TCP/IP 5 layer model

#	Layer name	protocol	Protocol data unit	addressing
5	Application	HTTP/SMTP/..	messages	n/a
4	Transport	TCP/UDP	segment	Port #'s
3	Network	IP	datagram	IP address
2	Data Link	Ethernet, Wi-Fi	frames	MAC address
1	physical	10 Base T, 802.11	bits	n/a

1. Physical layer - represents the physical devices that interconnect computers (specifications for the networking cables, connectors that joins devices together)
2. Data link layer - responsible for defining a common way of interpreting these signals so network devices can commuicate
3. Network layer - allows different networks to communicate with each other through routers(long distances)

//data link - getting data across the single link, the newtork layer is resposnible for getting data across a collection of networks
//the network layer deliver data between two individual nodes (IP Protocol)

4. Transport layer - sorts out which client and server are supposed to get that data
5. Application layer -

Devices:

a) **Hub** - a physical layer device that allows for connection from many computers at once
All devices connected to hub will end up talking to all other devices at the same time.
It's up to each system connected to the hub to determine if the incoming data was meant for them or to ignore it It causes a lot of noise on the network. It creates a **collision domain.**

Collision domain - a network segment where only one device can communicate at a time. If multiple systems try sending data at the same time, the electrical pulses sent across the cable can interfere with each other.This causes the systems have to wait for a period of time before they can try send their data again. It really slow down network communications.

b) **Switch** - a **data link layer** device, so the switch can actually inspect the contents of the ethernet protocol data being send around the network, determine which system the data is intended for, and then, only send that data to that one system.

Hubs and switches are the primiary devices used to connect computers on a single network, usually reffered to as LAN
But when we want to send data outside our local area network, there is when routers come to play

c) **Router** - a network layer device that knows how to forward data between independent networks

Routers share data with each other via **BGP (Border Gateway Protocol),** which lets them learn about the most optimal path for forward traffic.

We will refer to these devices as Nodes.

1.PHYSICAL LAYER

Cables

Copper cables
Devices communicate in binary (changing the voltage bewteen the two ranges)

Twisted pair - the twisted nature help protect again electromagnetic interference
How many pairs are in use depends on tehchnology being used. These cables allows for duplex communication (information can flow in both directions across the cable).

Fiber cables
Used in environment, where there is a lot electromagnetic interference from outside sources
Can transport data quicker, but they are more expensive
Fiber can also transport data across much longer distances without suffering potential data loss

Modulation:

A way of varying the voltage of this charge moving across the cable
Line coding - it allows devices on either end of the link to understand the electrical charge
Digital data 0101010101010101010010110 -> Digital signal (voltage) -> 111101010101 Digital Data

2. DATA LINK LAYER

Unicast, multicast, broadcast

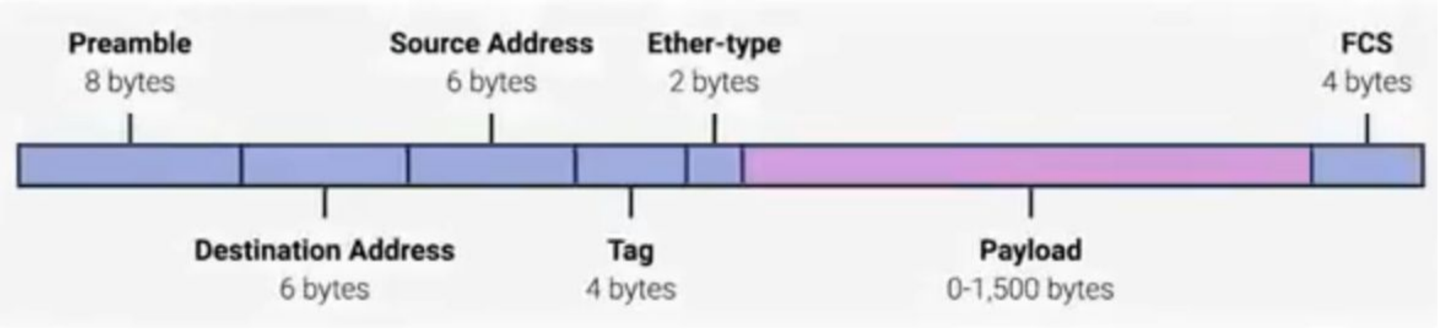
Unicast - transmission to one single address. At the ethernet level this is done by looking at the special bit in the destination MAC address. If the least significant bit in the first octet of a destination address is set to zero, it means that ethernet frame is intended for only the destination address.

If the least singificant bit in the first octet of a destination address is set to one, it means you’re dealing with a **multicast** frame.It’s similarly send to all devices on the local network segment. What is different, it will be accepted or discarded by each device depending on criteria.

Broadcast - send every single device at the same time, this is acomplished by using the special destination broadcast address: Ethernet Broadcast Address FF:FF:FF:FF:FF:FF

Ethernet Frame

Almost all sections are mandatory, and most of them have fixed size.



Preamble - 8 bytes(64 bits) - can itself be split into two sections:
[7 bytes] buffer between frames, or to synchronize internal clock, (regulate the speed at which they send data)
[1 byte] SFD = Start Frame Delimiter - Singnals to a receiving device that the preamble is over and that the actual frame contents will now follow

Destination/Source MAC address - the hardware address of the intended recipient (every address = 6 bytes)

Ether-Type Field [2 bytes] - used to describe the protocol of the contents of the frame

VLAN Tag (VLAN header) - indicates that the frame itself is what's called a VLAN frame (VLAN lets you have multiple logical LANs operating on the same physical equipment). Any frame with the VLAN tag will only be delivered out of the switch interface configured to relay this specific tag.

Payload = actual data (everything that isn't header)

