Learning outcome 2: Perform Basic Network Configuration

2.1 Classification of IP Addresses

❖ **Introduction**

An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet.

IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255. IP addresses are not random.

The IP address comprises two parts, the network ID and the host ID. You can use the network ID, which is the prefix, to identify the network on which the device is present. Host ID, which is the suffix, refers to a specific device on that network.

Why Use an IP Address?

IP addresses are not only essential when connecting to the internet but also performs other functions, which are:

1. **Identity for the host:** This function of the IP address is responsible for providing the network device that accesses the internet with a unique identity on the web.

   This identity allows the system to access data available on the internet and as an identifier for the hubs, routers, or switches it connects to and access data.

2. **Location of the host:** As the name suggests, the other function of the IP address provides the system's location on the network. This is beneficial because, in case of a hacking incident or spamming, you can track the perpetrator through the system's IP address used to execute the task.

❖ **Types of IP Addresses**

There are four different types of IP addresses:

- Public
- Private
- Static
- Dynamic

The **public** and **private** are indicative of the location of the network; private is being used inside a network while the public is used outside of a network

Static and **dynamic** indicate permanency.

A static IP address is one that was manually created, as opposed to having been assigned. A static address also does not change, whereas a dynamic IP address has been assigned by a (DHCP) server and is subject to change.

- **Public IP Addresses**

A public IP address is a unique IP address for the identification of a particular network. Internet service providers assign a public IP address to the router of a network, and each device connected to the network gets assigned its own IP address.

Every device outside this network recognizes the network with its IP address. A public address is a primary address that is associated with a whole network. Public IP addresses are either **static** or **dynamic** in nature.

- **Private IP Addresses**

Private IP addresses are unique addresses that belong to internet-connected devices like smartphones, computers, tablets, etc.

The router in a network generates a unique private IP address for every device that is connected to a network. This is also tied to the growth of the internet of things.

- **Dynamic IP address**

Dynamic IP addresses always keep changing. It is temporary and are allocated to a device every time it connects to the web. Dynamic IPs can trace their origin to a collection of IP addresses that are shared across many computers.

Dynamic IP addresses are another important type of internet protocol addresses. It is active for a specific amount of time; after that, it will expire.

- **Static IP Addresses**

A static IP address is a fixed address assigned to a device that remains constant. They are typically used for hosting websites or running servers.

By having a fixed IP address, users can easily connect domain names to their servers, ensuring that their websites or services are always accessible.

Static addresses are manually configured either on the device itself or by the network administrator.

- **IP address versions**

There are two versions of IP that currently coexist in the global Internet: IP version 4 (IPv4) and IP version 6 (IPv6). IP addresses are made up of binary values and drive the routing of all data over the Internet. IPv4 addresses are 32 bits long, and IPv6 addresses 128 bits long.

What Is IPv4?

IPv4 stands for Internet Protocol version 4. It is the underlying technology that makes it possible for us to connect our devices to the web.

IPv4 assigns 32-bit IP addresses to devices. Each address has four groups of numbers (8-bit sections called **octets**) separated by a period, such as: ***192.158.1.38***

The value of each octet ranges from 0 to 255, so the IPv4 model includes every address between 0.0.0.0 and 255.255.255.255. All IPv4 addresses have two parts:

- The **network ID** (the first three octets) that indicates which network the device is on.
- The **host ID** (the fourth octet) that identifies the specific device on that network.

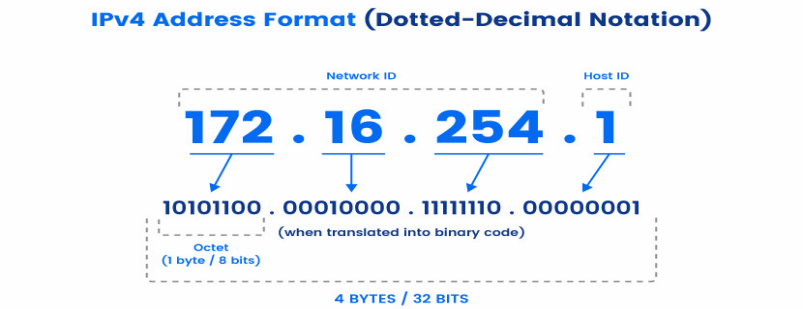
For example, if your home network has a 192.168.1.1 address, 192.168.1 is the network ID, while the final octet (1) is the host ID. In most networks, the router gets the .1 value by default.

IPv4 enables the creation and use of **4,294,967,296 unique addresses** (more commonly expressed as 2^32).

In the 1980s and 1990s, over 4 billion available addresses seemed sufficient to meet the demand of the online world.

The most common technique for reusing IPv4 addresses is **Network Address Translation (NAT)**. ***NAT*** enables you to represent a group of devices with a single IP address, which conserves ***bandwidth*** and slows down the depletion(*reduction*) of IP addresses.

We view IP addresses in human-readable notations, such as 66.94.29.13. However, computers only understand binary format, so the address we see as 66.94.29.13 stands for 01000010.01011110.00011101.00001101 in the "computer language."



IPv4 Features

Here are the main features of IPv4:

- Creates 32-bit IP addresses.
- Addresses use four 1-byte decimal numbers separated by a dot, a format that a human can easily read and even remember.
- Requires small amounts of memory to store address info in the network.
- Supported by nearly all devices and websites on the Internet.
- Offers video libraries and conferences.
- Enables the creation of a simple virtual communication layer over diversified(***different***) devices.

What Is IPv6?

IPv6 is the revised version of the Internet protocol designed to overcome the IPv4 limitations and address exhaustion problem.

It is a Protocol version and the successor to IPv4. IPv6 aims to fulfill the need for more IP addresses, the main issue of the previous IP. Another common name for IPv6 is **IPng (Internet Protocol next generation)**.

IPv6 uses 128-bit hexadecimal IP addresses. This model enables **2^128 unique addresses**.

The actual number is a bit lower as some IPs are reserved for special use.

IPv6 addresses are significantly longer than IPv4 variants (eight 16-bit blocks with groups of four symbols, often called **hextets** or **quartets**) and are alphanumeric. Also, whereas IPv4 relies on periods for formatting, IPv6 uses colons, such as in this example:

2001:0db8:0000:0001:0000:ff00:0032:7879

The model omits leading zeros (like in IPv4), and you'll sometimes find IP addresses that have a double colon (::) that designate any number of 0 bits (such as 1201:2db7::fa00:0040:6669, in which the third, fourth, and fifth hextets are 0000).

While IPv6 is more sustainable than IPv4, **the majority of the Internet still uses IPv4**. Upgrading all the routers, servers, and switches that have used IPv4 for decades takes a lot of time and money.

IPv6 Features

Here are the main features of IPv6:

- A 128-bit hexadecimal address scheme.
- Auto-configuration capabilities.
- Support for Quality of Service (QoS).
- Better multicast routing and simpler header format than IPv4.
- End-to-end connectivity at the IP layer, so there's no need for NAT.
- Integrated **Internet Protocol Security (IPSec)** with built-in authentication, encryption, and privacy support.

IPv4 vs IPv6: What's the difference?

Both IPv4 and IPv6 identify connected devices on the network. However, there are slight differences in the way they operate. IPv6 is the newer IP version and was introduced to address the limitations IPv4 posed on the availability of IP addresses.

The following is a list of differences between IPv4 and IPv6:

- IPv4 is 32-bit, whereas IPv6 is 128-bit.
- In IPv4, binary bits are separated by a dot (.); IPv6 separates binary bits by a colon (:).
- IPv4 follows the numeric addressing method and IPv6 is alphanumeric.
- IPv4 supports broadcast address, which is a type of special address that transmits data packets to every node on the network. IPv6 doesn't support broadcast, but instead uses a multicast address, which is a logical identifier for a collection of hosts on a network.
- IPv4 supports Variable Length Subnet Mask, but IPv6 doesn't.

Looking up an IP address

Windows 10 and Windows 11

1. Select **Start**>**Settings**>**Network & internet**>**Wi-Fi** and the Wi-Fi network you're connected to.
2. Under **Properties**, look for your IP address listed next to **IPv4 address**.

❖ Identification of IP address classes

The 32-bit IP address is divided into five sub-classes. These are:

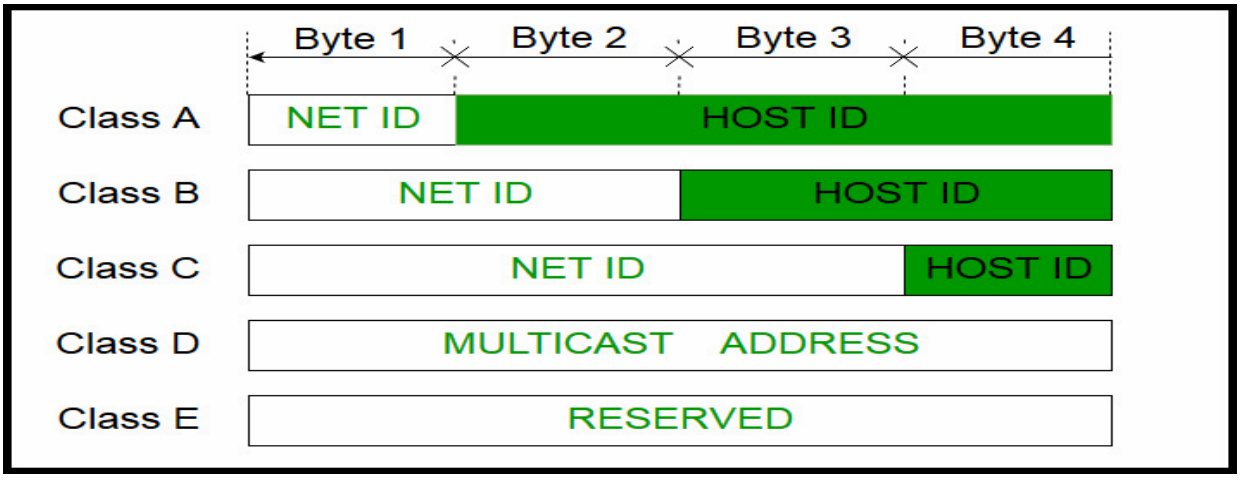
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses.
Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address.

The IPv4 address is divided into two parts: **Network ID(***Prefix***)** and **Host ID (***Suffix***)**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class.

Each ISP or network administrator assigns an IP address to each device that is connected to its network.



