vPC Peer-Gateway:

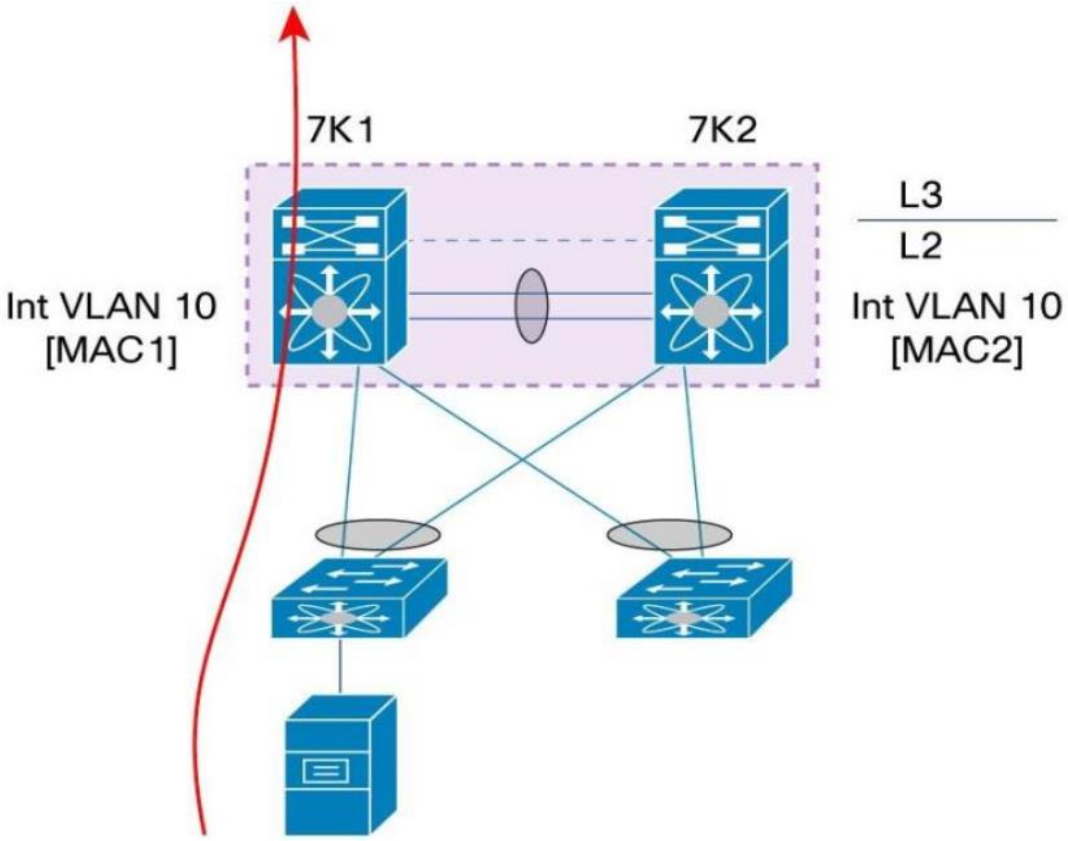
The "Peer-Gateway" feature is a part of VPC and is used to optimize traffic forwarding in certain scenarios. When you have a Nexus VPC configuration with two or more switches, the "Peer-Gateway" feature helps in routing traffic efficiently. It is often used in conjunction with the "peer-link" and "peer-keepalive" features in VPC configurations.

When a Nexus switch in a VPC configuration receives traffic from a downstream device like a server or another switch with the source MAC address belonging to the peer Nexus switch, the default behavior is to drop the traffic because it's seen as a MAC address inconsistency. This is done to prevent MAC address spoofing.

The "Peer-Gateway" feature allows the switch to recognize and accept traffic from the peer Nexus switch's MAC address when it arrives from a downstream device. This prevents traffic from being dropped unnecessarily and optimizes traffic forwarding.

Think of the Cisco Nexus VPC Peer-Gateway as a clever way for two important networking devices to cooperate. It helps them share information effectively and prevents confusion, even if one of them tries to act like the other for a little while. This ensures your network runs smoothly and reliably.

Cisco Nexus VPC Peer-Gateway is a helpful feature that prevents unnecessary confusion and disruptions in a network by making sure traffic gets to the right place, even if it has a mismatched MAC address.



When vPC Peer-Gateway feature is enabled Peer Devices will listen for the SVI MAC of other Peer. It keeps the forwarding of traffic local to the vPC peer device and avoids use of the peer-link. To enable Peer-Gateway feature it has no traffic impact. It was designed for devices like NAS that do not follow the standard ARP process to retrieve MAC of the gateway or F5 Load balancer which uses the source MAC for return traffic to keep the path symmetrical. You can configure vPC peer devices to act as the gateway even for packets that are destined to the vPC peer device's MAC address.

In some cases, like NAS servers, Servers with particular teaming technique might not send the any ARP request to discover gateway MAC address rather they use the MAC address received on the original request to build its response and NAS would reply to client request and these reply will be directed to SVI MAC address and not to HSRP VMAC address. Due to this it can create the undesired traffic flow in vPC.

This issue can be solved easily by Peer-gateway command under vPC Domain. If both vPC peer is configured with this command each of them can route packet out to vPC port.