CIDM 6303 NETWORKING

1.5 Ports and Protocols

Introduction to IP: internet protocol

TCP-Transmission control protocol

- Connection-oriented, reliable delivery (recovery from errors and can manage out of order messages or retransmission).

- It has a sequence order. Client>TCP data>Server and Server >TCP ACK >Client

UDP-User Datagram protocol

- Connectionless: no formal open or close to the connection.
- Unreliable delivery: no error recovery, no reordering of data or retransmission

No flow control-sender determine the amount of data transmitted.

Ipv4 sockets

- Server IP address, protocols, client IP address, server application port number

Non-ephemeral Ports

- Permanent port number: Ports 0 through 1,023 and Usually on a server or services

Ephemeral Ports

- Temporary port numbers (ports 1,024 through 65,535

Port numbers

- TCP and UDP ports can be any number between 0 and 63,535.

Ports on network

- Web server TCP/80, VoIP server UDP/5004 and Email server TCP/143

Common Ports

- Telnet on TCP port 23
- SSH (secure Shell) on Port 22
- DNS-Domain name system uses UDP/53 and TCP/53
- SMTP (simple mail transfer Protocol) uses TCP 25 or TCP 587 using TLS encryption.
- SFTP (secure FTP) uses TCP /22, FTP (file transfer protocol) uses TCP /20 and TCP /21
- DHCP (dynamic host configuration protocol) uses UDP 67 and 68
- HTTP and HTTPS uses TCP /80 and TCP /443 which uses SSL or TLS
- RDP (TCP /3389

- ICMP (internet control message protocol) we can use ping.

- Virtual Private Networks-encrypted private data traversing a public network.

1.6 Network Services

DHCP Overview

- Initially released 1997 which provide automatic IP across all networks and devices.
- create a DHCP scope for the config of the DHCP, add a subnet mask, lease duration, DNS server, default gateway, grouping of IP address called DHCP Pools,
- Dynamic assignment, automatic assignment of DHCP and static assignment

- Translate human readable names into computer readable IP address.
- Distributed database: many DNS server and has 13 root server cluster.

Types of DNS

Internal DNS: Managed on internal DNS, Configured, and maintained by the local team.

External DNS: Managed externally.

Recursive and Iterative DNS Queries

Recursive: delegate the lookup to a DNS Server, DNS server does the work and report back, large DNS cache provide a speed advantage.

Iterative: do all your queries yourself.

Authoritative and Non-Authoritative
Authoritative: The DNS server is the authority for the zone
Non-Authoritative: Does not contain the zone source file and probably cached info.

DNS Records:
Resource record (RR)-database records of DNS have over 30 record types in the DNS.
A record, AAAA records, CNAME, SRV, MX, NS, PTR, TXT

Network Time Protocol: The Network Time Protocol is used to synchronize the clocks in all our network devices.

2.1 Network devices

Multi-port repeater: Traffic going in one port is repeated to every other port.
Everything is half duplex.

Bridge: imagine a switch with two to four ports and connects different physical networks
OSI layer 2 devices.

Switch: Bridging done in hardware, An OSI layer 2 devices which has many ports and features With Multilayer switch.

Router: Routes traffic between IP subnets

Access Point: A wireless router is a router and an access point in a single device.

Cable Modem: used for transmission across multiple frequencies.

DSL Modem: ADSL uses telephone lines (Asymmetric digital subscriber line.

Repeater: receive signal, regenerate, resend (no forwarding decision to make).

Advanced Networking Device

Layer 3 capable switch: a switch (layer 2) and router (layer 3) in the same physical device.

Wireless networks everywhere: Wireless networking is pervasive.

Wireless Lan controller: centralized management of access points.

Load Balancer: distribute the load, fault tolerance, large scale implementation, configurable load, TCP offload, SSL offload.
Proxies: sit between the users and the external networks, receives the users' requests, and send the requests on their behalf.

VPN: encrypted data traversing a public network.

Networked devices

VoIP phones (voice over internet protocol, printer, card reader, camera, surveillance systems HVAC, Internet of things (IOT e.g., smart devices)

3.2 Organizational Policies

Plans and Procedures

Change management: How to make a change (upgrade software, change firewall config), having clear policies (frequency, duration, installation process).

Security incidents: User clicks an email attachment, DDOs, confidential info is stolen.

Disaster recovery plan: Disasters are many and varied, if a disaster happen IT should be ready, comprehensive plan.

Continuity of operation planning (COOP): There need to be an alternative, theses must be documented.

System life cycle: Managing asset disposal, disposal becomes a legal issue.

