

Conozca el proceso de elección de vPC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Tecnología PortChannel virtual](#)

[Función vPC](#)

[Prioridad de función de vPC](#)

[Cambio de función de vPC sin impacto](#)

[Comportamiento de los sistemas vPC cuando falla un enlace de par vPC](#)

[Bit persistente principal vPC](#)

[Restauración de vPC Delay](#)

[Vlan de interfaz de vPC Delay Restore](#)

[vPC Delay Restore mientras se utiliza la configuración de SVI escalada de 4000 SVI](#)

[Proceso de elección de vPC](#)

[Escenario de recuperación vPC](#)

[Ejemplo de interrupción de la red relevante para el bit persistente establecido incorrectamente](#)

Introducción

En este documento se describe el proceso de elección de rol de Virtual PortChannel (vPC) en los switches de la serie Nexus.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- vPC en switches de la serie Nexus
- Spanning Tree Protocol (STP)

Componentes Utilizados

La información de este documento se basa en la plataforma de switches Nexus serie 9000.

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.

Tecnología PortChannel virtual

Los PortChannel virtuales (vPC) permiten que los enlaces que están conectados físicamente a dos switches Cisco diferentes aparezcan como un único PortChannel para un tercer dispositivo. El tercer dispositivo puede ser un switch, un servidor o cualquier otro dispositivo de red que admita PortChannels IEEE 802.3ad. vPC también permite la creación de PortChannels de capa 2 que abarcan dos switches. En este momento, vPC se implementa en las plataformas Nexus de Cisco series 9000, 7000, 5000 y 3000 (con o sin Fabric Extenders Nexus de Cisco serie 2000).

 Nota: Las vPC del software Cisco NX-OS y los sistemas de switching virtual Cisco Catalyst Virtual Switching Systems (VSS) son de tecnologías similares. Para la tecnología Cisco EtherChannel, el término Multi-chassis EtherChannel (MCEC) se refiere indistintamente a cualquiera de las dos tecnologías.

Función vPC

Aunque ambos switches vPC aparecen como un único switch para un dispositivo de flujo descendente, entre ellos, dos switches vPC tienen roles vPC claramente definidos: vPC principal y vPC secundario.

Los roles de vPC no son preventivos, lo que significa que un dispositivo se puede configurar como vPC principal, pero funciona como dispositivo de par secundario vPC. Esto puede suceder en este escenario:

1. Cuando falla el dispositivo principal original, el dispositivo vPC secundario se convierte en el nuevo dispositivo principal.
2. Cuando el sistema se recupera, el dispositivo principal anterior es ahora el dispositivo secundario y viceversa.

El rol vPC define cuál de los dos dispositivos de par vPC procesa las unidades de datos del protocolo de puente (BPDU) y responde a las solicitudes del protocolo de resolución de direcciones (ARP). El rol vPC también define un conjunto de acciones que deben realizar vPC principal y vPC secundario en respuesta a una situación de desconexión del enlace de par vPC.

Prioridad de función de vPC

También puede utilizar el comando `role priority` en el modo de dominio vPC para influir en el proceso de elección de vPC. El rango de valores va de 1 a 65636 y el valor predeterminado es 32667. Un valor inferior significa que este switch tiene más posibilidades de ser el vPC principal.

Cuando cambia la prioridad de los dispositivos de par vPC, puede hacer que las interfaces de la red suban y bajen. Si desea volver a configurar la prioridad de rol para convertir un dispositivo vPC en el dispositivo principal, configure la prioridad de rol tanto en el dispositivo vPC principal con un valor de prioridad inferior como en el dispositivo vPC secundario con el valor superior. A

continuación, apague el enlace de par vPC en ambos dispositivos e ingrese el comando shutdown y, finalmente, vuelva a habilitar el canal de puerto en ambos dispositivos e ingrese el comando no shutdown.

Cambio de función de vPC sin impacto

La función de cambio de roles sin impacto de vPC proporciona un marco para cambiar los roles de vPC entre pares de vPC sin que ello afecte a los flujos de tráfico. El intercambio de funciones de vPC se realiza en función del valor de prioridad de funciones del dispositivo en el dominio vPC. Un dispositivo par vPC con menor prioridad de rol se selecciona como el dispositivo vPC principal cuando se ejecuta el comando `vpc role preempt`.

Consulte [Escenario de caso práctico de cambio de función de vPC sin impacto](#) para obtener más detalles.

Comportamiento de los sistemas vPC cuando falla un enlace de par vPC

Cuando el enlace de par vPC falla y el enlace de par keepalive vPC sigue activo, el dispositivo de par secundario vPC realiza estas operaciones:

1. Suspende sus puertos miembro de vPC.
2. Apaga la SVI asociada a la VLAN vPC.

Este comportamiento de protección de vPC redirige todo el tráfico de sur a norte al dispositivo principal vPC.



