Module 3 [Network Configuration]

Topic: Local area networking

• Assignment level Basic:

1. What is Network?

In information technology, a network is defined as **the connection of at least two computer systems**, either by a cable or a wireless connection. The simplest network is a combination of two computers connected by a cable. This type of network is called a **peer-to-peer network**. There is no hierarchy in this network; both participants have equal privileges. Each computer has access to the data of the other device and can **share resources** such as disk space, applications or peripheral devices (printers, etc.).

Today’s networks tend to be a bit more complex and don’t just consist of two computers. Systems with more than ten participants usually use **client-server networks**. In these networks, a central computer (server) provides resources to the other participants in the

network (clients).

 Definition: Network

A **network** is a group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data and sharing resources.

1. What is Internet & Intranet?

Let’s take a step back and define the term “intranet” in relation to some other technologies that it’s often confused with. At their most basic, internet, intranet, and extranet are defined as:

* The **internet** is a globally-connected network of computers that enables people to share information and communicate with each other.
* [An **intranet**](https://www.igloosoftware.com/platform/features/), on the other hand, is a private and internal network that enables people to store, organize, and share information within an organization.
* An **extranet** is a web portal that is accessible by an organization and its external vendors, partners, customers, or any other users that require access to restricted information.

Now that we understand the fundamentals of each, let’s discuss the differences between these three crucial types of networks.

**Intranet vs. internet**

Besides the spelling and pronunciation (which might sound forced and awkward at times), there are key differences between the first two. one of the most important being that an intranet is a platform that can be bought and sold ([or built](https://resources.igloosoftware.com/services/implementation/), in some cases), while the internet is the underlying technology that enables its connectivity. In terms of access, there are also differences between the two. Internet is a public network for all to use, while an intranet is private and internal to a given organization, for only its employees to connect and communicate.

• Assignment level Intermediate:

1. How many types of Network we used?

Computer Network is the interconnection of multiple devices. Mainly there are three types of computer networks: LAN (Local Area Network), WAN (Wide Area Network), and MAN (Metropolitan Area Network).

LAN is used to connect devices in a small area like a building, office, etc.

MAN covers the devices connected within a town or a city.

WAN covers a large geographical area such as a continent or a country. System Area Network, Home Area Network, and Campus Area Network are some other network types.

## Types of Computer Networks

Based on the size of the network, ownership, and distance covered by the network, there are three types of computer networks

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

## LAN (Local Area Network)

A Local Area Network (LAN) is a group of connected devices that are in a limited area such as a school, office, building, or home. It is a network mostly used for sharing hardware resources such as printers, files, scanners, etc. If we talk about the simplest LAN network then we will consider a computer and a printer connected in a home as the simplest network. The data transmission speed of the LAN is up to 10 Mbps.

## MAN (Metropolitan Area Network)

A Metropolitan Area Network or MAN is a network connecting devices across an entire town, entire city, or any other small region. This is a network larger than LAN but smaller than the WAN. WAN stands for Wide Area Network which is used to connect devices geographically such as across the country or continent. MAN network works between LAN and WAN. MAN can be used to connect multiple LAN networks. When one LAN uses modems, direct digit devices, and any other media types to connect with other LAN, then it covers a large area which is considered a Metropolitan Area Network (MAN).

## WAN (Wide Area Network)

WAN stands for Wide Area Network is a type of computer network which can cover a large geographical area such as a continent, or a country. The size of the WAN network is larger than the LAN and MAN network. When the size of the network grows more than the MAN then it is considered a WAN. Usually, telecommunication networks are considered a Wide Area Network. WAN Network could be interconnection between two or more LANs that are connected through telephone lines or radio waves

1. - Different between LAN & PAN?

