

Verifica e risoluzione dei problemi di connettività NAT di base

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Problema](#)

[Eseguire il ping di un router ma non di un altro](#)

[Risoluzione dei problemi](#)

[i dispositivi di rete esterni non possono comunicare con i router interni](#)

[Risoluzione dei problemi](#)

[Elenco di controllo per problemi comuni](#)

[La conversione non è installata nella tabella delle conversioni](#)

[La voce di traduzione corretta non è utilizzata](#)

[NAT funziona correttamente ma vi sono ancora problemi di connettività](#)

["%Nsistema AT Occupato - Riprova Più Tardi"](#)

[Una tabella di conversione grande aumenta l'utilizzo della CPU](#)

[La tabella ARP è vuota](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere i problemi di connettività IP in un ambiente NAT.

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.

Convenzioni

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

Problema

Questo documento descrive come risolvere i problemi di connettività IP in un ambiente NAT rivedendo i due esempi successivi:

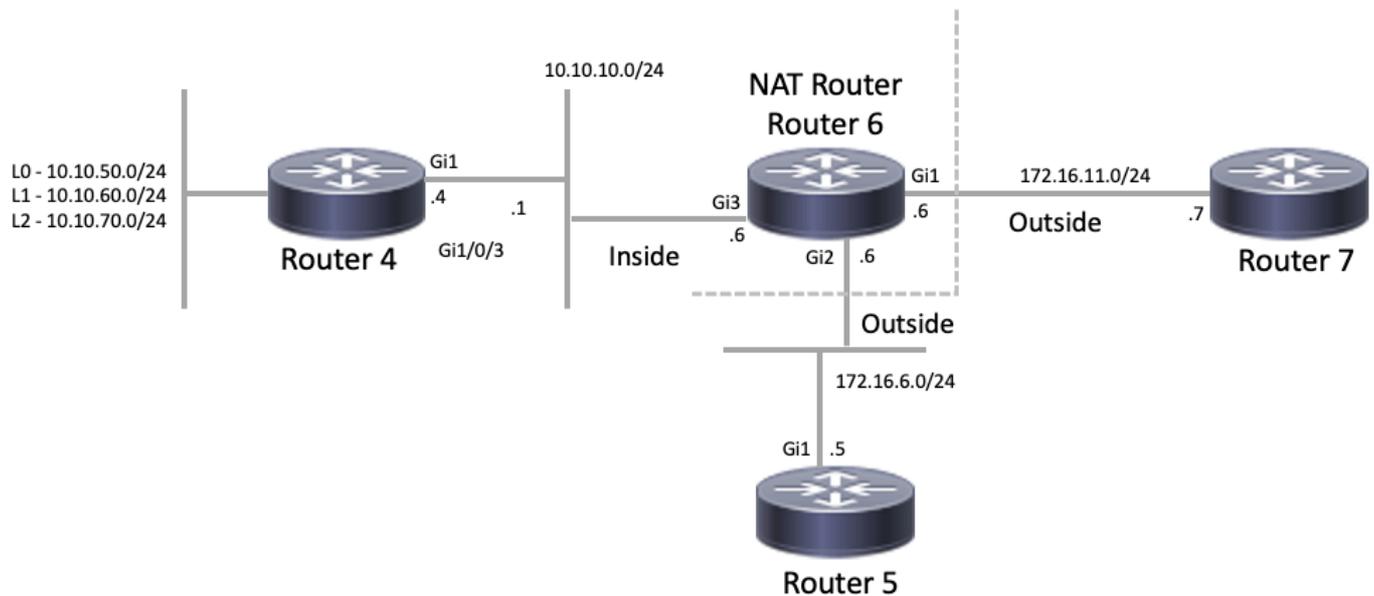
1. Eseguire il ping di un router ma non di un altro
2. i dispositivi di rete esterni non possono comunicare con i router interni

I passaggi di base seguenti sono utili per determinare se si è verificato un problema nelle operazioni NAT:

1. Verificare la configurazione e definire chiaramente cosa NAT deve raggiungere. In base all'analisi, è possibile stabilire se si è verificato un problema con la configurazione. Per informazioni sulla configurazione NAT, consultare il documento sulla [configurazione di Network Address Translation](#).
2. Verificare che la tabella di traduzione contenga le traduzioni corrette.
3. Utilizzare i comandi show e debug per verificare che la traduzione venga eseguita.
4. Esaminare attentamente cosa succede al pacchetto e verificare che i router dispongano delle informazioni di routing corrette per inoltrare il pacchetto.

