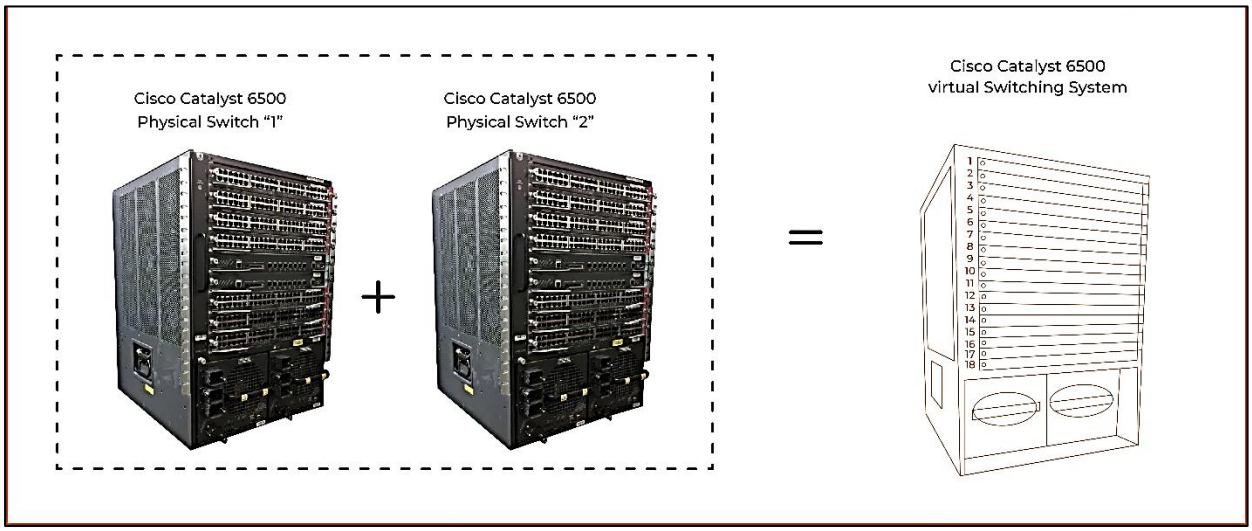
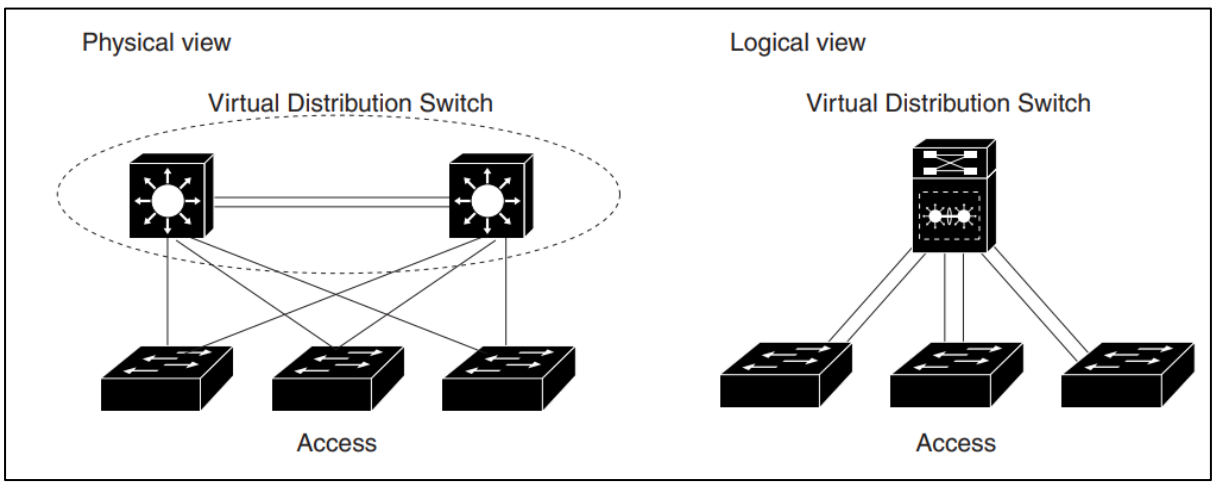
VSS- Virtual Switching System

- It is used to create one logical switch by combining **two physical switches.**
- It is a Cisco proprietary.
- This feature is supported on Catalyst 4500 , 6500 and 6800 modular switches.



A VSS in the distribution layer of the network interacts with the access and core networks as if it were a single switch—See image below.

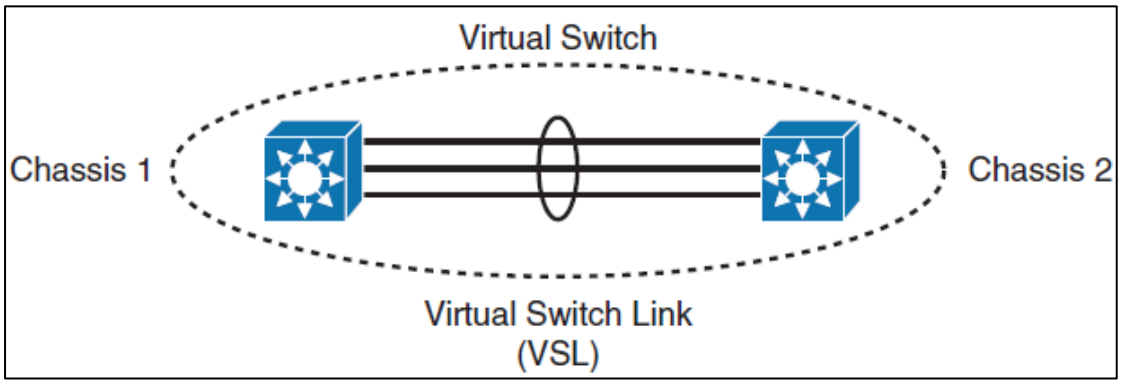


- When you create or restart a VSS, the peer chassis negotiate their roles. One chassis becomes the **active** chassis, and the other chassis becomes the **standby.**
- The **active chassis controls the VSS.** It runs the Layer 2 and Layer 3 control protocols for the switching modules on both chassis.
- The active chassis also provides management functions for the VSS, such as module online insertion and removal (OIR) and the console interface.

- The **standby chassis** monitors the active chassis using the **VSL.** *(Virtual Switch Link)*. If it detects failure, the standby chassis initiates a switchover and takes on the active role.
- VSS works on Cisco IOS **Stateful Switch Over** (SSO) & **Non-Stop Forwarding** (NSF) technologies.