LAN (Local Area Network) and PAN (Personal Area Network) are two types of networks that differ in terms of their size, coverage, and purpose. Here are the key differences between LAN and PAN:

1. **Size and Coverage:**
   * **LAN (Local Area Network):** LANs cover a relatively small geographic area, such as a single building, office, or campus. The size of a LAN can vary, but it typically encompasses a limited distance.
   * **PAN (Personal Area Network):** PANs are much smaller in size compared to LANs. They are designed for personal devices and operate within the immediate proximity of an individual, usually within a range of a few meters.
2. **Purpose:**
   * **LAN (Local Area Network):** LANs are designed to connect computers and devices within a specific location, such as a home, office, or campus. They facilitate the sharing of resources like files, printers, and internet connections among connected devices.
   * **PAN (Personal Area Network):** PANs are intended for personal devices and are often used for connecting devices like smartphones, tablets, laptops, and personal digital assistants. PANs enable communication and data sharing between these devices.
3. **Technologies Used:**
   * **LAN (Local Area Network):** LANs can use a variety of technologies, including Ethernet, Wi-Fi, and fiber optics, to connect devices within the network. Ethernet is commonly used for wired LANs, while Wi-Fi is prevalent in wireless LANs.
   * **PAN (Personal Area Network):** PANs typically use short-range wireless technologies such as Bluetooth and Zigbee. These technologies allow for easy and convenient connectivity between personal devices.
4. **Examples:**
   * **LAN (Local Area Network):** An example of a LAN is the network within an office building where computers are interconnected for file sharing, printing, and accessing shared resources.
   * **PAN (Personal Area Network):** A common example of a PAN is the connection between a smartphone and a laptop using Bluetooth for tasks like file transfer or internet sharing.
5. **Scope:**
   * **LAN (Local Area Network):** LANs cover a larger area compared to PANs and are designed to meet the networking needs of a group of people within a specific location.
   * **PAN (Personal Area Network):** PANs are highly personal and cover a very limited area, typically involving communication between devices carried or used by an individual.

In summary, LANs are larger networks designed to serve a specific geographic area, such as a building or campus, while PANs are smaller networks intended for personal devices and operate within the immediate vicinity of an individual.

• Assignment level advance:

1. Explain LAN?

A local area network (LAN) is a group of computers and peripheral devices that share a common communications line or wireless link to a server within a distinct geographic area. A local area network may serve as few as two or three users in a home office or thousands of users in a corporation's central office. Homeowners and information technology (IT) administrators set up LANs so that network nodes can communicate and share resources such as printers or network storage.

LAN networking requires [Ethernet](https://www.techtarget.com/searchnetworking/definition/Ethernet) cables and Layer 2 switches along with devices that can connect and communicate using Ethernet. Larger LANs often include Layer 3 switches or routers to streamline traffic flows.

A LAN enables users to connect to internal servers, websites and other LANs that belong to the same wide area network (WAN). Ethernet and Wi-Fi are the [two primary ways to enable LAN connections](https://www.techtarget.com/searchnetworking/answer/Wi-Fi-vs-Ethernet-Whats-the-difference-and-which-is-better). Ethernet is an Institute of Electrical and Electronics Engineers (IEEE) specification that enables computers to communicate with each other. Wi-Fi uses radio waves in the 2.4 gigahertz and 5 GHz spectrum to connect computers to the LAN.

Legacy LAN technologies, including token ring, Fiber Distributed Data Interface ([FDDI](https://www.techtarget.com/searchnetworking/definition/FDDI)) and Attached Resource Computer Network (ARCNET) have lost favor as Ethernet and Wi-Fi speeds increased and connectivity costs decreased.

## Understanding local area networking

There are two primary LAN types: wired LANs and wireless LANs ([WLANs](https://www.techtarget.com/searchmobilecomputing/definition/wireless-LAN)). A wired LAN uses switches and Ethernet cabling to connect endpoints, servers and internet of things (IoT) devices to the corporate network. For small businesses with only a handful of devices, a wired LAN can consist of a single unmanaged LAN switch with enough Ethernet ports to interconnect all devices. But larger LANs that connect thousands of devices require additional

hardware, software and configuration steps to ensure the network is performing optimally. This is where the concept of virtual LANs ([VLANs](https://www.techtarget.com/searchnetworking/definition/virtual-LAN)) comes into play.

1. - What are different types of LAN devices?