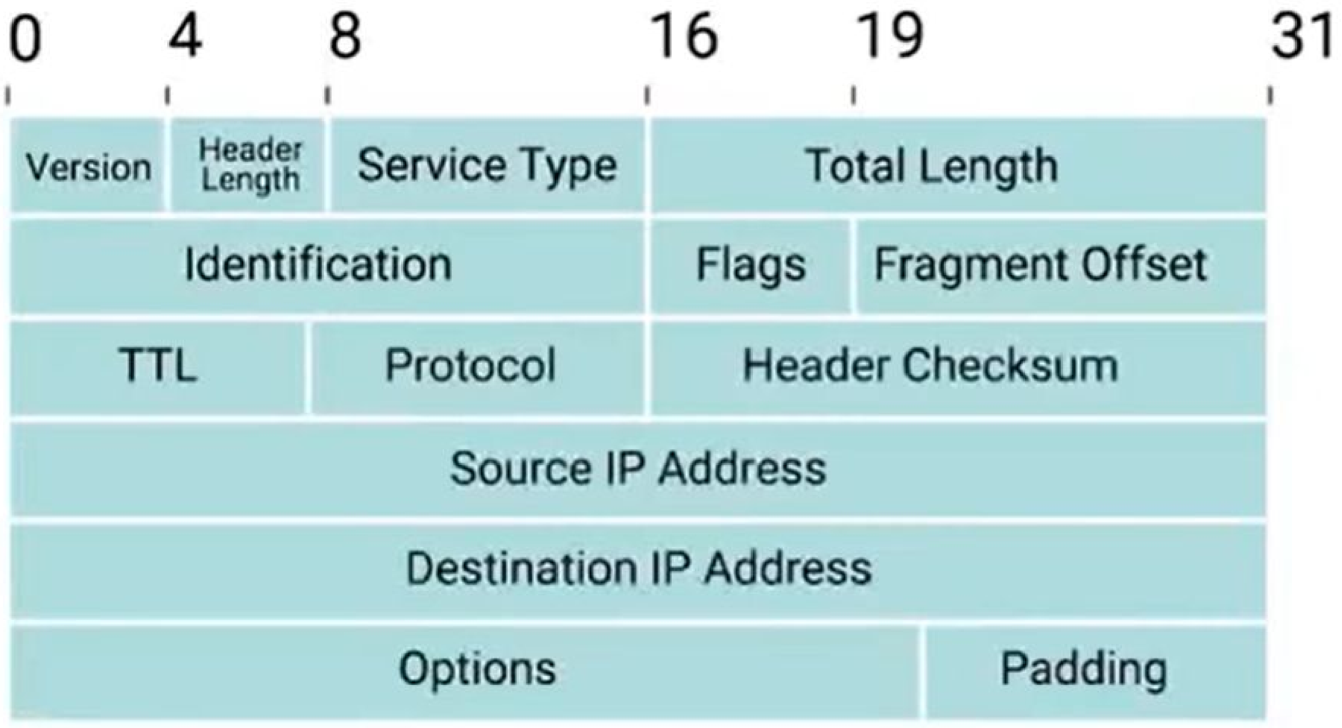
FCS: Frame Check Sequence: number that represents a checksum value for the entire frame. This checksum value is calculated by perfoming what's known as a *CRC: cyclical redundancy check* against the frame.

3.THE NETWORK LAYER

DHCP - Dynamic Host Configuration Protocol - assigns dynamic IP address

In most cases static IP addresses are reserved for servers and network devices while dynamic IP addresses are reserved for clients.

IP Datagram

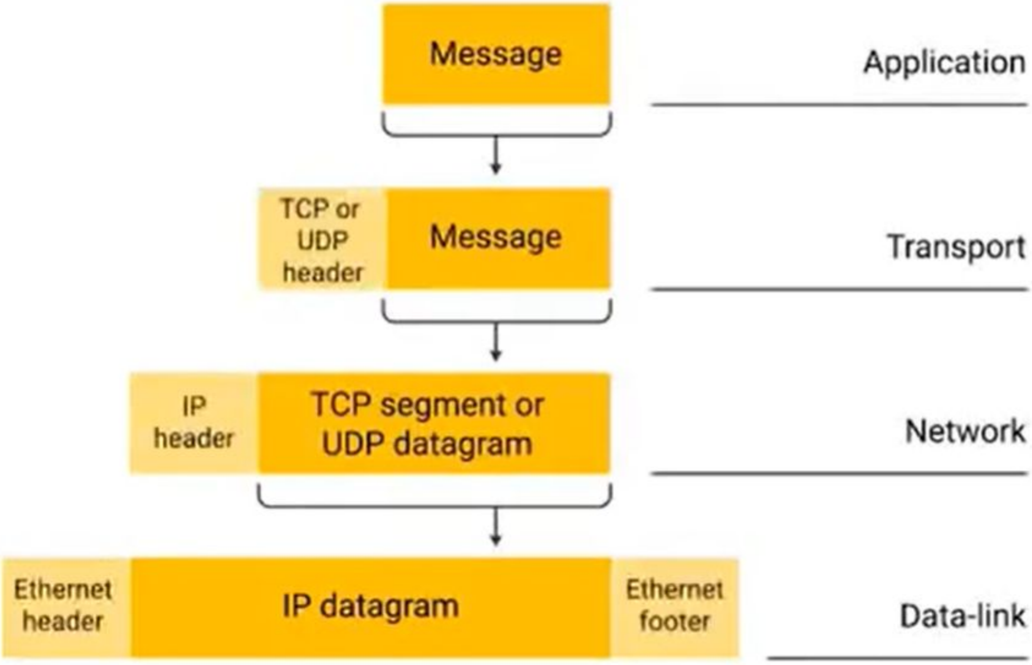


Version: IPv4 (or IPv6?)
Header Length: how long the entire header is (minimum 20 bytes!)
Service Type: to specify details about quality of service, or QoS(make routers able to decide which datagram is more important!
Total Length indicates the total length of the IP datagram it’s attached to
Identification - to group messages together

//If the amount of data that needs to be sent is larger than what can fit in a single datagram, the IP layer needs to split this data up into many individual packets

Flag - indicates if a datagram is allowed to be fragmented or has already been fragmented
Fragmentation Offset - contains values used by a receiving end to take all parts of the fragmented packet and put them back together in the correct order.
TTL (Time To Live) - indicates how many router hops a datagram can traverse before it’s thrown away. Every time a datagram reaches a new router, that router decrements the TTL field by one. Once this value reaches zero a router knows he doesn’t have to forward the data any futher. The main purpose of this field is to make sure that there isn’t a misconfiguration in routing that causes infinite loop, datagrams doesn’t spend the eternity to reach the destination.
Protocol - what transport layer protocol is being used (TCP or UDP?)
Header Checksum - a checksum of the contents of the entire IP datagram header (like a ethernet checksum)
Source/Destination IP Address fields (32bits)
IP options field - an optional field / is used to set special characteristics for datagrams // primarly used for testing puropses
Padding - just a series of zeros to ensure the header is the correct total size

The entire content of a IP datagram is encapsulated as a payload in the ethernet frame



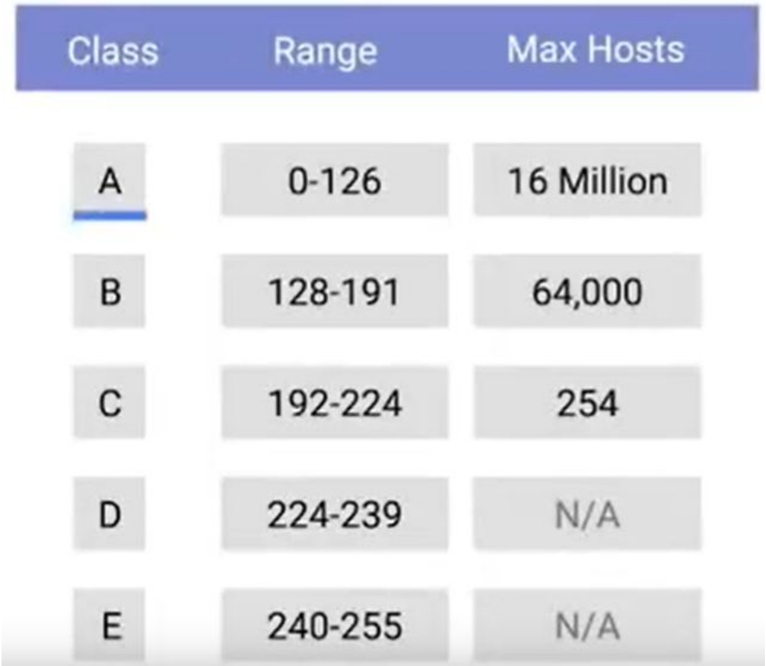
The payload in IP datagram is the TCP/UDP part

IP addresses classes

Gives us a way to break the total global IP space to descreet networks
IP addresses can be split into two sections: the network ID and the host ID
So for example: 9.100.100.100
9 will be network ID
100.100.100 will be host ID
This is why all IP addresses in IBM starts from 9.

