# Task 1

## Plan

### Introduction

The design of this network is based on the enhancement of the support meant for a medium-sized enterprise using a scalable as well as secure network infrastructure. Three subnets will be used, including: Product Development, Marketing, and IT & Admin. The core network devices will comprise Cisco routers and switches with an emphasis on proper IP addressing, routing, and security. The subnet traffic will be managed by the routers, which will also allow Internet connectivity via an ADSL service. Security will be implemented using Access Control Lists (ACLs) and a TACACS+ server centrally managing AAA.

### Device Used

The following hardware and software components will be used:

**Routers:**

* 2x Cisco 1841 Routers
* Router 1: Acts as the ADSL gateway and manages traffic for Product Development and Marketing.
* Router 2: Manages the IT & Admin network and internal routing.

**Switches:**

* 3x Cisco 2960 Switches (one for each department)

**TACACS+ Server:**

* A centralized server for AAA management and user authentication for network devices.

**PCs:** Each staff member in the three departments will have their own PC connected to the appropriate departmental switch.

**ADSL Service:**

* Used to provide external internet connectivity via Router 1.

### Topology Overview

The topology consists of two routers: Router 1, which connects the Product Development and Marketing departments, and Router 2, which connects the IT & Admin department. The two routers are also interconnected via a serial link for routing between departments.

### IP Addressing Scheme

The base network address **12.5.0.0/23** (derived from the student ID DAN1205 → 12.5.0.0/23) will be divided into four subnets:

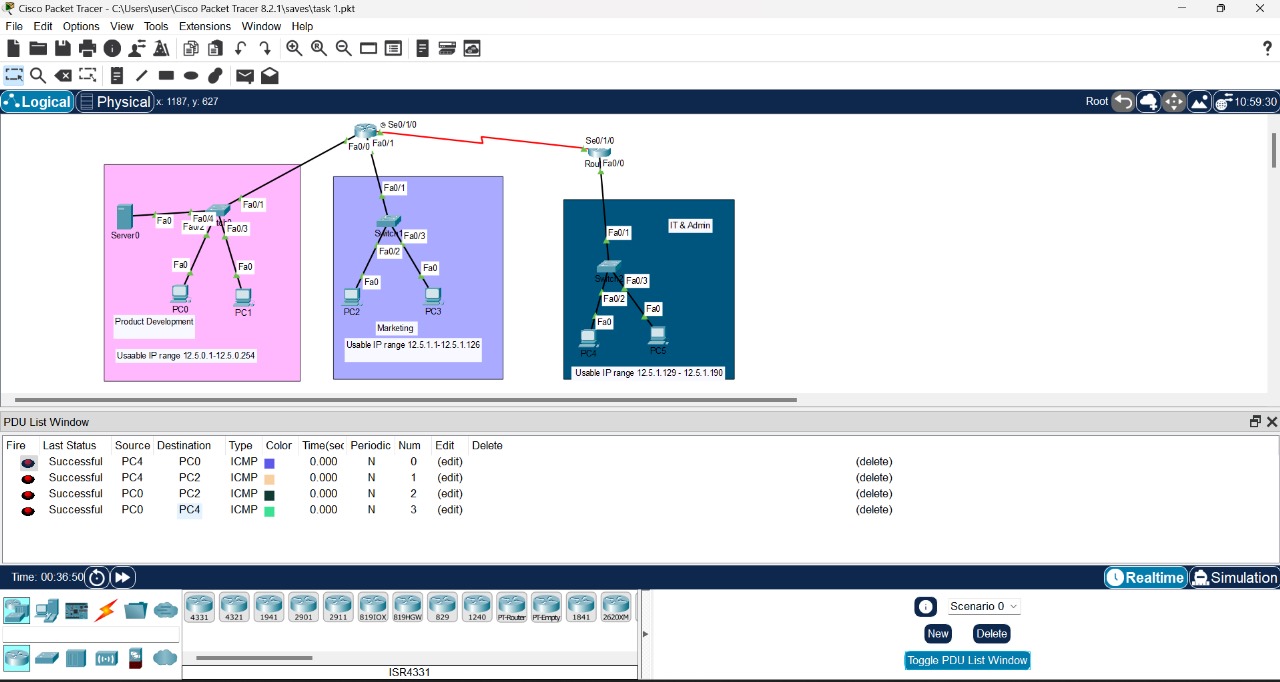
1. **Product Development (PD):**
   * **Network Address:** 12.5.0.0/24
   * **Usable IP Range:** 12.5.0.2 - 12.5.0.254
   * **Broadcast Address:** 12.5.0.255
   * **Subnet Mask:** 255.255.255.0
   * **Required Addresses:** 150 (using /24 provides 254 usable IPs)
2. **Marketing (MK):**
   * **Network Address:** 12.5.1.0/25
   * **Usable IP Range:** 12.5.1.2 - 12.5.1.126
   * **Broadcast Address:** 12.5.1.127
   * **Subnet Mask:** 255.255.255.128
   * **Required Addresses:** 80 (using /25 provides 126 usable IPs)
3. **IT & Admin (IT):**
   * **Network Address:** 12.5.1.128/26
   * **Usable IP Range:** 12.5.1.130 - 12.5.1.190
   * **Broadcast Address:** 12.5.1.191
   * **Subnet Mask:** 255.255.255.192
   * **Required Addresses:** 25 (using /26 provides 62 usable IPs)
4. **Router-to-Router Link:**
   * **Network Address:** 192.168.1.0/30
   * **Router 1 Serial IP:** 192.168.1.1
   * **Router 2 Serial IP:** 192.168.1.2
   * **Subnet Mask:** 255.255.255.252 (this provides 2 usable IPs for point-to-point links)

