Configurar e verificar o NAT nos Switches Catalyst 9000

Contents

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Informações de Apoio](#)
[Componentes Utilizados](#)
[Terminologia](#)
[Diagrama de Rede](#)
[Configurar](#)
[Exemplo de configurações](#)
[Verificar o NAT estático](#)
[Verificação de software](#)
[Verificação de hardware](#)
[Verificar o NAT dinâmico](#)
[Verificação de software](#)
[Verificação de hardware](#)
[Verificar a sobrecarga do NAT dinâmico (PAT)](#)
[Verificação de software](#)
[Verificação de hardware](#)
[Depurações em nível de pacote](#)
[Troubleshooting de Escala NAT](#)
[Conversão Somente de Endereço (AOT)](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e validar a Network Address Translation (NAT) na plataforma Catalyst 9000.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Endereçamento IP
- Listas de controle de acesso

Informações de Apoio

O caso mais comum para o NAT é o uso na conversão de espaço de rede IP privada em endereços roteáveis de Internet globalmente exclusivos.

O dispositivo que executa o NAT deve ter uma interface na rede interna (local) e uma interface na rede externa (global).

Um dispositivo NAT é responsável pela inspeção do tráfego de origem para determinar se ele requer uma conversão com base na configuração das regras de NAT.

Se uma conversão for necessária, o dispositivo converterá o endereço IP de origem local em um endereço IP globalmente exclusivo e o acompanhará em sua tabela de conversão de NAT.

Quando os pacotes voltam com um endereço roteável, o dispositivo verifica sua tabela NAT para ver se outra conversão está em ordem.

Em caso afirmativo, o roteador converte o endereço global interno de volta ao endereço local interno apropriado e roteia o pacote.

Componentes Utilizados

Com o Cisco IOS® XE 16.12.1, o NAT agora está disponível na licença do Network Advantage. Em todas as versões anteriores, ele está disponível na licença do DNA Advantage.

Platform	Recurso NAT introduzido
C9300	Cisco IOS® XE versão 16.10.1
C9400	Cisco IOS® XE versão 17.1.1
C9500	Cisco IOS® XE versão 16.5.1a
C9600	Cisco IOS® XE versão 16.11.1

Este documento é baseado na plataforma Catalyst 9300 com Cisco IOS® XE versão 16.12.4

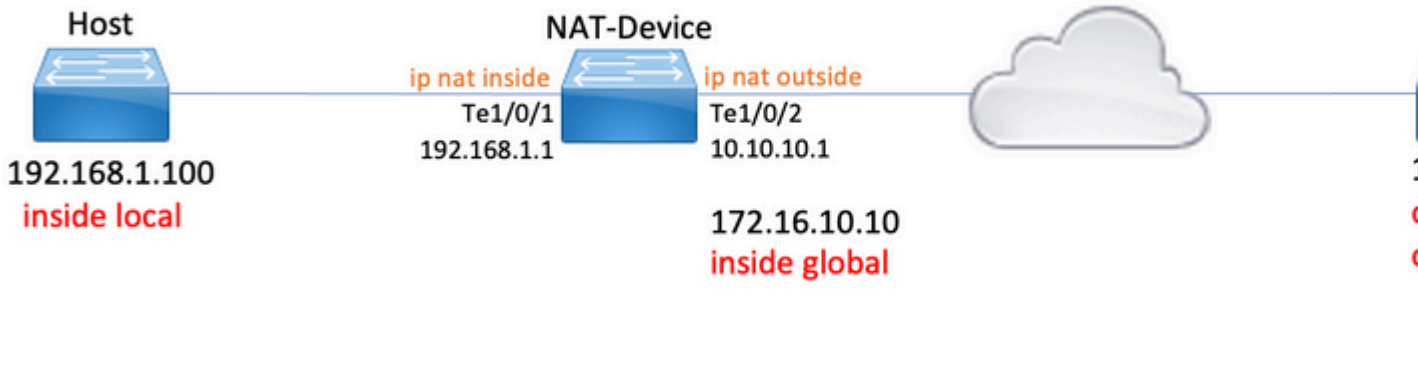
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Terminologia

NAT Estático	Permite o mapeamento 1 para 1 de um endereço local para um endereço global.
NAT dinâmica	Mapeia endereços locais para um pool de endereços globais.
NAT de sobrecarga	Mapeia endereços locais para um único endereço global que usa portas L4 exclusivas.
Local interno	O endereço IP atribuído a um host na rede interna.
Global interno	Esse é o endereço IP do host interno como ele aparece para a rede externa. Você pode pensar nisso como o endereço para o qual o local interno é convertido.
Local externo	O endereço IP de um host externo como aparece para a rede interna.
Global externo	O endereço IP atribuído a um host na rede externa. Na maioria dos casos, os endereços local externo e global externo são os mesmos.
FMAN-RP	Gerenciador de recursos RP. Este é o plano de controle do Cisco IOS® XE que passa informações de programação para o FMAN-FP.

FMAN-FP	Gerenciador de recursos FP. O FMAN-FP recebe informações do FMAN-RP e as passa ao FED.
FED	Forwarding Engine Driver (Driver do mecanismo de encaminhamento). O FMAN-FP usa o FED para programar informações do plano de controle para o Unified Access Data Plane (UADP) Application Specific Integrated Circuit (ASIC).

