CCA-102: Data Communications

ASSIGNMENT

1. What are the different types of networks?

Ans. **A computer network is a system in which multiple computers are connected to share information and resources.** Computer network varies with each other based on their functionality, geography, ownership, and communication media used.

So, in this blog, we are going to learn about various types of computer networks based on geographical areas they cover, functionality, ownership, and communication media used.

A computer network can be divided into the following types, based on the geographical area that they cover, they are:

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

Now, let us study these networks one by one:

LAN(Local Area Network)

A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc.

Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc. A LAN can use either wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed as **WLAN(Wireless Local Area Network)**.

Local Area Networks came under existence in around 1970s. IEEE developed the specifications for LAN. The speed of this network varies from 10mbps(Ethernet network) to 1gbps(FDDI or Gigabit Ethernet).

In other words, a LAN connects a relatively small number of machines in a relatively close geographical area. Bus, Ring, and Star topology are generally used in a local area network. In LAN, one computer can become a server in a star topology, serving all other computers called clients. Two different buildings can be connected very easily in LAN using a 'Bridge'.

Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. ***For example,*** a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LAN's are generally privately owned networks.

Following are the functionalities of a Local Area Network:

1. **File Serving:** In LAN, a large storage disk acts as a central storage repository.
2. **Print Serving:** Printers can be shared very easily in a LAN by various computers.
3. **Academic Support:** A LAN can be used in the classroom, labs, etc. for educational purposes.
4. **Manufacturing Support:** LAN can support the manufacturing and industrial environment.
5. **High Reliability:** Individual workstations might survive the network in case of failures.

Following are the advantages of a LAN:

1. File transfer and file access
2. Resource or peripherals sharing
3. Personal computing
4. Document distribution
5. Easy to design and troubleshoot
6. Minimum propagation delay
7. High data rate transfer
8. Low error rate
9. Easily scalable(devices can be added or removed very easily)

Following are the disadvantages of a LAN:

1. Equipment and support may be costly
2. Some hardware devices may not inter-operate properly

MAN(Metropolitan Area Network)

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).

The MAN spans over a geographical area of about 50km. The best example of MAN is the cable television network that spans over the whole city.

A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.

Uses of MAN are as follows:

1. MAN can be used for connecting the various offices of the same organization, spread over the whole city.
2. It can be used for communication in various governmental departments.

Following are the advantages of using MAN:

1. Large geographical area cover as compared to LAN
2. High-speed data connectivity
3. The Propagation delay of MAN is moderate

Following are the disadvantages of MAN:

1. It is hard to design and maintain a MAN
2. MAN is less fault-tolerant
3. It is costlier to implement
4. Congestions are more in a MAN

WAN(Wide Area Network)

A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example, the Internet.

A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.

In other words, WAN provides long distance transmission of data, voice, image, and video, over a large geographical area. A WAN may span beyond 100km range. It may be privately or publicly owned.

The protocols used in WAN are ISDN(Integrated Service Digital Network), SMDS(Switched Multi-Megabit Data Service), SONET(Synchronous Optical Network), HDLC(High Data Link Control), SDLC(Synchronous Data Link Control), etc.

The advantage of WAN is that it spans over a very large geographical area, and connects a huge mass of people.

Following are the disadvantages of WAN:

1. The propagation delay is more in a WAN
2. The data rate is low
3. The error rate is high
4. It is very complex to design a WAN

These are the types of network according to geographical area.

Following are the types of network, based on functionality:

- **Client-Server Network:** Client-Server network is a network in which a client runs the program and access data that are stored on the server. In this kind of network, one computer becomes the server, serving all other computers called clients.
- **Peer-to-Peer Network:** Peer-to-Peer network facilitates the flow of information from one peer to another without any central server. In other words, each node on a server acts as both client and server.

Following are the types of network, based on Ownership:

- **Private Network:** A private network is a network in which various restrictions are imposed to secure the network, to restrict unauthorized access. This type of network is privately owned by a single or group of people for their personal use. Local Area Network(LAN) can be used as a private network.
- **Public Network:** A public network is a network that has the least or no restrictions on it. It can be freely accessed by anyone, without any restrictions. This type of network is publicly owned by the government or NGOs. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as a public network.

