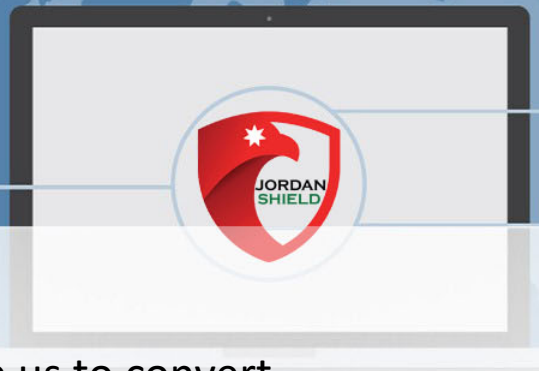
CSC – Jordan Shield Special Edition

Powered By : Mohammed Kher Al-Khawaldeh.

Cryptography

- Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Hashing

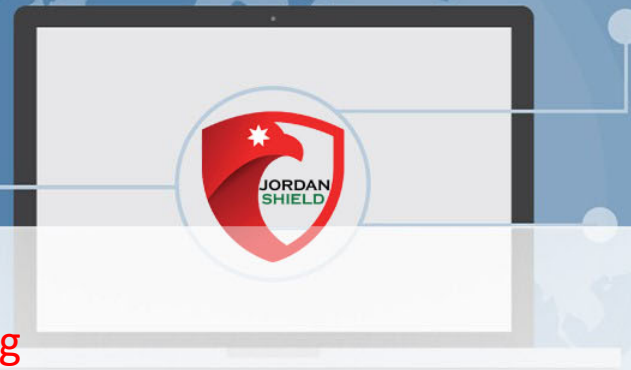


Hash : Irreversible mathematical code that help us to convert [User-Input] to fixed Length Output .

Examples on Hashes : MD5 , SHA-1 , SHA256 , SHA512 etc…

Its Called By [One – Way – Function]

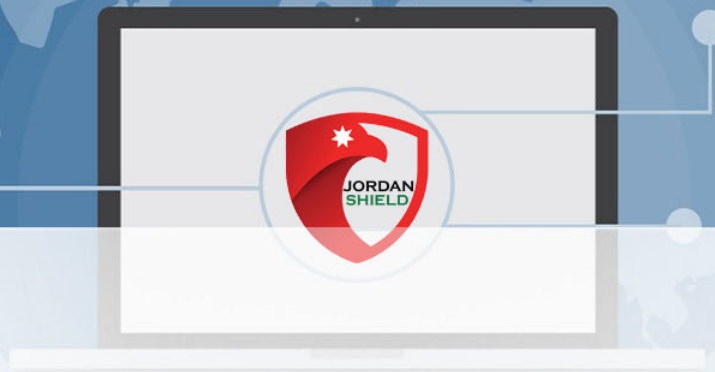
Encoding



Encoding : Encoding is the process of converting data from one to another.

Examples : Base64 , URL , HTML , Octal , ASCII , HEX , rot13 etc…

Encrypting



Encryption Types :

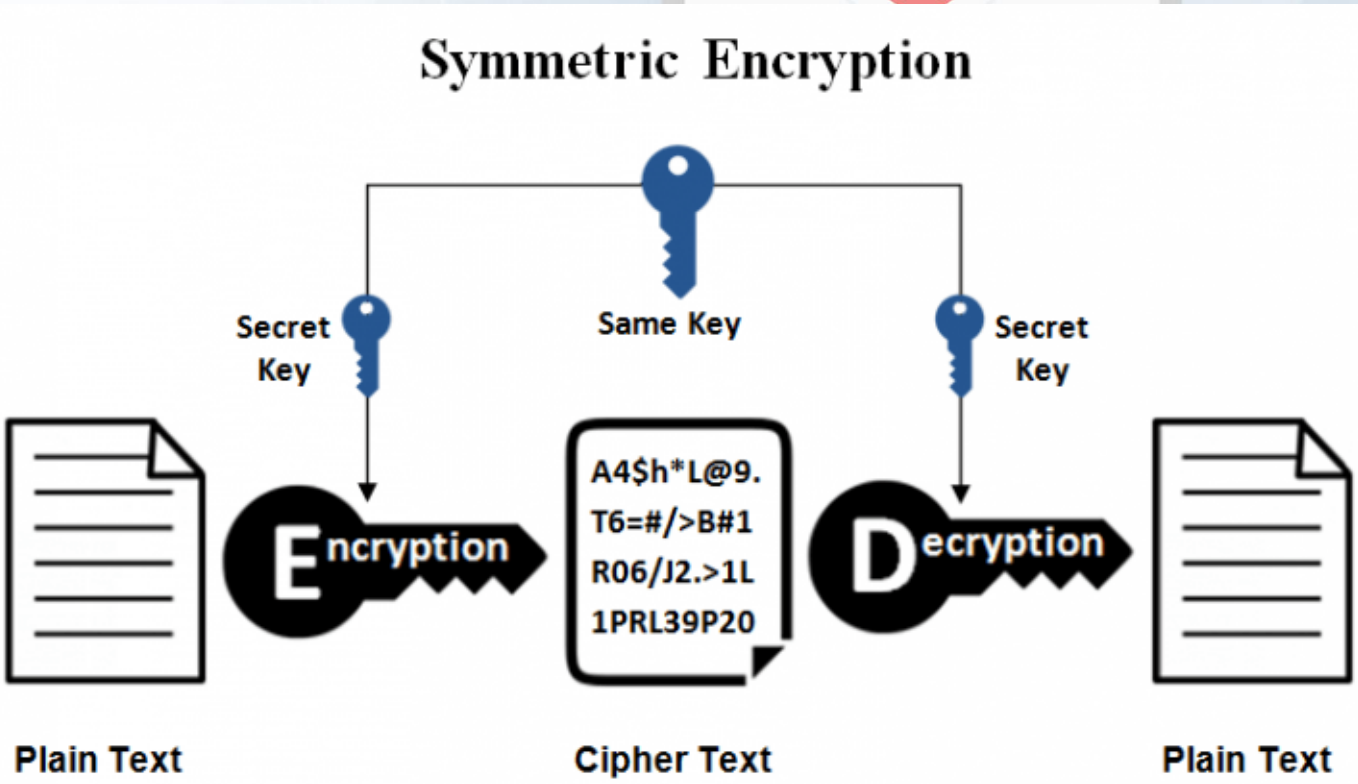
Symmetric Encryption

- Same Key E&D

Asymmetric Encryption

- Deferent Key E&D

Encrypting

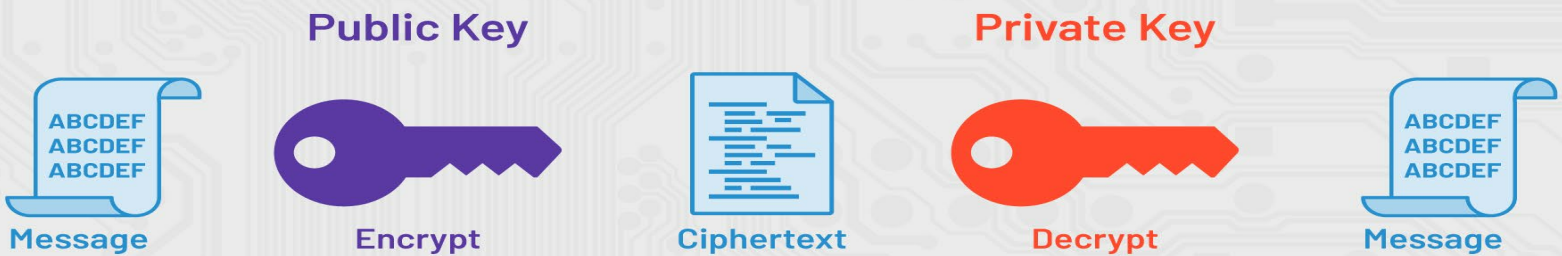

Symmetric Encryption
Secret Key
Same Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

Encrypting

Encrypting

Symmetric Encryption

Asymmetric Encryption



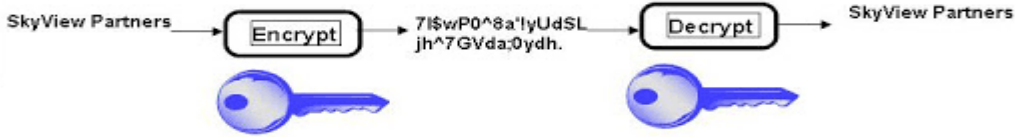
Encrypting

Types of Encryption

DES
TripleDES
AES
RC5

Symmetric Keys

- Encryption and decryption use the **same key**.



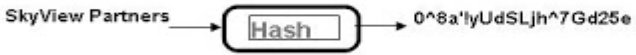
RSA
Elliptic Curve

Asymmetric keys

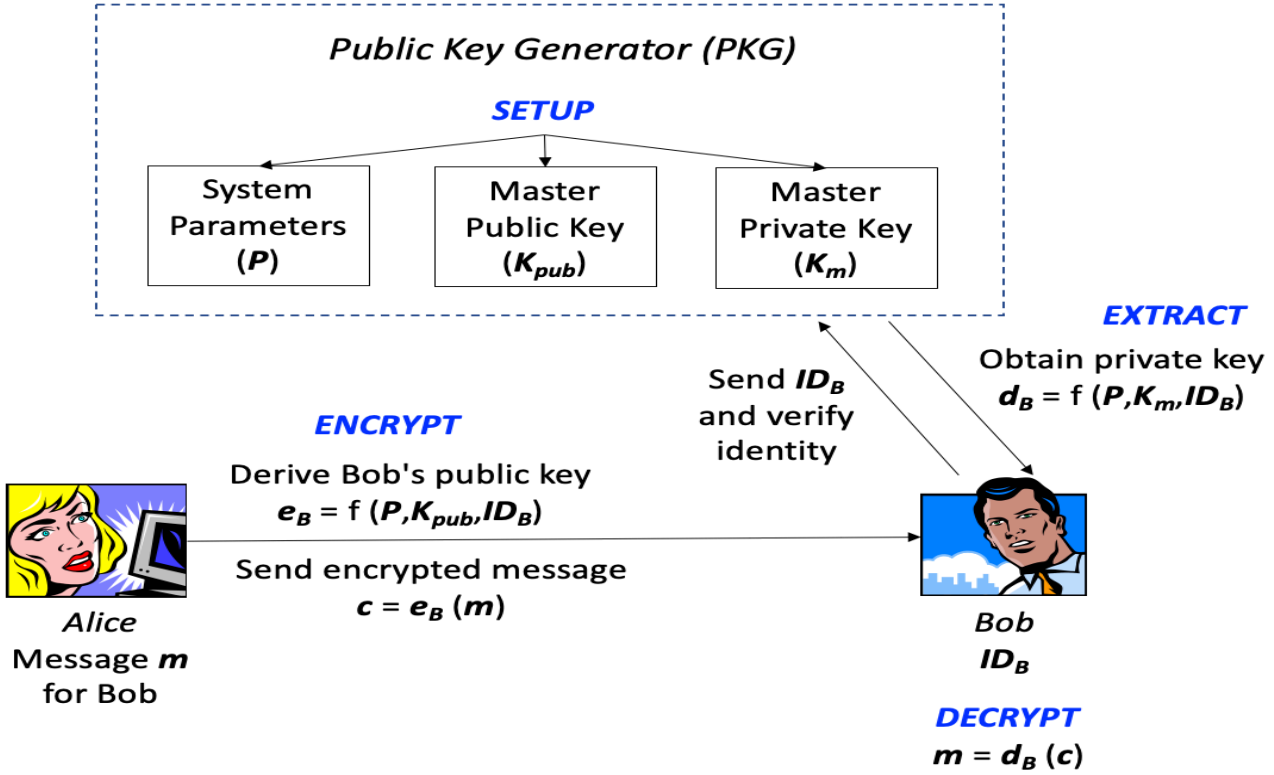
- Encryption and decryption use different keys, a **public key** and a **private key**.

MD5
SHA-1

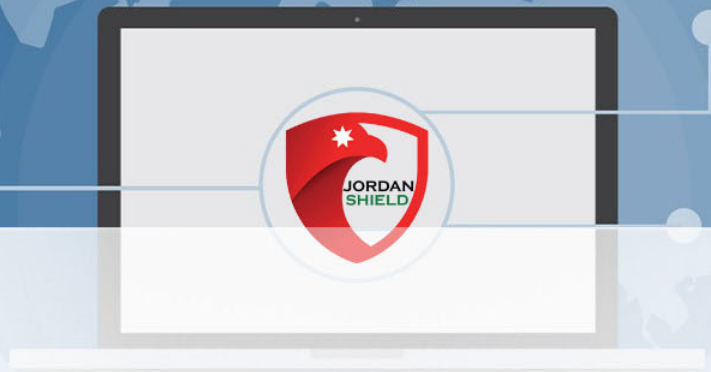
One-way hash



Encrypting


Public Key Generator (PKG)
SETUP
System Parameters (P)
Master Public Key (K_{pub})
Master Private Key (K_m)
EXTRACT
Obtain private key
d_B = f (P,K_m,ID_B)
Send ID_B and verify identity
ENCRYPT
Derive Bob's public key
e_B = f (P,K_{pub},ID_B)
Send encrypted message
$c = e_B (m)$
Alice
Message m for Bob
Bob
ID_B
DECRYPT
$m = d_B (c)$

