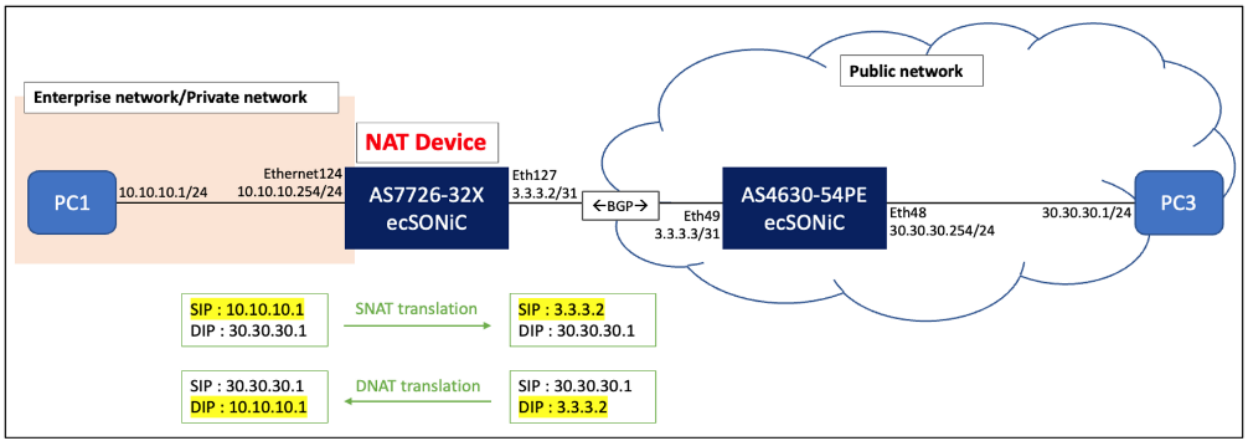
NAT(Network Address Translation)

NAT router enables private IP networks to communicate to the public networks (internet) by translating the private IP address to globally unique IP address. It also provides security by hiding the identity of the host in private network. For external hosts to be able to access the services hosted in the internal network, port address translation rules are added to map the incoming traffic to the internal hosts.

Static NAT

Topology:



Pre-configration:

Assign IP on all DUTs as shown above topology. (refer to the [Edgecore SONiC] Management and front port IPv4/IPv6 Address)

Configure BGP session between AS7726-32X and AS4630-54PE. (refer to the [Edgecore SONiC] BGP Step 1 - Establish BGP Session)

Procedure:

Step 1. Enable the NAT feature on NAT router.

admin@AS7726-32X:~$ sudo config nat feature enable

Step 2. Configure the zone on Ethernet127 as outside interface.

admin@AS7726-32X:~$ sudo config nat add interface Ethernet127 -nat_zone 1

Note:

- NAT zones refer to different network domains between which the NAT translation happens when the packet crosses between them.
- The L3 interface referred to for NAT purposes can be an Ethernet, VLAN or PortChannel or Loopback interface that are configured with IP address(es).
- By default, L3 interface is in NAT zone 0 which we refer to as an inside interface.

Step 3. Create static NAT.

admin@AS7726-32X:~$ sudo config nat add static basic 3.3.3.2 10.10.10.1 -nat_type dnat

Note:

NAT type (snat / dnat) to be applied on the Global IP address. Default value is dnat. This is an optional argument.

- If the "nat_type" is 'dnat':
  DNAT (Destination NAT) translation of the DIP/DPORT in the IP packet from 'global_ip' address and 'global_l4_port' to 'local_ip' address and 'local_l4_port'

  SNAT (Source NAT) translation of the SIP/SPORT in the IP packet from 'local_ip' address and 'local_port' to 'global_l4_ip' address and 'global_l4_port' when the packet crosses the zones.
- If the "nat_type" is 'snat' :
  SNAT translation of the SIP/SPORT in the IP packet from 'global_ip' address and 'global_l4_port' to 'local_ip' address and 'local_l4_port' when the packet crosses the zones.

