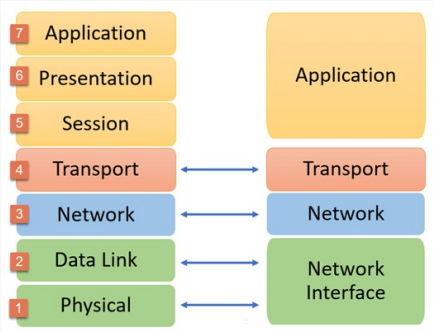
## OSI Layers

| Layers | Data Units | Functions |
|---|---|---|
| *Application Layer* | Data | Mail Services, Directory Services, FTAM |
| *Presentation Layer* | Data | Encryption/Decryption, Compression |
| *Session Layer* | Data | Session Establishment, Synchronization, Dialog Controller |
| *Transport Layer* | Segments, Datagram | Segmentation |
| *Network Layer* | Packets | Traffic control, Fragmentation, Routing |
| *Data Link Layer* | Frames | Flow control, Error control, Access control |
| *Physical Layer* | Bits | Bit Synchronization, Bit rate control, Physical Topologies |

## OSI x TCP/IP Model




## Types of Networks

| Type | Description |
|---|---|
| PAN | Personal Network is a network consisting of only a small number of devices owned by an individual. |
| LAN | A local area network is a network that covers a small area (for example, a company's network). |

## Types of Networks (cont)

| | |
|---|---|
| WAN | A wide Area Network is a network that includes many devices and covers a large area. Usually collectively owned. |
| MAN | MAN stands for Metropolitan Area Network. It is a computer network that connects a findnumber of LANs to form a larger network so that the computer resources can be shared. |

## Network Topologies

| Name | Description |
|---|---|
| Bus Topology | A bus topology, also called a line topology, is a type of network topology in which all network devices are connected through a central RJ-45 network cable or coaxial cable. |
| Ring Topology | A ring topology is a type of network topology in which each device is connected to two other devices on either side using RJ-45 or coaxial cables. |
| Star Topology | A star topology is a network topology in which each element of the network is physically connected to a central node such as a router, hub, or switch. In a star topology, hubs act as servers, and connecting nodes act as clients. |
| Mesh Topology | In a mesh topology, each node is connected to at least one other node and often to multiple nodes. Each node can send and receive messages from other nodes. |
| Tree Topology | A tree topology is a hybrid network topology in which star networks are interconnected by bus networks. Tree networks are hierarchical and each node can have any number of child nodes. |

## Network Topologies (cont)

| | |
|---|---|
| Hybrid Topology | A hybrid topology is a type of network topology that uses two or more different network topologies. These topologies can include mixed bus topologies, mesh topologies, ring topologies, star topologies, and tree topologies. |

## Advantages vs. Disadvantages Network Topologies

**BUS TOPOLOGY**

*Advantages*

- It is the easiest network topology for connecting peripherals or computers in a linear fashion.
- It works very efficiently well when there is a small network.
- The length of cable required is less than a star topology.
- It is easy to connect or remove devices in this network without affecting any other device.
- Very cost-effective as compared to other network topology i.e. mesh and star
- It is easy to understand topology.
- Easy to expand by joining the two cables together.

*Disadvantages*

- Bus topology is not great for large networks.
- Identification of problems becomes difficult if the whole network goes down.
- Troubleshooting individual device issues is very hard.
- Need terminators are required at both ends of the main cable.
- Additional devices slow the network down.
- If the main cable is damaged, the whole network fails or splits into two.
- Packet loss is high.
- This network topology is very slow as compared to other topologies.

**STAR TOPOLOGY**

*Advantages*

- It is very reliable – if one cable or device fails then all the others will still work
- It is high-performing as no data collisions can occur
- Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.
- Easier to put in
- Robust in nature

## Advantages vs. Disadvantages Network Topologies (cont)

- Easy fault detection because the link are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.
- If N devices are connected to every other in star, then the amount of cables required to attach them is N. So, it's easy to line up.

