



## **Cisco Nexus 3500 Series NX-OS Programmability Guide, Release 9.2(x)**

**First Published:** 2018-07-19

**Last Modified:** 2019-07-24

### **Americas Headquarters**

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2019 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### PREFACE

<b>Preface</b>	<b>xi</b>
Audience	xi
Document Conventions	xi
Related Documentation for Cisco Nexus 3000 Series Switches	xii
Documentation Feedback	xii
Communications, Services, and Additional Information	xii

---

### CHAPTER 1

<b>New and Changed Information</b>	<b>1</b>
New and Changed Information	1

---

### CHAPTER 2

<b>Bash</b>	<b>3</b>
About Bash	3
Accessing Bash	3
Escalate Privileges to Root	4
Examples of Bash Commands	5
Displaying System Statistics	5
Running Bash from CLI	5
Running Python from Bash	6

---

### CHAPTER 3

<b>Guest Shell</b>	<b>7</b>
About the Guest Shell	7
Guidelines and Limitations	8
Accessing the Guest Shell	12
Resources Used for the Guest Shell	13
Capabilities in the Guest Shell	13
NX-OS CLI in the Guest Shell	13

Network Access in Guest Shell	14
Access to Bootflash in Guest Shell	16
Python in Guest Shell	16
Python 3 in Guest Shell 2.x (Centos 7)	17
Installing RPMs in the Guest Shell	20
Security Posture for Guest Shell	21
Kernel Vulnerability Patches	21
ASLR and X-Space Support	21
Namespace Isolation	22
Root-User Restrictions	23
Resource Management	23
Guest File System Access Restrictions	24
Managing the Guest Shell	24
Disabling the Guest Shell	27
Destroying the Guest Shell	28
Enabling the Guest Shell	28
Replicating the Guest Shell	29
Exporting Guest Shell rootfs	30
Importing Guest Shell rootfs	30
Importing YAML File	31
show guestshell Command	35
Verifying Virtual Service and Guest Shell Information	35
Persistently Starting Your Application From the Guest Shell	37
Procedure for Persistently Starting Your Application from the Guest Shell	38
An Example Application in the Guest Shell	38
Troubleshooting Guest Shell Issues	39

**CHAPTER 4****Python API 41**

About the Python API	41
Using Python	41
Cisco Python Package	41
Using the CLI Command APIs	42
Invoking the Python Interpreter from the CLI	44
Display Formats	44

Non-interactive Python	46
Running Scripts with Embedded Event Manager	47
Python Integration with Cisco NX-OS Network Interfaces	47
Cisco NX-OS Security with Python	48
Examples of Security and User Authority	48
Example of Running Script with Scheduler	50

---

**CHAPTER 5****Scripting with Tcl 51**

About Tcl	51
Tclsh Command Help	51
Tclsh Command History	52
Tclsh Tab Completion	52
Tclsh CLI Command	52
Tclsh Command Separation	52
Tcl Variables	53
Telquit	53
Tclsh Security	53
Running the Tclsh Command	53
Navigating Cisco NX-OS Modes from the Tclsh Command	54
Tcl References	56

---

**CHAPTER 6****Ansible 57**

Prerequisites	57
About Ansible	57
Cisco Ansible Module	57

---

**CHAPTER 7****Puppet Agent 59**

About Puppet	59
Prerequisites	59
Puppet Agent NX-OS Environment	60
cispuppet Module	60

---

**CHAPTER 8****Using Chef Client with Cisco NX-OS 63**

About Chef	63
------------	----

Prerequisites 63  
 Chef Client NX-OS Environment 64  
 cisco-cookbook 64

---

**CHAPTER 9**

**Using Docker with Cisco NX-OS 67**

About Docker with Cisco NX-OS 67  
 Guidelines and Limitations 67  
 Prerequisites for Setting Up Docker Containers Within Cisco NX-OS 68  
 Starting the Docker Daemon 68  
 Configure Docker to Start Automatically 69  
 Starting Docker Containers: Host Networking Model 69  
 Starting Docker Containers: Bridged Networking Model 71  
 Mounting the bootflash and volatile Partitions in the Docker Container 72  
 Enabling Docker Daemon Persistence on Enhanced ISSU Switchover 72  
 Enabling Docker Daemon Persistence on the Cisco Nexus 9500 Series Switches Switchover 73  
 Resizing the Docker Storage Backend 74  
 Stopping the Docker Daemon 76  
 Docker Container Security 76  
   Securing Docker Containers With User namespace Isolation 77  
   Moving the cgroup Partition 77  
 Docker Troubleshooting 78  
   Docker Fails to Start 78  
   Docker Fails to Start Due to Insufficient Storage 79  
   Failure to Pull Images from Docker Hub (509 Certificate Expiration Error Message) 79  
   Failure to Pull Images from Docker Hub (Client Timeout Error Message) 79  
   Docker Daemon or Containers Not Running On Switch Reload or Switchover 80  
   Resizing of Docker Storage Backend Fails 80  
   Docker Container Doesn't Receive Incoming Traffic On a Port 81  
   Unable to See Data Port And/Or Management Interfaces in Docker Container 81  
   General Troubleshooting Tips 81

---

**CHAPTER 10**

**NX-API 83**

About NX-API 83  
 Feature NX-API 83

	Transport	84
	Message Format	84
	Security	84
	Using NX-API	84
	NX-API Management Commands	86
	Working With Interactive Commands Using NX-API	88
	NX-API Request Elements	88
	NX-API Response Elements	91
	About JSON (JavaScript Object Notation)	92
	CLI Execution	92
	XML and JSON Supported Commands	92
	Examples of XML and JSON Output	93
<hr/>		
<b>CHAPTER 11</b>	<b>NX-API Response Codes</b>	<b>95</b>
	Table of NX-API Response Codes	95
<hr/>		
<b>CHAPTER 12</b>	<b>NX-API Developer Sandbox</b>	<b>97</b>
	NX-API Developer Sandbox: NX-OS Releases Prior to 9.2(2)	97
	About the NX-API Developer Sandbox	97
	Guidelines and Limitations	98
	Configuring the Message Format and Command Type	98
	Using the Developer Sandbox	100
	Using the Developer Sandbox to Convert CLI Commands to Payloads	100
	NX-API Developer Sandbox: NX-OS Release 9.2(2) and Later	102
	About the NX-API Developer Sandbox	102
	Guidelines and Limitations	103
	Configuring the Message Format and Input Type	104
	Using the Developer Sandbox	106
	Using the Developer Sandbox to Convert CLI Commands to REST Payloads	106
	Using the Developer Sandbox to Convert from REST Payloads to CLI Commands	109
	Using the Developer Sandbox to Convert from RESTCONF to json or XML	114
<hr/>		
<b>CHAPTER 13</b>	<b>XML Support for ABM and LM in N3500</b>	<b>117</b>
	XML Support for ABM and LM in N3500	117

---

<b>CHAPTER 14</b>	<b>Converting CLI Commands to Network Configuration Format</b>	<b>125</b>
	Information About XMLIN	125
	Licensing Requirements for XMLIN	125
	Installing and Using the XMLIN Tool	126
	Converting Show Command Output to XML	126
	Configuration Examples for XMLIN	127

---

<b>CHAPTER 15</b>	<b>Model-Driven Telemetry</b>	<b>131</b>
	About Telemetry	131
	Telemetry Components and Process	131
	High Availability of the Telemetry Process	133
	Licensing Requirements for Telemetry	133
	Installing and Upgrading Telemetry	133
	Guidelines and Limitations	134
	Configuring Telemetry Using the CLI	139
	Configuring Telemetry Using the NX-OS CLI	139
	Configuration Examples for Telemetry Using the CLI	143
	Displaying Telemetry Configuration and Statistics	146
	Displaying Telemetry Log and Trace Information	151
	Configuring Telemetry Using the NX-API	153
	Configuring Telemetry Using the NX-API	153
	Configuration Example for Telemetry Using the NX-API	162
	Telemetry Model in the DME	165
	Additional References	166
	Related Documents	166

---

<b>CHAPTER 16</b>	<b>XML Management Interface</b>	<b>167</b>
	About the XML Management Interface	167
	About the XML Management Interface	167
	NETCONF Layers	167
	SSH xmlagent	168
	Licensing Requirements for the XML Management Interface	168
	Prerequisites to Using the XML Management Interface	169

Using the XML Management Interface	169
Configuring SSH and the XML Server Options	169
Starting an SSH Session	169
Sending the Hello Message	170
Obtaining the XSD Files	170
Sending an XML Document to the XML Server	171
Creating NETCONF XML Instances	171
RPC Request Tag rpc	172
NETCONF Operations Tags	173
Device Tags	174
Extended NETCONF Operations	176
NETCONF Replies	179
RPC Response Tag	180
Interpreting Tags Encapsulated in the Data Tag	180
Information About Example XML Instances	181
Example XML Instances	181
NETCONF Close Session Instance	181
NETCONF Kill-session Instance	182
NETCONF copy-config Instance	182
NETCONF edit-config Instance	182
NETCONF get-config Instance	184
NETCONF Lock Instance	184
NETCONF unlock Instance	185
NETCONF Commit Instance - Candidate Configuration Capability	186
NETCONF Confirmed-commit Instance	186
NETCONF rollback-on-error Instance	186
NETCONF validate Capability Instance	187
Additional References	187
<hr/>	
<b>APPENDIX A</b>	<b>Streaming Telemetry Sources 189</b>
	About Streaming Telemetry 189
	Guidelines and Limitations 189
	Data Available for Telemetry 189





## Preface

---

This preface includes the following sections:

- [Audience, on page xi](#)
- [Document Conventions, on page xi](#)
- [Related Documentation for Cisco Nexus 3000 Series Switches, on page xii](#)
- [Documentation Feedback, on page xii](#)
- [Communications, Services, and Additional Information, on page xii](#)

## Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

## Document Conventions

Command descriptions use the following conventions:

Convention	Description
<b>bold</b>	Bold text indicates the commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
<i>variable</i>	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
<>	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

## Related Documentation for Cisco Nexus 3000 Series Switches

The entire Cisco Nexus 3000 Series switch documentation set is available at the following URL:

<https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html>

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to [nexus3k-docfeedback@cisco.com](mailto:nexus3k-docfeedback@cisco.com). We appreciate your feedback.

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

### **Cisco Bug Search Tool**

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.





# CHAPTER 1

## New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 3500 Series NX-OS Programmability Guide, Release 9.2(x)*.

- [New and Changed Information, on page 1](#)

## New and Changed Information

This table summarizes the new and changed features for the *Cisco Nexus 3500 Series NX-OS Programmability Guide, Release 9.2(x)* and where they are documented.

**Table 1: New and Changed Features**

Feature	Description	Changed in Release	Where Documented
	Changed the document title from 9.x to 9.2(x)		Doc Title
Convert CLI commands for NETCONF	Support for converting NX-OS CLI commands to Network Configuration format is documented.	9.2(2)	<a href="#">Converting CLI Commands to Network Configuration Format, on page 125</a>
Updates to NX-API Developer Sandbox	Various enhancements have been added to the NX-API Developer Sandbox.	9.2(2)	<a href="#">NX-API Developer Sandbox, on page 97</a>
XML Management Interface	Support for managing the Cisco Nexus 3500 switches with an XML-based tool through the XML-based Network Configuration Protocol (NETCONF) is documented.	9.2(2)	<a href="#">XML Management Interface, on page 167</a>
Using Docker on Cisco NX-OS on a switch.	Added support for using Docker on Cisco NX-OS on a switch.	9.2(1)	<a href="#">Using Docker with Cisco NX-OS, on page 67</a>

Feature	Description	Changed in Release	Where Documented
Streaming telemetry on Cisco Nexus 3500XL.	Added support for streaming telemetry on the Cisco Nexus 3500XL.	9.2(1)	<a href="#">Model-Driven Telemetry, on page 131</a> and <a href="#">Streaming Telemetry Sources, on page 189</a>
gRPC chunking as part of telemetry.	Added support for gRPC chunking as part of telemetry.	9.2(1)	<a href="#">Model-Driven Telemetry, on page 131</a>
Changes to Guest Shell.	As a result of a kernel upgrade that is part of Release 9.2(1), some behaviors with Guest Shell have changed.	9.2(1)	<a href="#">Guest Shell, on page 7</a>



## CHAPTER 2

# Bash

---

- [About Bash, on page 3](#)
- [Accessing Bash, on page 3](#)
- [Escalate Privileges to Root, on page 4](#)
- [Examples of Bash Commands, on page 5](#)

## About Bash

In addition to the NX-OS CLI, Cisco Nexus 3500 Series devices support access to the Bourne-Again SHell (Bash). Bash interprets commands that you enter or commands that are read from a shell script. Using Bash enables access to the underlying Linux system on the device and to manage the system.

## Accessing Bash

In Cisco NX-OS, Bash is accessible from user accounts that are associated with the Cisco NX-OS dev-ops role or the Cisco NX-OS network-admin role.

The following example shows the authority of the dev-ops role and the network-admin role:

```
switch# show role name dev-ops

Role: dev-ops
  Description: Predefined system role for devops access. This role
  cannot be modified.
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
-----
Rule      Perm   Type      Scope      Entity
-----
4         permit command  conf t ; username *
3         permit command  bcm module *
2         permit command  run bash *
1         permit command  python *

switch# show role name network-admin

Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
-----
```

```

Rule      Perm      Type      Scope      Entity
-----
1         permit   read-write
switch#

```

Bash is enabled by running the **feature bash-shell** command.

The **run bash** command loads Bash and begins at the home directory for the user.

The following examples show how to enable the Bash shell feature and how to run Bash.

```

switch# configure terminal
switch(config)# feature bash-shell

switch# run bash
Linux# whoami
admin
Linux# pwd
/bootflash/home/admin
Linux#

```



**Note** You can also execute Bash commands with the **run bash <command>** command.

The following is an example of the **run bash <command>** command.

```
run bash whoami
```

## Escalate Privileges to Root

The privileges of an admin user can escalate their privileges for root access.

The following are guidelines for escalating privileges:

- Only an admin user can escalate privileges to root.
- Bash must be enabled before escalating privileges.
- Escalation to root is password protected.
- SSH to the switch using `root` username through a non-management interface will default to Linux Bash shell-type access for the root user. Type `vsh` to return to NX-OS shell access.

The following example shows how to escalate privileges to root and how to verify the escalation:

```

switch# run bash
Linux# sudo su root

```

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

- ```

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

```

```
Password:
```

```
Linux# whoami
```

```
root
Linux# exit
exit
```

## Examples of Bash Commands

This section contains examples of Bash commands and output.

### Displaying System Statistics

The following example shows how to display system statistics:

```
switch# run bash
Linux# cat /proc/meminfo
MemTotal:      3795100 kB
MemFree:       1472680 kB
Buffers:       136 kB
Cached:        1100116 kB
ShmFS:         1100116 kB
Allowed:       948775 Pages
Free:          368170 Pages
Available:     371677 Pages
SwapCached:    0 kB
Active:        1198872 kB
Inactive:      789764 kB
SwapTotal:     0 kB
SwapFree:      0 kB
Dirty:         0 kB
Writeback:     0 kB
AnonPages:     888272 kB
Mapped:        144044 kB
Slab:          148836 kB
SReclaimable: 13892 kB
SUnreclaim:   134944 kB
PageTables:    28724 kB
NFS_Unstable:  0 kB
Bounce:        0 kB
WritebackTmp:  0 kB
CommitLimit:  1897548 kB
Committed_AS: 19984932 kB
VmallocTotal: 34359738367 kB
VmallocUsed:   215620 kB
VmallocChunk: 34359522555 kB
HugePages_Total: 0
HugePages_Free: 0
HugePages_Rsvd: 0
HugePages_Surp: 0
Hugepagesize: 2048 kB
DirectMap4k:   40960 kB
DirectMap2M:   4190208 kB
Linux#
```

### Running Bash from CLI

The following example shows how to run a bash command from the CLI with the `run bash <command>` command:

```

switch# run bash ps -el
F S  UID  PID  PPID  C  PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
4 S  0    1    0  0  80  0  -   497 select ?      00:00:08 init
5 S  0    2    0  0  75 -5  -    0 kthrea ?      00:00:00 kthreadd
1 S  0    3    2  0 -40  -  -    0 migrat ?      00:00:00 migration/0
1 S  0    4    2  0  75 -5  -    0 ksofti ?      00:00:01 ksoftirqd/0
5 S  0    5    2  0  58  -  -    0 watchd ?      00:00:00 watchdog/0
1 S  0    6    2  0 -40  -  -    0 migrat ?      00:00:00 migration/1
1 S  0    7    2  0  75 -5  -    0 ksofti ?      00:00:00 ksoftirqd/1
5 S  0    8    2  0  58  -  -    0 watchd ?      00:00:00 watchdog/1
1 S  0    9    2  0 -40  -  -    0 migrat ?      00:00:00 migration/2
1 S  0   10    2  0  75 -5  -    0 ksofti ?      00:00:00 ksoftirqd/2
5 S  0   11    2  0  58  -  -    0 watchd ?      00:00:00 watchdog/2
1 S  0   12    2  0 -40  -  -    0 migrat ?      00:00:00 migration/3
1 S  0   13    2  0  75 -5  -    0 ksofti ?      00:00:00 ksoftirqd/3
5 S  0   14    2  0  58  -  -    0 watchd ?      00:00:00 watchdog/3

...

4 S  0  8864    1  0  80  0  -   2249 wait  ttyS0  00:00:00 login
4 S  2002 28073  8864  0  80  0  -   69158 select ttyS0  00:00:00 vsh
4 R  0  28264  3782  0  80  0  -   54790 select ?      00:00:00 in.dcos-telnet
4 S  0  28265  28264  0  80  0  -   2247 wait  pts/0  00:00:00 login
4 S  2002 28266  28265  0  80  0  -   69175 wait  pts/0  00:00:00 vsh
1 S  2002 28413  28266  0  80  0  -   69175 wait  pts/0  00:00:00 vsh
0 R  2002 28414  28413  0  80  0  -    887  -     pts/0  00:00:00 ps
switch#

```

## Running Python from Bash

The following example shows how to load Python and configure a switch using Python objects:

```

switch# run bash
Linux# python
Python 2.7.5 (default, May 16 2014, 10:58:01)
[GCC 4.3.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
Loaded cisco NxOS lib!
>>>
>>> from cisco import *
>>> from cisco.vrf import *
>>> from cisco.interface import *
>>> vrfobj=VRF('myvrf')
>>> vrfobj.get_name()
'myvrf'
>>> vrfobj.add_interface('Ethernet1/3')
True
>>> intf=Interface('Ethernet1/3')
>>> print intf.config()

!Command: show running-config interface Ethernet1/3
!Time: Thu Aug 21 23:32:25 2014

version 6.0(2)U4(1)

interface Ethernet1/3
 no switchport
 vrf member myvrf

>>>

```



## CHAPTER 3

# Guest Shell

---

- [About the Guest Shell, on page 7](#)
- [Guidelines and Limitations, on page 8](#)
- [Accessing the Guest Shell, on page 12](#)
- [Resources Used for the Guest Shell, on page 13](#)
- [Capabilities in the Guest Shell, on page 13](#)
- [Security Posture for Guest Shell, on page 21](#)
- [Guest File System Access Restrictions , on page 24](#)
- [Managing the Guest Shell, on page 24](#)
- [Verifying Virtual Service and Guest Shell Information, on page 35](#)
- [Persistently Starting Your Application From the Guest Shell, on page 37](#)
- [Procedure for Persistently Starting Your Application from the Guest Shell, on page 38](#)
- [An Example Application in the Guest Shell, on page 38](#)
- [Troubleshooting Guest Shell Issues, on page 39](#)

## About the Guest Shell

In addition to the NX-OS CLI and Bash access on the underlying Linux environment, the Cisco Nexus Series devices support access to a decoupled execution space running within a Linux Container (LXC) called the “Guest Shell”.

From within the Guest Shell the network-admin has the following capabilities:

- Access to the network over Linux network interfaces.
- Access to Cisco Nexus bootflash.
- Access to Cisco Nexus volatile tmpfs.
- Access to Cisco Nexus CLI.
- Access to Cisco NX-API REST.
- The ability to install and run python scripts.
- The ability to install and run 32-bit and 64-bit Linux applications.

Decoupling the execution space from the native host system allows customization of the Linux environment to suit the needs of the applications without impacting the host system or applications running in other Linux Containers.

On NX-OS devices, Linux Containers are installed and managed with the virtual-service commands. The Guest Shell will appear in the virtual-service show command output.




---

**Note** By default, the Guest Shell occupies approximately 35 MB of RAM and 200 MB of bootflash when enabled. Use the **guestshell destroy** command to reclaim resources if the Guest Shell is not used.

---

## Guidelines and Limitations

### Common Guidelines Across All Releases



#### Important

If you have performed custom work inside your installation of the Guest Shell, save your changes to bootflash, off-box storage, or elsewhere outside the Guest Shell root file system before performing a `guestshell upgrade`.

The `guestshell upgrade` command essentially performs a `guestshell destroy` and `guestshell enable` in succession.

- Use the `run guestshell` CLI command to access the Guest Shell on the Cisco Nexus device: The `run guestshell` command parallels the `run bash` command that is used to access the host shell. This command allows you to access the Guest Shell and get a Bash prompt or run a command within the context of the Guest Shell. The command uses password-less SSH to an available port on the localhost in the default network namespace.
- `sshd` utility can secure the pre-configured SSH access into the Guest Shell by listening on localhost to avoid connection attempts from outside the network. `sshd` has the following features
  - It is configured for key-based authentication without fallback to passwords.
  - Only `root` can read keys use to access the Guest Shell after Guest Shell restarts.
  - Only `root` can read the file that contains the key on the host to prevent a nonprivileged user with host Bash access from being able to use the key to connect to the Guest Shell. Network-admin users may start another instance of `sshd` in the Guest Shell to allow remote access directly into the Guest Shell, but any user that logs into the Guest Shell is also given network-admin privilege.




---

**Note** Introduced in Guest Shell 2.2 (0.2), the key file is readable for whom the user account was created for.

In addition, the Guest Shell accounts are not automatically removed, and must be removed by the network administrator when no longer needed.

Guest Shell installations before 2.2 (0.2) will not dynamically create individual user accounts.

---

- Installing the Cisco Nexus series switch software release on a fresh out-of-the-box Cisco Nexus switch will automatically enable the Guest Shell. Subsequent upgrades to the Cisco Nexus series switch software will not automatically upgrade Guest Shell.
- Guest Shell releases increment the major number when distributions or distribution versions change.
- Guest Shell releases increment the minor number when CVEs have been addressed. The Guest Shell will update CVEs only when CentOS makes them publically available.
- Cisco recommends using **yum update** to pick up third-party security vulnerability fixes directly from the CentOS repository. This provides the flexibility of getting updates as, and when, available without needing to wait for a Cisco NX-OS software update.

Alternatively, using the **guestshell update** command would replace the existing Guest Shell rootfs. Any customizations and software package installations would then need to be performed again within the context of this new Guest Shell rootfs.

### Upgrading from Guest Shell 1.0 to Guest Shell 2.x

Guest Shell 2.x is based on a CentOS 7 root file system. If you have an off-box repository of `.conf` files or utilities that pulled the content down into Guest Shell 1.0, you will need to repeat the same deployment steps in Guest Shell 2.x. Your deployment script may need to be adjusted to account for the CentOS 7 differences.

### Guest Shell 2.x

The Cisco NX-OS automatically installs and enables the Guest Shell by default on systems with sufficient resources. However, if the device is reloaded with a Cisco NX-OS image that does not provide Guest Shell support, the installer will automatically remove the existing Guest Shell and issue a `%VMAN-2-INVALID_PACKAGE`.



**Note** Systems with 4GB of RAM will not enable Guest Shell by default. Use the **guestshell enable** command to install and enable Guest Shell.

The **install all** command validates the compatibility between the current Cisco NX-OS image against the target Cisco NX-OS image.

The following is an example output from installing an incompatible image:

```
switch#
Installer will perform compatibility check first. Please wait.
uri is: /
2014 Aug 29 20:08:51 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully activated virtual service 'guestshell+'
Verifying image bootflash:/n9kpregs.bin for boot variable "nxos".
[#####] 100% -- SUCCESS
Verifying image type.
[#####] 100% -- SUCCESS
Preparing "" version info using image bootflash:/.
[#####] 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/.
[#####] 100% -- SUCCESS
Preparing "" version info using image bootflash:/.
[#####] 100% -- SUCCESS
Preparing "" version info using image bootflash:/.
```

```
[#####] 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/
[#####] 100% -- SUCCESS
Preparing "" version info using image bootflash:/
[#####] 100% -- SUCCESS
Preparing "" version info using image bootflash:/
[#####] 100% -- SUCCESS
"Running-config contains configuration that is incompatible with the new image (strict
incompatibility).
Please run 'show incompatibility-all nxos <image>' command to find out which feature
needs to be disabled.".
Performing module support checks.
[#####] 100% -- SUCCESS
Notifying services about system upgrade.
[# ] 0% -- FAIL.
Return code 0x42DD0006 ((null)).
"Running-config contains configuration that is incompatible with the new image (strict
incompatibility).
Please run 'show incompatibility-all nxos <image>' command to find out
which feature needs to be disabled."
Service "vman" in vdc 1: Guest shell not supported, do 'guestshell destroy' to remove
it and then retry ISSU
Pre-upgrade check failed. Return code 0x42DD0006 ((null)).
switch#
```




---

**Note** As a best practice, remove the Guest Shell with the **guestshell destroy** command before reloading an older Cisco Nexus image that does not support the Guest Shell.

---

### Pre-Configured SSHD Service

The Guest Shell starts an OpenSSH server upon boot up. The server listens on a randomly generated port on the localhost IP address interface 127.0.0.1 only. This provides the password-less connectivity into the Guest Shell from the NX-OS virtual-shell when the **guestshell** keyword is entered. If this server is killed or its configuration (residing in `/etc/ssh/sshd_config-cisco`) is altered, access to the Guest Shell from the NX-OS CLI might not work.

The following steps instantiate an OpenSSH server within the Guest Shell as root:

1. Determine which network namespace or VRF you want to establish your SSH connections through.
2. Determine the port that you want OpenSSH to listen on. Use the NX-OS command **show socket connection** to view ports already in use.




---

**Note** The Guest Shell `sshd` service for password-less access uses a randomized port starting at 17680 through 49150. To avoid port conflict, choose a port outside this range.

---

The following steps start the OpenSSH server. The examples start the OpenSSH server for management netns on IP address 10.122.84.34:2222:

1. Create the following files: `/usr/lib/systemd/system/sshd-mgmt.service` and `/etc/ssh/sshd-mgmt_config`. The files should have the following configurations:

```
-rw-r--r-- 1 root root 394 Apr 7 14:21 /usr/lib/systemd/system/sshd-mgmt.service
-rw----- 1 root root 4478 Apr 7 14:22 /etc/ssh/sshd-mgmt_config
```

2. Copy the Unit and Service contents from the `/usr/lib/systemd/system/ssh.service` file to `sshd-mgmt.service`.

3. Edit the `sshd-mgmt.service` file to match the following:

```
[Unit]
Description=OpenSSH server daemon
After=network.target sshd-keygen.service
Wants=sshd-keygen.service

[Service]
EnvironmentFile=/etc/sysconfig/ssh
ExecStartPre=/usr/sbin/sshd-keygen
ExecStart=/sbin/ip netns exec management /usr/sbin/sshd -f /etc/ssh/sshd-mgmt_config
-D $OPTIONS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartSec=42s
[Install]
WantedBy=multi-user.target
```

4. Copy the contents of `/etc/ssh/sshd-config` to `/etc/ssh/sshd-mgmt_config`. Modify the `ListenAddress` IP and port as necessary.

```
Port 2222
ListenAddress 10.122.84.34
```

5. Start the `systemctl` daemon using the following commands:

```
sudo systemctl daemon-reload
sudo systemctl start sshd-mgmt.service
sudo systemctl status sshd-mgmt.service -l
```

6. (Optional) Check the configuration.

```
ss -tnldp | grep 2222
```

7. SSH into Guest Shell:

```
ssh -p 2222 guestshell@10.122.84.34
```

8. Save the configuration across multiple Guest Shell or switch reboots.

```
sudo systemctl enable sshd-mgmt.service
```

9. For passwordless SSH/SCP and remote execution, generate the public and private keys for the user ID you want to user for SSH/SCP using the `ssh-keygen -t dsa` command.

The key is then stored in the `id_rsa` and `id_rsa.pub` files in the `/.ssh` directory:

```
[root@node01 ~]# cd ~/.ssh
[root@node02 .ssh]# ls -l
total 8
-rw-----. 1 root root 1675 May 5 15:01 id_rsa
-rw-r--r--. 1 root root 406 May 5 15:01 id_rsa.pub
```

10. Copy the public key into the machine you want to SSH into and fix permissions:

```
cat id_rsa.pub >> /root/.ssh/authorized_keys
chmod 700 /root/.ssh
chmod 600 /root/.ssh/*
```

11. SSH or SCP into the remote switch without a password:

```
ssh -p <port#> userid@hostname [<remote command>]
scp -P <port#> userid@hostname/filepath /destination
```

### localtime

The Guest Shell shares `/etc/localtime` with the host system.



**Note** If you do not want to share the same localtime with the host, this symlink can be broken and a Guest Shell specific `/etc/localtime` can be created.

```
switch(config)# clock timezone PDT -7 0
switch(config)# clock set 10:00:00 27 Jan 2017
Fri Jan 27 10:00:00 PDT 2017
switch(config)# show clock
10:00:07.554 PDT Fri Jan 27 2017
switch(config)# run guestshell
guestshell:~$ date
Fri Jan 27 10:00:12 PDT 2017
```

## Accessing the Guest Shell

In Cisco NX-OS, the Guest Shell is accessible to the network-admin. It is automatically enabled in the system and can be accessed using the **run guestshell** command. Consistent with the **run bash** command, these commands can be issued within the Guest Shell with the **run guestshell** *command* form of the NX-OS CLI command.



**Note** The Guest Shell is automatically enabled on systems with more than 4 GB of RAM.

```
switch# run guestshell ls -al /bootflash/*.ova
-rw-rw-rw- 1 2002 503 83814400 Aug 21 18:04 /bootflash/pup.ova
-rw-rw-rw- 1 2002 503 40724480 Apr 15 2012 /bootflash/red.ova
```



**Note** When running in the Guest Shell, you have network-admin level privileges.



**Note** The Guest Shell starting in 2.2(0.2) will dynamically create user accounts with the same as the user logged into switch. However, all other information is NOT shared between the switch and the Guest Shell user accounts.

In addition, the Guest Shell accounts are not automatically removed, and must be removed by the network administrator when no longer needed.

## Resources Used for the Guest Shell

By default, the resources for the Guest Shell have a small impact on resources available for normal switch operations. If the network-admin requires additional resources for the Guest Shell, the **guestshell resize** {*cpu* | *memory* | *roofs*} command changes these limits.

| Resource | Default | Minimum/Maximum |
|----------|---------|-----------------|
| CPU      | 1%      | 1/%             |
| Memory   | 256MB   | 256/3840MB      |
| Storage  | 200MB   | 200/2000MB      |

The CPU limit is the percentage of the system compute capacity that tasks running within the Guest Shell are given when there is contention with other compute loads in the system. When there is no contention for CPU resources, the tasks within the Guest Shell are not limited.



**Note** A Guest Shell reboot is required after changing the resource allocations. This can be accomplished with the **guestshell reboot** command.

## Capabilities in the Guest Shell

The Guest Shell has a number of utilities and capabilities available by default.

The Guest Shell is populated with CentOS 7 Linux which provides the ability to Yum install software packages built for this distribution. The Guest Shell is pre-populated with many of the common tools that would naturally be expected on a networking device including **net-tools**, **iproute**, **tcpdump** and OpenSSH. Python 2.7.5 is included by default as is the PIP for installing additional python packages.

By default the Guest Shell is a 64-bit execution space. If 32-bit support is needed, the glibc.i686 package can be Yum installed.

The Guest Shell has access to the Linux network interfaces used to represent the management and data ports of the switch. Typical Linux methods and utilities like **ifconfig** and **ethtool** can be used to collect counters. When an interface is placed into a VRF in the NX-OS CLI, the Linux network interface is placed into a network namespace for that VRF. The name spaces can be seen at `/var/run/netns` and the **ip netns** utility can be used to run in the context of different namespaces. A couple of utilities, **chvrf** and **vrinfo**, are provided as a convenience for running in a different namespace and getting information about which namespace/vrf a process is running in.

systemd is used to manage services in CentOS 7 environments, including the Guest Shell.

## NX-OS CLI in the Guest Shell

The Guest Shell provides an application to allow the user to issue NX-OS commands from the Guest Shell environment to the host network element. The **dohost** application accepts any valid NX-OS configuration or exec commands and issues them to the host network element.

When invoking the **dohost** command each NX-OS command may be in single or double quotes:

```
dohost "<NXOS CLI>"
```

The NX-OS CLI can be chained together:

```
[guestshell@guestshell ~]$ dohost "sh lldp time | in Hold" "show cdp global"
Holdtime in seconds: 120
Global CDP information:
CDP enabled globally
Refresh time is 21 seconds
Hold time is 180 seconds
CDPv2 advertisements is enabled
DeviceID TLV in System-Name(Default) Format
[guestshell@guestshell ~]$
```

The NX-OS CLI can also be chained together using the NX-OS style command chaining technique by adding a semicolon between each command. (A space on either side of the semicolon is required.):

```
[guestshell@guestshell ~]$ dohost "conf t ; cdp timer 13 ; show run | inc cdp"
Enter configuration commands, one per line. End with CNTL/Z.
cdp timer 13
[guestshell@guestshell ~]$
```




---

**Note** Starting with Guest Shell 2.2 (0.2), commands issued on the host through the **dohost** command are run with privileges based on the effective role of the Guest Shell user.

Prior versions of Guest Shell will run command with network-admin level privileges.

The **dohost** command fails when the number of UDS connections to NX-API are at the maximum allowed.

---

## Network Access in Guest Shell

The NX-OS switch ports are represented in the Guest Shell as Linux network interfaces. Typical Linux methods like view stats in `/proc/net/dev`, through `ifconfig` or `ethtool` are all supported:

The Guest Shell has a number of typical network utilities included by default and they can be used on different VRFs using the **chvrf vrf command** command.

```
[guestshell@guestshell bootflash]$ ifconfig Eth1-47
Eth1-47: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 13.0.0.47 netmask 255.255.255.0 broadcast 13.0.0.255
ether 54:7f:ee:8e:27:bc txqueuelen 100 (Ethernet)
RX packets 311442 bytes 21703008 (20.6 MiB)
RX errors 0 dropped 185 overruns 0 frame 0
TX packets 12967 bytes 3023575 (2.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Within the Guest Shell, the networking state can be monitored, but may not be changed. To change networking state, use the NX-OS CLI or the appropriate Linux utilities in the host bash shell.

The **tcpdump** command is packaged with the Guest Shell to allow packet tracing of punted traffic on the management or switch ports.

The **sudo ip netns exec management ping** utility is a common method for running a command in the context of a specified network namespace. This can be done within the Guest Shell:

```
[guestshell@guestshell bootflash]$ sudo ip netns exec management ping 10.28.38.48
PING 10.28.38.48 (10.28.38.48) 56(84) bytes of data.
64 bytes from 10.28.38.48: icmp_seq=1 ttl=48 time=76.5 ms
```

The **chvrf** utility is provided as a convenience:

```
guestshell@guestshell bootflash]$ chvrf management ping 10.28.38.48
PING 10.28.38.48 (10.28.38.48) 56(84) bytes of data.
64 bytes from 10.28.38.48: icmp_seq=1 ttl=48 time=76.5 ms
```



**Note** Commands that are run without the **chvrf** command are run in the current VRF/network namespace.

For example, to ping IP address 10.0.0.1 over the management VRF, the command is “**chvrf management ping 10.0.0.1**”. Other utilities such as **scp** or **ssh** would be similar.

Example:

```
switch# guestshell
[guestshell@guestshell ~]$ cd /bootflash
[guestshell@guestshell bootflash]$ chvrf management scp foo@10.28.38.48:/foo/index.html
index.html
foo@10.28.38.48's password:
index.html 100% 1804 1.8KB/s 00:00
[guestshell@guestshell bootflash]$ ls -al index.html
-rw-r--r-- 1 guestshe users 1804 Sep 13 20:28 index.html
[guestshell@guestshell bootflash]$
[guestshell@guestshell bootflash]$ chvrf management curl cisco.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://www.cisco.com/">here</a>.</p>
</body></html>
[guestshell@guestshell bootflash]$
```

To obtain a list of VRFs on the system, use the **show vrf** command natively from NX-OS or through the **dohost** command:

Example:

```
[guestshell@guestshell bootflash]$ dohost 'sh vrf'
VRF-Name  VRF-ID  State  Reason
default   1        Up     --
management 2        Up     --
red       6        Up     --
```

Within the Guest Shell, the network namespaces associated with the VRFs are what is actually used. It can be more convenient to just see which network namespaces are present:

```
[guestshell@guestshell bootflash]$ ls /var/run/netns
default management red
```

```
[guestshell@guestshell bootflash]$
```

To resolve domain names from within the Guest Shell, the resolver needs to be configured. Edit the `/etc/resolv.conf` file in the Guest Shell to include a DNS nameserver and domain as appropriate for the network.

Example:

```
nameserver 10.1.1.1
domain cisco.com
```

The nameserver and domain information should match what is configured through the NX-OS configuration.

Example:

```
switch(config)# ip domain-name cisco.com
switch(config)# ip name-server 10.1.1.1
switch(config)# vrf context management
switch(config-vrf)# ip domain-name cisco.com
switch(config-vrf)# ip name-server 10.1.1.1
```

If the Cisco Nexus device is in a network that uses an HTTP proxy server, the `http_proxy` and `https_proxy` environment variables must be set up within the Guest Shell also.

Example:

```
export http_proxy=http://proxy.esl.cisco.com:8080
export https_proxy=http://proxy.esl.cisco.com:8080
```

These environment variables should be set in the `.bashrc` file or in an appropriate script to ensure that they are persistent.

## Access to Bootflash in Guest Shell

Network administrators can manage files with Linux commands and utilities in addition to using NX-OS CLI commands. By mounting the system bootflash at `/bootflash` in the Guest Shell environment, the network-admin can operate on these files with Linux commands.

Example:

```
find . -name "foo.txt"
rm "/bootflash/junk/foo.txt"
```




---

**Note** While the name of the user within the Guest Shell is the same as when on the host, the Guest Shell is in a separate user namespace, and the uid does not match that of the user on the host. The file permissions for group and others will control the type of access the Guest Shell user has on the file.

---

## Python in Guest Shell

Python can be used interactively or python scripts can be run in the Guest Shell.

Example:

```
guestshell:~$ python
Python 2.7.5 (default, Jun 24 2015, 00:41:19)
[GCC 4.8.3 20140911 (Red Hat 4.8.3-9)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
guestshell:~$
```

The pip python package manager is included in the Guest Shell to allow the network-admin to install new python packages.

Example:

```
[guestshell@guestshell ~]$ sudo su
[root@guestshell guestshell]# pip install Markdown
Collecting Markdown
Downloading Markdown-2.6.2-py2.py3-none-any.whl (157kB)
100% |#####| 159kB 1.8MB/s
Installing collected packages: Markdown
Successfully installed Markdown-2.6.2
[root@guestshell guestshell]# pip list | grep Markdown
Markdown (2.6.2)
[root@guestshell guestshell]#
```




---

**Note** You must enter the **sudo su** command before entering the **pip install** command.

---

## Python 3 in Guest Shell 2.x (Centos 7)

Guest Shell 2.X provides a Centos 7.1 environment, which does not have Python 3 installed by default. There are multiple methods of installing Python 3 on Centos 7.1, such as using third-party repositories or building from source. Another option is using the Red Hat Software Collections, which supports installing multiple versions of Python within the same system.

To install the Red Hat Software Collections (SCL) tool:

1. Install the scl-utils package.
2. Enable the Centos SCL repository and install one of its provided Python 3 RPMs.

```
[admin@guestshell ~]$ sudo su
[root@guestshell admin]# yum install -y scl-utils | tail
Running transaction test
Transaction test succeeded
Running transaction
  Installing : scl-utils-20130529-19.el7.x86_64                1/1
  Verifying  : scl-utils-20130529-19.el7.x86_64                1/1

Installed:
  scl-utils.x86_64 0:20130529-19.el7

Complete!

[root@guestshell admin]# yum install -y centos-release-scl | tail
  Verifying : centos-release-scl-2-3.el7.centos.noarch          1/2
  Verifying : centos-release-scl-rh-2-3.el7.centos.noarch       2/2
```

```

Installed:
  centos-release-scl.noarch 0:2-3.el7.centos

Dependency Installed:
  centos-release-scl-rh.noarch 0:2-3.el7.centos

Complete!

