Nexus 7000 Chassis Replacement Procedure

Contents

Introduction

This document describes the steps needed to perform a chassis replacement in a Virtual Port Channel (vPC) environment. This scenario occurs due to hardware failure or feature/hardware support limitations.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Nexus operating system CLI
- vPC rules

Components Used

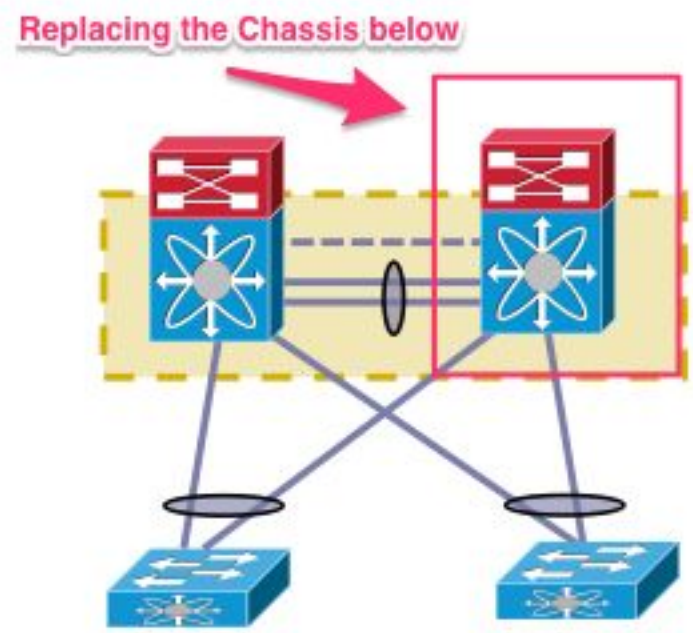
The information in this document is based on these software and hardware versions:

- Supervisor 1 Release 5.2(3a) or later
- Supervisor 2 Release 6.x or later

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, make sure that you understand the potential impact of any command.

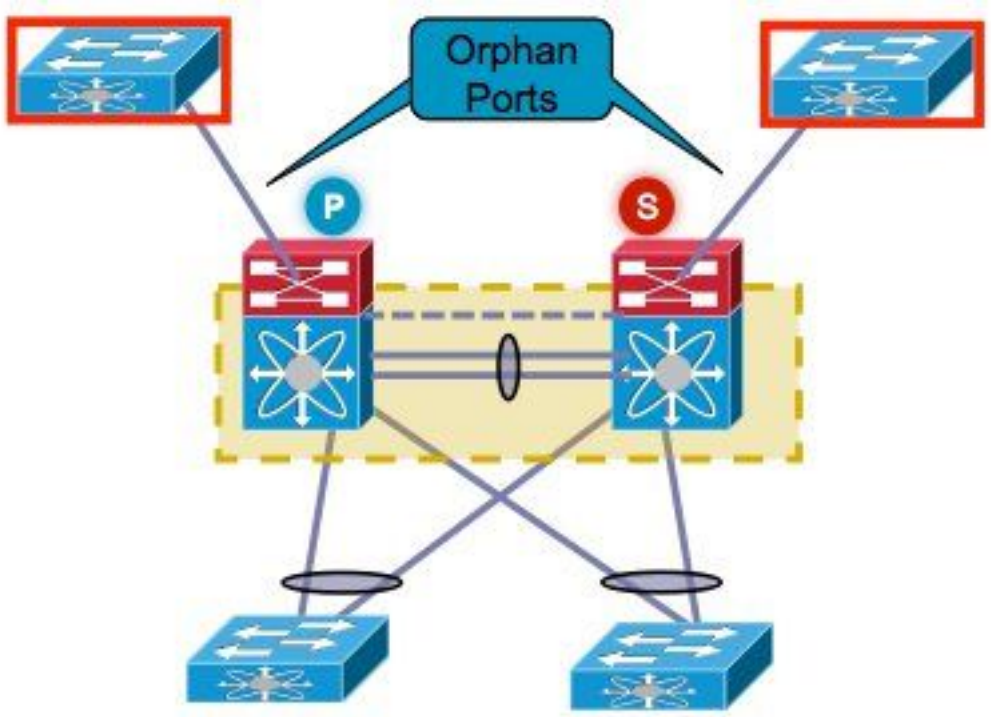
Replace a Cisco Nexus 7000 Series Switch

When you replace a Cisco Nexus 7000 Series switch, you must perform this procedure in order to ensure that there is minimal or no outage. This image illustrates how to replace the chassis.