  DNAT translation of the DIP/DPORT in the IP packet from 'local_ip' address and 'local_l4_port' to 'global_ip' address and 'global_l4_port'.

Step 4. Check the NAT configuration.

admin@AS7726-32X:~$ show nat config

Global Values

Admin Mode : enabled
Global Timeout : 600 secs
TCP Timeout : 86400 secs
UDP Timeout : 300 secs
Static Entries

Nat Type	IP Protocol	Global IP	Global Port	Local IP	Local Port	Twice-NAT Id
dnat	all	3.3.3.2	---	10.10.10.1	---	---

Pool Entries

Pool Name	Global IP Range	Global Port Range

NAT Bindings

Binding Name	Pool Name	Access-List	Nat Type	Twice-NAT Id

NAT Zones

Port	Zone
Ethernet124	0
Ethernet127	1

Step 5. Check NAT HW translation entries.

admin@AS7726-32X:~$ show nat translations

Static NAT Entries 2
Static NAPT Entries 0
Dynamic NAT Entries 0
Dynamic NAPT Entries 0
Static Twice NAT Entries 0
Static Twice NAPT Entries 0
Dynamic Twice NAT Entries 0
Dynamic Twice NAPT Entries 0
Total SNAT/SNAPT Entries 1
Total DNAT/DNAPT Entries 1
Total Entries 2

Protocol	Source	Destination	Translated Source	Translated Destination

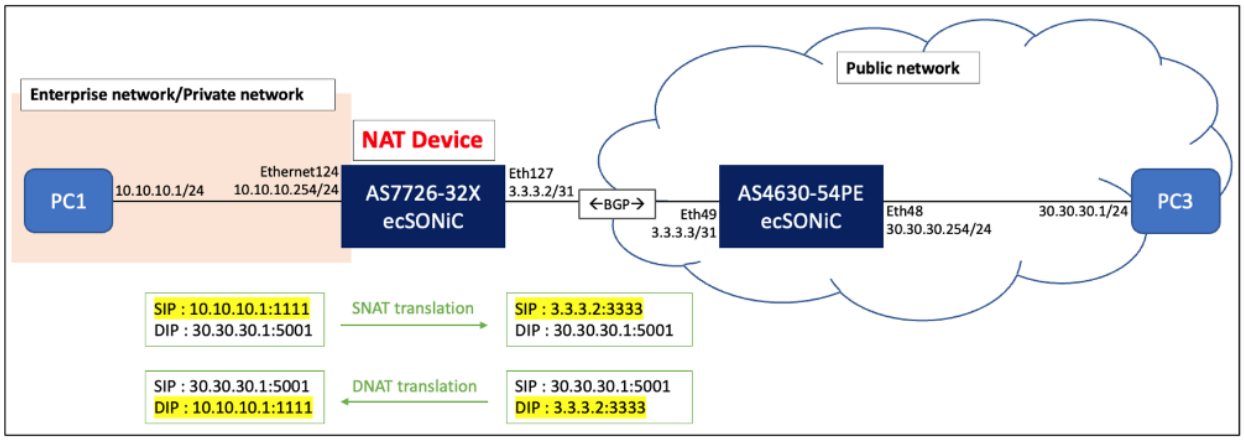
all --- 3.3.3.2 --- 10.10.10.1
all 10.10.10.1 --- 3.3.3.2 ---

Note:

Static NAT/NAPT entries are not timed out from the translation table.

