## 

|  |  |
| --- | --- |
| OSI Model  * **7. Application Layer**   + What is needed to make application ‘network aware’ * **6. Presentation**   + Used to convert data in a format that computer can read * **5. Session**   + The connection between two systems * **4. Transport**   + Disassembles data into packets to be sent across network   + Ensures data is recombined in correct manner * **3.Network**   + Logical Addresses   + IP addresses   + Routers * **2. Data link**   + Anything that works with a MAC address   + Network Cards   + Switches * **1. Physical**   + Cables | TCP/IP Model  * **4. Application**   + Application, Presentation, Session layer of OSI Model   + Anything that has to do with the application itself   + Email, FTP, Telnet, SSH... * **3. Transport (& session kinda)**   + Assembly/Disassembly   + TCP/UDP   + Whatever it takes to get from one application to the next * **2. Internet**   + IP Addresses     - Routers * **1. Network Interface (Link Layer)**   + Physical Cabling   + Network Cards   + MAC Address   + Data Link and Physical of OSI Model (anything that has to do with hardware) |

## Network Interface Card (NIC) (Layer 2 Data Link)

|  |  |
| --- | --- |
| Frame  * 1500bytes * Recipient MAC address - Sender’s MAC address - Type - Data - FCS   + FCS - 4-bytes long * Process   + NIC takes the payload   + adds the FCS,   + Adds Dest MAC and Source MAC -   + Then sends frame through cable to a hub/switch in the network     - The switch sends ***Unicast*** frames to the destination address     - The switch sends ***Broadcast*** frames to every system on the network | MAC Address  * 48-bit hexadecimal   + First 6 are NIC manufacturer OUI (Organizationally Unique Identifier) * Physical address of NIC * Unique ID across all network devices  Unicast vs. Broadcast  * **Unicast**   + Frames forwarded to specific MAC address * **Broadcast**   + Frames forwarded to all devices in the broadcast domain   + FF-FF-FF-FF-FF-FF |

## IP Addressing (Layer 3 Network Layer)

* Logical Addressing protocol for TCP/IP
* Makes sure that a piece of data gets to where it needs to go
* Unique identifier for each device on the network

### Routers

* Routers use IP addresses to forward packets where they need to go
* Connects multiple local area networks (LANs)
* Uses a routing table

## 

|  |  |
| --- | --- |
| Transport Layer (Layer 4)  * Transport protocol breaks up data into segments or datagrams   + Gives each segment a sequence number * **Transmission Control Protocol (TCP)**   + Connection Oriented * **User Datagram Protocol (UDP)**   + Connectionless   + Datagrams dont use sequence numbers |  |

Ports

* Unique to applications used on the internet
* First 1024 are ‘well known ports’

## Network Topologies

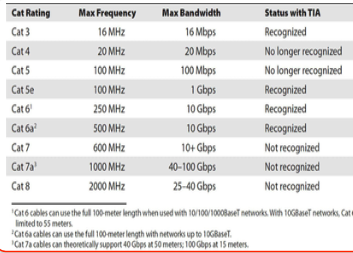
* **Bus**
  + Network all on one line
* **Ring**
* **Star**
  + Physical topology
* **Star-Bus**
  + Hybrid
  + Primary topology used today
* **Mesh**
  + Everyone connects to everyone
* **Physical vs. Logical**

## Cabling

### Coaxial

* **RG-58**
  + 50ohms
  + Networking
  + BNC
  + Old type
* **RG-59**
  + 75ohms
  + ~~CableTV, Cable Modems~~ Analog Video, CCTV
  + F Type
  + Short distance runs
* **RG-6**
  + 75ohms
  + CableTV, Cable Modems
  + F Type
  + Most common used today
  + Thicker, longer distance runs

### Twisted Pair

* Shielded
* Unshielded
* Connectors
  + RJ-45
  + RJ-11
* EIA/TIA 568A
* EIA/TIA 568B
  + Modern standard
* Solid Core vs Stranded Core
* Modern has 4 pairs
* CAT Ratings
  + 

### Fiber Optic

* Multimode
  + LED signals
  + Orange
  + Shorter distances
* Single mode
  + Lasers
  + Yellow
  + Longer distances
* Duplex
  + Two connectors
* Connectors
  + ST
    - BNC Type
    - Old - Duplex
  + SC
    - Square
    - Old - Duplex
  + FC
    - Screws in (threaded)
    - Old - Duplex
  + LC
  + MT-RJ
* Polishing
  + PC (Physical Contact)
    - Flat but rounded
  + UPC (Ultra Physical Contact)
    - Rounded
  + APC (Angled Physical Contact)
    - At an angle
  + Use UPC or APC for better quality

