

N Commands

- native-autonomous-fabric-num, on page 2
- node, on page 3
- node (Cisco IOA cluster node configuration submode), on page 4
- npiv enable, on page 5
- nport, on page 6
- nport pwwn, on page 7
- npv auto-load-balance disruptive, on page 8
- npv enable, on page 9
- npv traffic-map analysis clear, on page 10
- npv traffic-map server-interface, on page 11
- ntp abort, on page 12
- ntp allow, on page 13
- ntp authenticate, on page 15
- ntp authentication-key, on page 17
- ntp commit, on page 19
- ntp distribute, on page 20
- ntp logging, on page 22
- ntp peer, on page 23
- ntp server, on page 25
- ntp source-interface, on page 27
- ntp sync-retry, on page 29
- ntp trusted-key, on page 30
- nxapi http port *port-number*, on page 31
- nxapi https port *port-number*, on page 32
- nxapi ssl ciphers weak, on page 33
- nxapi ssl protocols, on page 34
- nxapi sandbox, on page 36
- nxapi trustpoint, on page 37
- nwwn (DPVM database configuration submode), on page 38
- nwwn (SAN extension configuration mode), on page 39

native-autonomous-fabric-num

To create an IVR persistent FC ID database entry, use the native-autonomous-fabric-num command in fcdomain database configuration submode. To delete all IVR persistent FC ID database entries for a given AFID and VSAN, use the **no** form of the command.

native-autonomous-fabric-num *afid-num* **native-vsan** *vsan-id* **domain** *domain-id*
no native-autonomous-fabric-num *afid-num* **native-vsan** *vsan-id* **domain** *domain-id*

Syntax Description

afid-num	Specifies the native AFID. The range is 1 to 64.
native-vsan *vsan-id*	Specifies the native VSAN ID. The range is 1 to 4093.
domain *domain-id*	Specifies the domain ID. The range is 1 to 239.

Command Default

None.

Command Modes

fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

There is only one domain ID associated with an AFID and VSAN. If you change the domain ID, all the associated FC ID mapping records are also changed.

Examples

The following example shows how to create an entry for a native AFID, VSAN, and domain:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)#
```

The following example shows how to remove all entries for a native AFID and VSAN:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# no native-autonomous-fabric-num 20 native-vsan 30
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

node

To configure Cisco SME switch, use the node command. To disable this command, use the no form of the command.

node {**local** | {*A.B.C.D* | *X*:*X*::*X* /*n* | *DNS name*}}
nonode {**local** | {*A.B.C.D* | *X*:*X*::*X* /*n* | *DNS name*}}

Syntax Description

local	Configures the local switch.
A.B.C.D	Specifies the IP address of the remote switch in IPv4 format.
X:X::X/n	Specifies the IP address of the remote switch in IPv6 format.
DNS name	Specifies the name of the remote database.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example adds the Cisco SME interface from a local switch:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)#
```

The following example adds the Cisco SME interface from a remote switch:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# node 171.71.23.33
switch(config-sme-cl-node)#
```

Related Commands

Command	Description
show sme cluster *cluster name* **node**	Displays Cisco SME node information about a local or remote switch.

node (Cisco IOA cluster node configuration submode)

To configure IOA switch, use the node command. To delete a node to the cluster, use the no form of the command.

node {**local** | *remote-node-name* **or** *ip-address*}
no node {**local** | *remote-node-name* **or** *ip-address*}

Syntax Description

local	Specifies local node as a part of the cluster.
remote-node-name	Specifies either through the DNS name or IPV4/IPV6 address.

Command Default

None.

Command Modes

Cisco IOA cluster node configuration submode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the local switch:

```
switch(config)# ioa cluster tape_vault
switch#(config-ioa-cl)# node local
switch(config-ioa-cl-node)# node 172.23.144.95
2009 May 19 21:06:57 sjc-sw2 %CLUSTER-2-CLUSTER_QUORUM_GAIN: Cluster 0x2143000dec3ee782 now
 has quorum with 1 nodes
2009 May 19 21:07:03 sjc-sw2 %CLUSTER-2-CLUSTER_QUORUM_GAIN: Cluster 0x2143000dec3ee782 now
 has quorum with 2 nodes
sjc-sw2(config-ioa-cl-node)# end
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

npiv enable

To enable N port identifier virtualization (NPIV) for all VSANs on a switch, use the **npiv enable** command in configuration mode. To disable NPIV, use the **no** form of the command.

npiv enable
no npiv enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

NPIV provides a means to assign multiple port IDs to a single N Port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level.