*Disadvantages*

- Requires more cable than a linear bus .
- If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.
- More expensive than linear bus topology due to the value of the connecting devices (network switches)
- If hub goes down everything goes down, none of the devices can work without hub.
- Hub requires more resources and regular maintenance because it's the central system of star .
- Extra hardware is required (hubs or switches) which adds to cost
- Performance is predicated on the one concentrator i.e. hub.

**RING TOPOLOGY**

*Advantages*

- In this data flows in one direction which reduces the chance of packet collisions.
- In this topology additional workstations can be added after without impacting performance of the network.
- Equal access to the resources.
- There is no need of server to control the connectivity among the nodes in the topology.
- It is cheap to install and expand.
- Minimum collision.
- Speed to transfer the data is very high in this type of topology.
- Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.
- Easy to manage.
- Ring network is extremely orderly organized where every device has access to the token and therefore the opportunity to transmit.

*Disadvantages*

- Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.

## Advantages vs. Disadvantages Network Topologies (cont)

- If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
- It is slower in performance as compared to the bus topology
- It is Expensive.
- Addition and removal of any node during a network is difficult and may cause issue in network activity.
- Difficult to troubleshoot the ring.
- In order for all the computer to communicate with each other, all computer must be turned on.
- Total dependence in on one cable.
- They were not Scalable.

**MESH TOPOLOGY**

*Advantage*

- Failure during a single device won't break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- Fault identification is straightforward.
- This topology provides multiple paths to succeed in the destination and tons of redundancy.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn't disrupt its processes.
- Adding new devices won't disrupt data transmissions.
- This topology has robust features to beat any situation.
- A mesh doesn't have a centralized authority.

*Disadvantage*

- It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- The cost to implement mesh is above other selections.
- There is a high risk of redundant connections.
- Each node requires a further utility cost to think about.
- Maintenance needs are challenging with a mesh.

**TREE TOPOLOGY**

## Advantages vs. Disadvantages Network Topologies (cont)

*Advantage*

- This topology is the combination of bus and star topology.
- This topology provides a hierarchical as well as central data arrangement of the nodes.
- As the leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
- The other nodes in a network are not affected if one of their nodes gets damaged or does not work.
- Tree topology provides easy maintenance and easy fault identification can be done.
- A callable topology. Leaf nodes can hold more nodes.
- Supported by several hardware and software vendors.
- Point-to-point wiring for individual segments.
- Tree Topology is highly secure.
- It is used in WAN.
- Tree Topology is reliable.

*Disadvantage*

- This network is very difficult to configure as compared to the other network topologies.
- The length of a segment is limited & the limit of the segment depends on the type of cabling used.
- Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.
- If the computer on the first level is erroneous, the next-level computer will also go under problems.
- Requires a large number of cables compared to star and ring topology.
- As the data needs to travel from the central cable this creates dense network traffic.
- The Backbone appears as the failure point of the entire segment of the network.
- Treatment of the topology is pretty complex.
- The establishment cost increases as well.
- If the bulk of nodes is added to this network, then the maintenance will become complicated.

**HYBRID TOPOLOGY**

*Advantages*

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.

## Advantages vs. Disadvantages Network Topologies (cont)

- It is very reliable.
- It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
- Error detecting and troubleshooting are easy.
- Handles a large volume of traffic.
- It is used to create large networks.
- The speed of the topology becomes fast when two topologies are put together.

*Disadvantages*

- It is a type of network expensive.
- The design of a hybrid network is very complex.
- There is a change in the hardware to connect one topology with another topology.
- Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.
- Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
- Installation is a difficult process.

*Uses*

- Hybrid Topology helps in keeping the full diversity of the computer network.
- Hybrid Topology is helpful when we require more than one topology in the system.
- Hybrid Topology helps in reducing the cost of the overall system.
- Hybrid Topology helps in easily running the system.
- Hybrid Topology is widely used in educational institutes, research organizations, finance sectors, etc.

