CCA-102: Data Communications

ASSIGNMENT

1. What are the different types of networks?

Ans: 11 Types of Networks in Use Today

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN)

We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

4. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

7. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

8. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called "SANs" as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical splitters to split an optical signal from one strand of single mode optical fiber into multiple signals to serve users and devices.

10. Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

11. Virtual Private Network (VPN)

By extending a private network across the Internet, a VPN lets its users send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection, users can access a private network remotely.

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

Ans:

BASIS FOR COMPARISON	UTP	STP
Basic	UTP (Unshielded twisted pair) is a cable with wires that are twisted together.	STP (Shielded twisted pair) is a twisted pair cable enclosed in foil or mesh shield.
Noise and crosstalk generation	High comparatively.	Less susceptible to noise and crosstalk.
Grounding cable	Not required	Necessarily required
Ease of handling	Easily installed as cables are smaller, lighter, and flexible.	Installation of cables is difficult comparatively.
Cost	Cheaper and does not require much maintenance.	Moderately expensive.
Data Rates	Slow comparatively.	Provides high data rates

3. What is difference between baseband and broadband transmission?

Ans: Baseband

Baseband transmissions typically use digital signaling over a single wire; the transmissions themselves take the form of either electrical pulses or light. The digital signal used in baseband transmission occupies the entire bandwidth of the network media to transmit a single data signal. Baseband communication is bidirectional, allowing computers to both send and receive data using a single cable. However, the sending and receiving cannot occur on the same wire at the same time.

Ethernet networks use baseband transmissions; notice the word "base"—for example, 10BaseT or 10BaseFL.

Using baseband transmissions, it is possible to transmit multiple signals on a single cable by using a process known as *multiplexing*. Baseband uses Time-Division Multiplexing

(TDM), which divides a single channel into time slots. The key thing about TDM is that it doesn't change how baseband transmission works, only the way data is placed on the cable.

Broadband

Whereas baseband uses digital signaling, broadband uses analog signals in the form of optical or electromagnetic waves over multiple transmission frequencies. For signals to be both sent and received, the transmission media must be split into two channels. Alternatively, two cables can be used: one to send and one to receive transmissions.

Multiple channels are created in a broadband system by using a multiplexing technique known as *Frequency-Division Multiplexing (FDM)*. FDM allows broadband media to accommodate traffic going in different directions on a single media at the same time.

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

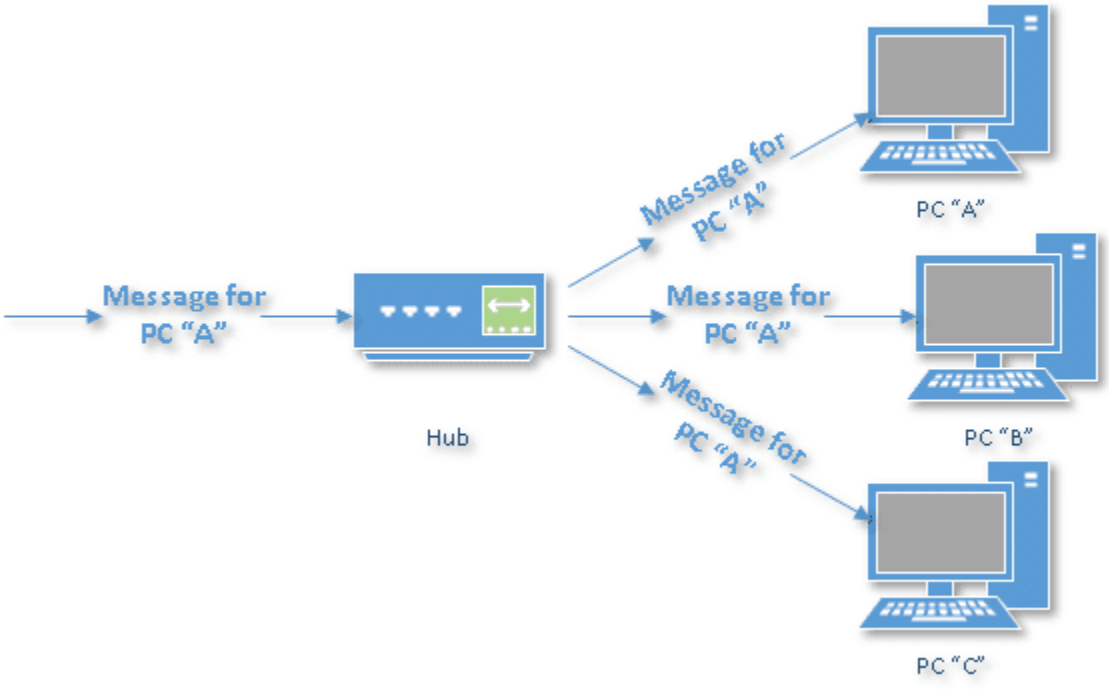
Ans: Hubs, switches, and routers are all devices that let you connect one or more computers to other computers, networked devices, or even other networks. Each has two or more connectors called ports, into which you plug the cables to make the connection.

