Network + Section 4 - TCP/IP Model

TCP/IP Model

- TCP/IP Model, TCP/IP Stack, DoD Model
- Most modern computer networks are TCP/IP based.
- First Layer is Network Interface - Network Interface Layer - Describes how to transmit bits across a network and determine how the network medium is going to be used (MAC address)
- Second Layer - Internet Layer - Where data is taken and packages into IP datagrams.
    - Examples of protocols throughout the Internet Layer are…
        - IP
        - ICMP
        - ARP
        - Reverse ARP
- Third Layer - Transport Layer - Defines the level of service and the status of the connections being used by TCP, UDP, or RTP.
    - TCP connection full
    - UDP connectionless
    - RTP real-time
- Fourth Layer - Application Layer - Dictates how programs are going to interface with the transport layer by conduction session management.
    - HTTP
    - Telnet
    - FTP
    - SSH
    - SNMP
    - DNS
    - SMTP
    - SSL/TLS
- OBJ 1.1 - Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.
- OBJ 1.5 - Explain common ports and protocols, their application, and encrypted alternative.
- OBJ 5.3 - Given a scenario use the appropriate network software tools and commands.

Data Transfer over Networks

- Ports - A logical opening on a system representing a service or application that's listening and waiting for traffic.
    - 0 to 63535
    - Well-Known/Reserved Ports - Ports 0 to 1023

- When Sending information across the internet will be sent as an Ipv4 packet.
- IPv4 Packet - Consists of a source address, destination address, IP flags, and protocol.

Ports and Protocols

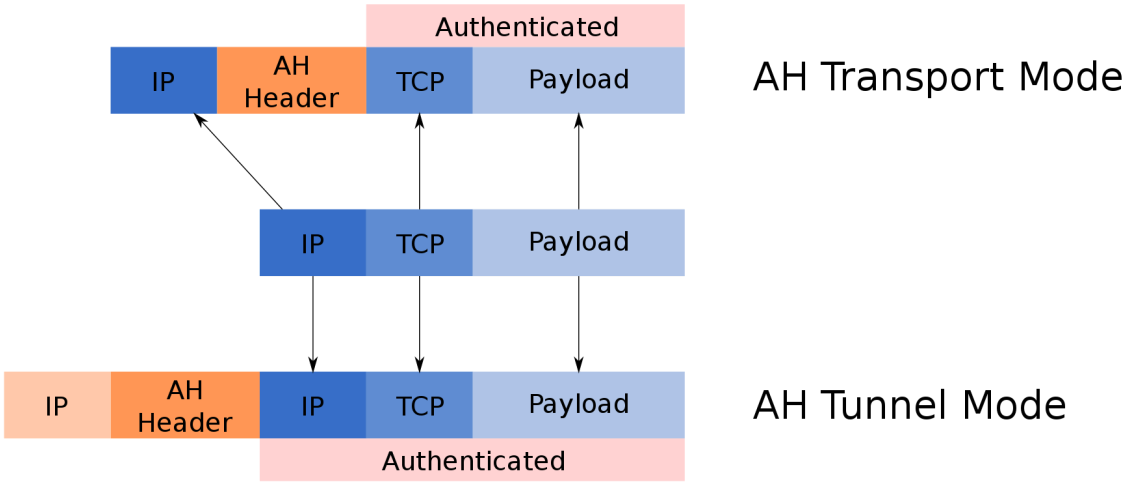
- File Transfer Protocol (FTP) - Ports 20, 21 - Provides insecure file transfers. Between client and server, there is no encryption.
- Secure Shell (SSH) - Port 22 - Provides a secure remote control of another machine causing a text-based environment. It's a cryptographic network protocol.
- Secure File Transfer Protocol (SFTP) - Port 22 - Provides secure file transfer. Tunneling FTP protocol through SSH.
- Telnet - Port 23 - Provides insecure remote control of another machine using a text-based environment. Never use telnet over insecure networks.
- Simple Mail Transfer Protocol (SMTP) - Port 25 - Provides the ability to send emails over the network.
- Domain Name Services (DNS) - Port 53 - Converts domain names to IP addresses, and IP addresses to domain names.
- Dynamic Host Control Protocol (DHCP) - Port 67, 68 - Automatically provides network parameters to your clients, such as their assigned IP address, subnet mask,default gateway, and the DNS server they should use.
- Trivial File Transfer Protocol (TFTP) - Port 69 - Used as a lightweight file transfer method for sending configuration files or network booting of an operating system. Transfer files in both directions over client server application. Stripped down version of FTP. Can be used to send config files to the router or switch or request.
- Hypertext Transfer Protocol (HTTP) - Port 80 - Used for insecure web browsing.
- Post Office Protocol Version 3 (POP3) - Port 110 - Used for receiving incoming emails. Only used for inbound or incoming emails, uses TCP/IP connection.
- Network Time Protocol (NTP) - Port 123 - Used to keep accurate time for clients on the network. NTP is useful to be able to sync up our time and dates across all network devices.
- Network Basic Input/Output System (NetBIOS) - Port 139 - Used for file and printer sharing in Windows network. If using file sharing in a Windows system most likely using port 139.
- Internet Mail Application Protocol (IMAP) - 143 - A newer method of retrieving incoming emails which improves upon the older POP3. IMAP allows end users to view and manipulate messages as if they were stored locally on their machine.
- Simple Network Management Protocol (SNMP) - Ports 161, 162 - Used to collect data about network devices and monitor their status. Monitor uptime downtime and any other states of any given device. Collect data about network devices.
- Lightweight Directory Access Protocol (LDAP) - Ports 389 - Used to provide directory services to your network. Industry standards for distributed directory information services LDAP and Active Directory use this port.