Following are the types of network, based on Transmission Media:

- **Bound/Guided Media Network:** Bounded/Guided media can also be referred to as wired media. This kind of networks provides a physical link between two nodes connected in a network. The physical links are directed towards a particular direction in the network. Co-axial, twisted pair, optical fiber cable, etc. can be used in such networks for connectivity. Local Area Network(LAN) and Metropolitan Area Network(MAN) can be used as a Bound/Guided media network.
- **Unbound/Unguided Media Network:** Unbounded/Unguided media can also be referred to as wireless media. This kind of network does not need any physical link for electromagnetic transmission. Radio waves, Microwaves, Infrared, etc. can be used in such networks for connectivity. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as an Unbound/Unguided media network.

This is all about the various types of computer networks. Hope you learned something new today.

2 . Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

Ans . Introduction to Computer Networking

- Responsibilities of a network engineer
- What is a Computer Network?
- Why we need computer networks?
- Different types devices used to create a computer network
- Client Operating Systems and Network Operating Systems (NOS)
- Common Network Application Software
- Local Area Networks (LAN) and Wide Area Networks (WAN)
- Campus Area Networks (CAN) and Metropolitan Area Network (MAN)
- Logical Classification of Computer Networks - Peer to Peer Networks and Client/Server Networks
- Logical Classification of Computer Networks - Centralized and Distributed Computer Network Models
- Internetworks, Internet, Intranet and Extranet
- What is a Network Protocol
- Difference between Proprietary and Standard Protocols
- What are RFCs (Request for Comments)
- Organizations which control Internet, Network Protocols and Standards
- What is network topology
- Difference between physical topology and logical topology
- Network Topologies - Bus Topology
- Network Topologies - Star Topology
- Network Topologies - Mesh, Ring and Hybrid Topologies
- Network Topologies - Partial-Mesh Topology
- Network Topologies - Full-Mesh Topology
- Advantages and disadvantages of full-mesh topology
- Network Topologies - Ring Topology
- Network Topologies - Dual Ring Topology
- Network Topologies - Hybrid Topology
- Network Topologies - Tree Topology
- Point-to-point Topology and Point-to-multipoint Topology
- What are wireless networks? Advantages and disadvantages of wireless networks.
- Ad hoc Wireless Topology
- Infrastructure Wireless Topology
- Wireless Mesh Topology
- Network Infrastructure Devices and Icons
- Network Infrastructure Devices - What is a Hub?
- Network Infrastructure Devices - What are Bridges and Switches?
- Network Infrastructure Devices - What is a Router?
- Network Infrastructure devices - What is a Firewall
- Main office (Head Office) and Branch Office Networks
- Site-to-Site Network Topologies - Hub and Spoke Toplogy
- Site-to-Site Network Topologies - Partial-Mesh Toplogy
- Site-to-Site Network Topologies - Full Mesh Topology
- What is NIC (Network Interface Card)
- Common Network Cable types
- Twisted pair cable bandwidth and frequency range

- Different types of shields used in STP (shielded twisted pair cable)
- TIA/EIA 568A and TIA/EIA-568B standards
- Straight-Through and Cross-Over cables
- What is Auto-MDIX feature in ethernet switches
- Difference between Baseband and Broadband
- Network Access Methods - CSMA/CD, CSMA/CA and Token Passing
- IEEE (Institute of Electrical and Electronics Engineers)
- IEEE 802 Standards
- IEEE 802.11 Standards
- LAN Technologies - Ethernet
- Ethernet Media Standards
- 100Base-TX Ethernet Media Standard
- 100Base-FX Ethernet Media Standard
- 4D-PAM5 encoding in Gigabit Ethernet
- 1000Base-T Ethernet Media Standard
- 1000Base-SX Ethernet Media Standard
- 1000Base-LX Ethernet Media Standard
- 10GBase-T 10 Gigabit Ethernet Media Standard
- 10GBase-SR 10 Gigabit Optical Fiber Ethernet Media Standard
- Meaning of 10/100/1000 Ethernet
- Twisted pair Cable categories for 1 Gigbit and 10 Gigabit networks
- Broadband over Power Line (IEEE 1901-2010 standard)
- What is Power over Ethernet (PoE)
- What is PoE (Power over Ethernet) Switch
- LAN Technologies - Token Ring
- Advantages and disadvantages of Fiber optic cable
- Structure of fiber optic cable (FOC)
- Single Mode Fiber Optic Cable (SMF fiber cable)
- Multimode Fiber Optic Cable (MMF fiber cable)
- Different types of fiber optic cables
- Fiber optic transceivers
- Fiber optic connectors
- LAN Technologies - Fibre Distributed Data Interface (FDDI)

3 . What is difference between baseband and broadband transmission?