VSL- Virtual Switch Link:

- To bond the two switches into one logical chassis, the control plane information must be exchanged between the two chassis in a timely manner.
- To facilitate this information exchange, a **dedicated link** is used to transfer both control plane & data plane traffic between the peer chassis**. This link is referred to as the virtual switch link (VSL).**



- Both **control & data traffic** is carried out on this Virtual Switch link.
- All frames that are sent across the VSL are encapsulated with a **Virtual Switch Header (VSH)**, which is added directly before the Ethernet Header to the frame by the **egress port** and stripped off on the other side of the VSL by the **ingress port.**
- It is **32 bytes** long.
- The VSL is implemented as an **EtherChannel** with up to eight links.
- The VSL gives control traffic higher priority than data traffic so that control messages are never discarded.
- The standby chassis monitors the active chassis using the VSL.

Interface Naming Convention:

In VSS mode, interfaces are specified using switch number (in addition to slot and port), because the same slot numbers are used on both chassis. For example, the interface **1/5/4** command specifies port 4 of the switching module in slot 5 of switch 1. The interface **2/5/4** command specifies port 4 on the switching module in slot 5 of switch 2.

Chassis and Modules

Table 4-1 VSS Hardware Requirements

Hardware	Count	Requirements
Chassis	2	All chassis supported with Supervisor Engine 6T in Cisco IOS Release 15.4SY support VSS mode. **Note** The two chassis need not be identical.
Supervisor Engines	2	Either two C6800-SUP6T or two C6800-SUP6T-XLsupervisor engines. The two supervisor engines must match exactly.
Switching Modules	2+	VSS mode support as shown in the Release Notes. In VSS mode, unsupported switching modules remain powered off.

The VSL EtherChannel supports only 40-Gigabit and 10-Gigabit Ethernet ports. The ports can be located on the supervisor engine (recommended) or on one of the following switching modules:

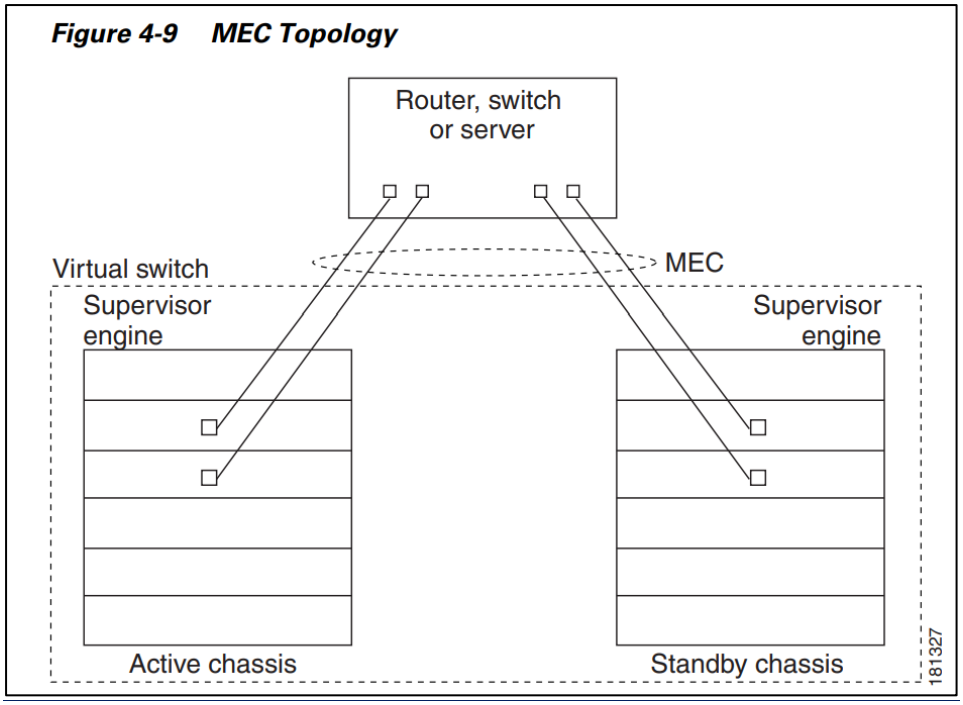
- WS-X6904-40G-2T
- WS-X6908-10GE
- WS-X6816-10T-2T
- WS-X6816-10G-2T
- C6800-32P-10G and C6800-32P-10G-XL
- C6800-16P-10G and C6800-16P-10G-XL
- C6800-8P-10G and C6800-8P-10G-XL

Use any of the 10-Gigabit or 40-Gigabit Ethernet ports on the supervisor engines to create the VSL between the two chassis.

- If you use 10-Gigabit Ethernet ports to form VSL, you can bundle a maximum of **8 links** to the VSL ether channel.
- If you use 40-Gigabit Ethernet ports to form VSL, you can bundle a maximum of **4 links** to the VSL ether channel.

Multichassis EtherChannels:

- A VSS MEC can connect to any network element that supports EtherChannel (such as a host, server, router, or switch)
- An MEC can support up to eight active physical links, which can be distributed in any proportion between the active and standby chassis.



- If a link within the MEC fails (and other links in the MEC are still operational), the MEC redistributes the load among the operational links, as in a regular port.
- If all links to the active chassis fail, the MEC becomes a regular EtherChannel with operational links to the standby chassis.
- If all links fail to the standby chassis, the MEC becomes a regular EtherChannel with operational links to the active chassis.
- If all links in an MEC fail, the logical interface for the EtherChannel is set to unavailable. Layer 2 control protocols perform the same corrective action as for a link-down event on a regular EtherChannel.
- If the standby chassis fails, the MEC becomes a regular EtherChannel with operational links on the active chassis. Connected peer switches detect the link failures and adjust their load-balancing algorithms to use only the links to the active chassis.

Dual-Active Detection:

- If the VSL fails, the standby chassis cannot determine the state of the active chassis.
- To ensure that switchover occurs without delay, the standby chassis assumes the active chassis has failed and initiates switchover to take over the active role.
- If the original active chassis is still operational, both chassis are now active. This situation is **called a dual-active scenario**.
- A dual-active scenario can have adverse effects on network stability.

The VSS supports these following methods for detecting a dual-active scenario:

- **Enhanced PAgP—**Uses PAgP messaging over the MEC links to communicate between the two chassis through a neighbour switch.
- **dual-active fast-hello**—Uses special hello messages over a backup Ethernet connection.
- **dual-homed FEX**—Uses SDP packets over the dual-homed RSL links to communicate between the two chassis.

