Networking Concepts

By Jani Ahamed Habeeb Mohamed

Table of Contents

1. Introduction to Five Layer Networking Model

Physical Layer: Bits, connectors and cables across devices with their signal patters
Data Link Layer: Frames, Ethernet/Wifi protocol standards operating on MAC addresses. They define standards as to how these bit signals have to be interpreted in a common way for network devices to communicate. The Ethernet standard defines protocols to get data to nodes on the same network or link.
Network Layer: Packets/Datagrams, IP address, Allows different networks to communicate with each other through routers. Internetwork is a collection of networks connected through router (Internet). IP is the heart of the network.
Transport Layer: Segments, TCP/UDP, Ports, Determines which client and server programs are supposed to get the data.
Sessions Layer: Creates setup, control/tears down the connection between local and remote application. (Full/Half Duplex communication) and establishes procedure for checkpointing, suspending, resuming and terminating a session between two related streams of data such as audio and video in web conferencing.(implemented in places which use Remote Procedure Calls)
Presentation Layer: Translates/does certain things required by application layer to bundle messages before sending/while receiving. Data formatting (encoding/decoding), compression/decompression (ASN, XML, EBCDIC, ASCII)
Application Layer: Messages, HTTP/SMTP, different application interact over web.

2. Network Devices

Cables :
Send signals between connected devices (point to point communication)
Copper : (multiple copper wires inside plastic insulator – changes voltage between two ranges to distinguish binary data and send it in cables – Cat5, Cat5e (reduce cross talk – i.e electrical pulse on one wire accidentally detected on another wire), Cat6 (most efficient to avoid cross talks, expensive and shorter range)– number of twists in pair of wires determine the transfer rate and usable links)
Fiber : Contains optical fibers that are Individual tiny tubes made out of glass about the width of human hair. Uses pulses of light to transmit binary information of underlying data. Used in places where there is lot of electro magnetic interference as it may impact signals sent in copper cables. Quickest, expensive, more fragile and bigger range of transmission without bigger loss.

Single network devices:
Primary devices used to connect computers in a local area network.
Hubs: Physical layer device that allows connection from many computers at once. Data sent from one system is received by every other system connected to the hub. It's the responsibility of the system to ignore unwanted messages. This causes a lot of unwanted noise and creates a collision domain (network segment where only one device can communicate at a time – if multiple devices communicate, there will be interference of signals (data collision), this will force the system to get into a quiet period and then try sending again)
Switches: Data Link layer device that can inspect the contents of the ethernet protocol frames and determines which system the data is intended for and only send data to that system. Eliminates collision domains resulting in higher throughput an fewer re-transmissions.

Multiple network devices:
Used to connect computers across different networks
Routers: Network layer device that **k**nows how to forward data between independent networks. Router inspect IP data to determine where to send it to. Routers have an internal table which stores information about how to route data across the world. Most common routers are the one at home which takes data from home/office (home-office routers) and gives it to the ISP. The Internet service provider once has the data will use a sophisticated router(core/backbone routers) to send this data to the intended recipient. Core routers are connected to many other routers to determine the right path and use Border Gateway Protocol (to share data with each other router and to get to know the most optimal path to forward traffic)

Servers and Clients:
Something providing the data is the server entity and something requesting or getting that is the client entity.

3. Physical Layer

Send signals between connected devices (point to point communication)
Copper cables carries constant electrical charge and bits are sent though that by a process called Modulation.
Modulation is a way of varying this voltage of the charge moving across the cable.
Line coding – electrical charge in a certain state is 0 or 1 (10 billion 0s/1s every second)
Twisted Pair Cable Pairs of copper wires twisted together. (single conduit of information) and helps prevents interference with twisting.Cat6 – 4 twisted pairs (duplex communication – information can flow in both directions simultaneously across the cable where as simplex is unidirectional), say 2 pairs of twisted cables for one direction communication and the other 2 pairs for other way communication. When something is degrading, full duplex turns to half duplex which means there is still 2 way communication but only one entity can communicate at any point of time.
Twisted pairs cables use four pairs of color coded copper wires (one solid and one striped)
Uni-shielded Twisted Pair: common, least expensive for home/office, basic protection from Radio Frequency Interference and crosstalk.
Shielded Twisted Pair: used in environments where RFI is a big problem. Braided Aluminum/copper shielding underneath the outer jacket to shield the four pairs of copper cables.
Foiled Twisted Pair: used in RFI prone environments, uses a thin foil that wraps the pairs of copper bundle

Straight through cables are knows as patch cables connect computers to hubs/switches.
A cable is straight through if color and stripe order are in same position on both ends
Computers and routers use: Pins 1 and 2 – orange wire for sending data Pins 3 and 6 – green wire for receiving data
Hubs and switches use: Pins 1 and 2 – green wire for sending data Pins 3 and 6 – orange wire for receiving data

Cross Over Cables: Used in older enterprise networks for direct connection.
Endpoint 1 of the Ethernet cable: Pins 1 & 2 - Green wires for sending data, Pins 3 & 6 - Orange wires for receiving data
Endpoint 2 of the Ethernet cable: Pins 1 & 2 - Orange wires for sending data Pins 3 & 6 - Green wires for receiving data

Network Ports and Patch Panels:
Twisted pairs are terminated with a plug (RJ45) that takes the individual internal wires and exposes them. RJ 45 cables are connected to RJ45 network ports on the devices. Link LED(will be lit when cable is properly connected between two powered on network devices) and Activity LED(will flash when the data transmission is happening) are present.
There might be network ports mounted on a wall. These ports will be connected to the network via cables that run through the walls and will eventually end in a patch panel (contains many network ports), its just a container for many end points. Cables then run from patch panels to switches or routers.

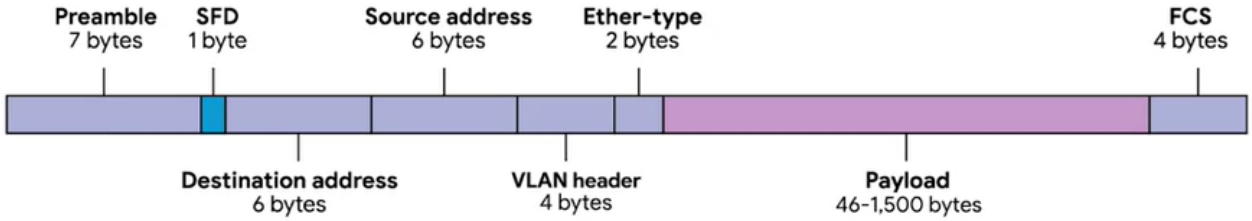
4. Data Link Layer

Ethernet – most common protocol used to send data across individual links. Provides an abstraction for the above layers from not caring about what is the kind of hardware used/physical layer.
Collision domain problem was solved by a technique called Carrier Sense Multiple Access with Collission Detection(CSMA/CD) – Used to determine when a communication channel is clear and is free to send data. Wait for a random interval when a collision is detected and then send.
Media Access Control Address (MAC) – globally unique identifier attached to a network interface.Its a 48 bit number represented by 6 groupings of 2 hexa decimal numbers
Octet: any number that can be represented by 8 bits
MAC address : 6 octets
First three octets : Organizationally unique identifier (OUI). These are assigned to HW manufacturers by IEEE.
Next three octets: Vendor assigned addresses
Unicast transmission is meant for one receiving address (Ethernet level – special bit in the destination MAC address)
Some quick examples of multicast MAC addresses:01:00.CC:CC.DD:DD and 09:00.AA:AA.BB:BB

Some quick examples of unicast MAC addresses:00:01:44:55:66:77 and 08:00:22:33.44:55

In an Ethernet MAC address, the least significant bit (LSB) of the first byte determines whether it is a unicast or multicast address. Specifically:
If the LSB is 0, it's a unicast address.
If the LSB is 1, it's a multicast address.
Let's examine the given MAC address: 0100.CCCC.DDDD
The LSB of the first byte (01) is 1.
Therefore, based on the LSB, this MAC address is a multicast address.
Broadcast is all Fs FF:FF:FF:FF:FF:FF
One set of binary data being sent from one point to another is data packet.
A highly structured collection of information presented in a specific order is ethernet frame.

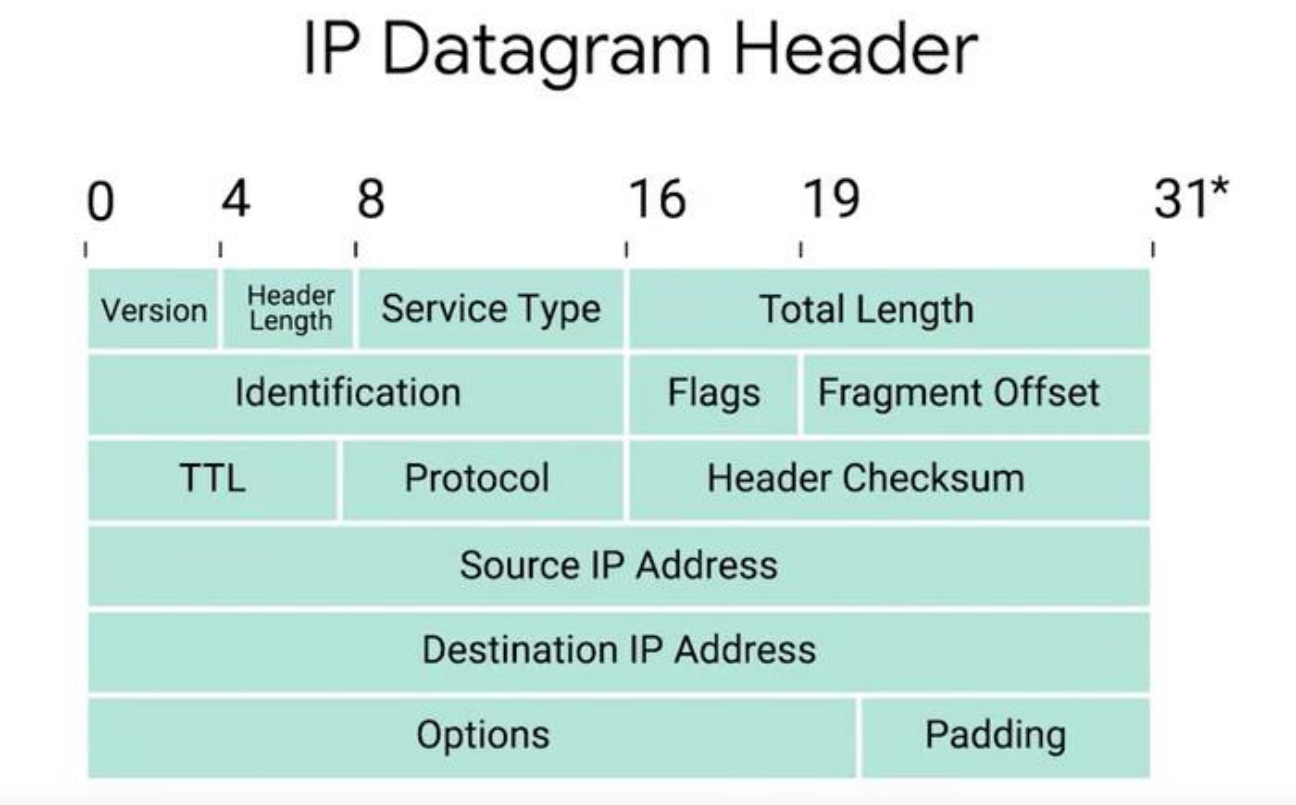
Dissect ethernet frame:



First 8 bytes (64 bits) – Preamble – split into two sections
First 7 bytes are bits if alternating 0s/1s used for internal clock synchronization for determining the speed of sending data or a buffer between frames and the last byte is the Start Frame Delimiter(SFD)
SFD will indicate the receiving device that the preamble is over and the actual data will follow
Destination MAC address 6 bytes : HW address of the intended recipient
Source MAC address 6 bytes: HW address of the sender.
Ether type : 2 bytes used to describe the protocol of the contents of the frame
Vlan Header : 4 bytes indicates this is a vlan frame, if a vlan header is present the ethertype follows it.
A virtual LAN is a technique that lets you have multiple logical LANs operating on the same physical equipment
Payload is actual data other than header 46 – 1500 bytes long
Frame check sequence : 4 bytes – checksum value for the entire frame. Checksum value is determined by Cyclical redundancy check against the frame. (used for data integrity)
A mathematical transformation that uses polynomial division to create a number that represents a larger set of data. It is an important concept for data integrity and is used all over computing, not just network transmissions

