BATCH :	B107 **AWS DevOps**
LESSON :	**Network**
DATE :	24.12.2022
SUBJECT :	**Network Protocols**

ZOOM GİRİŞLERİNİZİ LÜTFEN **LMS** SİSTEMİ ÜZERİNDEN YAPINIZ

- Proxy
- Domain- Sub domain
- TLD
- Bridge
- Router
- DHCP
- Subnet Mask

- Firewall
- Switch
- Hub
- WAP
- Routing Table
- Load Balancer
- Gateway
- NTP Server

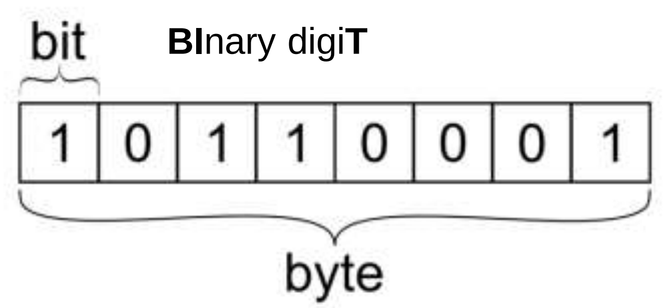
NETWORK Day 4

Contents

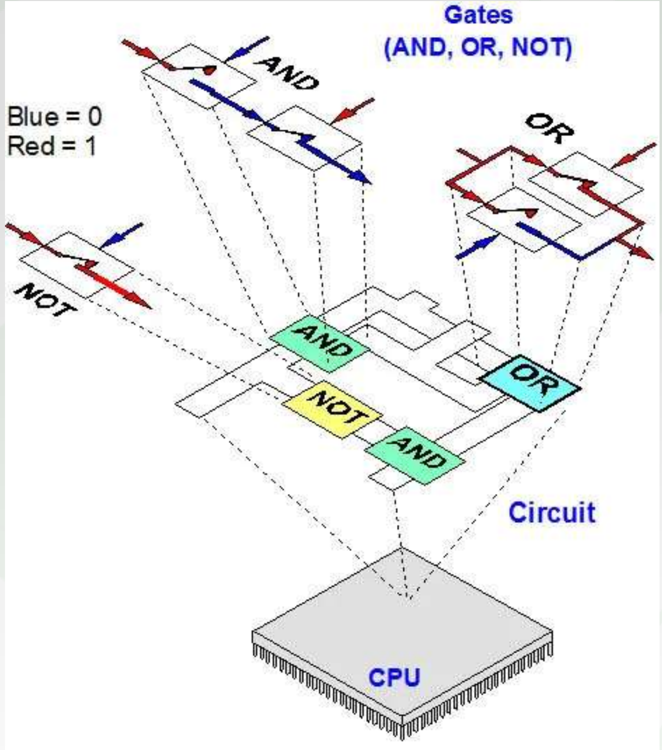
- Protocols
- Transmission

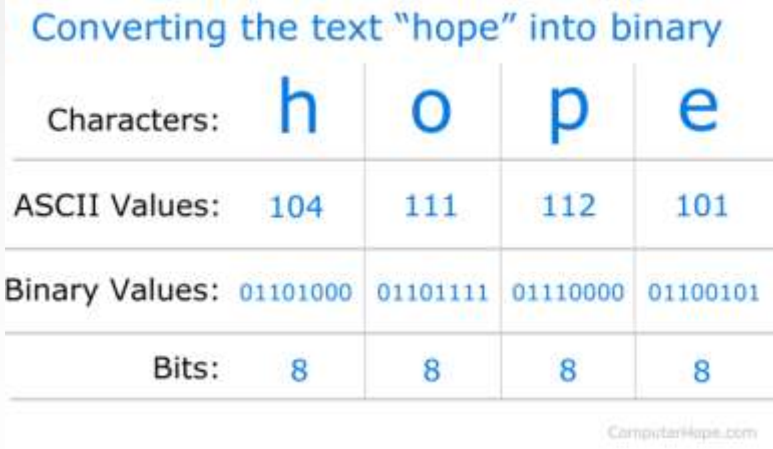
İçerik

- Protokoller
- İletim



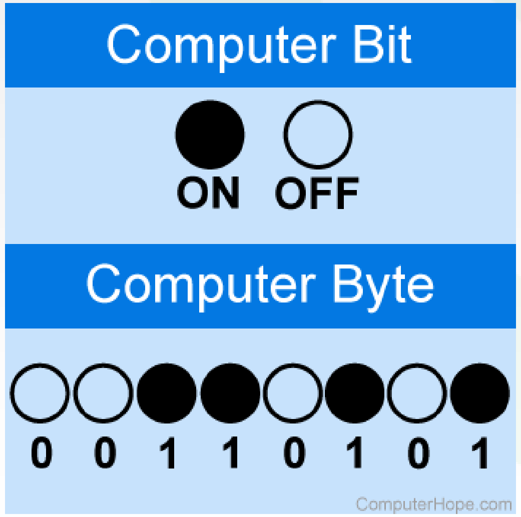
Simple electric circuit
On
Off



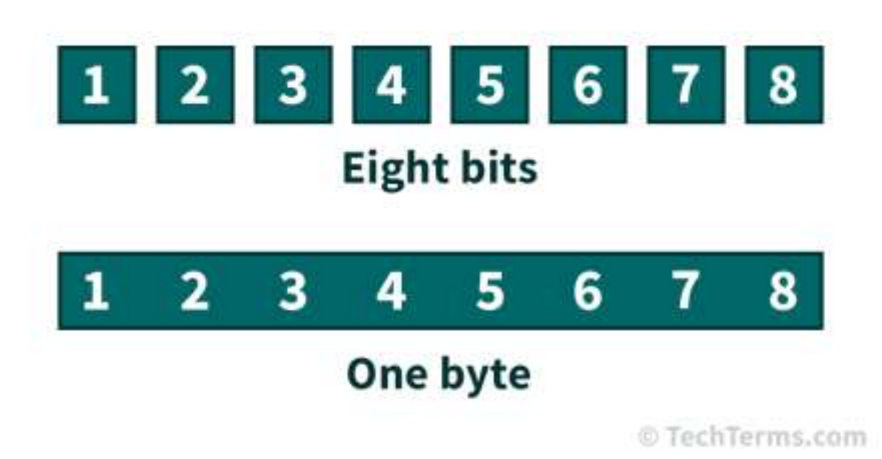

Converting the text "hope" into binary

Characters:	h	o	p	e
ASCII Values:	104	111	112	101
Binary Values:	01101000	01101111	01110000	01100101
Bits:	8	8	8	8

ComputerHope.com



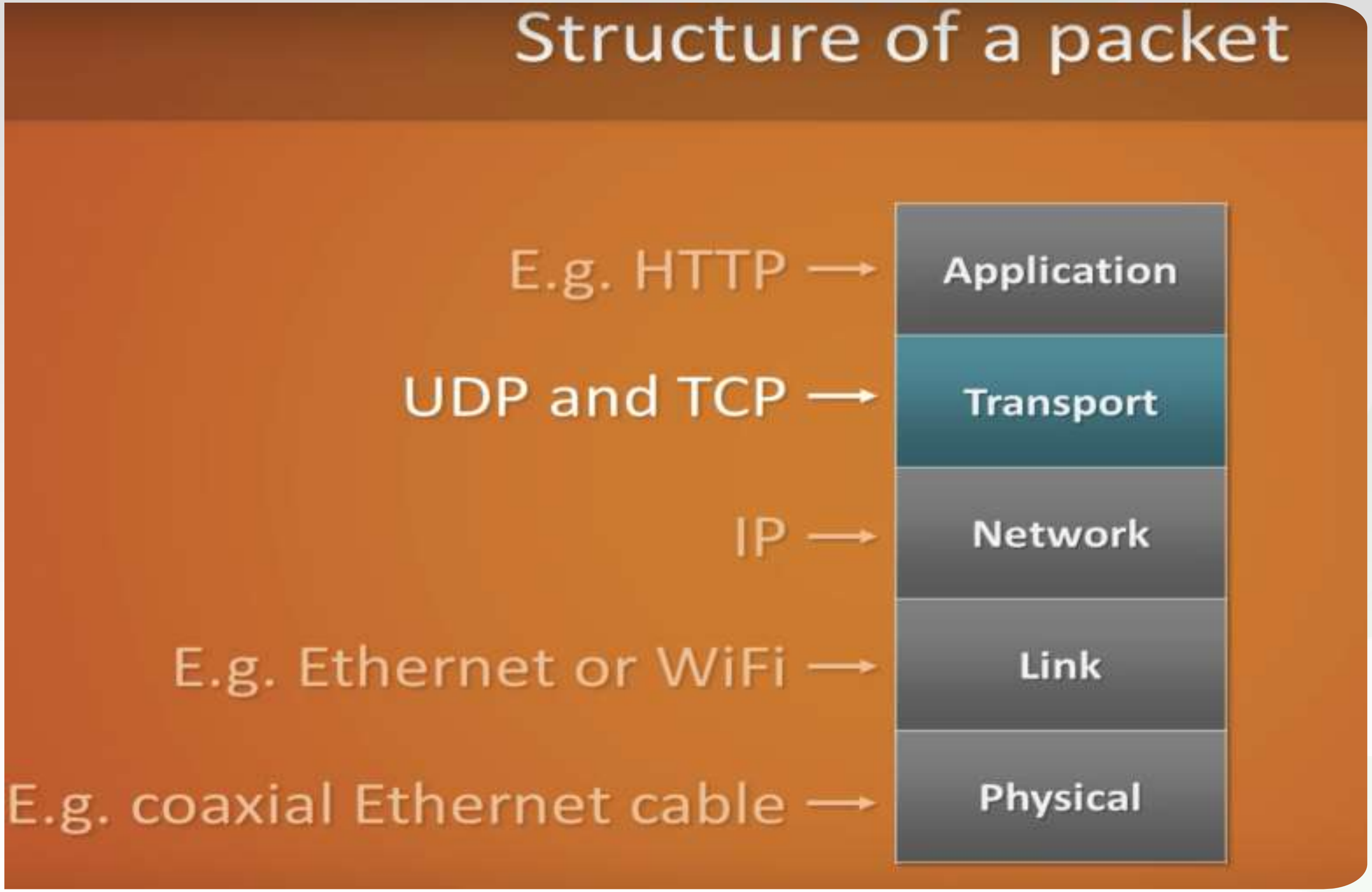
ComputerHope.com



© TechTerms.com

Unit	Equivalent to	Remarks
kilobyte (KB)	1024 bytes	Space used by 10 lines of text
1 megabyte (MB)	1024 kilobytes	Memory of the earliest PCs
gigabyte (GB)	1024 megabytes	Memory of today's PCs
1 terabyte (TB)	1024 gigabytes	Capacity of today's hard disks
petabyte (PB)	1024 terabytes	Space used for rendering Of film Avatar