Nota: cuando el enlace de par vPC está inactivo, ambos dispositivos de par vPC ya no pueden sincronizarse entre sí, por lo que el mecanismo de protección diseñado lleva al aislamiento de uno de los dispositivos de par (en este caso, el dispositivo de par secundario) de la ruta de datos.

Bit persistente principal vPC

vPC Primary Sticky bit es un mecanismo de protección programado introducido para evitar cambios de funciones innecesarios (que podrían causar interrupciones en la red) cuando el switch principal se recarga inesperadamente. vPC Primary Sticky Bit permite que el switch activo se adhiera a su función PRINCIPAL cuando un switch inactivo vuelve a estar activo o cuando un switch aislado se integra de nuevo en el dominio VPC.

Conmutación del bit persistente principal de vPC:

1. El valor de bit persistente principal de vPC se establece en TRUE en este escenario:

- El vPC principal actual se reinicia y el switch habilitado para vPC cambia su función de vPC secundario a vPC operacional principal. El bit fijo no se establece si la función cambia de vPC Operational Secondary (Secundario operativo de vPC) a vPC Primary (Principal de vPC).
- Un switch habilitado para vPC cambia su función de Ninguno establecido a Principal de vPC cuando caduca el temporizador de restauración de recarga (240 s de forma predeterminada).

2. El valor de bit persistente principal de vPC se establece en FALSE en los siguientes escenarios:

- Se reinicia un switch habilitado para vPC (el bit persistente se establece en FALSE de forma predeterminada).
- La prioridad de rol de vPC se cambia o se vuelve a introducir.

El bit principal persistente de vPC se informa en la estructura de componentes del software vPC Manager y se puede comprobar con este comando de modo NX-OS exec.

```
Campus_N7K2-VPC# show system internal vpcm info global | include ignore-case sticky
      Sticky Primary: TRUE
Campus_N7K2-VPC#
```

Restauración de vPC Delay

Después de que un dispositivo par vPC se recargue y vuelva a estar activo, el protocolo de routing necesita tiempo para volver a converger. El tramo de recuperación de vPC puede bloquear el tráfico enrutado desde el acceso a la agregación/núcleo hasta que se restablezca la conectividad de enlace ascendente de capa 3.

La función vPC Delay Restore retrasa la activación de los tramos de vPC en el dispositivo par vPC que se recupera. vPC Delay Restore permite que los protocolos de routing de capa 3 converjan antes de permitir el tráfico en los tramos de vPC. Esto se traduce en una restauración más fluida y cero pérdidas de paquetes durante la fase de recuperación (el tráfico se sigue desviando en el dispositivo de par vPC activo). Esta función está activada de forma predeterminada con un temporizador predeterminado de restauración vPC de 30 segundos. El temporizador se puede ajustar a una línea de base de convergencia de Capa 3 específica de 1 a 3600 segundos.

Vlan de interfaz de vPC Delay Restore

Para retrasar la aparición de las interfaces VLAN en el dispositivo par vPC restaurado, utilice la opción interfaces-vlan del comando delay restore. Esta función está activada de forma predeterminada con un temporizador predeterminado de restauración vPC de 10 segundos.

vPC Delay Restore mientras se utiliza la configuración de SVI escalada de 4000 SVI

Se introduce un nuevo comando `delay restore interface-VLAN batch <1-4094>` para configurar el marcador para activar las interfaces VLAN o de dominio de puente en un lote de 200 SVI a la vez. El comando de temporizador de restauración de retraso `vPC delay restore <valor de tiempo de espera>` se puede configurar en un valor mayor que la suma de todos los temporizadores por lotes configurados. Esto se hace para que el tramo VPC se active solo después de que todas las SVI se hayan activado por completo para evitar cualquier agujero negro de tráfico.

Ejemplo: 4000 VLAN, 200 lotes, 15 segundos de retraso

```
delay restore > (4000/200)x 15
```

Proceso de elección de vPC

En un sistema vPC, un dispositivo vPC por dispositivo se define como vPC principal y otro como vPC secundario, en función de estos parámetros y en este orden

1. vPC Primary sticky-bit establecido en 0 o 1.
2. Prioridad de rol de vPC definida por el usuario (el software Cisco NX-OS utiliza el valor numérico más bajo para seleccionar el dispositivo principal).
3. Valor de dirección MAC del sistema (el software Cisco NX-OS utiliza la dirección MAC más baja para seleccionar el dispositivo principal).

Este diagrama de flujo (Imagen 1) resume los pasos que ambos dispositivos de par vPC siguen durante el proceso de elección del switch principal vPC.