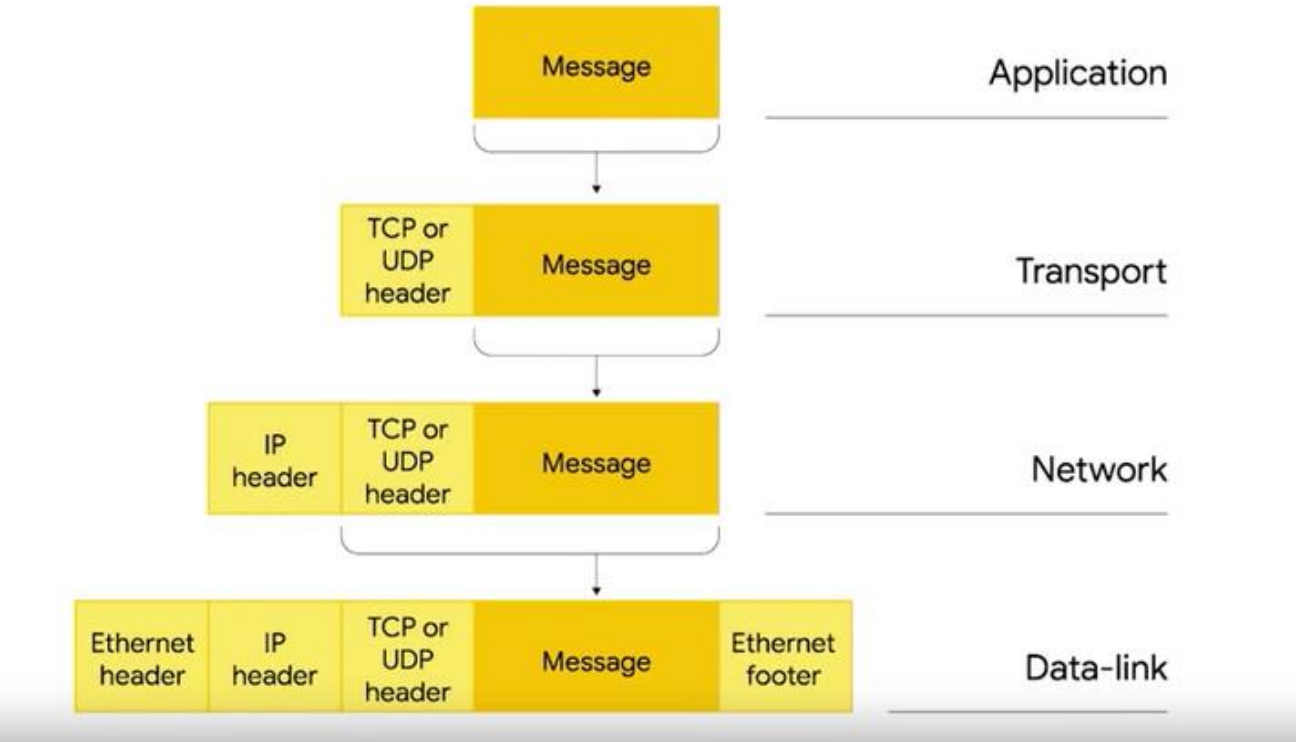
5. Network Layer

Dotted decimal format (12.34.56.78) – 32 bit 4 byte IP addresses.
IP addresses belong to the networks not to the devices attached to those networks.
Dynamic IP addresses are assigned through Dynamic Host Configuration Protocol (DHCP)
Static IP addresses are manually configured (servers and network devices)
Data packets in network layer are termed as IP data grams (packets) – a highly structured series of fields that are strictly defined.



Version (IPv4/IPv6) – first 4 bits
Header length (20 bytes (minimum length)– Ipv4) – 4 bits
Service Type field (8 bits – QoS related) – helps routers determine which IP datagram Is more important
Total Length – 16 bits – total length of the IP datagram its attached to.
Identification – 16 bits (used to group messages together)
The maximum size of a single IP data gram is 2^16 – 65535
If the size of data is more than what could fit in a single IP datagram payload, then IP splits those and tags then with same identification number so that the receiver could identify they are all part of same IP datagram
Flag (3 bits) – indicates if a datagram is allowed to be fragmented or has already been fragmented.
Fragment offset (13 bits) : Helps receiver to identify and put all fragments of a single IP datagram together.
TTL : 8 bits indicates how many router hops an IP data gram can hop before being thrown away. The main purpose of having TTL is because when there is a misconfiguration in network that could lead to endless cycle for datagram to try reaching a destination, decrementing this value leading to 0 on the way will discard the packet.
Protocol (8 bits) – what kind of transport protocol is being used – tcp/udp
Header checksum : 16 bits checksum for the entire IP datagram header. Since TTL gets modified at each router, checksum also changes.
Src IP address – 4 bytes – 32 bits
Dst IP address – 4 bytes – 32 bits
Options field (20 bits) – set special characteristics for datagrams used for testing purpose
Padding field (12 bits) – variable just to accommodate to a series of 0s to ensure header is correct total size.

Encapsulation is putting all these IP datagrams inside the ethernet payload.



IP addressed have two sections : Network ID (first octet)/Host ID(2nd,3rd and 4th octet)
Address class system : defining how global IP address space is split up.

Class A: Network ID (first octet)/Host ID(2nd,3rd and 4th octet)
Class B: Network ID (first, second octet)/Host ID(3rd and 4th octet)
Class C: Network ID (first, second and third octet)/Host ID(4th octet)

Class	Left-most bit	Starting IP address	Last IP address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

Address resolution Protocol(ARP) – used to identify the MAC address tied to an IP address
ARP table : list of IP and MAC address mapping
The process of taking a larger network and splitting it into smaller networks is subnetting

Picks up a portion of the host ID to form the subnet ID to break into smaller networks.
Core routers only care about network ID and send it to the Gateway router.
Gateway router uses additional information to send to the actual destination machine or the next router in path. Finally the host id is used to deliver the packet to the recipient.

Subnet masks are 32 bit numbers written out in four octets in decimal.

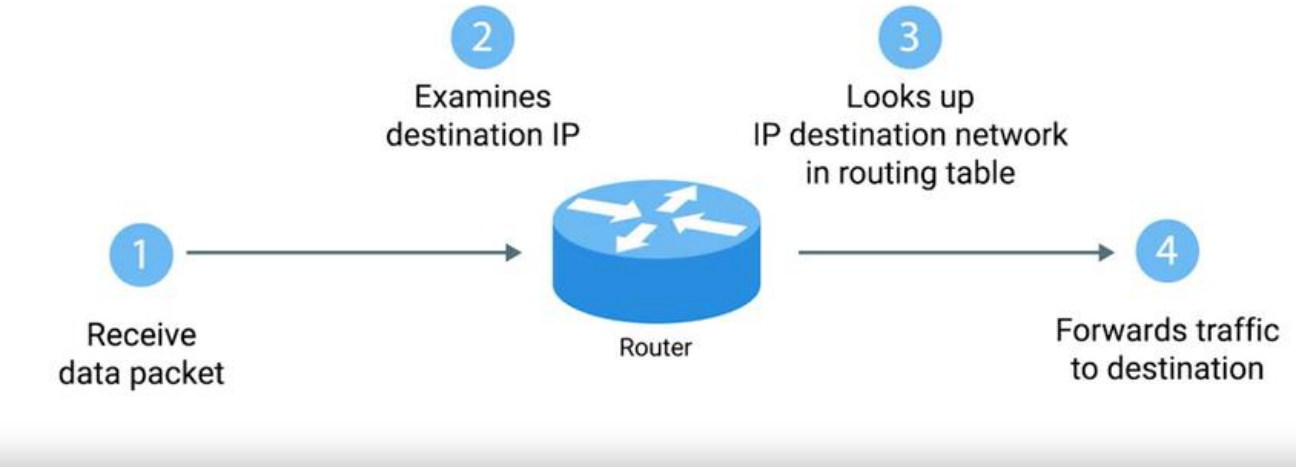
IP address	9	100	100	100
IP address *(in binary)*	0000 1001	0110 0100	0110 0100	0110 0100
Subnet mask *(in binary)*	1111 1111	1111 1111	1111 1111	0000 0000

255.255.255.0

First 8 bits are Class A network ID. Remaining are host IDs
However since subnet mask is 255.255.255.0, the second and third octet are the subnet IDs and the last octet of the subnet mask, since its 0, the corresponding IP address part Is the host ID.
Hosts can be assigned 1 – 254 as 0 is not used and 255 is from broadcast.

Router:
A router forwards traffic based on the destination IP address of that traffic.
Router will atleast be connected to two networks to route traffic

Basic routing:



9.100.100.100

255 . 255 . 255 . 224

11111111 11111111 11111111 11100000

/27

Shorthand is to just tag ip with /number of 1 bits in subnet mask.

Classless Inter Domain Routing: (CIDR)
Demarcation point is where one network or system ends and another one begins
With subnets, network IDs were same size and portion of host id was used for subnet IDs.
But with CIDR, even the network IDs are usable

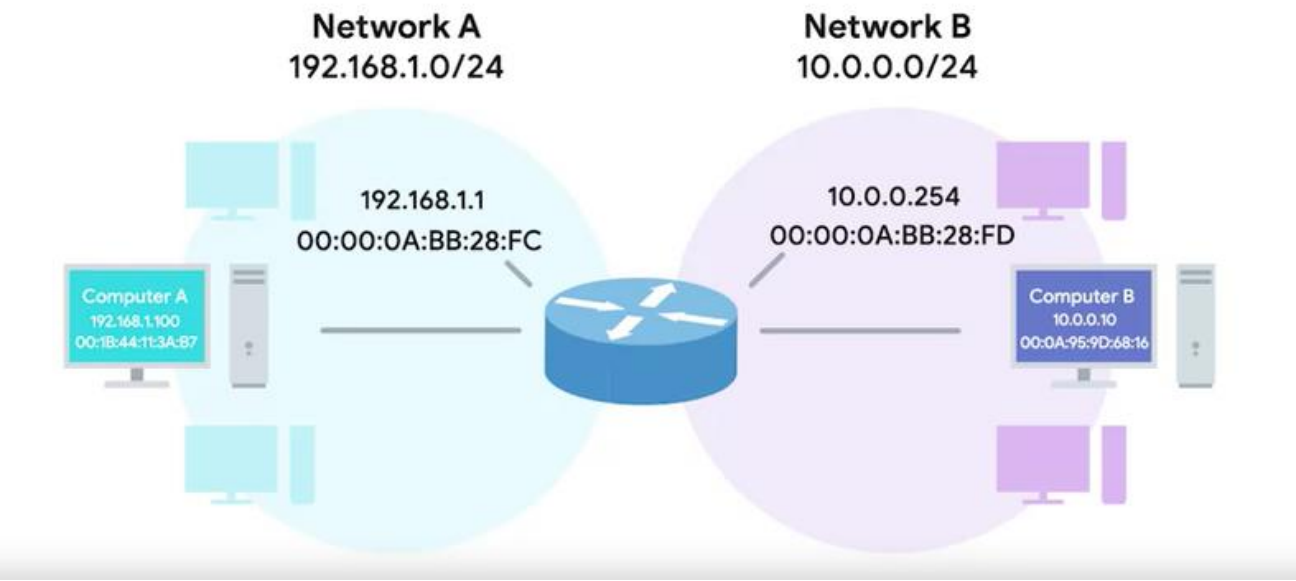
/24 network is 8 host bits. 2^8 = 256

256 - 2 = 254

254 + 254 = 508

/23 network is 9 host bits. 2^9 = 512

512 - 2 = 510



Packet from 192.168.1.100 to 10.0.0.10
So, Src: IP computer A, Dst IP: Computer B, Src MAC: Computer A, Dst MAC: Gateway
Computer A knows this IP is not local, so it sends it to the MAC address of the Gateway
Router now receives on interface 1 and removes the ethernet layer inspects the IP header and sees the destination IP field and gets to know from its routing table that the network 10.x.x.x is reachable via interface 2.
Now it construct a new ethernet header with src MAC as his and dest MAC as Computer B MAC and decrements TTL and recalculates checksum.
Router has routing table and ARP table
So L2 MAC (src changes on every hop) during routing, whereas Ips remain the same.

