Network Final Project Report

1. VLAN & Subnet Table

Branch	Department	VLAN ID	Subnet	Devices	Security Level	Gateway IP	DHCP Pool	Static IPs
1	HR	10	192.168.1.0/24	6	Medium	192.168.1.1	192.168.1.50-192.168.1.200	192.168.1.2-49
1	IT	20	192.168.2.0/24	6	High	192.168.2.1	192.168.2.50-192.168.2.200	192.168.2.2-49
1	Sales	30	192.168.3.0/24	6	Low	192.168.3.1	192.168.3.50-192.168.3.200	192.168.3.2-49
2	HR	40	192.168.4.0/24	6	Medium	192.168.4.1	192.168.4.50-192.168.4.200	192.168.4.2-49
2	IT	50	192.168.5.0/24	6	High	192.168.5.1	192.168.5.50-192.168.5.200	192.168.5.2-49
2	Sales	60	192.168.6.0/24	6	Low	192.168.6.1	192.168.6.50-192.168.6.200	192.168.6.2-49

2. Why /24 subnets are appropriate

- A /24 subnet provides 256 IP addresses (0-255).
- Deduct network address (x.x.x.0), broadcast (x.x.x.255), and gateway → ~253 usable addresses.
- Each department has 6 devices, so a /24 subnet is more than enough, leaving room for future expansion.
- This simplifies subnetting and VLAN management because each department gets its own clear, non-overlapping subnet.

3. IP Allocation Details

- **Gateway IP:** The first usable IP in each subnet (e.g., 192.168.1.1)
- **DHCP pool:** 50–200 (allows dynamic assignment to most devices while reserving low IPs for static devices)
- **Static IPs:** 2–49 (can assign to servers, printers, routers, VoIP phones, or critical devices)

- **Example for Branch 1, HR:**
  - Gateway: 192.168.1.1
  - DHCP: 192.168.1.50 → 192.168.1.200
  - Static: 192.168.1.2 → 192.168.1.49

4. Network Device Inventory

This inventory lists all required hardware for the two-branch topology, including the quantity for redundancy (2 switches per branch) and collision domain demonstration (1 hub per branch).

Device Type	Purpose	Branch 1 Qty	Branch 2 Qty	Total
Router (Cisco 2911)	Inter-VLAN Routing, WAN link, NAT, DHCP/DNS services.	1	1	**2**
Layer 2 Switch (Cisco 2960)	VLAN segmentation, Redundancy via STP, Access Layer connectivity.	2	2	**4**
PC (End Devices)	User endpoints for HR, IT, and Sales departments.	18 (6 per dept)	18 (6 per dept)	36
Server (Shared)	Hosts DNS, DHCP, and Web services.	1	0	**1**
Hub (Optional)	Demonstrate collision domains (used in Branch 1).	1	0	**1**

5. Device Naming Convention

All devices in Packet Tracer must be renamed using the following convention to ensure clarity and consistency for all team members.

Device Type	Naming Format	Example
Routers	`Branch[#]-Router`	`Branch1-Router`, `Branch2-Router`
Switches	`Branch[#]-Switch[#]`	`Branch1-Switch1`, `Branch2-Switch2`

PCs	`PC[#]-[Dept]-B[#]`	`PC1-HR-B1 through PC6-HR-B1`
Server	`WebServer-Shared`	`WebServer-Shared`
Hub	`Branch[#]-Hub`	`Branch1-Hub`

6. Network Diagram and Topology Overview

The network uses a Hybrid Topology to ensure resilience and performance.

- **Access Layer (Switches):** Each branch uses two switches (`-Switch1` and `-Switch2`) connected to each other via a Crossover link for redundancy, utilizing STP (Spanning Tree Protocol) to prevent loops. PCs connect to these switches.
- **Distribution/Core Layer (Routers):** One router per branch handles all Inter-VLAN traffic and connects the local network to the remote branch/WAN.
- **WAN Link:** The two routers are connected using a Serial Link to form a Wide Area Network (WAN).

7. Detailed Connection Log

This log specifies the exact connections and cable types for the implementation phase. All connections must be completed as listed below.

