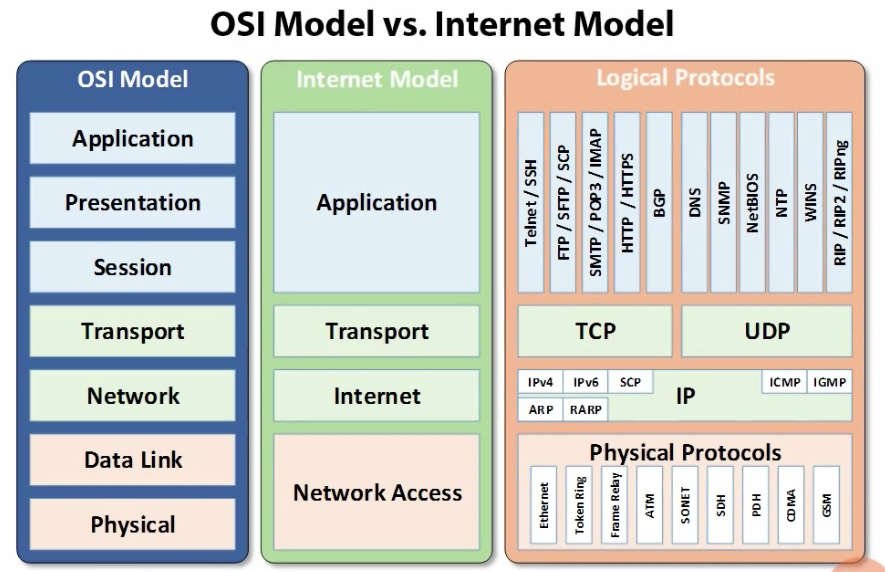
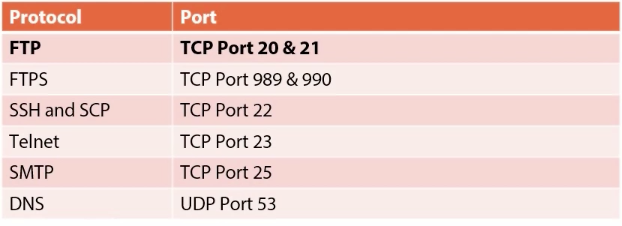
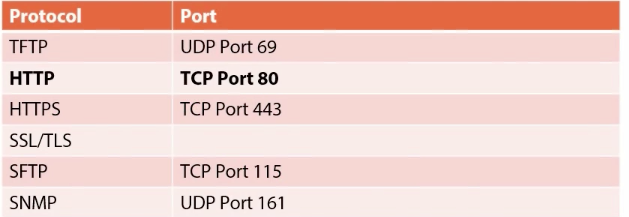
# CompTia Notes: Network security

* Security Configuration Parameters
  + Firewalls
  + Routers
  + Switches
  + Load Balancers
  + Web Security Gateways
  + Intrusion Detection and Prevention Systems
  + NIDS/NIPS Components
  + Reacting to Alerts
  + UTM and URL Filtering
  + Malware
* Secure Network Administration Principles
  + Securing the flow of traffic
  + Securing and separating Network Segments
  + Ensuring Availability
  + Reviewing security logs
* Network Design Elements
  + DMZ
  + Subnetting
  + VLANs, NAT, and PAT
    - Virtual Local Area Network, Network Address Translation, Port Address Translation
  + Telephony, Remote Access, and NAC
    - IP based voice communication (VOIP)
    - Traffic should be segmented with VLANS, increases security and can give it packet priority
    - NAC (network access/admission control) people working remotely
    - Can require anti-virus installed and up to date, certain OS/ patch level, or certain applications
    - Good for BYOD
  + Virtualization
    - Workstations, servers, storage, networking
    - Vmware, Microsoft Hyper-V, KVM, Oracle
    - Lower infrastructure cost, increased licensing costs
    - Can perform the same functions as its physical counterpart
    - Vmware allows you to monitor cpu use, workload, memory use, etc for guests and systems, also gives historical data
  + Cloud Concepts
    - Gives automation and self-service, extension of virtualization
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (Saas)
    - Increasing HA (High Availability) vs. DR (Disaster Recovery)
    - CAPEX to OPEX (Capital Expenditures to Operating Expenses) don’t have to invest as heavily into hardware, configuration, etc.