HTTP n HTTPS

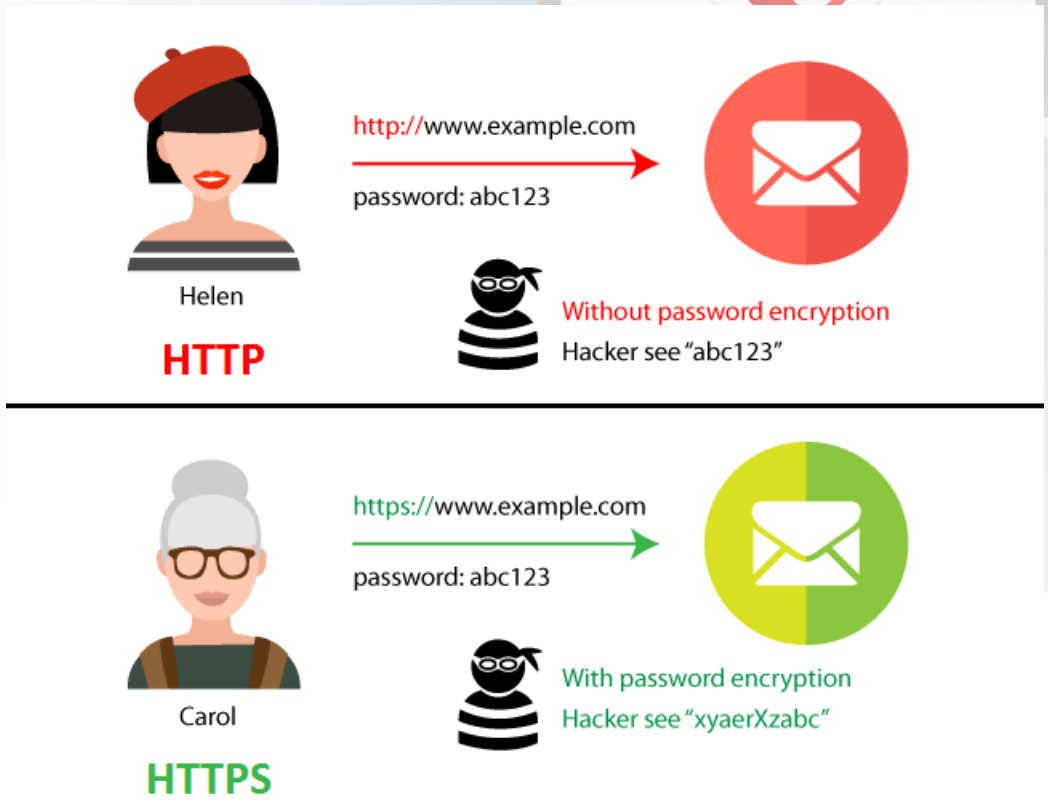


HTTP : Hyper Text Transfer Protocol

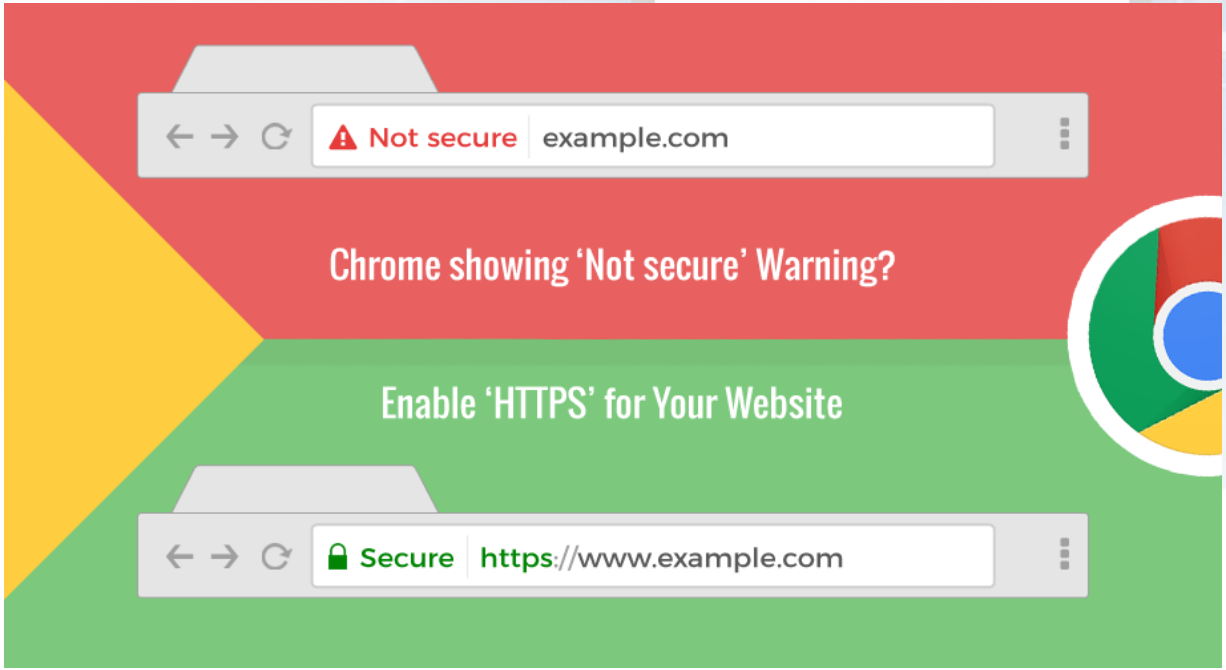
HTTPS : Hyper Text Transfer Protocol Secure

SSL : **Secure Sockets Layer**

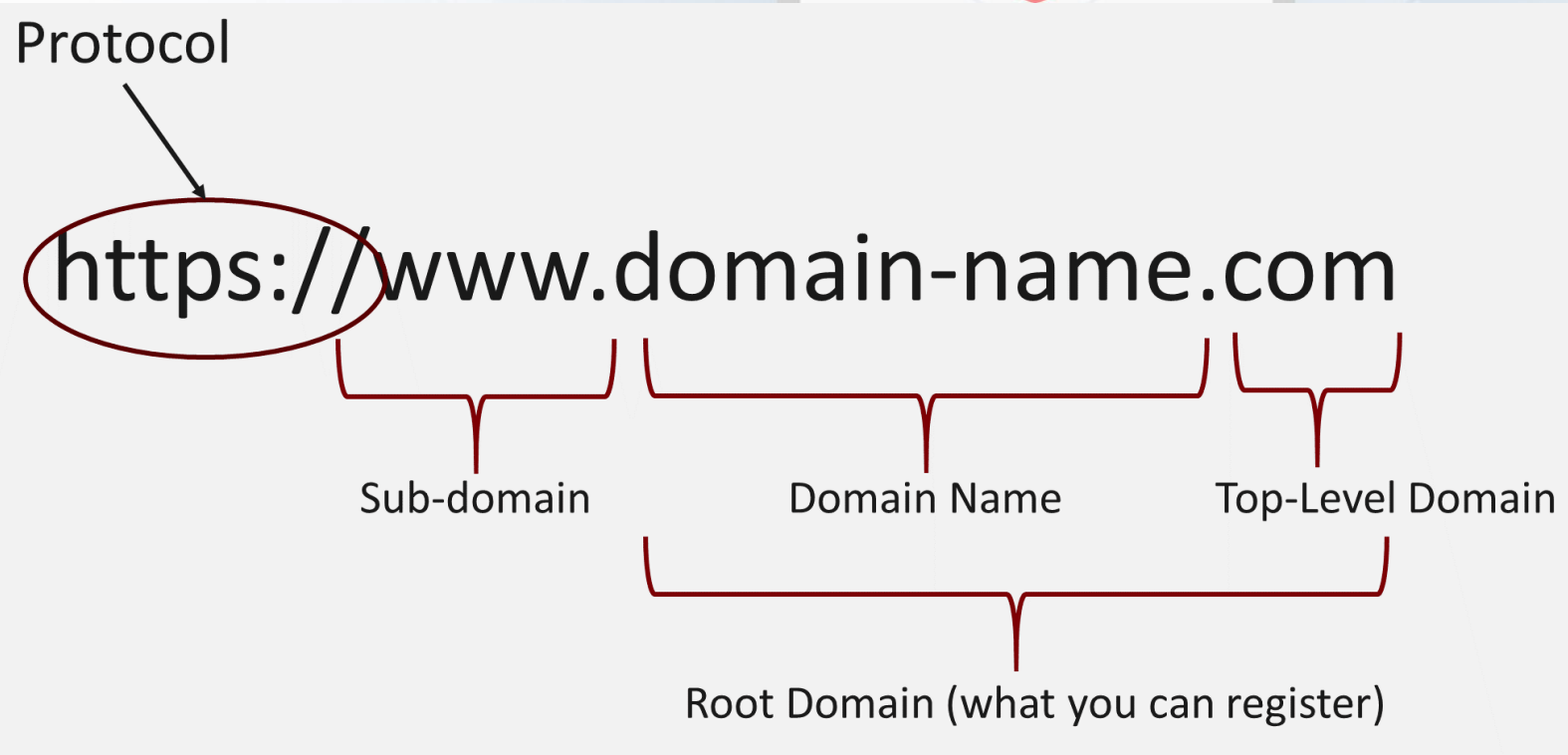
HTTP n HTTPS


http://www.example.com
password: abc123
Helen
HTTP
Without password encryption
Hacker see "abc123"
https://www.example.com
password: abc123
Carol
HTTPS
With password encryption
Hacker see "xyaerXzabc"

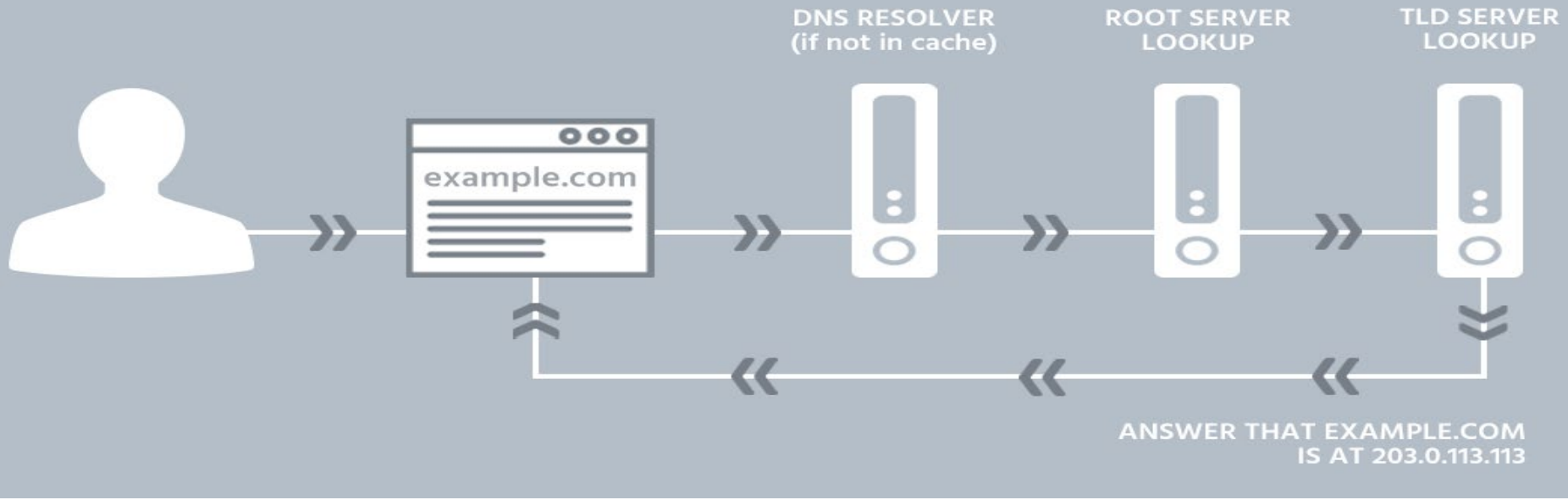
HTTP n HTTPS


Not secure
example.com
Chrome showing 'Not secure' Warning?
Enable 'HTTPS' for Your Website
Secure
https://www.example.com

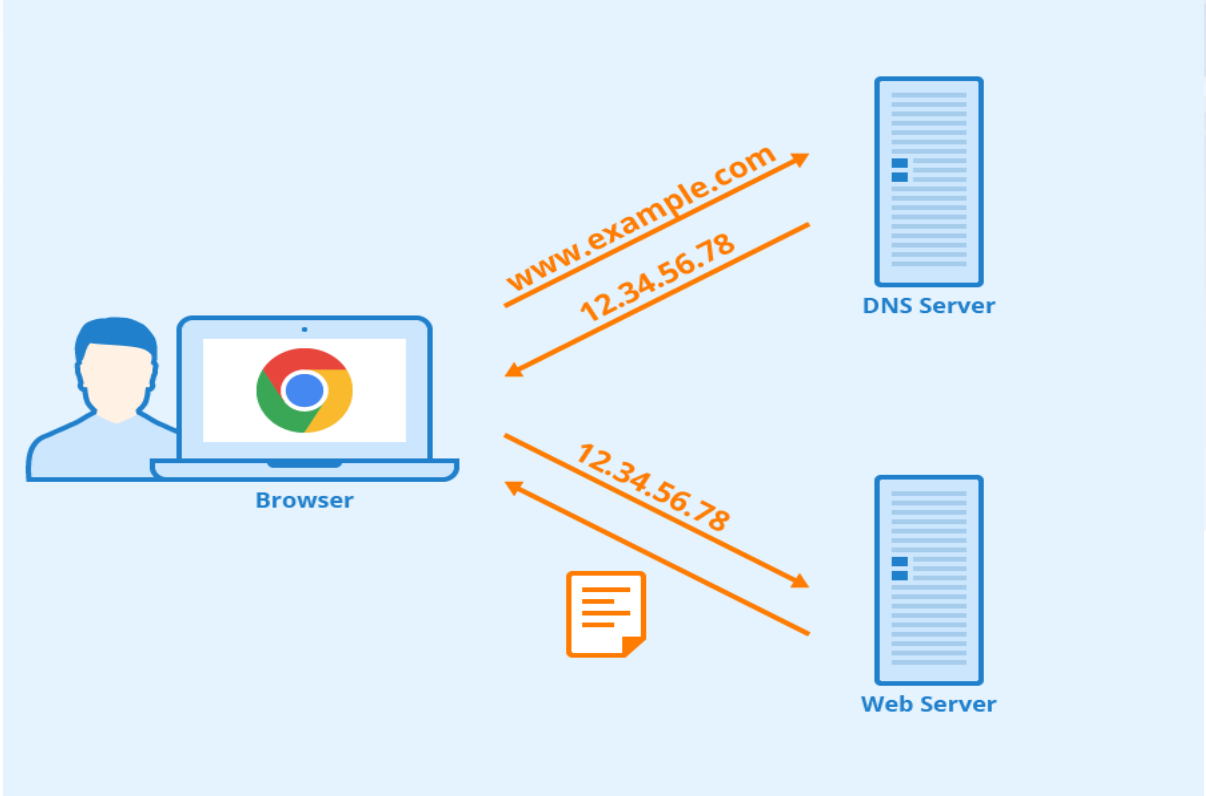
Domain


Protocol
https://www.domain-name.com
Sub-domain
Domain Name
Top-Level Domain
Root Domain (what you can register)

