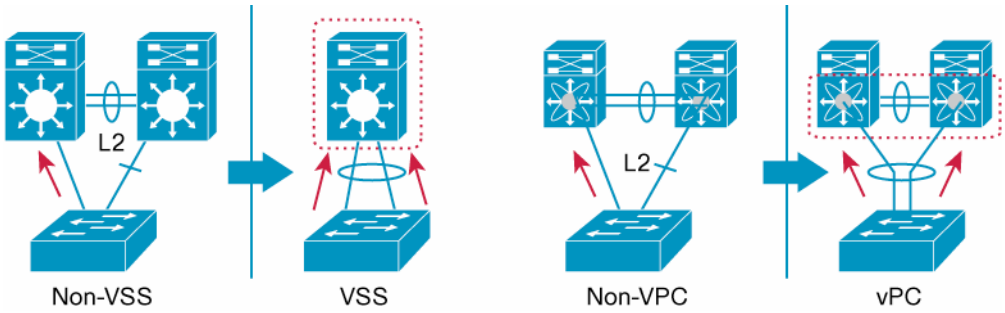
Cisco Catalyst 6500 VSS and Cisco Nexus 7000 vPC Interoperability and Best Practices

Introduction

The goal of this paper is to allow the end user to understand the interoperability and best practices when connecting Multichassis EtherChannel (MEC) on the Cisco® Catalyst® 6500 Virtual Switching System (VSS) with a Virtual Port Channel (vPC) on Cisco Nexus™ 7000. (See Figure 1.) Details on concepts and configuration requirements are outside the scope of this document.

Figure 1. Classic Spanning Tree Protocol Approach vs. VSS and vPC



Overview

In the traditional port channel model, link aggregation was only possible to a single device. MEC and vPC are two new port channel concepts that extend link aggregation across two physical switches. MEC and vPC address the multitude of new network connectivity challenges where link aggregation connectivity across two devices is required.

There are a number of benefits that VSS and vPC bring to network designs. Some of the major benefits of both of these technologies include:

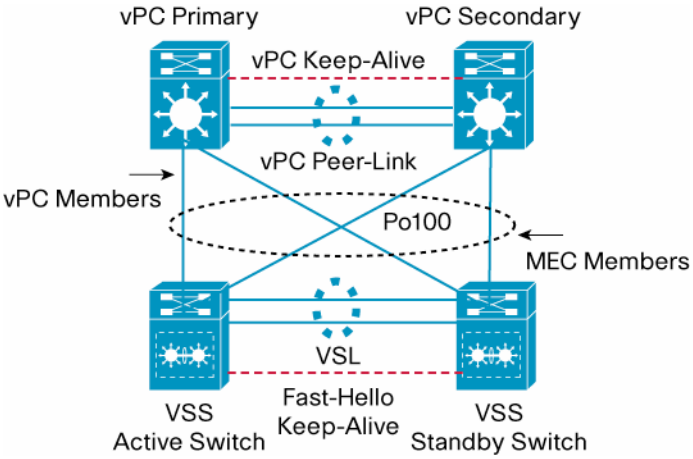
- Utilizes all available uplink bandwidth
- Allows the creation of resilient Layer 2 topologies based on link aggregation
- Eliminates the dependence of Spanning Tree Protocol in Layer 2 access distribution layer(s)
- Enables transparent server mobility, server highvailable (HA) clusters
- Scales available Layer 2 bandwidth
- Simplifies network design
- Dual-homed servers operating in active-active mode
- Provides faster convergence upon link failure
- Improves convergence time when a single device fails
- Reduces capex and opex

Prerequisite

Software requirements: Cisco IOS® Software Release 12.2(33)SXH1 and NX-OS 4.1(3) or later versions.

Hardware requirements: You must have two Cisco Catalyst 6500 VSS devices and two Cisco Nexus 7000 vPC devices equipped with 10GE interfaces for Virtual Switch Link (VSL)/vPC peer-link connectivity. (See Figure 2.)

Figure 2. vPC and VSS Interconnection



Operational Considerations

On the Cisco Catalyst 6500 VSS, both switches, which are part of a single domain, are merged into one, providing a single point for configuration management. All necessary MEC configurations are done on the active switch.

The Cisco Nexus 7000 vPC manages loosely coupled independent control planes between the vPC peers (two vPC peer devices of a single domain). Each vPC device can be independently managed without any changes to classic management infrastructure and tools. Cisco Nexus 7000 member ports participating in a single vPC should be configured consistently as it would be done for any standard port-channel members. In addition, consistency should be made sure of in the configuration of Spanning Tree Protocol, Hot Standby Router Protocol (HSRP), and Protocol Independent Multicast (PIM).