- **Hubs are "dumb" devices that pass on anything received on one connection to all other connections.**
- **Switches are semi-intelligent devices that learn which devices are on which connection.**
- **Routers are essentially small computers that perform a variety of intelligent tasks**.

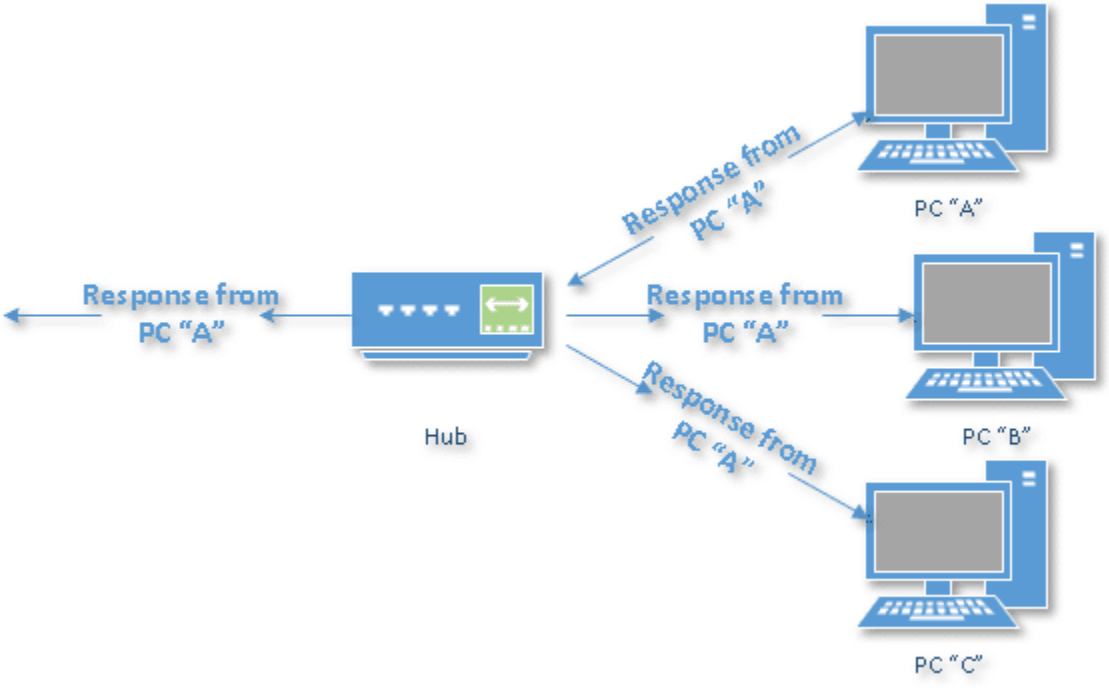
Hubs

A hub is the least expensive, least intelligent, and least complicated of the three. Its job is very simple: anything that comes in one port is sent out to the others. That's it.

If a message[1] comes in destined for computer "A", that message is sent out to all the other ports, regardless of which computer "A" is.



Incoming data passing through a hub.
When computer "A" responds, its response also goes out to every other port on the hub.