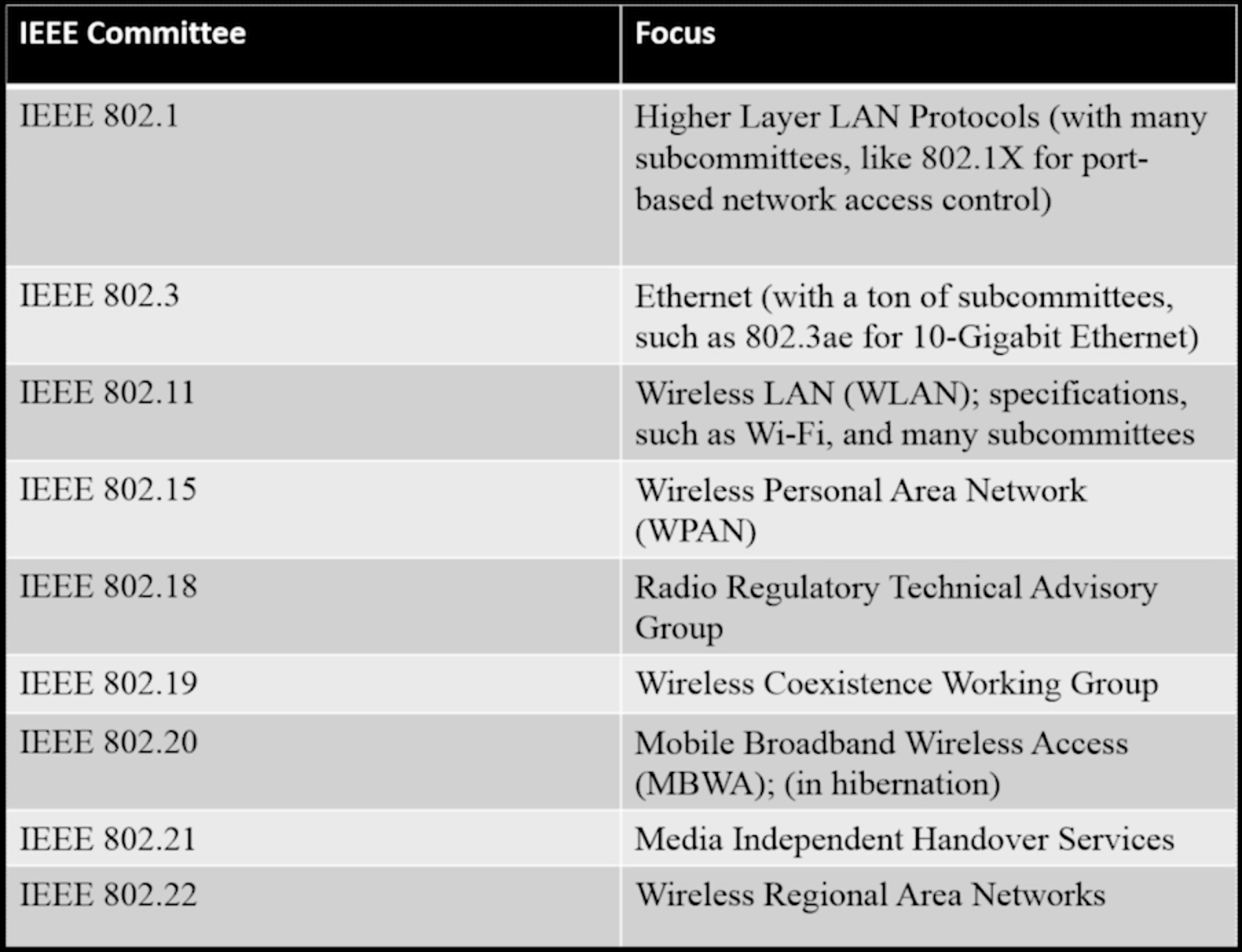
### Fire Rating

* Plenum Rating
  + Highest rating
* Riser
  + Between floors
* PVC - (non plenum rated)
  + No rating

### Legacy Network Connections

* Serial
  + RS-232
  + DB-Type
    - DB-25
    - DB-9
* Parallel ports
  + IEEE 1284

### IEEE

* Defines industry-wide standards that promote the use and implementation of networking technology
* 