[root@guestshell admin]# yum install -y rh-python36 | tail
warning: /var/cache/yum/x86_64/7/centos-scl-rh/packages/rh-python36-2.0-1.el7.x86_64.rpm:
  Header V4 RSA/SHA1 Signature, key ID f2ee9d55: NOKEY
http://centos.sonn.com/7.7.1908/os/x86_64/Packages/groff-base-1.22.2-8.el7.x86_64.rpm:
[Errno 12] Timeout on
http://centos.sonn.com/7.7.1908/os/x86_64/Packages/groff-base-1.22.2-8.el7.x86_64.rpm: (28,
  'Operation too slow. Less than 1000 bytes/sec transferred the last 30 seconds')
Trying other mirror.
Importing GPG key 0xF2EE9D55:
  Userid      : "CentOS SoftwareCollections SIG
(https://wiki.centos.org/SpecialInterestGroup/SCLO) <security@centos.org>"
  Fingerprint: c4db d535 blfb ba14 f8ba 64a8 4eb8 4e71 f2ee 9d55
  Package     : centos-release-scl-rh-2-3.el7.centos.noarch (@extras)
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-SIG-SCLO
  rh-python36-python-libs.x86_64 0:3.6.9-2.el7
  rh-python36-python-pip.noarch 0:9.0.1-2.el7
  rh-python36-python-setuptools.noarch 0:36.5.0-1.el7
  rh-python36-python-virtualenv.noarch 0:15.1.0-2.el7
  rh-python36-runtime.x86_64 0:2.0-1.el7
  scl-utils-build.x86_64 0:20130529-19.el7
  xml-common.noarch 0:0.6.3-39.el7
  zip.x86_64 0:3.0-11.el7

```

Complete!

Using SCL, it is possible to create an interactive bash session with Python 3's environment variables automatically setup.




---

**Note** The root user is not needed to use the SCL Python installation.

---

```

[admin@guestshell ~]$ scl enable rh-python36 bash
[admin@guestshell ~]$ python3
Python 3.6.9 (default, Nov 11 2019, 11:24:16)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-39)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>

```

The Python SCL installation also provides the pip utility.

```

[admin@guestshell ~]$ pip3 install requests --user
Collecting requests
  Downloading
https://files.pythonhosted.org/packages/51/1d/23c926cc841ea677cd02a00aba99ae0f828e89d72b2190f27c11d4b7fb/requests-2.22.0-py2.py3-none-any.whl
(57kB)
  100% |#####| 61kB 211kB/s
Collecting idna<2.9,>=2.5 (from requests)
  Downloading
https://files.pythonhosted.org/packages/14/2c/cd551c81d8e15200b1cf41cd03869a46fe7226e7450af7a6545b0c474c9/idna-2.8-py2.py3-none-any.whl
(58kB)
  100% |#####| 61kB 279kB/s
Collecting chardet<3.1.0,>=3.0.2 (from requests)
  Downloading
https://files.pythonhosted.org/packages/cc/a9/01ffbf562e4274b6487b4bb1dbbc7ca55c7510b22e4c51f1409844368/chardet-3.0.4-py2.py3-none-any.whl

```

```

(133kB)
100% |#####| 143kB 441kB/s
Collecting certifi>=2017.4.17 (from requests)
  Downloading
https://files.pythonhosted.org/packages/b9/63/d50cac98e05b006c55a39c3cf1db9db7b5a24b7890bc9cfc5b9e99/certifi-2019.11.28-py2.py3-none-any.whl
(156kB)
100% |#####| 163kB 447kB/s
Collecting urllib3!=1.25.0,!<1.25.1,<1.26,>=1.21.1 (from requests)
  Downloading
https://files.pythonhosted.org/packages/e8/74/6e4f91745020f967d0932b2b289b1009095734692ab88a4fe91b77f/urllib3-1.25.8-py2.py3-none-any.whl
(125kB)
100% |#####| 133kB 656kB/s
Installing collected packages: idna, chardet, certifi, urllib3, requests
Successfully installed certifi-2019.11.28 chardet-3.0.4 idna-2.8 requests-2.22.0
urllib3-1.25.8
You are using pip version 9.0.1, however version 20.0.2 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
[admin@guestshell ~]$ python3
Python 3.6.9 (default, Nov 11 2019, 11:24:16)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-39)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import requests
>>> requests.get("https://cisco.com")
<Response [200]>

```

The default Python 2 installation can be used alongside the SCL Python installation.

```

[admin@guestshell ~]$ which python3
/opt/rh/rh-python36/root/usr/bin/python3
[admin@guestshell ~]$ which python2
/bin/python2
[admin@guestshell ~]$ python2
Python 2.7.5 (default, Aug 7 2019, 00:51:29)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-39)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print 'Hello world!'
Hello world!

```

Software Collections makes it possible to install multiple versions of the same RPM on a system. In this case, it is possible to install Python 3.5 in addition to Python 3.6.

```

[admin@guestshell ~]$ sudo yum install -y rh-python35 | tail
Dependency Installed:
rh-python35-python.x86_64 0:3.5.1-13.e17
rh-python35-python-devel.x86_64 0:3.5.1-13.e17
rh-python35-python-libs.x86_64 0:3.5.1-13.e17
rh-python35-python-pip.noarch 0:7.1.0-2.e17
rh-python35-python-setuptools.noarch 0:18.0.1-2.e17
rh-python35-python-virtualenv.noarch 0:13.1.2-2.e17
rh-python35-runtime.x86_64 0:2.0-2.e17

```

Complete!

```

[admin@guestshell ~]$ scl enable rh-python35 python3
Python 3.5.1 (default, May 29 2019, 15:41:33)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-36)] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>

```



**Note** Creating new interactive bash sessions when multiple Python versions are installed in SCL can cause an issue where the libpython shared object file cannot be loaded. There is a workaround where you can use the **source scl\_source enable python-installation** command to properly set up the environment in the current bash session.

The default Guest Shell storage capacity is not sufficient to install Python 3. Use the **guestshell resize rootfs size-in-MB** command to increase the size of the file system. Typically, setting the rootfs size to 550 MB is sufficient.

## Installing RPMs in the Guest Shell

The `/etc/yum.repos.d/CentOS-Base.repo` file is set up to use the CentOS mirror list by default. Follow instructions in that file if changes are needed.

Yum can be pointed to one or more repositories at any time by modifying the `yumrepo_x86_64.repo` file or by adding a new `.repo` file in the `repos.d` directory.

For applications to be installed inside Guest Shell, go to the CentOS 7 repo at [http://mirror.centos.org/centos/7/os/x86\\_64/Packages/](http://mirror.centos.org/centos/7/os/x86_64/Packages/).

Yum resolves the dependencies and installs all the required packages.

```
[guestshell@guestshell ~]$ sudo chvrf management yum -y install glibc.i686
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: bay.uchicago.edu
* extras: pubmirrors.dal.coreospace.com
* updates: mirrors.cmich.edu
Resolving Dependencies
"-->" Running transaction check
"-->" Package glibc.i686 0:2.17-78.el7 will be installed
"-->" Processing Dependency: libfreebl3.so(NSSRAWHASH_3.12.3) for package:
glibc-2.17-78.el7.i686
"-->" Processing Dependency: libfreebl3.so for package: glibc-2.17-78.el7.i686
"-->" Running transaction check
"-->" Package nss-softokn-freebl.i686 0:3.16.2.3-9.el7 will be installed
"-->" Finished Dependency Resolution
```

Dependencies Resolved

---



---

Package Arch Version Repository Size

---



---

```
Installing:
glibc i686 2.17-78.el7 base 4.2 M
Installing for dependencies:
nss-softokn-freebl i686 3.16.2.3-9.el7 base 187 k
```

Transaction Summary

---



---

Install 1 Package (+1 Dependent package)

```
Total download size: 4.4 M
Installed size: 15 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
(1/2): nss-softokn-freebl-3.16.2.3-9.el7.i686.rpm | 187 kB 00:00:25
(2/2): glibc-2.17-78.el7.i686.rpm | 4.2 MB 00:00:30
```

---



---

```

Total 145 kB/s | 4.4 MB 00:00:30
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : nss-softokn-freebl-3.16.2.3-9.el7.i686 1/2
Installing : glibc-2.17-78.el7.i686 2/2
error: lua script failed: [string "%triggerin(glibc-common-2.17-78.el7.x86_64)"]:1: attempt
  to compare number with nil
Non-fatal "<"unknown">" scriptlet failure in rpm package glibc-2.17-78.el7.i686
Verifying : glibc-2.17-78.el7.i686 1/2
Verifying : nss-softokn-freebl-3.16.2.3-9.el7.i686 2/2

Installed:
glibc.i686 0:2.17-78.el7

Dependency Installed:
nss-softokn-freebl.i686 0:3.16.2.3-9.el7

Complete!

```




---

**Note** When more space is needed in the Guest Shell root file system for installing or running packages, the **guestshell resize roofs *size-in-MB*** command is used to increase the size of the file system.

---




---

**Note** Some open source software packages from the repository might not install or run as expected in the Guest Shell as a result of restrictions that have been put into place to protect the integrity of the host system.

---

## Security Posture for Guest Shell

Use of the Guest Shell in Cisco Nexus series devices is just one of the many ways the network admin can manage or extend the functionality of the system. The Guest Shell is intended to provide an execution environment that is decoupled from the native host context. This separation allows the introduction of software into the system that may not be compatible with the native execution environment. It also allows the software to run in an environment that does not interfere with the behavior, performance, or scale of the system.

### Kernel Vulnerability Patches

Cisco responds to pertinent Common Vulnerabilities and Exposures (CVEs) with platform updates that address known vulnerabilities.

### ASLR and X-Space Support

Cisco Nexus NX-OS supports the use of Address Space Layout Randomization (ASLR) and Executable Space Protection (X-Space) for runtime defense. The software in Cisco-signed packages make use of this capability. If other software is installed on the system, it is recommended that it be built using a host OS and development toolchain that supports these technologies. Doing so reduces the potential attack surface that the software presents to potential intruders.

## Namespace Isolation

The Guest Shell environment runs within a Linux container that makes use of various namespaces to decouple the Guest Shell execution space from that of the host. Starting in the NX-OS 9.2(1) release, the Guest Shell is run in a separate user namespace, which helps protect the integrity of the host system, as processes running as root within the Guest Shell are not root of the host. These processes appear to be running as uid 0 within the Guest Shell due to uid mapping, but the kernel knows the real uid of these processes and evaluates the POSIX capabilities within the appropriate user namespace.

When a user enters the Guest Shell from the host, a user of the same name is created within the Guest Shell. While the names match, the uid of the user within the Guest Shell is not the same as the uid on the host. To still allow users within the Guest Shell to access files on shared media (for example, `/bootflash` or `/volatile`), the common NX-OS gids used on the host (for example, `network-admin` or `network-operator`) are mapped into the Guest Shell such that the values are the same and the Guest Shell instance of the user is associated with the appropriate groups based on group membership on the host.

As an example, consider user `bob`. On the host, `bob` has the following uid and gid membership:

```
bash-4.3$ id
uid=2004(bob) gid=503(network-admin) groups=503(network-admin),504(network-operator)
```

When user `bob` is in the Guest Shell, the group membership from the host is set up in the Guest Shell:

```
[bob@guestshell ~]$ id
uid=1002(bob) gid=503(network-admin)
groups=503(network-admin),504(network-operator),10(wheel)
```

Files created by user `bob` in the host Bash shell and the Guest Shell have different owner ids. The example output below shows that the file created from within the Guest Shell has owner id 12002, instead of 1002 as shown in the example output above. This is due to the command being issued from the host Bash shell and the id space for the Guest Shell starting at id 11000. The group id of the file is `network-admin`, which is 503 in both environments.

```
bash-4.3$ ls -ln /bootflash/bob_*
-rw-rw-r-- 1 12002 503 4 Jun 22 15:47 /bootflash/bob_guestshell
-rw-rw-r-- 1 2004 503 4 Jun 22 15:47 /bootflash/bob_host
```

```
bash-4.3$ ls -l /bootflash/bob_*
-rw-rw-r-- 1 12002 network-admin 4 Jun 22 15:47 /bootflash/bob_guestshell
-rw-rw-r-- 1 bob network-admin 4 Jun 22 15:47 /bootflash/bob_host
```

The user is allowed to access the file due to the file permission settings for the `network-admin` group, and the fact that `bob` is a member of `network-admin` in both the host and Guest Shell.

Inside the Guest Shell environment, the example output below shows that the owner id for the file created by `bob` from the host is 65534. This indicates the actual id is in a range that is outside range of ids mapped into the user namespace. Any unmapped id will be shown as this value.

```
[bob@guestshell ~]$ ls -ln /bootflash/bob_*
-rw-rw-r-- 1 1002 503 4 Jun 22 15:47 /bootflash/bob_guestshell
-rw-rw-r-- 1 65534 503 4 Jun 22 15:47 /bootflash/bob_host
```

```
[bob@guestshell ~]$ ls -l /bootflash/bob_*
-rw-rw-r-- 1 bob network-admin 4 Jun 22 15:47 /bootflash/bob_guestshell
-rw-rw-r-- 1 65534 network-admin 4 Jun 22 15:47 /bootflash/bob_host
```

## Root-User Restrictions

As a best practice for developing secure code, it is recommend running applications with the least privilege needed to accomplish the assigned task. To help prevent unintended accesses, software added into the Guest Shell should follow this best practice.

All processes within the Guest Shell are subject to restrictions imposed by reduced Linux capabilities. If your application must perform operations that require root privileges, restrict the use of the root account to the smallest set of operations that absolutely requires root access, and impose other controls such as a hard limit on the amount of time that the application can run in that mode.

The set of Linux capabilities that are dropped for root within the Guest Shell follow:

- `cap_audit_control`
- `cap_audit_write`
- `cap_mac_admin`
- `cap_mac_override`
- `cap_mknod`
- `cap_net_broadcast`
- `cap_sys_boot`
- `cap_syslog`
- `cap_sys_module`
- `cap_sys_nice`
- `cap_sys_pacct`
- `cap_sys_ptrace`
- `cap_sys_rawio`
- `cap_sys_resource`
- `cap_sys_time`
- `cap_wake_alarm`

While the `net_admin` capability is not dropped, user namespace and the host ownership of the network namespaces prevents the Guest Shell user from modifying the interface state. As root within the Guest Shell, `bind` mounts may be used as well as `tmpfs` and `ramfs` mounts. Other mounts are prevented.

## Resource Management

A Denial-of-Service (DoS) attack attempts to make a machine or network resource unavailable to its intended users. Misbehaving or malicious application code can cause DoS as the result of over-consumption of connection bandwidth, disk space, memory, and other resources. The host provides resource-management features that ensure fair allocation of resources between Guest Shell and services on the host.

# Guest File System Access Restrictions

To preserve the integrity of the files within the Guest Shell, the file systems of the Guest Shell are not accessible from the NX-OS CLI.

`bootflash:` and `volatile:` of the host are mounted as `/bootflash` and `/volatile` within the Guest Shell. A network-admin can access files on this media using the NX-OS `exec` commands from the host or using Linux commands from within the Guest Shell.

## Managing the Guest Shell

The following are commands to manage the Guest Shell:

**Table 2: Guest Shell CLI Commands**

Commands	Description
<code>guestshell enable {package [guest shell OVA file   rootfs-file-URI]}</code>	<ul style="list-style-type: none"> <li>When <i>guest shell OVA file</i> is specified: Installs and activates the Guest Shell using the OVA that is embedded in the system image.  Installs and activates the Guest Shell using the specified software package (OVA file) or the embedded package from the system image (when no package is specified). Initially, Guest Shell packages are only available by being embedded in the system image.  When the Guest Shell is already installed, this command enables the installed Guest Shell. Typically this is used after a <b>guestshell disable</b> command.</li> <li>When <i>rootfs-file-URI</i> is specified: Imports a Guest Shell <b>rootfs</b> when the Guest Shell is in a destroyed state. This command brings up the Guest Shell with the specified package.</li> </ul>
<code>guestshell export rootfs package destination-file-URI</code>	Exports a Guest Shell <b>rootfs</b> file to a local URI (bootflash, USB1, etc.).
<code>guestshell disable</code>	Shuts down and disables the Guest Shell.

Commands	Description
<p><b>guestshell upgrade</b> {<b>package</b> [<i>guest shell OVA file</i>   <i>rootfs-file-URI</i>]}</p>	<ul style="list-style-type: none"> <li>• When <i>guest shell OVA file</i> is specified: <p>Deactivates and upgrades the Guest Shell using the specified software package (OVA file) or the embedded package from the system image (if no package is specified). Initially Guest Shell packages are only available by being embedded in the system image.</p> <p>The current rootfs for the Guest Shell is replaced with the rootfs in the software package. The Guest Shell does not make use of secondary filesystems that persist across an upgrade. Without persistent secondary filesystems, a <b>guestshell destroy</b> command followed by a <b>guestshell enable</b> command could also be used to replace the rootfs. When an upgrade is successful, the Guest Shell is activated.</p> <p>You are prompted for a confirmation prior to carrying out the upgrade command.</p> </li> <li>• When <i>rootfs-file-URI</i> is specified: <p>Imports a Guest Shell <b>rootfs</b> file when the Guest Shell is already installed. This command removes the existing Guest Shell and installs the specified package.</p> </li> </ul>
<p><b>guestshell reboot</b></p>	<p>Deactivates the Guest Shell and then reactivates it. You are prompted for a confirmation prior to carrying out the reboot command.</p> <p><b>Note</b> This is the equivalent of a <b>guestshell disable</b> command followed by a <b>guestshell enable</b> command in exec mode.</p> <p>This is useful when processes inside the Guest Shell have been stopped and need to be restarted. The <b>run guestshell</b> command relies on <code>sshd</code> running in the Guest Shell.</p> <p>If the command does not work, the <code>sshd</code> process may have been inadvertently stopped. Performing a reboot of the Guest Shell from the NX-OS CLI allows it to restart and restore the command.</p>

Commands	Description
<b>guestshell destroy</b>	<p>Deactivates and uninstalls the Guest Shell. All resources associated with the Guest Shell are returned to the system. The <b>show virtual-service global</b> command indicates when these resources become available.</p> <p>Issuing this command results in a prompt for a confirmation prior to carrying out the destroy command.</p>
<b>guestshell</b> <b>run guestshell</b>	Connects to the Guest Shell that is already running with a shell prompt. No username/password is required.
<b>guestshell run</b> <i>command</i> <b>run guestshell</b> <i>command</i>	<p>Executes a Linux/UNIX command within the context of the Guest Shell environment.</p> <p>After execution of the command you are returned to the switch prompt.</p>
<b>guestshell resize</b> [cpu   memory   rootfs]	<p>Changes the allotted resources available for the Guest Shell. The changes take effect the next time the Guest Shell is enabled or rebooted.</p> <p><b>Note</b>     Resize values are cleared when the <b>guestshell destroy</b> command is used.</p>
<b>guestshell sync</b>	On systems that have active and standby supervisors, this command synchronizes the Guest Shell contents from the active supervisor to the standby supervisor. The network-admin issues this command when the Guest Shell rootfs has been set up to a point that they would want the same rootfs used on the standby supervisor when it becomes the active supervisor. If this command is not used, the Guest Shell is freshly installed when the standby supervisor transitions to an active role using the Guest Shell package available on that supervisor.
<b>virtual-service reset force</b>	<p>In the event that the guestshell or virtual-services cannot be managed, even after a system reload, the reset command is used to force the removal of the Guest Shell and all virtual-services. The system needs to be reloaded for the cleanup to happen. No Guest Shell or additional virtual-services can be installed or enabled after issuing this command until after the system has been reloaded.</p> <p>You are prompted for a confirmation prior to initiating the reset.</p>




---

**Note** Administrative privileges are necessary to enable/disable and to gain access to the Guest Shell environment.

---




---

**Note** The Guest Shell is implemented as a Linux container (LXC) on the host system. On NX-OS devices, LXC's are installed and managed with the virtual-service commands. The Guest Shell appears in the virtual-service commands as a virtual service named `guestshell+`.

---




---

**Note** Virtual-service commands that do not pertain to the Guest Shell are being deprecated. These commands have been hidden in the NX-OS 9.2(1) release and will be removed in future releases.

The following exec keywords are being deprecated:

```
# virtual-service ?
connect Request a virtual service shell
install Add a virtual service to install database
uninstall Remove a virtual service from the install database
upgrade Upgrade a virtual service package to a different version
```

```
# show virtual-service ?
detail Detailed information config)
```

The following config keywords are being deprecated:

```
(config) virtual-service ?
WORD Virtual service name (Max Size 20)
```

```
(config-virt-serv)# ?
activate Activate configured virtual service
description Virtual service description
```

---

## Disabling the Guest Shell

The `guestshell disable` command shuts down and disables the Guest Shell.

When the Guest Shell is disabled and the system is reloaded, the Guest Shell remains disabled.

Example:

```
switch# show virtual-service list
Virtual Service List:
Name                               Status           Package Name
-----
guestshell+                        Activated       guestshell.ova
switch# guestshell disable
You will not be able to access your guest shell if it is disabled. Are you sure you want
to disable the guest shell? (y/n) [n] y

2014 Jul 30 19:47:23 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Deactivating virtual
service 'guestshell+'
```

```

2014 Jul 30 18:47:29 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully deactivated
virtual service 'guestshell+'
switch# show virtual-service list
Virtual Service List:
Name                Status                Package Name
guestshell+         Deactivated           guestshell.ova

```




---

**Note** The Guest Shell is reactivated with the **guestshell enable** command.

---

## Destroying the Guest Shell

The **guestshell destroy** command uninstalls the Guest Shell and its artifacts. The command does not remove the Guest Shell OVA.

When the Guest Shell is destroyed and the system is reloaded, the Guest Shell remains destroyed.

```

switch# show virtual-service list
Virtual Service List:
Name                Status                Package Name
-----
guestshell+         Deactivated           guestshell.ova

```

```
switch# guestshell destroy
```

```

You are about to destroy the guest shell and all of its contents. Be sure to save your work.
Are you sure you want to continue? (y/n) [n] y
2014 Jul 30 18:49:10 switch %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Destroying virtual service
'guestshell+'
2014 Jul 30 18:49:10 switch %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Successfully destroyed
virtual service 'guestshell +'

```

```

switch# show virtual-service list
Virtual Service List:

```




---

**Note** The Guest Shell can be re-enabled with the **guestshell enable** command.

---




---

**Note** If you do not want to use the Guest Shell, you can remove it with the **guestshell destroy** command. Once the Guest Shell has been removed, it remains removed for subsequent reloads. This means that when the Guest Shell container has been removed and the switch is reloaded, the Guest Shell container is not automatically started.

---

## Enabling the Guest Shell

The **guestshell enable** command installs the Guest Shell from a Guest Shell software package. By default, the package embedded in the system image is used for the installation. The command is also used to reactivate the Guest Shell if it has been disabled.

When the Guest Shell is enabled and the system is reloaded, the Guest Shell remains enabled.

Example:

```
switch# show virtual-service list
Virtual Service List:
switch# guestshell enable
2014 Jul 30 18:50:27 switch %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Installing virtual service
'guestshell+'
2014 Jul 30 18:50:42 switch %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Install success virtual
service 'guestshell+'; Activating

2014 Jul 30 18:50:42 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Activating virtual service
'guestshell+'
2014 Jul 30 18:51:16 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully activated
virtual service 'guestshell+'

switch# show virtual-service list
Virtual Service List:
Name                Status              Package Name
guestshell+         Activated           guestshell.ova
```

### Enabling the Guest Shell in Base Boot Mode

Beginning in the NX-OS 9.2(1) release, you can choose to boot your system in *base boot mode*. When you boot your system in base boot mode, the Guest Shell is not started by default. In order to use the Guest Shell in this mode, you must activate the RPMs containing the virtualization infrastructure as well as the Guest Shell image. Once you have done this, the Guest Shell and virtual-service commands will be available.

If the RPM activation commands are run in this order:

1. `install activate guestshell`
2. `install activate virtualization`

The Guest Shell container will be activated automatically as it would have been if the system had been booted in full mode.

If the RPM activation commands are run in the reverse order:

1. `install activate virtualization`
2. `install activate guestshell`

Then the Guest Shell will not be enabled until you run the **guestshell enable** command.

## Replicating the Guest Shell

Beginning with Cisco NX-OS release 7.0(3)I7(1), a Guest Shell **rootfs** that is customized on one switch can be deployed onto multiple switches.

The approach is to customize and then export the Guest Shell **rootfs** and store it on a file server. A POAP script can download (import) the Guest Shell **rootfs** to other switches and install the specific Guest Shell across many devices simultaneously.

## Exporting Guest Shell rootfs

Use the **guestshell export rootfs package** *destination-file-URI* command to export a Guest Shell **rootfs**.

The *destination-file-URI* parameter is the name of the file that the Guest Shell **rootfs** is copied to. This file allows for local URI options (bootflash, USB1, etc.).

The **guestshell export rootfs package** command:

- Disables the Guest Shell (if already enabled).
- Creates a Guest Shell import YAML file and inserts it into the /cisco directory of the **rootfs** ext4 file.
- Copies the **rootfs** ext4 file to the target URI location.
- Re-enables the Guest Shell if it had been previously enabled.

## Importing Guest Shell rootfs

When importing a Guest Shell **rootfs**, there are two situations to consider:

- Use the **guestshell enable package** *rootfs-file-URI* command to import a Guest Shell **rootfs** when the Guest Shell is in a destroyed state. This command brings up the Guest Shell with the specified package.
- Use the **guestshell upgrade package** *rootfs-file-URI* command to import a Guest Shell **rootfs** when the Guest Shell is already installed. This command removes the existing Guest Shell and installs the specified package.

The *rootfs-file-URI* parameter is the **rootfs** file stored on local storage (bootflash, USB, etc.).

When this command is executed with a file that is on bootflash, the file is moved to a storage pool on bootflash.

As a best practice, you should copy the file to the bootflash and validate the md5sum before using the **guestshell upgrade package** *rootfs-file-URI* command.




---

**Note** The **guestshell upgrade package** *rootfs-file-URI* command can be executed from within the Guest Shell.

---




---

**Note** The rootfs file is not a Cisco signed package, you must configure to allow unsigned packages before enabling as shown in the example:

```
(config-virt-serv-global)# signing level unsigned
Note: Support for unsigned packages has been user-enabled. Unsigned packages are not endorsed
by Cisco. User assumes all responsibility.
```

---



- 
- Note** To restore the embedded version of the rootfs:
- Use the **guestshell upgrade** command (without additional parameters) when the Guest Shell has already been installed.
  - Use the **guestshell enable** command (without additional parameters) when the Guest Shell had been destroyed.
- 



- 
- Note** When running this command from within a Guest Shell, or outside a switch using NX-API, you must set **terminal dont-ask** to skip any prompts.
- 

The **guestshell enable package *rootfs-file-URI*** command:

- Performs basic validation of the **rootfs** file.
- Moves the **rootfs** into the storage pool.
- Mounts the **rootfs** to extract the YAML file from the /cisco directory.
- Parses the YAML file to obtain VM definition (including resource requirements).
- Activates the Guest Shell.

Example workflow for **guestshell enable** :

```
switch# copy scp://user@10.1.1.1/my_storage/gs_rootfs.ext4 bootflash: vrf management
switch# guestshell resize cpu 8
Note: System CPU share will be resized on Guest shell enable
switch# guestshell enable package bootflash:gs_rootfs.ext4
Validating the provided rootfs
switch# 2017 Jul 31 14:58:01 switch %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Installing virtual
service 'guestshell+'
2017 Jul 31 14:58:09 switch %$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Install success virtual
service 'guestshell+'; Activating
2017 Jul 31 14:58:09 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Activating virtual service
'guestshell+'
2017 Jul 31 14:58:33 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully activated
virtual service 'guestshell+'
```



- 
- Note** Workflow for **guestshell upgrade** is preceded by the existing Guest Shell being destroyed.
- 



- 
- Note** Resize values are cleared when the **guestshell upgrade** command is used.
- 

## Importing YAML File

A YAML file that defines some user modifiable characteristics of the Guest Shell is automatically created as a part of the export operation. It is embedded into the Guest Shell **rootfs** in the /cisco directory. It is not a

complete descriptor for the Guest Shell container. It only contains some of the parameters that are user modifiable.

Example of a Guest Shell import YAML file:

```
---
import-schema-version: "1.0"
info:
  name: "GuestShell"
  version: "2.2(0.3)"
  description: "Exported GuestShell: 20170216T175137Z"
app:
  apptype: "lxc"
  cpuarch: "x86_64"
  resources:
    cpu: 3
    memory: 307200
    disk:
      - target-dir: "/"
        capacity: 250
...
```

The YAML file is generated when the **guestshell export rootfs package** command is executed. The file captures the values of the currently running Guest Shell.

The info section contains non-operational data that is used to help identify the Guest Shell. Some of the information will be displayed in the output of the **show guestshell detail** command.

The description value is an encoding of the UTC time when the YAML file was created. The time string format is the same as DTSTAMP in RFC5545 (iCal).

The resources section describes the resources required for hosting the Guest Shell. The value "/" for the target-dir in the example identifies the disk as the **rootfs**.




---

**Note** If resized values were specified while the Guest Shell was destroyed, those values take precedence over the values in the import YAML file when the **guestshell enable package** command is used.

---

The cpuarch value indicates the CPU architecture that is expected for the container to run.

You can modify the YAML file (such as the description or increase the resource parameters, if appropriate) after the export operation is complete .

Cisco provides a python script that you can run to validate a modified YAML file with a JSON schema. It is not meant to be a complete test (for example, device-specific resource limits are not checked), but it is able to flag common errors. The python script with examples is located at [https://github.com/datacenter/opennxos/tree/master/guestshell\\_import\\_export](https://github.com/datacenter/opennxos/tree/master/guestshell_import_export). The following JSON file describes the schema for version 1.0 of the Guest Shell import YAML .

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "Guest Shell import schema",
  "description": "Schema for Guest Shell import descriptor file - ver 1.0",
  "copyright": "2017 by Cisco systems, Inc. All rights reserved.",
  "id": "",
  "type": "object",
  "additionalProperties": false,
  "properties": {
    "import-schema-version": {
```

```

    "id": "/import-schema-version",
    "type": "string",
    "minLength": 1,
    "maxLength": 20,
    "enum": [
      "1.0"
    ]
  },
  "info": {
    "id": "/info",
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "name": {
        "id": "/info/name",
        "type": "string",
        "minLength": 1,
        "maxLength": 29
      },
      "description": {
        "id": "/info/description",
        "type": "string",
        "minLength": 1,
        "maxLength": 199
      },
      "version": {
        "id": "/info/version",
        "type": "string",
        "minLength": 1,
        "maxLength": 63
      },
      "author-name": {
        "id": "/info/author-name",
        "type": "string",
        "minLength": 1,
        "maxLength": 199
      },
      "author-link": {
        "id": "/info/author-link",
        "type": "string",
        "minLength": 1,
        "maxLength": 199
      }
    }
  },
  "app": {
    "id": "/app",
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "apptype": {
        "id": "/app/apptype",
        "type": "string",
        "minLength": 1,
        "maxLength": 63,
        "enum": [
          "lxc"
        ]
      },
      "cpuarch": {
        "id": "/app/cpuarch",
        "type": "string",
        "minLength": 1,
        "maxLength": 63,

```

```

    "enum": [
      "x86_64"
    ]
  },
  "resources": {
    "id": "/app/resources",
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "cpu": {
        "id": "/app/resources/cpu",
        "type": "integer",
        "multipleOf": 1,
        "maximum": 100,
        "minimum": 1
      },
      "memory": {
        "id": "/app/resources/memory",
        "type": "integer",
        "multipleOf": 1024,
        "minimum": 1024
      },
      "disk": {
        "id": "/app/resources/disk",
        "type": "array",
        "minItems": 1,
        "maxItems": 1,
        "uniqueItems": true,
        "items": {
          "id": "/app/resources/disk/0",
          "type": "object",
          "additionalProperties": false,
          "properties": {
            "target-dir": {
              "id": "/app/resources/disk/0/target-dir",
              "type": "string",
              "minLength": 1,
              "maxLength": 1,
              "enum": [
                "/"
              ]
            },
            "file": {
              "id": "/app/resources/disk/0/file",
              "type": "string",
              "minLength": 1,
              "maxLength": 63
            },
            "capacity": {
              "id": "/app/resources/disk/0/capacity",
              "type": "integer",
              "multipleOf": 1,
              "minimum": 1
            }
          }
        }
      }
    }
  },
  "required": [
    "memory",
    "disk"
  ]
}

```

```

        "required": [
            "apptype",
            "cpuarch",
            "resources"
        ]
    },
    "required": [
        "app"
    ]
}

```

## show guestshell Command

The output of the **show guestshell detail** command includes information that indicates whether the Guest Shell was imported or was installed from an OVA.

Example of the **show guestshell detail** command after importing **rootfs**.

```

switch# show guestshell detail
Virtual service guestshell+ detail
State                : Activated
Package information
  Name                : rootfs_puppet
  Path                : usb2:/rootfs_puppet
Application
  Name                : GuestShell
  Installed version   : 2.3(0.0)
  Description         : Exported GuestShell: 20170613T173648Z
Signing
  Key type            : Unsigned
  Method              : Unknown
Licensing
  Name                : None
  Version             : None

```

## Verifying Virtual Service and Guest Shell Information

You can verify virtual service and Guest Shell information with the following commands:

Command	Description
<pre> <b>show virtual-service global</b>  switch# <b>show virtual-service global</b>  Virtual Service Global State and Virtualization Limits:  Infrastructure version : 1.9 Total virtual services installed : 1 Total virtual services activated : 1  Machine types supported : LXC Machine types disabled : KVM  Maximum VCPUs per virtual service : 1  Resource virtualization limits: Name Quota Committed Available ----- system CPU (%) 20 1 19 memory (MB) 3840 256 3584 bootflash (MB) 8192 200 7992 switch# </pre>	<p>Displays the global state and limits for virtual services.</p>
<pre> <b>show virtual-service list</b>  switch# <b>show virtual-service list *</b>  Virtual Service List:  Name                Status           Package Name ----- guestshell+         Activated        guestshell.ova </pre>	<p>Displays a summary of the virtual services, the status of the virtual services, and installed software packages.</p>

Command	Description
<pre> <b>show guestshell detail</b>  switch# <b>show guestshell detail</b> Virtual service guestshell+ detail   State                : Activated   Package information     Name                : guestshell.ova     Path                : /isan/bin/guestshell.ova   Application     Name                : GuestShell     Installed version   : 2.2(0.2)     Description         : Cisco Systems Guest Shell   Signing     Key type            : Cisco key     Method              : SHA-1   Licensing     Name                : None     Version             : None   Resource reservation     Disk                : 250 MB     Memory              : 256 MB     CPU                 : 1% system CPU    Attached devices   Type                Name                Alias   -----   Disk                _rootfs   Disk                /cisco/core   Serial/shell   Serial/aux   Serial/Syslog       serial2   Serial/Trace       serial3 </pre>	<p>Displays details about the guestshell package (such as version, signing resources, and devices).</p>

## Persistently Starting Your Application From the Guest Shell

Your application should have a `systemd / systemctl` service file that gets installed in `/usr/lib/systemd/system/application_name.service`. This service file should have the following general format:

```

[Unit]
Description=Put a short description of your application here

[Service]
ExecStart=Put the command to start your application here
Restart=always
RestartSec=10s

[Install]
WantedBy=multi-user.target

```



**Note** To run `systemd` as a specific user, add `User=<username>` to the `[Service]` section of your service.

# Procedure for Persistently Starting Your Application from the Guest Shell

- 
- Step 1** Install your application service file that you created above into `/usr/lib/systemd/system/application_name.service`
  - Step 2** Start your application with `systemctl start application_name`
  - Step 3** Verify that your application is running with `systemctl status -l application_name`
  - Step 4** Enable your application to be restarted on reload with `systemctl enable application_name`
  - Step 5** Verify that your application is running with `systemctl status -l application_name`
- 

## An Example Application in the Guest Shell

The following example demonstrates an application in the Guest Shell:

```

root@guestshell guestshell]# cat /etc/init.d/hello.sh
#!/bin/bash

OUTPUTFILE=/tmp/hello

rm -f $OUTPUTFILE
while true
do
    echo $(date) >> $OUTPUTFILE
    echo 'Hello World' >> $OUTPUTFILE
    sleep 10
done
[root@guestshell guestshell]#
[root@guestshell guestshell]#
[root@guestshell system]# cat /usr/lib/systemd/system/hello.service
[Unit]
Description=Trivial "hello world" example daemon

[Service]
ExecStart=/etc/init.d/hello.sh &
Restart=always
RestartSec=10s

[Install]
WantedBy=multi-user.target
[root@guestshell system]#
[root@guestshell system]# systemctl start hello
[root@guestshell system]# systemctl enable hello
[root@guestshell system]# systemctl status -l hello
hello.service - Trivial "hello world" example daemon
   Loaded: loaded (/usr/lib/systemd/system/hello.service; enabled)
   Active: active (running) since Sun 2015-09-27 18:31:51 UTC; 10s ago
   Main PID: 355 (hello.sh)
   CGroup: /system.slice/hello.service
           ##355 /bin/bash /etc/init.d/hello.sh &
           ##367 sleep 10

```

```
Sep 27 18:31:51 guestshell hello.sh[355]: Executing: /etc/init.d/hello.sh &
[root@guestshell system]#
[root@guestshell guestshell]# exit
exit
[guestshell@guestshell ~]$ exit
logout
switch# reload
This command will reboot the system. (y/n)? [n] y
```

#### After reload

```
[root@guestshell guestshell]# ps -ef | grep hello
root      20      1  0 18:37 ?        00:00:00 /bin/bash /etc/init.d/hello.sh &
root      123     108  0 18:38 pts/4    00:00:00 grep --color=auto hello
[root@guestshell guestshell]#
[root@guestshell guestshell]# cat /tmp/hello
Sun Sep 27 18:38:03 UTC 2015
Hello World
Sun Sep 27 18:38:13 UTC 2015
Hello World
Sun Sep 27 18:38:23 UTC 2015
Hello World
Sun Sep 27 18:38:33 UTC 2015
Hello World
Sun Sep 27 18:38:43 UTC 2015
Hello World
[root@guestshell guestshell]#
```

Running under `systemd` / `systemctl`, your application is automatically restarted if it dies (or if you kill it). The Process ID is originally 226. After killing the application, it is automatically restarted with a Process ID of 257.

```
[root@guestshell guestshell]# ps -ef | grep hello
root      226      1  0 19:02 ?        00:00:00 /bin/bash /etc/init.d/hello.sh &
root      254     116  0 19:03 pts/4    00:00:00 grep --color=auto hello
[root@guestshell guestshell]#
[root@guestshell guestshell]# kill -9 226
[root@guestshell guestshell]#
[root@guestshell guestshell]# ps -ef | grep hello
root      257      1  0 19:03 ?        00:00:00 /bin/bash /etc/init.d/hello.sh &
root      264     116  0 19:03 pts/4    00:00:00 grep --color=auto hello
[root@guestshell guestshell]#
```

## Troubleshooting Guest Shell Issues

### Unable to Get Into Guest Shell After Downgrade to 7.0(3)I7

If you downgrade from the NX-OS 9.2(1) release to the NX-OS 7.0(3)7 release image (which does not have user namespace support) while the Guest Shell is in the process of activating or deactivating, you may run into the following condition where the Guest Shell activates, but you are unable to get into the Guest Shell. The reason for this issue is that if a reload is issued while the Guest Shell is in transition, the files within the Guest Shell can't get shifted back into an id range that is usable for NX-OS releases that don't have user namespace support.

```
switch# guestshell
Failed to mkdir .ssh for admin
admin RSA add failed
ERROR: Failed to connect with Virtual-service 'guestshell+'
switch#
```

```
switch# sh virt list

Virtual Service List:
Name           Status      Package Name
-----
guestshell+    Activated  guestshell.ova

switch# run bash ls -al /isan/vdc_1/virtual-instance/guestshell+/rootfs/
drwxr-xr-x  24 11000 11000 1024 Apr 11 10:44 .
drwxrwxrwx   4 root  root   80 Apr 27 20:08 ..
-rw-r--r--   1 11000 11000   0 Mar 21 16:24 .autorelabel
lrwxrwxrwx   1 11000 11000   7 Mar 21 16:24 bin -> usr/bin
```

To recover from this issue without losing the contents of the Guest Shell, reload the system with the previously-running NX-OS 9.2(x) image and let the Guest Shell get to the `Activated` state before reloading the system with the NX-OS 7.0(3)I7 image. Another option is to disable the Guest Shell while running NX-OS 9.2(x) and re-enable it after reloading with 7.0(3)I7.