DNS


DNS RESOLVER
(if not in cache)
ROOT SERVER
LOOKUP
TLD SERVER
LOOKUP
example.com
ANSWER THAT EXAMPLE.COM
IS AT 203.0.113.113

DNS


www.example.com
12.34.56.78
DNS Server
Browser
12.34.56.78
Web Server

IP Address

IP Address : Internet Protocol Address

Size : 32 bit OR 4 byte

All Range : 2^32 = 4,294,967,296 Addresses

1 Byte = 8 bits
1 KB = 1024 Byte
1 MB = 1024 KB
1 GB = 1024 MB

IPv4 :

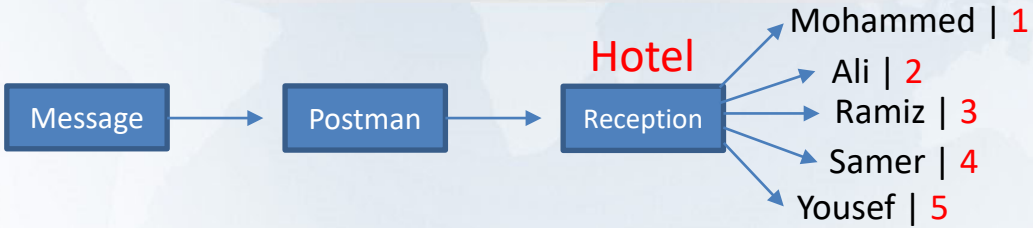
8 Bit 8 Bit 8 Bit 8 Bit

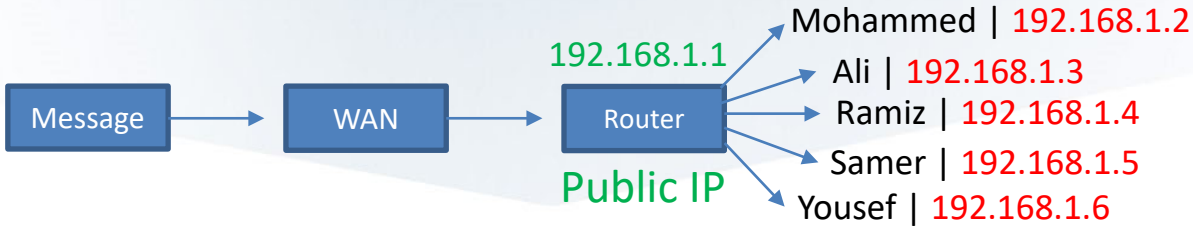
214.67.34.129

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	0	1	0	1	1	0

NAT

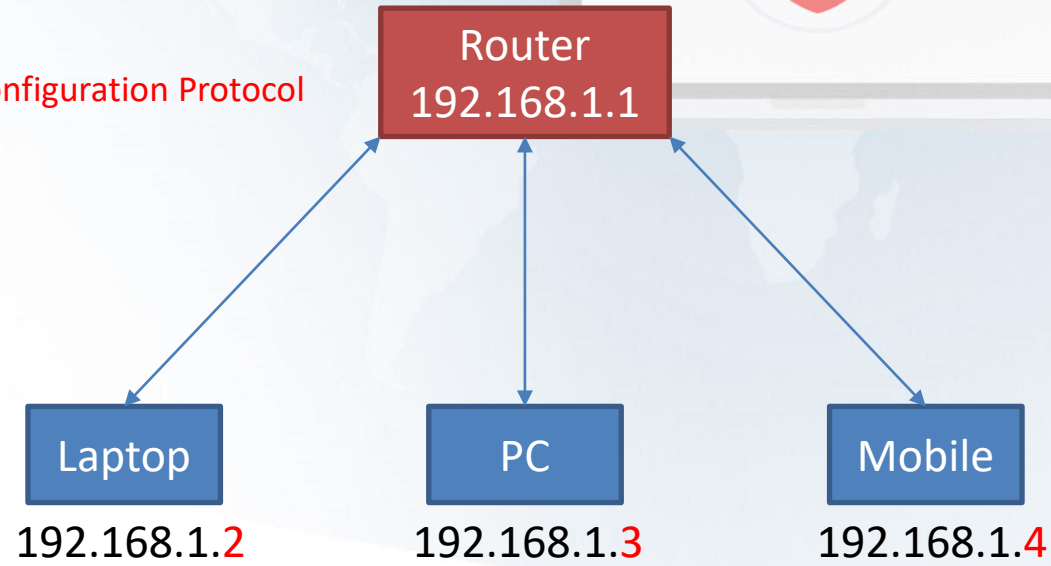
NAT : Network Address Translation





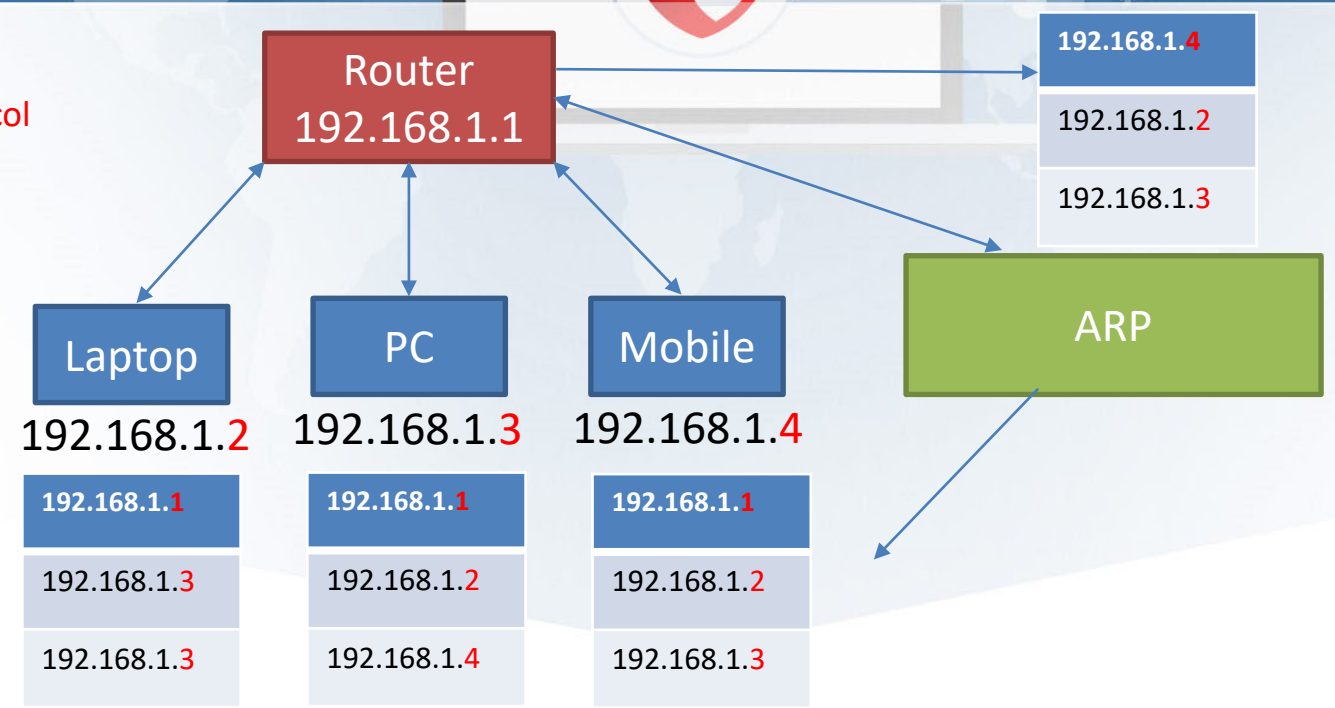
DHCP

DHCP : Dynamic Host Configuration Protocol



ARP

ARP : Address Resolution Protocol



MAC Address

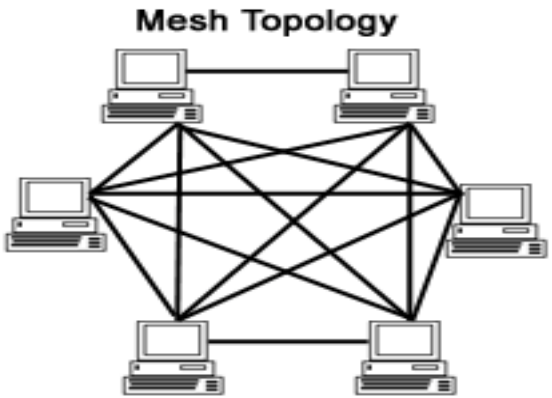
MAC : Media Access Control

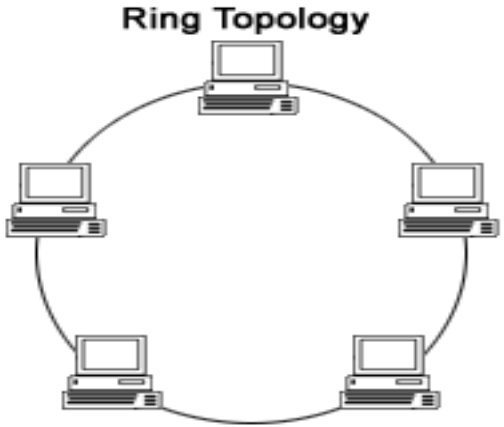
B4-2E-99-EC-F8-90

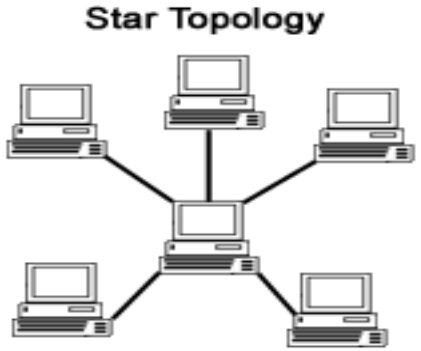
0 1 2 3 4 5 6
7 8 9 A B C D E F

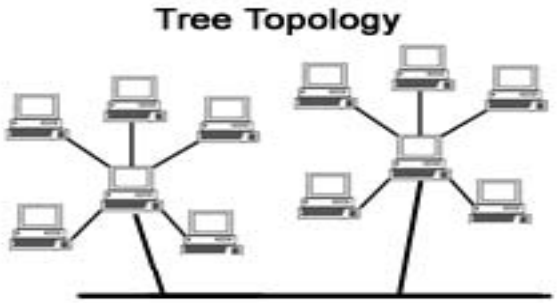
Counter :

