



Configuración y Troubleshooting de vPC

Comunidad de Cisco

Juan Carlos Gandaria - Escalation Engineer de DCRS
Osmar Reséndiz - Technical Consulting Engineer de DCRS

Jueves 17 de agosto de 2023



Conecte, Interactúe, ¡Colabore!

Soluciones

¡Acepte las soluciones correctas y felicite a quienes le ayudaron! Los foros de discusión tienen muchas entradas, de las cuales no todas cuentan con una respuesta correcta o válida.

Ayude a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución”.

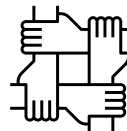
Aceptar como solución

Agradecimientos

¡Resalte el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndonos la oportunidad de ganar premios además de ser una muestra valiosa de ¡nuestro reconocimiento!

o Útil



Spotlight Awards

¡Nuevos ganadores cada mes!

Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros. Los Premios Spotlight se otorgan mensualmente para destacar a los miembros más destacados.

¡Ahora también puedes nominar a un candidato! [Haga clic aquí](#)



Juan Carlos Gandaria



Escalation Engineer

Escalation Engineer en el equipo de Data Center Routing and Switching (DCRS) dentro del Centro de Asistencia Técnica (TAC) global de Cisco que brinda soporte técnico. Con cinco años de experiencia en DCRS, participando principalmente en el crecimiento técnico del equipo de DCRS West Coast, Juan colabora con capacitación y documentación técnica.

Osmar Reséndiz

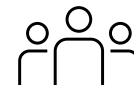


Technical Consulting Engineer

Technical Consulting Engineer en el equipo de Data Center Routing and Switching (DCRS) dentro del TAC Global. Titulado como Ingeniero en Comunicaciones y Electrónica, y actualmente está certificado en CCNA, CCNP Routing & Switching y DevNet.

Descargue la presentación

<https://bit.ly/CLdoc-aug23>



slido

Join at
slido.com
#4040 626

 Passcode: **sl4ksb**

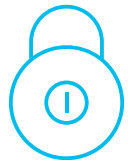


Agenda

1. Descripción de vPC y Terminología



2. Ventajas de VPC



3. vPC Escenarios de implementación

4. Mejores Prácticas con vPC



5. Laboratorio día 0

6. Pasos de troubleshooting



Join at
slido.com
#4040 626

🔍 Passcode:
sl4ksb

¿Qué es vPC?

A) Virtual Private Cloud

0%

B) Virtual Port-Channel

0%

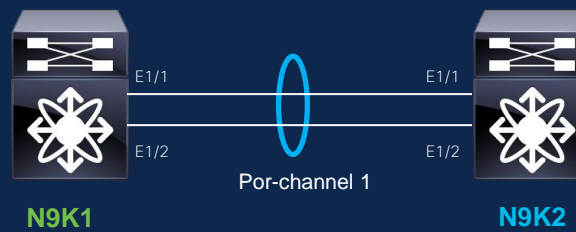
C) Virtual Port Client

0%

Descripción de vPC y terminología

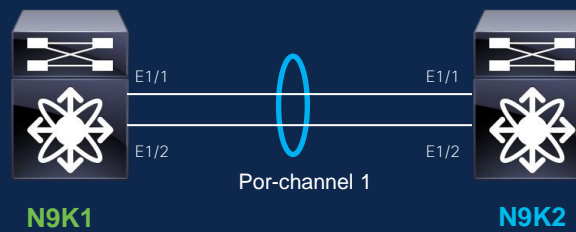
LACP Basics

- LACP es un protocolo basado en IEEE (802.3ad)



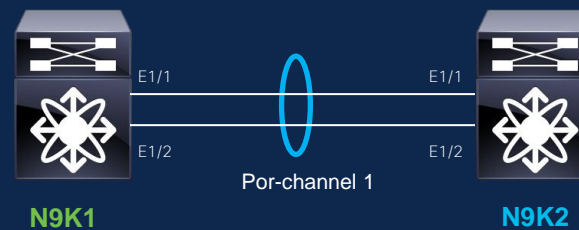
LACP Basics

- LACP es un protocolo basado en IEEE (802.3ad)
- Sirve para agrupar varias interfaces físicas en una interfaz virtual



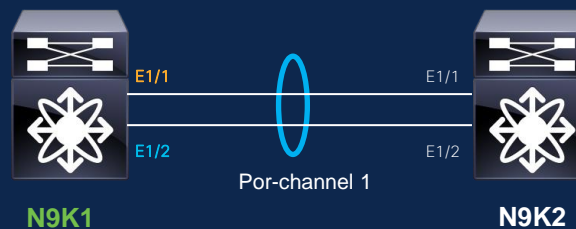
LACP Basics

- LACP es un protocolo basado en IEEE (802.3ad)
- Sirve para agrupar varias interfaces físicas en una interfaz virtual
- LACP intercambia una serie de PDUs para levantar la interfaz virtual



LACP Basics

- LACP es un protocolo basado en IEEE (802.3ad)
- Sirve para agrupar varias interfaces físicas en una interfaz virtual
- LACP intercambia una serie de PDUs para levantar la interfaz virtual



```
N9K1# show interface e1/1 | i i addr
Ethernet, address: 4c77.6d9b.10e4 (bia 4c77.6d9b.10e4)
```

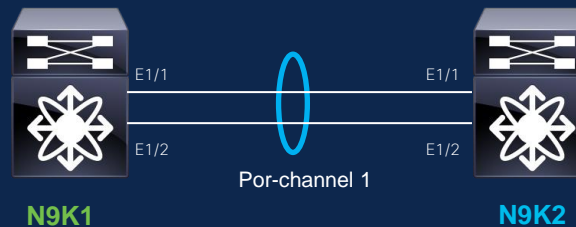
```
N9K1# show interface e1/2 | i Bia addr
Ethernet, address: 4c77.6d9b.10e8 (bia 4c77.6d9b.10e8)
```

```
N9K1# ethanalyzer local interface inband display-filter slow limit-captured-frames 0
Capturing on inband
```

```
20:56:32.079805 4c:77:6d:9b:10:e8 -> 01:80:c2:00:00:02 LACP Link Aggregation Control ProtocolVersion 1. Actor Port = 965 Partner Port = 709
20:56:41.618417 4c:77:6d:9b:10:e4 -> 01:80:c2:00:00:02 LACP Link Aggregation Control ProtocolVersion 1. Actor Port = 961 Partner Port = 705
```

LACP Basics

- LACP es un protocolo basado en IEEE (802.3ad)
- Sirve para agrupar varias interfaces físicas en una interfaz virtual
- LACP intercambia una serie de PDUs para levantar la interfaz virtual
- Dentro de los PDUs que se intercambian el LAG id de cada interfaz , este LAG-id tiene que ser el mismo en cada interfaz física.



```
N9k1# sh lACP interface ethernet 1/1 | i i lAg
```

```
Lag Id: [ [(1770, a8-c-d-96-43-7f, 5, 8000, 1c9), (1770, a8-c-d-96-c9-bf, 5, 8000, 1c9)] ]
```

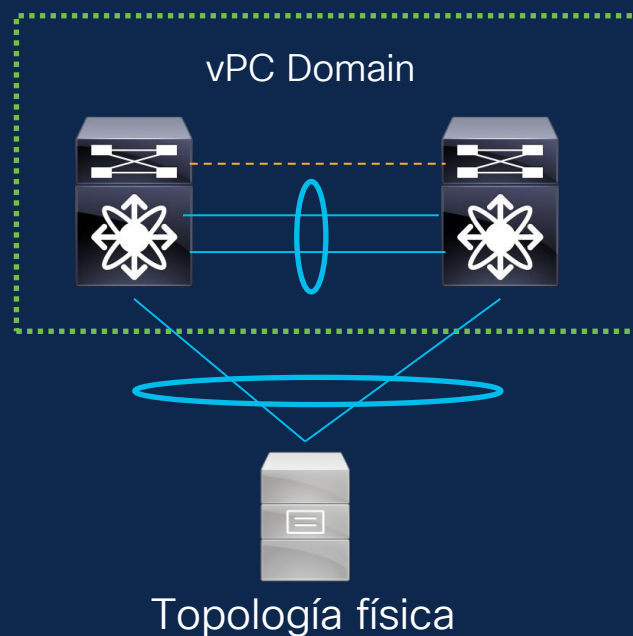
```
N9k1# sh lACP interface ethernet 1/2 | i i lAg
```

```
Lag Id: [ [(1770, a8-c-d-96-43-7f, 5, 8000, 1ca), (1770, a8-c-d-96-c9-bf, 5, 8000, 1ca)] ]
```

¿Qué es vPC?

vPC (virtual Port-Channel) es una tecnología de virtualización que presenta un par de Switches Nexus como una única entidad lógica de capa 2 hacia equipos de acceso o end hosts.

Un virtual port-channel permite que un equipo físicamente conectado a dos nexus diferentes aparezca conectado como un solo port-channel hacia un solo "Switch"

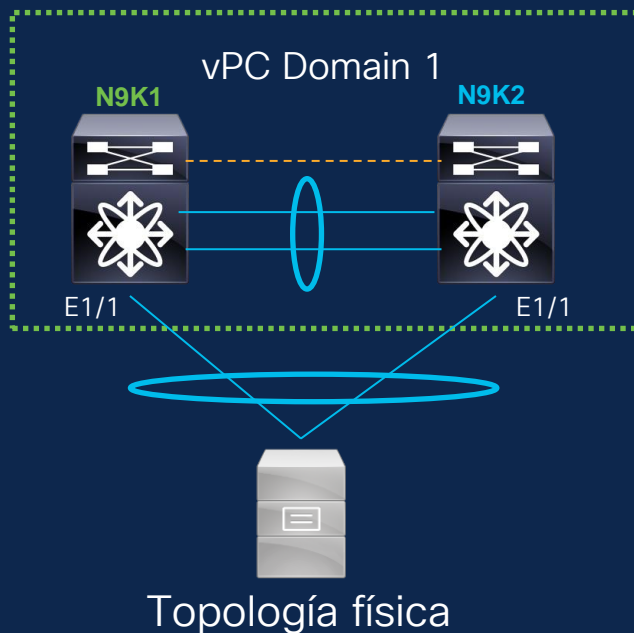


¿Qué es vPC?

Una vez que vPC es configurado, los dos vPC peers crearán una vPC system mac:

vPC system-mac = **00:23:04:ee:be:** <vpc domain-id en hexadecimal>

Esta mac será la utilizada en la parte de LAG id para formar los vPC port-channels



```
N9K1# sh lacp interface e1/1 | i i lag
Lag Id: [ [(7d0, 0-23-4-ee-be-01, 8008, 8000, 10d), (8000, 78-c-f0-ba-78-77, 7, 8000, 105)] ]

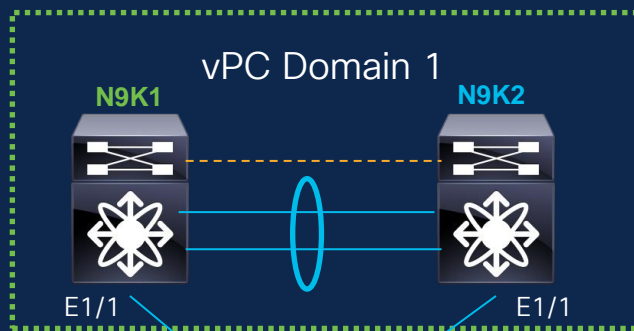
N9K2# sh lacp interface e1/1 | i i lag
Lag Id: [ [(7d0, 0-23-4-ee-be-01, 8008, 8000, 10d), (8000, 78-c-f0-ba-78-77, 7, 8000, 101)] ]
```

¿Qué es vPC?

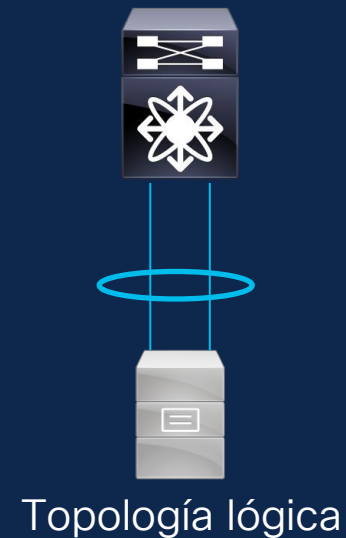
Una vez que vPC es configurado, los dos vPC peers crearán una vPC system mac:

vPC system-mac = **00:23:04:ee:be:** <vpc domain-id en hexadecimal>

Esta mac será la utilizada en la parte de LAG id para formar los vPC port-channels



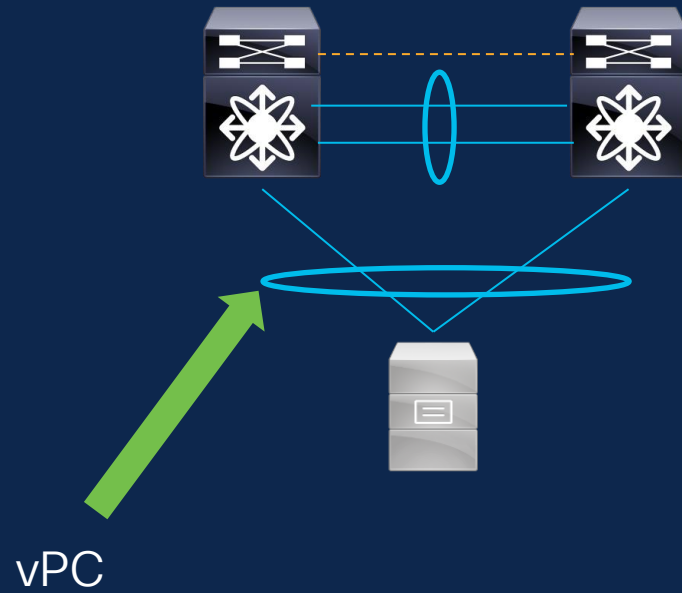
Topología física



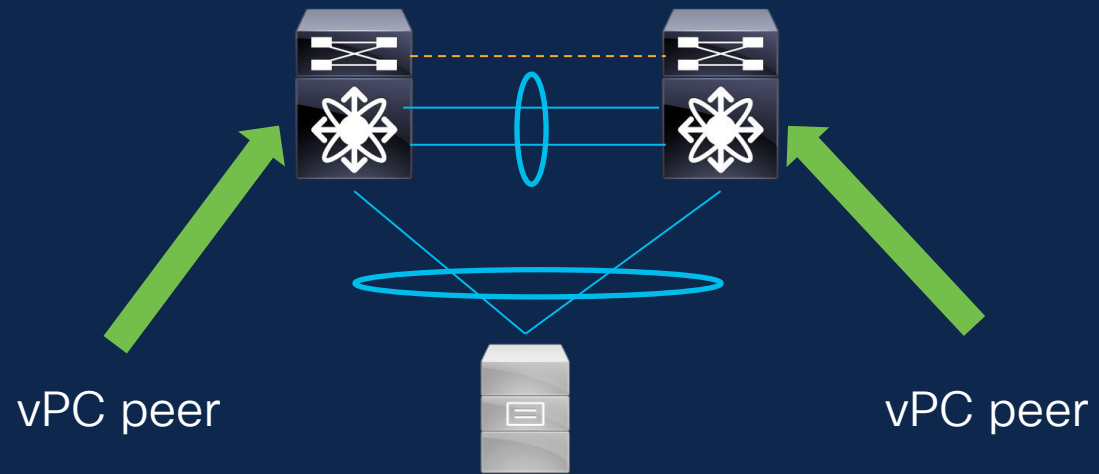
Topología lógica

Terminología

vPC

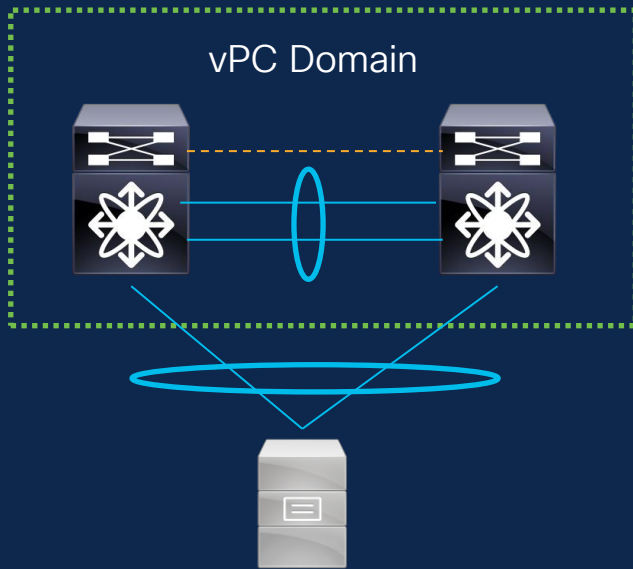


La combinación de port-channels entre vPC peers y un tercer equipo.



vPC Peer

Un vPC switch perteneciente al mismo dominio



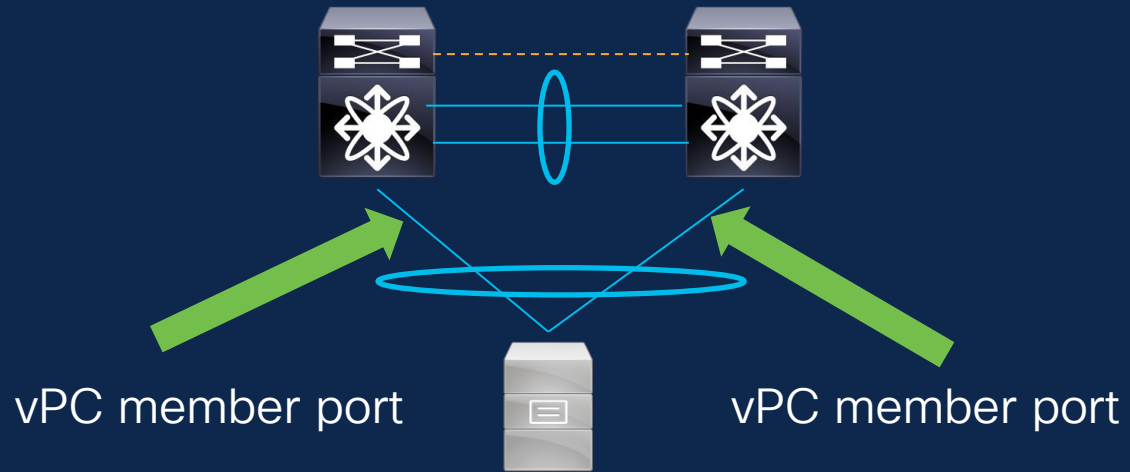
vPC Domain

Dominio que contiene dos vPC peers

Un vPC domain puede contener máximo dos equipos

vPC Member port

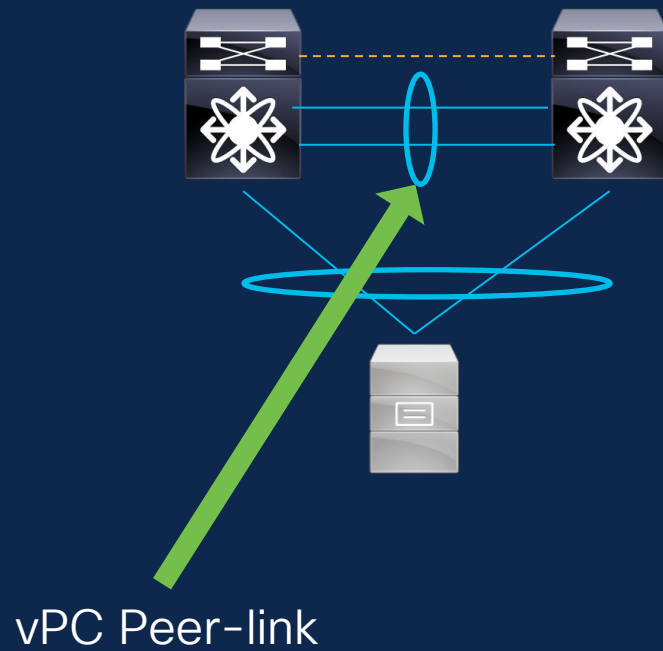
Uno de los puertos (miembros del port-channel) que forman parte de vPC



vPC Peer-link

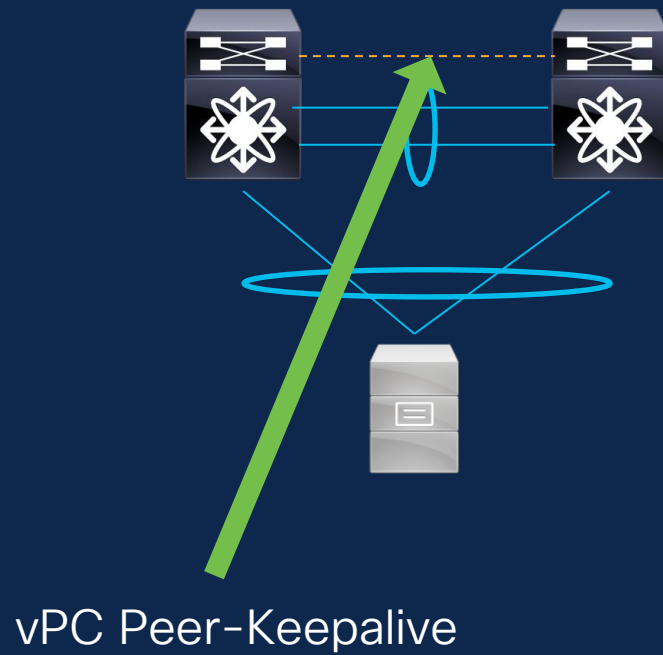
Puerto utilizado para sincronizar el estado entre equipos vPC.