## Type of Multiplexers

| Type | Description |
|---|---|

## Type of Multiplexers (cont)

| | |
|---|---|
| Frequency Division Multiplexing (FDM) | The frequency spectrum is divided into logical channels and each user has exclusive access to his channel. It transmits signals in several different frequency ranges and multiple video channels over a single cable. Each signal is modulated onto a different carrier frequency and the carrier frequencies are separated by guard bands. |
| Time Division Multiplexing (TDM) | Each user gets full bandwidth for a short period of time on a regular basis. The entire channel is dedicated to her one user, but only for a short time. |
| Wavelength Division Multiplexing | This is the same as FDM but applied to fiber, with the difference that here the operating frequency is much higher, actually in the optical range. Due to its extremely high bandwidth, fiber optic has great potential. |

## Network Devices

| Device | Description |
|---|---|
| Client | Any device, such as a workstation, laptop, tablet, or smartphone, that is used to access a network. |
| Server | Provides resources to network users, including email, web pages, or files. |

## Network Devices (cont)

| | |
|---|---|
| Hub | A Layer 1 device that does not perform any inspection of traffic. A hub simply receives traffic in a port and repeats that traffic out of all the other ports. |
| Switch | A Layer 2 device that makes its forwarding decisions based on the destination Media Access Control (MAC) address. A switch learns which devices reside off which ports by examining the source MAC address. The switch then forwards traffic only to the appropriate port, and not to all the other ports. |
| Router | A Layer 3 device that makes forwarding decisions based on Internet Protocol (IP) addressing. Based on the routing table, the router intelligently forwards the traffic out of the appropriate interface. |
| Multilayer | Can operate at both Layer 2 and Layer 3. Also called a Layer 3 switch, a multilayer switch is a high-performance device that can switch traffic within the LAN and forward packets between subnets. |
| Media | Media can be copper cabling, fiber-optic cabling, or radio waves. Media varies in its cost, bandwidth capacity, and distance limitation. |
| Analog Modem | Modem is short for modulator/demodulator. An analog modem converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. |

## Network Devices (cont)

| | |
|---|---|
| Broadband Modem | A digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the analog modem, but use higher broadband frequencies and transmission speeds. |
| Access Point | A network device with a built-in antenna, transmitter, and adapter that provides a connection point between WLANs and a wired Ethernet LAN. APs usually have several wired RJ-45 ports to support LAN clients. Most small office or home office (SOHO) routers integrate an AP. |

## IEEE Standards

| *Standards | *Description* |
|---|---|
| IEEE 802 | LAN/MAN |
| IEEE 802.1 | LAN/MAN Bridging and management |
| IEEE 802.1s | Multiple spanning tree |
| IEEE 802.1 w | Rapid reconfiguration of spanning tree |
| IEEE 802.1x | Port-based network access control |
| IEEE 802.2 | Logical Link Control (LLC) |
| IEEE 802.3 | CSMA/CD access method (Ethernet) |
| IEEE 802.3ae | 10 Gigabit Ethernet |
| IEEE 802.4 | Token passing bus access method and Physical layer specifications |
| IEEE 802.5 | Token Ring access method and Physical layer specifications |
| IEEE 802.6 | Distributed Queue Dual Bus (DQDB) access method and Physical layer specifications (MAN) |
| IEEE 802.7 | Broadband LAN |
| IEEE 802.8 | Fiber Optic |
| IEEE 802.9 | Isochronous LANs (standard withdrawn) |
| IEEE 802.10 | Interoperable LAN/MAN Security |

## IEEE Standards (cont)

| | |
|---|---|
| IEEE 802.11 | Wireless LAN MAC and Physical layer specifications |
| IEEE 802.11a | Wireless with speed upto 54 Mbps |
| IEEE 802.11b | Wireless with speed upto 11 Mbps |
| IEEE 802.11g | Wireless with speed upto 54 Mbps |
| IEEE 802.11n | Wireless with speed upto 600 Mbps |
| IEEE 802.12 | Demand-priority access method, physical layer and repeater specifications |
| IEEE 802.13 | not used |
| IEEE 802.14 | Cable modems (proposed standard was withdrawn) |
| IEEE 802.15 | Wireless Personal Area Network (WPAN) |
| IEEE 802.16 | Wireless Metropolitan Area Network (Wireless MAN) |
| IEEE 802.17 | Resilient Packet Ring (RPR) Access |