Note:

1. IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

1. While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

❖ Class A

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

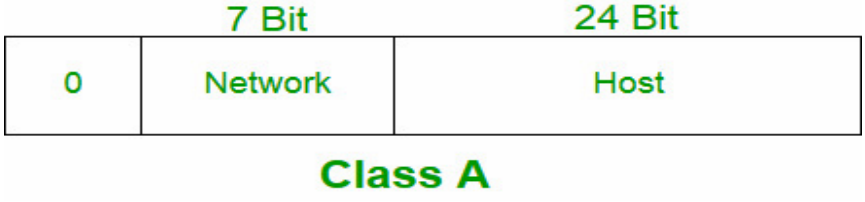
The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID.

The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x.

Therefore, class A has a total of:

2^24 – 2 = 16,777,214 used host ID

IP addresses belonging to class A ranges from 1.0.0.0 – 126.255.255.255.



❖ Class B

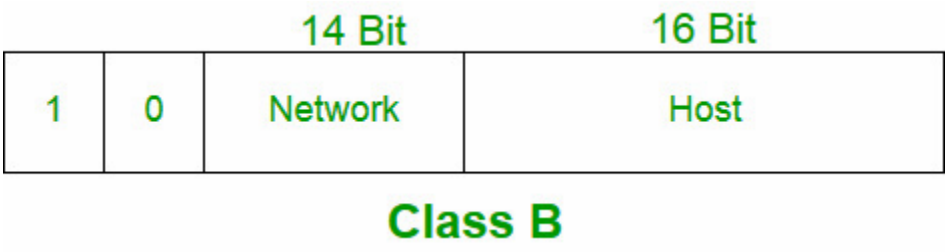
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.



❖ Class C

IP addresses belonging to class C are assigned to small-sized networks.

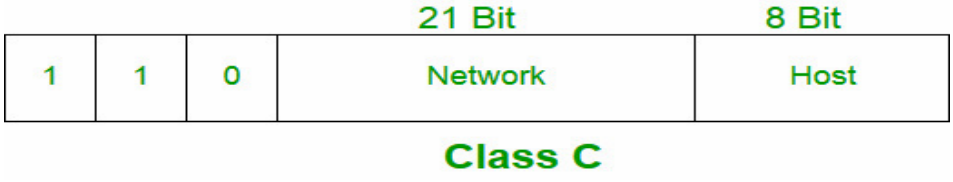
- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to 110.
The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address

. 2^8 – 2 = 254 host address

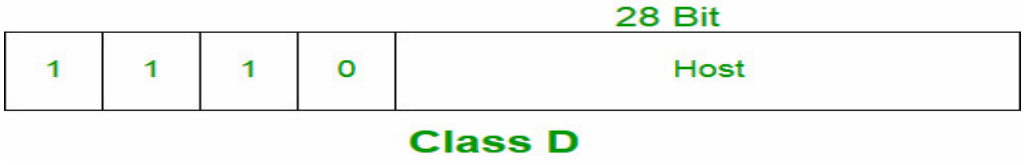
IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.



❖ Class D

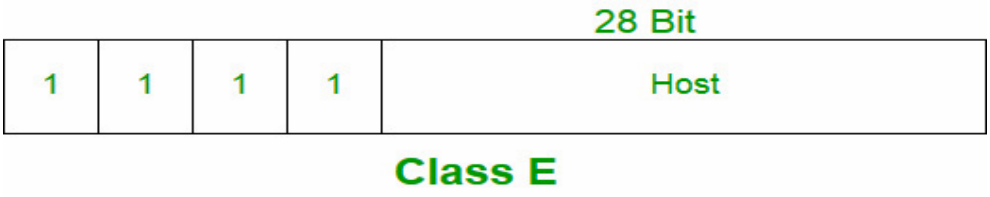
IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



❖ Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Rules for Assigning Host ID

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for Assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of IPv4 Classes

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Summary of IPv4 Classes(class A, B and C)

2.2 Calculation of IP addresses subnet masks
Introduction to subnet masks

- **Definition**

A subnet mask is a ***32-bit number*** created by setting the host bits to all ***0s*** and setting network bits to all ***1s***. In this way, the subnet mask is separated the IP address into the ***host address*** and ***network address***.

A subnet mask is a four-octet number used to identify the network ID portion of a 32-bit IP address.

The ***broadcast address*** is always assigned to the ***"255"*** address, and a ***network address*** is always assigned to the ***"0"*** address. Since the subnet mask is reserved for a special purpose, it cannot be assigned to the host.

In this way, the subnet mask separates the IP address into the network and host addresses.

A subnet mask is required on all class-based networks, even on networks that are not submitted. A *default subnet mask* is based on the IP address classes we discussed earlier and is used on networks that are not subdivided.

The default subnet masks are shown in dotted decimal format in table

IP Address Class	Default Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

- **Benefits of subnetting**

1. Improve network performance and speed

A single broadcast packet sends out information that reaches every device connected to that network because each device has an entry point into the network.

2. Reduce network congestion

Subnetting ensures that traffic destined for a device within a subnet stays in that subnet, which reduces congestion.

3. Boost network security

By splitting your network into subnets, you can control the flow of traffic .

4. Control network growth

One of the key benefits of subnetting is that it enables you to control the growth of your network.

5. Ease administration

By subnetting, you can create networks that have more logical host limits, as opposed to the limitations of IP addressing classes.

- **Binary system**

IP addresses are always written with the subnet mask. The following table lists the default subnet mask for all IP classes.

Class	Decimal notation	Binary notation
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111. 11111111.00000000.00000000
C	255.255.255.0	11111111. 11111111. 11111111.00000000

Identifying the class of an IP address (binary notation)
If an IP address is written in the binary notation, you can use the following rules to identify the class of the IP address.

- If the first bit is **OFF**, the address belongs to class **A**.
- If the first bit is **ON** and the second bit is **OFF**, the address belongs to class **B**.
- If the first two bits are **ON** and the third bit is **OFF**, the address belongs to class **C**.
- If the first three bits are **ON** and the fourth bit is **OFF**, the address belongs to class **D**.
- If the first four bits are **ON**, the address belongs to class **E**.

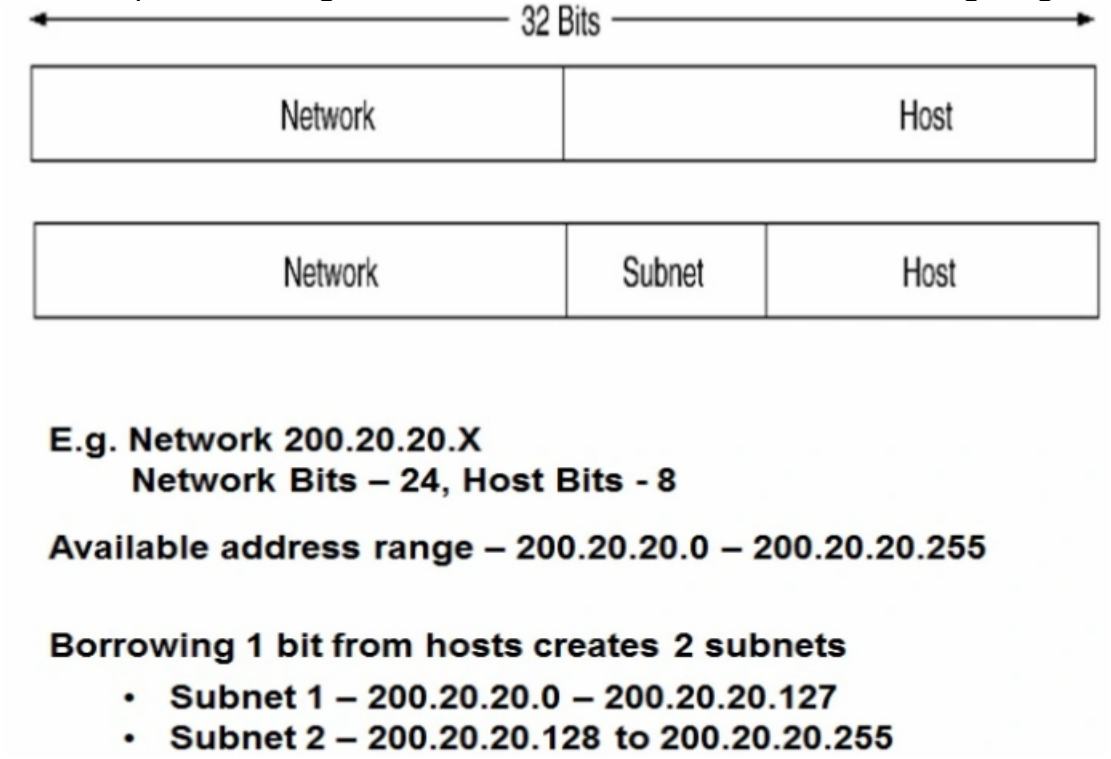
- **SUBNETTING**

IP **Subnetting** is the process of partitioning a bigger network into smaller networks by making use of some portion of the IP addresses normally allotted to hosts (i.e. one or more bytes are borrowed from the host portion of the IP address to partition the main network into different sub networks).

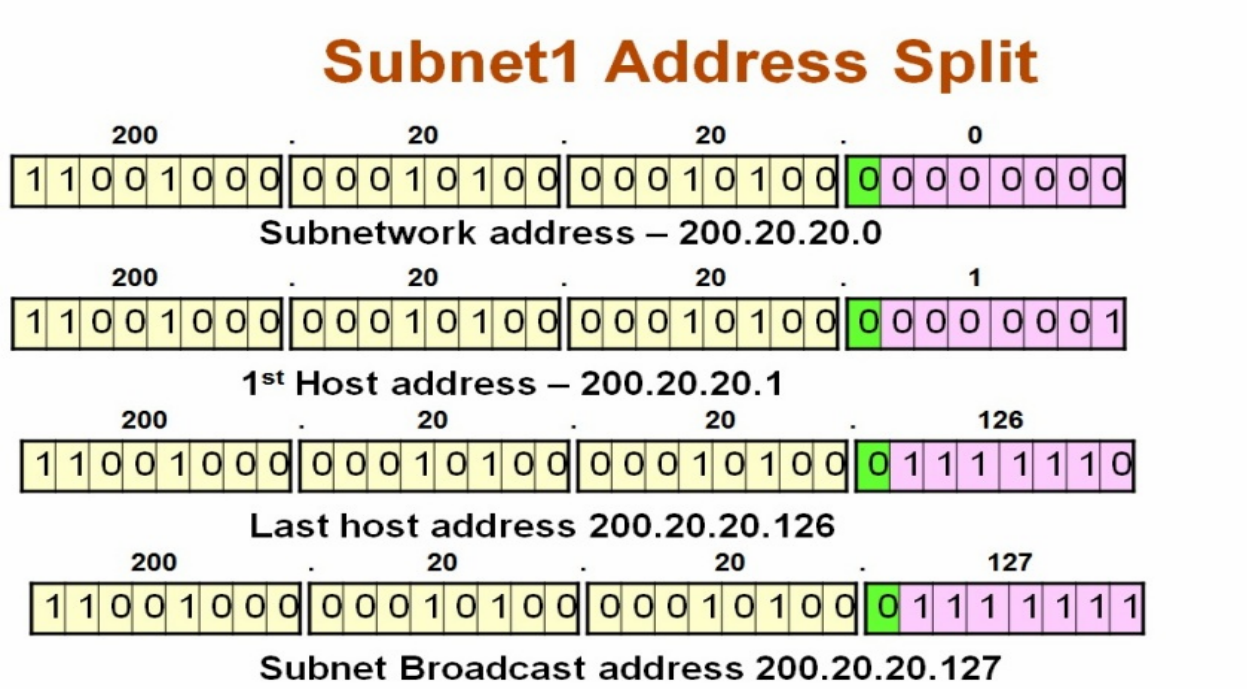
It is typically used when there is an administrative need to have more networks internally with lesser number of hosts in each of these small networks rather than a single big network with large number of hosts.

