



CHAPTER 2

Configuring Basic Interface Parameters

This chapter describes how to configure the basic interface parameters for interfaces managed by Cisco DCNM.



Note

The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter includes the following sections:

- [Information About the Basic Interface Parameters, page 2-1](#)
- [Licensing Requirements, page 2-9](#)
- [Guidelines and Limitations, page 2-10](#)
- [Configuring the Basic Interface Parameters, page 2-11](#)
- [Field Descriptions, page 2-25](#)
- [Additional References, page 2-34](#)
- [Feature History for Configuring Basic Interface Parameters, page 2-35](#)



Note

To configure the parameters that are specifically used for Layer 2 interfaces (access or trunking interfaces), see [Chapter 3, “Configuring Layer 2 Interfaces.”](#) To configure parameters that are specifically used for Layer 3 interfaces (routed interfaces, subinterfaces, VLAN interfaces, loopback interfaces, and IP tunnels), see [Chapter 4, “Configuring Layer 3 Interfaces.”](#)

Information About the Basic Interface Parameters

This section includes the following topics:

- [Description, page 2-2](#)
- [Beacon, page 2-2](#)
- [MDIX, page 2-2](#)
- [Debounce Timer, page 2-2](#)
- [Error Disabled, page 2-3](#)
- [Rate Mode, page 2-3](#)

Send document comments to nexus7k-docfeedback@cisco.com

- [Speed Mode and Duplex Mode, page 2-4](#)
- [Flow Control, page 2-5](#)
- [Port MTU Size, page 2-5](#)
- [Bandwidth, page 2-6](#)
- [Throughput Delay, page 2-6](#)
- [Administrative Status, page 2-6](#)
- [Unidirectional Link Detection Parameter, page 2-6](#)
- [Carrier Delay, page 2-9](#)
- [Port-Channel Parameters, page 2-9](#)

Description

For the Ethernet and management interfaces, you can configure the description parameter to provide a recognizable name for the interface. Using a unique name for each interface allows you to quickly identify the interface when you are looking at a listing of multiple interfaces.

For information on setting the description parameter for port-channel interfaces, see the [“Configuring a Port-Channel Description” section on page 5-20](#). For information on configuring this parameter for other interfaces, see the [“Configuring the Description” section on page 2-13](#).

Beacon

The beacon mode allows you to identify a physical port by flashing its link state LED with a green light. By default, this mode is disabled. To identify the physical port for an interface, you can activate the beacon parameter for the interface.

For information on configuring the beacon parameter, see the [“Configuring the Beacon Mode” section on page 2-14](#).

MDIX

The medium dependent interface crossover (MDIX) parameter enables or disables the detection of a crossover connection between devices. This parameter applies only to copper interfaces. By default, this parameter is enabled.

For information on configuring the MDIX parameter, see the [“Configuring the MDIX Parameter” section on page 2-16](#).

Debounce Timer

The debounce timer delays notification of a link change, which can decrease traffic loss due to network reconfiguration. You can configure the debounce timer separately for each Ethernet port and specify the delay time in milliseconds. By default, this parameter is set for 100 milliseconds.

Send document comments to nexus7k-docfeedback@cisco.com



Caution

Enabling the debounce timer causes the link-up and link-down detections to be delayed, which results in a loss of traffic during the debounce period. This situation might affect the convergence and reconvergence of some Layer 2 and Layer 3 protocols.

For information on configuring the debounce-timer parameters, see the “[Configuring the Debounce Timer](#)” section on page 2-16.

Error Disabled

A port is in the error-disabled (err-disabled) state when the port is enabled administratively (using the **no shutdown** command) but disabled at runtime by any process. For example, if UDLD detects a unidirectional link, the port is shut down at runtime. However, because the port is administratively enabled, the port status displays as err-disable. Once a port goes into the err-disable state, you must manually reenble it or you can configure a timeout value that provides an automatic recovery. By default, the automatic recovery is not configured, and by default the err-disable detection is enabled for all causes.

You can configure the automatic error-disabled recovery timeout for a particular error-disabled cause and configure the recovery period.

Rate Mode

On a 32-port 10-Gigabit Ethernet module, each set of four ports can handle 10 gigabits per second (Gb/s) of bandwidth. You can use the rate-mode parameter to dedicate that bandwidth to the first port in the set of four ports or share the bandwidth across all four ports.

[Table 2-1](#) identifies the ports that are grouped together to share each 10 Gb/s of bandwidth and which port in the group can be dedicated to utilize the entire bandwidth.

Table 2-1 *Dedicated and Shared Ports*

Ports Groups that Can Share Bandwidth	Ports that Can be Dedicated to Each 10-Gigabit Ethernet of Bandwidth
1, 3, 5, 7	1
2, 4, 6, 8	2
9, 11, 13, 15	9
10, 12, 14, 16	10
17, 19, 21, 23	17
18, 20, 22, 24	18
25, 27, 29, 31	25
26, 28, 30, 32	26

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

All ports in each port group must be part of the same virtual device context (VDC). For more information on VDCs, see the *Cisco DCNM Virtual Device Context Configuration Guide, Release 4.2*.

Speed Mode and Duplex Mode

The speed mode and duplex mode are interrelated for each Ethernet and management interface. By default, each of these interfaces autonegotiates its speed and duplex mode with the other interface, but you can change these settings. If you change the settings, be sure to use the same speed and duplex mode setting on both interfaces, or use autonegotiation for at least one of the interfaces. [Table 2-2](#) shows the settings that work for each type of Ethernet and management interface.

Table 2-2 Speed- and Duplex-Mode Settings Used for Ethernet and Management Interfaces

Module Type	Speed Mode Setting	Duplex Mode Setting	Operational Speed (Mb/s)	Operational Duplex Mode
32-port 10-Gigabit Ethernet	Auto ¹	Auto ¹	10,000	Full
48-port 10/100/1000 Ethernet	Auto ¹		1000	Full
			10 or 100	Half
	1000	Auto ¹ or full	1000	Full
	100	Auto ¹ or half	100	Half
		Full	100	Full
	10	Auto ¹ or half	10	Half
Full		10	Full	
Management	Auto ¹		1000	Full
			10 or 100	Half
	1000	Auto ¹ or full	1000	Full
	100	Auto ¹ or half	100	Half
		Full	100	Full
	10	Auto ¹ or half	10	Half
Full		10	Full	

1. Default setting

For information on setting the speed mode and duplex mode for port-channel interfaces, see the [“Configuring the Speed and Duplex Settings for a Port-Channel Interface”](#) section on page 5-21. For information on setting the speed and duplex speed for other interfaces, see the [“Configuring the Interface Speed and Duplex Mode”](#) section on page 2-17.

Send document comments to nexus7k-docfeedback@cisco.com

Flow Control

When the receive buffer for an Ethernet port that runs 1 Gb/s or faster fills, flow control enables that port to send an IEEE 802.3x pause frame to the transmitting port to request it to stop transmitting data for a specified amount of time. Transmitting ports, running at any speed, can receive the pause frames to stop their transmission of data.