## Cables (according to IEEE)

| Ethernet Standards | Data Rate | Cable Fiber Type | Maximum Distance |
|---|---|---|---|
| Ethernet (10Base-FL) | 10 Mbps | 50m or 62.5um Multimode @ 850nm | 2km |
| Fast Ethernet (100Base-FX) | 100 Mbps | 50m or 62.5um Multimode @ 1300nm | 2km |
| Fast Ethernet (100Base-SX) | 100 Mbps | 50m or 62.5um Multimode @ 850nm | 300m |
| Gigabit Ethernet (1000Base-SX) | 1000 Mbps | 50m Multimode @ 850nm | 550m |
| Gigabit Ethernet (1000Base-SX) | 1000 Mbps | 62.5um Multimode @ 850nm | 220m |
| Gigabit Ethernet (1000Base-LX) | 1000 Mbps | 50m or 62.5um Multimode @ 1300nm | 550m |
| Gigabit Ethernet (1000Base-LX) | 1000 Mbps | 9um Singlemode @1310nm | 5km |

## Cables (according to IEEE) (cont)

| | | | |
|---|---|---|---|
| Gigabit Ethernet (1000Base-LH) | 1000 Mbps | 9um Singlemode @1550nm | 70km |

## Types of Ethernet Networks

| Speed | Common Name | Informal IEEE Standard Name | Formal IEEE Standard Name | Cable Type, Maximum Length |
|---|---|---|---|---|
| 10 Mbps | Ethernet | 10BASE-T | 802.3 | Copper, 100 m |
| 100 Mbps | Fast Ethernet | 100BASE-T | 802.3u | Copper, 100 m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-LX | 802.3z | Fiber, 5000 m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-T | 802.3ab | Copper, 100 m |
| 10 Gbps | 10 Gig Ethernet | 10GBASE-T | 802.3an | Copper, 100 m |

## Transmission Media (Guided Media)

| Type of Media | Description |
|---|---|
| Twisted Pair Cable | It is a superimposed winding of two separately insulated conductors. As a rule, several such pairs are grouped together in a protective cover. They are the most widely used transmission media. |
| Coaxial Cable | It has a PVC or Teflon insulating layer and an outer plastic sheath containing two parallel conductors, each with a separate conformal protective cover. |

## Transmission Media (Guided Media) (cont)

| | |
|---|---|
| Optical Fiber Cable | It uses the concept of light reflection through a glass or plastic core. The core is surrounded by a less dense glass or plastic shell called the cladding. Used to transfer large amounts of data. |
| Stripline | Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett at the Air Force Cambridge Research Center in the 1950s. Stripline is the earliest form of planar transmission line. |
| Microstripline | Conductive material is separated from the ground plane by a dielectric layer. |

## Mode of Communication

| Type | Description | Example |
|---|---|---|
| Simplex Mode | In simplex mode, communication is one-way, like one-way. Only one of the two devices on the link can transmit, the other can only receive. Simplex mode allows data to be sent in one direction using the full capacity of the channel. | Television/Radio Signal |

## Mode of Communication (cont)

| | | |
|---|---|---|
| Half-Duplex Mode | In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device transmits, the other device can only receive and vice versa. Half-duplex mode is used when simultaneous communication in both directions is not required. | Walkie-Talkie |
| Full-Duplex Mode | In full-duplex mode, both stations can transmit and receive at the same time. In full-duplex mode, signals in one direction share the capacity of the link with signals in the other direction. This sharing can be done in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving. Or the capacity is divided between signals traveling in both directions. | Telephone call |

## Layers and their uses

| TCP/IP | OSI | Protocols | Devices/Apps |
|---|---|---|---|

## Layers and their uses (cont)

| | | | |
|---|---|---|---|
| Application | Application | DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP | Web server, Mail Server, browser, mail client |
| Application | Presentation | JPEG, MIDI, MPEG, PICT, TIFF | Web server, Mail Server, browser, mail client |
| Application | Session | NetBIOS, NFS, PAP, SCP, SQL, ZIP | Web server, Mail Server, browser, mail client |
| Transport | Transport | TCP, UDP, SPX, AppleTalk | Gateway |
| Internet | Network | ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP | Router, Firewall (Layer 3), Switch |
| Link | Data Link | ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring | Bridge, Switch (Layer 2) |
| Link | Physical | Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi | Hub |

