Network+ Full Detailed Notes

1. Networking Concepts

- LAN (Local Area Network): Covers a small geographic area like an office or building.
- WAN (Wide Area Network): Covers a broad area such as multiple cities or countries.
- MAN (Metropolitan Area Network): Larger than LAN but smaller than WAN, typically spans a city.
- PAN (Personal Area Network): Smallest network, for devices like Bluetooth connections.
- Internet: Global network connecting millions of private, public, academic, and business networks.
- Intranet: Private network used within an organization.
- Extranet: Controlled access to outsiders with specific permissions.
- Client-Server: Network model where one machine (server) provides resources to others (clients).
- Peer-to-Peer: All systems are equal, sharing resources directly with each other.

2. Network Topologies and Technologies

- Physical vs. Logical Topologies.
- Bus: All devices share a common backbone.
- Ring: Devices connected in a circular fashion.
- Star: Devices connected to a central device (typically a switch).
- Mesh: Devices are interconnected; offers high redundancy.
- Hybrid: Combination of two or more topologies.
- Ethernet: Wired LAN standard (IEEE 802.3).
- Wireless Standards: 802.11a/b/g/n/ac/ax (Wi-Fi generations).
- CSMA/CD and CSMA/CA: Media access control methods for Ethernet and Wi-Fi respectively.

3. Network Protocols and Ports

- Protocols: Set of rules for communication.
- TCP (Transmission Control Protocol): Connection-oriented, reliable delivery.
- UDP (User Datagram Protocol): Connectionless, fast but no guarantee of delivery.
- IP (Internet Protocol): Provides addressing and routing.
- ICMP: Used for diagnostics (e.g., ping).
- ARP: Resolves IP to MAC addresses.
- Common Ports: HTTP 80, HTTPS 443, FTP 21, SSH 22, DNS 53, DHCP 67/68, SMTP 25, POP3 110.

4. IP Addressing and Subnetting

- IPv4: 32-bit addressing (e.g., 192.168.1.1).
- IPv6: 128-bit addressing (e.g., 2001:0db8::1).
- Classes: A (1-126), B (128-191), C (192-223).
- CIDR Notation: e.g., /24 means 255.255.255.0.
- Subnetting: Dividing networks into smaller networks.
- Private IP Ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.
- Public IPs: Routable on the internet.

5. OSI and TCP/IP Models
- OSI: 7 Layers (Physical, Data Link, Network, Transport, Session, Presentation, Application).
- TCP/IP: 4 Layers (Network Interface, Internet, Transport, Application).
- Encapsulation: Wrapping data with protocol information at each layer.
- Devices and data units associated with each layer.

6. Networking Devices
- Hub: Basic device that broadcasts data.
- Switch: Operates at Layer 2, intelligent forwarding based on MAC.
- Router: Operates at Layer 3, forwards packets based on IP.
- Bridge: Connects two segments at Layer 2.
- Gateway: Translates between protocols.
- Firewall: Controls traffic based on rules.
- Access Point: Connects wireless clients to wired network.

7. Cabling and Connectors
- Copper Cable Types: UTP, STP.
- Fiber Optic: Single-mode, multi-mode.
- Coaxial: Used in cable internet.
- Connectors: RJ-45, RJ-11, LC, SC, ST.
- Wiring standards: T568A/B.

8. Wireless Networking
- Frequencies: 2.4 GHz (better range), 5 GHz (faster, less interference).
- Channels: Avoid overlap in 2.4GHz.
- Wireless Security: WEP (weak), WPA, WPA2, WPA3 (strongest).

- Authentication types: Open, PSK, Enterprise.

9. Network Services

- DHCP: Automatically assigns IP addresses.
- DNS: Resolves domain names to IP addresses.
- NAT: Translates private IPs to public.
- PAT: Port Address Translation.
- VPN: Secure tunnel over public network.
- Proxy: Acts as intermediary for requests.
- VLAN: Logically separates networks on the same switch.

10. Network Security Basics

- Threats: Phishing, Spoofing, DDoS, Malware.
- Security Devices: Firewalls, IDS (Intrusion Detection), IPS (Prevention).
- AAA: Authentication, Authorization, Accounting.
- Physical security: Locks, badges, video.
- Policies: Acceptable Use Policy (AUP), password policies.

11. Troubleshooting Methodology

1. Identify the problem.
2. Establish a theory of probable cause.
3. Test the theory.
4. Establish a plan of action.
5. Implement the solution.
6. Verify full system functionality.
7. Document findings.

12. Network Tools

- Cable Tester: Verifies wiring.
- Crimper: Attaches connectors to cables.
- Tone Generator and Probe: Traces cables.
- Multimeter: Electrical measurements.
- TDR/OTDR: Detects cable faults.
- Loopback Plug: Tests network interface.

- WiFi Analyzer: Diagnoses wireless signals.

--- END OF DETAILED NOTES ---