Common Networking terms

Access Point: Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication: Authentication refers to the verification of a transmitted message's integrity.

DMZ: (DeMilitarized Zone) is a part of an network that is located between a secure LAN and an insecure WAN. DMZs provide a way for some clients to have unrestricted access to the Internet.

Beacon Interval : Refers to the interval between packets sent sent by access points for the purposes of synchronizing wireless LANs.

DHCP : (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DNS :DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.

Domain Name : The domain name typically refers to an Internet site address.

DTIM:DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

Filter : Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall : Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.

Firmware : Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.

Fragmentation : Refers to the breaking up of data packets during transmission.

FTP :FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.

Gateway : Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Host Name : The name given to a computer or client station that acts as a source for information on the network.

HTTP : HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, *http://www.shabeeribm.in*).

ICMP : ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP : IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address : The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP: An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN: (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.

MAC Address: A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric: A number that indicates how long a packet takes to get to its destination.

MTU : MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT : NAT (Network Address Translation) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP :NTP (Network Time Protocol) is used to synchronize the realtime clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet : A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping : Ping (Packet INternet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port : Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE : PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

Preamble : Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roaming wireless enabled devices and access points.

Protocol : A protocol is a rule that governs the communication of data.

RIP : RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

RTS : RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server : Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP : SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

SNMP : SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network.

SSID : SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

Subnet Mask : Subnet Masks (SUBNETwork masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.

SysLog Server : A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP : (Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP : TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in realtime video and audio transmission).

The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

Telnet : Telnet is a terminal emulation protocol commonly used on the Internet and TCP- or IP-based networks.
Telnet is used for connecting to remote devices and running programs. Telnet is an integral component of the TCP/IP communications protocol.

UDP : (User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, realtime video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers : Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WEP : WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks.

Wireless LAN : Wireless LANs (WLANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WAN :
WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).

Via : Trendnet