Configure Virtual Port Channels

**Configure Virtual Port Channels**

In this lab exercise, you configure and verify vPCs on Cisco Nexus 7000 VDC and 5000 Series Switches.

Configuration of port channels commonly consists of two elements: configuring the physical ports and configuring the port channel interface. The physical ports need to be assigned to a channel group, which then bundles the ports together. A channel group always has an associated port channel interface, which has the same number as the channel group number. You can create the port channel interface before you assign the physical interfaces to a channel group. If you do not create the port channel interface beforehand, it is automatically created when you assign the first physical interface to the channel group.

After the interfaces have been successfully bundled into a channel group with an associated port channel number, you can then configure Layer 2 or Layer 3 settings on the port channel interface. Control plane protocols, such as STP and routing protocols, treat the port channel as a single link. STP will not block the links that are part of the port channel, and routing protocols only form a single routing adjacency across the port channel. Any configuration changes that you apply to the port channel are applied to each member interface of that port channel.

A vPC allows links that are physically connected to two different Cisco Nexus devices to appear as a single port channel by a third device. A vPC can provide multipathing, which allows you to create redundancy by enabling multiple parallel paths between nodes and load balancing traffic where alternative paths exist.

**Note**

The outputs in the lab were generated from Pod 8. Your output may vary, depending on the pod that you are working on. The variable *X* represents your pod number. Please refer to Job Aids for the values that are associated with your assigned pod.

**Note**

Click the **Initialize** button below to start the lab. Initialization takes 15–60 minutes. A progress bar will show you when the lab is initialized and active. Please be patient with the initialization process; several components are loading and getting ready!

After initialization is complete, start the lab within 10 minutes or it will be automatically terminated. After you have entered the active lab, do not navigate away from the lab page until you have completed that lab exercise or it will be terminated.

When the lab is active, the **Pod Number** tab on the right will tell you which pod is assigned to you.

**Verify Inter-Switch Connections and Configure Layer 3 Inter-Switch Interface**

In this activity, you will use CLI commands to verify the physical connections between your Cisco Nexus 7000 VDC and Cisco Nexus 5000 Series Switches.

Configure both Cisco Nexus 5000 Series Switches in your pod. Wherever the **show**command output or configuration commands are identical on both switches, only one example is shown.

**Step 1**

Open an SSH session to both of your Cisco Nexus 5000 Series Switches and 7000 VDCs. Log in using the user name **admin** and password **1234QWer**.

**Step 2**

Remove the Cisco fabricpath configuration on Cisco Nexus Series Switches.

Answer

Disable the fabricpath feature, which removes fabricpath configuration form interfaces and VLANs.

N7K-A-Pod8**# configure terminal**

N7K-A-Pod8(config)**# no feature-set fabricpath**

Feature-set Operation may take up to 95 minutes depending on the size of configuration.

N7K-A-Pod8(config)**# no vlan 50**

N7K-A-Pod8(config)**# interface ethernet 4/25-31**

N7K-A-Pod8(config-if-range)**# switchport mode trunk**

N7K-B-Pod8**# configure terminal**

N7K-B-Pod8(config)**# no feature-set fabricpath**

Feature-set Operation may take up to 95 minutes depending on the size of configuration.

N7K-B-Pod8(config)**# no vlan 50**

N7K-B-Pod8(config)**# interface ethernet 4/25-31**

N7K-B-Pod8(config-if-range)**# switchport mode trunk**

N5K-A-8**# configure terminal**

N5K-A-8(config)**# no feature-set fabricpath**

Feature-set Operation may take up to 95 minutes depending on the size of configuration.

N5K-A-8(config)**# no vlan 50**

N5K-A-8(config)**# interface ethernet 1/1-4**

N5K-A-8(config-if-range)**# switchport mode trunk**

N5K-A-8**# configure terminal**

N5K-A-8(config)**# no feature-set fabricpath**

Feature-set Operation may take up to 95 minutes depending on the size of configuration.

N5K-A-8(config)**# no vlan 50**

N5K-A-8(config)**# interface ethernet 1/1-4**

N5K-A-8(config-if-range)**# switchport mode trunk**

**Step 3**

Review the interface connectivity by examining the descriptions that are assigned to the interfaces. Compare the output to your topology diagram for all interfaces that are in use.

Answer

N7K-A-Pod8**# show interface description**

-------------------------------------------------------------------------------

Interface Description

-------------------------------------------------------------------------------

mgmt0 --

-------------------------------------------------------------------------------

Port Type Speed Description

-------------------------------------------------------------------------------

Eth4/25 eth 10G Connects to N7K-B-Pod8 4/25 - vPC peer-link

Eth4/26 eth 10G Connects to N7K-B-Pod8 4/26 - vPC peer-keepalive

Eth4/27 eth 10G Connects to 9396-A E1/8

Eth4/28 eth 10G Connects to 6248-A E1/8

Eth4/29 eth 10G Connects to 5672-A-8 E1/1

Eth4/30 eth 10G Connects to 5672-B-8 E1/1

Eth4/31 eth 10G Connects to N7K-B-Pod8 E4/31

Eth4/32 eth 10G --

N5K-A-8**# show interface description**

-------------------------------------------------------------------------------

Port Type Speed Description

-------------------------------------------------------------------------------

Eth1/1 eth 10G Connects to N7K-A-Pod8 E4/29

Eth1/2 eth 10G Connects to N7K-B-Pod8 E4/29

Eth1/3 eth 10G Connects to N5K-B-8 E1/3

Eth1/4 eth 10G Connects to N5K-B-8 E1/4

Eth1/5 eth 10G Connects to 2232PP-A F1

Eth1/6 eth 10G Connects to 2232PP-A F2

Eth1/7 eth 10G Connects to 2232PP-B F3

<... output omitted ...>

**Note**

Customize the topology in your lab guide by writing these interface numbers down. Make a note of the interface that is to be used for the vPC keepalive—you will configure this interface next.

**Step 4**

Verify the topology by using CDP.

Answer

While CDP is not discussed in this course, you should take the time to explore the **show** command output.