VSS Initialization:

- A VSS is formed when the two chassis and the VSL link between them become operational.
- The peer chassis communicate over the VSL to negotiate the chassis roles.
- If only one chassis becomes operational, it assumes the active role.
- The VSS forms when the second chassis becomes operational, and both chassis bring up their VSL interfaces.

Virtual Switch Link Protocol:

The VSLP includes the following protocols:

1. **Role Resolution Protocol—**The peer chassis use Role Resolution Protocol (RRP) to negotiate the role (active or standby) for each chassis.
2. **Link Management Protocol—**The Link Management Protocol (LMP) runs on all VSL links, and exchanges information required to establish communication between the two chassis. LMP identifies and rejects any unidirectional links. If LMP flags a unidirectional link, the chassis that detects the condition brings the link down and up to restart the VSLP negotiation. VSL moves the control traffic to another port if necessary.

System Initialization:

- If you boot both **chassis simultaneously,** the VSL **ports** become active, and the chassis will come up as **active and standby**. If priority is configured, the **higher priority** switch becomes **active.**
- If you boot up only **one chassis**, the VSL ports remain inactive, and the chassis comes up as **active**.
- When you subsequently boot up the **other chassis**, the VSL links become active, and the new chassis comes up as **standby**.

How to Configure a VSS:

following prerequisites must be fulfilled.

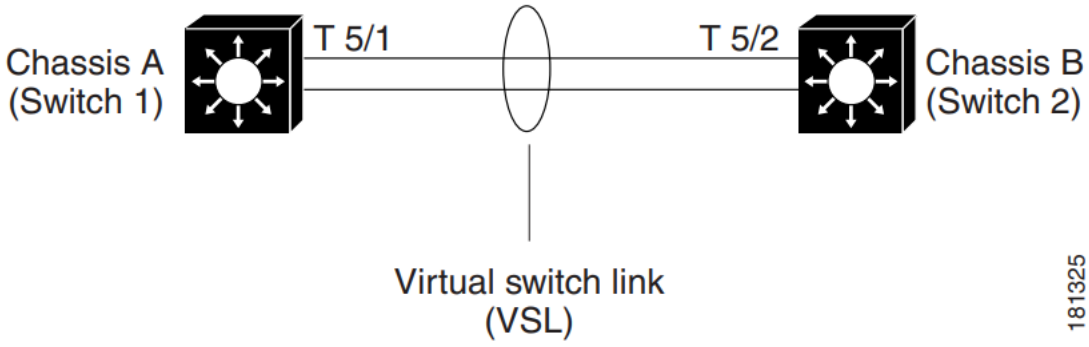
1. Both the switches must be in **standalone** mode.
2. **Easy VSS mode must be enabled** on both the switches.
3. **CDP** should be running between interfaces.

- ✓ The standalone mode is the **default operating** mode (a single chassis switch).
- ✓ VSS mode combines **two standalone switches** into one virtual switching system (VSS).

To convert two standalone chassis into a VSS, perform the following major activities:

- ✓ Save the standalone configuration files.
- ✓ Configure SSO and NSF on each chassis.
- ✓ Configure each chassis as a VSS.
- ✓ Convert to a VSS
- ✓ Configure the peer VSL information.

Figure 4-10 Example VSS



Two chassis, A and B, are converted into a VSS with virtual switch domain 100. 10-Gigabit Ethernet port 5/1 on Switch 1 is connected to 10-Gigabit Ethernet port 5/2 on Switch 2 to form the VSL.

Assigning Virtual Switch Domain and Switch Numbers:

- ✓ Configure the **same virtual switch domain** number on both chassis.
- ✓ The virtual switch domain is a number **between 1 and 255** and must be unique for each VSS in your network.
- ✓ Within the VSS, you must configure one chassis to be switch number 1 and the other chassis to be switch number 2.

Switch 1 Task

	Command	Purpose
Step 1	`Switch-1(config)# switch virtual domain 100`	Configures the virtual switch domain on Chassis A.
Step 2	`Switch-1(config-vs-domain)# switch 1`	Configures Chassis A as virtual switch number 1.
Step 3	`Switch-1(config-vs-domain)# exit`	Exits config-vs-domain.

Switch 2 Task

	Command	Purpose
Step 1	`Switch-2(config)# switch virtual domain 100`	Configures the virtual switch domain on Chassis B.
Step 2	`Switch-2(config-vs-domain)# switch 2`	Configures Chassis B as virtual switch number 2.
Step 3	`Switch-2(config-vs-domain)# exit`	Exits config-vs-domain.

Configuring the VSL Port Channel:

The VSL is configured with a **unique port channel** on each chassis.

Switch 1 Task

	Command	Purpose
Step 1	`Switch-1(config)# interface port-channel 10`	Configures port channel 10 on Switch 1.
Step 2	`Switch-1(config-if)# switch virtual link 1`	Associates Switch 1 as owner of port channel 10.
Step 3	`Switch-1(config-if)# no shutdown`	Activates the port channel.
Step 4	`Switch-1(config-if)# exit`	Exits interface configuration.

Switch 2 Task

	Command	Purpose
Step 1	`Switch-2(config)# interface port-channel 20`	Configures port channel 20 on Switch 2.
Step 2	`Switch-2(config-if)# switch virtual link 2`	Associates Switch 2 as owner of port channel 20.
Step 3	`Switch-2(config-if)# no shutdown`	Activates the port channel.
Step 4	`Switch-2(config-if)# exit`	Exits interface configuration mode.

Configuring the VSL Ports:

- ✓ You must add the VSL physical ports to the port channel.
- ✓ In the following example, 10-Gigabit Ethernet ports 3/1 and 3/2 on Switch 1 are connected to 10-Gigabit Ethernet ports 5/2 and 5/3 on Switch 2.
- ✓ For VSL line redundancy, configure the VSL with at least two ports per chassis.

Switch 1 Task

	Command	Purpose
Step 1	`Switch-1(config)# interface range tengigabitethernet 3/1-2`	Enters configuration mode for interface range tengigabitethernet 3/1-2 on Switch 1.
Step 2	`Switch-1(config-if)# channel-group 10 mode on`	Adds this interface to channel group 10.
Step 3	`Switch-1(config-if)# no shutdown`	Activates the port.