You must globally enable NPIV for all VSANs on the MDS switch to allow the NPIV-enabled applications to use multiple N port identifiers.



Note All of the N Port Identifiers are allocated in the same VSAN.

Examples

The following example enables NPIV for all VSANs on the switch:

```
switch# config terminal
switch(config)# npiv enable
```

The following example disables NPIV for all VSANs on the switch:

```
switch(config)# no npiv enable
```

Related Commands

Command	Description
show interface	Displays interface configurations.

nport

To configure the site and VSAN ID of the N ports, use the **nport** command. To delete the N port from the IOA cluster, use the **no** form of the command.

nport pwwn *pwwn* **site** *site name* **vsan** *vsan-id*
no nport pwwn *pwwn* **site** *site name* **vsan** *vsan-id*

Syntax Description

pwwn	Specifies the N port.
pwwn	Specifies the N port PWWN. The format is hh:hh:hh:hh:hh:hh:hh:hh.
site	Specifies an IOA site.
site name	Specifies an IOA site name. The maximum length is 31 characters.
vsan	Specifies the VSAN where this flow is accelerated.
vsan id	Specifies the VSAN ID where this flow is accelerated. The range is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the site and VSAN ID of the N port:

```
switch(config-ioa-cl)# nport pwwn 10:0:0:0:0:0:0:1 site SJC vsan 100
switch(config-ioa-cl)# no nport pwwn 11:0:0:0:0:0:0:1 site SJC vsan 100
switch(config-ioa-cl)# end
```

Related Commands

Command	Description
show ioa cluster summary	Displays the summary of all the IOA clusters.

nport pwwn

To configure the N Port pWWN for the SAN extension tuner, use the **nport pwwn** command in SAN extension configuration mode. To revert to the default value, use the **no** form of the command.

nport pwwn *pwwn-id* **vsan** *vsan-id* **interface gigabitethernet** *slot*/*port*
no nport pwwn *pwwn-id* **vsan** *vsan-id* **interface gigabitethernet** *slot*/*port*

Syntax Description

pwwn-id	Specifies the port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interface gigabitethernet *slot*/*port*	Specifies the Gigabit Ethernet interface slot and port.

Command Default

None.

Command Modes

SAN extension configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add an entry to the SAN extension tuner database:

```
switch# san-ext-tuner
switch(san-ext)# nport pwwn 11:22:33:44:55:66:77:88 vsan 1 interface gigabitethernet 1/1
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension configuration mode.
show san-ext-tuner	Shows SAN extension tuner information.

npv auto-load-balance disruptive

To enable autoload balance disruptive, use the npv auto-load-balance disruptive command in configuration mode. To disable this feature, use the no form of the command.

npv auto load-balancing disruptive
no npv auto load-balancing disruptive

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable autoload balance disruptive:

```
switch(config)# npv auto-load-balance disruptive
Enabling this feature may flap the server intefaces whenever load is not in a ba
lanced state. This process may result in traffic disruption. Do you want to proc
eed? (y/n):
Please enter y or n Y
switch(config)#
```

Related Commands

Command	Description
npv traffic-map server interface	Configures server interface traffic engineering.

npv enable

To enable N port virtualization (NPV), use the npv enable command in configuration mode. To disable this feature, use the no form of the command.

npv enable
no npv enable

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

When NPV is enabled, all configurations are erased and the switch is rebooted. The switch restarts in the NPV mode. All configuration and verification commands for NPV are available only when NPV is enabled on the switch. When you disable this feature, all related configurations are automatically erased and the switch is rebooted.

Examples

The following example shows how to enable NPV:

