



CHAPTER 2

Configuring CDP and NTP

This chapter describes how to configure the Cisco Discovery Protocol (CDP) and the Network Time Protocol (NTP) on a device.

This chapter includes the following sections:

- [Information About CDP and NTP, page 2-1](#)
- [Licensing Requirements for CDP and NTP, page 2-4](#)
- [Prerequisites for CDP and NTP, page 2-4](#)
- [Configuration Guidelines and Limitations, page 2-4](#)
- [Configuring CDP and NTP, page 2-5](#)
- [Verifying CDP and NTP Configuration, page 2-10](#)
- [CDP and NTP Example Configuration, page 2-11](#)
- [Default Settings, page 2-11](#)
- [Additional References, page 2-12](#)
- [Feature History for CDP and NTP, page 2-12](#)

Information About CDP and NTP

This section includes the following topics:

- [CDP Overview, page 2-1](#)
- [NTP Overview, page 2-2](#)
- [High Availability, page 2-3](#)

CDP Overview

Cisco Discovery Protocol (CDP) is a media- and protocol-independent protocol that runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. You can use CDP to discover and view information about all the Cisco devices that are directly attached to the device.

CDP gathers protocol addresses of neighboring devices and discovers the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other.

Send document comments to nexus7k-docfeedback@cisco.com.

Each device that you configure for CDP sends periodic advertisements to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain hold-time information, which indicates the length of time that a receiving device should hold CDP information before dismoduleing it. You can configure the advertisement or refresh timer and the hold timer.

CDP Version-2 (CDPv2) allows you to track instances where the native VLAN ID or port duplex states do not match between connecting devices.

CDP advertises the following type-length-value fields (TLVs):

- Device ID
- Address
- Port ID
- Capabilities
- Version
- Platform
- Native VLAN
- Full/Half Duplex
- MTU
- SysName
- SysObjectID
- Management Address
- Physical Location

All CDP packets include a VLAN ID. If you configure CDP on a Layer 2 access port, the CDP packets sent from that access port include the access port VLAN ID. If you configure CDP on a Layer 2 trunk port, the CDP packets sent from that trunk port include the lowest configured VLAN ID allowed on that trunk port. The trunk port can receive CDP packets that include any VLAN ID in the allowed VLAN list for that trunk port. For more information on VLANs, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0* at the following URL:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/layer2/configuration/guide/l2_nx-os_book.html.

NTP Overview

The Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows you to correlate events when you receive system logs and other time-specific events from multiple network devices.

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communication uses the Universal Time Coordinated (UTC) standard. An NTP server usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

NTP uses a stratum to describe how many NTP hops away that a network device is from an authoritative time source. A stratum 1 time server has an authoritative time source (such as an atomic clock) directly attached to the server. A stratum 2 NTP server receives its time through NTP from a stratum 1 NTP server, which in turn connects to the authoritative time source.

Send document comments to nexus7k-docfeedback@cisco.com.

NTP avoids synchronizing to a network device that may keep accurate time. NTP never synchronizes to a system that is not in turn synchronized itself. NTP compares the time reported by several network devices and does not synchronize to a network device that has a time that is significantly different than the others, even if its stratum is lower.

Cisco NX-OS cannot act as a stratum 1 server. You cannot connect to a radio or atomic clock. We recommend that the time service that you use for your network is derived from the public NTP servers available on the Internet.

If the network is isolated from the Internet, Cisco NX-OS allows you to configure a network device so that the device acts as though it is synchronized through NTP, when in fact it has determined the time using other means. Other network devices can then synchronize to that network device through NTP.

NTP Peers

NTP allows you to create a peer relationship between two networking devices. A peer can provide time on its own or connect to an NTP server. If both the local device and the remote peer point to different NTP servers, your NTP service is more reliable. The local device maintains the right time even if its NTP server fails by using the time from the peer.

Figure 2-1 displays a network with two NTP stratum 2 servers and two switches.

Figure 2-1 ***NTP Peer and Server Association***



In this configuration, switch 1 and switch 2 are NTP peers. switch 1 uses stratum-2 server 1, while switch 2 uses stratum-2 server 2. If stratum-2 server-1 fails, switch 1 maintains the correct time through its peer association with switch 2.

High Availability

Cisco NX-OS supports stateless restarts for CDP and NTP. After a reboot or a supervisor switchover, Cisco NX-OS applies the running configuration. For more information on high availability, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.0* at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/high_availability/configuration/guide

You can configure NTP peers to provide redundancy in case an NTP server fails.

Send document comments to nexus7k-docfeedback@cisco.com.

