Company Network Infrastructure with VPN, NAT & OSPF Multi-Area

Graduation Project Presentation

Project Link

Team Members:

- VLANs: Omar & Shehab
- DHCP: Youssef
- OSPF Multi-Area: Ahmed
- VPN: Seif
- NAT: Aser Osama

- Date: 9/5/2025

Project Overview

- **Goal:** Simulate a functional, secure, and scalable network for a company with HQ and two branches.

- **Focus:** Demonstrate CCNA & CCNP Enterprise Core concepts.

- **Key Technologies:** VLANs, Inter-VLAN Routing, DHCP, OSPF Multi-Area, Site-to-Site VPNs, NAT.

Agenda

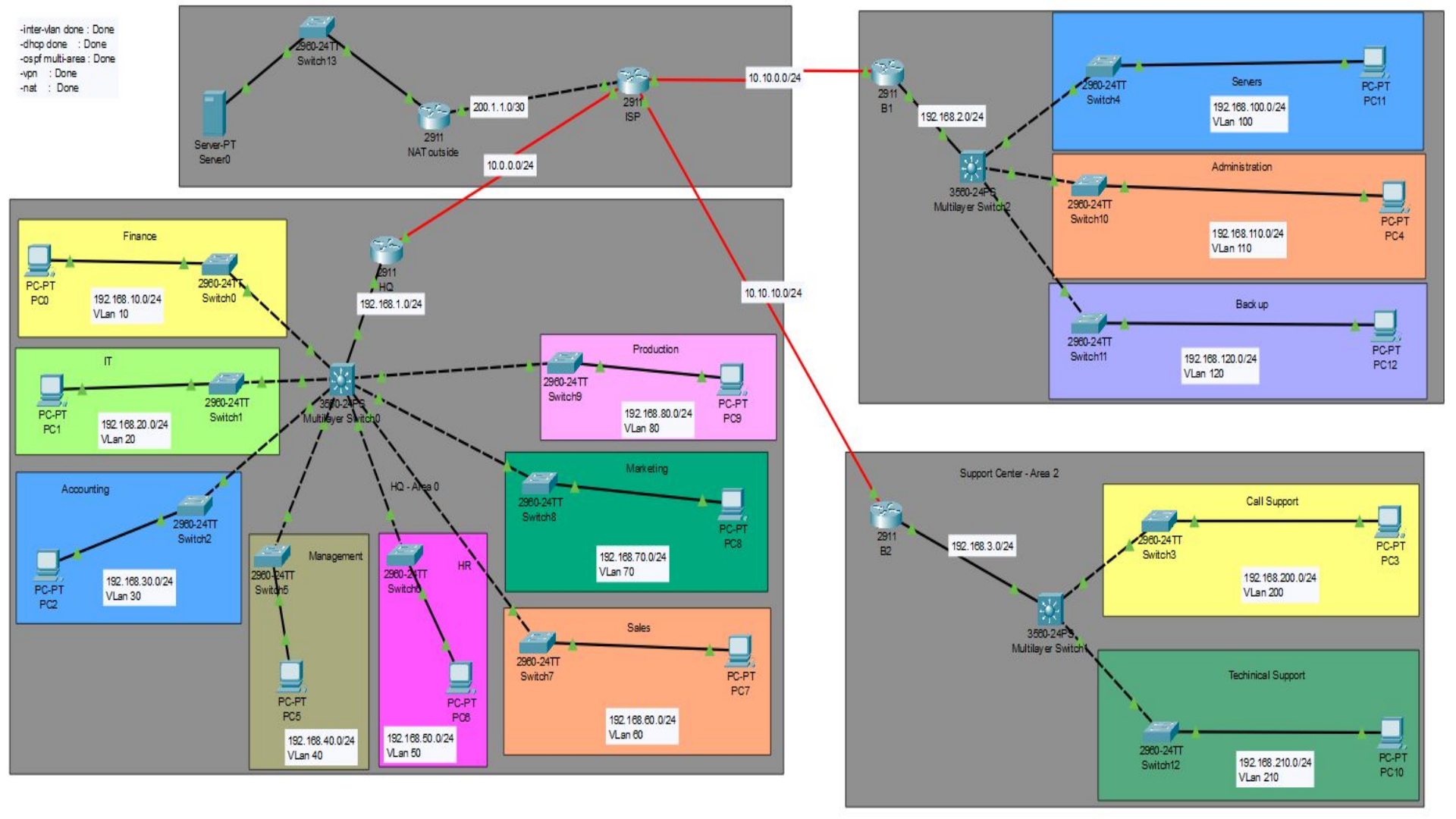
- Network Topology Overview
- VLANs & Inter-VLAN Routing (Omar & Shehab)
- DHCP Services (Youssef)
- OSPF Multi-Area Routing (Ahmed)
- VPN Connectivity (Seif)
- Network Address Translation (NAT) (Aser)
- Testing & Validation
- Challenges & Solutions
- Future Improvements
- Conclusion & Q&A