```
switch# config
switch(config)# npv enable
```

Related Commands

Command	Description
show npv status	Displays the NPV current status.

npv traffic-map analysis clear

To reset the link load values collected for NPV external interface utilization analysis, use the **npv traffic-map analysis clear** command.

npv traffic-map analysis clear

Command Default

None.

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.5(1)	This command was introduced.

Usage Guidelines

This command only resets the link load values to zero. It does not restart the sampling interval timer.

Examples

The following example displays how to reset the throughput values:

```
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# npv traffic-map analysis clear
```

Related Commands

Command	Description
show npv traffic-map proposed	Displays a proposed mapping of server interfaces to external interfaces.

npv traffic-map server-interface

To configure the server interface based traffic engineering, use the npv traffic-map server-interface command in configuration mode. To revert to the default value, use the no form of the command.

npv traffic-map server-interface if -range external-interface if-range
no npv traffic-map server-interface if-range external-interface if-range

Syntax Description

if-range	Range may vary from 1 to 1.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure NPV traffic map server interface:

```
switch(config)# npv traffic-map server-interface fc1/1 external-interface fc1/2
switch(config)# npv traffic-map server-interface fc1/4-5 external-interface fc1/6-7
switch(config)# no npv traffic-map server-interface fc1/4-5 external-interface fc1/6-7
switch(config)# no npv traffic-map server-interface fc1/1 external-interface fc1/2
switch(config)#
```

Related Commands

Command	Description
show npv-traffic-map	Displays information about the NPV traffic map.

ntp abort

To terminate and unlock the existing Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session on a switch, use the **ntp abort** command in configuration mode.

ntp abort

Syntax Description

This command has no other arguments or keywords.

Command Default

This command terminates the current NTP CFS session.

Command Modes

Configuration mode (config)

Command History

Release	Modification
2.0(x)	This command was introduced.

Examples

The following example displays how to terminate the NTP CFS distribution session in progress:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp abort
```

Related Commands

Command	Description
ntp commit	Commits the NTP configuration changes to the active configuration.
ntp distribute	Enables CFS distribution for NTP.
show ntp status	Displays the status of the NTP CFS distribution.

ntp allow

To enable processing of Network Time Protocol (NTP) control mode and private mode packets, use the **ntp allow** command. To disable this feature, use the **no** form of this command.

ntp allow {**private** | **control** [**rate-limit** *seconds*]}
no ntp allow {**private** | **control**}

Syntax Description

private	Specifies to process the private mode packets.
control	Specifies to process the control mode packets.
rate-limit *seconds*	Specifies the quiet period in which further control mode packets are ignored after processing one. The default time duration is 3 seconds, which means that a control mode packet is processed or responded every 3 seconds. Range is from 1 to 65535.

Command Default

Processing of control and private mode packets is disabled by default for security reasons.

Command Modes

Configuration mode (config)

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example displays how to enable the processing of private mode packets:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp allow private
```

The following example displays how to enable the processing or responding of control mode packets every 3 seconds:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp allow control
```

The following example displays how to enable the processing or responding of control mode packets every 10 seconds:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp allow control rate-limit 10
```

Related Commands

Command	Description
show ntp	Displays NTP information.

ntp authenticate

To prevent the system from synchronizing with unauthenticated, unconfigured NTP peers, use the **ntp authenticate** command. To allow synchronization with unauthenticated, unconfirmed NTP peers, use the **no** form of this command.

ntp authenticate
no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

Unkeyed NTP symmetric-active, broadcast, and multicast packets are trusted by default. This feature is disabled by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	This command was introduced.

Usage Guidelines

If the **ntp authenticate** command is specified, when a symmetric-active, broadcast, or multicast packet is received, the system will not synchronize to the peer unless the packet carries one of the authentication keys specified in the **ntp trusted-key** command.

Note This command does not authenticate peer associations configured via the **ntp server** and **ntp peer** commands. To authenticate NTP server and NTP peer associations, specify the **key** keyword.

Examples

The following example displays how to enable NTP authentication:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp authenticate
```

