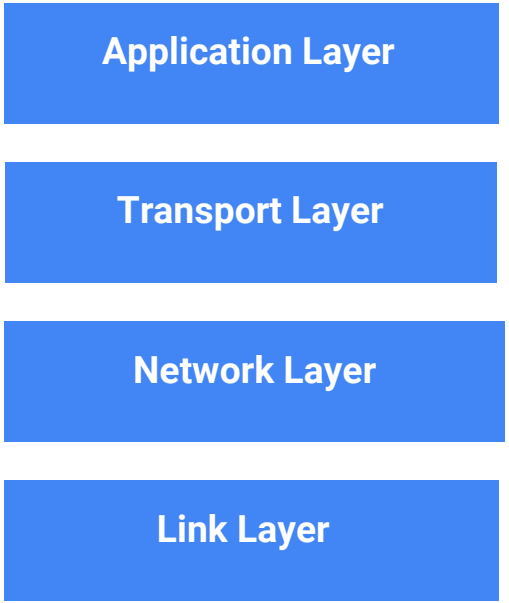
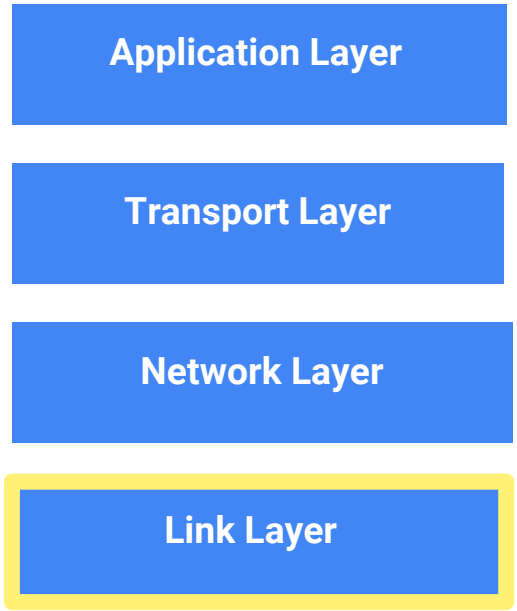
Intro to Computer Networks

4 Layer Internet Model

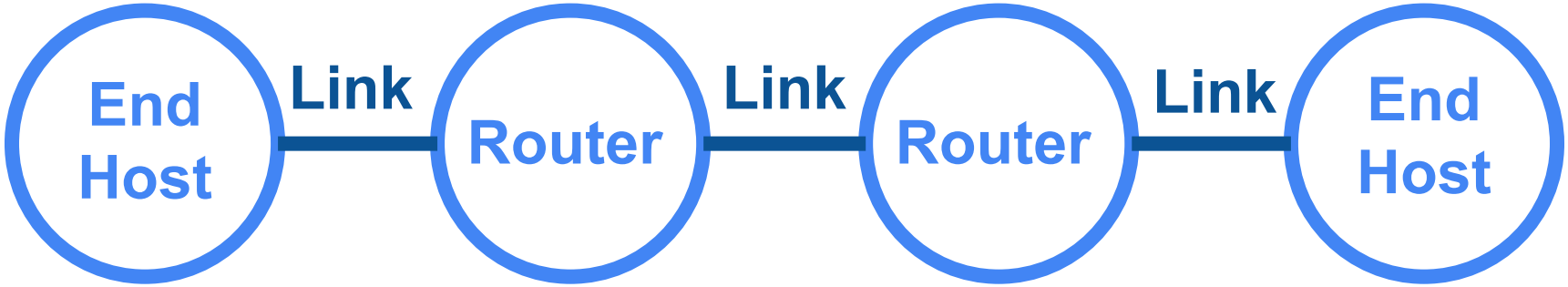


- Applications reuse the same building blocks for transmitting data
- The internet is made up of end hosts, links and routers
- The 4 Layer Internet Model is used to describe the operations that make up the internet

4 Layer Internet Model - Link Layer

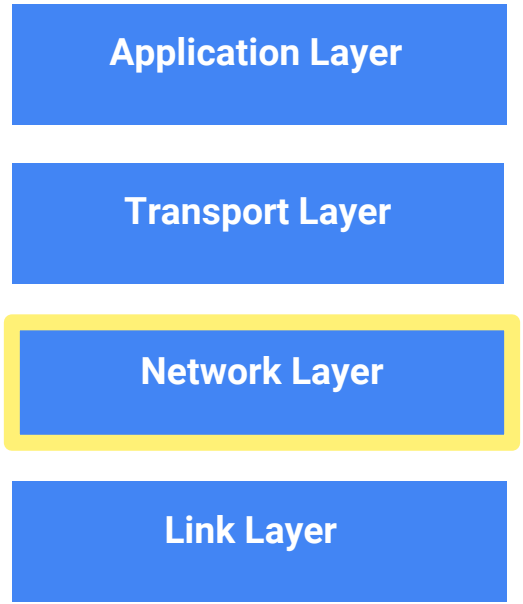


4 Layer Internet Model - Link Layer

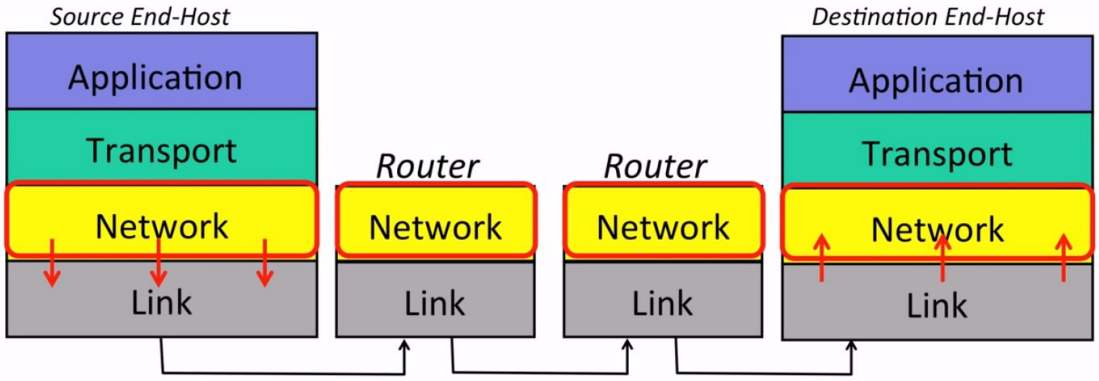


- Packets consist of the data to be delivered and a header with information about the data.
- The link layer is responsible for carrying data packets across one link at a time.
- Examples of link layer protocols are Ethernet and Wifi (802.11).

4 Layer Internet Model - Network Layer



4 Layer Internet Model - Network Layer

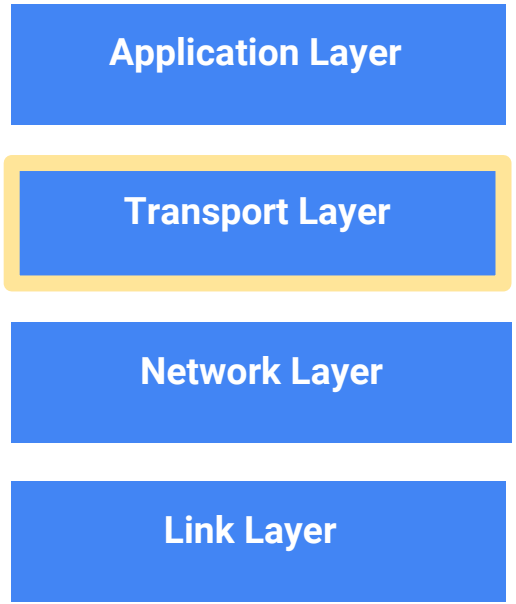


- The Network Layer is responsible for delivering packets end to end from the source to the destination.
- Network Layer packets are called datagrams.

- Examines the datagram and sends it one link at a time to its destination, without having to worry about how the link works.
- Restricted to using the Internet Protocol (IP).

Image source: Levis, Nick and Nick McKeown. Introduction to Computer Networking. Stanford University, March 2015, https://lagunita.stanford.edu/courses/Engineering/Networking-SP/SelfPaced.

4 Layer Internet Model - Transport Layer



- The Transport Layer ensures that the data sent by one application is correctly delivered to another.
- TCP (Transmission Control Protocol) guarantees correct, in order delivery of data and provides reliability.
- UDP is simpler and offers no delivery guarantees.