Ans . Difference between Broadband and Baseband Transmission

- Difficulty Level : Basic
- Last Updated : 19 Feb, 2021

Broadband system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.
Baseband is a digital signal is transmitted on the medium using one of the signal codes like NRZ, RZ Manchester biphase-M code etc. is called baseband transmission. These are following differences between Broadband and Baseband transmission.

Baseband transmission –

1. Digital signalling.
2. Frequency division multiplexing is not pssible.
3. Baseband is bi-directional transmission.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet is using Basebands for LAN.

Broadband transmission –

1. Analog signalling.
2. Transmission of data is unidirectional.
3. Signal travelling distance is long.
4. Frequency division multiplexing possible.
5. Simultaneous transmission of multiple signals over different frequencies.
6. Example : Used to transmit cable TV to premises.

S.No	Baseband Transmission	Broadband Transmission
1.	In baseband transmission, the type of signalling used is digital.	In broadband transmission, the type of signalling used is analog.
2.	Baseband Transmission is bidirectional in nature.	Broadband Transmission is unidirectional in nature.
3.	Signals can only travel over short distances.	Signals can be travelled over long distances without being attenuated.
4.	It works well with bus topology.	It is used with a bus as well as tree topology.
5.	In baseband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.

Attention reader! Don’t stop learning now. Get hold of all the important CS

5. What is the difference between a hub, modem, router and a switch?

Ans . Hub and Switch are both network connecting devices. Hub works at physical layer and is responsible to transmit the signal to port to respond where the signal was received whereas Switch enable connection setting and terminating based on need.

Following are the important differences between Hub and Switch.

A modem is the short way of saying “modulator, demodulator”. The primary purpose of a modem when used in a home networking environment is to establish a connection between your home internet connection and your ISP.

Now you may ask, why is this necessary? Well, the reason why we need modems is because unlike a router or a switch, different types of modems can transmit and receive data on different types of physical connections. For example, a DSL modem is capable of transferring data over a standard copper telephone line, a cable modem is capable of transferring data over a coax cable line, a fiber modem is capable of transferring data over a fiber optic line, a satellite modem is capable of transferring data over a satellite connection, and well, you get the gist. Each type of modem is capable of transferring data over a different type of physical connection using a set of communications standards, or protocols, that it was designed to support.

In the OSI Reference Model, the modem is considered a Layer 1 device. Modems transmit bits, which are essentially 0s and 1s. This is the most basic form of data.

A switch is simply a device that connects multiple devices on the same network. Unlike a router which is capable of creating and routing between multiple TCP/IP networks, a switch is a device that’s designed only to facilitate communications for devices on the same network.

5 . When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

Ans . Top 135 Networking Interview Questions and Answers

We have compiled the most frequently asked Networking Interview Questions and Answers that will help you to prepare for the Networking basics interview questions that an interviewer might ask you during your interview. In this list of Networking interview questions, we have covered all commonly asked basic and advanced interview questions on networking with detailed answers to help you clear the job interview.

The below list covers 130+ important interview questions for Networking for freshers candidates as well as Networking interview questions for experienced. This detailed guide of Network Engineer interview questions will help you to crack your Job interview easily.

Network Engineer Interview Questions and Answers

1) What is a Link?

A link refers to the connectivity between two devices. It includes the type of cables and protocols used for one device to be able to communicate with the other.

2) What are the layers of the OSI reference model?

There are 7 OSI layers: 1) Physical Layer, 2) Data Link Layer, 3) Network Layer, 4) Transport Layer, 5) Session Layer, 6) Presentation Layer, and 7) Application Layer.

3) What is the backbone network?

A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles the management of bandwidth and multiple channels.

4) What is a LAN?

LAN network

LAN stands for Local Area Network. It refers to the connection between computers and other network devices that are located within a small physical location.

5) What is a node?

A node refers to a point or joint where a connection takes place. It can be a computer or device that is part of a network. Two or more nodes are needed to form a network connection.

6) What are routers?

Router

Routers can connect two or more network segments. These are intelligent network devices that store information in its routing tables, such as paths, hops, and bottlenecks. With this info, they can determine the best path for data transfer. Routers operate at the OSI Network Layer.

7) What is a point to point link?

It refers to a direct connection between two computers on a network. A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers.

8) What is anonymous FTP?

Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed access to data in these servers do not need to identify themselves, but instead, log in as an anonymous guest.

9) What is a subnet mask?

A subnet mask is combined with an IP address to identify two parts: the extended network address and the host address. Like an IP address, a subnet mask is made up of 32 bits.

10) What is the maximum length allowed for a UTP cable?

A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.

11) What is data encapsulation?

Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.