Diagrama de Rede



Configurar

Exemplo de configurações

Configuração **de NAT estático** para converter 192.168.1.100 (local interno) em 172.16.10.10 (global interno):

<#root>

```
NAT-Device#
```

show run interface te1/0/1

```
Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/1
no switchport
ip address 192.168.1.1 255.255.255.0
```

ip nat inside **<-- NAT inside interface**

```
end

NAT-Device#
```

show run interface te1/0/2

```
Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/2
no switchport
ip address 10.10.10.1 255.255.255.0
```

ip nat outside **<-- NAT outside interface**

```
end
```

ip nat inside source static 192.168.1.100 172.16.10.10 **<-- static NAT rule**

```
NAT-Device#
```

show ip nat translations

```
Pro Inside global      Inside local      Outside local      Outside global
icmp 172.16.10.10:4    192.168.1.100:4   10.20.30.40:4      10.20.30.40:4
```

<-- active NAT translation

```
---  172.16.10.10      192.168.1.100     ---                ---
```

<-- static NAT translation added as a result of the configuration

Configuração **de NAT dinâmico** para converter 192.168.1.0/24 em 172.16.10.1 - 172.16.10.30:

<#root>

```
NAT-Device#
```

show run interface te1/0/1

```
Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/1
no switchport
ip address 192.168.1.1 255.255.255.0
```

ip nat inside **<-- NAT inside interface**

```
end

NAT-Device#
```

show run interface te1/0/2

```
Building configuration...
```

```
Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/2
no switchport
ip address 10.10.10.1 255.255.255.0
ip nat outside


<-- NAT outside interface


end
!
ip nat pool TAC-POOL 172.16.10.1 172.16.10.30 netmask 255.255.255.224      <-- NAT pool configuration


ip nat inside source list hosts pool TAC-POOL


<-- NAT rule configuration


!
ip access-list standard hosts                                              <-- ACL to match hosts to be


10 permit 192.168.1.0 0.0.0.255

NAT-Device#
show ip nat translations


Pro Inside global     Inside local     Outside local      Outside global
icmp 172.16.10.10:6   192.168.1.100:6  10.20.30.40:6      10.20.30.40:6
---  172.16.10.10     192.168.1.100    ---                ---
```

Configuração **de Sobrecarga de NAT Dinâmico (PAT)** para converter 192.168.1.0/24 em 10.10.10.1 (ip nat outside interface):

<#root>

```
NAT-Device#
show run interface te1/0/1


Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/1
no switchport
ip address 192.168.1.1 255.255.255.0
ip nat inside                              <-- NAT inside interface
```

```
end

NAT-Device#
show run interface te1/0/2


Building configuration...

Current configuration : 109 bytes
!
interface TenGigabitEthernet1/0/2
no switchport
ip address 10.10.10.1 255.255.255.0
ip nat outside                              <-- NAT outside interface


end
!
ip nat inside source list hosts interface TenGigabitEthernet1/0/2 overload          <-- NAT configuratio


!
ip access-list standard hosts                                                       <-- ACL to match hos


 10 permit 192.168.1.0 0.0.0.255
```

Observe que a porta incrementa no endereço global interno em 1 para cada conversão:

<#root>

```
NAT-Device#
show ip nat translations

Pro Inside global      Inside local      Outside local      Outside global
icmp 10.10.10.1:1024   192.168.1.100:1   10.20.30.40:1        10.20.30.40:1024


<-- Notice layer 4 port increments


icmp 10.10.10.1:1025   192.168.1.100:2   10.20.30.40:2        10.20.30.40:1025


<-- Notice layer 4 port increments


icmp 10.10.10.1:1026   192.168.1.100:3   10.20.30.40:3        10.20.30.40:1026
icmp 10.10.10.1:1027   192.168.1.100:4   10.20.30.40:4        10.20.30.40:1027
icmp 10.10.10.1:1028   192.168.1.100:5   10.20.30.40:5        10.20.30.40:1028
icmp 10.10.10.1:1029   192.168.1.100:6   10.20.30.40:6        10.20.30.40:1029
icmp 10.10.10.1:1030   192.168.1.100:7   10.20.30.40:7        10.20.30.40:1030
icmp 10.10.10.1:1031   192.168.1.100:8   10.20.30.40:8        10.20.30.40:1031
```

10.10.10.1:1024 = inside global

192.168.1.100:1 = inside local

Verificar o NAT estático

Verificação de software

Espera-se ver metade de uma conversão com NAT estático quando não há fluxo ativo convertido. Quando o fluxo se torna ativo, uma conversão dinâmica é criada

<#root>

NAT-Device#

show ip nat translations

```
Pro Inside global      Inside local      Outside local      Outside global
icmp 172.16.10.10:10   192.168.1.100:10  10.20.30.40:10     10.20.30.40:10
```

<-- dynamic translation

--- 172.16.10.10   192.168.1.100   ---   ---

<-- static configuration from NAT rule configuration

Com o comando **show ip nat translations verbose**, você pode determinar o tempo em que o fluxo foi criado e o tempo restante na conversão.

<#root>

NAT-Device#

show ip nat translations verbose

```
Pro Inside global Inside local Outside local Outside global
icmp 172.16.10.10:10 192.168.1.100:10 10.20.30.40:10 10.20.30.40:10
```

create 00:00:13, use 00:00:13, left 00:00:46,

<-- NAT timers

```
flags:
extended, use_count: 0, entry-id: 10, lc_entries: 0
--- 172.16.10.10 192.168.1.100 --- ---
create 00:09:47, use 00:00:13,
flags:
static, use_count: 1, entry-id: 9, lc_entries: 0
```

Verifique as estatísticas de NAT. O contador de ocorrências de NAT é incrementado quando um fluxo corresponde a uma regra de NAT e é criado.

O contador de erros de NAT é incrementado quando o tráfego corresponde a uma regra, mas não é possível criar a conversão.

<#root>

NAT-DEVICE#

show ip nat statistics

Total active translations: 1 (

1 static,

0 dynamic; 0 extended)

<-- 1 static translation

Outside interfaces:

TenGigabitEthernet1/0/1 <-- NAT outside interface

Inside interfaces:

TenGigabitEthernet1/0/2 <-- NAT inside interface

Hits: 0 Misses: 0 <-- NAT hit and miss counters.

```
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list hosts interface TenGigabitEthernet1/0/1 refcount 0
```

Para que a conversão ocorra, é necessário que haja uma adjacência para a origem e o destino do fluxo de NAT. Anote a ID da adjacência.

