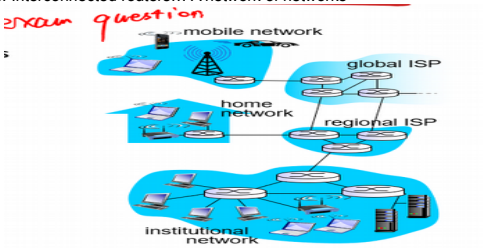
CSC 138
Quiz 1

- Access networks are usually connected with routers inbetween
- The network edge contains computing devices: hosts, mobile devices, etc
- A data center is usually in the network edge
- The access network can be wired or wirelessly connected
- Sac State's network could be an access network
- Packet switching cannot guarantee bandwidth from source to destination
- Packet switching uses only Frequency-Division multiplexing FDM
- Packet switching and circuit switching, one does not always perform better than the other
- In circuit switching, even if circuit segments are idle, others cannot use these segments (TDM)
- Circuit switching accommodates less users than packet switching
- Hosts infected by virus or worms can be used as a botnet to conduct DDoS attacks
- Worms do not involve any user involvement to be infected, such as an email attachment, they slide through networks. Trojans involve items such as downloading a bad email attachment, as they hide within a file secretly. Ransomware takes over your computer's data and tries to ransom the user in order for the user to get their data back. Viruses are basic viruses that are in files, similar to trojans, but less sneaky. Botnet (Bots) is a group of infected computers that are used, usually, for malicious intent; such as using them all to perform network requests to a specific host (aka DDoS attack).
- Packet sniffing involves an item scanning and recording all packets that cross its path, such as the WireShark packet sniffing program… Except that, I hope, isn't being used maliciously
- The major components of the internet consist of computing devices, end systems, communication links, packet switches, routers, and switches.
- The throughput of any end-to end system is the speed of the slowest link
- When a router doesn't have a sufficient buffer size for incoming packets, packet loss occurs
- Queue delay is caused by the packets being transmitted within a router, waiting for transmission
- Transmission delay (L/R) = store-and-forward delay, caused by a data-rate limitation in a network
- Nodal delay is the delay at a single router at the start of the packet being sent, D(Nodal)=D(processing)+D(queue)+D(transmission)+D(propagation)
- Propagation delay is the delay between the two routers divided by propagation speed: (d/s)
- Network Protocol: network protocols define format, order of messages sent and received among network entities, and actions taken on message transmission and receipt
- 5 Layers of the internet protocol stack: Application, Transport, network, (data) link, and physical
- There are 7 layers in ISO/OSI reference model: Presentation and Session
- **Calculating delay… (For 3 routers)**
  - **Total Transmission delay**
    - (L/R)*N
      - L = packet length
      - R = Transmission rate
      - N = how many of THIS exact router setup
  - **Total Signal Propagation Delay**
    - D/S
      - D = delay between communication links
      - S = signal propagation speed
  - **Total END-TO-END delay**
    - **(L/R)*N+D/S+R+Router Delay*(N-1)**
    - N, Only works if L and R are the same for all routers, otherwise individual inputs are needed for each one