12) Describe Network Topology

Network Topology refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect.

13) What is a VPN?

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

14) Briefly describe NAT

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share a single connection to the Internet.

15) What is the job of the Network Layer under the OSI reference model?

6. When troubleshooting computer network problems, what common hardware-related problems can occur?

Ans . Ethernet switches link Ethernet devices together by relaying Ethernet *frames* between the devices connected to the switches. By moving Ethernet frames between the switch *ports*, a switch links the traffic carried by the individual network connections into a larger Ethernet network.

Ethernet switches perform their linking function by *bridging* Ethernet frames between Ethernet *segments*. To do this, they copy Ethernet frames from one switch port to another, based on the *Media Access Control (MAC)* addresses in the Ethernet frames. Ethernet bridging was initially defined in the 802.1D IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.[1]

The standardization of bridging operations in switches makes it possible to buy switches from different vendors that will work together when combined in a network design. That's the result of lots of hard work on the part of the standards engineers to define a set of standards that vendors could agree upon and implement in their switch designs.

Bridges and Switches

The first Ethernet bridges were two-port devices that could link two of the original Ethernet system's coaxial cable segments together. At that time, Ethernet only supported connections to coaxial cables. Later, when twisted-pair Ethernet was developed and switches with many ports became widely available, they were often used as the central connection point, or hub, of Ethernet cabling systems, resulting in the name "switching hub." Today, in the marketplace, these devices are simply called switches.

Things have changed quite a lot since Ethernet bridges were first developed in the early 1980s. Over the years, computers have become ubiquitous, and many people use multiple devices at their jobs, including their laptops, smartphones, and tablets. Every VoIP telephone and every printer is a computer, and even building management systems and access controls (door locks) are networked. Modern buildings have multiple wireless access points (APs) to provide 802.11 Wi-Fi services for things like smartphones and tablets, and each of the APs is also connected to a cabled Ethernet system. As a result, modern Ethernet networks may consist of hundreds of switch connections in a building, and thousands of switch connections across a campus network.

What Is a Switch?

You should know that there is another network device used to link networks, called a *router*. There are major differences in the ways that bridges and routers work, and they both have advantages and disadvantages, as described in Routers or Bridges?. Very briefly, bridges move frames between Ethernet segments based on Ethernet addresses with little or no configuration of the bridge required. Routers move *packets* between networks based on high-level protocol addresses, and each network being linked must be configured into the router. However, both bridges and routers are used to build larger networks, and both devices are called switches in the marketplace.

TIP

We will use the words “bridge” and “switch” interchangeably to describe Ethernet bridges. However, note that “switch” is a generic term for network devices that may function as bridges, or routers, or even both, depending on their feature sets and configuration. The point is that as far as network experts are concerned, bridging and routing are different kinds of packet switching with different capabilities. For our purposes, we will follow the practices of Ethernet vendors who use the word “switch,” or more specifically, “Ethernet switch,” to describe devices that bridge Ethernet frames.

While the 802.1D standard provides the specifications for bridging local area network frames between ports of a switch, and for a few other aspects of basic bridge operation, the standard is also careful to avoid specifying issues like bridge or switch performance or how switches should be built. Instead, vendors compete with one another to provide switches at multiple price points and with multiple levels of performance and capabilities.

The result has been a large and competitive market in Ethernet switches, increasing the number of choices you have as a customer. The wide range of switch models and capabilities can be confusing. In Chapter 4, we discuss special purpose switches and their uses.

Operation of Ethernet Switches

Networks exist to move data between computers. To perform that task, the network software organizes the data being moved into Ethernet frames. Frames travel over Ethernet networks, and the data field of a frame is used to carry data between computers. Frames are nothing more than arbitrary sequences of information whose format is defined in a standard.

The format for an Ethernet frame includes a destination *address* at the beginning, containing the address of the device to which the frame is being sent.[2] Next comes a source address, containing the address of the device sending the frame. The addresses are followed by various other fields, including the data field that carries the data being sent between computers, as shown in Figure 1-1.

Figure 1-1. Ethernet frame format

Frames are defined at Layer 2, or the *Data Link Layer*, of the *Open Systems Interconnection (OSI)* seven-layer network model. The seven-layer model was developed to organize the kinds of information sent between computers. It is used to define how that information will be sent and to structure the development of standards for transferring information. Since Ethernet switches operate on local area network frames at the Data Link Layer, you will sometimes hear them called link layer devices, as well as Layer 2 devices or Layer 2 switches.[3]

Transparent Bridging

Ethernet switches are designed so that their operations are invisible to the devices on the network, which explains why this approach to linking networks is also called *transparent bridging*. “Transparent” means that when you connect a switch to an Ethernet system, no changes are made in the Ethernet frames that are bridged. The switch will automatically begin working without requiring any configuration on the switch or any changes on the part of the computers connected to the Ethernet network, making the operation of the switch transparent to them.