    - AWS
  + Layered Security
    - Multi-tiered approach
    - Physical: Guards, locks, cameras, badge assess areas
    - Tech: Network access controls, Desktop/server access controls, Strong passwords, anti-virus, Malware detection, intrusion detection/prevention systems
* Common Protocols and services
  + OSI Model
    - 7 parts: Application Presentation, Session, transport, network, datalink, physical (“All People Seem To Need Data Processing”)



* + - Important because makes things easier to change and modify (abstraction)
    - Common application Layer protocols and ports
      * FTP: file transport Protocol
      * FTPS: file transport protocol secure
      * SSH and SCP: secure shell / secure copy way to log into remote devices securely
      * Telnet: used for remote access and configuration, disable if possible. Insecure, communicates in clear text and is open to packet sniffers
      * SMTP: simple mail transport protocol. POP and IMAP moves email from server to client. No encryption inherent in the protocol, should use S/MIME or PGP for encryption. Disable the SMTP open relay feature to limit SPAM and relay attacks
      * DNS: Domain name server
    - Common application layer protocols and ports cont. 
      * TFTP: Trivial File Transfer Protocol, no authentication or encryption, should be disabled whenever possible
      * HTTP: hypertext transfer Protocol, no encryption or authentication, vulnerable to man in the middle attacks
      * HTTPS: hypertext transfer protocol secure, only as strong as the TLS layer, requires a trusted certificate.
      * SSL/TLS: secure sockets layer and transport layer security, adds confidentiality and data integrity by encapsulating other protocols, initiates stateful session with handshakes
      * SFTP: Secure FTP, tunnels through SSL
      * SNMP: Simple network management protocol
  + Transport Layer Protocols
    - TCP: Transmission control protocol, can be used to execute and DDOS
    - UDP: User Datagram Protocol
  + Internet Layer Protocols
    - IPv4/IPv6: two address schemes, doesn’t verify message accuracy (TCP) handles that, IPv6 has built in security
    - ICMP: Internet control message protocol, echo reply and echo request to test connectivity, useful for reporting and maintenance. Vulnerable to ping-of-death and Smurf attacks
    - ARP/RARP: Address Resolution Protocol/ Reverse ARP translates IP address to MAC address, no authentication, vulnerable to ARP spoofing, can be used for man in the middle attacks
  + SAN Protocols
    - Storage Area network, Fiber channel is predominant Protocol
    - Transports SCSI (small computer systems interface)
    - Can run at 2, 4, 8, or 16 gbps
  + Know which ones are secure and which ones aren’t, know common ports
* Wireless Security
  + WEP: Wired Equivalence Protocol, many vulnerabilities, not safe, 24-bit encryption
  + WPA/WPA2: WIFI Protected access, more safe, 128-bit encryption. WPA2 uses CCMP for enhanced security CC-MAC (Counter Message Cipher Block Chaining message authentication code protocol) WPA is backwards compatible with WEP
  + How wireless hacking works: set up rogue access point to block our network, then set up a similar network (evil twin) to fool someone connecting to the network. Then can ask for username and password to get their credentials.
  + Use Penetration testing tools to compromise WEP and WPA/WPA2, Kali Linux is one, lets you locate wireless networks, can capture packets and de-authenticate packets to kick users off of network and then capture their log in attempt info, then use a dictionary to rehash the password
  + EAP: Extensible Authentication Protocol, 5 types of Eap
    - EAP-TLS
    - EAP-PSK
    - EAP-MD5
    - LEAP – light weight extensible authentication protocol, created by Cisco to stop WEP insecurity, easy to configure, no digital certificates, since been deprecated
    - PEAP – created by Cisco, RSA, and Microsoft, digital certificate used on the authentication server, establishes encrypted channel between client and server via TLS tunnel
  + Best Practices:
    - Name network something generic
    - Disabling SSID Broadcast is a waste of time because SSID can be sniffed anyway
    - Use MAC filtering, Pre-select what mac addresses can connect to the WIFI network (still vulnerable to MAC spoofing)
    - Common Sense – Change default admin username and PW, use strongest encryption/ authentication available
    - Keep access points up to date (patches and firmware)
    - Antenna Placement- should be placed near the center of the area to be covered, antennas can be internal or external, Antennas can be omnidirectional or unidirectional
  + War Driving and War Chalking
    - People will drive by with can-tenas to assess signal strength, SSID broadcast, encryption etc.
    - War Chalking involves using chalk to signal information about what types of networks are present
  + Captive Portal
    - Authentication or acceptance page typically found in open and public networks
    - Vulnerable to packet sniffing
    - Once a user is authenticated a hacker could sniff the packets and determine address and MAC address then spoof them to gain access
    - Can put up a fake captive portal to be displayed to capture user credentials
  + VPN over open wireless
    - Can use IPSec or SSL to establish a secure connection in an unsecure environment