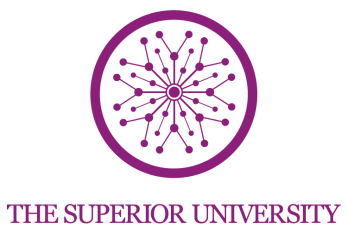
**

**SUBMITTED BY: M Akash Younas**

**SUBMITTED TO: Sir Rasikh Ali**

**ROLL NUMBER: BSSEM-F22-277**

**SECTION: 5D**

**DEPARTMENT OF SOFTWARE ENGINEERING**

**Small Office System Project Documentation**

**1. Introduction**

**Project Overview**

**The Small Office System project demonstrates the setup of a network infrastructure for a small office environment using Cisco Packet Tracer. The project aims to connect devices within the office and to the internet while ensuring network security, reliability, and scalability.**

**This network includes routers, switches, PCs, printers, and servers. Key configurations include static and dynamic routing, VLANs, DHCP, DNS, and basic security measures.**

**2. Project Objectives**

**The primary objectives are:**

1. **Connectivity: Ensure all devices are interconnected and have internet access.**
2. **Network Services: Provide DHCP for automatic IP assignment, DNS for name resolution, and FTP/HTTP for resource sharing.**
3. **Security: Implement VLANs, password protection, and ACLs to secure the network.**
4. **Scalability: Design a flexible topology for future expansion.**

**3. Network Requirements**

**Functional Requirements**

* **Internet access for all workstations.**
* **Internal communication between devices (e.g., file sharing, printing).**
* **Network segmentation for different departments.**

**Hardware Requirements**

| **Device** | **Quantity** | **Description** |
| --- | --- | --- |
| **Router** | **1** | **Cisco 2811 or similar** |
| **Switch** | **2** | **Cisco 2960 (Layer 2 switch)** |
| **PCs** | **6-10** | **End-user workstations** |
| **Server** | **1** | **For DHCP, DNS, FTP services** |
| **Printer** | **1** | **Network-enabled printer** |
| **Cabling** | **As needed** | **Ethernet cables (Cat5e/Cat6)** |

**Software Requirements**

* **Cisco Packet Tracer (version 7.2 or later).**
* **Windows/Linux OS for PCs in the simulation.**

**4. Network Design**

**Logical Topology**

**The logical topology includes:**

* **1 Router connected to an internet service provider (ISP).**
* **2 Switches connected to different departments (e.g., Admin and IT).**
* **PCs assigned to VLANs based on their departments.**

**Physical Topology**

* **Switch 1 connects to Admin PCs and the printer.**
* **Switch 2 connects to IT PCs and the server.**
* **Router connects to both switches and the ISP.**

**IP Addressing Scheme**

| **Device** | **IP Range** | **Subnet Mask** | **VLAN Assignment** |
| --- | --- | --- | --- |
| **Admin PCs** | **192.168.10.0/24** | **255.255.255.0** | **VLAN 10** |
| **IT PCs** | **192.168.20.0/24** | **255.255.255.0** | **VLAN 20** |
| **Server** | **192.168.30.2** | **255.255.255.0** | **VLAN 30** |
| **Router WAN** | **Dynamic (ISP)** | **Provided by ISP** | **N/A** |

**5. Network Configuration**

**Router Configuration**

**Step 1: Set the Router Hostname**

**Router> enable**

**Router# configure terminal**

**Router(config)# hostname OfficeRouter**

**Step 2: Configure Interfaces**

**OfficeRouter(config)# interface gigabitEthernet0/0**

**OfficeRouter(config-if)# ip address 192.168.10.1 255.255.255.0**

**OfficeRouter(config-if)# no shutdown**

**OfficeRouter(config)# interface gigabitEthernet0/1**

**OfficeRouter(config-if)# ip address 192.168.20.1 255.255.255.0**

**OfficeRouter(config-if)# no shutdown**

**Step 3: Enable Routing**

**OfficeRouter(config)# ip route 0.0.0.0 0.0.0.0 [ISP gateway IP]**

**Switch Configuration**

**Step 1: Set the Switch Hostname**

**bash**

**Copy code**

**Switch> enable**

**Switch# configure terminal**

**Switch(config)# hostname AdminSwitch**

**Step 2: Create VLANs**

**AdminSwitch(config)# vlan 10**

**AdminSwitch(config-vlan)# name Admin**

**AdminSwitch(config)# vlan 20**

**AdminSwitch(config-vlan)# name IT**

**Step 3: Assign Ports to VLANs**

**AdminSwitch(config)# interface fastEthernet0/1**

**AdminSwitch(config-if)# switchport mode access**

**AdminSwitch(config-if)# switchport access vlan 10**

**AdminSwitch(config)# interface fastEthernet0/2**

**AdminSwitch(config-if)# switchport mode access**

**AdminSwitch(config-if)# switchport access vlan 20**

**Server Configuration**

**Step 1: Configure DHCP on Server**

* **Go to the Services tab in Cisco Packet Tracer.**
* **Enable DHCP and configure IP ranges:**
  + **Pool: 192.168.10.0/24 for VLAN 10.**
  + **Pool: 192.168.20.0/24 for VLAN 20.**

**Step 2: Configure DNS on Server**

* **Enable the DNS service and add records:**
  + **Example: www.office.com -> 192.168.30.2.**

**PC Configuration**

**Step 1: Set PC to DHCP Mode**

* **Click on each PC, go to the Desktop tab, select IP Configuration, and choose DHCP.**

**6. Security Implementation**

**Password Protection**

**Enable Passwords on Router and Switch**

**bash**

**Copy code**

**OfficeRouter(config)# enable secret cisco123**

**OfficeRouter(config)# line vty 0 4**

**OfficeRouter(config-line)# password cisco123**

**OfficeRouter(config-line)# login**

**Access Control Lists (ACLs)**

**Example: Block Admin VLAN from accessing the IT VLAN**

**OfficeRouter(config)# access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255**

**OfficeRouter(config)# access-list 100 permit ip any any**

**OfficeRouter(config)# interface gigabitEthernet0/0**

**OfficeRouter(config-if)# ip access-group 100 in**

**7. Testing and Validation**

**Ping Test**

* **Use the ping command to test connectivity between devices:**

**PC> ping 192.168.20.1**

**Service Testing**

* **Verify DHCP: Ensure PCs receive correct IP addresses.**
* **Verify DNS: Access www.office.com from a PC browser.**
* **Verify VLAN Segmentation: Ping between VLANs to confirm isolation.**

**8. Troubleshooting**

1. **No Connectivity: Check cable connections and interface statuses (show ip interface brief).**
2. **No DHCP: Verify DHCP settings on the server.**
3. **Routing Issues: Verify static routes on the router.**

**9. Conclusion**

**The "Small Office System" project successfully demonstrates the design and implementation of a scalable and secure office network. It ensures efficient communication, proper network segmentation, and reliable internet access.**

**Future improvements could include implementing wireless access points or integrating advanced security features such as firewalls and intrusion detection systems.**