4 Layer Internet Model - Application Layer

Application Layer

Transport Layer

Network Layer

Link Layer

- The Application Layer sends data directly to its peer application at the destination
- Does not worry about how data is delivered

4 Layer Internet Model

- Each layer communicates with its adjoining layers, without regard to how the other layers communicate information.
- Headers are concatenated to the beginning of the packet before the data is then delivered across the internet

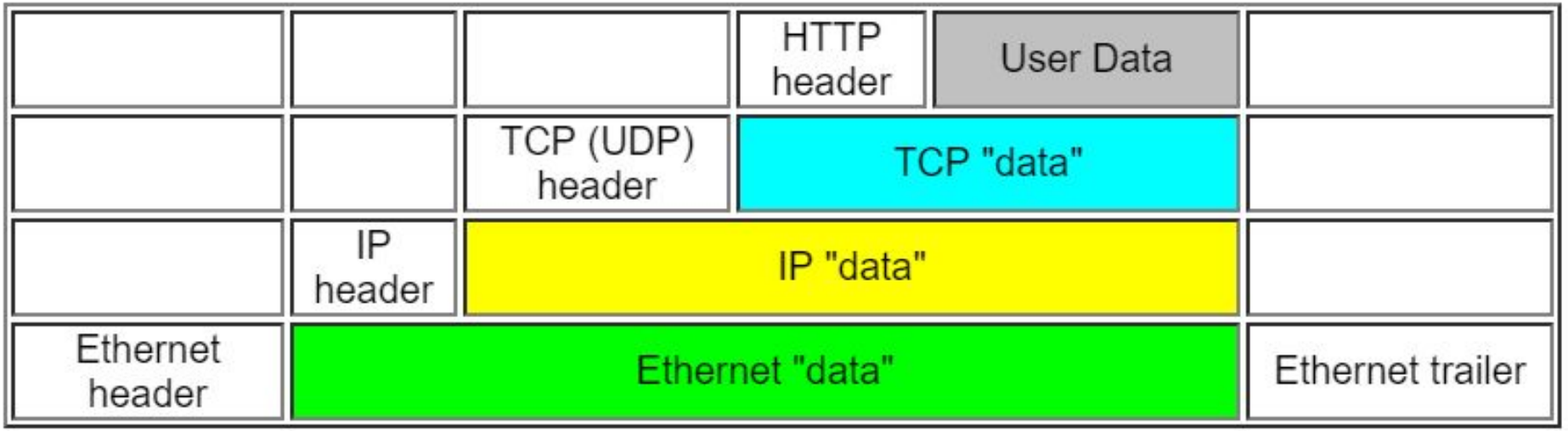
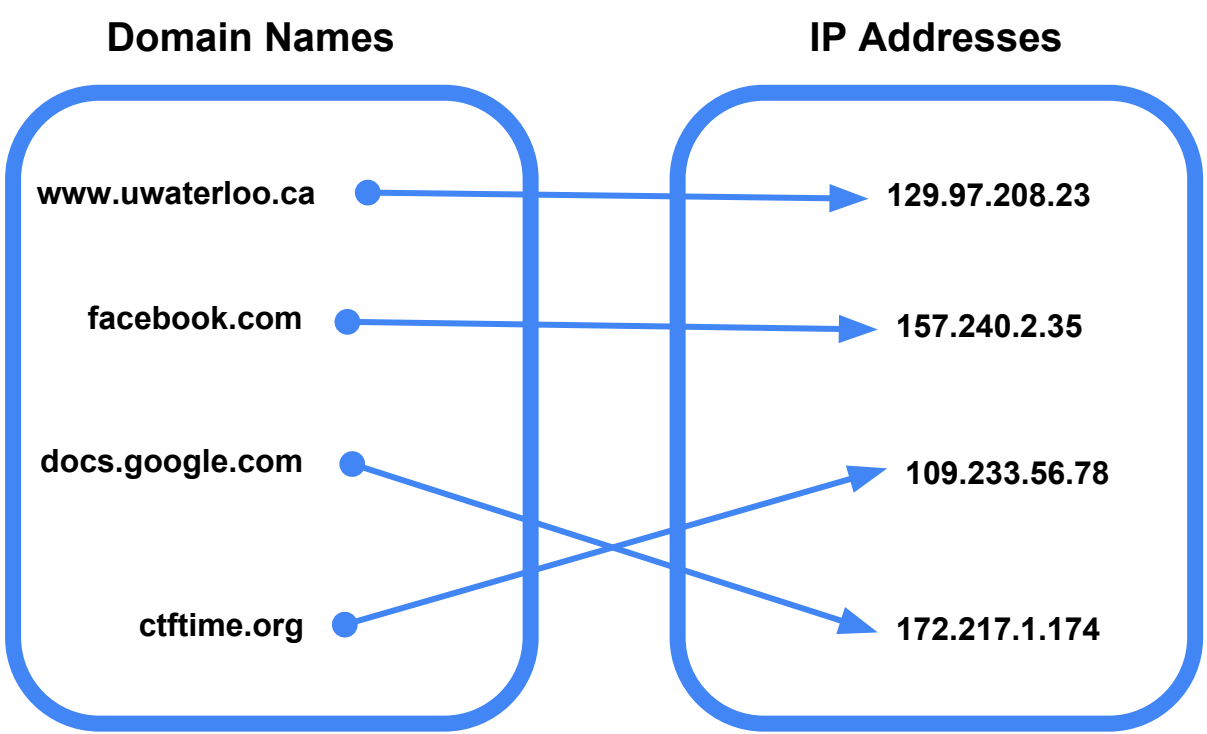


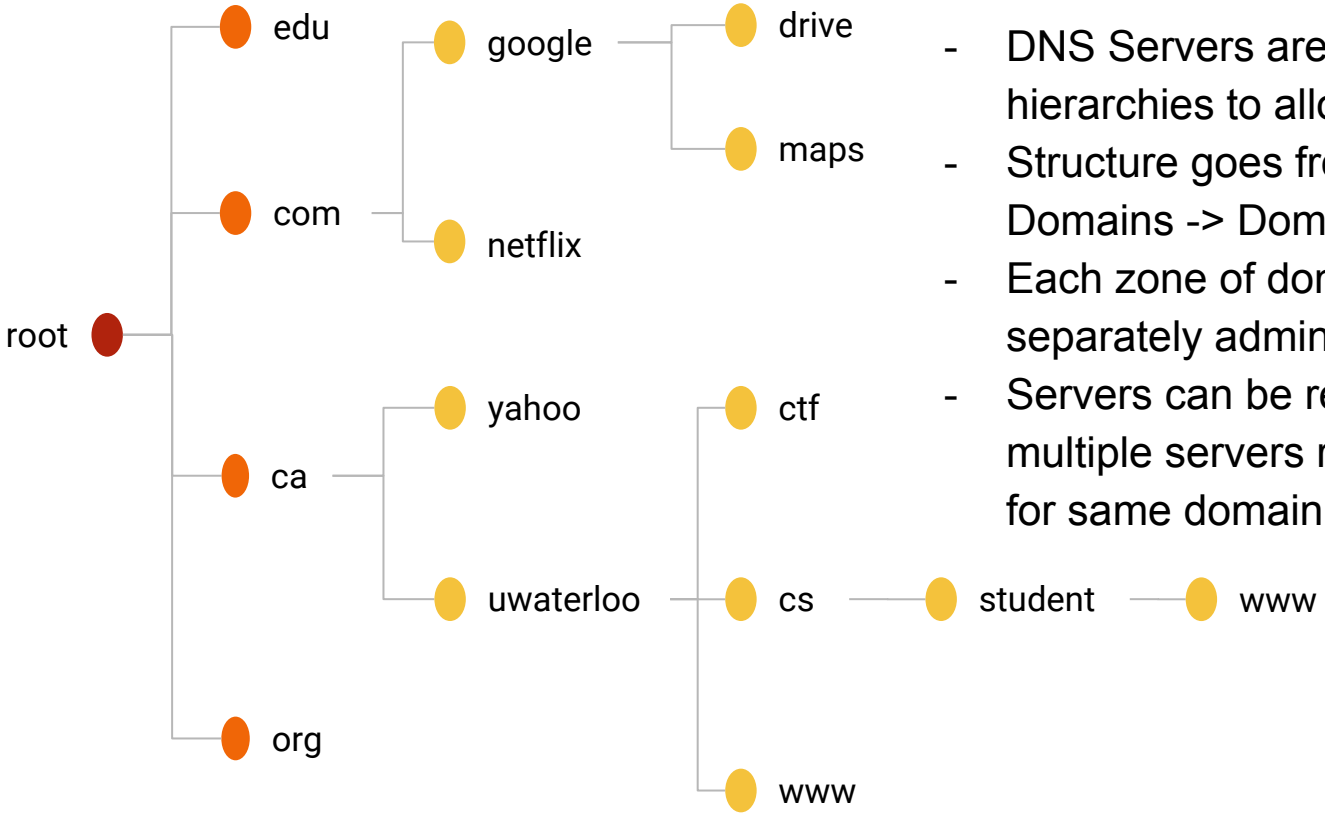
Image source: Taylor, Nolan. The Data Link Layer..The Indiana University Kelley School of Business, May 2009, http://home.kelley.iupui.edu/notaylor/S305/labs/datalink.htm.

