

Risoluzione dei problemi relativi a NAT sulle piattaforme Cat800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Caso aziendale: Esaurimento NAT \(pool esaurito\)](#)

[Possibile causa](#)

[Caso aziendale: NAT - Traduzione di indirizzi IP non nativi \(problema gatekeeper\)](#)

Introduzione

Questo documento descrive come risolvere i problemi NAT sulle piattaforme Cat800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- NAT (Network Address Translations)
- Cisco IOS XE

Per ulteriori informazioni su questi argomenti, vedere:

[Configurazione di Network Address Translation](#)

[Comprendere l'ordine di funzionamento NAT](#)

[Domande frequenti su Network Address Translation \(NAT\)](#)

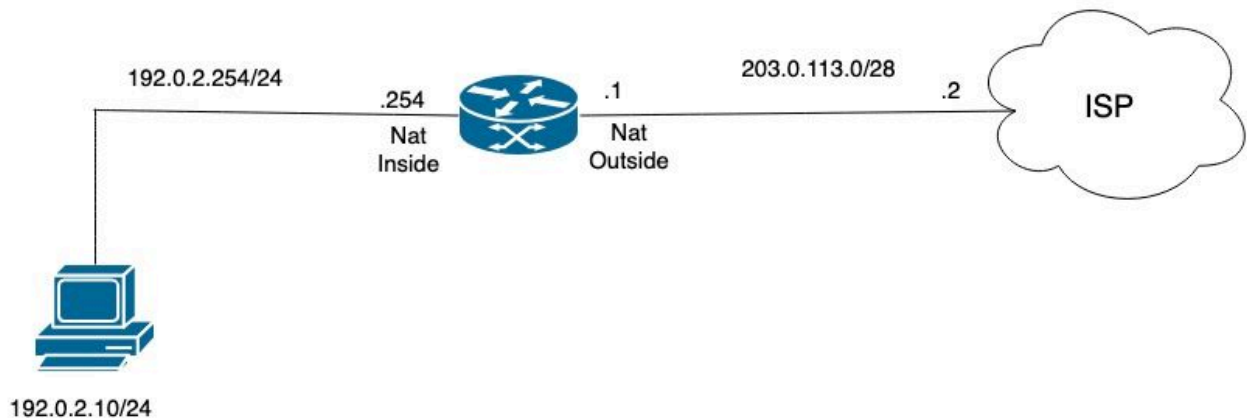
[Restrizioni per la configurazione di NAT per la conservazione degli indirizzi IP](#)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco IOS XE.

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



Topologia NAT

Caso aziendale: Esaurimento NAT (pool esaurito)

Questo messaggio di registro indica che il dispositivo ha tentato di allocare un indirizzo IP per NAT, ad esempio per una conversione NAT o PAT dinamica, ma l'allocazione non è riuscita. Questo si verifica in genere quando non vi sono indirizzi o porte disponibili rimanenti nel pool NAT configurato.

Le cause più comuni sono:

- Pool NAT esaurito (tutte le porte o gli indirizzi IP disponibili sono in uso).
- La configurazione NAT non dispone di indirizzi o risorse sufficienti per soddisfare le richieste di

traduzione correnti.

```
%NAT-6-ADDR_ALLOC_FAILURE: Address allocation failed; pool 2 may be exhausted [2] port range: NA, non-P
created by pkt: src_ip 192.0.2.13 dst_ip 192.x.x.40 src_port 0 dst_port 0 proto 1
```

Verificare il pool NAT per confermare l'intervallo di conversione degli indirizzi.

```
<#root>
```

```
NAT_R1#
```

```
show ip nat pool platform
```

```
Dump NAT pool config
```

```
ID: 2, Name: NAT_Pool, Type: Generic, Mask: 255.255.255.240
Flags: Unknown, Acct name:
Address range blocks: 1
```

```
Start: 203.0.113.3, End: 203.0.113.5
```

```
Last stats update: 07/31 13:08:43.708061785
```

```
Last refcount value: 3
```

Verificare la tabella di traduzione NAT e determinare il numero di traduzioni attive attualmente presenti.

```
<#root>
```

```
NAT_R1#
```

```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
--- 203.0.113.3 192.0.2.10 --- ---
--- 203.0.113.5 192.0.2.12 --- ---
--- 203.0.113.4 192.0.2.11 --- ---
icmp 203.0.113.5:0 192.0.2.12:0 198.51.100.30:0 198.51.100.30:0
icmp 203.0.113.3:0 192.0.2.10:0 198.51.100.10:0 198.51.100.10:0
icmp 203.0.113.4:0 192.0.2.11:0 198.51.100.20:0 198.51.100.20:0
```

```
Total number of translations: 6
```

Verificare se le gocce vengono visualizzate nelle statistiche NAT. Questo risultato indicherebbe che il traffico in entrata richiede la traduzione, ma si verificano cali a causa di problemi di allocazione NAT.

```
<#root>
```

```
NAT_R1#
```

```
show ip nat statistics
```

```
Total active translations: 6 (0 static, 6 dynamic; 3 extended)
```

```
Outside interfaces:
```

```
GigabitEthernet0/0/4
```

```
Inside interfaces:
```

```
GigabitEthernet0/0/3
```

```
Hits: 11094661606 Misses: 10
```

```
Reserved port setting disabled provisioned no
```

```
Expired translations: 1412
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 2] access-list 1 pool NAT_Pool
```

```
refcount 6
```

```
<---- Translations count
```

```
pool NAT_Pool: id 2, netmask 255.255.255.240
```

```
start 203.0.113.3 end 203.0.113.5
```

```
type generic, total addresses 3, allocated 3 (100%), misses 3559386331
```

```
nat-limit statistics:
```

