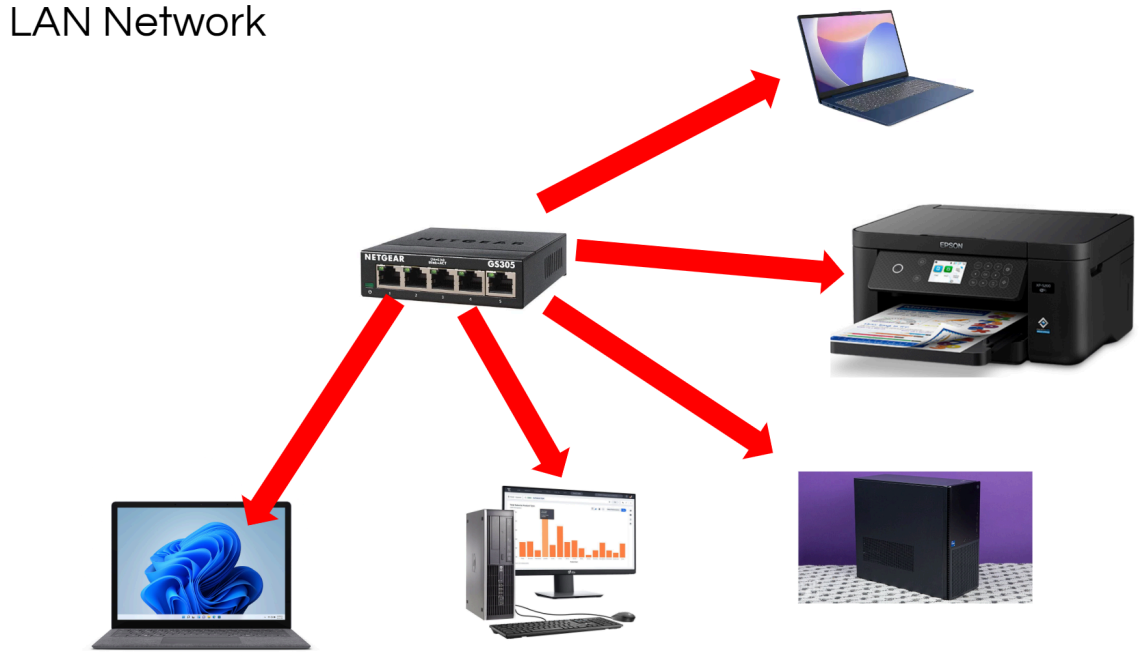
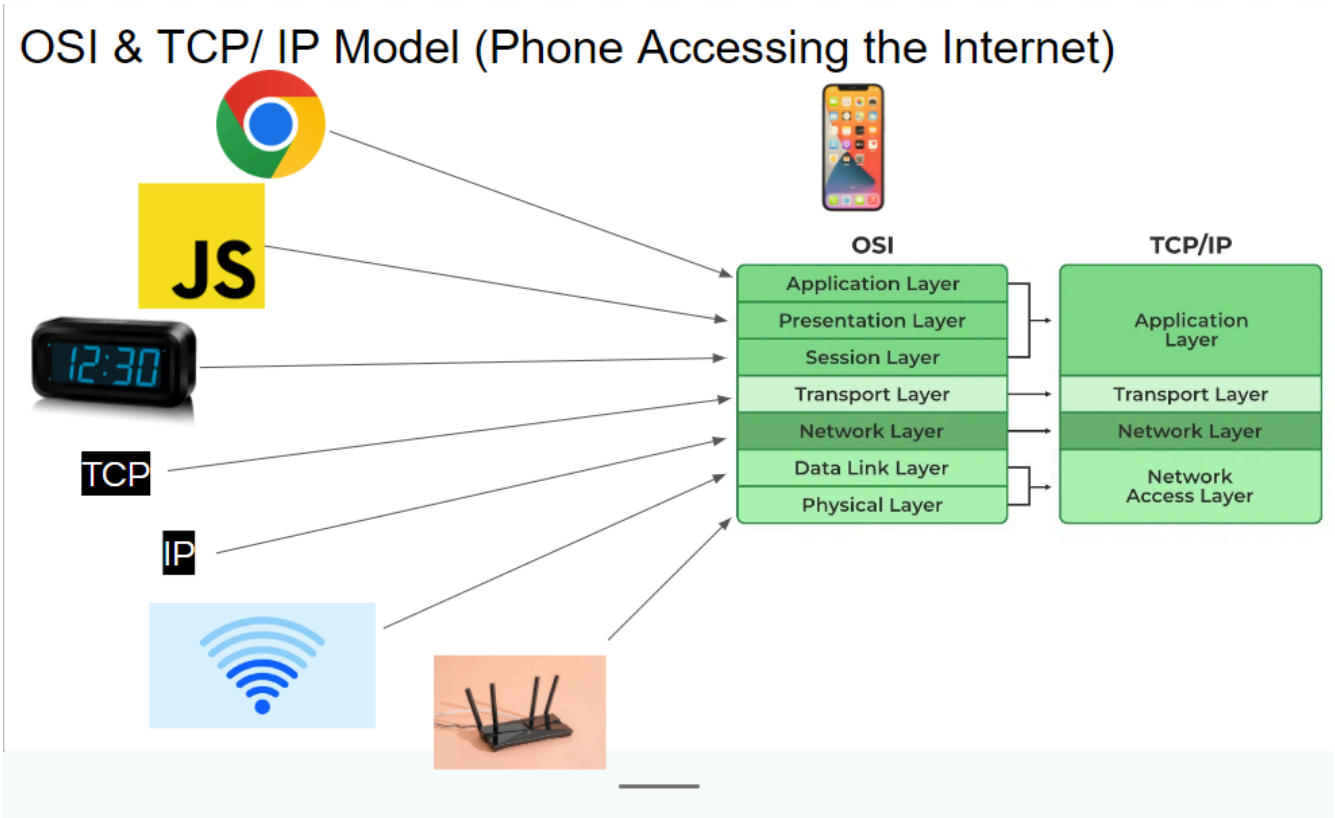
Network Topology