A. Inter-Branch WAN Link

From Device	Port	To Device	Port	Cable Type	Speed	Notes
Branch1-Router	S0/0/0	**Branch2-Router**	S0/0/0	Serial DCE	Serial	Branch1-Router is DCE (provides clocking)

B. Branch 1 Connections (LAN)

From Device	Port	To Device	Port	Cable Type	Speed	Notes

PCs (HR, IT, Sales)	Fa0	**Branch1-Switch1**	Fa0/1-18	Straight-through	100 Mbps	Access Link (Fa0/1-6=HR, Fa0/7-12=IT, Fa0/13-18=Sales)
Webserver-Shared	Fa0	**Branch1-Switch1**	Gi0/3	Straight-through	1000 Mbps	Static IP for Server/Services
Branch1-Switch1	Gi0/1	**Branch1-Switch2**	Gi0/1	Crossover	1000 Mbps	Switch Redundancy (Trunk)
Branch1-Switch1	Gi0/2	**Branch1-Router**	Gi0/0	Straight-through	1000 Mbps	Router Uplink (Trunk)
Branch1-Switch2	Gi0/2	**Branch1-Router**	Gi0/1	Straight-through	1000 Mbps	Router Uplink (Trunk, Secondary)
Branch1-Hub	Port 1	**Branch1-Switch2**	Fa0/24	Straight-through	100 Mbps	Optional Demo Link

C. Branch 2 Connections (LAN)

From Device	Port	To Device	Port	Cable Type	Speed	Notes
PCs (HR, IT, Sales)	Fa0	**Branch2-Switch1**	Fa0/1-18	Straight-through	100 Mbps	Access Link (Fa0/1-6=HR, Fa0/7-12=IT, Fa0/13-18=Sales)
Branch2-Switch1	Gi0/1	**Branch2-Switch2**	Gi0/1	Crossover	1000 Mbps	Switch Redundancy (Trunk)
Branch2-Switch1	Gi0/2	**Branch2-Router**	Gi0/0	Straight-through	1000 Mbps	Router Uplink (Trunk)
Branch2-Switch2	Gi0/2	**Branch2-Router**	Gi0/1	Straight-through	1000 Mbps	Router Uplink (Trunk, Secondary)

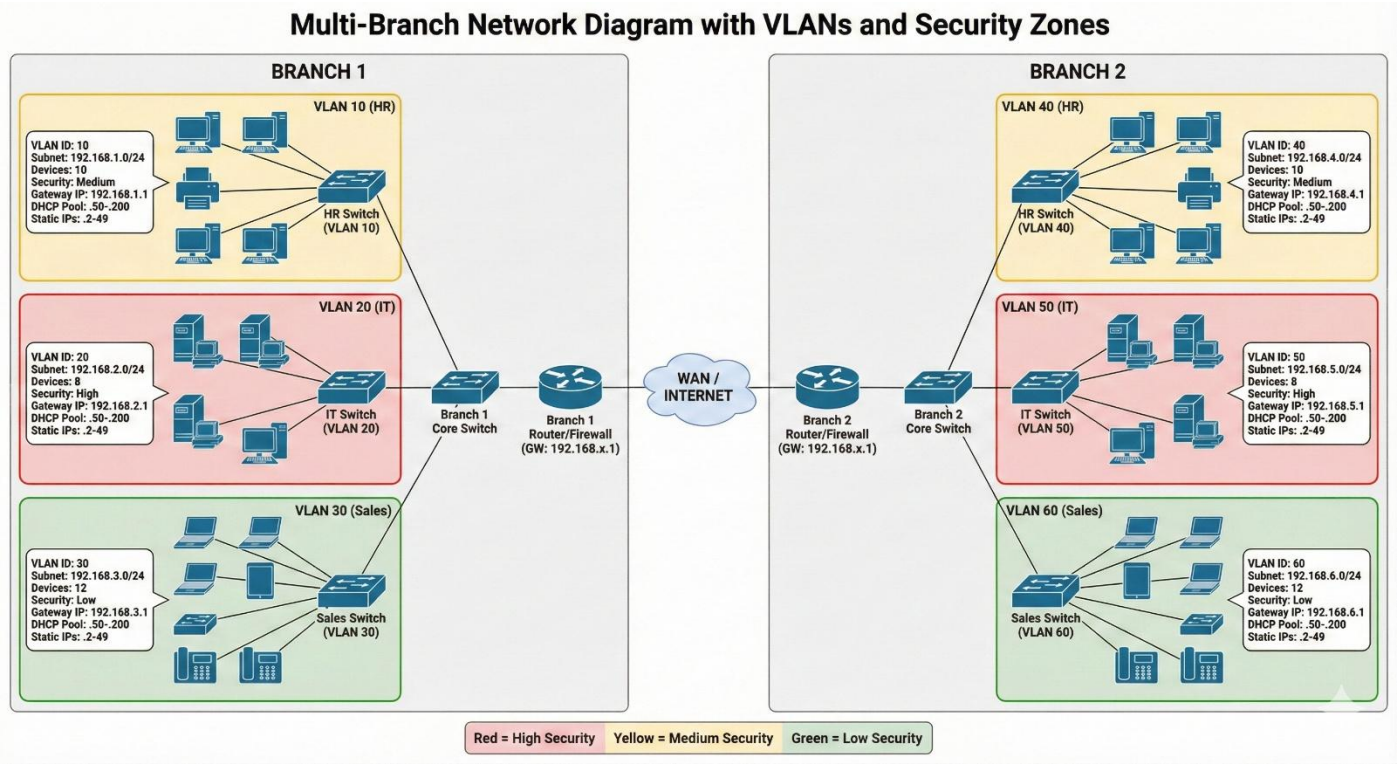
8. IP Address Planning

Branch	VLAN ID	Department	Subnet/Mask	Gateway IP (Router Sub-interface)