## Ethernet 802.3

* Nomenclature
* (10Base5, 1000Base…)
* Speed in mb/s
* Base/Broad
  + Base = 1 Channel
  + Broad = multichannels
* Length of cable
  + 10BaseT is most common

### Ethernet Frames

* *1500Bytes long*
* Preamble
  + Alternating 1’s and 0’s
* Destination MAC
* Source MAC
* Data/Ether Type
  + What kind of data
* DATA
  + 64 byte/octet minimum
    - Pad Fills up the rest of the data
  + 1522 bytes/octets maximum
  + Jumbo Frame
    - 9000bytes
    - Very high speed networks
  + MTU (Maximum Transmission Unit)
* FCS (Frame Check Sequence)
  + 32 bit
  + Used for Error Protection

|  |  |
| --- | --- |
| Ethernet Basics**10Base5**  * Drop cable * Uses BNC Connector? * Requires Terminating Resistor * Not used anymore * **10Base2**   + Use BNC T-Connector   + Requires Terminating Resistor   + Can support up to 30 clients. * **10BaseT**   + Old   + 10Mbps   + 100M   + 1024 nodes   + Star-bus: physical star, logical bus   + Cat 3 or better UTP cabling with RJ-45 * **10BaseFL**   + 10Mbps   + 2000m   + 1024 node limit.   + Star-bus: Physical star, logical bus   + Multimode fiber-optic cabling     - ST or SC connectors. * **CSMA/CD**   + Carrier Sense Multiple Access/Collision Detection   + Listen on the wire   + Uses random numbers to see who goes first when collision detected   + Old/no longer needed thanks to full duplexing * **Hubs**   + Essentially a repeater     - Sends frames out to all devices   + Switches replace hubs * **Switches**   + Replaces hubs   + Switches forward frames based on MAC address     - By Making a MAC address table   + Use Crossover cables (unless have auto-sensing ports) * **Terminating Twisted Pair**   + Crossover     - Have different ends     - Connects switches     - Suitable for direct link between two computers   + Straight Through (Patch Cable)     - Identical ends     - Suitable for connecting workstations to network devices   + 568A or 568B | Modern Ethernet  * **100BaseT**   + 100BaseT4     - Cat3   + 100BaseTX     - Cat5 and Cat5e     - Became 100BaseT standard   + 100Mbps   + 100Meters   + 1024 Node limit   + Cat5 or better   + RJ-45   + Saw the switch from hubs to switches and half-duplex to full-duplex * **100BaseFX**   + 100Mbps   + 2km   + 1024 node limit   + Star-bus: Physical star, logical bus.   + Multimode fiber with ST or SC connectors * **Gigabit Ethernet (1000BaseT/X)**   + **1000BaseT (802.3ab)**     - 1000BaseCX       * Twinax coaxial cable         + 25 meter     - Cat5e/6 UTP       * Cat6 is most common     - RJ - 45     - 100m   + **1000BaseX (802.3z)**     - 1000BaseSX       * Multimode       * 850nm       * LC common       * 220-250m     - 1000BaseLX       * Single mode       * 1300nm       * LC and SC       * 5km * **10 Gigabit Ethernet**    + **10GBaseT**     - Cat6 - 55m     - Cat6a - 100m   + **Fiber**     - 10GBaseSR       * Multimode       * 850nm       * LAN       * 26-400m     - 10GBaseSW       * Multimode       * 850nm       * SONET/WAN       * 26-400m     - 10GBaseLR       * Single mode       * 1310nm       * LAN       * 10km     - 10GBaseLW       * Single mode       * 1310 SONET/WAN       * 10km     - 10GBaseER       * Single Mode       * 1550 nm       * LAN       * 40km     - 10GBaseEW       * Single mode       * 1550 nm       * SONET/WAN       * 40km     - Connectors       * SFP, SFP+         + Small form factor transceivers * Spanning Tree Protocol   + Solves looping issues. |

## 7. TCP/IP Basics

### Converting IP Addressing and binary

* + Remember 128.

