Troubleshooting vPCs

About Troubleshooting vPCs

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

Initial Troubleshooting vPCs Checklist

Begin troubleshooting vPC issues by checking the following issues first:

Checklist	Done
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 connected to the management ports on both vPC peer devices?	
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. Otherwise, the vPC peer link will not come up.	
Verify that the vPC peer link is configured as a Layer 2 port channel trunk that allows only 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.	

Checklist	Done
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, perform one of these tasks:

Command	Purpose
show running-config vpc	Verifies the vPC configuration.
show vpc	Checks the status of the vPCs.
show vpc peer-keepalive	Checks the status of the vPC peer-keepalive link.
show vpc consistency-parameters	Verifies that the vPC peers have the identical type-1 parameters.
show tech-support vpc	Displays detailed technical support information for vPCs.
show port-channel summary	Verifies that the members in the port channel are mapped to the vPC.
show spanning-tree	Verifies that the following STP parameters are identical when STP is enabled: • BPDU filter • BPDU guard • Cost • Link type • Priority • VLANs (PVRST+)

The following example shows sample output for the **show vpc** command:

```
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 1
Peer status                       : peer link is down

vPC keep-alive status             : Suspended (Destination IP not reachable)
Configuration consistency status  : failed
Per-vlan consistency status       : success

Configuration inconsistency reason: Consistency Check Not Performed
Type-2 inconsistency reason       : Consistency Check Not Performed
vPC role                          : none established
```

```
Number of vPCs configured         : 2
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Disabled (due to peer configuration)
Auto-recovery status              : Disabled

vPC Peer-link status
---------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------
1    Po10   down   -


vPC status
----------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
2    Po20   down   failed      Peer-link is down          -



50   Po50   down   failed      Peer-link is down          -
```

Received Type 1 Configuration Element Mismatch

You might 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.

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 might 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 Ethernet module.

This example shows how to display the module hardware version:

```
switch# show module
Mod Ports Module-Type                       Model              Status
--- ----- ------------------------------------ ------------------ ----------
22   0    Fabric Module                       N9K-C9508-FM       ok
24   0    Fabric Module                       N9K-C9508-FM       ok
26   0    Fabric Module                       N9K-C9508-FM       ok
27   0    Supervisor Module                   N9K-SUP-A          active *
29   0    System Controller                   N9K-SC-A           active
30   0    System Controller                   N9K-SC-A           standby

Mod Sw               Hw
--- ---------------- ------
22  6.1(2)I1(1)      0.4040
24  6.1(2)I1(1)      0.4040
26  6.1(2)I1(1)      0.4040
27  6.1(2)I1(1)      0.4080
29  6.1(2)I1(1)      0.2170
30  6.1(2)I1(1)      0.2170
```

vPCs in Blocking State

vPCs might be in the blocking state because of bridge assurance (BA).

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

VLANs on a vPC Moved to Suspend State

VLANs on a vPC might move to the suspend state.

Symptom	Possible Cause	Solution
VLANs on a vPC are moved to the 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, we recommend 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 might 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 might get dropped due to the loop prevention mechanism in the 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. The peer gateway can be a workaround for this scenario. Read the configuration guide for more information about the peer gateway before you implement it.