# Configuring Port Channels



# About Port Channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to 32 individual active links into a port channel to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

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

You can apply port security to port channels. See the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide* for information about port security.

You can also change the port channel from Layer 3 to Layer 2. See the Configuring Layer 2 Interfaces chapter for information about creating Layer 2 interfaces.

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.

A Layer 2 port channel interface and it's member ports can have different STP parameters. Changing the STP parameters of the port channel does not impact the STP parameters of the member ports because a port channel interface takes precedence if the member ports are bundled.

**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 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 Overview section for information about LACP.

# Port Channels

A port channel bundles physical links into a channel group to create a single logical link that provides the aggregate bandwidth of up to 32 physical links. 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.

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 (see the “Configuring Port Channels” section).

**Note** The 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).

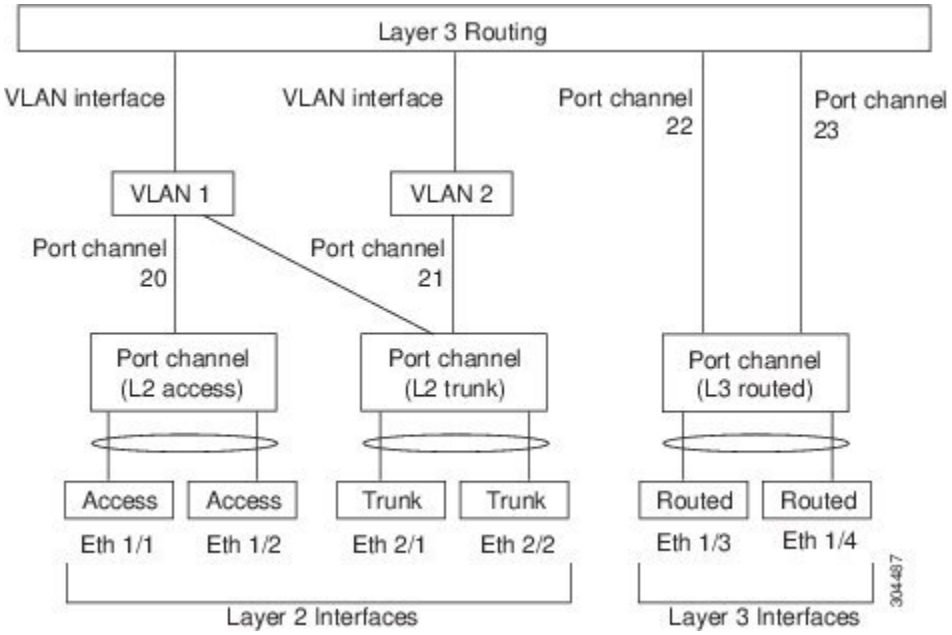
You can create port channels directly by creating the port-channel interface, or you can create a channel group that acts to aggregate individual ports into a bundle. When you associate an interface with a channel group, the software creates a matching port channel automatically if the port channel does 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.

# Port-Channel Interfaces

The following 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.

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 Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide for information about configuring static MAC addresses on Layer 3 port channels.

See the "Configuring Layer 2 Interfaces" chapter for information about configuring Layer 2 ports in access or trunk mode and the "Configuring Layer 3 Interfaces" chapter for information about configuring Layer 3 interfaces and subinterfaces.

# Basic Settings

You can configure the following basic settings for the 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.
- Description
- Duplex

- IP addresses
- Maximum Transmission Unit (MTU)
- Shutdown
- Speed

# 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:

- Network layer
- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- MTU size
- SPAN—Cannot be a SPAN source or a destination port
- Layer 3 ports—Cannot have subinterfaces
- Storm control
- Flow-control capability
- Flow-control configuration
- Media type, either copper or fiber

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
- 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

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

**Note** All the QoS service policies on the port-channel are implicitly applied on the member ports when they join the port-channel. You will not see QoS service policies in the running-config of the member ports. Use the command show policy-map interface ethernet <slot/port> to see the the policies applied on the member ports.

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 load- balancing mode to apply to all port channels that are configured on the entire device. You can configure one load-balancing mode for the entire device. 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.

The default load-balancing mode for Layer 3 interfaces is the source and destination IP L4 ports, 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-l4port.

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
- GRE inner IP headers with source, destination and source-destination

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.

You can configure load balancing either by the entire system or by specific modules.

**Note** Configuring hash load balancing applies to unicast and multicast traffic on Cisco Nexus 9200, 9300-EX, and 9300-GX Series switches.

The unicast and multicast traffic is load-balanced across port-channel links based on configured load-balancing algorithm displayed in **show port-channel load-balancing** command output.

The multicast traffic uses the following methods for load balancing with port channels:

- Multicast traffic with Layer 4 information—Source IP address, source port, destination IP address, destination port
- Multicast traffic without Layer 4 information—Source IP address, destination IP address
- Non-IP multicast traffic—Source MAC address, destination MAC address

**Note** Devices that run Cisco IOS can optimize the behavior of the member ports ASICs if a failure of a single member occurred by running the port-channel hash-distribution command. The Cisco Nexus 9000 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.

**Note** Devices that run Cisco IOS can optimize the behavior of the member ports ASICs if a failure of a single member occurred by running the port-channel hash-distribution command. The Cisco Nexus 9000 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 for the entire device.

# Symmetric Hashing

To be able 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-dst ip
- src-dst ip-l4port
- src-dst ip-l4port-vlan
- src-dst ip-vlan

# Guidelines and Limitations for ECMP

You might observe that load balancing with Layer 2/Layer 3 GW flows are not load balanced equally among all links when the switch comes up initially after reload. There are two CLIs to change the ECMP hash configuration in the hardware. The two CLI commands are mutually exclusive.

- Enter the **port-channel load-balance [src | src-dst | dst] mac** command for MAC-based only hash.
- For hash based on IP/Layer 4 ports, enter either the **ip load-share** or **port-channel load-balance** command.
- The **port-channel load-balance** command can overwrite the **ip load-share** command. It is better to enter the **port-channel load-balance** command which helps to set both the IP and MAC parameters.
- There are no options to force the hashing algorithm based on the IP/Layer 4 port. The default MAC configuration is always programmed as a part of the port channel configuration.
- ECMP resilient hashing is not supported for traffic flows over tunnel.

# Resilient Hashing

With the exponential increase in the number of physical links used in data centers, there is also the potential for an increase in the number of failed physical links. In static hashing systems that are used for load balancing flows across members of port channels or Equal Cost Multipath (ECMP) groups, each flow is hashed to a link. If a link fails, all flows are rehashed across the remaining working links. This rehashing of flows to links results in some packets being delivered out of order even for those flows that were not hashed to the failed link.

This rehashing also occurs when a link is added to the port channel or Equal Cost Multipath (ECMP) group. All flows are rehashed across the new number of links, which results in some packets being delivered out of order.

Resilient hashing maps flows to physical ports. In case a link fails, the flows assigned to the failed link are redistributed uniformly among the working links. The existing flows through the working links are not rehashed and their packets are not delivered out of order.

Resilient hashing is supported only for ECMP groups and not on part channel interfaces. Resiliency is guaranteed only upon deletion of a member in an ECMP group, not on adding a member to the ECMP group. When a link is added to the port channel or ECMP group, some of the flows hashed to the existing links are rehashed to the new link, but not across all existing links.

Resilient hashing also occurs when a link is added to the port channel or Equal Cost Multipath (ECMP) group. Resilient hashing is supported on both Layer 2 port-channel member links and Layer 3 ECMP paths on the routing table.

Beginning Cisco NX-OS Release 9.3(3), resilient hashing is supported on Cisco Nexus 92160YC-X, 92304QC, 9272Q, 9232C, 9236C, 92300YC switches.

Resilient hashing is supported only by ECMP groups and on port channel interfaces. When a link is added to the port channel or ECMP group, some of the flows hashed to the existing links are rehashed to the new link, but not across all existing links.

Resilient hashing maps flows to physical ports and it is supported for both ECMP groups and port channel interfaces.

If a physical link fails, the flows originally assigned to the failed link are redistributed uniformly among the remaining working links. The existing flows through the working links are not rehashed and hence are not impacted.

Resilient hashing supports IPv4 and IPv6 unicast traffic, but it does not support IPv4 multicast traffic.

Resilient hashing is supported on all the Cisco Nexus 9000 Series platforms. (NX-OS 7.0(3)I3(1) release and later). Beginning Cisco NX-OS Release 9.3(3), resilient hashing is supported on Cisco Nexus 92160YC-X, 92304QC, 9272Q, 9232C, 9236C, 92300YC switches.

# GTP Tunnel Load Balancing

GPRS Tunneling Protocol (GTP) is used mainly to deliver mobile data on wireless networks via Cisco Nexus 9000 Series switches as the core router. When two routers carrying GTP traffic are connected with link bundling, the traffic is required to be distributed evenly between all bundle members.

