

Verifica e risoluzione dei problemi relativi alle operazioni NAT di base

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Problema](#)

[Possibilità di eseguire il ping su un router ma non su un altro](#)

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

[Elenco di controllo per problemi comuni](#)

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

In questo documento vengono descritti i seguenti problemi:

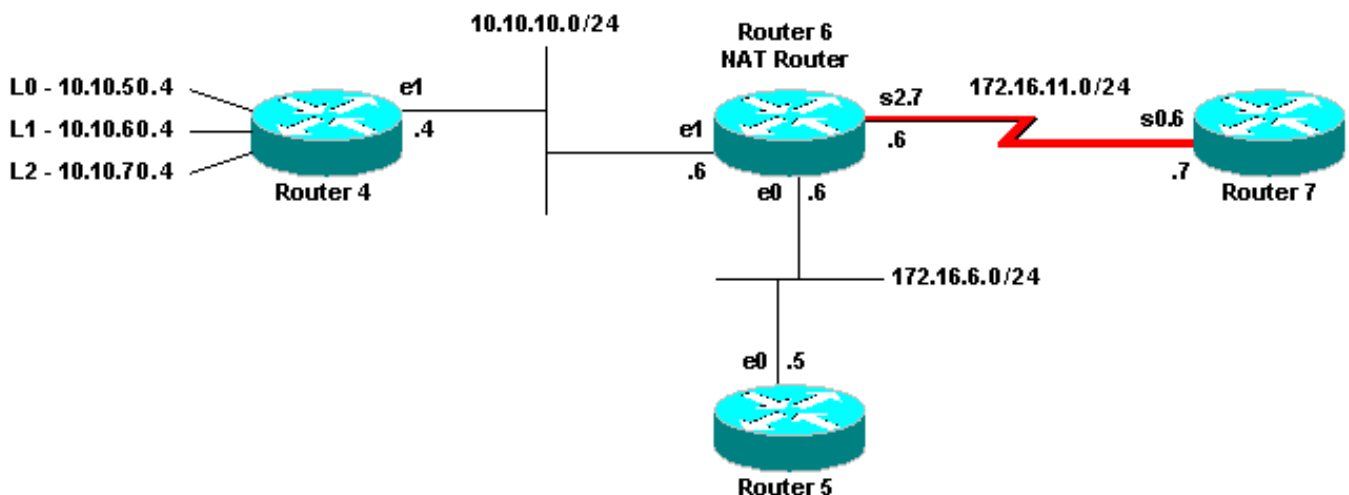
- Possibilità di eseguire il ping su un router ma non su un altro
- i dispositivi di rete esterni non possono comunicare con i router interni

Per determinare se il problema si verifica nelle operazioni NAT:

1. In base alla configurazione, definire chiaramente cosa NAT deve ottenere. È possibile stabilire se si è verificato un problema con la configurazione. Per informazioni sulla configurazione NAT, vedere [Configurazione di Network Address Translation: Per iniziare.](#)
2. Verificare che nella tabella delle conversioni siano presenti le conversioni 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 spostare il pacchetto.

- Possibilità di eseguire il ping su un router ma non su un altro

Nel diagramma di rete seguente il router 4 può eseguire il ping tra il router 5 (172.16.6.5) e il router 7 (172.16.11.7):



Il router 4 non può eseguire il ping tra il router 7

I protocolli di routing non eseguono i router. Il gateway predefinito del router 4 è il router 6. Il router 6 è configurato con NAT:

```
interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside !
interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside ! interface Serial2.7
point-to-point ip address 172.16.11.6 255.255.255.0 ip nat outside frame-relay interface-dlci
101 ! ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source list 7
pool test ip nat inside source static 10.10.10.4 172.16.6.14 ! access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4 access-list 7 permit 10.10.70.4
```

Per risolvere i problemi:

1. È necessario verificare che NAT funzioni correttamente. Dalla configurazione, l'indirizzo IP del router 4 (10.10.10.4) è stato convertito in modo statico nella versione 172.16.6.14. È possibile usare il comando **show ip nat translation** sul router 6 per verificare che la conversione esista nella tabella di conversione:

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global ---
172.16.6.14 10.10.10.4 --- ---
```

2. Verificare che questa conversione venga eseguita quando il router 4 genera traffico IP. A tale

scopo, è possibile usare il router 6, eseguire il **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. Monitorare il contatore per assicurarsi che aumenti man mano che riceve il traffico dal router 4. Il contatore aumenta 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.

