**Complete example**

* [**https://www.coursera.org/learn/computer-networking/lecture/BqSRb/all-the-layers-working-in-unison**](https://www.coursera.org/learn/computer-networking/lecture/BqSRb/all-the-layers-working-in-unison)

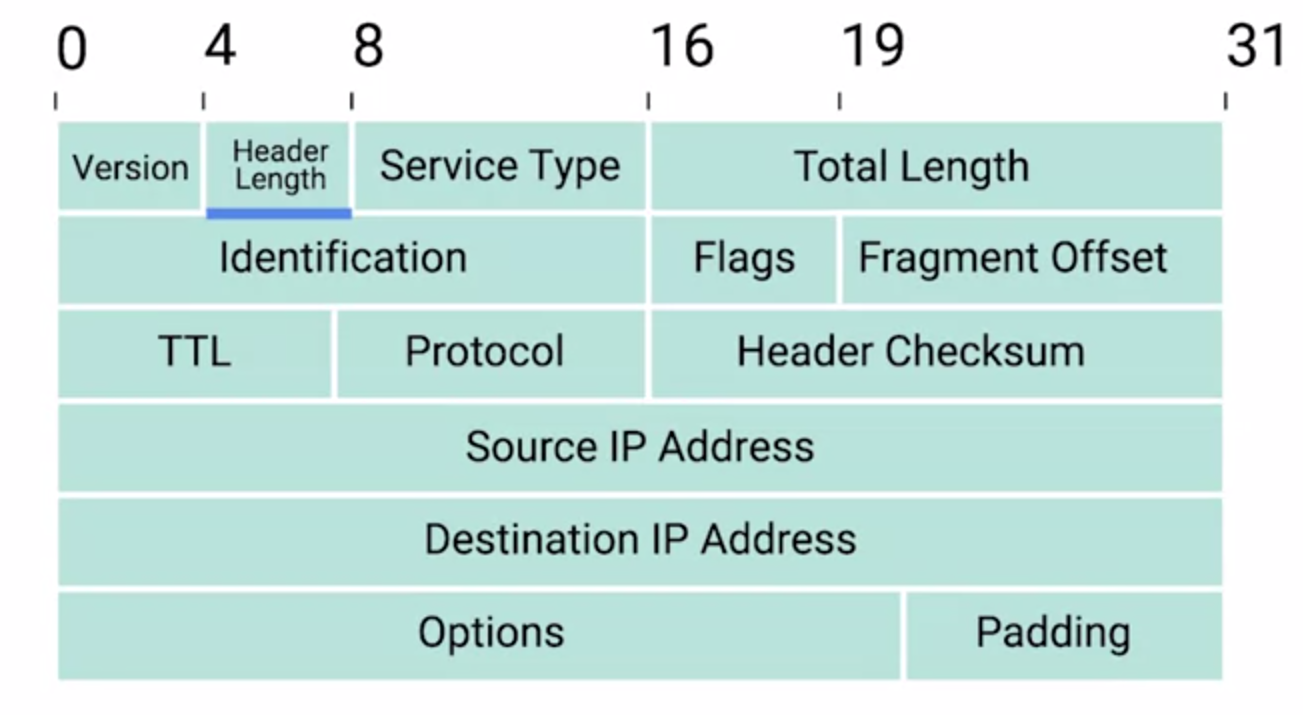
**Application layer**:application specific, messages

* Allows these applications to communicate in a way they understand
* Example protocol: HTTP, FTP, SMTP(email)
* HTTP: Protocol handling traffic between applications like browser and website server.
  + HTTPs stands for secure (Through SSL)

**Transport layer**: port(Application), TCP protocol, UDP protocol, Segment, sockets

* **Allows traffic to be directed to specific network applications**
* **socket** is one endpoint of a two-way communication link between two programs running on the network， A socket is bound to a port number
* Port: A 16-bit number that's used to direct traffic to specific services running on a networked computer
  + Application listen to port for coming request
  + Eg: 10.1.1.100:80, a **socket address**
  + Some example
    - HTTP: port 80
    - FTP: port 21
* multiplexing and demultiplexing traffic
  + Multiplexing means that nodes on the network have the ability to direct traffic toward many different receiving services(ports)
* TCP Segment: same, header + data pay load
  + Header is:
    - Source port and destination port
    - Sequence number
    - Acknowledgement number
    - Header length, control flag, window
    - Checksum
* Establish connection: 3-way handshake:
  + A way for two devices to ensure that they're speaking the same protocol and will be able to understand each other, after handshake, the TCP connection is established
  + SYN, SYN/ACK, ACK
* Close connection: 4-way handshake:
  + FIN, ACK, FIN, ACK
* Socket states: LISTEN; SYN\_SENT; SYN\_RECEIVED; ESTABLISHED; FIN\_WAIT; CLOSE\_WAIT; CLOSED.
* **Resend mechanism:** only TCP protocol is capable to decide when to resend lossed/dropped segment
* **UDP(user datagram protocol) :**a connectionless protocol
  + Anotherprotocol
  + No need to establish connection (eg when correctionness is not importation, like streaming media)
* Firewall: A device that blocks traffic that meets certain criteria
  + Block: port/ IP
  + Can be a variety of devices(host, router, standalone), hardware, software and os, and in different level of internet