Static NAPT/PAT (Network Address Port Translation/Port Address Translation)

Topology



Pre-configration:

Assign IP on all DUTs as shown above topology. (refer to the [Edgecore SONiC] Management and front port IPv4/IPv6 Address)

Configure BGP session between AS7726-32X and AS4630-54PE. (refer to the [Edgecore SONiC] BGP Step 1 - Establish BGP Session)

Procedure:

Step 1. Enable the NAT feature on NAT router. (Refer to Step1 of Static NAT)

Step 2. Configure the zone on Ethernet127 as outside interface. (Refer to Step2 of Static NAT)

Step 3. Create static NAPT.

admin@AS7726-32X:~$ sudo config nat add static tcp 3.3.3.2 33333 10.10.10.1 11111

Step 4. Check the NAT configuration.

admin@AS7726-32X:~$ show nat config

Global Values

Admin Mode : enabled
Global Timeout : 600 secs
TCP Timeout : 86400 secs
UDP Timeout : 300 secs
Static Entries

Nat Type	IP Protocol	Global IP	Global Port	Local IP	Local Port	Twice-NAT Id
dnat	TCP	3.3.3.2	33333	10.10.10.1	11111	---

Pool Entries

Pool Name	Global IP Range	Global Port Range

NAT Bindings

Binding Name	Pool Name	Access-List	Nat Type	Twice-NAT Id

NAT Zones

Port	Zone
Ethernet124	0
Ethernet127	1

Step 5. Check NAT HW translation entries.

admin@AS7726-32X:~$ show nat translations

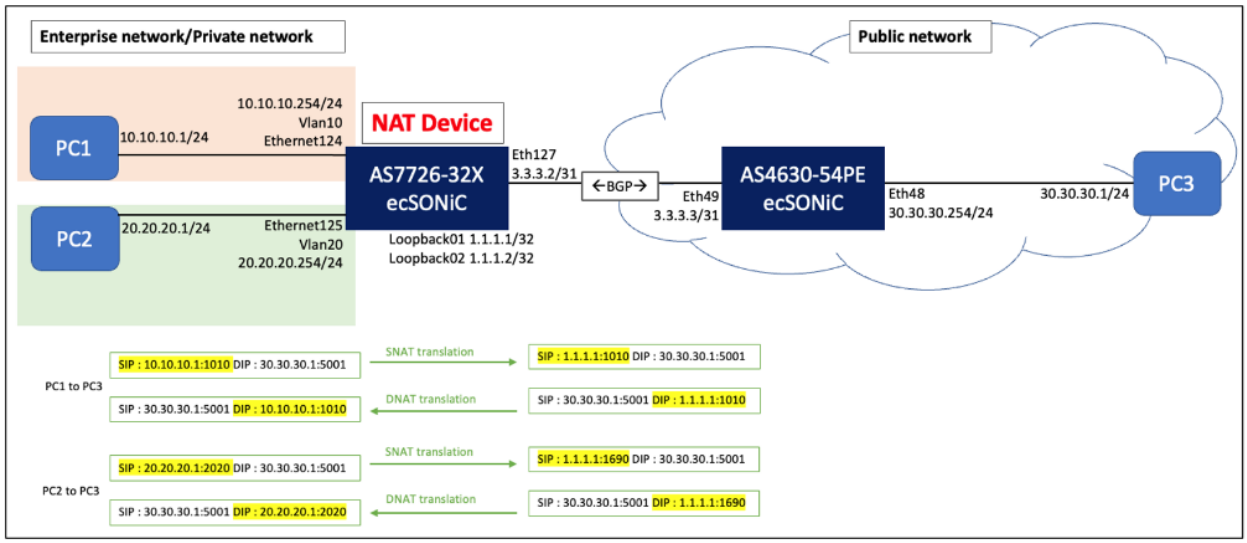
Static NAT Entries 0
Static NAPT Entries 2
Dynamic NAT Entries 0
Dynamic NAPT Entries 0
Static Twice NAT Entries 0
Static Twice NAPT Entries 0
Dynamic Twice NAT Entries 0

```
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries  ..... 1
Total DNAT/DNAPT Entries  ..... 1
Total Entries             ..... 2

Protocol   Source          Destination   Translated Source   Translated Destination
---------- ---------------- ------------ ------------------ ----------------------
tcp        ---              3.3.3.2:33333 ---                10.10.10.1:11111
tcp        10.10.10.1:11111 ---           3.3.3.2:33333      ---
```