In a MEC, there can be up to 8 member ports in a single distributed EtherChannel. Each vPC peer can have up to 8 active member links, and together, the pair has up to 16 active load balancing links. As a result, the maximum

number of interfaces that can participate in a single distributed EtherChannel when interconnecting VSS and vPC members is 8. It is recommended to have members in a EtherChannel to be in powers of 2. This allows optimal bandwidth and load-sharing of traffic across the channel.

As depicted in Figure 2, members of a vPC are distributed between each Cisco Nexus 7000. Since the vPC pairs are seen as a single MEC from the VSS perspective, one must make sure the member links that are participating in the MEC are bundled together with the same port-channel ID on the Cisco Catalyst 6500. On the Cisco Nexus 7000, one must also make sure the members are part of the same vPC ID. In Figure 2, the MEC is a single EtherChannel that is being formed between the vPC and the Cisco Catalyst 6500 pairs.

The packet forwarding for MEC and vPC has been enhanced to efficiently forward traffic locally on each switch. The hardware has been programmed to forward any traffic that ingresses (as long as there is one available link local on that switch) to egress the same device. Note: This enhancement is locally significant to the VSS and vPC domain; it does not affect the reverse traffic coming from the neighboring device(s).

When multiple members are part of the MEC, they can further be load-balanced using the hashing algorithm available on both the Cisco Catalyst 6500 and Cisco Nexus 7000 pairs. To achieve optimal traffic load balancing, an appropriate hashing algorithm can be selected according to the traffic pattern traversing the system.

It is worth noting that the load balancing scheme on the Cisco Catalyst 6500 and Cisco Nexus 7000 is global or with module granularity per forwarding engine (DFC in case of Cisco Catalyst 6500).

The load balancing options that are available for MEC and vPC are as follows:

Cisco Catalyst 6500 MEC Load-Balancing Options

```
VSS(config)#port-channel load-balance ?
 dst-ip                   Dst IP Addr
 dst-mac                  Dst Mac Addr
 dst-mixed-ip-port        Dst IP Addr and TCP/UDP Port
 dst-port                 Dst TCP/UDP Port
 mpls                     Load Balancing for MPLS packets
 src-dst-ip               Src XOR Dst IP Addr
 src-dst-mac              Src XOR Dst Mac Addr
 src-dst-mixed-ip-port    Src XOR Dst IP Addr and TCP/UDP Port
 src-dst-port             Src XOR Dst TCP/UDP Port
 src-ip                   Src IP Addr
 src-mac                  Src Mac Addr
 src-mixed-ip-port        Src IP Addr and TCP/UDP Port
 src-port                 Src TCP/UDP Port
```

Cisco Nexus 7000 vPC Load-Balancing Options

```
vPC(config)#port-channel load-balance ethernet ?
 dest-ip-port                    Destination IP address and L4 port
 dest-ip-port-vlan         Destination IP address, L4 port and VLAN
 destination-ip-vlan       Destination IP address and VLAN
 destination-mac           Destination MAC address
 destination-port          Destination L4 port
 source-dest-ip-port       Source & Destination IP address and L4 port
 source-dest-ip-port-vlan  Source & Destination IP address, L4 port and VLAN
 source-dest-ip-vlan       Source & Destination IP address and VLAN
 source-dest-mac           Source & Destination MAC address
 source-dest-port          Source & Destination L4 port
 source-ip-port            Source IP address and L4 port
 source-ip-port-vlan       Source IP address, L4 port and VLAN
 source-ip-vlan            Source IP address and VLAN
 source-mac                Source MAC address
 source-port               Source L4 port
 src-ip                    Src IP Addr
 src-mac                   Src Mac Addr
 src-mixed-ip-port         Src IP Addr and TCP/UDP Port
 src-port                  Src TCP/UDP Port
```

With both solutions, Cisco recommends dual-homed attached devices. It is not recommended to single attach a device to a VSS/vPC domain. This is in order to avoid suboptimal traffic patterns, unnecessary traffic traversing the VSL/vPC peer-link, and to limit the effects of the failure response system, which might blackhole traffic to a single attached device.

The neighboring device, be it a switch, router, or end host, does not need to have any specific requirement to support MEC. As long as each device supports the applicable port channel protocol (LACP, ON mode, or PAgP(+)), the neighboring devices can participate in a MEC or vPC.

EtherChannel Protocols

Even though MEC and vPC are distributed EtherChannels, they inherit all the properties of an EtherChannel used in traditional network. There are two EtherChannel protocols available today: PAgP and the industry standard LACP (802.3ad).

