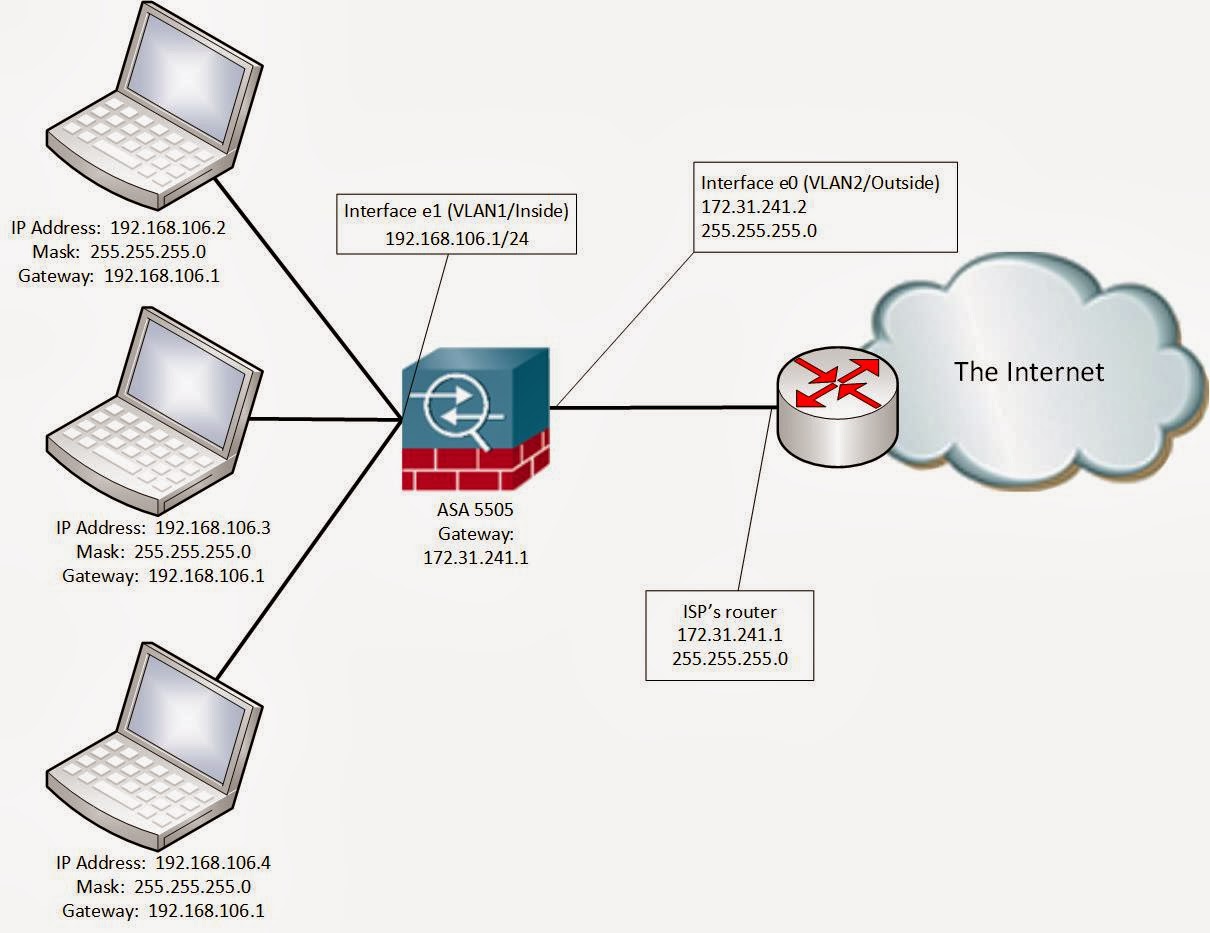
Networking Questionnaire

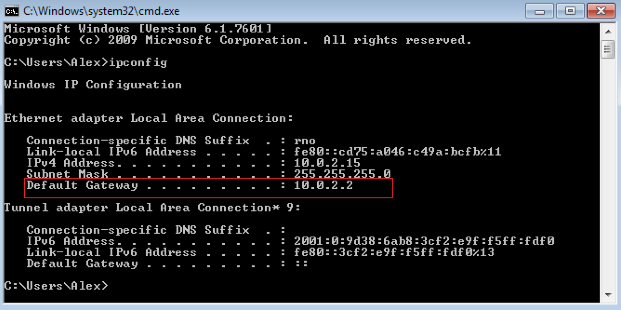
1. Default Gateway in IP

* A default gateway is the node in a computer network using the internet protocol suite that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.
* It serves as an access point or IP router that a networked computer uses to send information to a computer in another network or the internet. Default simply means that this gateway is used by default, unless an application specifies another gateway.
* The default server does not need to be a router; it may be a computer with two network adapters, where one is connected to the local subnet and the other is connected to an outside network.

Sample Gateway through IP 172.31.241.1:



Sample Default Gateway in a host machine/local:



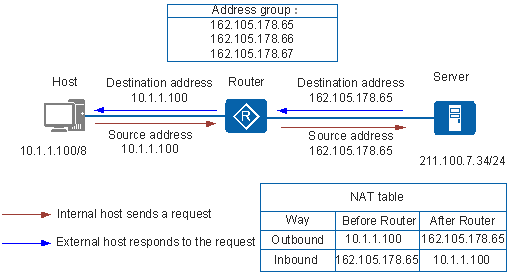
1. NAT -> SNAT and DNAT

NAT (Network Address Translation):

NAT is a process/technology where a router or a similar network device, translates one IP address into another specifically, a router translates an internal host's private IP address into its public IP address for outgoing traffic. It also translates its public IP address to an internal private address for incoming traffic.

* Improves security because internal hosts IP addresses are hidden.
* with IPv4 private addressing scheme conserves IPv4 address space and thus extends its lifespan.

Basic NAT example:



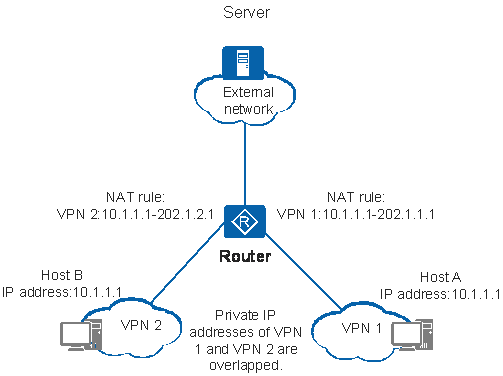
4 Types of NAT:

* Static/Source NAT (SNAT)
* Dynamic/Destination NAT (DNAT)