Network Topology Overview

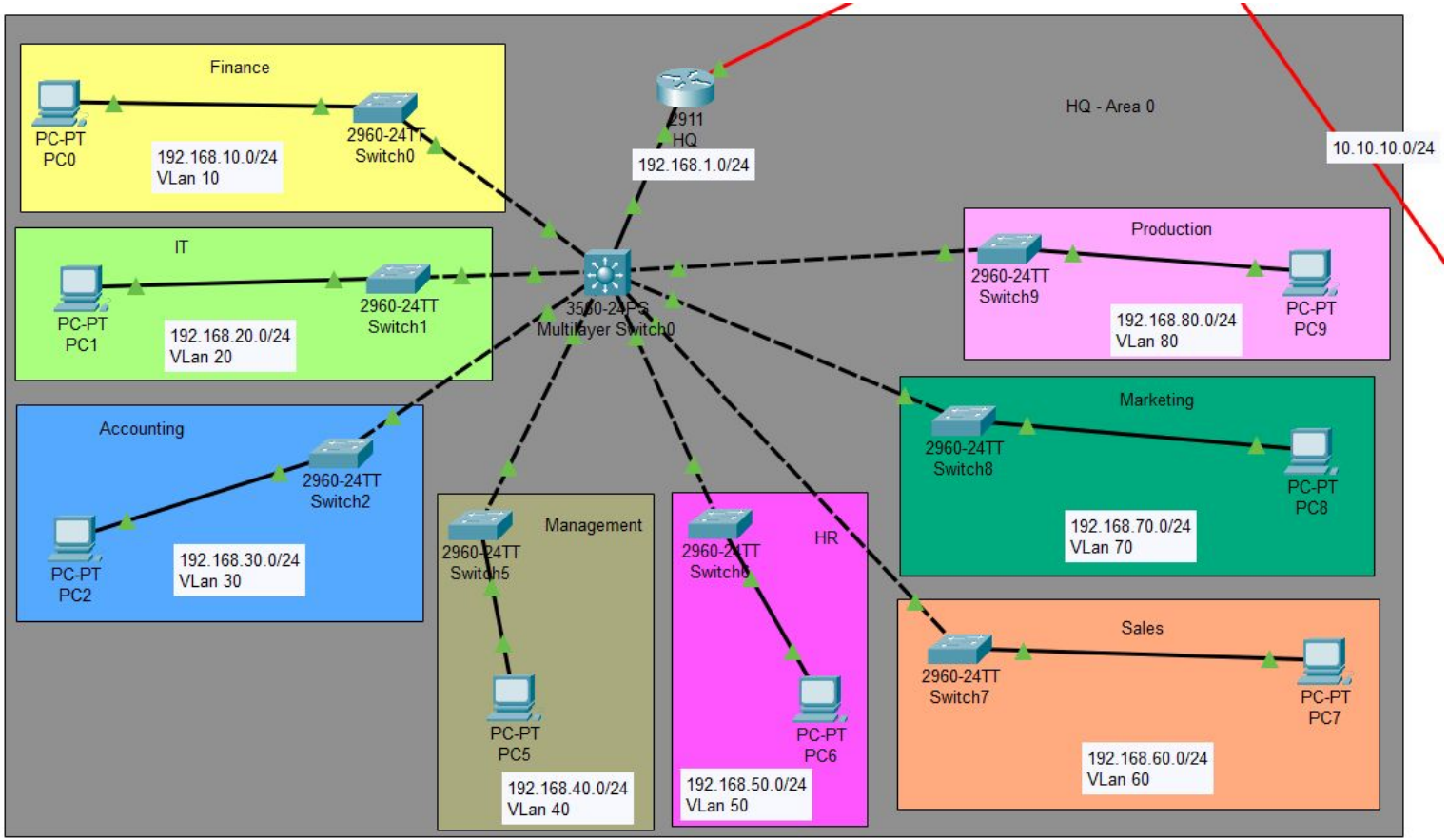
Key Components:

- Headquarter (HQ)
- Branch 1
- Branch 2
- ISP Router (simulating internet connectivity)
- Public Server (accessed via NAT)