El peer-link es una interfaz de capa 2 troncal que transporta vPC vlans.



vPC Peer-keepalive

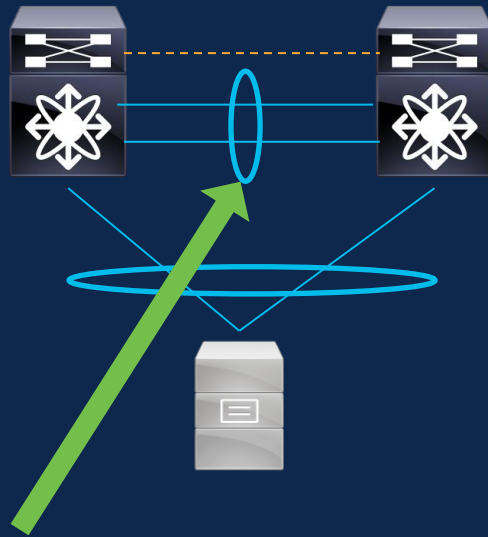
Es un puerto usado para monitorear que el vPC peer siga operativo.



vPC VLAN

VLAN que es transportada por el vPC peer-link.

Una vez que la VLAN es permitida en el peer-link se convierte en una vPC VLAN.



```
Show vpc
```

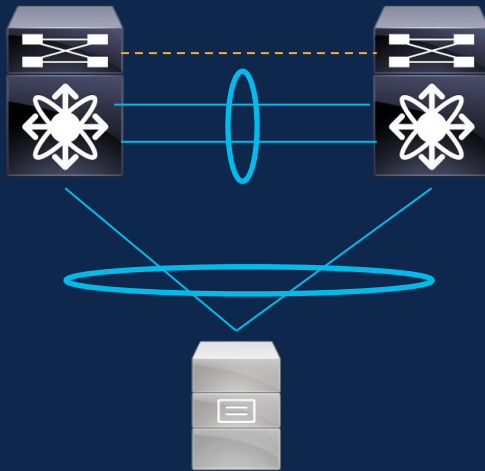
```
<Snipped>
```

```
vPC Peer-link status
```

id	Port	Status	Active vlans
1	Po3	up	1-2,100-105,999

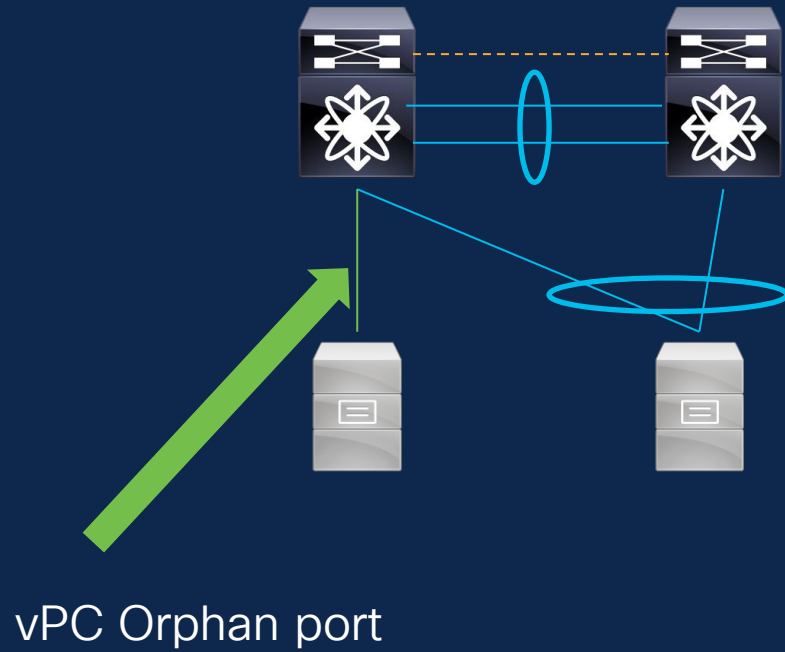
Non-vPC VLAN

VLAN que no es transportada en ningún vPC ni en el vPC peer-link



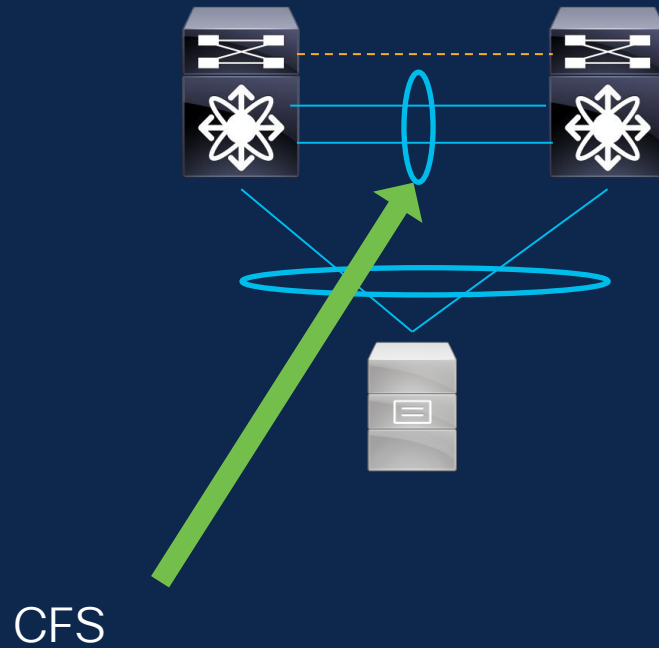
vPC Orphan port

Es un puerto conectado a un solo un vPC Peer

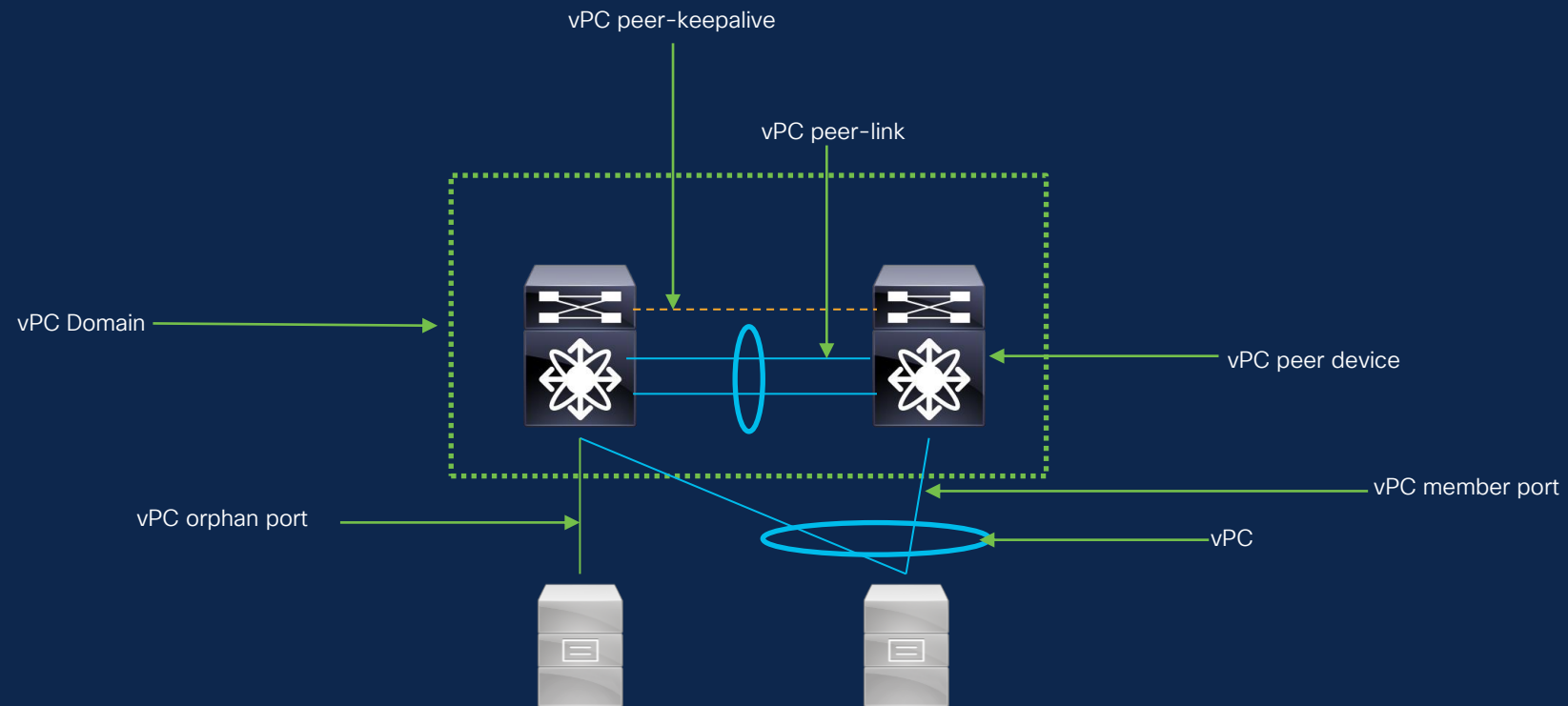


Cisco Fabric Services (CFS)

Protocolo corriendo sobre vPC peer-link que provee sincronización y mecanismos de chequeo entre los dos vPC peers



Terminología



vPC Loop avoidance rule

vPC Loop avoidance rule

vPC realiza una prevención de bucle a nivel de data-plane al contrario de spanning-tree, toda la lógica está implementada directamente en hardware en los puertos de vPC.

Un vPC peer siempre tratará de forwardear el tráfico localmente, si es posible. El vPC Peer-link normalmente no transporta tráfico de data-plane.

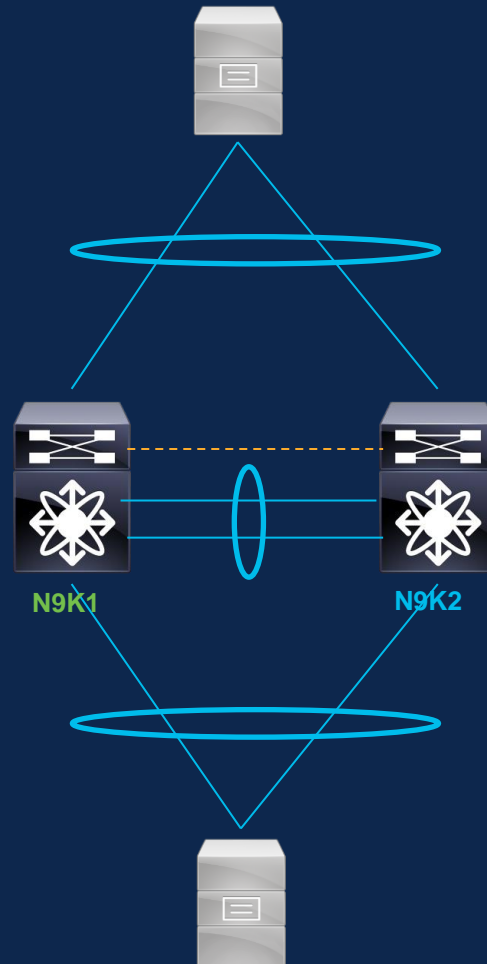
vPC Loop avoidance rule

La regla de Loop avoidance dice que:

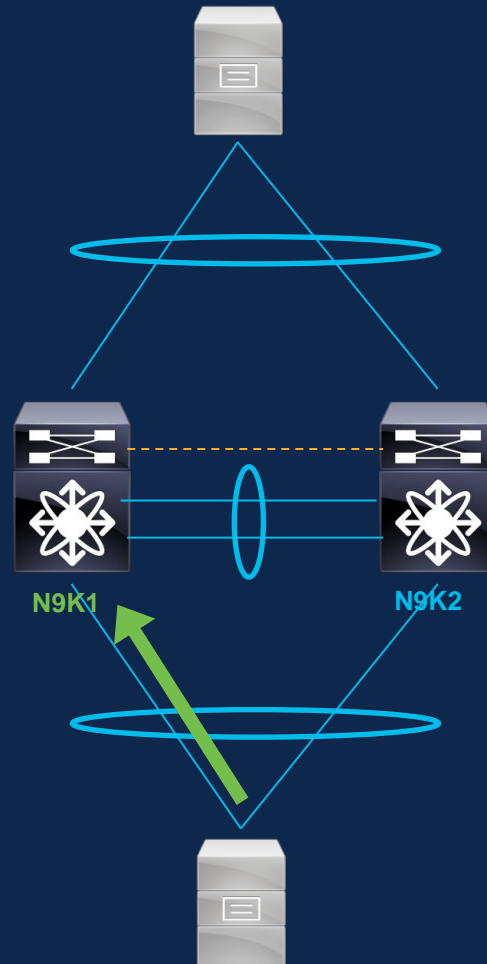
“El tráfico que viene de un puerto vPC y que cruza el peer-link, no esta permitido que salga por otro miembro de vPC, sin embargo puede salir por otro tipo de puerto (L3 port, orphan port...) ”

La única excepción a esta regla ocurre cuando un miembro de vPC se cae, los vPC peers intercambian los estados de los puertos y reprograman en HW la lógica de loop avoidance, en este caso el peer-link se usa como un camino alternativo para hacer forwarding del tráfico.

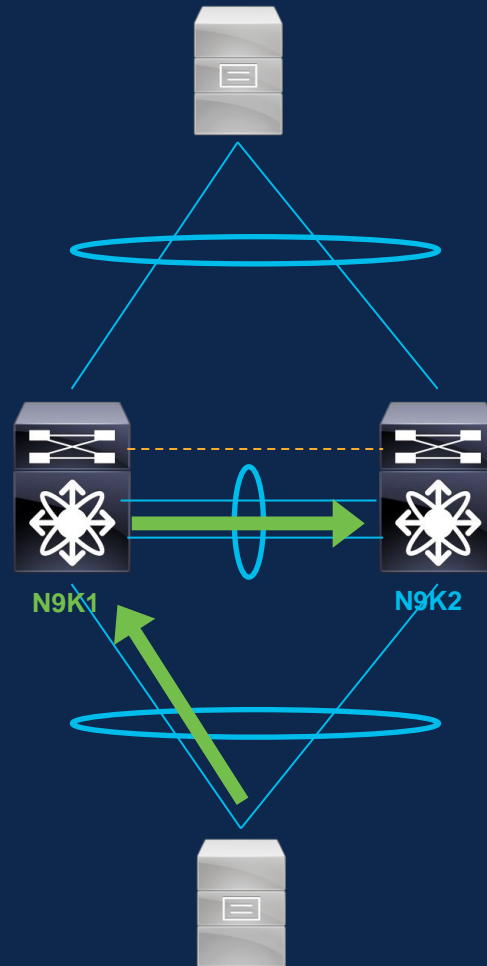
vPC Loop avoidance rule



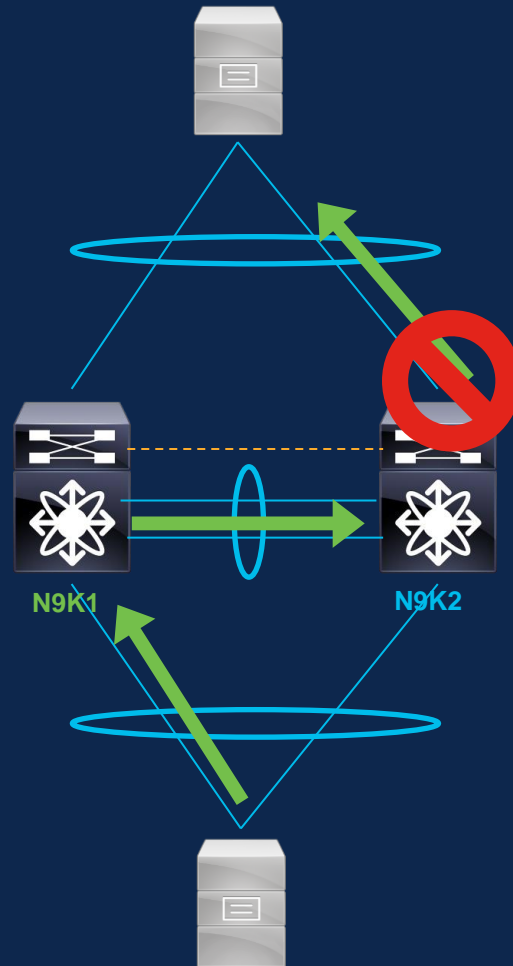
vPC Loop avoidance rule



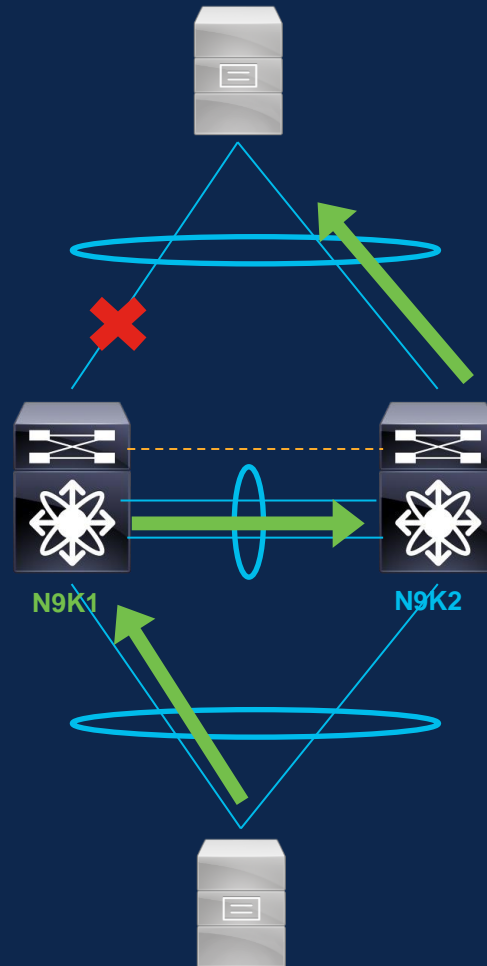
vPC Loop avoidance rule



vPC Loop avoidance rule



vPC Loop avoidance rule exception





Join at
slido.com
#4040 626

🔍 Passcode:
sl4ksb

¿Qué tan familiarizado estás con VPC?

