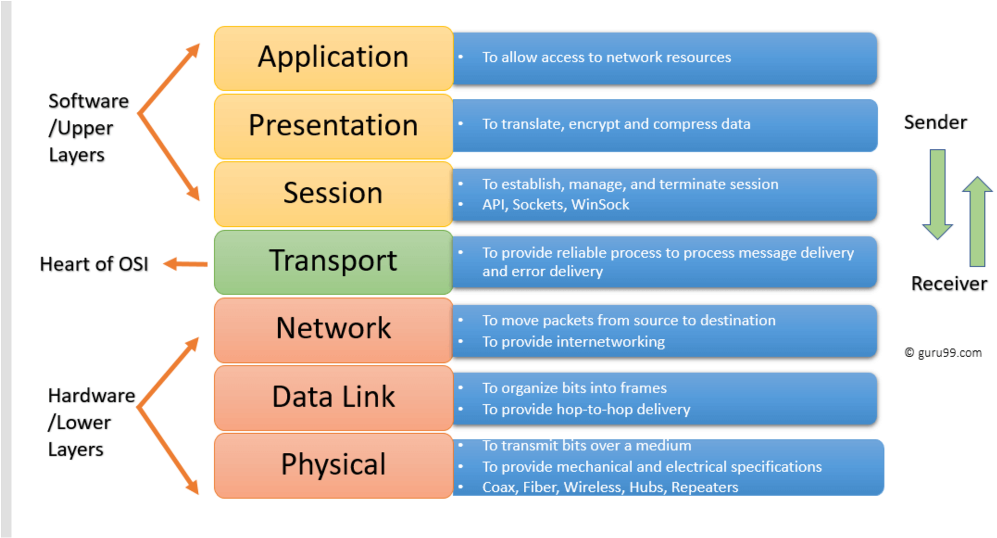
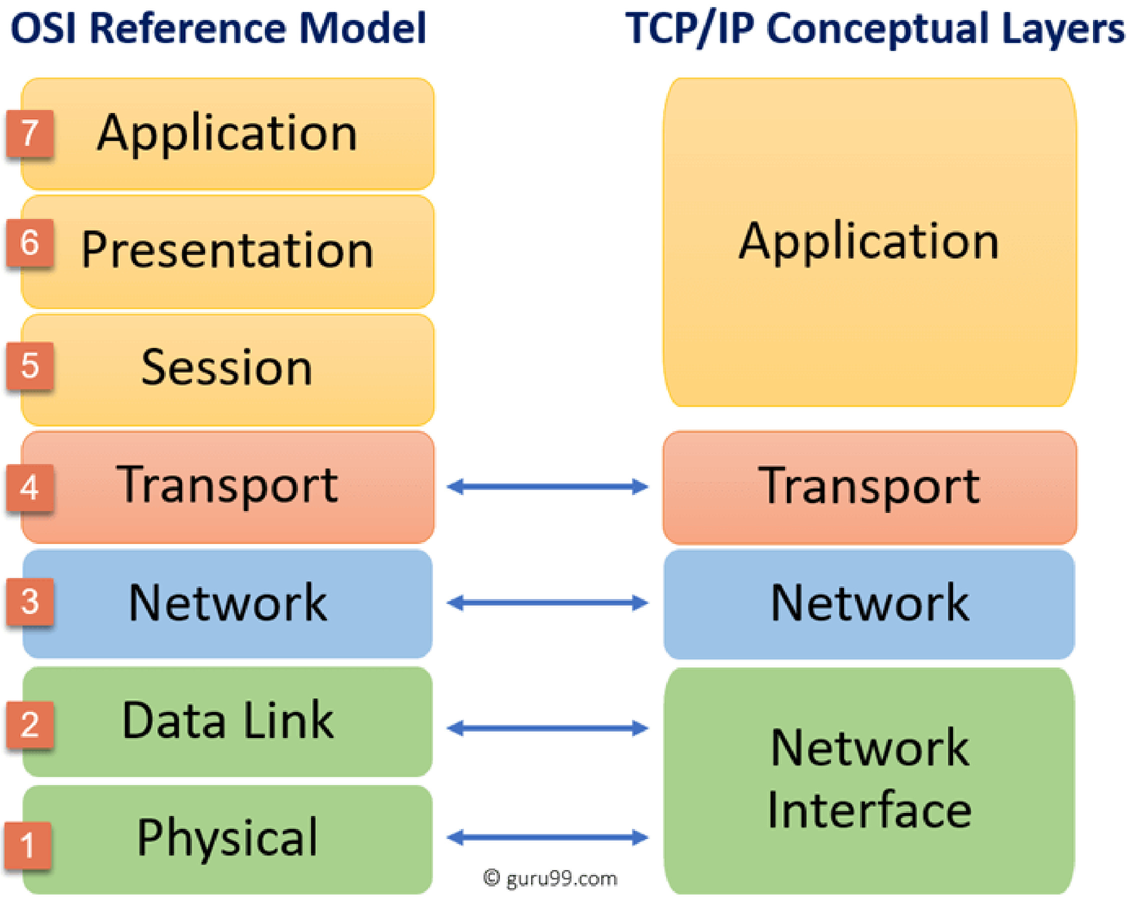
# Network

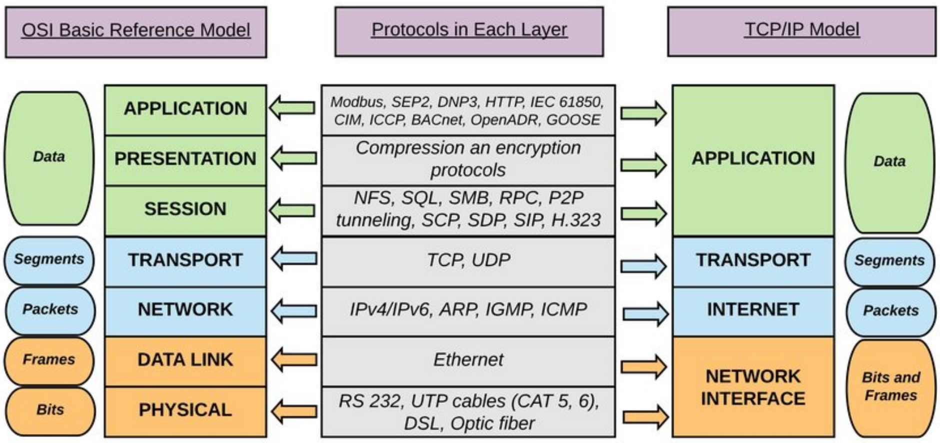
## Network OSI Model


Software /Upper Layers
Application
To allow access to network resources
Presentation
To translate, encrypt and compress data
Session
To establish, manage, and terminate session
API, Sockets, WinSock
Heart of OSI
Transport
To provide reliable process to process message delivery and error delivery
Network
To move packets from source to destination
To provide internetworking
Hardware /Lower Layers
Data Link
To organize bits into frames
To provide hop-to-hop delivery
Physical
To transmit bits over a medium
To provide mechanical and electrical specifications
Coax, Fiber, Wireless, Hubs, Repeaters
Sender
Receiver
© guru99.com

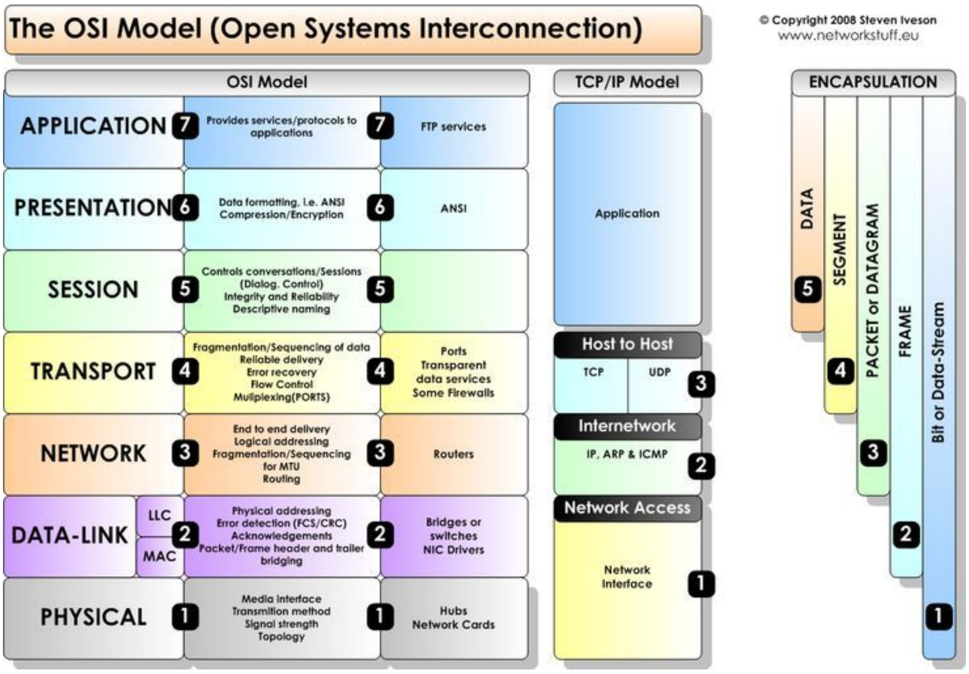
## OSI vs TCP/IP



## Application Layer - Protocol



| | OSI Basic Reference Model | Protocols in Each Layer | TCP/IP Model | |
|---|---|---|---|---|
| Data | APPLICATION | Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE | APPLICATION | Data |
| | PRESENTATION | Compression an encryption protocols | | |
| | SESSION | NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323 | | |
| Segments | TRANSPORT | TCP, UDP | TRANSPORT | Segments |
| Packets | NETWORK | IPv4/IPv6, ARP, IGMP, ICMP | INTERNET | Packets |
| Frames | DATA LINK | Ethernet | NETWORK INTERFACE | Bits and Frames |
| Bits | PHYSICAL | RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber | | |



The OSI Model (Open Systems Interconnection)

© Copyright 2008 Steven Iveson
www.networkstuff.eu

OSI Model

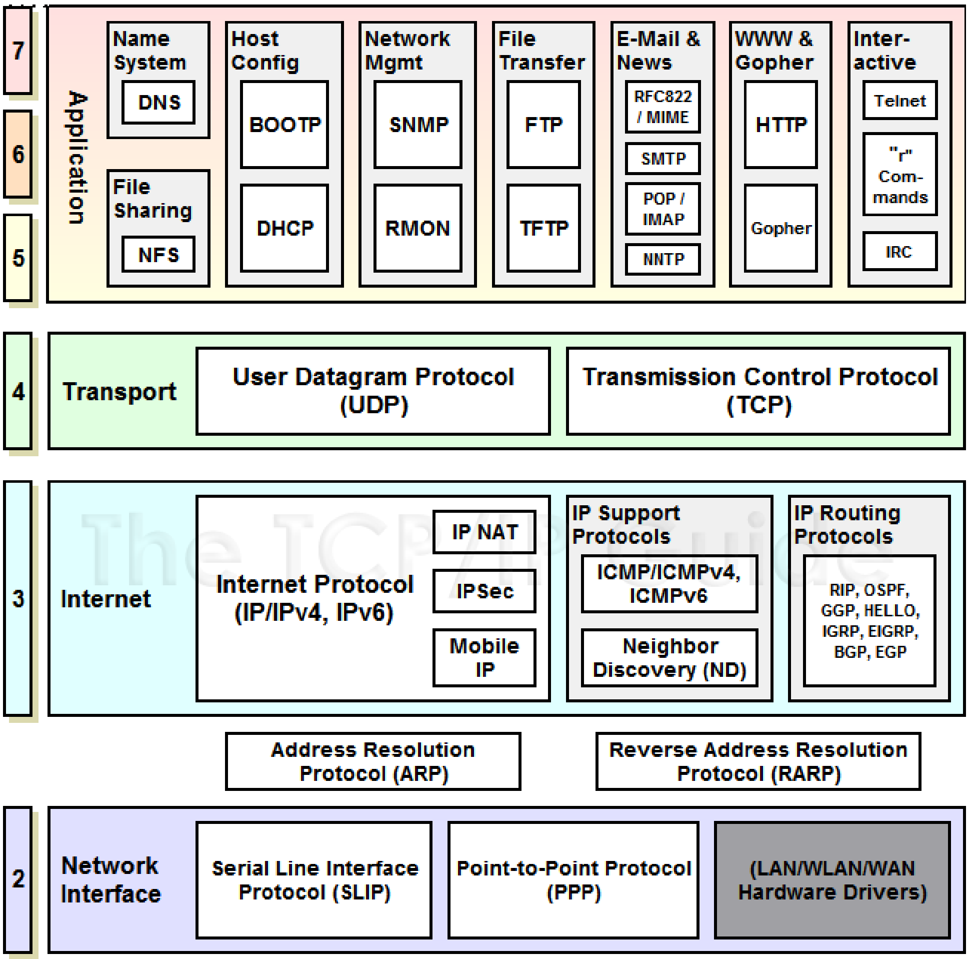
| Layer | | Function | | Examples |
|---|---|---|---|---|
| APPLICATION | 7 | Provides services/protocols to applications | 7 | FTP services |
| PRESENTATION | 6 | Data formatting, i.e. ANSI<br>Compression/Encryption | 6 | ANSI |
| SESSION | 5 | Controls conversations/Sessions<br>(Dialog. Control)<br>Integrity and Reliability<br>Descriptive naming | 5 | |
| TRANSPORT | 4 | Fragmentation/Sequencing of data<br>Reliable delivery<br>Error recovery<br>Flow Control<br>Muliplexing(PORTS) | 4 | Ports<br>Transparent data services<br>Some Firewalls |
| NETWORK | 3 | End to end delivery<br>Logical addressing<br>Fragmentation/Sequencing for MTU<br>Routing | 3 | Routers |
| DATA-LINK (LLC, MAC) | 2 | Physical addressing<br>Error detection (FCS/CRC)<br>Acknowledgements<br>Packet/Frame header and trailer<br>bridging | 2 | Bridges or switches<br>NIC Drivers |
| PHYSICAL | 1 | Media Interface<br>Transmition method<br>Signal strength<br>Topology | 1 | Hubs<br>Network Cards |

TCP/IP Model

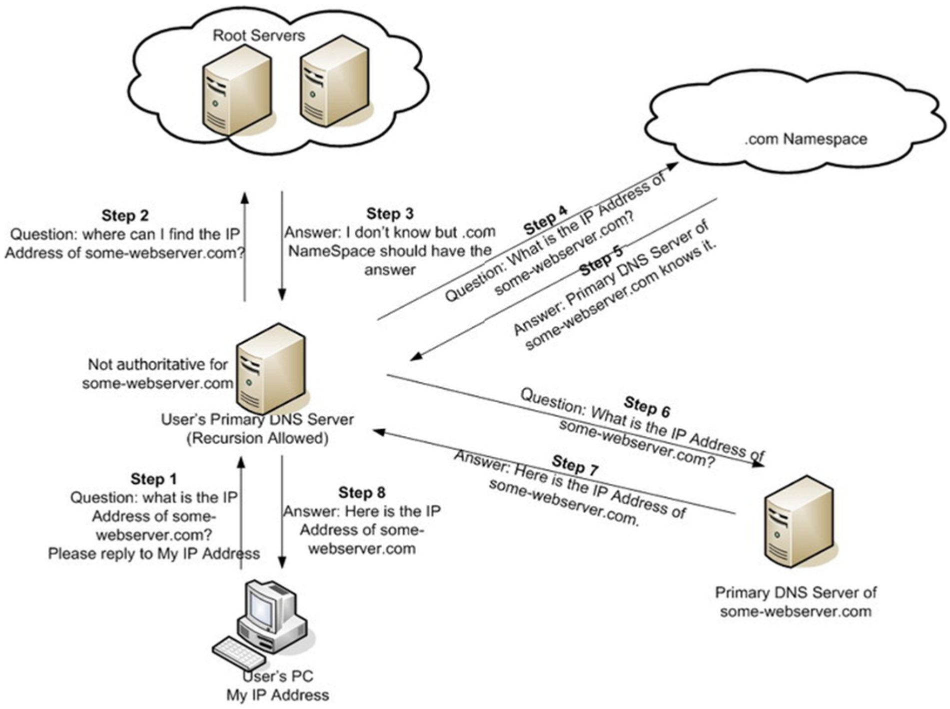
| Layer | | Contents |
|---|---|---|
| Application | | |
| Host to Host | 3 | TCP, UDP |
| Internetwork | 2 | IP, ARP & ICMP |
| Network Access | 1 | Network Interface |

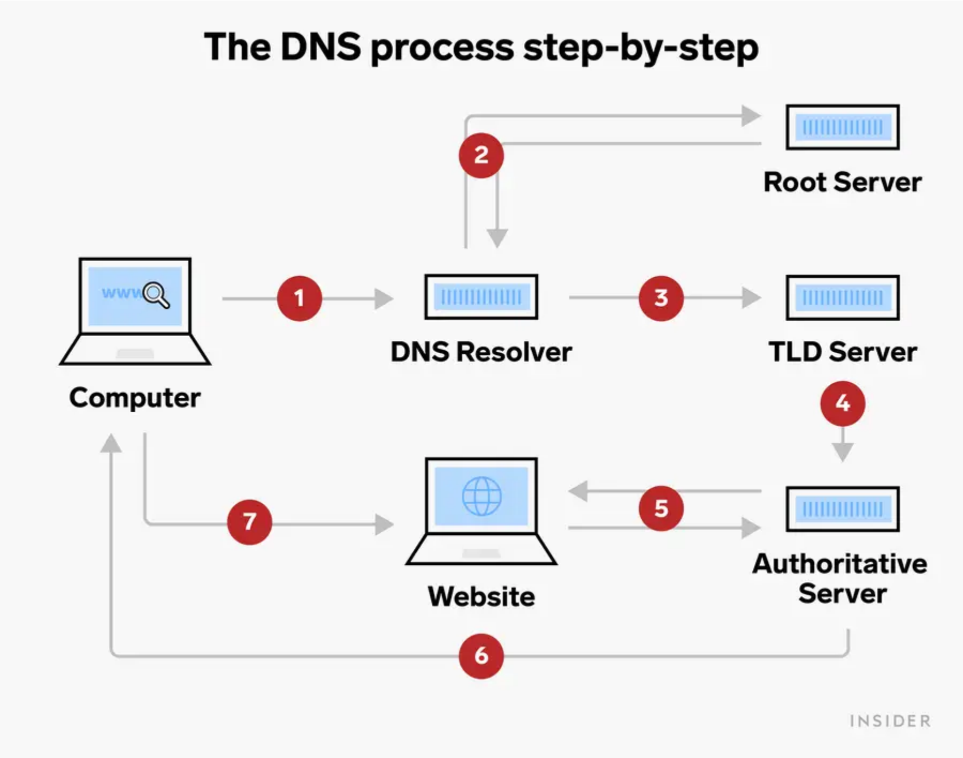
ENCAPSULATION

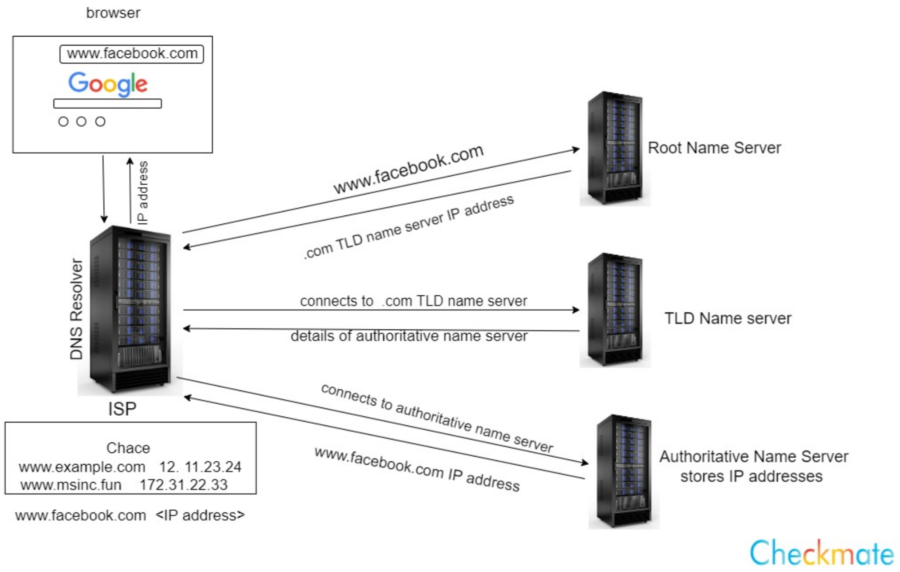
| Unit | Layer |
|---|---|
| DATA | 5 |
| SEGMENT | 4 |
| PACKET or DATAGRAM | 3 |
| FRAME | 2 |
| Bit or Data-Stream | 1 |

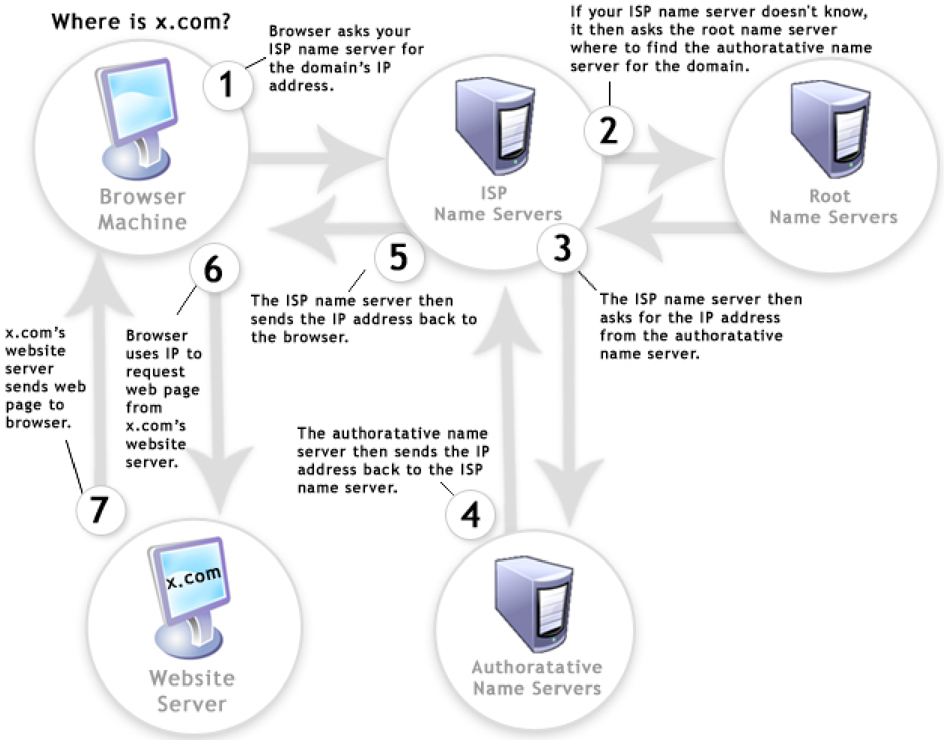


# Application Layer - DNS(Domain Name System)

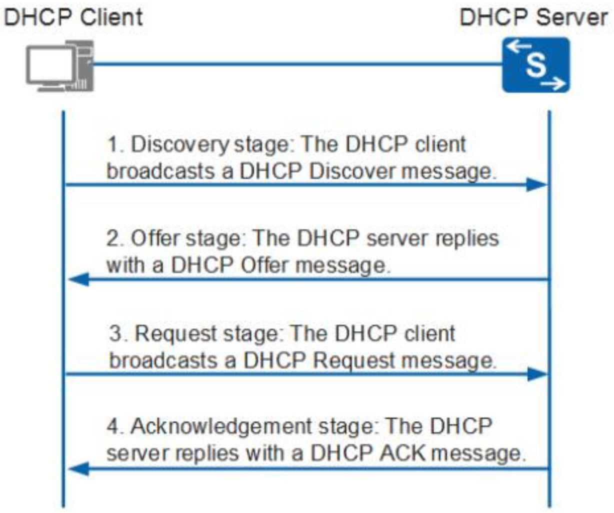

Root Servers
.com Namespace
Step 2
Question: where can I find the IP Address of some-webserver.com?
Step 3
Answer: I don't know but .com NameSpace should have the answer
Step 4
Question: What is the IP Address of some-webserver.com?
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.
Not authoritative for some-webserver.com
User's Primary DNS Server (Recursion Allowed)
Step 6
Question: What is the IP Address of some-webserver.com?
Step 7
Answer: Here is the IP Address of some-webserver.com.
Step 1
Question: what is the IP Address of some-webserver.com? Please reply to My IP Address
Step 8
Answer: Here is the IP Address of some-webserver.com
Primary DNS Server of some-webserver.com
User's PC
My IP Address

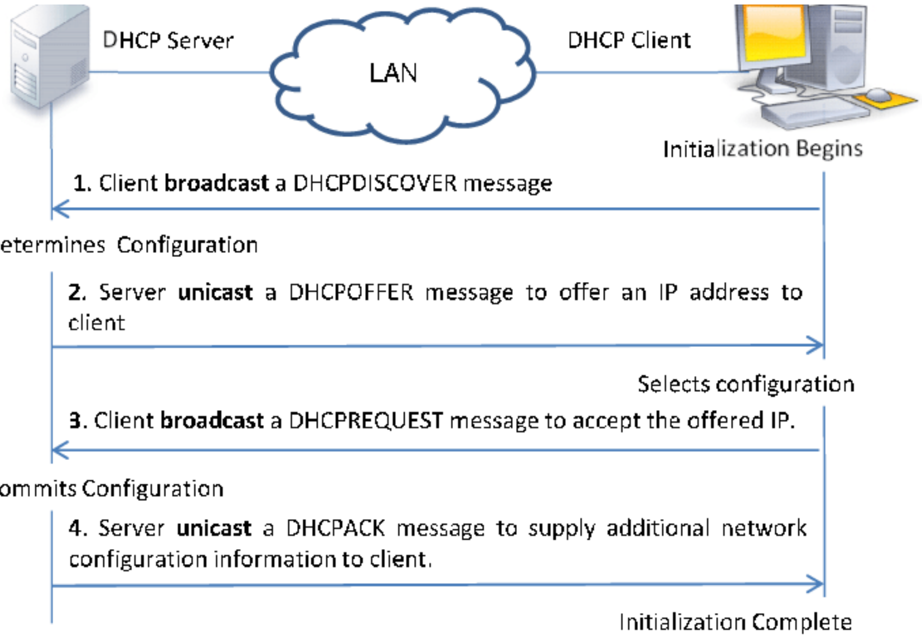

The DNS process step-by-step
Root Server
Computer
DNS Resolver
TLD Server
Website
Authoritative Server
1
2
3
4
5
6
7
www
INSIDER


browser
www.facebook.com
Google
IP address
DNS Resolver
ISP
Chace
www.example.com 12. 11.23.24
www.msinc.fun 172.31.22.33
www.facebook.com <IP address>
www.facebook.com
.com TLD name server IP address
Root Name Server
connects to .com TLD name server
details of authoritative name server
TLD Name server
connects to authoritative name server
www.facebook.com IP address
Authoritative Name Server
stores IP addresses
Checkmate


Where is x.com?
1
Browser asks your ISP name server for the domain's IP address.
If your ISP name server doesn't know, it then asks the root name server where to find the authoratative name server for the domain.
2
Browser Machine
ISP Name Servers
Root Name Servers
6
5
3
The ISP name server then sends the IP address back to the browser.
The ISP name server then asks for the IP address from the authoratative name server.
x.com's website server sends web page to browser.
Browser uses IP to request web page from x.com's website server.
The authoratative name server then sends the IP address back to the ISP name server.
7
4
x.com
Website Server
Authoratative Name Servers

# Application Layer - DHCP


DHCP Client
DHCP Server
S
1. Discovery stage: The DHCP client broadcasts a DHCP Discover message.
2. Offer stage: The DHCP server replies with a DHCP Offer message.
3. Request stage: The DHCP client broadcasts a DHCP Request message.
4. Acknowledgement stage: The DHCP server replies with a DHCP ACK message.



1. Client **broadcast** a DHCPDISCOVER message

Determines Configuration

2. Server **unicast** a DHCPOFFER message to offer an IP address to client

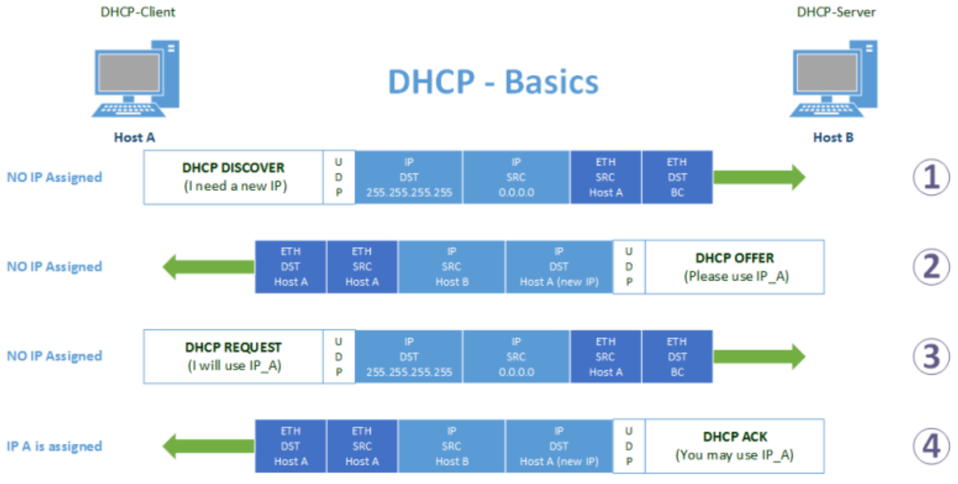
Selects configuration

3. Client **broadcast** a DHCPREQUEST message to accept the offered IP.

Commits Configuration

4. Server **unicast** a DHCPACK message to supply additional network configuration information to client.

Initialization Complete



NO IP Assigned | DHCP DISCOVER (I need a new IP) | UDP | IP DST 255.255.255.255 | IP SRC 0.0.0.0 | ETH SRC Host A | ETH DST BC | ①

NO IP Assigned | ETH DST Host A | ETH SRC Host A | IP SRC Host B | IP DST Host A (new IP) | UDP | DHCP OFFER (Please use IP_A) | ②

NO IP Assigned | DHCP REQUEST (I will use IP_A) | UDP | IP DST 255.255.255.255 | IP SRC 0.0.0.0 | ETH SRC Host A | ETH DST BC | ③

IP A is assigned | ETH DST Host A | ETH SRC Host A | IP SRC Host B | IP DST Host A (new IP) | UDP | DHCP ACK (You may use IP_A) | ④

# Application Layer - APIPA

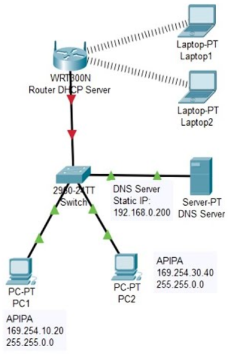
MAHA NETWORK
*All about EDUCATION*

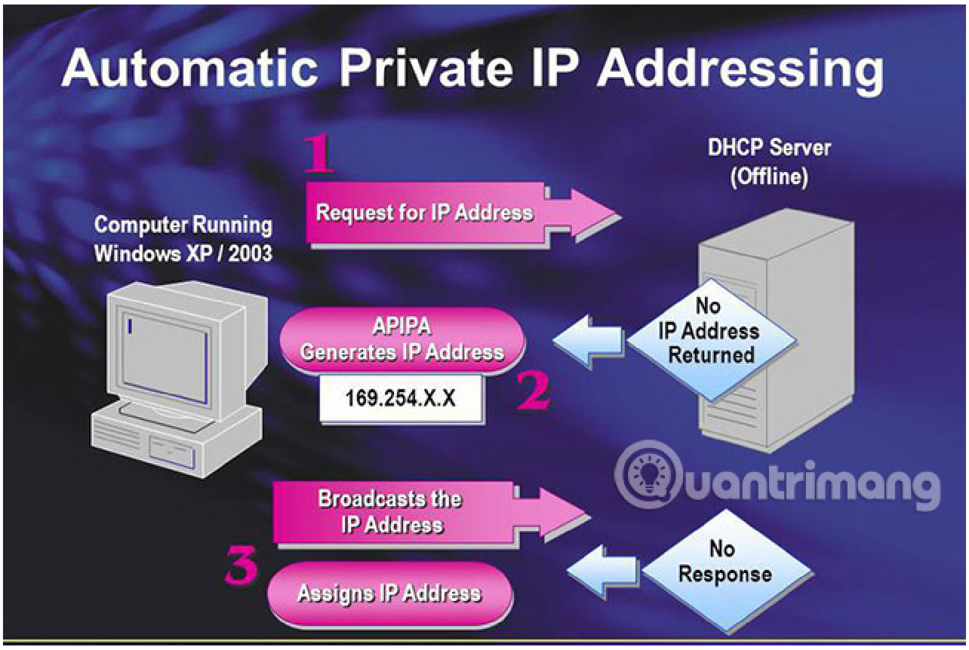
## APIPA Class B Private IP v4 Address

❖ **Automatic Private IP Address**

**169.254. x. x**

- ❑ **When connection between DHCP Server & N/W device (Switch) goes DOWN, APIPA addresses are AUTOMATICALLY created on END User Devices like Desktops, PCs, Laptops, Printers etc.**
- ❑ **END User Devices who have APIPA addresses can ONLY communicate INSIDE the own LOCAL N/W**
- ❑ **APIPA addresses DO NOT go out of their OWN N/W**
- ❑ **APIPA addresses are NOT ROUTABLE**
- ❑ **If APIPA addresses are seen on END Devices than this is a INTERNAL N/W problem**
- ❑ **Check the MEDIA or CABLE between DHCP server (Router) & N/W device (Switch) inside LOCAL N/W**





# Automatic Private IP Addressing

1

Request for IP Address

DHCP Server (Offline)

Computer Running Windows XP / 2003

APIPA Generates IP Address

169.254.X.X

2

No IP Address Returned

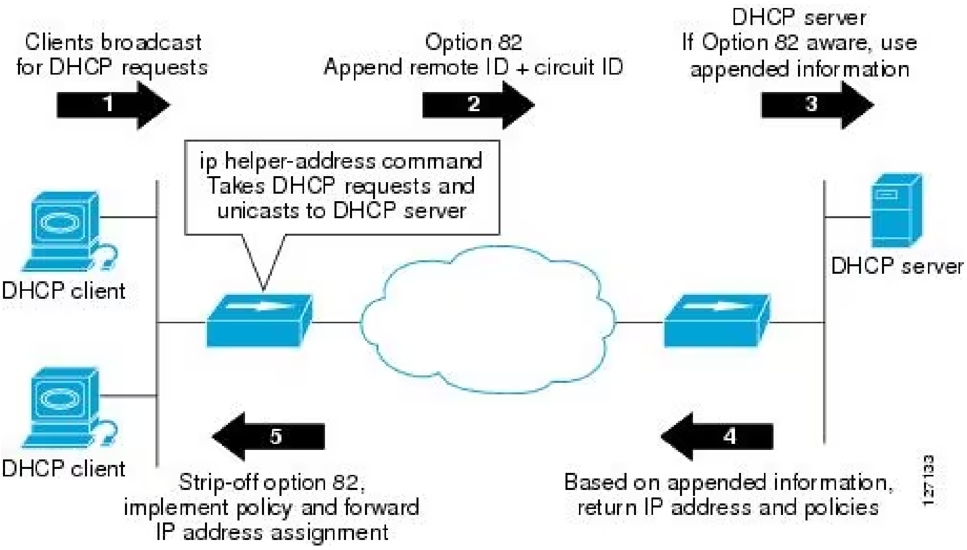
Broadcasts the IP Address

3

Assigns IP Address

No Response

# Application Layer - DHCP Relay = IP Helper



Clients broadcast for DHCP requests

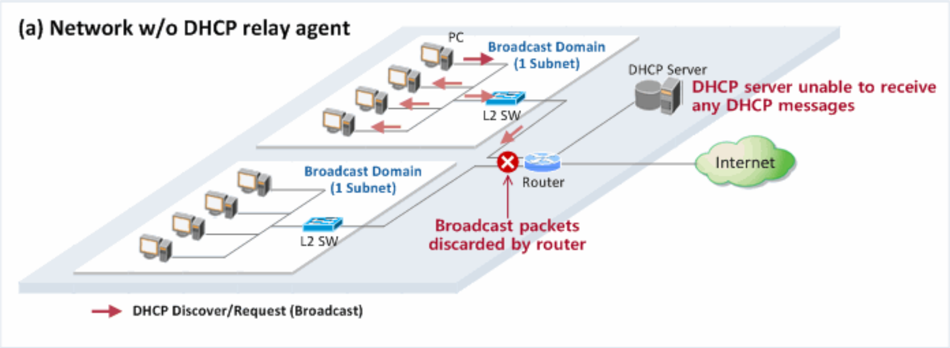
Option 82
Append remote ID + circuit ID

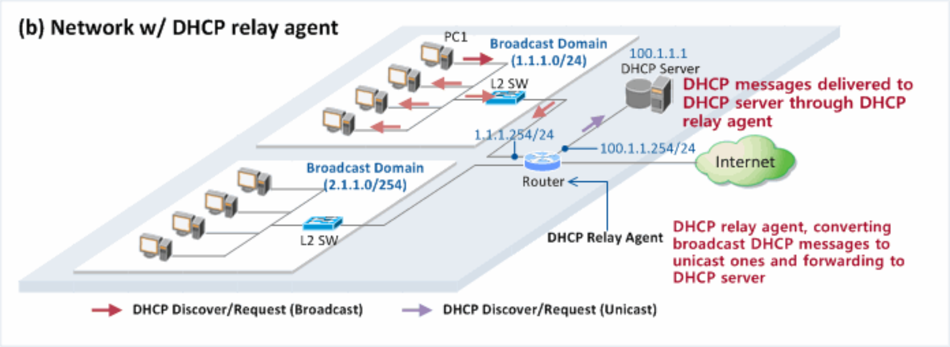
DHCP server
If Option 82 aware, use appended information

ip helper-address command
Takes DHCP requests and unicasts to DHCP server

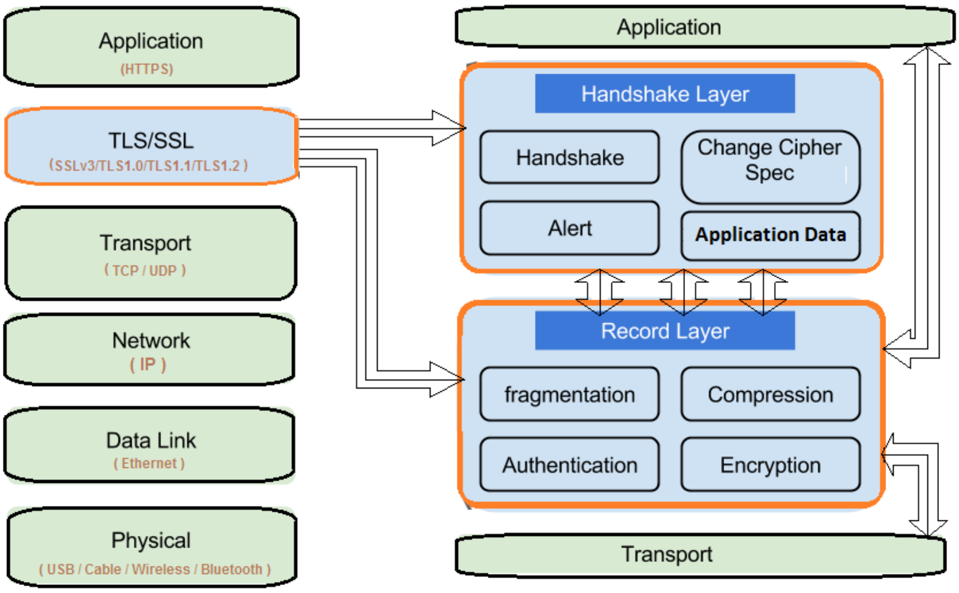
Strip-off option 82, implement policy and forward IP address assignment

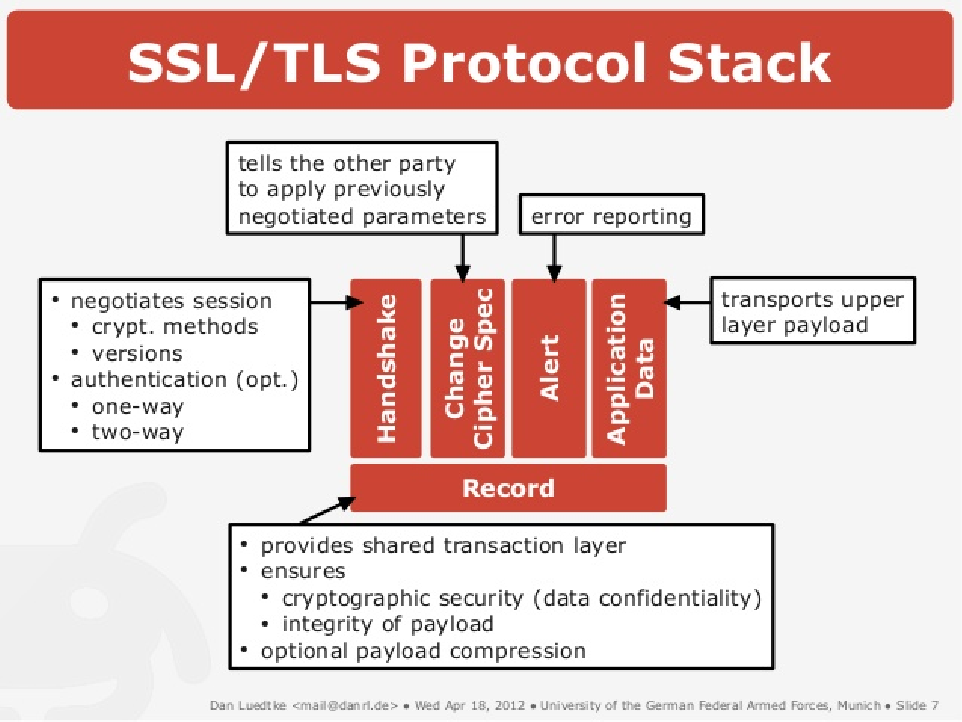
Based on appended information, return IP address and policies


(a) Network w/o DHCP relay agent
PC
Broadcast Domain (1 Subnet)
L2 SW
DHCP Server
DHCP server unable to receive any DHCP messages
Router
Internet
Broadcast Domain (1 Subnet)
L2 SW
Broadcast packets discarded by router
DHCP Discover/Request (Broadcast)


(b) Network w/ DHCP relay agent
PC1
Broadcast Domain (1.1.1.0/24)
L2 SW
100.1.1.1
DHCP Server
DHCP messages delivered to DHCP server through DHCP relay agent
1.1.1.254/24
100.1.1.254/24
Internet
Broadcast Domain (2.1.1.0/254)
Router
L2 SW
DHCP Relay Agent
DHCP relay agent, converting broadcast DHCP messages to unicast ones and forwarding to DHCP server
DHCP Discover/Request (Broadcast)
DHCP Discover/Request (Unicast)

# CyberSecurity - SSL and TLS





## SSL/TLS Protocol Stack

Handshake

Change Cipher Spec

Alert

Application Data

Record

tells the other party to apply previously negotiated parameters

error reporting

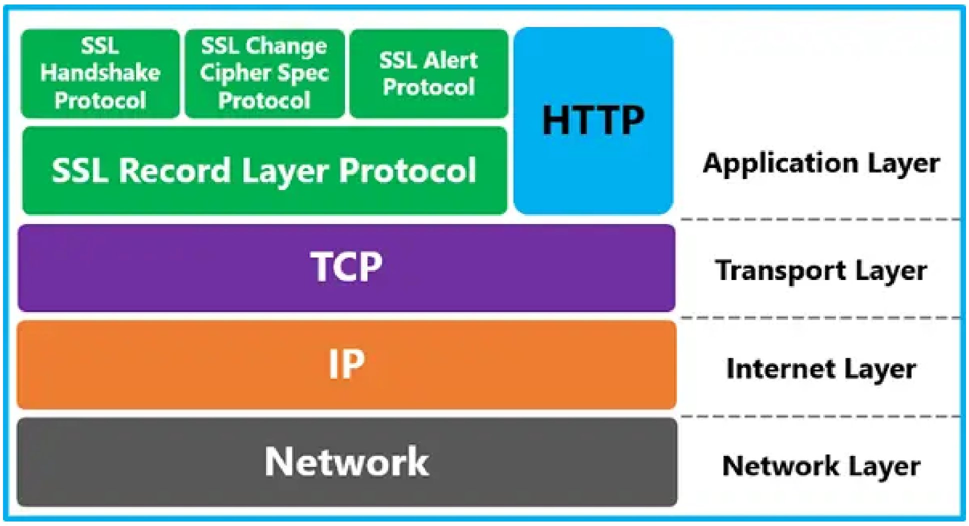
- negotiates session
  - crypt. methods
  - versions
- authentication (opt.)
  - one-way
  - two-way

transports upper layer payload

- provides shared transaction layer
- ensures
  - cryptographic security (data confidentiality)
  - integrity of payload
- optional payload compression

Dan Luedtke <mail@danrl.de> • Wed Apr 18, 2012 • University of the German Federal Armed Forces, Munich • Slide 7

# SSL(Secure Sockets Layers)



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

SSL Record Layer Protocol

Application Layer

TCP

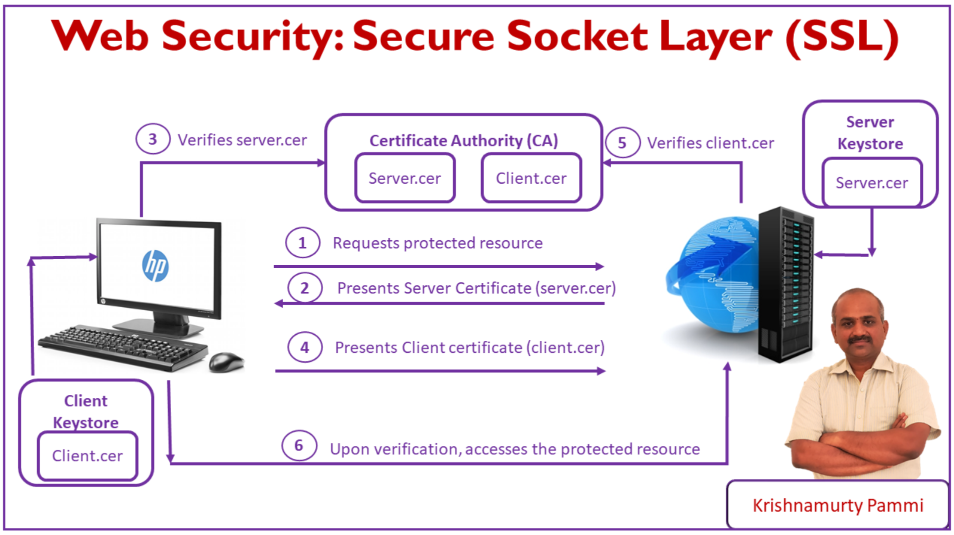
Transport Layer

IP

Internet Layer

Network

Network Layer



## Web Security: Secure Socket Layer (SSL)

Certificate Authority (CA)

Server.cer

Client.cer

Server Keystore

Server.cer

Client Keystore

Client.cer

3 Verifies server.cer

5 Verifies client.cer

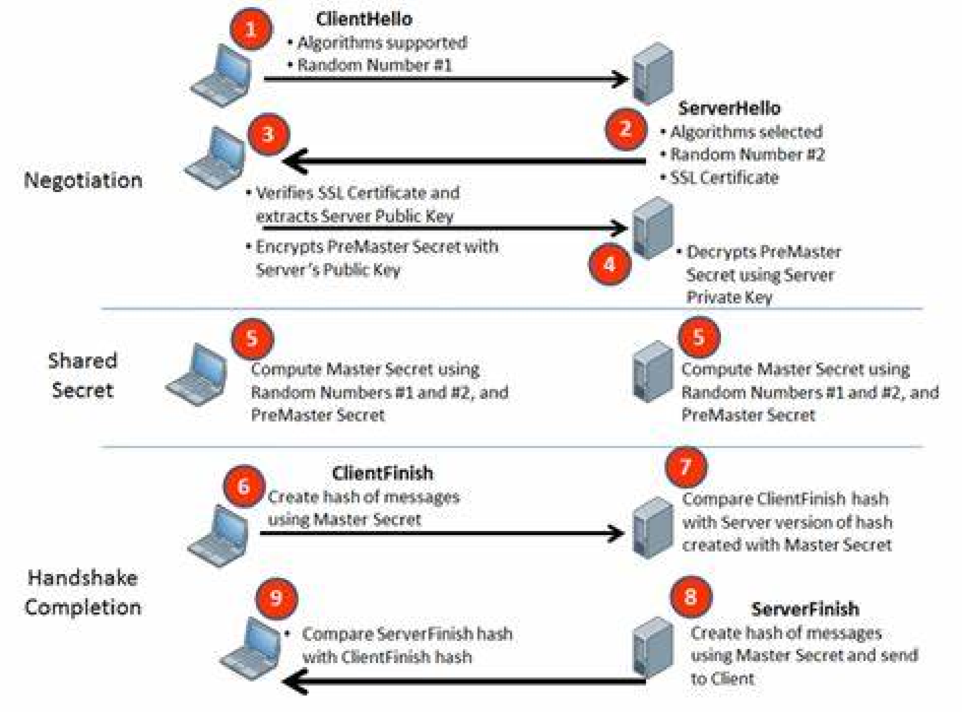
1 Requests protected resource

2 Presents Server Certificate (server.cer)

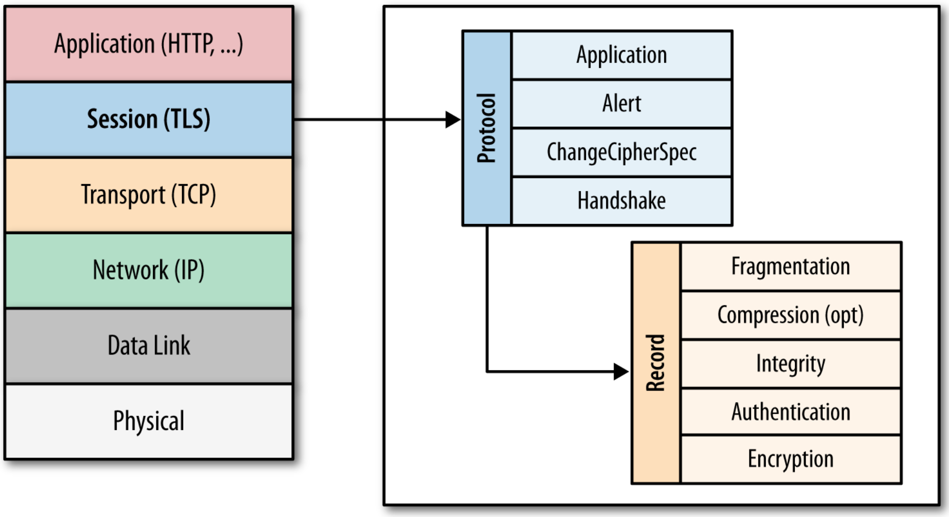
4 Presents Client certificate (client.cer)