To allow flow control to work between two ports, you must set the corresponding receive and send flow control parameters for both ports as enabled or desired. When you set the parameter to enabled, the send or receive flow-control function is activated regardless of the setting of the other port. When you set the parameter to desired, the send or receive flow-control function is activated if you set the corresponding flow-control state of the other port to enabled or desired. If you set one of the flow control states to disabled, flow control is disabled for that transmission direction. To see how the different port flow-control states affect the link flow-control state, see [Table 2-3](#).

Table 2-3 Port Flow-Control Influences on Link Flow Control

Port flow control states		Link Flow Control State
Port Receiving Data (Sends Pause Frames)	Port Transmitting Data (Receives Pause Frames)	
Enabled	Enabled	Enabled
Enabled	Desired	Enabled
Enabled	Disabled	Disabled
Desired	Enabled	Enabled
Desired	Desired	Enabled
Desired	Disabled	Disabled
Disabled	Enabled	Disabled
Disabled	Desired	Disabled
Disabled	Disabled	Disabled

For information on setting the flow-control parameters, see the “[Configuring the Flow Control](#)” section on [page 2-18](#).

Port MTU Size

The maximum transmission unit (MTU) size specifies the maximum frame size that an Ethernet port can process. For transmissions to occur between two ports, you must configure the same MTU size for both ports. A port drops any frames that exceed its MTU size.

By default, each port has an MTU of 1500 bytes, which is the IEEE 802.3 standard for Ethernet frames. Larger MTU sizes are possible for more efficient processing of data with less overhead. The larger frames, called jumbo frames, can be up to 9216 bytes in size, which is also the default system jumbo MTU size.

On a Layer 3 interface, you can configure an MTU size between 576 and 9216 bytes. You can configure up to 64 MTU settings for each I/O module.

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

The global LAN port MTU size applies to the traffic through a Layer 3 Ethernet LAN port that is configured with a nondefault MTU size.

For a Layer 2 port, you can configure an MTU size that is either the system default (1500 bytes) or the system jumbo MTU size (initially 9216 bytes).

**Note**

If you change the system jumbo MTU size, Layer 2 ports automatically use the system default MTU size (1500 bytes) unless you specify the new system jumbo MTU size for some or all of those ports.

For information on setting the MTU size, see the [“Configuring the MTU Size” section on page 2-19](#).

Bandwidth

Ethernet ports have a fixed bandwidth of 1,000,000 Kb at the physical level. Layer 3 protocols use a bandwidth value that you can set for calculating their internal metrics. The value that you set is used for informational purposes only by the Layer 3 protocols—it does not change the fixed bandwidth at the physical level. For example, the Interior Gateway Routing Protocol (IGRP) uses the minimum path bandwidth to determine a routing metric, but the bandwidth at the physical level remains at 1,000,000 Kb.

For information on configuring the bandwidth parameter for other interfaces, see the [“Configuring the Bandwidth” section on page 2-21](#).

Throughput Delay

Specifying a value for the throughput-delay parameter provides a value used by Layer 3 protocols; it does not change the actual throughput delay of an interface. The Layer 3 protocols can use this value to make operating decisions. For example, the IGRP can use the delay setting to differentiate between a satellite link and a land link. The delay value that you set is in the tens of microseconds.

For information on configuring the throughput-delay parameter, see the [“Configuring the Throughput Delay” section on page 2-21](#).

Administrative Status

The administrative-status parameter determines whether an interface is up or down. When an interface is administratively down, it is disabled and unable to transmit data. When an interface is administratively up, it is enabled and able to transmit data.

For information on configuring the administrative status parameter for port-channel interfaces, see the [“Shutting Down and Restarting the Port-Channel Interface” section on page 5-18](#). For information on configuring the administrative-status parameter for other interfaces, see the [“Shutting Down and Activating the Interface” section on page 2-22](#).

Unidirectional Link Detection Parameter

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

- [UDLD Overview, page 2-7](#)
- [Default UDLD Configuration, page 2-8](#)
- [UDLD Aggressive and Nonaggressive Modes, page 2-8](#)

UDLD Overview

The Cisco-proprietary Unidirectional Link Detection (UDLD) protocol allows devices that are connected through fiber-optic or copper (for example, Category 5 cabling) Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a device detects a unidirectional link, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops.

UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected LAN ports. When you enable both autonegotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic transmitted by the local device over a link is received by the neighbor but traffic transmitted from the neighbor is not received by the local device. If one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up. In this case, the logical link is undetermined, and UDLD does not take any action. If both fibers are working normally at Layer 1, then UDLD at Layer 2 determines whether those fibers are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation, because autonegotiation operates at Layer 1.

The Cisco Nexus 7000 Series device periodically transmits UDLD frames to neighbor devices on LAN ports with UDLD enabled. If the frames are echoed back within a specific time frame and they lack a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down. Devices on both ends of the link must support UDLD in order for the protocol to successfully identify and disable unidirectional links. You can configure the transmission interval for the UDLD frames, either globally or for the specified interfaces.



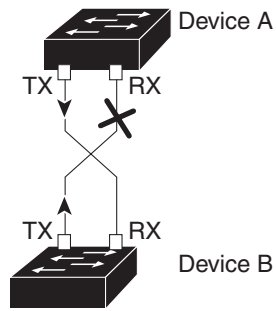
Note

By default, UDLD is locally disabled on copper LAN ports to avoid sending unnecessary control traffic on this type of media.

[Figure 2-1](#) shows an example of a unidirectional link condition. Device B successfully receives traffic from device A on the port. However, device A does not receive traffic from device B on the same port. UDLD detects the problem and disables the port.

Send document comments to nexus7k-docfeedback@cisco.com

Figure 2-1 Unidirectional Link



187781

Default UDLD Configuration

Table 2-4 shows the default UDLD configuration.

Table 2-4 UDLD Default Configuration

Feature	Default Value
UDLD global enable state	Globally disabled
UDLD per-port enable state for fiber-optic media	Enabled on all Ethernet fiber-optic LAN ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX LAN ports
UDLD aggressive mode	Disabled
UDLD message interval	15 seconds

For information on configuring the UDLD for the device and its port, see the “[Configuring the UDLD Mode](#)” section on page 2-23.

UDLD Aggressive and Nonaggressive Modes

UDLD aggressive mode is disabled by default. You can configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. If UDLD aggressive mode is enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD frame, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

To prevent spanning tree loops, nonaggressive UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When you enable the UDLD aggressive mode, the following occurs:

- One side of a link has a port stuck (both transmission and receive)
- One side of a link remains up while the other side of the link is down

In these cases, the UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

You enable the UDLD aggressive mode globally to enable that mode on all the fiber ports. You must enable the UDLD aggressive mode on copper ports on specified interfaces.

Carrier Delay

**Note**

You can configure the carrier delay timer only on VLAN network interfaces; you cannot configure this timer in any other interface modes. See [Chapter 4, “Configuring Layer 3 Interfaces”](#) for information on configuring VLAN network interfaces.

If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the device is not aware that a link-down event occurred. A large carrier delay timer results in fewer link-up/link-down events being detected. When you set the carrier delay time to 0, the device detects each link-up/link-down event that occurs.

In most environments, a lower carrier delay time is better than a higher one. The exact value that you choose depends on the nature of the link outages and how long you expect these linkages to last in your network. If your data links are subject to short outages (especially if those outages last less time than it takes for your IP routing to converge), you should set a long carrier delay value to prevent these short outages from causing unnecessary problems in your routing tables. However, if your outages tend to be longer, then you may want to set a shorter carrier delay time so that the outages are detected sooner, and the IP route convergence begins and ends sooner.