Dynamic NAT

Topology



Pre-configration:

Create vlan and assign IP on all DUTs as shown above topology. (refer to the [Edgecore SONiC] VLAN & Inter-VLAN Routing and [Edgecore SONiC] Management and front port IPv4/IPv6 Address)

Configure BGP session between AS7726-32X and AS4630-54PE. (refer to the [Edgecore SONiC] BGP Step 1 - Establish BGP Session)

Procedure:

Step 1. Create loopback interface and assign IP.

```
admin@AS7726-32X:~$ sudo config interface ip add Loopback01 1.1.1.1/32
admin@AS7726-32X:~$ sudo config interface ip add Loopback02 1.1.1.2/32
```

Note:

The Loopback interface IP address is used as the public IP address.

Step 2. Announce Loopback IP in FRR.

```
admin@AS7726-32X:~$ vtysh

Hello, this is FRRouting (version 8.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

AS7726-32X# configure
AS7726-32X(config)# router bgp 65001
AS7726-32X(config-router)# address-family ipv4
AS7726-32X(config-router-af)# network 1.1.1.1/32
AS7726-32X(config-router-af)# network 1.1.1.2/32
```

Step 3. Enable the NAT feature on NAT router.(Refer to Step1 of Static NAT)

Step 4. Configure the zone on Ethernet127 and Loopback interfaces as outside interface.

```
admin@AS7726-32X:~$ sudo config nat add interface Ethernet127 -nat_zone 1
admin@AS7726-32X:~$ sudo config nat add interface Loopback01 -nat_zone 1
admin@AS7726-32X:~$ sudo config nat add interface Loopback02 -nat_zone 1
```

Step 5. Creates the NAT pool for dynamic source NAT.

```
admin@AS7726-32X:~$ sudo config nat add pool A_pool 1.1.1.1-1.1.1.2 1000-2000
```

Step 4. Creates the NAT binding between a pool and an ACL.

```
admin@AS7726-32X:~$ sudo config nat add binding natA A_pool
```

Note:

ACL is an optional argument. If an ACL argument is not given, the NAT binding is applicable to match all traffic.

Step 5. Check the NAT configuration.

admin@AS7726-32X:~$ show nat config

Global Values

Admin Mode : enabled
Global Timeout : 600 secs
TCP Timeout : 86400 secs
UDP Timeout : 300 secs
Static Entries

Nat Type IP Protocol Global IP Global Port Local IP Local Port Twice-NAT Id
---------- ------------ ----------- ------------- ---------- ------------ ---------------
Pool Entries

Pool Name Global IP Range Global Port Range
---------- ----------------- -------------------
A_pool 1.1.1.1-1.1.1.2 1000-2000

NAT Bindings

Binding Name Pool Name Access-List Nat Type Twice-NAT Id
------------- ----------- ------------- ---------- -------------
natA A_pool snat ---
NAT Zones

Port Zone
---------- ------
Ethernet127 1
Loopback01 1
Loopback02 1
Vlan10 0
Vlan20 0

Step 6. Check NAT HW translation entries.

admin@AS7726-32X:~$ show nat translations

Static NAT Entries 0

```
Static NAPT Entries ..... 0
Dynamic NAT Entries ..... 0
Dynamic NAPT Entries ..... 4
Static Twice NAT Entries ..... 0
Static Twice NAPT Entries ..... 0
Dynamic Twice NAT Entries ..... 0
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries ..... 2
Total DNAT/DNAPT Entries ..... 2
Total Entries ..... 4

Protocol  Source  Destination  Translated Source  Translated Destination
--------- ------- ------------ ------------------ ----------------------
tcp       ---     1.1.1.1:1010 ---                10.10.10.1:1010
tcp       ---     1.1.1.1:1690 ---                20.20.20.1:2020
tcp       10.10.10.1:1010 ---  1.1.1.1:1010       ---
tcp       20.20.20.1:2020 ---  1.1.1.1:1690       ---
```

