# 

[**The Bits and Bytes of Computer Networking by Google**](#_83wjae9w0p7v) **2**

[The TCP/IP Five-Layer Network Model](#_vg1kpoaozqnf) 3

[The basics of Networking Devices](#_xariif6vfuae) 3

[Cables](#_p82w1ivs7152) 3

[Hubs and Switches](#_5swtq0po23j7) 4

[Switch](#_40igjm2g3xda) 4

[Routers](#_niztd2u2vzus) 4

[Servers, Clients](#_l35kk0ku6lh3) 4

[Physical Layer](#_9rubfwlis6pe) 4

[Twisted pair cabling and duplexing](#_mev3ebrvy8su) 5

[Network ports and Patch panels](#_khmjtri4gmc6) 5

[Ethernet and MAC Address](#_hm4hcb5unyaw) 5

[Unicast, Multicast](#_rquf1pjpsylf) 5

[Dissect Ethernet Frame](#_u3axbxrfvn0u) 5

[Network Layer](#_df9gu4ac2ijt) 6

[IP Addresses](#_h0dfd2xkyxt8) 6

[IP Datagrams](#_e4kg7vxka6qu) 6

[Subnetting](#_2x7fg0vkv7oo) 7

[Address Classes](#_6nyzavi0k7n4) 7

[ARP](#_cinaw36dlowk) 8

[Subnetting](#_uggcfxyqop6q) 8

[Subnet Masks](#_6c3hhqtxb3zn) 8

[CIDR](#_xveohky14q39) 9

[Routing](#_7e6k1xc8z1e4) 10

[Routing Table](#_npn3xz2h7m6k) 10

[Interior Gateway Protocols](#_52wrg6i00pwy) 10

[Exterior Gateway Protocols](#_u4q4k0fwnwae) 11

[Non - Routable Address Space](#_wppgoqsonsf9) 11

[Transport and Application Layers](#_3tlu6zandpmw) 12

[The Transport Layer](#_yw18kqex3ajm) 12

[Dissection of a TCP Segment](#_7doq8ifua2l8) 12

[TCP Control Flags and Three-Way Handshake](#_hmthlu6w1lz0) 13

[Connection-Oriented and Connec tionless Protocols](#_662laskdfc3) 14

[The Transport Layer](#_sn7e94c3w184) 14

[The Application Layer](#_2h7r07gtjdv4) 14

[Application Layer, OSI Model](#_wltmlyhs1ya6) 14

[Network Services](#_xkzhyp6uezdi) 15

[Domain Name System (DNS)](#_w9jnu2z5ar43) 15

[Process of Name Resolution](#_j3c89fm240y6) 15

[DNS and UDP](#_dk5s9cc3snjv) 16

[Name Resolution in Practice](#_58c673gtjobl) 16

[Anatomy of a Domain Name](#_7ysz1ltgc9sk) 16

[DNS Zones](#_fv80uf4km00y) 17

[Overview of DHCP](#_t61uskuskgsm) 17

[Basics of NAT](#_lz9rc22u8hvp) 18

[NAT And Transport Layer](#_kudjxqcu1ot9) 18

[NAT, Non-Routable Address Space, and the Limits of IPv4](#_jj121olmd0hm) 18

[VPN, Proxies](#_yzp3jty9yogu) 19

[Connecting to the Internet](#_v93zpuz2lbrs) 19

[Dial-up, Modems, and Point-to-Point Protocols](#_fuoc538ia8lc) 19

[Broadband Connections](#_yq3dkh2gowy5) 19

[Digital Subscriber Line](#_jc56w3y92z60) 19

[Cable Broadband](#_igkalz3m5h0q) 20

[Fiber Connection](#_x8x5j21vbcet) 20

[WAN - Wide Area Network](#_gffa48tibol0) 20

[Point-to-Point VPN](#_nvnwdsuihdil) 20

[Intro to Wireless Networking Technologies](#_t6s49t5x9bz3) 21

[Wireless Network Configurations](#_up9vkai8e8zb) 21

[Wireless Channels](#_jk8i7qg02rnt) 21

[Wireless Security](#_x1al06dmjnhb) 21

[Troubleshooting and the Future of Networking](#_hls7k0jy9dlj) 22

[Ping: Internet Control Message Protocol](#_rxtuaaoakwgs) 22

[Traceroute](#_liuh5ssi48tg) 22

[Testing Port Connectivity](#_5lpla3danta2) 22

[Name Resolution Tools](#_vkpcswdmhu6p) 22

[Public DNS Servers](#_xwv1o7161v5u) 22

[DNS Registration and Expiration](#_5l8mxm3q9amf) 22

[Hosts Files](#_pu2cxhr10epq) 22

[What is the Cloud?](#_eeb6sym70ij0) 23

[IPv6 Addressing and Subnetting](#_oq712hgv1w8h) 23

[IPv6 Headers](#_geugkphgsj3w) 23

[IPv6 and IPv4 Harmony](#_71l15uv3qfvz) 24

