TNE FINALS REVISION

# Ethernet

## Ethernet Encapsulation

1. LLC & MAC Sublayers
   1. LLC (Logical Link Control)
      1. Handles communication between upper and lower layers (802.2)
   2. MAC
      1. Part of the lower sublayer of the data link layer
      2. Implemented typically in the computers NIC (hardware)
      3. Responsibilities
         * Data encapsulation
         * Media access control

A computer screen shot of a computer

Description automatically generated

1. MAC Sublayer
   1. Responsible for data encapsulation and accessing the media.
   2. Data encapsulation includes:
      1. Ethernet frame
         * The internal structure of the ethernet frame.
      2. Ethernet Addressing
         * Includes both source and destination MAC address where ethernet frame is delivered from Ethernet NIC to Ethernet NIC in the same LAN.
      3. Ethernet Error detection
         * The ethernet frame itself includes FCS (Frame Check Sequence) trailer which is used for error detection.
   3. **[Media Access Control method]** CSMA/CD (Carrier Sense Multiple Access with Collision Detection) *Example is used as explanation.*
      1. PC 1 sends a frame.

A computer network diagram with a computer and a computer

Description automatically generated with medium confidence

* + 1. Hub receives the Frame.
    2. Hub sends the frame.

A diagram of a computer

Description automatically generated

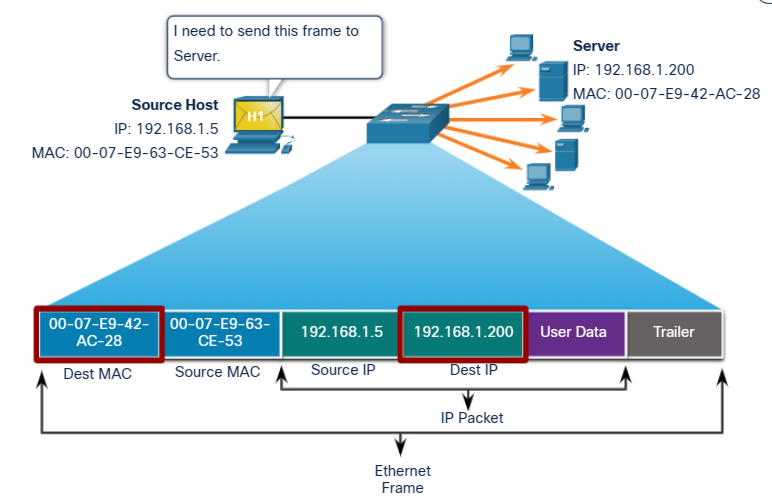
* + 1. If the frame is the expected one’s then PC will copy the entire frame otherwise the frame will be ignored.
    2. Examples of networks that uses this:
       - Wireless LAN
       - Legacy Bus-topology ethernet LAN
       - Legacy Ethernet LAN using a hub.
    3. These network **operates in half duplex mode** to avoid collision.
       - So, if PC1 is sending data, PC2 must be in a state where it can receive data.
    4. If two devices transmit frame at the same time, then collision will happen. This causes the frames sent to be corrupted and will need to be resent.
  1. **[Media Access Control method]** CSMA/CA (Collision Sense Multiple Access with Collision Avoidance)
     1. Uses same method as CSMA/CD but this is for wireless networks.
     2. Hard to detect collision in wireless networks so this CSMA/CA waits before transmitting its frames.
     3. Each device that’s transmitting data includes its time duration where this time duration information will be sent to other devices to know how long the medium is unavailable.

