

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

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

Examples

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

```
Router(config)# cns connect profile-1
Router(config-cns-conn)# discover interface Serial
Router(config-cns-conn)# template temp-A1 temp-A2
Router(config-cns-conn)# template temp-B1 temp-B2
Router(config-cns-conn)# exit
Router(config)#
```

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

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

15 Enter interface configuration mode and remove all commands in the temp-B2 template from the router's configuration.

16 Enter interface configuration mode and remove all commands in the temp-A2 template from the router's configuration.

Related Commands

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

transport event

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

transport event

no transport event

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

CNS inventory configuration (cns_inv)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	The command was modified. The command default was changed to enabled in Cisco IOS Release 15.1(2)T and later releases.

Usage Guidelines

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

Examples

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

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

Related Commands

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