1. El primer parámetro comprobado entre dos dispositivos durante el proceso de elección principal de vPC es vPC Primary Sticky Bit. Si el dispositivo par vPC gana esta comparación, se convierte en vPC principal independientemente del valor de prioridad de rol vPC configurado o de las direcciones MAC del sistema que tengan ambos pares.
2. Si ambos switches de par vPC tienen el mismo valor de bit fijo, el proceso de elección continúa con el siguiente paso para comparar la prioridad de rol de vPC definida por el usuario.
3. Si ambas funciones de vPC están configuradas con el mismo valor, el proceso de elección continúa para comparar las direcciones MAC del sistema.

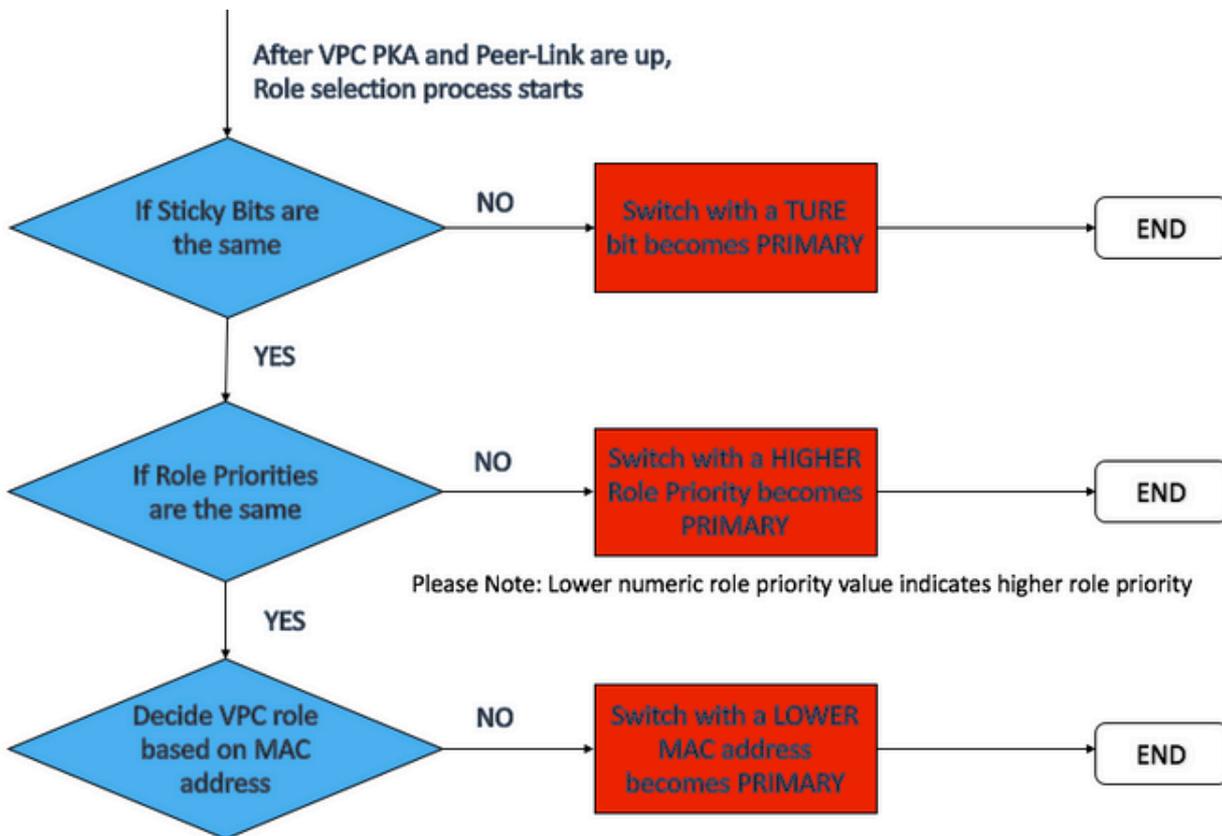


Imagen 1

Como se muestra en la imagen, cuando el switch vPC tiene el bit persistente principal de vPC establecido en 1 (condición TRUE) y su par con el bit persistente establecido en 0 (condición FALSE), el lado TRUE gana la elección y asume la función de vPC principal.

Bit fijo de par 1 de vPC establecido en 1	Bit fijo de par 2 de vPC establecido en 1	vPC principal
Falso (0)	Falso (0)	Corbata
Verdadero (1)	Falso (0)	Par 1 de vPC
Falso (0)	Verdadero (1)	Par 2 de vPC
Verdadero (1)	Verdadero (1)	Corbata

Escenario de recuperación vPC

Es importante comprender el proceso de elección de vPC y no se puede subestimar, especialmente en escenarios de recuperación de vPC.

