

Creación de Topologías para el Ruteo sobre el Canal de Puerto Virtual

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Topologías admitidas para routing en un entorno vPC](#)

[Notas y advertencias importantes](#)

[Información Relacionada](#)

Introducción

Este documento describe las topologías soportadas y no soportadas al crear adyacencias de protocolo de ruteo o PIM.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre cómo se configuran los protocolos de routing en los switches Nexus y otros routers. Cisco también recomienda conocer la configuración y el funcionamiento de vPC, las características de reenvío de vPC y el comportamiento de las mejoras de vPC Peer Gateway (mediante el comando de configuración de dominio vPC peer-gateway) y Routing/Layer 3 over vPC (mediante el comando de configuración de dominio vPC peer-router layer3). Para obtener más información sobre estas mejoras de vPC, consulte las secciones relevantes del documento [Introducción a las mejoras de Virtual Port-Channel \(vPC\)](#).

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se crean adyacencias de protocolo de routing o PIM entre dispositivos externos de capa 3 (L3) y

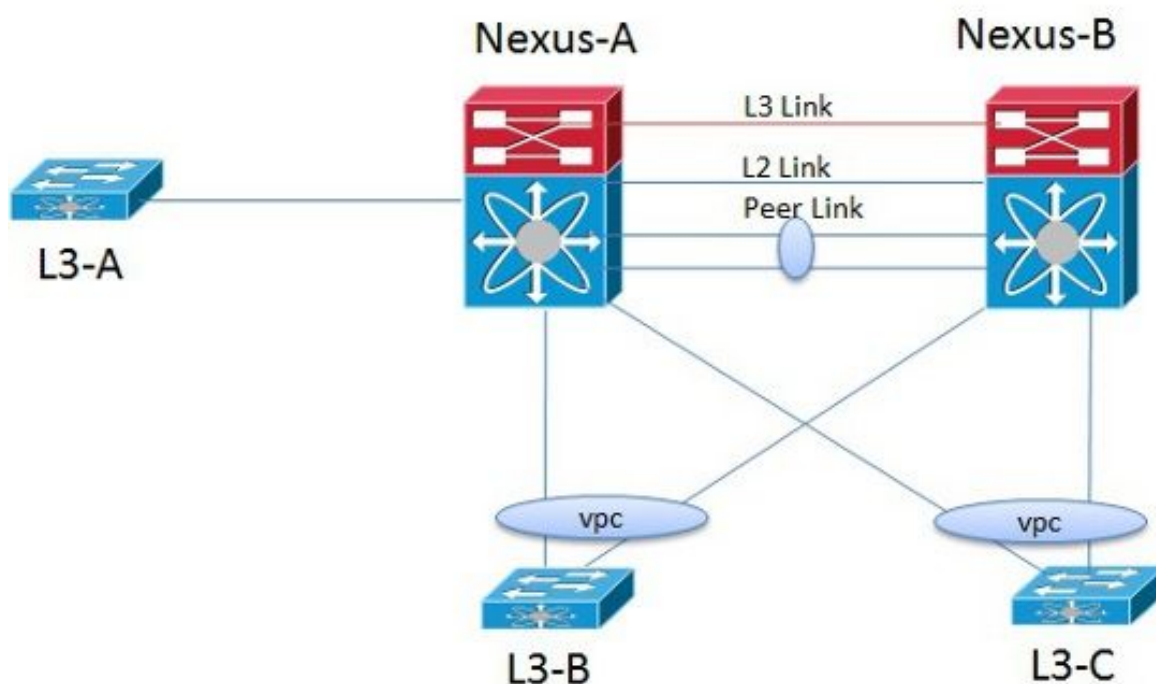
switches Cisco Nexus en un entorno de canal de puerto virtual (vPC). El término adyacencia de protocolo se utiliza en este documento para representar la formación de una relación de vecino de protocolo entre los dispositivos a los que se hace referencia. vPC+ no se trata en este artículo.

Topologías admitidas para routing en un entorno vPC

La topología mostrada en la figura 1 se puede utilizar para demostrar las diversas opciones de conectividad para las adyacencias de protocolo en un entorno vPC. Los switches Nexus se encuentran en un dominio vPC con estos detalles:

- Dos switches Nexus similares configurados en un dominio vPC.
- Tres dispositivos de capa 3 (L3-A, L3-B y L3-C) conectados a un par de switches Nexus.
- L3-A está conectado a un puerto huérfano en vPC Vlan.
- L3-B y L3-C están conectados con vPC a Nexus-A y Nexus-B.
- Nexus-A y Nexus-B tienen enlaces de capa 2 y capa 3 adicionales entre ellos.

