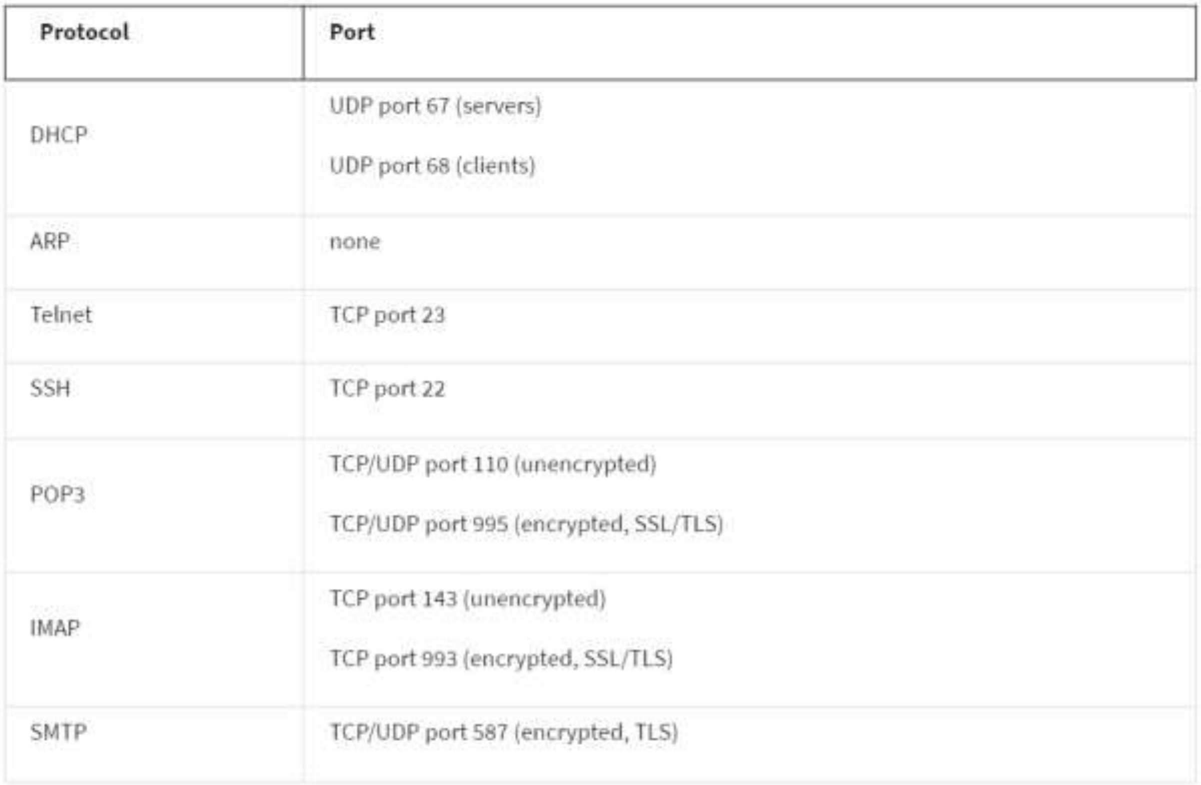
- A network protocol is a set of rules used by two or more devices on a network to describe the order of delivery and the structure of data.
- **Three categories of network protocols:**
  - **Communication protocols:**
    - Govern the exchange of information in network transmission
    - Dictate how the data is transmitted between devices and the timing of the communication.
    - Include methods to recover data lost in transit.
    - Contains TCP, UDP, HTTP, and DNS.
  - **Management Protocols:**
    - Used for monitoring and managing activity on a network.
    - Include protocols for error reporting and optimizing performance on the network.
    - Contains ICMP and SNMP
  - **Security Protocols:**
    - ensure that data is sent and received securely across a network
    - Contains HTTPS and SFTP

