Configuring Port Channels

This chapter describes how to configure port channels.

- Finding Feature Information, on page 1
- Feature History for Configuring Port Channels, on page 1
- Information About Port Channels, on page 2
- Prerequisites for Port Channeling, on page 16
- Guidelines and Limitations for Port Channels, on page 16
- Default Settings, on page 17
- Configuring Port Channels, on page 18
- Configuring Random Load Balance , on page 45
- Verifying Port-Channel Configurations, on page 47
- Monitoring the Port-Channel Interface Configuration, on page 48
- Configuration Examples for Port Channels, on page 49
- Related Documents, on page 50

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://bst.cloudapps.cisco.com/bugsearch and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

Feature History for Configuring Port Channels

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Release	Feature Information
LACP Fast Timers	8.2(4)	Improved the validation for the number of interfaces with LACP Fast Timers.

Feature Name	Release	Feature Information
GPRS Tunneling Protocol (GTP) Load Balance Support on M3-Series Modules	7.3(0)DX(1)	Improved port-channel and ECMP load balancing for GTP traffic with M3 modules.
Random Load Balance (Port Channel)	7.3(0)D1(1)	Added support for Random Load Balancing on port channels. Added the **random** keyword to **port-channel load-balance** command to improve load balancing across port channels.
DisplayPpolicy Errors on Interfaces and VLANs	6.2(2)	Added the **show interface status error policy** command.
Prevent Traffic-Drop During Bi-Directional Flow on F2 or F2e Modules	6.2(2)	Added the **asymmetric** keyword to **port-channel load-balance** command to improve load balancing across port channels.
Result Bundle Hash Load Balancing	6.1(3)	Support for the RBH modulo mode to improve load balancing across port channels.
Minimum Links for FEX Fabric Port Channel	6.1(3)	This feature was introduced.
Port Channels Hash Distribution	6.1(1)	Support for port channel hash distribution fixed and adaptive mode.
Load-Balancing Supports F2 Modules	6.0(1)	Added support for F2 modules on load-balancing across port channels.
Port Channels	5.2(1)	Support increased to 528 port channels.
Minimum Links and Maxbundle for LACP	5.1(1)	This feature was introduced.
Port Channels	4.2(1)	Support increased to 256 port channels.
Port Channels	4.0(1)	This feature was introduced.

Information About Port Channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to 8 individual active links into a port channel to provide increased bandwidth and redundancy. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel. Port channeling also load balances traffic on the M series module and across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

Note

- From Cisco NX-OS Release 5.1, you can bundle up to 16 active links into a port channel on the F-series module.

You cannot configure a shared interface to be part of a port channel. See the for more information about shared interfaces.

You can bundle up to 8 ports into a static port channel without using any aggregation protocol. On the M-series module, you can bundle up to 8 active and 8 standby on the M-series module and up to 16 ports on the F Series module. Starting from Cisco NX-OS Release 8.3(1), you can bundle up to 16 active links on M3 modules.

However, you can enable the LACP to use port channels more flexibly. Configuring port channels with LACP and static port channels require a slightly different procedure.

Note This device does not support Port Aggregation Protocol (PAgP) for port channels.

Each port can be in only one port channel. All the ports in a port channel must be compatible; they must use the same speed and duplex mode (see the "Compatibility Requirements" section). When you run static port channels with no aggregation protocol, the physical links are all in the on channel mode; you cannot change this mode without enabling LACP (see the "Port-Channel Modes" section).

You can create port channels directly by creating the port-channel interface, or you can create a channel group that acts to aggregate individual ports into a bundle. When you associate an interface with a channel group, the software creates a matching port channel automatically if the port channel does not already exist. In this instance, the port channel assumes the Layer 2 or Layer 3 configuration of the first interface. You can also create the port channel first. In this instance, the Cisco NX-OS software creates an empty channel group with the same channel number as the port channel and takes the default Layer 2 or Layer 3 configuration, as well as the compatibility configuration (see the "Compatibility Requirements" section).

Note The port channel is operationally up when at least one of the member ports is up and that port's status is channeling. The port channel is operationally down when all member ports are operationally down.

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. After you create a Layer 3 port channel, you can add an IP address to the port-channel interface and create subinterfaces on the Layer 3 port channel. You cannot combine Layer 2 and Layer 3 interfaces in the same port channel.

From Cisco NX-OS Release 4.2, you can apply port security to port channels. See the for information about port security. All ports in the port channel must be in the same virtual device context (VDC); you cannot configure port channels across VDCs.

You can also change the port channel from Layer 3 to Layer 2.

Any configuration changes that you apply to the port channel are applied to each member interface of that port channel. For example, if you configure Spanning Tree Protocol (STP) parameters on the port channel, the Cisco NX-OS software applies those parameters to each interface in the port channel.

Note After a Layer 2 port becomes part of a port channel, all switchport configurations must be done on the port channel; you can no longer apply switchport configurations to individual port-channel members. You cannot apply Layer 3 configurations to an individual port-channel member either; you must apply the configuration to the entire port channel.

You can create subinterfaces on a Layer 3 port channel, even though a subinterface is part of the logical port-channel interface. See the "Subinterfaces" section for more information about port-channel subinterfaces.

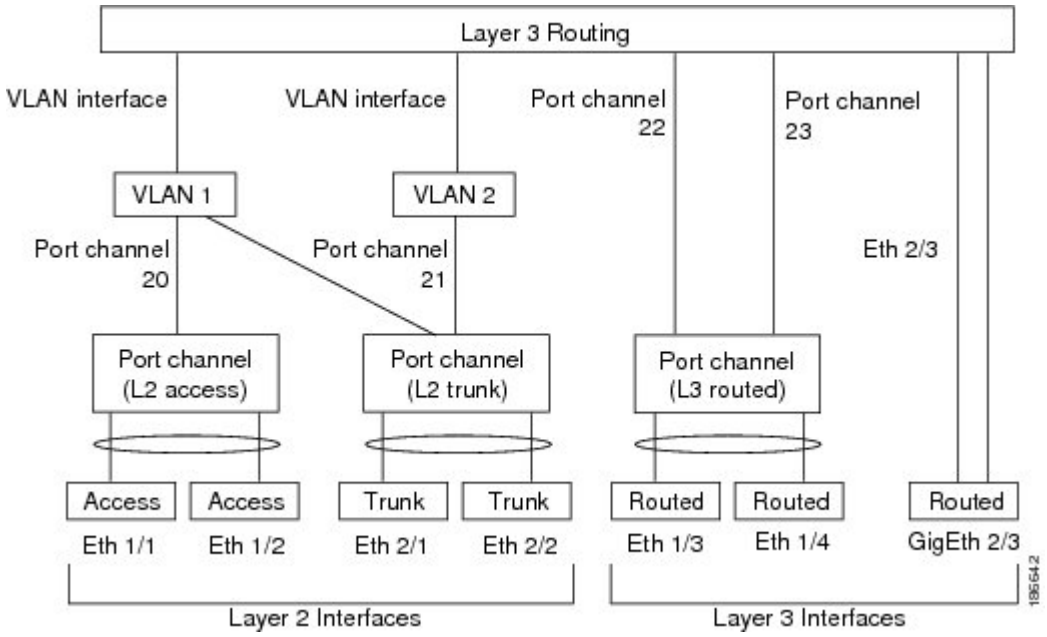
You can use static port channels, with no associated aggregation protocol, for a simplified configuration. For more flexibility, you can use the Link Aggregation Control Protocol (LACP), which is defined in IEEE 802.3ad. When you use LACP, the link passes protocol packets. You cannot configure LACP on shared interfaces.

See the "LACP" section for information about LACP.

Port-Channel Interfaces

The figure below shows port-channel interfaces.

Figure 1: Port-Channel Interfaces



You can classify port-channel interfaces as Layer 2 or Layer 3 interfaces. In addition, you can configure Layer 2 port channels in either access or trunk mode. Layer 3 port-channel interfaces have routed ports as channel members and might have subinterfaces.

From Cisco NX-OS Release 4.2(1), you can configure a Layer 3 port channel with a static MAC address. If you do not configure this value, the Layer 3 port channel uses the router MAC of the first channel member to come up. See the for information about configuring static MAC addresses on Layer 3 port channels.