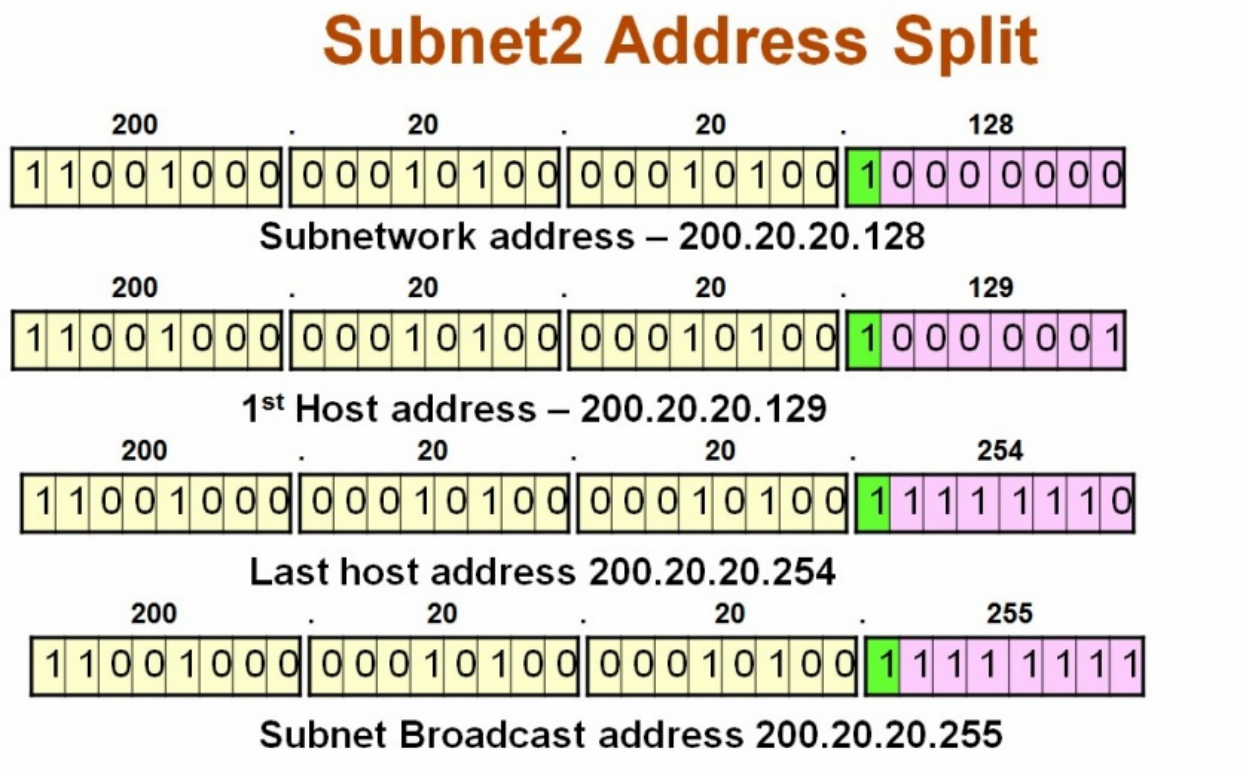
Simply, **Subnetting** is the practice of dividing a network into two or more smaller networks.

The concept of borrowing host bits to create subnets is illustrated in the diagram given below:



Two IP Subnets created by borrowing one bit from the host portion
The above example splits a single big network (200.20.20.0) with 254 hosts into two equal smaller subnetworks (200.20.20.0 and 200.20.20.128), each with 128 IP addresses.





Subnet Mask

- Subnet mask is similar in format to IP address : E.g. a.b.c.d
- It contains a one for bit positions belonging to the network or subnetwork and contains a zero for the host portion

For example, the default subnet masks for class A, B and C are:

- Class A – 255.0.0.0 or FF.0.0.0 or /8
- Class B – 255.255.0.0 or FF.FF.0.0 or /16
- Class C – 255.255.255.0 or FF.FF.FF.00 or /24

Note that the subnet masks can be denoted in three different formats as shown above. The first form (e.g. 255.0.0.0) is in decimal notation, the second form (e,g.FF.0.0.0) is in hexadecimal notation and the third form (e.g. /8) is in the /no-of-bits-for-network-and-subnetwork format.

In the above example, /8 for class A denotes that 8 bits are allotted to the network and subnetwork put together and the remaining 24 bits are for the host portion.

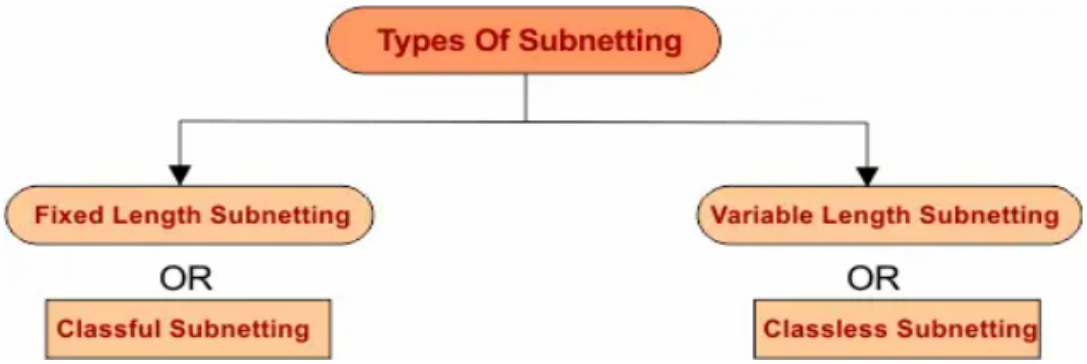
Getting the Subnet Address from the Host IP address and Subnet Mask

If we are given an end host address and the subnet mask, then we can get the subnetwork address by bit wise AND operation of the above two.

The example in the diagram given below illustrates the same:

Types of Subnetting

Subnetting of a network can be achieved through the following methods



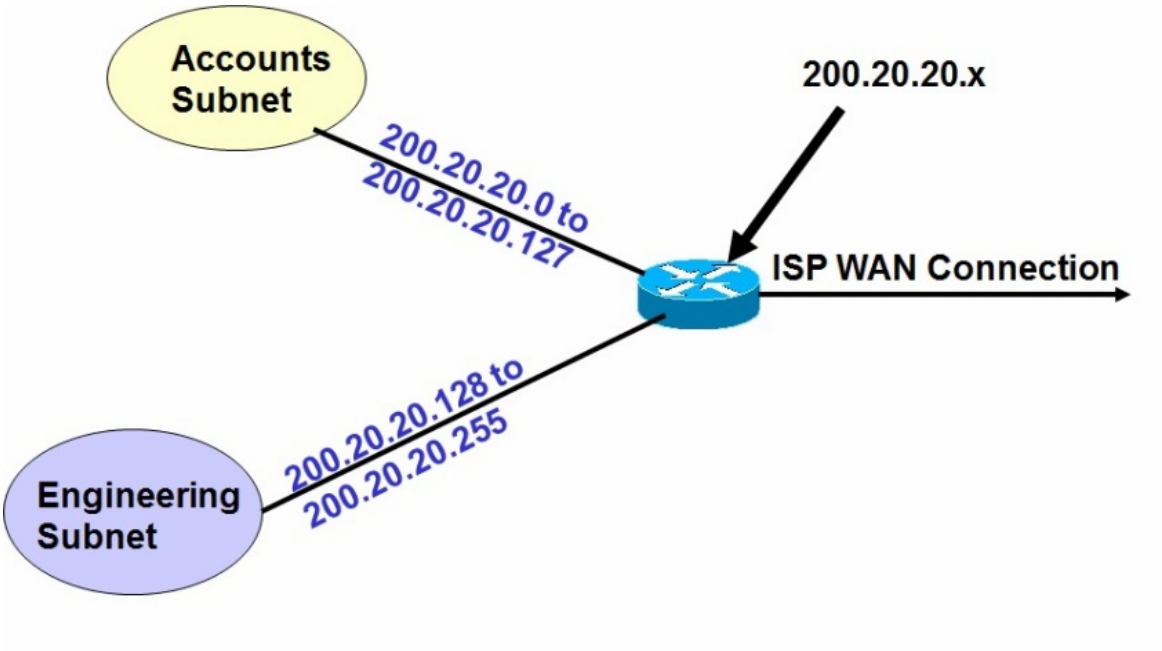
Examples for Subnet Creation

This post illustrates two examples for subnet creation. In the first example, an office network with two departments is taken and in the second example, an office network with four departments is taken.

Example 1: An office network with two subnets

Assume that the ISP has assigned the network 200.20.20.x with 256 IP addresses to the office and also assume that the office has two internal departments, namely Engineering and Accounts. The example splits this network internally into two equal subnetworks, so that each subnetwork can be used by a single department.