Switch 2 Task

	Command	Purpose
Step 1	`Switch-2(config)# interface range tengigabitethernet 5/2-3`	Enters configuration mode for interface range tengigabitethernet 5/2-3 on Switch 2.
Step 2	`Switch-2(config-if)# channel-group 20 mode on`	Adds this interface to channel group 20.
Step 3	`Switch-2(config-if)# no shutdown`	Activates the port.

Verifying the PFC Operating Mode:

Ensure that the PFC operating mode matches on both chassis.

Switch 1 Task

	Command	Purpose
Step 1	`Switch-1# show platform hardware pfc mode`	Ensures that the PFC operating mode matches on both chassis, to ensure that the VSS comes up in SSO redundancy mode.
Step 2	`Switch-1(config)# platform hardware vsl pfc mode non-xl`	(Optional) Sets the PFC operating mode to PFC4 on Chassis A.

Switch 2 Task

	Command	Purpose
Step 3	`Switch-2# show platform hardware pfc mode`	Ensures that the PFC operating mode matches on both chassis, to ensure that the VSS comes up in SSO redundancy mode.
Step 4	`Switch-2(config)# platform hardware vsl pfc mode non-xl`	(Optional) Sets the PFC operating mode to PFC4 on Chassis B.

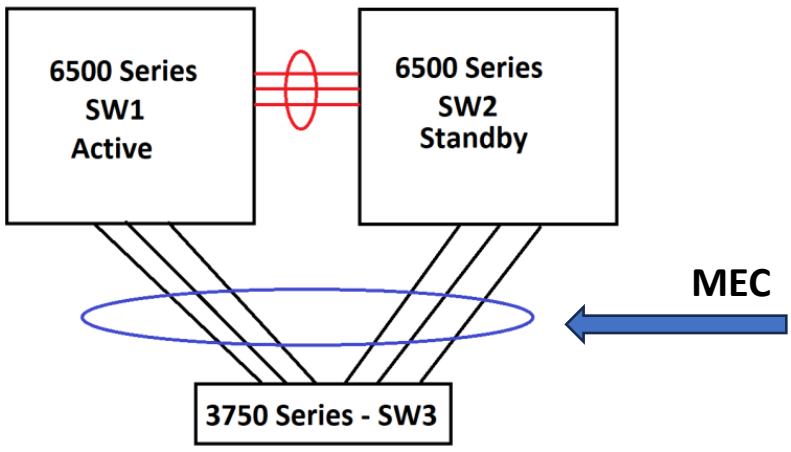
Displaying VSS Information:

Command	Purpose
`show switch virtual`	Displays the virtual switch domain number, and the switch number and role for each of the chassis.
`show switch virtual role`	Displays the role, switch number, and priority for each of the chassis in the VSS.
`show switch virtual link`	Displays the status of the VSL.

```
Router# show switch virtual
Switch mode                   : Virtual Switch
Virtual switch domain number  : 100
Local switch number           : 1
Local switch operational role: Virtual Switch Active
Peer switch number            : 2
Peer switch operational role  : Virtual Switch Standby

Router# show switch virtual role
Switch  Switch Status  Preempt     Priority  Role     Session ID
        Number         Oper(Conf)  Oper(Conf)         Local  Remote
-----------------------------------------------------------------
LOCAL    1     UP      FALSE(N)    100(100)  ACTIVE   0      0
REMOTE   2     UP      FALSE(N)    100(100)  STANDBY  8158   1991

In dual-active recovery mode: No

Router# show switch virtual link
VSL Status: UP
VSL Uptime: 4 hours, 26 minutes
VSL SCP Ping: Pass OK
VSL ICC (Ping): Pass
VSL Control Link: Te 1/5/1
```

Multi-Chassis EtherChannel (MEC):

Multi-chassis EtherChannel (MEC) is a Layer 2 multi-path technology. This form of EtherChannel allows a connected node to terminate the EtherChannel across the two physical Cisco Catalyst 6500/6800 Series.



vPC:

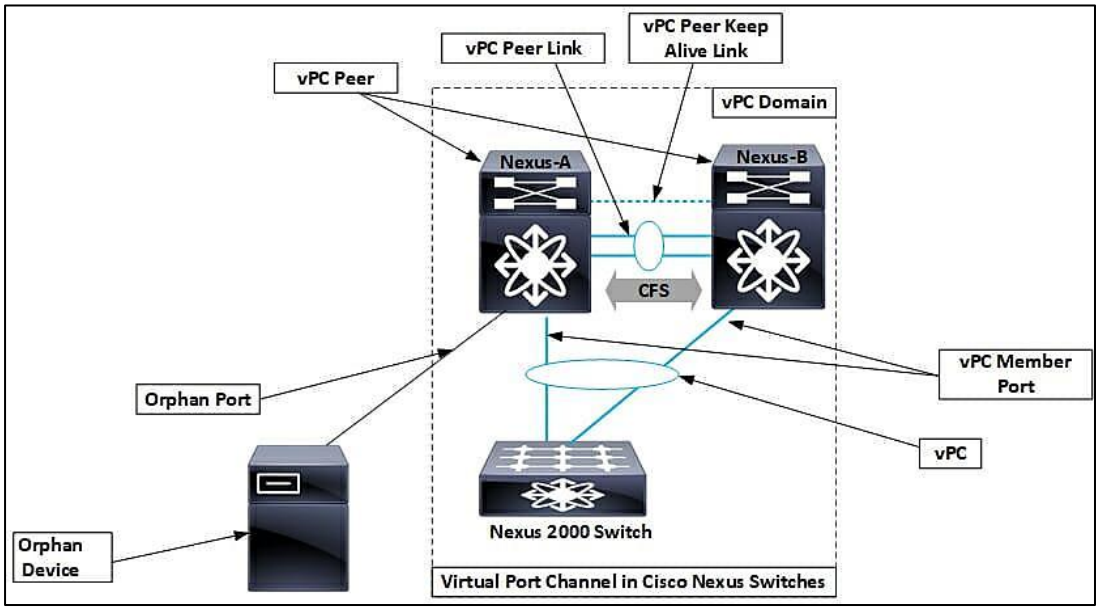
***Before we dive into vPC it is important to quickly review Port-Channels.*
A Port-Channel is a technology that provides a way to ***aggregate (bond) multiple interfaces*** *together. Traffic is then load balanced across each of the connections. ***