Eseguire il ping di un router ma non di un altro

Nel primo scenario, il router 4 può eseguire il ping tra il router 5 (172.16.6.5) e il router 7 (172.16.11.7):



Topologia NAT

<#root>

Router4#

ping 172.16.6.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:
 .!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
 Router4#

ping 172.16.11.7

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

Success rate is 0 percent (0/5)
 Router4#

Considerazioni importanti su questo scenario:

- Sui router non sono configurati protocolli di routing dinamico, vengono utilizzate solo route statiche.
- Il gateway predefinito del router 4 è il router 6.
- Il router 6 è configurato con NAT.

<#root>

```
interface GigabitEthernet1
ip address 172.16.11.6 255.255.255.0
```

```
ip nat outside
```

```

negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.6.6 255.255.255.0

ip nat outside

negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet3
ip address 10.10.10.6 255.255.255.0

ip nat inside

negotiation auto
no mop enabled
no mop sysid
!
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source static 10.10.10.4 172.16.11.70
!
ip access-list standard 7
10 permit 10.10.50.4
20 permit 10.10.60.4
30 permit 10.10.70.4

```

Risoluzione dei problemi

1. In primo luogo, devi determinare che NAT funziona correttamente. Dalla configurazione precedente, è possibile stabilire che l'indirizzo IP 10.10.10.4 del router 4 è stato convertito in modo statico in 172.16.6.14. È possibile utilizzare il comando `show ip nat translation` sul router 6 per verificare che la traduzione sia presente nella tabella di traduzione:

```
<#root>
```

```
NAT-Router#
```

```
show ip nat translations
```

```

Pro  Inside global      Inside local      Outside local      Outside global
---  172.16.6.14          10.10.10.4        ---                ---
Total number of translations: 1

```

```
NAT-Router#
```

2. Verificare che questa conversione venga eseguita quando il router 4 origina il traffico IP. È

possibile effettuare questa operazione in due modi dal Router 6. Eseguire un debug NAT o monitorare le statistiche NAT con il comando `show ip nat statistics`. Poiché i comandi debug sono l'ultima risorsa, iniziare con il comando `show`.

3. Controllare il contatore per verificare che aumenti man mano che riceve il traffico dal router 4. Il contatore viene incrementato ogni volta che la tabella di conversione viene utilizzata per tradurre un indirizzo.

4. Cancellare le statistiche, quindi visualizzare le statistiche, provare a eseguire il ping tra il router 7 e il router 4, quindi visualizzare nuovamente le statistiche.

```
<#root>
```

```
NAT-Router#
```

```
clear ip nat statistics
```

```
NAT-Router#
```

```
NAT-Router#
```

```
show ip nat statistics
```

```
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
```

```
Outside interfaces:
```

```
  GigabitEthernet1, GigabitEthernet2
```

```
Inside interfaces:
```

```
  GigabitEthernet3
```

```
Hits: 0 Misses: 0
```

```
Expired translations: 0
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 7 pool test refcount 0
```

```
  pool test: id 1, netmask 255.255.255.0
```

```
    start 172.16.11.70 end 172.16.11.71
```

```
    type generic, total addresses 2, allocated 0 (0%), misses 0
```

```
nat-limit statistics:
```

```
  max entry: max allowed 0, used 0, missed 0
```

```
In-to-out drops: 0 Out-to-in drops: 0
```

```
Pool stats drop: 0 Mapping stats drop: 0
```

```
Port block alloc fail: 0
```

```
IP alias add fail: 0
```

```
Limit entry add fail: 0
```

```
NAT-Router#
```

Dopo aver utilizzato il comando `ping 172.16.11.7` sul router 4, le statistiche NAT sul router 6 sono le seguenti:

```
<#root>
```

```
Router4#
```

```
ping 172.16.11.7
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router4#
```

```
NAT-Router#
```

```
show ip nat statistics
```

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  GigabitEthernet1, GigabitEthernet2
Inside interfaces:
  GigabitEthernet3