Figura 1: Topologías admitidas para routing en un entorno vPC



En función de la topología de la figura 1, la tabla 1 describe qué enlaces físicos admiten adyacencias de protocolo entre los dos switches Nexus y entre un switch Nexus y un dispositivo L3 conectado a su par vPC. Cada tipo de link utilizado para la adyacencia de protocolo se detalla y hace referencia a cualquier advertencia aplicable que se detalla en la Tabla 1.

Tabla 1: Adyacencias del Protocolo de Ruteo Soportadas en Interfaces Físicas

Serie de switches Nexus	Adyacencia de protocolo entre Nexus-A y Nexus-B	Adyacencia de protocolo entre L3-A y Nexus-B
-------------------------	---	--

<p>Nexus 95xx-R y 3xxxx-R</p>	<p>Enlace L3: compatible Enlace L2: compatible Enlace de par: compatible Adyacencia de PIM sobre el link de peer: Compatible ***</p>	<p>Enlace L3: N/D Enlace L2: admitido% Enlace de par: compatible; consulte la tabla 2 de requisitos Adyacencia PIM: admitida **</p>
<p>Nexus serie 3000/3100/3200/3400/3600</p>	<p>Enlace L3: compatible Enlace L2: compatible* Enlace de par: compatible Adyacencia de PIM sobre el link de peer: Compatible ***</p>	<p>Enlace L3: N/D Enlace de L2: compatible*% Enlace de par: compatible; consulte la tabla 2 de requisitos Adyacencia PIM: admitida **</p>
<p>Nexus serie 3500</p>	<p>Enlace L3: compatible Enlace L2: no compatible Enlace de par: compatible Adyacencia de PIM sobre el link de peer: admitida ***</p>	<p>Enlace L3: N/D Enlace L2: no compatible Enlace de par: compatible; consulte la tabla 2 de requisitos Adyacencia PIM: admitida **</p>
<p>Nexus serie 5000</p>	<p>Enlace L3: compatible Enlace L2: no compatible Enlace de par: compatible Adyacencia de PIM sobre el link de peer: Compatible ***</p>	<p>Enlace L3: N/D Enlace L2: no compatible Enlace de par: compatible; consulte la tabla 2 de requisitos Adyacencia de PIM: no compatible **</p>
<p>Nexus serie 6000</p>	<p>Enlace L3: compatible Enlace L2: no compatible Enlace de par: compatible</p>	<p>Enlace L3: N/D Enlace L2: no compatible Enlace de par: compatible;</p>

	Adyacencia de PIM sobre el link de peer: Compatible ***	consulte la tabla 2 de requisitos Adyacencia de PIM: no compatible **
Nexus serie 7000	Enlace L3: compatible Enlace L2: compatible Enlace de par: compatible Adyacencia de PIM sobre el link de peer: Compatible ***	Enlace L3: N/D Enlace L2: admitido% Enlace de par: compatible; consulte la tabla 2 de requisitos Adyacencia PIM: admitida **
Nexus serie 9000	Enlace L3: compatible Enlace L2: compatible* Enlace de par: compatible Adyacencia de PIM sobre el link de peer: Compatible ***	Enlace L3: N/D Enlace de L2: compatible*% Enlace de par: compatible; consulte la tabla 2 de requisitos Adyacencia PIM: admitida **

* Debe configurar una dirección MAC definida por el usuario en cada interfaz virtual (SVI) del switch VLAN relevante. Consulte Cisco bug ID [CSCus1343](#) para obtener más detalles.

** No se admite la adyacencia PIM en una VLAN vPC entre a) L3-A y Nexus-A o Nexus-B o b) entre L3-B o L3-C y Nexus-A o Nexus-B, independientemente de si el router o el switch de capa 3 está conectado a través de un puerto huérfano o un enlace de miembro vPC. Para todas las plataformas excepto la adyacencia PIM de Nexus 5000 o Nexus 6000 en una VLAN sin vPC entre a) L3-A y Nexus-A o Nexus-B o b) entre L3-B o L3-C y Nexus-A o Nexus-B es compatible si se establece a través del enlace L2.

*** Se admite la adyacencia PIM entre Nexus-A y Nexus-B; sin embargo, el tipo de modo disperso de PIM admitido (es decir, SSM, ASM y BiDIR) varía según la plataforma. Consulte las guías de configuración de la plataforma.

Se requiere una capacidad de router de par de capa 3 % para utilizar el enlace de par vPC como ruta de routing de tránsito (sin un enlace L2 paralelo).

La tabla 2 describe qué adyacencias de protocolo de routing se admiten en las VLAN vPC según la topología de la figura 1.