# 

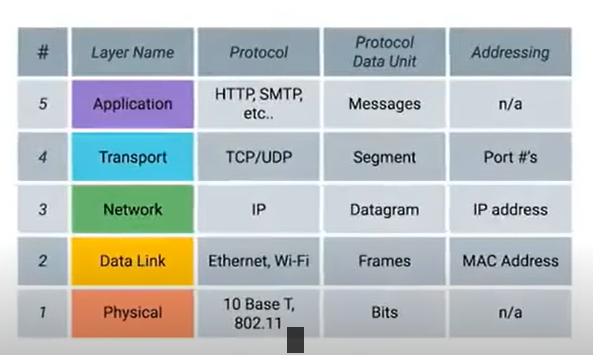
# 

# The Bits and Bytes of Computer Networking by Google

Protocol - a defined set of standards that computers must follow in order to communicate properly

Computer networking - the name we’ve given to the full scope of how computers communicate with each other

## The TCP/IP Five-Layer Network Model



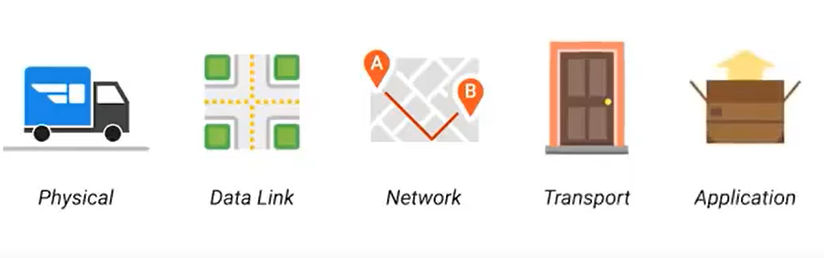
Physical layers - managing sending signals, wires and cables

Data Link - responsible for getting data across a single link

Network Layers - allow different networks communicate to each other using routers

Transport layer - Sorts out which client / server is supposed to get that data

Application Layer - Allow browsing web, receiving emails etc



### The basics of Networking Devices

#### Cables

Connect different devices to each other, allowing data to travel between them

Copper - Most common form, made up of multiple copper wires inside a plastic insulator.

Most common forms of copper twisted-pair cables are Cat5, Cat5e, Cat6

Crosstalk - When an electrical pulse on one wire is accidentally detected on another wire

Fiber optic cables - Contain individual optical fibers, tiny tubes made out of glass. Transform beams of light to represent 0’s and 1’s. Is not affected by electro-magnetic fields. Much more expensive and fragile.

#### Hubs and Switches

Hub - Physical layer that allows for connections from many computers at once

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

#### Switch

Similar to a hub, but Switch is a Data Link layer device. It can inspect the content of the Ethernet protocol data, determine which system must receive this data and send it only to that system. This greatly reduces or eliminates the sizes of Collision domains

#### Routers

Hubs and Switches are primarily used to connect computers on a single network, usually referred to as a LAN (local area network)

Router is a device that knows how to forward data between independent networks.

Router is a layer 3 device. Router can inspect IP data to determine where to send things. Routers store internal tables to determine how to route traffic between lots of different routers.

BGP - Border Gateway Protocol - Routers share data with each other via this protocol, which lets them learn about the most optimal paths to forward traffic.

#### Servers, Clients

Server - something that provides data

Client - something that requests data

### Physical Layer

Consists of devices and means of transferring bits across networks.

Bit - smallest representation of data

Modulation - a way of varying the voltage of the charge moving across the cable.

#### Twisted pair cabling and duplexing

Twisted pair - most common form of wire. Twisted nature helps against magnetic interference and crosstalk

A standard cat6 cable has 8 wires consisting of 4 twisted pairs in a single jacket. These cables allow for duplex communication

Full-Duplex communication - two-directional

Simplex communication - one-directional

Half-duplex - Two-directional but one device at a time, taking turns

#### Network ports and Patch panels

RJ45 Plug - Most common plug for network ports.