MAC table:

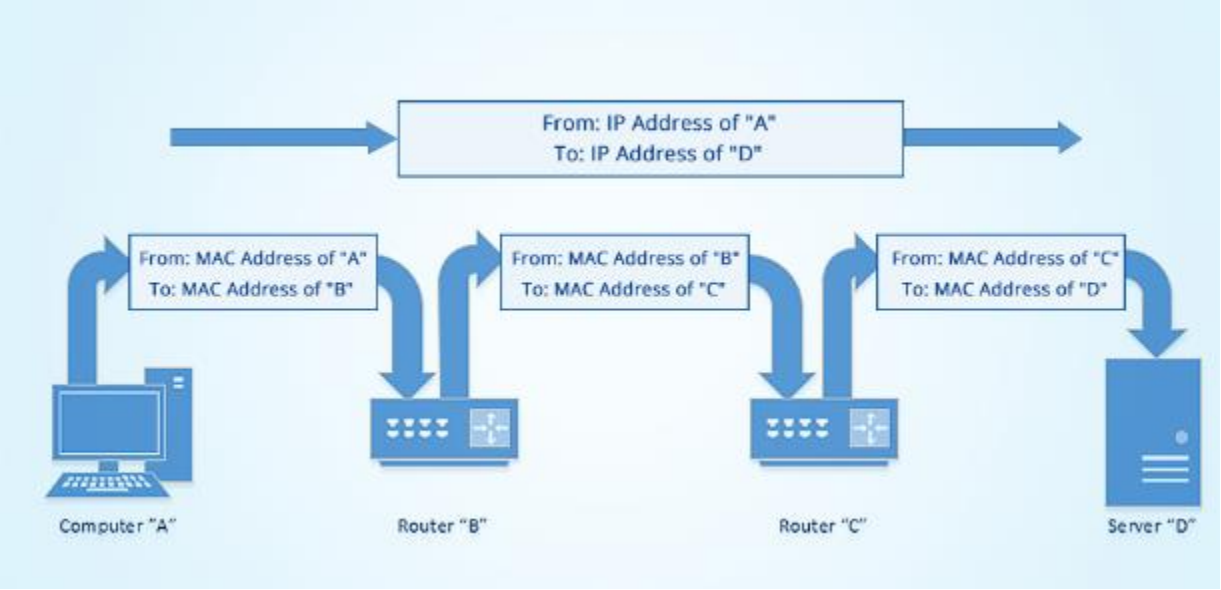
```
MAC Address       Address         Name                Interface           Flags
00:00:5e:00:01:0c 10.159.16.1     10.159.16.1         fxp0.0              none
fc:33:42:fe:dc:57 10.159.16.3     10.159.16.3         fxp0.0              none
9c:cc:83:8d:70:78 10.159.16.54    10.159.16.54        fxp0.0              none
00:a0:a5:7f:73:04 10.159.17.159   10.159.17.159       fxp0.0              none
00:a0:a5:9f:a0:c8 10.159.18.1     10.159.18.1         fxp0.0              none
44:aa:50:96:aa:19 30.65.0.2       30.65.0.2           fab0.0              permanent
30:b6:4f:8c:a7:07 30.66.0.1       30.66.0.1           fab1.0              permanent
fe:00:00:00:04:00 129.64.0.16     129.64.0.16         em0.0               none
fe:00:00:00:04:00 129.64.0.17     129.64.0.17         em0.0               none
aa:bb:cc:dd:ee:ff 192.168.1.1     192.168.1.1         em2.32768           none
```

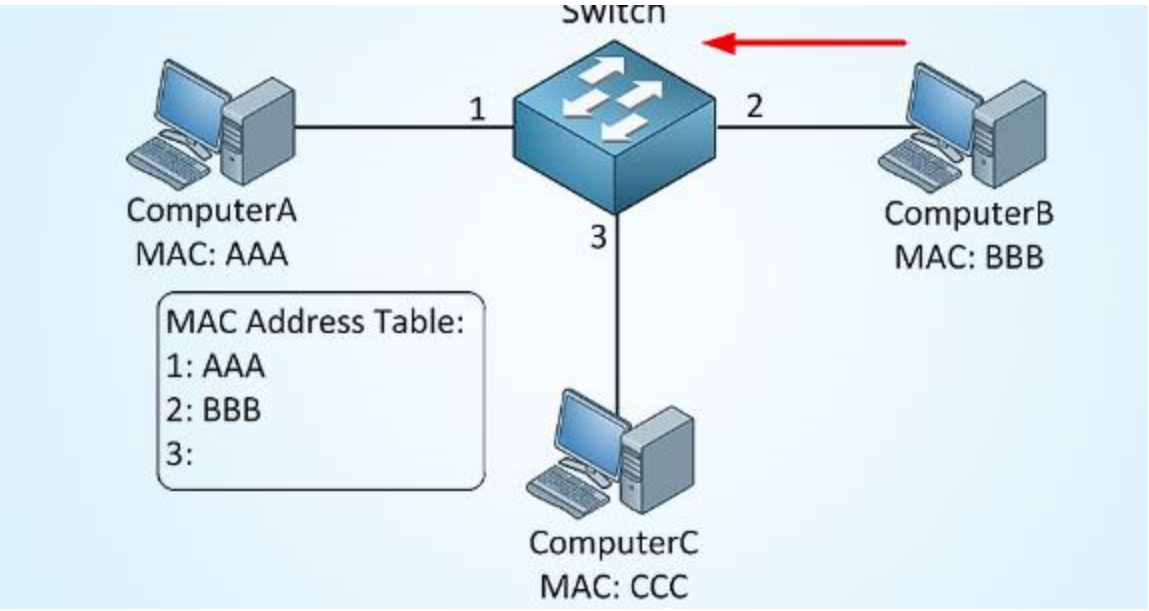
Routing table:

Basic Routing Table

Destination network	Next hop	Total hops	Interface
192.168.1.1/24	192.173.0.1	5	192.173.0.254
101.66.27.0/24	10.11.0.1	3	10.11.0.25
192.25.67.0/24	10.0.0.3	10	10.0.0.254

Nexthop is the ip address if the next router that should receive the data intended for the network under question and it is reachable via a certain interface and is certain hops away.





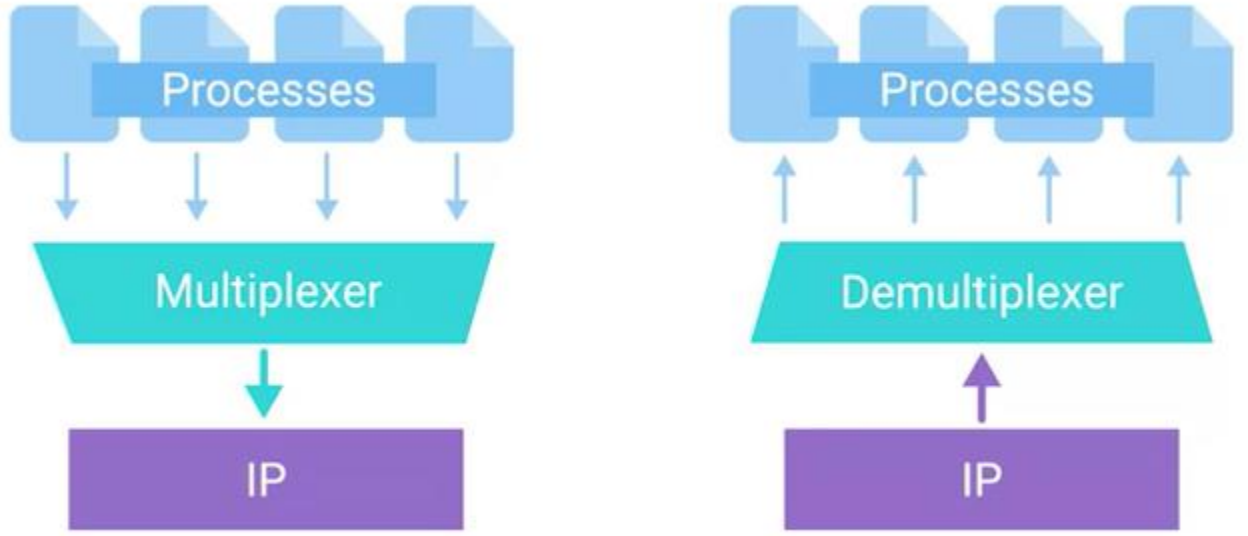
Routing protocols are used to learn about routes across the globe.
Interior (within an AS) and Exterior Gateway Protocol(between AS)
Interior : distance vector – every router has it own routing table where it maintains the distance or the number of hops for every other network and publishes it – no idea about the entire AS rather just basic information about neighboring router -> (RIP) and link state routing protocol (OSPF) – every interface of the router propagates all link related information to all other routers in the AS, then running Djikstra's algorithm the optimized shortest path for a destination network is determined.
Exterior : Border Gateway protocol (between routers on the edge of AS)
IANA – Internet Assigned Numbers authority maintains assignment of ASN and IP address assignment.

Non routable Address Space: Ranges of Ips set aside for use by anyone that cannot be routed to.
In non routable address space computers talk to each other but no gateway router will try to reach this network.

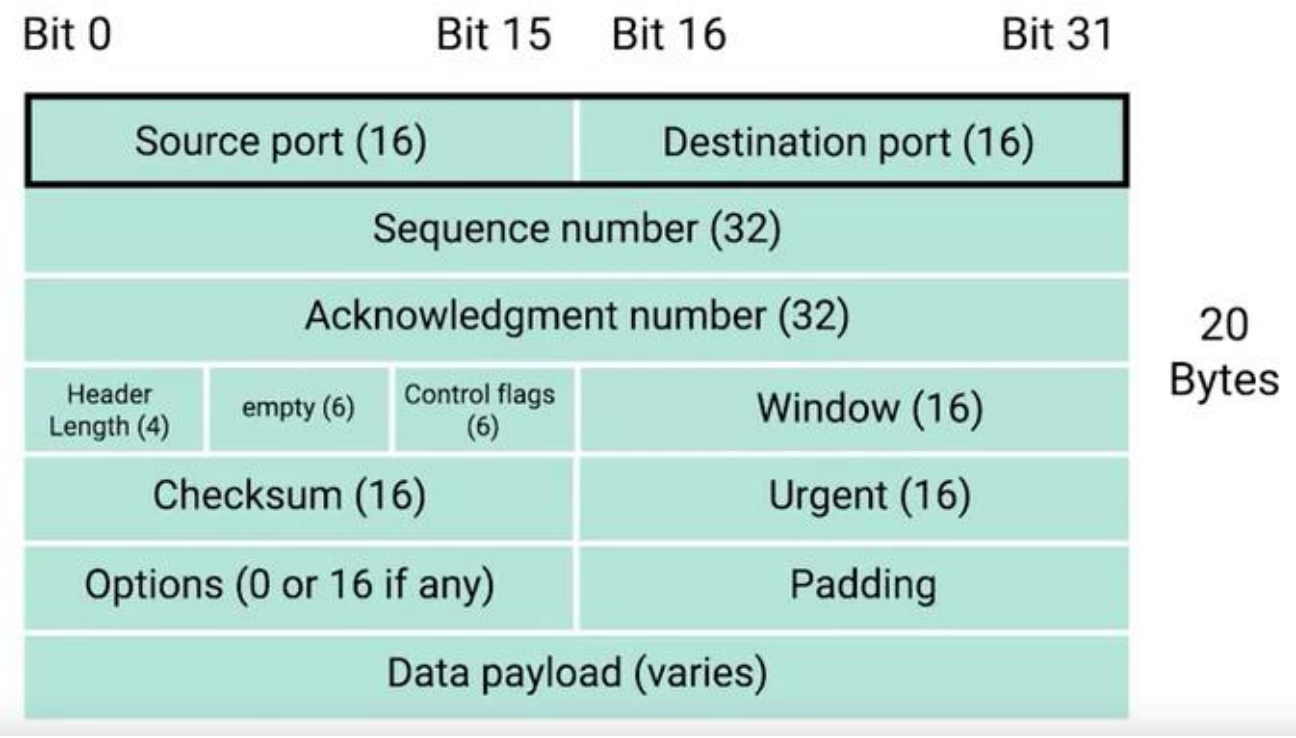
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

6. Transport and Application Layer

Programs running on the system in the network should be able to talk to each other.
Transport layer allows traffic to be redirected to specific network applications
Application layer allows applications to communicate in a way they understand.

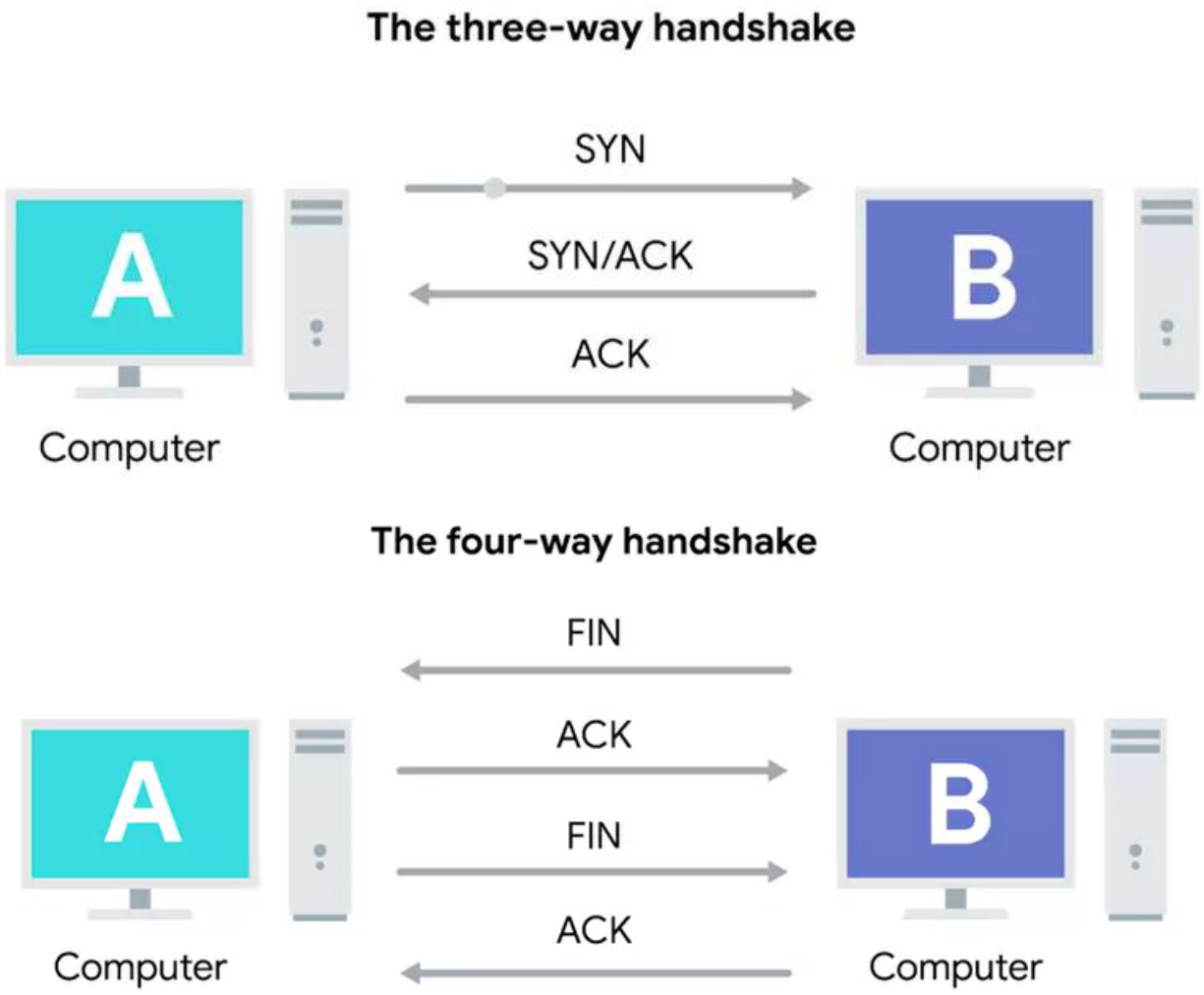


Multiplexing/Demultiplexing is done based on port numbers (16 bit number) that's used to redirect traffic to specific services in a computer.
10.1.1.100:80 – socket address/number
http : 80
ftp : 21
smtp : 25
printer : 9100
IP payload has TCP segment which is TCP header + data section.



