

# uso del NAT nelle reti sovrapposte

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene illustrato come utilizzare Network Address Translation (NAT) per reti sovrapposte. La sovrapposizione delle reti si verifica quando si assegna un indirizzo IP a un dispositivo della rete che è già legalmente di proprietà e assegnato a un dispositivo diverso in Internet o in una rete esterna. Una rete sovrapposta si può formare anche in occasione di una fusione tra aziende, se entrambe usano indirizzi IP a norma [RFC 1918](#). Le due reti devono comunicare tra loro, possibilmente senza dover reindirizzare tutti i dispositivi.

## [Prerequisiti](#)

### [Requisiti](#)

Una conoscenza di base di indirizzamento IP, routing IP e DNS (Domain Name System) è utile per comprendere i contenuti di questo documento.

### [Componenti usati](#)

Il supporto per NAT è iniziato nella versione 11.2 del software Cisco IOS®. Per ulteriori informazioni sul supporto della piattaforma, vedere [Domande frequenti su NAT](#).

### [Convenzioni](#)

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

## Configurazione

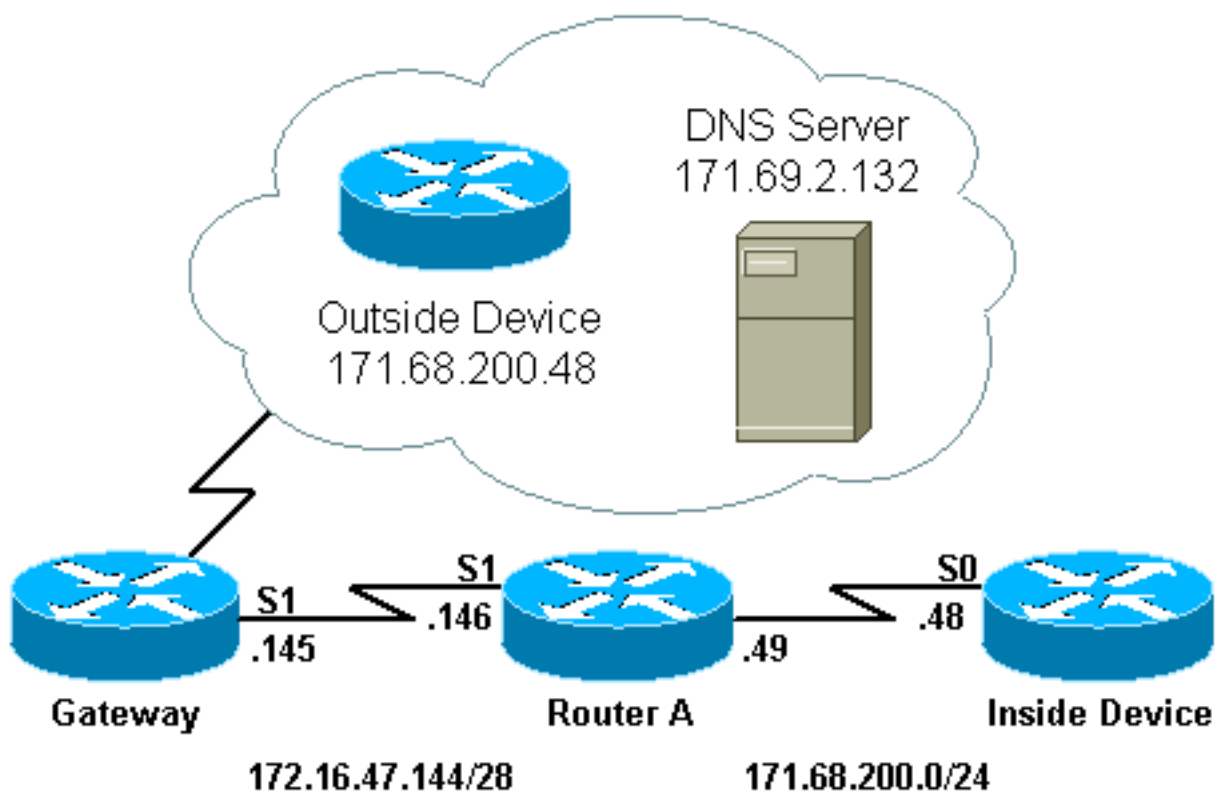
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

## Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.