The default carrier-delay time is 2 seconds or 50 milliseconds.

Port-Channel Parameters

A port channel is an aggregation of physical interfaces that comprise a logical interface. You can bundle up to eight individual interfaces into a port channel to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational if at least one physical interface within the port channel is operational.

You can create a Layer 2 port channel by bundling compatible Layer 2 interfaces, or you can create Layer 3 port channels by bundling compatible Layer 3 interfaces. You cannot combine Layer 2 and Layer 3 interfaces in the same port channel.

Any configuration changes that you apply to the port channel are applied to each interface member of that port channel.

For information on port channels and for information on configuring port channels, see [Chapter 5, “Configuring Port Channels.”](#)

Licensing Requirements

The following table shows the licensing requirements for this feature:

Send document comments to nexus7k-docfeedback@cisco.com

Product	License Requirement
DCNM	The basic interface parameters require a LAN Enterprise license.
NX-OS	The basic interface parameters 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> .



Note

Using VDCs requires an Advanced Services license.

Guidelines and Limitations

Follow these guidelines and limitations for configuring the basic interface parameters:

- Fiber-optic Ethernet ports must use Cisco-supported transceivers. To verify that the ports are using Cisco-supported transceivers, use the **show interface transceivers** command. Interfaces with Cisco-supported transceivers are listed as functional interfaces.
- A port can be either a Layer 2 or a Layer 3 interface; it cannot be both simultaneously. By default, each port is a Layer 3 interface.
- When configuring flow control for a local port, consider the following:
 - To receive pause frames when you do not know how the remote port send parameter is configured, set the local port receive parameter to desired.
 - To receive pause frames when you know that the remote port send parameter is enabled or desired, set the local port receive parameter to enabled.
 - To ignore received pause frames, set the local port receive parameter to disabled.
 - To send pause frames when you do not know how the remote port receive parameter is configured, set the local port send parameter to desired.
 - To send pause frames when you know that the remote port receive parameter is enabled or desired, set the local port send parameter to enabled.
 - To prevent the sending of pause frames, set the local port send parameter to disabled.
- You usually configure Ethernet port speed and duplex mode parameters to auto to allow the system to negotiate the speed and duplex mode between ports. If you decide to configure the port speed and duplex modes manually for these ports, consider the following:
 - Before you configure the speed and duplex mode for an Ethernet or management interface, see [Table 2-2 on page 2-4](#) for the combinations of speeds and duplex modes that can be configured at the same time.
 - If you set the Ethernet port speed to auto, the device automatically sets the duplex mode to auto.
 - If you configure an Ethernet port speed to a value other than auto (for example, 10, 100, or 1000 Mb/s), you must configure the connecting port to match. Do not configure the connecting port to negotiate the speed.

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

The device cannot automatically negotiate the Ethernet port speed and duplex mode if the connecting port is configured to a value other than auto.

**Caution**

Changing the Ethernet port speed and duplex mode configuration might shut down and reenables the interface.

Configuring the Basic Interface Parameters

When you configure an interface, you must specify the interface before you can configure its parameters.

The following sections explain how to specify the interface and configure each of its basic parameters:

- [Specifying the Interfaces to Configure, page 2-11](#)
- [Configuring the Description, page 2-13](#)
- [Configuring the Beacon Mode, page 2-14](#)
- [Changing the Bandwidth-Rate Mode, page 2-15](#)
- [Configuring the Error-Disabled State, page 2-15](#)[Configuring the MDIX Parameter, page 2-16](#)
- [Configuring the Debounce Timer, page 2-16](#)
- [Configuring the Interface Speed and Duplex Mode, page 2-17](#)
- [Configuring the Flow Control, page 2-18](#)
- [Configuring the MTU Size, page 2-19](#)
- [Configuring the Bandwidth, page 2-21](#)
- [Configuring the Throughput Delay, page 2-21](#)
- [Shutting Down and Activating the Interface, page 2-22](#)
- [Enabling or Disabling CDP, page 2-22](#)
- [Configuring the UDLN Mode, page 2-23](#)
- [Configuring the Carrier Delay Timer, page 2-24](#)

Specifying the Interfaces to Configure

Before you can configure the parameters for one or more interfaces of the same type, you must specify the type and the identities of the interfaces.

[Table 2-5](#) shows the interface types and identities that you should use for specifying the Ethernet and management interfaces.

Table 2-5 Information Needed to Identify an Interface for Configurations

Interface Type	Identity
Ethernet	I/O module slot numbers and port numbers on the module.
Management	0 (for port 0)

Send document comments to nexus7k-docfeedback@cisco.com

To display status and diagnostic information for SFP interfaces, see the “Field Descriptions” section on page 2-25.

DETAILED STEPS

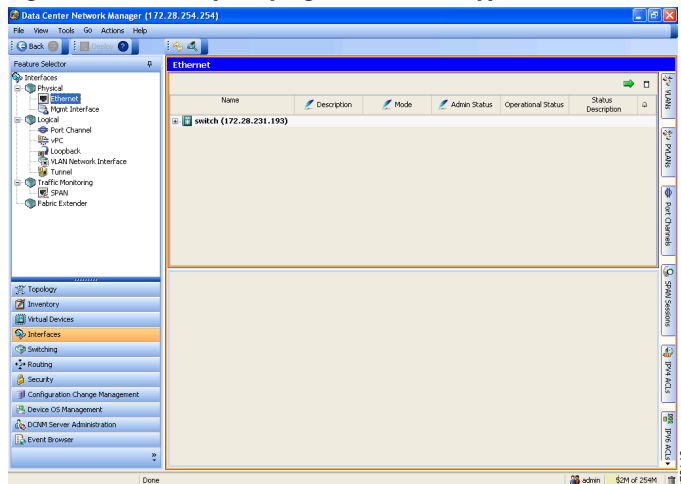
To specify the interfaces to configure, follow these steps:

- Step 1** From the Feature Selector pane, specify the type of interfaces that you are configuring by following these steps:
- a. Choose **Interfaces**.
 - b. Choose **Physical** or **Logical**.
 - To work with Ethernet interfaces or the management interface, choose **Physical**.
 - To work with port-channel interfaces, loopback interfaces, VLAN network interfaces, or tunnel interfaces, choose **Logical**.
 - c. If you are working with physical interfaces, choose one of the following interface types:
 - To configure Ethernet interface parameters, choose **Ethernet**.
 - To configure management interface parameters, choose **Mgmt Interface**.
 - d. If you are working with logical interfaces, choose one of the following interface types:
 - **Port Channel**
 - **Loopback**
 - **VLAN Network Interface**
 - **Tunnel**

The devices with the interface type that you specified appear in the Summary pane.

Figure 2-2 shows the Feature Selector items to choose to specify an interface type.

