IPv4

- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol and the first version to be widely deployed
- IPv4 is a frequently used communications protocol and is one of the core protocols for the Internet
- IP resides on the network layer of the OSI model

IP Addresses

- IP addresses consist of four octets (8-bits), each between 0 and 255.
- Examples include:
  - 12.5.24.2
  - 127.0.0.1
  - 192.168.3.54
  - 208.32.56.232
- In order for an IP address to function, there must be a properly configured IP address and compatible subnet mask
- To connect to the Internet (or any remote network), you will also need a gateway address and – optionally – a DNS server address

Classful Network Architecture

- The IPv4 classification system is known as a classful network architecture broken down into five sections: Classes A, B, and C are commonly used
- An Class A IP address, the first octet is the "network" portion

Class	IP Range (1st Octet)	Default Subnet Mask	Network ID / Host ID	Networks Possible	Usable Addresses
A	0 – 127	255.0.0.0	Net.Host.Host.Host	2^7 = 128	2^24 – 2 = 16,777,214
B	128 - 191	255.255.0.0	Net.Net.Host.Host	2^14 = 16,384	2^16 – 2 = 65,534
C	192 – 223	255.255.255.0	Net.Net.Net.Host	2^21 = 2,097,151	2^9 -2 = 254
D	224 - 239	N/A	N/A	N/A	N/A
E	240 - 255	N/A	N/A	N/A	N/A

→ IP address is base-10 number system representation, in binary when we say all 0's means 0.0.0.0 and all 1's mean 255.255.255.255

Subnetting

—> Dividing a larger network into small, more manageable sub-networks (subnets)

—> having a network portion and device portion of the device

Loopback Testing

- The range for Class A is 0–127
- The 127 network number isn't used by hosts as a logical IP address Instead, this network is used for *loopback IP addresses*, allowing for testing

—> loopback allows you to basically ping your own machine

ping 127.0.0.1

—> 127 is a loopback address

Usable Address

- Usable addresses are always going to be two less than the mathematical amount.
- The first and last addresses cannot be used
  - For network 172.24.3.X
  - The 0 (in binary) for the host address is the entire network
    - 172.24.3.0
  - The 1s (in binary) for the host address is the broadcast address
    - 172.24.3.255
- Class D and Class E are not used by regular hosts
  - Class D is used for what is known as ***multicasting***—transmitting data to multiple computers (or routers)
  - Class E was reserved for future use, but this has given way to IPv6 instead

IP Conflict

- IP conflicts occur when two devices have been assigned the same IP address
- Windows Error:
  There is an IP address conflict with another system on the network
- If there is an IP address conflict, the devices will have problems sending and receiving data

Public and Private Address

- IPv4 addresses are further classified as either public or private. Public IP addresses are ones that are exposed to the Internet
  - Devices connected to the Internet can potentially communicate with them
- Private IP addresses are hidden from the Internet and any other networks
  - Usually behind an IP proxy or firewall device
- Private Address

Class	Start of Range	End of Range
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Static and dynamic addresses

- Static IP address are addresses that are manually assigned to a host
- Dynamic IP addresses are more common than static IP addresses, whereas they automatically obtain an IP address (and other IP information)

APIPA

- APIPA is an acronym for Automatic Private IP Addressing
- It uses a single Class B network number: 169.254.0.0
- If a Windows client cannot get an IP address from a DHCP server and has not been configured statically, it will auto-assign a number on this network

-> but we can't talk to anyone on internet

-> Computers on local network can communicate though which is the advantage of APIPA

Default Gateway and DNS Server

- For a device to communicate on the Internet, a default gateway and DNS server must be assigned
- Default gateway – Provides a default route for TCP/IP hosts to use when communicating with hosts on remote networks
  The first IP address of the device that a client computer will look for when attempting to gain access outside the local network
- DNS Server – The server that provides name resolution of domain names to IP addresses