<#root>

NAT-Device#

show ip route 10.20.30.40

```
Routing entry for 10.20.30.40/32
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
* 10.10.10.2
Route metric is 0, traffic share count is 1

NAT-Device#
```

show platform software adjacency switch active f0

```
Adjacency id:
```

0x29(41)

<-- adjacency ID

```
Interface: TenGigabitEthernet1/0/1, IF index: 52, Link Type: MCP_LINK_IP
Encap: 0:ca:e5:27:3f:e4:70:1f:53:0:b8:e4:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

192.168.1.100

<-- source adjacency

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 464, HW handle: (nil) (created)

Adjacency id:
```

0x24 (36)

<-- adjacency ID

```
Interface: TenGigabitEthernet1/0/2, IF index: 53, Link Type: MCP_LINK_IP
Encap: 34:db:fd:ee:ce:e4:70:1f:53:0:b8:d6:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

10.10.10.2

<-- next hop to 10.20.30.40

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 452, HW handle: (nil) (created)
```

As depurações de NAT podem ser ativadas para verificar se o switch recebe tráfego e se isso cria um fluxo de NAT

> **Observação**: observe que o tráfego ICMP sujeito ao NAT é sempre tratado no software, de modo que as depurações de plataforma não mostram logs para o tráfego ICMP.

```
<#root>

NAT-Device#

debug ip nat detailed


IP NAT detailed debugging is on
NAT-Device#
*Mar 8 23:48:25.672: NAT: Entry assigned id 11

<-- receive traffic and flow created


*Mar 8 23:48:25.672: NAT: i: icmp (192.168.1.100, 11) -> (10.20.30.40, 11) [55]
*Mar 8 23:48:25.672: NAT:

s=192.168.1.100->172.16.10.10

, d=10.20.30.40 [55]NAT: dyn flow info download suppressed for flow 11

<-- source is translated


*Mar 8 23:48:25.673: NAT: o: icmp (10.20.30.40, 11) -> (172.16.10.10, 11) [55]
*Mar 8 23:48:25.674: NAT: s=10.20.30.40,

d=172.16.10.10->192.168.1.100

 [55]NAT: dyn flow info download suppressed for flow 11

<-- return source is translated


*Mar 8 23:48:25.675: NAT: i: icmp (192.168.1.100, 11) -> (10.20.30.40, 11) [56]
```

Quando o fluxo expira ou é excluído, você vê a ação DELETE nas depurações:

```
<#root>

*Mar 31 17:58:31.344: FMANRP-NAT: Received flow data, action:

DELETE


<-- action is delete
```

```
*Mar 31 17:58:31.344: id 2, flags 0x1, domain 0
src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40,
dst_global_addr 10.20.30.40, src_local_port 31783, src_global_port 31783,
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 0,
outside_mapping_id 0, inside_mapping_type 0,
outside_mapping_type 0
```

Verificação de hardware

Quando a regra NAT é configurada, o dispositivo programa essa regra no TCAM na região NAT 5. Confirme se a regra está programada no TCAM.

As saídas estão em hexadecimal, portanto, a conversão para o endereço IP é necessária.

<#root>

```
NAT-Device#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region NAT_1 (370) type 6 asic 3
=======================================================
Printing entries for region NAT_2 (371) type 6 asic 3
=======================================================
Printing entries for region NAT_3 (372) type 6 asic 3
=======================================================
Printing entries for region NAT_4 (373) type 6 asic 3
=======================================================
```

Printing entries for region NAT_5 (374) type 6 asic 3 <-- NAT Region 5

```
=======================================================
TAQ-2 Index-128 (A:1,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:ffffffff
Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
```

c0a80164

<--

inside local IP address 192.168.1.100 in hex (c0a80164)

```
AD 10087000:00000073

TAQ-2 Index-129 (A:1,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:ffffffff:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:
```

ac100a0a

```
:00000000
```

<-- inside global IP address 172.16.10.10 in hex (ac100a0a)

```
AD 10087000:00000073
```

Finalmente, quando o fluxo se torna ativo, a programação de hardware pode ser confirmada pela verificação de TCAM na região 1 do NAT.

<#root>

NAT-Device#

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

Printing entries for region

NAT_1

(370) type 6 asic 1

<-- NAT Region 1

```
==========================================================
TAQ-2 Index-32 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:06005ac9:00000000:00000017:00000000:00000000:
```

0a141e28:c0a80164

AD 10087000:000000b0

```
TAQ-2 Index-33 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:06000017:00000000:00005ac9:00000000:00000000:
```

ac100a0a:0a141e28

AD 10087000:000000b1

Starting at Index-32 Key1 from right to left:

c0a80164

= 192.168.1.100 (Inside Local)

0a141e28

= 10.20.30.40 (Outside Global)

00000017

= 23 (TCP destination port)

06005ac9

= 06 for TCP and 5ac9 is 23241 which is source port from "show ip nat translations" of the inside host

Repeat the same for Index-33 which is the reverse translation:

0a141e28

= 10.20.30.40 (Outside Global)

ac100a0a

= 172.16.10.10 (Inside Global)

00005ac9

= 23241 TCP Destination port

06000017

= 06 for TCP and 17 for TCP source port 23

Verificar o NAT dinâmico

Verificação de software

Confirme se o pool de endereços para o qual converter endereços IP internos está configurado.

Essa configuração permite que a rede 192.168.1.0/24 seja convertida em endereços 172.16.10.1 a 172.16.10.254

<#root>

NAT-Device#

show run | i ip nat

ip nat inside

<-- ip nat inside on inside interface

ip nat outside

<-- ip nat outside on outside interface

ip nat pool MYPOOL 172.16.10.1 172.16.10.254 netmask 255.255.255.0   <-- Pool of addresses to translate

ip nat inside source list hosts pool MYPOOL   <-- Enables hosts that match ACL "h

NAT-Device#

show ip access-list 10 <-- ACL to match hosts to be translated

Standard IP access list 10

```
10 permit 192.168.1.0, wildcard bits 0.0.0.255
NAT-Device#
```

Observe que com o NAT dinâmico ele não cria nenhuma entrada com apenas a configuração. Um fluxo ativo precisa ser criado antes que a tabela de conversão seja preenchida.

<#root>

```
NAT-Device#
```

show ip nat translations

<...empty...>

Verifique as estatísticas de NAT. O contador de ocorrências de NAT é incrementado quando um fluxo corresponde a uma regra de NAT e é criado.

O contador de erros de NAT é incrementado quando o tráfego corresponde a uma regra, mas não é possível criar a conversão.

