iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

APPLICATION NOTE

Network Address Translation using the RAPTOR iMX950

NAT is the process of mapping an internal IP address to an external IP address by changing the IP packets header while in transit through a routing device. NAT helps improve network security and decrease the number of public IP addresses required by an organization.

- NAT gateways sit between two networks, the inside network and the outside network.
- Devices on the inside network are usually assigned IP addresses that cannot be routed to external networks (e.g., networks in the 10.0.0.0/8 block). A few externally valid IP addresses are assigned to the gateway.
- The gateway makes outbound traffic from an inside system appear to be coming from one of the valid external addresses.
- The gateway takes incoming traffic intended for a valid external address and sends it to the correct internal system.
- NAT helps ensure security as each outgoing or incoming traffic request must pass through a translation process that also presents the opportunity to qualify or authenticate incoming streams and match them to outgoing requests.

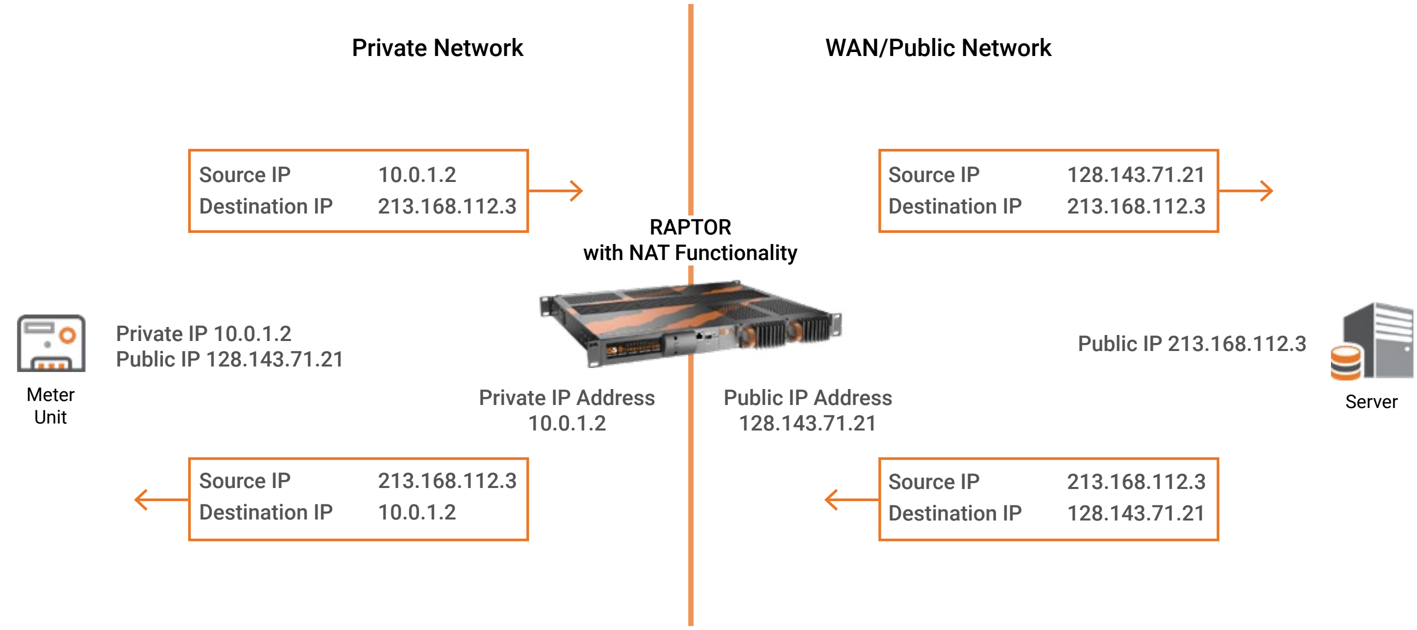
NAT Mechanism (Natting)

- The NAT mechanism (natting) is a router feature and is often part of a Corporate/Control room firewall. NAT gateways can map IP addresses in several ways:
    - From a local IP address to one global IP address statically;
    - From a local IP address to any of a rotating pool of global IP addresses a company may have;
    - From a local IP address plus a particular TCP port to a global IP address or one in a pool of ports;
- NAT devices have an address translation table.

Solution with NAT

- Most devices on the LAN communicate with each other using the inside local addresses (Private Network).
- Some devices on the LAN require to communicate a lot outside the network. These devices have inside global addresses, which means that they do not require translation.
- When a device on the LAN with an inside local address tries to communicate outside the network, the packet goes to one NAT RAPTOR.
- The NAT RAPTOR checks the routing table to see if it has an entry for the destination network. If it does, the NAT RAPTOR then translates the packet and creates an entry for it in the address translation table. The packet is dropped if the destination address is not in the routing table.
- The RAPTOR sends the packet to its destination using an inside global address.
- A device or equipment on the WAN / public network sends a packet to the inside / private network. The source address on the packet is called an outside global address. The destination address is called an inside global address.
- The NAT RAPTOR looks at the address translation table and determines that the destination address is mapped to a device on the LAN network.
- The NAT RAPTOR translates the inside global address of the packet to the inside local address and sends it to the destination computer.