Address class system is a way of defining how the global IP address space is split up.

Class A: 1: NETWORK ID,	2,3,4: HOST ID
Class B: 1,2 NETWORK ID	3,4 HOST ID
Class C: 1,2,3 NETWORK ID	4 HOST ID



Class	Range	Max Hosts
A	0-126	16 Million
B	128-191	64,000
C	192-224	254
D	224-239	N/A
E	240-255	N/A

So class A address can have 16 million variations of host IP addresses (supports 16 million hosts on each of 127 networks) while class C only 254 (!) (but 2 million networks!!)

Class D for multicasting

In practical terms this class system has mostly been replaced by **CIDR: Classless inter-domain routing**

ARP: Address Resolution Potocol

A protocol used to discover the hardware address of a node with a certain IP addres

Once an IP datagram has been fully formed and needs to be encapsulated inside the ethernet frame. That means that the transmitting device needs a destination MAC address to complete the ethernet frame header. Amost all network connected devices will retainging local arp table

ARP Table: a list of IP addresses and the MAC addresses associated with them. ARP Table entries expire after a short amount of time to ensure changes in the network are accounted for.

If there is no proper MAC address of given IP address in ARP Table, protocol have to send ARP Request FF:FF:FF:FF:FF:FF, which is send to hardware broadcast address of all Fs, this request is sent to every node in the local network.

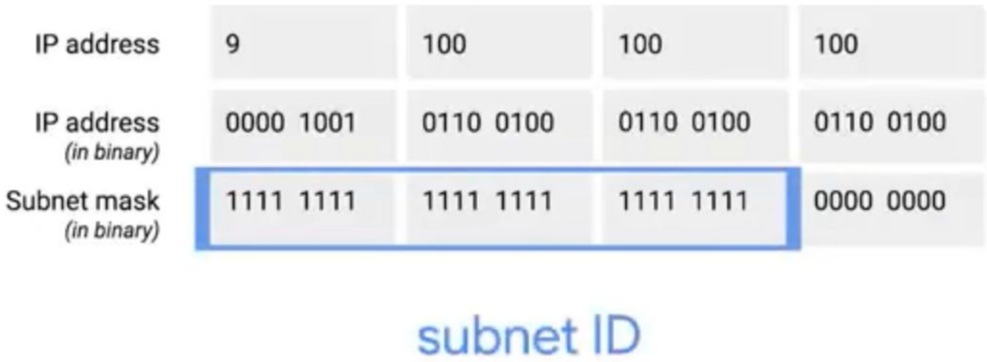
Subnetting

The process of taking a large newtork and splitting it up into many individual smaller subnetworks, or subnets

If you want to communicate with the IP address 9.100.100.100 core routers on the internet know that this address belongs to 9.0.0.0 class A network and then route the message to the gateway router responsible for the network by looking at the Network ID. A gateway router specifically serves as the entry-end-exit-path to a certain network. You can contrast this with core internet router, which may only speak to other core routers. Once your packet gets to the gateway router for the 9.0.0.0 class A network that router is now responsible for getting that data to the proper system, by looking at the host id.

In class A we can connect 16 millions hosts to each of 127 networks. That’s just way too many devices to connect to the same router. This is where subnetting comes in. With subnets you can split your large network up into many smaller ones. It’s individual subnets will all have their own gateway routers.

Subnets Masks



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

Subnet ID concept:
IP address is just 32 bots number. Without subnets certain bits are used for network id, and others for host id. In the world of subnets s ome bits that would normally comprise the host id will actually use the Subnet ID, with all three of these IDs represnted as single 32bit IP address, that can be delivered across many different networks. At the internet level core routers only care about the network ID, and use this to send the datagram along to the appriopriate gateway router to that network. That gateway router then has some additional

ifnormation that can use to send the datagram along the destination machine or the next router on the path. Finally - the host id is used by a last router to deliver the datagram to the intended recipent machine. Subnet IDs are calculated being known as subnet mask. Just like the IP address subnet masks are 32-bit numbers that are normally written as four octects in decimal.

The subnet mask is a binary number that has two sections. The beginning part, that is the mask itself (stream of ones). Just zeros comes after this. The subnet mask, which is the part of the number with all the ones tells us what we can ignore when we computing the host ID. The part with all the zeros tells us what to keep.
The puropose of the mask is to tell the router what part of the IP address is the subnet ID. (the part with ones). The network ID for the IP address is just the first octet. This leaves us with the remaining three octects. Let’s take the remaining octects and imagine them next to the subnet mask in binary form.

The numbers in the remaining octects that have corresponding one in the subnet mask are the **subnet ID.** The numbers that have a correspodning zero are the **host ID**

The size of the subnet is entirely defined by its subnet mask

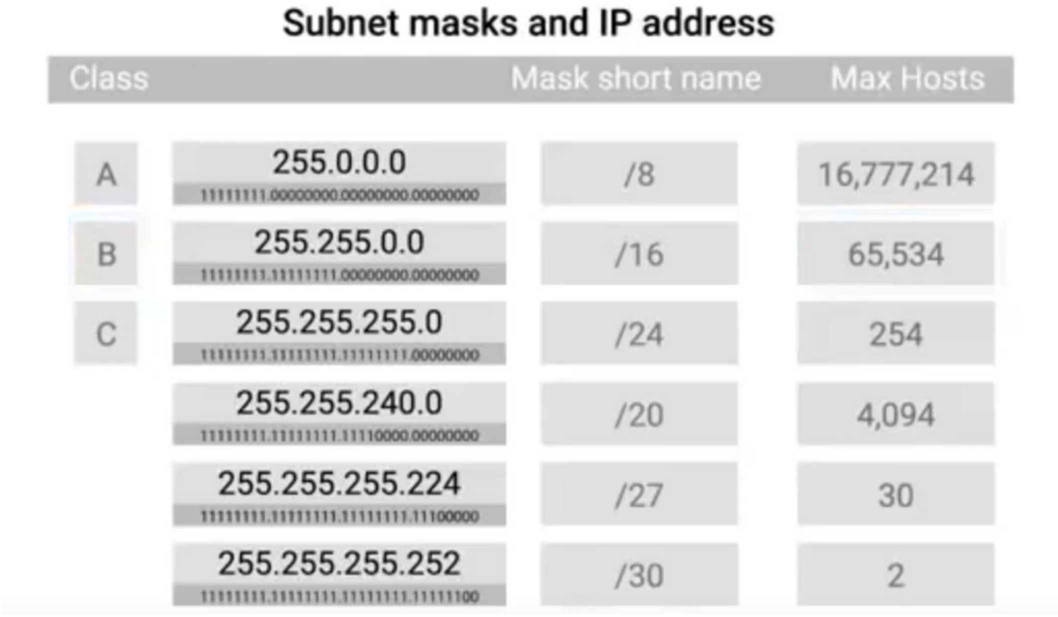
So when we have 255.255.255.0, we know that only the last octet is availabable for hosts ids regardless of what size the network and subnet IDs are.