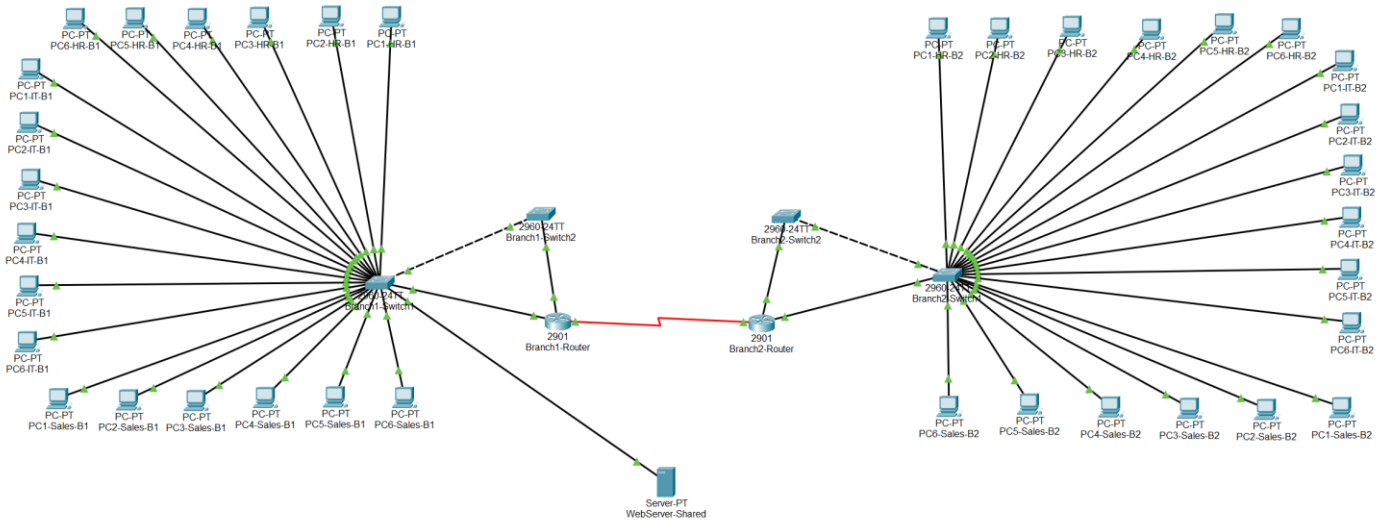
1	10	HR	192.168.1.0/24	192.168.1.1
1	20	IT	192.168.2.0/24	192.168.2.1
1	30	Sales	192.168.3.0/24	192.168.3.1
2	40	HR	192.168.4.0/24	192.168.4.1
2	50	IT	192.168.5.0/24	192.168.5.1
2	60	Sales	192.168.6.0/24	192.168.6.1

Link/Device	IP Address	Mask	Notes
WAN Link (Branch 1 Router S0/0/0)	10.0.0.1	255.255.255.0	DCE side (clock rate)
WAN Link (Branch 2 Router S0/0/0)	10.0.0.2	255.255.255.0	DTE side

9.Network Diagram



10. Packet Tracer Setup & Device Deployment



A. Design and topolgy creation

- Launched Cisco Packet Tracer and created a new project file.
- Designed a two-branch network consisting of Branch 1 and Branch 2.
- For each branch, added the following devices:
    - One Cisco 2901 router.
    - Two Cisco 2960 switches (BranchX-Switch1 and BranchX-Switch2).
    - Multiple end devices (PCs) representing different departments (HR, Sales, etc.).
- Placed a shared Web Server device in the lower part of the topology to be reachable from both branches.

B. Interconnection of Devices (LAN Links)

- Connected each PC to its local access switch using Copper Straight-Through cables on FastEthernet ports.
- Connected the WebServer-Shared FastEthernet0 interface to an available FastEthernet port on Branch1-Switch1 using a Copper Straight-Through cable.
- Configured all switch ports facing PCs and the web server as access ports in their respective VLANs (for example, HR, Sales, and Server VLANs as required by the task).