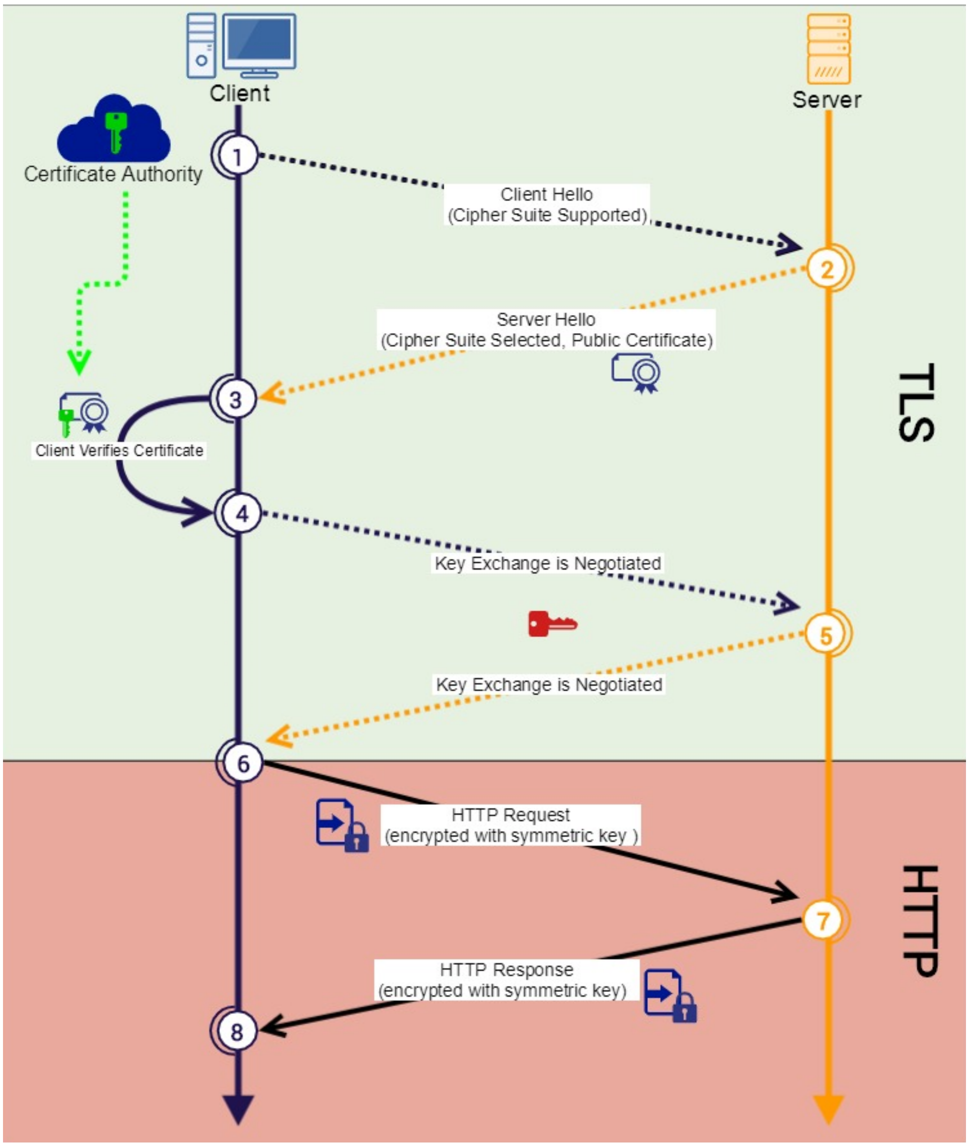
6 Upon verification, accesses the protected resource

Krishnamurty Pammi

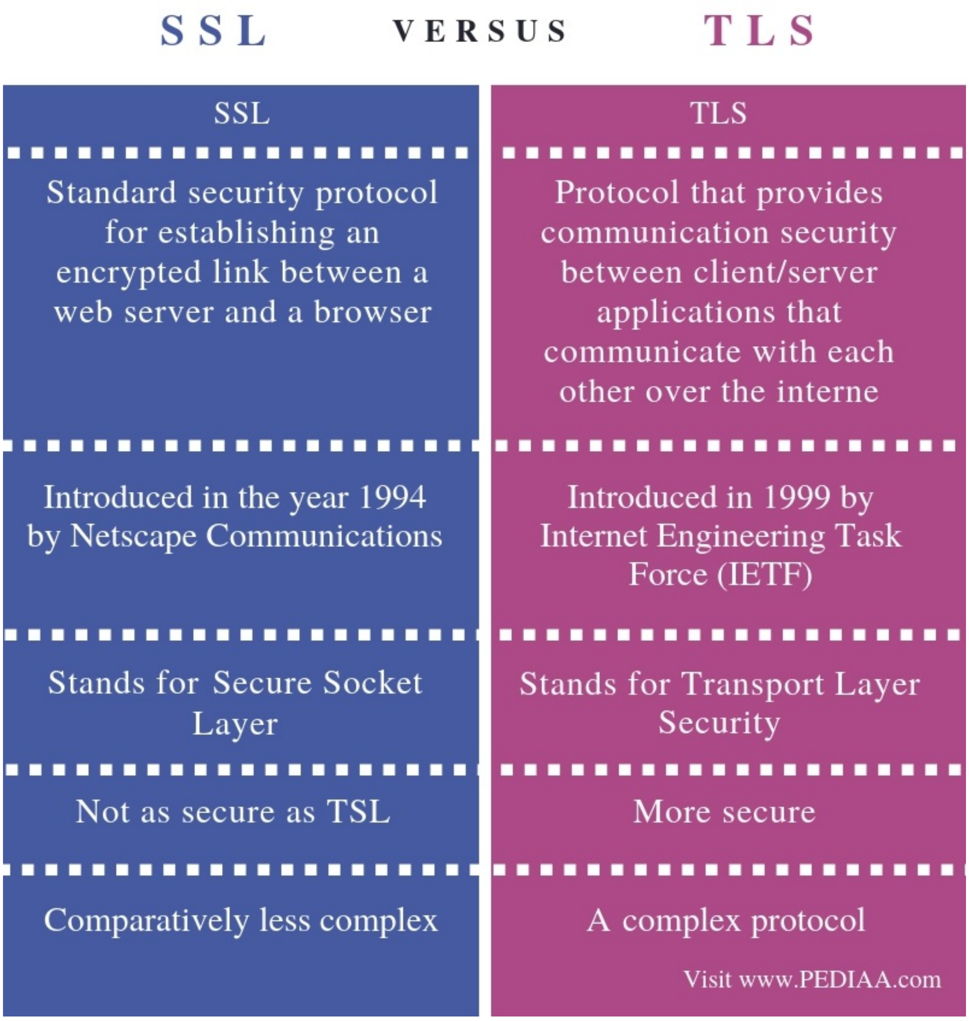

Negotiation
1 ClientHello
• Algorithms supported
• Random Number #1
2 ServerHello
• Algorithms selected
• Random Number #2
• SSL Certificate
3
• Verifies SSL Certificate and extracts Server Public Key
• Encrypts PreMaster Secret with Server's Public Key
4
• Decrypts PreMaster Secret using Server Private Key
Shared Secret
5 Compute Master Secret using Random Numbers #1 and #2, and PreMaster Secret
5 Compute Master Secret using Random Numbers #1 and #2, and PreMaster Secret
Handshake Completion
6 ClientFinish
Create hash of messages using Master Secret
7 Compare ClientFinish hash with Server version of hash created with Master Secret
8 ServerFinish
Create hash of messages using Master Secret and send to Client
9 • Compare ServerFinish hash with ClientFinish hash

# TLS(Transport Layer Security)




Client
Server
Certificate Authority
1
Client Hello
(Cipher Suite Supported)
2
Server Hello
(Cipher Suite Selected, Public Certificate)
3
Client Verifies Certificate
4
Key Exchange is Negotiated
5
Key Exchange is Negotiated
TLS
6
HTTP Request
(encrypted with symmetric key )
7
HTTP Response
(encrypted with symmetric key)
8
HTTP

## SSL vs TSL

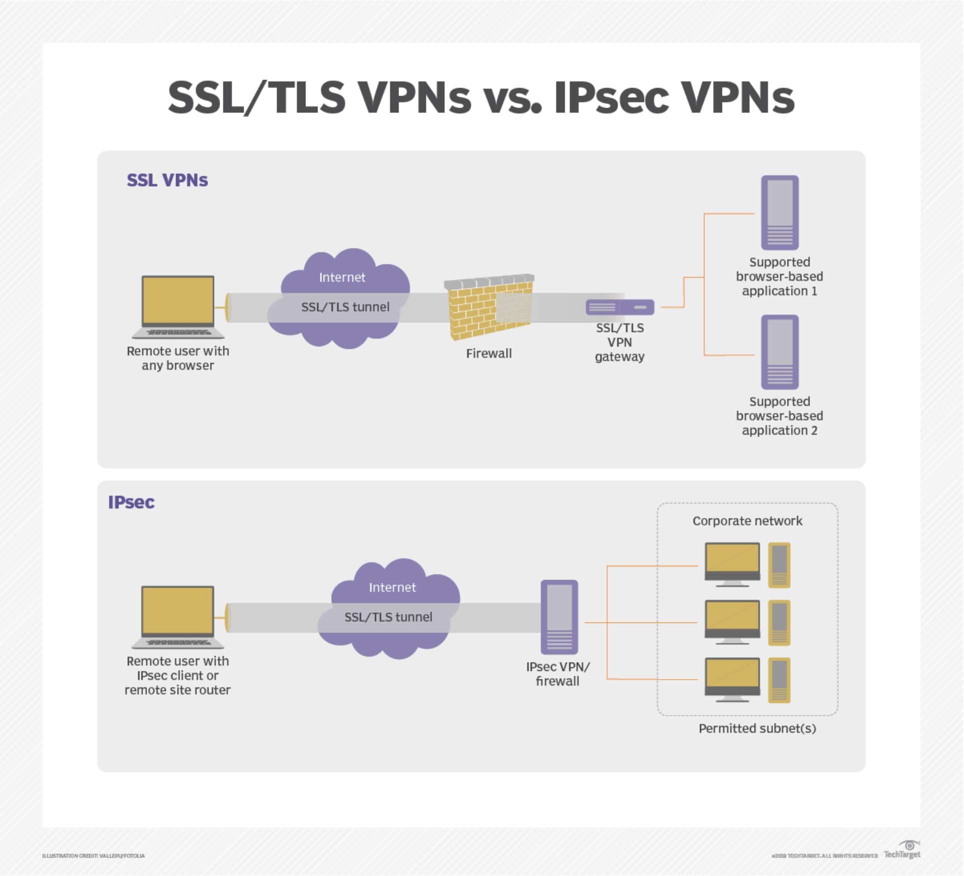


SSL VERSUS TLS

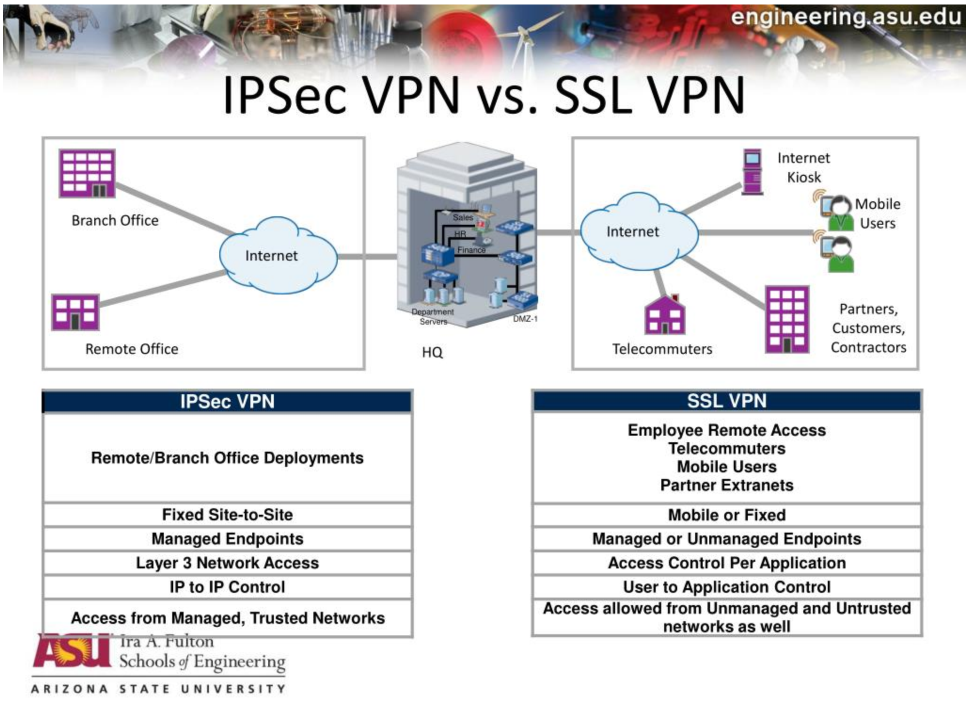
| SSL | TLS |
|---|---|
| Standard security protocol for establishing an encrypted link between a web server and a browser | Protocol that provides communication security between client/server applications that communicate with each other over the interne |
| Introduced in the year 1994 by Netscape Communications | Introduced in 1999 by Internet Engineering Task Force (IETF) |
| Stands for Secure Socket Layer | Stands for Transport Layer Security |
| Not as secure as TSL | More secure |
| Comparatively less complex | A complex protocol |

Visit www.PEDIAA.com

## CyberSecurity for VPN



SSL/TLS VPNs vs. IPsec VPNs
SSL VPNs
Remote user with any browser
Internet
SSL/TLS tunnel
Firewall
SSL/TLS VPN gateway
Supported browser-based application 1
Supported browser-based application 2
IPsec
Remote user with IPsec client or remote site router
Internet
SSL/TLS tunnel
IPsec VPN/ firewall
Corporate network
Permitted subnet(s)
ILLUSTRATION CREDIT: VALLEPU/FOTOLIA
©2019 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

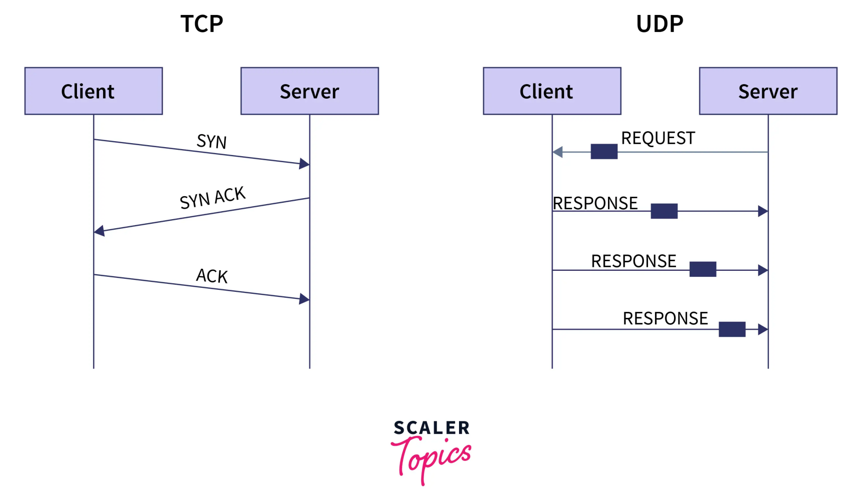


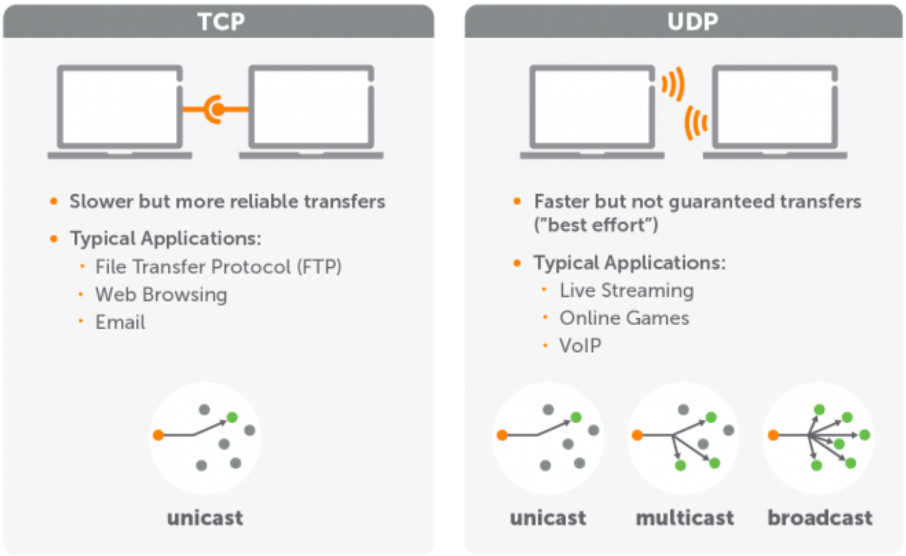
IPSec VPN vs. SSL VPN

| IPSec VPN |
|---|
| Remote/Branch Office Deployments |
| Fixed Site-to-Site |
| Managed Endpoints |
| Layer 3 Network Access |
| IP to IP Control |
| Access from Managed, Trusted Networks |

| SSL VPN |
|---|
| Employee Remote Access<br>Telecommuters<br>Mobile Users<br>Partner Extranets |
| Mobile or Fixed |
| Managed or Unmanaged Endpoints |
| Access Control Per Application |
| User to Application Control |
| Access allowed from Unmanaged and Untrusted networks as well |

# Transport Layer - TCP vs UDP



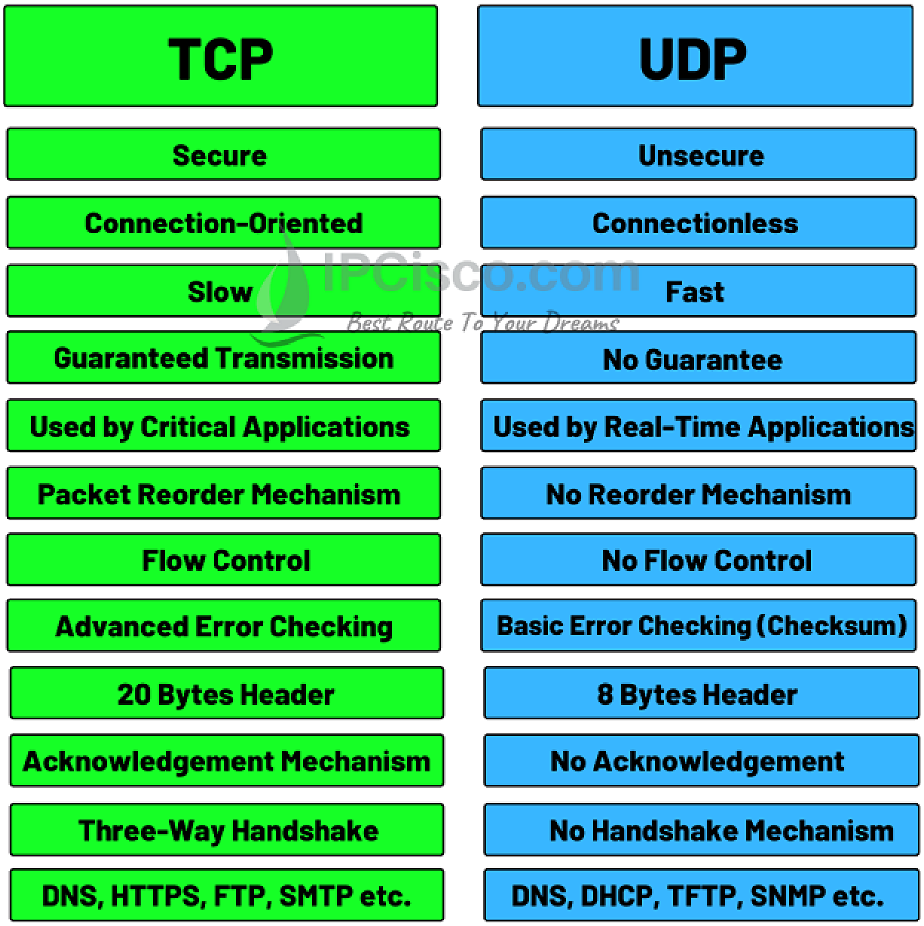


**TCP**

- Slower but more reliable transfers
- Typical Applications:
  - File Transfer Protocol (FTP)
  - Web Browsing
  - Email

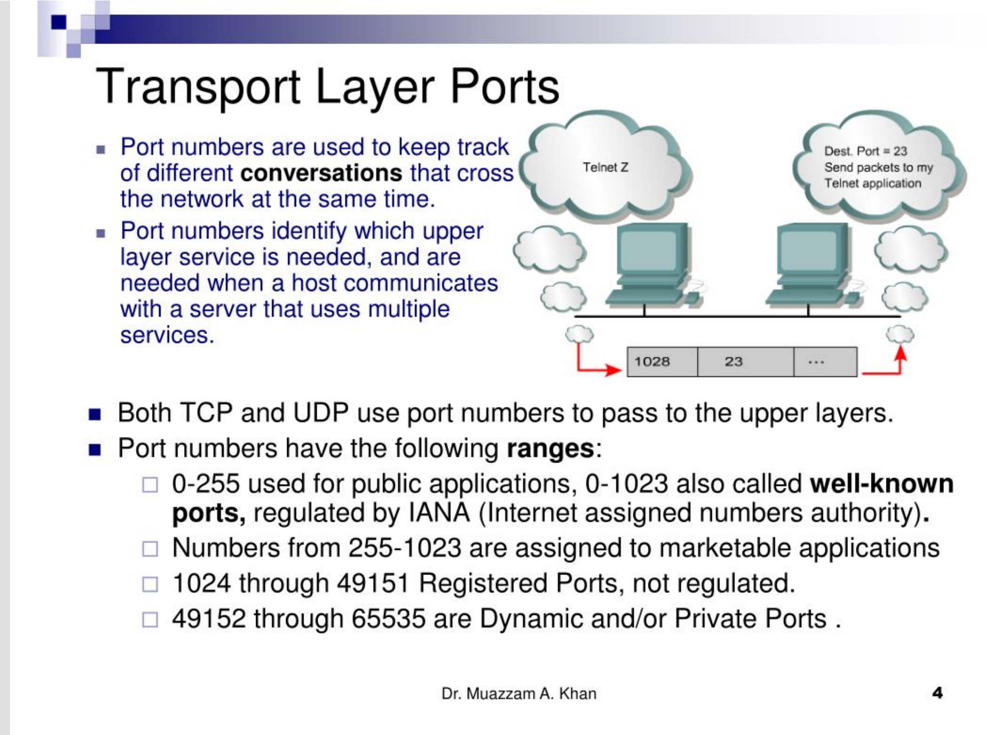
**UDP**

- Faster but not guaranteed transfers ("best effort")
- Typical Applications:
  - Live Streaming
  - Online Games
  - VoIP



| TCP | UDP |
|---|---|
| Secure | Unsecure |
| Connection-Oriented | Connectionless |
| Slow | Fast |
| Guaranteed Transmission | No Guarantee |
| Used by Critical Applications | Used by Real-Time Applications |
| Packet Reorder Mechanism | No Reorder Mechanism |
| Flow Control | No Flow Control |
| Advanced Error Checking | Basic Error Checking (Checksum) |
| 20 Bytes Header | 8 Bytes Header |
| Acknowledgement Mechanism | No Acknowledgement |
| Three-Way Handshake | No Handshake Mechanism |
| DNS, HTTPS, FTP, SMTP etc. | DNS, DHCP, TFTP, SNMP etc. |

## Transport Layer - TCP/UDP Port

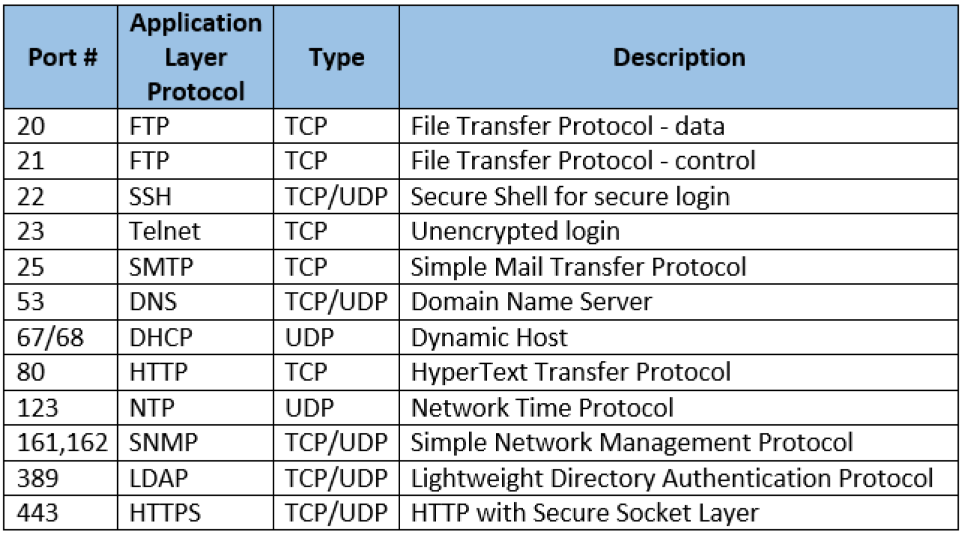


# Transport Layer Ports

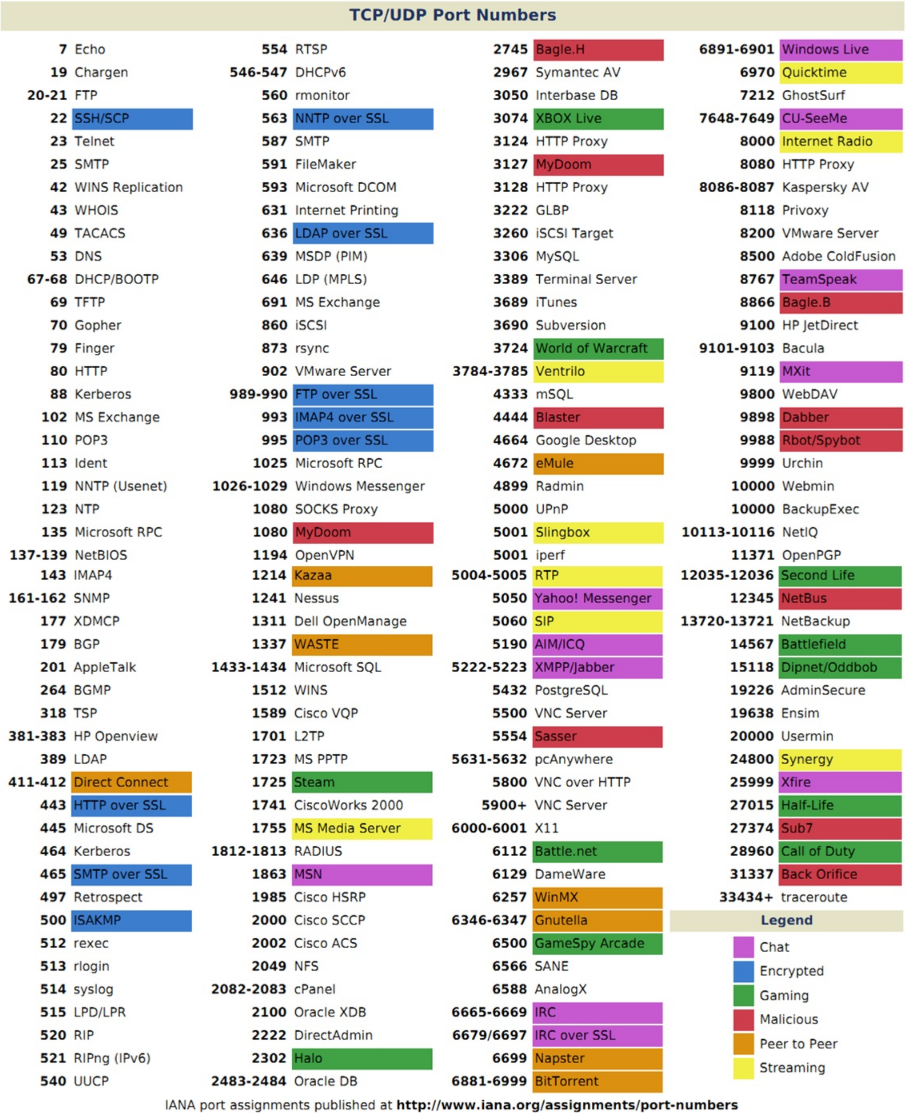
- Port numbers are used to keep track of different **conversations** that cross the network at the same time.
- Port numbers identify which upper layer service is needed, and are needed when a host communicates with a server that uses multiple services.

Telnet Z
Dest. Port = 23
Send packets to my
Telnet application
1028
23
...

- Both TCP and UDP use port numbers to pass to the upper layers.
- Port numbers have the following **ranges**:
  - □ 0-255 used for public applications, 0-1023 also called **well-known ports,** regulated by IANA (Internet assigned numbers authority)**.**
  - □ Numbers from 255-1023 are assigned to marketable applications
  - □ 1024 through 49151 Registered Ports, not regulated.
  - □ 49152 through 65535 are Dynamic and/or Private Ports .



| Port # | Application Layer Protocol | Type | Description |
|---|---|---|---|
| 20 | FTP | TCP | File Transfer Protocol - data |
| 21 | FTP | TCP | File Transfer Protocol - control |
| 22 | SSH | TCP/UDP | Secure Shell for secure login |
| 23 | Telnet | TCP | Unencrypted login |
| 25 | SMTP | TCP | Simple Mail Transfer Protocol |
| 53 | DNS | TCP/UDP | Domain Name Server |
| 67/68 | DHCP | UDP | Dynamic Host |
| 80 | HTTP | TCP | HyperText Transfer Protocol |
| 123 | NTP | UDP | Network Time Protocol |
| 161,162 | SNMP | TCP/UDP | Simple Network Management Protocol |
| 389 | LDAP | TCP/UDP | Lightweight Directory Authentication Protocol |
| 443 | HTTPS | TCP/UDP | HTTP with Secure Socket Layer |

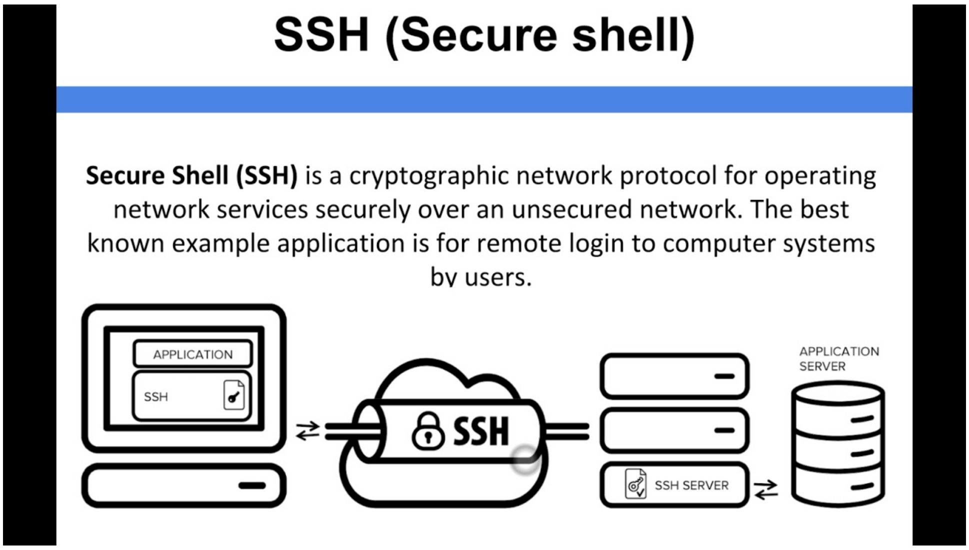


### TCP/UDP Port Numbers

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | Echo | 554 | RTSP | 2745 | 🟥 Bagle.H | 6891-6901 | 🟪 Windows Live |
| 19 | Chargen | 546-547 | DHCPv6 | 2967 | Symantec AV | 6970 | 🟨 Quicktime |
| 20-21 | FTP | 560 | rmonitor | 3050 | Interbase DB | 7212 | GhostSurf |
| 22 | 🟦 SSH/SCP | 563 | 🟦 NNTP over SSL | 3074 | 🟩 XBOX Live | 7648-7649 | 🟪 CU-SeeMe |
| 23 | Telnet | 587 | SMTP | 3124 | HTTP Proxy | 8000 | 🟨 Internet Radio |
| 25 | SMTP | 591 | FileMaker | 3127 | 🟥 MyDoom | 8080 | HTTP Proxy |
| 42 | WINS Replication | 593 | Microsoft DCOM | 3128 | HTTP Proxy | 8086-8087 | Kaspersky AV |
| 43 | WHOIS | 631 | Internet Printing | 3222 | GLBP | 8118 | Privoxy |
| 49 | TACACS | 636 | 🟦 LDAP over SSL | 3260 | iSCSI Target | 8200 | VMware Server |
| 53 | DNS | 639 | MSDP (PIM) | 3306 | MySQL | 8500 | Adobe ColdFusion |
| 67-68 | DHCP/BOOTP | 646 | LDP (MPLS) | 3389 | Terminal Server | 8767 | 🟪 TeamSpeak |
| 69 | TFTP | 691 | MS Exchange | 3689 | iTunes | 8866 | 🟥 Bagle.B |
| 70 | Gopher | 860 | iSCSI | 3690 | Subversion | 9100 | HP JetDirect |
| 79 | Finger | 873 | rsync | 3724 | 🟩 World of Warcraft | 9101-9103 | Bacula |
| 80 | HTTP | 902 | VMware Server | 3784-3785 | 🟨 Ventrilo | 9119 | 🟪 MXit |
| 88 | Kerberos | 989-990 | 🟦 FTP over SSL | 4333 | mSQL | 9800 | WebDAV |
| 102 | MS Exchange | 993 | 🟦 IMAP4 over SSL | 4444 | 🟥 Blaster | 9898 | 🟥 Dabber |
| 110 | POP3 | 995 | 🟦 POP3 over SSL | 4664 | Google Desktop | 9988 | 🟥 Rbot/Spybot |
| 113 | Ident | 1025 | Microsoft RPC | 4672 | 🟧 eMule | 9999 | Urchin |
| 119 | NNTP (Usenet) | 1026-1029 | Windows Messenger | 4899 | Radmin | 10000 | Webmin |
| 123 | NTP | 1080 | SOCKS Proxy | 5000 | UPnP | 10000 | BackupExec |
| 135 | Microsoft RPC | 1080 | 🟥 MyDoom | 5001 | 🟨 Slingbox | 10113-10116 | NetIQ |
| 137-139 | NetBIOS | 1194 | OpenVPN | 5001 | iperf | 11371 | OpenPGP |
| 143 | IMAP4 | 1214 | 🟧 Kazaa | 5004-5005 | 🟨 RTP | 12035-12036 | 🟩 Second Life |
| 161-162 | SNMP | 1241 | Nessus | 5050 | 🟪 Yahoo! Messenger | 12345 | 🟥 NetBus |
| 177 | XDMCP | 1311 | Dell OpenManage | 5060 | 🟨 SIP | 13720-13721 | NetBackup |
| 179 | BGP | 1337 | 🟧 WASTE | 5190 | 🟪 AIM/ICQ | 14567 | 🟩 Battlefield |
| 201 | AppleTalk | 1433-1434 | Microsoft SQL | 5222-5223 | 🟪 XMPP/Jabber | 15118 | 🟩 Dipnet/Oddbob |
| 264 | BGMP | 1512 | WINS | 5432 | PostgreSQL | 19226 | AdminSecure |
| 318 | TSP | 1589 | Cisco VQP | 5500 | VNC Server | 19638 | Ensim |
| 381-383 | HP Openview | 1701 | L2TP | 5554 | 🟥 Sasser | 20000 | Usermin |
| 389 | LDAP | 1723 | MS PPTP | 5631-5632 | pcAnywhere | 24800 | 🟨 Synergy |
| 411-412 | 🟧 Direct Connect | 1725 | 🟩 Steam | 5800 | VNC over HTTP | 25999 | 🟪 Xfire |
| 443 | 🟦 HTTP over SSL | 1741 | CiscoWorks 2000 | 5900+ | VNC Server | 27015 | 🟩 Half-Life |
| 445 | Microsoft DS | 1755 | 🟨 MS Media Server | 6000-6001 | X11 | 27374 | 🟥 Sub7 |
| 464 | Kerberos | 1812-1813 | RADIUS | 6112 | 🟩 Battle.net | 28960 | 🟩 Call of Duty |
| 465 | 🟦 SMTP over SSL | 1863 | 🟪 MSN | 6129 | DameWare | 31337 | 🟥 Back Orifice |
| 497 | Retrospect | 1985 | Cisco HSRP | 6257 | 🟧 WinMX | 33434+ | traceroute |
| 500 | 🟦 ISAKMP | 2000 | Cisco SCCP | 6346-6347 | 🟧 Gnutella | | **Legend** |
| 512 | rexec | 2002 | Cisco ACS | 6500 | 🟩 GameSpy Arcade | 🟪 | Chat |
| 513 | rlogin | 2049 | NFS | 6566 | SANE | 🟦 | Encrypted |
| 514 | syslog | 2082-2083 | cPanel | 6588 | AnalogX | 🟩 | Gaming |
| 515 | LPD/LPR | 2100 | Oracle XDB | 6665-6669 | 🟪 IRC | 🟥 | Malicious |
| 520 | RIP | 2222 | DirectAdmin | 6679/6697 | 🟪 IRC over SSL | 🟧 | Peer to Peer |
| 521 | RIPng (IPv6) | 2302 | 🟩 Halo | 6699 | 🟧 Napster | 🟨 | Streaming |
| 540 | UUCP | 2483-2484 | Oracle DB | 6881-6999 | 🟧 BitTorrent | | |

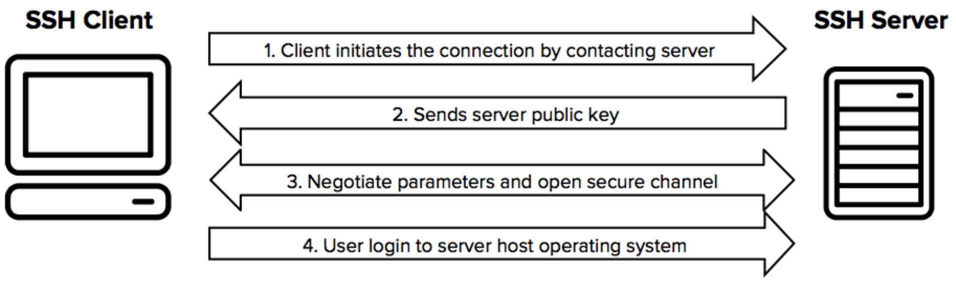
IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

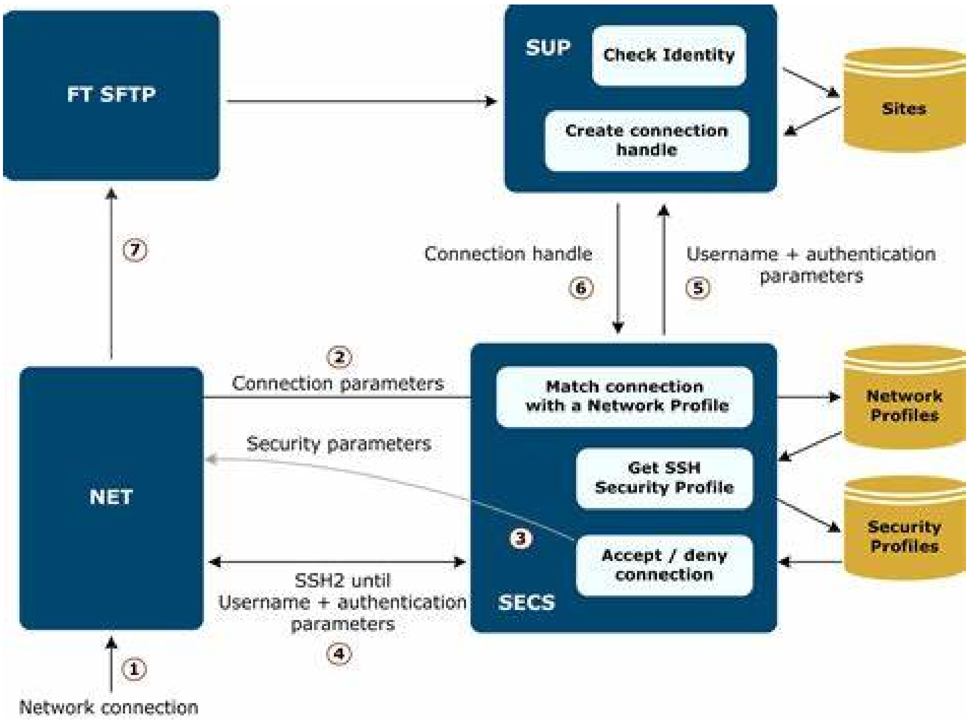
# Transport Layer - SSH(Secure Shell)



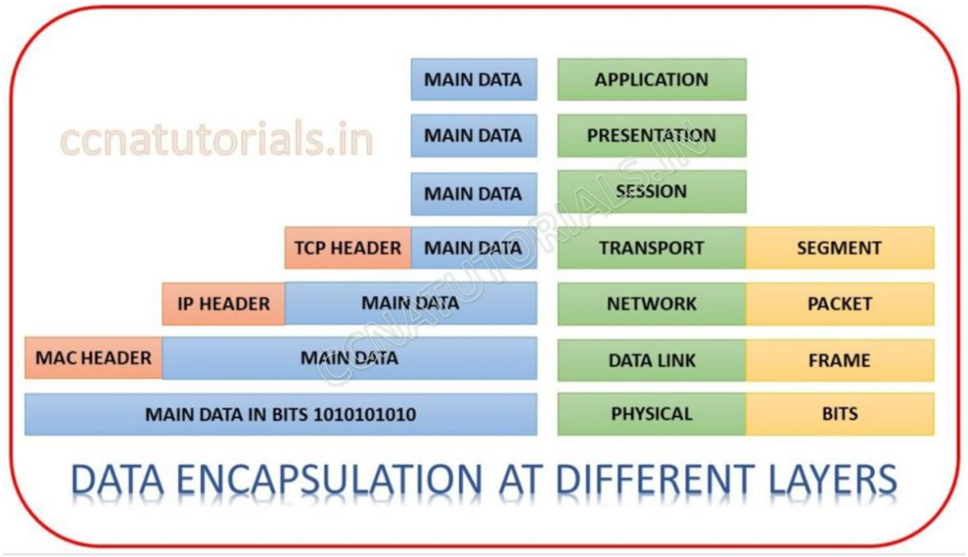
## SSH (Secure shell)

**Secure Shell (SSH)** is a cryptographic network protocol for operating network services securely over an unsecured network. The best known example application is for remote login to computer systems by users.


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

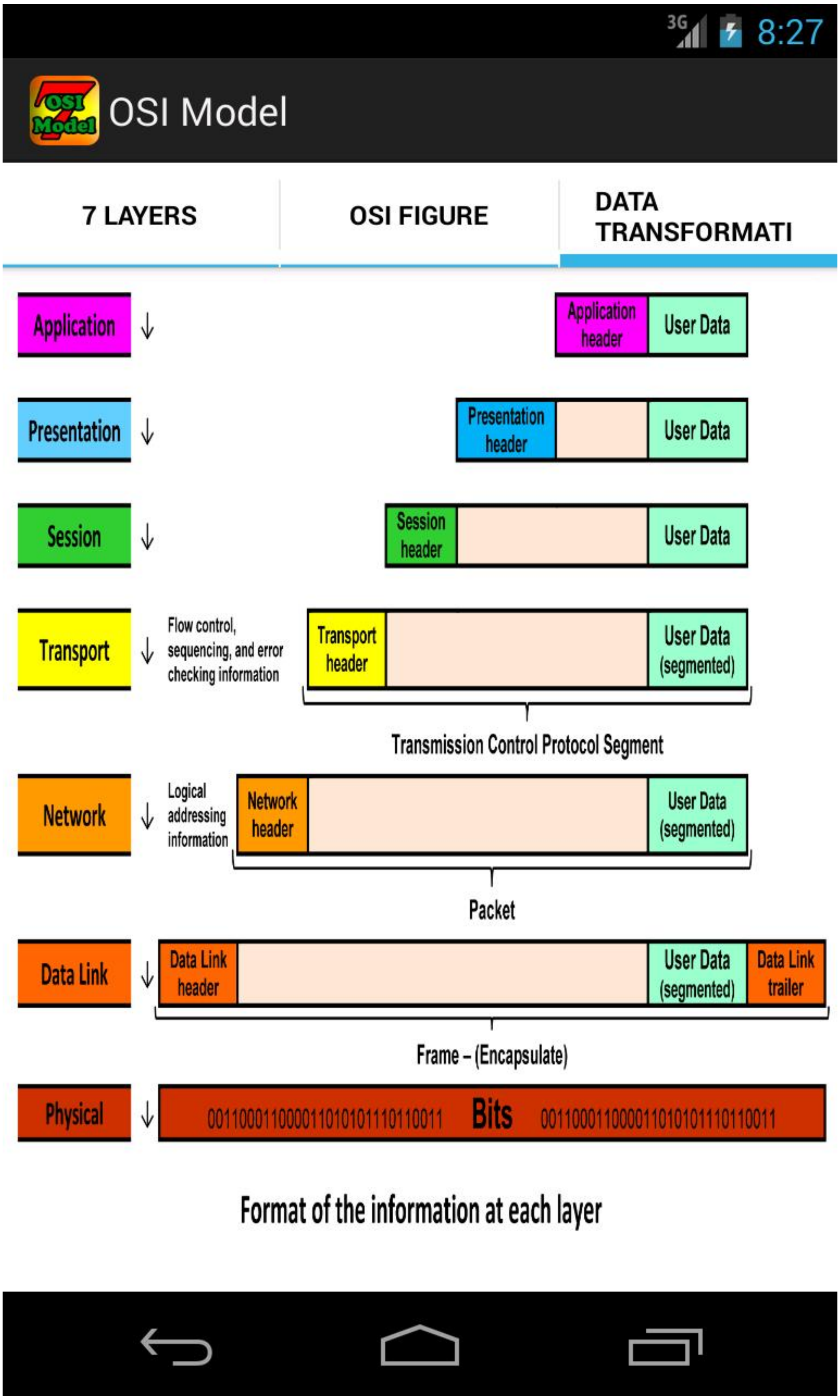


# Network Layer - Encapsulation and Communication

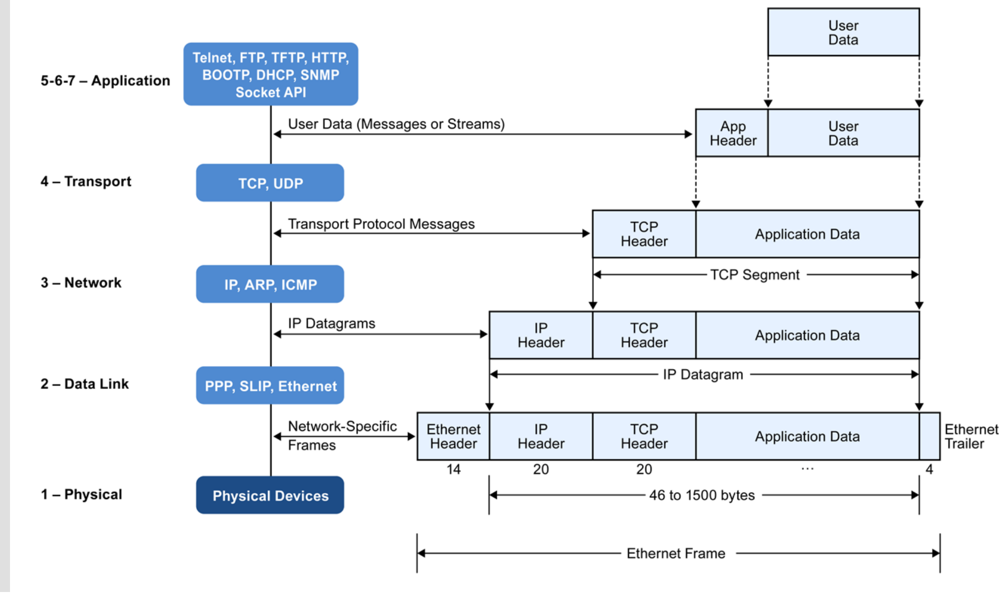


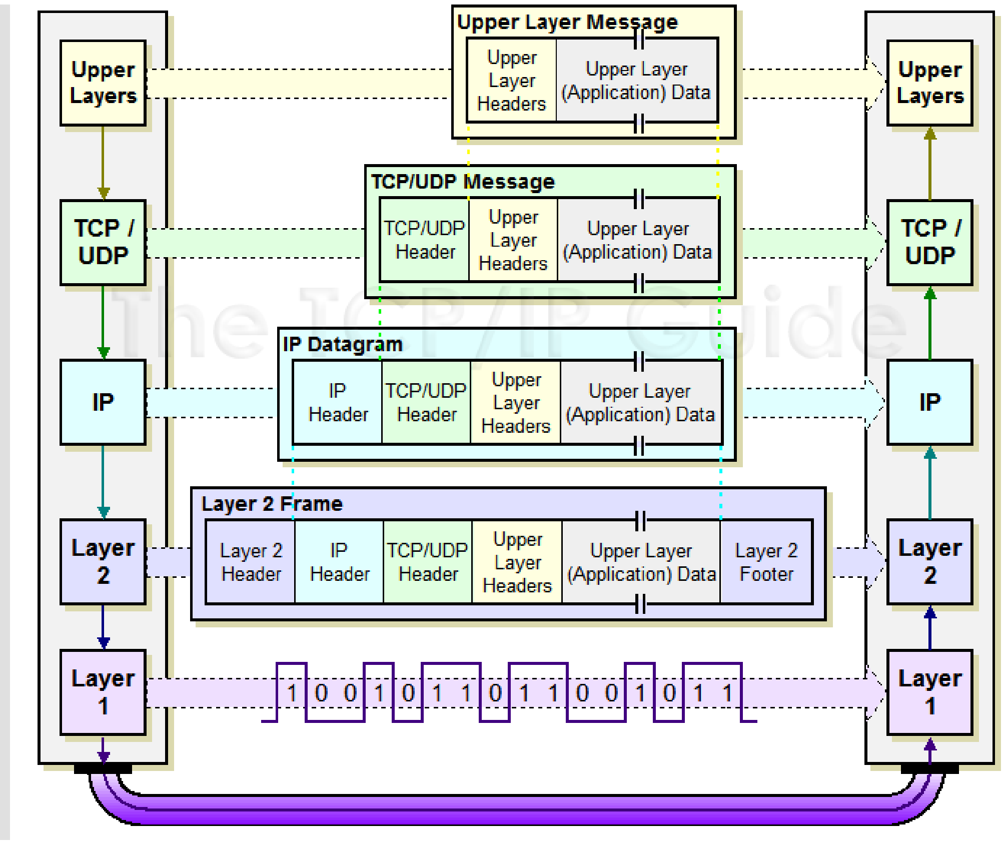
| | | |
|---|---|---|
| MAIN DATA | APPLICATION | |
| MAIN DATA | PRESENTATION | |
| MAIN DATA | SESSION | |
| TCP HEADER MAIN DATA | TRANSPORT | SEGMENT |
| IP HEADER MAIN DATA | NETWORK | PACKET |
| MAC HEADER MAIN DATA | DATA LINK | FRAME |
| MAIN DATA IN BITS 1010101010 | PHYSICAL | BITS |