Its is a good time to point out that in general a subnet can usually only contain two less than the total number of hosts ids availabable.

Having 255.255.255.0, we can have hosts from 0 to 255, but 0 is generally not used and 255 is normally reserved as a broadcast address for the subnet.

Subnet mask is a way for a computer to use AND operator to determine if an IP address exists on the same network. A computer that just perform this operation can now compare the results with its own network id to determine if the address is on the same network or on the different one.
Example: 9.100.100.100 AND 255.255.255.0 -> 9.100.100

As the internet continued to grow traditional subnetting just couldn’t keep up. With traditional subnetting and the address classes the network ID is always either 8 bit for class A, 16 bit for class B or 24bit class C network.



Subnet masks and IP address

Class		Mask short name	Max Hosts
A	255.0.0.0 11111111.00000000.00000000.00000000	/8	16,777,214
B	255.255.0.0 11111111.11111111.00000000.00000000	/16	65,534
C	255.255.255.0 11111111.11111111.11111111.00000000	/24	254
	255.255.240.0 11111111.11111111.11110000.00000000	/20	4,094
	255.255.255.224 11111111.11111111.11111111.11100000	/27	30
	255.255.255.252 11111111.11111111.11111111.11111100	/30	2

254 hosts availabable is too small for many use cases, but the 65534 is often way too large. Many companies eneded up with various class C networks too meet their needs, that means the routing tables ended up with

the bunch of entries for a bunch of class C networks, that were all actually routing to the same place. There is where CIDR comes to play

CIDR: Classes Inter-Domain Routing:

Is an even more flexible approach to describing blocks of IP addresses, it expends on the concept of subnetting by using subnet masks to demarcate networks (demarcate = to set something off)

Before we relied on the network id, subnet id and host id to deliver an ip datagram to the correct location. With CIDR the network ID and subnet ID are combined into one.
CIDR just abandons the concept of address classes entirely. The notation /27 etc. is a CIDR notation.

Routing

When a router receives an incoming package, it examines the destination IP address and determines which network it belongs to. On any complex network, like Internet, there are many different paths from point A to point B, routers try to pick the shortest possible path at all times.

Routing table:
-can vary a lot
But they all share a few thing in common: Columns:
Destination network: - will contain a row for each network that the router knows about, so (spearately IP and subnet mask, or together in CIDR notation)
Next hop: the IP address of the next router that should receive data intended for the destination networking question. Or it can just state that the network is directly connected and there arent any additional hops needed.
Total hops: - to keep track how far away the destination currently is. That way when it receives updated information from neighbouring routers it will know if it currently use the best path. Or if the better path is availabable.
Interface - the router also has to know which of his interfaces it should forward traffic matching the destination network.

In most cases routing tables are pretty simple. The really impressive part is that many core internet router have millions of rows in the routing table. This must be consulted for every single packet that flows through the router until it gets his final destination.

Routing protocols: protocols used by routers to speak to each other.

IGP: Interior Gateway Protocols

a) Link state protocols

Each router advertises the state of the link of each of its interfaces. These interfaces can be connected to other routers or can be direct reconnected to networks. The information about each router is propagated to every other router in the system. This know that every router on the system knows every detail about every other router on the system.The it can use complicated algorithms to find out which path is the best on each path. Link state protocol require more memory and much more computional power. As computer hardware become cheaper over years link state protocol have mostly replaced distance vector protocol

b) Distance-vector protocol

In older standards: just takes the routing table, which is a list of every network known to it, and how fare these networks are in terms of hops. Then the router send its list to evry neighbouring router, that is directly connected to him. In computer science a list is known as a vector. With a distance vector protocol routers don’t really know much about the total state of the autonomous system (collection of network: like in a big corporation), they just have some information about their neighbours.

EGP: Exterior Gateway Protocols

Are used to communicate data between routers representing the edges of an autonomous system.
Routers use Interior Gateway Protocols to share data across same organization, while Exterior Gateway Protocol when it comes to sharing data across different organizations.

IANA: Internet Assigned Numbers Authority

- a non-profit organization that hleps manage things like IP address allocation. The Internet wouldn't function without single authority for this source of issues, otherwise anyone colud try and use any IP space he wanted.
IANA is also responsible for **ASN: Autonomous System Number -**
ASN represents entire autonomous systems

Non-routable Address Space

IP was designed as 32 bit number, so only 4.294.967.295 unique numbers, so the IPv4 doesn't even have enough IP addresses availabable for every person on the planet.(7.5 billion). So in 1996 RfC (erquest-for-comments) was published and outlined number of networks defined as non-routable address space.

The primiary three ranges of non-routable address space are:
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
<u>They belong to no one and anyone can use them.</u> These ranges are free to anyone to use for internal networks. Interior Gateway Protcols will route this address spaces, so they are appropriate for use in inner auntonomous systems, but Exterior Gateway Protocol will not.

// NAT - Network Address Translation - allows Non-routable address space to communicate with other devies on Internet. Next module.

4.TRANSPORT LAYER

Allows traffic to be directed to specific network applications.
Handles multiplexing and demultiplexing