A) He escuchado sobre él

0%

B) Lo conozco pero no he trabajado con él

0%

C) Lo conozco y he trabajado con él en implementación y troubleshooting

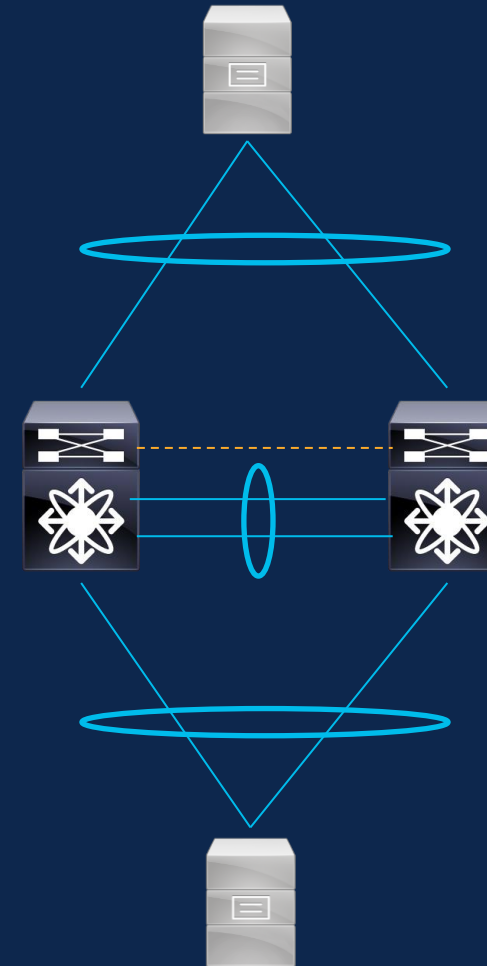
0%

Ventajas de vPC

Redundancia total de plataforma

La correcta configuración de un dominio de vPC nos permite obtener redundancia total en Capa 2, incluso en caso de que uno de los switches sufra una falla total.

Al ser un protocolo de Capa 2, permite un 'forwardeo' de paquetes del tipo Active/Active.

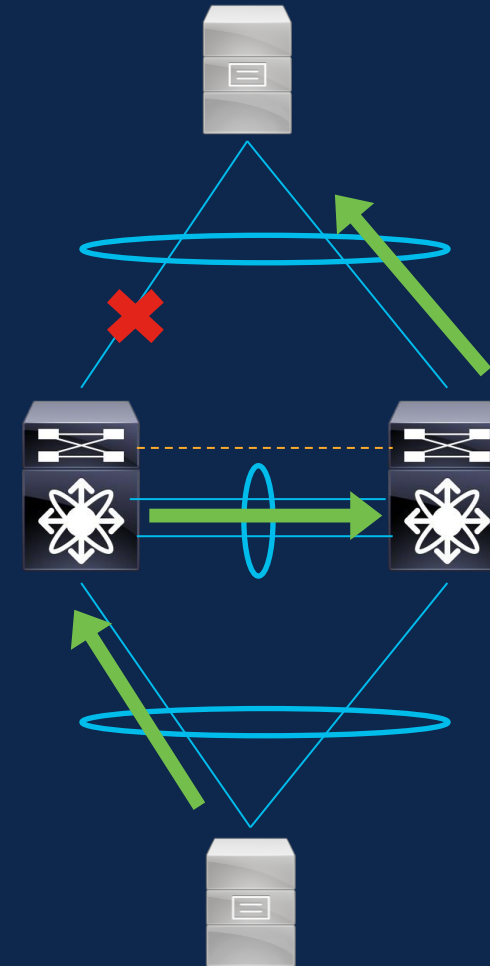


Redundancia total de plataforma

La correcta configuración de un dominio de vPC nos permite obtener redundancia total en Capa 2, incluso en caso de que uno de los switches sufra una falla total.

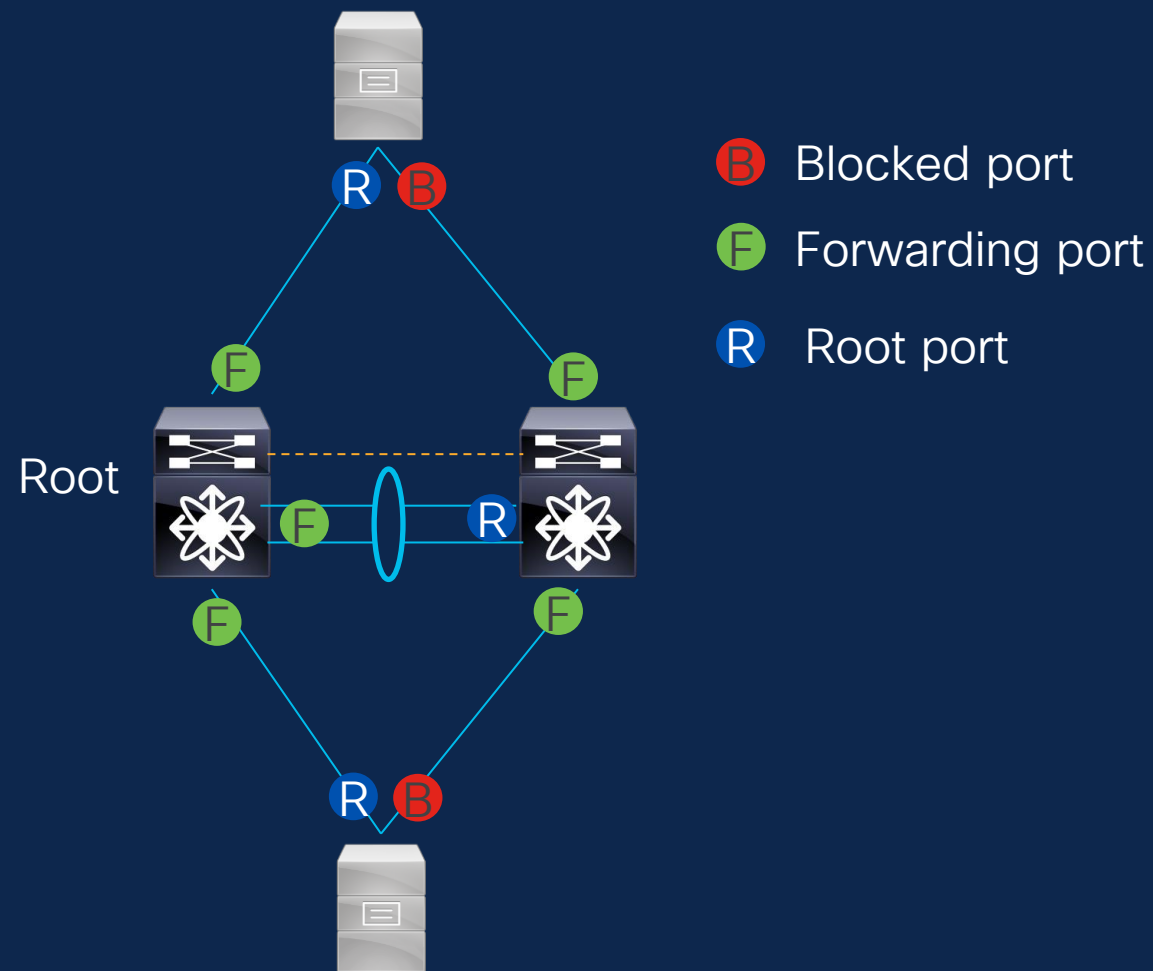
Al ser un protocolo de Capa 2, permite un 'forwardeo' de paquetes del tipo Active/Active.

Dado que los miembros de los vPC Port-Channels en ambos vPC Peers están activos simultáneamente, vPC ofrece un 'failover' completamente transparente, dado que desde la perspectiva de Capa 2, el Control Plane no cambia.



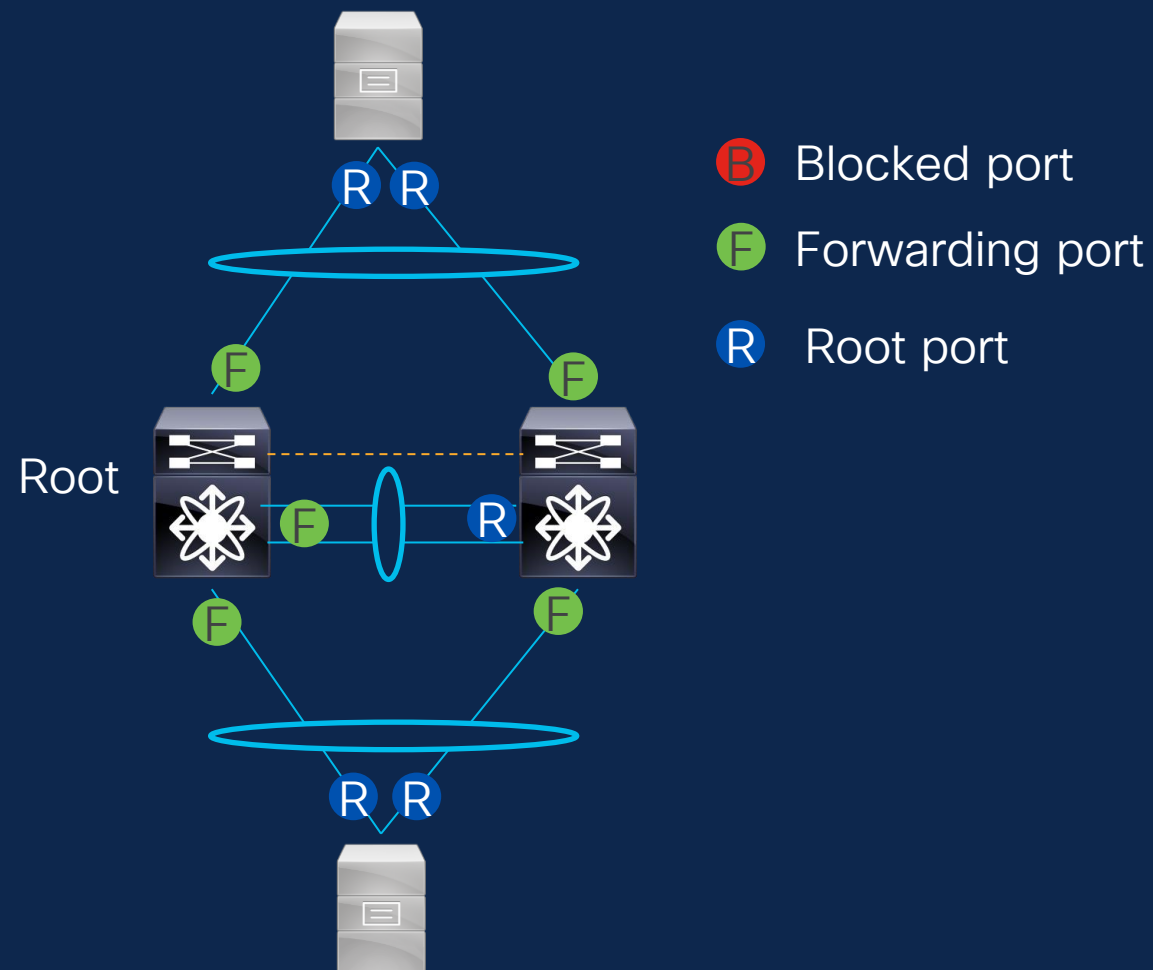
Topología de spanning-tree sin puertos bloqueados

Con la tecnología de vPC se puede tener port-channels con múltiples interfaces donde spanning-tree no bloqueará ningún puerto



Topología de spanning-tree sin puertos bloqueados

Con la tecnología de vPC se puede tener port-channels con múltiples interfaces donde spanning-tree no bloqueará ningún puerto



Escenarios Comunes de Falla

- Falla del vPC Peer Keep-Alive
- Falla del Peer Keep-Alive seguido de falla del Peer-Link (Split-Brain)
- Falla del vPC Peer-Link
- Inconsistencias en un Dominio de vPC

¿Cómo se asignan los roles en un Dominio de vPC?

Un Dominio de vPC tiene dos roles, Primary and Secondary.

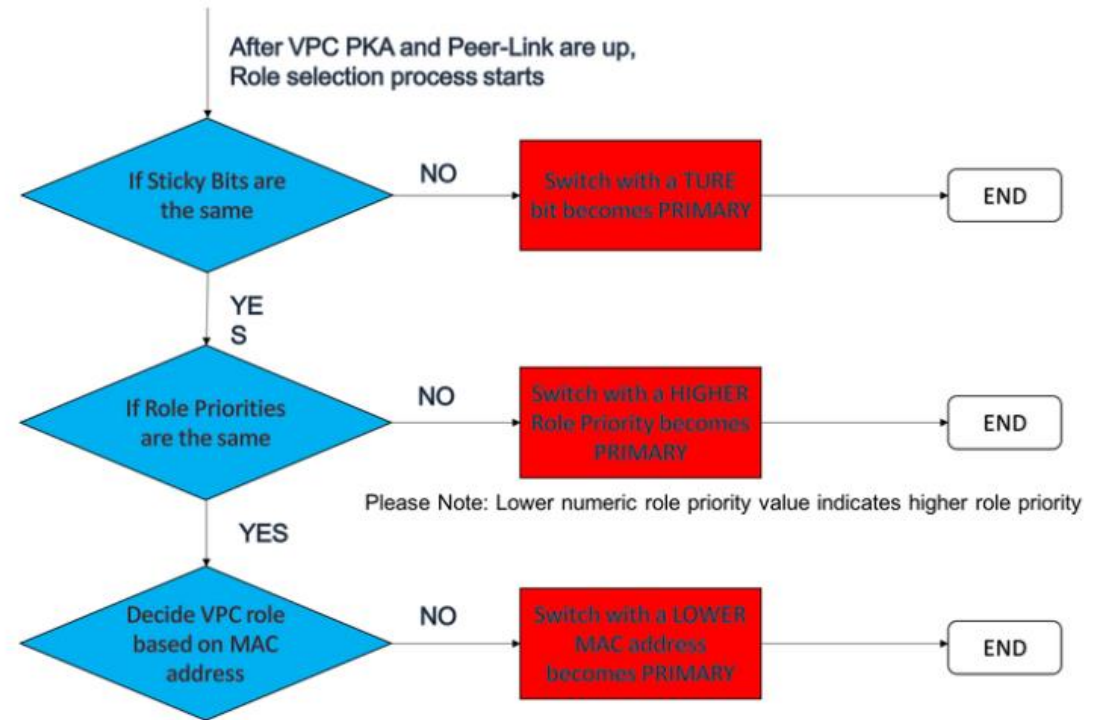
Este se determina por medio del valor de la prioridad de vPC configurada. La prioridad más baja siempre será la elegida. Por default es: 32667

El vPC Primary peer es quien se encarga del procesamiento spanning-tree BPDUS.

Para evitar conflictos en la elección del Primary Peer los vPC Peers usan un mecanismo llamado “Sticky-Bit”.

Sticky-Bit

- Sticky-bit es un mecanismo de protección programado para evitar un cambio de rol innecesario (que potencialmente puede causar disrupción en la red) cuando el vPC peer se reinicia.
- Sticky-bit permite que el nexus switch operativo mantenga el rol de primario cuando el switch que reinició regresa.
- Cuando el proceso de elección de rol de vPC es ejecutado, el nexus con el sticky-bit con el valor de TRUE se convierte en primario no importando los otros parámetros de elección.



Sticky-Bit

- Sticky-bit es un mecanismo de protección programado para evitar un cambio de rol innecesario (que potencialmente puede causar disrupción en la red) cuando el vPC peer se reinicia.
- El feature de sticky-bit fue introducido para permitir que el nexus switch operativo mantenga el rol de primario cuando el switch que reinició regresa.
- Cuando el proceso de elección de rol de vPC es ejecutado, el nexus con el sticky-bit con el valor de TRUE se convierte en primario no importando los otros parámetros de elección.

Verificación

```
show system internal vpcm info global | include ignore-case sticky
```

```
Sticky Master: TRUE
```

```

sh vpc
Legend:
      (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id           : 1
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : failed
Type-2 inconsistency reason : SVI type-2 configuration incompatible
vPC role                : primary
Number of vPCs configured : 1
Peer Gateway            : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Enabled, timer is off.(timeout = 240s)
Delay-restore status    : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Enabled
Virtual-peerlink mode   : Disabled

```

```

vPC Peer-link status
-----
id   Port   Status Active vlans
--   ---   -----
1    Po3    up     1-2,100-105,999

```

```

vPC status
-----
Id   Port           Status Consistency Reason           Active vlans
--   ---           -----
1    Po1            up     failed vPC type-1 configuration incompatible - STP interface port type inconsistent 2,100,105

```

Inconsistencias en un dominio de vPC

- La ‘running-configuration’ de ambos vPC Peers debe ser idéntica desde la perspectiva Capa 2.
- En caso de que la configuración no sea igual, diferentes alertas se mostrarán dentro del Dominio de VPC, algunas configuraciones se categorizan como de “Tipo 1” y otras de “Tipo 2”.

Inconsistencias Tipo 1

Las inconsistencias de Tipo 1 se activa cuando la configuración de STP no es igual, ya sea de forma global o en interfaces específicas.

Con una inconsistencia de Tipo 1, el dispositivo designado como Secondary cambiaría el estado de sus vPC member ports a "Down".

Parametro	Valor
Spanning-Tree Mode	Rapid PVST+ or MST
Spanning-Tree Enabled/Disabled state per VLAN	Yes or No
Spanning-Tree Region configuration for MST	Region Name, Region Revision, Region Instance to VLAN mapping
Spanning-tree Global Settings	Bridge Assurance Settings Port Type Settings Loop Guard Settings BPDU Filter Settings MST Simulate PVST enabled or disabled

Inconsistencias Tipo 1 (Global)

Inconsistencias Tipo 1 per vPC port-channel

Parámetro	Valor
Port-Channel LACP Mode	On, Active, Passive
Link Speed per Port-Channel	Speed in Mbps
Duplex mode per Port-Channel	Half-Duplex or Full-Duplex
Switchport mode per Port-Channel	Trunk or Access Native VLAN
STP interface settings	Port type Setting Loop Guard Root Guard
MST Simulate PVST	Enable or Disable
MTU per Port-Channel	Maximum Transmission Unit (MTU) Value

Inconsistencias Tipo 2

Las inconsistencias de Tipo 2 se presentan con problemas en la configuración de SVIs, VLAN Database, HSRP, QoS, ACLs y static MAC Entries.

Para las inconsistencias Tipo 2, ambos Peers mantienen sus links arriba, pero se generarán mensajes en el syslog.

Inconsistencias Tipo 2

Parámetro	Valor
Mac aging timers	MAC aging timer for a particular VLAN should be the same on both vPC peer devices
Static mac entries	Static MAC entries in a particular VLAN should be applied on both vPC peer devices.
VLAN interface (SVI)	Each peer device must have a VLAN interface configured for the same VLAN on both ends, and this VLAN interface must be in the same operational state.
ACL (Access Control List) configuration and parameters	ACL configurations should be identical on both vPC peer devices.
Quality of Service (QoS) configuration and parameters	QoS configuration should be identical on both vPC peer devices.
Spanning-tree protocol interface settings	Bridge Protocol Data Unit (BPDU) filter Link type (auto, point-to-point, shared) Cost Port-priority STP interface settings should be identical on both vPC peer devices.
VLAN database	You must create all VLANs on both the primary and secondary vPC peer devices, or the VLAN will be suspended. Those VLANs configured on only one peer device do not pass traffic using the vPC or vPC peer-link.
Port security	Network Access Control (NAC) Dynamic ARP Inspection (DAI) IP source guard (IPSG) Port security settings should be identical on both vPC peer devices.

