Resolución de Problemas de Inestabilidades BGP entre el Núcleo de Paquetes Ultra y el Switch Nexus Debido a una Configuración Incorrecta

Contenido

Introducción

En este documento se describe la solución para las inestabilidad del protocolo de gateway fronterizo (BGP) entre Cisco Ultra Packet Core (UPC) y el switch Nexus 9000 configurado con conexión BGP redundante.

Problema

Las inestabilidad de BGP se activan cuando una de las interfaces redundantes entre Cisco Ultra Packet Core y el switch Nexus se inactiva.

Condiciones

El nodo Ultra Packet Core (UPC) está conectado a Nexus Leaf A y Leaf B en puertos independientes. Se establecen los pares BGP IPv6 y se instalan las rutas predeterminadas en el nodo UPC. La figura 1 muestra el diagrama de red de alto nivel con ruta redundante a los switches de hoja.

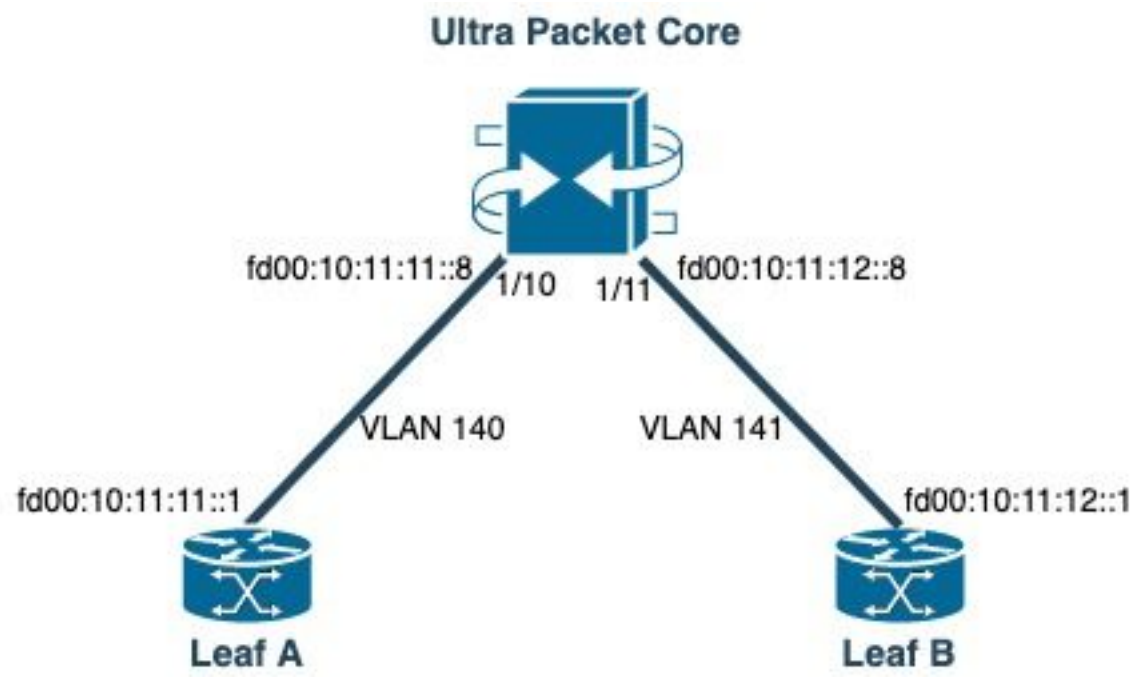

Figura 1: Diagrama de red

Configuración

Configuración de puerto UPC con VLAN y enlace de interfaz:

```
port ethernet 1/10
    no shutdown
    vlan 140
        no shutdown
        bind interface saegw_vlan140_1/10 saegw
#exit

#exit
port ethernet 1/11
    no shutdown
    vlan 141
        no shutdown
        bind interface saegw_vlan141_1/11 saegw
#exit
#exit
end
```

Configuración de la interfaz UPC con direcciones IP:

```
interface saegw_vlan140_1/10
  ip address 10.11.11..8 255.255.255.0
  ipv6 address fd00:10:11:11::8/64 secondary
  bfd interval 300 min_rx 300 multiplier 3
#exit
interface saegw_vlan141_1/11
  ip address 10.11.12.8 255.255.255.0
  ipv6 address fd00:10:11:12::8/64 secondary
  bfd interval 300 min_rx 300 multiplier 3
#exit
```

Configuración UPC BGP:

```
router bgp 25949
  router-id 172.19.20.30
  maximum-paths ebgp 4
  neighbor 10.11.11..1 remote-as 25949
  neighbor 10.11.11..1 fall-over bfd
  neighbor 10.11.12.1 remote-as 25949
  neighbor 10.11.12.1 fall-over bfd
  neighbor fd00:10:11:11::1 remote-as 25949
  neighbor fd00:10:11:12::1 remote-as 25949
  address-family ipv4
    neighbor 10.11.11..1 route-map accept_default in
    neighbor 10.11.11..1 route-map gw-1-OUT out
    neighbor 10.11.12.1 route-map accept_default in
    neighbor 10.11.12.1 route-map gw-1-OUT out
    redistribute connected
#exit
address-family ipv6
  neighbor fd00:10:11:11::1 activate
  neighbor fd00:10:11:11::1 route-map accept_v6_default in
  neighbor fd00:10:11:11::1 route-map allow_service_ips_v6 out
  neighbor fd00:10:11:12::1 activate
  neighbor fd00:10:11:12::1 route-map accept_v6_default in
  neighbor fd00:10:11:12::1 route-map allow_service_ips_v6 out
  redistribute connected
#exit

ipv6 prefix-list name accept_v6_default_routes seq 10 permit ::/0
route-map accept_v6_default permit 10
  match ipv6 address prefix-list accept_v6_default_routes
#exit
```