Domain Name System (DNS)



- DNS is a service that maps domain names to IP addresses
- The system must be able to map names to addresses, handle a huge number of records, have distributed control, and be able to handle individual node failures
- Used when browsing to different domains on the world wide web

Domain Name System (DNS)

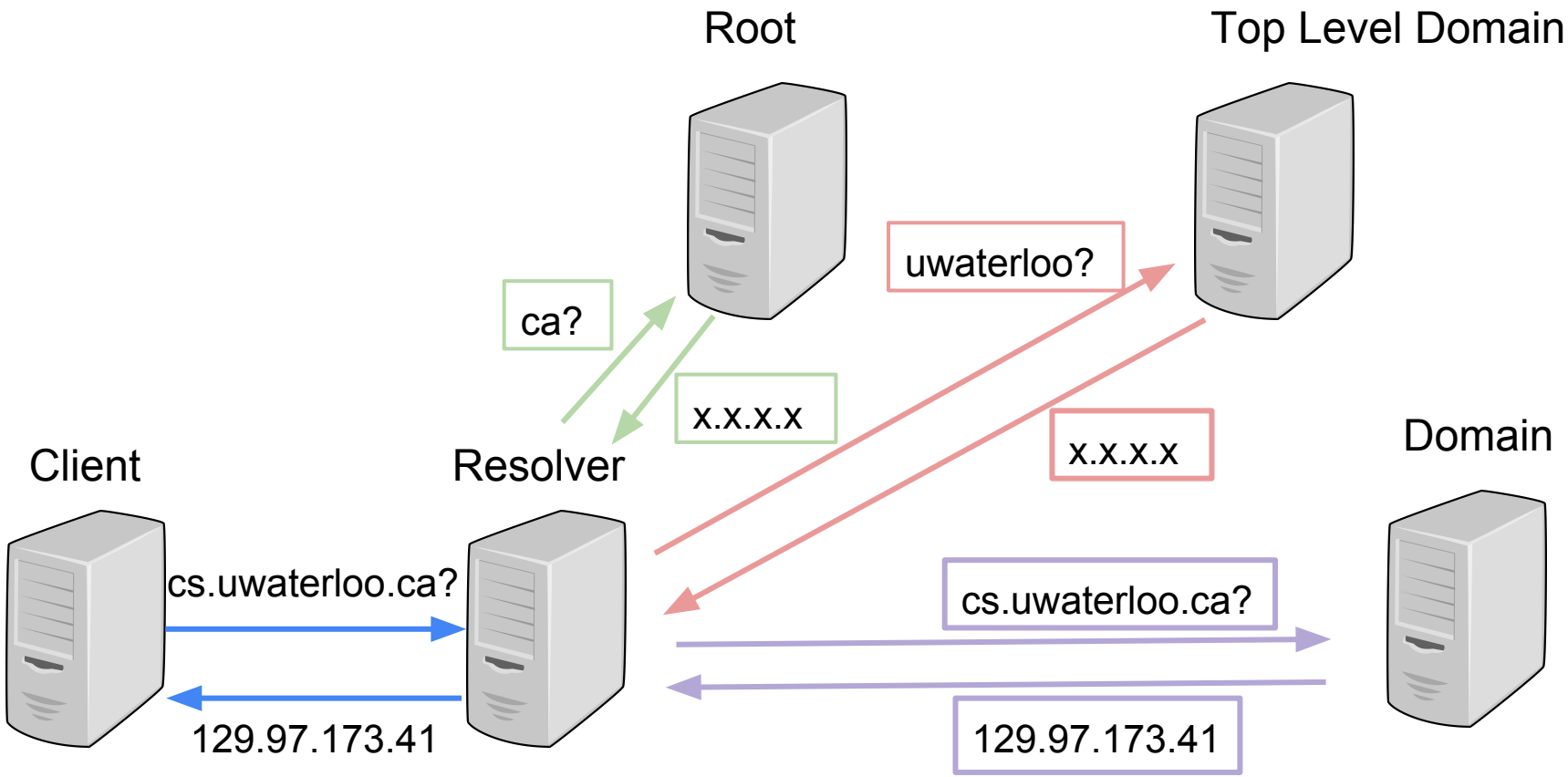


- DNS Servers are structured into hierarchies to allow distributed control
- Structure goes from root -> Top Level Domains -> Domains
- Each zone of domain names can be separately administered.
- Servers can be replicated (can have multiple servers responding to queries for same domain)

Domain Name System (DNS)

- Clients perform recursive queries to DNS resolvers which returns the desired IP address
- Resolvers perform non-recursive queries to DNS servers which return results one step at a time
- Resolvers cache results to increase efficiency of future queries
- See the following slide for a visual representation of a DNS Query

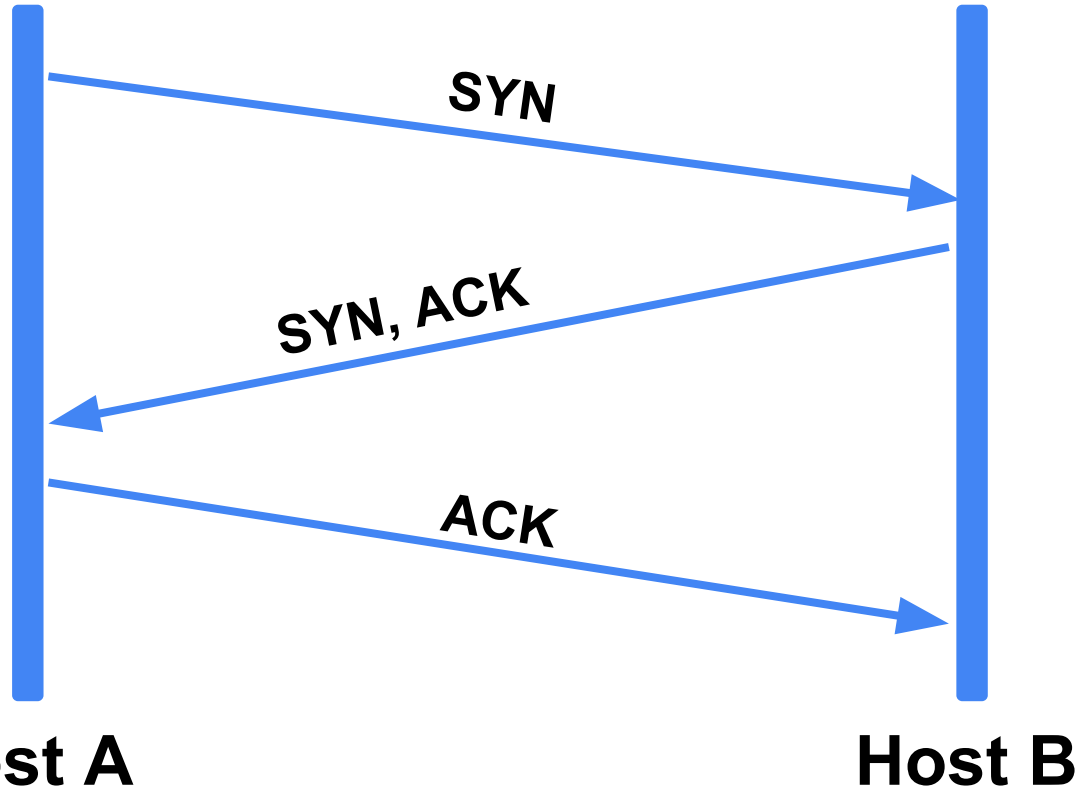
Domain Name System (DNS)



Transport Layer - TCP

- Most commonly used transport protocol: TCP (Transmission Control Protocol)
- Provides a reliable, end-to-end, bidirectional byte stream service
- TCP Properties:
  - Acknowledgements to indicate that data has been delivered
  - Checksums to detect corrupt data
  - Sequence numbers to detect missing data
  - Flow-control to prevent overrunning the receiver
  - Data is delivered to the application in the sequence that is was transmitted.

