

Fehlerbehebung bei NAT auf Catalyst 8000-Plattformen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Anwenderbericht: NAT-Erschöpfung \(Pool erschöpft\)](#)

[Mögliche Ursache](#)

[Anwenderbericht: NAT übersetzt nicht verbrauchte IP-Adressen \(Gatekeeper-Problem\)](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei NAT-Problemen auf Cat8000-Plattformen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Network Address Translations (NAT)
- Cisco IOS XE

Weitere Informationen zu diesen Themen finden Sie unter:

[Konfigurieren der Network Address Translation](#)

[Verständnis der NAT-Betriebsreihenfolge](#)

[Network Address Translation \(NAT\) - Häufig gestellte Fragen](#)

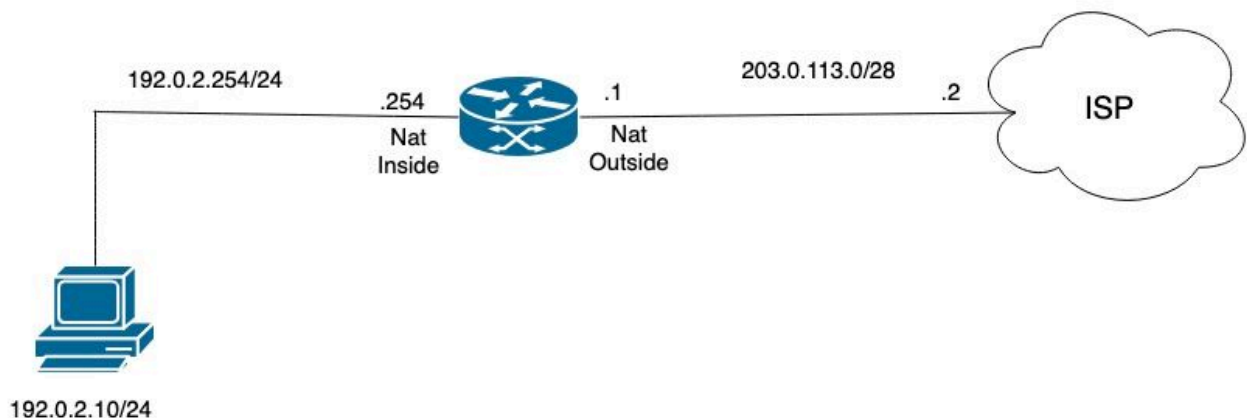
Einschränkungen für die Konfiguration von NAT zur Erhaltung von IP-Adressen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS XE Software.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm



NAT-Topologie

Anwenderbericht: NAT-Erschöpfung (Pool erschöpft)

Diese Protokollmeldung zeigt an, dass das Gerät versucht hat, eine IP-Adresse für NAT zuzuweisen, z. B. für eine dynamische NAT- oder PAT-Übersetzung, aber die Zuweisung war nicht erfolgreich. Dies tritt in der Regel dann auf, wenn im konfigurierten NAT-Pool keine verfügbaren Adressen oder Ports mehr vorhanden sind.

Zu den häufigen Ursachen gehören:

- Der NAT-Pool ist ausgelastet (alle verfügbaren IP-Adressen oder Ports werden verwendet).
- Die NAT-Konfiguration verfügt nicht über ausreichende Adressen oder Ressourcen, um die aktuellen Übersetzungsanforderungen zu erfüllen.

```
%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
```

Überprüfen Sie den NAT-Pool, um den Adressübersetzungsbereich zu bestätigen.

```
<#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
```

Überprüfen Sie die NAT-Übersetzungstabelle, und bestimmen Sie die Anzahl der derzeit vorhandenen aktiven Übersetzungen.

```
<#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

Überprüfen Sie, ob Verwerfungen in den NAT-Statistiken angezeigt werden. Dieses Ergebnis würde darauf hinweisen, dass eingehender Datenverkehr übersetzt werden muss, aber aufgrund von NAT-Zuweisungsproblemen verloren geht.

<#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#

Überprüfen Sie aus Plattformsicht die QFP-Datenpfad-NAT-Statistiken, um festzustellen, ob diese Verwerfungen dem festgestellten Problem entsprechen.

```
<#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

Überprüfen Sie die aktuelle Anzahl der Einträge, und vergleichen Sie die maxhost_count- und maxhost_himark-Werte:

- maxhost_count: zeigt die aktuellen Einträge auf dem Router.
- maxhost_himark: zeigt 7. Dies zeigt an, dass das Limit irgendwann erreicht wurde.

```
<#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
```

Mögliche Ursache

Die Anzahl der verwendbaren Adressen im NAT-Pool reicht von 3 bis 5. Probleme treten auf, wenn inaktive Übersetzungen in der NAT-Tabelle verbleiben, wodurch die Übersetzung von anderem Datenverkehr verhindert wird. Dieses Verhalten wird erwartet, da der Standard-NAT-Übersetzungstimeout 24 Stunden beträgt. Um dieses Problem zu beheben, konfigurieren Sie den Befehl `ip nat translation timeout`, um inaktive Übersetzungen zu löschen. Nach dieser Aktion muss die NAT-Tabelle gelöscht werden.

```
<#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
```

Anwenderbericht: NAT übersetzt nicht verbrauchte IP-Adressen (Gatekeeper-Problem)

Die NAT Gatekeeper-Funktion wurde entwickelt, um die Router-Leistung zu verbessern, indem die NAT-Engine vor der Verarbeitung von Nicht-NAT-Datenströmen geschützt wird. Wenn Pakete, die nicht NAT-fähig sind, eine NAT-fähige Schnittstelle passieren, werden sie in der Regel eingehend durchsucht, bevor NAT feststellt, dass keine Übersetzung erforderlich ist. Dieser Prozess ist für den Quantum Flow Processor (QFP) CPU-intensiv. Der Gatekeeper verringert dies, indem er einen kleinen Cache für Nicht-NAT-Datenflüsse unterhält, der es diesen Paketen ermöglicht, die NAT-Engine zu umgehen, sobald sie erkannt wurden, wodurch die CPU-Last verringert wird. Bei Einträgen im Gatekeeper-Cache erfolgt die Zeitüberschreitung relativ schnell, sodass Datenflüsse von der NAT-Engine neu bewertet werden können, falls sich die Netzwerkbedingungen ändern und der Datenfluss nun NAT unterliegen kann.

Dieser Mechanismus trägt zur Optimierung der Ressourcennutzung bei und verbessert die Gesamteffizienz des Systems, wenn gemischter NAT- und Nicht-NAT-Verkehr auf derselben Schnittstelle verarbeitet wird. Die Cachegröße für den Gatekeeper kann so konfiguriert werden, dass das Volumen an Nicht-NAT-Datenverkehr mit plattformabhängigen Standardwerten untergebracht wird. Die Anpassung der Cachegröße wird empfohlen, wenn auf einer NAT-Schnittstelle erheblicher Datenverkehr vorhanden ist, der nicht NAT ist.

Zusammenfassend lässt sich sagen, dass der NAT Gatekeeper:

- Schützt die NAT-Engine vor unnötiger Verarbeitung von Nicht-NAT-Datenströmen.
- Verwaltet einen Cache mit Nicht-NAT-Datenflüssen, damit diese die NAT-Verarbeitung umgehen können.
- Verwendet Timeouts für Cache-Einträge, um eine Neubewertung der Datenflüsse zu ermöglichen.
- Trägt zur Reduzierung der CPU-Auslastung beim QFP bei.
- Unterstützt konfigurierbare Cache-Größen zur Optimierung der Performance auf Basis von Datenverkehrsmustern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.