## Ethernet Frame

1. Ethernet Frame Fields
2. Min ethernet frame size = 64 bytes, Expected Maximum = 1518 bytes
3. This includes all the bytes from destination MAC address through FCS field.
4. Preamble is not included when describing the size of frame.
5. Frame < 64 bytes is considered as a **collision fragment** or **runt frame**. This will be automatically discarded by the receiving stations.
6. Frame > 1500 are considered as **Jumbo** or **baby giant frames.**
7. A diagram of a computer

   Description automatically generated
8. Details
   * + - **Preamble (7) & Start Frame Delimiter (1) fields**: used for synchronization between sending and receiving devices.
       - **Destination MAC Address field (6):** assist devices in determining whether the frame is addressed to them.
       - **Source MAC address (6) field**: Identifies the original NIC or interface of the frame.
       - **Type/Length (2):** identifies the upper layer protocol that is encapsulated in the Ethernet Frame.
       - **Data (46-1500) field**: contains encapsulated data from a higher layer (Layer 3 PDU or IPv4 packet).
       - **FCS (4) field**: To detect errors in frames. Uses CRC (Cyclic Redundancy Check)
         * CRC

Sending device include results of CRC in the FCS frame. The receiving device receives the frame and generates a CRC to compare and look for errors. If calculations matched = no error otherwise frame is dropped.

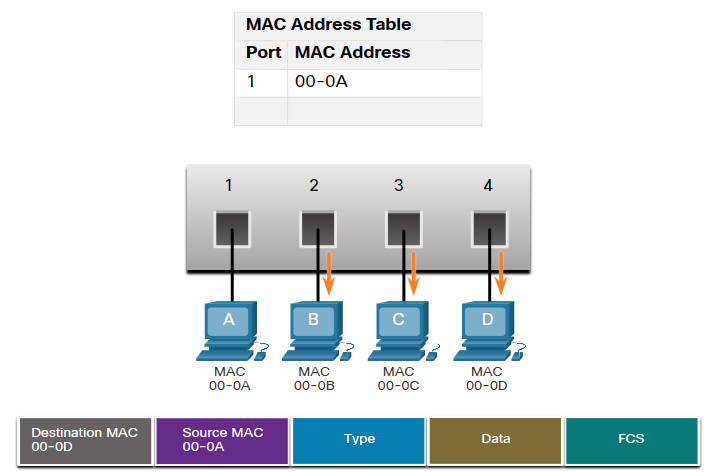
1. Why is there a range for size of frame:
   * + - Minimum is 64
         * So that any frame size below 64 can be detected by the devices and classify it as collision fragment or runt frame.
       - Maximum (above 1518)
         * The higher the frame size, higher the efficiency but higher frame size could also lead to errors prone frame. Errors are more likely to occur in higher frame size.
         * Larger frames also increases the latency. (Time take for frame transmission)
         * Higher frame, higher chances of collision.
2. Unicast MAC Address
3. Frames are sent from a single transmitting device to a single destination device.
4. 
5. A diagram of a server

   Description automatically generated
6. Based on the above diagram, H3 (Host: 192.168.1.5 [source]) request for a web page from the server (192.168.1.200 [destination]).
7. For a unicast packet to be sent/received, destination IP and Source IP should be in the IP Packet Header.
8. The IP & MAC address combine to deliver the data to one specific destination host.
9. The source host goes through a process called ARP (Address Resolution Protocol) to determine the MAC address associated with IPv4. Process for determining MAC address associated with IPv6 is called Neighbor Discovery (ND).
10. Source MAC address should always be a unicast.
11. Overview/Summary for Unicast MAC address and its process.
12. The PC request Web Page from the server.
13. First, **data is encapsulated into an ethernet frame**. The encapsulation process includes the addition of header and trailer. This Ethernet frame contains the destination and source MAC address, type of data being sent and error checking results.
14. Next, before sending the ethernet frame, the device **checks for the destination MAC address**. This is to ensure that the frame reaches the correct destination. To do so the frame **uses ARP to determine which device matches the specified MAC address**. Since the servers MAC matches then it’ll be chosen.
15. Once the device has the destination MAC address, the frame will be transmitted to the destination device.
16. Upon reaching the destination device, the **destination device will check whether its MAC address matches the frames MAC address**. If yes, then the destination device will take in the frame and process the data. Otherwise, the frame will be ignored.