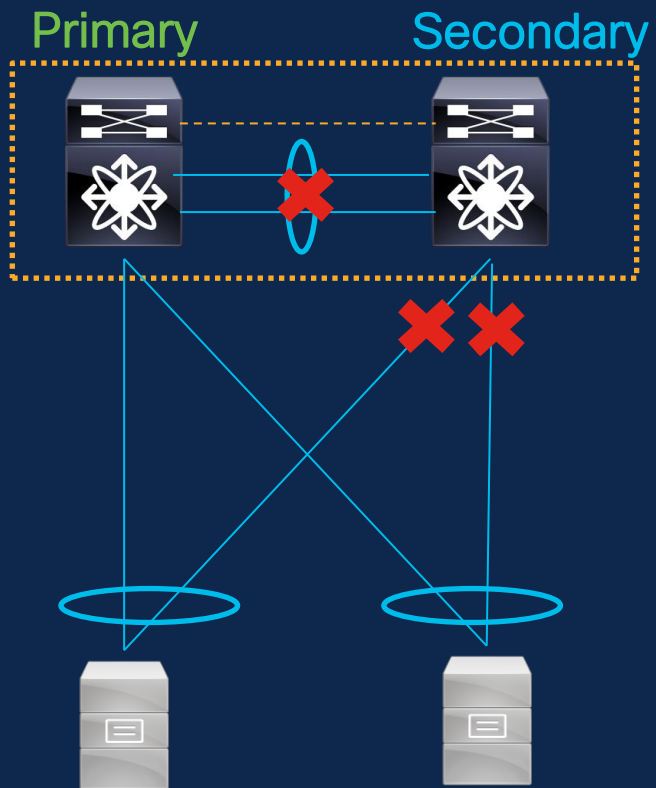
Inconsistencias Tipo 2

Parámetro	Valor
Cisco TrustSec	Cisco TrustSec configuration should be identical on both vPC peer devices.
Dynamic Host Configuration Protocol (DHCP) snooping	DHCP snooping configuration should be identical on both vPC peer devices.
Internet Group Management Protocol (IGMP) snooping	DHCP snooping configuration should be identical on both vPC peer devices.
Hot Standby Router Protocol (HSRP)	HSRP configuration should be identical on both vPC peer devices.
Protocol Independent Multicast (PIM)	PIM configuration should be identical on both vPC peer devices.
Gateway Load-Balancing Protocol (GLBP)	GLBP configuration should be identical on both vPC peer devices.
All routing protocol configurations	Routing configuration should be consistent on both vPC peer devices.

Falla del Peer-Link

En el caso de que todos los miembros del vPC Peer-Link se vayan abajo, el dominio de vPC reacciona de forma automática, mandando a "Down" a todos los puertos del vPC Secondary Peer.

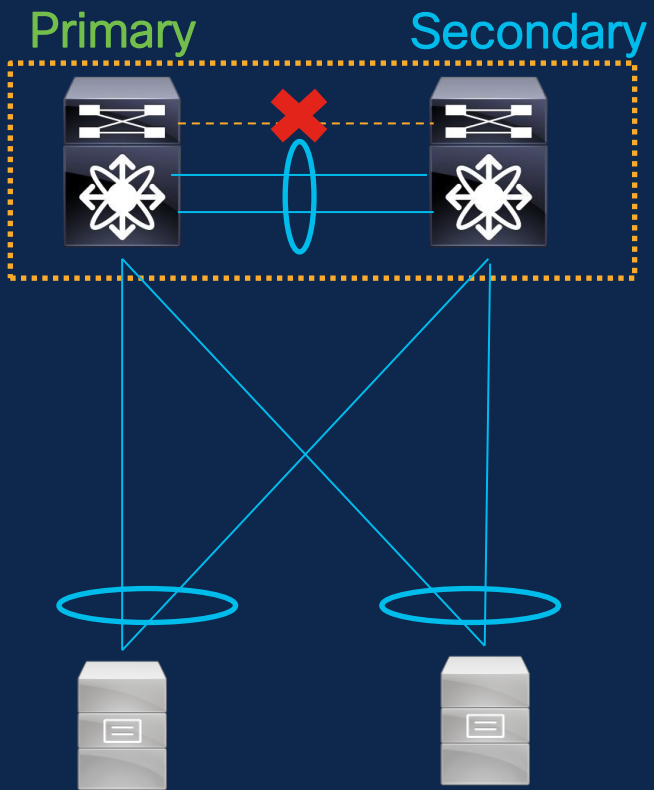
Dado que el Peer Keep-Alive sigue arriba, los vPC Peers son capaces de detectar que aún existe un Peer activo, así que no ocurre un cambio de roles entre los Peers.



Falla del Peer-Link

En el caso de que todos los miembros del vPC Peer-Link se vayan abajo, el dominio de vPC reacciona de forma automática, mandando a "Down" a todos los puertos del vPC Secondary Peer.

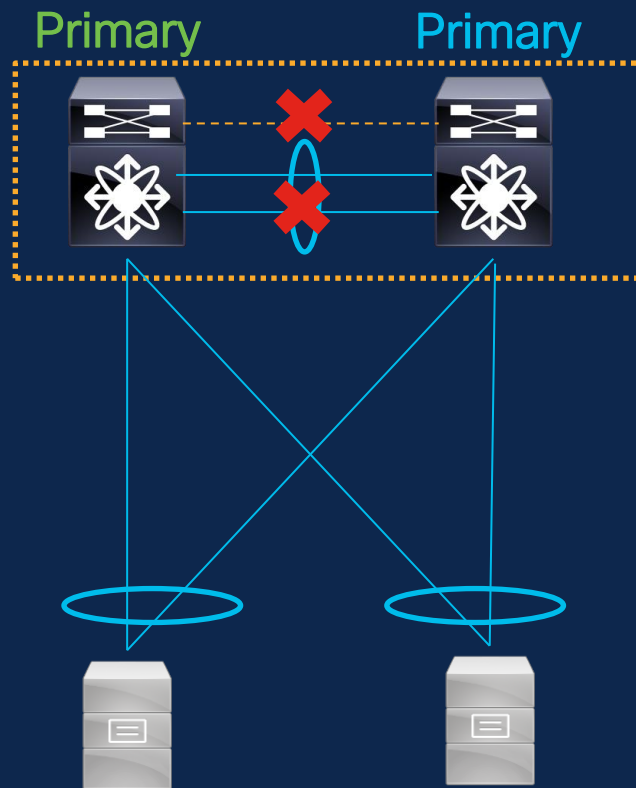
Dado que el Peer Keep-Alive sigue arriba, los vPC Peers son capaces de detectar que aún existe un Peer activo, así que no ocurre un cambio de roles entre los Peers.



Falla del Peer Keep-Alive

Cuando perdemos conectividad a la dirección IP del VPC Peer a través del VPC Peer Keep-Alive no hay ningún impacto.

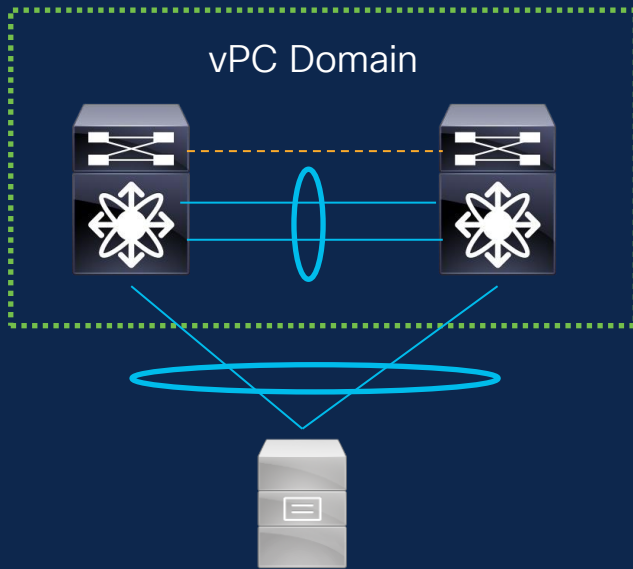
Falla del Peer Keep-Alive y seguido de falla del Peer-Link



Este es un escenario problemático, ya que cuando el Peer-Link se cae después de que el Keep-Alive no está activo, ambos vPC Peers tratan de asignarse el rol de vPC Primary, creando así lo que se conoce como un “Split-Brain” escenario.

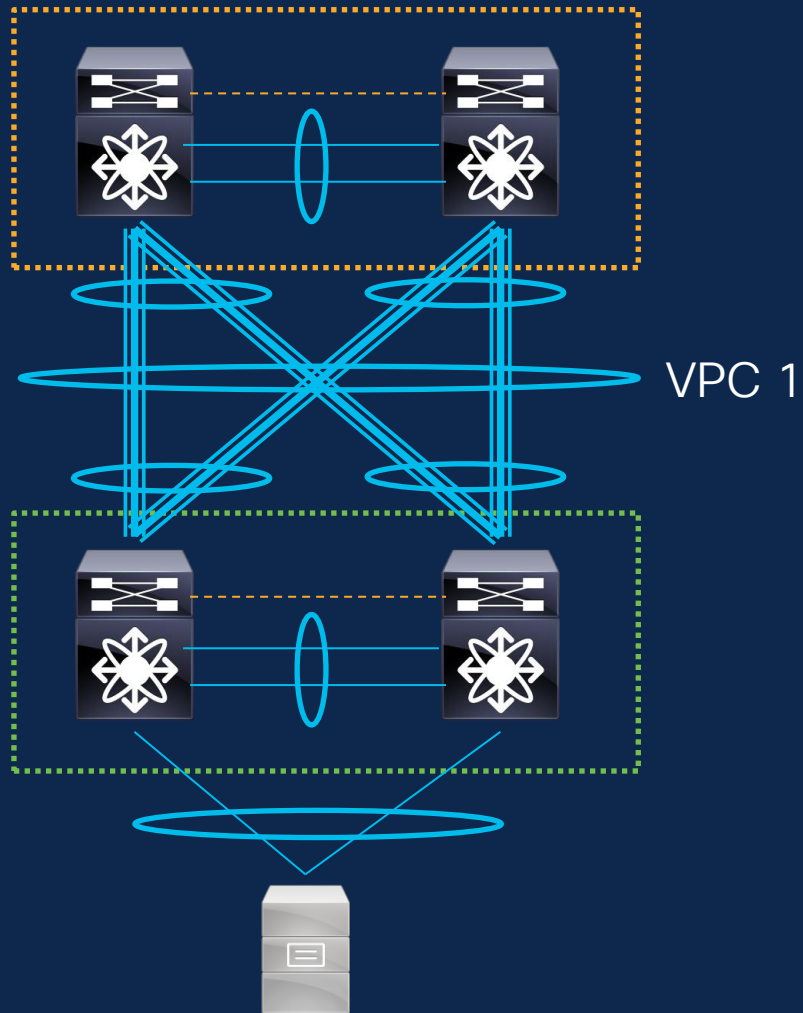
Esto puede ocasionar un escenario donde se envíen paquetes duplicados.

vPC Escenarios de implementación



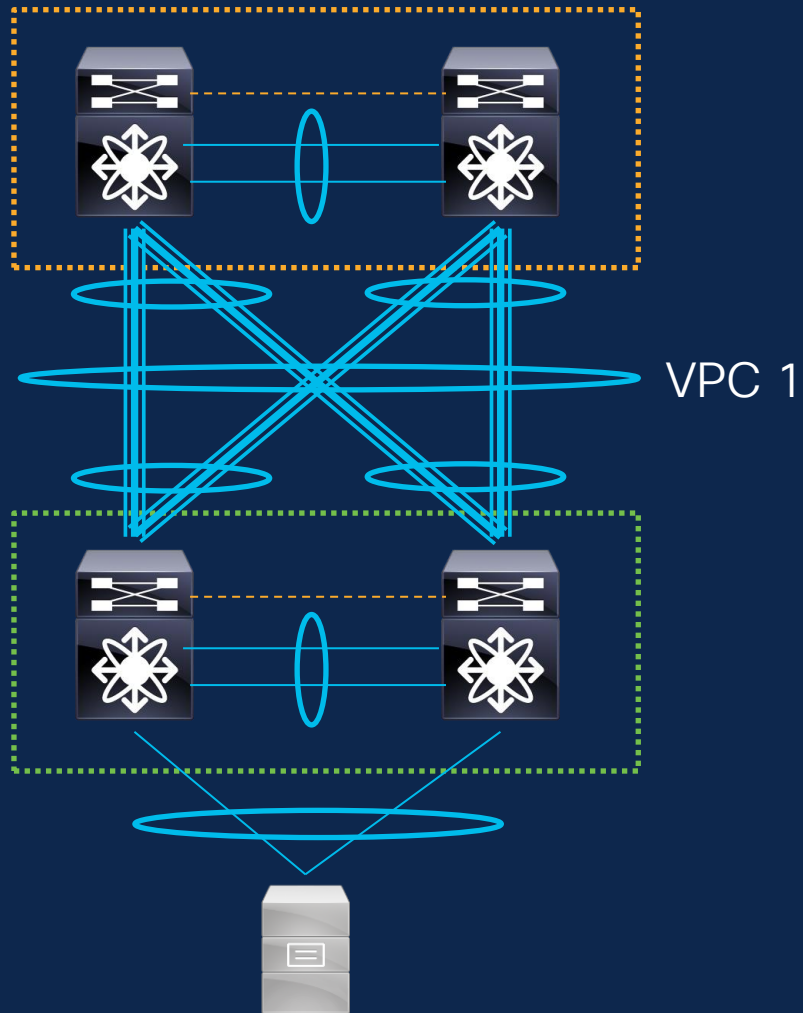
Single-sided vPC

Los equipos se encuentran directamente conectados a un par de nexus en vPC.



Double-sided vPC

Esta topología usa dos dominios de vPC en el cual la conexión entre los dos dominios es un vPC.



Double-sided vPC

Esta topología usa dos dominios de vPC en el cual la conexión entre los dos dominios es un vPC.



Join at
slido.com
#4040 626

🔑 Passcode:
sl4ksb

En el caso de que tu red consista de uno o varios Dominios de vPC complicado has encontrado el troubleshooting de este protocolo?

A) Sencillo

0%

B) Complicado

0%

C) Muy complicado

0%

D) No he troubleshootado vPC

0%

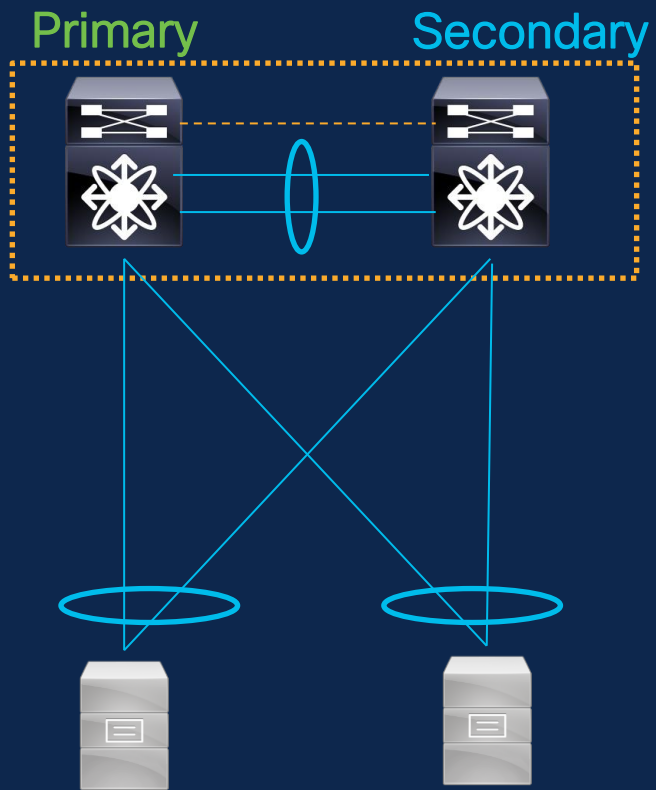
Mejores Prácticas con VPC

vPC Keep-Alive

- Cisco recomienda configurar una VRF dedicada para el tráfico del vPC Keep-Alive y asociar las interfaces de Capa 3 a esta VRF para mantenerlas en una tabla de ruteo independiente.
- vPC utilizará la VRF de management por default, lo cual también es una 'best-practice'.
- Podemos usar también una interfaz de Capa 2 para enviar vPC Keep-Alives, siempre y cuando se usen Non-vPC VLANs.

vPC Peer-Link

- Si se tiene un Nexus modular, usar una interfaz de cada módulo.
- Utilizar más de 1 interfaz física en el Port-Channel.
- Permitir solo las VLANs que serán vPC VLANs.
- No poner ningún equipo entre los dos VPC Peers. (El Peer-Link debe ser una conexión Point-to-Point).

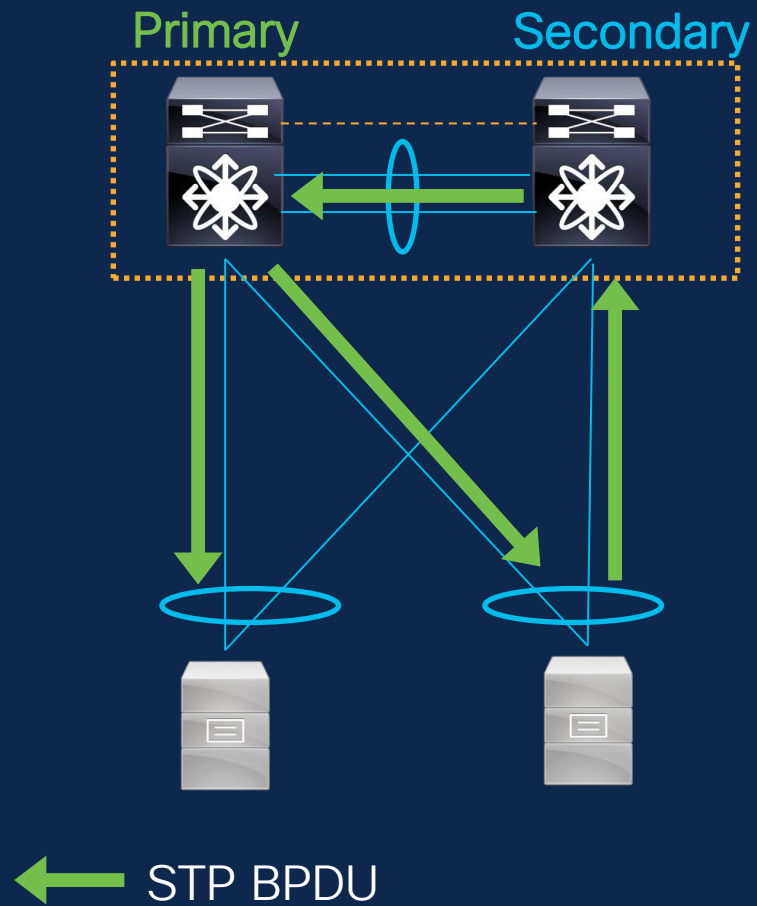


- Vista de spanning-tree sin peer-switch

VPC Peer-Switch

- El feature vPC peer-switch permite que un par de vPC switches actúen como una sola instancia de spanning-tree root en una topología de capa 2.
- Con el feature “peer-switch” ambos switches procesarán los BPDUs y generarán BPDUs con la vPC system mac como root.
- Uno de los requerimientos para usar este feature es que ambos vPC Peers deben tener la misma prioridad de STP configurada manualmente.
- Se recomienda utilizar este feature solo en el vPC que funge como el STP Root de la red.