* Port Address Translation (PAT)
* Port Forwarding
  1. SNAT (Static/Source NAT)

Static NAT indicates that a private IP address is statically bound to a public IP address when NAT is performed. Only this private IP address can be translated to this public IP address.

Static NAPT indicates that the combination of a private IP address, protocol number, and port number is statically bound to the combination of a public IP address, protocol number, and port number. Multiple private IP addresses can be translated to the same public IP address.

Static NAT/NAPT can also translate host IP addresses in the specified private address range to host IP addresses in the specified public address range. When an internal host accesses the external network, static NAT or NAPT translates the IP address of the internal host to a public address if the IP address of the internal host is in the specified address range. An external host can directly access an internal host if the private IP address translated from the IP address of the external host is in the specified internal address range.



* 1. DNAT (Dynamic/Destination NAT)

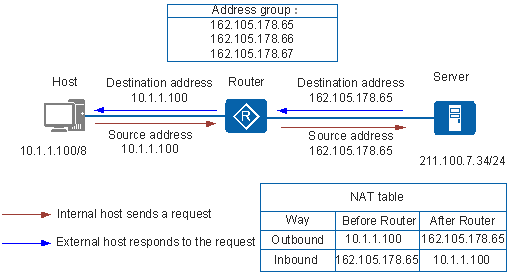
Destination network address translation (DNAT) is most often used to redirect packets destined for a particular IP address, or a specific port on an IP address, on one host to a different address and/or port, possibly on a different host. As this functionality is mostly used to forward packets arriving on a particular port to the same port on a different host it is often also referred to as port-forwarding.

