**Network Design for Accounts and Delivery Department**

**ABSTRACT**

This document presents a network design aimed at establishing a seamless connection between the Accounts and Delivery departments within an organization. The primary goal is to improve data sharing, communication, and operational efficiency while maintaining robust network security and scalability. The design includes a secure local area network (LAN) infrastructure with high-speed Ethernet and reliable wireless access points to ensure stable connectivity. Centralized file storage and secure access protocols enable real-time data sharing and collaboration between departments. Unified communication tools, such as VoIP, instant messaging, and video conferencing, are incorporated to facilitate effective interaction. To safeguard sensitive financial and operational data, the design implements advanced security measures, including firewalls, encryption, and access controls. Furthermore, the modular nature of the design ensures scalability, allowing for future growth and additional departmental integration. This comprehensive network design promotes efficiency, accuracy, and security, enhancing overall organizational performance.

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| NAME OF THE TOPICS | PAGE NUMBERS |
| 1.Introduction | 4 |
| 2.Problem Statement | 5 |
| 3.Requirements | 6 |
| 3.1 Hardware Requirements | 6 |
| 3.2 Logical Requirements | 6 |
| 4.Network Design | 7 |
| 4.1 Department Setup | 8 |
| 4.2 IP Addressing Plan | 8 |
| 5.Implementation Steps | 8 |
| 5.1 Setting Up the Physical Layout | 8 |
| 5.2 Configuring Devices | 8 |
| 5.3 Testing Connectivity | 9 |
| 6.Network Diagram | 10 |
| 7.Verification Results | 11 |
| 7.1 Ping Test Results | 11 |
| 8.Additional Recommendation | 12 |
| 9.Conclusion | 13-14 |

**FIGURES**

|  |  |
| --- | --- |
| NAME OF THE FIGURES | PAGE NUMBER |
| Fig-1 Network design in real life | 4 |
| Fig-2 Connections | 5 |
| Fig-3 Visual representation of network | 10 |
| Fig-4 Connection ping test | 14 |

**1. Introduction**

This document describes the detailed process of designing, implementing, and verifying a network to connect the Accounts and Delivery departments. The objective is to establish efficient communication using appropriate hardware, IP addressing, and connectivity testing in Cisco Packet Tracer.

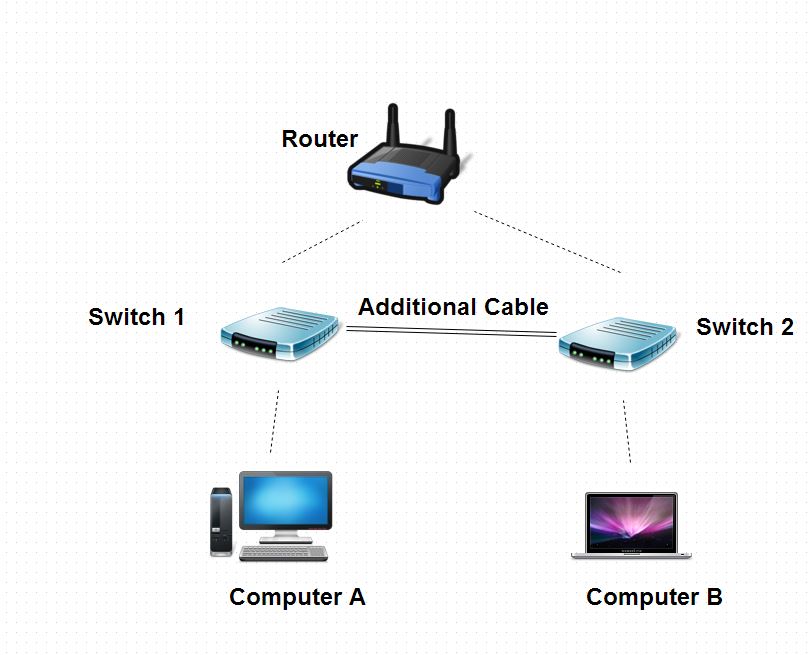


Fig-1 Network design in real life

**2. Problem Statement**

The task is to design a network in Cisco Packet Tracer for the Accounts and Delivery departments that meets the following requirements:

1. Each department has at least 2 PCs.

2. The network includes a router and switches to connect the departments.

3. The IP address 192.168.40.0/24 is used for configuration.

4. Ensure seamless connectivity across all devices.



Fig-2 Connections

**3. Requirements**

**3.1 Hardware Requirements**

|  |  |  |
| --- | --- | --- |
| **Component** | **Quantity** | **Purpose** |
| Router | 1 | To connect the Accounts and Delivery departments. |
| Switch | 2 | One switch per department for device connectivity. |
| PC | 4 | Two PCs per department for end-user access. |
| Ethernet Cables | 6 | For connecting PCs, switches, and routers. |

