

Configuración del Hoyo Negro Desencadenado Remoto IPV6 con BGP IPv6

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración relevante](#)

[Verificación](#)

[Caso de prueba 1](#)

[Caso de prueba 2](#)

[Caso de prueba 3](#)

[Troubleshoot](#)

Introducción

Este documento describe el comportamiento observado con el agujero negro desencadenado remoto IPV6 (RTBH). Muestra un escenario en el que el tráfico IPv6 se mantiene intencionalmente en espera en negro utilizando un route map.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- IPv6
- Border Gateway Protocol (BGP)

Componentes Utilizados

La información de este documento se basa en la versión 15.4 del software del IOS de Cisco.

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.

Antecedentes

El filtrado de RTBH es una técnica utilizada generalmente para evitar ataques de denegación de servicio (DoS). Un problema común observado con los ataques de DoS es que la red está inundada de grandes volúmenes de tráfico malintencionado o no deseado. Esto da como resultado el bloqueo de enlaces y otros problemas como el uso excesivo de CPU, etc. Esto priva al tráfico legítimo y tiene graves consecuencias en la red.

Según RFC 2545 , la dirección local del link se incluirá en el campo Siguiete Salto si y sólo si el altavoz BGP comparte una subred común con la entidad identificada por la dirección IPv6 global transportada en el campo Dirección de red del Siguiete Salto y el par al que se anuncia la ruta. En todos los demás casos, un altavoz BGP anunciará a su par en el campo Dirección de red solamente la dirección IPv6 global del salto siguiente.

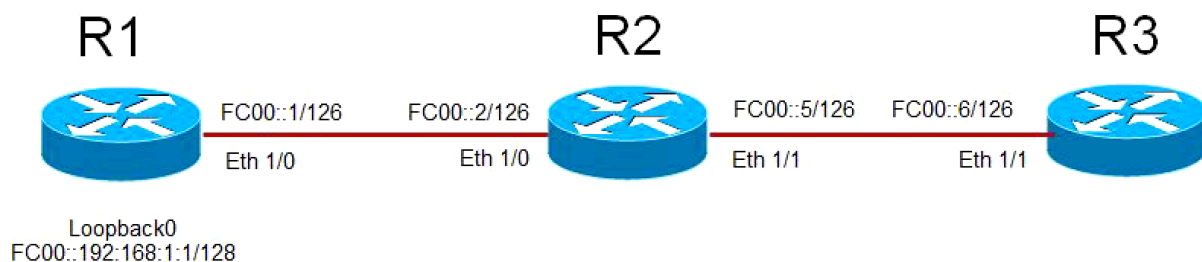
Básicamente significa que si tiene una relación de vecino EBGP IPv6 en una subred conectada directamente , entonces transporta la IP local de link así como la dirección IPv6 global como salto siguiente. Sin embargo, la solicitud de comando (RFC) no especifica cuál debe ser el preferido. Cisco prefiere la dirección local de link porque mientras envía el paquete siempre es la distancia más corta. Cuando utiliza RTBH, podría ser un problema y este documento explica cómo tratarlo.

Configurar

Este documento toma un caso práctico para explicar el comportamiento y los comandos usados para hacer que RTBH funcione.

Diagrama de la red

Esta imagen se utiliza como topología de ejemplo para el resto de este documento.



- R1 tiene relación de vecino EBGP con R2 y R2 tiene relación de vecino EBGP con R3.
- El router R1 anuncia su loopback 0 (FC00::192:168:1:1/128) a través de BGP a R2 y R2 lo anuncia a R3.
- R3 utiliza un route-map para establecer el siguiente salto para el prefijo de loopback de R1 en una dirección IPv6 ficticia que apunta a "NULL 0" en la tabla de ruteo.

Configuración relevante

Esta configuración se utiliza en diferentes routers para simular una situación en la que se utilizaría RTBH:

```
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
```

Verificación

Caso de prueba 1

Cuando no hay un routing basado en políticas (PBR) configurado en R3, en la tabla de routing, rutea al loopback de R1 en R3 apunta a la dirección local de enlace de R2 **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
    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
```

Caso de prueba 2

Cuando hay PBR configurado usando route-map **BLACKHOLE-PBR** en R3, se observa que para **FC00::192:168:1:1/128** (loopback de R1), el siguiente salto en la tabla de ruteo todavía apunta a la dirección local de link de R2 **FE80::A8BB:CCFF:FE00:A211**. Por lo tanto, el tráfico nunca se mantiene en espera en negro y, en su lugar, se rutea usando direcciones locales de link.

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
```

Caso de prueba 3

Para superar este comportamiento, utilice el comando de configuración de vecino BGP **disable-connected-check** en R3. Disable-connected-check se utiliza para suponer que la dirección IPv6 del vecino es sólo una dirección de salto . El escenario más común en el que se utiliza este comando es cuando se establece la relación de vecino EBGP en loopbacks para routers conectados directamente. En este caso, el comando da la impresión de que los routers están creando una relación de vecino EBGP y no están en una subred común. El vecindario podría estar entre loopbacks y por lo tanto, el router mientras anuncia el prefijo que no lleva la dirección local del link sino solamente la dirección IPv6 global .

Una vez agregado este comando , puede ver que la ruta para el loopback de R1 **192:168:1:1/128** en la tabla de ruteo de R3, señala al salto siguiente de acuerdo con route-map que es **FC00::192:168:1:3**. Ahora, ya que **FC00::192:168:1:3** tiene una ruta que apunta a Null 0, por lo tanto, el tráfico está en espera negra.

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)
```

Nota: Una nueva mejora [CSCuv60686](#) cambia este comportamiento para que route-map surta efecto sin utilizar el comando **disable-connected-check**.

Troubleshoot

Actualmente no hay información específica sobre la solución de problemas disponible para este documento.