Cisco

1. Explore the network

1.1 Globally Connected

- Networks affect the way we interact, learn, work, play.
- Host devices
  - Clients
  - Servers
  - Both

1.1.2 Networks of Many Sizes

- Small home network
- Small Office / Home Office Networks
- Medium to Large Networks
- World Wide Networks

1.1.3 Peer-to-Peer

- + Easy to set up
- + Less complexity
- + Lower cost
- + For simple tasks
- - No centralized administration
- - Not as secure
- - Not scalable
- - Slow performance

Joris Jamers
1TINa 2015-2016

2. LANs, WANs, and the Internet

2.1 Network Components

- Devices
  - End Devices
    - Desktop Computer
    - Laptop
    - Printer
    - IP Phone
    - Wireless Tablet
    - Telepresence Endpoint
  - Intermediary Network Devices
    - Wireless Router
    - LAN Switch
    - Router
    - Multilayer Switch
    - Firewall Appliance
- Media
  - Cables
    - Copper
    - Fiber Optic
  - Wireless
- Services

Important terms to remember :

- **Network Interface Card** : NIC provides the physical connection to the network at the PC or other end device
- **Physical Port** : Connector or outlet on a networking device where the media is connected to an end device or another networking device.
- **Interface** : Specialized ports on a networking device that connect to individual networks. Routers are used to interconnect networks, the ports on a router are referred to as **network interfaces**.

2.2 Local Area Network (LAN)

- A network infrastructure that provides access to users and end devices in a small geographical area, which is typically an enterprise, home, or small business network owned by an individual or IT department.
  - High speed bandwidth to internal end devices and intermediary devices.

2.3 Wide Area Network (WAN)

- A network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a telecommunications service provider.
  - WANs typically provide slower speed links between LANs.

2.4 Intranets and Extranets

2.4.1 Intranet

- Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization.

2.4.2 Extranet

- An organization may use an extranet to provide secure and safe access to individuals who work for a different organization, but require access to the organization's data. Examples of extranets include :
  - A company that is providing access to outside suppliers and contractors.
  - A hospital that is providing a booking system to doctors so they can make appointments for their patients.
  - A local office of education that is providing budget and personnel information to the schools in its districts.

2.5 Basic Device Configuration

Commando's :

- Changing switch hostname:
- `Switch(config)# hostname SW1`
- Configuring passwords:
- `SW1(config)# enable secret cisco`
- `SW1(config)# enable password cisco`
- Securing console port:
- `SW1(config)# line con 0`
- `SW1(config-line)# password cisco`
- `SW1(config-line)# login`
- Securing terminal lines:
- `SW1(config)# line vty 0 4`
- `SW1(config-line)# password cisco`
- `SW1(config-line)# login`
- Configuring banners:
- `SW1(config)# banner motd $`
- Giving the switch an IP address:
- `SW1(config)# interface vlan 1`
- `SW1(config-if)# ip address 172.16.1.11 255.255.255.0`
- `SW1(config-if)# no shutdown`
- Saving configuration:
- `SW1# copy running-config startup-config`

3. Network Protocols

3.1 TCP/IP Model

- **Application** Layer :
  - **Name System**
    - **DNS** (Domain Name System (or service))
      - Translates domain names, such as cisco.com, into IP addresses
  - **Host Config**
    - **BOOTP** (Bootstrap Protocol)
      - Enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine
    - **DHCP** (Dynamic Host Configuration Protocol)
      - Dynamically assigns IP addresses to client stations at start-up
      - Allows the addresses to be re-used when no longer needed
  - **Email**
    - **SMTP** (Simple Mail Transfer Protocol)
      - Enables clients to send email to a mail server
      - Enables servers to send email to other servers
    - **POP** (Post Office Protocol version 3 (POP3))
      - Enables clients to retrieve email from a mail server
      - Downloads email from the mail server to the desktop
    - **IMAP** (Internet Message Access Protocol)
      - Enables clients to access email stored on a mail server
      - Maintains email on the server
  - **File Transfer**
    - **FTP** (File Transfer Protocol)
      - Sets rules that enable a user on one host to access and transfer files to and from another host over a network
      - A reliable, connection-oriented, and acknowledged file delivery protocol
    - **TFTP** (Trivial File Transfer Protocol)
      - A simple, connectionless file transfer protocol
      - A best-effort, unacknowledged file delivery protocol
      - Utilizes less overhead than FTP
  - **Web**
    - **HTTP** (Hypertext Transfer Protocol)
      - Set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web

- **Transport** Layer
    - **UDP** (User Datagram Protocol)
        - Enables a process running on one host to send packets to a process running on another host
        - Does not confirm successful datagram transmission
    - **TCP** (Transmission Control Protocol)
        - Enables reliable communication between processes running on separate hosts
        - Reliable, acknowledged transmissions that confirm successful delivery
- **Internet** Layer
    - **IP** (Internet protocol)
        - Receives message segments from the transport layer
        - Packages messages into packets
        - Addresses packets for end-to-end delivery over an internetwork
    - **NAT** (Network Address Translation
        - Translates IP addresses from a private network into globally unique public IP addresses
  - **IP Support**
    - **ICMP** (Internet Control Message Protocol
        - Provides feedback from a destination host to a source host about errors in packet delivery
  - **Routing** Protocols
    - **OSPF** (Open Shortest Path First)
        - Link-state routing protocol
        - Hierarchical design based on areas
        - open standard interior routing protocol
    - **EIGRP** (Enhanced Interior Gateway Routing Protocol
        - Cisco proprietary routing protocol
        - Uses composite metric based on bandwidth, delay, load and reliability
- **Network Access** Layer
    - **ARP** (Address Resolution Protocol
        - Provides dynamic address mapping between an IP address and a hardware address
    - **PPP** (Point-to-Point Protocol)
        - Provides a means of encapsulating packets for transmission over a serial link
    - **Ethernet**
        - Defines the rules for wiring and signaling standards of the network access layer
    - **Interface Drivers**
        - Provides instruction to a machine for the control of a specific interface on a network device

The TCP/IP protocol suite is implemented as a TCP/IP stack on both the sending and receiving hosts to provide end-to-end delivery of applications over a network. The Ethernet protocols are used to transmit the IP packet over the physical medium used by the LAN.

3.2 Data Encapsulation

Encapsulation works from the top to bottom. At each layer, the upper layer information is considered data within the encapsulation protocol.

User Data → TCP Segment → IP packet → Ethernet Frame

3.3 De-encapsulation

De-encapsulation is reversed at the receiving host, and is known as the de-encapsulation. This is used by the receiving device to remove on or more protocol headers

Ethernet Frame → IP packet → TCP Segment → User Data

3.4 PDU (Protocol Data Units)

- Data (Application Layer) → clear text, encrypted or compressed
- Segments (Transport Layer) → segment for TCP
- Packets (Network layer) → the packet
- Frames (Data Link Layer) → the frame
- Bits (Physical layer) → is the bit or or “stream”

3.5 OSI Model

- 7. **A**pplication
  - The application layer contains protocols used for process-to-process communications
- 6. **P**resentation
  - The presentation layer provides for common representation of the data transferred between application layer services
- 5. **S**ession
  - The session layer provides services to the presentation layer to organize its dialogue and to manage data exchange
- 4. **T**ransport
  - The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end device
- 3. **N**etwork
  - The network layer provides services to echange the individual pieces of data over the network between identified end devices
- 2. **D**ata Link
  - The data link layer protocols describe methods for echanging data frames between devices over a common media

- 1. **P**hysical
  - The physical layer protocol describes the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical connections for bit transmission to and from a network device

All **P**eople **S**eem **T**o **N**eed **D**irty **P**orn

3.6 Data Access

The network and data link layers are responsible for delivering the data from the source device to the destination device. Protocols at both layers contain a source and destination address, but their addresses have different purposes.

3.6.1 Network layer

Responsible for delivering the IP packet from the original source to the final destination, either on the same network or to a remote network

The network layer addresses, or IP addresses, indicate the original source and final destination. An IP address contains two parts:

- **Network** portion → the left-most part of the address that indicates which network the IP address is a member. All devices on the same network will have the same network portion of the address.
- **Host** portion → the remaining part of the address that identifies a specific device on the network. The host portion is unique for each device on the network.

