Basic Concepts of NAT

Basic overview of NAT

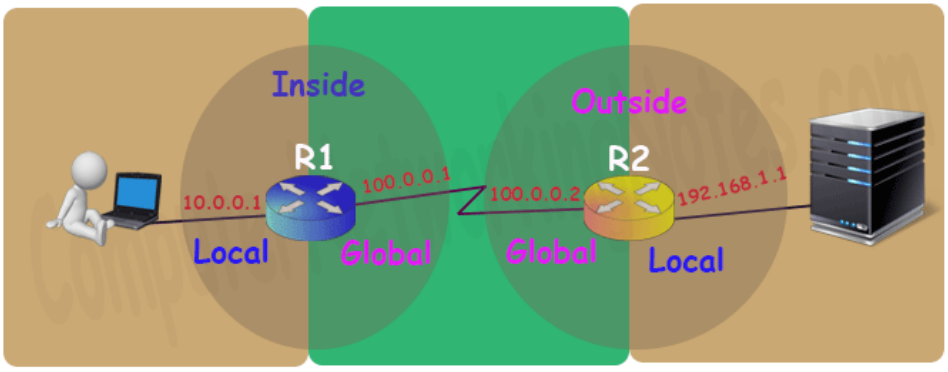
There are several situations where we need address translation such as, a network which do not have sufficient public IP addresses want to connect with the Internet, two networks which have same IP addresses want to merge or due to security reason a network want to hide its internal IP structure from the external world. NAT (Network Address Translation) is the process which translates IP address. NAT can be performed at firewall, server and router.

NAT Terminology

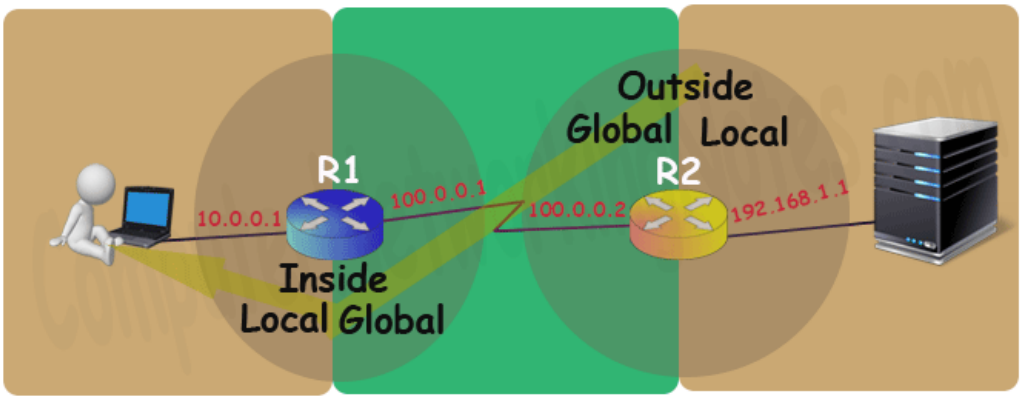
Before we understand NAT in details let's get familiar with four basic terms used in NAT.

Term	Description
Inside Local IP Address	Before translation source IP address located inside the local network.
Inside Global IP Address	After translation source IP address located outside the local network.
Outside Global IP Address	Before translation destination IP address located outside the remote network.
Outside Local IP Address	After translation destination IP address located inside the remote network.

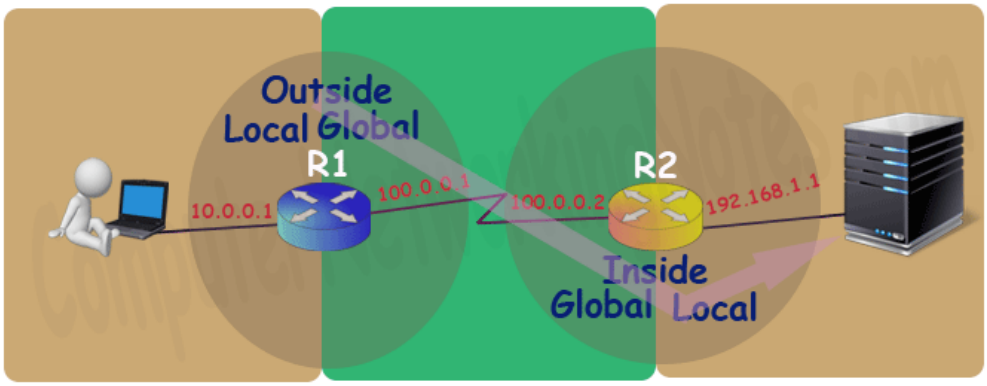
Let's understand these terms with an example. Suppose a user is browsing a website from his home computer. The network which connects his computer with internet is considered as a local network for him. Same as the network which connects the webserver where the website is located with internet is considered as a local network for webserver. The network which connects both networks on internet is considered as a global network.