MEC supports PAgP and standard IEEE 802.3ad with manual mode and LACP negotiation. vPC supports the standard IEEE 802.3ad manual mode and LACP negotiation. As best practice, LACP common protocol should be configured when connecting MEC and vPC as LACP makes sure of optimal convergence and configuration consistency checking. With LACP, it is best practice to have the LACP mode of operation set to active/active, keep the default timer values, and use the Unidirectional Link Detection (UDLD) feature for the link member integrity check.

Layer 2 EtherChannel

Both MEC and vPC support Layer 2 distributed EtherChannel. This allows the entire network to become loop free. Spanning-tree loops are eliminated due to the fact that Spanning Tree Protocol now runs on the EtherChannel logical port. In addition, each physical switch appears to be connected via a single logical link to a single logical switch.

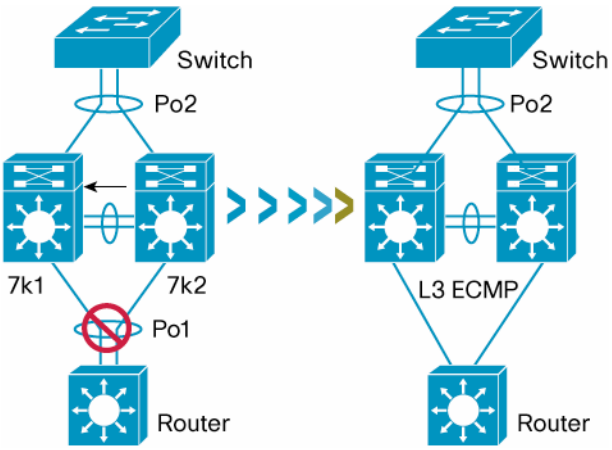
Layer 3 EtherChannel

These are routed port-channel interfaces, which offer an alternative to Equal Cost Multi-Path routing (ECMP). Layer 3 MECs are supported on VSS and can be used to reduce the number of Layer 3 routing neighbors.

Most standard Layer 3 topologies can be integrated into a vPC environment with minimal change. However, it is not supported to configure a vPC bundle as a Layer 3 port channel, or use a vPC link as an interconnect for a Layer 3 routed segment (that is, using Layer 2 port channels or trunks between the VSS and vPC pairs and running routing protocols with SVIs).

If the administrator expects to manage Layer 3 adjacencies between Cisco Nexus 7000 and Cisco Catalyst 6500 VSS, vPC is not appropriate for the interconnect with VSS. Rather, Layer 3 routed interfaces with ECMP should be configured (see Figure 3). In this scenario vPCs can be still preserved for devices connecting at Layer 2 and coexist with traditional Layer 3 routers.

Figure 3. Layer 3 Devices Attached to a vPC Domain



Managing the Layer 2 Network

Even though MEC and vPC do not rely on spanning-tree for reconvergence, Spanning Tree Protocol is still running in the background, and it should not be disabled. In the event that an external switch is connected into the topology or a misconfiguration occurs, Spanning Tree Protocol will take effect to protect the network from loops.

It is recommended to run Rapid-Per-VLAN-Spanning-Tree PVST+ (RPVST+) or MST on all devices in the network domain to achieve the optimal convergence time. The Cisco Catalyst 6500 runs PVST+ by default, and Cisco Nexus 7000 runs RPVST+ by default. For optimal convergence, the administrator should make sure the VSS pair, along with the remaining devices in the network, runs RPVST+ or MST. The distribution layer switch should carry the spanning-tree primary and secondary root for the common VLANs.

Managing the Layer 3 Network

In VSS, no First Hop Redundancy Protocol (FHRP) protocol is configured, as it is not needed. With vPC an FHRP such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) should be used.

The primary data-plane optimization made by vPC is specifically to allow local Layer 3 forwarding at both the ACTIVE and FHRP peer and the STANDBY FHRP peer. This provides in effect ACTIVE/ACTIVE FHRP behavior with no changes to current FHRP configuration or best practices to the FHRP protocol. The FHRP control protocol still shows ACTIVE/STANDBY HSRP states, with only the ACTIVE device responding to the ARP requests, but a packet destined to the shared FHRP MAC address will be accepted and routed on either the ACTIVE or STANDBY FHRP device.