Quiz 2

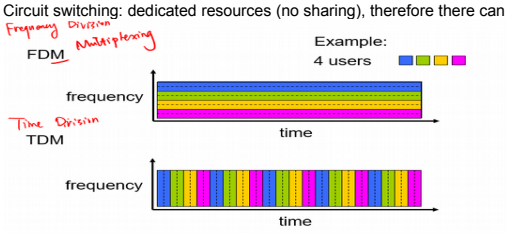
- The DNS for csus.edu is an authoritative DNS
- When you query a website such as test.com it will first contact the local DNS
- Iterated query of DNS name resolution: START -> Local -> Root -> Local -> TLD -> Local -> Authoritative -> Local -> END
- Recursive query: START -> Local -> Root -> TLD -> Authoritative -> TLD -> Root -> Local -> END
- An email server name is a MX DNS record
- A secondary name for a server is a CNAME DNS record
- A DNS server is labeled as NS (Name Server) in the DNS record(s)
- "A" stands for a regular entry in DNS such as any type of server other than MX (Mail Exchange server Record), CNAME (alternate server name entry), and NS (Name Server)
- Client/Server model has a single point of failure, as the server is the single point that must remain always on, as well as have a designated permanent IP, as well as clients not being able to send server data to each other (P2P)
- Packet loss is only acceptable in Real-Time video, as it will translate to missing frames, which will not affect the video as badly as the following, when packets are lost: Emails (It'll have missing data within the email, or be completely corrupt when reassembled), file transfer (File will be corrupted, incomplete), or web documents (If bad data within a site exists, there are many flaws, mainly the site's components will be missing/corrupt)
- For Real-Time video to be effective, throughput should be high
- HTTP is STATELESS, it doesn't maintain data.
- The HEAD method in HTTP is like the GET method, as it requests data without a specific object(s)
- Between the receiver's mail server and the user agent SMTP IS NOT USED
- In P2P, peers requesting data cannot be a seeder (aka ask for data AND send data)
- In DASH the client is intelligent and decides when and how to send data
- DASH a manifest file can be used to provide URLs for different chunks
- In DASH the client usually requests a chunk with the max coding rate based on bandwidth
- In DASH videos are divided into multiple chunks at the server side
- When a third party service is used to distribute the movies for a given site, the next step completed after the first contact of dns.movie.com for a given movie: URL for the movie at CDN.com
- Web caches reduce response time for clients, reduces traffic on an institutions access link, as well as needing to contact original servers if it does not have the requested object
- Increasing the speed of an access link does not ALWAYS outperform installing a local web cache in terms of response time
- In socket programming TCP starts off with 2 sockets created, NOT 1 (Welcome and Connection/Data)
- SOCK_STREAM indicates TCP protocol
- SOCK_DGRAM indicates UDP protocol
- HTTP is stateless
- HTTP keeps session info in the form of cookies
- HTTP sends "set-cookie" as header when identifying cookies in the HTTP message
- The HTTP header used, in addition to the GET message, for a web cache/proxy server to get the most up-to-date information is: "If-modified-since"
- HTTP Response Messages: (THESE ARE NOT ALL OF THEM)
  - 200 OK – successful, varies depending on the HTTP method
  - 301 Moved Permanently – URI has changed, new URI might be given
  - 302 Not Found – URI has changed temporarily
  - 304 Not Modified – Object has not changed from the cached version
  - 400 Bad Request – Server did not understand the request/invalid syntax
  - 401 Unauthorized – Client must authenticate itself before response is given
  - 403 Forbidden – Client does not have access rights, client identity might be unknown
  - 404 Not Found – Webpage/URI is not recognized
  - 405 Method Not Allowed – The specified HTTP method has been disabled
  - 418 I'm a teapot – the server refuses the attempt to brew coffee with a teapot
  - 429 Too Many Requests – Too many requests given/user is being rate limited
  - 451 Unavailable for Legal Reasons – Illegal resource (Ex: Gov. censored webpage)
  - 500 Internal Server Error – Server does not know how to handle said request
  - 501 Not Implemented – HTTP Method is not supported by the server
  - 502 Bad Gateway – Server, acting as a gateway, got an invalid response
  - 503 Service Unavailable – Server is down, maintenance, overloaded, etc.
  - 504 Gateway Timeout – similar to 502, although no response was granted soon enough
  - 505 HTTP Version Not Supported – HTTP Version is not supported
  - 511 Network Authentication Required – Client needs to authenticate itself before it can gain access to the network
- HTTP Methods:
  - GET – Used to retrieve information from the given server using the specific URI
  - HEAD – Same as GET, but transfers the status line and header section only, NO BODY
  - POST – Used to send data to the server, using HTML forms, such as form data
  - PUT – Replaces all current representations of the target resource with uploaded content, AKA saves data given by the client at the server level
  - DELETE – Removes all current representations of the target resource given by a URI, similar to PUT, except for deletions
  - CONNECT – Establishes a tunnel to the server ID'ed by a URI
  - OPTIONS – Describes the communication options for the target resource, finds supported HTTP METHODS that the server can receive and interpret
  - TRACE – Performs a message loop-back test along the path to the target resource, responds with a copy of the TRACE method for debugging purposes
  - URL METHOD?! – Similar to GET method that input is uploaded into the URL line instead of a from as it is done in POST
- All response messages start with HTTP/1.0 OR HTTP/1.1
- All HTTP Methods end with HTTP/1.1 OR HTTP/1.0

