Course Link: https://www.youtube.com/watch?v=QKfk7YFILws

Intro

- **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

TCP/IP Five-Layer Network Model

#	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc..	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

- **Physical Layer** - represents the physical devices that interconnect computers
- **Data Link Layer** - responsible for defining a common way of interpreting these signals so network devices can communicate
- **Network Layer** - allows different networks to communicate with each other through devices known as routers
    - **Internetwork** - a collection of networks connected together through routers, the most famous of these being the **internet**
    - **IP** is the heart of the internet and most smaller networks around the world
- **Transport Layer** - sorts out which client and server programs are supposed to get that data
- **Application Layer** - user interacts with this layer

Think of a package being delivered: **Physical Layer** is the delivery truck > **Data Link layer** is how it gets from one intersection to the next > **Network Layer** identifies which roads need to be taken to get from A to B > **Transport Layer** ensures delivery driver knows to knock on your door > **Application Layer** contents of the package itself

The Basics of Networking Devices

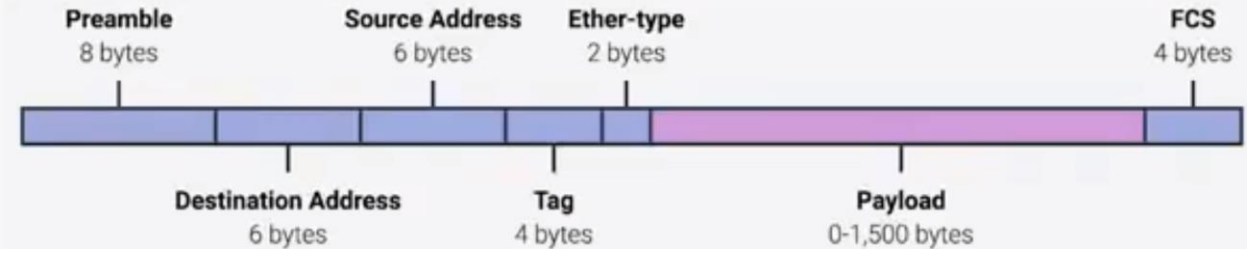
- **Cables** - connect different devices to each other, allowing data to be transmitted over them
    - The most common forms of copper twisted-pair cables used in networking are **Cat5, Cat5e,** and **Cat6** cables.
    - **Crosstalk** - when an electrical pulse on one wire is accidentally detected on another wire
- **Fiber Cables** - contain individual optical fibers, which are tiny tubes made out of glass about the width of a human hair
- **Hub** - physical layer device that allows for connections from many computers at once
- **Collision domain** - a network segment where only one device can communicate at a time, causes interference
- **Switch** - L2 device, manages data packets
- Hubs & Switches are the primary devices used to connect computers on a single network, usually referred to as a **LAN**, or **Local Area Network**
- **Router** - device that knows how to forward data between independent networks
    - **BGP (Border Gateway Protocol)** - routers share data with each other va this protocol, which lets them learn about the most optimal paths to forward traffic

The Physical Layer

- **Bit** - smallest representation of data that a computer can understand; it's a one or zero
- **Modulation** - varying the voltage of this charge moving across the cable
- **Duplex Communication** - the concept that information can flow in both directions across the cable ; **Simplex Communication** is unidirectional; **Half-duplex** is capable of duplex, but only 1 device communicates at a time
- **Network Ports** are generally directly attached to the devices that make up a computer network