- Hypertext Transfer Protocol Secure (HTTPS) - Port 443 - Used for secure web browsing. Does this over an encrypted tunnel using SSL Secure Sockets Layer or TLS Transport Layer Security. End-to-End encrypted tunnel.
- Server Message Block (SMB) - Port 445 - Used for Windows file and printer sharing services. NetBIOS is going to be used to do authentication over Port 139 then Server Message Block (SMB) will handle the actual passing out of those files and shares by sending data.
- System Logging Protocol (Syslog) - Port 514 - Used to send logging data back to a centralized server.
- Simple Mail Transfer Protocol Layer Security - (SMTP TLS) - Port 587 - Secure and encrypted way to send emails.
- Lightweight Directory Access Protocol Secure (LDAPS) - Port 636 - Provides secure directory services. Using an encrypted tunnel over SSL or TLS to make it more secure.
- Internet Message Access Protocol over SSL (IMAP over SSL) - Port 993 - Secure and encrypted way to receive emails.
- Post Office Protocol Version over SSL (POP3 over SSL) - Port 995 - Secure and encrypted way to receive emails. Does not maintain their read or unread status.
- Structured Query Language Protocol (SQL) - Port 1443 - Used for communication from a client to the database engine.
- SQLnet Protocol - Port 1521 - Used for communication from a client to an Oracle database. Provides a lot of the same functionality of Microsoft SQL.
- MySQL - Port 3306 - Used for communication from a client to the MySQL database engine. This is an open source protocol.
- Remote Desktop Protocol (RDP) - Port 3389 - Provides graphical remote control of another client or server. Proprietary protocol developed by Microsoft. RDP provides a full graphical user interface. Full control over mouse and keyboard.
- Session Initiation Protocol (SIP) - Port 5060, 5061 - Used to initiate VoIP and video calls. Provide signaling and controlling media communication sessions. (VoIP, Skype, FaceTime).

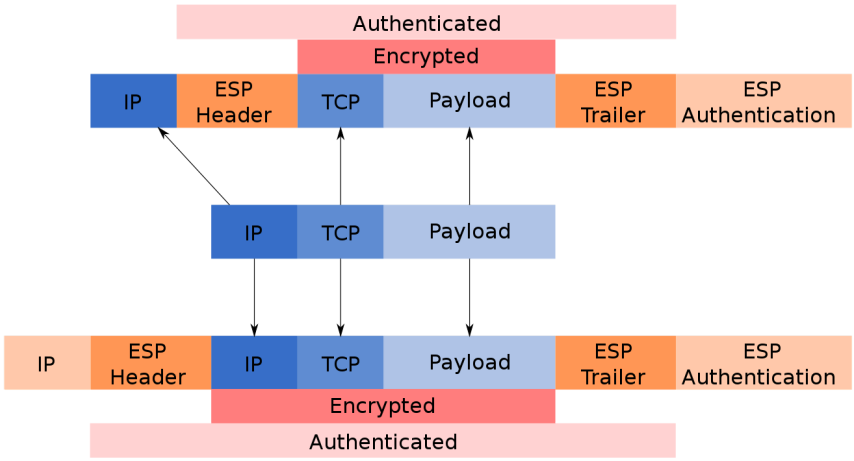
IP Protocol Types

- Transmission Control Protocol (TCP) - conducts a three-way handshake between a client and a server and then establishes the connection.
    - Windowing - continually renegotiates how much data can be sent and received. As data is sent, the recipient is going to verify to receiver all the packets that were sent as expected by sending ACK each time.
    - TCP is considered connection-oriented. Even if out of order TCP can rearrange things in the correct order.
- User Datagram Protocol (UDP) - Detects if packets are corrupted when they are received by a client using a checksum. Essentially fire and forget. Used for streaming video and music.

- Internet Control Message Protocol - Used to communicate information about network connectivity issues back to the sender. PIng uses ICMP. ICMP is listed as protocol number 1 inside the TCP/IP suite. Used as an error reporting mechanism and query service.
- Generic Routing Encapsulation (GRE) - Used as a simple and effective way to create a tunnel, called GRI tunnel, over a public network. Developed by Cisco to encapsulate an internet protocol network. GRE tunnel established over Router level, consider MTU size for this tunnel. 1400 bytes is recommended so it doesn't go over the 1500 maximum transmission size so it doesn't cause network connectivity issues.
    - GRE tunnel does not provide any encryption.
- Internet Protocol Security (IPSec) - Used to protect one or more data flow between peers. Set of secure communication protocols at the network or packet processing layer, used to protect one or more data flows between two peers.
    - Data confidentiality
    - Data integrity
    - Origin authentication
    - Anti-replay
    - IPSec lets you encrypt your tunnel to protect data from prying eyes.
    - Used heavily inside VPN's
    - IPSec uses two underlying protocols.
        - Authentication Header (AH) - A protocol within IPSec that provides integrity and authentication. Takes IP and Payload and hashes both of them. Then hash is used to create a new AH header which is added to the packet.



        - Encapsulating Security Payload (ESP) - Provides encryption and integrity for the data packets sent over IPSec. ESP is added after the standard IP header inside the packet. ESP is backwards compatible with most IP routers.


Authenticated
Encrypted
IP
ESP Header
TCP
Payload
ESP Trailer
ESP Authentication
ESP Transport Mode
IP
TCP
Payload
IP
ESP Header
IP
TCP
Payload
ESP Trailer
ESP Authentication
ESP Tunnel Mode
Encrypted
Authenticated