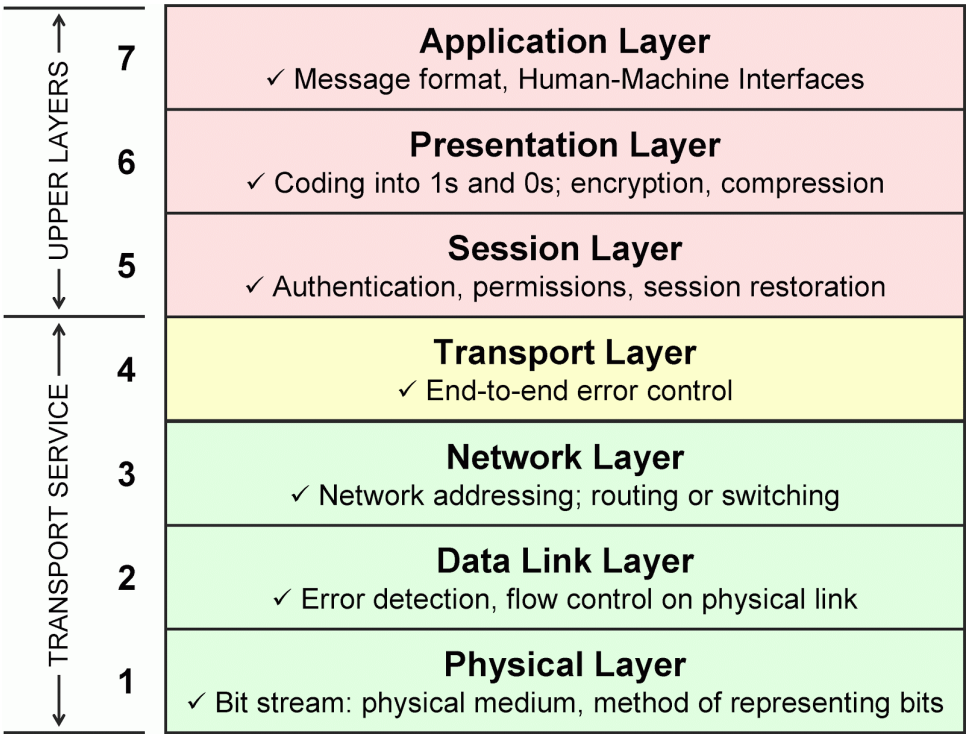
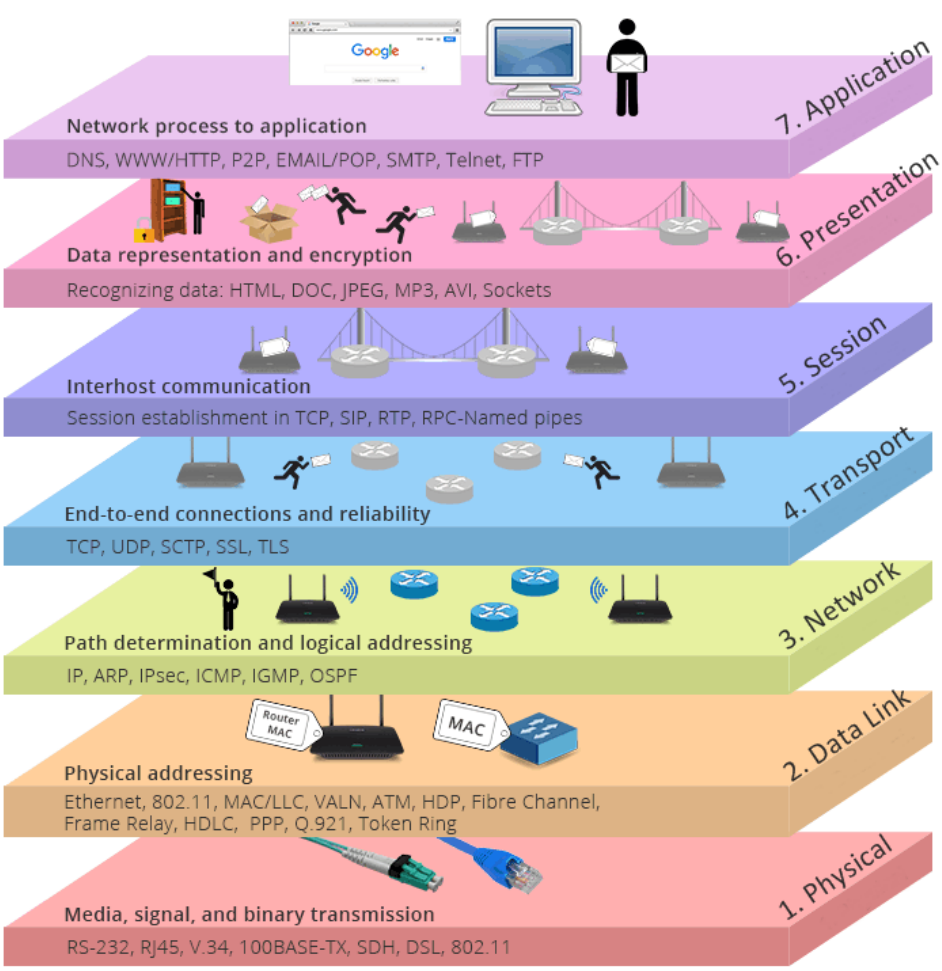
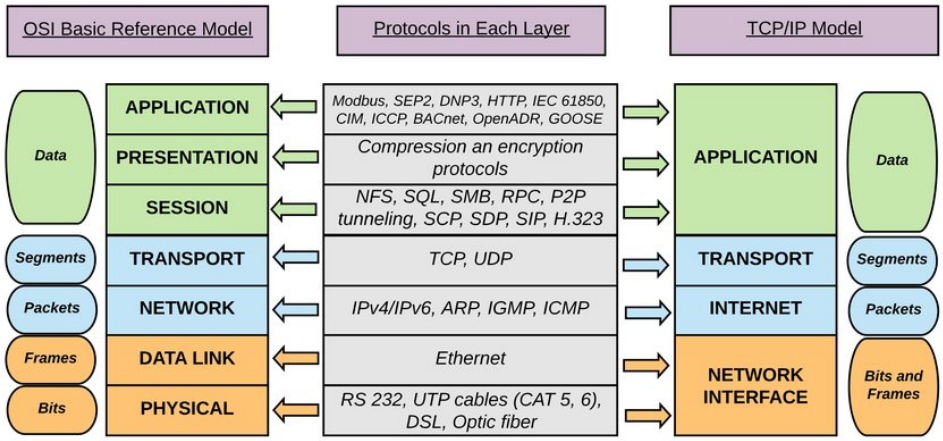
Network

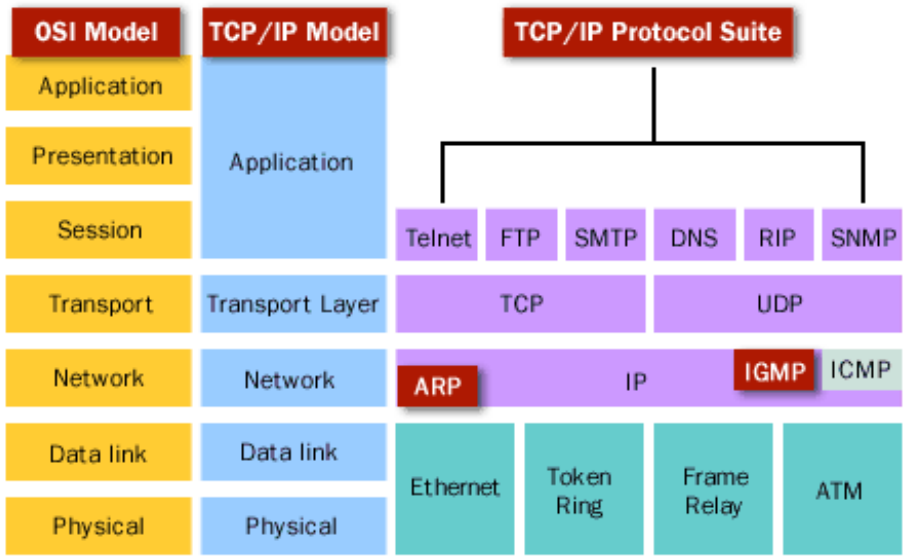
Network OSI Model

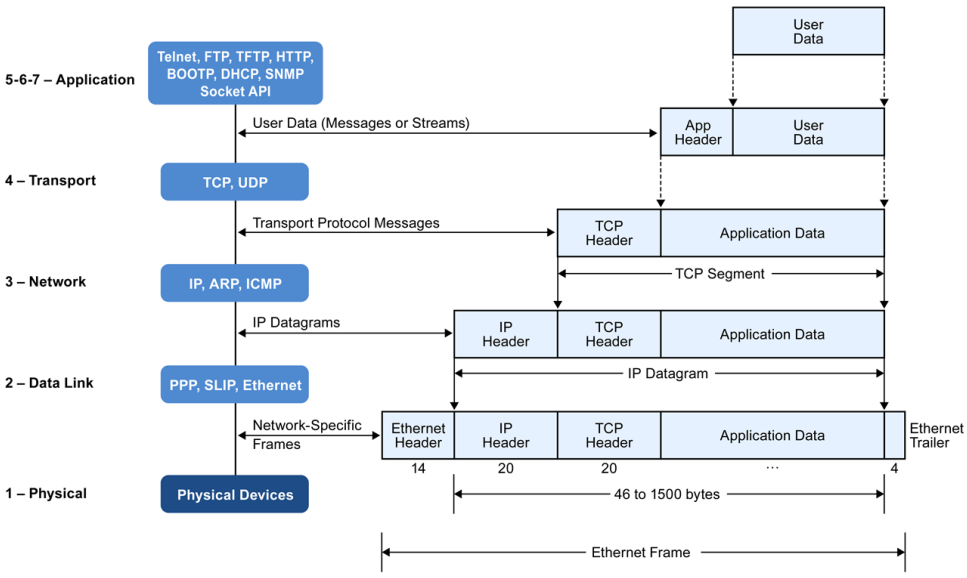


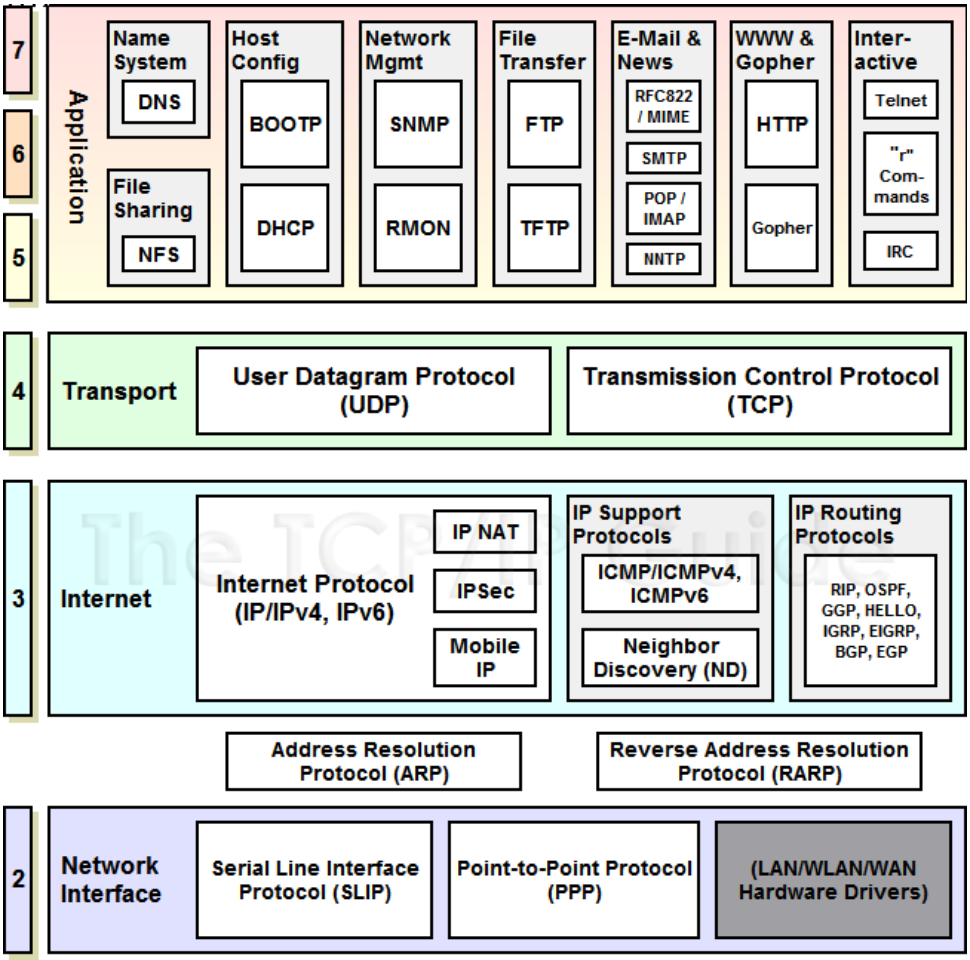


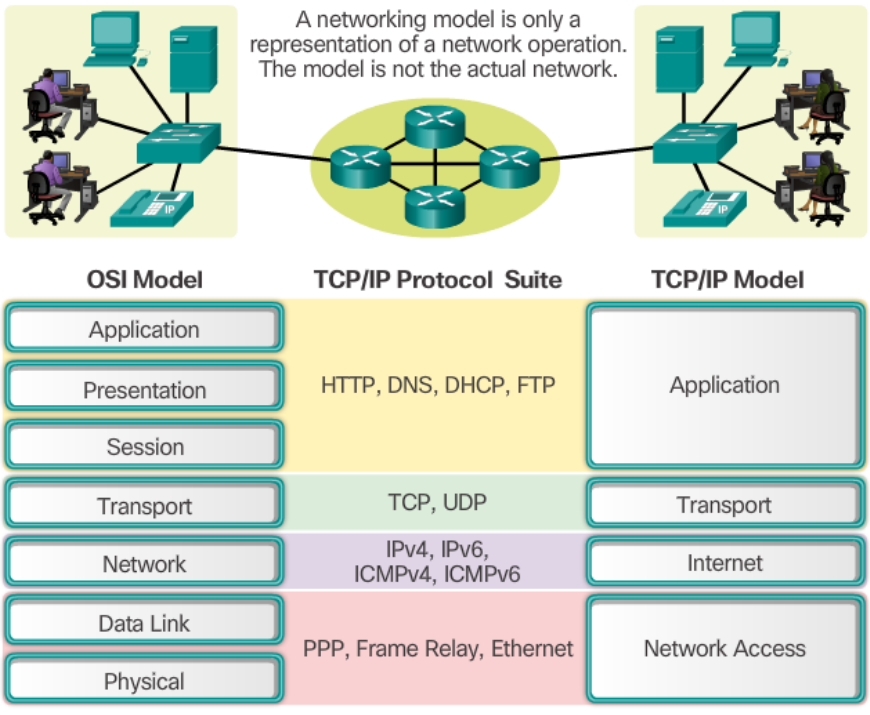
TPC/IP & Protocol

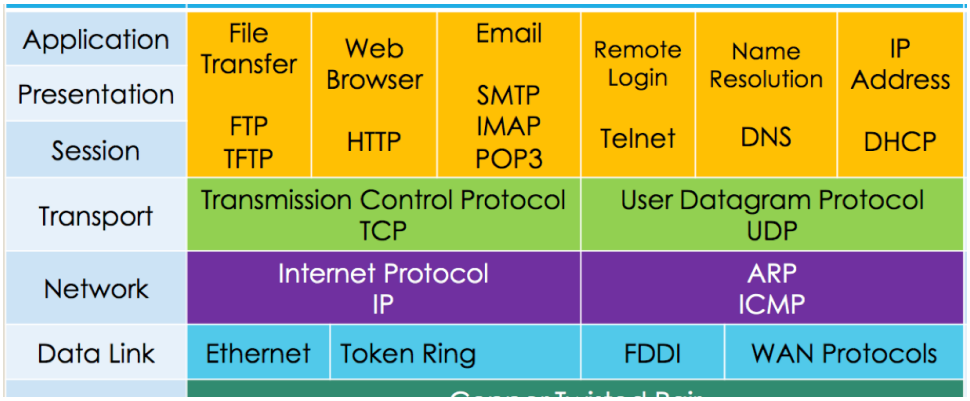


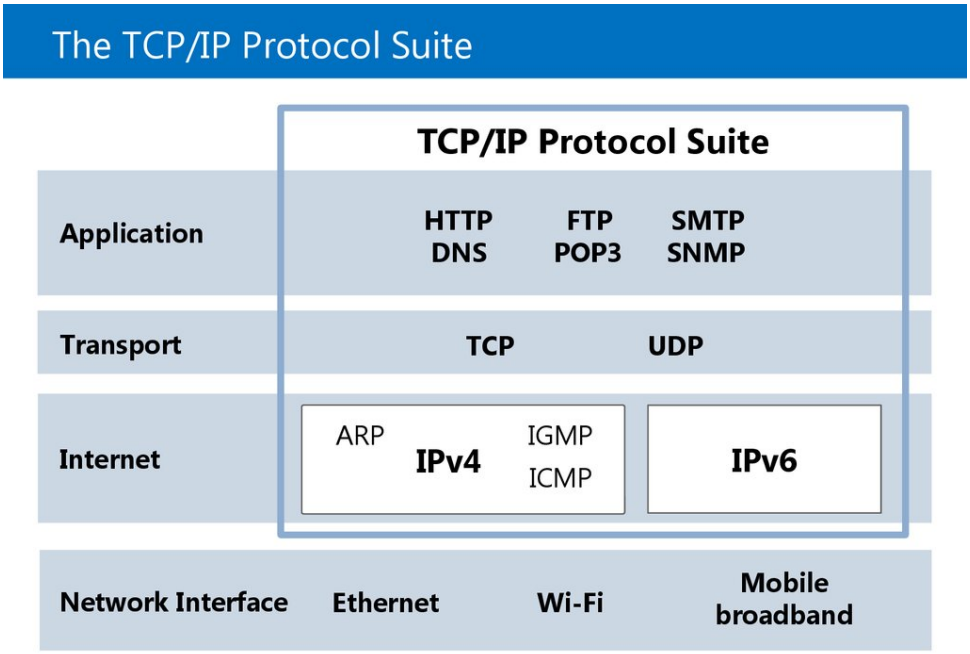




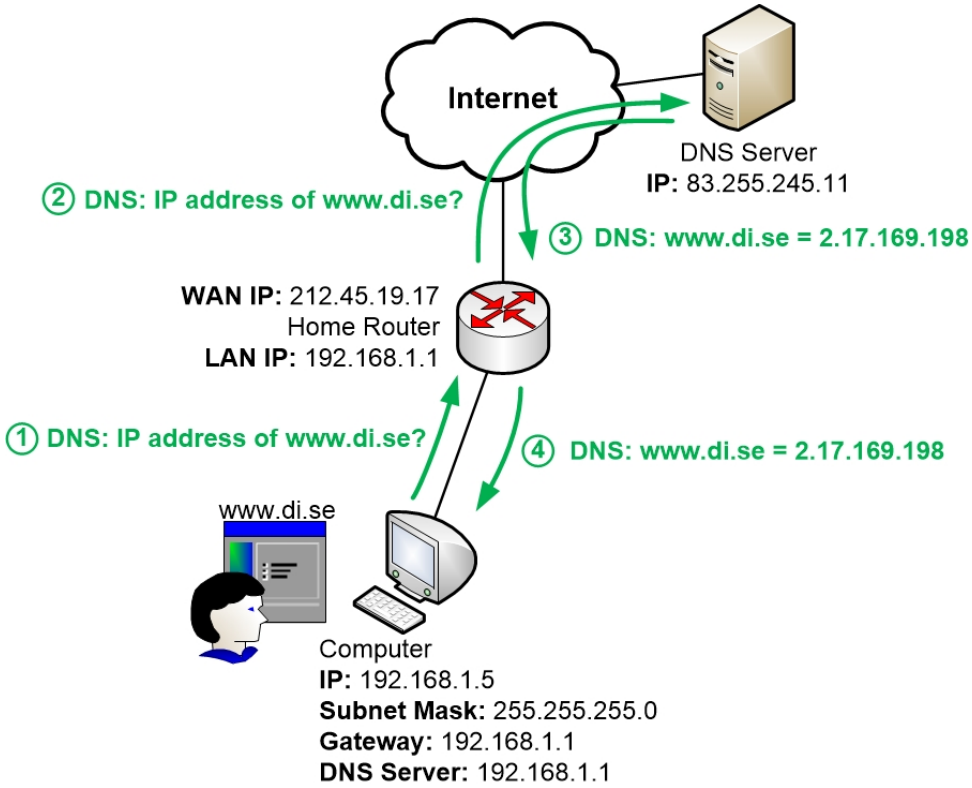

7
6
5
Application
Name System
DNS
File Sharing
NFS
Host Config
BOOTP
DHCP
Network Mgmt
SNMP
RMON
File Transfer
FTP
TFTP
E-Mail & News
RFC822 / MIME
SMTP
POP / IMAP
NNTP
WWW & Gopher
HTTP
Gopher
Inter-active
Telnet
"r" Com-mands
IRC
4
Transport
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
3
Internet
Internet Protocol (IP/IPv4, IPv6)
IP NAT
IPSec
Mobile IP
IP Support Protocols
ICMP/ICMPv4, ICMPv6
Neighbor Discovery (ND)
IP Routing Protocols
RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
2
Network Interface
Serial Line Interface Protocol (SLIP)
Point-to-Point Protocol (PPP)
(LAN/WLAN/WAN Hardware Drivers)

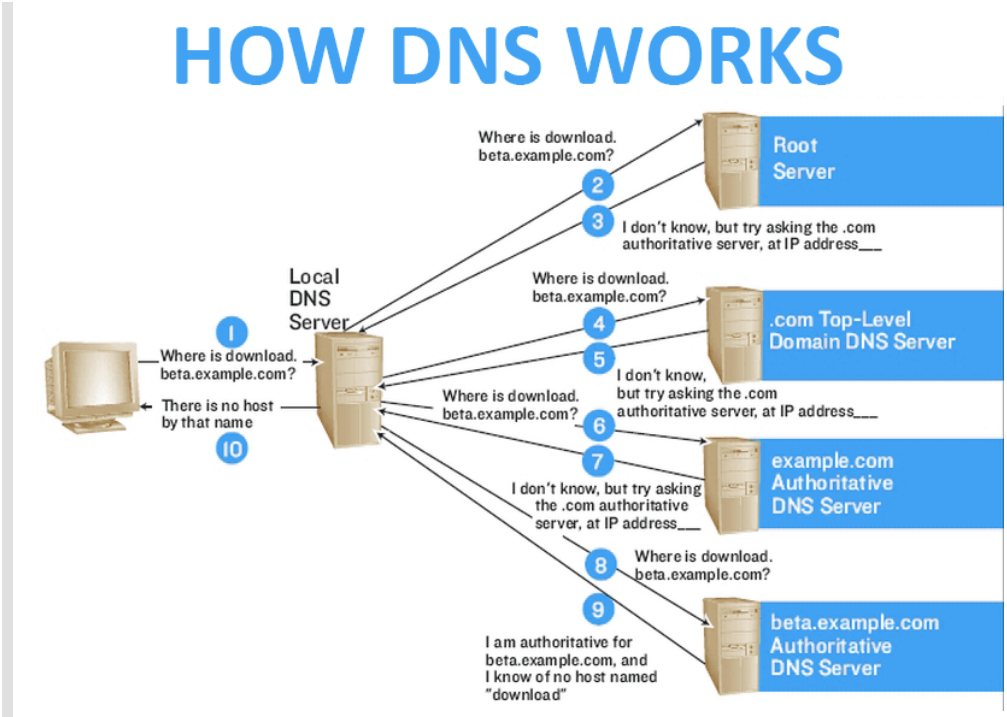

A networking model is only a representation of a network operation. The model is not the actual network.
OSI Model
TCP/IP Protocol Suite
TCP/IP Model
Application
Presentation
Session
HTTP, DNS, DHCP, FTP
Application
Transport
TCP, UDP
Transport
Network
IPv4, IPv6, ICMPv4, ICMPv6
Internet
Data Link
Physical
PPP, Frame Relay, Ethernet
Network Access

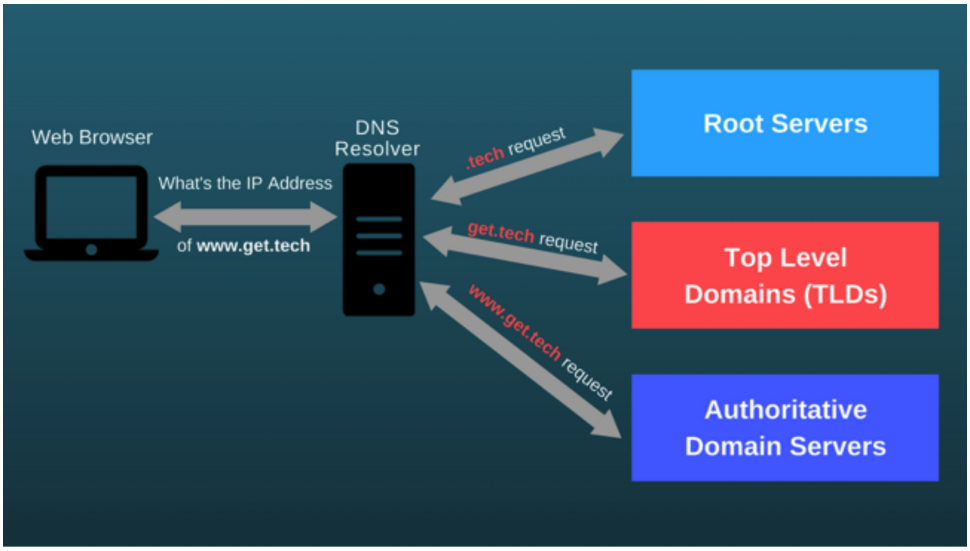


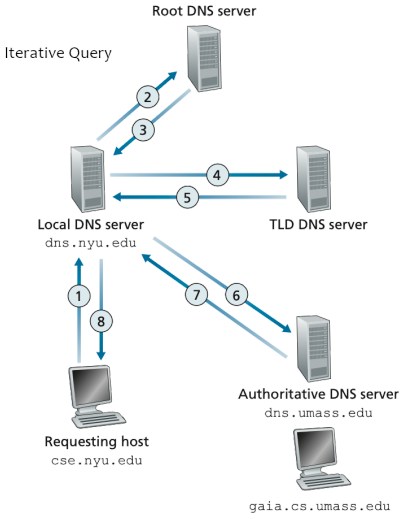


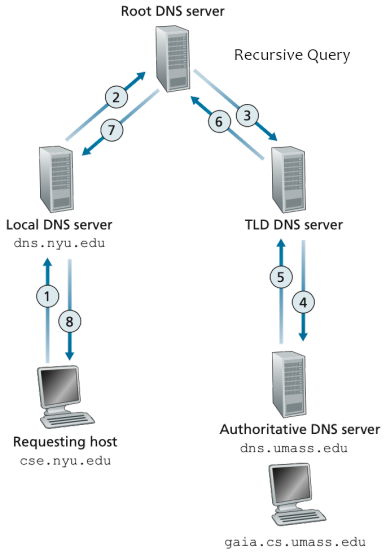
DNS(Domain Name System)


Internet
DNS Server
IP: 83.255.245.11
② DNS: IP address of www.di.se?
③ DNS: www.di.se = 2.17.169.198
WAN IP: 212.45.19.17
Home Router
LAN IP: 192.168.1.1
① DNS: IP address of www.di.se?
④ DNS: www.di.se = 2.17.169.198
www.di.se
Computer
IP: 192.168.1.5
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
DNS Server: 192.168.1.1

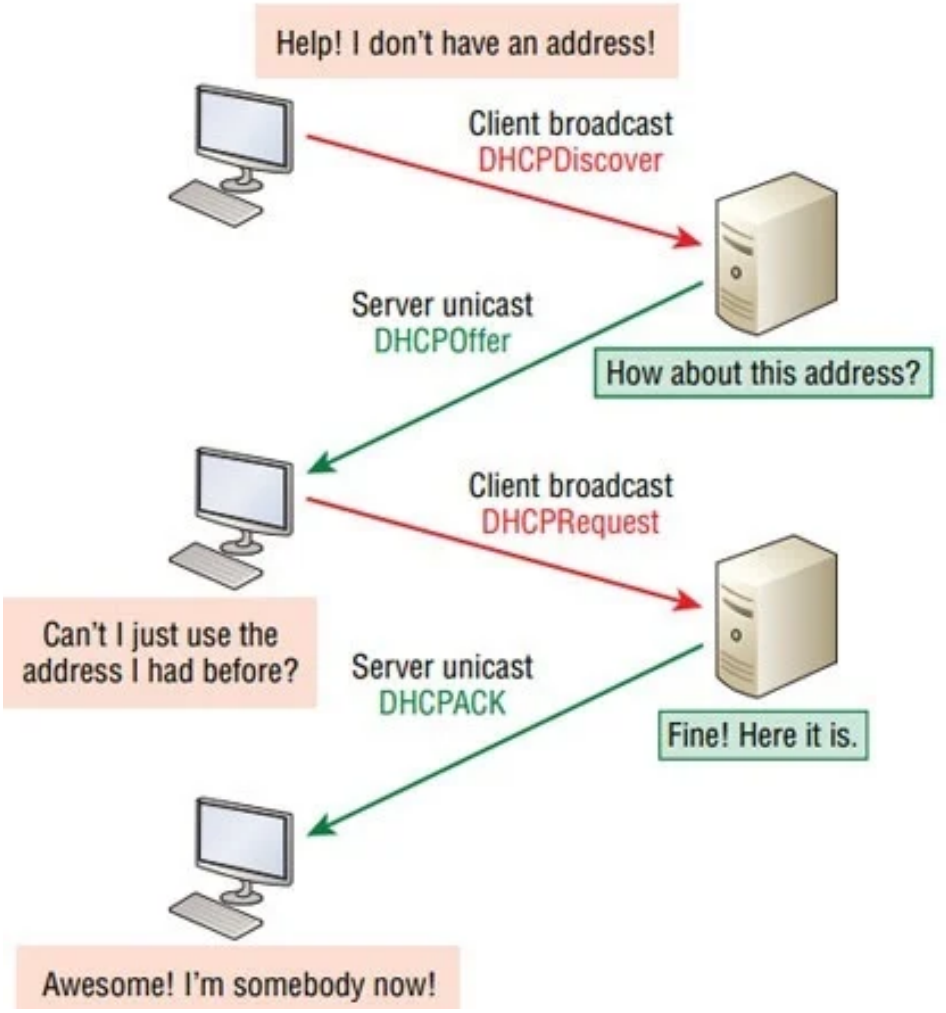

HOW DNS WORKS
Where is download. beta.example.com?
Root Server
I don't know, but try asking the .com authoritative server, at IP address___
Local DNS Server
Where is download. beta.example.com?
.com Top-Level Domain DNS Server
I don't know, but try asking the .com authoritative server, at IP address___
Where is download. beta.example.com?
There is no host by that name
Where is download. beta.example.com?
example.com Authoritative DNS Server
I don't know, but try asking the .com authoritative server, at IP address___
Where is download. beta.example.com?
beta.example.com Authoritative DNS Server
I am authoritative for beta.example.com, and I know of no host named "download"

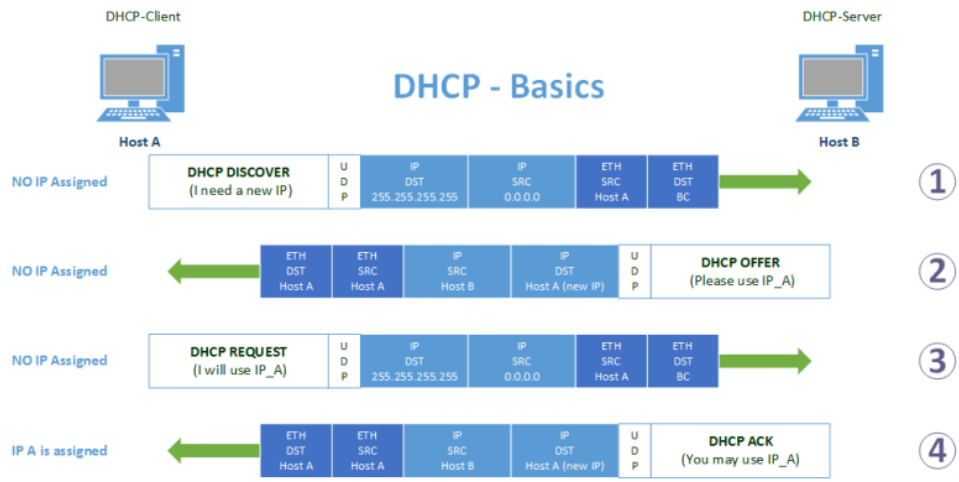

Web Browser
DNS Resolver
What's the IP Address
of www.get.tech
.tech request
get.tech request
www.get.tech request
Root Servers
Top Level Domains (TLDs)
Authoritative Domain Servers