La imagen 2 muestra una configuración de VPC típica, Nexus-01 es el VPC principal y Nexus-02 es el VPC secundario. Ambos tienen sus Bits pegajosos reconfigurados a FALSO de forma predeterminada.

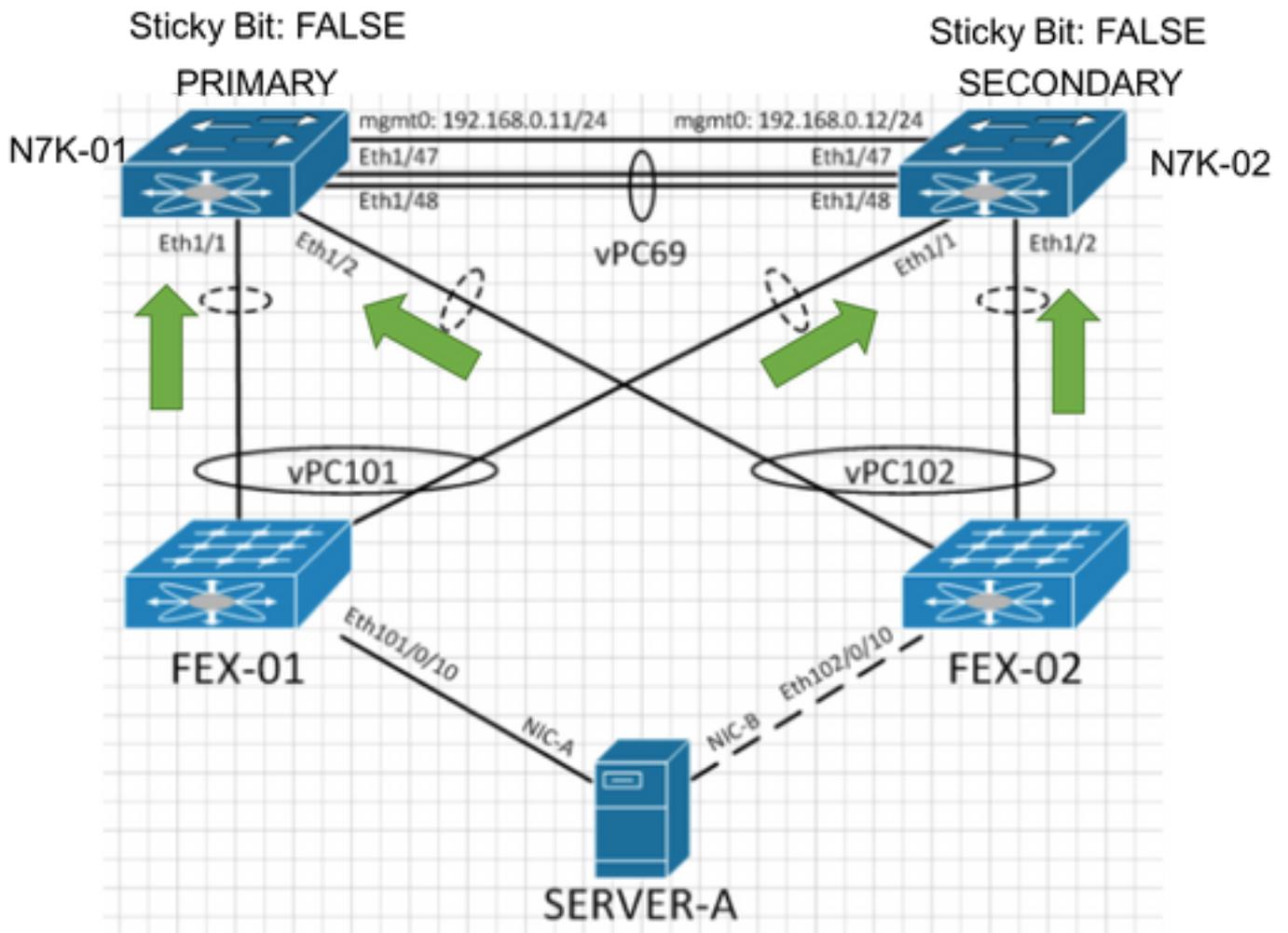


Imagen 2

Como se muestra en esta imagen, el Nexus-01 tiene ahora un corte de energía y se ha aislado de la red. Nexus-02 se promocionó a vPC principal y estableció vPC Sticky Bit en TRUE.

Y ahora el Nexus-02 se convierte en Operational Primary (Primario operativo) y el bit fijo se establece en TRUE.