```
router-6#clear ip nat statistics router-6# router-6# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces: Ethernet0, Serial2.7
Inside interfaces: Ethernet1
Hits: 0 Misses: 0 Expired translations: 0
Dynamic mappings: --
Inside Source access-list 7 pool test refcount 0 pool test: 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
router-6#
```

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

```
router-6#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces: Ethernet0, Serial2.7
Inside interfaces: Ethernet1
Hits: 5 Misses: 0 Expired translations: 0
Dynamic mappings: --
Inside Source access-list 7 pool test refcount 0 pool test: 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
```

Il comando **show** mostra che il numero di accessi è aumentato di cinque. Se il **ping** viene eseguito correttamente da un router Cisco, il numero di accessi aumenta di dieci. I cinque echi ICMP (Internet Control Message Protocol) inviati dal router di origine (router 4) vengono tradotti, e le cinque risposte echo ai pacchetti provenienti dal router di destinazione (router 7) devono essere tradotte, 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.

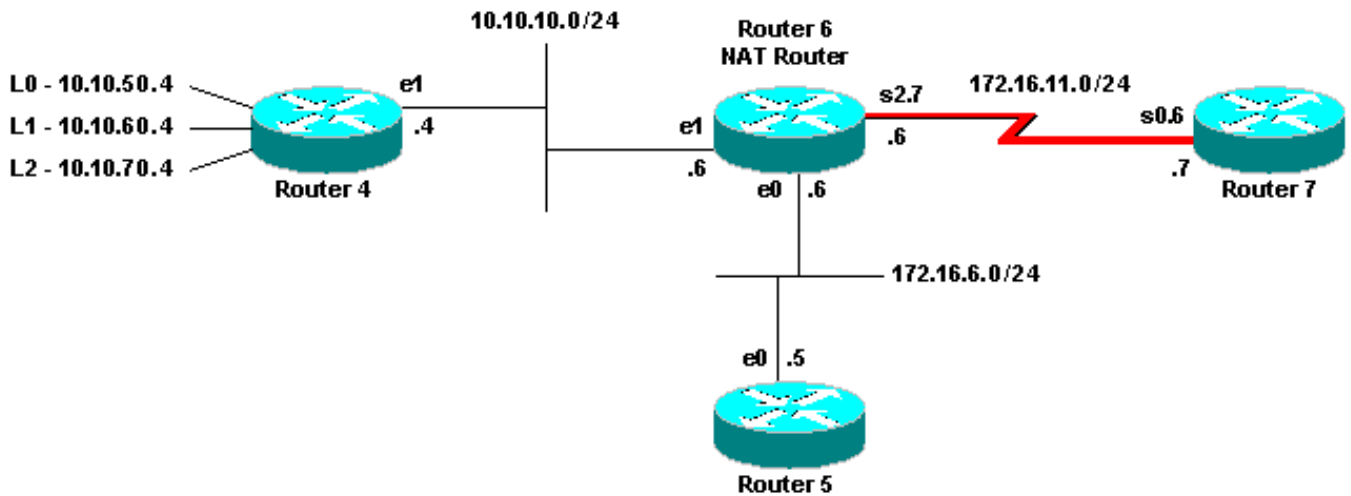
Verificare se è possibile trovare un motivo per cui il router 7 non invierebbe pacchetti di risposta echo al router 4. È possibile esaminare le funzionalità di NAT sul pacchetto. Il router 4 invia pacchetti echo ICMP con indirizzo di origine 10.10.10.4 e indirizzo di destinazione 172.16.11.7. Dopo l'esecuzione del NAT, il pacchetto ricevuto dal router 7 ha indirizzo di origine 172.16.6.14 e indirizzo di destinazione 172.16.11.7. Il router 7 deve rispondere a 172.16.6.14 e, poiché 172.16.6.14 non è connesso direttamente a router 7, è necessario un percorso per questa rete per rispondere. Controllare la tabella di routing del Router 7 per verificare che questa route sia presente.