Figure 1.0 — Solution with NAT

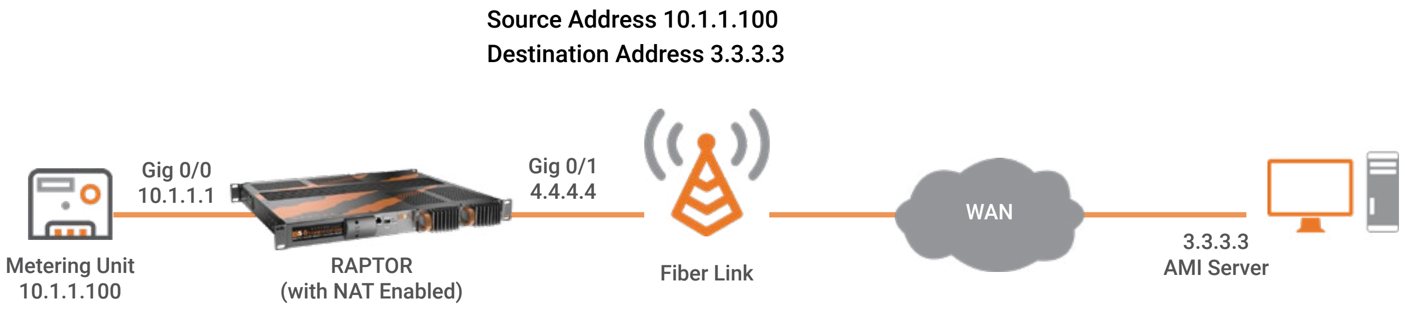


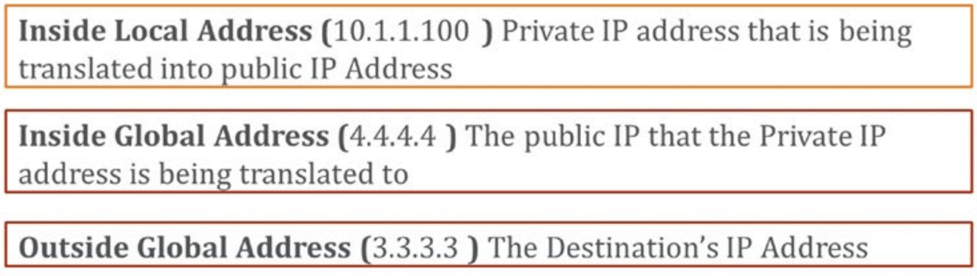
	LOCAL	GLOBAL
INSIDE	An IP address not routable on the internet and refers to a device inside our network	An IP address that is routable on the internet and refers to a device inside our network
OUTSIDE	An IP address not routable on the internet and refers to a device outside our network	An IP address that is routable on the internet and refers to a device outside our network

NAT Type

- Static NAT or one-to-one mapping is when a single private IP address is mapped with a single public IP address.
- Dynamic Translation (IP Masquerading) is when a large number of internal IP addresses are mapped to a single / pool of public IP addresses.
- Port Address Translation (PAT) is also known as NAT overload. Internal /local IP address with a particular TCP port to a global IP address or one in a pool of ports.

Figure 2.0 — Translation Modes





Inside Local Address (10.1.1.100 **)** Private IP address that is being translated into public IP Address

Inside Global Address (4.4.4.4 **)** The public IP that the Private IP address is being translated to

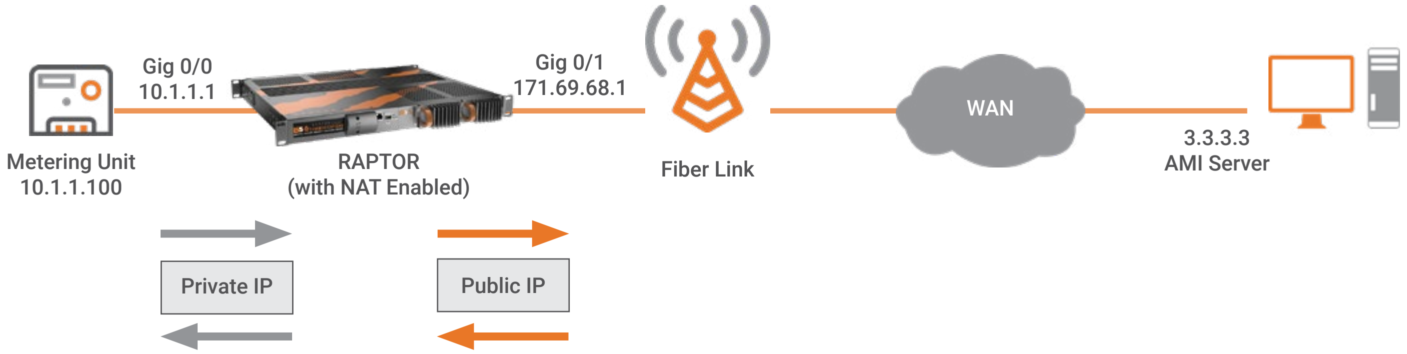
Outside Global Address (3.3.3.3 **)** The Destination's IP Address