N7K-A-Pod8**# show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - switch, H - Host, I - IGMP, r - Repeater,

V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID Local Intrfce Hldtme Capability Platform Port ID

MGMT-SW mgmt0 169 R S I WS-C2960XR-48 Gig1/0/1

N7K-B-Pod8(JAF1752AKGC)

Eth4/25 130 R S I s N7K-C7009 Eth4/25

N7K-B-Pod8(JAF1752AKGC)

Eth4/26 132 R S I s N7K-C7009 Eth4/26

UCS-A(SSI184706W7)

Eth4/28 142 S I s UCS-FI-6248UP Eth1/8

N5K-A-8(FOC1912R11S)

Eth4/29 164 R S I s N5K-C5672UP Eth1/1

N5K-B-8(FOC1912R0ZD)

Eth4/30 147 R S I s N5K-C5672UP Eth1/1

N7K-B-Pod8(JAF1752AKGC)

Eth4/31 132 R S I s N7K-C7009 Eth4/31

Total entries displayed: 7

N5K-A-8**# show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - switch, H - Host, I - IGMP, r - Repeater,

V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID Local Intrfce Hldtme Capability Platform Port ID

MGMT-SW mgmt0 121 R S I WS-C2960XR-48 Gig1/0/14

N7K-A-Pod8(JAF1752AKJA) Eth1/1 138 R S I s N7K-C7009 Eth4/29

N7K-B-Pod8(JAF1752AKGC) Eth1/2 141 R S I s N7K-C7009 Eth4/29

N5K-B-8(FOC1912R0ZD) Eth1/3 130 R S I s N5K-C5672UP Eth1/3

N5K-B-8(FOC1912R0ZD) Eth1/4 130 R S I s N5K-C5672UP Eth1/4

**Note**

For the Cisco Nexus 5000 Series output, note that the FEX does not appear as a neighbor. FEXs are seen as integrated extensions of the Cisco Nexus 5000 Series Switches, and not standalone switches.

**Step 5**

Verify that the required interfaces are operational.

Answer

N7K-A-Pod8**# show interface brief | include up**

Eth4/25 1 eth trunk up none 10G(D) --

Eth4/26 1 eth trunk up none 10G(D) --

Eth4/27 1 eth trunk up none 10G(D) --

Eth4/28 1 eth trunk up none 10G(D) --

Eth4/29 1 eth trunk up none 10G(D) --

Eth4/30 1 eth trunk up none 10G(D) --

Eth4/31 1 eth trunk up none 10G(D) --

<... output omitted ...>

N5K-A-8**# show interface brief | include up**

Eth1/1 1 eth trunk up none 10G(D) --

Eth1/2 1 eth trunk up none 10G(D) --

Eth1/3 1 eth trunk up none 10G(D) --

Eth1/4 1 eth trunk up none 10G(D) --

Eth1/5 1 eth fabric up none 10G(D) 101

Eth1/6 1 eth fabric up none 10G(D) 101

Po101 1 eth fabric up none a-10G(D) none

<... output omitted ...>

**Note**

All interfaces between the Cisco Nexus 7000 and 5000 Series Switches should be up.

**Step 6**

Configure a Layer 3 interface between your two Cisco Nexus 7000 VDCs that will be used for the vPC peer-keepalive. Both Cisco Nexus 7000 VDCs should use the interface with the peer-keepalive description from the previous step. The interfaces should be members of the VRF VPC-KEEPALIVE. The IP addresses are 209.165.200.225/24 (N7K-A) and 209.165.200.226/24 (N7K-B).

Answer

N7K-A-Pod8**#configure terminal**

N7K-A-Pod8(config)**# vrf context VPC-KEEPALIVE**

N7K-A-Pod8(config-vrf)**# interface ethernet 4/26**

N7K-A-Pod8(config-if)**# no switchport**

N7K-A-Pod8(config-if)**# vrf member VPC-KEEPALIVE**

Warning: Deleted all L3 config on interface Ethernet4/26

N7K-A-Pod8(config-if)**# ip addr 209.165.200.225/24**

N7K-B-Pod8**#configure terminal**

N7K-B-Pod8(config)**# vrf context VPC-KEEPALIVE**

N7K-B-Pod8(config-vrf)**# interface ethernet 4/26**

N7K-B-Pod8(config-if)**# no switchport**

N7K-B-Pod8(config-if)**# vrf member VPC-KEEPALIVE**

Warning: Deleted all L3 config on interface Ethernet4/26

N7K-B-Pod8(config-if)**# ip addr 209.165.200.226/24**

**Note**

The command **no switchport** converts the interface from a Layer 2 interface to a Layer 3 interface.

**Step 7**

Verify that the Layer 3 interfaces are up.

Answer

The vPC peer-keepalive link is a logical link that often runs over an OOB Layer 3 network and provides a Layer 3 communications path that is used as a secondary test in order to determine whether the remote vPC peer is operating properly. The peer-keepalive status is used to determine the status of the vPC peer when the vPC peer-link goes down. In this scenario, it helps the vPC switch to determine whether the peer-link itself has failed or whether the vPC peer has failed entirely.

N7K-A-Pod8(config-if)**# show ip interface brief vrf VPC-KEEPALIVE**

IP Interface Status for VRF "VPC-KEEPALIVE"(5)

Interface IP Address Interface Status

Eth4/26 209.165.200.225 protocol-up/link-up/admin-up

N7K-B-Pod8(config-if)**# show ip interface brief vrf VPC-KEEPALIVE**

IP Interface Status for VRF "VPC-KEEPALIVE"(5)

Interface IP Address Interface Status

Eth4/26 209.165.200.226 protocol-up/link-up/admin-up

**Step 8**

Verify connectivity to your peer Cisco Nexus 7000 VDC Layer 3 interface from the previous step.

Answer

N7K-A-Pod8(config-if)**# ping 209.165.200.226 vrf VPC-KEEPALIVE**

PING 209.165.200.226 (209.165.200.226): 56 data bytes

64 bytes from 209.165.200.226: icmp\_seq=0 ttl=254 time=1.378 ms

64 bytes from 209.165.200.226: icmp\_seq=1 ttl=254 time=1.207 ms

64 bytes from 209.165.200.226: icmp\_seq=2 ttl=254 time=1.232 ms

64 bytes from 209.165.200.226: icmp\_seq=3 ttl=254 time=1.203 ms

64 bytes from 209.165.200.226: icmp\_seq=4 ttl=254 time=1.212 ms

--- 209.165.200.226 ping statistics ---

5 packets transmitted, 5 packets received, 0.00% packet loss

round-trip min/avg/max = 1.203/1.246/1.378 ms

**Establish the vPC Domain**

In this activity, you will use CLI commands to configure and verify the vPC domain between your Cisco Nexus 7000 VDCs, including the vPC peer-keepalive and vPC peer-link.

**Note**

The vPC domain is configured on both vPC peer devices using the same domain ID, so that the two distinct switches are tied together to form one logical switch.

Both Cisco Nexus switches in a pod should be configured in this activity. Wherever the **show** command output or configuration commands are identical between switches, only one screenshot will be shown. Pay careful attention to which device output is being demonstrated.

**Step 9**

Configure the vPC domain ID. Use domain ID **10**.

Answer

The configuration is not accepted since the vPC feature has not been enabled.