If you do not have anything to preserve in the Guest Shell and you just want to recover it, you can destroy and recreate it without needing to change images.

### Unable to Access Files on bootflash from root in the Guest Shell

You may find that you are unable to access files on bootflash from root in the Guest Shell.

From the host:

```
root@switch# ls -al /bootflash/try.that
-rw-r--r-- 1 root root 0 Apr 27 20:55 /bootflash/try.that
root@switch#
```

From the Guest Shell:

```
[root@guestshellbootflash]# ls -al /bootflash/try.that
-rw-r--r-- 1 65534 host-root 0 Apr 27 20:55 /bootflash/try.that
[root@guestshellbootflash]# echo "some text" >> /bootflash/try.that
-bash: /bootflash/try.that: Permission denied
[root@guestshellbootflash]#
```

This may be due to the fact that, because the user namespace is being used to protect the host system, root in the Guest Shell is not actually the root of the system.

To recover from this issue, verify that the file permissions and group-id of the files allow for shared files on bootflash to be accessed as expected. You may need to change the permissions or group-id from the host Bash session.



## CHAPTER 4

# Python API

---

- [About the Python API](#) , on page 41
- [Using Python](#), on page 41

## About the Python API

Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an ideal language for scripting and rapid application development in many areas on most platforms.

The Python interpreter and the extensive standard library are freely available in source or binary form for all major platforms from the Python website:

<http://www.python.org/>

The same site also contains distributions of and pointers to many free third-party Python modules, programs and tools, and more documentation.

The Cisco Nexus Series devices support Python v2.7.5 in both interactive and noninteractive (script) modes and are available in the Guest Shell.

The Python scripting capability gives programmatic access to the device's command-line interface (CLI) to perform various tasks and Power On Auto Provisioning (POAP) or Embedded Event Manager (EEM) actions. Python also can be accessed from the Bash shell.

The Python interpreter is available in the Cisco NX-OS software.

## Using Python

This section describes how to write and execute Python scripts.

## Cisco Python Package

Cisco NX-OS provides a Cisco Python package that enables access to many core network-device modules, such as interfaces, VLANs, VRFs, ACLs, and routes. You can display the details of the Cisco Python package by entering the **help()** command. To obtain additional information about the classes and methods in a module,

you can run the help command for a specific module. For example, `help(cisco.interface)` displays the properties of the `cisco.interface` module.

For more Python modules, you can install the `python-modules-nxos` RPM (`python-modules-nxos-1.0.0-9.2.1.lib32_x86.rpm`) from [https://devhub.cisco.com/artifactory/open-nxos/9.2.1/x86\\_64/](https://devhub.cisco.com/artifactory/open-nxos/9.2.1/x86_64/). Refer to the "Manage Feature RPMs" section for instructions on installing an RPM.

The following is an example of how to display information about the Cisco Python package:

```
>>> import cisco
>>> help(cisco)
Help on package cisco:

NAME
    cisco

FILE
    /isan/python/scripts/cisco/__init__.py

PACKAGE CONTENTS
    acl
    bgp
    cisco_secret
    cisco_socket
    feature
    interface
    key
    line_parser
    md5sum
    nxcli
    ospf
    routemap
    routes
    section_parser
    ssh
    system
    tacacs
    vrf

CLASSES
    __builtin__.object
    cisco.cisco_secret.CiscoSecret
    cisco.interface.Interface
    cisco.key.Key
```

## Using the CLI Command APIs

The Python programming language uses three APIs that can execute CLI commands. The APIs are available from the Python CLI module.

These APIs are listed in the following table. You must enable the APIs with the `from cli import *` command. The arguments for these APIs are strings of CLI commands. To execute a CLI command through the Python interpreter, you enter the CLI command as an argument string of one of the following APIs:

Table 3: CLI Command APIs

API	Description
<b>cli()</b> Example: <pre>string = cli ("cli-command")</pre>	Returns the raw output of CLI commands, including control or special characters.  <b>Note</b> The interactive Python interpreter prints control or special characters 'escaped'. A carriage return is printed as '\n' and gives results that can be difficult to read. The <b>clip()</b> API gives results that are more readable.
<b>clid()</b> Example: <pre>json_string = clid ("cli-command")</pre>	Returns JSON output for cli-command, if XML support exists for the command, otherwise an exception is thrown.  <b>Note</b> This API can be useful when searching the output of show commands.
<b>clip()</b> Example: <pre>clip ("cli-command")</pre>	Prints the output of the CLI command directly to stdout and returns nothing to Python.  <b>Note</b> <pre>clip ("cli-command")</pre> is equivalent to <pre>r=cli("cli-command") print r</pre>

When two or more commands are run individually, the state is not persistent from one command to subsequent commands.

In the following example, the second command fails because the state from the first command does not persist for the second command:

```
>>> cli("conf t")
>>> cli("interface eth4/1")
```

When two or more commands are run together, the state is persistent from one command to subsequent commands.

In the following example, the second command is successful because the state persists for the second and third commands:

```
>>> cli("conf t ; interface eth4/1 ; shut")
```



**Note** Commands are separated with ";" as shown in the example. The semicolon (;) must be surrounded with single blank characters.

## Invoking the Python Interpreter from the CLI

The following example shows how to invoke Python from the CLI:



**Note** The Python interpreter is designated with the ">>>" or "... " prompt.

```
switch# python
Python 2.7.5 (default, Oct 8 2013, 23:59:43)
[GCC 4.6.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from cli import *
>>> import json
>>> cli('configure terminal ; interface loopback 5 ; no shut')
''
>>> intflist=json.loads(cli('show interface brief'))
>>> i=0
>>> while i < len(intflist['TABLE_interface']['ROW_interface']):
...     intf=intflist['TABLE_interface']['ROW_interface'][i]
...     i=i+1
...     if intf['state'] == 'up':
...         print intf['interface']
...
mgmt0
Ethernet2/7
Ethernet4/7
loopback0
loopback5
>>>
```

## Display Formats

The following examples show various display formats using the Python APIs:

Example 1:

```
>>> from cli import *
>>> cli("conf ; interface loopback 1")
''
>>> clip('where detail')
mode:
username:          admin
vdc:               switch
routing-context vrf: default
```

Example 2:

```
>>> from cli import *
>>> cli("conf ; interface loopback 1")
''
>>> cli('where detail')
' mode:          \n username:          admin\n vdc:
switch\n routing-context vrf: default\n'
>>>
```

Example 3:

```
>>> from cli import *
>>> cli("conf ; interface loopback 1")
```

```

''
>>> r = cli('where detail') ; print r
mode:
username:          admin
vdc:               EOR-1
routing-context vrf: default
>>>

```

#### Example 4:

```

>>> from cli import *
>>> import json
>>> out=json.loads(clid('show version'))
>>> for k in out.keys():
...     print "%30s = %s" % (k, out[k])
...
                                kern_uptm_secs = 21
                                kick_file_name = bootflash:///nxos.9.2.1.bin.S246
                                    rr_service = None
  module_id = Supervisor Module
  kick_tmstamp = 07/11/2018 00:01:44
  bios_cmpl_time = 05/17/2018
  bootflash_size = 20971520
  kickstart_ver_str = 9.2(1)
  kick_cmpl_time = 7/9/2018 9:00:00
  chassis_id = Nexus9000 C9504 (4 Slot) Chassis
  proc_board_id = SAL171211LX
  memory = 16077872
  manufacturer = Cisco Systems, Inc.
  kern_uptm_mins = 26
  bios_ver_str = 05.31
  cpu_name = Intel(R) Xeon(R) CPU D-1528 @ 1.90GHz
  kern_uptm_hrs = 2
  rr_usecs = 816550
  rr_sys_ver = 9.2(1)
  rr_reason = Reset Requested by CLI command reload
  rr_ctime = Wed Jul 11 20:44:39 2018
  header_str = Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
                                host_name = switch
                                    mem_type = kB
  kern_uptm_days = 0
>>>

```

## Non-interactive Python

A Python script can run in non-interactive mode by providing the Python script name as an argument to the Python CLI command. Python scripts must be placed under the bootflash or volatile scheme. A maximum of 32 command-line arguments for the Python script are allowed with the Python CLI command.

The Cisco Nexus Series device also supports the source CLI command for running Python scripts. The `bootflash:scripts` directory is the default script directory for the source CLI command.

The following example shows a script and how to run it:

```
switch# show file bootflash:deltaCounters.py
#!/isan/bin/python

from cli import *
import sys, time

ifName = sys.argv[1]
delay = float(sys.argv[2])
count = int(sys.argv[3])
cmd = 'show interface ' + ifName + ' counters'

out = json.loads(clid(cmd))
rxuc = int(out['TABLE_rx_counters']['ROW_rx_counters'][0]['eth_inucast'])
rxmc = int(out['TABLE_rx_counters']['ROW_rx_counters'][1]['eth_inmcast'])
rxbc = int(out['TABLE_rx_counters']['ROW_rx_counters'][1]['eth_inbcast'])
txuc = int(out['TABLE_tx_counters']['ROW_tx_counters'][0]['eth_outucast'])
txmc = int(out['TABLE_tx_counters']['ROW_tx_counters'][1]['eth_outmcast'])
txbc = int(out['TABLE_tx_counters']['ROW_tx_counters'][1]['eth_outbcast'])
print 'row rx_ucast rx_mcast rx_bcast tx_ucast tx_mcast tx_bcast'
print '=====
print '      %8d %8d %8d %8d %8d %8d' % (rxuc, rxmc, rxbc, txuc, txmc, txbc)
print '=====

i = 0
while (i < count):
    time.sleep(delay)
    out = json.loads(clid(cmd))
    rxucNew = int(out['TABLE_rx_counters']['ROW_rx_counters'][0]['eth_inucast'])
    rxmcNew = int(out['TABLE_rx_counters']['ROW_rx_counters'][1]['eth_inmcast'])
    rxbcNew = int(out['TABLE_rx_counters']['ROW_rx_counters'][1]['eth_inbcast'])
    txucNew = int(out['TABLE_tx_counters']['ROW_tx_counters'][0]['eth_outucast'])
    txmcNew = int(out['TABLE_tx_counters']['ROW_tx_counters'][1]['eth_outmcast'])
    txbcNew = int(out['TABLE_tx_counters']['ROW_tx_counters'][1]['eth_outbcast'])
    i += 1
    print '%-3d %8d %8d %8d %8d %8d' % \
        (i, rxucNew - rxuc, rxmcNew - rxmc, rxbcNew - rxbc, txucNew - txuc, txmcNew - txmc,
        txbcNew - txbc)

switch# python bootflash:deltaCounters.py Ethernet1/1 1 5
row rx_ucast rx_mcast rx_bcast tx_ucast tx_mcast tx_bcast
=====
              0       791         1         0    212739         0
=====
1           0         0         0         0         26         0
2           0         0         0         0         27         0
3           0         1         0         0         54         0
4           0         1         0         0         55         0
5           0         1         0         0         81         0
switch#
```

The following example shows how a source command specifies command-line arguments. In the example, *policy-map* is an argument to the `cgrep python` script. The example also shows that a source command can follow the pipe operator (`|`).

```
switch# show running-config | source sys/cgrep policy-map

policy-map type network-qos nw-pfc
policy-map type network-qos no-drop-2
policy-map type network-qos wred-policy
policy-map type network-qos pause-policy
policy-map type qos foo
policy-map type qos classify
policy-map type qos cos-based
policy-map type qos no-drop-2
policy-map type qos pfc-tor-port
```

## Running Scripts with Embedded Event Manager

On Cisco Nexus Series devices, Embedded Event Manager (EEM) policies support Python scripts.

The following example shows how to run a Python script as an EEM action:

- An EEM applet can include a Python script with an action command.

```
switch# show running-config eem

!Command: show running-config eem
!Time: Sun May  1 14:40:07 2011

version 6.1(2)I2(1)
event manager applet a1
  event cli match "show clock"
  action 1 cli python bootflash:pydate.py
  action 2 event-default
```

- You can search for the action that is triggered by the event in the log file by running the **show file logflash:event\_archive\_1** command.

```
switch# show file logflash:event_archive_1 | last 33

eem_event_time:05/01/2011,19:40:28 event_type:cli event_id:8 slot:active(1)
vdc:1 severity:minor applets:a1
eem_param_info:command = "exshow clock"
Starting with policy a1
Python

2011-05-01 19:40:28.644891
Executing the following commands succeeded:
python bootflash:pydate.py

PC_VSH_CMD_TLV(7679) with q
```

## Python Integration with Cisco NX-OS Network Interfaces

On Cisco Nexus Series devices, Python is integrated with the underlying Cisco NX-OS network interfaces. You can switch from one virtual routing context to another by setting up a context through the `cisco.vrf.set_global_vrf()` API.

The following example shows how to retrieve an HTML document over the management interface of a device. You can also establish a connection to an external entity over the inband interface by switching to a desired virtual routing context.

```
switch# python
Python 2.7.5 (default, Oct  8 2013, 23:59:43)
[GCC 4.6.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import urllib2
>>> from cisco.vrf import *
>>> set_global_vrf('management')
>>> page=urllib2.urlopen('http://172.23.40.211:8000/welcome.html')
>>> print page.read()
Hello Cisco Nexus 9000

>>>
>>> import cisco
>>> help(cisco.vrf.set_global_vrf)
Help on function set_global_vrf in module cisco.vrf:

set_global_vrf(vrf)
    Sets the global vrf. Any new sockets that are created (using socket.socket)
    will automatically get set to this vrf (including sockets used by other
    python libraries).

    Arguments:
      vrf: VRF name (string) or the VRF ID (int).

    Returns: Nothing

>>>
```

## Cisco NX-OS Security with Python

Cisco NX-OS resources are protected by the Cisco NX-OS Sandbox layer of software and by the CLI role-based access control (RBAC).

All users who are associated with a Cisco NX-OS network-admin or dev-ops role are privileged users. Users who are granted access to Python with a custom role are regarded as nonprivileged users. Nonprivileged users have limited access to Cisco NX-OS resources, such as the file system, guest shell, and Bash commands. Privileged users have greater access to all the resources of Cisco NX-OS.

### Examples of Security and User Authority

The following example shows how a privileged user runs commands:

```
switch# python
Python 2.7.5 (default, Oct  8 2013, 23:59:43)
[GCC 4.6.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('whoami')
admin
0
>>> f=open('/tmp/test','w')
>>> f.write('hello from python')
>>> f.close()
>>> r=open('/tmp/test','r')
>>> print r.read()
hello from python
```

```
>>> r.close()
```

The following example shows a nonprivileged user being denied access:

```
switch# python
Python 2.7.5 (default, Oct 8 2013, 23:59:43)
[GCC 4.6.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('whoami')
system(whoami): rejected!
-1
>>> f=open('/tmp/test','r')
Permission denied. Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
IOError: [Errno 13] Permission denied: '/tmp/test'
>>>
```

RBAC controls CLI access based on the login user privileges. A login user's identity is given to Python that is invoked from the CLI shell or from Bash. Python passes the login user's identity to any subprocess that is invoked from Python.

The following is an example for a privileged user:

```
>>> from cli import *
>>> cli('show clock')
'11:28:53.845 AM UTC Sun May 08 2011\n'
>>> cli('configure terminal ; vrf context myvrf')
''
>>> clip('show running-config l3vm')

!Command: show running-config l3vm
!Time: Sun May 8 11:29:40 2011

version 6.1(2)I2(1)

interface Ethernet1/48
  vrf member blue

interface mgmt0
  vrf member management
vrf context blue
vrf context management
vrf context myvrf
```

The following is an example for a nonprivileged user:

```
>>> from cli import *
>>> cli('show clock')
'11:18:47.482 AM UTC Sun May 08 2011\n'
>>> cli('configure terminal ; vrf context myvrf2')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/isan/python/scripts/cli.py", line 20, in cli
    raise cmd_exec_error(msg)
errors.cmd_exec_error: '% Permission denied for the role\n\nCmd exec error.\n'
```

The following example shows an RBAC configuration:

```
switch# show user-account
user:admin
      this user account has no expiry date
```

```

        roles:network-admin
user:pyuser
    this user account has no expiry date
    roles:network-operator python-role
switch# show role name python-role

```

## Example of Running Script with Scheduler

The following example shows a Python script that is running the script with the scheduler feature:

```

#!/bin/env python
from cli import *
from nxos import *
import os

switchname = cli("show switchname")
try:
    user = os.environ['USER']
except:
    user = "No user"
    pass

msg = user + " ran " + __file__ + " on : " + switchname
print msg
py_syslog(1, msg)
# Save this script in bootflash:///scripts

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature scheduler
switch(config)# scheduler job name testplan
switch(config-job)# python bootflash:///scripts/testplan.py
switch(config-job)# exit
switch(config)# scheduler schedule name testplan
switch(config-schedule)# job name testplan
switch(config-schedule)# time start now repeat 0:0:4
Schedule starts from Mon Mar 14 16:40:03 2011
switch(config-schedule)# end
switch# term mon
2011 Mar 14 16:38:03 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
10.19.68.246@pts/2
switch# show scheduler schedule
Schedule Name      : testplan
-----
User Name         : admin
Schedule Type     : Run every 0 Days 0 Hrs 4 Mins
Start Time        : Mon Mar 14 16:40:03 2011
Last Execution Time : Yet to be executed
-----
Job Name          Last Execution Status
-----
testplan          -NA-
=====
switch#
switch# 2011 Mar 14 16:40:04 switch %USER-1-SYSTEM_MSG: No user ran
/bootflash/scripts/testplan.py on : switch - nxpython
2011 Mar 14 16:44:04 switch last message repeated 1 time
switch#

```



## CHAPTER 5

# Scripting with Tcl

- [About Tcl, on page 51](#)
- [Running the Tclsh Command, on page 53](#)
- [Navigating Cisco NX-OS Modes from the Tclsh Command, on page 54](#)
- [Tcl References, on page 56](#)

## About Tcl

Tcl (pronounced "tickle") is a scripting language that increases flexibility of CLI commands. You can use Tcl to extract certain values in the output of a **show** command, perform switch configurations, run Cisco NX-OS commands in a loop, or define Embedded Event Manager (EEM) policies in a script.

This section describes how to run Tcl scripts or run Tcl interactively on Cisco NX-OS devices.

## Tclsh Command Help

Command help is not available for Tcl commands. You can still access the help functions of Cisco NX-OS commands from within an interactive Tcl shell.

This example shows the lack of Tcl command help in an interactive Tcl shell:

```
switch# tclsh
switch-tcl# set x 1
switch-tcl# puts ?
           ^
% Invalid command at '^' marker.
switch-tcl# configure ?
<CR>
  session  Configure the system in a session
  terminal Configure the system from terminal input

switch-tcl#
```



**Note** In the preceding example, the Cisco NX-OS command help function is still available but the Tcl **puts** command returns an error from the help function.

## Tclsh Command History

You can use the arrow keys on your terminal to access commands you previously entered in the interactive Tcl shell.




---

**Note** The **tclsh** command history is not saved when you exit the interactive Tcl shell.

---

## Tclsh Tab Completion

You can use tab completion for Cisco NX-OS commands when you are running an interactive Tcl shell. Tab completion is not available for Tcl commands.

## Tclsh CLI Command

Although you can directly access Cisco NX-OS commands from within an interactive Tcl shell, you can only execute Cisco NX-OS commands in a Tcl script if they are prepended with the Tcl **cli** command.

In an interactive Tcl shell, the following commands are identical and execute properly:

```
switch-tcl# cli show module 1 | incl Mod
switch-tcl# cli "show module 1 | incl Mod"
switch-tcl# show module 1 | incl Mod
```

In a Tcl script, you must prepend Cisco NX-OS commands with the Tcl **cli** command as shown in the following example:

```
set x 1
cli show module $x | incl Mod
cli "show module $x | incl Mod"
```

If you use the following commands in your script, the script fails and the Tcl shell displays an error:

```
show module $x | incl Mod
"show module $x | incl Mod"
```

## Tclsh Command Separation

The semicolon (;) is the command separator in both Cisco NX-OS and Tcl. To execute multiple Cisco NX-OS commands in a Tcl command, you must enclose the Cisco NX-OS commands in quotes ("").

In an interactive Tcl shell, the following commands are identical and execute properly:

```
switch-tcl# cli "configure terminal ; interface loopback 10 ; description loop10"
switch-tcl# cli configure terminal ; cli interface loopback 10 ; cli description loop10
switch-tcl# cli configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

switch(config-tcl)# cli interface loopback 10
switch(config-if-tcl)# cli description loop10
switch(config-if-tcl)#
```

In an interactive Tcl shell, you can also execute Cisco NX-OS commands directly without prepending the Tcl **cli** command:

```
switch-tcl# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(config-tcl)# interface loopback 10
switch(config-if-tcl)# description loop10
switch(config-if-tcl)#
```

## Tcl Variables

You can use Tcl variables as arguments to the Cisco NX-OS commands. You can also pass arguments into Tcl scripts. Tcl variables are not persistent.

The following example shows how to use a Tcl variable as an argument to a Cisco NX-OS command:

```
switch# tclsh
switch-tcl# set x loop10
switch-tcl# cli "configure terminal ; interface loopback 10 ; description $x"
switch(config-if-tcl)#
```

## Tclquit

The **tclquit** command exits the Tcl shell regardless of which Cisco NX-OS command mode is currently active. You can also press **Ctrl-C** to exit the Tcl shell. The **exit** and **end** commands change Cisco NX-OS command modes. The **exit** command terminates the Tcl shell only from the EXEC command mode.

## Tclsh Security

The Tcl shell is executed in a sandbox to prevent unauthorized access to certain parts of the Cisco NX-OS system. The system monitors CPU, memory, and file system resources being used by the Tcl shell to detect events such as infinite loops, excessive memory utilization, and so on.

You configure the initial Tcl environment with the **scripting tcl init** *init-file* command.

You can define the looping limits for the Tcl environment with the **scripting tcl recursion-limit** *iterations* command. The default recursion limit is 1000 iterations.

## Running the Tclsh Command

You can run Tcl commands from either a script or on the command line using the **tclsh** command.

**Note**

You cannot create a Tcl script file at the CLI prompt. You can create the script file on a remote device and copy it to the bootflash: directory on the Cisco NX-OS device.

### SUMMARY STEPS

1. **tclsh** [**bootflash:***filename* [*argument . . .* ]]

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>tclsh</b> [ <b>bootflash:filename</b> [ <i>argument . . .</i> ]]  <b>Example:</b> <pre>switch# tclsh ? &lt;CR&gt; bootflash: The file to run</pre>	<p>Starts a Tcl shell.</p> <p>If you run the <b>tclsh</b> command with no arguments, the shell runs interactively, reading Tcl commands from standard input and printing command results and error messages to the standard output. You exit from the interactive Tcl shell by typing <b>tclquit</b> or <b>Ctrl-C</b>.</p> <p>If you run the <b>tclsh</b> command with arguments, the first argument is the name of a script file containing Tcl commands and any additional arguments are made available to the script as variables.</p>

**Example**

The following example shows an interactive Tcl shell:

```
switch# tclsh
switch-tcl# set x 1
switch-tcl# cli show module $x | incl Mod
Mod Ports Module-Type Model Status
1 36 36p 40G Ethernet Module N9k-X9636PQ ok
Mod Sw Hw
Mod MAC-Address(es) Serial-Num

switch-tcl# exit
switch#
```

The following example shows how to run a Tcl script:

```
switch# show file bootflash:showmodule.tcl
set x 1
while {$x < 19} {
cli show module $x | incl Mod
set x [expr {$x + 1}]
}

switch# tclsh bootflash:showmodule.tcl
Mod Ports Module-Type Model Status
1 36 36p 40G Ethernet Module N9k-X9636PQ ok
Mod Sw Hw
Mod MAC-Address(es) Serial-Num

switch#
```

## Navigating Cisco NX-OS Modes from the Tclsh Command

You can change modes in Cisco NX-OS while you are running an interactive Tcl shell.

## SUMMARY STEPS

1. `tclsh`
2. `configure terminal`
3. `tclquit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>tclsh</b> <b>Example:</b> <pre>switch# tclsh switch-tcl#</pre>	Starts an interactive Tcl shell.
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>switch-tcl# configure terminal switch(config-tcl)#</pre>	Runs a Cisco NX-OS command in the Tcl shell, changing modes.  <b>Note</b> The Tcl prompt changes to indicate the Cisco NX-OS command mode.
Step 3	<b>tclquit</b> <b>Example:</b> <pre>switch-tcl# tclquit switch#</pre>	Terminates the Tcl shell, returning to the starting mode.

## Example

The following example shows how to change Cisco NX-OS modes from an interactive Tcl shell:

```
switch# tclsh
switch-tcl# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-tcl)# interface loopback 10
switch(config-if-tcl)# ?
  description  Enter description of maximum 80 characters
  inherit      Inherit a port-profile
  ip           Configure IP features
  ipv6        Configure IPv6 features
  logging      Configure logging for interface
  no          Negate a command or set its defaults
  rate-limit   Set packet per second rate limit
  shutdown    Enable/disable an interface
  this        Shows info about current object (mode's instance)
  vrf         Configure VRF parameters
  end         Go to exec mode
  exit        Exit from command interpreter
  pop         Pop mode from stack or restore from name
  push        Push current mode to stack or save it under name
  where       Shows the cli context you are in

switch(config-if-tcl)# description loop10
switch(config-if-tcl)# tclquit
```

```
Exiting Tcl  
switch#
```

## Tcl References

The following titles are provided for your reference:

- Mark Harrison (ed), *Tcl/Tk Tools*, O'Reilly Media, ISBN 1-56592-218-2, 1997
- Mark Harrison and Michael McLennan, *Effective Tcl/Tk Programming*, Addison-Wesley, Reading, MA, USA, ISBN 0-201-63474-0, 1998
- John K. Ousterhout, *Tcl and the Tk Toolkit*, Addison-Wesley, Reading, MA, USA, ISBN 0-201-63337-X, 1994.
- Brent B. Welch, *Practical Programming in Tcl and Tk*, Prentice Hall, Upper Saddle River, NJ, USA, ISBN 0-13-038560-3, 2003.
- J Adrian Zimmer, *Tcl/Tk for Programmers*, IEEE Computer Society, distributed by John Wiley and Sons, ISBN 0-8186-8515-8, 1998.



## CHAPTER 6

# Ansible

- [Prerequisites](#), on page 57
- [About Ansible](#), on page 57
- [Cisco Ansible Module](#), on page 57

## Prerequisites

Go to [https://docs.ansible.com/ansible/intro\\_installation.html](https://docs.ansible.com/ansible/intro_installation.html) for installation requirements for supported control environments.

## About Ansible

Ansible is an open-source IT automation engine that automates cloud provisioning, configuration management, application deployment, intraservice orchestration, and other IT needs.

Ansible uses small programs that are called Ansible modules to make API calls to your nodes, and apply configurations that are defined in playbooks.

By default, Ansible represents what machines it manages using a simple INI file that puts all your managed machines in groups of your own choosing.

More information can be found from Ansible:

Ansible	<a href="https://www.ansible.com/">https://www.ansible.com/</a>
Ansible Automation Solutions. Includes installation instructions, playbook instructions and examples, module lists, and so on.	<a href="https://docs.ansible.com/">https://docs.ansible.com/</a>

## Cisco Ansible Module

There are multiple Cisco NX-OS-supported modules and playbooks for Ansible, as per the following table of links:

NX-OS developer landing page.	<a href="#">Configuration Management Tools</a>
-------------------------------	------------------------------------------------

Ansible NX-OS playbook examples	<a href="#">Repo for ansible nxos playbooks</a>
Ansible NX-OS network modules	<a href="#">nxos network modules</a>



## CHAPTER 7

# Puppet Agent

This chapter includes the following sections:

- [About Puppet, on page 59](#)
- [Prerequisites, on page 59](#)
- [Puppet Agent NX-OS Environment, on page 60](#)
- [ciscopuppet Module, on page 60](#)

## About Puppet

The Puppet software package, developed by Puppet Labs, is an open source automation toolset for managing servers and other resources. The Puppet software accomplishes server and resource management by enforcing device states, such as configuration settings.

Puppet components include a puppet agent which runs on the managed device (node) and a Puppet Master (server). The Puppet Master typically runs on a separate dedicated server and serves multiple devices. The operation of the puppet agent involves periodically connecting to the Puppet Master, which in turn compiles and sends a configuration manifest to the agent. The agent reconciles this manifest with the current state of the node and updates state that is based on differences.

A puppet manifest is a collection of property definitions for setting the state on the device. The details for checking and setting these property states are abstracted so that a manifest can be used for more than one operating system or platform. Manifests are commonly used for defining configuration settings, but they also can be used to install software packages, copy files, and start services.

More information can be found from Puppet Labs:

Puppet Labs	<a href="https://puppetlabs.com">https://puppetlabs.com</a>
Puppet Labs FAQ	<a href="https://puppet.com/products/faq">https://puppet.com/products/faq</a>
Puppet Labs Documentation	<a href="https://puppet.com/docs">https://puppet.com/docs</a>

## Prerequisites

The following are prerequisites for the Puppet Agent:

- You must have a Cisco device and operating system software release that supports the installation.

- Cisco Nexus 3500 Series switch
- Cisco Nexus 3100 Series switch.
- Cisco Nexus 3000 Series switch.
- Cisco NX-OS release 7.0(3)I2(1) or later.
- You must have the required disk storage available on the device for virtual services installation and deployment of Puppet Agent.
  - A minimum of 450MB free disk space on bootflash.
- You must have Puppet Master server with Puppet 4.0 or later.
- You must have Puppet Agent 4.0 or later.

## Puppet Agent NX-OS Environment

The Puppet Agent software must be installed on a Cisco Nexus platform in the Guest Shell (the Linux container environment running CentOS). The Guest Shell provides a secure, open execution environment that is decoupled from the host.

Starting with the Cisco NX-OS Release 9.2(1), the Bash-shell (native WindRiver Linux environment underlying NX-OS) install of Puppet Agent is no longer supported.

The following provides information about agent-software download, installation, and setup:

Puppet Agent: Installation & Setup on Cisco Nexus switches (Manual Setup)	<a href="https://github.com/cisco/cisco-network-puppet-module/blob/develop/docs/README-agent-install.md">https://github.com/cisco/cisco-network-puppet-module/blob/develop/docs/README-agent-install.md</a>
---------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## ciscopuppet Module

The ciscopuppet module is a Cisco developed open-source software module. It interfaces between the abstract resources configuration in a puppet manifest and the specific implementation details of the Cisco Nexus NX-OS operating system and platform. This module is installed on the Puppet Master and is required for puppet agent operation on Cisco Nexus switches.

The ciscopuppet module is available on Puppet Forge.

The following provide additional information about the ciscopuppet module installation procedures:

ciscopuppet Module location (Puppet Forge)	<a href="https://forge.puppetlabs.com/puppetlabs/ciscopuppet">https://forge.puppetlabs.com/puppetlabs/ciscopuppet</a>
Resource Type Catalog	<a href="https://github.com/cisco/cisco-network-puppet-module/tree/master#resource-by-tech">https://github.com/cisco/cisco-network-puppet-module/tree/master#resource-by-tech</a>
ciscopuppet Module: Source Code Repository	<a href="https://github.com/cisco/cisco-network-puppet-module/tree/master">https://github.com/cisco/cisco-network-puppet-module/tree/master</a>

ciscopuppet Module: Setup & Usage	<a href="#">Cisco Puppet Module::README.md</a>
Puppet Labs: Installing Modules	<a href="https://docs.puppetlabs.com/puppet/latest/reference/modules_installing.html">https://docs.puppetlabs.com/puppet/latest/reference/modules_installing.html</a>
Puppet NX-OS Manifest Examples	<a href="https://github.com/cisco/cisco-network-puppet-module/tree/master/examples">https://github.com/cisco/cisco-network-puppet-module/tree/master/examples</a>
NX-OS developer landing page.	<a href="#">Configuration Management Tools</a>





## CHAPTER 8

# Using Chef Client with Cisco NX-OS

This chapter includes the following sections:

- [About Chef, on page 63](#)
- [Prerequisites, on page 63](#)
- [Chef Client NX-OS Environment, on page 64](#)
- [cisco-cookbook, on page 64](#)

## About Chef

Chef is an open-source software package developed by Chef Software, Inc. It is a systems and cloud infrastructure automation framework that deploys servers and applications to any physical, virtual, or cloud location, no matter the size of the infrastructure. Each organization is comprised of one or more workstations, a single server, and every node that will be configured and maintained by the chef-client. Cookbooks and recipes are used to tell the chef-client how each node should be configured. The chef-client, which is installed on every node, does the actual configuration.

A Chef cookbook is the fundamental unit of configuration and policy distribution. A cookbook defines a scenario and contains everything that is required to support that scenario, including libraries, recipes, files, and more. A Chef recipe is a collection of property definitions for setting state on the device. The details for checking and setting these property states are abstracted away so that a recipe may be used for more than one operating system or platform. While recipes are commonly used for defining configuration settings, they can also be used to install software packages, copy files, start services, and more.

The following references provide more information from Chef:

Topic	Link
Chef home	<a href="https://www.chef.io">https://www.chef.io</a>
Chef overview	<a href="https://docs.chef.io/chef_overview.html">https://docs.chef.io/chef_overview.html</a>
Chef documentation (all)	<a href="https://docs.chef.io/">https://docs.chef.io/</a>

## Prerequisites

The following are prerequisites for Chef:

- You must have a Cisco device and operating system software release that supports the installation:
  - Cisco Nexus 3500 Series switch
  - Cisco NX-OS Release 6.1(2)I3(4) or higher
- You must have the required disk storage available on the device for Chef deployment:
  - A minimum of 500 MB free disk space on bootflash
- You need a Chef server with Chef 12.4.1 or higher.
- You need Chef Client 12.4.1 or higher.

## Chef Client NX-OS Environment

The chef-client software must be installed on Cisco Nexus platforms. Customers can install chef-client in one of the Linux environments provided by the Cisco Nexus platform:

- Bash Shell—This is the native WindRiver Linux environment underlying Cisco NX-OS.
- Guest Shell—This is a secure Linux container environment running CentOS. Its advantage is a secure, open execution environment that is decoupled from the host.

The workflow for both use cases is similar.

The following documents provide step-by-step guidance on agent software download, installation, and setup:

Topic	Link
Chef Client (Native)	Latest information on Client RPM is available <a href="#">here</a> .
Chef Client (Guest Shell, CentOs7)	Latest information on Client RPM is available <a href="#">here</a> .
Chef Client: Installation and setup on Cisco Nexus platform (manual setup)	<a href="#">cisco-cookbook::README-install-agent.md</a>
Chef Client: Installation and setup on Cisco Nexus platform (automated installation using the Chef provisioner)	<a href="#">cisco-cookbook::README-chef-provisioning.md</a>

## cisco-cookbook

cisco-cookbook is a Cisco-developed open-source interface between the abstract resources configuration in a Chef recipe and the specific implementation details of the Cisco Nexus operating system and platforms. This cookbook is installed on the Chef Server and is required for proper Chef Client operation on Cisco Nexus devices.

cisco-cookbook can be found on Chef Supermarket.

The following documents provide additional detail for cisco-cookbook and generic cookbook installation procedures:

Topic	Link
cisco-cookbook location	<a href="https://supermarket.chef.io/cookbooks/cisco-cookbook">https://supermarket.chef.io/cookbooks/cisco-cookbook</a>
Resource Type Catalog	<a href="https://github.com/cisco/cisco-network-chef-cookbook#resource-by-tech">https://github.com/cisco/cisco-network-chef-cookbook#resource-by-tech</a>
cisco-cookbook: Source Code Repository	<a href="https://github.com/cisco/cisco-network-chef-cookbook">https://github.com/cisco/cisco-network-chef-cookbook</a>
cisco-cookbook: Setup and usage	<a href="#">cisco-cookbook::README.md</a>
Chef Supermarket	<a href="https://supermarket.chef.io">https://supermarket.chef.io</a>
NX-OS developer landing page.	<a href="#">Configuration Management Tools</a>





## CHAPTER 9

# Using Docker with Cisco NX-OS

---

This chapter contains the following topics:

- [About Docker with Cisco NX-OS, on page 67](#)
- [Guidelines and Limitations, on page 67](#)
- [Prerequisites for Setting Up Docker Containers Within Cisco NX-OS, on page 68](#)
- [Starting the Docker Daemon, on page 68](#)
- [Configure Docker to Start Automatically, on page 69](#)
- [Starting Docker Containers: Host Networking Model, on page 69](#)
- [Starting Docker Containers: Bridged Networking Model, on page 71](#)
- [Mounting the bootflash and volatile Partitions in the Docker Container, on page 72](#)
- [Enabling Docker Daemon Persistence on Enhanced ISSU Switchover, on page 72](#)
- [Enabling Docker Daemon Persistence on the Cisco Nexus 9500 Series Switches Switchover, on page 73](#)
- [Resizing the Docker Storage Backend, on page 74](#)
- [Stopping the Docker Daemon, on page 76](#)
- [Docker Container Security, on page 76](#)
- [Docker Troubleshooting, on page 78](#)

## About Docker with Cisco NX-OS

Docker provides a way to run applications securely isolated in a container, packaged with all its dependencies and libraries. See <https://docs.docker.com/> for more information on Docker.

Beginning with Release 9.2(1), support is now added for using Docker within Cisco NX-OS on a switch.

The version of Docker that is included on the switch is 1.13.1. The Docker daemon is not running by default. You must start it manually or set it up to automatically restart when the switch boots up.

This section describes how to enable and use Docker in the specific context of the Cisco Nexus switch environment. Refer to the Docker documentation at <https://docs.docker.com/> for details on general Docker usage and functionality.

## Guidelines and Limitations

Following are the guidelines and limitations for using Docker on Cisco NX-OS on a switch:

- Docker functionality is supported on the series switches with at least 8 GB of system RAM.

## Prerequisites for Setting Up Docker Containers Within Cisco NX-OS

Following are the prerequisites for using Docker on Cisco NX-OS on a switch:

- Enable the host Bash shell. To use Docker on Cisco NX-OS on a switch, you must be the root user on the host Bash shell:

```
switch# configure terminal
      Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature bash-shell
```

- If the switch is in a network that uses an HTTP proxy server, the `http_proxy` and `https_proxy` environment variables must be set up in `/etc/sysconfig/docker`. For example:

```
export http_proxy=http://proxy.esl.cisco.com:8080
export https_proxy=http://proxy.esl.cisco.com:8080
```

- Verify that the switch clock is set correctly, or you might see the following error message:

```
x509: certificate has expired or is not yet valid
```

- Verify that the domain name and name servers are configured appropriately for the network and that it is reflected in the `/etc/resolv.conf` file:

```
switch# conf t
      Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vrf context management
switch(config-vrf)# ip domain-name ?
WORD Enter the default domain (Max Size 64)

switch(config-vrf)# ip name-server ?
A.B.C.D Enter an IPv4 address
A:B::C:D Enter an IPv6 address

root@switch# cat /etc/resolv.conf
domain cisco.com #bleed
nameserver 171.70.168.183 #bleed
root@switch#
```

## Starting the Docker Daemon

When you start the Docker daemon for the first time, a fixed-size backend storage space is carved out in a file called `dockerpart` on the bootflash, which is then mounted to `/var/lib/docker`. If necessary, you can adjust the default size of this space by editing `/etc/sysconfig/docker` before you start the Docker daemon for the first time. You can also resize this storage space if necessary as described later on.

To start the Docker daemon:

---

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Start the Docker daemon.

```
root@switch# service docker start
```

**Step 3** Check the status.

```
root@switch# service docker status
dockerd (pid 3597) is running...
root@switch#
```

**Note** Once you start the Docker daemon, do not delete or tamper with the `dockerpart` file on the bootflash since it is critical to the docker functionality.

```
switch# dir bootflash:dockerpart
20000000000 Mar 14 12:50:14 2018 dockerpart
```

---

## Configure Docker to Start Automatically

You can configure the Docker daemon to always start up automatically when the switch boots up.

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Use the `chkconfig` utility to make the Docker service persistent.

```
root@switch# chkconfig --add docker
root@n9k-2#
```

**Step 3** Use the `chkconfig` utility to check the Docker service settings.

```
root@switch# chkconfig --list | grep docker
docker 0:off 1:off 2:on 3:on 4:on 5:on 6:off
root@switch#
```

**Step 4** To remove the configuration so that Docker does not start up automatically:

```
root@switch# chkconfig --del docker
root@switch# chkconfig --list | grep docker
root@switch#
```

---

## Starting Docker Containers: Host Networking Model

If you want Docker containers to have access to all the host network interfaces, including data port and management, start the Docker containers with the `--network host` option. The user in the container can

switch between the different network namespaces at `/var/run/netns` (corresponding to different VRFs configured in Cisco NX-OS) using the `ip netns exec <net_namespace> <cmd>`.

