

Secure Enterprise Network with VLAN, NAT & Simulated ISP

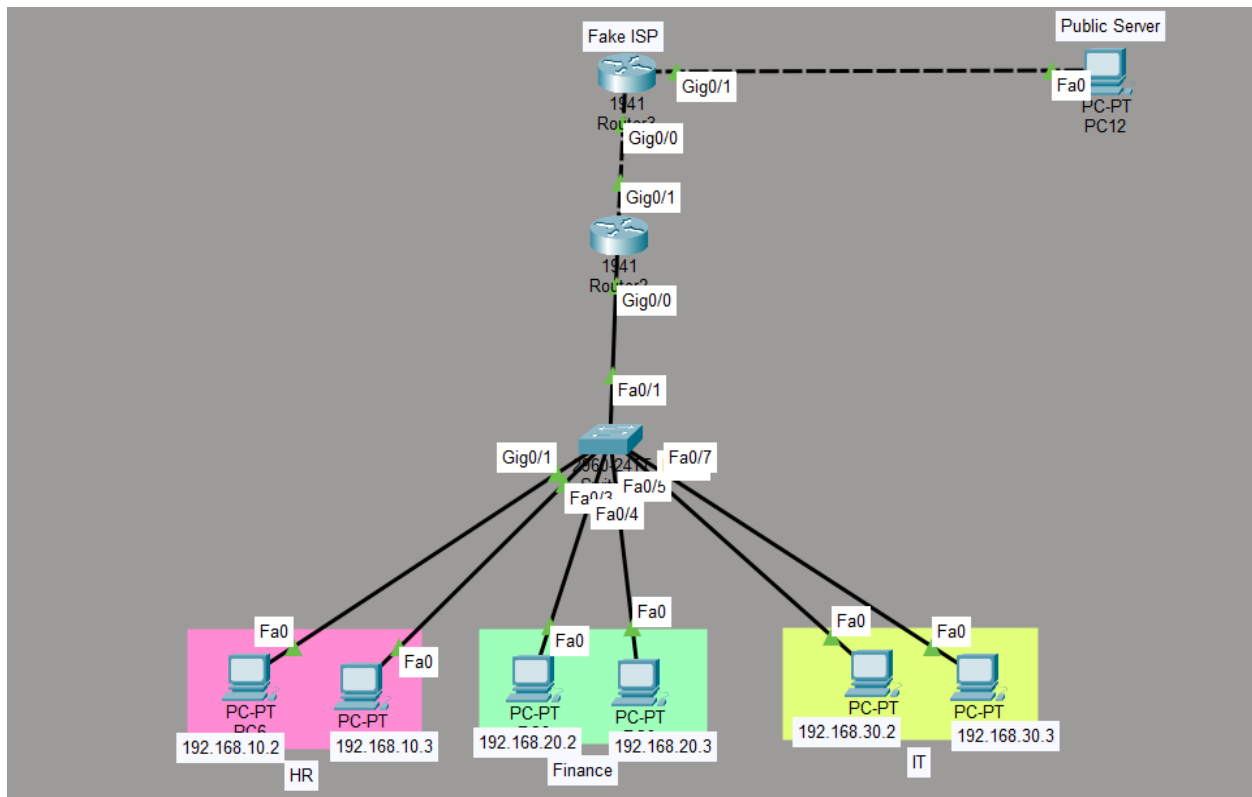
Name : M.A Jesowin Raja

Tools used : Cisco Packet Tracer

Project Objective:

The objective of this project is to design and implement a secure enterprise network using VLAN segmentation, inter-VLAN routing, and NAT to simulate real-world internet connectivity.

Network Architecture Diagram:



IP Addressing Table:

Department	VLAN	Network	Gateway
HR	10	192.168.10.0/24	192.168.10.1
IT	20	192.168.20.0/24	192.168.20.1
Finance	30	192.168.30.0/24	192.168.30.1

WAN Network:

200.0.0.0/30

Public Network:

8.8.8.0/24

Implementation Steps:

1. VLAN creation
2. Access port configuration
3. Trunk configuration
4. Router subinterface creation
5. Inter-VLAN routing
6. NAT configuration
7. ISP simulation setup
8. Public server configuration

Packet Flow Explanation:

1. PC sends request
2. Router translates IP
3. ISP forwards packet
4. Server replies
5. NAT reverses translation

Security Features:

- VLAN segmentation
- Network isolation
- NAT for IP masking
- Controlled inter-VLAN routing

Troubleshooting Commands Used:

- show ip route
- show ip nat translations
- show access-lists
- show ip interface brief

Conclusion:

This project demonstrates practical implementation of enterprise network architecture with security-focused segmentation and internet simulation. It strengthened my understanding of VLANs, NAT, routing, and network troubleshooting.