

인터페이스 Null0을 통해 IPv6 Black-Holding 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[샘플 구성](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 인터페이스 Null0을 통해 IPv6에서 Black-Holding을 구성하는 방법에 대해 설명합니다. Black Hole Routing은 관리자가 불법 소스의 트래픽 또는 DoS(Denial of Service) 공격에 의해 생성된 트래픽과 같은 원하지 않는 트래픽을 차단할 수 있는 방법입니다. 이 방법은 트래픽을 데드 인터페이스 또는 조사 정보를 수집하도록 설계된 호스트로 동적으로 라우팅하여 네트워크에 대한 공격의 영향을 완화합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- BGP 라우팅 프로토콜 및 해당 작업에 대한 이해
- IPv6 주소 지정 체계에 대한 이해

사용되는 구성 요소

이 문서의 정보는 Cisco 7200 Series Router with Cisco IOS® Software Release 15.0(1)을 기반으로 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

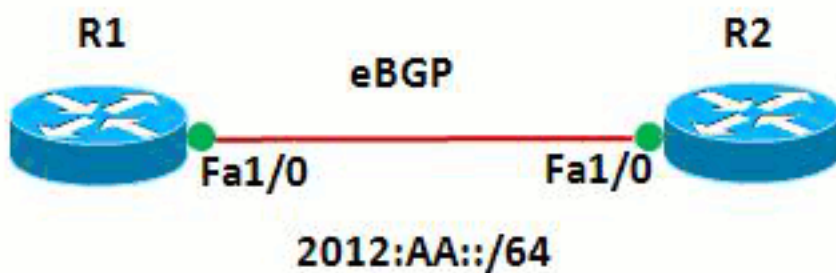
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 자세한 내용을 보려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 네트워크에서 라우터와 R1 및 R2는 서로 eBGP 관계를 형성합니다. 라우터는 내부적으로 통신하기 위해 OSPFv3을 사용합니다. 라우터 R1에서는 소스 주소가 20:20::20/128인 모든 패킷이 Null0으로 전달되는 방식으로 Null0의 컨피그레이션에 의해 블랙홀링을 수행합니다. 즉, Null0으로 라우팅된 모든 트래픽이 삭제됩니다.

샘플 구성

이 문서에서는 다음 구성을 사용합니다.

- [라우터 R1](#)
- [라우터 R2](#)

라우터 R1

```
!  
hostname R1  
!  
no ip domain lookup  
ip cef  
ipv6 unicast-routing  
ipv6 cef  
!  
!  
interface Loopback1
```

```
no ip address
ipv6 address AA::1/128
ipv6 enable
ipv6 ospf 10 area 0
!
interface Loopback10
no ip address
ipv6 address AA:10::10/128
ipv6 enable
!
interface FastEthernet1/0
no ip address
speed auto
duplex auto
ipv6 address 2012:AA::1/64
ipv6 enable
ipv6 ospf 10 area 0
!
router bgp 6501
bgp router-id 1.1.1.1
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor BB::1 remote-as 6502
neighbor BB::1 ebgp-multihop 2
neighbor BB::1 update-source Loopback1
!
address-family ipv4
exit-address-family
!
address-family ipv6
redistribute static
network AA:10::10/128
neighbor BB::1 activate
exit-address-family
!
ipv6 route 20:20::20/128 Null0
ipv6 router ospf 10
router-id 1.1.1.1
!
end
```

라우터 R2

```
!
hostname R2
!
ipv6 unicast-routing
ipv6 cef
!
!
interface Loopback1
no ip address
ipv6 address BB::1/128
ipv6 enable
ipv6 ospf 10 area 0
!
interface Loopback20
no ip address
ipv6 address 20:20::20/128
ipv6 enable
!
interface FastEthernet1/0
```

```

no ip address
speed auto
duplex auto
ipv6 address 2012:AA::2/64
ipv6 enable
ipv6 ospf 10 area 0
!
router bgp 6502
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor AA::1 remote-as 6501
  neighbor AA::1 ebgp-multihop 2
  neighbor AA::1 update-source Loopback1
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
    network 20:20::20/128
    neighbor AA::1 activate
  exit-address-family
  !
ipv6 router ospf 10
  router-id 2.2.2.2
!
end

```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

eBGP 컨피그레이션을 확인하려면 라우터 R1에서 [show ipv6 route bgp](#) 및 **show bgp ipv6 unicast** 명령을 사용합니다.