## Collision Detection

| Type | Description |
|---|---|
| Carrier Sense Multiple Access with Collision Detection (CSMA/CD) | In this method, after sending a frame, the station monitors the media to see if the transmission was successful. If successful, the transmission is terminated, otherwise the frame is retransmitted. |

## Collision Detection (cont)

| | |
|---|---|
| Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) | The basic idea behind CSMA/CA is that stations must be able to receive while transmitting in order to detect collisions from different stations. A collision in a wired network nearly doubles the energy of the received signal, allowing stations to detect a potential collision. |
| ALOHA | It was developed for wifi, but can also be used for shared media. Multiple stations can transmit data at the same time, which can lead to collisions and data corruption. |

## Transmission Media (Unguided Media)

| Type of Media | Description |
|---|---|
| Radio waves | hese are easy to generate and can penetrate buildings. There is no need to align the transmit and receive antennas. Frequency Range: 3kHz – 1GHz AM radios, FM radios, and cordless phones use radio waves for transmission. |
| Microwaves | Multiplexer types: line-of-sight transmission. H. Transmitting and receiving antennas should be placed properly. The distance a signal travels is directly proportional to the height of the antenna. Frequency Range: 1GHz – 300GHz They are mainly used for mobile telephony and television distribution. |

## Transmission Media (Unguided Media) (cont)

| | |
|---|---|
| Infrared | Infrared is used for short distance communication. Obstacles cannot be penetrated. This prevents interf-erence between systems. Frequency Range: 300GHz – 400THz It is used in TV remote controls, wireless mice, keyboards, printers, etc. |

## Computer Network Protocols

| Network Protocol | Description | Port Number |
|---|---|---|
| Ethernet | A family of protocols that specify how devices on the same network segment format and transmit data. | 44818, 2222 |
| Wi-Fi or WLAN | A family of protocols that deal with wireless transmission. | - |
| TCP | Splits data into packets (reassembles later). Error checking is also included, as the acknowledgment is expected to be sent within a specified timeframe. | 22 |
| UDP | User Datagram Protocol | 4096-65535 |
| IP | Every device has an IP address. Packets are “addressed” to ensure they reach the correct user. | - |
| HTTP | Used to access web pages from a web server. | 80 |
| HTTP’S | uses encryption to protect data. | 443 |
| FTP | File Transfer Protocol: Handles file uploads and downloads, transferring data and programs. | 21 |

## Computer Network Protocols (cont)

| | | |
|---|---|---|
| SMTP | SMTP server has a database of user email addresses. Internet Message Access Protocol: Handles incoming mail. | 587 |
| IMAP | Internet Message Access Protocol: Process incoming mail. | 993 |
| ARP | ARP finds a host’s hardware address (also known as MAC (Media Access Control) address) based on its known IP address. | - |
| DNS | DNS is the host name for the IP address translation service. DNS is a distributed database implemented on a hierarchy of name servers. It is an application layer protocol for messaging between clients and servers. | 53 |
| FTPS | FTPS is known as FTP SSL which refers to File Transfer Protocol (FTP) over Secure Sockets Layer (SSL) which is more secure from FTP. FTPS also called as File Transfer Protocol Secure. | 21 |
| POP3 | POP3 is a simple protocol that only allows downlo-ading messages from your Inbox to your local computer. | 110 |

| Computer Network Protocols (cont) | | |
|---|---|---|
| SIP | Session Initiation Protocol was designed by IETF and is described in RFC 3261. It's the protocol of application layer that describes the way to found out Internet telephone calls, video conferences and other multimedia connections, manage them and terminate them. | 5060,5061 |
| SMB | The SMB protocol was developed by Microsoft for direct file sharing over local networks. | 139 |
| SNMP | SNMP is an application layer protocol that uses UDP port numbers 161/162. SNMP is also used to monitor networks, detect network errors, and sometimes configure remote devices. | 161 |
| SSH | SSH (Secure Shell) is the permissions used by the SSH protocol. That is, a cryptographic network protocol used to send encrypted data over a network. | 22 |
| VNC | VNC stands for Virtual Network Communication. | 5900 |