The following example displays how to disable NTP authentication:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp authenticate
```

Related Commands

Command	Description
ntp authentication-key	Configures an NTP authentication key for a device to synchronize to a time source after enabling the NTP authentication.

Command	Description
ntp trusted-key	Specifies one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it.
show ntp authentication-status	Displays the status of NTP authentication.

ntp authentication-key

To configure a Network Time Protocol (NTP) authentication key for a device to synchronize to a time source after enabling the NTP authentication, use the **ntp authentication-key** command. To remove the NTP authentication key, use the **no** form of this command.

ntp authentication-key *id* **md5** *key* [**0** | **7**]
no ntp authentication-key *id* **md5** *key* [**0** | **7**]

Syntax Description

id	Authentication key identifier. The range is from 1 to 65535.
md5	Specifies the MD5 algorithm for authentication.
key	Authentication key. The maximum key size is 15.
0	(Optional) Specifies the encryption type to be *Clear* text.
7	(Optional) Specifies the encryption type to be *Encrypted*.

Command Default

No NTP keys are configured by default. When configuring an authentication key the default CLI encryption type is *clear text*.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	This command was introduced.

Usage Guidelines

Enable NTP authentication before configuring an NTP authentication key.

The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the **ntp trusted-key** command.

Authentication keys are always stored in the switch configuration in the encrypted format. If a user configures a key as *clear text*, the key will automatically be converted before installation into the configuration.

Examples

The following example displays how to configure an NTP authentication key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 key1_12
```

The following example displays how to remove the NTP authentication key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp authentication-key 42 md5 key1_12
```

Related Commands

Command	Description
show ntp authentication-keys	Displays a list of configured NTP authentication keys.

ntp commit

To apply pending Network Time Protocol (NTP) configuration to an NTP Cisco Fabric Services (CFS) enabled peers in a fabric, use the **ntp commit** command.

ntp commit

Syntax Description

This command has no other arguments or keywords.

Command Default

This command commits changes pending in the current NTP CFS session.

Command Modes

Configuration mode (config)

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Once the **ntp commit** command is issued, the running configuration is modified on all switches that are part of the NTP CFS domain. Use the **copy running-config startup-config fabric** command to save the running configuration to the startup configuration on all the switches.

Examples

The following example displays how to commit changes to the active NTP configuration:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp commit
```

Related Commands

Command	Description
ntp abort	Terminates the NTP configuration.
ntp distribute	Enables CFS distribution for NTP.
show ntp pending-diff	Displays the differences between the pending NTP configuration changes and the active NTP configuration.
show ntp status	Displays the status of the NTP CFS distribution.

ntp distribute

To enable Cisco Fabric Services (CFS) distribution of Network Time Protocol (NTP) configuration, use the **ntp distribute** command. To disable this feature, use the **no** form of the command.

ntp distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

NTP configuration distribution to other switches is disabled by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

In order to enable NTP distribution with CFS, you must have already enabled CFS distribution for the device using the **cfs distribute** command.

If CFS is disabled for NTP, then NTP does not distribute any configuration changes and does not accept a distribution from other devices in the fabric.

The **ntp distribute** command enables NTP to distribute its configurations through CFS. To distribute an NTP configuration change, enter the change and then use the **ntp commit** command.

After CFS distribution is enabled for NTP, then the entry of an NTP configuration command locks the fabric for NTP until the **ntp commit** command is entered. During the lock, no changes can be made to the NTP configuration by any other device in the fabric except the device where the lock was activated.

Before distributing the configuration changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the **ntp commit** command.