On router the interface which is connected with local network will be configured with inside local IP address and the interface which is connected with global network will be configured with inside global IP address. Inside and outside depend on where we are standing right now. For example in above network for user router R1 is inside and router R2 is outside.



While for webserver router R2 is inside and router R1 is outside.



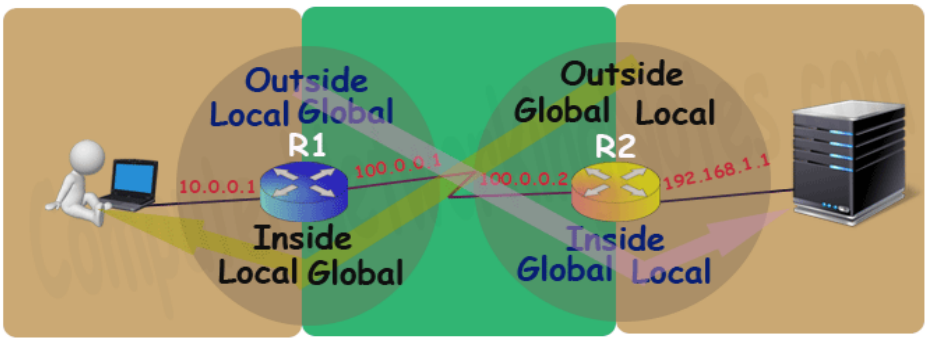
Basically on a NAT enabled router there are two types of interface inside local and inside global.

So, what about outside global and outside local? Well… these terms are used to explain the NAT process theoretically. Practically we never need to configure the outside local and outside global as they sound. For example let's discuss above example once again.

On R1 we will configure inside local address (10.0.0.1) and inside global address (100.0.0.1) which will become outside local address (10.0.0.1) and outside global address (100.0.0.1) for R2 respectively.

Same way on R2 we will configure inside local address (192.168.1.1) and inside global address (100.0.0.2) which will become outside local address (192.168.1.1) and outside global address (100.0.0.2) for R1 respectively.

So practically we only configure inside local and inside global. What is inside for one side is the outside for other side.



Types of NAT

There are three types of NAT; Static NAT, Dynamic NAT and PAT. These types define how inside local IP address will be mapped with inside global IP address.

Static NAT

In this type we manually map each inside local IP address with inside global IP address. Since this type uses one to one mapping we need exactly same number of IP address on both sides.

Dynamic NAT

In this type we create a pool of inside global IP addresses and let the NAT device to map inside local IP address with the available outside global IP address from the pool automatically.

PAT

In this type a single inside global IP address is mapped with multiple inside local IP addresses using the source port address. This is also known as PAT (Port Address Translation) or NAT over load.

