./

Learning Report – Networking



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be approved By** | **Remarks/Revision Details** |
| 1 |  | Name/PS No | Name/PS No | Module Owner Name | Comments |
| 2 | 15/02/21 |  |  |  |  |
| 3 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Document History**

**Network:**

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

**Type of Networks:**

There are various types of computer networks available. We can categorize them according to their size as well as their purpose.

* **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.

****

* **Local Area Network(LAN)**

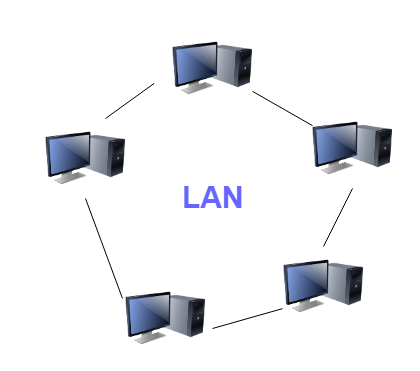
Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) their size,

(2) their transmission technology,

(3) their topology.

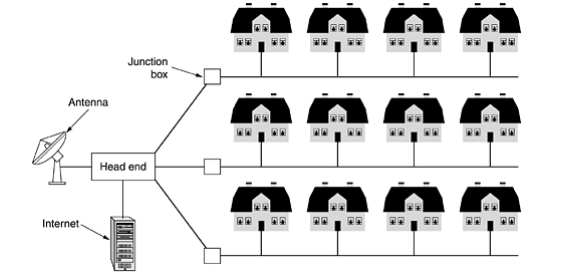
LANs are restricted in size.



* **Metropolitan Area Networks(MAN)**

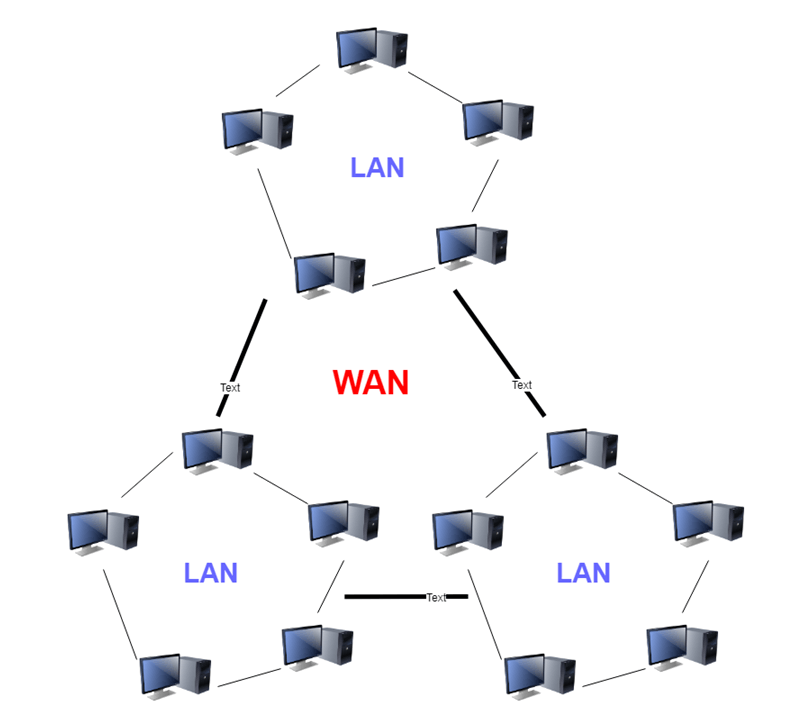
A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

* A metropolitan area network based on cable TV

****

* **Wide Area Networks**:

1. A wide area network, or WAN, spans a large geographical area, often a country or continent.
2. It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
3. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider.
4. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design.



**Network Topologies:**

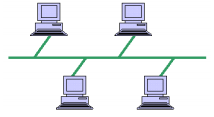
* Topology - Physical and logical network layout
* Physical: actual layout of the computer cables and other network devices
* Logical: the way in which the network appears to the devices that use it.

**Common topologies:**

* Bus, ring, star, mesh and wireless

**Bus topology:**

* Uses a trunk or backbone to which all of the computers on the network connect
* Systems connect to this backbone using T connectors or taps
* Coaxial cablings (10Base-2, 10Base5) were popular options years ago.

