Nexus 5000 and Single Homed FEX vPC Design Best Practices

Contents

Introduction

This document describes Virtual Port Channel (vPC) technology and provides a straight forward simple configuration to connect two Nexus 5000 units. This Design assumes two Nexus 5000 units, with 12 FEX single homed to each of the Nexus 5000.

Background Information

Data Center Switching

The Cisco Nexus family of switches is a primary part of the unified fabric pillar of the Cisco Data Center Business Advantage architectural framework. These switches are designed to meet the stringent requirements of the next-generation data center. Not simply bigger or faster, these switches offer these advantages:

- Infrastructure that can be scaled cost-effectively and that helps you increase energy, budget, and resource efficiency
- Transport 10/40 Gigabit Ethernet and unified fabric and can handle virtualization, Web 2.0 applications, and cloud computing
- Operational continuity where system availability is assumed and maintenance windows are rare or nonexistent

The Cisco Nexus 5000 Series Switches help you transform the data center with innovative, standards-based, multilayer, multiprotocol, and multipurpose Ethernet-based fabric. Now you can help enable any transport over Ethernet, including Layer 2 and Layer 3 traffic, and storage traffic, all on one common data center-class platform.

vPC

The biggest limitation in classic PortChannel communication is that the PortChannel operates only between two devices. In large networks, the support of multiple devices together is often a design requirement to provide some form of hardware failure alternate path. This alternate path is often

connected in a way that would cause a loop, limiting the benefits gained with PortChannel technology to a single path. To address this limitation, the Cisco NX-OS Software platform provides a technology called virtual PortChannel, or vPC.

Although a pair of switches acting as a vPC peer endpoint looks like a single logical entity to PortChannel-attached devices, the two devices that act as the logical PortChannel endpoint are still two separate devices. This environment combines the benefits of hardware redundancy with the benefits of PortChannel loop management. The other main benefit of migration to an all-PortChannel-based loop management mechanism is that link recovery is potentially much faster. Spanning Tree Protocol can recover from a link failure in approximately 6 seconds, while an all-PortChannel-based solution has the potential for failure recovery in less than a second. Although vPC is not the only technology that provides this solution, other solutions tend to have a number of deficiencies that limit their practical implementation, especially when deployed at the core or distribution layer of a dense high-speed network. All multichassis PortChannel technologies still need a direct link between the two devices acting as the PortChannel endpoints. This link is often much smaller than the aggregate bandwidth of the vPCs connected to the endpoint pair.

Cisco technologies such as vPC are specifically designed to limit the use of this ISL specifically to switch management traffic and the occasional traffic flow from a failed network port. Technologies from other vendors are not designed with this goal in mind, and in fact are dramatically limited in scale specifically because they require the use of the ISL for control traffic and approximately half the data throughput of the peer devices. For a small environment, this approach might be adequate, but it will not suffice for an environment in which many terabits of data traffic may be present.

Best Practice Design Objectives

A virtual PortChannel (vPC) allows links that are physically connected to two different Cisco Nexus™ 5000 Series devices to appear as a single PortChannel to a third device. The third device can be a Cisco Nexus 2000 Series Fabric Extender or a switch, server, or any other networking device.

Best Practice Design Technology Considerations

This design uses 2 Nexus 5672UP with 24 Fabric extender 2248G attached single homed (12 FEX attached on to each of the 5672UP)

vPC Concepts

This list defines critical vPC concepts:

vPC: vPC refers to the combined PortChannel between the vPC peer devices and the downstream device.

vPC peer switch: The vPC peer switch is one of a pair of switches that are connected to the special PortChannel known as the vPC peer link. One device is selected as the primary device, and the other is a secondary device.

vPC peer link: The vPC peer link is the link used to synchronize states between the vPC peer

devices. The vPC peer link carries control traffic between two vPC switches and also multicast, broadcast data traffic. In some link failure scenarios, it also carries unicast traffic. You should have at least two 10 Gigabit Ethernet interfaces for peer links.

vPC domain: This domain includes both vPC peer devices, the vPC peer keepalive link, and all the PortChannels in the vPC connected to the downstream devices. It is also associated with the configuration mode that you must use to assign vPC global parameters.

vPC peer keepalive link: The peer keepalive link monitors the vitality of a vPC peer switch. The peer keepalive link sends periodic keepalive messages between vPC peer devices. The vPC peer keepalive link can be a management interface or switched virtual interface (SVI). No data or synchronization traffic moves over the vPC peer keepalive link; the only traffic on this link is a message that indicates that the originating switch is operating and running vPC.

vPC member port: vPC member ports are interfaces that belong to the vPCs.

