

Understand Nexus 5500 and 5600 Series Switch Replacement Procedure

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Replace a Cisco Nexus 5500 and 5600 Series Switch](#)

[Before You Begin](#)

[Disconnect the Defective Chassis](#)

[Preparation Tasks](#)

[Isolate and Remove the Chassis](#)

[Introduce the Replacement Chassis](#)

[Prepare the Replacement Switch](#)

[Configure the Replacement Switch](#)

[Bring Up the Replacement Switch](#)

[Verify Status](#)

Introduction

This document describes the steps required to perform a Cisco Nexus 5500 and 5600 chassis replacement in a Virtual Port Channel (vPC) environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Nexus operating system CLI
- vPC rules

Components Used

The information in this document is based on these software and hardware versions:

- Software 7.3(13)N1(1)
- Hardware 5672UP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Replace a Cisco Nexus 5500 and 5600 Series Switch

When you replace a Cisco Nexus 5500 and 5600 Series switch in an environment, it is recommended you adhere to this procedure in order to ensure there is minimal or no outage.

Before You Begin

1. Once the Return Material Authorization (RMA) for the replacement chassis is processed, and the serial number for the chassis to be shipped is available, open a case with the licensing team in order to get the license rehosted to the new chassis.
2. Ensure a backup of the latest running configuration of the device is available on a USB drive or a File Transfer Protocol (FTP) server.
3. Have multiple connectivity tests ready, so these can be validated post-replacement. These tests must be confirmed to be working fine before the replacement, so they can be used as a reference if any issues are encountered post-replacement.

Disconnect the Defective Chassis

Preparation Tasks

In certain cases, a replacement is needed due to partial and not complete failure of a chassis. In these scenarios, additional steps can be taken in order to ensure the removal of the chassis does not cause a major impact.

1. Back up the running configuration of the device on a USB drive, FTP, Secure FTP (SFTP), or Trivial FTP (TFTP) server.
2. Identify all devices that are connected via orphan ports with the command `show vpc orphan-ports`. Connectivity loss is experienced on these devices once the chassis is disconnected, consider moving those connections to the VPC peer if critical services are running on those.
3. Plan to failover any active firewall/load balancer/similar devices that are running on the device to its VPC peer.
4. Gather the command output shown in this list from both Nexus switches in the VPC domain, so these can be used post-implementation in order to validate the correct status:

- **show version**
- show module
- show inventory
- show running-config
- show running switch-profile
- show int status
- show cdp neighbors
- show port-channel summary
- show vlan sum
- show span sum
- show vpc
- show vpc role
- show ip int brief vrf all
- show trunk
- show ip route vrf all
- show ip arp vrf all
- show mac address-table

Isolate and Remove the Chassis

Complete these steps on the switch to be replaced:

1. Establish a console for the Nexus. Ensure all terminal output is saved, so this can be used as a reference if any issues arise.
2. Shut down all south-facing vPC links, including uplinks to A/A FEXs. Check `show port-channel summary` and `show vpc` in order to ensure they are down.
3. Shut down all orphan ports, including uplinks to straight-through FEXs and physical L3 links. Check `show port-channel summary` and `show interface status` in order to ensure they are down.
4. Shut down all north-facing (core) vPC links. Check `show port-channel summary` and `show vpc` in order to ensure they are down.
5. Shut down the Peer Keep Alive (PKA) link. Check `show vpc peer-keepalive` and `show vpc` in order to ensure it is down.

```
<#root>
```

```
N5K-5672UP-1# show vpc peer-keepalive
```

```
vPC keep-alive status           : peer is not reachable through peer-keepalive
```

```
--Send status                   : Success  
--Last send at                  : 2023.10.04 01:31:09 824 ms  
--Sent on interface             :
```

```
--Receive status                : Failed
```

```
--Last update from peer        : (16) seconds, (360) msec
```

```
vPC Keep-alive parameters
```

```
--Destination                   : 10.82.138.244  
--Keepalive interval            : 1000 msec  
--Keepalive timeout             : 5 seconds  
--Keepalive hold timeout        : 3 seconds  
--Keepalive vrf                 : management  
--Keepalive udp port            : 3200  
--Keepalive tos                 : 192
```

```
<#root>
```

```
N5K-5672UP-1# sh vPC
```

```
Legend:
```