. 

**Advantages:**

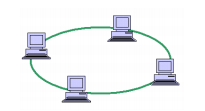
* Cheap and easy to implement
* Require less cable
* Does not use any specialized network equipment.

**Disadvantages:**

* Network disruption when computers are added or removed
* A break in the cable will prevent all systems from accessing the network.
* Difficult to troubleshoot

**Ring Topology:**

* Meaning that data travels in circular fashion from one computer to another on the network.
* Typically FDDI, SONET or Token Ring technology are used to implement a ring network.
* Ring networks are most commonly wired in a star configuration.
* Token Ring has multi-station access unit (MSAU), equivalent to hub or switch. MSAU performs the token circulation internally.

****

**Advantages:**

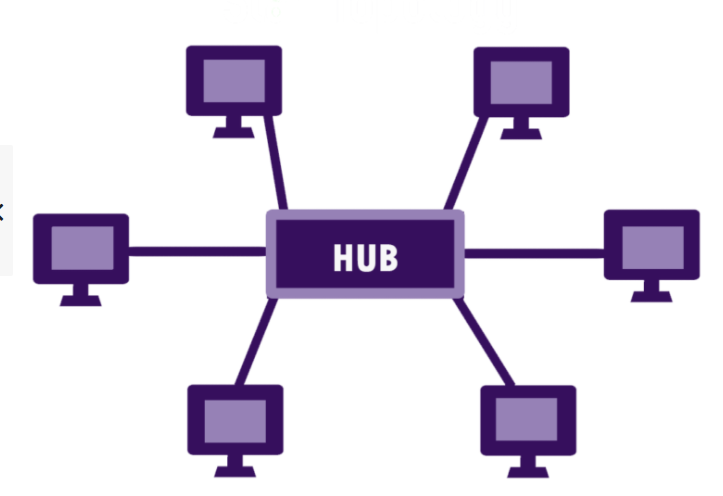
* Cable faults are easily located, making troubleshooting easier.
* Ring networks are moderately easy to install.

**Disadvantages:**

* Expansion to the network can cause network disruption.
* A single break in the cable can disrupt the entire network.

**Star Topology:**

* All computers/devices connect to a central device called hub or switch.
* Each device requires a single cable.
* point-to-point connection between the device and hub.
* Most widely implemented.
* Hub is the single point of failure.

****

**Advantages:**

* Easily expanded without disruption to the network.
* Cable failure affects only a single user.
* Easy to troubleshoot and isolate problems.

**Disadvantages:**

* Requires more cable.
* A central connecting device allows for a single point of failure.
* More difficult to implement.

**Mesh Topology:**

* Each computer connects to every other.
* High level of redundancy
* Rarely used.

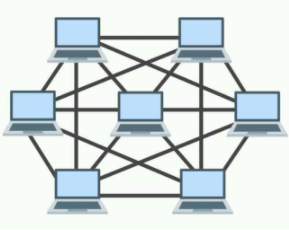
– Wiring is very complicated

– Cabling cost is high

– Troubleshooting a failed cable is tricky

– A variation hybrid mesh

– create point to point connection between specific network devices, often seen in WAN implementation.

****

**Advantages:**

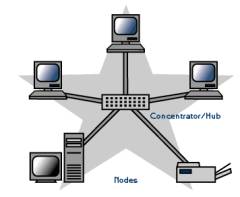
* Provides redundant paths between devices.
* The network can be expanded without disruption to current uses.

**Disadvantages:**

* Requires more cable than the other LAN topologies.
* Complicated implementation.

**Wired Networks:**

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second to 100Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today.



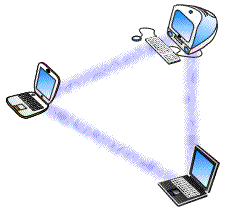
Some of the Ethernet standards are:

* 802.3 – It is a 10BASE5 thick coax, which has data rate of 10Mbps and operates on CSMA/CD (Carrier Sense Multiple Access with Collision Detection) process
* 802.3a – It is a 10BASE2 thin coax, which has data rate of 10Mbps.
* 802.3i – It is a 10BASET twisted pair cable, which has data rate of 10Mbps.
* 802.3j - 10Base-F (fiber optic)
* 802.3u – It is a 100BASET twisted pair cable, which has data rate of 100Mbps.
* 802.3x - Full duplex
* 802.3ae - 10-Gigabit Ethernet
* 802.3ba - 40Gbps & 100Gbps Ethernet

**Wireless Networks**

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. (Wi-fi.com)

An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.