Hits: 4

Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 7 pool test refcount 0
  pool test: id 1, netmask 255.255.255.0
    start 172.16.11.70 end 172.16.11.71
    type generic, total addresses 2, allocated 0 (0%), misses 0
nat-limit statistics:
  max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0 Out-to-in drops: 0
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT-Router#
```

Dai comandi show è possibile verificare il numero di accessi incrementato. Se il ping viene eseguito correttamente da un router Cisco, il numero di accessi aumenta di dieci. Vengono tradotti gli echi Internet Control Message Protocol (ICMP) inviati dal router di origine (router 4) e anche i pacchetti di risposta echo dal router di destinazione (router 7) devono essere tradotti, per un totale di dieci accessi. La perdita di cinque accessi è causata dalla mancata traduzione delle risposte echo o dal mancato invio delle risposte dal router 7.

Quindi, cercare di individuare il motivo per cui il router 7 non invierebbe i pacchetti di risposta echo al router 4. In questo momento, sono stati fatti i passi successivi:

- Il router 4 invia pacchetti echo ICMP con indirizzo di origine 10.10.10.4 e indirizzo di destinazione 172.16.11.7.
- Dopo l'esecuzione del NAT, il pacchetto ricevuto dal router 7 ha un indirizzo di origine 172.16.6.14 e un indirizzo di destinazione 172.16.11.7.
- Il router 7 deve rispondere alla versione 172.16.6.14 e, poiché la versione 172.16.6.14 non è collegata direttamente al router 7, per rispondere ha bisogno di un percorso per questa rete.



Nota: un'altra opzione per verificare se i pacchetti raggiungono il router di destinazione è usare un Embedded Packet Capture (EPC) o un pacchetto debug ip icmp/debug ip con un elenco di accesso (ACL).

A questo punto, è necessario controllare la tabella di routing del router 7 per verificare se esiste un percorso verso la versione 172.16.6.14:

```
<#root>
```

```
Router7#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP  
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR
& - replicated local route overrides by connected

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.11.0/24 is directly connected, GigabitEthernet1
L      172.16.11.7/32 is directly connected, GigabitEthernet1
Router7#
```

Dall'output precedente, è possibile notare che il router 7 non ha un percorso per la subnet 172.16.6.14 nella relativa tabella di routing. Dopo aver corretto questa condizione e aver aggiunto un percorso alla configurazione, il ping funziona. È utile monitorare le statistiche NAT con il comando show ip nat statistics. Tuttavia, in un ambiente NAT più complesso con diverse traduzioni, questo comando show non è più utile e occorre usare il debug sul router.

<#root>

Router7#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router7(config)#

ip route 172.16.6.0 255.255.255.0 172.16.11.6

Router7(config)#

end

Router7#

Router4#

ping 172.16.11.7

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Router4#

NAT-Router#

show ip nat statistics

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Outside interfaces:

GigabitEthernet1, GigabitEthernet2

Inside interfaces:

GigabitEthernet3

Hits: 9

Misses: 1

```
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 7 pool test refcount 0
  pool test: id 1, netmask 255.255.255.0
    start 172.16.11.70 end 172.16.11.71
    type generic, total addresses 2, allocated 0 (0%), misses 0
nat-limit statistics:
  max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0 Out-to-in drops: 0
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT-Router#
```

i dispositivi di rete esterni non possono comunicare con i router interni

Per risolvere questo problema, il router 4 può eseguire il ping tra il router 5 e il router 7, ma i dispositivi della rete 10.10.50.0 non possono comunicare con il router 5 o il router 7.

```
<#root>
```

```
Router4#
```

```
ping 172.16.11.7 source 10.10.50.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.10.50.4
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

```
Router4#
```

```
ping 172.16.6.5 source 10.10.50.4
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:
```