## Collision

1. Occurs when two or more devices are trying to send data at the same time on the same segment.
2. Collision causes:
   1. Data Loss
   2. Network Congestion
3. Collision is prevented by using:
   1. CSMA/CD
   2. CSMA/CA

## Frame forwarding Methods on Cisco Switches

1. If the destination MAC address is Unicast, the switch will look for a match between MAC address in Frame and in MAC address table. If matches, then it forwards the frame to the specified port. Or else It will be forwarded to all other ports.
2. 
3. Based on the above diagram, the destination MAC is 00-0D but 00-0D is nowhere to be found in the MAC address table. So the switch forwards the frame to all other ports except 00-0A.

## IPv4

1. Characteristics of IPv4
   1. Connectionless
   2. Best effort delivery
   3. Media independence
2. Network & Host portion
   1. Using example for class C:

192.168.10.3

Network Portion

Host Portion

1. Subnet Mask
   1. Used to identify the network/host portion of the IPv4 address.
2. Default Gateway
   1. Required to reach remote networks.
3. DNS server IPv4 address
   1. Required to translate domain name to IPv4 addresses.
4. “ANDing” method to determine IPv4 address.
   1. A diagram of numbers and a person pointing at the numbers

      Description automatically generated with medium confidence
5. Network Address (First address in range), Broadcast Address (Last address in range), First Usable host (After Broadcast Address), Last Usable host (Before Broadcast Address).
6. Unicast
   1. One device sending a message to another device in a one-to-one communication.
7. Broadcast
   1. A device sending message to all the devices on a network in a one-to-all communication.
8. Multicast
   1. It allows a host to send a single packet to a selected set of hosts that is subscribed to a multicast group.
   2. Not subscribed hosts will just ignore these packets.
9. Private address block
   1. Not unique and can be used internally within any network.
   2. A screenshot of a computer

      Description automatically generated
   3. For these types of networks, if they want to connect to the internet, their private IP should be changed to a public address. To do so, NAT (Network Address Translation) helps to convert/translate this private IP address to a public IP address which then the device can access the IP address.
10. Special use IPv4 address
    1. Network & Broadcast addresses
       1. Cannot use as an IP for assignment.
    2. Loopback address
       1. **127.0.0.0 to 127.255.255.255**
    3. Link-Local address
       1. **169.254.0.0 to 169.254.255.255**
    4. TEST-NET addresses
       1. **192.0.2.0 to 192.0.2.255**
    5. Experimental addresses
       1. **240.0.0.0 to 255.255.255.254**
11. IPv4 Packet header
    1. IPv4 protocol is used by the TCP/IP protocols at network layer.
    2. Used to ensure that the packet is delivered to the next stop on the way to its destination device.
    3. Data = whatever data is going to be sent.
    4. Header = where data is sent, where data is from
    5. A screen shot of a computer

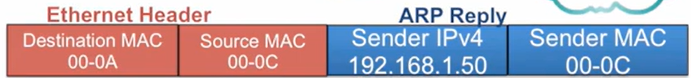
       Description automatically generated
    6. **Version**: Identifies this as an IPv4 Packet.
    7. **IHL (Internet Header Length):** The entire length of the IP header.
    8. **DS:** Determine the priority of each packet. Contains DSCP & ECN
    9. **DSCP (Differentiated Services Code Point)**: Type of service provided by the IPv4.
    10. **ECN (Explicit Congestion Notification)**: Carries info about congestion seen in the route.
    11. **Total Length**: Length of entire IP packet. (Header + Data)
    12. **Identification**: Used in fragmentation.
    13. **Flags**: If packet is too large to handle, these ‘flags’ tell if they can be fragmented or not. In this 3-bit flag, the MSB is set to 0.
    14. **Fragment Offset**: Tells the exact position of the fragment in the original IP packet.
    15. **Time-To-Live**: To limit the lifetime of a packet.
    16. **Protocol**: Tells the net layer at its destination host to which protocol this packet belongs to. This also identifies the next level protocols.
    17. **Header Checksum**: Used to detect corruption in the IPv4 header.
    18. **Source address**: represents the source IPv4 address off the packet. (Always the Unicast address)
    19. **Destination address**: Represents the destination IPv4 packet address. (can be Unicast, Multicast or Broadcast)

