



Cisco Networking Services Flow-Through Provisioning

The Cisco Networking Services Flow-Through Provisioning feature provides the infrastructure for automated configuration of large numbers of network devices. Based on Cisco Networking Services event and configuration agents, it eliminates the need for an onsite technician to initialize the device. The result is an automated workflow from initial subscriber-order entry through Cisco manufacturing and shipping to final device provisioning and subscriber billing. This focuses on a root problem of service providers and other similar business models; use of human labor in activating service.

- [Finding Feature Information, page 1](#)
- [Information About Cisco Networking Services Flow-Through Provisioning, page 2](#)
- [How to Configure Cisco Networking Services Flow-Through Provisioning, page 7](#)
- [Configuration Examples for Cisco Networking Services Flow-Through Provisioning, page 9](#)
- [Additional References, page 12](#)
- [Feature Information for Cisco Networking Services Flow-Through Provisioning, page 13](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Cisco Networking Services Flow-Through Provisioning

Cisco Networking Services Flow-Through Provisioning

The Cisco Networking Services Flow-Through Provisioning feature provides the infrastructure for automated configuration of large numbers of network devices. Based on Cisco Networking Services event and configuration agents, it eliminates the need for an onsite technician to initialize the device. The result is an automated workflow from initial subscriber-order entry through Cisco manufacturing and shipping to final device provisioning and subscriber billing. This functionality focuses on a root problem of today's service-provider and other similar business models: use of human labor in activating service.

To achieve such automation, Cisco Networking Services flow-through provisioning relies on standardized configuration templates that you create. However, the use of such templates requires a known fixed hardware configuration, uniform for all subscribers. There is no way to achieve this without manually pre-staging each linecard or module within each chassis. While the inventory within a chassis is known at time of manufacture, controlling which linecards or modules are in which slots thereafter is labor-intensive and error-prone.

To overcome these difficulties, Cisco Networking Services flow-through provisioning defines a new set of Cisco commands—the **cns** commands. When a remote device is first powered on, these commands do the following:

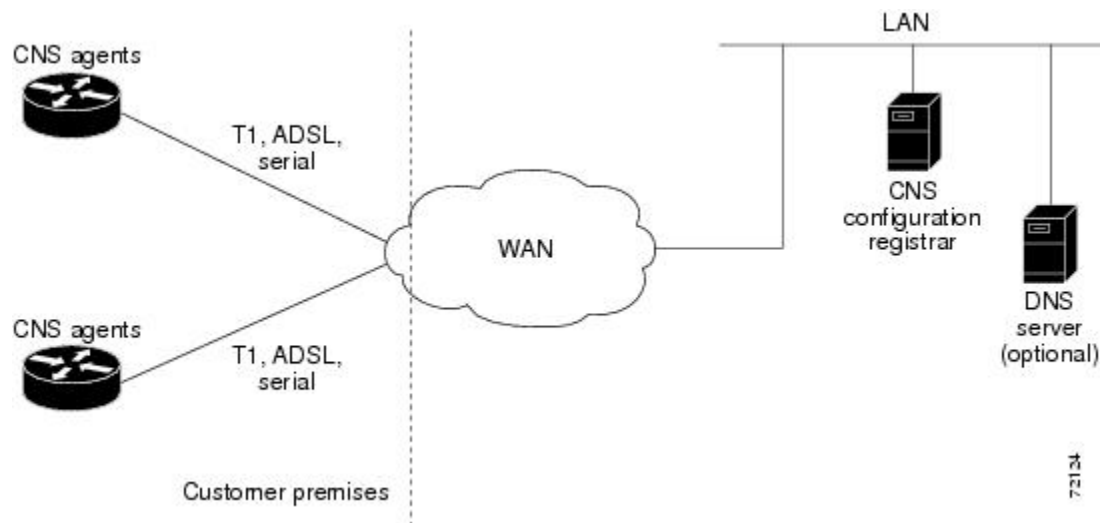
- 1 To each device interface in turn, applies a preset temporary bootstrap configuration that tries to contact the Cisco Networking Services configuration engine. A successful connection determines the connecting interface.
- 2 Connects, by way of software called a Cisco Networking Services agent, to a Cisco Networking Services configuration engine housed in a Cisco IE2100 device.
- 3 Passes to the Cisco Networking Services configuration engine a device-unique ID, along with a human-readable description of the device's linecard or module inventory by product number and location, in XML format.

