在Catalyst 9000交换机上配置并检验NAT

目录

简介

本文档介绍如何在Catalyst 9000平台上配置和验证网络地址转换(NAT)。

先决条件

要求

Cisco 建议您了解以下主题：

- IP 编址
- 访问控制列表

背景信息

NAT最常见的情况是将专用IP网络空间转换为全球唯一的Internet可路由地址。

执行NAT的设备需要有内部网络上的接口（本地）和外部网络上的接口（全局）。

NAT设备负责检查源流量，以确定它是否需要基于NAT规则配置的转换。

如果需要转换，设备会将本地源IP地址转换为全局唯一的IP地址，并在其NAT转换表中跟踪此情况。

当数据包使用可路由地址返回时，设备会检查其NAT表，以查看是否有其它转换正在进行。

如果是，路由器会将内部全局地址转换回相应的内部本地地址并路由数据包。

使用的组件

在Cisco IOS® XE 16.12.1 NAT中，Network Advantage许可证现在可用。在所有早期版本中，DNA Advantage许可证中均提供此功能。

Platform	引入的NAT功能
C9300	思科IOS® XE版本16.10.1
C9400	思科IOS® XE版本17.1.1
C9500	思科IOS® XE版本16.5.1a
C9600	思科IOS® XE版本16.11.1

本文档基于采用Cisco IOS® XE版本16.12.4的Catalyst 9300平台

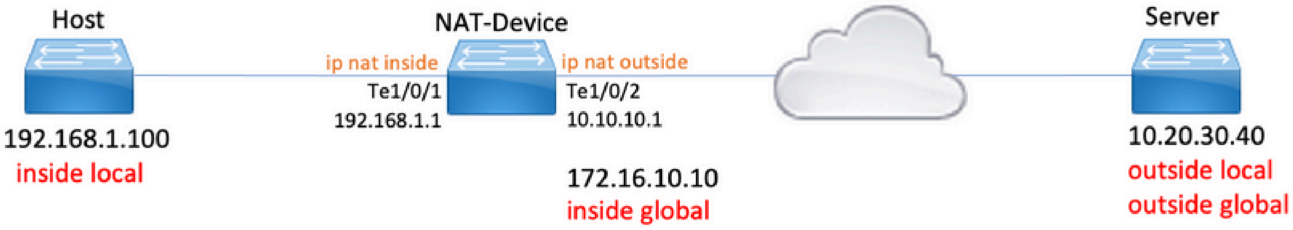
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

术语

静态NAT	允许本地地址到全局地址的一对一映射。
动态NAT	将本地地址映射到全局地址池。
过载NAT	将本地地址映射到使用唯一L4端口的单个全局地址。
内部本地	分配给内部网络中主机的 IP 地址。
内部全局	这是内部主机对外部网络显示的IP地址。您可以将此地址视为内部本地地址转换到的地址。
外部本地	外部主机显现给内部网络的 IP 地址。
外部全局	分配给外部网络上主机的IP地址。在大多数情况下，外部本地和外部全局地址相同。
FMAN-	功能管理器RP。这是Cisco IOS® XE的控制平面，它将编程信息传递给FMAN-FP。

RP	
FMAN-FP	功能管理器FP。FMAN-FP从FMAN-RP接收信息并将其传递给FED。
美联储	转发引擎驱动程序。FMAN-FP使用FED将来自控制平面的信息编程到统一接入数据平面(UADP)专用集成电路(ASIC)中。

网络图



配置

配置示例

将静态NAT配置转换192.168.1.100（内部本地）到172.16.10.10（内部全局）：

<#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
```

要将192.168.1.0/24转换为172.16.10.1 - 172.16.10.30的动态NAT配置：

<#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    ---                ---
```

用于将192.168.1.0/24转换到10.10.10.1(ip nat outside interface)的动态NAT过载(PAT)配置：

<#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
```

注意每个转换的内部全局地址上的端口增量为1:

<#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
```

检验静态NAT

软件验证

在没有转换活动流的情况下，预计会看到使用静态NAT转换的一半。 当流变为活动状态时，将创建动态转换

<#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
```

使用show ip nat translations verbose命令可以确定创建流的时间和转换时剩余的时间。

<#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
```

检查NAT统计信息。当流量与NAT规则匹配并创建时，NAT命中计数器会增加。

当流量与规则匹配时，NAT未命中计数器会增加，但我们无法创建转换。

<#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
```

要进行转换，需要与NAT流的源和目标建立邻接关系。记下邻接ID。

<#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)
```

可以启用NAT调试，以验证交换机是否收到流量以及是否创建了NAT流

注意：请注意，受NAT约束的ICMP流量始终在软件中处理，因此平台调试不会显示ICMP流量的日志。

<#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]
```

当流到期或被删除时，您会在调试中看到DELETE操作：

<#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
```

硬件验证

配置NAT规则后，设备在NAT区域5下的TCAM中对此规则进行编程。确认规则已在TCAM中编程。

输出以十六进制表示，因此需要转换为IP地址。

<#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
```

最后，当数据流活跃时，可以通过NAT区域1下的TCAM验证来确认硬件编程。

<#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
```

检验动态NAT

软件验证

确认已配置要将内部IP地址转换到的地址池。

此配置允许将网络192.168.1.0/24转换为地址172.16.10.1到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 "


