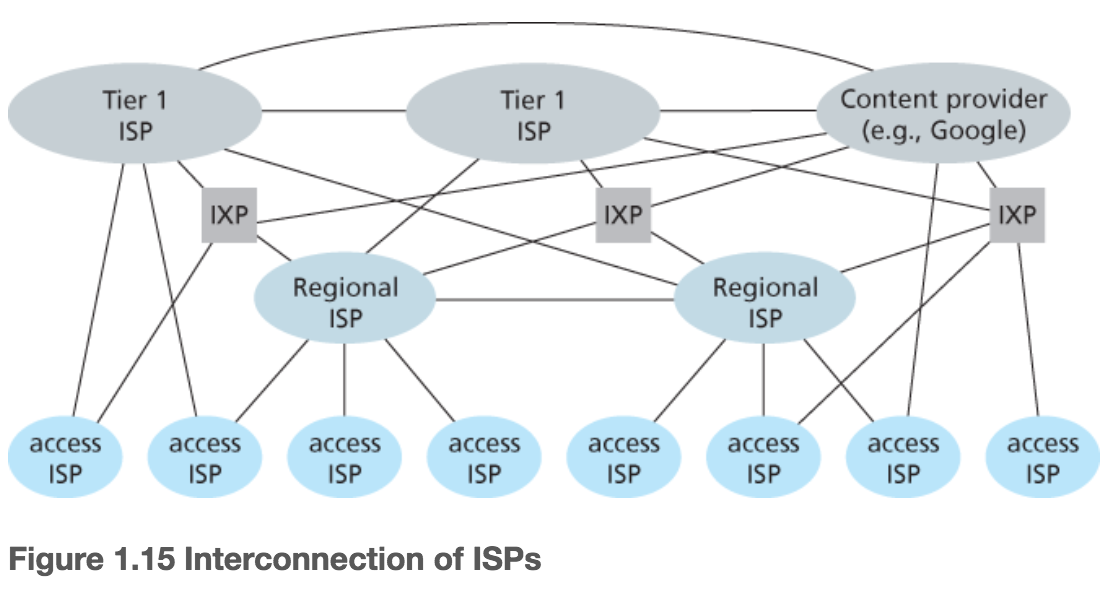
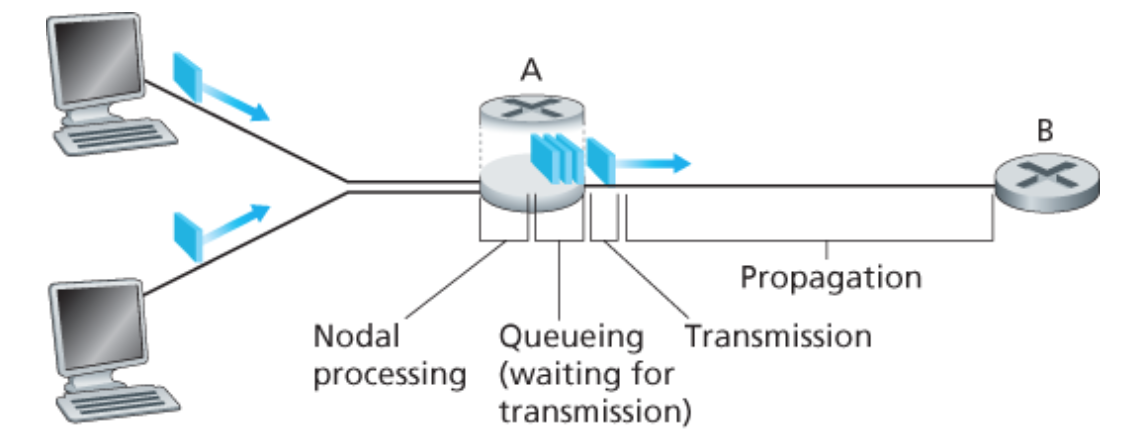
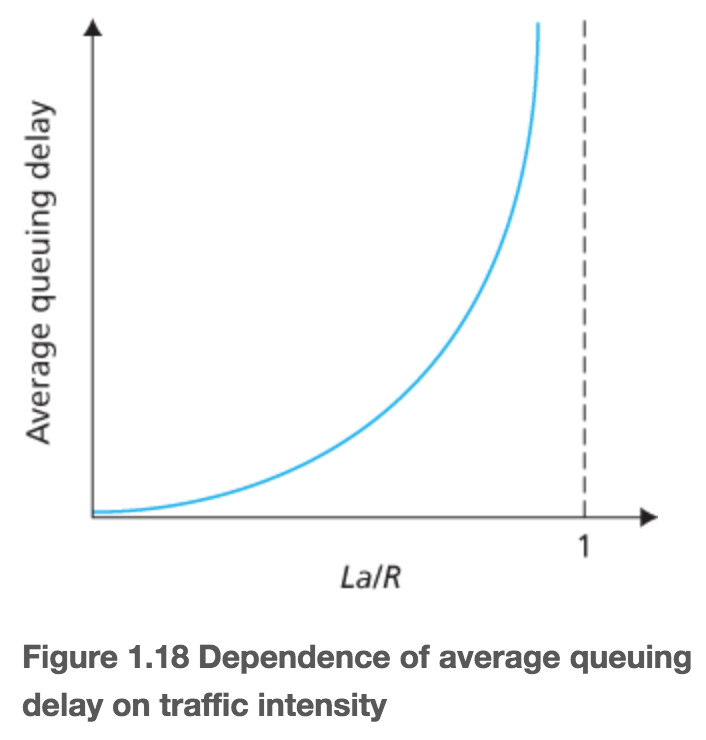
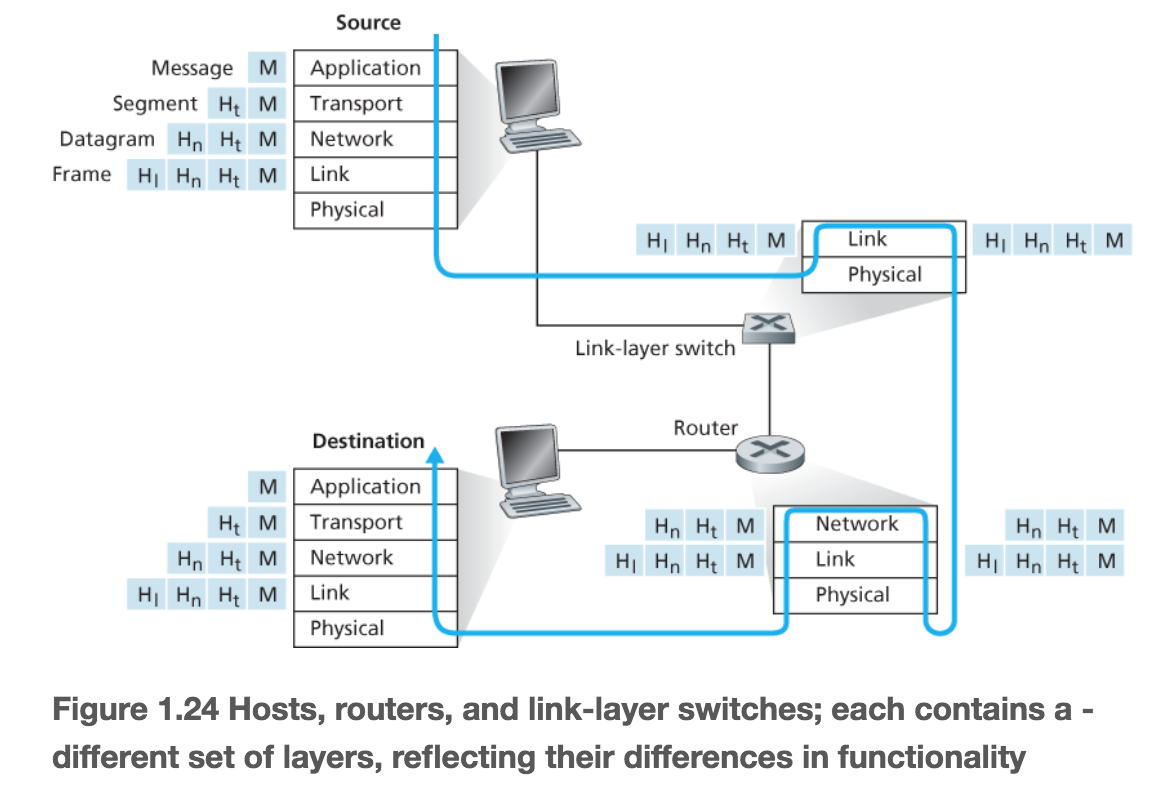
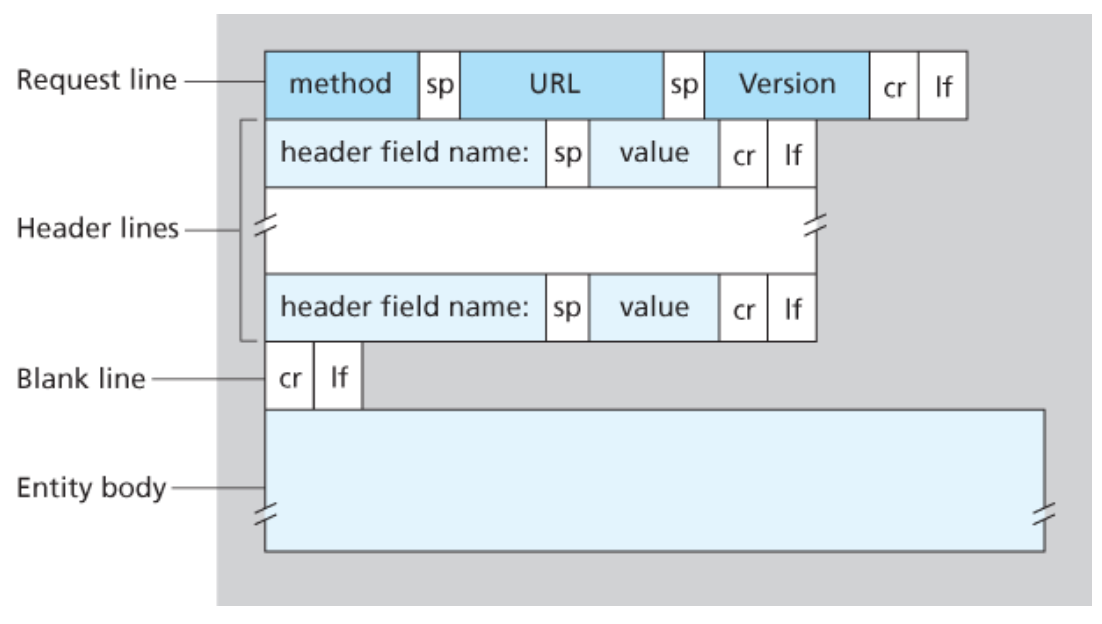
* **1.1 What is the Internet?**
* Hosts/end systems – anything that connects to the internet
  + Internet apps run on end systems, they do NOT run in packet switches in the network core
* Route/path – sequence of communication links and packet switches traversed by a packet
* ISP (Internet Service Provider) – how end systems access internet
  + Each is a network of packet switches and communication links
  + Provide variety of network access to end systems (DSL, LAN)
  + Provide internet access to content providers
  + ISPs that provide access to end systems must be interconnected
  + Lower-tier ISPs are interconnected via (inter)national upper-tier ISPs
  + Upper-tier ISP consists of high-speed routers interconnected with high speed fiber optic links
* Network Protocol – defines format and order of messages exchanged between 2+ communicating entities as well as the actions taken on the transmission and/or receipt of a message or other event
* **1.2 The Network Edge**
* A host (end system) can have 2 categories:
  + Clients – desktop and mobile PCs, smartphones, etc
  + Servers – powerful machines that store and distribute webpages, stream video, etc. Most servers reside in data centers
* Access Network – network that physically connects end system to the first router (aka the edge router) on a path from the end system to any other distant end system
* Asymmetric access – when downstream and upstream transmission rates are not the same
* DSL (digital subscriber line) – prevalent type of broadband residential access
  + Obtained through local telephone company (telco)
  + customer’s telco is also its ISP
  + each customer’s DSL modem uses existing telephone line to exchange data with a DSLAM (DSL access multiplexer) located in the telco’s local central office (CO)
  + the residential telephone line carries both data and traditional telephone signals simultaneously, which are encoded at different frequencies which makes the single DSL link appear as 3 separate links (so that phone and internet can happen at same time)
  + DSL is designed for short distances between the home and the CO (5-10 miles). Maximum downstream/upstream transmission rate is limited by distance between home and CO
* Cable Internet Access – prevalent type of broadband residential access
  + Uses existing cable TV infrastructure