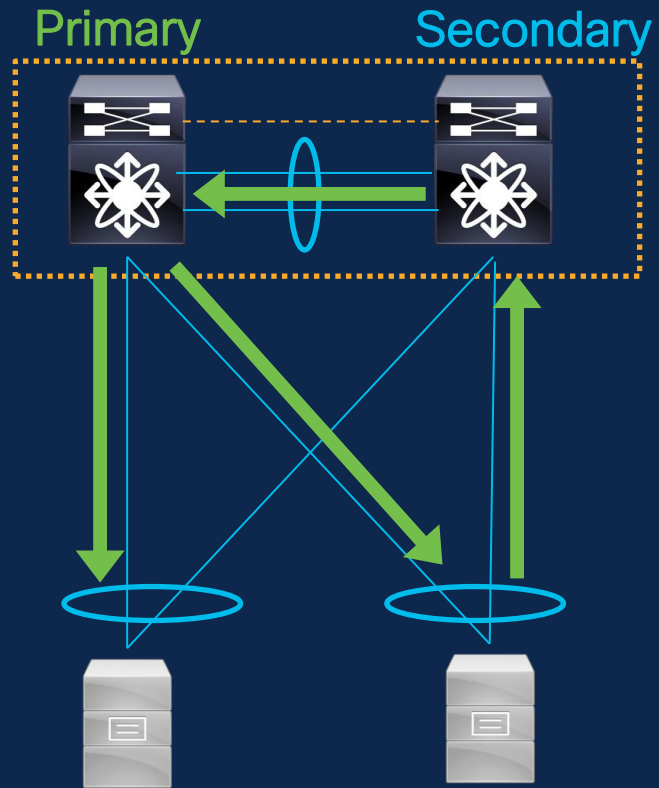
VPC Peer-Switch



- Procesamiento de spanning-tree sin peer-switch

- El feature vPC peer-switch permite que un par de vPC switches actúen como una sola instancia de spanning-tree root en una topología de capa 2.
- Con el feature “peer-switch” ambos switches procesarán los BPDUs y generarán BPDUs con la vPC system mac como root.
- Uno de los requerimientos para usar este feature es que ambos vPC Peers deben tener la misma prioridad de STP configurada manualmente.
- Se recomienda utilizar este feature solo en el vPC que funge como el STP Root de la red.

VPC Peer-Switch



← STP BPDU

- Procesamiento de spanning-tree sin peer-switch

```
show int po 3 | i i addr
```

```
Hardware: Port-Channel, address: 4c77.6d9b.10e4 (bia 4c77.6d9b.10e4)
```

```
show span vlan 101
```

```
MST1001
```

```
Spanning tree enabled protocol mstp
```

```
Root ID    Priority    5097
```

```
Address    a80c.0d96.437f
```

```
This bridge is the root
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID  Priority    5097 (priority 4096 sys-id-ext 1001)
```

```
Address    a80c.0d96.437f
```

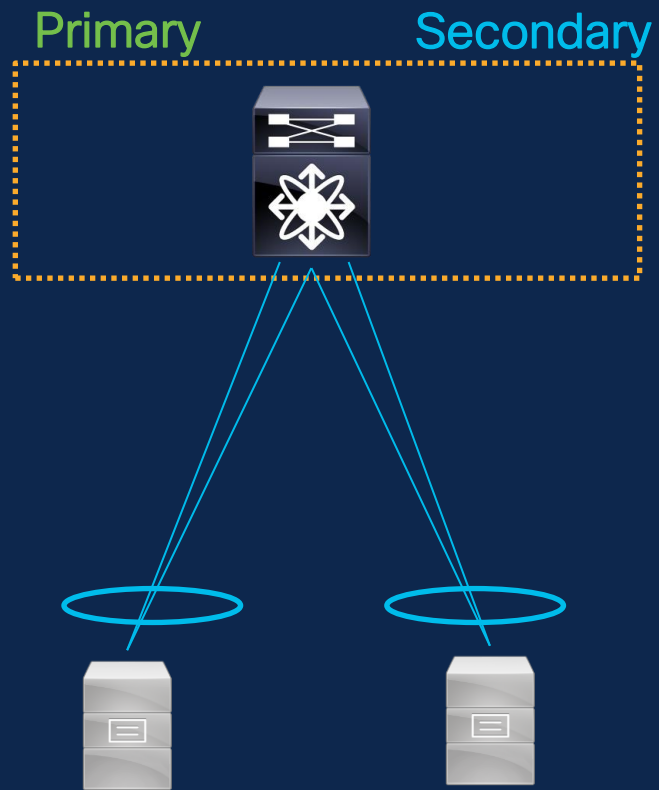
```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po3	Desg	FWD	1000	128.4098	(vPC peer-link) Network P2p

```
ethanalyzer local interface inband display-filter stp limit-cap 0
```

```
Capturing on 'ps-inb'
```

```
4c:77:6d:9b:10:e4 → 01:80:c2:00:00:00 STP 135 MST. Root = 4096/0/a8:0c:0d:96:43:7f Cost = 0 Port = 0x9002
```

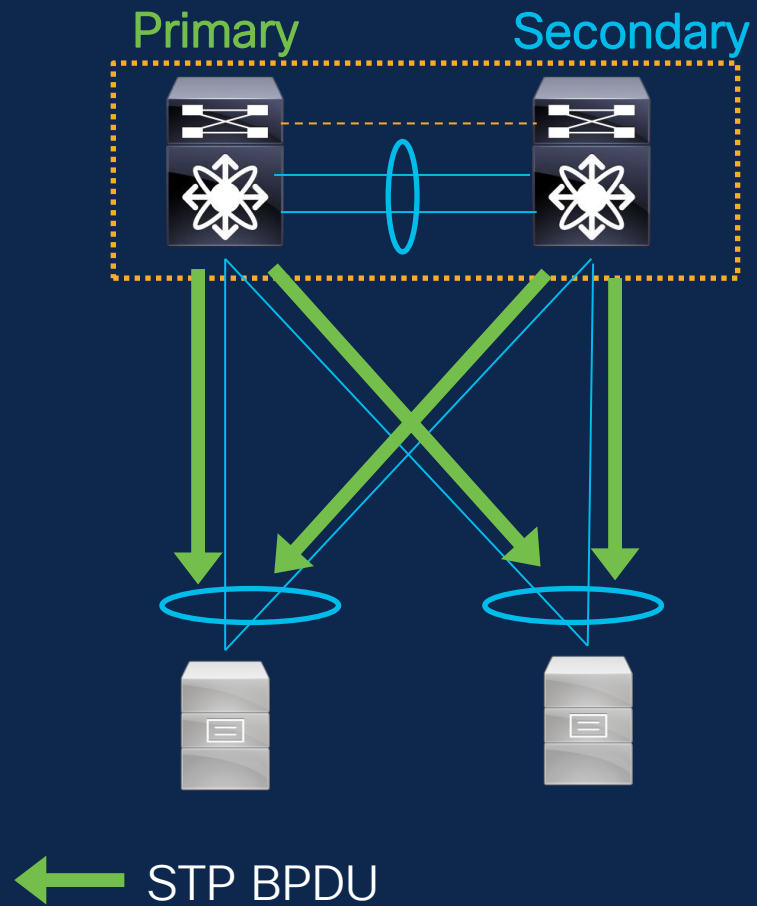


- Vista de spanning-tree con peer-switch

VPC Peer-Switch

- El feature vPC peer-switch permite que un par de vPC switches actúen como una sola instancia de spanning-tree root en una topología de capa 2.
- Con el feature “peer-switch” ambos switches procesarán los BPDUs y generarán BPDUs con la vPC system mac como root.
- Uno de los requerimientos para usar este feature es que ambos vPC Peers deben tener la misma prioridad de STP configurada manualmente.
- Se recomienda utilizar este feature solo en el vPC que funge como el STP Root de la red.

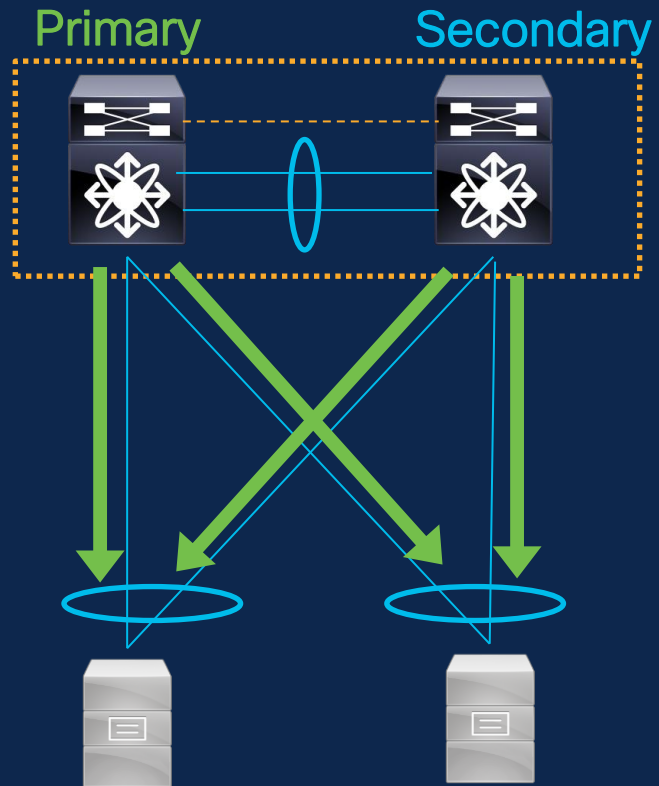
VPC Peer-Switch



- Procesamiento de spanning-tree con peer-switch

- El feature vPC peer-switch permite que un par de vPC switches actúen como una sola instancia de spanning-tree root en una topología de capa 2.
- Con el feature “peer-switch” ambos switches procesarán los BPDUs y generarán BPDUs con la vPC system mac como root.
- Uno de los requerimientos para usar este feature es que ambos vPC Peers deben tener la misma prioridad de STP configurada manualmente.
- Se recomienda utilizar este feature solo en el vPC que funge como el STP Root de la red.

VPC Peer-Switch



← STP BPDUs

- Procesamiento de spanning-tree con peer-switch

```
show int po 3 | i i addr
```

```
Hardware: Port-Channel, address: 4c77.6d9b.10e4 (bia 4c77.6d9b.10e4)
```

```
show span vlan 101
```

```
MST1001
```

```
Spanning tree enabled protocol mstp
```

```
Root ID Priority 5097
```

```
Address 0023.04ee.be64
```

```
This bridge is the root
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 5097 (priority 4096 sys-id-ext 1001)
```

```
Address 0023.04ee.be64
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

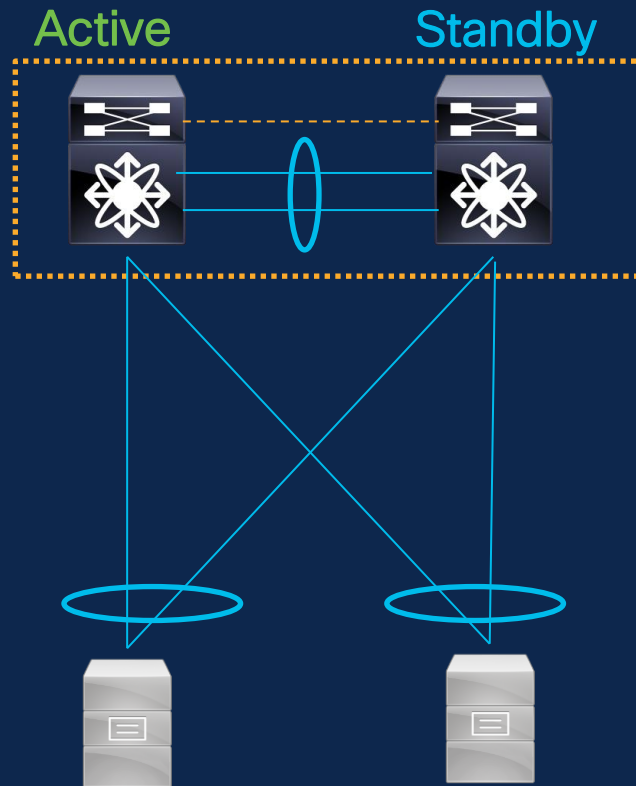
Interface	Role	Sts	Cost	Prio.Nbr	Type
Po3	Root	FWD	1000	128.4098	(vPC peer-link) Network P2p

```
ethanalyzer local interface inband display-filter stp limit-cap 0
```

```
Capturing on 'ps-inb'
```

```
4c:77:6d:9b:10:e4 → 01:80:c2:00:00:00 STP 135 MST. Root = 4096/0/00:23:04:ee:be:64 Cost = 0 Port = 0x9002
```

HSRP

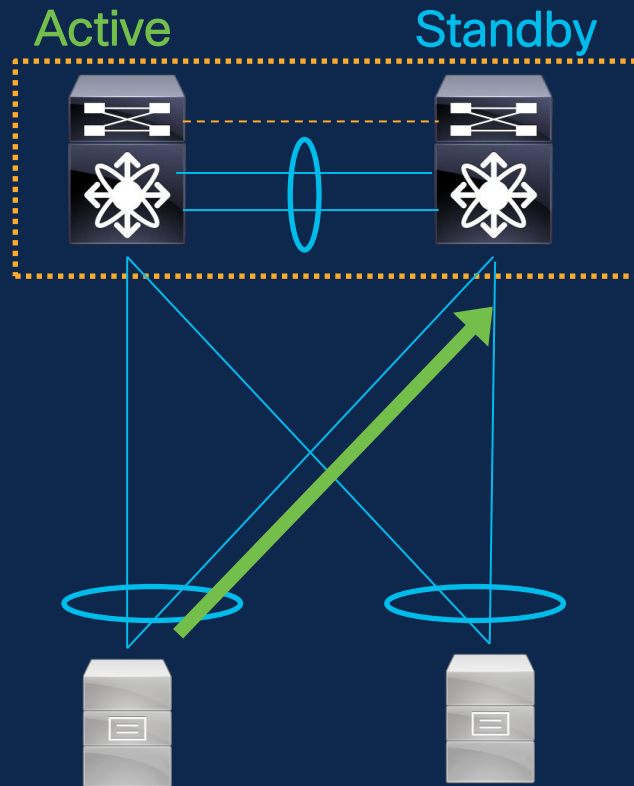


Peer-gateway

vPC Peer-Gateway permite que el vPC Peer funcione como el Gateway activo para los paquetes destinados a la Router MAC del vPC Peer.

Al habilitar 'peer-gateway', los dos vPC Peers activan una Gateway Flag a la MAC Address que funge como Gateway (G-Flag).

HSRP



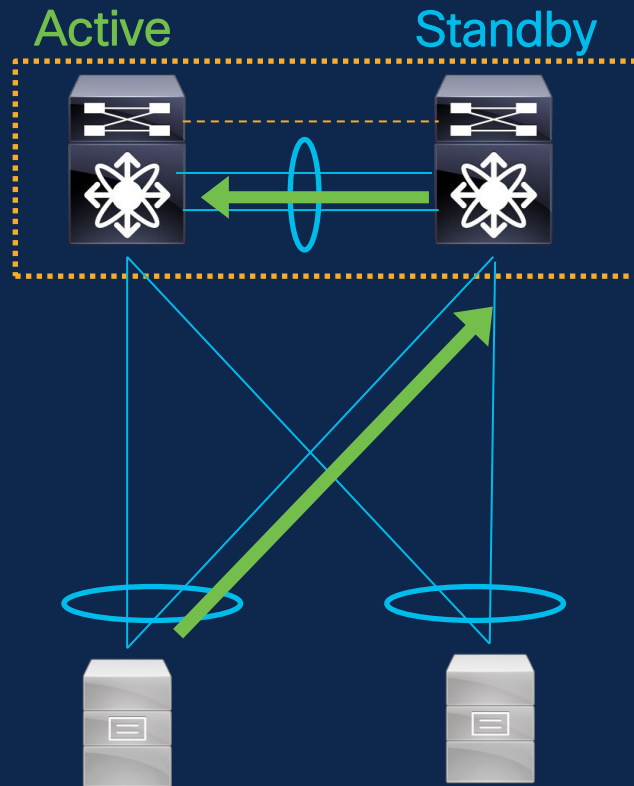
- Flujo del paquete sin peer-gateway

Peer-gateway

vPC Peer-Gateway permite que el vPC Peer funcione como el Gateway activo para los paquetes destinados a la Router MAC del vPC Peer.

Al habilitar 'peer-gateway', los dos vPC Peers activan una Gateway Flag a la MAC Address que funge como Gateway (G-Flag).

HSRP



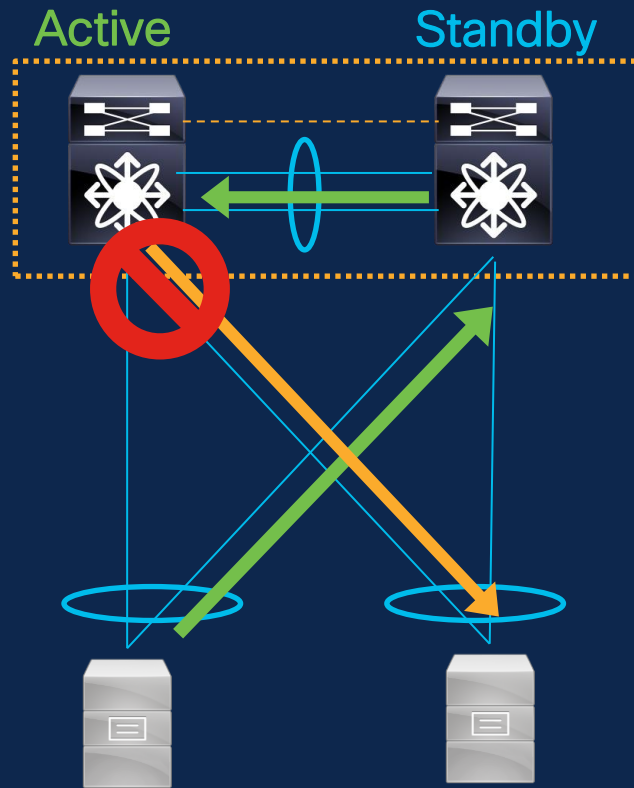
- Flujo del paquete sin peer-gateway

Peer-gateway

vPC Peer-Gateway permite que el vPC Peer funcione como el Gateway activo para los paquetes destinados a la Router MAC del vPC Peer.

Al habilitar 'peer-gateway', los dos vPC Peers activan una Gateway Flag a la MAC Address que funge como Gateway (G-Flag).

HSRP



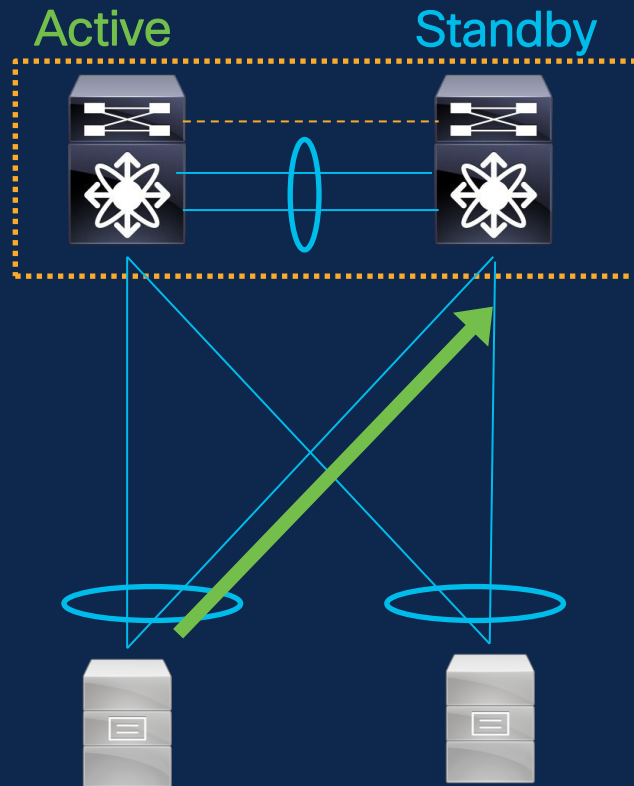
- Flujo del paquete sin peer-gateway

Peer-gateway

vPC Peer-Gateway permite que el vPC Peer funcione como el Gateway activo para los paquetes destinados a la Router MAC del vPC Peer.

