This article describes how to do basic troubleshooting of virtual Port Channel(vPC) problems on a Cisco Nexus 7000 NX-OS device.

Guide Contents
Troubleshooting Overview
Troubleshooting Installs, Upgrades, and Reboots
Troubleshooting Licensing
Troubleshooting VDCs
Troubleshooting CFS
Troubleshooting Ports
Troubleshooting vPCs {this section}
Troubleshooting VLANs
Troubleshooting STP
Troubleshooting Routing
Troubleshooting Unicast Traffic
Troubleshooting WCCP
Troubleshooting Memory
Troubleshooting FCoE
Troubleshooting Packet Flow Issues
Before Contacting Technical Support
Troubleshooting Tools and Methodology

Contents

Information About Troubleshooting vPCs

A vPC allows links that are physically connected to two different Cisco Nexus 7000 Series devices to appear as a single port channel by a third device.

See the Configuring vPC chapter in the Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide for more information on vPCs.

Initial Troubleshooting Checklist

Begin troubleshooting vPC issues by checking the following issues first:

Checklist	Check off
Verify that all vPC interfaces in a vPC domain are configured in the same virtual device context (VDC).	
Verify that you have a separate vPC peer-link and peer-keepalive link infrastructure for each VDC deployed.	
Is the vPC keepalive link mapped to a separate vrf? If not, it will be mapped to the management vrf by default. In this case, do you have a management switch connect to the management ports on both vPC peer devices?	
Verify that the vPC peer-link is configured on a N7K-M132XP-12. It is recommended to have at least two N7K-M132XP-12 for redundancy.	
Verify that both the source and destination IP addresses used for the peer-keepalive messages are reachable from the VRF associated with the vPC peer-keepalive link.	
Verify that the peer-keepalive link is up or the vPC peer-link will not come up.	
Verify that the vPC peer-link is configured as a Layer 2 Port Channel trunk which only allows vPC VLANs.	
Verify that the vPC number that you assigned to the port channel that connects to the downstream device from the vPC peer device is identical on both vPC peer devices.	
If you manually configured the system priority, verify that you assigned the same priority value on both vPC peer devices.	
Check the **show vpc consistency-parameters** command to verify that both vPC peer devices have identical type-1 parameters.	
Verify that the primary vPC is the primary STP root and the secondary vPC is the secondary STP root.	

Verifying vPCs Using the CLI

To verify vPCs using the CLI, follow these steps:

1. Use the **show running-config vpc** command to verify the vPC configuration.

2. Use the **show vpc** command to check the status of vPC.

3. Use the **show vpc peer-keepalive** command to check the status of the vPC peer-keepalive link.

4. Use the **show vpc consistency-parameters** command to verify that both the vPC peers have the identical type-1 parameters.

5. Use the **show port-channel summary** command toverify the members in the port channel are mapped to the vPC.

6. Use the **show cfs status** commands to verify that distribution over Ethernet is enabled.

7. If you enable STP, use the **show spanning-tree** command on both sides of the vPC peer link to verify that the following STP parameters are identical:

- BPDU Filter
- BPDU Guard
- Cost
- Link type
- Priority
- VLANs (PVRST+)

Received Type 1 Configuration Element Mismatch

You may have a problem where you cannot bring up a vPC link because of a type 1 configuration element mismatch.

Symptom	Possible Cause	Solution
Received a type 1 configuration element mismatch.	The vPC peer ports or membership ports do not have identical configurations.	Use the **show vpc consistency-parameters interface** command to determine where the configuration mismatch occurs.

Example: show vpc consistency-parameters Command Output

This example shows how to display the vPC consistency parameters on a port channel:

```
switch# show vpc consistency-parameters interface po 10
   Legend:
       Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value
-------------               ----  ---------------------- -----------------------
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
 VLAN Mapping
STP Loopguard               1     Disabled               Disabled
STP Bridge Assurance        1     Enabled                Enabled
STP Port Type               1     Normal                 Normal
STP MST Simulate PVST       1     Enabled                Enabled
Allowed VLANs               -     1-10,15-20,30,37,99    1-10,15-20,30,37,99
```

Cannot Enable the vPC Feature

You may receive an error when you enable the vPC feature.