  + Fiber optics connect the cable head end to neighborhood-level junctions (500-5000 homes) from which traditional coaxial cable is used to reach individual homes.
  + Referred to as HFC (hybrid fiber coax) because both fiber and coaxial cable are employed
  + Requires cable modems – external device connects to home PC through Ethernet port
    - Divide HFC network into 2 channels: downstream, upstream
  + CMTS (cable modem termination system) similar to DSLAM
  + IMPORTANT: cable is a shared broadcast medium
    - Every packet sent by the head end travels downstream on every link to every home
    - Every packet sent by a home travels on the upstream channel to the head end
    - So, if several users are simultaneously downloading a video file on the downstream channel, the rate at which each user receives its video file will be significantly lower than the aggregate cable downstream rate
    - Or, if only a few active users, they may receive web pages at full cable downstream rate because users rarely request a web page at exactly the same time
* FTTH (fiber to the home) – up and coming tech with higher speeds than DSL and cable
  + Provide optical fiber path from the CO directly to home
  + Potentially provide internet access in the gigabits per second range
* Satellite Link – can connect residence to the internet in areas where DSL, cable, and FTTH are not available
* Optical distribution networks
  + Direct fiber (simplest) – one fiber leaving the CO for each home. Each fiber is shared by many homes and gets split when it gets close to the homes. 2 competing optical distribution network architectures that perform the splitting:
    - AON (active optical networks) – essentially switched Ethernet
    - PON (passive optical networks)
      * used by Verizon FIOS
      * Each home has an ONT (optical network terminator) which is connected by dedicated optical fiber to a neighborhood splitter (typically has less than 100 homes on a single shared optical fiber) which connects to an OLT (optical line terminator) in the telco’s CO
      * All packets sent from OLT to the splitter are replicated at the splitter (similar to cable head end)
* Local Area Network (LAN) – used to connect end system to edge router
  + Ethernet – most prevalent
    - Ethernet users use twisted pair copper wire to connect to Ethernet switch which is then connected to larger internet
* Wireless LAN – users transmit/receive packets to/from an access point that is connected into the enterprise’s network (most likely using wired Ethernet) which is connected to wired internet.