Static NAT

- Static NAT is helpful when a network device inside an internal/private network needs to be accessible from the internet or WAN.
- Static translations are always in the translation table and entered directly into the configuration:

  ip nat static 10.1.1.100 171.69.68.10

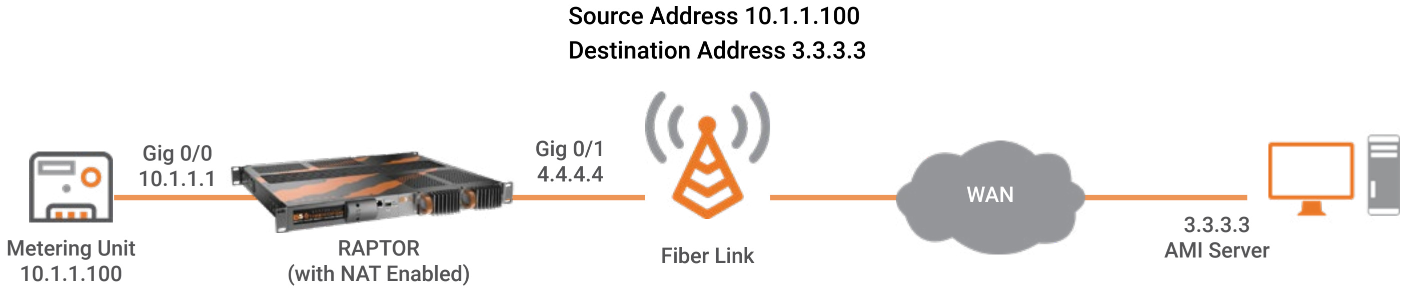
Figure 3.0 — Static NAT Mapping



In this case, we statically tell the router to translate a **single Inside local address** into a **single Inside Global Address**

Internal Metering Unit IP 10.1.1.100 is mapped to 4.4.4.2 (one of the Inside Global addresses from the WAN series IP block)

Figure 4.0 — Static NAT - Inside Local and Global

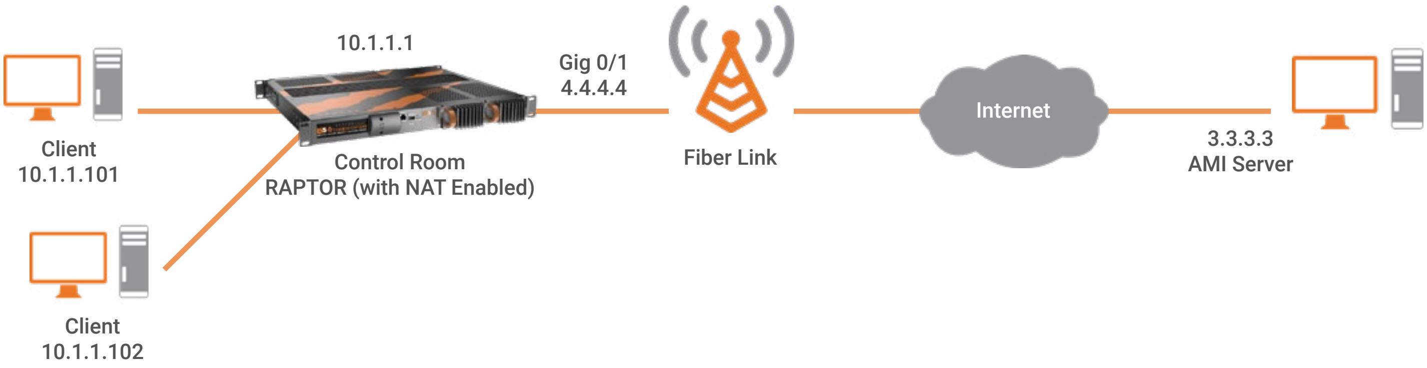


INSIDE GLOBAL	INSIDE LOCAL
4.4.4.2	**10.1.1.100**

Dynamic Translation

- Particular hosts /devices inside the Router / Firewall are identified based on each connection flowing through the firewall.
- A connection doesn't exist until an internal host/device requests a connection through the router /firewall to an external host, and Firewalls open ports only for the addressed host when a connection is established with the external host.
- IP routing could route back in; but, most Routers/ Firewalls block incoming source-routed packets.
- NAT only restricts external hosts from making connections to internal hosts.
- Some TCP /IP /UDP protocols won't work; protocols rely on separate connections back into the local network.

Figure 5.0 — Dynamic Source NAT-1



This type of NAT is where an Inside Local Address is mapped to Inside Global Address mapped from a pool of registered (public) IP addresses.

