

# Prácticas recomendadas de diseño de vPC de Nexus 5000 y FEX de una sola conexión

## Contenido

[Introducción](#)

[Antecedentes](#)

[Switching de Data Center](#)

[vPC](#)

[Objetivos de diseño de prácticas recomendadas](#)

[Consideraciones sobre la tecnología de diseño de prácticas recomendadas](#)

[Ejemplos de configuración](#)

[Información Relacionada](#)

## Introducción

Este documento describe la tecnología Virtual Port Channel (vPC) y proporciona una configuración sencilla y directa para conectar dos unidades Nexus 5000. Este diseño asume dos unidades Nexus 5000, con 12 FEX individuales conectados a cada Nexus 5000.

## Antecedentes

### Switching de Data Center

La familia de switches Cisco Nexus es una parte principal del pilar de Unified Fabric del marco arquitectónico de Cisco Data Center Business Advantage. Estos switches están diseñados para cumplir los estrictos requisitos del Data Center de última generación. Estos switches no son sencillamente más grandes o rápidos, sino que ofrecen estas ventajas:

- Infraestructura que se puede ampliar de forma rentable y que le ayuda a aumentar la eficiencia energética, presupuestaria y de recursos
- Transportar 10/40 Gigabit Ethernet y Unified Fabric y gestionar la virtualización, las aplicaciones Web 2.0 y el Cloud Computing
- Continuidad operativa donde se asume la disponibilidad del sistema y las ventanas de mantenimiento son escasas o inexistentes

Los switches Nexus de Cisco serie 5000 le ayudan a transformar el Data Center con un innovador fabric basado en estándares, multicapa, multiprotocolo y multifuncional basado en Ethernet. Ahora puede ayudar a habilitar cualquier transporte a través de Ethernet, incluido el tráfico de capa 2 y capa 3, y el tráfico de almacenamiento, todo en una plataforma común de clase de Data Center.

### vPC

La mayor limitación en las comunicaciones clásicas de PortChannel es que PortChannel funciona solamente entre dos dispositivos. En las redes grandes, la compatibilidad con varios dispositivos

es a menudo un requisito de diseño para proporcionar algún tipo de ruta alternativa de falla de hardware. Este trayecto alternativo se conecta a menudo de una manera que causaría un loop, limitando las ventajas obtenidas con la tecnología PortChannel a un solo trayecto. Para hacer frente a esta limitación, la plataforma de software Cisco NX-OS proporciona una tecnología denominada PortChannel virtual o vPC.

Aunque un par de switches que actúan como punto final de peer vPC parece una única entidad lógica para los dispositivos conectados a PortChannel, los dos dispositivos que actúan como punto final lógico de PortChannel siguen siendo dos dispositivos independientes. Este entorno combina las ventajas de la redundancia de hardware con las ventajas de la administración de loops de PortChannel. La otra ventaja principal de la migración a un mecanismo de administración de loop basado en todo el PortChannel es que la recuperación de link es potencialmente mucho más rápida. El protocolo de árbol de extensión puede recuperarse de una falla de link en aproximadamente 6 segundos, mientras que una solución basada en todo el canal de puerto tiene el potencial de recuperación de fallas en menos de un segundo. Aunque vPC no es la única tecnología que proporciona esta solución, otras soluciones tienden a tener una serie de deficiencias que limitan su implementación práctica, especialmente cuando se implementan en el núcleo o en la capa de distribución de una red densa de alta velocidad. Todas las tecnologías PortChannel de varios chasis aún necesitan un link directo entre los dos dispositivos que actúan como los terminales de PortChannel. Este enlace suele ser mucho más pequeño que el ancho de banda agregado de los vPC conectados al par de terminales.

Las tecnologías de Cisco, como vPC, están específicamente diseñadas para limitar el uso de esta ISL específicamente para el tráfico de administración de switches y el flujo de tráfico ocasional desde un puerto de red fallido. Las tecnologías de otros proveedores no se han diseñado teniendo en cuenta este objetivo y, de hecho, se limitan drásticamente en escala específicamente porque requieren el uso de ISL para controlar el tráfico y aproximadamente la mitad del rendimiento de datos de los dispositivos de peer. Para un entorno pequeño, este enfoque podría ser adecuado, pero no bastará para un entorno en el que puedan estar presentes muchos terabits del tráfico de datos.