Now,

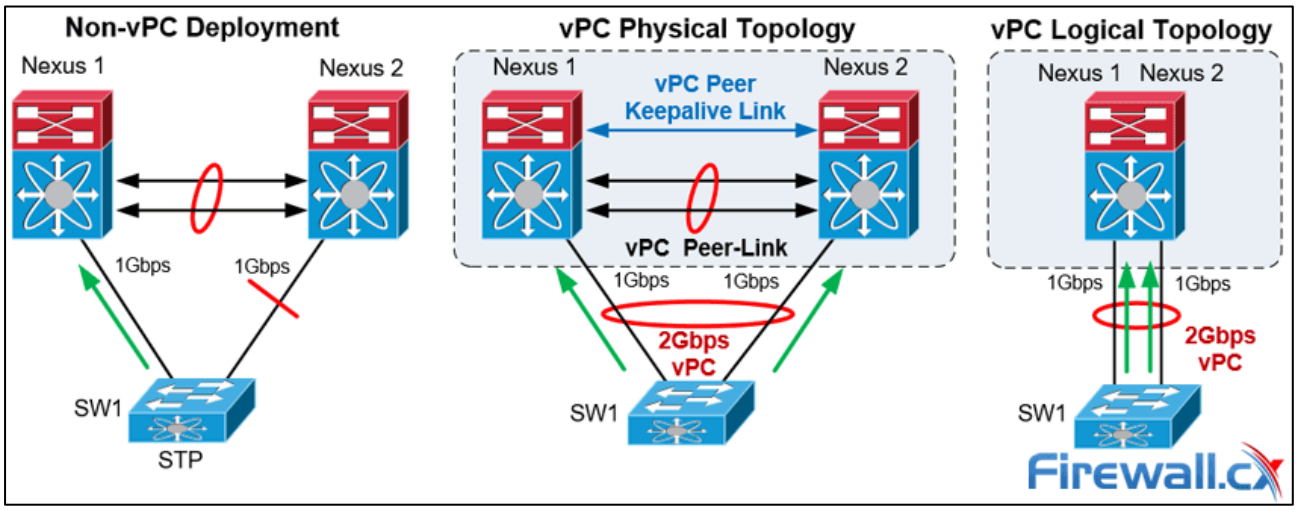
vPC (Virtual Port Channel) technology is a feature provided by Cisco in its **Nexus series switches or Cisco Nexus Fabric Extenders** to appear as a single port channel to a third device. It's a way to create a logical link aggregation between two physical switches, allowing them to appear as a single switch to connected devices.

- ✓ vPC is like Virtual Switch System (VSS) on the Catalyst 6500s switches and **Nexus family** switches.
- ✓ However, the key difference between **vPC and VSS** is that VSS creates a **single logical switch**. This results in a single control plane for both management and configuration purposes.
- ✓ Whereas with **vPC** each switch is managed and **configured independently.**
- ✓ It is important to remember that with vPC **both switches** are managed **independently**.
- ✓ This means you will need to **create and permit** your VLANs on both Nexus switches.

vPC Components:



- **vPC Domain** - Includes the vPC Peers, KeepAlive Links and the Port-Channels that use the vPC technology.
- **vPC Peer Switch** - The other switch within the vPC domain. Each switch is connected via the vPC peer link. It's also worth noting that one device is selected as primary and the other secondary.
- **vPC Member Port** - Ports included within the vPCs.
- **vPC Peer-Keepalive Link** - Connects both vPC peer switches and carries monitoring traffic to/from each peer switch. Monitoring is performed to ensure the switches are both operational and running vPC.
- **vPC Peer Link** - Connects both vPC peer switches and carries BPDUs, HSRPs, and MAC addresses to its vPC peer. In the event of vPC member port failure, it also carries unicast traffic to the peer switch.
- **Orphan Port** - An orphan port is a port that is configured with a vPC VLAN (i.e a VLAN that is carried over the vPC peer link) and is not configured as a vPC member port.



guidelines and recommendations

1. The same type of **Cisco Nexus switches** must be used for **vPC pairing**. It is not possible to configure vPC on a pair of switches consisting of a Nexus 7000 series and a Nexus 5000 series switch. **vPC is not possible between a Nexus 5000 and Nexus 5500 switches.**
2. The **vPC peers** must run **the same NX-OS** version except during the non-disruptive upgrade, that is, In-Service Software Upgrade (ISSU).
3. The **vPC Peer-Link** must consist of at least **two 10G Ethernet** ports in dedicated mode. Utilizing Ethernet ports from two different modules will improve the availability and redundancy should a module fail. Finally the use of 40G or 100G interfaces for vPC links will increase the bandwidth of the vPC Peer-Link.

4. **vPC keepalive link must be separate from the vPC Peer-Link**.
5. vPC can be configured in multiple VDCs, but the configuration is entirely independent. Each VDC for the Nexus 7000 Series switches requires its own vPC peer and keepalive links and cannot be shared among the VDCs.
6. The maximum number of switches in a **vPC domain is two.**
7. The maximum number of **vPC peers per switch or VDC is one.**
8. When Static routing from a device to vPC peer switches with next hop, FHRP virtual IP is supported.
9. Dynamic routing adjacency from vPC peer switches to any Layer3 device connected on a vPC is not supported. It is recommended that routing adjacencies are established on separate routed links.
10. vPC member ports must be on the same line card type e.g. M2 type cards at each end.

VSS vs VPC:

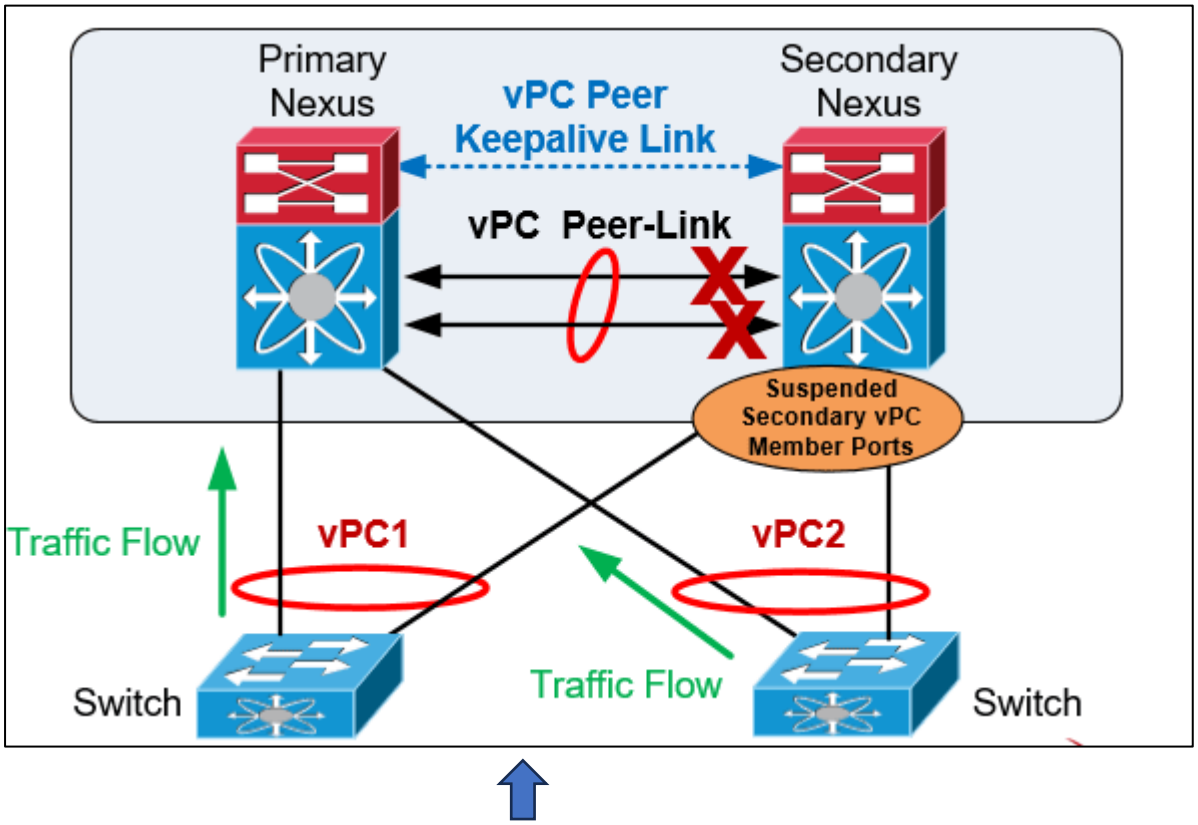
Features	Cisco VSS	Cisco vPC
Control Plane	1 Control Plane for both the Switches in VSS	Every Switch in vPC has its own Control Plane, So 2 Control Plane
Data Plane	1 Data Plane	1 Data Plane
Network Environment	Enterprise Networks	Data-Center Infrastructure
Switches	Calayst Switches	Nexus Switches
Switch Specifications	Cisco 4500, Cisco 6500 and Cisco 6800	Nexus 3K, 5K, 6K and Nexus 7K devices
Peer Link Bandwidth	10 Gbps	10 Gbps
Link Bundles	8	8,16,32 depends upon the Scenario
L2 Etherchannel	Yes	Yes
L3 Etherchannel	Yes	No
FHRP required	No	Yes
Dual Brain Scenario	PAgP+, BFD and Fast-Hello	vPC-Keepalive link
ISSU	Yes	Yes
SSO	Yes	Yes
NSF	Yes	Yes

VPC Peer-Link Design Guidelines:

- Member ports must be at **least 10GE interfaces.**
- Use only point-to-point without other devices between the vPC peers (Nexus switches). E.g. transceivers, microwave bridge link, etc.
- Use **at least two 10Gbps links spread between two separate** I/O module cards at each switch for best resiliency.
- The ports should be in **dedicated mode** for the oversubscribed modules.

- vPC Peer-Link ports should be located on a different I/O module than that used by the Peer Keepalive Link.

VPC Failure Scenario: VPC Peer-Link Failure:

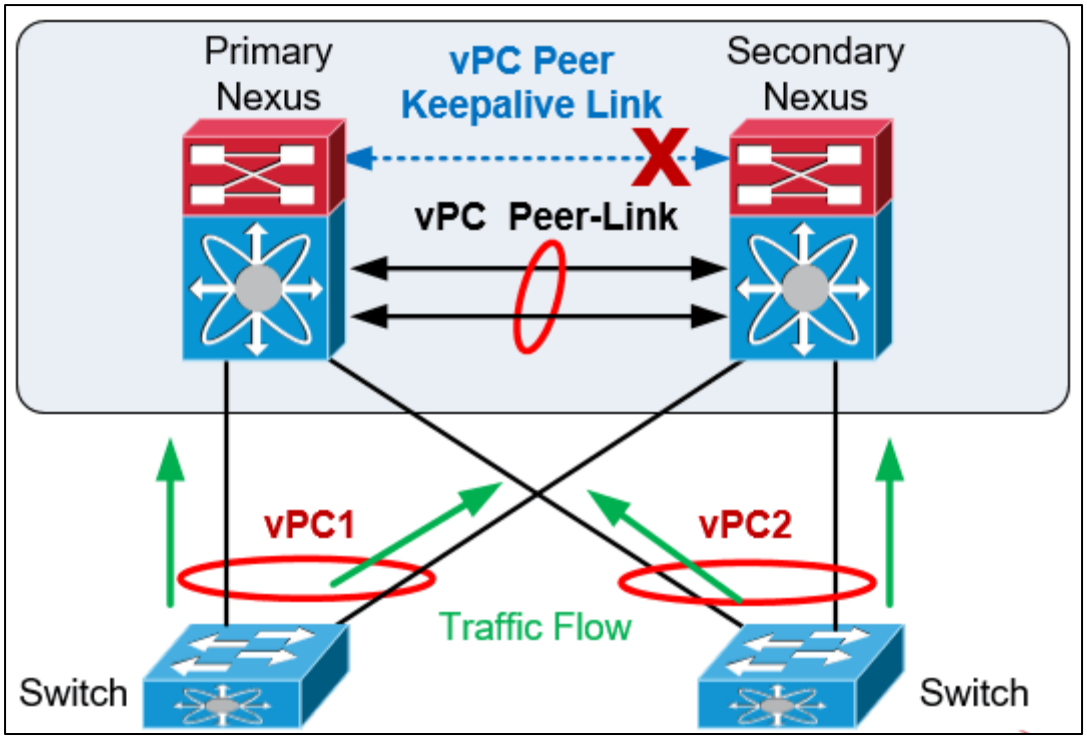


In the scenario the** vPC Peer-Links on the Secondary Nexus fail **the status of the** peer vPC **is examined using the** Peer Keepalive Link**:

If both vPC peers are active, the secondary vPC *(i.e. the switch with the higher priority)* disables all the vPC member ports to avoid uncertain traffic behavior and network loops which can result in service disruption.