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

```
vPC domain id                   : 100  
Peer status                     : peer adjacency formed ok
```

```
vPC keep-alive status           : peer is not reachable through peer-keepalive
```

```
Configuration consistency status : success  
Per-vlan consistency status      : success  
Type-2 consistency status       : success  
vPC role                         : secondary  
Number of vPCs configured       : 49
```

```
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Operational Layer3 Peer-router : Disabled
Auto-recovery status : Enabled (timeout = 240 seconds)
```

vPC Peer-link status

```
-----
id  Port  Status Active vlans
--  ---  -----
1   Po100 up      1
```

Then, from the vPC peer (switch not being replaced), shut down the vPC peer link. Check `show vpc` in order to ensure it went down, and also ensure this switch has either the vPC role of primary or secondary, operational primary.

<#root>

N5K-5672UP-1# sh vPC

Legend:

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

vPC domain id : 100

Peer status : peer link is down

vPC keep-alive status : peer is not reachable through peer-keepalive

Configuration consistency status : success

Per-vlan consistency status : success

Type-2 consistency status : success

vPC role : secondary, operational primary

Number of vPCs configured : 49

Peer Gateway : Disabled

Dual-active excluded VLANs : -

Graceful Consistency Check : Enabled

Operational Layer3 Peer-router : Disabled

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

vPC Peer-link status

```
-----
id  Port  Status Active vlans
--  ---  -----
1   Po100 down  -
```

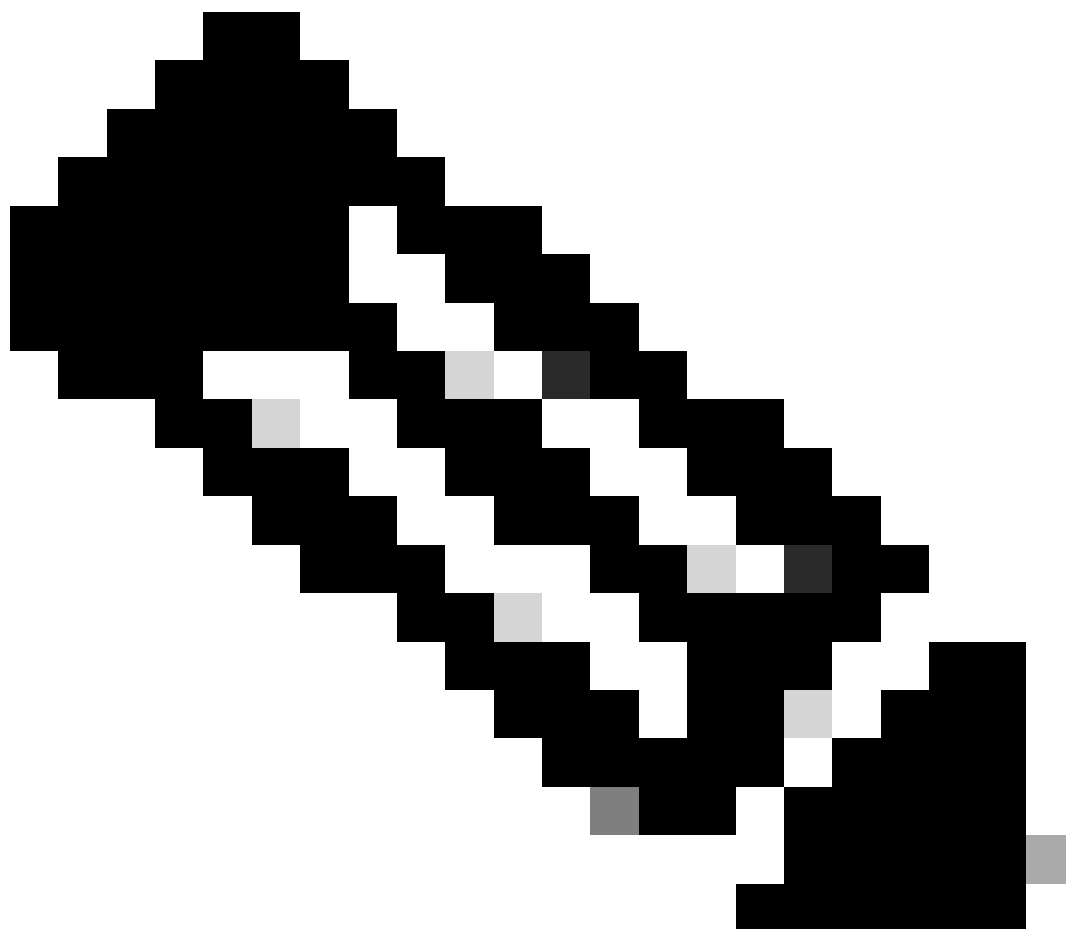
Once the switch to be replaced is completely isolated, confirm there is no connectivity issue in the environment.