### Address Resolution Protocol (ARP)

* + Sends out a broadcast address searching for the MAC address matched to the IP
  + Used when a computer knows the IP address but needs the MAC address
  + arp -a
    - ARP cache

### Classful Addressing (subnetting)

* + Internet Assigned Numbers Authority (IANA)
    - In charge of handing out IP addresses on the internet.
    - Breaks up chunks of IP addresses and hands them to the Regional Internet Registry (RIR)
      * RIR breaks up chunks and hands them to ISP’s
  + Class A
    - 255.0.0.0
  + Class B
    - 255.255.0.0
  + Class C
    - 255.255.255.0

### Classless Addressing (Subnet Masks)

* + Subnet masks splits up the IP address into Network portion and Host portion.
  + **Network ID**
    - Network ID is the 1’s portion
    - Cannot change.
  + **Host ID**
    - Host ID is the rest 0’s
    - Cannot use 0 or 255 in the host address.
    - Host uses subnet mask to determine if the destination is local or a remote network.
      * Traffic destined for outside of the local network is sent to the default gateway router.
  + **CIDR** (Classless Inter-Domain Routing) Subnetting
    - Subnet masks have all 1’s on the left and all 0’s on the right
    - The more subnets you have the fewer the hosts that are available.
    - **Calculating # of hosts using CIDR**
      * 2^(# of 0 or host bits) - 2

### Dynamic/Static IP addressing.

#### **Dynamic Host Configuration Protocol (DHCP)(*BOOTP on linux*)**

* + - Automatically assigns IP addresses from available pool.
    - Computer must be a DHCP client of the DHCP server
    - DHCP Server must be on the networks broadcast domain
      * Can use your router to create a DHCP Relay which allows a DHCP Server outside of the broadcast domain
      * And each broadcast domain must have only one DHCP Server
    - **DHCP Discover**
      * Performed when your computer is first booted up.
      * Sends out a Broadcast Address on the MAC address of all f’s (ff:ff:ff:ff:ff:ff)
      * DHCP server responds to this broadcast
    - **DHCP Offer**
      * DHCP Server receives Broadcast address of all f’s
      * Responds with a Unicast address called the **DHCP Offer**
    - **DHCP Request**
      * Client receives the DHCP Offer and accepts (rejects?) the offer
      * Sends out DHCP Request back to DHCP Server.
    - **DHCP Acknowledge**
      * DHCP Server stores this information and keeps traffic of clients using DHCP
  + DHCP Troubleshooting
    - Check if you have it setup correctly
      * Does it have a pool of IP Addresses
      * Is the IP Address correct etc…
    - Usually a bad server when you can connect to network devices like printers but cannot access the Internet…
    - Rogue Server
      * If you ever get an IP address other than your correct network ID...
    - If you are connected to a DHCP server and still get an APIPA address, make sure its working.

## Special IP Addresses

* + **Private Networks**
    - 10.x.x.x
    - 172.16.x.x - 172.31.x.x
    - 192.168.x.x
    - Used on internal networks not meant to be shared on the public internet
      * NAT Device provides a barrier (hides) from the Internet
  + **Loopback**
    - IPv4 - 127.x.x.x
    - IPv6 ::1
    - Used to ping yourself
    - Use with Loopback Device
  + **APIPA**
    - 169.254.x.x
    - Used when DHCP server is unavailable/down.
    - Can only be used locally.

## IP Scenarios

* + Duplicate IP Addresses
    - Is statistically possible.
    - Router doesnt know which computer to forward packets to.
  + Duplicate MAC Addresses
    - Happens with virtual machines
    - Cant connect to anything on the network.
  + Incorrect Gateway
    - Cant connect outside of your local network (cant access internet)
    - Man in the Middle attacks with rogue device
  + Incorrect Subnet Mask
    - Every computer on the local network (broadcast domain) must have the same Subnet Mask
    - Have two terminals ping each other.
      * When one can reach the other but the other person cannot, its a misconfigured Subnet Mask
  + Expired IP Address
    - DHCP server dies and unable to renew the DHCP Lease.
    - May also have APIPA address.
    - Check your DHCP server

## 8. Routing

### Routers

* + Filter and forward packets based on IP address.
    - *(Switches filter and forward packets based on MAC address)*
  + Routing Table
    - Address
    - Subnet
    - Gateway
    - Interface
    - Metric
  + Default Route
    - 0.0.0.0
    - Send to default route if no other destinations available
    - ARP’s the gateway to seek MAC address of destination
  + Gateway Routers
  + Not tied to ethernet
  + Routers only care where a packet is headed

### Ports

* + TCP packets have **Destination Port** and **Source Port**
    - **Destination Port**
      * Determines what type of service the packet is going to
        + i.e. 80, 443, 21, etc
    - **Source Port**
      * Incremental number Generated as an Ephemeral port by the computer.
      * A number well past 1024 up to 65535 depending on OS
  + 0-1023 ports are called well-known ports

