Basic Networking

DHCP--Dynamic Host Configuration Protocol--used to dynamically assign an IP address to a device on a network—DHCP server UDP port 67, client UDP port 68

ARP—maps IP addresses to MAC addresses on a LAN. ARP is done by broadcast and does not use ports. Cisco default timeout for IP to MAC addressing in ARP cache is 4 hours.

IMAP--Internet Message Access Protocol--allows access to email located on a remote server--allows syncing and access from multiple devices

POP3--Post Office Protocol 3--emails are downloaded from the mail server to a single device unless setting "Keep email on server" is enabled

SMTP--Simple Mail Transfer Protocol--used to send emails from a client to a server, also used to send emails between mail servers

----

telnet--provides command line interface to remote host--not encrypted--port 23

ssh -- secure shell -- replacement for telnet-- uses public key/private key -- port 22

----

ftp --file transfer protocol--used to send and receive files--not encrypted -- port 21

FTPS--replacement for FTP--uses SSL/TLS to encrypt. Two modes of operation: implicit mode (old, by default encrypts only the handshake) uses control port 990, data port 989; explicit mode users control port 21, then assigns another port as a data port,

SFTP--SSH File Transfer Protocol--replacement for ftp--piggybacks on an SSH connection/is an extension of SSH that provides file access(Not the same as FTPS.) (Not the same as Simple FIle Transfer Protocol.) (Not the same as running ftp over an ssh connection, it's a separate protocol with a separate standard.) There is a Secure File Transfer Program (sftp) that is a command line interface that uses the SFTP protocol.--port 22.

SCP--Secure Copy Protocol--uses SSH for data transfer. There is a Secure Copy program (scp) that is a command line interface that uses the SCP protocol.--port 22.

NOTE: there is an scp2 command line program that uses SFTP instead of SCP but has the same command line interface as the scp program.

SNMP—System Network Management Protocol—used to manage and monitor devices on IP networks. Transported over UDP. SNMP agent—receives requests on udp port 161, may generate notifications from any available port. SNMP manager—udp port 162.

NTP—Network Time Protocol—used to synchronize participating computers to within a few milliseconds of Coordinated Universal Time (UTC)—receive timestamps on UDP port 123

ICMP—Internet Control Message Protocol—used by internet devices (such as routers) to send error messages such as unreachability. Runs on top of IP, so does not use port numbers. Ping uses ICMP echo request/echo reply. Other responses include destination unreachable (unreachable host, unreachable network, unknown host, unknown network, etc.), redirect packets to an alternative route, timestamp/timestamp reply.

HTTP—protocol used for the world wide web—port 80.

- GET—retrieve web page (can also send data to web page as parameters appended to url), POST—modify and update a resource
- PUT—create a resource or overwrite it

HTTPS—a secure version of HTTP that runs over SSL/TLS—port 443.

LDAP—Lightweight Directory Access Protocol—access and maintain directory services—directory services can be any organized set of records—a subset of the ITU-T X.500 standard—TCP port 389. Some LDAP uses:

- Single sign on, where a password is shared between many services
- Look up printers and other services on a network
- Look up encryption certificates
- Store employee information (contact info, for example)
- Choose LDAP if frequent reads but few updates, a database for frequent updates

LDAPS—LDAP over SSL—an encrypted version of LDAP--TCP port 636.

XWindows—version X11 so often called X11—an X server (such as Xming on Windows) sits on your local machine and accepts input from you that it sends to a (possibly remote) client, and receives display information from the (possibly) remote client (xterm, xclock, xcalc, for example). This allows you to use a GUI that is located on a remote machine.—uses TCP port 60 plus a server/display port chosen from 6000-6063, wireshark looks for TCP on 6000-6002.

MPLS—Multi Protocol Label Switching—normally used in applications that need real time service

- When a packet first enters a network it is assigned to a Forwarding Equivalence Class (FEC).
    - A uni-directional label switched path (LSP) is established for each FEC to each destination, since it is unidirectional a different LSP is used for the return direction.
        - The LSPs have been pre-established for each FEC
            - One way this is done is by MPLS-enabled routers sending each other routing information by using the Label Distribution Protocol
- When an end user sends traffic into a network, a Label Edge router pushes a label onto the front of that packet.
    - Then when that packet is received at the next (internal) router, that router, which is a Label Switch Router, would look up that label in a table and replace it with a new label that directs the packet along the next top to the next MPLS router (could be either a Label Switch router or a Label Edge router).
    - When that packet reaches the edge of the MPLS domain area, it will have its label removed by another Label Edge router, and it will be send to the final LAN or host.
- MPLS can be used to do label switching/routing for most protocols, but is usually nowadays used for IP.