

Computer Networking Final Project Documentation

Project Overview

This final project involved the planning, configuration, and testing of a comprehensive multi-department enterprise network using Cisco Packet Tracer. The network includes multiple VLANs across three sections, routing through a mix of routers and Layer 3 switches, server services, DHCP, ACLs, NAT, Wi-Fi, and security protocols such as SSH.

Network Design Summary

- 3 main routers (Router0, Router1, Router2)
- 3 Layer 3 switches (one per section)
- 7 Layer 2 switches (including dedicated ones for server room and departments)
- Multiple end devices (PCs, laptops, IP phones, access points, printers)
- Separate VLANs for each department:
 - VLAN 10: Admin
 - VLAN 20: HR
 - VLAN 30: Finance
 - VLAN 40: Sales
 - VLAN 50: R&D
 - VLAN 60: Support
 - VLAN 99: Server Room
 - VLAN 150: Voice
 - VLAN 100: WAN Links

IP Addressing Scheme Highlights

- Subnets were carefully allocated using /27 ranges per VLAN
- WAN links used a /28 subnet in the 192.168.100.200 range
- Voice and Server Room services share adjacent subnets in the 192.168.100.224/27 range
- All gateways were assigned the first usable IP of each subnet

Routing

- **RIP Version 2** was used across all routers and L3 switches for dynamic routing
- **Static routes** were only used in specific cases (e.g., early server access)

Services Configured

- **DHCP:** Centralized DHCP server located in the Server Room, delivering dynamic IPs to all VLANs using ip helper-address
- **DNS, Web, FTP, and Email Servers:** All configured with static IPs and verified through pings

VoIP (Not Implemented)

Although a Call Manager Express (CME) router was placed and partially configured, VoIP setup was not completed due to ongoing registration issues with IP phones despite proper DHCP and routing. A working VoIP example using a smaller network was created and included separately to demonstrate understanding of CME and IP phone registration.

ACL & Security Configuration

To enhance security and control access within the network, four Access Control Lists (ACLs) were configured to fulfill project requirements and demonstrate security control at various layers of the topology.

ACL 1 – SSH Restriction

Only devices from the Admin VLAN (VLAN 10) are permitted to establish SSH sessions with network devices.

- **ACL Name:** SSH_ONLY_ADMIN
- **Applied on:** All routers, inbound on line vty 0 4

```
ip access-list extended SSH_ONLY_ADMIN
permit tcp 192.168.100.0 0.0.0.31 any eq 22
deny tcp any any eq 22
```

permit ip any any

ACL 2 – Server Room Protection

Only Admin VLAN is allowed to access resources in the Server Room (VLAN 99). All other VLANs are denied access.

- **ACL Name:** PROTECT_SERVERS
- **Applied on:** Router0, inbound on GigabitEthernet0/0/1

```
ip access-list extended PROTECT_SERVERS
permit ip 192.168.100.0 0.0.0.31 192.168.100.224 0.0.0.15
deny ip any 192.168.100.224 0.0.0.15
permit ip any any
```

ACL 3 – Inter-VLAN Control

HR (VLAN 20) is blocked from communicating with Finance (VLAN 30), but Admin is allowed.

- **ACL Name:** BLOCK_HR_TO_FINANCE
- **Applied on:** L3_Switch0, inbound on Vlan20

```
ip access-list extended BLOCK_HR_TO_FINANCE
deny ip 192.168.100.32 0.0.0.31 192.168.100.64 0.0.0.31
permit ip any any
```

ACL 4 – Internet Access Filtering (NAT Restriction)

Only Admin and R&D VLANs are allowed to access the internet. Others are denied by omission.








- **ACL Name:** Standard ACL 1
- **Applied on:** Router2 NAT config

```
access-list 1 permit 192.168.100.0 0.0.0.31
access-list 1 permit 192.168.100.128 0.0.0.31
ip nat inside source list 1 interface GigabitEthernet0/0/0 overload
```

```
interface GigabitEthernet0/0/1
ip nat inside
```

```
interface GigabitEthernet0/0/0
ip nat outside
```

Functionality Test Summary

-  Admin PCs can SSH into all routers
-  Admin PCs can reach Server VLAN (VLAN 99)
-  HR PCs cannot reach Server VLAN (blocked)
-  HR PCs cannot reach Finance
-  Admin PCs can reach Finance
-  Admin & R&D PCs can ping 8.8.8.8 (internet access via NAT)
-  HR, Sales, and Support PCs cannot access the internet

Conclusion

The network was designed and implemented to simulate a real-world enterprise scenario. All VLANs, routing protocols, NAT, DHCP, ACLs, and Wi-Fi were configured and tested successfully. The only component not completed was VoIP integration; however, it was tested separately in a lab environment to demonstrate understanding. This project showcases complete network segmentation, internal security control, and internet access management across a multi-tier architecture.