**Network layer**: IP, protocol, IP address, router, WAN, Datagram

* IP address:
  1. 4 8bits(0-255)
  2. Assigned in hierarchical order(ie. ISP, organization…)
  3. Auto(dyna) assign: DHCP(dynamic host config protocol) vs Static assign
  4. Two sections: **network ID**(first 8 bits) and **host ID**(remaining bits)
  5. 3 classes: first 8 bits:0-126(a),128-191(b)192-224(c)
* Private IP addresses used by the local network. Public IP address is what internet actually see
* Datagram dissection:
  1. 
  2. Max size:65535, any packet larger than that will be splitted(with an id)
  3. TTL(Time to live ): decrement in each step of the routers, when TTL reach 0, the datagram will be discarded
* **Gateway**:may be a router, firewall, server, or other device that enables traffic to flow in and out of the network(IP address).
* *ARP*(Address resolution protocol): discover MAC given an IP address→ route to the specific device within LAN
  1. ARP table: list of MAC associated to an IP address
  2. ARP table entries generally expire after a short amount of time to ensure changes in the network are accounted for.
* **Subnetting**: divide a large network into smaller subnets, each of the subnets have their own gateways
  1. Some of the **host id** part become **subnet id**
  2. ‘At the internet level, core routers only care about the network ID and use this to send the datagram along to the appropriate gateway router to that network. That gateway router then has some additional information**(subnet id**) that it can use to send that datagram along to the destination machine or the next router in the path, Finally, the host ID is used by that last router to deliver the datagram to the intended recipient machine.’
  3. **Subnet id** is calculated from **subnet mask**
  4. Common **subnet mask 255.255.255.0**
  5. CIDR: a different notation system, first k binary number is network, while the remaining is host
* **Routing** 
  1. Often handling by ISP, complex algorithms
  2. perfect example [Basic Routing Concepts - The Network Layer](https://www.coursera.org/learn/computer-networking/lecture/eCwJA/basic-routing-concepts)
  3. routing table
     + Component: Destination Network, Next Hop, Total Hops, Interface
* Routing protocols(algorithms):
  1. Interior gateway protocols: within organization or ISP(ie Autonomous system)
     + link state routing protocols
     + distance-vector protocols
  2. Exterior gateway protocols

**Data Link layer**:Ethernet, wifi, mac address, LAN, data frame

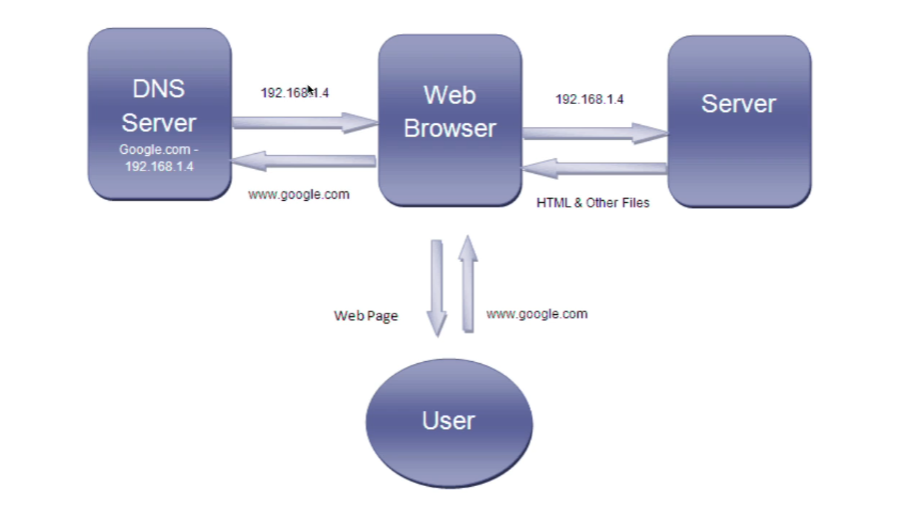
* Abstract all different physical medium
* Ethernet use CSMA/CD
* CSMA/CD:
  1. Used to determine when the channels are clear to transmit data
  2. solve collision domain problem
* MAC address
  1. Identifier to each device(having network interface)
  2. 6 groups of hexadecimals
  3. 24bits(OUI organizational unique id) + 24bits(VA vendor assigned)
* Unicast, multicase, broadcast
* Data Frame: data packet at data link
  1. preamble + MAC dest+ MAC source + VLAN tag + Ether-tpye + data + FCS
  2. VLAN: create multiple virtual LANs within an physical LAN(used to separate different LANs)
  3. Data: contain all the data packet from upper layer, 0-1500bytes
  4. FCS(frame check sequence):
     + CRC(cyclical redundancy check) algorithm
     + Sender CRC, get checksum, receiver CRC, get checksum, match the two