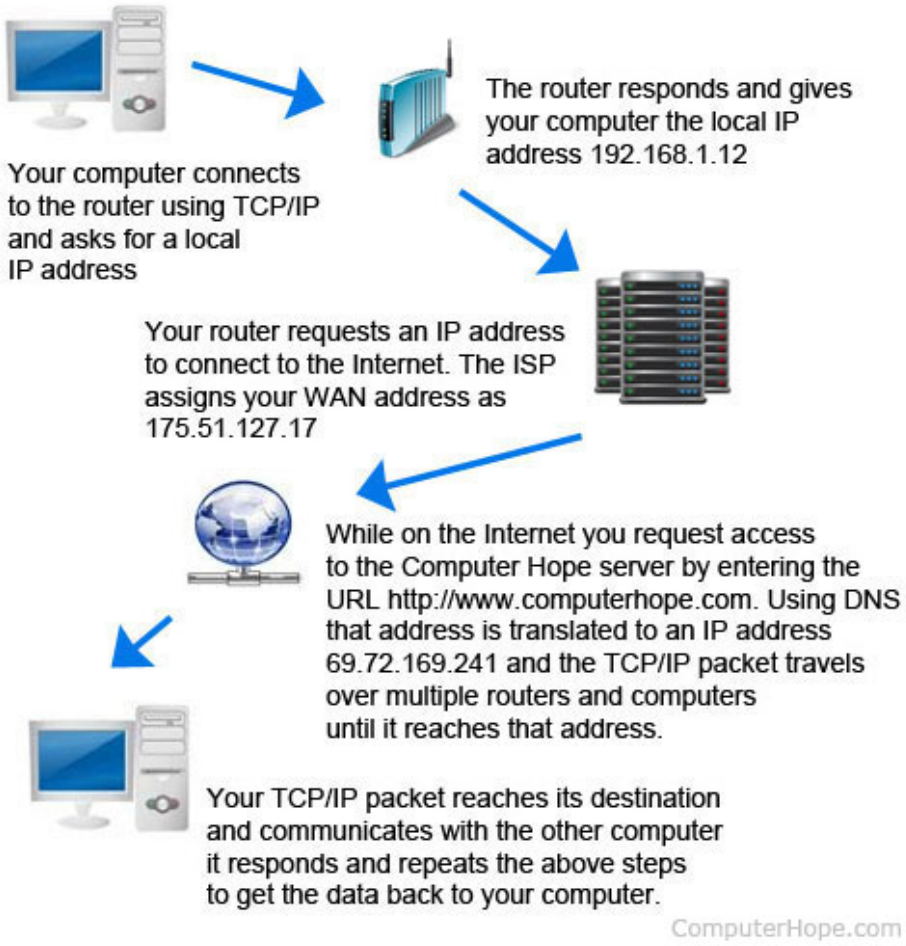

Root DNS server
Iterative Query
Local DNS server
dns.nyu.edu
TLD DNS server
Authoritative DNS server
dns.umass.edu
Requesting host
cse.nyu.edu
gaia.cs.umass.edu


Root DNS server
Recursive Query
Local DNS server
dns.nyu.edu
TLD DNS server
Authoritative DNS server
dns.umass.edu
Requesting host
cse.nyu.edu
gaia.cs.umass.edu

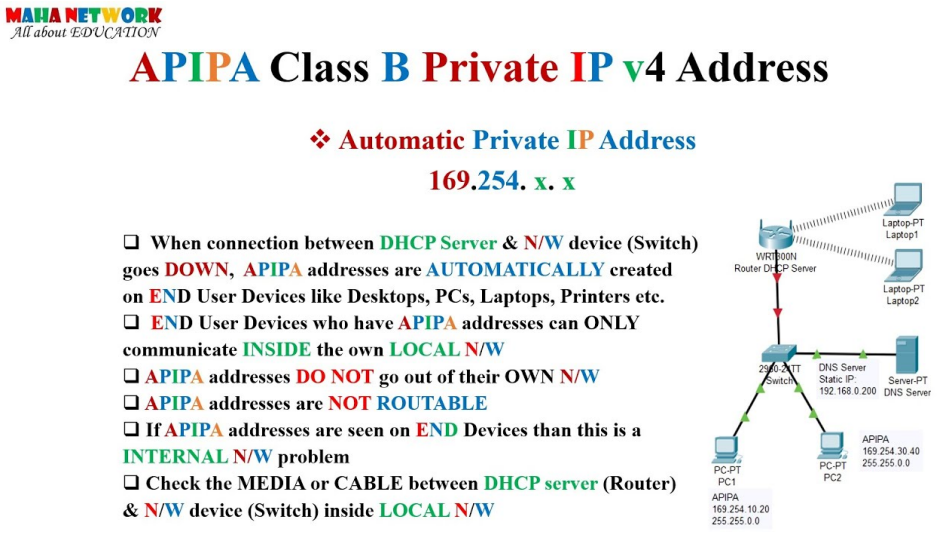
DHCP


Help! I don't have an address!
Client broadcast
DHCPDiscover
Server unicast
DHCPOffer
How about this address?
Client broadcast
DHCPRequest
Can't I just use the address I had before?
Server unicast
DHCPACK
Fine! Here it is.
Awesome! I'm somebody now!

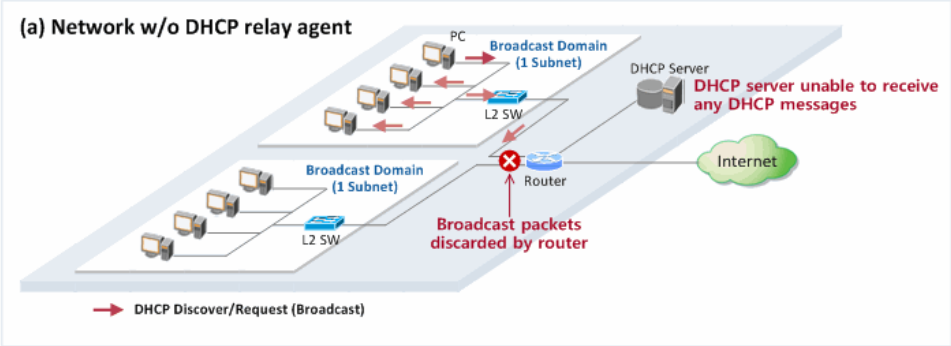

DHCP-Client
DHCP-Server
DHCP - Basics
Host A
Host B
NO IP Assigned
DHCP DISCOVER
(I need a new IP)
U D P
IP DST 255.255.255.255
IP SRC 0.0.0.0
ETH SRC Host A
ETH DST BC
1
NO IP Assigned
ETH DST Host A
ETH SRC Host A
IP SRC Host B
IP DST Host A (new IP)
U D P
DHCP OFFER
(Please use IP_A)
2
NO IP Assigned
DHCP REQUEST
(I will use IP_A)
U D P
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)
U D P
DHCP ACK
(You may use IP_A)
4

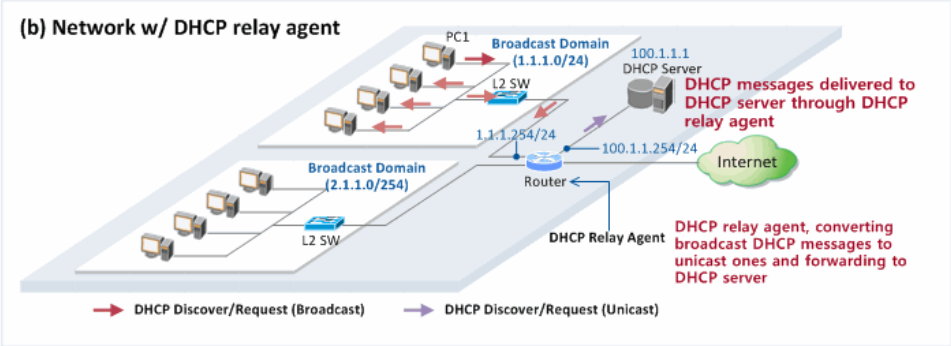


APIPA



DHCP Relay = IP Helper





Port

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		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

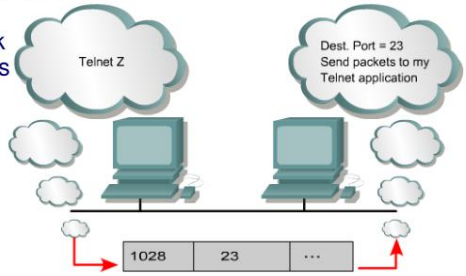
Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

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

Transport Layer Ports

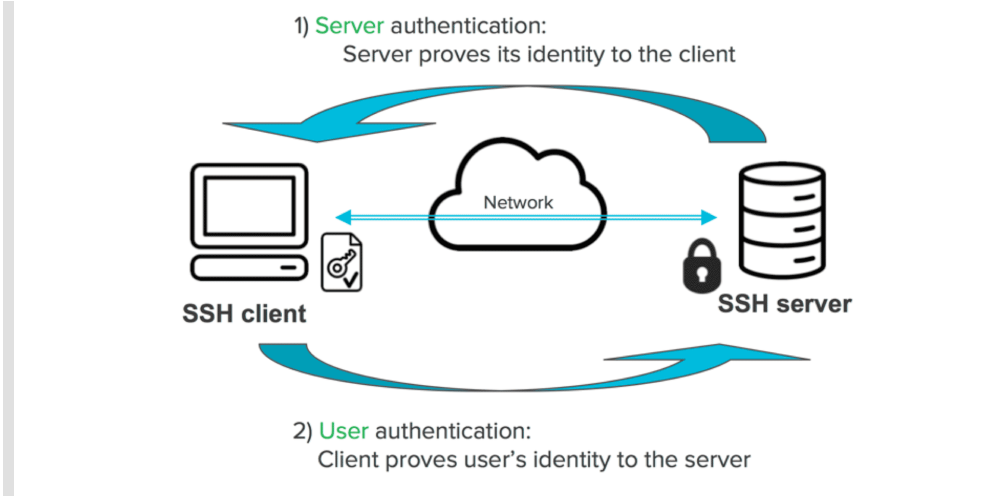
- Port numbers are used to keep track of different **conversations** that cross the network at the same time.
- Port numbers identify which upper layer service is needed, and are needed when a host communicates with a server that uses multiple services.

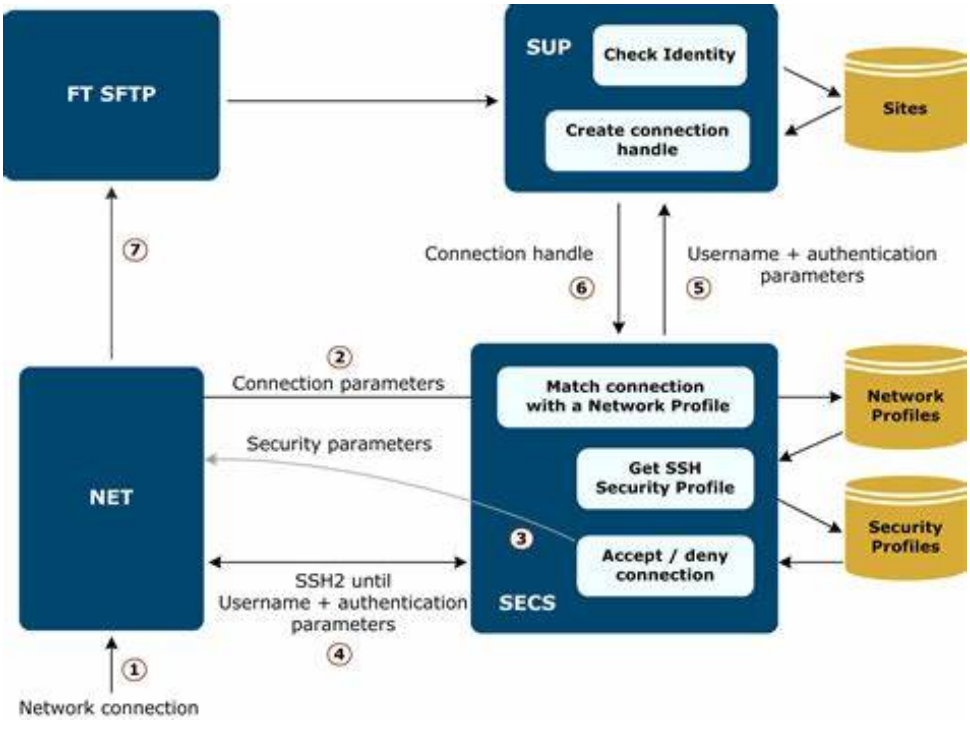


- Both TCP and UDP use port numbers to pass to the upper layers.
- Port numbers have the following **ranges**:
  - 0-255 used for public applications, 0-1023 also called **well-known ports,** regulated by IANA (Internet assigned numbers authority)**.**
  - Numbers from 255-1023 are assigned to marketable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

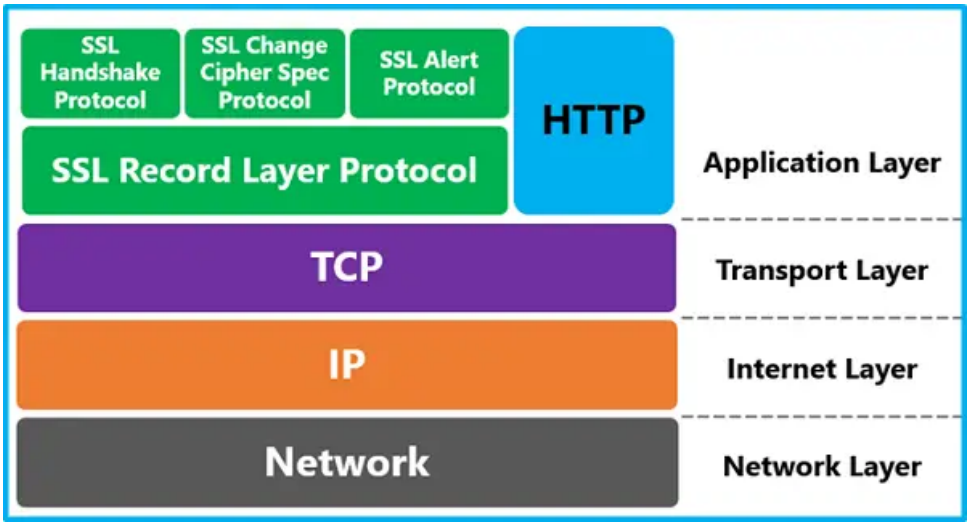
Dr. Muazzam A. Khan 4

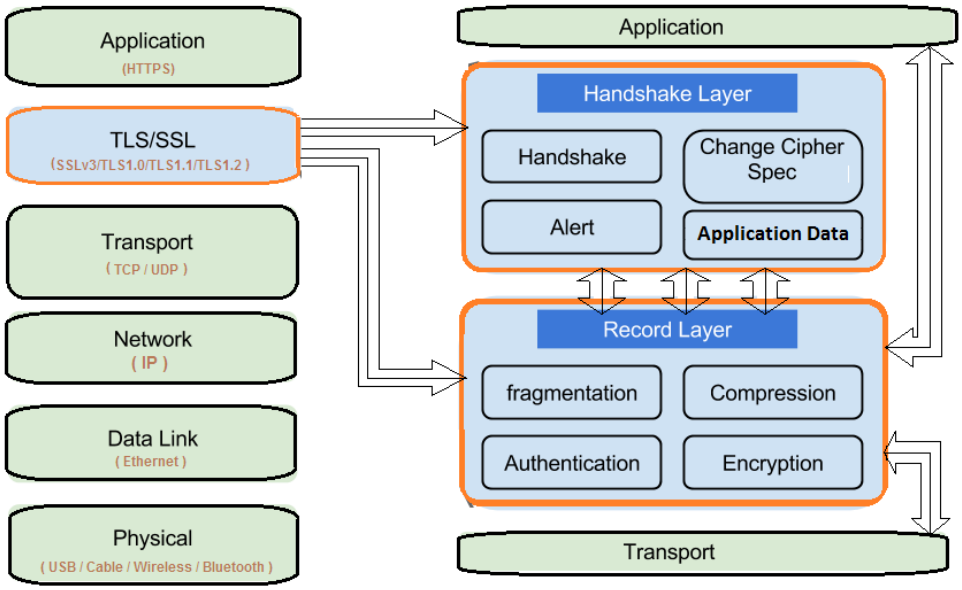
SSH(Secure Shell)

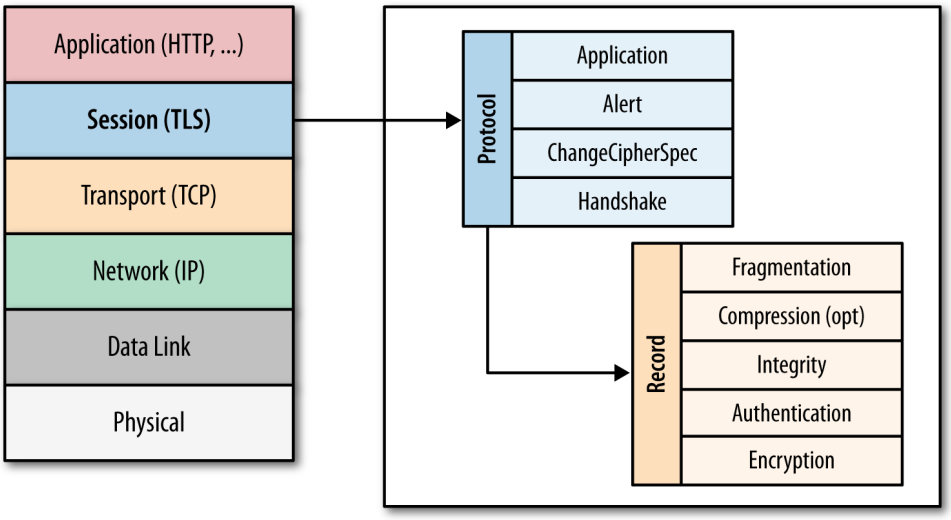


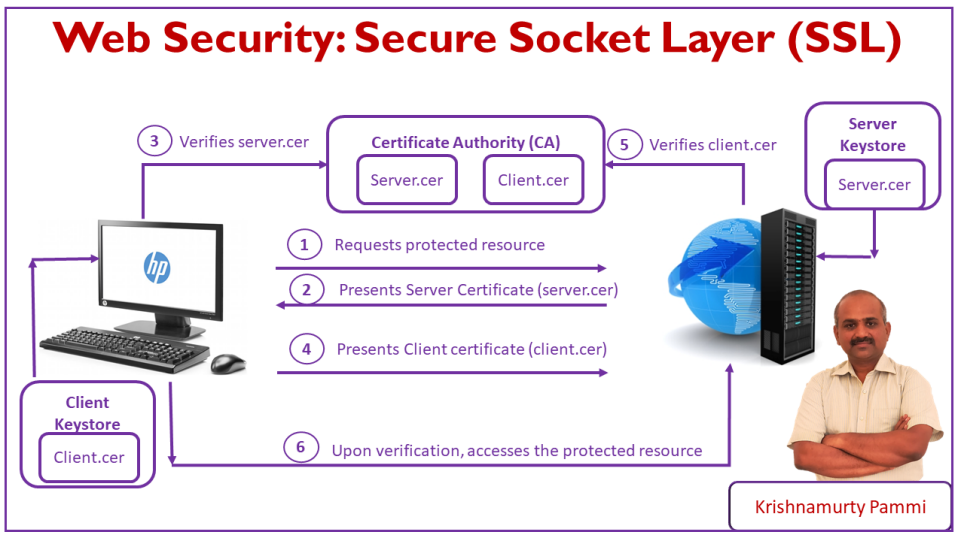


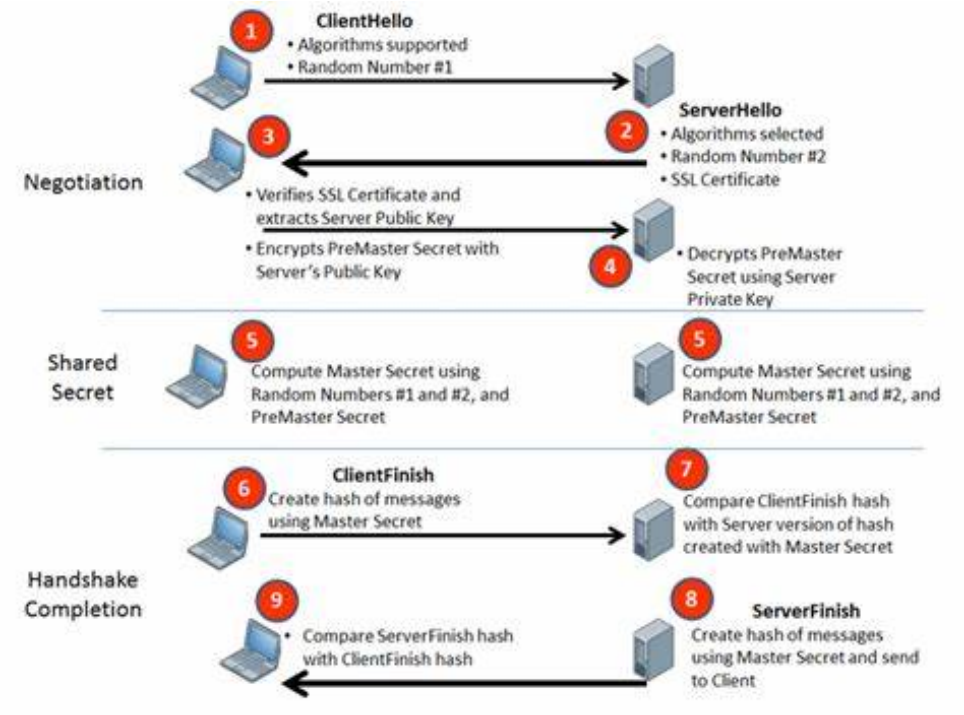
SSL(Secure Sockets Layers)

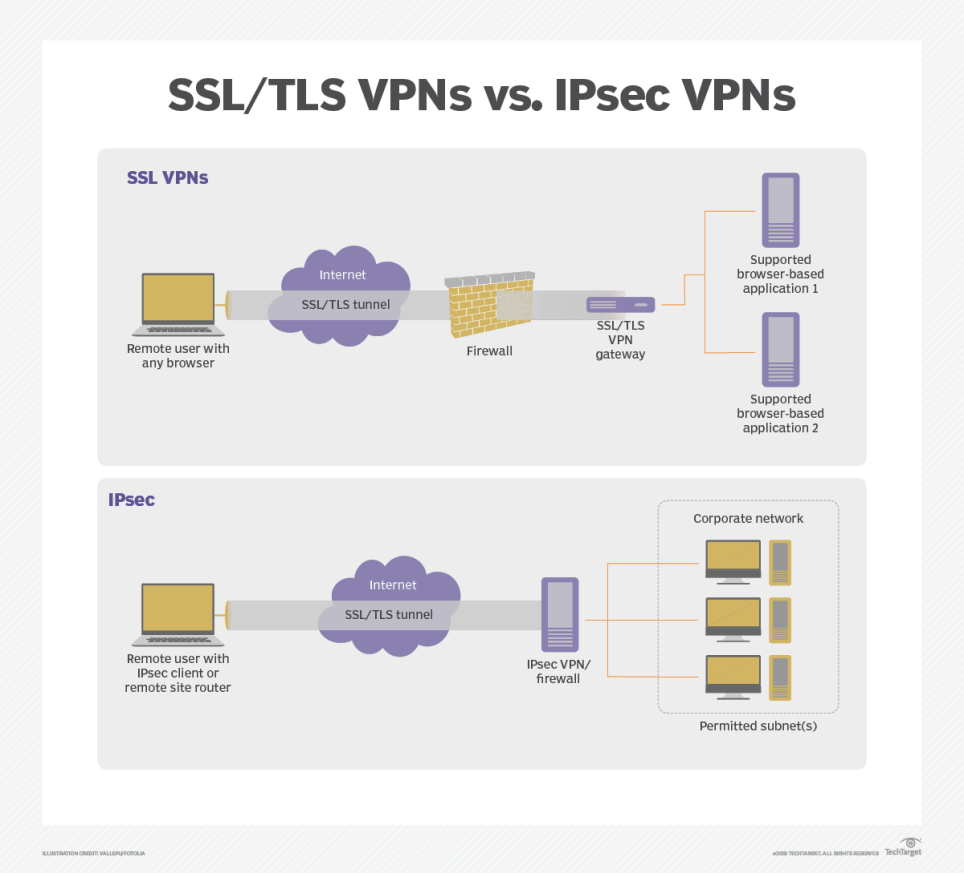


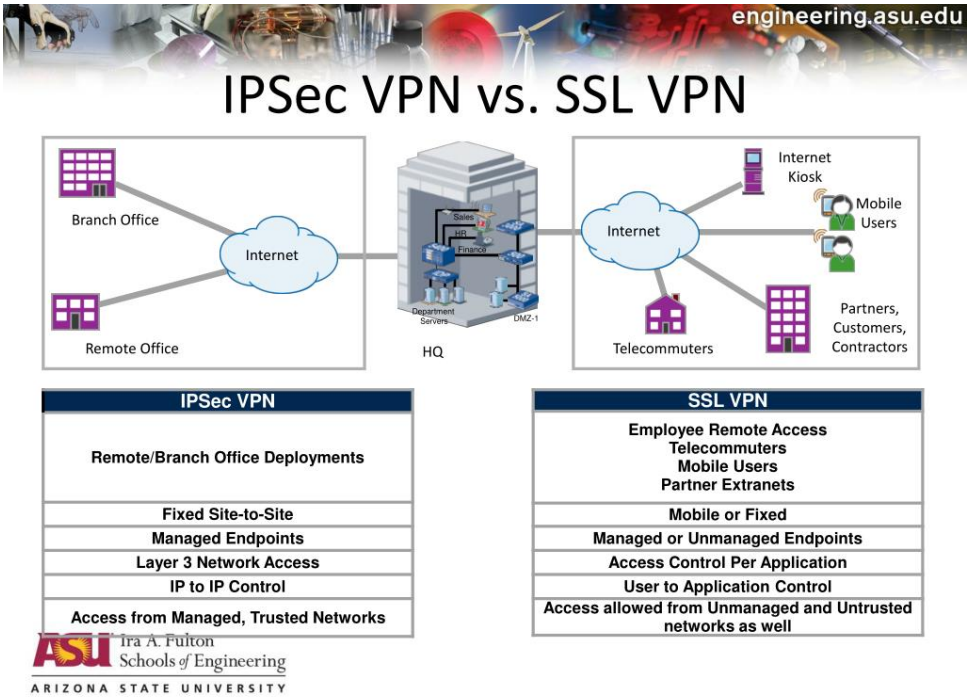

Application
(HTTPS)
TLS/SSL
(SSLv3/TLS1.0/TLS1.1/TLS1.2)
Transport
(TCP / UDP)
Network
(IP)
Data Link
(Ethernet)
Physical
(USB / Cable / Wireless / Bluetooth)
Application
Handshake Layer
Handshake
Change Cipher Spec
Alert
Application Data
Record Layer
fragmentation
Compression
Authentication
Encryption
Transport


Application (HTTP, ...)
Session (TLS)
Transport (TCP)
Network (IP)
Data Link
Physical
Protocol
Application
Alert
ChangeCipherSpec
Handshake
Record
Fragmentation
Compression (opt)
Integrity
Authentication
Encryption

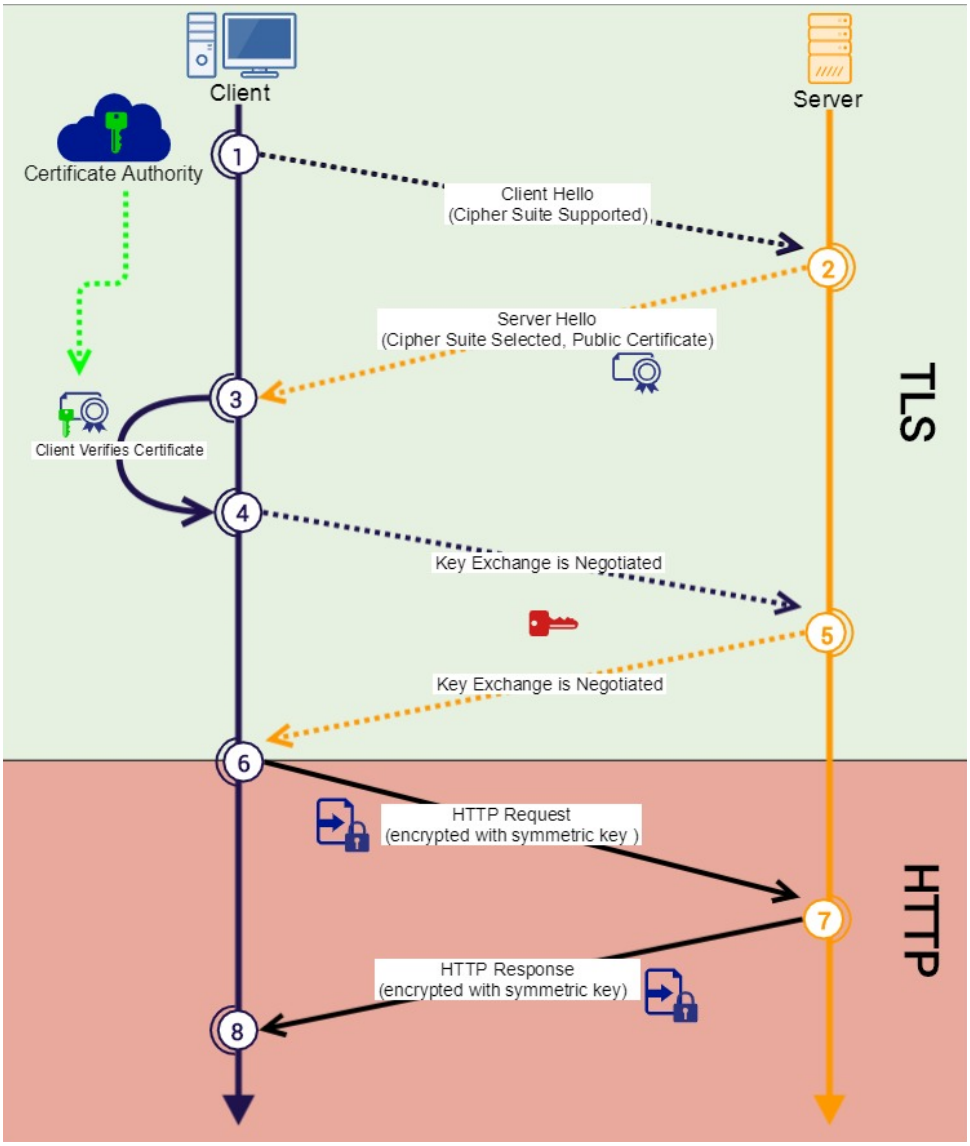

Web Security: Secure Socket Layer (SSL)
3 Verifies server.cer
Certificate Authority (CA)
Server.cer
Client.cer
5 Verifies client.cer
Server Keystore
Server.cer
1 Requests protected resource
2 Presents Server Certificate (server.cer)
4 Presents Client certificate (client.cer)
Client Keystore
Client.cer
6 Upon verification, accesses the protected resource
Krishnamurty Pammi