## Objetivos de diseño de prácticas recomendadas

Un PortChannel virtual (vPC) permite que los enlaces que están conectados físicamente a dos dispositivos Cisco Nexus™ serie 5000 diferentes aparezcan como un único PortChannel a un tercer dispositivo. El tercer dispositivo puede ser un Fabric Extender Nexus de Cisco serie 2000 o un switch, servidor o cualquier otro dispositivo de red.

## Consideraciones sobre la tecnología de diseño de prácticas recomendadas

Este diseño utiliza 2 Nexus 5672UP con 24 Fabric Extender 2248G conectados con un solo enlace (12 FEX conectados a cada 5672UP)

Conceptos de vPC

Esta lista define los conceptos críticos de vPC:

vPC: vPC hace referencia al PortChannel combinado entre los dispositivos de par vPC y el dispositivo de flujo descendente.

**Switch de par vPC:** El switch de par vPC es uno de un par de switches que están conectados al PortChannel especial conocido como link de par vPC. Se selecciona un dispositivo como dispositivo principal y el otro como dispositivo secundario.

**Enlace de par vPC:** El enlace de par vPC es el enlace utilizado para sincronizar estados entre los dispositivos de par vPC. El enlace de par vPC transporta el tráfico de control entre dos switches vPC y también el tráfico de datos de difusión y multidifusión. En algunos escenarios de falla de link, también transporta tráfico de unidifusión. Debe tener al menos dos interfaces 10 Gigabit Ethernet para los links de peer.

**dominio vPC:** Este dominio incluye ambos dispositivos de par vPC, el enlace keepalive de par vPC y todos los PortChannels del vPC conectados a los dispositivos de flujo descendente. También está asociado al modo de configuración que debe utilizar para asignar parámetros globales vPC.

**Enlace de keepalive de peer vPC:** El enlace de señal de mantenimiento del par monitorea la vitalidad de un switch de par vPC. El enlace de señal de mantenimiento de par envía mensajes periódicos de señal de mantenimiento entre los dispositivos de par vPC. El enlace de señal de mantenimiento de par vPC puede ser una interfaz de administración o una interfaz virtual conmutada (SVI). Ningún tráfico de datos o sincronización se mueve sobre el enlace keepalive del par vPC; el único tráfico en este link es un mensaje que indica que el switch de origen está funcionando y ejecutando vPC.

**puerto de miembro vPC:** Los puertos de miembro de vPC son interfaces que pertenecen a los vPC.

## Ejemplos de configuración

### Configuración de vPC

La configuración de vPC en Cisco Nexus serie 5000 incluye los siguientes pasos:

**Paso 1.** Configure la dirección IP de la interfaz de administración y la ruta predeterminada.

```
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
```

**Paso 2.** Habilite vPC y el protocolo de control de agregación de enlaces (LACP).

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

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

### Paso 3. Cree una VLAN.

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

### Paso 4. Cree el dominio vPC.

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

### Paso 5. Configure la prioridad de rol de vPC (opcional).

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

### Paso 6. Configure el link de keepalive del par. La dirección IP de la interfaz de administración para el switch 2 Nexus de Cisco serie 5000 es 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 ::-----
```

### Paso 7. Configure el enlace de par vPC. Tenga en cuenta que, al igual que en el caso de un troncal entre switches normal, el enlace troncal debe estar activado para las VLAN a las que pertenece el puerto miembro vPC.

```
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
```

### Paso 8. Configure los Fabric Extenders Nexus de Cisco serie 2000 y la interfaz de fabric.

```
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
```

Paso 9. Mueva la interfaz de Fabric Extender a vPC. Después de que se conecte el Fabric Extender 100 (fex 100), cree el PortChannel para la interfaz eth100/1/1 y mueva el PortChannel al vPC. Tenga en cuenta que el número de PortChannel y el número vPC pueden ser diferentes, pero el número vPC debe ser el mismo en ambos switches Nexus de Cisco serie 5000.

```
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
```

Los pasos de configuración para el segundo switch, Cisco Nexus 5000 Series Switch 2, son:

```
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
```

## Información Relacionada

- [Informes técnicos sobre los switches Nexus de Cisco serie 7000](#)
- [Switches de la serie Cisco Nexus 5000](#)
- [Guía de configuración rápida de PortChannel virtual](#)
- [Fabric Extenders Nexus de Cisco serie 2000](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)