TELECOMMUNICATIONS AND NETWORK SECURITY

1. NETWORK ARCHITECTURE AND DESIGN
    - 1.1 Fundamental network concepts
        - a. Simplex, half-duplex, and full-duplex communication
        - b. LANs, WANs, MANs, and PANs
        - c. Internet, Intranet, and Extranet
    - 1.2 The OSI model
        - a. Layer 1: Physical
        - b. Layer 2: Data Link
        - c. Layer 3: Network
        - d. Layer 4: Transport
        - e. Layer 5: Session
        - f. Layer 6: Presentation
        - g. Layer 7: Application
    - 1.3 The TCP/IP model
        - a. Network Access Layer
        - b. Internet Layer
        - c. Host-to-Host Transport Layer
        - d. Application Layer
        - e. MAC addresses
            - EUI-64 MAC addresses
        - f. IPv4
        - g. IPv6
        - h. TCP
            - TCP ports
        - i. UDP
        - j. ICMP
    - 1.4 Application-Layer TCP/IP protocols and concepts
        - a. Telnet
        - b. FTP
        - c. SSH
        - d. SMTP, POP, and IMAP
        - e. DNS
        - f. HTTP and HTTPS
    - 1.5 LAN technologies and protocols
        - a. Ethernet
    - 1.6 WAN technologies and protocols
        - a. T1s, T3s, E1s, and E3s
        - b. Frame Relay
        - c. MPLS
2. NETWORK DEVICES AND PROTOCOLS
    - 2.1 Repeaters and hubs
    - 2.2 Bridges
    - 2.3 Switches
    - 2.4 Routers
    - 2.5 Firewalls
        - a. Packet filter
        - b. Stateful firewalls
        - c. Proxy firewalls

- Application-Layer Proxy firewalls

d. Modem

2.6 Intrusion Detection Systems and Intrusion Prevention Systems

2.7 Endpoint security

a. Antivirus

b. Application whitelisting

c. Removable media controls

d. Disk encryption

3. SECURE COMMUNICATIONS

3.1 Authentication protocols and frameworks

a. PAP and CHAP

b. 802.1X and EAP

3.2 VPN

a. PPP

b. IPsec

3.3 Remote meeting technology