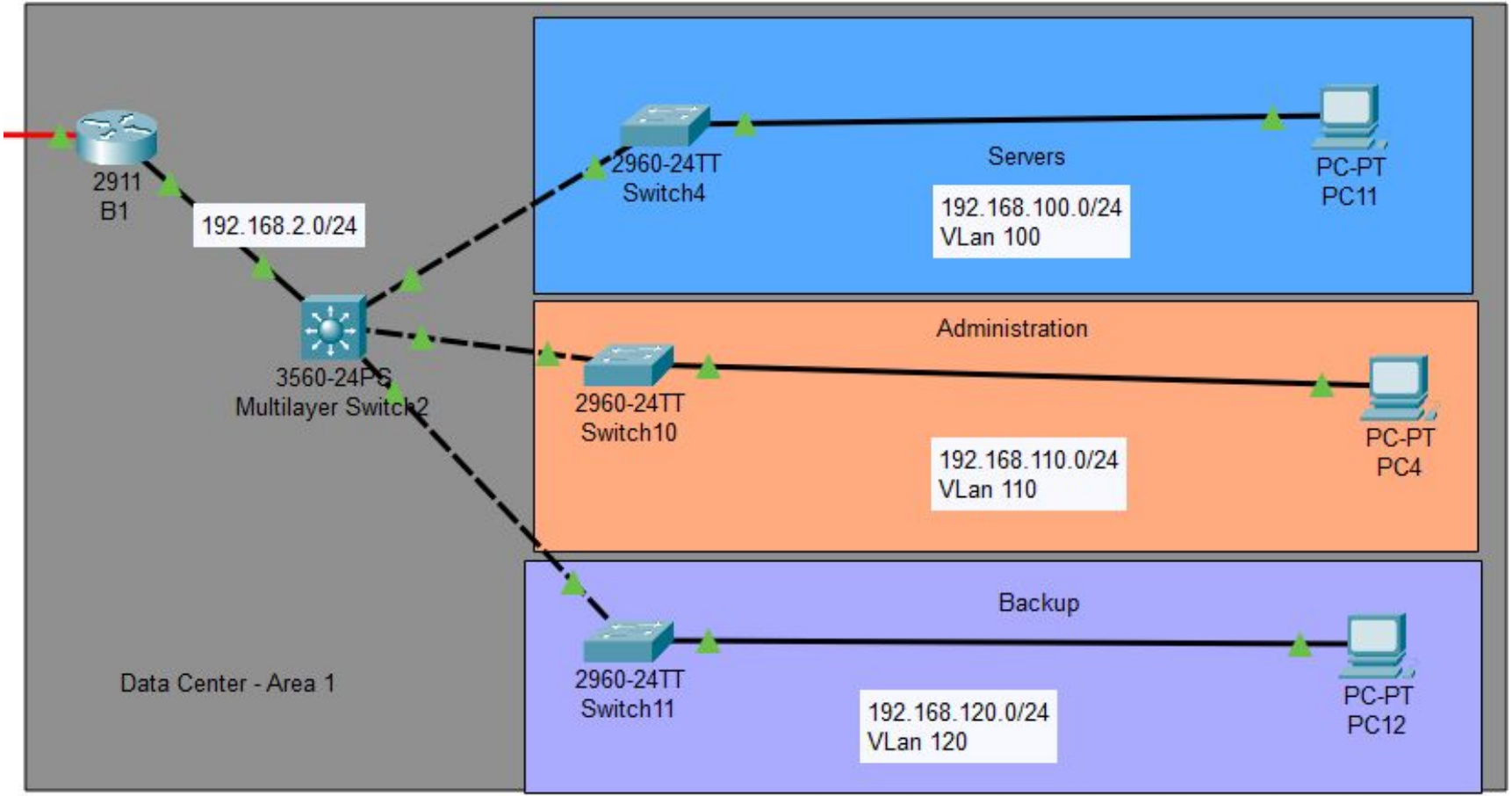
- **Connectivity:** Routers, Layer 3 Switches, Layer 2 Switches.


-inter-vlan done : Done
-dhcp done : Done
-ospf multi-area : Done
-vpn : Done
-nat : Done
2960-24TT
Switch13
Server-PT
Server0
200.1.1.0/30
2911
NAT outside
2911
ISP
10.10.0.0/24
10.0.0.0/24
2911
B1
192.168.2.0/24
3560-24PS
Multilayer Switch2
2960-24TT
Switch4
Servers
192.168.100.0/24
VLan 100
PC-PT
PC11
Administration
2960-24TT
Switch10
192.168.110.0/24
VLan 110
PC-PT
PC4
Back up
2960-24TT
Switch11
192.168.120.0/24
VLan 120
PC-PT
PC12
2911
HQ
192.168.1.0/24
10.10.10.0/24
Finance
PC-PT
PC0
192.168.10.0/24
VLan 10
2960-24TT
Switch0
IT
PC-PT
PC1
192.168.20.0/24
VLan 20
2960-24TT
Switch1
3560-24PS
Multilayer Switch0
Production
2960-24TT
Switch9
192.168.80.0/24
VLan 80
PC-PT
PC9
Accounting
2960-24TT
Switch2
PC-PT
PC2
192.168.30.0/24
VLan 30
HQ - Area 0
Marketing
2960-24TT
Switch8
PC-PT
PC8
192.168.70.0/24
VLan 70
Management
2960-24TT
Switch5
PC-PT
PC5
192.168.40.0/24
VLan 40
HR
2960-24TT
Switch6
PC-PT
PC6
192.168.50.0/24
VLan 50
Sales
2960-24TT
Switch7
PC-PT
PC7
192.168.60.0/24
VLan 60
Support Center - Area 2
2911
B2
192.168.3.0/24
3560-24PS
Multilayer Switch1
Call Support
2960-24TT
Switch3
PC-PT
PC3
192.168.200.0/24
VLan 200
Techinical Support
2960-24TT
Switch12
192.168.210.0/24
VLan 210
PC-PT
PC10