Note:

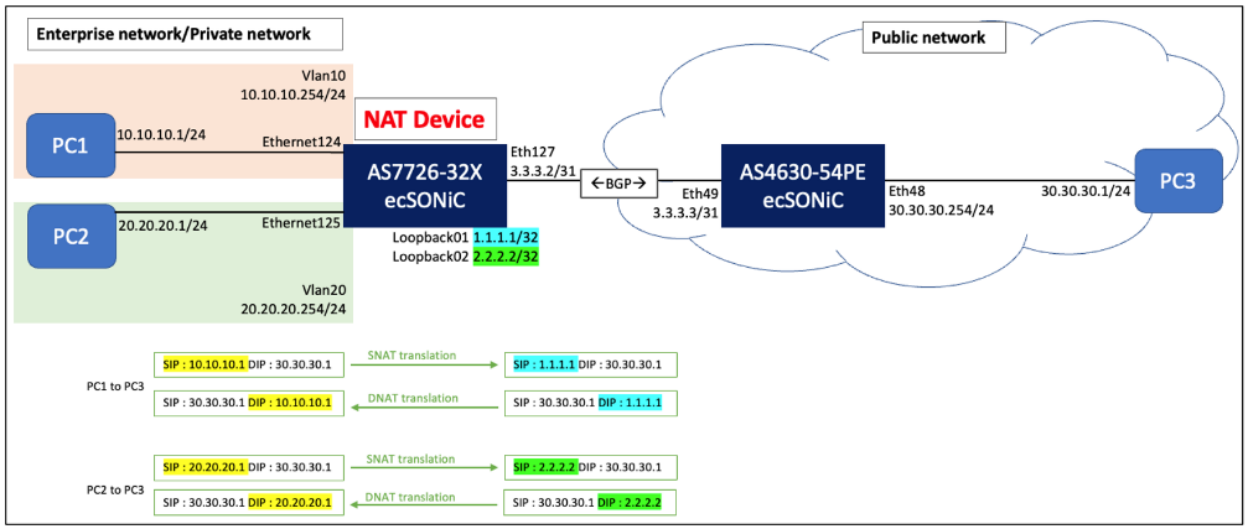
For dynamic NAT/NAPT, the hardware entry is created when:

- 3-way handshaking is established for TCP.
- Received the first packet for UDP.

ICMP protocol is NAT translated in software method. No use any hardware translation entry.

Dynamic NAT with ACL

Topology



Pre-configration:

Create vlan and assign IP on all DUTs as shown above topology. (refer to the [Edgecore SONiC] VLAN & Inter-VLAN Routing and [Edgecore SONiC] Management and front port IPv4/IPv6 Address)

Configure BGP session between AS7726-32X and AS4630-54PE. (refer to the [Edgecore SONiC] BGP Step 1 - Establish BGP Session)

Procedure:

Step 1. Create loopback interface and assign IP.(Refer to Step1 of Dynamic NAT)

Step 2. Announce Loopback IP in FRR.(Refer to Step2 of Dynamic NAT)

Step 3. Create ACL tables and rules to classify hosts.

```
admin@AS7726-32X:~$ sudo config acl add table ACL_A L3  -s  ingress -p Vlan10
admin@AS7726-32X:~$ sudo config acl add table ACL_B L3  -s  ingress -p Vlan20
admin@AS7726-32X:~$ sudo cat ACL.json
{"ACL_RULE": {
      "ACL_A|ACE1": {
        "PRIORITY": "100",
```

```
        "SRC_IP": "10.10.10.0/24",
        "PACKET_ACTION": "forward"
      },
      "ACL_B|ACE1": {
        "PRIORITY": "100",
        "SRC_IP": "20.20.20.0/24",
        "PACKET_ACTION": "forward"
      }
    }
}
admin@AS7726-32X:~$ sudo config load ACL.json -y
Running command: /usr/local/bin/sonic-cfggen -j ACL.json --write-to-db
```