——> Default Gateway
Gives the ability to talk to other devices

ipconfig /all

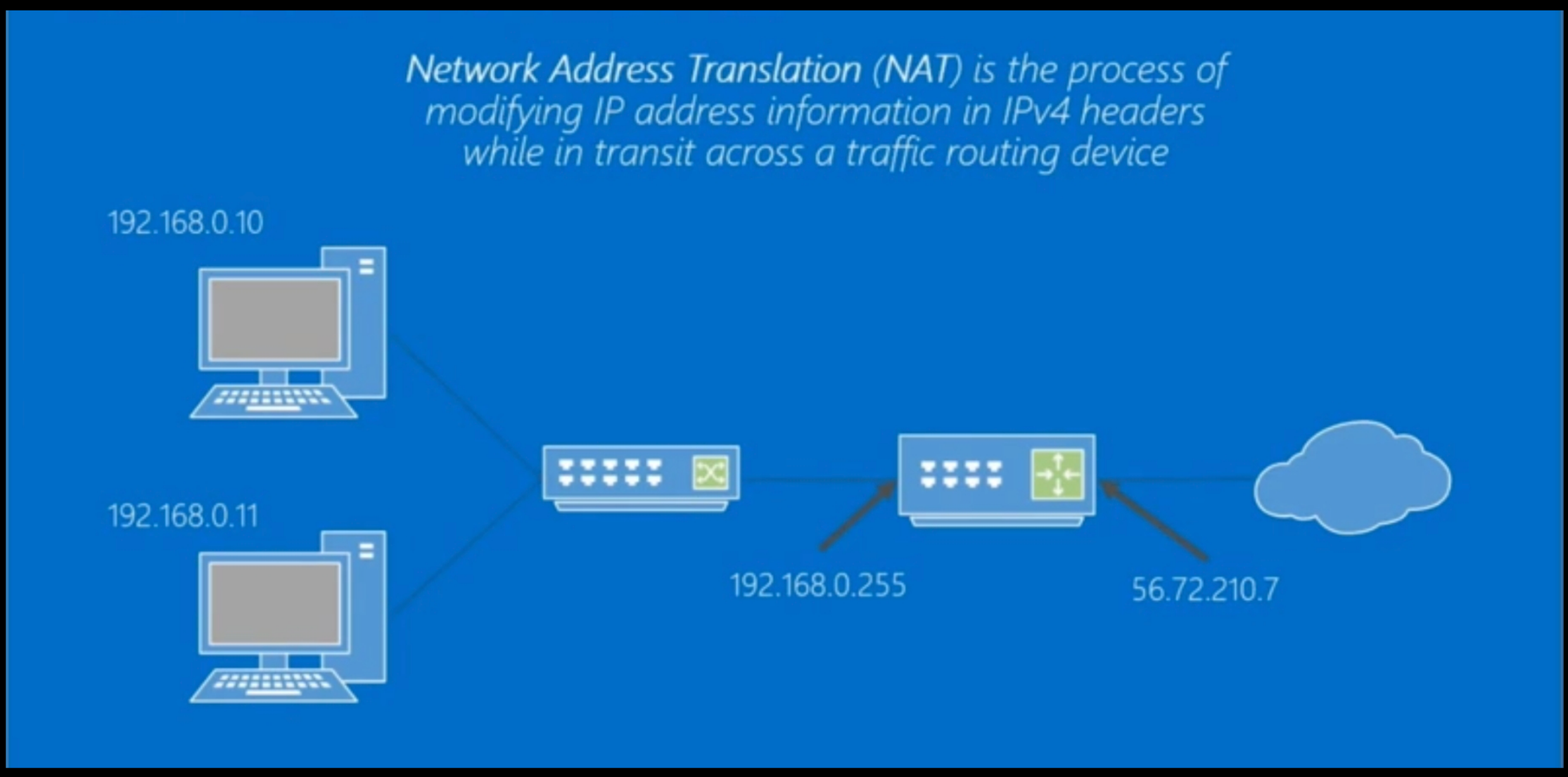
——> gives more details ip addresses, subnet mask and DNS server etc.

Network Address Translation

- Network address translation (NAT) provides a method for translating IPv4 addresses of devices on one network into IPv4 addresses of devices on a different network
- NAT was developed to provide a temporary solution to the IPv4 address issue
- Enables one address space (private) to be re-mapped to another address space, or perhaps re-mapped to a single public IP address

→ allows devices in private network to access internet

→ provides security by hiding internel network structure



→ NAT device translates internel network to internet facing

—> NAT occurs b/w LAN and WAN

Subnetting

- Subnetting is the subdivision of your logical IP network
- By default, all computers are on one subnet or network with no divisions involved.
- My modifying the default subnet mask, you can subnet your network into multiple smaller networks.