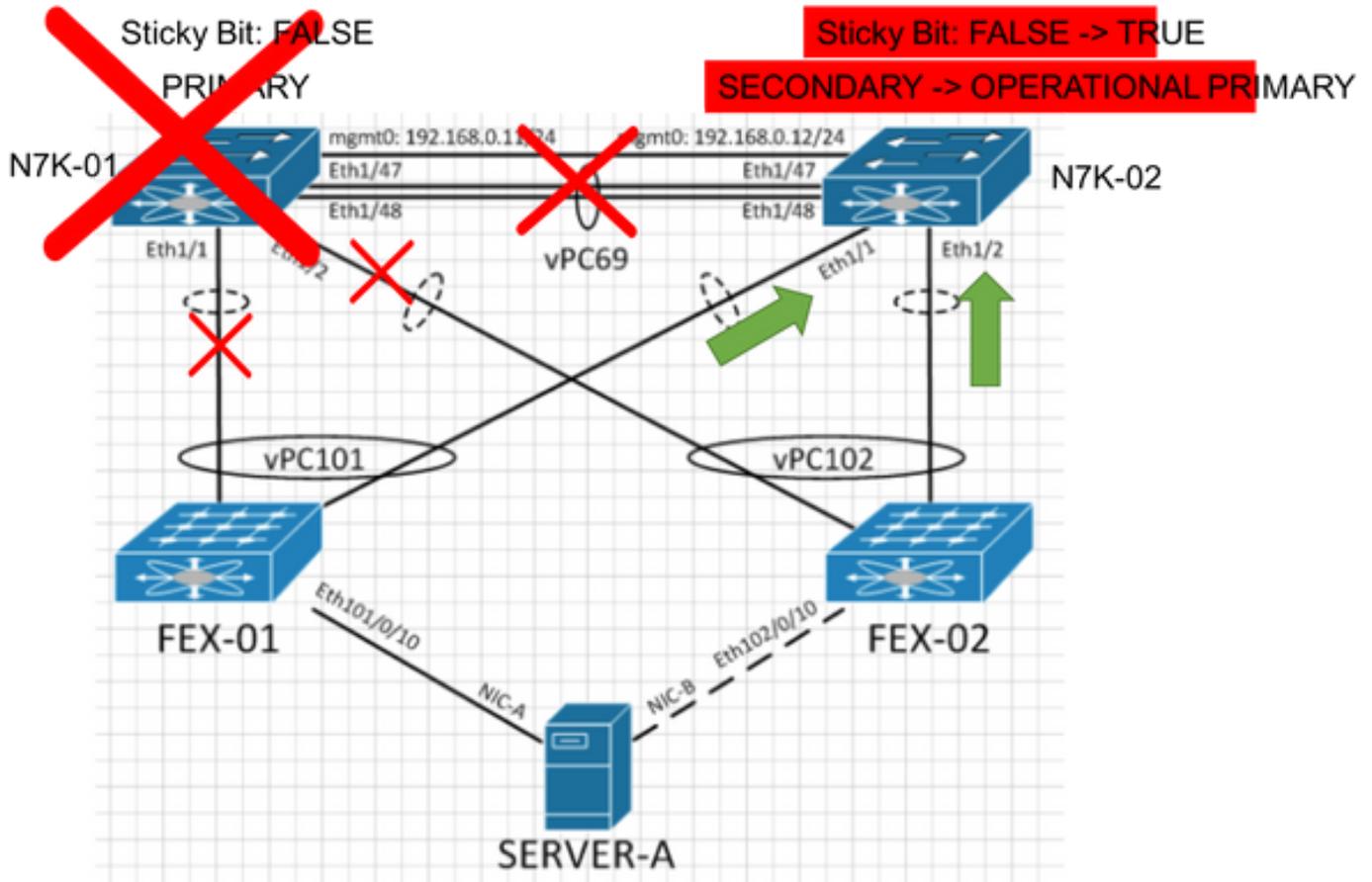


Imagen 3

Como se muestra en esta imagen, cuando el Nexus-01 vuelve a estar online después de que se haya restablecido el corte de electricidad, el Nexus-02 conserva la función PRIMARIO operativo independientemente de su prioridad de función (porque tiene un bit realmente pegajoso) y el Nexus-01 desempeña la función SECUNDARIO cuando se conecta. Sólo Nexus-01 inicia el proceso de inicialización de VPC, mientras que Nexus-02 permanece como PRIMARIO y reenvía el tráfico de la forma habitual. Por lo tanto, no se observa ninguna interrupción en la red.

Hay dos temporizadores asociados con el proceso de inicialización de vPC en Nexus-01, que ahora es el dispositivo secundario operativo de vPC:

- delay restore SVI (10 segundos de forma predeterminada)
- delay restore (30 segundos de forma predeterminada)

Como resultado, puede esperar un tiempo de recuperación de 40 segundos en Nexus-01 después de que Nexus-01 se vuelva a introducir en la red como dispositivo secundario vPC. Sin embargo, dado que Nexus-02 desempeña la función principal, todo el tráfico pasa ahora a través de Nexus-01, como se ha mencionado anteriormente, no se observa ninguna interrupción en la red.

