IPv4 And IPv6 Addressing
Lecture _3

Asst.Prof. Dr. Abbas Abdulazeez Abdulhameed

College of Science / Computer Department

abbasabdulazeez@uomustansiriyah.edu.iq

Purpose of an IP address

- Unique Identification of:
  - Source
    - How would the recipient know where the message
      came from?
    - How would you know who hacked into your network (network/data security)
  - Destination
    - How would you send data to other network
- Network Independent Format
  - IP over anything

Addressing in Internetworks

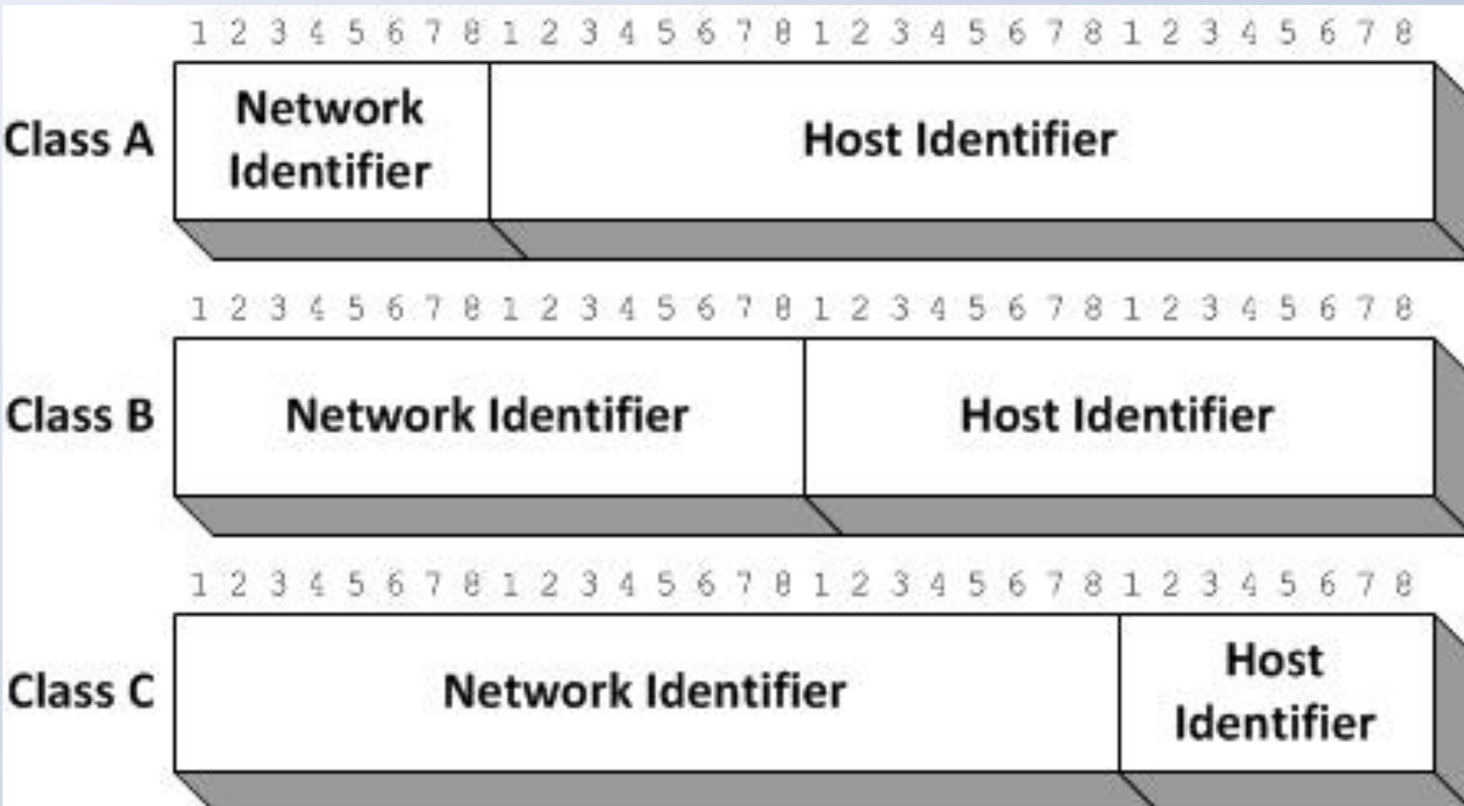
- The problem we have
  - More than one physical network
  - Different Locations
  - Larger number of hosts/computer systems
  - Need a way of numbering them all
- We use a structured numbering system
  - Hosts that are connected to the same physical network may have "similar" IP addresses