Next, we will look at the basic functions used in a bridge to make it possible to forward Ethernet frames from one port to another.

Address Learning

An Ethernet switch controls the transmission of frames between switch ports connected to Ethernet cables using the traffic *forwarding* rules described in the IEEE 802.1D bridging standard. Traffic forwarding is based on address learning. Switches make traffic forwarding decisions based on the 48-bit media access control (MAC) addresses used in LAN standards, including Ethernet.

To do this, the switch learns which devices, called *stations* in the standard, are on which segments of the network by looking at the source addresses in all of the frames it receives. When an Ethernet device sends a frame, it puts two addresses in the frame. These two addresses are the *destination* address of the device it is sending the frame to, and the *source* address, which is the address of the device sending the frame.

The way the switch "learns" is fairly simple. Like all Ethernet interfaces, every port on a switch has a unique factory-assigned *MAC address*. However, unlike a normal Ethernet device that accepts only frames addressed directed to it, the Ethernet interface located in each port of a switch runs in *promiscuous* mode. In this mode, the interface is programmed to receive *all* frames it sees on that port, not just the frames that are being sent to the MAC address of the Ethernet interface on that switch port.

As each frame is received on each port, the switching software looks at the source address of the frame and adds that source address to a table of addresses that the switch maintains. This is how the switch automatically discovers which stations are reachable on which ports.

Figure 1-2 shows a switch linking six Ethernet devices. For convenience, we're using short numbers for station addresses, instead of actual 6-byte MAC addresses. As stations send traffic, the switch receives every frame sent and builds a table, more formally called a *forwarding database*, that shows which stations can be reached on which ports. After every station has transmitted at least one frame, the switch will end up with a forwarding database such as that shown in Table 1-1.

7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?

Ans . he knowledge of Networking is the most crucial requirement for every interview. Often, these questions seem really easy, but turn up to be confusing when you go on to answer them. In this article, you will be learning some of the most important Networking Interview Questions along with the answers.

To begin with, here are the ten most important Networking Interview Questions:

Does not perform filtering	Filters packets before forwarding them	Highly configured to filter and send packets
Least intelligent, least expensive and least complex	Similar to a hub, but more effective	Extremely smart and complex

Q2. What is a link?

A link basically is the connection between two or more computers or devices. It can be anything depending on whether it is a physical connection or a wireless one. Physical links include cables, hubs, switches, etc and wireless links wireless access points, routers, etc.

Q3. What do you mean by a Node?

The point of intersection in a network is called a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in case there are computers, there will be three nodes and so on. It is not necessary for a node to be a computer, it can be any communicating device such as a printer, servers, modems, etc.

Q4. What does a backbone network mean?

In any system, backbone is the most principle component that supports all other components. Similarly, in networking, a Backbone Network is a Network that interconnects various parts of the network to which it belongs and has a high capacity connectivity infrastructure.

Q5. What is Network Topology?

The physical layout of the computer network is called as Network Topology. It gives the design of how all the devices are connected in a network.	Description

Bus Topology	All the devices share a common communication line
Star Topology	All nodes are connected to a central hub device
Ring Topology	Each node connects to exactly two other nodes
Mesh Topology	Each node is connected to one or more nodes
Tree Topology (Hierarchical Topology)	Similar to star topology and inherits the bus topology
Daisy Chain Topology	All nodes are connected linearly
Hybrid Topology	Nodes are connected in more than one topology styles
Point-to-Point Topology	Connects two hosts such as computers, servers, etc

Q6. Explain what is LAN?

A LAN or Local Area Network the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:

- Topology: The arrangement of nodes within the network
- Protocol: Refer to the rules for the transfer of data
- Media: These devices can be connected using optic fibers, twisted-pair wires, etc

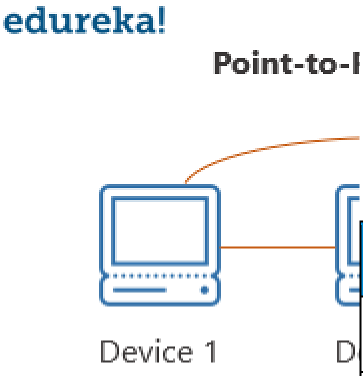
Q7. What are Routers?