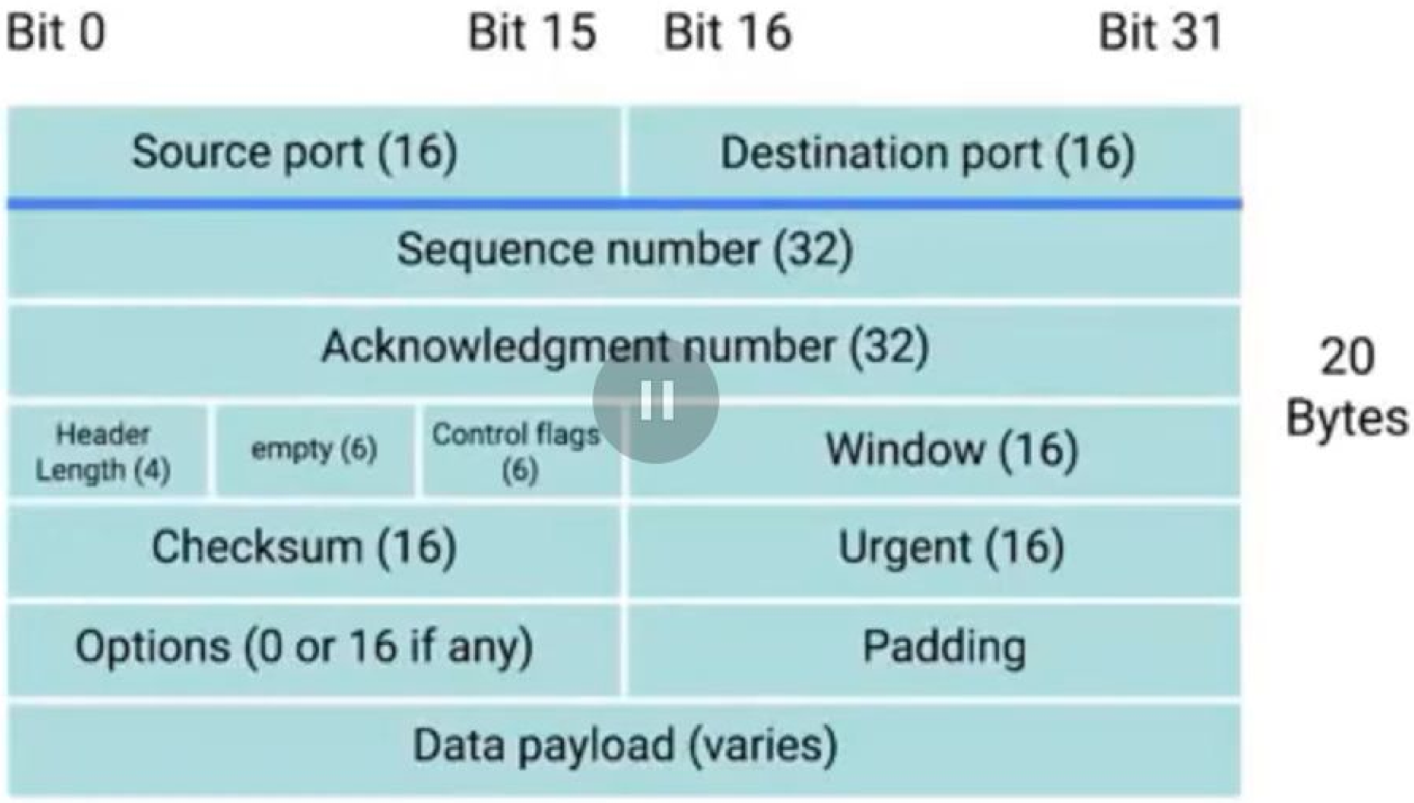
Multiplexing - the nodes in the traffic layer has the ability to direct traffic forward many different receiving services
Demultiplexing - it's taking traffic that is all in the same node and delivering it to the proper receiving process

Port - [16-bit number] - is used to direct traffic to specific services running on a networked computer.
Different network services are listening on specific ports for incoming request. For example the traiditonal port for http is port 80. If you want to request a webpage from the web server running on, computer listening on IP 10.1.1.100, the traffic will be directed for port 80 on that computer.
Socket number: is the IP:PORT, for example 10.1.1.100:80

Just like the ethernet frame encapsulate an IP datagram, an IP datatgram encapsulate a TCP segment. An ethernet frame has a payload section, which is just the entire content of the IP datagram. Remember also, that the IP datagram has also a payload section, and it is known as a **TCP segment.**

TCP segment

TCP segment: TCP header + data section: this data section is just another payload section, for where application data places its data. TCP header is split for many parts and contain a lot of informtion.



Destination port - is the port of the service the traffic is intended for (for example 80 when trafic is about to reach webserver running on a certain IP)
Source port - is a high-numbered pot chosen from special section of ports known as ephemeral ports. Is responsible for keeping lot of outgoing connections separate
A source port is needed somewhat the webserver replies the computer making the original request can send this data to the program that is actually requesting it. In this way webserver responds to your request to view the webpage. This response is reveived by your web browser and not your work processor.
Sequence number: The TCP layer splits too large data to many segments. The sequence number is to keep track of which segment out of many this particular segment might be
Acknowledgement number - is a lot like the sequence number. Is the number of the next expected segment. It's like: this is segment one, it's expected the next one will be two.
Data offset field (Header length) - how long is the TCP header.
Control flags - reserved for six TCP control flags
Windows - specifies the range of sequence numbers that might be sent before an acknowledgement is required
Checksum - just like checksum field in ethernet and IP level. Once all of the segment has been received by recipent, the checksum is calculated across the entire segment and is compared with the checksum in the header, to make sure it was no data loss, or corrupted along the way.
Urgent - used in conjunction with one of TCP control flags to point out particular segments that might be more important than others.
Options - (rarely used), it is sometimes used for more complicated flow control protocols
Padding - just stream of zeros to make sure the data payload section begins at the expected location

TCP Control Flags

URG /urgent**/**- a value of one here indicates that the segment is considered urgent and that the urgent pointer field has more data about this.
ACK - a value of one in this field means that the acknowledgement number field should be examined.
PSH - push/ - the transmitting device wants the receiving device to push currently-buffered data to the applicsation on the receiving end as soon as possible
//buffer is to keep some data in one place in memory, before sending it to another place
By keeping some data in a buffer, the TCP protocol can in the meantime send another, more important data
RST - reset/ one of the sides in a TCP connection hasn't been able to properly recover from a series of missing or malformed segments
(Wait, I can't get together what you mean, let's start over from the scratch!)
SYN /synchronize/- is used when first establishing a TCP connection and makes sure the receiving end knows to examine the sequence number field.
FIN /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.

Three-way-handshake

Computer A sends the TCP segment to computer B with a SYN flag.
(Let's establish a connection, and look at my sequence number field, so we know where the conversation starts!)

Computer B the responds wth a TCP segment with both SYN and ACK flags.
(*Sure!/ Let's establish a connection, and I acknowledged your sequence number!)*

Computer A responds with ACK flag
(*I acknowledgemented your acknowledgement. Let's start sending data!)*

It's way of saying hi occurs every time a TCP connection is established anywhere.

Handshake - a way for two devices to ensure that they're speaking the same protocol and will be able to understand each other

When duplex communication there is four way handshake, so
<-----FIN   --->ACK ----->FIN   ←--ACK

TCP Socket States

Socket - the instantiation(the actual implementation of something defined elsewhere) of an end-point in a potential TCP connection.
TCP Sockets require actual programs to instantiate them. You can constrast them with a port. This is more like vitual descripted thing. You can send traffic to any point you want,but you will only get response if the program has opened the socket at this point.
TCP Sockets can exists in a lot of states.

LISTEN - a TCP socket is ready and listening for incoming connection (only server side)
SYN_SENT - a synchronization request has been sent, but the connection hasn't been established yet. (client side)
SYN-RECEIVED: a socket previously in a LISTEN state has received a synchronization request and sent a SYN/ACK back.
ESTABLISHED - the TCP connection is in working order and both sides are free to send each other data
FIN_WAIT - a FIN has been sent, but the corresponding ACK from the other end hasn't been received yet.