The TCP/IP Model



Structure of a packet

E.g. HTTP → Application

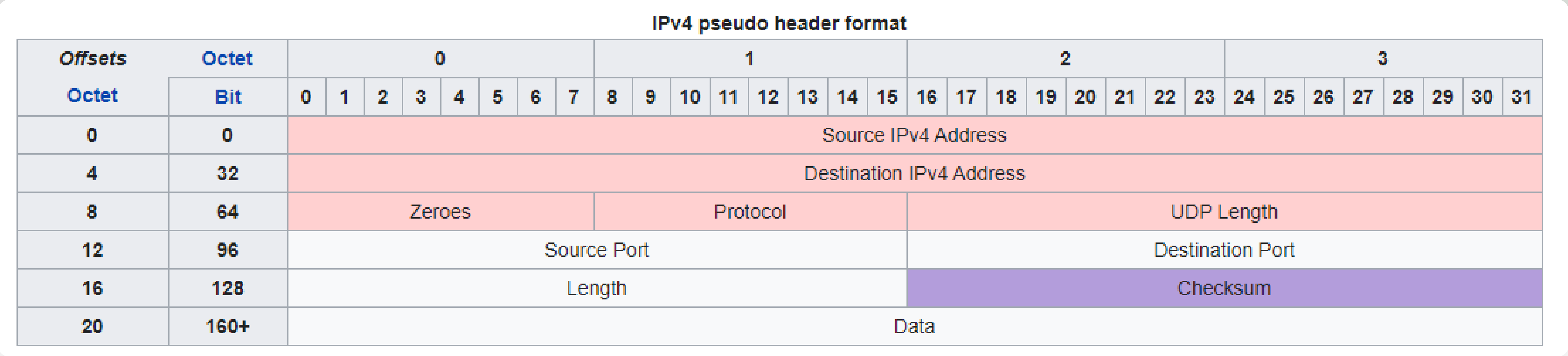
UDP and TCP → Transport

IP → Network

E.g. Ethernet or WiFi → Link

E.g. coaxial Ethernet cable → Physical

UDP – User Datagram Protocol Packet Header

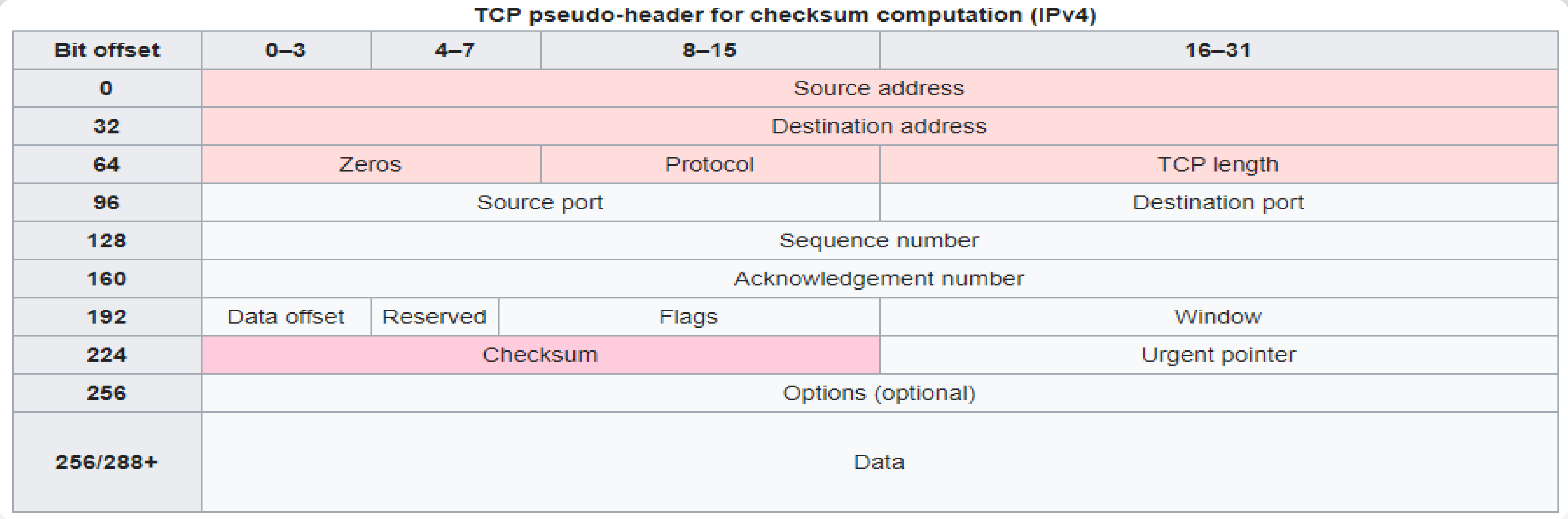


IPv4 pseudo header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source IPv4 Address																															
4	32	Destination IPv4 Address																															
8	64	Zeroes								Protocol								UDP Length															
12	96	Source Port																Destination Port															
16	128	Length																Checksum															
20	160+	Data																															

- UDP – User Datagram Protocol
- UDP is suitable for purposes where error checking and correction are not required or performed at the application layer.
- UDP avoids the overhead of connection operations, thus it is fast.
- It is the core protocol of IP in Transport Layer.
- Example: For large packages with TV, Game, Stream broadcasts

TCP - Transmission Control Protocol Packet Header

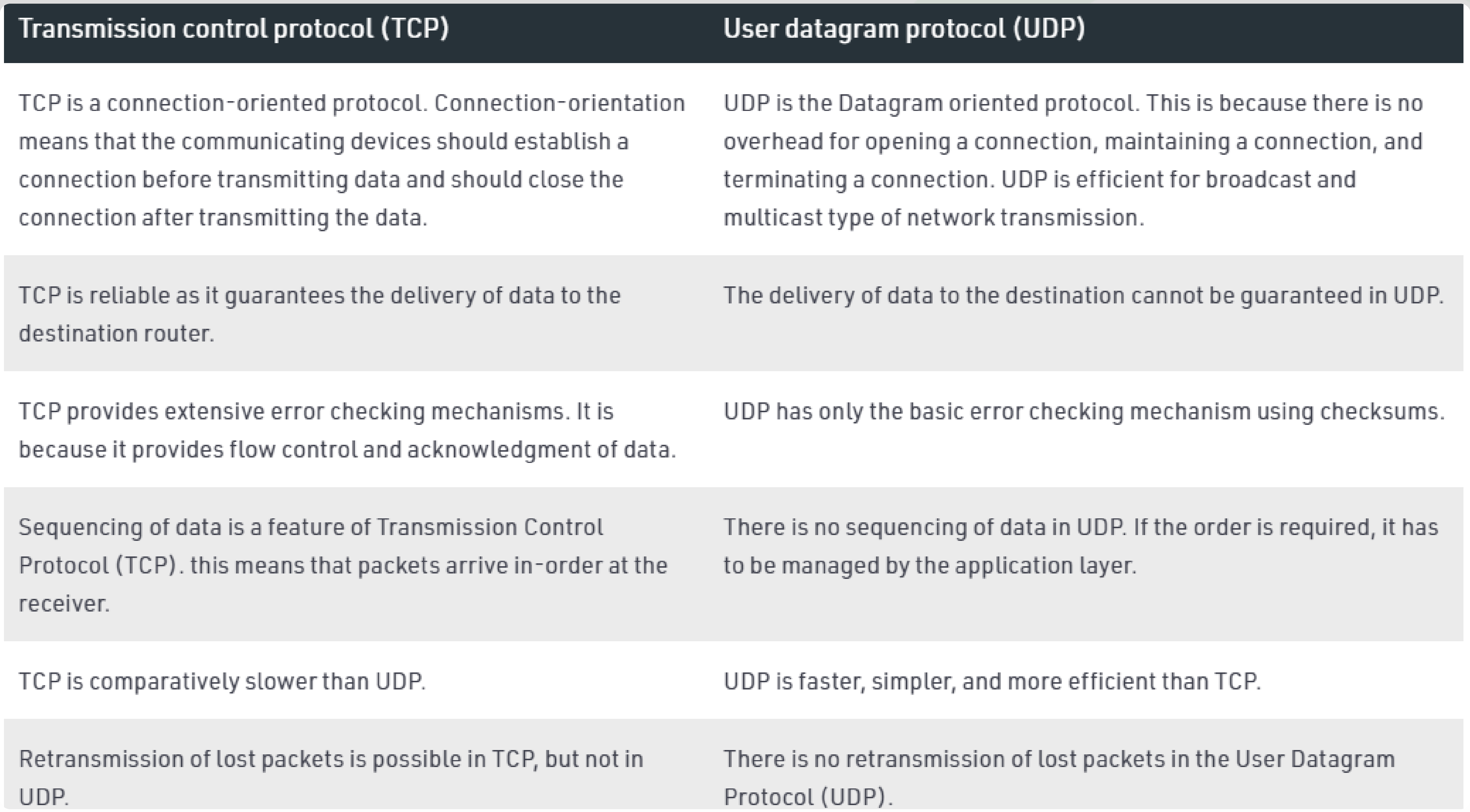


TCP pseudo-header for checksum computation (IPv4)

Bit offset	0–3	4–7	8–15	16–31
0	Source address			
32	Destination address			
64	Zeros		Protocol	TCP length
96	Source port			Destination port
128	Sequence number			
160	Acknowledgement number			
192	Data offset	Reserved	Flags	Window
224	Checksum			Urgent pointer
256	Options (optional)			
256/288+	Data			

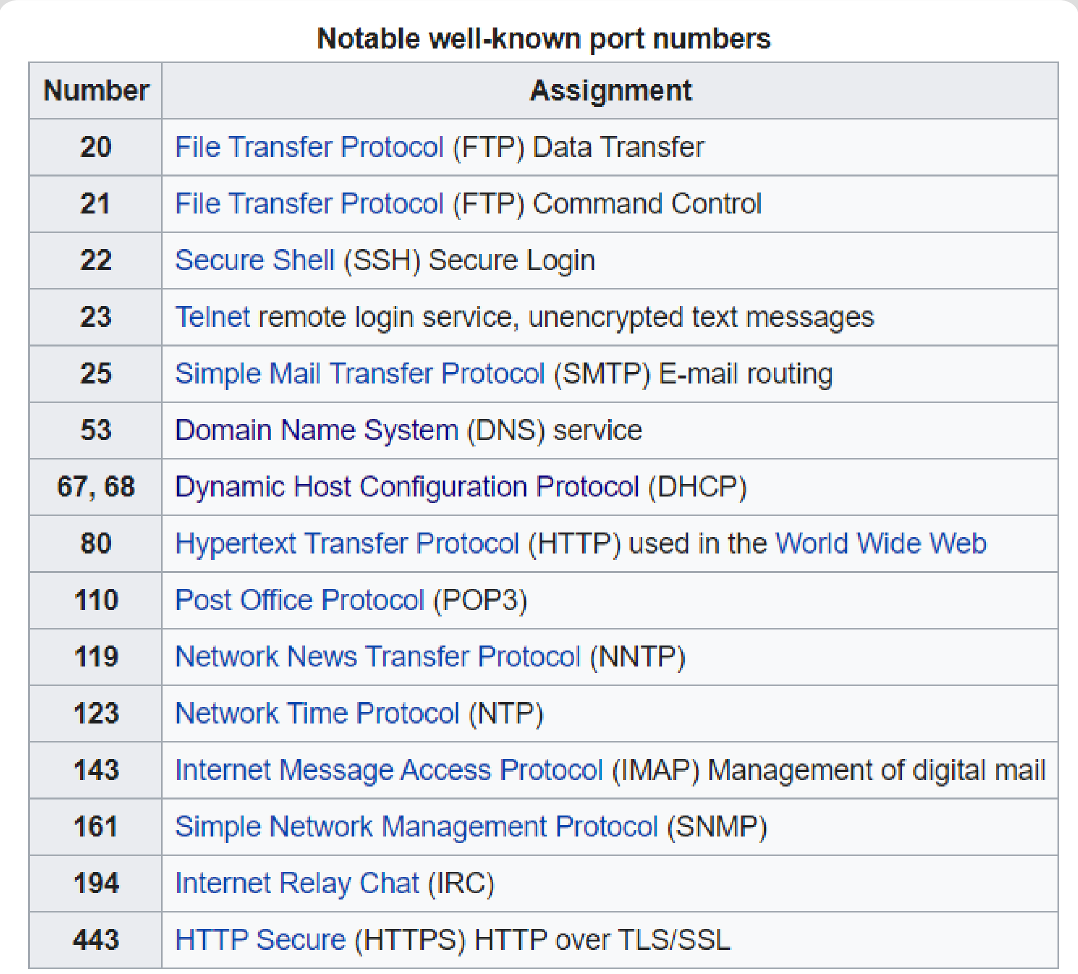
- **Transmission Control Protocol (TCP)**
  - □ TCP provides reliable, sequential and error-controlled delivery of data stream between applications running on computers communicating over an IP network.
  - □ It is the core protocol of IP in Transport Layer
  - □ Example: www, email, remote administration, and file transfer , SSL/TLS

TCP vs UDP



Transmission control protocol (TCP)	User datagram protocol (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).

Port Numbers



Notable well-known port numbers

Number	Assignment
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

□ The app's credential

□ A different number is assigned for each application

□ Firewall blocks except what is known

□ A virtual number is assigned – IANA

□ 16-bit, from 0 to 65535

□ The most known and used ones are between 0-1023 (System Ports)

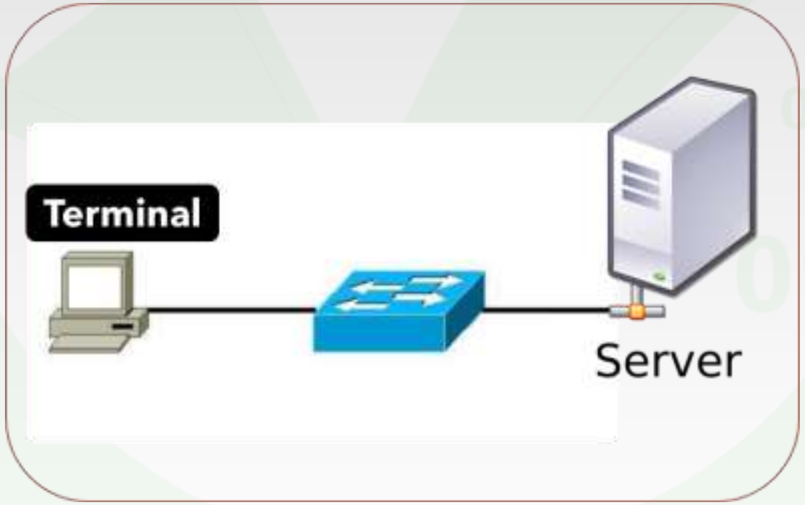
Telnet (TCP 23)

- telnet google.com 80

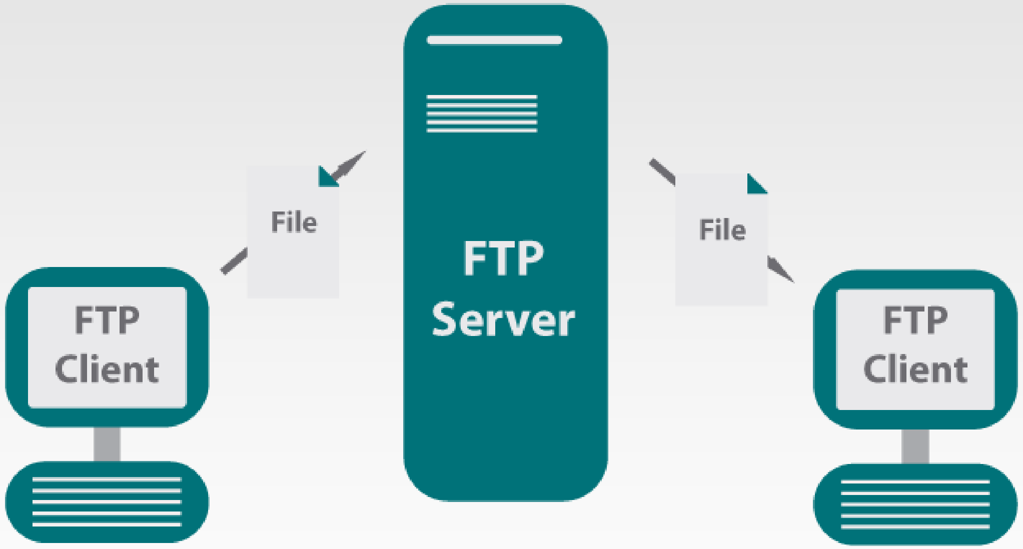
- **Telnet (TCP 23)**
  - □ It is used to remotely access a machine on the network.
  - □ A Telnet server can use software (known as a Telnet client) to access the command line interface (CLI) of another remote machine running the program.
  - □ It is not recommended to use because data, username and passwords are sent in plain text.