## ARP (Address Resolution Protocol)

1. ARP is used in a device **to determine the destination MAC address of a local device when it knows its IPv4 address.**
2. Basic functions:
   1. Resolving IPv4 addresses to MAC addresses.
   2. Maintaining a table of IPv4 to MAC address mapping.
3. ARP table
   1. Stored temporarily in the RAM.
   2. This table will be used by the sending device where the device will search for the IPv4 address with its corresponding MAC address.
      1. If Destination IP is on same network with the source IP, then the device will look for the destination IP in the ARP table.
      2. If Destination IP is on a different network, then the device will look for the destination Ips default gateway in the ARP table.
   3. ARP request
      1. A device first checks its ARP cache whether the IPv4 address with corresponding MAC address is there or not. If no then, the device requests for a ARP request.
      2. So, the Ethernet Frame that wanted to be sent will be kept on hold and ARP request is created.
      3. A blue and red rectangle with white text

         Description automatically generated
      4. The ARP request contains the **target IPv4, target MAC, Source MAC** and **Destination MAC.** The destination MAC of the ARP will be a broadcast address. Then this request will be sent to the switch, which then the switch will flood it out to all other ports.
      5. Next, every device will compare their IP with the IP in the ARP request. If the IP doesn’t match, then the device won’t send out an **ARP reply**.
      6. If matches, then the device will send out an ARP reply which contains the target MAC address.
      7. A computer screen shot of a computer

         Description automatically generated
   4. ARP Reply
      1. This is how the ARP replies looks:



* + 1. In this case PC C is sending the ARP reply so it sends the ARP reply containing its MAC address.
    2. PC A receives the ARP reply and stores the information in its ARP cache.

A computer diagram with a computer network

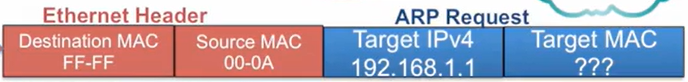
Description automatically generated with medium confidence

* + 1. PC A will now go back to the initial frame and fills in the Destination MAC by using the info in the ARP cache.
    2. Finally, it can now send the frame to the destinated PC which is PC C in this case.
  1. ARP in remote communications

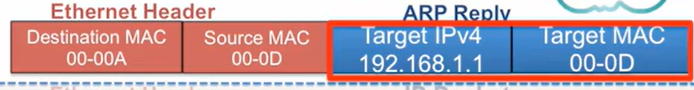
A computer diagram with a computer network

Description automatically generated with medium confidence

* + 1. Every process is the same. Since the destination IP is a remote address, during ARP request instead of using remote address as the destination IP, it uses the sending devices default gateway. So, the ARP request would look like this:



* + 1. This is how the ARP reply looks like:



* + 1. All other processes are the same.

## Inter-VLAN routing

1. Why is routing needed?
   1. Responsible for the routing of the traffic between networks.
2. Default Gateway
   1. Identifies the router a packet is sent to when the destination is not on the same local network subnet.
3. Inter-VLAN routing
   1. Process of forwarding the network traffic from one VLAN to another VLAN.
4. Router-On-A-Stick Inter-VLAN Routing
   1. This method overcomes the limitations of Legacy Inter-VLAN routing.
   2. This method does not scale beyond 50 VLANS.
      1. Can cause network congestion.
5. Legacy Inter-VLAN (Each VLAN needs a port)