| Computer Network Protocols (cont) | | |
|---|---|---|
| RPC | Remote Procedure Call (RPC) is a powerful technique for building distributed client-server based applications. It is based on extending traditional calls to local procedures so that the called procedure does not have to be in the same address space as the calling procedure. | 1024 to 5000 |
| NFS | NFS uses file handles to uniquely identify the file or directory on which the current operation is being performed. Internet Control Message Protocol (ICMP) to provide error control. Used for reporting errors and administrative queries. | 2049 |
| ICMP | Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. | - |
| BOOTP | Bootstrap Protocol (BOOTP) is a network protocol used by network management to assign IP addresses to each member of that network in order to join other network devices through a main server. | 67 |
| DHCP | Dynamic Host Configuration Protocol (DHCP) is an application layer protocol. DHCP is based on a client-server model, based on discoveries, offers, requests, and ACKs. | 68 |

| Computer Network Protocols (cont) | | |
|---|---|---|
| NAT | Network Address Translation (NAT) is the process of translating one or more local IP addresses into one or more global IP addresses, or vice versa, in order to provide Internet access to local hosts. | 5351 |
| PPP | Point-to-Point Protocol (PPP) is basically an asymmetric protocol suite for various connections or links without framing. H. Raw bit pipe. PPP also expects other protocols to establish connections, authenticate users, and carry network layer data as well. | 1994 |
| RIP | Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between source and destination networks. | 520 |
| OSPF | Open Shortest Path First (OSPF) is a link-state routing protocol used to find the best path between a source and destination router using its own shortest path first). | 89 |
| EIGRP | Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol used to find the best path and deliver packets between any two Layer 3 devices. | 88 |

| Computer Network Protocols (cont) | | |
|---|---|---|
| BGP | Border Gateway Protocol (BGP) is a protocol used to exchange Internet routing information and is used between ISPs in different ASes. | 179 |
| STP | Spanning Tree Protocol (STP) is used to create a loop-free network by monitoring the network, tracking all connections, and shutting down the least redundant connections. | 0 to 255 |
| RARP | RARP, stand for Reverse Address Resolution Protocol, is a computer network-based protocol used by client computers to request IP addresses from a gateway server's Address Resolution Protocol table or cache. | - |
| LDAP | The D-channel LAPD or Link Access Protocol is basically the Layer 2 protocol normally required for the ISDN D-channel. It is derived from the LAPB (Link Access Protocol Balanced) protocol. | - |
| IPsec | IP Security (IPSec) is a standard suite of Internet Engineering Task Force (IETF) protocols between two communication points on IP networks to provide data authentication, integrity, and confidentiality. It also defines encrypted, decrypted, and authenticated packets. | 4500 |

| Computer Network Protocols (cont) | | |
|---|---|---|
| ASCII | ASCII (American Standard Code for Information Interchange) is the standard character encoding used in telecommunications. The ASCII representation “ask-ee” is strictly a 7-bit code based on the English alphabet. ASCII codes are used to represent alphanumeric data. | 9500 |
| EBCDIC | EBCDIC (Extended Binary Encoded Decimal Interchange Code) (pronounced “ehb-suh-dik” or “ehb-kuh-dik”) is an alphanumeric binary code developed by IBM to run large-scale computer systems . | - |
| X.25 PAD | X.25 is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) protocol standard simply for Wide Area Network (WAN) communications that basically describes how the connections among user devices and network devices are established and maintained. | - |