SSH (TCP 22)

- **Secure Shell**
  - It is used to remotely access a machine on the Internet.
  - Public Key and private key pair are used
  - Unlike telnet, data transmission is sent by encrypted username-password. Therefore, it is more secure.
  - It is widely used in the industry for remote CLI access and server management.

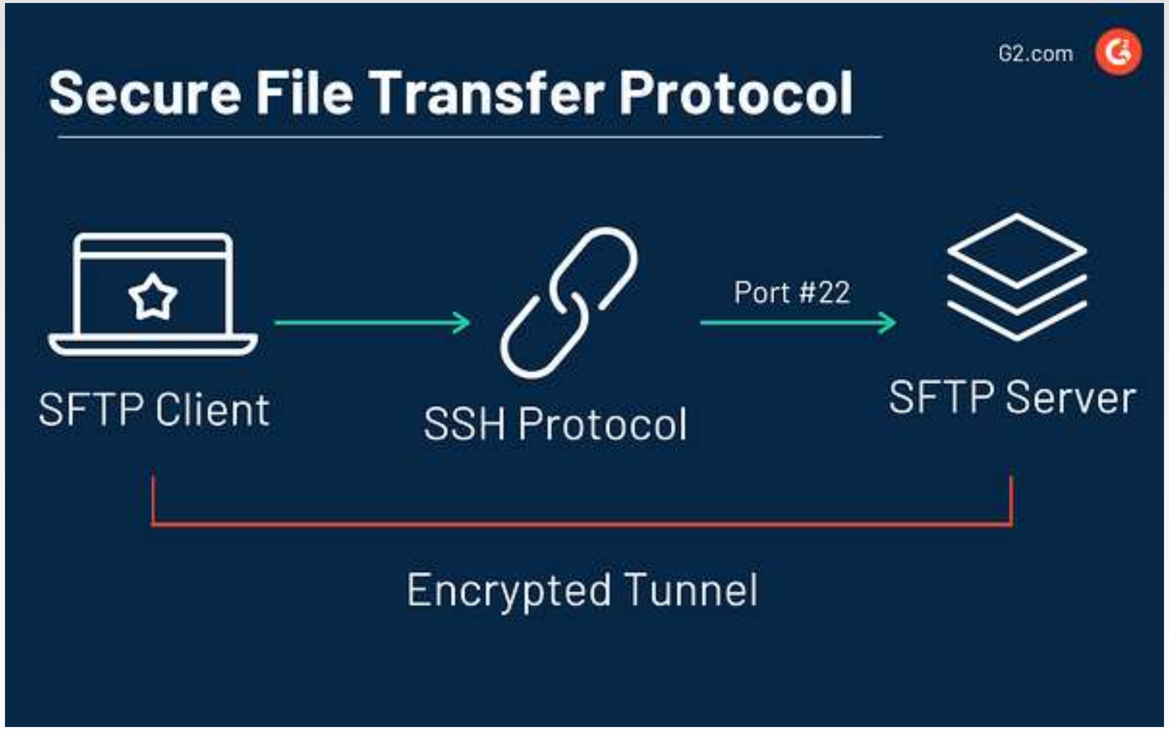


FTP(TCP 20-21)



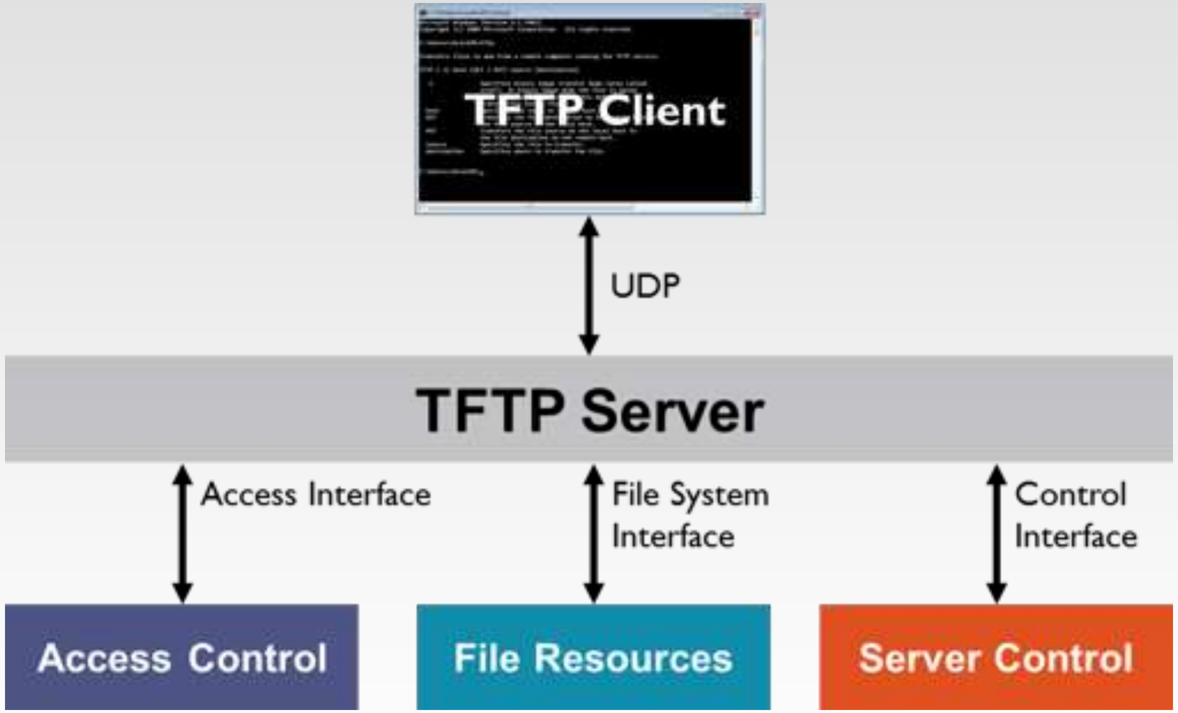
- **File Transfer Protocol**
- FTP is one of the first developed internet protocols. Uses TCP service.
- With FTP protocol;
- File transfer is done from one computer to another computer.
- With the help of a series of commands provided with the protocol, file sending/receiving operations are performed between two computers.

SFTP(TCP 22)



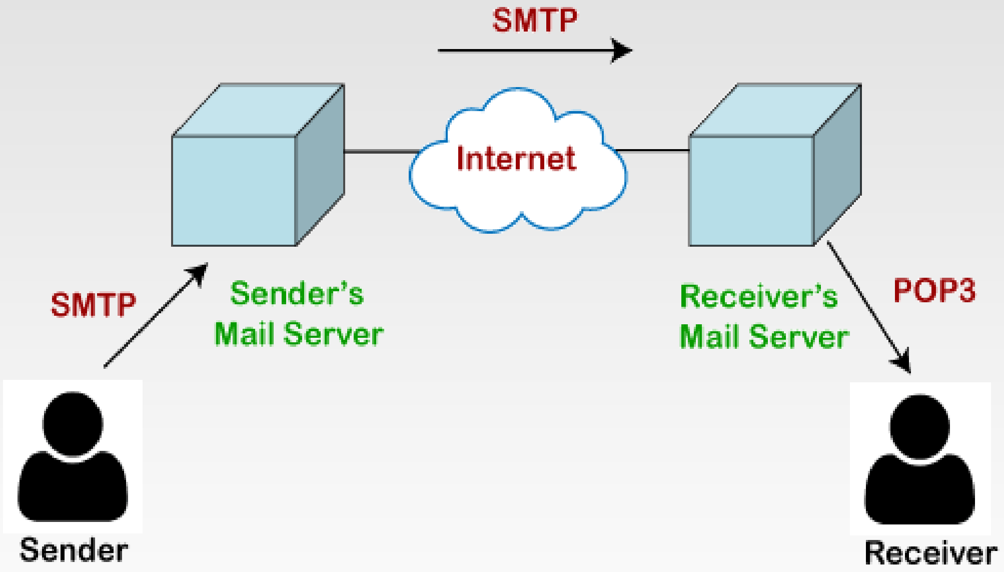
- **Secure File Transfer Protocol**
- Unlike FTP, SSH infrastructure and commands are used.
- It is more reliable.
- File transfer from one computer to another computer
- Public Key and private key pair are used

TFTP(UDP 69)



- **Trivial File Transfer Protocol**
- The TFTP protocol only supports simple file sending and receiving.
- File deletion, moving and renaming are not supported.
- It is fast.

POPv3 (TCP 110)



- □ **Post Office Protocol**
- □ It allows us to download, delete and read incoming mails from the server.
- □ Latest version is 3

IMAP (TCP 143/993)

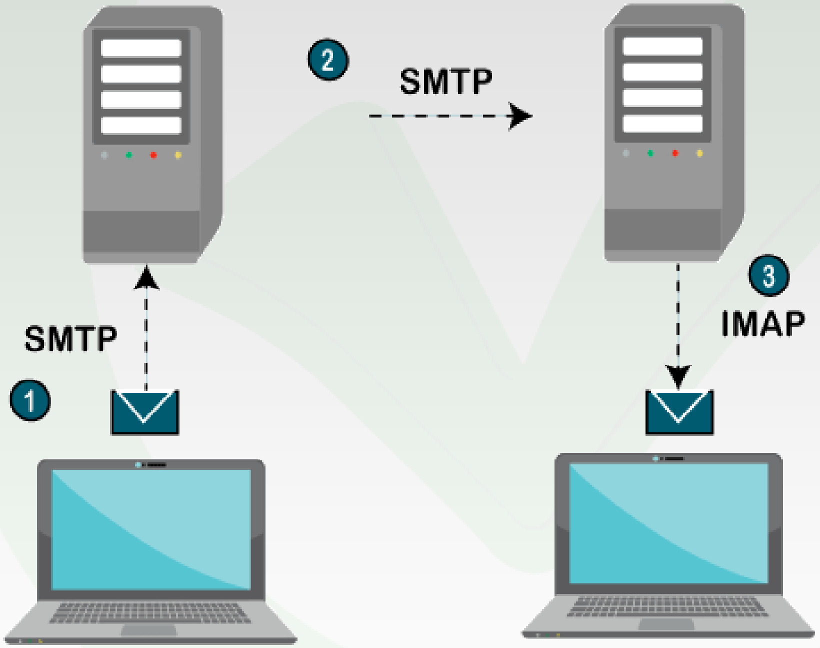
- **Internet Message Access Protocol**

□ Download, read, delete, mark as read, spam, create folder

□ Sync with all devices

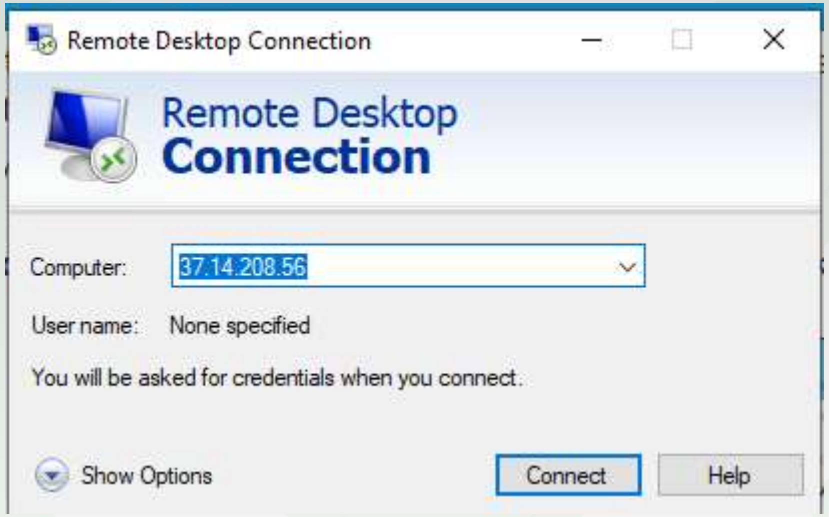
□ Port 143: Non-encrypted IMAP port

□ Port 993: IMAP encrypted



RDP (TCP 3389)