Local Area Network (LAN) devices are hardware components that enable the communication and connection of devices within a limited geographic area, such as a home, office, or campus. Here are some common types of LAN devices:

1. **Router:**
   * **Function:** Connects multiple networks together, typically a local network to the internet.
   * **Role:** Manages data traffic between the local network and external networks.
2. **Switch:**
   * **Function:** Connects devices within the same local network and uses MAC addresses to forward data only to the specific device.
   * **Role:** Provides efficient and high-speed data transfer within the local network.
3. **Hub:**
   * **Function:** Connects multiple devices in a LAN, but unlike a switch, it broadcasts data to all devices in the network.
   * **Role:** Simple and inexpensive, but can lead to network congestion.
4. **Access Point (AP):**
   * **Function:** Enables wireless devices to connect to a wired LAN using Wi-Fi.
   * **Role:** Extends the reach of the local network wirelessly.
5. **Bridge:**
   * **Function:** Connects two or more network segments and operates at the Data Link layer.
   * **Role:** Filters and forwards data based on MAC addresses, reducing traffic in each segment.
6. **Gateway:**
   * **Function:** Connects different types of networks (e.g., LAN to WAN), translating data between different protocols or formats.
   * **Role:** Enables communication between networks with different architectures.
7. **Network Interface Card (NIC):**
   * **Function:** Installed in computers and devices to enable them to connect to a network.
   * **Role:** Provides a physical interface for data transmission between the device and the network.
8. **Repeater:**
   * **Function:** Extends the range of a network by amplifying and retransmitting signals.
   * **Role:** Useful in large networks to overcome signal degradation over long distances.
9. **Firewall:**
   * **Function:** Monitors and controls incoming and outgoing network traffic based on predefined security rules.
   * **Role:** Enhances network security by preventing unauthorized access and protecting against cyber threats.
10. **Proxy Server:**
    * **Function:** Acts as an intermediary between a user's device and the internet to control and filter web content.
    * **Role:** Improves security and performance by caching frequently requested content.

These devices work together to create a functional and efficient local network, providing connectivity and facilitating data transfer among devices within a specific area.

Topic: configured Network

• Assignment Level Basic

1. What is configured network?

Network configuration is the process of assigning network settings, policies, flows, and controls. In a [virtual network](https://www.vmware.com/in/topics/glossary/content/virtual-networking.html), it’s easier to make network configuration changes because physical network devices appliances are replaced by software, removing the need for extensive manual configuration.

Network configuration can also be automated and managed via a centralized configuration manager network configuration manager, further reducing manual IT workload and making it easier to:

* **Maintain** a network
* **Make** configuration changes
* **Relaunch** devices
* **Track** and report data

Some network configuration basics include switch/router configuration, host configuration, software and firewall configuration, and network topology which can be controlled through rest APIs.

## **Why is network configuration important?**

The right network configuration is essential to supporting the flow of traffic through a network, and it can also support and enhance [network security](https://www.vmware.com/in/security/network-security.html) and improve network stability. In addition, the use of network [configuration management](https://www.vmware.com/in/topics/glossary/content/configuration-management.html)manager and or configuration tools can provide a number of benefits, including:

* Automated data tracking and reporting, allowing administrators to spot any configuration changes and potential threats or issues
* An easy way to make bulk changes, such as a blanket password change in a situation where passwords are compromised
* The means to swiftly roll back network settings to a previous configuration
* Reduced downtime, thanks to increased visibility and the ability to quickly identify changes
* Streamlined maintenance and repair of network devices (physical or virtual) and connections
* The ability to relaunch a device when it fails, thanks to centralized storage management of device configurations

2. How do we configure network?

Network server configuration refers to the process of setting up and configuring the hardware and software of a network server to get it up and running. It involves multiple steps including configuring the operating system, network protocols, security settings, user access, shared resources, and network services. Thorough attention to the server configuration is essential for ensuring the performance, stability, and security of the server as well as the network.

## **STEPS FOR CONFIGURING A NETWORK SERVER**

Here are the steps for configuring a network server:

1. [Set Up User Accounts](https://www.itjones.com/blogs/how-to-configure-a-network-server#set-up-user-accounts)
2. [Configure Network Settings](https://www.itjones.com/blogs/how-to-configure-a-network-server#configure-network-settings)
3. [Install And Configure Applications](https://www.itjones.com/blogs/how-to-configure-a-network-server#install-and-configure-applications)
4. [Set Up Shared Resources](https://www.itjones.com/blogs/how-to-configure-a-network-server#set-up-shared-resources)
5. [Configure Security Measures](https://www.itjones.com/blogs/how-to-configure-a-network-server#configure-security-measures)
6. [Set Server Backup](https://www.itjones.com/blogs/how-to-configure-a-network-server#set-server-backup)
7. [Test The Server](https://www.itjones.com/blogs/how-to-configure-a-network-server#test-the-server)

• Assignment level Intermediate .