The Data Link Layer

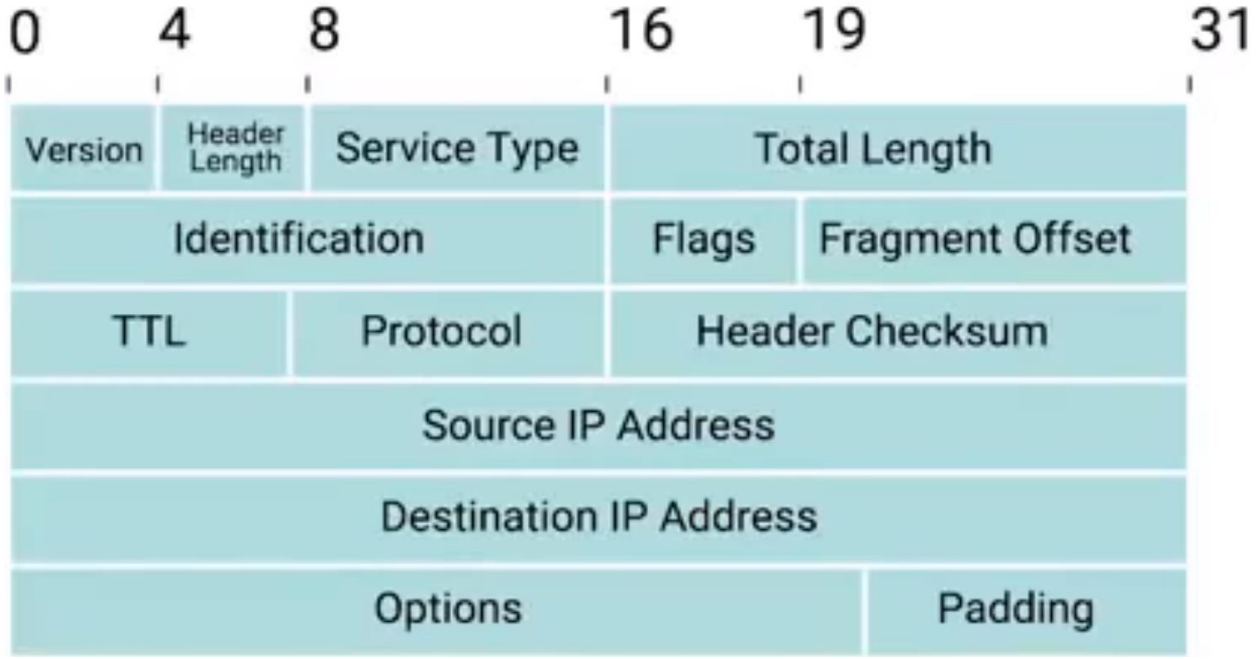
- **CSMA/CD** - used to determine when the communications channels are clear, and when a device is free to transmit data.
- **MAC Address** - globally unique identifier attached to an individual network interface; it's a 48-bit number normally represented by six groupings of two hexadecimal numbers,
    - Hexadecimal - way to represent numbers using 16 digits
        - 0123456789ABCDEF
- **Octet** - in computer networking, any number that can be represented by 8 bits
- Organizationally Unique Identifier (**OUI**) - the first three octets of a MAC address
- Ethernet uses MAC addresses to ensure that the data it sends has both an address for the machine that sent the transmission, as well as the one the transmission was intended for
- **Unicast** transmission is always meant for just one receiving address
    - If the least significant bit in the first octet of a destination address is set to **zero**, it means that the ethernet frame is intended for **only the destination address**
    - If it's set to **one**, it means you're dealing with a **multicast frame**
- **Data Packet** - an all-encompassing term that represents any single set of binary data being sent across a network link
- **Ethernet Frame** - a highly structured collection of information presented in a specific order



- **Preamble** - 8 bytes (or 64 bits) long, and can itself be split into two sections
- **SFD** (start frame delimiter) - signals to a receiving device that the preamble is over and that the actual frame contents will now follow
- **Destination Address** - the hardware address of the intended recipient
- **EtherType Field** - 16 bits long and used to describe the protocol of the contents of the frame
- **VLAN Header** - indicates that the frame itself is what's called a VLAN frame
    - **VLAN** (virtual LAN) - a technique that lets you have multiple logical LANs operating on the same physical equipment
- **Payload** - in networking terms, is the actual data being transported, which is everything that isn't a header
- **Frame Check Sequence** - a 4-byte (or 32-bit) number that represents a checksum value for the entire frame
    - **Checksum value** is calculated by performing what's known as a cyclical redundancy check against the frame
- **CRC** (cyclical redundancy check) - an important concept for data integrity, and is used all over computing, not just network transmissions

The Network Layer

- IP Addresses belong to networks, not the devices connected to the networks
- In most cases, **static** IP addresses are reserved for servers and network devices, while **dynamic** IP addresses are reserved for clients
- **IP Datagram** - a highly structured series of fields that are strictly defined