To achieve load balancing, Cisco Nexus 9000 Series switches use 5-tuple load balancing mechanism. The load balancing mechanism takes into account the source IP, destination IP, protocol, Layer 4 resource and destination port (if traffic is TCP or UDP) fields from the packet. In the case of GTP traffic, a limited number of unique values for these fields restrict the equal distribution of traffic load on the tunnel.

In order to avoid polarization for GTP traffic in load balancing, a tunnel endpoint identifier (TEID) in the GTP header is used instead of a UDP port number. Since the TEID is unique per tunnel, traffic can be evenly load balanced across multiple links in the bundle.

Beginning Cisco Nexus Release 7.0(3)I7(3), GTP Tunnel Load Balancing is supported on Cisco Nexus 9300-EX platform switches.

Beginning Cisco Nexus Release 7.0(3)I7(4), GTP Tunnel Load Balancing is supported on Cisco Nexus 9300-FX and 9364C platform switches.

Beginning Cisco Nexus Release 9.3(3) GTP Tunnel Load Balancing is supported on Cisco Nexus 9500 platform switches with 9700-EX and 9700-FX line cards. However, GTP Tunnel Load Balancing for IPv6 flow is supported only on Cisco Nexus 9500 platform switches with FM-E2 fabric modules. It is not supported on Cisco Nexus 9500 platform switches with FM-E fabric modules.. Because the hardware control is same for both Port-channel and ECMP, enabling either port-channel load-balance or ip load-sharing with GTP option enables GTP TEID based load balancing for both the cases. In multi encapsulated packets, if the GTP header is a part of outer header, it picks up GTP TEIF from outer layer for hashing. If the GTP header is a part of inner header, it picks up GTP TEIF from inner layer for hashing.

GTP Tunnel Load Balancing is supported on Cisco Nexus 9300-EX, 9300-FX, 9300-FX2, 9364C, and 9300-GX platform switches.

This feature overrides the source and destination port information with the 32-bit TEID value that is present in GTPU packets.

GTP tunnel load balancing feature adds support for:

- GTP with IPv4/IPv6 transport header on physical interface
- GTP traffic over TE tunnel
- GTPU with UDP port 2152

The **ip load-sharing address source-destination gtpu** command enables the GTP tunnel load balancing.

To know the egress interface for GTP traffic after load balancing, use **show cef {ipv4 | ipv6} exact-route** command with TEID in place of L4 protocol source and destination port number. Use 16MSBist of TEID in source port and 16LSBits of TEID in destination port.

The **port-channel load-balance src-dst gtpu** command enables GTP packets with UDP destination port number 2152 to load balance based on the GTP TEID value. This command enables the switch to load balance for GTP packets even if the outer five tuples (*src-ip*, *dst-ip*, *ip proto*, *L4 sport*, *L4 dport*) are same. Because the hardware controls for port channel and ECMP are same, enabling either port-channel load-balance or ip load-sharing with GTP option enables GTP TEID based load balancing.

- The **port-channel load-balance src-dst gtpu** command is applicable for both GTP packets, with or without VXLAN encapsulation
- When GTP header is a part of the outer layer, the **port-channel load-balance src-dst gtpu** command picks up GTP TEID from outer layer for hashing.
- When GTP header is part of inner layer, the **port-channel load-balance src-dst gtpu** command picks up GTP TEID from inner layer for hashing.

You need to set the protocol field to 17 and set the value for other parameters when you use the **show port-channel load-balance forwarding-path** command. An example is listed below.

```
switch(config)# show port-channel load-balance forwarding-path interface port-channel 2
src-ip 1.1.1.1 dst-ip 2.2.2.2 gtpteid
0x3 protocol 17
```

# LACP

LACP allows you to configure up to 16 interfaces into a port channel.

## LACP Overview

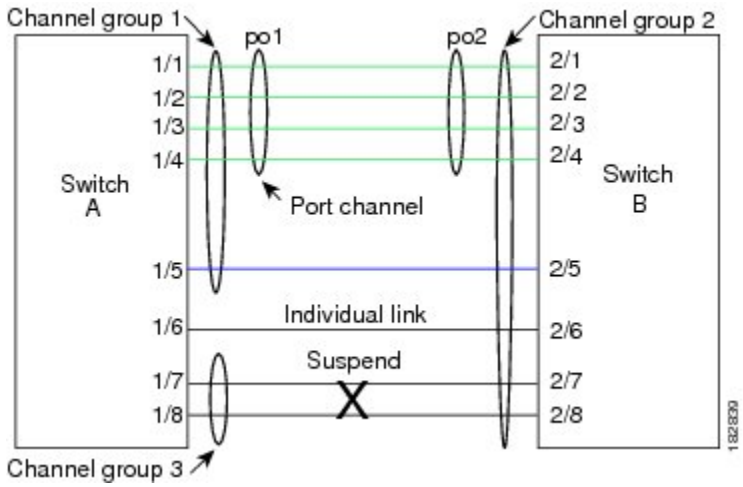
The Link Aggregation Control Protocol (LACP) for Ethernet is defined in IEEE 802.1AX and IEEE 802.3ad. This protocol controls how physical ports are bundled together to form one logical channel.

**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.

The system automatically takes a checkpoint before disabling the feature, and you can roll back to this checkpoint. See the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide for information about rollbacks and checkpoints.

The following figure 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 32 interfaces in a channel group.

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

**Note** If you downgrade a Cisco Nexus 9500 series switch that is configured to use LACP vPC convergence feature, that runs Cisco NX-OS Release 7.0(3)I7(5) to a lower release, the configuration is removed. You must configure the LACP vPC convergence feature again when you upgrade the switch.

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 either **active** or **passive**. You can configure 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.

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.

The following table describes the channel modes.

***Table 1: Channel Modes for Individual Links in a Port Channel***

| Channel Mode | Description |
|---|---|
| **passive** | The LACP is enabled on this port channel and the ports are in a passive negotiating state. Ports responds to LACP packets that it receives but does not initiate LACP negotiation. |
| **active** | The LACP is enabled on this port channel and the ports are in an active negotiating state. Ports initiate negotiations with other ports by sending LACP packets. |

| Channel Mode | Description |
|---|---|
| **on** | The LACP is disabled on this port channel and the ports are in a non-negotiating state. The **on** state of the port channel represents the static mode.<br><br>The port will not verify or negotiate port channel memberships. If you attempt to change the channel mode to active or passive before enabling LACP, the device displays an error message. 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 **on** state is the default port-channel mode<br><br>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.<br><br>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. |

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.

Two devices can form an LACP port channel when their ports are in different LACP modes if the modes are compatible as in the following example:

***Table 2: Channel Modes Compatibility***

| Device 1 > Port-1 | Device 2 > Port-2 | Result |
|---|---|---|
| Active | Active | Can form a port channel. |
| Active | Passive | Can form a port channel. |
| Passive | Passive | Cannot form a port channel because no ports can initiate negotiation. |
| On | Active | Cannot form a port channel because LACP is enabled only on one side. |
| On | Passive | Cannot form a port channel because LACP is not enabled. |

Ports can form an LACP port channel when they are in different LACP modes if the modes are compatible as in the following 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

This section describes the LACP 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.

**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.

# LACP-Enabled and Static Port Channels Differences

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

***Table 3: Port Channels with LACP Enabled and Static Port Channels***

| Configurations | Port Channels with LACP Enabled | Static Port Channels |
|---|---|---|
| Protocol applied | Enable globally | Not applicable |
| Channel mode of links | Can be either:<br>• Active<br>• Passive | Can only be On |
| Maximum number of links in channel | 32 | 32 |

# LACP Compatibility Enhancements

When a Cisco Nexus 9000 Series device is connected to a non-Nexus peer, its graceful failover defaults may delay the time that is taken to bring down a disabled port 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 suspended state if it does not receive an LACP PDU from the peer. **lacp suspend-individual** is a default configuration on Cisco Nexus 9000 series switches. This command puts the port in suspended state if it does not receive any LACP PDUs. In some cases, although this feature helps in preventing loops created due to misconfigurations, it can cause servers fail to boot up because they require LACP to logically bring up the port. You can put a port into an individual state by using the **no lacp suspend-individual**. Port in individual sate takes attributes of the individual port based on the port configuration.

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 put a port into an individual state by using the **no lacp suspend-individual**.

LACP port-channels exchange LACP PDUs for quick bundling of links when connecting a server and a switch. However, the links go into suspended state when the PDUs are not received.

The **delayed LACP** feature enables one port-channel member, the delayed-LACP port, to come up first as a member of a regular port-channel before LACP PDUs are received. After it is connected in LACP mode, other members, the auxiliary LACP ports, are brought up. This avoids having the links becoming suspended when PDUs are not received.