```
router-7#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 4 subnets
C 172.16.12.0 is directly connected, Serial0.8
C 172.16.9.0 is directly connected, Serial0.5
C 172.16.11.0 is directly connected, Serial0.6
C 172.16.5.0 is directly connected, Ethernet0
```

È possibile notare che la tabella di routing del router 7 non ha un percorso per 172.16.6.14. Una volta aggiunta questa route, il ping funziona. È utile monitorare le statistiche NAT con il comando **show ip nat statistics**. In un ambiente NAT più complesso con diverse traduzioni, questo comando **show** non è più utile. È quindi possibile eseguire i **debug** sul router.

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

Con il problema, il router 4 può eseguire il ping sia sul router 5 che sul router 7, ma i dispositivi della rete 10.10.50.0 non possono comunicare con il router 5 o il router 7. Lo schema della rete è:



La rete non può comunicare con il router

```
interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside
media-type 10BaseT ! interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside
media-type 10BaseT ! interface Serial2.7 point-to-point ip address 172.16.11.6 255.255.255.0 ip
nat outside frame-relay interface-dlci 101 ! ip nat pool test 172.16.11.70 172.16.11.71 prefix-
length 24 ip nat inside source list 7 pool test ip nat inside source static 10.10.10.4
172.16.6.14 ! access-list 7 permit 10.10.50.4 access-list 7 permit 10.10.60.4 access-list 7
permit 10.10.70.4
```

Indicare il comportamento previsto di NAT. Dalla configurazione del router 6, si sa che NAT deve convertire dinamicamente 10.10.50.4 al primo indirizzo disponibile nel pool NAT "test". Il pool è composto dagli indirizzi 172.16.11.70 e 172.16.11.71. Da questo problema, si può 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 una route connessa direttamente; se non ne ha già una, il router 5 deve avere una route 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:

```
router-5#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.9.0 is directly connected, Serial1 S
172.16.11.0 [1/0] via 172.16.6.6 C 172.16.6.0 is directly connected, Ethernet0 C 172.16.2.0 is
directly connected, Serial0
```

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:

```
router-6#show ip nat translation 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 --- ---
```

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 un **ping** inviato, originato dalla versione 10.10.50.4 e destinato alla versione 172.16.11.7, la tabella di conversione nel router 6 mostra:

```
router-6#show ip nat translation 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 --- ---
```

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** sul router 6 mentre si invia un **ping** inviato dalla versione 10.10.50.4 e destinato alla versione 172.16.11.7. I risultati del **debug** sono riportati nel seguente esempio di codice.

Nota: Quando si usa un comando **debug** su un router, è possibile sovraccaricare il router e renderlo inutilizzabile. procedere sempre con estrema cautela e, se possibile, non eseguire mai il **debug** su un router di produzione critico senza la supervisione di un tecnico del supporto tecnico Cisco.

:

```
router-6# show log 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]
```

Come si può vedere dall'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 convertito nuovamente in 10.10.50.4. Questo modello viene ripetuto per tutto il resto del **debug**. Ciò significa che il router 6 converte i pacchetti in entrambe le direzioni.

Revisione:

1. Il router 4 invia un pacchetto proveniente dalla versione 10.10.50.4 destinato alla versione 172.16.11.7.
2. Il router 6 esegue il NAT sul pacchetto e inoltra un pacchetto con origine 172.16.11.70 e 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 6 esegue il 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 6 instrada il pacchetto alla versione 10.10.50.4 in base alle informazioni contenute nella tabella di routing del router 6. Per controllare se il Router 6 ha la route necessaria nella sua tabella di routing, usare il comando `show ip route`.