<#root>

```
NAT-DEVICE#
```

show ip nat statistics

```
Total active translations: 3794 (1 static,
```

3793 dynamic

```
; 3793 extended)
```

<-- dynamic translations

```
Outside interfaces:
```

TenGigabitEthernet1/0/1 <-- NAT outside interface

```
Inside interfaces:
```

TenGigabitEthernet1/0/2 <-- NAT inside interface

Hits: 3793

```
 Misses: 0
```

<-- 3793 hits

```
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
```

Dynamic mappings: <-- rule for dynamic mappings

```
-- Inside Source
[Id: 1]
```

access-list hosts interface TenGigabitEthernet1/0/1

```
 refcount 3793
```

<-- NAT rule displayed

Confirme se a adjacência com a origem e o destino está presente

<#root>

```
NAT-Device#
```

show platform software adjacency switch active f0

```
Number of adjacency objects: 4

Adjacency id:
```

0x24(36)

<-- adjacency ID

```
Interface: TenGigabitEthernet1/0/2, IF index: 53, Link Type: MCP_LINK_IP
Encap: 34:db:fd:ee:ce:e4:70:1f:53:0:b8:d6:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

10.10.10.2

<-- adjacency to destination

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 449, HW handle: (nil) (created)

Adjacency id:
```

0x25 (37)

<-- adjacency ID

```
Interface: TenGigabitEthernet1/0/1, IF index: 52, Link Type: MCP_LINK_IP
Encap: 0:ca:e5:27:3f:e4:70:1f:53:0:b8:e4:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
```

```
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:
```

192.168.1.100

<-- source adjacency

```
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 451, HW handle: (nil) (created)
```

Depois que as adjacências forem confirmadas, se houver um problema com o NAT, você poderá começar com depurações de NAT independentes de plataforma

<#root>

```
NAT-Device#
```

debug ip nat

```
IP NAT debugging is on
NAT-Device#
```

debug ip nat detailed

```
IP NAT detailed debugging is on

NAT-Device#
```

show logging

```
*May 13 01:00:41.136: NAT: Entry assigned id 6
*May 13 01:00:41.136: NAT: Entry assigned id 7
*May 13 01:00:41.136: NAT: i:
```

tcp (192.168.1.100, 48308)

```
 -> (10.20.30.40, 23) [30067]
```

<-- first packet ingress without NAT

```
*May 13 01:00:41.136: NAT: TCP Check for Limited ALG Support
*May 13 01:00:41.136: NAT:
```

s=192.168.1.100->172.16.10.10

```
, d=10.20.30.40 [30067]NAT: dyn flow info download suppressed for flow 7
```

<-- confirms source address translation

```
*May 13 01:00:41.136: NAT: attempting to setup alias for 172.16.10.10 (redundancy_name , idb NULL, flags
*May 13 01:00:41.139: NAT: o:
```

tcp (10.20.30.40, 23)

```
 -> (172.16.10.10, 48308) [40691]
```

<-- return packet from destination to be translated

```
*May 13 01:00:41.139: NAT: TCP Check for Limited ALG Support
*May 13 01:00:41.139: NAT: s=10.20.30.40,
```

d=172.16.10.10->192.168.1.100

```
 [40691]NAT: dyn flow info download suppressed for flow 7
```

<-- return packet is translated

```
*May 13 01:00:41.140: NAT: i: tcp (192.168.1.100, 48308) -> (10.20.30.40, 23) [30068]
```

Você também pode depurar a operação NAT FMAN-RP:

<#root>

```
NAT-Device#
```

debug platform software nat all

```
NAT platform all events debugging is on

Log Buffer (100000 bytes):

*May 13 01:04:16.098: FMANRP-NAT: Received flow data, action:
```

ADD

<-- first packet in flow so we ADD an entry

```
*May 13 01:04:16.098: id 9, flags 0x1, domain 0
```

src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40

,

<-- verify inside local/global and outside local/global

```
dst_global_addr 10.20.30.40, src_local_port 32529, src_global_port 32529,
```

dst_local_port 23, dst_global_port 23

,

<-- confirm ports, in this case they are for Telnet

```
proto 6, table_id 0 inside_mapping_id 1,
outside_mapping_id 0, inside_mapping_type 2,
outside_mapping_type 0
*May 13 01:04:16.098: FMANRP-NAT: Created TDL message for flow info:
ADD id 9
*May 13 01:04:16.098: FMANRP-NAT: Sent TDL message for flow data config:
ADD id 9
```

```
*May 13 01:04:16.098: FMANRP-NAT: Received flow data, action:

 MODIFY            <-- subsequent packets are MODIFY


*May 13 01:04:16.098: id 9, flags 0x1, domain 0
src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40,
dst_global_addr 10.20.30.40, src_local_port 32529, src_global_port 32529,
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 1,
outside_mapping_id 0, inside_mapping_type 2,
outside_mapping_type 0
*May 13 01:04:16.098: FMANRP-NAT: Created TDL message for flow info:
MODIFY id 9
*May 13 01:04:16.098: FMANRP-NAT: Sent TDL message for flow data config:
MODIFY id 9
```

Se a regra for removida por qualquer motivo, como expiração ou remoção manual, uma ação DELETE será observada:

<#root>

```
*May 13 01:05:20.276: FMANRP-NAT: Received flow data, action:

DELETE           <-- DELETE action


*May 13 01:05:20.276: id 9, flags 0x1, domain 0
src_local_addr 192.168.1.100, src_global_addr 172.16.10.10, dst_local_addr 10.20.30.40,
dst_global_addr 10.20.30.40, src_local_port 32529, src_global_port 32529,
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 0,
outside_mapping_id 0, inside_mapping_type 0,
outside_mapping_type 0
```

Verificação de hardware

Verifique se a regra NAT que corresponde ao tráfego a ser convertido foi adicionada corretamente no hardware na região NAT 5:

<#root>

```
NAT-Device#

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_


Printing entries for region

NAT_1

 (370) type 6 asic 1

<<<< empty due to no active flow
```

```
=========================================================
Printing entries for region NAT_2 (371) type 6 asic 1
=========================================================
Printing entries for region NAT_3 (372) type 6 asic 1
=========================================================
Printing entries for region NAT_4 (373) type 6 asic 1
=========================================================
Printing entries for region NAT_5 (374) type 6 asic 1
=========================================================
TAQ-2 Index-128 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:fffffff8:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:ac100a00:00000000
AD 10087000:00000073

TAQ-2 Index-129 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:
```

ffffff00

```
Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
```

c0a80100

```
AD 10087000:00000073
```

ffffff00 = 255.255.255.0 in hex

c0a80100 = 192.168.1.0 in hex which matches our network in the NAT ACL

Por fim, você precisa confirmar se a tradução ativa está programada corretamente na região 1 de TCAM de NAT