Which port in the port-channel comes up first depends on the port-priority value of the ports. A member link in a port channel with lowest priority value, will come come up first as a LACP delayed port. Regardless of the operational status of the links, the configured priority of a LACP port is used to select the delayed-lacp port

This feature supports Layer 2 port channels, trunk mode spanning tree, and vPC and has the following limitations:

- Delayed LACP feature does not work on a device where no **lacp suspend-individual** is already configured.
- You cannot configure **no lacp suspend-individual**on a device where delayed LACP feature is already implemented.
- Using **no lacp suspend-individual** and **lacp mode delay** on a same port channel is not recommended because it can put non-lacp delayed ports in individual state. As a best practice, you must avoid combining these two configurations.
- Not supported on Layer 3 port channels.
- Not supported on Cisco Nexus 9500 Switches and FEX HIF and FEX fabric ports.

# Delayed LACP

LACP port-channels exchange LACP PDUs for quick bundling of links when connecting a server and a switch. However, the links go into suspended state when the PDUs are not received.

The delayed LACP feature enables one port-channel member, the delayed-LACP port, to come up first as a member of a regular port-channel before LACP PDUs are received. After it is connected in LACP mode, other members, the auxiliary LACP ports, are brought up. This avoids having the links becoming suspended when PDUs are not received.

Which port in the port-channel comes up first depends on the port-priority value of the ports. A member link in a port channel with lowest priority value, will come come up first as a LACP delayed port. Regardless of the operational status of the links, the configured priority of a LACP port is used to select the delayed-lacp port

This feature supports Layer 2 port channels, trunk mode spanning tree, and vPC and has the following limitations:

- Delayed LACP feature does not work on a device where no **lacp suspend-individual** is already configured.
- You cannot configure **no lacp suspend-individual**on a device where delayed LACP feature is already implemented.
- Using **no lacp suspend-individual** and **lacp mode delay** on a same port channel is not recommended because it can put non-lacp delayed ports in individual state. As a best practice, you must avoid combining these two configurations.
- Not supported on Layer 3 port channels.

- Not supported on Cisco Nexus 9500 Switches and FEX HIF and FEX fabric ports.

# LACP Port-Channel Minimum Links and MaxBundle

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

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 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.

When the LACP fast timer rate is configured on port channel member ports, LACP PDUs are exchanged every second. A timeout occurs when three consecutive LACP PDUs are missed. During a system switchover and ISSU, LACP PDUs may not be transmitted in 1-second intervals, which might result in a time out and subsequent reinitialization of the peer port. Beginning with Cisco NX-OS Release 9.3(1), the following Cisco Nexus 9500 Series switches support LACP fast timers during a user-initiated system switchover:

- Cisco Nexus 9500 Series switches with N9K-C9504-FM-E, N9K-C9508-FM-E, N9K-C9516-FM-E, N9K-C9508-FM-E2, or N9K-C9516-FM-E2 fabric modules
- Cisco Nexus 9500 Series switches with N9K-X9736C-EX, N9K-X9732C-EX, N9K-X9732C-FX, N9K-X97160YC-EX, N9K-X9732C-EXM, N9K-X9736C-FX, N9K-X9788TC-FX, or N9K-X97284YC-FX line cards

ISSU and ungraceful switchovers are not supported with LACP fast timers.

## 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.

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.

**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. 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 9000 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 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

Port channeling has the following configuration guidelines and limitations:

- For scaled port-channel deployments on Cisco Nexus 9516 switch with Gen 1 line cards, you need to use the **port-channel scale-fanout** command followed by **copy run start** and **reload** commands.
- **show** commands with the **internal** keyword are not supported.
- The LACP port-channel minimum links and maxbundle feature is not supported for host interface port channels.
- 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 the "Configuring Basic Interface Parameters" chapter 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.
- When sending IPv6 traffic with encapsulated NVGRE packets, traffic is not load shared across all available uplinks. Only one uplink is used. However, with IPv4 encapsulated NVGRE traffic, traffic is sent across all uplinks. This is applicable to Cisco Nexus 9300-FX3 switches platforms in Cisco NXOS Release 10.1(1).
- 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.
- 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.
- Port-channels are not supported on generation 1 100G line cards (N9K-X9408PC-CFP2) or generic expansion modules (N9K-M4PC-CFP2).
- Port-channels are supported on devices with generation 2 (and later) 100G interfaces.
- The port channel might be affected by the limitations of the Application Leaf Engine (ALE) uplink ports on Cisco Nexus 9300 and 9500 Series devices:Limitations for ALE Uplink Ports.
- Resilient hashing for port channels is not supported on Cisco Nexus 9200, Cisco Nexus 9300-EX, and Cisco Nexus 9500 switches with 9700-EX line cards.
- Resilient hashing (port-channel load-balancing resiliency) and VXLAN configurations are not compatible with VTEPs using ALE uplink ports.

**Note** Resilient hashing is disabled by default.

- The maximum number of subinterfaces for a satellite/FEX port is 63.

- On a Cisco Nexus 92300YC switch, the first 24 ports that are part of the same quadrant. All the ports in the same quadrant must have same speed. Having different speed on ports in a quadrant is not supported. Following are the first 24 ports on the Cisco Nexus 92300YC switch that share same quadrant:
  - 1,4,7,10
  - 2,5,8,11
  - 3,6,9,12
  - 13,16,19,22
  - 14,17,20,23
  - 15,18,21,24
- On a Cisco Nexus 9500 switch with a X96136YC-R line card, the ports 17–48 are part of the same quadrant. Ports in the same quadrant must have same speed (1/10G or 25G) on all ports. Having different speed on ports in a quadrant is not supported. If you set different speed in any of the ports in a quadrant, the ports go into error disable state. Interfaces in same quadrant are:
  - 17–20
  - 21–24
  - 25–28
  - 29–32
  - 33–36
  - 37–40
  - 41–44
  - 45–48
- For a given set of ports in the same quadrant, you must use a transceiver of the same speed. You should not mix speeds within a set of ports in the same quadrant. The port numbers that share same quadrant are as follows:
  - 1,4,7,10
  - 2,5,8,11
  - 3,6,9,12
  - 13,16,19,22
  - 14,17,20,23
  - 15,18,21,24
  - 25,28,31,34
  - 26,29,32,35
  - 27,30,33,36
  - 37,40,43,46

  - 38,41,44,47
  - 39,42,45,48
- Resilient hashing is supported on Cisco Nexus 9500 Series switches with N9K-X9636C-R, N9K-X9636Q-R, N9K-X9636C-RX, and N9K-X96136YC-R line cards.
- Port-channel symmetric hashing is supported on Cisco Nexus 9200, 9300-EX, 9300-FX/FX2, and 9300-GX platform switches and Cisco Nexus 9500 platform switches with N9K-X9732C-EX, N9K-X9736C-EX, N9K-X9736C-FX, and N9K-X9732C-FX line cards.
- ECMP symmetric hashing is supported on Cisco Nexus 9200, 9300-EX, and 9300-FX/FX2/FX3 platform switches and Cisco Nexus 9500 platform switches with N9K-X9732C-EX, N9K-X9736C-EX, N9K-X9736C-FX, and N9K-X9732C-FX line cards.
- GRE inner headers are supported on the following switches:
  - Cisco Nexus 9364C platform switches
  - Cisco Nexus 9336C-FX2, 9348GC-FXP, 93108TC-FX, 93180YC-FX, and 93240YC-FX2 platform switches
  - Cisco Nexus 9300-GX platform switches.
  - Cisco Nexus 9300-FX3 platform switches
  - Cisco Nexus 9500 platform switches with N9K-X9736C-FX line cards
- Beginning with Cisco NX-OS Release 9.3(6), Cisco Nexus 9300-FX2 platform switches support the coexistence of VXLAN and IP-in-IP tunneling. For more information, including limitations, see the **VXLAN and IP-in-IP Tunneling** section in the *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x)*.
- Beginning with Cisco Nexus 9000 NX-OS release 10.2(1), the **[no] lacp suspend-individual** configuration is allowed on port channels that are in admin up state. This feature is supported on all Cisco Nexus 9000 series platform switches.
- Beginning with Cisco Nexus 9000 NX-OS release 10.2(1), the **[no] lacp suspend-individual pxe** configuration supports PXE boot and prevents L2 loop due to server misconfiguration. This configuration allows only one port-channel member to be in individual (I) state for both regular port-channels and across vPC peers. Both **lacp suspend-individual** and **lacp suspend-individual pxe** are the same configurations and show up in the show running as a unified show lacp suspend-individual. For vPC subsystems, this configuration must be applied on both vPC legs. If not, the vPC secondary will be brought down. This feature is supported on all Cisco Nexus 9000 series platform switches. However, FEX is not supported.
- For FEX interfaces using LACP, all DME oper/runtime properties for the FEX interfaces does not get updated. All runtime updates for FEX ports happens from FEX LACP process context and are not communicated to the parent switch.This is a day-1 behaviour.
- Beginning with Cisco NX-OS Release 10.3(1)F, the hashing based on src/dst ip and src/dst L4 port number is supported on Cisco Nexus 9808 platform switches.
- From Cisco NX-OS Release 10.4(1), Layer 3 port-channel is supported on Cisco Nexus 9800, and 9332D-H2R switches.

