Class Notes:

8/15/18: Encapsulation, 5 Layer networking model

* Encapsulation: adding headers as we move down the stack
* De-encapsulation: removing those headers as we move up the stack

Chapter 2: Application Layer –

* Simple: network apps exchange messages
* Socket: source IP, dest IP, sending port ID, dest port ID
* Local machine (OS) assigns source port number
* API: Application Program Interface (process uses API)
* UDP: User Datagram Protocol
  + “unreliable”
  + A lot less overhead
* URL: Uniform Resource Locator – three things (hostname/path/filename)
* RTT = round trip time (client to server to client)
  + Total = 2\*RTT + file transmit time

HTTP:

* Cookie: opaque piece of data
  + If there is no cookie on the computer, then one is created (in a local folder) with an identification code. This code is then sent to the server with a HTTP message and then the server access its backend database to show to the client the data stored in the cookie on the server side (shopping cart, recently viewed items, etc.)

FTP:

* Port 21
* Active AND passive modes (this is important)
* Two connections: control and data (control is out-of-band)
* Tear down and reestablish connections frequently (for each new connection)
* Foot stomp!

Firewall:

* Should block all incoming connections

SMTP:

* Port 25
* Messages must be in 7-bit ASCII

Push/Pull:

* HTTP: pull
* SMTP: push only

Multipurpose Internet Mail Extensions (MIME)

Base 64:

* How we encode characters to send via email along with attachments
* Need to have an index table (this is not encryption)
* Strings probably end in “=” or “==” (pad to account for extra digits when you encode)

POP/IMAP/HTTP: Used to retrieve email from server to client

* POP3
  + Port 110
  + Sent in plaintext
  + Cannot read email if deleted from server
  + Stateless
* IMAP:
  + Stateful – remembers folders

DNS: Domain Name Service (distribute database)

* 13 root servers around the world (global phenomenon)
* Foot Stomp: (3 level’s names) Root, Top-level Domain, Authoritative
* Foot Stomp: example of how DNS works
  + Recursive versus iterative
* Flush dns after making any changes to the network
* Port 53

ICANN:

* Manage DNS root servers
* Governing body for the internet

Client/Server Socket Interaction: UDP

UDP = User Datagram Protocol

Socket Programming with TCP:

* Uses handshake between welcoming socket, client socket, and connection socket

Multiplexing:

Process = ports

Host = IP

UDP: Port 88

Web servers will have a different socket for each TCP connection (this is for both persistent and non-persistent HTTP connections)

Reliable Data Transfer with TCP:

* ACKs help us recover from errors
* Stop-and-Wait Operation/Performance is going to be on EXAM #2
* Useful Work = Time it takes to transmit data onto the wire (transmission delay)
* Dropped packets are wasted time (not useful work)
* 1460 = MSS for TCP/IP ethernet packets
* ACK = “ASK” (slide 61 – middle request from host B to host A)
* ACK Flag tells the receiver that the acknowledgement number means something (significant).
* WINCAP, NCAP (NCAP might be better/best)?

TCP Reliable Data Transfer:

* TEST: just remember if you are above the threshold or below the threshold (TCP slow start and congestion control)
* Use TCP Reno for HW and test
* Events that drop us down: timeout or 3 duplicate ACKs
  + 3 Duplicate ACKs (window and threshold drop to half) means we are still receiving data (drop rate in half)
  + Timeout (drop to 1) – something is really wrong.
* TEST: understand behavior on slide 93 (dropping, raising, linear, exponential)
* Stephens Graph: need to create this for the lab

Network Layer:

* Control Pane & Data Plane:
  + Routing Algorithm is created and controlled in the control plane of the network
  + Data Plane just decides what outbound interface the packet should be sent on (depending on destination IP address).
* SDN:
  + Remote controller interacts with local control agents
  + Control agents are within each router
  + Uses OpenFlow (FOOT STOMP) protocol for RC to communicate with CA
* TEST: Need to study slides 11 & 12
* TEST: make sure that you match the longest first. It will check every entry in the table

IP:

* TEST: understand what each one of the fields does in an IP header
* TEST: only a ROUTER decrements the TTL number in the header
* Fragmented packets are ONLY reassembled at the destination host
* A switch does not have an IP address
* Take the router out and you can make a subnet with each of the outgoing connections on the router
* TEST: need to know which IP addresses can be added to what subnet.
* CIDR: Classless InterDomain Routing
  + Address format: a.b.c.d/x
  + X is the prefix
* DHCP (on the TEST):
  + Provides: Subnet mask, default gw address, DNS server name and address
  + Always broadcast
  + Ports: 68 (client broadcasts server to this port), 67 (DHCP server broadcasts to this port on the client)
* NAT (on the TEST):
  + NAT is a security enhancement
  + We can put port forwarding on a router to enable web servers inside of a NAT (obscured) network. Example: can use a web server inside of a subnet even though there is only one public IP address for the entire subnet.
* IPv6 “Flow”: Is just all the headers

Routing Algorithm Classification:

* Link State
  + Forwards neighbor information to everyone on the network (foot stomp)
  + Make sure you actually build the forwarding table
  + Dijkstra’s Algorithm
  + Foot Stomp: slide 15, building forwarding table
  + Will be a routing problem on the exam
* Distance-Vector Algorithms
  + Decentralized
  + Routing table only sent to neighbors
  + Bellman-Ford Equation

Autonomous System (AS) Routing:

* IGP (Interior Gateway Protocols) is the same as Intra-AS Routing
  + OSPF
    - Set links to whatever you want
    - Added security
    - KNOW: Hierarchical setup makes the network more manageable
  + RIP
  + IGRP
* BGP (Border Gateway Protocol) is the same as Inter-AS Routing
  + Advertisement: the path (AS4, AS3, AS1), and then the next hop (which is the IP address of the router that sent the information.
  + Policy is going to trump the technical “best path” more than we think.
* Intra-AS depends on performance
* Inter-AS depends on policy

\*\*Routers have physical, data link, and network layer only (not transport).

Data Link Layer:

* Packets are now called frames
* KNOW: layers
* Ethernet: does not provide reliable data transfer
* Frame: adds header and trailer (frames the data, transport, and IP information)
* A Frame can detect and CORRECT errors
* Semi-Autonomous: physical device (ethernet network adapter) checks frames for its hard-coded MAC address
* CRC is what everyone uses (can find and fix most errors)

MAC Protocols:

* Channel Partitioning (TDMA, FDMA, chipping code)
* Taking Turns
* Random Access

TDMA: Time Division Multiple Access

Slotted Aloha: Answers: 1/n and 1/e

EXAM: Broadcast and then unicast (ARP networking)

Ethernet:

\*Never collisions in networks with a switch

Only protocol with a minimum data value (must be 46 or more bytes)

t + (Tau-1) + Tau is about t+2Tau

Maximum length between nodes is 2500 meters (thicknet)

100 meters for ethernet – between host and switch (between active devices)

TEST: Framing PPP data frame. Framed with “7E”

Need to escape 00-1F, 7D, and 7E with an escape character (7D)

Test - BSSID: MAC address of the wireless access point (the wireless interface)