Patch Panel - device containing many network ports, a container for ports.

#### Ethernet and MAC Address

CSMA/CD - Used to determine when the communication channels are clear, and a device is free to transmit data. It checks if there is no data being transferred, a node is free to send data.

MAC Address - a globally unique identifier attached to an individual network interface.

MAC Address consists of 6 octets of 8 bits = 48 bits

First 3 octets - Organizationally Unique identifier (OUI)

Last 3 octets - Vendor Assigned

#### Unicast, Multicast

Unicast - meant for 1 receiving address

Multicast frame - Sent to every device but with condition that the receiver can understand

Broadcast - sent to every device on LAN

### Dissect Ethernet Frame

Data Packet - All-encompassing term that represents any single set of binary data being sent across a network link

At Ethernet level - Ethernet frame - highly structured collection of information presented in a specific order



Preamble - 8 bytes long, can be split in 2 sections. Ends with SFD

SFD - Signals to a receiving device that the preamble is over

Destination, Source MAC Addresses

Ether Type - used to describe the protocol of the contents of the frame

VLAD header - indicated that the frame itself is a VLAN Frame

VLAN - Technique that lets you have multiple logical LANs operating on the same physical equipment

Payload - actual data being transported. Can be 46 to 500 bytes long.

FCS - Frame check sequence. 32 bit number that represents checksum value. Calculated using Cyclical Redundancy Check (CRC)

CRC - Important concept for data integrity, used all over computing. A mathematical transformation. Included for the receiving network to infer if it received corrupt data.

### Network Layer

#### IP Addresses

32 Bit number, grouped by 4 octets, notated in decimal by 8 bits

172.16.254.1

IP Addresses belong to networks, not to devices attached to those networks

DHCP - Assigns Dynamic Address - reserved for clients

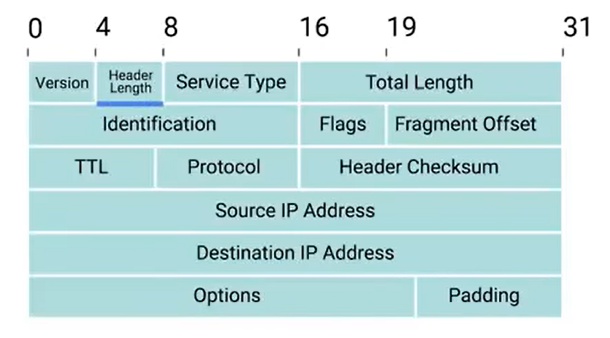
Static IP Addresses - reserved for servers and network devices

#### IP Datagrams

A highly structured series of fields

The most common version of IP - IPv4

Header of IP Datagram:



Largest datagram is the largest number in Total length - 65535 bits

Fragmentation - Splitting a datagram in many smaller datagrams

TTL - Time to live - 8 bit field, that indicates how many routers a datagram can hop on. Main purpose - infinite loops

Encapsulation - Each layer below encapsulates the entire packet of the above layer

### Subnetting

Split in 2 - Network Id and Host Id

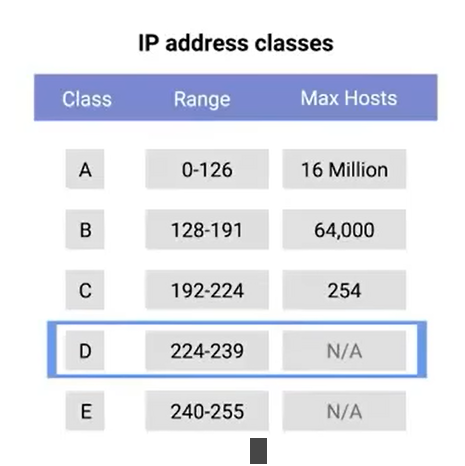
#### Address Classes

Class A, B, C

A - first octet for Network Id, last 3 - Host Id,

B - first 2 octets for Network Id, Last 2 - Host Id

C - First 3 Octets for Network Id, Last 1 - Host Id



Class D - For multicast over network

Class E - Unassigned, for testing purposes

#### ARP

Address Resolution Protocol - Used to discover the hardware address of a node with a certain IP Address