In turn, the configuration engine does the following:

- 1 Locates in a Lightweight Directory Access Protocol (LDAP) directory, based on the device IDs, a predefined configuration template for the main chassis and subconfiguration template for each linecard or module.
- 2 Substitutes actual slot numbers from the chassis inventory for the template's slot-number parameters, thus resolving the templates into subscriber-specific configurations that match the true linecard or module slot configuration.
- 3 Downloads this initial configuration to the target device. The Cisco Networking Services agent directly applies the configuration to the device.

The figure below shows the Cisco Networking Services flow-through provisioning architecture.

Figure 1: Cisco Networking Services Flow-Through Provisioning Architecture



Cisco Networking Services Flow-Through Provisioning Configurations

Cisco Networking Services flow-through provisioning involves three different types of configuration on the remote device:

Bootstrap configuration

You specify the preset bootstrap configuration on which this solution depends as part of your order from Cisco using Cisco Configuration Express, an existing service integrated with the Cisco.com order-entry tool. You specify a general-subscriber nonspecific bootstrap configuration that provides connectivity to the Cisco Networking Services configuration engine. Cisco then applies this configuration to all the devices of that order in a totally automated manufacturing step. This configuration runs automatically on power-on.

Initial configuration

The Cisco Networking Services configuration engine downloads an initial configuration, once only, to replace the temporary bootstrap configuration. You can either save or not save it in the device's nonvolatile NVRAM memory:

- If you save the configuration, the bootstrap configuration is overwritten.
- If you do not save the configuration, the download procedure repeats each time that the device powers off and then back on. Repeating the download procedure enables the device to update to the current Cisco configuration without intervention.

Incremental (partial) configuration

On subsequent reboot, incremental or partial configurations are performed to update the configuration without the network having to shut down. Such configurations can be delivered either in a push operation that you initiate or a pull operation on request from the device.

Unique IDs

Key to Cisco Networking Services Flow-through provisioning is the capability to associate, with each device, a simple, manageable, and unique ID that is compatible with your systems for order entry, billing, provisioning, and shipping and can also link your order-entry system to the Cisco order-fulfillment system. Such an ID must have the following characteristics:

- Be available from manufacturing as part of order fulfillment.
- Be recordable on the shipping carton and chassis.
- Be available to the device's Cisco software.
- Be modifiable after the device is first powered up.
- Be representative of both a specific chassis and a specific entry point into your network.

To define such an ID, Cisco Networking Services flow-through provisioning equips the Cisco Networking Services agent with a new set of commands—the **cn**s commands—with which you specify how configurations should be done and, in particular, how the system defines unique IDs. You enable the Cisco software to auto-discover the unique ID according to directions that you specify and information that you provide, such as chassis serial number, MAC address, IP address, and several other possibilities. The **cn**s commands are part of the bootstrap configuration of the manufactured device, specified to Cisco Configuration Express at time of order.

Within this scope, Cisco Configuration Express and the **cn**s commands also allow you to define custom asset tags to your own specifications, which are serialized during manufacture and automatically substituted into the unit's bootstrap configuration.

Cisco appends tags to the carton for all the various types of IDs supported by the **cn**s commands, so that these values can be bar-code read at shipping time and fed back into your systems. Alternatively, these IDs are also available through a direct XML-software interface between your system and the Cisco order-status engine, eliminating the need for bar-code reading. The Cisco Networking Services agent also provides a feedback mechanism whereby the remote device can receive XML events or commands to modify the device's ID, in turn causing that same device to broadcast an event indicating the old/new IDs.

Management Point

On most networks, a small percentage of individual remote devices get configured locally. This can potentially be a serious problem, not only causing loss of synchronization across your network but also opening your system to the possibility that an automatic reconfiguration might conflict with an existing configuration and cause a device to become unusable or even to lose contact with the network.

To address this problem, you can designate a management point in your network, typically on the Cisco IE2100 Cisco Networking Services configuration engine, and configure it to keep track of the configurations on all remote devices.

To enable this solution, configure the Cisco Networking Services agent to publish an event on the Cisco Networking Services event bus whenever any change occurs to the running configuration. This event indicates exactly what has changed (old/new), eliminating the need for the management point to perform a highly unscalable set of operations such as telnetting into the device, applying a script, reading back the entire running configuration, and determining the difference between old and new configurations. Additionally, you can arrange for Simple Network Management Protocol (SNMP) notification traps of configuration changes occurring through the SNMP MIB set.

