**Project No: 1**

**Title**

**Home office network**

**Student Name: Mubeen Riasat.**

**Table of contents**

* Introduction
* Project overview
* Objectives
* Scope
* Methodology
* System Architecture
* Implementation details
* Results and Analysis
* Conclusion
* References
* **Introduction**

**SOHO** allows computers in a home office or remote office to connect to a corporate network, or access centralized, shared resources. It is a LAN mainly referred to as a business category involving a small number of workers usually from 01 to 10. SOHO provides a lot of benefits such as easy-to-use and setup networks etc. introducing a small home office setup using Cisco Packet Tracer involves simulating a network environment with routers, switches, computers, servers and other networking devices. “Router” act as the gateway to the internet for your home office network. “Switch” provide connectivity to multiple devices within the home office network. “Security” firewalls use for security.

* **Project overview**

**Small office home office** network refers to a type of local area network connection designed for small businesses. SOHO networks can be a small wired Ethernet LAN or a combination of wired and wireless computers.

**Goals of SOHO is to achieve**

Security

Scalability

Reliability

Good performance, and resource sharing.

**In this SOHO network,** we designed network to increased productivity. With a SOHO network, multiple devices can be connected and share resources such as printers and files. This increases productivity by enabling faster access to information.

In this network, we use PCs, switches, routers and server to connect the devices with each other.

* **Objectives**

Objectives of this SOHO are:

1. Setup a small home office network with a reliable router.
2. Connect the workstation and printer.
3. Configure a file server for centralized storage.
4. Enable remote access for work-from-home scenarios.
5. Implement security measures.
6. Regularly backup important files.

* Scope

Nowadays, a home network lets you share your broadband internet connection with multiple people and people and devices. This means that everyone in the family can use their devices at the same time.

SOHO switches are typically designed without fans (to reduce noise impact), they should not be placed in poorly ventilated areas. Prolonged operation in such condition may lead to temperature increases and device shutdown, adversely affecting business operations.

SOHO is a small network contain LAN, in this number of workers usually from 1 to 10.

* **Methodology**

Tools used in this network are:

1. **Hardware:** workstation, printer, file server.
2. **Network components:** router and switches.
3. **Remote access:** VPN or remote desktop.

SOHO switch is an important item in SOHO network. The SOHO switch is responsible for connecting all devices in your network and ensuring all the devices can see each other.

SOHO router is a three part devices; modem to convert signals to what your ISP needs (cable, DSL etc) the routing function to protect you from the wild-slide.

* **System architecture**
* Use two switches to connect devices.
* Use 1 router to connect 2 LAN networks.
* Use server for security or other purpose.
* Also use printers in both LAN.

The following framework for this project is:

1. Start the network by designing its network topology. Make the physical layout (switches, routers etc).
2. Configuration of all devices according to the network.
3. Proper connectivity between devices.
4. Implement the basic security measures such as setting the password for device.
5. Documentation the network design, configurations and any special conditions. This document will be helpful for troubleshooting and future expansion.

