Multinational School Network Architecture Design

This document details the network architecture design for a multinational school with two buildings. The design focuses on scalability, security, and efficient segmentation for various departments. It incorporates VLANs, inter-VLAN routing, OSPF, NAT, DNS, and essential security measures like port security, NTP, and syslog. The design also emphasizes future development and mitigation against potential threats.

team:

1 Tasneem Ashraf El-sayed Abdelrahman

2 Ahmed Mohamed Elsayed Metwally

3 Ahmed Maher Ragab El nagdy.

4 Muhammad Elsayed Muhammad Abdelaal.

5 Ahmed Zakria Attia Ibrahim

6 Mohamed Osama Mohamed Mohamed

Eng: Ayman Basha

Network Topology

1

Building A

Each building connects to a central distribution switch. This switch acts as the gateway for inter-VLAN routing and connects to the main router facilitating internet access.

2

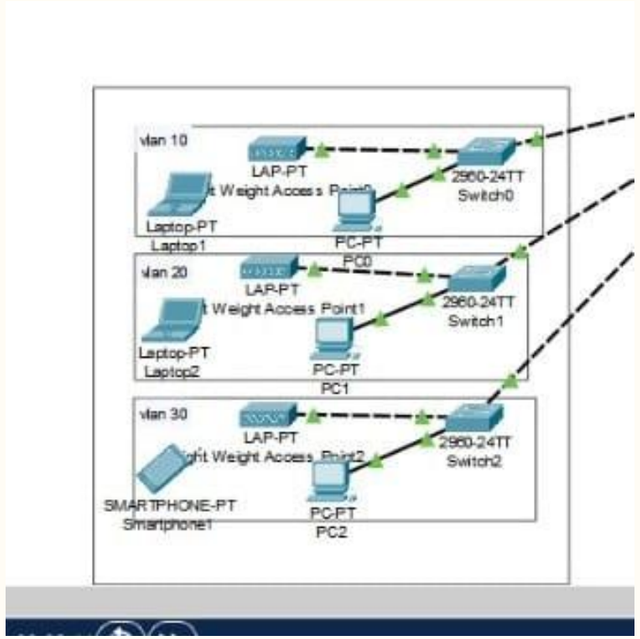
Building B

The topology mirrors Building A's setup, ensuring redundancy and load balancing between the two buildings.