1.How to check the ip address?

### For Wi-Fi connection

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

### For Ethernet connection

1. Select **Start** > **Settings** > **Network & internet** > **Ethernet**.
2. Under **Properties**, look for your IP address listed next to **IPv4 address**

Right-click the Windows Start menu and select Run. Type cmd in the search field and click OK. In Command Prompt, type ipconfig and hit Enter. Scroll to IPv4 Address to see your local IP address

2.How to check the ip address through cmd ?

To check the IP address of your computer through the Command Prompt (CMD) on Windows, you can use the following steps:

1. **Open Command Prompt:**
   * Press **Win + R** to open the Run dialog.
   * Type **cmd** and press Enter.
2. **Run the Command:**
   * In the Command Prompt window, type the following command and press Enter:

bashCopy code

ipconfig

1. **Find Your IP Address:**
   * Look for the "IPv4 Address" under the network adapter you are using. It might be labeled as "Ethernet adapter" if you are using a wired connection or "Wireless LAN adapter" if you are using Wi-Fi.
   * Your IP address will be displayed next to the "IPv4 Address."

Here is an example of what the output might look like:

bashCopy code

Ethernet adapter Ethernet: Connection-specific DNS Suffix . : IPv4 Address. . . . . . . . . . . : 192.168.1.2 Subnet Mask . . . . . . . . . . . : 255.255.255.0 Default Gateway . . . . . . . . . : 192.168.1.1

In this example, the IPv4 Address is "192.168.1.2."

If you're using a different operating system, the commands might vary. Let me know if you need instructions for a specific operating system.

3.How can we enter static address in network adapter?

#### A-Connecting directly to the access point via Ethernet cable:

1. In **Windows**, click **Start**and type network connections. In the search results click **View network connections**.  
2. Right click on **Ethernet (Local Area Connection)** and click **Properties**.

3. Select **Internet Protocol Version 4 (TCP/IPv4) >** and click **Properties**.

4. Select **Use the following IP address**. Enter IP address 192.168.0.210 in the **IP address** field.   
Enter 255.255.255.0 in the **subnet mask** field.  
Click **OK**twice.

Your Ethernet adapter is now configured with static IP 192.168.0.210 and the access point web interface is accessible at <http://192.168.0.100>

B-**How to Set a Static IP Address**

1. Access the Control Panel. In the Windows search bar, type in “ncpa. ...
2. Select the Network Adapter. ...
3. Select Properties. ...
4. Select Internet Protocol Version 4 (TCP/IPv4) ...
5. Manually enter IP address and subnet mask. ...
6. Save Settings. ...
7. Revert Back to DHCP.

• Assignment Level Advanced

1. Do a practical to release the packets from the adapter.

Yes , we are complete done a practical to release the packet from the adapter .

Capturing network traffic with tools such as Wireshark and tcpdump is fairly straightforward. Where many administrators run into trouble is understanding what they've captured.

This article explains the primary components of captured data and relates this information to the [TCP/IP](https://www.techtarget.com/searchnetworking/definition/TCP-IP) model. The article's purpose is not covering [how to use Wireshark](https://www.techtarget.com/searchsecurity/tip/Wireshark-tutorial-How-to-sniff-network-traffic) or its features and options. I provide only the basic steps to capture packets -- enough for you to grab a packet and apply the interpretive information provided throughout.

Take the following steps to initiate a capture in Wireshark:

1. Open Wireshark.
2. Set a capture filter, and select the interface on which to capture.
3. Start the capture.
4. Generate traffic by connecting to a website, pinging a remote device or attempting any other network connection.
5. Stop the capture.

