coggle
made for free at coggle.it

# NAT Operation

## IPv4 Private Address Space

There are **not enough public IPv4 addresses** to assign a unique address to each device connected to the Internet.

Networks are commonly implemented using private IPv4 addresses, as defined in **RFC 1918**.

| Start of Range | End of Range | Number of Address Bits Allowed for User Allocation in the Range | Number of Bits in a Mask that uses the Entire Range as a Subnet | Corresponding Subnet Mask |
|---|---|---|---|---|
| 10.0.0.0 | 10.255.255.255 | 24 | 8 | 255.0.0.0 |
| 172.16.0.0 | 172.31.255.255 | 20 | 12 | 255.240.0.0 |
| 192.168.0.0 | 192.168.255.255 | 16 | 16 | 255.255.0.0 |

These private addresses are used within an organization or site to allow devices to communicate locally.

But **private IPv4 addresses cannot be routed over the Internet.**

**To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must first be translated to a public address.**

**NAT** provides the **translation** of private addresses to public addresses.

Without NAT, the exhaustion of the IPv4 address space would have occurred well before the year 2000.

## What is NAT?

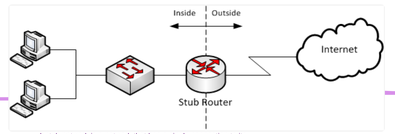
Its primary use is to **conserve public IPv4 addresses.**

NAT has an added benefit of **adding a degree of privacy and security to a network,** because it **hides internal IPv4 addresses** from outside networks.

It does this by allowing networks to use private IPv4 addresses internally and providing translation to a public address only when needed.

NAT-enabled routers can be configured with one or more valid public IPv4 addresses. These public addresses are known as the **NAT pool**.

A NAT router typically operates at the border of a **stub network**.



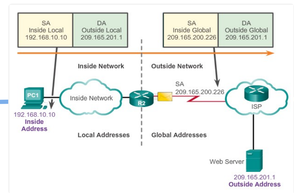

A stub network is a network that has a single connection to its neighboring network, one way in and one way out of the network

The connection to the ISP may use a private address or a public address that is shared among customers.

## NAT Characteristics

### NAT Terminology

In NAT terminology, the **inside network** is the set of networks that is subject to translation. The **outside network** refers to all other networks.




NAT includes four types of addresses:

- **Inside address** - The address of the device which is being translated by NAT.
- **Outside address** - The address of the destination device.
- **Inside local address**: The address of the source as seen from inside the network. In the figure,
- **Inside global address**: The address of source as seen from the outside network.
- **Outside local address**: he address of the destination as seen from the inside network
- **Outside global address**: the address of the destination as seen from the outside network.
- **Local address** - A local address is any address that appears on the inside portion of the network.
- **Global address** - A global address is any address that appears on the outside portion of the network.

**When determining which type of address is used, it is important to remember that NAT terminology is always applied from the perspective of the device with the translated address:**

NAT also uses the concept of local or global with respect to addresses:

### Static NAT

**One-to-one** address mapping between local and global addresses.

These mappings are **configured by the network administrator and remain constant**.

Static NAT is particularly useful for web servers or devices that must have a consistent address that is accessible from the Internet

It is also useful for devices that must be accessible by authorized personnel when offsite (ssh)

**It is also useful for devices that must be accessible by authorized personnel when offsite**

### Dynamic address translation (dynamic NAT)

Dynamic NAT uses a **pool** of public addresses and assigns them on a first-come, first-served basis. **(many-to-many)**

Translations are made on an as-available basis; for example, if there are 100 inside local addresses and 10 inside global addresses, then at any given time only 10 of the 100 inside local addresses can be translated.

**Similar to static NAT, dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.**

### Types of NAT

### Port Address Translation (PAT)

Maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.

For example, if there are 100 inside local addresses and 10 inside global addresses, **PAT uses ports** as an additional parameter to provide a multiplier effect, making it possible to reuse any one of the 10 inside global addresses up to 65,536 times (depending on whether the flow is based on UDP, TCP, or ICMP).

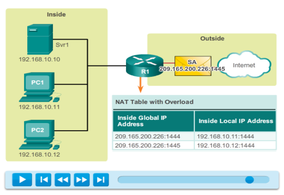
When the NAT router receives a packet from the client, it uses its source port number to uniquely identify the specific NAT translation.

#### Next Available Port

There is a good chance that port numbers may have already been attached to other active sessions.