```
router-6#show ip route Codes: C - connected, S - static, I - IGRP, 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, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.8.0 is directly connected, Serial1 C
172.16.10.0 is directly connected, Serial2.8 C 172.16.11.0 is directly connected, Serial2.7 C
172.16.6.0 is directly connected, Ethernet0 C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets C 10.10.10.0 is directly connected, Ethernet1
```

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 informazioni sulla configurazione, fare riferimento a Configurazione di Network Address Translation: [Per iniziare](#).
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 è 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, controllare:

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.

- **La NAT funziona correttamente, ma i problemi di connettività rimangono**

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.

- **La conversione NAT sulla porta 80 non funziona**

Ciò significa che la traduzione NAT per la porta 80 non funziona, ma la traduzione per altre porte funziona normalmente.

Per risolvere il problema:

1. Eseguire i comandi **debug ip nat translation** e **debug ip packet** per verificare che le traduzioni siano corrette e che la voce di traduzione corretta sia installata nella tabella di traduzione.
2. Verificare che il server risponda.
3. Disabilitare il server HTTP.
4. Cancellare le tabelle NAT e ARP.

- **%NAT: System busy. Try later**

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. Se il messaggio di errore viene visualizzato quando è configurata la funzionalità HSRP SNAT, configurare questi comandi per risolvere il problema: Router(config)#standby delay minimum 20 - Ricaricamento 20 Router(config)#standby 2 ritardo anticipato minimo 20 ricaricamento 20 sincronizzazione 10

- **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**.

- **% Public ip-address already mapped (Internal ip-address -> Public ip-address)**

Questo messaggio viene visualizzato quando si cerca di configurare due indirizzi IP interni in modo che un indirizzo IP pubblico sia in ascolto sulle stesse porte.

```
% X.X.X.X already mapped (172.30.62.101 -> X.X.X.X)
```

Per risolvere questo problema, configurare l'indirizzo IP pubblico in modo che abbia due indirizzi IP interni e utilizzare due indirizzi IP pubblici nel DNS.

- **La tabella ARP è vuota**

Questo è il risultato della `no-alias` sulle voci NAT. OSPF (Open Shortest Path First) `no-alias` indica che il router non risponde agli 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.

- **Bad token 0, wanted TOK_NUMBER|TOK_PUNCT**

Il messaggio di errore Bad token 0, wanted TOK_NUMBER|TOK_PUNCT (Token corrotto 0, token desiderato TOK_NUMBER|TOK_PUNCT) è solo un messaggio informativo e non ha alcun impatto sul normale comportamento del dispositivo.

Bad token 0, wanted TOK_NUMBER|TOK_PUNCT

L'errore indica che NAT tenta di correggere l'indirizzo di un FTP di layer 4 e non riesce a trovare gli indirizzi IP che deve tradurre nel pacchetto. Il motivo per cui il messaggio include i token è che gli indirizzi IP nel pacchetto vengono trovati dalla ricerca di un token, o di un set di simboli, nel pacchetto IP, per trovare i dettagli da tradurre.

All'inizio di una sessione, il client e il server FTP concordano sull'uso di due canali, un canale di controllo e un canale dati. Questi sono entrambi indirizzi IP con numeri di porta diversi. Il client e il server FTP negoziano un secondo canale dati in cui trasferire i file. Il pacchetto scambiato tramite il canale di controllo ha il formato "PORT,i,i,i,i,p,p", dove i,i,i,i sono i quattro byte di un indirizzo IP e p,p specifica la porta. NAT cerca di trovare la corrispondenza con questo schema e di tradurre indirizzo/porta, se necessario. NAT deve tradurre entrambi gli schemi di canale. Analizza quindi i numeri nel flusso dei comandi finché non ritiene di aver trovato un comando di porta da convertire. Quindi analizza la traduzione, che calcola con lo stesso formato.

Se il pacchetto è danneggiato o i comandi del server o del client FTP non sono corretti, NAT non è in grado di calcolare correttamente la conversione e l'errore viene generato. È possibile impostare il client FTP su "passivo" in modo che avvii entrambi i canali.

Informazioni correlate

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