- **Remote Desktop Protocol**
  - □ It is a proprietary protocol developed by Microsoft that provides a graphical interface for connecting to a computer.
  - □ While the user is using the RDP client software for this purpose, the other computer must be running the RDP server software.
- **Windows** - **mstsc.exe**
- **Linux - Remmina**

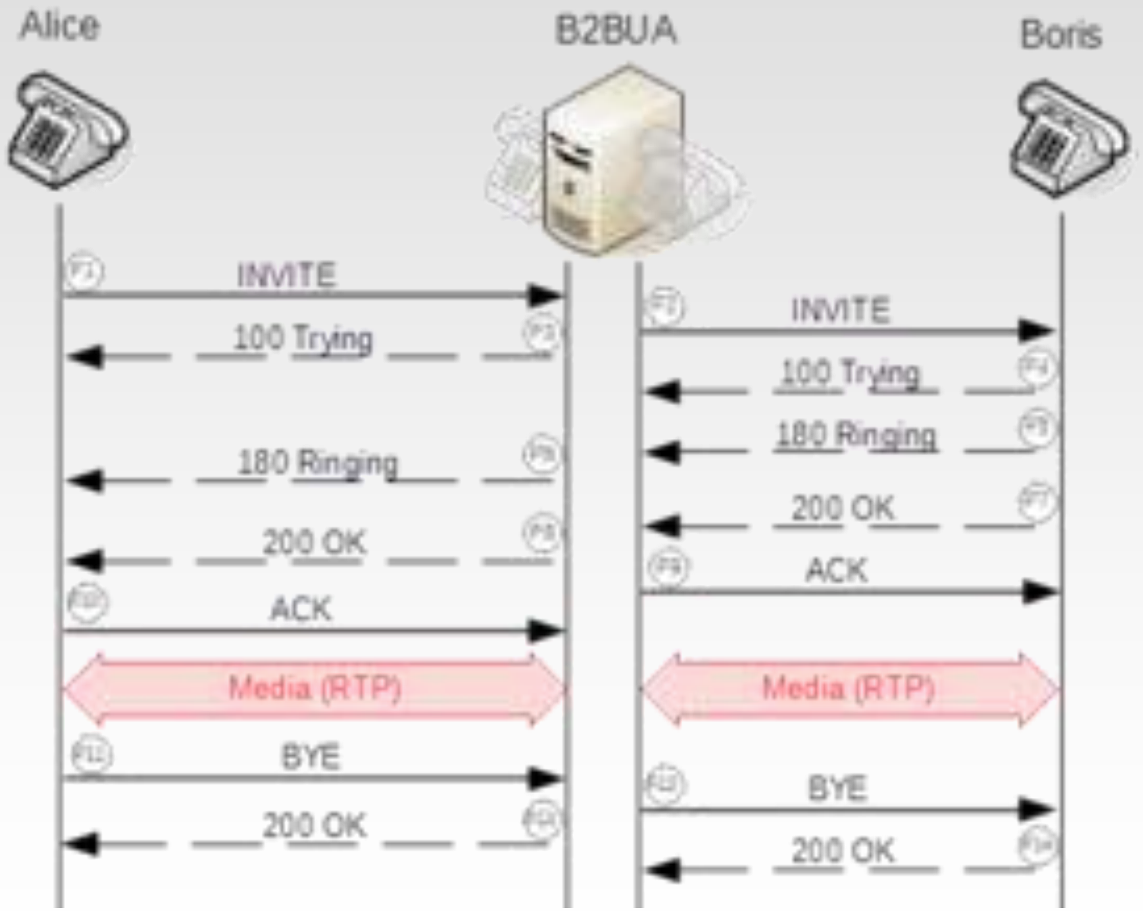


Computer: 37.14.208.56

User name: None specified

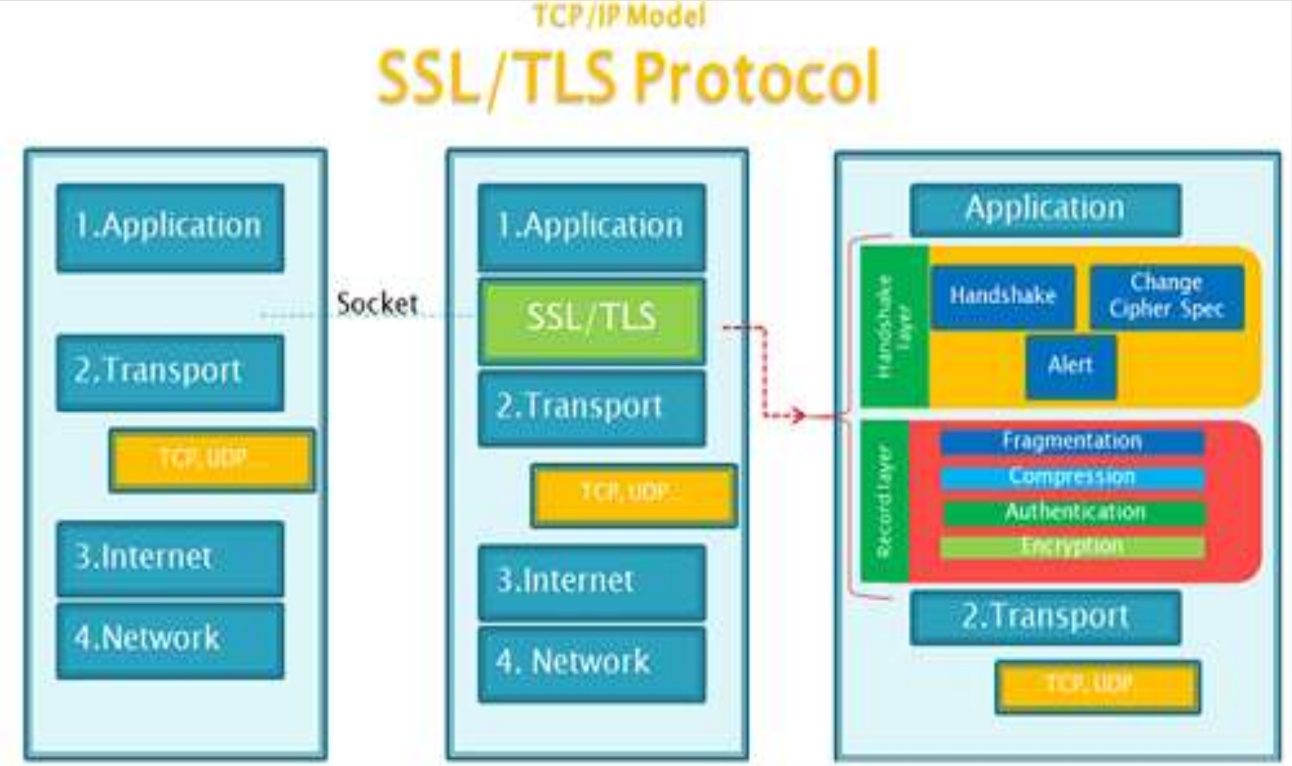
You will be asked for credentials when you connect.

SIP (VoIP) (UDP-TCP 5060/5061)



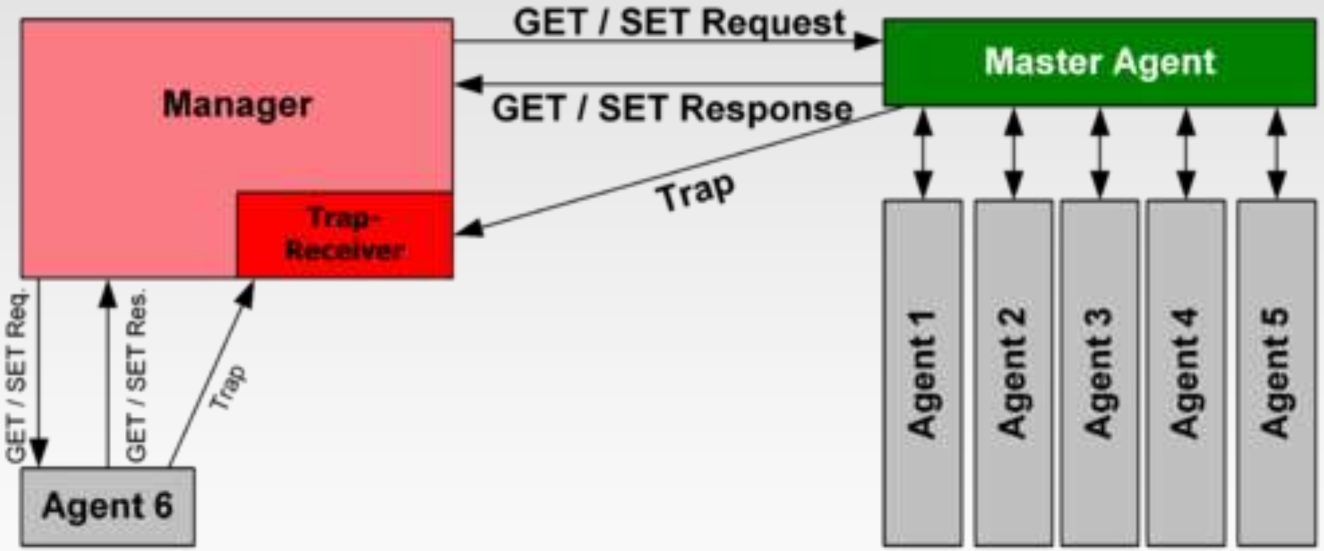
- **Session Initiation Protocol**
- Port 5060 is usually used for unencrypted signaling traffic.
- Port 5061 is typically used for Transport Layer Security (TLS) encrypted traffic.
- Used to start, maintain and end real-time sessions with audio, video and messaging applications.

TLS / SSL (TCP 995 / 465)



- **Transport Layer Security and Secure Sockets Layer**
  - Cryptographic protocols designed to provide communication security over a computer network.
  - V1.3SSL Netscape company has produced its own original SSL certificate.

SNMP (UDP 161 / TCP 25)



- **Simple Network Management Protocol**

□ Protocol for collecting and editing information about managed devices in IP networks and modifying this information to change device behavior.

□ NICs, cable modems, routers, switches, servers, workstations, printers, and more

HTTP (TCP 80) HTTPS (TCP 443)

The Hypertext Transfer Protocol **(HTTP)** is the foundation of the World Wide Web, and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack.

Hypertext Transfer Protocol secure **(HTTPS)** is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer.

LDAP (TCP 389) - NTP (UDP 123)

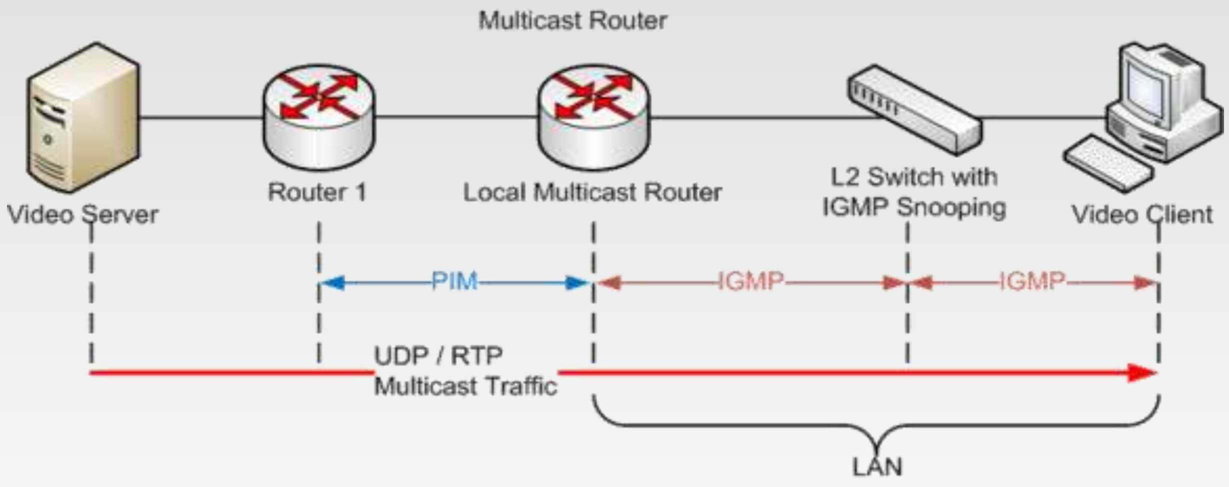
Lightweight Directory Access Protocol (LDAP)

- Directory services play an important role in the development of intranet and Internet applications by allowing the sharing of information about users, systems, networks, services and applications throughout the network.
- For example, directory services can provide any organized set of records, often with a hierarchical structure, such as a corporate email directory.

Network Time Protocol (NTP)

- It is used for clock synchronization between computer systems on the network.