The diagram given below illustrates the office network with two departments and a subnet being created for each of the two departments

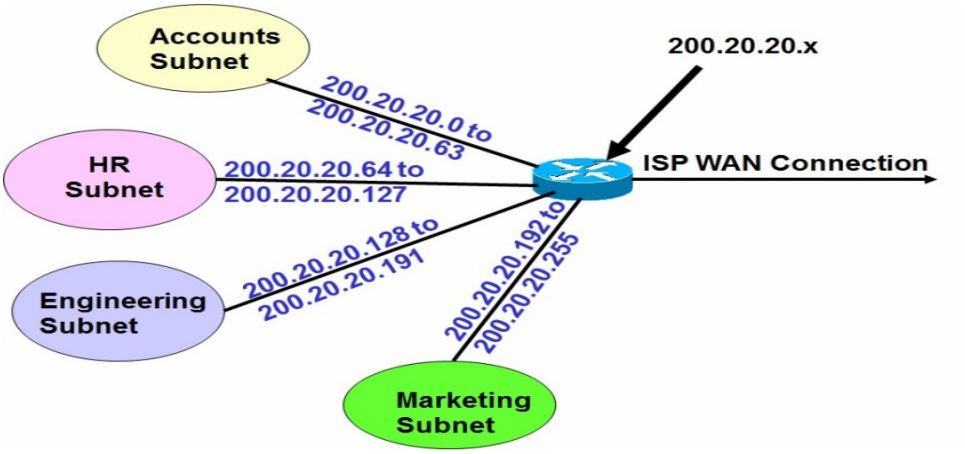


An office with two subnetworks

Example 2: An office network with four subnets

Assume that the ISP has assigned the network 200.20.20.x with 256 IP addresses to the office and also assume that the office has four internal departments, namely Engineering, HR, Marketing and Accounts. The example splits this network internally into four equal subnetworks, so that each subnetwork can be used by a single department.

The diagram given below illustrates the office network with four departments and a subnet being created for each of the four departments



An office network with four internal subnets

The diagram given below illustrates the process of borrowing 2 bits from the host portion of the network, in order to create four subnets

Network 200.20.20.X

Network Bits – 24, Host Bits - 8

Available address range – 200.20.20.0 – 200.20.20.255

Borrowing 2 bits from hosts creates 4 subnets

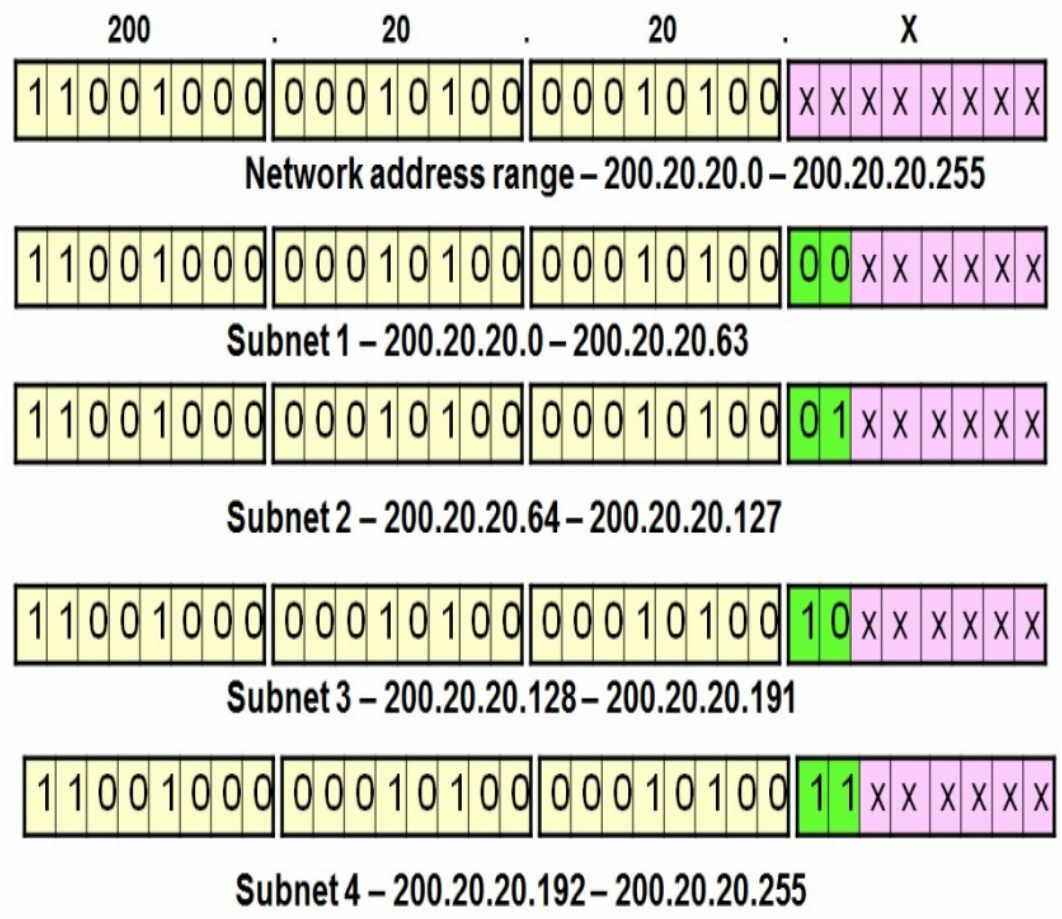
- **Subnet 1 – 200.20.20.0 to 200.20.20.63**
- **Subnet 2 – 200.20.20.64 to 200.20.20.127**
- **Subnet 3 – 200.20.20.128 to 200.20.20.191**
- **Subnet 4 – 200.20.20.192 to 200.20.20.255**

Subnet mask for Network is /26 or 255.255.255.192

Four Subnets created from a single network

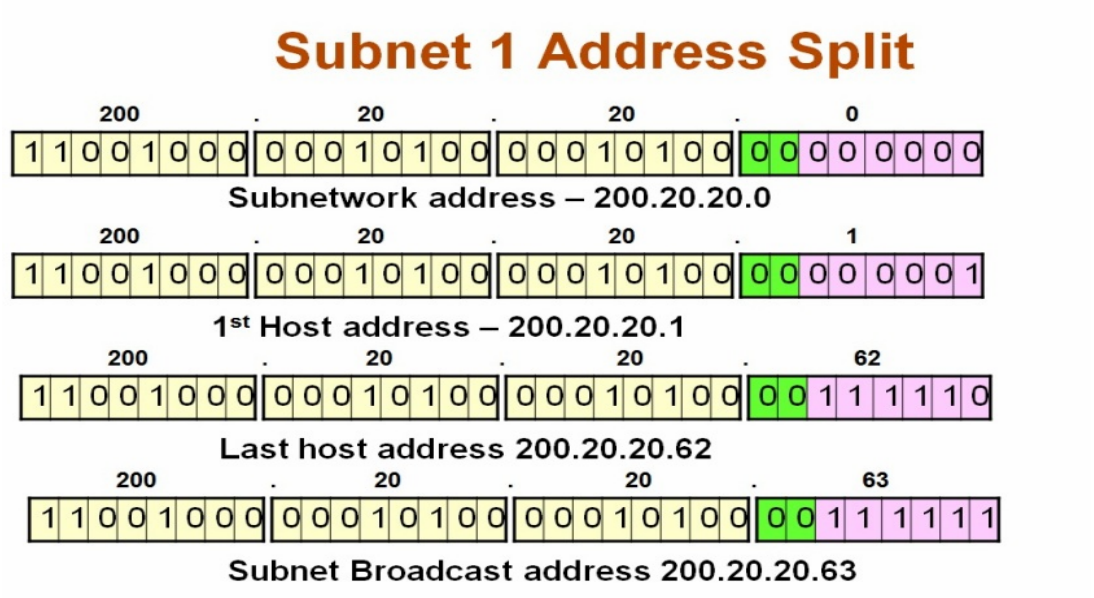
The diagram given below illustrates the basic splitting of the main ISP assigned address space into four internal subnets of equal size. Note that the first two bits of the host (25th and 26th bits of the IP address space) are borrowed to create four subnets.

The first subnet has a value of 00, the second subnet has a value of 01, the third subnet has a value of 10 and the fourth subnet has a value of 11 in these two bit positions allotted for the subnet, as highlighted in green color in the diagram below:



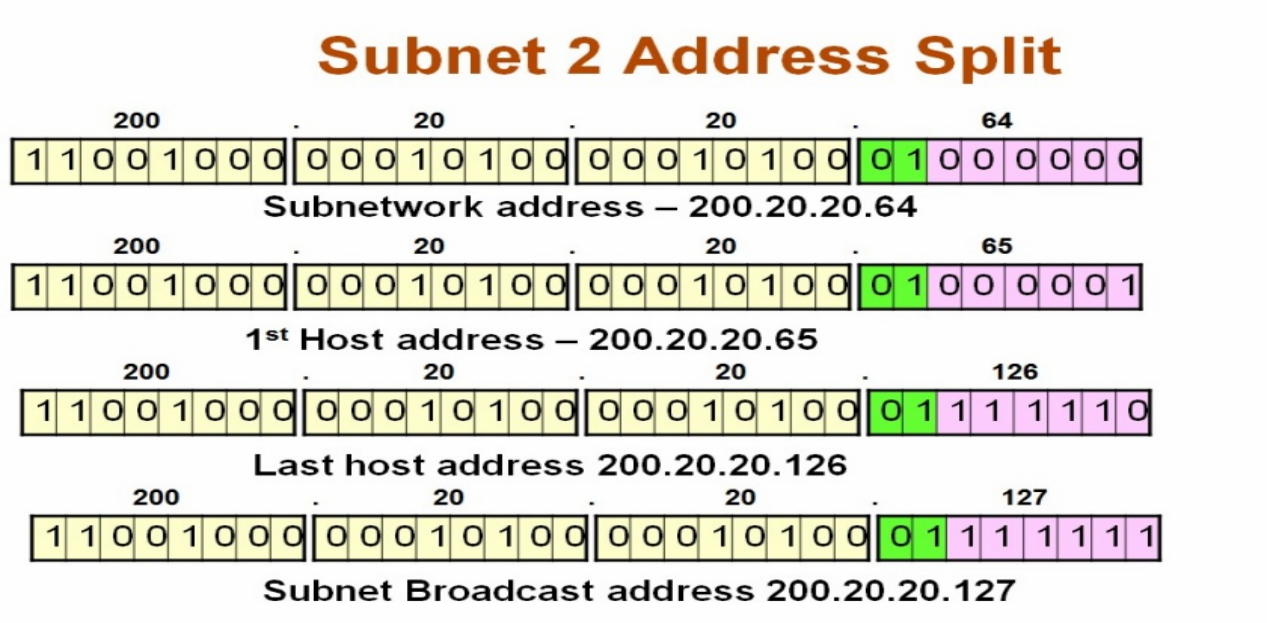
Four subnets with their IP address assignment shown in binary format

The diagram given below illustrates the different addresses assigned to the first department (Accounts).