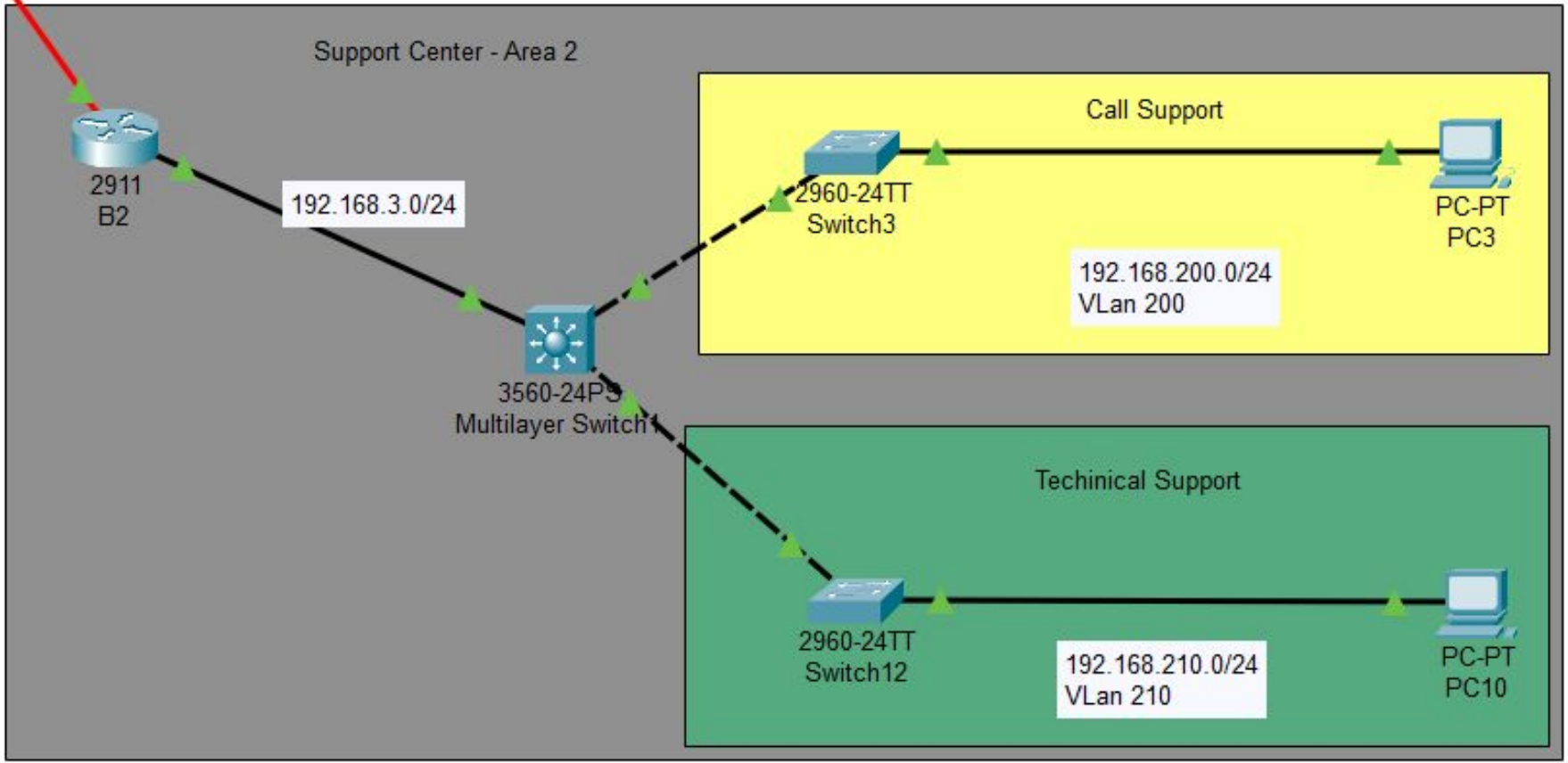
HQ Setup


Finance
PC-PT
PC0
192.168.10.0/24
VLan 10
2960-24TT
Switch0
2911
HQ
192.168.1.0/24
HQ - Area 0
10.10.10.0/24
IT
PC-PT
PC1
192.168.20.0/24
VLan 20
2960-24TT
Switch1
3560-24PS
Multilayer Switch0
Production
2960-24TT
Switch9
192.168.80.0/24
VLan 80
PC-PT
PC9
Marketing
2960-24TT
Switch8
PC-PT
PC8
192.168.70.0/24
VLan 70
Accounting
2960-24TT
Switch2
PC-PT
PC2
192.168.30.0/24
VLan 30
Management
2960-24TT
Switch5
PC-PT
PC5
192.168.40.0/24
VLan 40
HR
2960-24TT
Switch6
PC-PT
PC6
192.168.50.0/24
VLan 50
Sales
2960-24TT
Switch7
PC-PT
PC7
192.168.60.0/24
VLan 60