Symptom	Possible Cause	Solution

Cannot enable the vPC feature.	The hardware is incompatible with the vPC.	Use the **show module** command to determine the hardware version of each N7K-M132XP-12 Ethernet module. The hardwere version must be 1.3 or later to enable the vPC feature.

Example: show module Command Output

This example shows how to display the module hardware version:

```
switch# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------- ------------------ ------------
2    32     10 Gbps Ethernet Module           N7K-M132XP-12      ok
3    48     10/100/1000 Mbps Ethernet Module  N7K-M148GT-11      ok
5    0      Supervisor module-1X              N7K-SUP1           active *
6    0      Supervisor module-1X              N7K-SUP1           ha-standby
10   32     10 Gbps Ethernet Module           N7K-M132XP-12      ok

Mod  Sw              Hw
---  --------------  ------
2    4.1(5)          1.2
3    4.1(5)          1.0  >>> Must be 1.3 or later.
```

vPC in Blocking State

vPC may be in the blocking state because of Bride Assurance (BA).

Symptom	Possible Cause	Solution
vPC is in blocking state.	BPDU only sends on a single link of a port-channel. If BA dispute is detected, the entire vPC will be in the blocking state.	Do not enable BA on vPC.

VLANs on a vPC moved to suspend state

VLANs on a vPC may move to the suspend state.

Symptom	Possible Cause	Solution
VLANs on a vPC moved to suspend state.	VLANs allowed on the vPC have not been allowed on the vPC peer=link.	All VLANs allowed on a vPC must also be allowed on the vPC peer-link. Also, it is recommended that only vPC VLANs are allowed on the vPC peer-link.

Hosts with an HSRP Gateway Cannot Access Beyond Their VLAN

When HSRP is enabled on both vPC peer devices on a VLAN and hosts on that VLAN set the HSRP as their gateway, they may not able to reach anything outside their own VLAN.

Symptom	Possible Cause	Solution
Hosts with an HSRP gateway cannot access beyond their VLAN.	If the host gateway mac-address is mapped to the physical MAC address of any one of the vPC peer-devices, packets may get dropped due to the loop prevention mechanism in vPC.	Map the host gateway's mac-address to the HSRP MAC address and not the physical MAC address of any one of the vPC peer-devices. Peer-gateway can be a workaround for this scenario. Please read the configuration guide for peer-gateway for further information before implementing it.

Traffic Disrupted when the Primary vPC Device Goes Down

Traffic may remain disrupted when the N7K-M132XP-12 module on the primary vpc device goes down.

Symptom	Possible Cause	Solution
Traffic disrupted when the primary vPC device goes down.	All core facing interfaces and vPC peer-links are configured on a single N7K-M132XP-12 module.	Enable object tracking. With object tracking enabled, all vPC on the primary will shut down. The vPC secondary will take over as the operational primary and all the vPC on the secondary will stay up. As a result, traffic will still be flowing thru the secondary which became operational primary.

See Also

Troubleshooting Ports

Further Reading

The following links contain further information on this topic from Cisco.com:

Configuring vPCs (Cisco Nexus 7000 Series Interfaces Configuration Guide)

Nexus 5000 Virtual PortChannel Quick Configuration Guide

External Links

The following links contain content developed by external authors. Cisco does not review this content for accuracy.

Our Nexus Data Center Network - To vPC or not to vPC

Nexus 7000 Virtual Portchannel Part 1

Nexus 7000 Virtual Portchannel Part 2

Nexus 7000 Virtual Portchannel Part 3

vPC (Virtual Port-Channel) and the Nexus 5000 Platform

Blog on Cisco Nexus Features (VLANs, vPCs)