Step 4. Check ACL tables and rules.

```
admin@AS7726-32X:~$ show acl table
Name   Type   Binding   Description   Stage
------ ------ --------- ------------- -------
ACL_A  L3     Vlan10    ACL_A         ingress
ACL_B  L3     Vlan20    ACL_B         ingress

admin@AS7726-32X:~$ show acl rule
Table   Rule     Priority  Action    Match
------- ------ ---------- -------- ---------------------
ACL_A   ACE1         100  forward   SRC_IP: 10.10.10.0/24
ACL_B   ACE1         100  forward   SRC_IP: 20.20.20.0/24
```

Step 5. Enable the NAT feature on NAT router. (Refer to Step1 of Static NAT)

Step 6. Configure the zone on Ethernet127 and Loopback interfaces as outside interface.(Refer to Step2 of Static NAT)

Step 7. Creates two NAT bindings between pools and ACLs.

```
admin@AS7726-32X:~$ sudo config nat add pool pool_A 1.1.1.1
admin@AS7726-32X:~$ sudo config nat add pool pool_B 2.2.2.2
admin@AS7726-32X:~$ sudo config nat add binding natA pool_A ACL_A
admin@AS7726-32X:~$ sudo config nat add binding natB pool_B ACL_B
```

Step 8. Check the NAT configuration.

```
admin@AS7726-32X:~$ show nat config
```

Global Values

Admin Mode : enabled
Global Timeout : 600 secs
TCP Timeout : 86400 secs
UDP Timeout : 300 secs
Static Entries

Nat Type	IP Protocol	Global IP	Global Port	Local IP	Local Port	Twice-NAT Id

Pool Entries

Pool Name	Global IP Range	Global Port Range
pool_A	1.1.1.1	---
pool_B	2.2.2.2	---

NAT Bindings

Binding Name	Pool Name	Access-List	Nat Type	Twice-NAT Id
natA	pool_A	ACL_A	snat	---
natB	pool_B	ACL_B	snat	---

NAT Zones

Port	Zone
Ethernet127	1
Loopback01	1
Loopback02	1
Vlan10	0
Vlan20	0

Step 9. Check NAT HW translation entries.

admin@AS7726-32X:~$ show nat translations

Static NAT Entries 0
Static NAPT Entries 0
Dynamic NAT Entries 4
Dynamic NAPT Entries 0
Static Twice NAT Entries 0
Static Twice NAPT Entries 0
Dynamic Twice NAT Entries 0

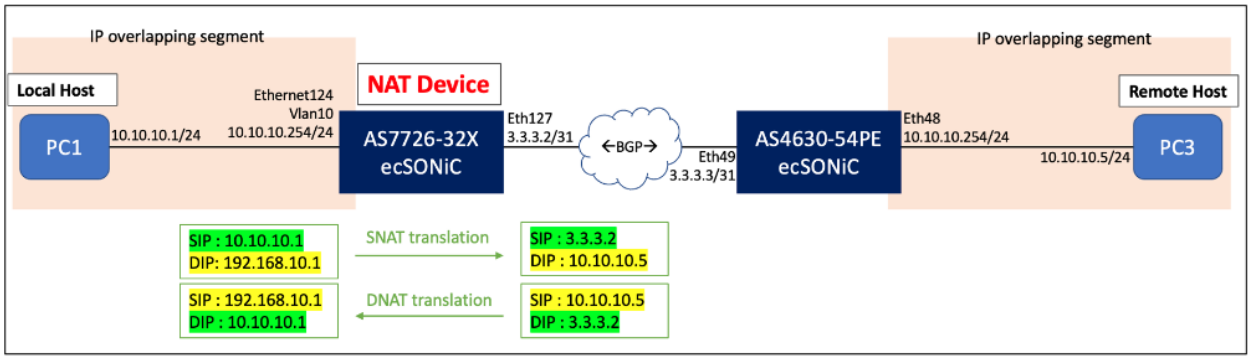
```
Dynamic Twice NAPT Entries ..... 0
Total SNAT/SNAPT Entries  ..... 2
Total DNAT/DNAPT Entries  ..... 2
Total Entries             ..... 4

Protocol   Source      Destination   Translated Source   Translated Destination
---------- ----------  ------------  ------------------  ----------------------
all        20.20.20.1  ---           2.2.2.2             ---
all        10.10.10.1  ---           1.1.1.1             ---
all        ---         2.2.2.2       ---                 20.20.20.1
all        ---         1.1.1.1       ---                 10.10.10.1
```