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

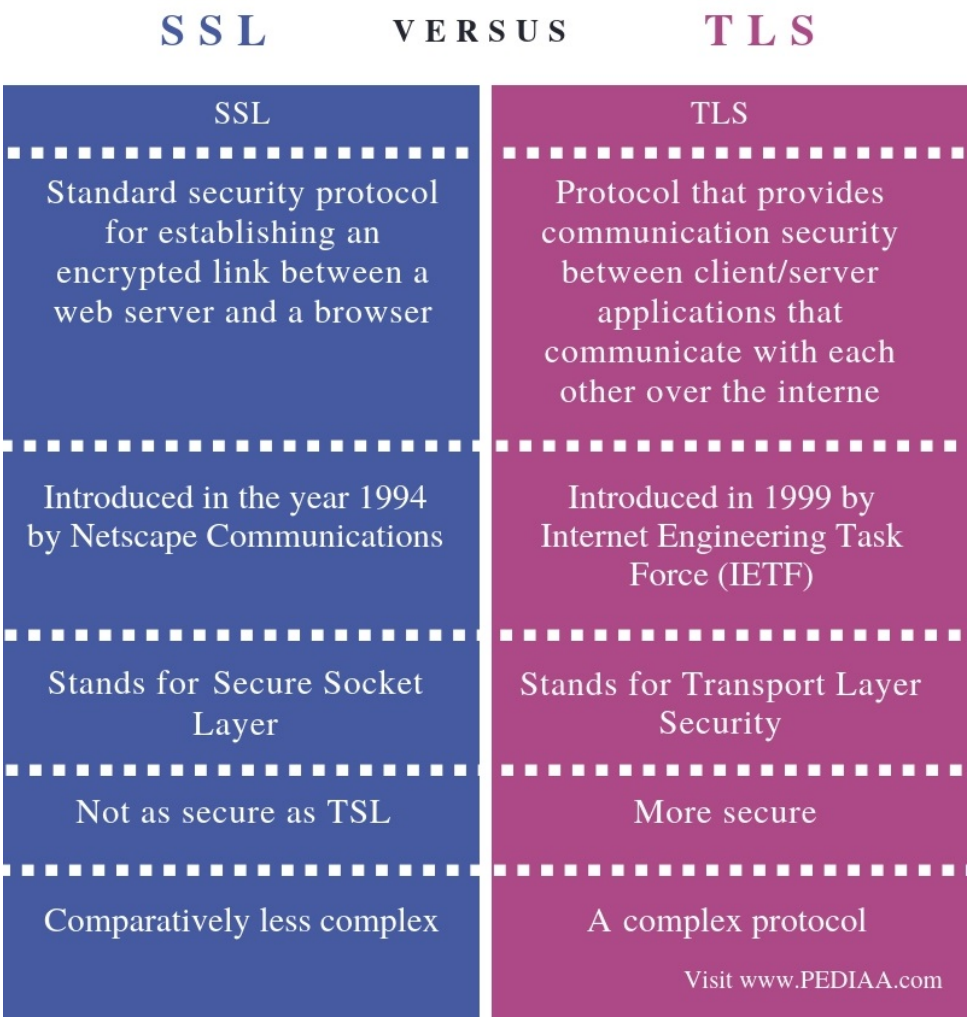

SSL/TLS VPNs vs. IPsec VPNs
SSL VPNs
Internet
SSL/TLS tunnel
Remote user with any browser
Firewall
SSL/TLS VPN gateway
Supported browser-based application 1
Supported browser-based application 2
IPsec
Corporate network
Internet
SSL/TLS tunnel
Remote user with IPsec client or remote site router
IPsec VPN/ firewall
Permitted subnet(s)


engineering.asu.edu
IPSec VPN vs. SSL VPN
Branch Office
Internet
Remote Office
HQ
Internet
Internet Kiosk
Mobile Users
Telecommuters
Partners, Customers, Contractors
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
Telecommuters
Mobile Users
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
ASU Ira A. Fulton Schools of Engineering
ARIZONA STATE UNIVERSITY

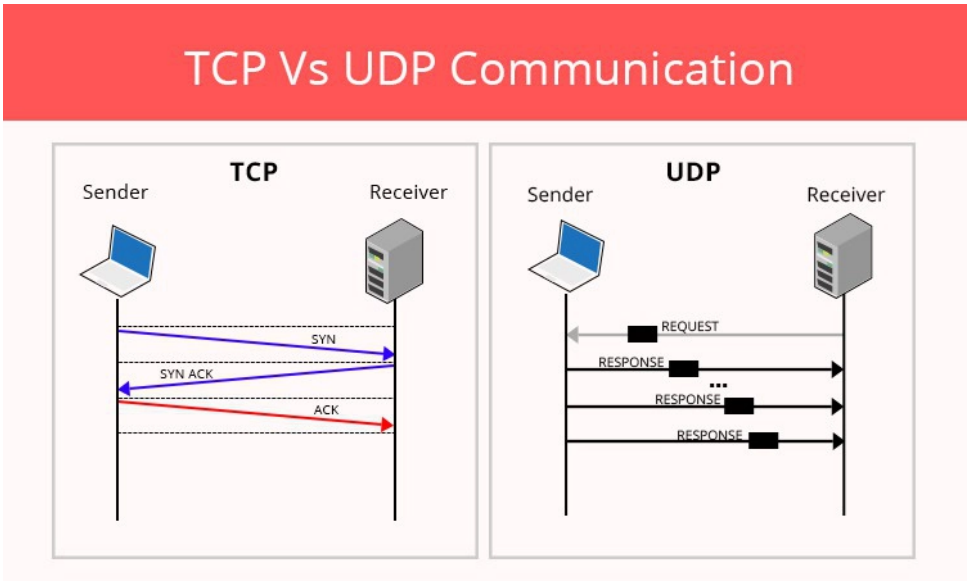
TLS

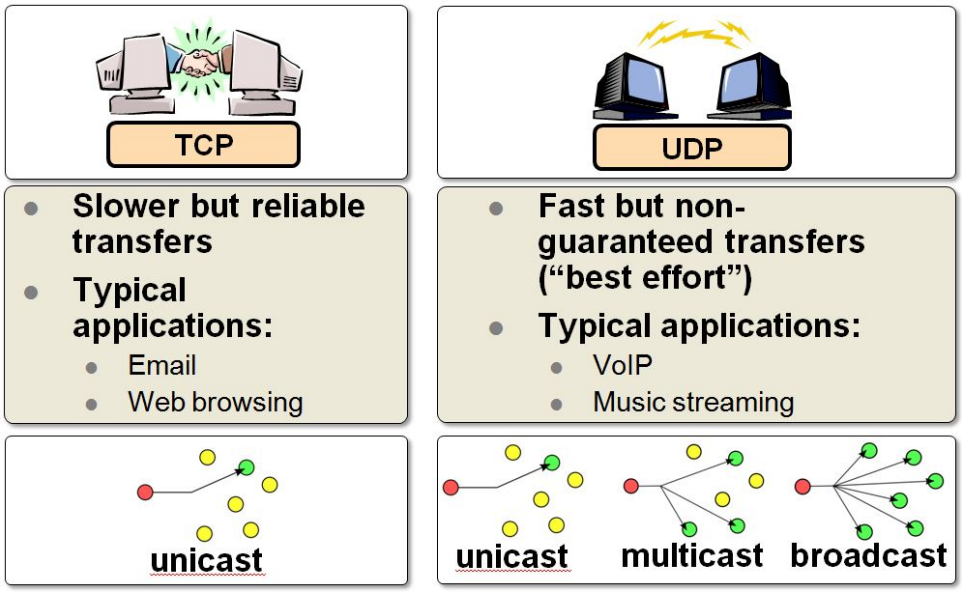

Client
Server
Certificate Authority
1
Client Hello
(Cipher Suite Supported)
2
Server Hello
(Cipher Suite Selected, Public Certificate)
3
Client Verifies Certificate
4
Key Exchange is Negotiated
5
Key Exchange is Negotiated
6
HTTP Request
(encrypted with symmetric key)
7
HTTP Response
(encrypted with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

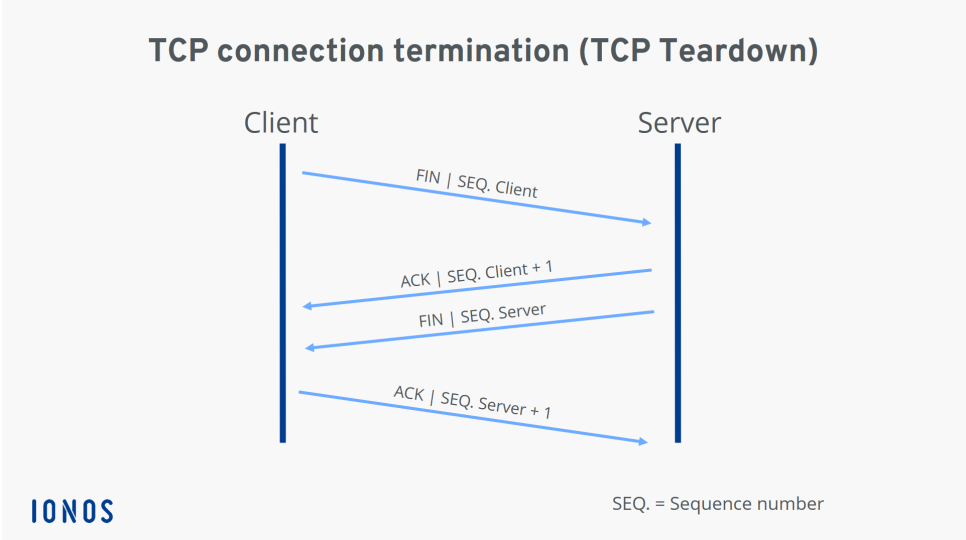
SSL vs TSL



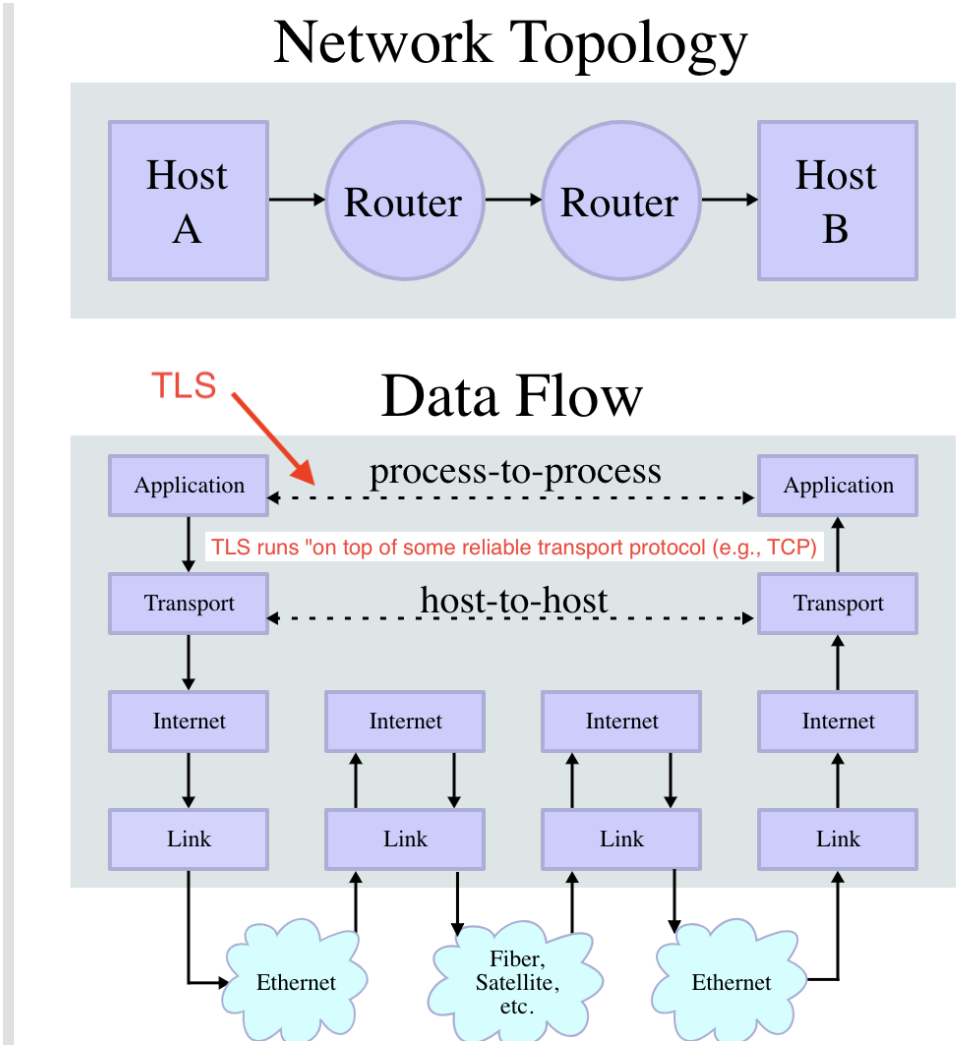
Network Layer - TCP vs UDP



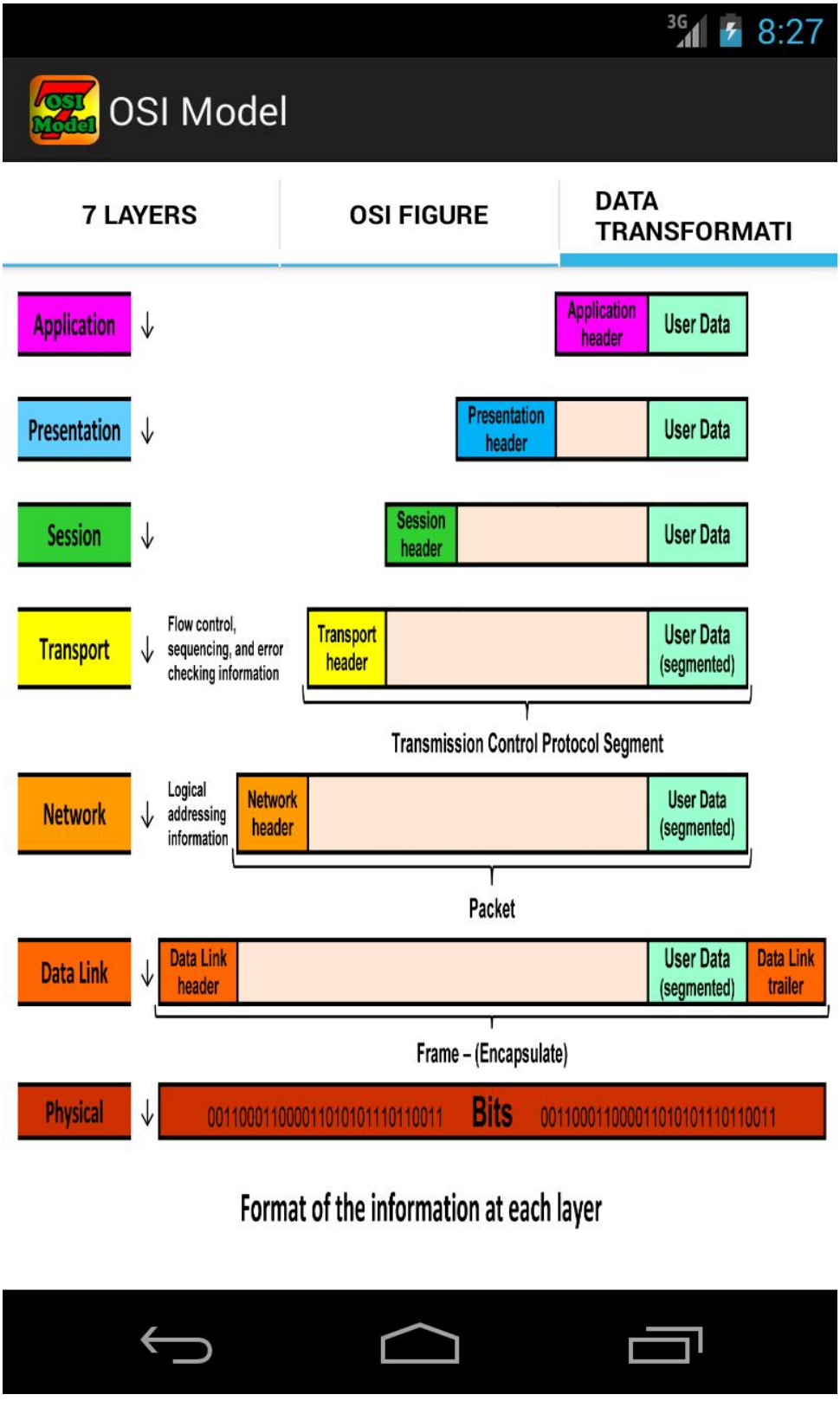

TCP
Slower but reliable transfers
Typical applications:
Email
Web browsing
unicast
UDP
Fast but non-guaranteed transfers ("best effort")
Typical applications:
VoIP
Music streaming
unicast
multicast
broadcast

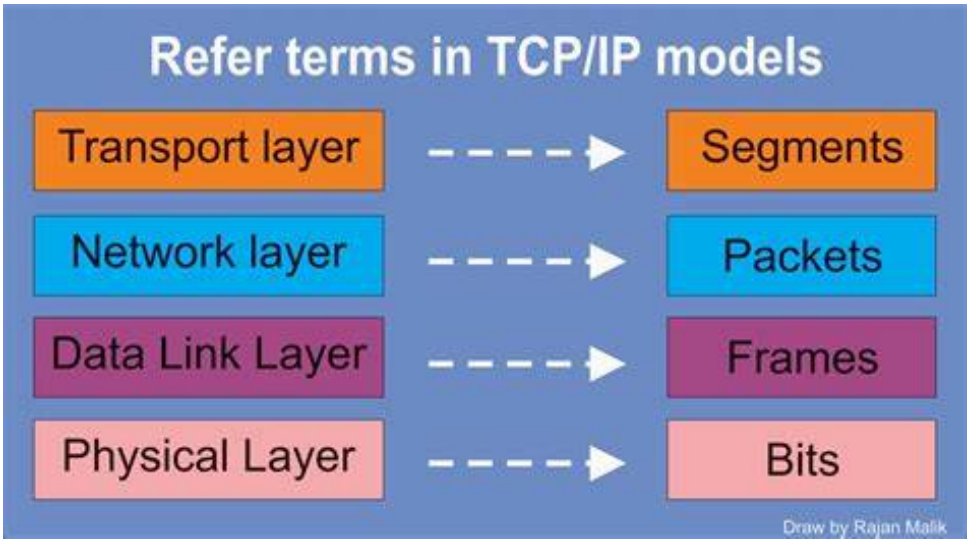

TCP connection termination (TCP Teardown)
Client
Server
FIN | SEQ. Client
ACK | SEQ. Client + 1
FIN | SEQ. Server
ACK | SEQ. Server + 1
IONOS
SEQ. = Sequence number

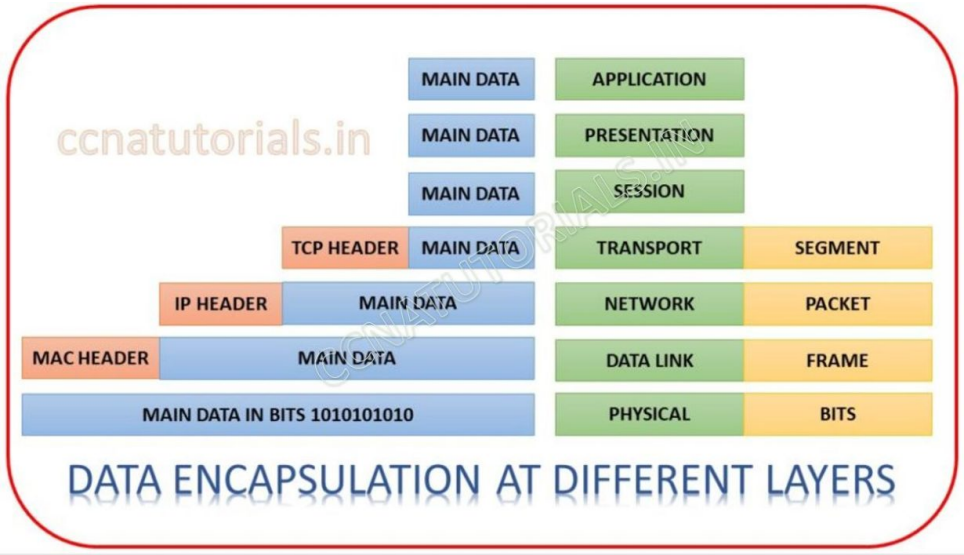
Data Flow

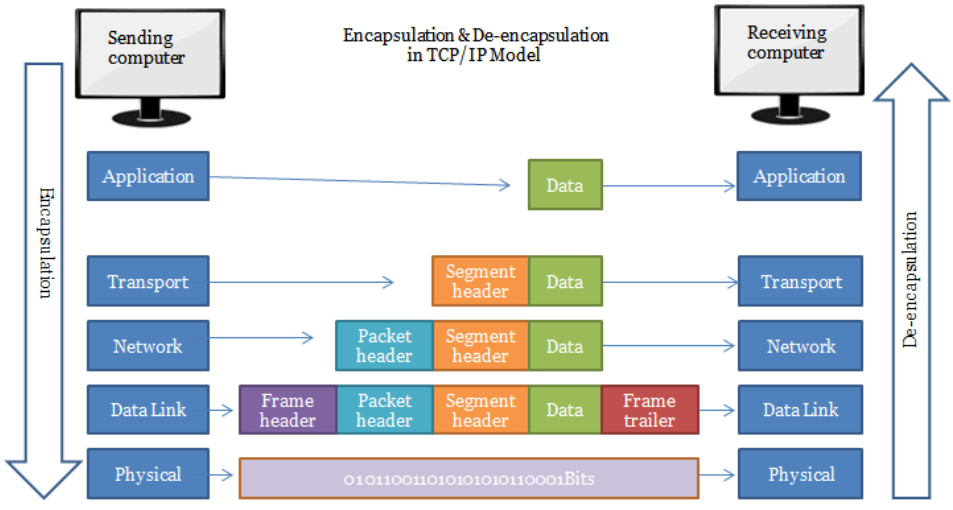


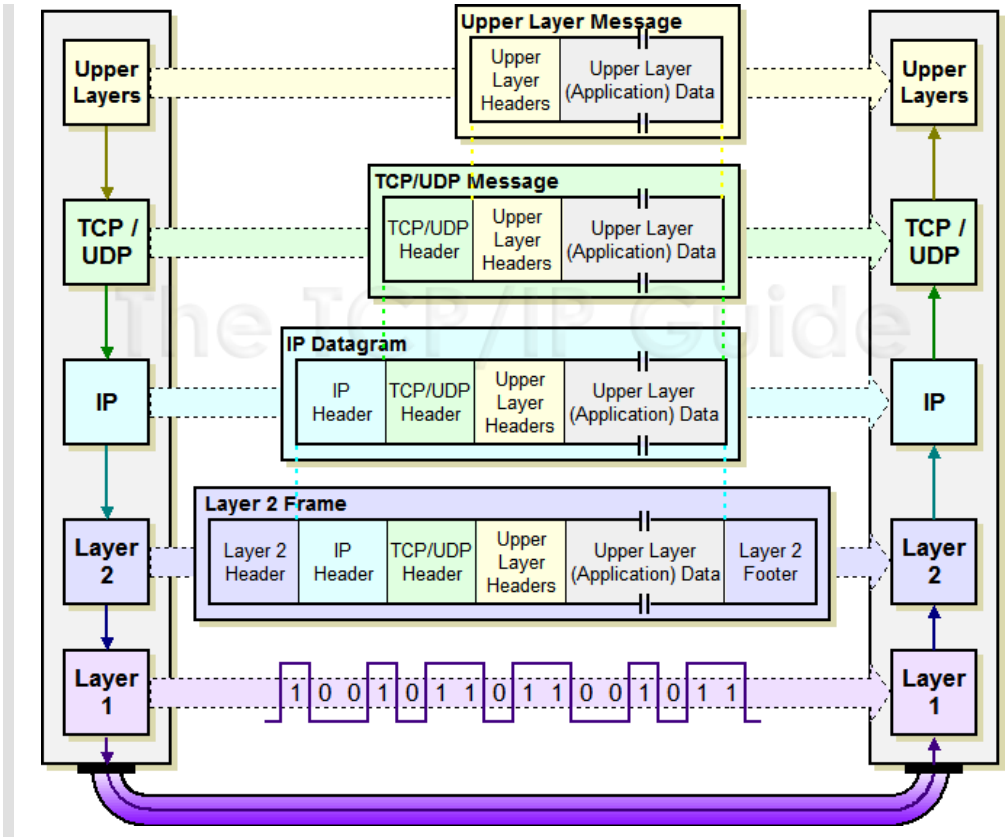
Encapsulation

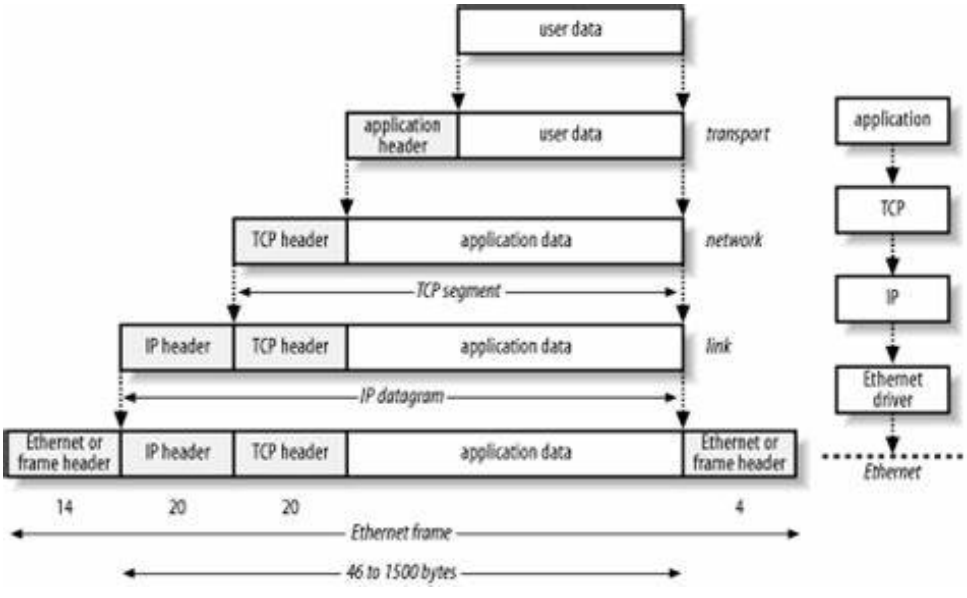

8:27
OSI Model
7 LAYERS
OSI FIGURE
DATA TRANSFORMATI
Application
Application header
User Data
Presentation
Presentation header
User Data
Session
Session header
User Data
Transport
Flow control, sequencing, and error checking information
Transport header
User Data (segmented)
Transmission Control Protocol Segment
Network
Logical addressing information
Network header
User Data (segmented)
Packet
Data Link
Data Link header
User Data (segmented)
Data Link trailer
Frame – (Encapsulate)
Physical
00110001100001101010111010011 Bits 00110001100001101010111010011
Format of the information at each layer

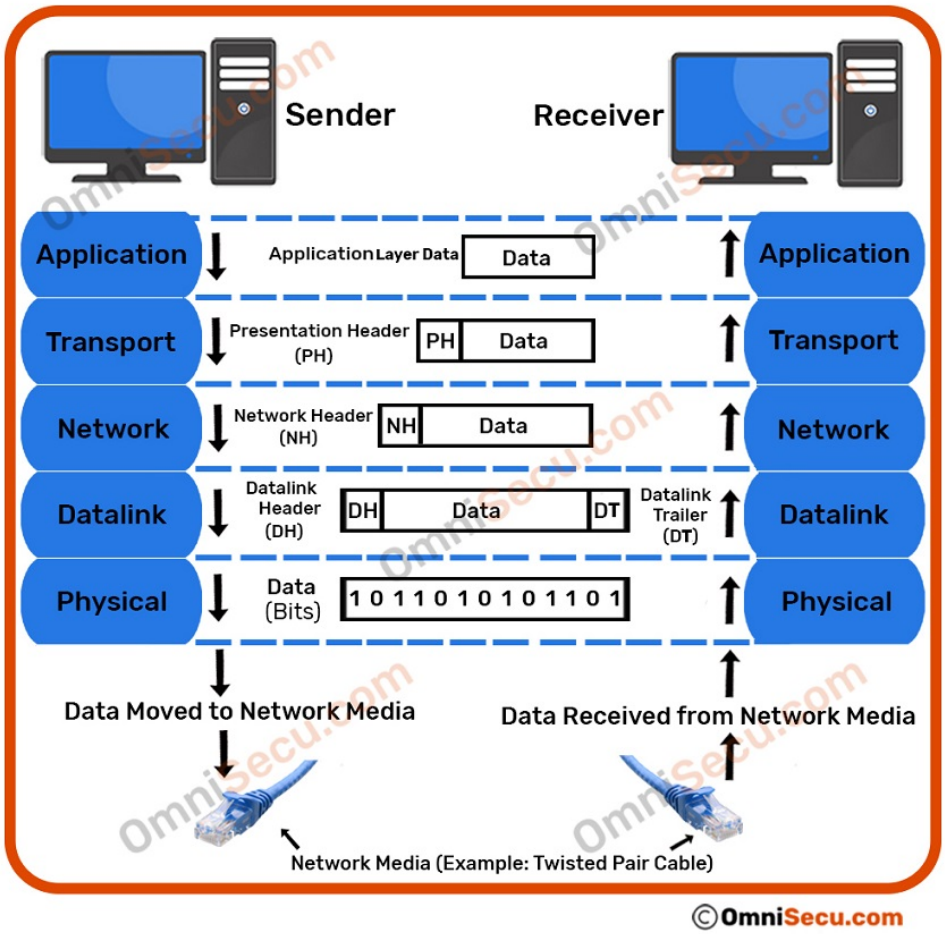

Refer terms in TCP/IP models
Transport layer
Segments
Network layer
Packets
Data Link Layer
Frames
Physical Layer
Bits
Draw by Rajan Malik


ccnatutorials.in
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

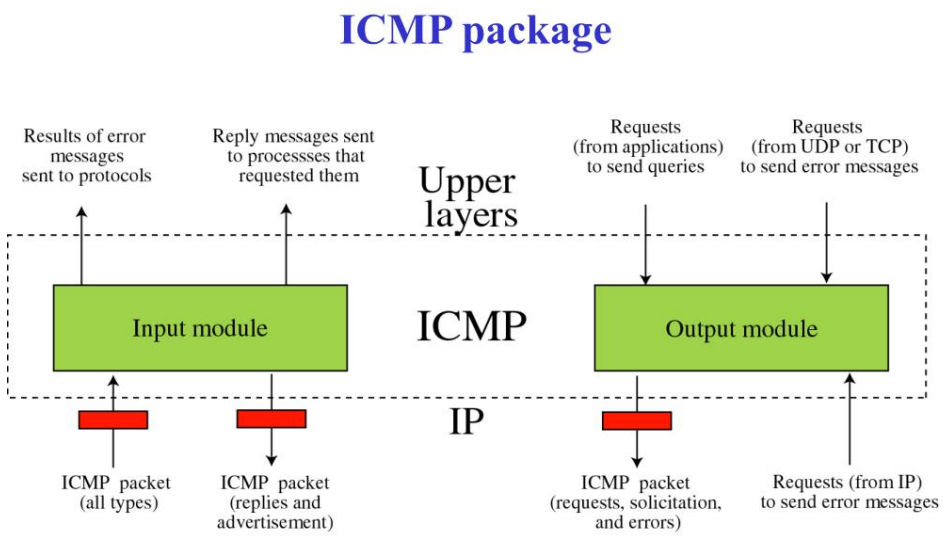

Sending computer
Encapsulation & De-encapsulation in TCP/IP Model
Receiving computer
Encapsulation
De-encapsulation
Application
Data
Application
Transport
Segment header
Data
Transport
Network
Packet header
Segment header
Data
Network
Data Link
Frame header
Packet header
Segment header
Data
Frame trailer
Data Link
Physical
0101100110101010101100001Bits
Physical


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
IP Datagram
IP Header
Layer 2 Frame
Layer 2 Header
Layer 2 Footer
1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 1


user data
application header
transport
TCP header
application data
network
TCP segment
IP header
link
IP datagram
Ethernet or frame header
14
20
20
4
Ethernet frame
46 to 1500 bytes
application
TCP
IP
Ethernet driver
Ethernet

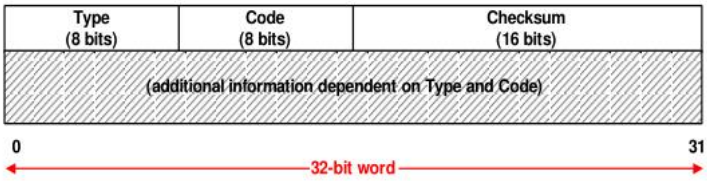

Sender
Receiver
Application
Transport
Network
Datalink
Physical
Application Layer Data
Data
Presentation Header (PH)
PH
Data
Network Header (NH)
NH
Data
Datalink Header (DH)
DH
Data
DT
Datalink Trailer (DT)
Data (Bits)
1 0 1 1 0 1 0 1 0 1 1 0 1
Data Moved to Network Media
Data Received from Network Media
Network Media (Example: Twisted Pair Cable)
©OmniSecu.com

ICMP vs IGMP


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

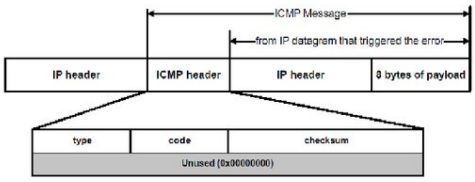
ICMP: A helper protocol to IP

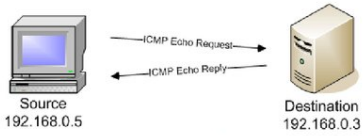
- The **Internet Control Message Protocol (ICMP)** is the protocol used for error and control messages in the Internet.
- ICMP provides an error reporting mechanism of routers to the sources.
- All ICMP packets are encapsulated as IP datagrams.
- The packet format is simple:



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)





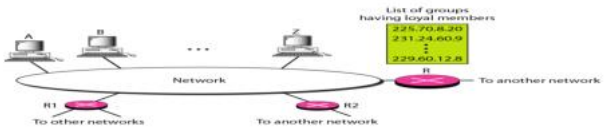
The host must respond to all echo requests with an echo reply containing the exact data received in the request message

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.

