رواد مصر الرقمية

SECURE INTER-BRANCH COMMUNICATION

DEPI final project Cisco Cyber Secuirty Track

Our Team

1. Ahmed Ramadan Mohammed Al Muqaimy
2. Ahmed Nabawy Ahmed Ghorab
3. Islam Mahmoud Wahba Shalaby
4. Yousef Nabil Muhammad Sabry Shahin

Introduction

In this project, we designed a secure network connecting two branch offices in different countries. Each branch uses VLANs to organize internal traffic, and the branches are linked via a VPN tunnel for secure communication. OSPF routing was implemented to ensure efficient traffic flow, and Multilayer Switches were used to enhance performance by combining switching and routing functions. HSRP was applied for redundancy, ensuring network reliability, and a DHCP Server was set up to automate IP address assignment within the VLANs. This project highlights essential CCNA concepts such as VLANs, VPN, OSPF, DHCP, and network security.

Project Timeline

Phase 1 - Planning and Design

- Gather project requirements and define objectives.
- Design the network topology using VLANs to segment traffic between departments.
- Plan for routing using OSPF to ensure efficient communication between branches.
- Identify VPN tunneling needs for secure inter-branch communication.
- Plan for NAT to manage IP address translation and ensure proper internal/external communication.

Project Timeline

Phase 2 - VLAN and OSPF Configuration:

- Configure VLANs to segment the network into different logical domains.
- Set up OSPF for dynamic routing between branch offices, ensuring optimal path selection.
- Verify communication between VLANs within each branch.

Project Timeline

Phase 3 - VPN and NAT Setup

- Establish a VPN tunnel between the two branches to secure data transmission.
- Configure NAT (Network Address Translation) to allow internal devices to communicate with external networks while hiding internal IP addresses.
- Test the VPN connection to ensure secure communication and verify NAT functionality.

Project Timeline

Phase 4 - Port Security and Network Optimization

- Implement Port Security on switches to limit the number of devices connected to each port, preventing unauthorized access.
- Test the Port Security configurations to ensure compliance with security policies.
- Optimize OSPF routing and verify the security of the VPN tunnel.

Project Timeline

Phase 5 - Final Testing and Deployment

- Conduct comprehensive testing of the entire network, including VLANs, OSPF, NAT, VPN, and Port Security.
- Troubleshoot and resolve any remaining issues.
- Finalize the network setup and prepare documentation for project delivery.

Problems

During the implementation of our project, we encountered several challenges, including:

OSPF Configuration Issues

- We faced difficulties in properly configuring the OSPF protocol, which impacted the routing between the branch offices.

Problems

During the implementation of our project, we encountered several challenges, including:

NAT Configuration Challenges

- Configuring Network Address Translation (NAT) presented some obstacles, particularly in ensuring proper IP address translations between internal and external networks.