Twice NAT

Twice NAT or Double NAT is a NAT variation where both the Source IP and the Destination IP addresses are modified as a packet crosses the address zones. It is typically used in the communication between networks with overlapping private addresses.

Topology



Pre-configration:

Create vlan and assign IP on all DUTs as shown above topology. (refer to the [Edgecore SONiC] VLAN & Inter-VLAN Routing and [Edgecore SONiC] Management and front port IPv4/IPv6 Address)

Configure BGP session between AS7726-32X and AS4630-54PE. (refer to the [Edgecore SONiC] BGP Step 1 - Establish BGP Session)

Procedure:

Step 1. Create Static route to PC3 in FRR.

admin@AS7726-32X:~$ vtysh

Hello, this is FRRouting (version 8.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

AS7726-32X#
AS7726-32X# configure
AS7726-32X(config)# ip route 10.10.10.5/32 3.3.3.3

Step 2. Enable the NAT feature on NAT router.(Refer to Step1 of Static NAT)

Step 3. Configure the zone on Ethernet127 as outside interface. (Refer to Step2 of Static NAT)

Step 4. Create static Twice NAT.

admin@AS7726-32X:~$ sudo config nat add static basic 3.3.3.2 10.10.10.1 -nat_type dnat -twice_nat_id 1
admin@AS7726-32X:~$ sudo config nat add static basic 10.10.10.5 192.168.10.1 -nat_type snat -twice_nat_id 1

Note:

When a host matching a dynamic NAT pool binding sends traffic to host with a matching DNAT Static NAT/NAPT entry in the same 'twice_nat_id' group, a bi-directional Twice NAT/NAPT entry is created for the traffic flow.

The Static NAT/NAPT entry that is part of a Twice NAT group is not added used for single NAT'ting in the hardware.

Step 5. Check the NAT configuration.

admin@AS7726-32X:~$ show nat config

Global Values

Admin Mode : enabled
Global Timeout : 600 secs
TCP Timeout : 86400 secs
UDP Timeout : 300 secs

Static Entries

Nat Type	IP Protocol	Global IP	Global Port	Local IP	Local Port	Twice-NAT Id
dnat	all	3.3.3.2	---	10.10.10.1	---	1
snat	all	10.10.10.5	---	192.168.10.1	---	1

Pool Entries

Pool Name	Global IP Range	Global Port Range

NAT Bindings

Binding Name	Pool Name	Access-List	Nat Type	Twice-NAT Id

NAT Zones

Port	Zone
Ethernet127	1
Vlan10	0

Step 6. Check NAT HW translation entries.

admin@AS7726-32X:~$ show nat translations

Static NAT Entries 0
Static NAPT Entries 0
Dynamic NAT Entries 0
Dynamic NAPT Entries 0
Static Twice NAT Entries 2
Static Twice NAPT Entries 0
Dynamic Twice NAT Entries 0
Dynamic Twice NAPT Entries 0
Total SNAT/SNAPT Entries 2
Total DNAT/DNAPT Entries 2
Total Entries 2

Protocol	Source	Destination	Translated Source	Translated Destination
all	10.10.10.1	192.168.10.1	3.3.3.2	10.10.10.5
all	10.10.10.5	3.3.3.2	192.168.10.1	10.10.10.1