Basic Settings

You can configure the following basic settings for a port-channel interface:

- Bandwidth—Use this setting for informational purposes only; this setting is to be used by higher-level protocols.
- Delay—Use this setting for informational purposes only; this setting is to be used by higher-level protocols.
- Interface Description—Use this setting to provide a unique name for each interface so that you can quickly identify the interface when you are looking at a listing of multiple interfaces.
- Duplex—By default, each interface autonegotiates its duplex mode with the other interface, but you can change these settings. If you change the settings, be sure to use the same duplex mode setting on both interfaces, or use autonegotiation for at least one of the interfaces.
- Flow control—Use this setting 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.
- IP addresses—Both IPv4 and IPv6
- Maximum Transmission Unit (MTU)—Use this setting to specify the maximum frame size that an Ethernet port can process.
- Shutdown—Use this setting to bring down or up an interface.
- Speed—By default, each interface autonegotiates its speed mode with the other interface, but you can change these settings. If you change the settings, be sure to use the same speed mode setting on both interfaces, or use autonegotiation for at least one of the interfaces.

Compatibility Requirements

When you add an interface to a channel group, the software checks certain interface attributes to ensure that the interface is compatible with the channel group. For example, you cannot add a Layer 3 interface to a Layer 2 channel group. The Cisco NX-OS software also checks a number of operational attributes for an interface before allowing that interface to participate in the port-channel aggregation.

The compatibility check includes the following operational attributes:

- (Link) speed capability
- Access VLAN
- Allowed VLAN list
- Check rate mode
- Duplex capability
- Duplex configuration
- Flow-control capability
- Flow-control configuration
- Layer 3 ports—(Cannot have subinterfaces)
- MTU size

- Media type, either copper or fiber
- Module Type
- Network layer
- Port mode
- SPAN—(Cannot be a SPAN source or a destination port)
- Speed configuration
- Storm control
- Tagged or untagged
- Trunk native VLAN

Use the **show port-channel compatibility-parameters** command to see the full list of compatibility checks that the Cisco NX-OS uses.

You can only add interfaces configured with the channel mode set to **on** to static port channels, and you can only add interfaces configured with the channel mode as **active** or **passive** to port channels that are running LACP. You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, the software suspends that port in the port channel.

Alternatively, you can force ports with incompatible parameters to join the port channel if the following parameters are the same:

- (Link) Speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Flow-control capability
- Flow-control configuration

When the interface joins a port channel, some of its individual parameters are removed and replaced with the values on the port channel as follows:

- Bandwidth
- Delay
- Extended Authentication Protocol over UDP
- VRF
- IP address (v4 and v6)
- MAC address
- Spanning Tree Protocol
- NAC
- Service policy

- Access control lists (ACLs)

Many interface parameters remain unaffected when the interface joins or leaves a port channel as follows:

- Beacon
- Description
- CDP
- LACP port priority
- Debounce
- UDLD
- MDIX
- Rate mode
- Shutdown
- SNMP trap

If you configure subinterfaces for the port-channel interface and remove a member port from the port channel, the configuration of the port-channel subinterface does not propagate to the member ports.

Note When you delete the port channel, the software sets all member interfaces as if they were removed from the port channel.

See the "LACP Marker Responders" section for information about port-channel modes.

Load Balancing Using Port Channels

The Cisco NX-OS software load balances traffic across all operational interfaces in a port channel by hashing the addresses in the frame to a numerical value that selects one of the links in the channel. Port channels provide load balancing by default. Port-channel load balancing uses MAC addresses, IP addresses, or Layer 4 port numbers to select the link. Port-channel load balancing uses either source or destination addresses or ports, or both source and destination addresses or ports.

You can configure the load-balancing mode to apply to all port channels that are configured on the entire device or on specified modules. The per-module configuration takes precedence over the load-balancing configuration for the entire device. You can configure one load-balancing mode for the entire device, a different mode for specified modules, and another mode for the other specified modules. You cannot configure the load-balancing method per port channel.

You can configure the type of load-balancing algorithm used. You can choose the load-balancing algorithm that determines which member port to select for egress traffic by looking at the fields in the frame.

Note The default load-balancing mode for Layer 3 interfaces is the source and destination IP address, and the default load-balancing mode for non-IP traffic is the source and destination MAC address. Use the **port-channel load-balance** command to set the load-balancing method among the interfaces in the channel-group bundle. The default method for Layer 2 packets is src-dst-mac. The default method for Layer 3 packets is src-dst-ip. For additional information about this command, see the Cisco Nexus 7000 Series NX-OS Interfaces Command Reference.

F1-series modules do not support load balancing of non-IP traffic based on a MAC address. If ports on an F1-series module are used in a port channel and non-IP traffic is sent over the port channel, Layer 2 traffic might get out of order. From Cisco NX-OS Release 6.0(1), load balancing supports F2 modules.

You can configure the device to use one of the following methods to load balance across the port channel:

- Destination MAC address
- Source MAC address
- Source and destination MAC address
- Destination IP address
- Source IP address
- Source and destination IP address
- Source TCP/UDP port number
- Destination TCP/UDP port number
- Source and destination TCP/UDP port number

Non-IP and Layer 3 port channels both follow the configured load-balancing method, using the source, destination, or source and destination parameters. For example, when you configure load balancing to use the source IP address, all non-IP traffic uses the source MAC address to load balance the traffic while the Layer 3 traffic load balances the traffic using the source IP address. Similarly, when you configure the destination MAC address as the load-balancing method, all Layer 3 traffic uses the destination IP address while the non-IP traffic load balances using the destination MAC address.

Note You cannot configure load balancing using port channels per virtual device context (VDC). You must be in the default VDC to configure this feature; if you attempt to configure this feature from another VDC, the system displays an error.

You can configure load balancing either by the entire system or by specific modules, regardless of the VDC. The port-channel load balancing is a global setting across all VDCs.

If the ingress traffic is Multiprotocol Label Switching (MPLS) traffic, the software looks under the labels for the IP address on the packet.

Multicast traffic inherits the same port-channel load balancing configuration as unicast traffic. This is applicable for both system-wide and module-specific load balancing configurations.

Note Devices that run Cisco IOS can optimize the behavior of the member ports of ASICs if a failure of a single member occurred if you enter the **port-channel hash-distribution** command. The Cisco Nexus 7000 Series device performs this optimization by default and does not require or support this command. Cisco NX-OS does support the customization of the load-balancing criteria on port channels through the **port-channel load-balance** command either for the entire device or on a per-module basis. See the *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference* for information about this command.

Cisco NX-OS Release 6.1(3) supports a new Result Bundle Hash (RBH) mode to improve load balancing on port-channel members on Cisco Nexus 7000 M Series I/O XL modules and on F Series modules. With the new RBH modulo mode, the RBH result is based on the actual count of port-channel members.

Symmetric Hashing

To effectively monitor traffic on a port channel, it is essential that each interface connected to a port channel receives both forward and reverse traffic flows. Normally, there is no guarantee that the forward and reverse traffic flows will use the same physical interface. However, when you enable symmetric hashing on the port channel, bidirectional traffic is forced to use the same physical interface and each physical interface in the port channel is effectively mapped to a set of flows.

When symmetric hashing is enabled, the parameters used for hashing, such as the source and destination IP address, are normalized before they are entered into the hashing algorithm. This process ensures that when the parameters are reversed (the source on the forward traffic becomes the destination on the reverse traffic), the hash output is the same. Therefore, the same interface is chosen.

Only the following load-balancing algorithms support symmetric hashing:

- src ip
- dst ip rotate
- dst ip
- src ip rotate
- src-dst ip
- src ip-l4port
- dst ip-l4port rotate
- dst ip-l4port
- src ip-l4port rotate
- src-dst ip-l4port-vlan
- dst ip-vlan
- src ip-vlan rotate
- src-dst ip-vlan
- src l4port
- dst l4port rotate

- dst l4port
- src l4port rotate
- src-dst l4port
- src mac
- dst mac rotate
- dst mac
- src mac rotate
- src-dst mac

Random Load Balancing (Port Channel)

Random load balancing on port channels is a software solution that enables better port-link bandwidth utilization for GPRS Tunneling Protocol (GTP) over IP-UDP packets. The existing M1, M2, F1, F2 and F2e line card hardware does not have the capability to perform random load balancing and hence, this software solution helps in load balancing and optimizing the port channels bandwidth. Random load balancing is supported only on F3 series line cards. Random load balancing is applicable on all types of traffic and is effective on egress ports of Layer 3 traffic. The Cisco NX-OS software does random load balancing of all traffic across all interfaces in a port channel by using polynomial scheme.