IGMP



Internet Group Management Protocol (IGMP)

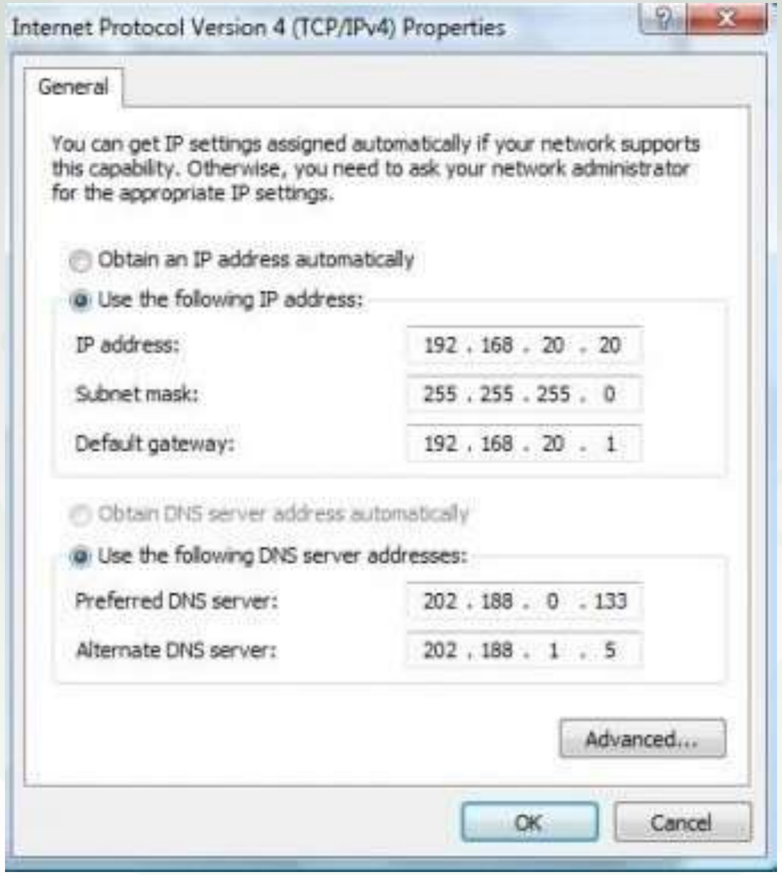
- IGMP is an integral part of IP multicast, allowing the network to route multicast transmissions only to the hosts that request them.
- IGMP can be used for one-to-many network applications such as online video streaming and gaming, allowing for more efficient use of resources while supporting such applications.

DHCP (UDP 67/68)

Dynamic Host Configuration Protocol **(DHCP)** is a network management protocol used on Internet Protocol (IP) local area networks. A DHCP server must be present on the network. A device connected to the network requests an IP address from the DHCP server using the DHCP protocol; the server assigns a unique address to the device, identifying it for TCP/IP communication, and supplies other network configuration parameters.

In the absence of a DHCP server, a device that needs an IP address must be manually assigned a static address by a network administrator, or must assign itself an **APIPA** address (which will not enable it to communicate outside its local subnet).

A device configured to use dynamic (DHCP) addressing that is connected to a different network will be assigned an address on that network without needing to be reconfigured. However if the address of a device must be known—for example, a printer which processes print jobs sent to its IP address—a known static address is required.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 20 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 20 . 1

○ Obtain DNS server address automatically

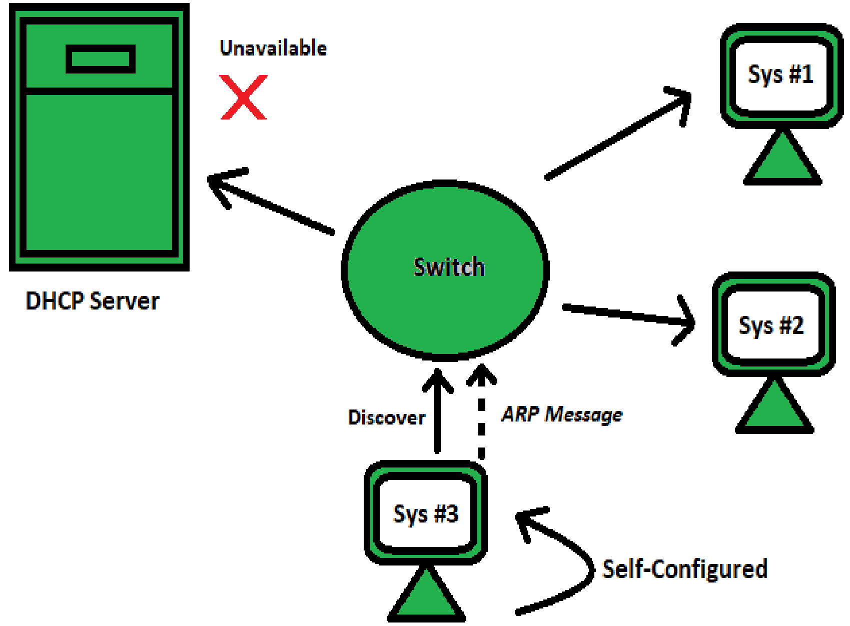
● Use the following DNS server addresses:

Preferred DNS server: 202 . 188 . 0 . 133

Alternate DNS server: 202 . 188 . 1 . 5

APIPA Automatic Private IP Addressing

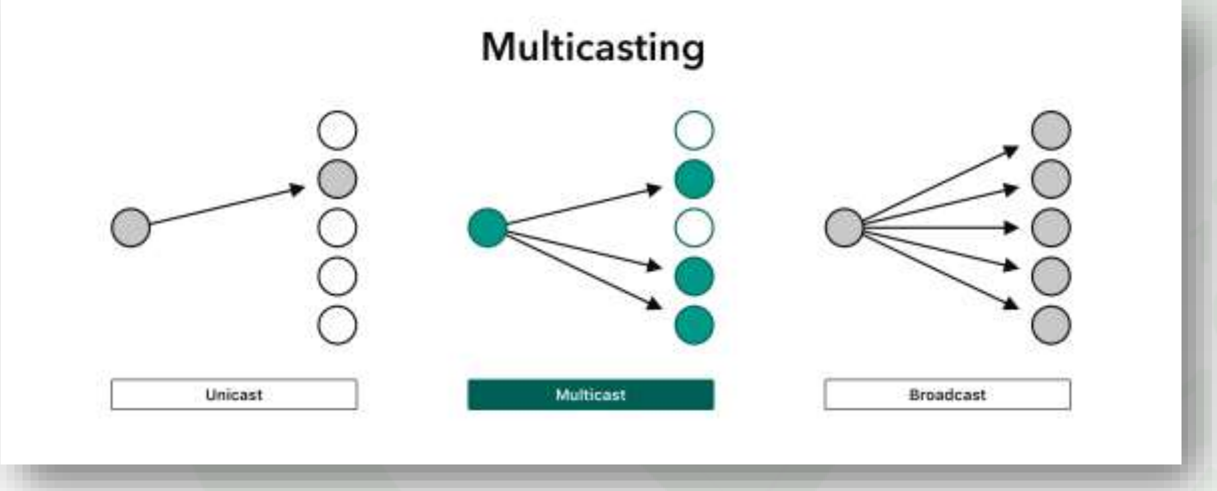
- □ **Characteristics**
- Communication can be established properly if not getting response from DHCP Server.
- APIPA regulates the service, by which always checking response and status of the main DHCP server in a specific period of time.
- □ **Advantages**
- It can be used as a backup of DHCP because when DHCP stops working then APIPA has the ability to assign IP to the networking hosts.
- It stops unwanted broadcasting.
- It uses ARP(Address Resolution Protocol) to confirm the address isn't currently in use.
- □ **Disadvantages**
- APIPA IP addresses can slow your network.
- APIPA does not provide network gateway as DHCP does.
- □ **Limitations**
- APIPA addresses are restricted for use in local area network.
- APIPA configured devices follow the peer to peer communication rule.



IPv4 link-local addresses are assigned from address block ***169.254***.*0.0/16* (*169.254.0.0* through *169.254.255.255*).

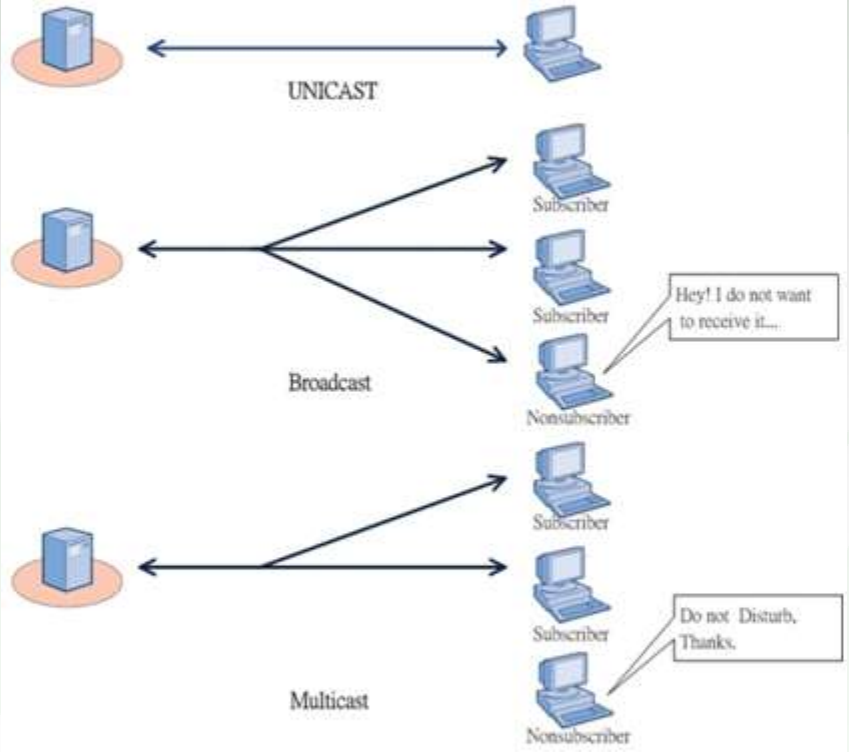
Network Transmission Types

- **Unicast**
  - 1 sender and 1 receiver
  - Destination NIC MAC address
  - Pinging a specific computer
  - Browsing a web site
- **Multicast**
  - A sender and a group of receivers–Sales Department
  - Destination NIC MAC address but a part of a group
  - Send e-mail to mailing list
  - Sending programs to only subscribers of a TV channel



Network Transmission Types

- **Broadcast**
  - Sender to all of the devices on the network
  - Destination NIC MAC ff:ff:ff:ff:ff:ff
  - The radio station broadcast
  - Twitter, open to everyone



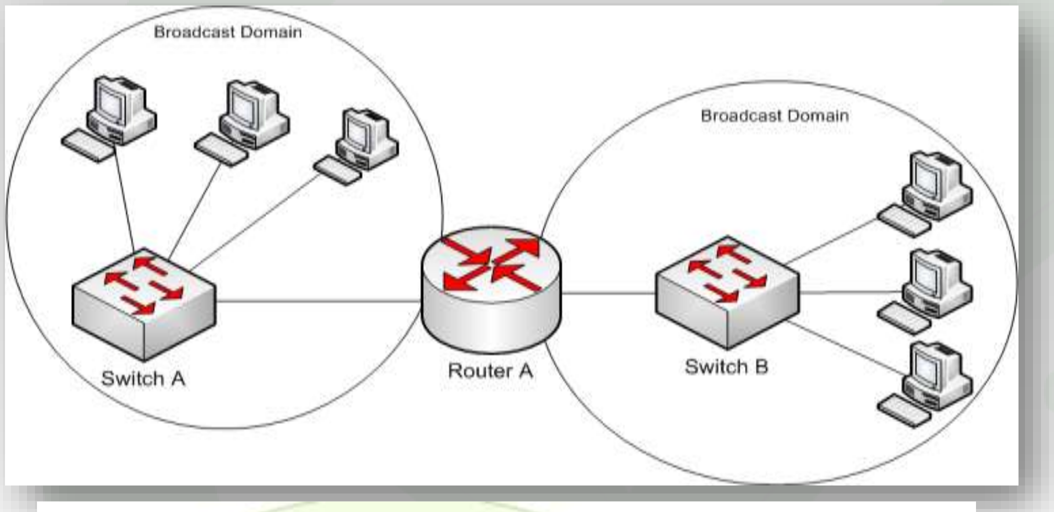
Broadcast Domain & Collision Domain

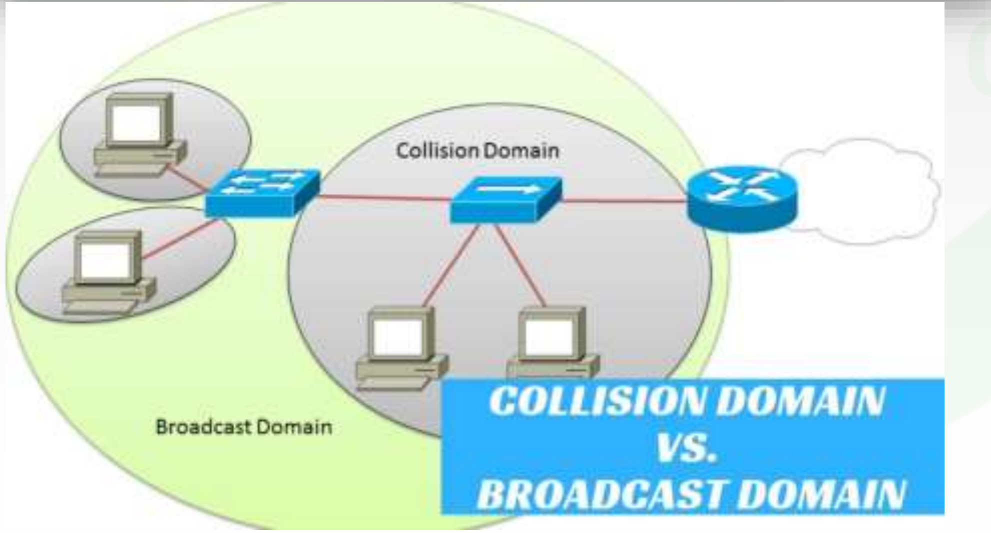
- **Broadcast Domain**

  A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments.