Point-to-Point Event Bus

Today's business environment requires that you be able to ensure your customers a level of service not less than what they are actually paying for. Toward this end, you activate service-assurance applications that broadcast small poll/queries to the entire network while expecting large responses from a typically small subset of devices according to the criteria of the query.

For these queries to be scalable, it is necessary for the replying device to bypass the normal broadcast properties of the event bus and instead reply on a direct point-to-point channel. While all devices need the benefit of the broadcasted poll so that they can all be aware of the query to which they may need to reply, the devices do not have to be aware of each others' replies. Massive copying and retransmission of device query replies, as part of the unnecessary reply broadcast, is a serious scalability restriction.

To address this scalability problem, the Cisco Networking Services event bus has a point-to-point connection feature that communicates directly back to the poller station.

Benefits of Cisco Networking Services Flow-Through Provisioning

Automated Configuration

Cisco Networking Services flow-through provisioning simplifies installation by moving configuration requirements to the Cisco Networking Services configuration engine and allowing the Cisco configuration to update automatically. The registrar uses popular industry standards and technologies such as XML, Active Directory Services Interface (ADSI)/Active Directory, HTTP/Web Server, ATM Switch Processor (ASP), and Publish-Subscribe Event Bus. The Cisco Networking Services configuration agent enables the Cisco Networking Services configuration engine to configure remote devices in a plug-and-play manner.

Unique IP Addresses and Hostname

Cisco Networking Services flow-through provisioning uses DNS reverse lookup to retrieve the hostname by passing the IP address, then assigns the IP address and optionally the hostname to the remote device. Both IP address and hostname are thus guaranteed to be unique.

Reduced Technical Personnel Requirements

Cisco Networking Services flow-through provisioning permits remote devices to be installed by a person with limited or no technical experience. Because configuration occurs automatically on connection to the network, a network engineer or technician is not required for installation.

Rapid Deployment

Because a person with limited or no technical experience can install a remote device immediately without any knowledge or use of Cisco software, the device can be sent directly to its final premises and be brought up without technician deployment.

Direct Shipping

Devices can be shipped directly to the remote end-user site, eliminating warehousing and manual handling. Configuration occurs automatically on connection to the network.

Remote Updates

Cisco Networking Services flow-through provisioning automatically handles configuration updates, service additions, and deletions. The Cisco Networking Services configuration engine performs a push operation to send the information to the remote device.

Security

Event traffic to and from the remote device is opaque to unauthorized listeners or intruders to your network. Cisco Networking Services agents leverage the latest security features in Cisco software.

Cisco Networking Services Event Agent Parameters

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

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

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



Note

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

How to Configure Cisco Networking Services Flow-Through Provisioning

Configuring the Cisco Networking Services Event and EXEC Agents

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	cns config partial <i>{host-name ip-address}</i> [encrypt] <i>[port-number]</i> [source interface name] [inventory] Example: Device(config)# cns config partial 172.28.129.22 80	(Optional) Starts the Cisco Networking Services configuration agent, which provides Cisco Networking Services configuration services to Cisco clients, and initiates an incremental (partial) configuration. <ul style="list-style-type: none"> • Use the optional <i>port-number</i> argument to specify the port number for the configuration server. The default is 80. • Use the optional source keyword and <i>ip-address</i> argument to specify the use of an IP address as the source for Cisco Networking Services configuration agent communications. • Use the optional inventory keyword to send an inventory of the linecards and modules in the device to the Cisco Networking Services configuration engine as part of the HTTP request.