C. Inter-Switch and Router–Switch Connections

- Connected Branch1-Switch1 to Branch1-Switch2 with a Copper CrossOver cable to provide redundancy.
- Connected Branch2-Switch1 to Branch2-Switch2 in the same way.
- Connected each branch router to its main switch (BranchX-Switch1) using a GigabitEthernet link (Gi0/x) and Copper Straight-Through cable.
- Verified that Spanning Tree Protocol (STP) was running to prevent switching loops; one redundant link became a blocking/alternate port as expected.

D. WAN Connection Between Branch Routers

- Installed serial WAN modules on both Branch1-Router and Branch2-Router (HWIC-type module) via the Physical tab in Packet Tracer.
- Powered off the routers before inserting modules and powered them back on afterwards.
- Created the WAN link between Branch1-Router Serial0/3/0 and Branch2-Router Serial0/3/0 using a Serial DCE/DTE cable.

E. Testing and Verification

- Verified physical connectivity in Packet Tracer by checking that all links showed green (or STP-blocked where expected) after configuration.
- Saved the Packet Tracer project and captured the final topology screenshot as evidence of successful network implementation.

11. VLAN Configuration

Objective: To improve network performance and security, we segmented the network into Virtual Local Area Networks (VLANs). This divides the broadcast domain into smaller logical groups, ensuring that traffic from one department (e.g., Sales) remains isolated from others (e.g., HR) unless routed through the secure gateway.

Implementation Details: We configured three distinct VLANs on the access switches with the following port assignments to allow for future scalability:

- **VLAN 10 (HR):** Assigned to Ports Fa0/1 – Fa0/6.

- **VLAN 20 (IT):** Assigned to Ports Fa0/9 – Fa0/16.
- **VLAN 30 (Sales):** Assigned to Ports Fa0/17 – Fa0/24.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8
10   hr                               active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6
20   IT                               active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
30   sales                            active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

12. Broadcast and Collision Domains Analysis

A. Broadcast Domains Analysis

- A broadcast domain is the extent of the network where a broadcast frame will be heard. In our design, broadcast domains are bounded by Routers and VLANs.
- **VLAN Segmentation:** By configuring VLANs, we have logically separated the broadcast domains within the Layer 2 switches. A broadcast sent by an HR employee in Branch 1 (VLAN 10) is blocked from reaching IT (VLAN 20) or Sales (VLAN 30).
- **Router Segmentation:** The routers at each branch stop broadcasts from crossing the WAN link, preventing local broadcast storms from affecting the remote branch.
- **Total Broadcast Domains:** We have identified 7 distinct broadcast domains in this topology:
    1. **Branch 1 HR** (VLAN 10)
    2. **Branch 1 IT** (VLAN 20)
    3. **Branch 1 Sales** (VLAN 30)
    4. **Branch 2 HR** (VLAN 40)
    5. **Branch 2 IT** (VLAN 50)
    6. **Branch 2 Sales** (VLAN 60)

7. **WAN Link** (The dedicated network `10.0.0.0/30` connecting the two routers)

B. Collision Domains Analysis

- A collision domain is a network segment where data packets can collide with one another while being sent on a shared medium. If two devices transmit at the same time in the same collision domain, a collision occurs, and both devices must wait and retransmit.
- **Network Design Analysis:** In this project, we utilized a fully switched network architecture using Cisco 2960 Switches. Unlike legacy hubs, which place all connected devices into a single shared collision domain, switches utilize micro-segmentation.
    - **Micro-Segmentation:** Each port on a Cisco switch is its own independent collision domain.
    - **Full-Duplex:** Because each device has its own dedicated lane to the switch, devices can send and receive data simultaneously (Full-Duplex) without any risk of collision.
- **Collision Domain Count:** Since every active Ethernet cable in a switched network represents one collision domain, the total count is calculated based on the active connections:

a) Branch 1:

- 18 PCs connected to switch ports = **18 Collision Domains**
- 1 Link connecting Switch 1 to Switch 2 = **1 Collision Domain**
- 2 Links connecting Router to Switch = **2 Collision Domain**
- Branch 1 Total: **21 Collision Domains**

b) Branch 2:

- 18 PCs connected to switch ports = **18 Collision Domains**
- 1 Link connecting Switch 1 to Switch 2 = **1 Collision Domain**
- 2 Link connecting Router to Switch **= 2 Collision Domain**
- Branch 2 Total: **21 Collision Domains**

c) **WAN:**

- 1 Serial link connecting Branch 1 Router to Branch 2 Router = **1 Collision Domain**

d) **Grand Total:** The network contains approximately **43 distinct collision domains**. This high number is positive; it indicates that traffic is perfectly segmented, eliminating the performance bottlenecks associated with shared media.