Configuration Example(s)

vPC Configuration

vPC configuration on the Cisco Nexus 5000 Series includes these steps:

Step 1. Configure the management interface IP address and default route.

```
N5k-1(config)# int mgmt 0
N5k-1(config-if)# ip address 172.25.182.51/24
N5k-1(config-if)# vrf context management
N5k-1(config-vrf)# ip route 0.0.0.0/0 172.25.182.1
```

Step 2. Enable vPC and Link Aggregation Control Protocol (LACP).

```
N5k-1(config)# feature vpc
N5k-1(config)# feature lacp
```

Step 3. Create a VLAN.

```
N5k-1(config)#vlan 101
```

Step 4. Create the vPC domain.

```
N5k-1(config)# vpc domain 1
```

Step 5. Configure the vPC role priority (optional).

```
N5k-1(config-vpc-domain)# role priority 1000
```

Step 6. Configure the peer keepalive link. The management interface IP address for Cisco Nexus 5000 Series Switch 2 is 172.25.182.52.

```
N5k-1(config-vpc-domain)# peer-keepalive destination 172.25.182.52
Note:
--------:: Management VRF will be used as the default VRF ::--------
```

Step 7. Configure the vPC peer link. Note that, as for a regular interswitch trunk, trunking must be turned on for the VLANs to which the vPC member port belongs.

```
N5k-1(config-vpc-domain)# int ethernet 1/17-18
N5k-1(config-if-range)# channel-group 1 mode active
N5k-1(config-if-range)# int po1
N5k-1(config-if)# vpc peer-link
N5k-1(config-if)# switchport mode trunk
N5k-1(config-if)# switchport trunk allowed vlan 1,101
```

Step 8. Configure the Cisco Nexus 2000 Series Fabric Extenders and the fabric interface.

```
N5k-1(config)#feature fex
N5k-1(config)# fex 100
N5k-1(config-fex)# pinning max-links 1
Change in Max-links will cause traffic disruption.
N5k-1(config-fex)# int e1/7-8
N5k-1(config-if-range)# channel-group 100
N5k-1(config-if-range)# int po100
N5k-1(config-if)# switchport mode fex-fabric
N5k-1(config-if)# fex associate 100
```

Step 9. Move the fabric extender interface to vPC. After fabric extender 100 (fex 100) comes online, create the PortChannel for interface eth100/1/1 and move the PortChannel to the vPC. Note that the PortChannel number and vPC number can be different, but the vPC number must be the same on both Cisco Nexus 5000 Series Switches.

```
N5k-1(config-if)# int ethernet 100/1/1
N5k-1(config-if)# channel-group 10
N5k-1(config-if)# int po10
N5k-1(config-if)# vpc 10
N5k-1(config-if)# switchport access vlan 101
```

The configuration steps for the second switch, Cisco Nexus 5000 Series Switch 2, are:

```
N5k-2(config)# int mgmt 0
N5k-2(config-if)# ip address 172.25.182.52/24
N5k-2(config-if)# vrf context management
N5k-2(config-vrf)# ip route 0.0.0.0/0 172.25.182.1
N5k-2(config)# feature vpc
N5k-2(config)# feature lacp
N5k-2(config)#vlan 101
N5k-2(config)# vpc domain 1
N5k-2(config-vpc-domain)# peer-keepalive destination 172.25.182.51
Note:
--------:: Management VRF will be used as the default VRF ::--------
N5k-2(config-vpc-domain)# int ethernet 1/17-18
N5k-2(config-if-range)# channel-group 1 mode active
N5k-2(config-if-range)# int po1
N5k-2(config-if)# vpc peer-link
N5k-2(config-if)# switchport mode trunk
N5k-2(config-if)# switchport trunk allowed vlan 1,101
N5k-2(config)# feature fex
N5k-2(config)# fex 100
N5k-2(config-fex)# pinning max-links 1
Change in Max-links will cause traffic disruption.
N5k-2(config-fex)# int e1/9-10
N5k-2(config-if-range)# channel-group 100
N5k-2(config-if-range)# int po100
N5k-2(config-if)# switchport mode fex-fabric
N5k-2(config-if)# fex associate 100
N5k-2(config-if)# int ethernet 100/1/1
N5k-2(config-if)# channel-group 10
N5k-2(config-if)# int po10
N5k-2(config-if)# vpc 10
N5k-2(config-if)# switchport access vlan 101
```

Related Information

- **Cisco Nexus 7000 Series Switches White Papers**
- **Cisco Nexus 5000 Series Switches**
- **Virtual PortChannel Quick Configuration Guide**
- **Cisco Nexus 2000 Series Fabric Extenders**
- **Technical Support & Documentation - Cisco Systems**