Destination Port : Port of the service that the traffic is intended for
Source port or ephemeral ports : high numbered ports chosen from special section of ports (lot of outgoing connections separate)
Sequence number: 32 bit number used to keep track of where in a sequence of TCP segments this one is expected to be.
Acknowledgement number : number of the next expected segment
Data offset or Header length: 4 bit number that communicates how long the TCP header for this segment is
Empty : 6 bits
Control TCP flags : 6 bits
Window : 16 bits specifies the range of sequence numbers that might be sent before an acknowledgement is required
Urgent: is used in conjunction with tcp control flags to point out particular segments that might be more important than others.
Options: used for more complicated flow control protocols
Padding : makes sure payload starts at specified location.
Synchronization (SYN) – It is used in first step of connection establishment phase or 3-way handshake process between the two hosts. Only the first packet from sender as well as receiver should have this flag set. This is used for synchronizing sequence number i.e. to tell the other end which sequence number they should accept.
Acknowledgement (ACK) – It is used to acknowledge packets which are successful received by the host. The flag is set if the acknowledgement number field contains a valid acknowledgement number.
In given below diagram, the receiver sends an ACK = 1 as well as SYN = 1 in the second step of connection establishment to tell sender that it received its initial packet.
Finish (FIN) – It is used to request for connection termination i.e. when there is no more data from the sender, it requests for connection termination. This is the last packet sent by sender. It frees the reserved resources and gracefully terminate the connection.
Reset (RST) – It is used to terminate the connection if the RST sender feels something is wrong with the TCP connection or that the conversation should not exist. One of the sides of the TCP connection hasn't been able to properly recover from a series of missing malformed segments.
Urgent (URG) – It is used to indicate that the data contained in the packet should be prioritized and handled urgently by the receiver. This flag is used in combination with the Urgent Pointer field to identify the location of the urgent data in the packet.

Push (PSH) –Transmitting device wants the receiver to push currently buffered data immediately to the application on the receiving side. It is used to request immediate data delivery to the receiving host, without waiting for additional data to be buffered on the sender's side. This flag is commonly used in applications such as real-time audio or video streaming.
Window (WND) – It is used to communicate the size of the receive window to the sender. The window size is the amount of data that the receiving host is capable of accepting at any given time. The sender should limit the amount of data it sends based on the size of the window advertised by the receiver.
Checksum (CHK) – It is used to verify the integrity of the TCP segment during transmission. The checksum is computed over the entire segment, including the header and data fields, and is recalculated at each hop along the network path.
Sequence Number (SEQ) – It is a unique number assigned to each segment by the sender to identify the order in which packets should be received by the receiver. The sequence number is used in conjunction with the acknowledgement number to ensure reliable data transfer and to prevent duplicate packets.



Socket: The instantiation of an end point in a TCP connection.
Listen : A TCP socket is ready and listening for incoming connections (server)
SYN_SENT: A synchronization request has been sent but connection not established yet (client)
SYN_RECEIVED: A socket previously in Listen state has recevied a SYN request and has reponded with SYN/ACK. (server)
Established: TCP connection is in working order and both sides are free to send data(client and server)
FIN_WAIT: A FIN has been sent but ACK has not been received

CLOSE_WAIT:The connection has been closed at the TCP layer but the application that opened that socket connection has not released hold on the socket yet.
CLOSED: The connection has been completely closed and no further communication is possible.

System Ports are identified as ports 1 through 1023. System ports are reserved for common applications like FTP (port 21) and Telnet over TLS/SSL (port 992). Many still are not assigned. Note: Modern operating systems do not use system ports for outbound traffic.

User Ports are identified as ports 1024 through 49151. Vendors register user ports for their specific server applications. The IANA has officially registered some but not all of them.

Ephemeral Ports (Dynamic or Private Ports) are identified as ports 49152 through 65535. Ephemeral ports are used as temporary ports for private transfers. Only clients use ephemeral ports

Firewall : device that blocks traffic that meet certain criteria

Apache Microsoft IIS and nginx are all web servers
Session layer is responsible for facilitating communication between actual applications and tranport layer
Presentation layer makes sure unencapsulated application layer data is able to be understood by the application (encryption/compression).

7. Network Services

DNS – Domain Name System – mapping between domain names and their respective IPs(name resolution)
Domain Names : Something that can be resolved by DNS
For specific HW – there is MAC address
For every node in the N/W – IP address, Subnet Mask, Gateway Address and DNS server
Caching Name Servers – provided by ISP(Store known domain name lookups for a certain amount of time) - caching
Recursive Name Servers – provided by ISP (Store known domain name lookups for a certain amount of time) – performs full DNS resolution requests
TTL is the time to live – configured by owner of domain name for how long a name server is allowed to cache an entry before doing a full resolution again.
Anycast: route traffic to different destinations depending on location, congestion or link health.
Root Name Servers – 13 authorities that provide root name lookup as a service. Root servers respond back to the DNS requests with a TLD name server that has to be queried
TLD Name Servers – Top level domain, represents top of the hierarchical DNS name resolution system
For each TLD there is a TLD name server
www.google.com (com is TLD)
TLD responds with what authoritative name server to contact (anycast)
Authoritative Name Servers – actual organization that holds the site – actual IP is returned from here

DNS (port 53) uses UDP (request and response for dns lookup can fit in a single datagram of udp)
DNS application has error recovery – will query again if response not received
If DNS response it too big to fit in a UDP datagram, response is given as too large, then DNS over TCP is used.

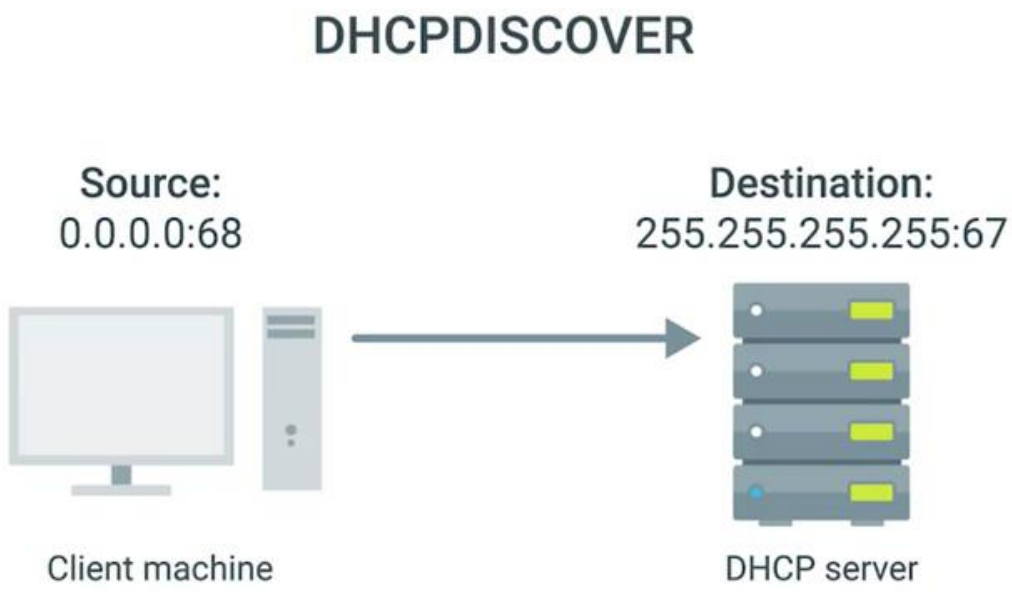
Resource Record Types:
A Record: Used to point a certain domain name at a certain IPv4 address
Single domain name can have 1 or more A record (DNS round robin)
Quad A record – Ipv6 instead of Ipv4 (round robin is used for load balancing of traffic rate to a web site handled by multiple A records)
CNAME record: Used to redirect traffic from one domain to another domain name (Microsoft.com to www.microsoft.com)
By setting canonical names, maintainability is easy), if ip changes just one A record change is done.

MX Record: Mail exchange record – resource record to deliver mail to correct server
SRV (service record) – define location of various specific services – calendar and scheduling
(TX)Text record:some descriptive text for a domain
Administration and definition of TLDs is done by ICANN Internet Corporation for Assigned Names and Numbers
.com – Top level domain
Google – domain (where control moves from TLD name server to authoritative name server)
Www – sub domain
Fully Qualified Domain Name
A registrar is some one who can sell unregistered domain names – has agreement with ICANN
DNS can support upto127 levels of domain in total for a single FQDN
Each individual section can only be 63 characters long
Complete FQDN is 255 characters long.
DNS Zones – allows for easier control over multiple levels of domain.
Zone files : Simple configuration files that declare all resource records for a particular zone.
Contains SOA (start of authority – declares the zone and the name of the name server that it is authoritative for), resource record declaration
NS records - other names servers responsible for this zone.
Reverse lookup zone files:DNS resolveres ask for an IP and get the FQDN with it returned

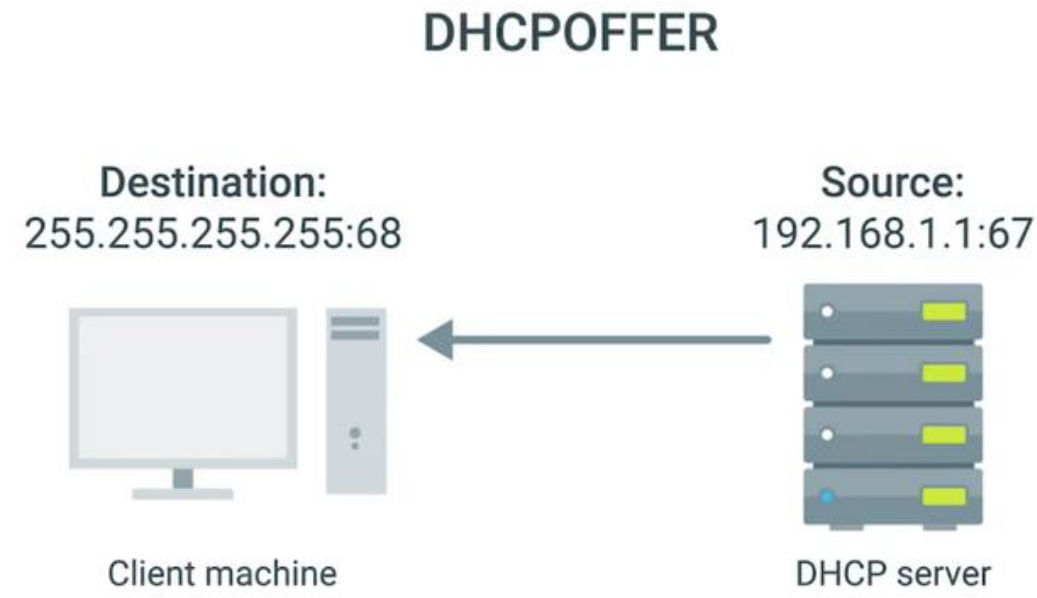
DHCP :Dynamic Host Configuration Protocol : Application layer protocol that automates the configuration process of hosts on a network.
Dynamic IP allocation to hosts connecting to it and requesting

Automatic allocation : A range of IP addresses is set aside for assignment purposes
Fixed allocation:Requires a manually specified list of MAC/IP addresses