13. Inter-VLAN Routing, NAT, DHCP & DNS Configuration

Inter-VLAN routing enables communication between different VLANs on the same router, while NAT (Network Address Translation) provides security by hiding internal IP addresses from external networks. DHCP (Dynamic Host Configuration Protocol) automates IP address assignment, and DNS (Domain Name System) translates domain names to IP addresses, simplifying network usability.

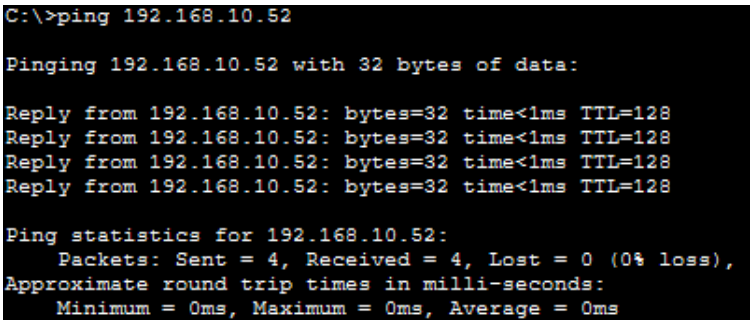
A. Router Sub-Interface Configuration for Inter-VLAN Routing

- Each VLAN has a sub-interface on the router that acts as its gateway.
- 802.1Q encapsulation lets one physical interface carry traffic for multiple VLANs.
- This allows the router to route traffic between HR, IT, and Sales while keeping them logically separated.

Branch	VLAN ID	Department	Sub-Interface	Gateway IP	Encapsulation
1	10	HR	Gi0/0.10	192.168.1.1	dot1Q
1	20	IT	Gi0/0.20	192.168.2.1	dot1Q
1	30	Sales	Gi0/0.30	192.168.3.1	dot1Q
2	40	HR	Gi0/0.40	192.168.4.1	dot1Q
2	50	IT	Gi0/0.50	192.168.5.1	dot1Q
2	60	Sales	Gi0/0.60	192.168.6.1	dot1Q

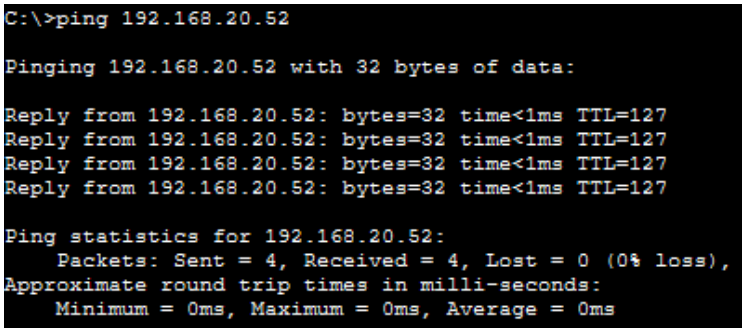
- Devices in each VLAN use the gateway IP in this table as their default router.
- For example, HR in Branch 1 sends traffic to 192.168.1.1 when contacting another VLAN or branch.

- Inner VLAN routing**:** Done by PC1-HR-BR1



B. Inter-Branch Routing (WAN Link Configuration)

- The two routers are linked over a separate WAN subnet (10.0.0.0/24).
- One side is DCE (provides clock), the other is DTE.
- Static routes tell each router which remote VLANs are behind the other router.
- Result: any VLAN in Branch 1 can reach any VLAN in Branch 2 through the WAN link.
- Inner branch routing**:** Done by PC1-HR-BR1



C. NAT (Network Address Translation) Configuration

- NAT hides internal addresses (192.168.x.x) behind the router's external/WAN address.
- When internal devices go out, NAT replaces their source IP with the router's IP.
- Replies are translated back to the original internal IPs.
- PAT/overload lets many internal devices share a single external IP using different ports.

NAT Component	Purpose	Configuration idea
Inside interface	Marks LAN-facing side	ip nat inside on Gi0/0
Outside interface	Marks WAN-facing side	ip nat outside on S0/0/0
ACL 1	Selects internal traffic to translate	permit 192.168.0.0 0.0.255.255
Overload	Many internal IPs use one external IP (PAT)	ip nat inside source list 1 interface S0/0/0 overload

- NAT is only applied when traffic leaves towards the WAN, not between VLANs inside the branches.
- Branch 1 NAT Inner/outer ports:

```
Router#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0.10 , GigabitEthernet0/0.20 , GigabitEthernet0/0.30
Hits: 4  Misses: 9
Expired translations: 0
Dynamic mappings:
```

- Branch 2 NAT Inner/outer ports:

```
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0
Hits: 0  Misses: 6
Expired translations: 0
Dynamic mappings:
```

D. DHCP Pool Configuration

- DHCP gives IP addresses automatically instead of configuring each PC manually.
- Each VLAN has its own pool that matches its subnet.
- Low addresses are reserved for static devices (routers, servers); mid-range is for clients.