3.6.2 Data link layer

Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network

When the sender and receiver of the IP packet are on the same network, the data link frame is sent directly to the receiving device. On a Ethernet network, the data link addresses are known as Ethernet (Media Access Control) addresses. MAC addresses are physically embedded on the Ethernet NIC

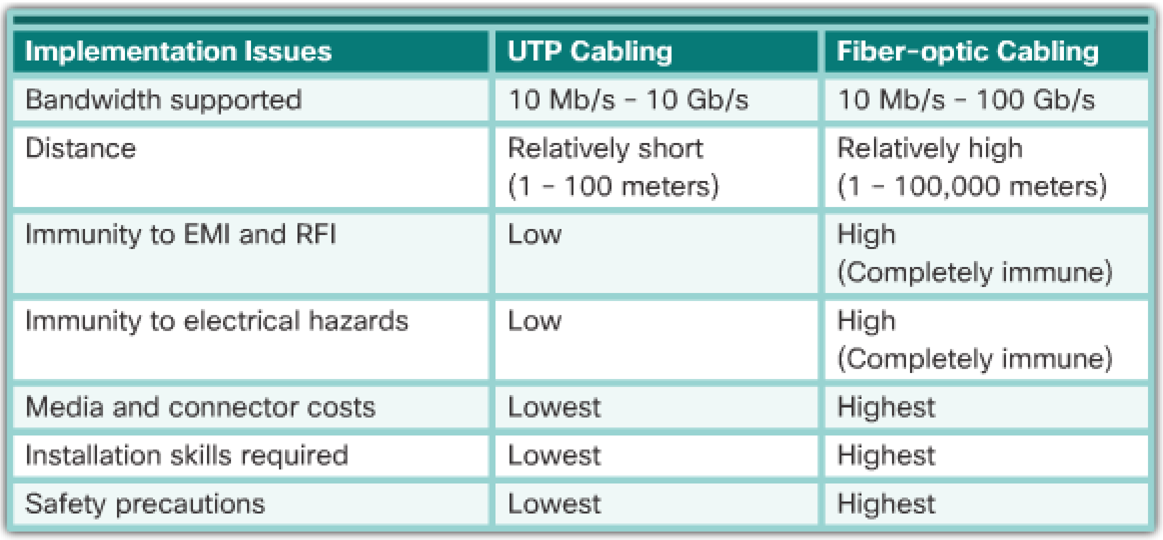
- Source MAC address → This is the data link address, or the Ethernet mac address, of the device that sends the data link frame with the encapsulated IP packet. The MAC address of the Ethernet NIC

4. Network Access

4.1 Network Media

- **Copper Cabling**
    - Inexpensive
    - Easy to install
    - Low resistance to electrical current
    - Limited by distance and signal interference
        - **Unshielded Twisted-Pair** (UTP)
            - Most common networking media
            - Used for interconnecting network hosts with intermediate networking devices, such as switches and routers
            - Twisting the wires helps protect against signal interference from other wires
                - Ethernet **Straight-through** : Most common type of networking cable. It is commonly used to interconnect a host to a switch and a switch to a router
                - Ethernet **Crossover** : A cable used to interconnect similar devices. For example to connect a switch to a switch, a host to a host, or a router to a router
                - **Rollover** : A cisco proprietary cable used to connect a workstation to a router or switch console port
        - **Shielded Twisted-Pair** (STP)
            - Better noise protection than UTP cabling
            - STP is more expensive
            - Harder to install
        - **Coaxial**
            - Used to transmit electronical signals
            - This cable is replaced with UTP
- **Fiber-Optic Cabling**
    - Longer distances
    - Higher bandwith
    - Immune to EMI and RFI (Radio Frequency Interference)
    - Commonly used to interconnect network devices
    - Flexible but thin → Light pipe
    - Used in **4 types of industry** :
        - **Enterprise** networks : backbone cabling applications and interconnecting infrastructure devices
        - **Fiber-to-the-Home** (FTTH) : used to provide always-on broadband services to home and small businesses
        - **Long-Haul networks** : Used by service providers to connect countries and cities
        - **Submarine networks** : Used to provide reliable high-speed, high-capacity solutions cable of surviving in harsh undersea environments up to transoceanic distances.

- **Fiber** VS **Copper**
  - Fiber optic are not electrical conductors, so immune to electromagnetic interference



Implementation Issues	UTP Cabling	Fiber-optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively high (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

- **Wireless Media**
  - Wireless media carry electromagnetic signals, that represent the binary digits of data communication using radio or microwave frequencies.
  - Greatest mobility of all media
  - Wireless is quickly gaining in popularity in enterprise networks
  - Areas of **concern** :
    - **Coverage area** : wireless data communication works well in open environments. However, certain construction materials used in buildings and structures, local terrain will limit the effective coverage
    - **Interference** : Wireless is susceptible to interference and can be disrupted by common devices → wireless phones,…
    - **Security** : Requires no access to a physical strand of media. Therefor devices and users, not authorized for access to the network can gain access to the transmission. Network security is a major component of wireless network administration
    - **Shared media** : WLANs operate in half-duplex which means only one device can send or receive at a time. The wireless medium is shared amongst all wireless users. More users → Less bandwidth

4.2 Data link layer

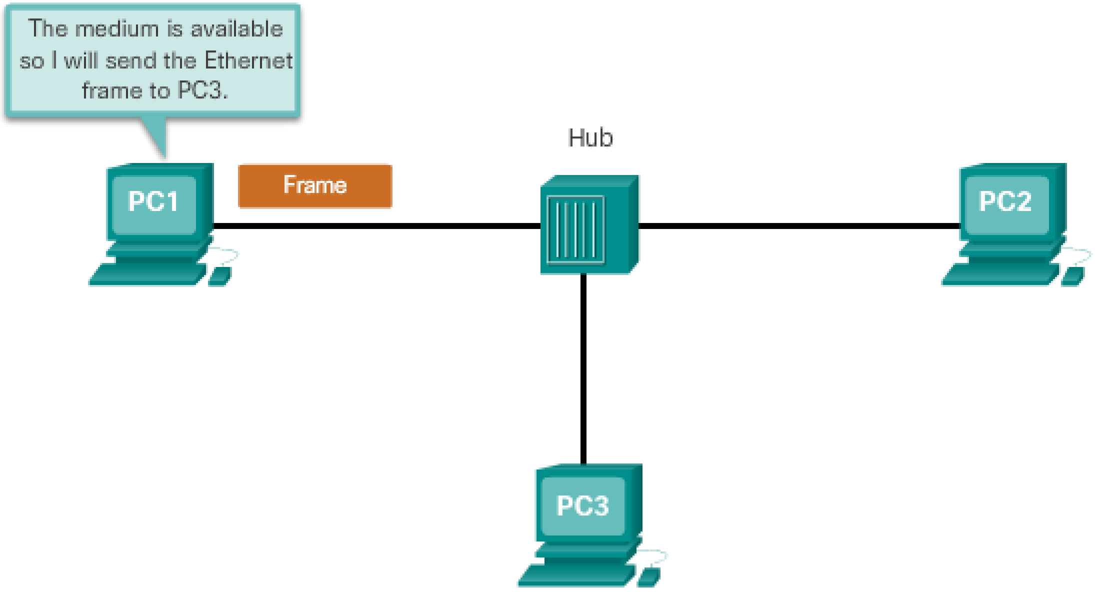
Data link layer of the OSI model (layer 2) is responsible for :

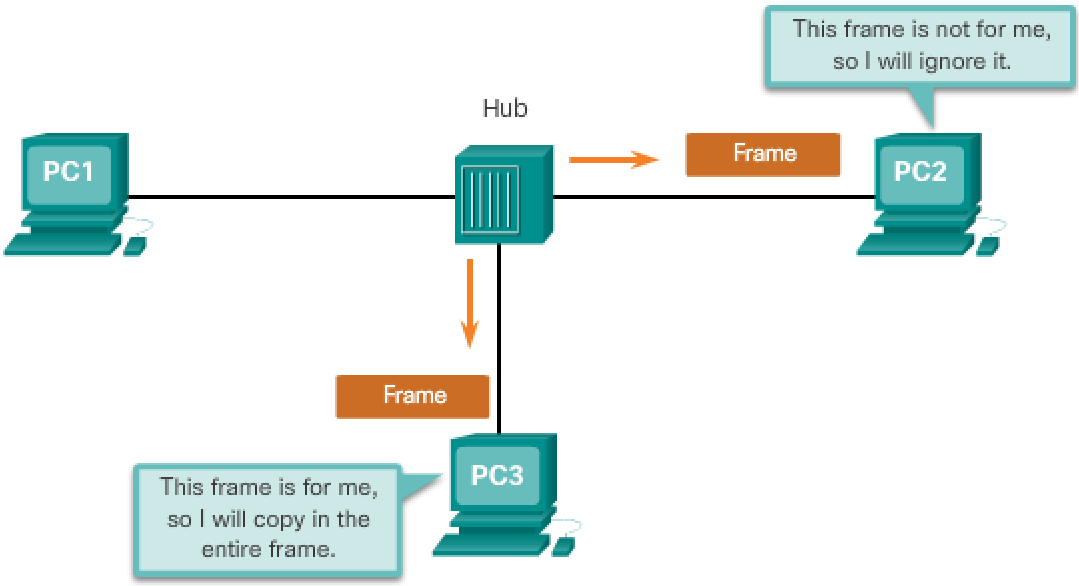
- Allowing the upper layers to access the media
- Accepting layer 3 packets and packaging them into frames
- Preparing network data for the physical network
- Controlling how data is placed and received on the media
- Exchanging frames between nodes over a physical network media, such as UTP or fiber-optic
- Receiving and directing packets to an upper layer protocol
- Performing error detection

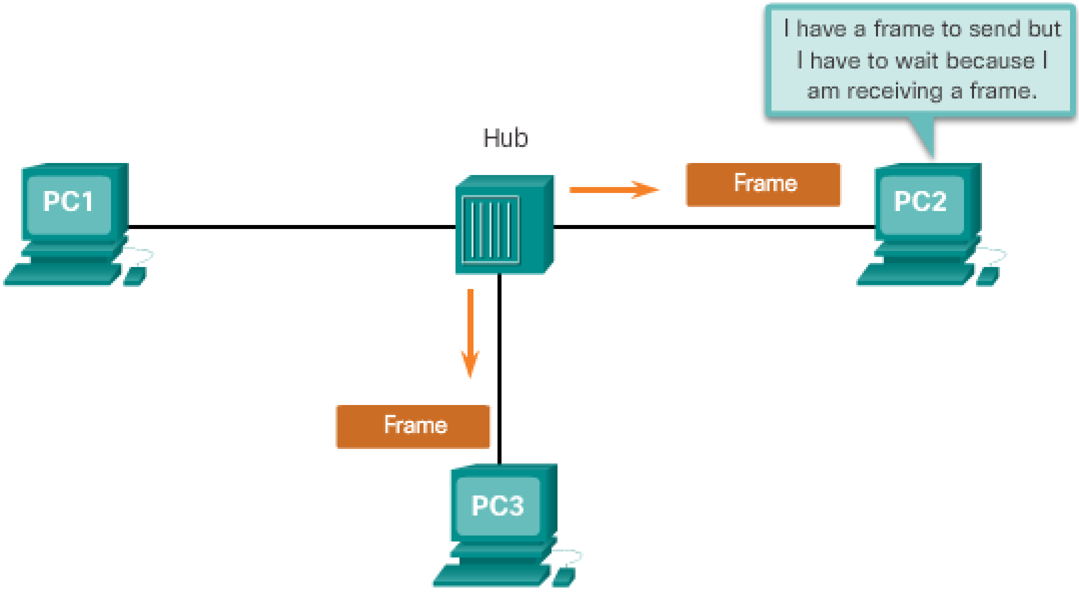
4.3 CSMA/CD

The Carrier Sense Multiple Access/Collision Detection process is used in half-duplex Ethernet LANs.