### Step 1 Load Bash and become superuser.

```
switch# run bash sudo su -
```

### Step 2 Start the Docker container.

Following is an example of starting an Alpine Docker container on the switch and viewing all the network interfaces. The container is launched into the management network namespace by default.

```
root@switch# docker run --name=alpinerun -v /var/run/netns:/var/run/netns:ro,rslave --rm --network
host --cap-add SYS_ADMIN -it alpine
/ # apk --update add iproute2
fetch http://dl-cdn.alpinelinux.org/alpine/v3.7/main/x86_64/APKINDEX.tar.gz
fetch http://dl-cdn.alpinelinux.org/alpine/v3.7/community/x86_64/APKINDEX.tar.gz
(1/6) Installing libelf (0.8.13-r3)
(2/6) Installing libmnl (1.0.4-r0)
(3/6) Installing jansson (2.10-r0)
(4/6) Installing libnftnl-libs (1.0.8-r1)
(5/6) Installing iptables (1.6.1-r1)
(6/6) Installing iproute2 (4.13.0-r0)
Executing iproute2-4.13.0-r0.post-install
Executing busybox-1.27.2-r7.trigger
OK: 7 MiB in 17 packages
/ #
/ # ip netns list
management
default
/ #
/ # ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default
link/ipip 0.0.0.0 brd 0.0.0.0
3: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN group default
link/gre 0.0.0.0 brd 0.0.0.0
...
/ #
/ # ip netns exec default ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/16 scope host lo
valid_lft forever preferred_lft forever
2: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default
link/ether 42:0d:9b:3c:d4:62 brd ff:ff:ff:ff:ff:ff
3: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default
link/ipip 0.0.0.0 brd 0.0.0.0
...
```

# Starting Docker Containers: Bridged Networking Model

If you want Docker containers to only have external network connectivity (typically through the management interface) and you don't necessarily care about visibility into a specific data port or other Cisco Nexus switch interface, you can start the Docker container with the default Docker bridged networking model. This is more secure than the host networking model described in the previous section since it also provides network namespace isolation.

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Start the Docker container.

Following is an example of starting an Alpine Docker container on the switch and installing the `iproute2` package.

```
root@switch# docker run -it --rm alpine
/ # apk --update add iproute2
fetch http://dl-cdn.alpinelinux.org/alpine/v3.7/main/x86_64/APKINDEX.tar.gz
fetch http://dl-cdn.alpinelinux.org/alpine/v3.7/community/x86_64/APKINDEX.tar.gz
(1/6) Installing libelf (0.8.13-r3)
(2/6) Installing libmnl (1.0.4-r0)
(3/6) Installing jansson (2.10-r0)
(4/6) Installing libnftnl-libs (1.0.8-r1)
(5/6) Installing iptables (1.6.1-r1)
(6/6) Installing iproute2 (4.13.0-r0)
Executing iproute2-4.13.0-r0.post-install
Executing busybox-1.27.2-r7.trigger
OK: 7 MiB in 17 packages
/ #
/ # ip netns list
/ #
```

**Step 3** Determine if you want to set up user namespace isolation.

For containers using the bridged networking model, you can also set up user namespace isolation to further improve security. See [Securing Docker Containers With User namespace Isolation, on page 77](#) for more information.

You can use standard Docker port options to expose a service from within the container, such as `sshd`. For example:

```
root@switch# docker run -d -p 18877:22 --name sshd_container sshd_ubuntu
```

This maps port 22 from within the container to port 18877 on the switch. The service can now be accessed externally through port 18877, as shown in the following example:

```
root@ubuntu-vm# ssh root@ip_address -p 18887
```

# Mounting the bootflash and volatile Partitions in the Docker Container

You can make the `bootflash` and `volatile` partitions visible in the Docker container by passing in the `-v /bootflash:/bootflash` and `-v /volatile:/volatile` options in the run command for the Docker container. This is useful if the application in the container needs access to files shared with the host, such as copying a new NX-OS system image to bootflash.



**Note** This `-v` command option allows for any directory to be mounted into the container and may result in information leaking or other accesses that may impact the operation of the NX-OS system. Limit this to resources such as `/bootflash` and `/volatile` that are already accessible using NX-OS CLI.

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Pass in the `-v /bootflash:/bootflash` and `-v /volatile:/volatile` options in the run command for the Docker container.

```
root@switch# docker run -v /bootflash:/bootflash -v /volatile:/volatile -it --rm alpine
/# ls /
bin          etc          media        root         srv          usr
bootflash   home         mnt          run          sys          var
dev          lib          proc         sbin         tmp          volatile
/ #
```

# Enabling Docker Daemon Persistence on Enhanced ISSU Switchover

You can have both the Docker daemon and any running containers persist on an Enhanced ISSU switchover. This is possible since the bootflash on which the backend Docker storage resides is the same and shared between both Active and Standby supervisors.

The Docker containers are disrupted (restarted) during the switchover, so they will not be running continuously.

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Before starting the switchover, use the `chkconfig` utility to make the Docker service persistent.

```
root@switch# chkconfig --add docker
root@n9k-2#
```

**Step 3** Start any containers using the `--restart unless-stopped` option so that they will be restarted automatically after the switchover.

The following example starts an Alpine container and configures it to always restart unless it is explicitly stopped or Docker is restarted:

```
root@switch# docker run -dit --restart unless-stopped alpine
root@n9k-2#
```

The Docker containers are disrupted (restarted) during the switchover, so they will not be running continuously.

---

## Enabling Docker Daemon Persistence on the Cisco Nexus 9500 Series Switches Switchover

You can have both the Docker daemon and any running containers persist on a switchover between two separate physical supervisors with distinct bootflash partitions. However, for the Cisco Nexus 9500 series switch, the bootflash partitions on both supervisors are physically separate. You will therefore need to copy the `dockerpart` file manually to the standby supervisor before performing the switchover.

---

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Start any containers using the `--restart unless-stopped` option so that they will be restarted automatically after the switchover.

The following example starts an Alpine container and configures it to always restart unless it is explicitly stopped or Docker is restarted:

```
root@switch# docker run -dit --restart unless-stopped alpine
root@n9k-2#
```

Note that the Docker containers will be disrupted (restarted) during the switchover, so they will not be running continuously.

**Step 3** Before starting the switchover, use the `chkconfig` utility to make the Docker service persistent.

```
root@switch# chkconfig --add docker
root@n9k-2#
```

**Step 4** Copy the Docker backend storage partition from the active to the standby supervisor bootflash:

```
root@switch# service docker stop
Stopping dockerd: dockerd shutdown

root@switch# cp /bootflash/dockerpart /bootflash_sup-remote/
```

```
root@switch# service docker start
```

---

## Resizing the Docker Storage Backend

After starting or using the Docker daemon, you can grow the size of the Docker backend storage space according to your needs.

---

### Step 1 Disable the Guest Shell.

If you do not disable the Guest Shell, it may interfere with the resize.

```
switch# guestshell disable
You will not be able to access your guest shell if it is disabled. Are you sure you want to disable
the guest shell? (y/n) [n] y
switch# 2018 Mar 15 17:16:55 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Deactivating virtual
service 'guestshell+'
2018 Mar 15 17:16:57 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully deactivated virtual
service 'guestshell+'
```

### Step 2 Load Bash and become superuser.

```
switch# run bash sudo su -
```

### Step 3 Get information on the current amount of storage space available.

```
root@switch# df -kh /var/lib/docker
Filesystem Size Used Avail Use% Mounted on
/dev/loop12 1.9G 7.6M 1.8G 1% /var/lib/docker
root@n9k-2#
```

### Step 4 Stop the Docker daemon.

```
root@switch# service docker stop
Stopping dockerd: dockerd shutdown
```

### Step 5 Get information on the current size of the Docker backend storage space (/bootflash/dockerpart).

```
root@switch# ls -l /bootflash/dockerpart
-rw-r--r-- 1 root root 2000000000 Mar 15 16:53 /bootflash/dockerpart
root@n9k-2#
```

### Step 6 Resize the Docker backend storage space.

For example, the following command increases the size by 500 megabytes:

```
root@switch# truncate -s +500MB /bootflash/dockerpart
root@n9k-2#
```

### Step 7 Get updated information on the size of the Docker backend storage space to verify that the resizing process was completed successfully.

For example, the following output confirms that the size of the Docker backend storage was successfully increased by 500 megabytes:

```
root@switch# ls -l /bootflash/dockerpart
-rw-r--r-- 1 root root 2500000000 Mar 15 16:54 /bootflash/dockerpart
root@n9k-2#
```

**Step 8** Check the size of the filesystem on `/bootflash/dockerpart`.

```
root@switch# e2fsck -f /bootflash/dockerpart
e2fsck 1.42.9 (28-Dec-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/bootflash/dockerpart: 528/122160 files (0.6% non-contiguous), 17794/488281 blocks
```

**Step 9** Resize the filesystem on `/bootflash/dockerpart`.

```
root@switch# /sbin/resize2fs /bootflash/dockerpart
resize2fs 1.42.9 (28-Dec-2013)
Resizing the filesystem on /bootflash/dockerpart to 610351 (4k) blocks.
The filesystem on /bootflash/dockerpart is now 610351 blocks long.
```

**Step 10** Check the size of the filesystem on `/bootflash/dockerpart` again to confirm that the filesystem was successfully resized.

```
root@switch# e2fsck -f /bootflash/dockerpart
e2fsck 1.42.9 (28-Dec-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/bootflash/dockerpart: 528/154736 files (0.6% non-contiguous), 19838/610351 blocks
```

**Step 11** Start the Docker daemon again.

```
root@switch# service docker start
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Starting dockerd with args '--debug=true':
```

**Step 12** Verify the new amount of storage space available.

```
root@switch# df -kh /var/lib/docker
Filesystem Size Used Avail Use% Mounted on
/dev/loop12 2.3G 7.6M 2.3G 1% /var/lib/docker
```

**Step 13** Exit out of Bash shell.

```
root@switch# exit
logout
switch#
```

**Step 14** Enable the Guest Shell, if necessary.

```
switch# guestshell enable

switch# 2018 Mar 15 17:12:53 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Activating virtual service
'guestshell+'
switch# 2018 Mar 15 17:13:18 switch %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully activated
virtual service 'guestshell+'
```

---

## Stopping the Docker Daemon

If you no longer wish to use Docker, follow the procedures in this topic to stop the Docker daemon.

---

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Stop the Docker daemon.

```
root@switch# service docker stop
Stopping dockerd: dockerd shutdown
```

**Step 3** Verify that the Docker daemon is stopped.

```
root@switch# service docker status
dockerd is stopped
root@switch#
```

**Note** You can also delete the `dockerpart` file on the bootflash at this point, if necessary:

```
switch# delete bootflash:dockerpart
Do you want to delete "/dockerpart" ? (yes/no/abort) y
switch#
```

---

## Docker Container Security

Following are the Docker container security recommendations:

- Run in a separate user `namespace` if possible.
- Run in a separate network `namespace` if possible.
- Use `cgroups` to limit resources. An existing `cgroup` (`ext_ser`) is created to limit hosted applications to what the platform team has deemed reasonable for extra software running on the switch. Docker allows use of this and limiting per-container resources.
- Do not add unnecessary POSIX capabilities.

## Securing Docker Containers With User namespace Isolation

For containers using the bridged networking model, you can also set up user namespace isolation to further improve security. See <https://docs.docker.com/engine/security/usersns-remap/> for more information.

**Step 1** Determine if a `dockremap` group already exists on your system.

A `dockremap` user must already be set up on your system by default. If the `dockremap` group doesn't already exist, follow these steps to create it.

a) Enter the following command to create the `dockremap` group:

```
root@switch# groupadd dockremap -r
```

b) Create the `dockremap` user, unless it already exists:

```
root@switch# useradd dockremap -r -g dockremap
```

c) Verify that the `dockremap` group and the `dockremap` user were created successfully:

```
root@switch# id dockremap
uid=999(dockremap) gid=498(dockremap) groups=498(dockremap)
root@switch#
```

**Step 2** Add the desired re-mapped ID and range to the `/etc/subuid` and `/etc/subgid`.

For example:

```
root@switch# echo "dockremap:123000:65536" >> /etc/subuid
root@switch# echo "dockremap:123000:65536" >> /etc/subgid
```

**Step 3** Using a text editor, add the `--usersns-remap=default` option to the `other_args` field in the `/etc/sysconfig/docker` file.

For example:

```
other_args="--debug=true --usersns-remap=default"
```

**Step 4** Restart the Docker daemon, or start it if it is not already running, using `service docker [re]start`.

For example:

```
root@switch# service docker [re]start
```

Refer to the Docker documentation at <https://docs.docker.com/engine/security/usersns-remap/> for more information on configuring and using containers with user namespace isolation.

## Moving the `cgroup` Partition

The `cgroup` partition for third-party services is `ext_ser`, which limits CPU usage to 25% per core. Cisco recommends that you run your Docker container under this `ext_ser` partition.

If the Docker container is run without the `--cgroup-parent=/ext_ser/` option, it can get up to the full 100% host CPU access, which can interfere with the regular operation of Cisco NX-OS.

**Step 1** Load Bash and become superuser.

```
switch# run bash sudo su -
```

**Step 2** Run the Docker container under the `ext_ser` partition.

For example:

```
root@switch# docker run --name=alpinerrun -v /var/run/netns:/var/run/netns:ro,rslave --rm --network
host --cgroup-parent=/ext_ser/ --cap-add SYS_ADMIN -it alpine
/ #
```

## Docker Troubleshooting

These topics describe issues that can arise with Docker containers and provides possible resolutions.

### Docker Fails to Start

**Problem:** Docker fails to start, showing an error message similar to the following:

```
switch# run bash
bash-4.3$ service docker start
Free bootflash: 39099 MB, total bootflash: 51771 MB
Carving docker bootflash storage: 2000 MB
2000+0 records in
2000+0 records out
2000000000 bytes (2.0 GB) copied, 22.3039 s, 89.7 MB/s
losetup: /dev/loop18: failed to set up loop device: Permission denied
mke2fs 1.42.9 (28-Dec-2013)
mkfs.ext4: Device size reported to be zero. Invalid partition specified, or
partition table wasn't reread after running fdisk, due to
a modified partition being busy and in use. You may need to reboot
to re-read your partition table.

Failed to create docker volume
```

**Possible Cause:** You might be running Bash as an admin user instead of as a root user.

**Solution:** Determine if you are running Bash as an admin user instead of as a root user:

```
bash-4.3$ whoami
admin
```

Exit out of Bash and run Bash as root user:

```
bash-4.3$ exit
switch# run bash sudo su -
```

## Docker Fails to Start Due to Insufficient Storage

**Problem:** Docker fails to start, showing an error message similar to the following, due to insufficient bootflash storage:

```
root@switch# service docker start
Free bootflash: 790 MB, total bootflash: 3471 MB
Need at least 2000 MB free bootflash space for docker storage
```

**Possible Cause:** You might not have enough free bootflash storage.

**Solution:** Free up space or adjust the `variable_dockerstrg` values in `/etc/sysconfig/docker` as needed, then restart the Docker daemon:

```
root@switch# cat /etc/sysconfig/docker
# Replace the below with your own docker storage backend boundary value (in MB)
# if desired.
boundary_dockerstrg=5000

# Replace the below with your own docker storage backend values (in MB) if
# desired. The smaller value applies to platforms with less than
# $boundary_dockerstrg total bootflash space, the larger value for more than
# $boundary_dockerstrg of total bootflash space.
small_dockerstrg=300
large_dockerstrg=2000
```

## Failure to Pull Images from Docker Hub (509 Certificate Expiration Error Message)

**Problem:** The system fails to pull images from the Docker hub with an error message similar to the following:

```
root@switch# docker pull alpine
Using default tag: latest
Error response from daemon: Get https://registry-1.docker.io/v2/: x509: certificate has
expired or is not yet valid
```

**Possible Cause:** The system clock might not be set correctly.

**Solution:** Determine if the clock is set correctly or not:

```
root@n9k-2# sh clock
15:57:48.963 EST Thu Apr 25 2002
Time source is Hardware Calendar
```

Reset the clock, if necessary:

```
root@n9k-2# clock set hh:mm:ss { day month | month day } year
```

For example:

```
root@n9k-2# clock set 14:12:00 10 feb 2018
```

## Failure to Pull Images from Docker Hub (Client Timeout Error Message)

**Problem:** The system fails to pull images from the Docker hub with an error message similar to the following:

```

root@switch# docker pull alpine
Using default tag: latest
Error response from daemon: Get https://registry-1.docker.io/v2/: net/http: request canceled
while waiting for connection (Client.Timeout exceeded while awaiting headers)

```

**Possible Cause:** The proxies or DNS settings might not be set correctly.

**Solution:** Check the proxy settings and fix them, if necessary, then restart the Docker daemon:

```

root@switch# cat /etc/sysconfig/docker | grep proxy
#export http_proxy=http://proxy.esl.cisco.com:8080
#export https_proxy=http://proxy.esl.cisco.com:8080
root@switch# service docker [re]start

```

Check the DNS settings and fix them, if necessary, then restart the Docker daemon:

```

root@switch# cat /etc/resolv.conf
domain cisco.com #bleed
nameserver 171.70.168.183 #bleed
root@switch# # conf t
    Enter configuration commands, one per line. End with CNTL/Z.
    switch(config)# vrf context management
    switch(config-vrf)# ip domain-name ?
    WORD Enter the default domain (Max Size 64)

    switch(config-vrf)# ip name-server ?
    A.B.C.D Enter an IPv4 address
    A:B::C:D Enter an IPv6 address
root@switch# service docker [re]start

```

## Docker Daemon or Containers Not Running On Switch Reload or Switchover

**Problem:** The Docker daemon or containers do not run after you have performed a switch reload or switchover.

**Possible Cause:** The Docker daemon might not be configured to persist on a switch reload or switchover.

**Solution:** Verify that the Docker daemon is configured to persist on a switch reload or switchover using the `chkconfig` command, then start the necessary Docker containers using the `--restart unless-stopped` option. For example, to start an Alpine container:

```

root@switch# chkconfig --add docker
root@switch#
root@switch# chkconfig --list | grep docker
docker 0:off 1:off 2:on 3:on 4:on 5:on 6:off
root@switch# docker run -dit --restart unless-stopped alpine

```

## Resizing of Docker Storage Backend Fails

**Problem:** An attempt to resize the Docker backend storage failed.

**Possible Cause:** You might not have Guest Shell disabled.

**Solution:** Use the following command to determine if Guest Shell is disabled:

```

root@switch# losetup -a | grep dockerpart
root@n9k-2#

```

The command should not display any output if Guest Shell is disabled.

Enter the following command to disable the Guest Shell, if necessary:

```
switch# guestshell disable
```

If you still cannot resize the Docker backend storage, you can delete `/bootflash/dockerpart`, then adjust the `[small_]large_dockerstrg` in `/etc/sysconfig/docker`, then start Docker again to get a fresh Docker partition with the size that you want.

## Docker Container Doesn't Receive Incoming Traffic On a Port

**Problem:** The Docker container doesn't receive incoming traffic on a port.

**Possible Cause:** The Docker container might be using a netstack port instead of a kstack port.

**Solution:** Verify that any ephemeral ports that are used by Docker containers are within the kstack range. Otherwise any incoming packets can get sent to netstack for servicing and dropped.

```
switch# show socket local-port-range
Kstack local port range (15001 - 58000)
Netstack local port range (58001 - 63535) and nat port range (63536 - 65535)
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sockets local-port-range <start_port> <end_port>
switch# run bash sudo su -
root@switch# cat /proc/sys/net/ipv4/ip_local_port_range
15001 58000
root@switch#
```

## Unable to See Data Port And/Or Management Interfaces in Docker Container

**Problem:** You are unable to see the data port or management interfaces in the Docker container.

**Solution:**

- Verify that the Docker container is started in the host network namespace with all host namespaces mapped in using the `-v /var/run/netns:/var/run/netns:ro,rslave --network host` options.
- Once in the container, you will be in the management network namespace by default. You can use the `ip netns` utility to move to the default (`init`) network namespace, which has the data port interfaces. The `ip netns` utility might need to be installed in the container using `yum`, `apk`, or something similar.

## General Troubleshooting Tips

**Problem:** You have other issues with Docker containers that were not resolved using other troubleshooting processes.

**Solution:**

- Look for `dockerd` debug output in `/var/log/docker` for any clues as to what is wrong.
- Verify that your switch has 8 GB or more of RAM. Docker functionality is not supported on any switch that has less than 8 GB of RAM.





# CHAPTER 10

## NX-API

---

- [About NX-API, on page 83](#)
- [Using NX-API, on page 84](#)
- [XML and JSON Supported Commands, on page 92](#)

### About NX-API

On Cisco Nexus devices, command-line interfaces (CLIs) are run only on the device. NX-API improves the accessibility of these CLIs by making them available outside of the switch by using HTTP/HTTPS. You can use this extension to the existing Cisco Nexus CLI system on the Cisco Nexus 3500 Series devices. NX-API supports **show** commands, configurations, and Linux Bash.

NX-API supports JSON-RPC, JSON, and XML formats.

### Feature NX-API

- Feature NX-API is required to be enabled for access the device through sandbox.
- `| json` on the device internally uses python script to generate output.
- NX-API can be enabled either on http/https via ipv4:

```
BLR-VXLAN-NPT-CR-179# show nxapi
nxapi enabled
HTTP Listen on port 80
HTTPS Listen on port 443
BLR-VXLAN-NPT-CR-179#
```
- NX-API is internally spawning third-party NGINX process, which handler receive/send/processing of http requests/response:

```
nxapi certificate {httpsCRT |httpskey}
nxapi certificate enable
```
- NX-API Certificates can be enabled for https
- Default port for nginx to operate is 80/443 for http/https respectively. It can also be changed using the following CLI command:

```
nxapi {http|https} port port-number
```

## Transport

NX-API uses HTTP/HTTPS as its transport. CLIs are encoded into the HTTP/HTTPS POST body.

The NX-API backend uses the Nginx HTTP server. The Nginx process, and all of its children processes, are under Linux cgroup protection where the CPU and memory usage is capped. If the Nginx memory usage exceeds the cgroup limitations, the Nginx process is restarted and restored.



---

**Note** The Nginx process continues to run even after NX-API is disabled using the `no feature NXAPI` command. This is required for other management-related processes.

---

## Message Format



---

**Note**

- NX-API XML output presents information in a user-friendly format.
- NX-API XML does not map directly to the Cisco NX-OS NETCONF implementation.
- NX-API XML output can be converted into JSON or JSON-RPC.

---

## Security

NX-API supports HTTPS. All communication to the device is encrypted when you use HTTPS.

NX-API is integrated into the authentication system on the device. Users must have appropriate accounts to access the device through NX-API. NX-API uses HTTP basic authentication. All requests must contain the username and password in the HTTP header.



---

**Note** You should consider using HTTPS to secure your user's login credentials.

---

You can enable NX-API by using the **feature** manager CLI command. NX-API is disabled by default.

## Using NX-API

The commands, command type, and output type for the Cisco Nexus 3500 Series devices are entered using NX-API by encoding the CLIs into the body of a HTTP/HTTPS POST. The response to the request is returned in XML, JSON, or JSON-RPC output format.

You must enable NX-API with the **feature** manager CLI command on the device. By default, NX-API is disabled.

The following example shows how to configure and launch the NX-API Sandbox:

- Enable the management interface.

```
switch# conf t
switch(config)# interface mgmt 0
switch(config)# ip address 198.51.100.1/24
switch(config)# vrf context management
switch(config)# ip route 203.0.113.1/0 1.2.3.1
```

- Enable the NX-API **nxapi** feature.

```
switch# conf t
switch(config)# feature nxapi
```

The following example shows a request and its response in XML format:

#### Request:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ins_api>
  <version>0.1</version>
  <type>cli_show</type>
  <chunk>0</chunk>
  <sid>session1</sid>
  <input>show switchname</input>
  <output_format>xml</output_format>
</ins_api>
```

#### Response:

```
<?xml version="1.0"?>
<ins_api>
  <type>cli_show</type>
  <version>0.1</version>
  <sid>eoc</sid>
  <outputs>
    <output>
      <body>
        <hostname>switch</hostname>
      </body>
      <input>show switchname</input>
      <msg>Success</msg>
      <code>200</code>
    </output>
  </outputs>
</ins_api>
```

The following example shows a request and its response in JSON format:

#### Request:

```
{
  "ins_api": {
    "version": "0.1",
    "type": "cli_show",
    "chunk": "0",
    "sid": "session1",
    "input": "show switchname",
    "output_format": "json"
  }
}
```

#### Response:

```
{
  "ins_api": {
```

```

    "type": "cli_show",
    "version": "0.1",
    "sid": "eoc",
    "outputs": {
      "output": {
        "body": {
          "hostname": "switch"
        },
        "input": "show switchname",
        "msg": "Success",
        "code": "200"
      }
    }
  }
}

```

### Using the Management Interface for NX-API calls

It is recommended to use the management interface for NX-API calls.

When using non-management interface and a custom port for NX-API an entry should be made in the CoPP policy to prevent NX-API traffic from hitting the default copp entry which could unfavorably treat API traffic.



#### Note

It is recommended to use the management interface for NX-API traffic. If that is not possible and a custom port is used, the "copp-http" class should be updated to include the custom NX-API port.

The following example port 9443 is being used for NX-API traffic.

This port is added to the copp-system-acl-http ACL to allow it to be matched under the copp-http class resulting on 100 pps policing. (This may need to be increased in certain environments.)

```

!
ip access-list copp-system-acl-http
 10 permit tcp any any eq www
 20 permit tcp any any eq 443
 30 permit tcp any any eq 9443 <-----
!
class-map type control-plane match-any copp-http
 match access-group name copp-system-acl-http
!
!
policy-map type control-plane copp-system-policy
 class copp-http
  police pps 100
!

```

## NX-API Management Commands

You can enable and manage NX-API with the CLI commands listed in the following table.

**Table 4: NX-API Management Commands**

NX-API Management Command	Description
<b>feature nxapi</b>	Enables NX-API.

NX-API Management Command	Description
<b>no feature nxapi</b>	Disables NX-API.
<b>nxapi {http   https} port <i>port</i></b>	Specifies a port.
<b>no nxapi {http   https}</b>	Disables HTTP/HTTPS.
<b>show nxapi</b>	Displays port information.
<b>nxapi certificate {httpsert certfile   httpskey keyfile} <i>filename</i></b>	Specifies the upload of the following: <ul style="list-style-type: none"> <li>• HTTPS certificate when <code>httpsert</code> is specified.</li> <li>• HTTPS key when <code>httpskey</code> is specified.</li> </ul> <p>Example of HTTPS certificate:</p> <pre>nxapi certificate httpsert certfile bootflash:cert.crt</pre> <p>Example of HTTPS key:</p> <pre>nxapi certificate httpskey keyfile bootflash:privkey.key</pre>
<b>nxapi certificate enable</b>	Enables a certificate.

Following is an example of a successful upload of an HTTPS certificate:

```
switch(config)# nxapi certificate httpsert certfile certificate.crt
Upload done. Please enable. Note cert and key must match.
switch(config)# nxapi certificate enable
switch(config)#
```

Following is an example of a successful upload of an HTTPS key:

```
switch(config)# nxapi certificate httpskey keyfile bootflash:privkey.key
Upload done. Please enable. Note cert and key must match.
switch(config)# nxapi certificate enable
switch(config)#
```

In some situations, you might get an error message saying that the certificate is invalid:

```
switch(config)# nxapi certificate httpskey keyfile bootflash:privkey.key
Upload done. Please enable. Note cert and key must match.
switch(config)# nxapi certificate enable
Ngix certificate invalid.
switch(config)#
```

This might occur if the key file is encrypted. In that case, the key file must be decrypted before you can install it. You might have to go into Guest Shell to decrypt the key file, as shown in the following example:

```
switch(config)# guestshell
[b3456@guestshell ~]$
[b3456@guestshell bootflash]$ /bin/openssl rsa -in certfilename.net.pem -out clearkey.pem

Enter pass phrase for certfilename.net.pem:
writing RSA key
[b3456@guestshell bootflash]$
[b3456@guestshell bootflash]$ exit
switch(config)#
```

See [Guest Shell](#), on page 7 for more information on Guest Shell.

If this was the reason for the issue, you should now be able to successfully install the certificate:

```
switch(config)# nxapi certificate httpskey keyfile bootflash:privkey.key
Upload done. Please enable. Note cert and key must match.
switch(config)# nxapi certificate enable
switch(config)#
```

## Working With Interactive Commands Using NX-API

To disable confirmation prompts on interactive commands and avoid timing out with an error code 500, prepend interactive commands with **terminal dont-ask**. Use `;` to separate multiple interactive commands, where each `;` is surrounded with single blank characters.

Following are several examples of interactive commands where **terminal dont-ask** is used to avoid timing out with an error code 500:

```
terminal dont-ask ; reload module 21
terminal dont-ask ; system mode maintenance
```

## NX-API Request Elements

NX-API request elements are sent to the device in XML format or JSON format. The HTTP header of the request must identify the content type of the request.

You use the NX-API elements that are listed in the following table to specify a CLI command:

**Table 5: NX-API Request Elements**

NX-API Request Element	Description
version	Specifies the NX-API version.

NX-API Request Element	Description
<i>type</i>	<p>Specifies the type of command to be executed.</p> <p>The following types of commands are supported:</p> <ul style="list-style-type: none"> <li>• <b>cli_show</b> CLI <b>show</b> commands that expect structured output. If the command does not support XML output, an error message is returned.</li> <li>• <b>cli_show_ascii</b> CLI <b>show</b> commands that expect ASCII output. This aligns with existing scripts that parse ASCII output. Users are able to use existing scripts with minimal changes.</li> <li>• <b>cli_conf</b> CLI configuration commands.</li> <li>• <b>bash</b> Bash commands. Most non-interactive Bash commands are supported by NX-API.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Each command is only executable with the current user's authority.</li> <li>• The pipe operation is supported in the output when the message type is ASCII. If the output is in XML format, the pipe operation is not supported.</li> <li>• A maximum of 10 consecutive <b>show</b> commands are supported. If the number of <b>show</b> commands exceeds 10, the 11th and subsequent commands are ignored.</li> <li>• No interactive commands are supported.</li> </ul>

NX-API Request Element	Description						
<i>chunk</i>	<p>Some <b>show</b> commands can return a large amount of output. For the NX-API client to start processing the output before the entire command completes, NX-API supports output chunking for <b>show</b> commands.</p> <p>Enable or disable chunk with the following settings:</p> <table border="1" data-bbox="786 485 1477 596"> <tr> <td data-bbox="786 485 899 541">0</td> <td data-bbox="899 485 1477 541">Do not chunk output.</td> </tr> <tr> <td data-bbox="786 541 899 596">1</td> <td data-bbox="899 541 1477 596">Chunk output.</td> </tr> </table> <p><b>Note</b> Only <b>show</b> commands support chunking. When a series of <b>show</b> commands are entered, only the first command is chunked and returned.</p> <p>The output message format is XML. (XML is the default.) Special characters, such as &lt; or &gt;, are converted to form a valid XML message (&lt; is converted into &amp;lt; &gt; is converted into &amp;gt;).</p> <p>You can use XML SAX to parse the chunked output.</p> <p><b>Note</b> When chunking is enabled, the message format is limited to XML. JSON output format is not supported when chunking is enabled.</p>	0	Do not chunk output.	1	Chunk output.		
0	Do not chunk output.						
1	Chunk output.						
<i>sid</i>	<p>The session ID element is valid only when the response message is chunked. To retrieve the next chunk of the message, you must specify a <i>sid</i> to match the <i>sid</i> of the previous response message.</p>						
<i>input</i>	<p>Input can be one command or multiple commands. However, commands that belong to different message types should not be mixed. For example, <b>show</b> commands are cli_show message type and are not supported in cli_conf mode.</p> <p><b>Note</b> Except for <b>bash</b>, multiple commands are separated with ";". (The ; must be surrounded with single blank characters.)</p> <p>For <b>bash</b>, multiple commands are separated with ";". (The ; is <b>not</b> surrounded with single blank characters.)</p> <p>The following are examples of multiple commands:</p> <table border="1" data-bbox="786 1587 1477 1814"> <tr> <td data-bbox="786 1587 911 1665">cli_show</td> <td data-bbox="911 1587 1477 1665">show version ; show interface brief ; show vlan</td> </tr> <tr> <td data-bbox="786 1665 911 1740">cli_conf</td> <td data-bbox="911 1665 1477 1740">interface Eth4/1 ; no shut ; switchport</td> </tr> <tr> <td data-bbox="786 1740 911 1814">bash</td> <td data-bbox="911 1740 1477 1814">cd /bootflash;mkdir new_dir</td> </tr> </table>	cli_show	show version ; show interface brief ; show vlan	cli_conf	interface Eth4/1 ; no shut ; switchport	bash	cd /bootflash;mkdir new_dir
cli_show	show version ; show interface brief ; show vlan						
cli_conf	interface Eth4/1 ; no shut ; switchport						
bash	cd /bootflash;mkdir new_dir						

NX-API Request Element	Description				
<i>output_format</i>	The available output message formats are the following:				
	<table border="1"> <tr> <td data-bbox="824 344 1062 394">xml</td> <td data-bbox="1062 344 1515 394">Specifies output in XML format.</td> </tr> <tr> <td data-bbox="824 394 1062 453">json</td> <td data-bbox="1062 394 1515 453">Specifies output in JSON format.</td> </tr> </table>	xml	Specifies output in XML format.	json	Specifies output in JSON format.
	xml	Specifies output in XML format.			
json	Specifies output in JSON format.				
<p><b>Note</b> The Cisco Nexus 3500 Series CLI supports XML output, which means that the JSON output is converted from XML. The conversion is processed on the switch.</p> <p>To manage the computational overhead, the JSON output is determined by the amount of output. If the output exceeds 1 MB, the output is returned in XML format. When the output is chunked, only XML output is supported.</p> <p>The content-type header in the HTTP/HTTPS headers indicate the type of response format (XML or JSON).</p>					

## NX-API Response Elements

The NX-API elements that respond to a CLI command are listed in the following table:

**Table 6: NX-API Response Elements**

NX-API Response Element	Description
version	NX-API version.
type	Type of command to be executed.
sid	Session ID of the response. This element is valid only when the response message is chunked.
outputs	<p>Tag that encloses all command outputs.</p> <p>When multiple commands are in <code>cli_show</code> or <code>cli_show_ascii</code>, each command output is enclosed by a single output tag.</p> <p>When the message type is <code>cli_conf</code> or <code>bash</code>, there is a single output tag for all the commands because <code>cli_conf</code> and <code>bash</code> commands require context.</p>
output	<p>Tag that encloses the output of a single command output.</p> <p>For <code>cli_conf</code> and <code>bash</code> message types, this element contains the outputs of all the commands.</p>
input	Tag that encloses a single command that was specified in the request. This element helps associate a request input element with the appropriate response output element.
body	Body of the command response.

NX-API Response Element	Description
code	Error code returned from the command execution.  NX-API uses standard HTTP error codes as described by the Hypertext Transfer Protocol (HTTP) Status Code Registry ( <a href="http://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml">http://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml</a> ).
msg	Error message associated with the returned error code.

## About JSON (JavaScript Object Notation)

JSON is a light-weight text-based open standard designed for human-readable data and is an alternative to XML. JSON was originally designed from JavaScript, but it is language-independent data format. The JSON/CLI Execution is currently supported in Nexus 3500.



**Note** The NX-API/JSON functionality is now available on the Cisco Nexus 3500 Series platform.

The two primary Data Structures that are supported in some way by nearly all modern programming languages are as follows:

- Ordered List :: Array
- Unordered List (Name/Value pair) :: Objects

JSON/JSON-RPC/XML output for a show command can also be accessed via sandbox.

## CLI Execution

### Show\_Command | json

#### Example Code

```
BLR-VXLAN-NPT-CR-179# show cdp neighbors | json
{"TABLE_cdp_neighbor_brief_info": {"ROW_cdp_neighbor_brief_info": [{"ifindex": "83886080", "device_id": "SW-SPARSHA-SAVBU-F10", "intf_id": "mgmt0", "ttl": "148", "capability": ["switch", "IGMP_cnd_filtering"], "platform_id": "cisco WS-C2960 S-48TS-L", "port_id": "GigabitEthernet1/0/24"}, {"ifindex": "436207616", "device_id": "BLR-VXLAN-NPT-CR-178 (FOC1745R01W)", "intf_id": "Ethernet1/1", "ttl": "166", "capability": ["router", "switch", "IGMP_cnd_filtering", "Supports-STP-Dispute"], "platform_id": "N3K-C3132Q-40G", "port_id": "Ethernet1/1"}]}}
BLR-VXLAN-NPT-CR-179#
```

## XML and JSON Supported Commands

The NX-OS supports redirecting the standard output of various **show** commands in the following structured output formats:

- XML
- JSON
- JSON Pretty, which makes the standard block of JSON-formatted output easier to read

Converting the standard NX-OS output to JSON, JSON Pretty, or XML format occurs on the NX-OS CLI by "piping" the output to a JSON or XML interpreter. For example, you can issue the **show ip access** command with the logical pipe (|) and specify JSON, JSON Pretty, or XML, and the NX-OS command output will be properly structured and encoded in that format. This feature enables programmatic parsing of the data and supports streaming data from the switch through software streaming telemetry. Most commands in Cisco NX-OS support JSON, JSON Pretty, and XML output.

Selected examples of this feature follow.

## Examples of XML and JSON Output

This example shows how to display the unicast and multicast routing entries in hardware tables in JSON format:

```
switch(config)# show hardware profile status | json
{"total_lpm": ["8191", "1024"], "total_host": "8192", "max_host4_limit": "4096",
 "max_host6_limit": "2048", "max_mcast_limit": "2048", "used_lpm_total": "9", "u
sed_v4_lpm": "6", "used_v6_lpm": "3", "used_v6_lpm_128": "1", "used_host_lpm_tot
al": "0", "used_host_v4_lpm": "0", "used_host_v6_lpm": "0", "used_mcast": "0", "
used_mcast_oif1": "2", "used_host_in_host_total": "13", "used_host4_in_host": "1
2", "used_host6_in_host": "1", "max_ecmp_table_limit": "64", "used_ecmp_table":
"0", "mfib_fd_status": "Disabled", "mfib_fd_maxroute": "0", "mfib_fd_count": "0"
}
switch(config)#
```

This example shows how to display the unicast and multicast routing entries in hardware tables in XML format:

```
switch(config)# show hardware profile status | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0:fib">
  <nf:data>
    <show>
      <hardware>
        <profile>
          <status>
            <_XML_OPT_Cmd_dynamic_tcam_status>
              <_XML_OPT_Cmd_dynamic_tcam_status__readonly__>
                <_readonly__>
                  <total_lpm>8191</total_lpm>
                  <total_host>8192</total_host>
                  <total_lpm>1024</total_lpm>
                  <max_host4_limit>4096</max_host4_limit>
                  <max_host6_limit>2048</max_host6_limit>
                  <max_mcast_limit>2048</max_mcast_limit>
                  <used_lpm_total>9</used_lpm_total>
                  <used_v4_lpm>6</used_v4_lpm>
                  <used_v6_lpm>3</used_v6_lpm>
                  <used_v6_lpm_128>1</used_v6_lpm_128>
                  <used_host_lpm_total>0</used_host_lpm_total>
                  <used_host_v4_lpm>0</used_host_v4_lpm>
                  <used_host_v6_lpm>0</used_host_v6_lpm>
                  <used_mcast>0</used_mcast>
                  <used_mcast_oif1>2</used_mcast_oif1>
                  <used_host_in_host_total>13</used_host_in_host_total>
                  <used_host4_in_host>12</used_host4_in_host>
                  <used_host6_in_host>1</used_host6_in_host>
                </_readonly__>
              </_XML_OPT_Cmd_dynamic_tcam_status__readonly__>
            </_XML_OPT_Cmd_dynamic_tcam_status>
          </status>
        </profile>
      </hardware>
    </show>
  </nf:data>
</nf:rpc-reply>
```

```

        <max_ecmp_table_limit>64</max_ecmp_table_limit>
        <used_ecmp_table>0</used_ecmp_table>
        <mfib_fd_status>Disabled</mfib_fd_status>
        <mfib_fd_maxroute>0</mfib_fd_maxroute>
        <mfib_fd_count>0</mfib_fd_count>
    </__readonly__>
</__XML__OPT_Cmd_dynamic_tcam_status__readonly__>
</__XML__OPT_Cmd_dynamic_tcam_status>
</status>
</profile>
</hardware>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```

This example shows how to display LLDP timers configured on the switch in JSON format:

```

switch(config)# show lldp timers | json
{"ttl": "120", "reinit": "2", "tx_interval": "30", "tx_delay": "2", "hold_mplier": "4", "notification_interval": "5"}
switch(config)#