Both platforms support the common Layer 3 unicast and multicast routing protocols (RIP, EIGRP, OSPF, BGP, IS-IS, PIM, MSDP). In order to achieve minimal traffic disruption, it is highly recommended to enable Nonstop Forwarding (NSF) within each routing protocol. While the Cisco Catalyst 6500 supports the prestandard Cisco NSF, it introduced support for IETF NSF (aka Graceful Restart); the Cisco Nexus 7000 supports the IETF version only. As a result, NSF IETF should be explicitly configured under the routing protocols in VSS. No further configuration is required on the Cisco Nexus 7000 pairs as they run by default NSF IETF graceful-restart. Each neighbor device that will become Layer 3 adjacent must not only have NSF configured, but the same mode of NSF must be enabled to successfully operate a graceful failover. Timers for the routing protocols should be tuned according to Layer 3 routing protocol best practices for optimal convergence.

Dual Active Detection Protocols

When the VSL or vPC peer-link fails between the pair of switches, a dual-active situation occurs. Both platforms gracefully remove one of the devices to eliminate any implications.

VSS offers three dual-active detection options:

1. PAgP+
2. Layer 3 Bidirectional Forwarding (BFD)
3. Fast-Hello Keepalive

One of these dual-active detection protocols must be enabled for successful detection of dual-active scenario. VSS shuts down all the interfaces on the ACTIVE switch (except the VSL and any interfaces that were preconfigured with the ‘exclude’ command). This leaves the STANDBY switch (new ACTIVE now) to be the only switch that is actively forwarding. For VSS it is recommended to enable Fast Hello as the dual-active detection.

vPC uses the vPC peer-keepalive link to run hello messages that are used to detect a dual-active scenario. A Gigabit Ethernet port can be used to carry the peer-keepalive messages. A dedicated VRF is recommended to isolate these control messages from common data packets. When an out-of-band network infrastructure is present, the management interfaces of the Cisco Nexus 7000 supervisor could be also used to carry keep-alive connectivity using the dedicated management VRF. When the vPC peer-link is no longer detected, a dual-active situation occurs, and the system disables all vPC port channel member on the "secondary" vPC peer (lower vPC role priority value). Also SVI interfaces associated to a vPC VLAN are suspended on the secondary switch. As a result, in this condition only the “primary” vPC peer actively forwards traffic on the vPC VLANs. Multiple peer-keepalive links can be used to increase resiliency of the dual-active detection mechanism.

Summary

Optimal convergence times can be achieved by making sure of dual-homed connectivity throughout the network. Cisco Catalyst 6500 VSS systems should enable NSF and SSO; Cisco Nexus 7000 systems should be built using supervisor redundancy to use the full hardware and NX-OS high-availability feature set.

Both the Cisco Catalyst 6500 and the Cisco Nexus 7000 offer a variety of high-availability features. Some of the primary features to highlight are In Service Software Upgrade (ISSU), Stateful Switchover (SSO), and Nonstop Forwarding (NSF). The operation and the behavior of these features are unique to the respective platform and can be independently executed without affecting the interoperability between the two platforms. Additional information on high-availability features for the Cisco Nexus 7000 and the Cisco Catalyst 6500 can be found in the reference section or on Cisco.com.

Failure scenario(s) that occurs locally on either the Cisco Catalyst 6500 or Cisco Nexus 7000 will behave the same if either of these devices were to connect to another switch. For example, in the event that a link in the MEC or vPC failure occurs, traffic will rehash to the next available link in the respective port-channel. Additional information on failure scenarios and troubleshooting is outside the scope of this document.

The interoperability between the Cisco Catalyst 6500 and Cisco Nexus 7000 is a workable solution that can be deployed in a network. By combining both virtualization technologies on each platform, you can take advantage of having a fully redundant, highly available network that eliminates the reliance of Spanning Tree Protocol and provides maximum bandwidth utilization.

Document References

Cisco Catalyst 6500 VSS

- Configuration Guide for VSS Feature: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html
- White Paper on VSS: https://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/white_paper_c11_429338.pdf
- VSS Design Guide for Campus: https://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/VSS30dg/campusVSS_DG.html
- Tech Notes on VSS: http://cco/en/US/products/ps9336/prod_configuration_examples_list.html

Cisco Nexus 7000 vPC

- Configuration Guide for vPC Feature: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/interfaces/configuration/guide/if_vPC.html
- White Paper on vPC: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/white_paper_c11-516396.html
- vPC in Cisco Data Center Validated Designs: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html - wp1053500
- Cisco Nexus 7000 Continuous Operations and High Availability: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/ps9512/White_Paper_Continuous_Operations_High_Availability.html
- Testing Cisco's Media-Centric Data Center: Cisco Nexus 7000 Series Switches: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/brochure_C02-552494-00.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-589890-00 03/10