ARP Table - List of IP Addresses and MAC addresses associated with them

ARP table entries generally expire after a short amount of time for updates

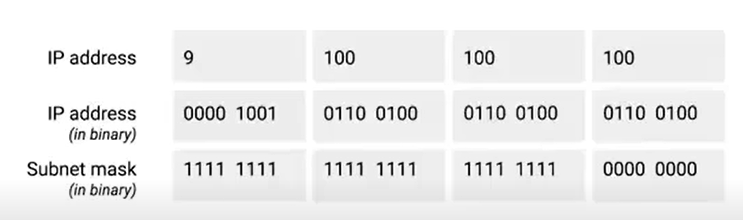
#### Subnetting

A process of taking a large network and splitting it up into many individual and smaller subnets

##### Subnet Masks

Core routers use Network ID to send datagram to the Gateway router. Gateway router has additional information to send data to the next gateway router or to the machine.

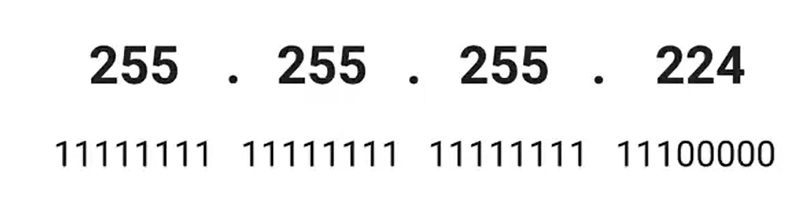
Subnet Masks are 32 bit numbers that are written as 4 octets in decimal.



Part with All 1’s - we can ignore

Part with All 0’s - what we keep as Host Id

A subnet can have 2 less than the total number of Host Ids available. 0 Is not used, and 255 is used for broadcasting to the subnet



Shorthand way to writing subnet mask

255.255.255.244 - /27 (27 bits in mask)

8 bit number - 2^8 - 0-255 values

16 bit number - 2^16 values

Computer can use AND operator to determine the Network ID of the destination IP, compare with its own network ID to determine if they are in the same network space

#### CIDR

Classless inter domain routing

Demarcation point - Describe where one network or system ends and another begins.

Previously we relied on Network Id, Host Id, Subnet Id to determine correct location

CIDR Network Id, Subnet Id are combined to one.

CIDR Notation:

Abandons concept of classes

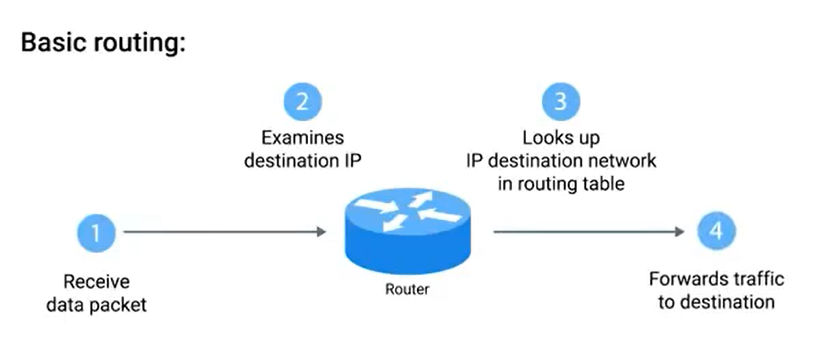
9.100.100.100 with mask 255.255.255.0 -> 9.100.100.100/24

in CIDR you care only about the mask and not about classes of networks

Adding one more bit from subnet mask to host Ids space gives you 2x + 2 more hosts

### Routing

Router - A network device that forwards traffic depending on the destination address of that traffic. Has at least 2 network interfaces



#### Routing Table

Destination Network Column - Row for each network that Router knows About, Network Id and Netmask

Nexthop - IP Address of the next router that should receive data

Total Hops - Many paths from A to B, router keeps track how many hops from this target

Interface - Which of its interfaces to forward traffic, matching destination table out of