Virtualization Support

Cisco NX-OS supports multiple instances of CDP (one instance in each virtual device context (VDC)) but only one instance of NTP on the entire platform. You must configure NTP in the default VDC. By default, Cisco NX-OS places you in the default VDC unless you specifically configure another VDC. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0* at the following URL:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/virtual_device_context/configuration/guide/vdc_nx-os_book.html

Licensing Requirements for CDP and NTP

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	CDP and NTP require 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 NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/licensing/configuration/guide/nx-os_licensing.html

Prerequisites for CDP and NTP

CDP and NTP have the following prerequisites:

- If you configure NTP, you must have connectivity to at least one server that is running NTP.
- If you configure NTP, you must be in the default VDC.
- You cannot configure NTP in any other VDC except the default VDC.

If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0* at the following URL:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/virtual_device_context/configuration/guide/vdc_nx-os_book.html

Configuration Guidelines and Limitations

CDP has the following configuration guidelines and limitations:

- CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.
- CDP must be enabled on the device or you cannot enable it on any interfaces.
- You can configure CDP on physical interfaces and port channels only.

NTP has the following configuration guidelines and limitations:

Send document comments to nexus7k-docfeedback@cisco.com.

- You should have a peer association with another device only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as backup. If you have two servers, you can configure several devices to point to one server and the remaining devices point to the other server. You can then configure peer association between these two servers to create a more reliable NTP configuration.
- If you only have one server, you should configure all the devices as clients to that server.
- You can configure up to 64 NTP entities (servers and peers).

Configuring CDP and NTP

This section includes the following topics:

- [Enabling or Disabling the CDP Feature, page 2-5](#)
- [Enabling or Disabling CDP on an Interface, page 2-6](#)
- [Configuring Optional CDP Parameters, page 2-8](#)
- [Enabling or Disabling the NTP Protocol, page 2-8](#)
- [Configuring an NTP Server and Peer, page 2-9](#)



Note

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Enabling or Disabling the CDP Feature

CDP is enabled on the device by default. You can disable CDP on the device and then re-enable it.

CDP must be enabled on the device before you enable CDP on any interfaces. If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces; the system does not return an error message.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **feature cdp**
3. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	feature cdp Example: switch(config)# feature cdp	Enables the CDP feature on the entire device. This is enabled by default
Step 3	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Saves this configuration change.

Use the **no feature cdp** command to disable the CDP feature on the device and remove all associated configuration.

Command	Purpose
no feature cdp Example: switch(config)# no feature cdp	Disables the CDP feature on the entire device and removes all associated configuration.

This example shows how to enable the CDP feature:

```
switch# config t
switch(config)# feature cdp
```

Enabling or Disabling CDP on an Interface

CDP is enabled by default on an interface. You can disable CDP on an interface.

If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces; the system does not return an error message.

BEFORE YOU BEGIN

Ensure that CDP is enabled on the device (see the [“Enabling or Disabling the CDP Feature”](#) section on page 2-5).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **interface** *interface-type slot/port*
3. **cdp enable**

Send document comments to nexus7k-docfeedback@cisco.com.

4. `show cdp interface interface-type slot/port`
5. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>confi g t</code> Example: switch# <code>confi g t</code> switch(config)#	Enters configuration mode.
Step 2	<code>interface interface-type slot/port</code> Example: switch(config)# <code>interface ethernet 1/2</code> switch(config-if)#	Enters interface configuration mode.
Step 3	<code>cdp enable</code> Example: switch(config-if)# <code>cdp enable</code>	Enables CDP on this interface. This is enabled by default.
Step 4	<code>show cdp interface interface-type slot/port</code> Example: switch(config-if)# <code>show cdp interface ethernet 1/2</code>	(Optional) Displays CDP information for an interface.
Step 5	<code>copy running-config startup-config</code> Example: switch(config-if)# <code>copy running-config startup-config</code>	(Optional) Saves this configuration change.

This example shows how disable CDP on Ethernet 1/2:

```
switch# confi g t
switch(config)# interface ethernet 1/2
switch(config-if)# no cdp enable
switch(config-if)# copy running-config startup-config
```

This example shows how enable CDP on port channel 2:

```
switch# confi g t
switch(config)# interface port-channel 2
switch(config-if)# cdp enable
switch(config-if)# copy running-config startup-config
```

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring Optional CDP Parameters

You can use the following optional commands in global configuration mode to modify CDP:

Command	Purpose
cdp advertise {v1 v2} Example: <pre>switch(config)# cdp advertise v1</pre>	Sets the CDP version supported by the device. The default is v2.
cdp format device-id {mac-address other serial-number} Example: <pre>switch(config)# cdp format device-id mac-address</pre>	Sets the CDP device ID. The options are as follows: <ul style="list-style-type: none"> • mac-address—MAC address of the chassis. • other—Chassis serial number • serial-number—Chassis serial number/Organizationally Unique Identifier (OUI) The default is other.
cdp holdtime seconds Example: <pre>switch(config)# cdp holdtime 150</pre>	Sets the time that CDP holds onto neighbor information before dismoduleing it. The range is from 10 to 255 seconds. The default is 180 seconds.
cdp timer seconds Example: <pre>switch(config)# cdp timer 50</pre>	Sets the refresh time when CDP sends advertisements to neighbors. The range is from 5 to 254 seconds. The default is 60 seconds.