LACP

LACP allows you to configure up to 16 interfaces into a port channel. A maximum of 8 interfaces can be active, and a maximum of 8 interfaces can be placed in a standby state on the M-series modules.

From Cisco NX-OS Release 5.1, you can bundle up to 16 active links into a port channel on the F-Series module.

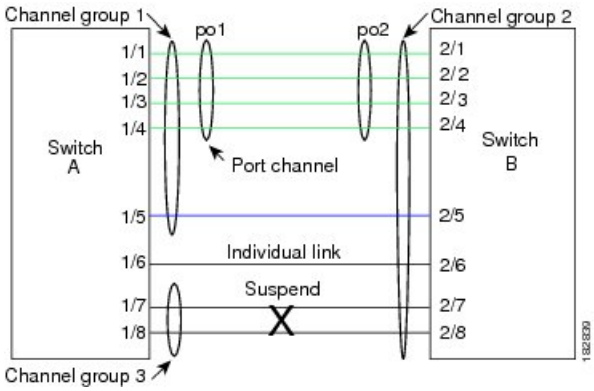
Note You must enable LACP before you can use LACP. By default, LACP is disabled.

See the "Enabling LACP" section for information about enabling LACP.

From Cisco NX-OS Release 4.2, the system automatically takes a checkpoint before disabling the feature, and you can roll back to this checkpoint. See the for information about rollbacks and checkpoints.

The figure below shows how individual links can be combined into LACP port channels and channel groups as well as function as individual links.

Figure 2: Individual Links Combined into a Port Channel



With LACP, you can bundle up to 16 interfaces in a channel group. If the channel group has more than 8 interfaces, the remaining interfaces are in hot standby for the port channel associated with this channel group on the M-series modules.

From Cisco NX-OS Release 5.1, you can bundle up to 16 active links into a port channel on the F-series module.

Note When you delete the port channel, the software automatically deletes the associated channel group. All member interfaces revert to their original configuration.

You cannot disable LACP while any LACP configurations are present.

Port-Channel Modes

Individual interfaces in port channels are configured with channel modes. When you run static port channels with no aggregation protocol, the channel mode is always set to on.

After you enable LACP globally on the device, you enable LACP for each channel by setting the channel mode for each interface to active or passive. You can configure either channel mode for individual links in the LACP channel group when you are adding the links to the channel group.

Note You must enable LACP globally before you can configure an interface in either the active or passive channel mode.

Table 1: Port-Channel Modes

Channel Mode	Description
passive	LACP mode that places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.
active	LACP mode that places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.

Channel Mode	Description
on	All static port channels (that are not running LACP) remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. You enable LACP on each channel by configuring the interface in that channel for the channel mode as either active or passive. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the LACP channel group. The default port-channel mode is on.

Both the passive and active modes allow LACP to negotiate between ports to determine if they can form a port channel based on criteria such as the port speed and the trunking state. The passive mode is useful when you do not know whether the remote system, or partner, supports LACP.

Ports can form an LACP port channel when they are in different LACP modes if the modes are compatible as seen in these examples:

- A port in active mode can form a port channel successfully with another port that is in active mode.
- A port in active mode can form a port channel with another port in passive mode.
- A port in passive mode cannot form a port channel with another port that is also in passive mode, because neither port will initiate negotiation.
- A port in on mode is not running LACP and cannot form a port channel with another port that is in active or passive mode.

LACP ID Parameters

LACP System Priority

Each system that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or you can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also uses the system priority during negotiation with other devices. A higher system priority value means a lower priority.

The system ID is different for each VDC.

Note The LACP system ID is the combination of the LACP system priority value and the MAC address.

LACP Port Priority

Each port that is configured to use LACP has an LACP port priority. You can accept the default value of 32768 for the LACP port priority, or you can configure a value between 1 and 65535. LACP uses the port priority with the port number to form the port identifier.

LACP uses the port priority to decide which ports should be put in standby mode when there is a limitation that prevents all compatible ports from aggregating and which ports should be put into active mode. A higher port priority value means a lower priority for LACP. You can configure the port priority so that specified

ports have a lower priority for LACP and are most likely to be chosen as active links, rather than hot-standby links.

LACP Administrative Key

LACP automatically configures an administrative key value equal to the channel-group number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:

- Port physical characteristics, such as the data rate and the duplex capability
- Configuration restrictions that you establish

LACP Marker Responders

You can dynamically redistribute the data traffic by using port channels. This redistribution might result from a removed or added link or a change in the load-balancing scheme. Traffic redistribution that occurs in the middle of a traffic flow can cause misordered frames.

LACP uses the Marker Protocol to ensure that frames are not duplicated or reordered due to this redistribution. The Marker Protocol detects when all the frames of a given traffic flow are successfully received at the remote end. LACP sends Marker PDUs on each of the port-channel links. The remote system responds to the Marker PDU once it receives all the frames received on this link prior to the Marker PDU. The remote system then sends a Marker Responder. Once the Marker Responders are received by the local system on all member links of the port channel, the local system can redistribute the frames in the traffic flow with no chance of misordering. The software supports only Marker Responders.

Differences Between LACP-Enabled Port Channels and Static Port Channels

The table below summarizes the major differences between port channels with LACP enabled and static port channels.

Table 2: Differences Between LACP-Enabled Port Channels and Static Port Channels

Configuration	Port Channels with LACP Enabled	Static Port Channels
Protocol applied	Enable globally	Not applicable
Channel mode of links	Can be either: • Active • Passive	Can only be On
Maximum number of links in channel	16	8 Starting from Cisco NX-OS Release 5.1, the maximum number of links supported in a channel is 16 on the Fseries modules.

LACP Compatibility Enhancements

Several new commands have been added in Release 4.2(3) to address interoperability issues and to assist with faster LACP protocol convergence.

When a Cisco Nexus 7000 Series device is connected to a non-Nexus peer, its graceful failover defaults may delay the time taken for a disabled port to be brought down or cause traffic from the peer to be lost. To address these conditions, the **lacp graceful-convergence** command was added.

By default, LACP sets a port to the suspended state if it does not receive an LACP PDU from the peer. In some cases, although this feature helps in preventing loops created due to misconfigurations, it can cause servers to fail to boot up because they require LACP to logically bring up the port. You can place a port in an individual state by using the **no lacp suspend-individual** command.

LACP Port-Channel Minimum Links and MaxBundle

A port channel aggregates similar ports to provide increased bandwidth in a single manageable interface.

With the Cisco NX-OS Release 5.1, the introduction of the minimum links and maxbundle feature further refines LACP port-channel operation and provides increased bandwidth in one manageable interface.

The LACP port-channel minimum links feature does the following:

- Configures the minimum number of ports that must be linked up and bundled in the LACP port channel.
- Prevents the low-bandwidth LACP port channel from becoming active.
- Causes the LACP port channel to become inactive if there are few active members ports to supply the required minimum bandwidth.

The LACP MaxBundle defines the maximum number of bundled ports allowed in a LACP port channel.

The LACP MaxBundle feature does the following:

- Defines an upper limit on the number of bundled ports in an LACP port channel.
- Allows hot-standby ports with fewer bundled ports. (For example, in an LACP port channel with five ports, you can designate two of those ports as hot-standby ports.)

Note The minimum links and maxbundle feature works only with LACP port channels. However, the device allows you to configure this feature in non-LACP port channels, but the feature is not operational.

LACP Offload to Fabric Extenders

To reduce the load on the control plane of the Cisco Nexus 7000 Series device, Cisco NX-OS provides the ability to offload link-level protocol processing to the Fabric Extender CPU. This feature is supported by LACP by default as soon as there is at least one LACP port channel configured on a Fabric Extender.