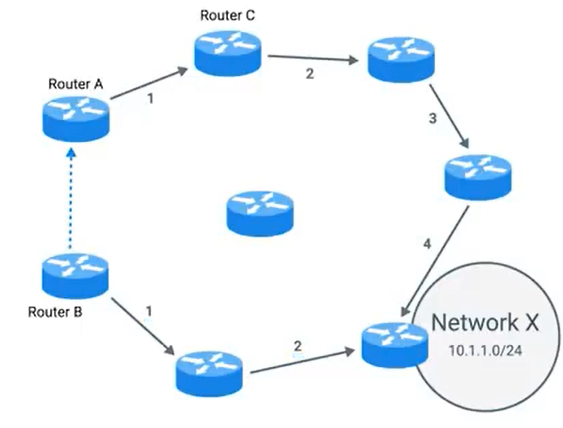
#### Interior Gateway Protocols

Used by routers to share information within a single autonomous system

Autonomous system - a collection of networks that all fall under the control of a single network operator

Link state routing protocols - Every router in the system knows all information about every other router in the system - More modern approach

Distance vector protocol - Old approach - Takes its routing table, sends this list to every neighboring router.



#### Exterior Gateway Protocols

Used to communicate data between routers, when they need to share info between different organizations

IANA - Responsible for ASN and IP address allocation

ASN - 32 bit numbers, assigned to individual autonomous systems. as single decimal number.

### Non - Routable Address Space

Ranges of IPs set aside for use by anyone that cannot be routed to.

3 ranges of non-routable addresses, Anyone can use them

10.0.0/8

172.16.0.0/12

192.168.0.0/16

These ranges are free to use for internal networks.

They can be used within autonomous systems via interior gateway protocols, but exterior gateway protocols will not

## Transport and Application Layers

### The Transport Layer

Multiplexing - nodes on network have the ability to direct traffic towards many receiving servers

Demultiplexing - taking traffic aimed at the same node and delivering it to the proper receiving server

Transport layer handles multiplexing and demultiplexing through ports

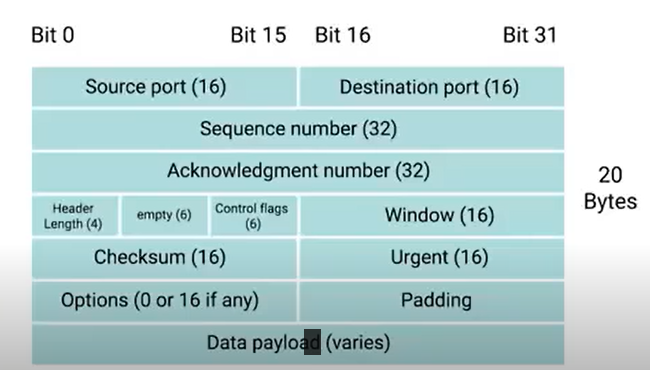
Port - a 16-bit number that’s used to direct traffic to specific services running on a networked computer

Ports are denoted by decimal number after IP - Socket Address

10.1.1.100:80

21 - FTP port, used for transferring files from one computer to another.

#### Dissection of a TCP Segment



Made up of a TCP Header and Data

Header:

Source / Destination Ports

Sequence number - if the segment is split into many sequences

Acknowledgment number - Next segment number

#### TCP Control Flags and Three-Way Handshake

URG - Urgent

ACK - Acknowledged

PSH - Push

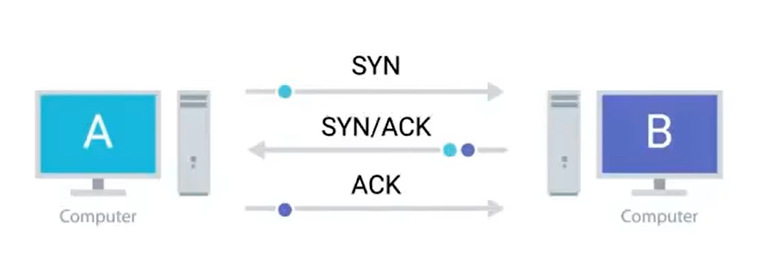
RST - One of the sides of TCP Connection hasn’t been able to properly recover from a series of missing or malformed segments

FIN - Finish

Handshake

A way for 2 devices to ensure that they’re speaking the same protocol and will be able to understand each other

Three-way Handshake - Way to start connection



Four-way handshake - Way to End connection



TCP Socket State

LISTEN - a TCP Socket is ready and listening for incoming connections - Server Side

SYN\_SENT - A synchronization request has been sent but connection not established - Client Side

SYN-RECEIVED - A socket previously in a LISTEN state has received a synchronization request and sent a SYN/ACK Back - Server side

ESTABLISHED - TCP Connection is in working order - On both Server and Client side

FIN\_WAIT - FIN Sent but ACK not received

CLOSE\_WAIT - Connection has been closed at TCP layer, but the application that opened the socket hasn’t released its hold on the socket yet