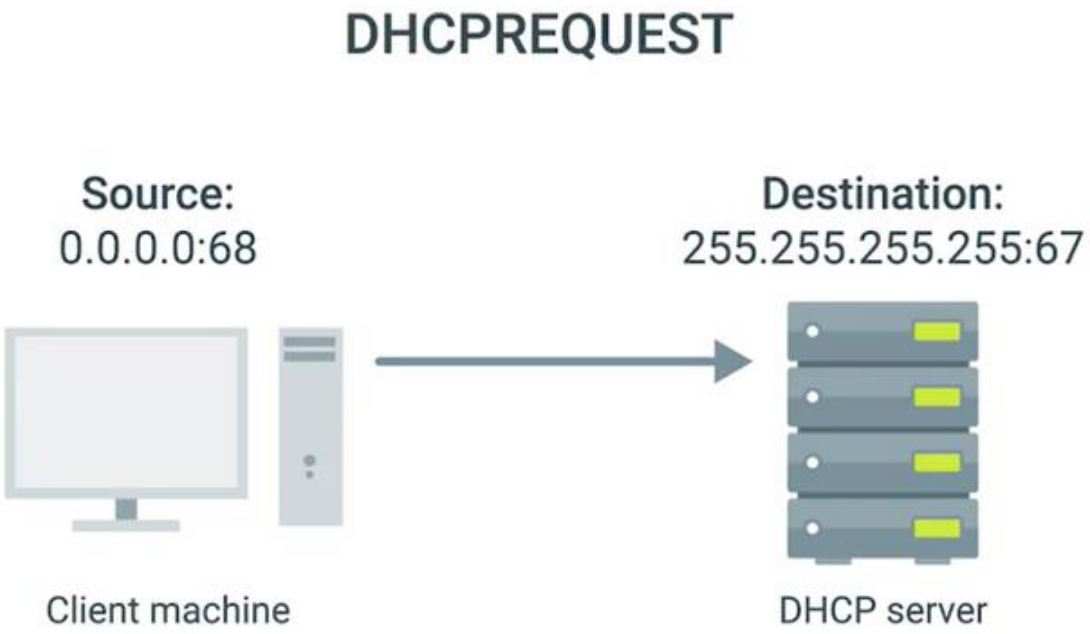
NTP : Network Time Protocol – used to keep all computers in network synchronized in time.
DHCP discovery: the process by which a client configured to use DHCP attempts to get network configuration information.
Client sends DHCP discover message to find DHCP server
DHCP listens on UDP 67, all DHCP requests are sent from port 68 to a broadcast destination IP
Src ip : 0.0.0.0 dst ip 255.255.255.255
Every node of the local area network gets the request



Response is DHCP offer message



Offer is also broadcast, received by every host, but the response will have information of client MAC address
DHCP client can respond to the offer with DHCP request message



DHCP ACK is sent back and IP assignment is done
DHCP Lease
DHCP uses transaction IDs
1hr limit

Network Address Translation (NAT) is a technology that allows the gateway usually a router or firewall to rewrite the source IP of an outgoing IP datagram while retaining the original IP inorder to rewrite it into the response.
IP masquerading – a firewall having NAT changing the src ip of packet from host to itself (one to many NAT)
Port preservation : src port used by host is the same used by router
Port forwarding : where specific destination ports can be configured to always be delivered to specific nodes.

Virtual Private Networks:
Allows extension of a private or local network to hosts that might not work on the same local network
Tunnelling protocol
Remote client gets a virtual interface assigned with ip which is of the same address space of the network that the VPN is established to
VPNs work on the payload section of the Transport layer to carry an encrypted payload that carries an internal set of packets (network . transport and application layer)
Two factor authentication is used by VPNs
Proxy Service : A server that acts on behalf of a client in order to access another service
Anonymity, security, content filtering, increased performance.
Reverse Proxy: A service that might appear to be a single server to several clients but actually represents many servers living behind it.

8. POTS, Dial Ups and Wireless

Dial up connection uses POTS for data transfer by actually dialing a phone number. – MODEMS
From PC digital to MODEM and then converted to ANALOG through telephone exchange.
Baud rate – how many bits can be transferred over a second in a phone line
Public switched telephone network
Anything that isn't dialup is broadband
T carrier technologies invented by AT&T to transmit multiple phone calls over single link
Digital Subscriber lines – Digital subscriber Lines Access Multiplexers (DSLAMS)
ADSL – Asymettric – faster download and slower upload
SDSL – Symmetric – same speed upload/download
HDSL – High bit rate
Cable Broadband – shared bandwidth technology – managed by cable modem. Device that sits on edge of consumer network connect it to cable modem termination system
FTTX, FTTN – Fiber to the neighborhood and then COAX
FTTP – to the building
FTTH – to the home
FTTP – to the premises
Optical network terminator – converts data from protocol the fiber can understand to those that twise copper can understand.

Point to Point – Site to Site VPNs between Devices
IEEE 802.11 Wireless standard(wifi) – radio waves
Frequency band : A certain section of the radio spectrum that's been agreed upon to be used for certain communication(North America radio Frequency FM bands - 88 and 108MHz)
Wifi 2.4 and 5 Ghz bands
802.11b
802.11a
802.11g
802.11n
802.1ac
802.11 – physical and data link layers

Frame control field

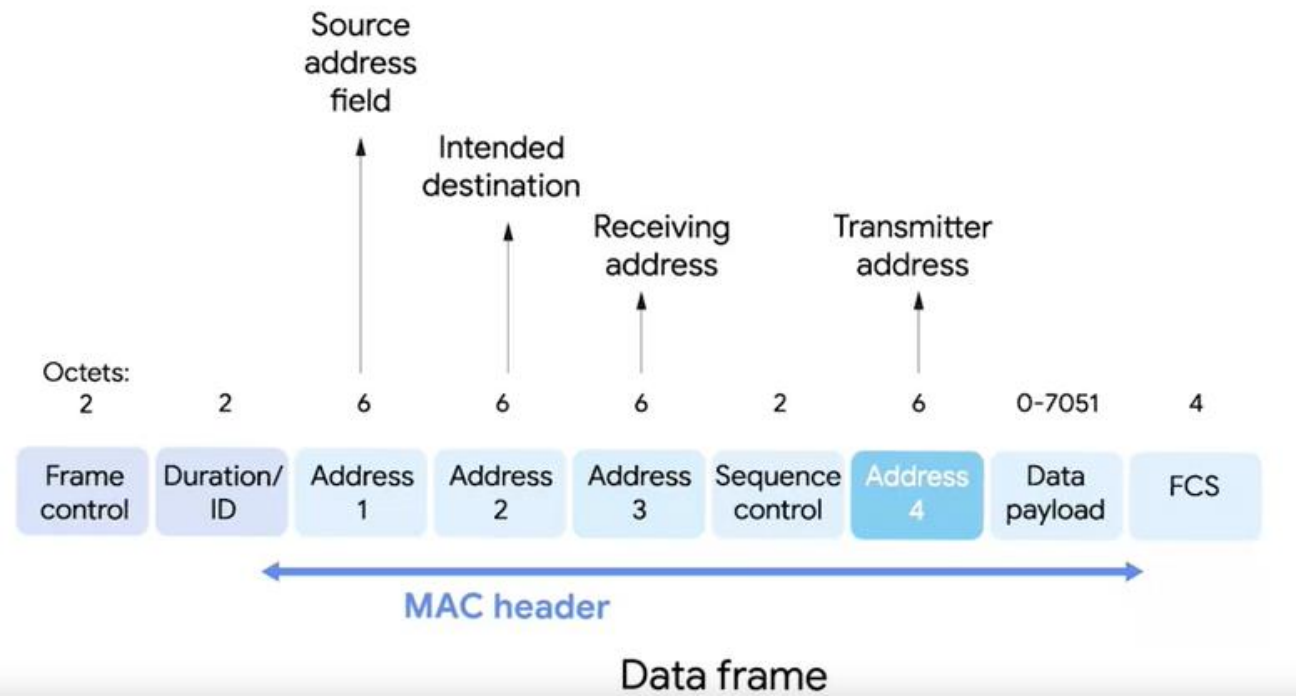
Is 16 bits long and contains a number of subfields that are used to describe how the frame itself should be processed

Duration field

It specifies how long the total frame is, so the receiver knows how long it should expect to have to listen to this transmission

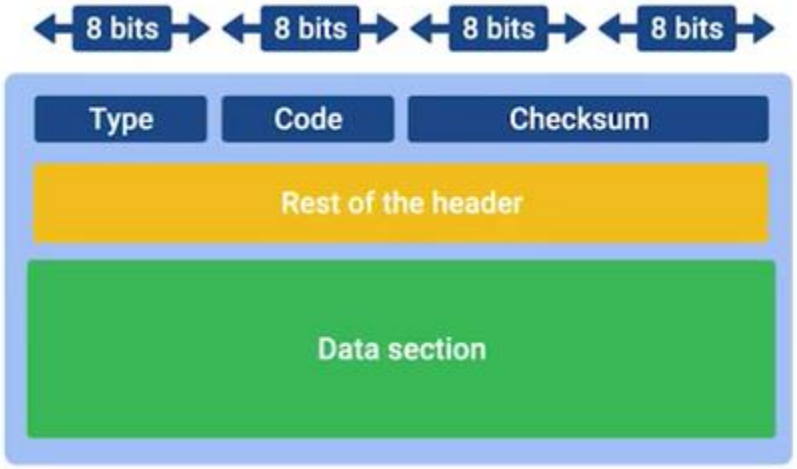
Wireless access point

A device that bridges the wireless and wired portions of a network



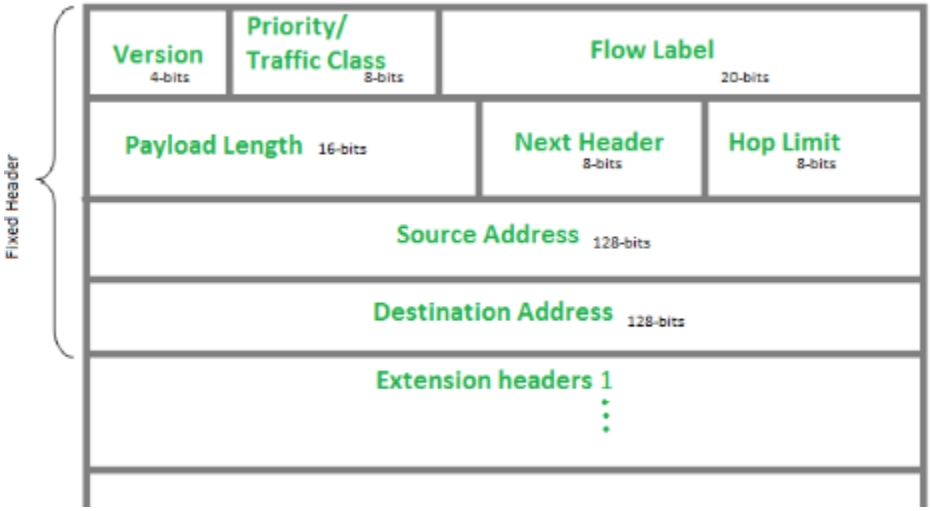
Adhoc networks where devices talk directly to each other
WLANS – where access points help talk
Mesh – hybrid of above
Channels are individual smaller sections of the overall frequency band used by wireless network
WEP (wired equivalent privacy) – low level privacy encryption
Wifi protected access
WPA2 – 256 bit key
MAC filtering

ICMP:



Traceroute send packets with increased ttl to find intermediate paths
Netcat nc (can send application data through keyboard) input is host and port
Nslookup for name resolution
Public name servers – anyone can use (level 3 – 4.2.2.1 to 4.2.2.6), 8.8.8.8 8.8.4.4 (google)
Original way numbered network addresses were corelated to words – host files
A single physical machine(host) could run many individual virtual instances called guests
Hypervisor : software that runs and manages the virtual machines while offering these guests a virtual Operating platform that's indistinguishable from actual hardware

Public cloud – large cluster of machines run by another company
Private clouds – own premises physically hosted
IAAS - no worry about building own servers or network
PAAS – platform is provided to run their services
SAAS – software centrally managed and licensed for use
2001:0db8 – reserved ipv6 for documentation and education
FF00:: multicast
::1 loopback
FE80:: link local unicast addresses
64 network + 64 host = 128 bits



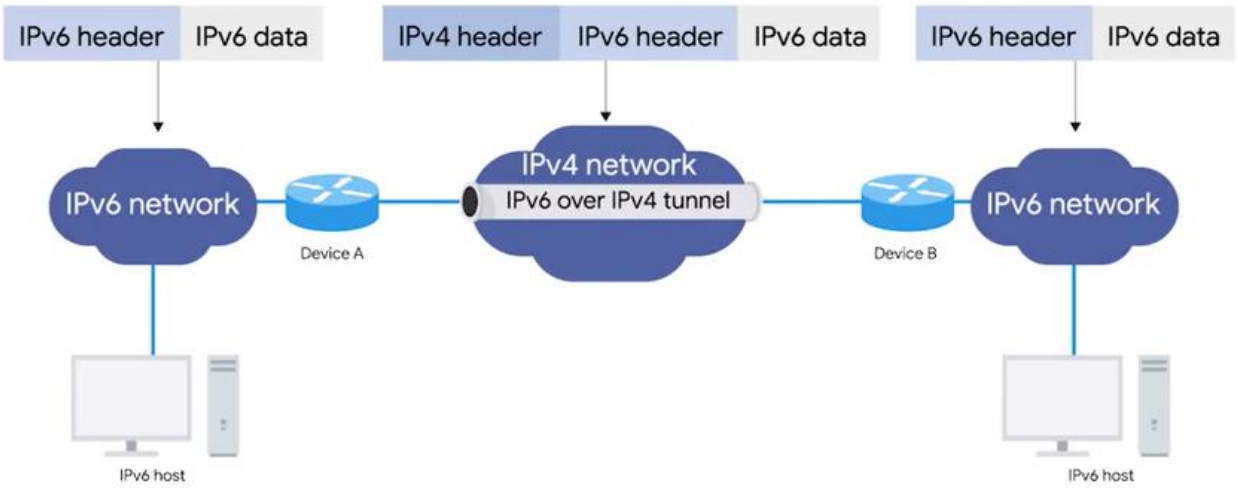
Version (4 bit) + 8 bit (traffic class) + flow label(20 bit) -> QOS + 16 bit payload length + 16 bit next header 8 bit hop limit ttl + src and dst ip + data payload