- **Collision Domain**

  A collision domain is, as the name implies, the part of a network where packets collide when two devices send a packet at the same time on the shared network segment. The packets collide and they must send the packets again, which reduces network efficiency. This is often in a hub environment, because each port on a hub is in the same collision domain. By contrast, each port on a bridge, a switch or a router is in a separate collision domain.

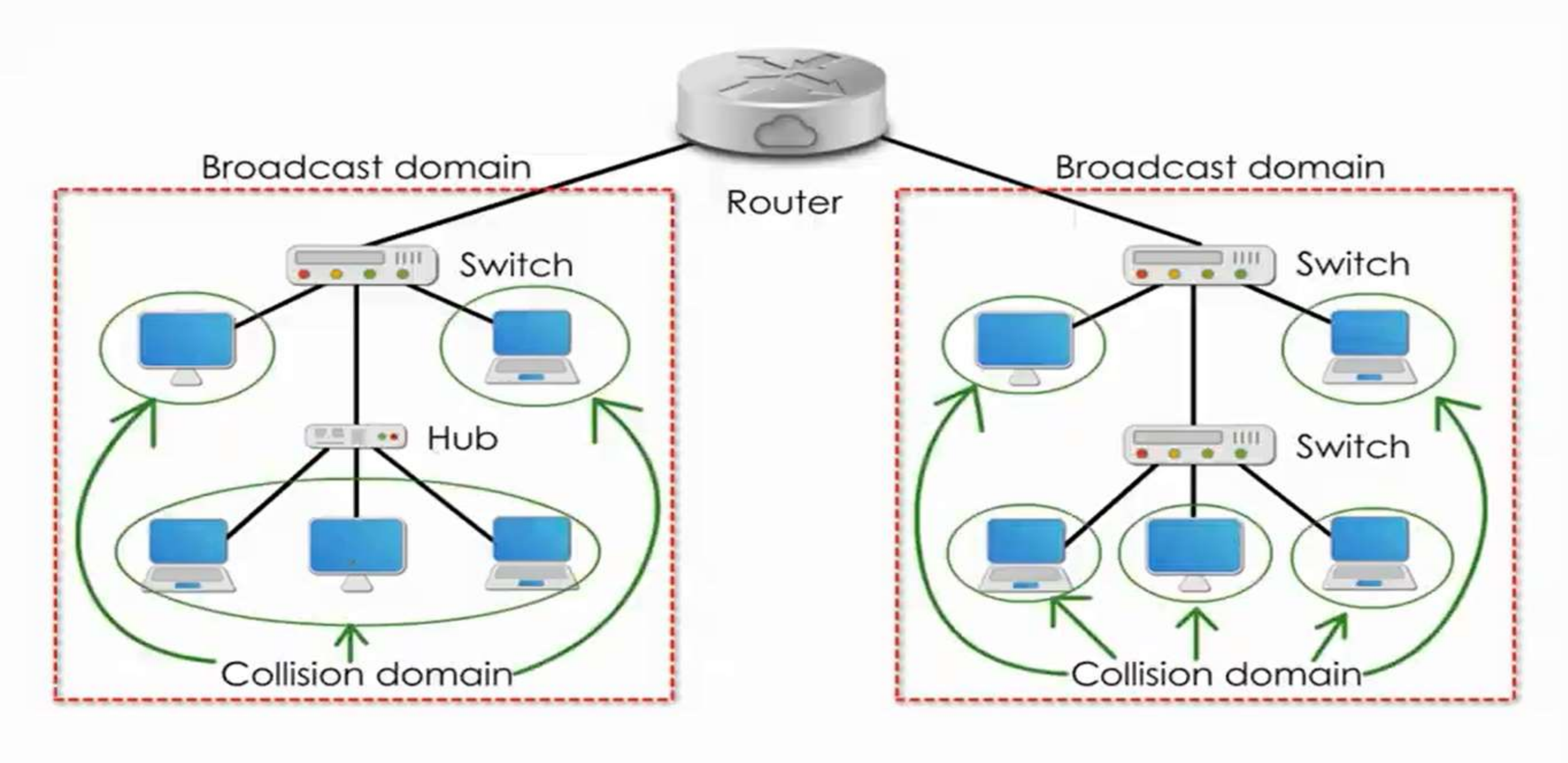




Broadcast Domain & Collision Domain

- Network elements such as Switch, Router and Bridge prevent collisions.

- Hubs can create collision domains.

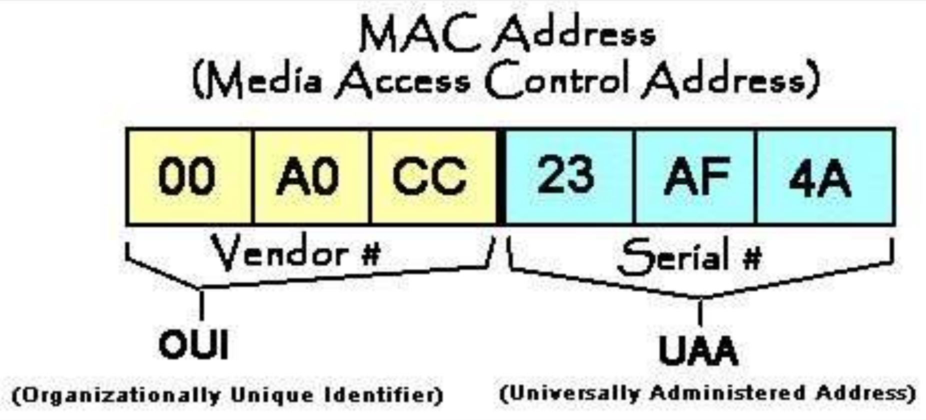


MAC Address

- MAC address distributions are managed by the IEEE.
- Data Link Layer address
- Since MAC is a 48-bit (6 bytes) address, it can be used to identify 2^{48} = 281,474,976,710,656 different network cards.
- MAC address (Physical address, Hardware address) provides identification of network hardware.
- The MAC address is an information encoded by the manufacturer to the computer's ethernet card. Manufacturers buy MAC address ranges.
- MAC is used to transfer frames between units that are physically connected to each other in the same network.

MAC Adres

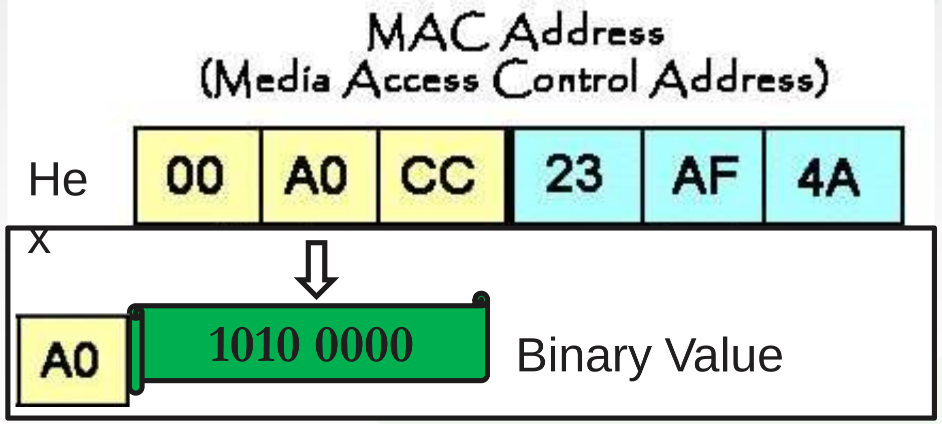
- **48 bit MAC**
  - Recorded in **NIC’s ROM**, can be changed programmatically.



MAC Address
(Media Access Control Address)

00	A0	CC	23	AF	4A

Vendor #
Serial #
OUI
(Organizationally Unique Identifier)
UAA
(Universally Administered Address)

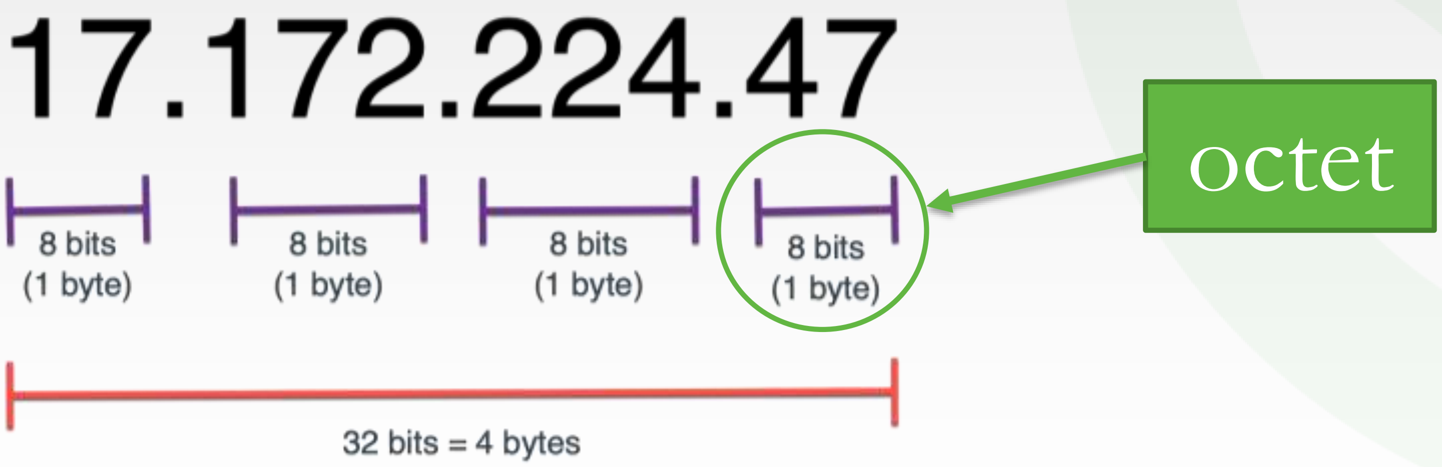


MAC Address
(Media Access Control Address)

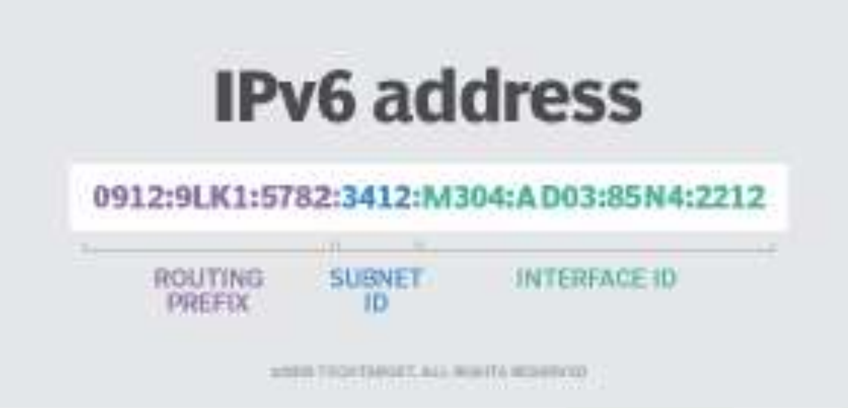
00	A0	CC	23	AF	4A

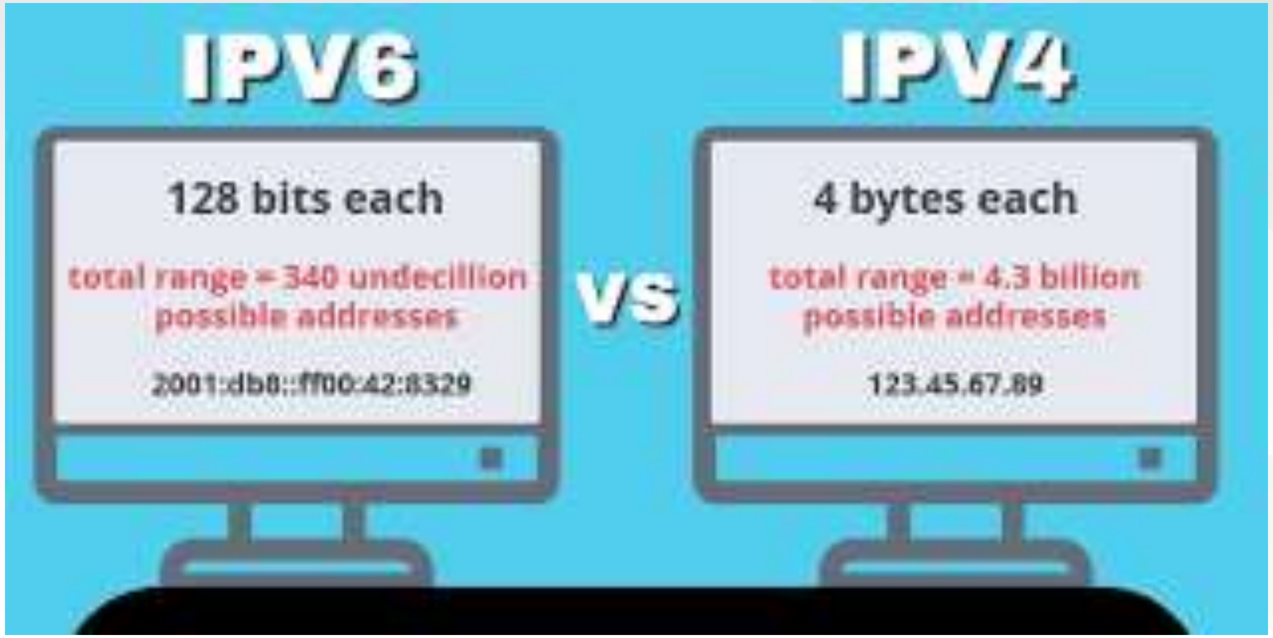
IP Address

- IP address:
  - Network Layer address
  - Used to send data packets
  - **32-bit** → **17.172.224.47 (IPv.4)**