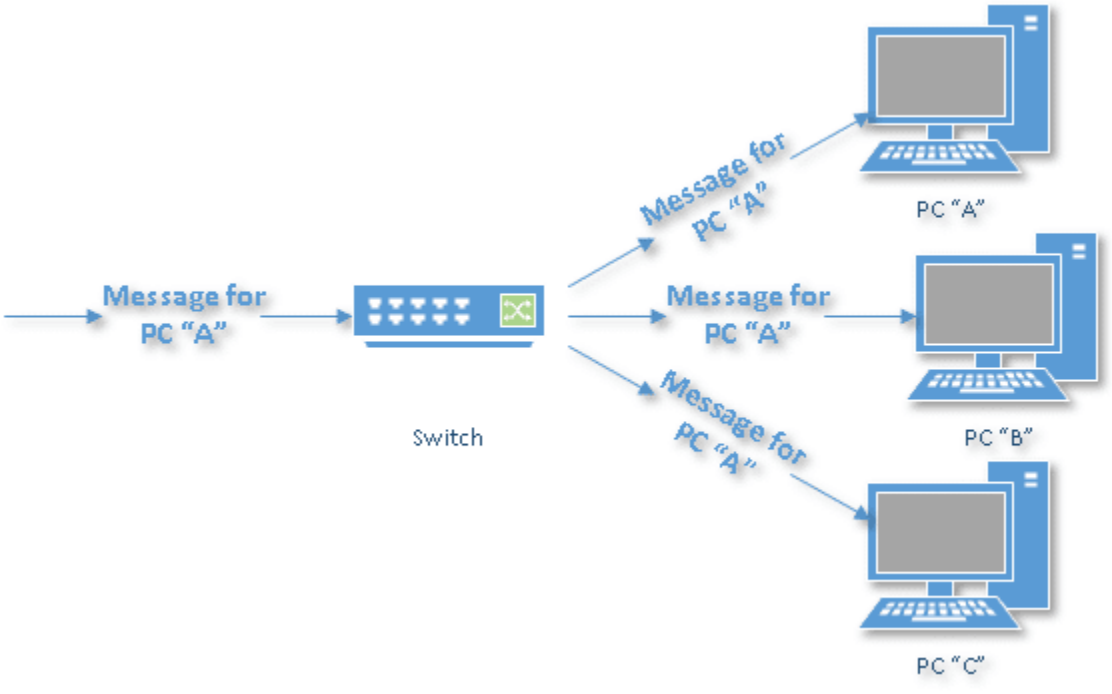
Returned response passing through a hub.
Every computer connected to the hub "sees" everything every other computer on the hub does. It's up to the computers themselves to decide if a message is for them and whether or not it should be paid attention to. The hub itself is blissfully ignorant of the data being transmitted.

For many years, hubs were quick and easy ways to connect computers in small networks. In recent years, hubs aren't as common, and switches have come into greater use.

Switches

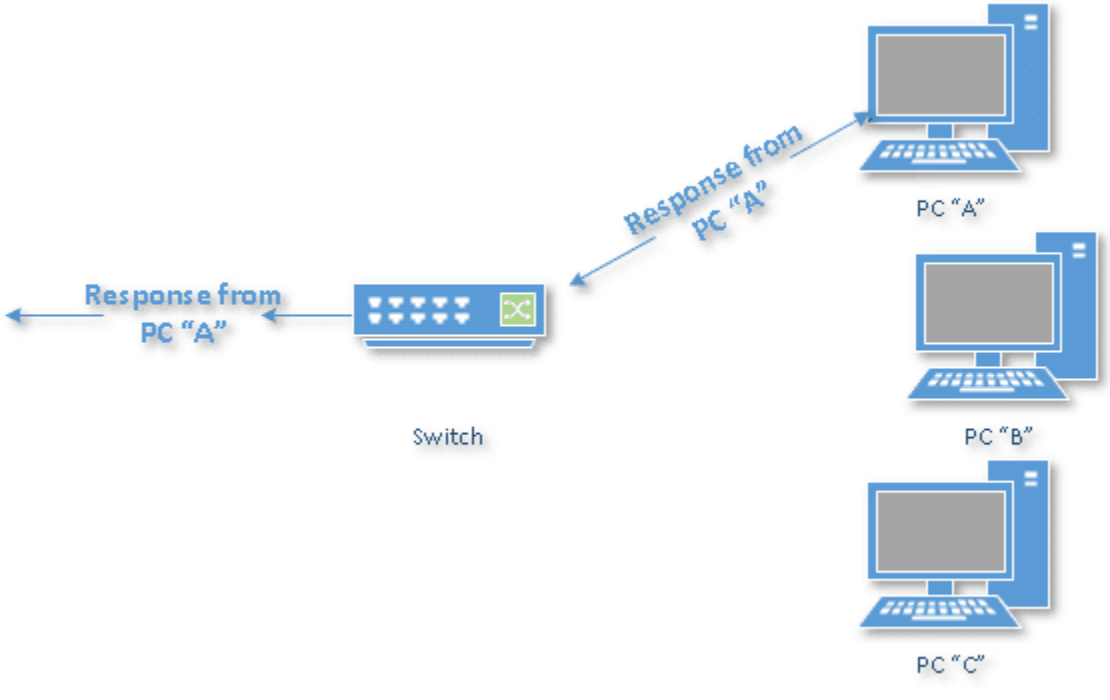
A switch does what a hub does, but more efficiently. By paying attention to the traffic that comes across it, it learns which computers are connected to which port.

Initially, a switch knows nothing, and simply sends on incoming messages to all ports.