If two devices transmit at the same time, a collision will occur. Both devices will detect the collision on the network. This is done by the NIC comparing data transmitted with data received, or by recognizing the signal amplitude is higher than normal on the media. The data sent by both devices will be corrupted and will need to be resent

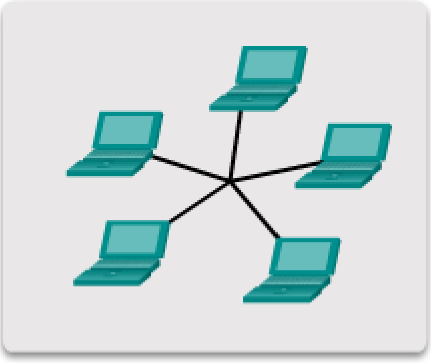

The medium is available so I will send the Ethernet frame to PC3.
Hub
PC1
Frame
PC2
PC3


Hub
PC1
PC2
PC3
Frame
Frame
This frame is not for me, so I will ignore it.
This frame is for me, so I will copy in the entire frame.

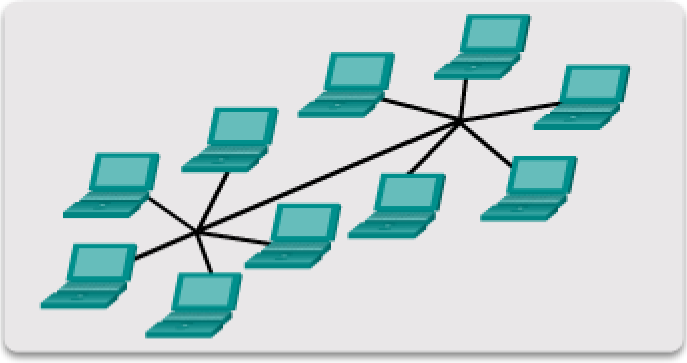

Hub
PC1
PC2
PC3
Frame
Frame
I have a frame to send but I have to wait because I am receiving a frame.

4.4 Physical Topologies

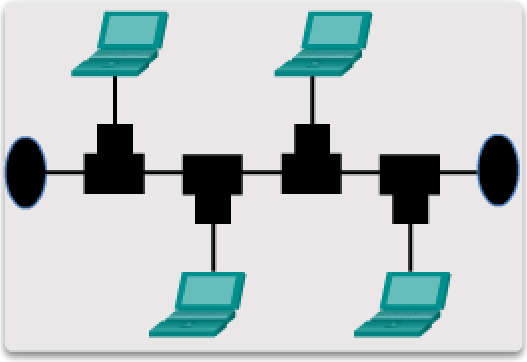
- **Star topology** : End devices are connected to a central intermediate device. Early star topologies interconnected end devices using Ethernet hubs. However, star topologies now use Ethernet switches. The star topology is easy to install, very scalable and easy to troubleshoot
- **Extended star** : Additional Ethernet switches interconnect other star topologies
- **Bus** : All end systems are chained to each other and terminated in some form on each end. Infrastructure devices such as switches are not required to interconnect the end devices. Using coax cables because it was inexpensive and easy to set up
- **Ring** : End systems are connected to their respective neighbor forming a ring. Unlike bus topology, the ring does not need to be terminated, Ring topologies were used in legacy fiber distributed data interface and token ring networks



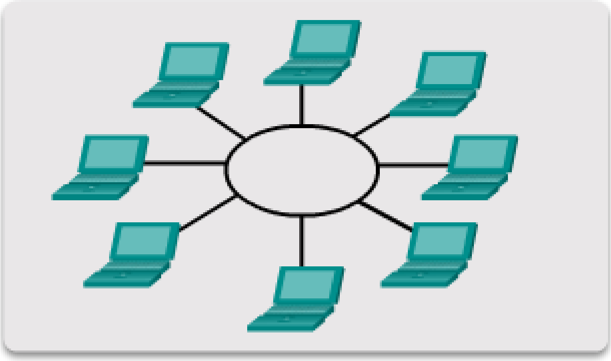
Star topology



Extended star topology



Bus topology



Ring topology

4.5 Media access control

Some network topologies share a common medium with multiple nodes. These are called multi-access networks. Ethernet LANs and WLANs are examples of a multi-access network. At any one time, there may be a number of devices attempting to send and receive data using the same network media.

- **Contention-based access** : All nodes operating in half-duplex compete for the use of the medium, but only one device can send at a time.
    - LANs using hubs
- **Controlled access** : Each node has its own time to use the medium. These networks are inefficient because a device must wait its turn to access the medium
    - Ring LANs

4.6 Frame fields

Generic frame field types include :

- **Frame start and stop indicator flags** : Used to identify the beginning and the end limits of the frame
- **Addressing** : indicates the source and destination nodes on the media
- **Type** : identifies the layer 3 protocol in the data field
- **Control** : Identifies special flow control services such as quality of service (QoS). QoS is used to give forwarding priority to certain types of messages. Data link frames carrying voice over IP (VoIP) packets normally receive priority because they are sensitive to delay
- **Data** : Contains the frame payload (i.e., packet header, segment header, and the data)
- **Error detection** : These frame fields are used for error detection and are included after the data to form the trailer

5. Ethernet

5.1 Ethernet Frame Fields

Ethernet is the most widely used LAN technology today

It operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.

The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. Including all bytes from the Destination MAC address field trough the Frame Check Sequence (FCS) field.

Frame < 64 bytes → collision fragment or runt frame → discarded by receiving stations.

Frame > 1518 or < 64 → device drops the frame → likely the result of collisions or unwanted signals therefore considered invalid

- Fields :
    - **Preamble** : Preamble (7 bytes) + start of frame (1 byte) are used for syncing between sending and receiving devices
    - **Destination MAC address** : (6 bytes) identifier for the intended recipient. Used by layer 2 to assist devices in determining if a frame is addressed to them.
    - **Source MAC address** : (6 bytes) identifies the frame's originating NIC or interface. Must be a unicast address.
    - **EtherType** : (2 bytes) identifies the upper layer protocol encapsulated in the Ethernet frame. Common values are, in hex, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP
    - **Data** : contains the encapsulated data from a higher layer
    - **FCS** (Frame Check Sequence Field) : used to detect errors in the frame

5.2 Mac Address

Is a 48-bit binary value expressed as 12 hex digits (4 bits per hex digit). MAC addressing provides a method for device identification at the lower level of the OSI model. Although Ethernet has now transitioned to full-duplex NICs and switches, it is still possible that a device that is not the intended destination will receive a Ethernet frame.

- **Structure** :
    - All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes.
    - All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes
- **NOTE** : It is possible for duplicating MAC addresses to exist due to mistakes during manufacturing or in some virtual machine implementation methods. In either case, it will be necessary to modify the MAC address with a new NIC or in software.

Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast and multicast communications.

A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to a single destination device.

Broadcast MAC Address

A broadcast packet contains a destination IPv4 address that has all ones (1s) in the host portion. All hosts on that local network will receive and process the packet. Many network protocols such as DHCP and ARP use broadcast.

Multicast MAC Address

Multicast addresses allow a source device to send a packet to a group of devices. Source will always be a unicast address.

5.3 Destination on Same Network

Layer 2 or physical addresses, like Ethernet MAC addresses, have different purpose. These addresses are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network

If the destination IP is on the same network the MAC address will be the MAC address of the destination end device.

5.4 Destination on Remote Network

If the destination IP address in on a remote network, the destination MAC address will be the address of the host's default gateway, the router's NIC.

When the router receives the Ethernet frame, it de-encapsulates the Layer 2 information. Using the destination IP address, it determines the next-hop device, and the encapsulates the IP packet in a new data link frame for the outgoing interface. Along each link in a path, an IP packet is encapsulated in a frame specific to the particular data link technology associated with that link such as Ethernet

5.5 ARP (Address Resolution Protocol)

Every device with an IP address on an Ethernet network also has an Ethernet MAC address. When a device sends an Ethernet frame, it contains these two addresses :

- Destination MAC address
- Source MAC address

To determine the destination MAC address, the device uses ARP, ARP provides two basic functions :

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings

5.5.1 Functions

When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table in its memory to find the MAC address that is mapped to the IPv4 address. This table is called the ARP table or the ARP cache. This wil be stored in the RAM of the device.