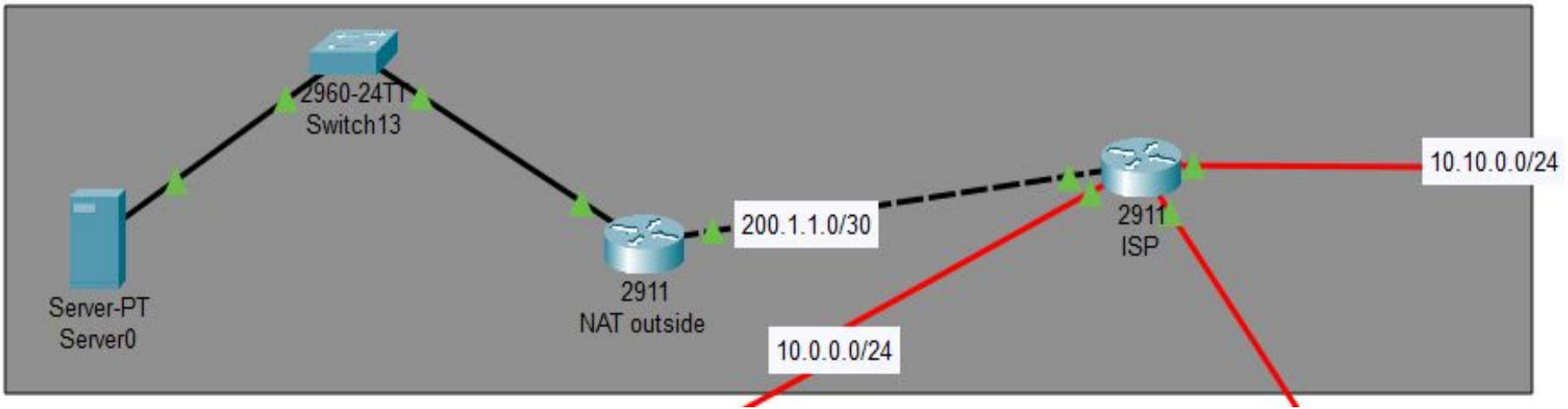
Branch 1


2911
B1
192.168.2.0/24
3560-24PS
Multilayer Switch2
Data Center - Area 1
2960-24TT
Switch4
Servers
192.168.100.0/24
VLan 100
PC-PT
PC11
Administration
2960-24TT
Switch10
192.168.110.0/24
VLan 110
PC-PT
PC4
Backup
2960-24TT
Switch11
192.168.120.0/24
VLan 120
PC-PT
PC12

Branch 2


Support Center - Area 2
2911
B2
192.168.3.0/24
3560-24PS
Multilayer Switch1
Call Support
2960-24TT
Switch3
PC-PT
PC3
192.168.200.0/24
VLan 200
Techinical Support
2960-24TT
Switch12
192.168.210.0/24
VLan 210
PC-PT
PC10

ISP & Server Configuration



VLANs:

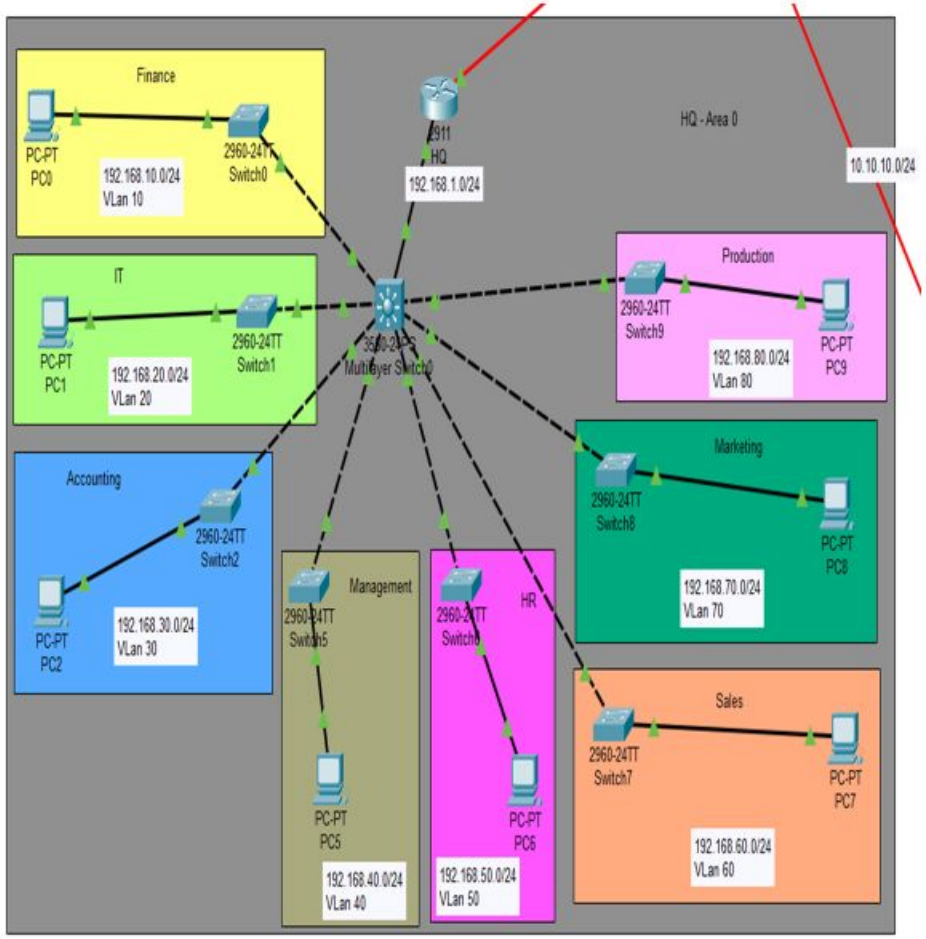
- **Presented by:** Omar kamel
- **What are VLANs?**
  - Logical segmentation of a physical network into separate logical networks.
- **Key Concepts of VLANs Design:**
  - Smaller Broadcast Domains
  - Improve security .
  - Improved IT Efficiency and reduce cost.
  - Each VLAN will have its own unique range of IP addressing.
- **Our VLAN Design:**
  - **HQ:** Finance (10), IT (20), Accounting (30), Management (40), HR (50), Sales (60), Marketing (70), Production (80).
  - **Branch 1:** Servers (100), Administration (110), Backup (120).
  - **Branch 2:** Tech Support (200), Call Support (210).

How to create VLANs:
Switch# configure terminal
Switch(config)# vlan vlan-id
Switch(config-vlan)# name vlan-name Switch(config-vlan)# end

Port Assignment in VLANs:
Switch# configure terminal
Switch(config)# interface interface-id
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan-id
Switch(config-if)# end

Trunk in VLANs:
Switch# configure terminal
Switch(config)# interface interface-id
Switch(config-if)# switchport mode trunk Switch(config-if)# switchport trunk native vlan vlan-id.
Switch(config-if)# switchport trunk allowed vlan vlan-list
Switch(config-if)# end

For Check:
Switch# show vlan brief



Inter-VLAN Routing

- **Presented by:** Shehab Eldeen Khaled

- **What is Inter-VLAN?**

  - Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

  - As VLANs are separate broadcast domains, they cannot talk to each other directly without a Layer 3 device to route between them.

- **Key Concepts of Inter-VLANs Design:**

  - Hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a Layer 3 switch to provide routing services.

  - Enabled by Layer 3 Switches using Switched Virtual Interfaces (SVIs).

  - Each SVI acts as the default gateway for its VLAN (e.g., 192.168.10.2 for VLAN 10).

  - Trunk ports configured between Layer 2 and Layer 3 switches.

Firstly:

- The configurations on the layer 2 switches is the same

Configurations on layer 3 switch:

1- Define VLANs :

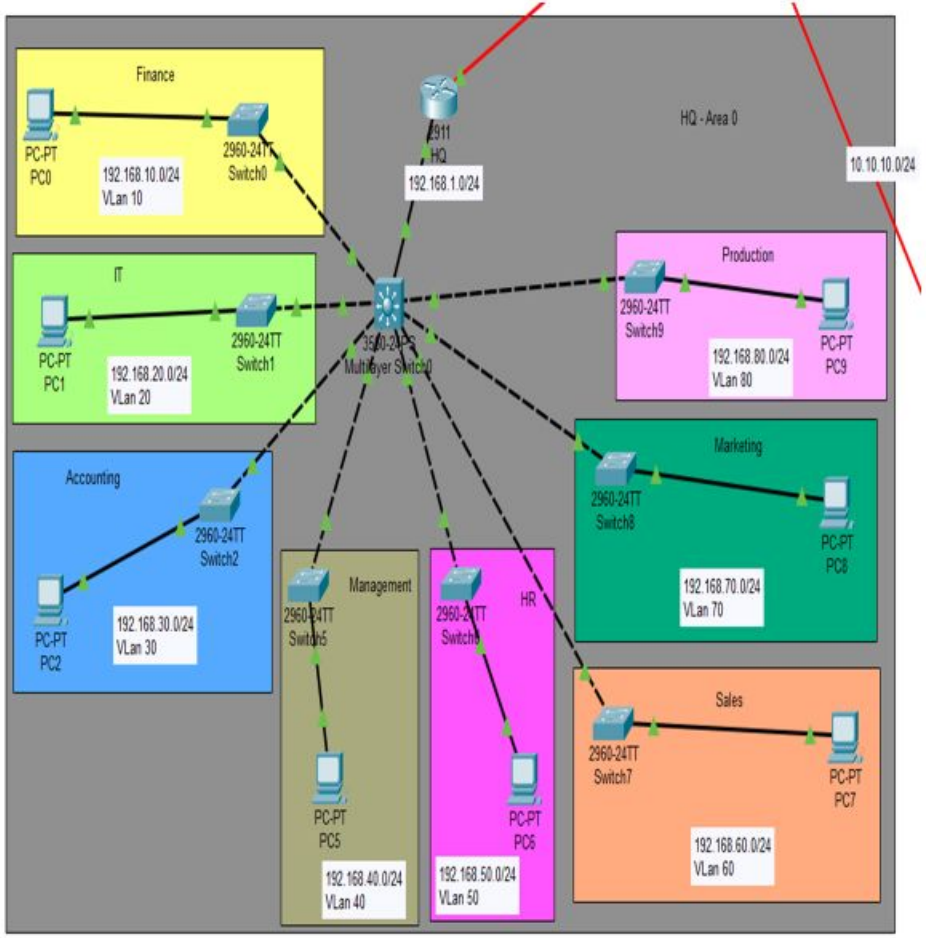
```
Switch# configure terminal
Switch(config)# vlan vlan-id
Switch(config-vlan)# name vlan-name
Switch(config-vlan)# end
```