A router is some device that transfers the data packets within a network. It basically performs the traffic directing functions within a network. A data packet can be anything such as an email, a web page, etc. Routers are located at the place where two or more networks meet or the gateways.

Routers can either be stand-alone devices or virtual. Stand-alone routers are traditional devices where as virtual routers are actually softwares that act like physical ones.

Q8. What is a Point-to-Point Network?

A Point-to-Point network refers to a physical connection between two nodes. It can be between any device of a network such as a computer, printer, etc.



For example, as you can see in the above diagram, all the nodes are connected to each other i.e Device 1 is connected to Device 2 and Device 3 , Device 2 is connected to Device 3 and Device 1 and Device 3 is connected to Device 2 and Device 1 using physical links.

Q9. What is OSI Model?

OSI stands for Open Systems Interconnection. It is a conceptual model that standardizes communication functions of telecommunication. It has 7 layers which are:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Q10. Give a brief about each layer in the OSI Model.

To learn about Network Programming in Java and Python in detail refer to the following blogs:

-

by anonymous FTP?

An anonymous FTP is a way of allowing a user to access data that is public. The user does not need to identify himself to the server and has to log in as anonymous.

So in case you are asked to use anonymous ftp, make sure you add “anonymous” in place of your user id. Anonymous FTPs are very effective while distributing large files to a lot of people, without having to give huge numbers of usernames and password combinations.

Q12. What is the meaning of Network?

A network is a connection between different devices. These devices communicate with each other using physical or wireless connections. Physical connections include twisted pair cables, optic fibers, and coaxial cables..wireless networks can be established with the help of waves such as radio waves infrared waves and microwaves
Networks basically serve many purposes such as:

8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans. A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.

11) What is data encapsulation?

Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.

12) Describe Network Topology

Network Topology refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect.

13) What is a VPN?

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

14) Briefly describe NAT

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share a single connection to the Internet.

15) What is the job of the Network Layer under the OSI reference model?

The Network layer is responsible for data routing, packet switching, and control of network congestion. Routers operate under this layer.

16) How does a network topology affect your decision to set a network?

Network topology dictates what media you must use to interconnect devices. It also serves as a basis on what materials, connectors, and terminations that is applicable for the setup.

17) What is RIP?

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

18) What are the different ways of securing a computer network?

There are several ways to do this. Install a reliable and updated anti-virus program on all computers. Make sure firewalls are setup and configured correctly. User authentication will also help a lot. All these combined would make a highly secured network.

19) What is NIC?

NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

20) What is WAN?

9. Discuss TCP/IP model in detail.

- ANS . A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
    - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:

    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
    - It provides connectionless service and end-to-end delivery of transmission.
    - It is an unreliable protocol as it discovers the errors but not specify the error.
    - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
    - **UDP consists of the following fields:**
      Source port address: The source port address is the address of the application program that has created the message.
      Destination port address: The destination port address is the address of the application program that receives the message.
      Total length: It defines the total number of bytes of the user datagram in bytes.
      Checksum: The checksum is a 16-bit field used in error detection.
    - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

10 . What is a Web Browser (Browser)? Give some example of browsers.

ANs . hat Is a Browser?

A web browser, or browser for short, is a computer software application that enables a person to locate, retrieve, and display content such as webpages, images, video, as well as other files on the World Wide Web.

Browsers work because every web page, image, and video on the web has its own unique Uniform Resource Locator (URL), allowing the browser to identify the resource and retrieve it from the web server.

What Is the Difference Between a Search Engine and a Browser?

Some people confuse web browsers and search engines, but they are not the same and perform different roles. A search engine is essentially a type of website that stores searchable information about other websites (common examples of search engines are Google, Bing, Yahoo, and Baidu). However, to connect to a website's server and display its webpages requires a browser. Some examples of browsers can be found below.

5 Popular Browsers

1. Google Chrome

Chrome, created by internet giant Google, is the most popular browser in the USA, perceived by its computer and smartphone users as fast, secure, and reliable. There are also many options for customization in the shape of useful extensions and apps that can be downloaded for free from the Chrome Store. Chrome also allows easy integration with other Google services, such as Gmail. Due to the success of the "Chrome" brand name, Google has now extended it to other products, for example, Chromebook, Chromebox, Chromecast, and Chrome OS.

2. Apple Safari

Safari is the default on Apple computers and phones, as well as other Apple devices. It's generally considered to be an efficient browser, its slick design being in keeping with the ethos of Apple. Originally developed for Macs, Safari has become a significant force in the mobile market due to the domination of iPhones and iPads. Unlike some of the other browsers listed, Safari is exclusive to Apple, it doesn't run on Android devices, and the Windows version of Safari is no longer supported by important security updates from Apple.