**Some wireless networking standards are:**

* 802.11a - 802.11a applies to wireless local area networks and supports a maximum a maximum connect rate of 54Mbps throughput in the 5GHz band.
* 802.11b - 802.11b applies to wireless local area networks and supports a maximum connect rate of 11Mbps with fallback to 5.5, 2, and 1Mbps in the 2.4GHz ISM band
* 802.11n- This standard works on both the 2.4 GHZ and 5 GHZ bands, its net data ranges from 54Mbits/s to 600Mbits/s.

**Queuing:**

Regardless of how simple or how sophisticated the rest of the resource allocation mechanism is, each router must implement some queuing discipline that governs how packets are buffered while waiting to be transmitted. The queuing algorithm can be thought of as allocating both bandwidth (which packets get transmitted) and buffer space (which packets get discarded). It also directly affects the latency experienced by a packet by determining how long a packet waits to be transmitted. This section introduces two common queuing algorithms first-in, first-out (FIFO) and fair queuing (FQ)—and identifies several variations that have been proposed.

**Scheduling:**

In computing, **s**cheduling is the method by which work is assigned to resources that complete the work. The work may be virtual computation elements such as threads, processes or data flows, which are in turn scheduled onto hardware resources such as processors, network links or expansion cards

## **IPv4 addresses:**

* An IP address (*internet protocol address*) is a numerical representation that uniquely identifies a specific interface on the network.
* IPv4 addresses are 32-bit binary numbers, consisting of the two sub addresses (identifiers), identify the network and the host to the network, with an imaginary boundary separating the two. An IP address is, as such, generally shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form.
* For example, the address **168.212.226.204** represents the 32-bit binary number 10101000.11010100.11100010.11001100.
* The binary number is important because that will determine which class of network the IP address belongs to.
* An IPv4 address is typically expressed in dotted-decimal notation, with every eight bits (octet) represented by a number from one to 255, each separated by a dot.
* An example IPv4 address would look like this:192.168.17.22
* IPv4 addresses are composed of two parts. The first numbers in the address specify the network, while the latter numbers specify the specific host. A subnet mask specifies which part of an address is the network part, and which part addresses the specific host.
* A packet with a destination address that is not on the same network as the source address will be forwarded, or routed, to the appropriate network. Once on the correct network, the host part of the address determines which interface the packet gets delivered to.

## **IPv6 addresses:**

* To avoid the seemingly reoccurring issue in technology, where a specification’s limitation seems more than sufficient at the time, but inevitably becomes too small, the designers of IPv6 created an enormous address space for IPv6. The address size was increased from 32 bits in IPv4 to 128 bits in IPv6.
* The IPv6 has a theoretical limit of 3.4 x 1038 addresses.
* IPv6 addresses are represented by eight sets of four hexadecimal digits, and each set of numbers is separated by a colon.
* An example IPv6 address would look like this:

(2DAB: FFFF:0000:3EAE:01AA:00FF:DD72:2C4A)

* With IPv6 addresses being so long, there are conventions to allow for their abbreviation. First, leading zeros from any one group of numbers may be eliminated. For example, :0033: can be written as :33:
* Any consecutive sections of zeros can be represented by a double colon. This may be done only once in any address.
* The number of sections removed using this abbreviation can be determined as the number required to bring the address back up to eight sections.
* Like in IPv4 certain address blocks are reserved for private networks. These addresses are not routed over the public internet. In IPv6, private addresses are called Unique Local Addresses (ULA). Addresses from the FC00:: /7 block are ignored and not routed by default.
* In both IPv4 and IPv6, remembering the IP address of every device is not possible, except on the smallest of networks. Name resolution provides a way to lookup an IP address from an easier to use name.