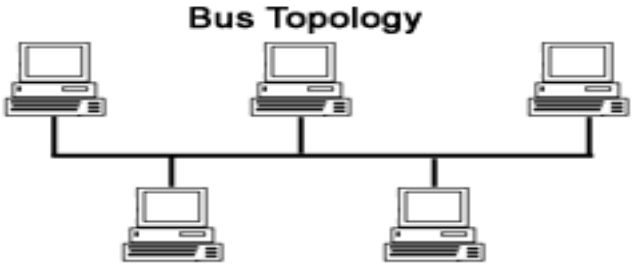
Network Topology





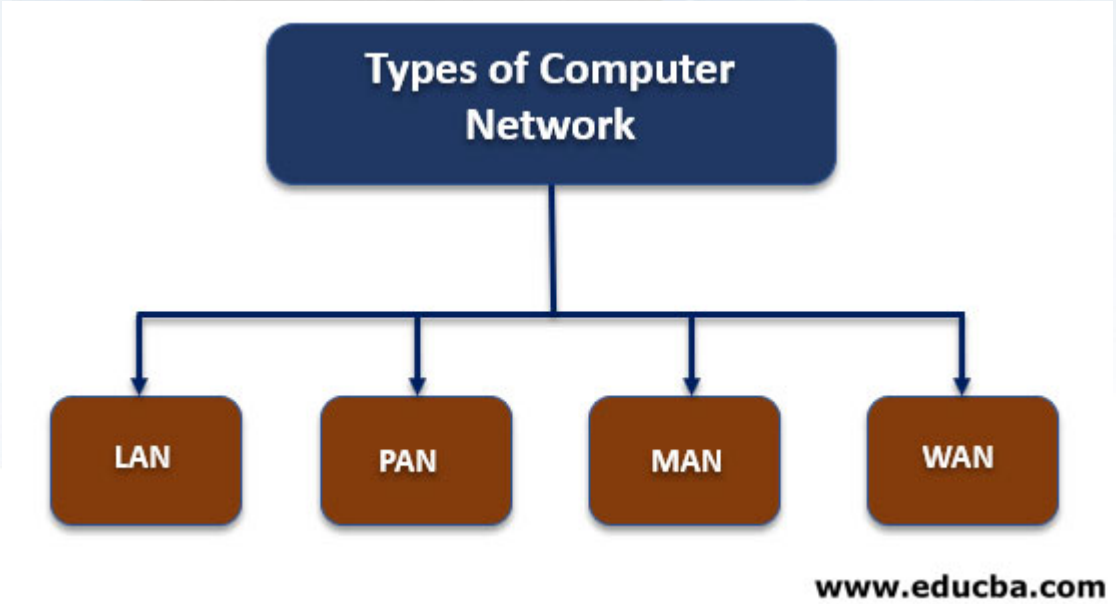




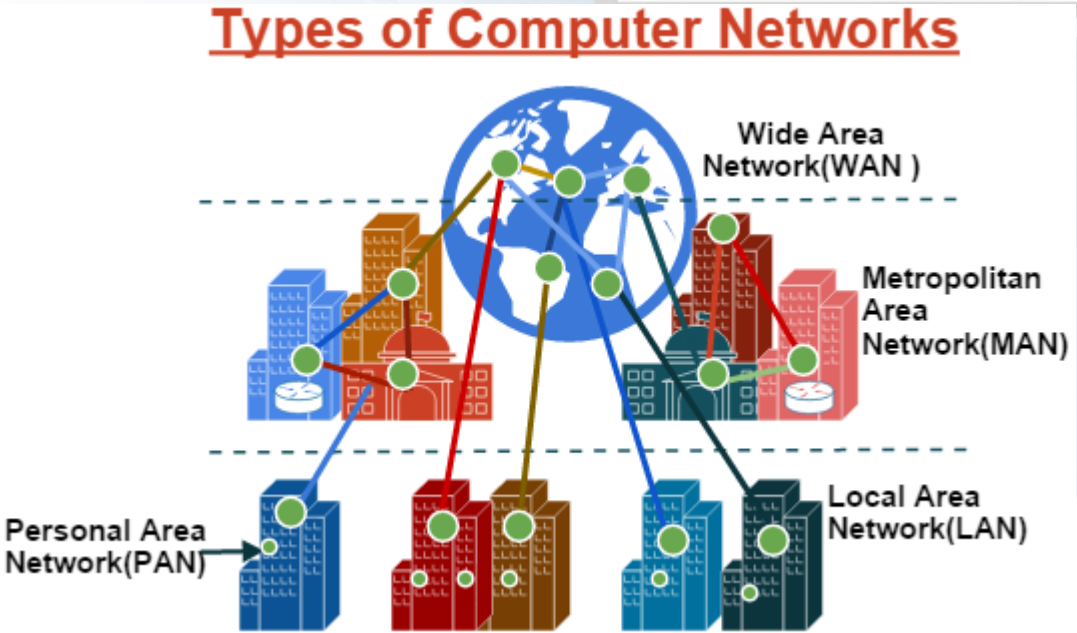


Network Types

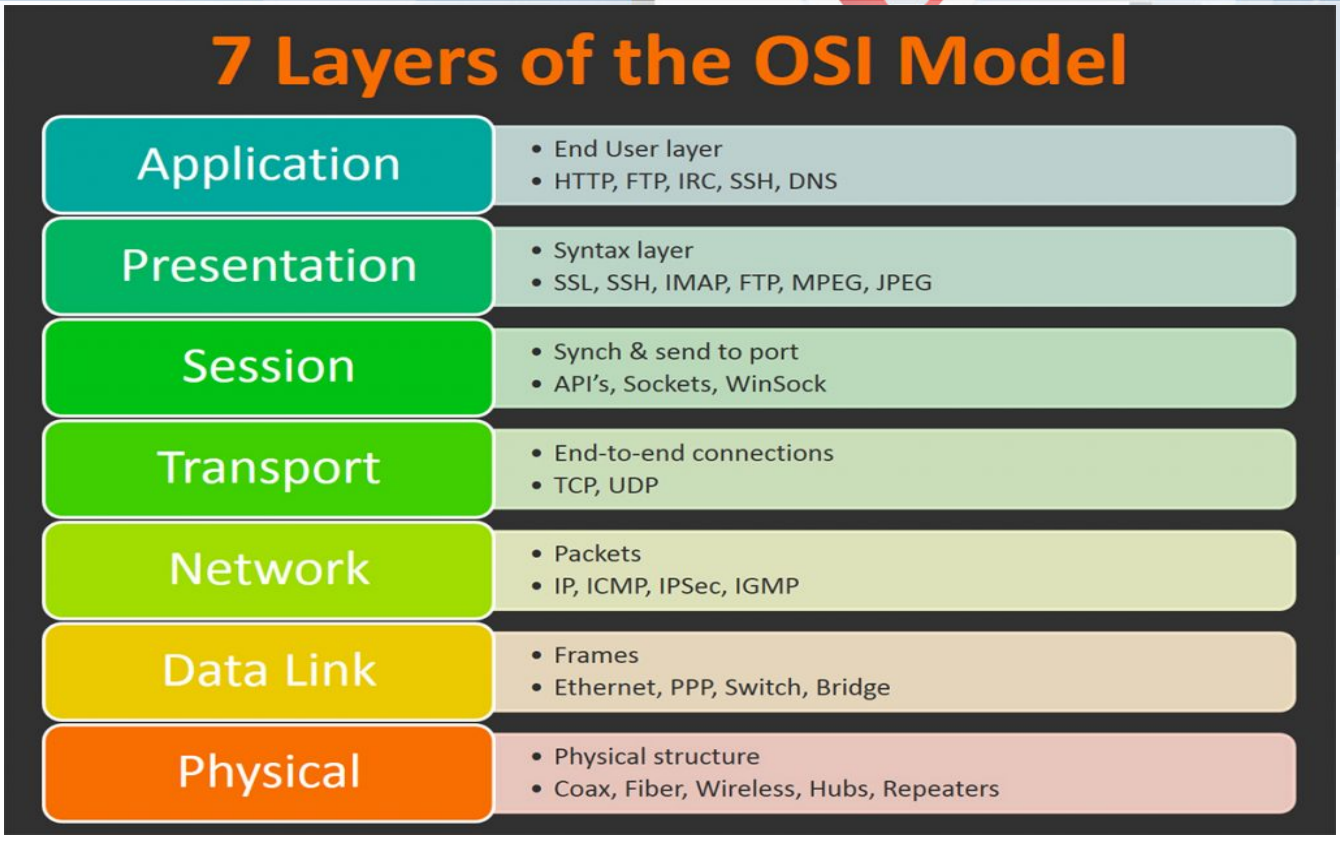
LAN : Local Area Network
PAN : Personal Area Network
MAN : Metropolitan Area Network
WAN : Wide Area Network
WLAN : Wireless Local Area Network



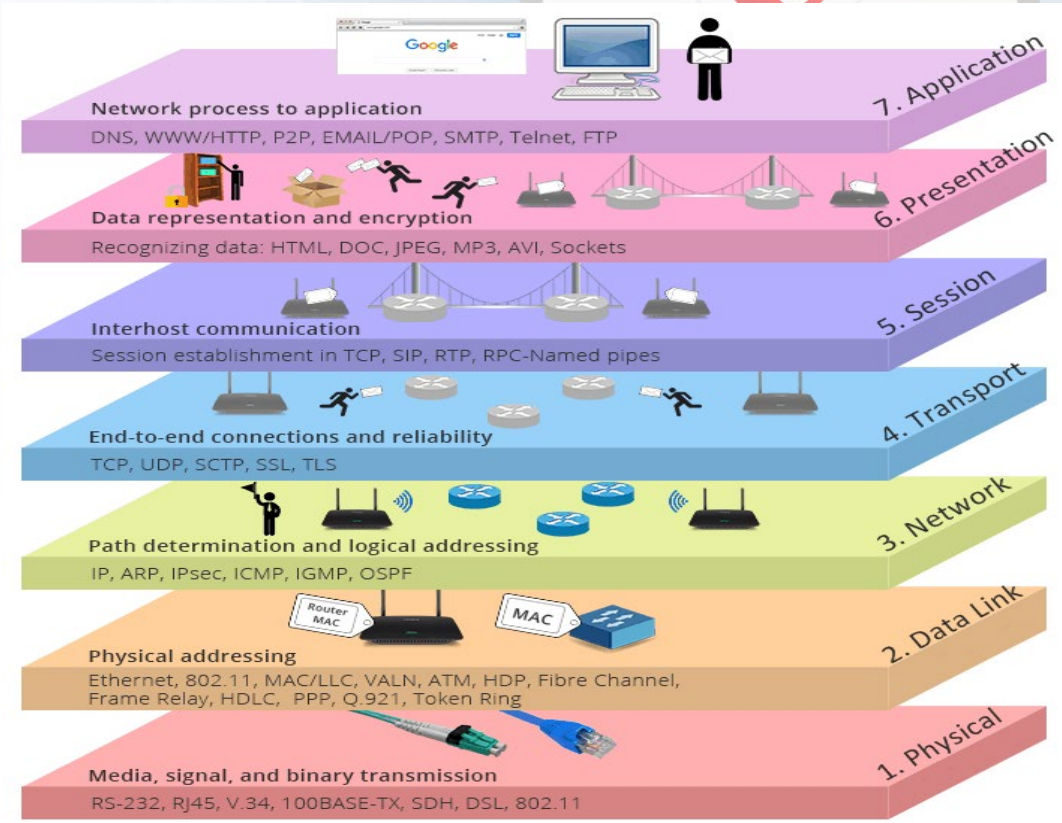
Network Types



OSI Model

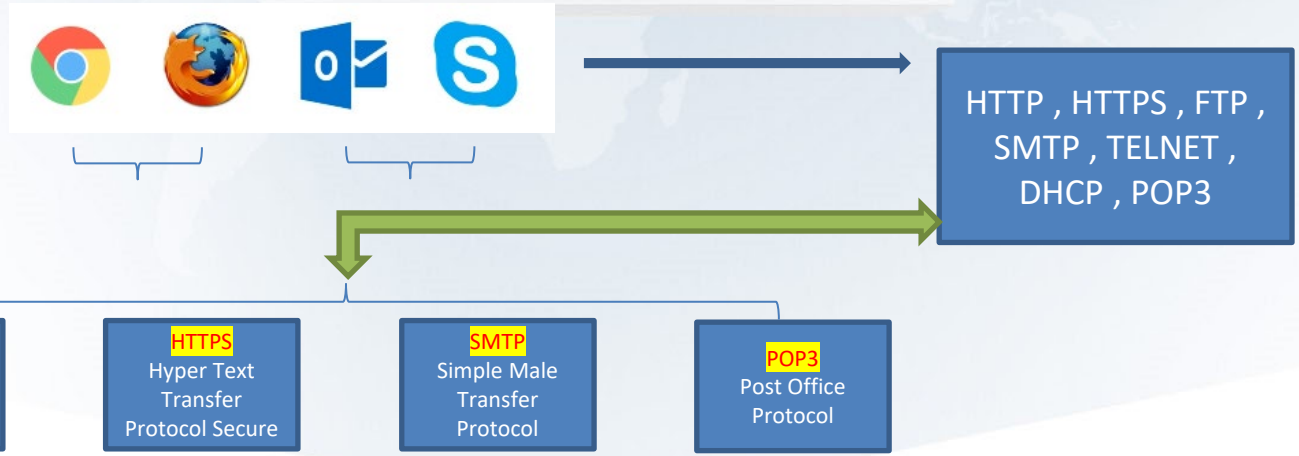

7 Layers of the OSI Model
Application
• End User layer
• HTTP, FTP, IRC, SSH, DNS
Presentation
• Syntax layer
• SSL, SSH, IMAP, FTP, MPEG, JPEG
Session
• Synch & send to port
• API's, Sockets, WinSock
Transport
• End-to-end connections
• TCP, UDP
Network
• Packets
• IP, ICMP, IPSec, IGMP
Data Link
• Frames
• Ethernet, PPP, Switch, Bridge
Physical
• Physical structure
• Coax, Fiber, Wireless, Hubs, Repeaters