How This Topology Supports Network Management -
In this topology, a managed switch is being used to manage all of the devices contained within the LAN network. Managed switches are commonly used to enable centralized configuration, monitoring, and device management. An admin of this network is able to remotely control devices, send files, and distribute commands to the devices connected to this network. This network allows traffic monitoring, which enables secure communication within devices through early detection and troubleshooting.

Network Protocols and Architectures



Subnetting

Network Address: 172.25.144.0/21
Host Count: 50
Subnet Mask: /21 = 255.255.248.0
New Subnet Mask: /26 = 255.255.255.192
Subnet Range: 172.25.146.192 - 172.25.146.255
Network Address: 172.25.146.192
Broadcast Address: 172.25.146.255

Implement Network Security Fundamentals

Firewall Rule
Goal: Using Next-Generation Firewall, completely block access to X across this network.
Action: Deny
Protocol: Any
Source IP: 192.168.1.0/24 (Random IP)
Source Port: Any

Destination IP: 199.16.156.0/22
Destination Port: 80 or 443

IDS Configuration
Traffic Type: TCP
Source Port: 104.244.46.0/24
Destination Port: 104.244.46.0/24
Action: Creates an alert when traffic is detected on the X IP range
Message: “X Access Detected” is logged

IPS Configuration
Traffic Type: TCP
Source Port: 104.244.46.0/24
Destination Port: 104.244.46.0/24
Action: Blocks packets, preventing connection

Detected Event Example

IDS Example:
Twitter Access Detected - Source: 192.168.1.100 Destination: 8.25.194.20 Port: 443

IPS Example
Twitter Traffic Blocked - Source: 192.168.1.100 Destination: 8.25.194.20 Port: 443