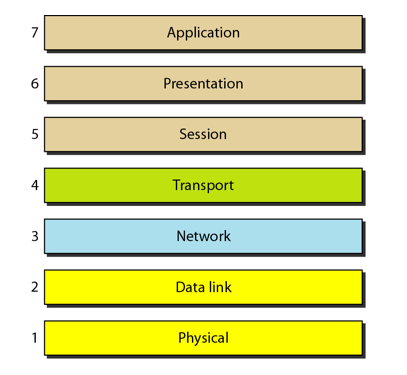
**OSI**

**Open System Interconnection:**

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Introduction:

OSI (Open Systems Interconnection) is used to understand how data is transfer from one device to another. It has 7 layers. It is a reference model for how applications communicate over a network. This model focuses on providing a visual design of how each communications layer is built on top of the other.

****

* Application, Presentation, Session layer are the software layers
* Transport Layer is the heart of the OSI layer
* Network, Datalink, Physical layers are the hardware layers

Layer 7: The Application Layer:  
  
The top layer of an OSI model (layer seven) is the application layer that delivers network services or protocols that comply with an end-user’s data to the end-user. It provides protocols that allow software to send and receive information and present meaningful data to users.  
  
Examples of Layer 7 applications include web browsers such as Google Chrome or Firefox, as well as apps such as Office, Outlook, and Skype. The services provided by each of these applications permit the application layer to supply and receive data from the Presentation layer.  
  
A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).  
  
**Layer 6: Presentation layer:**  
  
Presentation layer get the data from the Application layer. The data is in the form of numbers and characters. Presentation layer convert that characters and numbers to machine understandable binary format

* Example conversion of ASCII to EBCDIC (Extended Binary Coded Decimal Interchange Code)
* This process is known as translation. Before the data is transmitted to the presentation layer reduces the number of bits that are used to represent the original data.
* This bit reduction process is called data compression and it can be Lossy or Lossless.
* To maintain the integrity of data, before transmission data is encrypted at the sender side and data is decrypted at the receiver side.
* Here SSL (Secure Sockets Layer) protocol is used for encrypting and decrypting the data.
* Some of the protocols used in presentation layer are SSH, IMAP, MPEG, JPEG

**Layer 5: Session Layer:**

Session layer helps in setting up and managing connections enabling sending and receiving of data followed by termination of connections or sessions

* Session layer has its helpers called APIs (Application Programming interfaces)
* NETBIOS (Network Basic Input output System) is an example of APIs which allows applications of different computers to communicate with each other. Just before a session or connection is established with the server.
* Server perform a function called authentication. It is a process of verifying who you are.
* For this server uses a username and password. Once the username and password are matched the session or a connection is established between your computer and the server
* After the authentication session layer check for authorization
* This process is determined if you have permission to access a file. If not you will get a message saying you are not authorized to access this page.
* These are the two functions authentication and authorization are performed by the session layer

**Layer 4: Transport Layer:**

Transport layer controls the reliability of communication through Segmentation, Flow control, Error control.

* + Segmentation:
    - In segmentation, the data received from the session layer is divided into small data units called as segments.
    - Each segment contains a source and destination port number and a sequence number.
    - Port number help to direct each segment to the correct application
    - Sequence number helps to reassemble the segments in correct order to form correct message at the receiver.
  + Flow Control:
    - In flow control the transport layer controls the amount of data being transmitted.
    - For example, a mobile is connected to a server, Here server can transmit data maximum at 100Mbps and our mobile can process data maximum at 10Mbps. Now we are downloading the file from the server. Server start sending the file at 50Mbps which is greater than the rate our mobile can process.
    - So the mobile phone tell the transmission layer to slow down the data transmission rate up to 10Mbps so that no data can get lost. Like this wise versa.
* Error Control:
* Transport layer also help in error control, if some data does not arrive the destination. Transport layer uses automatic repeat request scheme to retransmit the lost or corrupted data.
* A group of bits called checksum is added to each segment by the transport layer to find out the received corrupted segment
* Protocols for transport layer:
* Transmission Control protocol (TCP)

1. TCP is the connection oriented transmission
2. It provided feedback that data delivered or not.
3. Lost data can be recovered in TCP

* User Datagram Protocol (UDP)