OSI Model

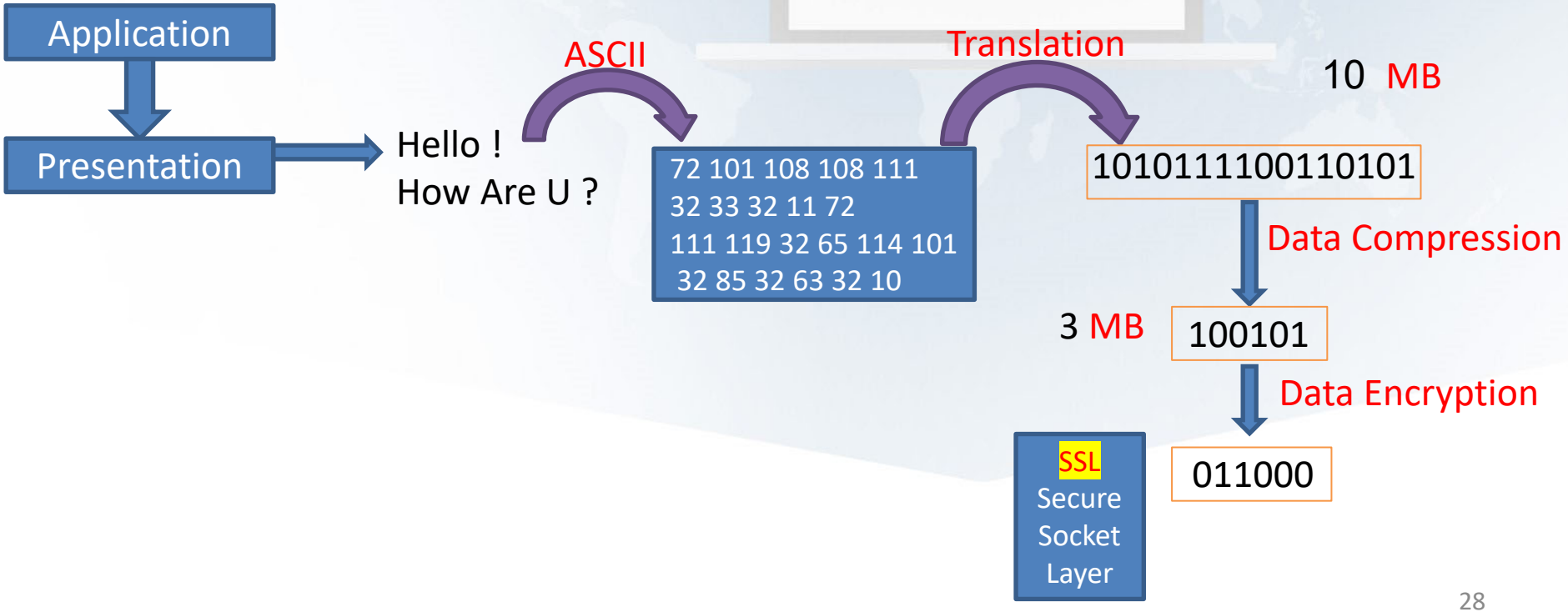

7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Application Layer

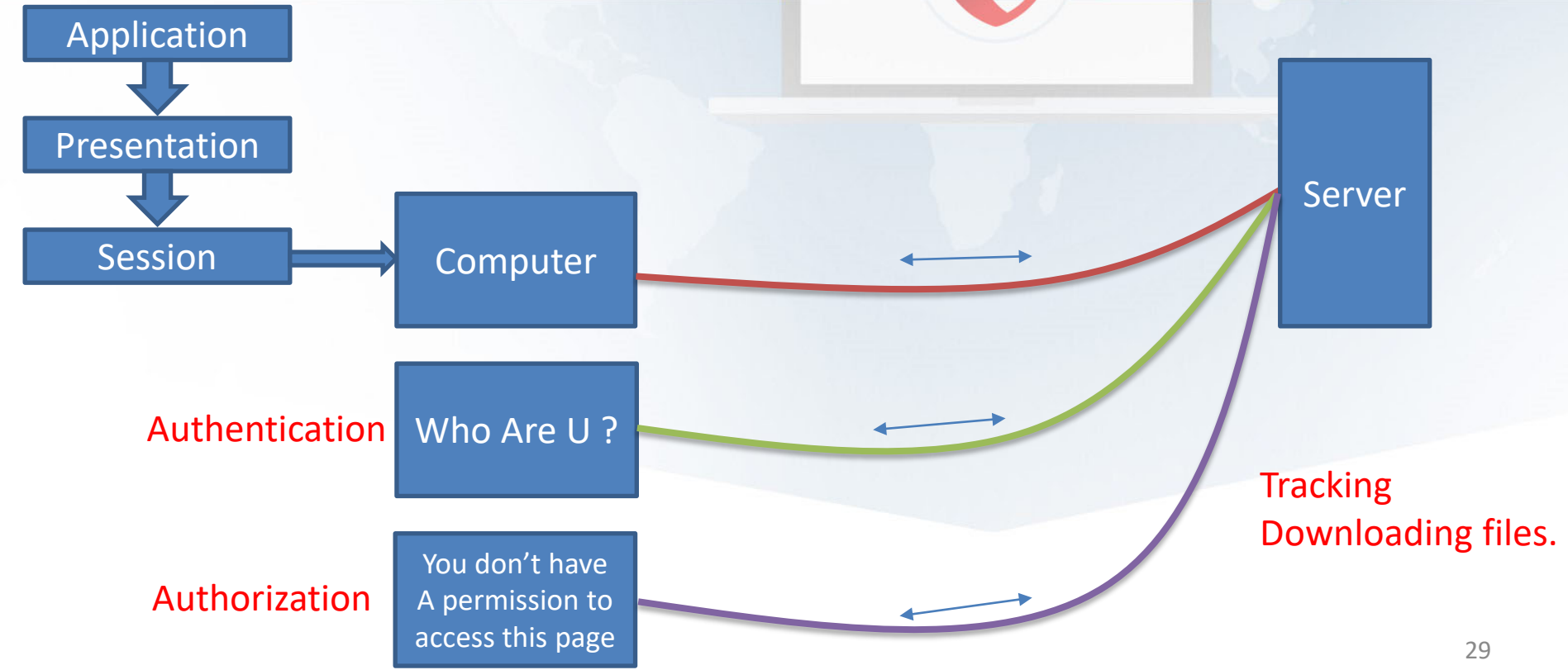
Application Layer : Network Application



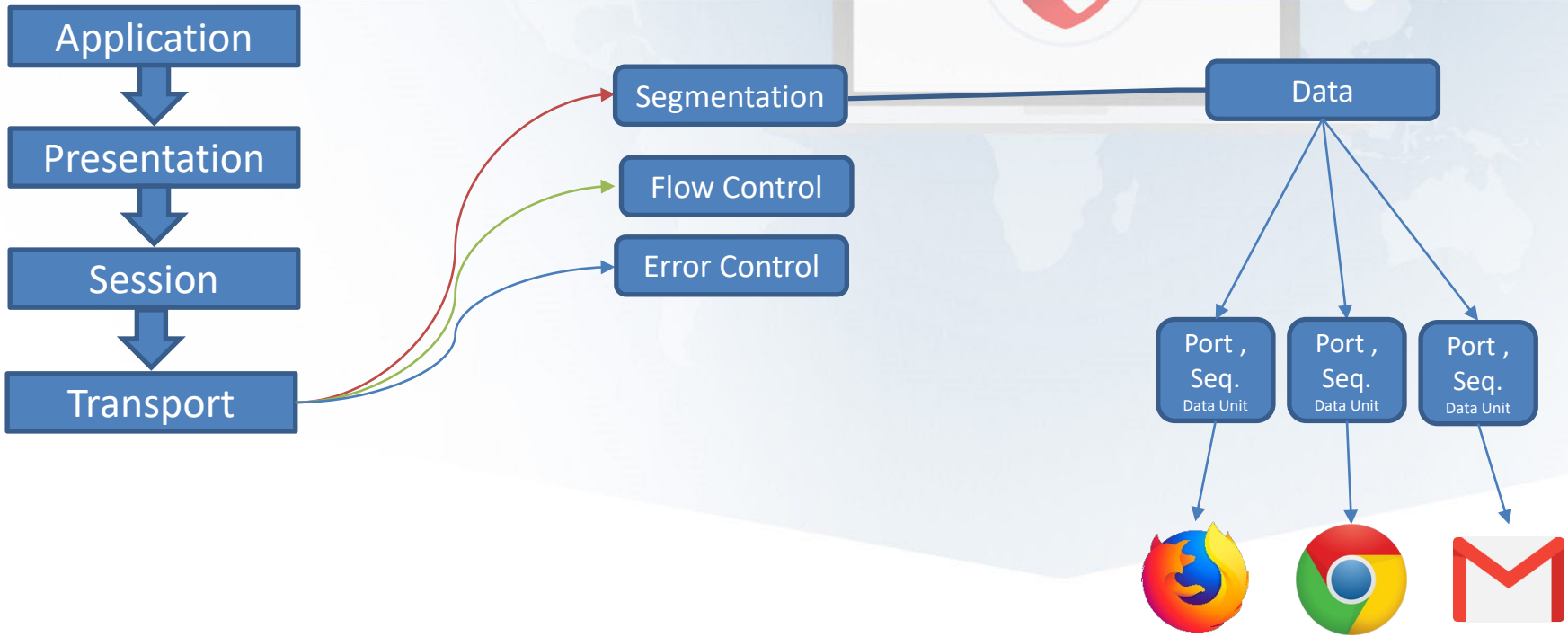
Presentation Layer



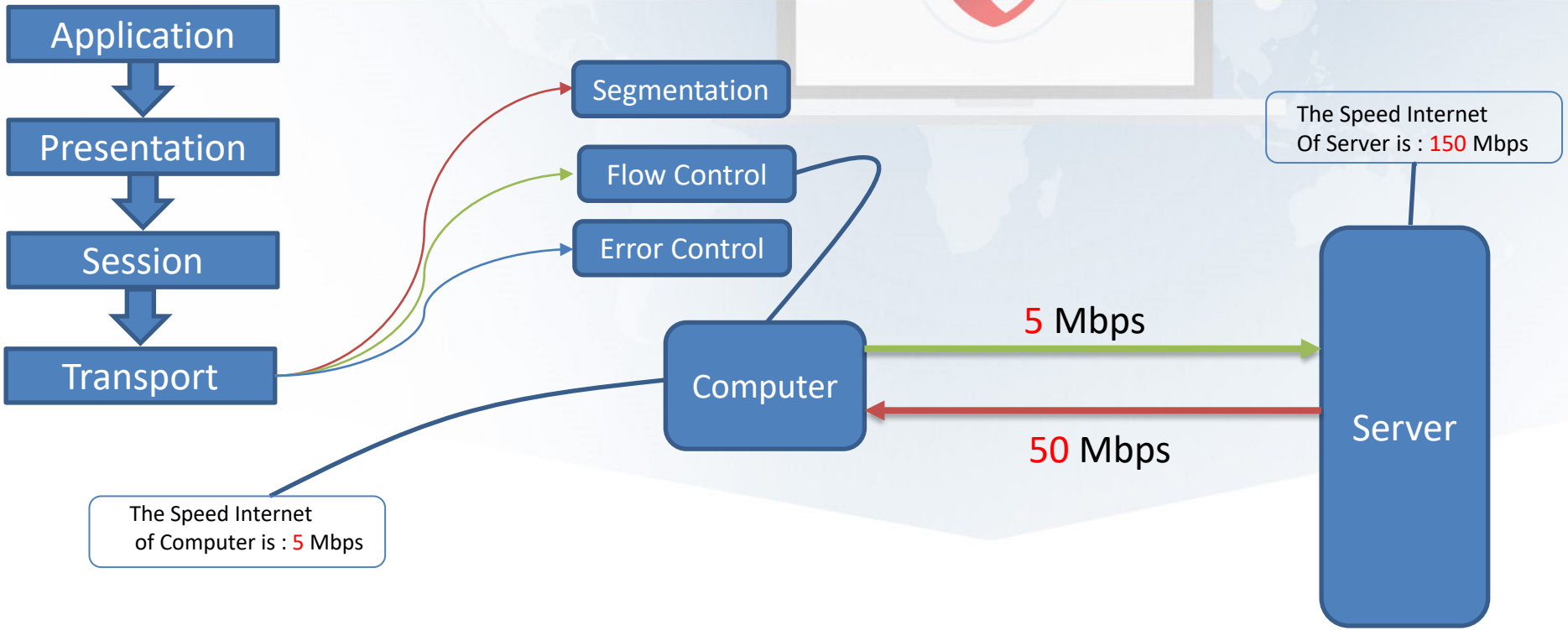
Session Layer



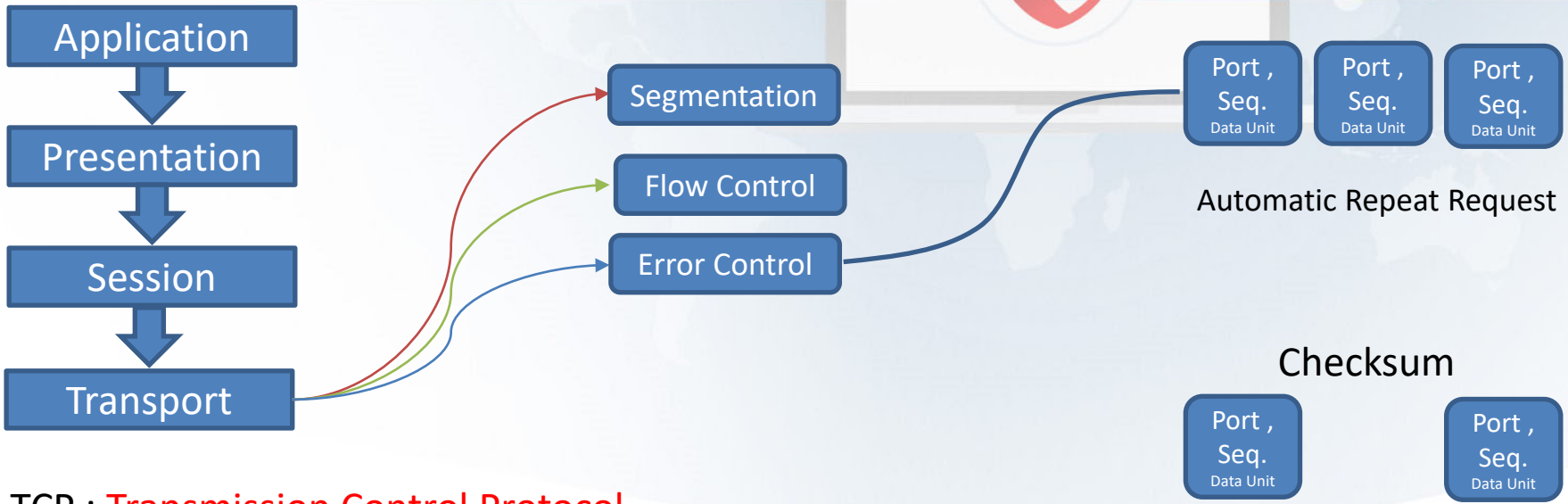
Transport Layer



Transport Layer



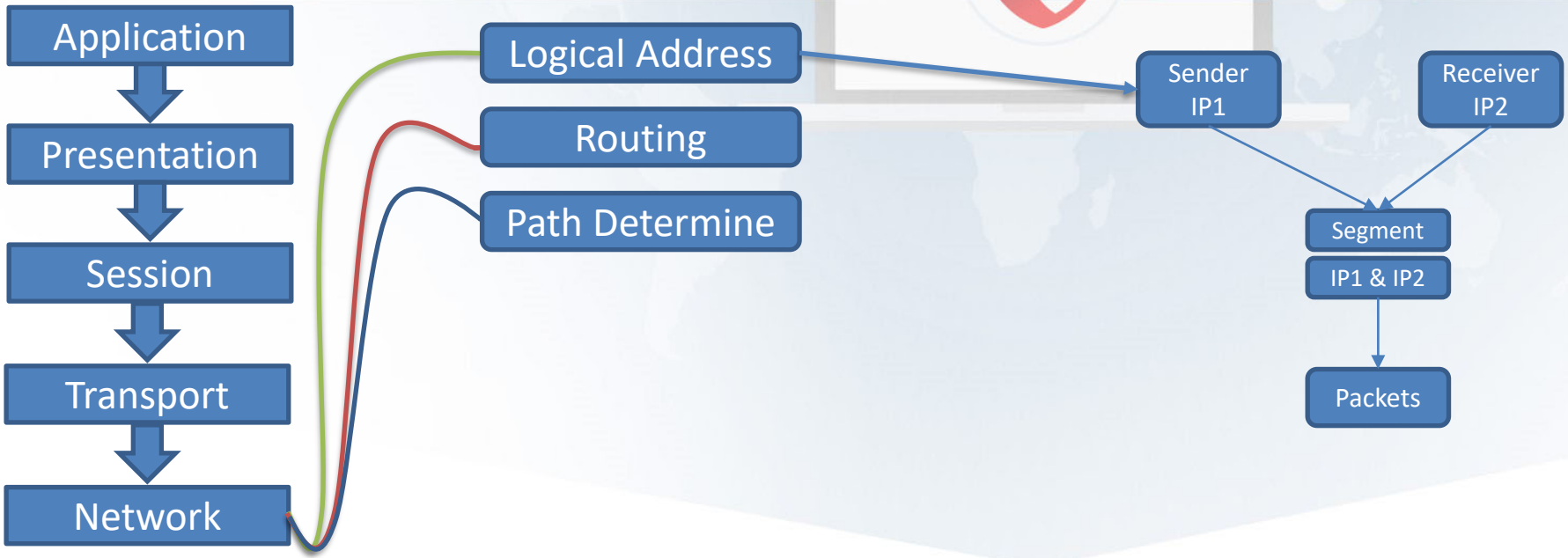
Transport Layer



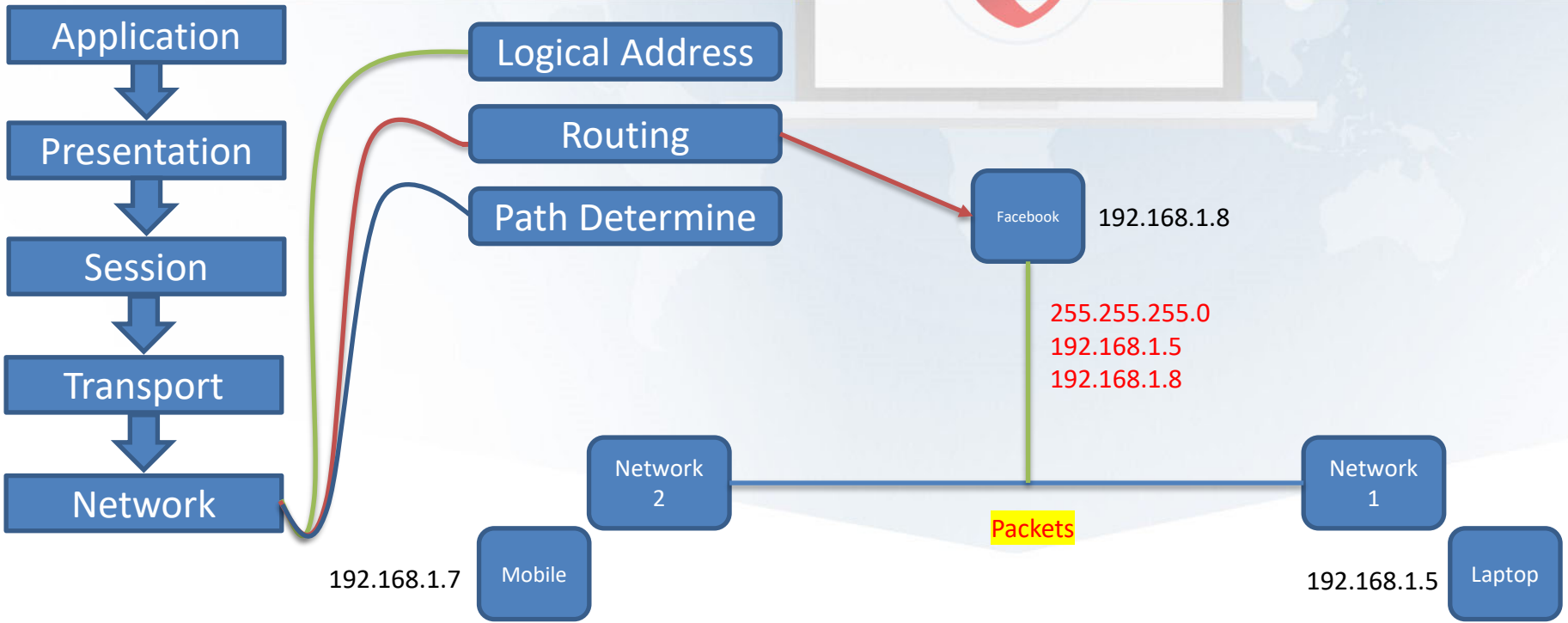
TCP : Transmission Control Protocol

UDP : User Datagram Protocol

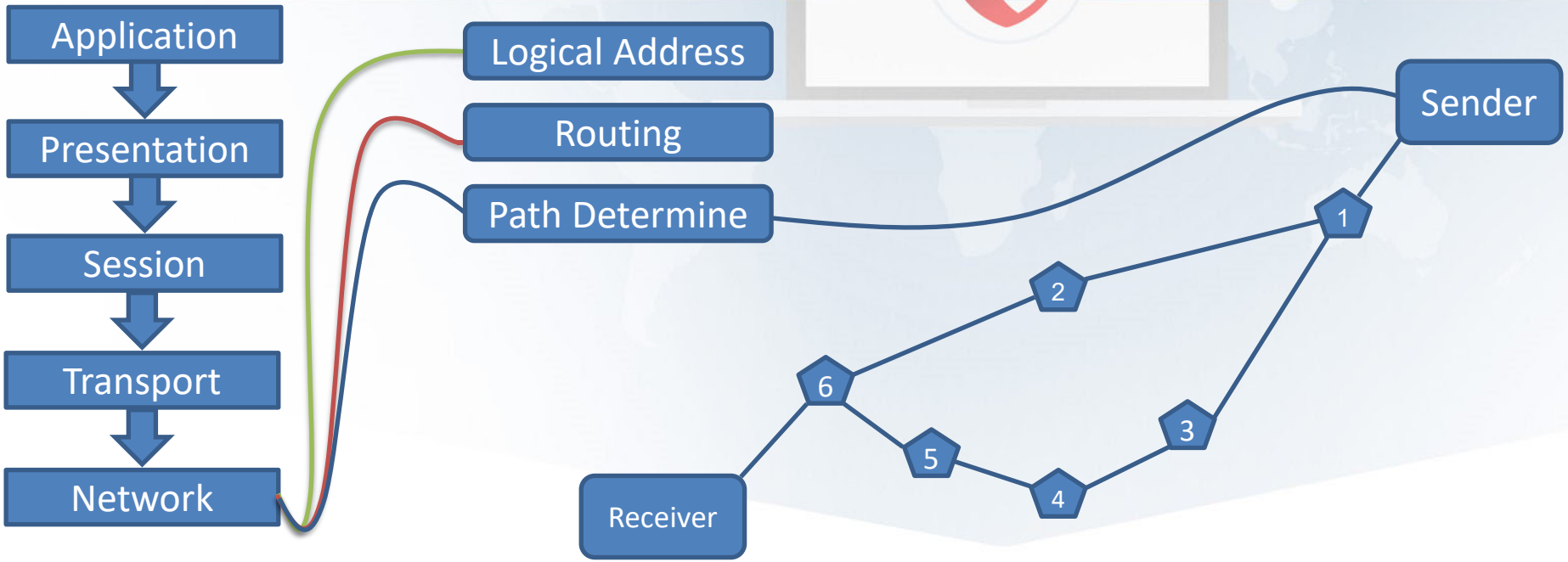
Network Layer



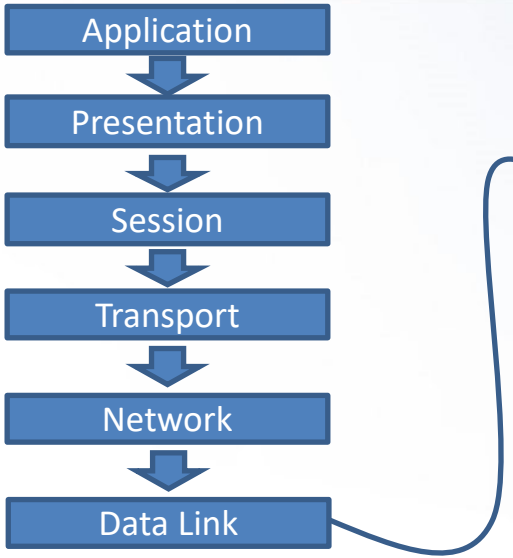
Network Layer

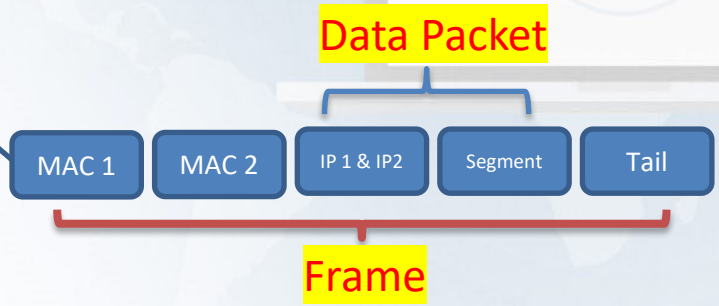


Network Types



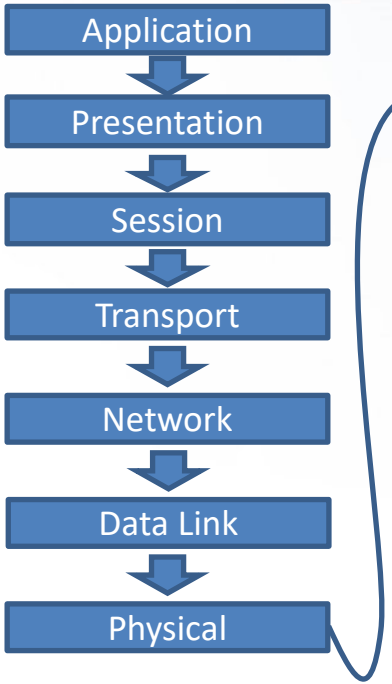
Data Link





MAC 1 : Sender
MAC 2 : Receiver

Physical



Hi !

Transport Layer

Packet

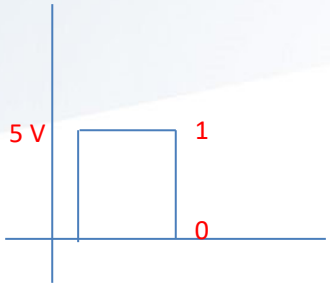
Sender IP | Receiver IP | Segment