Slides for Chapter 1

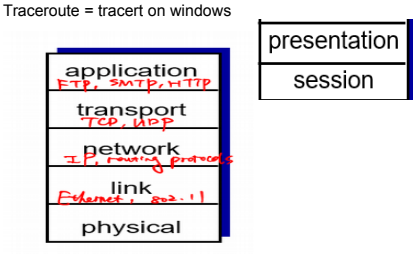
- Hosts = end systems
- Communication links – fiber, copper, radio, satellite.
- Transmission rate = bandwidth
- Packet switches forward packets. The 2 examples: Routers + Switches
- Internet Standards: RFC – Request for comments, IETF – Internet Engineering Task Force
- Network edge: Hosts (Clients + Servers)
- Access networks, physical media: wired + wireless
- Network core: Interconnected routers… A network of networks
  - exam question
  

- Dedicated link vs Shared link: Dedicated = Each network has its own link. Shared = many networks connected to a single link
- FDM – frequency division multiplexing, different channels on different frequencies (Shared Link)
- Access Net: Home, Insitutional, or Mobile
- NAT – Network Address Translation is a method of remapping one IP address space into another by modifying net address info in Internet Protocol datagram packet headers while they are in transit across a traffic routing device
- Guided media: Copper, fiber, coax. Unguided media: radio

- Twisted Pair (TP) is the network cable standard with 2 insulated copper wires
- Terms: Coaxial cable, fiber optic cable, NIC (Network Interface Card), Radio, LAN (Local Area Network), Microwave (Radio link type), WAN (Wide Area Network), Satellite (Radio Link type)
- Packet Switching: Hosts break application-layer messages into packets
  - Forwarding packets router to router, from source to destination, at full link capacity
- Store-and-forward: wait for the entire packet to arrive before forwarding from within the router
- Routing: determines source destination route taken by packets
- Forwarding: moves packets from router's inputs to appropriate router output
- Circuit switching: dedicated resources (no sharing), therefore there can be idle links



- (N^2-N)/2 -> network of networks, how many are connected, when all need to be connected
- Internet Exchange Point: a third-party entity consisting of routers which allow multiple ISP to peer together instead of using a direct link
- A peering link is a direct link between ISP's, without an IXP
- Regional Net = A Regional ISP
- Content Provider Network = Content Distribution Network, such as Google, using their own World-Wide Private TCP IP network of servers to provide content & services to end users
- PoP = Point of presence, a group of one or more routers at the same location in the providers's network where customer ISP's can connect into the provider ISP
- Traceroute = tracert on windows



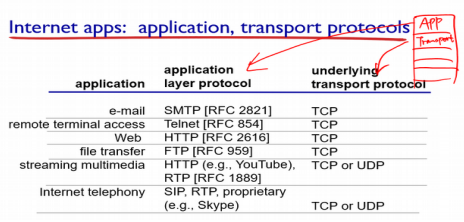
- IP spoofing uses fake addresses to pretend to be the destination, instead steals data between the source and destination, AKA man-in-the-middle attack

Slides for Chapter 2

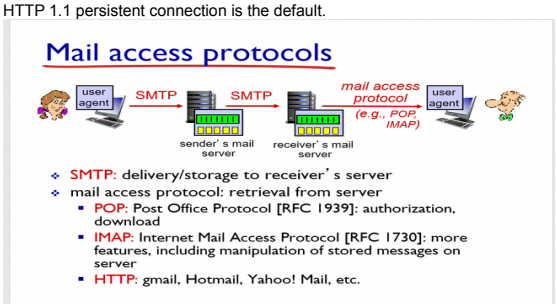
- (Client-Server Architecture) Servers are always-on hosts, with permanent IP addresses, usually in data centers
- (Client-Server Architecture) Clients communicate with servers, maybe be intermittently connected, can have dynamic IP addresses, and no not directly communicate with each other
- P2P = Peer To Peer: NOT always-on, arbitrary end systems communicate with each other, peers connect to peers, self-scalability – new peers bring new service capacity, as well as service demands, peers are intermittently connected and change IP addresses, complex management
- Process: program running within a host
- Within the *same host* two processes communication = inter-process communication
- Transport, network, link, & physical are controlled by the OS
- Application, process, & socket are controlled by the developer
- Application Layer Protocol: types of messages exchanged (Request, response), message syntax (What fields and how fields are delineated), message semantics (Meaning of info in fields), rules (When & How to send msgs), open protocols, proprietary protocols (Skype)
- Reliable data transfer, timing, throughput, or security: Transport service focus/type