1. UDP is the connectionless transmission it is faster than the
2. It doesn’t provide any feedback where it delivered data or not
3. Lost data can’t be recovered

**LAYER 3: Network Layer:**

1. Network layer work for the transmission of the received data segment from one computer to the another located in different networks.
2. Data units in network layer are called packets. It is the layer where routers to decide the function of network layer are logical addressing, routing and path determination.
3. IP addressing (IPv4, IPv6) done in network layer is called logical addressing.
4. Every computer in a network has a unique IP addressing
5. IP address is assigned to each data packet to ensure that data can reach the correct destination.
6. Routing is a method of moving the data packets from source to destination and it is based on the logical address format of IPv4 or IPv6.
7. Based on IP address and Mask routing decisions are made in a computer.

* Path Determination

A computer can be connected to internet server for a computer in a number of ways. Choosing the best delivery path for the data delivery from source to destination.

* Protocols used
* OSPF (Open Shortest path first border)
* BGP (Boarder Gateway protocol)
* IS-IS (Intermediate System To Intermediate)

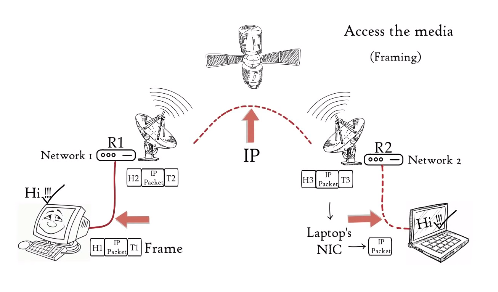
These are the protocols to determine the best path for data delivery.

**Layer 2: Data Link Layer:**

1. Data link layer receives data from the Network layer. data packets contain IP address of sender and receiver
2. There are 2 types of addressing

* Logical addressing: It is done at network layer where the segment is assigned with the sender and receiver IP address to form a data packet.
* Physical addressing: It is done at the data link layer where the data packets are assigned with the MAC address of sender and receiver and form a frame.
* Data unit in Data link layer is called frame

1. Example if we want to transfer the data from computer to the laptop here computer is connected to the router through an ethernet cable and laptop connects with the wireless network.
2. Data link layer add some data as head and tail to an IP packet form it as a frame and passes through the ethernet cable. The router de capsulate as a packet and encapsulate as a frame
3. At the other end router, de capsulate as a packet and encapsulate again as a frame.
4. The laptop receives this wireless data link frame de capsulate it and then forward IP packet to network layer.
5. Finally arrives application layer. Application layer protocol make the received data and visible on the computer screen.
6. Network layer and higher-level layers are able to transfer data over media with the help of Data link layer.
7. That is data link layer provides access to media for higher layer of OSI model

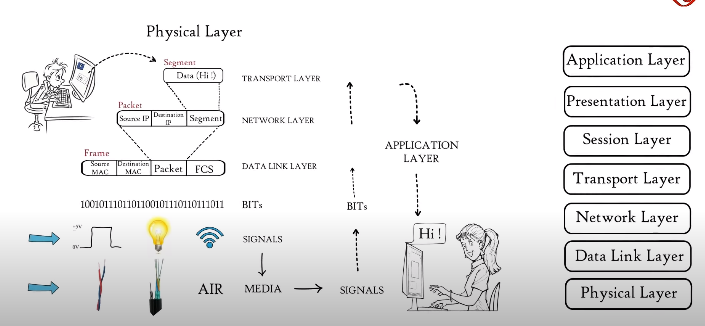
****

**Layer 1: Physical Layer:**

Physical layer converts the binary digits into signal and transmit over the local media.

1. It can be the electric signal in case of copper cable or LAN cable.
2. Light signal in case of optical fiber.
3. Radio signal in case of air

* At the receiver signal convert it to bits and pass it to data link layer as a frame. Frames is further de capsulate as the data move to higher layers finally data is moved to application layer.
* Application layer protocol makes the senders message visible in the application in the receiver’s computers screen.
* In this way, the OSI model is helping to transfer data between distant hosts.