Before You Begin

1. Once the Return Material Authorization (RMA) for the replacement chassis is created, ensure that a case is opened with the licensing team in order to get the license rehosted on the new chassis. The Licensing team can generate a new license file for the replacement chassis. The generation of new license file does not invalidate the current license on the chassis. Keep the email with the license key.
2. Save the running configuration of all VDCs (Virtual Device Contexts).
3. Back up the running configuration for all VDCs on the bootflash and on a FTP/Secure FTP (SFTP)/TFTP server.
4. Identify that all devices are connected via orphan ports on the target Nexus 7000. Connectivity loss is experienced in case the environment is supported by the orphan ports that do not have a redundant link back into the network.



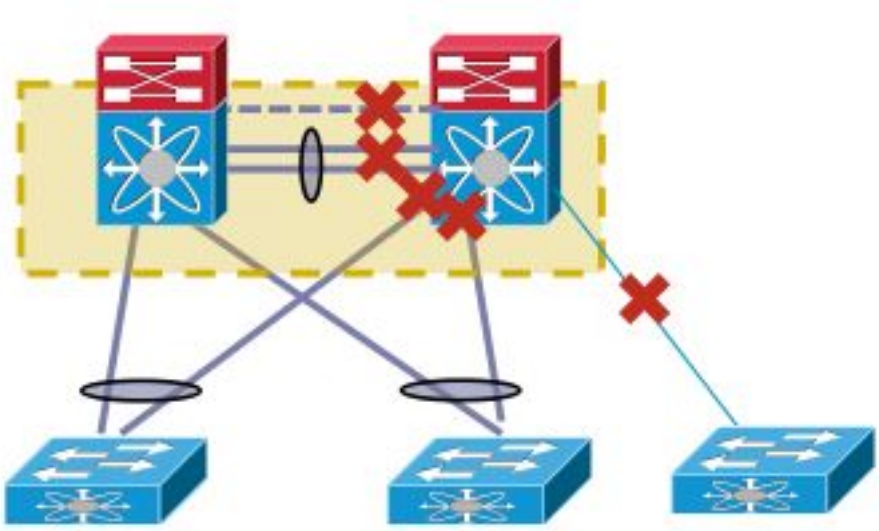
5. Plan to failover any active firewall/load balancer/similar devices that are currently on the target Nexus 7000 to the other Nexus 7000.
6. Gather the command output shown in this list from both Nexus 7000s (save for the post-implementation verification). This has to be completed per VDC also. show versionshow moduleshow inventoryshow vPCshow vPC roleshow port-channel summaryshow span sumshow vlan sumshow running-configshow ip int brief vrf allshow int statusshow cdp neishow trunkpings to specific servers in order to confirm their reachability or use the appropriate Network Management Systems (NMS) toolas per the environment of every customer, the additional command outputs must be captured

Chassis Replacement Window

There are two ways to perform the chassis replacement. Option 1 documents a more controlled approach that provides a customer the ability to perform the steps in phases, but takes more time. A second option is also available. Both the options listed are independent of the vPC role.

Option 1. Phased Approach

1. Shut down all vPC links on the chassis that are replaced. This applies to the VDC in which the vPC is configured.
2. Shut down all the Layer 3 physical links.
3. Shut down all orphan ports.
4. Shut down the Peer Keep Alive (PKA) link.
5. Shut down the peer link. Irrespective of the vPC role, the other side keeps the vPC link up since these steps lead to a dual active scenario.
6. Confirm that there is no connectivity issue.



Complete these steps in order to replace the switch:

1. Power down the target Nexus 7000.
2. Unplug the cables from the modules.
3. Install the new switch.
4. Install the supervisors and modules.
5. Power on the switch.
6. Verify that the supervisor comes up with the correct NX-OS version.

Complete these steps in order to install the license:

1. Install the license for the chassis, obtained in step 1 in the "Before You Begin" section.
2. Copy the configuration from the bootflash to the running configuration.
3. Verify that the configuration is consistent with the backup.

Bring the switch back into production. It is important to check the LACP role and sticky bit before you bring up the interfaces. The next section goes through the steps.

LACP Role Check

When the peer-link comes up between two vPC peers, apart from the vPC roles, the LACP permanent roles are also decided (one peer become the Master, while the other becomes the Slave).

An LACP role election occurs if both peers have same role (either master or slave). The system with the lower MAC address wins as master and this election is not governed by the vPC role priority configuration.