<#root>

```
NAT-Device#
```

show ip nat translations

```
Pro Inside global       Inside local        Outside local      Outside global
tcp 172.16.10.10:54854  192.168.1.100:54854 10.20.30.40:23     10.20.30.40:23
--- 172.16.10.10        192.168.1.100       ---                ---

NAT-Device#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region
```

NAT_1

```
 (370) type 6 asic 1
=========================================================
TAQ-2 Index-32 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
```

Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:0600d646:00000000:00000017:00000000:00000000:

0a141e28

:

c0a80164

AD 10087000:000000b0

TAQ-2 Index-33 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:06000017:00000000:0000d646:00000000:00000000:

ac100a0a

:

0a141e28

AD 10087000:000000b1

Printing entries for region NAT_2 (371) type 6 asic 1
===
Printing entries for region NAT_3 (372) type 6 asic 1
===
Printing entries for region NAT_4 (373) type 6 asic 1
===
Printing entries for region NAT_5 (374) type 6 asic 1
===

Starting at Index-32 Key 1 from right to left:

c0a80164

 - 192.168.1.100 (inside local)

0a141e28

 - 10.20.30.40 (outside local/global)

00000017

 - TCP port 23

0600d646

 - 6 for TCP protocol and 54854 for TCP source port

Starting at Index-33 Key 1 from right to left

0a141e28

 - 10.20.30.40 destination address

ac100a0a

 - 172.16.10.10 (inside global source IP address)

0000d646

 - TCP source port

06000017

- TCP protocol 6 and 23 for the TCP destination port

Verificar a sobrecarga do NAT dinâmico (PAT)

Verificação de software

Os processos de registro para verificar o PAT são os mesmos do NAT dinâmico. Você só precisa confirmar a conversão de porta correta e se as portas estão programadas corretamente no hardware.

O PAT é obtido pela palavra-chave "overload" anexada à regra NAT.

<#root>

NAT-Device#

show run | i ip nat

ip nat inside

<-- ip nat inside on NAT inside interface

ip nat outside

<-- ip nat outside on NAT outside interface

ip nat pool MYPOOL 172.16.10.1 172.16.10.254 netmask 255.255.255.0 <-- Address pool to translate to

ip nat inside source list hosts pool MYPOOL overload <-- Links ACL hosts to address pool

Confirme se a adjacência com a origem e o destino está presente

<#root>

NAT-Device#

show ip route 10.20.30.40

Routing entry for 10.20.30.40/32
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
*

10.10.10.2

Route metric is 0, traffic share count is 1

NAT-Device#

show platform software adjacency switch active f0

Number of adjacency objects: 4

Adjacency id:

0x24

(36)

<-- adjacency ID

Interface: TenGigabitEthernet1/0/2, IF index: 53, Link Type: MCP_LINK_IP
Encap: 34:db:fd:ee:ce:e4:70:1f:53:0:b8:d6:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:

10.10.10.2 <-- adjacency to destination

IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 449, HW handle: (nil) (created)

Adjacency id:

0x25

(37)

<-- adjacency ID

Interface: TenGigabitEthernet1/0/1, IF index: 52, Link Type: MCP_LINK_IP
Encap: 0:ca:e5:27:3f:e4:70:1f:53:0:b8:e4:8:0
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
Flags: no-l3-inject
Incomplete behavior type: None
Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr:

192.168.1.100 <-- source adjacency

IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 451, HW handle: (nil) (created)

Confirme se a conversão é adicionada à tabela de conversão quando o fluxo está ativo. Observe que com o PAT não há uma meia entrada criada como com o NAT dinâmico.

Controle os números de porta nos endereços locais internos e globais internos.

<#root>

NAT-Device#

show ip nat translations

```
Pro Inside global      Inside local        Outside local      Outside global
tcp 172.16.10.10:1024  192.168.1.100:52448 10.20.30.40:23     10.20.30.40:23
```

Verifique as estatísticas de NAT. O contador de ocorrências de NAT é incrementado quando um fluxo corresponde a uma regra de NAT e é criado.

O contador de erros de NAT é incrementado quando o tráfego corresponde a uma regra, mas não é possível criar a conversão.

<#root>

NAT-DEVICE#

show ip nat statistics

Total active translations: 3794 (1 static,

3793 dynamic

; 3793 extended)

<-- dynamic translations

Outside interfaces:

TenGigabitEthernet1/0/1 **<-- NAT outside interface**

Inside interfaces:

TenGigabitEthernet1/0/2 **<-- NAT inside interface**

Hits: 3793

Misses: 0

<-- 3793 hits

CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0

Dynamic mappings:

<-- rule for dynamic mappings

-- Inside Source
[Id: 1]

access-list hosts interface TenGigabitEthernet1/0/1

refcount 3793

<-- NAT rule displayed

As depurações de NAT independente de plataforma mostram que a conversão de porta ocorre:

<#root>

NAT-Device#

debug ip nat detailed

IP NAT detailed debugging is on
NAT-Device#

debug ip nat

IP NAT debugging is on

NAT-device#

show logging

Log Buffer (100000 bytes):