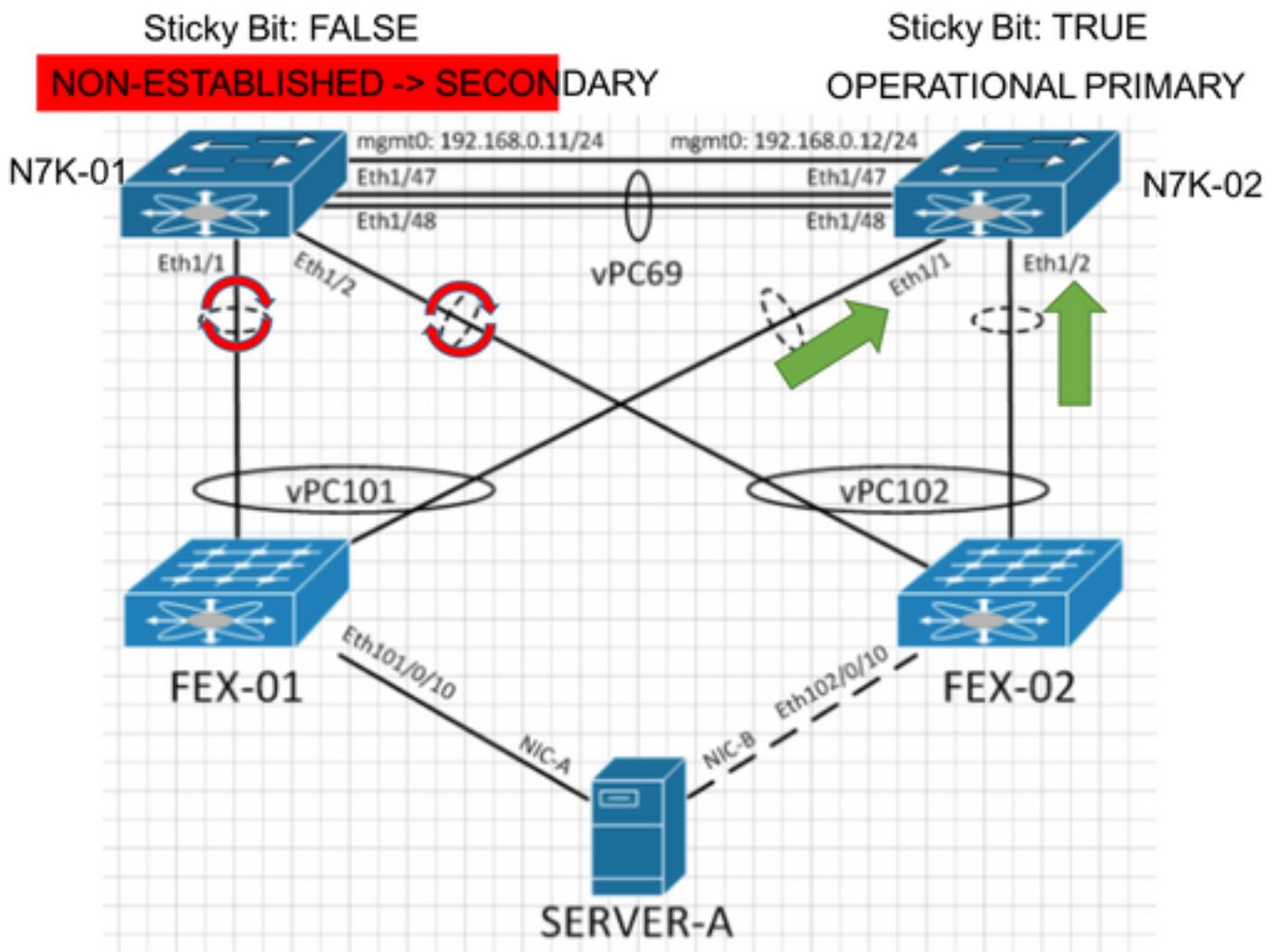


Imagen 4

Ejemplo de interrupción de la red relevante para el bit persistente establecido incorrectamente

La interrupción de la red se debe a un bit persistente configurado INCORRECTAMENTE cuando se introduce de nuevo un switch aislado (Nexus-02) en el dominio VPC

Sin embargo, se puede producir una interrupción de la red después de que un switch aislado se introduzca de nuevo en el dominio VPC si los bits persistentes no se configuran correctamente en ambos switches Nexus. Antes de que un switch aislado se introduzca de nuevo en el dominio VPC, su bit persistente debe establecerse en FALSE. (Para obtener información sobre los procedimientos para sustituir un chasis N7K, consulte [Procedimiento de sustitución del chasis Nexus 7000](#).)

