잘못된 컨피그레이션으로 인한 Ultra Packet Core와 Nexus 스위치 간의 BGP 플랩 트러블슈팅

목차

소개

이 문서에서는 Cisco UPC(Ultra Packet Core)와 이중 BGP 연결로 구성된 Nexus 9000 스위치 간의 BGP(Border Gateway Protocol) 플랩 솔루션에 대해 설명합니다.

문제

BGP 플랩은 Cisco Ultra Packet Core와 Nexus 스위치 사이의 이중 인터페이스 중 하나가 플랩할 때 트리거됩니다.

조건

UPC(Ultra Packet Core) 노드는 별도의 포트에서 Nexus Leaf A 및 Leaf B에 연결됩니다. BGP IPv6 피어가 설정되고 기본 경로가 UPC 노드에 설치됩니다. 그림 1은 리프 스위치에 대한 이중화 경로가 포함된 상위 레벨 네트워크 다이어그램을 보여줍니다.

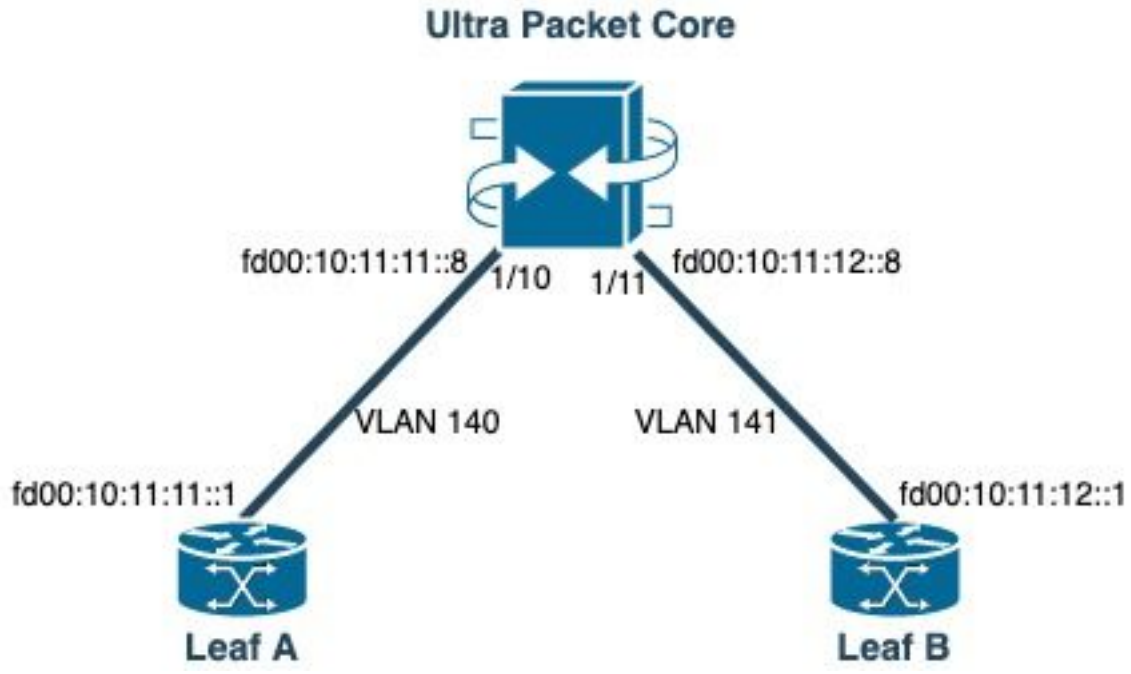

그림 1: 네트워크 다이어그램

설정

VLAN 및 인터페이스 바인딩을 통한 UPC 포트 컨피그레이션:

```
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
```

IP 주소를 사용하는 UPC 인터페이스 컨피그레이션:

```
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 구성:

```
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 스위치 구성:

```
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
```

분석

처음에는 UPC 인터페이스(fd00:10:11:12::8) 중 하나와 Nexus 스위치(fd00:10:11:12::1)간 정상적인 BGP 통신이 관찰되며, 여기에는 TCP ACK 메시지가 포함됩니다.

```
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
```

UPC에 대한 Leaf-B 인터페이스에 오류가 발생할 경우, 다른 VLAN인 vlan140에 속하는 인터페이스 fd00:10:11:11::1의 Leaf-A에 대한 UPC(소스: fd00:10:11:12::8)에서 새 BGP 연결 시도를 시작하는 로그에서 잘못된 동작이 나타납니다.

```
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
```

잘못된 인터페이스에서 전송된 잘못된 BGP SYN 메시지로 인해 BGP 다운이 발생합니다. Nexus가 자체 연결된 경로를 광고하고 UPC가 BGP를 통해 중단된 인터페이스에 대한 경로를 받으면 UPC는 다른 발신 IP를 사용하는 다른 인터페이스를 통해 연결을 시도합니다.

솔루션

이 문서의 Condition 섹션에서 설명하는 컨피그레이션으로 인해 UPC는 두 인터페이스에서 두 Leaf의 연결된 경로 정보를 수신하므로, 인터페이스 중 하나가 다운되면 UPC는 다른 인터페이스를 통해 해당 Leaf와의 통신을 시도합니다.

UPC가 잘못된 인터페이스에서 BGP 연결 설정 메시지를 전송하지 않도록 하려면 고려할 컨피그레이션 변경 사항을 확인하십시오.

1. UPC 컨피그레이션에서 update-source 제공합니다. 이 컨피그레이션은 기본 인터페이스가 다운된 경우 다른 인터페이스로부터의 BGP 연결을 방지합니다. 예를 들어, saegw_vlan140_1/10(fd00:10:11:11::1/64)이 다운되면 노드는 BGP 피어 fd00:10:11:11::8에 대해 발신 인터페이스 saegw_vlan141_1/11을 사용할 수 없습니다.
   다음은 샘플 컨피그레이션입니다.

   ```
   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. Nexus 컨피그레이션에서 잘못된 인터페이스에서 접두사를 차단합니다.
   예를 들어, neighbor fd00:10:11:11::1을 통한 이중화 leaf에 대한 경로를 거부합니다

   ```
   neighbor fd00:10:11:11::1
   update prefix list to deny fd00:10:11:12::8/64
   ```
3. Nexus 스위치에서 VTEP에서 VXLAN을 통해 외부 노드로 피어링하는 EBGP는 테넌트 VRF에 있어야 하며 update-source 의 loopback Cisco Nexus 9000 컨피그레이션 가이드에서 권장하는 인터페이스(VXLAN을 통한 피어링)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.