**Physical layer**: cable, bit

* An encoder, noisy digital signal chain, decoder model
* Plug: RJ45, link light(orange) when connected, activity light(green) when transmitting
* Electrical Magnetic field

**Others**:

* **Data packet**: abstraction any data that is sent through a network, not specific to any layer
* **Encapsulation**: each data packet from upper layer is encapsulated in lower data packet
* troubleshooting network
  + ipconfig
  + **Ping**: check connectivity
    - 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.
    - $ ping 8.8.8.8
    - $ ping 1m0uto.cc
  + **Traceroute**: trace routers
    - Trace the intermediate router address from host to the destination
    - $ traceroute 1m0uto.cc, $mtr
    - >tracert 1m0uto.cc, >pathping (in Windows)
  + Test port connectivity
    - $ nc -z -v google.com 80 <destination, port>, try to establish connection to destination through port
    - >Test-NetConnection
  + DNS lookup
    - $ nslookup google.com
* **DNS**(Domain Name System): A global and highly distributed network service(**domain name server**) that resolves strings of letters(**domain name**) into IP addresses for you -- a process called **name resolution**

****

* + Example of domain name: <https://www.namesilo.com/>
  + Domain name servers:
    - caching name servers, recursive name servers (local lookup)
    - root name servers, TLD(top level domain) name servers, authoritative name servers (full lookup)
  + DNS record types:
    - A record
    - Quad A record(IPv6)
    - CNAME(Canonical Name record): A CNAME record is used to redirect traffic from one domain name to another.
      * Example: Domain name without www; github page publish
    - MX record(email exchange)
    - SRV record
    - TXT record
  + Domain name:
    - .com(or similar): *top level domain*
    - google: *Domain*, used to demarcate where control moves from a TLD name server to an authoritative name server
    - www: subdomain
* DHCP (Dynamic Host Configuration Protocol):
  + Application layer service(need lower layers support)
  + Automatic configure network setting for host in a network
  + For end clients who don’t need statics and common known IPs
  + 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
  + The DHCP lease has an **expiration time,** when host disconnect, the IP will also be released
  + address allocation Dynamic, automatic, fix
  + Process
    - HOST broadcast , src port 68, dest port 67
    - DHCP server received, and allocate IP, then broadcast
    - HOST confirm(broadcast)
    - DHCP ack(broadcast)
* NAT(Network address translation)
  + Map an IP address to another IP address
  + 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 for return to the source host
  + Purpose: hide IPs in local network (**IP masquerading**) for security purpose; preserve IPv4 addresses
  + Port preservation; port forwarding
* VPN(Virtual Private Network): a concept
  + Scenario: (work from home) employee, not physically connect to the private company network/ sub companies in different location share the same company network
  + Allow host in other network to act like they were in the local network
  + VPN is a concept rather than a specific protocol, can be many implementations
  + Use encrypted tunnels to connect remote devices
  + **Point2point VPN: establish VPN tunnel between two(or more) sites(a group of user)**
* Proxy service: a concept
  + A server that acts on behalf of a client in order to access another service
  + Client Host ↔ **proxy server** ↔ target server
  + Anonymity, security, bypass firewall, forbid unwanted connection
  + Reverse proxy:
    - Make many server appear to be a single server(proxy server) to client
    - (For big company, single server is unable to handle the traffic)
* WAN(wide area network) technology: Acts like a single network(LAN), but physically spans across multiple physical locations
* **Cloud**
  + 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
  + X as a Service
    - IaaS Infrastructure as a Service: You shouldn’t have to worry about building your own network or your own servers
    - PaaS Platform: A subset of cloud computing where a platform is provided for customers to run their services
    - SaaS: A way of licensing the use of software to others while keeping that software centrally hosted and managed
* Wireless:
  + Cellular network
  + Wifi
  + Bluetooth
  + IoT Internet of Things

Device:

HUB: LAN, broadcast, cause collision domain(obsolete)

Switch: use MAC, no collision

Router: forward data between different networks, maintaining a routing table

* WHATITDO: Receive packet, examine IP, lookup IP routing table, forward to destination
* Routers have at least 2 network interface(since it connect different networks) and at least 2 IP addresses
* Home router: forward to the ISP router
* ISP router: different LAN routing schedule through BGP(border gateway protocol)