The sending device will search for its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's destination IPv4 address is on the same network as the source IPv4 address, the device will search the ARP table for the destination IPv4 address
- If the destination IPv4 address is on a different network then the source IPv4 address, the device will search the ARP table for the IPv4 address of the default gateway

If there is no entry found the device will send an ARP request.

5.5.2 Issues

ARP broadcasts

As a broadcast frame, an ARP request is received and processed by every device on the local network. On a typical business network, these broadcasts would probably have minimal impact on the network, if a large number of devices were to be powered up and all start accessing network services at the same time, there could be some reduction in performance for a short period of time.

ARP spoofing

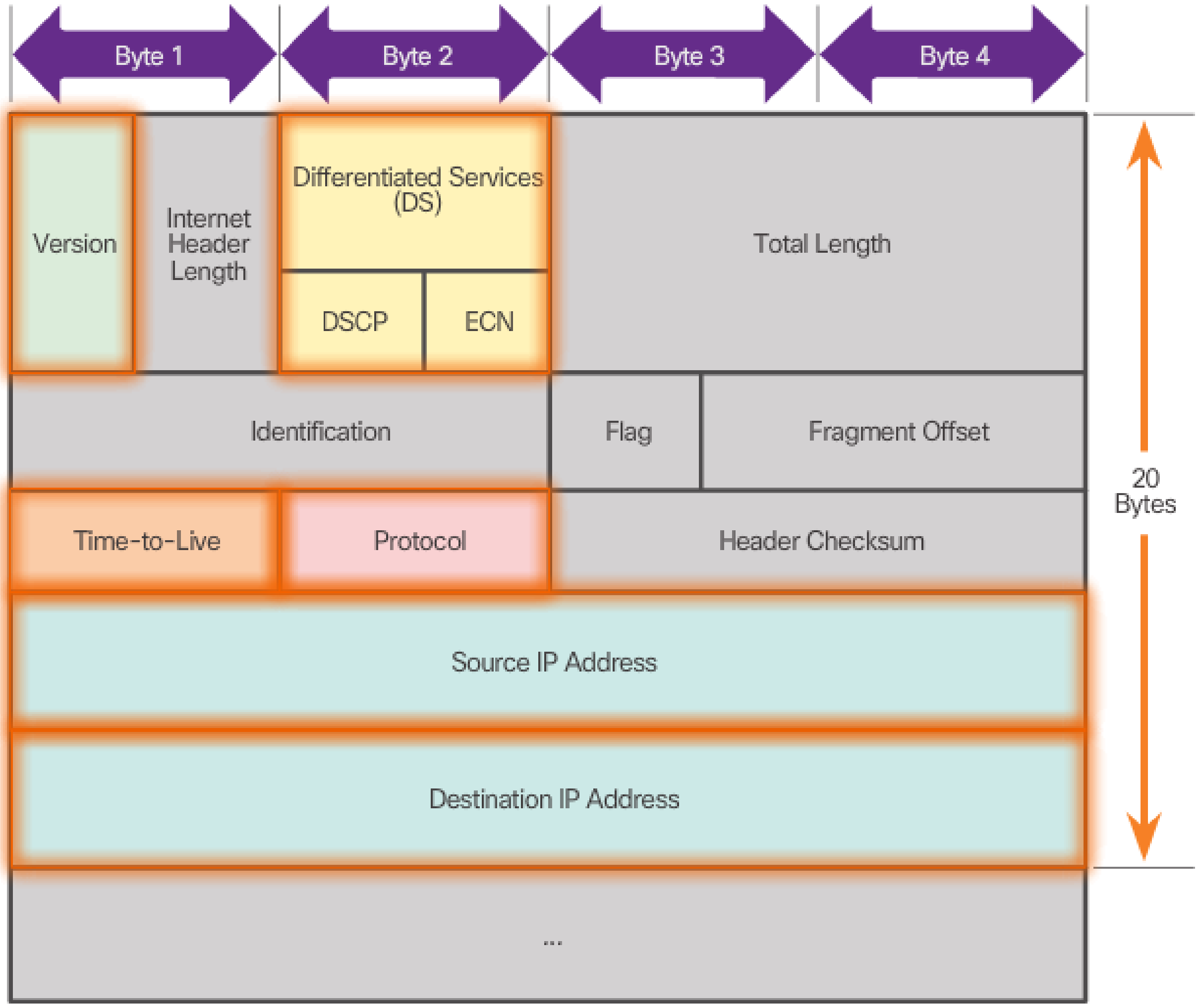
In some cases, the use of ARP can lead to a potential security risk known as ARP spoofing or ARP poisoning. This is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.

6. Network layer

6.1 IPv4

Significant fields in the IPv4 header include :

- **Version** : Contains a 4-bit binary value set to 0100 that identifies this as an IP version 4 packet
- **Differentiated Services (DS)** : Formerly called the type of services (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet
- **Time-To-Live (TTL)** : Contains a 8-bit binary value that is used to limit the lifetime of a packet. The packet sender sends the initial TTL value, and it is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol **(ICMP)** Time exceeded message to the source IP address
- **Protocol** : This 8-bit binary value indicates the data payload type that the packet is carrying. Common values include ICMP(1), TCP(6), and UDP(17)
- **Source IP Address** : Contains a 32-bit binary value that represents the source IP address of the packet
- **Destination IP Address** : Contains a 32-bit binary value that represents the destination IP address of the packet



6.1.1 Limitations of IPv4

- **IP address depletion** : limited number of unique public IPv4 addresses available
- **Internet routing table expansion** : IPv4 routes consume a great deal of memory and processor resources on internet routers
- **Lack of end-to-end connectivity** : Network Address Translation (NAT) is a technology commonly implemented within IPv4 networks. NAT provides a way for multiple devices to share a single public IPv4 address. However, because the public IPv4 address is shared, the IPv4 address of an internal network host is hidden. This can be problematic for technologies that require end-to-end connectivity.

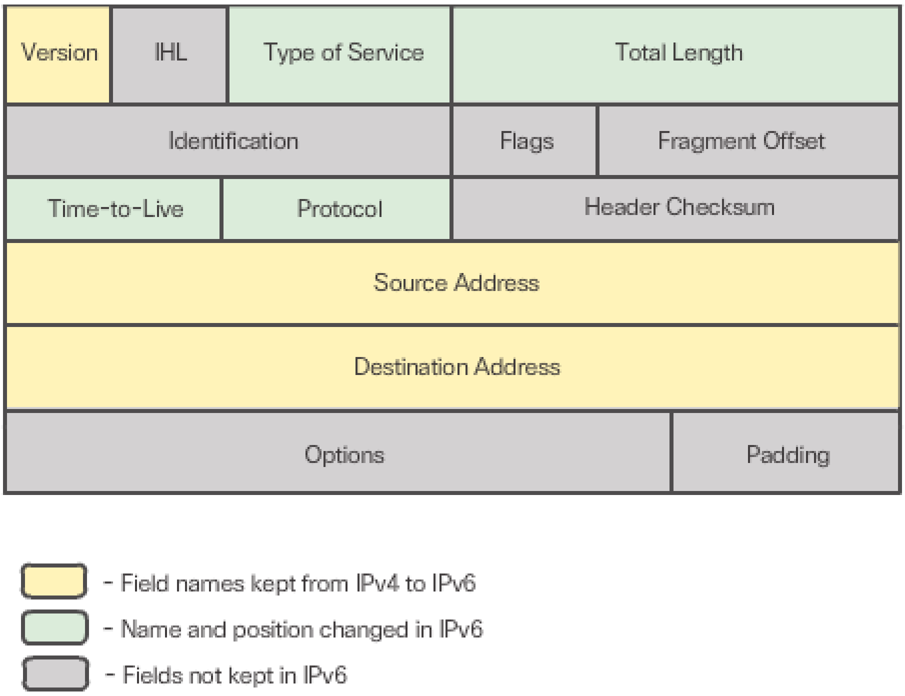
6.2 IPv6

IPv6 overcomes the limitations of IPv4 and is a powerful enhancement with features that better suit current and foreseeable network demands

Improvements include :

- **Increased address space** : IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits.
- **Improved packet handling** : The IPv6 header has been simplified with fewer fields
- **Eliminates the need for NAT** : with such a large number of public IPv6 addresses, NAT between a private IPv4 and a public IPv4 is not needed. This avoids some of the NAT-induced application problems.

IPv4 Header



🟨 Version	⬜ IHL	🟩 Type of Service	🟩 Total Length	
⬜ Identification			⬜ Flags	⬜ Fragment Offset
🟩 Time-to-Live	🟩 Protocol		⬜ Header Checksum	
🟨 Source Address				
🟨 Destination Address				
⬜ Options				⬜ Padding

🟨 - Field names kept from IPv4 to IPv6

🟩 - Name and position changed in IPv6

⬜ - Fields not kept in IPv6

6.3 Default gateway

Default gateway is the network device that can route traffic to other networks. It is the router that can route traffic out of the local network.

If the LAN is like a room the default gateway is like a doorway. If you want to get to another room you have to find the doorway.