*May 18 23:52:20.296: NAT: address not stolen for 192.168.1.100, proto 6 port 52448
*May 18 23:52:20.296: NAT: Created portlist for proto tcp globaladdr 172.16.10.10
*May 18 23:52:20.296: NAT: Allocated Port for 192.168.1.100 -> 172.16.10.10:

wanted 52448 got 1024<-- confirms PAT is used

*May 18 23:52:20.296: NAT: Entry assigned id 5
*May 18 23:52:20.296: NAT: i: tcp (192.168.1.100, 52448) -> (10.20.30.40, 23) [63338]
*May 18 23:52:20.296: NAT: TCP Check for Limited ALG Support
*May 18 23:52:20.296: NAT: TCP

s=52448->1024

, d=23

<-- confirms NAT overload with PAT

*May 18 23:52:20.296: NAT:

s=192.168.1.100->172.16.10.10, d=10.20.30.40

[63338]NAT: dyn flow info download suppressed for flow 5

<-- shows inside translation

```
*May 18 23:52:20.297: NAT: attempting to setup alias for 172.16.10.10 (redundancy_name , idb NULL, flags
*May 18 23:52:20.299: NAT: o: tcp (10.20.30.40, 23) -> (172.16.10.10, 1024) [55748]
*May 18 23:52:20.299: NAT: TCP Check for Limited ALG Support
*May 18 23:52:20.299: NAT: TCP s=23,
```

d=1024->52448

<-- shows PAT on return traffic

```
*May 18 23:52:20.299: NAT: s=10.20.30.40, d=172.16.10.10->192.168.1.100 [55748]NAT: dyn flow info downlo
```

<#root>

```
NAT-Device#
```

debug platform software nat all

```
NAT platform all events debugging is on
NAT-Device#

*May 18 23:52:20.301: FMANRP-NAT: Received flow data, action:
```

ADD <-- first packet in flow ADD operation

```
*May 18 23:52:20.301: id 5, flags 0x5, domain 0
```

src_local_addr 192.168.1.100, src_global_addr 172.16.10.10

```
, dst_local_addr 10.20.30.40,
```

<-- source translation

```
dst_global_addr 10.20.30.40,
```

src_local_port 52448, src_global_port 1024

```
,
```

<-- port translation

```
dst_local_port 23, dst_global_port 23,
proto 6, table_id 0 inside_mapping_id 1,
outside_mapping_id 0, inside_mapping_type 2,
outside_mapping_type 0
<snip>
```

Verificação de hardware

Confirme se a regra NAT está instalada corretamente no hardware na região NAT 5

<#root>

```
NAT-Device#
show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_


Printing entries for region
NAT_1
 (370) type 6 asic 1
<-- NAT_1 empty due to no active flow


=========================================================
Printing entries for region NAT_2 (371) type 6 asic 1
=========================================================
Printing entries for region NAT_3 (372) type 6 asic 1
=========================================================
Printing entries for region NAT_4 (373) type 6 asic 1
=========================================================
Printing entries for region NAT_5 (374) type 6 asic 1
=========================================================
TAQ-2 Index-128 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:fffffffc:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:ac100a00:00000000
AD 10087000:00000073

TAQ-2 Index-129 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:
ffffff00


Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
c0a80100


AD 10087000:00000073


ffffff00 = 255.255.255.0 in hex for our subnet mask in NAT ACL


c0a80100 = 192.168.1.0 in hex for our network address in NAT ACL
```

Por fim, você pode verificar se o fluxo de NAT está programado no TCAM de hardware em NAT_Region 1 quando o fluxo está ativo

<#root>

```
NAT-Device#
show ip nat translations


Pro Inside global      Inside local        Outside local  Outside global
tcp 172.16.10.10:1024  192.168.1.100:20027 10.20.30.40:23 10.20.30.40:23

NAT-Device#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

Printing entries for region

NAT_1

(370) type 6 asic 1

<-- NAT region 1

==========
TAQ-2 Index-32 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:

06004e3b

:00000000:

00000017

:00000000:00000000:

0a141e28

:

c0a80164

AD 10087000:000000b0

TAQ-2 Index-33 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0000f000:ff00ffff:00000000:0000ffff:00000000:00000000:ffffffff:ffffffff
Key1 00009000:

06000017

:00000000:

00000400

:00000000:00000000:

0a141e28

:

0a141e28

AD 10087000:000000b1

Starting at Index-32 Key1 from right to left:

c0a80164

- 192.168.1.100 (inside local source address)

0a141e28

- 10.20.30.40 (inside global address/outside local address)

00000017

```
- 23 (TCP destination port)

06004e3b

- TCP source port 20027 (4e3b) and TCP protocol 6



Starting at Index-33 Key1 from right to left:

0a141e28

 - 10.20.30.40 (outside global address/outside local address)

ac100a0a

 - 172.16.10.10 (inside global)

00000400

 - TCP inside global source port 1024

06000017

 - TCP protocol 6 and TCP source port 23
```

Depurações em nível de pacote

O primeiro pacote em um fluxo que corresponde a uma regra NAT no hardware deve ser apontado para a CPU do dispositivo para ser processado. Para exibir saídas de depuração relacionadas ao caminho de punt, você pode habilitar os rastreamentos do caminho de punt FED para o nível de depuração para garantir que o pacote seja pontuado. O tráfego de NAT que precisa de recursos da CPU vai para a fila da CPU de Tráfego de Trânsito.

Verifique se a fila de CPU do tráfego de trânsito vê pacotes apontados ativamente para ela.

<#root>

```
NAT-DEVICE#

show platform software fed switch active punt cpuq clear <-- clear statistics



NAT-DEVICE#

show platform software fed switch active punt cpuq 18    <-- transit traffic queue

Punt CPU Q Statistics
=============================================

CPU Q Id :

18

CPU Q Name :
```

CPU_Q_TRANSIT_TRAFFIC

Packets received from ASIC : 0 **<-- no punt traffic for NAT**

Send to IOSd total attempts : 0
Send to IOSd failed count : 0
RX suspend count : 0
RX unsuspend count : 0
RX unsuspend send count : 0
RX unsuspend send failed count : 0
RX consumed count : 0
RX dropped count : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count : 0
RX packets dq'd after intack : 0
Active RxQ event : 0
RX spurious interrupt : 0
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

Replenish Stats for all rxq:

Number of replenish : 0
Number of replenish suspend : 0
Number of replenish un-suspend : 0

NAT-DEVICE#

show platform software fed switch active punt cpuq 18 **<-- after new translation**

Punt CPU Q Statistics
==========

CPU Q Id : 18
CPU Q Name : CPU_Q_TRANSIT_TRAFFIC

Packets received from ASIC : 5 **<-- confirms the UADP ASIC punts to**

Send to IOSd total attempts : 5
Send to IOSd failed count : 0
RX suspend count : 0
RX unsuspend count : 0
RX unsuspend send count : 0
RX unsuspend send failed count : 0
RX consumed count : 0
RX dropped count : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count : 5
RX packets dq'd after intack : 0
Active RxQ event : 5
RX spurious interrupt : 0
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