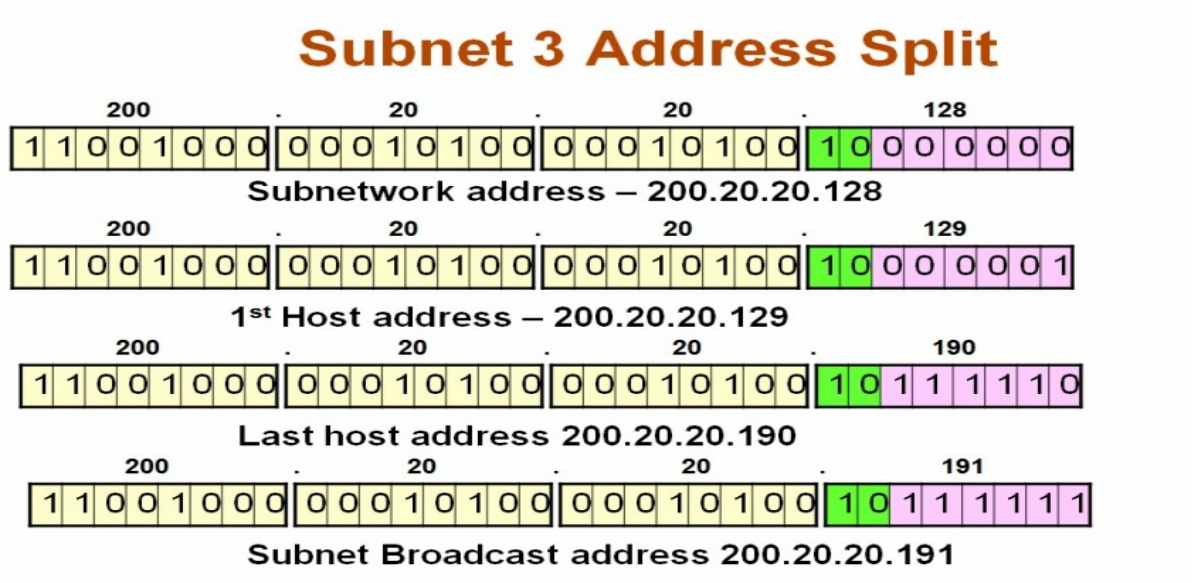
IP address assignment inside Subnet 1

The diagram given below illustrates the different addresses assigned to the second department (HR).



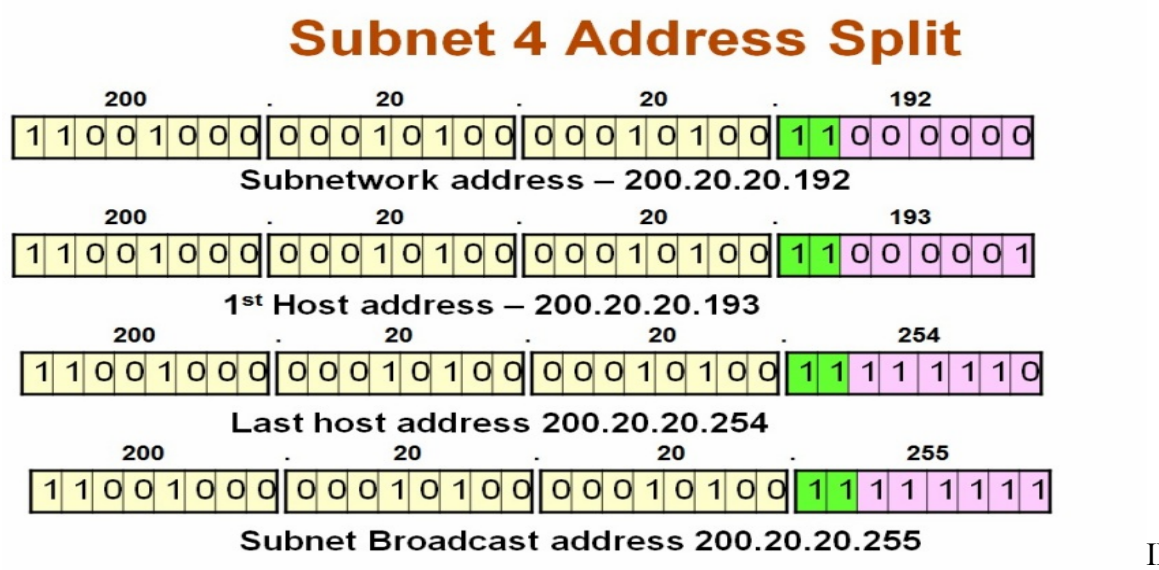
IP address assignment inside Subnet 2

The diagram given below illustrates the different addresses assigned to the third department (Engineering).



IP address assignment inside Subnet 3

The diagram given below illustrates the different addresses assigned to the fourth department (Marketing).



IP address assignment inside Subnet 4

Special Subnets

In Subnetting some **Subnet Masks** are used specifically sometimes. These are **/24, /30, /31/** and **/32.**

- /24 **is the Subnet Mask that is usually used in the** local networks **by default.**
- /32 **is the Subnet Mask used generally on** Loopback **and** System **interfaces.**
- /31 **is the Subnet Mask used on** point-to-point links.
- /30 **is also widely used in Service Provider Networks for** point-to-point connections.

Subnetting example

The first thing we need to do is to decide how many hosts per subnet we need. In our example, we need sub-networks with at least 50 usable addresses. To calculate the required host bits, we find the smallest power of 2 equal to or greater than the number of required hosts plus two (for the network and broadcast addresses). In this case, 50 + 2 = 52. The smallest power of 2 equal to or greater than 52 is 2^6 (64).

Ok, so we have 8 original host bits. For subnets with at least 50 usable host addresses, we need 6 host bits. Therefore, we are left with 2 bits that we can convert to subnet bits.

To calculate the new subnet mask of the sub-networks, we add the subnet bits to the original mask - 24+2 = /26.

2.3 Assigning IP Address

IP address can assigned to a device either statically, dynamically or automatically.

- **Static**

A static IP address (also referred to as a manual IP address or static IP configuration) is an IP address that remains unchanged over time.

Your IP address remains the same (or static) each time you connect (from the same location). Your IP address may change if you connect to a different network in a different location.

When a device is assigned a static IP address, the address does not change. Most devices use dynamic IP addresses, which are assigned by the network when they connect and change over time.

To set a static IP address in Windows 7, 8, and 10:

- Click **Start Menu** > **Control Panel** > **Network and Sharing Center** or **Network and Internet > Network and Sharing Center.**
- Click **Change adapter settings**.
- Right-click on **Wi-Fi** or **Local Area Connection.**
- Click **Properties**.
- Select **Internet Protocol Version 4 (TCP/IPv4)**.
- Click **Properties**.
- Select **Use the following IP address**.
- Enter the **IP address**, **Subnet mask**, **Default gateway**, and **DNS server**.
- Click **OK**.

- **Dynamic**

It is a temporary address for devices connected to a network that continually changes over time.

Your IP address may change each time you connect.

Most IP address assigned by your ISP will be dynamic IP addresses.

On Windows 10, you can configure a network adapter to use a static IP address manually, or you can use an automatically assigned configuration using the local Dynamic Host Configuration Protocol (DHCP) server.

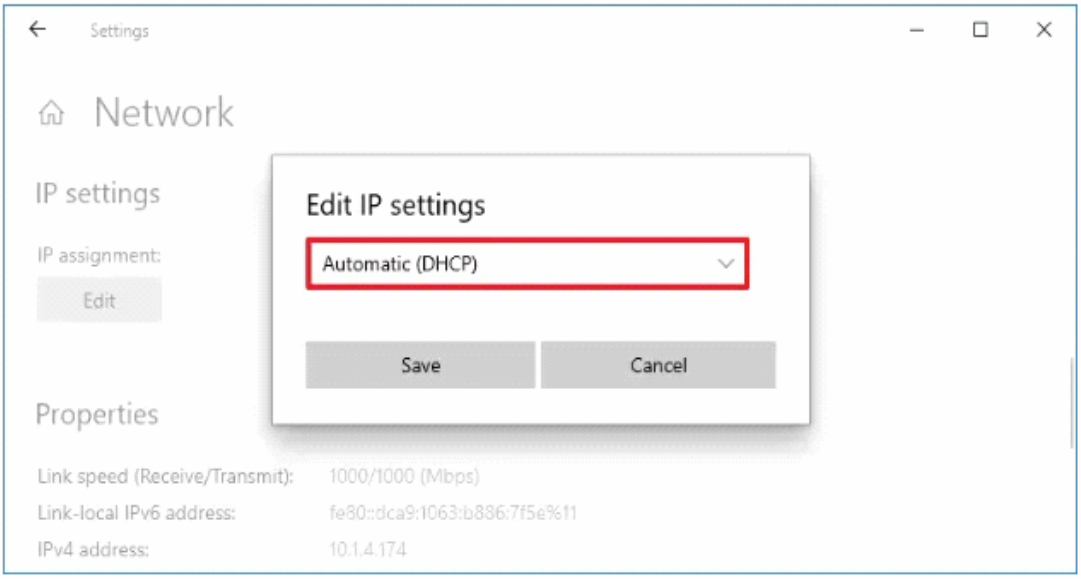
Although using a static IP address is recommended for devices that provide services to network users, as its configuration never changes, it may come a time when you may no longer need this configuration, and a dynamically assigned network configuration will be more suited.

Change to dynamic IP address (DHCP) from Settings

To enable DHCP to obtain a TCP/IP configuration automatically on Windows 10, use these steps:

- Open Settings on Windows 10.
- Click on Network & Internet.
- Click on Ethernet or Wi-Fi.
- Click the network connection.
- Under the "IP settings" section, click the Edit button.

- Use the Edit IP settings drop-down menu and select the Automatic (DHCP) option.