****

#### TCP:

* The most common protocol used in the transport layer is TCP (Transmission Control Protocol). This is a connection oriented protocol. TCP offers reliable, peer-acknowledged, ordered, session-based connectivity between two hosts.
* All the features mentioned above are provided by the TCP layer itself. This means, that it may operate with other, unreliable, protocols in the lower layers and that this shouldn't affect the communication from the application layer perspective.

##### TCP Reliability:

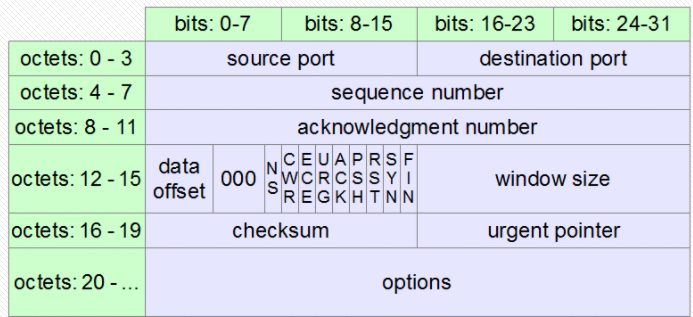
* During sending data, TCP assures that data has been provided to the recipient.
* The receiver checks if the received packet was intact during transmission (by checking the checksum of the data) and, if so, the receiver confirms it by sending an acknowledgement to the sender.
* If the sender doesn't receive the acknowledgement for a message within some period, it will resend the lost packet.
* After several unsuccessful attempts, TCP assumes that the receiver is unreachable and informs the application layer that the transmission has failed.

##### TCP Ordering:

* The TCP header contains a field with the message sequence number. The sequence number is incremented by one for every message sent.
* During receiving data, TCP rearranges incoming packets and put them in the right order. Thanks to that, the application layer doesn't need to care about the ordering of network packets.

##### TCP Header:

* The TCP header consists of 20 or more bytes. The size depends on the fact whether the optional *options* field is used. The maximum size of the *options* field is 40 bytes, thus the maximum size of the whole header is 60 bytes.



**The TCP header structure:**

* Two applications need to establish a session to exchange data. TCP requires three messages to create the session.
* **SYN** - the first application (the client) sends a *synchronize* packet to the host. The message contains a random sequence number, which has been set by the client.
* **SYN-ACK** - the host responds to the client. It increases the sequence number from the client by one and sends it back in the message as an acknowledgement number. Also, the response message contains another sequence number chosen randomly by the host.
* **ACK** - the client sends an acknowledgement message to the host. The message contains both received numbers increased by one.

When the transmission is completed, the session should be terminated. Each side can terminate the session. The second side is supposed to acknowledge that.

**TCP Usage:**

TCP is widely used by protocols and applications that require high reliability. It is not as fast as UDP but, if configured properly, it still provides quite good speed together with high quality of transmitted data.

There are a lot of application layer protocols that are most mostly used together with TCP. Some of the most popular ones are:

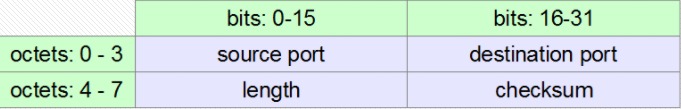
* HTTP, HTTPS
* FTP
* SMTP
* Telnet

#### UDP (User Datagram Protocol):

* The second popular protocol that is used in the transport layer is UDP (User Datagram Protocol or Universal Datagram Protocol), a simpler, connectionless protocol. One program just sends some packages to another, without creating any kind of relation between them.
* Due to its simplicity UDP is faster than TCP. On the other hand, it doesn't provide such reliability as TCP.
* There is no guarantee that the messages would reach the receiver. UDP doesn't deliver packets in the same order that they were sent.
* It is up to the application to check that the received messages are intact and to deal with data in the correct order.

##### UPD Header:

* The UDP header is 8-byte long. It is much shorter and simpler than the corresponding TCP header.



##### UDP Usage:

* UDP is preferred if unimportant data is transmitted or the communication has to be really fast. For example, UDP is used for DNS requests (because of a huge number of clients sending many short messages to relatively few DNS servers). Similarly, during audio and video transmission the loss of some packets is not so damaging to the receiver.
* There are a lot of application layer protocols that use UDP, for example:
* DNS
* DHCP
* TFTP
* SNMP
* RIP
* VOIP