**3.2 Logical Requirements**

1. IP Addressing must use the 192.168.40.0/24 network.

2. A single router must serve as the default gateway for both departments.

3. Connectivity testing (pinging) must show successful communication between devices.

**4. Network Design**

**4.1 Department Setup**

|  |  |  |  |
| --- | --- | --- | --- |
| **Department** | **Device** | **Quantity** | **Connections** |
| Accounts Department | PCs | 2 | Connected to Accounts Switch |
|  | Switch | 1 | Connected to Router and Accounts PCs |
| Delivery Department | PCs | 2 | Connected to Delivery Switch |
|  | Switch | 1 | Connected to Router and Delivery PCs |

**4.2 IP Addressing Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| Router(G0/0) | 192.16.8.40.1 | 255.255.255.0 | - |
| Accounts-PC1 | 192.16.8.40.2 | 255.255.255.0 | 192.16.8.40.1 |
| Accounts-PC2 | 192.16.8.40.3 | 255.255.255.0 | 192.16.8.40.1 |
| Delivery-PC1 | 192.16.8.40.4 | 255.255.255.0 | 192.16.8.40.1 |
| Delivery-PC2 | 192.16.8.40.5 | 255.255.255.0 | 192.16.8.40.1 |

**5. Implementation Steps**

**5.1 Setting Up the Physical Layout**

1. Add the following devices to the Cisco Packet Tracer workspace:

1 Router, 2 Switches, and 4 PCs.

2. Use Ethernet cables to make the following connections:

Connect Accounts-PC1 and Accounts-PC2 to the Accounts Switch.

Connect Delivery-PC1 and Delivery-PC2 to the Delivery Switch.

Connect both switches to the Router.

**5.2 Configuring Devices**

Router Configuration

Access the router's interface and assign the IP address:

Router> enable

Router# configure terminal

Router(config)# interface gig0/0

Router(config-if)# ip address 192.168.40.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router# end

Router# write memory

**PC Configuration**

**On each PC:**

Navigate to Desktop > IP Configuration.

Enter the IP Address, Subnet Mask, and Default Gateway.

**5.3 Testing Connectivity**

1. Open the Command Prompt on each PC.

2. Use the ping command to test connectivity between:

Devices within the same department.

Devices across departments (e.g., Accounts-PC1 to Delivery-PC2).

**6. Network Diagram**

Add a visual representation of the network in Cisco Packet Tracer.

Diagram should include:

Router connected to two switches.

Each switch connected to two PCs.

Proper labeling of devices and IP addresses.

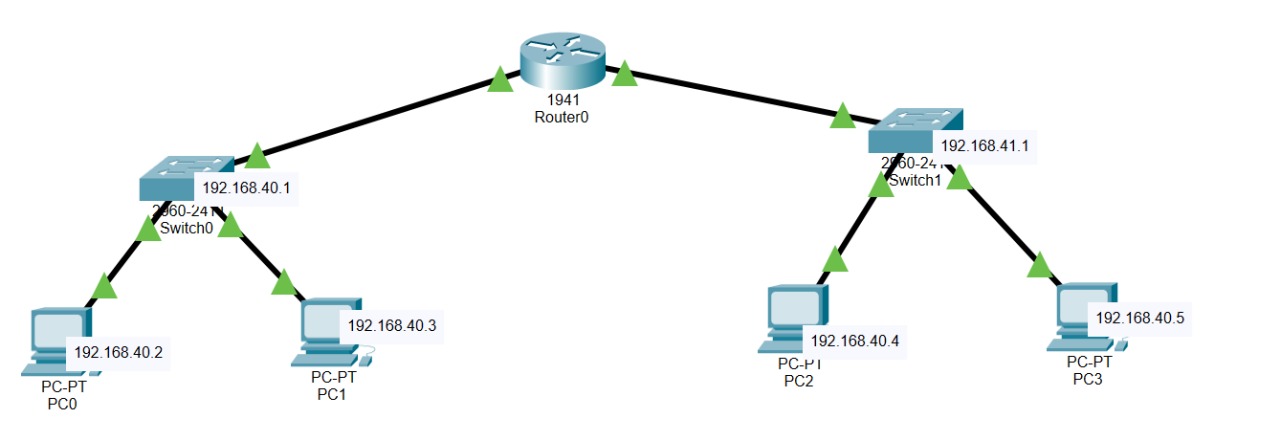


Fig-3 Visual representation of network

**7. Verification Results**

**7.1 Ping Test Results**

|  |  |  |
| --- | --- | --- |
| **Source Device** | **Destination Device** | **Ping Result** |
| Account-PC1 | Account-PC2 | Successful |
| Account-PC1 | Delivery-PC1 | Successful |
| Account-PC1 | Delivery-PC2 | Successful |
| Delivery-PC1 | Delivery-PC2 | Successful |