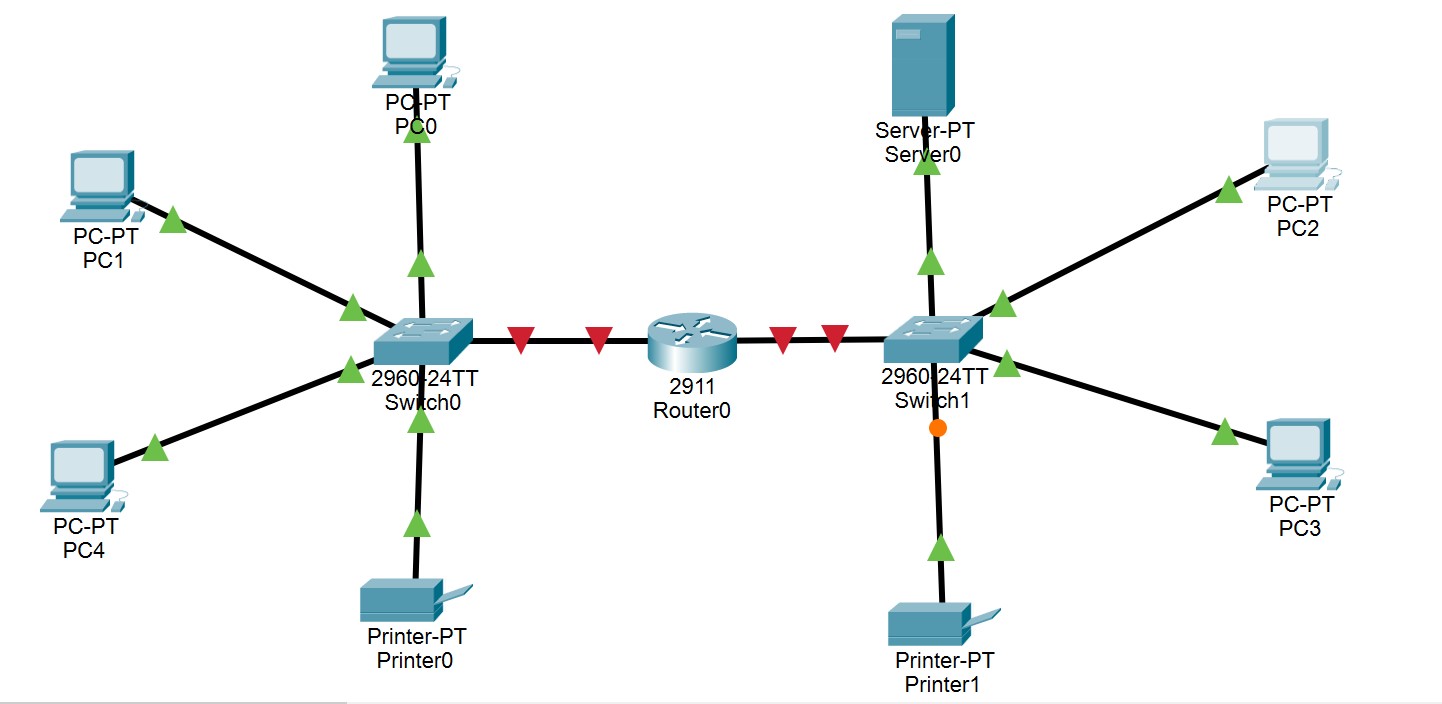
* **Implementation detail**

Implementation details of this SOHO network in cisco packet tracer are:

* Open your PC and open the cisco packet tracer.
* Design two LANs.
* Take two PCs, one printer and one server in first LAN.
* Take one switch in first LAN to connect the devices.
* Take three PCs and one printer in second LAN.
* One switch for second LAN to connect the devices.
* In first LAN connect all devices i.e. printer, server, PCs to switch through a copper straight wire.
* In second LAN also connect all the devices to switch through wire.
* Now use one Router to connect both LANs with each other.
* Connect the router to both switches by copper straight wire.

Now we have this type of network:

In this image we have red arrows on connection lines of router because we not configure the router. After the configuration of router our SOHO network will be correct.



**IP Addresses & Default Gateways:**

|  |  |  |
| --- | --- | --- |
| Devices | IP Addresses | Default Gateway |
| PC0 | 192.168.1.2 | 192.168.1.1 |
| PC1 | 192.168.1.3 | 192.168.1.1 |
| PC2 | 192.168.1.4 | 192.168.1.1 |
| PC3 | 128.16.1.3 | 192.16.1.1 |
| PC4 | 128.16.1.4 | 192.16.1.1 |
| printer 0 | 192.168.1.5 | 192.168.1.1 |
| printer 1 | 128.16.1.5 | 192.16.1.1 |
| Router | LAN1:192.168.1.1  LAN2:192.16.1.1 | No gateway |
| server | 128.16.1.2 | 192.16.1.1 |

* **For Telnet**

First open the router and go to the CLI

Following commands are used:

Enable

Configure terminal

Interface FastEthernet0/0

No shutdown

IP address 192.168.0.1 255.255.255.0

Exit

Hostname enable password cisco

Line vty o 15

Password 123

**For FTP**  hostname linux

Exit (press enter and enter)

Write enter

Then go to the PC and ping the IP Address and then telnet IP address.

* For FTP go to the server, click on services.
* On the FTP, set username is Maha134 and password is 1234 on the options like save, ok and add.
* Now go to the PC, click on Text Editor and type any text i.e. “hi how are you? This is the file of the PC which PC we opened.
* Save filename PC-150 then ok.
* Open the PC and click on command prompt write the following command:
* dir then ftp and IP address of server.
* Give the username and password.

* **Firewall**

Following instruction for firewall are:

1. Click on server and go to firewall, select the action “deny” and select the protocol “ICMP”.
2. Remote IP “0.0.0.0” and subnet mask will be “255.255.255.255”.