Examples

The following example displays how to distribute the active NTP configuration to the fabric:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp distribute
```

Related Commands

Command	Description
cfs distribute	Globally enables CFS distribution for all applications on the device.
clear ntp session	Clears the application configuration session, discards pending changes, and releases the lock on a fabric.
ntp abort	Terminates the NTP configuration.
ntp allow	Enables processing of the control mode and private mode packets.

Command	Description
ntp commit	Commits the NTP configuration changes to the active configuration.
show cfs status	Displays the global CFS distribution status for the device.
show ntp pending-diff	Displays the differences between the pending NTP configuration changes and the active NTP configuration.
show ntp status	Displays the status of the NTP CFS distribution.

ntp logging

To enable Network Time Protocol (NTP) logging to generate NTP event syslogs, use the **ntp logging** command. To disable NTP logging, use the **no** form of this command.

ntp logging
no ntp logging

Syntax Description

This command has no other arguments or keywords.

Command Default

NTP logging is disabled by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	This command was introduced.

Examples

The following example displays how to enable NTP logging:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp logging
```

The following example displays how to disable NTP logging:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp logging
```

Related Commands

Command	Description
show ntp logging-status	Displays the NTP logging status.
show ntp statistics	Displays the NTP statistics.

ntp peer

To configure a device as a Network Time Protocol (NTP) peer, use the **ntp peer** command. To remove the device as an NTP peer, use the **no** form of this command.

ntp peer {*ip-address ipv6-address dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]
no ntp peer {*ip-address ipv6-address dns-name*}

Syntax Description

ip-address	IPv4 address.
ipv6-address	IPv6 address.
dns-name	Domain Name Server (DNS) name.
key *id*	(Optional) Key ID. The range is from 1 to 65535.
prefer	(Optional) Specifies the given NTP peer as the preferred one.
maxpoll *interval*	(Optional) Maximum interval to poll a peer, in seconds. Default interval is 6.
minpoll *interval*	(Optional) Minimum interval to poll a peer, in seconds. Default interval is 4.

Command Default

No NTP peers are configured by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	Added the **key** *id* keyword.
2.0(x)	This command was introduced.

Usage Guidelines

The **ntp peer** command is part of the NTP Cisco Fabric Services (CFS) distribution.

NX-OS NTP supports time stamp references for NTP versions 4, 3, and 2. The version used is based on negotiation with each peer. Order of version priorities is, from highest to lowest, v4 to v3 to v2.

An NTP server is an authoritative source of NTP updates. The local device will follow the time of a server, but the server will not update from the local device's time. NTP peers send out updates and also adjust to incoming peer updates so that all peers converge to the same time. A device may have associations with multiple servers or peers.

In some versions of NX-OS, NTP will not sync to a time source if difference between the time source and the local clock is greater than 1 day. To force the switch to update with the received NTP time use the **ntp sync-retry** command after enabling NTP on the switch and waiting several minutes for peering to stabilize.

If you configure a key to be used while communicating with the NTP peer, make sure that the key exists as a trusted key on the device.

Examples

The following example displays how to configure an NTP peer:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp peer 190.0.2.1 key 123 prefer minpoll 4 maxpoll 10
```

The following example displays how to remove the NTP peer:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp peer 190.0.2.1
```

Related Commands

Command	Description
ntp server	Configures an NTP server.
ntp sync-retry	Restarts NTP service and resynchronizes to peers.
show ntp peers	Displays all the NTP peers.
show ntp peer-status	Displays the status for all the server and peers.

ntp server

To configure a device as a Network Time Protocol (NTP) server, use the **ntp server** command. To remove the device as an NTP peer, use the **no** form of this command.

ntp server {*ip-address ipv6-address dns-name*} [**key** *id*][**prefer**][**maxpoll** *interval*][**minpoll** *interval*]
no ntp server {*ip-address ipv6-address dns-name*}

Syntax Description

ip-address	IPv4 address.
ipv6-address	IPv6 address.
dns-name	Domain Name Server (DNS) name.
key *id*	(Optional) Key ID. The range is from 1 to 65535.
prefer	(Optional) Specifies the given NTP peer as the preferred one.
maxpoll *interval*	(Optional) Maximum interval to poll a peer, in seconds. Default interval is 6.
minpoll *interval*	(Optional) Minimum interval to poll a peer, in seconds. Default interval is 4.

Command Default

No NTP server are configured by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	Added the **key** *id* keyword.
2.0(x)	This command was introduced.

Usage Guidelines

The **ntp server** command is part of the NTP Cisco Fabric Services (CFS) distribution.

NX-OS NTP supports time stamp references for NTP versions 4, 3, and 2. The version used is based on negotiation with each peer. Order of version priorities is, from highest to lowest, v4 to v3 to v2.

An NTP server is an authoritative source of NTP updates. The local device will follow the time of a server, but the server will not update from the local device's time. NTP peers send out updates and also adjust to incoming peer updates so that all peers converge to the same time. A device may have associations with multiple servers or peers.

In some versions of NX-OS, NTP will not sync to a time source if difference between the time source and the local clock is greater than 1 day. To force the switch to update with the received NTP time use the **ntp sync-retry** command after enabling NTP on the switch and waiting several minutes for peering to stabilize.

If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.

Examples

The following example displays how to configure an NTP server:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 190.0.2.1 key 123 prefer minpoll 4 maxpoll 10
```