IPv4 Addressing

- **IP Address**
  - 32-bit address
  - Four 8-bit decimal values between 0 and 255 separated by periods (octets)
- **Subnet Mask**
  - 32-bit value of 0's and 1's
  - 1's designate network bits, 0's are host bits

		Network	Host
Examples:	IP Address	192.168.43.	100
	Subnet Mask	255.255.255.	0

IPv4 Classful Addressing



The three IPv4 address classes

IPv4 Address Classes

IP Address Class	*Class A*	*Class B*	*Class C*
First bit values (binary)	0	10	110
First byte value (decimal)	0–127	128–191	192–223
Number of network identifier bits	8	16	24
Number of host identifier bits	24	16	8
Number of possible networks	126	16,384	2,097,152
Number of possible hosts	16,777,214	65,534	254

Classless Inter-Domain Routing

- Classful addressing was gradually phased out by a series of subnetting methods, including variable length subnet masking (VLSM) and, eventually, **Classless Inter-Domain Routing (CIDR)**.
- **CIDR** is a subnetting method that enables administrators to place the division between the network bits and the host bits anywhere in the address, not just between octets.

CIDR

CIDR notation: **192.168.43.0/26**

- Where the **/26** means 26 bits of the address are used as the network identifier
- In binary, the subnet mask translates to: **11111111.11111111.1111111.11000000** or **255.255.255.192** in decimal
- This would allow us to divide this address into **4 networks**, each with up to **62 hosts**

CIDR 192.168.43.0/26 Networks

Network Address	***Starting IP Address***	***Ending IP Address***	***Subnet Mask***
192.168.43.0	192.168.43.1	192.168.43.62	255.255.255.192
192.168.43.64	192.168.43.65	192.168.43.126	255.255.255.192
192.168.43.128	192.168.43.129	192.168.43.190	255.255.255.192
192.168.43.192	192.168.43.193	192.168.43.254	255.255.255.192

Public and Private IPv4 Addressing

- Registered IP addresses are not necessary for workstations that merely access resources on the Internet
- The three blocks of addresses allocated for private use are as follows:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

IPv4 Subnetting

- Allows you to split one IP address range into multiple networks (e.g., you can take the 10.0.0.0/8 private IP address range and use the entire second octet as a subnet ID).
- This creates up to 256 subnets with up to 65,536 hosts.
- The subnet masks will be 255.255.0.0 and the network addresses will proceed as follows:
  - 10.0.0.0/16
  - 10.1.0.0/16
  - 10.2.0.0/16
  - …
  - 10.255.0.0/16
- When you are working on an existing network, the subnetting process is more difficult.

Calculate IPv4 Subnets

1. Determine how many subnet identifier bits you need to create the required number of subnets.
2. Subtract the subnet bits you need from the host bits and add them to the network bits.
3. Calculate the subnet mask by adding the network and subnet bits in binary form and converting the binary value to decimal.
4. Take the least significant subnet bit and the host bits, in binary form, and convert them to a decimal value.
5. Increment the network identifier (including the subnet bits) by the decimal value you calculated to determine the network addresses of your new subnets.