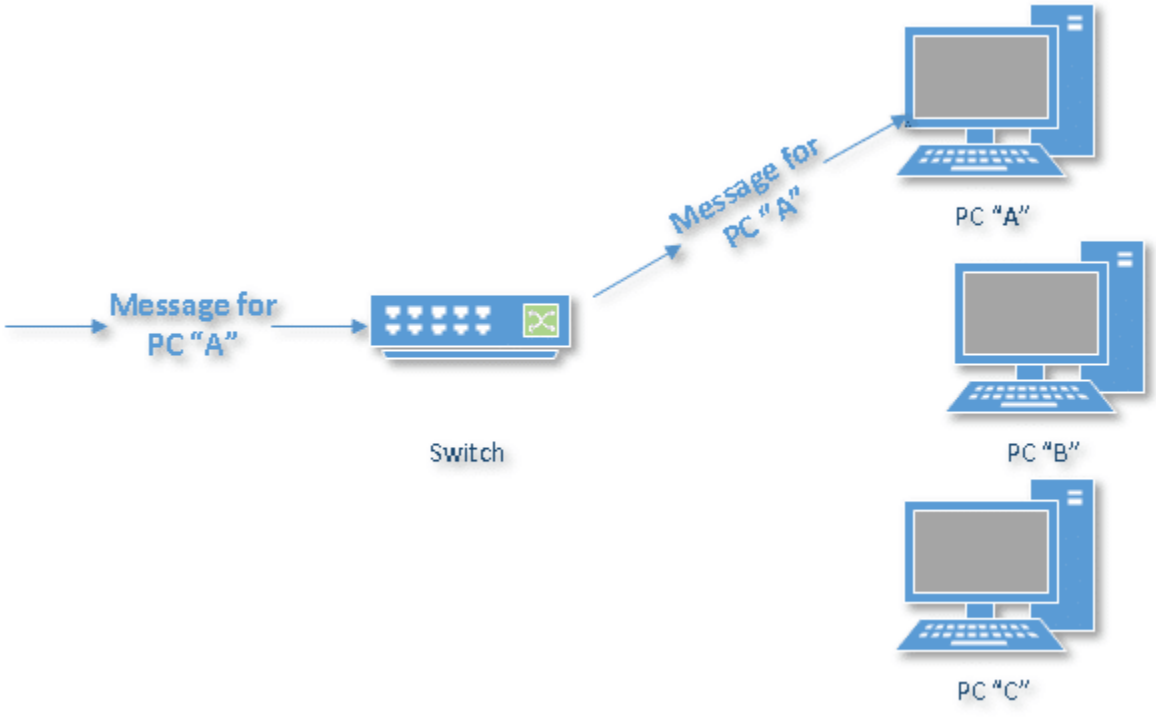
Incoming data passing through a switch.

Just by accepting that first message, however, the switch has learned something: it knows on which connection the *sender* of the message is located. Thus, when machine "A" responds to the message, the switch only needs to send that message out to the one connection.



Returned response passing through a switch.

By processing the response, the switch has learned something else: it now knows on which connection machine “A” is located. That means subsequent messages destined for machine “A” need only be sent to that one port.



Second incoming message passing through a switch.

Switches learn the location of the devices they are connected to almost instantaneously. The result is, most network traffic only goes where it needs to, rather than to every port. On busy networks, this can make the network *significantly* faster.

Routers

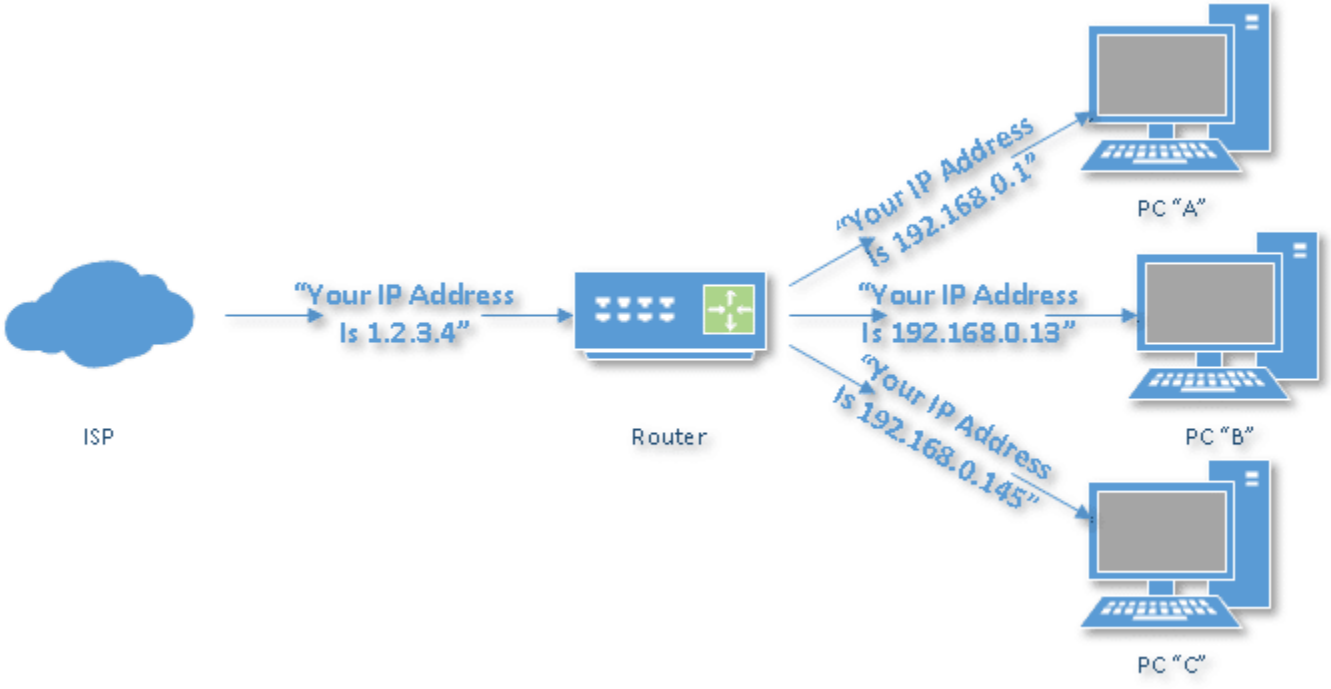
A router is the smartest and most complicated of the three. Routers come in all shapes and sizes, from small, four-port broadband routers to large industrial-strength devices that drive the internet itself.

