Describe vPC Architecture
The vPC architecture comprises components such as vPC links, vPC peers, and domain IDs.

The vPC architecture consists of the following components:

vPC peers: The core of the vPC architecture is a pair of Cisco Nexus switches. This pair of switches acts as a single logical switch, which allows other devices to connect to the two chassis.

vPC domain: The vPC domain includes the two vPC peer devices, the vPC peer-keepalive link, the vPC peer link, and all the port channels in the vPC domain that are connected to the downstream devices. A numerical vPC domain ID identifies the vPC. You can have only one vPC domain ID on each device.

vPC peer-keepalive link: The peer-keepalive link is a logical link that often runs over an out-of-band network. It provides a Layer 3 communications path that is used as a secondary test to determine if the remote peer is operating properly. No data or synchronization traffic is sent over the vPC peer-keepalive link, only IP packets that indicate that the originating switch is operating and running a vPC. The peer-keepalive status is used to determine the status of the vPC peer when the vPC peer link goes down. In this scenario, the vPC peer-keepalive link helps the vPC switch to determine if the peer link itself failed, or if the vPC peer failed entirely. The peer-keepalive link must be operational before the vPC peer link can come online.

vPC peer link: This link is used to synchronize states between the vPC peer devices. The two ends must be on 10 GE or 40 GE interfaces. This link is used to create the illusion of a single control plane. It forwards BPDUs and LACP packets to the primary vPC switch from the secondary vPC switch to affect a single control plane.

vPC: A vPC is a combined port channel that spans the two vPC peer switches. The downstream device that is connected on the vPC sees the vPC peer switches as a single logical switch. The downstream device is not required to support the vPC itself. It connects to the vPC peer switches using a regular port channel, which can be statically configured or negotiated through LACP.

vPC member port: A member port is a port on one of the vPC peers that is a member of one of the vPCs that is configured on the vPC peers.

vPC VLAN: This VLAN is carried over the peer link and used to communicate via vPC with a peer device.

Non-vPC VLAN: This VLAN is not carried over the peer link.

Orphan device: This term refers to a device that is connected to a vPC domain using regular links instead of connecting through a vPC. Devices that are connected to one vPC peer are considered as orphan devices. VLANs configured on an orphan device cross the peer link.

Orphan port: This term refers to a switch port that is connected to an orphan device. The term is also used for vPC ports whose members are all connected to a single vPC peer. This situation can occur if a device that is connected to a vPC loses all its connections to one of the vPC peers. A non-vPC interface on a switch where other ports in the same VLAN are configured as vPC interfaces is also an orphan port.

Cisco Fabric Services: The Cisco Fabric Services protocol is a reliable messaging protocol that is designed to support rapid stateful configuration message passing and synchronization. The vPC peers use the Cisco Fabric Services protocol to synchronize data plane information and implement necessary configuration checks. vPC peers must synchronize the Layer 2 forwarding table between the vPC peers.

The following are the general guidelines to follow when deploying a vPC topology:

The switches in a vPC domain, the peer switches, must be of the same type. For example, you can connect a pair of Cisco Nexus 9300 series switches; but you cannot connect a Cisco Nexus 9300 series switch to a Cisco Nexus 9500 series switch within a vPC domain. You can connect a pair of Cisco Nexus 9300-EX switches, but you cannot connect a Cisco Nexus 9300-EX switch to a Cisco Nexus 9300-FX switch in a vPC domain.

You must configure the peer-keepalive link and adjacency between peers must be formed before the system can establish the vPC peer link.

You must manually configure both vPC peer devices; the configuration is not sent from one device to the other.

Only Layer 2 port channels can be in vPCs.

You must ensure that all the necessary configuration parameters are compatible on both sides of the vPC peer link.

To accommodate increased traffic when the vPC goes down and traffic needs to cross the peer-link, the best practice is to use multiple high-bandwidth interfaces (such as the 40G interfaces for the Cisco Nexus 9000 switches) across line cards for the peer-link.

Layer 3 over vPC is supported on Cisco Nexus 9000 Series switches for Layer 3 unicast communication only. Layer 3 over vPC is not supported for Layer 3 multicast traffic.

vPC peers must run the same Cisco NX-OS release.