

Настройте IPv6 удаленная инициированная черная дыра с BGP IPv6

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Соответствующая конфигурация](#)

[Проверка](#)

[Контрольный пример 1](#)

[Контрольный пример 2](#)

[Контрольный пример 3](#)

[Устранение неполадок](#)

Введение

Этот документ описывает поведение, замеченное с Удаленной инициированной черной дырой (RTBH) IPv6. Это показывает сценарий, где трафик IPv6 является преднамеренно черным перфорируемым использованием Карты маршрутизации.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- IPv6
- Border Gateway Protocol (BGP)

Используемые компоненты

Сведения в этом документе основываются на Cisco IOS Software Release 15.4 версий.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Фильтрация RTBH является способом, обычно используемым для предотвращения атаки типа отказ в обслуживании (DOS). Типичная проблема, замеченная с атаками DoS, - то, что сеть лавинно рассылаётся огромными громкостями нежелательного / вредоносного трафика. Это приводит к дросселированию ссылки и другим проблемам как высокая загрузка CPU и т.д. Это исчерпало ресурсы легальный трафик и приводит к серьезным результатам в сети.

Согласно RFC 2545, локальный для канала адрес должен быть включен в поле Next Hop, если и только если динамик BGP совместно использует общую подсеть с объектом, определенным глобальным адресом IPv6, который несут в поле Network Address of Next Hop и узле, к которому объявляется маршрут. Во всех других случаях динамик BGP должен объявить к его узлу в поле Network Address только глобальный адрес IPv6 следующего перехода.

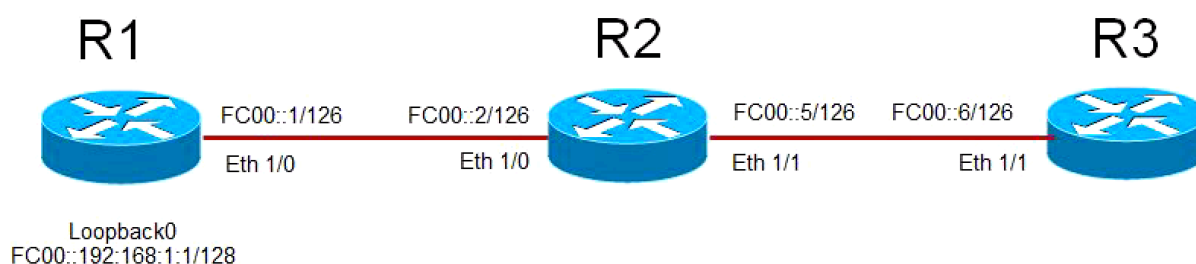
Это в основном означает, что, если у вас есть отношение Соседа по протоколу EBGP IPv6 в напрямую подключенной подсети, тогда это несет Локальный IP Ссылки, а также Глобальный адрес IPv6 как следующий переход. Однако Запрос о команде (RFC) не задает, какой должен быть предпочтен. Cisco предпочитает Локальный адрес канала, потому что, в то время как это передает пакет, это всегда - кратчайшее расстояние. При использовании RTBH это могла быть проблема, и этот документ объясняет, как иметь дело с ним.

Настройка

Этот документ берет вариант использования для объяснения поведения, и команды использовали получать работу RTBH.

Схема сети

Этот образ используется в качестве примера топологии для отдыха этого документа.



- R1 имеет отношение Соседа по протоколу EBGP с R2, и R2 имеет отношение Соседа по протоколу EBGP с R3.
- Маршрутизатор R1 объявляет свой loopback 0 (FC00:: 192:168:1:1/128) через BGP к R2 и R2 объявляет его к R3.
- R3 использует route-мар для установки следующего перехода для петлевого префикса R1 к фиктивному адресу IPv6, который указывает к "NULL 0" в таблице маршрутизации.

Соответствующая конфигурация

Эта конфигурация используется на других маршрутизаторах для моделирования ситуации,

где RTBH использовался бы:

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 activateR2
```

```
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 activateR3
```

```
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
```

Проверка

Контрольный пример 1

Когда нет никакой маршрутизации на основе политик (PBR), настроенной на R3, в таблице маршрутизации, маршруте к loopback R1 на точках R3 к локальному адресу канала 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
```

Контрольный пример 2

Когда существует PBR, настроенный с помощью **ПОМЕЩАТЬ-В-ЧЕРНЫЙ-СПИСОК-PBR** route-мар на R3, замечено что для **FC00::192:168:1:1/128** (loopback R1), неподвижные точки таблицы маршрутизации next-hop in к локальному адресу канала R2 **FE80::A8BB:CCFF:FE00:A211**. Поэтому трафик никогда не не черный перфорируемый и вместо этого маршрутизировавшие локальные адреса канала использования.

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
```

Контрольный пример 3

Для преодоления этого поведения используйте команду настройки Соседнего BGP узел **disable-connected-check** на R3. **Disable-connected-check** используется, чтобы предположить, что адрес IPv6 соседнего узла является только одним переходом путь. Наиболее распространенный scenario, где эта команда используется, - когда отношение Соседа по протоколу EBGP установлено на loopback для непосредственно подключенных маршрутизаторов. В этом случае команда производит впечатление, что маршрутизаторы строят отношения Соседа по протоколу EBGP и не находятся на общей подсети. Соседство могло быть через loopback и следовательно, маршрутизатор, в то время как это объявляет префикс, который не несет локальный адрес канала, но только Глобальный адрес IPv6.

Как только эта команда добавлена, вы видите, что маршрут для loopback R1 **192:168:1:1/128** в таблице маршрутизации R3, точек к следующему переходу в route-map соответствия, который является **FC00:: 192:168:1:3**. Теперь, начиная с **FC00:: 192:168:1:3** имеет маршрут, указывающий на Пустой 0, поэтому, трафик черный перфорированный.

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)
```

Примечание: Новый [CSCuv60686](#) усовершенствования изменяет это поведение так, чтобы route-map вступил в силу, не используя команду **disable-connected-check**.

Устранение неполадок

В настоящее время нет никаких определенных сведений об устранении проблем, доступных для этого документа.