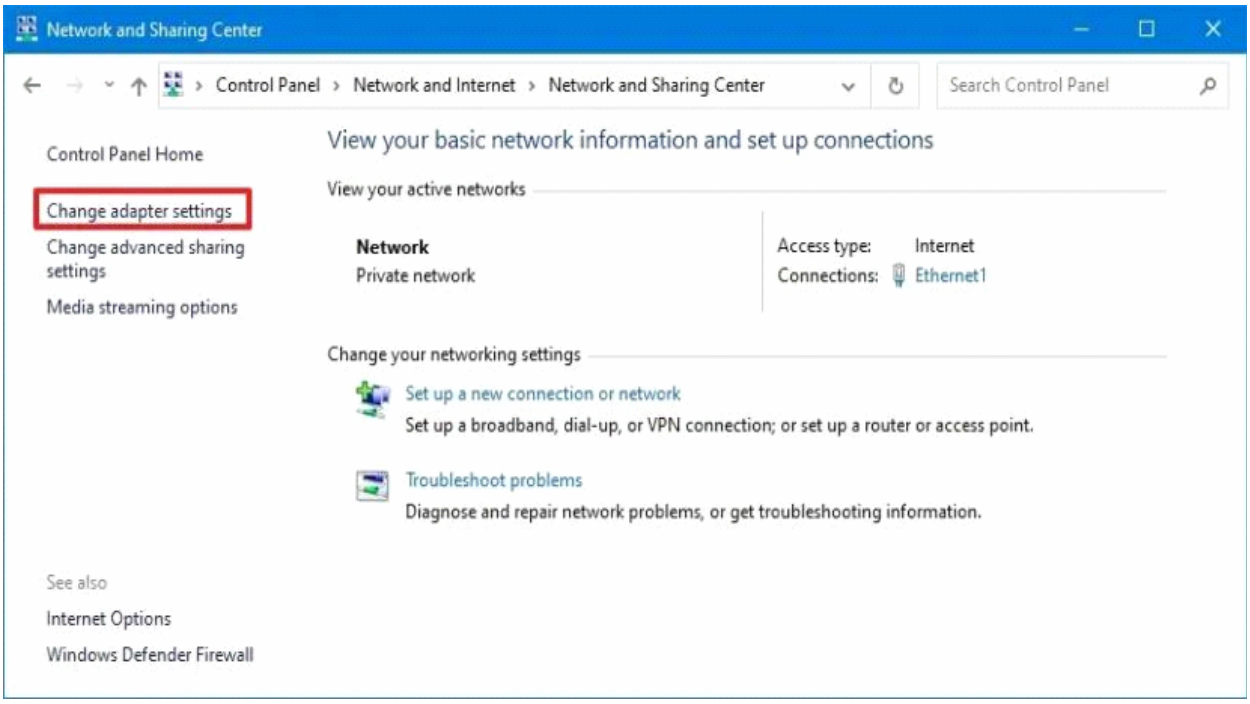


- Click the Save button.

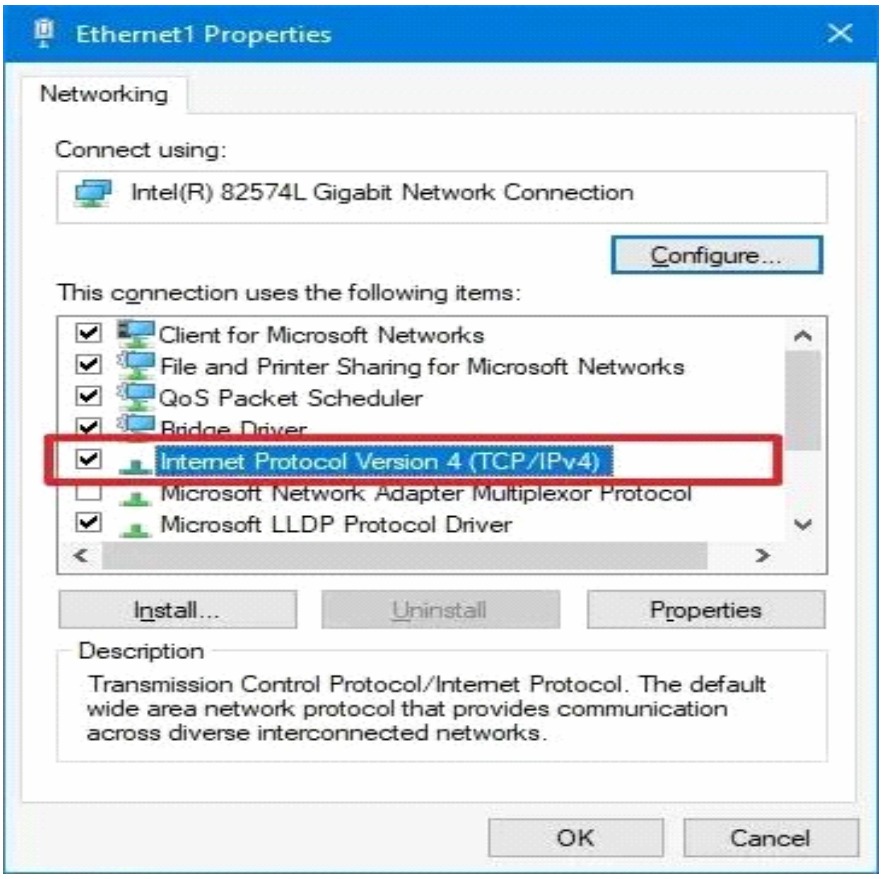
Change to dynamic IP address (DHCP) from Control Panel

To configure a network adapter to use a dynamic IP address using Control Panel, use these steps:

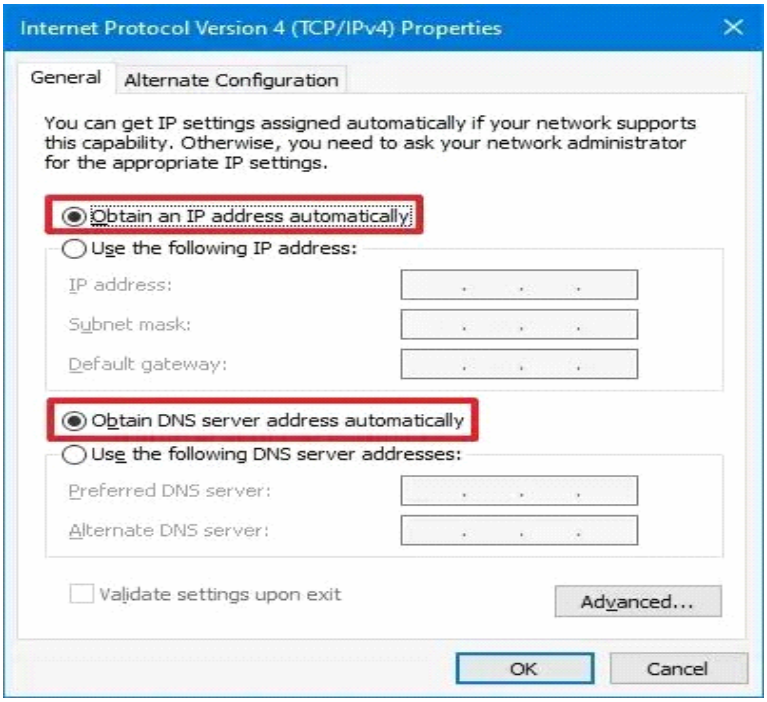
- Open Control Panel.
- Click on Network and Internet.
- Click on Network and Sharing Center.
- On the left pane, click the “Change adapter settings” option.



- Right-click the network adapter and select the Properties option.
- Select the “Internet Protocol Version 4 (TCP/IPv4)” option.
- Click the Properties button.



- Select the “Obtain an IP address automatically” option.
- Select the “Obtain the following DNS server address automatically” option.



- Click the OK button.

After completing the steps, the statically assigned TCP/IP configuration will no longer be available, and the computer will automatically request a dynamic network configuration from the network.

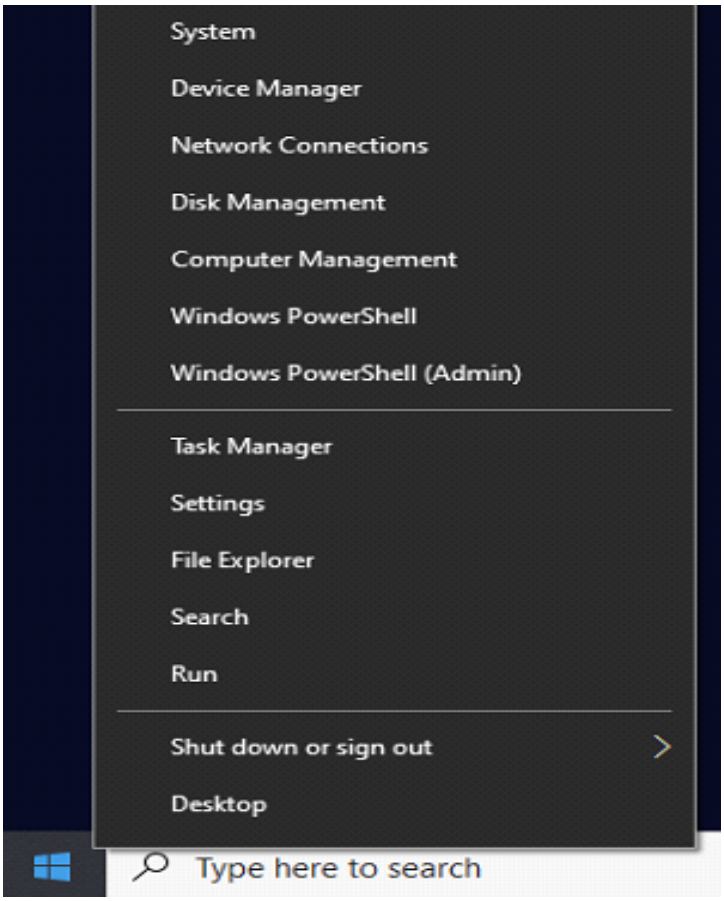
What is the difference between a dynamic and static IP address?
When a device is assigned a *static* IP address, the address does not change. Most devices use *dynamic* IP addresses, which are assigned by the network when they connect and change over time.