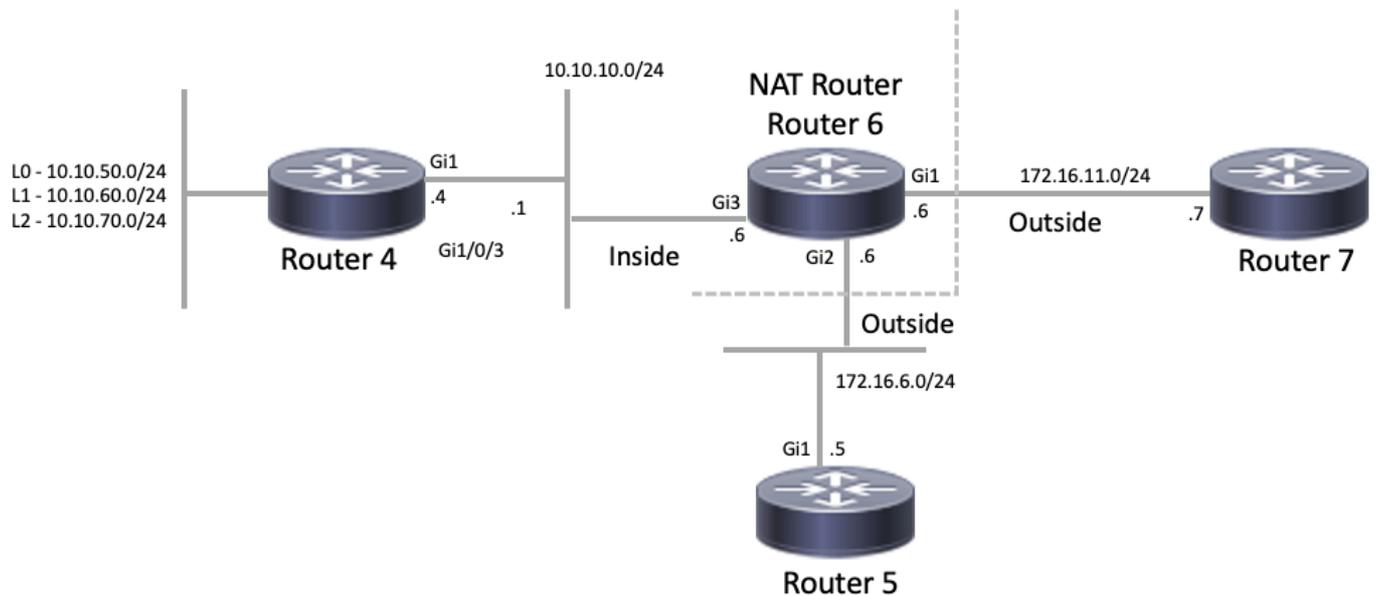
```
Packet sent with a source address of 10.10.50.4
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

```
Router4#
```

Il diagramma di rete per questo problema rimane lo stesso:



Topologia NAT

<#root>

```
interface GigabitEthernet1
ip address 172.16.11.6 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
!
```

```
interface GigabitEthernet2
ip address 172.16.6.6 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
!
```

```
interface GigabitEthernet3
ip address 10.10.10.6 255.255.255.0
ip nat inside
negotiation auto
no mop enabled
no mop sysid
!
```

```
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source static 10.10.10.4 172.16.11.70
```

```
!
ip access-list standard 7
10 permit 10.10.50.4
20 permit 10.10.60.4
30 permit 10.10.70.4
```

Risoluzione dei problemi

Dalla configurazione del router 6, è possibile osservare che NAT deve convertire dinamicamente 10.10.50.4 nel primo indirizzo disponibile nel pool NAT chiamato test. Il pool è costituito dagli indirizzi 172.16.11.70 e 172.16.11.71. Da questo problema, è possibile capire che i pacchetti ricevuti dai router 5 e 7 hanno un indirizzo di origine 172.16.11.70 o 172.16.11.71. Questi indirizzi si trovano sulla stessa subnet del router 7, quindi il router 7 deve avere un percorso connesso direttamente a questa subnet. Se tuttavia non ne ha già uno, il router 5 deve avere un percorso alla subnet.

Per verificare se la tabella di routing del Router 5 contiene l'indirizzo 172.16.11.0, usare il comando show ip route:

```
<#root>
```

```
Router5#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
       172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.6.0/24 is directly connected, GigabitEthernet1
L       172.16.6.5/32 is directly connected, GigabitEthernet1
S 172.16.11.0/24 [1/0] via 172.16.6.6
```

Usare il comando show ip route per verificare che la tabella di routing del Router 7 contenga l'indirizzo 172.16.11.0 come subnet connessa direttamente:

```
<#root>
```

```
Router7#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
```

- o - ODR, P - periodic downloaded static route, l - LISP
- a - application route
- + - replicated route, % - next hop override, p - overrides from PFR
- & - replicated local route overrides by connected

Gateway of last resort is not set