N7K-A-Pod8**# configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

N7K-A-Pod8(config)**# vpc domain 10**

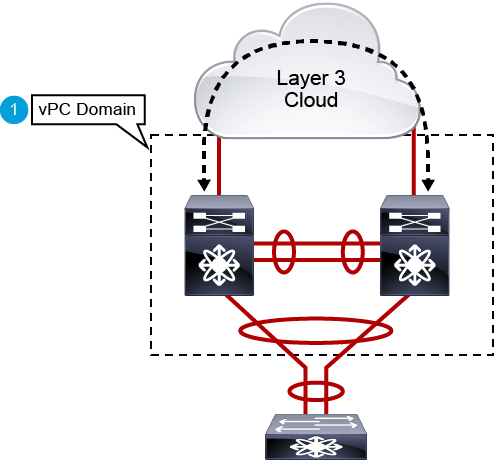
^

% Invalid command at '^' marker.

N7K-A-Pod8(config)**# vpc domain ?**

^

% Invalid command at '^' marker.



**Step 10**

Enable the vPC feature.

Answer

N7K-A-Pod8(config)**# feature vpc**

N7K-B-Pod8(config)**# feature vpc**

**Step 11**

Configure the vPC domain ID. Use domain ID **10**.

Answer

The vPC domain MAC address is not yet determined. The vPC peers must first communicate via the vPC peer-link in order to negotiate the vPC role

N7K-A-Pod8(config)**# vpc domain ?**

<1-1000> Domain id

N7K-A-Pod8(config)**# vpc domain 10**

N7K-A-Pod8(config-vpc-domain)**#**

N7K-A-Pod8(config-vpc-domain)**# show vpc role**

vPC Role status

----------------------------------------------------

vPC role : none established

vPC system-mac : 00:00:00:00:00:00

vPC system-priority : 32667

vPC local system-mac : e4:c7:22:15:33:c9

vPC local role-priority : 0

N7K-B-Pod8(config)**# vpc domain 10**

N7K-B-Pod8(config-vpc-domain)**# show vpc role**

vPC Role status

----------------------------------------------------

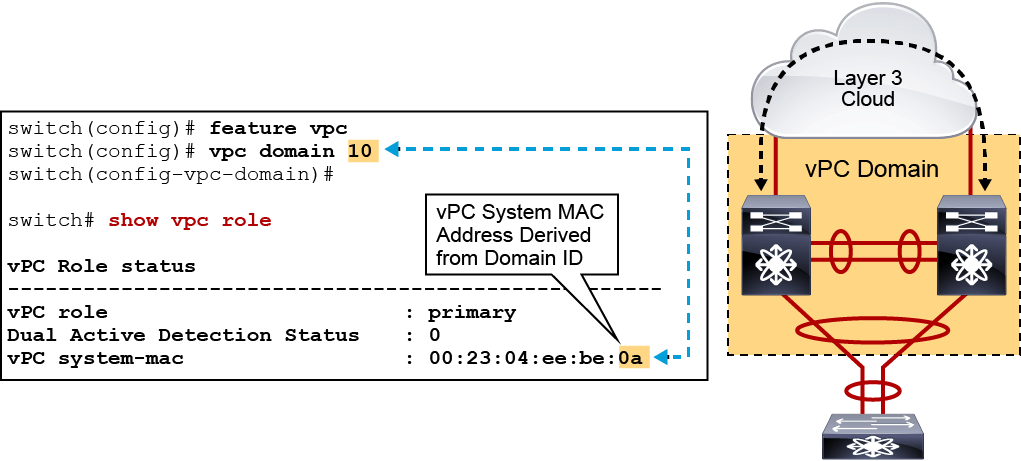
vPC role : none established

vPC system-mac : 00:00:00:00:00:00

vPC system-priority : 32667

vPC local system-mac : e4:c7:22:15:2c:49

vPC local role-priority : 0



The domain ID can be any value between 1 and 1000, and the same value must be configured on both switches forming the vPC pair. The vPC peer devices use the vPC domain ID to automatically assign a unique vPC system MAC address. Each vPC domain has a unique MAC address that is used as a unique identifier for the specific vPC-related operation. Although the devices use the vPC system MAC addresses only for link-scope operations, such as LACP, it is recommended that you create each vPC domain within the contiguous Layer 2 network with a unique domain ID. You can also configure a specific MAC address for the vPC domain rather than having Cisco NX-OS Software assign the address.

**Step 12**

Review the status of the vPC.

Answer

N7K-A-Pod8(config-vpc-domain)**# show vpc**

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 10

Peer status : peer link not configured

vPC keep-alive status : Disabled

Configuration consistency status : failed

Configuration inconsistency reason : vPC peer-link does not exist

Per-vlan consistency status : failed

Type-2 consistency status : failed

Type-2 inconsistency reason : vPC peer-link does not exist

vPC role : none established

Number of vPCs configured : 0

Peer Gateway : Disabled

Dual-active excluded VLANs and BDs : -

Graceful Consistency Check : Enabled

Auto-recovery status : Enabled (timeout = 240 seconds)

Operational Layer3 Peer-router : Disabled

Self-isolation : Disabled

Recall the main components of vPC: The domain, the peer-keepalive, the peer link, and the downstream port channels. The **show vpc**command provides output on each of these components. Since you have only configured the domain ID up to this point you expect to see error conditions in the output (peer link not configured, and so on). You will review this output again to see how it changes.

**Step 13**

Configure the vPC peer-keepalive link. The destination address that is used in this command is the IP address of your peer Cisco Nexus 7000 VDC, which is also the address that you pinged in the last activity. Confirm the status of the peer-keepalive link.

Answer

N7K-A-Pod8(config-vpc-domain)**# peer-keepalive destination 209.165.200.226 source 209.165.200.225 vrf VPC-KEEPALIVE**

N7K-B-Pod8(config-vpc-domain)**# peer-keepalive destination 209.165.200.225 source 209.165.200.226 vrf VPC-KEEPALIVE**

N7K-A-Pod8(config-vpc-domain)**#show vpc peer-keepalive**

vPC keep-alive status : peer is alive

--Peer is alive for : (66609) seconds, (346) msec

--Send status : Success

--Last send at : 2015.10.28 18:35:38 264 ms

--Sent on interface : Eth4/26

--Receive status : Success

--Last receive at : 2015.10.28 18:35:38 266 ms

--Received on interface : Eth4/26

--Last update from peer : (0) seconds, (806) msec

vPC Keep-alive parameters

--Destination : 209.165.200.226

--Keepalive interval : 1000 msec

--Keepalive timeout : 5 seconds

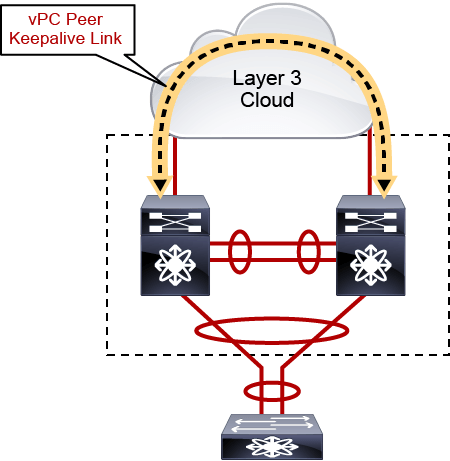
--Keepalive hold timeout : 3 seconds

--Keepalive vrf : VPC-KEEPALIVE

--Keepalive udp port : 3200

--Keepalive tos : 192

By default, the vPC peer keepalive packets are routed in the management VRF and use the OOB mgmt 0 interface. You can configure the vPC peer keepalive to use a different VRF, but you should take care that the peer keepalive traffic is not routed across the vPC peer link.



