Network Address Translation

Network address translation

Network Address Translation (NAT) is a networking feature that ensures smooth and efficient roaming for Automated Guided Vehicles (AGVs) by using a single public IP address for AGVs to access the outside network and assigns port numbers to each application on the AGV, managing data flow for both downstream and upstream directions.

This feature is supported from UIW Release 17.16.1 only.

NAT functionalities

This feature supports the following functionalities:

- NAT with Port Translation (NAPT)
- Source NAT (SNAT)

NAT with Port Translation (NAPT) for downstream traffic manages and routes incoming data packets to the correct inside device. It uses an address table to find a specific application's inside private IP address and port number to forward the packet. For more information, see Downstream Data Flow using NAPT for AGVs.

Source NAT (SNAT) for upstream traffic modifies the source IP address and port numbers of the outgoing packets from inside network devices before sending them to an external network. For more information, see Upstream Data Flow using SNAT for AGVs.

Note

- NAT is supported only in the Layer 2 mode of the AP.
- The NAT/PAT feature supports rules configuration for TCP and UDP traffic only.

Advantage of NAT

A common IP address scheme for on-board vehicle systems reduces the complexity of uniquely identifying all vehicle equipment and facilitates access from external systems.

Downstream data flow using NAPT for AGVs

Downstream data flow using NAPT for AGVs is a network communication process that

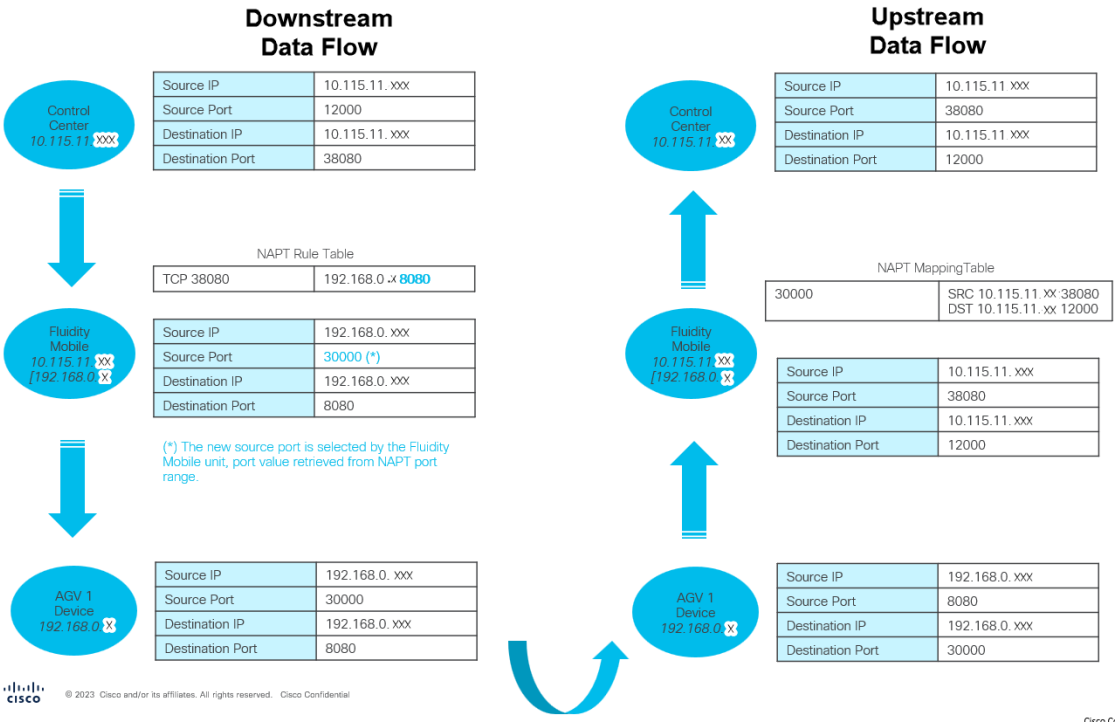
- enables data flow from the outside network to the AGV's inside network
- uses the AP as a gateway between the outside and inside networks
- employs NAPT address tables to find the inside private IP address and port number of specific applications to forward packets.

NAPT functionality for AGVs

By using NAPT:

- Devices from the outside network can connect to services on the AGVs' inside network.
- APs in the AGVs' inside network can direct data flow to specific ports.

Figure 1: Example of downstream data flow using NAPT:



Assign port numbers using NAPT for AGVs

NAPT assigns different port numbers to various services on an AGV. This ensures that responses from the outside network is sent to the correct service on the AGV.