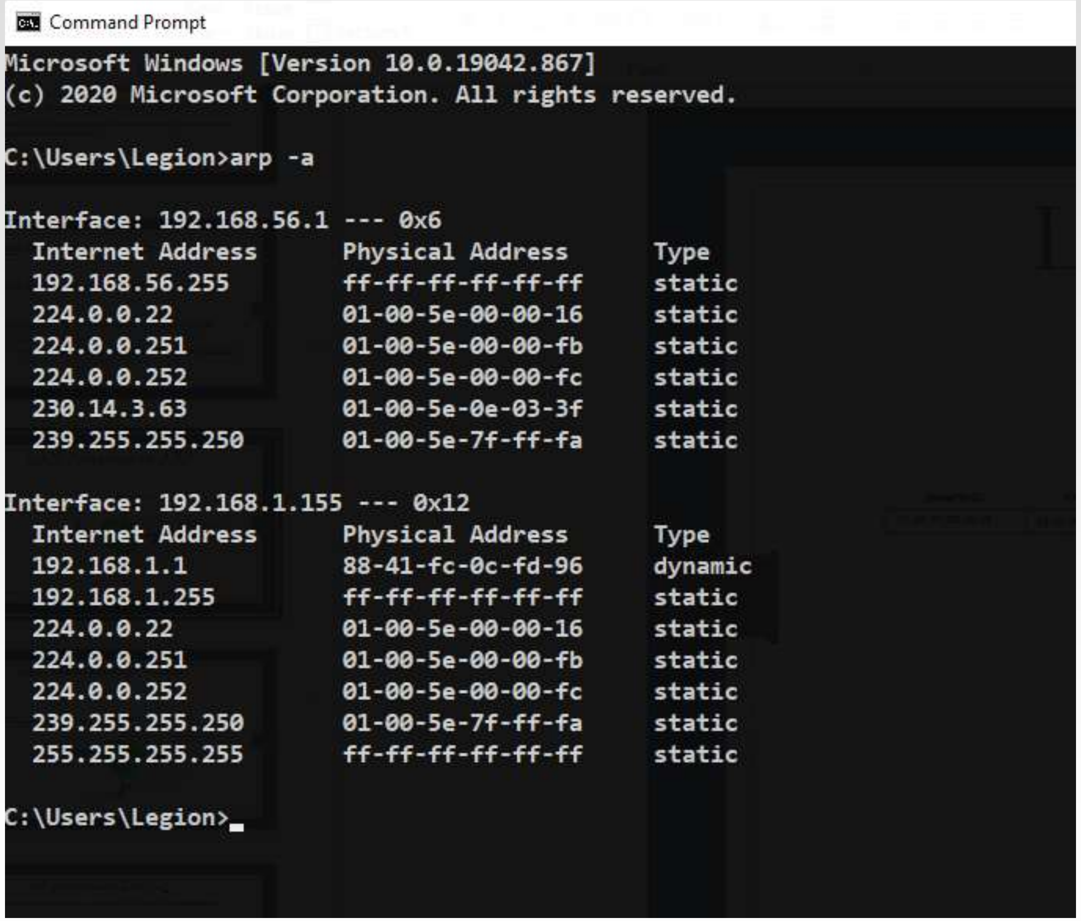


IP Address


IPv6 address
0912:9LK1:5782:3412:M304:AD03:85N4:2212
ROUTING PREFIX
SUBNET ID
INTERFACE ID
©2020 TECHTARGET. ALL RIGHTS RESERVED


IPV6
128 bits each
total range = 340 undecillion possible addresses
2001:db8::ff00:42:8329
VS
IPV4
4 bytes each
total range = 4.3 billion possible addresses
123.45.67.89

ARP - Address Resolution Protocol

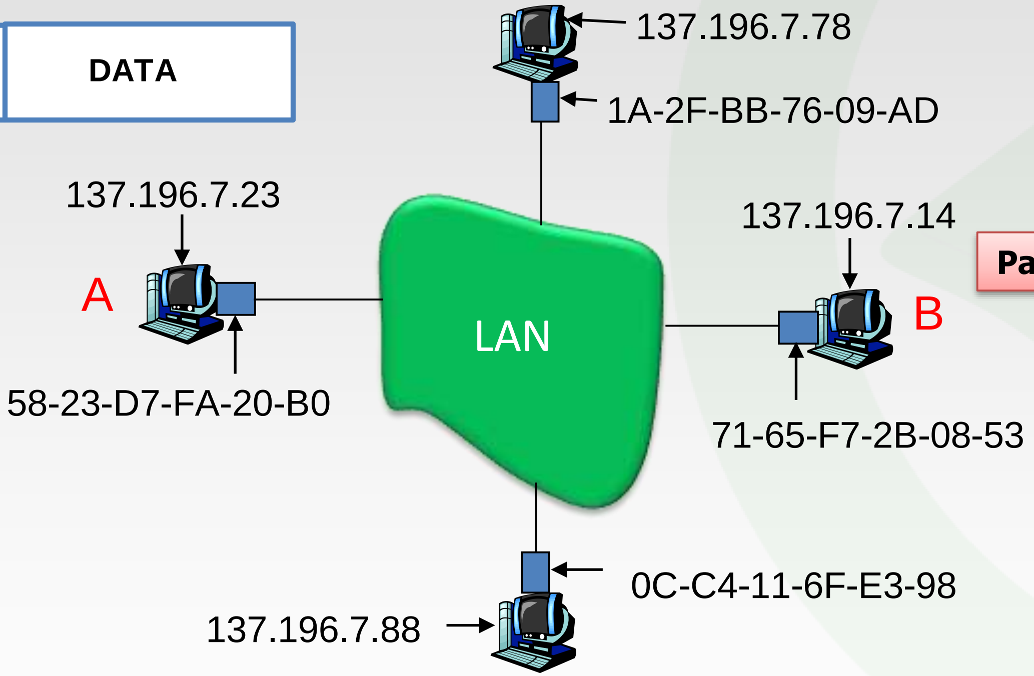


```
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Legion>arp -a

Interface: 192.168.56.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  230.14.3.63           01-00-5e-0e-03-3f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.155 --- 0x12
  Internet Address      Physical Address      Type
  192.168.1.1           88-41-fc-0c-fd-96     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Legion>_
```

- Ip - MAC table
- arp -a

LAN and ARP

Receiver MAC	Sender MAC	
71-65-F7-2B-08-53	58-23-D7-FA-20-B0	DATA



Paket Bana geldi

Every device on a LAN has a MAC address.

ARP: The same LAN

- A wants to send packets to B. But B's MAC is not in A's ARP table.
- A broadcasts an ARP query packet containing B's IP address.
- Destination MAC address = FF-FF-FF-FF-FF-FF
- All nodes in the LAN receive the ARP query. (Broadcast)
- B receives the ARP packet and sends the reply packet containing its MAC (Unicast- only 1 sender and only 1 receiver)
- A keeps the IP and MAC address pair until it expires.
- Unrefreshed information expires. (TTL-time to live)

Packet
Source:A   Destination:B

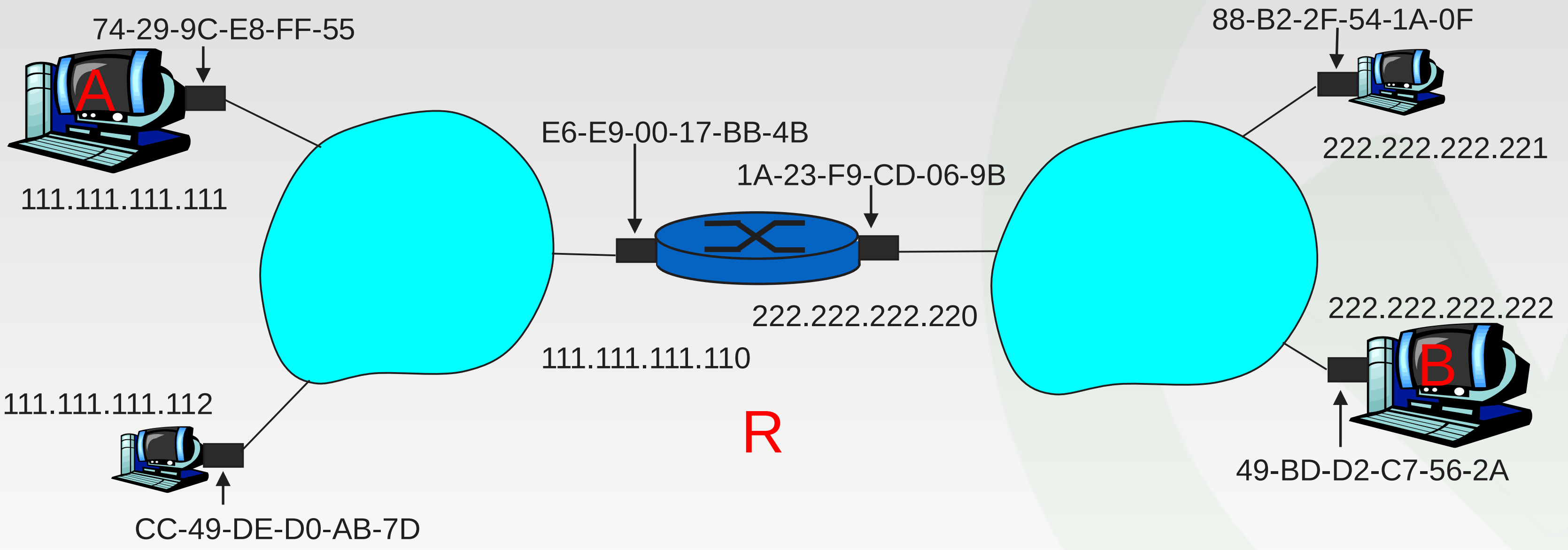
ARP query to find out MAC of B

ARP query is broadcast, all devices receive

Only B sends reply to ARP packet containing MAC

A records Ip and MAC of B along with TTL

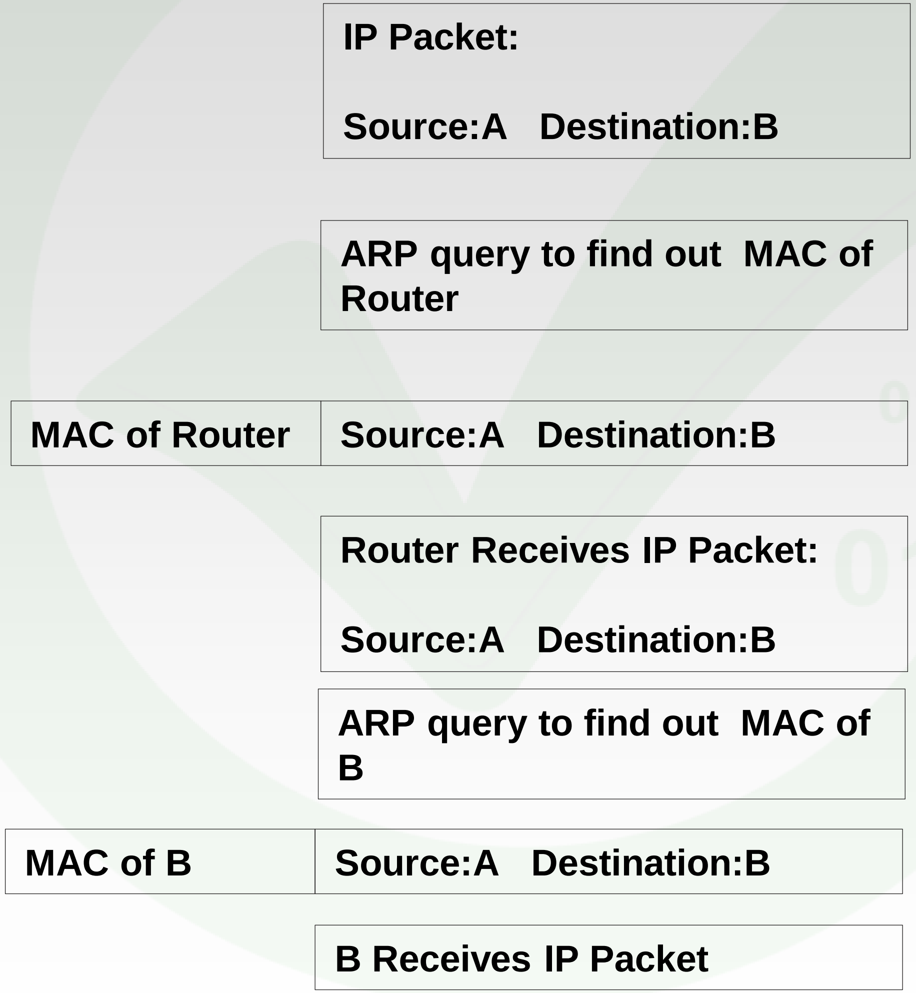
Routing



- It is desired to send Packets from A to B over R and it is assumed that A knows B's IP address.
- R Router has ARP table for each IP network.