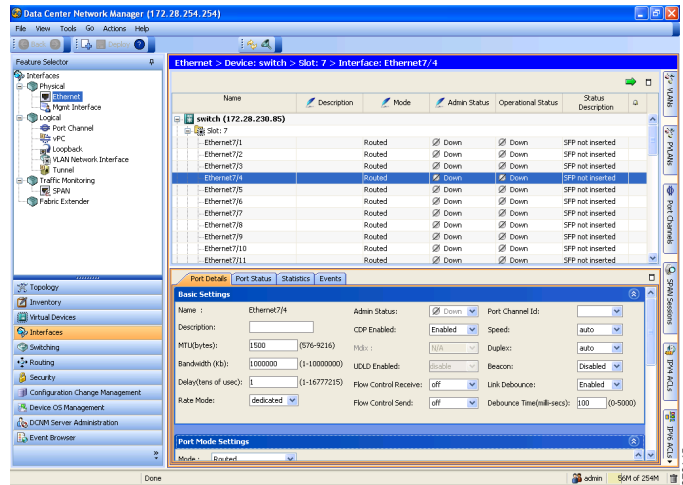
Figure 2-2 Specifying an Interface Type



- Step 2** From the Summary pane, specify the device and (optionally) the port in one of the following ways:
- If you specified the Ethernet interface type, expand the device, expand the slot for the appropriate I/O module, and click the appropriate port as shown in Figure 2-3.

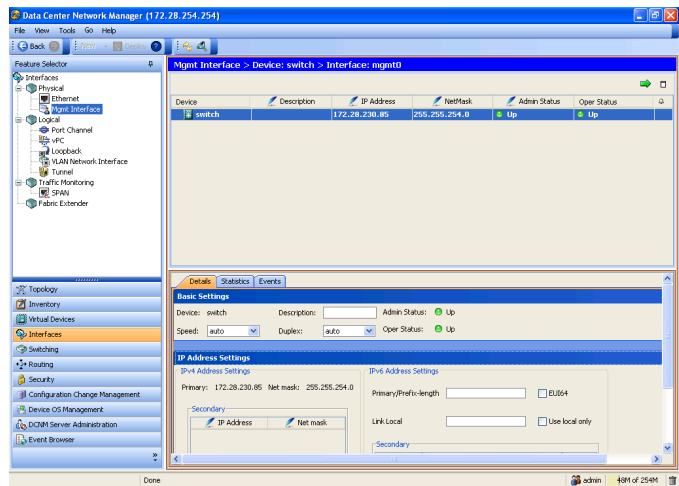
Send document comments to nexus7k-docfeedback@cisco.com

Figure 2-3 Specifying a Port for an Ethernet Interface



- If you specified the management interface type, click the device as shown in [Figure 2-4](#).

Figure 2-4 Specifying a Device for a Management Interface



Tabs and sections for displaying detailed information for the interface that you specified appear in the Details pane.

Configuring the Description

You can provide textual interface descriptions for the Ethernet and management interfaces. Descriptions can be a maximum of 80 case-sensitive alphanumeric characters.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical**.
- Step 2** Choose **Ethernet** or **Mgmt Interface**.
The devices with the interface type that you specified appear in the Summary pane.
- Step 3** From the Summary pane, specify the interface by doing one of the following:
- To configure the Ethernet interface, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - To configure the management interface, click the device that you are configuring.
Tabs appear for the device information in the Details pane. The Details tab is active but its sections are not expanded.
- Step 4** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
- Step 5** In the Description field, enter the appropriate textual description for the interface.
- Step 6** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the Beacon Mode

You can enable the beacon mode for an Ethernet port to flash its LED to confirm its physical location.

DETAILED STEPS

To enable or disable the beacon mode, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.
- Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
- Step 3** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
- Step 4** From the Beacon drop-down list, choose **Enabled** or **Disabled**.
- Step 5** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to nexus7k-docfeedback@cisco.com

Changing the Bandwidth-Rate Mode

On a 32-port 10-Gigabit Ethernet module, each set of four ports can handle 10 gigabits per second (Gb/s) of bandwidth. You can use the rate-mode parameter to dedicate that bandwidth to the first port in the set of four ports or share the bandwidth across all four ports.

DETAILED STEPS

To enable dedicated or shared rate mode, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.
 - Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - Step 3** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
 - Step 4** If you have selected a port that allows dedicated rate mode, from the Rate Mode drop-down list, choose **dedicated** or **shared**.
 - Step 5** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the Error-Disabled State

You can view the reason an interface moves to the error-disabled state and configure automatic recovery.

DETAILED STEPS

To configure the detection and automatic recovery of error-disabled interfaces, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.
 - Step 2** From the Summary pane, click the device.
Tabs appear for the device information in the Details pane.
 - Step 3** Click the Error Disable Settings Section.
The section expands and separate fields for Detection and Recovery appear.
 - Step 4** In the Detection section, click the causes for which you want to detect all error-disable interfaces.
 - Step 5** In the Recovery Interval field of the Recovery section, enter the automatic recovery time interval that you want in seconds.
The range is 30 to 65535 seconds.
 - Step 6** In the Recovery section, click the error-disabled causes from which you want the interfaces to automatically recover.

Send document comments to nexus7k-docfeedback@cisco.com

Step 7 (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring the MDIX Parameter

If you need to detect the type of connection (crossover or straight) with another copper Ethernet port, enable the medium dependent independent crossover (MDIX) parameter for the local port. By default, this parameter is enabled.

BEFORE YOU BEGIN

You must enable MDIX for the remote port.

DETAILED STEPS

To enable or disable an MDIX connection, follow these steps:

- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.
- Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
- Step 3** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
- Step 4** From the Mdx drop-down list, choose either **enabled** or **disabled**.
- Step 5** ((Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the Debounce Timer

You can enable or disable the debounce timer by using the Link Debounce and Debounce Time fields. In the Link Debounce field, you enable or disable the timer. In the Debounce Time field, you specify the time in milliseconds (ms).



Note

If you specify a time of 0 ms, the timer is disabled even if you enable the timer in the Link Debounce field.

DETAILED STEPS

To enable or disable the debounce timer, follow these steps:

- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.

Send document comments to nexus7k-docfeedback@cisco.com

- Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
- Step 3** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
- Step 4** From the Link Debounce drop-down list, choose **Enabled** or **Disabled**.
- Step 5** From the Debounce Time field, type the number of milliseconds (0 to 5000) for the debounce time.
A time of 0 milliseconds effectively disables the debounce timer. A time of 1 to 5000 milliseconds is used only if you enabled the timer.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the Interface Speed and Duplex Mode

The interface speed and duplex mode are interrelated, so you should configure both of their parameters at the same time.

To see which speeds and duplex modes you can configure together for Ethernet and management interfaces, see [Table 2-2 on page 2-4](#).



Note

The interface speed that you specify can affect the duplex mode used for an interface, so you should set the speed before setting the duplex mode. If you set the speed for autonegotiation, the duplex mode is automatically set to be autonegotiated. If you specify 10- or 100-Mb/s speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mb/s (1 Gb/s) or faster, full duplex is automatically used.

BEFORE YOU BEGIN

Make sure that the remote port has a speed setting that supports your changes for the local port. If you want to set the local port to use a specific speed, you must set the remote port for the same speed or set the local port to autonegotiate the speed.