The following example displays how to remove the NTP server:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp server 190.0.2.1
```

Related Commands

Command	Description
ntp peer	Configures a device as an NTP peer.
ntp sync-retry	Restarts NTP service and resynchronizes to peers.
show ntp peers	Displays all the NTP peers.
show ntp peer-status	Displays the status for all the server and peers.

ntp source-interface

To override the default source address of Network Time Protocol (NTP) packets sent from the switch, use the **ntp source-interface** command. To remove an NTP source interface, use the **no** form of this command.

ntp source-interface {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number* }
no ntp source-interface {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number* }

Syntax Description

ethernet *slot/port.sub-interface*	Ethernet interface.
mgmt *number*	Management interface (mgmt 0).
port-channel *number*	Port channel number.

Command Default

This default source address of NTP packets is mgmt0.

Command Modes

Configuration mode (config)

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Only a single **ntp source-interface** command can be specified. All NTP packets sent through all interfaces will use the address specified by this command as the source address.

Examples

The following example displays how to configure an Ethernet interface:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp source-interface ethernet 2/2
```

The following example displays how to remove an Ethernet interface:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp source-interface ethernet 2/2
```

The following example displays how to configure the management 0 interface:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp source-interface mgmt 0
```

The following example displays how to remove the management 0 interface:

```
switch# configure
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp source-interface mgmt 0
```

The following example displays how to configure a port channel:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp source-interface port-channel 1
```

The following example displays how to remove the port channel:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp source-interface port-channel 1
```

Related Commands

Command	Description
show ntp source-interface	Displays information about the configured NTP source interface.

ntp sync-retry

To retry synchronization with configured servers, use the **ntp sync-retry** command.

ntp sync-retry

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.1(1b)	Added a note.
3.3(1a)	This command was introduced.

Usage Guidelines

None.



Note If the user changes the mgmt0 IP address, NX-OS should conditionally do an internal **ntp synchronization-retry**.

Examples

The following example displays the sup-fc0 message logs:

```
switch# ntp sync-retry
```

Related Commands

Command	Description
ntp distribute	Enables CFS distribution for NTP.
show ntp	Displays NTP information.

ntp trusted-key

To configure one or more keys that a time source must provide in its Network Time Protocol (NTP) packets in order for the device to synchronize to it, use the **ntp trusted-key** command. To remove the NTP trusted key, use the **no** form of this command.

ntp trusted-key *id*
no ntp trusted-key *id*

Syntax Description

id	Trusted key identifier. The range is from 1 to 65535.

Command Default

No trusted keys are configured by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	This command was introduced.

Usage Guidelines

You must configure an NTP authentication key using the **ntp authentication-key** command before configuring an NTP trusted key. You must use the NTP authentication key as the NTP trusted key number.