Routing

- A creates an IP packet with source A and destination B.
- A uses ARP for the MAC of R, whose IP is 111.111.111.110.
- A targeting R's MAC, Prepares the frame containing the A-to-B IP datagram.
- A sends the frame and R receives it.
- R extracts the IP packet from the Frame and knows that the packet will go to B.
- R uses ARP to find out B's MAC address.
- R frames and sends the A-to-B IP packet destined for B.



IP Packet:

Source:A Destination:B

ARP query to find out MAC of Router

MAC of Router | Source:A Destination:B

Router Receives IP Packet:

Source:A Destination:B

ARP query to find out MAC of B

MAC of B | Source:A Destination:B

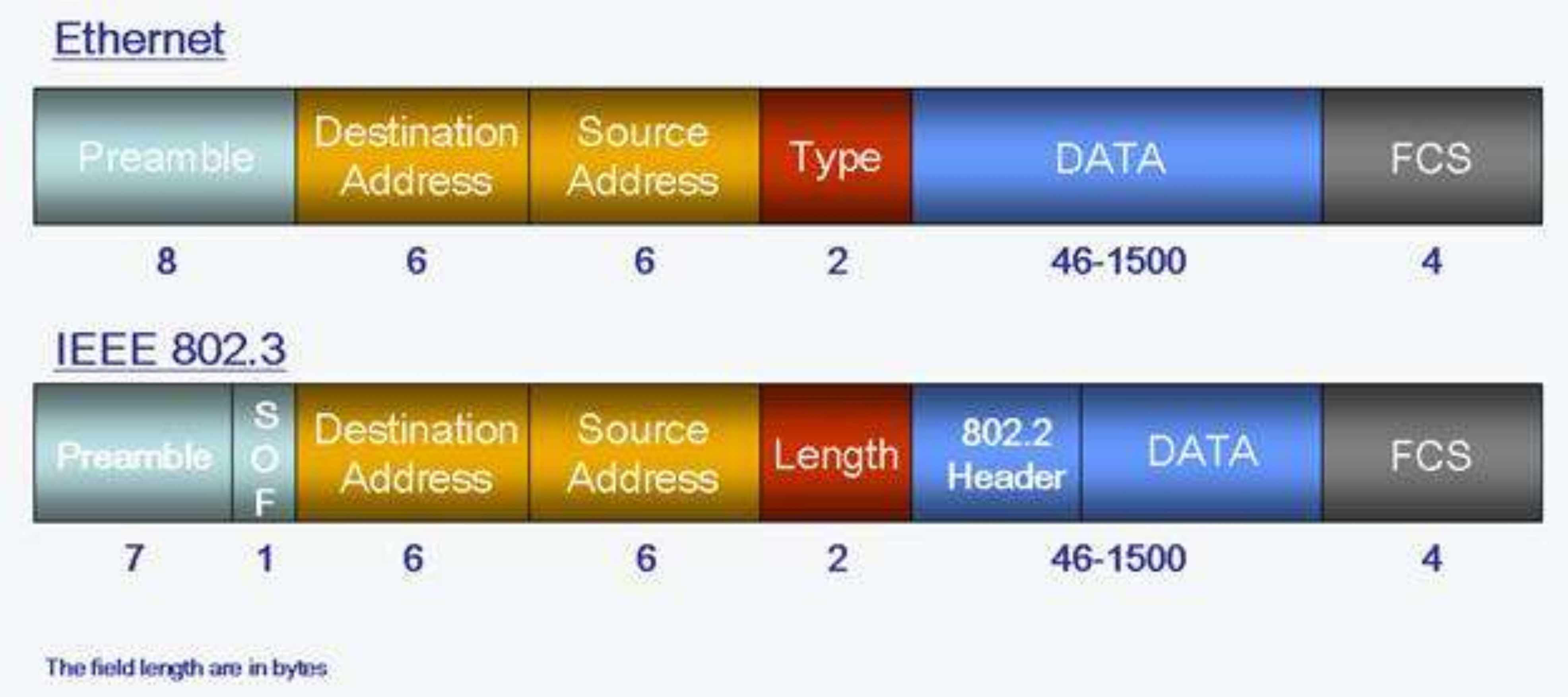
B Receives IP Packet

Ethernet

- In the 1980s, the Wired LAN standard was developed by IEEE and this standard was named 802.3
- It determines how and in what format the machines on a network will communicate.
- Speed: Between 10 Mbps – 10 Gbps
- It works on Data Link and Physical Layer.

  - CSMA/CD –
  - Carrier Sense Multiple Access / Collision Detection
    - Collision – Reduces network efficiency
    - In case of collision frames are sent again

Ethernet Frame Structure



Ethernet

Preamble	Destination Address	Source Address	Type	DATA	FCS
8	6	6	2	46-1500	4

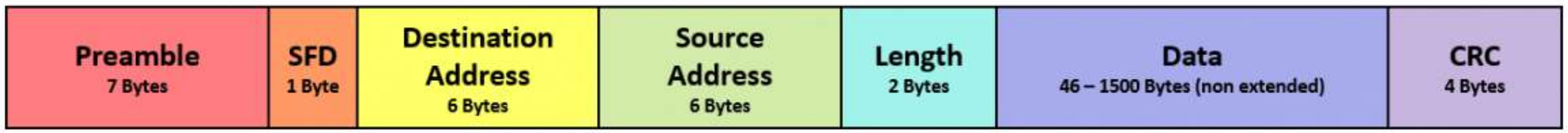
IEEE 802.3

Preamble	SOF	Destination Address	Source Address	Length	802.2 Header	DATA	FCS
7	1	6	6	2	46-1500		4

The field length are in bytes

Ethernet Frame Structure

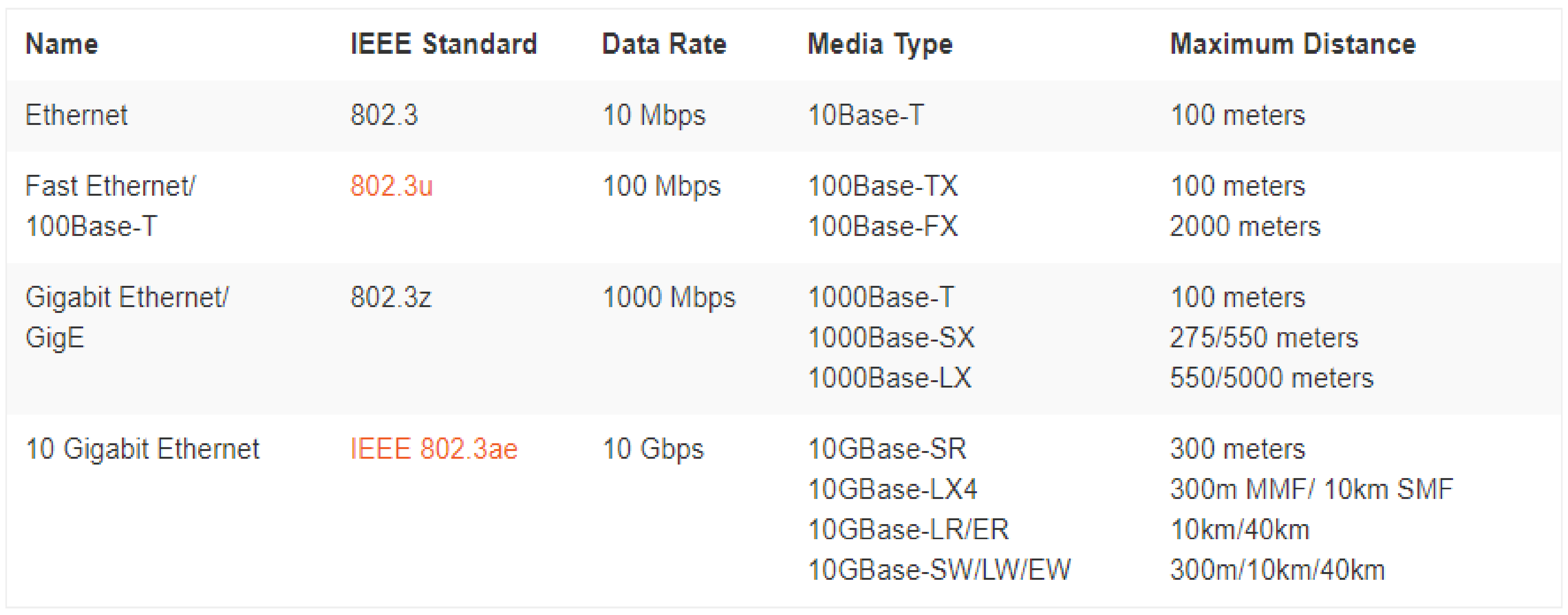
- The ethernet card (NIC) of the sending node embeds the IP+Datagram in the Ethernet frame.
- Preamble - 7 bits, Synchronizes timing between sender/receiver
- SFD: 1 byte, warns that is the last chance for synchronization
- Addresses: 6 byte or 48 bit mac address
- MAC addresses of the sending node and the receiving node
- Length: Length of entire frame
- CRC: Code for error checking



Preamble 7 Bytes	SFD 1 Byte	Destination Address 6 Bytes	Source Address 6 Bytes	Length 2 Bytes	Data 46 – 1500 Bytes (non extended)	CRC 4 Bytes

Ethernet Frame Format

Ethernet



Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Terms

Broadcast
Unicast
Multicast
MAC Address
IP v4
IP v6

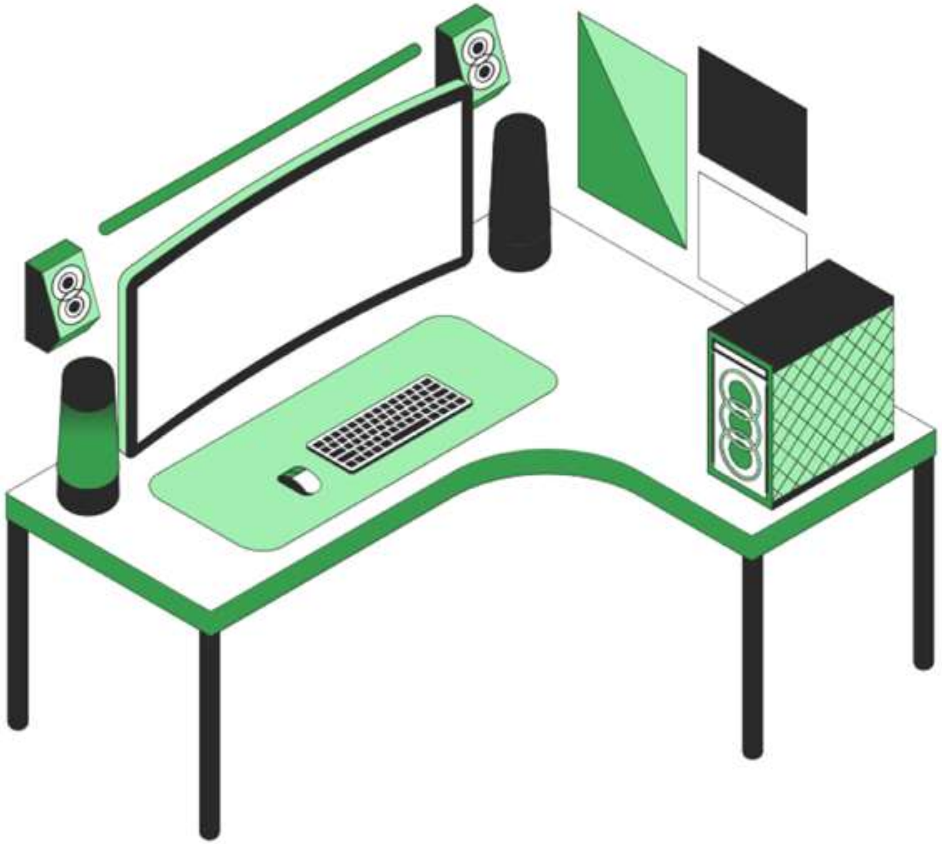
İpconfig
Ping

Broadcast Domain
Collision Domain

RDP

Binary
Hexadecimal

Bit
Byte
Kilobyte
Megabyte
Gigabyte
Terabyte



Do you have any questions?

Send it to us! We hope you learned something new.