Typically, the RAPTOR in a network keeps a table of global mapping IP addresses, and when an inside IP address requests access to the internet, the router takes an IP address from the global table that is not at the time being used by another private IP address.

INSIDE LOCAL ADDRESS	INSIDE GLOBAL ADDRESS	OUTSIDE GLOBAL ADDRESS
10.1.1.101	**4.4.4.2**	**3.3.3.3**
10.1.1.102	**4.4.4.3**	**3.3.3.3**

Static versus Dynamic NAT

Static NAT :

- When we need to be able to initiate a connection from both the inside and outside interfaces.
- Or we want a specific host to be translated to a specific IP address.

Dynamic translations:

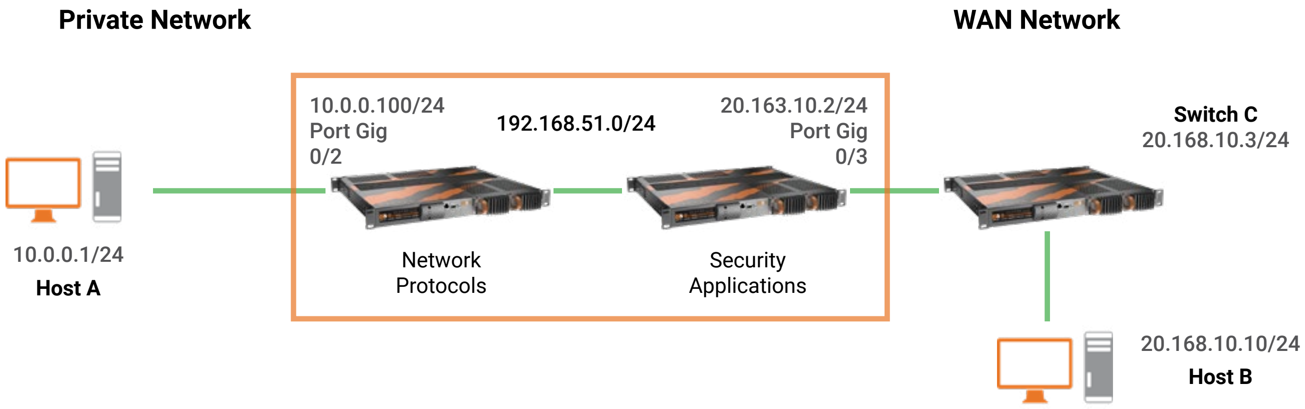
- When we want to initiate a connection from only the inside or only the outside.

Static NAT Configuration

Prerequisite:

The steps needed to enable the iMX950 security features must have been performed. This document assumes that the steps listed in iS5Com-Application-Note_Basics-of-ICS-and-SCADA-Firewall.pdf were performed.

Figure 6.0 — Static NAT LAB



1. From Host A, you should be able to ping Switch C IP 20.168..10.3

For example: ping 20.168.10.3 from Host A (IP 10.0.0.1)

Step result: You should see something similar to the following:

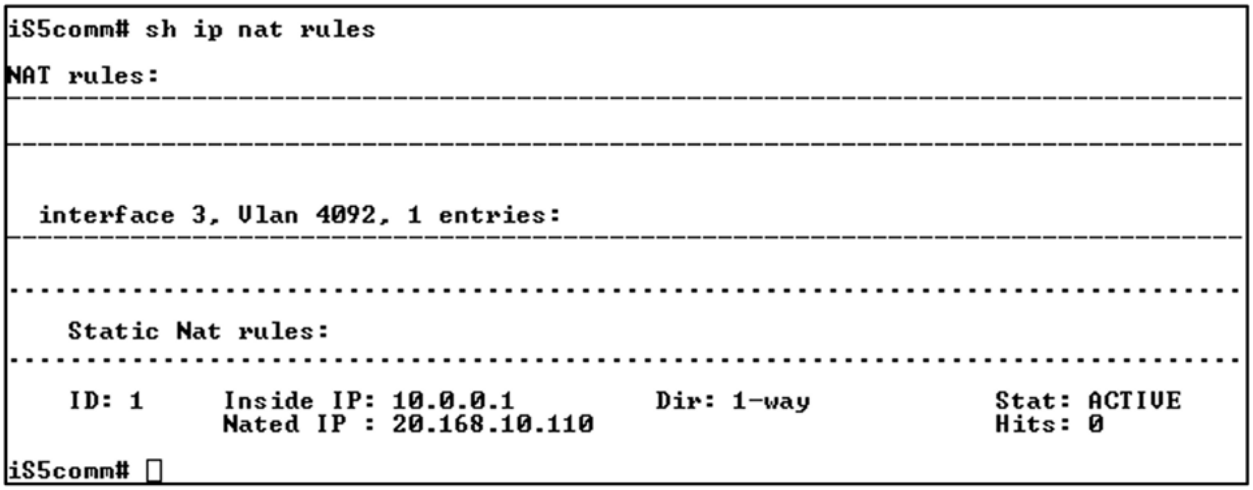
```
C:\>ping 20.168.10.3
Pinging 20.168.10.3 with 32 bytes of data:
Reply from 20.168.10.3: bytes=32 time=3ms TTL=64
Reply from 20.168.10.3: bytes=32 time=1ms TTL=64
Reply from 20.168.10.3: bytes=32 time=1ms TTL=64
Reply from 20.168.10.3: bytes=32 time=1ms TTL=64

Ping statistics for 20.168.10.3:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

2. In this LAB exercise, static NAT is used to map the address 10.0.0.1 to 20.168.10.110.

   a. Execute the following commands:

```
iS5comm# configure terminal
iS5comm(config)# set ip nat enable
iS5comm(config)# interface gigabitethernet 0/3
iS5comm(config-if)# ip nat static 10.0.0.1 20.168.10.110
iS5comm(config-if)# exit
iS5comm(config)# exit
iS5comm# show ip nat rules
```

STEP RESULT: Text similar to the following appears in the terminal:



```
iS5comm# sh ip nat rules
NAT rules:
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------


  interface 3, Vlan 4092, 1 entries:
--------------------------------------------------------------------------------

................................................................................
    Static Nat rules:
................................................................................
    ID: 1      Inside IP: 10.0.0.1          Dir: 1-way              Stat: ACTIVE
               Nated IP : 20.168.10.110                             Hits: 0

iS5comm# 
```

Now ping from **Host B to NATed IP 20.168.10.110**, and you are able to ping that IP

```
C:\>ping 20.168.10.110

Pinging 20.168.10.110 with 32 bytes of data:
Reply from 20.168.10.110: bytes=32 time=6ms TTL=64
Reply from 20.168.10.110: bytes=32 time=5ms TTL=64
Reply from 20.168.10.110: bytes=32 time=6ms TTL=64
Reply from 20.168.10.110: bytes=32 time=4ms TTL=64

Ping statistics for 20.168.10.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 5ms
```

Dynamic SNAT Configuration

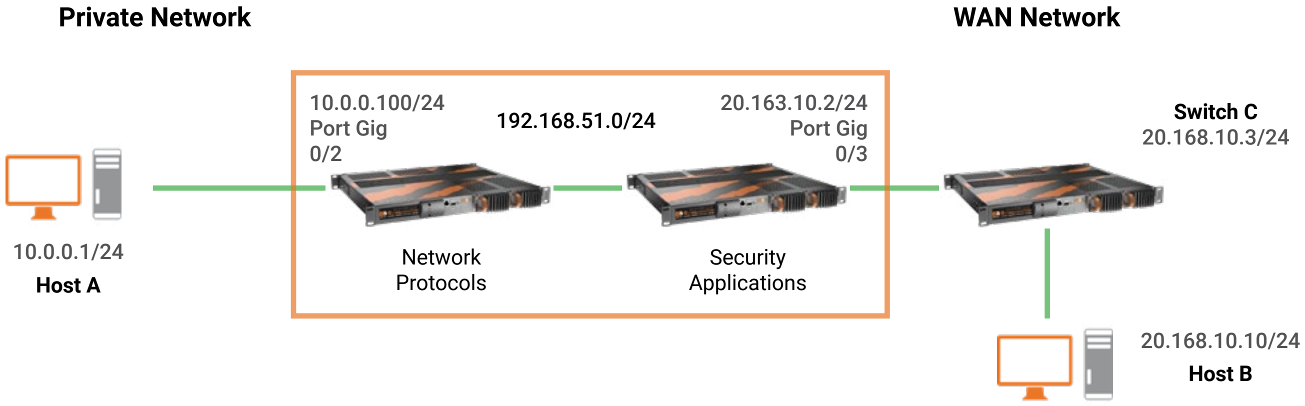
Traffic appears to originate from an IP address on the WAN interface network, even if it originates from an inside network. The IP address is drawn from a pool of IP addresses.

Prerequisite:

The steps needed to enable the iMX950 security features must have been performed. This document assumes that the steps listed in iS5Com-Application-Note_Basics-of-ICS-and-SCADA-Firewall.pdf were performed.

For the LAB exercise, the following network diagram is used:

Figure 7.0 — Dynamic SNAT LAB



1. From Host A (10.0.0.1) should be able to ping Switch C (20.168.10.3)

For example: ping 20.168.10.3

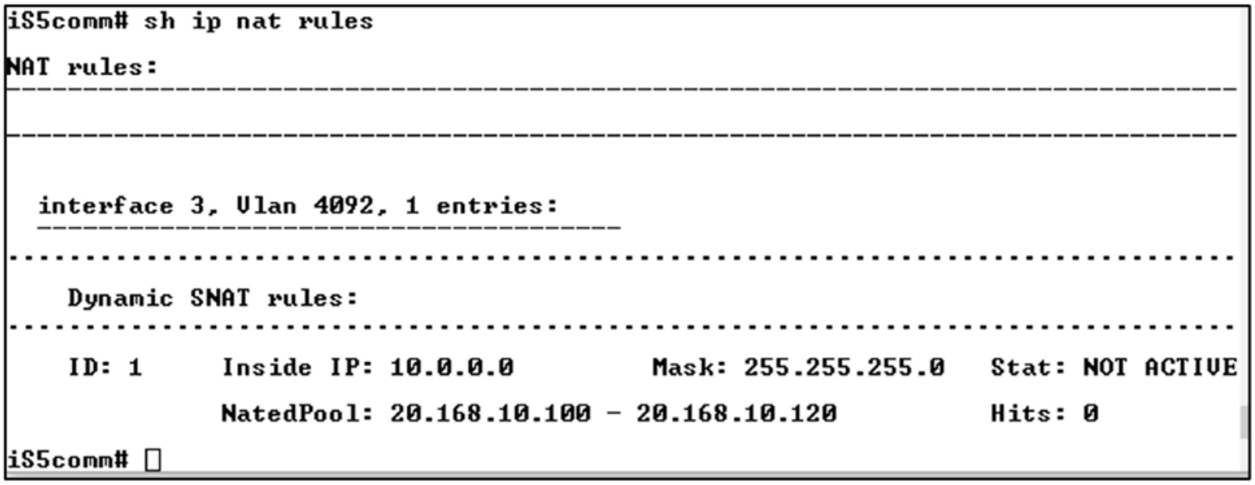
Step result:

```
C:\>ping 20.168.10.3
Pinging 20.168.10.3 with 32 bytes of data:
Reply from 20.168.10.3: bytes=32 time=5ms TTL=64
Reply from 20.168.10.3: bytes=32 time=1ms TTL=64
Reply from 20.168.10.3: bytes=32 time=2ms TTL=64
Reply from 20.168.10.3: bytes=32 time=1ms TTL=64

Ping statistics for 20.168.10.3:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 5ms, Average = 4ms
```

2. Dynamic SNAT is used to map the subnet 10.0.0.0/24 to an address in the range of 20.168.10.100 - 20.168.10.120.

   a. Execute the following commands:

```
iS5comm# configure terminal
iS5comm(config)# set ip nat enable
iS5comm(config)# interface gigabitethernet 0/3
iS5comm(config-if)# ip nat pool 10.0.0.0 255.255.255.0 20.168.10.100 20.168.10.120
iS5comm(config-if)# end
iS5comm# show ip nat rules
```



```
iS5comm# sh ip nat rules
NAT rules:
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------


  interface 3, Vlan 4092, 1 entries:
  --------------------------------------
................................................................................
    Dynamic SNAT rules:
................................................................................
    ID: 1      Inside IP: 10.0.0.0         Mask: 255.255.255.0    Stat: NOT ACTIVE
               NatedPool: 20.168.10.100 - 20.168.10.120           Hits: 0
iS5comm# 
```

3. Test the NAT configuration.

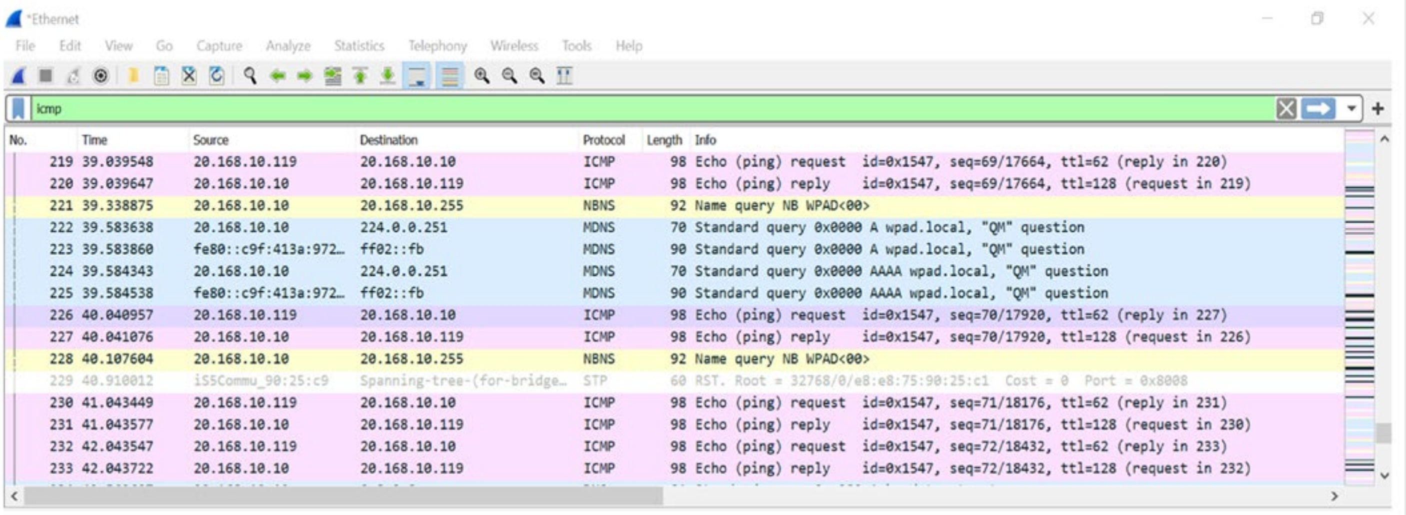
   a. Ping from Host A(10.0.0.1) to Host B(20.168.10.10)

   STEP RESULT: The pings succeed and are received by Host B(20.168.10.10) as if they came from an IP address ranging from 20.168.10.100-120.

   Running a program such as Wireshark on Host B(20.168.10.10) provides evidence of this.

   NOTE: If you want any subnet to be NATted into the address pool and not just the 10.0.0.0/24 network, you could use the following command:

   ip nat pool 0.0.0.0 0.0.0.0 20.168.10.100 20.168.10.120



icmp