- **Automatic**

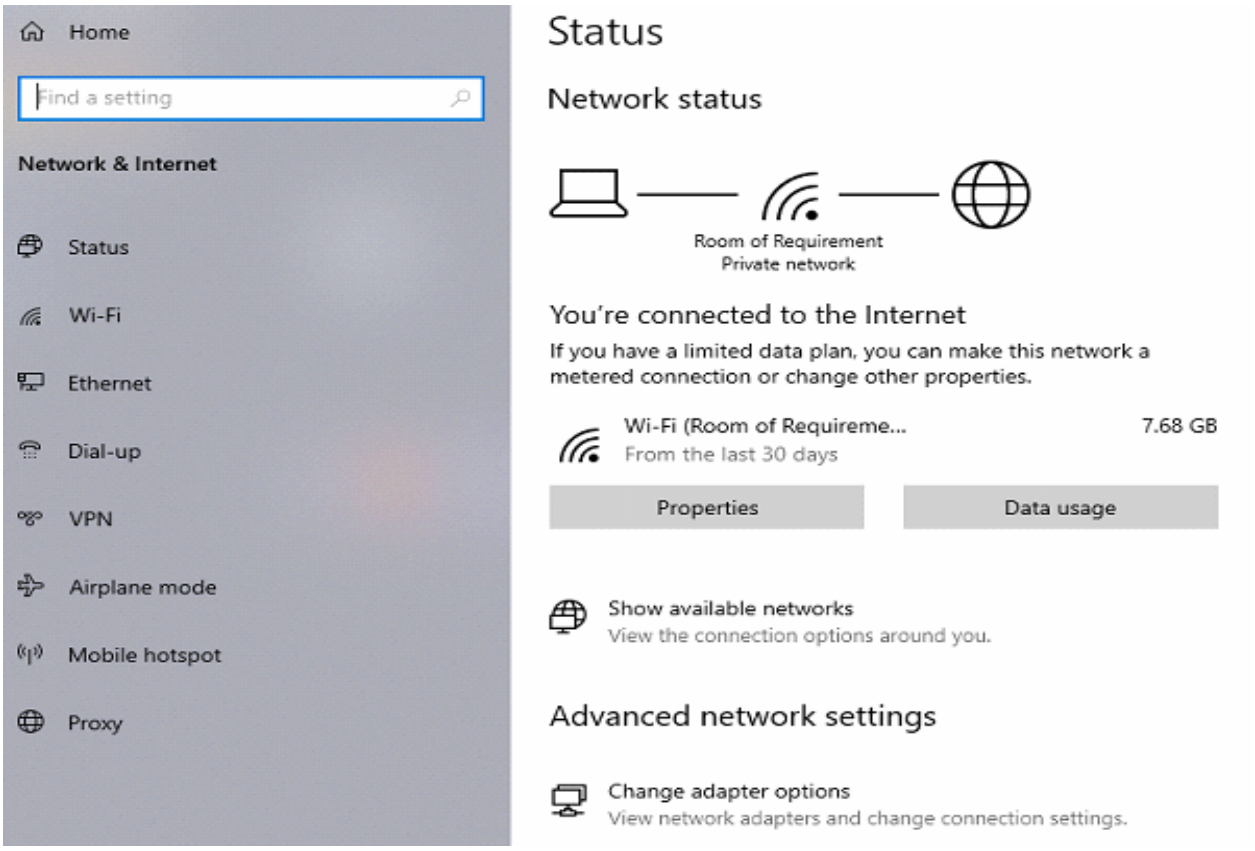
Automatic Private IP Addressing, also known as APIPA or Auto IP, is a method of automatically assigning IP addresses to networked computers and printers.

Windows 10

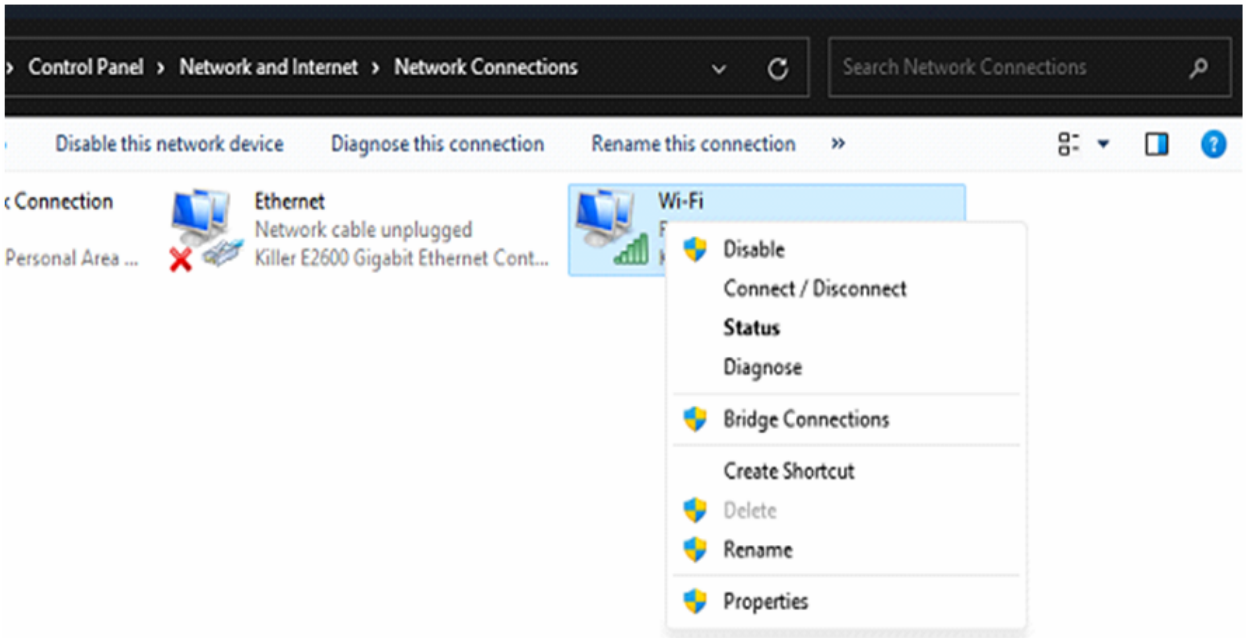
1. Right-click on the Windows icon then select **Network Connections**.



2. Under Advanced network settings click on **Change adapter options**.

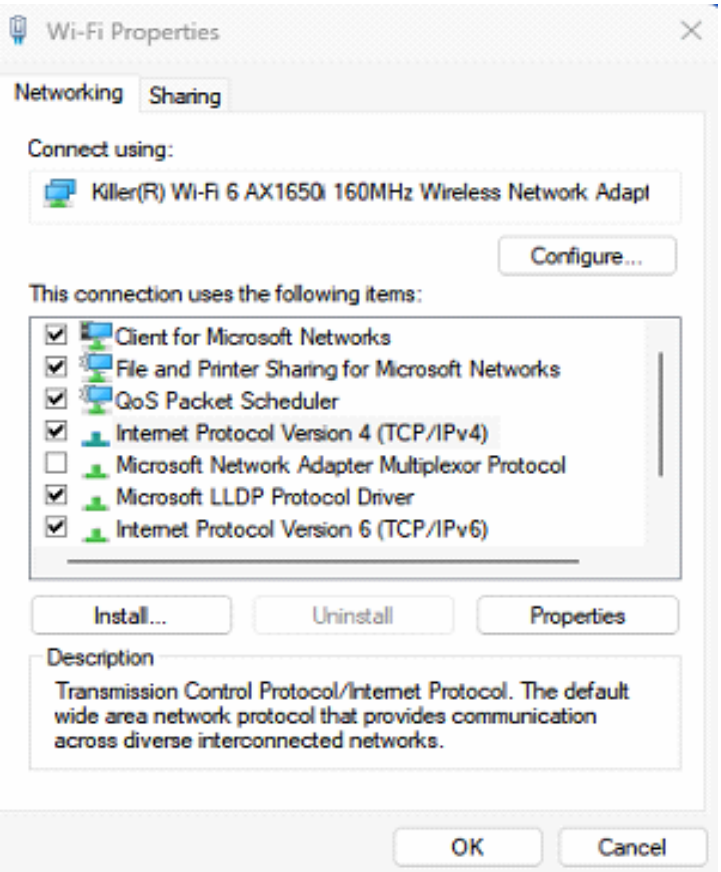


3. Right-click on **Wi-Fi** then select **Properties**.

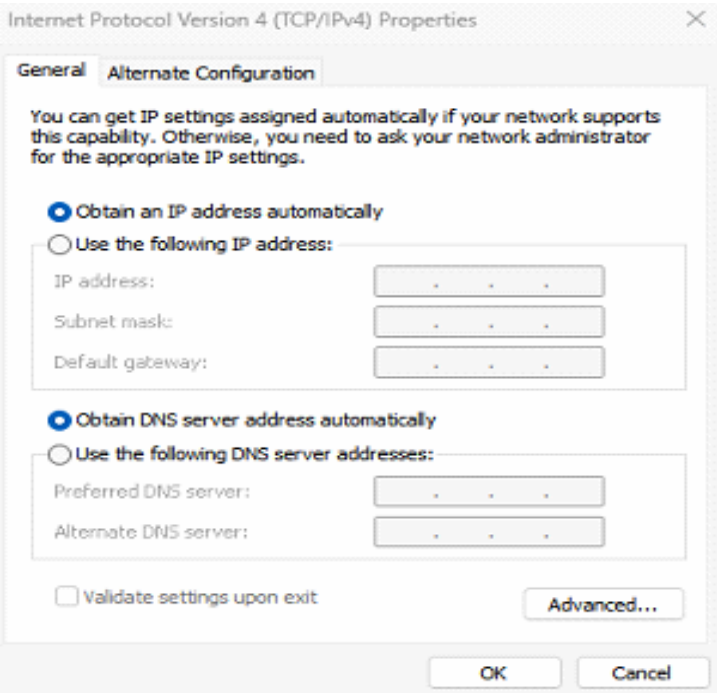


If your computer is connected wired to the router, right-click on **Ethernet** then select **Properties**.

4. Select **Internet Protocol Version 4 (TCP/IPv4)** then click on **Properties**.



5. Select **Obtain an IP address automatically** then click **OK**.



2.4 Configuration of Basics Network Device.

Before you can use any network device, you need to perform some basic configuration steps, such as setting up the device name, password, IP address, and default gateway.

These steps help you identify and access the device on the network, as well as establish connectivity with other devices.

- **Device Configuration Modes**

In networking, device configuration modes refer to different operational states or modes that network devices can be in during the configuration process. These modes provide administrators with specific interfaces and commands to perform various configuration tasks.

Two common device configuration modes are:

1. User EXEC Mode

User EXEC (Executive) mode is the initial mode a user enters when connecting to a network device, such as a router or switch.

It provides limited access to basic monitoring commands, allowing users to view information such as device status, system statistics, and basic troubleshooting commands.

This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device.

The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
Example:
Router>

2. Privileged EXEC Mode

Privileged EXEC mode, often referred to as Privileged Mode or Enable Mode, provides elevated access to the full range of device commands and configurations.

Users can enter Privileged EXEC mode from User EXEC mode by using the enable command and providing the required password.

In this mode, administrators can perform configuration tasks, view more detailed system information, and execute privileged commands.

The prompt in Privileged EXEC mode typically ends with the # symbol.

Example:
Router#

Commands to enter Privileged EXEC mode:

Router> enable
Password: [Enter Password]

Configuration Mode and Sub configuration Modes

To configure the device, the user must enter global configuration mode, which is commonly called global config mode.

Global configuration mode is identified by a prompt that ends (config)# after the device name, such as Switch(config)#.

Global configuration mode is accessed before other specific configuration modes. From the global config mode, the user can enter different sub configuration modes.

Global Configuration mode allows administrators to make changes to the device's global configuration settings, this includes configuring interfaces, setting up routing protocols, and making system-wide changes.

Users can enter Global Configuration mode from Privileged EXEC mode using the configure terminal command.