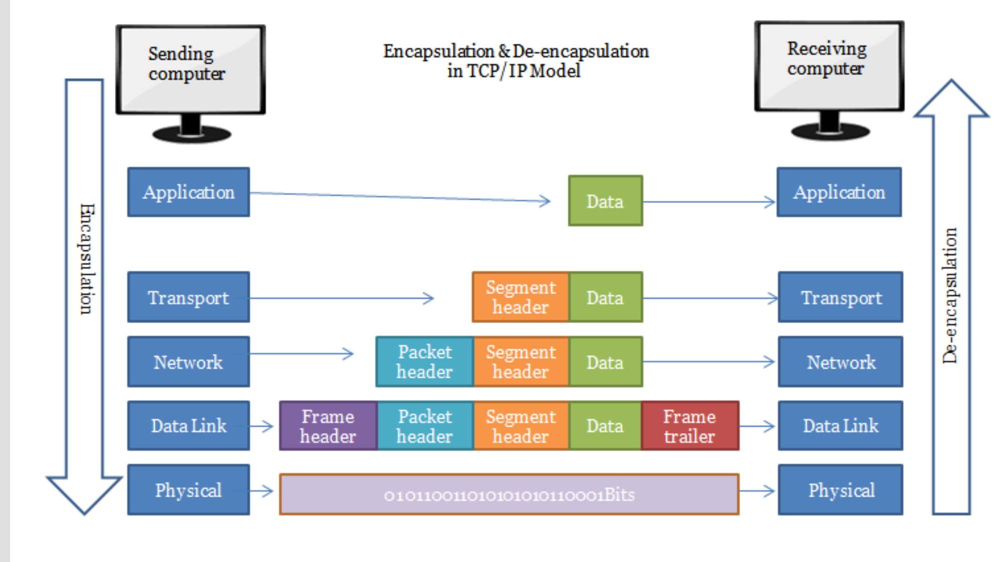
DATA ENCAPSULATION AT DIFFERENT LAYERS

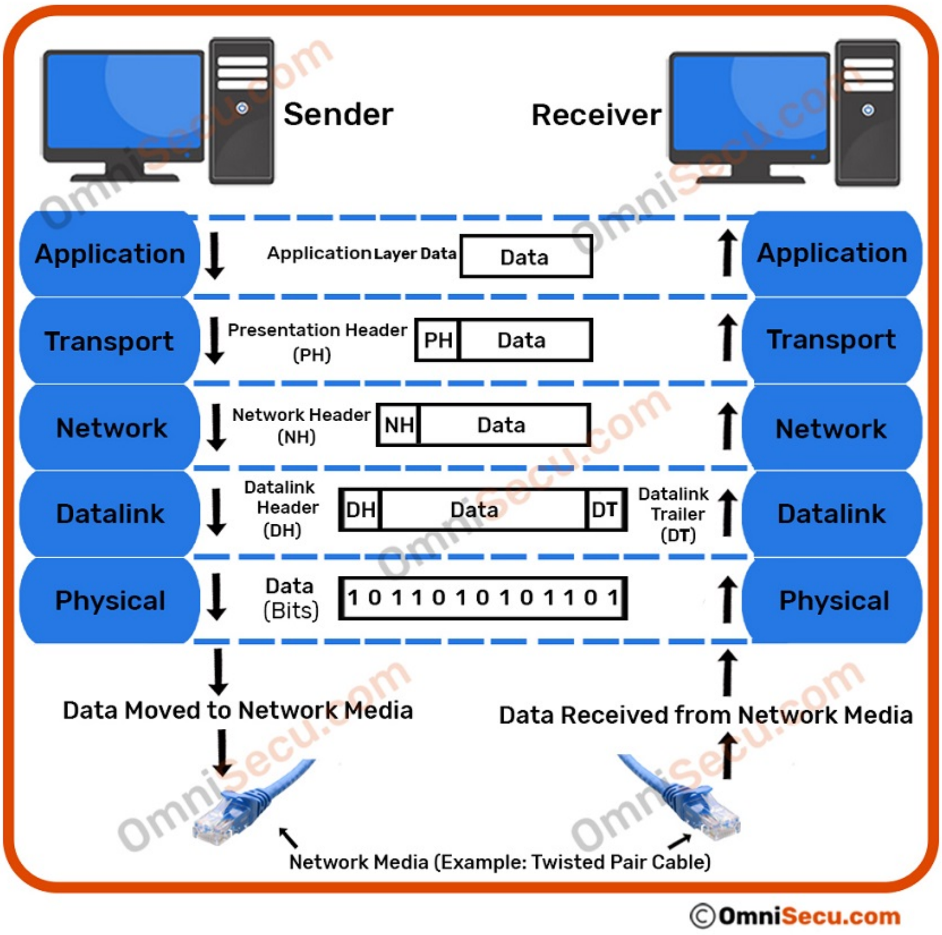


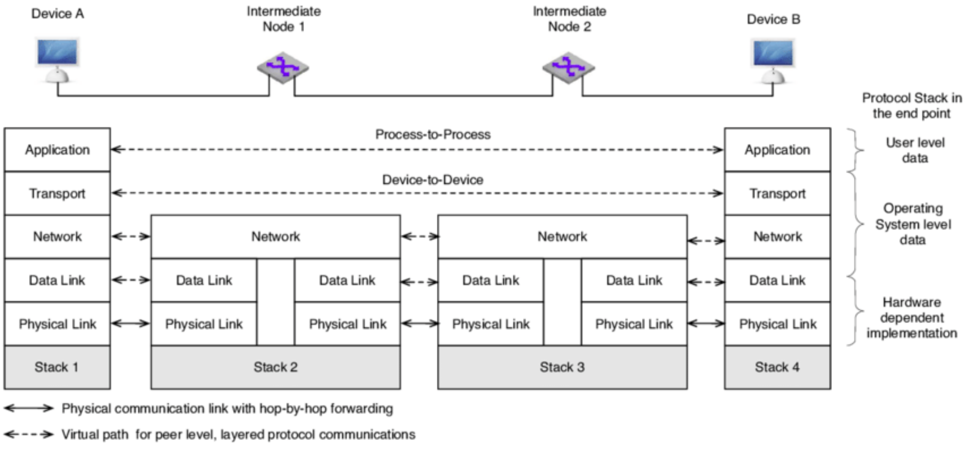
Format of the information at each layer


5-6-7 – Application
Telnet, FTP, TFTP, HTTP, BOOTP, DHCP, SNMP Socket API
User Data
User Data (Messages or Streams)
App Header
User Data
4 – Transport
TCP, UDP
Transport Protocol Messages
TCP Header
Application Data
TCP Segment
3 – Network
IP, ARP, ICMP
IP Datagrams
IP Header
TCP Header
Application Data
IP Datagram
2 – Data Link
PPP, SLIP, Ethernet
Network-Specific Frames
Ethernet Header
IP Header
TCP Header
Application Data
Ethernet Trailer
14
20
20
...
4
1 – Physical
Physical Devices
46 to 1500 bytes
Ethernet Frame

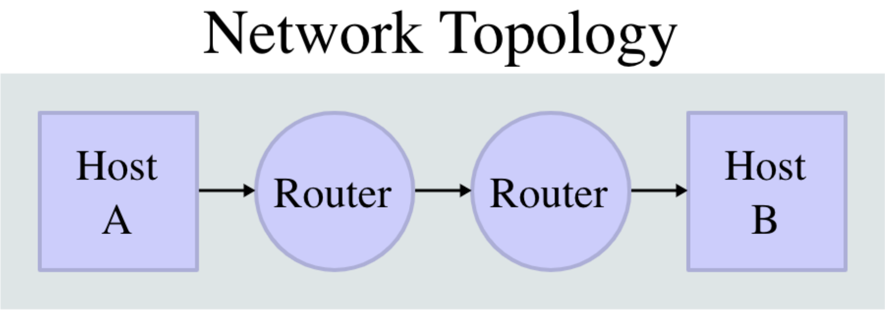

Upper Layers
TCP / UDP
IP
Layer 2
Layer 1
Upper Layer Message
Upper Layer Headers
Upper Layer (Application) Data
TCP/UDP Message
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
IP Datagram
IP Header
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
Layer 2 Frame
Layer 2 Header
IP Header
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
Layer 2 Footer
1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 1
Upper Layers
TCP / UDP
IP
Layer 2
Layer 1
The TCP/IP Guide

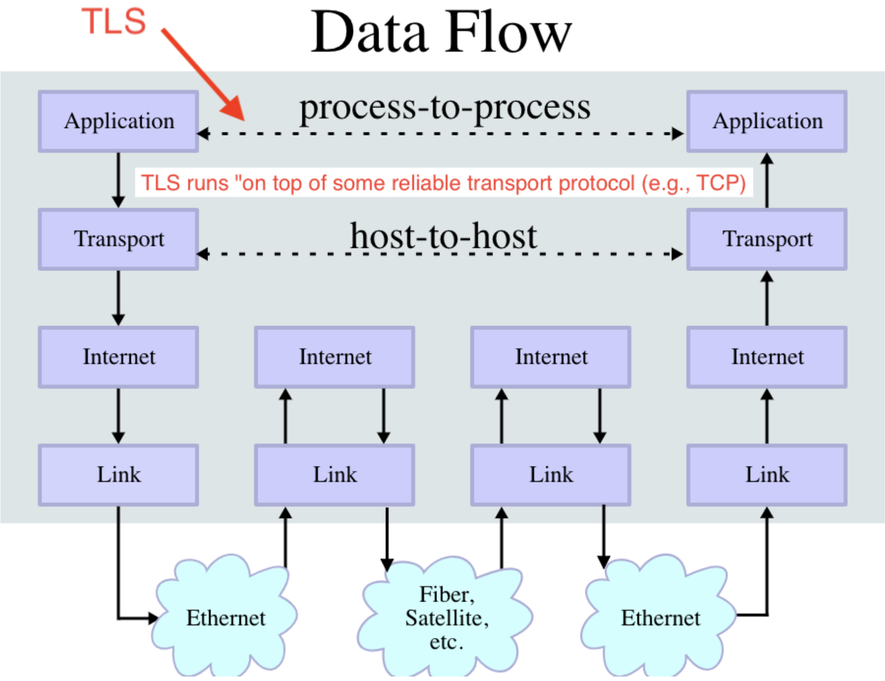

Sending computer
Encapsulation & De-encapsulation in TCP/IP Model
Receiving computer
Encapsulation
Application
Data
Application
Transport
Segment header
Data
Transport
Network
Packet header
Segment header
Data
Network
Data Link
Frame header
Packet header
Segment header
Data
Frame trailer
Data Link
Physical
0101100110101010110001Bits
Physical
De-encapsulation

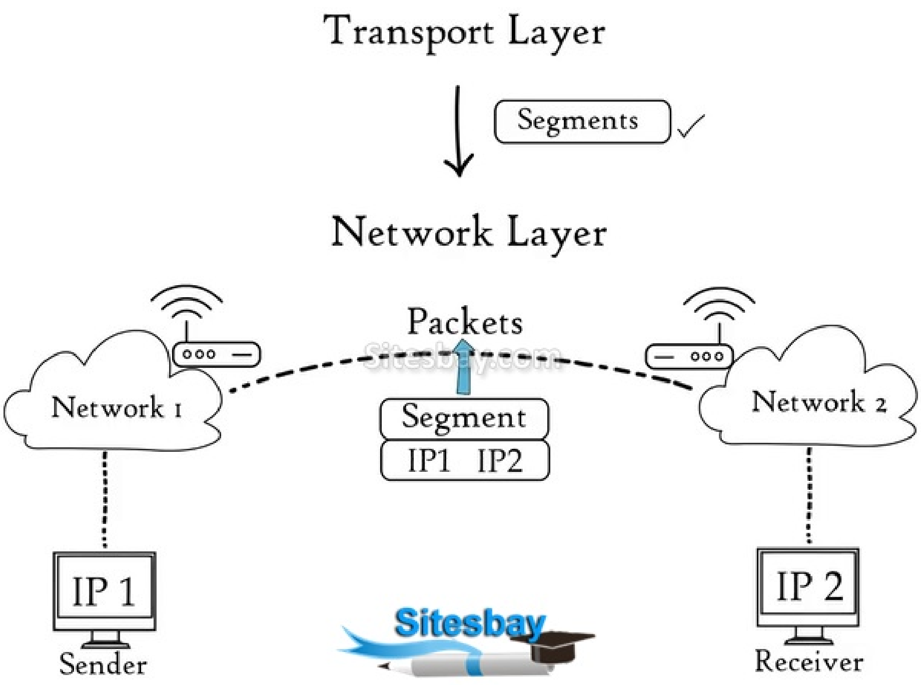


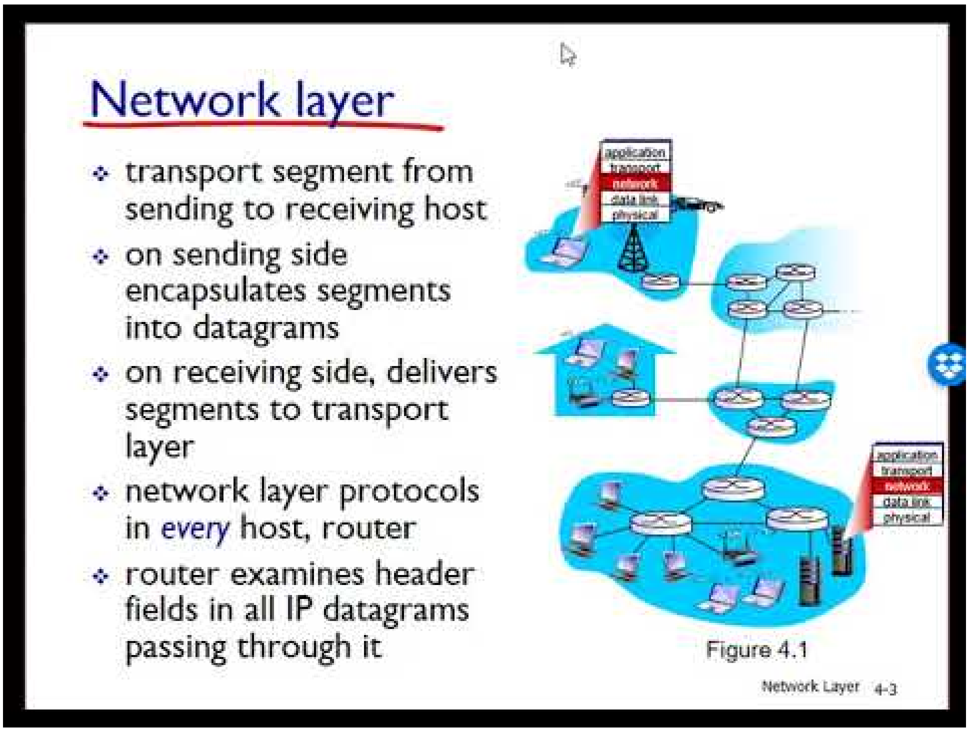

Device A
Intermediate Node 1
Intermediate Node 2
Device B
Protocol Stack in the end point
Process-to-Process
Device-to-Device
Application
Transport
Network
Data Link
Physical Link
Stack 1
Stack 2
Stack 3
Stack 4
User level data
Operating System level data
Hardware dependent implementation
Physical communication link with hop-by-hop forwarding
Virtual path for peer level, layered protocol communications

## Network Layer - Data Flow


Network Topology
Host A
Router
Router
Host B


TLS
Data Flow
Application
process-to-process
Application
TLS runs "on top of some reliable transport protocol (e.g., TCP)
Transport
host-to-host
Transport
Internet
Internet
Internet
Internet
Link
Link
Link
Link
Ethernet
Fiber, Satellite, etc.
Ethernet


Transport Layer
Segments ✓
Network Layer
Packets
Network 1
Network 2
Segment
IP1 IP2
IP 1
Sender
IP 2
Receiver
Sitesbay



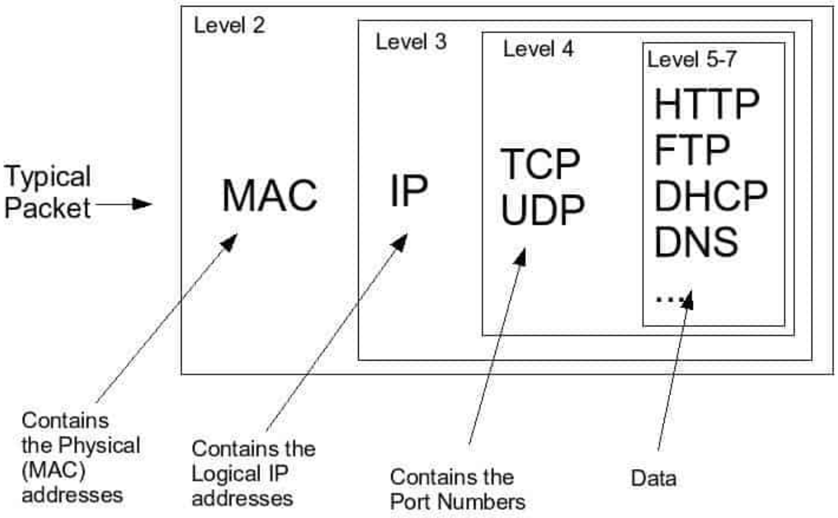
## Network layer

- transport segment from sending to receiving host
- on sending side encapsulates segments into datagrams
- on receiving side, delivers segments to transport layer
- network layer protocols in *every* host, router
- router examines header fields in all IP datagrams passing through it

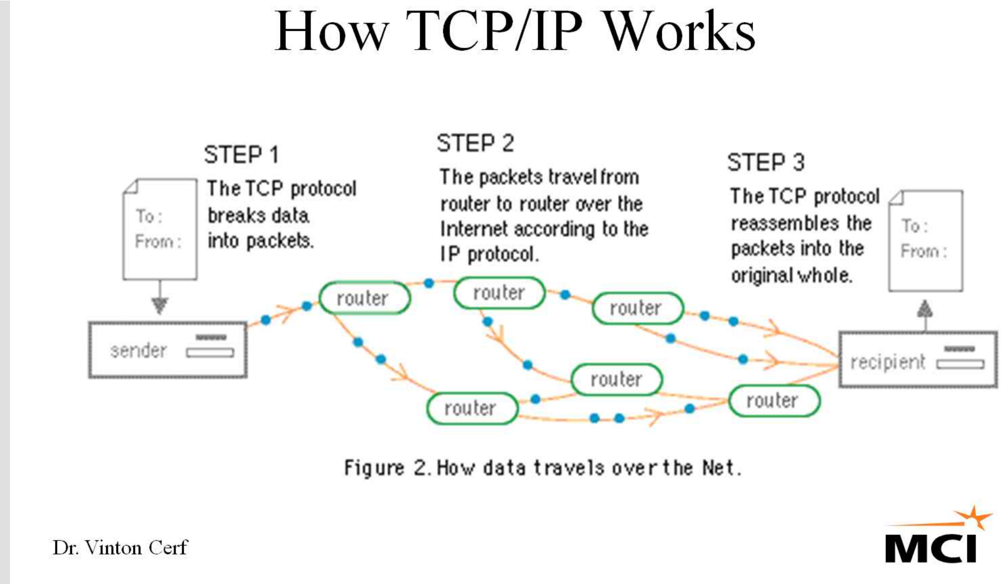
Figure 4.1

Network Layer 4-3

## Network Layer - Packet


Typical Packet
Level 2
MAC
Level 3
IP
Level 4
TCP
UDP
Level 5-7
HTTP
FTP
DHCP
DNS
...
Contains the Physical (MAC) addresses
Contains the Logical IP addresses
Contains the Port Numbers
Data

## Network Layer - Packet Switch



# How TCP/IP Works

STEP 1

The TCP protocol breaks data into packets.

STEP 2

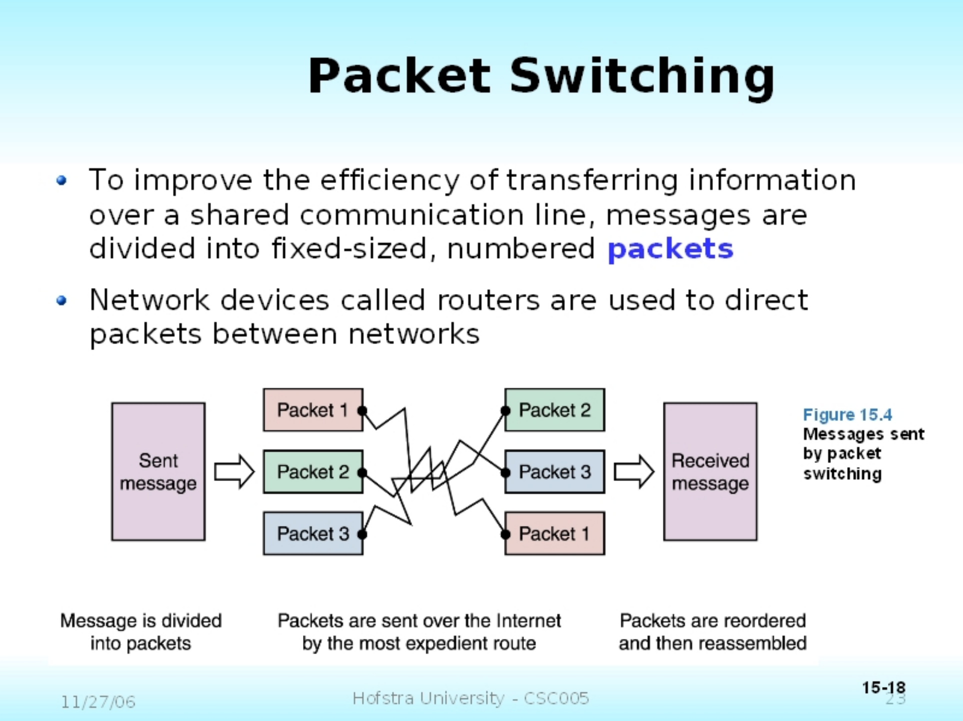
The packets travel from router to router over the Internet according to the IP protocol.

STEP 3

The TCP protocol reassembles the packets into the original whole.

Figure 2. How data travels over the Net.

Dr. Vinton Cerf



# Packet Switching

- To improve the efficiency of transferring information over a shared communication line, messages are divided into fixed-sized, numbered **packets**
- Network devices called routers are used to direct packets between networks

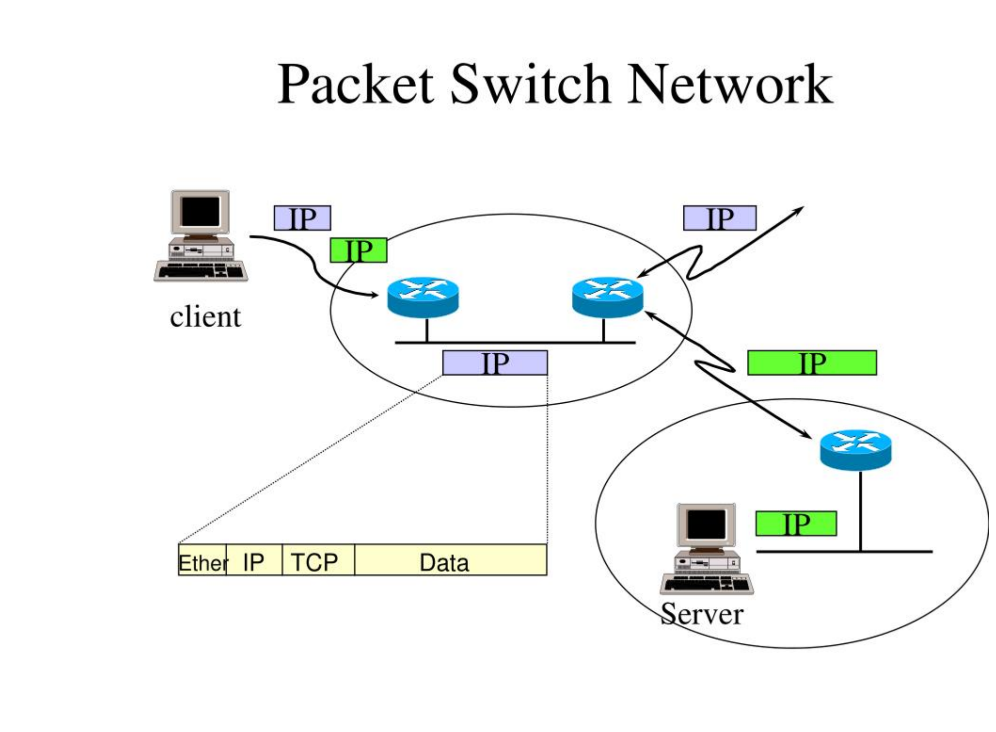
**Figure 15.4**
**Messages sent by packet switching**

Message is divided into packets

Packets are sent over the Internet by the most expedient route

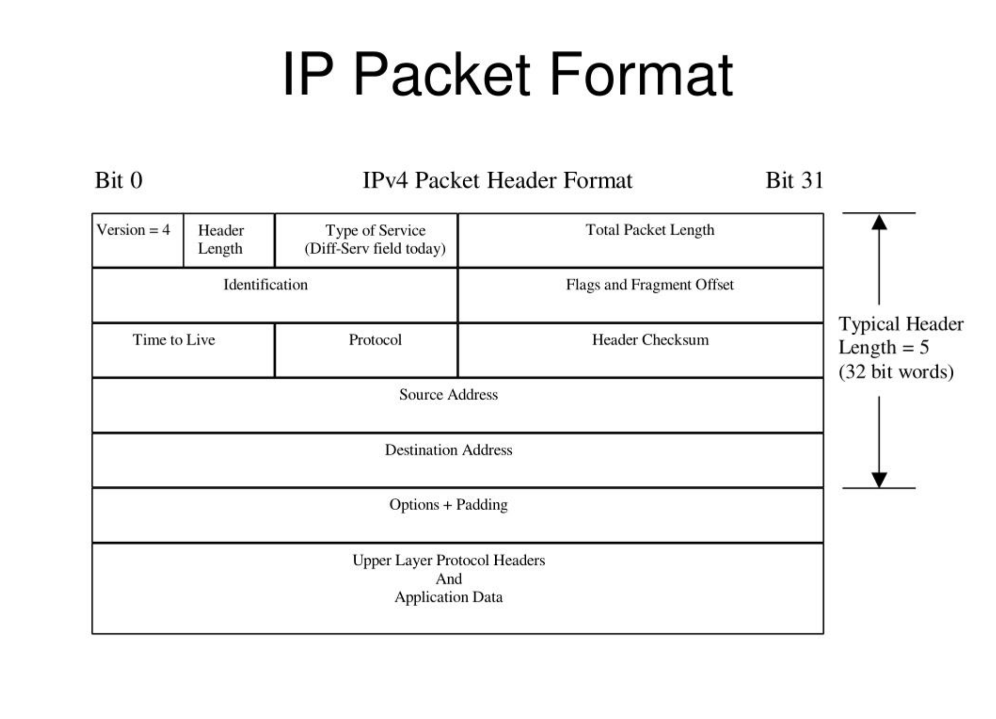
Packets are reordered and then reassembled

11/27/06 Hofstra University - CSC005 15-18 23



# Packet Switch Network

## Network Layer - IP Packet Format

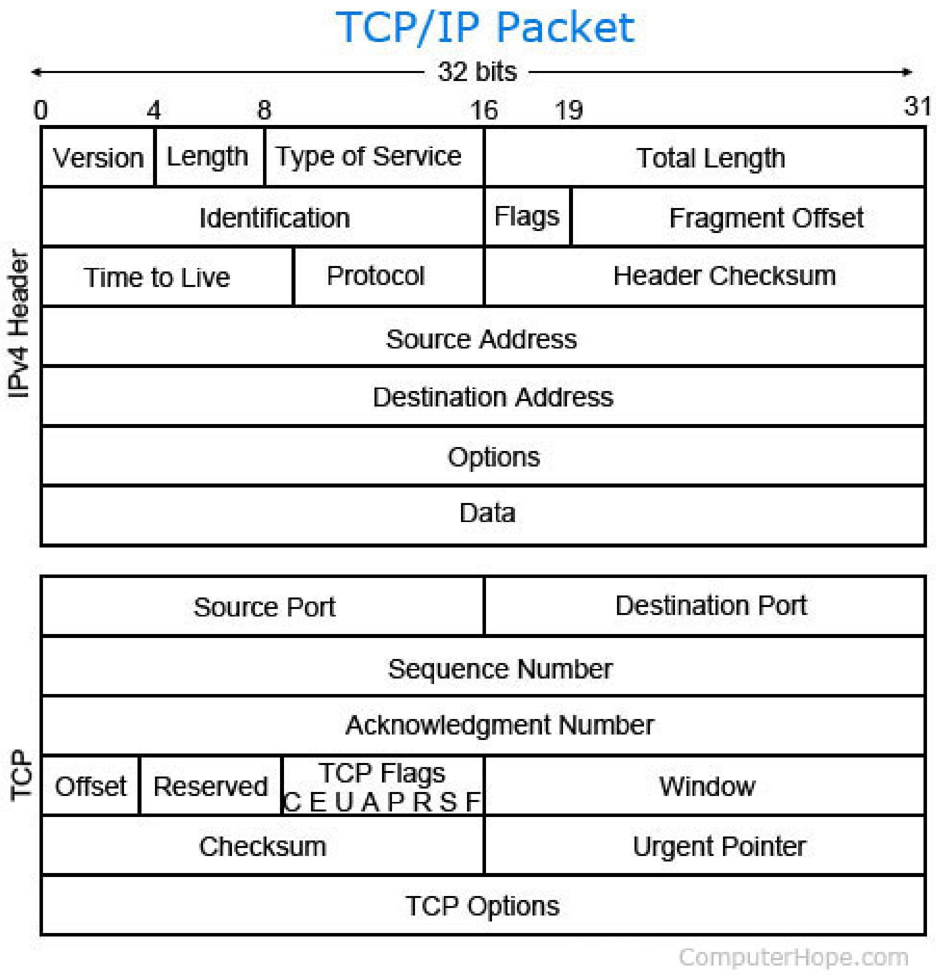


# IP Packet Format

Bit 0 IPv4 Packet Header Format Bit 31

| | | | |
|---|---|---|---|
| Version = 4 | Header Length | Type of Service (Diff-Serv field today) | Total Packet Length |
| Identification | | | Flags and Fragment Offset |
| Time to Live | | Protocol | Header Checksum |
| Source Address | | | |
| Destination Address | | | |
| Options + Padding | | | |
| Upper Layer Protocol Headers<br>And<br>Application Data | | | |

Typical Header Length = 5 (32 bit words)



# Network Layer - IP4 vs IP6

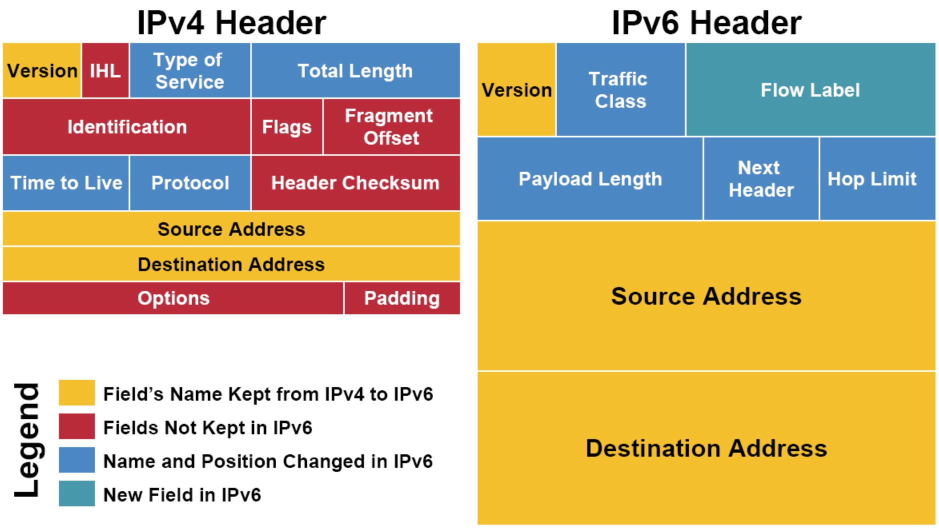
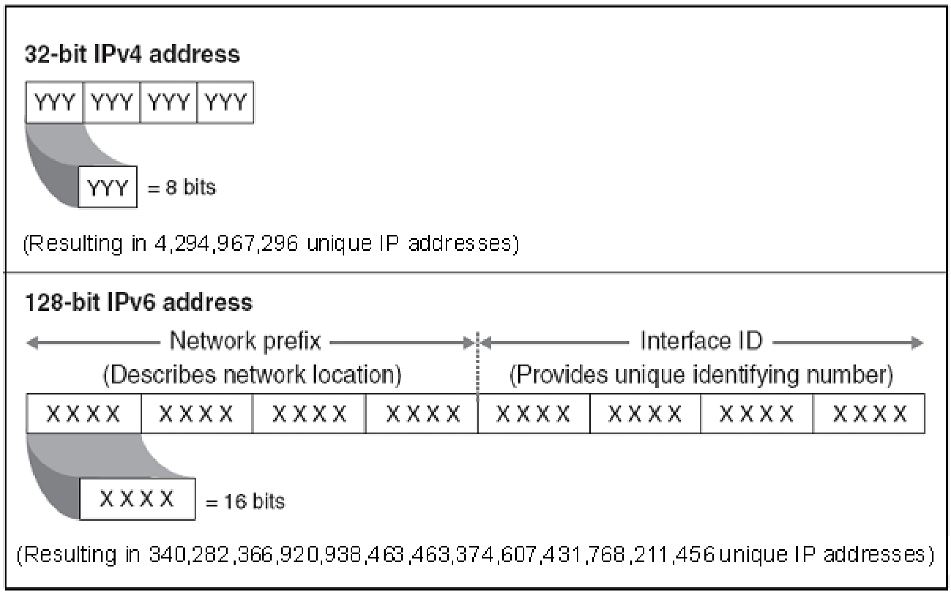
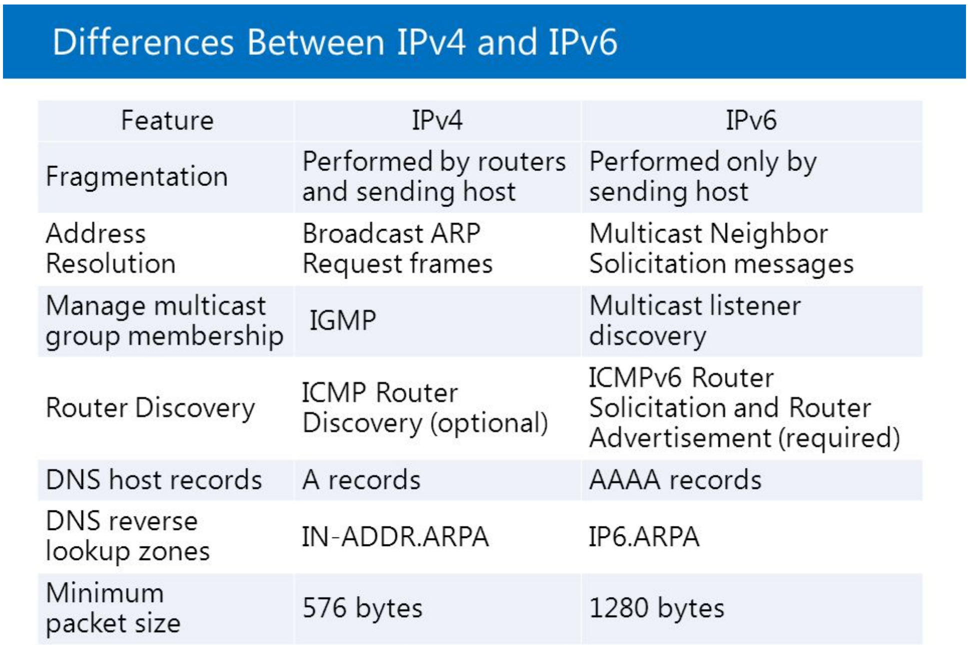


Figure 1: Comparison of IPv6 and IPv4 Address Scheme

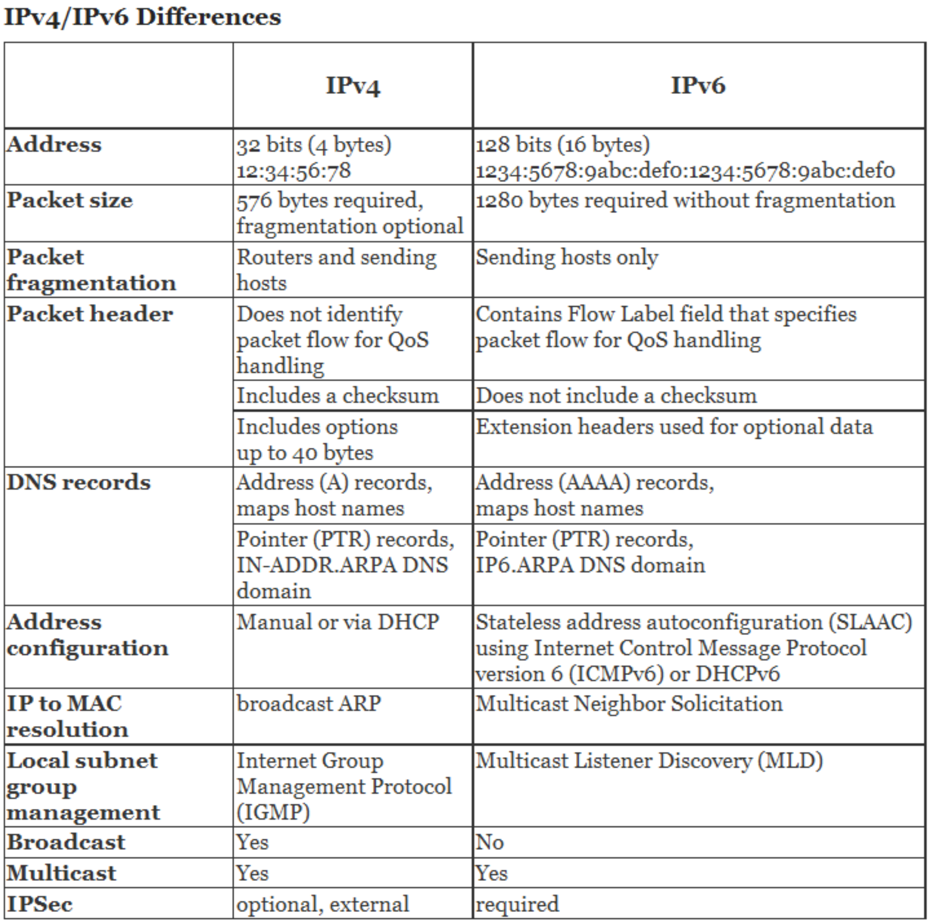

32-bit IPv4 address
YYY
YYY
YYY
YYY
YYY
= 8 bits
(Resulting in 4,294,967,296 unique IP addresses)
128-bit IPv6 address
Network prefix
(Describes network location)
Interface ID
(Provides unique identifying number)
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
XXXX
= 16 bits
(Resulting in 340,282,366,920,938,463,463,374,607,431,768,211,456 unique IP addresses)

Source: GAO.



## Differences Between IPv4 and IPv6

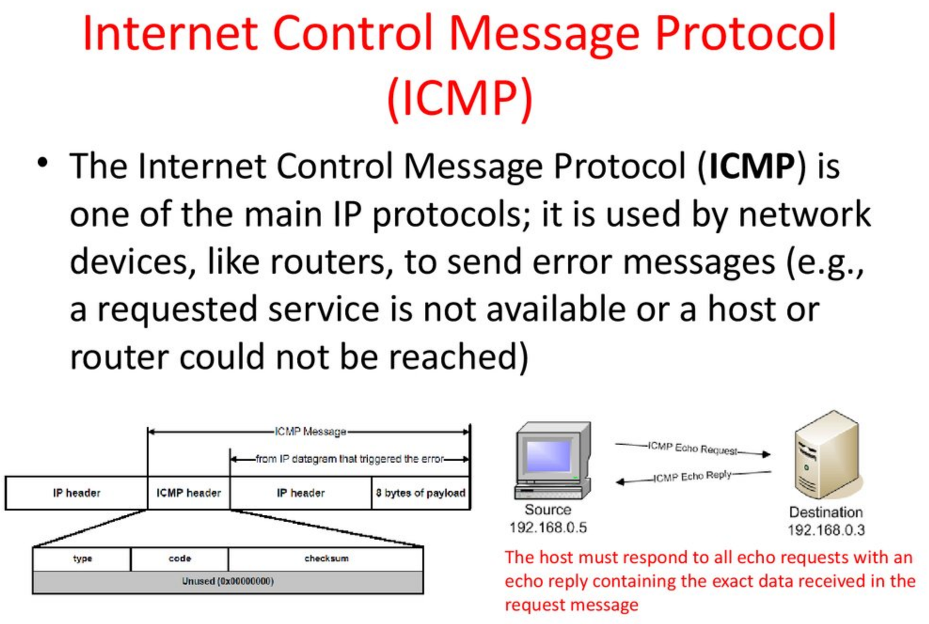
| Feature | IPv4 | IPv6 |
|---|---|---|
| Fragmentation | Performed by routers and sending host | Performed only by sending host |
| Address Resolution | Broadcast ARP Request frames | Multicast Neighbor Solicitation messages |
| Manage multicast group membership | IGMP | Multicast listener discovery |
| Router Discovery | ICMP Router Discovery (optional) | ICMPv6 Router Solicitation and Router Advertisement (required) |
| DNS host records | A records | AAAA records |
| DNS reverse lookup zones | IN-ADDR.ARPA | IP6.ARPA |
| Minimum packet size | 576 bytes | 1280 bytes |



**IPv4/IPv6 Differences**

| | IPv4 | IPv6 |
|---|---|---|
| **Address** | 32 bits (4 bytes)<br>12:34:56:78 | 128 bits (16 bytes)<br>1234:5678:9abc:def0:1234:5678:9abc:def0 |
| **Packet size** | 576 bytes required, fragmentation optional | 1280 bytes required without fragmentation |
| **Packet fragmentation** | Routers and sending hosts | Sending hosts only |
| **Packet header** | Does not identify packet flow for QoS handling | Contains Flow Label field that specifies packet flow for QoS handling |
| | Includes a checksum | Does not include a checksum |
| | Includes options up to 40 bytes | Extension headers used for optional data |
| **DNS records** | Address (A) records, maps host names | Address (AAAA) records, maps host names |
| | Pointer (PTR) records, IN-ADDR.ARPA DNS domain | Pointer (PTR) records, IP6.ARPA DNS domain |
| **Address configuration** | Manual or via DHCP | Stateless address autoconfiguration (SLAAC) using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6 |
| **IP to MAC resolution** | broadcast ARP | Multicast Neighbor Solicitation |
| **Local subnet group management** | Internet Group Management Protocol (IGMP) | Multicast Listener Discovery (MLD) |
| **Broadcast** | Yes | No |
| **Multicast** | Yes | Yes |
| **IPSec** | optional, external | required |

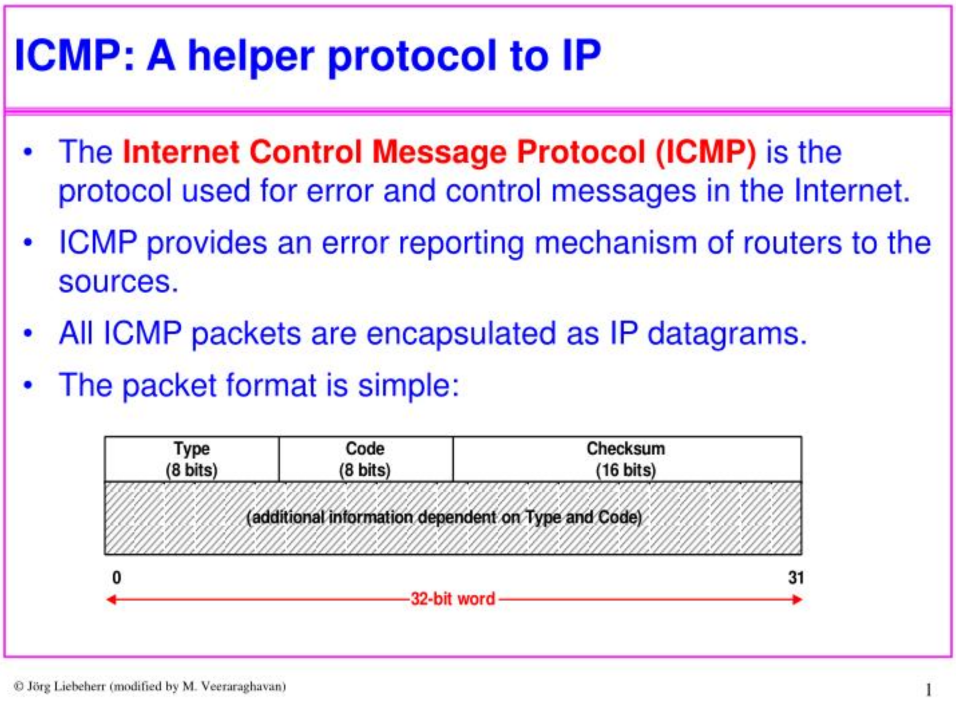
# Network Layer - ICMP



## Internet Control Message Protocol (ICMP)

- The Internet Control Message Protocol (**ICMP**) is one of the main IP protocols; it is used by network devices, like routers, to send error messages (e.g., a requested service is not available or a host or router could not be reached)

The host must respond to all echo requests with an echo reply containing the exact data received in the request message



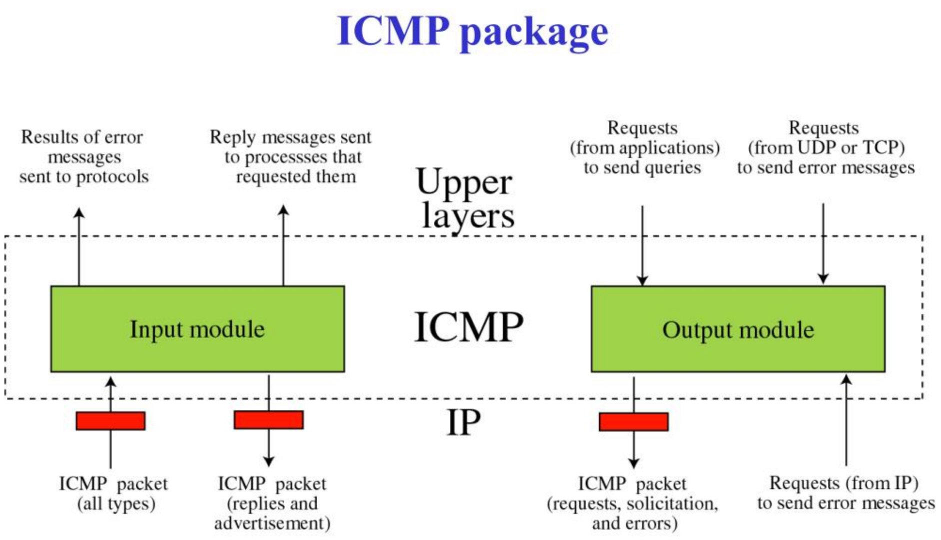
## ICMP: A helper protocol to IP

- The **Internet Control Message Protocol (ICMP)** is the protocol used for error and control messages in the Internet.
- ICMP provides an error reporting mechanism of routers to the sources.
- All ICMP packets are encapsulated as IP datagrams.
- The packet format is simple:

Type
(8 bits)
Code
(8 bits)
Checksum
(16 bits)
(additional information dependent on Type and Code)
0
31
32-bit word

© Jörg Liebeherr (modified by M. Veeraraghavan)

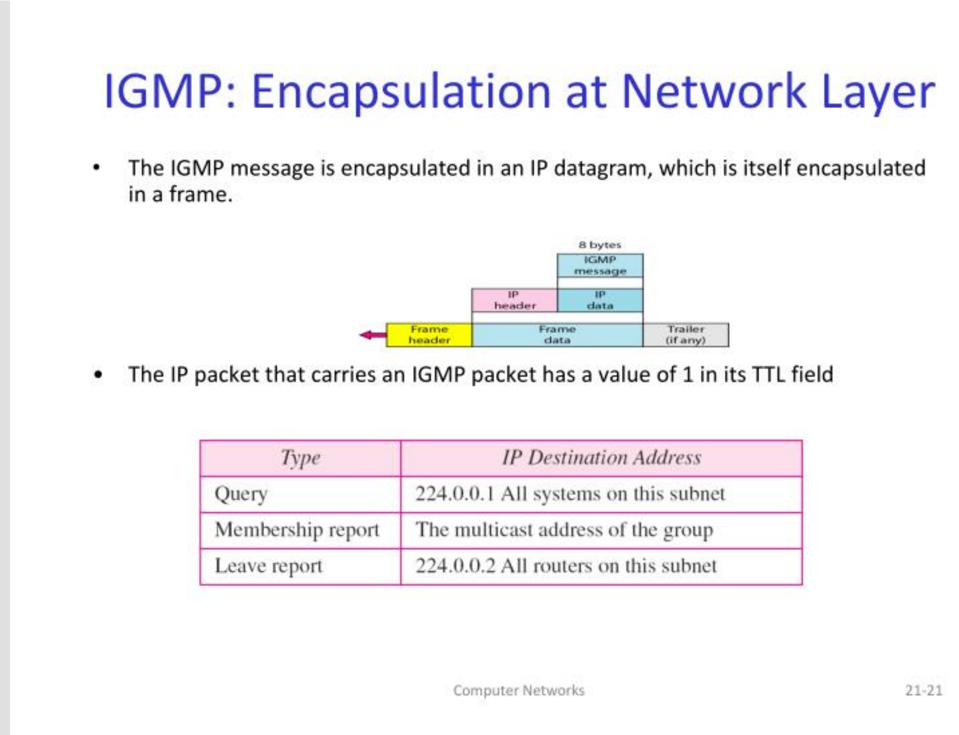
1



## ICMP package

Results of error messages sent to protocols
Reply messages sent to processses that requested them
Upper layers
Requests (from applications) to send queries
Requests (from UDP or TCP) to send error messages
Input module
ICMP
Output module
IP
ICMP packet (all types)
ICMP packet (replies and advertisement)
ICMP packet (requests, solicitation, and errors)
Requests (from IP) to send error messages

# Network Layer - IGMP

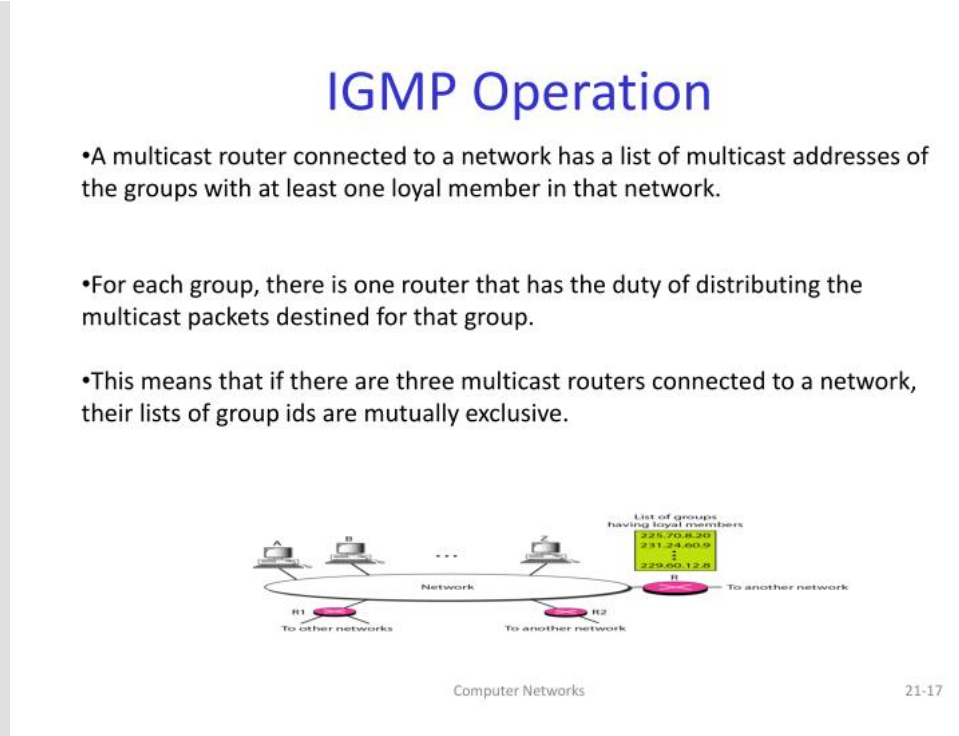


# IGMP: Encapsulation at Network Layer

- The IGMP message is encapsulated in an IP datagram, which is itself encapsulated in a frame.