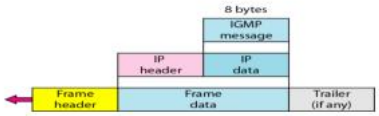
•For each group, there is one router that has the duty of distributing the multicast packets destined for that group.

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



IGMP: Encapsulation at Network Layer

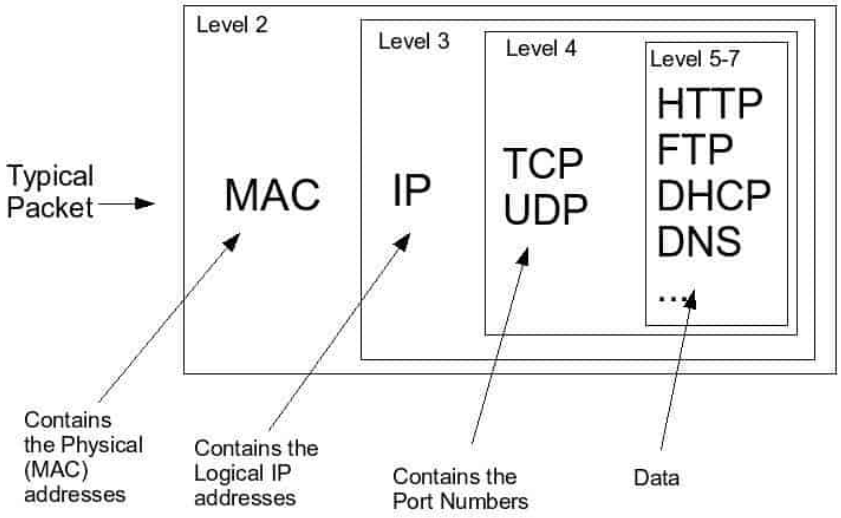
- The IGMP message is encapsulated in an IP datagram, which is itself encapsulated in a frame.



- 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

Packet

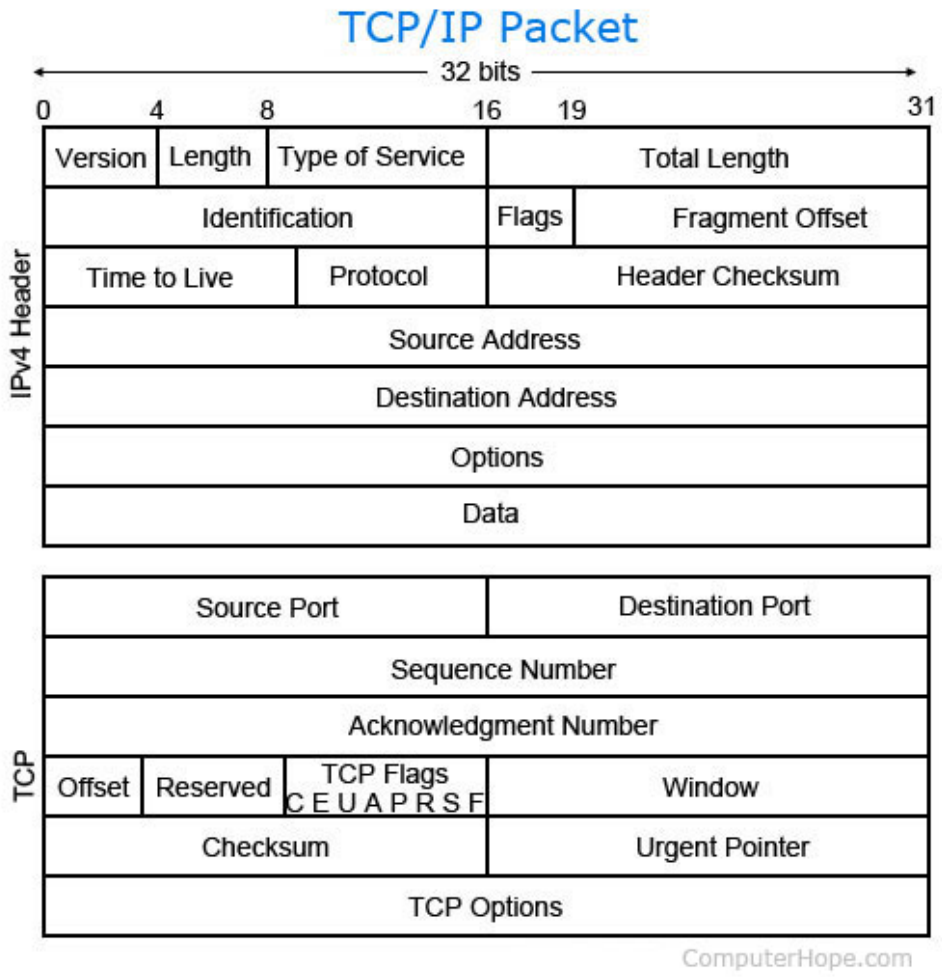


IP Packet Format

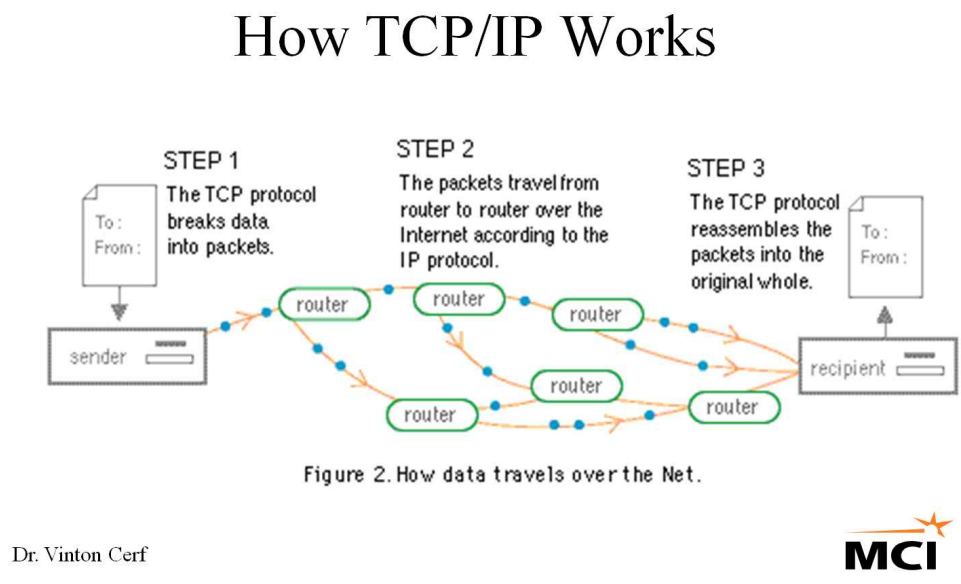
Bit 0 IPv4 Packet Header Format Bit 31

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 And Application Data			

Typical Header Length = 5 (32 bit words)



Packet Switch



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

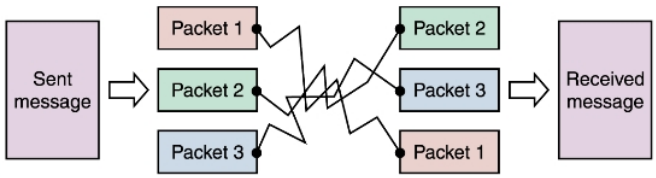
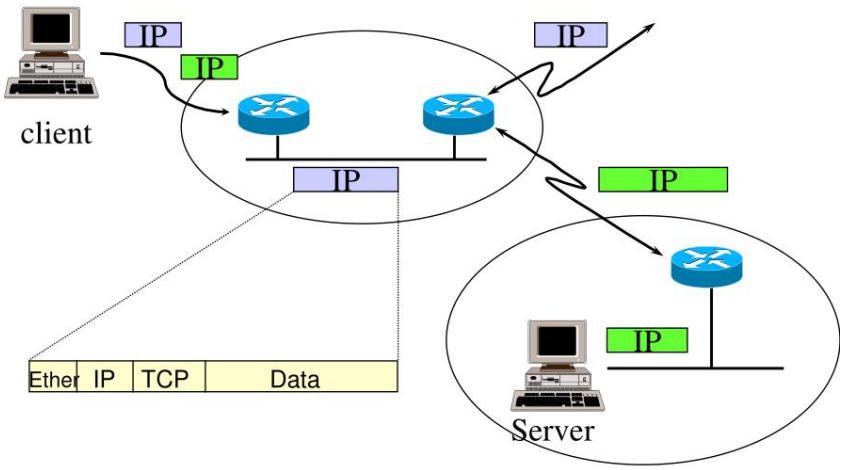


Figure 15.4 Messages sent by packet switching

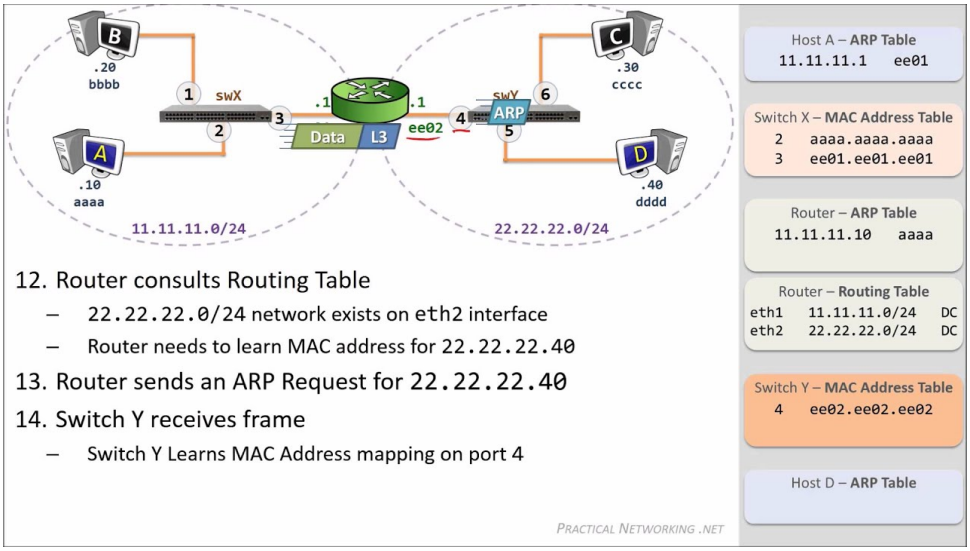
Message is divided into packets | Packets are sent over the Internet by the most expedient route | Packets are reordered and then reassembled

Packet Switch Network



ARP(Address Resolution Protocl) / RARP (ReverseAddress Resolution Protocl)

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



IP4 vs IP6

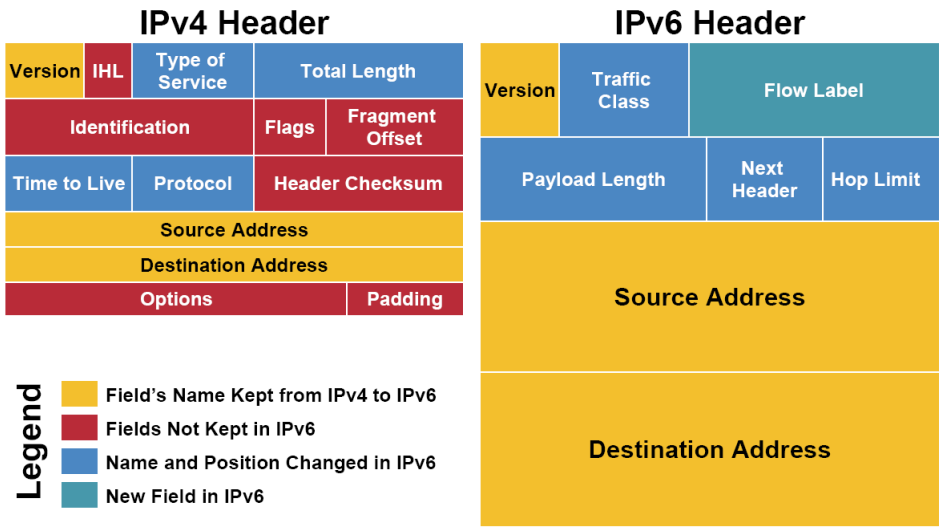
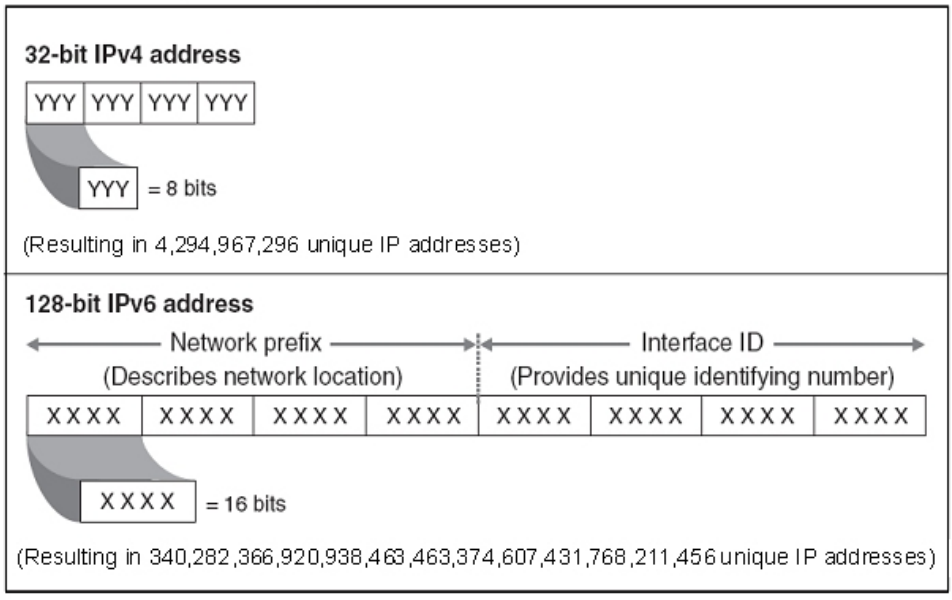


Figure 1: Comparison of IPv6 and IPv4 Address Scheme



Source: GAO.

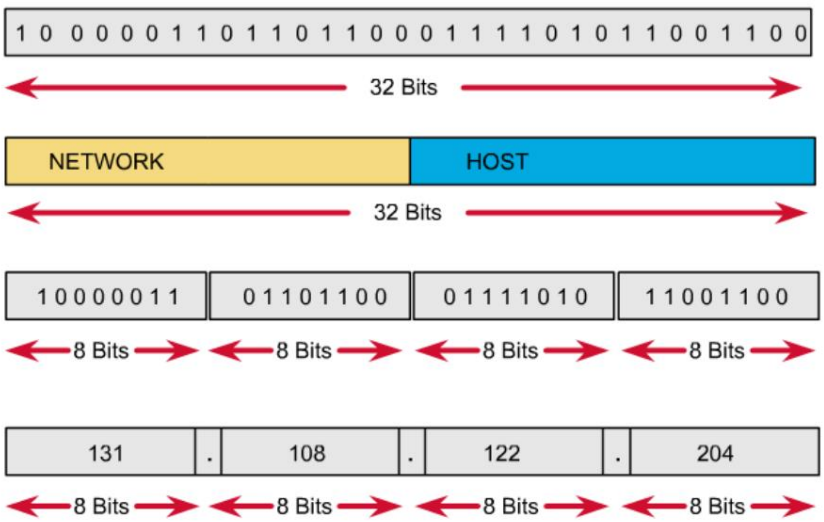
Differences Between IPv4 and IPv6

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

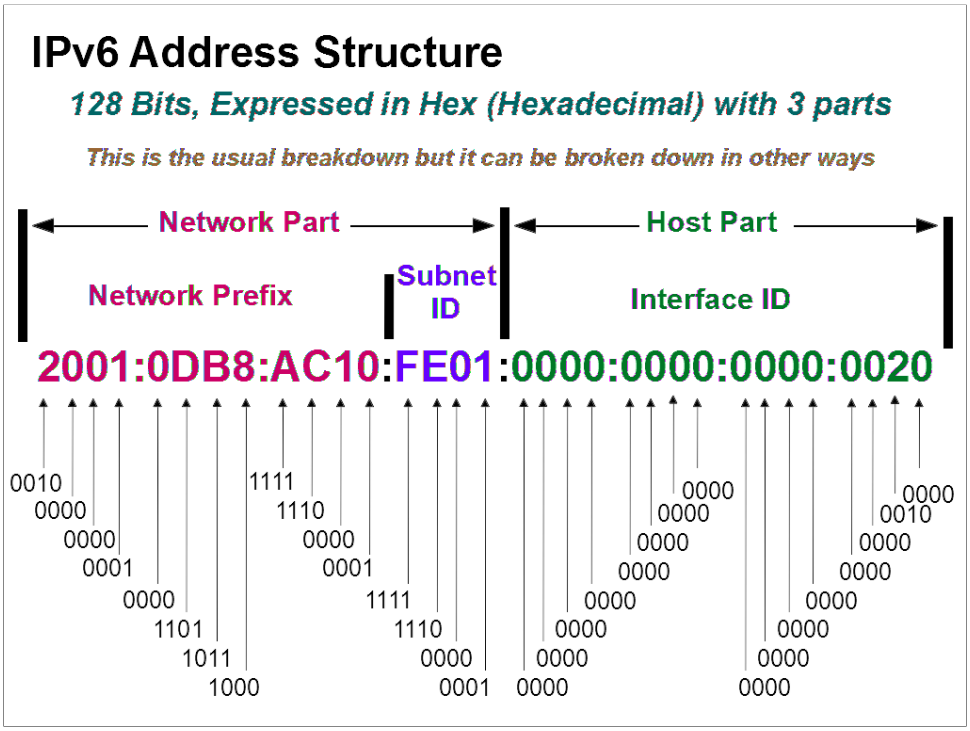
IPv4/IPv6 Differences

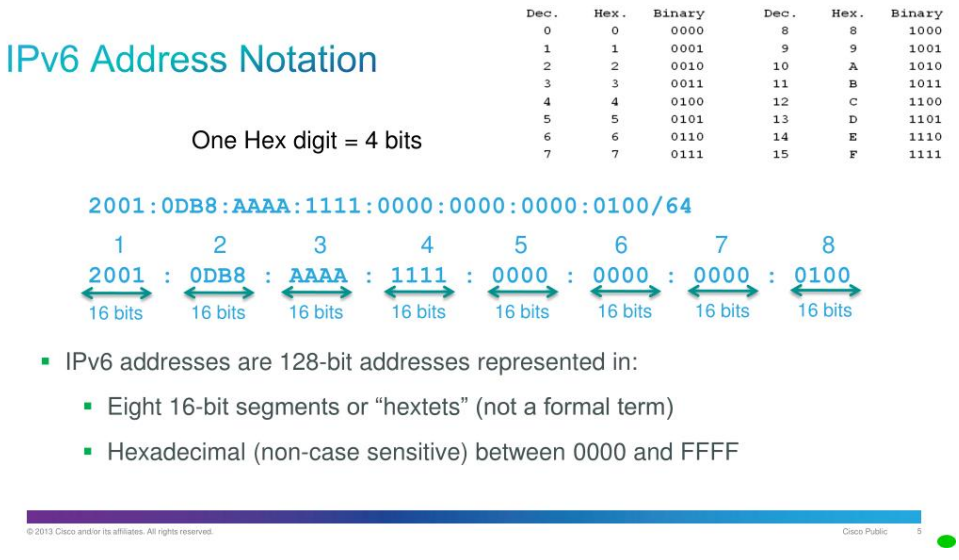
	IPv4	IPv6
Address	32 bits (4 bytes) 12:34:56:78	128 bits (16 bytes) 1234:5678:9abc:def0:1234:5678:9abc:def0
Packet size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet fragmentation	Routers and sending hosts	Sending hosts only
Packet header	Does not identify 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

IP Address



Class	Private Address Ranges
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255
Loopback	127.0.0.0 – 127.255.255.255 (127.0.0.1)


IPv6 Address Structure
128 Bits, Expressed in Hex (Hexadecimal) with 3 parts
This is the usual breakdown but it can be broken down in other ways
Network Part
Host Part
Network Prefix
Subnet ID
Interface ID
2001:0DB8:AC10:FE01:0000:0000:0000:0020
0010 0000 0000 0001 0000 1101 1011 1000
1111 1110 0000 0001 1111 1110 0000 0001
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0010 0000 0000 0000 0000 0000 0000


IPv6 Address Notation
One Hex digit = 4 bits
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
2001:0DB8:AAAA:1111:0000:0000:0000:0100/64
1 2 3 4 5 6 7 8
2001 : 0DB8 : AAAA : 1111 : 0000 : 0000 : 0000 : 0100
16 bits 16 bits 16 bits 16 bits 16 bits 16 bits 16 bits 16 bits
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
© 2013 Cisco and/or its affiliates. All rights reserved.
Cisco Public 5

IP Range

Global Addresses

Class	First Octet value	Range	No. of Network	No. of Hosts / Network
A	00000000 – 01111111 (0 – 127)	1.0.0.1 – 126.255.255.254	126	2^{24} - 2
B	10000000 – 10111111 (128 – 191)	128.1.0.1 – 191.255.255.254	16000	65000
C	11000000 – 11011111 (192 – 223)	192.0.1.1 – 223.255.255.254	2 Million	254
D	11100000 – 11101111 (224 – 239)	224.0.0.0 – 239.255.255.255	Multicast addresses	
E	11110000 – 11111111 (240 – 255)	240.0.0.0 – 254.255.255.254	Future use	

In class **A 127.0.0.1 – 127.255.255.255** addresses are reserved for loopback & diagnostic purpose.

IP Address Ranges

IP Address Class	First Octet Binary Value	First Octet Decimal Value	Possible Number of Hosts
Class A	1-126	00000001 to 01111110*	16,777,214
Class B	128-191	10000000 to 10111111	65,534
Class C	192-223	11000000 to 11011111	254

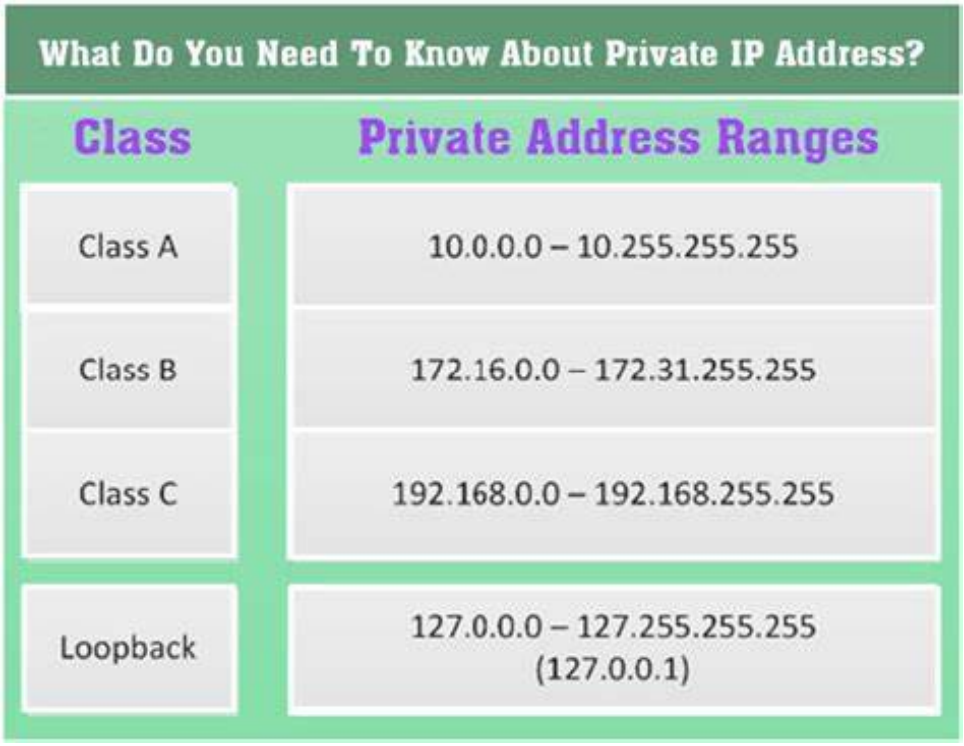
***127 (011111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.**

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

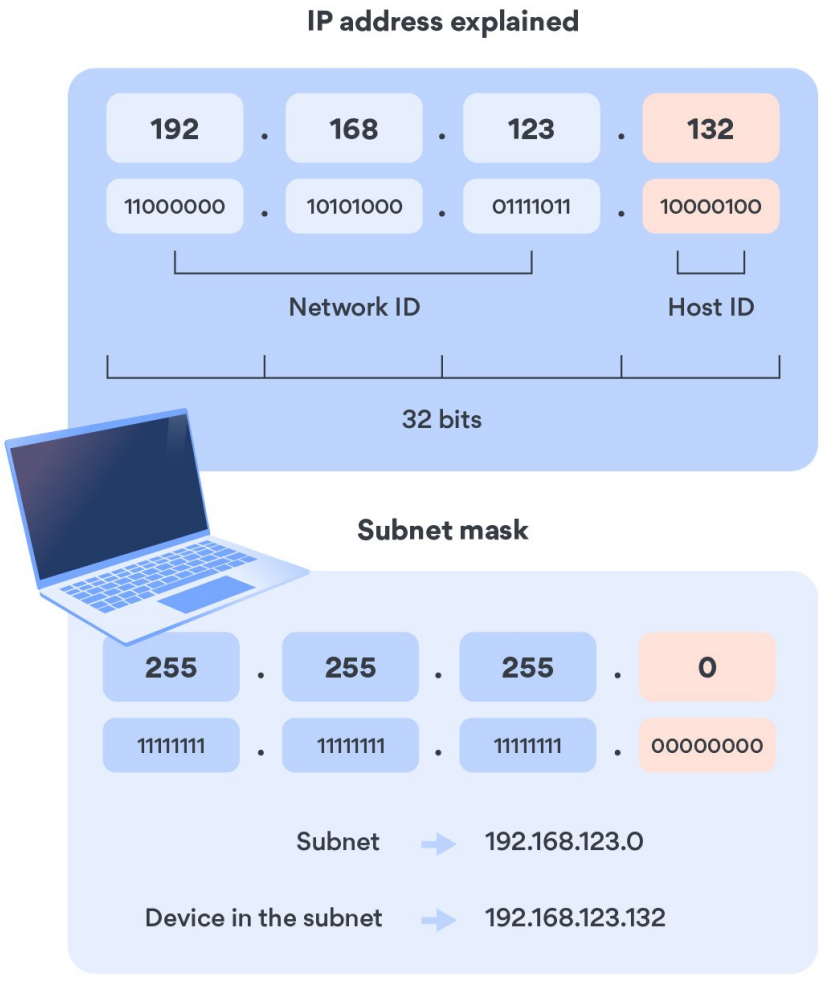
- example:
  - 192.168.1.0/24 (mask: 255.255.255.0 | 256 hosts) - 256 networks
  - 172.17.0.0/16 (mask: 255.255.0.0 | 65.536 hosts) 256 networks

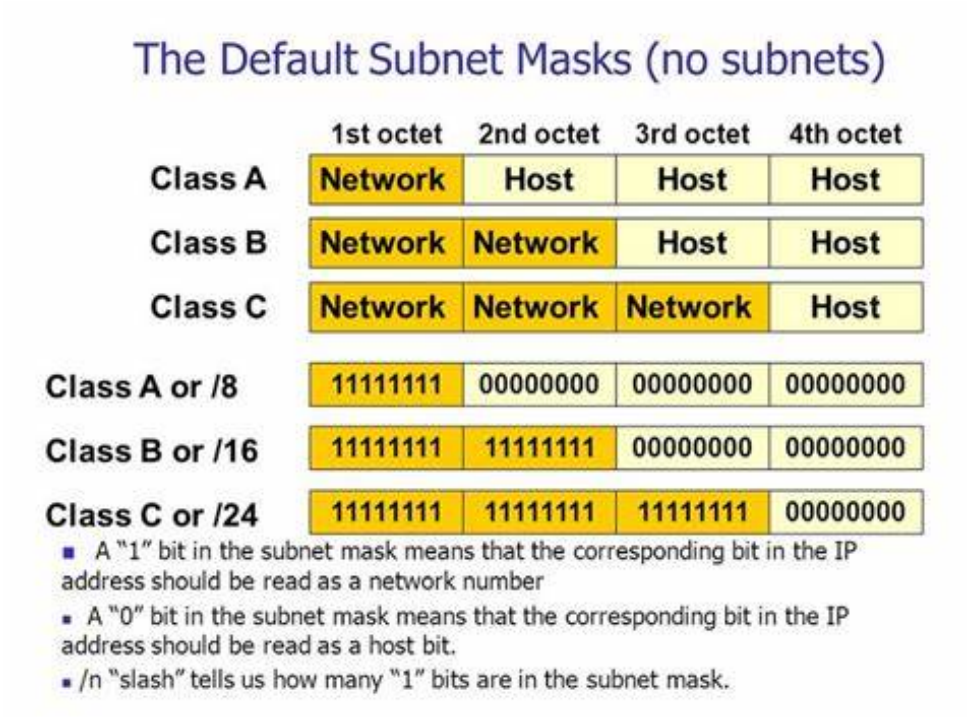


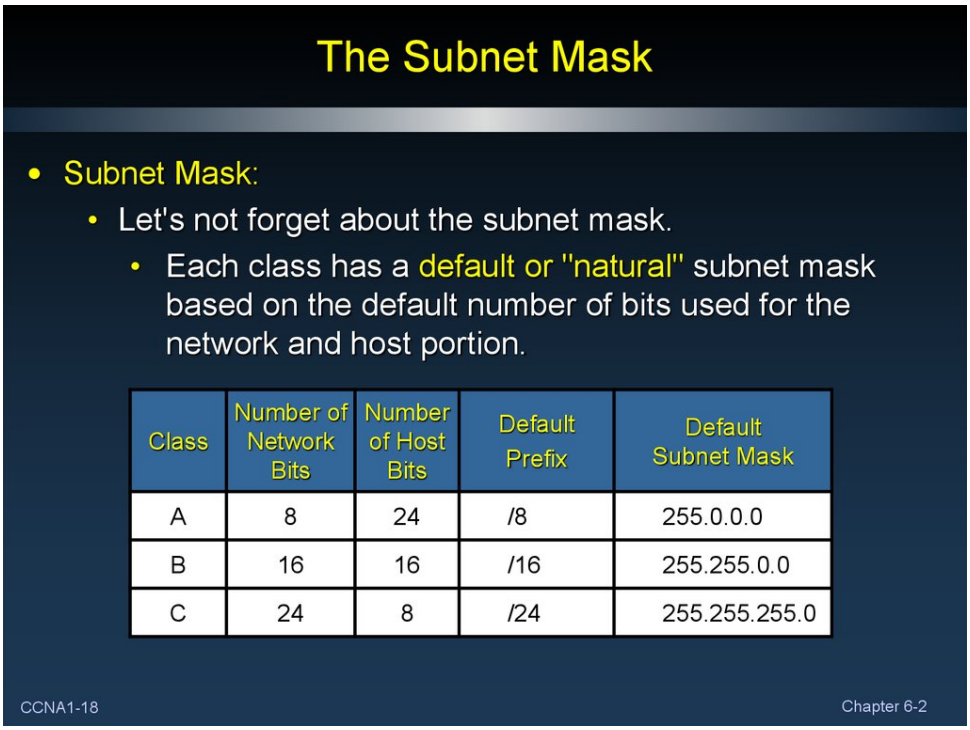
Subnet Mask

Subnet Mask

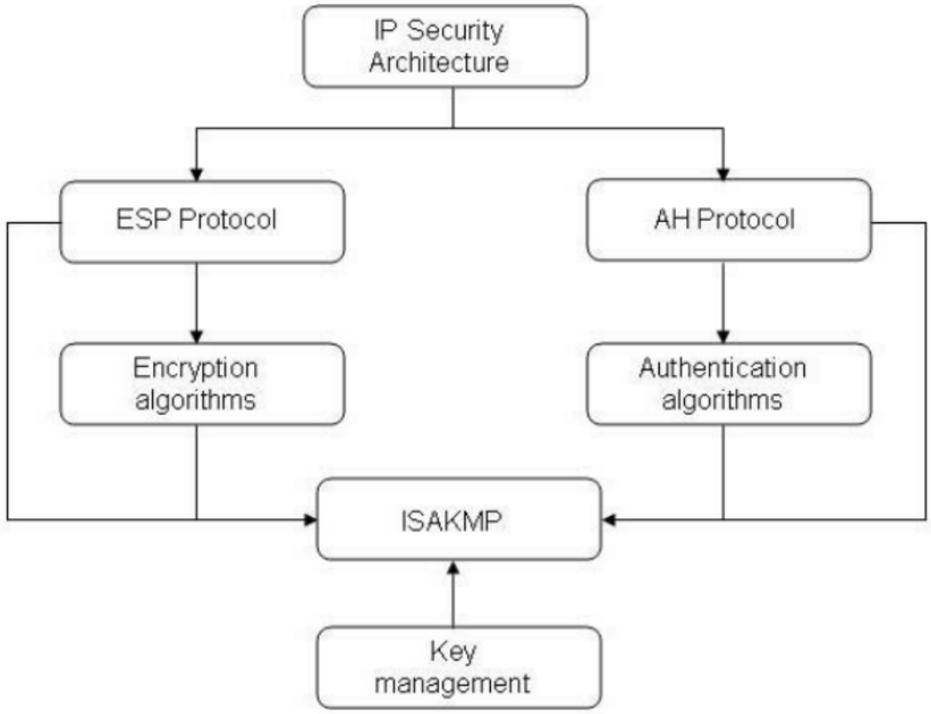
Suffix	Hosts	32-Borrowed=CIDR	2^Borrowed = Hosts	Binary=> dec = Suffix
.255	1	/32	0	11111111
.254	2	/31	1	11111110
.252	4	/30	2	11111100
.248	8	/29	3	11111000
.240	16	/28	4	11110000
.224	32	/27	5	11100000
.192	64	/26	6	11000000
.128	128	/25	7	10000000