A diagram of a network

Description automatically generated

1. Inter-VLAN routing

A diagram of a blue object with white text

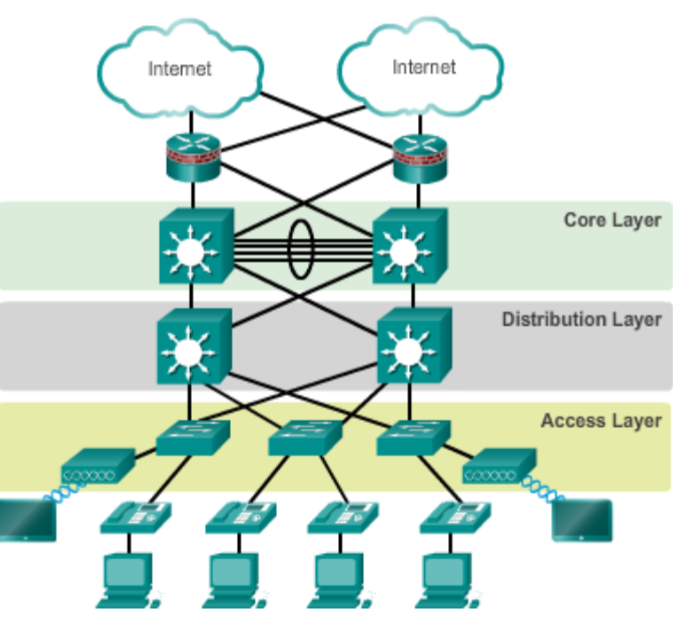
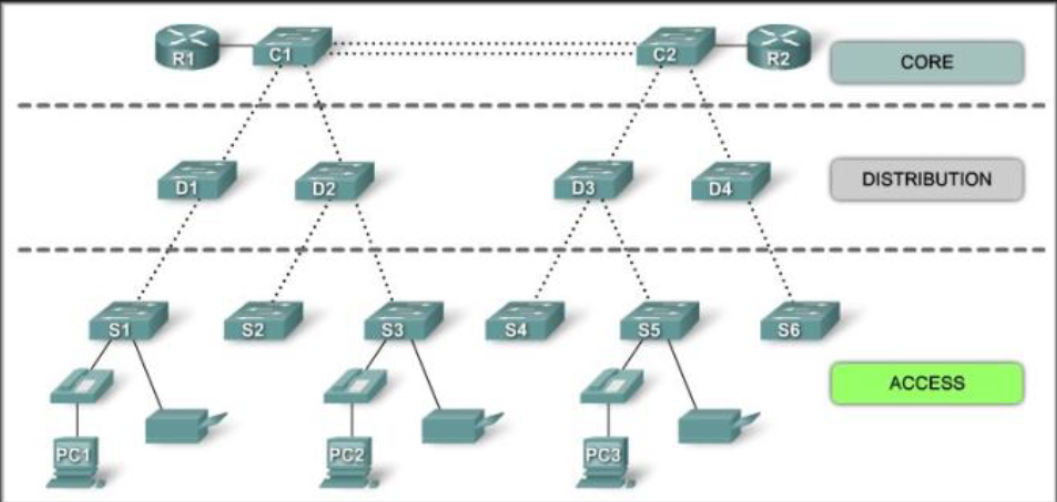
Description automatically generated

1. Router-on-a-stick Inter-VLAN routing

A diagram of a computer network

Description automatically generated

## LAN Design

1. Hierarchical design model layers:
   1. Access
   2. Distribution
   3. Core
2. 
3. Access Layer
   1. Includes switches and wireless access points.
   2. Main purpose:
      1. Allow devices to connect to a network.
      2. Controls which devices are allowed (e.g., Port Security) to access the network.
   3. Can be expanded through wireless connectivity.
4. Distribution Layer
   1. Collects the data received from the access layer switches before it is transmitted to the core layer for its routing to the destination.
   2. Controls the flow of the network traffic.
   3. VLAN
      1. Allows us to segment the traffic on the switch into several subnetworks.
   4. Distribution layer switches
      1. High performance
      2. Have high availability and redundancy to ensure reliability.
5. Core Layer
   1. It is a high-speed backbone of the internetwork.
   2. Very important for interconnection between the distribution layer devices so core must be
      1. Highly redundant
      2. Highly available
   3. Can also connect to Internet resources.
   4. In smaller networks
      1. Core and distribution layer are combined (Collapsed network)
6. Logical Layout
   1. Layers are separated into a well-defined hierarchy.
   2. Easy to see which switch performs which function.
   3. No Intra-Layer connection
      1. The devices within the same layer do not directly communicate.
      2. They connect to the device in another layer.
   4. 
7. Physical Layout
   1. Try to maintain visibility into network design.
   2. Often access layer and distribution switches are installed in wiring closet of each floor.
      1. This connects to the devices that need to access the network.
8. Design Principles
   1. Network diameter
      1. Number of devices a packet must go through in order to reach its destination.
      2. ⬆️ Diameter, ⬆️ Latency.
   2. Bandwidth aggregation
      1. Combining several parallel link into one logical link
      2. **EtherChannel.**
   3. Redundancy
      1. Doubling the network connection between devices.
      2. Double the device.
      3. But Expensive to implement redundant network.