Situations where NAT is used

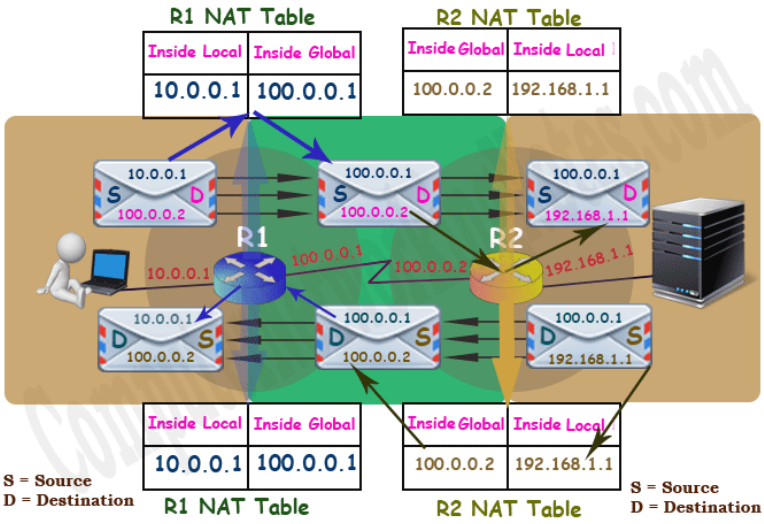
There are no hard and fast rules about where we should use NAT or where we should not use the NAT. Whether we should use the NAT or not is purely depends on network requirement for example NAT is the best solution in following situations: -

- Our network is built with private IP addresses and we want to connect it with internet. As we know to connect with internet we require public IP address. In this situation we can use NAT device which will map private IP address with public IP address.
- Two networks which are using same IP address scheme want to merge. In this situation NAT device is used to avoid IP overlapping issue.

- We want to connect multiple computers with internet through the single public IP address. In this situation NAT is used to map the multiple IP addresses with single IP address through the port number.

How NAT Works

To understand how NAT works, let's take one more example. In this example a user is accessing a web server. User and Webserver both are connected through the NAT devices. Both user and webserver are using private IP addresses which are not routable on the internet. Now let's understand how NAT makes this communication possible.



User generates a data packet for web server. This packet has source address 10.0.0.1 and destination address 100.0.0.2.

Here source address is the correct address but why the packet has destination address 100.0.0.2 instead of actual destination address 192.168.1.1?

When a system needs to connect with the website, it uses DNS server to resolve the IP address of the website. DNS server advertises the global IP address of the website. Outsider can connect with the website through the advertised IP address only. In our example the global IP address of web server is 100.0.0.2. For this reason the packet has the destination address 100.0.0.2 instead of 192.168.1.1.

This packet reaches at R1. Since this packet contains private IP address in source filed which is not routable on internet, R1 has to update the private IP address with a routable public IP address before forwarding this packet.

R1 checks NAT table for available public IP addresses. Depending on what type of NAT (Static, Dynamic or PAT) is configured one routable public IP will be picked from NAT table for this packet.

In our example 100.0.0.1 is picked for this packet. Now R1 will replace 10.0.0.1 with 100.0.0.1 in the source filed of the packet and forward it to the R2.

R2 receives this packet and reads the destination IP address. R2 looks in NAT table to find out the actual IP address of the destination. Since the NAT table of R2 has an entry for the address 100.0.0.2 which maps it with the address 192.168.1.1, R2 will replace the destination address 100.0.0.2 with the address 192.168.1.1 and forward it to the web server.

Webserver will process this packet and reply with its own packet. This packet has source address 192.168.1.1 and destination address 100.0.0.1.

Since webserver received this packet from 100.0.0.1 so it will reply to it instead of 10.0.0.1.

R2 receives this packet. Before forwarding this packet R2 will replace the source IP address with the mapped IP address in NAT table. In this example 192.168.1.1 will be replaced with 100.0.0.2.

R1 receives this packet and checks its destination address. R1 will perform a query in NAT table to figure out the IP address which is associated with this destination IP address. Since this destination IP address 100.0.0.1 is mapped with 10.0.0.1, R1 will replace this destination IP address 100.0.0.1 with 10.0.0.1 and forward it to the PC.

From user's point of view the IP address of the webserver is 100.0.0.2. While from web server's point of view the IP address of the user is 100.0.0.1. This way both user and webserver will never know to whom they are communicating actually.

Advantages and disadvantages of NAT

Nat provides following advantages: -

- NAT solves IP overlapping issue.
- NAT hides internal IP structure from external world.
- NAT allows us to connect with any network without changing IP address.
- NAT allows us to connect multiple computers with internet through the single the public IP address.

NAT has following disadvantages: -

- NAT adds additional delay in network.
- Several applications are not compatible with NAT.
- End to end IP traceability will not work with NAT.
- NAT hides actual end device.