- The IP packet that carries an IGMP packet has a value of 1 in its TTL field

| *Type* | *IP Destination Address* |
|---|---|
| Query | 224.0.0.1 All systems on this subnet |
| Membership report | The multicast address of the group |
| Leave report | 224.0.0.2 All routers on this subnet |

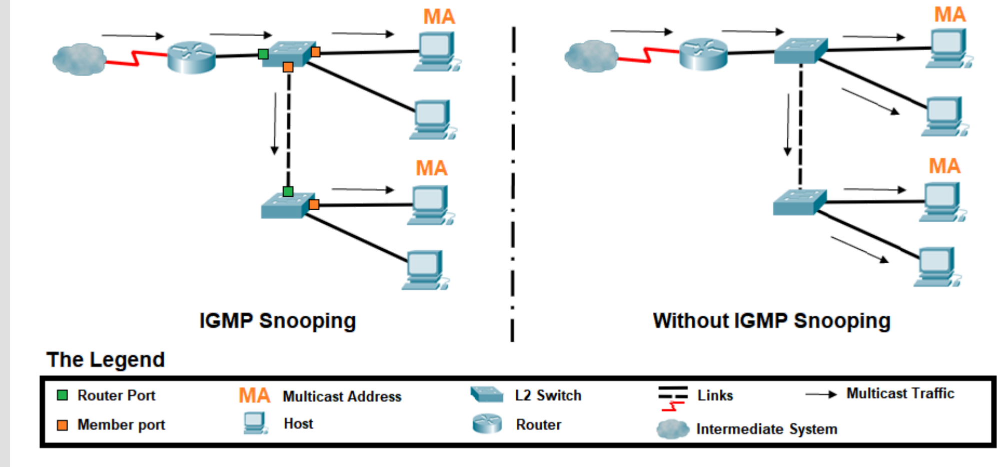


# IGMP Operation

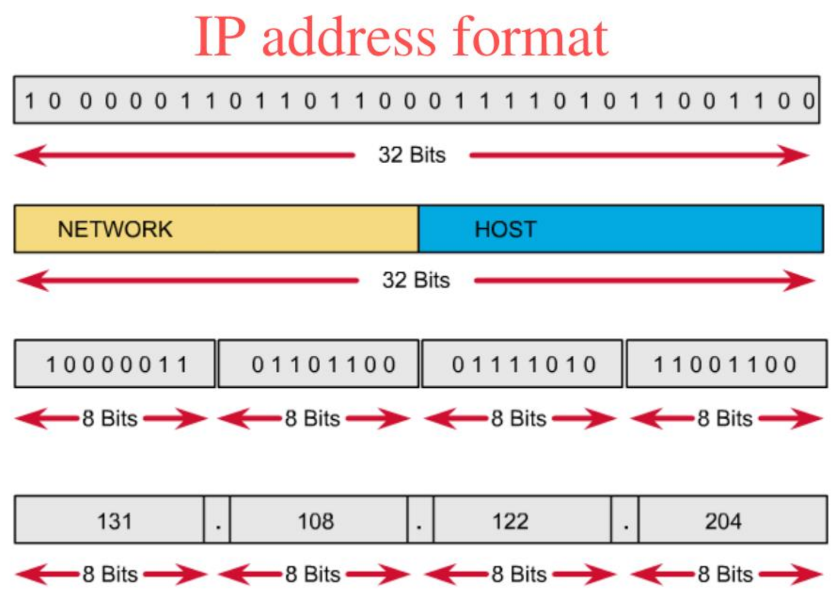
•A multicast router connected to a network has a list of multicast addresses of the groups with at least one loyal member in that network.

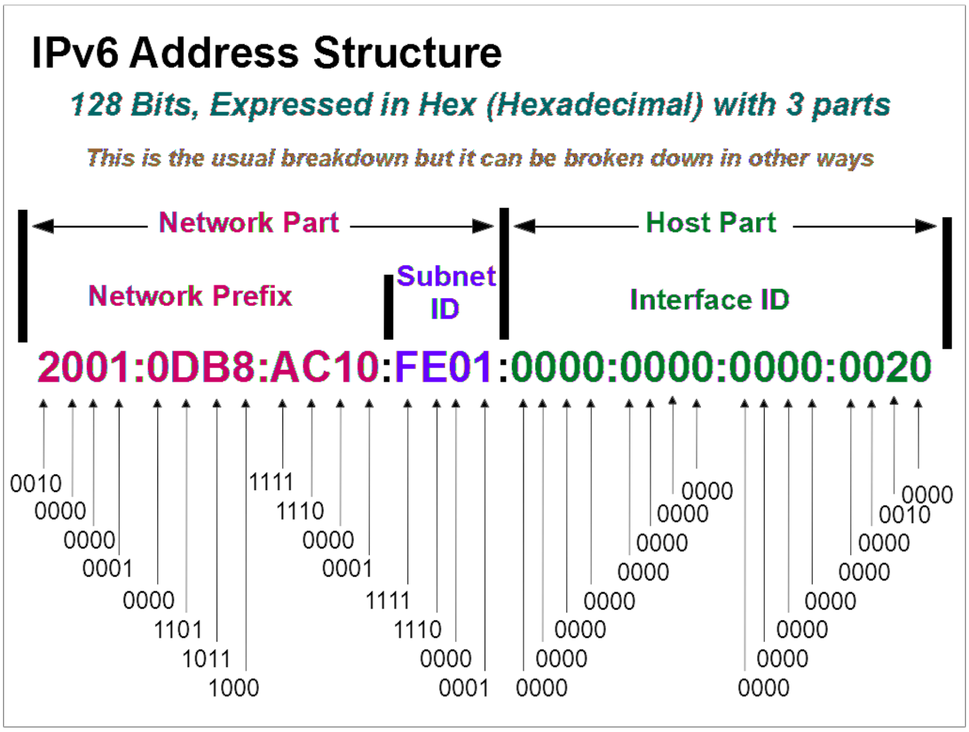
•For each group, there is one router that has the duty of distributing the multicast packets destined for that group.

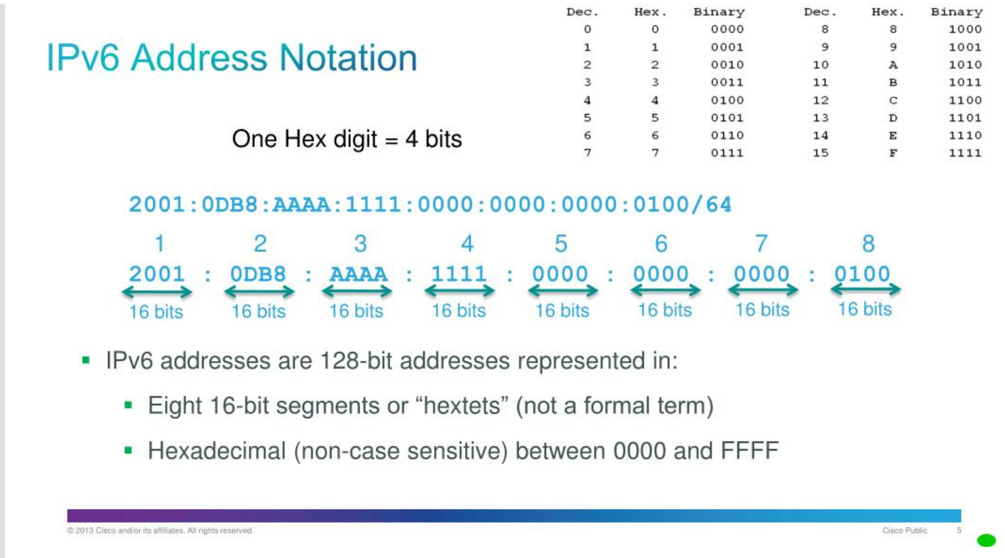
•This means that if there are three multicast routers connected to a network, their lists of group ids are mutually exclusive.



# Network Layer - IP Address







## IPv6 Address Notation

| Dec. | Hex. | Binary | Dec. | Hex. | Binary |
|---|---|---|---|---|---|
| 0 | 0 | 0000 | 8 | 8 | 1000 |
| 1 | 1 | 0001 | 9 | 9 | 1001 |
| 2 | 2 | 0010 | 10 | A | 1010 |
| 3 | 3 | 0011 | 11 | B | 1011 |
| 4 | 4 | 0100 | 12 | C | 1100 |
| 5 | 5 | 0101 | 13 | D | 1101 |
| 6 | 6 | 0110 | 14 | E | 1110 |
| 7 | 7 | 0111 | 15 | F | 1111 |

One Hex digit = 4 bits

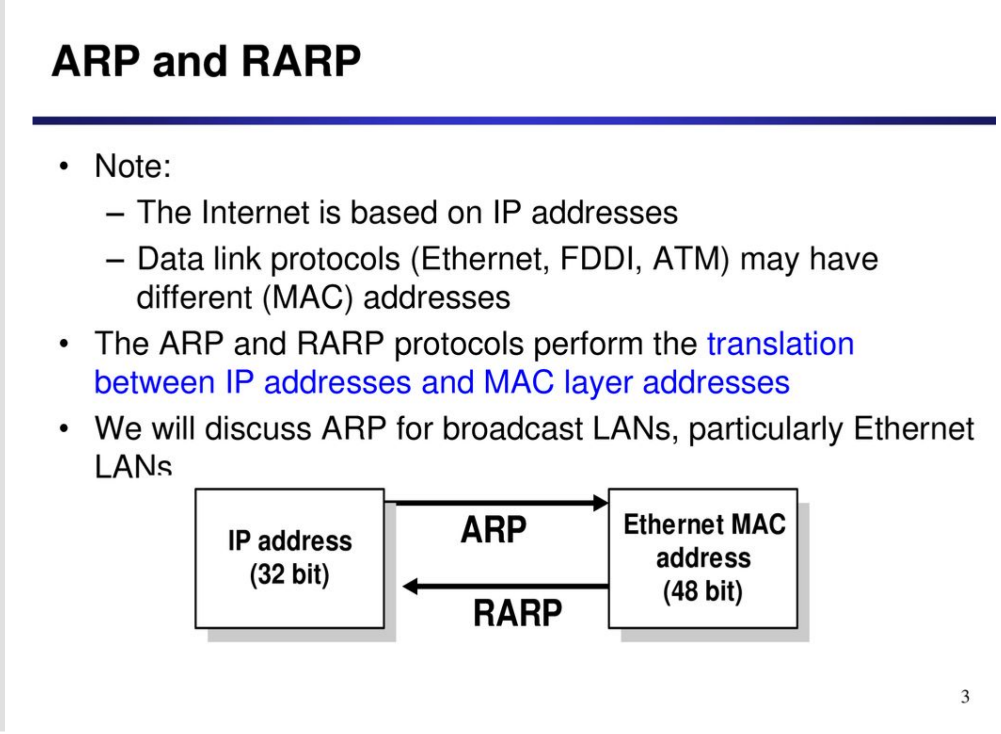
2001:0DB8:AAAA:1111:0000:0000:0000:0100/64

- IPv6 addresses are 128-bit addresses represented in:
  - Eight 16-bit segments or "hextets" (not a formal term)
  - Hexadecimal (non-case sensitive) between 0000 and FFFF

Cisco Public 5

# Network Layer - ARP(Address Resolution Protocl) / RARP (ReverseAddress Resolution Protocl)

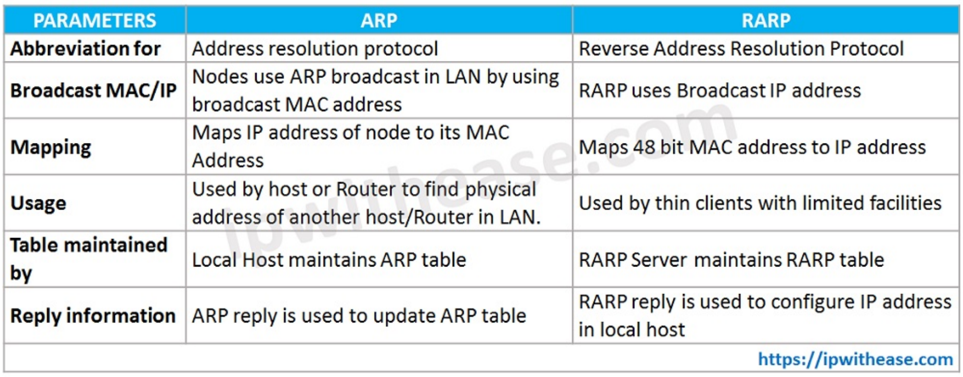
- ARP: resolve IP Address to MAC Address
- RARP: resolve MAC Address to IP Address



## ARP and RARP

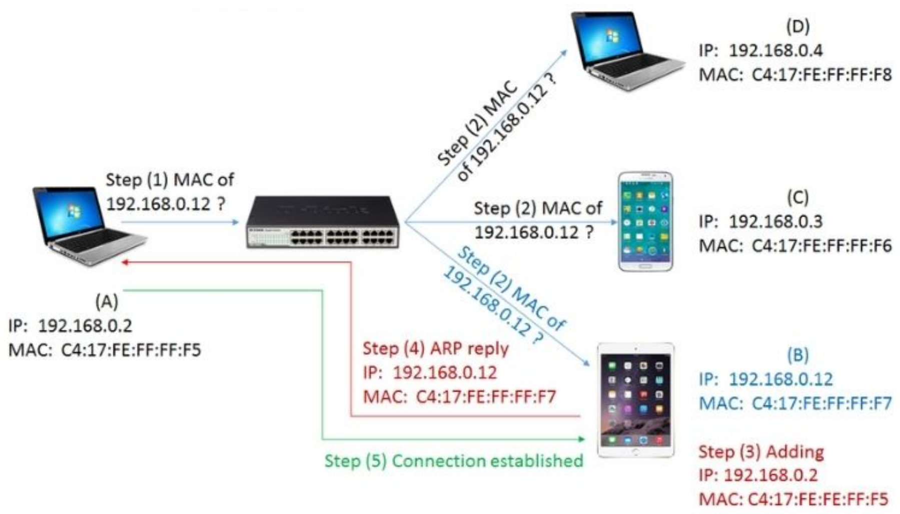
- Note:
  - The Internet is based on IP addresses
  - Data link protocols (Ethernet, FDDI, ATM) may have different (MAC) addresses
- The ARP and RARP protocols perform the translation between IP addresses and MAC layer addresses
- We will discuss ARP for broadcast LANs, particularly Ethernet LANs

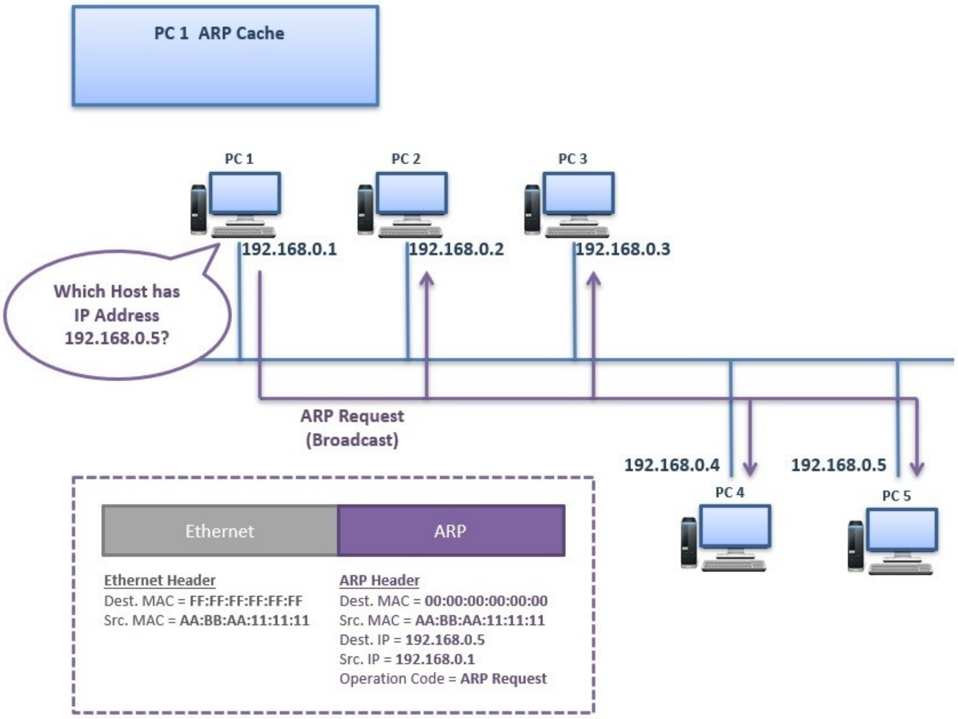
3

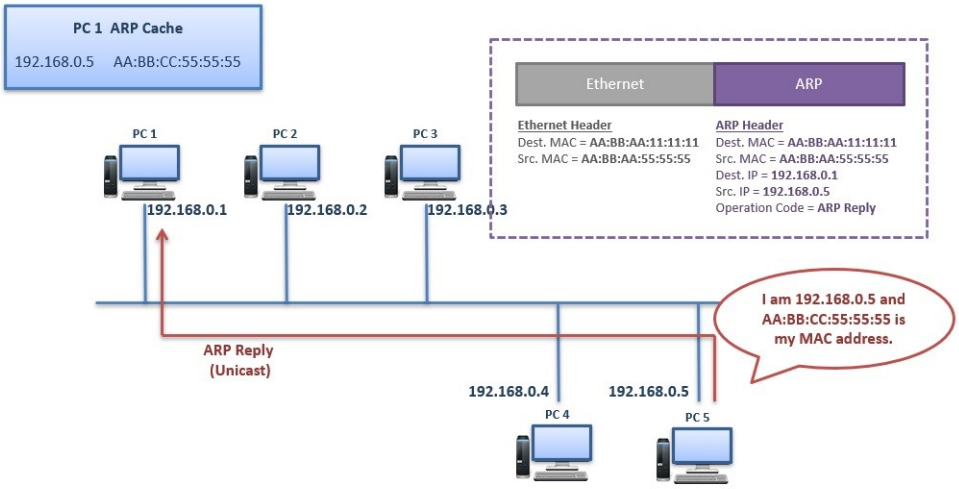


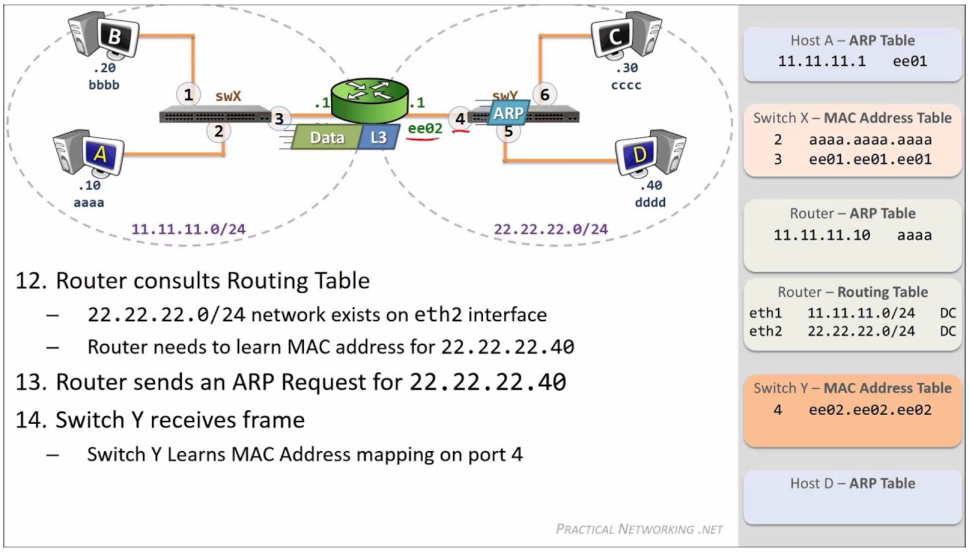
| PARAMETERS | ARP | RARP |
|---|---|---|
| Abbreviation for | Address resolution protocol | Reverse Address Resolution Protocol |
| Broadcast MAC/IP | Nodes use ARP broadcast in LAN by using broadcast MAC address | RARP uses Broadcast IP address |
| Mapping | Maps IP address of node to its MAC Address | Maps 48 bit MAC address to IP address |
| Usage | Used by host or Router to find physical address of another host/Router in LAN. | Used by thin clients with limited facilities |
| Table maintained by | Local Host maintains ARP table | RARP Server maintains RARP table |
| Reply information | ARP reply is used to update ARP table | RARP reply is used to configure IP address in local host |

https://ipwithease.com


(D)
IP: 192.168.0.4
MAC: C4:17:FE:FF:FF:F8
Step (2) MAC of 192.168.0.12 ?
Step (1) MAC of 192.168.0.12 ?
Step (2) MAC of 192.168.0.12 ?
(C)
IP: 192.168.0.3
MAC: C4:17:FE:FF:FF:F6
Step (2) MAC of 192.168.0.12 ?
(A)
IP: 192.168.0.2
MAC: C4:17:FE:FF:FF:F5
Step (4) ARP reply
IP: 192.168.0.12
MAC: C4:17:FE:FF:FF:F7
(B)
IP: 192.168.0.12
MAC: C4:17:FE:FF:FF:F7
Step (5) Connection established
Step (3) Adding
IP: 192.168.0.2
MAC: C4:17:FE:FE:FF:F5


PC 1 ARP Cache
PC 1
PC 2
PC 3
192.168.0.1
192.168.0.2
192.168.0.3
Which Host has IP Address 192.168.0.5?
ARP Request (Broadcast)
192.168.0.4
192.168.0.5
PC 4
PC 5
Ethernet
ARP
Ethernet Header
Dest. MAC = FF:FF:FF:FF:FF:FF
Src. MAC = AA:BB:AA:11:11:11
ARP Header
Dest. MAC = 00:00:00:00:00:00
Src. MAC = AA:BB:AA:11:11:11
Dest. IP = 192.168.0.5
Src. IP = 192.168.0.1
Operation Code = ARP Request


PC 1 ARP Cache
192.168.0.5 AA:BB:CC:55:55:55
PC 1
PC 2
PC 3
192.168.0.1
192.168.0.2
192.168.0.3
Ethernet
ARP
Ethernet Header
Dest. MAC = AA:BB:AA:11:11:11
Src. MAC = AA:BB:AA:55:55:55
ARP Header
Dest. MAC = AA:BB:AA:11:11:11
Src. MAC = AA:BB:AA:55:55:55
Dest. IP = 192.168.0.1
Src. IP = 192.168.0.5
Operation Code = ARP Reply
ARP Reply (Unicast)
I am 192.168.0.5 and AA:BB:CC:55:55:55 is my MAC address.
192.168.0.4
192.168.0.5
PC 4
PC 5



12. Router consults Routing Table
    - 22.22.22.0/24 network exists on eth2 interface
    - Router needs to learn MAC address for 22.22.22.40
13. Router sends an ARP Request for 22.22.22.40
14. Switch Y receives frame
    - Switch Y Learns MAC Address mapping on port 4

Host A – **ARP Table**

| | |
|---|---|
| 11.11.11.1 | ee01 |

Switch X – **MAC Address Table**

| | |
|---|---|
| 2 | aaaa.aaaa.aaaa |
| 3 | ee01.ee01.ee01 |

Router – **ARP Table**

| | |
|---|---|
| 11.11.11.10 | aaaa |

Router – **Routing Table**

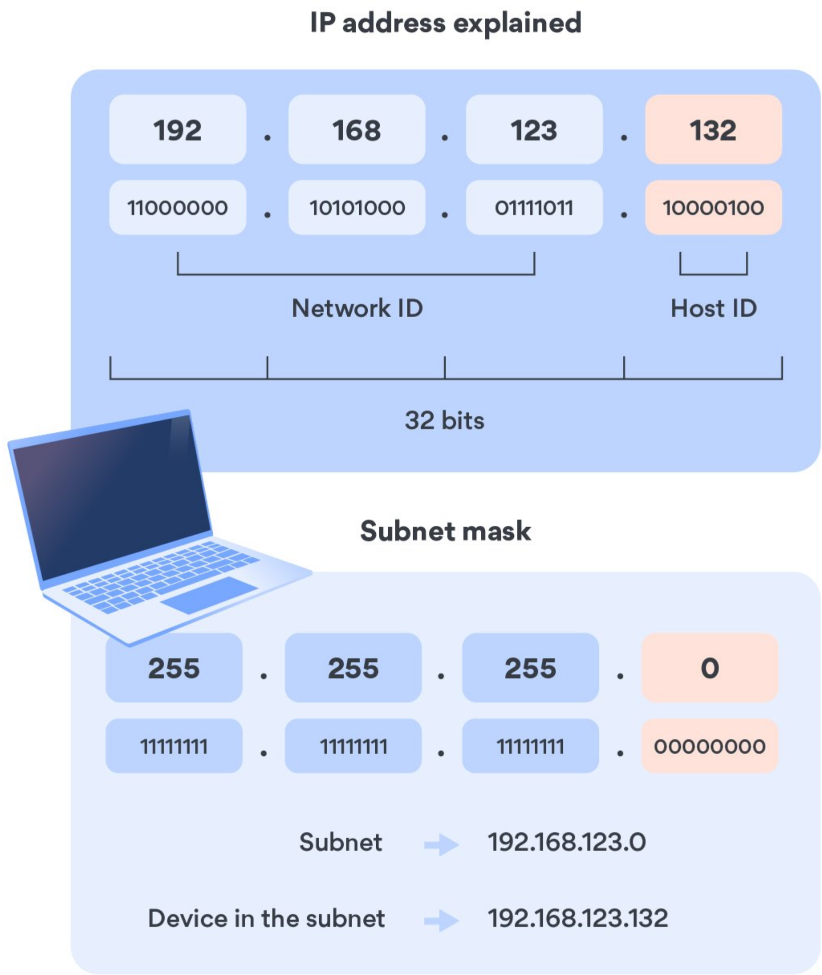
| | | |
|---|---|---|
| eth1 | 11.11.11.0/24 | DC |
| eth2 | 22.22.22.0/24 | DC |

Switch Y – **MAC Address Table**

| | |
|---|---|
| 4 | ee02.ee02.ee02 |

Host D – **ARP Table**

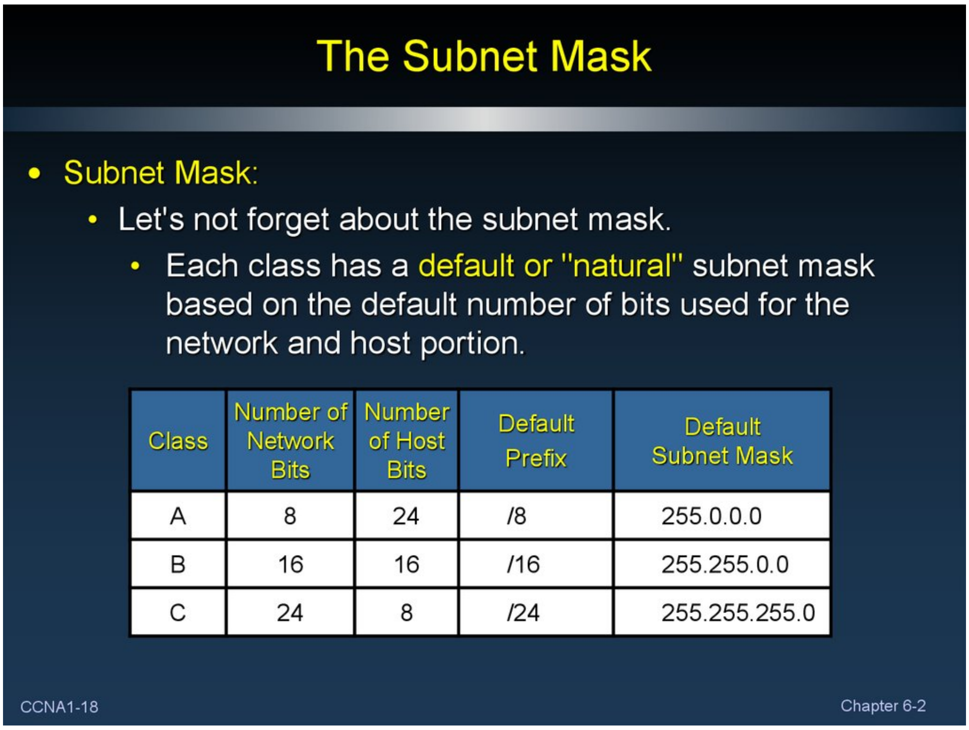
## Network Layer - Subnet Mask


**IP address explained**

**Subnet mask**

Subnet → 192.168.123.0

Device in the subnet → 192.168.123.132



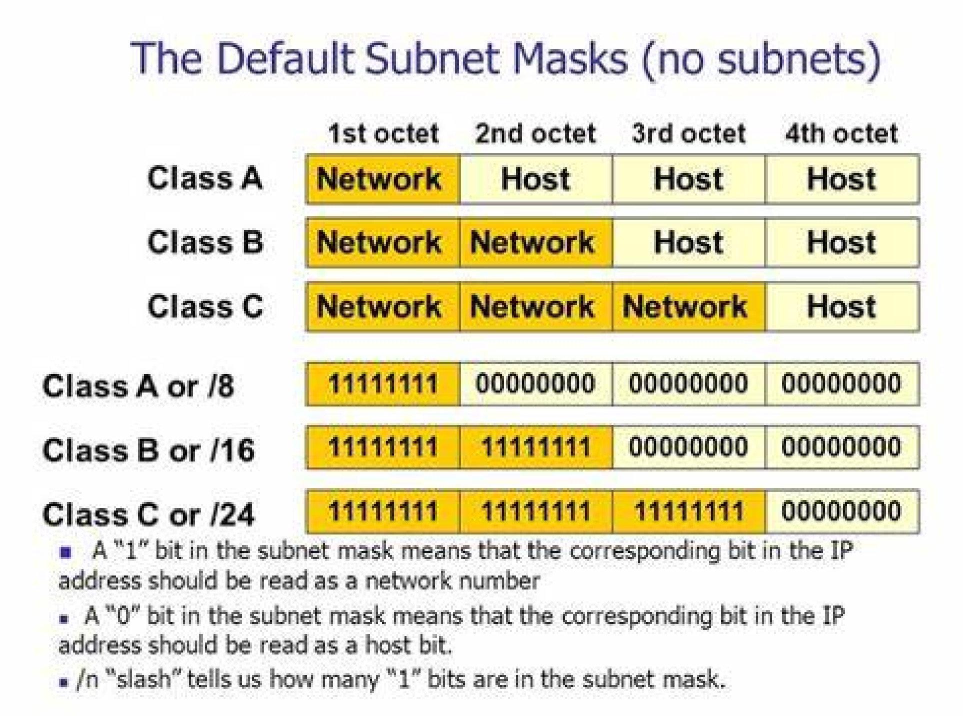
# The Subnet Mask

- Subnet Mask:
  - Let's not forget about the subnet mask.
    - Each class has a default or "natural" subnet mask based on the default number of bits used for the network and host portion.

| Class | Number of Network Bits | Number of Host Bits | Default Prefix | Default Subnet Mask |
|---|---|---|---|---|
| A | 8 | 24 | /8 | 255.0.0.0 |
| B | 16 | 16 | /16 | 255.255.0.0 |
| C | 24 | 8 | /24 | 255.255.255.0 |

CCNA1-18

Chapter 6-2

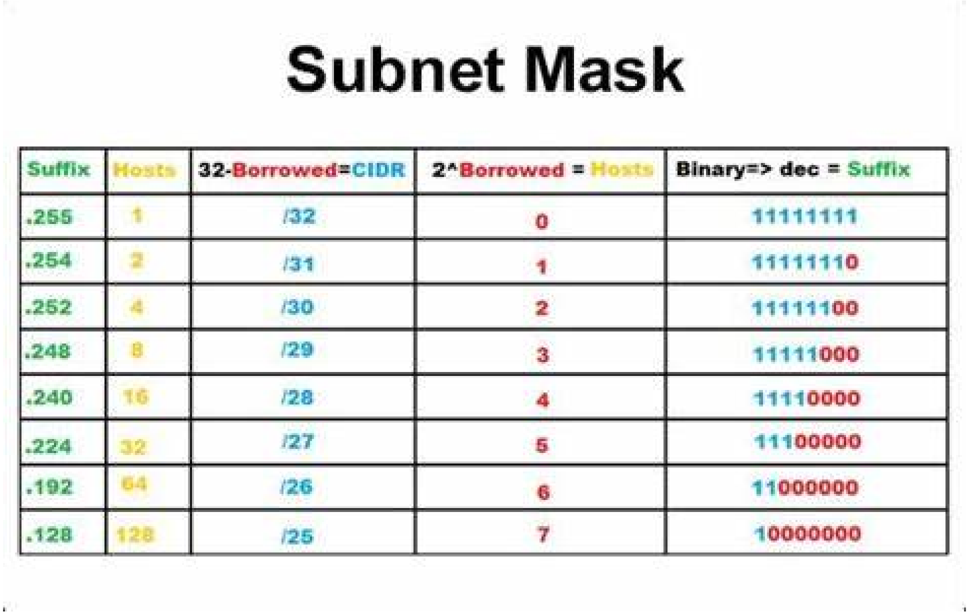


## The Default Subnet Masks (no subnets)

| | 1st octet | 2nd octet | 3rd octet | 4th octet |
|---|---|---|---|---|
| Class A | Network | Host | Host | Host |
| Class B | Network | Network | Host | Host |
| Class C | Network | Network | Network | Host |

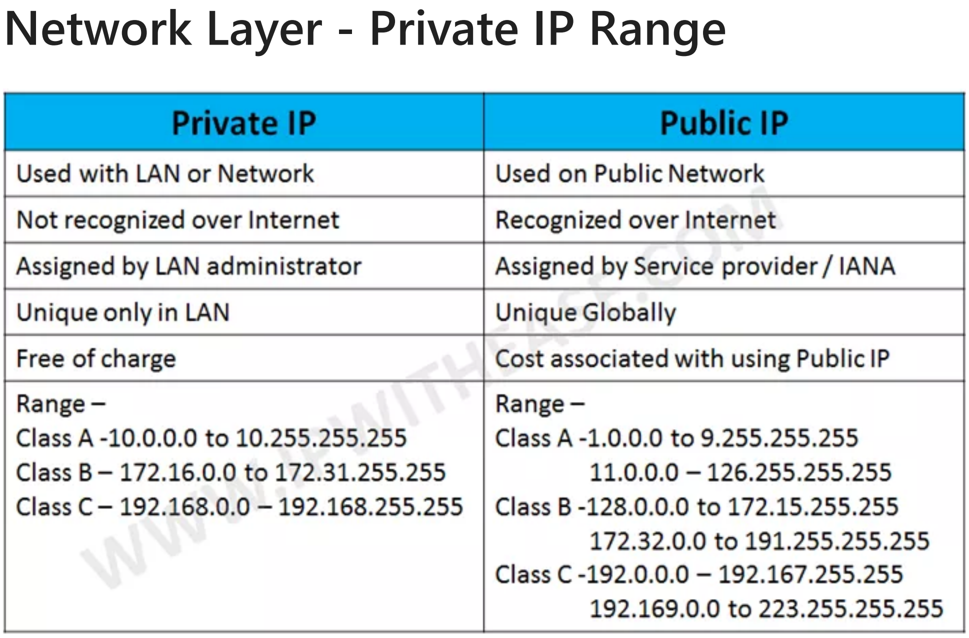
| | | | | |
|---|---|---|---|---|
| Class A or /8 | 11111111 | 00000000 | 00000000 | 00000000 |
| Class B or /16 | 11111111 | 11111111 | 00000000 | 00000000 |
| Class C or /24 | 11111111 | 11111111 | 11111111 | 00000000 |

- A "1" bit in the subnet mask means that the corresponding bit in the IP address should be read as a network number
- A "0" bit in the subnet mask means that the corresponding bit in the IP address should be read as a host bit.
- /n "slash" tells us how many "1" bits are in the subnet mask.



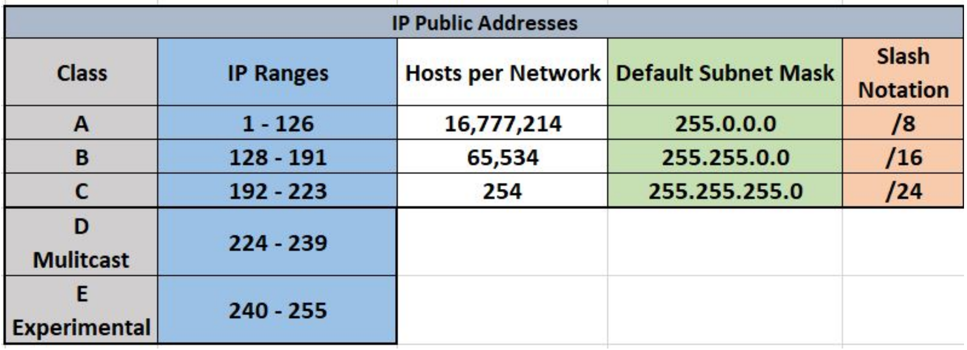
## Subnet Mask

| Suffix | Hosts | 32-Borrowed=CIDR | 2^Borrowed = Hosts | Binary=> dec = Suffix |
|---|---|---|---|---|
| .255 | 1 | /32 | 0 | 11111111 |
| .254 | 2 | /31 | 1 | 11111110 |
| .252 | 4 | /30 | 2 | 11111100 |
| .248 | 8 | /29 | 3 | 11111000 |
| .240 | 16 | /28 | 4 | 11110000 |
| .224 | 32 | /27 | 5 | 11100000 |
| .192 | 64 | /26 | 6 | 11000000 |
| .128 | 128 | /25 | 7 | 10000000 |

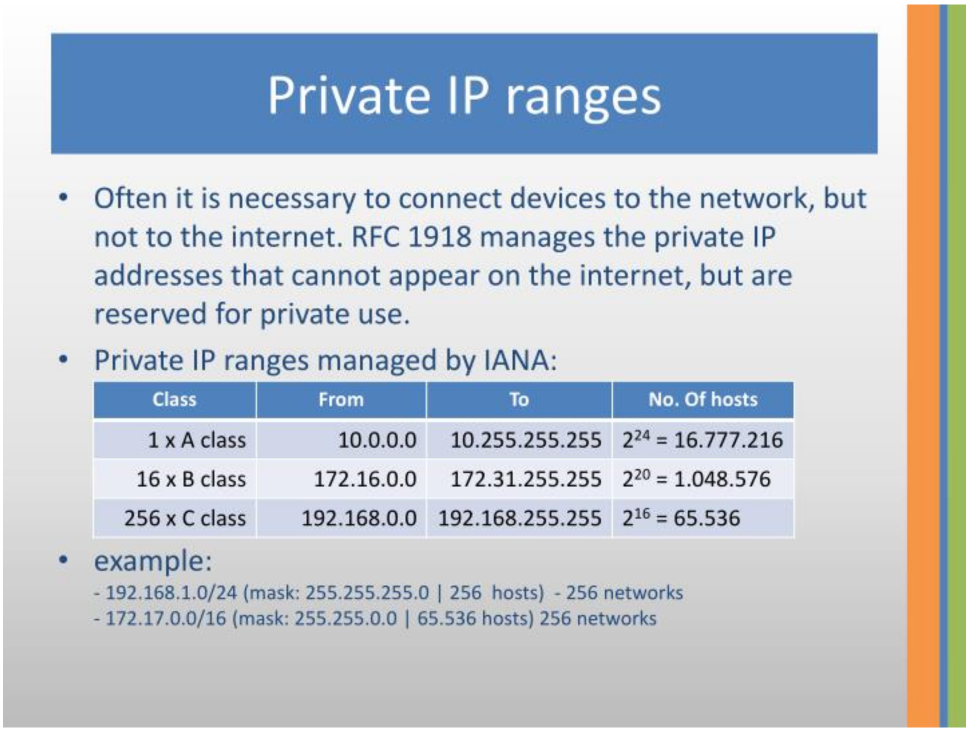


# Network Layer - Private IP Range

| Private IP | Public IP |
|---|---|
| Used with LAN or Network | Used on Public Network |
| Not recognized over Internet | Recognized over Internet |
| Assigned by LAN administrator | Assigned by Service provider / IANA |
| Unique only in LAN | Unique Globally |
| Free of charge | Cost associated with using Public IP |
| Range –<br>Class A -10.0.0.0 to 10.255.255.255<br>Class B – 172.16.0.0 to 172.31.255.255<br>Class C – 192.168.0.0 – 192.168.255.255 | Range –<br>Class A -1.0.0.0 to 9.255.255.255<br>11.0.0.0 – 126.255.255.255<br>Class B -128.0.0.0 to 172.15.255.255<br>172.32.0.0 to 191.255.255.255<br>Class C -192.0.0.0 – 192.167.255.255<br>192.169.0.0 to 223.255.255.255 |



| IP Public Addresses | | | | |
|---|---|---|---|---|
| Class | IP Ranges | Hosts per Network | Default Subnet Mask | Slash Notation |
| A | 1 - 126 | 16,777,214 | 255.0.0.0 | /8 |
| B | 128 - 191 | 65,534 | 255.255.0.0 | /16 |
| C | 192 - 223 | 254 | 255.255.255.0 | /24 |
| D<br>Mulitcast | 224 - 239 | | | |
| E<br>Experimental | 240 - 255 | | | |

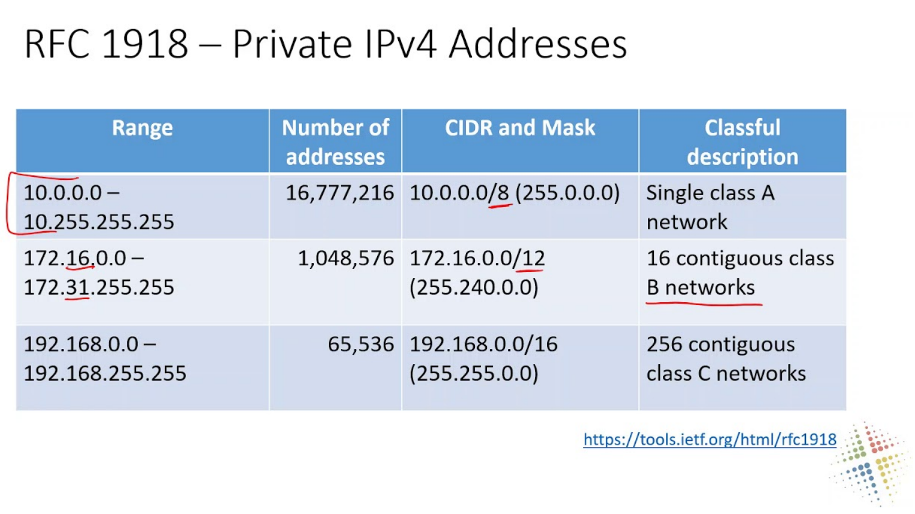


## Private IP ranges

- Often it is necessary to connect devices to the network, but not to the internet. RFC 1918 manages the private IP addresses that cannot appear on the internet, but are reserved for private use.
- Private IP ranges managed by IANA:

| Class | From | To | No. Of hosts |
|---|---|---|---|
| 1 x A class | 10.0.0.0 | 10.255.255.255 | $2^{24}$ = 16.777.216 |
| 16 x B class | 172.16.0.0 | 172.31.255.255 | $2^{20}$ = 1.048.576 |
| 256 x C class | 192.168.0.0 | 192.168.255.255 | $2^{16}$ = 65.536 |

- example:
  - 192.168.1.0/24 (mask: 255.255.255.0 | 256 hosts) - 256 networks
  - 172.17.0.0/16 (mask: 255.255.0.0 | 65.536 hosts) 256 networks

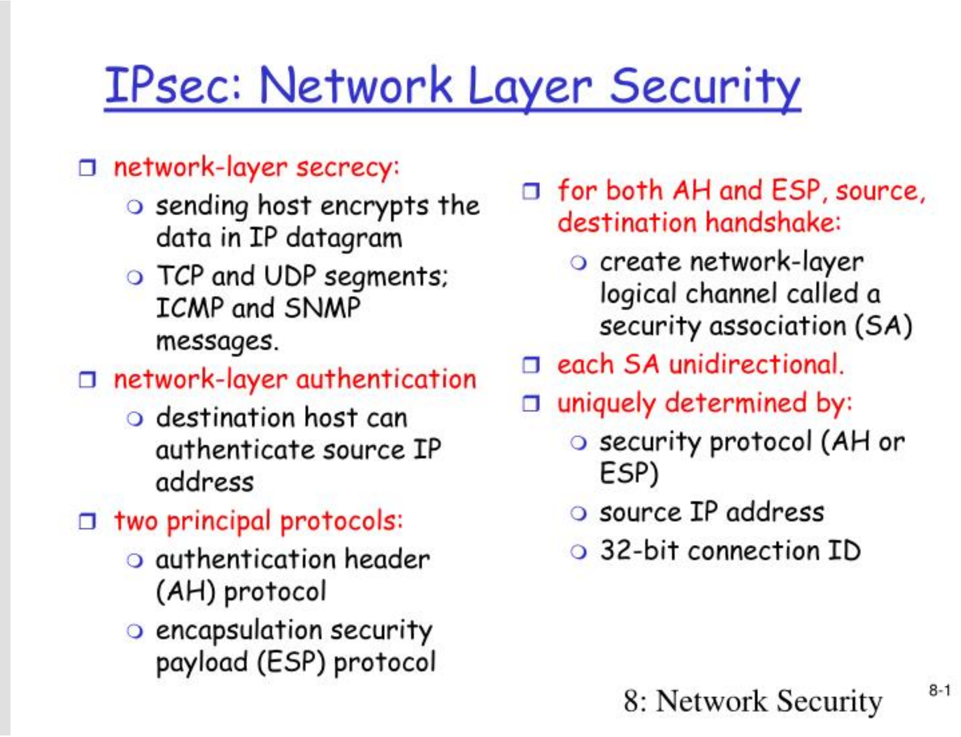


## RFC 1918 – Private IPv4 Addresses

| Range | Number of addresses | CIDR and Mask | Classful description |
|---|---|---|---|
| 10.0.0.0 – 10.255.255.255 | 16,777,216 | 10.0.0.0/8 (255.0.0.0) | Single class A network |
| 172.16.0.0 – 172.31.255.255 | 1,048,576 | 172.16.0.0/12 (255.240.0.0) | 16 contiguous class B networks |
| 192.168.0.0 – 192.168.255.255 | 65,536 | 192.168.0.0/16 (255.255.0.0) | 256 contiguous class C networks |

https://tools.ietf.org/html/rfc1918

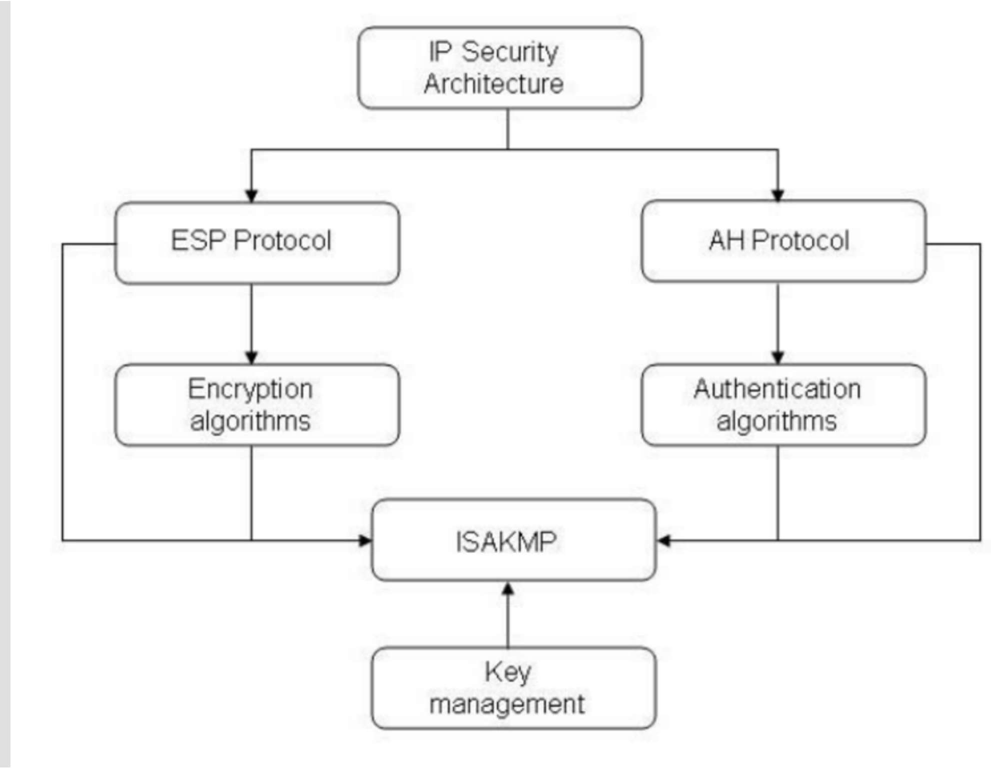
# CyberSecurity - IPSec

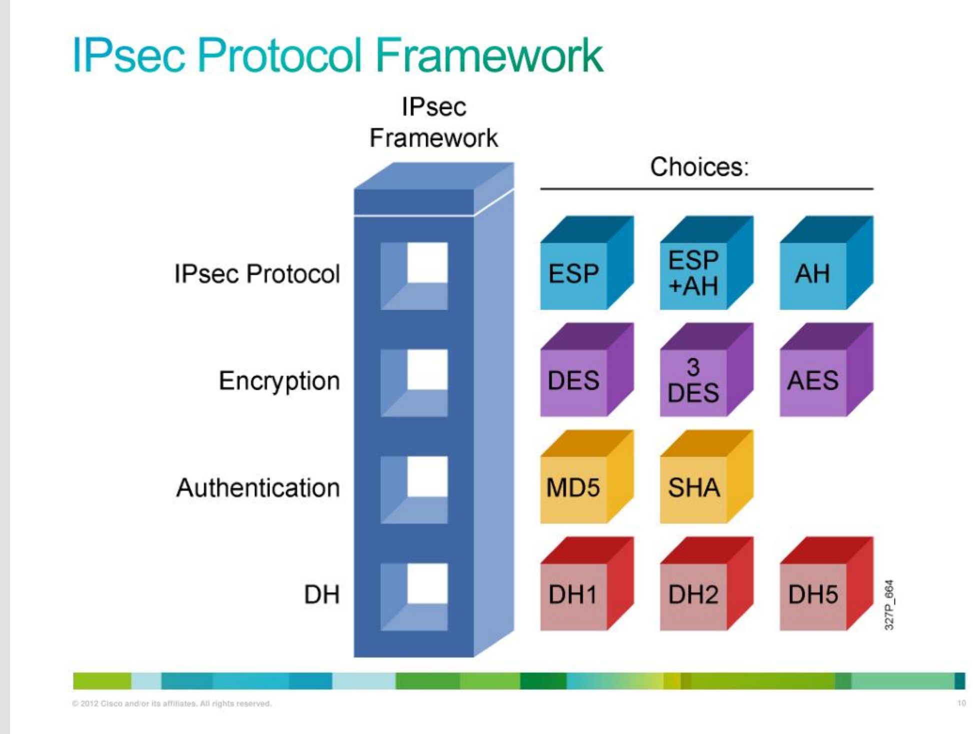


# IPsec: Network Layer Security

- network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages.
- network-layer authentication
  - destination host can authenticate source IP address
- two principal protocols:
  - authentication header (AH) protocol
  - encapsulation security payload (ESP) protocol
- for both AH and ESP, source, destination handshake:
  - create network-layer logical channel called a security association (SA)
- each SA unidirectional.
- uniquely determined by:
  - security protocol (AH or ESP)
  - source IP address
  - 32-bit connection ID