The peer-keepalive provides a heartbeat between the vPC peer switches, which is used to detect and resolve a dual-active condition when the vPC peer-link fails. The peer-keepalives are IP-based and can be routed across an IP network if required.

Because it is vital that peer-keepalives never be carried on the vPC peer-link, consider these recommendations for the peer-keepalive infrastructure:

* For Cisco Nexus 9000 and 7000 Series Switches, it is recommended that you create a separate VRF instance specifically for the vPC peer-keepalive. By assigning a specific routed port to this VRF, you can ensure that the peer-keepalive traffic is always carried on that link and never carried on the peer link. For high availability, the port that is used for the peer-keepalive should be terminated on a different I/O module than the links that form the peer link. If it is not possible to allocate a dedicated port for the peer-keepalive, the OOB management interface mgmt 0 can be used. In this case, it is important that the management ports on both supervisors are connected to the OOB management network. Do not use Ethernet crossover cables to connect the management ports on the vPC peers to each other back-to-back, because the peer-keepalive link will fail on supervisor switchover. If neither of these options is available, an upstream Layer 3 network in the core or aggregation layer of the data center could be used for the peer-keepalive.
* For the Cisco Nexus 5000 Series Switches, the recommendations are slightly different: It is recommended to use the OOB management interface mgmt 0 for the peer-keepalive if possible. If this option is not available, a dedicated port with an associated VLAN and SVI should be used. If it is also not possible to dedicate a separate port for the peer-keepalive, then an in-band Layer 3 network can be used. However, you should take care that the VLAN associated with the peer-keepalive connection is not allowed on the vPC peer link if this option is used.

| Deployment Option | Nexus 5000/5500 | Nexus 9000 and 7000 |
| --- | --- | --- |
| Dedicated non-mgmt port | Use a dedicated port and VLAN | Use a dedicated routed port in a separate VRF (a Gigabit Ethernet port is sufficient) |
| OOB mgmt | Use the OOB management interface mgmt0 | Use the OOB management interface mgmt0 |
| In-band | Use an in-band Layer 3 network | Use an upstream Layer 3 network |

**Step 14**

Configure a traditional port channel between your Cisco Nexus 7000 switch VDC and your pod peer VDC, which will be used as the vPC peer-link. Use channel group number 10. Do not use LACP. Refer to your topology, or use the **show interface description** command, to confirm which Layer 2 interface between your Cisco Nexus 7000 switch VDCs is used for the vPC peer-link.

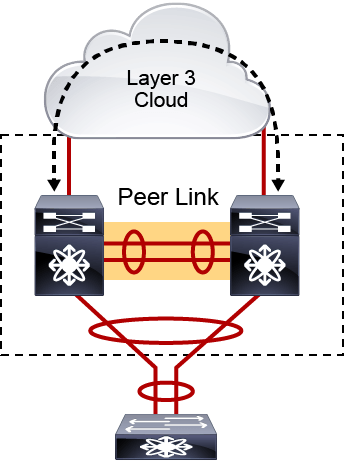
Answer

N7K-A-Pod8(config-vpc-domain)**# interface ethernet 4/25**

N7K-A-Pod8(config-if)**# channel-group 10**

N7K-B-Pod8(config-vpc-domain)**# interface ethernet 4/25**

N7K-B-Pod8(config-if)**# channel-group 10**



While the channel group number can be any value between 1 and 4096, matching the port channel number with the vPC domain number may help with troubleshooting. The system automatically creates a port channel interface using the same number.

**Step 15**

Configure the port channel interface as a vPC peer-link.

Answer

Messages are generated automatically by the system.

N7K-A-Pod8(config-if)**# interface port-channel 10**

N7K-A-Pod8(config-if)**# vpc peer-link**

Warning:

Ensure that VPC peer-link member ports on both peers use identical VDC types (limit-resource module-type VDC config command).

Please note that spanning tree port type is changed to "network" port type on vPC peer-link.

This will enable spanning tree Bridge Assurance on vPC peer-link provided the STP Bridge Assurance (which is enabled by default) is not disabled.

N7K-B-Pod8(config-if)**# interface port-channel 10**

N7K-B-Pod8(config-if)**# vpc peer-link**

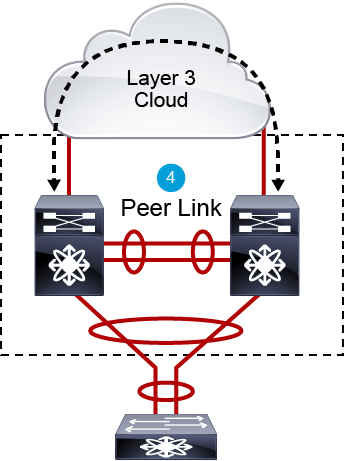
Warning:

Ensure that VPC peer-link member ports on both peers use identical VDC types (limit-resource module-type VDC config command).

Please note that spanning tree port type is changed to "network" port type on vPC peer-link.

This will enable spanning tree Bridge Assurance on vPC peer-link provided the STP Bridge Assurance (which is enabled by default) is not disabled.

The vPC peer-link is used to create the illusion of a single control plane by forwarding BPDUs and LACP packets to the primary vPC switch from the secondary vPC switch. The peer link is also used to synchronize MAC address tables between the vPC peers and to synchronize IGMP entries for IGMP snooping. The peer link provides the necessary transport for multicast traffic and for the traffic of orphaned ports.



The vPC peer-link carries essential vPC traffic between the vPC peer switches. The vPC peer-link is a port channel, which should consist of at least two dedicated 10-Gigabit Ethernet links (this lab only uses a single link) terminated on two different I/O modules if at all possible (the goal is high availability).

The vPC peer-link should be configured as a trunk. The allowed VLAN list for the trunk should be configured in such a way that only vPC VLANs (VLANs that are present on any vPCs) are allowed on the trunk. It is not recommended to carry non-vPC VLANs on the vPC peer link, because this configuration could cause severe traffic disruption for the non-vPC VLANs if the vPC peer link fails.