2- Define its interfaces as trunk:

```
Switch# configure terminal
Switch(config)# interface interface-id
Switch(config-if)# switchport trunk encapsulation dot1Q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan vlan-id.
Switch(config-if)# switchport trunk allowed vlan vlan-list
Switch(config-if)# end
```

3- Apply routing and make SVIs and give them IPs :

```
Switch# configure terminal
Switch(config)# ip routing
Switch(config)# interface interface vlan-id
Switch(config)# interface interface vlan-id
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
```



DHCP Services

Presented by: Youssef

- **What is DHCP?**
  - Dynamic Host Configuration Protocol.
  - Automatically assigns IP addresses, subnet masks, default gateways, and DNS servers to clients.
  - Simplifies network administration.
- **Our DHCP Setup:**
  - Configured on Layer 3 switches at each location (HQ, Branch 1, Branch 2).
  - Separate DHCP pool for each VLAN.
  - **Default Gateway:** Correctly set to the SVI IP address (e.g., .2) for each VLAN.

OSPF Multi-Area: Smart Routing for Our Company

Presented by: Ahmed Alaa

What is OSPF?

- Think of OSPF (Open Shortest Path First) as a very smart GPS for our network data.
- It helps our routers learn the network map and find the best paths quickly and efficiently.
- It's a "link-state" protocol, meaning routers build a full picture of their local area.

Why Divide Our Network into "Areas"?**

- **Imagine Our Whole Company Network as One Big City:**

    - If it's one giant area, any small road closure (network change) could cause traffic jams everywhere as every GPS recalculates everything. This is slow and inefficient.

- **Multi-Area OSPF is like dividing our "City" into "Districts":**

    - **Smaller "Local Maps":** Routers primarily need to know their own "district" (Area) in detail, and just get summaries about other districts. This means smaller routing tables.

    - **Faster Reactions to Local Changes:** If a change happens in Branch 1's "district," only routers in Branch 1 fully recalculate. Others just get an update. This means less CPU work.

    - **More Stable:** A problem in one "district" (like a link failure) is less likely to cause major disruptions in other districts.

    - **Room to Grow:** Makes it easier to expand our company network in the future.

Our OSPF "Districts" (Areas) in This Project**

- **AREA 0 (The Backbone Area):** Our HQ
  - This is the central hub, the main highway system of our OSPF network.
  - All other "districts" (Areas) *must* connect to Area 0.
  - **Includes:** The HQ Router, the HQ Multilayer Switch, and all HQ VLANs (Finance, IT, Accounting, etc. – `192.168.10.0/24` to `192.168.80.0/24`).
- **AREA 1 (A Standard Area):** Branch 1
  - This is a distinct "district" connected to our Area 0 backbone.
  - **Includes:** The Branch 1 Router (B1), Branch 1 Multilayer Switch, and Branch 1 VLANs (Servers, Administration, Backup – `192.168.100.0/24` to `192.168.120.0/24`).
- **AREA 2 (A Standard Area):** Branch 2
  - Another "district," also connected to Area 0.
  - **Includes:** The Branch 2 Router (B2), Branch 2 Multilayer Switch, and Branch 2 VLANs (Call Support, Technical Support – `192.168.200.0/24` & `192.168.210.0/24`).
- Our HQ Router is the "Area Border Router" (ABR). It's special because it connects to Area 0 AND it also connects to Area 1 and Area 2.