DETAILED STEPS

To configure the interface speed and duplex mode, follow these steps:

- Step 1** From the Feature Selector pane, choose **Interfaces > Physical**.
- Step 2** Choose **Ethernet** or **Mgmt Interface**.
The devices with the interface type that you specified appear in the Summary pane.
- Step 3** From the Summary pane, specify the interface by doing one of the following:
- To configure the Ethernet interface, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - To configure the management interface, click the device that you are configuring.

Send document comments to nexus7k-docfeedback@cisco.com

Tabs appear for the device information in the Details pane. The Details tab is active but its sections are not expanded.

- Step 4** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
- Step 5** In the Speed field, choose the appropriate speed for your port.
- Step 6** In the Duplex field, choose **full**, **half**, or **auto**.
If one of these options is not available, change the interface speed (see the previous step).
- Step 7** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring the Flow Control

For Ethernet ports that run at 1 Gb/s or faster, you can enable or disable the port's ability to send and receive flow-control pause frames. For Ethernet ports that run slower than 1 Gb/s, you can enable or disable only the port's ability to receive pause frames.

When enabling flow control for the local port, you either fully enable the local port to send or receive frames regardless of the flow-control setting of the remote port, or you set the local port to use the desired setting used by the remote port. If you enable both the local and remote port for flow control, or set the desired flow control of the other port, or set a combination of those two states, flow control is enabled for those ports.



Note

For ports that run at 10 Gb/s, you cannot use the desired state for the send or receive parameter.

BEFORE YOU BEGIN

Make sure that the remote port has the corresponding setting for the flow control that you need. If you want the local port to send flow-control pause frames, make sure that the remote port has a receive parameter set to on or desired. If you want the local port to receive flow-control frames, make sure that the remote port has a send parameter set to on or desired. If you do not want to use flow control, you can set the remote port's send and receive parameters to off.

DETAILED STEPS

To configure the interface flow control, follow these steps:

- Step 1** From the Feature Selector, choose **Interfaces > Physical > Ethernet**.
The Summary pane lists the devices with Ethernet interfaces.
- Step 2** From the Summary pane, expand the switch, expand the slot, and select the port.
The Details pane shows tabs and an unexpanded Basic Settings section for the port.
- Step 3** From the Details pane, click **Port Details** and **Basic Settings**.
The Basic Settings section expands to show the basic parameters used for multiple features.
- Step 4** From the Flow Control Receive drop-down list, choose how to receive flow control frames as follows:
- To disable the receiving of pause frames, choose **off**.

Send document comments to nexus7k-docfeedback@cisco.com

- To use the send flow control setting for the receive flow control setting, choose **desired**.
- To enable the receiving of pause frames regardless of the send setting for the other port, choose **on**.

Step 5 From the Flow Control Send drop-down list, choose **desired**, **on**, or **off**.

- To disable the sending of pause frames, choose **off**.
- To use the receive flow control setting for the send flow control setting, choose **desired**.
- To enable the sending of pause frames regardless of the receive setting for the other port, choose **on**.

Step 6 (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring the MTU Size

You can configure the maximum transmission unit (MTU) size for Layer 2 and Layer 3 Ethernet interfaces. For Layer 3 interfaces, you can configure the MTU to be between 576 and 9216 bytes (even values are required). For Layer 2 interfaces, you can configure the MTU to be either the system default MTU (1500 bytes) or the system jumbo MTU size (which has the default size of 9216 bytes).



Note

You can change the system jumbo MTU size, but if you change that value, you should also update the Layer 2 interfaces that use that value so that they use the new system jumbo MTU value. If you do not update the MTU value for Layer 2 interfaces, those interfaces will use the system default MTU (1500 bytes).

By default, Cisco NX-OS configures Layer 3 parameters. If you want to configure Layer 2 parameters, you need to switch the port mode to Layer 2.

You change the port mode by clicking Port Details and Port Mode Settings in the Details pane and then choosing a Layer 2 mode (Access, Trunk, PVLAN Host, or PVLAN Promiscuous).

After changing the port mode to Layer 2, you can return to configuring Layer 3 interfaces by changing the port mode again, by clicking Port Details and Port Mode Settings, and then choosing a Layer 3 mode (Routed).

This section includes the following topics:

- [Configuring the Interface MTU Size, page 2-19](#)
- [Configuring the System Jumbo MTU Size, page 2-20](#)

Configuring the Interface MTU Size

For Layer 3 interfaces, you can configure an MTU size that is between 576 and 9216 bytes.

For Layer 2 interfaces, you can configure all Layer 2 interfaces to use either the default MTU size (1500 bytes) or the system jumbo MTU size (default size of 9216 bytes).

If you need to use a different system jumbo MTU size for Layer 2 interfaces, see the [“Configuring the System Jumbo MTU Size” section on page 2-20](#).

DETAILED STEPS

To change an interface MTU size, follow these steps:

Send document comments to nexus7k-docfeedback@cisco.com

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
- The devices with Ethernet interfaces appear in the Summary pane.
- Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
- Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
- Step 3** If you are configuring Layer 2 interfaces, from the Summary pane, double-click the Mode settings, and then choose **Access**, **Trunk**, **PVLAN Host**, or **PVLAN Promiscuous** from the Mode drop-down list.



Note If you need to switch back to working with Layer 3 interfaces, choose **Routed** from the Mode drop-down list.

- Step 4** From the Details pane, expand the **Basic Settings** section.
- The Basic Settings section shows the basic parameters.
- Step 5** In the MTU field, type the preferred MTU size as follows:
- For Layer 2 interfaces, type either the default MTU size (1500) or the system jumbo MTU size (default size of 9216). If you have changed the system jumbo MTU size, you can use the new size for the system jumbo MTU size.
 - For Layer 3 interfaces, type an MTU size between 576 and 9216.
- Step 6** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the System Jumbo MTU Size

You can configure the system jumbo MTU size, which can be used to specify the MTU size for Layer 2 interfaces. You can specify an even number between 1500 and 9216. If you do not configure the system jumbo MTU size, it defaults to 1500 bytes.

DETAILED STEPS

To configure the system jumbo MTU size, follow these steps:

-
- Step 1** From the Feature Selector, choose **Interfaces > Physical > Ethernet**.
- The devices for the type that you specified appear in the Summary pane.
- Step 2** From the Summary pane, click on the device.
- Tabs appear for the device information in the Details pane. The Details tab is active but its sections are not expanded.
- Step 3** From the Details pane, expand the **MTU Settings** section.
- Step 4** The MTU Settings section shows the system jumbo MTU information.
- Step 5** In the Jumbo MTU field, enter the size as an even integer between 1500 and 9216.
- Step 6** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to nexus7k-docfeedback@cisco.com

Configuring the Bandwidth

You can configure the bandwidth for Ethernet interfaces. The physical level uses an unchangeable bandwidth of 1 GB, but you can configure a value of 1 to 10,000,000 Kb for Level 3 protocols.

DETAILED STEPS

To change the interface bandwidth, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.
 - Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - Step 3** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
 - Step 4** In the Bandwidth field, type the number of kilobits (between 1 and 10,000,000 [omit the commas]) for the bandwidth.
 - Step 5** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the Throughput Delay

You can configure the interface throughput delay for Ethernet interfaces. The actual delay time does not change, but you can set an informational value between 1 and 16777215, where the value represents the number of tens of microseconds.

