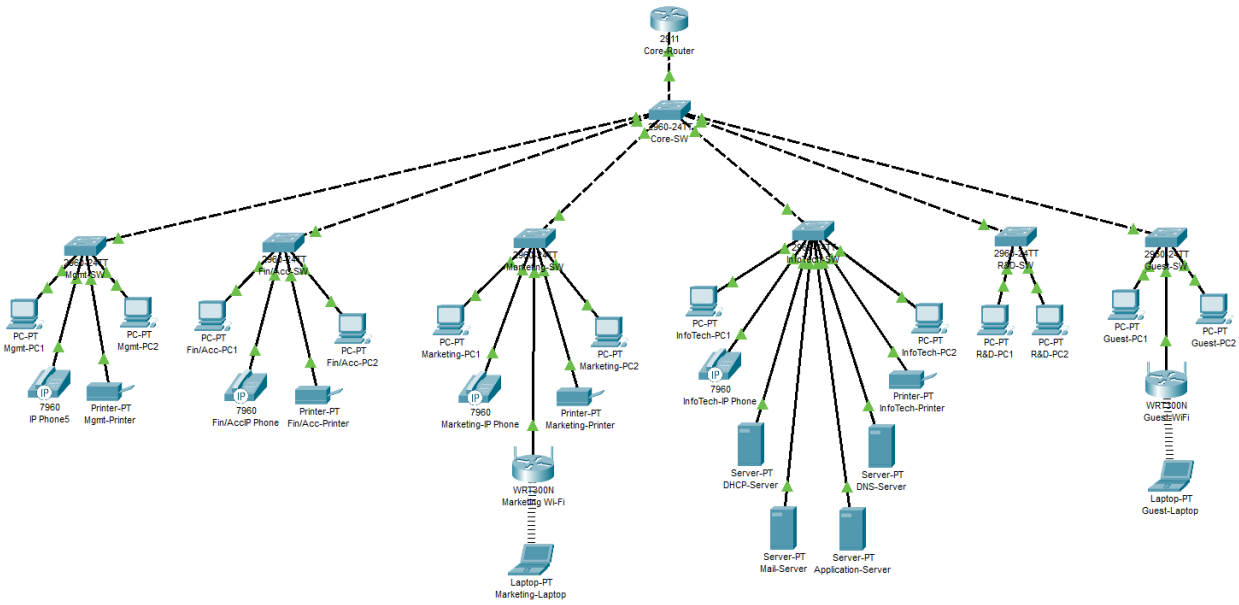
Title: Network Security Design Assignment

Subtitle: Secure and Resilient Network Design for a Small Company



Student Name: Ahndre Walters

Submission Date: March 9th, 2025

Declaration: I certify that this submission is my original work and complies with the guidelines for this assignment.

TABLE OF CONTENTS

Q1: **Firewall Rules**:

i. Deny pings from the internet
ii. Deny mail leaving R&D subnet
iii. Deny requests from internet to R&D
iv. Deny Guest VLAN access to all other VLANs
v. Allow DNS, DHCP, HTTP/HTTPS from all user VLANs to Server VLAN
vi. Deny IP phone VLAN access to the internet
vii. Allow only IT VLAN to SSH/Telnet into networking devices
viii. Deny inbound HTTP (port 80) from internet to internal VLANs
ix. Allow Finance VLAN to access App Server on port 443 only
x. Deny Marketing VLAN from communicating with R&D VLAN

Justification for mandatory rules:

a. **Deny pings from internet**: This blocks ICMP Echo Requests to prevent reconnaissance activities such as ping sweeps, which attackers use to identify active systems. Reducing response to pings limits visibility of the network from outside attackers.

b. **Deny mail leaving R&D**: R&D departments typically contain sensitive and proprietary data. Blocking outgoing mail prevents potential exfiltration of confidential information and helps enforce internal data handling policies.

c. **Deny internet requests to R&D**: Prevents direct access to the R&D VLAN from external sources, reducing the attack surface and exposure to malware or targeted threats. This is critical in safeguarding research data.

Q2: Department Printer/IP Phone Exceptions

- **Department 1 without printer or IP phone**: Guest
  Reason: Guest VLANs are designed for temporary and untrusted devices. Introducing permanent assets like printers or IP phones increases risk and exposure to internal threats. Devices in this VLAN are isolated by default.
- **Department 2 without printer or IP phone**: R&D
  Reason: R&D handles confidential intellectual property. Minimizing connected devices helps reduce attack vectors and ensures tighter data control. The focus is on minimal exposure.

Q3: Unique Device and Reason:

- **Unique device**: Wireless Router in Marketing Department
  Reason: Marketing requires flexibility for mobile devices, presentations, and client interaction. A dedicated wireless router supports these needs but must be properly firewalled and isolated from core networks to avoid lateral movement by potential threats.

Q4: Subnetting Details:

- **Number of subnets for /27 mask:** 8
- **Number of usable hosts on each subnet:** 30

Network ID address	First usable host IP address	Last usable host IB address	Broadcast IP address
192.168.40.0	192.168.40.1	192.168.40.30	192.168.40.31
192.168.40.32	192.168.40.33	192.168.40.62	192.168.40.63
192.168.40.64	192.168.40.65	192.168.40.94	192.168.40.95
192.168.40.96	192.168.40.97	192.168.40.126	192.168.40.127
192.168.40.128	192.168.40.129	192.168.40.158	192.168.40.159

These subnets are assigned per department, ensuring logical separation while leaving room for future growth.

Q5: Inter-Department Communication Strategies

1. **Access Control Lists (ACLs)**

   ACLs can restrict communication between departments by filtering traffic based on source/destination IP and port. For instance, IT can access all VLANs while Finance is restricted to accessing only the App Server.

2. **Router-on-a-Stick with Inter-VLAN Routing**

   A router with sub interfaces for each VLAN enables secure inter-VLAN communication. Combined with firewall rules and ACLs, this method maintains segmentation while allowing essential traffic.

3. **Authentication and Role-Based Access Control (RBAC)**

   Centralized authentication using RADIUS or TACACS+ ensures only authorized personnel access specific systems. Combined with logging and VLAN restrictions, it enforces security across departments.

Additional Required Elements Covered:

- **Segmentation**: All departments use distinct VLANs/subnets for isolation.
- **Scalability**: Subnetting with /27 supports 30 hosts per subnet and leaves room for growth.
- **Redundancy**: Design includes core router and switches with a modular layout for failover.
- **Servers**: Mail, DNS, DHCP, and App servers are logically placed in a dedicated Server VLAN.
- **Security vs Functionality**: Secure communication permitted only where business-critical; R&D and Guest are tightly isolated.
- **Packet Tracer verification**: All links functional with no errors (green arrows).
- P**rinter/IP Phone exclusions**: Justified exclusions for Guest and R&D departments.
- **Firewall rules**: All 10 rules implemented with sound technical and business rationale.
- **IP Addressing Plan**: Fully documented subnets and usable ranges per VLAN.