A re-election causes vPC LACP port-channels to re-initialize, which leads to a possible traffic outage.

Enter these commands in order to check the LACP role:

```
show system internal vpcm info all | i "LACP Role"
show system internal vpcm info all | i "LACP Per"
```

Recommendation

Before you introduce an already isolated vPC device back into production, check the LACP roles on both boxes. If the same role, disable auto recovery with **no auto-recovery** under the vPC

domain on both peers and reload the isolated device. After reload, the isolated device comes up with the LACP role 'none established' and can be introduced into the vPC without LACP role re-election.

Sticky Bit Check

Check to ensure that the sticky bit is set to false.

1. Enter the **show sys internal vpcm info all | i i stick** command in order to check whether the sticky bit is set to false.
2. If the sticky bit is set to false, continue to step 5. If the sticky bit is set to true, reconfigure the vPC role priority. This means to reapply the original configuration for the role priority. If the role priority is default, then reapply the default. In this example, the role priority is 2000 and the same value is reapplied.
   ```
   show system internal vpcm info all | i "LACP Role"
   show system internal vpcm info all | i "LACP Per"
   ```
   Note: This step resets the sticky bit from true to false.
3. Enter the **show sys internal vpcm info all | i i stick** command in order to determine if the sticky bit is set to false.
4. If the sticky bit is still true, reload the VDC or chassis.
5. If the sticky bit is false, bring up the PKA and Peer Link (PL).

Example output:

```
N7K# show system internal vpcm info all | i i sticky
        Sticky Master: FALSE
```

Bring Up the Physical Interfaces

1. Bring up the PKA link.
2. Bring up the vPC PL.
3. Confirm that the vPC role is established correctly.
4. Bring up the vPC links one by one by not shutting the interface.
5. Bring up the orphan ports.
6. Bring up the Layer 3 physical interfaces.

Once the steps are completed, verify that there are no connectivity issues.

Take a snapshot of the same outputs gathered earlier and compare for validation.

- show version
- show module
- show inventory
- show vPC
- show vPC role
- show port-channel summary
- show span sum
- show vlan sum
- show running-config
- show ip int brief vrf all
- show int status
- show cdp nei

- show trunk
- pings to specific servers in order to confirm their reachability or use the appropriate NMS tool
- as per the environment of every customer, the additional command outputs must be captured

Option 2. Direct Replacement

The difference between the Direct Replacement and Phased Approach is that the approach of shutting down the individual links is not used in Direct Replacement.

1. Power down the target Nexus 7000.
2. Unplug the cables from the modules.
3. Install the new switch.
4. Install the supervisors and modules.
5. Power on the switch.
6. Verify that the supervisor comes up with the correct NX-OS version.

Complete these steps in order to install the license:

1. Install the license for the chassis. This was obtained in step 1 in the "Before You Begin" section.
2. Copy the configuration from the bootflash to the running configuration.
3. Verify the configuration is consistent with the backup.

Complete these steps in order to bring the switch back into production:

1. Power down the Nexus 7000 again. Connect all the links back on the Nexus 7000.
2. Power it back up. The vPC comes back up after the initial state is established.
3. Take a snapshot of the commands in order to compare them post replacement.

This is similar to a Nexus 7000 reboot, in which the Nexus 7000 is expected to recover seamlessly.

The two approaches laid out have their advantages and disadvantages. Option 1 gives more control at the expense of a longer change window. There is no recommendation as to which approach is the best because it depends on the type of network and the type of application hosted.

How to Ensure the vPC Sticky Bit is Set Correctly

This section explains how to ensure that the vPC sticky bit is set correctly in order to avoid a possible outage when an isolated switch is integrated into the vPC fold.

Complete these steps before you bring up the PKA and PL:

1. Enter the **show sys internal vpcm info all | i i stick** command in order to check whether the sticky bit is set to false.
2. If the sticky bit is set to false, then continue to step 5. If the sticky bit is set to true then reconfigure the vPC role priority. This means to reapply what the original configuration is for the role priority. If the role priority is default, then reapply the default. In this example, the role priority is 2000 and the same value is reapplied.

   ```
   N7K# show system internal vpcm info all | i i sticky
           Sticky Master: FALSE
   ```

   Note: This step resets the sticky bit from true to false.

3. Enter the **show sys internal vpcm info all | i i stick** command in order to determine if the sticky bit is set to false.
4. If the sticky bit is still true, reload the VDC or chassis.
5. If the sticky bit is false, bring up the PKA and PL.