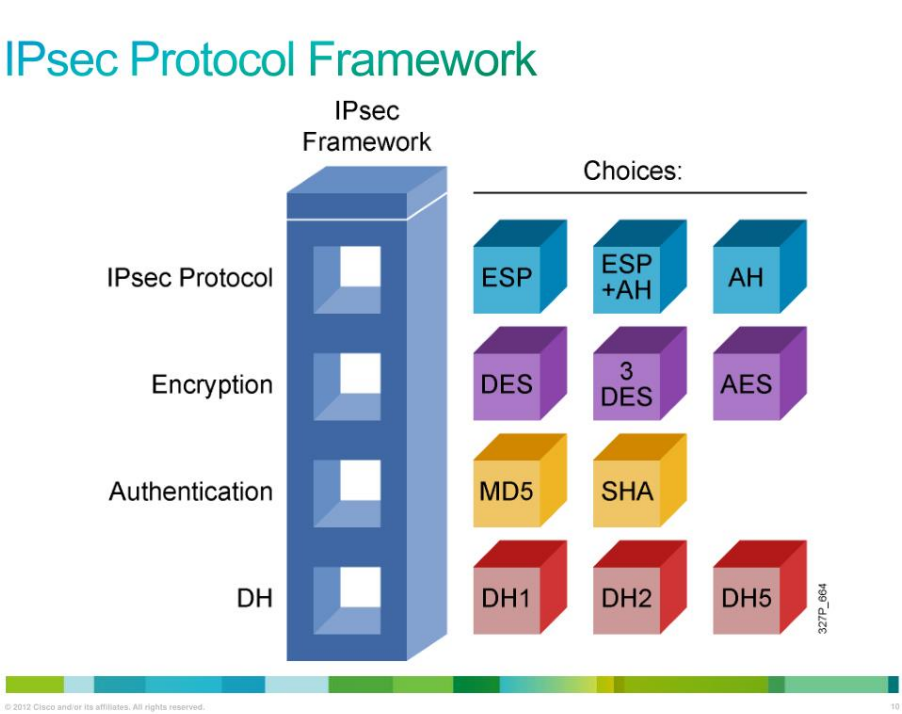


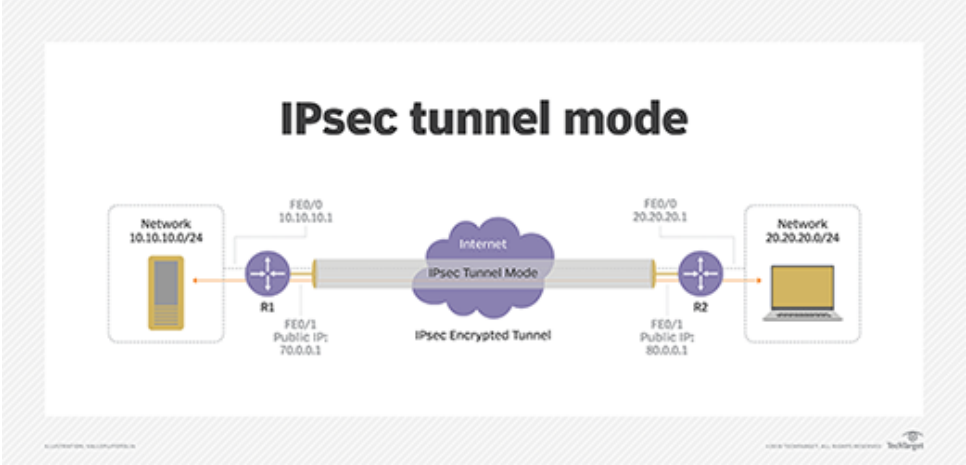

The Default Subnet Masks (no subnets)
1st octet
2nd octet
3rd octet
4th octet
Class A
Network
Host
Host
Host
Class B
Network
Network
Host
Host
Class C
Network
Network
Network
Host
Class A or /8
11111111
00000000
00000000
00000000
Class B or /16
11111111
11111111
00000000
00000000
Class C or /24
11111111
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.

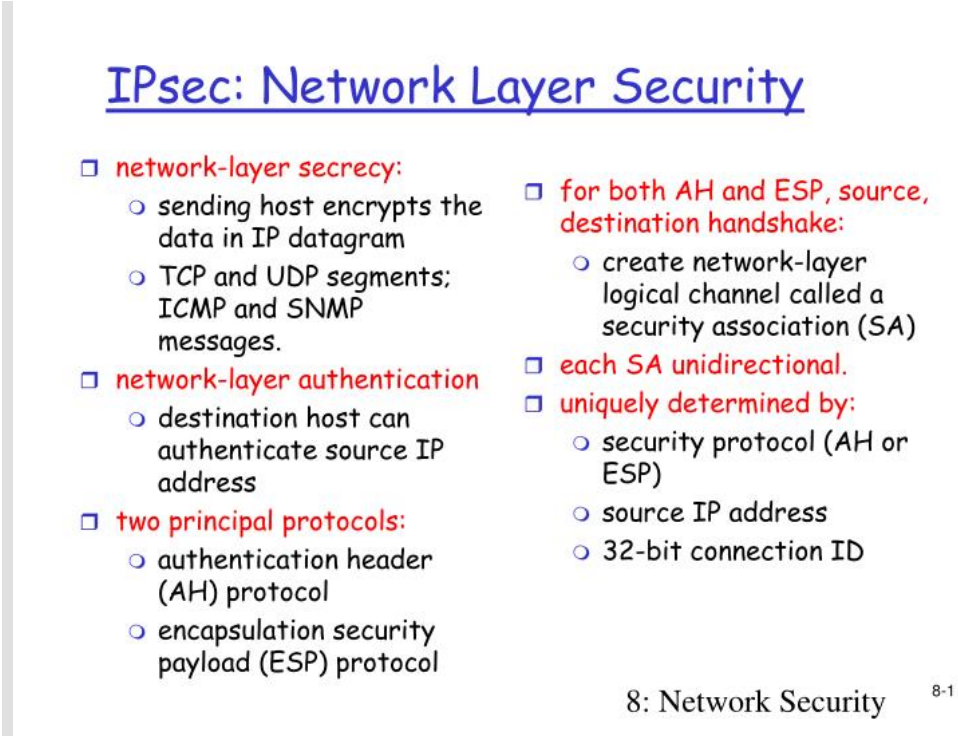

The Subnet Mask
Subnet Mask:
Let's not forget about the subnet mask.
Each class has a default or "natural" subnet mask based on the default number of bits used for the network and host portion.
Class
Number of Network Bits
Number of Host Bits
Default Prefix
Default Subnet Mask
A
8
24
/8
255.0.0.0
B
16
16
/16
255.255.0.0
C
24
8
/24
255.255.255.0
CCNA1-18
Chapter 6-2

IPSec


IP Security Architecture
ESP Protocol
AH Protocol
Encryption algorithms
Authentication algorithms
ISAKMP
Key management


IPsec Protocol Framework
IPsec Framework
Choices:
IPsec Protocol
Encryption
Authentication
DH
ESP
ESP +AH
AH
DES
3 DES
AES
MD5
SHA
DH1
DH2
DH5
327P_864
© 2012 Cisco and/or its affiliates. All rights reserved.
10


IPsec tunnel mode
Network 10.10.10.0/24
FE0/0 10.10.10.1
R1
FE0/1 Public IP: 70.0.0.1
Internet
IPsec Tunnel Mode
IPsec Encrypted Tunnel
FE0/0 20.20.20.1
R2
FE0/1 Public IP: 80.0.0.1
Network 20.20.20.0/24



IPsec: Network Layer Security

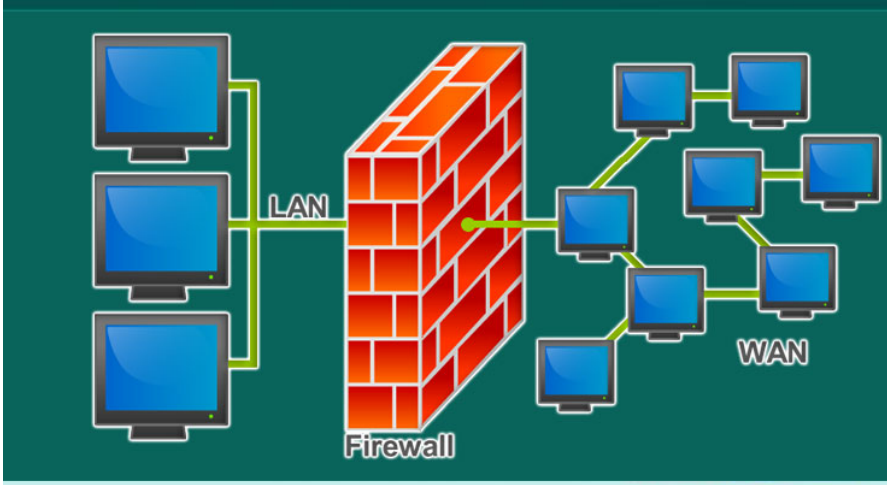
- network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages.
- network-layer authentication
  - destination host can authenticate source IP address
- two principal protocols:
  - authentication header (AH) protocol
  - encapsulation security 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

Network Equipment

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.

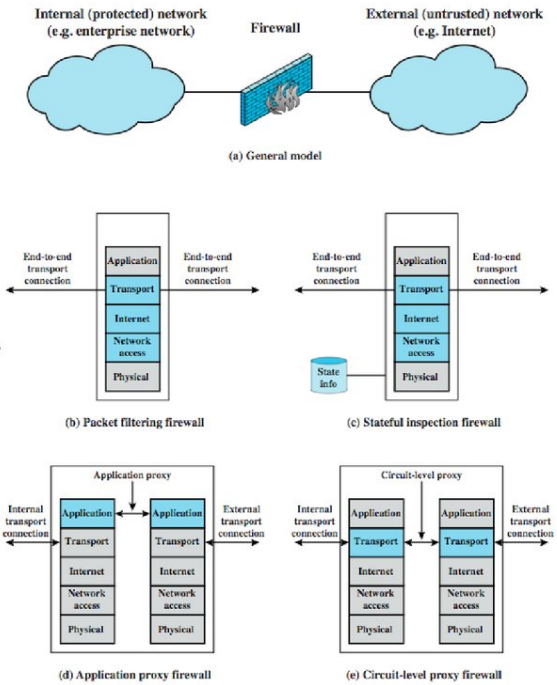
It simply prevents unauthorized access to or from a private network. Used to enhance the security of computers connected to a network, such as LAN or the Internet. Considered as an integral part of a comprehensive security framework for your network.

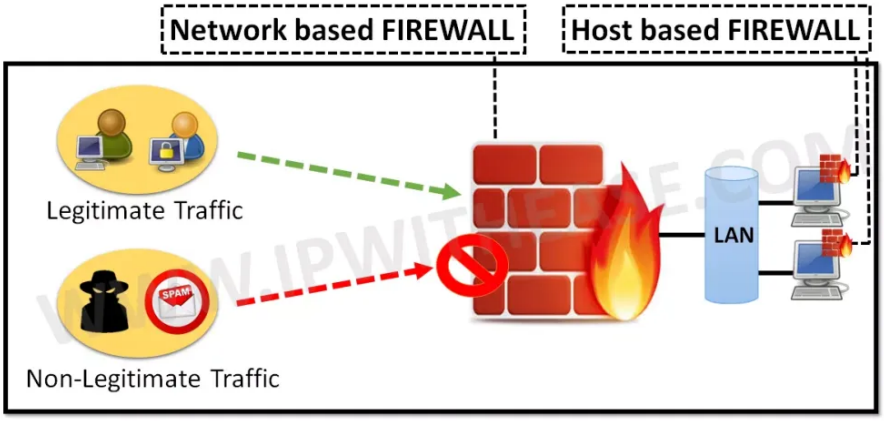
WiZXPERT

Types of Firewalls

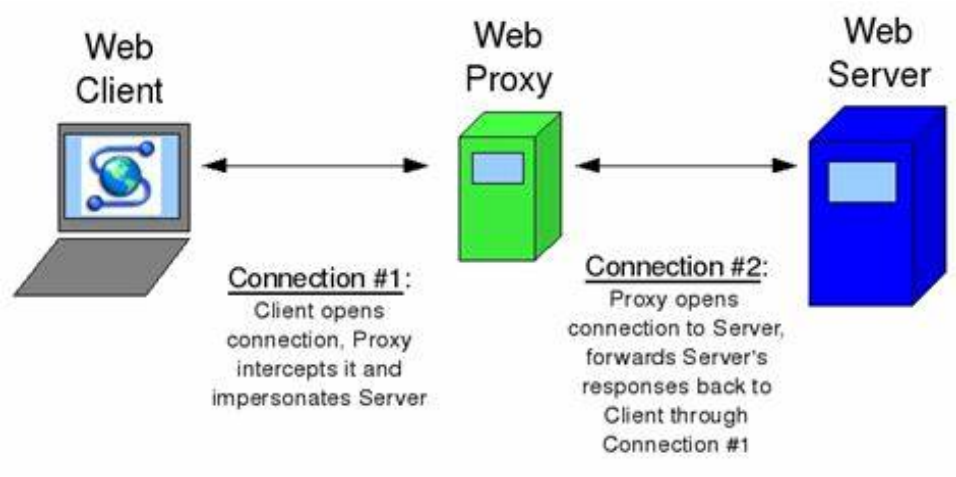
Positive (negative) filter: Allow (reject) packets that meet a criteria

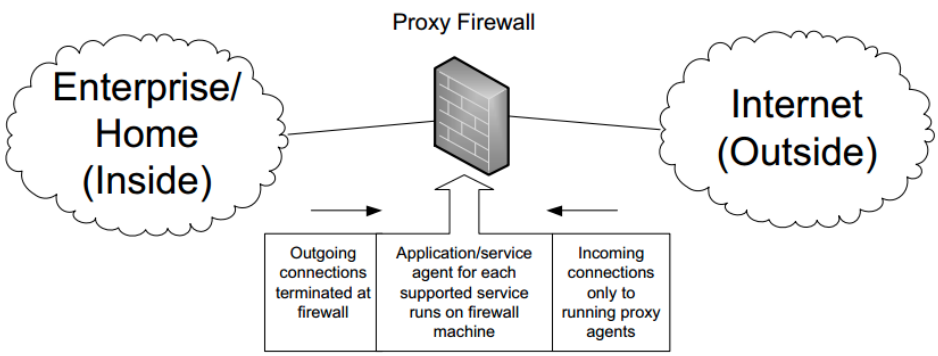
Stateful inspection: Keeps track of TCP connections





Proxy





Proxy Cache

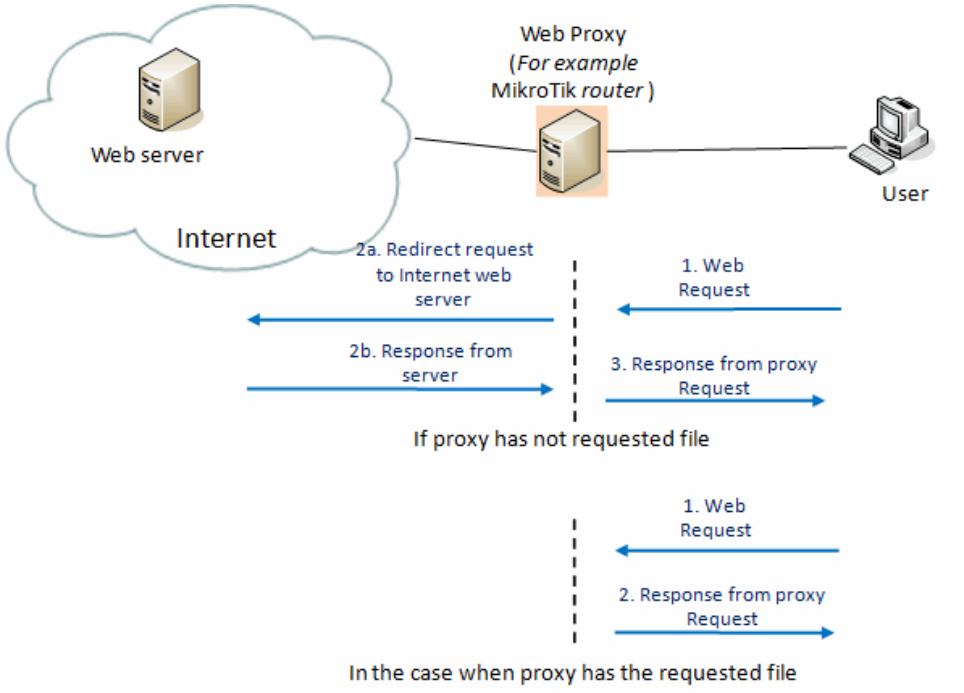
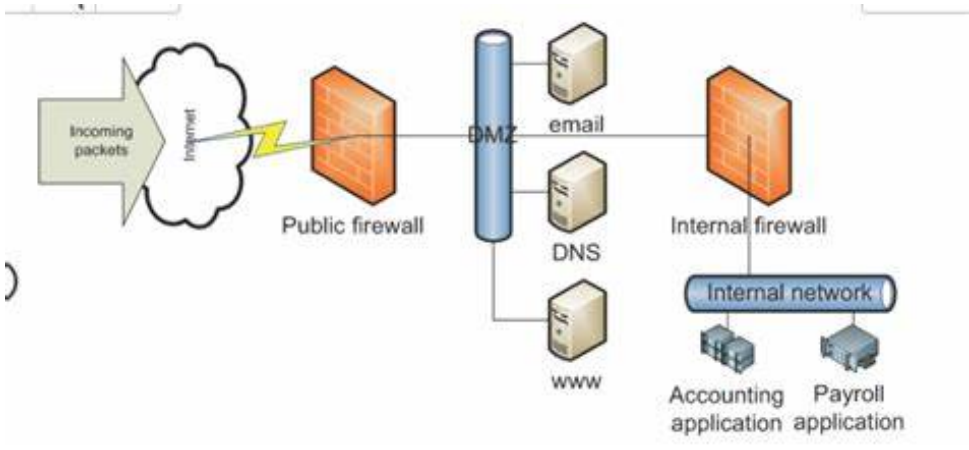


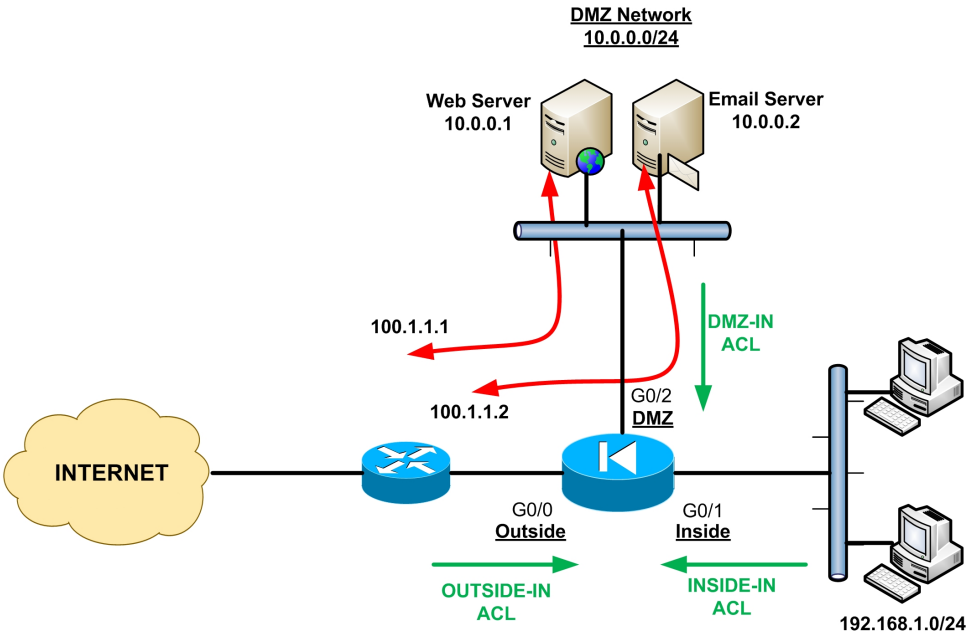
Figure 10.1. Web proxy basic operation scheme

ACL (Access Control List)

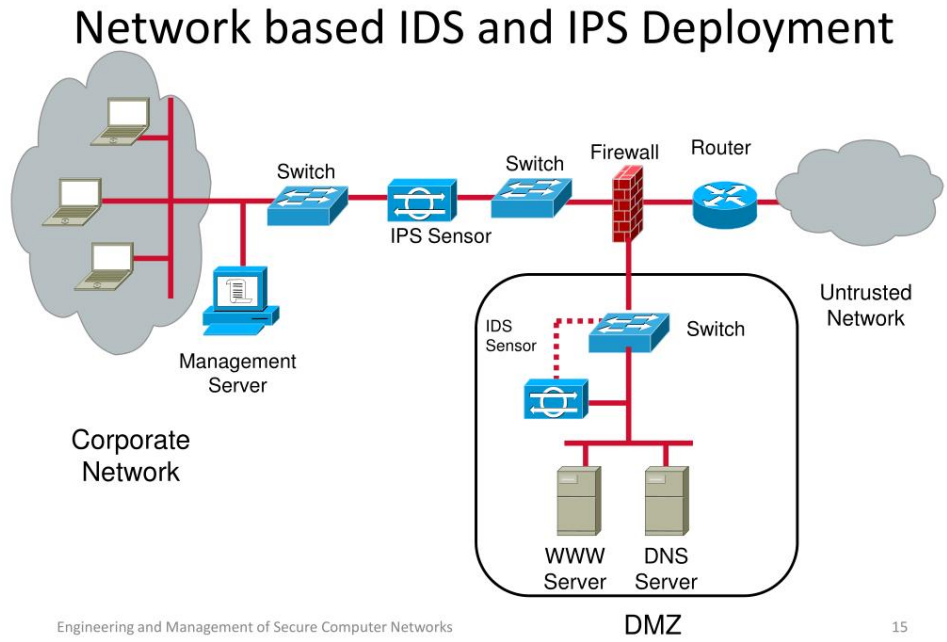
Parameter	ACL	Firewall
Asset Type	Feature on Layer 3 devices and Firewalls	Hardware or Software
Stateful/Stateless inspection	Performs stateless inspection	Performs Stateful inspection
Scope wrt OSI	Upto Layer 4	Upto Layer 7
Security	Low	High
Intrusion detection	Not possible	Possible
Target deployment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

DMZ





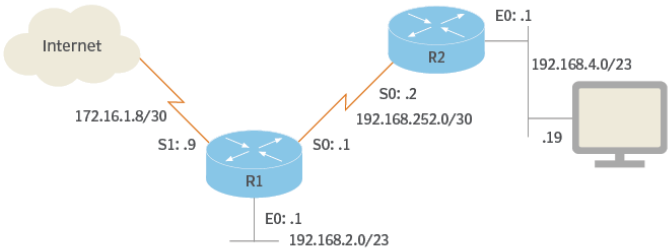
IPS/IDS



Routing Table

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

Routing Protocol

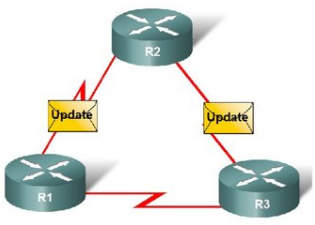
Dynamic IP Routing Protocols

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

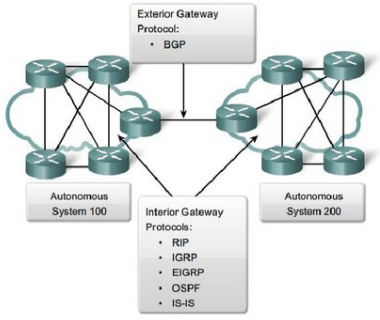
There are quite many dynamic routing protocols for routing IP packets. The most common protocols are:

- **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).

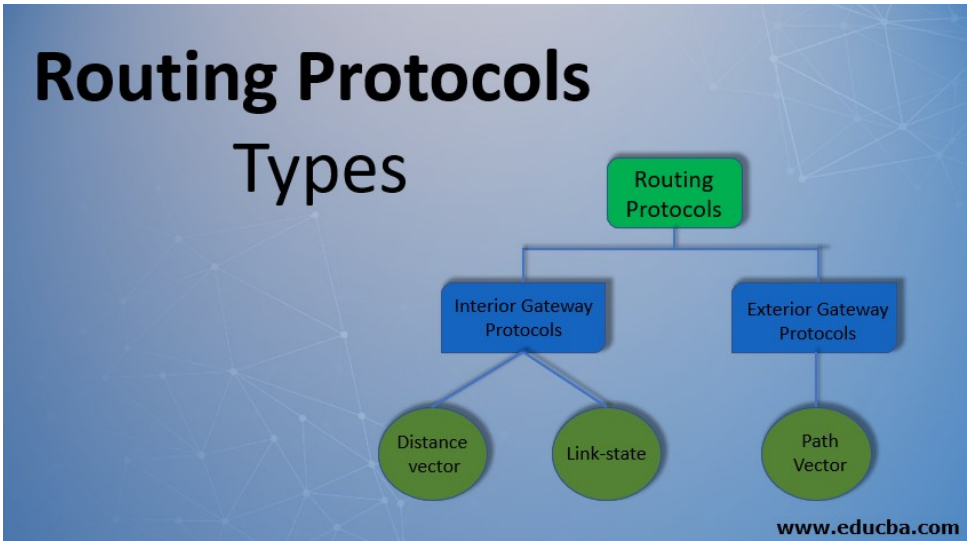
Routers Dynamically Pass Updates

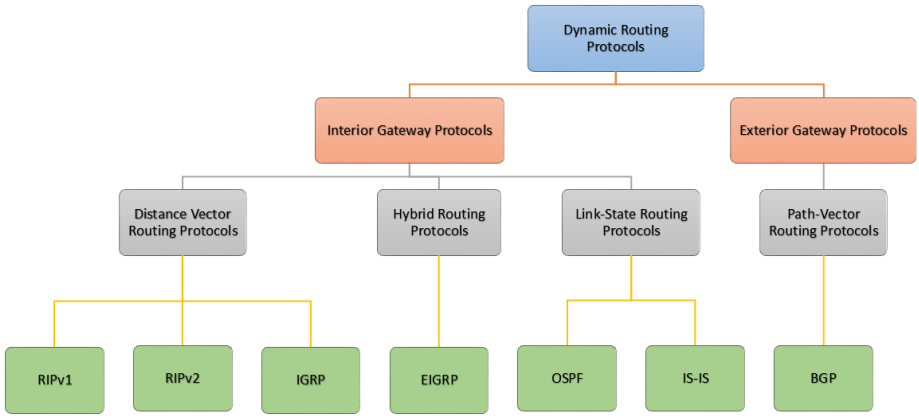


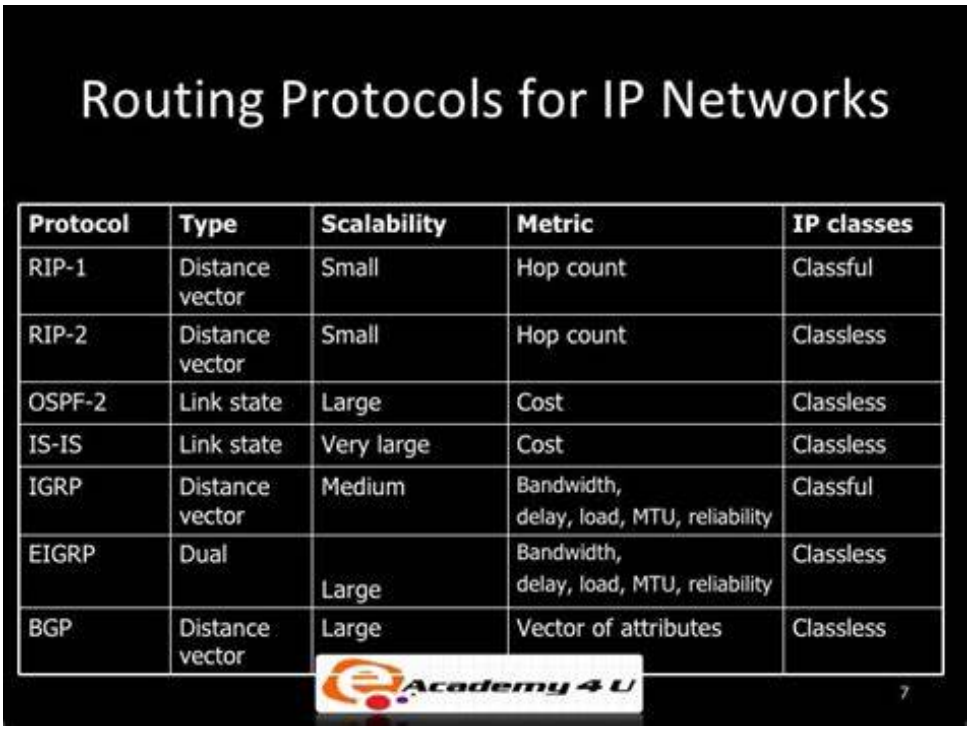
IGP vs. EGP Routing Protocols



16

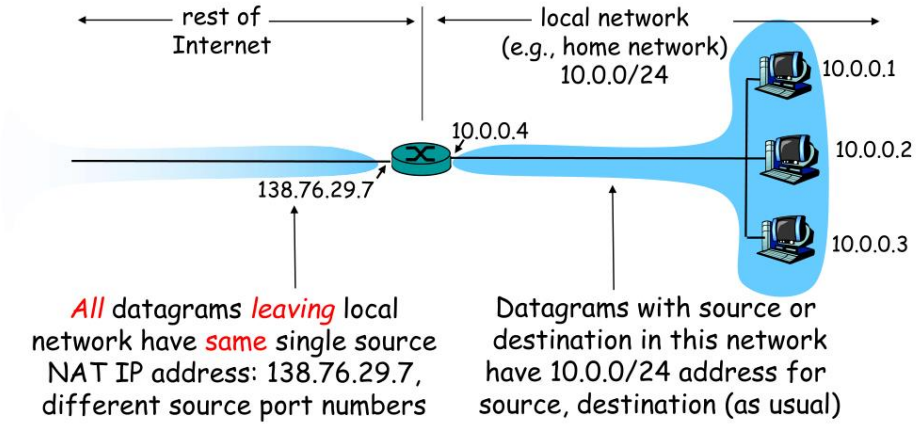






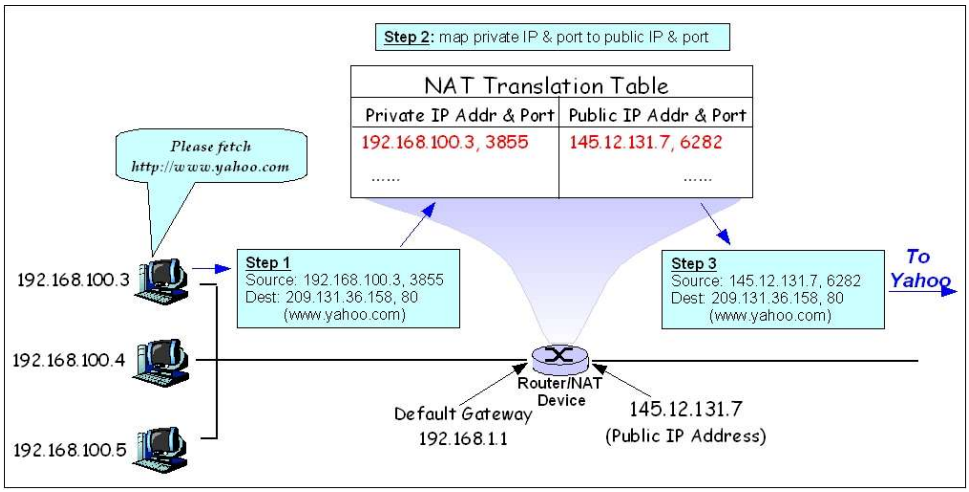
NAT(Network Address Translation)