Configuración del switch Nexus 9000:

```
Interface vlan140
ipv6 address fd00:10:11:11::1/64
no ipv6 redirects

interface vlan141
ipv6 address fd00:10:11:12::1/64
no ipv6 redirects

vrf upc
address-family ipv4 unicast
advertise l2vpn evpn
maximum-paths ibgp 2
address-family ipv6 unicast
advertise l2vpn evpn
maximum-paths ibgp 2
neighbor fd00:10:11:12::5
remote-as 25949
address-family ipv6 unicast
neighbor fd00:10:11:12::6
remote-as 25949
address-family ipv6 unicast
neighbor fd00:10:11:12::8
remote-as 25949
address-family ipv6 unicast
```

Análisis

Inicialmente, se observa una comunicación BGP normal entre una de las interfaces UPC (fd00:10:11:12::8) y el switch Nexus (fd00:10:11:12::1 pertenece a vlan141) que incluye mensajes

TCP ACK:

```
2023-01-01 01:01:59.000000 fd00:10:11:12::8 -> fd00:10:11:12::1 TCP 35813 > bgp [ACK] Seq=250
Ack=8664 Win=31744 Len=0 TSV=2412344062 TSER=531234647
2023-01-01 01:01:59.000087 fd00:10:11:12::8 -> fd00:10:11:12::1 TCP 35813 > bgp [ACK] Seq=250
Ack=11520 Win=37376 Len=0 TSV=2412344062 TSER=531234647
2023-01-01 01:01:59.000162 fd00:10:11:12::8 -> fd00:10:11:12::1 TCP 35813 > bgp [ACK] Seq=250
Ack=14376 Win=43008 Len=0 TSV=241234062 TSER=531234647
2023-01-01 01:01:59.000281 fd00:10:11:12::8 -> fd00:10:11:12::1 TCP 35813 > bgp [ACK] Seq=250
Ack=17232 Win=49152 Len=0 TSV=2412344062 TSER=531234647
2023-01-01 01:01:59.000936 fd00:10:11:12::8 -> fd00:10:11:12::1 TCP 35813 > bgp [ACK] Seq=250
Ack=20663 Win=48640 Len=0 TSV=2412344063 TSER=531234647
```

Si la interfaz Leaf-B falla hacia UPC, se observa un comportamiento incorrecto en los registros donde el UPC inicia un nuevo intento de conexión BGP (fuente: fd00:10:11:12::8) hacia Leaf-A en la interfaz fd00:10:11:11::1, que pertenece a una VLAN diferente, vlan140.

```
2023-01-01 22:36:12.370117 fd00:10:11:12::8 -> fd00:10:11:11::1 TCP 41987 > bgp [SYN] Seq=0
Win=14400 Len=0 MSS=1440 TSV=2412347369 TSER=0 WS=9
```

Este mensaje SYN de BGP no válido enviado en la interfaz incorrecta provoca la caída de BGP. Cuando Nexus anuncia su propia ruta conectada y UPC obtiene una ruta para la interfaz que estaba fuera de servicio a través de BGP, UPC intenta la conexión a través de otra interfaz con una IP saliente diferente/incorrecta.

Solución

Debido a la configuración mencionada en la sección Condición de este artículo, dado que UPC recibe la información de ruta conectada de ambas Hojas de ambas interfaces, cuando una de las interfaces está inactiva, UPC intenta comunicarse con esa Hoja a través de la otra interfaz.

Para evitar que UPC envíe los mensajes de establecimiento de conexión BGP desde la interfaz incorrecta, estos son los cambios de configuración que se deben considerar:

1. En la configuración de UPC, agregue update-source para el vecino. Esta configuración evita que la conexión BGP de una interfaz diferente, si la interfaz principal está inactiva. Por ejemplo, cuando saegw_vlan140_1/10 (fd00:10:11:11::1/64) está inactivo, el nodo no puede utilizar la interfaz de salida saegw_vlan141_1/11 para el par BGP fd00:10:11:11::8.
   A continuación se incluye una configuración de ejemplo:

   ```
   neighbor fd00:10:11:11::1 update-source fd00:10:11:11::8
   neighbor fd00:10:11:12::1 update-source fd00:10:11:12::8
   ```

2. En la configuración de Nexus, bloquee los prefijos de las interfaces incorrectas.
   Por ejemplo, denegamos rutas para la hoja redundante sobre el vecino fd00:10:11:11::1

   ```
   neighbor fd00:10:11:11::1
   update prefix list to deny fd00:10:11:12::8/64
   ```

3. En el switch Nexus, el par EBGP desde VTEP a un nodo externo a través de VXLAN debe estar en un VRF de arrendatario y debe utilizar el update-source de un loopback interfaz (iguales a través de VXLAN), como se recomienda en la Guía de configuración de Cisco Nexus 9000

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).