LACP Fast Timers

You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lacp rate** command to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only

on LACP-enabled interfaces. To configure the LACP fast time rate, see the "Configuring the LACP Fast Timer Rate" section.

ISSU and stateful switchover cannot be guaranteed with LACP fast timers.

Minimum Number of Links on the FEX Fabric Port Channel

In a network configuration of dual-homed hosts (active/standby), you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) to support a minimum number of links for fabric port channels.

When the number of fabric port-channel links falls below the specified threshold, the host-facing FEX interfaces are brought down, which allows for a NIC switchover on the connection between the host and the FEX. The automatic recovery of the FEX interfaces to the standby FEX is triggered when the number of fabric port-channel links reaches the specified threshold.

Virtualization Support

You must configure the member ports and other port-channel related configuration from the virtual device context (VDC) that contains the port channel and member ports. You can use the numbers from 1 to 4096 in each VDC to number the port channels and you can reuse these port-channel numbers in different VDCs. For example, you can configure port channel 100 in VDC1 and also configure a different port channel 100 in VDC2.

However, the LACP system ID is different for each VDC. For more information about LACP, see the "LACP" section.

Note See the for complete information about VDCs and assigning resources.

All ports in one port channel must be in the same VDC. When you are using LACP, all possible 8 active ports and all possible 8 standby ports must be in the same VDC. The port channels can originate in one VDC (with all ports in that channel in the same VDC) and partner with a port channel in another VDC (again, all ports in that channel must be in that VDC).

Note The port-channeling load-balancing mode works either for a single module or across the entire device. You must configure load balancing using port channels in the default VDC. You cannot configure load balancing using port channels within specified VDCs. See the "Load Balancing Using Port Channels" section for more information about load balancing.

High Availability

Port channels provide high availability by load balancing traffic across multiple ports. If a physical port fails, the port channel is still operational if there is an active member in the port channel. You can bundle ports from different modules and create a port channel that remains operational even if a module fails because the settings are common across the module.

Port channels support stateful and stateless restarts. A stateful restart occurs on a supervisor switchover. After the switchover, the Cisco NX-OS software applies the runtime configuration after the switchover.

The port channel goes down if the operational ports fall below the configured minimum links number.

Note See the Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide for complete information about high-availability features.

Prerequisites for Port Channeling

Port channeling has the following prerequisites:

- You must be logged onto the device.
- All ports in the channel group must be in the same VDC.
- All ports for a single port channel must be either Layer 2 or Layer 3 ports.
- All ports for a single port channel must meet the compatibility requirements. See the "Compatibility Requirements" section for more information about the compatibility requirements.
- You must configure load balancing from the default VDC.

Guidelines and Limitations for Port Channels

Port channeling has the following configuration guidelines and limitations:

- The LACP port-channel minimum links and maxbundle feature is not supported for host interface port channels.
- You must enable LACP before you can use that feature.
- You can configure multiple port channels on a device.
- Do not put shared and dedicated ports into the same port channel. (See "Configuring Basic Interface Parameters," for information about shared and dedicated ports.)
- For Layer 2 port channels, ports with different STP port path costs can form a port channel if they are compatibly configured with each other. See the "Compatibility Requirements" section for more information about the compatibility requirements.
- In STP, the port-channel cost is based on the aggregated bandwidth of the port members.
- After you configure a port channel, the configuration that you apply to the port-channel interface affects the port-channel member ports. The configuration that you apply to the member ports affects only the member port where you apply the configuration.
- LACP does not support half-duplex mode. Half-duplex ports in LACP port channels are put in the suspended state.
- You must remove the port-security information from a port before you can add that port to a port channel. Similarly, you cannot apply the port-security configuration to a port that is a member of a channel group.

- Do not configure ports that belong to a port-channel group as private VLAN ports. While a port is part of the private VLAN configuration, the port-channel configuration becomes inactive.
- Channel member ports cannot be a source or destination SPAN port.
- You cannot configure the ports from an F1- and an M1-series module in the same port channel because the ports will fail to meet the compatibility requirements.
- You cannot configure the ports from an M1- and an M2-series module in the same port channel.
- You cannot configure the ports from an F2e- and an F3-series module in the same port channel because the ports will fail to meet the compatibility requirements.
- You cannot configure the ports from an F3- and M3-series module in the same port channel because the ports will fail to meet the compatibility requirements.
- You cannot configure the ports from an F4- and M3-series module in the same port channel because the ports will fail to meet the compatibility requirements.
- You cannot configure the ports from an F3- and F4-series module in the same port channel because the ports will fail to meet the compatibility requirements.
- You cannot configure the ports from an M2- and F3/M3/F4-Series Module in the same port channel because the ports will fail to meet the compatibility requirements.
- From Cisco NX-OS Release 5.1, you can bundle up to 16 active links into a port channel on the F1-series module.
- F1-series modules do not support load balancing of non-IP traffic based on a MAC address. If ports on an F1-series module are used in a port channel and non-IP traffic is sent over the port channel, Layer 2 traffic might get out of order.
- Only F series and the XL type of M-series modules support the RBH modulo mode.
- Random load balance on port channel is supported only on F3-series modules. Ensure both sides of the port channel are F3 modules only.

Default Settings

Table 3: Default Port-Channel Parameters

Parameter	Default
Port channel	Admin up
Load-balancing method for Layer 3 interfaces	Source and destination IP address
Load-balancing method for Layer 2 interfaces	Source and destination MAC address
Load balancing per module	Disabled
RBH modulo mode	Disabled
LACP	Disabled

Parameter	Default
Channel mode	on
LACP system priority	32768
LACP port priority	32768
Minimum links for LACP	1
Maxbundle	16
Minimum links for FEX fabric port channel	1
Random load balancing (port channels)	Disabled

Configuring Port Channels

Creating a Port Channel

You can create a port channel before you create a channel group. The software automatically creates the associated channel group.

Before you begin

- Enable LACP if you want LACP-based port channels.
- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode. The range is from 1 to 4096. The Cisco NX-OS software automatically creates the channel group if it does not already exist.
Step 3	switch(config-if)# **show port-channel summary**	Displays information about the port channel.
Step 4	(Optional) switch(config-if)# **show interface status error policy** [**detail**]	Displays the interfaces and VLANs that produce an error during policy programming to ensure that policies are consistent with hardware policies.

	Command or Action	Purpose
		Use the **detail** command to display the details of the interfaces that produce an error.
Step 5	(Optional) switch(config-if)# **no shutdown**	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up. If policies do not correspond, the errors are placed in an error-disabled policy state.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Use the **no interface port-channel** command to remove the port channel and delete the associated channel group.

Command	Purpose
no interface port-channel *channel-number*	Removes the port channel and deletes the associated channel group.

Example

This example shows how to create a port channel:

```
switch# configure terminal
switch (config)# interface port-channel 1
```

See the "Compatibility Requirements" section for details on how the interface configuration changes when you delete the port channel.

Adding a Layer 2 Port to a Port Channel

You can add a Layer 2 port to a new channel group or to a channel group that already contains Layer 2 ports. The software creates the port channel associated with this channel group if the port channel does not already exist.

Before you begin

- Enable LACP if you want LACP-based port channels.
- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.
- All Layer 2 member ports must run in full-duplex mode and at the same speed.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode. The range is from 1 to 4096. The Cisco NX-OS software automatically creates the channel group if it does not already exist.
Step 3	switch(config-if)# **switchport**	Configures the interface as a Layer 2 access port.
Step 4	(Optional) switch(config-if)# **switchport mode trunk**	Configures the interface as a Layer 2 trunk port.
Step 5	(Optional) switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}	Configures necessary parameters for a Layer 2 trunk port.
Step 6	switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	Configures the port in a channel group and sets the mode. The channel-number range is from 1 to 4096. This command creates the port channel associated with this channel group if the port channel does not already exist. All static port-channel interfaces are set to mode on. You must set all LACP-enabled port-channel interfaces to active or passive. The default mode is on. Forces an interface with some incompatible configurations to join the channel. The forced interface must have the same speed, duplex, and flow control settings as the channel group. **Note** The force option fails if the port has a QoS policy mismatch with the other members of the port channel.
Step 7	(Optional) switch(config-if)# **show interface** *type slot/port*	Displays interface information.
Step 8	(Optional) switch(config-if)# **show interface status error policy** [**detail**]	Displays the interfaces and VLANs that produce an error during policy programming to ensure that policies are consistent with hardware policies. Use the **detail** command to display the details of the interfaces that produce an error.

