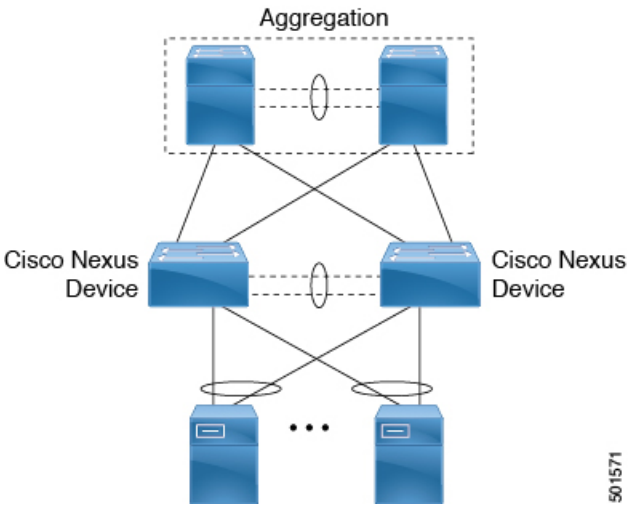
Minimizing the Impact of a Disruptive Upgrade

A non-ISSU upgrade is a disruptive upgrade that results in the reload of the Cisco Nexus device and the Fabric Extenders. The reload is a cold reboot that brings down the control plane and the data plane. The reload causes disruptions to the connected servers and hosts. When a vPC is deployed in the access layer, it is possible to minimize the impact of a non-ISSU upgrade. When one of the vPC switches is being reset during the upgrade process, all the server traffic can flow through its vPC peer.

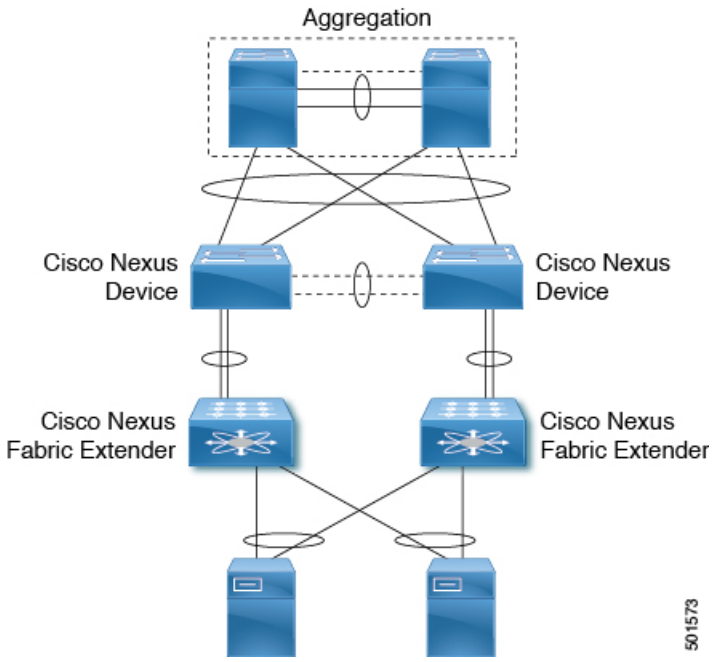
Upgrading a Direct vPC or a Single-Homed FEX Access Layer

The following figures show topologies in which the access layer includes a vPC configuration to hosts or downstream switches.

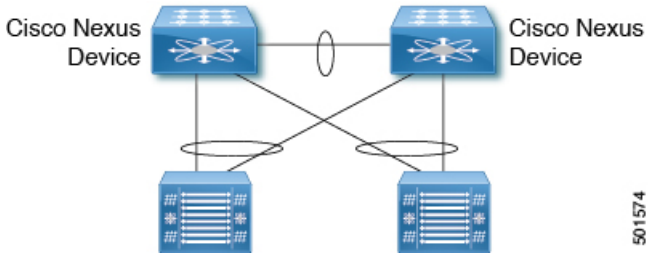
Hosts Directly Connected to vPC Peers



vPC Peered Dual-Supervisor Virtual Modular System Single-Homed FEXes



Cisco Nexus Device Connected to Downstream Switches



To upgrade the access layer without a disruption to hosts, follow these tasks:

- Upgrade the first vPC switch (vPC primary switch). During this upgrade, the switch is reloaded. When the switch is reloaded, the servers or the downstream switch detects a loss of connectivity to the first switch and starts forwarding traffic to the second (vPC secondary) switch.
- Verify that the upgrade of the switch has completed successfully. At the completion of the upgrade, the switch restores vPC peering, connected Nexus 2000 FEXes, and all the links.
- Upgrade the second switch. Repeating the same process on the second switch causes the second switch to reload during the upgrade process. During this reload, the first (upgraded) switch forwards all the traffic to/from servers.
- Verify that the upgrade of the second switch has completed successfully.