Al habilitar 'peer-gateway', los dos vPC Peers activan una Gateway Flag a la MAC Address que funge como Gateway (G-Flag).

HSRP



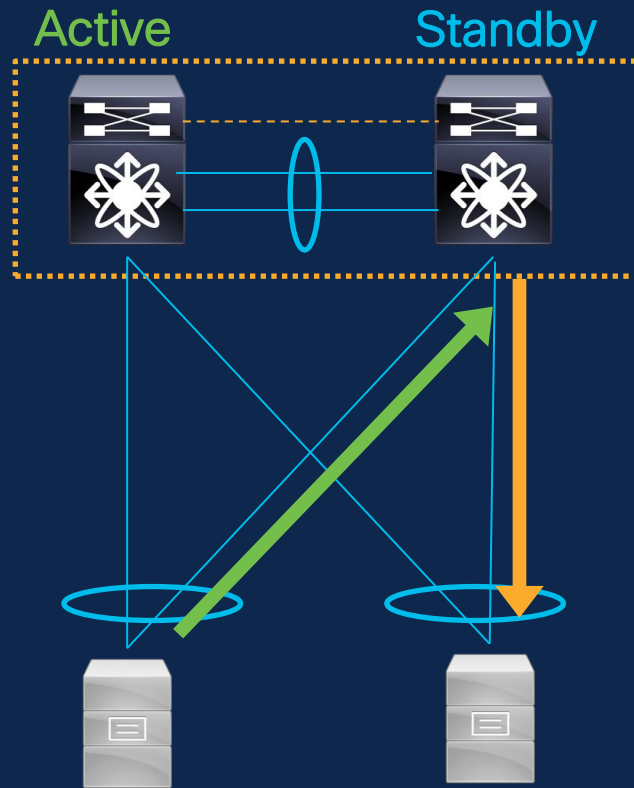
- Flujo del paquete peer-gateway

Peer-gateway

vPC Peer-Gateway permite que el vPC Peer funcione como el Gateway activo para los paquetes destinados a la Router MAC del vPC Peer.

Al habilitar 'peer-gateway', los dos vPC Peers activan una Gateway Flag a la MAC Address que funge como Gateway (G-Flag).

HSRP



- Flujo del paquete con-gateway

Peer-gateway

vPC Peer-Gateway permite que el vPC Peer funcione como el Gateway activo para los paquetes destinados a la Router MAC del vPC Peer.

Al habilitar 'peer-gateway', los dos vPC Peers activan una Gateway Flag a la MAC Address que funge como Gateway (G-Flag).

```
sh run vpc
```

```
vpc domain 100  
  peer-keepalive destination 10.122.164.79 source 10.122.165.182  
  peer-gateway
```

```
sh vpc
```

```
vPC domain id           : 1  
Peer status             : peer adjacency formed ok  
vPC keep-alive status  : peer is alive  
vPC role                : primary  
Number of vPCs configured : 1
```

```
<Snipped>
```

```
Peer Gateway           : Enabled
```

```
sh hsrp interface vlan 101 | i i virtual
```

```
Virtual IP address is 10.100.1.1 (Cfged)  
Virtual mac address is 0000.0c9f.f001 (Default MAC)
```

```
Sh mac ad address 0000.0c9f.f001
```

```
Legend:
```

```
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC  
age - seconds since last seen,+ - primary entry using vPC Peer-Link,  
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
G 101	0000.0c9f.f001	static	-	F	F	sup-eth1 (R)

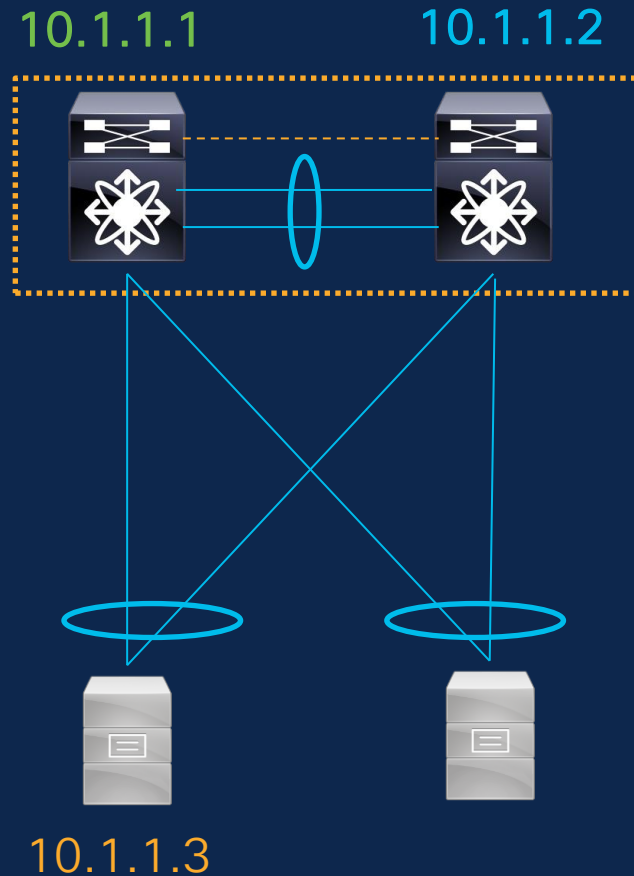
Peer-gateway

VPC Layer3 Peer-Router

“layer3 peer-router” es un comando que se agregó al ecosistema de NXOS a partir de la versión 7.1(1)D1 para poder soportar adyacencias de routing protocols sobre un dominio de vPC.

Este feature permite que el TTL del paquete no se decremente cuando tiene que cruzar el Peer-Link.

Antes de este 'enhancement', para poder tener routing a través de un dominio de vPC era obligatorio usar un link de L3 dedicado entre ambos vPC Peers.



← OSPF unicast update hacia 10.1.1.1

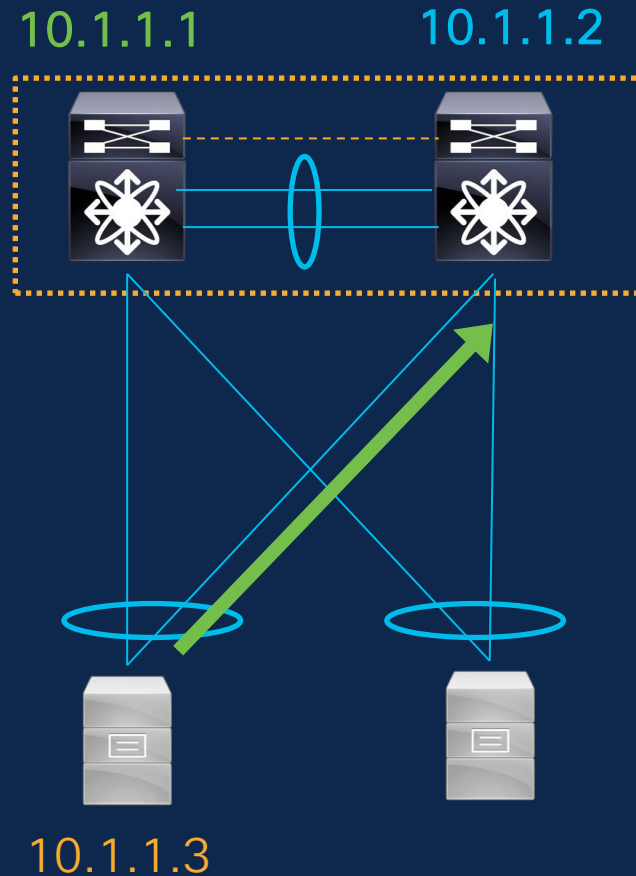
- Flujo del paquete sin layer3 peer-router

VPC Layer3 Peer-Router

“layer3 peer-router” es un comando que se agregó al ecosistema de NXOS a partir de la versión 7.1(1)D1 para poder soportar adyacencias de routing protocols sobre un dominio de vPC.

Este feature permite que el TTL del paquete no se decremente cuando tiene que cruzar el Peer-Link.

Antes de este 'enhancement', para poder tener routing a través de un dominio de vPC era obligatorio usar un link de L3 dedicado entre ambos vPC Peers.



← OSPF unicast update hacia 10.1.1.1

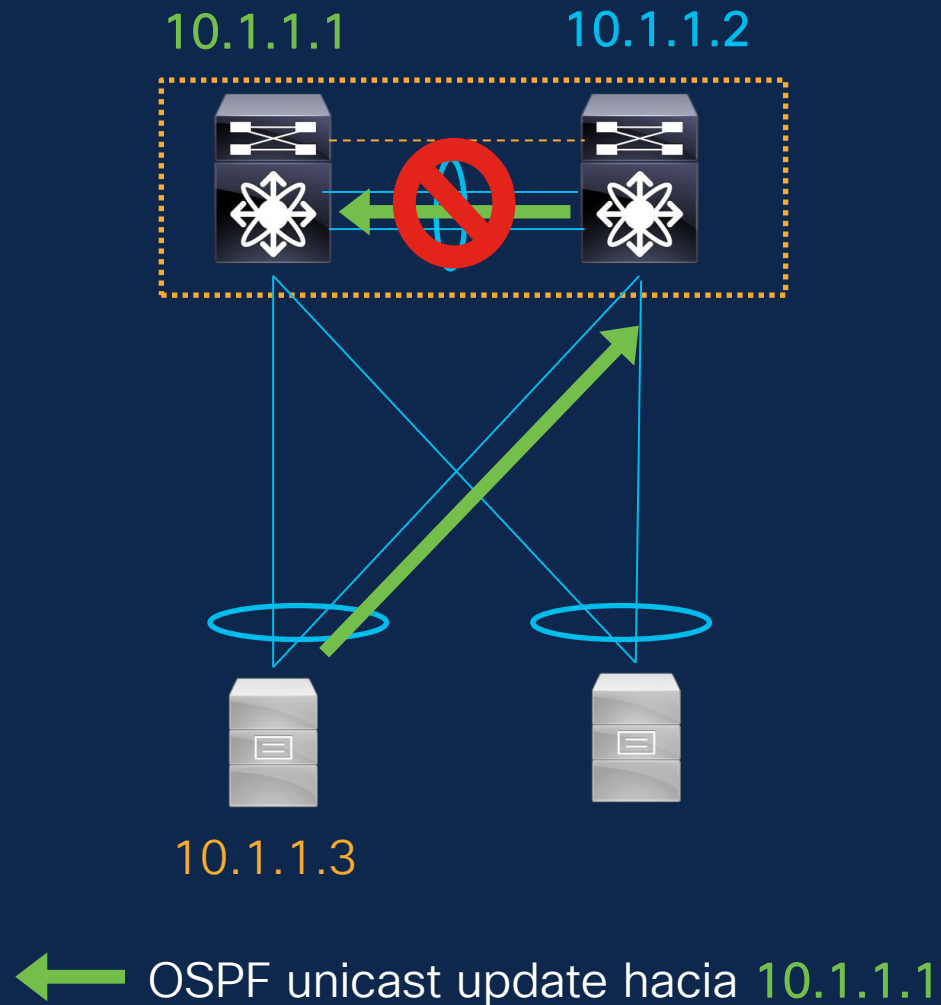
- Flujo del paquete sin layer3 peer-router

VPC Layer3 Peer-Router

“layer3 peer-router” es un comando que se agregó al ecosistema de NXOS a partir de la versión 7.1(1) D1 para poder soportar adyacencias de routing protocols sobre un dominio de vPC.

Este feature permite que el TTL del paquete no se decremente cuando tiene que cruzar el Peer-Link.

Antes de este 'enhancement', para poder tener routing a través de un dominio de vPC era obligatorio usar un link de L3 dedicado entre ambos vPC Peers.



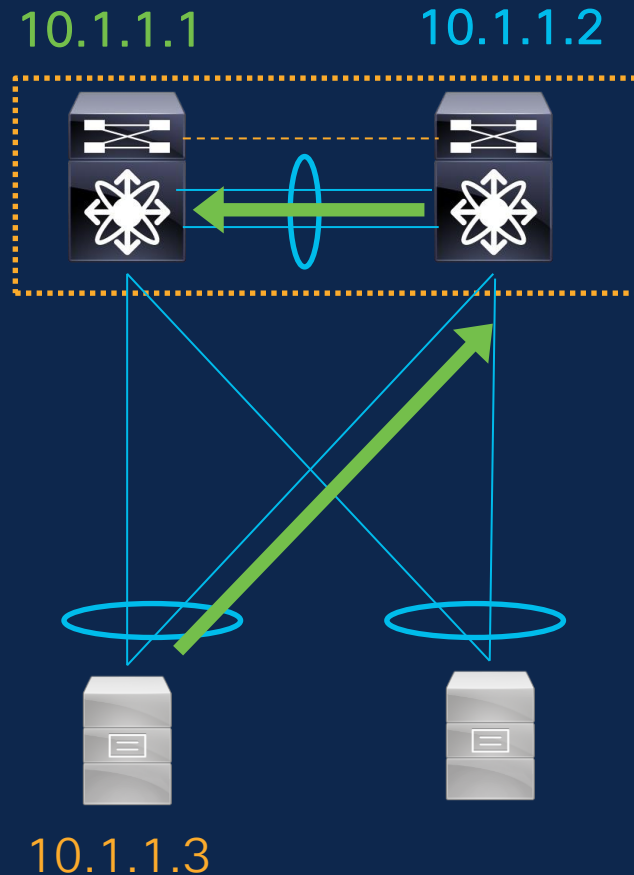
- Flujo del paquete sin layer3 peer-router

VPC Layer3 Peer-Router

“layer3 peer-router” es un comando que se agregó al ecosistema de NXOS a partir de la versión 7.1(1)D1 para poder soportar adyacencias de routing protocols sobre un dominio de vPC.

Este feature permite que el TTL del paquete no se decremente cuando tiene que cruzar el Peer-Link.

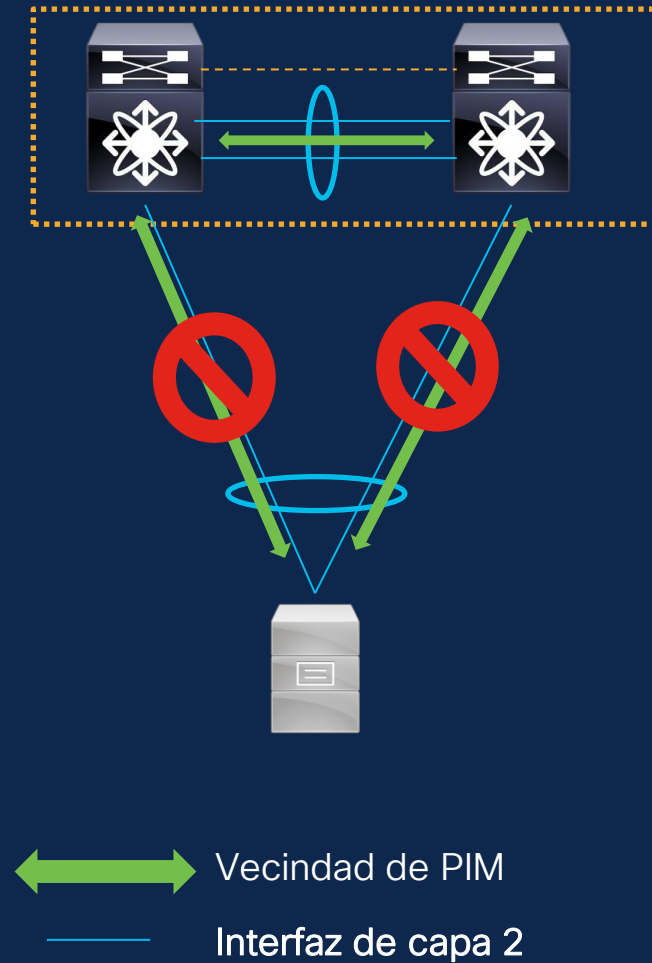
Antes de este 'enhancement', para poder tener routing a través de un dominio de vPC era obligatorio usar un link de L3 dedicado entre ambos vPC Peers.



← OSPF unicast update hacia 10.1.1.1

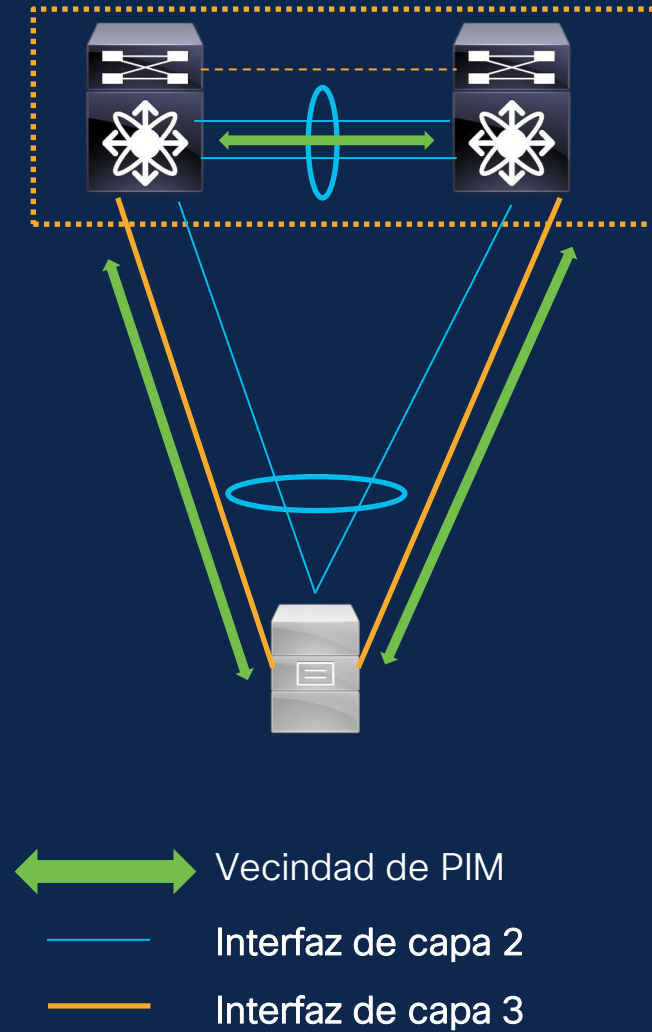
- Flujo del paquete con layer3 peer-router

Vecindades de PIM



- En vPC la única adyacencia de PIM sobre vPC VLANs permitía es con el vPC peer
- Cualquier otra adyacencia con otro equipo usando vPC VLANS no es soportado
- Para tener adyacencia con otro equipo con vPC se necesita un link dedicado de capa 3 o un link de capa 2 dedicado con una non-vPC vlan

Vecindades de PIM



- En vPC la única adyacencia de PIM sobre vPC VLANs permitía es con el vPC peer
- Cualquier otra adyacencia con otro equipo usando vPC VLANS no es soportado
- Para tener adyacencia con otro equipo con vPC se necesita un link físico dedicado de capa 3 configurado con una ip o un link de capa 2 dedicado con una non-vPC vlan

vPC Domain id

El ID del Dominio de vPC se utiliza para generar la MAC Virtual que los vPC Peers utilizarán en sus paquetes de LACP, así como en sus paquetes de STP.

Como recomendación general, no se debe tener dos dominios de vPC con el mismo ID dentro del mismo dominio de Broadcast.

Esto podría causar conflictos para la estabilidad de STP en las VLANs afectadas. Especialmente si el feature 'peer-switch' está habilitado, ya que, al habilitarlo, el procesamiento del BPDU cambia para todas las VLANs, no sólo para las vPC VLANs.

Laboratorio día 0

Features

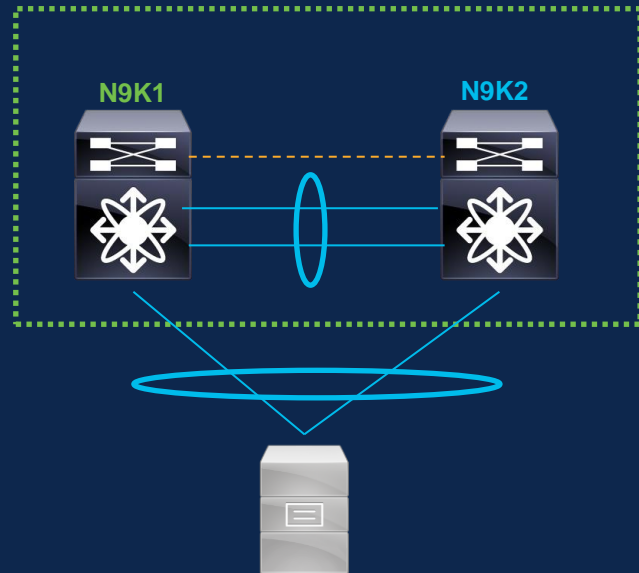
Feature vpc

Feature lacp

Feature ospf

Feature hsrp

Definiendo vPC peer-keepalive



Definiendo vPC peer-keepalive



Configuración

N9K1