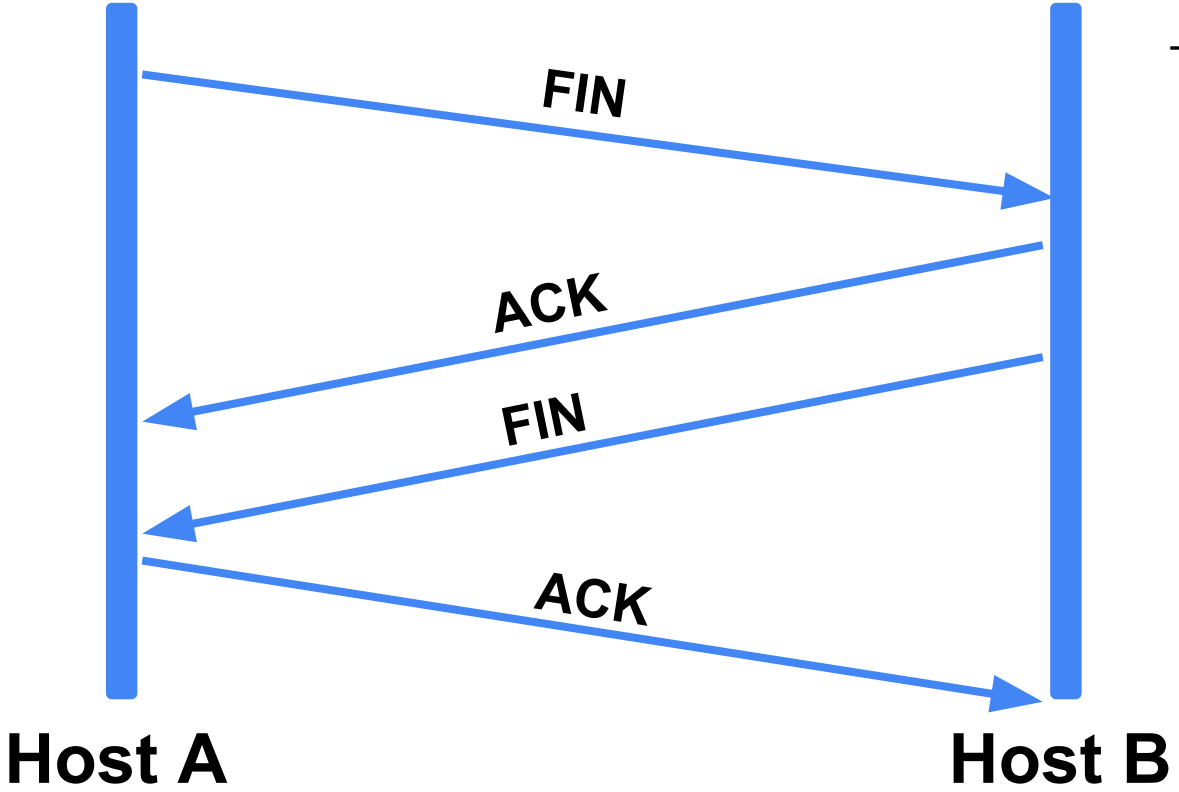
Transport Layer - TCP



TCP Connection Setup:

1. A sends SYN (synchronize) message to B
2. B acknowledges SYN message from A and sends back SYN message
3. A acknowledges SYN message from B

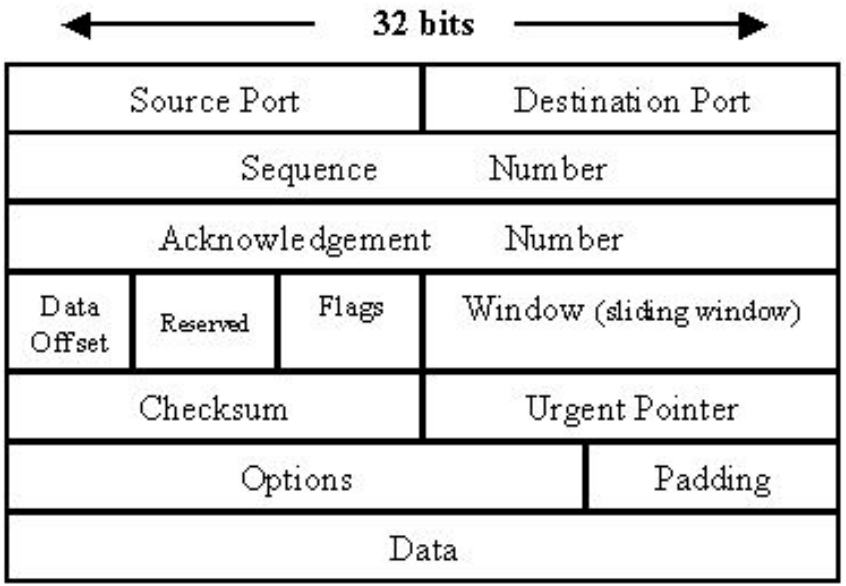
Transport Layer - TCP



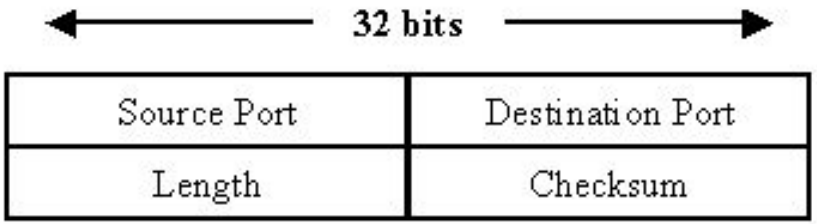
TCP Connection Teardown:

1. A sends FIN message to B, indicating that A has no more data to send
2. B acknowledges FIN message from A (now has the decision to keep sending data or terminate connection by sending FIN message)
3. A acknowledges FIN message from B to terminate connection

Transport Layer - TCP vs UDP



TCP Header



UDP Header

UDP (User Datagram Protocol)

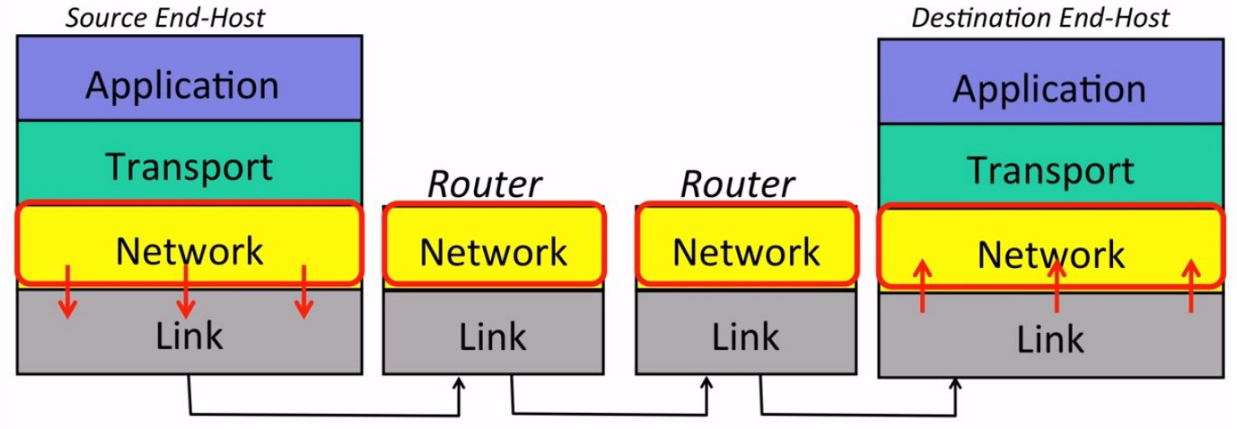
- Much simpler than TCP
- Provides no connection
- Provides no reliability
- Lightweight and fast
- Used with application that don't need reliability (ie DNS, DHCP)

Transport Layer - ICMP

ICMP (Internet Control Message Protocol)

- Communicates network layer information between hosts and routers
- Reports error conditions and helps us diagnose network problems
- Technically a transport layer protocol since it runs above the network layer
- Provides no reliability (a simple service)
- Relied on by command line tools like *ping* and *traceroute*