**8. Additional Recommendations**

**Security**: Implement VLANs and access control lists (ACLs) for better network security.

**Scalability**: Use subnetting if more departments or devices are added in the future.

**Monitoring**: Implement a monitoring tool like SNMP to track network performance.

**9. Conclusion**

The network design successfully connects the Accounts and Delivery departments. All devices are assigned unique IP addresses and communicate seamlessly as verified by ping tests. The solution is scalable, secure, and meets all given requirements.

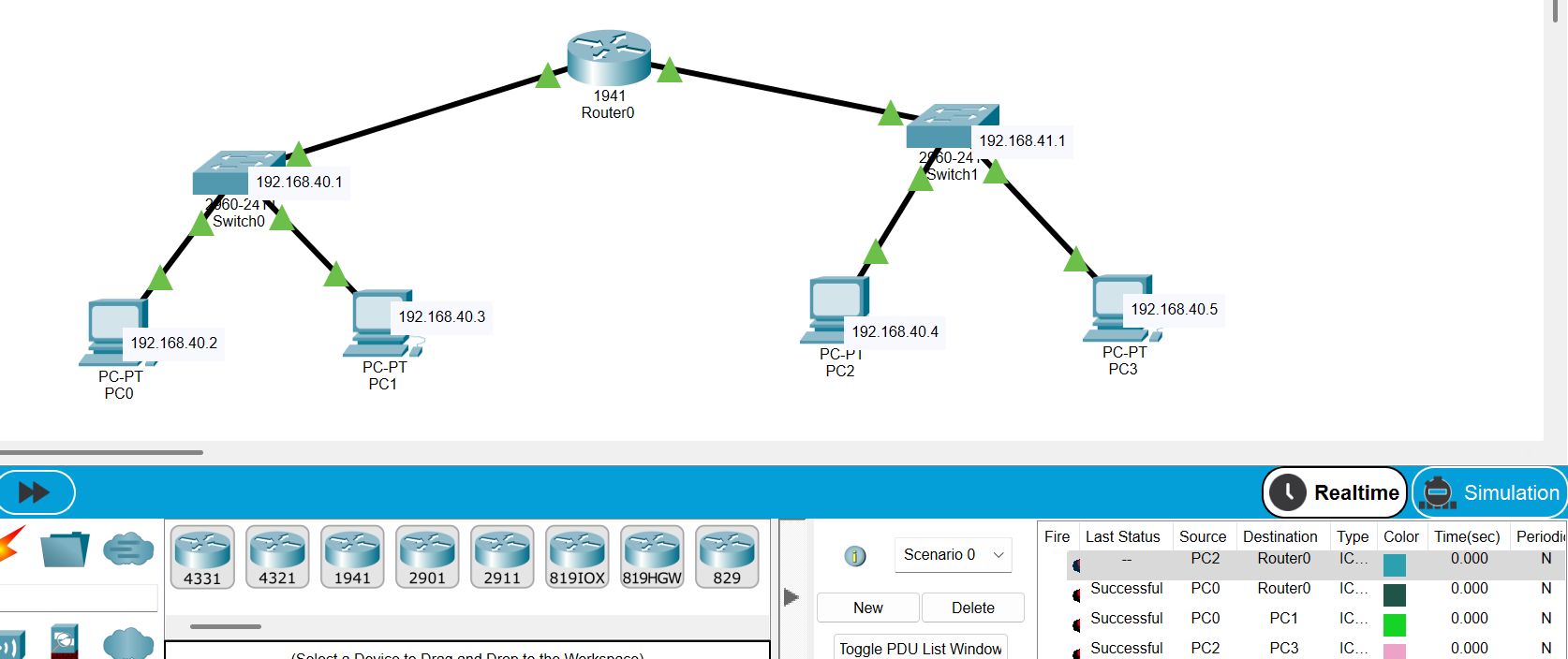


Fig-4 Connection ping test