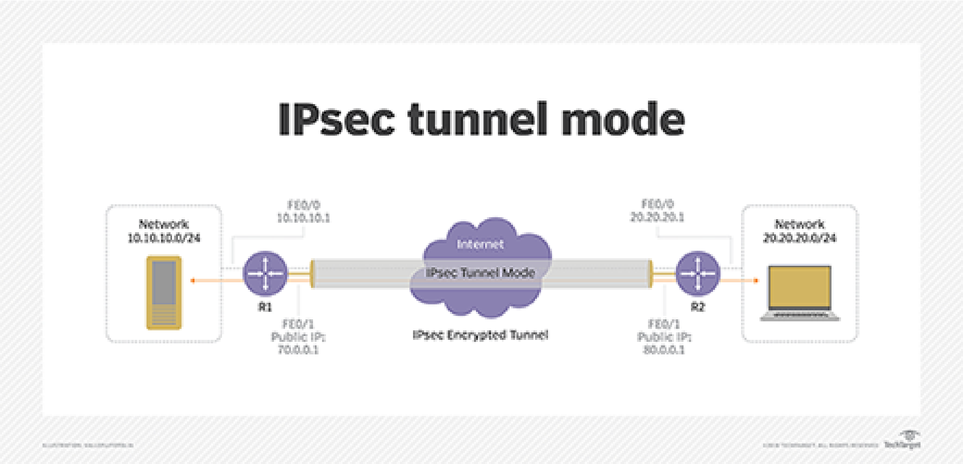
8: Network Security 8-1





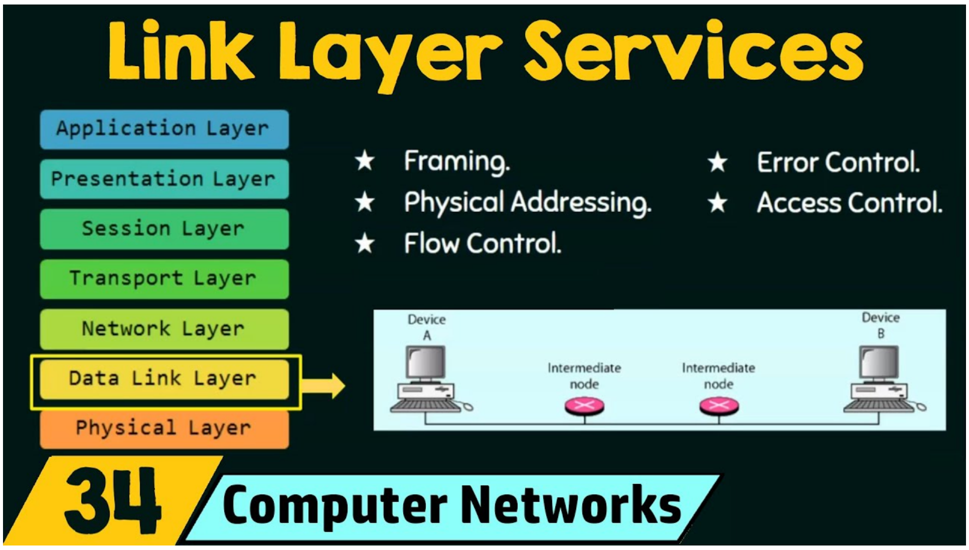
IPsec Protocol Framework

| IPsec Framework | Choices: | | |
|---|---|---|---|
| IPsec Protocol | ESP | ESP +AH | AH |
| Encryption | DES | 3 DES | AES |
| Authentication | MD5 | SHA | |
| DH | DH1 | DH2 | DH5 |



IPsec tunnel mode

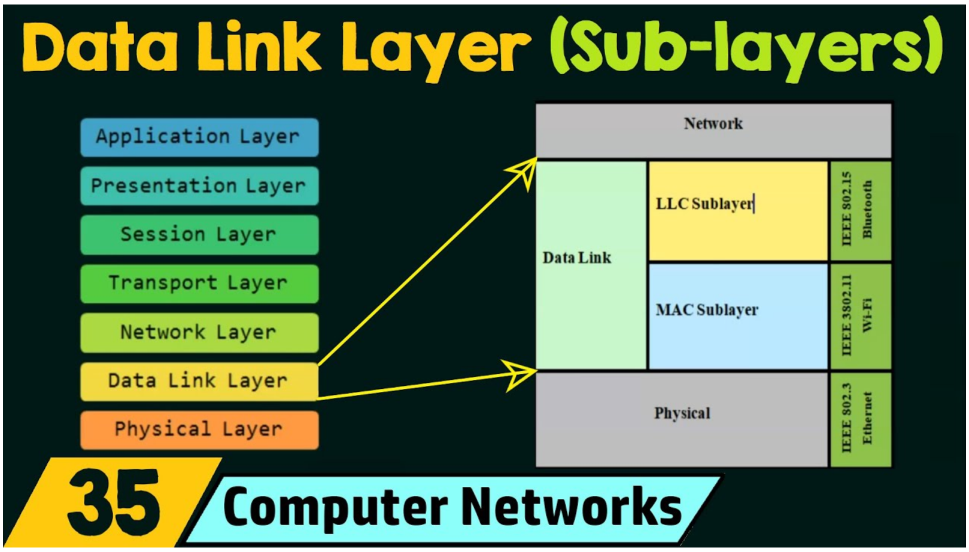
## Datalink Layer

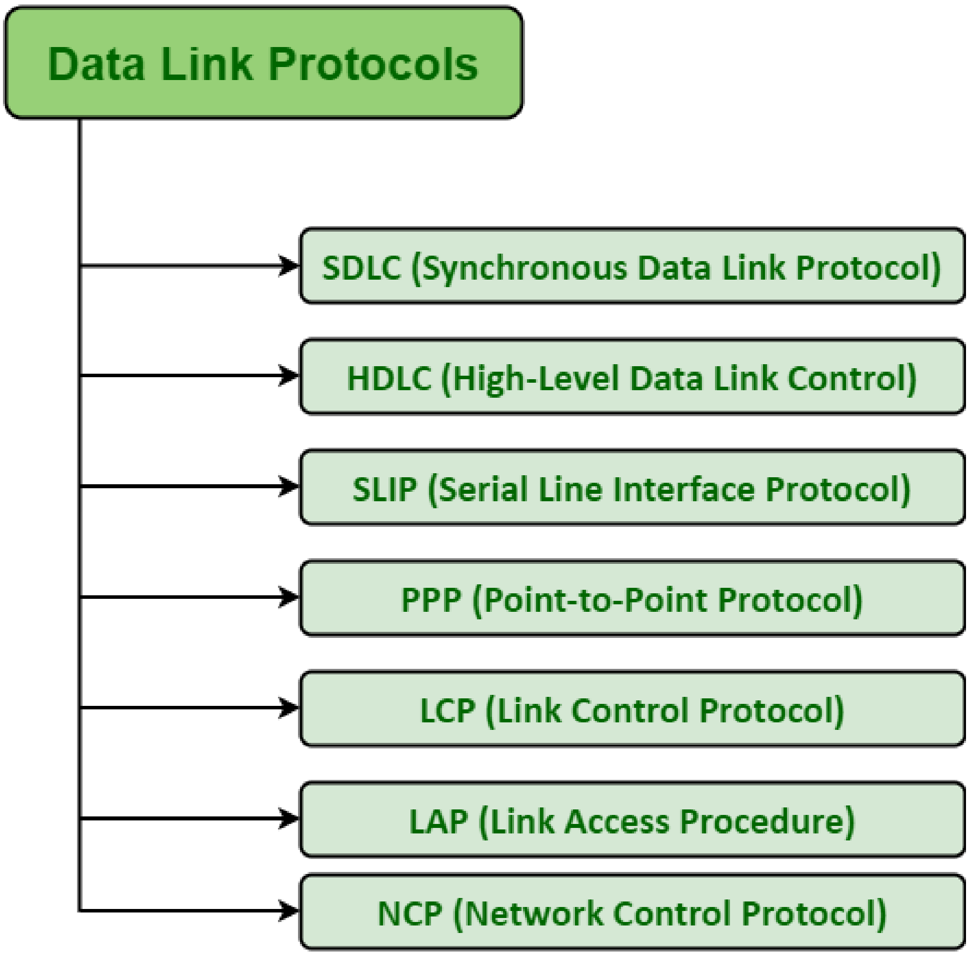


Link Layer Services

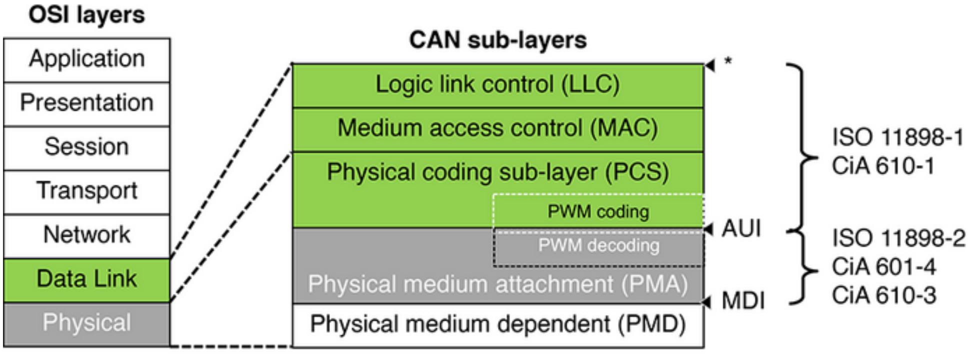
- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

★ Framing.
★ Physical Addressing.
★ Flow Control.
★ Error Control.
★ Access Control.

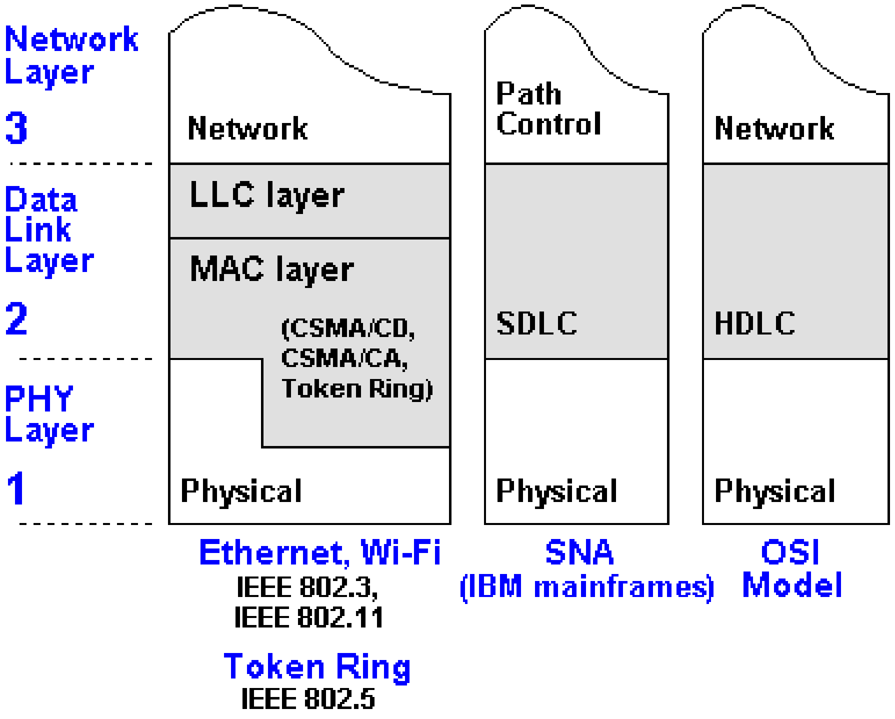


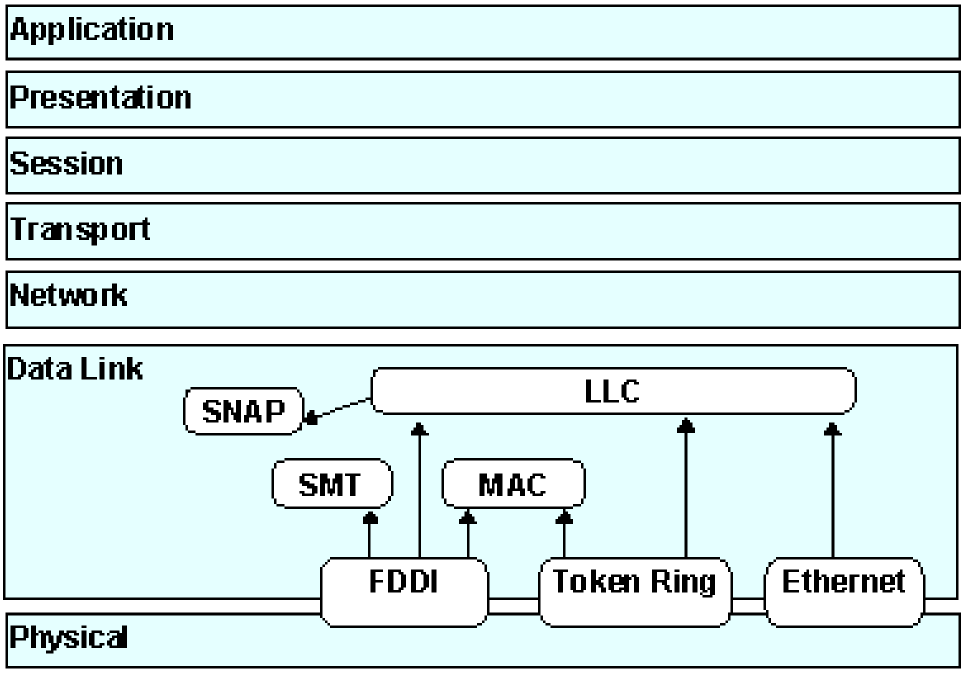

Data Link Protocols

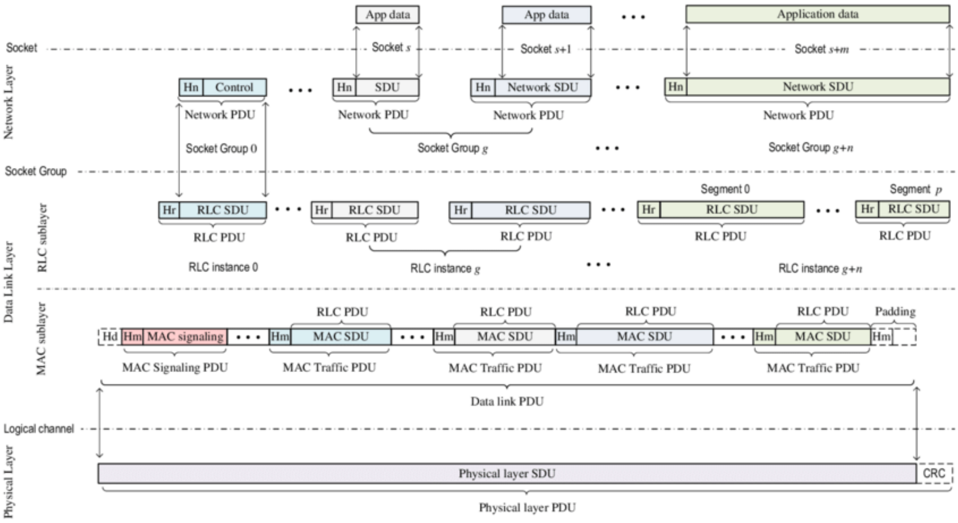
- SDLC (Synchronous Data Link Protocol)
- HDLC (High-Level Data Link Control)
- SLIP (Serial Line Interface Protocol)
- PPP (Point-to-Point Protocol)
- LCP (Link Control Protocol)
- LAP (Link Access Procedure)
- NCP (Network Control Protocol)



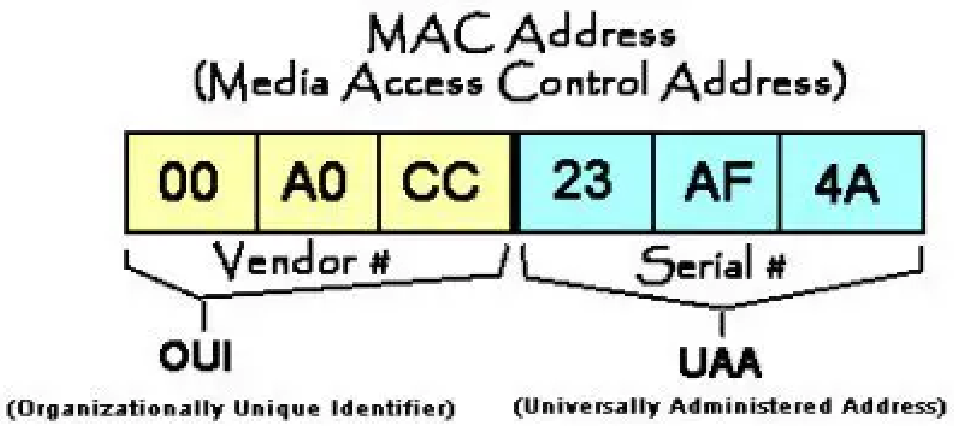
**Key**
AUI attachment unit interface
MDI medium dependent interface
* not (yet) standardized

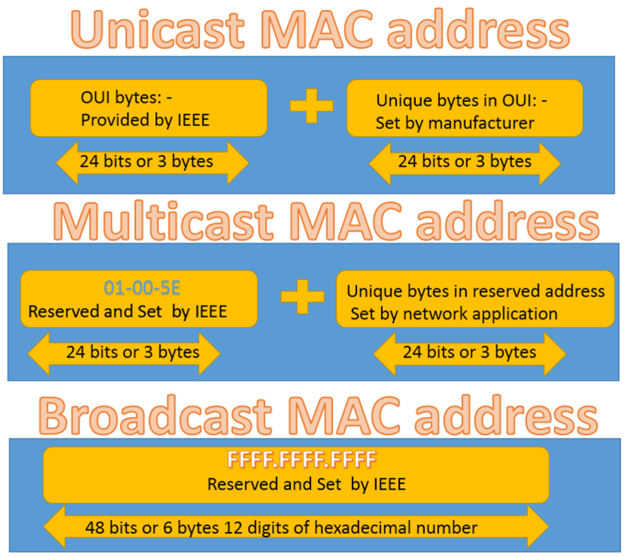

Network Layer 3
Data Link Layer 2
PHY Layer 1
Network
LLC layer
MAC layer
(CSMA/CD, CSMA/CA, Token Ring)
Physical
Path Control
SDLC
Physical
Network
HDLC
Physical
Ethernet, Wi-Fi
IEEE 802.3, IEEE 802.11
Token Ring
IEEE 802.5
SNA
(IBM mainframes)
OSI Model


Application
Presentation
Session
Transport
Network
Data Link
SNAP
LLC
SMT
MAC
FDDI
Token Ring
Ethernet
Physical


Socket
Network Layer
App data
Socket s
App data
Socket s+1
Application data
Socket s+m
Hn
Control
Hn
SDU
Hn
Network SDU
Hn
Network SDU
Network PDU
Network PDU
Network PDU
Network PDU
Socket Group 0
Socket Group g
Socket Group g+n
Socket Group
Data Link Layer
RLC sublayer
Segment 0
Segment p
Hr
RLC SDU
RLC PDU
RLC instance 0
RLC instance g
RLC instance g+n
MAC sublayer
RLC PDU
Padding
Hd
Hm
MAC signaling
MAC SDU
MAC Signaling PDU
MAC Traffic PDU
Data link PDU
Logical channel
Physical Layer
Physical layer SDU
CRC
Physical layer PDU

## Datalink Layer - MAC Address


MAC Address
(Media Access Control Address)
00
A0
CC
23
AF
4A
Vendor #
Serial #
OUI
(Organizationally Unique Identifier)
UAA
(Universally Administered Address)



Unicast MAC address

OUI bytes: -
Provided by IEEE

Unique bytes in OUI: -
Set by manufacturer

24 bits or 3 bytes

24 bits or 3 bytes

Multicast MAC address

01-00-5E
Reserved and Set by IEEE

Unique bytes in reserved address
Set by network application

24 bits or 3 bytes

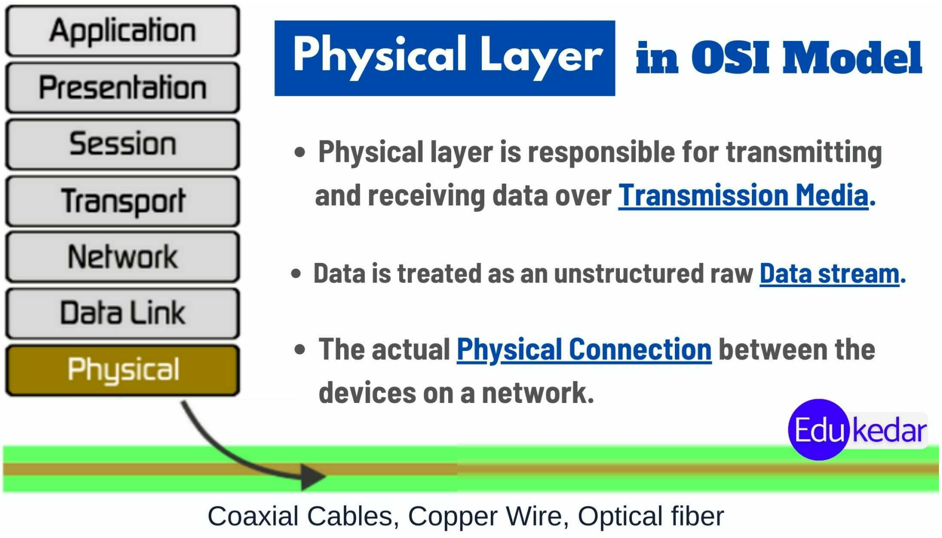
24 bits or 3 bytes

Broadcast MAC address

FFFF.FFFF.FFFF
Reserved and Set by IEEE

48 bits or 6 bytes 12 digits of hexadecimal number

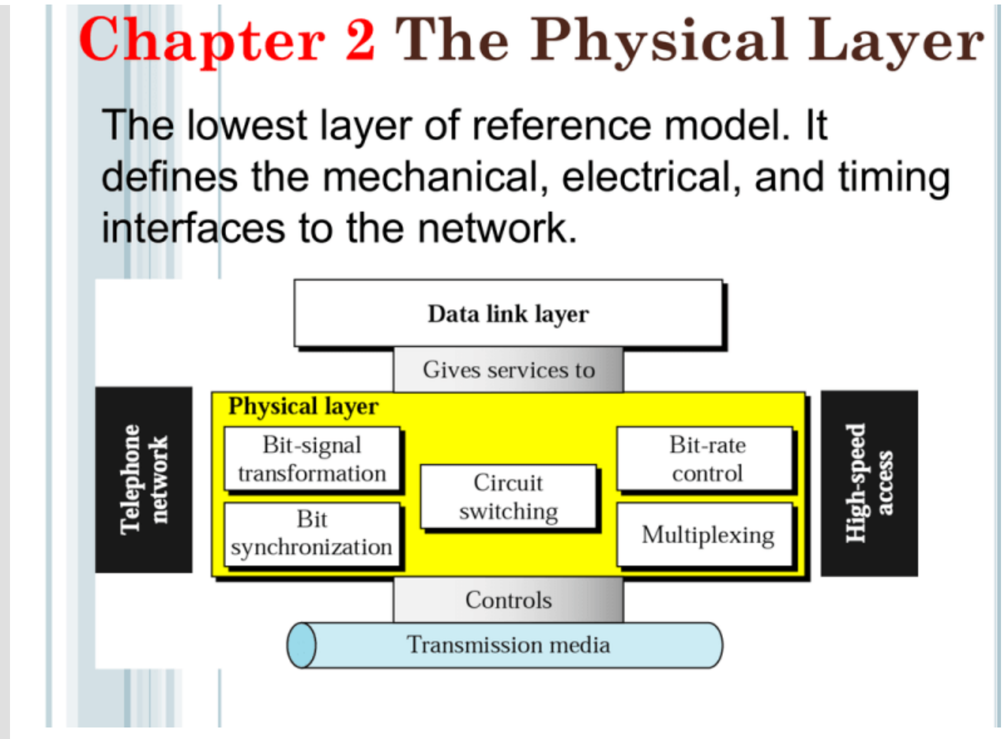
## Physical Layer



Physical Layer in OSI Model

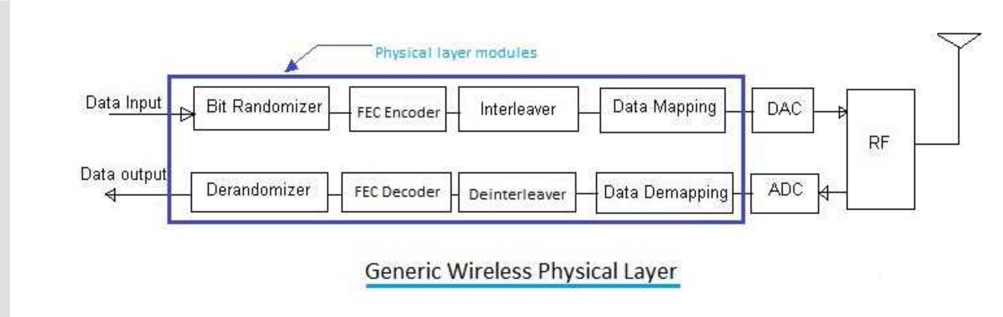
- Physical layer is responsible for transmitting and receiving data over Transmission Media.
- Data is treated as an unstructured raw Data stream.
- The actual Physical Connection between the devices on a network.

Coaxial Cables, Copper Wire, Optical fiber

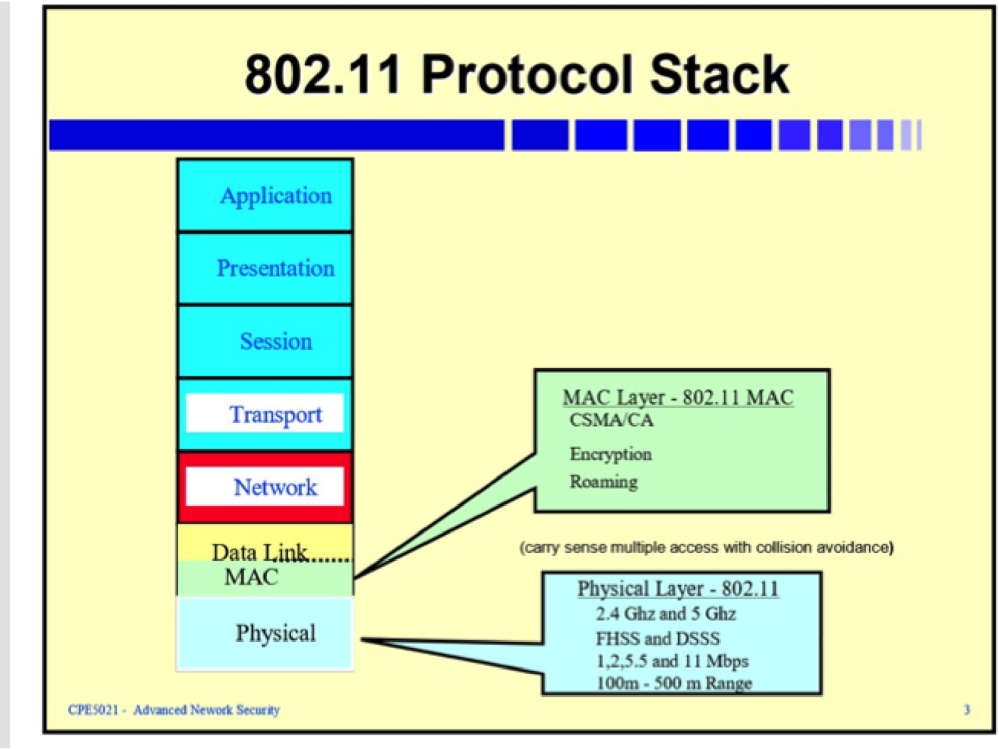


# Chapter 2 The Physical Layer

The lowest layer of reference model. It defines the mechanical, electrical, and timing interfaces to the network.



Generic Wireless Physical Layer



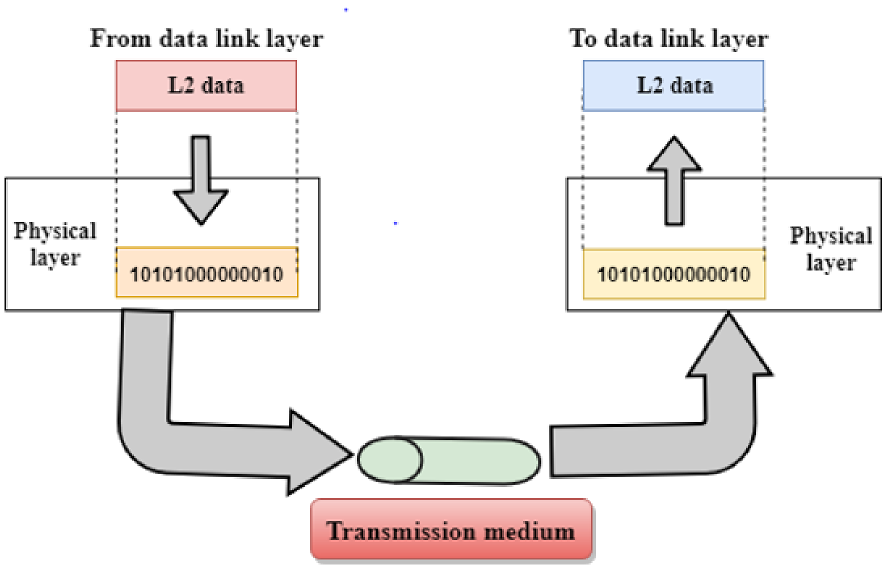
## 802.11 Protocol Stack

MAC Layer - 802.11 MAC
CSMA/CA
Encryption
Roaming

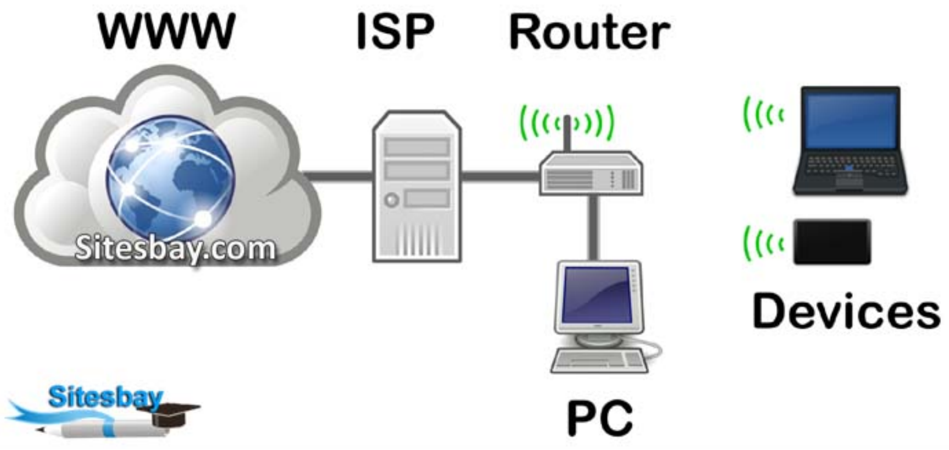
(carry sense multiple access with collision avoidance)

Physical Layer - 802.11
2.4 Ghz and 5 Ghz
FHSS and DSSS
1,2,5.5 and 11 Mbps
100m - 500 m Range

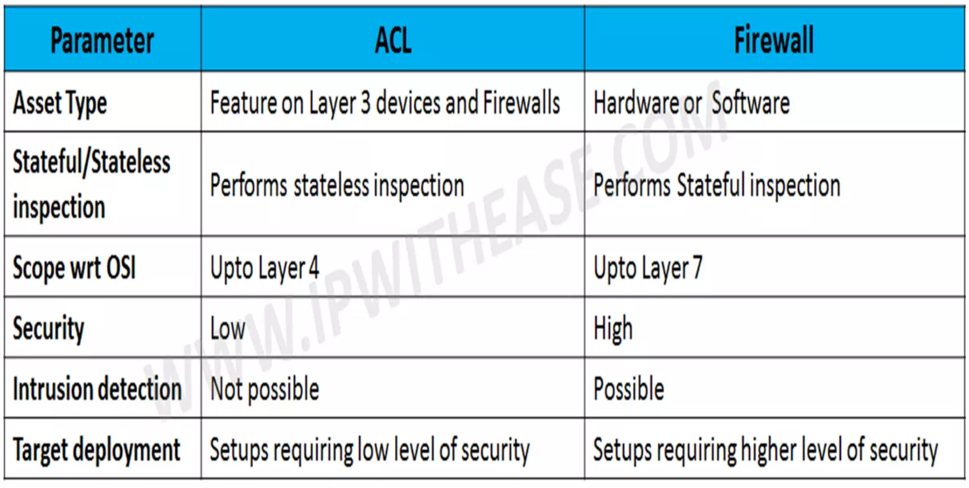
CPE5021 - Advanced Nework Security 3



## Router

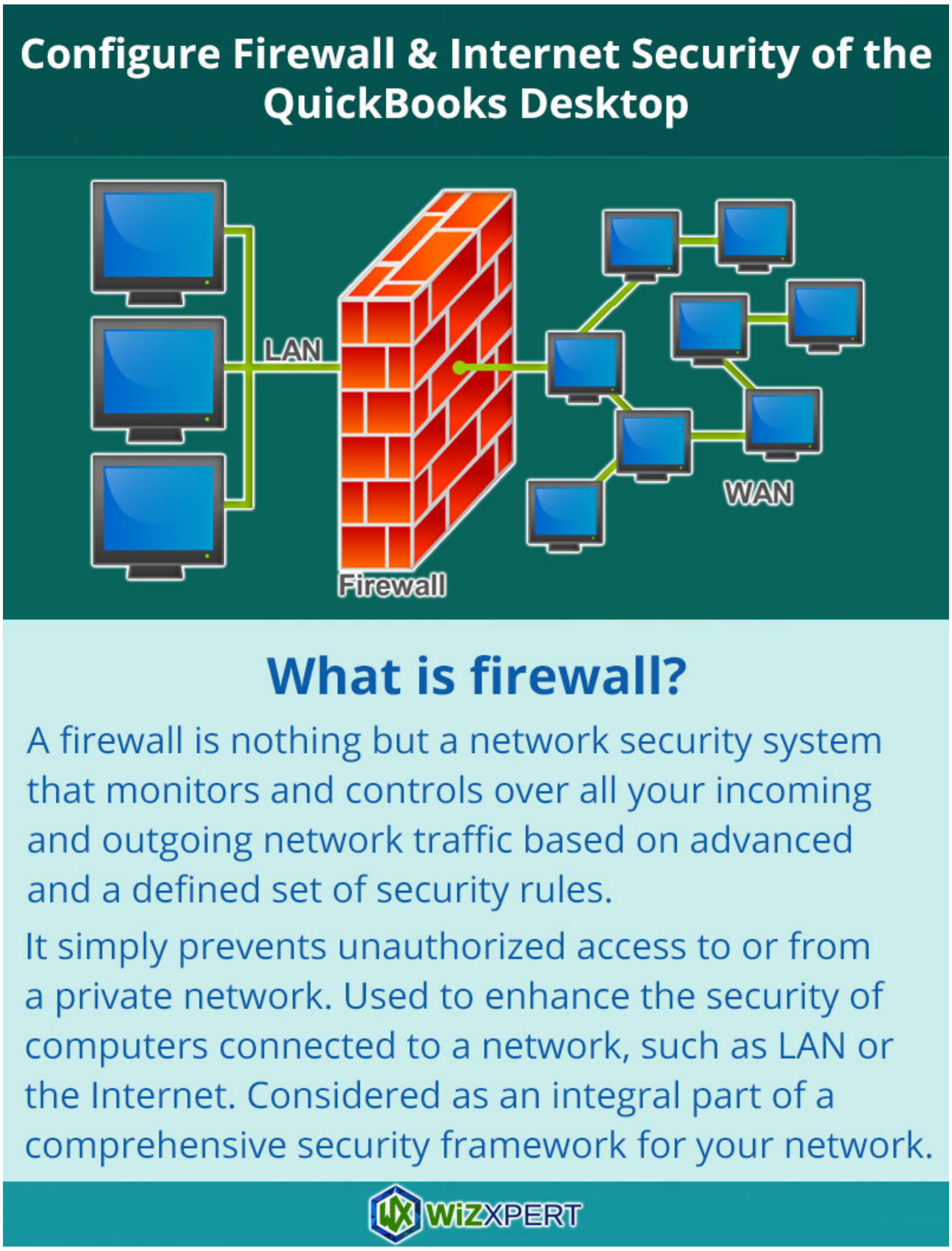


## ACL (Access Control List)



| Parameter | ACL | Firewall |
|---|---|---|
| Asset Type | Feature on Layer 3 devices and Firewalls | Hardware or Software |
| Stateful/Stateless inspection | Performs stateless inspection | Performs Stateful inspection |
| Scope wrt OSI | Upto Layer 4 | Upto Layer 7 |
| Security | Low | High |
| Intrusion detection | Not possible | Possible |
| Target deployment | Setups requiring low level of security | Setups requiring higher level of security |

## Firewall

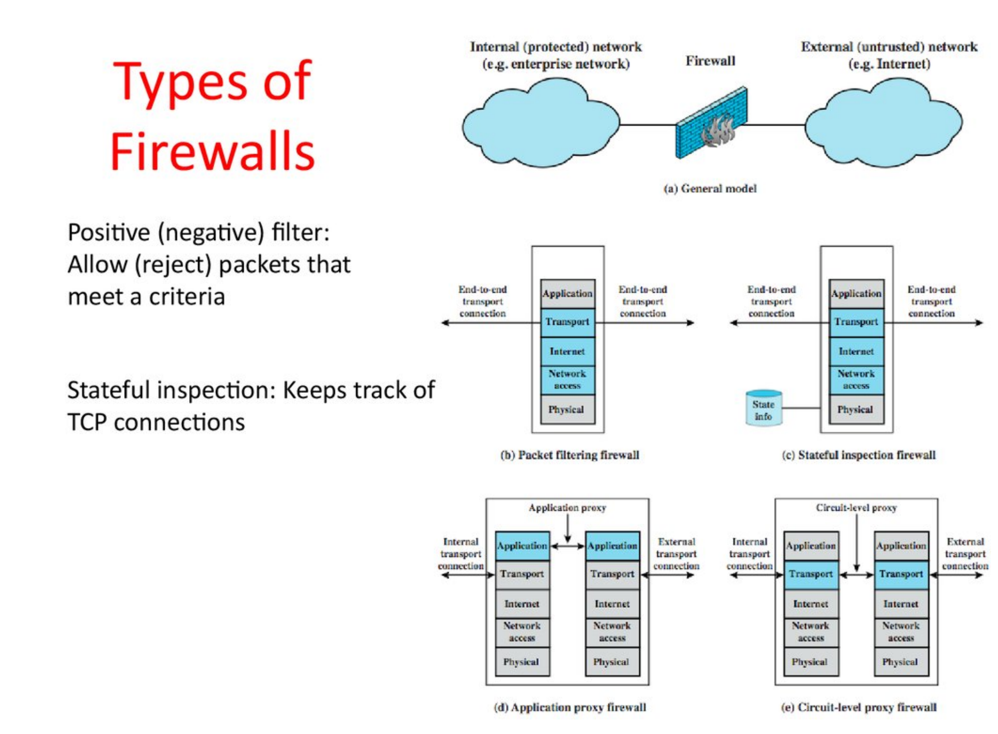


## Configure Firewall & Internet Security of the QuickBooks Desktop

## What is firewall?

A firewall is nothing but a network security system that monitors and controls over all your incoming and outgoing network traffic based on advanced and a defined set of security rules.

It simply prevents unauthorized access to or from a private network. Used to enhance the security of computers connected to a network, such as LAN or the Internet. Considered as an integral part of a comprehensive security framework for your network.



## Types of Firewalls

Positive (negative) filter: Allow (reject) packets that meet a criteria

Stateful inspection: Keeps track of TCP connections

Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info
Application proxy
Internal transport connection
External transport connection
Circuit-level proxy

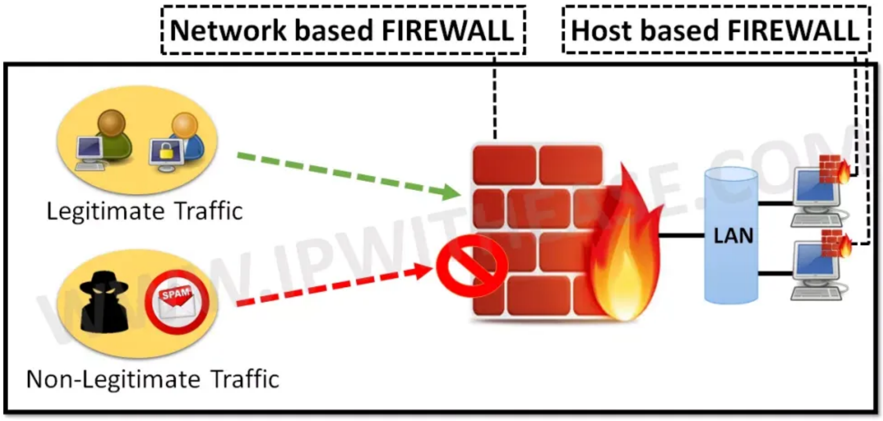
(a) General model

(b) Packet filtering firewall

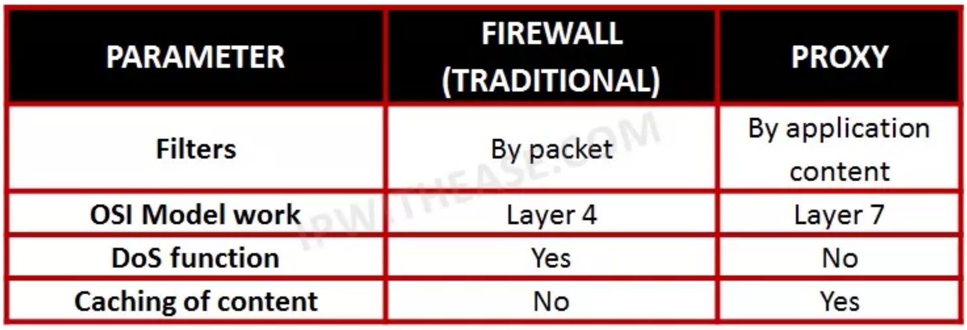
(c) Stateful inspection firewall

(d) Application proxy firewall

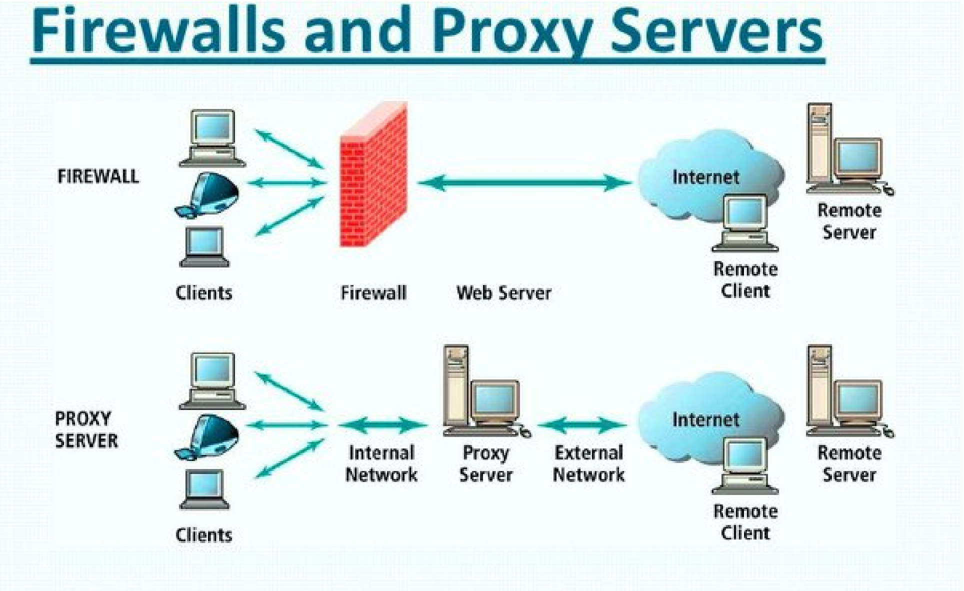
(e) Circuit-level proxy firewall

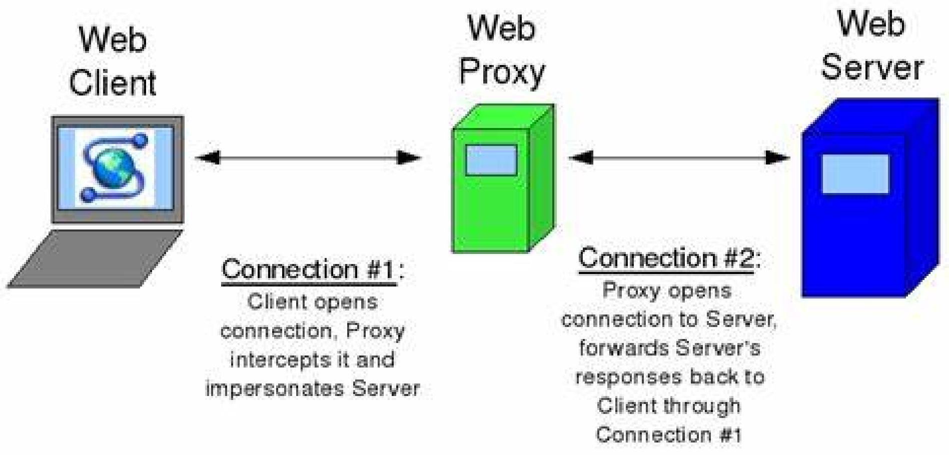


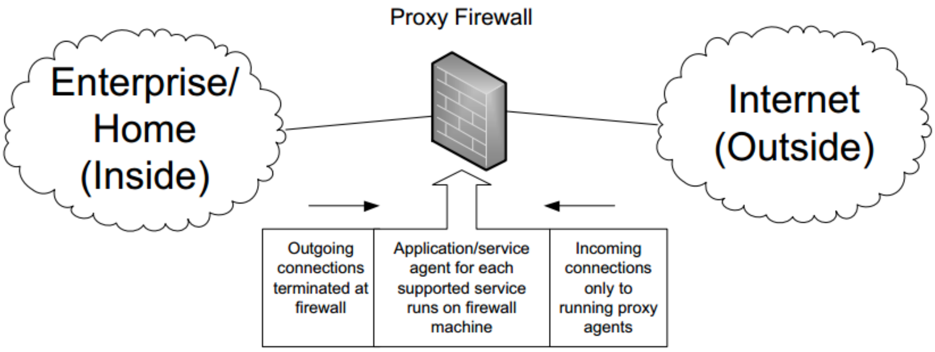
## Proxy



| PARAMETER | FIREWALL (TRADITIONAL) | PROXY |
|---|---|---|
| Filters | By packet | By application content |
| OSI Model work | Layer 4 | Layer 7 |
| DoS function | Yes | No |
| Caching of content | No | Yes |




Web Client
Web Proxy
Web Server
Connection #1: Client opens connection, Proxy intercepts it and impersonates Server
Connection #2: Proxy opens connection to Server, forwards Server's responses back to Client through Connection #1


Proxy Firewall
Enterprise/ Home (Inside)
Internet (Outside)
Outgoing connections terminated at firewall
Application/service agent for each supported service runs on firewall machine
Incoming connections only to running proxy agents

