



Port Channels and Trunking

This chapter describes how to identify and resolve problems related to port channels and trunking. This chapter contains the following sections:

- [Information About Port Channels and Trunking, on page 1](#)
- [Guidelines for Troubleshooting Asymmetric Port Channels, on page 2](#)
- [Initial Troubleshooting Checklist, on page 2](#)
- [Problems with Port Channels and Trunking, on page 3](#)
- [Port Channels and Trunking Troubleshooting Commands, on page 5](#)

Information About Port Channels and Trunking

Port Channel Overview

Port channels aggregate multiple physical interfaces into one logical interface to provide higher bandwidth, load balancing, and link redundancy.

A port channel performs the following functions:

- Increases the aggregate bandwidth on a link by distributing traffic among all functional links in the channel.
- Balances load across multiple links and maintains optimum bandwidth usage.
- Provides high availability. If one link fails, traffic carried previously on this link is switched to the remaining links. If a link goes down in a port channel, the upper protocol is not aware of it. To the upper protocol, the link is still there although the bandwidth is diminished. The MAC address tables are not affected by link failures.

Port Channel Restrictions

The following are port channel restrictions:

- Port channels do not support ACLs.
- Port channels do not support NetFlow.

Trunking Overview

Trunking, also known as VLAN trunking, enables interconnected ports to transmit and receive frames through more than one VLAN over the same physical link. Trunking and port channels function as follows:

- Port channels enable several physical links to be combined into one aggregated logical link.
- Trunking enables a link to carry (trunk) the traffic for multiple VLANs.

Guidelines for Troubleshooting Asymmetric Port Channels

When you are troubleshooting asymmetric port channels, follow these guidelines:

- Use APC when you want to configure a port channel whose members are connected to two different upstream switches.
- APC depends on Cisco Discovery Protocol (CDP). Make sure CDP is enabled on the VSM and upstream switches.
- Physical ports within an APC get assigned subgroup IDs based on the CDP information received from upstream switches.
- You can manually configure subgroup IDs in interface configuration submode.
- Make sure that you configure subgroup CDP either with a port profile or on the port channel interface.
- Ports in APC come up only when they are assigned subgroup IDs manually or through CDP.
- Enter the **show cdp neighbors** command on the VSM and check the output.
- After the ports come up, check that ports are put in the correct subgroups by entering the **module vem module-number execute vemcmd show pc** command on the VEM.
- Use the **debug port-channel trace** command to collect information.

Initial Troubleshooting Checklist

Use the following checklist to begin troubleshooting port channel and trunking issues:

Checklist	Completion Status
Use the show port-channel compatibility-parameters command to determine the port channel requirements.	
Ensure that all interfaces in the port channel have the same destination device for Link Aggregation Control Protocol (LACP) channels. By using the Asymmetric Port Channel (APC) feature in Cisco Nexus 1000V, the ports in ON mode channel can be connected to two different destination devices. Note APC is supported only on mode channels. It is not supported for LACP channels.	
Verify that either side of a port channel is connected to the same number of interfaces.	
Verify that each interface is connected to the same type of interface on the other side.	
Verify that all required VLANs on a trunk port are in the allowed VLAN list.	
Verify that all the members trying to form a port channel are on the same module.	

Checklist	Completion Status
Verify that the port channel configuration is present in the profile used by the physical ports.	
Configure APC if the ports are connected to different upstream switches.	
If the upstream switch does not support port channels, make sure that you configure APC in the profile. In addition, make sure that you have no more than two ports in the APC.	

Problems with Port Channels and Trunking

A Port Channel Cannot be Created

Possible Cause	Solution
The maximum number of port channels has been reached for the system.	Enter the show port-channel summary command to verify the number of port channels already configured. You can have a maximum of 256 port channels on Cisco Nexus 1000V.

Newly-Added Interface Does Not Come Online In a Port Channel

Possible Cause	Solution
The port channel mode is on.	<ol style="list-style-type: none"> 1. Make sure that you have the port channel configuration in the port profile (port group) used by that interface. 2. Check if a port channel is already present on the module that is using the same port profile. If there is, check the running configuration on the port channel and the newly added interface. The interface does not come up if the port channel configurations are different. 3. If the port channel configuration is different, apply the difference on the newly added interface. Remove the port and then add it back.
Interface parameters are not compatible with those of the existing port.	To force the physical interface to take on the parameters of the port channel, see Forcing Port Channel Characteristics onto an Interface, on page 3 . Use this procedure only if you want to configure the port channel manually and not through the port profile.

Forcing Port Channel Characteristics onto an Interface

You can force the physical interface to take on the characteristics of the port channel. Use this procedure only if you want to configure the port channel manually and not through the port profile.

Before you begin

- Log in to the CLI in configuration mode.

- Make sure that the forced interface has the same speed, duplex, and flow control settings as the channel group.

Procedure

Step 1 Enter the interface configuration mode using the **interface ethernet slot/port** command.

You are placed into interface configuration mode.

Example:

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

Step 2 Force the physical interface with an incompatible configuration to join the channel group using the **channel-group channel-number force** command.

The physical interface with an incompatible configuration is forced to join the channel group.

Example:

```
switch(config-if)# channel-group 5 force
switch(config-if)
```

Verifying a Port Channel Configuration

You can debug port channels configured through a port profile.

Before you begin

Log in to the CLI in configuration mode.

Procedure

Step 1 Verify that you have configured a port channel in the profile.

```
switch# show port-profile name profile-name
```

Step 2 Display summary port channel information.

```
switch# show port-channel summary
```

Step 3 Debug the port channel configuration.

```
switch# debug port-channel trace
```

VLAN Traffic Does Not Traverse Trunk

Possible Cause	Solution
A VLAN is not in the allowed VLAN list.	Add the VLAN to the allowed VLAN list. Use the switchport trunk allowed vlan add <i>vlan-id</i> command in the profile used by the interface.

Port Channels and Trunking Troubleshooting Commands

The following commands help you to troubleshoot port channels and trunking:

- **show port-channel summary**
- **show port-channel internal event-history interface port-channel *channel-number***
- **show port-channel internal event-history interface ethernet *slot-number***
- **show system internal ethpm event-history interface port-channel *channel-number***
- **show system internal ethpm event-history interface ethernet *slot-number***
- **show vlan internal trunk interface ethernet *slot-number***
- **show vlan internal trunk interface port-channel *channel-number***
- **debug port-channel error**
- **module vem *module-number* execute vemcmd show port**
- **module vem *module-number* execute vemcmd show pc**
- **module vem *module-number* execute vemcmd show trunk**