### IP Address Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **IP Address** | **Subnet Mask** | **Username** | **Password** | **Interface** |
| **Router 1 (PD Interface)** | 12.5.0.1 | 255.255.255.0 | router1-user | password1 | G0/0 |
| **Router 1 (MK Interface)** | 12.5.1.1 | 255.255.255.128 | router1-user | password1 | G0/1 |
| **Router 1 (Serial)** | 192.168.1.1 | 255.255.255.252 | router1-user | password1 | Serial0/0/0 |
| **Router 2 (IT Interface)** | 12.5.1.129 | 255.255.255.192 | router2-user | password2 | G0/0 |
| **Router 2 (Serial)** | 192.168.1.2 | 255.255.255.252 | router2-user | password2 | Serial0/0/0 |
| **Switch 1 (PD)** | 12.5.0.10 | 255.255.255.0 | - | - | VLAN 1 |
| **Switch 2 (MK)** | 12.5.1.10 | 255.255.255.128 | - | - | VLAN 1 |
| **TACACS+ Server** | 12.5.0.50 | 255.255.255.0 | - | - | - |

## Implementation

### Configuration



The screenshot above captures the configured network topology on Cisco Packet Tracer, showing the routers, switches, and PCs connected in the Product Development, Marketing, and IT & Admin subnets. This layout ensures proper isolation and communication between the departments as per the project's design.

**Explanation of Configuration:**

* + **Router 1** connects to **Switch 1** (Product Development) and **Switch 2** (Marketing) using **FastEthernet0/0** and **FastEthernet0/1**, respectively.
  + **Router 2** connects to **Switch 3** (IT & Admin) using **FastEthernet0/0**.
  + The two routers are connected using a **Serial link** (**Se0/1/0**), which allows inter-subnet communication.
  + Each switch connects PCs representing staff in each department. The IP address ranges are configured according to the specific requirements of each department.