  + User must be within a few tens of meters to the access point (WiFi)
* Wide-Area Wireless Access (3G and LTE) – user needs to be a few tens of meters of the base station
  + Employ same wireless infrastructure used for cellular telephony to send/receive packets through a base station that is operated by the cellular network provider
* Physical Medium – something a bit must be sent across between each transmitter-receiver pair.
  + Can take many shapes and forms
  + Does not have to be the same type for each transmitter-receiver pair along the path
  + Examples: twisted-pair copper wire, coaxial cable, multimode fiber-optic cable, terrestrial radio spectrum, and satellite radio spectrum
  + Guided media (1/2 types of physical media)
    - Waves are guided along a solid medium such as a fiber optic cable, twisted-pair copper wire, or coaxial cable
  + Unguided Media (2/2 types of physical media)
    - Waves propogate in the atmosphere and in outer space such as wireless LAN or digital satellite channel
* Physical link cost is minor compared to other networking costs. So, builders install all physical links in every room in a home even if just one is used.
* Guided and Unguided Transmission Mediums
* Twisted-Pair Copper Wire
  + Least expensive and most commonly used
  + Used by telephone networks for 100+ years
  + Two insulated copper wires, each 1mm thick, arranged in spiral pattern. Wires are twisted to reduce electrical interference from similar pairs nearby
  + A number of pairs are bundled together in a cable by wrapping the pairs in a protective shield
  + A wire pair constitutes one communication link
  + UTP (unshielded twisted pair) – used for computer networks within a building (LANs). Data rates depend on thickness of wire and distance between transmitter and receiver
  + Commonly used for residential internet access
* Coaxial Cable
  + 2 copper conductors that are concentric (not parallel)
  + common in cable TV systems
  + can be used as a guided shared medium (a number of end systems can be connected directly to the cable with each host receiving whatever is sent by the other end systems)
* Fiber Optics
  + Thin, flexible medium that conducts pulses of light. Each pulse represents a bit
  + One optical fiber can support up to tens/hundreds of gigabits per second
  + Immune to electromagnetic interference, have low signal attenuation, and are very hard to tap
  + The preferred long-haul guided transmission media (especially for overseas links)
  + Optical devices (transmitters, receivers, and switches) have a high cost so it is not used for short-haul transport
* Terrestrial Radio Channels
  + Carry signals in the electromagnetic spectrum
  + Require no physical wire to be installed, penetrate walls, provide connectivity to a mobile user
  + Environmental considerations: path loss and shadow fading (decrease the signal strength as it travels and goes through/around obstructing objects) multipath fading (signal reflection off of interfering objects), and interference (other transmissions and electromagnetic signals)
  + 3 groups: (1) very short distance 1-2 meters wireless headsets, keyboards and medical devices, (2) local areas 10-100s meters, (3) wide area tens of kilometers cellular access technologies
* Satellite Radio Channels
  + Links 2+ earth-based microwave transmitter/receivers (aka ground stations)
  + satellite receives transmissions on one frequency band, regenerates the signal using a repeater and transmits the signal on another frequency
  + two types of satellites used:
    - Geostationary
      * Permanently remain above the same spot on earth 36,000 km above Earth’s service
      * Substantial signal propagation delay of 280 milliseconds
    - Low-earth orbiting (LEO)
      * Much closer to earth and do not remain permanently above one spot on earth (rotate around earth)
      * Communicate with each other and with ground stations
* **1.3 The Network Core**
* Network core – mesh of packet switches and links that interconnects the Internet’s end systems
* Message – what end systems exchange with one another. Contain anything
* Packets – smaller chunks of messages. Packets are transmitted over each communication link at a rate equal to the full transmission rate of the link. if a source end system or a packet switch is sending a packet of L bits over a link with transmission rate R bits/sec, then the time to transmit the packet is L / R seconds
* Packet Switches
  + Routers (1 type)
  + Link-layer switches (2nd type)
  + Store-and-forward transmission – what most packet switches use at the inputs to the links
    - packet switch must receive entire packet before it transmits the first bit of the packet onto the outbound link
    - source begins to transmit at time 0; at time L/R seconds source has transmitted entire packet AND entire packet has been received and stored at the router (not accounting for propagation delay) it can begin to transmit the packet onto the outbound link towards its destination; at time 2L/R router has transmitted entire packet and entire packet has been received by the destination. Total delay is 2L/R
      * Total delay would be L/R if switch forwarded bits as soon as it received them instead of waiting for the entire packet
      * End-to-end-delay of a message with a number packets traveling over a path of N links each of rate R (so there are N-1 routers) is N(L/R).
        + Example: by time 3L/R, destination has received first two packets and the router has received the third packet
* Propogation Delay – the time it takes for the bits to travel across the wire at near the speed of light
* Output buffer (output queue)
  + there is one for each link attached to a paket switch
  + Stores packets the router is about to send into that link
  + *Key for packet switching*.

Queueing delay

* + If arriving packet needs to be transmitted onto a link but the link is busy, the packet waits in the output buffer
  + Variable and depend on level of congestion
  + Packet loss occurs if an arriving packet finds that the buffer is completely full. Either the arriving packet or one of the already queued packets will be dropped.
* How the Internet forwards a packet
  + Every system has an address (IP address) that has a hierarchal structure (like postal address)
  + Router has a *forwarding table* that maps destination addresses to that router’s outbound links
  + Router examines address and searches its forwarding table to find the appropriate outbound link
  + Like asking for directions along your trip instead of having directions with you
* Routing protocol – used to automatically set forwarding tables. It may determine shortest path from each router to each destination and use those results to configure forwarding tables in the routers
* 2 approaches to moving data through network of links and switches (circuit switching and packet switching)
* Circuit – connection between sender and receiver that guarantees a connection for the switches on the path between sender and receiver. Guarantees constant transmission rate in the network’s lines
* Circuit-switched networks – resources needed along a path (buffers, link transmission rate) are reserved for duration of the communication session between the end systems (example: traditional telephone networks)
  + Dedicated end to end connection
* Packet-switched networks – resources are not reserved; session’s messages use the resources on demand and may have to wait for access to a communication link (internet) nothing is guaranteed, may have to wait
* A circuit in a link is implemented with either FDM or TDM
* FDM (frequency division multiplexing)
  + frequency spectrum of a link is divided among the connections established across the link.
