

# Configurazione di Black-Holing IPv6 tramite interfaccia Null0

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Esempi di configurazione](#)

[Verifica](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene descritto come configurare Black-Holing in IPv6 tramite l'interfaccia Null0. Black Hole Routing è un metodo che consente all'amministratore di bloccare il traffico indesiderato, ad esempio il traffico proveniente da fonti illegali o il traffico generato da un attacco Denial of Service (DoS), instradando dinamicamente il traffico a un'interfaccia inattiva o a un host progettato per raccogliere informazioni da esaminare, in modo da ridurre l'impatto dell'attacco alla rete.

## [Prerequisiti](#)

### [Requisiti](#)

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Conoscenza del protocollo di routing BGP e del relativo funzionamento
- Conoscere lo schema di indirizzamento IPv6

### [Componenti usati](#)

Per la stesura del documento, è stato usato un router Cisco serie 7200 con software Cisco IOS<sup>®</sup> versione 15.0(1).

### [Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni](#)

[nei suggerimenti tecnici.](#)

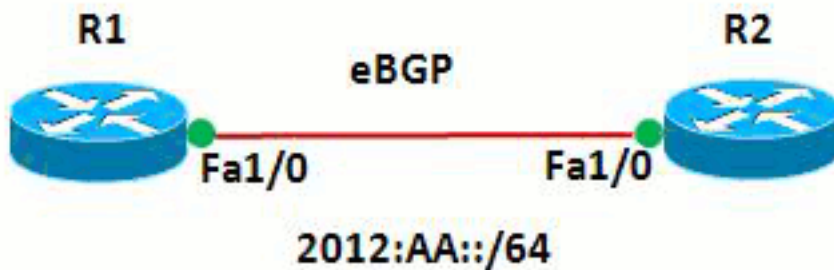
## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



In questa rete, i router R1 e R2 formano una relazione eBGP tra loro. I router utilizzano OSPFv3 per comunicare internamente. Nel router R1, la funzione Black-Holing viene ottenuta tramite la configurazione di Null0 in modo che tutti i pacchetti con indirizzo di origine 20:20:20/128 vengano indirizzati a Null0. In altre parole, tutto il traffico indirizzato a Null0 viene scartato.

## Esempi di configurazione

Nel documento vengono usate queste configurazioni:

- [Router R1](#)
- [Router R2](#)

### Router 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
```

## Router 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

```

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Per verificare la configurazione eBGP, utilizzare i comandi [show ipv6 route bgp](#) e [show bgp ipv6 unicast](#) nel router R1.

### Router R1

#### mostra route ipv6

```

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.

```

Per verificare quali sono le route ricevute da BGP, utilizzare il comando **show bgp ipv6 unicast**.

```
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
*>
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.
```

Usare l'origine come interfaccia di loopback 20 per provare a eseguire il ping tra il router R1 e il router R2.

```
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.
```

Provare a eseguire il ping tra il router R1 e il router R2 senza usare l'interfaccia di loopback come origine.

```
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.
```

Se l'istruzione **ipv6 route 20:20:20/128 Null0** viene rimossa dal router R1, la route 20:20:20/128 annunciata dal router R2 viene installata nella tabella di routing del router R1. Di seguito viene riportato l'output di esempio:

**Nel router R1**

```
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.

```

Provare a eseguire il ping tra il router R1 e il router R2 con l'origine come interfaccia di loopback Lo 20.

```
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.*

## [Informazioni correlate](#)

- [Filtraggio dei fori neri attivato in remoto](#)
- [Supporto tecnologia BGP](#)
- [Supporto della tecnologia IP versione 6](#)
- [Case study del protocollo BGP](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)