192.168.1.1 = 0:0:0:0:0:ffff:c0a8:0101

Mapped ipv4 address

IPv6 tunnels

Servers take incoming IPv6 traffic and encapsulate it within traditional IPv4 datagram



IPv6 tunnel broker

Companies that provide IPv6 tunneling endpoints for you, so you don't have to introduce additional equipment to your network

9. DNS

Actually in a URL there is a final .
www.website.com. (last dot) is the root server out of 13 (FQDN -> Fully qualified domain name)
Domain naming server or system
Root Server - > top level domain server
.com -is TLD
SLD -> second level domain server (www.learning.linkedin.com)
Domain names are reserved and registered by domain registrar(ICANN register)
Subdomain(learning)
Forward(domain to ip) and reverse lookup(ip to domain)
Authoritative name server is the ip which actually holds the domain or service we are looking for

DNS lookup happens with DNS resolver (it could be on your PC or LAN or internet)
DNS resolver returns the information in its cache (non recursive query)
DNS response is marked as non-authoritative
DNS resolver does a recursive lookup if it does not have the information (authoritative)
Recursive name servers only know about root name servers
Dig is a linux command for looking up DNS records
A record – ipv4 address
Quad A record – IPV6 address
TTL – amount of time dns resolver will store this record in cache
CNAME – short canonical form for the actual website address we are typing in -> FQDN
MX – mail exchange records (preference – lower the better among many)
SPF – sender policy framework or TXT record – authenticate incoming/outgoing mail (human readable notes)
NS – name server - has all name servers included
SOA – start of authority – name, serial, refresh, expire , ttl (primary name server)
PTR – opposite of A and AAAA (reverse lookup)
SRV – Service – some additional info required for instant messaging service

DNS forwarding – forwarding to external DNS resolvers (public)
DNS Security – spoofing – (attacker changes the domain name)
DNS hijacking – redirect to wrong dns server
DNS Cache poisoning – alter dns records in server
Change DNS port settings, redundant DNS Server
DNSSEC- checks the authenticity of DNS queries using digital signatures, firewall

Cat /etc/resolv.conf – dns server(name server)
/etc/hosts
Dns lookup – host
Nslookup
Dig
resolvectl

HTTP is stateless but not session less (maintains cookies to remember some states)
Server will place cookies in the browser cache and next time that information from cache is sent back to the server
First TCP established
Then HTTP method is sent – with url of the requested resource
TCP connected closed and recreated for every request
Multiplexing can be done with HTTP/2

On the URL -> there is protocol http/https
Uniform resource name – which has the domain/host.
Invisible connection port : 443 (https) or 80
Next is respurce path
By default – index.htm or default.htm

?=Optional URL query- user id or other filtering actions
GET – 200 OK, 404 Not found 405 Not allowed 403 Forbidden (host with resource + authentication header or cookie)
POST – create a new resource(201 created 401 unauthorized 409 conflict 404 not found) – requests an id to track
PUT – Update an existing singleton resource based on ID (200 Ok 204 no content 404 not found 405 method not allowed)
PATCH – modify without replacing entirely based on ID
DELETE – remove a singleton resource based on ID
HEAD – just get the response header from the resource without touching it
OPTIONS – description of the communication option
TRACE – loopback of the request
Each method has a request response pair

1xx – information
2xx – success
3xx – redirection
4xx – client error
5xx – server error

SSL/TLS
Symmetric:
Rc4 – 2048
3des – 168
Blowfish – 448
AES – 256

Asymmetric:
RSA – 4096
Diffie hellman

Client sends – list of supported ciphers
Server selects strongest cipher and sends PKI certificate that contains servers public key and host name
Client generates and sends unique session key (encrypted with public key of server)
Webserver decrypts with private key.
Both sides know the symmetric session key

PKI components:
Certificate authority- issues, renews and revokes certificate
Registration authority – subordinate of CA – manages certificates
CRL – Certificate revocation list – Online certificate status protocol – OCSP – verification of certificate validity using a serial number
Certificate template – blueprint used when issuing certificate.
Certificate – signature of CA, expiry info and key

Certificate authorities issue certificates.
Certificates contain digital signature of the issuing CA which is signed by private key which can be validated with public key of that Cas

PKI certificates – X.509 digital
Has version and serial number along with digital signature of CA, algorithm used, validity, usage details, URL or domain or email address, public key and private key
Wildcard certiticate can be a single certificate that can match all sub domains under it

Stapling
Certificate owners can periodically check for their certificate validity, clients connecting to the server will receive ocsp status for that website

Public key pinning – through http header, trusting devices download a trusted copy of servers certificate which includes its public key
Lifecycle:
Certificate request - public and private key is generated
Private keys can be made available to trusted third parties
Certificate signing request is generated with the public key
CSR is sent to certificate authority for signing
Simple Certificate enrollment protocol
Certificate issuance – manual or automated
The certificate is stored in device trusted certificate store
Certificate Usage and Revocation
Certificate renewal – norm is 2 yrs
Certificate expiry

Encrypt for yourself – use private key of yours
Encrypt for others – public key of others

explain how a computer in home can connect to office local network through vpn.. explain in detail with private / public ip addresses

ChatGPT

ChatGPT

Sure, let's go through the steps of how a computer at home can connect to an office local network through a VPN, considering private and public IP addresses. This scenario typically involves a Remote Access VPN.

Scenario Overview:

- **Home Computer (Client):** The computer at home that wants to connect to the office network.
- **Home Router:** The router at the user's home that connects to the internet.
- **Internet:** The public network through which the home computer connects to the office network.
- **Office Router:** The router at the office that connects to the internet and the office local network.
- **Office Local Network:** The private network within the office.

Steps:

9.1.1.1 ***1. Configuration at the Office:***

- **Public IP Address:** The office router has a public IP address assigned by the Internet Service Provider (ISP). This is the IP address visible on the internet.
- **VPN Server:** The office router is configured as a VPN server. It has a private IP address on its internal interface facing the office local network.
- **VPN Configuration:** The VPN server is configured with a VPN protocol (e.g., IPSec, SSL/TLS, or others) and authentication methods.

9.1.1.2 ***2. Home Router Configuration:***

- **Public IP Address:** The home router also has a public IP address assigned by the ISP.
- **NAT (Network Address Translation):** The home router performs NAT, translating private IP addresses of devices within the home network to its public IP address when accessing the internet.

9.1.1.3 ***3. VPN Client Configuration:***

- **VPN Client Software:** The home computer needs VPN client software. This software establishes a secure connection to the office VPN server.

- **VPN Configuration:** The user configures the VPN client with the public IP address of the office router, VPN protocol, and necessary authentication details.

9.1.1.4 *4. VPN Connection Establishment:*

- **Initiation:** The user initiates the VPN connection from the home computer.
- **Authentication:** The VPN client authenticates itself with the VPN server using pre-configured credentials or other authentication methods.
- **Secure Tunnel:** A secure and encrypted tunnel is established between the home computer and the office router over the internet.

9.1.1.5 *5. Data Transfer:*

- **Encrypted Data:** All data transmitted between the home computer and the office network is encrypted within the VPN tunnel, ensuring security.

9.1.1.6 *6. Routing:*

- **Routing Table Update:** Upon VPN connection, the routing tables are updated. The home computer knows to route traffic intended for the office local network through the VPN tunnel.

9.1.1.7 *7. Office Local Network Access:*

- **Access to Resources:** The home computer can now access resources on the office local network as if it were physically present in the office.

Key Points:

- **Public IP Addresses:** The routers at both the home and office have public IP addresses, but private IP addresses are used within the local networks.
- **Encryption:** The VPN tunnel ensures that data is encrypted, providing a secure connection.
- **Routing:** The routing tables are updated to direct traffic for the office local network through the VPN tunnel.

This setup allows a user working from home to securely connect to the office local network, access resources, and work as if physically present in the office.

You

how tunnel is setup?

ChatGPT

ChatGPT

Setting up a tunnel in the context of a VPN involves the creation of a secure, encrypted pathway through which data can be transmitted between two networks or devices. The process typically involves the configuration of various parameters, protocols, and security measures. Let's take a closer look at how a tunnel is set up:

Components Involved:

1. **Tunnel Endpoints:**
   - Each end of the tunnel is referred to as a tunnel endpoint.
   - In the case of a VPN, the tunnel endpoints are usually the routers or devices responsible for establishing the secure connection.
2. **VPN Protocols:**

- Various protocols can be used to implement VPN tunnels, such as IPSec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security), L2TP (Layer 2 Tunneling Protocol), and others.
- The choice of protocol depends on factors like security requirements, network architecture, and compatibility.

Steps to Set Up a Tunnel:

1. **Configuration at Both Ends:**
   - Configure the settings on both ends of the tunnel, specifying details such as tunnel endpoints, encryption algorithms, authentication methods, and other parameters.
2. **Authentication:**
   - Establish methods for authenticating the tunnel endpoints to ensure that only authorized devices can establish the tunnel.
3. **Encryption Configuration:**
   - Specify the encryption algorithms and keys that will be used to secure the data transmitted through the tunnel.
   - This ensures the confidentiality and integrity of the data.
4. **Key Exchange:**
   - Establish a mechanism for securely exchanging encryption keys between the tunnel endpoints.
   - Key exchange protocols, such as IKE (Internet Key Exchange), are commonly used for this purpose.
5. **Tunnel Establishment:**
   - Initiate the process of tunnel establishment, during which the tunnel endpoints negotiate and agree on the parameters for secure communication.
   - This involves the exchange of control messages to set up the tunnel.
6. **Data Transmission:**
   - Once the tunnel is established, data can be transmitted through it securely.
   - The data is encapsulated within the secure tunnel, protecting it from eavesdropping or tampering.

Example using IPSec:

1. **Tunnel Configuration:**
   - Specify the tunnel endpoints' IP addresses.
   - Define the encryption algorithm (e.g., AES), hash algorithm (e.g., SHA-256), and other parameters.
2. **Authentication:**
   - Choose an authentication method, such as pre-shared keys or digital certificates, to verify the identities of the tunnel endpoints.
3. **Key Exchange:**
   - Use a key exchange protocol like IKE to securely negotiate and exchange encryption keys between the tunnel endpoints.
4. **Tunnel Establishment:**
   - IKE initiates the negotiation process, and once agreement is reached, the tunnel is established.
5. **Data Transmission:**
   - Data is encapsulated within IPSec packets, ensuring secure transmission through the tunnel.

Key Considerations:

- **Network Address Translation (NAT):**
  - If either endpoint is behind a NAT device, additional considerations may be needed, such as NAT traversal mechanisms.
- **Firewall Configuration:**
  - Ensure that firewalls along the route allow the VPN traffic to pass through.
- **Monitoring and Maintenance:**
  - Regularly monitor the VPN tunnel for performance, and implement maintenance tasks such as updating keys.

Setting up a tunnel involves careful configuration and coordination between the tunnel endpoints to establish a secure and encrypted pathway for data transmission. The specific steps may vary based on the chosen VPN protocol and the devices involved.

You

explain tls vpn tunnel

ChatGPT

ChatGPT

Transport Layer Security (TLS) can be used to create a VPN tunnel, providing a secure and encrypted communication channel between two endpoints. This approach is often referred to as a TLS VPN or SSL VPN. TLS is commonly used to secure web traffic through HTTPS, but it can also be utilized to establish VPN connections. Here's an explanation of how a TLS VPN tunnel works:

Components Involved:

1. **TLS Protocol:**
   - TLS is a cryptographic protocol that ensures the confidentiality and integrity of data transmitted over a network.
   - It operates at the transport layer of the OSI model, providing a secure communication channel.
2. **VPN Server and Client:**
   - The VPN server and client are the endpoints of the TLS VPN tunnel.
   - The server typically resides in the target network (e.g., corporate network), while the client is a device connecting remotely.