  + Link dedicates a frequency band to each connection for the duration of the connection
  + For telephone networks, typically 4kHz
  + Bandwidth – width of the band
  + Radio stations use this between 88mHz and 108 mHz
* TDM (time division multiplexing)
  + Time divided into frames of fixed duration, each frame is divided into a fixed number of time slots
  + When network establishes connection across a link, it dedicates one time slot in every frame to the connection
  + Slots are dedicated for the sole use of that connection
  + One time slot available for use in every frame to transmit the connection’s data
* Why Packet switching is bad
  + Not suitable for real time services because of its variable/unpredictable queuing delays
* Why Packet switching is good
  + Has better sharing of transmission capacity than circuit switching
  + Simpler, more efficient, less costly than circuit switching
  + Can perform better than packet switching based on number of users at once
* Why circuit switching is bad
  + wasteful because dedicated circuits are idle during silent periods
  + complicated because establishing end to end circuits and reserving end to end transmission is complicated requires complex signaling software to switches
* Circuit switching pre-allocates use of transmission link regardless of demand with allocated but unneeded link time going unused
* Packet switching allocates link use on demand
* Tier-1 ISPs
  + About a dozen of these
  + Regional ISPs connect to one
* PoPs (points of presence)
  + Exist in all levels of network hierarchy (except bottom/access ISP level)
  + One or more routers (at the same location) in the provider’s network where customer ISPs can connect into the provider ISP
  + Customer can lease high speed link from third party telecommunications provider to directly connect one of its routers to a router at the PoP
* Multi-home
  + To connect 2 or more provider ISPs, or many regional ISPs and a tier-1 ISP, or many tier01 ISPs
  + Allows ISP to continue to send/receive packets into the internet even if one of its providers has a failure
* Peer
  + Pair of nearby ISPs can directly connect their networks together so that all the traffic between them passes over the direct connection rather than through upstream intermediaries
  + Settlement-free (neither ISP pays the other)
* IXP (internet Exchange Point)
  + Network structure 4
  + Meeting point where many ISPs can peer together
  + Typically a stand-alone building with its own switches
* Content-provider networks
  + Google
  + This on top of network structure 4 creates network structure 5
* 
* **1.4 Delay, Loss, and Throughput in Packet-Switched Networks**
* Delays a packet goes through passing from one node (host or router) to another node (host or router)
  + Nodal Processing delay
    - Time needed to examine the packet’s header and determine where to direct it
    - Can include time needed to check for bit-level errors that occurred in transmitting it
    - For high-speed routers, microseconds or less
  + Queuing delay
    - Packet waits at the queue to be transmitted onto the link
    - Length of delay dpends on number of earlier-arriving packets that are also waiting
    - Delay is 0 if queue is empty and no other packet is currently being transmitted
    - Can be microseconds to milliseconds
  + Transmission delay
    - Because of FIFO manner of transmitting packets
    - Length of packet is L bits, transmission rate of the link from router A to B is R bits/sec. For 10 Mbps Ethernet link, R = 10 Mbps.
    - Transmission delay is L/R – amount of time required to push (transmit) all of the packet’s bits into the link
    - Microseconds to milliseconds
  + Propagation delay
    - Once a bit is pushed into the link, this delay is the time required to propagate from the beginning of the link to router B
    - In the range of 2x10^8 meters/sec to 3x10^8 meters/sec (a little less than the speed of light)
    - This delay is d/s where s is the distance between router A and B and s is the propagation speed of the link
  + Total nodal delay – all of the previous delays together
    - d\_nodal = d\_proc + d\_queue + d\_trans + d\_prop
  + 
  + Transmission delay vs propagation delay
    - Transmission
      * time required for the router to push out the packet
      * function of the packet’s length and transmission rate of the link
    - Propagation
      * Time it takes a bit to propagate from one router to the next
      * Function of the distance between 2 routers (does not deal with packet’s length or transmission rate of link)
* Queuing delay is special
  + When characterizing it, use statistical measures (average queuing delay, variance of it, probability it exceeds some value)
  + Traffic intensity – La/R where we assume each packet is L bits, a is the average rate at which packets arrive at the queue, and R is the transmission rate in bits/sec
    - If La/R > 1, the rate at which bits arrive at the queue exceeds rate at which they are transmitted from the queue. Here, the queue will increase without bound and the queuing delay will approach infinity
    - Make sure traffic intensity is no greater than 1
    - If traffic arrives periodically, no queuing delay
    - If traffic is in bursts, can be significant average queuing delay. Packet 1 has no delay. Packet 2 has L/R queuing delay. Packet n has queuing delay of (n-1)L/R seconds
  + 
* Packet Loss
  + A queue can not hold infinite packets
  + If a packet arrives to a full queue, the router will drop that packet and it will be lost
  + Queuing delay never actually gets to infinity because of packet loss
* End-to-End Delay – *d\_end-end = N(d\_proc + d\_trans + d\_prop)*
  + N-1 routers between source host and destination host because source sends N special packets into the network, addressed to the destination, marked 1-N
  + d\_proc is processing delay at each router and at source host, transmission ate out of each router and out of source host is R bits/sec, d\_proc is propagation on each link, d\_trans = L/R where L is packet size
* Other delays
  + End system wanting to transmit a packet into a shared medium (like wifi or cable modem) may purposefully delay its transmission as part of its protocol
  + Media packetization delay – time to fill a packet
* Throughput
  + Instantaneous throughput – at any time, the rate (bits/sec) at which Host B is receiving the file
  + Average throughput – F bits in the file takes T seconds for Host B to receive all F bits, the average throughput is F/T bits/sec
* **1.5 Protocal Layers and their Service Models**
* Layered Architecture
  + Allows us to discuss well-defined specific part of a large/complex system
  + Layer provides the same service to the layer above it and uses same services from layer below it
  + Can change implementation of one layer without changing remainder of the system (modularity)
  + Issues with layering:
    - One layer may duplicate lower-layer functionality
    - Functionality at one layer may need information that is presented only in another layer (violates the goal of separate layers)
* Each protocol belongs to one layer
* Service model of a layer – services that a layer offers to the layer above
* Protocol stack – the protocols of the various layers together
* Internet protocol stack (5 layers)
  + Application (top layer)
    - Where network applications and their protocols reside
    - Includes many protocols:
      * HTTP provides web document request and transfer
      * SMTP provides transfer of e-mail
      * FTP provides transfer of files between 2 end systems
    - Application layer protocol is distributed over many end systems which the application in one using the protocol to exchange packets of information (the message) in another.
  + Transport
    - Transports application-layer messages between application endpoints
    - Two transport protocols:
      * TCP provides connection oriented service to its appls. Guarantees delivery of application layer messages to destination and flow control. Breaks up long messages into shorter segments and provides congestion control
      * UDP provides connectionless service to its apps.
    - Transport layer packet = segment
  + Network
    - Moves network-layer packets (datagrams) between hosts
    - Provides service of delivering segment to the transport layer in the destination host
    - Includes IP protocol which defines the fields in the datagram and how the end systems/routers act on these fields.