CLOSE_WAIT - the connection has been closed at the TCP layer, but that the application that opened the socket hasn't been realesed its hold on the socket yet.
CLOSED - the connection has been filly terminated and that no further communication is possible

Choosing the way how to name the socket state is universal and does not depend on TCP protocol, so may vary on different operating systems.

Connection-Oriented and Connectionless Protocols

TCP(Transmission Control Protocol)
Our protocols at lower levels like IP and ethernet use chcecksum to ensure that all the data they received was correct. But we have never discussed any attempts to resending data, that doesn't passed this check. That is because, that is entirely up to transport layer protocol.

If some segments have to be resent due to errors at lower layers, it doesn't matter if they arrived slightly out of order. This is because sequence numbers allow for all the data to put back together in right order.

UDP(User Data Protocol) as connectionless protocol does not rely on connection, and does not even support the concept of acknowledgement
Streaming video with UDP:
each frame of video is a individual UDP datagram, for the best viewing experience you may hope that every single frame will arrive to the viewer, but it doesn't really matter if few of them get lost on the way, the video will still be pretty watchable, unless lost a lot of its frames.
You may actually be able to send higher quality video with UDP, that's because you be saving more availabable bandwidth for actual data transfer instead of overhead establishing connections and acknowledgements.

Firewalls

Transportation Layer Firewalls:
Have a configuration that enables them to block traffic to certain ports, while allowing traffic to other ports

5.APPLICATION LAYER

Just like with every other layer TCP segments have a generic data sections. These payload section is entire content of whatever data application want to send to each other (contents of webpage, streaming video contetn of Netflix app etc.).

In this layer there are a lot of different protocols. But they are all standardized, like for the same type of application they have to speak the same protocols (web browsers Chrome, Internet Explorer, Safari). Web browsers and web servers communicate with HTTP.

>> NETWORKING SERVICES

DNS: Domain Name Server:

A global and highlt distributed network service that resolves strings of letters into IP addresses for you.
Domain names -> IP addresses

1,2 are generally provided by ISP and often occur together. Also, any given dns server can fulfil many of these roles at once.
1. Caching - puropose is to store known domain name lookups for a certain amount of time.
//your ISP or local network will probably have caching name server availalabe
2. Recursive - perform full DNS resolution request
3. Root name server
4. TLD name server (top level domain)
5. Authoritative

DNS: TTL

All domain names in the global DNS system have a **TTL (time-to-love)** = value /in seconds/ that can be configured by the owner of a domain name for how long a name server is alowed to cache an entry before it should discard it and perdorm a full resolution again.

Several years ago it was normal for these TTLs to be really long, sometimes a full day or more. This is because, the general bandwidth availabable on Internet was just much less, so network adminisrators didn't want to waste bandwidth by constantly performing full DNS lookups. As the Internet has grown and gone faster these TTLs for most of domains has dropped to from few minutes to few hours. But it is important to know, that sometimes you still run some domain names with very long TTLs. It means that it can take up to take length of the total TTL for a changing a DNS record to be known to the entire Internet.

DNS: Full Recursive Resolution

0. The original computer sends a UDP packet to a local name server at port 53 asking for the IP for food.com

1. Contact the **root name server -**they are responsible for directing queries for the apropriate TLD Name Server.

// there are 13 root servers
// in the past this 13 root servers were distributed to very specific geographic regions, but today they are mostly distributed across the globe via Anycast) - Anycast is a technique that's used to reoute traffic to different destinations depending on factors like location, congestion, or link health
// it's better to think of them as 13 authorities that provide root name lookups as a servers

2. The root servers send **response** to DNS lookup **with a TLD name server** that should be queried
3. The TLD name server respond with a redirect to authoritative name server to contact
4. Authoritative name servers are responsible for the last two parts of any domain name.

In fact, your local computer will generally have its own temporary cache as well, that way it doesn't have to bother it's local nam eserver for any TCP connection either.

DNS uses UDP for a transport layer. If DNS does not get any response, just resend query.

DNS: Resource Record Types:

DNS operates with a set of defined resource record types. This allow for different kind of DNS resolutions to take place. There are dozens of different resrouce record types., but a lot of them serves to a very specialized purposes. We will cover the most basic ones there:
A record: - is used to point a certain domain name at certain IPv4 IP address. A single A record is developed for a single domain name. But a single domain name can have multiple A records too. This allows for a

technique named **DNS Round robin** - to be used to balance traffic across multiple IPs. This concept involves operating over a list of items - one by one - in order.
For example for address www.microsoft.com, we can configure four A records at the authoritative name servers for www.microsoft.com domain.
10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 - when the DNS resolver forms a lookup for the www.microsoft.com all four IPs wil be returned in the order first configured. The DNS resolving computer wil know that it should try to use the first entry, but it knows about all four, just in case connection to 10.1.1.1 fails. The next computer that perform a DNS lookup to www.microsoft.com will also receive all four IPs in a response but the order will change. The first entry would be 10.1.1.2.

AAAA - (Quad A) record: very similar but return IPv6 address instead of IPv4 address

CNAME record:(Canonical name) is used to redirect traffic from one domain name to another
By configuring a CNAME record for microsoft.com that resolves to www.microsoft.com teh resolving client will then know to perform another resolution attempt, this time to www.microsoft.com and then use IP returned as the second attempt.
//we could do the same thing with a A record, by setting the same A record for both microsoft.com and www.microsoft.com, and that would be just fine, but if the underlying IP address ever changes we need to change it in two places: in A records for both microsoft.com and www.microsoft.com

MX record - (Mail eXchange) - is used in order to deliver email to the correct server. Many companies run their web and mail servers on different machines with different IPs. The MX record makes it easy to ensure that email gets delivered to company mail server while other traffic will get delivered to the web server.

SRV record - service record- is used to define the location of various specific services.

TXT record - text / it's entirely free-form / clever engineers figured out ways to use it to communicate data that not originally intended to be communicated by a system like DNS. Is often use to communicate the configuration preferences about network services.

Anatomy of a Domain Name

Administration and definition of TLDs is handled by non-profit organization **ICANN (The Internet Corporation for Assigned Names and Numbers)**

The **www** portion is known as subdomain, sometimes reffered to as a hostname

DNS can technically support up to 127 levels of domain in total for a single fuly qualified domain name

DNS Zones - allows to make a multiple subdomains like la.company.com, paris.company.com and shanghai.company.com
Zones are configured by zone files - simple configuration files that declare all resource records for a particular zone.
Contain: **SOA**, resource record declaration

Start of authoritry SOA - declares the zone and the name of the name server that is authoritative for it.

NS records - indicate other name servers that might also be responsible for this zone

Reverse lookup zone files - these let DNS resolvers ask for an IP and get **FQDN(fully qualified domain, (www.google.com)** associated with it returned

DHCP

DHCP: Dynamic Host Configuration Protocol - an application layer protocol that automates the configuration process of hosts on a network. The entire point of DHCP is to help configure the network layer itself.

Dynamic allocation - a range of IP addresses is set aside for client devices and one of these IPs is issued to these devices when teh request one. So the IP of a computer can be deifferent almost every time it connects to network.