DETAILED STEPS

To change the informational value of the interface throughput delay, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
The devices with Ethernet interfaces appear in the Summary pane.
 - Step 2** From the Summary pane, expand the device, expand the slot, and click the port.
Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - Step 3** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
 - Step 4** In the Delay field, type the number of tens of microseconds to use for the delay time.
For example, for a delay of 10,000 microseconds, type 1000.
 - Step 5** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to nexus7k-docfeedback@cisco.com

Shutting Down and Activating the Interface

You can shut down and restart Ethernet or management interfaces. When you shut down interfaces, they become disabled and all monitoring displays show them as being down. This information is communicated to other network servers through all dynamic routing protocols. When the interfaces are shut down, the interface is not included in any routing updates. To activate the interface, you must restart the device.

DETAILED STEPS

To change the administrative status for an interface, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical**.
- Step 2** Choose **Ethernet** or **Mgmt Interface**.
- The devices with the interface type that you specified appear in the Summary pane.
- Step 3** From the Summary pane, specify the interface by doing one of the following:
- To configure the Ethernet interface, expand the device, expand the slot, and click the port. Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - To configure the management interface, click the device that you are configuring. Tabs appear for the device information in the Details pane. The Details tab is active but its sections are not expanded.
- Step 4** From the Details pane, expand the **Basic Settings** section.
- The Basic Settings section shows the basic parameters.
- Step 5** From the Admin Status drop-down list, choose **Down**.
- Step 6** From the Admin Status drop-down list, choose **Up**.
- Step 7** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Enabling or Disabling CDP



Note

For complete information on configuring the Cisco Discovery Protocol (CDP) using the command-line interface (CLI), see the *Cisco NX-OS System Management Configuration Guide*.

You can enable or disable CDP for Ethernet and management interfaces. This protocol works only when you have it enabled on both interfaces on the same link.


BEFORE YOU BEGIN

Make sure that the remote port also has this protocol enabled.

DETAILED STEPS

To enable or disable CDP for an interface, follow these steps:

Send document comments to nexus7k-docfeedback@cisco.com

-
- Step 1** Choose **Interfaces > Physical**.
- Step 2** Choose **Ethernet** or **Mgmt Interface**.
- The devices with the interface type that you specified appear in the Summary pane.
- Step 3** From the Summary pane, specify the interface by doing one of the following:
- To configure the Ethernet interface, expand the device, expand the slot, and click the port. Tabs appear for the port information in the Details pane. The Port Details tab is active but its sections are not expanded.
 - To configure the management interface, click the device that you are configuring. Tabs appear for the device information in the Details pane. The Details tab is active but its sections are not expanded.
- Step 4** From the Details pane, expand the **Basic Settings** section.
- The Basic Settings section shows the basic parameters.
- Step 5** From the CDP Enabled drop-down list, choose **Enabled** or **Disabled**.
-  **Note** For CDP to function, you must set both interfaces on the same link to Enabled. CDP cannot function if one or both interfaces have their CDP Enabled parameter set to Disabled.
-
- Step 6** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the UDLD Mode

You can configure normal or aggressive unidirectional link detection (UDLD) modes for Ethernet interfaces on devices configured to run UDLD. Before you can enable a UDLD mode for an interface, you must make sure that UDLD is already enabled on the device that includes the interface. UDLD must also be enabled on the other linked interface and its device.

To use the normal UDLD mode, you must configure one of the ports for normal mode and configure the other port for the normal or aggressive mode. To use the aggressive UDLD mode, you must configure both ports for the aggressive mode.

By default, UDLD is disabled for the 48-port, 10/100/1000 Ethernet module ports but the normal UDLD mode is enabled for the 32-port, 10-Gigabit Ethernet module ports.

BEFORE YOU BEGIN

You must enable UDLD for the other linked port and its device.

- 1.

DETAILED STEPS

To enable or disable the beacon mode, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.
- Step 2** The devices with Ethernet interfaces appear in the Summary pane.

Send document comments to nexus7k-docfeedback@cisco.com

- Step 3** From the Summary pane, click the device with the interface that will be using UDLD.
- Step 4** Choose **Actions > Enable UDLD**.
- Step 5** From the Summary pane, expand the switch, expand the slot, and click the port.
Tabs and unexpanded sections for the port appear in the Details pane.
- Step 6** From the Details pane, expand the **Basic Settings** section.
The Basic Settings section shows the basic parameters.
- Step 7** From the UDLD Enabled drop-down list, choose **Enabled, Disabled, Aggressive, or Global**.



Note To configure the UDLD message interval, use the Command Line Interface. See *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.x* for information on configuring this parameter.

- Step 8** (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring the Carrier Delay Timer

The carrier delay timer sets a time during which all link-down/link-up events are not detected by any of the other software on the device. When you configure a longer carrier delay time, fewer link-down/link-up events are recorded. When you configure the carrier delay time to 0, the device detects each link-down/link-up event.



Note You can configure the carrier delay timer only on VLAN network interfaces; you cannot configure this timer in any other interface modes.

You use the VLAN Network Interface pane to configure the carrier delay timer.

DETAILED STEPS

To set the carrier-delay timer, follow these steps:

- Step 1** From the Feature Selector pane, choose **Interfaces > Logical > VLAN Network Interface**.
- Step 2** From the Contents pane, in the Summary pane, double-click on the device that you want.
- Step 3** Click the VLAN network interface that you want to configure the carrier delay timer on.
The system highlights the selected VLAN network interface, and tabs appear in the Details pane.
- Step 4** In the Details pane, click the **Details** tab.
- Step 5** Click the **Basic Settings** section.
- Step 6** In the Carrier Delay field, enter the value that you want for this timer.
- Step 7** In the Carrier Delay field, click the pull-down menu and choose secs or msecs.
The default value is 2 seconds.

Send document comments to nexus7k-docfeedback@cisco.com

Step 8 (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Table 2-6 *Default Basic Interface Parameter Settings*

Parameters	Default
Description	Blank
Beacon	Disabled
Debounce timer	100 milliseconds
Bandwidth	Data rate of interface
Throughput delay	100 microseconds
Administrative status	Shutdown
MTU	1500 bytes
UDLD global	Globally disabled
UDLD per-port enable state for fiber-optic media	Enabled on all Ethernet fiber-optic LAN ports
UDLD per-port enable state for copper media	Disabled on all Ethernet 10/100 and 1000BASE-TX LAN ports
UDLD message interval	Disabled
UDLD aggressive mode	Disabled
Carrier delay	2 seconds or 50 milliseconds
Error disable	Disabled
Error disable recovery	Disabled
Error disable recovery interval	300 seconds
Link debounce	Enabled
Port profile	Disabled

Field Descriptions

This section describes the fields shown on the Ethernet pane and includes the following:

- [Device: Device Details: MTU Settings Section, page 2-26](#)
- [Device: Device Details: Error Disable Settings Section, page 2-26](#)
- [Device: Device Status Tab, page 2-27](#)
- [Port: Port Details: Basic Settings Section, page 2-27](#)
- [Port: Port Details: Port Mode Settings Section, page 2-28](#)
- [Port: Port Details: Advanced Settings Section, page 2-30](#)
- [Port: Port Status: Port Status Section, page 2-31](#)
- [Port: Port Status: Port Status SFP Section, page 2-32](#)
- [Port: Port Status: Port SFP Diagnostics Section, page 2-33](#)

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

Device: Device Details: MTU Settings Section

Table 2-7 Device: Device Details: MTU Settings Section

Field	Description
Jumbo MTU	System jumbo maximum transmission unit (MTU) size in bytes. The range is 1500 to 9216. The default is 1500.