VLAN	Pool Name	Network	Gateway	DHCP Range	Excluded Range	DNS Server
10 (HR)	HR-VLAN10	192.168.1.0/24	192.168.1.1	192.168.1.50–200	192.168.1.1–49, 201–254	192.168.1.100
20 (IT)	IT-VLAN20	192.168.2.0/24	192.168.2.1	192.168.2.50–200	192.168.2.1–49, 201–254	192.168.1.100

VLAN	Pool Name	Network	Gateway	DHCP Range	Excluded Range	DNS Server
30 (Sales)	Sales-VLAN30	192.168.3.0/24	192.168.3.1	192.168.3.50–200	192.168.3.1–49, 201–254	192.168.1.100

- When a PC boots, it sends a DHCP request and receives IP, mask, gateway and DNS from the correct pool based on its VLAN.
- Branch 1 Router DHCP POOL:

```
Router#show ip dhcp pool

Pool HR-VLAN10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.1         192.168.10.1     - 192.168.10.254    6     / 6      / 254

Pool IT-VLAN20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.20.1         192.168.20.1     - 192.168.20.254    6     / 6      / 254

Pool Sales-VLAN30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.30.1         192.168.30.1     - 192.168.30.254    6     / 6      / 254
```

- Branch 2 Router DHCP POOL:

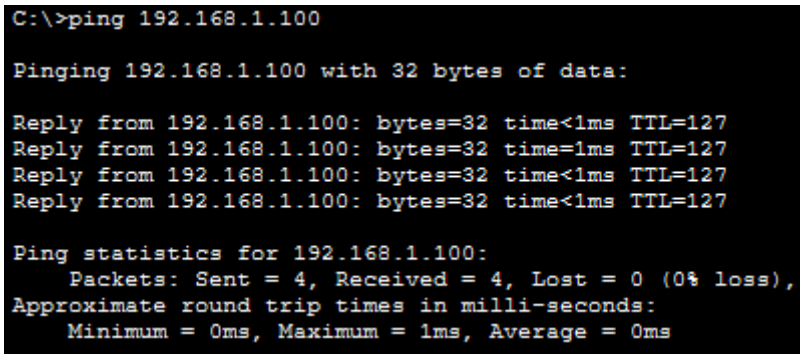
```
Router#show ip dhcp pool

Pool HR-VLAN40 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.40.1         192.168.40.1     - 192.168.40.254    6     / 6      / 254

Pool IT-VLAN50 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.50.1         192.168.50.1     - 192.168.50.254    6     / 6      / 254

Pool SALES-VLAN60 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 5
 Excluded addresses             : 6
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.60.1         192.168.60.1     - 192.168.60.254    5     / 6      / 254
```

E. DNS Configuration

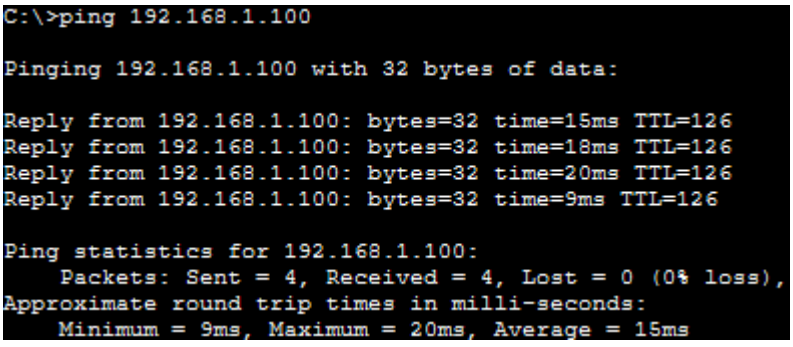
- DNS lets users type names (like www.company.local) instead of IP addresses.
- The shared server in Branch 1 runs DNS for the whole company.
- Clients learn the DNS server IP through DHCP.
- DNS Records on WebServer-Shared:

Domain Name	IP Address	Purpose
www.company.local	192.168.1.100	Main internal web portal
mail.company.local	192.168.1.101	Internal mail service

- If the web service moves to a new IP, only the DNS record changes; users keep using the same name.
- Branch 1:



- Branch 2:



14. Security Configuration

A. ACL:

- To enforce a "Least Privilege" security model, we implemented Extended ACL 100 on the Branch 1 and 2 Routers. This configuration was applied inbound on the

Sales sub-interface (`Gi0/0.30`) to restrict access to sensitive departments while maintaining internet connectivity.