```

This example shows how to display LLDP timers configured on the switch in XML format:

```

switch(config)# show lldp timers | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:lldp">
  <nf:data>
    <show>
      <lldp>
        <timers>
          <__XML__OPT_Cmd_lldp_show_timers__readonly__>
            <__readonly__>
              <ttl>120</ttl>
              <reinit>2</reinit>
              <tx_interval>30</tx_interval>
              <tx_delay>2</tx_delay>
              <hold_mplier>4</hold_mplier>
              <notification_interval>5</notification_interval>
            </__readonly__>
          </__XML__OPT_Cmd_lldp_show_timers__readonly__>
        </timers>
      </lldp>
    </show>
  </nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```



# CHAPTER 11

## NX-API Response Codes

- [Table of NX-API Response Codes, on page 95](#)

### Table of NX-API Response Codes

The following are the possible NX-API errors, error codes, and messages of an NX-API response.



**Note** The standard HTTP error codes are at the Hypertext Transfer Protocol (HTTP) Status Code Registry (<http://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>).

**Table 7: NX-API Response Codes**

NX-API Response	Code	Message
SUCCESS	200	Success.
CUST_OUTPUT_PIPED	204	Output is piped elsewhere due to request.
BASH_CMD_ERR	400	Input Bash command error.
CHUNK_ALLOW_ONE_CMD_ERR	400	Chunking only allowed to one command.
CLI_CLIENT_ERR	400	CLI execution error.
CLI_CMD_ERR	400	Input CLI command error.
IN_MSG_ERR	400	Request message is invalid.
NO_INPUT_CMD_ERR	400	No input command.
PERM_DENY_ERR	401	Permission denied.
CONF_NOT_ALLOW_SHOW_ERR	405	Configuration mode does not allow <b>show</b> .
SHOW_NOT_ALLOW_CONF_ERR	405	Show mode does not allow configuration.
EXCEED_MAX_SHOW_ERR	413	Maximum number of consecutive show commands exceeded. The maximum is 10.

MSG_SIZE_LARGE_ERR	413	Response size too large.
BACKEND_ERR	500	Backend processing error.
CREATE_CHECKPOINT_ERR	500	Error creating a checkpoint.
FILE_OPER_ERR	500	System internal file operation error.
LIBXML_NS_ERR	500	System internal LIBXML NS error.
LIBXML_PARSE_ERR	500	System internal LIBXML parse error.
LIBXML_PATH_CTX_ERR	500	System internal LIBXML path context error.
MEM_ALLOC_ERR	500	System internal memory allocation error.
SERVER_BUSY_ERR	500	Request is rejected because the server is busy.
USER_NOT_FOUND_ERR	500	User not found from input or cache.
XML_TO_JSON_CONVERT_ERR	500	XML to JSON conversion error.
BASH_CMD_NOT_SUPPORTED_ERR	501	Bash command not supported.
CHUNK_ALLOW_XML_ONLY_ERR	501	Chunking allows only XML output.
JSON_NOT_SUPPORTED_ERR	501	JSON not supported due to large amount of output.
MSG_TYPE_UNSUPPORTED_ERR	501	Message type not supported.
PIPE_OUTPUT_NOT_SUPPORTED_ERR	501	Pipe operation not supported.
PIPE_XML_NOT_ALLOWED_IN_INPUT	501	Pipe XML is not allowed in input.
RESP_BIG_JSON_NOT_ALLOWED_ERR	501	Response has large amount of output. JSON not supported.
STRUCT_NOT_SUPPORTED_ERR	501	Structured output unsupported.
ERR_UNDEFINED	600	Undefined.



# CHAPTER 12

## NX-API Developer Sandbox

- [NX-API Developer Sandbox: NX-OS Releases Prior to 9.2\(2\)](#), on page 97
- [NX-API Developer Sandbox: NX-OS Release 9.2\(2\) and Later](#), on page 102

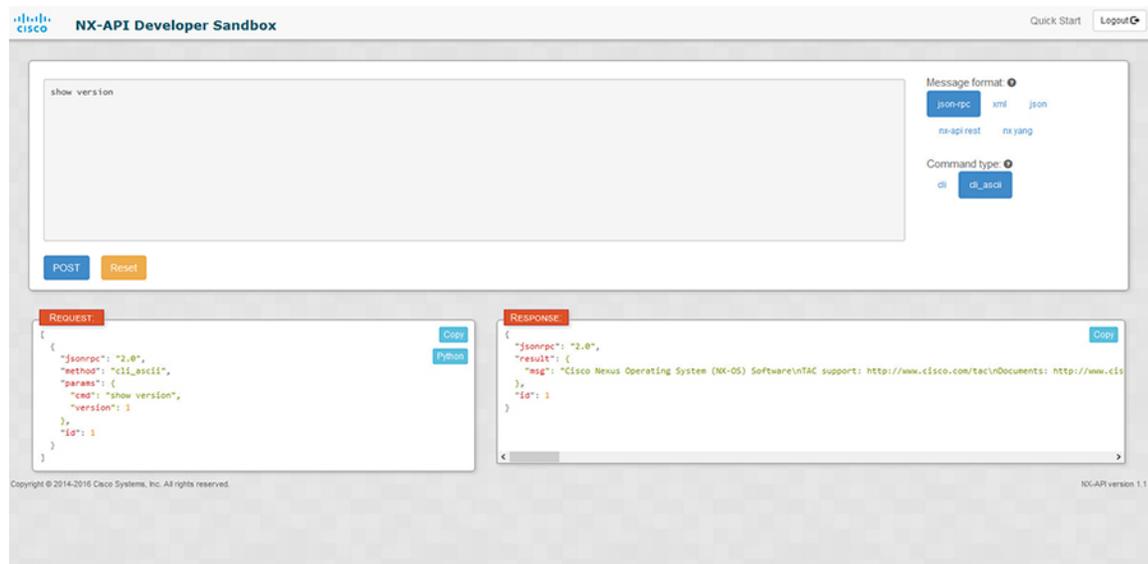
### NX-API Developer Sandbox: NX-OS Releases Prior to 9.2(2)

#### About the NX-API Developer Sandbox

The NX-API Developer Sandbox is a web form hosted on the switch. It translates NX-OS CLI commands into equivalent XML or JSON payloads, and converts NX-API REST payloads into their CLI equivalents.

The web form is a single screen with three panes — Command (top pane), Request, and Response — as shown in the figure.

**Figure 1: NX-API Developer Sandbox with Example Request and Output Response**



Controls in the Command pane allow you to choose a message format for a supported API, such as NX-API REST, and a command type, such as XML or JSON. The available command type options vary depending on the selected message format.

When you type or paste one or more CLI commands into the Command pane, the web form converts the commands into an API payload, checking for configuration errors, and displays the resulting payload in the Request pane. If you then choose to post the payload directly from the Sandbox to the switch, using the POST button in the Command pane, the Response pane displays the API response.

Conversely, when you type an NX-API REST designated name (DN) and payload into the Command pane and select the **nx-api rest** Message format and the **model** Command type, Developer Sandbox checks the payload for configuration errors, then the Response pane displays the equivalent CLIs.

## Guidelines and Limitations

Following are the guidelines and limitations for the Developer Sandbox:

- Clicking **POST** in the Sandbox commits the command to the switch, which can result in a configuration or state change.
- Some feature configuration commands are not available until their associated feature has been enabled.

## Configuring the Message Format and Command Type

The **Message Format** and **Command Type** are configured in the upper right corner of the Command pane (the top pane). For **Message Format**, choose the format of the API protocol that you want to use. The Developer Sandbox supports the following API protocols:

**Table 8: NX-OS API Protocols**

Protocol	Description
json-rpc	A standard lightweight remote procedure call (RPC) protocol that can be used to deliver NX-OS CLI commands in a JSON payload. The JSON-RPC 2.0 specification is outlined by <a href="http://jsonrpc.org">jsonrpc.org</a> .
xml	Cisco NX-API proprietary protocol for delivering NX-OS CLI or bash commands in an XML payload.
json	Cisco NX-API proprietary protocol for delivering NX-OS CLI or bash commands in a JSON payload.
nx-api rest	Cisco NX-API proprietary protocol for manipulating and reading managed objects (MOs) and their properties in the internal NX-OS data management engine (DME) model. For more information about the Cisco Nexus 3000 and 9000 Series NX-API REST SDK, see <a href="https://developer.cisco.com/site/cisco-nexus-nx-api-references/">https://developer.cisco.com/site/cisco-nexus-nx-api-references/</a> .
nx yang	The YANG ("Yet Another Next Generation") data modeling language for configuration and state data.

When the **Message Format** has been chosen, a set of **Command Type** options are presented just below the **Message Format** control. The **Command Type** setting can constrain the input CLI and can determine the **Request** and **Response** format. The options vary depending on the **Message Format** selection. For each **Message Format**, the following table describes the **Command Type** options:

Table 9: Command Types

Message format	Command type
json-rpc	<ul style="list-style-type: none"> <li>cli — show or configuration commands</li> <li>cli-ascii — show or configuration commands, output without formatting</li> </ul>
xml	<ul style="list-style-type: none"> <li>cli_show — show commands. If the command does not support XML output, an error message will be returned.</li> <li>cli_show_ascii — show commands, output without formatting</li> <li>cli_conf — configuration commands. Interactive configuration commands are not supported.</li> <li>bash — bash commands. Most non-interactive bash commands are supported.</li> </ul> <p><b>Note</b> The bash shell must be enabled in the switch.</p>
json	<ul style="list-style-type: none"> <li>cli_show — show commands. If the command does not support XML output, an error message will be returned.</li> <li>cli_show_ascii — show commands, output without formatting</li> <li>cli_conf — configuration commands. Interactive configuration commands are not supported.</li> <li>bash — bash commands. Most non-interactive bash commands are supported.</li> </ul> <p><b>Note</b> The bash shell must be enabled in the switch.</p>
nx-api rest	<ul style="list-style-type: none"> <li>cli — configuration commands</li> <li>model — DN and corresponding payload.</li> </ul>
nx yang	<ul style="list-style-type: none"> <li>json — JSON structure is used for payload</li> <li>xml — XML structure is used for payload</li> </ul>

### Output Chunking

In order to handle large show command output, some NX-API message formats support output chunking for show commands. In this case, an **Enable chunk mode** checkbox appears below the **Command Type** control along with a session ID (**SID**) type-in box.

When chunking is enabled, the response is sent in multiple "chunks," with the first chunk sent in the immediate command response. In order to retrieve the next chunk of the response message, you must send an NX-API request with **SID** set to the session ID of the previous response message.

## Using the Developer Sandbox

### Using the Developer Sandbox to Convert CLI Commands to Payloads



**Tip** Online help is available by clicking **Quick Start** in the upper right corner of the Sandbox window. Additional details, such as response codes and security methods, can be found in the NX-API CLI chapter. Only configuration commands are supported.

**Step 1** Configure the **Message Format** and **Command Type** for the API protocol you want to use.

For detailed instructions, see [Configuring the Message Format and Command Type, on page 98](#).

**Step 2** Type or paste NX-OS CLI configuration commands, one command per line, into the text entry box in the top pane.

You can erase the contents of the text entry box (and the **Request** and **Response** panes) by clicking **Reset** at the bottom of the top pane.

**Step 3** Click the **Convert** at the bottom of the top pane.

If the CLI commands contain no configuration errors, the payload appears in the **Request** pane. If errors are present, a descriptive error message appears in the **Response** pane.

The screenshot displays the NX-API Developer Sandbox interface. At the top left is the Cisco logo and the title "NX-API Developer Sandbox". On the top right are "Quick Start" and "Logout" links. The main area is divided into several sections:

- Request pane:** A large text area containing a JSON payload:

```
api/mo/sys.json
{
  "topSystem": {
    "attributes": {
      "name": "REST2CLI"
    }
  }
}
```

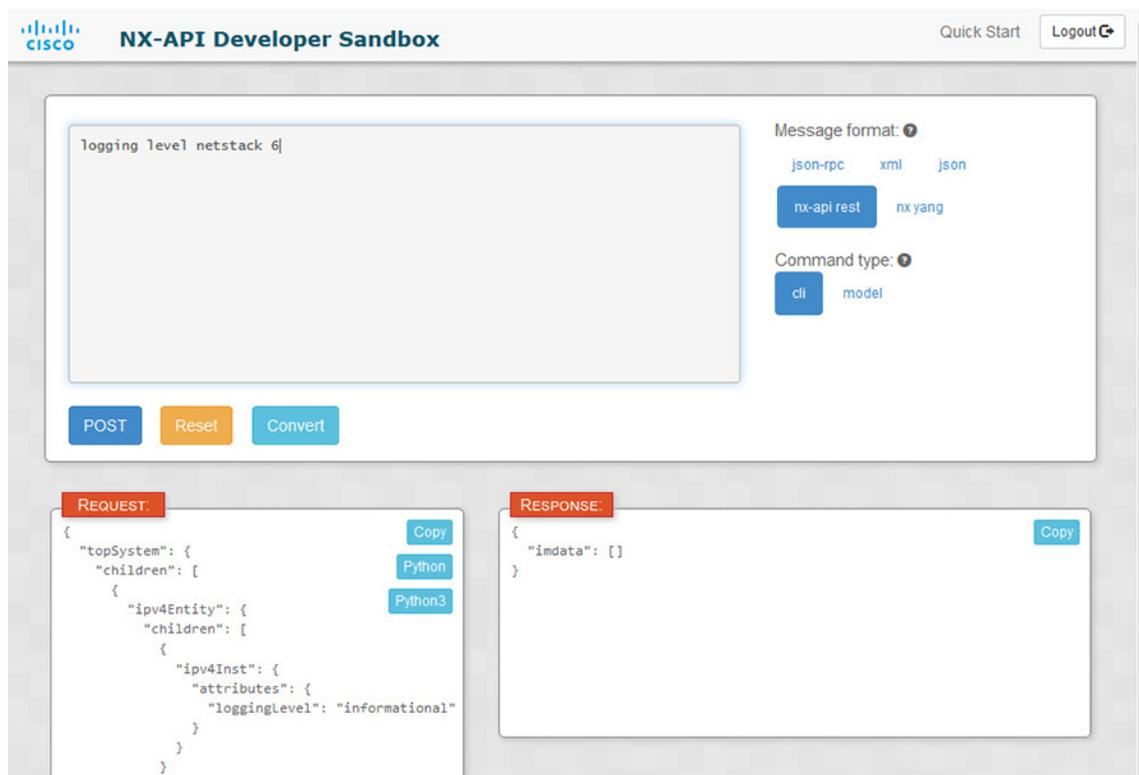
Below this text area are "Convert" and "Reset" buttons.
- Message format:** A dropdown menu with options "json-rpc", "xml", and "json". The "nx-api rest" option is selected.
- Command type:** A dropdown menu with options "cli" and "model". The "model" option is selected.
- CLI pane:** A text area with a red header "CLI:" containing the text "hostname REST2CLI" and a "Copy" button.
- ERROR pane:** A text area with a red header "ERROR:" and a "Copy" button. It is currently empty.

At the bottom left, there is a status bar that says "Waiting for bam.nr-data.net...". At the bottom right, there is a copyright notice: "Copyright © 2014-2016 Cisco Systems, Inc. All rights reserved." and the version "NX-API version 1.1".

**Step 4** When a valid payload is present in the **Request** pane, you can click **POST** to send the payload as an API call to the switch.

The response from the switch appears in the **Response** pane.

**Warning** Clicking **POST** commits the command to the switch, which can result in a configuration or state change.



**Step 5** You can copy the contents of the **Request** or **Response** pane to the clipboard by clicking **Copy** in the pane.

**Step 6** You can obtain a Python implementation of the request on the clipboard by clicking **Python** in the **Request** pane.

## NX-API Developer Sandbox: NX-OS Release 9.2(2) and Later

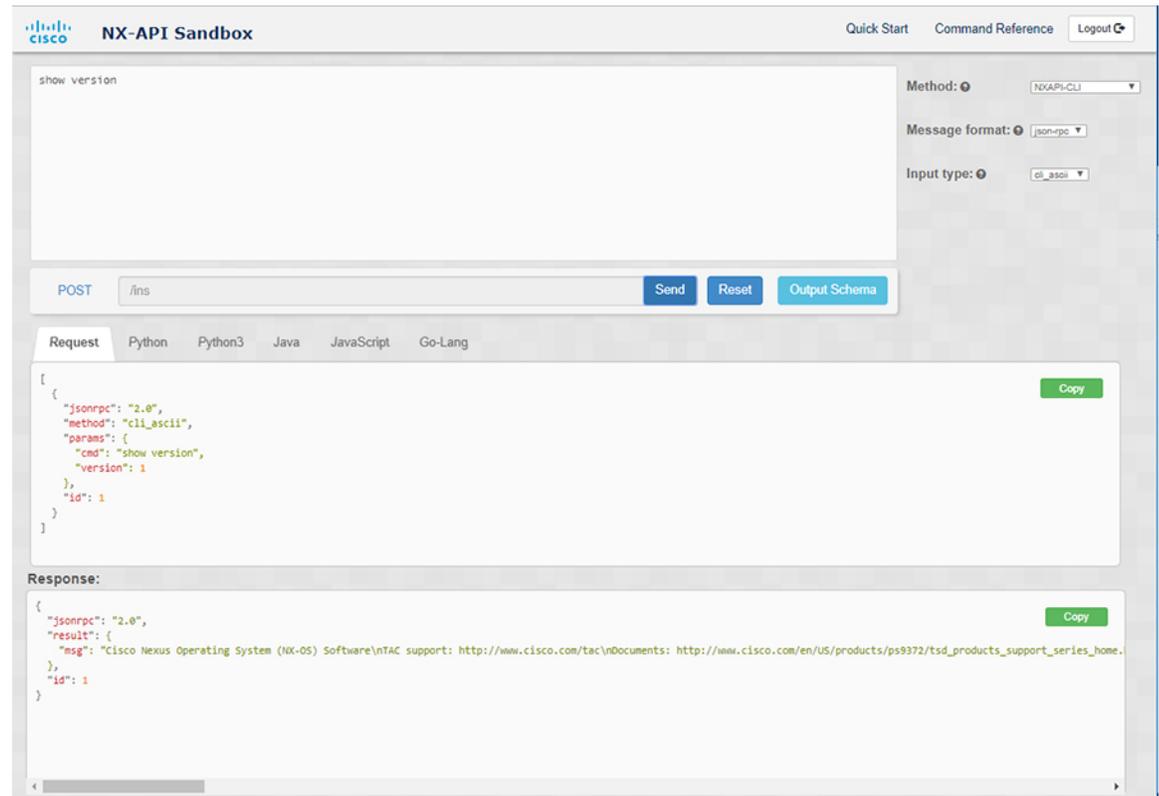
### About the NX-API Developer Sandbox

The Cisco NX-API Developer Sandbox is a web form hosted on the switch. It translates NX-OS CLI commands into equivalent XML or JSON payloads and converts NX-API REST payloads into their CLI equivalents.

The web form is a single screen with three panes — Command (top pane), Request (middle pane), and Response (bottom pane) — as shown in the figure below. The designated name (DN) field is located between the Command and Request panes (seen in the figure below located between the **POST** and **Send** options).

The Request pane also has a series of tabs. Each tab represents a different language: **Python**, **Python3**, **Java**, **JavaScript**, and **Go-Lang**. Each tab enables you to view the request in the respective language. For example, after converting CLI commands into an XML or JSON payload, click the **Python** tab to view the request in Python, which you can use to create scripts.

Figure 2: NX-API Developer Sandbox with Example Request and Output Response



Controls in the Command pane enable you to choose a supported API, such as NX-API REST, an input type, such as model (payload) or CLI, and a message format, such as XML or JSON. The available options vary depending on the chosen method.

When you choose the NX-API-REST (DME) method, type or paste one or more CLI commands into the Command pane, and click **Convert**, the web form converts the commands into a REST API payload, checking for configuration errors, and displays the resulting payload in the Request pane. If you then choose to post the payload directly from the sandbox to the switch (by choosing the **POST** option and clicking **SEND**), the Response pane displays the API response. For more information, see [Using the Developer Sandbox to Convert CLI Commands to REST Payloads, on page 106](#)

Conversely, the Cisco NX-API Developer Sandbox checks the payload for configuration errors then displays the equivalent CLIs in the Response pane. For more information, see [Using the Developer Sandbox to Convert from REST Payloads to CLI Commands, on page 109](#)

## Guidelines and Limitations

Following are the guidelines and limitations for the Developer Sandbox:

- Clicking **Send** in the Sandbox commits the command to the switch, which can result in a configuration or state change.
- Some feature configuration commands are not available until their associated feature has been enabled.

- Using Sandbox to convert with DN is supported only for finding the DN of a CLI config. Any other workflow, for example, using DME to convert DN for CLI configuration commands is not supported.
- The Command pane (the top pane) supports a maximum of 10,000 individual lines of input.

## Configuring the Message Format and Input Type

The **Method**, **Message format**, and **Input type** are configured in the upper right corner of the Command pane (the top pane). For **Method**, choose the format of the API protocol that you want to use. The Cisco NX-API Developer Sandbox supports the following API protocols:

*Table 10: NX-OS API Protocols*

Protocol	Description
NXAPI-CLI	Cisco NX-API proprietary protocol for delivering NX-OS CLI or bash commands in an XML or a JSON payload.
NXAPI-REST (DME)	<p>Cisco NX-API proprietary protocol for manipulating and reading managed objects (MOs) and their properties in the internal NX-OS data management engine (DME) model. The NXAPI-REST (DME) protocol displays a drop-down list that enables you to choose from the following methods:</p> <ul style="list-style-type: none"> <li>• <b>POST</b></li> <li>• <b>GET</b></li> <li>• <b>PUT</b></li> <li>• <b>DELETE</b></li> </ul> <p>For more information about the Cisco Nexus 3000 and 9000 Series NX-API REST SDK, see <a href="https://developer.cisco.com/site/cisco-nexus-nx-api-references/">https://developer.cisco.com/site/cisco-nexus-nx-api-references/</a>.</p>
RESTCONF (Yang)	<p>The YANG ("Yet Another Next Generation") data modeling language for configuration and state data.</p> <p>The RESTCONF (Yang) protocol displays a drop-down list that enables you to choose from the following methods:</p> <ul style="list-style-type: none"> <li>• <b>POST</b></li> <li>• <b>GET</b></li> <li>• <b>PUT</b></li> <li>• <b>PATCH</b></li> <li>• <b>DELETE</b></li> </ul>

When you choose the **Method**, a set of **Message format** or **Input type** options are displayed in a drop-down list. The **Message format** can constrain the input CLI and determine the **Request** and **Response** format. The options vary depending on the **Method** you choose.

The following table describes the **Input/Command type** options for each **Message format**:

Table 11: Command Types

Method	Message format	Input/Command type
NXAPI-CLI	json-rpc	<ul style="list-style-type: none"> <li>cli — show or configuration commands</li> <li>cli-ascii — show or configuration commands, output without formatting</li> <li>cli-array — show commands. Similar to cli, but with cli_array, data is returned as a list of one element, or an array, within square brackets, [ ].</li> </ul>
NXAPI-CLI	xml	<ul style="list-style-type: none"> <li>cli_show — show commands. If the command does not support XML output, an error message will be returned.</li> <li>cli_show_ascii — show commands, output without formatting</li> <li>cli_conf — configuration commands. Interactive configuration commands are not supported.</li> <li>bash — bash commands. Most non-interactive bash commands are supported.</li> </ul> <p><b>Note</b> The bash shell must be enabled in the switch.</p>
NXAPI-CLI	json	<ul style="list-style-type: none"> <li>cli_show — show commands. If the command does not support XML output, an error message will be returned.</li> <li>cli_show_array — show commands. Similar to cli_show, but with cli_show_array, data is returned as a list of one element, or an array, within square brackets [ ].</li> <li>cli_show_ascii — show commands, output without formatting</li> <li>cli_conf — configuration commands. Interactive configuration commands are not supported.</li> <li>bash — bash commands. Most non-interactive bash commands are supported.</li> </ul> <p><b>Note</b> The bash shell must be enabled in the switch.</p>
NXAPI-REST (DME)		<ul style="list-style-type: none"> <li>cli — CLI to model conversion</li> <li>model — Model to CLI conversion.</li> </ul>

Method	Message format	Input/Command type
RESTCONF (Yang)	<ul style="list-style-type: none"> <li>• json — JSON structure is used for payload</li> <li>• xml — XML structure is used for payload</li> </ul>	

### Output Chunking

In order to handle large show command output, some NX-API message formats support output chunking for show commands. In this case, an **Enable chunk mode** check box appears below the **Command Type** control along with a session ID (**SID**) type-in box.

When chunking is enabled, the response is sent in multiple "chunks," with the first chunk sent in the immediate command response. In order to retrieve the next chunk of the response message, you must send an NX-API request with **SID** set to the session ID of the previous response message.

## Using the Developer Sandbox

You can use the Cisco NX-API Developer Sandbox to make multiple conversions, including the following:

### Using the Developer Sandbox to Convert CLI Commands to REST Payloads



#### Tip

- Online help is available by clicking the help icons (?) next to the field names located in the upper-right corner of the Cisco NX-API Developer Sandbox window.
- For additional details, such as response codes and security methods, see the *NX-API CLI* chapter.
- Only configuration commands are supported.

The Cisco NX-API Developer Sandbox enables you to convert CLI commands to REST payloads.

**Step 1** Click the **Method** drop-down list and choose **NXAPI-REST (DME)**.

The **Input** type drop-down list appears.

**Step 2** Click the **Input** type drop-down list and choose **cli**.

**Step 3** Type or paste NX-OS CLI configuration commands, one command per line, into the text entry box in the top pane.

You can erase the contents of the text entry box (and the **Request** and **Response** panes) by clicking **Reset** at the bottom of the top pane.

Enter DME payload here.

Method:  NXAPI-REST (DME)

Input type:  model

/api/mo/sys.json

Send Reset Convert

Request Python Python3 Java JavaScript Go-Lang

Copy

Response:

Copy

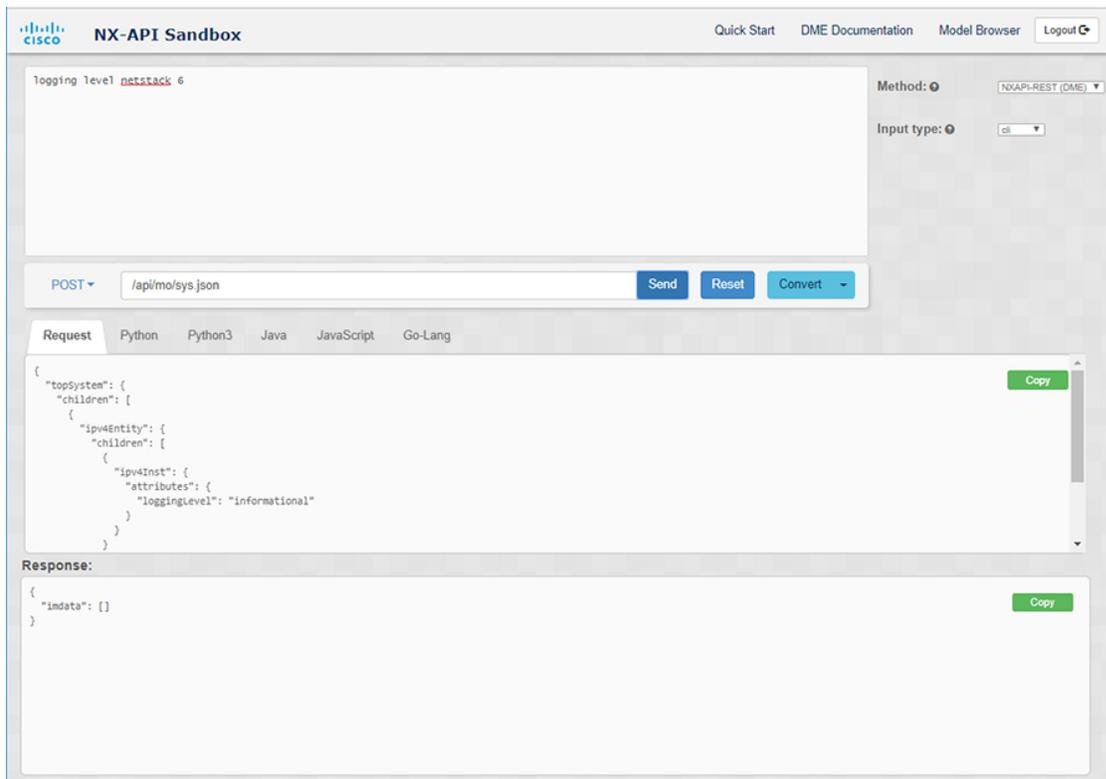
**Step 4** Click **Convert**.

If the CLI commands contain no configuration errors, the payload appears in the **Request** pane. If errors are present, a descriptive error message appears in the **Response** pane.

**Step 5** (Optional) To send a valid payload as an API call to the switch, click **Send**.

The response from the switch appears in the **Response** pane.

**Warning** Clicking **Send** commits the command to the switch, which can result in a configuration or state change.



**Step 6** (Optional) To obtain the DN for an MO in the payload:

- a. From the **Request** pane, choose **POST**.
- b. Click the **Convert** drop-down list and choose **Convert (with DN)**.

The payload appears with a **dn** field that contains the DN that corresponds to each MO in the payload.

**Step 7** (Optional) To overwrite the current configuration with a new configuration:

- a. Click the **Convert** drop-down list and choose **Convert (for Replace)**. The **Request** pane displays a payload with a **status** field set to **replace**.
- b. From the **Request** pane, choose **POST**.
- c. Click **Send**.

The current configuration is replaced with the posted configuration. For example, if you start with the following configuration:

```
interface eth1/2
  description test
  mtu 1501
```

Then use **Convert (for Replace)** to POST the following configuration:

```
interface eth1/2
  description testForcr
```

The `mtu` configuration is removed and only the new description (`testForcr`) is present under the interface. This change is confirmed when entering `show running-config`.

**Step 8** (Optional) To copy the contents of a pane, such as the **Request** or **Response** pane, click **Copy**. The contents of the respective pane is copied to the clipboard.

**Step 9** (Optional) To convert the request into an of the formats listed below, click on the appropriate tab in the **Request** pane:

- **Python**
- **Python3**
- **Java**
- **JavaScript**
- **Go-Lang**

---

## Using the Developer Sandbox to Convert from REST Payloads to CLI Commands

The Cisco NX-API Developer Sandbox enables you to convert REST payloads to corresponding CLI commands. This option is only available for the NXAPI-REST (DME) method.

**Tip**

- Online help is available by clicking help icons (?) next to the Cisco NX-API Developer Sandbox field names. Click a help icon get information about the respective field.

For additional details, such as response codes and security methods, see the chapter *NX-API CLI*.

- The top-right corner of the Cisco NX-API Developer Sandbox contains links for additional information. The links that appear depend on the **Method** you choose. The links that appear for the NXAPI-REST (DME) method:

- **NX-API References**—Enables you to access additional NX-API documentation.
- **DME Documentation**—Enables you to access the NX-API DME Model Reference page.
- **Model Browser**—Enables you to access Visore, the Model Browser. Note that you might have to manually enter the IP address for your switch to access the Visore page:

`https://management-ip-address/visore.html`.

---

**Step 1** Click the **Method** drop-down list and choose **NXAPI-REST (DME)**.

**Example:**

The screenshot shows the NX-API Sandbox interface. At the top, there is a navigation bar with the Cisco logo, the title "NX-API Sandbox", and links for "Quick Start", "DME Documentation", "Model Browser", and "Logout". Below the navigation bar is a large text area for entering the DME payload. To the right of this area are two dropdown menus: "Method" set to "NX-API-REST (DME)" and "Input type" set to "model". Below the text area is a text input field containing the path "/api/mo/sys.json", followed by "Send", "Reset", and "Convert" buttons. Below the input field is a tabbed interface with tabs for "Request", "Python", "Python3", "Java", "JavaScript", and "Go-Lang". The "Request" tab is active, showing a large empty text area with a "Copy" button in the top right corner. Below the "Request" tab is a "Response:" section, also with a large empty text area and a "Copy" button in the top right corner.

**Step 2** Click the **Input Type** drop-down list and choose **model**.

**Step 3** Enter the designated name (DN) that corresponds to the payload in the field above the Request pane.

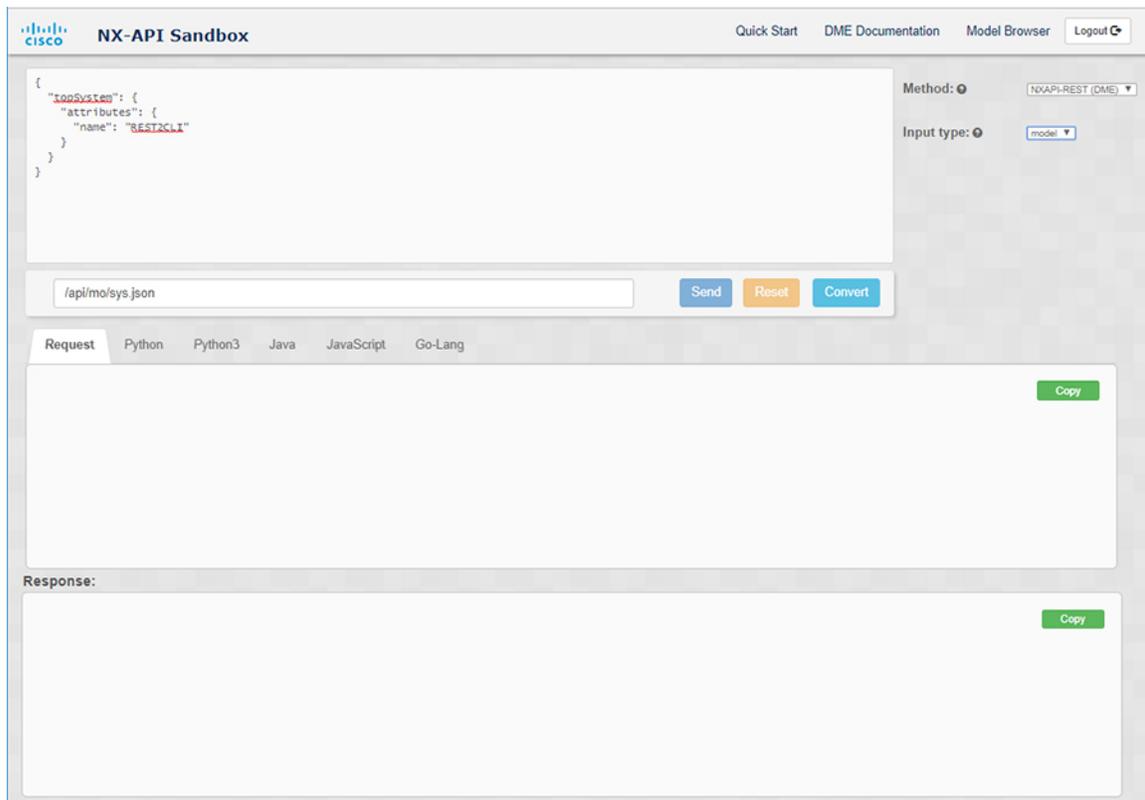
**Step 4** Enter the payload in the Command pane.

**Step 5** Click **Convert**.

**Example:**

For this example, the DN is `/api/mo/sys.json` and the NX-API REST payload is:

```
{
  "topSystem": {
    "attributes": {
      "name": "REST2CLI"
    }
  }
}
```



When you click on the **Convert** button, the CLI equivalent appears in the **CLI** pane as shown in the following image.

The screenshot displays the Cisco NX-API Sandbox interface. At the top left is the Cisco logo and the text "NX-API Sandbox". Navigation links include "Quick Start", "DME Documentation", "Model Browser", and "Logout".

The main area contains a code editor with a REST payload:
 

```
{
  "topSystem": {
    "attributes": {
      "name": "REST2CLI"
    }
  }
}
```

 To the right of the editor are controls for "Method" (set to "NX-API-REST (DME)") and "Input type" (set to "model"). Below the editor is a text input field containing "/api/mo/sys.json" and three buttons: "Send", "Reset", and "Convert".

Below the editor, there are tabs for "Request", "Python", "Python3", "Java", "JavaScript", and "Go-Lang". The "Request" tab is active, showing the converted CLI command: "hostname REST2CLI". A green "Copy" button is located to the right of the command.

Below the request, there is a "Response:" section with a large empty text area and a green "Copy" button to its right.

**Note** The Cisco NX-API Developer Sandbox cannot convert all payloads into equivalent CLIs, even if the sandbox converted the CLIs to NX-API REST payloads. The following is a list of possible sources of error that can prevent a payload from completely converting to CLI commands:

**Table 12: Sources of REST2CLI Errors**

Payload Issue	Result
<p>The payload contains an attribute that does not exist in the MO.</p> <p>Example:</p> <pre>api/mo/sys.json {   "topSystem": {     "children": [       {         "interfaceEntity": {           "children": [             {               "l1PhysIf": {                 "attributes": {                   "id": "eth1/1",                   "fakeattribute": "totallyFake"                 }               }             }           ]         }       }     ]   } }</pre>	<p>The <b>Error</b> pane will return an error related to the attribute.</p> <p>Example:</p> <p><b>CLI</b></p> <p><b>Error</b> unknown attribute 'fakeattribute' in element 'l1PhysIf'</p>
<p>The payload includes MOs that aren't yet supported for conversion:</p> <p>Example:</p> <pre>api/mo/sys.json {   "topSystem": {     "children": [       {         "dhcpEntity": {           "children": [             {               "dhcpInst": {                 "attributes": {                   "SnoopingEnabled": "yes"                 }               }             }           ]         }       }     ]   } }</pre>	<p>The <b>Error</b> Pane will return an error related to the unsupported MO.</p> <p>Example:</p> <p><b>CLI</b></p> <p><b>Error</b> The entire subtree of "sys/dhcp" is not converted.</p>

## Using the Developer Sandbox to Convert from RESTCONF to json or XML



### Tip

- Online help is available by clicking the help icon (?) in the upper-right corner of the Cisco NX-API Developer Sandbox window.
- Click on the **Yang Documentation** link in the upper right corner of the Sandbox window to go to the Model Driven Programmability with Yang page.
- Click on the **Yang Models** link in the upper right corner of the Sandbox window to access the YangModels GitHub site.

**Step 1** Click the **Method** drop-down list and choose **RESTCONF (Yang)**.

### Example:

**Step 2** Click **Message format** and choose either **json** or **xml**.

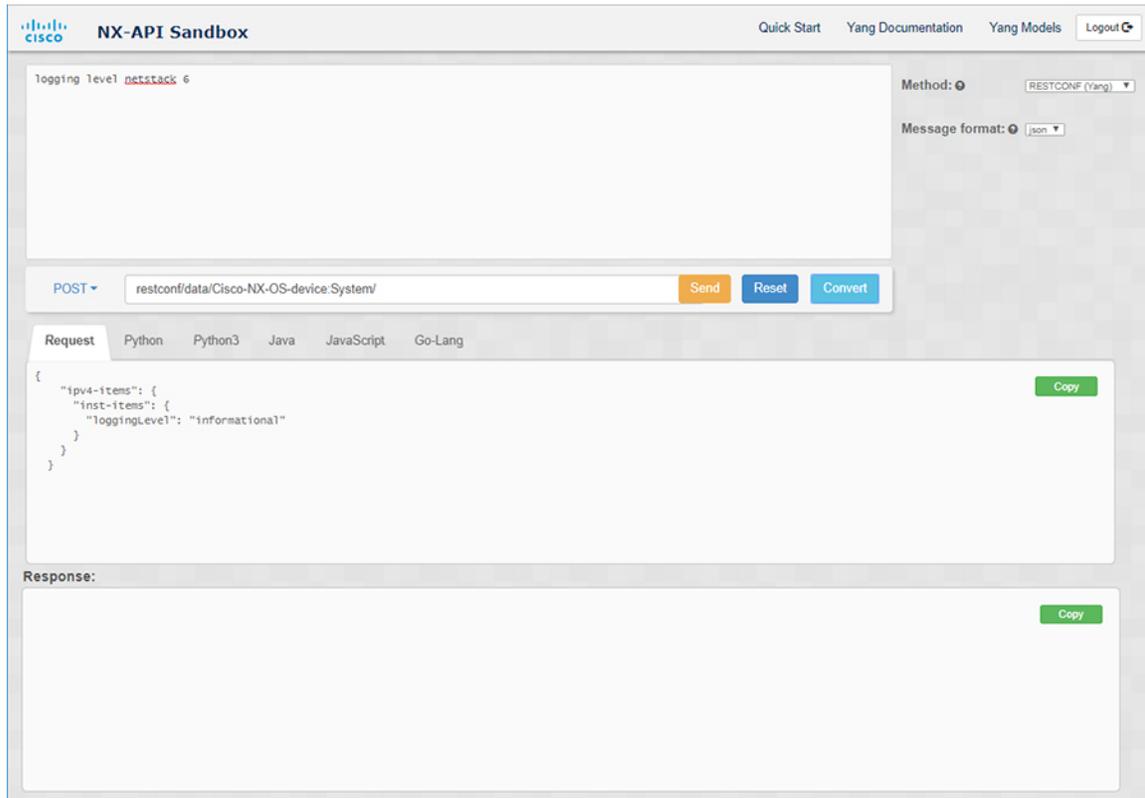
**Step 3** Enter a command in the text entry box in the top pane.

**Step 4** Choose a message format.

**Step 5** Click **Convert**.

### Example:

For this example, the command is `logging level netstack 6` and the message format is json:



The screenshot shows the NX-API Developer Sandbox interface. At the top, there is a navigation bar with the Cisco logo, "NX-API Sandbox", and links for "Quick Start", "Yang Documentation", "Yang Models", and "Logout". The main area is divided into several sections:

- Command Input:** A text area containing the command `Logging level netstack 6`.
- Method:** A dropdown menu set to "RESTCONF (Yang)".
- Message format:** A dropdown menu set to "json".
- Request:** A dropdown menu set to "POST" and a text input field containing the URL `restconf/data/Cisco-NX-OS-device:System/`. Below this are "Send", "Reset", and "Convert" buttons.
- Request Body:** A text area showing the JSON request body: 