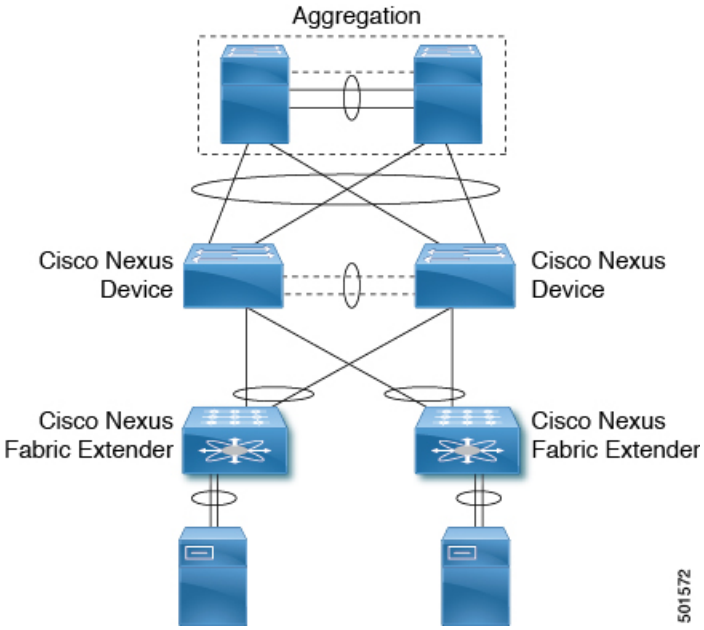
Note Flows that are forwarded to a switch during an upgrade on the switch will failover to the second switch. Also, flows are redistributed when vPC peers are active. The traffic disruption is limited to the time required for the server or host to detect the link-down and link-up events and to redistribute the flows.

Upgrading a Dual-Homed FEX Access Layer

A disruptive upgrade causes a switch and connected Fabric Extenders (FEX) to reload. The time required for a FEX to reload is less than the time required for a switch to reload. When hosts are connected to a dual-homed FEX, it is possible to keep the traffic disruption of the hosts to the same time as required by the FEX to download the image and reload (depending on the hardware platform it can be anywhere between 10 to 20 minutes), instead of the time required for an upgrade of the entire access layer.

The following figure shows a dual-homed FEX topology in which the access layer includes a vPC configuration to hosts or downstream switches.

vPC-Peered Dual-Supervisor Virtual Modular System Dual-Homed FEXes



The following dual-homed FEX procedure is supported only for an upgrade and not for a downgrade.

Procedure

Step 1 Upgrade the vPC primary switch with the new image. During the upgrade process, the switch is reloaded. When the switch is reloaded, only singled-homed FEXes connected to the switch are reloaded and dual-homed FEXes are not reloaded. Servers connected to the dual-homed FEXes retain network connectivity through the vPC secondary switch.

Step 2 Verify that the upgrade of the vPC primary switch is completed successfully. At the completion of the upgrade, the vPC primary switch restores vPC peering. However, dual-homed FEXes are connected only to the secondary vPC switch.

Note

- The FEX remains online on the vPC secondary switch while the vPC primary switch is reloaded.
- On the vPC primary switch after the upgrade, the FEXes connected to the switch are in active-active mismatch state.

Step 3 On the vPC secondary switch, shut the NIF (FEX uplink). The FEX downloads the new image from the vPC primary switch and it comes online on the newly upgraded switch. The servers connected to the dual-homed FEXes lose connectivity. Bring up the NIF (FEX uplink) on the vPC secondary.

Note
Only the vPC primary switch displays that the FEX is online because the vPC secondary switch does not have the new image. The secondary switch displays the FEX in an active-active version mismatch state.

Step 4 Upgrade the vPC secondary switch with the new image. During the upgrade process, the switch is reloaded. When the switch is reloaded, only singled-homed FEXes connected to the switch are reloaded and dual-homed FEXes are not reloaded.

Step 5 Verify that the upgrade of the vPC secondary switch is completed successfully. At the completion of the upgrade, the vPC secondary switch restores vPC peering. Dual-homed FEXes connect to both the peer switches and start forwarding traffic.