Protocols

* FTP – File transfer Protocol
  + Port 20 for FTP server operations, port 21 for client operations.
  + The protocol used to download files from an FTP server to a client computer
* DHCP – Dynamic Host Configuration Protocol
  + Port 67, 68
  + Auto assigns IP address to computers within the network (DORA)
    - DHCPDISCOVER->DHCPOFFER->DHCPREQUEST->DHCPACK
    - Initializing->Selecting->Requesting->Binding->Renewing->Rebinding
      * A Client issues a DHCP DISCOVER message via a broadcast. 255.255.255.255
      * DHCP server receives the message and replies with the DHCP Offer as a broadcast message with the client’s MAC
      * Once the client receives the DHCP OFFER, it sends a DHCP REQUEST message to the server which accepts the network configuration
      * The DHCP server sends a DHCP ACK message to acknowledge the DHCP REQUEST
      * The client then uses the network configuration and is on the network.
* LDAP – Lightweight Directory Access Protocol
  + Set of open protocols used to access and modify centrally stored info over a network
* UDP – User Datagram Protocol – P362
  + UDP provides a connectionless communication delivery service. UDP uses datagrams to send network communication.
  + A datagram requires an IP address and a UDP port for communication to be successful. Because UDP does not establish a connection for data transfer, the transmission of the data is considered unreliable. Packets are numbered in the same manner as TCP segments; however, no sequence packet specifies how to arrange the packets. If a client does not receive a data packet, no retransmission of the data packet is done because the client does not send acknowledgment packets during a UDP session.
* ARP – Address Resolution Protocol
  + Determines the MAC address of a host when only the IP address is known

Services

* SSH – Secure Shell
  + Port 22
  + A program used for logging into and executing commands on a remote machine.
  + Provides secure encrypted communication between two untrusted hosts over an unsecure network.
* TELNET –
  + Port 23 – uses TCP communication over the default port 23
  + Allows communication between Windows/Unix & command…interface
  + Remote control and remote configuration of servers (Plain text – unsecure).
* DNS – Domain name service
  + Port 53
  + Resolves domain names to IP addresses
    - A domain name is entered into a web browser
    - The browser asks the ISP’s DNS server to resolve the request
    - If the ISP’s DNS can’t resolve the domain name it asks a root server
    - If the root server does not know it will ask another name server that knows about “.com” domains.
    - The server answers the request with the IP address (it is marked as authoritative).
    - The ISP’s DNS responds to the web browser with the IP address
    - The query is cached for ….?
  + Root servers are run by ICANN -> US company

TCP/IP & Handshake

* + TCP – Transmission Control Protocol
    - TCP provides a connection-oriented communication exchange, Because TCP establishes a connection before hosts can exchange data, the data exchange is considered to be reliable. TCP uses sequence numbers and acknowledgment numbers to provide the reliable communication exchange. The connection is based on a three-way handshake that synchronizes the sequence numbers and acknowledgment numbers. TCP breaks data packets into segments and assigns each packet a sequence number. The source host must acknowledge each segment, and if no acknowledgment packet is received, the data is retransmitted. To protect validity of the data, a checksum is added to each segment sent. The checksum servers act as a parity check for the data, and if the checksum calculation performed by the client does not match the checksum sent by the server, the data is considered corrupt and the packet is discarded.
    - TCP uses a parameter called the window size to specify the amount of data that can be buffered on a single connection. The window size is an operating system independent parameter, and therefore a default value on a Microsoft operating system does not apply to a Unix operating system; however, the window size is negotiated between client and server during the three-way handshake.
    - Because TCP uses the three-way handshake, the time to transmit the data is longer than when using UDP, and therefore, is considered to be slower in network data transfer.
  + IP – Internet Protocol
    - IP governs placing IP addressing and routing information on data packets. IP also uses a mathematical calculation called ANDing to determine whether a packet needs to be sent to a router. IP provides packet fragmentation, also called segmenting. When IP receives a packet that is too large to transmit, IP breaks the packet into smaller sections and number each packet, so the packet can be reassembled on the receiving client. In addition, IP on a router governs decrementing a packets Time-To-Live (TTL) as it passes through the router. Each packet on a network has a default TTL, and when the TTL reaches 0, the packet is discarded, or what is sometimes called, stored in the bit bucket. To avoid network congestion, it is recommended that an administrator periodically empty the bit bucket.
* Subnetting – a subnetwork or subnet is a logically visible subdivision of an IP network. The practives of dividing a network in to subnetworks is called subnetting.
  + All computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. This results in the logical division of an IP address into two fields, a network or routing prefix and the rest field. The rest field is a specific identifier for the computer or the network interface.
  + The routing prefix is expressed in CIDR notation. It is written as the first address of a network followed by the bit-length of the prefix, separated by a slash (*/*) character. For example, 192.168.1.0/24 is the prefix of the Internet Protocol Version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the rest (8 bits) reserved for host addressing. The IPv6 address specification 2001:db8::/32 is a large network for 296 hosts, having a 32-bit routing prefix. In IPv4 the routing prefix is also specified in the form of the **subnet mask**, which is expressed in quad-dotted decimal representation like an address. For example, 255.255.255.0 is the network mask for the 192.168.1.0/24 prefix.
  + Traffic between subnetworks is interchanged with special gateway computers called routers; they constitute logical or physical borders between the subnets.
  + The benefits of subnetting vary with each deployment scenario. In the address allocation architecture of the Internet using Classless Inter-Domain Routing (CIDR) and in large organizations, it is necessary to allocate address space efficiently. It may also enhance routing efficiency, or have advantages in network management when subnetworks are administratively controlled by different entities in a larger organization. Subnets may be arranged logically in a hierarchical architecture, partitioning an organization's network address space into a tree-like routing structure.
* Fault Isolation

Misc.

* NFS - Network File System
* SAN
* \*RSH\*
* \*SAMBA\*
* \*CVS\* - Concurrent Versions System
* WINS – Windows Internet naming service
  + Ports 137, 138, and 139
  + Resolves NetBIOS names on a Microsoft network
* HTTP – HyperText Transfer Protocol
  + Port 80
* HTTPS - HyperText Transfer Protocol Secure
  + Port 443
* POP3 Post Office Protocol version 3
* Secure POP3
* IMAP4 – Internet Message Access Protocol
  + Port 143
  + Allows client access to other boxes such as deleted items, sent items, etc.
  + Most of the newest internet mail clients are IMAP4 compliant
* Secure IMAP4
  + Port 995
* SMTP – Simple Mail Transport Protocol
  + Port 25
  + Mail Drop services, POP3, IMAP4, etc. cannot send. They only receive
  + SMTP is used for sending mail from one SMTP to another SMTP server.
  + The SMTP server has its own MX (Mail exchanger) record in the DNS database that corresponds to the domain for which it is configured to receive mail.
  + When equipped for two-way communication, mail clients are configured with the address of a POP3 server to receive mail and the address of an SMTP server to send mail. The clients can configure server parameters in the properties sheets of the mail client, basing the choices on an FQDN or IP address. SMTP uses TCP for communication
* What is the OSI model?
  + Physical
  + Datalink
  + Network
  + Transport
  + Session
  + Presentation
  + application
* Given the ip address of 10.0.0.25 with the subnet mask of 255.255.255.0 how many addresses are available on the subnet?
  + 254
* What would the broadcast address be
  + 10.0.0.255
* What slash is that subnet?
  + /24