```
{  "ipv4-items": {    "inst-items": {      "loggingLevel": "informational"    }  }}
```

 A "Copy" button is located to the right of the text area.
- Response:** A text area labeled "Response:" which is currently empty. A "Copy" button is located to the right of the text area.

**Example:**

For this example, the command is `logging level netstack 6` and the message format is xml:

The screenshot shows the NX-API Sandbox interface. At the top, there is a header with the Cisco logo and the text "NX-API Sandbox". To the right of the header are links for "Quick Start", "Yang Documentation", "Yang Models", and a "Logout" button. Below the header, there is a text area containing the RESTCONF request: "logging level `netstack` 6". To the right of this text area, there are two dropdown menus: "Method" set to "RESTCONF (Yang)" and "Message format" set to "xml". Below the text area, there is a "POST" dropdown menu, a text input field containing "restconf/data/Cisco-NX-OS-device:System/", and three buttons: "Send", "Reset", and "Convert". Below this, there is a "Request" tab selected, with other tabs for "Python", "Python3", "Java", "JavaScript", and "Go-Lang". The "Request" tab shows the XML response:
 

```
<ipv4-items>
<inst-items>
  <loggingLevel>informational</loggingLevel>
</inst-items>
</ipv4-items>
```

 To the right of the XML response is a green "Copy" button. Below the "Request" tab, there is a "Response:" label and an empty text area with a green "Copy" button to its right.

**Step 6** You can also convert the request into the following formats by clicking on the appropriate tab in the **Request** pane:

- Python
- Python3
- Java
- JavaScript
- Go-Lang

**Note** The Java-generated script does not work if you choose the PATCH option from the drop-down menu in the area above the Request tab. This is a known limitation with Java and is expected behavior.



## CHAPTER 13

# XML Support for ABM and LM in N3500

- [XML Support for ABM and LM in N3500](#) , on page 117

## XML Support for ABM and LM in N3500

The following commands show XML Output for ABM and LM:

### show hardware profile buffer monitor sampling

#### CLI :

```
MTC-8(config)# show hardware profile buffer monitor sampling

Sampling CLI issued at: 05/25/2016 04:18:56

Sampling interval: 200
```

#### XML :

```
MTC-8(config)# show hardware profile buffer monitor sampling | xml

<?xml version="1.0" encoding="ISO-8859-1"?>

<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:mtc_usd_cli">

  <nf:data>

    <show>

      <hardware>

        <profile>

          <buffer>

            <monitor>

              <__XML__BLK_Cmd_show_hardware_profile_buffer_monitor_summary>

                <__XML__OPT_Cmd_show_hardware_profile_buffer_monitor__readonly__>

                  <__readonly__>

                    <cmd_name>Sampling CLI</cmd_name>
```

```

<cmd_issue_time>05/25/2016 04:19:12</cmd_issue_time>

<TABLE_sampling>

  <ROW_sampling>

    <sampling_interval>200</sampling_interval>

  </ROW_sampling>

</TABLE_sampling>

</__readonly__>

</__XML__OPT_Cmd_show_hardware_profile_buffer_monitor__readonly__>

</__XML__BLK_Cmd_show_hardware_profile_buffer_monitor_summary>

</monitor>

</buffer>

</profile>

</hardware>

</show>

</nf:data>

</nf:rpc-reply>

]]>]]>

```

### show hardware profile buffer monitor detail | xml

**XML :**

```

<show>
  <hardware>
    <profile>
      <buffer>
        <monitor>
          <__XML__BLK_Cmd_show_hardware_profile_buffer_monitor_summary>
            <__XML__OPT_Cmd_show_hardware_profile_buffer_monitor__readonly__>
              <__readonly__>
                <cmd_name>Detail CLI</cmd_name>
                <cmd_issue_time>10/02/2001 10:58:58</cmd_issue_time>
                <TABLE_detail_entry>
                  <ROW_detail_entry>
                    <detail_util_name>Ethernet1/1</detail_util_name>
                    <detail_util_state>Active</detail_util_state>
                  </ROW_detail_entry>
                <ROW_detail_entry>
                  <time_stamp>10/02/2001 10:58:58</time_stamp>
                  <__XML__DIGIT384k_util>0</__XML__DIGIT384k_util>
                  <__XML__DIGIT768k_util>0</__XML__DIGIT768k_util>
                  <__XML__DIGIT1152k_util>0</__XML__DIGIT1152k_util>
                  <__XML__DIGIT1536k_util>0</__XML__DIGIT1536k_util>
                  <__XML__DIGIT1920k_util>0</__XML__DIGIT1920k_util>
                  <__XML__DIGIT2304k_util>0</__XML__DIGIT2304k_util>
                  <__XML__DIGIT2688k_util>0</__XML__DIGIT2688k_util>
                  <__XML__DIGIT3072k_util>0</__XML__DIGIT3072k_util>
                  <__XML__DIGIT3456k_util>0</__XML__DIGIT3456k_util>
                </ROW_detail_entry>
              </__readonly__>
            </__XML__OPT_Cmd_show_hardware_profile_buffer_monitor__readonly__>
          </__XML__BLK_Cmd_show_hardware_profile_buffer_monitor_summary>
        </monitor>
      </buffer>
    </profile>
  </hardware>
</show>

```

```
<_XML_DIGIT3840k_util>0</_XML_DIGIT3840k_util>
<_XML_DIGIT4224k_util>0</_XML_DIGIT4224k_util>
<_XML_DIGIT4608k_util>0</_XML_DIGIT4608k_util>
<_XML_DIGIT4992k_util>0</_XML_DIGIT4992k_util>
<_XML_DIGIT5376k_util>0</_XML_DIGIT5376k_util>
<_XML_DIGIT5760k_util>0</_XML_DIGIT5760k_util>
<_XML_DIGIT6144k_util>0</_XML_DIGIT6144k_util>
</ROW_detail_entry>
<ROW_detail_entry>
  <time_stamp>10/02/2001 10:58:57</time_stamp>
  <_XML_DIGIT384k_util>0</_XML_DIGIT384k_util>
  <_XML_DIGIT768k_util>0</_XML_DIGIT768k_util>
  <_XML_DIGIT1152k_util>0</_XML_DIGIT1152k_util>
  <_XML_DIGIT1536k_util>0</_XML_DIGIT1536k_util>
  <_XML_DIGIT1920k_util>0</_XML_DIGIT1920k_util>
  <_XML_DIGIT2304k_util>0</_XML_DIGIT2304k_util>
  <_XML_DIGIT2688k_util>0</_XML_DIGIT2688k_util>
  <_XML_DIGIT3072k_util>0</_XML_DIGIT3072k_util>
  <_XML_DIGIT3456k_util>0</_XML_DIGIT3456k_util>
  <_XML_DIGIT3840k_util>0</_XML_DIGIT3840k_util>
  <_XML_DIGIT4224k_util>0</_XML_DIGIT4224k_util>
  <_XML_DIGIT4608k_util>0</_XML_DIGIT4608k_util>
  <_XML_DIGIT4992k_util>0</_XML_DIGIT4992k_util>
  <_XML_DIGIT5376k_util>0</_XML_DIGIT5376k_util>
  <_XML_DIGIT5760k_util>0</_XML_DIGIT5760k_util>
  <_XML_DIGIT6144k_util>0</_XML_DIGIT6144k_util>
</ROW_detail_entry>
<ROW_detail_entry>
  <time_stamp>10/02/2001 10:58:56</time_stamp>
  <_XML_DIGIT384k_util>0</_XML_DIGIT384k_util>
  <_XML_DIGIT768k_util>0</_XML_DIGIT768k_util>
  <_XML_DIGIT1152k_util>0</_XML_DIGIT1152k_util>
  <_XML_DIGIT1536k_util>0</_XML_DIGIT1536k_util>
  <_XML_DIGIT1920k_util>0</_XML_DIGIT1920k_util>
  <_XML_DIGIT2304k_util>0</_XML_DIGIT2304k_util>
  <_XML_DIGIT2688k_util>0</_XML_DIGIT2688k_util>
  <_XML_DIGIT3072k_util>0</_XML_DIGIT3072k_util>
  <_XML_DIGIT3456k_util>0</_XML_DIGIT3456k_util>
  <_XML_DIGIT3840k_util>0</_XML_DIGIT3840k_util>
  <_XML_DIGIT4224k_util>0</_XML_DIGIT4224k_util>
  <_XML_DIGIT4608k_util>0</_XML_DIGIT4608k_util>
  <_XML_DIGIT4992k_util>0</_XML_DIGIT4992k_util>
  <_XML_DIGIT5376k_util>0</_XML_DIGIT5376k_util>
  <_XML_DIGIT5760k_util>0</_XML_DIGIT5760k_util>
  <_XML_DIGIT6144k_util>0</_XML_DIGIT6144k_util>
</ROW_detail_entry>
<ROW_detail_entry>
  <time_stamp>10/02/2001 10:58:55</time_stamp>
  <_XML_DIGIT384k_util>0</_XML_DIGIT384k_util>
  <_XML_DIGIT768k_util>0</_XML_DIGIT768k_util>
  <_XML_DIGIT1152k_util>0</_XML_DIGIT1152k_util>
  <_XML_DIGIT1536k_util>0</_XML_DIGIT1536k_util>
  <_XML_DIGIT1920k_util>0</_XML_DIGIT1920k_util>
  <_XML_DIGIT2304k_util>0</_XML_DIGIT2304k_util>
  <_XML_DIGIT2688k_util>0</_XML_DIGIT2688k_util>
  <_XML_DIGIT3072k_util>0</_XML_DIGIT3072k_util>
  <_XML_DIGIT3456k_util>0</_XML_DIGIT3456k_util>
  <_XML_DIGIT3840k_util>0</_XML_DIGIT3840k_util>
  <_XML_DIGIT4224k_util>0</_XML_DIGIT4224k_util>
  <_XML_DIGIT4608k_util>0</_XML_DIGIT4608k_util>
  <_XML_DIGIT4992k_util>0</_XML_DIGIT4992k_util>
  <_XML_DIGIT5376k_util>0</_XML_DIGIT5376k_util>
  <_XML_DIGIT5760k_util>0</_XML_DIGIT5760k_util>
  <_XML_DIGIT6144k_util>0</_XML_DIGIT6144k_util>
```

```

</ROW_detail_entry>
<ROW_detail_entry>
  <time_stamp>10/02/2001 10:58:54</time_stamp>
  <__XML__DIGIT384k_util>0</__XML__DIGIT384k_util>
  <__XML__DIGIT768k_util>0</__XML__DIGIT768k_util>
  <__XML__DIGIT1152k_util>0</__XML__DIGIT1152k_util>
  <__XML__DIGIT1536k_util>0</__XML__DIGIT1536k_util>
  <__XML__DIGIT1920k_util>0</__XML__DIGIT1920k_util>
  <__XML__DIGIT2304k_util>0</__XML__DIGIT2304k_util>
  <__XML__DIGIT2688k_util>0</__XML__DIGIT2688k_util>
  <__XML__DIGIT3072k_util>0</__XML__DIGIT3072k_util>
  <__XML__DIGIT3456k_util>0</__XML__DIGIT3456k_util>
  <__XML__DIGIT3840k_util>0</__XML__DIGIT3840k_util>
  <__XML__DIGIT4224k_util>0</__XML__DIGIT4224k_util>
  <__XML__DIGIT4608k_util>0</__XML__DIGIT4608k_util>
  <__XML__DIGIT4992k_util>0</__XML__DIGIT4992k_util>
  <__XML__DIGIT5376k_util>0</__XML__DIGIT5376k_util>
  <__XML__DIGIT5760k_util>0</__XML__DIGIT5760k_util>
  <__XML__DIGIT6144k_util>0</__XML__DIGIT6144k_util>
</ROW_detail_entry>

```

### show hardware profile buffer monitor brief

**XML :**

```

show hardware profile buffer monitor brief | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:mtc_usd_cli">
  <nf:data>
    <show>
      <hardware>
        <profile>
          <buffer>
            <monitor>
              <__XML__BLK_Cmd_show_hardware_profile_buffer_monitor_summary>
                <__XML__OPT_Cmd_show_hardware_profile_buffer_monitor__readonly__>
                  <__readonly__>
                    <cmd_name>Brief CLI</cmd_name>
                    <cmd_issue_time>03/21/2016 09:06:38</cmd_issue_time>
                    <TABLE_ucst_hdr>
                      <ROW_ucst_hdr>
                        <ucst_hdr_util_name>Buffer Block 1</ucst_hdr_util_name>
                        <ucst_hdr_1sec_util>0KB</ucst_hdr_1sec_util>
                        <ucst_hdr_5sec_util>0KB</ucst_hdr_5sec_util>
                        <ucst_hdr_60sec_util>N/A</ucst_hdr_60sec_util>
                        <ucst_hdr_5min_util>N/A</ucst_hdr_5min_util>
                        <ucst_hdr_1hr_util>N/A</ucst_hdr_1hr_util>
                        <ucst_hdr_total_buffer>Total Shared Buffer Available = 5397 Kbytes
                      </ucst_hdr_total_buffer>
                      <ucst_hdr_class_threshold>Class Threshold Limit = 5130 Kbytes
                    </ucst_hdr_class_threshold>
                  </ROW_ucst_hdr>
                </TABLE_ucst_hdr>
                <TABLE_brief_entry>
                  <ROW_brief_entry>
                    <brief_util_name>Ethernet1/45</brief_util_name>
                    <brief_1sec_util>0KB</brief_1sec_util>
                    <brief_5sec_util>0KB</brief_5sec_util>
                    <brief_60sec_util>N/A</brief_60sec_util>
                    <brief_5min_util>N/A</brief_5min_util>
                    <brief_1hr_util>N/A</brief_1hr_util>
                    <brief_util_name>Ethernet1/46</brief_util_name>
                    <brief_1sec_util>0KB</brief_1sec_util>

```



```
<brief_5min_util>N/A</brief_5min_util>
<brief_1hr_util>N/A</brief_1hr_util>
```

### show hardware profile latency monitor sampling

#### CLI

```
MTC-8(config)# show hardware profile latency monitor sampling

Sampling CLI issued at: 05/25/2016 04:19:54

Sampling interval: 20
```

#### XML

```
MTC-8(config)# show hardware profile latency monitor sampling | xml

<?xml version="1.0" encoding="ISO-8859-1"?>

<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:mtc_usd_cli">

  <nf:data>

    <show>

      <hardware>

        <profile>

          <latency>

            <monitor>

              <__XML__BLK_Cmd_show_hardware_profile_latency_monitor_summary>

                <__XML__OPT_Cmd_show_hardware_profile_latency_monitor__readonly__>

                  <__readonly__>

                    <cmd_issue_time>05/25/2016 04:20:06</cmd_issue_time>

                    <device_instance>0</device_instance>

                    <TABLE_sampling>

                      <ROW_sampling>

                        <sampling_interval>20</sampling_interval>

                      </ROW_sampling>

                    </TABLE_sampling>

                  </__readonly__>

                </__XML__OPT_Cmd_show_hardware_profile_latency_monitor__readonly__>

              </__XML__BLK_Cmd_show_hardware_profile_latency_monitor_summary>

            </monitor>

          </latency>
```

```

    </profile>
  </hardware>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

### show hardware profile latency monitor threshold

#### CLI

```
MTC-8(config)# show hardware profile latency monitor threshold
```

```
Sampling CLI issued at: 05/25/2016 04:20:53
```

```
Threshold Avg: 3000
```

```
Threshold Max: 300000
```

#### XML

```
MTC-8(config)# show hardware profile latency monitor threshold | xml
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:mtc_usd_cli">
```

```
<nf:data>
```

```
<show>
```

```
<hardware>
```

```
<profile>
```

```
<latency>
```

```
<monitor>
```

```
<__XML__BLK_Cmd_show_hardware_profile_latency_monitor_summary>
```

```
<__XML__OPT_Cmd_show_hardware_profile_latency_monitor__readonly__>
```

```
<__readonly__>
```

```
<cmd_issue_time>05/25/2016 04:21:04</cmd_issue_time>
```

```
<device_instance>0</device_instance>
```

```
<TABLE_threshold>
```

```
<ROW_threshold>
```

```
<threshold_avg>3000</threshold_avg>
```

```
<threshold_max>300000</threshold_max>
```

```
</ROW_threshold>
```

```
        </TABLE_threshold>
    </__readonly__>
    </__XML__OPT_Cmd_show_hardware_profile_latency_monitor__readonly__>
    </__XML__BLK_Cmd_show_hardware_profile_latency_monitor_summary>
</monitor>
</latency>
</profile>
</hardware>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
```



# CHAPTER 14

## Converting CLI Commands to Network Configuration Format

- [Information About XMLIN, on page 125](#)
- [Licensing Requirements for XMLIN, on page 125](#)
- [Installing and Using the XMLIN Tool, on page 126](#)
- [Converting Show Command Output to XML, on page 126](#)
- [Configuration Examples for XMLIN, on page 127](#)

### Information About XMLIN

The XMLIN tool converts CLI commands to the Network Configuration (NETCONF) protocol format. NETCONF is a network management protocol that provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses XML-based encoding for configuration data and protocol messages. The NX-OS implementation of the NETCONF protocol supports the following protocol operations: <get>, <edit-config>, <close-session>, <kill-session>, and <exec-command>.

The XMLIN tool converts show, EXEC, and configuration commands to corresponding NETCONF <get>, <exec-command>, and <edit-config> requests. You can enter multiple configuration commands into a single NETCONF <edit-config> instance.

The XMLIN tool also converts the output of show commands to XML format.

### Licensing Requirements for XMLIN

*Table 13: XMLIN Licensing Requirements*

Product	License Requirement
Cisco NX-OS	XMLIN requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

# Installing and Using the XMLIN Tool

You can install the XMLIN tool and then use it to convert configuration commands to NETCONF format.

## Before you begin

The XMLIN tool can generate NETCONF instances of commands even if the corresponding feature sets or required hardware capabilities are not available on the device. But, you might still need to install some feature sets before entering the **xmlin** command.

## SUMMARY STEPS

1. switch# **xmlin**
2. switch(xmlin)# **configure terminal**
3. Configuration commands
4. (Optional) switch(config)(xmlin)# **end**
5. (Optional) switch(config-if-verify)(xmlin)# **show commands**
6. (Optional) switch(config-if-verify)(xmlin)# **exit**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>xmlin</b>	
<b>Step 2</b>	switch(xmlin)# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	Configuration commands	Converts configuration commands to NETCONF format.
<b>Step 4</b>	(Optional) switch(config)(xmlin)# <b>end</b>	Generates the corresponding <edit-config> request.  <b>Note</b> Enter the <b>end</b> command to finish the current XML configuration before you generate an XML instance for a <b>show</b> command.
<b>Step 5</b>	(Optional) switch(config-if-verify)(xmlin)# <b>show commands</b>	Converts <b>show</b> commands to NETCONF format.
<b>Step 6</b>	(Optional) switch(config-if-verify)(xmlin)# <b>exit</b>	Returns to EXEC mode.

# Converting Show Command Output to XML

You can convert the output of show commands to XML.

## Before you begin

Make sure that all features for the commands you want to convert are installed and enabled on the device. Otherwise, the commands fail.

You can use the **terminal verify-only** command to verify that a feature is enabled without entering it on the device.

Make sure that all required hardware for the commands you want to convert are present on the device. Otherwise, the commands fail.

Make sure that the XMLIN tool is installed.

**SUMMARY STEPS**

1. switch# *show-command* | **xmlin**

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	switch# <i>show-command</i>   <b>xmlin</b>	Enters global configuration mode.  <b>Note</b> You cannot use this command with configuration commands.

# Configuration Examples for XMLIN

The following example shows how the XMLIN tool is installed on the device and used to convert a set of configuration commands to an <edit-config> instance.

```

switch# xmlin
*****
Loading the xmlin tool. Please be patient.
*****
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright © 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
% Success
switch(config-if-verify)(xmlin)# cdp enable
% Success
switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec"
xmlns:m1="http://www.cisco.com/nxos:6.2.2.:configure__if-eth-base" message-id="1">
  <nf:edit-config>
    <nf:target>
      <nf:running/>
    </nf:target>
  <nf:config>
    <m:configure>

```

```

<m:terminal>
  <interface>
    <__XML_PARAM_interface>
      <__XML_value>Ethernet2/1</__XML_value>
      <ml:cdp>
        <ml:enable/>
      </ml:cdp>
    </__XML_PARAM_interface>
  </interface>
</m:terminal>
</m:configure>
</nf:config>
</nf:edit-config>
</nf:rpc>
]]>]]>
    
```

The following example shows how to enter the **end** command to finish the current XML configuration before you generate an XML instance for a **show** command.

```

switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
switch(config-if-verify)(xmlin)# show interface ethernet 2/1
*****
Please type "end" to finish and output the current XML document before building a new one.
*****
% Command not successful

switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec" message-id="1">
  <nf:edit-config>
    <nf:target>
      <nf:running/>
    </nf:target>
    <nf:config>
      <m:configure>
        <m:terminal>
          <interface>
            <__XML_PARAM_interface>
              <__XML_value>Ethernet2/1</__XML_value>
            </__XML_PARAM_interface>
          </interface>
        </m:terminal>
      </m:configure>
    </nf:config>
  </nf:edit-config>
</nf:rpc>
]]>]]>

switch(xmlin)# show interface ethernet 2/1
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager" message-id="1">
  <nf:get>
    <nf:filter type="subtree">
      <show>
        <interface>
          <__XML_PARAM_ifeth>
            <__XML_value>Ethernet2/1</__XML_value>
          </__XML_PARAM_ifeth>
        </interface>
      </show>
    </nf:filter>
  </nf:get>
</nf:rpc>
    
```

```
        </interface>
    </show>
</nf:filter>
</nf:get>
</nf:rpc>
]]>]]>
switch(xmlin) # exit
switch#
```

The following example shows how you can convert the output of the **show interface brief** command to XML.

```
switch# show interface brief | xmlin
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager"

message-id="1">
  <nf:get>
    <nf:filter type="subtree">
      <show>
        <interface>
          <brief/>
        </interface>
      </show>
    </nf:filter>
  </nf:get>
</nf:rpc>
]]>]]>
```





## CHAPTER 15

# Model-Driven Telemetry

---

- [About Telemetry, on page 131](#)
- [Licensing Requirements for Telemetry, on page 133](#)
- [Installing and Upgrading Telemetry, on page 133](#)
- [Guidelines and Limitations, on page 134](#)
- [Configuring Telemetry Using the CLI, on page 139](#)
- [Configuring Telemetry Using the NX-API, on page 153](#)
- [Additional References, on page 166](#)

## About Telemetry

Collecting data for analyzing and troubleshooting has always been an important aspect in monitoring the health of a network.

Cisco NX-OS provides several mechanisms such as SNMP, CLI, and Syslog to collect data from a network. These mechanisms have limitations that restrict automation and scale. One limitation is the use of the pull model, where the initial request for data from network elements originates from the client. The pull model does not scale when there is more than one network management station (NMS) in the network. With this model, the server sends data only when clients request it. To initiate such requests, continual manual intervention is required. This continual manual intervention makes the pull model inefficient.

A push model continuously streams data out of the network and notifies the client. Telemetry enables the push model, which provides near-real-time access to monitoring data.

## Telemetry Components and Process

Telemetry consists of four key elements:

- **Data Collection** — Telemetry data is collected from the Data Management Engine (DME) database in branches of the object model specified using distinguished name (DN) paths. The data can be retrieved periodically (frequency-based) or only when a change occurs in any object on a specified path (event-based). You can use the NX-API to collect frequency-based data.
- **Data Encoding** — The telemetry encoder encapsulates the collected data into the desired format for transporting.

NX-OS encodes telemetry data in the Google Protocol Buffers (GPB) and JSON format.

- **Data Transport** — NX-OS transports telemetry data using HTTP for JSON encoding and the Google remote procedure call (gRPC) protocol for GPB encoding. The gRPC receiver supports message sizes greater than 4MB. (Telemetry data using HTTPS is also supported if a certificate is configured.)

Starting with Cisco Nexus 9.2(1), UDP and secure UDP (DTLS) are supported as telemetry transport protocols. You can add destinations that receive UDP. The encoding for UDP and secure UDP can be GPB or JSON.

Use the following command to configure the UDP transport to stream data using a datagram socket either in JSON or GPB:

```
destination-group num
  ip address xxx.xxx.xxx.xxx port xxxx protocol UDP encoding {JSON | GPB }
```

Where *num* is a number between 1 and 4095.

Example for IPv4 destination:

```
destination-group 100
  ip address 171.70.55.69 port 50001 protocol UDP encoding GPB
```

The UDP telemetry will be sent with the following header:

```
typedef enum tm_encode_ {
    TM_ENCODE_DUMMY,
    TM_ENCODE_GPB,
    TM_ENCODE_JSON,
    TM_ENCODE_XML,
    TM_ENCODE_MAX,
} tm_encode_type_t;

typedef struct tm_pak_hdr_ {
    uint8_t version; /* 1 */
    uint8_t encoding;
    uint16_t msg_size;
    uint8_t secure;
    uint8_t padding;
} __attribute__((packed, aligned(1))) tm_pak_hdr_t;
```

Use the first 6 bytes in the payload to successfully process telemetry data using UDP, using one of the following methods:

- Read the information in the header to determine which decoder to use to decode the data, JSON or GPB, if the receiver is meant to receive different types of data from multiple end points, or
- Remove the header if you are expecting one decoder (JSON or GPB) but not the other




---

**Note** Depending on the receiving operation system and the network load, using the UDP protocol may result in packet drops.

---

- **Telemetry Receiver** — A telemetry receiver is a remote management system or application that stores the telemetry data.

The GPB encoder stores data in a generic key-value format. The encoder requires metadata in the form of a compiled `.proto` file to translate the data into GPB format.

In order to correctly receive and decode the data stream, the receiver requires the `.proto` file that describes the encoding and the transport services. The encoding decodes the binary stream into a key value string pair.

A telemetry `.proto` file that describes the GPB encoding and gRPC transport is available on Cisco's GitLab: <https://github.com/CiscoDevNet/nx-telemetry-proto>

## High Availability of the Telemetry Process

High availability of the telemetry process is supported with the following behaviors:

- **System Reload** — During a system reload, any telemetry configuration and streaming services are restored.
- **Process Restart** — If the telemetry process freezes or restarts for any reason, configuration and streaming services are restored when telemetry is restarted.

## Licensing Requirements for Telemetry

Product	License Requirement
Cisco NX-OS	Telemetry requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

## Installing and Upgrading Telemetry

### Installing the Application

The telemetry application is packaged as a feature RPM and included with the NX-OS release. The RPM is installed by default as part of the image bootup. After installation, you can start the application using the **feature telemetry** command. The RPM file is located in the `/rpms` directory and is named as follows:

As in the following example:

### Installing Incremental Updates and Fixes

Copy the RPM to the device bootflash and use the following commands from the `bash` prompt:

```
feature bash
run bash sudo su
```

Then copy the RPM to the device bootflash. Use the following commands from the `bash` prompt:

```
yum upgrade telemetry_new_version.rpm
```

The application is upgraded and the change appears when the application is started again.

### Downgrading to a Previous Version

To downgrade the telemetry application to a previous version, use the following command from the `bash` prompt:

```
yum downgrade telemetry
```

### Verifying the Active Version

To verify the active version, run the following command from the switch `exec` prompt:

```
show install active
```




---

**Note** The `show install active` command will only show the active installed RPM after an upgrade has occurred. The default RPM that comes bundled with the NX-OS will not be displayed.

---

## Guidelines and Limitations

Telemetry has the following configuration guidelines and limitations:

- Telemetry is supported in Cisco NX-OS releases that support the data management engine (DME) Native Model.
- Support is in place for DME data collection, NX-API data sources, Google protocol buffer (GPB) encoding over Google Remote Procedure Call (gRPC) transport, and JSON encoding over HTTP.
- The smallest sending interval (cadence) supported is five seconds for a depth of 0. The minimum cadence values for depth values greater than 0 depends on the size of the data being streamed out. Configuring cadences below the minimum value may result in undesirable system behavior.
- Up to five remote management receivers (destinations) are supported. Configuring more than five remote receivers may result in undesirable system behavior.
- In the event that a telemetry receiver goes down, other receivers will see data flow interrupted. The failed receiver must be restarted. Then start a new connection with the switch by unconfiguring then reconfiguring the failed receiver's IP address under the destination group.
- Telemetry can consume up to 20% of the CPU resource.
- To configure SSL certificate based authentication and the encryption of streamed data, you can provide a self signed SSL certificate with `certificate ssl cert path hostname "CN"` command.
- QoS Explicit Congestion Notification (ECN) statistics are supported only on Cisco Nexus 9364C, 9336C-FX, and 93240YC-FX switches.

### Configuration Commands After Downgrading to an Older Release

After a downgrade to an older release, some configuration commands or command options might fail because the older release may not support them. As a best practice when downgrading to an older release, unconfigure and reconfigure the telemetry feature after the new image comes up to avoid the failure of unsupported commands or command options.

The following example shows this procedure:

- Copy the telemetry configuration to a file:

```
switch# show running-config | section telemetry
feature telemetry
```

```

telemetry
 destination-group 100
   ip address 1.2.3.4 port 50004 protocol gRPC encoding GPB
   use-chunking size 4096
 sensor-group 100
   path sys/bgp/inst/dom-default depth 0
 subscription 600
  dst-grp 100
   snsr-grp 100 sample-interval 7000
switch# show running-config | section telemetry > telemetry_running_config
switch# show file bootflash:telemetry_running_config
feature telemetry
telemetry
 destination-group 100
   ip address 1.2.3.4 port 50004 protocol gRPC encoding GPB
   use-chunking size 4096
 sensor-group 100
   path sys/bgp/inst/dom-default depth 0
 subscription 600
  dst-grp 100
   snsr-grp 100 sample-interval 7000
switch#

```

- Execute the downgrade operation. When the image comes up and the switch is ready, copy the telemetry configurations back to the switch:

```

switch# copy telemetry_running_config running-config echo-commands
`switch# config terminal`
`switch(config)# feature telemetry`
`switch(config)# telemetry`
`switch(config-telemetry)# destination-group 100`
`switch(conf-tm-dest)# ip address 1.2.3.4 port 50004 protocol gRPC encoding GPB `
`switch(conf-tm-dest)# sensor-group 100`
`switch(conf-tm-sensor)# path sys/bgp/inst/dom-default depth 0`
`switch(conf-tm-sensor)# subscription 600`
`switch(conf-tm-sub)# dst-grp 100`
`switch(conf-tm-sub)# snsr-grp 100 sample-interval 7000`
`switch(conf-tm-sub)# end`
Copy complete, now saving to disk (please wait)...
Copy complete.
switch#

```

### gRPC Error Behavior

The switch client will disable the connection to the gRPC receiver if the gRPC receiver sends 20 errors. You will then need to unconfigure then reconfigure the receiver's IP address under the destination group to enable the gRPC receiver. Errors include:

- The gRPC client sends the wrong certificate for secure connections,
- The gRPC receiver takes too long to handle client messages and incurs a timeout. Avoid timeouts by processing messages using a separate message processing thread.

### Telemetry Compression for gRPC Transport

Telemetry compression support is available for gRPC transport. You can use the **use-compression gzip** command to enable compression. (Disable compression with the **no use-compression gzip** command.)

The following example enables compression:

```
switch(config)# telemetry
switch(config-telemetry)# destination-profile
switch(config-tm-dest-profile)# use-compression gzip
```

The following example shows compression is enabled:

```
switch(conf-tm-dest)# show telemetry transport 0 stats

Session Id:                0
Connection Stats
  Connection Count         0
  Last Connected:         Never
  Disconnect Count        0
  Last Disconnected:      Never
Transmission Stats
  Compression:            gzip
  Source Interface:       loopback1(1.1.3.4)
  Transmit Count:         0
  Last TX time:           None
  Min Tx Time:            0          ms
  Max Tx Time:            0          ms
  Avg Tx Time:            0          ms
  Cur Tx Time:            0          ms
```

```
switch2(config-if)# show telemetry transport 0 stats

Session Id: 0
Connection Stats
Connection Count 0
Last Connected: Never
Disconnect Count 0
Last Disconnected: Never
Transmission Stats
Compression: disabled
Source Interface: loopback1(1.1.3.4)
Transmit Count: 0
Last TX time: None
Min Tx Time: 0 ms
Max Tx Time: 0 ms
Avg Tx Time: 0 ms
Cur Tx Time: 0 ms
switch2(config-if)#
```

The following is an example of use-compression as a POST payload:

```
{
  "telemetryDestProfile": {
    "attributes": {
      "adminSt": "enabled"
    },
    "children": [
      {
        "telemetryDestOptCompression": {
          "attributes": {
            "name": "gzip"
          }
        }
      }
    ]
  }
}
```

### Support for gRPC Chunking

Starting with Release 9.2(1), support for gRPC chunking has been added. For streaming to occur successfully, you must enable chunking if gRPC has to send an amount of data greater than 12MB to the receiver.

gRPC chunking has to be done by the gRPC user. Fragmentation has to be done on the gRPC client side and reassembly has to be done on the gRPC server side. Telemetry is still bound to memory and data can be dropped if the memory size is more than the allowed limit of 12MB for telemetry. In order to support chunking, use the telemetry `.proto` file that is available at Cisco's GibLab, which has been updated for gRPC chunking, as described in [Telemetry Components and Process, on page 131](#).

The chunking size is between 64 and 4096 bytes.

Following shows a configuration example through the NX-API CLI:

```
feature telemetry
!
telemetry
  destination-group 1
    ip address 171.68.197.40 port 50051 protocol gRPC encoding GPB
    use-chunking size 4096
  destination-group 2
    ip address 10.155.0.15 port 50001 protocol gRPC encoding GPB
    use-chunking size 64
  sensor-group 1
    path sys/intf depth unbounded
  sensor-group 2
    path sys/intf depth unbounded
  subscription 1
    dst-grp 1
    snsr-grp 1 sample-interval 10000
  subscription 2
    dst-grp 2
    snsr-grp 2 sample-interval 15000
```

Following shows a configuration example through the NX-API REST:

```
{
  "telemetryDestGrpOptChunking": {
    "attributes": {
      "chunkSize": "2048",
      "dn": "sys/tm/dest-1/chunking"
    }
  }
}
```

The following error message will appear on systems that do not support gRPC chunking, such as the Cisco MDS series switches:

```
MDS-9706-86(conf-tm-dest)# use-chunking size 200
ERROR: Operation failed: [chunking support not available]
```

### NX-API Sensor Path Limitations

NX-API can collect and stream switch information not yet in the DME using `show` commands. However, using the NX-API instead of streaming data from the DME has inherent scale limitations as outlined:

- The switch backend dynamically processes NX-API calls such as `show` commands,
- NX-API spawns several processes that can consume up to a maximum of 20% of the CPU.

- NX-API data translates from the CLI to XML to JSON.

The following is a suggested user flow to help limit excessive NX-API sensor path bandwidth consumption:

1. Check whether the **show** command has NX-API support. You can confirm whether NX-API supports the command from the VSH with the pipe option: `show <command> | json` or `show <command> | json pretty`.




---

**Note** Avoid commands that take the switch more than 30 seconds to return JSON output.

---

2. Refine the **show** command to include any filters or options.
  - Avoid enumerating the same command for individual outputs; i.e., `show vlan id 100`, `show vlan id 101`, etc.. Instead, use the CLI range options; i.e., `show vlan id 100-110,204`, whenever possible to improve performance.

If only the summary/counter is needed, then avoid dumping a whole show command output to limit the bandwidth and data storage required for data collection.
3. Configure telemetry with sensor groups that use NX-API as their data sources. Add the **show** commands as sensor paths
4. Configure telemetry with a cadence of 5 times the processing time of the respective **show** command to limit CPI usage.
5. Receive and process the streamed NX-API output as part of the existing DME collection.

### Telemetry VRF Support

Telemetry VRF support allows you to specify a transport VRF. This means that the telemetry data stream can egress via front-panel ports and avoid possible competition between SSH/NGINX control sessions.

You can use the **use-vrf** *vrf-name* command to specify the transport VRF.

The following example specifies the transport VRF:

```
switch(config)# telemetry
switch(config-telemetry)# destination-profile
switch(config-tm-dest-profile)# use-vrf test_vrf
```

The following is an example of use-vrf as a POST payload:

```
{
  "telemetryDestProfile": {
    "attributes": {
      "adminSt": "enabled"
    },
    "children": [
      {
        "telemetryDestOptVrf": {
          "attributes": {
            "name": "default"
          }
        }
      }
    ]
  }
}
```

```

    }
  ]
}

```

# Configuring Telemetry Using the CLI

## Configuring Telemetry Using the NX-OS CLI

The following steps enables streaming telemetry, and configures the source and destination of the data stream. These steps also include optional steps to enable and configure SSL/TLS certificates and GPB encoding.

### Before you begin

Your switch must be running Cisco NX-OS Release 9.2(1) or a later release.

### SUMMARY STEPS

1. (Optional) **openssl** *argument*
2. **configure terminal**
3. **feature telemetry**
4. **feature nxapi**
5. **nxapi use-vrf management**
6. **telemetry**
7. (Optional) **certificate** *certificate\_path host\_URL*
8. (Optional) Specify a transport VRF and/or enable telemetry compression for gRPC transport.
9. **sensor-group** *sgrp\_id*
10. (Optional) **data-source** *data-source-type*
11. **path** *sensor\_path depth 0 [filter-condition filter]*
12. **destination-group** *dgrp\_id*
13. (Optional) **ip address** *ip\_address port port protocol procedural-protocol encoding encoding-protocol*
14. **ip\_version address** *ip\_address port portnum*
15. **subscription** *sub\_id*
16. **snsr-grp** *sgrp\_id sample-interval interval*
17. **dst-grp** *dgrp\_id*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) <b>openssl</b> <i>argument</i>  <b>Example:</b> Generate an SSL/TLS certificate using a specific argument, such as the following:	Create an SSL/TLS certificate on the server that will receive the data, where <i>private.key</i> file is the private key and the <i>public.crt</i> is the public key.

	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>To generate a private RSA key: <b>openssl genrsa -cipher -out filename.key cipher-bit-length</b> For example: <pre>switch# openssl genrsa -des3 server.key 2048</pre></li> <li>To write the RSA key: <b>openssl rsa -in filename.key -out filename.key</b> For example: <pre>switch# openssl rsa -in server.key -out server.key</pre></li> <li>To create a certificate that contains the public/private key: <b>openssl req -encoding-standard -new -new filename.key -out filename.csr -subj '/CN=localhost'</b> For example: <pre>switch# openssl req -sha256 -new -key server.key -out server.csr -subj '/CN=localhost'</pre></li> <li>To create a public key: <b>openssl x509 -req -encoding-standard -days timeframe -in filename.csr -signkey filename.key -out filename.csr</b> For example: <pre>switch# openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt</pre></li> </ul>	
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enter the global configuration mode.
<b>Step 3</b>	<b>feature telemetry</b>	Enable the streaming telemetry feature.
<b>Step 4</b>	<b>feature nxapi</b>	Enable nxapi.
<b>Step 5</b>	<b>nxapi use-vrf management</b>	Enable the VRF management to be used for nxapi communication.
<b>Step 6</b>	<b>telemetry</b>  <b>Example:</b> <pre>switch(config)# telemetry switch(config-telemetry)#</pre>	Enter configuration mode for streaming telemetry.