Device: Device Details: Error Disable Settings Section

Table 2-8 Device: Device Details: Error Disable Settings Section

Field	Description
Discovery	
Select cause	Either all causes for the interface to be error-disabled or a specific cause.
Acl exception	ACL installation failures causes error-disabled state.
Link state flapping	The error-disabled status of a link that is rapidly going up and down.
Loopback	Loopback interface will be error-disabled.
Recovery	
Recovery Interval (sec)	The time interval for an interface to recover from an error-disabled state.
Select cause	Specified to enable error-disable recovery on an interface for all causes or for one of the following specific causes.
Link State Flapping	The interface is moving rapidly between the UP state and the DOWN state.
BPDU Guard	The BPDU Guard feature.
Psecure Violation	Psecure violation.
Storm Control	Storm control violation.
Security Violation	Port security violation.
UDLD	UDLD failure.

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

Device: Device Status Tab

Table 2-9 Device: Device Status Tab

Field	Description
Port Mode	<i>Display only.</i> Operational mode of the interface. It will be one of the following types: <ul style="list-style-type: none"> • Access • Trunk • PVLAN Host • PVLAN Promiscuous • Routed
Total	<i>Display only.</i> The total number of each port mode available in the device.
Active	<i>Display only.</i> The number of active ports for each port mode.
Admin Down	<i>Display only.</i> The number of ports that are administratively down for each port mode.
Operationally Down	<i>Display only.</i> The number of ports that are operationally down for each port mode.

Port: Port Details: Basic Settings Section

Table 2-10 Port: Port Details: Basic Settings Tab

Field	Description
Name	<i>Display only.</i> Interface name.
Description	Textual description (80 character maximum) of the interface.
MTU	Maximum transmission unit size in bytes. The range is 576 to 9216. The default is 1500.
Bandwidth	Bandwidth informational value used by Layer 3 protocols (this value does not change the actual bandwidth of the interface). The range is 1 to 10,000,000. The default is 10,000,000.
Delay	Throughput delay informational value used by Layer 3 protocols (this value does not change the actual throughput delay for the interface). The range is 1 to 16,777,215. The default is 1.
Rate Mode	Rate mode for selected port on those modules and ports that allow shared or dedicated rate mode.
Admin status	Administrative status for the interface. The choices are Up or Down. The default is Down.
CDP Enabled	Cisco Discovery Protocol used to learn about other connected devices. The choices are Enabled or Disabled. The default is Enabled.
Mdix	Medium dependent interface crossover (MDIX) detects crossover connections between interfaces. The choices are Enabled or Disabled. The default is Enabled.

Send document comments to nexus7k-docfeedback@cisco.com

Table 2-10 Port: Port Details: Basic Settings Tab

Field	Description
UDLD Enabled	Unidirectional Link Detection monitors the physical connections between interfaces to detect and disable unidirectional links. The choices are Enabled or Disabled. The default is Enabled.
Flow Control Receive	Received pause frames that request a pause in data transmission for a specific amount of time. This feature can be turned off, turned on, or set to a desired state (enabled if the Flow Control Send parameter for the other interface is enabled or set to desired). The choices are off, desired, or on. The default is desired.
Flow Control Send	Sent pause frames that request a pause in data transmission for the other interface for a specific amount of time. This feature can be turned off, turned on, or set to a desired state (enabled if the Flow Control Receive parameter for the other interface is enabled or set to desired). The choices are off, desired, or on. The default is desired.
Port Channel Id	Port channel that interface belongs to, if any. The default is blank.
Speed	Interface speed in megabits per second (Mb/s). The choices are 10, 100, 1000, or auto. The default is auto. The setting for this parameter determines the values that you can use for duplex mode.
Duplex mode	Duplex mode for the interface. The choices are full, half, and auto. The default is auto.
Beacon	LED to identify the interface on its module in the chassis. The choices are Enabled or Disabled. The default is Disabled.
Link Debounce	Notification of a link change that was delayed. The choices are Enabled or Disabled. The default is Enabled.
Debounce Time	Debounce delay time in milliseconds. The range is 0 to 5000. The default is 100.

Port: Port Details: Port Mode Settings Section

Table 2-11 Port: Port Details: Port Mode Settings: Section

Field	Description
Mode	Valid values are as follows: <ul style="list-style-type: none"> • Access • Trunk • PVLAN Host • PVLAN Promiscuous • Routed
Access	
Access VLAN	Access VLAN for this access port. The default access VLAN is the default VLAN, or VLAN1.

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

Table 2-11 Port: Port Details: Port Mode Settings: Section (continued)

Field	Description
Trunk	
Encapsulation	Field not available. IEEE 802.1Q is the only supported encapsulation method.
Allowed VLANs	VLANs allowed to transmit data on this port. The range is 1 to 4094, and the default is 1. Note VLANs 3968 to 4047 and 4094 are allocated for internal device use and do not carry data traffic.
Native VLAN	Native VLAN for this trunk port. The default Native VLAN is the default VLAN, or VLAN1.
PVLAN Host	
Primary Vlan	<i>Display only.</i> The primary VLAN associated with the secondary VLAN(s) to which this port belongs Note This value displays after you choose the secondary VLAN using the Secondary VLAN field.
Secondary VLAN	Secondary VLAN paired with primary VLAN. The type of secondary VLANs is either community or isolated.
PVLAN Promiscuous	
Primary Vlan	<i>Display only.</i> The primary VLAN associated with the secondary VLAN(s) to which this port belongs Note This value displays after you choose the secondary VLAN using the Secondary VLAN field.
Secondary VLAN	Secondary VLAN paired with primary VLAN. The type of secondary VLANs is either community or isolated. Note You can select multiple secondary VLANs, all that have the same primary VLAN, for each private VLAN promiscuous port.
Routed	
IPv4 Address Settings	
Primary	IPv4 address, in dotted decimal notation.
Net mask	Network mask for the IPv4 address in dotted decimal notation.
Secondary: IP Address	Secondary IPv4 address, in dotted decimal notation. You can configure multiple secondary addresses for an interface.
Secondary: Net mask	Network mask for the secondary IPv4 address in dotted decimal notation.
Helper: IP Address	Helper address used to enable the forwarding of User Datagram Protocol (UDP) broadcasts.
IPv6 Address Settings	
Primary/Prefix-length	IPv6 prefix in x:x:x::x/length format.
EUI64	IPv6 address that is in the extended universal identifier (EUI)-64 format.
Link Local	IPv6 link local address in an x:x:x::x format.
Use local only	Link local address that overrides automatically generated IPv6 address.

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

Table 2-11 Port: Port Details: Port Mode Settings: Section (continued)

Field	Description
Secondary: IP Address	Secondary IPv6 prefix in an x:x:x::x/length format. You can configure multiple secondary addresses for an interface.
Secondary: EUI64	Secondary IPv6 address that is in the extended universal identifier (EUI)-64 format.