```
interface mgmt0
  description VPC Keepalive
  ip address 1.1.1.1/24
  vrf member management
```

N9K2

```
interface mgmt0
  description VPC Keepalive
  ip address 1.1.1.2/24
  vrf member management
```

Definiendo vPC peer-keepalive



Verificación

N9K1

```
ping 1.1.1.2 source 1.1.1.1 vrf management
PING 1.1.1.2 (1.1.1.2) from 1.1.1.1 : 56 data bytes
64 bytes from 1.1.1.2 : icmp_seq=0 ttl=251 time=0.83 ms
64 bytes from 1.1.1.2 : icmp_seq=1 ttl=251 time=0.697 ms
64 bytes from 1.1.1.2 : icmp_seq=2 ttl=251 time=0.701 ms
64 bytes from 1.1.1.2 : icmp_seq=3 ttl=251 time=0.649 ms
64 bytes from 1.1.1.2 : icmp_seq=4 ttl=251 time=0.651 ms
```

--- 1.1.1.2 ping statistics ---

5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.649/0.705/0.83 ms

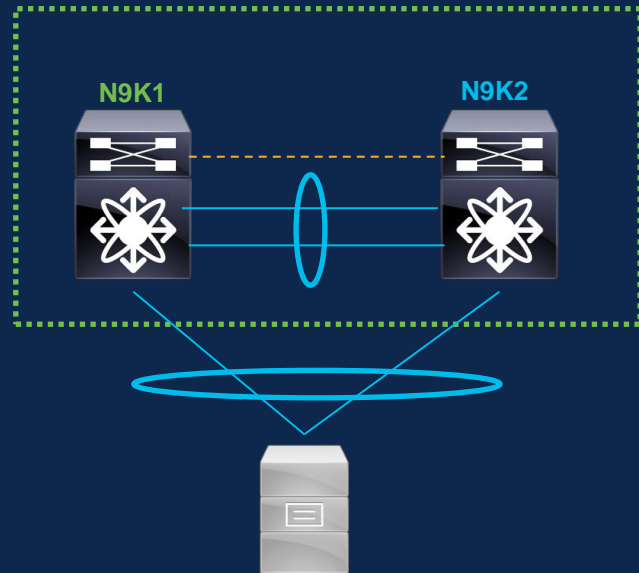
N9K2

```
ping 1.1.1.1 source 1.1.1.2 vrf management
PING 1.1.1.1 (1.1.1.1) from 1.1.1.2 : 56 data bytes
64 bytes from 1.1.1.1 : icmp_seq=0 ttl=251 time=0.895 ms
64 bytes from 1.1.1.1 : icmp_seq=1 ttl=251 time=0.678 ms
64 bytes from 1.1.1.1 : icmp_seq=2 ttl=251 time=0.621 ms
64 bytes from 1.1.1.1 : icmp_seq=3 ttl=251 time=0.663 ms
64 bytes from 1.1.1.1 64.79: icmp_seq=4 ttl=251 time=0.668 ms
```

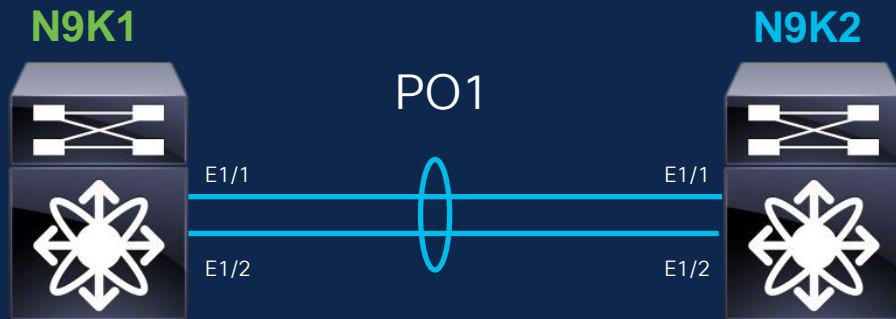
--- 1.1.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.621/0.704/0.895 ms

Definiendo vPC peer-link



Definiendo vPC peer-link



Configuración

N9K1

```
interface port-channel 1

interface Ethernet1/1-2
  channel-group 1 mode active

interface port-channel1
  description vPC-peer-link
  switchport
  switchport mode trunk
```

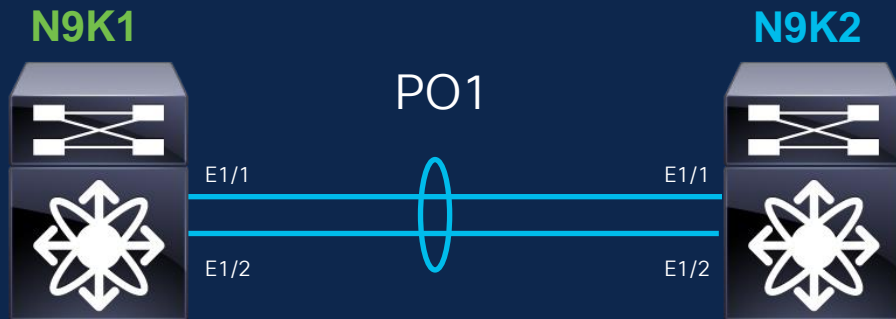
N9K2

```
interface port-channel 1

interface Ethernet1/1-2
  channel-group 1 mode active

interface port-channel1
  description vPC-peer-link
  switchport
  switchport mode trunk
```

Definiendo vPC peer-link



Verificación

N9K1

```
sh port-channel summary interface port-channel 1
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        b - BFD Session Wait
        S - Switched     R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

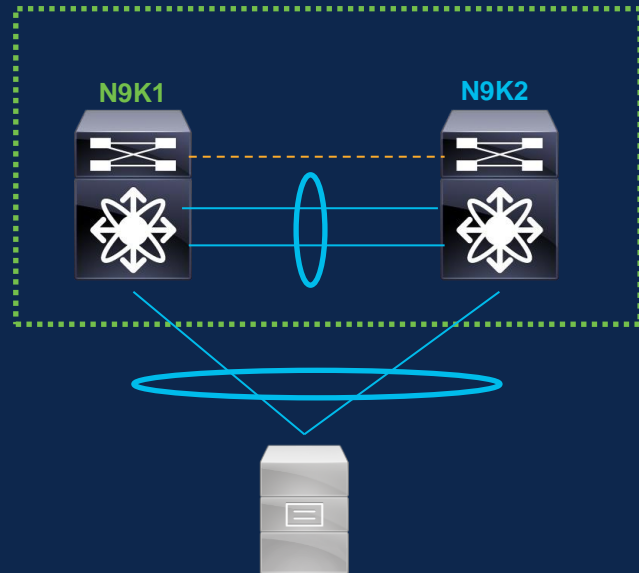
Group	Port-Channel	Type	Protocol	Member Ports
1	Pol(SU)	Eth	LACP	Eth1/1(P) Eth1/1(P)

N9K2

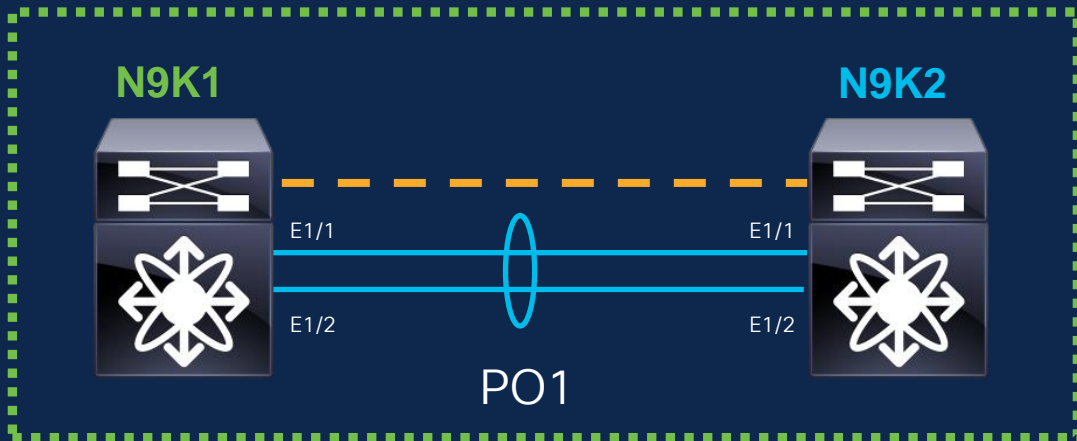
```
sh port-channel summary interface port-channel 1
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        b - BFD Session Wait
        S - Switched     R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

Group	Port-Channel	Type	Protocol	Member Ports
1	Pol(SU)	Eth	LACP	Eth1/1(P) Eth1/1(P)

Configuración de vPC



Configuración de vPC



Configuración

N9K1

```
vpc domain 1
  peer-keepalive destination 1.1.1.2 source 1.1.1.1

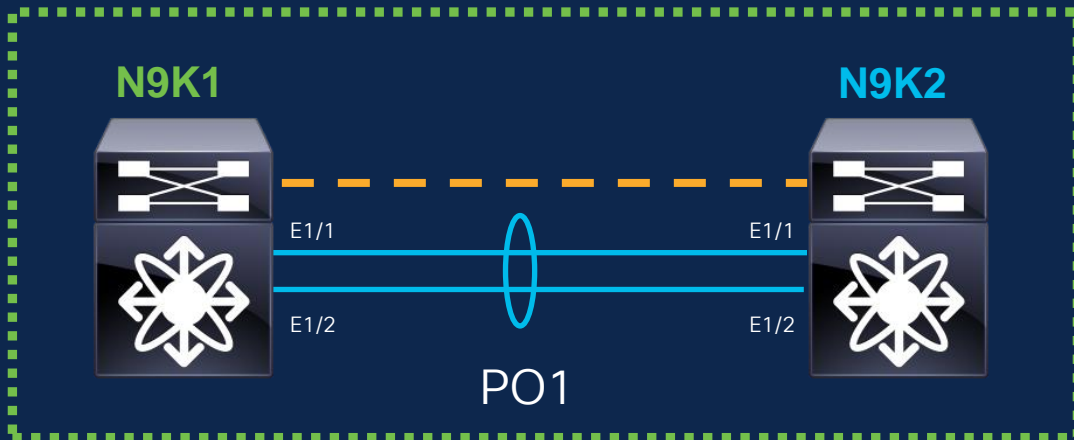
interface port-channel1
  vpc peer-link
```

N9K2

```
vpc domain 1
  peer-keepalive destination 1.1.1.1 source 1.1.1.2

interface port-channel1
  vpc peer-link
```

Configuración de vPC



Verificación

N9K1

```
show vpc
```

```
Legend:
```

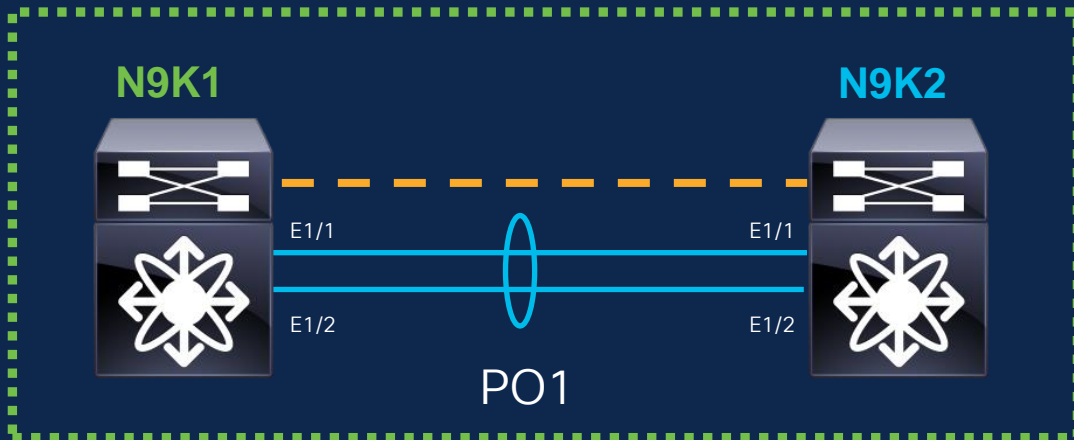
```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 1
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
Type-2 inconsistency reason : success
vPC role                : primary
Number of vPCs configured : 0
Peer Gateway            : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Enabled, timer is off.(timeout = 240s)
Delay-restore status     : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Enabled
Virtual-peerlink mode   : Disabled
```

vPC Peer-link status

```
-----
id      Port      Status Active vlans
-----
1       Po1       up      1-2,100-105,999
-----
```

Configuración de vPC



Verificación

N9K2

```
show vpc
```

```
Legend:
```

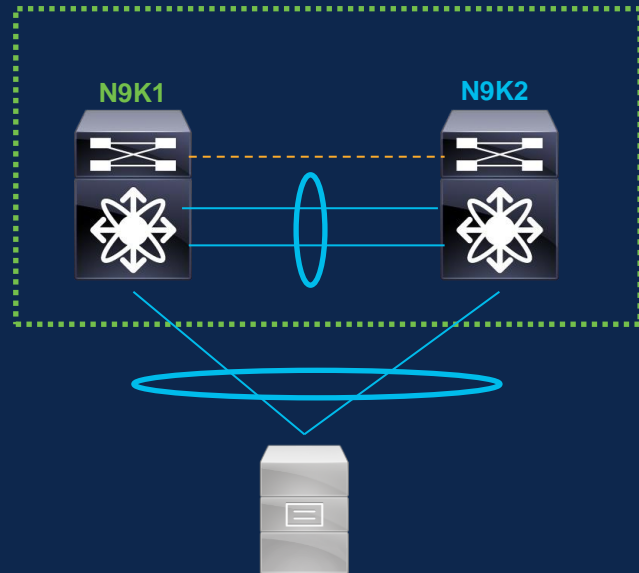
```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 1
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
Type-2 inconsistency reason : success
vPC role                 : secondary
Number of vPCs configured : 0
Peer Gateway            : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Enabled, timer is off.(timeout = 240s)
Delay-restore status     : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Enabled
Virtual-peerlink mode    : Disabled
```

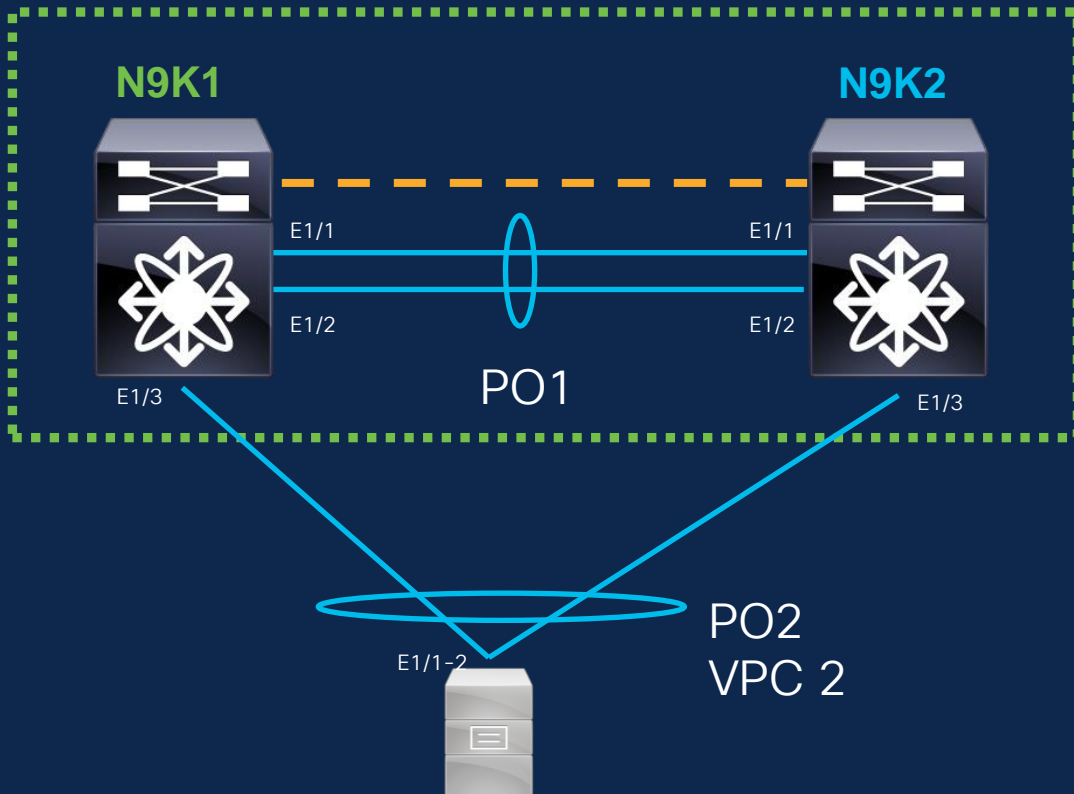
vPC Peer-link status

```
-----
id      Port      Status Active vlans
-----
1       Po1       up      1-2,100-105,999
-----
```

Configuración de vPC



Configuración de vPC



Configuración

N9K1

```
interface port-channel2
  description VPC 2
```

```
interface Ethernet1/3
```

```
  description Downlink to HOST
  channel-group 8 mode active
  no shutdown
```

```
interface port-channel2
  description VPC 2
  switchport
  switchport mode trunk
  vpc 2
  no shutdown
```

N9K2

```
interface port-channel2
  description VPC 2
```

```
interface Ethernet1/3
```

```
  description Downlink to HOST
  channel-group 8 mode active
  no shutdown
```