PAT assigns the first available port number starting from the beginning of the appropriate port group 0–511, 512–1,023, or 1,024–65,535.

When there are no more ports available and there is more than one external address in the address pool, **PAT moves to the next address to try to allocate the original source port.** This process continues until there are no more available ports or external IPv4 addresses.




### Packets without a Layer 4 Segment

PAT translates most common protocols carried by IPv4 that do not use TCP or UDP as a transport layer protocol. The most common of these is **ICMPv4**.

For example, ICMPv4 query messages, echo requests, and echo replies include a **Query ID**

ICMPv4 uses the Query ID to identify an echo request with its corresponding echo reply. The Query ID is incremented with each echo request sent. PAT uses the Query ID instead of a Layer 4 port number.

### Pros and Cons of NAT

#### Advantages of NAT

NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.

NAT increases the flexibility of connections to the public network.

Provides consistency for internal network addressing schemes

Provides the side effect of hiding users and other devices' IPv4 addresses. ( **Some people consider this a security feature, however most experts agree that NAT does not provide security. A stateful firewall is what provides security on the edge of the network.**)

#### Disadvantages of NAT

Performance is degraded: NAT increases forwarding delays because the translation of each IPv4 address within the packet headers takes time.

End-to-end functionality is degraded

End-to-end IP traceability is lost.

Tunneling becomes more complicated: complicates the use of tunneling protocols, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

nitiating TCP connections can be disrupted.

# Configure NAT

Chapter 9 NAT for IPv4

## Configure Static NAT

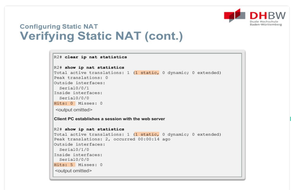
### Configuring Static NAT

There are two basic tasks when configuring static NAT translations.

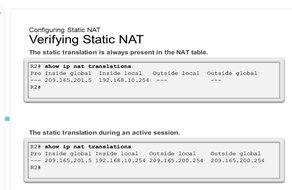
**Step 1. Create a mapping** between the inside local address and the inside global addresses: R1(config)#**ip nat inside source static** ***local-ip global-ip***

**Step 2.** The **interfaces** participating in the translation are configured as **inside or outside** relative to NAT: R1(config-if)#**ip nat inside|outside**

### Verifying Static NAT




**Show ip nat statistics** command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number of addresses that have been allocated.




**show ip nat translations** shows active NAT translations.

To verify that the NAT translation is working, use **clear ip nat translations** to clear statistics from any past translations.

Static translations, unlike dynamic translations, are always in the NAT table.

## Configure Dynamic NAT

Steps:
Create pool
Create ACL

Step 1. Define the **pool** of addresses that will be used for translation using the **ip nat pool** ***name start-ip end-ip*** {**netmask** ***netmask***|**prefix-length** ***prefix-length***}command.
R1(config)#**ip nat pool name** Nat-Pool-1 209.165.200.226 209.165.200.240 **netmask** 255.255.255.224

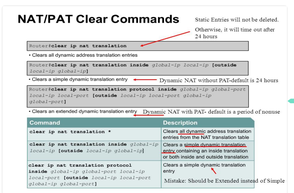
**Step 2.** Configure a standard **ACL** to identify (permit) only those addresses that are to be translated.

**Step 3. Bind the ACL to the pool:**
**ip nat inside source list** ***access-list-number*** **pool** ***pool-name***

**ip nat inside source list 1 pool My-Pool**

**Step 4.** The **interfaces** participating in the translation are configured as **inside or outside** relative to NAT: R1(config-if)#**ip nat inside|outside**

### Verifying Dynamic NAT




## Configure PAT

### Configuring PAT: Address Pool

| | |
|---|---|
| **Step 1** | Define a pool of global addresses to be used for overload translation.<br><br>**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* \| **prefix-length** *prefix-length*} |
| **Step 2** | Define a standard access list permitting the addresses that should be translated.<br><br>**access-list** *access-list-number* **permit** *source* [*source-wildcard*] |
| **Step 3** | Establish overload translation, specifying the access list and pool defined in prior steps.<br><br>**ip nat inside source list** *access-list-number* **pool** *name* **overload** |
| **Step 4** | Identify the inside interface.<br><br>**interface** *type number*<br>**ip nat inside** |
| **Step 5** | Identify the outside interface.<br><br>**interface** *type number*<br>**ip nat outside** |

### Configuring PAT: Single address