- From Cisco NX-OS Release 10.4(2)F, Layer 3 port-channel is supported on Cisco Nexus 9232E-B1 switch.
- Beginning with Cisco NX-OS Release 10.4(1)F, the hashing based on src/dst ip and src/dst L4 port number is supported on the following Cisco Nexus Switches:
  - Cisco Nexus 9804 Platform switches
  - Cisco Nexus X98900CD-A, and KX9836DM-A line cards with Cisco Nexus 9808 and 9804 switches.
- Beginning with Cisco NX-OS Release 10.3(2)F, the symmetric port-channel load balancing based on inner-header for GTP packets is supported on Cisco Nexus 9300-FX/FX2 ToR switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, the hashing based on src/dst ip and src/dst L4 port number is supported on N9KX98900CD-A and N9KX9836DM-A line cards with Cisco Nexus 9808 and 9804 switches.
- Beginning with Cisco NX-OS Release 10.4(2)F, the hashing based on src/dst ip and src/dst Layer 4 port number is supported on Cisco Nexus C9232E-B1 switch.

# Default Settings

The following table lists the default settings for port-channel parameters.

***Table 4: Default Port-Channel Parameters***

| Parameters | 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 |
| LACP | Disabled |
| Channel mode | on |
| LACP system priority | 32768 |
| LACP port priority | 32768 |
| Minimum links for LACP | 1 |
| Maxbundle | 32 |
| Minimum links for FEX fabric port channel | 1 |

# Configuring Port Channels

**Note** See the "Configuring Basic Interface Parameters" chapter for information about configuring the maximum transmission unit (MTU) for the port-channel interface. See the "Configuring Layer 3 Interfaces" chapter for information about configuring IPv4 and IPv6 addresses on the port-channel interface.

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

## Creating a Port Channel

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

**Note** When the port channel is created before the channel group, the port channel should be configured with all of the interface attributes that the member interfaces are configured with. Use the **switchport mode trunk** {*allowed vlan vlan-id* | *native vlan-id*} command to configure the members.

This is required only when the channel group members are Layer 2 ports (switchport) and trunks (switchport mode trunk).

**Note** 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*<br>**Example:**<br>`switch(config)# no interface port-channel 1` | Removes the port channel and deletes the associated channel group. |

### Before you begin

Enable LACP if you want LACP-based port channels.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **show port-channel summary**

4. **no shutdown**
5. **copy running-config startup-config**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *channel-number*<br>**Example:**<br>`switch(config)# interface port-channel 1`<br>`switch(config-if)` | 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** | **show port-channel summary**<br>**Example:**<br>`switch(config-router)# show port-channel summary` | (Optional) Displays information about the port channel. |
| **Step 4** | **no shutdown**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)# int e3/1`<br>`switch(config-if)# no shutdown` | (Optional) 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 5** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

### 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.

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

| Command | Purpose |
|---|---|
| **no channel-group**<br>**Example:**<br>`switch(config)# no channel-group` | Removes the port from the channel group. |

### Before you begin

Enable LACP if you want LACP-based port channels.

All Layer 2 member ports must run in full-duplex mode and at the same speed

## SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **switchport**
4. **switchport mode trunk**
5. **switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}
6. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
7. **show interface** *type slot/port*
8. **no shutdown**
9. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface** *type slot/port*<br>**Example:**<br>`switch(config)# interface ethernet 1/4`<br>`switch(config-if)#` | Specifies the interface that you want to add to a channel group, and enters the interface configuration mode. |
| **Step 3** | **switchport**<br>**Example:**<br>`switch(config)# switchport` | Configures the interface as a Layer 2 access port. |
| **Step 4** | **switchport mode trunk**<br>**Example:** | (Optional) Configures the interface as a Layer 2 trunk port. |

| | Command or Action | Purpose |
|---|---|---|
| | `switch(config)# switchport mode trunk` | |
| **Step 5** | **switchport trunk** {**allowed vlan** *vlan-id* \| **native** *vlan-id*}<br>**Example:**<br>`switch(config)# switchport trunk native 3`<br>`switch(config-if)#` | (Optional) Configures necessary parameters for a Layer 2 trunk port. |
| **Step 6** | **channel-group** *channel-number* [**force**] [**mode** {**on** \| **active** \| **passive**}]<br>**Example:**<br>• `switch(config-if)# channel-group 5`<br>• `switch(config-if)# channel-group 5 force` | 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**.<br>(Optional) 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.<br>**Note** The **force** option fails if the port has a QoS policy mismatch with the other members of the port channel. |
| **Step 7** | **show interface** *type slot/port*<br>**Example:**<br>`switch# show interface port channel 5` | (Optional) Displays interface information. |
| **Step 8** | **no shutdown**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)# int e3/1`<br>`switch(config-if)# no shutdown` | (Optional) 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 9** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

### 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.

**Note** Use the **no channel-group** command to remove the port from the channel group. The port reverts to its original configuration. You must reconfigure the IP addresses for this port.

| Command | Purpose |
|---|---|
| **no channel-group**<br>**Example:**<br>`switch(config)# no channel-group` | Removes the port from the channel group. |

### Before you begin

Enable LACP if you want LACP-based port channels.

Remove any IP addresses configured on the Layer 3 interface.

## SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **no switchport**
4. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
5. **show interface** *type slot/port*
6. **no shutdown**
7. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface** *type slot/port*<br>**Example:**<br>`switch(config)# interface ethernet 1/4`<br>`switch(config-if)#` | Specifies the interface that you want to add to a channel group, and enters the interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **no switchport**<br>**Example:**<br>`switch(config-if)# no switchport` | Configures the interface as a Layer 3 port. |
| **Step 4** | **channel-group** *channel-number* [**force**] [**mode** {**on** \| **active** \| **passive**}]<br>**Example:**<br>• `switch(config-if)# channel-group 5`<br>• `switch(config-if)# channel-group 5 force` | Configures the port in a channel group and sets the mode. The channel-number range is from 1 to 4096. The Cisco NX-OS software creates the port channel associated with this channel group if the port channel does not already exist.<br>(Optional) 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** | **show interface** *type slot/port*<br>**Example:**<br>`switch# show interface ethernet 1/4` | (Optional) Displays interface information. |
| **Step 6** | **no shutdown**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)# int e3/1`<br>`switch(config-if)# no shutdown` | (Optional) 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 7** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

### 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)# 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.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **bandwidth** *value*
4. **delay** *value*
5. **exit**
6. **show interface port-channel** *channel-number*
7. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *channel-number*<br>**Example:**<br>`switch(config)# interface port-channel 2`<br>`switch(config-if)#` | Specifies the port-channel interface that you want to configure, and enters the interface mode. |
| **Step 3** | **bandwidth** *value*<br>**Example:**<br>`switch(config-if)# bandwidth 60000000`<br>`switch(config-if)#` | Specifies the bandwidth, which is used for informational purposes. The range is from 1 to 3,200,000,000 kbs. The default value depends on the total active interfaces in the channel group. |
| **Step 4** | **delay** *value*<br>**Example:**<br>`switch(config-if)# delay 10000`<br>`switch(config-if)#` | 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. |
| **Step 5** | **exit**<br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits the interface mode and returns to the configuration mode. |
| **Step 6** | **show interface port-channel** *channel-number*<br>**Example:**<br>`switch# show interface port-channel 2` | (Optional) Displays interface information for the specified port channel. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **shutdown**
4. **exit**
5. **show interface port-channel** *channel-number*
6. **no shutdown**
7. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *channel-number*<br>**Example:**<br>`switch(config)# interface port-channel 2`<br>`switch(config-if)#` | Specifies the port-channel interface that you want to configure, and enters the interface mode. |
| **Step 3** | **shutdown**<br>**Example:**<br>`switch(config-if)# shutdown`<br>`switch(config-if)#` | Shuts down the interface. No traffic passes and the interface displays as administratively down. The default is no shutdown.<br>**Note** Use the **no shutdown** command to open the interface.<br>The interface displays as administratively up. If there are no operational problems, traffic passes. The default is no shutdown. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **exit**<br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits the interface mode and returns to the configuration mode. |
| **Step 5** | **show interface port-channel** *channel-number*<br>**Example:**<br>`switch(config-router)# show interface port-channel 2` | (Optional) Displays interface information for the specified port channel. |
| **Step 6** | **no shutdown**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)# int e3/1`<br>`switch(config-if)# no shutdown` | (Optional) 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 7** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **description**
4. **exit**
5. **show interface port-channel** *channel-number*
6. **copy running-config startup-config**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *channel-number*<br>**Example:**<br>`switch(config)# interface port-channel 2`<br>`switch(config-if)#` | Specifies the port-channel interface that you want to configure, and enters the interface mode. |
| **Step 3** | **description**<br>**Example:**<br>`switch(config-if)# description engineering`<br>`switch(config-if)#` | 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 this parameter before the description displays in the output. |
| **Step 4** | **exit**<br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits the interface mode and returns to the configuration mode. |
| **Step 5** | **show interface port-channel** *channel-number*<br>**Example:**<br>`switch# show interface port-channel 2` | (Optional) Displays interface information for the specified port channel. |
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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.