Port: Port Details: Advanced Settings Section

Table 2-12 Port: Port Details: Advance Settings Section

Field	Description
IPv4 ACL	
Incoming Ipv4 Traffic	IPv4 ACL that filters ingress traffic on the interface. By default, this list is blank.
Outgoing Ipv4 Traffic	IPv4 ACL that filters egress traffic on the interface. By default, this list is blank.
IPv6 ACL	
Incoming Ipv6 Traffic	IPv6 ACL that filters ingress traffic on the interface. By default, this list is blank.
Outgoing Ipv6 Traffic	IPv6 ACL that filters egress traffic on the interface. By default, this list is blank.
MAC ACL	
Incoming Traffic	MAC ACL that filters ingress traffic on the interface. By default, this list is blank.
Security	
Dot1x	<i>Display only.</i> Whether dot1x is enabled or disabled.
Traffic Storm Control	<i>Display only.</i> Whether traffic storm control is enabled or disabled.
IP Source Guard	<i>Display only.</i> Whether IP Source Guard is enabled or disabled.
Port Security	<i>Display only.</i> Whether port security is enabled or disabled.
SPAN	
Use Interface as SPAN	Source or destination for this interface.
Session ID	SPAN session ID where interface is applied.
Type	<i>Display only.</i> Session type.
Direction: Ingress	Monitor ingress packets.
Direction: Egress	Monitor egress packets.

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

Port: Port Status: Port Status Section

Table 2-13 Port: Port Status: Port Status Section

Field	Description
Operational Status	<p><i>Display only.</i> Operational status of the interface. The default is down. Valid values are as follows:</p> <ul style="list-style-type: none"> • Up • Down
Status Description	<p><i>Display only.</i> Description of operational status, as follows:</p> <ul style="list-style-type: none"> • Connected—Cable is connected to the interface and is operationally up. • Admin down—Interface is configured as administratively down. • Channel down—Interface is a member of a port channel that is operationally down. • Disabled—Interface is configured as administratively down. • Error disabled—Interface is in the error disabled state. • Hardware failure—There is a hardware failure at the interface. • Inactive—Interface is inactive. • Initializing—Interface is initializing during the bootup process. • Not connected—Cable has not been connected to the interface. • SFP not inserted—SFP connector has not been connected to the interface. • Link failure—Cable connecting interface to another interface failed. • Interface removed—Physical port is broken or physically disconnected from the interface. • Incompatible admin mode—Admin mode on this interface is incompatible with admin mode configured on connected interface. • Incompatible admin speed—Speed configured on this interface is incompatible with speed configured on connected interface. • Suspended by mode—Problems in mode configuration cause physical to be suspended. • Suspended by speed—Problems in speed configuration cause physical to be suspended. • Upgrade in progress—Software upgrade is in progress on physical port. • Port channel member down—Port is down and is a member of a port channel. • Module removed—Module with the port is not in chassis. • Unsupported transceiver—A transceiver that is not Cisco approved is inserted into the port. • Unknown—Port is operationally down for unknown reasons.
Speed	<p><i>Display only.</i> Transmission speed of the interface. The default is auto.</p>

Send document comments to nexus7k-docfeedback@cisco.com

Table 2-13 Port: Port Status: Port Status Section (continued)

Field	Description
Duplex	<i>Display only.</i> Duplex operation on the interface. The default is auto.
UDLD	<i>Display only.</i> Status of UDLD. The default is disabled. Valid values are as follows: <ul style="list-style-type: none"> • Enabled • Disabled
Flow Control Send	<i>Display only.</i> Status of sending pause frames. The default is off. Valid values are as follows: <ul style="list-style-type: none"> • off • desired • on
Flow Control Receive	<i>Display only.</i> Status of receiving pause frames. The default is off. Valid values are as follows: <ul style="list-style-type: none"> • off • desired • on
Hardware Type	<i>Display only.</i> Hardware type of the port.

Port: Port Status: Port Status SFP Section

Table 2-14 Port: Port Status: Port Status SFP Section

Field	Description
Name	<i>Display only.</i> Name of SFP device.
Part Number	<i>Display only.</i> Part number of SFP device.
Revision	<i>Display only.</i> Revision number of SFP device.
Serial Number	<i>Display only.</i> Serial number of SFP device.
Nominal Bitrate	<i>Display only.</i> Bitrate for SFP device.
Link Length for 9/125um	<i>Display only.</i> Length for 9/125um for SFP device.
Link Length for 50/125um	<i>Display only.</i> Length for 50/125um for SFP device.
Link Length for 62.5/125um	<i>Display only.</i> Length for 62.5/125um for SFP device.
Cisco Id	<i>Display only.</i> Cisco ID for SFP device.
Extended Cisco Id	<i>Display only.</i> Extended Cisco ID for SFP device.

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

Port: Port Status: Port SFP Diagnostics Section

Table 2-15 Port: Port Status: Port SFP Diagnostics Section

Field	Description
Refresh Frequency	Frequency at which information refreshes. The range is from 30 seconds to 5 minutes, in 30-second intervals.
Temperature (celsius)	<p><i>Display only.</i> Temperature of the SFP device for the following values:</p> <ul style="list-style-type: none"> • Current Diagnostic Value • High Alarm • Low Alarm • High Warning • Low Warning • Status
Voltage (volts)	<p><i>Display only.</i> Voltage of the SFP device for the following values:</p> <ul style="list-style-type: none"> • Current Diagnostic Value • High Alarm • Low Alarm • High Warning • Low Warning • Status
Current (milli amps)	<p><i>Display only. Display only.</i> Current of the SFP device for the following values:</p> <ul style="list-style-type: none"> • Current Diagnostic Value • High Alarm • Low Alarm • High Warning • Low Warning • Status

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

Table 2-15 Port: Port Status: Port SFP Diagnostics Section (continued)

Field	Description
Tx Power (decibels)	<p><i>Display only. Display only.</i> Transmitted power of the SFP device for the following values:</p> <ul style="list-style-type: none"> • Current Diagnostic Value • High Alarm • Low Alarm • High Warning • Low Warning • Status
Rx Power (decibels)	<p><i>Display only.</i> Received power of the SFP device for the following values:</p> <ul style="list-style-type: none"> • Current Diagnostic Value • High Alarm • Low Alarm • High Warning • Low Warning • Status

Additional References

For additional information related to implementing Feature-1, see the following sections:

- [Related Documents, page 2-35](#)
- [Standards, page 2-35](#)
- [Feature History for Configuring Basic Interface Parameters, page 2-35](#)

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

Related Documents

Related Topic	Document Title
Command reference	<i>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference</i>
Layer 2 switching	<i>Cisco DCNM Layer 2 Switching Configuration Guide, Release 4.x</i>
CDP	<i>Cisco Nexus 7000 Series NX-OS System Management Command Reference</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Configuring Basic Interface Parameters

Table 2-16 lists the release history for this feature.

Table 2-16 Feature History for Configuring Basic Interface Parameters

Feature Name	Releases	Feature Information
Basic interface settings	4.0(1)	These features were introduced.
SFP information	4.1(2)	Added display information on SFP interfaces.
Carrier delay	4.1(2)	Configures a timer that allows you to not see some quick interface up/down changes.

Send document comments to nexus7k-docfeedback@cisco.com