Network Layer

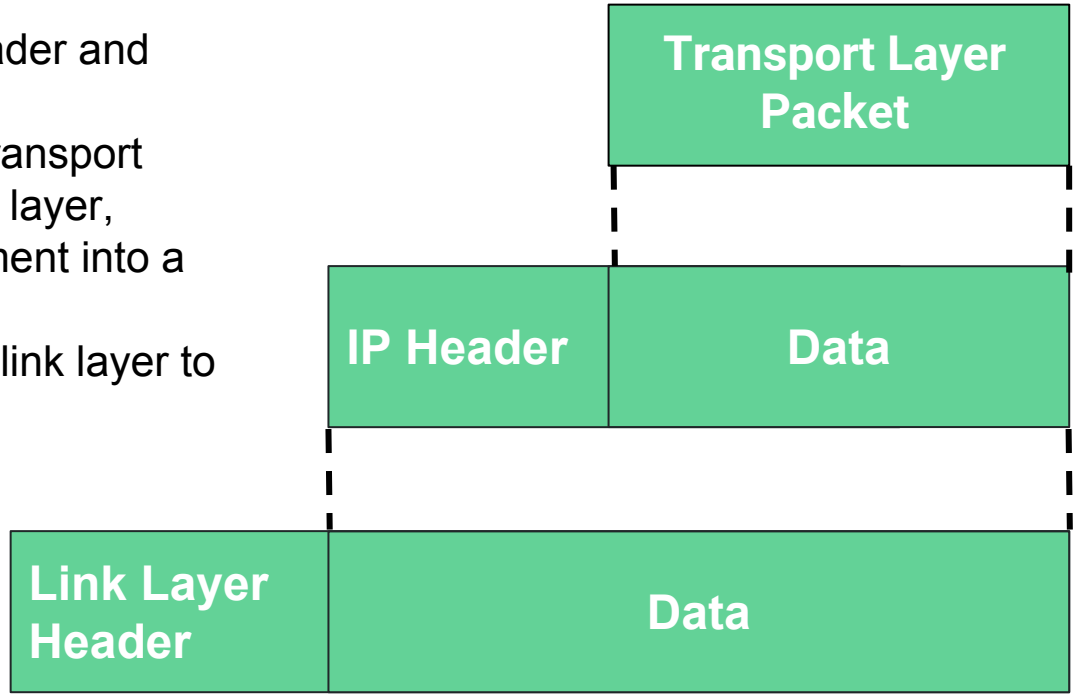


- The Network Layer is responsible for delivering data end-to-end from source to destination
- It is restricted to using the Internet Protocol (IP)

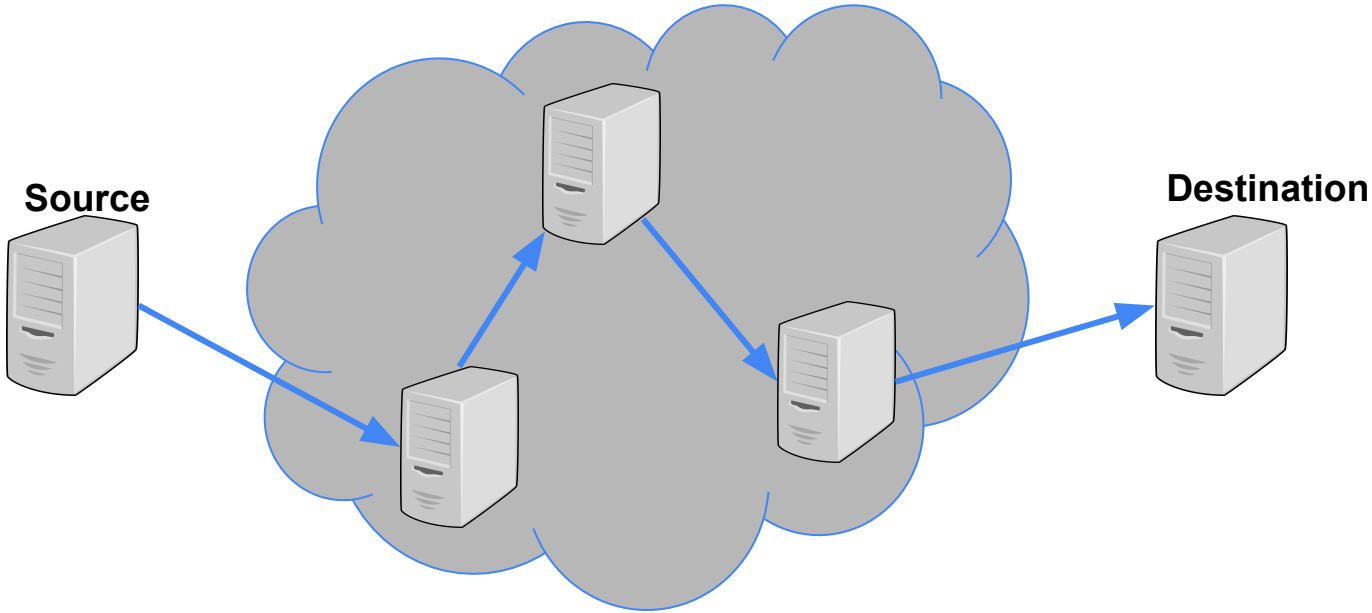
Image source: Levis, Nick and Nick McKeown. Introduction to Computer Networking. Stanford University, March 2015, https://lagunita.stanford.edu/courses/Engineering/Networking-SP/SelfPaced.

Layers - Recap

- IP datagrams consist of a header and data
- The transport layer hands a transport segment down to the network layer, which puts the transport segment into a new IP datagram
- IP sends the datagram to the link layer to be sent off to the first router