This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

Examples

The following example displays how to configure an NTP trusted key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp trusted-key 42
```

The following example displays how to remove the NTP trusted key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp trusted-key 42
```

Related Commands

Command	Description
ntp authentication-key	Configures an NTP authentication key for a device to synchronize to a time source after enabling the NTP authentication.
show ntp authentication-keys	Displays a list of configured NTP authentication keys.
show ntp source-interface	Displays the status of NTP authentication.

nxapi http port *port-number*

To configure an HTTP port to access the NX-API Developer Sandbox, use the **nxapi http port** *port-number* command in global configuration mode. To disable HTTP, use the **no** form of this command.

nxapi http port *port-number*
no nxapi http

Syntax Description

port	HTTP port number
port-number	Specifies the HTTP port number. The range is from 0 to 65535. **Note** The default HTTP port number to access the NX-API Developer Sandbox is 8080.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

The **feature nxapi** command must be used to enable the NX-API feature before you configure HTTP to access the NX-API Developer Sandbox.

Ensure that the *port-number* configured is not used by other services like SSH, Telnet.

The following example shows how to configure an HTTP port to access the NX-API Developer Sandbox:

```
switch# configure terminal
switch(config)# feature nxapi
switch(config)# nxapi http port 1010
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.
nxapi sandbox	Enables the NX-API Developer Sandbox.
nxapi https port *port-number*	Configures an HTTPS port to access the NX-API Developer Sandbox.

nxapi https port *port-number*

To configure an HTTPS port to access the NX-API Developer Sandbox, use the **nxapi https** command in global configuration mode. To disable HTTPS, use the **no** form of this command.

nxapi https port *port-number*
no nxapi https

Syntax Description

port	HTTPS port number.
port-number	Specifies the HTTPS port number. The range is from 0 to 65535.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

The **feature nxapi** command must be used to enable the NX-API feature before you configure HTTPS to access the NX-API Developer Sandbox.

Ensure that the *port-number* configured is not used by other services like SSH, Telnet.

The following example shows how to configure an HTTPS port to access the NX-API Developer Sandbox:

```
switch# configure terminal
switch(config)# feature nxapi
switch(config)# nxapi https port 443
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.
nxapi sandbox	Enables the NX-API Developer Sandbox.
nxapi http port *port-number*	Configures an HTTP port to access the NX-API Developer Sandbox.

nxapi ssl ciphers weak

To allow weak SSL ciphers for NX-API HTTPS connections, use the **nxapi ssl ciphers weak** command. To disable accepting weak ciphers, use the **no** form of this command.

nxapi ssl ciphers weak

no nxapi ssl ciphers weak

Command Default

Starting from Cisco MDS NX-OS 8.3(1) weak ciphers are disabled by default. Prior releases allow weak ciphers by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Weak ciphers are defined as encryption or decryption algorithms that use key sizes that are less than 128 bits.

The following ciphers are disabled by the **no** option:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- secp256r1
- ffdhe3072

The following example displays how to allow weak SSL ciphers for NX-API HTTPS connections:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# nxapi ssl ciphers weak
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.

nxapi ssl protocols

To configure accepted Secure Sockets Layer (SSL) transports for NX-API HTTPS connections, use the **nxapi ssl protocols** command. To return to the default list of accepted SSL transports, use the **no** form of this command.

nxapi ssl protocols { [**SSLv3**] [**TLSv1**] [**TLSv1.1**] [**TLSv1.2**] [**TLSv1.3**] }

no nxapi ssl protocols

Syntax Description

SSLv3	Specifies the SSL version 3.
TLSv1	Specifies the Transport Layer Security (TLS) version 1.0.
TLSv1.1	Specifies the Transport Layer Security (TLS) version 1.1.
TLSv1.2	Specifies the Transport Layer Security (TLS) version 1.2.
TLSv1.3	Specifies the Transport Layer Security (TLS) version 1.3.

Command Default

Starting in Cisco MDS NX-OS 8.3(1), only TLS1.1 and TLS1.2 are enabled by default.

Starting in Cisco MDS NX-OS 8.5(1), only TLS1.2 is enabled by default.