Network Layer

Frame

Sender MAC | Receiver MAC | Packet | FCS

Data Link Layer

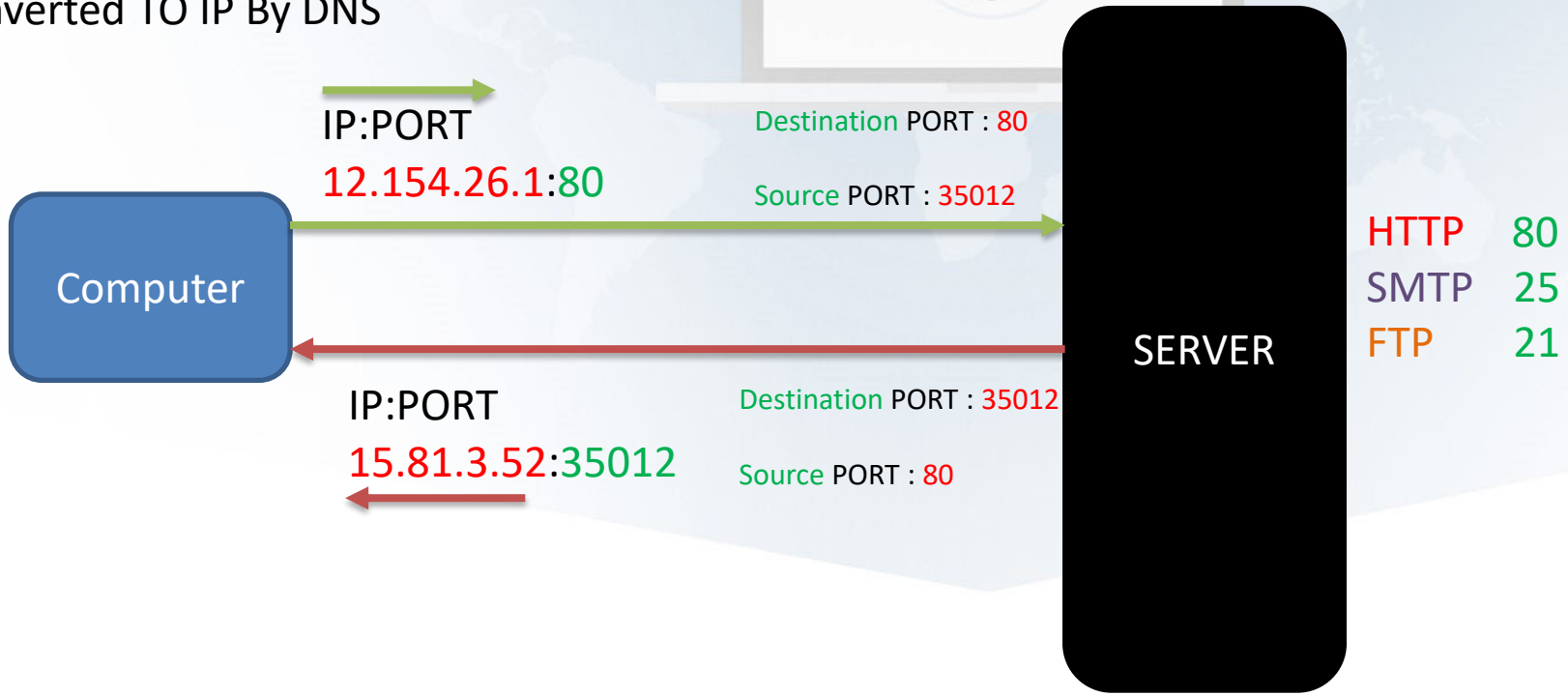


Frame Like : 10111001100110011111001010

Physical Convert it to : Electric Signal

PORTS

URL Converted TO IP By DNS



PORTS

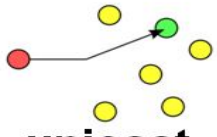
Most Ports Must Be Known

Protocol	NAME	TYPE	PORT
DNS	Domain Name System	TCP/UDP	53
SMTP	Simple Main Transfer Protocol	TCP	25
HTTP	Hyper Text Transfer Protocol	TCP	80
HTTPS	Hyper Text Transfer Protocol Secure	TCP	443
FTP Control	File Transfer Protocol Control	TCP	21
FTP Data	File Transfer Protocol Data	TCP	20
SMB	Server Message Block	TCP	445
DHCP	Dynamic Host Configuration Protocol	TCP	67,68
SSH	Secure Shell	TCP	22
TELNET	Telnet	TCP	23
POP3	Post Office Protocol 3	TCP	110
SNMP	Simple Network Management Protocol	UDP	161

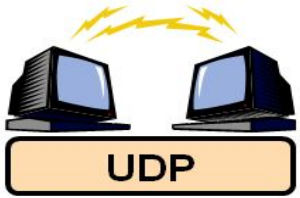
TCP vs UDP

TCP

- Slower but reliable transfers
- Typical applications:
  - Email
  - Web browsing