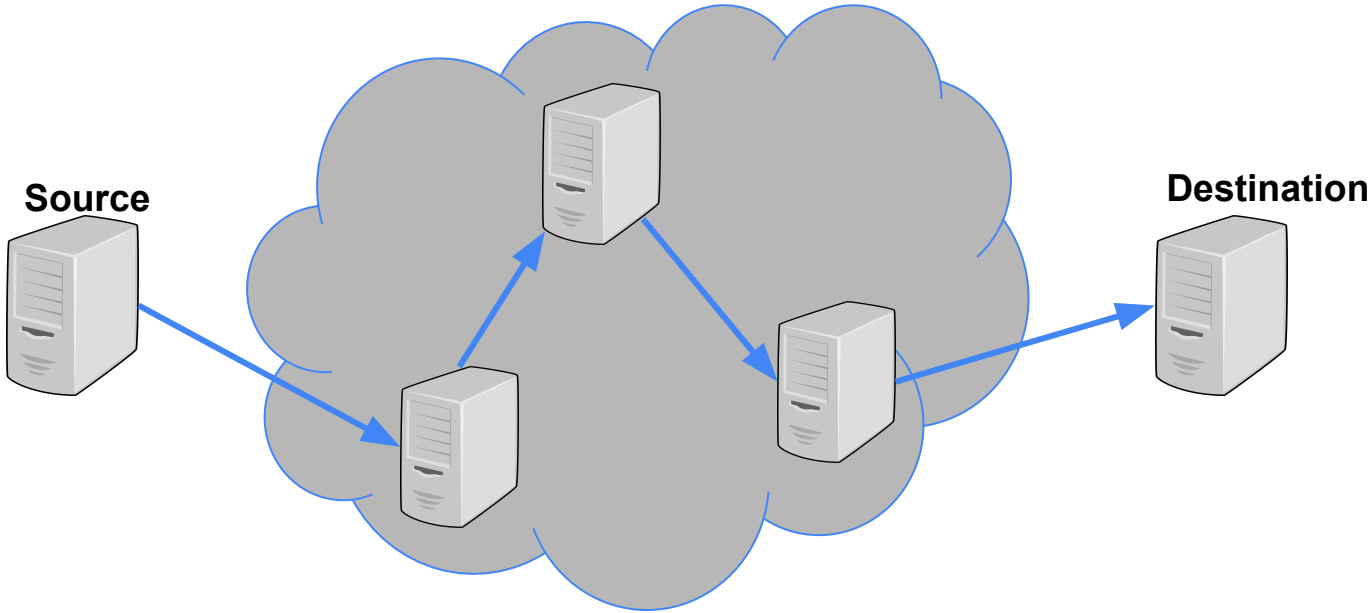


Internet Protocol



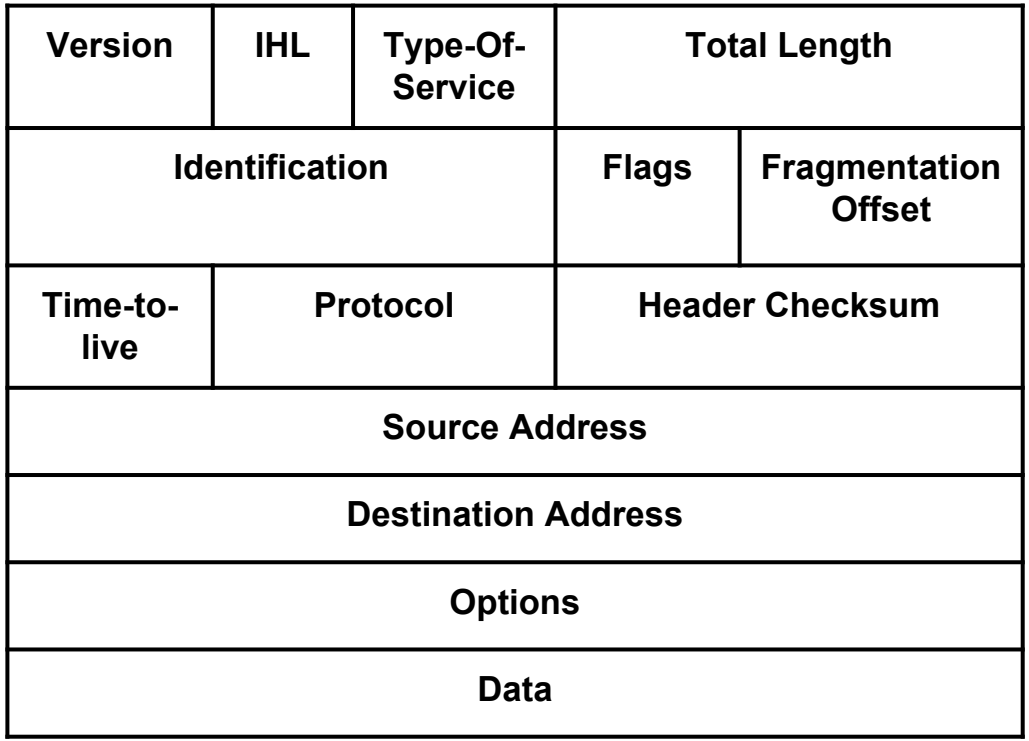
- The destination address in the IP header helps the router decide where to send the datagram next
- The source address in the IP header lets the receiver know where to send a response
- Datagrams are routed hop by hop from source to destination

Internet Protocol



- IP is unreliable and simple
- Simplicity keeps the network minimal, fast, and easy to maintain
- Reliably/unreliable services can be built on top of IP
- The simple design allows IP to work over any link layer

Internet Protocol



Header Fields

TTL (Time To Live): prevents packets from looping forever

ID, Flags, Fragmentation Offset: IP fragments packets if they are too long for the link layer; these fields help the end host put them back together

Checksum: reduces chances of corrupt data and delivery to the wrong destination

Version: IPv4 or IPv6

Options: enable more functionality

IHL: Internet Header Length

Type-of-Service: how important the packet is

Protocol: what is inside the data field (ex: 6 for a TCP segment)

IPv4 vs IPv6

172.217.1.3

IPv4:

- 32 bit long addresses, 4 groups of 8 bits
- Not enough to keep up with the growth of the internet

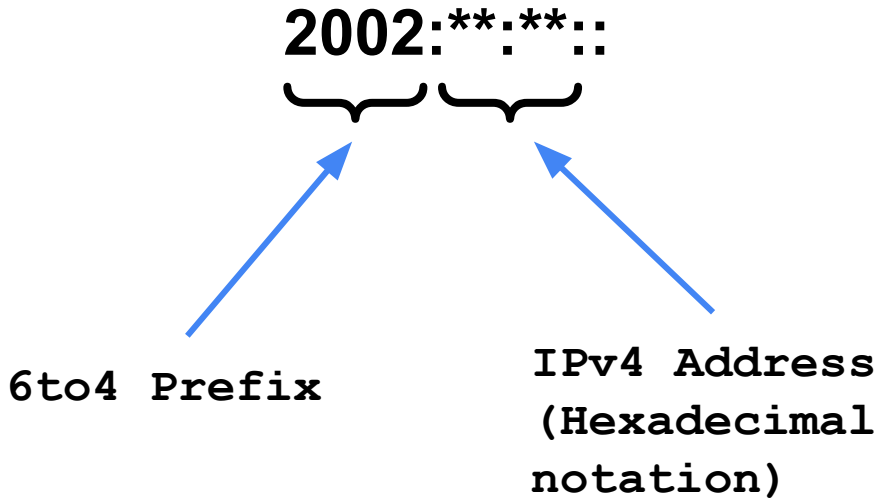
2607:f8b0:400b:80f::2003

IPv6:

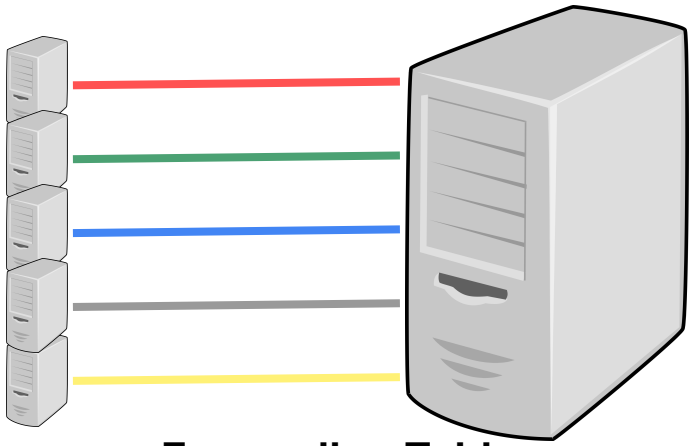
- 128 bit long addresses, 8 groups of 18 bits
- We are in the process of transitioning from IPv4 to IPv6

6to4 IP Addresses

We can translate between IPv4 and IPv6 addresses using 6to4 addresses.



IP Routing



Forwarding Table

x.x.x.x | 1
171.33.x.x | 2
23.x.x.x | 3
23.33.5.x | 4
171.32.x.x | 5

- Internet routers have many different links, so they use forwarding tables to decide where to send the data they are given
- Forwarding tables consist of a set of partial IP addresses
- Routers make decisions based off of the longest prefix match (LPM) algorithm
- The algorithm chooses the most specific address in the forwarding table that matches the IP header's destination address
- Example: 23.33.5.5 would go to link 4
  23.128.3.0 would go to link 3
  179.5.4.2 would go to link 1

Subnet Masks

```
216.3.128.12     → 11011000.00000011.10000000.00001100
255.255.255.0    → 11111111.11111111.11111111.00000000
                   --------------------------------------
216.3.128.0      ← 11011000.00000011.10000000.00000000
```

- A subnet is an organization of connected network devices
- Subnet masks separate the IP address into 2 components: the network and the host addresses
- We can calculate the network address by performing bitwise AND operations
- In the example above, 216.3.128.12 is the IP address, 255.255.255.0 is the subnet mask, and 216.3.128.0 is the network address.

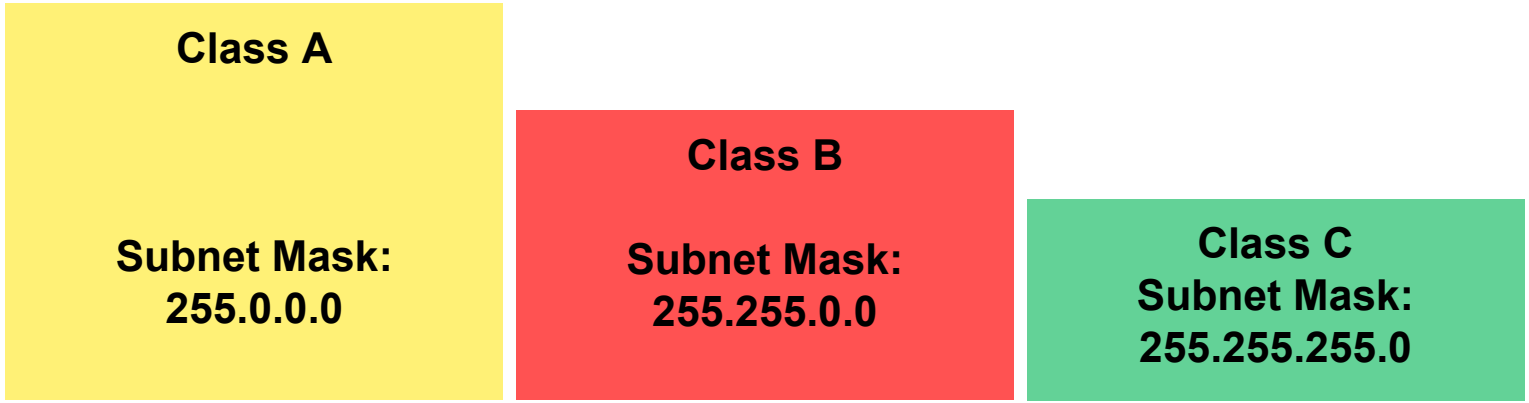
Why Subnet?

```
Web Host Network Address: 216.3.128.0

 216.3.128.(0000 0000)  (1st half assigned to the web host)
 216.3.128.(1000 0000)  (2nd half assigned to the customers)
```

- We can use subnetting to divide networks into multiple parts
- Every time a network is divide into 2 subnets, we lose the ability to use 2 addresses since one must correspond to the network IP and one must correspond to the broadcast IP.