Automatic allocation - a range of IP addresses is set aside for assignment purposes

The main difference between the two above is that DHCP server is asked to keep track of which IP is assigned to cartain device in the past. If possible the DHCP will give the same IP address to the same machine the next time it connects to network.

Fixed allocation - requires a manually specified list of MAC addresses and their corresponding IPs. When it can't assign the IP specified in a list to the given device then it can also use automatic or dynamic allocation or refuse to assign the IP at all.

So DHCP can be used for more than just IP, subnet mask, gateway and DNS configuration. DHCP can also assign things like NTP:
NTP: Network Time Protocol - is used to keep all computers on a network synchronized in time.

DHCP DISCOVERY- the process by which a client configured to use DHCP attempts to get network configuration information.

1. Since the machine doesn't have the IP and it doesn't know the IP of the DHCP server a specially crypted broadcast message is formed. DHCP listens at UDP port 67, and DHCP discovery messages are always sent from UDP port 68. So DHCP discovery message is encapsulated in a UDP datagram with the destination port of 67 and the source port of 68. That is encapsulated into the IP datagram, where the destnation IP is 255.255.255.255, and the source IP of 0.0.0.0. That broadcast message will be delivered to every node on the local area network. If the DHCP server is present it will receive this message.

2. The DHCP server examins its own configuration to decide which if any address to offer to a client. This depends on its configuration if it is dynamic, automatic or fixed allocation. The resposne will be sent as the DHCPOFFER message with the destinatiomn port of 68, and source port of 67, with IP 255.255.255.255, so the DHCPOFFER is also a broadcast, it will reach every machine in the nework. The original client will recognize that this message was inteded for itself. This is because the DHCPOFFER has the field that specifies the MAC address of the client that sent the DHCP DISCOVERY message.

3. The client will now process the IP offer, to see what IP was offered to him. Technically, the DHCP client would reject this offer. However, the client often will response the DHCP Server with DHCP REQUEST message "Yes, I would like to have the IP that you have offered to me". Since the IP hasn't been assigned yet, it is again sent from IP 0.0.0.0 to 255.255.255.255.

4. The DHCP server receives the DHCP REQUEST message and respond with a DHCP ACK. The client will again know that the broadcast message was intended for itself because of the presence of its MAC address.

DHCP LEASE might last for days or just for a short amount of time. Once DHCP lease expire the DHCP client have to renegotiate a new lease by performing the DHCP Discovery process all over again.

NAT (Network Address Tranaslation)

Different operating systems has implemented the details of NAT in different ways. But the concepts are the same.

Basically: It takes one IP address and translate it into another.

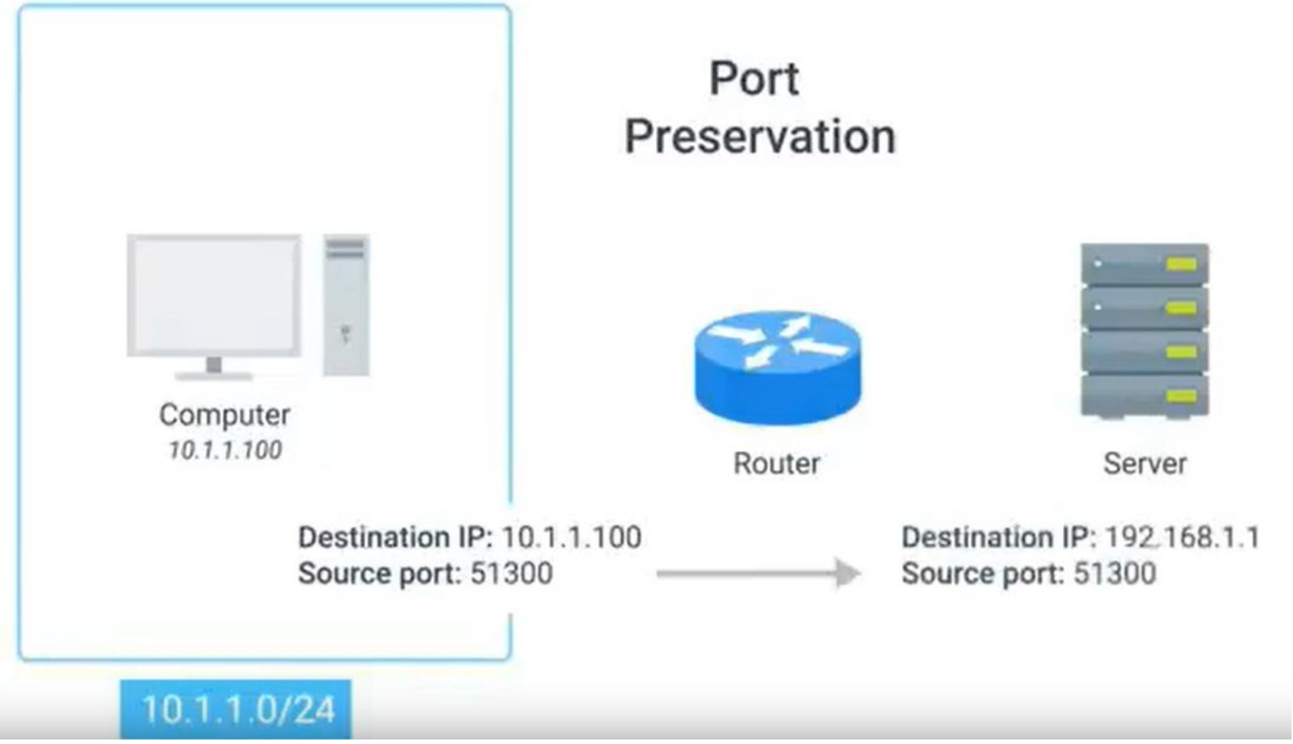
Definition: a technology that allows a gateway, usually a router or firewall, to rewrite the source IP of an outgoing IP datagram while retaining the original IP in order to rewrite it into the response.

Normally(**without NAT**), a router will inspect the content of a IP datagram, decrement the TTL by one, recalculate the checksum and forward the rest of the data at the network layer without touching it. **But with NAT**, the router will also rewrite the source IP address, which in this instance becomes router IP in network B. When the datagram gets to computer 2 in Network B, it will look like it was originated from the router, not from computer in the Network A. Now, computer 2 send its response which is sent back to the router. The router, knowing that the message is intended to computer 1, rewrites destination IP address before forwarding it alone. What NAT is actually doing here is hiding the IP of computer 1 from computer 2 (**IP masquerading)** It's important security concept. The most basic concept here is that no one can establish a connection to your computer if they don't know what IP address it has. When all IPs in Network A are translated to routers own, the entire address space of Netwrok A is protected and invisible, this is known as **One-to-many NAT.**

NAT and Transport Layer Difficulties

NAT at the network layer is pretty easy to follow. One IP address is translated to another by a device, usually router. But at the transport layer things are a little bit more complicated.
With One-to-many NAT, router has to find out which response (that is directed to its address!) is directed to which address in Network A.