It is recommended that you enable bridge assurance on the vPC peer-link and use UDLD to protect against unidirectional link failures.

**Step 16**

Assign a description to the port channel interface, and verify that the interface description has been added.

Answer

N7K-A-Pod8(config-if)**# interface port-channel 10**

N7K-A-Pod8(config-if)**# description vpc peer-link between Cisco Nexus 7000 switch VDCs**

N7K-A-Pod8(config-if)**# show interface description**

-------------------------------------------------------------------------------

Interface Description

-------------------------------------------------------------------------------

mgmt0 --

-------------------------------------------------------------------------------

Port Type Speed Description

-------------------------------------------------------------------------------

Eth4/25 eth 10G Connects to N7K-B-Pod8 4/25 - vPC peer-link

Eth4/26 eth 10G Connects to N7K-B-Pod8 4/26 - vPC peer-keepalive

Eth4/27 eth 10G Connects to 9396-A E1/8

Eth4/28 eth 10G Connects to 6248-A E1/8

Eth4/29 eth 10G Connects to 5672-A-8 E1/1

Eth4/30 eth 10G Connects to 5672-B-8 E1/1

Eth4/31 eth 10G Connects to N7K-B-Pod8 E4/31

Eth4/32 eth 10G --

-------------------------------------------------------------------------------

Interface Description

-------------------------------------------------------------------------------

Po10 vpc peer-link between Cisco Nexus 7000 switch VDCs

**Step 17**

When both Cisco Nexus 7000 VDCs include the port channel configuration, verify that the port channel interface is operational.

Answer

N7K-A-Pod8(config-if)**# show port-channel summary**

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

--------------------------------------------------------------------------------

Group Port- Type Protocol Member Ports

Channel

--------------------------------------------------------------------------------

10 Po10(SU) Eth NONE Eth4/25(P)

**Step 18**

Verify the details of the port channel interface.

Answer

N7K-A-Pod8(config-if)**# show interface port-channel 10**

**port-channel10 is up**

admin state is up

Hardware: Port-Channel, address: b0aa.771c.cb70 (bia b0aa.771c.cb70)

Description: vpc peer-link between Cisco Nexus 7000 switch VDCs

MTU 9216 bytes, BW 10000000 Kbit, DLY 10 usec

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, medium is broadcast

Port mode is trunk

full-duplex, 10 Gb/s

Input flow-control is off, output flow-control is off

Auto-mdix is turned off

Switchport monitor is off

EtherType is 0x8100

Members in this channel: Eth4/25

Last clearing of "show interface" counters never

<... output omitted ...>

**Step 19**

Review the status of the vPC once again.

Answer

N7K-A-Pod8(config-if)**# show vpc**

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 10

Peer status : peer adjacency formed ok

vPC keep-alive status : peer is alive

Configuration consistency status : success

Per-vlan consistency status : success

Type-2 consistency status : success

vPC role : secondary

Number of vPCs configured : 0

Peer Gateway : Disabled

Dual-active excluded VLANs and BDs : -

Graceful Consistency Check : Enabled

Auto-recovery status : Enabled (timeout = 240 seconds)

Operational Layer3 Peer-router : Disabled

Self-isolation : Disabled

vPC Peer-link status

--------------------------------------------------------------------------------

id Port Status Active vlans Active BDs

-- ---- ------ -------------------------------------------------------------

1 Po10 up 1,12  **-**

Now we see the **peer status : peer adjacency formed ok** output, which confirms the peer-link adjacency is established over the Layer 2 end-to-end link.

VLANs 1 and 12 are shown as Active over the port channel interface. VLAN 12 is left from the VRF lab.

**Step 20**

Review the status of the vPC roles.

Answer

N7K-A-Pod8(config-if)**# show vpc role**

vPC Role status

----------------------------------------------------

vPC role : secondary

vPC system-mac : 00:23:04:ee:be:0a

vPC system-priority : 32667

vPC local system-mac : e4:c7:22:15:33:c9

vPC local role-priority : 32667

N7K-B-Pod8(config-if)**# show vpc role**

vPC Role status

----------------------------------------------------

vPC role : primary

vPC system-mac : 00:23:04:ee:be:0a

vPC system-priority : 32667

vPC local system-mac : e4:c7:22:15:2c:49

vPC local role-priority : 32667

Now that the vPC peer-link has been formed, the system MAC address has been determined; the last octet (0A, or decimal 10) is derived from the vPC domain ID.

There are two defined vPC roles: primary and secondary. The vPC role defines which of the two vPC peer devices processes BPDUs and responds to ARP (for example). The vPC **peer-switch** and **peer-gateway** commands will affect this processing as well, but this is beyond the scope of this class.

**Step 21**

Save the configuration of each switch.

Answer

N7K-A-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

N7K-B-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

**Configure the vPC Member Interfaces**

In this activity, you will configure and verify port channel interfaces on your Cisco Nexus 5000 Series Switches that are connected to your Cisco Nexus 7000 VDC vPC domain.

Complete these steps on both Cisco Nexus 7000 VDCs and Cisco Nexus 5000 Series Switches.

Configure both Cisco Nexus 5000 Series Switches in your pod. Wherever the **show**command output or configuration commands are identical on both switches, only one example is shown.

**Step 22**

Refer to your topology diagram to confirm the interfaces between your Cisco Nexus 5000 Series Switch and Cisco Nexus 7000 VDC that will be placed into the port channel.

Answer

N5K-A-8**# show interface description | include Connects**

Eth1/1 eth 10G Connects to N7K-A-Pod8 E4/29

Eth1/2 eth 10G Connects to N7K-B-Pod8 E4/29

Eth1/3 eth 10G Connects to N5K-B-8 E1/3

Eth1/4 eth 10G Connects to N5K-B-8 E1/4

Eth1/5 eth 10G Connects to 2232PP-A F1

Eth1/6 eth 10G Connects to 2232PP-A F2

Eth1/7 eth 10G Connects to 2232PP-B F3

Po101 eth 10G Connects to 2200-A FEX 101

N5K-A-8**# show interface brief | include up**

Eth1/1 1 eth trunk up none 10G(D) --

Eth1/2 1 eth trunk up none 10G(D) --

Eth1/3 1 eth trunk up none 10G(D) --

Eth1/4 1 eth trunk up none 10G(D) --

Eth1/5 1 eth fabric up none 10G(D) --

Eth1/6 1 eth fabric up none 10G(D) --

Po101 1 eth fabric up none a-10G(D) none

<output omitted>

N5K-A-8**# show cdp neighbor**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - switch, H - Host, I - IGMP, r - Repeater,

V - VoIP-Phone, D - Remotely-Managed-Device,

s - Supports-STP-Dispute

Device-ID Local Intrfce Hldtme Capability Platform Port ID

MGMT-SW mgmt0 125 R S I WS-C2960XR-48 Gig1/0/14

N7K-A-Pod8(JAF1752AKJA)

Eth1/1 167 R S I s N7K-C7009 Eth4/29

N7K-B-Pod8(JAF1752AKGC)

Eth1/2 129 R S s N7K-C7009 Eth4/29

N5K-B-8(FOC1912R0ZD)

Eth1/3 170 R S I s N5K-C5672UP Eth1/3

N5K-B-8(FOC1912R0ZD)

Eth1/4 170 R S I s N5K-C5672UP Eth1/4

**Step 23**

Which interfaces of each Cisco Nexus 5000 Series Switch connect to each Cisco Nexus 7000 switches? Complete the table.

