Configure and Verify NAT on Catalyst 9000 Switches

Introduction

This document describes how to configure and validate Network Address Translation (NAT) on the Catalyst 9000 platform.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IP Addressing
- Access Control Lists

Background Information

The most common case for NAT is for use in the translation of private IP network space into globally unique Internet routable addresses.

The device that performs NAT is required to have an interface on the inside network (local) and an interface on the outside network (global).

A NAT device is responsible for the inspection of source traffic to determine if it requires a translation based on the NAT rules configuration.

If a translation is required, the device translates the local source IP address to a globally unique IP address and keep track of this in its NAT translation table.

When packets come back in with a routable address, the device checks its NAT table to see if another translation is in order.

If so, the router translates the inside global address back to the appropriate inside local address and routes the packet.

Components Used

With Cisco IOS® XE 16.12.1 NAT is now available on the Network Advantage license. On all earlier releases, it is available on the DNA Advantage license.

Platform	NAT Feature Introduced
C9300	Cisco IOS® XE Version 16.10.1
C9400	Cisco IOS® XE Version 17.1.1
C9500	Cisco IOS® XE Version 16.5.1a
C9600	Cisco IOS® XE Version 16.11.1

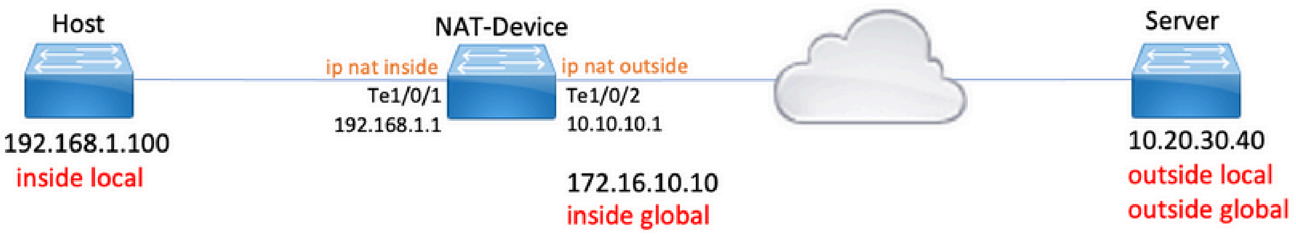
This document is based on the Catalyst 9300 platform with Cisco IOS® XE Version 16.12.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Terminology

Static NAT	Allows for a 1-to-1 mapping of a local address to a global address.
Dynamic NAT	Maps local addresses to a pool of global addresses.
Overload NAT	Maps local addresses to a single global address that uses unique L4 ports.
Inside Local	The IP address assigned to a host on the inside network.
Inside Global	This is the IP address of the inside host as it appears to the outside network. You can think of this as the address that the inside local is translated to.
Outside Local	The IP address of an outside host as it appears to the inside network.
Outside Global	The IP address that is assigned to a host on the outside network. In most cases the outside local and outside global addresses are the same.
FMAN-RP	Feature Manager RP. This is the control plane of Cisco IOS® XE that passes programming information to FMAN-FP.
FMAN-FP	Feature Manager FP. FMAN-FP receives information from FMAN-RP and passes it to FED.
FED	Forwarding Engine Driver. FMAN-FP uses the FED to program information from the control plane into the Unified Access Data Plane (UADP) Application Specific Integrated Circuit (ASIC).

Network Diagram



Configure

Example Configurations

Static NAT configuration to translate 192.168.1.100 (inside local) to 172.16.10.10 (inside global):

<#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
```

Dynamic NAT configuration to translate 192.168.1.0/24 to 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    ---                ---
```

Dynamic NAT Overload (PAT) configuration to translate 192.168.1.0/24 to 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
```

Notice the port increments on the inside global address by 1 for each translation:

<#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
```

Verify Static NAT

Software Verification

It is expected to see half of a translation with static NAT when there is no active flow translated. When the flow becomes active a dynamic translation is created

<#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
```

With the command **show ip nat translations verbose** you can determine the time the flow was created and the amount of time left on the translation.

<#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
```

Check NAT statistics. The NAT hit counter increments when a flow matches a NAT rule and is created.

The NAT miss counter increments when traffic matches a rule but we are unable to create the translation.

<#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
```

For the translation to occur there needs to be an adjacency to the source and destination of the NAT flow. Take note of the adjacency 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)
```

NAT debugs can be enabled to verify the switch receives traffic and if its creates a NAT flow

Note: Note that ICMP traffic that is subject to NAT is always handled in software so the platform debugs do not show logs for ICMP traffic.

<#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]

<snip>
```

When the flow expires or is deleted you see the DELETE action in the debugs:

<#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
```

Hardware Verification

When the NAT rule is configured the device programs this rule in TCAM under NAT Region 5. Confirm the rule is programmed in TCAM.

The outputs are in hex so conversion to IP address is required.

<#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
```

Finally, when the flow becomes active the hardware programming can be confirmed by verification of TCAM under NAT Region 1.

<#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
```

Verify Dynamic NAT

Software Verification

Confirm the pool of addresses to translate inside IP addresses to is configured.