The simples way to do it:
Port preservation - a technique where the source port chosen by a client is the same port used by the router.



Even with a large set of ports, it is still possible for two different computers on the network to both choose the same source port around same time.

Port forwarding - a technique where specific destination ports can be configured to always be delivered to specific nodes.

VPN

A technology that allows for the extension of a private or local network to hosts that might not be on that local network.
The most popular use case: Emplyers can acces using VPN the business newtork when they are not in the office.

VPNs are a tunneling protocols, they provide access to something not locally availabable. When establishing a VPN connection you may also say, that BPN tunnel has been established. This would provision the computer with a virtual interface with an IP that matches the address space of the network which has established a connection with. By sending data out of this virtual interface the computer can access internal resources just like it was physically connected to the private network.

Most VPNs work by using the payload section of the transport layer to carry an encrypted payload, that actually contains the entire set of packets. The network, the transport and the application layers of the packet intended to traverse the remote network. Bascially, this payload is carried to the VPN end-point, where all the other layers are crypted away and discarded. Then, payload is unencrypted, living the VPN server with the top three layers of a new packet. This gets encapsulated with the proper data link layer information and send out across the network. This process is completed in the inverse: opposite direction. VPN usually requires strict authentication procedures in order to assure that it can only be connected to by computers and users authorized to do so.

In fact, VPNs were one of the first technologies with two-factor authentication.

Two-factor-authentication: a technique where more than just a username and password are required to authenticate. Usually, a short numerical token is generated by the user by specialized part of hardware or software.

VPNs can also be used to establish **side to side connectivity.**
VPN Server ----router   ///////TUNNEL//////   router2   VPN Server2
In this way two separately two physically sperated offices might be able to act as one network

PROXY

A server that acts on behalf of a client in order to access another service
Cons:

- Anonymity
- Security
- Content filtering
- Increased perfomance

Examples from earlier notes: Gateway Routers.
The concecpt of a proxy is just a concept of an abstraction. It does not refer to any specific implementation. Proxies exist at almost every layer of our networking model.

WEB PROXY
Several year ago was used by companies to increase perfomance. If someone requested the same webpage, it could just return cache data, instead have to retrieve the fresh copy every time. This kind o proxy is pretty old. Most companies now have fast connection, so providing cached versions of webapages is not a big deal for them. Also, the web began to be more dynamic.
The web proxy still can be used for example in work place, when we want to hide that we enter a censored website.

REVERSE PROXY
A service that might appear to be a single server to external clients, but actually represents many servers living behind it. A good example of it, is how many websites are architected today, very popular websites like twitter receives so much traffic, that is no way a single web server could possibly handle all of it. A website that is popular, may need many many servers in order to keep up with processing all incoming request. From the client persepctive

it looks that he is connected to a same server, but actually the reverse proxy server is distributing these incoming requests to lots of different physical servers.

Proxy server is any server that works as intermediary between client and server.

WAN

WAN (Wide Area Network Technologies) - acts like a single network but spends across multiple physical locations. WAN technologies usually require that you contract the link across the Internet with your ISP.

We have network A at one side of the contry, and network B on the second one.
Each of these networks ends on demarcation point, which is where ISPs takes over. The area between each demarcation point and ISP core network is called the local loop

WAN works by using number of different protocols at the data link layer to transport your data from one side to another.

A popular alternatives to WAN technologies are point-to-point)site-to-site) VPNs, WANs are faster than them, but since we can have everything in the cloud, like email servers etc. we don't need to still spend so much money on WAN, while we can use VPNs as well to still have a contact within the company.

>>WIRELESS COMMUNICATION

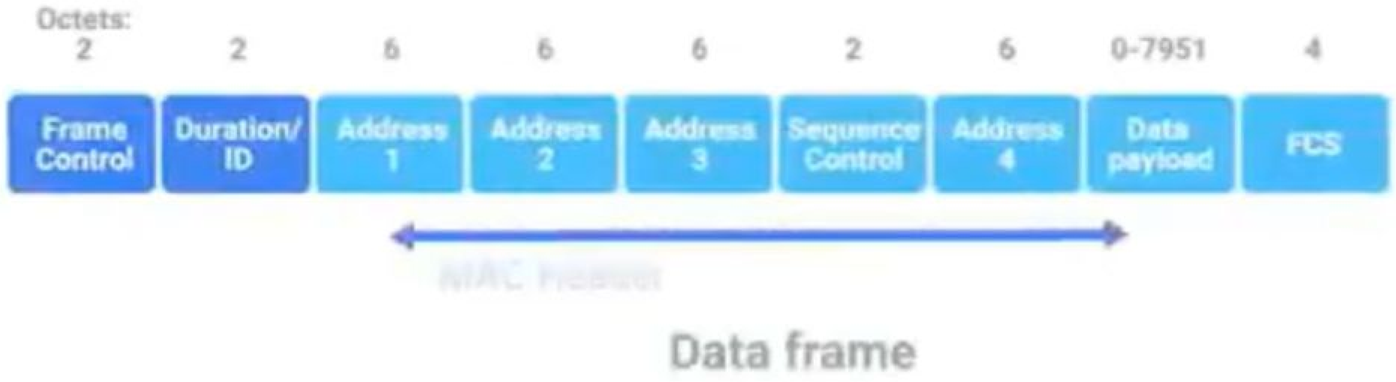
IEEE 802.11 standards -> this set of sepcifications make up a set of technologies we call **WiFi**

Wireless networking devices communicate using **radiowaves**

Frequency band - a certain section of the radio spectrum that's been agred upon to be used for certain communications

In terms of our networking layer, we should think of 802.11 protocols, as defining how we operate at both the physical and the data link layers.

802.11 frame:



Frame control - describe how the frame itself should process // for example: what version of 802.11 was used //
Duration/ID - specify how long the total frame is //the receiver thanks to that can know how to listen //
Address 1: the MAC address of the sending device
Address 2 - intended destination //MAC of the access point that should receive the frame//
.../
Data payload
Frame Check Sequence field - contains a checksum, frequency redundancy check/ just like ethernet

Wireless Network Configuration.

Ad-hoc - nodes speak directly to each other //there isnt really any network supporting instrustructure//are the most popular ones!

Wireless LANS - one or more accespoints acts like a bridge betweenthe wireless network

Mesh network - is a local network topology in which the infrastructure nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients

Wireless LAN/WLAN - consists of one or more access points, which acts like bridges between the wireless and wired networks. The wire network operates as normal LAN,

Wireless Channels

Individual smaller sections of the overall frequency band used by a wireless network.

Collision domain is any one network segment where one computer can inerrupt another,

All devices in question have to stop transmission, they wait a random amount of time and try again. This slow things down.

//Switches remember which computer lives on which physicasl interfaces, so traffic is only send to the node is intended to. // we have similar problem with wireless networks.

Channels helps to fix this problem.

Wireless Security

WEP / WPA / WPA2

MAC filtering - you configure your access points to only allow for connections from a specific set of MAC addresses belonging to devices you trust