Taylor Earl

* Security
  + Symmetric
    - The key is used to both encrypt and decrypt
    - Need to have somewhere to share the key
  + Asymmetric
    - One key to encrypt and one key to decrypt
    - (Public - private Key encryption)
      * Public - You can share with anyone. Made free.
      * Private - Keep that locked down. Nobody can see it
    - Slower, takes more work, complex
    - Use this to share a symmetric key
* Public / Private Key
* DCHP (Dynamic Host Configuration Protocol)
  + Transport Layer
  + UDP Protocol (typically)
  + Port -
    - Server - 67
    - Client - 68
    - Why
      * The server might respond back with a broadcast. So we don’t want to mess up someone listening on a certain port
  + Assigning IP address
  + Need to know default router
  + Subnet mask
  + DNS Server
* DNS (Domain Name Service)
  + Translate a domain name into a ip address
  + UDP
  + Server
  + Port 53
  + TLD’s
    - COM
      * Google
      * Yahoo
    - EDU
      * Weber
        + cs

Icarus

* + - GOV
      * USDA
  + Secondary can only COPY from the primary
* Telnet
  + Process
    - IAC
      * Interpert as control
    - Could be
      * WILL
        + response do or don’t
      * WON'T
      * DO
        + response a will or wont
      * DON’T
    - ECHO
* Socket
  + Sock\_stream
    - TCP (Stream oriented)
  + Sock\_DGRAM
    - UDP (sends datagram)
* Ports
  + Telnet - 23
  + SSH - 22
  + FTP - 21 Server
  + FTP - 20 Data
  + HTTP - 80
  + SMTP - 25
  + SSL - 443
* Review
  + Subnetting
* Routing Table
  + Classful Routing
    - 3 tables
  + Classless Routing
    - 1 table
    - Longest mask first
* RIP Timers
  + 1 - Periodic timer per router
    - Every 30 seconds send out request for routes
  + 1 - Expiration timer per route
    - 180 seconds
  + 1 - Garbage collection timers per expired route
    - Keeps around in case it comes back, or tells everyone else it’s not a valid route
    - 120 seconds
  + 20 routes
  + 4 routes no info
    - lasts 200 seconds
  + 2 routes no info
    - lasts 500 seconds
* Multicasting
* OSI model
* Final Study Guide
* Application Layer Intro
  + Sockets API
    - socket
    - bind
    - listen
    - accept
    - connect
    - send
    - recv
    - sendto
    - recvfrom
    - sendall
    - shutdown
    - close
    - SOCK\_STREAM
    - SOCK\_DGRAM
  + Concurrency
    - Many things on the same socket
* DHCP
  + What is it
    - Dynamic Host Configuration Protocol
  + Which transport layer protocol
    - UDP
  + Which port(s)Same network vs different network communication
  + Why does the client explicitly bind a port
    - Port -
      * Server - 67
      * Client - 68
      * Why
        + The server might respond back with a broadcast. So we don’t want to mess up someone listening on a certain port
* DNS
  + What is it
    - Domain Name Service
  + Which transport layer protocol
    - UDP
  + Which port
    - Port 53
  + Benefits of hierarchical namespace
    - You can go from generic to specific. Allows it to be set up per need of the group.
  + Domains and Zones
    - A zone is a portion of a domain. The domain is the authoritative figure
  + Root Server, Primary Server and Secondary Servers
    - Root is the highest up. That passes onto a list of Primary Servers. Secondary can only copy from the primary.
  + Inverse, Generic, and Country Domains
    - Generic
      * .com
      * .edu
      * .gov
    - Country
      * .us
      * .ca
      * .jp
    - Inverse
      * Map an address to the domain
* TELNET
  + What is it
    - Text oriented communication
  + Which transport layer protocol
    - TCP
  + Which port
    - 23
  + Security
    - Not secure. Plain text used. No encryption
  + NVT ASCII
    - Network Virtual Terminal that uses ASCII
  + Control Characters
    - IAC
      * Interpret as control
  + WILL WONT DO DON'T
    - Could be
      * WILL
        + response do or don’t
      * WON'T
      * DO
        + response a will or wont
      * DON’T
* SSH
  + What is it
    - Allows you to securely perform network tasks over unprotected internet
  + Which transport layer protocol
    - TCP
  + Which port
    - 22
  + Security Tunnelling
    - Allows you to do normal things securely. Point user machine to a port on another computer that’s pointing to a local port
* FTP
  + What is it
    - File Transfer Protocol
  + Which transport layer protocol
    - TCPl
  + Which port(s)
    - FTP - 21 Server
    - FTP - 20 Data
  + Control Channel
    - One of two channels. Handles the commands and short responses
  + Data Channel
    - Transfers data. Reestablished for every connection
  + PASV
    - Ensures that all data comes from inside and none gets transferred outside
  + Security
    - Hard to secure. If you try to do it with SSH it will only protect the control channel
* TFPT
  + What is it
    - Trivial File Transfer Protocol
  + Which transport layer protocol
    - UDP
  + Which port
    - 69
  + Comparison to FTP
    - TFTP is a VERY barebones version of FTP. Less work and maintenance. No user authentication
* HTTP
  + What is it
    - Hyper Text Transfer Protocol
  + Which transport layer protocol
    - Mostly TCP
  + Which port
    - 80
  + URLStatic vs. Dynamic
    - Static URLs point to a specific hosted file, where dynamic URLs let a database on the server side handle what to show you
  + Active
    - Server sends a copy of the script to be processed on the user end
  + Request/Response Format
    - Requests using a header
  + Data delimiter
    - Used to separate values in first line
  + Persistence vs Non-Persistence
    - Persistence uses one connection
    - Non-persistence uses a new tcp connection every time
* SMTP, POP, IMAP
  + What are they used for
    - Different mail servers
  + Which transport layer protocol
    - TCP
  + Which port
    - SMTP
      * 25
    - POP
      * 110
    - IAMP
      * 143
* Security
  + CIA
  + Symmetric-key encrption (shared-key)
    - How it protects CIA
  + Assymetric-key encryption (public/private-key)
    - How it protects CIA
  + Which key is used when
  + Who has which key
  + Certificate Authorities
* OSI Model
  + Application, Presentation, Session, Transport, Network, Data Link, Physical
  + Network Routes packets between networks
* SUBNETTING
* IPV6
  + More addresses, better header, no broadcast, "future proof", backwards compatible.
* Why don’t we use CMSA/CD with 10gb ethernet?
  + 10G Ethernet works only in full-duplex mode and does not support CSMA/CD, the common Ethernet collision method used to gain access to the physical medium.
* RIP
  + Message oriented?
* ARP
  + But it was like if comp a sends arp request to comp b who sees it type of deal
  + Unicast or broadcast?
  + Message oriented?
* Classful addresses
  + a
  + b
  + c
  + d
* Why does an ATM network have to use ATMARP instead of just ARP?