	Command or Action	Purpose
Step 7	(Optional) <b>certificate</b> <i>certificate_path host_URL</i>  <b>Example:</b> <pre>switch(config-telemetry)# <b>certificate</b> /bootflash/server.key localhost</pre>	Use an existing SSL/TLS certificate.
Step 8	(Optional) Specify a transport VRF and/or enable telemetry compression for gRPC transport.  <b>Example:</b> <pre>switch(config-telemetry)# <b>destination-profile</b> switch(conf-tm-dest-profile)# <b>use-vrf default</b> switch(conf-tm-dest-profile)# <b>use-compression gzip</b> switch(conf-tm-dest-profile)# <b>use-retry size 10</b> switch(conf-tm-dest-profile)# <b>source-interface</b> loopback1</pre>	<ul style="list-style-type: none"> <li>• Enter the <b>destination-profile</b> command to specify the default destination profile.</li> <li>• Enter any of the following commands: <ul style="list-style-type: none"> <li>• <b>use-vrf</b> <i>vrf</i> to specify the destination vrf.</li> <li>• <b>use-compression gzip</b> to specify the destination compression method.</li> <li>• <b>use-retry size</b> <i>size</i> to specify the send retry details, with a retry buffer size between 10 and 1500 megabytes.</li> <li>• <b>source-interface</b> <i>interface-name</i> to stream data from the configured interface to a destination with the source IP address.</li> </ul> </li> </ul> <p><b>Note</b> After configuring the <b>use-vrf</b> command, you need to configure a new destination IP address within the new VRF. However, you may re-use the same destination IP address by un-configuring and re-configuring the destination. This ensures that the telemetry data streams to the same destination IP address in the new VRF.</p>
Step 9	<b>sensor-group</b> <i>srgp_id</i>  <b>Example:</b> <pre>switch(config-telemetry)# <b>sensor-group 100</b> switch(conf-tm-sensor)#</pre>	Create a sensor group with ID <i>srgp_id</i> and enter sensor group configuration mode.  Currently only numeric ID values are supported. The sensor group defines nodes that will be monitored for telemetry reporting.
Step 10	(Optional) <b>data-source</b> <i>data-source-type</i>  <b>Example:</b> <pre>switch(config-telemetry)# <b>data-source NX-API</b></pre>	Select a data source. Select from either DME or NX-API as the data source.  <b>Note</b> DME is the default data source.
Step 11	<b>path</b> <i>sensor_path</i> <b>depth 0</b> [ <b>filter-condition</b> <i>filter</i> ]  <b>Example:</b> <ul style="list-style-type: none"> <li>• The following command is applicable for DME, not for NX-API:</li> </ul> <pre>switch(conf-tm-sensor)# <b>path</b> sys/bd/bd-[vlan-100] <b>depth 0</b> <b>filter-condition</b> eq(l2BD.operSt, "down")</pre>	Add a sensor path to the sensor group. <ul style="list-style-type: none"> <li>• The <b>depth</b> setting specifies the retrieval level for the sensor path. Depth settings of <b>0 - 32</b>, <b>unbounded</b> are supported.</li> </ul>

	Command or Action	Purpose
	<p>Use the syntax below for state-based filtering to trigger only when <b>operSt</b> changes from <b>up</b> to <b>down</b>, with no notifications of when the MO changes.</p> <pre>switch(conf-tm-sensor)# path sys/bd/bd-[vlan-100] depth 0 filter-condition and(updated(12BD.operSt),eq(12BD.operSt,"down"))</pre> <ul style="list-style-type: none"> <li>The following command is applicable for NX-API, not for DME:</li> </ul> <pre>switch(conf-tm-sensor)# path "show interface" depth 0</pre>	<p><b>Note</b> <b>depth 0</b> is the default depth.</p> <p>NX-API-based sensor paths can only use <b>depth 0</b>.</p> <p>If a path is subscribed for the event collection, the depth only supports 0 and unbounded. Other values would be treated as 0.</p> <ul style="list-style-type: none"> <li>The optional <b>filter-condition</b> parameter can be specified to create a specific filter for event-based subscriptions.</li> </ul> <p>For state-based filtering, the filter will return both when a state has changed and when an event has occurred during the specified state. That is, a filter condition for the DN <b>sys/bd/bd-[vlan]</b> of <b>eq(12Bd.operSt, "down")</b> will trigger when the operSt changes, and when the DN's property changes while the operSt remains <b>down</b>, such as a <b>no shutdown</b> command is issued while the vlan is operationally <b>down</b>.</p> <p><b>Note</b> query-condition parameter — For DME, based on the DN, the query-condition parameter can be specified to fetch MOTL and ephemeral data with the following syntax: query-condition "rsp-foreign-subtree=applied-config"; query-condition "rsp-foreign-subtree=ephemeral".</p>
<b>Step 12</b>	<p><b>destination-group</b> <i>dgrp_id</i></p> <p><b>Example:</b></p> <pre>switch(conf-tm-sensor)# destination-group 100 switch(conf-tm-dest)#</pre>	<p>Create a destination group and enter destination group configuration mode.</p> <p>Currently <i>dgrp_id</i> only supports numeric ID values.</p>
<b>Step 13</b>	<p>(Optional) <b>ip address</b> <i>ip_address</i> <b>port</b> <i>port</i> <b>protocol</b> <i>procedural-protocol</i> <b>encoding</b> <i>encoding-protocol</i></p> <p><b>Example:</b></p> <pre>switch(conf-tm-sensor)# ip address 171.70.55.69 port 50001 protocol gRPC encoding GPB switch(conf-tm-sensor)# ip address 171.70.55.69 port 50007 protocol HTTP encoding JSON  switch(conf-tm-sensor)# ip address 171.70.55.69 port 50009 protocol UDP encoding JSON</pre>	<p>Specify an IPv4 IP address and port to receive encoded telemetry data.</p> <p><b>Note</b> gRPC is the default transport protocol.</p> <p>GPB is the default encoding.</p>
<b>Step 14</b>	<p><b>ip_version</b> <b>address</b> <i>ip_address</i> <b>port</b> <i>portnum</i></p> <p><b>Example:</b></p>	<p>Create a destination profile for the outgoing data.</p>

	Command or Action	Purpose
	<code>switch(conf-tm-dest)# ip address 1.2.3.4 port 50003</code>	When the destination group is linked to a subscription, telemetry data is sent to the IP address and port specified by this profile.
<b>Step 15</b>	<b>subscription</b> <i>sub_id</i> <b>Example:</b> <code>switch(conf-tm-dest)# subscription 100</code> <code>switch(conf-tm-sub)#</code>	Create a subscription node with ID and enter the subscription configuration mode. Currently <i>sub_id</i> only supports numeric ID values. <b>Note</b> When subscribing to a DN, check whether the DN is supported by DME using REST to ensure that events will stream.
<b>Step 16</b>	<b>snsr-grp</b> <i>sgrp_id</i> <b>sample-interval</b> <i>interval</i> <b>Example:</b> <code>switch(conf-tm-sub)# snsr-grp 100 sample-interval 15000</code>	Link the sensor group with ID <i>sgrp_id</i> to this subscription and set the data sampling interval in milliseconds. An interval value of 0 creates an event-based subscription, in which telemetry data is sent only upon changes under the specified MO. An interval value greater than 0 creates a frequency-based subscription, in which telemetry data is sent periodically at the specified interval. For example, an interval value of 15000 results in the sending of telemetry data every 15 seconds.
<b>Step 17</b>	<b>dst-grp</b> <i>dgrp_id</i> <b>Example:</b> <code>switch(conf-tm-sub)# dst-grp 100</code>	Link the destination group with ID <i>dgrp_id</i> to this subscription.

## Configuration Examples for Telemetry Using the CLI

This example creates a subscription that streams data for the `sys/bgp` root MO every 5 seconds to the destination IP 1.2.3.4 port 50003.

```
switch(config)# telemetry
switch(config-telemetry)# sensor-group 100
switch(conf-tm-sensor)# path sys/bgp depth 0
switch(conf-tm-sensor)# destination-group 100
switch(conf-tm-dest)# ip address 1.2.3.4 port 50003
switch(conf-tm-dest)# subscription 100
switch(conf-tm-sub)# snsr-grp 100 sample-interval 5000
switch(conf-tm-sub)# dst-grp 100
```

This example creates a subscription that streams data for `sys/intf` every 5 seconds to destination IP 1.2.3.4 port 50003, and encrypts the stream using GPB encoding verified using the `test.pem`.

```
switch(config)# telemetry
switch(config-telemetry)# certificate /bootflash/test.pem foo.test.google.fr
switch(conf-tm-telemetry)# destination-group 100
switch(conf-tm-dest)# ip address 1.2.3.4 port 50003 protocol gRPC encoding GPB
switch(config-dest)# sensor-group 100
switch(conf-tm-sensor)# path sys/bgp depth 0
switch(conf-tm-sensor)# subscription 100
```

```
switch(config-tm-sub)# snsr-grp 100 sample-interval 5000
switch(config-tm-sub)# dst-grp 100
```

This example creates a subscription that streams data for `sys/cdp` every 15 seconds to destination IP 1.2.3.4 port 50004.

```
switch(config)# telemetry
switch(config-telemetry)# sensor-group 100
switch(config-tm-sensor)# path sys/cdp depth 0
switch(config-tm-sensor)# destination-group 100
switch(config-tm-dest)# ip address 1.2.3.4 port 50004
switch(config-tm-dest)# subscription 100
switch(config-tm-sub)# snsr-grp 100 sample-interval 15000
switch(config-tm-sub)# dst-grp 100
```

This example creates a cadence-based collection of `show` command data every 750 seconds.

```
switch(config)# telemetry
switch(config-telemetry)# destination-group 1
switch(config-tm-dest)# ip address 172.27.247.72 port 60001 protocol gRPC encoding GPB
switch(config-tm-dest)# sensor-group 1
switch(config-tm-sensor)# data-source NX-API
switch(config-tm-sensor)# path "show system resources" depth 0
switch(config-tm-sensor)# path "show version" depth 0
switch(config-tm-sensor)# path "show environment power" depth 0
switch(config-tm-sensor)# path "show environment fan" depth 0
switch(config-tm-sensor)# path "show environment temperature" depth 0
switch(config-tm-sensor)# path "show process cpu" depth 0
switch(config-tm-sensor)# path "show nve peers" depth 0
switch(config-tm-sensor)# path "show nve vni" depth 0
switch(config-tm-sensor)# path "show nve vni 4002 counters" depth 0
switch(config-tm-sensor)# path "show int nve 1 counters" depth 0
switch(config-tm-sensor)# path "show policy-map vlan" depth 0
switch(config-tm-sensor)# path "show ip access-list test" depth 0
switch(config-tm-sensor)# path "show system internal access-list resource utilization" depth
0
switch(config-tm-sensor)# subscription 1
switch(config-tm-sub)# dst-grp 1
switch(config-tm-dest)# snsr-grp 1 sample-interval 750000
```

This example creates an event-based subscription for `sys/fm`. Data is streamed to the destination only if there is a change under the `sys/fm` MO.

```
switch(config)# telemetry
switch(config-telemetry)# sensor-group 100
switch(config-tm-sensor)# path sys/fm depth 0
switch(config-tm-sensor)# destination-group 100
switch(config-tm-dest)# ip address 1.2.3.4 port 50005
switch(config-tm-dest)# subscription 100
switch(config-tm-sub)# snsr-grp 100 sample-interval 0
switch(config-tm-sub)# dst-grp 100
```

During operation, you can change a sensor group from frequency-based to event-based, and change event-based to frequency-based by changing the sample-interval. This example changes the sensor-group from the previous example to frequency-based. After the following commands, the telemetry application will begin streaming the `sys/fm` data to the destination every 7 seconds.

```
switch(config)# telemetry
switch(config-telemetry)# subscription 100
switch(conf-tm-sub)# snsr-grp 100 sample-interval 7000
```

Multiple sensor groups and destinations can be linked to a single subscription. The subscription in this example streams the data for Ethernet port 1/1 to four different destinations every 10 seconds.

```
switch(config)# telemetry
switch(config-telemetry)# sensor-group 100
switch(conf-tm-sensor)# path sys/intf/phys-[eth1/1] depth 0
switch(conf-tm-sensor)# destination-group 100
switch(conf-tm-dest)# ip address 1.2.3.4 port 50004
switch(conf-tm-dest)# ip address 1.2.3.4 port 50005
switch(conf-tm-sensor)# destination-group 200
switch(conf-tm-dest)# ip address 5.6.7.8 port 50001 protocol HTTP encoding JSON
switch(conf-tm-dest)# ip address 1.4.8.2 port 60003
switch(conf-tm-dest)# subscription 100
switch(conf-tm-sub)# snsr-grp 100 sample-interval 10000
switch(conf-tm-sub)# dst-grp 100
switch(conf-tm-sub)# dst-grp 200
```

A sensor group can contain multiple paths, a destination group can contain multiple destination profiles, and a subscription can be linked to multiple sensor groups and destination groups, as shown in this example.

```
switch(config)# telemetry
switch(config-telemetry)# sensor-group 100
switch(conf-tm-sensor)# path sys/intf/phys-[eth1/1] depth 0
switch(conf-tm-sensor)# path sys/epId-1 depth 0
switch(conf-tm-sensor)# path sys/bgp/inst/dom-default depth 0

switch(config-telemetry)# sensor-group 200
switch(conf-tm-sensor)# path sys/cdp depth 0
switch(conf-tm-sensor)# path sys/ipv4 depth 0

switch(config-telemetry)# sensor-group 300
switch(conf-tm-sensor)# path sys/fm depth 0
switch(conf-tm-sensor)# path sys/bgp depth 0

switch(conf-tm-sensor)# destination-group 100
switch(conf-tm-dest)# ip address 1.2.3.4 port 50004
switch(conf-tm-dest)# ip address 4.3.2.5 port 50005

switch(conf-tm-dest)# destination-group 200
switch(conf-tm-dest)# ip address 5.6.7.8 port 50001

switch(conf-tm-dest)# destination-group 300
switch(conf-tm-dest)# ip address 1.2.3.4 port 60003

switch(conf-tm-dest)# subscription 600
switch(conf-tm-sub)# snsr-grp 100 sample-interval 7000
switch(conf-tm-sub)# snsr-grp 200 sample-interval 20000
switch(conf-tm-sub)# dst-grp 100
switch(conf-tm-sub)# dst-grp 200

switch(conf-tm-dest)# subscription 900
switch(conf-tm-sub)# snsr-grp 200 sample-interval 7000
switch(conf-tm-sub)# snsr-grp 300 sample-interval 0
switch(conf-tm-sub)# dst-grp 100
```

```
switch(conf-tm-sub)# dst-grp 300
```

You can verify the telemetry configuration using the **show running-config telemetry** command, as shown in this example.

```
switch(config)# telemetry
switch(config-telemetry)# destination-group 100
switch(conf-tm-dest)# ip address 1.2.3.4 port 50003
switch(conf-tm-dest)# ip address 1.2.3.4 port 50004
switch(conf-tm-dest)# end
switch# show run telemetry

!Command: show running-config telemetry
!Time: Thu Oct 13 21:10:12 2016

version 7.0(3)I5(1)
feature telemetry

telemetry
destination-group 100
ip address 1.2.3.4 port 50003 protocol gRPC encoding GPB
ip address 1.2.3.4 port 50004 protocol gRPC encoding GPB
```

You can specify transport VRF and telemetry data compression for gRPC using the **use-vrf** and **use-compression gzip** commands, as shown in this example.

```
switch(config)# telemetry
switch(config-telemetry)# destination-profile
switch(conf-tm-dest-profile)# use-vrf default
switch(conf-tm-dest-profile)# use-compression gzip
switch(conf-tm-dest-profile)# sensor-group 1
switch(conf-tm-sensor)# path sys/bgp depth unbounded
switch(conf-tm-sensor)# destination-group 1
switch(conf-tm-dest)# ip address 1.2.3.4 port 50004
switch(conf-tm-dest)# subscription 1
switch(conf-tm-sub)# dst-grp 1
switch(conf-tm-sub)# snsr-grp 1 sample-interval 10000
```

## Displaying Telemetry Configuration and Statistics

Use the following NX-OS CLI **show** commands to display telemetry configuration, statistics, errors, and session information.

### show telemetry control database

This command displays the internal databases that reflect the configuration of telemetry.

```
switch# show telemetry control database ?
<CR>
> Redirect it to a file
>> Redirect it to a file in append mode
destination-groups Show destination-groups
destinations Show destinations
sensor-groups Show sensor-groups
sensor-paths Show sensor-paths
subscriptions Show subscriptions
| Pipe command output to filter
```

```
switch# show telemetry control database
```

```
Subscription Database size = 1
```

```
-----
Subscription ID      Data Collector Type
-----
100                  DME NX-API
```

```
Sensor Group Database size = 1
```

```
-----
Sensor Group ID  Sensor Group type  Sampling interval(ms)  Linked subscriptions
-----
100              Timer              10000 (Running)        1
```

```
Sensor Path Database size = 1
```

```
-----
Subscribed Query Filter  Linked Groups  Sec Groups  Retrieve level  Sensor Path
-----
No                        1              0           Full            sys/fm
```

```
Destination group Database size = 2
```

```
-----
Destination Group ID  Refcount
-----
100                   1
```

```
Destination Database size = 2
```

```
-----
Dst IP Addr      Dst Port  Encoding  Transport  Count
-----
192.168.20.111   12345     JSON      HTTP       1
192.168.20.123  50001     GPB       gRPC       1
```

### show telemetry control stats

This command displays the statistic regarding the internal databases regarding configuration of telemetry.

```
switch# show telemetry control stats
show telemetry control stats entered
```

```
-----
Error Description                                     Error Count
-----
Chunk allocation failures                             0
Sensor path Database chunk creation failures         0
Sensor Group Database chunk creation failures        0
Destination Database chunk creation failures         0
Destination Group Database chunk creation failures   0
Subscription Database chunk creation failures        0
Sensor path Database creation failures               0
Sensor Group Database creation failures              0
Destination Database creation failures               0
Destination Group Database creation failures         0
Subscription Database creation failures              0
Sensor path Database insert failures                 0
Sensor Group Database insert failures                0
```

```

Destination Database insert failures 0
Destination Group Database insert failures 0
Subscription insert to Subscription Database failures 0
Sensor path Database delete failures 0
Sensor Group Database delete failures 0
Destination Database delete failures 0
Destination Group Database delete failures 0
Delete Subscription from Subscription Database failures 0
Sensor path delete in use 0
Sensor Group delete in use 0
Destination delete in use 0
Destination Group delete in use 0
Delete destination(in use) failure count 0
Failed to get encode callback 0
Sensor path Sensor Group list creation failures 0
Sensor path prop list creation failures 0
Sensor path sec Sensor path list creation failures 0
Sensor path sec Sensor Group list creation failures 0
Sensor Group Sensor path list creation failures 0
Sensor Group Sensor subs list creation failures 0
Destination Group subs list creation failures 0
Destination Group Destinations list creation failures 0
Destination Destination Groups list creation failures 0
Subscription Sensor Group list creation failures 0
Subscription Destination Groups list creation failures 0
Sensor Group Sensor path list delete failures 0
Sensor Group Subscriptions list delete failures 0
Destination Group Subscriptions list delete failures 0
Destination Group Destinations list delete failures 0
Subscription Sensor Groups list delete failures 0
Subscription Destination Groups list delete failures 0
Destination Destination Groups list delete failures 0
Failed to delete Destination from Destination Group 0
Failed to delete Destination Group from Subscription 0
Failed to delete Sensor Group from Subscription 0
Failed to delete Sensor path from Sensor Group 0
Failed to get encode callback 0
Failed to get transport callback 0
switch# Destination Database size = 1

```

```

-----
Dst IP Addr      Dst Port  Encoding  Transport  Count
-----
192.168.20.123  50001    GPB       gRPC       1
-----

```

### show telemetry data collector brief

This command displays the brief statistic regarding the data collection.

```
switch# show telemetry data collector brief
```

```

-----
Collector Type      Successful Collections  Failed Collections
-----
DME                 143                     0
-----

```

### show telemetry data collector details

This command displays details statistic regarding the data collection which includes breakdown of all sensor paths.

```
switch# show telemetry data collector details
```

```
-----
Succ Collections      Failed Collections      Sensor Path
-----
150                   0                       sys/fm
```

### show telemetry event collector errors

This command displays the errors statistic regarding the event collection.

```
switch# show telemetry event collector errors
```

```
-----
Error Description  Error Count
-----
APIC-Cookie Generation Failures                          - 0
Authentication Failures                                  - 0
Authentication Refresh Failures                          - 0
Authentication Refresh Timer Start Failures              - 0
Connection Timer Start Failures                          - 0
Connection Attempts                                      - 3
Dme Event Subscription Init Failures                     - 0
Event Data Enqueue Failures                              - 0
Event Subscription Failures                              - 0
Event Subscription Refresh Failures                      - 0
Pending Subscription List Create Failures                 - 0
Subscription Hash Table Create Failures                   - 0
Subscription Hash Table Destroy Failures                  - 0
Subscription Hash Table Insert Failures                   - 0
Subscription Hash Table Remove Failures                   - 0
Subscription Refresh Timer Start Failures                 - 0
Websocket Connect Failures                               - 0
```

### show telemetry event collector stats

This command displays the statistic regarding the event collection which includes breakdown of all sensor paths.

```
switch# show telemetry event collector stats
```

```
-----
Collection Count  Latest Collection Time  Sensor Path
-----
```

### show telemetry control pipeline stats

This command displays the statistic for the telemetry pipeline.

```
switch# show telemetry pipeline stats
Main Statistics:
  Timers:
    Errors:
      Start Fail      =      0

  Data Collector:
```

```

Errors:
  Node Create Fail = 0

Event Collector:
  Errors:
    Node Create Fail = 0    Node Add Fail = 0
    Invalid Data = 0

Queue Statistics:
  Request Queue:
    High Priority Queue:
      Info:
        Actual Size = 50    Current Size = 0
        Max Size = 0      Full Count = 0

      Errors:
        Enqueue Error = 0    Dequeue Error = 0

    Low Priority Queue:
      Info:
        Actual Size = 50    Current Size = 0
        Max Size = 0      Full Count = 0

      Errors:
        Enqueue Error = 0    Dequeue Error = 0

  Data Queue:
    High Priority Queue:
      Info:
        Actual Size = 50    Current Size = 0
        Max Size = 0      Full Count = 0

      Errors:
        Enqueue Error = 0    Dequeue Error = 0

    Low Priority Queue:
      Info:
        Actual Size = 50    Current Size = 0
        Max Size = 0      Full Count = 0

      Errors:
        Enqueue Error = 0    Dequeue Error = 0

```

**show telemetry transport**

This command displays all configured transport sessions.

```
switch# show telemetry transport
```

Session Id	IP Address	Port	Encoding	Transport	Status
0	192.168.20.123	50001	GPB	gRPC	Connected

**show telemetry transport <session-id>**

This command displays detailed session information for a specific transport session.

```
switch# show telemetry transport 0
```

```
Session Id: 0
```

```

IP Address:Port      192.168.20.123:50001
Encoding:            GPB
Transport:           gRPC
Status:              Disconnected
Last Connected:     Fri Sep 02 11:45:57.505 UTC
Tx Error Count:     224
Last Tx Error:      Fri Sep 02 12:23:49.555 UTC

```

```
switch# show telemetry transport 1
```

```

Session Id:         1
IP Address:Port    10.30.218.56:51235
Encoding:          JSON
Transport:         HTTP
Status:            Disconnected
Last Connected:    Never
Last Disconnected: Never
Tx Error Count:    3
Last Tx Error:     Wed Apr 19 15:56:51.617 PDT

```

### show telemetry transport <session-id> stats

This command displays details of a specific transport session.

```
switch# show telemetry transport 0 stats
```

```

Session Id:         0
IP Address:Port    192.168.20.123:50001
Encoding:          GPB
Transport:         GRPC
Status:            Connected
Last Connected:    Mon May 01 11:29:46.912 PST
Last Disconnected: Never
Tx Error Count:    0
Last Tx Error:     None

```

### show telemetry transport <session-id> errors

This command displays detailed error statistics for a specific transport session.

```
switch# show telemetry transport 0 errors
```

```

Session Id:         0
Connection Stats
  Connection Count   1
  Last Connected:    Mon May 01 11:29:46.912 PST
  Disconnect Count   0
  Last Disconnected: Never
Transmission Stats
  Transmit Count:    1225
  Last TX time:      Tue May 02 11:40:03.531 PST
  Min Tx Time:       7 ms
  Max Tx Time:       1760 ms
  Avg Tx Time:       500 ms

```

## Displaying Telemetry Log and Trace Information

Use the following NX-OS CLI commands to display the log and trace information.

**show tech-support telemetry**

This NX-OS CLI command collects the telemetry log contents from the tech-support log. In this example, the command output is redirected into a file in bootflash.

```
switch# show tech-support telemetry > bootflash:tmst.log
```

**show system internal telemetry trace**

The **show system internal telemetry trace** [**tm-events** | **tm-errors** | **tm-logs** | **all**] command displays system internal telemetry trace information.

```
switch# show system internal telemetry trace all
Telemetry All Traces:
Telemetry Error Traces:
[07/26/17 15:22:29.156 UTC 1 28577] [3960399872][tm_cfg_api.c:367] Not able to destroy dest
  profile list for config node rc:-1610612714 reason:Invalid argument
[07/26/17 15:22:44.972 UTC 2 28577] [3960399872][tm_stream.c:248] No subscriptions for
  destination group 1
[07/26/17 15:22:49.463 UTC 3 28577] [3960399872][tm_stream.c:576] TM_STREAM: Subscriptoin
  1 does not have any sensor groups
```

```
3 entries printed
Telemetry Event Traces:
[07/26/17 15:19:40.610 UTC 1 28577] [3960399872][tm_debug.c:41] Telemetry xostrace buffers
  initialized successfully!
[07/26/17 15:19:40.610 UTC 2 28577] [3960399872][tm.c:744] Telemetry statistics created
  successfully!
[07/26/17 15:19:40.610 UTC 3 28577] [3960399872][tm_init_n9k.c:97] Platform intf:
  grpc_traces:compression,channel
switch#
```

```
switch# show system internal telemetry trace tm-logs
```

```
Telemetry Log Traces:
0 entries printed
switch#
```

```
switch# show system internal telemetry trace tm-events
```

```
Telemetry Event Traces:
[07/26/17 15:19:40.610 UTC 1 28577] [3960399872][tm_debug.c:41] Telemetry xostrace buffers
  initialized successfully!
[07/26/17 15:19:40.610 UTC 2 28577] [3960399872][tm.c:744] Telemetry statistics created
  successfully!
[07/26/17 15:19:40.610 UTC 3 28577] [3960399872][tm_init_n9k.c:97] Platform intf:
  grpc_traces:compression,channel
[07/26/17 15:19:40.610 UTC 4 28577] [3960399872][tm_init_n9k.c:207] Adding telemetry to
  cgroup
[07/26/17 15:19:40.670 UTC 5 28577] [3960399872][tm_init_n9k.c:215] Added telemetry to
  cgroup successfully!
```

```
switch# show system internal telemetry trace tm-errors
```

```
Telemetry Error Traces:
0 entries printed
switch#
```

# Configuring Telemetry Using the NX-API

## Configuring Telemetry Using the NX-API

In the object model of the switch DME, the configuration of the telemetry feature is defined in a hierarchical structure of objects as shown in [Telemetry Model in the DME, on page 165](#). Following are the main objects to be configured:

- **fmEntity** — Contains the NX-API and Telemetry feature states.
  - **fmNxapi** — Contains the NX-API state.
  - **fmTelemetry** — Contains the Telemetry feature state.
- **telemetryEntity** — Contains the telemetry feature configuration.
  - **telemetrySensorGroup** — Contains the definitions of one or more sensor paths or nodes to be monitored for telemetry. The telemetry entity can contain one or more sensor groups.
    - **telemetryRtSensorGroupRel** — Associates the sensor group with a telemetry subscription.
    - **telemetrySensorPath** — A path to be monitored. The sensor group can contain multiple objects of this type.
  - **telemetryDestGroup** — Contains the definitions of one or more destinations to receive telemetry data. The telemetry entity can contain one or more destination groups.
    - **telemetryRtDestGroupRel** — Associates the destination group with a telemetry subscription.
    - **telemetryDest** — A destination address. The destination group can contain multiple objects of this type.
  - **telemetrySubscription** — Specifies how and when the telemetry data from one or more sensor groups is sent to one or more destination groups.
    - **telemetryRsDestGroupRel** — Associates the telemetry subscription with a destination group.
    - **telemetryRsSensorGroupRel** — Associates the telemetry subscription with a sensor group.
  - **telemetryCertificate** — Associates the telemetry subscription with a certificate and hostname.

To configure the telemetry feature using the NX-API, you must construct a JSON representation of the telemetry object structure and push it to the DME with an HTTP or HTTPS POST operation.



---

**Note** For detailed instructions on using the NX-API, see the *Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference*.

---

### Before you begin

Your switch must be configured to run the NX-API from the CLI:

```
switch(config)# feature nxapi

nxapi use-vrf vrf_name
nxapi http port port_number
```

## SUMMARY STEPS

1. Enable the telemetry feature.
2. Create the root level of the JSON payload to describe the telemetry configuration.
3. Create a sensor group to contain the defined sensor paths.
4. (Optional) Add an SSL/TLS certificate and a host.
5. Define a telemetry destination group.
6. Define a telemetry destination profile.
7. Define one or more telemetry destinations, consisting of an IP address and port number to which telemetry data will be sent.
8. Enable gRPC chunking and set the chunking size, between 64 and 4096 bytes.
9. Create a telemetry subscription to configure the telemetry behavior.
10. Add the sensor group object as a child object to the **telemetrySubscription** element under the root element (**telemetryEntity**).
11. Create a relation object as a child object of the subscription to associate the subscription to the telemetry sensor group and to specify the data sampling behavior.
12. Define one or more sensor paths or nodes to be monitored for telemetry.
13. Add sensor paths as child objects to the sensor group object (**telemetrySensorGroup**).
14. Add destinations as child objects to the destination group object (**telemetryDestGroup**).
15. Add the destination group object as a child object to the root element (**telemetryEntity**).
16. Create a relation object as a child object of the telemetry sensor group to associate the sensor group to the subscription.
17. Create a relation object as a child object of the telemetry destination group to associate the destination group to the subscription.
18. Create a relation object as a child object of the subscription to associate the subscription to the telemetry destination group.
19. Send the resulting JSON structure as an HTTP/HTTPS POST payload to the NX-API endpoint for telemetry configuration.

## DETAILED STEPS

	Command or Action	Purpose
Step 1	Enable the telemetry feature. <b>Example:</b> <pre>{   "fmEntity" : {     "children" : [{       "fmTelemetry" : {         "attributes" : {           "adminSt" : "enabled"         }       }     ]   } }</pre>	The root element is <b>fmTelemetry</b> and the base path for this element is <code>sys/fm</code> . Configure the <b>adminSt</b> attribute as <code>enabled</code> .

	Command or Action	Purpose
	<pre>     ]   } } </pre>	
<b>Step 2</b>	<p>Create the root level of the JSON payload to describe the telemetry configuration.</p> <p><b>Example:</b></p> <pre> {   "telemetryEntity": {     "attributes": {       "dn": "sys/tm"     },   } } </pre>	<p>The root element is <b>telemetryEntity</b> and the base path for this element is <code>sys/tm</code>. Configure the <b>dn</b> attribute as <code>sys/tm</code>.</p>
<b>Step 3</b>	<p>Create a sensor group to contain the defined sensor paths.</p> <p><b>Example:</b></p> <pre> "telemetrySensorGroup": {   "attributes": {     "id": "10",     "rn": "sensor-10"   },   "dataSrc": "NX-API",   "children": [{   }] } </pre>	<p>A telemetry sensor group is defined in an object of class <b>telemetrySensorGroup</b>. Configure the following attributes of the object:</p> <ul style="list-style-type: none"> <li>• <b>id</b> — An identifier for the sensor group. Currently only numeric ID values are supported.</li> <li>• <b>rn</b> — The relative name of the sensor group object in the format: <b>sensor-<i>id</i></b>.</li> <li>• <b>dataSrc</b> — Selects the data source from <b>DEFAULT</b>, <b>DME</b>, or <b>NX-API</b>.</li> </ul> <p>Children of the sensor group object will include sensor paths and one or more relation objects (<b>telemetryRtSensorGroupRel</b>) to associate the sensor group with a telemetry subscription.</p>
<b>Step 4</b>	<p>(Optional) Add an SSL/TLS certificate and a host.</p> <p><b>Example:</b></p> <pre> {   "telemetryCertificate": {     "attributes": {       "filename": "root.pem"       "hostname": "c.com"     }   } } </pre>	<p>The <b>telemetryCertificate</b> defines the location of the SSL/TLS certificate with the telemetry subscription/destination.</p>
<b>Step 5</b>	<p>Define a telemetry destination group.</p> <p><b>Example:</b></p> <pre> {   "telemetryDestGroup": {     "attributes": {       "id": "20"     }   } } </pre>	<p>A telemetry destination group is defined in <b>telemetryEntity</b>. Configure the <b>id</b> attribute.</p>

	Command or Action	Purpose
<b>Step 6</b>	Define a telemetry destination profile. <b>Example:</b> <pre data-bbox="253 405 862 806"> {   "telemetryDestProfile": {     "attributes": {       "adminSt": "enabled"     },     "children": [       {         "telemetryDestOptSourceInterface": {           "attributes": {             "name": "lo0"           }         }       ]     ]   } } </pre>	A telemetry destination profile is defined in <b>telemetryDestProfile</b> . <ul data-bbox="911 365 1487 541" style="list-style-type: none"> <li>• Configure the <b>adminSt</b> attribute as <i>enabled</i>.</li> <li>• Under <b>telemetryDestOptSourceInterface</b>, configure the <b>name</b> attribute with an interface name to stream data from the configured interface to a destination with the source IP address.</li> </ul>
<b>Step 7</b>	Define one or more telemetry destinations, consisting of an IP address and port number to which telemetry data will be sent. <b>Example:</b> <pre data-bbox="253 1041 837 1314"> {   "telemetryDest": {     "attributes": {       "addr": "1.2.3.4",       "enc": "GPB",       "port": "50001",       "proto": "gRPC",       "rn": "addr-[1.2.3.4]-port-50001"     }   } } </pre>	A telemetry destination is defined in an object of class <b>telemetryDest</b> . Configure the following attributes of the object: <ul data-bbox="911 968 1487 1619" style="list-style-type: none"> <li>• <b>addr</b> — The IP address of the destination.</li> <li>• <b>port</b> — The port number of the destination.</li> <li>• <b>rn</b> — The relative name of the destination object in the format: <b>path-[path]</b>.</li> <li>• <b>enc</b> — The encoding type of the telemetry data to be sent. NX-OS supports:               <ul data-bbox="963 1234 1487 1367" style="list-style-type: none"> <li>• Google protocol buffers (GPB) for gRPC.</li> <li>• JSON for C.</li> <li>• GPB or JSON for UDP and secure UDP (DTLS).</li> </ul> </li> <li>• <b>proto</b> — The transport protocol type of the telemetry data to be sent. NX-OS supports:               <ul data-bbox="963 1486 1487 1619" style="list-style-type: none"> <li>• gRPC</li> <li>• HTTP</li> <li>• VUDP and secure UDP (DTLS)</li> </ul> </li> </ul>
<b>Step 8</b>	Enable gRPC chunking and set the chunking size, between 64 and 4096 bytes. <b>Example:</b> <pre data-bbox="253 1829 269 1850"> { </pre>	See <a href="#">Support for gRPC Chunking, on page 137</a> for more information.