```
Replenish Stats for all rxq:
----------------------------------------
Number of replenish : 18
Number of replenish suspend : 0
Number of replenish un-suspend : 0
----------------------------------------
```

Troubleshooting de Escala NAT

Suporte de hardware atual para o número máximo de entradas de TCAM de NAT, conforme ilustrado na tabela:

Observação: cada conversão de NAT ativa requer 2 entradas TCAM.

Platform	Número máximo de entradas TCAM
Catalyst 9300	5000
Catalyst 9400	14000
Catalyst 9500	14000
Alto desempenho do Catalyst 9500	15500
Catalyst 9600	15500

Se você suspeitar de um problema com a escala, poderá confirmar o número total de conversões de NAT TCP/UDP para verificar em relação a um limite de plataforma.

<#root>

```
NAT-Device#
show ip nat translations | count tcp

Number of lines which match regexp =
621             <-- current number of TCP translations

NAT-Device#
show ip nat translations | count udp

Number of lines which match regexp =
4894            <-- current number of UDP translations
```

Se você tiver esgotado o espaço de TCAM de NAT, o módulo NAT no hardware do switch não poderá processar essas conversões. Neste cenário, o tráfego sujeito à conversão de NAT é direcionado para a CPU do dispositivo para ser processado.

Isso pode causar latência e pode ser confirmado por meio de quedas que incrementam a fila do vigilante do plano de controle, que é responsável pelo tráfego de punt NAT. A fila da CPU para onde o tráfego NAT vai é "Tráfego de trânsito".

<#root>

NAT-Device#

show platform hardware fed switch active qos queue stats internal cpu policer

```
                          CPU Queue Statistics
============================================================================================
                                              (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
<snip>
14   13     Sw forwarding              Yes     1000      1000     0            0
15   8      Topology Control           Yes     13000     16000    0            0
16   12     Proto Snooping             Yes     2000      2000     0            0
17   6      DHCP Snooping              Yes     500       500      0            0

18   13     Transit Traffic            Yes     1000      1000     34387271     399507


<-- drops for NAT traffic headed towards the CPU


19   10     RPF Failed                 Yes     250       250      0            0
20   15     MCAST END STATION          Yes     2000      2000     0            0
<snip>
```

Confirme o espaço TCAM do NAT disponível no código 17.x. Essa saída é de um 9300 com o modelo NAT ativado para que o espaço seja maximizado.

<#root>

NAT-DEVICE#

show platform hardware fed switch active fwd-asic resource tcam utilization

```
Codes: EM - Exact_Match, I - Input, O - Output, IO - Input & Output, NA - Not Applicable

CAM Utilization for ASIC [0]
Table                  Subtype      Dir      Max     Used    %Used       V4       V6     MPLS    Other
-------------------------------------------------------------------------------------------------------
Mac Address Table      EM           I       32768       22    0.07%        0        0        0       22
Mac Address Table      TCAM         I        1024       21    2.05%        0        0        0       21
L3 Multicast           EM           I        8192        0    0.00%        0        0        0        0
L3 Multicast           TCAM         I         512        9    1.76%        3        6        0        0
L2 Multicast           EM           I        8192        0    0.00%        0        0        0        0
L2 Multicast           TCAM         I         512       11    2.15%        3        8        0        0
IP Route Table         EM           I       24576       16    0.07%       15        0        1        0
IP Route Table         TCAM         I        8192       25    0.31%       12       10        2        1
QOS ACL                TCAM         IO       1024       85    8.30%       28       38        0       19
Security ACL           TCAM         IO       5120      148    2.89%       27       76        0       45
Netflow ACL            TCAM         I         256        6    2.34%        2        2        0        2

PBR ACL                TCAM         I        5120       24    0.47%       18        6        0        0


Netflow ACL            TCAM         O         768        6    0.78%        2        2        0        2
```

```
Flow SPAN ACL          TCAM         IO       1024       13    1.27%       3        6         0        4
Control Plane          TCAM         I         512      281   54.88%     130      106         0       45
Tunnel Termination     TCAM         I         512       18    3.52%       8       10         0        0
Lisp Inst Mapping      TCAM         I         512        1    0.20%       0        0         0        1
Security Association   TCAM         I         256        4    1.56%       2        2         0        0
Security Association   TCAM         O         256        5    1.95%       0        0         0        5
CTS Cell Matrix/VPN
Label                  EM           O        8192        0    0.00%       0        0         0        0
CTS Cell Matrix/VPN
Label                  TCAM         O         512        1    0.20%       0        0         0        1
Client Table           EM           I        4096        0    0.00%       0        0         0        0
Client Table           TCAM         I         256        0    0.00%       0        0         0        0
Input Group LE         TCAM         I        1024        0    0.00%       0        0         0        0
Output Group LE        TCAM         O        1024        0    0.00%       0        0         0        0
Macsec SPD             TCAM         I         256        2    0.78%       0        0         0        2
```

Confirme o espaço TCAM do NAT disponível no código 16.x. Essa saída é de um 9300 com o modelo de Acesso SDM, de modo que o espaço disponível para entradas NAT TCAM não é maximizado.

<#root>

```
NAT-DEVICE#
```

`show platform hardware fed switch active fwd-asic resource tcam utilization`

```
CAM Utilization for ASIC [0]
 Table                                              Max Values        Used Values
--------------------------------------------------------------------------------
Unicast MAC addresses                              32768/1024         20/21
L3 Multicast entries                                8192/512           0/9
L2 Multicast entries                                8192/512           0/11
Directly or indirectly connected routes            24576/8192          5/23
QoS Access Control Entries                          5120               85
Security Access Control Entries                     5120              145
Ingress Netflow ACEs                                 256               8
Policy Based Routing ACEs                           1024              24 <-- NAT usage in PRB TCAM