```
No.   Time        Source                   Destination              Protocol  Length  Info
  219 39.039548   20.168.10.119            20.168.10.10             ICMP        98 Echo (ping) request  id=0x1547, seq=69/17664, ttl=62 (reply in 220)
  220 39.039647   20.168.10.10             20.168.10.119            ICMP        98 Echo (ping) reply    id=0x1547, seq=69/17664, ttl=128 (request in 219)
  221 39.338875   20.168.10.10             20.168.10.255            NBNS        92 Name query NB WPAD<00>
  222 39.583638   20.168.10.10             224.0.0.251              MDNS        70 Standard query 0x0000 A wpad.local, "QM" question
  223 39.583860   fe80::c9f:413a:972…      ff02::fb                 MDNS        90 Standard query 0x0000 A wpad.local, "QM" question
  224 39.584343   20.168.10.10             224.0.0.251              MDNS        70 Standard query 0x0000 AAAA wpad.local, "QM" question
  225 39.584538   fe80::c9f:413a:972…      ff02::fb                 MDNS        90 Standard query 0x0000 AAAA wpad.local, "QM" question
  226 40.040957   20.168.10.119            20.168.10.10             ICMP        98 Echo (ping) request  id=0x1547, seq=70/17920, ttl=62 (reply in 227)
  227 40.041076   20.168.10.10             20.168.10.119            ICMP        98 Echo (ping) reply    id=0x1547, seq=70/17920, ttl=128 (request in 226)
  228 40.107604   20.168.10.10             20.168.10.255            NBNS        92 Name query NB WPAD<00>
  229 40.910012   iS5Commu_90:25:c9        Spanning-tree-(for-bridge… STP       60 RST. Root = 32768/0/e8:e8:75:90:25:c1  Cost = 0  Port = 0x8008
  230 41.043449   20.168.10.119            20.168.10.10             ICMP        98 Echo (ping) request  id=0x1547, seq=71/18176, ttl=62 (reply in 231)
  231 41.043577   20.168.10.10             20.168.10.119            ICMP        98 Echo (ping) reply    id=0x1547, seq=71/18176, ttl=128 (request in 230)
  232 42.043547   20.168.10.119            20.168.10.10             ICMP        98 Echo (ping) request  id=0x1547, seq=72/18432, ttl=62 (reply in 233)
  233 42.043722   20.168.10.10             20.168.10.119            ICMP        98 Echo (ping) reply    id=0x1547, seq=72/18432, ttl=128 (request in 232)
```

4. Disable the NAT and repeat Step 3.

   a. Execute these commands

   iS5comm# configure terminal

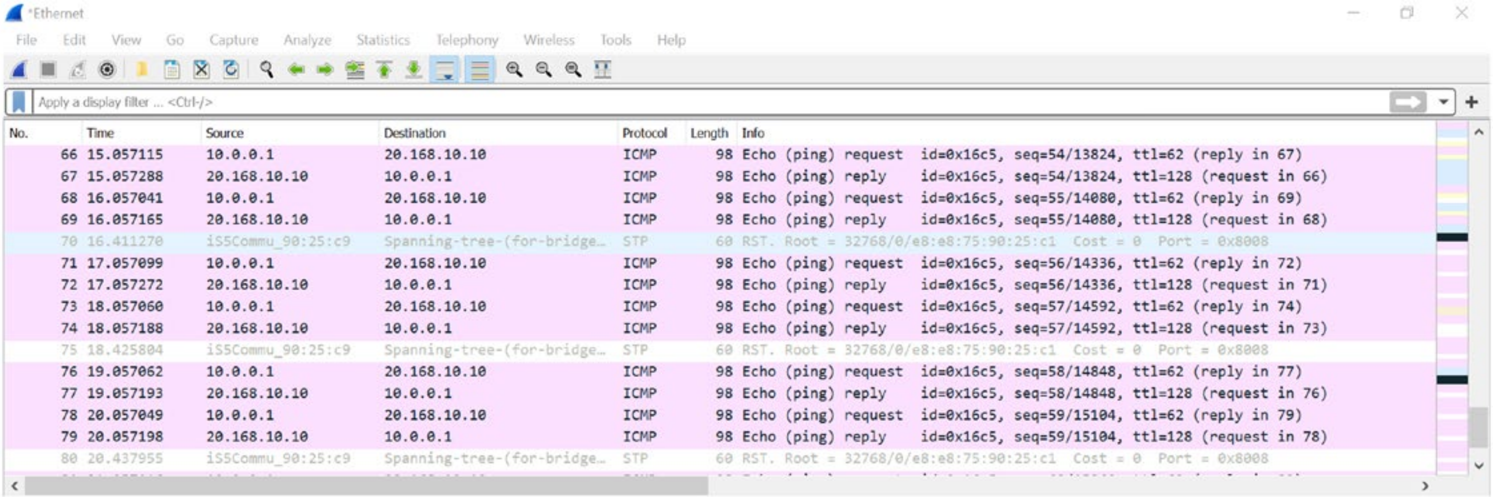
   iS5comm(config)# set ip nat disable

   iS5comm(config)# exit

   iS5comm#

   b. Ping **Host B**(20.168.10.10) from **Host A**(10.0.0.1)

Result: The pings succeed and are received by 20.168.10.10 as if they came from 10.0.0.1



No.	Time	Source	Destination	Protocol	Length	Info
66	15.057115	10.0.0.1	20.168.10.10	ICMP	98	Echo (ping) request id=0x16c5, seq=54/13824, ttl=62 (reply in 67)