3. Microsoft Internet Explorer and Edge

Although it has been discontinued, Internet Explorer is worthy of mention as it was the go-to browser in the early days of the internet revolution, with usage share rising to 95% in 2003. However, its relatively slow start-up speed meant that many users turned to Chrome and Firefox in the years that followed. In 2015, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on Windows 10, making Internet Explorer 11 the final version to be released. At the time of writing, the market share of Microsoft Edge remains lower than Internet Explorer, which is still used by many people around the world.

4. Mozilla Firefox

Unlike Chrome, Safari, Internet Explorer, and Microsoft Edge, Firefox is an open-source browser, created by community members of the Mozilla Foundation. It is perhaps the most customizable of the main browsers, with many add-ons and extensions to choose from. In late 2003, it had a usage share of 32.21% before gradually losing out to competition from Google Chrome. It currently remains a strong competitor in the "desktop" field but has a lower market share in the mobile arena, where Google Chrome and Apple Safari tend to dominate.

5. Opera

Another web browser worthy of mention is Opera, which is designed for Microsoft Windows, Android, iOS, macOS, and Linux operating systems. It has some interesting features and is generally considered to be a reliable option by many users. Many of its earlier features have gone on to be incorporated into rival browsers. It also has a distinct user interface. At the time of writing, Opera has a usage of just 2.28% but remains influential, albeit from the fringes.

Which Browser Am I Using Right Now?

If you don't know or are unsure which browser or version that you are using to view this article right now, there are a number of ways to find out.

Probably the easiest way is to use a website which tells you. I've listed examples of three below (click on a link to find out):

- What's My Browser
- WhatIsMyBrowser.com
- thismachine.info

Another way to find out which browser you are using is through the browser itself. Browsers vary in their setup and layout, so it's impossible to give advice that works in every case. However, if you click on the browser's drop-down menu, usually found in the top right-hand corner of the page, then click on "help" and then "about," it will tell you which browser and version you are using in most cases.

This content is accurate and true to the best of the author’s knowledge and is not meant to substitute for formal and individualized advice from a qualified professional.

12 . What is the Internet & WWW? What are the uses of internet in our daily life?

ANs . Difference Between WWW and Internet

The terms World Wide Web (WWW) and the Internet are so often used interchangeably that the fundamental difference between the two is easily forgotten.

In simple words, WWW is just a common point of connectivity for information sharing that is facilitated by a global network of computers.

The internet, on the other hand, is a connection between computers and countless other devices that form a huge network of systems.

This article will further highlight the differences between WWW and the Internet within the context of the IAS Exam.

Differences between WWW and Internet

WWW (World Wide Web)	Internet
The World Wide Web is the common system for navigating the internet. It is not the only system that can be used for such access, but it is by far the most common one.	The internet is a public network of network with a maze of wired and wireless connections between separate groups of servers computers and countless devices from around the world
The World Wide Web is distinguished from other systems through its use of HTTP (Hypertext Transfer Protocol). It can be safely said that the HTTP is the language of the World Wide Web	Along with Internters, there also exist the Intranets, which is the same type of information network but more privatized in order to control access.
WWW is more software-oriented as compared to the Internet	Internet is primarily hardware-based.

The HTTP along with being the language of the World Wide Web also governs it by dealing with linking of files, documents and other resources	The internet is governed by a set of rules and regulations collectively known as Internet Protocol (IP). The IP deals with data transmitted through the internet.
The invention of the World Wide Web can be credited to Sir Tim Berners Lee. During his work at the European Organization for Nuclear Research in 1989, he had developed the basic idea of the WWW to merge the evolving technologies of computers, data networks and hypertext into a powerful and easy to use global information system.	The first workable prototype of the Internet was the ARPANET (Advanced Research Project Agency Network) in the late 1960s. After its adoption on January 1st 1983, researchers began to develop a "network of networks" which evolved into the modern form of the Internet

Both the World Wide Web and the Internet are concepts covered under the Science and Technology Segment of the UPSC IAS Exam. Aspirants can study this segment through the links given below

- Science and Technology Notes for UPSC
- How to Tackle Science and Technology for UPSC
- General Science Preparation for UPSC
- Science and Technology MCQs for UPSC
- Difference Between Hardware and Software

Aspirants can find more Difference Between Articles, by visiting the linked page

Difference Between WWW and Internet – Download PDF Here

Become familiar with the general pattern of the IAS Exam by visiting the IAS Syllabus page. For more exam-related preparation materials, refer to the links given in the table below:

Related Links

NCERT Bo Download		NCERT Notes for UPSC 2021
Intangible Cultural Heritage		PIB Summary and Analysis
Biological Weathering		WPI Index

13 . What is an Internet Service Provider? Give some example of ISP in India.

our individual homes).