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

```
In-to-out drops: 3559337007
```

```
Out-to-in drops: 0 <---- drops from in to out
```

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

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

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

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

```
NAT_R1#
```

Dal punto di vista della piattaforma, rivedere le statistiche NAT del datapath QFP per determinare se queste perdite corrispondono al problema osservato.

```
<#root>
```

```
NAT_R1#
```

```
show platform hardware qfp active feature nat datapath stats
```

Counter	Value
number_of_session	3
udp	0
tcp	0
icmp	3
non_extended	3
statics	0
static_net	0
entry_timeouts	1
hits	585149
misses	0
cgn_dest_log_timeouts	0
ipv4_nat_alg_bind_pkts	0
ipv4_nat_alg_sd_not_found	0
ipv4_nat_alg_sd_tail_not_found	0
ipv4_nat_rx_pkt	154
ipv4_nat_tx_pkt	18791285989
<snip>	
ipv4_nat_non_natted_in2out_pkts	144
ipv4_nat_non_nated_out2in_pkts	0
<snip>	
ipv4_nat_cfg_rcvd	8
ipv4_nat_cfg_rsp	9
Subcode#14 ADDR_ALLOC_FAIL	5216959285

Verificare il numero corrente di voci e confrontare i valori maxhost_count e maxhost_himark:

- maxhost_count: mostra le voci correnti sul router.
- maxhost_himark: mostra 7, ciò indica che il limite è stato raggiunto in un determinato punto.

<#root>

NAT_R1#

```
show platform hardware qfp active feature nat datapath limit
```

```
maxhost_limit 131072
```

```
maxhost_count 5
```

```
maxhost_fail 0
```

```
maxhost_himark 7
```

```
total limit entries 0 hash tbl 0x0 max entries 0 limit_chunk 0x0 allvrf limit 0  
acl limit 0 acl count 0 acl fail 0 acl_id 0x0
```

Possibile causa

Il numero di indirizzi utilizzabili nel pool NAT è compreso tra 3 e 5. I problemi si verificano quando le traduzioni inattive rimangono nella tabella NAT, impedendo la traduzione di altro traffico. Questo comportamento è previsto, in quanto il timeout di conversione NAT predefinito è di 24 ore. Per risolvere il problema, configurare il comando `ip nat translation timeout` per cancellare le traduzioni inattive dopo questa azione la tabella NAT deve essere cancellata.

```
<#root>
```

```
NAT_R1(config)#
```

```
ip nat translation timeout 10800
```

```
NAT_R1(config)#end
```

```
NAT_R1#
```

```
clear ip nat translation *
```

```
NAT_R1#
```

```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global  
--- 203.0.113.5 192.0.2.11 --- ---  
--- 203.0.113.4 192.0.2.10 --- ---  
icmp 203.0.113.4:0 192.0.2.10:0 198.51.100.10:0 198.51.100.10:0  
icmp 203.0.113.5:0 192.0.2.11:0 198.51.100.20:0 198.51.100.20:0  
Total number of translations: 4
```

Caso aziendale: NAT - Traduzione di indirizzi IP non nativi (problema gatekeeper)

La funzionalità Gatekeeper NAT è progettata per migliorare le prestazioni del router proteggendo il motore NAT dall'elaborazione di flussi non NAT. Quando i pacchetti non NAT attraversano un'interfaccia abilitata NAT, in genere vengono sottoposti a ricerche estese prima che NAT determini che la traduzione non è necessaria. Questo processo richiede un utilizzo intensivo della CPU sul Quantum Flow Processor (QFP). Il Gatekeeper riduce questo problema mantenendo una piccola cache di flussi non NAT, permettendo a questi pacchetti di ignorare il motore NAT una volta identificato, riducendo così il carico della CPU. Le voci nella cache Gatekeeper scadono relativamente rapidamente, consentendo al motore NAT di rivalutare i flussi nel caso in cui le condizioni della rete cambino e il flusso possa ora essere soggetto a NAT.

Questo meccanismo aiuta a ottimizzare l'utilizzo delle risorse e migliora l'efficienza complessiva del sistema quando si tratta di traffico misto NAT e non NAT sulla stessa interfaccia. Le dimensioni della cache per il Gatekeeper possono essere configurate per adattarsi al volume di traffico non NAT, con valori predefiniti basati sulla piattaforma. La regolazione delle dimensioni della cache è consigliata quando è presente un traffico non NAT significativo su un'interfaccia NAT.

In sintesi, il Gatekeeper NAT:

- Protegge il motore NAT dall'elaborazione non necessaria di flussi non NAT.
- Mantiene una cache di flussi non NAT per consentire loro di ignorare l'elaborazione NAT.
- Utilizza timeout sulle voci della cache per consentire la rivalutazione dei flussi.
- Consente di ridurre l'utilizzo della CPU sul QFP.
- Supporta dimensioni della cache configurabili per ottimizzare le prestazioni in base ai modelli di traffico.

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).