**SUMMARY STEPS**

1. **configure terminal**
2. **interface port-channel** *channel-number*

3. **speed** {**10** | **100** | **1000** | **auto**}
4. **duplex** {**auto** | **full** | **half**}
5. **exit**
6. **show interface port-channel** *channel-number*
7. **copy running-config startup-config**

**DETAILED STEPS**

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

**Note** Use the **no port-channel load-balance** command to restore the default load-balancing algorithm of source-dest-mac for non-IP traffic and source-dest-ip for IP traffic.

| Command | Purpose |
|---|---|
| **no port-channel load-balance**<br>**Example:**<br>`switch(config)# no port-channel load-balance` | Restores the default load-balancing algorithm. |

### Before you begin

Enable LACP if you want LACP-based port channels.

### SUMMARY STEPS

1. **configure terminal**
2. **port-channel load-balance** *method* {**dst ip** | **dst ip-gre** | **dst ip-l4port** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst l4port** | **dst mac** | **src ip** | **src ip-gre** | **src ip-l4port** | **src ip-l4port-vlan** | **src ip-vlan** | **src l4port** | **src mac** | **src-dst ip** | **src-dst ip-gre** | **src-dst ip-l4port** [**symmetric**] | **src-dst ip-l4port-vlan** | **src-dst ip-vlan** | **src-dst l4port** | **src-dst mac**} [**module** | **fex** {*fex-range* | *all*}] [ **dst inner-header** ] | **src inner-header** | **src-dst inner-header** ] [**rotate** *rotate*]
3. **port-channel load-balance** *method* {**dst ip** | **dst ip-port-vlan** | **dst ip-vlan** | **dst mac** | **dst port** | **src-dst ip** [**symmetric**] | **src-dst ip-gre** | **source-dst mac** | **source-dst port** | **src-ip port** | **src-dst ip-l4port** [**symmetric**] | **src-dst ip-l4port-vlan** [ **symmetric**] | **src-dst ip-vlan** [**symmetric**] | **src-dst l4port** | **src-dst mac** | **src-ip-port-vlan** | **src ip-vlan** | **src mac** | **src-port** | **hash-modulo** [**force**]} [**module** *module-number* | **fex** {*fex-range* | *all*}] [**asymmetric**] [**rotate** *rotate*]
4. **show port-channel load-balance**
5. **show port-channel load-balance** [**forwarding-path interface port-channel** *channel-number* |**src-ip** *src-ip* |**dst-ip** *dst-ip* |**protocol** *protocol* |**gtp-teid** *gtp-teid* |**module** *module_if*]
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `switch# configure terminal`<br>`switch(config)#` | |
| **Step 2** | **port-channel load-balance** *method* {**dst ip** \| **dst ip-gre** \| **dst ip-l4port** \| **dst ip-l4port-vlan** \| **dst ip-vlan** \| **dst l4port** \| **dst mac** \| **src ip** \| **src ip-gre** \| **src ip-l4port** \| **src ip-l4port-vlan** \| **src ip-vlan** \| **src l4port** \| **src mac** \| **src-dst ip** \| **src-dst ip-gre** \| **src-dst ip-l4port** [**symmetric**] \| **src-dst ip-l4port-vlan** \| **src-dst ip-vlan** \| **src-dst l4port** \| **src-dst mac**} [**module** \| **fex** {*fex-range* \| *all*}] [ **dst inner-header** ] \| **src inner-header** \| **src-dst inner-header** ] [**rotate** *rotate*]<br>**Example:**<br>• `switch(config)# port-channel load-balance src-dst mac`<br>`switch(config)#`<br>• `switch(config)# no port-channel load-balance src-dst mac`<br>`switch(config)#`<br>• `switch(config)# port-channel load-balance dst inner-header`<br>`switch(config)#`<br>• `switch(config)# port-channel load-balance src inner-header`<br>`switch(config)#`<br>• `switch(config)# port-channel load-balance src-dst inner-header`<br>`switch(config)#`<br>• `switch(config)# no port-channel load-balance src-dst mac asymmetric module 1`<br>`switch(config)#` | 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-l4port** for both IPv4 and IPv6, and the default for non-IP is **src-dst mac**.<br>Use the **no port-channel load-balance src-dst mac asymmetric** command to revert back to the default system settings (symmetrical).<br>**Note** If a module-based configuration already exists, it takes precedence over the default system settings.<br>Use the **no port-channel load-balance src-dst mac asymmetric module** command at module level to revert back to system level settings (symmetrical).<br>**Note** GRE inner IP headers supports source, destination and source-destination.<br>**Note** Only the following load-balancing algorithms support symmetric hashing:<br>• src-dst ip<br>• src-dst ip-l4port<br>• src-dst ip-l4port-vlan<br>• src-dst ip-vlan |
| **Step 3** | **port-channel load-balance** *method* {**dst ip** \| **dst ip-port-vlan** \| **dst ip-vlan** \| **dst mac** \| **dst port** \| **src-dst ip** [**symmetric**] \| **src-dst ip-gre** \| **source-dst mac** \| **source-dst port** \| **src-ip port** \| **src-dst ip-l4port** [**symmetric**] \| **src-dst ip-l4port-vlan** [ **symmetric**] \| **src-dst ip-vlan** [**symmetric**] \| **src-dst l4port** \| **src-dst mac** \| **src-ip-port-vlan** \| **src ip-vlan** \| **src mac** \| **src-port** \| **hash-modulo** [**force**]} [**module** *module-number* \| **fex** {*fex-range* \| *all*}] [**asymmetric**] [**rotate** *rotate*]<br>**Example:**<br>• `switch(config)# port-channel load-balance src-dst mac asymmetric`<br>`switch(config)#`<br>• `switch(config)# no port-channel load-balance src-dst mac asymmetric`<br>`switch(config)#` | 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-dest-mac**.<br>Use the **no port-channel load-balance src-dst mac asymmetric** command to revert back to the default system settings (symmetrical).<br>**Note** If a module-based configuration already exists, it takes precedence over the default system settings.<br>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 |
|---|---|---|
| | • `switch(config)# no port-channel load-balance src-dst mac asymmetric module 1`<br>`switch(config)#` | **Note** Only the following load-balancing algorithms support symmetric hashing:<br>• src-dst ip<br>• src-dst ip-l4port<br>• src-dst ip-l4port-vlan<br>• src-dst ip-vlan |
| **Step 4** | **show port-channel load-balance**<br>**Example:**<br>`switch(config-router)# show port-channel load-balance` | (Optional) Displays the port-channel load-balancing algorithm. |
| **Step 5** | **show port-channel load-balance** [**forwarding-path interface port-channel** *channel-number* \|**src-ip** *src-ip* \|**dst-ip** *dst-ip* \|**protocol** *protocol* \|**gtp-teid** *gtp-teid* \|**module** *module_if*]<br>**Example:**<br>`switch# show port-channel load-balance forwarding-path`<br>`load-balance` | (Optional) Identifies the port in the EtherChannel interface that forwards the packet. |
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