One way to think of a router is as a computer[2] that can be programmed to understand, manipulate, and act on the data it handles.

A router operates as a switch for basic routing: it learns the location of the computers sending traffic, and routes information only to the necessary connections.

Consumer-grade routers perform (at minimum) two additional and important tasks: DHCP and NAT.

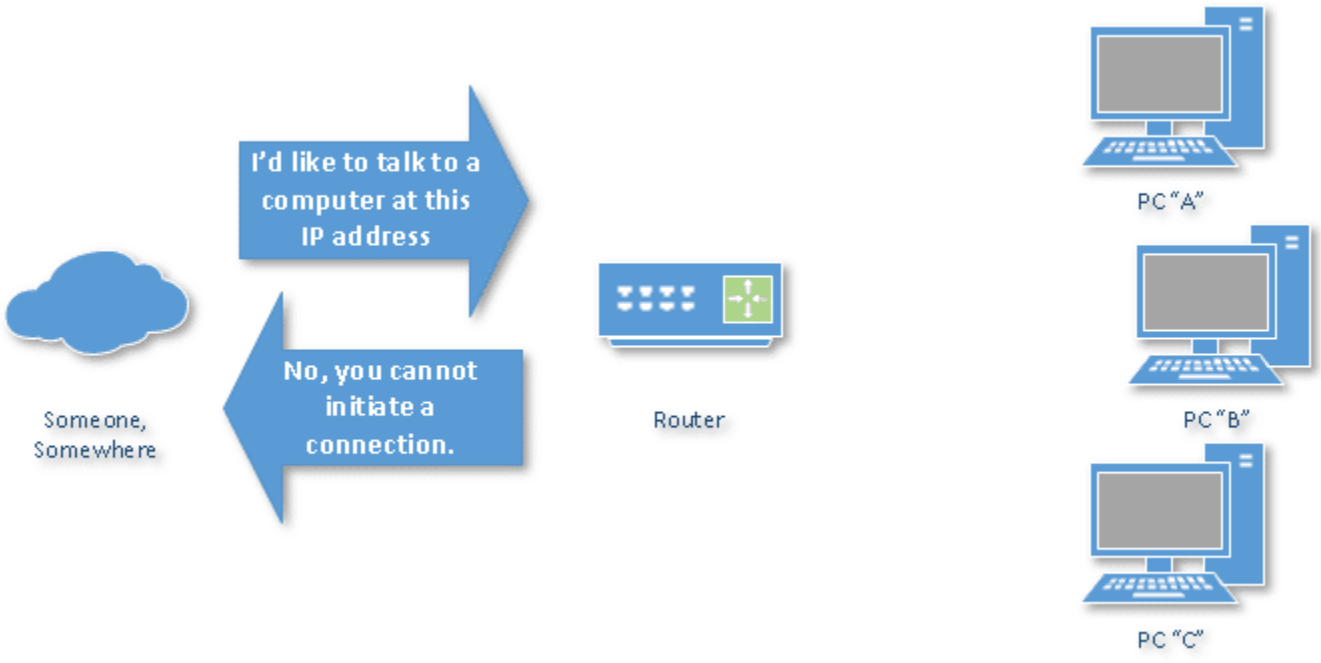
DHCP — Dynamic Host Configuration Protocol — is how dynamic IP addresses are assigned. When it first connects to the network, a device asks for an IP address to be assigned to it, and a DHCP server responds with an IP address assignment. A router connected to your ISP-provided internet connection will ask your ISP’s server for an IP address; this will be your IP address on the internet. Your local computers, on the other hand, will ask the router for an IP address, and these addresses are local to your network.



