Introduction

This document describes the behavior seen with IPV6 Remote Triggered Black Hole (RTBH). It shows a scenario where IPv6 traffic is intentionally black holed using a route map.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IPv6
- Border Gateway Protocol (BGP)

Components Used

The information in this document is based on Cisco IOS Software Release 15.4 version.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

RTBH filtering is a technique generally employed to prevent denial of service (DoS) attack. A common problem seen with DoS attacks is that network is flooded with huge volumes of unwanted/malicious traffic. This results in link choking and other problems like high CPU etc. This starves out legitimate traffic and results in serious implications on network.

As per RFC 2545 ,The link-local address shall be included in the Next Hop field if and only if the
BGP speaker shares a common subnet with the entity identified by the global IPv6 address carried in the Network Address of Next Hop field and the peer the route is being advertised to. In all other cases a BGP speaker shall advertise to its peer in the Network Address field only the global IPv6 address of the next hop.

It basically means that if you have a IPv6 EBGP neighbor relationship on directly connected subnet, then it carries the Link Local IP as well as Global IPv6 address as a next hop. However, Request for Command (RFC) does not specify which one should be preferred. Cisco prefers Link local address because while it sends the packet it is always the shortest distance. When you use RTBH, it could be an issue and this document explains how to deal with it.

**Configure**

This document takes a use case to explain the behavior and the commands used to get RTBH working.

**Network Diagram**

This image is used as a sample topology for rest of this document.

![Network Diagram](image)

- R1 has EBGP neighbor relationship with R2 and R2 has EBGP neighbor relationship with R3.
- Router R1 advertises its loopback 0 (FC00::192:168:1:1/128) via BGP to R2 and R2 advertises it to R3.
- R3 uses a route-map to set next hop for R1’s loopback prefix to a dummy IPv6 address that points to "NULL 0" in routing table.

**Relevant Configuration**

This configuration is used on different routers to simulate a situation where RTBH would be used:

```
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
end

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

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

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

Verify

Test case 1

When there is no policy based routing (PBR) configured on R3, in routing table, route to R1’s loopback on R3 points to R2’s link local address FE80::A8BB:CCFF:FE00:A211.
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

  65500 5 (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

Test case 2

When there is PBR configured using route-map BLACKHOLE-PBR on R3, it is observed that for FC00::192:168:1:1/128 (R1’s loopback), next-hop in routing table still points to R2’s link local address FE80::A8BB:CCFF:FE00:A211. Therefore, the traffic is never black holed and instead routed using link local addresses.

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

Test case 3
In order to overcome this behavior, use BGP neighbor configuration command `disable-connected-check` on R3. Disable-connected-check is used to assume that neighbor’s IPv6 address is only one hop way. The most common scenario where this command is used is when EBGP neighbor relationship is established on loopbacks for directly connected routers. In this case, the command gives an impression that routers are building EBGP neighbor relationship and are not on common subnet. Neighborship could be across loopbacks and hence, router while it advertises the prefix which does not carry the link local address but only the Global IPv6 address.

Once this command is added, you can see that route for R1’s loopback `192:168:1:1/128` in routing table of R3, points to the next hop in accordance route-map that is `FC00::192:168:1:3`. Now, since `FC00::192:168:1:3` has a route pointing to Null 0, therefore, traffic is black holed.

**BGP Configuration**

```plaintext
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
```
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)
```

**Note:** A new enhancement [CSCuv60686](#) changes this behavior so that route-map takes effect without using the command `disable-connected-check`.

**Troubleshoot**

There is currently no specific troubleshooting information available for this document.