Type	Decimal	Binary
Class A	255.0.0.0	11111111.00000000.00000000.00000000
Class B	255.255.0.0	11111111.11111111.00000000.00000000
Class C	255.255.255.0	11111111.11111111.11111111.00000000

Subnet IDs

Subnet ID#	*Subnet ID Binary Equivalent*	*Host IP Range in Binary*	*Host IP in Decimal*
0	0000	0000–1111	0–15 (not recommended)
1	0001	0000–1111	16–31
2	0010	0000–1111	32–47
3	0011	0000–1111	48–63
4	0100	0000–1111	64–79
5	0101	0000–1111	80–95
6	0110	0000–1111	96–111
7	0111	0000–1111	112–127
8	1000	0000–1111	128–143
9	1001	0000–1111	144–159
10	1010	0000–1111	160–175
11	1011	0000–1111	176–191
12	1100	0000–1111	192–207
13	1101	0000–1111	208–223
14	1110	0000–1111	224–239
15	1111	0000–1111	240–255 (not recommended)

NetID	*SubnetID*	*HostID*	*Mask*		*# of Usable Subnets*	*# of Hosts per*
24	0	8	255.255.255.0	/24	N/A	254
24	1	7	255.255.255.128	/25	N/A	N/A
24	2	6	255.255.255.192	/26	2	62
24	3	5	255.255.255.224	/27	6	30
24	4	4	255.255.255.240	/28	14	14
24	5	3	255.255.255.248	/29	30	6
24	6	2	255.255.255.252	/30	62	2
24	7	1	255.255.255.254	/31	N/A	N/A
24	8	0	255.255.255.255	/32	N/A	N/A

IPv6

- IPv6 is the new generation of IP addressing for the Internet
- IPv6 solves many of the limitations of IPv4, including address space and security
- IPv6 addresses are represented as 8 groups of 4 hexadecimal digits
- IPv6 is not backward compatible with IPv4
- IPv6 is a 128-bit system while IPv4 is only a 32-bit system
  - IPv4 allows approximately 4.3 billion IP addresses
  - IPv6 allows 3.4 X 10^38 (340 undecillion) addresses

Types

- Unicast address: Packet is delivered to a single network interface
  There are two types of unicast addresses:
  - Global unicast addresses are routable and displayed directly to the Internet
  - Link local address are automatically configured addresses to communicate with devices on the same link (subnet)
- Anycast address: Identifies multiple interfaces, but the packet is delivered to the nearest of the network interfaces (routing distance)
- Multicast address: Packet is delivered to multiple network interfaces

Components

- IPv6 addresses are broken down into three parts:
  - Site prefix: The first three groups of numbers that define the "network"
  - Subnet ID: Defines the individual subnet of the network that the address is located on
  - Interface ID: The individual host IP portion
  - IPv6 Address: 2001:4860:0000:2001:0000:0000:0000:0068

Site Prefix	Subnet ID	Interface ID
2001.4860.0000 48 bits	2001 16 bits	0000:0000:0000:0068 64 bits

Dual IP Stack ⟶ allows to communicate with the both ipv4 and ipv6 address on local network

- A *dual IP stack* exists when there are two Internet Protocol software implementations in an operating system, one for IPv4 and another for IPv6
- Dual stack IP hosts can run IPv4 and IPv6 independently, or they can use a hybrid implementation, which is the most commonly used method for modern operating systems

IPv4-Mapped Addresses

- IPv4-mapped addresses have the first 80 bits set to 0 (note the double colon), the next 16 set to 1 (shown as ffff), and the last 32 bits populated by the IPv4 address
- These addresses look like IPv6 addresses, other than the last 32 bits, which are written in the customary dot-decimal notation.
- IPv4-mapped IPv6 address for address 10.254.254.1 is ::ffff:10.254.254.1

IPv4 to IPv6 Tunneling

- IPv6 packets can be encapsulated inside IPv4 datagrams.
- In Microsoft operating systems, this is generally done with the Teredo adapter, which is a virtual adapter or "pseudo-interface," not a physical network adapter. An example of one of these addresses would be:

  Fe80::5efe:10.0.0.2%2