Nota: con la introducción de la mejora del routing/capa 3 sobre vPC mediante el comando de configuración de dominio vPC peer-router de capa 3, todas las plataformas de switching Nexus admiten ahora adyacencias de protocolo de routing unidifusión a través del enlace de par vPC. Antes del desarrollo de esta función, el soporte variaba según la plataforma. Para actualizar a una versión de NX-OS que admita la mejora de routing/capa 3 sobre vPC de una versión anterior, se pueden interrumpir las topologías actuales hasta que se active el comando de configuración de dominio vPC peer-router de capa 3. La mejora del routing/capa 3 en vPC no añade compatibilidad para una adyacencia PIM en una VLAN vPC.

Tabla 2: Compatibilidad con adyacencias de protocolos de routing en VLAN vPC

Serie de switches Nexus	L3-A a L3-B or L3-A a L3-C	L3-A, L3-B o L3-C a Nexus-A o Nexus-B
Nexus 95xx-R y 3xxxx-R Series	Yes	*7.0(3)F3(3) y posteriores con el comando de configuración de dominio vPC de router de par de capa 3 activado
Nexus 3000/3100/3200/3400/3600	Yes	*7.0(3)F3(3) y posteriores con el comando de configuración de dominio vPC de router de par de capa 3 activado
Nexus serie 3500	Yes	* 6.0(2)A8(x) y posterior con el comando de configuración de dominio vPC de router de par de capa 3 habilitado
Nexus serie 5000	Yes	* 7.3(0)N1(1) y posterior con el comando de configuración de dominio vPC de router de par de capa 3 habilitado
Nexus serie 6000	Yes	* 7.3(0)N1(1) y posterior con el comando de configuración de dominio vPC de router de par de capa 3 habilitado
Nexus serie 7000	Yes	* ** 7.2(0)D1(1) y posterior con el comando de configuración de dominio vPC de router de par de capa

		3 habilitado
Nexus serie 9000	Yes	* 7.0(3)I5(1) y posterior con el comando de configuración de dominio vPC de router de par de capa 3 habilitado

* Esta función requiere la configuración explícita del comando de configuración de dominio vPC de peer-router de capa 3.

** No compatible con tarjetas de línea de las series M1, F1, F2 y M2.

Notas y advertencias importantes

- El modelo de iguales de L3-A a Nexus-A siempre es compatible con L2/L3.
- El peering L3-B a L3-C siempre se soporta para L2/L3.
- Cuando una sesión BFD está sobre SVI que utiliza el Peer-Link de Port-Channel virtual (vPC), la función de eco BFD no es compatible. Debe inhabilitar la función de eco BFD para todas las sesiones sobre SVI entre los nodos de peer vPC que utilizan el comando de configuración de interfaz no bfd echo.
- Si el enlace de par vPC se configura en un módulo de 1/10 Gigabit Ethernet (F1-Series) de 32 puertos Cisco Nexus (N7K-F132XP-15), debe incluir la VLAN de routing de copia de seguridad de L3 en la lista de VLAN especificada por el comando peer-gateway exclude-vlan.
- Para todas las plataformas Nexus, no se admite una adyacencia PIM en un vPC o un puerto huérfano vPC. Para formar una adyacencia PIM admitida, debe tener una conexión de capa 3 desde cada switch Nexus al router PIM relevante o formar la adyacencia PIM en una VLAN que no sea vPC.
- Los switches Nexus 5000, 5500, 5600 y 6000 en un dominio vPC que reciben tráfico multicast desde una VLAN vPC o vPC donde un receptor multicast sólo es accesible a través del link de par vPC deben tener presente el comando de configuración global vpc bind-vrf default vlan {vlan-id}. Para cada VRF, se debe definir una VLAN independiente y la VLAN definida no se debe utilizar ya para el tráfico de producción. Además, cuando tiene una topología vPC con puertos huérfanos o conexiones de Capa 3 y el tráfico multicast debe pasar a través del link de peer para alcanzar estos receptores, no se envía al receptor a menos que tenga el comando vpc bind-vrf default vlan {vlan_id}. Para cada VRF, se puede configurar un vlan_id separado, donde la VLAN no se utiliza ya para el tráfico de producción. Para obtener más detalles, consulte la [Guía de Configuración de Interfaces NX-OS de Nexus serie 5500](#), la [Guía de Configuración de Interfaces NX-OS de Nexus serie 5600](#) y la [Guía de Configuración de Interfaces NX-OS de Nexus serie 6000](#).

Información Relacionada

- [Comprender las mejoras del canal de puerto virtual \(vPC\)](#)

- [Routing de copia de seguridad de vPC de capa 3 con F1 y gateway de par](#)
- [N5500/N6000 Enlace de una instancia de VRF a un vPC](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).