Egress Netflow ACEs                                  768               8
Flow SPAN ACEs                                      1024              13
Control Plane Entries                                512              255
Tunnels                                              512              17
Lisp Instance Mapping Entries                       2048              3
Input Security Associations                          256               4
SGT_DGT                                             8192/512           0/1
CLIENT_LE                                           4096/256           0/0
INPUT_GROUP_LE                                      1024               0
OUTPUT_GROUP_LE                                     1024               0
Macsec SPD                                           256               2
```

O espaço de hardware disponível para NAT TCAM pode ser aumentado por uma alteração no modelo SDM para preferir o NAT. Isso aloca o suporte de hardware para o número máximo de entradas de TCAM.

<#root>

```
NAT-Device#conf t
Enter configuration commands, one per line. End with CNTL/Z.
NAT-Device(config)#
```

sdm prefer nat

Se você comparar o SDM antes e depois da conversão para o modelo NAT, poderá confirmar se o espaço TCAM utilizável é trocado por entradas de controle de acesso de QoS e ACEs de roteamento baseado em política (PBR - Policy Based Routing).

PBR TCAM é onde o NAT é programado.

<#root>

```
NAT-Device#
```

show sdm prefer

```
Showing SDM Template Info

This is the Access template.
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 1024
L2 Multicast entries: 8192
Overflow L2 Multicast entries: 512
L3 Multicast entries: 8192
Overflow L3 Multicast entries: 512
Directly connected routes: 24576
Indirect routes: 8192
Security Access Control Entries: 5120
QoS Access Control Entries: 5120
```

Policy Based Routing ACEs: 1024 <-- NAT

<...snip...>

```
NAT-Device#
```

show sdm prefer

```
Showing SDM Template Info

This is the NAT template.
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 1024
L2 Multicast entries: 8192
Overflow L2 Multicast entries: 512
L3 Multicast entries: 8192
Overflow L3 Multicast entries: 512
Directly connected routes: 24576
Indirect routes: 8192
Security Access Control Entries: 5120
QoS Access Control Entries: 1024
```

```
Policy Based Routing ACEs: 5120       <-- NAT

<snip>
```

Conversão Somente de Endereço (AOT)

A AOT é um mecanismo que pode ser usado quando o requisito de NAT é converter apenas o campo de endereço IP e não as portas de camada 4 de um fluxo. Se isso atender aos requisitos, a AOT poderá aumentar muito o número de fluxos a serem convertidos e encaminhados no hardware.

- A AOT é mais eficaz quando a maioria dos fluxos de NAT é destinada a um único ou pequeno conjunto de destinos.
- A AOT está desabilitada por padrão. Depois de habilitado, é necessário limpar as conversões de NAT atuais.

Observação: a AOT é suportada apenas com NAT estático e NAT dinâmico que não inclui PAT.

Isso significa que as únicas configurações NAT possíveis que permitem a AOT são:

```
#ip nat inside source static <source> <destination>
#ip nat inside source list <list> pool <pool name>
```

Você pode habilitar a AOT com este comando:

<#root>

```
NAT-Device(config)#
```

no ip nat create flow-entries

Confirme se a regra NAT da AOT está programada corretamente. Essa saída é de uma conversão de NAT estático.

<#root>

```
NAT-DEVICE#
```

show running-config | include ip nat

```
ip nat outside
ip nat inside
```

no ip nat create flow-entries   <-- AOT enabled

ip nat inside source static 10.10.10.100 172.16.10.10   <-- static NAT enabled

```
NAT-DEVICE#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region NAT_1 (376) type 6 asic 1
=====================================================
Printing entries for region NAT_2 (377) type 6 asic 1
=====================================================
Printing entries for region NAT_3 (378) type 6 asic 1
=====================================================
Printing entries for region NAT_4 (379) type 6 asic 1
=====================================================
Printing entries for region NAT_5 (380) type 6 asic 1
=====================================================
TAQ-1 Index-864 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 3300f000:00000000:00000000:00000000:00000000:00000000:00000000:ffffffff
Key1 21009000:00000000:00000000:00000000:00000000:00000000:00000000:
```

0a0a0a64

```
AD 10087000:00000073

TAQ-1 Index-865 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Mask1 0300f000:00000000:00000000:00000000:00000000:00000000:ffffffff:00000000
Key1 02009000:00000000:00000000:00000000:00000000:00000000:
```

ac100a0a

```
:00000000
AD 10087000:00000073
```

0a0a0a64 = 10.10.10.100 (inside local)
ac100a0a = 172.16.10.10 (inside global)

Verifique a entrada da AOT no TCAM através da confirmação de que somente o endereço IP origem e destino está programado quando o fluxo se torna ativo.

<#root>

```
NAT-DEVICE#
```

show platform hardware fed switch active fwd-asic resource tcam table pbr record 0 format 0 | begin NAT_

```
Printing entries for region NAT_1 (376) type 6 asic 1
=====================================================
Printing entries for region NAT_2 (377) type 6 asic 1
=====================================================
TAQ-1 Index-224 (A:0,C:1) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Mask1 0000f000:00000000:00000000:00000000:00000000:00000000:ffffffff:ffffffff
Key1 00009000:00000000:00000000:00000000:00000000:00000000:
```

c0a80164:0a0a0a64 <-- no L4 ports, only source and destination IP is programmed

```
AD 10087000:000000b2

TAQ-1 Index-225 (A:0,C:1) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
```

```
Mask1 0000f000:00000000:00000000:00000000:00000000:00000000:ffffffff:00000000
Key1 00009000:00000000:00000000:00000000:00000000:00000000:
```

ac100a0a

```
:00000000
AD 10087000:000000b3
```

0a0a0a64 = 10.10.10.100 in hex (inside local IP address)

c0a80164 = 192.168.1.100 in hex (outside local/outside global)
ac100a0a = 172.16.10.10 (inside global)

Informações Relacionadas

- Guia de configuração de NAT do Catalyst 9300 17.3.x
- Guia de configuração de NAT do Catalyst 9400 17.3.x
- Guia de configuração de NAT do Catalyst 9500 17.3.x
- Guia de configuração de NAT do Catalyst 9600 17.3.x
- Suporte Técnico e Documentação - Cisco Systems

Interno da Cisco Informações

CSCvz46804 Aprimoramento para adicionar um syslog quando os recursos de TCAM de NAT estiverem esgotados ou quando uma entrada de NAT não puder ser programada com êxito.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.