application	data loss	throughput	time sensitive
file transfer	no loss	elastic	no
e-mail	no loss	elastic	no
Web documents	no loss	elastic	no
real-time audio/video	loss-tolerant	audio: 5kbps-1Mbps video:10kbps-5Mbps	yes, 100's msec
stored audio/video	loss-tolerant	same as above	yes, few secs
interactive games	loss-tolerant	few kbps up	yes, 100's msec
text messaging	no loss	Elastic	yes and no

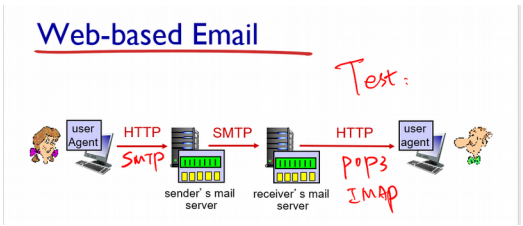
- TCP: reliable transport, flow control, congestion control. Does not provide timing, throughput, security. Connection-Oriented: Setup required between client and server
- UDP: Unreliable data transfer. Does not provide: Reliability, flow control, congestion control, timing, throughput, security, or connection setup. Saves time due to no connection setup, faster, header is smaller then TCP



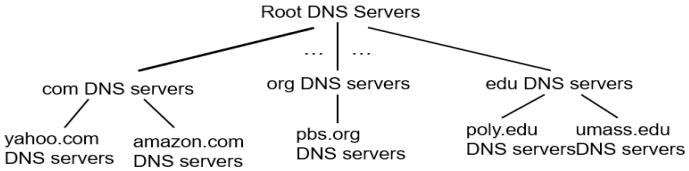
-
- SSL: Secure Socket Layer, APPLICATION LAYER
- Non-persistent HTTP vs Persistent HTTP: Non -> one object at a time over TCP, connection then closed, downloading multiple objects requires multiple connections. Persistent -> Multiple objects can be sent over single TCP connection between client and server
- RRT: Round-Trip-Time, time between request and response
- Non-Persistent HTTP: 2RTTs per object, OS overhead for each TCP connection, browsers often open parallel TCP connections
- Persistent HTTP: Server leaves connection open after sending response, subsequent HTTP messages between same client/server, client sends requests as soon as it encounters a referenced object, as little as ONE RTT for all referenced objects
- KeepAlive means persistent connection. This is used in HTTP1.0 as an option. In HTTP 1.1 persistent connection is the default.



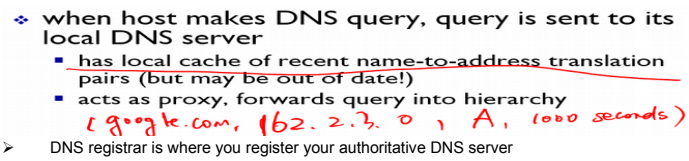
-



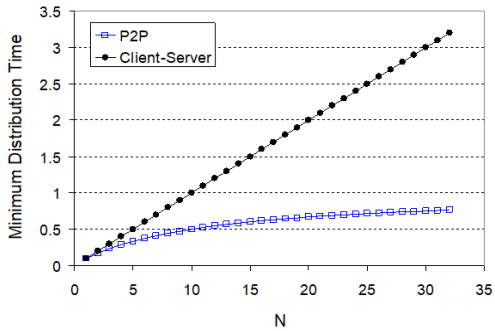
-
- DNS: Domain Name System
-



- TLD servers: responsible for .com, .org, .net, etc… domains
- Authoritative DNS server: organizations OWN DNS server(s)
- Local DNS: Does NOT belong to hierarchy, each ISP, residential, company, university has one.
-



- DNS registrar is where you register your authoritative DNS server
  - (networkutopia.cock, dns1.networkutopia.cock, NS)
  - (dns1.networkutopia.cock, 212.212.212.1, A)
- DNS Poisoning sends bogus replies to DNS server which it then caches



-
- CBR: Constant Bit Rate… VBR: Variable bit rate