### 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-port module 5
```

# Configuring Load Balancing using Port Channels for MPLS Tagged Traffic

### Before you begin

- The configurations port-channel load-balance and mpls load-sharing options for mpls cannot co-exist.
- For MPLS tagged L2 traffic, you can use the port-channel load-balance configuration with mpls options.
- Configuration of feature-set mpls and port-channel load-balance with mpls options are mutually exclusive.
- The port-channel load-balance with mpls option feature cannot co-exist with vxlan feature.

- The following are the guidelines and limitations for the port-channel load-balance with `<non-mpls options>` with mpls label-ip:
  - Both SRC and DST L2 addresses fields are overloaded with all 4 labels stack on MPLS in ASIC. SRC-MAC is overloaded with top 3 labels and DST-MAC is overloaded with remaining 4th label. Enabling this feature can omit SRC and DST L2 MAC fields of the MPLS IP packet for hashing.
    - If the non mpls option which has impact on SRC or DST L2 address fields. It impacts label stack hash calculation.

- The following are the guidelines and limitations for the port-channel load-balance with `<non-mpls options>` with mpls label-only:
  - Both SRC and DST IP address fields are overloaded with MPLS label stack (9 labels) in ASIC (i.e. SRC-IP is overloaded with top 5 labels & DST-IP is overloaded with botom 4 labels). So, turning on this variant in general could ignore SRC & DST IP fields of the MPLS packet for hashing.
  - If the <non-mpls options> contain 'SRC IP' only variant, then only top 5 MPLS labels (for label stack size of 9) would be considered for hashing.
  - If the <non-mpls options> contain only DST IP variant, it considers only botom 4 MPLS labels for hashing (for the MPLS label of stack size 9). For an example, MPLS packet which has only 5 labels, none of these labels are considered for hashing. If you have MPLS packet with 7 labels, only botom 2 labels is considered for hashing.
  - If the <non-mpls options> contain doesn't have both SRC and DST IP fields, none of the labels are considered for hashing.
  - L4 SRC and DST ports would not be considered for hashing.

## SUMMARY STEPS

1. **configure terminal**
2. **port-channel load-balance src-dst ip-l4port mpls** {**label-ip**|**label-only**}
3. (Optional) **show port-channel load-balance**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **port-channel load-balance src-dst ip-l4port mpls** {**label-ip**|**label-only**}<br>**Example:**<br>`switch(config)# port-channel load-balance src-dst ip-l4port mpls label-ip` | Specifies the load-balancing for MPLS using port-channel.<br>label-ip – Specifies load sharing based on MPLS label and IP.<br>label-only - Specific load sharing based on MPLS label only. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | (Optional) **show port-channel load-balance**<br>**Example:**<br>`switch(config)# show port-channel load-balance` | Displays the port-channel load-balancing algorithm. |

### Example

The following is an example of load-balance configuration with mpls option:

```
switch# show port-channel load-balance
System config:
Non-IP: src-dst mac
IP: src-dst ip-l4port mpls label-ip rotate 0
Port Channel Load-Balancing Configura□□on for all modules:
Module 1:
Non-IP: src-dst mac
IP: src-dst ip-l4port mpls label-ip rotate 0
```

# Configuring Inner Header GTP

Follow this procedure to enable/disable the GTP inner-header hashing:

### SUMMARY STEPS

1. **configure terminal**
2. **[no] port-channel load-balance src-dst inner-header gtp [symmetric]**
3. **[no] hash-mode {gtp-inner-v4 | gtp-inner-v6}**
4. **show port-channel load-balance**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **[no] port-channel load-balance src-dst inner-header gtp [symmetric]**<br>**Example:**<br>`switch(config)# port-channel load-balance src-dst inner-header gtp`<br>`switch(config)#` | Enables/disables the GTP inner-header based load balancing.<br>This global command sets up the UDF tcam for both IPv4/IPv6 GTP packets.<br>The symmetric load-balancing will be done using **source-ip**, **dest-ip**, **source-port** and **dest-ip** inner IP header fields. Default is asymmetric hashing<br>The port can be a physical port or Port-channel. The actual load balancing will happen on egress port. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **[no] hash-mode {gtp-inner-v4 \| gtp-inner-v6}**<br>**Example:**<br>for IPv4<br>`switch(config)# hash-mode gtp-inner-v4`<br>`switch(config)#`<br>For IPv6<br>`switch(config)# hash-mode gtp-inner-v6`<br>`switch(config)#` | Enables/disables the hashing for IPv4/IPv6 GTP packets. |
| **Step 4** | **show port-channel load-balance**<br>**Example:**<br>`switch(config)# show port-channel load-balance`<br>`switch(config)#` | Displays the port-channel load-balancing algorithm. |

# 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.

### SUMMARY STEPS

1. **configure terminal**
2. **feature lacp**
3. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **feature lacp**<br>**Example:**<br>`switch(config)# feature lacp` | Enables LACP on the device. |
| **Step 3** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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.

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **channel-group** *number* **mode** {**active** | **on** | **passive**}
4. **show port-channel summary**
5. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface** *type slot/port*<br>**Example:**<br>`switch(config)# interface ethernet 1/4`<br>`switch(config-if)#` | Specifies the interface that you want to add to a channel group, and enters the interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **channel-group** *number* **mode** {**active** \| **on** \| **passive**}<br>**Example:**<br>`switch(config-if)# channel-group 5 mode active` | 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.<br>When you run port channels with no associated aggregation protocol, the port-channel mode is always on.<br>The default port-channel mode is **on**. |
| **Step 4** | **show port-channel summary**<br>**Example:**<br>`switch(config-if)# show port-channel summary` | (Optional) Displays summary information about the port channels. |
| **Step 5** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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

You can configure the LACP minimum links feature. Although minimum links and maxbundles work only in LACP, you can enter the CLI commands for these features for non-LACP port channels, but these commands are nonoperational.

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

| Command | Purpose |
|---|---|
| **no lacp min-links**<br>**Example:**<br>`switch(config)# no lacp min-links` | Restores the default port-channel minimum links configuration. |

### Before you begin

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp min-links** *number*
4. **show running-config interface port-channel** *number*

### DETAILED STEPS

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

#### Example

This example shows how to configure the minimum number of port-channel member interfaces to be up/active for the port-channel to be up/active:

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# lacp min-links 3
```

# Configuring the LACP Port-Channel MaxBundle

You can configure the LACP maxbundle feature. Although minimum links and maxbundles work only in LACP, you can enter the CLI commands for these features for non-LACP port channels, but these commands are nonoperational.

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

| Command | Purpose |
|---|---|
| **no lacp max-bundle**<br>**Example:**<br>`switch(config)# no lacp max-bundle` | Restores the default port-channel max-bundle configuration. |

### Before you begin

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

## SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp max-bundle** *number*
4. **show running-config interface port-channel** *number*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *number*<br>**Example:**<br>`switch(config)# interface port-channel 3`<br>`switch(config-if)#` | Specifies the interface to configure, and enters the interface configuration mode. |
| **Step 3** | **lacp max-bundle** *number*<br>**Example:**<br>`switch(config-if)# lacp max-bundle` | Specifies the port-channel interface to configure max-bundle.<br>The default value for the port-channel max-bundle is 16. The allowed range is from 1 to 32.<br>**Note** Even if the default value is 16, the number of active members in a port channel is the minimum of the pc_max_links_config and pc_max_active_members that is allowed in the port channel. |
| **Step 4** | **show running-config interface port-channel** *number*<br>**Example:**<br>`switch(config-if)# show running-config interface port-channel 3` | (Optional) Displays the port-channel max-bundle configuration. |

### Example

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

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# 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. HA and SSO are not supported when the LACP fast rate timer is configured.

**Note** Configuring **lacp rate fast** is not recommended on the vPC Peer-Links. When **lacp rate fast** is configured on the vPC Peer-Link member interfaces, an alert is displayed in the syslog messages only when the LACP logging level is set to 5.

### Before you begin

Ensure that you have enabled the LACP feature.

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **lacp rate fast**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface** *type slot/port*<br>**Example:**<br>`switch(config)# interface ethernet 1/4`<br>`switch(config-if)#` | Specifies the interface to configure and enters the interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **lacp rate fast**<br>**Example:**<br>`switch(config-if)# lacp rate fast` | Configures the fast rate (one second) at which LACP control packets are sent to an LACP-supported interface.<br>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.

### Before you begin

Enable LACP.

### SUMMARY STEPS

1. **configure terminal**
2. **lacp system-priority** *priority*
3. **show lacp system-identifier**
4. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **lacp system-priority** *priority*<br>**Example:**<br>`switch(config)# lacp system-priority 40000` | 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.<br>**Note** Each VDC has a different LACP system ID because the software adds the MAC address to this configured value. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **show lacp system-identifier**<br>**Example:**<br>`switch(config-if)# show lacp system-identifier` | (Optional) Displays the LACP system identifier. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup 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.

### Before you begin

Enable LACP.

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **lacp port-priority** *priority*
4. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface** *type slot/port*<br>**Example:**<br>`switch(config)# interface ethernet 1/4`<br>`switch(config-if)#` | Specifies the interface that you want to add to a channel group, and enters the interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **lacp port-priority** *priority*<br>**Example:**<br>`switch(config-if)# lacp port-priority 40000` | Configures the port priority for use with LACP. Valid values are from 1 through 65535, and higher numbers have a lower priority. The default value is 32768. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config-if)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup 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
```

# Configuring LACP System MAC and Role

You can configure the MAC address used by the LACP for protocol exchanges and the optional role. By default, the LACP uses the VDC MAC address. By default, the role is primary.

Use the **no lacp system-mac** command to make LACP use the default (VDC) MAC address and default role.

This procedure is supported on the Cisco Nexus 9336C-FX2, 93300YC-FX2, and 93240YC-FX2-Z switches.

### Before you begin

LACP must be enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **lacp system-mac** *mac-address* **role** *role-value*
3. (Optional) **show lacp system-identifier**
4. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal` | Enter global configuration mode. |
| **Step 2** | **lacp system-mac** *mac-address* **role** *role-value*<br>**Example:** | Specifies the MAC address to use in the LACP protocol exchanges. The role is optional. Primary is the default. |

| | Command or Action | Purpose |
|---|---|---|
| | `switch(config)# lacp system-mac 000a.000b.000c role primary`<br>`switch(config)# lacp system-mac 000a.000b.000c role secondary` | |
| **Step 3** | (Optional) **show lacp system-identifier**<br>**Example:**<br>`switch(config)# show lacp system-identifier` | Displays the configured MAC address. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

### Example

The following example shows how to configure the role of a switch as primary.