Reserved outside port numbers for NAPT configuration

Protocol / Port Number	Service	Notes
TCP and UDP	—	Port numbers from 1 to 1023 are not allowed on both TCP and UDP protocols.
UDP/1812-1813	RADIUS	—
UDP/6600 UDP/6610	Industrial Wireless Monitor	On-Premises UDP and ping

Protocol / Port Number	Service	Notes
UDP/<telemetry port>	Industrial Wireless Telemetry	• Port number configured for Industrial Wireless Telemetry protocol varies. • The default value configured for Telemetry is 30000.

NAPT rule on AP

A NAPT rule is a network address and port translation rule that sends data flow to specific ports on inside hosts. A typical NAPT rule consists of `<Protocol, Global Destination Port, Translated Local Destination IP, Translated Local Destination Port>`, where the protocol can be either UDP or TCP.

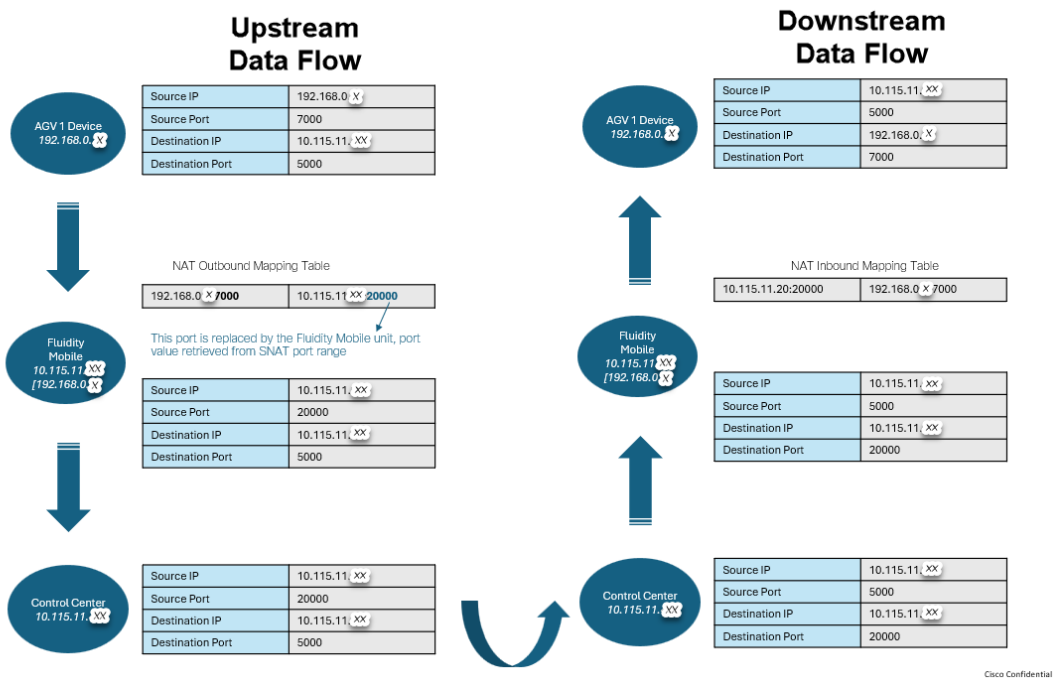
Upstream data flow using SNAT for AGVs

Upstream data flow using Source Network Address Translation (SNAT) for AGVs is a network process that transmits data from the inside network to the outside network through an access point gateway. SNAT modifies outgoing packet headers, changing the source IP address and source port in outgoing packets to match the public IP and port.

Network flow characteristics

The AP serves as a gateway between the inside and outside networks. The AP sends a packet from the inside network to the outside network. SNAT then changes the source IP address and source port in the outgoing packets to match the public IP and port.

Figure 2: Example of upstream data flow using SNAT:



Configure NAPT using CLI

Configure NAPT functionality to enable downstream data flow on the AP.

Perform this task to configure NAPT functionality to enable downstream data flow on the AP.

Procedure

Step 1 Use the **configure ip nat enable** command to enable the NAT rules on the AP.

Example:

```
Device# configure ip nat enable
```

Note
You can use the **configure ip nat disable** command to disable the NAT configuration on the AP.

Step 2 Use the **configure ip nat inside ipv4** *ipv4-address netmask* command to configure inside IPv4 address on the NAT.

