Probleemoplossing BGP-flaps tussen Ultra Packet Core en Nexus Switch vanwege onjuiste configuratie

Inhoud

[Inleiding](#)
[Probleem](#)
[Voorwaarden](#)
[Configuratie](#)
[Analyse](#)
[Oplossing](#)

Inleiding

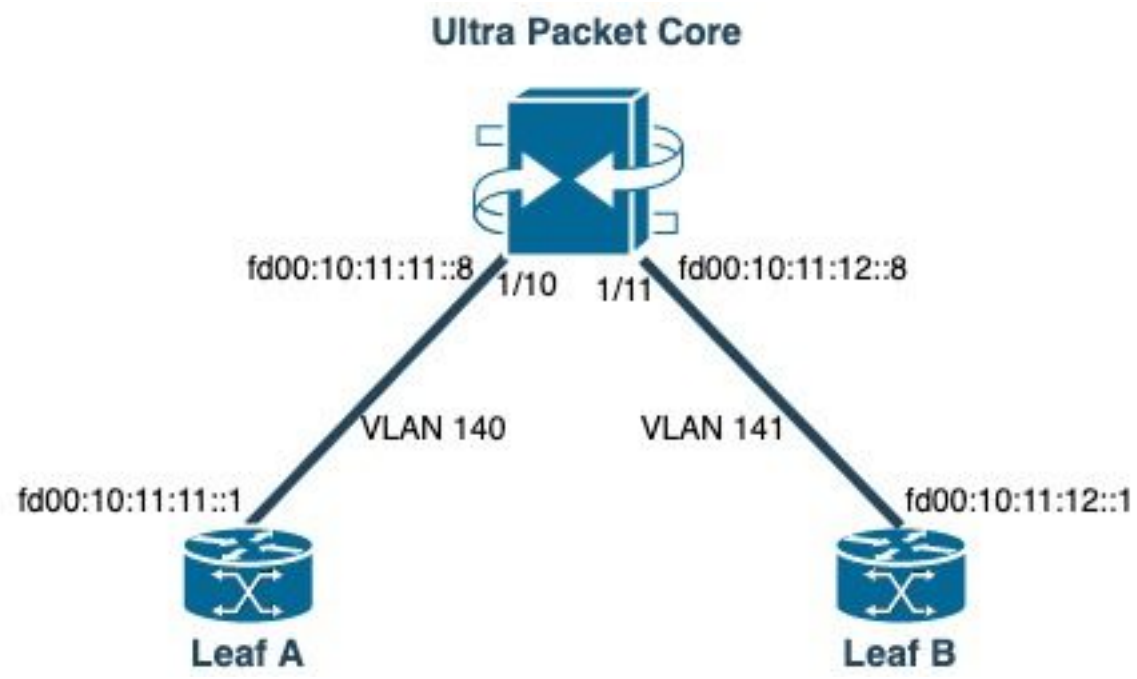
Dit document beschrijft de oplossing voor de BGP-flaps (BGP) tussen Cisco Ultra Packet Core (UPC) en Nexus 9000 switch die zijn geconfigureerd met redundante BGP-verbinding.

Probleem

BGP-flaps worden geactiveerd wanneer een van de redundante interfaces tussen de Cisco Ultra Packet Core en Nexus switch flaps.

Voorwaarden

De Ultra Packet Core (UPC) knooppunt is verbonden met Nexus Leaf A en Leaf B op afzonderlijke poorten. De BGP IPv6-peers worden ingesteld en de standaardroutes worden geïnstalleerd op de UPC-knooppunt. Afbeelding 1 toont het netwerkdiagram op hoog niveau met redundant pad naar Blade switches.



Afbeelding 1: Netwerkdiagram

Configuratie

UPC-poortconfiguratie met VLAN en interfaceband:

```
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
```

UPC-interfaceconfiguratie met IP-adressen:

```
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
```

UPC BGP-configuratie:

```
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
```

Nexus 9000 switch configuratie:

```
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
```

Analyse

Aanvankelijk wordt een normale BGP-communicatie tussen een van de UPC-interfaces (fd00:10:11:12:8) en de Nexus-switch (fd00:10:11:12:1:1 behoort tot vlan141) waargenomen, die

TCP ACK-berichten omvat:

```
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
```

Bij een storing van de Leaf-B-interface naar UPC, wordt een onjuist gedrag gezien in de logs waar een nieuwe BGP-verbindingspoging wordt geïnitieerd door de UPC (bron: fd00:10:11:12:8) naar de Leaf-A op interface fd00:10:11:11:11:1, die tot een ander VLAN behoort, 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
```

Dergelijk ongeldig BGP SYN-bericht verzonden op de verkeerde interface resulteert in de BGP-down. Wanneer de Nexus zijn eigen verbonden route adverteert en UPC een route krijgt voor de interface die was down over BGP, dan probeert UPC verbinding via een andere interface met een andere/verkeerde uitgaande IP.

Oplossing

Vanwege de configuratie in het gedeelte Conditie van dit artikel, aangezien UPC de verbonden routegegevens van beide pagina's van beide interfaces ontvangt, probeert UPC, wanneer een van de interfaces niet beschikbaar is, via de andere interface met dat blad te communiceren.

Om te voorkomen dat UPC de BGP-verbindingsinstallatieberichten vanuit de verkeerde interface verstuurt, staan hier de configuratiewijzigingen ter overweging:

1. In een UPC-configuratie toevoegen update-source voor de buurvrouw. Deze configuratie voorkomt dat de BGP-verbinding via een andere interface wordt uitgevoerd als de hoofdinterface niet actief is. Bijvoorbeeld, wanneer saegw_vlan140_1/10 (fd00:10:11:11:1/64) is neer dan kan de knoop geen uitgaande interface saegw_vlan141_1/11 voor BGP peer fd00:10:11:11::8 gebruiken.
   Hier is een voorbeeldconfiguratie :

   ```
   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. In de Nexus configuratie, blokkeer de prefixes van de verkeerde interfaces.
   Bijvoorbeeld, ontkennen wij routes voor het overtollige blad over buur fd00:10:11:11::1

   ```
   neighbor fd00:10:11:11::1
   update prefix list to deny fd00:10:11:12::8/64
   ```
3. In Nexus switch moet de EBGP-peer van de VTEP naar een extern knooppunt via VXLAN zich in een huurder VRF bevinden en gebruik maken van de update-source van een loopback interface (peer-over-VXLAN) zoals aanbevolen in de Cisco Nexus 9000 configuratiehandleiding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.