CLOSED - connection has been fully terminated

#### Connection-Oriented and Connec tionless Protocols

Connection-Oriented Protocol (TCP) - Establishes connection and uses this to ensure that all data has been properly transmitted through constant acknowledgments

Connectionless Protocols (UDP) - Does not support connections or acknowledgments, just send a packet to a destination port. Video, Music streaming

### The Transport Layer

Firewall - A device that blocks traffic on some criteria

### The Application Layer

Protocols: HTTP, SMTP

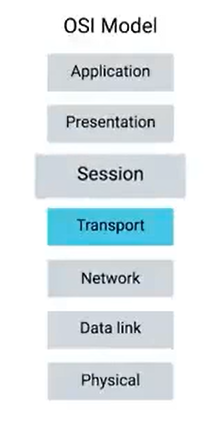
HTTP - Web Browser

FTP - File Transfer

#### Application Layer, OSI Model

OSI - Open Systems Interconnection

7 Layers



Session Layer - Facilitates communication between application and transport layers

Presentation Layer - Responsible for making sure that the unencapsulated application layer data is able to be understood by the application in question

#### 

## Network Services

### Domain Name System (DNS)

A global and highly distributed network service that resolved strings of letters into IP Addresses for you

Domain name - something that can be resolved by DNS

If the website changes IP Address, it can simply change the DNS to resolve the domain name to new IP Address

It also allows organizations to resolve the user to a data center closest to him for better speed. I.e if you are in this region, resolve to this IP address

### Process of Name Resolution

DNS Server must be configured on the host to work on the network properly.

Types of DNS Servers:

1. Caching Name servers
2. Recursive name servers
3. Root name servers
4. TLD name servers
5. Authoritative name servers

Caching and recursive name servers - Purpose is to store known domain name lookups for a certain amount of time

TTL - Value in seconds for how long a name server should cache in DNS Server.

Full Recursive Resolution

1. Root name Servers via Anycast - a technique used to route traffic to different destinations based on factors
2. Root servers respond with TLD Name servers for the caching name server to lookup
   1. TLD - Top level domain: .com, .net etc
3. TLD Name servers respond with redirect with the authoritative name server
4. Authoritative name server responds with the IP of the required DNS

Host DNS Server also has local cache

### DNS and UDP

DNS uses UDP for the transport layer instead of TCP. UDP is connectionless. DNS can generate a lot of traffic. TCP would create a lot of overhead.

### Name Resolution in Practice

A record - used to point a certain domain name at a certain IPv4 IP Address. One A record for one domain name. But a domain name can have multiple A records

DNS Round-robin

Iterating over a list of A Records one by one in order. Ensures an equal balance of entries for each record on the list.

Quad A Record - returns an IPv6 Address

CNAME Records - used to redirect traffic from one domain name to another

MX record - mail exchange

SRV record - service record

TXT record - text

### Anatomy of a Domain Name

www.google.com

Top level Domain (TLD) - The last part of a domain name, .com, .net etc

Domain - second part of the domain name (google) - Used to demarcate where control moves from a TLD name server to an authoritative name server

Sub-domain, Host - www

Fully Qualified Domain Name (FQDN) - Host name, Sub-domain, domain, top level domain

Rules:

1. Up to 127 sub-domains for FQDN allowed
2. Each section can only by 63 chars long
3. Complete FQDN - 255 characters

### DNS Zones

Allows for easier control over multiple levels of a domain

company.com can be split in 3 DNS zones

la.company.com

pa.company.com

ch.company.com

Each sub-domain will have authoritative zones

Zone file - Simple configuration file that declare all resource records for a particular zone

Zone file has to contain:

1. SOA - Start of Authority - Declares the zone and the name of the name server that is authoritative for it
2. NS records - Indicate other name servers that might also be responsible for this zone
3. Reverse Lookup zone files - let DNS Resolvers ask for an IP and get the FQDN associated with it returned. These files are the same as Zone files, but they have Pointer Resource record (PTR) Instead of A records and Quad A records. PTR Resolved IP to a name

### Overview of DHCP

Dynamic Host Configuration Protocol - Application Layer protocol that automates the configuration process of hosts on a network

With DHCP, a machine can query the DHCP Server when it connects to the network and receive all network configurations in one go

It reduces administrative overhead, and addresses the problem of what IP to assign to what machine.