- Routes traffic to other networks
- Has a local IP address in the same address range as the other hosts on the network
- Can take data in and forward data out

6.4 Router

Regardless of their function, size or complexity, all router models are essentially computers. Just like computers, tablets and smart devices routers also require :

- Central processing units (CPU)
- Operating systems (OS)
- Memory consistent of random-access memory (RAM), read-only memory (ROM), nonvolatile random-access memory (NVRAM), and flash

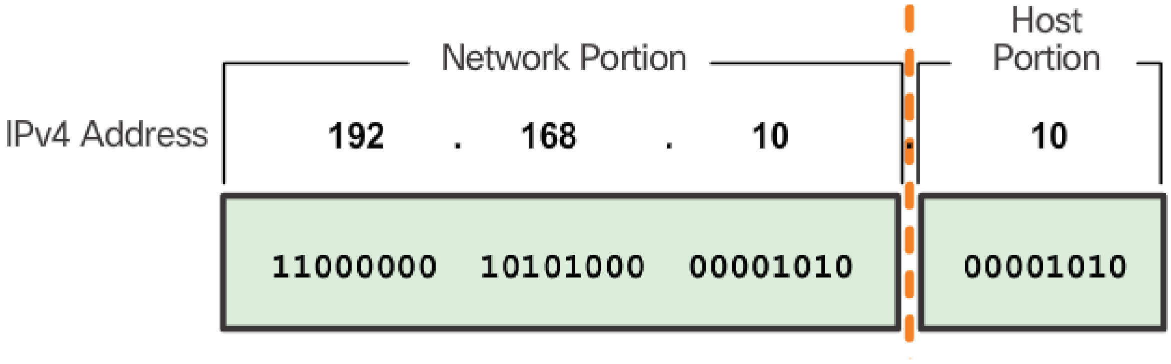
The CPU requires an OS to provide routing and switching functions. The Cisco Internetwork Operating System (IOS) is the system software used for most Cisco devices regardless of the size and type of the device. Used for routers, LAN switches, small wireless access points, large routers with dozens of interfaces and many others.

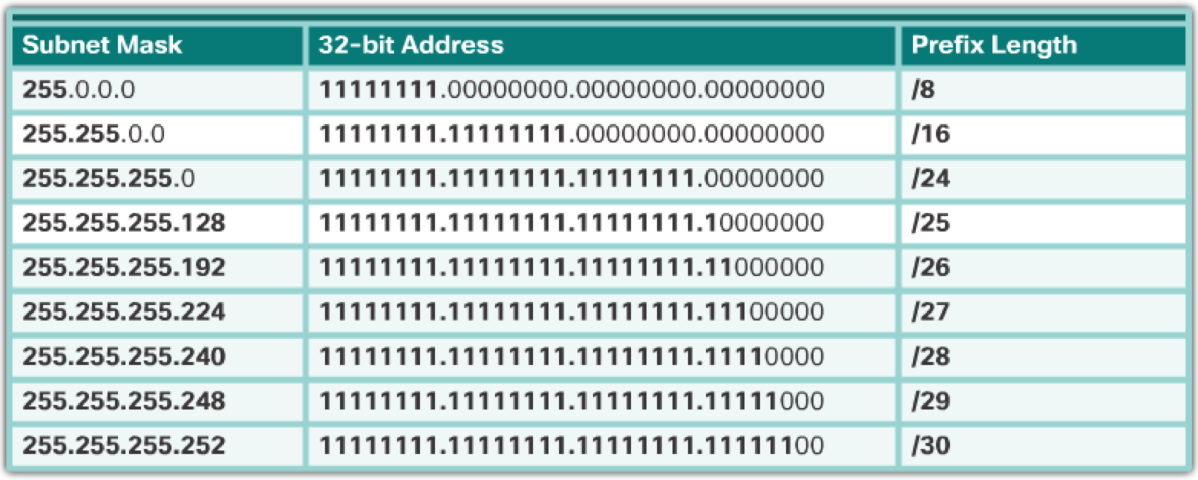
Cisco routers uses four types of memory :

- **RAM** : Volatile memory to store apps, processes and data needed to be executed by the CPU →FAST
- **ROM** : Non-Volatile memory to store crucial operational instructions and limited IOS.
- **NVRAM** : Permanent storage for the startup configuration (startup-config)
- **Flash** : Non-Volatile computer memory used as permanent storage for the IOS and other system related files such as log files, voice configuration files, HTML files,…

7. Explore the network

7.1 IP addressing & subnet masks





Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

7.1.1 Types of addresses in a network

- **Network** Address :
  - Address and subnet mask refer to a network. All hosts within the network share the same network address. The host portion is all 0's
- **Host** addresses :
  - First host address :
    - First available host IP address in that network. The host portion always has all 0s and ends with a 1
  - Last host address :
    - Last available host IP address in that network. The host portion always has all 1s and ends with a 0
- **Broadcast** Address :
  - A special address that communicates with all hosts in a network. For instance, when a host sends a packet to the network broadcast IPv4 address, all other hosts in the network receive the packet. The broadcast address uses the highest address in the network range. The host portion is all 1s

7.1.2 IPv4 Communication

- **Unicast** :
  - The process of sending a packet from one host to an individual host
- **Broadcast** :
  - The process of sending a packet from one host to all hosts in the network
- **Multicast** :
  - The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

7.1.3 Public and private IPv4 Addresses

- Public IPv4 addresses are addresses which are globally routed between ISP (Internet Service Provider) routers. However, not all available IPv4 addresses can be used on the internet. There are blocks of addresses called private addresses that are used by most organizations to assign IPv4 addresses to internal hosts
- Specifically, the private address blocks are :
  - 10.0.0.0/8 = 10.0.0.0 → 10.255.255.255
  - 172.16.0.0/12 = 172.16.0.0 → 172.31.255.255
  - 192.168.0.0/16 = 192.168.0.0 → 192.168.255.255

7.1.4 Classful and Classless

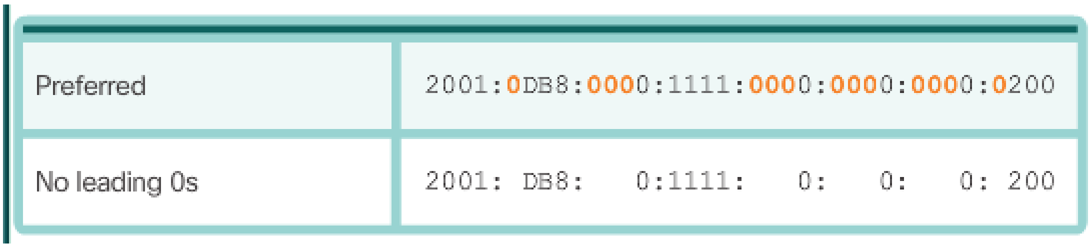
- Classful addressing was abandoned in the late ’90 for the newer and current classless addressing system. However, there are still classful remnants in networks today. For example, when you assign a IPv4 address to a computer, the operating system examines the address being assigned to determine if this address is a class A, class B or class C. The operating system then assumes the prefix used by that class and makes the default subnet mask assignment.
- This new set of standards allowed service providers to allocate IPv4 addresses on any address bit boundary instead of only by class.

7.2 IPv6 address

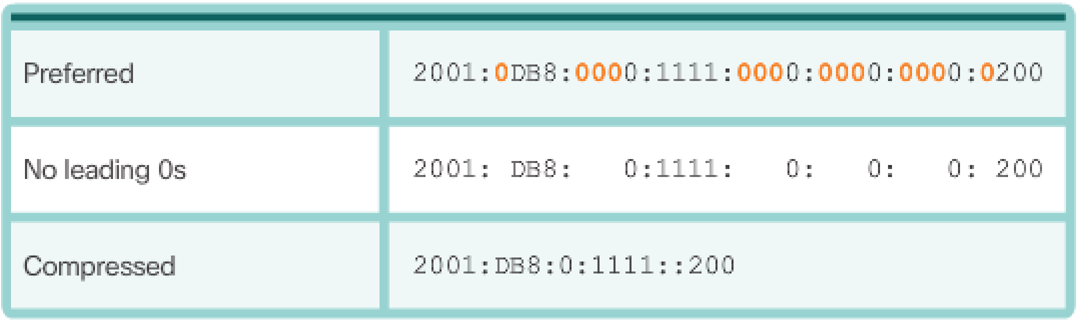
7.2.1 IPv6 address representation

- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every 4 bit is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. This is not case sensitive.
- **Prefix** = 64 bits

Interface ID = 64 bits



Preferred	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001: DB8: 0:1111: 0: 0: 0: 200



Preferred	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001: DB8: 0:1111: 0: 0: 0: 200
Compressed	2001:DB8:0:1111::200

7.2.2 IPv6 Address types

- **Unicast**
- **Multicast**
- **Anycast** (→ Beyond the scope of this course)
- IPv6 has **NO!!! broadcast** address. However there's an IPv6 all-nodes multicast address that essentially gives the same result

8. Subnetting IP networks

8.1 Broadcast Domains

In an Ethernet LAN, devices use broadcasts to locate :

- **Other devices** : A device uses Address Resolution Protocol (ARP) which sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address.
- **Services** : A host typically acquires its IP address configuration using the Dynamic Host Configuration Protocol (DHCP) which sends broadcasts on the local network to locate a DHCP server

8.2 Problems with Large Broadcast Domains

A large broadcast domain is a network that connects many hosts. A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network. Resulting in :