	Command or Action	Purpose
		Note The optional encrypt keyword is available only in images that support SSL.
Step 4	logging cns-events [<i>severity-level</i>] Example: Device(config)# logging cns-events 2	(Optional) Enables XML-formatted system event message logging to be sent through the Cisco Networking Services event bus. <ul style="list-style-type: none"> Use the optional <i>severity-level</i> argument to specify the number or name of the desired severity level at which messages should be logged. The default is level 7 (debugging).
Step 5	cns exec [encrypt] [<i>port-number</i>] [source { <i>ip-address</i> <i>interface-type-number</i> }] Example: Device(config)# cns exec source 172.17.2.2	(Optional) Enables and configures the Cisco Networking Services EXEC agent, which provides Cisco Networking Services EXEC services to Cisco clients. <ul style="list-style-type: none"> Use the optional <i>port-number</i> argument to specify the port number for the EXEC server. The default is 80. Use the optional source keyword and <i>ip-address/interface-type number</i> argument to specify the use of an IP address as the source for Cisco Networking Services EXEC agent communications. Note The optional encrypt keyword is available only in images that support SSL.
Step 6	cns event { <i>hostname</i> <i>ip-address</i> } [encrypt] [<i>port-number</i>] [backup] [failover-time <i>seconds</i>] [keepalive <i>seconds</i> <i>retry-count</i>] [source <i>ip-address</i> <i>interface-name</i>][clock-timeout <i>time</i>] [reconnect-time <i>time</i>] Example: Device(config)# cns event 172.28.129.22 source 172.22.2.1	Configures the Cisco Networking Services event gateway, which provides Cisco Networking Services event services to Cisco clients. <ul style="list-style-type: none"> The optional encrypt keyword is available only in images that support SSL. Use the optional <i>port-number</i> argument to specify the port number for the event server. The default is 11011 with no encryption and 11012 with encryption. Use the optional backup keyword to indicate that this is the backup gateway. Before configuring a backup gateway, ensure that a primary gateway is configured. Use the optional failover-time keyword and <i>seconds</i> argument to specify a time interval in seconds to wait for the primary gateway route after the route to the backup gateway is established. Use the optional keepalive keyword with the <i>seconds</i> and <i>retry-count</i> arguments to specify the keepalive timeout in seconds and the retry count. Use the optional source keyword and <i>ip-address/interface-name</i> argument to specify the use of an IP address as the source for Cisco Networking Services event agent communications. Use the optional clock-timeout keyword to specify the maximum time, in minutes, that the Cisco Networking Services event agent will wait for the clock to be set for transports (such as SSL) that require an accurate clock. Use the optional reconnect-time keyword to specify the configurable upper limit of the maximum retry timeout.

	Command or Action	Purpose
		Note Until the cns event command is entered, no transport connections to the Cisco Networking Services event bus are made and therefore no other Cisco Networking Services agents are operational.
Step 7	exit Example: Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

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

Configuration Examples for Cisco Networking Services Flow-Through Provisioning

Example: Cisco Networking Services Flow-Through Provisioning

Example: Cisco Configuration Express File Using T1 over HDLC Protocol

The following example shows use of the Cisco Configuration Express file to configure the remote device before delivery to its final premises. In the example, 172.28.129.22 is the IP address of the Cisco Networking Services configuration engine.

```
cns config initial 172.28.129.22 no-persist
!cns configure and event agents
cns event 172.28.129.22
controller t1 0
!T1 configuration
framing esf
linecode b8zs
channel-group 0 timeslots 1-24 speed 64
exit
cns id s0:0 ipaddress
interface s0:0
!Assigns IP address to s0:0
ip address slarp retry 2
exit
ip route 10.0.0.0 0.0.0.0 s0:0
!IP static route
end
```

Example: T1 Configuration Template

The following example shows use of the T1 configuration template to build the configuration for use on T1:

```
hostname ${LDAP://this:attrName=IOShostname}
enable password ${LDAP://this:attrName=IOSpassword}
controller T1 0
clock source ${LDAP://this:attrName=IOST1-clocksource}
linecode ${LDAP://this:attrName=IOST1-line}
framing ${LDAP://this:attrName=IOST1-framing}
channel-group ${LDAP://this:attrName=IOST1-channel-group}
timeslots ${LDAP://this:attrName=IOST1-timeslots}
speed ${LDAP://this:attrName=IOST1-speed}
```

Example: Voice Configuration Template

The following example shows use of the voice configuration template to build the configuration for using voice:

```
voice-port 1/1
codec ${LDAP://this:attrName=IOSvoice-port1}
exit
dial-peer voice 1 pots
application ${LDAP://this:attrName=IOSdial-peer1}
port 1/1
```