Enabling or Disabling the NTP Protocol

NTP is enabled on the device by default. You can disable NTP on the device and then re-enable it.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **ntp enable**
3. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code> Example: switch# <code>config t</code> switch(config)#	Enters configuration mode.
Step 2	<code>ntp enable</code> Example: switch(config)# <code>ntp enable</code>	Enables or disables the NTP protocol on the entire device. This is enabled by default
Step 3	<code>copy running-config startup-config</code> Example: switch(config)# <code>copy running-config startup-config</code>	(Optional) Saves this configuration change.

Use the **no ntp enable** command to disable the NTP protocol.

Command	Purpose
<code>no ntp enable</code> Example: switch(config)# <code>no ntp enable</code>	Disables the NTP protocol on the device.

This example shows how to disable the NTP protocol:

```
switch# config t
switch(config)# no ntp enable
```

Configuring an NTP Server and Peer

You can configure NTP using IPv4 addresses, IPv6 addresses, or domain name server (DNS) names.

BEFORE YOU BEGIN

Ensure that you are in the default VDC (or use the **switchback** command).

SUMMARY STEPS

1. `config t`
2. `ntp server {ip-address | ipv6-address | dns-name}`
3. `ntp peer {ip-address | ipv6-address | dns-name}`
4. `show ntp peers`
5. `copy running-config startup-config`

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	ntp server {ip-address ipv6-address dns-name} Example: switch(config)# ntp server 192.0.2.10	Forms an association with a server.
Step 3	ntp peer {ip-address ipv6-address dns-name} switch(config)# ntp peer 2001:0db8::4101	Forms an association with a peer. You can specify multiple peer associations.
Step 4	show ntp peers Example: switch(config)# show ntp peers	(Optional) Displays the configured server and peers. Note A domain name is resolved only when you have a DNS server configured.
Step 5	copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	(Optional) Saves this configuration change.

This example shows how to configure an NTP server and peer:

```
switch# config t
switch(config)# ntp server 192.0.2.10
switch(config)# ntp peer 2001:0db8::4101
```

Verifying CDP and NTP Configuration

To display CDP configuration information, perform one of the following tasks:

Command	Purpose
show cdp all	Displays all interfaces that have CDP enabled.
show cdp entry {all name entry-name}	Displays the CDP database entries.
show cdp global	Displays the CDP global parameters.
show cdp interface interface-type slot/port	Displays the CDP interface status.
show cdp neighbors {device-id interface interface-type slot/port} [detail]	Displays the CDP neighbor status. The device-id keyword is supported in Cisco NX-OS Release 4.0(2) and later.
show cdp traffic interface interface-type slot/port	Displays the CDP traffic statistics on an interface.

Send document comments to nexus7k-docfeedback@cisco.com.

Use the **clear cdp counters** command to clear CDP statistics on an interface.

Use the **clear cdp table** command to clear the CDP cache for one or all interfaces.

To display NTP configuration information, perform one of the following tasks:

Command	Purpose
show ntp peer-status	Displays the status for all NTP servers and peers.
show ntp peers	Displays all the NTP peers.
show ntp statistics {io local memory peer {ip-address dns-name}}	Displays the NTP statistics
show ntp status	Displays the NTP distribution status

Use the **clear ntp session** command to clear the NTP sessions.

Use the **clear ntp statistics** command to clear the NTP statistics.

CDP and NTP Example Configuration

This example enables the CDP feature and configures the refresh and hold timers:

```
config t
feature cdp
cdp timer 50
cdp holdtime 100
```

This example configures an NTP server:

```
config t
ntp server 192.0.2.10
```

Default Settings

Table 2-1 lists the default settings for CDP and NTP parameters.

Table 2-1 Default CDP and NTP Parameters

Parameters	Default
CDP	Enabled globally and on all interfaces
CDP version	Version 2
CDP device ID	Serial number
CDP timer	60 seconds
CDP hold timer	180 seconds
NTP	Disabled

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

Additional References

For additional information related to implementing CDP and NTP, see the following sections:

- [Related Documents, page 2-12](#)
- [MIBs, page 2-12](#)

Related Documents

Related Topic	Document Title
CDP and NTP CLI commands	<i>Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 4.0</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/system_management/command/reference/sm_cmd_ref.html
VDCs and VRFs	<i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/virtual_device_context/configuration/guide/vdc_nx-os_book.html

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> • CISCO-CDP-MIB • CISCO-NTP-MIB 	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for CDP and NTP

[Table 2-2](#) lists the release history for this feature.

Table 2-2 Feature History for CDP and NTP

Feature Name	Releases	Feature Information
NTP protocol	4.0(3)	Added ability to disable the NTP protocol.