Como se muestra en la imagen 5, el Nexus-01 está configurado con una prioridad de rol de VPC mayor que el Nexus-02, y el Nexus-02 tiene el bit persistente establecido en TRUE. Los enlaces E1/1 y E1/2 de Nexus-01 se encuentran en estado de reenvío, mientras que E1/1 y E1/2 se encuentran en estado de apagado.

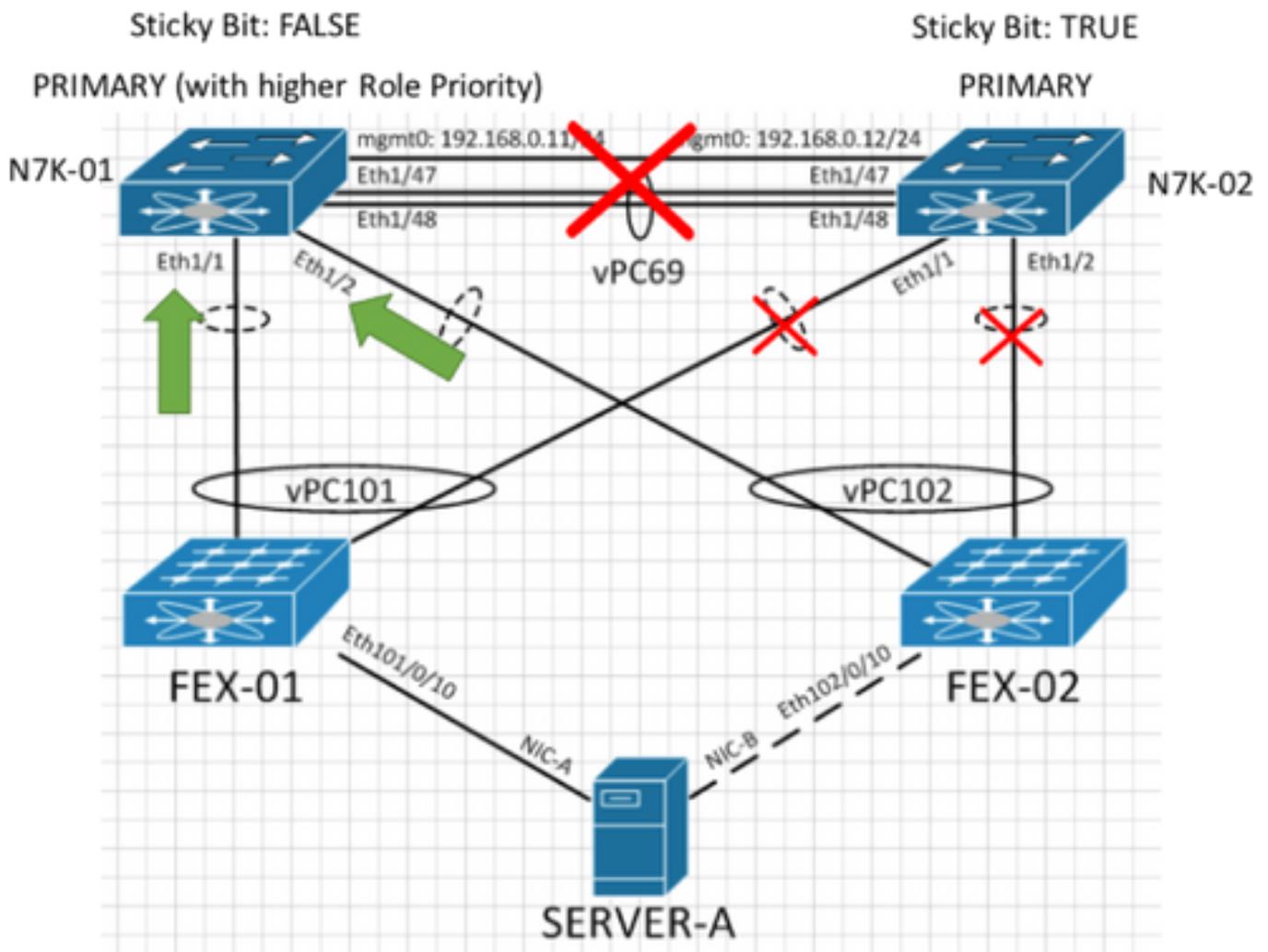


Imagen 5

Cuando se restauran el PKA y el enlace de par, Nexus-02 desempeña la función PRINCIPAL independientemente de su prioridad de función (porque tiene un bit persistente TRUE) y obliga al Nexus-01 a convertirse en SECUNDARIO y el proceso de inicialización de VPC comienza en el Nexus-01. Por lo tanto, VPC suspende el enlace E1/1 y E1/2 del Nexus-01 y se conecta después de que caduquen los temporizadores de restauración de retransmisión (40 segundos de forma predeterminada). En este caso, se observa una interrupción de la red de 40 segundos después de restaurar el PKA y el enlace de par, como se muestra en la imagen 6.