Steps to Set Up a TLS VPN Tunnel:

1. **Configuration of TLS Parameters:**
   - Specify TLS parameters such as the version of TLS (e.g., TLS 1.2, TLS 1.3), encryption algorithms (e.g., AES), and authentication methods (e.g., certificates).
2. **Certificate Exchange:**
   - The VPN server and client exchange digital certificates to verify each other's identities.
   - Certificates are issued by a trusted Certificate Authority (CA) and include public keys.
3. **TLS Handshake:**
   - The TLS handshake process occurs between the server and client to negotiate encryption parameters and establish a secure connection.
   - It involves several steps, including key exchange and mutual authentication.
4. **Session Key Generation:**

- During the TLS handshake, a session key is generated. This key is used for symmetric encryption, providing a secure and efficient way to encrypt and decrypt data during the session.

5. **VPN Tunnel Establishment:**
   - Once the TLS handshake is successful, a secure TLS VPN tunnel is established between the server and client.
   - All data transmitted through the tunnel is encrypted using the session key.
6. **Data Transmission:**
   - Data is encapsulated within TLS/SSL packets and transmitted securely through the established tunnel.
   - The TLS layer ensures that the data remains confidential and tamper-proof.
7. **Authentication and Authorization:**
   - The server authenticates the client based on its digital certificate.
   - Additional authorization checks may be performed to ensure that the client has the right to access specific resources.

Advantages of TLS VPN:

- **Ease of Use:**
  - TLS VPNs are often easier to set up compared to other VPN technologies.
  - TLS is widely supported by various devices and operating systems.
- **Secure Communication:**
  - TLS provides strong encryption and ensures the confidentiality and integrity of data during transmission.
- **Flexibility:**
  - TLS VPNs can be used for various applications, including remote access and site-to-site connections.
- **Compatibility:**
  - TLS is commonly supported by web browsers and doesn't require special client software in many cases.

Considerations:

- **Performance:**
  - While TLS provides strong security, the encryption and decryption processes can introduce some overhead, affecting performance.
- **Protocol Versions:**
  - Ensure that the chosen TLS version is up-to-date and secure, considering potential vulnerabilities in older versions.

A TLS VPN tunnel provides a secure and flexible way to establish encrypted connections over the internet, making it suitable for remote access scenarios or secure communication between networks.
In a TLS VPN scenario, the TLS header and payload are encapsulated within the transport layer (commonly TCP) and the original IP and Ethernet headers are not changed. The TLS protocol operates at the application layer, securing the payload (application-layer data) within a TLS record. This TLS record, along with the original transport layer headers, is then transmitted over the network.

Here's a breakdown of the structure:

1. **Original Ethernet, IP, and TCP Headers:**
   - The data transmission starts with the original Ethernet, IP, and TCP headers, which encapsulate the application-layer data.
2. **TLS Record:**
   - The TLS Record encapsulates the application-layer data (TLS payload), the TLS header, and any necessary TLS Handshake messages.
   - The TLS Record includes metadata like the content type, version, and length.
3. **Encrypted TLS Record:**
   - The TLS Record is encrypted, ensuring the confidentiality and integrity of the application-layer data.
4. **Transport Layer Header (TCP/UDP):**
   - The encrypted TLS Record is treated as payload data and is encapsulated within the original transport layer header (commonly TCP, sometimes UDP in DTLS).
5. **Original IP Header:**
   - The transport layer (TCP/UDP) header, including the encrypted TLS Record, is encapsulated within the original IP header.
6. **Original Ethernet Header:**
   - The entire packet, including the original IP and transport layer headers with the encrypted TLS Record, is encapsulated within the original Ethernet header.

In summary, the TLS header and payload are part of the TLS Record, and the original IP and TCP headers are retained without modification. The TLS Record, along with the original transport layer headers, is transmitted over the network. The TLS encryption provides end-to-end security for the application-layer data, and the encapsulation within the transport layer ensures proper routing and delivery through the network.

10. Glossary

Bit: The smallest representation of data that a computer can understand
Border Gateway Protocol (BGP): A protocol by which routers share data with each other
Broadcast: A type of Ethernet transmission, sent to every single device on a LAN
Broadcast address: A special destination used by an Ethernet broadcast composed by all Fs
Cable categories: Groups of cables that are made with the same material. Most network cables used today can be split into two categories, copper and fiber
Cables: Insulated wires that connect different devices to each other allowing data to be transmitted over them
Carrier-Sense Multiple Access with Collision Detection (CSMA/CD): CSMA/CD is used to determine when the communications channels are clear and when the device is free to transmit data
Client: A device that receives data from a server
Collision domain: A network segment where only one device can communicate at a time
Computer networking: The full scope of how computers communicate with each other
Copper cable categories : These categories have different physical characteristics like the number of twists in the pair of copper wires. These are defined as names like category (or cat) 5, 5e, or 6, and how quickly data can be sent across them and how resistant they are to outside interference are all related to the way the twisted pairs inside are arranged
Crosstalk: Crosstalk is when an electrical pulse on one wire is accidentally detected on another wire
Cyclical Redundancy Check (CRC): A mathematical transformation that uses polynomial division to create a number that represents a larger set of data. It is an important concept for data integrity and is used all over computing, not just network transmissions
Data packet: An all-encompassing term that represents any single set of binary data being sent across a network link
Datalink layer: The layer in which the first protocols are introduced. This layer is responsible for defining a common way of interpreting signals, so network devices can communicate
Destination MAC address: The hardware address of the intended recipient that immediately follows the start frame delimiter
Duplex communication: A form of communication where information can flow in both directions across a cable
Ethernet: The protocol most widely used to send data across individual links
Ethernet frame: A highly structured collection of information presented in a specific order
EtherType field: It follows the Source MAC Address in a dataframe. It's 16 bits long and used to describe the protocol of the contents of the frame
Fiber cable: Fiber optic cables contain individual optical fibers which are tiny tubes made of glass about the width of a human hair. Unlike copper, which uses electrical voltages, fiber cables use pulses of light to represent the ones and zeros of the underlying data
Five layer model: A model used to explain how network devices communicate. This model has five layers that stack on top of each other: Physical, Data Link, Network, Transport, and Application
Frame check sequence: It is a 4-byte or 32-bit number that represents a checksum value for the entire frame
Full duplex: The capacity of devices on either side of a networking link to communicate with each other at the exact same time
Half-duplex: It means that, while communication is possible in each direction, only one device can be communicating at a time
Hexadecimal: A way to represent numbers using a numerical base of 16
Hub: It is a physical layer device that broadcasts data to every computer connected to it
Internet Protocol (IP): The most common protocol used in the network layer
Internet Service Provider (ISP): A company that provides a consumer an internet connection
Internetwork: A collection of networks connected together through routers - the most famous of these being the Internet
Line coding: Modulation used for computer networks
Local Area Network (LAN): A single network in which multiple devices are connected
MAC(Media Access Control) address: A globally unique identifier attached to an individual network interface. It's a 48-bit number normally represented by six groupings of two hexadecimal numbers
Modulation: A way of varying the voltage of a constant electrical charge moving across a standard copper network cable

Multicast frame: If the least significant bit in the first octet of a destination address is set to one, it means you're dealing with a multicast frame. A multicast frame is similarly set to all devices on the local network signal, and it will be accepted or discarded by each device depending on criteria aside from their own hardware MAC address
Network layer: It's the layer that allows different networks to communicate with each other through devices known as routers. It is responsible for getting data delivered across a collection of networks
Network port: The physical connector to be able to connect a device to the network. This may be attached directly to a device on a computer network, or could also be located on a wall or on a patch panel
Network switch: It is a level 2 or data link device that can connect to many devices so they can communicate. It can inspect the contents of the Ethernet protocol data being sent around the network, determine which system the data is intended for and then only send that data to that one system
Node: Any device connected to a network. On most networks, each node will typically act as a server or a client
Octet: Any number that can be represented by 8 bits
Organizationally Unique Identifier (OUI): The first three octets of a MAC address
OSI model: A model used to define how network devices communicate. This model has seven layers that stack on top of each other: Physical, Data Link, Network, Transport, Session, Presentation, and Application
Patch panel: A device containing many physical network ports
Payload: The actual data being transported, which is everything that isn't a header
Physical layer: It represents the physical devices that interconnect computers
Preamble: The first part of an Ethernet frame, it is 8 bytes or 64 bits long and can itself be split into two sections
Protocol: A defined set of standards that computers must follow in order to communicate properly is called a protocol
Router: A device that knows how to forward data between independent networks
Server: A device that provides data to another device that is requesting that data, also known as a client
Simplex communication: A form of data communication that only goes in one direction across a cable
Source MAC address: The hardware address of the device that sent the ethernet frame or data packet. In the data packet it follows the destination MAC address
Start Frame Delimiter (SFD): The last byte in the preamble, that signals to a receiving device that the preamble is over and that the actual frame contents will now follow
Transmission Control Protocol (TCP): The data transfer protocol most commonly used in the fourth layer. This protocol requires an established connection between the client and server
Transport layer: The network layer that sorts out which client and server programs are supposed to get the data
Twisted pair cable: The most common type of cabling used for connecting computing devices. It features pairs of copper wires that are twisted together
Unicast transmission: A unicast transmission is always meant for just one receiving address
User Datagram Protocol (UDP): A transfer protocol that does not rely on connections. This protocol does not support the concept of an acknowledgement. With UDP, you just set a destination port and send the data packet
Virtual LAN (VLAN): It is a technique that lets you have multiple logical LANs operating on the same physical equipment
VLAN header: A piece of data that indicates what the frame itself is. In a data packet it is followed by the EtherType
Address class system: **A system which defines how the global IP address space is split up**
Address Resolution Protocol (ARP): **A protocol used to discover the hardware address of a node with a certain IP address**
ARP table: **A list of IP addresses and the MAC addresses associated with them**
ASN: **Autonomous System Number is a number assigned to an individual autonomous system**
Demarcate: **To set the boundaries of something**
Demarcation point: **Where one network or system ends and another one begins**
Destination network: **The column in a routing table that contains a row for each network that the router knows about**
DHCP: **A technology that assigns an IP address automatically to a new device. It is an application layer protocol that automates the configuration process of hosts on a network**
Dotted decimal notation: **A format of using dots to separate numbers in a string, such as in an IP address**

Dynamic IP address: **An IP address assigned automatically to a new device through a technology known as Dynamic Host Configuration Protocol**
Exterior gateway: **Protocols that are used for the exchange of information between independent autonomous systems**
Flag field: **It is used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already been fragmented**
Fragmentation: **The process of taking a single IP datagram and splitting it up into several smaller datagrams**
Fragmentation offset field: **It contains values used by the receiving end to take all the parts of a fragmented packet and put them back together in the correct order**
Header checksum field: **A checksum of the contents of the entire IP datagram header**
Header length field: **A four bit field that declares how long the entire header is. It is almost always 20 bytes in length when dealing with IPv4**
IANA: **The Internet Assigned Numbers Authority, is a non-profit organization that helps manage things like IP address allocation**
Identification field: **It is a 16-bit number that's used to group messages together**
Interface: **For a router, the port where a router connects to a network. A router gives and receives data through its interfaces. These are also used as part of the routing table**
Interior gateway: **Interior gateway protocols are used by routers to share information within a single autonomous system**
IP datagram: **A highly structured series of fields that are strictly defined**
IP options field: **An optional field and is used to set special characteristics for datagrams primarily used for testing purposes**
Network Address Translation (NAT): **A mitigation tool that lets organizations use one public IP address and many private IP addresses within the network**
Next hop: **The IP address of the next router that should receive data intended for the destination networking question or this could just state the network is directly connected and that there aren't any additional hops needed. Defined as part of the routing table**
Non-routable address space: **They are ranges of IPs set aside for use by anyone that cannot be routed to**
Padding field: **A series of zeros used to ensure the header is the correct total size**
Protocol field: **A protocol field is an 8-bit field that contains data about what transport layer protocol is being used**
Routing protocols: **Special protocols the routers use to speak to each other in order to share what information they might have**
Service type field: **A eight bit field that can be used to specify details about quality of service or QoS technologies**
Static IP address: **An IP address that must be manually configured on a node**
Subnet mask: **32-bit numbers that are normally written as four octets of decimal numbers**
Subnetting: **The process of taking a large network and splitting it up into many individual smaller sub networks or subnets**
Time-To-Live field (TTL): **An 8-bit field that indicates how many router hops a datagram can traverse before it's thrown away**
Total hops: **The total number of devices data passes through to get from its source to its destination. Routers try to choose the shortest path, so fewest hops possible. The routing table is used to keep track of this**
Total length field: **A 16-bit field that indicates the total length of the IP datagram it's attached to**
ACK flag: **One of the TCP control flags. ACK is short for acknowledge. A value of one in this field means that the acknowledgment number field should be examined**
Acknowledgement number: **The number of the next expected segment in a TCP sequence**
Application layer: **The layer that allows network applications to communicate in a way they understand**
Application layer payload: **The entire contents of whatever data applications want to send to each other**
CLOSE: **A connection state that indicates that the connection has been fully terminated, and that no further communication is possible**
CLOSE_WAIT: **A connection state that indicates that the connection has been closed at the TCP layer, but that the application that opened the socket hasn't released its hold on the socket yet**
Connection-oriented protocol: **A data-transmission protocol that establishes a connection at the transport layer, and uses this to ensure that all data has been properly transmitted**