Wireshark captures an immense amount of data quickly if you don't use a filter. While this might be what you want, be sure to set an effective filter if you know the protocols for the service you're troubleshooting. And don't run the capture any longer than you must. Wireshark has various search and [filter options](https://gitlab.com/wireshark/wireshark/-/wikis/CaptureFilters), but a targeted capture is much easier to work with.

I use Wireshark in this article because it is common, has a relatively simple GUI and is flexible. But many other powerful protocol analyzers are available, [such as tcpdump](https://www.techtarget.com/searchnetworking/tutorial/How-to-capture-and-analyze-traffic-with-tcpdump). You can analyze the content you capture with those tools using the information below.

Wireshark is powerful and has many options beyond this article's scope, including network analysis and performance information. Also, note that Wireshark v3 organizes the output into three vertically stacked window panes. Wireshark v4 uses the same three panes, but the Packet Details pane is in the lower-left corner -- it was the middle pane in v3 -- and the Packet Bytes pane is in the lower-right corner.

2. Do a practical to renew the lease of the ip address.

Yes , we are complete done a practical to renew the lease of the ip address .

# Release and Renew IP Address in Windows

Computers connected to a network use an Internet Protocol address (IP address) to be identified and communicate with other computers using the Internet Protocol. While some IP addressing is set manually (each computer is configured manually, including their IP address in a given network), most obtain an IP address assigned by a server running a service called the Dynamic Host Configuration Protocol (DHCP). Usually this process of obtaining/being assigned an address happens automatically, but there may be instances where this may not work as expected. Troubleshooting network connectivity issues on a Windows computer may sometimes require releasing a DHCP lease (address assigned for a pre-determined period of time) and renewing a lease (acquiring an IP address with a new lease).

## **The ipconfig command**

When you type "ipconfig /renew" into the command line, that command **orders your DHCP client to renegotiate an IP address lease with the DHCP server on your router**. On a Windows computer, use the following information to release and renew your IP address:

* Go to "Start > Run" and type "cmd" (no quotes), then select "OK"

Type "ipconfig /release" (no quotes) and press "Enter"

Once the prompt returns, type "ipconfig /renew" (no quotes), then hit "Enter,"

* Finally, type "exit" (without quotes) then press "Enter" to close the window

3. Do a practical to check the connectivity to the google

Yes , we are complete done a practical tp check the connectivity to the google .

To check connectivity to Google, you can use several methods depending on your platform. Here are a few general steps:

**1. Ping Command (Windows, macOS, Linux)**

1. **Windows:** Open Command Prompt and type:

bashCopy code

ping google.com

1. **macOS/Linux:** Open Terminal and type:

bashCopy code

ping google.com

This will send packets to Google's servers and report the round-trip time. If successful, it indicates that your computer can reach Google.

**2. Traceroute (Windows, macOS, Linux)**

1. **Windows:** Open Command Prompt and type:

bashCopy code

tracert google.com

1. **macOS/Linux:** Open Terminal and type:

bashCopy code

traceroute google.com

Traceroute shows the path that packets take to reach their destination. It helps identify where the connection might be failing.

**3. Browser**

Try opening Google in your web browser. If you can access Google's search page, it indicates that your internet connection is working, and you can connect to Google.

**4. Network Diagnostics (Windows, macOS)**

1. **Windows:**
   * Go to "Settings" > "Update & Security" > "Troubleshoot."
   * Run the "Internet Connections" troubleshooter.
2. **macOS:**
   * Go to "System Preferences" > "Network."
   * Click on your active network connection and then click "Assist me" > "Diagnostics."

**5. Firewall and Security Software**

Check if your firewall or security software is blocking the connection to Google. Temporarily disable them and see if the issue persists.

**6. DNS Configuration**

Ensure your DNS settings are configured correctly. You can try using Google's public DNS servers (8.8.8.8 and 8.8.4.4).

**7. Network Cable and Wi-Fi Connection**

For physical connections, check that your network cable is plugged in securely. If you're using Wi-Fi, make sure you're connected to the correct network and that the signal is strong.

**8. Router Reboot**

Sometimes, simply rebooting your router can resolve connectivity issues.

If these steps don't resolve the issue, there may be a problem with your internet service provider (ISP) or a broader network issue. Contact your ISP for further assistance.