    - Routing protocols determine routes the datagrams take between source and destination
    - One IP protocol, many routing protocols
    - Often called the IP layer
  + Link
    - Moves packet from one node to the next one in its route
    - At each node, network layer passes datagram down to link layer which delivers datagram to next node in the route. At next node, passes datagram up to network layer
    - Some link layer protocols provide reliable delivery (Ethernet, wifi, and cable)
    - Frames – link layer packets
  + Physical (bottom layer)
    - Moves the individual bits within the frame from one node to the next
    - Protocols are link dependent and depend on actual transmission medium of the link (like twisted pair copper wire)
* OSI Model (Open Systems Interconnection model)
  + Mandated by the ISO (International Organization for Standardization)
  + 7 layers (the ones with same names as internet protocol stack are largely the same) 2 additional layers
    - Application
    - Presentation
      * Provides services that allow communicating apps to interpret the meaning of data exchanged. Include data compression, encryption, and description (which frees the apps from worrying about the internal format the data is stored/represented)
    - Session
      * Provides delimiting and synchronization of data exchange. Includes means to build a checkpoint and recovery scheme
    - Transport
    - Network
    - Data link
    - Physical
* 
* Encapsulation – illustrated above
  + At the sending host, an application-layer message (M) is passed to transport layer. The transport layer appends additional information to M (transport-layer header information) that will be used by the receiver side transport layer. The transport-layer segment encapsulates application-layer message
* At each layer, a packet has 2 fields
  + Header fields
  + Payload fields – typically a packet from the above layer
* **1.6 Networks Under Attack**
* Malware – bad stuff on the internet that can enter and infect our devices
  + Botnet – thousands of compromised devices
  + Self-replicating
  + Virus – require user interaction to infect user’s device
  + Worm – malware that enter a device without explicit user interaction
* Denial of Service (DoS) attacks
  + Renders something unusable by legitimate users
  + Three general categories:
    - Vulnerability Attack - Send well crafted messages to vulnerable application or operating system on a target host
    - Bandwidth Flooding - Attack sends deluge of packets to target host so that target’s access link becomes clogged preventing legitimate packets from reaching server
      * If server has access rate of R bps, attacker needs to send traffic at rate of R bps to cause damage
      * Distributed DoS (DDoS) attach – attacker controls many sources and has each blast traffic at the target. Common today. Are hard to detect and defend against than DoS attacks from a single host
    - Connection Flooding – attacker establishes large number of half/fully open TCP connections at the target host. Host stops accepting legitimate connections
* Packet sniffer
  + passive receiver that records copy of every packet that flies by (mostly happens with wireless devices)
  + wireshark lab have students make a packet sniffer
  + passive means they do not inject packets into a channel which makes it hard to detect
* IP Spoofing
  + ability to inject packets into the internet with false source address
  + need end-point authentication to solve this
* **2.1 Principles of Network Applications**
* Application Architecture – designed by the developer and dictates how the app is structured over the various hosts. Developer will probably draw on one of two architectural paradigms
  + Client-server architecture
    - Server is a host that is always on and services requests from other hosts called clients
    - Server has fixed well known address
    - Since server is always on, client can contact server by sending a packet to server’s IP address
    - Data center – houses large number of hosts, used to create powerful virtual server
  + Peer-to-peer (P2P) architecture
    - Minimal/no reliance on dedicated servers in data center
    - Application uses direct communication between pairs of intermittently connected hosts called peers
    - Peers are end systems controlled by users
    - Self-scalability – each peer generates workload by requesting files but ALSO adds service capacity to the system by distributing files to other peers
  + Some applications have hybrid (P2P and client server architecture)
    - Example: for messaging apps, servers track IP addresses of users but user-to-user messages are sent directly between the hosts
* Process – program that is running within an end system
* Client and Server Processes
  + With any pair of processes, one is called the client and the other the server. With p2p each host is often both but is either client or server when we look at pairs of processes
* Socket
  + software interface that allows a process to send and receive messages
* API (Application Programming Interface)
  + Socket that interfaces between application layer and transport layer within a host
  + Developer has control over everything on application layer side
  + Developer has control of 2 things on transport-layer side:
    - Chose of transport protocol
    - Ability to fix a few transport-layer parameters like max buffer and max segment sizes
* Addressing processes
  + To identify receiving process, needs 2 pieces of information:
    - Address of the host
    - Identifier that specifies the receiving process in the destination host
    - Host is identified by its IP address (32 bits)
    - Sending process must identifies the receiving process (receiving socket) in the host by its port number
* Reliable data transfer – when a protocol (at the transport layer) provides a guaranteed data delivery service
* Loss-tolerant applications – are ok with minute amount of lost data (example: video callings apps)
* Throughput
  + In context of a communication session between 2 processes along a network path: the rate at which the sending process can deliver bits to the receiving process
  + Available throughput can fluctuate with time b/c other session can share bandwidth randomly
  + Transport layer could provide guaranteed available throughput at some specified rate of r bits/sec
  + Bandwidth-sensitive apps have throughput requirements
  + Elastic applications can use as much or as little throughput as is available
* Timing
  + Transport-layer protocol can provide timing guarantees
  + Appealing to interactive real-time applications
* Security
  + Transport protocol can provide an app with security services
  + Encrypt/decrypt data
* TCP Services
  + Connection oriented service
    - Client and server exchange transport-layer control information before application-level messages begin to flow (handshaking procedure)
    - This alerts the client and server to prepare for onslaught of packets
    - TCP connection exists between the sockets after the handshaking phase
    - Full-duplex connection (both processes can send messages at same time)
    - When finished sending messages, the app must tear down the connection
  + Reliable data transfer service
    - TCP delivers all data sent without error and in the proper order
  + Congestion control
    - Good for general welfare of the internet
    - Throttles a sending process when the network is congested between sender and receiver
    - Attempts to limit each TCP connection to its fair share of network bandwidth
* UDP Services
  + No frills, lightweight transport protocol
  + Connectionless (no handshaking)
  + Unreliable data transfer service – no guarantee the receiving process with get the message, no guarantee on correct order
  + No congestion control – sending side of UDP can pump data into the layer below (network layer) at any rate
* Application layer protocol – defines how an app’s processes (running on different hosts) pass messages to each other. It defines:
  + Types of messages exchanged (request/response messages)
  + Syntax of the various message types (fields in the message and how the fields are delineated)
  + Semantics of the fields – meaning of the information in the fields
  + Rules determining when/how a process sends/responds to messages
* **2.2 The Web and HTTP**
* HyperText Transfer Protocol (HTTP) – web’s application layer protocol
  + Implemented on 2 programs (client and server program) executing on different end systems, talk to each other by exchanging HTTP messages
  + defines structure of these messages and how the client/server exchange them
  + defines how Web clients request Web pages from web servers and how servers transfer pages to clients
  + uses TCP as its underlying transport protocol
    - HTTP client first initiates a TCP connection with the server. Then the browser and server processes access TCP through their socket interfaces
    - Server sends requested files to clients without storing any state information about the client (stateless protocol)
    - Client-server application architecture
  + Does not specify how a client interprets a page
* Web terminology
  + Web page (document) consists of objects
    - Most consist of a base HTML file and several referenced objects
  + Object – file that is addressable by a single URL
  + Web browser – implement client side of HTTP (browser and client used interchangeably)
  + Web servers – implement server side of HTTP, house Web objects, each addressable by a URL
* Non-persistent connection – each request/response pair is sent over a separate TCP connection
  + each TCP connection is closed after the server sends the object
  + connection does not persist for other objects (so for web page with 10 images and 1 HTML file, 11 TCP connections are generated)
  + problems:
    - TCP buffers must be allocated for every single connection (each object needs different connection)
    - TCP variables must be kept in both client and server
    - Causes significant burden
    - Each object suffers delivery delay of two RTTS (one to establish TCP connection and one to request/receive and object)
* Persistent Connections – request/response pairs sent over same TCP connection
  + Multiple web pages residing on same server can be sent from server to the same client over a single connection
  + Requests for objects can be pipelined – made back to back without waiting for replies to pending requests
  + Typically, HTTP server closes connection when unused for a period of time (timeout interval)
* Round trip time (RTT) – time it takes for a small packet to travel from client to server and then back to the client
  + Includes packet-propagation delays, packet-queuing delays in intermediate routers and switches, and packet processing delays
  + When someone clicks a hyper link, like a three way handshake.
    - Roughly, total time is 2 RTTs + transmission time at server of HTML file
* HTTP Message Format
* Request Message
  1. GET /somedir/page.html HTTP/1.1
  2. Host: [www.someschool.edu](http://www.someschool.edu)
  3. Connection: close
  4. User-agent: Mozilla/5.0
  5. Accept-language: fr
  + Request line – first line of HTTP request message.