```
interface port-channel2
  description VPC 2
  switchport
  switchport mode trunk
  vpc 2
  no shutdown
```

Host

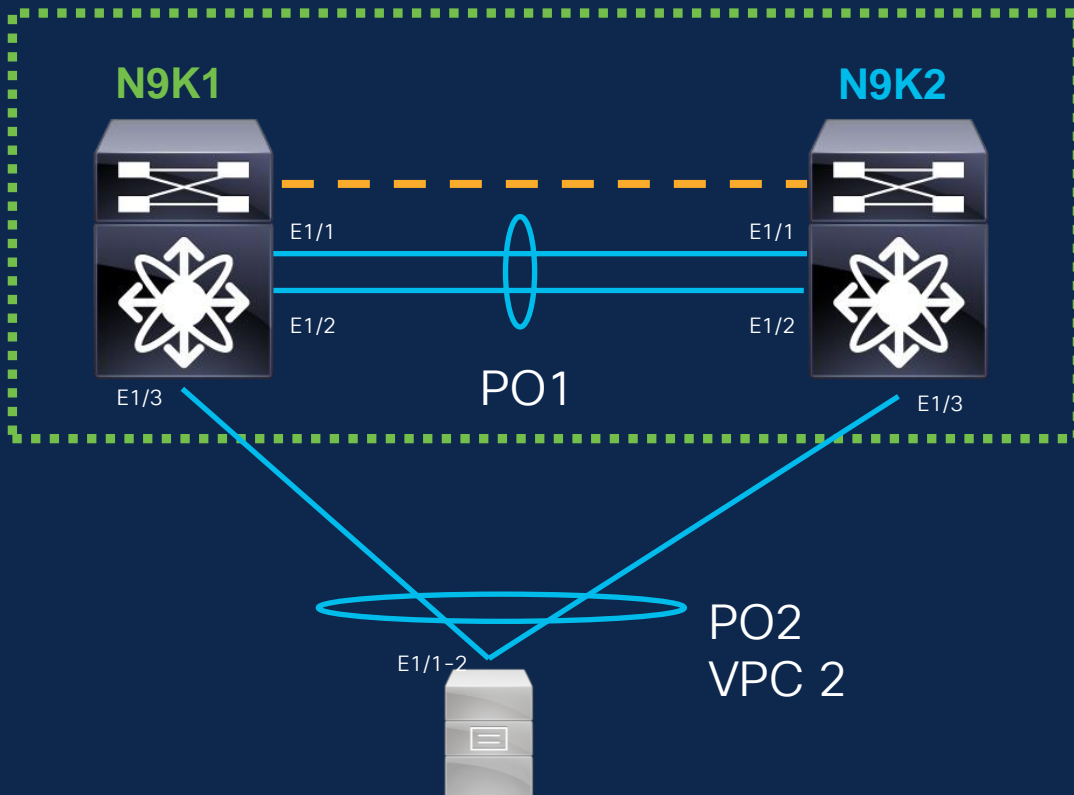
```
interface port-channel2
  description vpc connection
```

```
interface Ethernet1/1-2
```

```
  description uplink to vpc
  channel-group 3 mode active
  no shutdown
```

```
interface port-channel3
  description vpc connection
  switchport
  switchport mode trunk
  no shutdown
```

Configuración de vPC



Verificación

N9K1

```
show vpc
Legend:
```

```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 1
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : primary
Number of vPCs configured : 1
```

<Snipped>

vPC Peer-link status

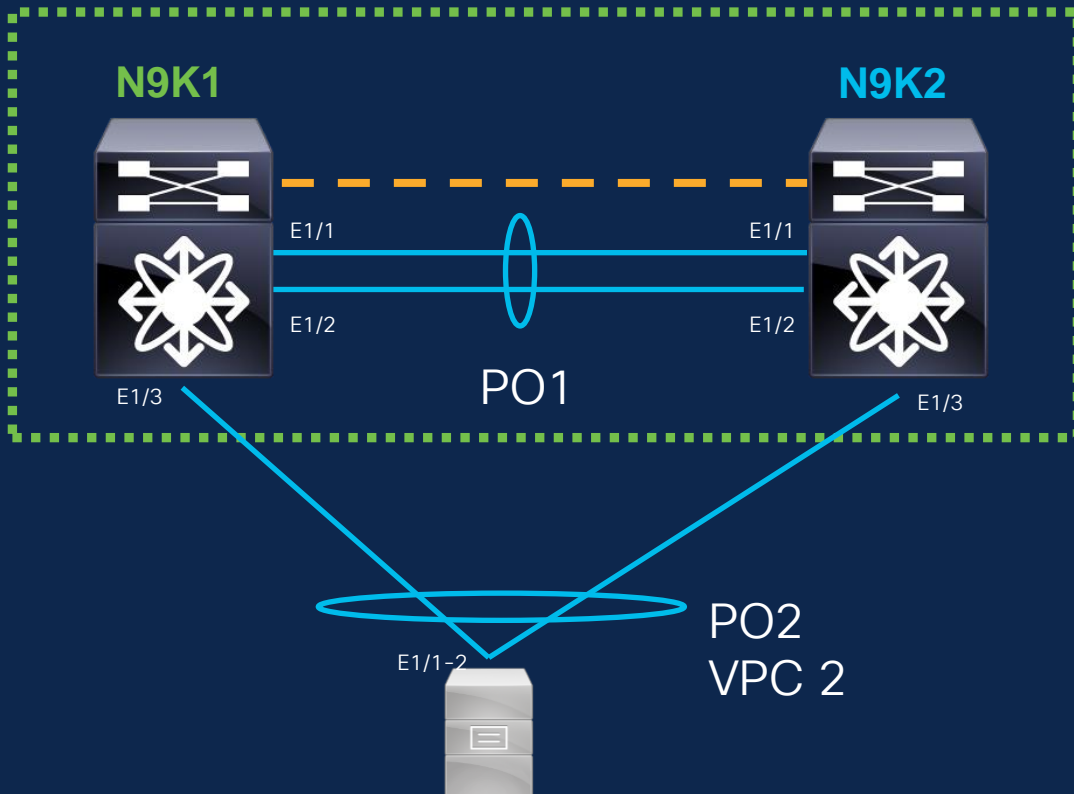
id	Port	Status	Active vlans
1	Po1	up	1-2,100-105,999

vPC status

Id	Port	Status	Consistency	Reason	Active vlans
2	Po2	up	success	success	2,100,105

Please check "show vpc consistency-parameters vpc <vpc-num>" for the consistency reason of down vpc and for type-2 consistency reasons for any vpc.

Configuración de vPC



Verificación

N9K2

```
show vpc
Legend:
```

```
(*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id           : 1
Peer status              : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : secondary
Number of vPCs configured : 1
```

```
<Snipped>
```

```
vPC Peer-link status
```

id	Port	Status	Active vlans
1	Po1	up	1-2,100-105,999

```
vPC status
```

Id	Port	Status	Consistency	Reason	Active vlans
2	Po2	up	success	success	2,100,105

Please check "show vpc consistency-parameters vpc <vpc-num>" for the consistency reason of down vpc and for type-2 consistency reasons for any vpc.

Pasos de troubleshooting

```
sh vpc
```

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

```
vPC domain id          : 1
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : failed
Type-2 inconsistency reason : SVI type-2 configuration incompatible
vPC role               : primary
Number of vPCs configured : 1
Peer Gateway           : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Enabled, timer is off.(timeout = 240s)
Delay-restore status   : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Enabled
Virtual-peerlink mode  : Disabled
```

vPC Peer-link status

```
-----
id   Port   Status Active vlans
--   --
1    Po3    up     1-2,100-105,999
-----
```

vPC status

```
-----
Id   Port           Status Consistency Reason           Active vlans
--   --
8    Po8            up     success    success           2,100,105
-----
```

VPC

```
sh vpc consistency-parameters global
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name	Type	Local Value	Peer Value
STP MST Simulate PVST	1	Enabled	Enabled
STP Port Type, Edge	1	Normal, Disabled,	Normal, Disabled,
BPDUFilter, Edge BPDUGuard		Enabled	Enabled
STP MST Region Name	1	CZ	CZ
STP Disabled	1	None	None
STP Mode	1	MST	MST
STP Bridge Assurance	1	Enabled	Enabled
STP Loopguard	1	Disabled	Disabled
STP MST Region Instance to VLAN Mapping	1		
STP MST Region Revision	1	1	1
Interface-vlan admin up	2	100-103, 105	100-103
Interface-vlan routing capability	2	1,100-103,105	1,100-103
VTP password	2		
VTP pruning status	2	Disabled	Disabled
VTP version	2	1	1
VTP mode	2	Transparent	Transparent
VTP domain	2		
Xconnect Vlans	1		
QoS (Cos)	2	([0-7], [], [], [], [], [])	([0-7], [], [], [], [], [])
Network QoS (MTU)	2	(1500, 1500, 1500, 1500, 1500, 1500)	(1500, 1500, 1500, 1500, 1500, 1500)
Network Qos (Pause: T->Enabled, F->Disabled)	2	(F, F, F, F, F, F)	(F, F, F, F, F, F)
Input Queuing (Bandwidth)	2	(0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)
Input Queuing (Absolute Priority: T->Enabled, F->Disabled)	2	(F, F, F, F, F, F)	(F, F, F, F, F, F)
Output Queuing (Bandwidth Remaining)	2	(0, 0, 0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)
Output Queuing (Absolute Priority: T->Enabled, F->Disabled)	2	(T, F, F, F, F, F)	(T, F, F, F, F, F)
Allowed VLANs	-	1-2,100-105,999	1-2,100-105,999
Local suspended VLANs	-	-	-

VPC

```

sh vpc
Legend:
      (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 1
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : failed
Type-2 inconsistency reason : SVI type-2 configuration incompatible
vPC role               : primary
Number of vPCs configured : 1
Peer Gateway           : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Enabled, timer is off.(timeout = 240s)
Delay-restore status   : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Enabled
Virtual-peerlink mode  : Disabled

```

```

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po3    up     1-2,100-105,999

```

```

vPC status
-----
Id   Port           Status Consistency Reason           Active vlans
--   -
1    Po1             up     failed      vPC type-1
                                     configuration
                                     incompatible - STP
                                     interface port type
                                     inconsistent
                                     2,100,105

```

VPC



```
sh vpc consistency-parameters interface port-channel 8
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name	Type	Local Value	Peer Value
-----	----	-----	-----
delayed-lacp	1	disabled	disabled
	1	-	
mode	1	active	active
Switchport Isolated	1	0	0
Interface type	1	port-channel	port-channel
LACP Mode	1	on	on
Virtual-ethernet-bridge	1	Disabled	Disabled
Speed	1	10 Gb/s	10 Gb/s
Duplex	1	full	full
MTU	1	9216	9216
Port Mode	1	trunk	trunk
Native Vlan	1	2	2
Admin port mode	1	trunk	trunk
STP Port Guard	1	Default	Default
STP Port Type	1	Normal Port	Edge Trunk Port
STP MST Simulate PVST	1	Default	Default
lag-id	1	[(7d0, 0-23-4-ee-be-64, 8008, 0, 0), (8000, 78-c-f0-ba-78-77, 7, 0, 0)]	[(7d0, 0-23-4-ee-be-64, 8008, 0, 0), (8000, 78-c-f0-ba-78-77, 7, 0, 0)]
Allow-Multi-Tag	1	Disabled	Disabled
Vlan xlt mapping	1	Disabled	Disabled
vPC card type	1	N9K EOR LC	N9K EOR LC
Allowed VLANs	-	2,100,105	2,100,105
Local suspended VLANs	-	-	-
Spine-01-084385(config-if)#			

VPC


```
sh hsrp interface vlan 101 | i i virtual
```

```
Virtual IP address is 10.100.1.1 (Cfgd)  
Virtual mac address is 0000.0c9f.f001 (Default MAC)
```

```
Sh mac ad address 0000.0c9f.f001
```

Legend:

* - primary entry, **G - Gateway MAC**, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen, + - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
G 101	0000.0c9f.f001	static	-	F	F	sup-eth1 (R)

```
attach module 1
```

```
Attaching to module 1 ...  
To exit type 'exit', to abort type '$.'
```

```
module-1# sh hardware internal tah rmac  
Instance : 0
```

```
=====
```

Mac-Address	Vlan	Flag
a8:0c:0d:96:43:7f	0	SYSTEM
a8:0c:0d:96:c9:bf	100	VPC PEER
00:00:0c:9f:f0:01	101	VRMAC
3c:8b:7f:92:a6:3f	4415	IFMAC

```
Instance : 1
```

```
=====
```

Mac-Address	Vlan	Flag
a8:0c:0d:96:43:7f	0	SYSTEM
a8:0c:0d:96:c9:bf	100	VPC PEER
00:00:0c:9f:f0:01	101	VRMAC
3c:8b:7f:92:a6:3f	4415	IFMAC

Peer-gateway

```
Spine-01-084385# show system internal vpcm info interface po8
```

```
port-channel8 - if_index: 0x16000007  
-----
```

```
Interface configured as vPC
```

```
IF Elem Information:
```

```
if_index: 0x16000007  
is_mcec: TRUE  
mcec_num : 8  
Number of allowed vlans(cfg_vlans): 3, Bitset: 2,100,105
```

```
MCECM DB Information:
```

```
if_index: 0x16000007  
vPC number: 8  
vPC state: Up   Old Compat Status: Pass  
Compat Status: Pass  
Reason Code: SUCCESS
```

```
<snip>
```

```
vPC Peer Information:
```

```
Peer number: 8  
Peer state: Up  
Number of configured VLANs on peer: 3, Bitset: 2,100,105  
Number of Up VLANs on peer: 3, Bitset: 2,100,105  
Card type: N9K EOR LC
```

```
PSS Information:
```

```
if_index: 0x16000007  
vPC number: 8  
vPC state: Up   Old Compat Status: Pass  
Compat Status: Pass  
Number of Up VLANs: 3, Bitset: 2,100,105  
Number of Suspended VLANs: 0, Bitset:  
Card type: N9K EOR LC
```

VPC Loop Avoidance

<continuación>

vPC Peer Information:

```
Peer number: 8
Peer state: Up
Number of configured VLANs on peer: 3, Bitset: 2,100,105
Number of Up VLANs on peer: 3, Bitset: 2,100,105
Card type: N9K EOR LC
```

Shared Database Information:

```
if_index: 0x16000007
vPC number: 8
Local state: Up Remote state: Up      Number of Up Vlans: 3, Bitset: 2,100,105
Bitset of Peer VLANs: 2,100,105
Reference Count: 0
vPC MAC: 00:26:f0:08:00:00

Peer card type: 4
```

VPC Loop Avoidance

```
Spine-01-084385# show system internal eltm info interface po8
```

```
ELTM Detailed info for Interface port-channel8
cr_flags = INTF LIF , LIF = 4502 (0x1196), LTL = 6 (0x6) (S 0x0, P 0x0)
IF_INDEX = 369098759 (0x16000007), SHARED 0x0
SEC_LTL info:
    sec_ltl = 0 (0x0), A/D progress = FALSE
    sec_ltl_cnt = 0, trig_ifidx = NULL
State = UP_FRR_NTFN_SENT = FALSE
Layer = L2, Mode = TRUNK tag_native_vlan = 0 admin_port_mode = 0x100000
Operational VLAN's (3):
    2,100,105
Voice vlan 4096
Members: Eth1/4
Configured Members: Eth1/4
SDB Members: Eth1/4
egress_vsl_drop = 1 << si el PO estuviera abajo en el vPC Peer este valor sería 0
global id (only for fabric pc) = 0
Interface Features:
    ipv4_en = 0, ipv4_mcast_en = 0, df_mask = 0, mpls_en = 0
    v4_table_id = 0 (0x0), ipsg_en = 0
    per_pkt_ls_en = 0, icmp_redirect = 1, v4_same_if_check = 0
    ipv6_redirect = 1 ipv6_en = 0, ipv6_mcast_en = 0
    v6_table_id = 0 (0x0), v6_same_if_check = 0
    mtu = 1500 (0x5dc), f_index = 0 (0x0), span_mode: 0 dot1x_ma_en: 0
    bd = 2 (0x2), buffer_boost=0, openflow_en=0 span_buffer_cfg: 0, outer_bd=512 sw_mac_learn=0
```

VPC Loop Avoidance

Clausura





¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 25 de agosto de 2023

<https://bit.ly/CLdoc-aug23>



Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.



Nuestras Redes Sociales

LinkedIn

[Cisco Community](#)

Twitter

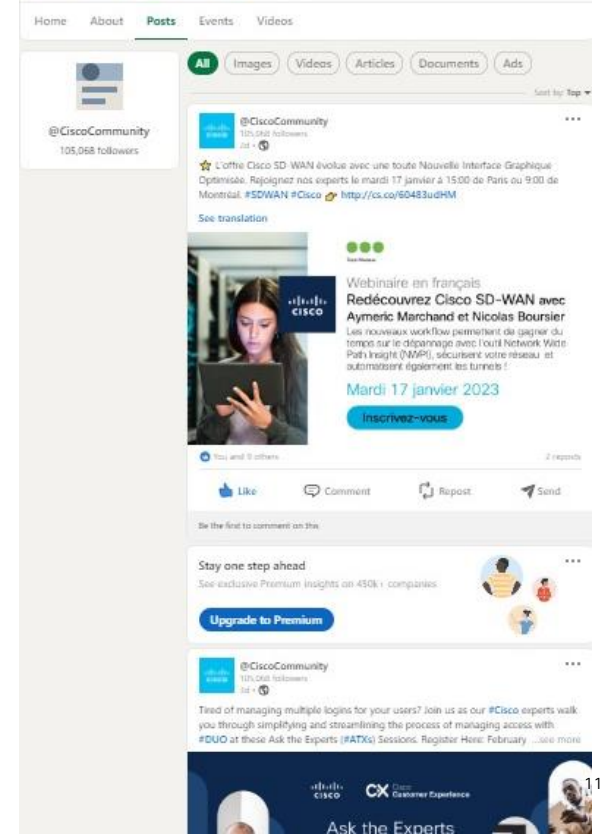
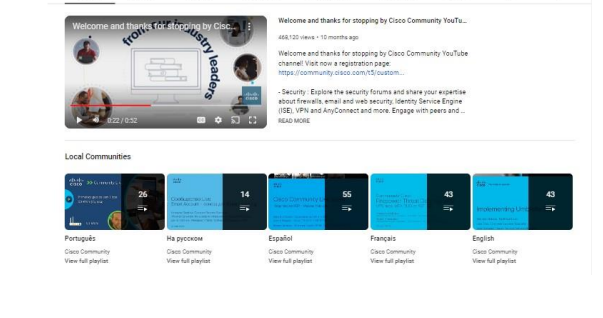
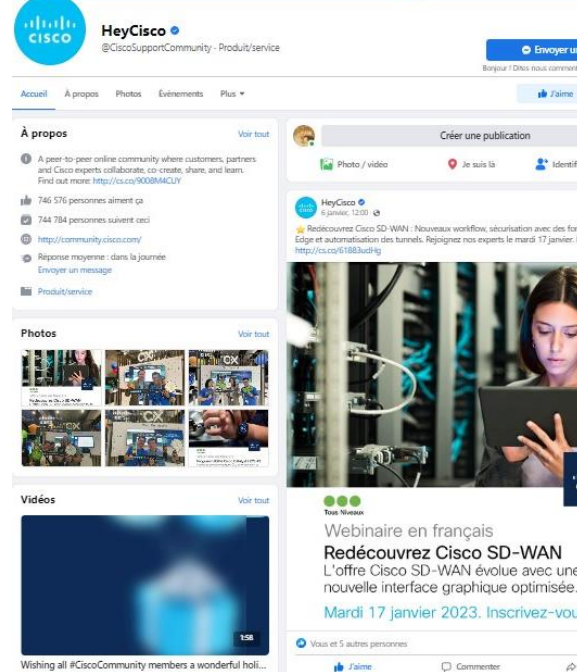
[@CiscoCommunity](#)

YouTube

[CiscoCommunity](#)

Facebook

[CiscoCommunity](#)





The bridge to possible