```
Switch1# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch1# sh run  | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role primary
```

The following example shows how to configure the role of a switch as secondary.

```
Switch2# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch2# sh run | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role secondary
```

# 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

Enable LACP.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**

4. **no lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

**DETAILED STEPS**

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

## Reenabling LACP Graceful Convergence

If the default LACP graceful convergence is once again required, you can reenable convergence.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

### DETAILED STEPS

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

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.

### Before you begin

Enable LACP.

## SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **no lacp suspend-individual**
4. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *number*<br>**Example:**<br>`switch(config)# interface port-channel 1`<br>`switch(config-if)#` | Specifies the port channel interface to configure and enters the interface configuration mode. |
| **Step 3** | **no lacp suspend-individual**<br>**Example:**<br>`switch(config-if)# no lacp suspend-individual` | Disables LACP individual port suspension behavior on the port channel.<br>**Note** When you have this configuration, as well as multiple members configured as part of the same port channel interface, then if the members do not receive any LACP PDUs from the partner, all of them will transition to Individual (I) state. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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)# no lacp suspend-individual
```

# Disabling LACP Suspend Individual PXE

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 pxe** command on edge ports.

### Before you begin

Enable LACP.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **no lacp suspend-individual pxe**
4. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *number*<br>**Example:**<br>`switch(config)# interface port-channel 1`<br>`switch(config-if)#` | Specifies the port channel interface to configure and enters the interface configuration mode. |
| **Step 3** | **no lacp suspend-individual pxe**<br>**Example:** | Disables LACP individual port suspension behavior on the port channel. |

| | Command or Action | Purpose |
|---|---|---|
| | `switch(config-if)# no lacp suspend-individual pxe` | **Note** • When you have this configuration, as well as multiple members configured as part of the same port channel interface, then if the members do not receive any LACP PDUs from the partner, only one port will transition to the Individual (I) state and the rest ports will go to Suspended (S) state. If any port comes up in the P state, there will be no port in I state. Note that across vPC peers, there will be one port in the I state.<br>• If the peer device hashes traffic onto a suspended port, the traffic will get dropped. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) 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)# no lacp suspend-individual pxe
```

# Reenabling LACP Suspend Individual

You can reenable the default LACP individual port suspension.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp suspend-individualpxe**
4. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **interface port-channel** *number*<br>**Example:**<br>`switch(config)# interface port-channel 1`<br>`switch(config-if)#` | Specifies the port channel interface to configure and enters the interface configuration mode. |
| **Step 3** | **lacp suspend-individualpxe**<br>**Example:**<br>`switch(config-if)# lacp suspend-individual` | Enables LACP individual port suspension behavior on the port channel.<br>**Note** Though you configure lacp suspend-individual pxe, the show running command will only show lacp suspend-individual and not lacp suspend individual pxe. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

### Example

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

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

switch(config-if)# lacp suspend-individualpxe
```

# Configuring Delayed LACP

The delayed LACP feature enables one port channel member, the delayed LACP port, to come up first as a member of a regular port channel before LACP PDUs are received. You configure the delayed LACP feature using the **lacp mode delay**command on a port channel followed by configuring the LACP port priority on a one member port of the port channel.

You configure the delayed LACP with the **lacp mode delay**command followed by configuring the LACP port priority. (7.0(3)I1(2) and later)

**Note** You cannot configure delayed LACP, when the LACP individual port suspension behavior (**no lacp suspend-individual**) has already been configured. Similarly, the LACP individual port suspension behavior cannot be configured when the delayed LACP is already configured.

**Note** Delayed LACP is not supported on Layer 3 port channels, FEX modules, or the Cisco Nexus 9500 Series switch.

**Note** When **no lacp suspend-individual** and the delayed LACP feature are configured on the same port, the non-delayed LACP ports belonging to the port are in individual state. When LACP is established, the member should be moved to up state.

As a best practice, do not use **no lacp suspend-individual** together with the delayed LACP feature on the same port channel.

**Note** For vPC, you must enable the delayed LACP on both vPC switches.

**Note** For vPC, when the delayed LACP port is on the primary switch and the primary switch fails to boot, you need to remove the vPC configuration on the delayed LACP port-channel of the acting primary switch and flap the port-channel for a new port to be chosen as the delayed LACP port on the existing port-channel.

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp mode delay**
4. **lacp port-priority** *number*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **interface port-channel** *number* | Specifies the port channel interface to configure and enters the interface configuration mode. |
| **Step 3** | **lacp mode delay** | Enables delayed LACP.<br>**Note** To disable delayed LACP, use the **no lacp mode delay** command.<br>Otherwise, the delayed LACP port stays in delayed LACP mode until the first LACP PDU arrives.<br>Complete the configuration of the delayed LACP by configuring the LACP port priority. See the "Configuring the LACP Port Priority" section for details.<br>The priority of a LACP port determines the election of the delayed LACP port. The port with the lowest numerical priority is elected.<br>When two or more ports have the same best priority, the VDC system MAC is used to determine which vPC is used. |

| | Command or Action | Purpose |
|---|---|---|
| | | Then within a non-vPC switch or the elected vPC switch, the smallest of the ethernet port names is used.<br>When the delayed LACP feature is configured and made effective with a port channel flap, the delayed LACP port operates as a member of a regular port channel, allowing data to be exchanged between the server and switch. After receiving the first LACP PDU, the delayed LACP port transitions from a regular port member to a LACP port member.<br>**Note** The election of the delayed LACP port is not complete or effective until the port channel flaps on the switch or at a remote server. |
| **Step 4** | **lacp port-priority** *number* | Specifies the LACP port-priority.<br>The priority of a LACP port determines the election of the delayed LACP port. The port with the lowest numerical priority is elected.<br>When two or more ports have the same priority, the VDC system MAC address is used to determine which vPC is selected. If that criterion cannot determine the election, then the ethernet name of the port determines the election of the LACP port.<br>**Note** The election of the delayed LACP port is not complete or effective until the port-channel flaps on the switch or at a remote server. |

### Example

The following example configures delayed LACP.

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# lacp mode delay


switch# config terminal
switch(config)# interface ethernet 1/1
switch(config-if)# lacp port-priority 1
switch(config-if)# channel-group 1 mode active
```

The following example disables delayed LACP.

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# no lacp mode delay
```

# Configuring Port Channel Hash Distribution

Cisco NX-OS supports the adaptive and fixed hash distribution configuration for 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

### SUMMARY STEPS

1. **configure terminal**
2. **no port-channel hash-distribution** {**adaptive** | **fixed**}
3. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **no port-channel hash-distribution** {**adaptive** | **fixed**}<br>**Example:**<br>`switch(config)# port-channel hash-distribution adaptive`<br>`switch(config)#` | Specifies the port-channel hash distribution at the global level.<br>The default is adaptive mode.<br>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 3** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

#### Example

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

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** {*channel-number* | *range*}
3. **no port-channel port hash-distribution** {**adaptive** | **fixed**}
4. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface port-channel** {*channel-number* | *range*}<br>**Example:**<br>`switch# interface port-channel 4`<br>`switch(config-if)#` | Specifies the interface to configure, and enters the interface configuration mode. |
| **Step 3** | **no port-channel port hash-distribution** {**adaptive** | **fixed**}<br>**Example:**<br>`switch(config-if)# port-channel port hash-distribution adaptive`<br>`switch(config-if)` | Specifies the port-channel hash distribution at the port channel level.<br>There is no default.<br>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** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Copies the running configuration to the startup configuration. |

#### Example

This example shows how to configure hash distribution as a global-level command:

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

# Enabling ECMP Resilient Hashing

Resilient ECMP ensures minimal impact to the existing flows when members are deleted from an ECMP group. This is achieved by replicating the existing members in a round-robin fashion at the indices that were previously occupied by the deleted members.