Topic: Wireless networking

• Assignment level Basic:

1-What is the difference between WEP and WPA?

**1-**[Wired Equivalent Privacy (WEP)](https://www.geeksforgeeks.org/securing-wireless-and-mobile-devices/)**:**

Wired Equivalent Privacy (WEP) is a security protocol for wireless networks which provides data confidentiality comparable to a traditional wired network. It was introduced in 1999. It provides wireless security through the use of an encryption key. It uses an old encryption method that is Rivest Cipher 4 (RC4). It uses 40 bit key and 24 bit random number.

**2-**[Wi-Fi Protected Access (WPA)](https://www.geeksforgeeks.org/wpa-full-form/)**:**

Wi-Fi Protected Access (WPA) is a security protocol which is used in securing wireless networks and designed to replace the WEP protocol. It was developed by the Wi-Fi Alliance in 2003. It was designed to replace the WEP protocol and it uses Rivest Cipher 4 (RC4) and Temporal Key Integrity Protocol (TKIP) for encryption. WPA key is 256 bit key.

|  |  |  |
| --- | --- | --- |
| **S.No.** | **WEP** | **WPA** |
| 01. | WEP stands for Wired Equivalent Privacy. | WPA stands for Wi-Fi Protected Access. |
| 02. | It is a security protocol for wireless networks which provides data confidentiality comparable to a traditional wired network. | It is a security protocol which is used in securing wireless networks and designed to replace the WEP protocol. |
| 03. | Wired Equivalent Privacy (WEP) was introduced in 1999 means before WPA. | Wi-Fi Protected Access (WPA) was developed by the Wi-Fi Alliance in 2003 means after WEP. |
| 04. | It provides wireless security through the use of an encryption key. | It provides wireless security through the use of a password. |
| 05. | Data Privacy (Encryption) method is Rivest Cipher 4 (RC4). | Data Privacy (Encryption) method is Rivest Cipher 4 (RC4) and Temporal Key Integrity Protocol (TKIP). |
| 06. | Authentication method in WEP is Open system authentication or shared key authentication. | Authentication method in WPA is WPA-PSK and WPA-Enterprise. |
| 07. | Data integrity is provided through CRC 32. | Data integrity is provided through Message integrity code. |
| 08. | It uses 40 bit key and 24 bit random number. | WPA key is 256 bit key. |
| 09. | Key management is not provided in WEP. | Key management is provided through 4 way handshaking mechanism. |
| 10. | In WEP no protection against reply attacks. | In WPA sequence counter is implemented for reply protection. |
| 11. | It is possible to deploy on current hardware infrastructure. | It is possible to deploy on both previous and current hardware infrastructure. |

2-What is Wireless Network?

A **wireless network** is a [computer network](https://en.wikipedia.org/wiki/Computer_network) that uses [wireless](https://en.wikipedia.org/wiki/Wireless) data connections between [network nodes](https://en.wikipedia.org/wiki/Network_node). Wireless networking allows homes, [telecommunications networks](https://en.wikipedia.org/wiki/Telecommunications_network) and business installations to avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.] Admin telecommunications networks are generally implemented and administered using [radio communication](https://en.wikipedia.org/wiki/Radio_communication). This implementation takes place at the physical level (layer) of the OSI model network structure.

Examples of wireless networks include [cell phone networks](https://en.wikipedia.org/wiki/Cell_phone_network), [wireless local area networks (WLANs)](https://en.wikipedia.org/wiki/WLAN), wireless [sensor](https://en.wikipedia.org/wiki/Sensor) networks, satellite communication networks, and terrestrial [microwave](https://en.wikipedia.org/wiki/Microwave) networks.

A wireless network allows devices to stay connected to the network but roam untethered to any wires. [Access points](https://www.cisco.com/c/en/us/solutions/small-business/networking/wireless.html) amplify Wi-Fi signals, so a device can be far from a [router](https://www.cisco.com/c/en/us/solutions/small-business/networking/routers.html) but still be connected to the network. When you connect to a Wi-Fi hotspot at a cafe, a hotel, an airport lounge, or another public place, you're connecting to that business's wireless network.