	Command or Action	Purpose
Step 9	(Optional) switch(config-if)# **no shutdown**	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up. If policies do not correspond, the errors are placed in an error-disabled policy state.
Step 10	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Use the **no channel-group** command to remove the port from the channel group.

Table 4: Removing a Port From the Channel Group

Command	Purpose
no channel-group	Removes the port from the channel group.

Example

This example shows how to add a Layer 2 Ethernet interface 1/4 to channel group 5:

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5
```

Adding a Layer 3 Port to a Port Channel

You can add a Layer 3 port to a new channel group or to a channel group that is already configured with Layer 3 ports. The software creates the port channel associated with this channel group if the port channel does not already exist.

If the Layer 3 port that you are adding has a configured IP address, the system removes that IP address before adding the port to the port channel. After you create a Layer 3 port channel, you can assign an IP address to the port-channel interface. You can also add subinterfaces to an existing Layer 3 port channel.

Before you begin

- Enable LACP if you want LACP-based port channels.
- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.
- Remove any IP addresses configured on the Layer 3 interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode. The range is from 1 to 4096. The Cisco NX-OS software automatically creates the channel group if it does not already exist.
Step 3	switch(config-if)# **no switchport**	Configures the interface as a Layer 2 access port.
Step 4	switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	Configures the port in a channel group and sets the mode. The channel-number range is from 1 to 4096. This command creates the port channel associated with this channel group if the port channel does not already exist. All static port-channel interfaces are set to mode on. You must set all LACP-enabled port-channel interfaces to active or passive. The default mode is on. Forces an interface with some incompatible configurations to join the channel. The forced interface must have the same speed, duplex, and flow control settings as the channel group.
Step 5	(Optional) switch(config-if)# **show interface** *type slot/port*	Displays interface information.
Step 6	(Optional) switch(config-if) **show interface status error policy** [**detail**]	Displays the interfaces and VLANs that produce an error during policy programming to ensure that policies are consistent with hardware policies. Use the **detail** command to display the details of the interfaces that produce an error.
Step 7	(Optional) switch(config-if) **no shutdown**	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up. If policies do not correspond, the errors are placed in an error-disabled policy state.
Step 8	(Optional) switch(config-if) **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Use the **no channel-group** command to remove the port from the channel group.

Table 5: Removing a Port From the Channel Group

Command	Purpose
no channel-group	Removes the port from the channel group.

Example

This example shows how to add a Layer 3 Ethernet interface 1/5 to channel group 6 in on mode:

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# channel-group 6
```

This example shows how to create a Layer 3 port-channel interface and assign the IP address:

```
switch# configure terminal
switch(config)# interface port-channel 4
switch(config-if)# ip address 192.0.2.1/8
```

Configuring the Bandwidth and Delay for Informational Purposes

The bandwidth of the port channel is determined by the number of total active links in the channel.

You configure the bandwidth and delay on port-channel interfaces for informational purposes.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **bandwidth** *value*	Specifies the bandwidth, which is used for informational purposes. The range is from 1 to 80,000,000 kbs. The default value depends on the total active interfaces in the channel group.
Step 4	switch(config-if)# **delay** *value*	Specifies the throughput delay, which is used for informational purposes. The range is from 1 to 16,777,215 tens of microseconds. The default value is 10 microseconds. **Note** Prior to Cisco Release 4.2(1), the default delay value was 100 microseconds.

	Command or Action	Purpose
Step 5	switch(config-if)# **exit**	Exits the interface mode and returns to the configuration mode.
Step 6	(Optional) switch(config)# **show interface port-channel** *channel-number*	Displays interface information for the specified port channel.
Step 7	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the informational parameters of the bandwidth and delay for port channel 5:

```
switch# configure terminal
switch (config)# interface port-channel 5
switch(config-if)# bandwidth 60000000
switch(config-if)# delay 10000
switch(config-if)#
```

Shutting Down and Restarting the Port-Channel Interface

You can shut down and restart the port-channel interface. When you shut down a port-channel interface, no traffic passes and the interface is administratively down.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **shutdown** | **no shutdown**	Shuts down the interface. No traffic passes and the interface displays as administratively down. The default is no shutdown. The **no shutdown** command opens the interface. The interface displays as administratively up. If there are no operational problems, traffic passes. The default is no shutdown.
Step 4	switch(config-if)# **exit**	Exits the interface mode and returns to the configuration mode.

	Command or Action	Purpose
Step 5	switch# **show interface port-channel** *channel-number*	Displays interface information for the specified port channel.
Step 6	(Optional) switch# **show interface status error policy** [**detail**]	Displays the interfaces and VLANs that produce an error during policy programming to ensure that policies are consistent with hardware policies. Use the **detail** command to display the details of the interfaces that produce an error.
Step 7	(Optional) switch# **no shutdown**	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up. If policies do not correspond, the errors are placed in an error-disabled policy state.
Step 8	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to bring up the interface for port channel 2:

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# no shutdown
```

Configuring a Port-Channel Description

You can configure a description for a port channel.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode. The range is from 1 to 4096. The Cisco NX-OS software automatically creates the channel group if it does not already exist.
Step 3	switch(config-if)# **description**	Allows you to add a description to the port-channel interface. You can use up to 80 characters in the description. By default, the description does not display; you must configure

	Command or Action	Purpose
		this parameter before the description displays in the output.
Step 4	switch(config-if)# **exit**	Exits the interface mode and returns to the configuration mode.
Step 5	(Optional) switch(config-if)# **show interface port-channel** *channel-number*	Displays interface information for the specified port channel.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to add a description to port channel 2:

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# description engineering
```

Configuring the Speed and Duplex Settings for a Port-Channel Interface

You can configure the speed and duplex settings for a port-channel interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **speed** {**10** | **100** | **1000** | **auto**}	Sets the speed for the port-channel interface. The default is auto for autonegotiation.
Step 4	switch(config-if)# **duplex** {**auto** | **full** | **half**}	Sets the duplex for the port-channel interface. The default is auto for autonegotiation.
Step 5	switch(config-if)# **exit**	Exits the interface mode and returns to the configuration mode.
Step 6	(Optional) switch# **show interface port-channel** *channel-number*	Displays interface information for the specified port channel.
Step 7	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to set port channel 2 to 100 Mb/s:

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# speed 100
```

Configuring Flow Control

You can enable or disable the capability of the port-channel interfaces that run at 1 Gb or higher to send or receive flow-control pause packets. For port-channel interfaces that run at lower speeds, you can enable or disable only the capability of the port-channel interfaces to receive pause packets.

Note The settings have to match at both the local and remote ends of the link so that flow control can work properly.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **flowcontrol** {**receive** | **send**} {**desired** | **off** | **on**}	Sets the flow control parameters for sending and receiving the pause packets for the port-channel interface. The default is desired.
Step 4	switch(config-if)# **exit**	Exits the interface mode and returns to the configuration mode.
Step 5	(Optional) switch# **show interface port-channel** *channel-number*	Displays interface information for the specified port channel.
Step 6	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the port-channel interface for port channel group 2 to send and receive pause packets:

```
switch# configure terminal
switch(config)# interface port-channel 2
```

```
switch(config-if)# flowcontrol receive on
switch(config-if)# flowcontrol send on
```

Configuring Load Balancing Using Port Channels

You can configure the load-balancing algorithm for port channels that applies to the entire device or to only one module regardless of the VDC association. Module-based load balancing takes precedence over device-based load balancing.

Before you begin

- Enable LACP if you want LACP-based port channels.
- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **port-channel load-balance** *method* {**dst ip** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst mac** | **dst l4port** | **dst ip-l4port** | **src-dst ip** | **src-dst mac** | **src-dst l4port** | **src-dst ip-l4port** | **src-dst ip-vlan** | **src-dst ip-l4port-vlan** | **src ip** | **src ip-l4port-vlan** | **src ip-l4port** | **src ip-vlan** | **src mac** | **src l4port** | **hash-modulo** [**force**]} [**gtp-teid**] [**module** *module-number* | **fex** {*fex-range* | **all**}] [**asymmetric**] [**rotate** *rotate*]	Specifies the load-balancing algorithm for the device or module. The range depends on the device. The default for Layer 3 is **src-dst ip** for both IPv4 and IPv6, and the default for non-IP is **src-dst mac**. **Note** The **asymmetric** keyword is valid with the **src-dst ip** command and F2 or F2e modules only. As F2 or F2e modules are symmetric by default, the **asymmetric** keyword prevents a traffic-drop occurring during bi-directional flow. A warning message prompts you that an F2 or F2e module needs to be enabled. This improves load-balancing and avoids any disruption to the system. Use the **no port-channel load-balance src-dst mac asymmetric** command to revert back to the default system settings (symmetrical). **Note** If a module-based configuration already exists, it takes precedence over the default system settings. Use the **no port-channel load-balance src-dst mac asymmetric module** command at module level to revert back to system level settings (symmetrical).

	Command or Action	Purpose
		Note The **module**, **asymmetric**, and **rotate** keywords are invalid with the **hash-modulo** command. When the **gtp-teid** keyword is specified in a packet that includes a GTP header field, the port-channel member selected depends not only on the already specified packet header fields such as MAC address, IP address, and L4 ports, but also on the 32-bit Tunnel Endpoint Identifier (TEID) header field. The packet must enter a port on an M3 module for the TEID header field to be used in the port-channel load-balancing. When the **gtp-teid** keyword is specified in a packet, the packet's TEID header field is used in port-channel member selection only if the packet contains an IPv4 or IPv6 header field followed by a UDP header field with the destination port 2152 and a GTP version 1 header field with the Protocol Type 1. All the other GTP header fields are considered GTP control messages. To avoid reordering of the GTP control messages in the network between GTP endpoints, NX-OS does not include the TEID header fields of the GTP control messages in its channel member selection. **Note** The **gtp-teid** keyword is supported only on M3 modules and does not affect the behavior of the other modules. Starting from Cisco NX-OS Release 8.3(1), the **gtp-teid** keyword is also supported on F4 modules.
Step 3	(Optional) **show port-channel load-balance**	Displays the port-channel load-balancing algorithm.
Step 4	(Optional) switch# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Use the **no port-channel load-balance** to restore the default load-balancing algorithm of src-dst mac for non-IP traffic and src-dst ip for IP traffic.

Command	Purpose
no port-channel load-balance	Restores the default load-balancing algorithm.

Example

This example shows how to configure source IP load balancing for port channels on module 5:

```
switch# configure terminal
switch(config)# port-channel load-balance src-ip-l4port module 5
```

This example shows how to configure different combinations for symmetric port channel load balancing for a port channel connected to switch1 and switch2. Use the same **rotate** *rotate-value* as listed in the following configuration combinations.

```
 ! Configure port-channel hash distribution at the global level!

switch1(config)# port-channel hash-distribution fixed
Switch2(config)# port-channel hash-distribution fixed


! Configure symmetric port-channel load balancing combinations on both
switch1 and switch2 of a port channel.!

!Combination 1!

switch1(config)# port-channel load-balance src ip
Switch2(config)# port-channel load-balance dst ip rotate 4

!Combination 2!

switch1(config)# port-channel load-balance dst ip
Switch2(config)# port-channel load-balance src ip rotate 4

!Combination 3!

switch1(config)# port-channel load-balance src ip-l4port
Switch2(config)# port-channel load-balance dst ip-l4port rotate 6

!Combination 4!

switch1(config)# port-channel load-balance dst ip-l4port
Switch2(config)# port-channel load-balance src ip-l4port rotate 6

!Combination 5!

switch1(config)# port-channel load-balance src ip-l4port vlan
Switch2(config)# port-channel load-balance dst ip-l4port rotate 8

!Combination 6!

switch1(config)# port-channel load-balance dst ip-l4port vlan
Switch2(config)# port-channel load-balance src ip-l4port rotate 8

!Combination 7!

switch1(config)# port-channel load-balance src ip-vlan
Switch2(config)# port-channel load-balance dst ip-vlan rotate 8

!Combination 8!

switch1(config)# port-channel load-balance dst ip-vlan
Switch2(config)# port-channel load-balance src ip-vlan rotate 8

!Combination 9!
```

```
switch1(config)# port-channel load-balance src l4port
Switch2(config)# port-channel load-balance dst l4port rotate 2

!Combination 10!

switch1(config)# port-channel load-balance dst l4port
Switch2(config)# port-channel load-balance src l4port rotate 2

!Combination 11!

switch1(config)# port-channel load-balance src mac
Switch2(config)# port-channel load-balance dst mac rotate 6

!Combination 12!

switch1(config)# port-channel load-balance dst mac
Switch2(config)# port-channel load-balance src mac rotate 6
```

Enabling LACP

LACP is disabled by default; you must enable LACP before you begin LACP configuration. You cannot disable LACP while any LACP configuration is present.

LACP learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once LACP identifies correctly matched Ethernet links, it group the links into a port channel. The port channel is then added to the spanning tree as a single bridge port.

To configure LACP, you must do the following:

- Enable LACP globally by using the **feature lacp** command.
- You can use different modes for different interfaces within the same LACP-enabled port channel.
- You can change the mode between active and passive for an interface only if it is the only interface that is designated to the specified channel group.

Before you begin

Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature lacp**	Enables LACP on the device.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable LACP:

```
switch# configure terminal
switch(config)# feature lacp
```

Configuring LACP Port-Channel Port Modes

After you enable LACP, you can configure the channel mode for each individual link in the LACP port channel as active or passive. This channel configuration mode allows the link to operate with LACP.

When you configure port channels with no associated aggregation protocol, all interfaces on both sides of the link remain in the on channel mode.

Before you begin

Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **channel-group** *number* **mode** {**active** | **on** | **passive**}	Specifies the port mode for the link in a port channel. After LACP is enabled, you configure each link or the entire channel as active or passive. When you run port channels with no associated aggregation protocol, the port-channel mode is always on. The default port-channel mode is on.
Step 4	(Optional) switch(config-if)# **show port-channel summary**	Displays summary information about the port channels.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to set the LACP-enabled interface to the active port-channel mode for Ethernet interface 1/4 in channel group 5:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

Configuring LACP Port-Channel Minimum Links

From Cisco NX-OS Release 5.1, you can configure the LACP minimum links feature. Although minimum links and maxbundles work only in LACP, you can enter the commands for these features for non-LACP port channels, but these commands are nonoperational.

Before you begin

Ensure that you are in the correct port-channel interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **lacp min-links** *number*	Specifies the port-channel interface to configure the number of minimum links and enters the interface configuration mode. The range is from 1 to 16.
Step 4	(Optional) switch(config-if)# **show running-config interface port-channel** *number*	Displays the port-channel minimum links configuration.

Use the **no lacp min-links** command to restore the default port-channel minimum links configuration.

Table 6: Restoring the Default Port-Channel Minimum Links Configuration

Command	Purpose
no lacp min-links	Restores the default port-channel minimum links configuration.

Example

This example shows how to configure the minimum number of port-channel interfaces on module 3:

```
switch# configure terminal
switch(config)# lacp min-links 3
```

Configuring the LACP Port-Channel MaxBundle

From Cisco NX-OS Release 5.1, you can configure the LACP maxbundle feature. Although minimum links and maxbundles work only in LACP, you can enter the commands for these features for non-LACP port channels, but these commands are nonoperational.

Before you begin

Ensure that you are in the correct port-channel interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **lacp max-bundle** *number*	Specifies the port-channel interface to configure max-bundle, and enters the interface configuration mode. The default value for the port-channel max-bundle is 16. The allowed range is from 1 to 16.
Step 4	(Optional) switch(config-if)# **show running-config interface port-channel** *number*	Displays the port-channel minimum links configuration.

Use the **no lacp max-bundle** command to restore the default port-channel max-bundle configuration.

Table 7: Restoring the Default Port-Channel Max-Bundle Configuration

Command	Purpose
no lacp max-bundle	Restores the default port-channel max-bundle configuration.

Example

This example shows how to configure the port channel interface max-bundle on module 3:

```
switch# configure terminal
switch(config)# lacp max-bundle 3
```

Configuring the LACP Fast Timer Rate

You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lacp rate** command to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces.

Note We do not recommend changing the LACP timer rate. In-service software upgrade (ISSU) and stateful switchover (SSO) are not supported with the LACP fast rate timer.

Note The number of interfaces validated with LACP Fast Timers in Cisco NX-OS Release 8.2(4) are:

- 250 physical member ports with port-channel in Layer 3 mode.
- 100 physical member ports with port-channel in Layer 2 mode with 1000 RSTP instances active on the system.

Before you begin

- Ensure that you have enabled the LACP feature.
- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **lacp rate fast**	Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface. To reset the timeout rate to its default, use the **no** form of the command.

Example

This example shows how to configure the LACP fast rate on Ethernet interface 1/4:

```
switch# configure terminal
```

```
switch(config)# interface ethernet 1/4
switch(config-if)# lacp rate fast
```

This example shows how to restore the LACP default rate (30 seconds) on Ethernet interface 1/4:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no lacp rate fast
```

Configuring the LACP System Priority

The LACP system ID is the combination of the LACP system priority value and the MAC address.