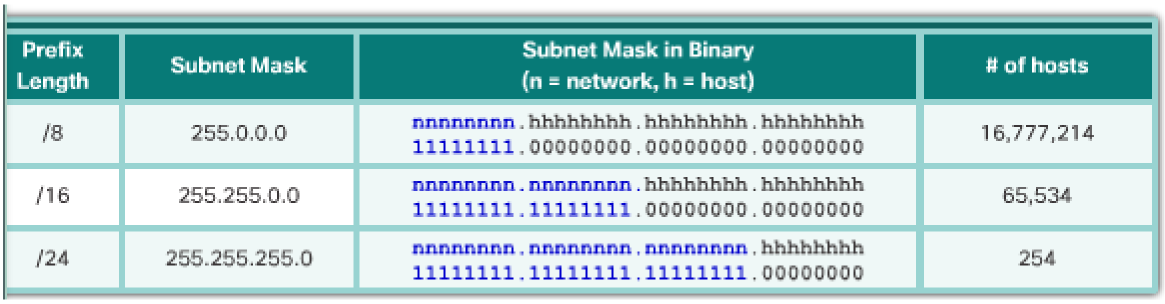
- Slow network operations → due to the significant amount of traffic
- Slow device operations → device must accept and process each broadcast packet

8.3 Reasons for subnetting

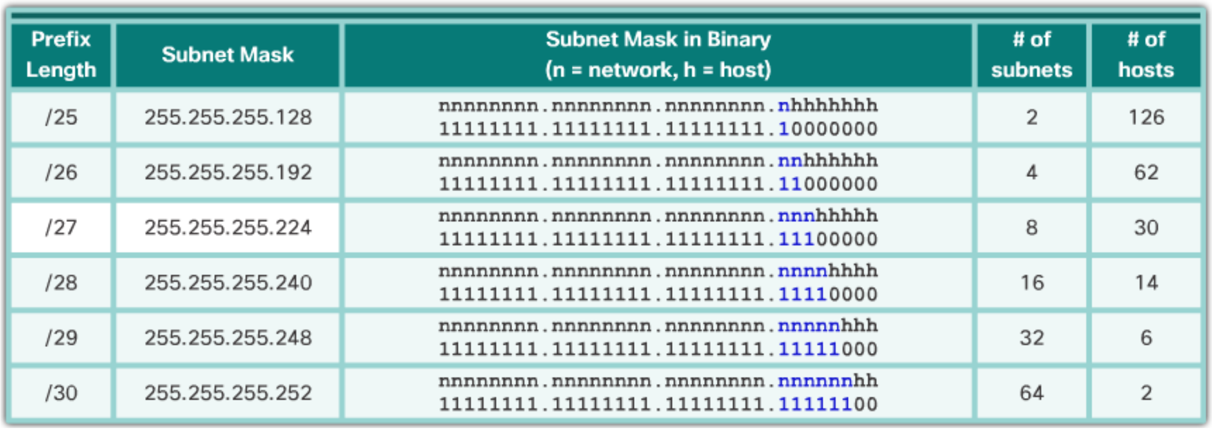
Subnetting reduces overall network traffic and improves network performance. It also enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together.

There are various ways of using subnets to help manage network devices. Network administrators can group devices and services into subnets that are determined by:

- Locations : such as floors in buildings
- Organizational unit
- Device type
- Any other division that makes sense for the network



Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254



Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

- Subnetting between IPv4 and IPv6 is pretty much the same, the only difference is scale
- IPv6 subnetting is easier to implement than IPv4, because there is no conversion to binary required. To determine the next available subnet, just count up in hexadecimal.

HERHAAL NU DIE LEUKE OEFENINGEN VAN SUBNETTEN DIE JE SOWIESO KEIGOED HEBT MEEGEDAAN IN DE LES CISCO.

9. Transport Layer

9.1 Role of the transport layer

- Responsible for establishing a temporary communication session between two applications and delivering data that is sent from an application on a source host to an application on a destination host.
- Transport layer = link between the application layer
- It ensures that even with multiple applications running on a device, all applications receive the correct data

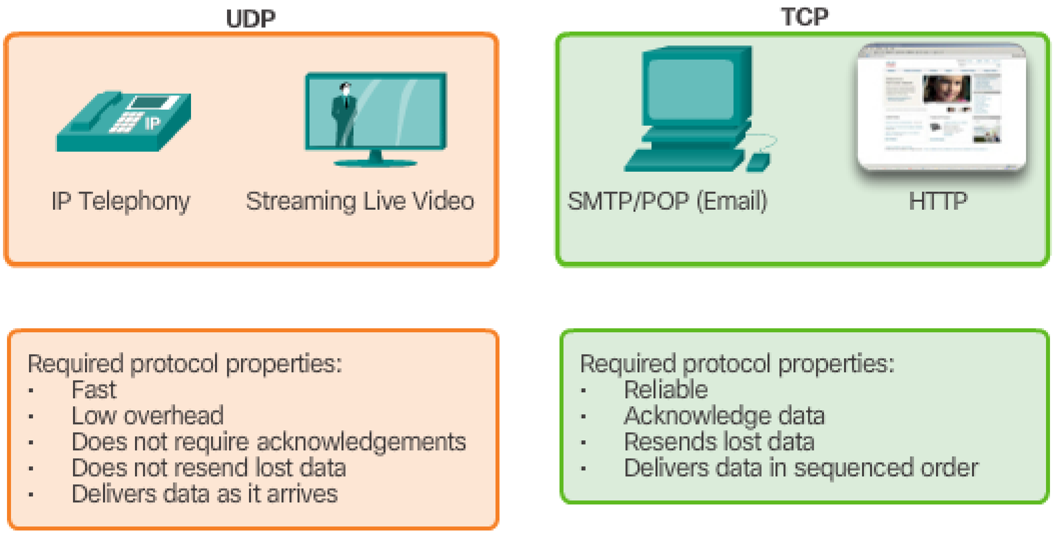
9.2 TCP (Transport Control Protocol) and UDP (User Datagram Protocol)

TCP transport sends packages that are tracked from source to destination.

With TCP, there are three basic operations of reliability :

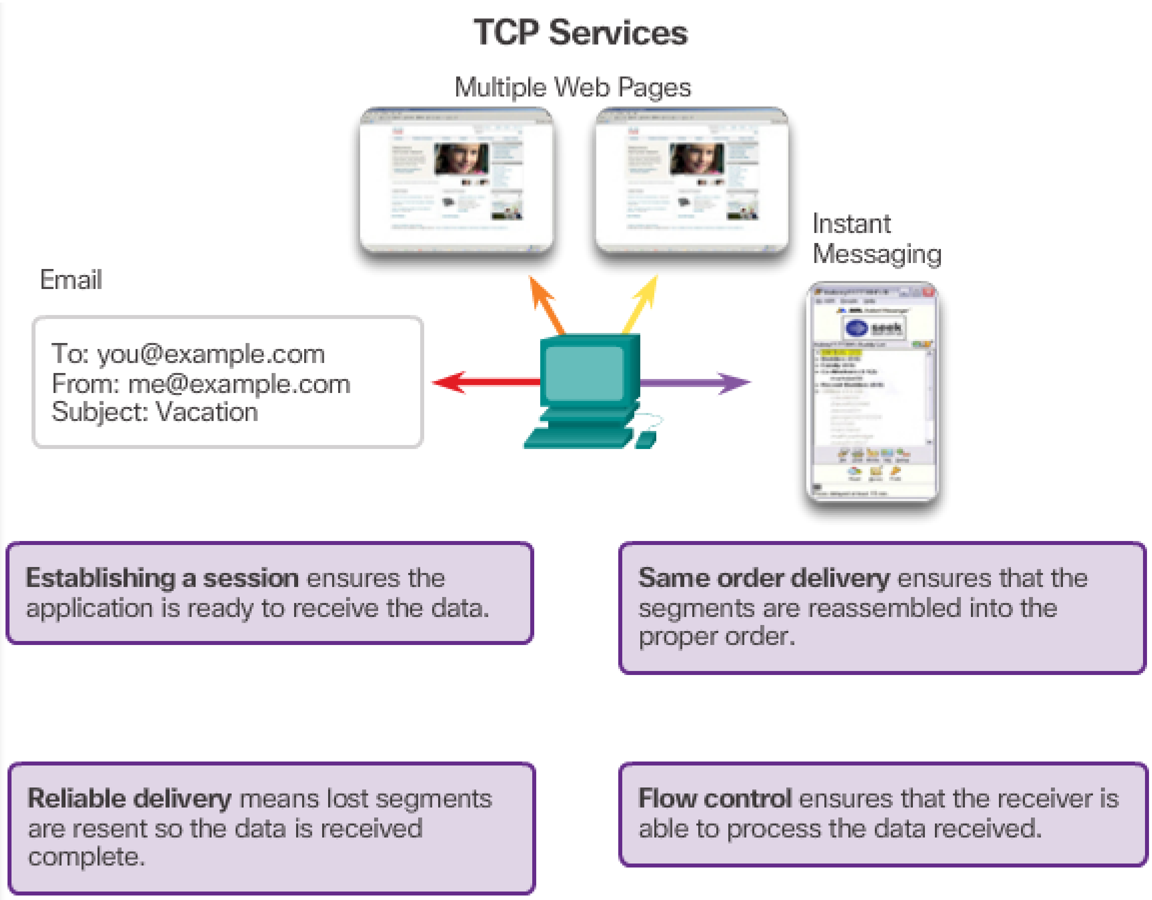
- Numbering and tracking data segments transmitted to a specific host from a specific application
- Acknowledging received data
- Retransmitting any unacknowledged data after a certain period of time

UDP provides the basic functions for delivering data segments between the appropriate applications, with a very little overhead and data checking. UDP is known as best-effort delivery protocol. In the context of networking best-effort delivery is referred to as unreliable because there is no acknowledgement that the data is received at the destination.