Example: Remote Device

The following example shows a remote device configuration:

```
Router# show running-config
Current configuration: 1659 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname tira-24V
!
!
network-clock base-rate 64k
ip subnet-zero
ip cef
!
ip audit notify log
ip audit po max-events 100
!
class-map match-any voice
match access-group 100
!
!
policy-map qos
class voice
priority percent 70
voice service voip
h323
!
no voice confirmation-tone
voice-card 0
!
!
controller T1 0
framing sf
linecode ami
!
controller T1 1
```

```

mode cas
framing esf
linecode b8zs
ds0-group 0 timeslots 1 type e&m-immediate-start
ds0-group 1 timeslots 2 type e&m-immediate-start
!
!
interface Ethernet0
ip address 10.1.1.2 255.255.0.0
!
interface Serial0
bandwidth 1536
ip address 10.11.11.1 255.255.255.0
no ip mroute-cache
load-interval 30
clockrate 148000
!
ip classless
ip route 223.255.254.254 255.255.255.0 10.3.0.1
!
no ip http server
ip pim bidir-enable
!
access-list 100 permit udp any range 16384 32767 any
access-list 100 permit tcp any any eq 1720
call rsvp-sync
!
voice-port 1:0
timeouts wait-release 3
!
voice-port 1:1
timeouts wait-release 3
!
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 1000 pots
destination-pattern 1000
port 1:0
forward-digits 0
!
dial-peer voice 1001 pots
destination-pattern 1001
no digit-strip
port 1:1
forward-digits 0
!
dial-peer voice 2000 voip
destination-pattern 2000
session target ipv4:10.11.11.2
codec g711ulaw
!
dial-peer voice 2001 voip
destination-pattern 2001
session target ipv4:10.11.11.2
signal-type ext-signal
codec g711ulaw
!
!
line con 0
line aux 0
line 2 3
line vty 0 4

```

Example: Using a Serial Interface

The following example shows configuration of a serial interface to connect to and download a configuration from a Cisco IE2100 Cisco Networking Services configuration engine. The IE2100 IP address is 10.1.1.1. The gateway IP address to reach the 10.1.1.0 network is 10.11.11.1. The Cisco Networking Services default

ID is the hostname, so that the **cns id** command is not needed. However, the **hostname** command is key to retrieving the configuration file on the Cisco Networking Services configuration engine.

This configuration auto-tries every serial interface on the remote router, applies the **config-cli** commands to that interface, and tries to ping the address specified in the **cns config initial** command. When it succeeds, it performs a normal initial configuration.

```
! Initial basic configuration (serial interface) PPP
cns connect serial retry-interval 1 retries 1
config-cli ip address negotiated
config-cli encapsulation ppp
config-cli ip directed-broadcast
config-cli no keepalive
config-cli no shutdown
exit
hostname 26ML
ip route 10.1.1.1 255.255.255.0 10.11.11.1
cns config initial 10.1.1.1 no-persist
cns inventory config
! Initial basic configuration (serial interface) HDLC
cns config connect serial retry-interval 1 retries 1
config-cli ip address slarp retry 1
config-cli no shutdown
exit
hostname tira-36V
ip route 10.1.1.1 255.255.255.0 10.11.11.1
cns config initial 10.1.1.1 no-persist
cns inventory config
Incremental configuration (serial interface)
cns config partial 10.1.1.1
cns event 10.1.1.1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco Networking Services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Cisco Networking Services Command Reference
Cisco Networking Services Configuration Engine	Cisco CNS Configuration Engine Administrator Guide, 1.3

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Networking Services Flow-Through Provisioning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Cisco Networking Services Flow-Through Provisioning

Feature Name	Releases	Feature Information
Cisco Networking Services Flow-Through Provisioning	Cisco IOS XE Release 3.8S 12.2(8)T	<p>The Cisco Networking Services Flow-Through Provisioning feature provides the infrastructure for automated configuration of large numbers of network devices. Based on Cisco Networking Services event and configuration agents, it eliminates the need for an onsite technician to initialize the device. The result is an automated workflow from initial subscriber-order entry through Cisco manufacturing and shipping to final device provisioning and subscriber billing. This focuses on a root problem of service providers and other similar business models; use of human labor in activating service.</p> <p>The following commands were introduced or modified by this feature: cns config cancel, cns config initial, cns config partial, cns event, cns id, cns inventory, cns mib-access encapsulation, cns notifications encapsulation, config-cli, debug cns config, debug cns event, debug cns management, debug cns xml-parser, line cli, show cns config connections, show cns config outstanding, show cns event stats, show cns event subject.</p> <p>Note The cns config connect-intf was replaced by the cns connect and cns template connect commands.</p>