IPv6 BGP를 사용하여 IPV6 원격 트리거된 블랙 홀 구성

목차

소개

이 문서에서는 IPv6 RTBH(Remote Triggered Black Hole)에서 표시되는 동작을 설명합니다. IPv6 트래픽이 경로 맵을 사용하여 의도적으로 블랙아웃되는 시나리오를 보여 줍니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IPv6
- BGP(Border Gateway Protocol)

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Software Release 15.4 버전을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

RTBH 필터링은 일반적으로 DoS(서비스 거부) 공격을 방지하기 위해 사용되는 기술입니다.DoS 공격에서 흔히 볼 수 있는 문제는 네트워크에 수많은 원치 않는/악성 트래픽이 넘쳐나고 있다는 것입니다.이로 인해 링크 고장이나 높은 CPU 등의 기타 문제가 발생합니다.따라서 합법적인 트래픽이 시작되고 네트워크에 심각한 영향을 미칩니다.

RFC 2545에 따라 BGP 스피커가 Network Address of Next Hop(다음 홉의 네트워크 주소) 필드에 전달되는 전역 IPv6 주소로 식별된 엔티티와 공통 서브넷을 공유하며 경로가 광고되는 피어를 공유하는 경우에만 링크-로컬 주소가 Next Hop 필드에 포함됩니다.다른 모든 경우 BGP 스피커는 Network Address(네트워크 주소) 필드에서 피어에 다음 홉의 전역 IPv6 주소만 광고합니다.

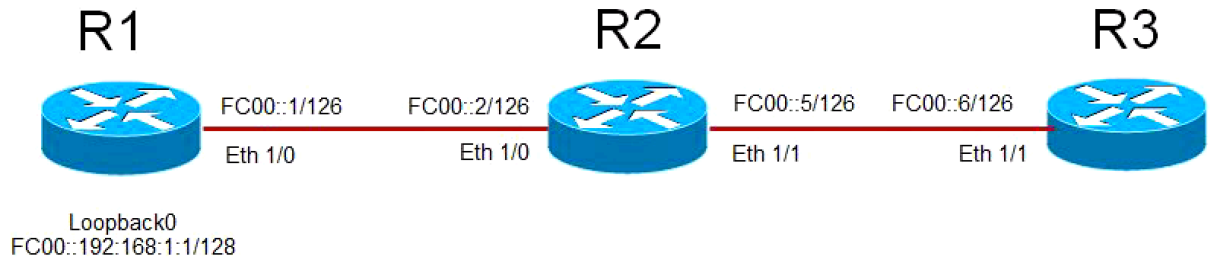
이는 기본적으로 직접 연결된 서브넷에 IPv6 EBGP 인접 관계가 있는 경우 Link Local IP 및 Global IPv6 주소를 다음 홉으로 전달합니다.그러나 RFC(Request for Command)는 어떤 것을 선호할지를 지정하지 않습니다.Cisco는 패킷을 전송하는 동안 항상 가장 짧은 거리이므로 Link 로컬 주소를 선호합니다.RTBH를 사용하는 경우 문제가 될 수 있으며 이 문서에서는 RTBH를 처리하는 방법을 설명합니다.

구성

이 문서에서는 사용 사례를 사용하여 RTBH를 작동하는 데 사용되는 동작 및 명령을 설명합니다.

네트워크 다이어그램

이 이미지는 이 문서의 나머지 부분에 대한 샘플 토폴로지로 사용됩니다.



- R1은 R2와 EBGP 네이버 관계를 가지며 R2는 R3과 EBGP 네이버 관계를 가집니다.
- 라우터 R1은 R2에 BGP를 통해 루프백 0(FC00::192:168:1:1/128)을 알리고 R2는 R3에 광고합니다.
- R3는 경로 맵을 사용하여 R1의 루프백 접두사에 대한 다음 홉을 라우팅 테이블에서 "NULL 0"을 가리키는 더미 IPv6 주소로 설정합니다.

관련 구성

이 컨피그레이션은 RTBH가 사용되는 상황을 시뮬레이션하기 위해 다른 라우터에서 사용됩니다.

R1

```
interface Ethernet1/0
 no ip address
 ipv6 address FC00::1/126
end
```

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address FC00::192:168:1:1/128
 !
 router bgp 65500
 bgp router-id 192.168.1.1
 bgp log-neighbor-changes
 neighbor FC00::2 remote-as 65501
 !
 address-family ipv6
network FC00::/126
 network FC00::192:168:1:1/128
 neighbor FC00::2 activate
```

R2

```
interface Ethernet1/0
 no ip address
 ipv6 address FC00::2/126
end
!
interface Ethernet1/1
 no ip address
 ipv6 address FC00::5/126
!
router bgp 65501
 bgp router-id 192.168.1.2
 bgp log-neighbor-changes
 neighbor FC00::1 remote-as 65500
 neighbor FC00::6 remote-as 65502
 !
 address-family ipv6
 network FC00::/126
 network FC00::4/126
 neighbor FC00::1 activate
 neighbor FC00::6 activate
```

R3

```
interface Ethernet1/1
 no ip address
 ipv6 address FC00::6/126
end
!
ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
 match ipv6 address prefix-list BLACKHOLE-PREFIX
 set ipv6 next-hop FC00::192:168:1:3
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
!
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate
 neighbor FC00::5 route-map BLACKHOLE-PBR in
```

다음을 확인합니다.

테스트 사례 1

R3에 구성된 PBR(정책 기반 라우팅)이 없는 경우 라우팅 테이블에서 R3의 R1 루프백으로 라우팅 하면 R2의 링크 로컬 주소 FE80::A**8BB:CCFF:FE00:A211로 연결됩니다**.

