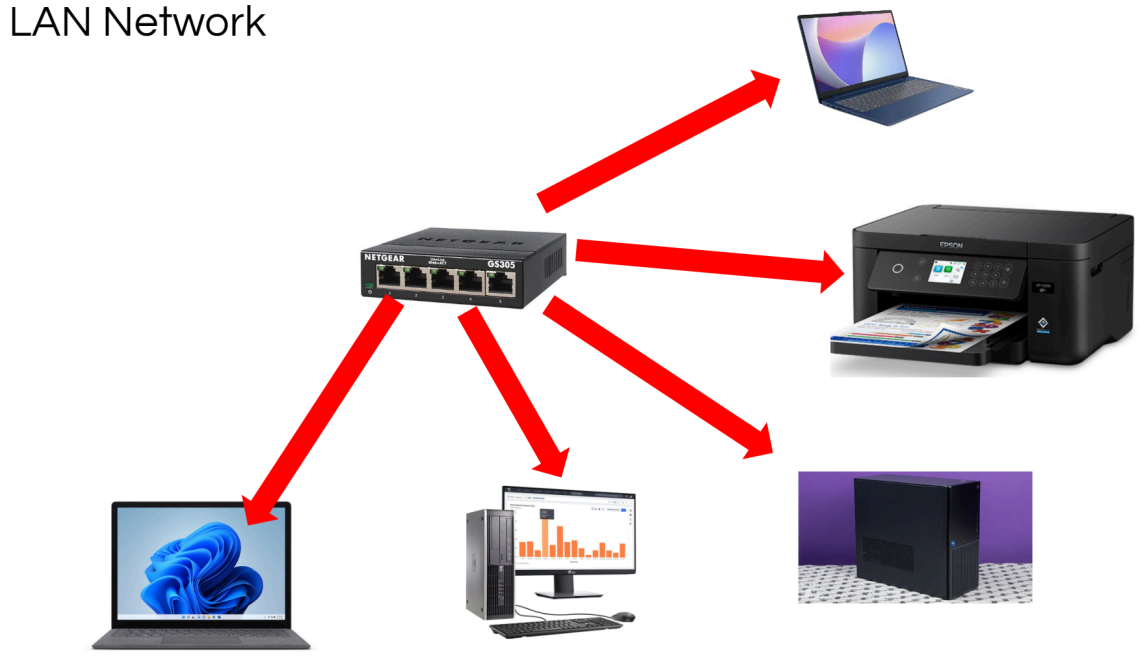
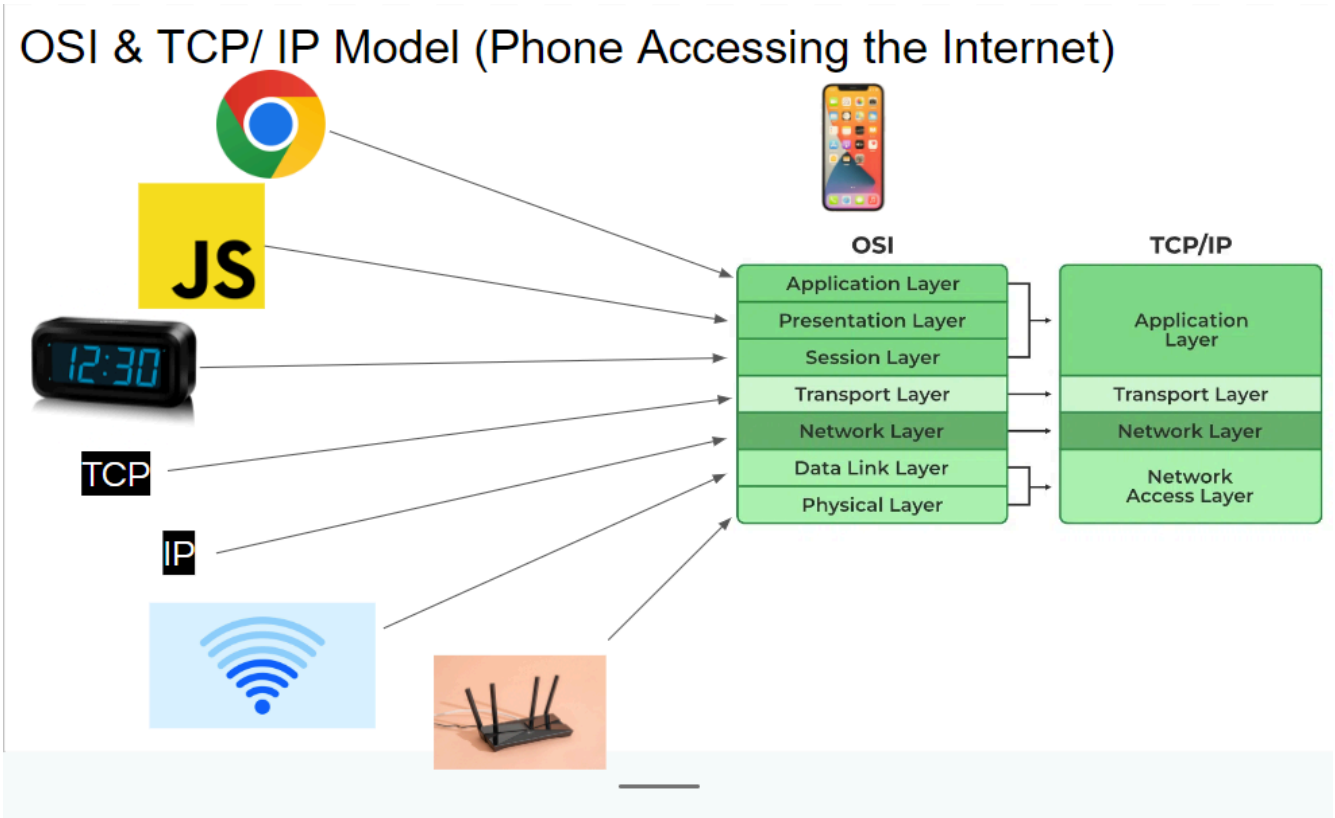
Network Topology