## Proxy Cache

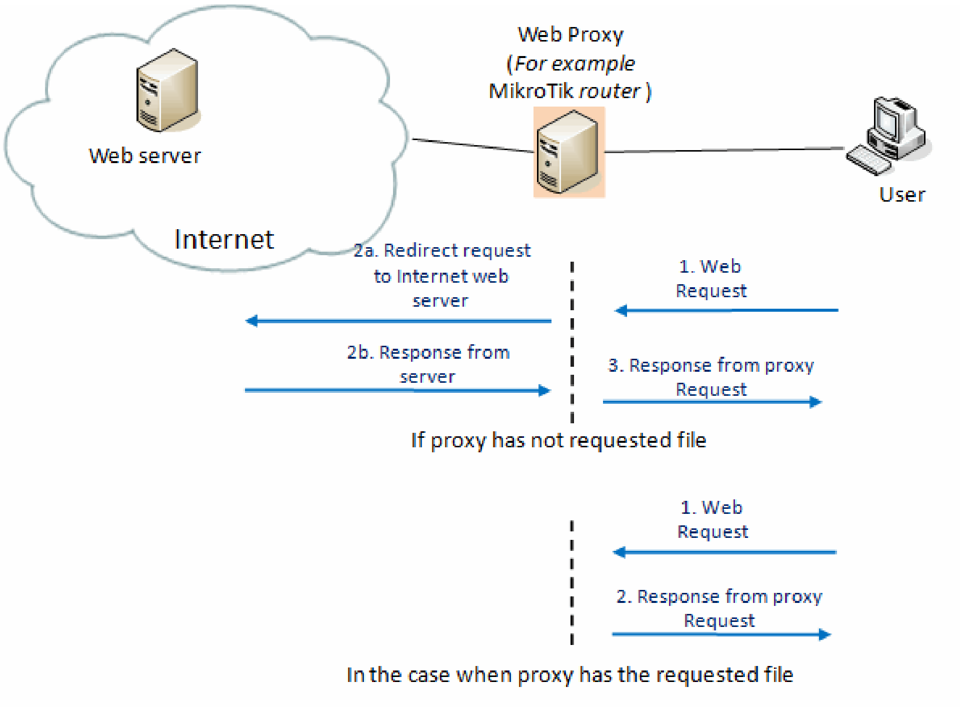
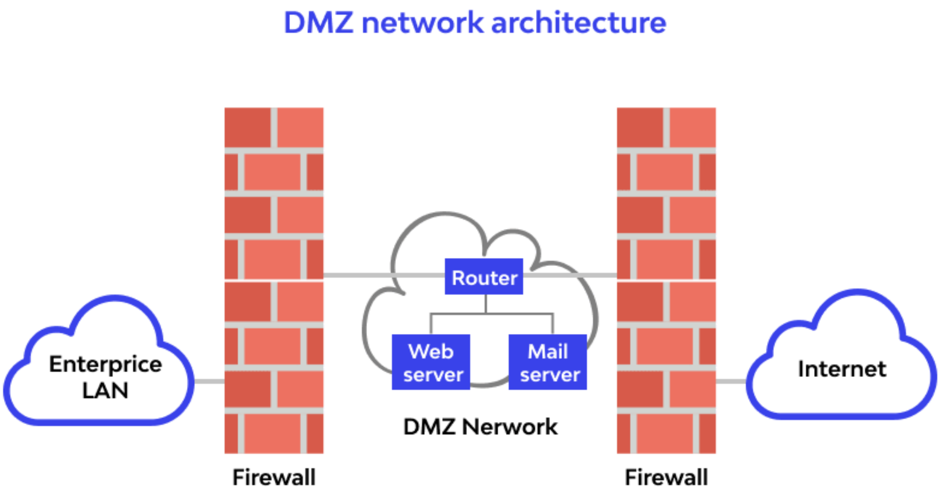
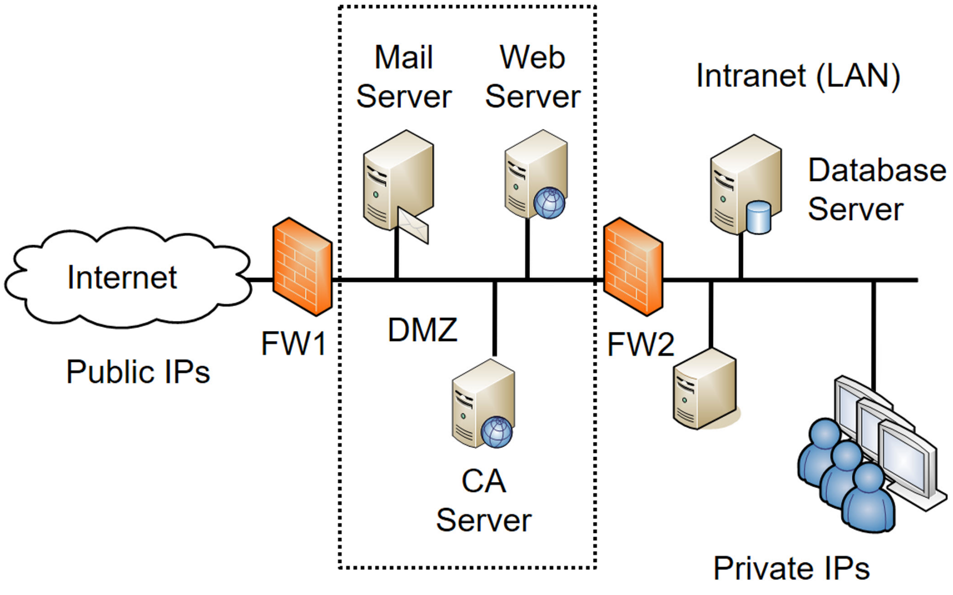
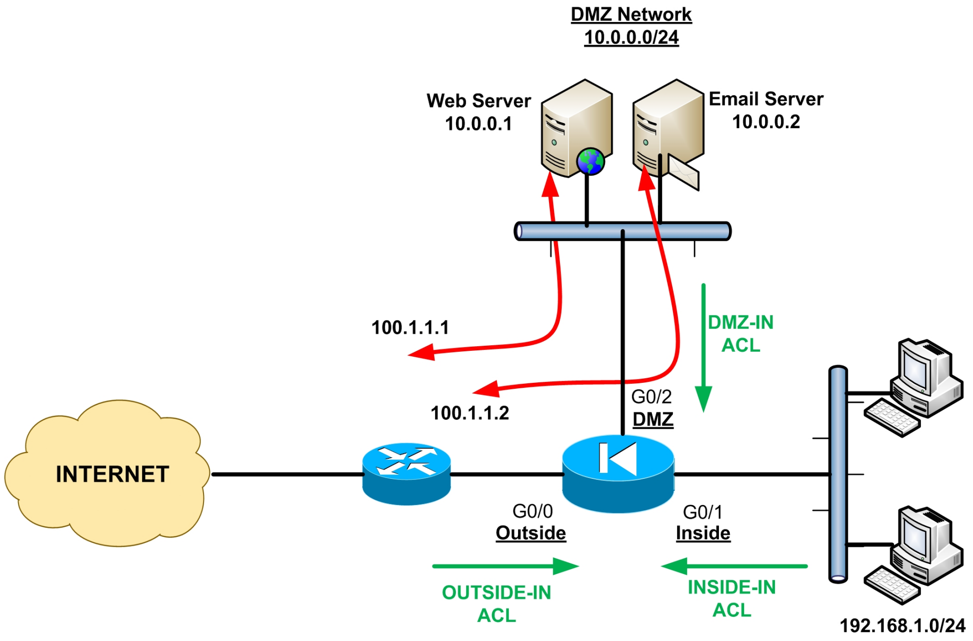

Web Proxy
(For example
MikroTik router )
Web server
Internet
User
2a. Redirect request to Internet web server
2b. Response from server
1. Web Request
3. Response from proxy Request
If proxy has not requested file
1. Web Request
2. Response from proxy Request
In the case when proxy has the requested file

Figure 10.1. Web proxy basic operation scheme

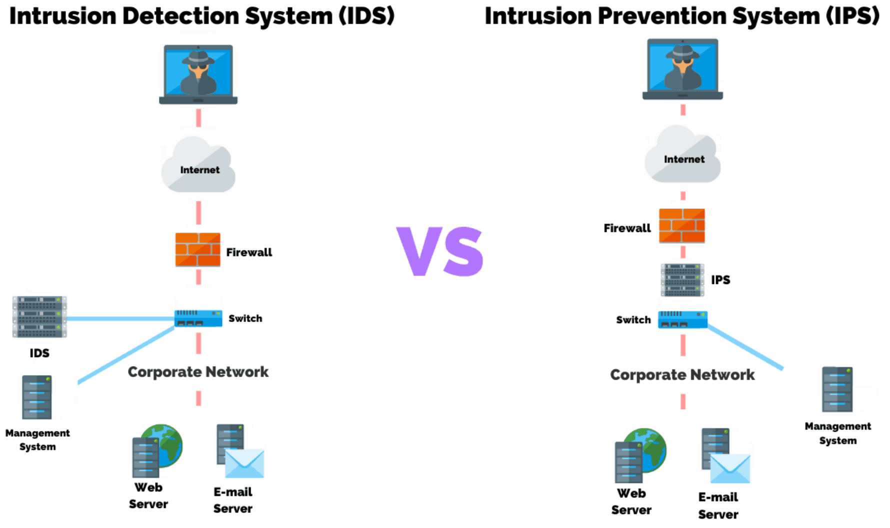
# DMZ

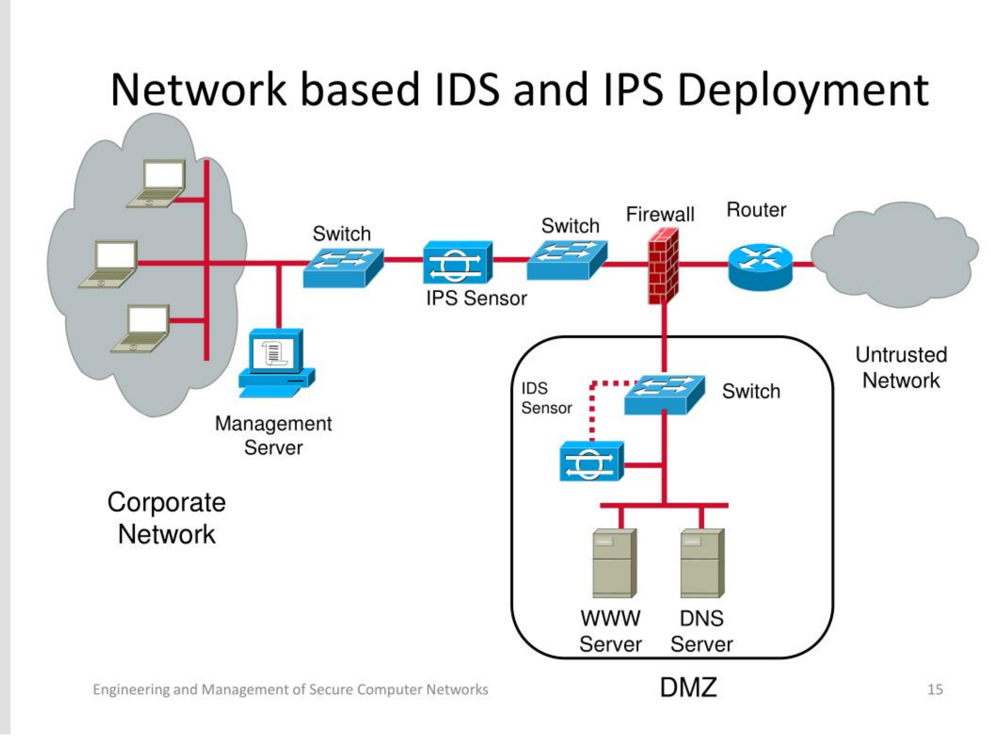



Mail Server
Web Server
Intranet (LAN)
Database Server
Internet
Public IPs
FW1
DMZ
FW2
CA Server
Private IPs


DMZ Network
10.0.0.0/24
Web Server
10.0.0.1
Email Server
10.0.0.2
100.1.1.1
DMZ-IN
ACL
100.1.1.2
G0/2
DMZ
INTERNET
G0/0
Outside
G0/1
Inside
OUTSIDE-IN
ACL
INSIDE-IN
ACL
192.168.1.0/24

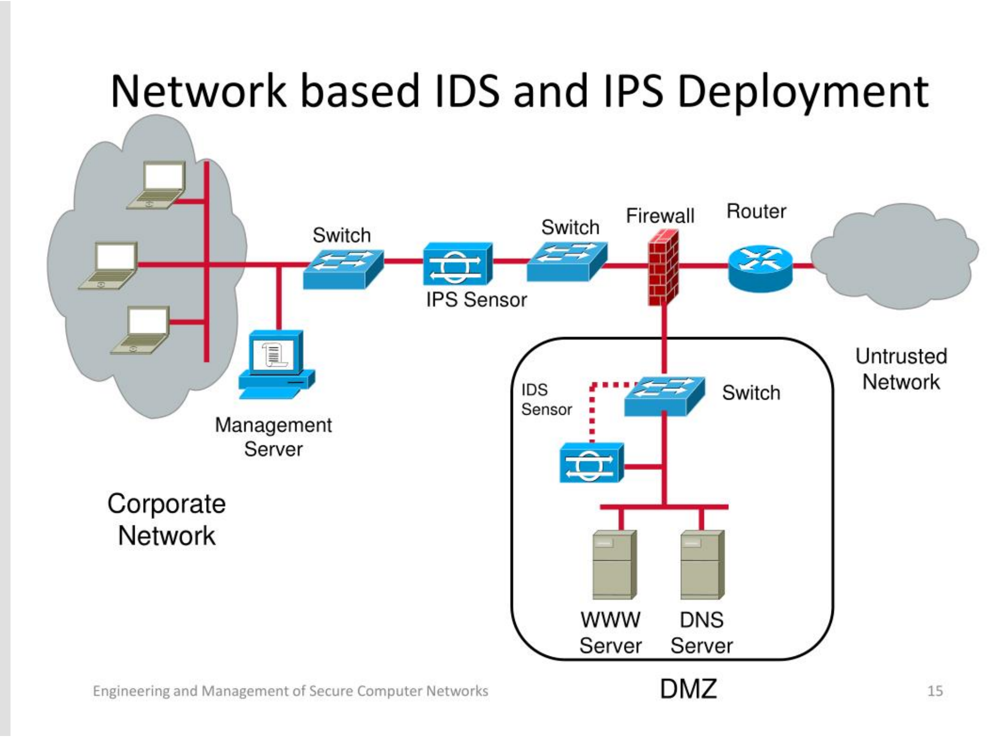
# IPS/IDS


Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)
Internet
Firewall
Switch
IDS
Corporate Network
Management System
Web Server
E-mail Server
VS
Internet
Firewall
IPS
Switch
Corporate Network
Management System
Web Server
E-mail Server



Network based IDS and IPS Deployment

Engineering and Management of Secure Computer Networks 15



Network based IDS and IPS Deployment

Engineering and Management of Secure Computer Networks 15

# Routing Protocol

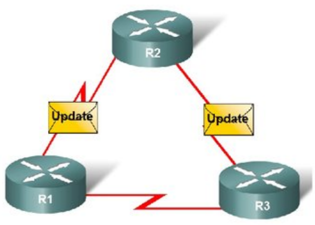
# Dynamic IP Routing Protocols

Routing Protocols learn and **dynamically** share information about the networks connected to each other therefore these protocols are called **dynamic protocols**.

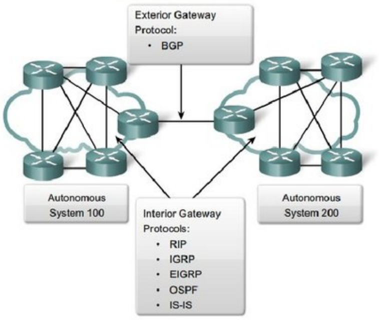
There are quite many dynamic routing protocols for routing IP packets. The most common protocols are:

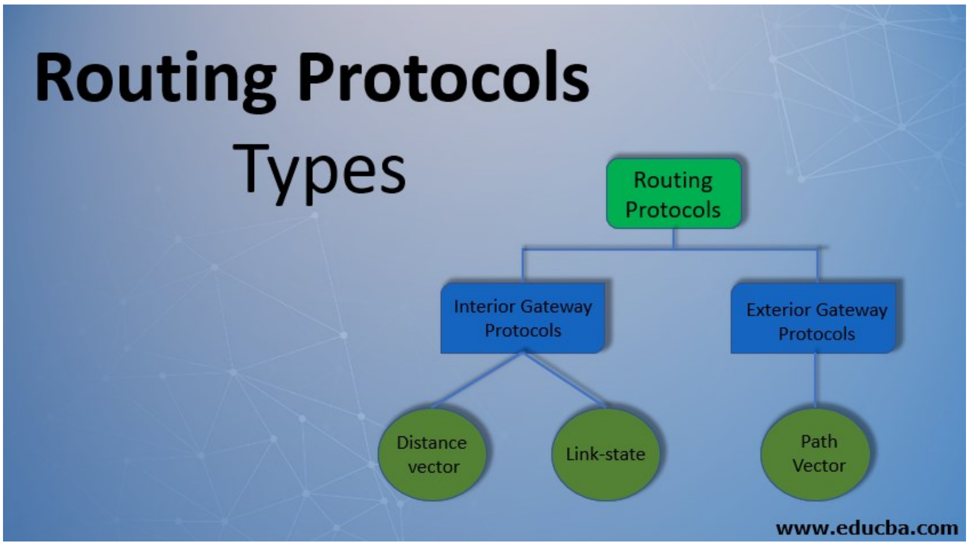
- **RIP** (Routing Information Protocol);
- **IGRP** (Interior Gateway Routing Protocol);
- **EIGRP** (Enhanced Interior Gateway Routing Protocol);
- **OSPF** (Open Shortest Path First);
- **IS-IS** (Intermediate System-to-Intermediate System) *(pronounced "i-s i-s" or more commonly "Eye-Sis");*
- **BGP** (Border Gateway Protocol).

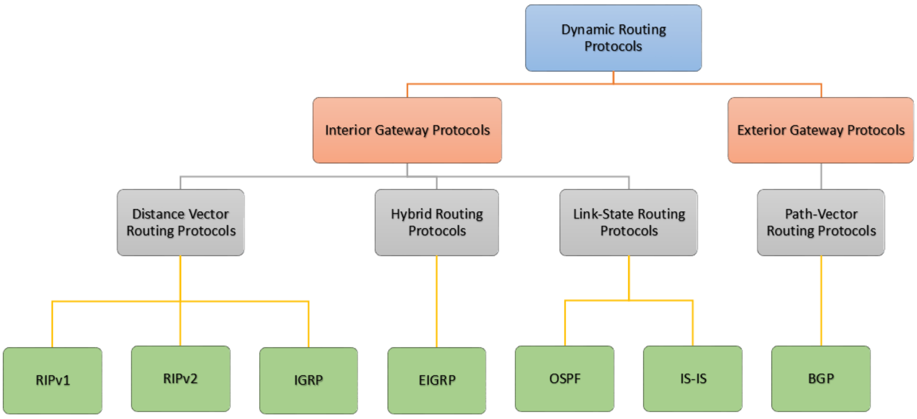
Routers Dynamically Pass Updates

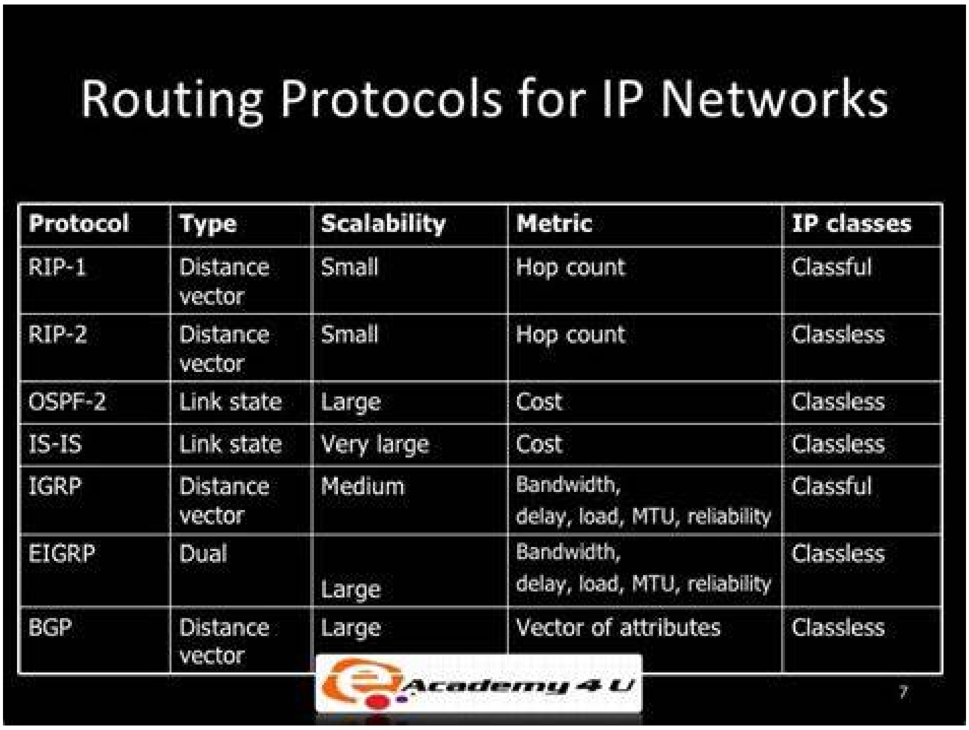


IGP vs. EGP Routing Protocols





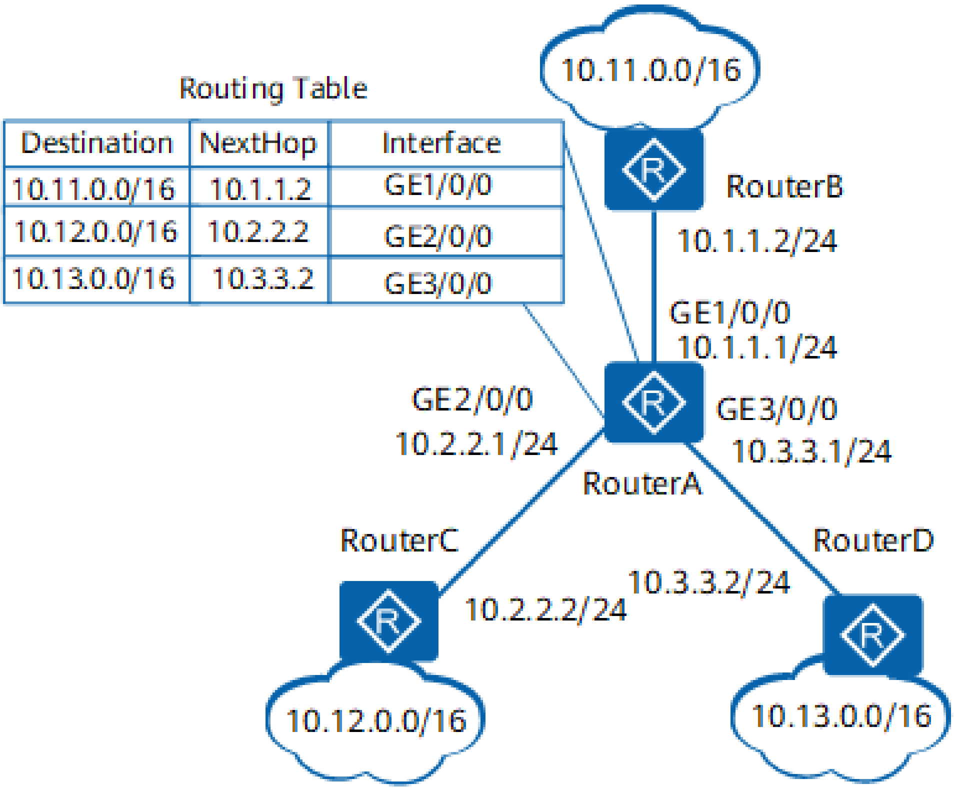

Dynamic Routing Protocols
Interior Gateway Protocols
Exterior Gateway Protocols
Distance Vector Routing Protocols
Hybrid Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocols
RIPv1
RIPv2
IGRP
EIGRP
OSPF
IS-IS
BGP



## Routing Protocols for IP Networks

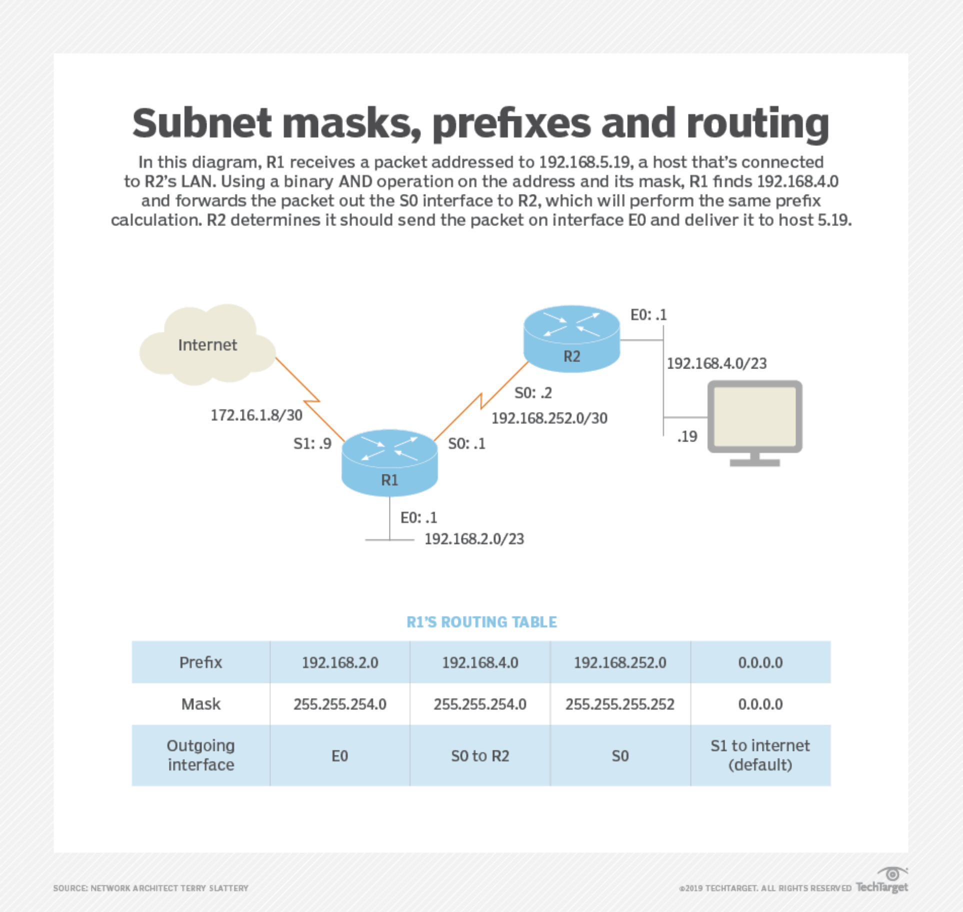
| Protocol | Type | Scalability | Metric | IP classes |
|---|---|---|---|---|
| RIP-1 | Distance vector | Small | Hop count | Classful |
| RIP-2 | Distance vector | Small | Hop count | Classless |
| OSPF-2 | Link state | Large | Cost | Classless |
| IS-IS | Link state | Very large | Cost | Classless |
| IGRP | Distance vector | Medium | Bandwidth, delay, load, MTU, reliability | Classful |
| EIGRP | Dual | Large | Bandwidth, delay, load, MTU, reliability | Classless |
| BGP | Distance vector | Large | Vector of attributes | Classless |

## Routing Table



Routing Table

| Destination | NextHop | Interface |
|---|---|---|
| 10.11.0.0/16 | 10.1.1.2 | GE1/0/0 |
| 10.12.0.0/16 | 10.2.2.2 | GE2/0/0 |
| 10.13.0.0/16 | 10.3.3.2 | GE3/0/0 |



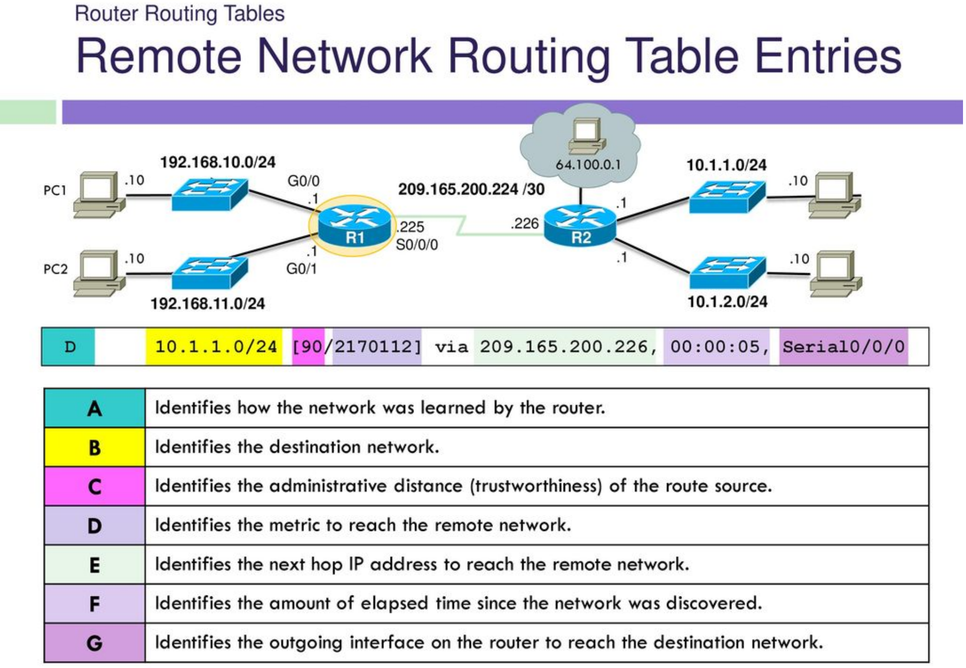
## Subnet masks, prefixes and routing

In this diagram, R1 receives a packet addressed to 192.168.5.19, a host that's connected to R2's LAN. Using a binary AND operation on the address and its mask, R1 finds 192.168.4.0 and forwards the packet out the S0 interface to R2, which will perform the same prefix calculation. R2 determines it should send the packet on interface E0 and deliver it to host 5.19.

R1'S ROUTING TABLE

| Prefix | 192.168.2.0 | 192.168.4.0 | 192.168.252.0 | 0.0.0.0 |
|---|---|---|---|---|
| Mask | 255.255.254.0 | 255.255.254.0 | 255.255.255.252 | 0.0.0.0 |
| Outgoing interface | E0 | S0 to R2 | S0 | S1 to internet (default) |

SOURCE: NETWORK ARCHITECT TERRY SLATTERY



Router Routing Tables

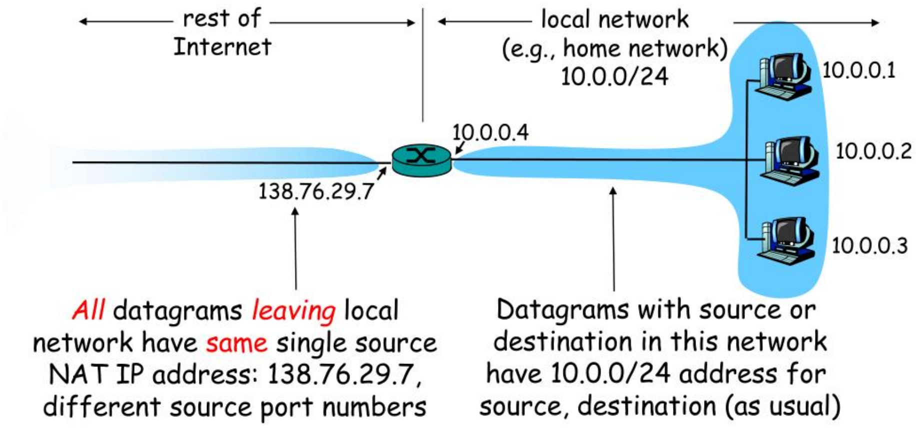
## Remote Network Routing Table Entries

```
D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
```

| | |
|---|---|
| A | Identifies how the network was learned by the router. |
| B | Identifies the destination network. |
| C | Identifies the administrative distance (trustworthiness) of the route source. |
| D | Identifies the metric to reach the remote network. |
| E | Identifies the next hop IP address to reach the remote network. |
| F | Identifies the amount of elapsed time since the network was discovered. |
| G | Identifies the outgoing interface on the router to reach the destination network. |

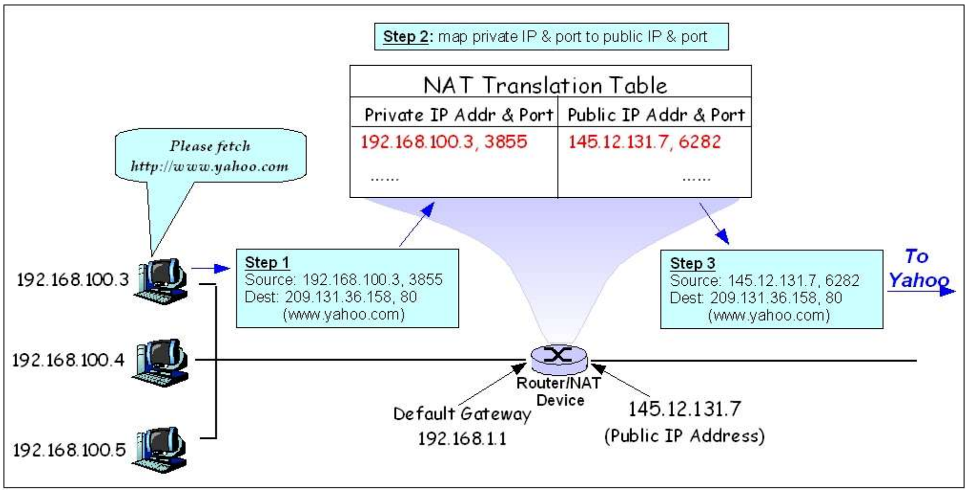
# NAT(Network Address Translation)

# NAT: Network Address Translation



*All* datagrams *leaving* local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)


Please fetch http://www.yahoo.com
192.168.100.3
192.168.100.4
192.168.100.5
Router/NAT Device
Default Gateway 192.168.1.1
145.12.131.7 (Public IP Address)
To Yahoo

**Step 2:** map private IP & port to public IP & port

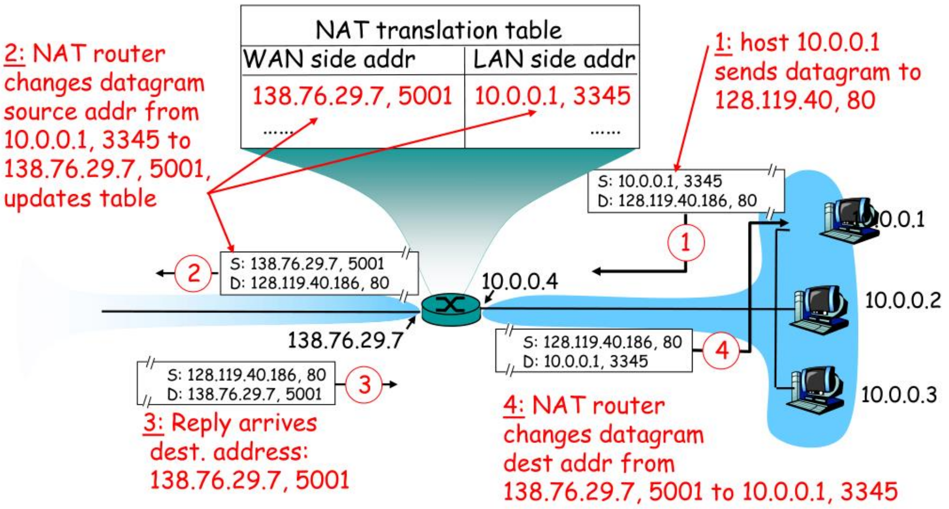
NAT Translation Table

| Private IP Addr & Port | Public IP Addr & Port |
|---|---|
| 192.168.100.3, 3855 | 145.12.131.7, 6282 |
| ...... | ...... |

**Step 1**
Source: 192.168.100.3, 3855
Dest: 209.131.36.158, 80
(www.yahoo.com)

**Step 3**
Source: 145.12.131.7, 6282
Dest: 209.131.36.158, 80
(www.yahoo.com)

# NAT: Network Address Translation



NAT translation table

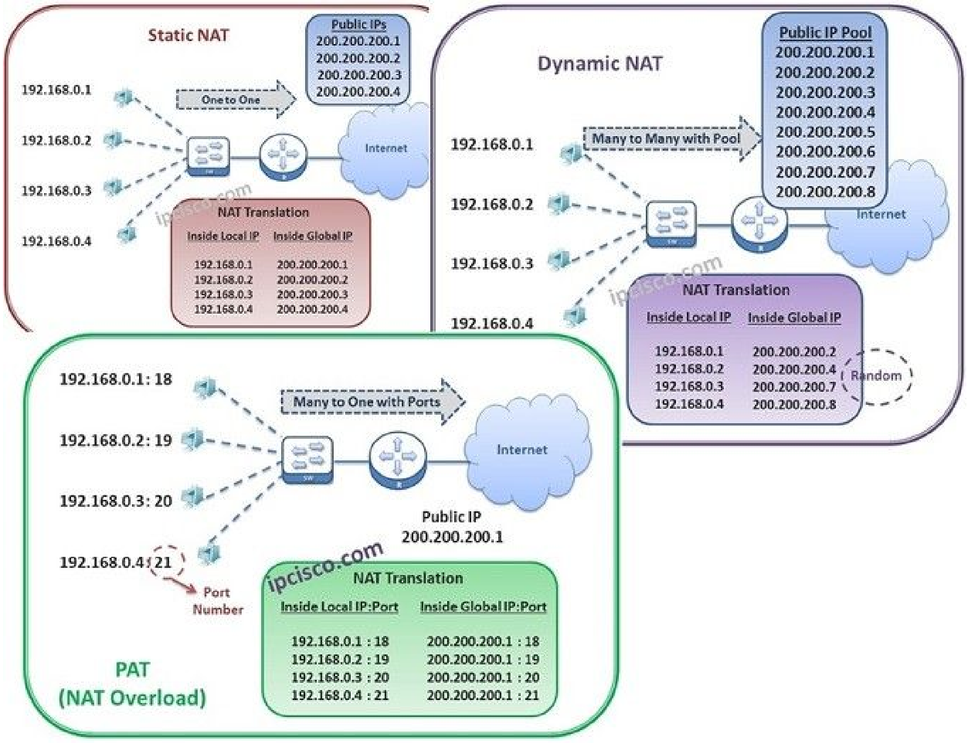
| WAN side addr | LAN side addr |
|---|---|
| 138.76.29.7, 5001 | 10.0.0.1, 3345 |
| ...... | ...... |

1: host 10.0.0.1 sends datagram to 128.119.40, 80

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

3: Reply arrives dest. address: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345



NAT Translation

| Inside Local IP | Inside Global IP |
|---|---|
| 192.168.0.1 | 200.200.200.1 |
| 192.168.0.2 | 200.200.200.2 |
| 192.168.0.3 | 200.200.200.3 |
| 192.168.0.4 | 200.200.200.4 |

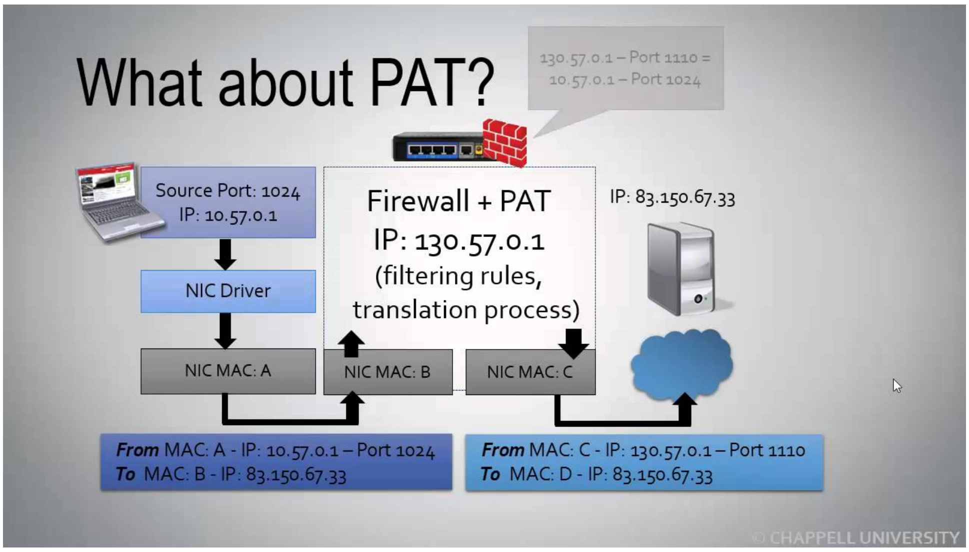
NAT Translation

| Inside Local IP | Inside Global IP |
|---|---|
| 192.168.0.1 | 200.200.200.2 |
| 192.168.0.2 | 200.200.200.4 |
| 192.168.0.3 | 200.200.200.7 |
| 192.168.0.4 | 200.200.200.8 |

NAT Translation

| Inside Local IP:Port | Inside Global IP:Port |
|---|---|
| 192.168.0.1 : 18 | 200.200.200.1 : 18 |
| 192.168.0.2 : 19 | 200.200.200.1 : 19 |
| 192.168.0.3 : 20 | 200.200.200.1 : 20 |
| 192.168.0.4 : 21 | 200.200.200.1 : 21 |

# PAT(Port Address Translation)



What about PAT?

130.57.0.1 – Port 1110 =
10.57.0.1 – Port 1024

Source Port: 1024
IP: 10.57.0.1

NIC Driver

NIC MAC: A

Firewall + PAT
IP: 130.57.0.1
(filtering rules,
translation process)

NIC MAC: B

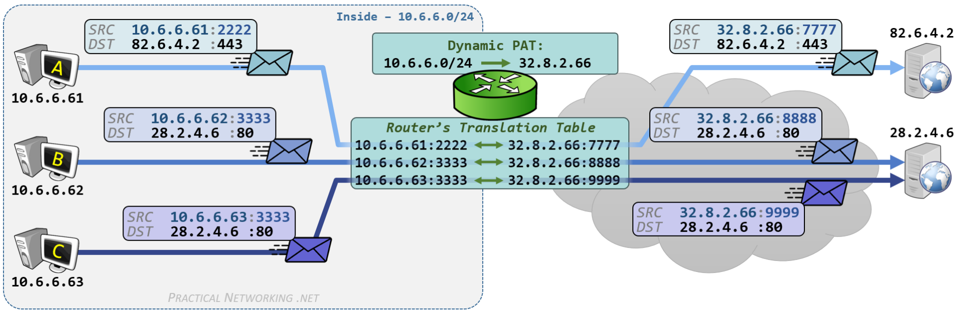
NIC MAC: C

IP: 83.150.67.33

***From*** MAC: A - IP: 10.57.0.1 – Port 1024
***To*** MAC: B - IP: 83.150.67.33

***From*** MAC: C - IP: 130.57.0.1 – Port 1110
***To*** MAC: D - IP: 83.150.67.33

© CHAPPELL UNIVERSITY



SRC 10.6.6.61:2222
DST 82.6.4.2 :443

SRC 10.6.6.62:3333
DST 28.2.4.6 :80

SRC 10.6.6.63:3333
DST 28.2.4.6 :80

Dynamic PAT:
10.6.6.0/24 ⟶ 32.8.2.66

Router's Translation Table

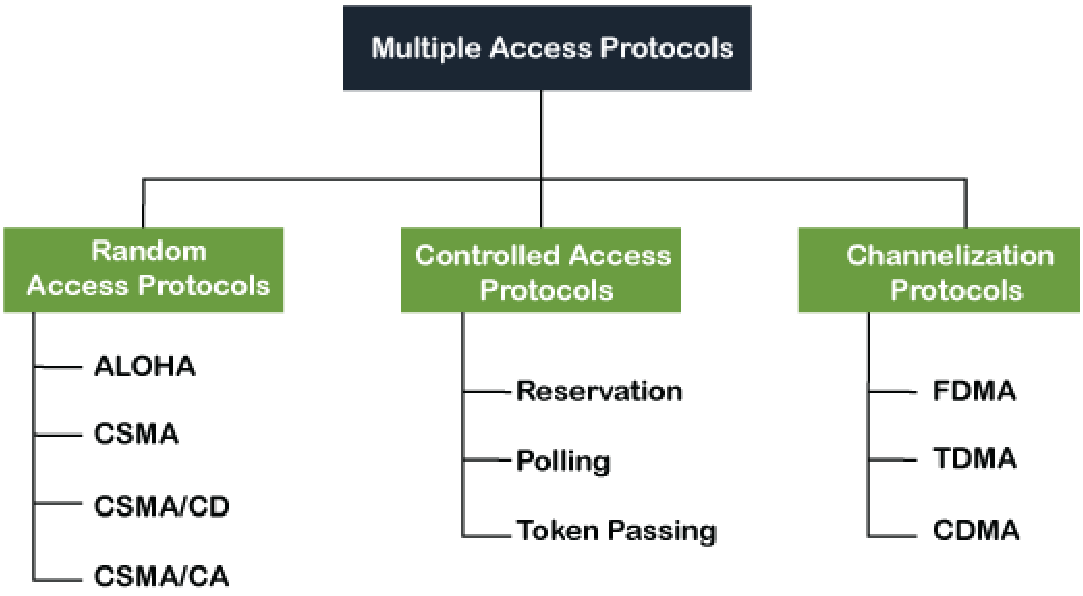
```
10.6.6.61:2222 ⟷ 32.8.2.66:7777
10.6.6.62:3333 ⟷ 32.8.2.66:8888
10.6.6.63:3333 ⟷ 32.8.2.66:9999
```

SRC 32.8.2.66:7777
DST 82.6.4.2 :443

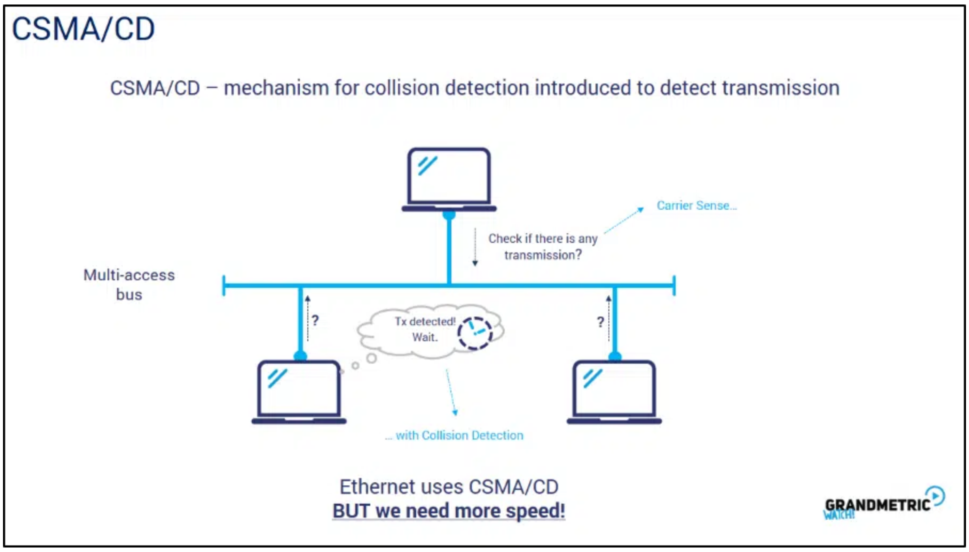
SRC 32.8.2.66:8888
DST 28.2.4.6 :80

SRC 32.8.2.66:9999
DST 28.2.4.6 :80

# Mutiple Access Protocols



# CSMA/CD

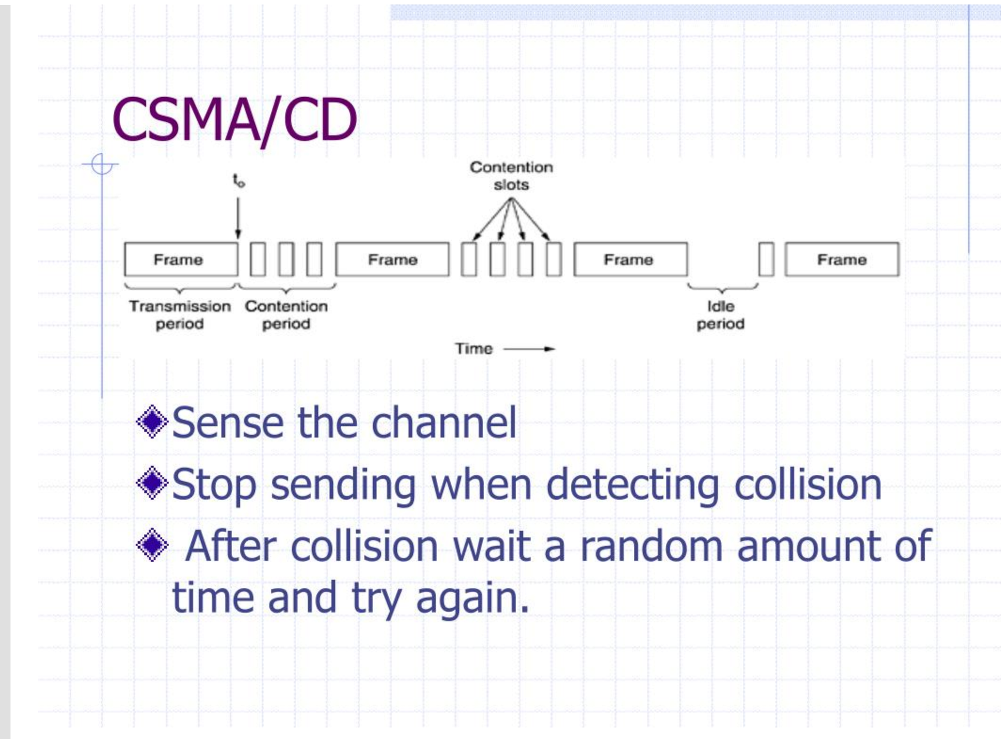


CSMA/CD

CSMA/CD – mechanism for collision detection introduced to detect transmission

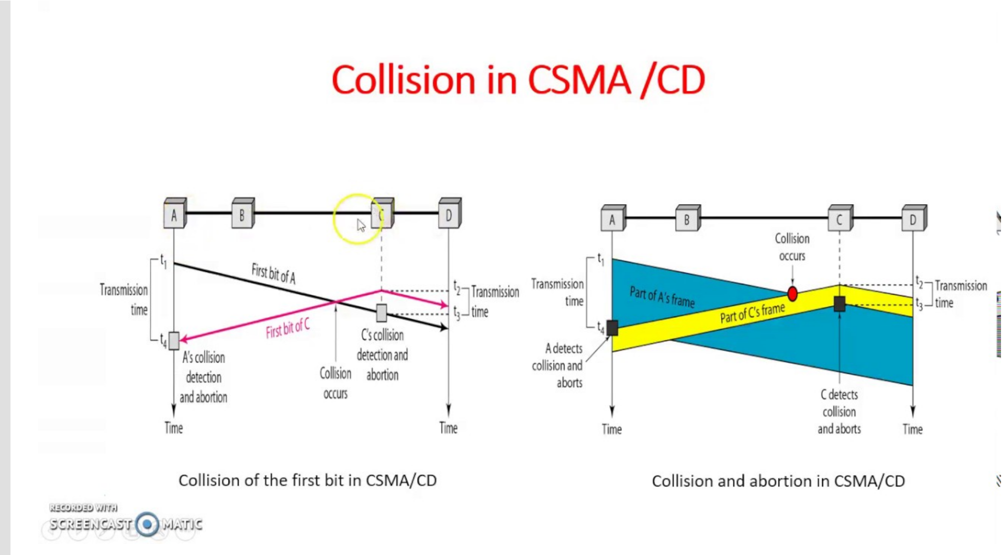
Carrier Sense...
Check if there is any transmission?
Multi-access bus
?
Tx detected! Wait.
?
... with Collision Detection

Ethernet uses CSMA/CD
**BUT we need more speed!**



# CSMA/CD

- Sense the channel
- Stop sending when detecting collision
- After collision wait a random amount of time and try again.