| Computer Network Protocols (cont) | | |
|---|---|---|
| HDLC | High-Level Data Link Control (HDLC) commonly uses the term “frame” to denote units or logs of units of data that are frequently transmitted or transmitted from one station to another, express. Each frame on the link must start and end with a flag sequence field (F). | - |
| SLIP | SLIP stands for Serial Line Internet Protocol. It is a TCP/IP implementation which was described under RFC 1055 (Request for Comments). | - |
| LAP | Link Access Procedure (LAP) is basically considered as an ITU family of Data Link Layer (DLL) protocols that are subsets of High-Level Data Link Control (HDLC). LAP is particularly derived from IBM’s System Development Life Cycle (SDLC). | - |
| NCP | Network Control Protocol (NCP) is a set of protocols that are part of Point-to-Point Protocol (PPP). | 524 |
| Mobile IP | Mobile IP is a communication protocol (created by extending the Internet Protocol, IP) that allows a user to move from one network to another using the same her IP address. | 434 |

## Computer Network Protocols (cont)

| | | |
|---|---|---|
| VOIP | Voice over Internet Protocol (VoIP), is a technology that allowing you to make voice calls over a broadband Internet connection instead of an analog (regular) phone line. Some VoIP services allow you to call people using the same service, but others may allow you to call anyone. | 5060 |
| LDAP | Lightweight Directory Access Protocol (LDAP) is an internet protocol works on TCP/IP, used to access information from directories. LDAP protocol is basically used to access an active directory. | 389 |
| GRE | GRE or Generic Routing Encapsulation is a tunneling protocol developed by Cisco. It encapsulates IP packets i.e. deliverable inner packets into outer packets. | 47 |
| AH | The HTTP headers Authorization header is a request type header that used to contains the credentials information to authenticate a user through a server. If the server responds with 401 Unauthorized and the WWW-Authenticate header not usually. | 51 |

## Computer Network Protocols (cont)

| | | |
|---|---|---|
| ESP | Encapsulation security payload, also abbreviated as ESP plays a very important role in network security. ESP or Encapsulation security payload is an individual protocol in IPSec. | 500 |
| NNTP | Network News Transfer Protocol (NNTP) is the underlying protocol of UseNet, which is a worldwide discussion system which contains posts or articles which are known as news. | 119 |
| RPC-DCOM | DCOM- Distributed Component Object Model– helps remote object via running on a protocol known as the Object Remote Procedure Call (ORPC). | - |
| IRC | Internet Relay Chat (IRC) is an Internet application that was developed by Jakko Oikarinen in Finland. Chat is the most convenient immediate way to communicate with others via Internet. | 6667 |

## OSI Protocols

**Application Layer Protocols**

*TELNET*: Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.

*DNS*: DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.abcd.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.

## OSI Protocols (cont)

*DHCP*: DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.

*FTP*: FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.

*SMTP*: SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25 and 587.

*HTTP*: HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers, but this protocol can also be used for several other purposes. HTTP is a stateless protocol (network protocol in which a client sends requests to server and server responses back as per the given state), which means the server is not responsible for maintaining the previous client's requests. HTTP uses port number 80.. *NFS*: NFS stands for Network File System. This protocol allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally. NFS uses the port number 2049.

*SNMP*: SNMP stands for Simple Network Management Protocol. This protocol gathers data by polling the devices from the network to the management station at fixed or random intervals, requiring them to disclose certain information. SNMP uses port numbers 161 (TCP) and 162 (UDP).

**Presentation Layers Protocols**

*Apple Filing Protocol (AFP)*: Apple Filing Protocol is the proprietary network protocol (communications protocol) that offers services to macOS or the classic macOS. This is basically the network file control protocol specifically designed for Mac-based platforms.

*Lightweight Presentation Protocol (LPP)*: Lightweight Presentation Protocol is that protocol which is used to provide ISO presentation services on the top of TCP/IP based protocol stacks.

## OSI Protocols (cont)

*NetWare Core Protocol (NCP)*: NetWare Core Protocol is the network protocol which is used to access file, print, directory, clock synchronization, messaging, remote command execution and other network service functions.

*Network Data Representation (NDR)*: Network Data Representation is basically the implementation of the presentation layer in the OSI model, which provides or defines various primitive data types, constr-ucted data types and also several types of data representations.

*External Data Representation (XDR)*: External Data Representation (XDR) is the standard for the description and encoding of data. It is useful for transferring data between computer architectures and has been used to communicate data between very diverse machines. Converting from local representation to XDR is called encoding, whereas converting XDR into local representation is called decoding.