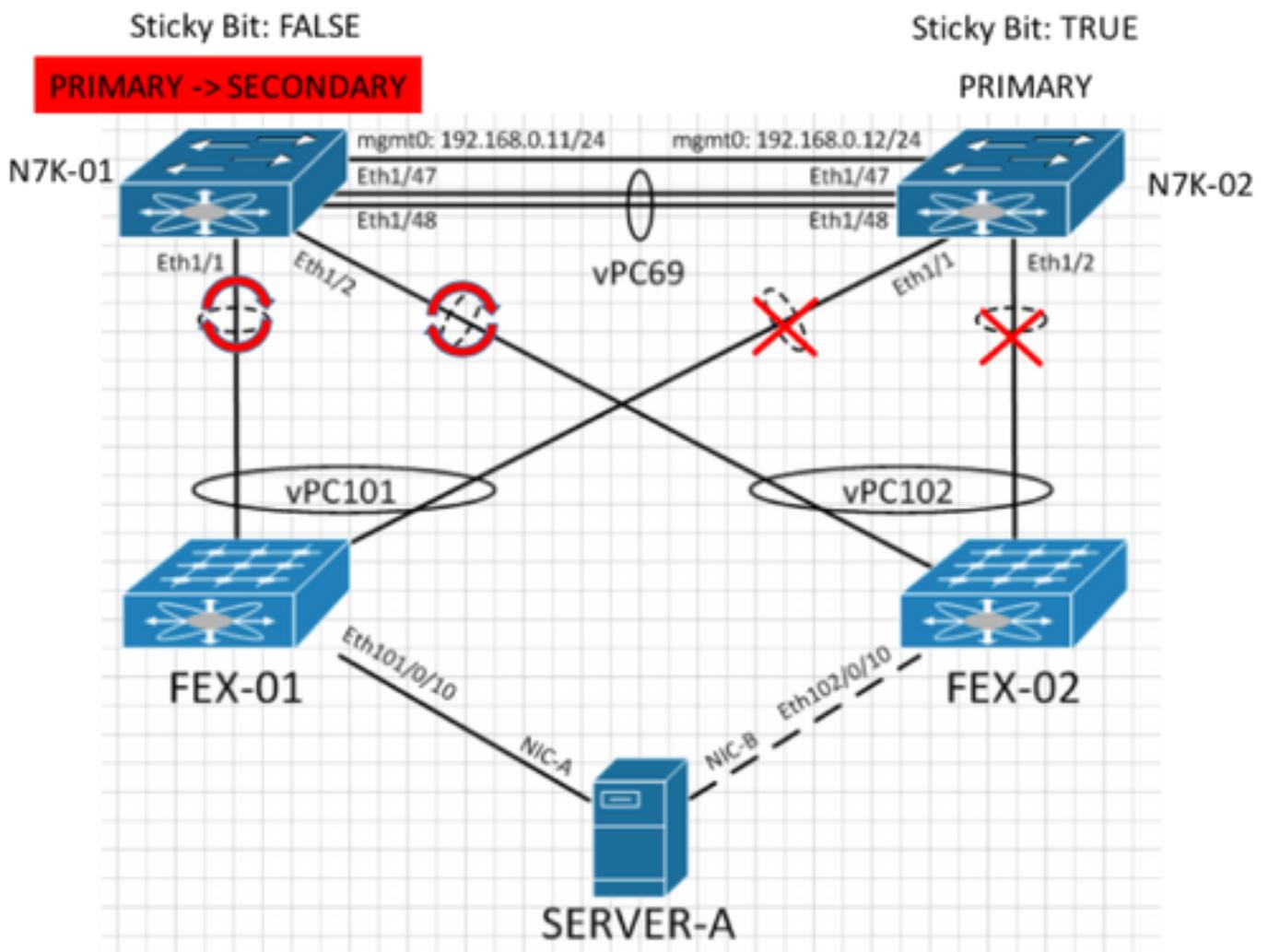


Imagen 6

✎ Nota: cuando se vuelve a introducir un Nexus en el dominio vPC, debe asegurarse de que no haya ningún cambio de función de vPC en el dispositivo vPC activo. Para evitar un cambio de función de vPC cuando los bits persistentes de ambos switches se establecen en el mismo valor, el dispositivo vPC activo debe tener una prioridad de función más alta para poder conservar su función PRINCIPAL. Consulte la Imagen 1 de este documento para obtener más información sobre el proceso de elección de roles de VPC.

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).