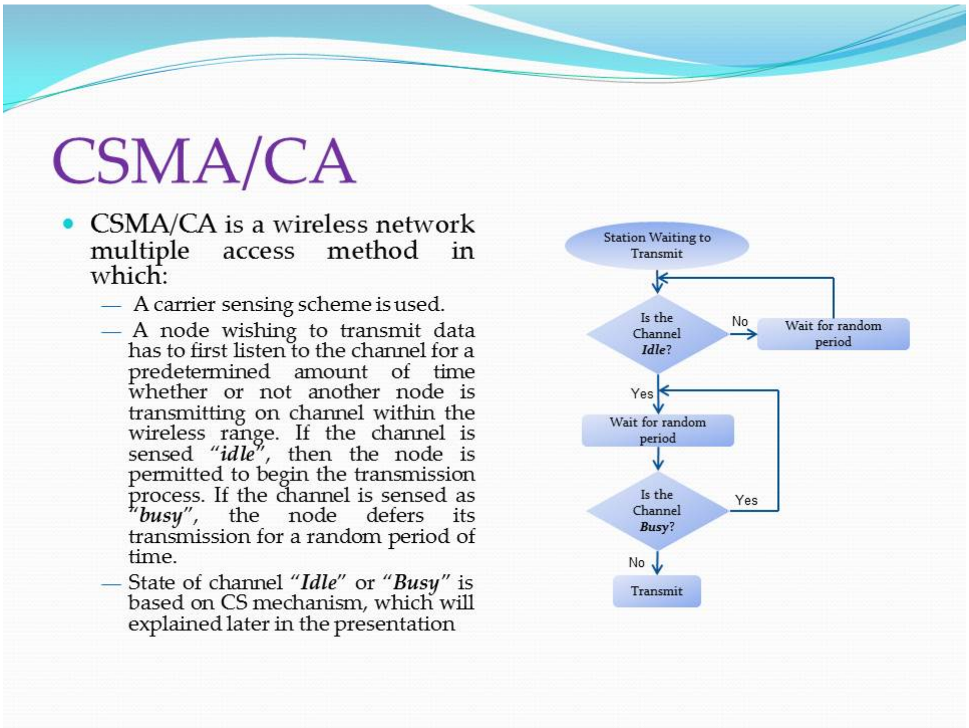


## Collision in CSMA /CD

Collision of the first bit in CSMA/CD

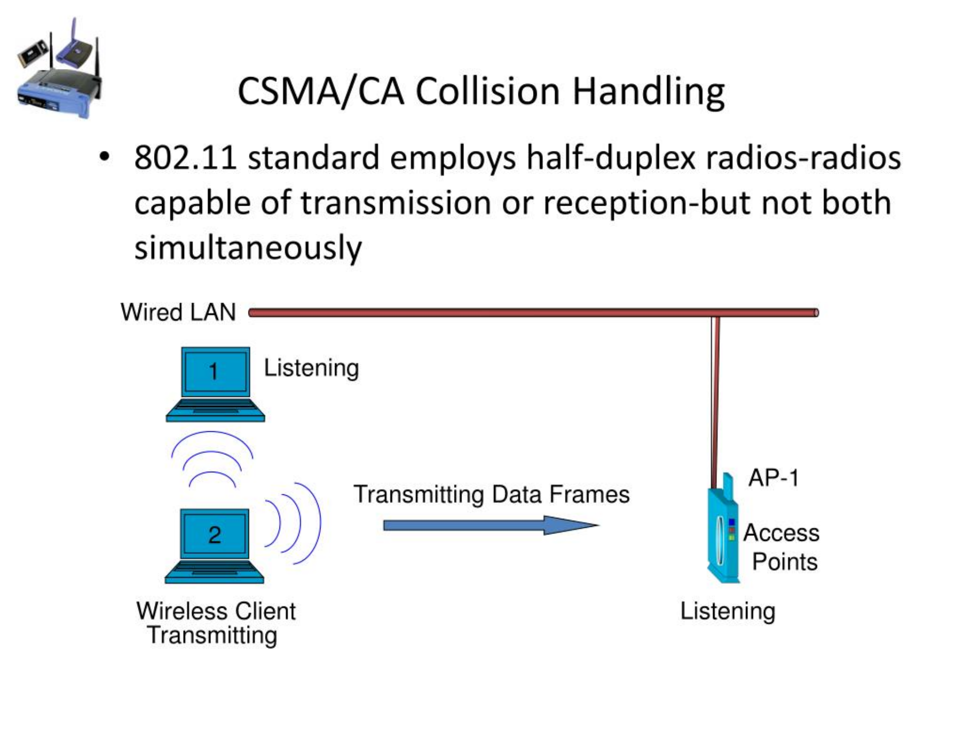
Collision and abortion in CSMA/CD

# CSMA/CA



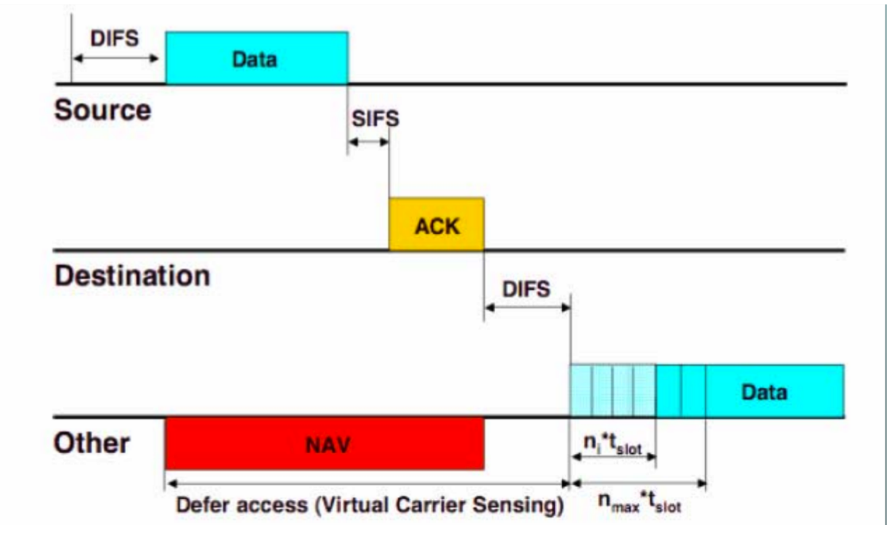
# CSMA/CA

- CSMA/CA is a wireless network multiple access method in which:
  - — A carrier sensing scheme is used.
  - — A node wishing to transmit data has to first listen to the channel for a predetermined amount of time whether or not another node is transmitting on channel within the wireless range. If the channel is sensed *"idle"*, then the node is permitted to begin the transmission process. If the channel is sensed as *"busy"*, the node defers its transmission for a random period of time.
  - — State of channel *"Idle"* or *"Busy"* is based on CS mechanism, which will explained later in the presentation



## CSMA/CA Collision Handling

- 802.11 standard employs half-duplex radios-radios capable of transmission or reception-but not both simultaneously



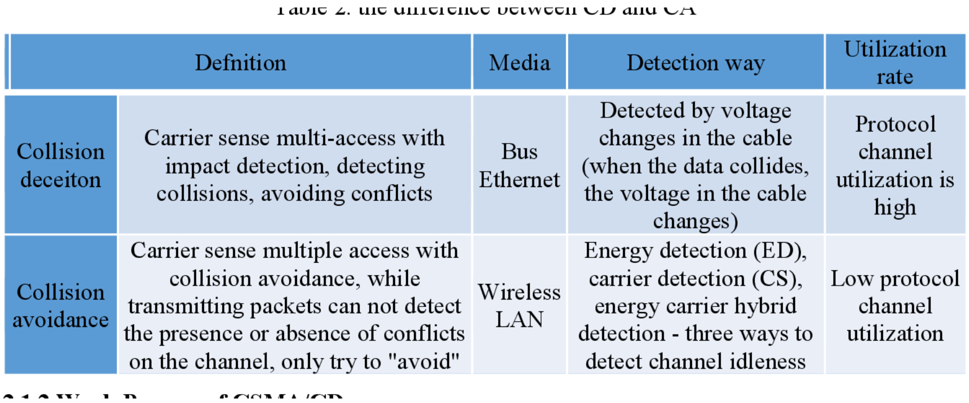
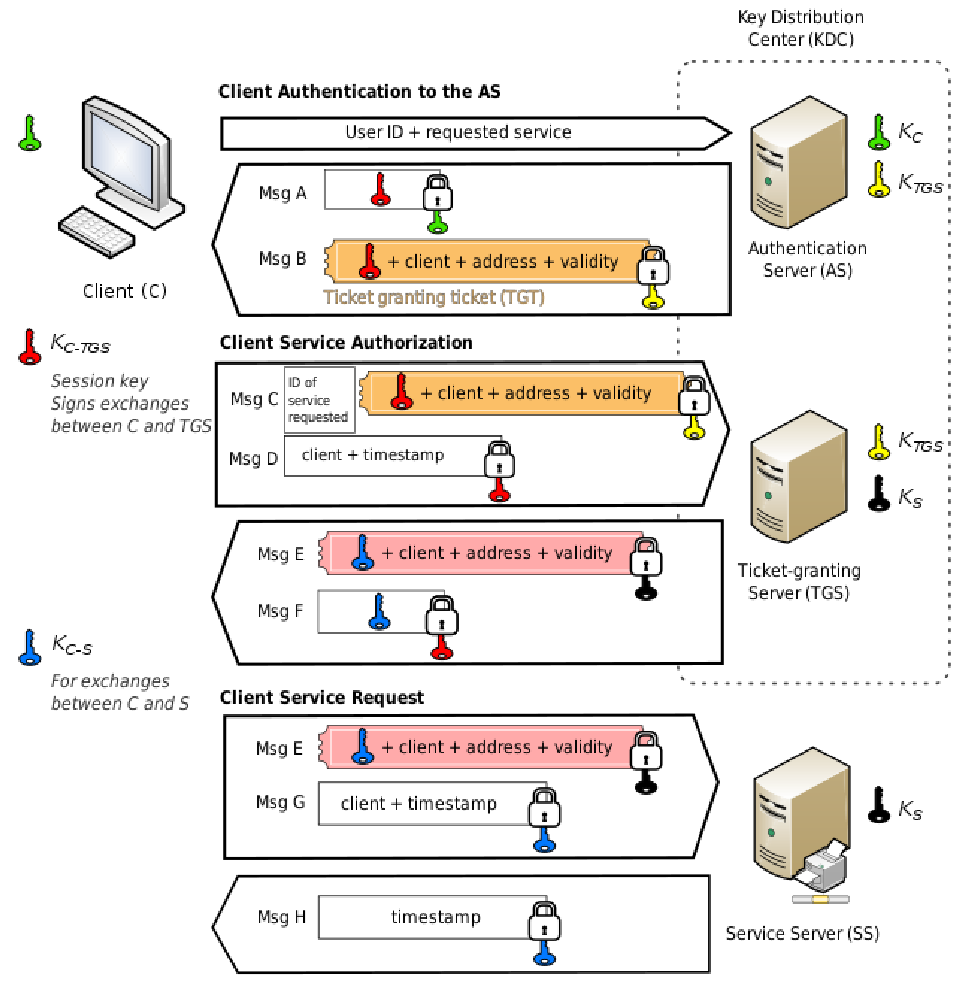


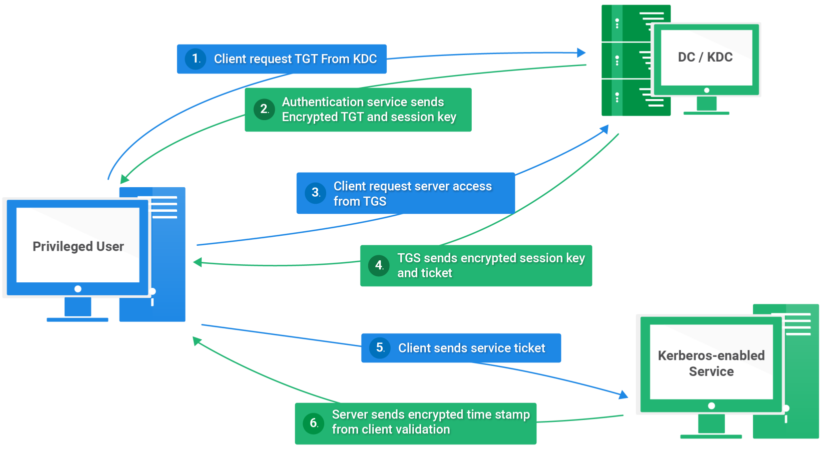
Table 2: the difference between CD and CA

| Defnition | | Media | Detection way | Utilization rate |
|---|---|---|---|---|
| Collision deceiton | Carrier sense multi-access with impact detection, detecting collisions, avoiding conflicts | Bus Ethernet | Detected by voltage changes in the cable (when the data collides, the voltage in the cable changes) | Protocol channel utilization is high |
| Collision avoidance | Carrier sense multiple access with collision avoidance, while transmitting packets can not detect the presence or absence of conflicts on the channel, only try to "avoid" | Wireless LAN | Energy detection (ED), carrier detection (CS), energy carrier hybrid detection - three ways to detect channel idleness | Low protocol channel utilization |

2.1.2 Work Process of CSMA/CD

# Kerberos


Key Distribution Center (KDC)
Client Authentication to the AS
User ID + requested service
Msg A
Msg B
+ client + address + validity
Ticket granting ticket (TGT)
$K_C$
$K_{TGS}$
Authentication Server (AS)
Client (C)
$K_{C-TGS}$
Session key
Signs exchanges between C and TGS
Client Service Authorization
Msg C
ID of service requested
+ client + address + validity
Msg D
client + timestamp
$K_{TGS}$
$K_S$
Msg E
+ client + address + validity
Msg F
Ticket-granting Server (TGS)
$K_{C-S}$
For exchanges between C and S
Client Service Request
Msg E
+ client + address + validity
Msg G
client + timestamp
$K_S$
Msg H
timestamp
Service Server (SS)



1 Client request TGT From KDC

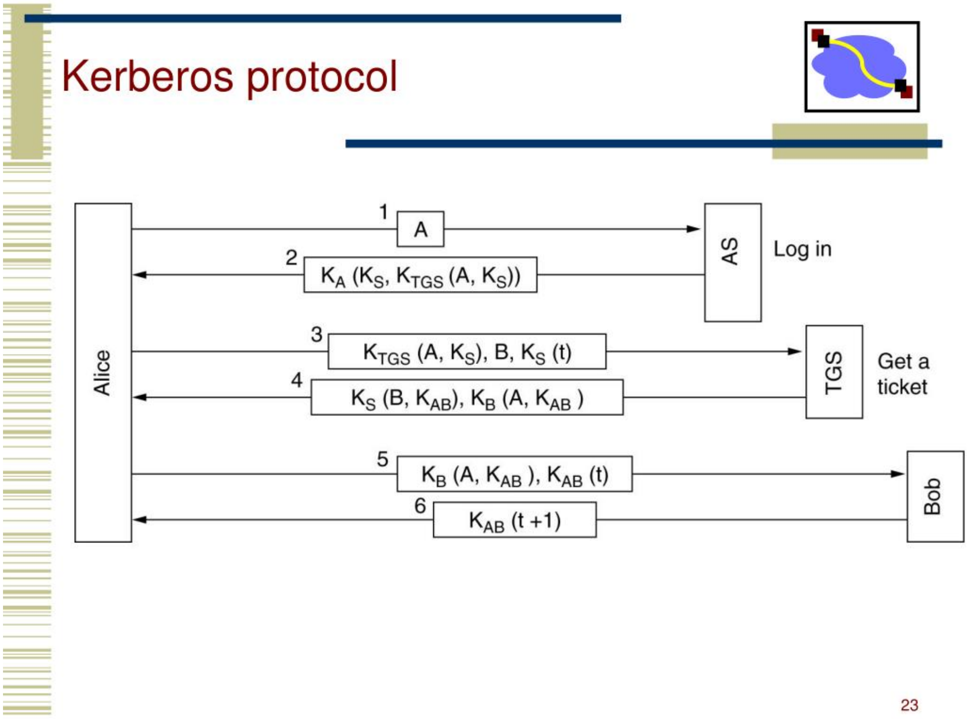
2 Authentication service sends Encrypted TGT and session key

3 Client request server access from TGS

4 TGS sends encrypted session key and ticket

5 Client sends service ticket

6 Server sends encrypted time stamp from client validation



Kerberos protocol

1 $A$ — Log in

2 $K_A (K_S, K_{TGS} (A, K_S))$

3 $K_{TGS} (A, K_S), B, K_S (t)$ — Get a ticket

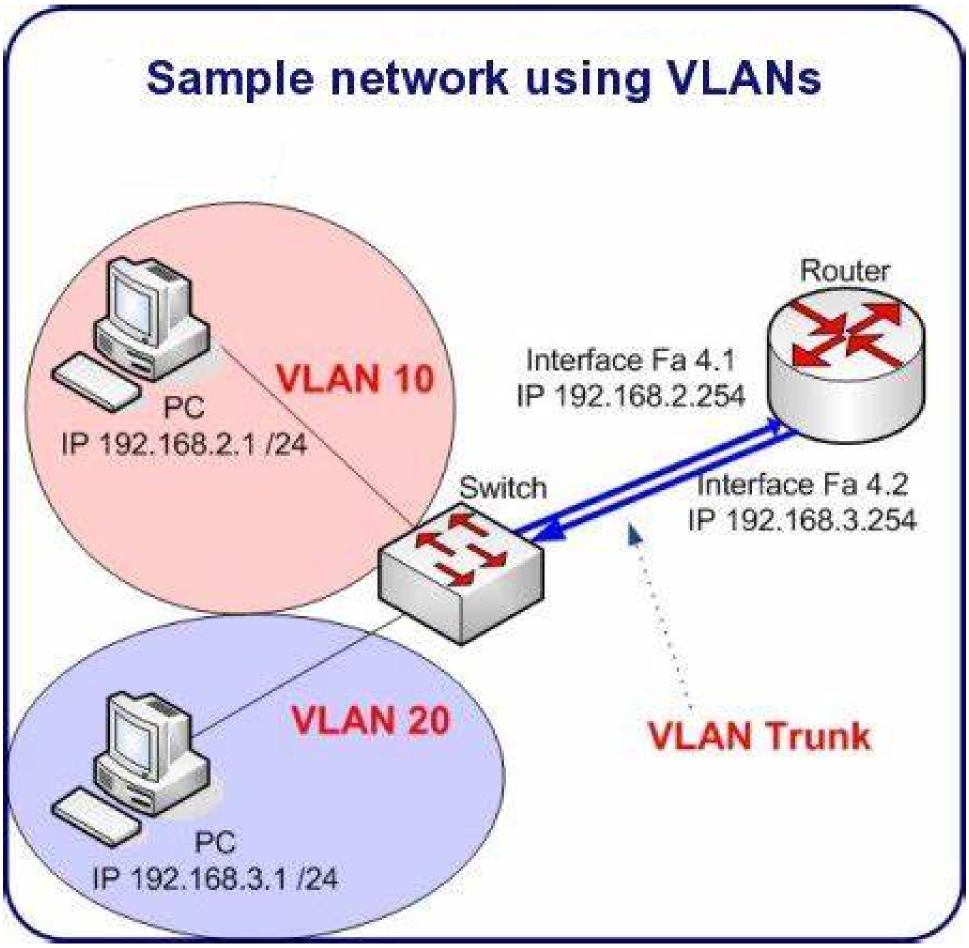
4 $K_S (B, K_{AB}), K_B (A, K_{AB})$

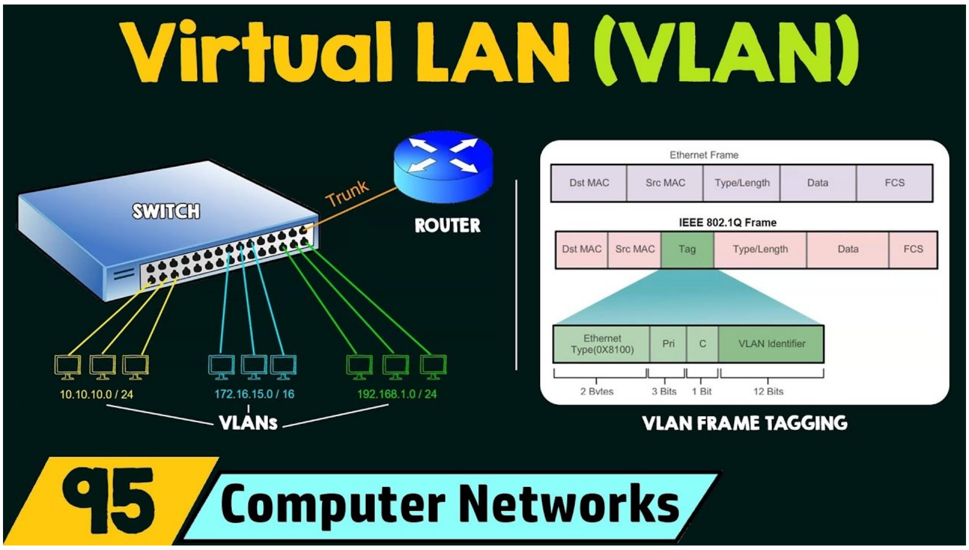
5 $K_B (A, K_{AB}), K_{AB} (t)$

6 $K_{AB} (t +1)$

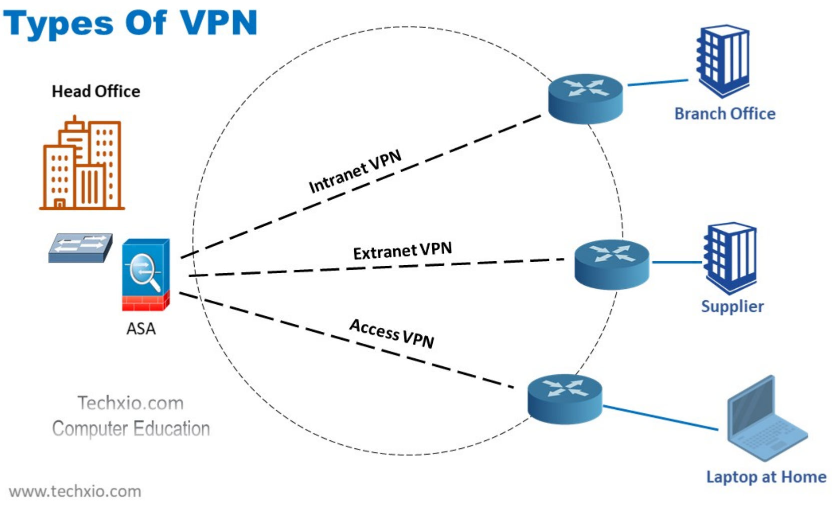
23

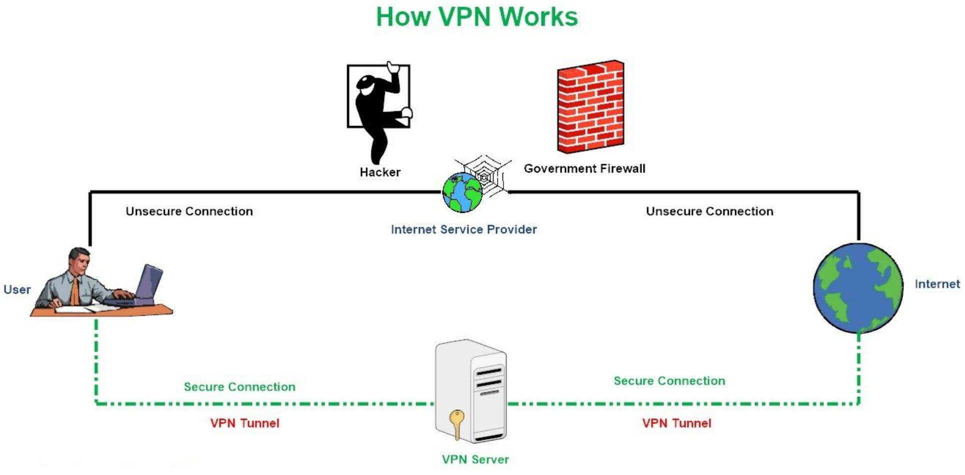
# VLAN

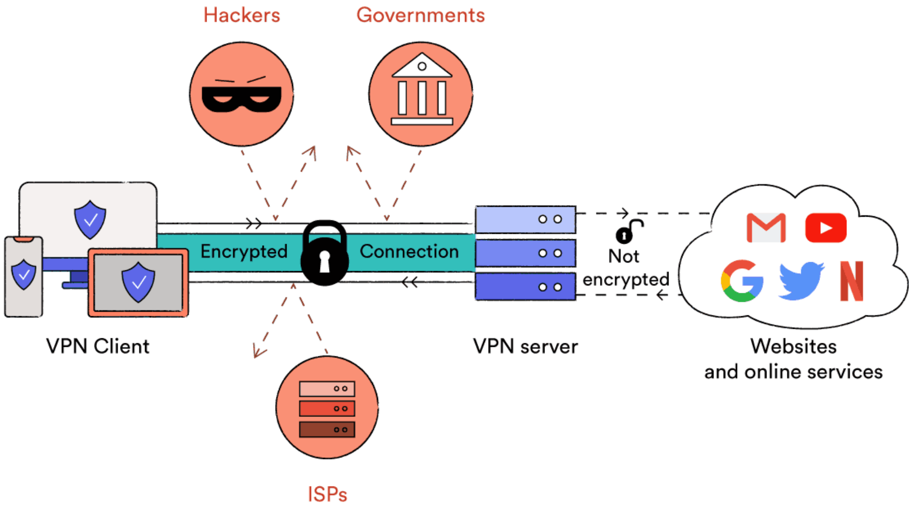

Sample network using VLANs
Router
Interface Fa 4.1
IP 192.168.2.254
Interface Fa 4.2
IP 192.168.3.254
Switch
VLAN 10
PC
IP 192.168.2.1 /24
VLAN 20
PC
IP 192.168.3.1 /24
VLAN Trunk

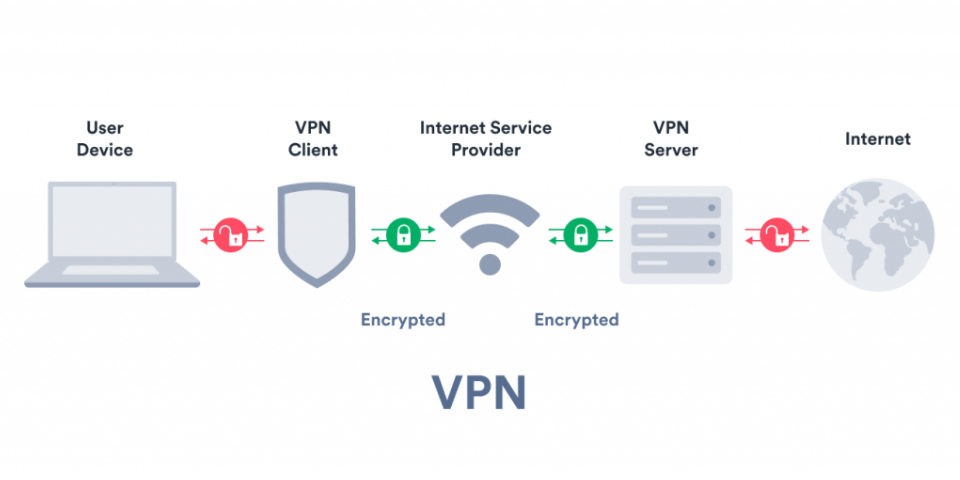

Virtual LAN (VLAN)
SWITCH
Trunk
ROUTER
10.10.10.0 / 24
172.16.15.0 / 16
192.168.1.0 / 24
VLANs
Ethernet Frame
Dst MAC
Src MAC
Type/Length
Data
FCS
IEEE 802.1Q Frame
Dst MAC
Src MAC
Tag
Type/Length
Data
FCS
Ethernet Type(0X8100)
Pri
C
VLAN Identifier
2 Bytes
3 Bits
1 Bit
12 Bits
VLAN FRAME TAGGING
95
Computer Networks

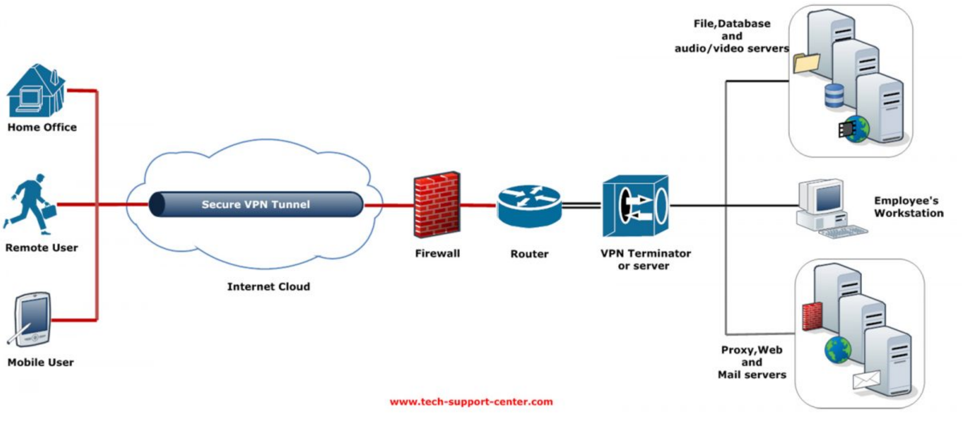
## VPN


Types Of VPN
Head Office
ASA
Intranet VPN
Extranet VPN
Access VPN
Branch Office
Supplier
Laptop at Home
Techxio.com
Computer Education
www.techxio.com

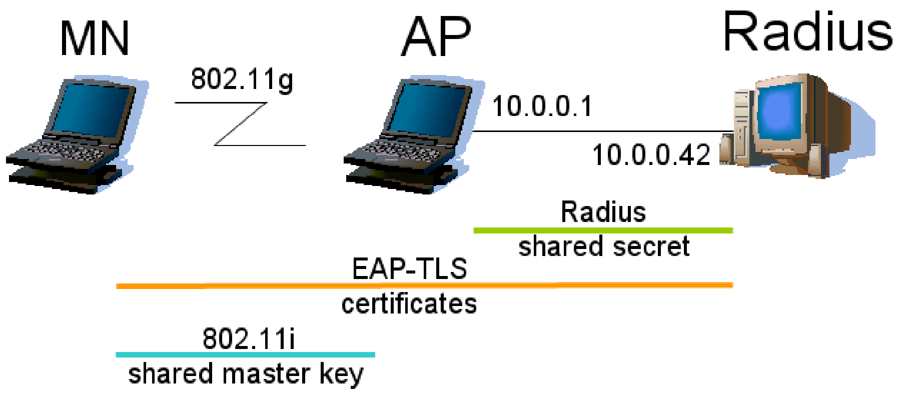

How VPN Works
Hacker
Government Firewall
Unsecure Connection
Internet Service Provider
Unsecure Connection
User
Internet
Secure Connection
Secure Connection
VPN Tunnel
VPN Tunnel
VPN Server

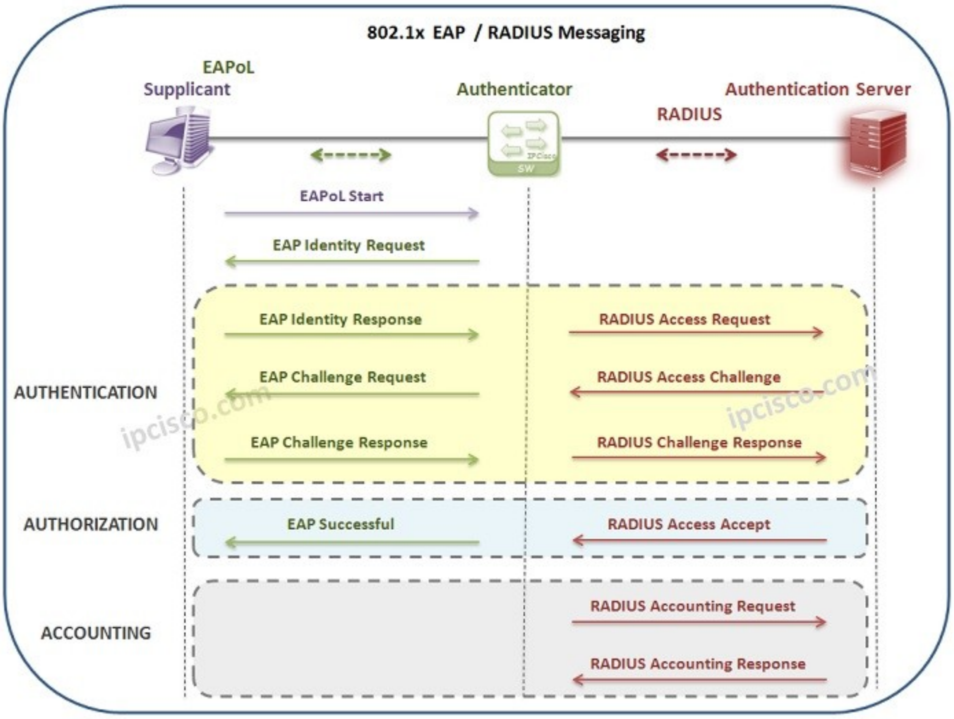

Hackers
Governments
Encrypted
Connection
Not encrypted
VPN Client
VPN server
Websites and online services
ISPs





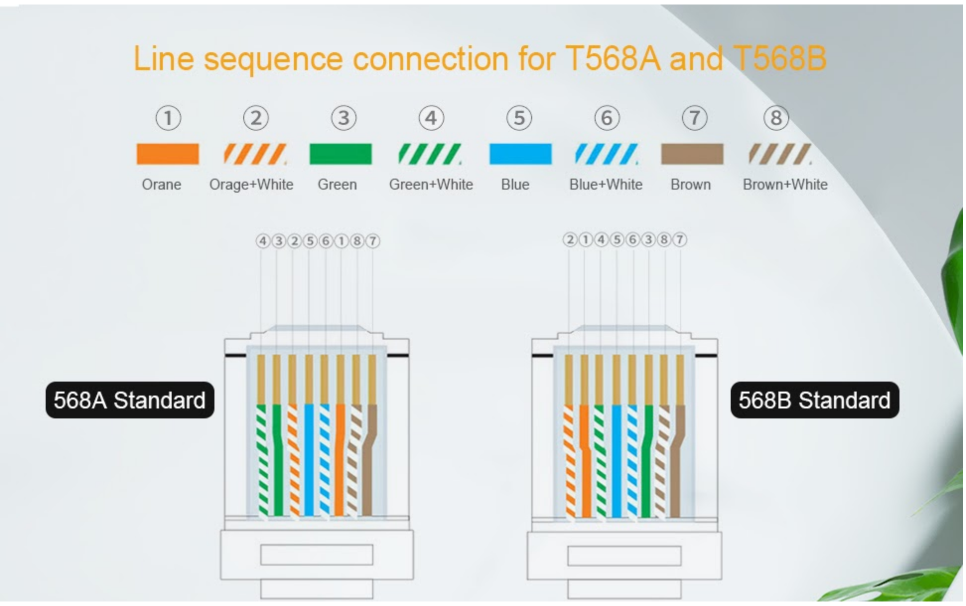
## EAP and RADIUS



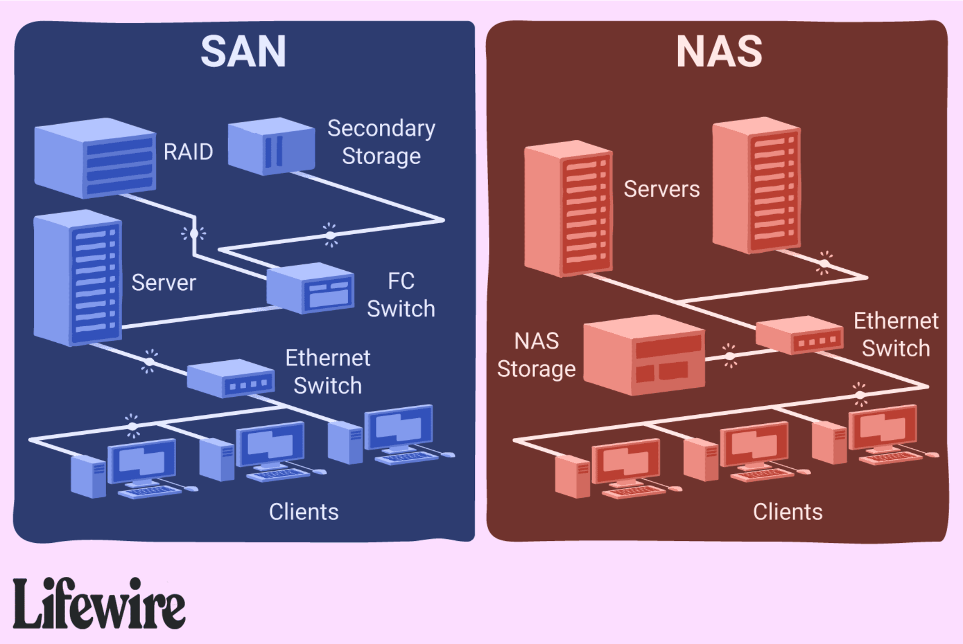


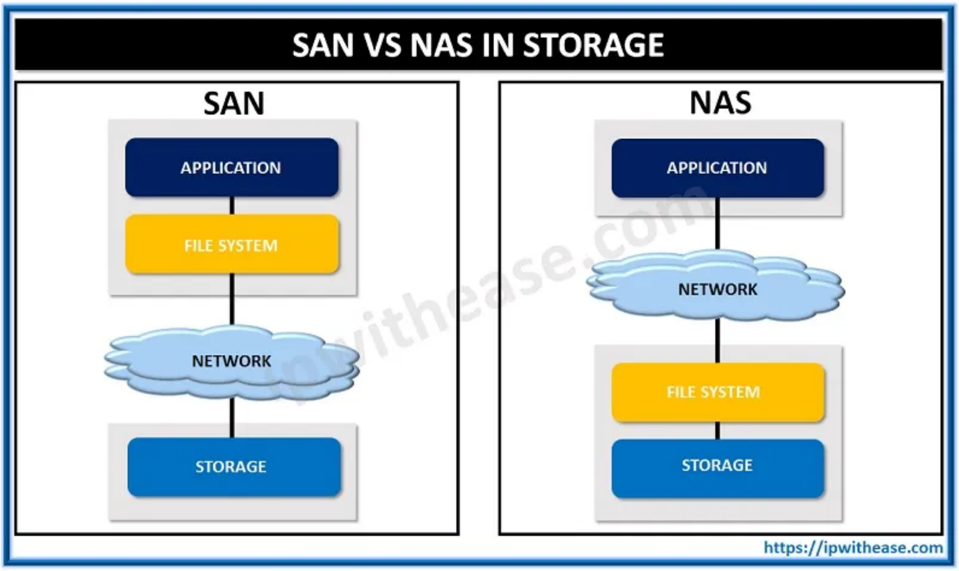
# Cable

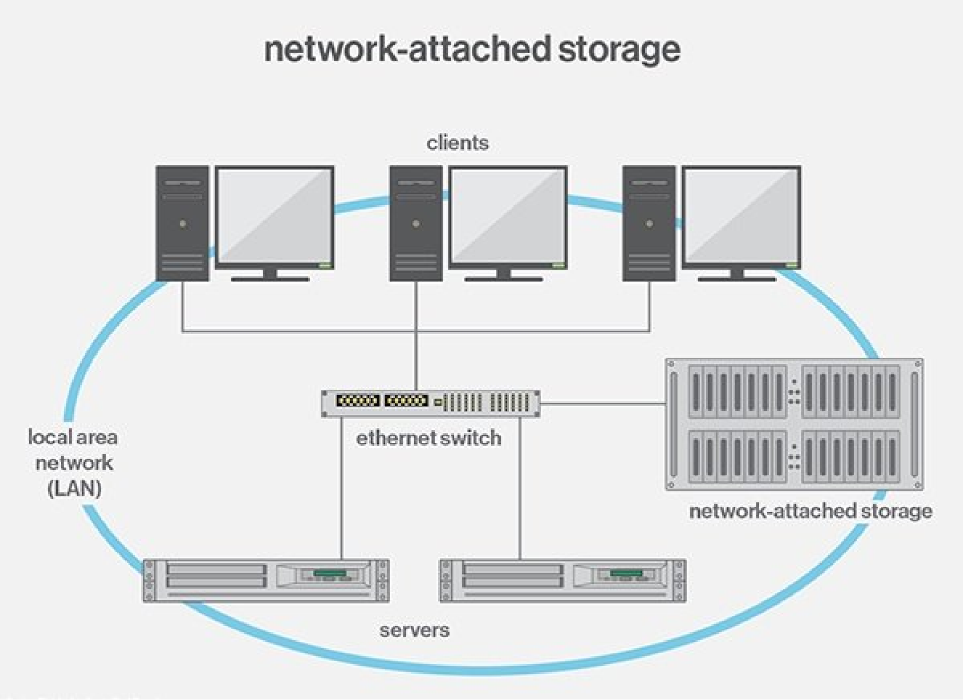
| Category | Standard Bandwidth | Max Data Rate | Shielding |
|---|---|---|---|
| **Cat5e** | 100MHz (up to 350) | 1000Mbps | UTP or STP |
| **Cat6** | 250MHz (up to 550) | 1000Mbps | UTP or STP |
| **Cat6A** | 500MHz (up to 550) | 10Gbps | UTP or STP |
| **Cat7** | 600MHz | 10Gbps | Shielded only |
| **Cat8** | 2000MHz | 25Gbps or 40Gbps | Shielded only |

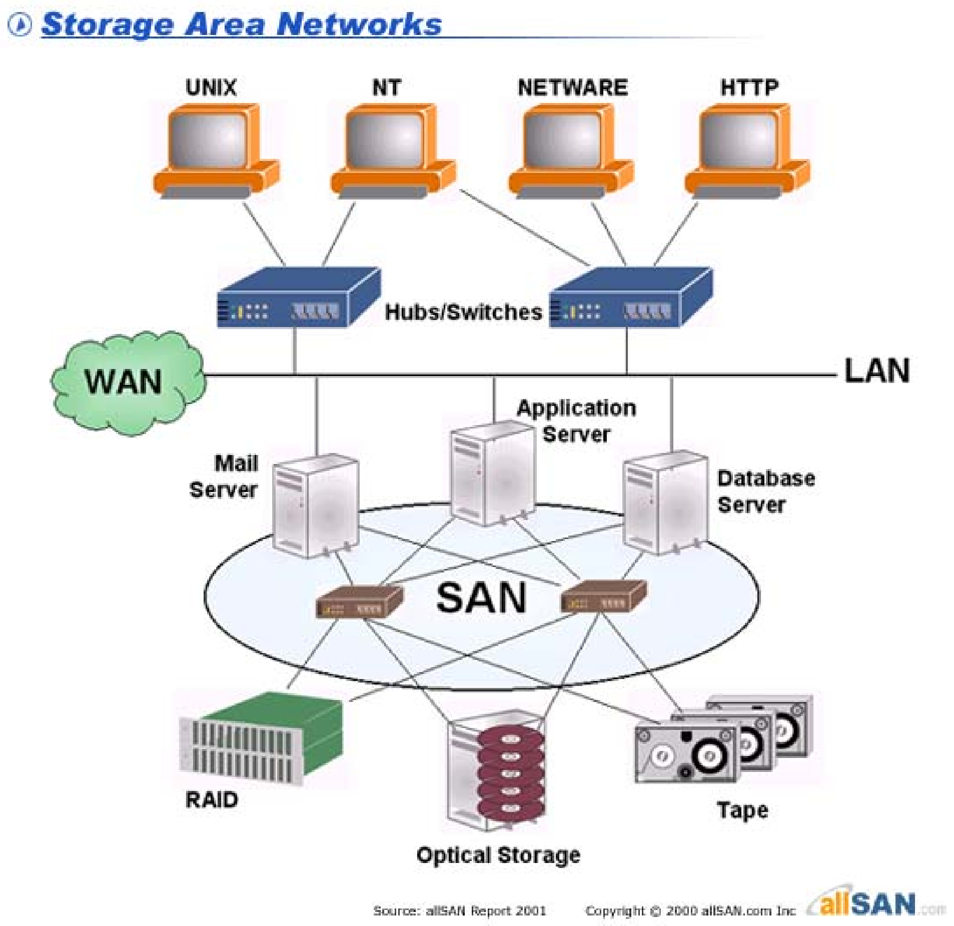


# NAS vs SAN


SAN
RAID
Secondary Storage
Server
FC Switch
Ethernet Switch
Clients
NAS
Servers
NAS Storage
Ethernet Switch
Clients
Lifewire

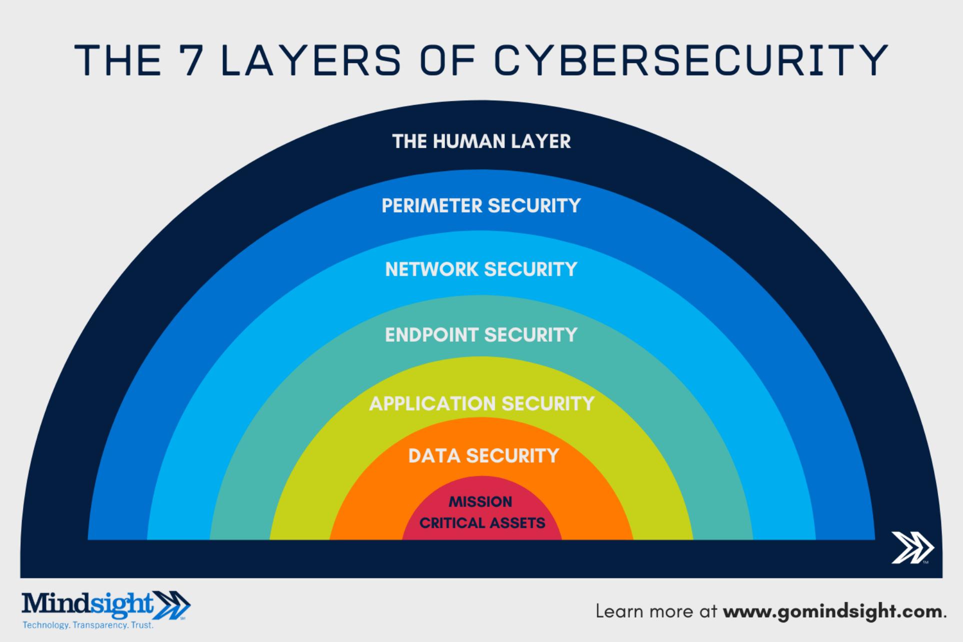

SAN VS NAS IN STORAGE
SAN
APPLICATION
FILE SYSTEM
NETWORK
STORAGE
NAS
APPLICATION
NETWORK
FILE SYSTEM
STORAGE
ipwithease.com
https://ipwithease.com

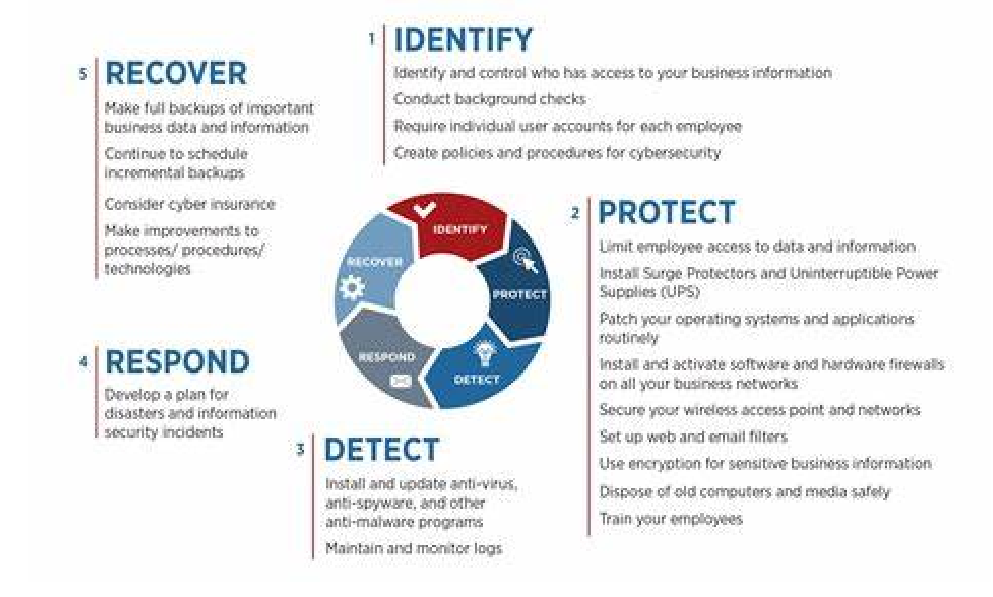

network-attached storage
clients
local area network (LAN)
ethernet switch
network-attached storage
servers



Source: allSAN Report 2001 Copyright © 2000 allSAN.com Inc

# CyberSecurity





## 1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

## 2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

## 3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

## 4 RESPOND

Develop a plan for disasters and information security incidents

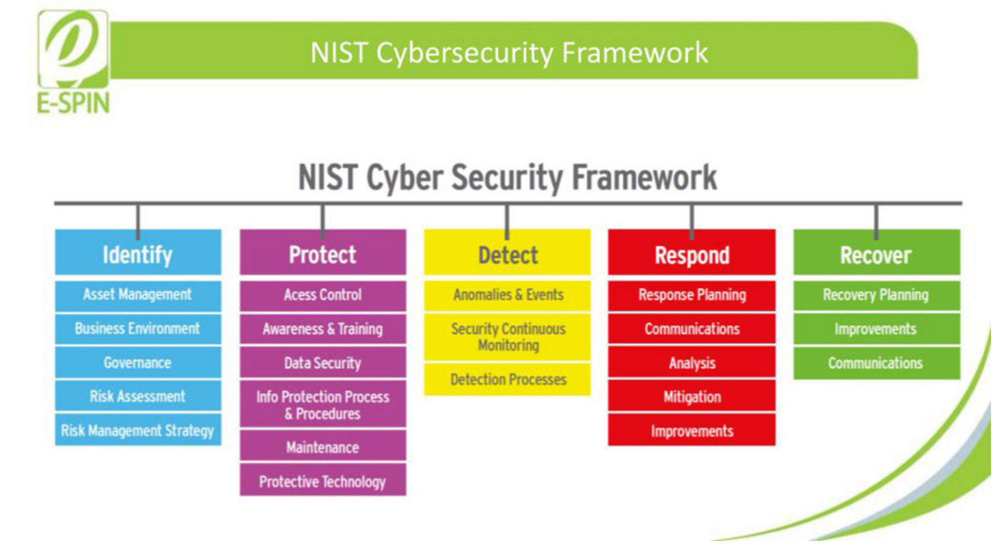
## 5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

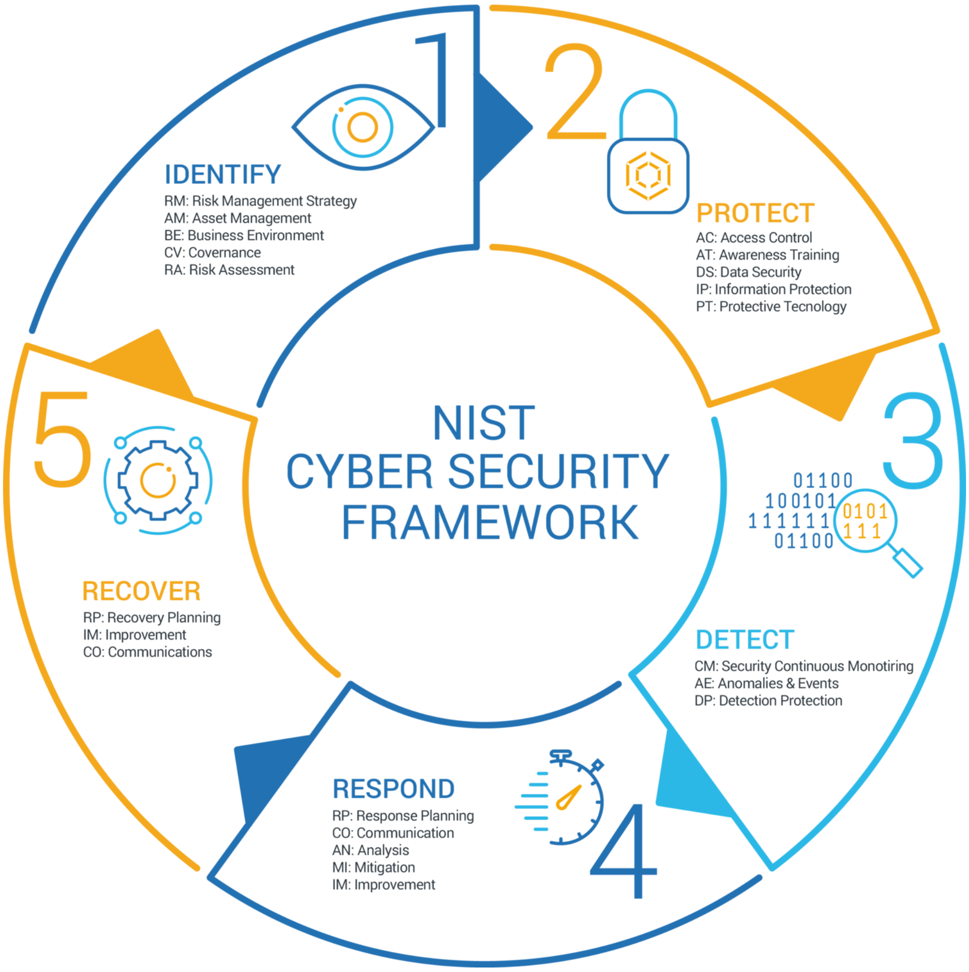


E-SPIN

## NIST Cybersecurity Framework

### NIST Cyber Security Framework

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset Management | Acess Control | Anomalies & Events | Response Planning | Recovery Planning |
| Business Environment | Awareness & Training | Security Continuous Monitoring | Communications | Improvements |
| Governance | Data Security | Detection Processes | Analysis | Communications |
| Risk Assessment | Info Protection Process & Procedures | | Mitigation | |
| Risk Management Strategy | Maintenance | | Improvements | |
| | Protective Technology | | | |