Standard operating procedures: Operational procedure, software upgrades, documentation is the key.

Service Level Agreement (SLA): minimum terms for service provided, uptime, response time agreement.

Non-disclosure agreement (NDA): protect confidential info, confidentiality agreement between parties.

Security policies

Password Policy: make password strong, increase password entropy, prevent password reuse.

Acceptable use policies (AUP): what is acceptable use of company asset.

Bring your own device (BYOD):

Remote access policies: easy to control internal communication, policy for everyone.

Data Loss Prevention (DLP): detailed policies needed to define what is allowed.

Network documentation

Floor plans: Overlay the wired and wireless network, used for planning.

Physical network maps: Follow the physical wire and devices.

Distribution frames: Passive cable termination, usually mounted on the wall, all transport media.
Main Distribution frame: central point of the network, termination point for wan links, good test point.

Logical network maps: useful for planning and collaboration.

Others: Managing your cable, Labeling, site survey, Audit, and assessment report

4.4 Remote Access

VPNs: Virtual private networks, concentrators

1. **Client to site VPN**: on demand access from a remote device, some software can be configured as always-on.
2. **Site-to-site VPN**: Always -on, Firewall often act as VPN concentrators.
3. **Full Tunnel**: all traffic is sent to the corporate network sending via the full tunnel which is then distributed to the remote user.
4. **Spilt Tunnel**: allow client to communicate to the internet without using any resources located on the VPN concentrator.
5. **Clientless VPNs**: create a VPN tunnel without a separate VPN application.

Remote desktop connection: share a desktop from a remote location, RDP (client for Mac OS).

Remote desktop gateway: combine a VPN with Microsoft remote desktop, client connect to the remote desktop gateway, remote desktop gateway connects internally to RDP servers over TCP 3389.

- Its act as a proxy to all RDP services

Secure Shell (SSH): encrypted console communication over TCP 22

Cloud-hosted virtual desktop: A virtual desktop infrastructure in the cloud, access from almost any Operating Systems (IOS, Windows, Mac OS, Linux).

Out-of-band management: The network isn't available, connect a modem, console router/comm server.

5.3 Software Tools

Wireless packet analysis: wireless networks are incredibly easy to monitor, some network drivers wont capture wireless info, view wireless specific information.

Protocol analyzers: Solve complex apps issue, gather frames on the network, view traffic patterns, large scale storage. Example is Wireshark.

Speed Test Sites: Bandwidth testing, provide useful pre and post change analysis, measure at different times of the day, not all sites are the same. E.g., Use ISP sites, speedof.me, speedtest.net or use Iperf.

Iperf: Performance monitoring and speed testing, need two computers (client and server), support across many operating systems.

IP and Port Scanners: Active (scan for IP address and open ports), pick a range of IP address, visually map the networks, rogue system detection. Examples NMAP, Angry IP scanner.

NetFlow: gather traffic statistics from all traffic flows, NetFlow, probe and collector, usually a separate reporting app.

TFTP Server (Trivial file transfer protocol): a bare min file transfer protocol, your device is the TFTP server, many options available for Windows, Linux, and Mac OS.

Terminal emulator: such as SSH (secure shell) and Windows Terminal.

Command Line Tools

Ping: test reachability which uses ICMP.

Ipconfig/Ifconfig/IP: most of your troubleshooting start with your IP address, determine the TCP/IP and network adapter information.

- Ipconfig—Windows TCP/IP configuration.
- Ifconfig – Linux interface configuration
- Ip address – the latest Linux utility.

Nslookup and dig: lookup info from the DNS servers,

- Nslookup: Both Windows and POSIX based.
- Dig: More advanced domain info.

Traceroute: Determine the route a packet takes to its destination (tracert-windows or traceroute - Linux/macOS/UNIX), take advantage of ICMP time to live extended error message, not all devices will reply with ICMP time exceeded message.

Address Resolution Protocol: Determine a mac address based on an Ip address and uses Arp -a.

Netstat: Get network statistics, netstat -a (show all active connection), netstat -b (show binaries), netstat -n (do not resolves names).

Hostname: View FQDN and IP address of the devices, it available on windows, Linux, macOS

Route: View the device routing table, Windows uses route print, Linux/macOS and windows and uses netstat -r

Telnet: Telnet over TCP 23, login to device remotely, in the clear communication, great utility for checking a port or application.

Tcpdump: capture packets from the command line, available in UNIX Linux, apply filter view in real time, save the data use in another application.

Nmap: network mapper, port scan, OS scan, service scan.