Example:

```
Device# configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

Step 3 Use the **configure ip nat inside port range** *first-port-number second-port-number* command to configure inside port range on the NAT.

Example:

```
Device# configure ip nat inside port range 32000 33000
```

Inside port valid range is from 30000 to 35000. This range should not overlap the SNAT range.

Step 4 Use the **configure ip nat entry add proto** {**TCP** | **UDP**} **outside port** *outside-port-number* **inside ipv4** *inside-ipv4-address* **port** *inside-port-number* command to configure protocol, outside port value, inside IPv4 address, and inside port value on the NAT.

Example:

```
Device# configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2 port
8080
```

Step 5 Use the **write** command to save the current configuration.

Example:

```
Device#write
```

Step 6 Use the **reload** command to reload the device.

Example:

```
Device#reload
```

NAPT configuration example

This reference provides the configuration steps for Network Address Port Translation (NAPT) to enable address translation between inside and outside networks with port mapping capabilities.

```
Device# configure ip nat enable
Device# configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device# configure ip nat inside port range 32000 33000
Device# configure ip nat entry add proto TCP outside port 38080 inside ipv4 192.168.0.2
port 8080
Device# write
Device# reload
```

Configure SNAT using CLI

This task enables SNAT functionality to allow upstream data flow on the access point by configuring NAT rules, inside IPv4 addresses, outside port ranges, and saving the configuration.

Perform this task to configure SNAT functionality to enable upstream data flow on the AP.

Follow these steps to configure SNAT using CLI:

Procedure

Step 1 Use the **configure ip nat enable** command to enable the NAT rules on the AP.

Example:

```
Device# configure ip nat enable
```

Note
You can use the configure **ip nat disable** command to disable the NAT configuration on the AP.

Step 2 Use the **configure ip nat inside ipv4** *ipv4-address netmask* command to configure inside IPv4 address on the NAT.

Example:

```
Device# configure ip nat inside ipv4 192.168.70.2 255.255.255.0
```

Step 3 Use the **configure ip nat outside port range** *left-limit-port-number right-limit-port-number* command to configure outside port range on the NAT.

Example:

```
Device# configure ip nat outside port range 22000 23000
```

Outside port valid range is from 20000 to 25000. This range should not overlap the NAPT range.

Step 4 Use the **write** command to save the current configuration.

Example:

```
Device# write
```

Step 5 Use the **reload** command to reload the device.

Example:

```
Device# reload
```

SNAT configuration example

A sample configuration of SNAT to enable network address translation between inside and outside network parameters.

```
Device# configure ip nat enable
Device# configure ip nat inside ipv4 192.168.0.1 255.255.255.0
Device# configure ip nat outside port range 22000 23000
Device# write
Device# reload
```

Delete NAT rule using CLI

This task deletes a specific NAT rule on the AP.

Procedure

Use the **configure ip nat entry del** command to delete the specific NAT rule on the AP.

Example:

```
Device# configure ip nat entry del 0
```

Delete all NAT rules

This task deletes all NAT rules on the AP.

Procedure

Use the **configure ip nat entry del all** command to delete all the NAT rules on the AP.

Example:

```
Device#configure ip nat entry del all
```

Verify NAT configuration using CLI

The **show ip nat config** command displays the status of NAT configuration.

```
Device# show ip nat config
NAT: enabled
IP: 192.168.1.144
Netmask: 255.255.255.0
NAPT port range: 30000-35000
SNAT port range: 22000-23000
TCP timeout: 300
UDP timeout: 300
NAT max rules: 100
```

Verify NAT translations using CLI

The **show ip NAT translations** command displays all the NAT translations.

```
Device# show ip nat translations

NAT: enabled

Port NAT Translations
---------------------

TCP Translations
(192.168.50.4, 4000, 192.168.50.1, 34200) => (10.115.11.157, 4443, 10.115.11.250, 51010)
(10.115.11.250, 51010, 10.115.11.157, 4443) => (192.168.50.1, 34200, 192.168.50.4, 4000)

UDP Translations
None

Source NAT Translations
-----------------------
```

```
TCP Translations
(192.168.50.4, 51178, 10.115.11.250, 4000) => (10.115.11.157, 20292, 10.115.11.250, 4000)
(10.115.11.250, 4000, 10.115.11.157, 20292) => (10.115.11.250, 4000, 192.168.50.4, 51178)

UDP Translations
(10.115.11.250, 3000, 10.115.11.157, 22068) => (10.115.11.250, 3000, 192.168.50.4, 38318)
(192.168.50.4, 38318, 10.115.11.250, 3000) => (10.115.11.157, 22068, 10.115.11.250, 3000)
```