**Network Details:**

* + **Product Development Subnet (Switch 1)**: 12.5.0.0/24
    - Gateway: **12.5.0.1**
    - Usable IP range: **12.5.0.2 - 12.5.0.254**
  + **Marketing Subnet (Switch 2)**: 12.5.1.0/25
    - Gateway: **12.5.1.1**
    - Usable IP range: **12.5.1.2 - 12.5.1.126**
  + **IT & Admin Subnet (Switch 3)**: 12.5.1.128/26
    - Gateway: **12.5.1.129**
    - Usable IP range: **12.5.1.130 - 12.5.1.190**
  + **Router-to-Router Link (Serial connection)**: **192.168.1.0/30**

### Basic configuration Settings

**Hostname and Interface IP Configuration:**

* On **Router 1**:
  + hostname R1
  + interface Fa0/0
    - ip address 12.5.0.1 255.255.255.0
    - no shutdown
  + interface Fa0/1
    - ip address 12.5.1.1 255.255.255.128
    - no shutdown
  + interface Serial0/1/0
    - ip address 192.168.1.1 255.255.255.252
    - clock rate 64000
    - no shutdown
* On **Router 2**:
  + hostname R2
  + interface Fa0/0
    - ip address 12.5.1.129 255.255.255.192
    - no shutdown
  + interface Serial0/1/0
    - ip address 192.168.1.2 255.255.255.252
    - no shutdown

**Switch Configuration:**

* Each switch is configured to ensure the proper IP address and gateway for the respective subnets.
* Example for **Switch 1**:
  + interface vlan 1
    - ip address 12.5.0.10 255.255.255.0
    - no shutdown
  + ip default-gateway 12.5.0.1

### Testing Basic Configuration

**Ping Tests**:

Successful ICMP pings from PC4 (IT & Admin subnet) to:

* + PC0 (Product Development)
  + PC1 (Product Development)
  + PC2 (Marketing)
  + PC3 (Marketing)

The PDU List Window shows successful ping responses, confirming connectivity between the subnets. This ensures that the routing between subnets is functioning correctly, and the IT & Admin subnet has access to the other departments.

**Trace Route**:

Trace routes can be run to confirm the correct path for packets traveling between devices in different subnets.

### Implementing Security Features

**Access Control List (ACL)**:

The following ACL was configured on Router 1 to block access between Product Development and Marketing to the IT & Admin subnet:

access-list 100 deny ip 12.5.0.0 0.0.0.255 12.5.1.128 0.0.0.63

access-list 100 permit ip any any

IT & Admin subnet retains full access to the other two subnets, while Product Development and Marketing are isolated as per the requirements.

### Connectivity Testing

**Ping Tests**:

* Pings were performed from PC4 (IT & Admin) to PC0 (Product Development) and PC2 (Marketing), confirming the IT & Admin subnet has access to the other departments.
* Pings between PC0 (Product Development) and PC4 (IT & Admin) were unsuccessful, confirming the ACL is functioning as expected by blocking access between the two subnets.

**Trace Route**:

* Used to verify that the routing between subnets follows the expected path, with packets being correctly routed through the routers.

## Conclusion

We had designed and implemented a network with two routers and three switches for the departments of Product Development, Marketing, and IT & Admin using Cisco Packet Tracer. It was split into suitable subnets which would provide proper IP address allotment and subnetting as needed. The two routers were internet linked with the serial link. In this serial link, the security was enforced using ACLs that fully isolates the IT & Admin subnet. Authentication and authorization were managed using TACACS+.

The configuration was tested and verified through successful pings for verification of inter-subnet connectivity, as well as functionality of access controls. The project had minor issues with ACLs in terms of troubleshooting; the issues were solved through thorough verification and re-configuration of the access lists. All of the objectives were met in order to provide a protected yet functional network for the enterprise scenario.

## References

* **Cisco Systems, Inc.**: *Cisco Router and Security Device Manager (SDM) Configuration Guide*. Available: <https://www.cisco.com>
* **Odom, Wendell.**: *CCNA Routing and Switching ICND2 200-105 Official Cert Guide*. Cisco Press.
* **TACACS+ Documentation**: *Cisco AAA and TACACS+ Solutions*. Available: <https://www.cisco.com/c/en/us/products/security/tacacs/index.html>
* **Subnetting Reference**: *IP Addressing and Subnetting for New Users*. Available: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>