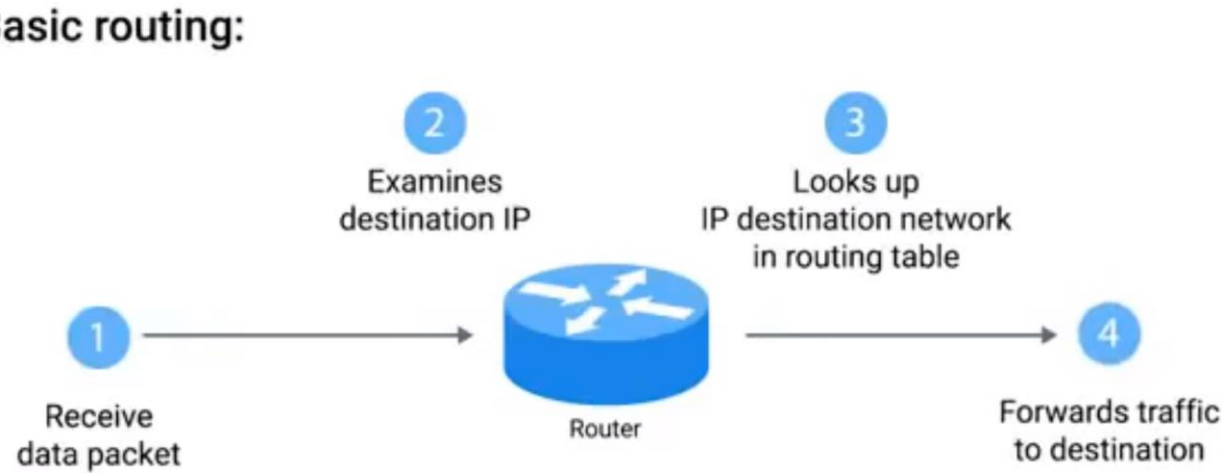
- **Header Length Field** - almost always 20 bytes in length when dealing with IPv4

- **Service Type Field** - these 8 bits can be used to specify details about quality of service, **QoS**, technologies
- **Total Length Field** - indicates the total length of the IP datagram it's attached to
- **Identification field** - 16-bit number that's used to group messages together
- **Flag Field** - 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 up into several smaller datagrams
- **TTL** (time to live) field - an 8-bit field that indicates how many router hops a datagram can traverse before it's thrown away
- **Protocol field** - another 8-bit field that contains data about what transport layer protocol is being used
- **Header checksum field** - a checksum of the contents of the entire IP datagram header
- **IP options field** - an optional field and is used to set special characteristics for datagrams primarily used for testing purposes
- **Padding field** - a series of zeros used to ensure the header is the correct total size
- IP addresses can be split into two sections: the **network ID** and the **host ID**
- **Address Class System** - a way of defining how the global IP address space is split up

IP address classes

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

- **ARP** (Address Resolution Protocol) - a protocol used to discover the hardware address of a node with a certain IP address
- **ARP Table** - list of IP addresses and the MAC addresses associated with them
- **Subnetting** - the process of taking a large network and splitting it up ito many individual and smaller subnetworks, or subnets
- **Subnet Masks** - 32-bit numbers that are normally written out as four octets in decimal
- Two of the most important operators are **OR** and **AND**
- In computer logic, a **1** represents **true** and a **0** represents **false**
- A subnet mask is a way for a computer to use **AND operators** to determine if an IP address exists on the same network
- **Demarcation point** - to describe where on network or system ends and another one begins
- **Router** - a network device that forwards traffic depending on the destination address of that traffic



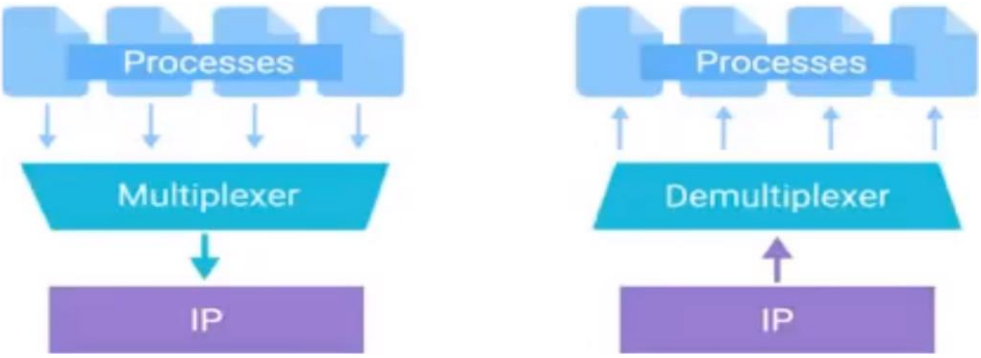
- **Routing Protocols** fall into two main categories: **interior gateway protocols** and **exterior gateway protocols**
    - **Interior gateway protocols** are further split into two categories: **Link state routing protocols** and **distance-vector protocols**
- **Interior gateway protocols** - used 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
- In computer science, a **list** is known as a **vector**
- **RFC 1918**