NAT: Network Address Translation

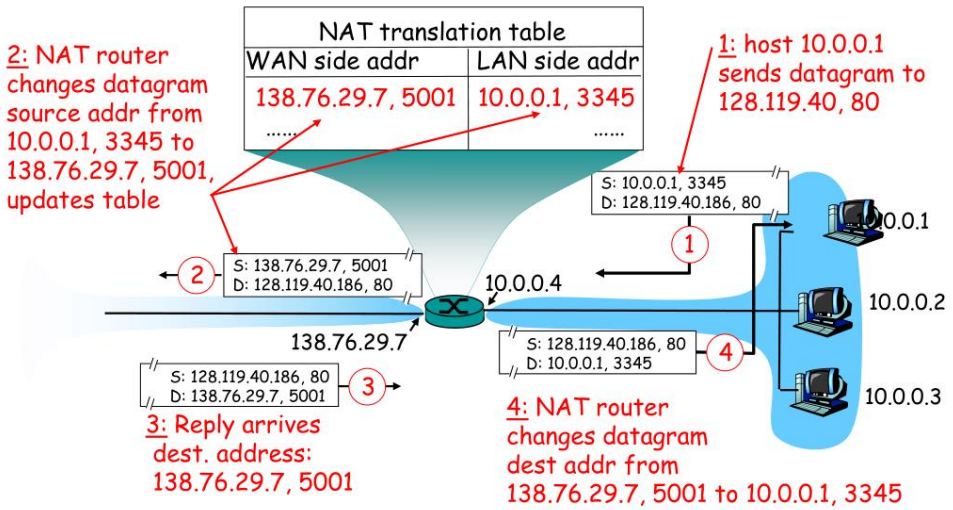


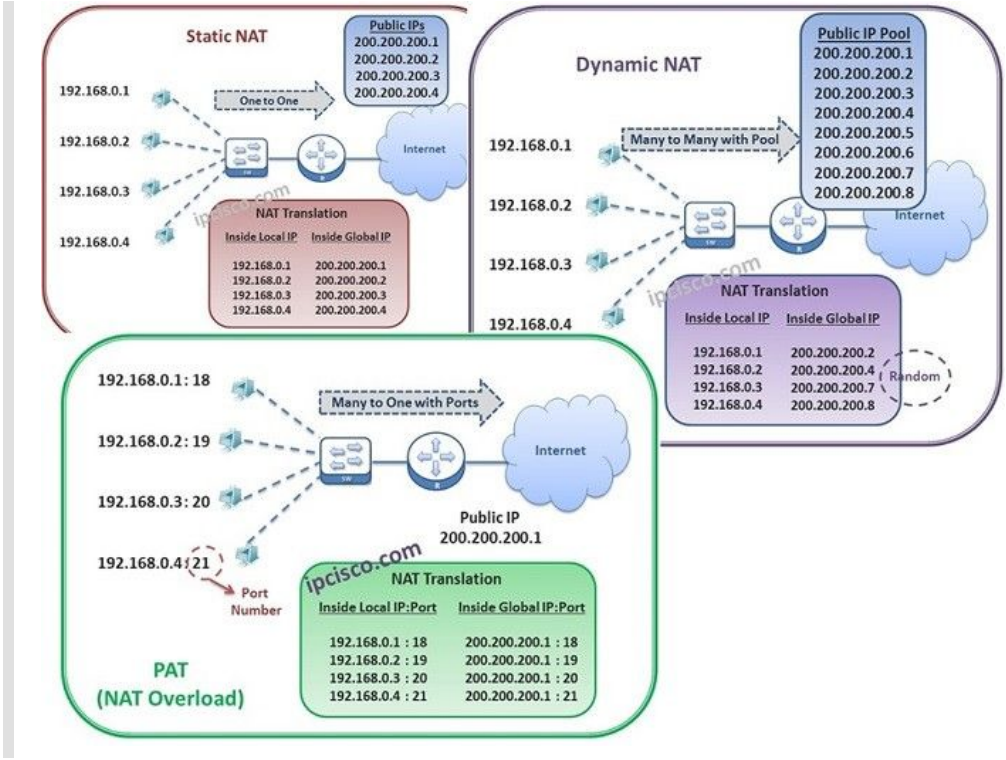
All datagrams leaving local network have same single source NAT IP address: 138.76.29.7, different source port numbers

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

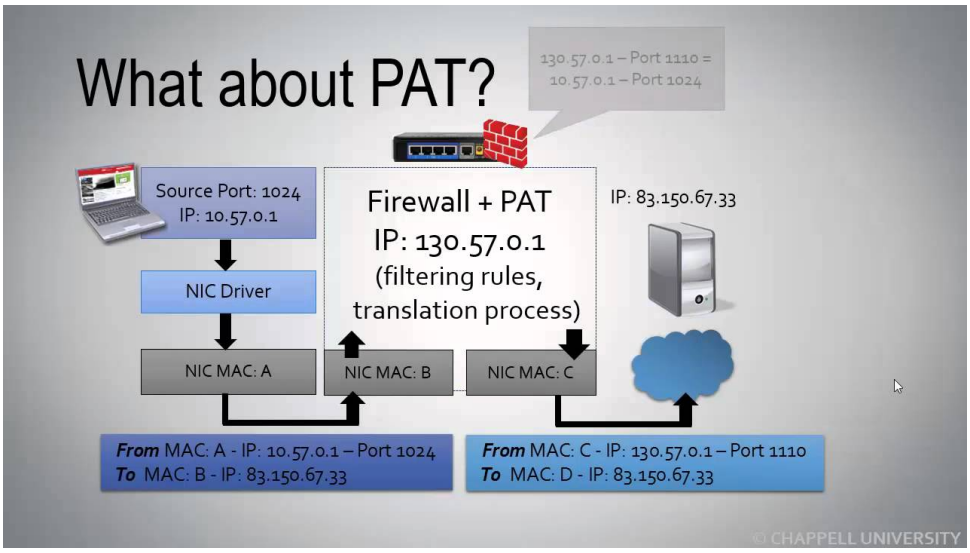


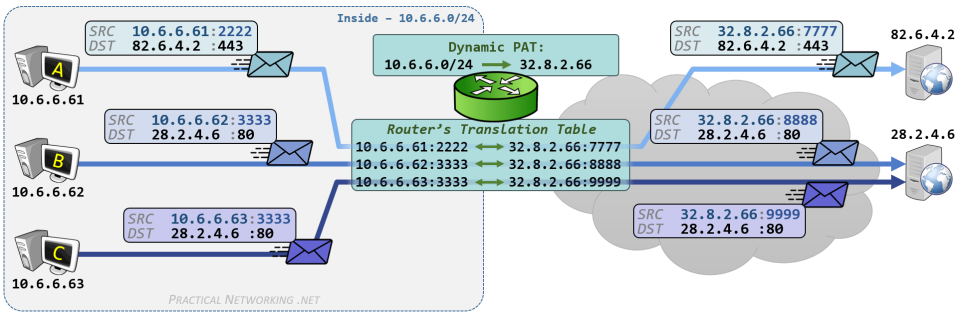
NAT: Network Address Translation



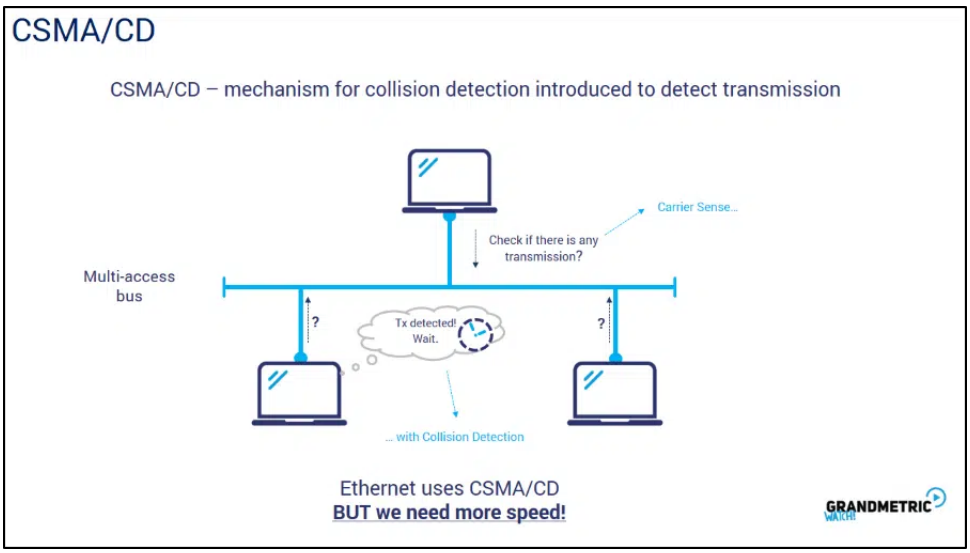


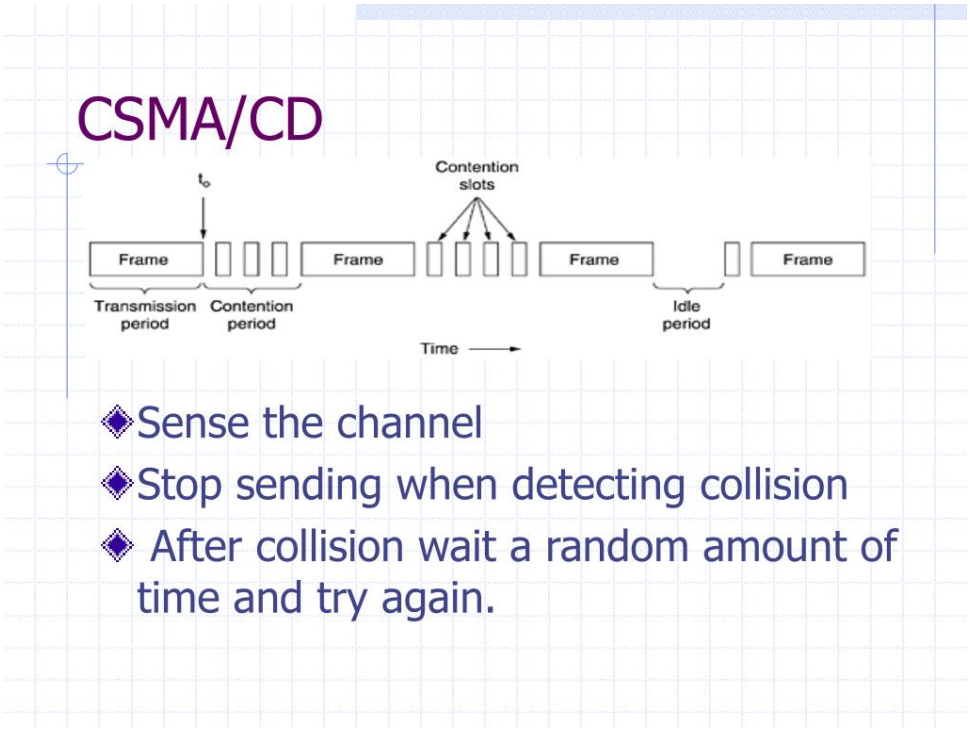
PAT(Port Address Translation)

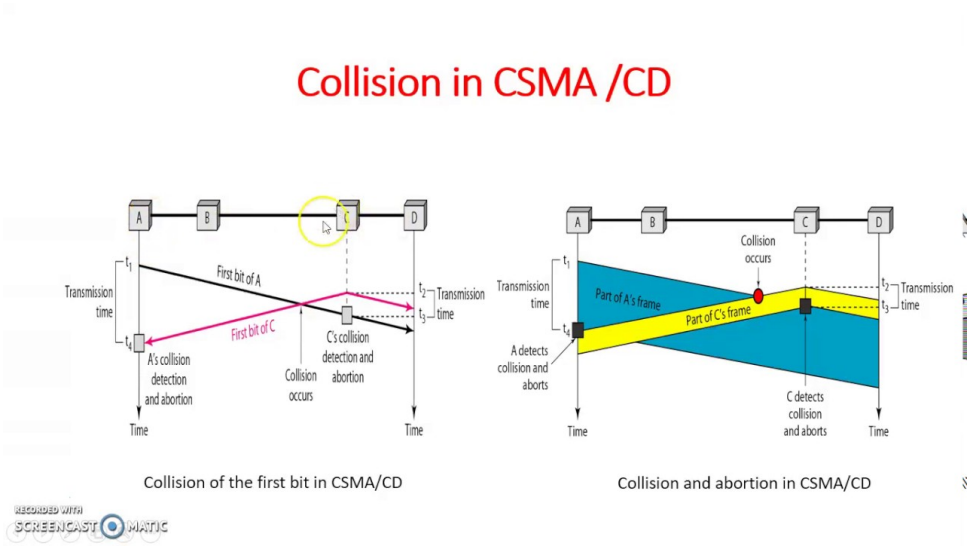




CSMA/CD


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!
GRANDMETRIC

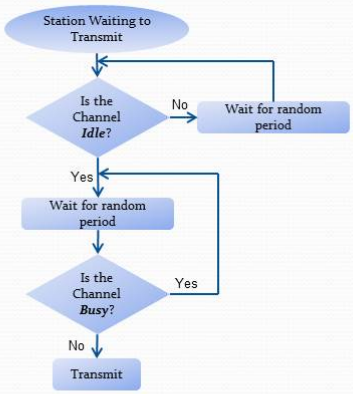

CSMA/CD
Contention slots
Frame
Frame
Frame
Frame
Transmission period
Contention period
Idle period
Time
Sense the channel
Stop sending when detecting collision
After collision wait a random amount of time and try again.


Collision in CSMA /CD
A
B
C
D
Transmission time
First bit of A
First bit of C
A's collision detection and abortion
Collision occurs
C's collision detection and abortion
Time
Collision occurs
Part of A's frame
Part of C's frame
A detects collision and aborts
C detects collision and aborts
Collision of the first bit in CSMA/CD
Collision and abortion in CSMA/CD
RECORDED WITH SCREENCAST-O-MATIC

CSMA/CA

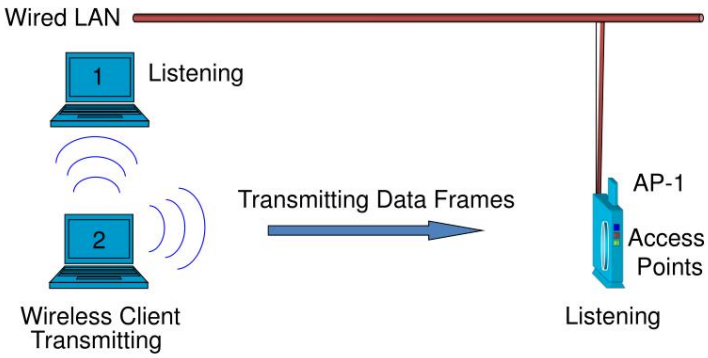
CSMA/CA

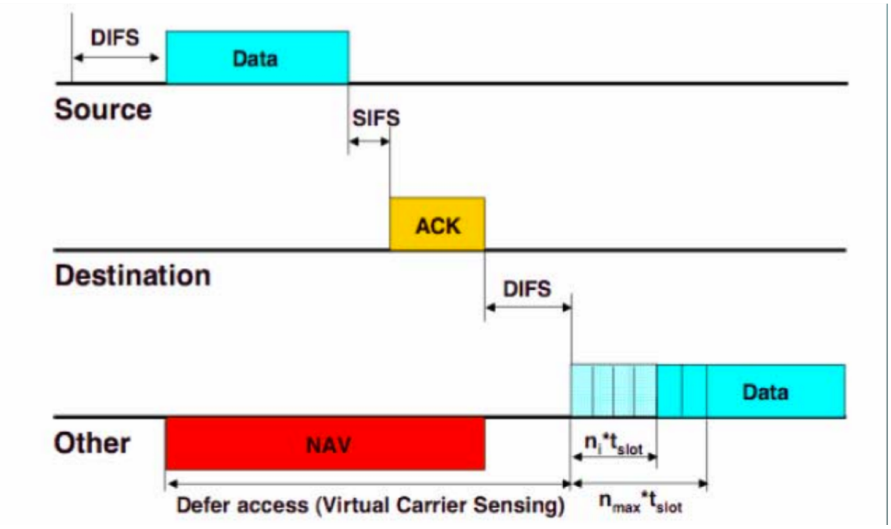
- CSMA/CA is a wireless network multiple access method in which:
  - A carrier sensing scheme is used.
  - A node wishing to transmit data has to first listen to the channel for a predetermined amount of time whether or not another node is transmitting on channel within the wireless range. If the channel 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



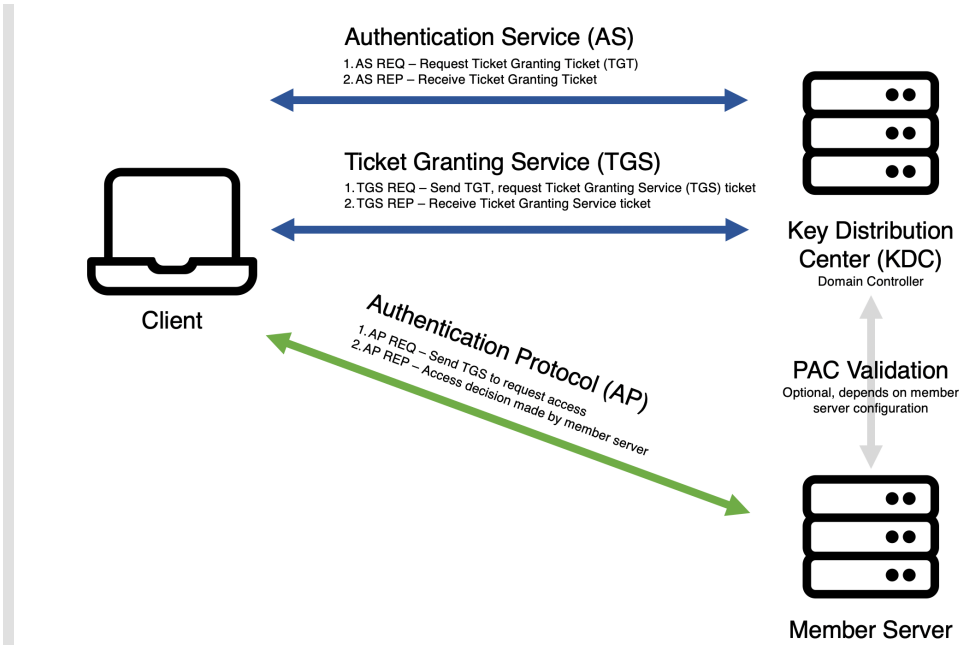
CSMA/CA Collision Handling

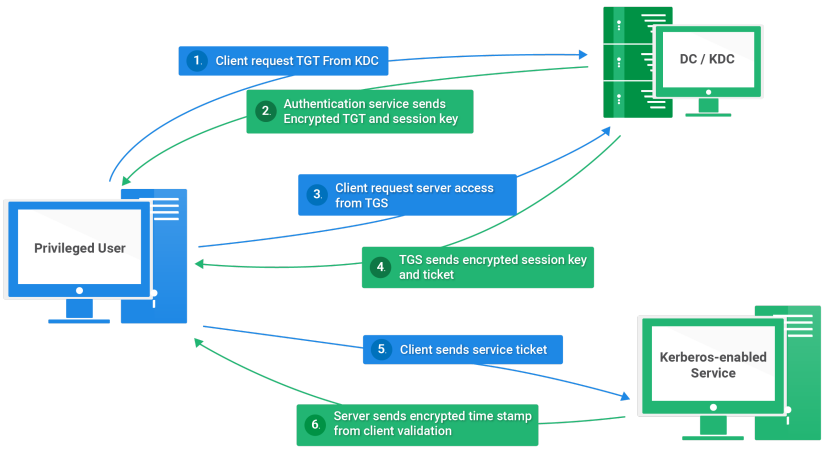
- 802.11 standard employs half-duplex radios-radios capable of transmission or reception-but not both simultaneously

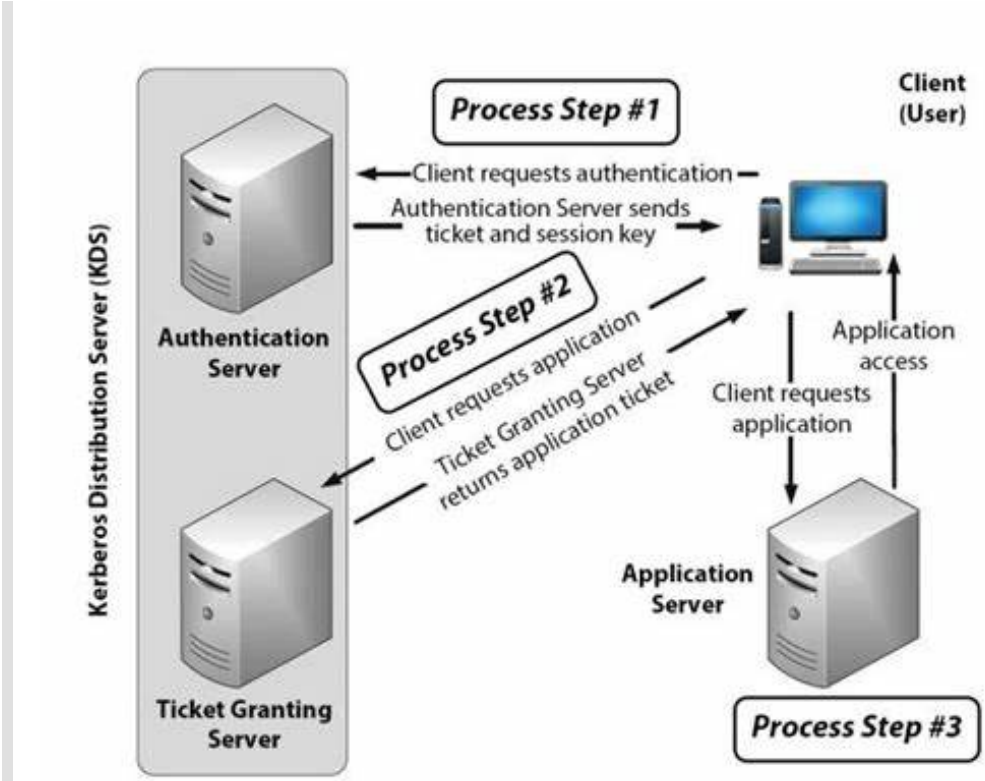


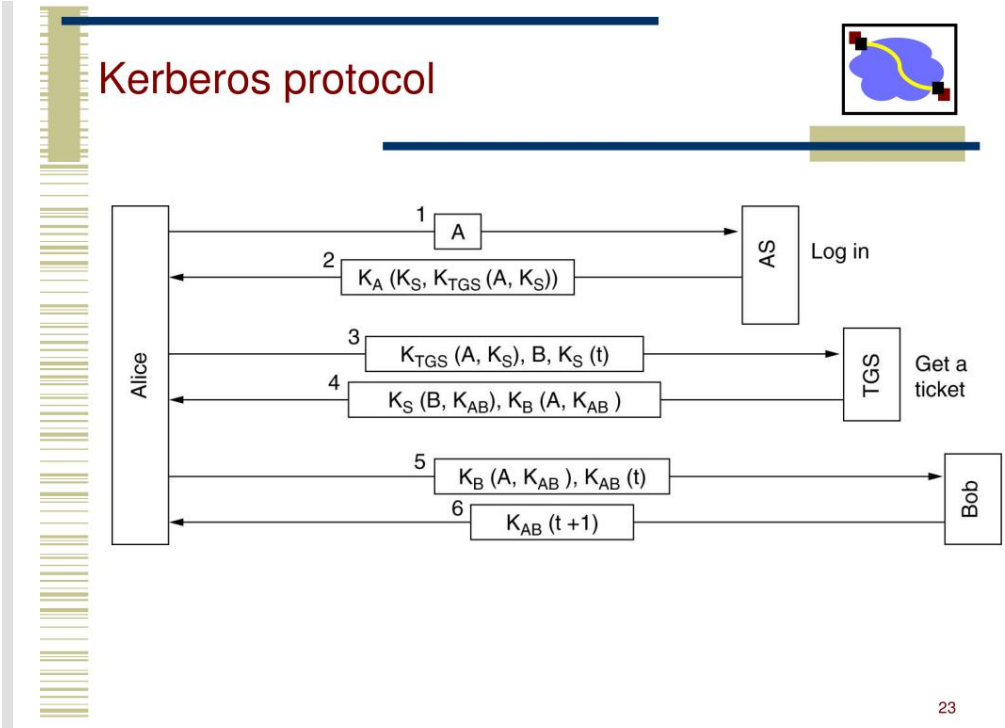


Kerberos

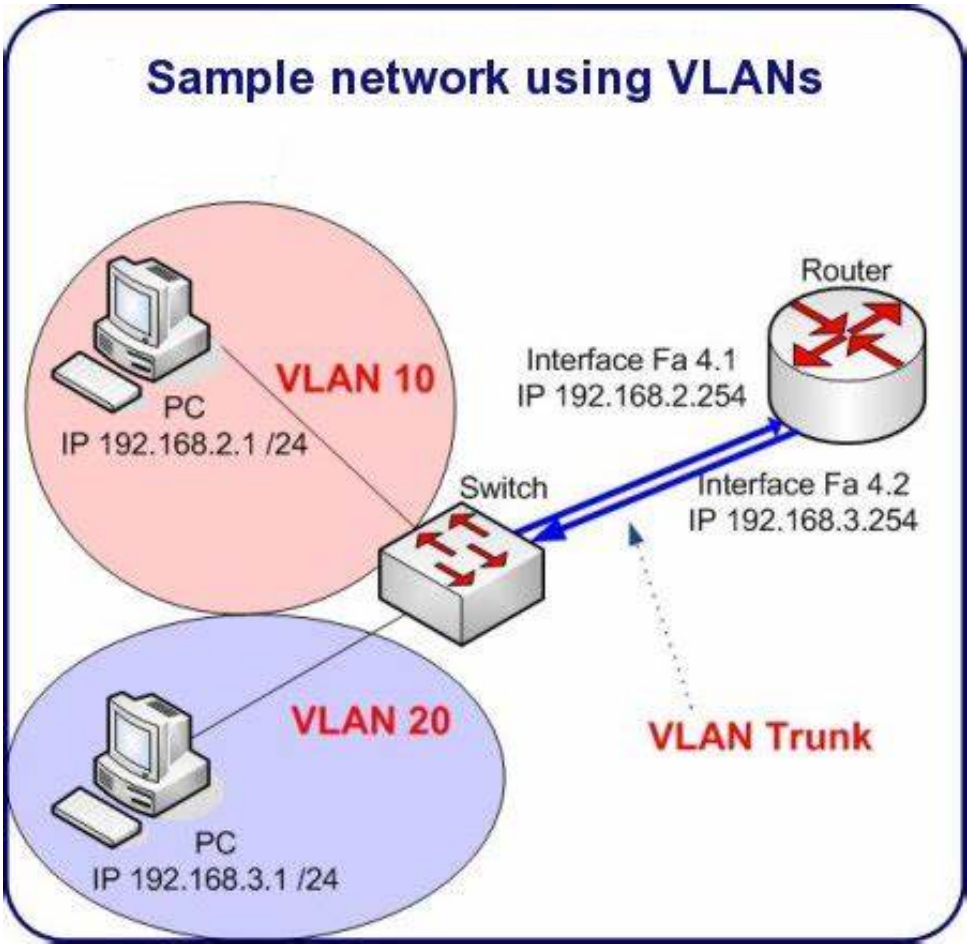

Authentication Service (AS)
1. AS REQ – Request Ticket Granting Ticket (TGT)
2. AS REP – Receive Ticket Granting Ticket
Ticket Granting Service (TGS)
1. TGS REQ – Send TGT, request Ticket Granting Service (TGS) ticket
2. TGS REP – Receive Ticket Granting Service ticket
Client
Key Distribution Center (KDC)
Domain Controller
Authentication Protocol (AP)
1. AP REQ – Send TGS to request access
2. AP REP – Access decision made by member server
PAC Validation
Optional, depends on member server configuration
Member Server


1 Client request TGT From KDC
DC / KDC
2 Authentication service sends Encrypted TGT and session key
3 Client request server access from TGS
Privileged User
4 TGS sends encrypted session key and ticket
5 Client sends service ticket
Kerberos-enabled Service
6 Server sends encrypted time stamp from client validation

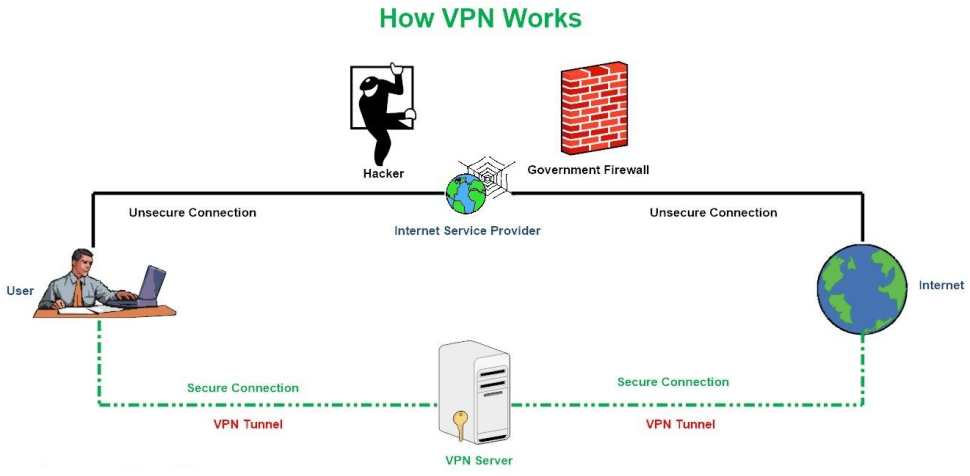

Process Step #1
Client (User)
Client requests authentication
Authentication Server sends ticket and session key
Process Step #2
Client requests application
Ticket Granting Server returns application ticket
Application access
Client requests application
Kerberos Distribution Server (KDS)
Authentication Server
Ticket Granting Server
Application Server
Process Step #3

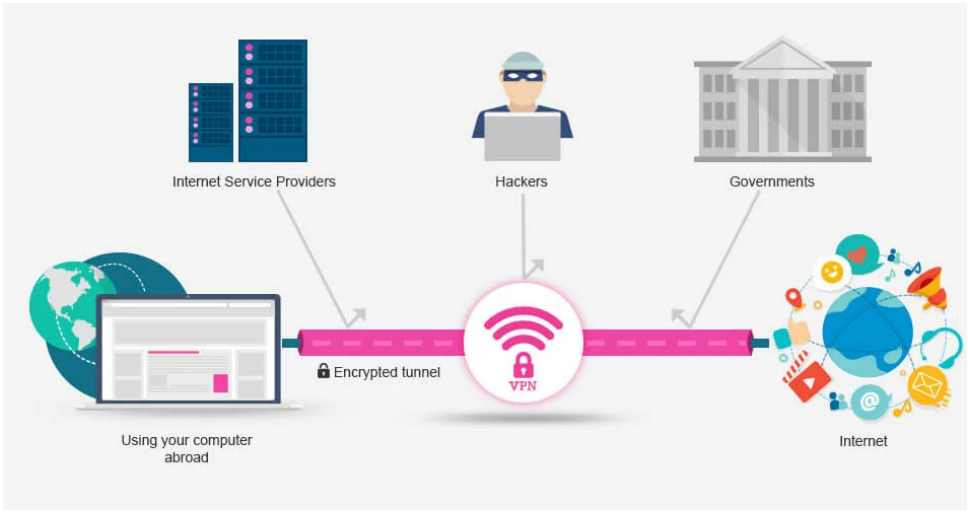

Kerberos protocol
1 A
2 K_A (K_S, K_{TGS} (A, K_S))
AS
Log in
3 K_{TGS} (A, K_S), B, K_S (t)
4 K_S (B, K_{AB}), K_B (A, K_{AB})
TGS
Get a ticket
Alice
5 K_B (A, K_{AB}), K_{AB} (t)
6 K_{AB} (t +1)
Bob
23