After this is completed, power down the switch, unplug the cables and unrack it.

Introduce the Replacement Chassis

Prepare the Replacement Switch

1. Rack the new switch.
 2. Establish a console for the replacement switch. Ensure all terminal output is saved, so this can be used as a reference if any issues arise.
 3. Install the power supplies, fans, and expansion modules if applicable. These components are usually not included in the Return Material Authorization (RMA), so they must be taken from the switch to be replaced.
-



Note: When RMA is processed for a 5548P or 5548UP chassis running Layer 3 services, the Layer 3 I/O module with product ID N55-D160L3 or N55-D160L3-V2 is not included. This Layer 3 (L3) module must be taken from the chassis in order to be replaced and put into the replacement switch. The process of removing and installing the L3 module can be found in the [Cisco Nexus 5000 Series Hardware Installation Guide](#), section **Replacing an I/O Module for a Cisco Nexus 5548 Switch**.

4. Power on the switch.
5. Copy the required system and kickstart images, configuration backup, and licenses to the switch

bootflash.

6. Load the corresponding software version on the switch.

7. Install the license for the chassis obtained in Step 1. in the [Before You Begin](#) section.

Configure the Replacement Switch

1. If breakout is used, apply this configuration to the corresponding interfaces and reload the chassis or expansion module as needed.

2. If FEXs are used, provision the corresponding FEX modules by using [Module Pre-Provisioning](#).



Warning: If using dual-homed FEXs, you must ensure that the FEXs modules are provisioned on the replacement chassis before bringing their links up. After this, ensure to configure all FEX server ports the same as the VPC peer. Failing to accomplish this can cause the FEX server ports to move to the inactive state.

3. If configuration sync is used, use the `show run switch-profile` obtained from Step 4. in [Preparation tasks if the switch to be replaced is still connected to the network](#) in order to restore the switch-profile configuration. If switch-profile backup is not available, you can retrieve it from the VPC peer by executing the `show run switch-profile` on that one. Switch-profile configuration must be identical on both

VPC peers, except for the `sync-peers destination [ip address]` command.

- In order to restore the switch-profile configuration, enter the `config sync` in the terminal, and then `switch-profile [name]`.
 - Paste the switch-profile backup configuration, then run `verify` and `commit` for the changes to be applied.
 - Confirm switch-profile configuration is identical on both switches, by checking `show run switch-profile` on both vPC peers.
4. Copy the remainder of the backup configuration (except for the switch-profile configuration) by issuing `copy bootflash:[backup config] running-config:`.
 5. Verify that the `show running-config` is consistent with the backup.
 6. Ensure all ethernet interfaces are shutdown, so these can be brought up in a controlled manner. Mgmt0 and Switched VLAN Interfaces (SVIs) can remain in the admin-up state.
 7. Save the configuration to startup by issuing `copy running-config startup-config`.
 8. Connect the mgmt0 and ethernet ports, including FEX ports.