Dynamic NAT translates the private IP address of a device to the public IP address and establishes a mapping between the private and public address. When the response packet reaches the device, the public IP address is translated to the private IP address and then forwarded to the host. In this way, intranet users can access external networks.

To make the DNAT example, and especially the DNAT caveats discussed in the next section, easier to understand let's examine what happens when a packet arrives on the WAN interface destined for an address and port which we have decided to forward.

1. A packet arrives at our public address with that address set as its destination address and its source address set to that of the originating host.
2. The packet traverses the PREROUTING chain of the nat table and encounters our DNAT rule where its destination address is modified to that specified in the --to-destination option.
3. The firewall host makes a routing decision and sends the packet out of the correct interface destined for the address which was just rewritten. The packet's source address is unchanged and still represents the originating host.
4. The packet arrives at the host we specified. This host then generates a response packet which it sends back to the originating host. As the source address was unchanged it should be sent back via the default gateway which will be the firewall host in the previous step.
5. The packet is received by the firewall host which sees that it is destined for the same host which it just performed the DNAT operation for. It therefore modifies the source address of the returning packet so that it looks like it came from the address it was destined for before it was DNATed in step two.
6. The packet arrives at the host which requested it and, as its source address is the same as that to which the original request was sent, is gratefully received.

Provides an almost completely transparent mechanism which enables a host on one network to appear as if it is handling requests when in fact a different host, possibly on a different network, is responding. This makes it ideal when we want to host a variety of services on different machines but only have a single public facing address.



1. IP Assignment

Routers

IP Gateway

Ethernet Switch

ARP table

VLAN Table

MAC Table

RIB/FIB Table

1. ARP:

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a Media Access Control or MAC address.

The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol ([IP](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol)) in use today, an IP address is 32-bits long, but MAC addresses are 48-bits long.

ARP works between network layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer.

ARP can also be used for IP over other LAN technologies, such as token ring, fibre distributed data interface (FDDI) and IP over ATM. In IPv6, which uses 128-bit addresses, ARP has been replaced by the Neighbor Discovery protocol.

**Proxy ARP**

Proxy ARP enables a network proxy to answer ARP queries for IP addresses that are outside the network. This allows packets to be successfully transferred from one [subnetwork](https://searchnetworking.techtarget.com/definition/subnetwork) to another.

When an ARP inquiry packet is broadcast, the [routing table](https://searchnetworking.techtarget.com/definition/routing-table) is examined to find which device on the LAN can reach the destination fastest. This device, which is often a [router](https://searchnetworking.techtarget.com/definition/router), becomes a [gateway](https://internetofthingsagenda.techtarget.com/definition/gateway) for forwarding packets outside the network to their intended destinations.

**ARP spoofing and ARP cache poisoning**

Any LAN that uses ARP must be wary of ARP spoofing, also referred to as ARP poison routing or ARP cache poisoning. ARP spoofing is a [device attack](https://internetofthingsagenda.techtarget.com/definition/device-attack) in which a [hacker](https://searchsecurity.techtarget.com/definition/hacker) broadcasts false ARP messages over a LAN in order to link an attacker's MAC address with the IP address of a legitimate computer or server within the network. Once a link has been established, the target computer can send frames meant for the original destination to the hacker's computer first as well as any data meant for the legitimate IP address.

ARP spoofing can have serious impacts on enterprises. When used in their simplest form, ARP spoofing attacks can steal sensitive information. However, the attacks can also go beyond this and facilitate other malicious attacks, including:

* [man-in-the-middle attacks](https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM)
* [denial-of-service attacks](https://searchsecurity.techtarget.com/definition/denial-of-service)
* [session hijacking](https://searchsoftwarequality.techtarget.com/definition/session-hijacking)