Modes of DHCP:

1. 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
2. Automatic Allocation - A range of IP Addresses is set aside for assignment purposes. The main difference - DHCP Server is asked to keep track to which users they assigned which IPs, and assign the same IP to the same machine if possible
3. Fixed Allocation - Requires a manually specified list of MAC addresses and their corresponding IPs

U can also use DHCP to assign Network Time Protocols, 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

4 Steps of DHCP Discovery / DHCP Lease

1. Server Discovery - DHCP Discover message to the network, broadcasted for specific port from a specific port and waiting for answer
2. DHCP checks its configuration, and returns an offer message (broadcasts to the network to a specific port)
3. Client Processes the offered IP, and can reject the offer, or responds with DHCP Request message (broadcast)
4. Responds with DHCP Ack (Broadcast)
5. Client now can use the configuration presented by DHCP, and configures its own network layer.

Lease - because DHCP Discovery IP Address has lifespan

### Basics of NAT

NAT - Network Address Translation - Takes IP Address and translates it into another.

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 response

IP Masquerading (One-to-many NAT) - IP masquerading is a process where one computer acts as an IP gateway for a network. All computers on the network send their IP packets through the gateway, which replaces the source IP address with its own address and then forwards it to the internet. Perhaps the source IP port number is also replaced with another port number, although that is less interesting. All hosts on the internet see the packet as originating from the gateway.

### NAT And Transport Layer

Port Preservation - Source port chosen by a client is the same port used by the router

Port Forwarding - Technique where specific destination ports can be configured to always be delivered to specific nodes - allows for IP masquerading and simplifies how external users use services in the same organization

### NAT, Non-Routable Address Space, and the Limits of IPv4

Using NAT and Non-Routable Address Space, Many nodes on network can use only one IPv4 Address (of the gateway) to communicate to outside world

### VPN, Proxies

VPN - Technology that allows for the extension of a private or local network to hosts that might not be on that local network

A tunneling protocol. VPN Tunnel

VPNs work by using the payload section of the transport layer to carry an encrypted payload that actually contains a second set of packets

Proxy Services - A server that acts on behalf of a client in order to access another service

1. Anonymity
2. Security
3. Content Filtering
4. Increased Performance

Proxy is an abstraction

Web Proxies - Proxy for web traffic - for increased performance. Also they can inspect the data requested and allow or deny depending on what’s requested.

Reverse proxy - A service that might appear to be a single server to external clients, but actually represents many servers living behind it. Also reverse proxies can be used for decrypting the requests.

Proxy is any servers that act as intermediary between a client and server.

## Connecting to the Internet

### Dial-up, Modems, and Point-to-Point Protocols

Modems - Modulator / Demodulator - take computer data and turn into audible wavelengths transmitted over telephone systems.

Baud rate - measurement of how many bits can be passed across a phone line in a second

Computers could send data at about 110 bits/second

### Broadband Connections

Broadband - any connectivity technology that is not dial-up connection. This connection is long-lasting

T-carrier technologies

Transmitting multiple phone calls over a single link

### Digital Subscriber Line

Like Dial-ups, they establish connection over phone lines, but they are long running, working on different wavelengths than audio signals and don’t interfere with an audio line.

ADLS, SLDS - Asymmetric DSL / Symmetric DSL

### Cable Broadband

Coaxial Cables, used for TV transmission, used for internet connection.

Like dial-up, it works on different frequencies for no interference, and deliver high speed internet.

Cable modem - Manages cable connection, connects it to Cable management termination system, which connects lots of cable connections to an ISPs core network.

### Fiber Connection

Light and signal degrades over distance.

FTTX - Fiber to the X

FTTN - Fiber to the Neighbourhood - Fiber to the single cabinet that serves population, Copper cables will be used from this cabinet

FTTB - Fiber to the Building - Fiber used for individual building, and copper cables inside building

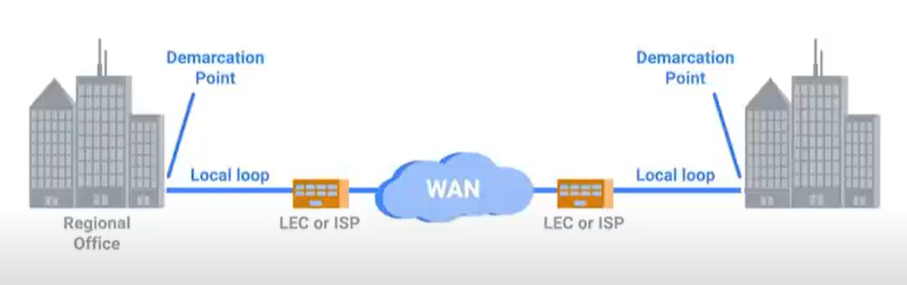
FTTH - Fiber to the Home - Fiber to each individual residence.

