Networking

A network is a group of computers and computing devices connected together through communication

channels.

-A network is used to:

* + Allow the connected devices to communicate with each other
  + Enable multiple users to share devices over the network, such as printers and scanners
  + Share and manage information across computers easily.

-IP Addresses

* Devices attached to a network must have at least one unique network address identifier known as the IP (Internet Protocol) address.
* The address is essential for routing packets of information through the network.

-IPv4 and IPv6

* There are two different types of IP addresses available: IPv4 (version 4) and IPv6 (version 6).
* IPv4 uses 32-bits for addresses; there are only 4.3 billion unique addresses available.
* NAT enables sharing one IP address among many locally connected computers, each of which has a unique address only seen on the local network.
* IPv6 uses 128-bits for addresses; this allows for 3.4 X 1038 unique addresses.

-Decoding IPv4 Addresses

* A 32-bit IPv4 address is divided into four 8-bit sections called octets.
* Network addresses are divided into 5 classes: A, B, C, D and E.
* Classes A, B and C are further classified in 2 parts: Network address(Net ID) & Host address(Host ID).
* The Net ID is used to identify the network, while the Host ID is used to identify a host in the network.
* Class D is used for special multicast applications.
* Class E is reserved for future use.

-Class A Network Addresses

* Class A addresses use the first octet of an IP address as their Net ID and use the other three octets as the Host ID.

-Class B Network Addresses

* Class B addresses use the first two octets of the IP address as their Net ID and the last two octets as the Host ID.

-Class C Network Addresses

* Class C addresses use the first three octets of the IP address as their Net ID and the last octet as their Host ID.

-IP Address Allocation

* You can assign IP addresses to computers over a network either manually or dynamically.
* Mannual- static IP
* Dynamic- Dynamic Host Configuration Protocol (DHCP).

-Name Resolution

* Name Resolution is used to convert numerical IP address values into a human-readable format known as the hostname.

-Network Configuration Files

* Network configuration files are essential to ensure that interfaces function correctly. They are located in the /etc directory tree.

-Network Interfaces

* Network interfaces are a connection channel between a device and a network.
* Physically, network interfaces can proceed through a network interface card (NIC).
* Or can be more abstractly implemented as software.
* Information about a particular network interface or all network interfaces can be reported by the ip and ifconfig utilities.

-The ip Utility

* To view the IP address:
* $ /sbin/ip addr show
* To view the routing information:
* $ /sbin/ip route show

-ping

* ping is used to check whether or not a machine attached to the network can receive and send data; i.e. it confirms that the remote host is online and is responding.
* ping is frequently used for network testing and management; however, its usage can increase network load unacceptably.

-route

* A network requires the connection of many nodes.
* Data moves from source to destination by passing through a series of routers and potentially across multiple networks.
* Servers maintain routing tables containing the addresses of each node in the network.
* The IP routing protocols enable routers to build up a forwarding table that correlates final destinations with the next hop addresses.
* We can use the route utility or the newer ip route command to view or change the IP routing table to add, delete, or modify specific routes to specific hosts or networks.
* Show current routing table- $ route –n or ip route
* Add static route- $ route add -net address or ip route add
* Delete static route- $ route del -net address or ip route del

-traceroute

* traceroute is used to inspect the route which the data packet takes to reach the destination host.
* Which makes it quite useful for troubleshooting network delays and errors.
* By using traceroute, you can isolate connectivity issues between hops, which helps resolve them faster.

-More Networking Tools

* ethtool- Queries network interfaces and can also set various parameters such as the speed
* netstat- Displays all active connections and routing tables. Useful for monitoring performance and troubleshooting
* nmap- Scans open ports on a network. Important for security analysis
* tcpdump- Dumps network traffic for analysis
* iptraf- Monitors network traffic in text mode
* mtr- Combines functionality of ping and traceroute and gives a continuously updated display
* dig- Tests DNS workings. A good replacement for host and nslookup