### SUMMARY STEPS

1. **configure terminal**
2. **hardware profile ecmp resilient**
3. **copy running-config startup-config**
4. **reload**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **hardware profile ecmp resilient**<br>**Example:**<br>`switch(config)# hardware profile ecmp resilient` | Enables ECMP resilient hashing and displays the following: **Warning: The command will take effect after next reload.**<br>**Note** This command is not supported on Cisco Nexus 9808/9804 platform switches. |
| **Step 3** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | Copies the running configuration to the startup configuration. |
| **Step 4** | **reload**<br>**Example:**<br>`switch(config)# reload` | Reboots the switch. |

# Disabling ECMP Resilient Hashing

### Before you begin

ECMP resilient hashing is enabled.

### SUMMARY STEPS

1. **configure terminal**
2. **no hardware profile ecmp resilient**
3. **copy running-config startup-config**
4. **reload**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `switch# configure terminal` | |
| **Step 2** | **no hardware profile ecmp resilient**<br>**Example:**<br>`switch(config)# no hardware profile ecmp resilient` | Disables ECMP resilient hashing and displays the following: **Warning: The command will take effect after next reload.** |
| **Step 3** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | Copies the running configuration to the startup configuration. |
| **Step 4** | **reload**<br>**Example:**<br>`switch(config)# reload` | Reboots the switch. |

# Configuring ECMP Load Balancing

To configure the ECMP load-sharing algorithm, use the following command in global configuration mode:

### Before you begin

### SUMMARY STEPS

1. **ip load-sharing address** {**destination port destination** | **source-destination** [**port source-destination** | **gre** | **gtpu** | **ipv6-flowlabel** | **ttl** | **udf offset** *offset* **length** *length* | **symmetricinner** *allgreheader*]} [**universal-id** *seed*] [**rotate** *rotate*] [**concatenation**]
2. (Optional) **show ip load-sharing**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **ip load-sharing address** {**destination port destination** \| **source-destination** [**port source-destination** \| **gre** \| **gtpu** \| **ipv6-flowlabel** \| **ttl** \| **udf offset** *offset* **length** *length* \| **symmetricinner** *allgreheader*]} [**universal-id** *seed*] [**rotate** *rotate*] [**concatenation**]<br>**Example:**<br>`ip load-sharing address source-destination`<br>**Example:**<br>`switch(config)# ip load-sharing address source-destination ipv6-flowlabel`<br>**Example:**<br>`switch(config)# ip load-sharing address source-destination ttl`<br>**Example:** | Configures the ECMP load-sharing algorithm for data traffic.<br>• The **gre** option specifies the source-destination value for the Generic Routing Encapsulation (GRE) key.<br>• The **gtpu** option specifies the GPRS Tunneling Protocol (GTP) tunnel endpoint identifier (TEID) value for the port source-destination.<br>• The **ipv6-flowlabel** option includes the IPv6 flow label for computing ECMP hashing. It ensures that traffic flows are distributed on all links based on different flow label values. Enabling or disabling this option also enables or disables it for port-channel load-balancing if Layer 4 parameters are enabled using the **port-channel load-balance** command. Only the following devices support this option: |

| Command or Action | Purpose |
| --- | --- |
| `switch(config)# ip load-sharing address source-destination udf offset 8 length 8`<br>**Example:**<br>`switch(config)# [no] ip load-sharing address source-destination port source-destination symmetric`<br>**Example:**<br>`switch(config)# ip load-sharing address source-destination port source-destination inner [all\|greheader]` | • Cisco Nexus 9364C and 9300-EX/FX/FX2 platform switches<br>• Cisco Nexus 9500 platform switches with X9700-EX/FX line cards and FM-E2 fabric modules in all routing modes<br>• Cisco Nexus 9500 platform switches with X9700-EX/FX line cards and FM-E fabric modules in non-hierarchical routing modes where IPv6 routes are programmed in the line card<br>• Beginning with Cisco NX-OS Release 9.3(5), Cisco Nexus N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C9364C-GX switches support this option.<br>• The **ttl** option includes time-to-live information for computing ECMP hashing. It ensures that traffic flows are distributed on all links based on different TTL values. For IPv4 flows, it is based on ttl values. For IPv6 flows, it is based on hop limit. Enabling or disabling this option also enables or disables it for port-channel load-balancing if Layer 4 parameters are enabled using the **port-channel load-balance** command. Only Cisco Nexus 9364C and 9300-EX/FX/FX2 platform switches support this option. Beginning with Cisco NX-OS Release 9.3(5), Cisco Nexus N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C9364C-GX switches support this option.<br>• The **udf** option includes the user-defined field for computing ECMP hashing. You can configure the offset base and the length of the UDF field (in bits). The range for the offset base is from 0 to 127 bytes. The range for the length of the UDF field is from 1 to 32 bits. Enabling or disabling this option also enables or disables it for port-channel load-balancing if Layer 4 parameters are enabled using the **port-channel load-balance** command. Only Cisco Nexus 9364C and 9300-EX/FX/FX2 platform switches support this option. Beginning with Cisco NX-OS Release 9.3(5), Cisco Nexus N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C9364C-GX switches support this option.<br>• The **symmetric** option enables symmetric hashing globally. To disable ECMP symmetric hashing, use the **no** keyword in the command. You must execute this command in global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** Ensure that the configured **universal-id** seed value is consistent across the nodes in the path of ECMP symmetric hashing for symmetric hashing to work effectively.<br><br>• The **inner** option enables inner header based hashing for GRE traffic globally. To disable inner header based hashing, use the **no** keyword in the command. You must execute this command in global configuration mode.<br>  • **all** : Configuring this option for GRE encapsulated packets starts using inner headers to hash onto a path in ECMP, which may impact other encapsulation types as well. This is supported on Cisco Nexus 9364C and 9300-EX/FX/FX2 platform switches; and Cisco Nexus 9500 platform switches with X9700-EX/FX line cards.<br>  • **greheader** : Configuring this option only for GRE encapsulated packets, starts using inner headers to hash onto a path in ECMP. This is supported on Cisco Nexus 9364C and 9300-FX/FX2 platform switches; and Cisco Nexus 9500 platform switches with X9700-FX line cards.<br><br>The following options are available for all IP load sharing configurations:<br>• The **universal-id** option sets the random seed for the hash algorithm and shifts the flow from one link to another.<br>You do not need to configure the universal ID. Cisco NX-OS chooses the universal ID if you do not configure it. The *universal-id* range is from 1 to 4294967295.<br>• The **rotate** option causes the hash algorithm to rotate the link picking selection so that it does not continually choose the same link across all nodes in the network. It does so by influencing the bit pattern for the hash algorithm. This option shifts the flow from one link to another and load balances the already load-balanced (polarized) traffic from the first ECMP level across multiple links.<br>If you specify a *rotate* value, the 64-bit stream is interpreted starting from that bit position in a cyclic rotation. The *rotate* range is from 1 to 63, and the default is 32. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** With multi-tier Layer 3 topology, polarization is possible. To avoid polarization, use a different rotate bit at each tier of the topology.<br>**Note** To configure a rotation value for port channels, use the **port-channel load-balance src-dst ip-l4port rotate** *rotate* command.<br>• The **concatenation** option ties together the hash tag values for ECMP and the hash tag values for port channels in order to use a stronger 64-bit hash. If you do not use this option, you can control ECMP load-balancing and port-channel load-balancing independently. The default is disabled. |
| **Step 2** | (Optional) **show ip load-sharing**<br>**Example:**<br>`switch(config)# show ip load-sharing address source-destination` | Displays the ECMP load-sharing algorithm for data traffic. |

# Verifying the ECMP Resilient Hashing Configuration

To display ECMP Resilient Hashing configuration information, perform one of the following tasks:

| Command | Purpose |
|---|---|
| `switch(config)# show running-config \| grep "hardware profile ecmp resilient`<br>`hardware profile ecmp resilient`<br>`switch(config)#` | Displays the enabled status. |
| `switch(config)# show running-config \| grep "hardware profile ecmp resilient`<br>`switch(config)#` | Displays the disabled status. |

# Verifying the Port-Channel Configuration

To display port-channel configuration information, perform one of the following tasks:

| 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**}} | Sets three different sampling intervals to bit-rate and packet-rate statistics. |

| Command | Purpose |
|---|---|
| **show port-channel compatibility-parameters** | Displays the parameters that must be the same among the member ports in order to join a port channel. |
| **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.<br>Beginning with Cisco NX-OS Release 10.3(2)F, the GTP inner-header based load balancing option is supported on Cisco Nexus 9300-FX/FX2 ToR switches. |
| **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. |

# Monitoring the Port-Channel Interface Configuration

Use the following commands to display port-channel interface configuration information.

| 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**}} | Sets three different sampling intervals to bit-rate and packet-rate statistics. |
| **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. |

| Command | Purpose |
|---|---|
| **show interface counters errors** [**module** *module*] | Displays information about the number of error packets. |
| **show lacp counters** | Displays statistics for LACP. |

# Example Configurations 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

| Related Topic | Document Title |
|---|---|
| System management | *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* |
| High availability | *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide* |
| Licensing | *Cisco NX-OS Licensing Guide* |