VPN Connectivity

- **Presented by:** Seif

- **What is VPN?**

    - **Virtual Private Network:** Creates a secure, encrypted tunnel over an untrusted network (like the Internet).

- **Our VPN Setup:**

    - **Site-to-Site IPsec VPNs:**

        - HQ ↔ Branch 1

        - HQ ↔ Branch 2

    - **Purpose:** Secure communication between company sites.

    - **ACLs (Access Control Lists):** Used to define "interesting traffic" – what traffic should be encrypted and sent through the VPN tunnel.

VPN Configuration Summary:

1. IKE Phase 1 (ISAKMP Policy):

- **Authentication:** Pre-shared key
- **Encryption:** AES
- **Hashing:** SHA
- **DH Group:** 5 (Strong DH for key exchange)

2. Pre-Shared Keys (PSK):

- **HQ ↔ B1:** crypto isakmp key Pass address 10.10.0.2
- **HQ ↔ B2:** crypto isakmp key Pass address 10.10.10.2

3. IPSec Transform Set Protocol:

- **ESP Encryption:** AES
- **Integrity:** SHA-HMAC

4. Crypto ACLs (Traffic to Encrypt):

- **HQ → B1 (ACL 110):** All traffic from 192.168.10.0/24 to 192.168.100.0/24, 110.0/24, 120.0/24 (Repeated for all HQ subnets: 20.0/24 to 80.0/24)
- **HQ → B2 (ACL 120):** All traffic from 192.168.10.0/24 to 192.168.200.0/24, 210.0/24 (Repeated for all HQ subnets: 20.0/24 to 80.0/24)
- **B1/B2 → HQ (ACL 100):** Reverse of HQ ACLs (mirrored subnets)

5. Crypto Maps:

- **HQ:** crypto map HQ (2 peers: B1 10.10.0.2, B2 10.10.10.2)
- **B1/B2:** Single peer (HQ 10.0.0.1)

6. Application to Interfaces:

- **HQ:** interface se0/2/1 → crypto map HQ
- **B1:** interface se0/3/0 → crypto map B1
- **B2:** interface se0/3/0 → crypto map B2

Network Address Translation (NAT)

- **Presented by:** Aser

- **What is NAT?**

  - Translates private IP addresses (used within our company network) to a public IP address (for internet access).

  - Conserves public IP addresses and adds a layer of security.

- **Our NAT Setup:**

  - Configured on the Internal Router using PAT.

  - **PAT (Port Address Translation) / NAT Overload:** Allows multiple internal devices to share a single public IP address.

  - Enables internal hosts to reach the simulated public server (and the internet).

Network Address Translation (NAT)

- **The Commands Used:**

1) Configure inside interface (LAN)

interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
no shutdown
exit

2) **Configure outside interface (WAN)**

interface Serial0/0/0
ip address 203.0.113.2 255.255.255.252
ip nat outside
no shutdown
Exit

3) **Access list to match inside local addresses**

access-list 1 permit 192.168.1.0 0.0.0.255

4) **NAT Overload configuration**

ip nat inside source list 1 interface Serial0/0/0 overload

5) To verify:

show ip nat translations
show ip nat statistics

Testing & Validation

- **Comprehensive testing was performed:**

  - ping tests: Across VLANs, between HQ and branches (over OSPF and VPN).

  - show commands: show ip route, show ip ospf neighbor, show crypto isakmp sa, show crypto ipsec sa.

  - DHCP: Verified IP lease acquisition on PCs.

  - NAT: Verified translation when accessing the public server.

  - VPN: Debug commands and traffic simulation.

Project Results

- **VLANs & DHCP:** Devices correctly received IPs and gateways. Inter-VLAN routing successful.

- **OSPF Multi-Area:** Full route exchange achieved between all areas, demonstrating efficient routing.

- **VPN:** Secure tunnels established between HQ and both branches.

- **NAT:** Internal hosts successfully accessed the public server with proper address translation.

- **Overall:** A functional, secure, and scalable network design was successfully implemented.

Challenges & Solutions

- **DHCP Default Gateway:** Initially misconfigured (.1 instead of .2). Corrected to match SVI IPs.

    - Learning: Careful attention to gateway addresses in DHCP pools is crucial.

- **VPN Misconfiguration:** Initial VPN setup required debugging of ISAKMP/IPsec parameters and ACLs.

    - Learning: VPN troubleshooting involves systematic checks of phases, policies, and interesting traffic.

Future Improvements

- Add more end devices (PCs, printers) for realistic load.
- Configure IP Phones & DSL in the Call Support VLAN.
- Integrate basic network monitoring tools (e.g., SNMP).
- Implement redundancy (e.g., HSRP, redundant links).
- Enhance security with more detailed Firewall ACLs.

Conclusion

- Successfully designed and simulated a multi-branch company network.

- Demonstrated practical application of core networking concepts.

- The project provides a solid foundation for understanding complex enterprise network solutions.

Thank You & Questions