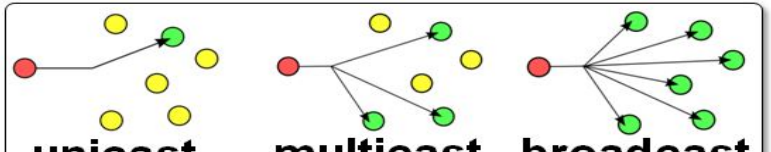


unicast



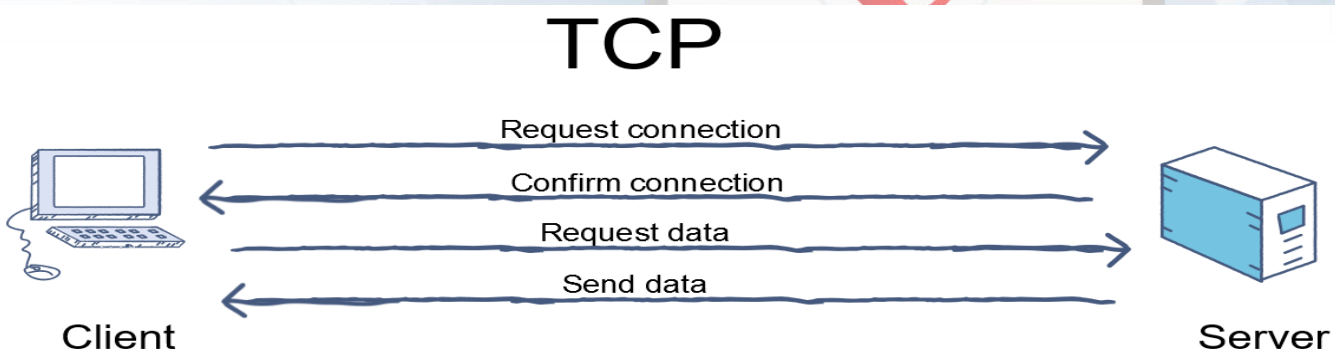
UDP

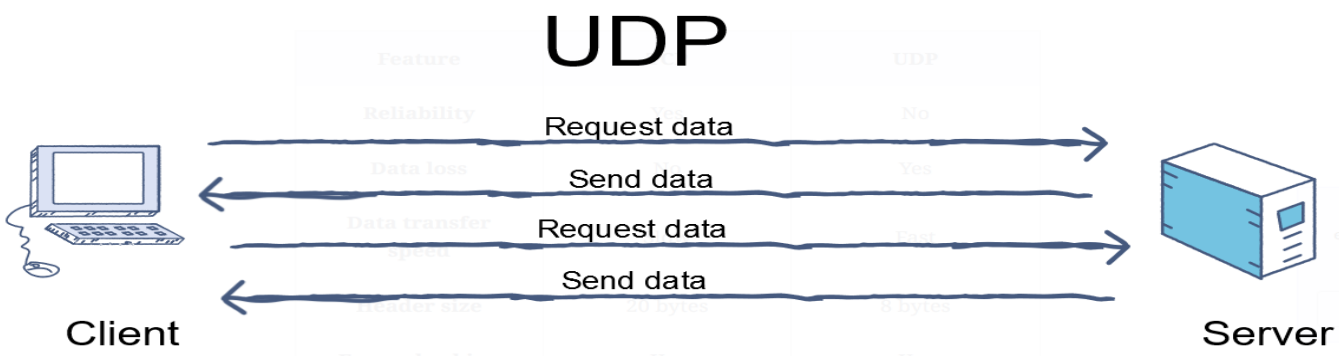
- Fast but non-guaranteed transfers (“best effort”)
- Typical applications:
  - VoIP
  - Music streaming



unicast multicast broadcast

TCP vs UDP


TCP
Request connection
Confirm connection
Request data
Send data
Client
Server


UDP
Request data
Send data
Request data
Send data
Client
Server

TCP vs UDP

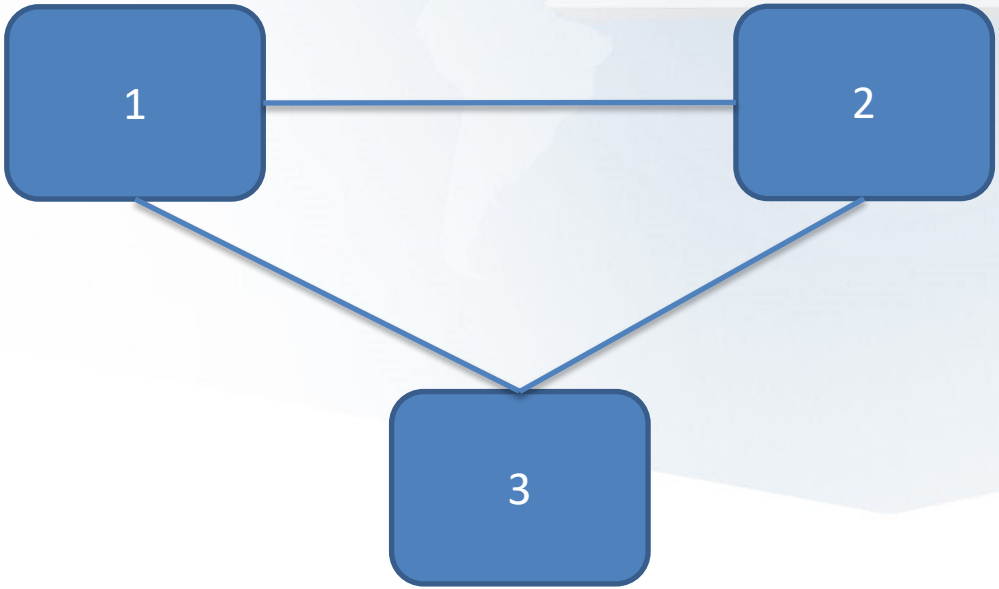
Feature	TCP	UDP
Reliability	Yes	No
Data loss	No	Yes
Data transfer speed	Slow	Fast
Header size	20 bytes	8 bytes
Error checking	Yes	Yes
Error recovery	Yes	No
Flow control	Yes	No

Repeater

Repeater : Regenerate incoming electrical signal
In physical devices [Ethernet , WIFI] .

We use repeater in distance limitation in LAN.

HUB



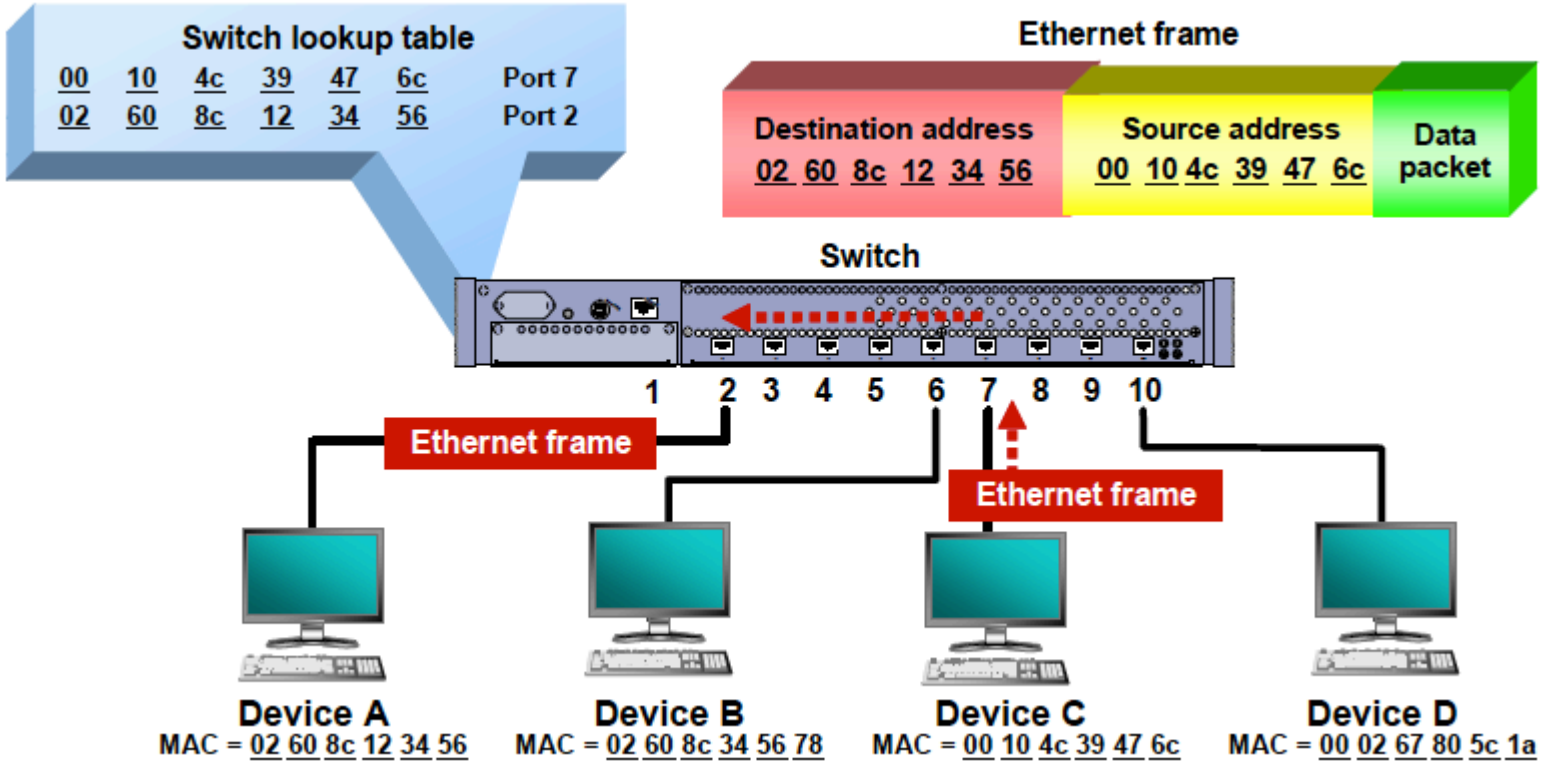
HUB

HUB

Bridge

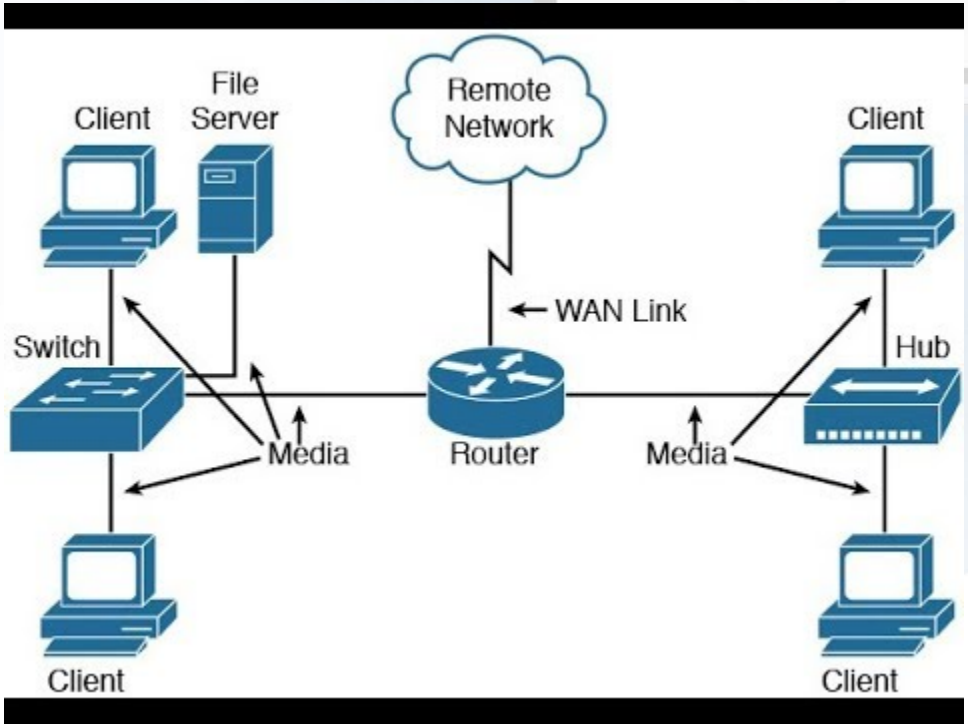
Bridge

SWITCH


Switch lookup table
00 10 4c 39 47 6c Port 7
02 60 8c 12 34 56 Port 2
Ethernet frame
Destination address
02 60 8c 12 34 56
Source address
00 10 4c 39 47 6c
Data packet
Switch
1 2 3 4 5 6 7 8 9 10
Ethernet frame
Ethernet frame
Device A
MAC = 02 60 8c 12 34 56
Device B
MAC = 02 60 8c 34 56 78
Device C
MAC = 00 10 4c 39 47 6c
Device D
MAC = 00 02 67 80 5c 1a