Required protocol properties:
- Fast
- Low overhead
- Does not require acknowledgements
- Does not resend lost data
- Delivers data as it arrives

Required protocol properties:
- Reliable
- Acknowledge data
- Resends lost data
- Delivers data in sequenced order



TCP Services

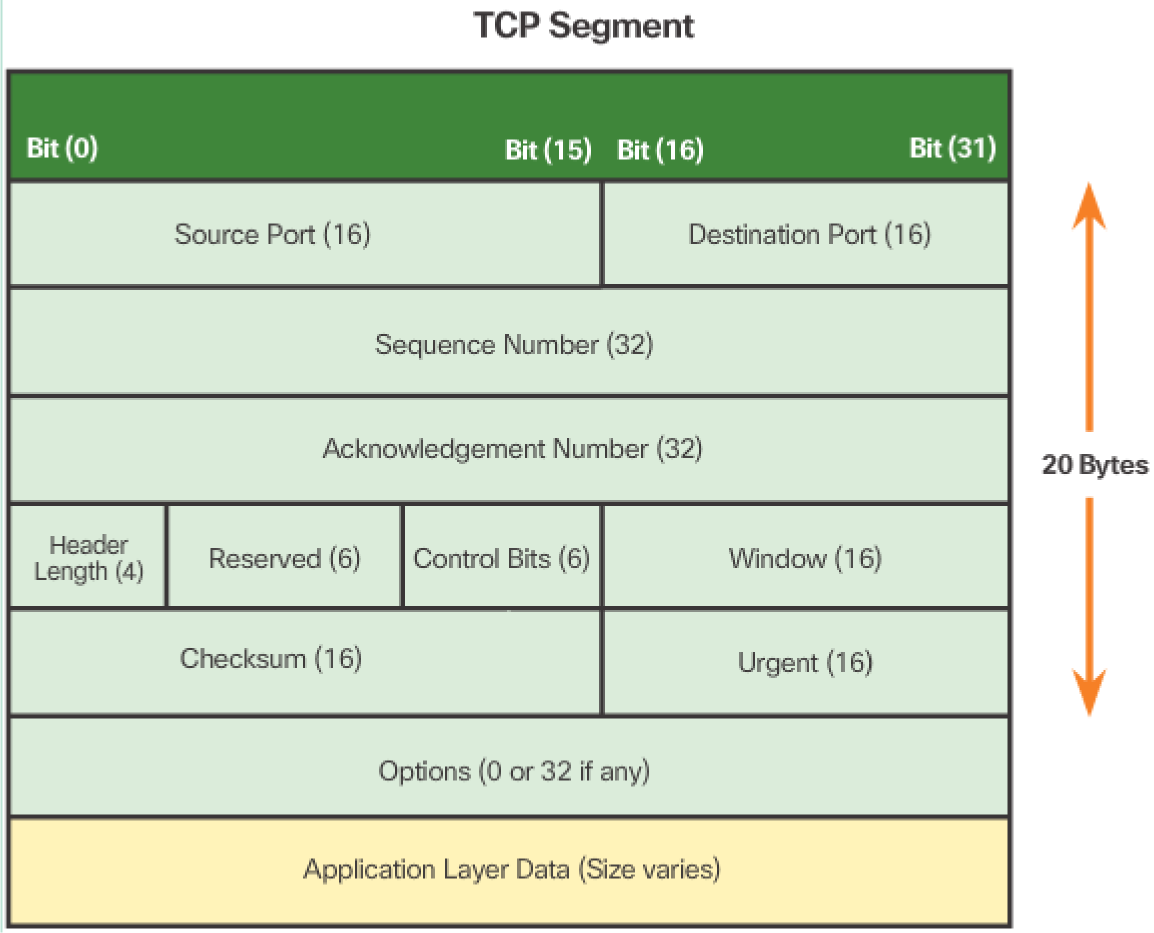
To: you@example.com
From: me@example.com
Subject: Vacation

Establishing a session ensures the application is ready to receive the data.

Same order delivery ensures that the segments are reassembled into the proper order.

Reliable delivery means lost segments are resent so the data is received complete.

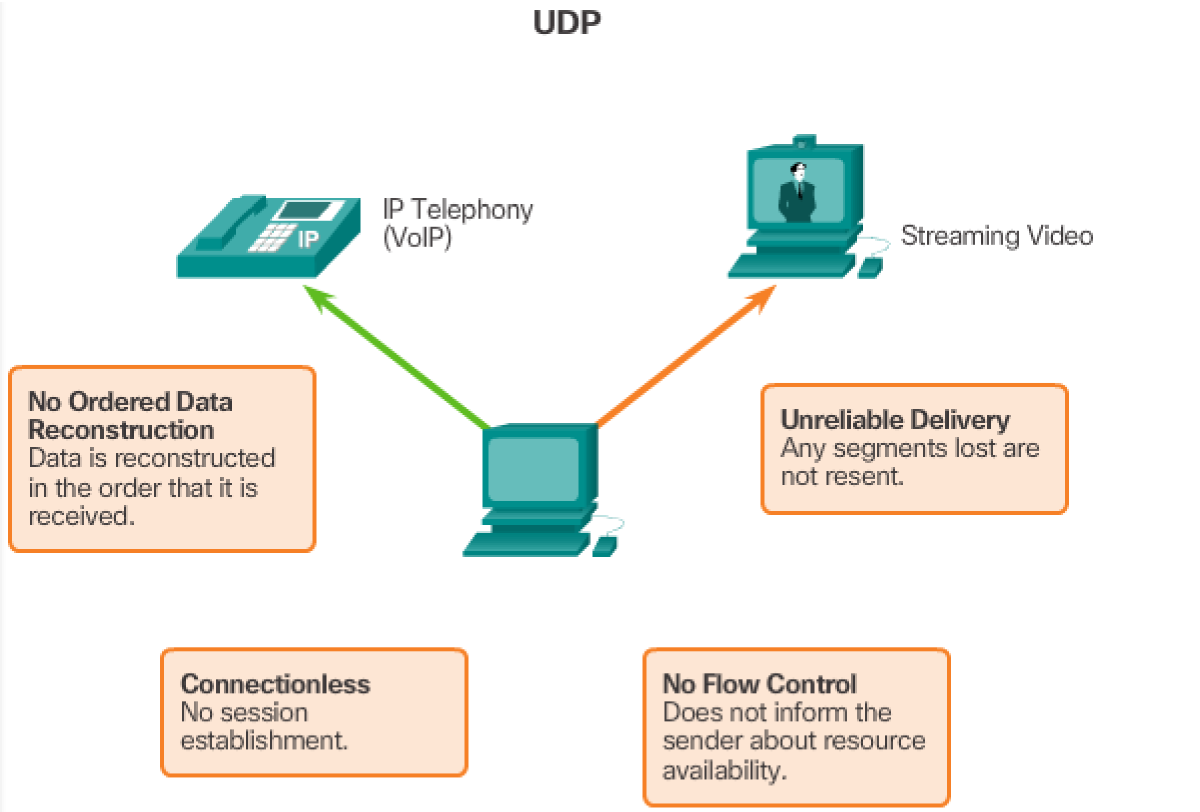
Flow control ensures that the receiver is able to process the data received.



TCP Segment

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Source Port (16)		Destination Port (16)	
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length (4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)		Urgent (16)	
Options (0 or 32 if any)			
Application Layer Data (Size varies)			

- **Source Port, Destination port** : used to identify the app
- **Sequence number** : used for data reassembly purposes
- **Acknowledgment number** : indicates the data that has been received
- **Header length** : known as “data offset”. Indicates the length of the TCP segment header
- **Reserved** : This field is reserved for the future
- **Control bits** : Includes bit codes or flags, which indicate the purpose and function of the TCP segment
- **Window size** : Indicates the number of bytes that can be accepted at one time
- **Checksum** : Used for error checking of the segment header and data
- **Urgent** : Indicates if data is urgent



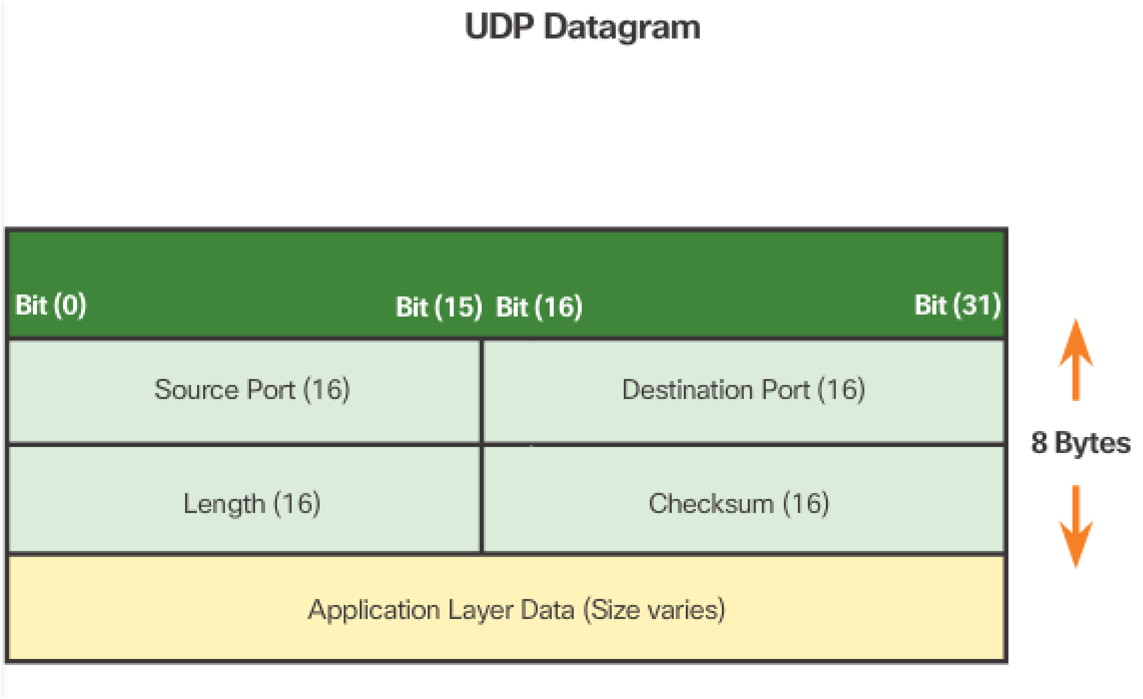
UDP

No Ordered Data Reconstruction
Data is reconstructed in the order that it is received.