    - Has 3 fields
      * Method field
        + GET – used most often; requests an object with requested object in the URL field (this time, somedir/page.html is being requested)
        + POST
        + HEAD – similar to GET method. When server receives request with this method, responds with an HTTP message but leaves out requested object. Used for debugging
        + PUT – used in conjunction with web publishing tools. Allows user to upload an object to a specific path (directory) on a specific web server
        + DELETE – allows a user (or app) to delete an object on a web server
      * URL field
      * HTTP version field
  + Header lines – lines after request line
    - Line 02: specifies the host on which the object resides. This information is required by web proxy caches
    - Line 03: browser tells to do non-persistent connections
    - Line 04: specifies user agent (browser type that is making the request to the server) this is so the server can send different versions of the same object to different types of user agents
    - Line 05: indicates user prefers to receive French version of the object. Accept-language: header is one of many content negotiation headers available in HTTP
  + Entity body
    - Empty with GET method
    - Used with POST method
  + 
* Response Message
  1. HTTP/1.1 200 OK
  2. Connection: close
  3. Date: Tue, 18 Aug 2015 15:44:04 GMT
  4. Server: Apache/2.2.3 (CentOS)
  5. Last-Modified: Tue, 18 Aug 2015 15:11:03 GMT
  6. Content-Length: 6821
  7. Content-Type: text/html
  8. (data data data data data data …)
  + this message has 3 sections:
    - status line (line 01)
      * 3 fields
        + protocol version field (HTTP/1.1)

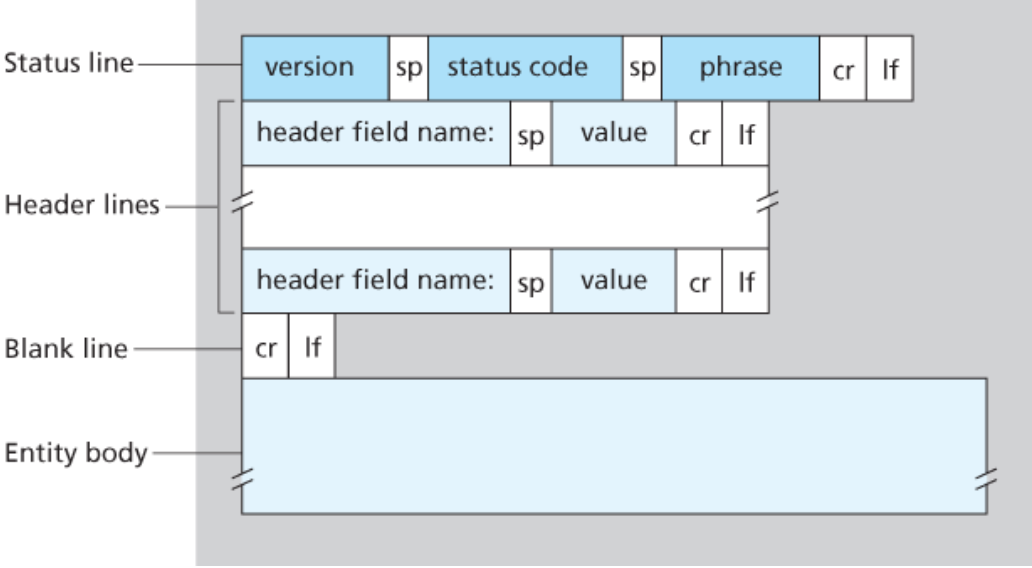
200 OK: request succeeded and information is returned in the response

301 Moved Permanently: requested object has been permanently moved to Location: header of the response message

400 Bad Request: generic error code, server can’t understand request

404 Not Found: document doesn’t exist on the server

505 HTTP Version Not Supported: requested HTTP protocol version is not supported by server

* + - * + status code
        + corresponding status message
    - header lines (lines 02-07)
      * line 03: indicates time and date when HTTP response was created and sent by the server NOT the time when object was created or last modified
      * line 04: indicates message was generated by apache web server (analogous to user-agent in request message)
      * line 05: critical for object caching
      * line 06: indicates number of bytes in the object being sent
      * line 07: OFFICIALLY indicates object in the entity body is html text
    - entity body (line 09)
    - 
* **2.4 DNS – The Internet’s Directory Service**
* Hostname – one way to identify a host; mnemonic, difficult for routers to process, for humans (www.facebook.com)
* IP Addresses – one way to identify a host; consists of four bytes and has rigid hierarchal structure (121.7.106.83)
* Domain Name System (DNS) – main task is to be a directory service that translates hostnames to IP addresses
  + Is a distributed database implemented in a hierarchy of DNS servers
  + Is an application-layer protocol that allows hosts to query the distributed database
  + Often UNIX machines running the Berkeley Internet Name Domain (BIND) software
  + Runs over UDP uses port 53
  + Commonly employed by other application-layer protocols (HTTP and SMTP) to translate user supplied hostnames to IP addresses
  + Adds additional delay (sometimes substantial) to the applications that use it
  + Desired IP address is often cached in nearby DNS server which reduces DNS network traffic as well as the average DNS delay
  + Host aliasing – host with complicated hostname can have one or more alias names. The original complicated hostname is called the canonical hostname
  + Mail server aliasing – same as above but for email
  + Load distribution – busy sites are replicated over many servers with each running on a different end system and having a different IP address. For replicated web serbvers, set of IP addresses is associated with one canonical hostname.
    - When client makes DNS query for a name mapped to seberal addresses, server responds with entire set of IP addresses but rotates ordering of the addresses within each reply. Client sends HTTP request message to first IP address listed. So, DNS rotation distributes traffic among replicated servers.
* **1. Layering and Encapsulation (1.5)**
* - The layers and their functions
* - Packet Encapsulation
* **2. Circuit and Packet Switching (1.3-1.4)**
* - Definition of delay types
* - How to compare circuit and packet switching
* **3. HTTP protocol (2.2)**
* - Basic commands
* - Message format
* **4. Domain Name System (2.4)**
* - Zones
* - Iterative vs. Recursive queries
* **5. TCP congestion control (3.7)**
* - Slow Start
* - Fast Recovery
* - Additive Increase/Multiplicative Decrease
* **6. Weighted Fair Queuing (4.2)**
* - Packet Finish Numbers
* - Virtual Time
* - Weights
* **7. CIDR forwarding (4.3)**
* - Addresses and Prefixes
* - Longest Prefix Match
* **8. Sub-Nets (4.3)**
* -Subnet masks
* **9. Link State Routing  (5.2)**
* - Flooding
* - Dijkstra's Shortest-Path Algorithm
* **10. Distance Vector Routing (5.2)**
* - Vector exchanges
* - Convergence rate for increase/decrease
* - Poisoned Reverse
* **6.1 Introduction to the Link Layer**
* link layer – moves datagram rom one node to adjacent node over single communication link
* node – any device that runs a link-layer protocol
  + includes hosts, routers, switches, and wifi access points
* link – communication channel that connects adjacent nodes along the communication path
* link-layer frame – what a transmitting node encapsulates the datagram in over a given link
* services that can be offered by link-layer protocol:
  + Framing
    - Frame consists of
      * Data field – where network-layer datagram is inserted
      * Many header fields
    - Frame structure is specified by the link-layer protocol
    - Most link-layer protocols encapsulate each network layer datagram within a link-layer frame before transmission over the link
  + Link Access - Medium access control (MAC) protocol specifices rules by which a frame is transmitted onto the link
    - Point to point links – single sender at one end of the link and single receiver at other end (MAC protocol is simple/nonexistent: sender sends frame when link is idle)
    - Many nodes share single broadcast link – (multiple access problem) MAC protocol servers to coordinate frame transmissions of the many nodes
  + Reliable Delivery – guarantees to move each network-layer datagram across link without error
    - Can be achieved with acknowledgements and retransmissions
    - Often used for links prone to high error rates (like wireless links) with the goal of correcting the error locally (on the link where the error occurs) instead of forcing end-to-end retransmission of the data by transportation or application-layer protocol
    - Can be unnecessary overhead for low bit-error links (like fiber, coax, and twisted-pair copper links)
  + Error Detection and Correction
    - Bit errors can be caused by signal attenuation and electromagnetic noise
    - Prevent bit errors by having the transmitting node include error detection bits in the frame and having receiving node perform error check
    - Usually more sophisticated than transport and network layer error detections and implemented in hardware
* Where is the Link Layer Implemented?