Command to enter Global Configuration mode:

Router# configure terminal

Two common sub configuration modes include:

- **Line Configuration Mode** :Used to configure **console, SSH or Telnet.**

There are several ways to access the CLI environment and configure the device.

The most common methods are:

- **Console:** The advantage of using a console port is that the device is accessible even if no networking services have been configured, such as when performing an initial configuration of the networking device.

  When performing an initial configuration, a computer running terminal emulation software is connected to the console port of the device using a special cable.
  Configuration commands for setting up the switch or router can be entered on the connected computer.

- **SSH:** SSH is the recommended method for remote management because it provides a secure connection.

  SSH provides encrypted password authentication and transport of session data. This keeps the user ID, password, and the details of the management session private.

  Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.

- **Telnet:** Best practice dictates to use SSH instead of Telnet for remote management CLI connections. Cisco IOS includes a Telnet server and a Telnet client that can be used to establish Telnet sessions with other devices.

Once you have your router and Switch you are on the road to configuring your own network.

- **Interface Configuration Mode:** Used to configure a **switch port** or **router network interface**.

Users enter Interface Configuration mode from Global Configuration mode by specifying the interface type and number.
The prompt in Interface Configuration mode typically ends with (config-if)#.

Example:

Router(config-if)#

Command to enter Interface Configuration mode:

Router(config)# interface gigabitEthernet0/0

Router(config-if)#

2.5 Host name1111111111111111111

It seems like there might be a typo in your question as "Host name1111111111111111111" appears to be a repetition of the phrase "Host name" with a sequence of '1's.

A hostname in networking typically refers to the unique name assigned to a device on a network.

A hostname helps identify and distinguish devices within a network. Hostnames are used in various networking contexts, including DNS (Domain Name System) and device configuration.

In a network, a hostname is a unique name of a computer or device (host). It is also known as a computer name, site name, or node name, which identifies a hardware device or host on the network.

Both network nodes and physical addresses can be described by hostnames, which contain different domains under one host.

Hostnames are translated into IP addresses with the help of using domain name systems in the local networks and wide area networks like the Internet.

Each host name is mapped to a unique IP address by a local or remote DNS server, through which the device is identified on a network. Therefore, hostnames make it easy to remember websites on the Internet and names of devices on a network as they are simply used as human-readable labels.

In networking, a valid hostname usually follows certain rules:

- **Length:** It should be between 1 and 63 characters.
- **Characters:** It can include letters (a-z, A-Z), numbers (0-9), and hyphens (-).
- **No Spaces:** Spaces are not allowed in hostnames.
- **No Special Characters:** Most special characters are not allowed, except for hyphens.

2.6 Banner message

In networking, a banner message refers to a message or warning that is displayed to users when they log in to a network device or service.

This message is commonly presented in the form of a text banner and serves various purposes, including legal notices, security warnings, or informational messages.

Banner messages are typically configured on network devices such as routers, switches, and servers.

Here are the common types of banner messages in networking:

- **Login Banner:**
  A login banner is displayed to users when they log in to a network device or service. It often includes legal disclaimers, terms of use, or other notifications.

- **Example login banner:**
  - Welcome to the Network
  - Unauthorized access is prohibited.

- **MOTD (Message of the Day) Banner:**
  A MOTD banner is a message that is displayed to users upon successful login. It can provide general information, updates, or news.

  Example MOTD banner:
  - **Network Maintenance:** Expect brief outages between 10:00 PM and 12:00 AM tonight.

- **Banner for Remote Access:**

For devices with remote access capabilities, a banner may be configured to inform users of the remote access policy, legal restrictions, or security warnings.

Example remote access banner:

- This system is for authorized users only. Unauthorized access is prohibited and may be subject to legal action.

❖ **Security Warning Banner:**
A security warning banner is often used to warn users about monitoring, auditing, or legal consequences related to unauthorized access.

Example security warning banner:

- All activities on this network are monitored and logged. Unauthorized access will be reported to law enforcement.

2.7 Reload Device

Reloading or rebooting a network device is a common administrative task in networking. This process is often performed to apply configuration changes, troubleshoot issues, or implement software updates.

The method to reload a device may vary based on the specific device, but here are general steps using a Cisco router or switch as an example.

Please note that similar principles can be applied to other networking devices.

Reload a Cisco Router or Switch steps:

1. Access Privileged EXEC Mode:

Router> enable

2. Access Global Configuration Mode:

Enter Global Configuration mode using the configure terminal command:

Router# configure terminal

3. Issue Reload Command:

Enter the reload command to initiate the reload process:

Router(config)# reload

4. Confirm Reload:

The device will prompt you to confirm the reload. You may specify a time delay if needed or simply press Enter to proceed immediately.

System configuration has been modified. Save? [yes/no]:

2.8 Configure port

Configuring a port in networking typically involves setting parameters and options for a specific network interface on a device, such as a router, switch, or server.

The exact steps and commands for configuring a port depend on the device's operating system and the specific type of port (e.g., Ethernet, serial, or virtual interfaces).

Below, I'll provide a general guide using Cisco devices as an example. Keep in mind that other devices and vendors may have different command structures.

Configuring a Port on a Cisco Switch or Router steps:

1. Access Privileged EXEC Mode:
Connect to the device using a console cable, Telnet, or SSH.

Enter Privileged EXEC mode using the enable command:
Router> enable

2. Access Global Configuration Mode:
Enter Global Configuration mode using the configure terminal command:
Router# configure terminal

3. Navigate to Interface Configuration Mode:
Depending on the device, locate the interface you want to configure.

For example, to configure a GigabitEthernet interface:
Router(config)# interface GigabitEthernet0/1

4. Configure Parameters:

Set specific parameters for the interface. The options available depend on the type of interface.

Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# description This is a description for the interface
Router(config-if)# speed 1000
Router(config-if)# duplex full

5. Verify Configuration:
Verify the configuration using commands such as **show running-config** or **show interface GigabitEthernet0/1.**

6. Save Configuration:
Save the configuration to the startup configuration so that it persists across reboots:
Router# write memory

2.9 Configure Device passwords
Configuring device passwords is a critical aspect of network security.
Passwords help control access to network devices, ensuring that only authorized personnel can make configuration changes or access sensitive information.

Keep in mind that different devices or vendors may have variations in syntax and procedures.

Below are general steps to configure passwords on a Cisco **router** or **switch** as an example.

1. Access Privileged EXEC Mode:
Connect to the device using a console cable, Telnet, or SSH.
Enter Privileged EXEC mode using the enable command:
Router> enable

2. Access Global Configuration Mode:
Enter Global Configuration mode using the configure terminal command:
Router# configure terminal

3. Set Enable Password:
Configure an enable password to control access to Privileged EXEC mode:
Router(config)# enable password your_enable_password

Alternatively, configure an enable secret password (strongly recommended for enhanced security):
Router(config)# enable secret your_enable_secret_password
If both an enable password and enable secret password are configured, the enable secret takes precedence.

Configure Console and Virtual Terminal (VTY) Passwords:
Set passwords for console access (physical connection) and VTY lines (virtual connections for Telnet or SSH):
Router(config)# line console 0
Router(config-line)# password your_console_password
Router(config-line)# login
Router(config-line)# exit
Router(config)# line vty 0 15
Router(config-line)# password your_vty_password
Router(config-line)# login
Router(config-line)# exit

Configure Auxiliary (AUX) Port Password:
If your device has an auxiliary port, set a password for it:
Router(config)# line aux 0
Router(config-line)# password your_aux_password
Router(config-line)# login
Router(config-line)# exit

Encrypt Passwords:
For additional security, enable password encryption to encrypt stored passwords in the configuration:

Router(config)# service password-encryption

Exit Global Configuration mode:

```
Router(config)# exit
```

Save Configuration:

Save the configuration to the startup configuration so that it persists across reboots:

```
Router# write memory
```

2.10 Save configuration

Saving the configuration on a network device ensures that any changes made to the device's configuration are preserved and will persist across reboots.

The specific command to save the configuration may vary depending on the device's operating system.

Below are examples for a Cisco router or switch and a typical network device:
Cisco Router or Switch:
Access Privileged EXEC Mode:
Connect to the device using a console cable, Telnet, or SSH.

Enter Privileged EXEC mode using the enable command:

```
Router> enable
```

Save Configuration to Startup Configuration:
Enter the following command to save the current running configuration to the startup configuration:

```
Router# write memory
```

Alternatively, you can use the shorter command copy running-config startup-config:

```
Router# copy running-config startup-config
```

Save Configuration to Non-Volatile Memory:
The specific command to save the configuration may vary. Here are some common alternatives:

```
Device(config)# write memory
Device(config)# copy running-config startup-config
```

3. Testing network Interconnection

Testing network interconnection involves verifying the connectivity and proper functioning of network devices and connections.

This is the testing of the connection of two separate networks or their elements to check if the connected elements communicate with each other properly.
In network there may be**: Physical Testing, Unit Testing and Integration Testing.**

- **Physical Testing**

It is designed to assess the operational status of network connections, identifying issues in signal strength, interference, and connectivity. This category encompasses a variety of testing tools,

including network cable testers, Ethernet test devices, and more specialized equipment like cable network certifiers.

The physical network consists of the cables (coaxial cable, twisted pair, fiber optic, and telephone lines) that connect the different hardware residing on the network, the adapter used on computers connected to the network (hosts), and any concentrators, repeaters, routers, or bridges used in the network.

- **Unit Testing**

  Unit testing is the process of testing the smallest testable parts of your network, often referred to as units.
  The main goal of unit testing is to validate that each unit of the software performs as designed.
  Since it is concentrated on a small segment, it helps in identifying and fixing bugs at an early stage.

- **Integration Testing**

  While unit testing focuses on individual components, integration testing takes a step further to test how these components work together.
  It checks the data communication among these modules and detects interface defects.
  Integration testing is crucial because even if individual units function as designed, issues can still arise when they interact with each other.

Various tools and methods can be used for testing network interconnection. Here are some common approaches:

1. Ping Test:
The ping command is a fundamental tool for testing connectivity between devices.
To test connectivity to a specific device, use the following command:
ping [IP_address_or_hostname]

2. Traceroute (or Tracepath) Test:
The traceroute or tracepath command helps identify the route that packets take from the source to the destination.
To trace the route to a specific device, use the following command:

3. Telnet/SSH Connectivity:
Use Telnet or SSH to check if you can establish a connection to a remote device.
For Telnet:

4. Network Diagnostics Tools:
Network diagnostic tools, such as Wireshark, allow you to capture and analyze network traffic.
Analyze captured packets to identify communication issues or abnormal.

5. Network Scanning Tools:
Use network scanning tools, like Nmap, to discover devices on a network and check their open ports.

END OF LO 2