라우터 R1

show ipv6 route

```

R1#show ipv6 route bgp
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-
user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R -
RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea,
IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor
Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
!--- The router R2 advertises the network 20:20::20/128,
!--- but still the routing table is empty.

```

BGP에서 수신한 경로를 확인하려면 **show bgp ipv6 unicast** 명령을 사용합니다.

```

R1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1

```

```

Status codes: s suppressed, d damped, h history, *
valid, > best, I - internal,
              r RIB-failure, S Stale
Origin codes: I - IGP, e - EGP, ? - incomplete

Network      Next Hop      Metric LocPrf
Weight Path
* 20:20::20/128 BB::1          0
0 6502 I
*>           ::          0
32768 ?
*> AA:10::10/128 ::          0
32768 I
!--- Note that the route 20:20::20/128 is received, !---
- but it is not installed in the routing table.

```

라우터 R2에서 라우터 R1을 ping하기 위해 소스를 루프백 인터페이스 20으로 사용합니다.

```
R2#ping ipv6 AA:10::10 source lo20
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AA:10::10, timeout is 2 seconds:
Packet sent with a source address of 20:20::20
.....
Success rate is 0 percent (0/5)
!--- The reason is the ICMP packet reaches !--- router R1 with source address as !---
20:20::20/128 and therefore gets dropped.

```

루프백 인터페이스를 소스로 사용하지 않고 라우터 R2에서 라우터 R1을 ping해 보십시오.

```
R2#ping AA:10::10
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to AA:10::10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/61/180 ms
!--- In this case, the ICMP packet has !--- the source address as BB::1.

```

ipv6 route 20:20::20/128 Null0 문이 라우터 R1에서 제거되면 라우터 R2에 의해 광고되는 경로 20:20::20/128이 라우터 R1의 라우팅 테이블에 설치됩니다. 다음은 샘플 출력입니다.

라우터 R1에서

```
R1(config)#no ipv6 route 20:20::20/128 Null0
```

```

!--- The Null0 command is removed from router R1.
R1#show bgp ipv6 unicast BGP table version is 7, local
router ID is 1.1.1.1 Status codes: s suppressed, d
damped, h history, * valid, > best, I - internal, r RIB-
failure, S Stale Origin codes: I - IGP, e - EGP, ? -
incomplete Network Next Hop Metric LocPrf Weight Path *>
20:20::20/128      ::          0
32768 ?
*                   BB::1          0
0 6502 I
*> AA:10::10/128   ::          0
32768 I
!--- After the removal of the statement, !--- the route

```

```
20:20::20/128 is shown as best route. R1#show ipv6 route
bgp
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-
user Static route
        B - BGP, HA - Home Agent, MR - Mobile Router, R -
RIP
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea,
IS - ISIS summary
        D - EIGRP, EX - EIGRP external, ND - Neighbor
Discovery
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B 20:20::20/128 [20/0]
  via BB::1

!--- You can see that the route is displayed in routing
table.
```

이제 루프백 인터페이스 Lo 20으로 소스를 사용하여 라우터 R2에서 라우터 R1을 ping해 보십시오.

```
R2#ping ipv6 AA:10::10 source lo20
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to AA:10::10, timeout is 2 seconds:

Packet sent with a source address of 20:20::20

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/54/140 ms

!--- You can see that the ping is successful.

관련 정보

- [원격으로 트리거된 블랙홀 필터링](#)
- [BGP 기술 지원](#)
- [IP 버전 6 기술 지원](#)
- [BGP 사례 연구](#)
- [기술 지원 및 문서 - Cisco Systems](#)