This configuration allows the 192.168.1.0/24 network to be translated to addresses 172.16.10.1 to 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#
```

Notice with dynamic NAT it does not create any entries with only the configuration. An active flow needs to be created before the translation table is populated.

<#root>

```
NAT-Device#
```

```
show ip nat translations
```

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

Check NAT statistics. The NAT hit counter increments when a flow matches a NAT rule and is created.

The NAT miss counter increments when traffic matches a rule but we are unable to create the translation.

<#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
```

Confirm adjacency to source and destination is present

<#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)
```

After adjacencies are confirmed if an issue with NAT is present you can start with platform independent NAT debugs

<#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]
```

You can also debug FMAN-RP NAT operation:

<#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
```

If the rule is removed for any reason such as expiry or manual removal a DELETE action is observed:

<#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
```

Hardware Verification

Check if the NAT rule that matches traffic to be translated is properly added in hardware under NAT region 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
```

Lastly, you need to confirm the active translation is programmed correctly in NAT TCAM Region 1

<#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
```

Verify Dynamic NAT Overload (PAT)

Software Verification

The log processes to verify PAT are the same as dynamic NAT. You just need to confirm the correct port translation and that the ports are programmed correctly in hardware.

PAT is achieved by the "overload" keyword appended to the NAT rule.

<#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
```

Confirm adjacency to source and destination is present

<#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)
```

Confirm the translation is added to the translation table when the flow is active. Notice with PAT there is not a half entry created as it is with Dynamic NAT.

Keep track of the port numbers on the inside local and inside global addresses.

<#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
```

Check NAT statistics. The NAT hit counter increments when a flow matches a NAT rule and is created.

The NAT miss counter increments when traffic matches a rule but we are unable to create the translation.

<#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
```

Platform Independent NAT debugs show the port translation occurs:

```
<#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>
```

Hardware Verification

Confirm the NAT rule is installed properly with in hardware under NAT Region 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
```

Lastly you can check the NAT flow is programmed into hardware TCAM under NAT_Region 1 when the flow is active

<#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

Packet Level Debugs

The first packet in a flow that matches a NAT rule in hardware must be punted to the device CPU to be processed. To view punt path related debug outputs you can enable the FED punt path traces to debug level to ensure the packet is punted. NAT traffic that needs CPU resources goes into the Transit Traffic CPU queue.

Check if the Transit Traffic CPU Queue sees packets actively punted to it.

<#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 Scale Troubleshooting

Current hardware support for maximum number of NAT TCAM entries as illustrated in the table:

Note: Each active NAT translation requires 2 TCAM entries.

Platform	Maximum Number of TCAM Entries
Catalyst 9300	5000
Catalyst 9400	14000
Catalyst 9500	14000
Catalyst 9500 High Performance	15500
Catalyst 9600	15500

If you suspect an issue with scale, you can confirm the number of total TCP/UDP NAT translations to check against a platform limit.

<#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
```

If you have exhausted your NAT TCAM space then the NAT module in the switch hardware is unable to process these translations. In this scenario traffic that is subject to NAT translation is punted to the device CPU to be processed..

This can cause latency and can be confirmed via drops that increment in the control-plane policer queue, which is responsible for NAT punt traffic. The CPU queue where NAT traffic goes is "Transit Traffic".

<#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>
```

Confirm NAT TCAM space available in 17.x code. This output is from a 9300 with the NAT template activated so the space is maximized.

<#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
```

Confirm NAT TCAM space available in 16.x code. This output is from a 9300 with the SDM Access template so the available space for NAT TCAM entries is not maximized.

<#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
```

Available hardware space for NAT TCAM can be increased by a change to the SDM template to prefer NAT. This allocates hardware support for the maximum number of TCAM entries.

<#root>

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

```
sdm prefer nat
```

If you compare SDM before and after conversion to the NAT template you can confirm that usable TCAM space is swapped for QoS Access Control Entries and Policy Based Routing (PBR) ACEs.

PBR TCAM is where NAT is programmed.

<#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>
```

Address Only Translation (AOT)

AOT is a mechanism that can be used when the requirement for NAT is to only translate the IP address field and not the layer 4 ports of a flow. If this meets requirements then AOT can greatly increase the number of flows to be translated and forwarded in hardware.

- AOT is most effective when the majority of NAT flows are destined to a single or small set of destinations.
- AOT is disabled by default. After it is enabled it is required to clear the current NAT translations.

Note: AOT is only supported with static NAT and dynamic NAT that does not include PAT.

This means the only possible NAT configurations that allow for AOT are:

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

You can enable AOT with this command:

<#root>

```
NAT-Device(config)#

no ip nat create flow-entries
```

Confirm the AOT NAT rule is programmed correctly. This output is from a static NAT translation.

<#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)
```

Verify the AOT entry in TCAM through confirmation that only the source and destination IP address is programmed when the flow becomes active.

<#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)
```

Related Information

- Catalyst 9300 17.3.x NAT Configuration Guide
- Catalyst 9400 17.3.x NAT Configuration Guide
- Catalyst 9500 17.3.x NAT Configuration Guide
- Catalyst 9600 17.3.x NAT Configuration Guide
- Technical Support & Documentation - Cisco Systems