	Command or Action	Purpose
	<pre> "telemetryDestGrpOptChunking": {   "attributes": {     "chunkSize": "2048",     "dn": "sys/tm/dest-1/chunking"   } } </pre>	
<b>Step 9</b>	<p>Create a telemetry subscription to configure the telemetry behavior.</p> <p><b>Example:</b></p> <pre> "telemetrySubscription": {   "attributes": {     "id": "30",     "rn": "subs-30"   },   "children": [{   } } </pre>	<p>A telemetry subscription is defined in an object of class <b>telemetrySubscription</b>. Configure the following attributes of the object:</p> <ul style="list-style-type: none"> <li>• <b>id</b> — An identifier for the subscription. Currently only numeric ID values are supported.</li> <li>• <b>rn</b> — The relative name of the subscription object in the format: <b>subs-id</b>.</li> </ul> <p>Children of the subscription object will include relation objects for sensor groups (<b>telemetryRsSensorGroupRel</b>) and destination groups (<b>telemetryRsDestGroupRel</b>).</p>
<b>Step 10</b>	<p>Add the sensor group object as a child object to the <b>telemetrySubscription</b> element under the root element (<b>telemetryEntity</b>).</p> <p><b>Example:</b></p> <pre> {   "telemetrySubscription": {     "attributes": {       "id": "30"     }   },   "children": [{     "telemetryRsSensorGroupRel": {       "attributes": {         "sampleIntvl": "5000",         "tDn": "sys/tm/sensor-10"       }     }   ] } </pre>	
<b>Step 11</b>	<p>Create a relation object as a child object of the subscription to associate the subscription to the telemetry sensor group and to specify the data sampling behavior.</p> <p><b>Example:</b></p> <pre> "telemetryRsSensorGroupRel": {   "attributes": {     "rType": "mo",     "rn": "rssensorGroupRel-[sys/tm/sensor-10]",     "sampleIntvl": "5000",     "tCl": "telemetrySensorGroup", </pre>	<p>The relation object is of class <b>telemetryRsSensorGroupRel</b> and is a child object of <b>telemetrySubscription</b>. Configure the following attributes of the relation object:</p> <ul style="list-style-type: none"> <li>• <b>rn</b> — The relative name of the relation object in the format: <b>rssensorGroupRel-[sys/tm/sensor-group-id]</b>.</li> <li>• <b>sampleIntvl</b> — The data sampling period in milliseconds. An interval value of 0 creates an event-based subscription, in which telemetry data is sent only upon changes under the specified MO. An</li> </ul>

	Command or Action	Purpose
	<pre>         "tDn": "sys/tm/sensor-10",         "tType": "mo"       }     }   } </pre>	<p>interval value greater than 0 creates a frequency-based subscription, in which telemetry data is sent periodically at the specified interval. For example, an interval value of 15000 results in the sending of telemetry data every 15 seconds.</p> <ul style="list-style-type: none"> <li>• <b>tCl</b> — The class of the target (sensor group) object, which is <b>telemetrySensorGroup</b>.</li> <li>• <b>tDn</b> — The distinguished name of the target (sensor group) object, which is <b>sys/tm/sensor-group-id</b>.</li> <li>• <b>rType</b> — The relation type, which is <b>mo</b> for managed object.</li> <li>• <b>tType</b> — The target type, which is <b>mo</b> for managed object.</li> </ul>
<p><b>Step 12</b></p>	<p>Define one or more sensor paths or nodes to be monitored for telemetry.</p> <p><b>Example:</b></p> <p>Single sensor path</p> <pre> {   "telemetrySensorPath": {     "attributes": {       "path": "sys/cdp",       "rn": "path-[sys/cdp]",       "excludeFilter": "",       "filterCondition": "",       "path": "sys/fm/bgp",       "secondaryGroup": "0",       "secondaryPath": "",       "depth": "0"     }   } } </pre> <p><b>Example:</b></p> <p>Single sensor path for NX-API</p> <pre> {   "telemetrySensorPath": {     "attributes": {       "path": "show interface",       "path": "show bgp",       "rn": "path-[sys/cdp]",       "excludeFilter": "",       "filterCondition": "",       "path": "sys/fm/bgp",       "secondaryGroup": "0",       "secondaryPath": "",       "depth": "0"     }   } } </pre>	<p>A sensor path is defined in an object of class <b>telemetrySensorPath</b>. Configure the following attributes of the object:</p> <ul style="list-style-type: none"> <li>• <b>path</b> — The path to be monitored.</li> <li>• <b>rn</b> — The relative name of the path object in the format: <b>path-[path]</b></li> <li>• <b>depth</b> — The retrieval level for the sensor path. A depth setting of <b>0</b> retrieves only the root MO properties.</li> <li>• <b>filterCondition</b> — (Optional) Creates a specific filter for event-based subscriptions. The DME provides the filter expressions. For more information regarding filtering, see the Cisco APIC REST API Usage Guidelines on composing queries:  <a href="https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html#d25e1534a1635">https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html#d25e1534a1635</a></li> </ul>

	Command or Action	Purpose
	<pre> } }  <b>Example:</b> Multiple sensor paths  {   "telemetrySensorPath": {     "attributes": {       "path": "sys/cdp",       "rn": "path-[sys/cdp]",       "excludeFilter": "",       "filterCondition": "",       "path": "sys/fm/bgp",       "secondaryGroup": "0",       "secondaryPath": "",       "depth": "0"     }   } }, {   "telemetrySensorPath": {     "attributes": {       "excludeFilter": "",       "filterCondition": "",       "path": "sys/fm/dhcp",       "secondaryGroup": "0",       "secondaryPath": "",       "depth": "0"     }   } } </pre> <p><b>Example:</b> Single sensor path filtering for BGP disable events:</p> <pre> {   "telemetrySensorPath": {     "attributes": {       "path": "sys/cdp",       "rn": "path-[sys/cdp]",       "excludeFilter": "",       "filterCondition": "eq(fmBgp.operSt.\"disabled\")",       "path": "sys/fm/bgp",       "secondaryGroup": "0",       "secondaryPath": "",       "depth": "0"     }   } } </pre>	
<p><b>Step 13</b></p>	<p>Add sensor paths as child objects to the sensor group object (<b>telemetrySensorGroup</b>).</p>	

	Command or Action	Purpose
<b>Step 14</b>	Add destinations as child objects to the destination group object ( <b>telemetryDestGroup</b> ).	
<b>Step 15</b>	Add the destination group object as a child object to the root element ( <b>telemetryEntity</b> ).	
<b>Step 16</b>	<p>Create a relation object as a child object of the telemetry sensor group to associate the sensor group to the subscription.</p> <p><b>Example:</b></p> <pre>"telemetryRtSensorGroupRel": {   "attributes": {     "rn": "rtsensorGroupRel-[sys/tm/subs-30]",      "tCl": "telemetrySubscription",     "tDn": "sys/tm/subs-30"   } }</pre>	<p>The relation object is of class <b>telemetryRtSensorGroupRel</b> and is a child object of <b>telemetrySensorGroup</b>. Configure the following attributes of the relation object:</p> <ul style="list-style-type: none"> <li>• <b>rn</b> — The relative name of the relation object in the format: <b>rtsensorGroupRel-[sys/tm/subscription-id]</b>.</li> <li>• <b>tCl</b> — The target class of the subscription object, which is <b>telemetrySubscription</b>.</li> <li>• <b>tDn</b> — The target distinguished name of the subscription object, which is <b>sys/tm/subscription-id</b>.</li> </ul>
<b>Step 17</b>	<p>Create a relation object as a child object of the telemetry destination group to associate the destination group to the subscription.</p> <p><b>Example:</b></p> <pre>"telemetryRtDestGroupRel": {   "attributes": {     "rn": "rtdestGroupRel-[sys/tm/subs-30]",     "tCl": "telemetrySubscription",     "tDn": "sys/tm/subs-30"   } }</pre>	<p>The relation object is of class <b>telemetryRtDestGroupRel</b> and is a child object of <b>telemetryDestGroup</b>. Configure the following attributes of the relation object:</p> <ul style="list-style-type: none"> <li>• <b>rn</b> — The relative name of the relation object in the format: <b>rtdestGroupRel-[sys/tm/subscription-id]</b>.</li> <li>• <b>tCl</b> — The target class of the subscription object, which is <b>telemetrySubscription</b>.</li> <li>• <b>tDn</b> — The target distinguished name of the subscription object, which is <b>sys/tm/subscription-id</b>.</li> </ul>
<b>Step 18</b>	<p>Create a relation object as a child object of the subscription to associate the subscription to the telemetry destination group.</p> <p><b>Example:</b></p> <pre>"telemetryRsDestGroupRel": {   "attributes": {     "rType": "mo",     "rn": "rsdestGroupRel-[sys/tm/dest-20]",     "tCl": "telemetryDestGroup",     "tDn": "sys/tm/dest-20",     "tType": "mo"   } }</pre>	<p>The relation object is of class <b>telemetryRsDestGroupRel</b> and is a child object of <b>telemetrySubscription</b>. Configure the following attributes of the relation object:</p> <ul style="list-style-type: none"> <li>• <b>rn</b> — The relative name of the relation object in the format: <b>rsdestGroupRel-[sys/tm/destination-group-id]</b>.</li> <li>• <b>tCl</b> — The class of the target (destination group) object, which is <b>telemetryDestGroup</b>.</li> <li>• <b>tDn</b> — The distinguished name of the target (destination group) object, which is <b>sys/tm/destination-group-id</b>.</li> <li>• <b>rType</b> — The relation type, which is <b>mo</b> for managed object.</li> <li>• <b>tType</b> — The target type, which is <b>mo</b> for managed object.</li> </ul>

	Command or Action	Purpose
Step 19	Send the resulting JSON structure as an HTTP/HTTPS POST payload to the NX-API endpoint for telemetry configuration.	The base path for the telemetry entity is <code>sys/tm</code> and the NX-API endpoint is:  <code>{{URL}}/api/node/mo/sys/tm.json</code>

### Example

The following is an example of all the previous steps collected into one POST payload (note that some attributes may not match):

```
{
  "telemetryEntity": {
    "children": [{
      "telemetrySensorGroup": {
        "attributes": {
          "id": "10"
        }
      }
    ]
  },
  {
    "telemetryDestGroup": {
      "attributes": {
        "id": "20"
      }
      "children": [{
        "telemetryDest": {
          "attributes": {
            "addr": "10.30.217.80",
            "port": "50051",
            "enc": "GPB",
            "proto": "gRPC"
          }
        }
      ]
    }
  },
  {
    "telemetrySubscription": {
      "attributes": {
        "id": "30"
      }
      "children": [{
        "telemetryRsSensorGroupRel": {
          "attributes": {
            "sampleIntvl": "5000",

```





```

    }
  ]]
}
}
}

```

### Filter Conditions on BGP Notifications

The following example payload enables notifications that trigger when the BFP feature is disabled as per the `filterCondition` attribute in the `telemetrySensorPath` MO. The data is streamed to 10.30.217.80 port 50055.

```
POST https://192.168.20.123/api/node/mo/sys/tm.json
```

Payload:

```

{
  "telemetryEntity": {
    "children": [{
      "telemetrySensorGroup": {
        "attributes": {
          "id": "10"
        }
      }
    ]
  },
  "telemetryDestGroup": {
    "attributes": {
      "id": "20"
    }
  },
  "telemetrySubscription": {
    "attributes": {
      "id": "30"
    }
  }
}

```



```

|         |         @name:depth
|         |         @type:RetrieveDepth
|
|-----mo [name:DestGroup]
|         |         @name:DestGroup
|         |         @label:Destination Group
|         |--property
|         |         @name:id
|         |         @type:string:Basic
|         |
|         |-----mo [name:Dest]
|         |         @name:Dest
|         |         @label:Destination
|         |--property
|         |         @name:addr [key]
|         |         @type:address:Ip
|         |         @name:port [key]
|         |         @type:scalar:Uint16
|         |         @name:proto
|         |         @type:Protocol
|         |         @name:enc
|         |         @type:Encoding
|
|-----mo [name:Subscription]
|         |         @name:Subscription
|         |         @label:Subscription
|         |--property
|         |         @name:id
|         |         @type:scalar:Uint64
|         |-----reldef
|         |         @name:SensorGroupRel
|         |         @to:SensorGroup
|         |         @cardinality:ntom
|         |         @label:Link to sensorGroup entry
|         |--property
|         |         @name:sampleIntvl
|         |         @type:scalar:Uint64
|         |
|         |-----reldef
|         |         @name:DestGroupRel
|         |         @to:DestGroup
|         |         @cardinality:ntom
|         |         @label:Link to destGroup entry

```

### DNs Available to Telemetry

For a list of DNs available to the telemetry feature, see [Streaming Telemetry Sources](#), on page 189.

## Additional References

### Related Documents

Related Topic	Document Title
Example configurations of telemetry deployment for VXLAN EVPN.	<a href="#">Telemetry Deployment for VXLAN EVPN Solution</a>



## CHAPTER 16

# XML Management Interface

---

This section contains the following topics:

- [About the XML Management Interface, on page 167](#)
- [Licensing Requirements for the XML Management Interface, on page 168](#)
- [Prerequisites to Using the XML Management Interface, on page 169](#)
- [Using the XML Management Interface, on page 169](#)
- [Information About Example XML Instances, on page 181](#)
- [Additional References, on page 187](#)

## About the XML Management Interface

### About the XML Management Interface

You can use the XML management interface to configure a device. The interface uses the XML-based Network Configuration Protocol (NETCONF), which allows you to manage devices and communicate over the interface with an XML management tool or program. The Cisco NX-OS implementation of NETCONF requires you to use a Secure Shell (SSH) session for communication with the device.

NETCONF is implemented with an XML Schema (XSD) that allows you to enclose device configuration elements within a remote procedure call (RPC) message. From within an RPC message, you select one of the NETCONF operations that matches the type of command that you want the device to execute. You can configure the entire set of CLI commands on the device with NETCONF. For information about using NETCONF, see the [Creating NETCONF XML Instances, on page 171](#) and [RFC 4741](#).

For more information about using NETCONF over SSH, see [RFC 4742](#).

This section includes the following topics:

- [NETCONF Layers, on page 167](#)
- [SSH xmlagent, on page 168](#)

### NETCONF Layers

The following are the NETCONF layers:

Table 14: NETCONF Layers

Layer	Example
Transport protocol	SSHv2
RPC	<rpc>, <rpc-reply>
Operations	<get-config>, <edit-config>
Content	show or configuration command

The following is a description of the four NETCONF layers:

- SSH transport protocol—Provides a secure, encrypted connection between a client and the server.
- RPC tag—Introduces a configuration command from the requestor and the corresponding reply from the XML server.
- NETCONF operation tag—Indicates the type of configuration command.
- Content—Indicates the XML representation of the feature that you want to configure.

## SSH xmlagent

The device software provides an SSH service that is called xmlagent that supports NETCONF over SSH Version 2.



**Note** The xmlagent service is referred to as the XML server in the Cisco NX-OS software.

NETCONF over SSH starts with the exchange of a hello message between the client and the XML server. After the initial exchange, the client sends XML requests, which the server responds to with XML responses. The client and server terminate requests and responses with the character sequence >. Because this character sequence is not valid in XML, the client and the server can interpret when the messages end, which keeps communication in sync.

The XML schemas that define XML configuration instances that you can use are described in the [Creating NETCONF XML Instances, on page 171](#) section.

## Licensing Requirements for the XML Management Interface

Product	Product
Cisco NX-OS	The XML management interface requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

# Prerequisites to Using the XML Management Interface

The XML management interface has the following prerequisites:

- You must install SSHv2 on the client PC.
- You must install an XML management tool that supports NETCONF over SSH on the client PC.
- You must set the appropriate options for the XML server on the device.

## Using the XML Management Interface

This section describes how to manually configure and use the XML management interface. Use the XML management interface with the default settings on the device.

### Configuring SSH and the XML Server Options

By default, the SSH server is enabled on the device. If you disable SSH, you must enable it before you start an SSH session on the client PC.

You can configure XML server options to control the number of concurrent sessions and the timeout for active sessions. You can also enable XML document validation and terminate XML sessions.



---

**Note** The XML server timeout applies only to active sessions.

---

For more information about configuring SSH, see the Cisco NX-OS security configuration guide for your platform.

For more information about the XML commands, see the Cisco NX-OS system management configuration guide for your platform.

### Starting an SSH Session

You can start an SSHv2 session on the client PC with a command similar to the following:

```
ssh2 username@ip-address -s xmlagent
```

Enter the login username, the IP address of the device, and the service to connect to. The xmlagent service is referred to as the XML server in the device software.



---

**Note** The SSH command syntax can differ from the SSH software on the client PC.

---

If you do not receive a hello message from the XML server, verify the following conditions:

- The SSH server is enabled on the device.
- The XML server max-sessions option is adequate to support the number of SSH connections to the device.

- The active XML server sessions on the device are not all in use.

## Sending the Hello Message

When you start an SSH session to the XML server, the server responds immediately with a hello message that informs the client of the server's capabilities. You must advertise your capabilities to the server with a hello message before the server processes any other requests. The XML server supports only base capabilities and expects support only for the base capabilities from the client.

The following are sample hello messages from the server and the client.



**Note** You must end all XML documents with `]]>]]>` to support synchronization in NETCONF over SSH.

### Hello Message from the server

```
<?xml version="1.0"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capability>
  </capabilities>
  <session-id>25241</session-id>
</hello>]]>]]>
```

### Hello Message from the Client

```
<?xml version="1.0"?>
<nc:hello xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nc:capabilities>
    <nc:capability>urn:ietf:params:xml:ns:netconf:base:1.0</nc:capability>
  </nc:capabilities>
</nc:hello>]]>]]>
```

## Obtaining the XSD Files

- Step 1** From your browser, navigate to the Cisco software download site at the following URL:  
<http://software.cisco.com/download/navigator.html>  
The Download Software page opens.
- Step 2** In the Select a Product list, choose **Switches > Data Center Switches > platform > model**.
- Step 3** If you are not already logged in as a registered Cisco user, you are prompted to log in now.
- Step 4** From the Select a Software Type list, choose **NX-OS XML Schema Definition**.
- Step 5** Find the desired release and click **Download**.
- Step 6** If you are requested, follow the instructions to apply for eligibility to download strong encryption software images.

The Cisco End User License Agreement opens.

**Step 7** Click **Agree** and follow the instructions to download the file to your PC.

## Sending an XML Document to the XML Server

To send an XML document to the XML server through an SSH session that you opened in a command shell, you can copy the XML text from an editor and paste it into the SSH session. Although typically you use an automated method to send XML documents to the XML server, you can verify the SSH connection to the XML server with this method.

Follow these guidelines for this method:

- Verify that the XML server sent the hello message immediately after you started the SSH session by looking for the hello message text in the command shell output.
- Send the client hello message before you send any XML requests. Because the XML server sends the hello response immediately, no additional response is sent after you send the client hello message.
- Always terminate the XML document with the character sequence `]]>]]>`.

## Creating NETCONF XML Instances

You can create NETCONF XML instances by enclosing XML device elements within an RPC tag and NETCONF operation tags. The XML device elements are defined in feature-based XML schema definition (XSD) files, which enclose available CLI commands in an XML format.

The following are the tags that are used in the NETCONF XML request in a framework context. Tag lines are marked with the following letter codes:

- X—XML declaration
- R—RPC request tag
- N—NETCONF operation tags
- D—Device tags

### NETCONF XML Framework Context

```
X <?xml version="1.0"?>
R <nc:rpc message-id="1" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
  xmlns="http://www.cisco.com/nxos:1.0:nfcli">
N <nc:get>
N <nc:filter type="subtree">
D <show>
D <xml>
D <server>
D <status/>
D </server>
D </xml>
D </show>
N </nc:filter>
N </nc:get>
R </nc:rpc>]]>]]>
```



**Note** You must use your own XML editor or XML management interface tool to create XML instances.

## RPC Request Tag `rpc`

All NETCONF XML instances must begin with the RPC request tag `<rpc>`. The example *RPC Request Tag* `<rpc>` shows the `<rpc>` element with its required **message-id** attribute. The message-id attribute is replicated in the `<rpc-reply>` and can be used to correlate requests and replies. The `<rpc>` node also contains the following XML namespace declarations:

- NETCONF namespace declaration—The `<rpc>` and NETCONF tags that are defined in the "urn:ietf:params:xml:ns:netconf:base:1.0" namespace, are present in the netconf.xsd schema file.
- Device namespace declaration—Device tags encapsulated by the `<rpc>` and NETCONF tags are defined in other namespaces. Device namespaces are feature-oriented. Cisco NX-OS feature tags are defined in different namespaces. *RPC Request Tag* `<rpc>` is an example that uses the nfcli feature. It declares that the device namespace is "xmlns=http://www.cisco.com/nxos:1.0:nfcli". nfcli.xsd contains this namespace definition. For more information, see section on *Obtaining the XSD Files*.

### RPC Tag Request

```
<nc:rpc message-id="315" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns=http://www.cisco.com/nxos:1.0:nfcli">
...
</nc:rpc>]]>]]>
```

### Configuration Request

The following is an example of a configuration request.

```
<?xml version="1.0"?>
<nc:rpc message-id="16" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0:if_manager">
  <nc:edit-config>
    <nc:target>
      <nc:running/>
    </nc:target>
    <nc:config>
      <configure>
        <__XML__MODE__exec_configure>
          <interface>
            <ethernet>
              <interface>2/30</interface>
              <__XML__MODE_if-ethernet>
                <__XML__MODE_if-eth-base>
                  <description>
                    <desc_line>Marketing Network</desc_line>
                  </description>
                </__XML__MODE_if-eth-base>
              </__XML__MODE_if-ethernet>
            </ethernet>
          </interface>
        </__XML__MODE__exec_configure>
      </configure>
    </nc:config>
  </nc:edit-config>
</nc:rpc>]]>]]>
```

\_\_XML\_\_MODE tags are used internally by the NETCONF agent. Some tags are present only as children of a certain \_\_XML\_\_MODE. By examining the schema file, you can find the correct mode tag that leads to the tags representing the CLI command in XML.

## NETCONF Operations Tags

NETCONF provides the following configuration operations:

**Table 15: NETCONF Operations in Cisco NX-OS**

NETCONF Operation	Description	Example
close-session	Closes the current XML server session.	<a href="#">NETCONF Close Session Instance, on page 181</a>
commit	Sets the running configuration to the current contents of the candidate configuration.	<a href="#">NETCONF Commit Instance - Candidate Configuration Capability, on page 186</a>
confirmed-commit	Provides parameters to commit the configuration for a specified time. If this operation is not followed by a commit operation within the confirm-timeout period, the configuration is reverted to the state before the confirmed-commit operation.	<a href="#">NETCONF Confirmed-commit Instance , on page 186</a>
copy-config	Copies the content of source configuration datastore to the target datastore.	<a href="#">NETCONF copy-config Instance, on page 182</a>
delete-config	Operation not supported.	—
edit-config	Configures features in the running configuration of the device. You use this operation for configuration commands.	<a href="#">NETCONF edit-config Instance, on page 182</a> <a href="#">NETCONF rollback-on-error Instance , on page 186</a>
get	Receives configuration information from the device. You use this operation for <b>show</b> commands. The source of the data is the running configuration.	<a href="#">Creating NETCONF XML Instances, on page 171</a>
get-config	Retrieves all or part of a configuration	<a href="#">NETCONF get-config Instance, on page 184</a>
kill-session	Closes the specified XML server session. You cannot close your own session. See the close-session NETCONF operation.	<a href="#">NETCONF Kill-session Instance, on page 182</a>

NETCONF Operation	Description	Example
lock	Allows the client to lock the configuration system of a device.	<a href="#">NETCONF Lock Instance, on page 184</a>
unlock	Releases the configuration lock that the session issued.	<a href="#">NETCONF unlock Instance, on page 185</a>
validate	Checks a candidate configuration for syntactical and semantic errors before applying the configuration to the device.	<a href="#">NETCONF validate Capability Instance , on page 187</a>

## Device Tags

The XML device elements represent the available CLI commands in XML format. The feature-specific schema files contain the XML tags for CLI commands of that particular feature. See the [Obtaining the XSD Files, on page 170](#) section.

Using this schema, it is possible to build an XML instance. In the following examples, the relevant portions of the ncli.xsd schema file that was used to build [Creating NETCONF XML Instances, on page 171](#) is shown.

The following example shows XML device tags.

### show xml Device Tags

```
<xs:element name="show" type="show_type_Cmd_show_xml"/>
<xs:complexType name="show_type_Cmd_show_xml">
  <xs:annotation>
    <xs:documentation>to display xml agent information</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:choice maxOccurs="1">
      <xs:element name="xml" minOccurs="1" type="xml_type_Cmd_show_xml"/>
      <xs:element name="debug" minOccurs="1" type="debug_type_Cmd_show_debug"/>
    </xs:choice>
  </xs:sequence>
  <xs:attribute name="xpath-filter" type="xs:string"/>
  <xs:attribute name="uses-namespace" type="nxos:bool_true"/>
</xs:complexType>
```

The following example shows the server status device tags.

### server status Device Tags

```
<xs:complexType name="xml_type_Cmd_show_xml">
  <xs:annotation>
    <xs:documentation>xml agent</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="server" minOccurs="1" type="server_type_Cmd_show_xml"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="server_type_Cmd_show_xml">
  <xs:annotation>
    <xs:documentation>xml agent server</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:choice maxOccurs="1">
```

```

<xs:element name="status" minOccurs="1" type="status_type_Cmd_show_xml"/>
<xs:element name="logging" minOccurs="1" type="logging_type_Cmd_show_logging_facility"/>
</xs:choice>
</xs:sequence>
</xs:complexType>

```

The following example shows the device tag response.

### Device Tag Response

```

<xs:complexType name="status_type_Cmd_show_xml">
  <xs:annotation>
    <xs:documentation>display xml agent information</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="__XML_OPT_Cmd_show_xml__readonly__" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:group ref="og_Cmd_show_xml__readonly__" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<xs:group name="og_Cmd_show_xml__readonly__">
  <xs:sequence>
    <xs:element name="__readonly__" minOccurs="1" type="__readonly__type_Cmd_show_xml"/>
  </xs:sequence>
</xs:group>
<xs:complexType name="__readonly__type_Cmd_show_xml">
  <xs:sequence>
    <xs:group ref="bg_Cmd_show_xml_operational_status" maxOccurs="1"/>
    <xs:group ref="bg_Cmd_show_xml_maximum_sessions_configured" maxOccurs="1"/>
    <xs:group ref="og_Cmd_show_xml_TABLE_sessions" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>

```



**Note** “\_\_XML\_OPT\_Cmd\_show\_xml\_\_readonly\_\_” is optional. This tag represents the response. For more information on responses, see the [RPC Response Tag, on page 180](#) section.

You can use the | XML option to find the tags you can use to execute a <get>. The following is an example of the | XML option.

### XML Example

```

Switch#> show xml server status | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0:nfcli">
  <nf:data>
    <show>
      <xml>
        <server>
          <status>
            <__XML_OPT_Cmd_show_xml__readonly__>
              <__readonly__>
                <operational_status>
                  <o_status>enabled</o_status>
                </operational_status>
              <maximum_sessions_configured>

```

```

<max_session>8</max_session>
</maximum_sessions_configured>
</__readonly__>
</__XML_OPT_Cmd_show_xml__readonly__>
</status>
</server>
</xml>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

From this response, you can see that the namespace defining tag to execute operations on this component is `http://www.cisco.com/nxos:1.0:nfcli` and the `nfcli.xsd` file can be used to build requests for this feature.

You can enclose the NETCONF operation tags and the device tags within the RPC tag. The `</rpc>` end-tag is followed by the XML termination character sequence.

## Extended NETCONF Operations

Cisco NX-OS supports an `<rpc>` operation named `<exec-command>`. The operation allows client applications to send CLI configuration and show commands and to receive responses to those commands as XML tags.

The following is an example of the tags that are used to configure an interface. Tag lines are marked with the following letter codes:

- X—XML declaration
- R—RPC request tag
- EO—Extended operation

### Configuration CLI Commands Sent Through `<exec-command>`

```

X <?xml version="1.0"?>
R <nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="3">
EO <nxos:exec-command>
EO <nxos:cmd>conf t ; interface ethernet 2/1 </nxos:cmd>
EO <nxos:cmd>channel-group 2000 ; no shut; </nxos:cmd>
EO </nxos:exec-command>
R </nf:rpc>]]>]]>

```

The following is the response to the operation:

### Response to CLI Commands Sent Through `<exec-command>`

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="3">
<nf:ok/>
</nf:rpc-reply>
]]>]]>

```

The following example shows how the show CLI commands that are sent through the `<exec-command>` can be used to retrieve data.

**show CLI Commands Sent Through <exec-command>**

```
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="110">
<nxos:exec-command>
<nxos:cmd>show interface brief</nxos:cmd>
</nxos:exec-command>
</nf:rpc>]]>]]>
```

The following is the response to the operation.

**Response to the show CLI commands Sent Through <exec-command>**

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0"
xmlns:mod="http://www.cisco.com/nxos:1.0:if_manager" message-id="110">
<nf:data>
<mod:show>
<mod:interface>
<mod: __XML_OPT_Cmd_show_interface_brief__readonly__>
<mod: __readonly__>
<mod:TABLE_interface>
<mod:ROW_interface>
<mod:interface>mgmt0</mod:interface>
<mod:state>up</mod:state>
<mod:ip_addr>172.23.152.20</mod:ip_addr>
<mod:speed>1000</mod:speed>
<mod:mtu>1500</mod:mtu>
</mod:ROW_interface>
<mod:ROW_interface>
<mod:interface>Ethernet2/1</mod:interface>
<mod:vlan>--</mod:vlan>
<mod:type>eth</mod:type>
<mod:portmode>routed</mod:portmode>
<mod:state>down</mod:state>
<mod:state_rsn_desc>Administratively down</mod:state_rsn_desc>
<mod:speed>auto</mod:speed>
<mod:ratemode>D</mod:ratemode>
</mod:ROW_interface>
</mod:TABLE_interface>
</mod: __readonly__>
</mod: __XML_OPT_Cmd_show_interface_brief__readonly__>
</mod:interface>
</mod:show>
</nf:data>
</nf:rpc-reply>
]]>]]>
```

The following table provides a detailed explanation of the operation tags:

**Table 16: Tags**

Tag	Description
<exec-command>	Executes a CLI command.

Tag	Description
<cmd>	Contains the CLI command. A command can be a show or configuration command. Separate multiple configuration commands by using a semicolon “;”. Multiple show commands are not supported. You can send multiple configuration commands in different <cmd> tags as part of the same request. For more information, see the Example in <i>Configuration CLI Commands Sent Through &lt;exec-command&gt;</i> .

Replies to configuration commands that are sent through the <cmd> tag are as follows:

- <nf:ok>: All configure commands are executed successfully.
- <nf:rpc-error>: Some commands have failed. The operation stops on the first error, and the <nf:rpc-error> subtree provides more information on what configuration failed. Notice that any configuration that is executed before the failed command would have been applied to the running configuration.

The following example shows a failed configuration:

### Failed Configuration

```
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="3">
<nxos:exec-command>
<nxos:cmd>configure terminal ; interface ethernet2/1 </nxos:cmd>
<nxos:cmd>ip address 1.1.1.2/24 </nxos:cmd>
<nxos:cmd>no channel-group 2000 ; no shut; </nxos:cmd>
</nxos:exec-command>
</nf:rpc>]]]]>
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="3">
<nf:rpc-error>
<nf:error-type>application</nf:error-type>
<nf:error-tag>invalid-value</nf:error-tag>
<nf:error-severity>error</nf:error-severity>
<nf:error-message>Ethernet2/1: not part of port-channel 2000
</nf:error-message>
<nf:error-info>
<nf:bad-element>cmd</nf:bad-element>
</nf:error-info>
</nf:rpc-error>
</nf:rpc-reply>
]]]]>
```

Because of a command execution, the interface IP address is set, but the administrative state is not modified (the no shut command is not executed). The reason the administrative state is not modified is because the no port-channel 2000 command results in an error.

The <rpc-reply> results from a show command that is sent through the <cmd> tag that contains the XML output of the show command.

You cannot combine configuration and show commands on the same <exec-command> instance. The following example shows a configuration and **show** command that are combined in the same instance.

## Combination of Configuration and show Commands

```
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="110">
<nxos:exec-command>
<nxos:cmd>conf t ; interface ethernet 2/1 ; ip address 1.1.1.4/24 ; show xml
server status </nxos:cmd>
</nxos:exec-command>
</nf:rpc>]]>]]>
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="110">
<nf:rpc-error>
<nf:error-type>application</nf:error-type>
<nf:error-tag>invalid-value</nf:error-tag>
<nf:error-severity>error</nf:error-severity>
<nf:error-message>Error: cannot mix config and show in exec-command. Config cmds
before the show were executed.
Cmd:show xml server status</nf:error-message>
<nf:error-info>
<nf:bad-element>cmd</nf:bad-element>
</nf:error-info>
</nf:rpc-error>
</nf:rpc-reply>
]]>]]>
```

The show command must be sent in its own `<exec-command>` instance as shown in the following example:

## Show CLI Commands Sent Through `<exec-command>`

```
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="110">
<nxos:exec-command>
<nxos:cmd>show xml server status ; show xml server status </nxos:cmd>
</nxos:exec-command>
</nf:rpc>]]>]]>
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nxos="http://www.cisco.com/nxos:1.0" message-id="110">
<nf:rpc-error>
<nf:error-type>application</nf:error-type>
<nf:error-tag>invalid-value</nf:error-tag>
<nf:error-severity>error</nf:error-severity>
<nf:error-message>Error: show cmds in exec-command shouldn't be followed by anything
</nf:error-message>
<nf:error-info>
<nf:bad-element>&lt;cmd&gt;</nf:bad-element>
</nf:error-info>
</nf:rpc-error>
</nf:rpc-reply>
]]>]]>
```

## NETCONF Replies

For every XML request sent by the client, the XML server sends an XML response enclosed in the RPC response tag `<rpc-reply>`.

This section contains the following topics:

- [RPC Response Tag, on page 180](#)
- [Interpreting Tags Encapsulated in the Data Tag, on page 180](#)

## RPC Response Tag

The following example shows the RPC response tag `<rpc-reply>`.

### RPC Response Elements

```
<nc:rpc-reply message-id="315" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns=http://www.cisco.com/nxos:1.0:nfcli">
<ok/>
</nc:rpc-reply>]]]]>
```

The elements `<ok>`, `<data>`, and `<rpc-error>` can appear in the RPC response. The following table describes the RPC response elements that can appear in the `<rpc-reply>` tag.

**Table 17: RPC Response Elements**

Element	Description
<code>&lt;ok&gt;</code>	The RPC request completed successfully. This element is used when no data is returned in the response.
<code>&lt;data&gt;</code>	The RPC request completed successfully. The data associated with the RPC request is enclosed in the <code>&lt;data&gt;</code> element.
<code>&lt;rpc-error&gt;</code>	The RPC request failed. Error information is enclosed in the <code>&lt;rpc-error&gt;</code> element.

## Interpreting Tags Encapsulated in the Data Tag

The device tags encapsulated by the `<data>` tag contain the request followed by the response. A client application can safely ignore all tags before the `<readonly>` tag. The following is an example:

### RPC-reply data

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0:if_manager">
<nf:data>
<show>
<interface>
<__XML__OPT_Cmd_show_interface_brief__readonly__>
<__readonly__>
<TABLE_interface>
<ROW_interface>
<interface>mgmt0</interface>
<state>up</state>
<ip_addr>xx.xx.xx.xx</ip_addr>
<speed>1000</speed>
<mtu>1500</mtu>
</ROW_interface>
<ROW_interface>
<interface>Ethernet2/1</interface>
```

```

<vlan>--</vlan>
<type>eth</type>
<portmode>routed</portmode>
<state>down</state>
<state_rsn_desc>Administratively down</state_rsn_desc>
<speed>auto</speed>
<ratemode>D</ratemode>
</ROW_interface>
</TABLE_interface>
</__readonly__>
</__XML__OPT_Cmd_show_interface_brief__readonly__>
</interface>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

<\_\_XML\_\_OPT.\*> and <\_\_XML\_\_BLK.\*> appear in responses and are sometimes used in requests. These tags are used by the NETCONF agent and are present in responses after the <\_\_readonly\_\_> tag. They are necessary in requests and should be added according to the schema file to reach the XML tag that represents the CLI command.

## Information About Example XML Instances

### Example XML Instances

This section provides the examples of the following XML instances:

- [NETCONF Close Session Instance, on page 181](#)
- [NETCONF Kill-session Instance, on page 182](#)
- [NETCONF copy-config Instance, on page 182](#)
- [NETCONF edit-config Instance, on page 182](#)
- [NETCONF get-config Instance, on page 184](#)
- [NETCONF Lock Instance, on page 184](#)
- [NETCONF unlock Instance, on page 185](#)
- [NETCONF Commit Instance - Candidate Configuration Capability, on page 186](#)
- [NETCONF Confirmed-commit Instance, on page 186](#)
- [NETCONF rollback-on-error Instance, on page 186](#)
- [NETCONF validate Capability Instance, on page 187](#)

### NETCONF Close Session Instance

The following example shows the close-session request, followed by the close-session response.

#### Close-session Request

```

<?xml version="1.0"?>
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0">
<nc:close-session/>
</nc:rpc>]]>]]>

```

**Close-session Response**

```
<nc:rpc-reply xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0" message-id="101">
<nc:ok/>
</nc:rpc-reply>]]>]]>
```

**NETCONF Kill-session Instance**

The following example shows the kill-session request followed by the kill-session response.

**Kill-session Request**

```
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0">
<nc:kill-session>
<nc:session-id>25241</nc:session-id>
</nc:kill-session>
</nc:rpc>]]>]]>
```

**Kill-session Request**

```
<nc:rpc message-id="101" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0">
<nc:kill-session>
<nc:session-id>25241</nc:session-id>
</nc:kill-session>
</nc:rpc>]]>]]>
```

**NETCONF copy-config Instance**

The following example shows the copy-config request followed by the copy-config response.

**Copy-config Request**

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<copy-config>
<target>
<running/>
</target>
<source>
<url>https://user@example.com:passphrase/cfg/new.txt</url>
</source>
</copy-config>
</rpc>
```

**Copy-config Response**

```
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
```

**NETCONF edit-config Instance**

The following example shows the use of NETCONF edit-config.

## Edit-config Request

```
<?xml version="1.0"?>
<nc:rpc message-id="16" xmlns:nc="urn:iETF:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0:if_manager">
<nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<configure>
<_XML_MODE__exec_configure>
<interface>
<ethernet>
<interface>2/30</interface>
<_XML_MODE_if-ethernet>
<_XML_MODE_if-eth-base>
<description>
<desc_line>Marketing Network</desc_line>
</description>
</_XML_MODE_if-eth-base>
</_XML_MODE_if-ethernet>
</ethernet>
</interface>
</_XML_MODE__exec_configure>
</configure>
</nc:config>
</nc:edit-config>
</nc:rpc>]]>]]>
```

## Edit-config Response

```
<?xml version="1.0"?>
<nc:rpc-reply xmlns:nc="urn:iETF:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:1.0:if_manager" message-id="16">
<nc:ok/>
</nc:rpc-reply>]]>]]>
```

The operation attribute in edit-config identifies the point in configuration where the specified operation is performed. If the operation attribute is not specified, the configuration is merged into the existing configuration data store. Operation attribute can have the following values:

- create
- merge
- delete

The following example shows how to delete the configuration of interface Ethernet 0/0 from the running configuration.

### Edit-config: Delete Operation Request

```
xmlns="urn:iETF:params:xml:ns:netconf:base:1.0">
<edit-config>
<target>
<running/>
</target>
<default-operation>none</default-operation>
<config xmlns:xc="urn:iETF:params:xml:ns:netconf:base:1.0">
<top xmlns="http://example.com/schema/1.2/config">
```

```

<interface xc:operation="delete">
<name>Ethernet0/0</name>
</interface>
</top>
</config>
</edit-config>
</rpc>]]>]]>

```

### Response to edit-config: Delete Operation

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>]]>]]>

```

## NETCONF get-config Instance

The following example shows the use of NETCONF get-config.

### Get-config Request to Retrieve the Entire Subtree

```

<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-config>
<source>
<running/>
</source>
<filter type="subtree">
<top xmlns="http://example.com/schema/1.2/config">
<users/>
</top>
</filter>
</get-config>
</rpc>]]>]]>

```

### Get-config Response with Results of the Query

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<data>
<top xmlns="http://example.com/schema/1.2/config">
<users>
<user>
<name>root</name>
<type>superuser</type>
<full-name>Charlie Root</full-name>
<company-info>
<dept>1</dept>
<id>1</id>
</company-info>
</user>
<!-- additional <user> elements appear here... -->
</users>
</top>
</data>
</rpc-reply>]]>]]>

```

## NETCONF Lock Instance

The following example shows the use of NETCONF lock operation.

The following examples show the lock request, a success response, and a response to an unsuccessful attempt.

### Lock Request

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<lock>
<target>
<running/>
</target>
</lock>
</rpc>]]>]]>
```

### Response to Successful Acquisition of Lock

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/> <!-- lock succeeded -->
</rpc-reply>]]>]]>
```

### Response to Unsuccessful Attempt to Acquire the Lock

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<rpc-error> <!-- lock failed -->
<error-type>protocol</error-type>
<error-tag>lock-denied</error-tag>
<error-severity>error</error-severity>
<error-message>
Lock failed, lock is already held
</error-message>
<error-info>
<session-id>454</session-id>
<!-- lock is held by NETCONF session 454 -->
</error-info>
</rpc-error>
</rpc-reply>]]>]]>
```

## NETCONF unlock Instance

The following example shows the use of the NETCONF unlock operation.

### unlock request

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<unlock>
<target>
<running/>
</target>
</unlock>
</rpc>
```

### response to unlock request

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
<ok/>
</rpc-reply>
```

## NETCONF Commit Instance - Candidate Configuration Capability

The following example shows the commit operation and the commit reply:

### Commit Operation

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<commit/>
</rpc>
```

### Commit Reply

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
```

## NETCONF Confirmed-commit Instance

The following example shows the confirmed-commit operation and the confirmed-commit reply.

### Confirmed Commit Request

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<commit>
<confirmed/>
<confirm-timeout>120</confirm-timeout>
</commit>
</rpc>]]>]]>
```

### Confirmed Commit Response

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>]]>]]>
```

## NETCONF rollback-on-error Instance

The following example shows the use of NETCONF rollback on error capability. The string `urn:ietf:params:netconf:capability:rollback-on-error:1.0` identifies the capability.

The following example shows how to configure rollback on error and the response to this request.

### Rollback-on-error capability

```
<rpc message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
<target>
<running/>
```

```

</target>
<error-option>rollback-on-error</error-option>
<config>
<top xmlns="http://example.com/schema/1.2/config">
<interface>
<name>Ethernet0/0</name>
<mtu>100000</mtu>
</interface>
</top>
</config>
</edit-config>
</rpc>]]>]]>

```

### Rollback-on-error response

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>]]>]]>

```

## NETCONF validate Capability Instance

The following example shows the use of the NETCONF validate capability. The string `urn:ietf:params:netconf:capability:validate:1.0` identifies the capability.

### Validate request

```

xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<validate>
<source>
<candidate/>
</source>
</validate>
</rpc>]]>]]>

```

### Response to validate request

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>]]>]]>

```

## Additional References

This section provides additional information that is related to implementing the XML management interface.

### Standards

Standards	Title
No new or modified standards are supported by this feature. Support for existing standards has not been modified by this feature.	—

**RFCs**

<b>RFCs</b>	<b>Title</b>
<a href="#">RFC 4741</a>	NETCONF Configuration Protocol
<a href="#">RFC 4742</a>	Using the NETCONF Configuration Protocol over Secure Shell (SSH)



## APPENDIX **A**

# Streaming Telemetry Sources

---

- [About Streaming Telemetry, on page 189](#)
- [Guidelines and Limitations, on page 189](#)
- [Data Available for Telemetry, on page 189](#)

## About Streaming Telemetry

The streaming telemetry feature of the Cisco Nexus 3000 and 9000 switches continuously streams data out of the network and notifies the client, providing near-real-time access to monitoring data.

## Guidelines and Limitations

Following are the guideline and limitations for streaming telemetry:

- The telemetry feature is available in Cisco Nexus 3000 and 9000 switches.
- Switches with less than 8 GB of memory do not support telemetry. The Cisco Nexus 3500-XL has 16 GB of memory and therefore supports telemetry.

## Data Available for Telemetry

For each component group, the distinguished names (DNs) in the appendix of the [NX-API DME Model Reference](#) can provide the listed properties as data for telemetry.





## INDEX

### B

- Bash [3, 5](#)
  - accessing [3](#)
  - examples [5](#)
  - feature bash-shell [3](#)
- Bourne-Again SHell, *See* Bash

### N

- NX-API [83, 84, 86, 88, 91, 95, 97, 102](#)
  - CLI [84](#)
  - cookie [84](#)
  - management commands [86](#)
  - message format [84](#)
  - request elements [88](#)
  - response codes [95](#)
  - response elements [91](#)
  - security [84](#)
  - transport [84](#)
  - user interface [97, 102](#)

### P

- Python [41, 42, 44, 46, 47, 48](#)
  - about API [41](#)
  - Cisco package [41](#)
  - CLI command API [42](#)
  - display format examples [44](#)
  - embedded event manager (EEM) [47](#)

### Python (*continued*)

- invoking [44](#)
- non-interactive [46](#)
- NX-OS network interfaces [47](#)
- NX-OS security [48](#)
- scripts [41](#)

### S

- show tech-support telemetry [151](#)

### T

- tcl [51, 52, 53, 56](#)
  - cli commands [52](#)
  - command separation [52](#)
  - history [52](#)
  - no interactive help [51](#)
  - options [53](#)
  - references [56](#)
  - sandbox [53](#)
  - security [53](#)
  - tab completion [52](#)
  - telquit command [53](#)
  - variables [53](#)
- telemetry [133](#)
  - high availability [133](#)
  - installing [133](#)
- Tool Command Language, *See* tcl