Intro to Transport & Application Layers

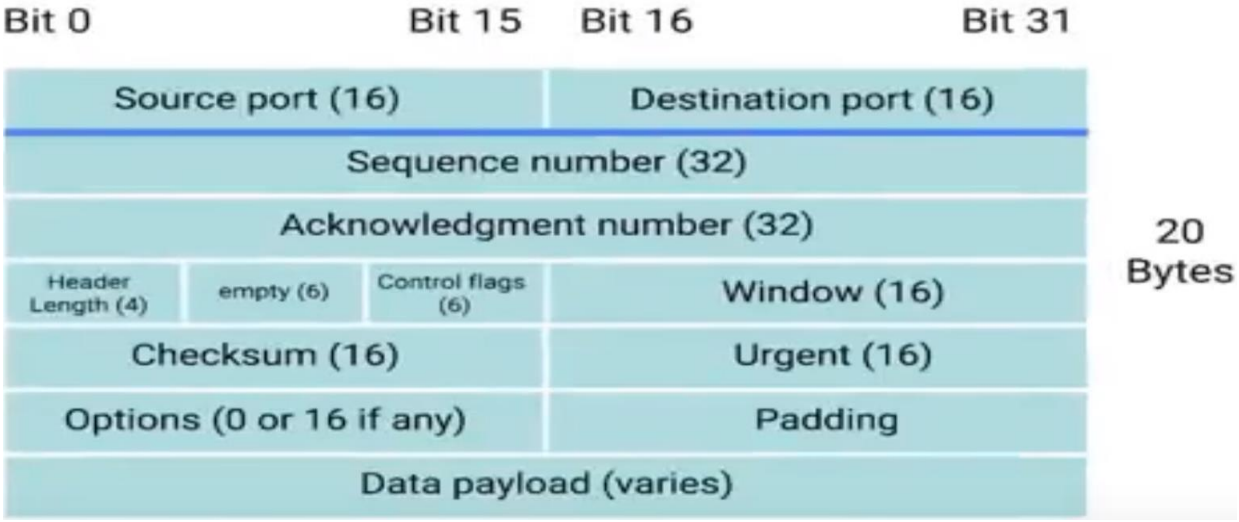
- **Transport layer** - allows traffic to be directed to specific network applications
- **Application layer** - allows these applications to communicate in a way the understand

The Transport Layer

- Multiplexing & Demultiplexing



- **Port** - a 16-bit number that's used to direct traffic to a specific service running on a networked computer
- **TCP Segment** - made up of a TCP header and a data section
- TCP Header:



- **Sequence number** - the number of the current segment
- **Acknowledgement number** - the number of the next expected segment
- **Data offset field** - a 4-bit number that communicates how long the TCP header for this segment is
- **TCP window** - specifies the range of sequence numbers that might be sent before an acknowledgement is required
- **TCP Checksum** - operates just like the checksum fields at the IP and ethernet level
- **Urgent pointer field** - used in conjunction with one of the TCP control flags to point out particular segments that might be more important than others
- **Options field** - it is sometimes used for more complicated flow control protocol
- **TCP 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** (acknowledged) - 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 application on the receiving end as soon as possible
    - **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
    - **SYN** (synchronized) - it's 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
    - 3 way handhake:

    - **Handshake** - a way for two devices to ensure that they're speaking the same protocol and will be able to understand each other
    - When closing the connection - 4 way handshake:

- **Socket** - the instantiation of an end-point in a potential TCP connection
    - **Instantiation** - the actual implementation of something defined elsewhere
    - **LISTEN** - a TCP socket is ready and listening for incoming connections
    - **SYN_SENT** - a synchronization request has been sent, but the connection hasn't been established yet
    - **SYN_RECIEVED** - 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 the application that opened the socket hasn't released its hold on the socket yet
    - **CLOSED** - the connection has been fully terminated and that no further communication is possible
- **Connection-oriented protocol** - establishes a connection, and uses this to ensure that all data has been properly transmitted
- **Firewall** - a device that blocks traffic that meets certain criteria