FTTP - Fiber to the Premises

Optical Network Terminator - Converts data from protocols the fiber network can understand, to those that more traditional, copper networks can understand

### WAN - Wide Area Network

Acts like a single network, but spans over multiple locations.



### Point-to-Point VPN

Popular alternative to WAN

Establishes VPN Between 2 sites

### Intro to Wireless Networking Technologies

A way to network without wires

IEEE 802.11 - Protocols that define Wi-fi

802.11 = physical and data link layers



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

Wireless Access Point - A device that bridges the wireless and wired portions of the network

### Wireless Network Configurations

Ad-hoc Network - No network infrastructure. Devices connect directly to each other

WLAN - Wireless LAN - One or more access points which act as bridges between wireless and wired devices.

Mesh networks - Only wireless Access points

### Wireless Channels

Channel - Individual, smaller sections of the overall frequency band used by a wireless network

### Wireless Security

Wireless is less secure than Wired

WEP - Wired Equivalent Privacy - Weak encryption algorithm.

WPA - Wifi protected access - More Secure than WEP

WPA2 - More secure than WPA

MAC Filtering - configure access points to only allow connections from specific MAC Addresses

## Troubleshooting and the Future of Networking

### Ping: Internet Control Message Protocol

ICMP - Internet Control Message Protocol

Ping - lets you send a special type of ICMP message called an Echo Request. If the destination is up and running and able to communicate on the network, it’ll send back an ICMP Echo Reply

### Traceroute

Utility that lets you discover the path between two nodes and gives you information about each hop along the way

mtr, pathping - Alternatives to Traceroute, more long-lasting traceroutes

### Testing Port Connectivity

netcat - Linux / MacOS

Test-NetConnection - Windows

### Name Resolution Tools

nslookup - nslookup hostname - says what server was used and resolution result to find the ip address.

### Public DNS Servers

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

Most public DNS servers are available globally through anycast

### DNS Registration and Expiration

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

### Hosts Files

A flat file that contains, on each line, a network address followed by the host name it can be referred to as

Loopback address - a way of sending network traffic to yourself

127.0.0.1 - localhost

Host files are a popular way for computer viruses to disrupt and redirect users’ traffic

### What is the Cloud?

Cloud Computing - A technological approach where computing resources are provisioned in a shareable way, so that lots of users get what they need, when they need

Hardware Virtualization - Allows the concepts of physical machine and logical machine to be abstracted from each other

Virtualization - A single physical machine, called a host, could run many individual virtual instances, called guests

Hypervisor - A piece of software that runs and manages virtual machines, while also offering these guests a virtual operating platform that’s indistinguishable from actual hardware

Hybrid cloud - A term describing situations where companies might run things on a private cloud, and other things on public cloud

### IPv6 Addressing and Subnetting

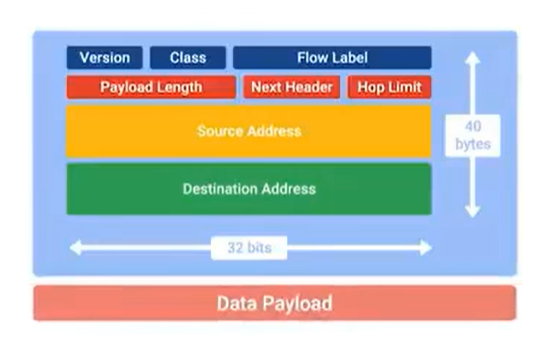
First 64 bits - Network ID

Second 64 bits - Host ID

The same subnetting as IPv4

### IPv6 Headers

Much simpler that IPv4



### IPv6 and IPv4 Harmony

IPv6 has addresses that can directly correlate to IPv4

IPv4 traffic can travel across IPv6 network

IPv6 Tunnels - Servers that take incoming IPv6 traffic and encapsulate it within traditional IPv4 Datagram

IPv6 Tunnel Broker - Companies that provide IPv6 tunneling endpoints for you.