Si noti che il dispositivo interno ha lo stesso indirizzo IP del dispositivo esterno con cui desidera comunicare.



## Configurazioni

Il router A è configurato per NAT in modo da convertire il dispositivo interno in un indirizzo del pool "test-loop" e il dispositivo esterno in un indirizzo del pool "test-dns". Per una spiegazione di come questa configurazione facilita la sovrapposizione, vedere la tabella di configurazione riportata di seguito.

Router A
<pre>! version 11.2 no service udp-small-servers no service tcp-small-servers ! hostname Router-A</pre>

```

!
!
ip domain-name cisco.com
ip name-server 171.69.2.132
!
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 nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
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

```

Affinché la configurazione indicata in precedenza consenta di evitare la sovrapposizione quando il dispositivo interno comunica con il dispositivo esterno, è necessario che utilizzi il nome di dominio del dispositivo esterno.

Il dispositivo interno non può utilizzare l'indirizzo IP del dispositivo esterno perché è uguale all'indirizzo assegnato a se stesso (il dispositivo interno). Pertanto, il dispositivo interno invierà una query DNS per il nome di dominio del dispositivo esterno. L'indirizzo IP del dispositivo interno sarà l'origine di questa query e verrà convertito in un indirizzo del pool "test-loop" perché il comando **ip nat inside source list** è configurato.

Il server DNS risponde all'indirizzo proveniente dal pool "test-loop" con l'indirizzo IP associato al nome di dominio del dispositivo esterno nel payload del pacchetto. L'indirizzo di destinazione del pacchetto di risposta viene riconvertito nell'indirizzo del dispositivo interno e l'indirizzo nel payload del pacchetto di risposta viene quindi convertito in un indirizzo dal pool "test-dns" a causa del comando **ip nat outside source list**. Pertanto, il dispositivo interno viene a sapere che l'indirizzo IP

del dispositivo esterno è uno degli indirizzi del pool "test-dns" e utilizzerà tale indirizzo per comunicare con il dispositivo esterno. A questo punto, il router con NAT si occupa delle traduzioni.

Questo processo è illustrato in dettaglio nella sezione [Risoluzione dei problemi](#). I dispositivi che utilizzano indirizzi sovrapposti possono comunicare tra loro senza utilizzare il DNS, ma in questo caso è necessario configurare il protocollo NAT statico. Di seguito è riportato un esempio di come ciò possa essere fatto.

## Router A

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname Router-A  
!  
!  
  
ip domain-name cisco.com  
ip name-server 171.69.2.132  
!  
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 nat pool test-loop 172.16.47.161 172.16.47.165  
prefix-length 28  
ip nat inside source list 7 pool test-loop  
ip nat outside source static 171.68.200.48 172.16.47.177  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.16.47.145  
ip route 172.16.47.160 255.255.255.240 Serial0  
!--- This line is necessary to make NAT work for return  
traffic. !--- The router needs to have a route for the  
pool to the inside !--- NAT interface so it knows that a  
translation is needed. 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
```

Con la configurazione precedente, quando il dispositivo interno desidera comunicare con il dispositivo esterno, può ora utilizzare l'indirizzo IP 172.16.47.177 e DNS non necessario. Come mostrato sopra, la traduzione dell'indirizzo del dispositivo interno viene ancora eseguita in modo dinamico, il che significa che il router deve ricevere i pacchetti dal dispositivo interno prima che venga creata una traduzione. Per questo motivo, il dispositivo interno deve avviare tutte le connessioni affinché il dispositivo interno e quello esterno possano comunicare. Se è necessario che il dispositivo esterno avvii le connessioni con il dispositivo interno, anche l'indirizzo del dispositivo interno deve essere configurato staticamente.

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Il processo con cui il dispositivo interno ha utilizzato il DNS per comunicare con il dispositivo esterno, come descritto in precedenza, può essere visualizzato in dettaglio con il seguente processo di risoluzione dei problemi.

Al momento non sono disponibili traduzioni nella tabella di traduzione per il comando **show ip nat translation**. Negli esempi seguenti vengono invece utilizzati i comandi **debug ip packet** e **debug ip nat**.

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

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

Quando il dispositivo interno invia la query DNS al server DNS, che risiede all'esterno del dominio NAT, l'indirizzo di origine della query DNS (l'indirizzo del dispositivo interno) viene convertito a causa dei comandi **ip nat inside**. Questa condizione può essere rilevata nell'output del comando **debug** riportato di seguito.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]  
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward  
  UDP src=6988, dst=53
```

Quando il server DNS invia una risposta DNS, il payload della risposta DNS viene tradotto a causa dei comandi **esterni ip nat**.