At this point traffic continues flowing through the Primary vPC without any disruptions.

VPC Failure Scenario: VPC Peer Keepalive Link Failure

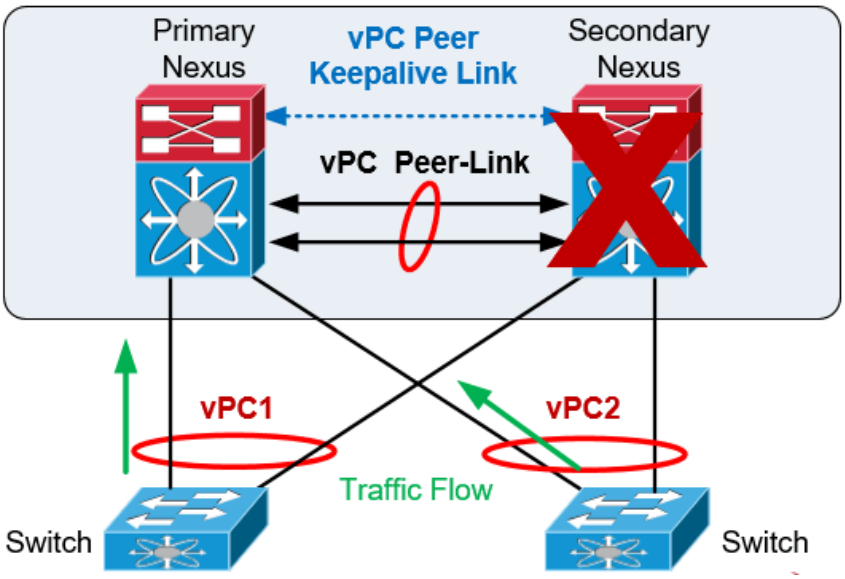


*In the event the **Peer Keepalive Link** fails it will not have a negative effect on the operation of the vPC, which will continue forwarding traffic. The **Keepalive Link** is used as a **secondary test** mechanism to confirm the **vPC peer** is live in case the **Peer-Link** goes down:*

1. During a **Keepalive Link** failure there is no change of roles between the vPC (primary/secondary) and no down time in the network.

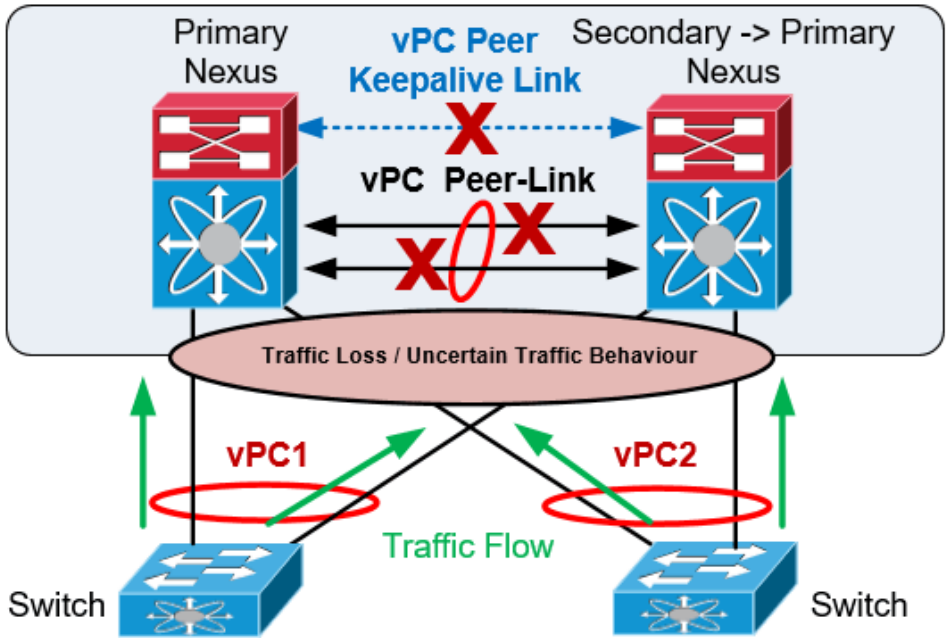
2. As soon as the **Keepalive Link** is restored the vPC will continue to operate.

VPC Failure Scenario: VPC Peer Switch Failure



In the case of a **vPC peer switch total failure**, the remote switch learns from the failure via the **Peer Keepalive link** since no keepalive messages are received. The data traffic is forwarded by utilizing the remaining links til the failed switch recovers. It should be noticed that the **Keepalive messages** are used only when all the links in the **Peer-Link** fail:

VPC Failure Scenario: Dual Active or Split Brain



- ✓ The **Dual-Active** or **Split Brain** vPC failure scenario occurs when the **Peer Keepalive Link** fails followed by the **Peer-Link**. Under this condition both switches undertake the **vPC primary roles**.

- ✓ If this happens, the **vPC primary switch** will **remain** as the **primary** and the **vPC secondary switch** will become **operational primary** causing severe network instability and outage:

Cisco Nexus VPC Configuration Example

- we used two **Nexus 5548** data centre switches.

- two Nexus 5548 were given hostnames **N5k-Primary** & **N5k-Secondary**

Step 1: Enable the vPC Feature and Configure the vPC Domain ID on Both Switches

```
N5k-Primary(config)# feature vpc

N5k-Primary(config)# vpc domain 1

N5k-Primary(config-vpc-domain)# show vpc role

vPC Role status

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

vPC role                          : none established

Dual Active Detection Status      : 0

vPC system-mac                    : 00:23:04:ee:be:01

vPC system-priority               : 32667

vPC local system-mac              : 8c:60:4f:2c:b3:01

vPC local role-priority           : 0
```

Now we configure the Nexus Secondary switch using the same commands:

```
N5k-Secondary(config)# feature vpc

N5k-Secondary(config)# vpc domain 1

N5k-Secondary(config-vpc-domain)# show vpc role

vPC Role status

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

vPC role                          : none established

Dual Active Detection Status      : 0

vPC system-mac                    : 00:23:04:ee:be:01

vPC system-priority               : 32667

vPC local system-mac              : 8c:60:4f:aa:c2:3c

vPC local role-priority           : 0
```

