Come evitare loop di routing quando si utilizza un NAT dinamico

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Esempio di rete](#)
[Convenzioni](#)
[Scenario di esempio](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive uno scenario in cui i pacchetti si collegano in loop tra il router NAT e il router adiacente sull'interfaccia esterna quando si utilizza il servizio NAT (Dynamic Network Address Translation) a causa del traffico destinato a un indirizzo IP non utilizzato in un pool NAT e della presenza di un percorso predefinito sul router NAT che inoltra questi pacchetti all'esterno.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

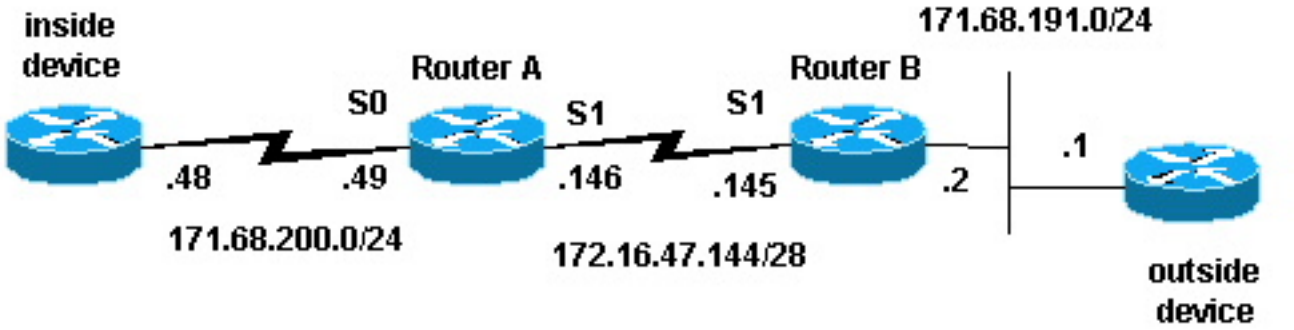
Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Per creare lo scenario di esempio è stata utilizzata la topologia seguente.



Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Scenario di esempio

Nella topologia sopra descritta, il router A è configurato con NAT in modo da convertire i pacchetti provenienti dalla rete 171.68.200.0/24 in un intervallo di indirizzi definiti dal pool NAT "test-loop". La configurazione del router A è la seguente (tutti gli altri router sono configurati con route statiche per ottenere la connettività):

```
hostname Router-A
!
!
ip nat pool test-loop 172.16.47.161 172.16.47.165 prefix-length 28
ip nat inside source list 7 pool test-loop
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

```
line vty 0 4
 login
!
end
```

Usando il debug di conversione NAT e i comandi di debug dei pacchetti IP, abbiamo generato un ping dal router sul dispositivo interno. Il ping ha funzionato ed è stata generata una voce della tabella di conversione. Nell'output seguente, viene mostrato che il debug dei pacchetti IP e il debug IP NAT sono attivi e che al momento non sono presenti voci nella tabella di conversione.

Nota: i comandi **debug** generano una quantità significativa di output. Utilizzarli solo quando il traffico sulla rete IP è basso, in modo che le altre attività del sistema non siano influenzate negativamente.

```
Router-A# show debug
Generic IP:
  IP packet debugging is on (detailed)
  IP NAT debugging is on
Router-A# show ip nat translations
Router-A#
```

Il router interno (dispositivo interno) genera un pacchetto ICMP con indirizzo di origine 171.68.200.48 e indirizzo di destinazione 171.68.191.1 (indirizzo del dispositivo esterno). L'output di **debug** riportato di seguito mostra un pacchetto IP con indirizzo IP di origine 171.68.200.48 che viene convertito in 172.16.47.161. Il pacchetto arriva all'interfaccia Serial0 e viene destinato all'interfaccia Serial1.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [401]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

L'output del comando **debug** seguente visualizza il pacchetto IP di ritorno con indirizzo IP di destinazione 172.16.47.161, convertito nuovamente in 171.68.200.48. Il pacchetto viene inserito nell'interfaccia Serial1 e destinato all'interfaccia serial0.

```
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [401]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

L'output del comando **debug** visualizza lo scambio di ping tra il dispositivo interno ed il dispositivo esterno:

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [402]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [402]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [403]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [403]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [404]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [404]
```

```
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [405]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [405]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

Usando il comando **show ip nat translation**, nella tabella delle traduzioni viene visualizzata una voce per il dispositivo interno.

```
Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
```

Ora che la tabella di conversione contiene una traduzione del dispositivo interno, è possibile eseguire correttamente il ping tra il dispositivo esterno e l'indirizzo globale del dispositivo interno, come mostrato nell'output di debug generato dal router-A riportato di seguito.

Nota: il pacchetto originato dal dispositivo esterno ha un indirizzo di origine 171.68.191.1 e un indirizzo di destinazione 172.16.47.161 (l'indirizzo globale interno nella tabella di conversione).

```
Router-A#
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [108]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [108]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [109]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [109]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [110]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [110]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [111]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [111]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [112]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [112]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
```

L'output di debug seguente mostra ciò che può accadere quando un dispositivo esterno tenta di avviare la comunicazione con un indirizzo di destinazione che è un indirizzo IP inutilizzato nel pool del ciclo di test. Il comando **clear ip nat translation** è stato usato per cancellare la tabella di conversione e un ping è stato inviato a un indirizzo IP non usato all'interno del pool di test-loop.

Il dispositivo esterno invia un pacchetto ICMP destinato all'indirizzo globale interno 172.16.47.161.

Tuttavia, l'interfaccia di output è la stessa dell'interfaccia di input per questo pacchetto.

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

Il protocollo NAT converte i pacchetti da un indirizzo esterno a un indirizzo interno prima di inoltrarli. In questo caso, la tabella di conversione non contiene alcuna voce, quindi il router A può solo inoltrare il pacchetto. Il router A si basa sul suo percorso predefinito per instradare i pacchetti, rinviandoli all'interfaccia Serial1, che a sua volta causa un loop che potrebbe alla fine far crollare la linea seriale.

Per evitare questo tipo di loop di routing, non creare mai pacchetti dai dispositivi esterni agli indirizzi globali interni. Tuttavia, poiché questa impostazione è difficile da applicare, è possibile aggiungere una route statica per gli indirizzi globali interni con un hop successivo null0 in Router-A. In questo modo, quando un dispositivo esterno invia i pacchetti destinati a un indirizzo globale interno e non c'è alcuna voce nella tabella di conversione, il router A instrada il pacchetto a null0, evitando il loop. Utilizzando l'esempio precedente, la route statica avrà il seguente aspetto:

```
ip route 172.16.47.160 255.255.255.252 null0.
```

Informazioni correlate

- Pagina di supporto NAT
- Pagina di supporto per i protocolli di routing IP
- Pagina di supporto per il routing IP
- Supporto tecnico – Cisco Systems