### Network Address Translation/Port Address Translation (NAT/PAT)

* + PAT translates internal IP addresses to an internet address and tracks the packets
  + **Static NAT (Port Forwarding)**
    - Sends specific traffic to one internal IP address
    - *\*Someone can hack you if they know your internal IP address*
  + **Dynamic NAT (Pooled NAT)**
    - DNAT has a limited pool of internet addresses to give to a number of internal devices
* Port Forwarding:
  + Allows external devices to have internal communication through a router
  + Port triggering will open an alternative assigned port when the initial port is contacted (e.g. FTP)

### Demilitarized Zone (DMZ)

* + A spot on your network you allow access from the public
    - Webserver etc
  + Enabling DMZ when setting up port forwarding places that device outside the protection of that router.

### Static Routing

* + Routing Tables

## TCP/IP

* Ethernet frames are used by switches and routers
* TCP (Network 3 Layer)
  + Connection-oriented
    - Uses a 3-way handshake process
    - Syn, Syn-ack, Ack
* UDP
  + Connectionless-oriented
  + Low-overhead with one-way communication.
* ICMP (Layer 2 Internet)
  + (Ping)
* IGMP (Layer 2 Internet)
  + Provides multicasting support
    - Multicast addresses start with 224

Web Servers

* HTTP:
  + Port 80
  + Microsoft IIS
  + Apache (Open Source)
  + Netstat -a if web server running
* HTTPS:
  + Port 443
* FTP
  + Listens for commands on TCP:20
  + Responds with data on TCP:21
  + SFTP
    - Secure FTP
    - Uses TLS and SSL
  + TFTP
* Email
* Sending
  + SMTP (Simple Mail Transfer Protocol)
    - TCP:25
* Receiving
* POP3
  + TCP:110
  + Older
* IMAP4
  + TCP 143
* STARTTLS: 587
* STLS
  + Current approach to running secure email protocols.
* Remote Login
  + Telnet
    - Maybe oldest program on the internet.
    - Needs a telnet client and telnet server
    - Has login but unsecure (in the clear)
  + SSH
    - Secure Shell
    - Needs an ssh client and ssh server
    - Encrypted
* NTP
  + Network Time Protocol
  + Port 123

### Network Naming

* DNS
  + Domain Name Server
  + Associates IP addresses with text domain name.
  + Troubleshooting:

### Securing TCP/IP

* Encryption
* Cleartext is any unencrypted data
* Algorithms use keys to encrypt cleartext into ciphertext.
* Symmetric Encryption
  + Uses the same key to encrypt and decrypt.
* Asymmetric Encryption
  + Uses a public key / private key to encrypt/decrypt ciphertext
  + Public keys encrypt
  + Private keys decrypt
* Cryptographic Hashes
  + Used for verifying data, not for encryption
  + Hash values are always fixed size
  + Common Hashes
    - MD5
    - SHA-1
    - SHA-2
* Identification/Authentication/Authorization
  + Authentication requires sharing of something you know, something you have or something you do
  + Federated system trust is inherited from a different trusted system.
  + Authorization
    - What can you do now that you have been authenticated
    - Access Control List
      * Mandatory Access Control (MAC)
        + Uses labels
      * Discretionary Access Control (DAC)
        + Gives creators control over permissions
      * Role-based Access Control (RBAC)
        + Uses groups
  + RADIUS
    - A RADIUS client is an intermediary agent between a RADIUS supplicant and a RADIUS server
    - A RADIUS database of authenticated users and passwords may reside outside the RADIUS server.
    - Uses UDP Ports 1812-1813
      * Or uses UDP ports 1645-1646.
    - TACACS+ uses TCP port 49
  + PPP
  + Kerberos
    - Windows proprietary service
    - Authentication authorization for wired networks
    - Key Distribution Center (KDC)
      * Authentication Service (AS)
      * Ticket-granting Service (TGS)
      * Ticket Granting Ticket
        + Timestamped by client and sent to TGS
        + TGT Issues tokens based on timestamp
    - Relies heavily on timestamps
  + EAP
    - EAP enables flexible authentication
    - Used to connect to wireless networks
    - EAP-PSK
      * Everyone uses a pre-shared key
  + Protected Extensible Authentication Protocol (PEAP)
    - * Has username/password login
    - EAP-MD5
      * Uses a hash
    - EAP-TLS(TTLS)
      * Uses certificates
  + Single Sign-on
    - Windows Active Directory (Most common)
    - Used in LANs primarily
    - Security Assertion Markup Language (SAML)