## Risk Management

BEST CYBERSECURITY PRACTICES

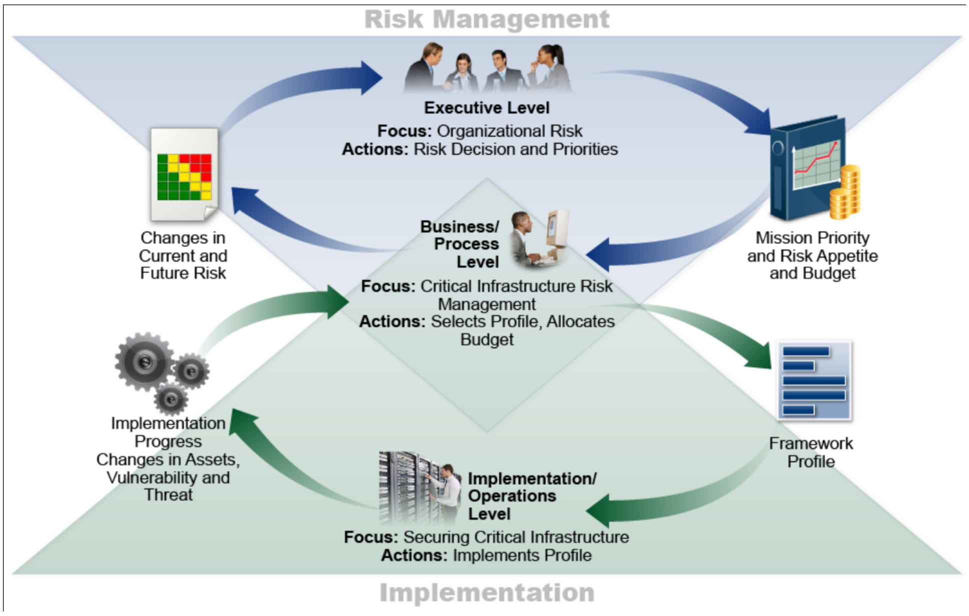
01 Install and regularly update protective software

02 Apply a strong password policy

03 Use multi-factor authentication

04 Make regular backups

Drudesk
Drupal Support On Demand



Risk Management

**Executive Level**
**Focus:** Organizational Risk
**Actions:** Risk Decision and Priorities

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

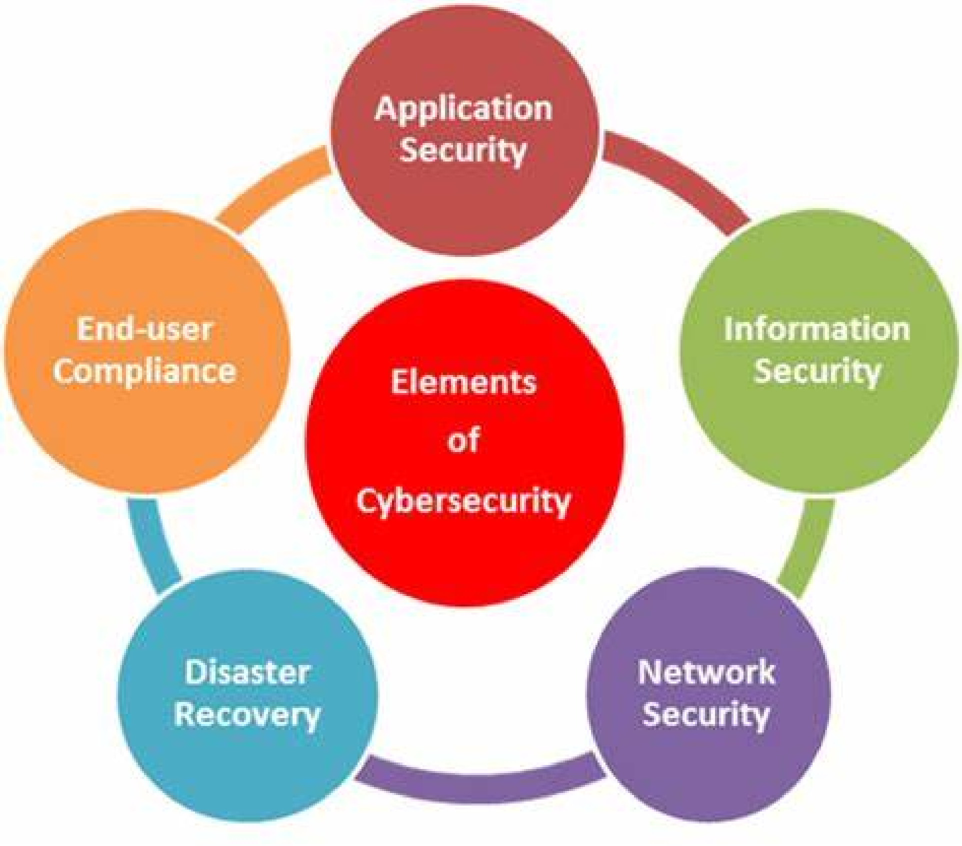
**Business/ Process Level**
**Focus:** Critical Infrastructure Risk Management
**Actions:** Selects Profile, Allocates Budget

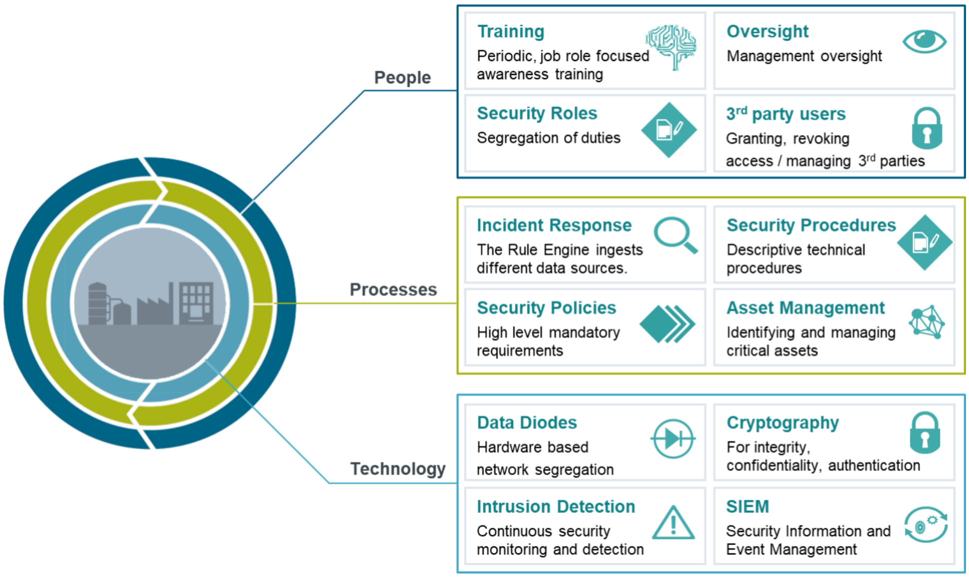
Implementation Progress Changes in Assets, Vulnerability and Threat

Framework Profile

**Implementation/ Operations Level**
**Focus:** Securing Critical Infrastructure
**Actions:** Implements Profile

Implementation





**Training**
Periodic, job role focused awareness training

**Oversight**
Management oversight

**Security Roles**
Segregation of duties

**3rd party users**
Granting, revoking access / managing 3rd parties

**Incident Response**
The Rule Engine ingests different data sources.

**Security Procedures**
Descriptive technical procedures

**Security Policies**
High level mandatory requirements

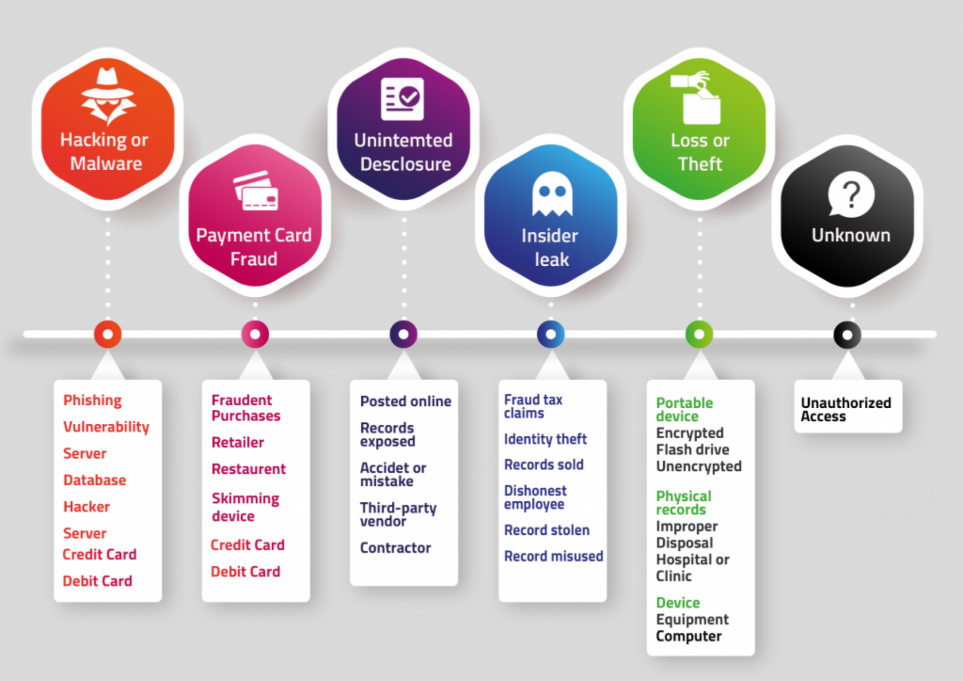
**Asset Management**
Identifying and managing critical assets

**Data Diodes**
Hardware based network segregation

**Cryptography**
For integrity, confidentiality, authentication

**Intrusion Detection**
Continuous security monitoring and detection

**SIEM**
Security Information and Event Management



Hacking or Malware
- Phishing
- Vulnerability
- Server
- Database
- Hacker
- Server
- Credit Card
- Debit Card

Payment Card Fraud
- Fraudent Purchases
- Retailer
- Restaurent
- Skimming device
- Credit Card
- Debit Card

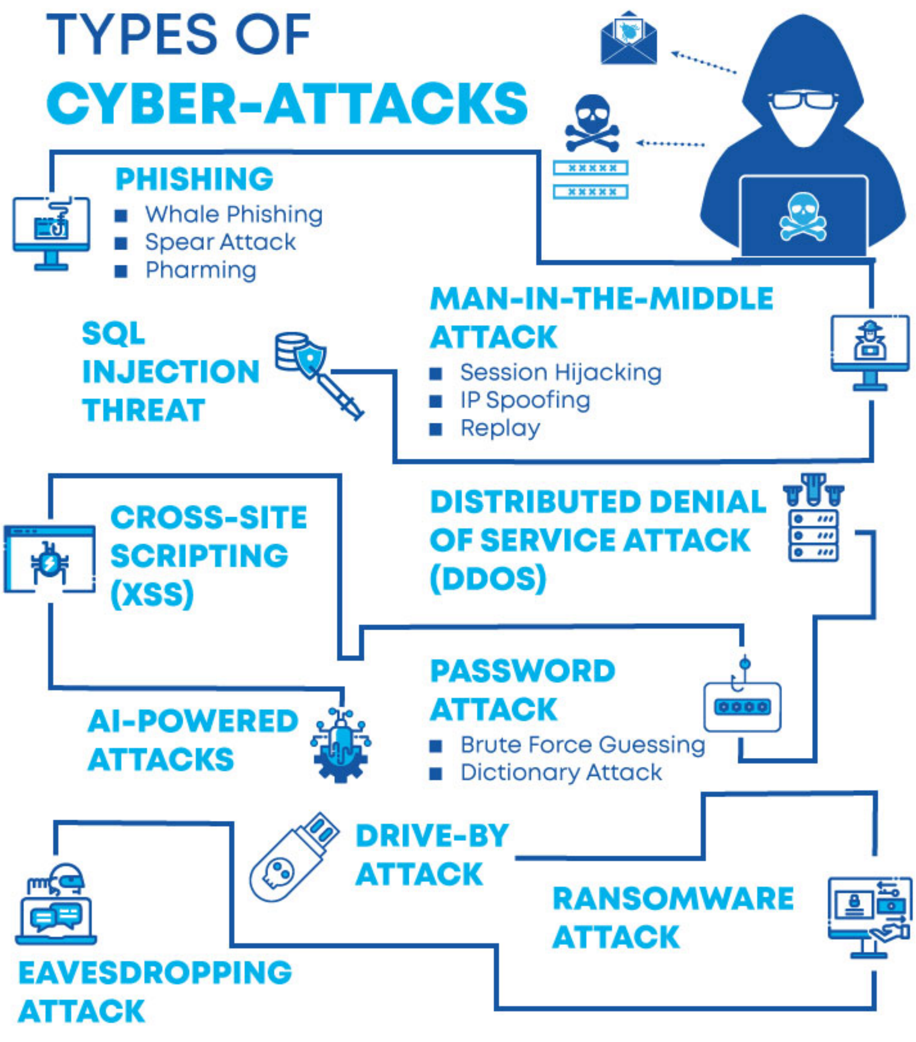
Unintemted Desclosure
- Posted online
- Records exposed
- Accidet or mistake
- Third-party vendor
- Contractor

Insider leak
- Fraud tax claims
- Identity theft
- Records sold
- Dishonest employee
- Record stolen
- Record misused

Loss or Theft
- Portable device
- Encrypted Flash drive Unencrypted
- Physical records
- Improper Disposal Hospital or Clinic
- Device
- Equipment Computer

Unknown
- Unauthorized Access

## Cybersecurity Attacks



TYPES OF CYBER-ATTACKS

PHISHING
- Whale Phishing
- Spear Attack
- Pharming

SQL INJECTION THREAT

MAN-IN-THE-MIDDLE ATTACK
- Session Hijacking
- IP Spoofing
- Replay

CROSS-SITE SCRIPTING (XSS)

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

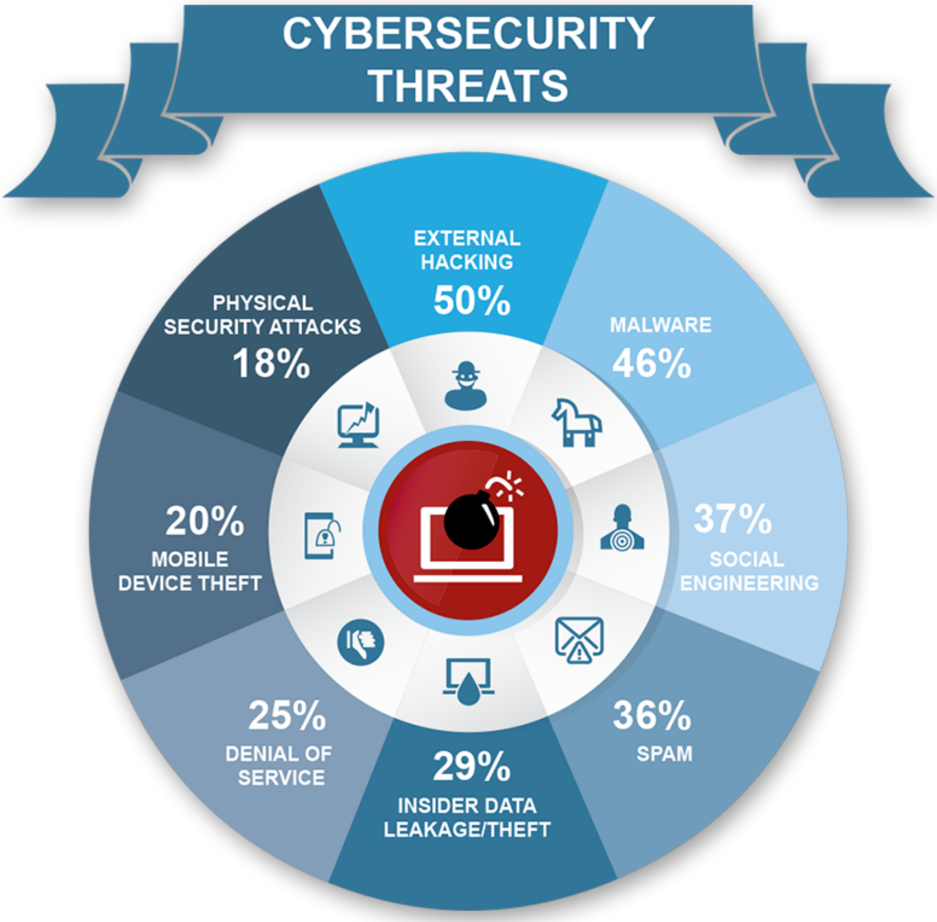
AI-POWERED ATTACKS

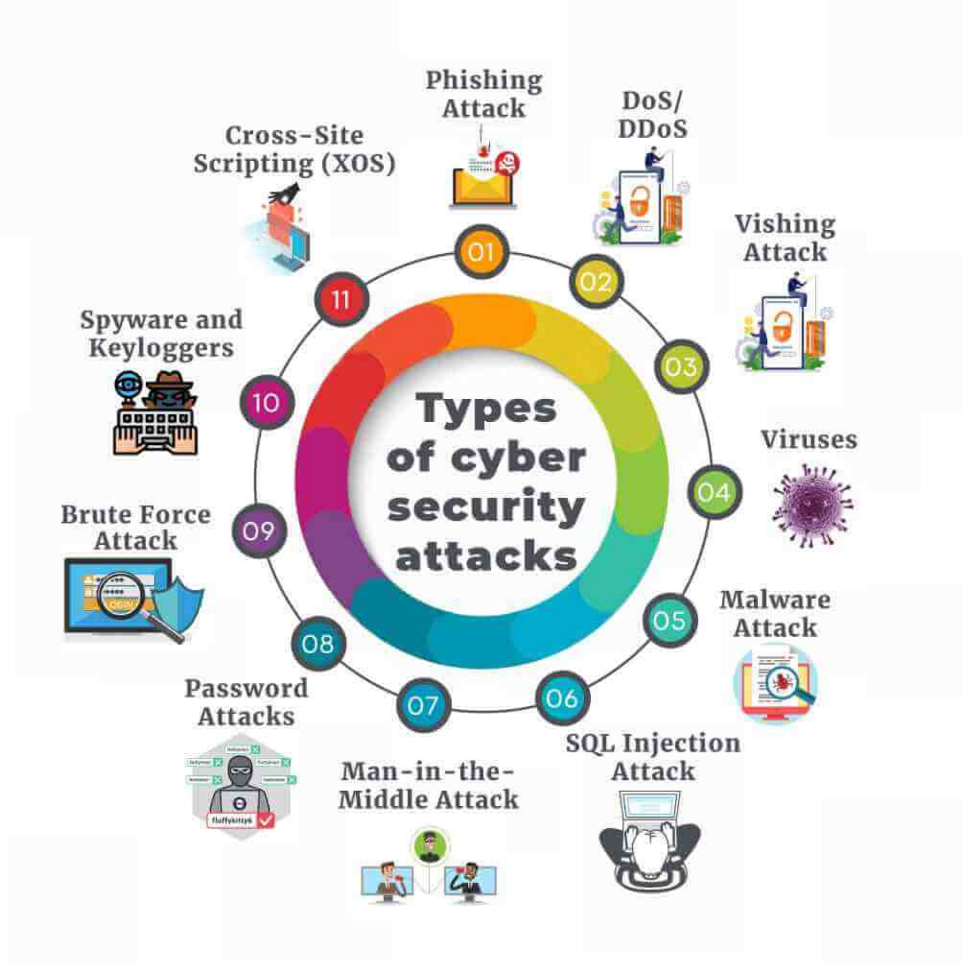
PASSWORD ATTACK
- Brute Force Guessing
- Dictionary Attack

DRIVE-BY ATTACK

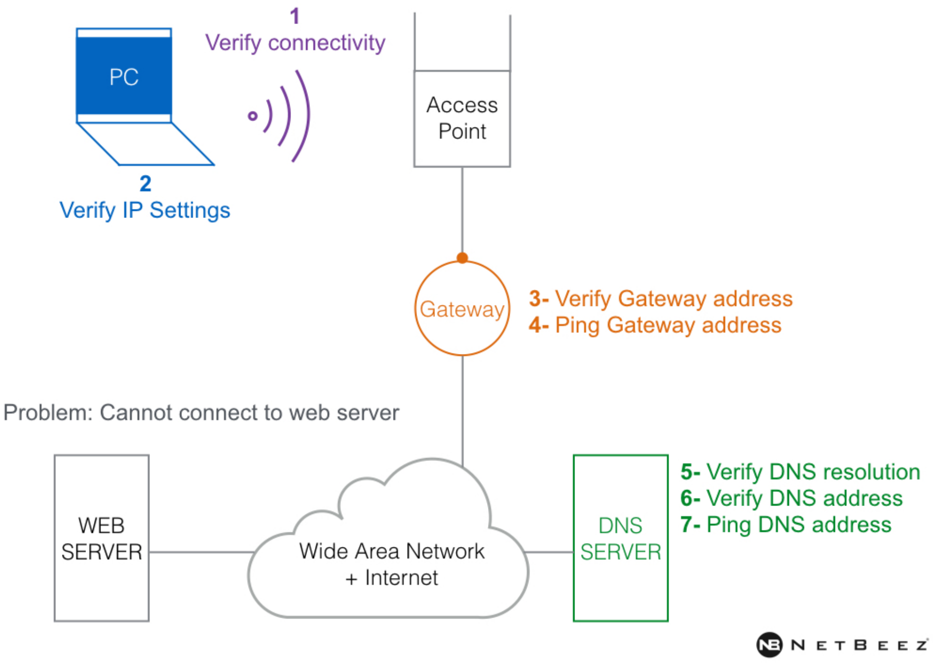
RANSOMWARE ATTACK

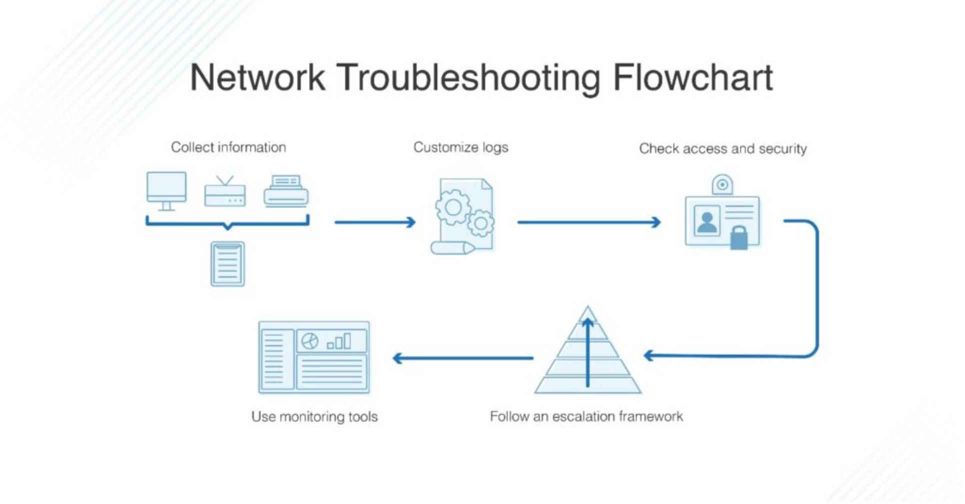
EAVESDROPPING ATTACK

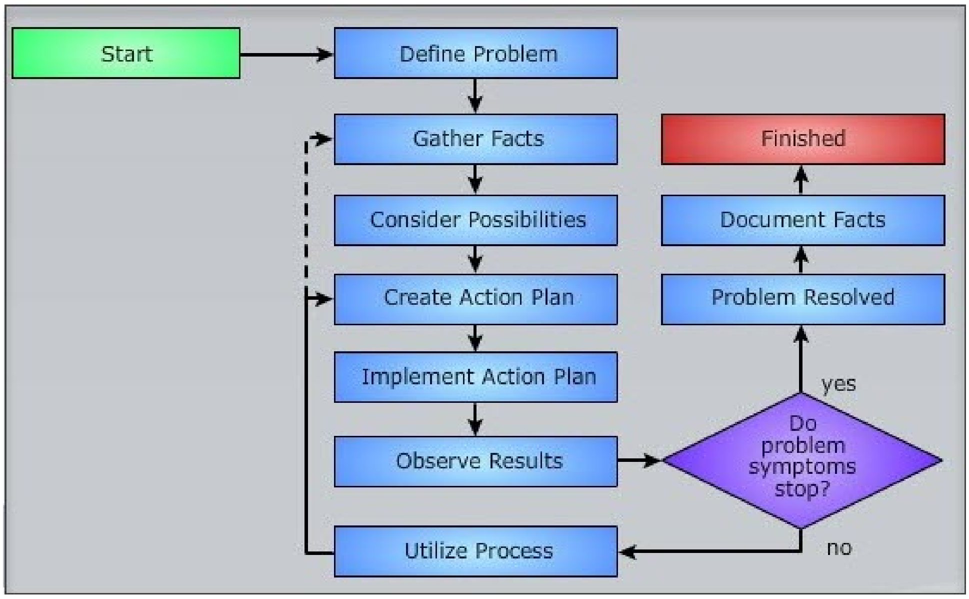




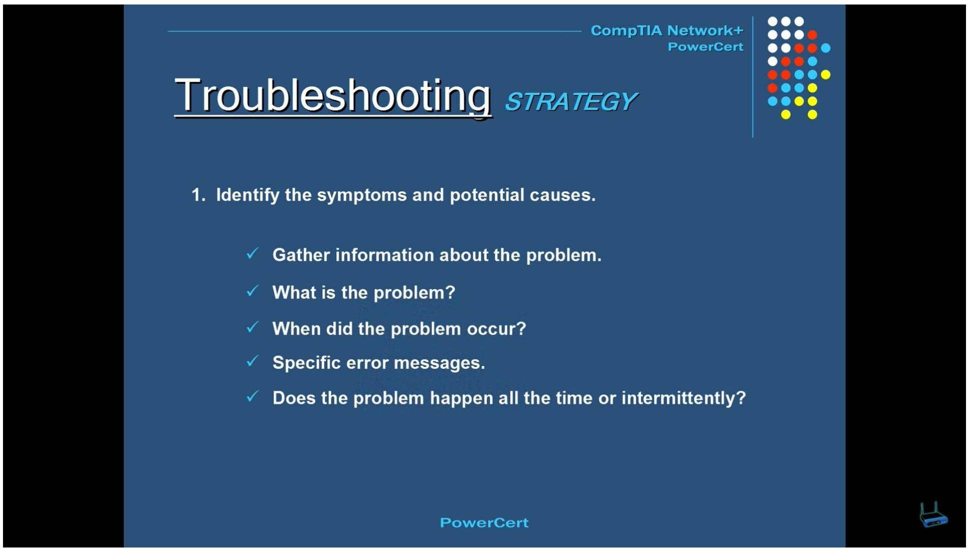
# Network Troubleshooting




Network Troubleshooting Flowchart
Collect information
Customize logs
Check access and security
Use monitoring tools
Follow an escalation framework



# Troubleshooting Strategy



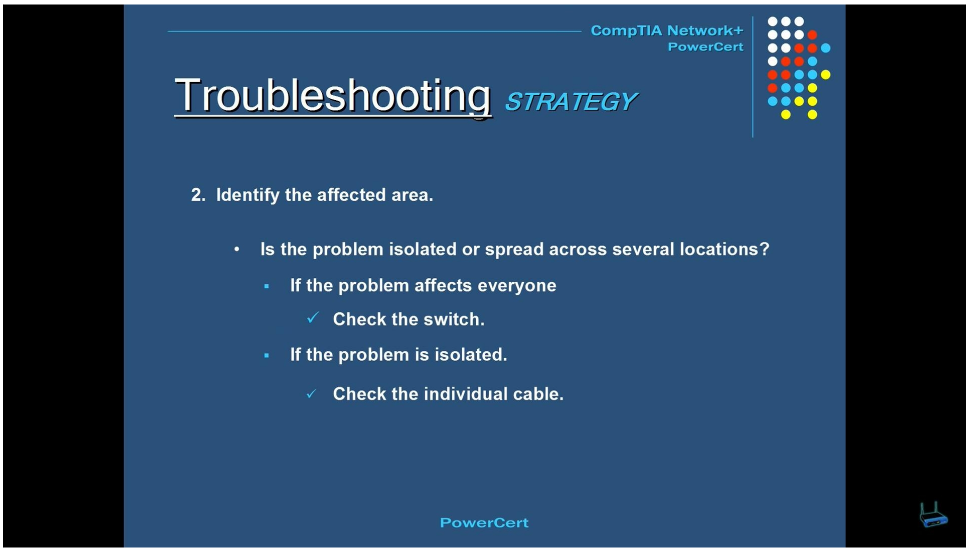
CompTIA Network+
PowerCert

# Troubleshooting *STRATEGY*

1. Identify the symptoms and potential causes.

- ✓ Gather information about the problem.
- ✓ What is the problem?
- ✓ When did the problem occur?
- ✓ Specific error messages.
- ✓ Does the problem happen all the time or intermittently?

PowerCert



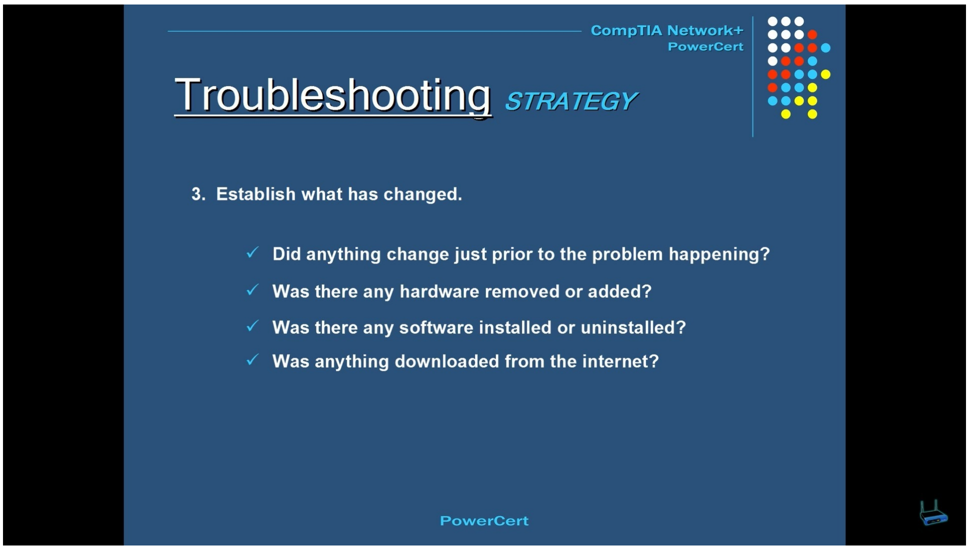
CompTIA Network+
PowerCert

# Troubleshooting *STRATEGY*

2. Identify the affected area.

- Is the problem isolated or spread across several locations?
  - If the problem affects everyone
    - ✓ Check the switch.
  - If the problem is isolated.
    - ✓ Check the individual cable.

PowerCert



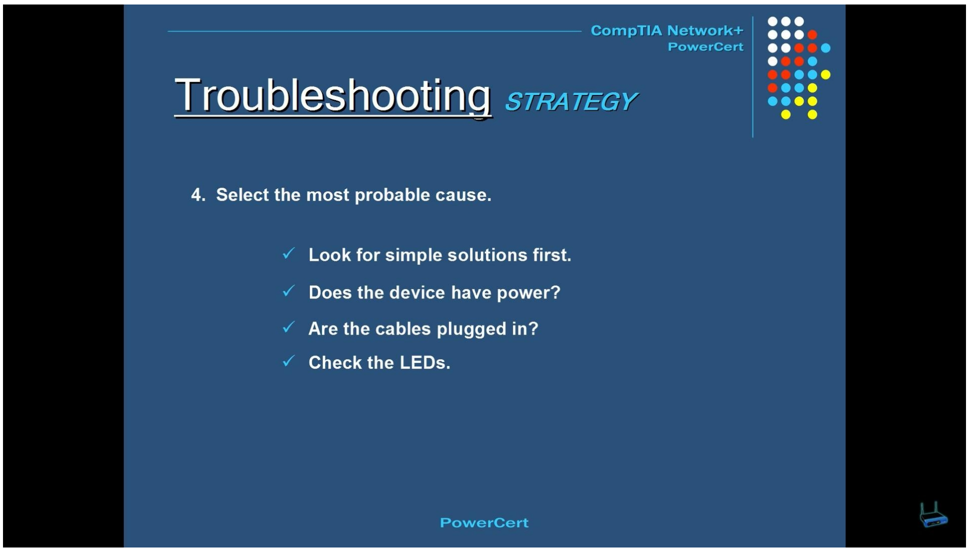
CompTIA Network+
PowerCert

# Troubleshooting *STRATEGY*

3. Establish what has changed.

- ✓ Did anything change just prior to the problem happening?
- ✓ Was there any hardware removed or added?
- ✓ Was there any software installed or uninstalled?
- ✓ Was anything downloaded from the internet?

PowerCert



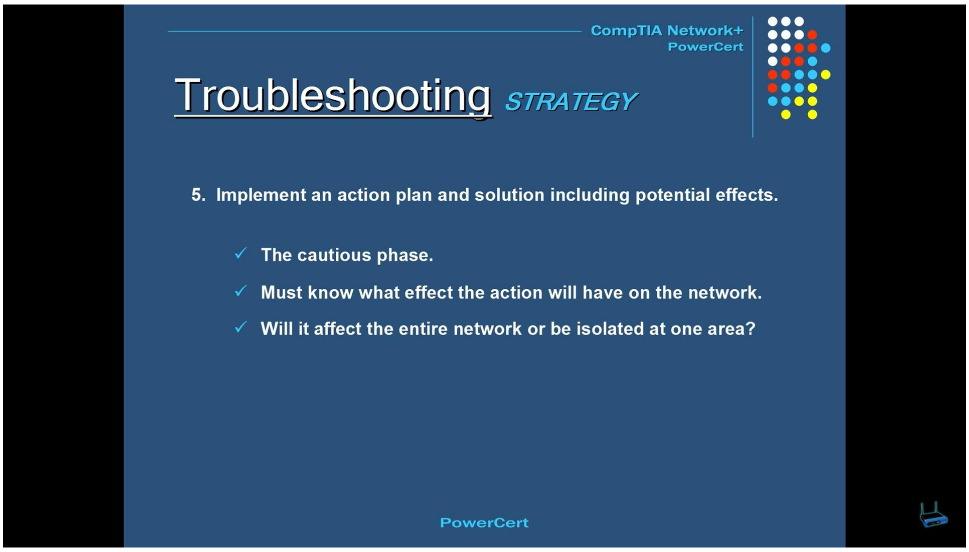
CompTIA Network+
PowerCert

## Troubleshooting *STRATEGY*

4. Select the most probable cause.

- ✓ Look for simple solutions first.
- ✓ Does the device have power?
- ✓ Are the cables plugged in?
- ✓ Check the LEDs.

PowerCert



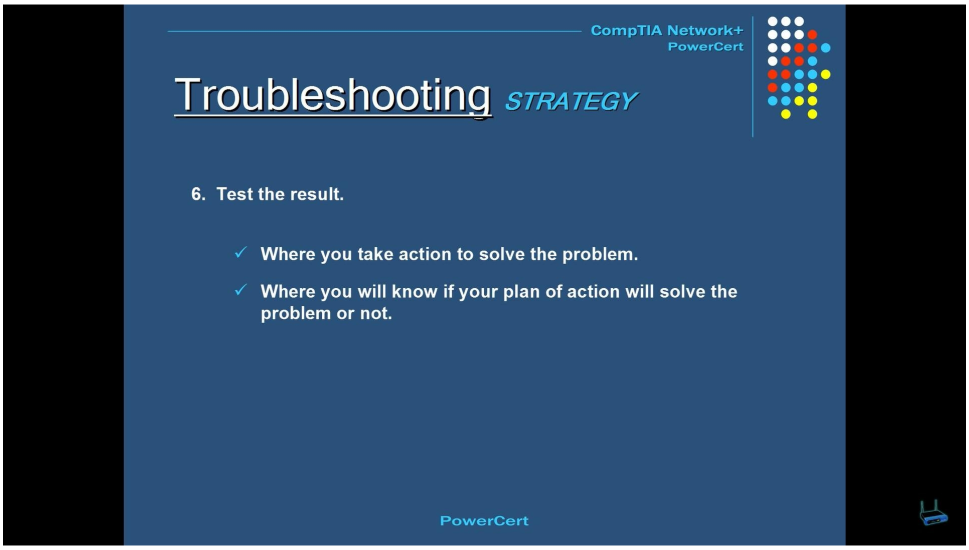
CompTIA Network+
PowerCert

## Troubleshooting *STRATEGY*

5. Implement an action plan and solution including potential effects.

- ✓ The cautious phase.
- ✓ Must know what effect the action will have on the network.
- ✓ Will it affect the entire network or be isolated at one area?

PowerCert



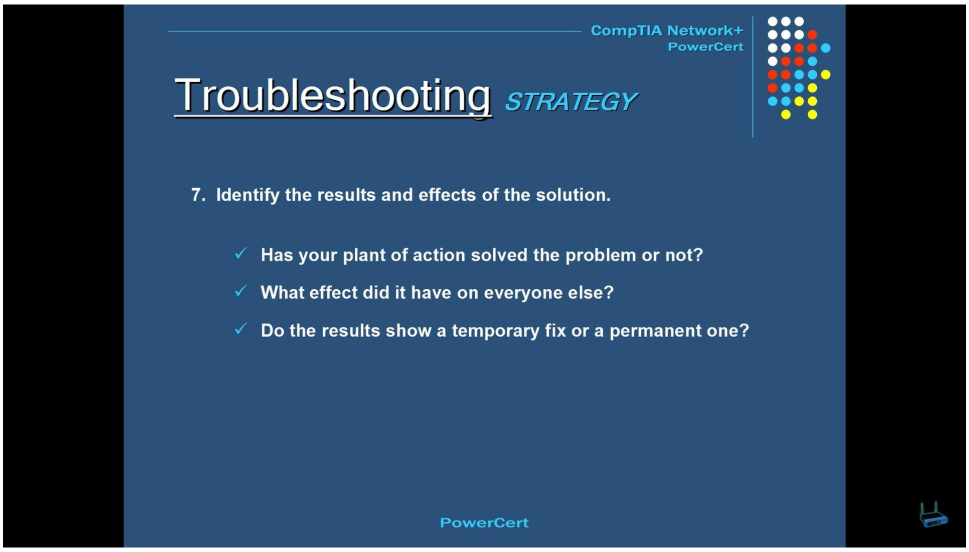
CompTIA Network+
PowerCert

## Troubleshooting *STRATEGY*

6. Test the result.

- ✓ Where you take action to solve the problem.
- ✓ Where you will know if your plan of action will solve the problem or not.

PowerCert



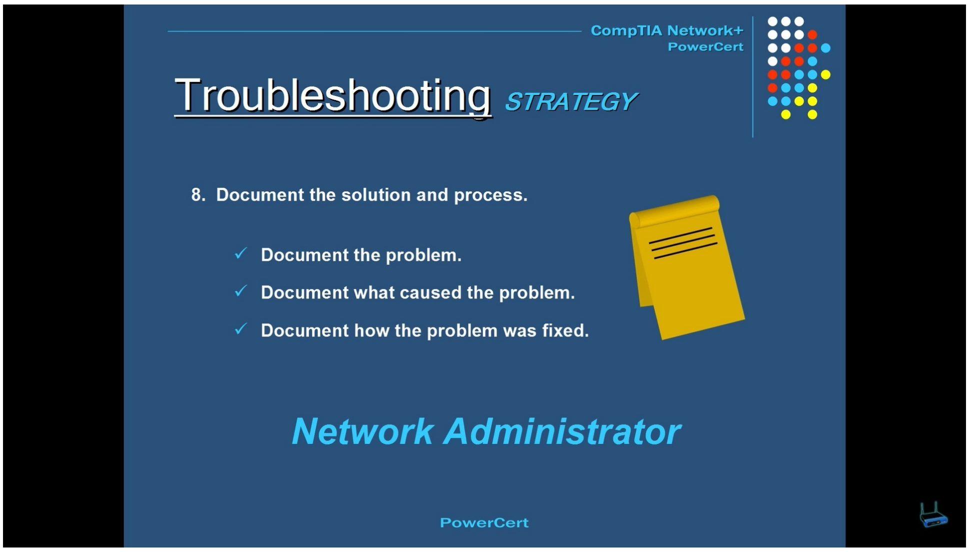
CompTIA Network+
PowerCert

## Troubleshooting *STRATEGY*

7. Identify the results and effects of the solution.

- ✓ Has your plant of action solved the problem or not?
- ✓ What effect did it have on everyone else?
- ✓ Do the results show a temporary fix or a permanent one?

PowerCert



CompTIA Network+
PowerCert

## Troubleshooting *STRATEGY*

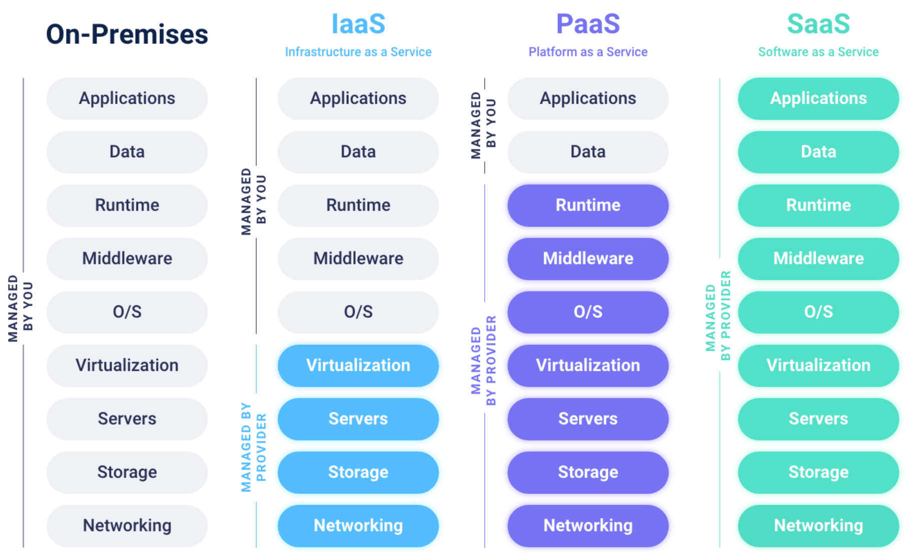
8. Document the solution and process.

- ✓ Document the problem.
- ✓ Document what caused the problem.
- ✓ Document how the problem was fixed.

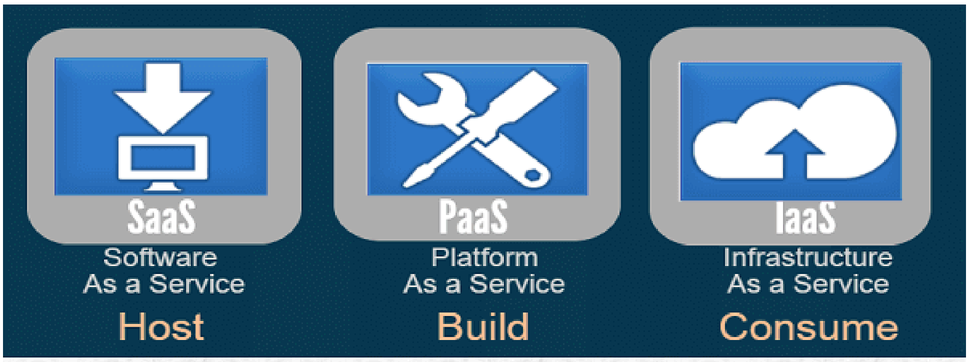
*Network Administrator*

PowerCert

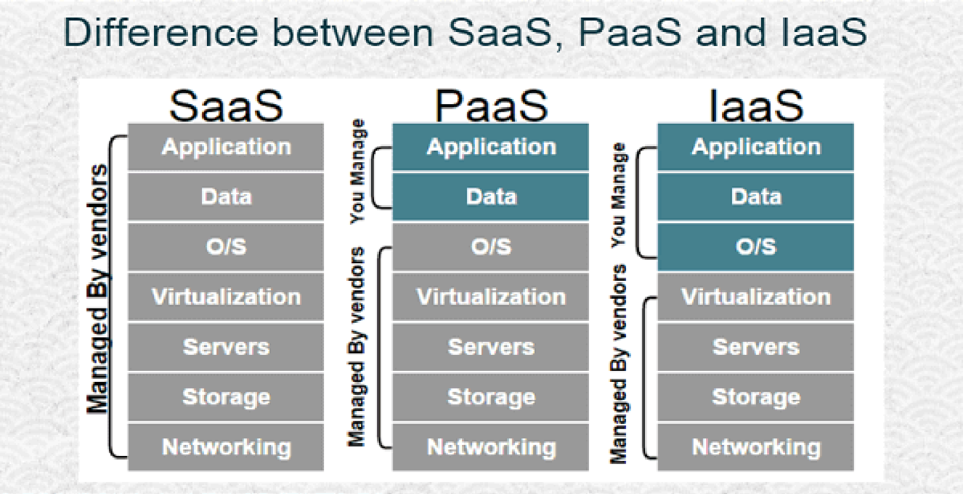
# Could Computing - Iaas Paas Saas



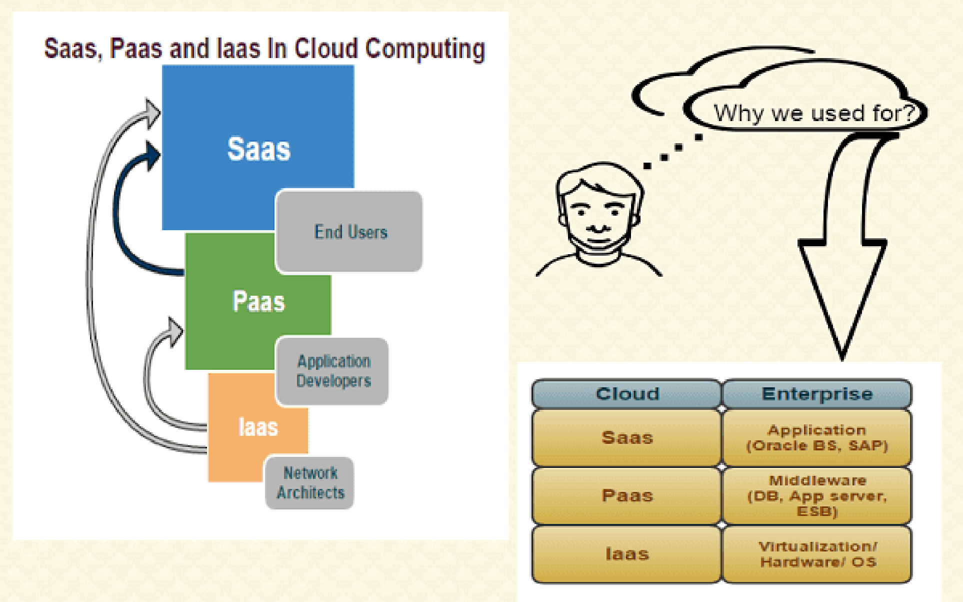
| On-Premises | IaaS<br>Infrastructure as a Service | PaaS<br>Platform as a Service | SaaS<br>Software as a Service |
|---|---|---|---|
| Applications | Applications | Applications | Applications |
| Data | Data | Data | Data |
| Runtime | Runtime | Runtime | Runtime |
| Middleware | Middleware | Middleware | Middleware |
| O/S | O/S | O/S | O/S |
| Virtualization | Virtualization | Virtualization | Virtualization |
| Servers | Servers | Servers | Servers |
| Storage | Storage | Storage | Storage |
| Networking | Networking | Networking | Networking |



## Difference between SaaS, PaaS and IaaS

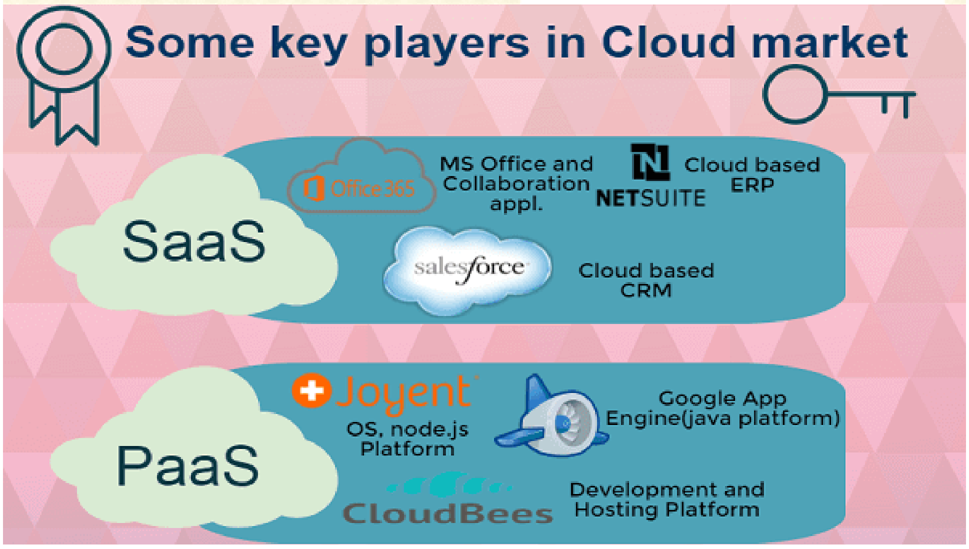


## How Structured in Cloud Computing?



| Cloud | Enterprise |
|---|---|
| Saas | Application (Oracle BS, SAP) |
| Paas | Middleware (DB, App server, ESB) |
| Iaas | Virtualization/ Hardware/ OS |

## Some key players in Cloud market



-- Memo End --

IaaS
rackspace
Cloud Servers
Dropbox
Simply Storage
Akamai
Content Delivery Network