You can reuse the same configuration for the system priority values in more than one VDC.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **lacp system-priority** *priority*	Configures the system priority for use with LACP. Valid values are from 1 through 65535, and higher numbers have a lower priority. The default value is 32768. **Note** Each VDC has a different LACP system ID because the software adds the MAC address to this configured value.
Step 3	(Optional) switch(config)# **show lacp system-identifier**	Displays the LACP system identifier.
Step 4	(Optional) switch(config)# **show running-config interface port-channel** *number*	Displays the port-channel minimum links configuration.

Example

This example shows how to set the LACP system priority to 2500:

```
switch# configure terminal
switch(config)# lacp system-priority 2500
```

Configuring the LACP Port Priority

When you enable LACP, you can configure each link in the LACP port channel for the port priority.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **lacp port-priority** *priority*	Configures the port priority for use with LACP. Valid values are from1 through 65535, and higher numbers have a lower priority. The default value is 32768.
Step 4	(Optional) switch(config-if)# **show running-config interface port-channel** *number*	Displays the port-channel minimum links configuration.

Example

This example shows how to set the LACP port priority for Ethernet interface 1/4 to 40000:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# lacp port-priority 40000
```

Disabling LACP Graceful Convergence

By default, LACP graceful convergence is enabled. In situations where you need to support LACP interoperability with devices where the graceful failover defaults may delay the time taken for a disabled port to be brought down or cause traffic from the peer to be lost, you can disable convergence. If the downstream access switch is not a Cisco Nexus device, disable the LACP graceful convergence option.

Note The port channel has to be in the administratively down state before the command can be run.

Before you begin

- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.
- Enable LACP.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **shutdown**	Administratively shuts down the port channel.
Step 4	switch(config-if)# **no lacp graceful-convergence**	Disables LACP graceful convergence on the port channel.
Step 5	switch(config-if)# **no shutdown**	Brings the port channel administratively up.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to disable LACP graceful convergence on a port channel:

```
switch# configure terminal
switch(config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp graceful-convergence
switch(config-if)# no shutdown
```

Re-Enabling LACP Graceful Convergence

If the default LACP graceful convergence is once again required, you can re-enable convergence.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **shutdown**	Administratively shuts down the port channel.
Step 4	switch(config-if)# **lacp graceful-convergence**	Enables LACP graceful convergence on the port channel.
Step 5	switch(config-if)# **no shutdown**	Brings the port channel administratively up.

	Command or Action	Purpose
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable LACP graceful convergence on a port channel:

```
switch# configure terminal
switch(config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lacp graceful-convergence
switch(config-if)# no shutdown
```

Disabling LACP Port

LACP sets a port to the suspended state if it does not receive an LACP PDU from the peer. This process can cause some servers to fail to boot up as they require LACP to logically bring up the port.

Note You should only enter the **lacp suspend-individual** command on edge ports. The port channel has to be in the administratively down state before you can use this command.

Before you begin

- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.
- Enable LACP.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **shutdown**	Administratively shuts down the port channel.
Step 4	switch(config-if)# **no lacp suspend-individual**	Disables LACP individual port suspension behavior on the port channel.
Step 5	switch(config-if)# **no shutdown**	Brings the port channel administratively up.

	Command or Action	Purpose
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to disable LACP individual port suspension on a port channel:

```
switch# configure terminal
switch(config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp suspend-individual
switch(config-if)# no shutdown
```

Re-Enabling LACP Port

You can re-enable the default LACP individual port suspension.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *channel-number*	Specifies the port-channel interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **shutdown**	Administratively shuts down the port channel.
Step 4	switch(config-if)# **lacp suspend-individual**	Enables LACP individual port suspension behavior on the port channel.
Step 5	switch(config-if)# **no shutdown**	Brings the port channel administratively up.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to re-enable the LACP individual port suspension on a port channel:

```
switch# configure terminal
switch(config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lacp suspend-individual
switch(config-if)# no shutdown
```

Configuring Port-Channel Hash Distribution

From Cisco NX-OS Release 6.1(1), the adaptive and fixed hash distribution configuration is supported at both global and port-channel levels. This option minimizes traffic disruption by minimizing Result Bundle Hash (RBH) distribution changes when members come up or go down so that flows that are mapped to unchange RBH values continue to flow through the same links. The port-channel level configuration overrules the global configuration. The default configuration is adaptive globally, and there is no configuration for each port channel, so there is no change during an ISSU. No ports are flapped when the command is applied, and the configuration takes effect at the next member link change event. Both modes work with RBH module or non-module schemes.

During an ISSD to a lower version that does not support this feature, you must disable this feature if the fixed mode command is being used globally or if there is a port-channel level configuration.

Configuring Port-Channel Hash Distribution at the Global Level

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-channel hash-distribution** {**adaptive** | **fixed**}	Specifies the port-channel hash distribution at the global level. • **adaptive**—This is the default mode. RBH values are asymmetric. • **fixed**—Peer port connections must be in an ascending order. RBH values are distributed symmetrically as per the ascending order of the port. The number of buckets in each port is equal. While configuring this command, the following warning is displayed: This global command does not take effect until the next member link event (link down/up/no shutdown/shutdown). Do you still want to continue(y/n)? [yes]
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure adaptive hash distribution at the global level:

```
configure terminal
 port-channel hash-distribution adaptive
show port-channel rbh-distribution
```

```
ChanId    Member port    RBH values         Num of buckets
--------  -------------  -----------------  ----------------
 3022      Eth15/5        0                  1
 3022      Eth15/21       4                  1
 3022      Eth15/6        1                  1
 3022      Eth15/13       2                  1
 3022      Eth15/14       3                  1
```

Configuring Port-Channel Hash Distribution at the Port-Channel Level

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** {*channel-number* | *range*}	Specifies the interface to configure, and enters the interface configuration mode.
Step 3	switch(config-if)# **[no] port-channel hash-distribution** {**adaptive** | **fixed**}	Specifies the port-channel hash distribution at the global level. • **adaptive**—This is the default mode. RBH values are asymmetric. • **fixed**—Peer port connections must be in an ascending order. RBH values are distributed symmetrically as per the ascending order of the port. The number of buckets in each port is equal. While configuring this command, the following warning is displayed: The command does not take effect until the next member link event (link down/up/no shutdown/shutdown). Do you still want to continue(y/n)? [yes]
Step 4	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure fixed hash distribution at the port channel level:

```
configure terminal
 interface port-channel 3010
  port-channel hash-distribution fixed
show port-channel rbh-distribution interface port-channel 3021
ChanId    Member port    RBH values         Num of buckets
--------  -------------  -----------------  ----------------
 3021      Eth15/23       0                  1
 3021      Eth15/24       1                  1
```

```
3021      Eth15/25       2                 1
3021      Eth15/26       3                 1
```

Configuring RBH Modulo Mode

Enabling RBH modulo mode flaps all port channels.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-channel load-balance hash-modulo**	Enables the RBH modulo mode. This command reinitializes all port channels so there is an option to continue or not continue. **Note** This command is rejected if the current system-wide module types include the M1-Series module. To remove the M1-Series module type from the system-wide configuration, enter the **system module-type f1, f2, m1xl, m2xl** command.
Step 3	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable the RBH modulo mode:

```
switch# configure terminal
switch(config)# port-channel load-balance hash-modulo
```

Configuring Minimum Links on the FEX Fabric Port Channel

From Cisco NX-OS Release 6.1(3), you can configure a minimum number of links for the FEX fabric port channel so that when a certain number of FEX fabric port-channel member ports go down, the host-facing interfaces of the FEX are suspended.

Before you begin

Ensure that you are in the correct port-channel interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface port-channel** *number*	Specifies the interface to configure and enters the interface configuration mode.
Step 3	switch(config-if)# **switchport**	Configures the interface as a Layer 2 access port.
Step 4	switch(config-if)# **switchport mode fex-fabric**	Sets the port channel to support an external Fabric Extender.
Step 5	switch(config-if)# [**no**] **port-channel min-links** *number*	Configures the minimum number of links on the FEX fabric port channel. The range is from 1 to 16.
Step 6	(Optional) switch(config-if)# **show port-channel summary**	Displays summary information about the port channels.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure the minimum number of links for the FEX fabric port channel:

```
switch# configure terminal
switch(config)# interface port-channel 100
switch(config-if)# switchport
switch(config-if)# switchport mode fex-fabric
switch(config-if)# port-channel min-links 3
switch(config-if)# show port-channel summary
Flags: D - Down P - Up in port-channel (members) I - Individual
H - Hot-standby (LACP only) s - Suspended r - Module-removed
S - Switched R - Routed U - Up (port-channel)
M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port- Type Protocol Member Ports Channel
--------------------------------------------------------------------------------
101 Po101(SM) Eth NONE Eth10/46(P) Eth10/47(P) Eth10/48(P)
```

Configuring Random Load Balance

Configuring Random Load Balance on a Port Channel

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure interface port-channel.

switch(config)# **interface port-channel** *port-channel-number*

Step 3 Configure random load balance for the port-channel interface. Use the **no** form of the following command to disable the random load balance feature.

switch(config-if)# **egress port-channel load-balance random**

Note
This will override the default system or module-wide port-channel load balance settings. To configure random load balancing for ingress traffic, configure the **egress port-channel load-balance random** command on an switch virtual interface (SVI) on Layer 3.

Configuring Random Load Balance on an Interface

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure a port-channel interface:

switch(config)# **interface** *interface-name*

Step 3 Configure random load balance for the interface. Use the **no** form of the following command to disable the random load balance feature.

switch(config-if)# **egress port-channel load-balance random**

Note
The ingress Layer 3 interface or a port-channel interface performs random load balance on the Layer 2 or Layer 3 egress interface and port-channel interface.

Configuring random load balance on a single physical interface is useful in scenarios where traffic comes in from an ingress Layer 3 interface and goes out of a port-channel interface.

Configuring Random Load Balance for a VLAN

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure a VLAN:

switch(config)# **vlan** *vlan-id*

Step 3 Enter VLAN configuration mode:

switch(config-vlan)# **vlan configuration** *vlan-id*

Step 4 Configure random load balance for the VLAN. Use the **no** form of the following command to disable the random load balance feature.

switch(config-if)# **egress port-channel load-balance random**

Note
Random load balance is applied on all the Layer 2 ingress interfaces under the VLAN. The ingress interfaces perform random load balance on all the Layer 2 or Layer 3 port-channel egress interfaces.

Configuring Random Load Balance for an SVI

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure a switch virtual interface (SVI):

switch(config)# **vlan** *vlan-range*

Step 3 Enter VLAN configuration mode:

switch(config)# **vlan configuration** *vlan-range*

Step 4 Configure random load balance for the SVI for ingress traffic. Use the **no** form of the following command to disable the random load balance feature.

switch(config-vlan-config)# **egress port-channel load-balance random**

Example: Configuring Random Load Balance

This example shows how to configure random load balance on a port-channel interface:

```
configure terminal
    interface port-channel 44
       egress port-channel load-balance random
```

This example shows how to configure random load balance on a physical interface:

```
configure terminal
    interface Ethernet6/1
       egress port-channel load-balance random
```

This example shows how to configure random load balance on a VLAN:

```
configure terminal
    vlan 100
       vlan configuration 100
         egress port-channel load-balance random
```

This example shows how to configure random load balance on a switch virtual interface (SVI) for ingress traffic:

```
configure terminal
    vlan 2-10
    vlan configuration 2-10
       egress port-channel load-balance random
```

Verifying Port-Channel Configurations

Use the following commands to verify port-channel configurations:

Table 8: Verifying Port-Channel Configurations

Command	Purpose
show interface port-channel *channel-number*	Displays the status of a port-channel interface.
show feature	Displays enabled features.
load-interval {**interval** *seconds* {**1** | **2** | **3**}}	From Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series devices, sets three different sampling intervals to bit-rate and packet-rate statistics.
show port-channel compatibility-parameters	Displays the parameters that must be the same among the member ports in order to join a port channel.

Command	Purpose
show port-channel database [**interface port-channel** *channel-number*]	Displays the aggregation state for one or more port-channel interfaces.
show port-channel load-balance	Displays the type of load balancing in use for port channels.
show port-channel rbh distribution	Displays the distribution of RBH values across port-channel interfaces.
show port-channel summary	Displays a summary for the port-channel interfaces.
show port-channel traffic	Displays the traffic statistics for port channels.
show port-channel usage	Displays the range of used and unused channel numbers.
show lacp {**counters** [**interface port-channel** *channel-number*] | [**interface** *type/slot*] | **neighbor** [**interface port-channel** *channel-number*] | **port-channel** [**interface port-channel** *channel-number*] | **system-identifier**]]}	Displays information about LACP.
show running-config interface port-channel *channel-number*	Displays information about the running configuration of the port-channel.
show interface status error policy [**detail**]	Displays errors on interfaces and VLANs that are inconsistent with hardware policies. The **detail** command displays the details of the interfaces and VLANs that receive an error.

For more information about these commands, see the Cisco Nexus 7000 Series NX-OS Interfaces Command Reference.

Monitoring the Port-Channel Interface Configuration

Use the following commands to display port-channel interface configurations:

Table 9: Monitoring the Port-Channel Interface Configuration

Command	Purpose
clear counters interface port-channel *channel-number*	Clears the counters.
clear lacp counters [**interface port-channel** *channel-number*]	Clears the LACP counters.
load-interval {**interval** *seconds* {**1** | **2** | **3**}}	From Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series devices, sets three different sampling intervals to bit-rate and packet-rate statistics.

Command	Purpose
show interface counters [**module** *module*]	Displays input and output octets unicast packets, multicast packets, and broadcast packets.
show interface counters detailed [**all**]	Displays input packets, bytes, and multicast and output packets and bytes.
show interface counters errors [**module** *module*]	Displays information about the number of error packets.
show lacp counters	Displays statistics for LACP.

See the Cisco Nexus 7000 Series NX-OS Interfaces Command Reference for information about these commands.

Configuration Examples for Port Channels

This example shows how to create an LACP port channel and add two Layer 2 interfaces to that port channel:

```
switch# configure terminal
switch(config)# feature lacp
switch(config)# interface port-channel 5
switch(config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 1/7
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode
```

This example shows how to add two Layer 3 interfaces to a channel group. The Cisco NX-OS software automatically creates the port channel.

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch(config)# interface ethernet 2/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch(config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8
```

Related Documents

Table 10: Related Documents

Related Topic
Cisco Nexus 7000 Series NX-OS Interfaces Command Reference
Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide
Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x
Cisco NX-OS Licensing Guide
VLANs, MAC address tables, private VLANs, and the Spanning Tree Protocol.
Cisco Nexus 7000 Series NX-OS FabricPath Command Reference
Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide

Standards

Table 11: Standards

Standards	Title
IEEE 802.3ad	—

MIBs

Table 12: MIBs

MIBs	MIBs Link
• IEEE8023-LAG-CAPABILITY • CISCO-LAG-MIB	To locate and download MIBs, go to: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.s