## STP (Spanning Tree Protocol)

1. STP ensures that there’s is only one logical path between all destinations on the network by intentionally blocking redundant paths that could lead to a loop.
2. Port is considered blocked when:
   1. The user data can’t leave or enter the path.
   2. This does not include BPDU (Bridge Protocol Data Unit) frames that are used by STP to prevent loops.
   3. Physical paths still exist to provide redundancy, but it’ll be blocked to prevent loop.
3. STP uses STA (Spanning Tree Algorithm) to determine which port to block.
   1. The algorithm elects one switch as the Root Bridge and uses it as a reference point to do STP calculations.
4. Electing the root bridge
   1. A BID (Bridge ID) is used to identify each bridge/switch. This is used in determining the root bridge.
   2. Components:
      1. 2-byte Bridge Priority
         * 32768 default.
      2. 6-byte MAC address
   3. Lowest Bridge ID is the root.
      1. If same priority, then lowest MAC address will be chosen.
5. Electing the root-port
   1. Every non-root switch elects a root port.
   2. The root port is the port closest to the root bridge in terms of the overall cost to the root bridge.
   3. Cost table

A white sheet with numbers and black text

Description automatically generated

1. Designated Port
   1. Has the lowest internal root path cost to the root bridge.
   2. Designated ports:
      1. On a root bridge

A diagram of a computer network

Description automatically generated

* + 1. When there is a root port

A diagram of a computer network

Description automatically generated

* + 1. When there’s is not root port

A diagram of a computer network

Description automatically generated

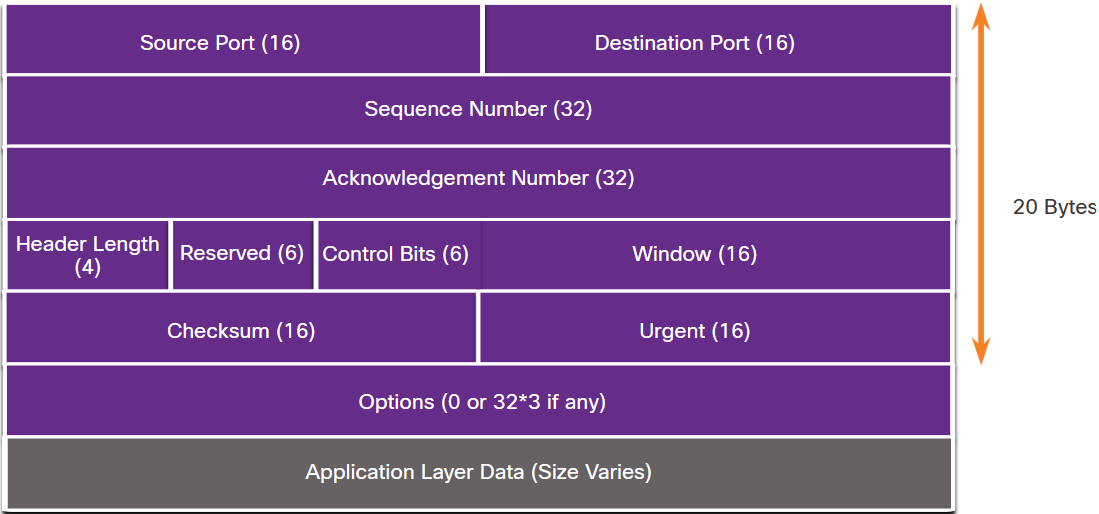
* + 1. Ports that are not a root port or a designated port, will be elected as the alternate or a blocked port.