```

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S      172.16.6.0/24 [1/0] via 172.16.11.6
C 172.16.11.0/24 is directly connected, GigabitEthernet1
L      172.16.11.7/32 is directly connected, GigabitEthernet1

```

Controllare la tabella di conversione NAT e verificare che la traduzione prevista esista. Poiché la traduzione desiderata viene creata in modo dinamico, è innanzitutto necessario inviare il traffico IP proveniente dall'indirizzo appropriato. Dopo l'invio di un ping, inviato dalla versione 10.10.50.4 e destinato alla versione 172.16.11.7, la tabella di conversione nel router 6 (router NAT) mostra l'output successivo:

<#root>

NAT-Router#

show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.6.14	10.10.10.4	---	---

172.16.11.70 10.10.50.4

--- ---
Total number of translations: 2

Poiché la traduzione prevista si trova nella tabella di traduzione, si sa che i pacchetti echo ICMP sono tradotti correttamente. Un'opzione è che è possibile monitorare le statistiche NAT, ma che non è utile in un ambiente complesso. In alternativa, è possibile eseguire il debug della NAT sul router NAT (Router 6). è possibile eseguire il comando debug ip nat mentre si invia un ping da 10.10.50.4 destinato a 172.16.11.7. I risultati del debug sono riportati nel seguente esempio di codice:

 Nota: l'uso del comando debug su un router potrebbe sovraccaricarlo e renderlo inutilizzabile. procedere sempre con estrema cautela e, se possibile, cercare di ottenere l'assistenza di un TAC Cisco prima di eseguire il debug su un router di produzione critico.

<#root>

NAT-Router#

```
show logging
```

```
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 39 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 39 messages logged
  Trap logging: level informational, 33 message lines logged
```

```
Log Buffer (4096 bytes):
```

```
05:32:23: NAT: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [70]
05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70]
05:32:25: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71]
05:32:25: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [71]
05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72]
05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72]
05:32:29: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [73]
05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73]
05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74]
05:32:31: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [74]
```

```
Router7#show monitor capture cap buffer brief
```

```
-----
# size timestamp source destination dscp protocol
-----
0 114 0.000000 172.16.11.70 -> 172.16.11.7 0 BE ICMP
1 114 2.000000 172.16.11.70 -> 172.16.11.7 0 BE ICMP
2 114 4.000000 172.16.11.70 -> 172.16.11.7 0 BE ICMP
3 114 6.001999 172.16.11.70 -> 172.16.11.7 0 BE ICMP
4 114 8.001999 172.16.11.70 -> 172.16.11.7 0 BE ICMP
```

Come mostrato nell'output del debug precedente, la prima riga mostra l'indirizzo di origine 10.10.50.4 convertito in 172.16.11.70. La seconda riga mostra l'indirizzo di destinazione 172.16.11.70 che viene convertito nuovamente in 10.10.50.4. Questo modello viene ripetuto per il resto del debug. Ciò significa che il router NAT converte i pacchetti in entrambe le direzioni. Inoltre, dall'acquisizione dei pacchetti, è possibile notare che il router 7 riceve effettivamente i pacchetti ICMP con origine 172.16.11.70 e destinazione 172.16.11.7.

I passaggi successivi rappresentano un riepilogo dello stato corrente del problema:

1. Il router 4 invia un pacchetto proveniente dalla versione 10.10.50.4 e destinato alla versione 172.16.11.7 (o 172.16.6.5 a seconda della prova eseguita).
2. Il router NAT esegue una conversione NAT sul pacchetto e lo inoltra con un'origine 172.16.11.70 e una destinazione 172.16.11.7.
3. Il router 7 invia una risposta con origine 172.16.11.7 e destinazione 172.16.11.70.
4. Il router NAT (router 6) esegue il protocollo NAT sul pacchetto, dando luogo a un pacchetto con indirizzo di origine 172.16.11.7 e indirizzo di destinazione 10.10.50.4.

5. Il router NAT (router 6) instrada il pacchetto alla versione 10.10.50.4 in base alle informazioni contenute nella tabella di routing.

A questo punto, è necessario usare i comandi show ip route e show ip cef per verificare che il router NAT (router 6) abbia i percorsi necessari nella relativa tabella di routing.

```
<#root>
```

```
NAT-Router#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
        n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        H - NHRP, G - NHRP registered, g - NHRP registration summary
        o - ODR, P - periodic downloaded static route, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PfR
        & - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.10.10.0/24 is directly connected, GigabitEthernet3
L    10.10.10.6/32 is directly connected, GigabitEthernet3
172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.16.6.0/24 is directly connected, GigabitEthernet2
L    172.16.6.6/32 is directly connected, GigabitEthernet2
L    172.16.6.14/32 is directly connected, GigabitEthernet2
C    172.16.11.0/24 is directly connected, GigabitEthernet1
L    172.16.11.6/32 is directly connected, GigabitEthernet1
L    172.16.11.70/32 is directly connected, GigabitEthernet1
```