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

Access Control Measures

ACL Configuration

Device: Proxy Server
Protocol: HTTPS
Requirement: Filter traffic based on website/app certificate validation status

1) Enable SSL Certificate inspection/validation on the proxy server
2) Allow website with valid certificates
3) Deny websites with expired, untrusted, or unknown certificates

Access Control Model

Discretionary Access Control (DAC)

Access Control to Information: Through company ownership
Flexibility for Accessing Information: High
Access Complexity: Very Complex
Support for Multilevel Database System: No
System: Unix Based Systems

Steps

- For both Windows and Unix systems
- Restrict users from disabling SSL validation in their browsers
- Enforce SSL/TLS validation to prevent certificate warning from being ignored
- Create group policy for all machines

User Access Level

Employees

- Employees are limited to website with valid SSL/TLS Certificates
- Attempts to access untrusted websites are automatically blocked
- Employees log in through Single Sign-On using Google Workspace
- SSO Enforces strict certificate validation for accessing services and websites
- Access to resources are managed centrally
- All SSO login attempts are logged in a central location

Admins

- Admins are granted access to all websites
- Admins are allowed to bypass standard web filtering rules
- Must provide justification however
- Access to dangerous websites are automatically logged and reviewed
- Admin access is constantly monitored
- All activity are logged for maintaining accountability
- Admins authenticate via a different SSO System than employees
- Admins are required to use multiple types of MFA
- Some options include (Biometrics, Pins, Devices, Notifications)

Secure Wireless Networks

WPA 3 Configuration

Network SSID: Billyboy
Passphrase: S3cure@Net!2024
Firmware: Pfsense Firewall
Authentication Protocol: WPA3
Encryption Method: AES-GCMP/ AES - CCMP

Disable WPA2 to ensure WPA 3 works properly on the router

Wireless Intrusion Prevention System (WIPS) Configuration

- Set monitoring policies
- Block rogue access points
- Create a whitelist of authorized MAC addressed in a given network
- Detect and block attacks
- Enable detection for DoS attacks
- Set email alerts for unauthorized access attempts
- Keep logs in a centralized location

Utilize Network Security Tools

Wireshark Capture

Vulnerability Scanner Report

Network Penetration Testing Tool