**Nota:** NAT non controlla il payload della risposta DNS a meno che non si verifichi una conversione nell'intestazione IP del pacchetto di risposta. Vedere il comando `ip nat outside source list 7 pool` nella configurazione del router descritta sopra.

Il primo messaggio NAT nell'output di debug seguente mostra che il router riconosce la risposta DNS e converte l'indirizzo IP all'interno del payload in 172.16.47.177. Il secondo messaggio NAT mostra il router che traduce la destinazione della risposta DNS in modo che possa inoltrare una risposta al dispositivo interno che ha eseguito la query DNS iniziale. La parte di destinazione dell'intestazione, l'indirizzo globale interno, viene convertita nell'indirizzo locale interno.

Il payload della risposta DNS è tradotto:

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

La parte di destinazione dell'intestazione IP nel pacchetto di risposta DNS viene convertita:

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=6988
```

Esaminiamo un'altra query DNS e rispondiamo:

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```

Ora che il payload del DNS è stato tradotto, la nostra tabella di traduzione ha una voce per gli indirizzi locali e globali esterni del dispositivo esterno. Con queste voci nella tabella, ora possiamo tradurre completamente l'intestazione dei pacchetti ICMP scambiati tra il dispositivo interno e il dispositivo esterno. Esaminiamo questo scambio nell'output del comando debug.

L'output seguente mostra l'indirizzo di origine (all'interno dell'indirizzo del dispositivo) da tradurre.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
```

Qui viene tradotto l'indirizzo di destinazione (indirizzo esterno locale del dispositivo).

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
```

Dopo la traduzione, il pacchetto IP ha il seguente aspetto:

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

L'output seguente mostra l'indirizzo di origine (indirizzo del dispositivo esterno) tradotto sul pacchetto restituito.

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
```

A questo punto, viene tradotto l'indirizzo di destinazione (indirizzo globale del dispositivo) del pacchetto restituito.

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
```

Dopo la traduzione, il pacchetto restituito avrà il seguente aspetto:

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0
```

Lo scambio di pacchetti continua tra il dispositivo interno e il dispositivo esterno.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]  
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]  
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]  
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]  
IP: s=172.16.47.177 (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=172.16.47.177 [408]  
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]  
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]  
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]  
IP: s=172.16.47.177 (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=172.16.47.177 [409]  
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]  
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]  
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]  
IP: s=172.16.47.177 (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=172.16.47.177 [410]  
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]  
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward  
ICMP type=8, code=0  
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]  
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]  
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward  
ICMP type=0, code=0
```

Una volta completato lo scambio di pacchetti tra l'esterno e l'interno, possiamo vedere la tabella di traduzione, che ha tre voci. La prima voce è stata creata quando il dispositivo interno ha inviato una query DNS. La seconda voce è stata creata durante la conversione del payload della risposta DNS. La terza voce è stata creata quando il ping è stato scambiato tra il dispositivo interno e il dispositivo esterno. La terza voce è un riepilogo delle prime due voci e viene utilizzata per traduzioni più efficienti.

```
Router-A# show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.47.161	171.68.200.48	---	---
---	---	---	172.16.47.177	171.68.200.48
---	172.16.47.161	171.68.200.48	172.16.47.177	171.68.200.48

È importante notare che quando si cerca di stabilire una connettività tra due reti sovrapposte eseguendo un NAT dinamico su un singolo router Cisco, è necessario utilizzare il DNS per creare una traduzione globale da locale a esterno. Se non si utilizza il DNS, la connettività può essere stabilita con NAT statico, ma è più difficile da gestire.

## Informazioni correlate

- [Pagina di supporto NAT](#)
- [Supporto tecnico – Cisco Systems](#)