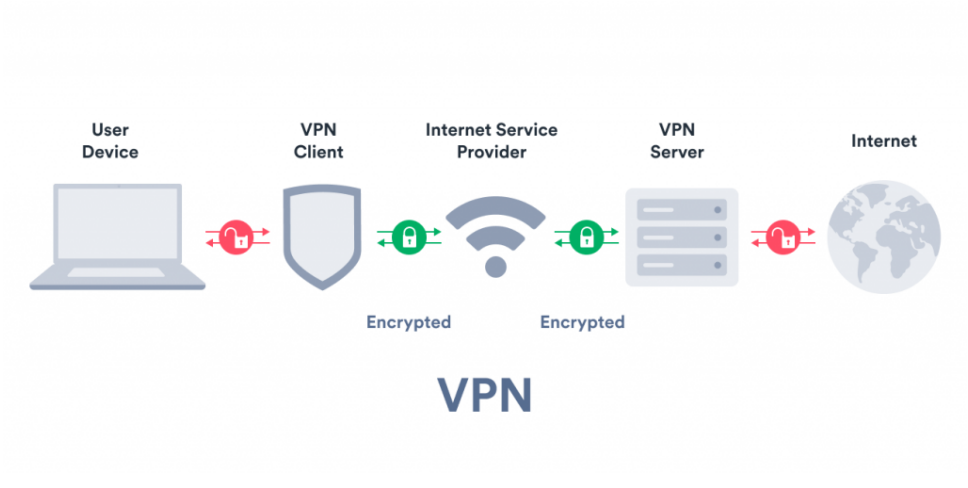
VLAN

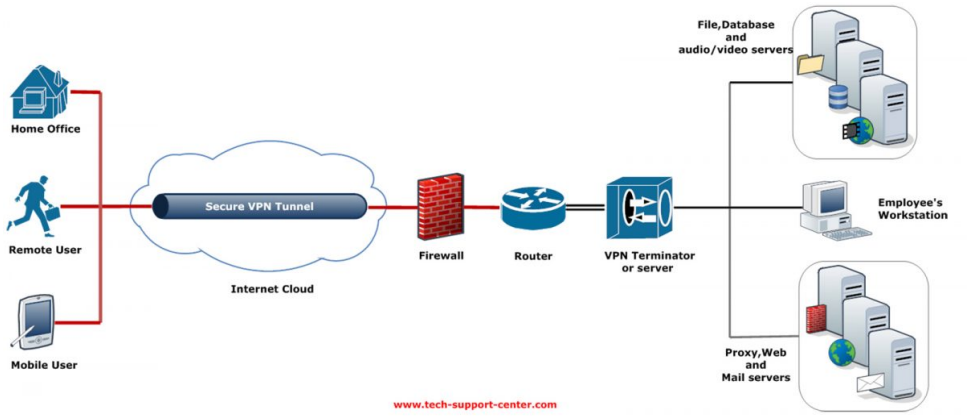

Sample network using VLANs
Router
Interface Fa 4.1
IP 192.168.2.254
VLAN 10
PC
IP 192.168.2.1 /24
Switch
Interface Fa 4.2
IP 192.168.3.254
VLAN 20
VLAN Trunk
PC
IP 192.168.3.1 /24

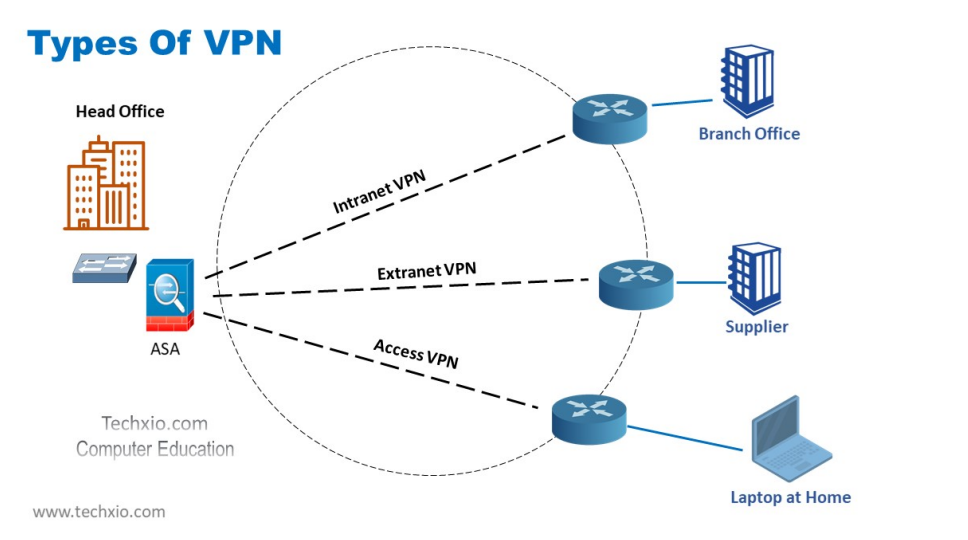
VPN


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

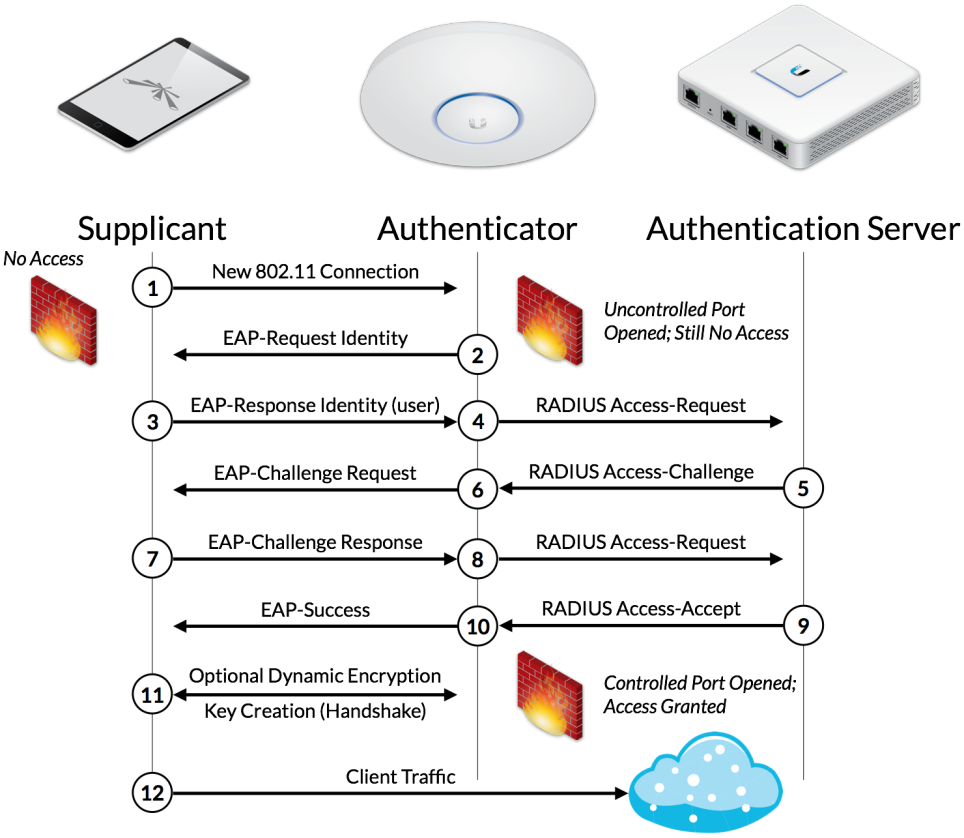

Internet Service Providers
Hackers
Governments
Encrypted tunnel
VPN
Using your computer abroad
Internet


User Device
VPN Client
Internet Service Provider
VPN Server
Internet
Encrypted
Encrypted
VPN


Home Office
Remote User
Mobile User
Secure VPN Tunnel
Internet Cloud
Firewall
Router
VPN Terminator or server
File,Database and audio/video servers
Employee's Workstation
Proxy,Web and Mail servers
www.tech-support-center.com

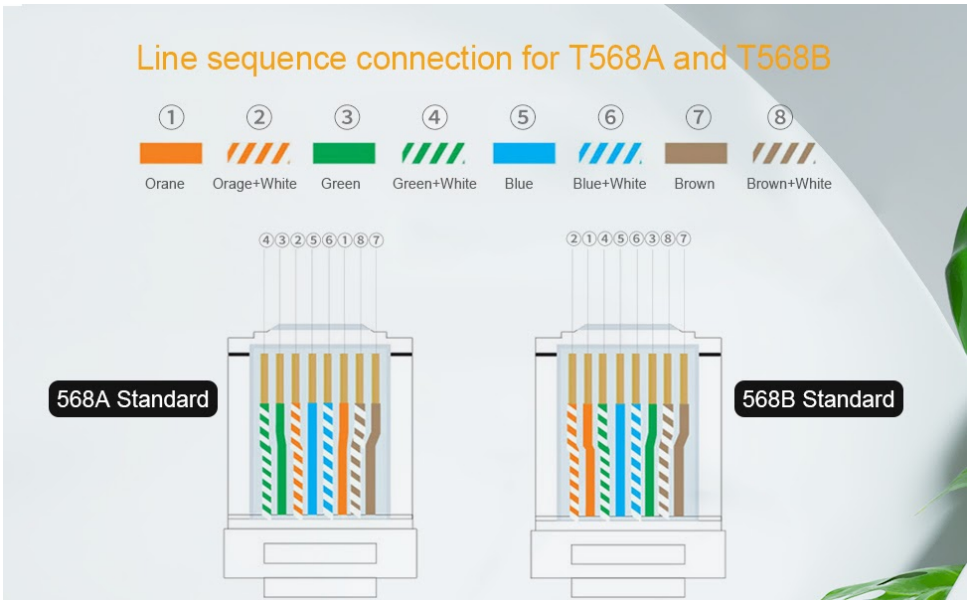

Types Of VPN
Head Office
Branch Office
Intranet VPN
Extranet VPN
Supplier
ASA
Access VPN
Techxio.com
Computer Education
Laptop at Home
www.techxio.com

802.1X Authentication (EAP & RADIUS)

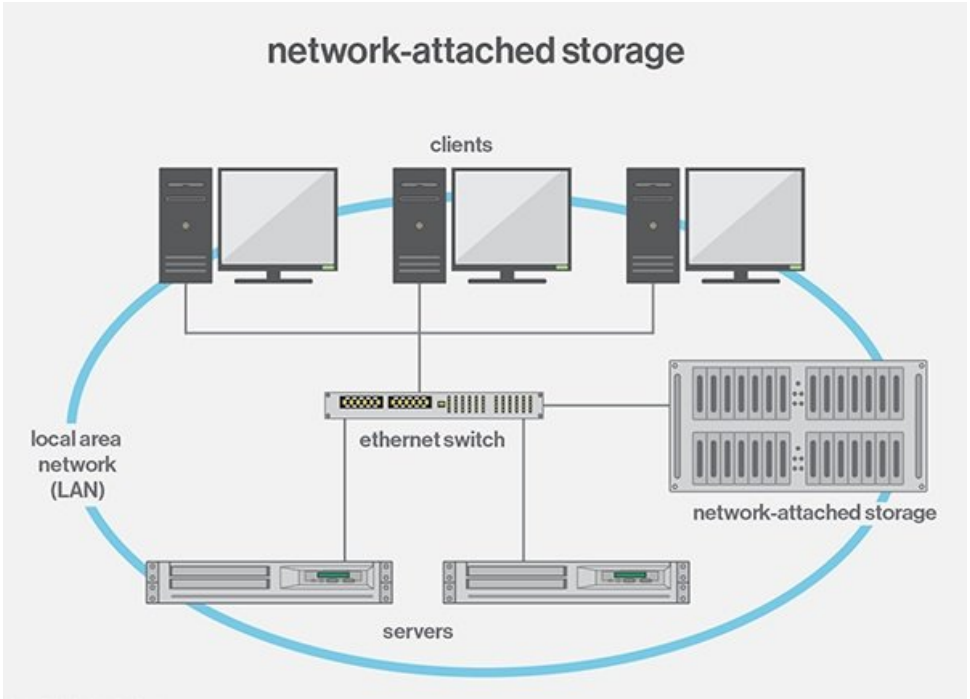


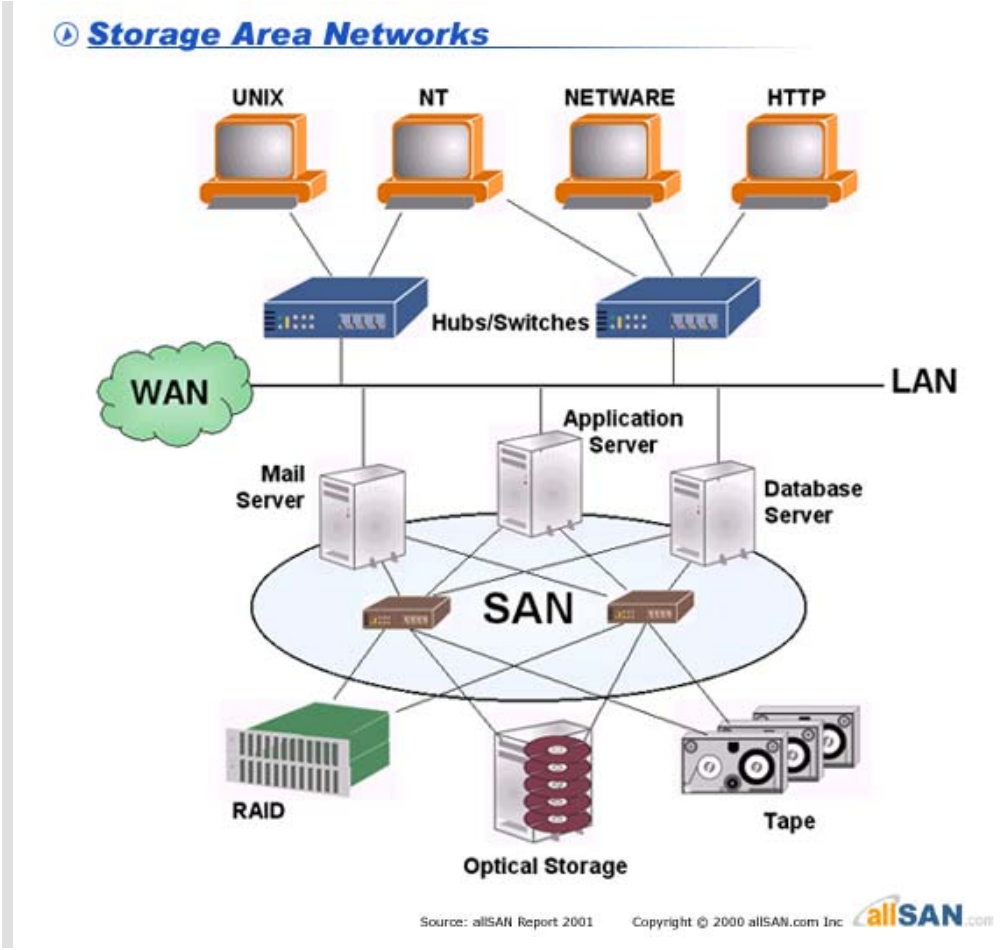
Cable

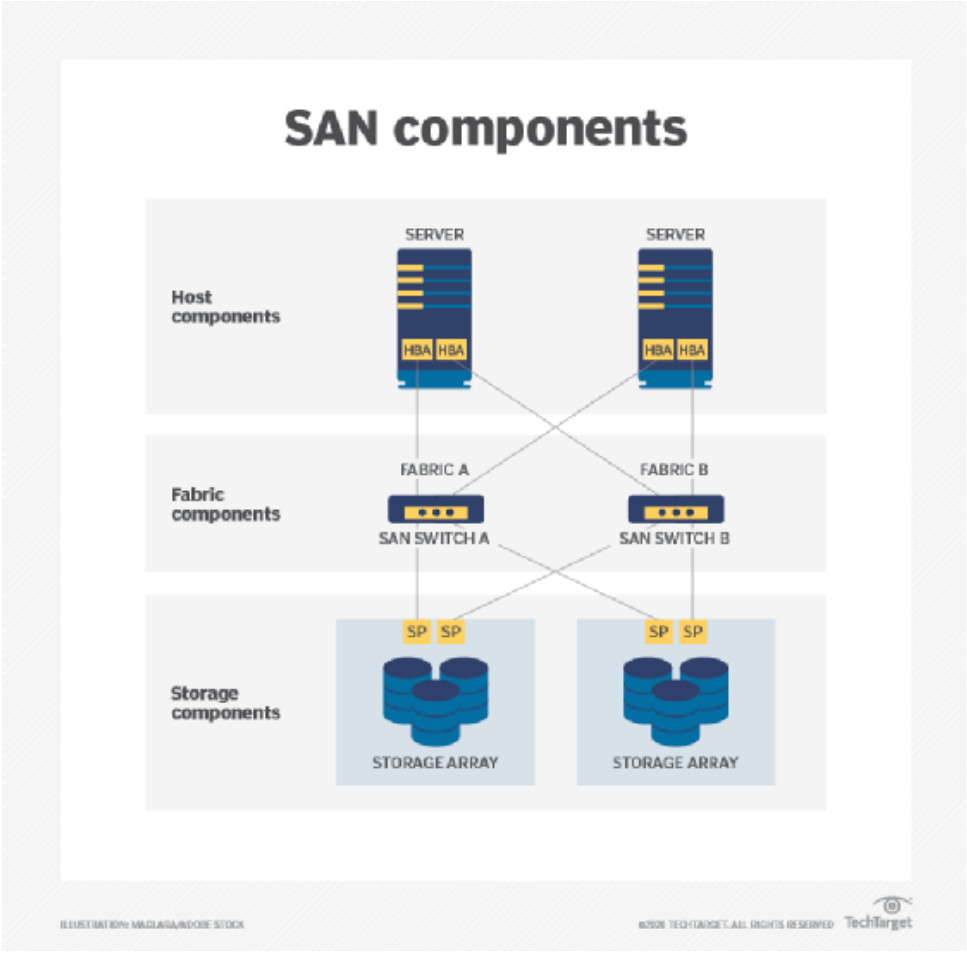
Category	Standard Bandwidth	Max Data Rate	Shielding
Cat5e	100MHz (up to 350)	1000Mbps	UTP or STP
Cat6	250MHz (up to 550)	1000Mbps	UTP or STP
Cat6A	500MHz (up to 550)	10Gbps	UTP or STP
Cat7	600MHz	10Gbps	Shielded only
Cat8	2000MHz	25Gbps or 40Gbps	Shielded only



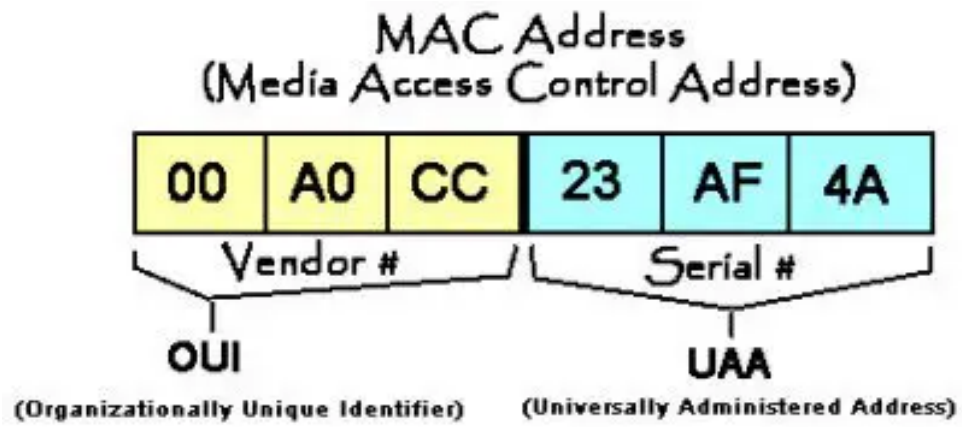
NAS vs SAN

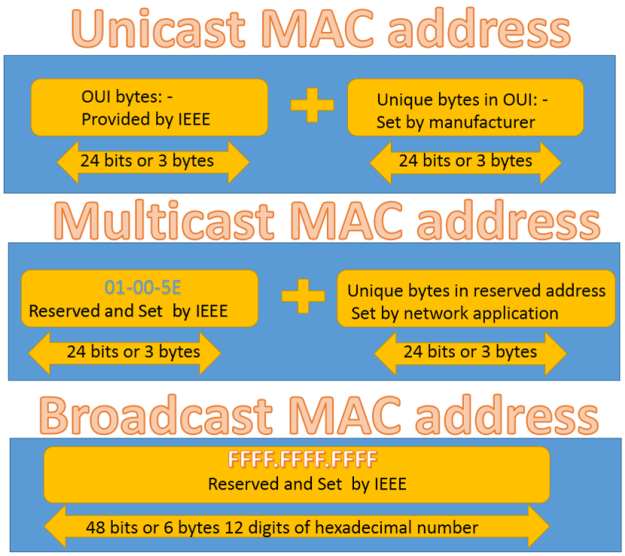




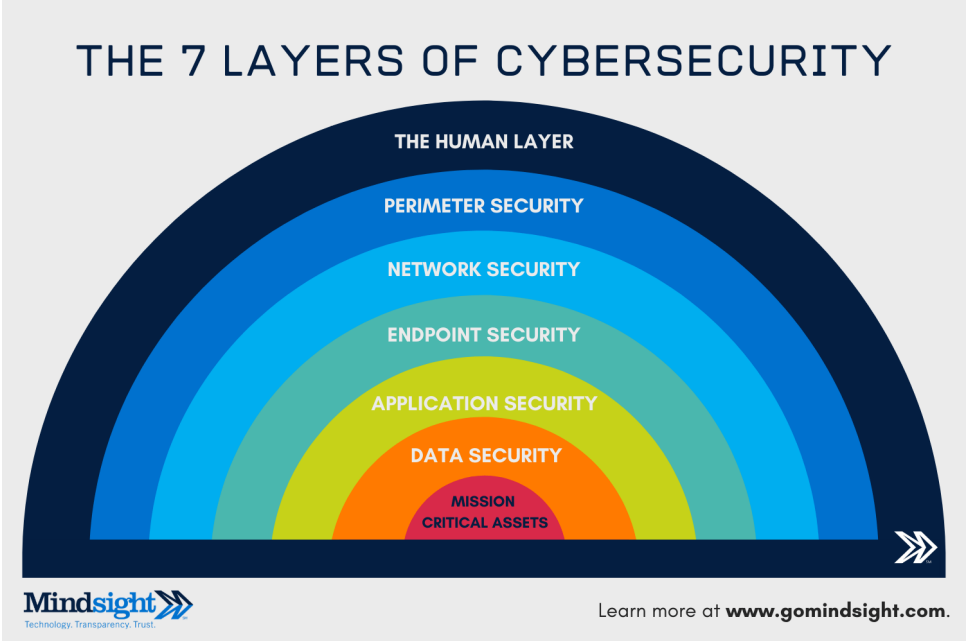


Datalink Layer MAC Address

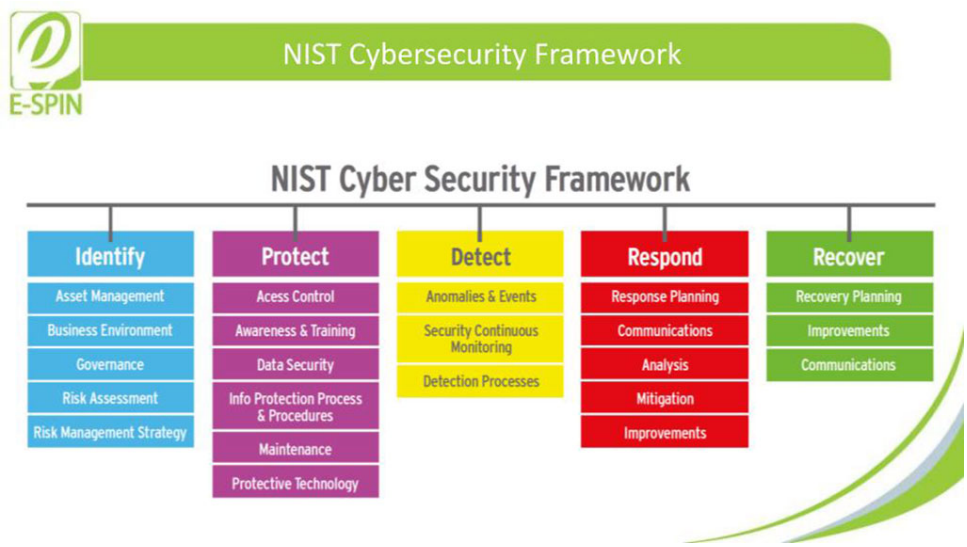




CyberSecurity

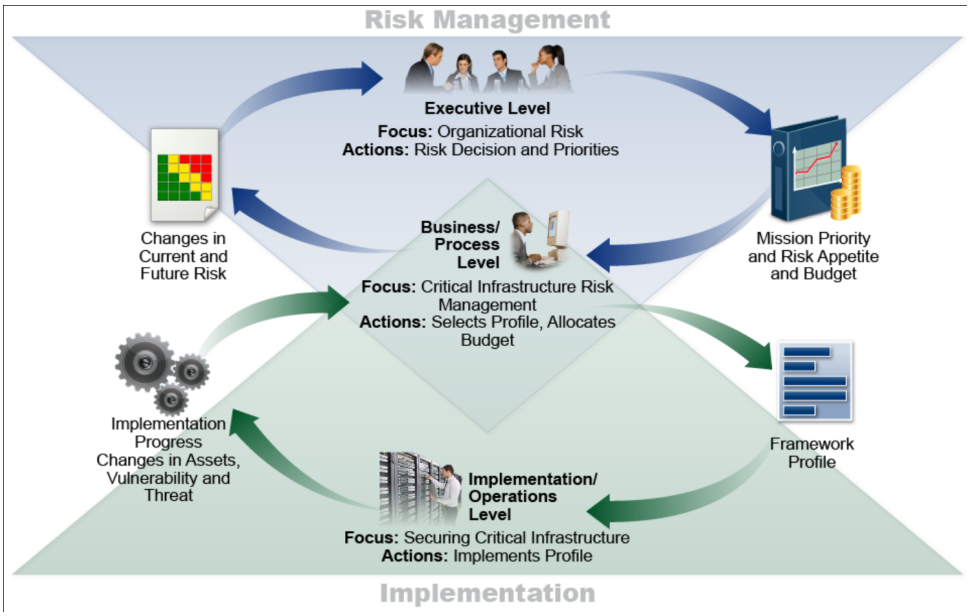



1 IDENTIFY
Identify and control who has access to your business information
Conduct background checks
Require individual user accounts for each employee
Create policies and procedures for cybersecurity
2 PROTECT
Limit employee access to data and information
Install Surge Protectors and Uninterruptible 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
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

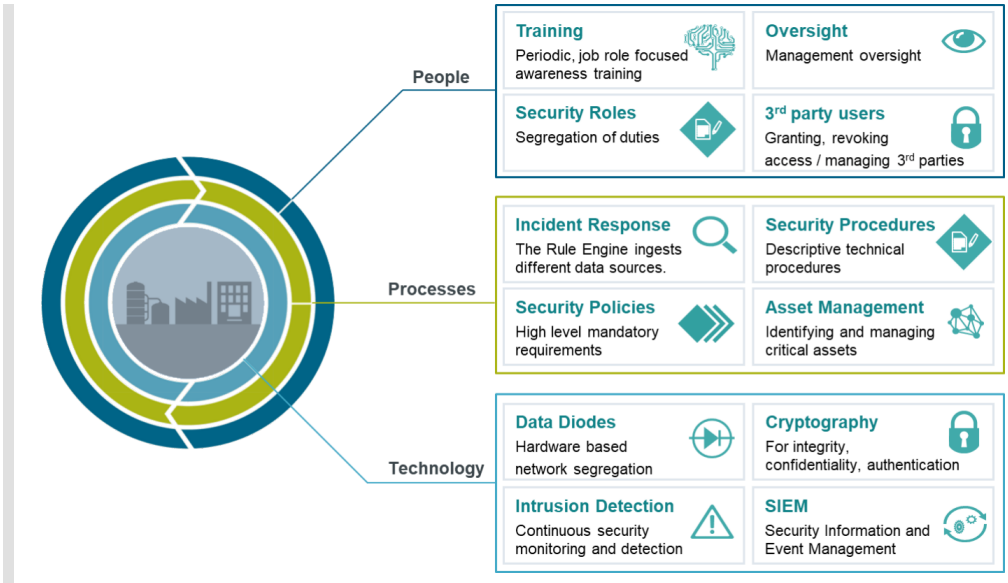

E-SPIN
NIST Cybersecurity Framework
NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Acess Control
Awareness & Training
Data Security
Info Protection Process & Procedures
Maintenance
Protective Technology
Detect
Anomalies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

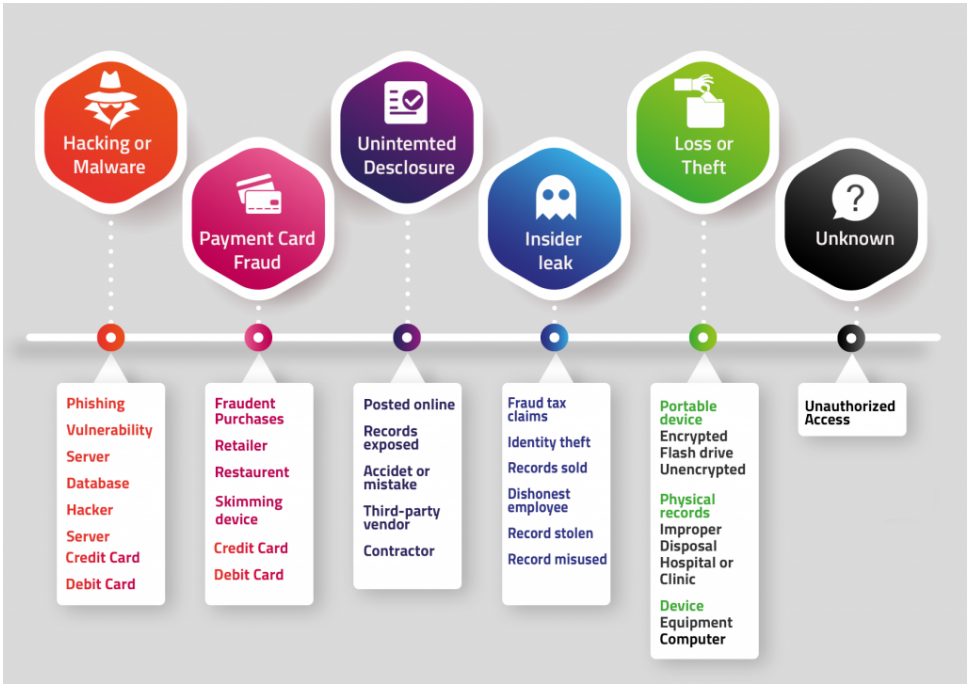
Risk Management


BEST CYBERSECURITY PRACTICES
01
Install and regularly update protective software
02
Apply a strong password policy
Use multi-factor authentication
03
Make regular backups
04
Drudesk
Drupal Support On Demand

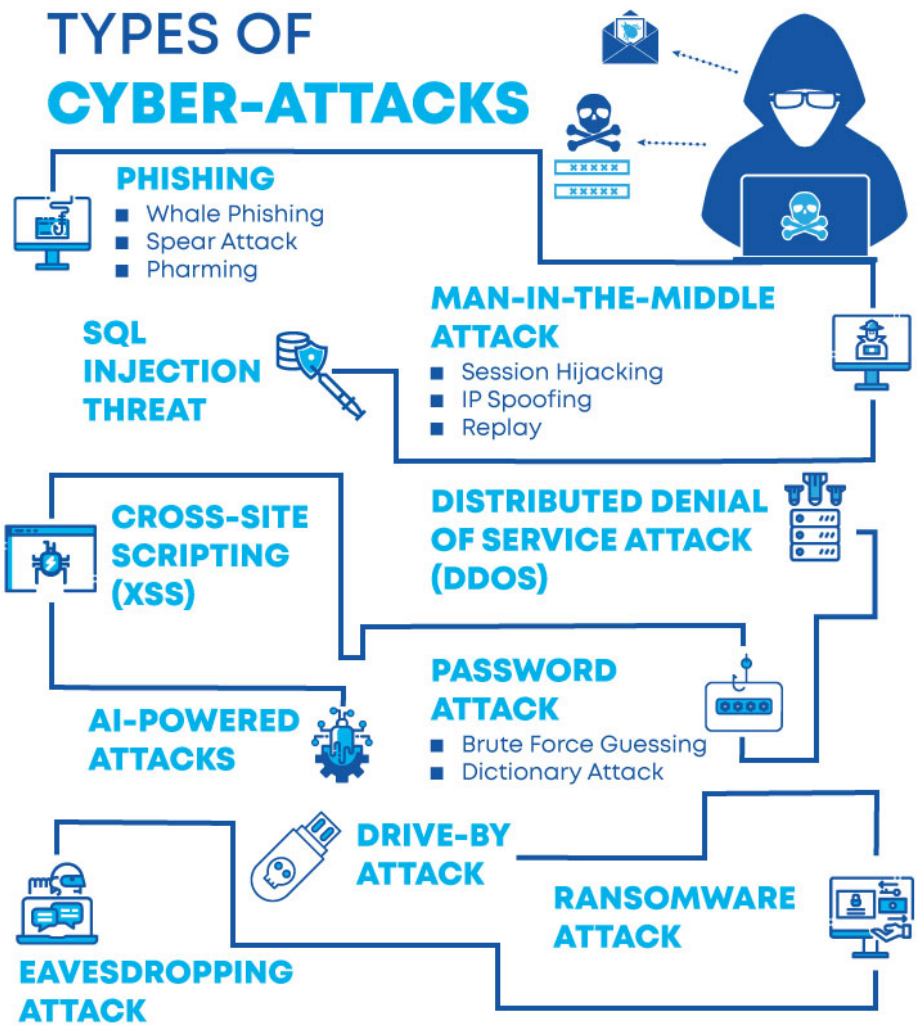

Risk Management
Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Mission Priority and Risk Appetite and Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