The Application Layer

- **OSI**
    - **Session layer** - facilitating the communication between actual **applications** and the **transport layer**
    - **Presentation layer** - responsible for making sure that the unencapsulated application layer data is able to be understood by the application in question

Networking Services

- **DNS** (Domain Name System) - a global and highly distributed network service that resolves strings of letters into IP addresses for you
    - **Domain Name** - the term we use for something that can be resolved by DNS
    - 5 primary types of DNS servers:
        i. Caching name servers
        ii. Recursive name servers
        iii. Root name servers
        iv. TLD name servers
        v. Authoritative name servers
    - **Caching** & **recursive name server** - generally provided by ISP, purpose is to store known domain name lookups for a certain amount of time

- **Anycast** - a technique that's used to route traffic to different destinations depending on factors like location, congestion, or link health
- Uses UDP
- An **A record** is used to point a certain domain name at a certain IPv4 IP address
- **CNAME** record is used to redirect traffic from one domain name to another
- **MX record**- mail exchange
- **SRV record** - service record
- **TXT record** - text
- **TLD** - top level domain, last part of the domain name (.com, .net, .edu, etc.)
    i. Handled by ICANN - internet corporation for assigned names and numbers | nonprofit sister org to IANA
- **Domain** - used to demarcate where control moved from a TLD name server to an authoritative name server (second part of domain name)
    i. Subdomain = www
- **Fully qualified domain name (FQDN)** - when you combine subdomain, domain, and TLD
- **DNS Zones** - allow for easier control over multiple levels of a domain
    i. **Zone files** - simple config files that declare all resource records for a particular zone
    ii. **Start of authority (SOA)** - declares the zone and the name of the name server that is authoritative for it
    iii. **NS records** - indicate other name servers that might also be responsible for this zone
    iv. **Reverse lookup zone files** - these let DNS resolvers ask for an IP and get the FQDN associated with it returned
    v. **Pointer record (PTR)** - resolves an IP to a name

- **DHCP** (dynamic host configuration protocol) - an application layer protocol that automates the configuration process of hosts on a network
    - **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
    - **Automatic allocation** - a range of IP addresses is set aside for assignment purposes
    - **Fixed allocation** - requires a manually specified list of MAC address and their corresponding IPs
    - **Network time protocol (NTP)** - used to keep all computer on a network synchronized in time
    - **DHCP discovery** - the process by which a client configured to use DHCP attempts to get network configuration information
- **NAT** (network address translation) - 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
    - **Port preservation** - a technique where the 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
- **VPN** (virtual private networks) - technology that allows for the extension of a private or local network to hosts that might not be on that local network
- **Broadband** - any connectivity technology that isn't dial-up internet

Wireless Networks

- **Frequency band** - a certain section of the radio spectrum that's been agreed upon to be used for certain communications (2.4GHz & 5GHz are most common)

- **802.11** protocols = physical and data link layers
- **Wireless access point** - a device that bridges the wireless and wired portions of a network
- **Channels** - individual, smaller sections of the overall frequency band used by a wireless network

Troubleshooting & Future of Networking

- **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** message type
- **Traceroute** - a utility that lets you discover the path between two nodes, and gives you information about each hop along the way
- **Nslookup** - utilized for DNS info
- **Registrar** - an organization responsible for assigning individual domain names to other organizations or individuals
- **Loopback address** - way to send network traffic to yourself (127.0.0.1)
- **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 it
    - **Virtualization** - a single physical machine, called a host, could run many individual virtual instances, called guests
    - **Hypervisor** - software that runs and manages virtual machines, while also offering these guests a virtual os platform that's indistinguishable from actual hardware
    - **Public cloud** - a large cluster of machines run by another company
    - **Private cloud** - used by a single large corporation and generally physically hosted on its own premises
    - **Hybrid cloud** - a term used to describe situations where companies might run things like their most sensitive proprietary technologies on a private cloud, while entrusting their less-sensitive servers to a public cloud
- **IPv6** - 128 bits , provides an undecillion number of addresses
    - Two rules when it comes to shortening IPv6 addresses.
        - The **first** is that you can remove any leading zeros from a group
        - The **second** is that any number of consecutive groups composed of just zeroes can be replaced with two colons