Starting in Cisco MDS NX-OS 9.4(1), both TLS1.2 and TLS1.3 are enabled by default on the following Cisco MDS 9000 series fabric switches:

- MDS 9124V switches
- MDS 9132T switches
- MDS 9148T switches
- MDS 9148V switches
- MDS 9220i switches
- MDS 9396T switches
- MDS 9396V switches

Starting in Cisco MDS NX-OS 9.4(2), both TLS1.2 and TLS1.3 are enabled by default on all the Cisco MDS 9700 series switches:

- MDS 9718 Director switches
- MDS 9710 Director switches
- MDS 9706 Director switches

Command Modes

Global configuration (config)

Command History

Release	Modification
9.4(2)	TLS1.3 is supported on MDS 9700 series Director switches.
9.4(1)	TLS1.3 is supported on MDS 9000 series fabric switches.
1.1(1)	This command was introduced.

Usage Guidelines

Older versions of SSL transport protocol are easier to exploit. Enable only the most recent versions of SSL transport protocol that the connecting devices support for the most secure connections to NX-API.

The following example displays how to allow TLS versions 1.0, 1.1 and 1.2 HTTPS connections to NX-API:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# nxap ssl protocol TLSv1 TLSv1.1 TLSv1.2
```

The following example displays how to allow only TLS version 1.2 HTTPS connections to NX-API:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# nxapi ssl protocols TSLv1.2
```

Note Ensure there is no space at the end of the SSL protocol command as it is not accepted as a valid configuration.

Related Commands

Command	Description
feature nx-api	Enables NX-API.

nxapi sandbox

To enable the NX-API Developer Sandbox, use the **nxapi sandbox** command in global configuration mode. To disable the NX-API Developer Sandbox, use the **no** form of this command.

nxapi sandbox
no nxapi sandbox

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

The **feature nxapi** command must be used to enable the NX-API feature before you enable the NX-API Developer Sandbox.

The following example shows how to enable the NX-API Developer Sandbox:

```
switch# configure terminal
switch(config)# feature nxapi
switch(config)# nxapi sandbox
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.

nxapi trustpoint

Use the **nxapi trustpoint** command to link certificates and keys in the trustpoint repository so NX-API can use them. To delete the configuration, enter the **no** form of the command.

[**no**] **nxapitrustpoint***trustpoint-label*

no	(Optional) Negate a command or set its defaults
nxapi	Configure NX-API
trustpoint	Configure parameters related to the trustpoint.
trustpoint-label	Label or profile for an existing trustpoint identity.

Command Default

None

Command Modes

Exec mode

Command History

Release	Modification
8.5(1)	This command was introduced.

Usage Guidelines

You must configure a trustpoint before you use this command.

Example

The following example shows how to configure a trustpoint label or profile called nxapi-client-certificates for use by NX-API.

```
switch# configure terminal
switch(config)# nxapi trustpoint nxapi-client-certificates
```

Related Commands

Table 1: Related Commands

Command Syntax	Description
show nxapi	Displays NX-API status.

nwwn (DPVM database configuration submode)

To add a device to a dynamic port VSAN membership (DPVM) database using the nWWN, use the **nwwn** command in DPVM database configuration submode. To remove a device from a DPVM database using the nWWN, use the **no** form of the command.

nwwn *nwwn-id* **vsan** *vsan-id*
no nwwn *nwwn-id* **vsan** *vsan-id*

Syntax Description

nwwn-id	Specifies the node WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

DPVM database configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to add an entry to the DPVM database:

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)# nwwn 11:22:33:44:55:66:77:88 vsan 1
```

The following example shows how to delete an entry from the DPVM database:

```
switch(config-dpvm-db)# no nwwn 11:22:33:44:55:66:77:88 vsan 1
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

nwwn (SAN extension configuration mode)

To configure the nWWN for the SAN extension tuner, use the **nwwn** command in SAN extension configuration submode.

nwwn *nwwn-id*

Syntax Description

nwwn-id	Specifies the nWWN address. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Command Default

None.

Command Modes

SAN extension configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add an entry to the SAN extension tuner database:

```
switch# san-ext-tuner
switch(san-ext)# nwwn 20:42:00:0b:46:79:f1:80
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension configuration mode.
show san-ext-tuner	Shows SAN extension tuner information.