```
BGP Configuration

router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
 !
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate


BGP has both next-hops.

R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 65501 65500
   FC00::5 (FE80::A8BB:CCFF:FE00:A211) from FC00::5 (192.168.1.2)
     Origin IGP, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0


Routing Table has Link Local address as the next-hop.

R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
 Known via "bgp 65502", distance 20, metric 0, type external
 Route count is 1/1, share count 0
 Routing paths:
   FE80::A8BB:CCFF:FE00:A211, Ethernet1/1
     MPLS label: nolabel
     Last updated 00:02:45 ago


Destination is reachable

R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

테스트 사례 2

R3에서 route-map BLACKHOLE-**PBR**을 사용하여 구성된 PBR이 있는 경우 **FC00::192:168:1/128**(R1 루프백)의 라우팅 테이블에 있는 next-hop은 여전히 R2의 링크 로컬 주소

FE80::A BB:CCFF:FC:FC:FC 00:A211. 따라서 트래픽은 블랙박싱되지 않고 링크 로컬 주소를 사용하여 라우팅됩니다.

BGP Configuration

```
ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
 match ipv6 address prefix-list BLACKHOLE-PREFIX
 set ipv6 next-hop FC00::192:168:1:3
!
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
 !
 address-family ipv4
 no neighbor FC00::5 activate
 exit-address-family
 !
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate
 neighbor FC00::5 route-map BLACKHOLE-PBR in
```

Next-hop in BGP changes to the one defined in route-map.

```
R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 65501 65500
   FC00::192:168:1:3 (FE80::A8BB:CCFF:FE00:A211) from FC00::5 (192.168.1.2)
     Origin IGP, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0
```

New next-hop is not reachable and points to Null 0

```
R3#show ipv6 route FC00::192:168:1:3
Routing entry for FC00::192:168:1:3/128
 Known via "static", distance 1, metric 0
 Route count is 1/1, share count 0
 Routing paths:
   directly connected via Null0
     Last updated 00:19:23 ago
```

Routing table still uses Link Local address as next-hop.

```
R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
 Known via "bgp 65502", distance 20, metric 0, type external
 Route count is 1/1, share count 0
 Routing paths:
FE80::A8BB:CCFF:FE00:A211, Ethernet1/1
     MPLS label: nolabel
```

```
     Last updated 00:00:41 ago


Destination is still reachable.

R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

테스트 사례 3

이 동작을 극복하려면 R3에서 BGP neighbor configuration 명령 disable-connected-check를 사용합니다. disable-connected-check는 네이버의 IPv6 주소가 하나의 홉으로만 간주하는 데 사용됩니다 .이 명령이 사용되는 가장 일반적인 시나리오는 직접 연결된 라우터의 루프백에서 EBGP 인접 관계가 설정되는 경우입니다.이 경우 이 명령은 라우터가 EBGP 네이버 관계를 구축하고 있으며 공통 서브넷에 있지 않다는 인상을 줍니다.인접 라우터는 루프백 전반에 걸쳐 있을 수 있으므로 라우터는 링크 로컬 주소를 전달하지 않고 전역 IPv6 주소만 전달하는 접두사를 광고합니다.

이 명령이 추가되면 R3 라우팅 테이블에서 R1의 루프백 192:168:1:1/128에 대한 경로가 FC00::192:168:1:3인 route-map에 따라 다음 홉을 가리키는지 확인할 수 있습니다. 이제 FC00::192:168:1:3에 Null 0을 가리키는 경로가 있으므로 트래픽은 블랙홀입니다.

```
BGP Configuration

ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
 match ipv6 address prefix-list BLACKHOLE-PREFIX
 set ipv6 next-hop FC00::192:168:1:3
!
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
 bgp router-id 192.168.1.3
 bgp log-neighbor-changes
 neighbor FC00::5 remote-as 65501
neighbor FC00::5 disable-connected-check
 !
 address-family ipv4
 no neighbor FC00::5 activate
 exit-address-family
 !
 address-family ipv6
 network FC00::4/126
 neighbor FC00::5 activate
 neighbor FC00::5 route-map BLACKHOLE-PBR in


Next-hop in BGP changes to the one defined in route-map. There is no Link Local Address.

R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
```

```
Paths: (1 available, best #1, table default)
 Not advertised to any peer
 Refresh Epoch 1
 65501 65500
   FC00::192:168:1:3 from FC00::5 (192.168.1.2)
     Origin IGP, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0


Routing table uses the new next-hop.

R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
 Known via "bgp 65502", distance 20, metric 0, type external
 Route count is 1/1, share count 0
 Routing paths:
FC00::192:168:1:3
     MPLS label: nolabel
     Last updated 00:00:37 ago


New next-hop is pointed to Null 0. Traffic will be dropped.

R3#show ipv6 route FC00::192:168:1:3
Routing entry for FC00::192:168:1:3/128
 Known via "static", distance 1, metric 0
 Route count is 1/1, share count 0
 Routing paths:
   directly connected via Null 0
     Last updated 02:18:03 ago


Destination is not reachable

R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

참고: CSCuv60686 **disable-connected-check** route-map .

문제 해결

현재 이 문서에 대해 사용 가능한 특정 문제 해결 정보가 없습니다.