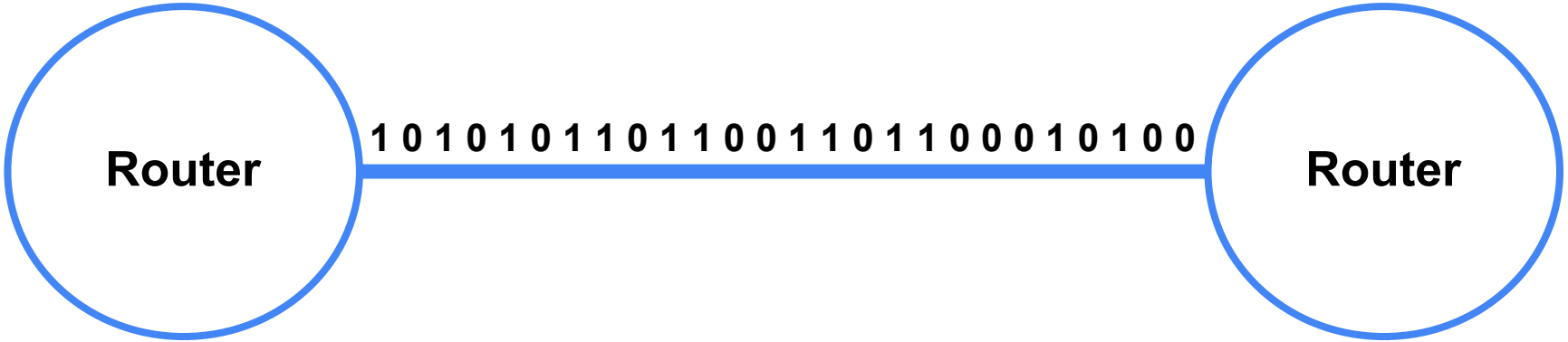
Classless InterDomain Routing (CIDR)



`Web Host Address: 216.3.128.0(/25) <- CIDR notation`

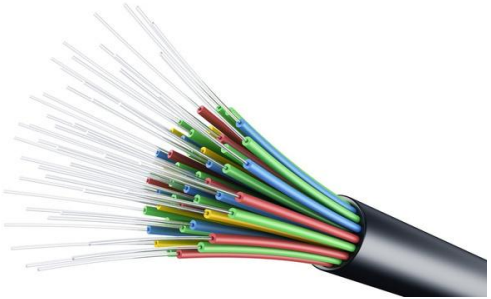
- IP addresses were originally assigned using classes (A-D)
- Each class corresponds to a size of a block of addresses
- This was wasteful so we've begun using Classless InterDomain Routing
- We can represent addresses with their subnet masks in CIDR notation
- The number next to the slash indicates the number of bits assigned to the network address

Link Layer



- The Link Layer is responsible for delivering frames across links between an end host and a router or two routers
- Its key functions are Medium Access Control (MAC), error detection and correction, and message delineation
- Data is translated to bits before being sent across the link

Link Layer



Methods of data transfer:

Electricity

- Data can be transmitted using pulses of electricity through copper wire
- Signal is lost over long distances
- Cheap method of data transfer

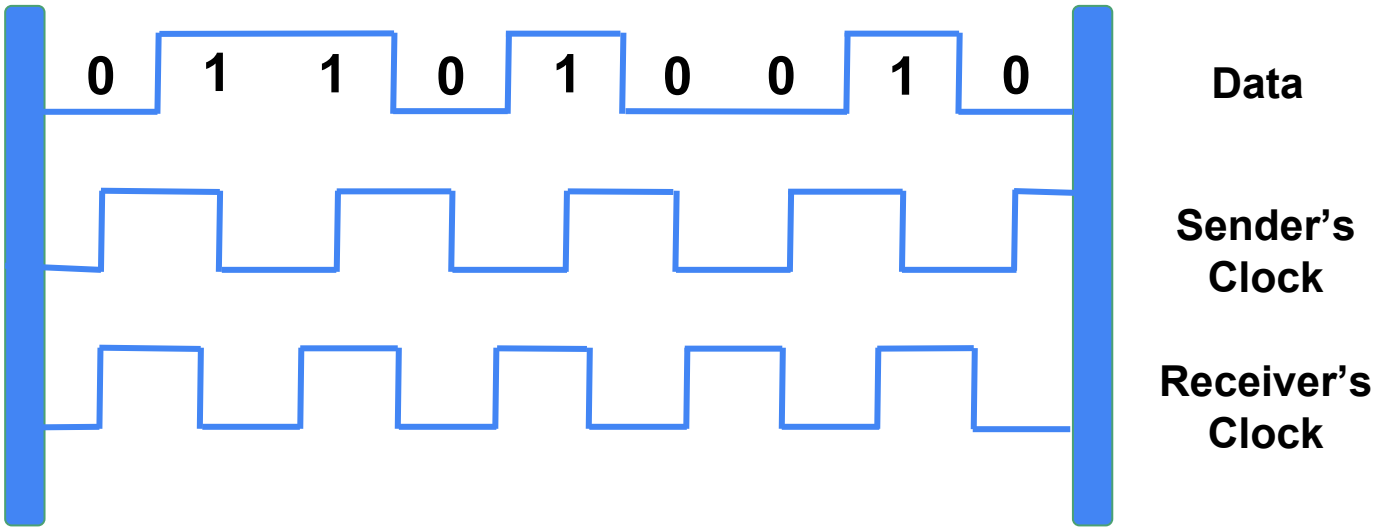
Light

- Data can be transmitted by bounding light up and down the length of fiber optic cables
- No signal loss (this method is used for long distances) and very fast (travels at the speed of light)
- Very expensive

Radio Waves

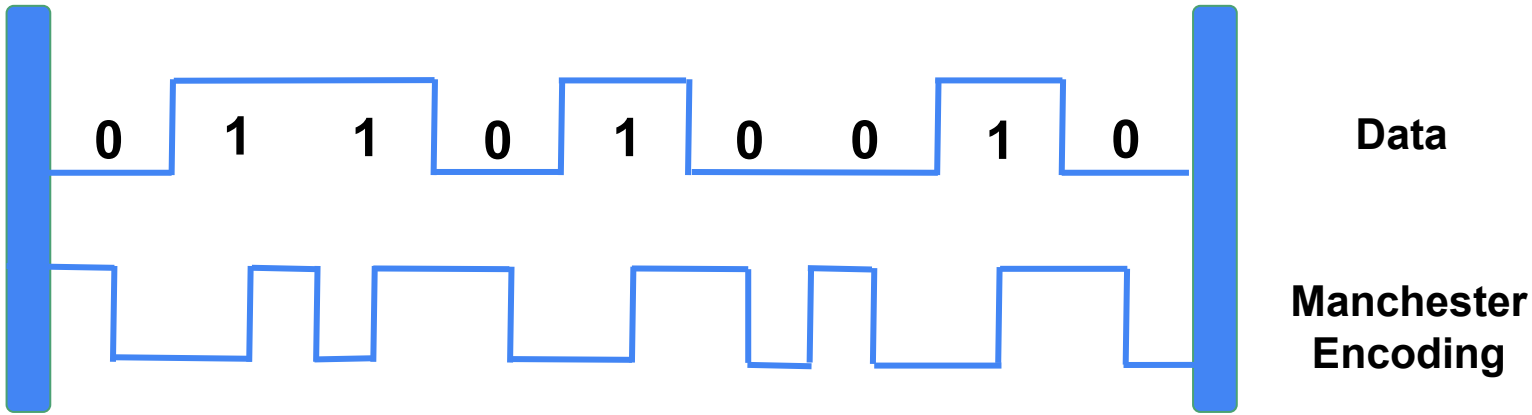
- Wireless mediums use radio waves of different frequencies
- Signal loss occurs over long distances

Message Delineation



- Message Delineation is figuring out where a message starts and where it ends
- If the receiver is accepting data at a slower rate than the sender is sending it, errors occur
- Routers have clock recovery units to sync up their rates of data transmission to ensure that all data is properly received

Message Delineation - Manchester Encoding



Manchester Encoding:

- Use one transition for every bit of data (0 = transition down, 1 = transition up)
- Receiver will be able to match up their clock with the rate at which it sees transitions
- Disadvantage: we insert more transitions than we really need. In the worst case, we are doubling bandwidth

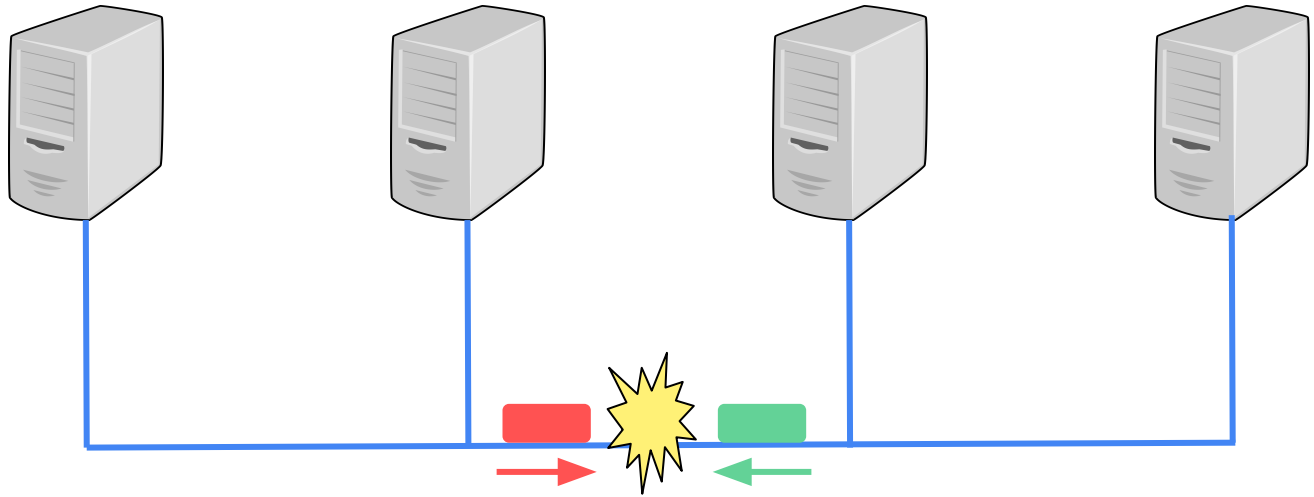
Message Delineation - 4b/5b Encoding

Data	4b/5b
0000	11110
0001	01001
0010	10100
0011	10101
...	...

4b/5b Encoding

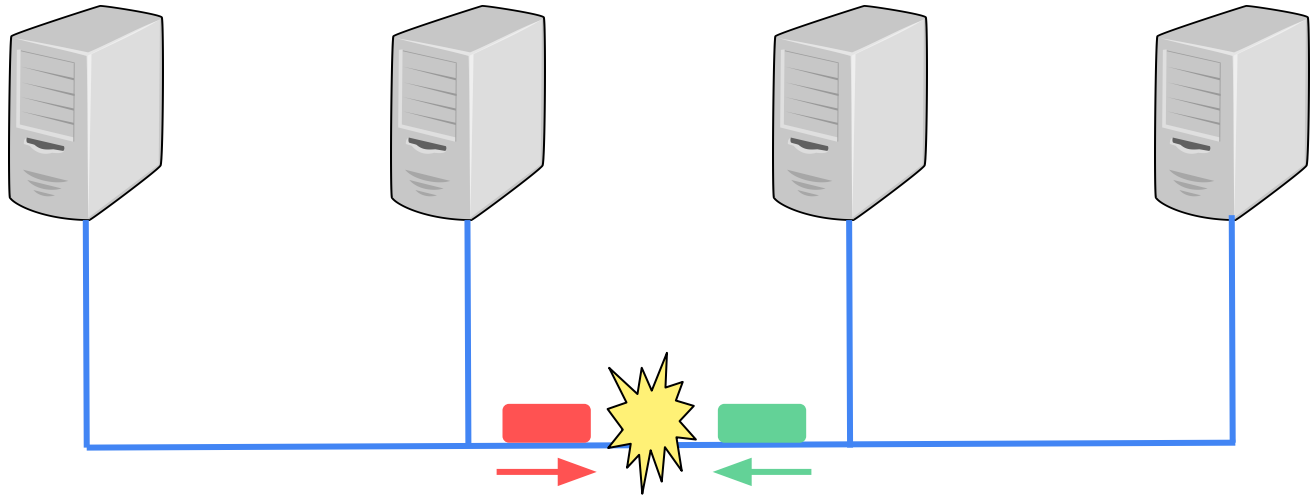
- If we have 4 bits of data to transmit, send 5 instead
- Choose a sequence of 5 bits that has enough transitions for the receiver to tell what clock is being used
- Sender and receiver have an agreed upon mapping of 4 to 5 bit pairs
- More efficient than Manchester coding
- Fewer transitions makes the clock recovery more difficult

Medium Access Control (MAC)



- We often have multiple hosts sharing a medium (cable, air space, etc.), so the Link Layer has to decide who gets to send data and when
- Goal of Medium Access Control (MAC) Protocols is to allow high usage of a shared channel, keep it fair among host, have a simple and low cost of implementation, and remain robust to errors

Medium Access Control (MAC)



Aloha Protocol

- Have data to send? Transmit it
- If it collides with another, try again later

CSMA/CD Protocol

- Check that the line is quiet before transmitting
- If a collision is detected, stop transmitting, wait a random amount of time, and repeat from beginning

Error Detection and Correction

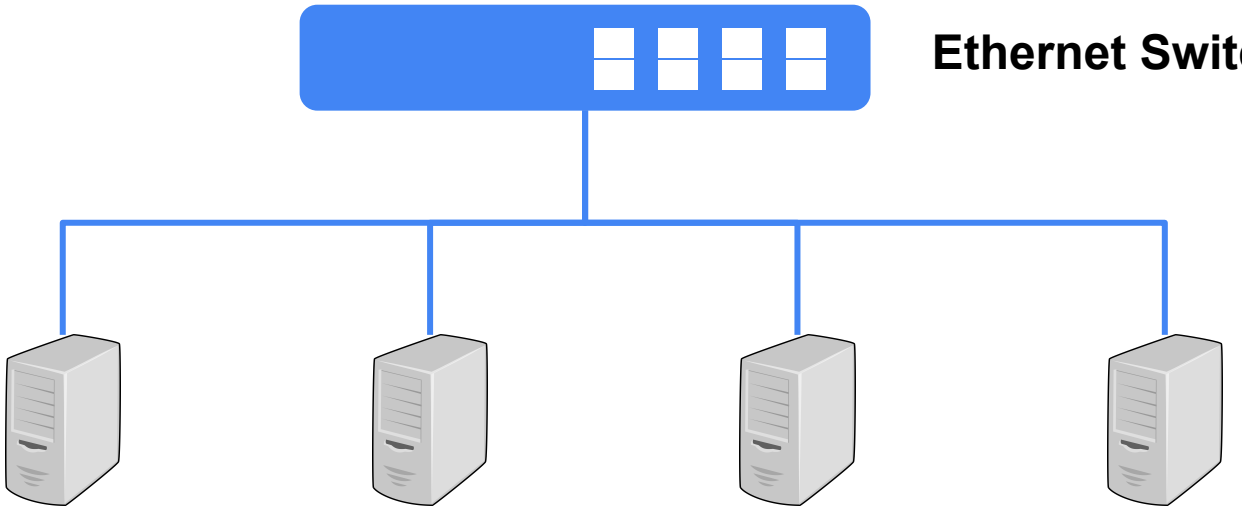
- The Link Layer is prone to a lot of collisions and errors since data is sent over cables and through waves.
- Adding some redundancy at the physical layer can greatly improve the link layer's ability to transmit data correctly
- Examples of Coding Algorithms: Reed-Solomon, Convolutional codes, Hamming codes
- These algorithms proactively add additional data so that the receiver can correct potential errors

Ethernet

Ethernet Frame Format

- Preamble: trains the clock recovery unit
- SFD (Start of Frame Delimiter): indicates the start of the frame
- Destination Address/Source Address: physical addresses
- Type: what data is being transmitted
- Pad: to ensure the frame is of proper length
- CRC (Cyclic Redundancy Check): checks sequence to detect bit errors

Ethernet



- Ethernet switches are located in the centre of a network and are used to route data from one host to another within the network, while preventing collisions
- Forwarding: the switch forwards packets based on a forwarding table. If the destination address is in the table, send to that address. Otherwise, broadcast to all hosts
- Learning: the switch examines the source addresses of arriving traffic to populate the forwarding table