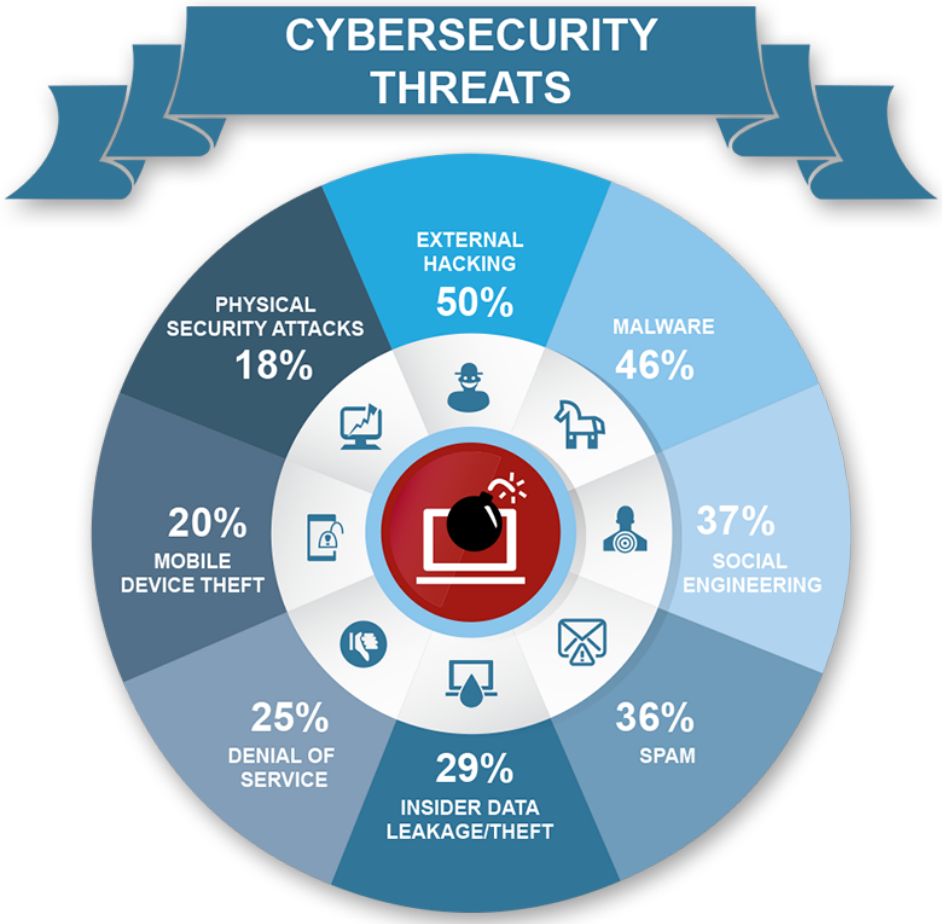

Application Security
Information Security
Network Security
Disaster Recovery
End-user Compliance
Elements of Cybersecurity

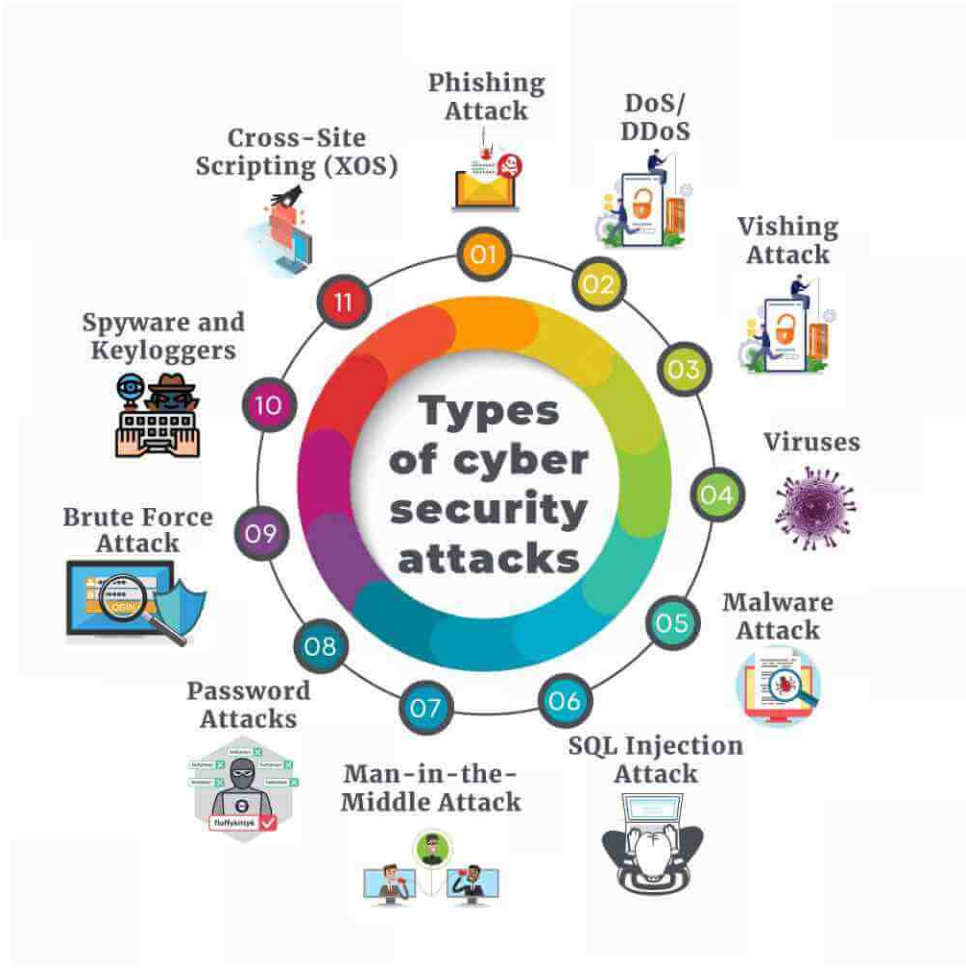

People
Processes
Technology
Training
Periodic, job role focused awareness training
Oversight
Management oversight
Security Roles
Segregation of duties
3rd party users
Granting, revoking access / managing 3rd parties
Incident Response
The Rule Engine ingests different data sources.
Security Procedures
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



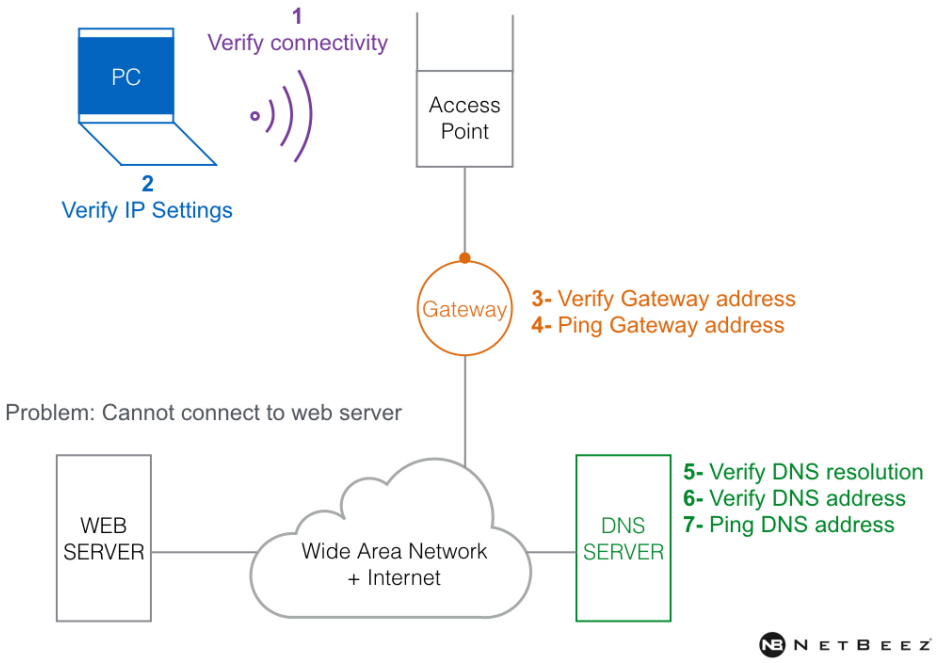
Cybersecurity Attacks

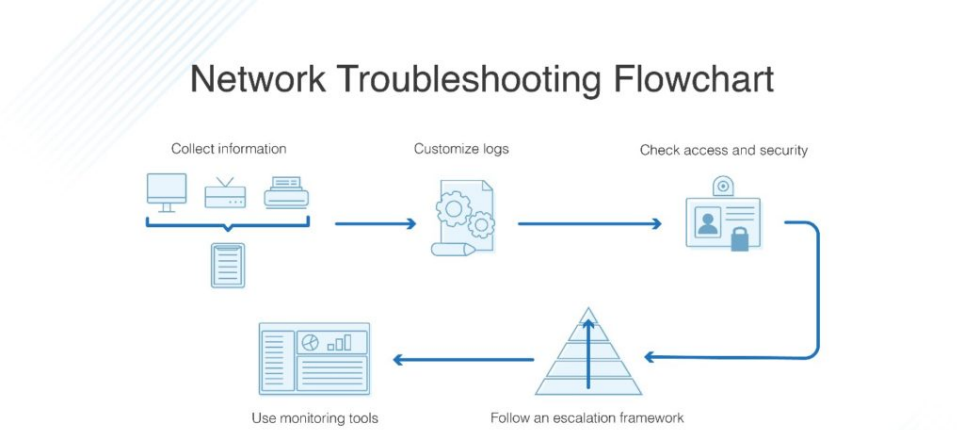


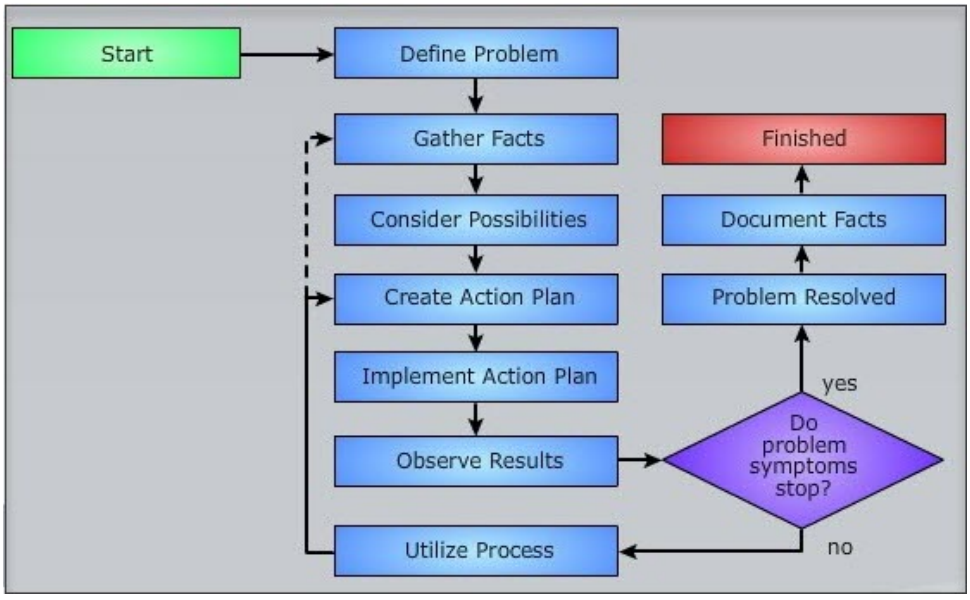




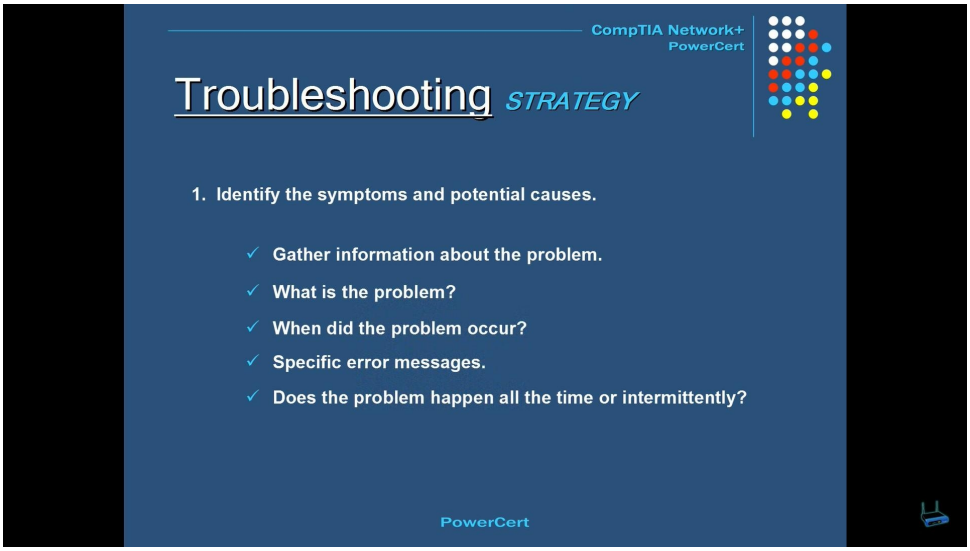
Network Troubleshooting

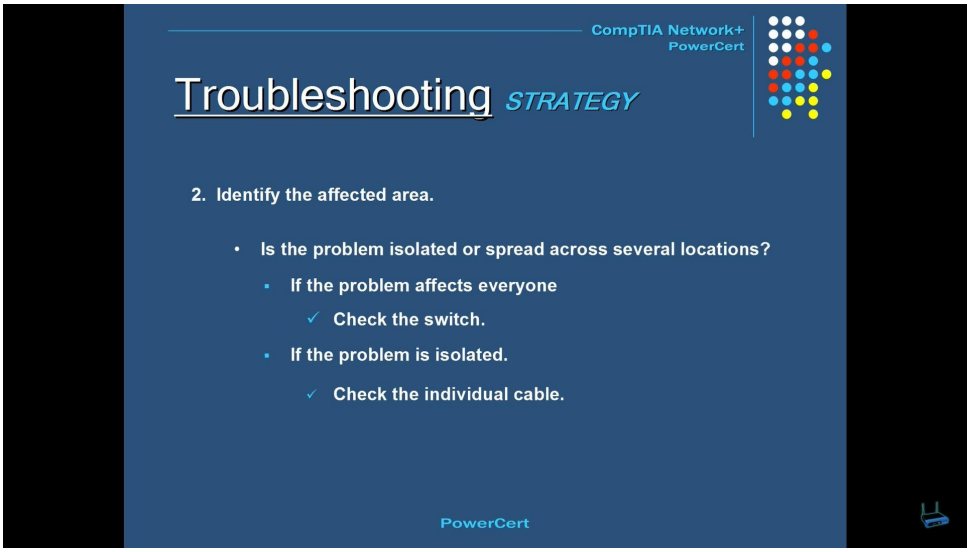


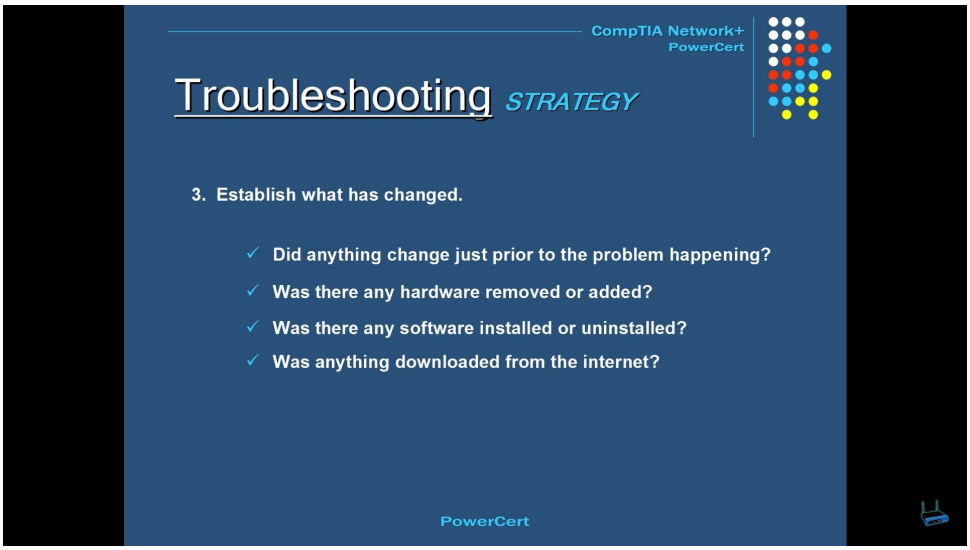


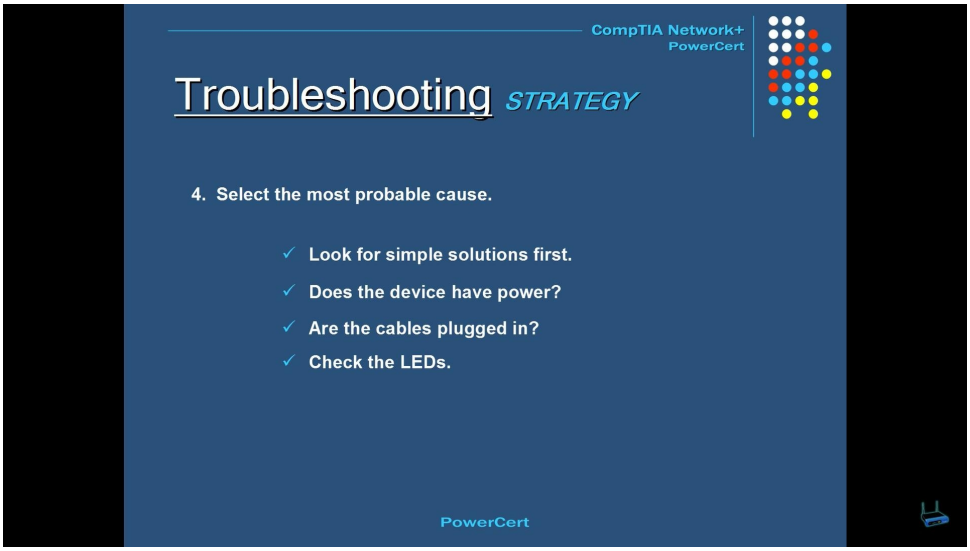


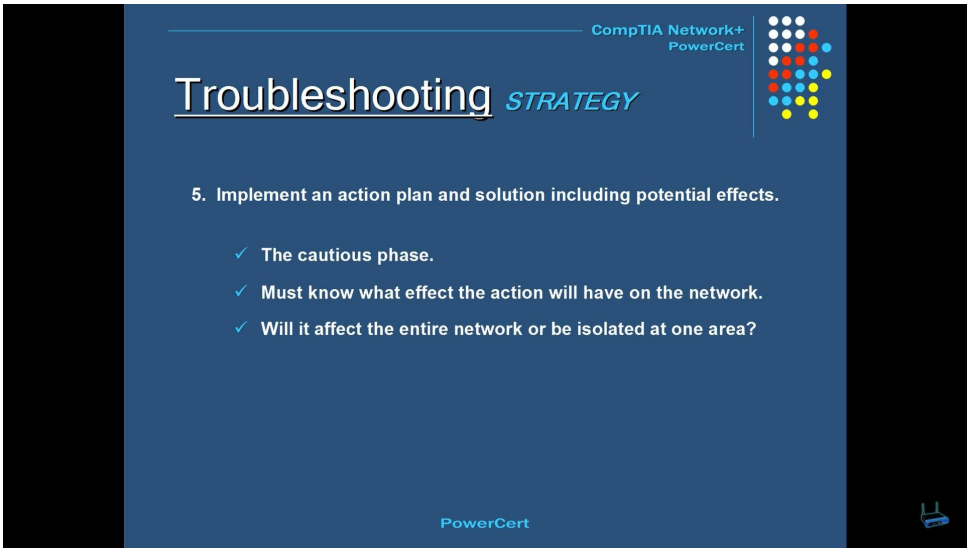
Troubleshooting Strategy

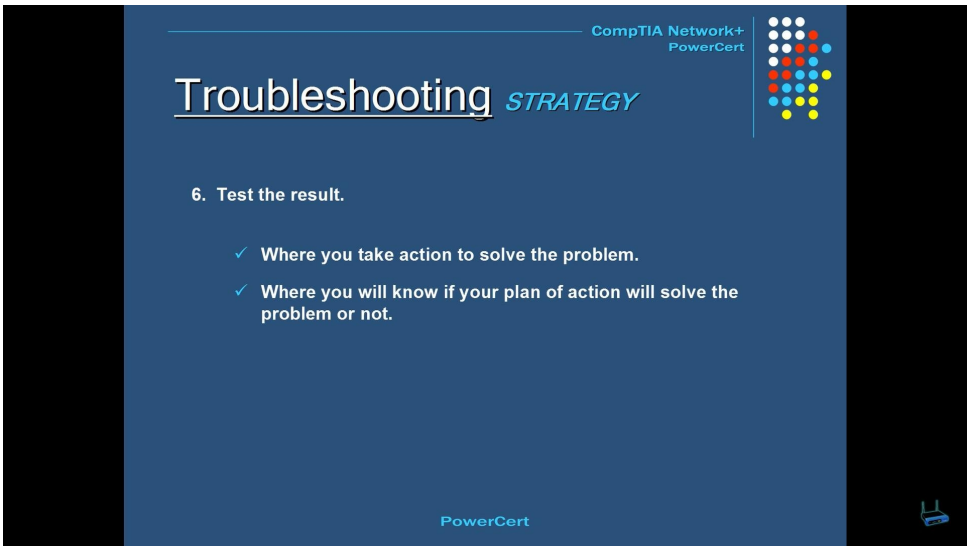

CompTIA Network+
PowerCert
Troubleshooting STRATEGY
1. Identify the symptoms and potential causes.
✓ Gather information about the problem.
✓ What is the problem?
✓ When did the problem occur?
✓ Specific error messages.
✓ Does the problem happen all the time or intermittently?
PowerCert

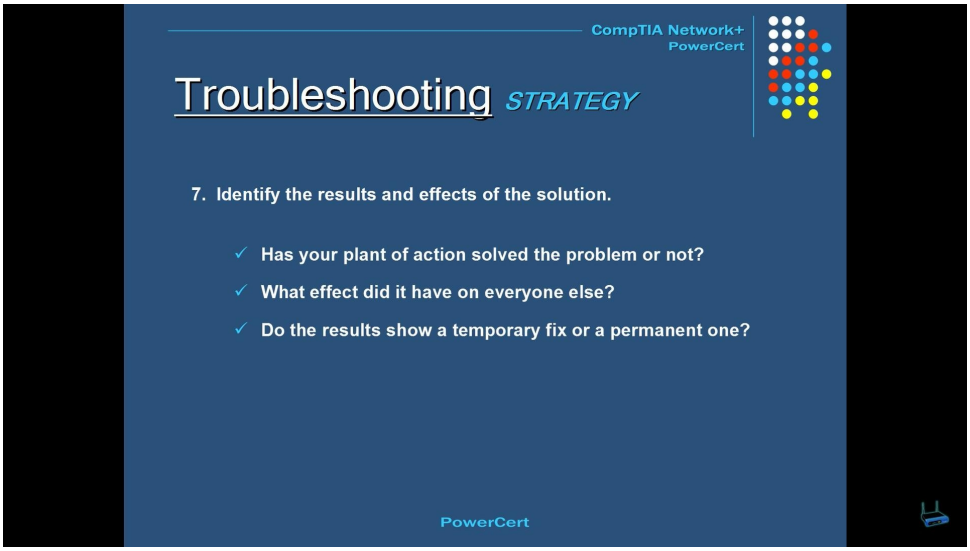

CompTIA Network+
PowerCert
Troubleshooting STRATEGY
2. Identify the affected area.
• Is the problem isolated or spread across several locations?
▪ If the problem affects everyone
✓ Check the switch.
▪ If the problem is isolated.
✓ Check the individual cable.
PowerCert

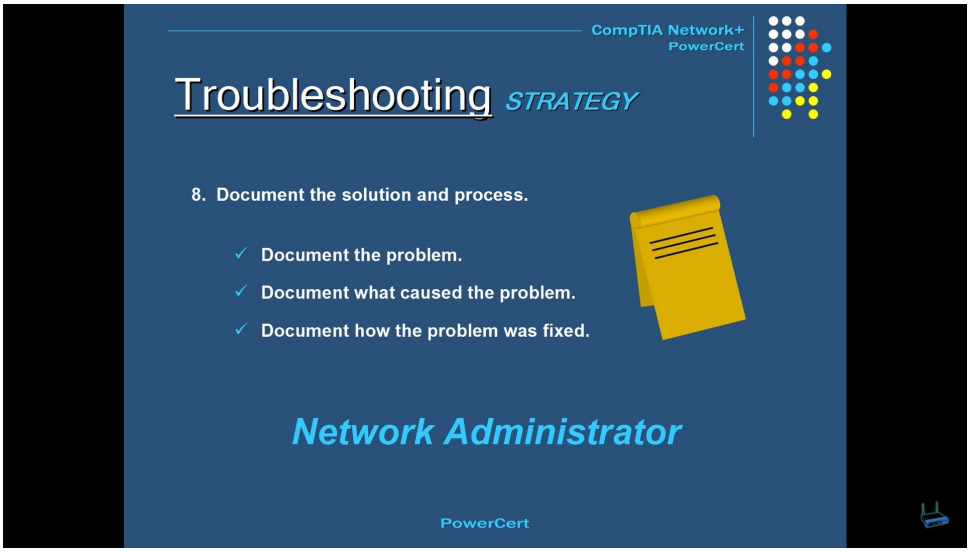

CompTIA Network+
PowerCert
Troubleshooting STRATEGY
3. Establish what has changed.
✓ Did anything change just prior to the problem happening?
✓ Was there any hardware removed or added?
✓ Was there any software installed or uninstalled?
✓ Was anything downloaded from the internet?
PowerCert


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

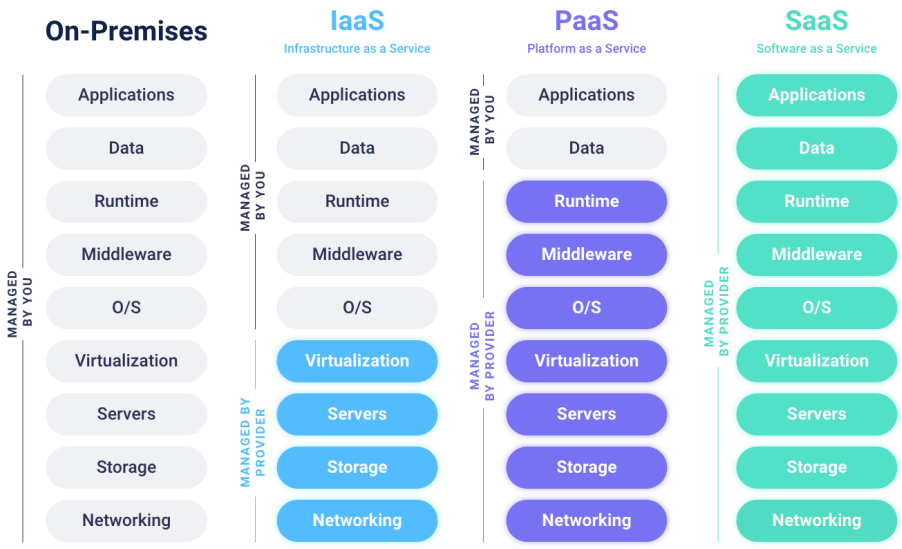

CompTIA Network+
PowerCert
Troubleshooting STRATEGY
5. Implement an action plan and solution including potential effects.
✓ The cautious phase.
✓ Must know what effect the action will have on the network.
✓ Will it affect the entire network or be isolated at one area?
PowerCert

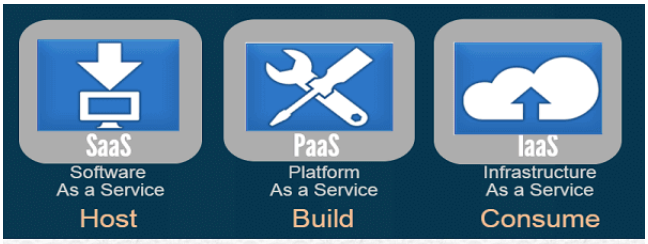

CompTIA Network+
PowerCert
Troubleshooting STRATEGY
6. Test the result.
✓ Where you take action to solve the problem.
✓ Where you will know if your plan of action will solve the problem or not.
PowerCert

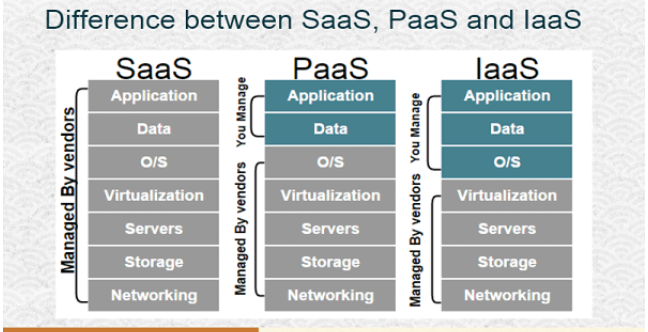


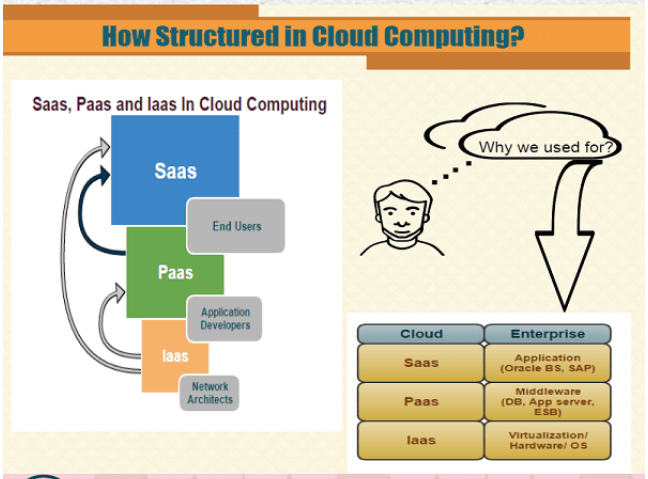


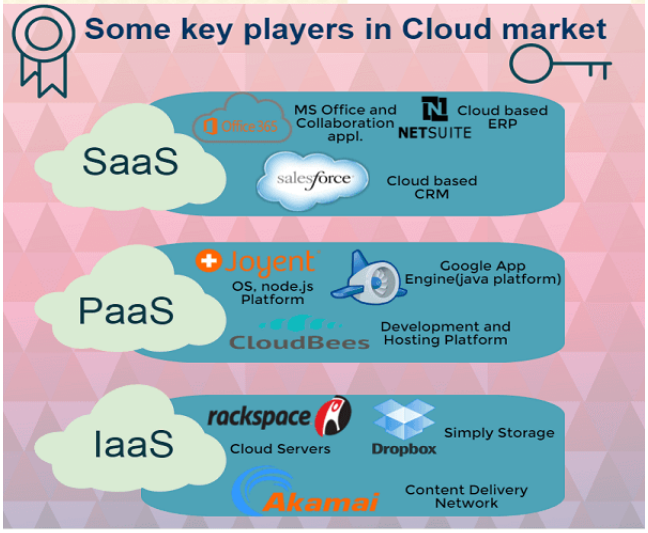
Could Computing - Iaas Paas Saas











ASSIGNMENT Help
changing the way we learn

-- Memo End --