  + In a router’s line card
  + Implemented in a network adapter (aka network interface card NIC) – at the heart of the adapter is the link-layer controller, a single special-purpose chip that implements many of the link layer services
  + Much is implemented in hardware
  + The software component of the link layer implements higher-level link layer functionality like assembling link layer addressing information and activating the controller hardware
* **6.2 Error Detection and Correction Techniques**
* Data that needs to be protected includes
  + Datagram passed down from network layer that needs to be sent across the link
  + Link-level addressing information
  + Sequence numbers
  + Other fields in the link frame header

Undetected bit errors – receiver is unaware that received information contains bit errors, the smaller the probability of undetected bit errors, the larger the overhead

Parity Checks

* + Single Parity Bit (simplest)
    - Information sent is D has d bits.
      * In even parity scheme, sender includes one additional bit and chooses its value such that the ottal number of 1s is d+1 bits is even.
      * In odd parity schemes, parity bit value is chosen such that there is an odd number of 1s
    - Receiver only needs to count number of 1s received in the d+1 bits. Knows an error has occurred (more specifically, an odd number of bit errors have occurred) if there is an odd number of 1-valued bits in an even parity scheme
    - Doesn’t work when errors happen in clusters/bursts which could result in 50% undetected errors for single bit parity
  + Two dimensional parity scheme
    - Parity of both column and row containing the flipped bit well be in error
    - Allows receiver to both detect and correct the error using column and row indices
    - Can detect (but can’t correct) any combination of two errors in a packet
* Forward error correction (FEC) – ability of the receiver to both detect and correct errors
  + These techniques are used in audio storage and playback devices
  + Can be used by themselves in network setting or in conjunction with link-layer ARQ techniques
  + Allows for immediate correction of errors at the receiver – avoids round trip propagation delay
* Checksumming Methods
  + D bits of data are treated as sequence of k-bit integers
  + Require relatively little packet overhead
  + Provide weak protection against errors (compared to cyclic redundancy check)
  + One method:
    - Sum k-bit integers and use resulting sum as error-detection bits
    - Internet checksum – bytes of data are treated as 16 bit integers and summed
      * The first complement of the sum forms the internet checksum that is carried in the segment header
      * Receiver checks checksum by taking 1s complement of the sum of the received data (including checksum) and checking whether the result is all 1 bits. If any are 0, an error is indicated
      * In TCP and UDP, internet checksum is computed over all fields
      * In IP, checksum is computed over IP header
* Checksumming used at transport layer, cyclic redundancy check used at link layer
* Cyclic Redundancy Check (CRC)
  + Based on CRC codes aka polynomial codes since it is possible to view the bit string as a polynomial whose coefficients are 0 and 1 with operation on the bit string as polynomial arithmetic
  + Consider d-bit piece of data D. sender and receiver first agree on an r+1 bit pattern known as a generator, G. the most significant (leftmost) bit of G is 1. For D, sender will choose r additional bits, R and append them to D such that d+r bit pattern is exactly divisible by G using modulo-2 arithmetic
  + Receiver divides d+r received bits by G. if remainder is nonzero, there is an error
  + In modulo-2 arithmetic, addition and subtraction are the same, are equivalent to XOR
    - 1011 XOR 0101 = 1110
    - 1001 XOR 1101 = 0100
  + multiplication and division are the same. Multiplication by 2^k left shifts a bit pattern by k places
    - D x 2^r XOR R = d+r bit pattern
    - D x 2^r XOR R = nG
    - R = remainder(D x 2^r)/G
  + CRC standards can detect burst errors of fewer than r+1 bits
  + A burst of length greater than r+1 bits is detected with probability 1-.5^r
  + Each CRC standard can detect any odd number of bit errors
* 6.3 Multiple Access Links and Protocols
* two types of network links
  + point to point link – one sender at one end and one receiver at the other. Examples:
    - point to point protocol (PPP)
    - high-level data link control (HDLC)
  + broadcast link – multiple sending and receiving nodes all connected to same single shared broadcast channel
    - when one node transmits a frame, channel broadcasts the frame and each other node receives a copy
    - examples: Ethernet and wireless LANs
* collide – when more than two nodes transmit frames at the same time, the frames collide at all of the receivers. None of the receiving nodes can make sense of the frames that were transmitted. All frames are lost and broadcast channel is wasted during the collision interval.
* multiple access protocols – how nodes regulate their transmission into shared broadcast channel
  + coordinates transmissions of active nodes (3 types of protocols)
  + ideally, multiple access protocol for broadcast channel of rate R bits per second should have
    - if 1 node has data to send, node has throughput of R bps
    - if M nodes have data to send, each node has throughput of R/M bps. (each node has average transmission rate of R/M not instantaneous rate of R/M)
    - protocol is decentralized
    - protocol is simple, not expensive to implement
  + channel partitioning protocols
    - if channel supports N nodes and transmission rate of channel is R bps, time division multiplexing divides time into time frames. Each time frame is divided into time slots (the link layer frame is also called a packet, is not the time frame). Each time slot is assigned to one of N nodes. When a node has a packet to send, it transmits the packet’s bits during its assigned time slot in the revolving TDM frame. Slot sizes are chosen so that a single packet can be transmitted during a slot time.
      * TDM avoids collisions and is perfectly fair. Each node gets dedicated transmission rate of R/N bps duringe ach frame time
      * TDM has two major drawbacks
        + A node is limited to a average rate of R/N bps even when it is the only node with packets to send
        + A node must always wait for its turn in the transmission sequence even if its the only node with a frame to send
    - FDM divides R bps channel into different frequencies, each with bandwidth R/N and assigns each frequency to one of the N nodes. It creates N smaller channels of R/N bps out of the single, larger R bps channel.
      * avoids collisions and divides bandwidth fairly
      * FDM has a disadvantage in that each node is limited to a bandwidth of R/N even when it’s the only node with packets to send
    - Code Division Multiple Access (CDMA) assigns a different code to each node. Each node uses its unique code to encode the data bits it sends. If codes are chosen carefully, CDMA networks can have different nodes transmit simultaneously, the receivers correctly receive sender’s encoded data bits.
      * Has anti-jamming properties
      * Used a lot in cellular telephony and wireless channels
  + random access protocols – transmitting node always transmits at the full rate of the channel (R bps). When collisions occur, each node involved repeatedly retransmits its frame (packet) until its frame gets through without collision. Node does not instantly retransmit the collided frame, it waits a random delay before retransmitting the frame.