ISPs provide the same service, except that they use different types of media to do so. ISPs bridge distant locations between cities, states, and countries. Because of these high speed backbone systems, we are able receive an email within seconds, stream our favorite movie without interruption, and play online games with no lag whatsoever.

Satellites

Let's go over the different types of media that are used in order to give you a broader understanding of how ISPs work.

Customers who live in remote locations, such as farms, deserts, and mountainous areas, may require a **satellite Internet service**. This involves transmitting and receiving data from a satellite orbiting about 22,000 miles above the earth. Although satellite communication is not as fast as other mediums, it does provide flexibility with limited environmental impact, and there is not as much need for support from the local telecommunications company.

These satellite terminals can also be used when setting up natural disaster recovery centers. For example, FEMA used a satellite terminal during Hurricane Katrina, since the public telecommunication infrastructure was severely damaged.

Fiber Optics

Fiber optics, or fiber, is a transmission medium used to transmit light instead of electrical voltage, like copper. The great thing about fiber is that it transmits Internet traffic at the speed of light!

Fiber has great qualities, such as being very reliable and immune to electromagnetic interference, unlike copper. Fiber has the bandwidth capability from 10 gigabits per second all the way up to 31 terabits per second. Without boosting stations (which boost or amplify the signal as it travels, and commonly used with copper), fiber can transmit signals up to 150 miles without regeneration. Right now, there are fiber cables that run along the ocean floor, connecting countries across the globe through high speed Internet access. Pretty cool!

Copper Cables

ISPs will more likely supply home users with a **copper** medium, such as that used for DSL or cable broadband. This works by sending electrical pulses through a copper wire. Broadband is cheap and provides excellent Internet service to the home user. It uses existing media found commonly in homes, such as your cable and telephone outlets, to provide users with Internet access. Most ISPs will provide their customers with equipment such as modems and routers to complete the installation and receive Internet access.

A typical home router is designed to route data between different networks using IP, or Internet Protocol. Whereas a modem simply establishes a connection between your home network and your ISP, a router helps facilitate communications between your home's network and the ISP's network. This is why your computer's IP address on your home network is different than the public IP address your ISP assigned you.

In the OSI Reference Model, the router is considered a Layer 3 device. Routers transmit packets and more importantly have the capability to transmitting data through different networks.

Typically, home routers also include built-in switches in order to provide the ability for multiple devices to be connected on the same network. Business or enterprise routers on the other hand may not include this functionality and requires a separate, standalone switch for this purpose.

14 . Discuss the difference between MAC address, IP address and Port address.

ANs . Difference between MAC Address and IP Address

- Difficulty Level : Easy
- Last Updated : 23 Dec, 2020

Both MAC Address and IP Address are used to uniquely defines a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.

The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

Let’s see the difference between MAC Address and IP Address:

S.NO	MAC Address	IP Address
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or eight byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card’s Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can’t be found easily by third party.	IP Address can be found by third party.

15 . How do we view my Internet browser's history?

ANs How do I view my Internet browser's history?

Updated: 11/13/2018 by Computer Hope

Today, all major browsers have functionality that allows you to quickly and easily view your Internet browser's history. However, as multiple devices contain browser history, there are multiple ways to view as well. To proceed, choose your devices from the section below and follow the instructions.

Desktop or laptop computer

If you are using Windows, Linux, or macOS, there are quick shortcut key combinations that allow you to view your history.

Windows and Linux users: Ctrl+H

Apple users: Command + Shift + H

Once one of the above shortcut keys is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.

Android phone or tablet running Google Chrome

Users who are running Google Chrome on their Android phone or tablet can view their history with the following steps.

1. Open the Google Chrome Internet browser.
2. In the upper-right corner of the screen **tap the** ⋮ **icon**.
3. In the drop-down menu that appears, select **history** and shown in the image.
4. The following page contains your device's history.

iPhone or iPad running Safari

Users who are running Safari for iOS on their iPhone or iPad can view their history with the following steps.

1. On your device, open the Safari Internet browser.
2. In the lower-left corner of the browser window, press and hold the back arrow.
3. The next screen contains your browser's history.