## Link Aggregation

1. Allows redundant links between devices that will not be blocked by STP.
2. EtherChannel uses link aggregation technology.
3. EtherChannel
   1. Grouping of several Fa/Gi ports into one logical channel.
   2. Port Channel = name given to the configured EtherChannel group.
   3. Advantage of EtherChannel
      1. There’s no need for upgrades since it relies on the existing switchports.
      2. Aggregation is seen as one logical link by STP.
         * Can avoid the block that STP will establish.
      3. If a link goes down, there’s no need for recalculation.
      4. Easy configuration & management.

## Transport Layer

1. TCP (Transmission Control Protocol)
   1. Helps in the exchange of messages between different devices over a network.
   2. Features:
      1. Establishes a session.
      2. Ensures reliable delivery.
         * During transmission, the frame can be lost/corrupted, TCP ensures that each segment sent by the source reaches the destination.
      3. Provide same order delivery.
         * TCP ensures that the segments are reassembled into proper order.
      4. Support flow control.
   3. TCP header



* + 1. **Source Port**: Identifies the source application by port number.
    2. **Destination Port**: Identifies the destination application by port number.
    3. **Sequence Number**: Used for data reassembly purposes.
    4. **Acknowledgement Number**: Indicates the data has been received and the next byte expected from the source.
    5. **Header Length**: Indicates the length of the TCP fragment header.
    6. **Reserved**: Reserved for future use.
    7. **Control bits**: Indicates the purpose and the function of the TCP segment.
    8. **Window size**: Number of bytes that can be accepted at one time.
    9. **Checksum**: For error checking of the TCP header and data.
    10. **Urgent**: Indicates if the contained data is urgent.
  1. Applications of TCP
     1. SSH
     2. FTP
     3. SMTP
     4. HTTP

1. UDP (User Datagram Protocol)
   1. It’s a best effort transport protocol.
   2. Used to send short messages to other host on an IP network.
   3. Features:
      1. Data is reconstructed in the order that it is received.
      2. No session is established.
      3. Any segments that are lost are not resent.
      4. The sending is not informed about the resource availability.
   4. UDP header

A purple box with white text

Description automatically generated

* + 1. **Source Port:** Identify the source application by port number.
    2. **Destination Port:** Identify the destination application by port number.
    3. **Length:** The length of the UDP datagram header.
    4. **Checksum:** Used for error checking in the datagram header and data.
  1. Applications:
     1. Video Conferencing
     2. DHCP
     3. DNS
     4. SNMP

1. Port Number
   1. Both TCP & UDP uses port number.
      1. To manage multiple/simultaneous conversations.
   2. Socket pairs
      1. Combination of source IP and source port number.
   3. Port Number groups
      1. Well-Known ports
         * 0 – 1023
      2. Registered port
         * 1024 – 49151
      3. Private and/or dynamic port
         * 49152 – 65535

A screenshot of a computer

Description automatically generated

* 1. **Netstat** command
     1. Used to display the list of protocols, local address with port number, foreign address and port number, and connection state.

## IPv6

1. 2001:0db8:0000:0000:a111:b222:c333:abcd
2. It’s called HEXTET(Hexadecimal).
3. Each hexadecimal character represents 4 binary numbers.
4. 2001:0db8:0000:0000:a111:b222:c333:abcd /64

Network Portion Host Portion

1. Compressing
   1. 2001:0db8:0000:0000:a111:b222:c333:abcd
      1. Remove continuous zero (Only once can add double colon)

2001:0db8:0000:0000:a111:b222:c333:abcd

Result:

2001:0db8::a111:b222:0000:abcd

* + 1. Take all the leading zero from leading hextet

2001:0db8::a111:b222:0000:abcd

Result:

2001:db8::a111:b222:0:abcd