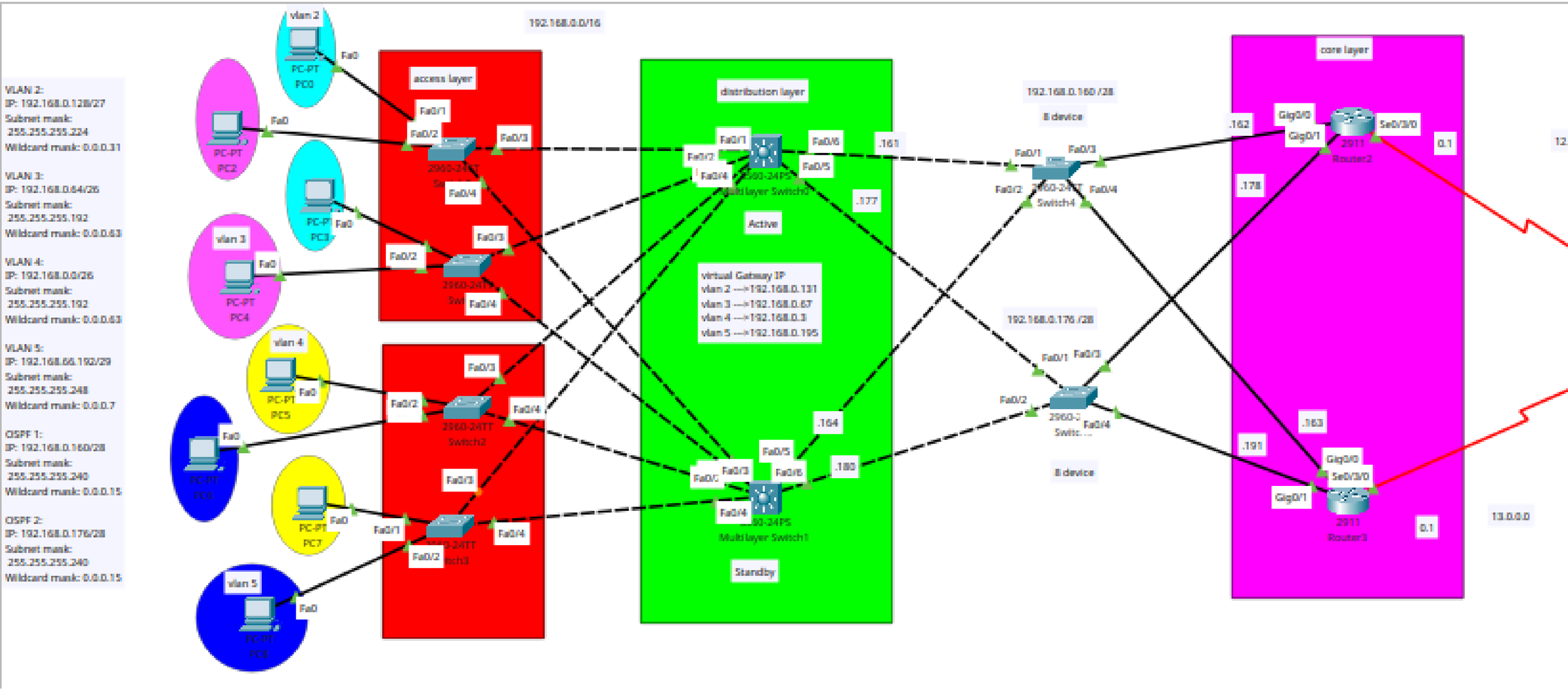
Problems

During the implementation of our project, we encountered several challenges, including:

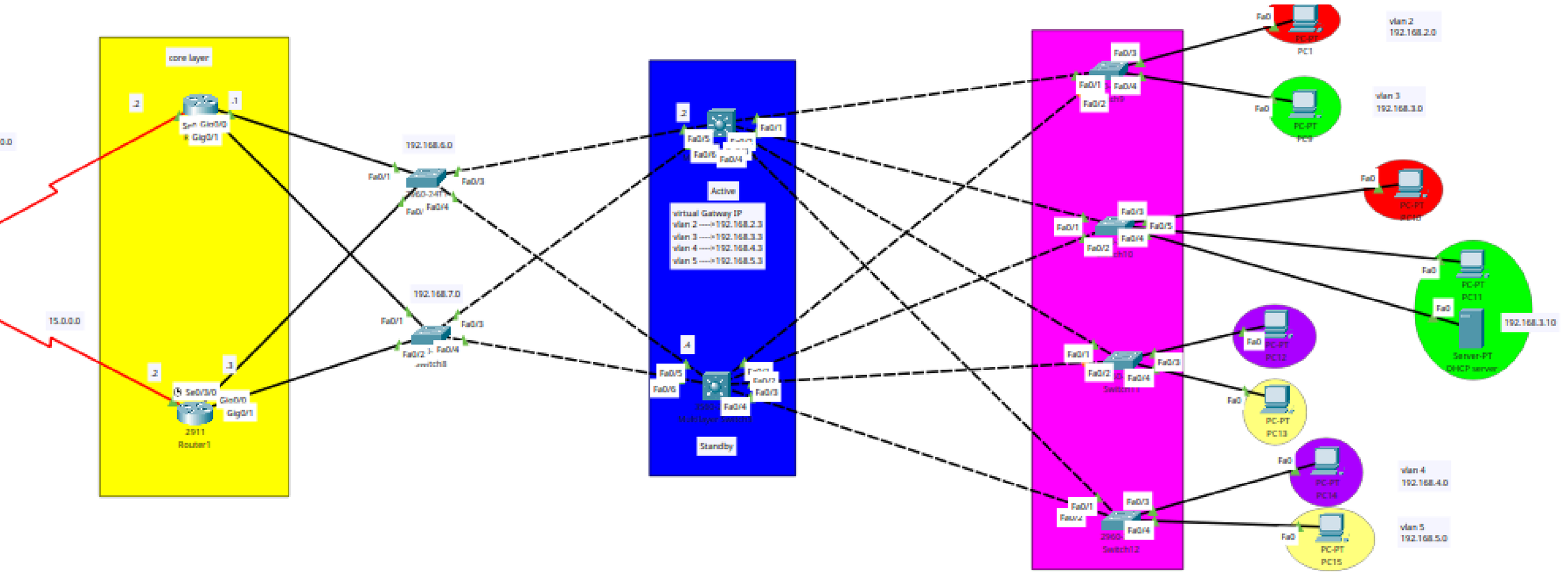
VPN Tunneling Problems

- We encountered issues with establishing and maintaining the VPN tunnel, which affected secure communication between the branches.

Branch 1 Topology


VLAN 2:
IP: 192.168.0.128/27
Subnet mask:
.255.255.255.224
Wildcard mask: 0.0.0.31
VLAN 3:
IP: 192.168.0.64/26
Subnet mask:
.255.255.255.192
Wildcard mask: 0.0.0.63
VLAN 4:
IP: 192.168.0.0/26
Subnet mask:
.255.255.255.192
Wildcard mask: 0.0.0.63
VLAN 5:
IP: 192.168.66.192/29
Subnet mask:
.255.255.255.248
Wildcard mask: 0.0.0.7
OSPF 1:
IP: 192.168.0.160/28
Subnet mask:
.255.255.255.240
Wildcard mask: 0.0.0.15
OSPF 2:
IP: 192.168.0.176/28
Subnet mask:
.255.255.255.240
Wildcard mask: 0.0.0.15
192.168.0.0/16
access layer
distribution layer
core layer
192.168.0.160 /28
8 device
192.168.0.176 /28
8 device
vlan 2
vlan 3
vlan 4
vlan 5
PC-PT PC0
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
PC-PT PC6
PC-PT PC7
PC-PT PC8
Fa0
Fa0/1
Fa0/2
Fa0/3
Fa0/4
Fa0/5
Fa0/6
2960-24TT
Switch2
Switch4
2960-24PS
Multi layer Switch2
Multi layer Switch1
Active
Standby
virtual Gateway IP
vlan 2 ---->192.168.0.131
vlan 3 ---->192.168.0.67
vlan 4 ---->192.168.0.3
vlan 5 ---->192.168.0.195
.161
.177
.164
.180
.162
.178
.163
.191
Gig0/0
Gig0/1
Se0/3/0
2911
Router2
Router3
0.1
13.0.0.0

Branch 2 Topology


core layer
.2
.1
Gig0/1
.2
.3
Se0/3/0
Gig0/0
Gig0/1
2911
Router1
15.0.0.0
192.168.6.0
Fa0/1
Fa0/3
Fa0/4
192.168.7.0
Fa0/1
Fa0/3
Fa0/4
.2
Fa0/5
Fa0/6
Fa0/1
Fa0/4
Active
virtual Gatway IP
vlan 2 ----->192.168.2.3
vlan 3 ----->192.168.3.3
vlan 4 ----->192.168.4.3
vlan 5 ----->192.168.5.3
.4
Fa0/5
Fa0/6
Fa0/3
Fa0/4
Standby
Fa0/3
Fa0/1
Fa0/4
Fa0/2
Fa0/3
Fa0/1
Fa0/5
Fa0/2
Fa0/4
Fa0/3
Fa0/1
Fa0/3
Fa0/2
Fa0/4
Fa0/3
Fa0/1
Fa0/3
Fa0/4
Fa0
PC-PT
PC1
vlan 2
192.168.2.0
Fa0
PC-PT
PC9
vlan 3
192.168.3.0
Fa0
PC-PT
PC10
Fa0
PC-PT
PC11
Fa0
Server-PT
DHCP server
192.168.3.10
Fa0
PC-PT
PC12
Fa0
PC-PT
PC13
Fa0
PC-PT
PC14
vlan 4
192.168.4.0
Fa0
PC-PT
PC15
vlan 5
192.168.5.0

THANK YOU