Project Documentation

Securing a Small Business Network

Submitted By:

Ahmed Elsayed
Saeed Mohamed
Mohamed Gamal
Martin Amgad
Mohamed Ashraf

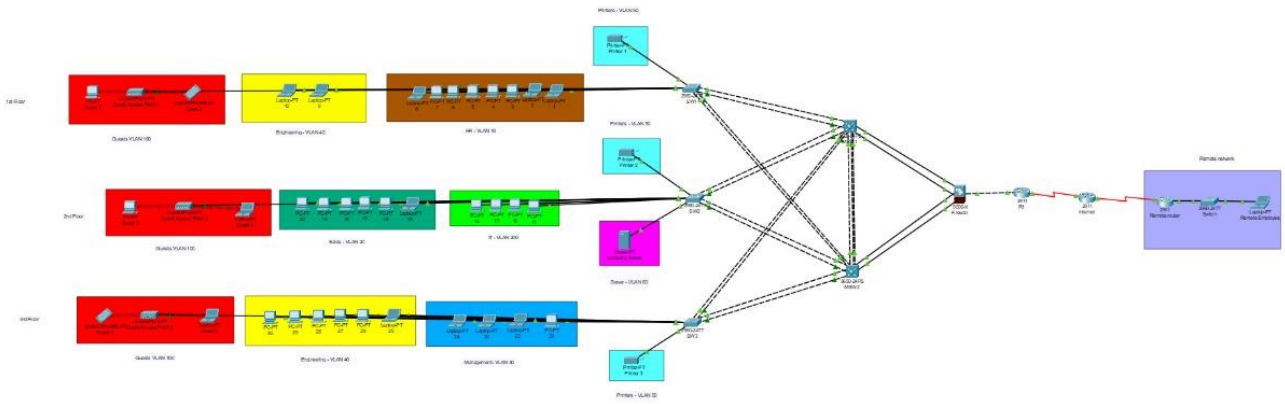
Under The Supervision Of :

Eng youssef selim

Project Overview:

This project focuses on designing, configuring, and securing a network for a small business with 30 employees. The network supports employee workstations, printers, a small server, and guest Wi-Fi. Critical requirements include secure remote access, network segmentation, and protection against cyber threats such as malware and unauthorized access.

Network Topology:



First Week: Network Design

The network topology consists of:

- **Router:**
  Connecting the internal network to the internet and providing routing services to the network.
- **Multilayer Switches (MSW1, MSW2):** Routing between VLANs and acting as distribution switches, supporting network segmentation.
- **Access Switches (SW1, SW2, SW3):** Connecting end devices such as employee workstations, printers, and servers.
- **Wireless Access Points:** Providing separate, but secure, Wi-Fi for both employees and guests.
- **Firewall:** Securing the internal network and controlling traffic between internal segments and the outside world.

Network Segments:

- **Employee Workstations:** Separated for departments like HR, Sales, Management, Engineering, IT.
- **Server Segment:** Hosting sensitive data and providing services like DHCP.
- **Guest Network:** Isolated from the internal network.

2. IP Addressing Scheme

- **Subnetting:** The network is divided into segments using VLANs. Each VLAN has its own IP address range to improve network segmentation and management.
  - HR: 192.168.0.0/27 ○ Sales:
  192.168.0.80/28 ○ Management:
  192.168.0.112/28 ○ Engineering:
  192.168.0.32/27 ○ Printers:
  192.168.0.96/28 ○ IT:
  192.168.0.64/28 ○ Guest
  Network: 192.168.1.0/24 ○
  Servers: 192.168.0.128 / 28

3. Security Measures

- **Firewall Rules:** Implemented to secure the network and block unauthorized access.
- **VPN:** Implemented for secure remote access.
- **Network Segmentation:** Ensured by using VLANs to separate traffic and improve security.

Second Week: Configuration and Implementation

1. Device Configuration

- **Routers and Switches (used protocols):**
  - Configured VLANs for different departments.
  - **VLAN Trunking Protocol (VTP):** Configured to manage VLANs. ○ **EtherChannel:** Configured for switch interconnection, enhancing redundancy.
  - **SSH:** Configured for secure management of network devices, ensuring encrypted communication during remote access to switches and routers. And a dedicated VLAN is configured for Access Switches to support SSH access.

○ **EtherChannel**: Aggregate multiple physical links into a single logical link to increase bandwidth and provide redundancy.

- **Spanning Tree (RSTP)**: Ensures a loop-free topology in the network. Utilized PortFast to reduce delays for end devices, and BPDU Guard to protect against misconfigurations. Defined primary and secondary root bridges to optimize traffic flow.
- **Switch Access Interfaces, Port-Security & DHCP Snooping:** Configured access interfaces for end devices. Applied port-security to limit MAC addresses per port, preventing unauthorized devices. Enabled DHCP snooping to ensure DHCP responses only come from trusted sources, preventing rogue servers.
- **SVIs (Switch Virtual Interfaces) & HSRP:** Implemented SVIs on MSW1 and MSW2 to route between VLANs, enabling inter-VLAN communication. Also configured HSRP for redundancy, allowing failover between the 2 multilayer switches to maintain network availability.
- **DHCP Relays:** Configured on MSW1 and MSW2 to forwarded DHCP requests from different VLANs to the dedicated DHCP server in VLAN 60, enabling dynamic IP assignment across the network.
- **OSPF (Open Shortest Path First):** Deployed OSPF as the routing protocol between MSW1, MSW2, Firewall, and Company Router to efficiently share routing information and dynamically adjust paths in case of network changes.
- **NAT (Network Address Translation):** Configured NAT (with 'overload' configuration) on Company router to translate private IP addresses to public addresses, enabling devices in the internal network to access the internet.

- **Access Control Lists (ACLs):** Applied on 2 MSWs to control traffic in the network and isolate guest network from accessing other network resources.
- **Firewall:** Configured to filter traffic between internal and external networks, using ACLs on inside and outside interfaces.

3. Secure Remote Access

- **VPN Configuration:**
    - Remote users access the network securely, with encryption ensuring the confidentiality of data.
    - User rights and access levels are properly configured on Firewall using ACLs to prevent unauthorized access and allow for VPN users to access the network.

Third Week: Security Implementation and Testing

1. Security Hardening

- Vulnerability Assessment is made by checking unsecure services and possible attacks like DDOS
- **Device Security:** Default passwords changed, and unnecessary services are disabled such as HTTP, FTP, and Telnet.
- **Port Security:** Configured to restrict devices that can connect to the network.
- **ACLs & Firewall:** Using ACLs, we could control the traffic inside the network and the traffic coming from outside. For example, disabled the "ICMP echo" requests coming from outside of the network.

Example Configuration: Port Security on Switch 1 for VLAN 10 (HR):

```
interface range f0/1-8
switchport mode access switch
access vlan 10 switchport port-
security
switchport port-security mac-address sticky switchport
port-security violation protect
```

Fourth Week: Documentation and Presentation

1. Network Documentation

The following documents were prepared:

- **Network Diagrams:** Illustrating the network topology with all components.
- **IP Addressing Scheme:** Subnetting details.
- **Device Configuration Files:** Including routers, switches, firewalls, and VPN setup.

2. Security Procedures

Security policies include:

- **Firewall Rules and VPN Configuration:**
To safeguard remote access and network communication.
- **Incident Response Plan:**
Steps to monitor, detect, and handle security breaches or suspicious activities.