67	15.057288	20.168.10.10	10.0.0.1	ICMP	98	Echo (ping) reply id=0x16c5, seq=54/13824, ttl=128 (request in 66)
68	16.057041	10.0.0.1	20.168.10.10	ICMP	98	Echo (ping) request id=0x16c5, seq=55/14080, ttl=62 (reply in 69)
69	16.057165	20.168.10.10	10.0.0.1	ICMP	98	Echo (ping) reply id=0x16c5, seq=55/14080, ttl=128 (request in 68)
70	16.411270	iS5Commu_90:25:c9	Spanning-tree-(for-bridge…	STP	60	RST. Root = 32768/0/e8:e8:75:90:25:c1 Cost = 0 Port = 0x8008
71	17.057099	10.0.0.1	20.168.10.10	ICMP	98	Echo (ping) request id=0x16c5, seq=56/14336, ttl=62 (reply in 72)
72	17.057272	20.168.10.10	10.0.0.1	ICMP	98	Echo (ping) reply id=0x16c5, seq=56/14336, ttl=128 (request in 71)
73	18.057060	10.0.0.1	20.168.10.10	ICMP	98	Echo (ping) request id=0x16c5, seq=57/14592, ttl=62 (reply in 74)
74	18.057188	20.168.10.10	10.0.0.1	ICMP	98	Echo (ping) reply id=0x16c5, seq=57/14592, ttl=128 (request in 73)
75	18.425804	iS5Commu_90:25:c9	Spanning-tree-(for-bridge…	STP	60	RST. Root = 32768/0/e8:e8:75:90:25:c1 Cost = 0 Port = 0x8008
76	19.057062	10.0.0.1	20.168.10.10	ICMP	98	Echo (ping) request id=0x16c5, seq=58/14848, ttl=62 (reply in 77)
77	19.057193	20.168.10.10	10.0.0.1	ICMP	98	Echo (ping) reply id=0x16c5, seq=58/14848, ttl=128 (request in 76)
78	20.057049	10.0.0.1	20.168.10.10	ICMP	98	Echo (ping) request id=0x16c5, seq=59/15104, ttl=62 (reply in 79)
79	20.057198	20.168.10.10	10.0.0.1	ICMP	98	Echo (ping) reply id=0x16c5, seq=59/15104, ttl=128 (request in 78)
80	20.437955	iS5Commu_90:25:c9	Spanning-tree-(for-bridge…	STP	60	RST. Root = 32768/0/e8:e8:75:90:25:c1 Cost = 0 Port = 0x8008

5. To remove Dynamic SNAT perform the following steps.
   a. Execute these commands

```
iS5comm# configure terminal
iS5comm(config)# interface gigabitethernet 0/3
iS5comm(config-if)# no ip nat pool 10.0.0.0 255.255.255.0 20.168.10.100 20.168.10.120
iS5comm(config-if)# exit
iS5comm(config)# exit
```

Result: The Dynamic SNAT configuration is removed.

CONCLUSION

Using the NAT functionality in RAPTOR, we can reuse private IP addresses and enhance security for private substation networks by keeping internal addressing private from external networks.

ABOUT iS5 COMMUNICATIONS INC.

iS5 Communications Inc. (“iS5Com”) is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility sub-stations, roadside transportation, rail, and industrial applications. iS5Com’s services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions.

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

For more information, visit: is5com.com

toll free: +1-844-520-0588 | fax: +1-289-401-5206 | info@is5com.com
technical support: +1-844-475-8324 | support@is5com.com
Address: 5895 Ambler Dr, Mississauga, ON L4W 5B7