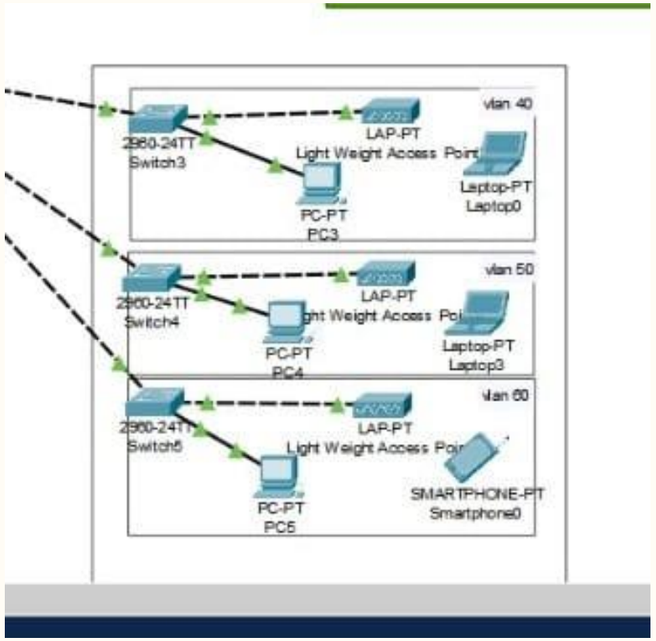
3

Internet & Servers

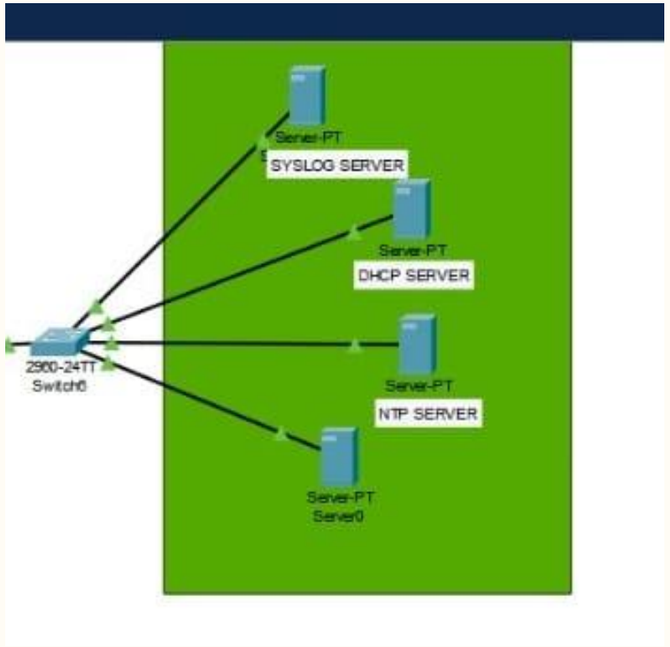
The main router connects to the internet and internal servers, including the web and DNS servers. Redundant internet connections are recommended for high availability.



Building 1



Building 2



Internet & Servers

IP Addressing and VLAN Segmentation

Building A	VLAN ID	Subnet	Department
A	10	192.168.10.0/24	HR
A	20	192.168.20.0/24	Teachers
A	30	192.168.30.0/24	Operations
Building B	VLAN ID	Subnet	Department
B	40	192.168.40.0/24	HR
B	50	192.168.50.0/24	Teachers
B	60	192.168.60.0/24	Operations