- Domain Name System (DNS) is a protocol that translates internet domain names into IP addresses
- Simple Network Management Protocol (SNMP) is a network protocol used for monitoring and managing devices on a network.
- **Hypertext Transfer Protocol Secure (HTTPS):**
  - Provides a secure method of communication between clients and website servers.
  - A secure version of HTTP that uses secure sockets layer/transport layer security (SSL/TLS) encryption on all transmissions so that malicious actors cannot read the information contained.
- Secure File Transfer Protocol (SFTP) is a secure protocol used to transfer files from one device to another over a network.
- **Dynamic Host Configuration Protocol (DHCP):**
  - An application layer protocol used on a network to configure devices
  - Assigns a unique IP address and provides the addresses of the appropriate DNS server and default gateway for each device
- **Secure shell protocol (SSH):**
  - An application layer protocol that provides an alternative for secure authentication and encrypted communication
  - Used to create a secure connection with a remote system
- **Telnet:**
  - An application layer protocol that allows a device to communicate with another device or server.
  - Sends all information in clear text
  - Uses command line prompts to control another device similar to secure shell (SSH), but Telnet is not as secure as SSH

Created By: Abdelrahim Alsadiq

- Post office protocol (POP) is an application layer protocol used to manage and retrieve email from a mail server.
- Internet Message Access Protocol (IMAP) used for incoming email. It downloads the headers of emails, but not the content. The content remains on the email server, which allows users to access their email from multiple devices.
- **Simple Mail Transfer Protocol (SMTP):**
    - Used to transmit and route email from the sender to the recipient's address.
    - Works with Message Transfer Agent (MTA) software, which searches DNS servers to resolve email addresses to IP addresses, to ensure emails reach their intended destination.



Protocol	Port
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22
POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)
SMTP	TCP/UDP port 587 (encrypted, TLS)

- IEEE 802.11 (Wi-Fi): A set of standards that define communication for wireless LANs
- **Wired equivalent privacy (WEP):**
  - A wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections.
  - The oldest of the wireless security standards.
- **Wi-Fi Protected Access (WPA)**
  - Developed to improve upon WEP, address the security issues that it presented, and replace it.
  - Still has vulnerabilities. Malicious actors can use a key reinstallation attack (or KRACK attack) to decrypt transmissions using WPA.
- **The second version of Wi-Fi Protected Access (WPA2)**
  - Improves upon WPA by using the Advanced Encryption Standard (AES) and the Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP) which provides encapsulation and ensures message authentication and integrity
  - Considered the security standard for all Wi-Fi transmissions today
  - Still vulnerable to KRACK attacks
- **The third version of Wi-Fi Protected Access (WPA3)**
  - Addresses the authentication handshake vulnerability to KRACK attacks
  - Uses Simultaneous Authentication of Equals (SAE), a password-authenticated, cipher-key-sharing agreement.
  - Has increased encryption to make passwords more secure by using 128-bit encryption

- Subnetting: The subdivision of a network into logical groups called subnets
- Network segmentation: A security technique that divides the network into segments
- Proxy server: A server that fulfills the requests of its clients by forwarding them to other servers
  - Forward proxy server: A server that regulates and restricts a person's access to the internet
  - Reverse proxy server: A server that regulates and restricts the internet's access to an internal server
- **Firewall: A network security device that monitors traffic to or from your network**
  - Hardware firewall is considered the most basic way to defend against threats to a network, inspects each data packet before it's allowed to enter the network.
  - Software firewall performs the same functions as a hardware firewall, but it's not a physical device. Instead, it's a software program installed on a computer or on a server.
  - Cloud-based firewalls: Software firewalls that are hosted by the cloud service provider
- Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats. A stateful firewall analyzes network traffic for characteristics and behavior that appear suspicious and stops them from entering the network.
- Stateless refers to a class of firewall that operates based on predefined rules and does not keep track of information from data packets. A stateless firewall only acts according to preconfigured rules set by the firewall administrator. The rules programmed by the firewall administrator tell the device what to accept and what to reject.

- Next generation firewall (NGFW) provides more security than a stateful firewall. It performs more in-depth security functions like deep packet inspection and intrusion protection.
- Port filtering: A firewall function that blocks or allows certain port numbers to limit unwanted communication
- **Security zone: A segment of a company's network that protects the internal network from the internet**
  - Uncontrolled zone: The portion of the network outside the organization
  - Controlled zone: A subnet that protects the internal network from the uncontrolled zone
- Virtual private network (VPN): A network security service that changes your public IP address and masks your virtual location so that you can keep your data private when you are using a public network like the internet