Answer

| 5672UP | Local Interface | 7000 VDC | Remote Interface | Port Channel |
| --- | --- | --- | --- | --- |
| N5K-A | Ethernet 1/1 | N7K-A | Ethernet / | 201 |
| N5K-A | Ethernet 1/2 | N7K-B | Ethernet / | 201 |
| N5K-B | Ethernet 1/1 | N7K-A | Ethernet / | 202 |
| N5K-B | Ethernet 1/2 | N7K-B | Ethernet / | 202 |

**Step 24**

Configure a traditional port channel over the links between your Cisco Nexus 5000 Series Switch and the two Cisco Nexus 7000 switches. The channel group numbers must be unique, since each connects to the same Cisco Nexus 7000 VDC. Use channel group number **201** on N5K-A, and channel group number **202**on N5K-B. Use LACP.

Answer

N5K-A-8**#config t**

N5K-A-8(config)**# feature lacp**

N5K-A-8(config)**# int e 1/1-2**

N5K-A-8(config-if-range)**# channel-group 201 mode active**

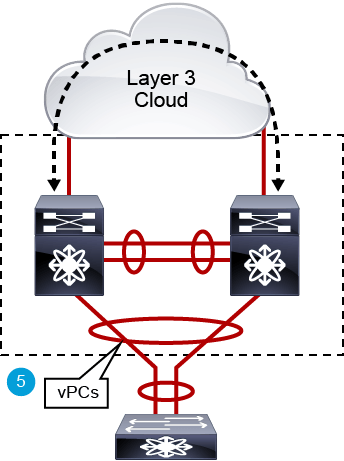
N5K-B-8**#config t**

N5K-B-8(config)**# feature lacp**

N5K-B-8(config)**# int e 1/1-2**

N5K-B-8(config-if-range)**# channel-group 202 mode active**

The **active** keyword specifies to use IEEE 802.1ax LACP to form the port channel. Before configuring LACP, you must enable the feature.



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 several operational attributes for an interface, before allowing that interface to participate in the port channel aggregation. Use the **show port-channel compatibility-parameters** command to see the complete list of compatibility checks that Cisco NX-OS Software uses.

**Step 25**

Assign a description to the port channel interface.

Answer

N5K-A-8(config-if-range)**# interface port-channel 201**

N5K-A-8(config-if)**# description PC connection to vPC Domain 10**

N5K-B-8(config-if-range)**# interface port-channel 202**

N5K-B-8(config-if)**# description PC connection to vPC Domain 10**

**Note**

The Cisco Nexus 5000 Series Switches will not be aware that they are connected to two different devices. The vPC allows both Cisco Nexus 7000 VDCs to behave as if they are one logical switch.

**Step 26**

Verify that the port channel interface is operational.

Answer

N5K-A-8(config-if)**# show port-channel summary**

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

--------------------------------------------------------------------------------

Group Port- Type Protocol Member Ports

Channel

--------------------------------------------------------------------------------

101 Po101(SU) Eth NONE Eth1/5(P) Eth1/6(P)

201 Po201(SD) Eth LACP Eth1/1(I) Eth1/2(I)

Why is the state of the port channel SD (down)?

**Step 27**

Further details relating to the port channel state are visible in the output of other commands.

Answer

N5K-A-8(config-if)**# show interface port-channel 201 brief**

----------------------------------------------------------------------------------

Port-channel VLAN Type Mode Status Reason Speed Protocol

Interface

----------------------------------------------------------------------------------

Po201 1 eth trunk down No operational members 10G(D) lacp

N5K-A-8(config-if)**# show interface port-channel 201**

port-channel201 is down (No operational members)

Hardware: Port-Channel, address: 0000.0000.0000 (bia 0000.0000.0000)

Description: vPC connection to vPC Domain 100

MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA

Port mode is trunk

auto-duplex, 10 Gb/s

Input flow-control is off, output flow-control is off

Switchport monitor is off

EtherType is 0x8100

Members in this channel: Eth1/1, Eth1/2

Last clearing of "show interface" counters never

<... output omitted ...>

**Step 28**

A port channel requires configuration on both ends of the links! Configure the traditional port channel on your Cisco Nexus 7000 VDC. For ease of management, the channel group numbers should match the numbering used on your Cisco Nexus 5000 Series Switches (channel group number **201** on N5K-A, and channel group number **202** on N5K-B).

Answer

N7K-A-Pod8(config-if)**# feature lacp**

N7K-A-Pod8(config)**# interface e4/29**

N7K-A-Pod8(config-if)**# channel-group 201 mode active**

N7K-A-Pod8(config-if)**# interface e4/30**

N7K-A-Pod8(config-if)**# channel-group 202 mode active**

N7K-B-Pod8(config-if)**# feature lacp**

N7K-B-Pod8(config)**# interface e4/29**

N7K-B-Pod8(config-if)**# channel-group 201 mode active**

N7K-B-Pod8(config-if)**# interface e4/30**

N7K-B-Pod8(config-if)**# channel-group 202 mode active**

Note the following:

* If a PortChannel is not configured on both switches terminating the port channel, the PortChannel ports will show as Individual state (I) and run regular spanning tree. In this case, you have configured the port channels on both Cisco Nexus 5000 Switches, but not on the Cisco Nexus 7000 Switches.
* Be sure to refer to the connection table you populated above to verify that you are configuring the correct interfaces.
* Since each Cisco Nexus 7000 VDC connects to both Cisco Nexus 5000 Series Switches, you will configure two port channels on each Cisco Nexus 7000 VDC.

**Step 29**

Assign a description to the port channel interfaces.

Answer

N7K-A-Pod8(config-if)**# interface port-channel 201**

N7K-A-Pod8(config-if)**# description vPC member connection to N5K-A**

N7K-A-Pod8(config-if)**# interface port-channel 202**

N7K-A-Pod8(config-if)**# description vPC member connection to N5K-B**

**Step 30**

Verify that the port channel interface is now operational on each Cisco Nexus 5000 Series Switch.

