Network Address Translation (NAT)

NAT is the world's largest bandage.

It's purpose is to provide connectivity between hosts that are not located on the same LAN and one or both do not have public IPv4 addresses.

The solution involves a NAT router, which translates IP addresses to permit routing.

The original solution, or traditional NAT, is known, technically, as Unidirectional NAT.

The essence of this solution is that the NAT router replaces the private address of the sending host with a public address. It later reverses the process when it receives a response from the destination host.

See Figure 112: Operation Of Unidirectional (Traditional/Outbound) NAT in the TCP/IP Guide.

Bidirectional NAT

- The NAT router provisions public IP addresses for use with local hosts that have private addresses.
- These public IP addresses are published using a local DNS server.
- Requests to these addresses by external hosts are translated by the NAT router, thereby permitting external hosts to connect to local hosts that have private addresses.

Port-Based, or overloaded, NAT uses port numbers to multiplex private addresses rather than provisioning a public address for each local host.

Overlapping or "Twice NAT" is used when both source and destination addresses are private.

- Such a situation can occur when two local networks are connected due to a corporate merger.
- For example, suppose that each network, being private, was provisioned in the range 192.168.0.0/16, a common strategy.
- A NAT router would need to translate both the source and destination addresses in order permit communication between hosts that are connected to different networks.

Motivation -- NAT was created because of the scarcity of public IPv4 addresses.

Advantages

- Quick and simple solution to the problem of IPv4 address shortage
- Permits greater flexibility and control over the local network
- Some claim that NAT increases security by acting as a firewall. In fact, NAT does not function as a firewall; however, it does impede connectivity, which can prevent some hacker attacks.

Disadvantages:

- Lack of inbound connectivity is the main problem
- It can interfere with certain security protocols, such as IPSec