Enterprise Campus Network Design Using Cisco Packet Tracer

Irfan Hameed

July 16, 2025

Objective

To design and implement an enterprise-grade campus network using Cisco Packet Tracer that demonstrates industry-standard configurations including routing, switching, redundancy, security, and remote management.

Tools Used

- Cisco Packet Tracer
- VLSM IP Addressing
- DHCP, DNS, FTP, Email, Syslog, NTP Servers
- HSRP for gateway redundancy
- NAT, ACLs, Port Security
- SSH, AAA (TACACS+)

Network Topology Overview

- Multiple VLANs for HR, IT, Finance, and Server Departments
- Two routers configured for HSRP
- Two Layer 2 switches for segmentation and access
- Cloud connected via NAT to simulate internet access
- Centralized server for multiple services

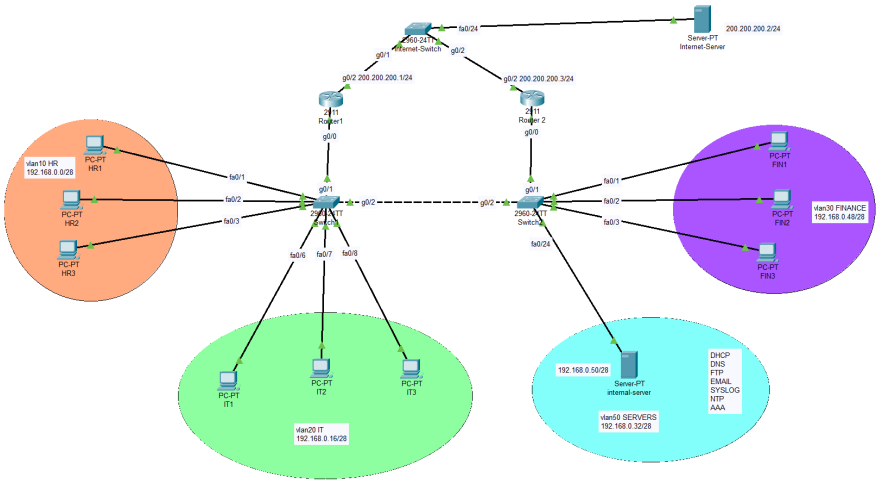

Figure 1: Enterprise Network Topology with VLANs, Routers, and Servers

VLAN and IP Subnet Plan (VLSM)

Department	VLAN ID	IP Range	Subnet Mask
HR	10	192.168.0.0 - 192.168.0.15	/28
IT	20	192.168.0.16 - 192.168.0.31	/28
Finance	30	192.168.0.32 - 192.168.0.47	/28
Server	50	192.168.0.48 - 192.168.0.63	/28

Router Configuration Overview

Router on a Stick

- Subinterfaces configured for inter-VLAN routing
- DHCP relay enabled using `ip helper-address`

HSRP Configuration

```
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 192.168.0.1 255.255.255.240
standby 10 ip 192.168.0.2
standby 10 priority 110
standby 10 preempt
```

NAT Configuration

```
interface GigabitEthernet0/2
 ip nat outside
```

```
interface GigabitEthernet0/0 subinterfaces
 ip nat inside

ip nat inside source list 1 interface GigabitEthernet0/2 overload
access-list 1 permit 192.168.0.0 0.0.0.255
```

DHCP Configuration (on Server)

```
ip dhcp excluded-address 192.168.0.1 192.168.0.2
ip dhcp pool HR
 network 192.168.0.0 255.255.255.240
 default-router 192.168.0.2 (virtual ip)
 dns-server 192.168.0.50
```

ACL Configuration (HR-FILTER)

```
ip access-list extended HR_FILTER
deny ip 192.168.0.0 0.0.0.15 192.168.0.16 0.0.0.15
deny ip 192.168.0.0 0.0.0.15 192.168.0.32 0.0.0.15
permit ip 192.168.0.0 0.0.0.15 any
interface GigabitEthernet0/1.10
 ip access-group HR_FILTER in
```

AAA + SSH Configuration

```
ip domain-name company.local
crypto key generate rsa
username admin privilege 15 secret admin321

line con 0
 login authentication TACACS_LINE

line vty 0 4
 login authentication SSH_AUTHEN
 transport input ssh

ip ssh version 2
aaa new-model
aaa authentication login SSH_AUTHEN group tacacs+ local
aaa authentication login TACACS_LINE group tacacs+ local
tacacs-server host 192.168.0.50 key cisco321
```

Switch Configuration Overview

- VLAN creation and trunking

- PortFast and BPDU Guard enabled on access ports
- SSH configured for remote access
- Port Security to limit MAC addresses on access ports

Server Configuration

- DHCP Server with excluded IPs
- DNS server resolving internal names
- FTP and Email services for testing
- Syslog server to receive router logs
- TACACS+ AAA server for centralized login
- NTP server for time synchronization

Security Features Implemented

- ACLs for department-level access control
- HSRP for gateway redundancy
- NAT to simulate public internet access
- Port Security on access ports
- Remote management using SSH with AAA
- Syslog for monitoring

Access Control Lists (ACLs)

Example: HR-FILTER ACL

```
ip access-list extended HR-FILTER
 deny ip 192.168.0.0 0.0.0.15 192.168.0.16 0.0.0.15
 deny ip 192.168.0.0 0.0.0.15 192.168.0.32 0.0.0.15
 permit ip 192.168.0.0 0.0.0.15 any
```

Testing and Verification

- Ping and traceroute tests across VLANs
- HSRP failover testing
- DHCP address assignment verification
- ACL behavior tested with successful and denied pings
- SSH tested using PC terminal
- Logs verified on Syslog server

Challenges and Troubleshooting Experience

During this project, I encountered several real-world challenges that enhanced my problem-solving and troubleshooting skills.

DHCP Issue due to ACL Conflict

At one stage, DHCP stopped working and end devices were not receiving IP addresses. I verified all DHCP pool configurations, interface settings, and helper addresses — but the issue persisted.

To isolate the problem, I simulated DHCP traffic using Packet Tracer's simulation mode and discovered that the DHCP OFFER packet was being blocked.

The root cause: an extended ACL applied on the router interface was denying UDP broadcasts from DHCP. After modifying the ACL to allow necessary DHCP traffic (UDP ports 67 and 68), the issue was resolved.

This experience taught me:

- How to use simulation mode for protocol-level debugging
- How ACLs can unintentionally block critical services
- The importance of iterative testing and verification

Conclusion

This project simulates a robust enterprise network with realistic configurations used in real-world IT environments. It demonstrates key concepts such as segmentation, security, redundancy, and remote management — making it a strong portfolio piece for entry-level roles in network support, system administration, or cybersecurity.