Answer

N5K-A-8(config-if)**# show port-channel summary**

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

--------------------------------------------------------------------------------

Group Port- Type Protocol Member Ports

Channel

--------------------------------------------------------------------------------

101 Po101(SU) Eth NONE Eth1/5(P) Eth1/6(P)

201 Po201(SU) Eth LACP Eth1/1(s) Eth1/2(P)

Why is the state of one of the port channel interfaces (**s)** (which means suspended)? Think back to one of the advantages of vPC over STP.

**Step 31**

On your Cisco Nexus 7000 VDC, the port channel interfaces 201 and 202 are currently not configured as vPCs members; rather they are only configured as traditional port channels. To confirm the configuration, review the output of the **show vpc** command, and verify that there are no member ports at the bottom of the output. To form a vPC, each of the port channels must be bound together as a single vPC within the vPC domain.

Answer

N7K-A-Pod8(config-if)**# show vpc brief**

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 10

Peer status : peer adjacency formed ok

vPC keep-alive status : peer is alive

Configuration consistency status : success

Per-vlan consistency status : success

Type-2 consistency status : success

vPC role : secondary

Number of vPCs configured : 0

Peer Gateway : Disabled

Dual-active excluded VLANs and BDs : -

Graceful Consistency Check : Enabled

Auto-recovery status : Enabled (timeout = 240 seconds)

Operational Layer3 Peer-router : Disabled

Self-isolation : Disabled

vPC Peer-link status

--------------------------------------------------------------------------------

id Port Status Active vlans Active BDs

-- ---- ------ -------------------------------------------------------------

1 Po10 up 1,12 -

N7K-A-Pod8(config-if)**# int port-channel 201**

N7K-A-Pod8(config-if)**# vpc 201**

N7K-A-Pod8(config-if)**# int port-channel 202**

N7K-A-Pod8(config-if)**# vpc 202**

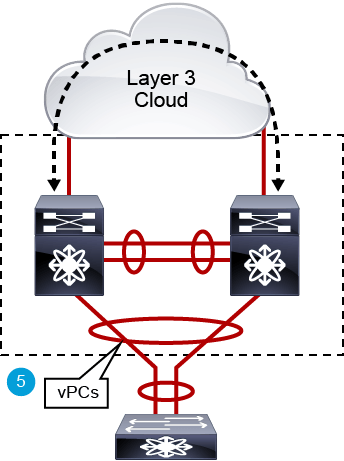
N7K-B-Pod8(config-if)**# int port-channel 201**

N7K-B-Pod8(config-if)**# vpc 201**

N7K-B-Pod8(config-if)**# int port-channel 202**

N7K-B-Pod8(config-if)**# vpc 202**

Once the vPC domain has been properly established, the individual vPCs can be configured. To configure a vPC, a port channel must be configured on both vPC peer switches. These two port channels must then be associated with each other by assigning a vPC number to the port channel interfaces. The vPC port number is unique for the vPC within the vPC domain and must be identical on the two peer switches.



Note the following:

* As with regular port channels, vPC member ports should have a compatible and consistent configuration. You should ensure that the configurations on vPC member ports are not only compatible on a single switch but also between peer switches.
* The port channel number and the vPC number do not have to be the same, but it is recommended that you keep them the same for ease of management.
* The vPC number must be the same on both switches for the same vPC.

**Step 32**

Verify that the port channel interface is now operational on each Cisco Nexus 5000 Series Switch.

Answer

Recall that port channel 101 or 102 was configured in an earlier lab for the FEX.

N5K-A-8(config-if-range)**# show port-channel summary**

Flags: D - Down P - Up in port-channel (members)

I - Individual H - Hot-standby (LACP only)

s - Suspended r - Module-removed

S - Switched R - Routed

U - Up (port-channel)

M - Not in use. Min-links not met

--------------------------------------------------------------------------------

Group Port- Type Protocol Member Ports

Channel

--------------------------------------------------------------------------------

101 Po101(SU) Eth NONE Eth1/5(P) Eth1/6(P)

201 Po201(SU) Eth LACP Eth1/1(P) Eth1/2(P)

**Step 33**

Verify on each Cisco Nexus 7000 VDC that the newly created vPCs are now part of the vPC domain.

Answer

N7K-A-Pod8(config-if)**# show vpc brief**

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 10

Peer status : peer adjacency formed ok

vPC keep-alive status : peer is alive

Configuration consistency status : success

Per-vlan consistency status : success

Type-2 consistency status : success

vPC role : secondary

Number of vPCs configured : 2

Peer Gateway : Disabled

Dual-active excluded VLANs and BDs : -

Graceful Consistency Check : Enabled

Auto-recovery status : Enabled (timeout = 240 seconds)

Operational Layer3 Peer-router : Disabled

Self-isolation : Disabled

vPC Peer-link status

--------------------------------------------------------------------------------

id Port Status Active vlans Active BDs

-- ---- ------ -------------------------------------------------------------

1 Po10 up 1,12 -

vPC status

**------------------------------------------------------**

id Port Status Consistency Active VLANs

**----- ------------ ------ ----------- ----------------**

201 Po201 up success 1,12

202 Po202 up success 1,12

**Step 34**

Save the configurations of all switches.

Answer

N5K-A-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete, now saving to disk (please wait)...

N7K-A-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

N5K-B-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete, now saving to disk (please wait)...

N7K-B-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

**Optimize vPC**

In this activity, you will optimize vPCs using the **peer-gateway** and **peer-switch**commands.

Both Cisco Nexus switches in a pod should be configured in this activity. Wherever the **show** command output or configuration commands are identical between switches, only one example will be shown. Pay careful attention to which device output is being demonstrated.

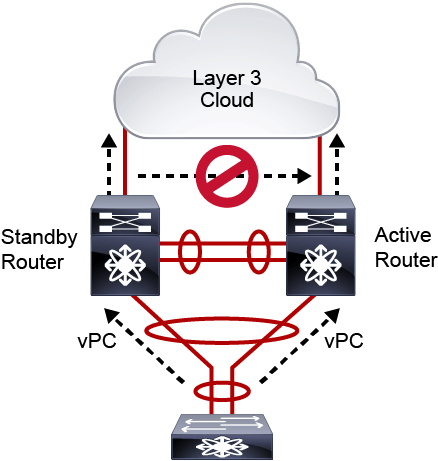
Perform this activity on both Cisco Nexus 7000 VDCs.

**Step 35**

Optimize vPC using the peer-gateway feature.