    - Slotted ALOHA protocol – requires all nodes synchronize their transmissions to start at the beginning of a slot
      * Assume: all frames consist of exactly L bits. Time is divided into slots of size L/R seconds (slot equals the time to transmit one frame). Nodes start to transmit frames only at the beginnings of slots. Nodes are synchronized so that each node knows when the slots begin. If two or more frames collide in a slot, all nodes detect the collision event before the slot ends.
      * Let p be a probability. The operation of slotted ALOHA in each node is simple:
        + When the node has a fresh frame to send, it waits until the beginning of the next slot and transmits the entire frame in the slot
        + If there isn’t a collision, the node has successfully transmitted its frame and thus need not consider retransmitting the frame. If there is a collision, the node detects the collision before the en dof the slot. The node retransmits its frame in each subsequent slot with probability p until the frame is transmitted without collision
      * Retransmitting with probability p, we mean that the ode effectively tosses a biased coin; the event heads corresponds to ‘retransmit’ which occurs with probability p. tails corresponds to ‘skip the slot and toss the coin again in next slot’. This occurs with probability 1-p. all nodes involved in the collision toss their coins independently.
      * Advantages: allows a node to transmit continuously at the full rate R when the node is the only active one. is highly decentralized because each node detects collisions and independently decides when to retransmit. Slotted aloha is extremely simple protocol.
      * When there are multiple active nodes, a fraction of the slots will have collisions and will therefore be ‘wasted’. Another fraction of the slots will be empty because all active nodes refrain from transmitting as a result of the probabilistic transmission policy.
      * The only ‘unwasted’ slots will be those in which exactly 1 node transmits – it is called a successful slot
      * Efficiency is defined as the long-run fraction of successful slots in the case where there are a large number of active nodes, each always having a large number of frames to send. (if no form of access control were used, efficiency is 0)
        + Each node attempts to transmit a frame in each slot with probability p (assume each node always has a frame to send). There are N nodes. Th eprobability that a given slot is a successful slot is the probability that one of the nodes transmits and the remaning N-1 nodes do not. The probability that a given node transmits is p; the probability that the remaining nodes do not transmit is (1-p)^(N-1). The probability a given node has a success is **p(1-p)^(N-1).** The probability that any one of the N nodes has a success is **Np(1-p)^(N-1)**
        + To find the maximum efficiency for N active nodes, we have to find the p\* that maximizes this expression. To obtain the max efficiency for a large number of active nodes, we take **the limit of** **Np\*(1-p\*)^(N-1) as N approaches infinity. The max efficiency of the protocol given is 1/e = 0.37.** at best only 37% of slots do useful work when large number of nodes have many frames to transmit. The effective transmission rate of the channel is only 0.37R bps. 37% of slots go empty and 26% have collisions
    - ALOHA – unslotted, fully decentralized protocol. When a frame first arrives, (when a network-layer datagram is passed down from the network layer at the sending node) the node immediately transmits the frame in its entirety into the broadcast channel. If there is a collision, the node will immediately (after completely transmitting its collided frame) retransmit the frame with probability p. otherwise, the node waits for a frame transmission time. After it waits, it transmits the frame with probability p or waits for another frame time with probability 1-p.
  + taking-turns protocols
* **6.4.1 Link-Layer Addressing and ARP**
* Hosts and routers have both link-layer addresses and network-layer addresses.
* Address Resolution Protocol (ARP) – provides a mechanism to translate IP addresses to link-layer addresses
* MAC Addresses (aka LAN addresses or Physical Addresses)
  + Hosts and routers’ adapters have link-layer addresses
  + So, host/router with many network interfaces will have many link-layer addresses associated with it
  + Link-layer switches do NOT have link-layer addresses for their interfaces that connect hosts to routers
  + For most LANs (Ethernet and 802.11 wireless LANs) MAC address is 6 bytes long (2^48 possible MAC addresses) – typically expressed in hexadecimal
  + Assume an adapter’s MAC address is fixed
  + No two adapters have the same address because the IEEE manages MAC address space – a company who manufactures adapters purchases a chunk of address space consisting of 2^24 addresses. IEEE allocates these addresses by fixing the first 24 bits of a MAC address and letting the company create unique combinations for the last 24 bits of each adapter
  + Adapter’s MAC address has flat structure (not hierarchical) and doesn’t change no matter where the adapter goes (like a person’s SSN)
  + In contrast, IP addresses have hierarchal structure (network part vs host part) and host’s IP addresses needs to be changed when the host moves – it changes the network to which it is attached (like a person’s address)
  + When adapter receives a frame, checks to see whether the destination MAC address matches its own. If it matches, adapter extracts enclosed datagram and passes it up the protocol stack. Else, it discards it
  + If sending adapter wants all other adapters on LAN to receive AND process a frame it is about to send, it inserts special MAC *broadcast* *address* into the destination address field of the frame
* Why hosts/routers have both MAC and network-layer addresses
  + If adapters were assigned IP addresses instead of ‘neutral’ MAC addresses, adapters would not easily be able to support other network-layer protocols b/c LANs are designed for arbitrary network-layer protocols not just for IP and internet
  + If there was no MAC address, the network-layer address would have to be stored in the adapter RAM and reconfigured every time the adapter was moved or powered up
  + OR if no addresses are used in adapters, host would be interrupted by every single frame sent on the LAN including frames destined for other hosts
* Three types of addresses: host names for application layer, IP addresses for network layer, MAC addresses for link layer
* Address Resolution Protocol (ARP)
  + Translates between network-layer addresses and MAC addresses
  + To send an IP datagram from one host A to another host B, A must give its adapter the IP datagram and the MAC address for the destination. A will then construct a link-layer frame with the destination’s MAC address and send the frame into the LAN
    - An ARP module in the sending host takes any IP address on the same LAN as input and returns the corresponding MAC address
  + ARP resolves an IP address to a MAC address
  + Analogous to DNS (which resolves host names to IP addresses) but DNS resolves host names for hosts anywhere in the internet while ARP resolves IP addresses only for hosts/router interfaces on the same subnet
  + ARP packet is encapsulated within a link-layer frame and architecturally lies above the link layer. ARP packet has fields containing link layer addresses BUT also contains network-layer addresses. ARP straddles boundary between link and network layers
* ARP table
  + Each host/router has one in its memory
  + Contains mappings of IP addresses to MAC addresses
  + contains a time-to-live (TTL) - indicates when each mapping will be deleted from the table
  + doesn’t contain an entry for every host/router on the subnet
  + typical expiration time is 20 minutes from when an entry is placed in an ARP table
  + if ARP table doesn’t have entry for the destination
    - sender constructs an ARP packet
      * its fields include sending and receiving IP/MAC addresses
    - ARP query and response packets have same format
      * Query packet queries all the other hosts/routers on the subnet to determine the MAC address corresponding to the IP address that is being resolved
  + Query ARP is sent within a broadcast frame but response ARP is sent within standard frame
  + ARP is plug-and-play – ARP table gets built automatically – doesn’t have to be configured by a system admin. If a host becomes disconnected from the subnet, it’s entry is deleted from the other ARP tables in the subnet
* When a host on subnet A wants to send network-layer datagram to router on subnet B
* **3.7.1 (and figure 3.55) Fairness**
* A congestion control mechanism is fair if the average transmission rate of each connection is approximately R/K (for K TCP connections going through a bottleneck link with transmission rate R bps) – each connection gets equal share of the link bandwidth
* 4.3.4
* 6.2.3
* 8.2.2
* 8.3
* 9.5.2 (and figure 9.14 and week 12 extra slides see announcement for link)
* week 12 slides
* 7.2