IP address assignments to and through a router.

NAT — Network Address Translation- – is the way the router *translates* the IP addresses of packets that cross the internet/local network boundary. When computer "A" sends a packet, the IP address that it's "from" is that of computer "A" — 192.168.0.1, in the example above. When the router passes that on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP — 1.2.3.4, in the example. It also keeps track, so if there's a response the router knows to do the translation in reverse, replacing the internet IP address with the local IP address for machine "A", and then sending that response packet on to machine "A".

A side effect of NAT is that machines on the internet cannot *initiate* communications to local machines; they can only respond to communications initiated by them. This means that the router also acts as an effective firewall.



Router acting as a firewall blocking outside access.

Malware that spreads by trying to independently connect to your computer over the network cannot do so.

All routers include some kind of user interface for configuring how the router treats traffic. Really large routers include the equivalent of a full-blown programming language to describe how they should operate, as well as the ability to communicate with other routers to describe or determine the best way to get network traffic from point A to point B.

Your modem is a box that connects your home network to the wider Internet. A router is a box that lets all of your wired and wireless devices use that Internet connection at once and also allows them to talk to one another without having to do so over the Internet. Often, your Internet service provider will give you one box that serves as both modem and router, but they're still different technologies; not all modems include routers and not all routers have modems. You need both, integrated or not, in order to provide an Internet connection for all the devices in your home.

We recommend using a separate modem and router, if you can. Since modem technology changes slowly, you can usually use a modem for years, until it breaks, but you might need to replace a router because you want better coverage, because you've added more devices to your network and your old router isn't keeping up, or because you want to take advantage of the latest improvements in Wi-Fi technology. You can often save money on your monthly Internet bill if you buy your own modem and router instead of using the ones your ISP provides, though this is usually true only if you have cable Internet, not DSL or fiber, and the situation is more complicated if you get phone service from your ISP as well.

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

Ans: The Media Access Control address (MAC address) for any network adapter is hard coded into the card itself. Each manufacturer of network adapters has a group of characters assigned that refer specifically to that company. I believe that is the first 1/2 of the MAC address which is 12 hexadecimal characters long. But the MAC address is part and parcel of the network adapter, just as your internal organs are part of you. When you move to a new house, you take your liver with you. In the same way, when you move a NIC to a different computer, it takes its MAC address with it.

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

Ans: We have to check the LAN DRIVER Has been installed.

Most of the time, the troubleshooting's comes from cables (Optical fibers included).

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

Ans: The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

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

Ans: Difference between Static and Dynamic IP address:

S.NO	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
1.	It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2.	Static imp address does not change any time, it means if a static imp address is provided then it can't be changed or modified.	While dynamic imp address change any time.
3.	Static imp address is less secure.	While in dynamic imp address, there is low amount of risk than static imp address's risk.

S.NO	STATIC IP ADDRESS	DYNAMIC IP ADDRESS
4.	Static imp address is difficult to designate.	While dynamic imp address is easy to designate.
5.	The device designed by static imp address can be trace.	But the device designed by dynamic imp address can't be trace.
6.	Static imp address is more stable than dynamic imp address.	While dynamic imp address is less stable than static imp address.
7.	The cost to maintain the static imp address is higher than dynamic imp address.	While the maintaining cost of dynamic imp address is less than static imp address.
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.

