Network Address Translation (NAT)

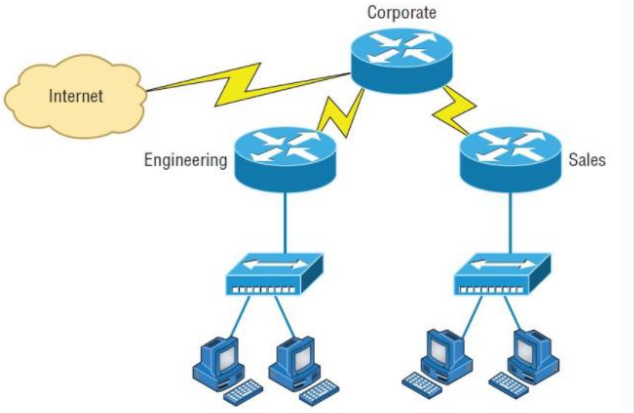
Similar to **Classless Inter-Domain Routing (CIDR)**, the original intention for **NAT** was to *slow the depletion of available IP address space* by allowing many private IP addresses to be represented by some smaller number of public IP addresses. Since then, it's been discovered that NAT is also a useful tool for network migrations and mergers, server load sharing, and creating "virtual servers."

At times, NAT really decreases the overwhelming amount of public IP addresses required in your networking environment. And NAT comes in very handy when two companies that have duplicate internal addressing schemes merge. NAT is also great to have around when an organization changes its ISP and the networking manager doesn't want the hassle of changing the internal address scheme.

Here's a list of situations when it's best to have NAT on your side:

- You need to connect to the Internet and your hosts don't have globally unique IP addresses.
- You change to a new ISP that requires you to renumber your network.
- You need to merge two intranets with duplicate addresses.

You typically use NAT on a border router. See the below figure, where NAT would be configured on the Corporate router.



Where to configure NAT

While NAT has many advantages, it also has disadvantages too.

Advantages	Disadvantages
Conserves legally registered addresses.	Translation introduces switching path delays.
Reduces address overlap occurrences.	Loss of end-to-end IP traceability.
Increases flexibility when connecting to the Internet.	Certain applications will not function with NAT enabled.
Eliminates address renumbering as the network changes.	

Types of NAT

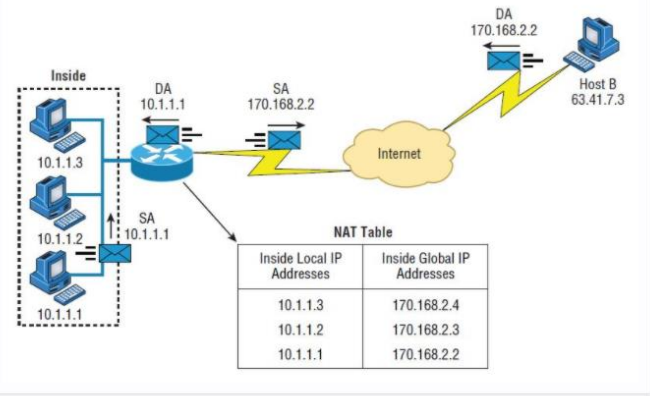
- **Static NAT (SNAT)** - This type of NAT is designed to allow one-to-one mapping between local and global addresses. Keep in mind that the static version requires you to have one real Internet IP address for every host on your network.
- **Dynamic NAT (DNAT)** - This version gives you the ability to map an unregistered IP address to a registered IP address from a pool of registered IP addresses. You don't have to statically configure your router to map an inside-to-an-outside address as you would using static NAT, but you do have to have enough real, bona fide IP addresses for everyone who's going to be sending packets to and receiving them from the Internet.
- **Overloading** - This is the most popular type of NAT configuration. Understand that overloading really is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address—many-to-one—by using different ports. It's also known as **Port Address Translation (PAT)**. And by using PAT (NAT Overload), you get to have thousands of users connect to the Internet using only one real global IP address. NAT Overload is the real reason we haven't run out of valid IP addresses on the Internet.

Match the sentences with the correct definition?

It is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address—many-to-one—by using different ports.	overloading ✔
It gives you the ability to map an unregistered IP address to a registered IP address from a pool of registered IP addresses.	Dynamic NAT (DNAT) ✔
It is designed to allow one-to-one mapping between local and global addresses.	Static NAT (SNAT) ✔

Check

How NAT Works

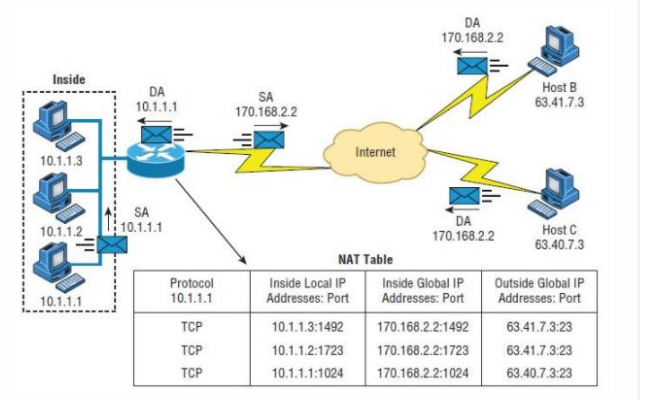


Basic NAT translation

In the above example, host `10.1.1.1` sends an outbound packet to the border router configured with NAT. The router identifies the IP address as an inside local IP address destined for an outside network, translates the address, and documents the translation in the NAT table.

The packet is sent to the outside interface with the new translated source address. The external host returns the packet to the destination host, and the NAT router translates the inside global IP address back to the inside local IP address using the NAT table.

Let's take a look at a more complex configuration using overloading, or what is also referred to as PAT.



NAT overloading example (PAT)

With overloading, all inside hosts get translated to one single IP address, hence the term overloading. Again, the reason we have not run out of available IP addresses on the Internet is because of overloading (PAT).

Take a look at the NAT table in the above figure again. In addition to the inside local IP address and outside global IP address, we now have **port** numbers. These port numbers help the router identify which host should receive the return traffic.

Port numbers are used at the **Transport layer** to identify the localhost in this example. If we had to use IP addresses to identify the source hosts, that would be called static NAT, and we would run out of addresses. PAT allows us to use the **Transport layer** to identify the hosts, which in turn allows us to use (theoretically) up to 65,000 hosts with one real IP address.

Using a router or firewall, you can also perform port forwarding, which is translating the port number of a packet to a new destination. The destination may be a predetermined network port (using an IP protocol, but typically TCP or UDP ports) on a host within a private network behind a NAT router. Based on the received port number, a remote host can communicate to servers behind the NAT gateway to the local network.