A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. A wired network has some disadvantages when compared to a wireless network. The biggest disadvantage is that your device is tethered to a router. The most common wired networks use cables connected at one end to an Ethernet port on the network router and at the other end to a computer or other device.

Previously it was thought that wired networks were faster and more secure than wireless networks. But continual enhancements to wireless network technology such as the [Wi-Fi 6](https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-6.html) networking standard have eroded speed and security differences between wired and wireless networks.

• Assignment level Intermediate :

1. What is a wireless network connection?

wireless network connection refers to a connection between devices or systems without the need for physical cables or wires. Instead, it relies on radio waves or infrared signals to transmit data between devices. Wireless networking has become widespread and is commonly used for various purposes, including internet access, file sharing, printing, and connecting devices within a local area network (LAN).

There are different wireless technologies and standards that enable wireless connectivity, such as Wi-Fi (Wireless Fidelity), Bluetooth, Zigbee, and cellular networks (3G, 4G, 5G). Wi-Fi is one of the most common wireless technologies used for connecting devices like smartphones, laptops, tablets, and other devices to the internet and local networks. Bluetooth is often used for short-range connections between devices like smartphones, headphones, and other peripherals. Wireless networks provide the flexibility and convenience of mobility since devices can communicate with each other without being physically tethered by cables.

1. Top of Form

A wireless network allows devices to stay connected to the network but roam untethered to any wires. [Access points](https://www.cisco.com/c/en/us/solutions/small-business/networking/wireless.html) amplify Wi-Fi signals, so a device can be far from a [router](https://www.cisco.com/c/en/us/solutions/small-business/networking/routers.html) but still be connected to the network. When you connect to a Wi-Fi hotspot at a cafe, a hotel, an airport lounge, or another public place, you're connecting to that business's wireless network.

A wired network uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. A wired network has some disadvantages when compared to a wireless network. The biggest disadvantage is that your device is tethered to a router. The most common wired networks use cables connected at one end to an Ethernet port on the network router and at the other end to a computer or other device.

Previously it was thought that wired networks were faster and more secure than wireless networks. But continual enhancements to wireless network technology such as the [Wi-Fi 6](https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-6.html) networking standard have eroded speed and security differences between wired and wireless networks.

2-What are the basic concepts of networking?

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily. In this article, we are going to discuss the basics which everyone must know before going deep into Computer Networking.

Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.

* Basic Terminologies of Computer Networks .
* **Network:**A network is a collection of computers and devices that are connected together to enable communication and data exchange.
* **Nodes:**Nodes are devices that are connected to a network. These can include computers, Servers, Printers, [Routers,](https://www.geeksforgeeks.org/introduction-of-a-router/) [Switches](https://www.geeksforgeeks.org/types-of-switches-in-computer-network/), and other devices.
* **Protocol:**A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include [TCP/IP](https://www.geeksforgeeks.org/tcp-ip-model/), [HTTP](https://www.geeksforgeeks.org/http-full-form/), and [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/).
* **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
* **Service Provider Networks:**These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
* **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
* **DNS:**The [Domain Name System (DNS)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
* **Firewall:**A [firewall](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/) is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

## Types of Enterprise Computer Networks

* **LAN:**A [Local Area Network (LAN)](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/)is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
* **WAN:**A [Wide Area Network (WAN)](https://www.geeksforgeeks.org/wan-full-form/) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
* **Cloud Networks:**[Cloud Networks](https://www.geeksforgeeks.org/cloud-networking/) can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

• Assignment level advance:

1. What do you need to know about networking?

Networking refers to the practice of connecting computers and other devices to share resources and information. Here are some fundamental concepts and terms related to networking:

1. **Network:**
   * A network is a collection of interconnected devices that can communicate and share resources.
   * Networks can be classified based on their geographical scope as Local Area Network (LAN), Wide Area Network (WAN), and Metropolitan Area Network (MAN).
2. **Protocols:**
   * Communication on a network is governed by protocols, which are sets of rules that define how data is transmitted and received.
   * Common network protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), and more.
3. **IP Addressing:**
   * IP (Internet Protocol) addresses uniquely identify devices on a network. There are two versions: IPv4 and IPv6.
   * IPv4 addresses are expressed as four sets of numbers separated by dots (e.g., 192.168.1.1).
4. **Subnetting:**
   * Subnetting involves dividing a large network into smaller sub-networks to improve performance and security.
5. **Routing:**
   * Routers are devices that direct data traffic between different networks.
   * Routing protocols, such as RIP (Routing Information Protocol) or OSPF (Open Shortest Path First), help routers make decisions about the best paths for data to travel.
6. **Switching:**
   * Switches are devices that connect devices within the same network. They operate at the data link layer and use MAC addresses to forward data to the correct device.
7. **Firewalls:**
   * Firewalls are security devices that control and monitor network traffic based on predetermined security rules.
8. **DNS (Domain Name System):**
   * DNS translates human-readable domain names (e.g., [www.example.com](http://www.example.com/)) into IP addresses.
9. **DHCP (Dynamic Host Configuration Protocol):**
   * DHCP automatically assigns IP addresses and other network configuration information to devices on a network.
10. **Wireless Networking:**
    * Wi-Fi is a popular wireless networking technology that allows devices to connect to a network without physical cables.
11. **Network Security:**
    * Security measures, such as encryption, VPNs (Virtual Private Networks), and firewalls, are crucial to protect networks from unauthorized access and data breaches.
12. **Bandwidth and Latency:**
    * Bandwidth refers to the amount of data that can be transmitted over a network in a given time.
    * Latency is the time it takes for data to travel from the source to the destination.

Understanding these fundamental concepts will provide a solid foundation for working with computer networks and troubleshooting connectivity issues. Advanced topics may include load balancing, virtualization, and cloud networking.

Top of Form

2-How do you explain computer networking ?

Computer networking is a field of study and practice that involves the interconnection of computers and other devices to enable them to communicate and share resources. The primary goal of computer networking is to facilitate the exchange of information and resources among different devices, allowing them to work together efficiently. Here are some key concepts to help explain computer networking:

1. **Communication Protocols:**
   * Communication protocols are a set of rules and conventions that devices follow to exchange information. Examples include TCP/IP (Transmission Control Protocol/Internet Protocol), which is fundamental to the Internet, and HTTP (Hypertext Transfer Protocol), which is used for web communication.
2. **Devices in a Network:**
   * **Nodes/Devices:** These are the individual computers, servers, routers, switches, and other devices connected to the network.
   * **Endpoints:** Devices like computers, smartphones, and tablets that generate and consume data.
3. **Topologies:**
   * The physical or logical arrangement of devices in a network is known as its topology. Common topologies include star, bus, ring, and mesh.
4. **Networking Components:**
   * **Router:** Connects different networks and directs data between them.
   * **Switch:** Connects devices within a local area network (LAN) and uses MAC addresses to forward data to the correct destination.
   * **Hub:** Basic networking device that connects multiple devices in a LAN.
   * **Firewall:** Protects a network by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.
5. **Types of Networks:**
   * **Local Area Network (LAN):** Connects devices within a limited geographical area, such as a home, office, or campus.
   * **Wide Area Network (WAN):** Spans a larger geographical area, connecting LANs across cities or countries.
   * **Wireless Networks:** Use radio waves or infrared signals for communication, allowing devices to connect without physical cables.
6. **Internet:**
   * The Internet is a global network of interconnected networks. It enables communication and resource-sharing on a global scale.
7. **Protocols and Services:**
   * **IP (Internet Protocol):** Assigns unique addresses to each device on a network.
   * **DNS (Domain Name System):** Translates human-readable domain names into IP addresses.
   * **HTTP/HTTPS:** Protocols for web communication.
   * **FTP (File Transfer Protocol):** Used for transferring files between devices.
8. **Security:**
   * Network security involves measures to protect data and resources from unauthorized access, attacks, and vulnerabilities.
9. **Data Transmission:**
   * **Data packets:** Information is broken down into small packets for efficient transmission. Each packet contains a portion of the data, along with source and destination addresses.
10. **Wireless Networking:**
    * Involves technologies like Wi-Fi and cellular networks, allowing devices to connect without physical cables.

Understanding these basic concepts can provide a foundation for exploring more advanced topics in computer networking, such as network design, optimization, and troubleshooting.

Top of Form