9. Discuss TCP/IP model in detail.

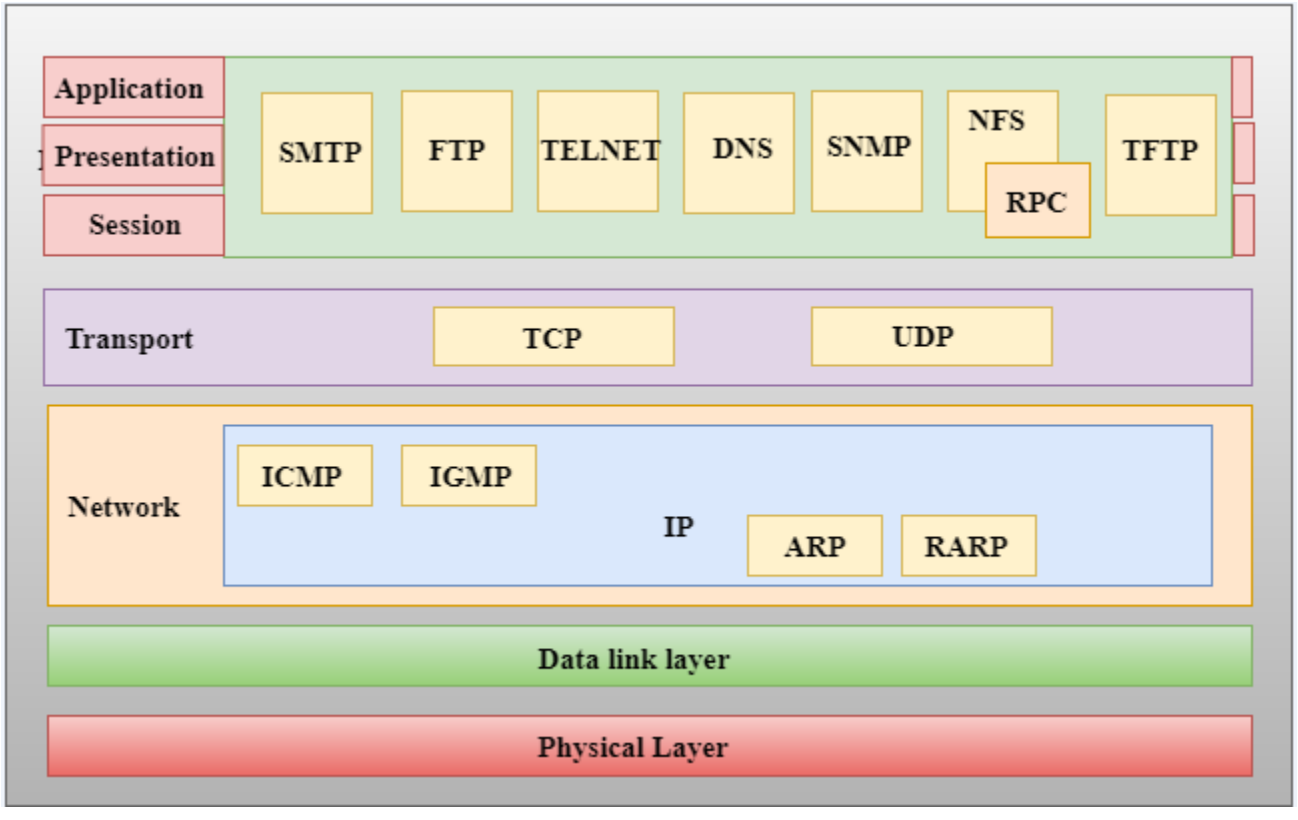
Ans: TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.

TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link la physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functio correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP mode layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functi

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



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

Ans: A **web browser** is a type of software that allows you to find and view websites on the Internet. Even if you didn't know it, you're using a web browser right now to read this page! There are many different web browsers, but some of the most common ones include **Google Chrome**, **Internet Explorer**, **Safari**, **Microsoft Edge**, and **Mozilla Firefox**.

11. What is a search engine? Give example.

Ans: A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. Search engines utilize automated software applications (referred to as robots, bots, or spiders) that travel along the Web, following links from page to page, site to site. The information gathered by the spiders is used to create a searchable index of the Web.

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

Ans: *The Internet* is a global network of networks while *the Web*, also referred formally as World Wide Web (www) is collection of information which is accessed via *the Internet*. Another way to look at this difference is; *the Internet* is infrastructure while *the Web* is service on top of that infrastructure. Alternatively, *the Internet* can be viewed as a big book-store while *the Web* can be viewed as collection of books on that store. At a high level, we can even think of *the Internet* as hardware and *the Web* as software!

1. **Online Booking**

Online booking is an astonishing tool on the internet. By this, we can book a train ticket, flight ticket (International and domestic), and you can book a taxi which will pick-up you from your doorstep.

In the present climate, you do not have to wait in queue for hours for ticket booking at the ticket counter. Now, while sitting at home you can book tickets online with the help of the laptop, tab, or Smartphone provided you should have an internet connection.

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

Ans: A company that provides subscribers with access to the Internet. BSNL, Airtel, Vodafone etc. are some examples of ISP in India.

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

Ans:

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 six 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.

Port Address Translation (PAT) is an extension of Network **Address** Translation (NAT) that permits multiple devices on a LAN to be mapped to a single public IP **address** to conserve IP **addresses**.