- **The ACL enforces the following rules:**
    - **Deny:** Sales Department (192.168.30.0/24) to HR Department (192.168.10.0/24).
    - **Deny:** Sales Department (192.168.30.0/24) to IT Department (192.168.20.0/24).
    - **Permit:** All other traffic (e.g., Internet/Web Server access).

```
show access-lists
Standard IP access list 1
    10 permit 192.168.0.0 0.0.255.255
Extended IP access list 100
    10 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 (8 match(es))
    15 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
    20 permit ip any any
```

B. Port Security:

- **Objective**: To prevent unauthorized devices from physically connecting to the network, we implemented Port Security on the access switches. This ensures that only authorized company computers can send traffic through specific wall jacks.
- **Implementation Details**: We configured the following settings on all Access Ports (FastEthernet 0/1–23):
- **Maximum MAC Addresses**: 1 (Only one device allowed per port).
- **Violation Mode**: Shutdown (The port physically turns off if a violation occurs).
- **MAC Address Learning**: Sticky (The switch automatically learns and saves the authorized PC's MAC address).

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)        (Count)
--------------------------------------------------------------------------
       Fa0/1        1          1                0         Shutdown
       Fa0/2        1          1                0         Shutdown
       Fa0/3        1          1                0         Shutdown
       Fa0/4        1          1                0         Shutdown
       Fa0/5        1          1                0         Shutdown
       Fa0/6        1          1                0         Shutdown
       Fa0/7        1          1                0         Shutdown
       Fa0/8        1          0                0         Shutdown
       Fa0/9        1          1                0         Shutdown
      Fa0/10        1          1                0         Shutdown
      Fa0/11        1          1                0         Shutdown
      Fa0/12        1          1                0         Shutdown
      Fa0/13        1          1                0         Shutdown
      Fa0/14        1          1                0         Shutdown
      Fa0/15        1          0                0         Shutdown
      Fa0/16        1          0                0         Shutdown
      Fa0/17        1          1                0         Shutdown
      Fa0/18        1          1                0         Shutdown
      Fa0/19        1          1                0         Shutdown
      Fa0/20        1          1                0         Shutdown
      Fa0/21        1          1                0         Shutdown
      Fa0/22        1          1                0         Shutdown
      Fa0/23        1          0                0         Shutdown
      Fa0/24        1          0                0         Shutdown
--------------------------------------------------------------------------
Switch#
```

15. Testing

A. Connectivity: Ping IT to HR

- **What it checks:** Inter-VLAN Routing (Layer 3).
- **The Logic:** By default, computers in different VLANs (like HR and IT) are in separate "rooms" and cannot talk to each other.
- **What it proves:** It proves your Router-on-a-Stick configuration is working. The router successfully accepted the packet from the HR VLAN, routed it to the correct gateway, and sent it down to the IT VLAN.

```
C:\>ping 192.168.10.51

Pinging 192.168.10.51 with 32 bytes of data:

Reply from 192.168.10.51: bytes=32 time<1ms TTL=127
Reply from 192.168.10.51: bytes=32 time=2ms TTL=127
Reply from 192.168.10.51: bytes=32 time<1ms TTL=127
Reply from 192.168.10.51: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

B. Security (ACL): Ping Sales to HR and to IT (Fails)

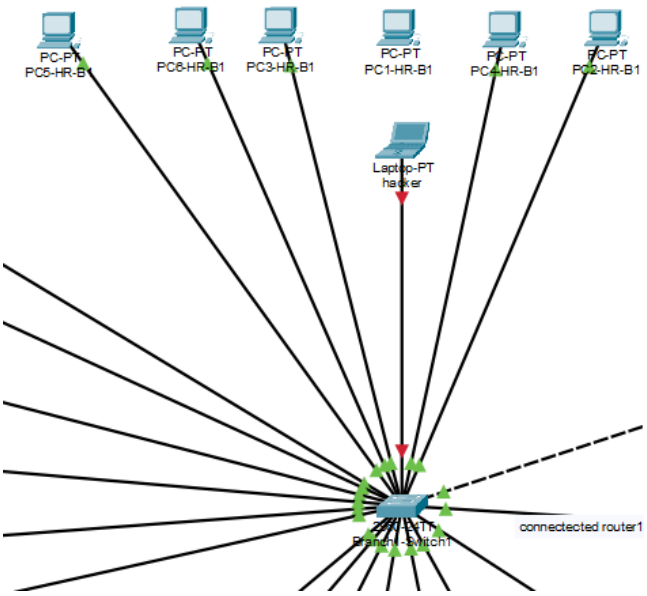
- **What it checks:** Access Control Lists (Packet Filtering).
- **The Logic:** You want to restrict "Low Security" users (Sales) from accessing "Medium Security" data (HR).
- **What it proves:** It proves your Firewall Rules are active. The router inspected the packet source (Sales IP), matched it against your "Deny" rule, and dropped the packet before it could reach HR an IT.

```
Pinging 192.168.20.51 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.20.51:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

C. Security (port security): Unknown Pc connection

- **What it checks:** Port Security (Layer 2 Security).
- **The Logic:** Prevents a physical intruder from unplugging a company device and plugging in their own laptop to steal data.

- **What it proves:** It proves the Switch is actively monitoring MAC addresses. It successfully detected a "Rogue" device (the laptop) and physically shut down the port to protect the network.