```
NAT-Router#
```

```
show ip route 10.10.50.4
```

```
% Subnet not in table
```

```
NAT-Router#
```

```
show ip cef 10.10.50.4
```

```
0.0.0.0/0
```

```
no route
```

```
NAT-Router#
```

Dopo aver aggiunto il percorso mancante nel router NAT, il ping ha esito positivo:

```
<#root>
```

```
NAT-Router#
```

```
configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
NAT-Router(config)#
```

```
ip route 10.10.50.4 255.255.255.255 10.10.10.4
```

```
NAT-Router(config)#end
```

```
NAT-Router#
```

```
Router4#
```

```
ping 172.16.11.7 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

Packet sent with a source address of 10.10.50.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

```
Router4#
```

```
ping 172.16.6.5 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:

Packet sent with a source address of 10.10.50.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```
Router4#
```

Elenco di controllo per problemi comuni

Utilizzare questo elenco di controllo per la risoluzione dei problemi più comuni.

La conversione non è installata nella tabella delle conversioni

Se la traduzione appropriata non è installata nella tabella di traduzione, verificare quanto segue:

1. La configurazione sia corretta. È difficile ottenere NAT per ottenere quello che si desidera a volte. Per alcune informazioni della Guida sulla configurazione, fare riferimento a [Configurazione di Network Address Translation](#).
2. Non ci sono elenchi degli accessi in entrata che negano l'ingresso dei pacchetti dal router NAT.
3. Il router NAT ha il percorso appropriato nella tabella di routing se il pacchetto va dall'interno all'esterno. Per ulteriori informazioni, fare riferimento a Ordini delle operazioni NAT.
4. L'elenco degli accessi a cui fa riferimento il comando NAT autorizzi tutte le reti necessarie.
5. Gli indirizzi del pool NAT siano sufficienti. Questo può essere un problema solo se NAT non è configurato per la congestione.
6. Le interfacce del router siano adeguatamente definite come NAT interna o NAT esterna.
7. Per la traduzione del payload dei pacchetti DNS (Domain Name System), verificare che la traduzione avvenga sull'indirizzo nell'intestazione IP del pacchetto. Se ciò non accade, il processo NAT non esamina il payload del pacchetto.

La voce di traduzione corretta non è utilizzata

Se la voce di traduzione corretta è installata nella tabella di traduzione ma non viene utilizzata, verificare quanto segue:

1. Verificare che non vi siano elenchi degli accessi in entrata che negano l'ingresso dei pacchetti dal router NAT.
2. Per i pacchetti che vanno dall'interno all'esterno, verificare che vi sia un percorso verso la destinazione, poiché questo viene controllato prima della traduzione. Per ulteriori informazioni, fare riferimento a Ordini delle operazioni NAT.

NAT funziona correttamente ma vi sono ancora problemi di connettività

Risolvere il problema di connettività:

1. Verificare la connettività sul Layer 2.
2. Verificare le informazioni di indirizzamento del Layer 3.
3. Cercare i filtri pacchetti che causano il problema.

"%Nsistema AT Occupato - Riprova Più Tardi"

Il messaggio di errore try later (prova più tardi) viene visualizzato quando viene eseguito un comando show relativo a NAT o un comando show running-config o write memory. Ciò è causato dall'aumento delle dimensioni della tabella NAT, che esaurisce la memoria del router.

1. Ricaricare il router per risolvere il problema.
2. Questo errore si verifica in genere nelle piattaforme legacy. Si consiglia di mantenere aggiornato il software del dispositivo.

Una tabella di conversione grande aumenta l'utilizzo della CPU

Un host può inviare centinaia di traduzioni, che provocano un elevato utilizzo della CPU. In altre parole, la tabella può diventare così grande da utilizzare il 100% della CPU. Il comando ip nat translation max-entries 300 crea il limite di 300 per host o un limite aggregato della quantità di traduzioni sul router. Come soluzione alternativa, usare il comando ip nat translation max-entries all-hosts 300.

La tabella ARP è vuota

Questo è il risultato dell'`no-alias` opzione sulle voci NAT. L'`no-alias` opzione indica che il router non risponde per gli indirizzi e non installa una voce ARP. Se un altro router utilizza un pool NAT come pool globale interno costituito da indirizzi su una subnet collegata, viene generato un alias per tale indirizzo in modo che il router possa rispondere alle richieste Address Resolution Protocol (ARP) per tali indirizzi. In questo modo il router dispone di voci ARP per gli indirizzi falsi.

Informazioni correlate

- [Domande frequenti \(FAQ\) sul Network Address Translation \(NAT\)](#)
- [Supporto e download - Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).