Save all this process and add it.

1. Now select the action “allow” and select the protocol “ICMP”.
2. IP will be “0.0.0.0” & select the subnet mask “255.255.255.255”.

Save all options and add it.

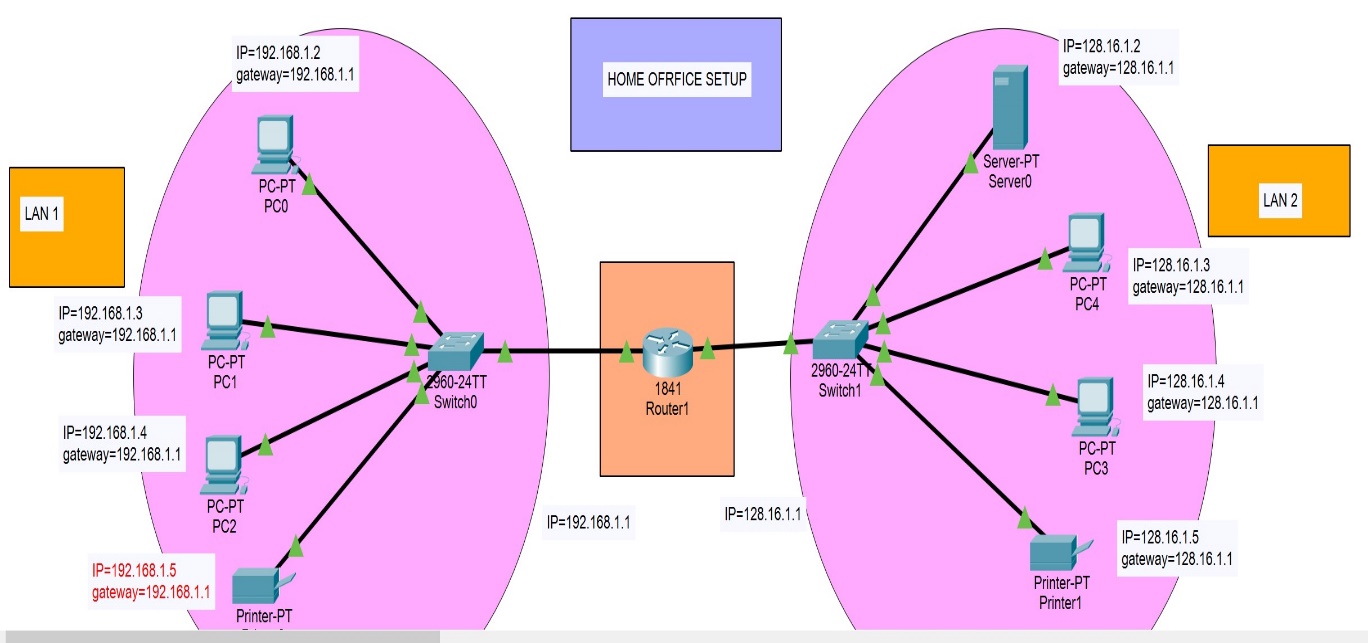
1. Go to the PC, ping “128.16.1.2”.

With this address this will not ping because of firewall.

1. Click on the same PC, and go to the web browser from desktop.

128.16.1.2, press enter it.

Now we have this type of network



* **Results and analysis**

To analyze the results obtained from the home office network project, we need to consider the data, metrics, and observations gathered during the implementation.

**Data:** This could include information on network performance, uptime, security incidents, remote access usage, backup success rate etc.

**Metrics:** key performance indicators such as network speed, latency, downtime, remote access utilization, backup completion time etc.

**Observations:** insights gained during the project implementation, usability issues etc.

In conclusion, analyzing the data, metrics and observation from the home office network project provides the insights into its performance, security posture, and usability. Addressing any issues identified and continuously monitoring ad optimizing the network ensure a reliable and secure home office environment, supporting remote work effectiveness.

* **Conclusion**

In conclusion, the successful implementation of the SOHO network project has provided a robust foundation for efficient remote work operations. By fulfilling the prerequisites of the hardware setup, network components and remote access capabilities, the project has enabled seamless connectivity and collaboration within the SOHO environment.

Overall, the home office network project has not only met the defined objectives but has also laid the groundwork for a secure, efficient, and productive remote work environment.

Moving forward, continuous monitoring, maintenance, and periodic updates will be essential to sustain optimal performance and address evolving needs and challenges un the dynamic landscape of remote work.