Unreliable Delivery
Any segments lost are not resent.

Connectionless
No session establishment.

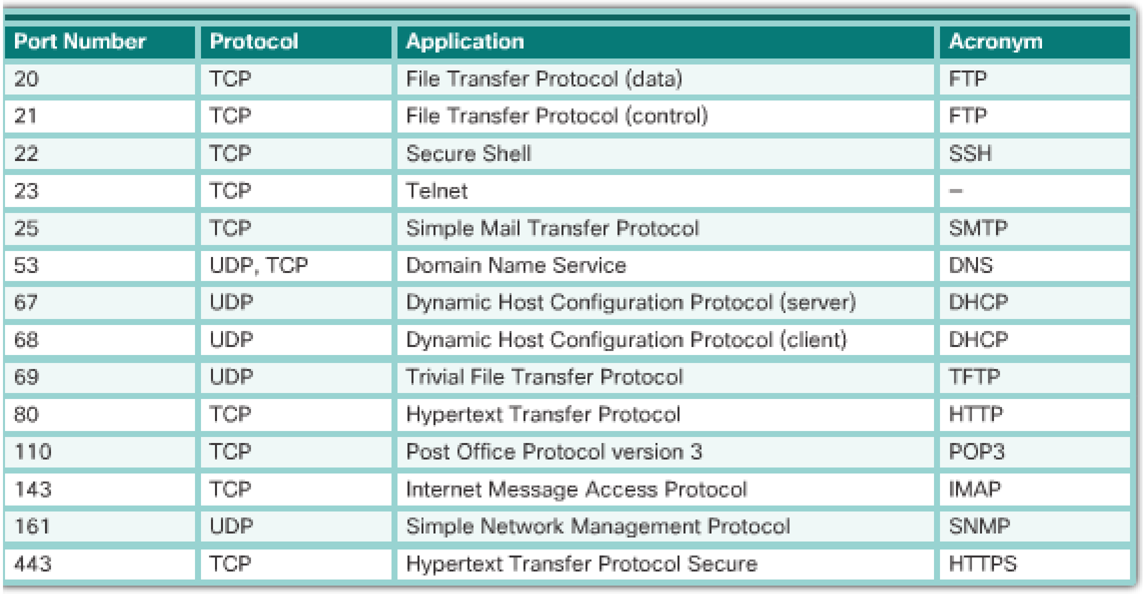
No Flow Control
Does not inform the sender about resource availability.



UDP is a stateless protocol, meaning neither the client, nor the server is obligated to keep track of the state of the communication session.

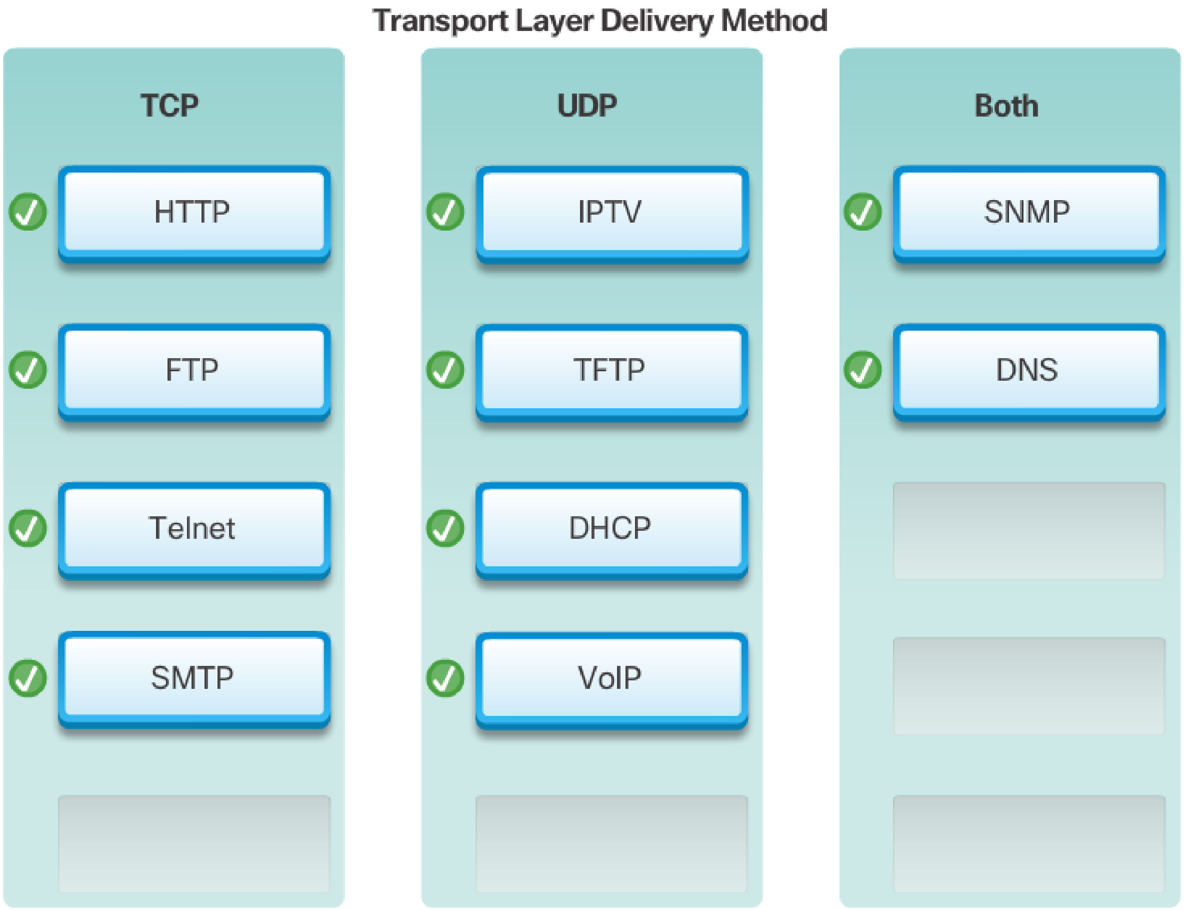
One of the most important requirements for delivering live video and voice over the network is that the data continues to flow quickly. Live video and voice applications can tolerate some data loss with minimal or no noticeable effect, and are perfectly suited to **UDP**

9.3 Port numbers



Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS

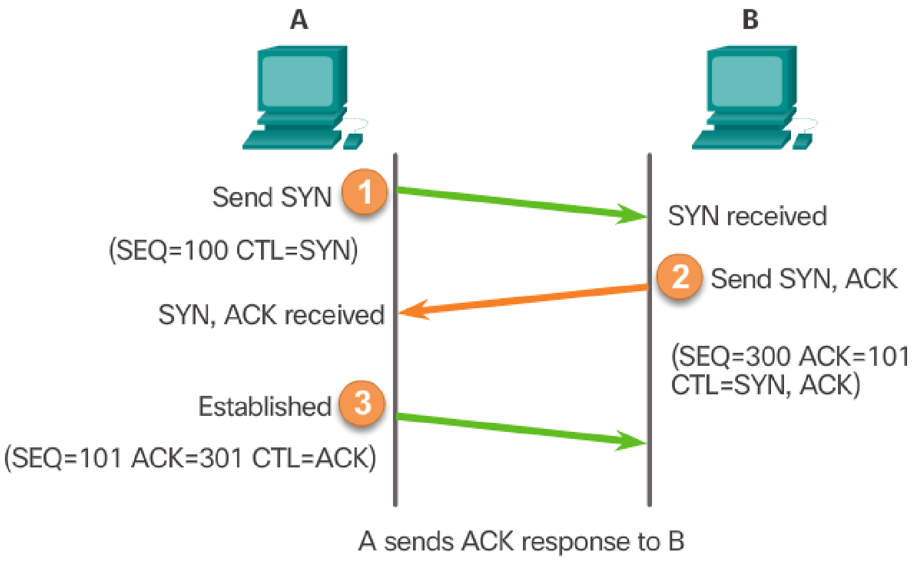
9.4 UDP or TCP



Transport Layer Delivery Method

TCP	UDP	Both
✓ HTTP	✓ IPTV	✓ SNMP
✓ FTP	✓ TFTP	✓ DNS
✓ Telnet	✓ DHCP	
✓ SMTP	✓ VoIP	

9.5 Three Way Handshake



- **1 :** The initiating client requests a client-to-server communication session with the server
- **2 :** The server acknowledges the client-to-server communication session and requests a server-to-client communication session
- **3 :** The initiating client acknowledges the server-to-client communication session.

HOOFDSTUK 10 & 11 STAAT NIET IN DE DOELSTELLINGENPUNTJES MAAR ZOU IK TOCH NOG MAAR EENS DOORLEZEN.