Answer

Recall that both vPC peers present themselves to all downstream devices as a single, logical unit, creating a need to define roles between the two vPC peers (primary and secondary) to determine which vPC peer processes the different broadcast and multicast control packets (like BPDUs and ARPs) sent upstream to both vPC peers.



Similarly, when using FHRP within a vPC domain, the vPC peers use a system generated virtual MAC address to respond to default gateway ARP requests. Depending on the FHRP, usually only one (active/standby, master/backup) of the vPC peers is elected to respond as the default gateway utilizing the virtual MAC address.

If a downstream device does not perform a typical default gateway ARP request at boot up, there is a chance that this downstream device may use the hardware MAC address of the secondary/standby/backup vPC peer as the default gateway. By default the secondary/standby/backup vPC peer would forward the packet over the vPC peer-link to the primary/active/master vPC peer.

The vPC peer-gateway capability allows a vPC switch to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer. This feature enables local forwarding of such packets without the need to cross the vPC peer-link. In this scenario, the feature optimizes the use of the peer-link and avoids potential traffic loss in FHRP scenarios.

The peer-gateway feature must be configured on both primary and secondary vPC peers and be nondisruptive to the operations of the device or to the vPC traffic. When this feature is enabled, IP redirects are automatically disabled on all interface VLANs that are associated with a vPC VLAN. This feature avoids generation of IP redirect messages for packets that are switched through the peer-gateway router.

N7K-A-Pod8(config-if)**# vpc domain 10**

N7K-A-Pod8(config-vpc-domain)**# peer-gateway**

This peer-gateway config may cause traffic loss. Do you want to continue (y/n)? [n] y

**Step 36**

Optimize vPC using the peer switch.

Answer

In addition to enabling the peer-switch feature, you should also set the best possible spanning tree bridge priority value on both peer switches. This setting forces the vPC switch pair to become the root of the spanning tree for the vPC VLANs.

N7K-A-Pod8(config-vpc-domain)**# show spanning-tree root**

Root Hello Max Fwd

Vlan Root ID Cost Time Age Dly Root Port

---------------- -------------------- ------- ----- --- --- ----------------

VLAN0001 32769 8c60.4f6c.6c3c 3 2 20 15 port-channel10

VLAN0012 32780 e4c7.2215.2c49 2 2 20 15 port-channel10

N7K-B-Pod8(config-vpc-domain)**# show spanning-tree root**

Root Hello Max Fwd

Vlan Root ID Cost Time Age Dly Root Port

---------------- -------------------- ------- ----- --- --- ----------------

VLAN0001 32769 8c60.4f6c.6c3c 1 2 20 15 port-channel202

VLAN0012 32780 e4c7.2215.2c49 0 2 20 15This bridge is root

N7K-A-Pod8(config-vpc-domain)**# peer-switch**

N7K-B-Pod8(config-if)**# vpc domain 10**

N7K-B-Pod8(config-vpc-domain)**# peer-switch**

N7K-A-Pod8(config-vpc-domain)**# show spanning-tree root**

Root Hello Max Fwd

Vlan Root ID Cost Time Age Dly Root Port

---------------- -------------------- ------- ----- --- --- ----------------

VLAN0001 32769 0023.04ee.be0a 0 2 20 15 This bridge is root

VLAN0012 32780 0023.04ee.be0a 0 2 20 15This bridge is root

N7K-B-Pod8(config-vpc-domain)**# show spanning-tree root**

Root Hello Max Fwd

Vlan Root ID Cost Time Age Dly Root Port

---------------- -------------------- ------- ----- --- --- ----------------

VLAN0001 32769 0023.04ee.be0a 0 2 20 15 This bridge is root

VLAN0012 32780 0023.04ee.be0a 0 2 20 15This bridge is root

**Step 37**

Save the configurations of both Cisco Nexus 7000 and Cisco Nexus 5000 Series Switches.

Answer

N7K-A-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

N5K-A-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

N7K-B-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

N5K-B-Pod8(config-if)**# copy running-config startup-config**

[########################################] 100%

Copy complete.

**Verify vPC Consistency Parameters**

In this activity, you will use CLI commands to verify vPC consistency parameters.

Complete these steps on both Cisco Nexus 7000 VDCs.

**Step 38**

Verify vPC consistency parameters.

Answer

N7K-A-Pod8(config-vpc-domain)**# show vpc consistency-parameters global**

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name Type Local Value Peer Value

------------- ---- ---------------------- -----------------------

STP MST Simulate PVST 1 Enabled Enabled

STP Port Type, Edge 1 Normal, Disabled, Normal, Disabled,

BPDUFilter, Edge BPDUGuard Disabled Disabled

STP MST Region Name 1 "" ""

STP Disabled 1 None None

STP Mode 1 Rapid-PVST Rapid-PVST

STP Bridge Assurance 1 Enabled Enabled

STP Loopguard 1 Disabled Disabled

STP MST Region Instance to 1

VLAN Mapping

STP MST Region Revision 1 0 0

Interface-vlan admin up 2 12 12

Interface-vlan routing 2 1,12 1,12

capability

Allowed VLANs - 1,12 1,12

Local error VLANs - - -

After you enable the vPC feature and configure the peer-link on both vPC peer devices, CFS messages provide a copy of the configuration on the local vPC device configuration to the remote vPC peer device. The system determines whether any of the crucial configuration parameters differ on the two devices. The parameters must be configured identically or the vPC moves into “suspend” mode. The per-interface parameters must be consistent per interface, and the global parameters must be consistent globally:

* Port channel mode: on, off, or active
* Link speed per channel
* Duplex mode per channel
* Trunk mode per channel, including native VLAN, VLANs allowed on trunk, and the tagging of native VLAN traffic
* STP mode
* STP region configuration for MST
* Enabled or disabled state per VLAN
* STP global settings, including Bridge Assurance setting, port type, and loop guard settings
* STP interface settings, including port type, loop guard, and root guard
* MTU

**Note**

If the **show vpc brief** command displays failed consistency checks, you can use the **show vpc consistency-parameters** command to find the specific parameters that caused the consistency check to fail. The **global** option on this command allows you to verify the consistency of the global parameters between the two peer switches. The **vpc** or **interface** options can be used to verify consistency between the port channel configurations for vPC member ports.

**Step 39**

Verify the vPC configuration.

Answer

N7K-A-Pod8(config-vpc-domain)**# show running-config vpc**

!Command: show running-config vpc

!Time: Wed Oct 28 18:44:18 2015

version 7.2(0)D1(1)

feature vpc

vpc domain 10

peer-switch

peer-keepalive destination 209.165.200.226 source 209.165.200.225 vrf VPC-KEEPALIVE

peer-gateway

interface port-channel10

vpc peer-link

interface port-channel201

vpc 201

interface port-channel202

vpc 202