Supernetting

- Allows contiguous networks to be added to a routing table with one entry to reduce the size of Internet routing tables.
- For example:

  172.16.43.0/24

  172.16.44.0/24

  172.16.45.0/24

  172.16.46.0/24

  172.16.47.0/24
- Can all be expressed in one supernet address: 172.16.40.0/21

Assigning IPv4 Addresses

To assign IPv4 addresses, there are three basic methods:

- Manual configuration
- Dynamic Host Configuration Protocol (DHCP)
- Automatic Private IP Addressing (APIPA)

Manual IPv4 Address Configuration

- Manually enter IP address, subnet mask, default gateway and DNS servers.
- Use a GUI or command line.
- Not difficult, but it can be time consuming on a large network.
- Difficult to troubleshoot if information is entered incorrectly.

Dynamic Host Configuration Protocol (DHCP)

- Client computers are configured to Obtain an IP address automatically.
- DHCP Servers on the network contain a pool of addresses and other IPv4 configuration.
- Clients request configuration at boot up.
- DHCP Servers respond to the requests.
- IPv4 configurations are leased for a period of time and renewed as necessary.
- No addresses are duplicated.

Automatic Private IP Addressing (APIPA)

- A DHCP failover mechanism used by all current Microsoft Windows operating systems.
- If a system fails to locate a DHCP server on the network, APIPA takes over and automatically assigns an address on the 169.254.0.0/16 network to the computer.
- For a small network that consists of only a single LAN, APIPA is a simple and effective alternative to installing a DHCP server.

IPv6 Addressing

IPv6 Addressing

- Designed to increase the size of the IP address space (128 bit), thus providing addresses for many more devices than IPv4
- Reduces the size of the routing tables because the size of the addresses provides for more than the two levels of subnetting currently possible with IPv4

Introducing IPv6

- IPv6 addresses use a notation called colon-hexadecimal format
- Eight 16-bit hexadecimal numbers, separated by colons:
  XX:XX:XX:XX:XX:XX:XX:XX
- Each X represents eight bits (or 1 byte), which in hexadecimal notation is represented by two characters, as in:
  21cd:0053:0000:0000:e8bb:04f2:003c:c394

Contracting IPv6 Addresses

- When an IPv6 address has two or more consecutive eight-bit blocks of zeroes, you can replace them with a double colon (but you can only use one double colon in any IPv6 address):
  21cd:0053::e8bb:04f2:003c:c394
- You can also remove the leading zeros in any block where they appear:
  21cd:53::e8bb:4f2:3c:c394

Expressing IPv6 Network Addresses

- No subnet masks in IPv6
- Network addresses use the same slash notation as CIDR:

  21cd:53::/64
- This is the contracted form for the following network address:

  21cd:0053:0000:0000/64

IPv6 Address Types

IPv6 supports three address types:

- **Unicast:** Provides one-to-one transmission service to individual interfaces, including server farms sharing a single address. IPv6 supports several types of unicast addresses, including global, link-local, and unique local.
- **Multicast:** Provides one-to-many transmission service to groups of interfaces identified by a single multicast address.
- **Anycast:** Provides one-to-one-of-many transmission service to groups of interfaces, only the nearest of which (measured by the number of intermediate routers) receives the transmission.

Global Unicast Addresses

The current official format for global unicast addresses consists of the following elements:

- **Global routing prefix:** A 48-bit field beginning with the 001 FP value, the hierarchical structure of which is left up to the RIR
- **Subnet ID:** Formerly known as the SLA, a 16-bit field that organizations can use to create an internal hierarchy of sites or subnets
- **Interface ID:** A 64-bit field identifying a specific interface on the network

Subnet IDs

Organizations have a16-bit subnet ID with which to create an internal subnet hierarchy, if desired. Here are some of the possible subnetting options:

- **One-level subnet:** By setting all subnet ID bits to 0, all computers in the organization are part of a single subnet. This option is only suitable for smaller organizations.
- **Two-level subnet:** By creating a series of 16-bit values, you can split the network into as many as 65,536 subnets. This is the functional equivalent of IPv4 subnetting, but with a much larger subnet address space.
- **Multi-level subnet:** By allocating specific numbers of subnet ID bits, you can create multiple levels of subnets, sub-subnets, and sub-sub-subnets; suitable for an enterprise of almost any size.