During the final stages of testing, I encountered an issue where DHCP failed to assign IP addresses to devices in VLAN 20 (HR), despite having a functioning DHCP server, correctly configured pools, and operational DHCP across all other VLANs. After extensive troubleshooting — including verifying trunk links, IP helper addresses, ACLs, and routing paths — the issue persisted only in VLAN 20.

To ensure continuity and network functionality, I configured static IP addresses for all devices in VLAN 20 that would have otherwise received DHCP leases. While DHCP continues to operate normally in all other VLANs, this workaround allowed me to complete the project with full connectivity and functionality for the HR department.

I plan to further investigate this VLAN-specific issue separately, but for the purposes of this project, the static configuration ensures reliable performance and meets the functional requirements.

Overall not the result I wanted but I ended up not prioritizing this as much over my other finals so didn't get the result I wanted. I will look up more stuff and hopefully get some hands-on experience because Cisco Packet Tracer has some weird limitations that annoyed me.

Pings:

Admin PC to HR PC

```
C:\>ping 192.168.100.37

Pinging 192.168.100.37 with 32 bytes of data:

Reply from 192.168.100.37: bytes=32 time<1ms TTL=127
Reply from 192.168.100.37: bytes=32 time<1ms TTL=127
Reply from 192.168.100.37: bytes=32 time<1ms TTL=127
Reply from 192.168.100.37: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Finance to Sales

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=4ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>|
```

Support to R&D

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.133

Pinging 192.168.100.133 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.133: bytes=32 time=15ms TTL=127
Reply from 192.168.100.133: bytes=32 time<1ms TTL=127
Reply from 192.168.100.133: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.133:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 5ms

```

Pc to Printer in own vlan

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.34

Pinging 192.168.100.34 with 32 bytes of data:

Reply from 192.168.100.34: bytes=32 time<1ms TTL=128
Reply from 192.168.100.34: bytes=32 time<1ms TTL=128
Reply from 192.168.100.34: bytes=32 time<1ms TTL=128
Reply from 192.168.100.34: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Pc to DHCP Server

```

C:\>ping 192.168.100.226

Pinging 192.168.100.226 with 32 bytes of data:

Reply from 192.168.100.226: bytes=32 time=2ms TTL=124
Reply from 192.168.100.226: bytes=32 time=11ms TTL=124
Reply from 192.168.100.226: bytes=32 time=13ms TTL=124
Reply from 192.168.100.226: bytes=32 time=17ms TTL=124

Ping statistics for 192.168.100.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 10ms

```

PC to DNS server

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.227

Pinging 192.168.100.227 with 32 bytes of data:

Request timed out.
Reply from 192.168.100.227: bytes=32 time=16ms TTL=124
Reply from 192.168.100.227: bytes=32 time=8ms TTL=124
Reply from 192.168.100.227: bytes=32 time=10ms TTL=124

Ping statistics for 192.168.100.227:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 16ms, Average = 11ms
C:\>

```

PC to Router

```
C:\>ping 192.168.100.201

Pinging 192.168.100.201 with 32 bytes of data:

Reply from 192.168.100.201: bytes=32 time=6ms TTL=254
Reply from 192.168.100.201: bytes=32 time=4ms TTL=254
Reply from 192.168.100.201: bytes=32 time<1ms TTL=254
Reply from 192.168.100.201: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.100.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 2ms
```

PC to Internet

```
C:\>ping 8.8.8.9

Pinging 8.8.8.9 with 32 bytes of data:

Reply from 8.8.8.9: bytes=32 time=4ms TTL=123
Reply from 8.8.8.9: bytes=32 time=5ms TTL=123
Reply from 8.8.8.9: bytes=32 time=9ms TTL=123
Reply from 8.8.8.9: bytes=32 time=14ms TTL=123

Ping statistics for 8.8.8.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 14ms, Average = 8ms
```

NAT Translations

```
Router2#show ip nat translations

Pro Inside global      Inside local    Outside local    Outside global
icmp 209.165.200.225:1 192.168.100.133:1 8.8.8.9:1       8.8.8.9:1
icmp 209.165.200.225:2 192.168.100.133:2 8.8.8.9:2       8.8.8.9:2
icmp 209.165.200.225:3 192.168.100.133:3 8.8.8.9:3       8.8.8.9:3
icmp 209.165.200.225:4 192.168.100.133:4 8.8.8.9:4       8.8.8.9:4

Router2#
```