Bring Up the Replacement Switch

1. Confirm mgmt0 port is up.
2. Bring up the vPC peer-keepalive link. Check `show interface status`, `show vpc peer-keepalive`, and `show vpc` in order to ensure it is up and operational.
3. Ensure that the sticky bit is set to false in the replacement switch. Enter the `show sys internal vpcm info all | i i stick` command in order to check whether the sticky bit is set to false. If the sticky bit is set to true, reapply the already configured vPC role priority. If the sticky bit is still true after this, reload the replacement chassis.

Note: If the sticky bit is set to false on both chassis, configure a higher priority (lower numerical value) on the switch that is connected to the network already and not being replaced.

4. Before bringing up the vPC peer-link, ensure the peer-keepalive is operational, and the vPC role is set to **none established** on the replacement switch:

```
<#root>
```

```
N5K-5672UP-2# sh vPC
```

```
Legend:
```

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

```
vPC domain id           : 100
Peer status              : peer link is down
vPC keep-alive status    : peer is alive
```

```
Configuration consistency status : failed
Per-vlan consistency status      : success
Configuration inconsistency reason: Consistency Check Not Performed
```



```

Type-2 inconsistency reason      : Consistency Check Not Performed
vPC role                        : none established

Number of vPCs configured       : 49
Peer Gateway                    : Disabled
Dual-active excluded VLANs     : -
Graceful Consistency Check     : Disabled (due to peer configuration)
Auto-recovery status           : Enabled (timeout = 240 seconds)

```

vPC Peer-link status

```

-----
id  Port  Status Active vlans
--  ---  -----
1   Po100  down   -

```

5. If any other status is observed in the vPC role, reload the replacement switch one more time with just vPC peer-keepalive operational and all other interfaces in the shutdown state. The vPC peer-keepalive must come up before the auto-recovery timer expires (default 240 seconds) so that the vPC role is set to **none established**. If the vPC keep-alive is configured on an expansion module and takes a long time to boot, causing the auto-recovery timer to expire before it comes up, you can resolve this issue by configuring a higher auto-recovery timer. Use the command `auto-recovery reload-delay 3600` under the vPC domain configuration.



Warning: Do not proceed with the next step until the vPC peer-keepalive is operational and the vPC role is set to **none established**.

-
5. Bring up the vPC peer link. Check `show vpc` in order to ensure it is up, and confirm that the vPC role is established to secondary.
 6. Bring up all north-facing (core) vPC links. Check the `show port-channel summary` and `show vpc` in order to ensure they are up.
 7. Bring up all orphan ports, including uplinks to straight through FEXs, and physical L3 links. Check `show port-channel summary` and `show interface status` in order to ensure they are up.
 8. Bring up all the south-facing vPC links, including uplinks to A/A FEXs. Check `show port-channel summary` and `show vpc` in order to ensure they are up.
 9. Once all interfaces are brought up, verify all vPCs and FEX are operational.
 10. If `switch-profiles/config-sync` is used, enter `config sync` in the terminal, and then `switch-profile [name]`. After this, run `verify` and `commit` in order to ensure the profile is in sync.

Verify Status

Review the command output shown in this list from both Nexus switches in the VPC domain in order to validate the correct status.

- **show version**
- show module
- show inventory
- show running-config
- show running switch-profile
- show switch-profile status
- show int status
- show cdp neighbors
- show port-channel summary
- show vlan sum
- show span sum
- show vpc
- show vpc role
- show ip int brief vrf all
- show trunk
- show ip route vrf all
- show ip arp vrf all
- show mac address-table

Then, confirm the tests performed in Step 3. from [Before You Begin](#) are still working correctly.