Inter-VLAN Routing and OSPF

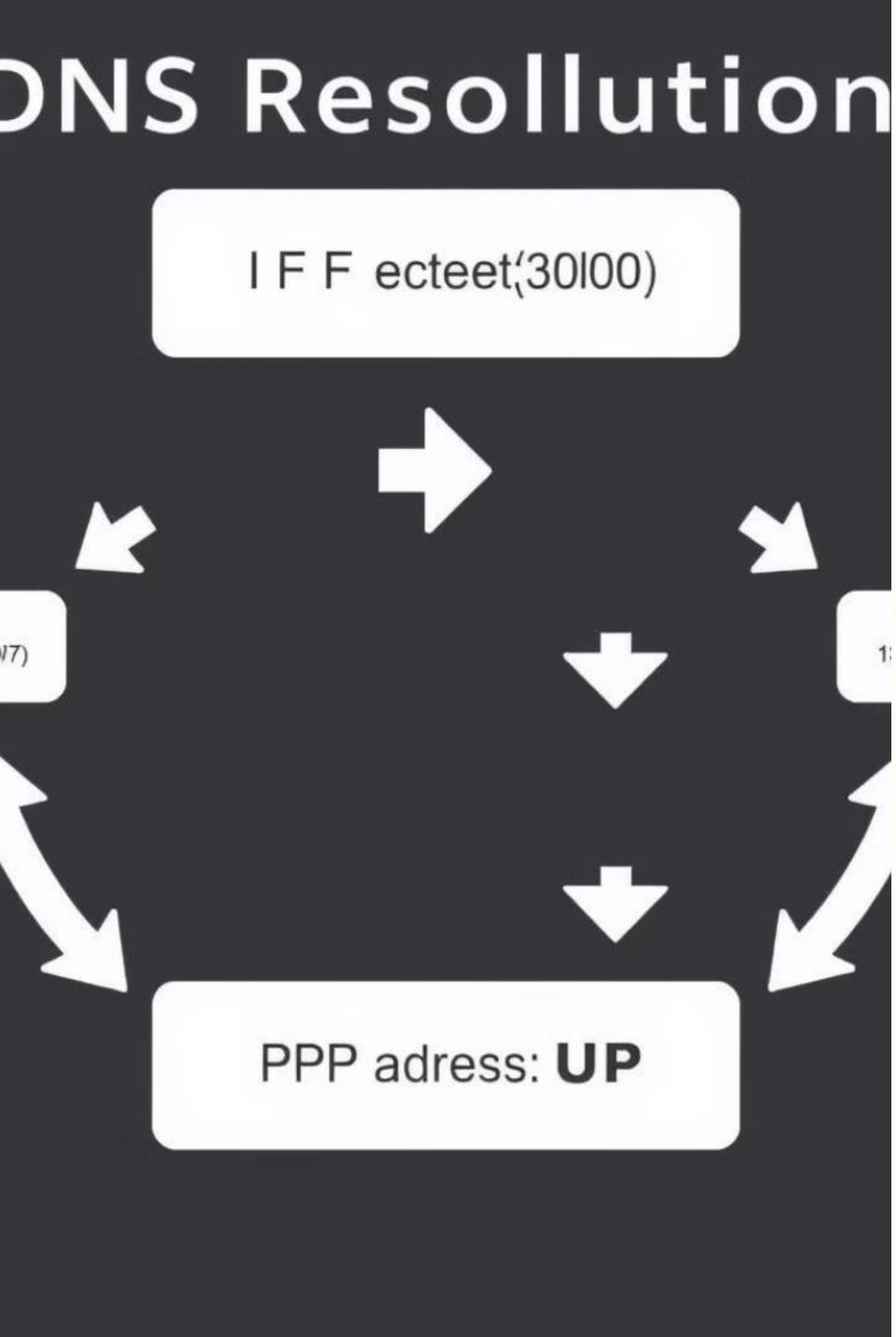
The core switch will act as a Layer 3 switch, performing inter-VLAN routing. OSPF (Open Shortest Path First) will be implemented to ensure dynamic routing between VLANs across both buildings. This provides redundancy and optimal path selection.

Web Server and Public IP

The school's web server will be hosted internally and assigned a private IP address (e.g., 192.168.70.10). A public IP address (e.g., 203.0.113.1) will be assigned to the school's main router. NAT (Network Address Translation) will translate internal private addresses to the public IP for internet access and vice versa.

Network Address Translation (NAT)

NAT will be configured on the main router to allow internal devices to access the internet using the school's public IP address. Port forwarding will be used to direct incoming traffic on port 80 (HTTP) and 443 (HTTPS) to the internal web server.



DNS Server Configuration

An internal DNS server will be configured to resolve internal hostnames and provide local DNS resolution. It will also forward external DNS requests to public DNS servers for internet name resolution. This improves name resolution speed and reduces reliance on external DNS.

Security Measures

1 Port Security

Port security will be implemented on all switches to restrict access based on MAC addresses, preventing unauthorized devices from connecting to the network.

2 NTP Server

An internal NTP server will synchronize the time on all network devices, ensuring accurate time stamps for logs and security events. This helps with accurate event correlation and analysis.

3 Syslog Server

A dedicated syslog server will collect logs from all network devices, providing centralized log management and analysis. This assists in identifying security threats, troubleshooting, and compliance reporting.

Connectivity Testing and Troubleshooting

Connectivity will be thoroughly tested using ping, traceroute, and other network diagnostic tools. Troubleshooting steps include checking cabling, verifying configurations, analyzing logs, and testing network connectivity from various points within the network. Detailed documentation of troubleshooting procedures will be maintained.

Recommendations for Future Development

Implement a robust firewall solution to control network access and protect against external threats. Regularly update firmware on all network devices to patch security vulnerabilities. Conduct periodic security audits and vulnerability assessments to proactively identify and mitigate security risks.