Subnet ID Example

To support a large international enterprise, you could split the subnet ID as follows:

- **Country (4 bits):** Creates up to 16 subnets representing countries in which the organization has offices
- **State (6 bits):** Creates up to 64 sub-subnets within each country, representing states, provinces, or other geographical divisions
- **Office (2 bits):** Creates up to 4 sub-sub-subnets within each state or province, representing offices located in various cities
- **Department (4 bits):** Creates up to 16 sub-sub-sub-subnets within each office, representing the various departments or divisions.

To create a subnet ID for a particular office, it is up to the enterprise administrators to assign values for each field.

Interface IDs

- The interface ID contains a unique identifier for a specific interface on the network.
- The Institute for Electrical and Electronic Engineers (IEEE) defines the format for the 48-bit MAC address assigned to each network adapter by the manufacturer, as well as the EUI-64 identifier format derived from it.
- A privacy problem with this method of deriving interface IDs from the computer’s hardware—the location of a mobile computer might be tracked based on its IPv6 address.
- Instead of using MAC addresses, Windows operating systems generate random interface IDs by default.

Link-Local Unicast Addresses

- In IPv6, systems that assign themselves an address automatically create a **link-local unicast address**, which is the equivalent of an APIPA address in IPv4.
- All link local addresses have the same network identifier: a 10-bit FP of 1111111010 followed by 54 zeroes, resulting in:

  fe80:0000:0000:0000/64
- In its more compact form, the link-local network address is:

  fe80::/64

Unique Local Unicast Addresses

These are the same as private addresses in IPv4, with the following format:

- **Global ID:** A 48-bit field beginning with an 8-bit FP of 11111101 in binary, or fd00::/8 in hexadecimal. The remaining 40 bits of the global ID are randomly generated.
- **Subnet ID:** A 16-bit field that organizations can use to create an internal hierarchy of sites or subnets.
- **Interface ID:** A 64-bit field identifying a specific interface on the network.

Special Addresses

- **Loopback address**: Any messages sent to it are returned back to the sending system.

  0:0:0:0:0:0:0:1 or **::1**

- **Unspecified address:** The address the system uses while requesting an address from a DHCP server.

  0:0:0:0:0:0:0:0

Multicast Addresses

Multicast addresses always begin with an FP value of **11111111**, in binary, or **ff** in hexadecimal. The entire multicast address format is as follows:

- **FP:** An 8-bit field that identifies the message as a multicast.
- **Flags:** A 4-bit field that specifies whether the multicast address contains the address of a rendezvous point (0111), is based on a network prefix (0010), and is permanent (0000) or transient (0001).
- **Scope:** A 4-bit field that specifies how widely routers can forward the address. Values include interface-local (0001), link-local (0010), site-local (0101), organization-local (1000), and global (1110).
- **Group ID:** A 112-bit field uniquely identifying a multicast group.

Anycast Addresses

- Used to identify the routers within a given address scope and send traffic to the nearest router, as determined by the local routing protocols.
- Can be used to identify a particular set of routers in the enterprise, such as those that provide access to the Internet.
- To use anycasts, the routers must be configured to recognize the anycast addresses.

Assigning IPv6 Addresses

As with IPv4, a Windows computer can obtain an IPv6 address by three possible methods:

- **Manual allocation:** A user or administrator manually supplies an address and other information for each network interface.
- **Self-allocation:** The computer creates its own address using a process called stateless address autoconfiguration.
- **Dynamic allocation:** The computer solicits and receives an address from a Dynamic Host Configuration Protocol (DHCPv6) server on the network.