*Secure Socket Layer (SSL)*: The Secure Socket Layer protocol provides security to the data that is being transferred between the web browser and the server. SSL encrypts the link between a web server and a browser, which ensures that all data passed between them remains private and free from attacks.

**Session Layer Protocols**

*AppleTalk Data Stream Protocol (ADSP)*: ADSP is that type of protocol which was developed by Apple Inc. and it includes a number of features that allow local area networks to be connected with no prior setup. This protocol was released in 1985.
This protocol rigorously followed the OSI model of protocol layering. ADSP itself has two protocols named: AppleTalk Address Resolution Protocol (AARP) and Name Binding Protocol (NBP), both aimed at making system self-configuring.

*Real-time Transport Control Protocol (RTCP)*: RTCP is a protocol which provides out-of-band statistics and control information for an RTP (Real-time Transport Protocol) session. RTCP's primary function is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistical information such as transmitted octet and packet counts or packet loss to the partic-ipants in the streaming multimedia session.

*Point-to-Point Tunneling Protocol (PPTP)*: PPTP is a protocol which provides a method for implementing virtual private networks. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP (Point-to-Point Protocol) packets This protocol provides security levels and remote access levels comparable with typical VPN (Virtual Private Network) products.

*Password Authentication Protocol (PAP)*: Password Authentication Protocol is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users.

## OSI Protocols (cont)

Almost all network operating systems, remote servers support PAP. PAP authentication is done at the time of the initial link establishment and verifies the identity of the client using a two-way handshake (Client-sends data and server in return sends Authentication-ACK (Acknowledgement) after the data sent by client is verified completely).. *Remote Procedure Call Protocol (RPCP)*: Remote Procedure Call Protocol (RPCP) is a protocol that is used when a computer program causes a procedure (or a sub-routine) to execute in a different address space without the programmer explicitly coding the details for the remote interaction. This is basically the form of client-server interaction, typically implemented via a request-response message-passing system.

*Sockets Direct Protocol (SDP)*: Sockets Direct Protocol (SDP) is a protocol that supports streams of sockets over Remote Direct Memory Access (RDMA) network fabrics.

The purpose of SDP is to provide an RDMA-accelerated alternative to the TCP protocol. The primary goal is to perform one particular thing in such a manner which is transparent to the application.

**Transport Layer Protocols**

*Transmission Control Protocol (TCP)*
*User Datagram Protocol (UDP)*
*Stream Control Transmission Protocol (SCTP)*
*Datagram Congestion Control Protocol (DCCP)*
*AppleTalk Transaction Protocol (ATP)*
*Fibre Channel Protocol (FCP)*
*Reliable Data Protocol (RDP)*
*Reliable User Data Protocol (RUDP)*
*Structured Steam Transport (SST)*
*Sequenced Packet Exchange (SPX)*

**Data Link Layer Protocols**

*Synchronous Data Link Protocol (SDLC)*
*High-Level Data Link Protocol (HDLC)*
*Serial Line Interface Protocol (SLIP)for encoding*
*Point to Point Protocol (PPP)*
*Link Access Procedure (LAP)*
*Link Control Protocol (LCP)*
*Network Control Protocol (NCP)*

**Physical Layer Protocols**

*Ethernet with 1000BASE-T.*

## OSI Protocols (cont)

*Ethernet with 1000BASE-SX.*
*Ethernet at 100BaseT.*
*Synchronous Digital Hierarchy/Optical Synchronisation.*
*Physical-layer variations in 802.11.*
*Bluetooth.*
*Networking for controllers.*
*U.S. Serial Bus*

## Network Layer Services

| Type | Description |
|---|---|
| Packet-izing | The process of encapsulating data (also called payload) received from upper layers of the network into network layer packets at the source and decapsulating the payload from the network layer packets at the destination is called packetization. |
| Routing and Forwarding | These are two other services provided by the network layer. A network has many routes from a source to a destination. The network layer sets some strategies for finding the best possible route. This process is called routing. |