Connectionless protocol: **A data-transmission protocol that allows data to be exchanged without an established connection at the transport layer. The most common of these is known as UDP, or User Datagram Protocol**
Data offset field: **The number of the next expected segment in a TCP packet/datagram**
Demultiplexing: **Taking traffic that's all aimed at the same node and delivering it to the proper receiving service**
Destination port: **The port of the service the TCP packet is intended for**
ESTABLISHED: **Status indicating that the TCP connection is in working order, and both sides are free to send each other data**
FIN: **One of the TCP control flags. FIN is short for finish. When this flag is set to one, it means the transmitting computer doesn't have any more data to send and the connection can be closed**
FIN_WAIT: **A TCP socket state indicating that a FIN has been sent, but the corresponding ACK from the other end hasn't been received yet**
Firewall: **It is a device that blocks or allows traffic based on established rules**
FTP: **An older method used for transferring files from one computer to another, but you still see it in use today**
Handshake: **A way for two devices to ensure that they're speaking the same protocol and will be able to understand each other**
Instantiation: **The actual implementation of something defined elsewhere**
Listen: **It means that a TCP socket is ready and listening for incoming connections**
Multiplexing: **It means that nodes on the network have the ability to direct traffic toward many different receiving services**
Options field: **It is sometimes used for more complicated flow control protocols**
Port: **It is a 16-bit number that's used to direct traffic to specific services running on a networked computer**
Presentation layer: **It is responsible for making sure that the unencapsulated application layer data is actually able to be understood by the application in question**
PSH flag: **One of the TCP control flags. PSH is short for push. This flag means that the transmitting device wants the receiving device to push currently- buffered data to the application on the receiving end as soon as possible**
RST flag: **One of the TCP control flags. RST is short for reset. This flag means that one of the sides in a TCP connection hasn't been able to properly recover from a series of missing or malformed segments**
Sequence number: **A 32-bit number that's used to keep track of where in a sequence of TCP segments this one is expected to be**
Server or Service: **A program running on a computer waiting to be asked for data**
Session layer: **The network layer responsible for facilitating the communication between actual applications and the transport layer**
Socket: **The instantiation of an endpoint in a potential TCP connection**
Source port: **A high numbered port chosen from a special section of ports known as ephemeral ports**
SYN flag: **One of the TCP flags. SYN stands for synchronize. This flag is used when first establishing a TCP connection and make sure the receiving end knows to examine the sequence number field**
SYN_RECEIVED: **A TCP socket state that means that a socket previously in a listener state, has received a synchronization request and sent a SYN_ACK back**
SYN_SENT: **A TCP socket state that means that a synchronization request has been sent, but the connection hasn't been established yet**
TCP checksum: **A mechanism that makes sure that no data is lost or corrupted during a transfer**
TCP segment: **A payload section of an IP datagram made up of a TCP header and a data section**
TCP window: **The range of sequence numbers that might be sent before an acknowledgement is required**
URG flag: **One of the TCP control flags. URG is short for urgent. A value of one here indicates that the segment is considered urgent and that the urgent pointer field has more data about this**
Urgent pointer field: **A field used in conjunction with one of the TCP control flags to point out particular segments that might be more important than others**

A record: **The most common resource record, used to point a certain domain name at a certain IPv4 IP address**

Anycast: **A technique that's used to route traffic to different destinations depending on factors like location, congestion, or link health**
Automatic allocation: **A range of IP addresses is set aside for assignment purposes**
Caching and recursive name servers: **They are generally provided by an ISP or your local network, and their purpose is to store domain name lookups for a certain amount of time**
CNAME: **A resource record used to map one domain to another**
DHCP discovery: **The process by which a client configured to use DHCP attempts to get network configuration information**
Domain Name System (DNS): **A global and highly distributed network service that resolves strings of letters, such as a website name, into an IP address**
DNS zones: **A portion of space in the Domain Name System (DNS) that is controlled by an authoritative name server**
Domain: **Used to demarcate where control moves from a top-level domain name server to an authoritative name server**
Domain name: **A website name; the part of the URL following www.**
Dynamic allocation: **A range of IP addresses is set aside for client devices and one of these IPs is issued to these devices when they request one**
Fixed allocation: **Requires a manually specified list of MAC address and the corresponding IPs**
Fully qualified domain name: **When you combine all the parts of a domain together**
IP masquerading: **The NAT obscures the sender's IP address from the receiver**
MX record: **It stands for mail exchange and this resource record is used in order to deliver email to the correct server**
Name resolution: **This process of using DNS to turn a domain name into an IP address**
Network Address Translation (NAT): **A mitigation tool that lets organizations use one public IP address and many private IP addresses within the network**
NS record: **It indicates other name servers that may also be responsible for a particular zone**
NTP servers**: Used to keep all computers on a network synchronized in time**
Pointer resource record: **It resolves an IP to a name**
Port forwarding: **A technique where specific destination ports can be configured to always be delivered to specific nodes**
Port preservation**: A technique where the source port chosen by a client, is the same port used by the router**
Proxy service**: A server that acts on behalf of a client in order to access another service**
Quad A (AAAA) record: **It is very similar to an A record except that it returns in IPv6 address instead of an IPv4 address**
Recursive name servers: **Servers that perform full DNS resolution requests**
Reverse lookup zone files: **They let DNS resolvers ask for an IP, and get the FQDN associated with it returned**
Reverse proxy: **A service that might appear to be a single server to external clients, but actually represents many servers living behind it**
Round robin: **It is a concept that involves iterating over a list of items one by one in an orderly fashion**
SRV record: **A service record used to define the location of various specific services**
Start of authority: **A declaration of the zone and the name of the name server that is authoritative for it**
Top Level Domain (TLD): **The top level of the DNS or the last part of a domain name. For example, the "com" in www.weather.com**
Time-To-Live field (TTL): **An 8-bit field that indicates how many router hops a datagram can traverse before it's thrown away**
Two-factor authentication: **A technique where more than just a username and password are required to authenticate. Usually, a short-lived numerical token is generated by the user through a specialized piece of hardware or software**
TXT record: **It stands for text and was originally intended to be used only for associating some descriptive text with a domain name for human consumption**
Types of DNS servers: **There are five primary types of DNS servers; caching name servers, recursive name servers, root name servers, TLD name servers, and authoritative name servers**
Virtual Private Network (VPN): **A technology that allows for the extension of a private or local network, to a host that might not work on that same local network**
Zone Files: **Simple configuration files that declare all resource records for a particular zone**

Ad-Hoc network: A network configuration without supporting network infrastructure. Every device involved with the ad-hoc network communicates with every other device within range, and all nodes help pass along messages

Asymmetric Digital Subscriber Line (ADSL): A device that establishes data connections across phone lines and different speeds for uploading and downloading data

Baud rate: A measurement of how many bits could be passed across a phone line in a second

Bluetooth: The most common short range wireless network

Broadband: Any connectivity technology that isn't dial-up Internet

Cable modem: A device that sits at the edge of a consumer's network and

connects it to the cable modem termination system

Cable modem termination system: Connects lots of different cable connections

to an ISP's core network

Channels: Individual, smaller sections of the overall frequency band used by a wireless network

Collision domain: A network segment where only one device can communicate at a time

Data payload section: Has all of the data of the protocols further up the stack of a frame

Dial-up: Uses POTS for data transfer, and gets its name because the connection is established by actually dialing a phone number

DSL: Digital subscriber line was able to send much more data across the wire than traditional dial-up technologies by operating at a frequency range that didn't interfere with normal phone calls

DSLAM: Digital Subscriber Line Access Multiplexers are devices that connect multiple DSL connections to a high-speed digital communications channel

Duration field: Specifies how long the total frame is

Frame check sequence: It is a 4-byte or 32-bit number that represents a checksum value for the entire frame

Frame control field: 16 bits long, it contains a number of sub-fields that are used to

describe how the frame itself should be processed

Frequency band: A certain section of the radio spectrum that's been agreed upon to be used for certain communications

FTTB: Fiber to the building, fiber to the business or even fiber to the basement, since this is generally where cables to buildings physically enter. FTTB is a setup where fiber technologies are used for data delivery to an individual building

FTTH: Fiber to the home. This is used in instances where fiber is actually run to each individual residents in a neighborhood or apartment building

FTTN: Fiber to the neighborhood. This means that fiber technologies are used to deliver data to a single physical cabinet that serves a certain amount of the population

FTTP: Fiber to the premises. FTTH and FTTB may both also be referred to as FTTP

FTTX: Stands for fiber to the X, where the X can be one of many things

HDSL: High Bit-rate Digital Subscriber Lines. These are DSL technologies that provision speeds above 1.544 megabits per second

MAC filtering: Access points are configured to only allow for connections from a specific set of MAC addresses belonging to devices you trust

Mesh networks: Like ad-hoc networks, lots of devices communicate with each other device, forming a mesh if you were to draw lines for all the links between all the nodes

Metered connection: An internet connection where all data transfer usage is tracked. Cell phone plans that have a limit on data usage per month or that charge based on usage are examples of metered connections

Non-metered connection: A connection where your data usage is not tracked or limited, instead you are charged a flat fee for unlimited and unrestricted usage. A Wi-Fi connection is an example of a non-metered connection

Optical Network Terminator: Converts data from protocols the fiber network can

understand to those that are more traditional twisted pair copper networks can understand

Pairing: When a wireless peripheral connects to a mobile device, and the two devices exchange information, sometimes including a PIN or password, so that they can remember each other

Point-To-Point VPN: Establishes a VPN tunnel between two sites but VPN tunneling logic is handled by network devices at either side, so that users don't all have to establish their own connections

Receiving address: The MAC address of the access point that should receive the frame

Symmetric Digital Subscriber Line (SDSL): A device that establishes data connections across phone lines and has upload and download speeds that are the same

Sequence control field: A field that is 16 bits long and mainly contains a sequence number used to keep track of ordering the frames

Short-range wireless network: It is what mobile devices uses to connect to their peripherals

T-Carrier technologies: Technologies Invented to transmit multiple phone calls over a single link. Eventually, they also became common transmission systems to transfer data much faster than any dial-up connection could handle

Transmitter address: The MAC address of whatever has just transmitted the frame

Wi-Fi Protected Access (WPA): A security program that uses a 128-bit key to protect wireless computer networks, which makes it more difficult to crack than WEP

Wide area network: Acts like a single network but spans across multiple physical locations. WAN technologies usually require that you contract a link across the Internet with your ISP

Wired Equivalence Privacy (WEP): An encryption technology that provides a very low level of privacy. WEP should really only be seen as being as safe as sending unencrypted data over a wired connection

Wireless access point: A device that bridges the wireless and wired portions of a network

Wireless LANS (WLANS): One or more access points act as a bridge between a wireless and a wired network

Wireless networking: Networks you connect to through radios and antennas

Cloud computing: The concept and technological approach of accessing data, using applications, storing files, etc. from anywhere in the world as long as you have an internet connection

Error detection: The ability for a protocol or program to determine that something went wrong

Error recovery: The ability for a protocol or program to attempt to fix an error

Flow label field: 20-bit field that's used in conjunction with the traffic class field for routers to make decisions about the quality of service level for a specific datagram

Hop limit field: An 8-bit field that's identical in purpose to the TTL field in an IPv4 header

Host file: A simple text file that consists of one or more lines, each of which contains a hostname and an IP address

Hybrid cloud: A cloud computing environment that combines on-premises private cloud resources with public cloud resources

Hypervisor: A piece of software that runs and manages virtual machines while also

offering guests a virtual operating platform that's indistinguishable from actual hardware

ICMP: Internet control message protocol is used by router or remote hosts to communicate error messages when network problems prevent delivery of IP packets

ICMP payload: Piece of the packet which lets the recipient of the message know which of their transmissions caused the error being reported

Infrastructure as a Service (IaaS): A subset of cloud computing where a network and servers are provided for customers to run their services

IPv6 tunnel brokers: Companies that provide IPv6 tunneling endpoints for you, so you don't have to introduce additional equipment to your network

IPv6 tunnel: IPv6 tunnel servers on either end of a connection take incoming IPv6 traffic and encapsulate it within traditional IPv4 datagrams

Link-local unicast address: Allow for local network segment communications and are configured based upon a host's MAC address

Loopback address: An IP address that always points to itself. This type of address is used to test internal pathing through the TCP/IP protocols

Multicast: A way of addressing groups of hosts all at once

Next header field: Defines what kind of header is immediately after this current one

Payload length field: 16-bit field that defines how long the data payload section of the datagram is

Platform as a service: A subset of cloud computing where a platform is provided for customers to run their services

Private cloud: When a company owns the services and the rest of the cloud infrastructure, whether on-site or in a remote data center

Public cloud: The cloud services provided by a third party

Public DNS servers: Name servers specifically set up so that anyone can use them for free

Registrar: An organization responsible for assigning individual domain names to other organizations or individuals

Software as a Service (SaaS): A way of licensing the use of software to others while keeping that software centrally hosted and managed

Traffic class field: An 8-bit field that defines the type of traffic contained within the IP datagram and allows for different classes of traffic to receive different priorities

Version field: First field in an IP header that specifies the version of IP

Virtualization: A single physical machine called a host runs many individual virtual instances called guests

https://spun.io/2018/05/04/bitwise-operations-and-common-uses-decoding-ipv4-headers-using-and-and-bitwise-shifts/