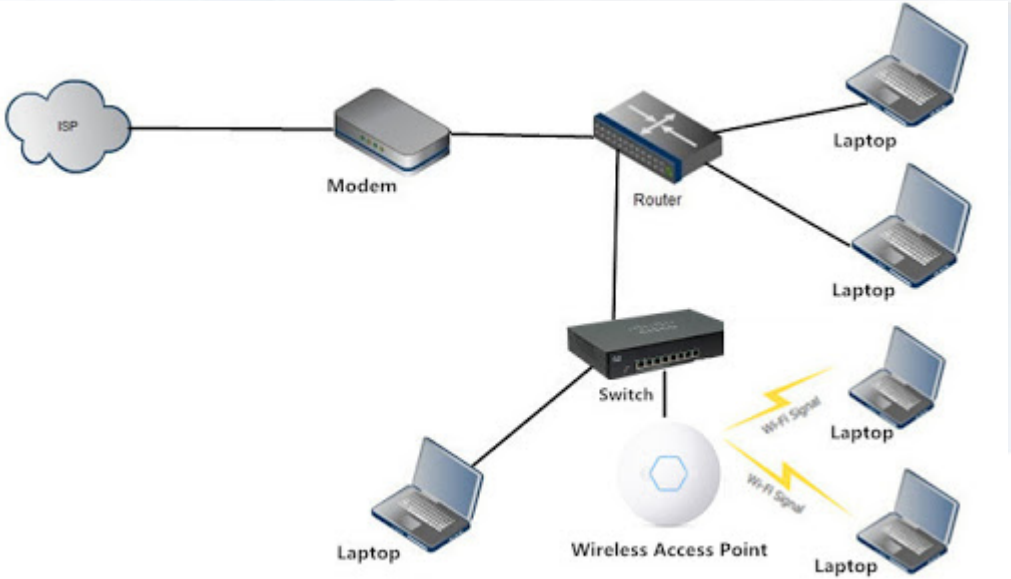
ROUTER

10.2.3.0



192.168.1.0

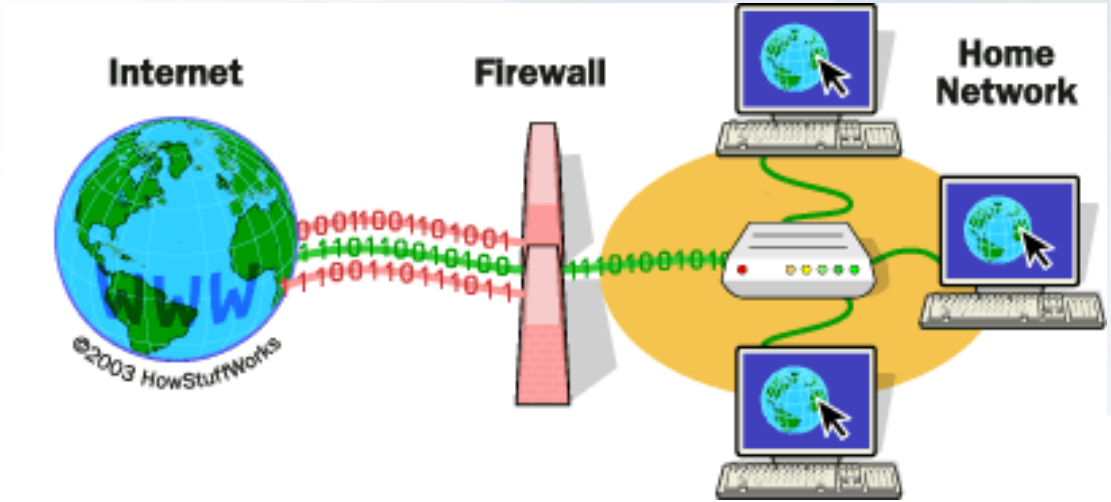
Access Point



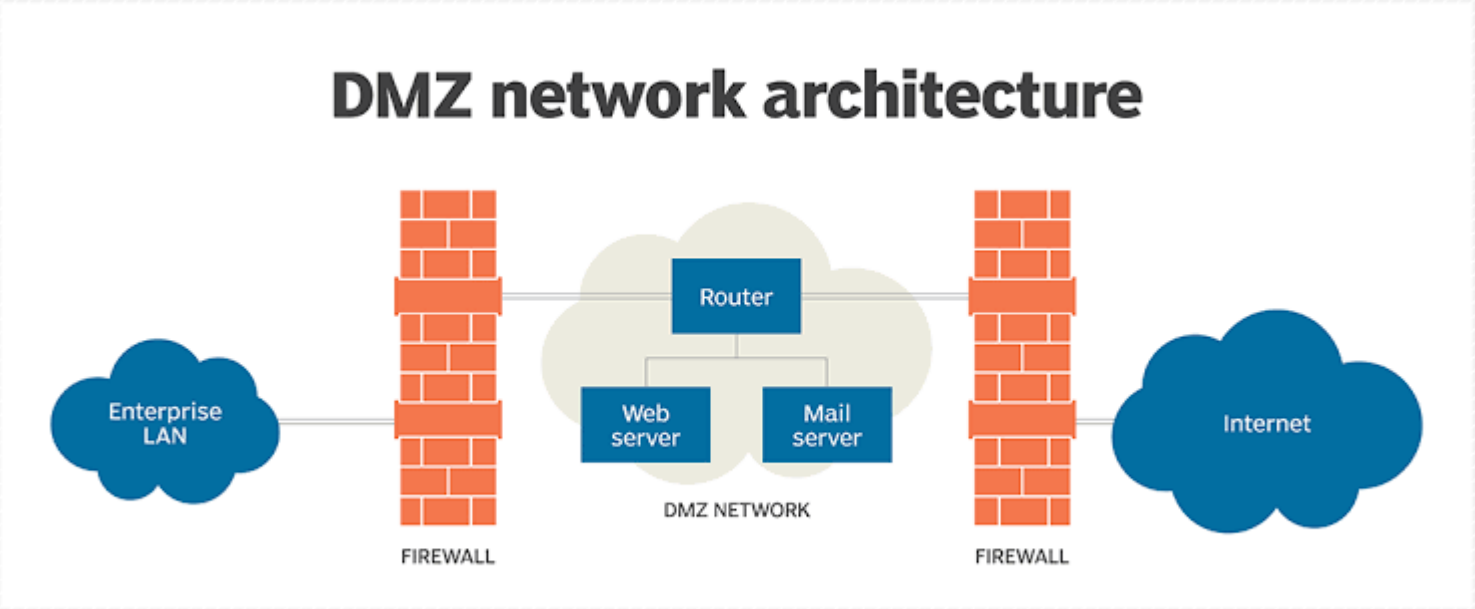
Firewall


FORTINET
FortiGate 90E
USB
CONSOLE
PWR
STA
ALARM
HA
WAN 1
DMZ
WAN 2
HA
1
3
5
7
9
11
2
4
6
8
10
12

Firewall

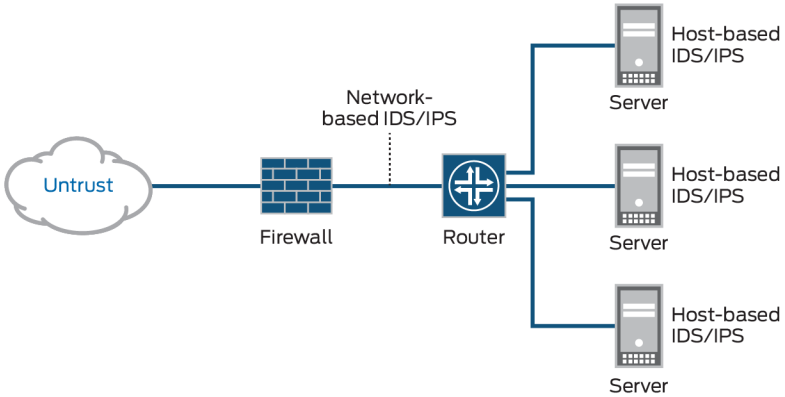


Firewall

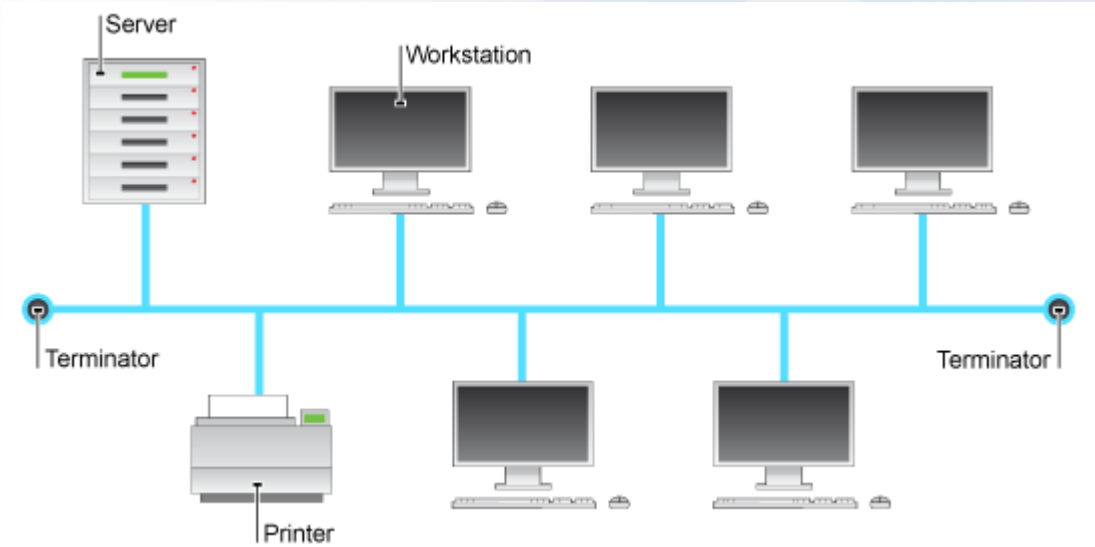

DMZ network architecture
Enterprise LAN
FIREWALL
Router
Web server
Mail server
DMZ NETWORK
FIREWALL
Internet

IDS / IPS

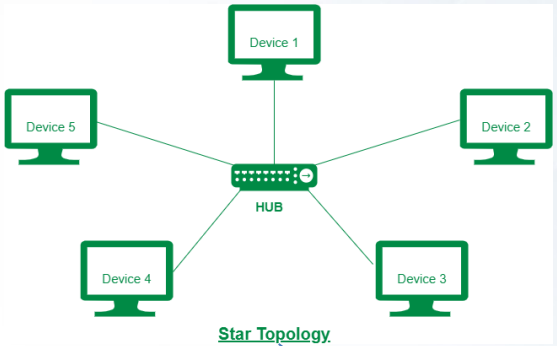
IDS / IPS

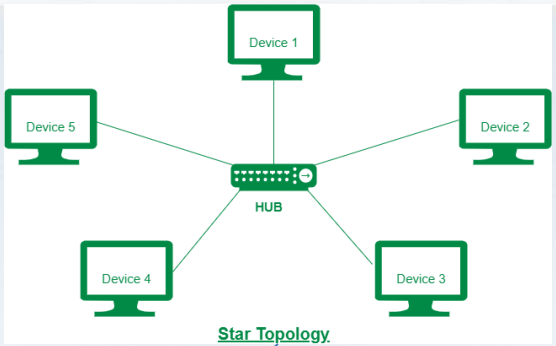

Host-based
IDS/IPS
Server
Network-
based IDS/IPS
Untrust
Firewall
Router
Host-based
IDS/IPS
Server
Host-based
IDS/IPS
Server

BUS Topology

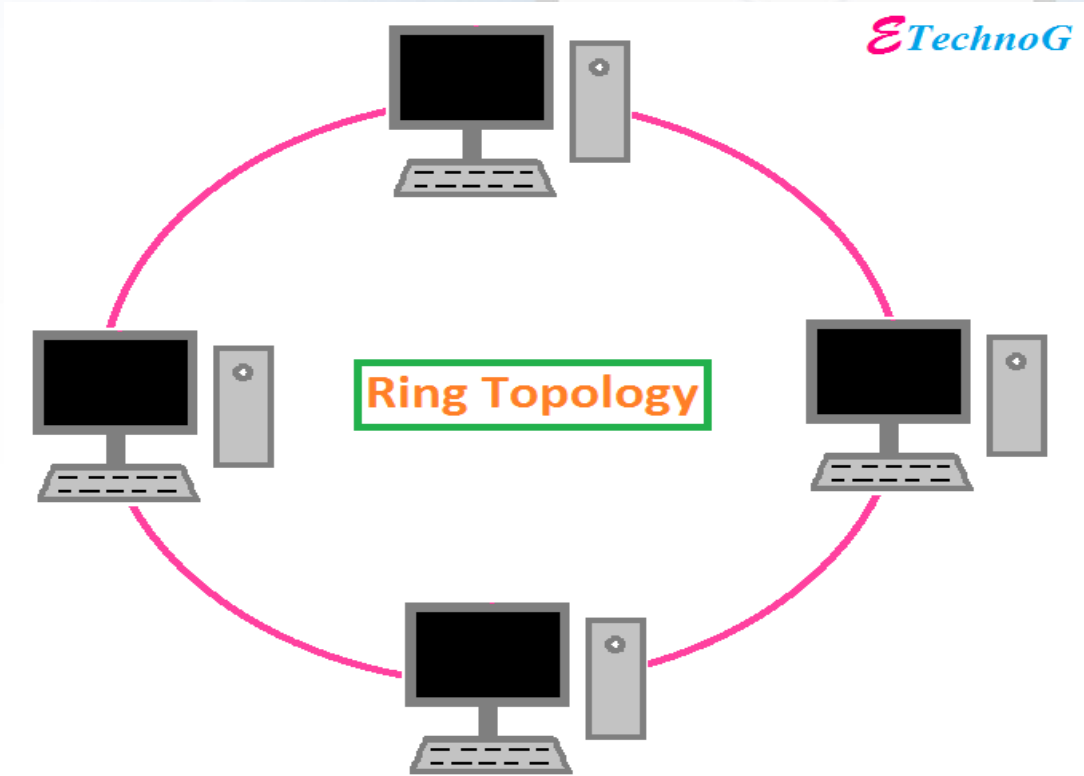


Star Topology

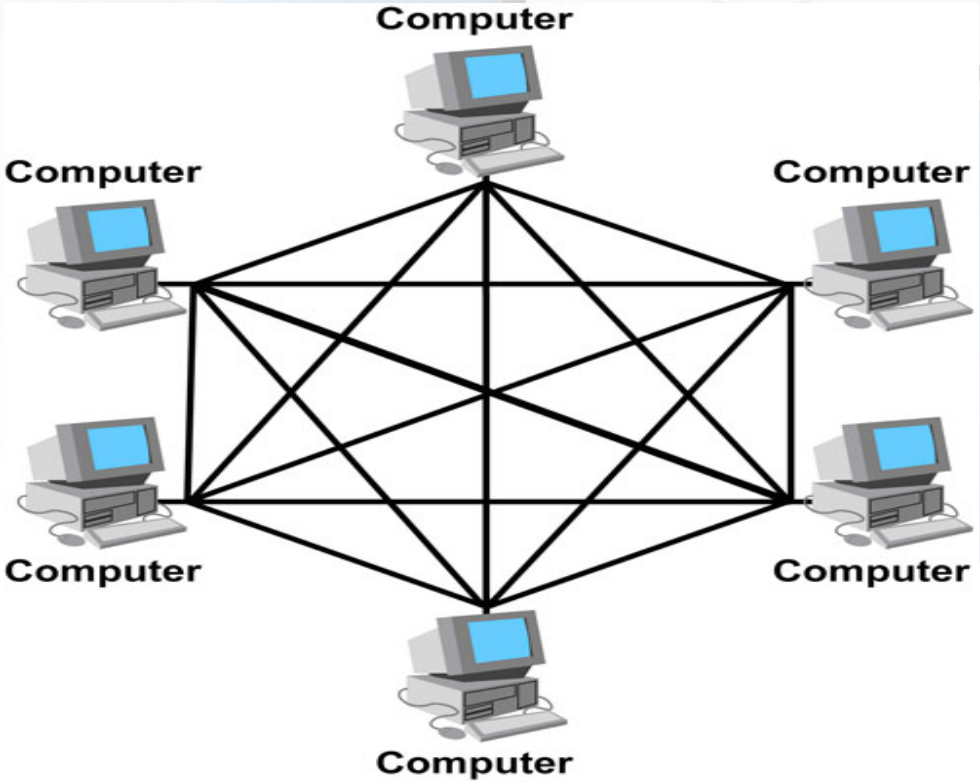




Ring Topology



Mesh Topology



IDS / IPS