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#
```

请注意，使用动态NAT时，不会仅使用配置创建任何条目。需要在填充转换表之前创建活动流。

<#root>

```
NAT-Device#

show ip nat translations


<...empty...>
```

检查NAT统计信息。当流量与NAT规则匹配并创建时，NAT命中计数器会增加。

当流量与规则匹配时，NAT未命中计数器会增加，但我们无法创建转换。

<#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
```

确认存在与源和目标的邻接关系

<#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)
```

在确认邻接关系后，如果存在NAT问题，您可以开始进行独立于平台的NAT调试

<#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, flag
*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]
```

您还可以调试FMAN-RP NAT操作：

<#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
```

如果规则因任何原因（例如到期或手动删除）而被删除，则会执行DELETE操作：

<#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
```

硬件验证

检查是否在NAT区域5下的硬件中正确添加了与要转换的流量匹配的NAT规则：

<#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
```

最后，您需要确认活动转换在NAT TCAM区域1中编程正确

<#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

检验动态NAT过载(PAT)

软件验证

用于验证PAT的日志进程与动态NAT相同。您只需要确认正确的端口转换以及在硬件中正确编程端口。

PAT通过附加到NAT规则的“overload”关键字实现。

<#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
```

确认存在与源和目标的邻接关系

<#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)
```

确认当流处于活动状态时，转换已添加到转换表中。请注意，使用PAT时，不会像使用动态NAT时那样创建半条目。

跟踪内部本地地址和内部全局地址上的端口号。

<#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
```

检查NAT统计信息。当流量与NAT规则匹配并创建时，NAT命中计数器会增加。

当流量与规则匹配时，NAT未命中计数器会增加，但我们无法创建转换。

<#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
```

独立于平台的NAT调试显示发生端口转换：

<#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, flag
*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 downl
```

<#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>
```

硬件验证

确认NAT规则已正确安装在NAT区域5下的硬件中

<#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
```

最后，当流处于活动状态时，可以检查NAT流已编程到NAT_Region 1下的硬件TCAM中

<#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
```

数据包级别调试

必须将流中与硬件中的NAT规则匹配的第一个数据包传送到要处理的设备CPU。要查看与传送路径相关的调试输出，您可以启用FED传送路径跟踪到调试级别，以确保数据包传送成功。需要CPU资源的NAT流量进入中转流量CPU队列。

检查传输流量CPU队列是否看到数据包被主动转发到它。

<#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
-------------------------------------------
```

NAT扩展故障排除

当前硬件支持的最大数量NAT TCAM条目，如下表所示：

注意：每个活动NAT转换需要2个TCAM条目。

Platform	TCAM条目的最大数量
Catalyst 9300	5000
Catalyst 9400	14000
Catalyst 9500	14000
Catalyst 9500高性能	15500
Catalyst 9600	15500

如果怀疑存在扩展问题，您可以确认要检查平台限制的TCP/UDP NAT转换总数。

<#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
```

如果您耗尽了NAT TCAM空间，则交换机硬件中的NAT模块无法处理这些转换。在此场景中，需要进行NAT转换的流量将被传送到要处理的设备CPU。

这可能导致延迟，并且可以通过控制平面策略器队列中增加（负责NAT传送流量）的丢弃进行确认。NAT流量进入的CPU队列是“传输流量”。

<#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>
```

确认17.x代码中可用的NAT TCAM空间。此输出来自激活NAT模板的9300，因此空间最大化。

<#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
```

确认16.x代码中可用的NAT TCAM空间。此输出来自带有SDM Access模板的9300，因此NAT TCAM条目的可用空间不会最大化。

<#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
```

通过更改SDM模板以首选NAT，可以增加NAT TCAM的可用硬件空间。这将为TCAM条目的最大数量分配硬件支持。

<#root>

```
NAT-Device#conf t
```

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

sdm prefer nat
```

如果将SDM在转换前后与NAT模板进行比较，您可以确认可用TCAM空间已交换为QoS访问控制条目和基于策略的路由(PBR)ACE。

PBR TCAM是对NAT进行编程的地方。

<#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>
```

仅地址转换(AOT)

AOT是一种机制，当NAT要求仅转换IP地址字段而不是流的第4层端口时，可以使用此机制。如果这符合要求，则AOT可以大大增加硬件中要转换和转发的流的数量。

- 当大部分NAT流发往单个或少量目标集时，AOT最有效。
- 默认情况下禁用AOT。启用后，需要清除当前的NAT转换。

注：仅静态NAT和不包括PAT的动态NAT支持AOT。

这意味着仅允许AOT的NAT配置如下：

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

您可以使用以下命令启用AOT:

<#root>

```
NAT-Device(config)#

no ip nat create flow-entries
```

确认AOT NAT规则已正确编程。此输出来自静态NAT转换。

<#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)
```

通过确认当流变为活动状态时仅对源和目标IP地址进行编程，验证TCAM中的AOT条目。

<#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)
```

相关信息

- Catalyst 9300 17.3.x NAT配置指南
- Catalyst 9400 17.3.x NAT配置指南
- Catalyst 9500 17.3.x NAT配置指南
- Catalyst 9600 17.3.x NAT配置指南
- 技术支持和文档 - Cisco Systems

思科内部 信息

CSCvz46804 增强功能，可在耗尽NAT TCAM资源或无法成功编程NAT条目时添加系统日志。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。