```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-------------------------------------------------------------------
        Fa0/1        1           1                1          Shutdown
-------------------------------------------------------------------
```

D. Services: Web Browser showing the company page

- **What it checks:** DNS Resolution & HTTP Access.
- **The Logic:** Employees shouldn't have to memorize IP addresses (like 192.168.1.100) to access services.
- **What it proves:** This is a "Full Stack" test. It proves:
  - **Connectivity:** The PC can reach the Server.
  - **DNS:** The PC can ask "Who is www.company.local?" and get an answer.
  - **HTTP:** The Server is running a website and serving pages.

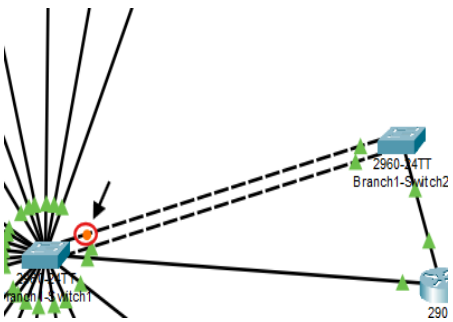
E. Internet: NAT Table with translation

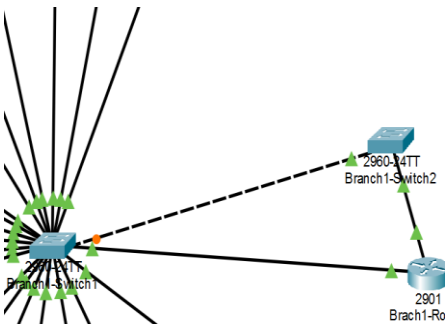
- **What it checks:** Network Address Translation (NAT).
- **The Logic:** Private IPs (192.168.x.x) act like internal extension numbers; they can't work on the public internet. They must be translated to a Public IP (10.0.0.x).
- **What it proves:** It proves your router is successfully masking internal IP addresses. It shows the router swapping the private source IP for its own public WAN IP so the traffic can leave the building.

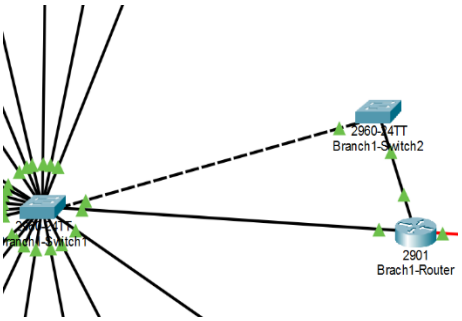
```
show ip nat translations
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 10.0.0.1:1        192.168.10.55:1    10.0.0.2:1         10.0.0.2:1
icmp 10.0.0.1:2        192.168.10.55:2    10.0.0.2:2         10.0.0.2:2
icmp 10.0.0.1:3        192.168.10.55:3    10.0.0.2:3         10.0.0.2:3
icmp 10.0.0.1:4        192.168.10.55:4    10.0.0.2:4         10.0.0.2:4
```

F. Redundancy: STP

- **What it checks:** Spanning Tree Protocol (Fault Tolerance).
- **The Logic:** If a main cable breaks, the network shouldn't crash. A backup cable needs to be ready to take over.
- **What it proves**: It proves your network creates High Availability. It shows that the backup link (which was blocked/Orange to prevent loops) automatically woke up and turned Green when the primary link failed.







13. Individual Contribution

Mesk Khaled	Network Planning
Basmala Moataz	Topology Design
Asmaa Mahmoud	Packet Tracer Setup
Mohamed Amgad	DHCP, DNS, NAT
Ziad Yasser	VLAN Configuration
Adham Ashraf	ACL, port security, Testi