Step 2: Choose a Peer Keepalive Deployment Option

On the first switch we create **VLAN 23 with an SVI** (assign an IP address to the VLAN interface) and make it a member of the **VRF instance** created for this purpose. We complete the configuration by assigning **Ethernet 1/32** to **VLAN 23**:

```
N5k-Primary(config)# vlan 23

N5k-Primary(config-vlan)# name keepalive

N5k-Primary(config)# vrf context keepalive

interface Vlan23

  vrf member keepalive

  ip address 192.168.1.1/24

interface Ethernet1/32

  switchport access vlan 23

  speed 1000

  duplex full
```

We follow the same configuration steps on our Secondary Nexus switch:

```
N5k-Secondary (config)# vlan 23

N5k-Secondary(config-vlan)# name keepalive

N5k-Secondary(config)# vrf context keepalive


interface Vlan23

  vrf member keepalive

  ip address 192.168.1.2/24


interface Ethernet1/32

  switchport access vlan 23

  speed 1000

duplex full
```

The ping connectivity test between the Peer Keepalive Links is successful:

```
N5k-Secondary# ping 192.168.1.1 vrf keepalive

PING 192.168.1.1 (192.168.1.1): 56 data bytes

36 bytes from 192.168.1.2: Destination Host Unreachable

Request 0 timed out

64 bytes from 192.168.1.1: icmp_seq=1 ttl=254 time=3.91 ms

64 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=3.05 ms

64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=1.523 ms

64 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=1.501 ms
```

Step 3: Establish the vPC Peer Keepalive Link

By default, the **vPC Peer Keepalive packets** are routed in the **management VRF** and use the **Out-Of-Band** (**OOB**) **mgmt interface**.

It is, however, highly recommended to configure the **vPC Peer Keepalive link** to **use a separate VRF instance** to ensure that the peer keepalive *traffic is always carried on that link and never on the **Peer-Link***.

```
N5k-Primary(config)# vpc domain 1

N5k-Primary (config-vpc-domain)# peer-keepalive destination
192.168.1.2 source 192.168.1.1 vrf keepalive
```

Configuration of the Secondary vPC follows:

```
N5k-Secondary(config)# vpc domain 1

N5k-Secondary(config-vpc-domain)# peer-keepalive destination
192.168.1.1 source 192.168.1.2 vrf keepalive
```

We can verify the status of the **vPC Peer Keepalive Link** using the **show vpc peer-keepalive** command on both switches:

```
N5k-Primary# show vpc peer-keepalive

vPC keep-alive status            : peer is alive

--Peer is alive for              : (95) seconds, (201) msec

--Send status                    : Success

--Last send at                   : 2017.06.22 23:03:50 720 ms

--Sent on interface              : Vlan23

--Receive status                 : Success

--Last receive at                : 2017.06.22 23:03:50 828 ms

--Received on interface          : Vlan23

--Last update from peer          : (0) seconds, (201) msec
```

```
vPC Keep-alive parameters
--Destination                  : 192.168.1.2
--Keepalive interval           : 1000 msec
--Keepalive timeout            : 5 seconds
--Keepalive hold timeout       : 3 seconds
--Keepalive vrf                : keepalive
--Keepalive udp port           : 3200
--Keepalive tos                : 192
```

Verifying the status of the **vPC Peer Keepalive Link** on our Secondary switch:

```
N5k-Secondary# show vpc peer-keepalive
vPC keep-alive status          : peer is alive
--Peer is alive for            : (106) seconds, (385) msec
--Send status                  : Success
--Last send at                 : 2017.06.22 22:46:32 106 ms
--Sent on interface            : Vlan23
--Receive status               : Success
--Last receive at              : 2017.06.22 22:46:32 5 ms
--Received on interface        : Vlan23
--Last update from peer        : (0) seconds, (333) msec
vPC Keep-alive parameters
--Destination                  : 192.168.1.1
--Keepalive interval           : 1000 msec
--Keepalive timeout            : 5 seconds
--Keepalive hold timeout       : 3 seconds
```

```
--Keepalive vrf                 : keepalive
--Keepalive udp port            : 3200
--Keepalive tos                 : 192
```

Step 4: Configure the vPC Peer-Link

First, we need to **enable** the **lacp feature** then create our high-capacity port channel between the two switches to carry all necessary traffic.

The interfaces **Eth1/2** and **Eth1/3** are selected to become members of the **vPC Peer-Link** in LACP mode. In addition, the **vPC** is 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. **VLAN 10** has been created and allowed on the **vPC Peer-Link**:

```
N5k-Primary (config)# feature lacp
N5k-Primary(config)# interface ethernet 1/2-3
N5k-Primary(config-if-range)# description *** VPC PEER LINKS ***
N5k-Primary(config-if-range)# channel-group 23 mode active
N5k-Primary(config)# vlan 10
N5k-Primary(config)# interface port-channel 23
N5k-Primary(config-if)# description *** VPC PEER LINKS ***
N5k-Primary(config-if)# switchport mode trunk
N5k-Primary(config-if)# switchport trunk allowed vlan 10
N5k-Primary(config-if)# vpc peer-link
N5k-Primary(config-if)# spanning-tree port type network
```

An identical configuration follows for our Secondary switch:

```
N5k-Secondary(config)# feature lacp
```

```
N5k-Seondary(config)# interface ethernet 1/2-3

N5k-Secondary(config-if-range)# description *** VPC PEER LINKS
***

N5k-Secondary(config-if-range)# channel-group 23 mode active

N5k-Seondary(config)# vlan 10

N5k-Secondary(config)# interface port-channel 23

N5k-Secondary(config-if)# description *** VPC PEER LINKS ***

N5k-Secondary(config-if)# switchport mode trunk

N5k-Secondary(config-if)# switchport trunk allowed vlan 10

N5k-Secondary(config-if)# vpc peer-link

N5k-Secondary(config-if)# spanning-tree port type network
```

We can perform a final check on our vPC using the **show vpc** command:

```
N5k-Primary# show vpc

Legend:

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

vPC domain id                     : 1

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                          : primary

Number of vPCs configured         : 0

Peer Gateway                      : Disabled
```

```
Dual-active excluded VLANs        : -

Graceful Consistency Check        : Enabled

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

vPC Peer-link status

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

id   Port   Status Active vlans

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

1    Po23   up     10
```

References:

https://www.firewall.cx/cisco/cisco-data-center/introduction-nexus-family-nx-os-ios-differences.html

https://www.firewall.cx/cisco/cisco-data-center/nexus-vpc-configuration-design-operation-troubleshooting.html