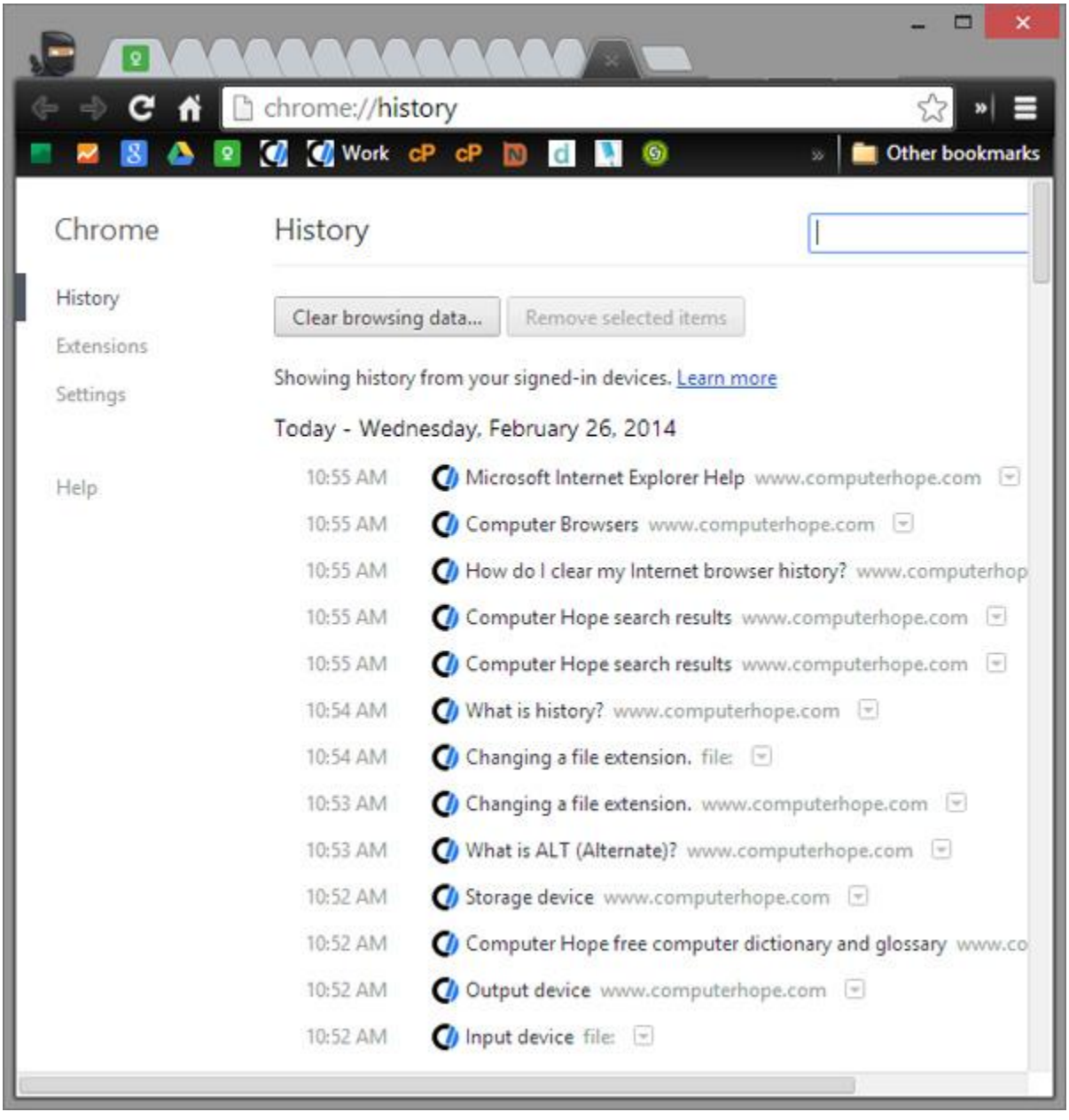
15. How do we view my Internet browser's history?

Ans: 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

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.


chrome://history
Work
Other bookmarks
Chrome
History
Extensions
Settings
Help
History
Clear browsing data...
Remove selected items
Showing history from your signed-in devices. Learn more
Today - Wednesday, February 26, 2014
10:55 AM Microsoft Internet Explorer Help www.computerhope.com
10:55 AM Computer Browsers www.computerhope.com
10:55 AM How do I clear my Internet browser history? www.computerhop
10:55 AM Computer Hope search results www.computerhope.com
10:55 AM Computer Hope search results www.computerhope.com
10:54 AM What is history? www.computerhope.com
10:54 AM Changing a file extension. file:
10:53 AM Changing a file extension. www.computerhope.com
10:53 AM What is ALT (Alternate)? www.computerhope.com
10:52 AM Storage device www.computerhope.com
10:52 AM Computer Hope free computer dictionary and glossary www.co
10:52 AM Output device www.computerhope.com
10:52 AM Input device file: