

# **SMALL OFFICE NETWORK SCENARIO**

## **MINI PROJECT REPORT**

*Submitted by*

**M. Raghava Varma**

**[Reg No: RA2011003010887]**

**K Sai Manikanta Pitchaiah**

**[Reg No: RA2011003010893]**

**Pendyala Praveen Reddy**

**[Reg No: RA2011003010886]**

**H V S S Subhash Pabbineedi**

**[Reg No: RA2011003010868]**

*Under the Guidance of*

**Dr. M Baskar**

(Associate Professor, Dept of Computing Technologies)

*in partial fulfillment of the requirements for the degree of*

**BACHELOR OF TECHNOLOGY  
in  
COMPUTER SCIENCE ENGINEERING**



**DEPARTMENT OF COMPUTING TECHNOLOGIES**

**COLLEGE OF ENGINEERING AND TECHNOLOGY**  
**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**  
**KATTANKULATHUR**  
**603 203 JUNE-2022**



**COLLEGE OF ENGINEERING AND TECHNOLOGY**  
**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**  
**KATTANKULATHUR**  
**603 203 JUNE-2022**

**BONAFIDE CERTIFICATE**

**Register No.** RA2011003010887,  
RA2011003010893,  
RA2011003010886,  
RA2011003010868.

Certified to be the bonafide record of work done by  
M.Raghava Varma, K Sai Manikanta Pitchaiah, Pendyala Praveen Reddy, H V S S Subhash Pabbineedi of  
CSE-CORE, B. Tech Degree course in the Practical **18CSS202J- Computer Communications**  
in SRM Institute of Science and Technology, Kattankulathur during the academic year 2021-2022.

**Date:**

**Lab Incharge**

**Examiner-1**

**HOD Signature**

**Examiner-2**

**Abstract:** Different users are there for the project; the users are present in different Department at different places. By this, a request is induced by one of the other users to interface with other user/users or sharing some data with them. And The user Data Can be Stored in the Server Where they can access it any time There can be a condition where a message is to be broadcasted to entire Office by a user. So, this paper is about communication among divergent users present at different sites, sharing this Different network. ONS Stands for the Office network scenario.

**Keyword:** ONS, CCNA, CISCO, IP, ROUTER, RIP(**R**outing **I**nformation **P**rotocol).

## **1. INTRODUCTION OF SMALL NETWORK DESIGN FOR OFFICE**

Small office computing has a character quite different from the computing environments that support large organizations, often called enterprise networks. Enterprise networks may have thousands of users, and involve a complex array of servers, mainframe systems, wide-area network links and the like. An enterprise network may serve multiple geographical locations and multiple buildings at each location. It is not unusual for an enterprise network to include several thousand devices. Such a network relies on a backbone network that channels data among locations and local area networks at each site. An enterprise network includes sophisticated equipment that must be maintained by highly trained network administrators.

Smaller organizations have more modest computing and networking requirements. They might have a dozen or so computers and a few laser printers. The network for the small office must allow members of the organization to share information, as well as printers and other peripherals. The computing needs of most small organizations can be met by a single LAN with one or two servers, using off-the-shelf components. Unlike the enterprise network, a small office LAN usually can be managed by one person with only moderate technical knowledge and experience.

While the small office network doesn't match the scale of its enterprise cousin, many of the same issues apply to both. The design of a small network must be simple, yet functional, secure and scalable. As the business grows, the network must easily expand with it. Even if the scale of the initial environment is small, avoid making technology decisions that might limit your company as it expands.

## **Assessing Functional Requirements**

Before you begin designing your network, have a clear sense of what you need it to accomplish. One prerequisite to network design is a complete assessment of expected functionality. Set aside some time to think about all the tasks you want to automate or make more efficient through your computer network. What business applications do you need to support? Do you simply need to provide shared access to word processing files, or do you have multiuser databases to support? Do you need electronic mail? Web servers? Point-of-sale operations? Will you require Internet access? Once you have considered all the business tasks and functions you expect to implement on the network, write them down and assign priorities to each item. As you begin deploying your plan, you might need to consider which parts you can do now and which can be addressed later. Take care of critical business functions first.

## ***Sizing the Network***

Have a clear idea of your network's expected size, considering its number of users and their intensity of use. Be sure to plan for future growth by building in lots of extra capacity from the beginning. Calculate what capacity you might need in two or three years. Consider the number of new users as well as dramatic increases in data storage needs per user. Your network should be designed to grow easily with incremental additions of existing technologies.

## ***Follow a Standard Approach***

It is important that you build your small business network using standard, industry-proven components. As business relationships change, you may need to interconnect your network with others. Protect your investment by building a network that is likely not to pose compatibility problems. If you are an independent branch of a larger organization, be consistent with umbrella group's practices and standards. Even if you are expected to maintain a separate network today, you may need to be part of its wide-area network in the future.

## ***Connectivity***

What types of external connections will your network need? Is Internet access necessary? If so, will a dial-up connection suffice, or will you need a full-time dedicated link? How much bandwidth? Will you need to connect with private networks, such as your home office network? One of the most challenging aspects of the small office network involves setting up links to external networks. Not only are these the most technically complex tasks of implementing a network, but they also carry significant costs.

## ***Creating the General Design***

Once you have assessed the new network's functional requirements and relative scale, you are ready to begin the design work. Network design involves several layers. You will need to make decisions on each of the following:

- Network type. Options include Ethernet, ATM or token ring. Most small networks are based on Ethernet, but even within this category there are options: Shared media 10Base-T, switched 10Base-T, shared media 100Base-T, and switched 100Base-T. To make a decision, you will need to scrutinize the relative bandwidth the network must support. The greater your need to support multimedia applications such as streaming audio or video, the more you will need a pricier high-bandwidth solution.
- The physical network. This includes network cabling, faceplates, and other issues of basic infrastructure. The kind of cabling you install depends on the network type you selected.
- Network communications equipment. To operate the network, you will need devices such as Ethernet hubs and routers.
- Network operating system. Currently, Microsoft Windows NT Server and Novell NetWare dominate this area. Some environments may require Unix-based servers. It is also possible to design a peer-to-peer network based on NT Workstation.
- Network server hardware.
- Data backup hardware and software.
- Client workstations. Consider the hardware (PC, Mac, etc.) and operating system (Windows 95 or 98, Windows NT, MacOS, etc.).

## ***Final Design: Making Technology Choices***

In the early design phase, we were painting in broad strokes. Now we must consider each aspect in detail. Each section below will take a closer look at the technology choices available, and describe how they apply to the small business network environment.

### **NETWORK TYPES:**

One of the first decisions in computer environment design is the selection of the network type- a group of products that work together, even if they are manufactured by different companies. Products in the same group each follow the same networking rules, and you can count on them to work together properly. Today's most common network types include Ethernet, token ring, and ATM. Each of these three offers a viable alternative for supporting a LAN, each with its own costs and performance benefits. As we will see, Ethernet stands as the prevailing technology and generally is the most appropriate choice for small business networks. Once you select a network

type, the network cards, cabling and network software you choose must be compatible with that group.

### ***Token Ring***

Token-ring networks can be found primarily in environments with a significant amount of IBM equipment. This network type uses a token-passing protocol; each computer communicates on the network only when presented with the network token. Computers read incoming data packets and transmit outgoing ones as the token rotates throughout the network. Token-ring networks became popular in organizations using IBM mainframes, and continue to be used to a limited degree. At one time, token-ring networks outperformed Ethernet, but this is no longer the case. Token-ring network cards are significantly more expensive than Ethernet cards, and much harder to find. A quick check of a couple of recent networking product catalogs showed dozens of Ethernet cards and not a single token-ring card. The only reason to consider basing a small business network design on token ring is in deference to some prevailing concern, such as compatibility with a larger organizational network.

### ***ATM***

Asynchronous transfer mode (ATM) follows a fundamentally different approach and competes with Ethernet for backbone networks and high-performance LANs. In an ATM network, data are broken into small fixed-size cells and switched in virtual circuits established between computers. Most ATM networks operate at a very respectable 145 Mbps. Today, ATM is most commonly found as the backbone technology for enterprise networks. ATM switches are much more expensive than Ethernet hubs, and they require a significant effort to configure. Like token-ring cards, ATM cards for desktop computers are high-priced and hard to find. A small organization would use an ATM-based LAN only if it required an extremely high-performance network to support data-intensive applications such as large-scale imaging projects.

### ***Ethernet***

Almost all small networks will use some type of Ethernet, the most inexpensive and flexible option. Network communications catalogs are stuffed with Ethernet products from a variety of vendors. As a reflection of Ethernet's dominance, most business-class desktop computers come with Ethernet ports built directly onto the motherboard.

Ethernet is associated with a set of networking rules called CSMA/CD (Carrier Sense Multiple Access with Collision Detection), formally specified by IEEE 802.3. These network rules describe how devices on the network communicate with one another. Ethernet is a broadcast network, in which all nodes have access to all datagrams or data packets. Each packet has an origin and destination address, and each computer should open the packet only if the destination address matches its own network address. The

network supports multiple devices per segment, and each device can transmit on the network at any time. If devices transmit exactly at the same time, however, a collision occurs and the transmissions are lost. Therefore, each station must check after it transmits to see if a collision occurred and, in the event of a collision, wait a random interval and retransmit.

Most varieties of Ethernet operate at 10 Mbps, and each of the nodes on a segment share this bandwidth. The stations on a segment share the overall available bandwidth and can cause collisions with one another in the process. The amount of overall bandwidth available to each station decreases and the likelihood of excessive collisions goes up as the number of stations per segment increases. The lower the number of stations per segment, the better your network will function. Various options are available to divide networks into multiple segments and to reduce the nodes per active segment.

### ***Past their Prime: Thick and Thinwire Ethernet***

There are several types of Ethernet cabling, some of which are obsolete. The original version of Ethernet, 10Base-5, or Thick Ethernet, relied on a rigid cable and required you literally to drill into the cable to install taps for each device on the network. While Thick Ethernet may still be in service in some older networks, it is obsolete and should not be used for new installations. 10Base-2, or Thinwire Ethernet, based on a thin, flexible RG-58 coaxial cable and BNC connectors, was extremely popular for a number of years because it was much easier to use than Thick Ethernet. No communications equipment was required—you just connected the network cards via the cables, and you had a functional network. Communications equipment was necessary only if you had multiple Ethernet segments that needed to be connected. The main problem with Thinwire Ethernet was its linear bus topology, where all the computers on a segment were chained together. If any single connector or cable along the segment had a problem, the entire segment would not function. Thinwire Ethernet also had limitations on the number of computers per segment and on the length of each segment; it, too, should be considered obsolete and avoided for any new network.

### ***10Base-T Ethernet***

The primary type of Ethernet in use today is 10Base-T, which operates at 10 Mbps and follows a star topology using unshielded twisted-pair cabling.

10Base-T Ethernet networks are very easy to set up. This flavor of Ethernet relies on hubs. Each computer has a dedicated cable that connects its Ethernet card to a port on the hub. Ethernet hubs are relatively passive and require little or no configuration. In most cases, you can plug in the hub to power, connect the cable and you've got an active network. As we'll see later, there are several features to choose from when buying a hub, but almost all types are essentially plug-and-play devices.

You will need drop cables to connect your computers to the network. Pre-built Ethernet cables are available from local computer stores and mail-order companies. You can also build your own, but it's seldom worth the effort. An Ethernet drop cable must be constructed from Category 5 unshielded twisted-pair cable, and terminated with RJ-45 connectors. These connectors look much like those for a telephone jack, except RJ-45s have eight connectors instead of four.

If you are working in a small space, you may be able to connect all the computers in your network directly to the hub without putting new wiring in the walls. But in most cases you will need to have a new cabling system installed in your building to support your network.

The most common, and least expensive, devices used with 10Base-T are shared media hubs, which represent a logical Ethernet segment. Each device connected to a port on a shared media hub shares the bandwidth of a 10-Mbps Ethernet segment and competes for collisions. Multiple hubs can be cascaded together, so that all the devices on multiple physical devices still form a logical Ethernet segment. Each port on a shared media hub connects via a UTP cable to a 10Base-T interface on a network device such as a computer or printer.

When selecting an Ethernet hub, be sure to consider manageability issues. Large networks require remote management capabilities for all devices on the network; each device must be capable of communicating all aspects of its operation with a central management device through protocols such as SNMP (Simple Network Management Protocol), as well as support common implementations such as MIB-2. Most large networks will have one or more dedicated workstations monitoring the network, with the capability to monitor the status of each device, measure overall network performance and alert a network administrator when a device fails, or when its performance falls below acceptable thresholds. Ethernet hubs are classified as either managed or non-managed. If your network is large and relies on central management, it is important to purchase manageable Ethernet hubs. Managed hubs are a requirement of most enterprise networks. Typically, you can purchase one hub with management capabilities, and cascade stackable units from that hub that can rely on the base unit for management. With smaller networks, you may be able to save considerable expense by purchasing unmanaged hubs. Manageability is a relatively expensive feature. If your environment is small and does not use centralized network management, it is not cost-effective to buy managed hubs; most small office networks will work quite well without managed devices. But if you buy non-managed hubs in a managed environment, you will miss out on the ability to monitor and tune the performance of your network, and to detect and repair many network problems in time to head off a total failure.

### ***Switched Ethernet***



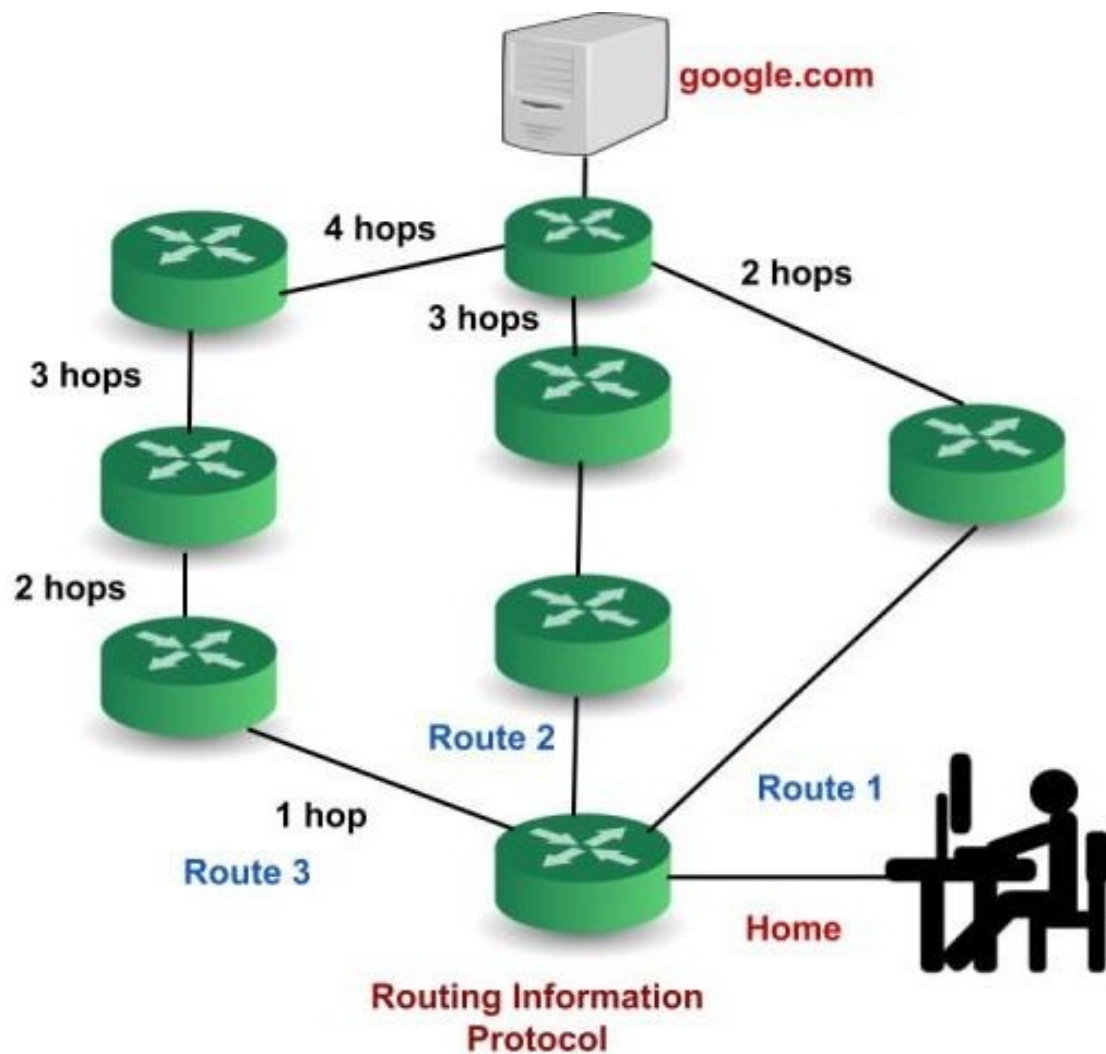
As we noted above, a shared media hub, or a group of hubs cascaded together, represent a logical Ethernet segment. One of the advances in Ethernet technology involves the use of switching technology. Switching greatly improves both the overall performance of an Ethernet network and the bandwidth available to each station, and it minimizes the impact of errors. The major difference between a shared media hub and an Ethernet switch is that each port on an Ethernet switch is its own logical segment. A device connected to a port on an Ethernet switch has a full 10-Mbps bandwidth to itself and need not contend with other devices for collisions. No special hardware is needed on the devices that connect to an Ethernet switch. The same network interface used for shared media 10Base-T hubs will work with an Ethernet switch. From that device's perspective, connecting to a switched port is just like being the only computer on the network segment. The main disadvantage of using Ethernet switches is that they can cost several times more than a shared media hub.

One common use for an Ethernet switch is to break a large network into segments. While it is possible to attach a single computer to each port on an Ethernet switch, it is also possible to connect other devices such as a shared media Ethernet hub. If your network is large enough to require multiple Ethernet hubs, you could connect each of those hubs to a switch port so that each hub is a separate Ethernet segment. Remember that if you simply cascade them off each other directly, the combined network is a single logical Ethernet segment.

### **Fast Ethernet**

Though Ethernet traditionally has been a 10 Mbps technology, faster versions are now available. While the 10 Mbps variety continues to be the most widely implemented, 100 Mbps Ethernet is rapidly catching on. To operate at this speed, you need network cards and hubs designed for 100Base-T, both of which are now sold by many vendors. While they cost more than 10Base-T, they make a remarkable difference in performance. You can implement 100Base-T on a small network at a very reasonable cost, especially if you stick with unmanaged, non-switched hubs. Even if you choose to go with 10Base-T hubs, consider purchasing network cards that can operate at either 10 or 100 bps. 10/100Base-T cards cost only a little more than ones that operate at 10 Mbps, and give you much more flexibility for upgrading your network in the future. Most 100Base-T hubs will automatically sense whether the card connected to each port is 10 or 100 Mbps and operate accordingly. For even higher performance, you can purchase 100Base-T switched hubs. You can expect significantly higher performance with such a device, but it will also add to your costs.

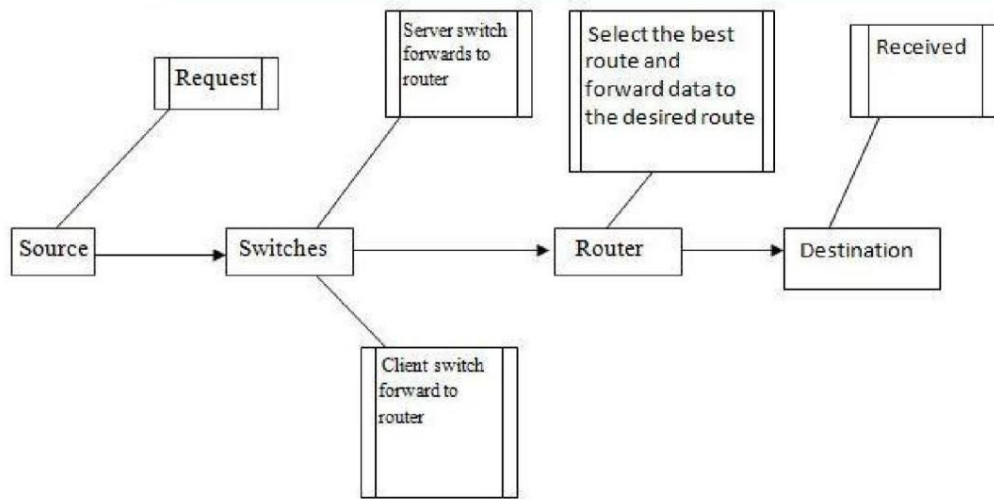
## 2. BASIC ARCHITECTURE :



The basic architecture of ONS generally makes use of various types of computers, router, servers, switches, Printer, personal PC's and Laptops.

## 3. WORKING OF ONS

This job with respect to the Office Networking Scenario is to provide a systematic, secure, valid, dependable communication among different departments. The work is done keeping in mind the complexity and cost factor. Various departments can simply divide the required data without any problem and can exchange their data without going to them physically, for example like a phone call, thus conserving energy and time.



Major components and their communication

## 4. REQUIREMENTS

The following division talk about the requirements interconnected to the interfaces for using communication by taking lots of data. These data combine client, software interfaces and other hardware that privilege the system to take its loads

### 4.1 User Interfaces

The requirements represent in this module discuss the ONS interfaces. The requirements are gathered in order to the main characteristics implemented in the system. The requirements always maintain the movements interconnected with the subheading characteristics.

### 4.2 Interface Formats

- The screen will be shown in virtual topology which that the Office designed.
- The network simulator that is Cisco Packet Tracer is a straightforward ,easy for implementation and gives a visual attraction of graphical user interface.
- It will display four switches ,different VLANs and 4 routers interconnected with each other.
- By clicking administrator, it will open graphical user interface for respective device.
- The configuration can be done by selecting CLI (command line interface).

**4.3 System Interface** In this scenario, giving data to any end device. Unauthorized user is not able to access ! "And appear a log in form to the authorized user by giving login credentials. We can reset the password by the help of network administrator.

**4.4 Hardware Interfaces** To run the cisco packet simulator, we need some basic requirements,

That is given below:-

- Random access memory (RAM): 512 MB
- Central Processing Unit (CPU): Intel Pentium Dual core.
- Storage: 500 MB of free disk space
- Display resolution: 800 x 600

Recommended H/w:

- CPU: Intel Pentium III 1.0 GHz
- Display resolution: 1024 x 768
- Storage: 300 MB free disk space
- RAM: > 512 MB Run the module i.e., for a live project (a network),

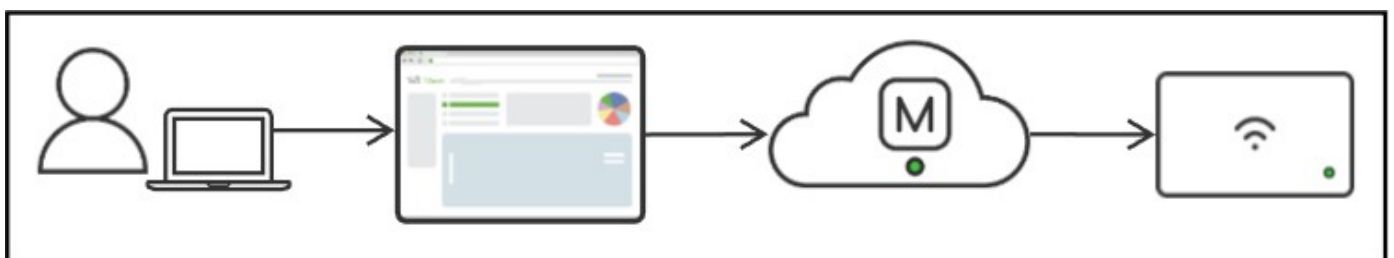
the hardware requirements are:

1. 3 Switches (Cisco 2960 switch) and 1 Switch (Cisco PT-Switch)
2. 4 Router (Cisco 1941 router)
3. PC (Generic) Computer system for server Cross over cable Straight through cable
4. Server
5. Printer
6. Meraki Server

### Meraki Server:

The Meraki cloud solution is a centralized management service that allows users to manage all of their Meraki network devices via a single simple and secure platform.

Users are able to deploy, monitor, and configure their Meraki devices via the Meraki dashboard web interface or via APIs. Once a user makes a configuration change, the change request is sent to the Meraki cloud and is then pushed to the relevant device(s).

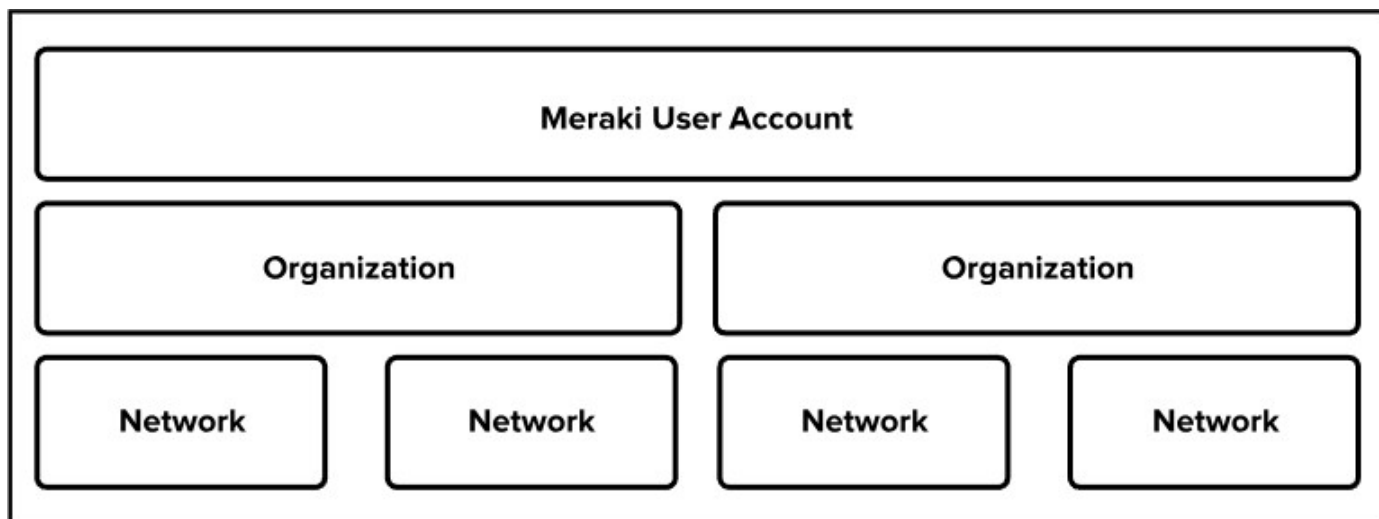


**The Meraki dashboard:** A modern web browser-based tool used to configure Meraki devices and services.

**Account:** A Meraki user's account, used for accessing and managing their Meraki organizations.

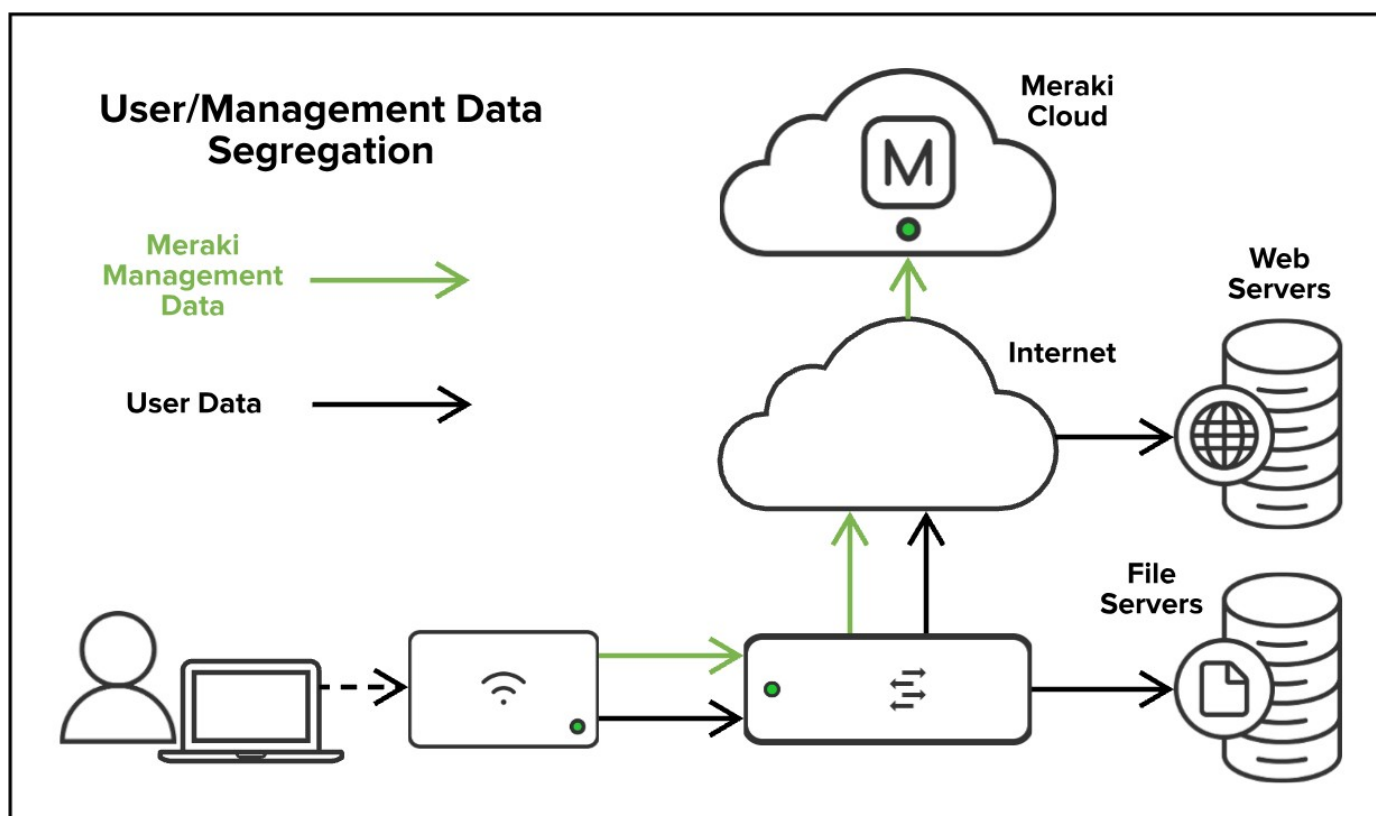
**Organization:** A logical container for Meraki networks managed by one or more accounts.

**Network:** A logical container for a set of centrally managed Meraki devices and services.



**Management data:** The data (configuration, statistics, monitoring, etc.) that flows from Meraki devices (wireless access points, switches, security appliances) to the Meraki cloud over a secure internet connection.

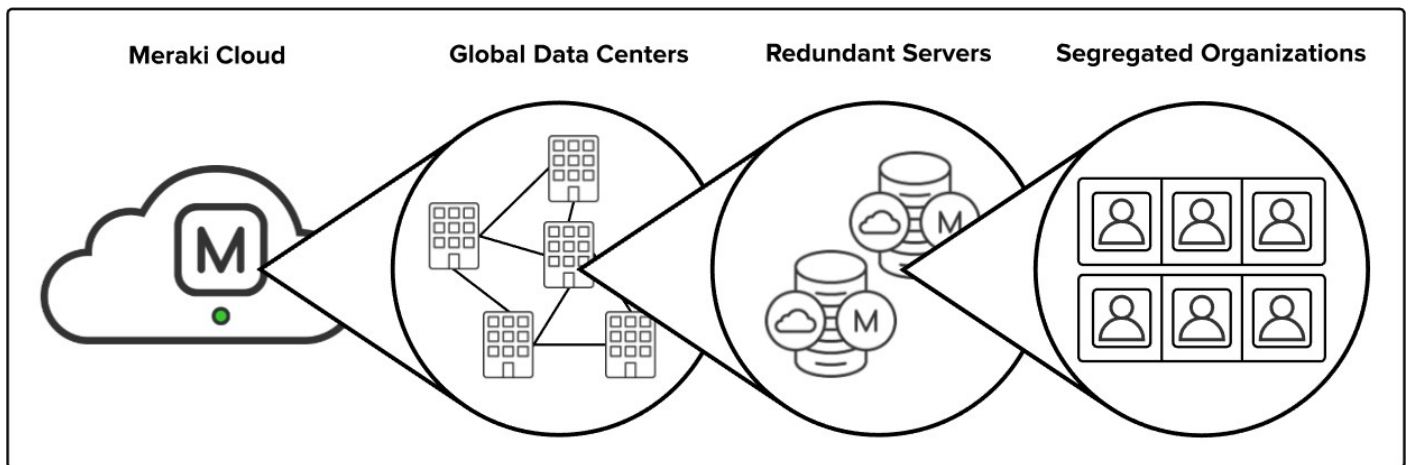
**User data:** Data related to user traffic (web browsing, internal applications, etc.). User data does not flow through the Meraki cloud, instead flowing directly to their destination on the LAN or across the WAN.



## Meraki Cloud Architecture

The Meraki cloud is the backbone of the Meraki management solution. This "cloud" is a collection of highly reliable multi-tenant servers strategically distributed around the world at Meraki data centres. The servers at these data centres are powerful hosting computers comprised of many separate user accounts. They are called multi-tenant servers because the accounts share (equal) computing resources on their host (the server). However, even though

these accounts share resources, Meraki ensures that customer information is kept secure by restricting organization access based on account authentication, as well as hashing authentication information such as user passwords or API keys.



#### 4.5 Software Interfaces:

The requirements required in the ONS are as follows:

- Operating System: - Microsoft Windows 7 or above.
- Cisco Packet Tracer

#### 4.6 Communication Interfaces

- The execution of the system will be in the existing network.
- The system is mainly based on a client-server application where the server providing data to access all the services.

### 6. IP DESCRIPTION OF ONS

An IP address is a numerical tag assigned to each device (e.g., computer, printer, etc.) taking part in a computer network that uses the Internet Protocol for any communication. It is a 32-bit number. One is IPv4 and the other is IPv6. IPv4 is of 32 bit and is represented as X.X.X.X i.e., each octet is parted by a dot. For e.g.: 191.157.2.2 .In this project IPv4 is used. The assignment of IP address is reliant upon the number of hosts existing in the network. Depending on the number of hosts present in the Office; for this network the IP to be used is a class C IP addresses i.e., 192.168.10.0 with a subnet mask of 255.255.255.224. And this IP is then distributed among different VLANs and ports for communication. The larger IP is fragmented into smaller networks by using the idea of VLSM (Variable Length Subnet Mask). Variable Length Subnet Masking (VLSM) - is a method that permits network administrators to divide an IP address space into subnets of different sizes. VLSM is the breaking down of IP addresses into subnets (multiple levels) and assigning it based on the individual needs on a network.

**Routing Information Protocol (RIP)** is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

### **Hop Count**

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

### **Features of RIP**

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust routing information received from neighbour routers. This is also known as *Routing on rumours*.

### **RIP versions :**

There are three versions of routing information protocol – **RIP Version1**, **RIP Version2**, and **RIPng**.

## **7. PRODUCT FEATURES**

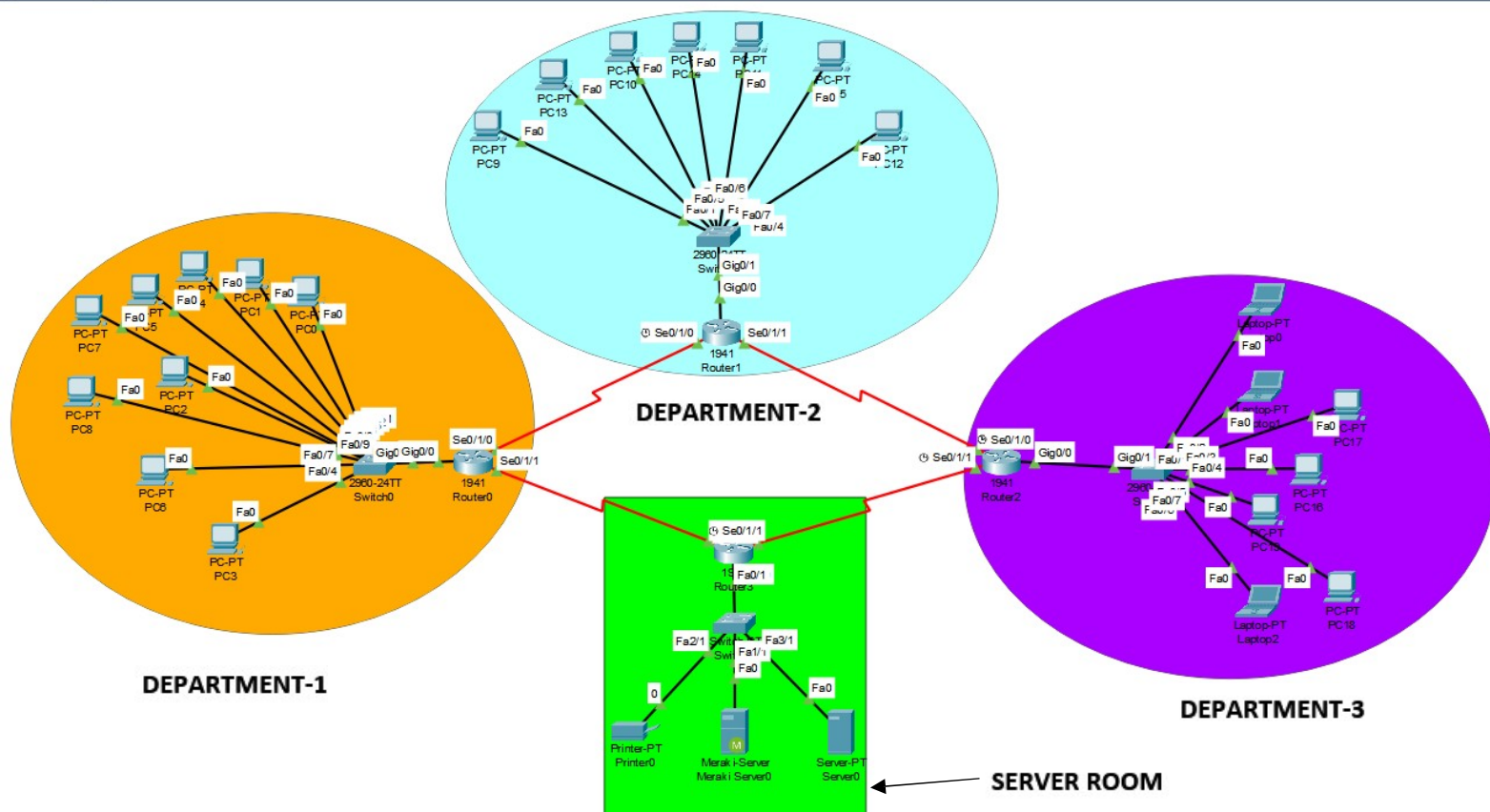
1. This network is based on client-server architecture.
2. Tree topology is used here.
3. 4 client switches are present for the four levels of Department and they are associated to a server switch.
4. All the departments are categorized into various VLANs, which are connected to the 4 switches based on the sequence in which they are accommodated on the storey.
5. Likewise, various departments limited into VLANs and share switches corresponding to their levels.
6. A request is made by any system of any department and it is forwarded to client switch which furthermore transmits it to the server.



7. Port-securitys are there that are executed on various ports of the switches and gives reliability.
8. The data is then transferred to its connected router.
9. Router serves as DHCP server for assigning IPs to the host computers and also generally routes the data to the desired destination.
10. All appliances are under the reliability of their respective passwords known to the network executive only.
11. User can change the password any time they want to.

**8 . SCOPE OF ONS** This project is given us an efficient methodology connected among all computers that are used in a respective Office. Apart from interconnection, the project economical is made the topology by keeping in mind about the cost. The most important points are authentication and security to prevent the unauthorized access.

## 9. RESULTS OF ONS





## PC-0 Pinging with Meraki Server

The screenshot displays the Cisco Packet Tracer interface. In the foreground, the 'PC0' window is open, showing the 'Desktop' tab with a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>PING 192.168.11.2'. The output indicates a successful ping with 4 packets sent and received, 0% loss, and an average round trip time of 8ms. The background shows a network topology with various devices including switches, routers, and servers.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

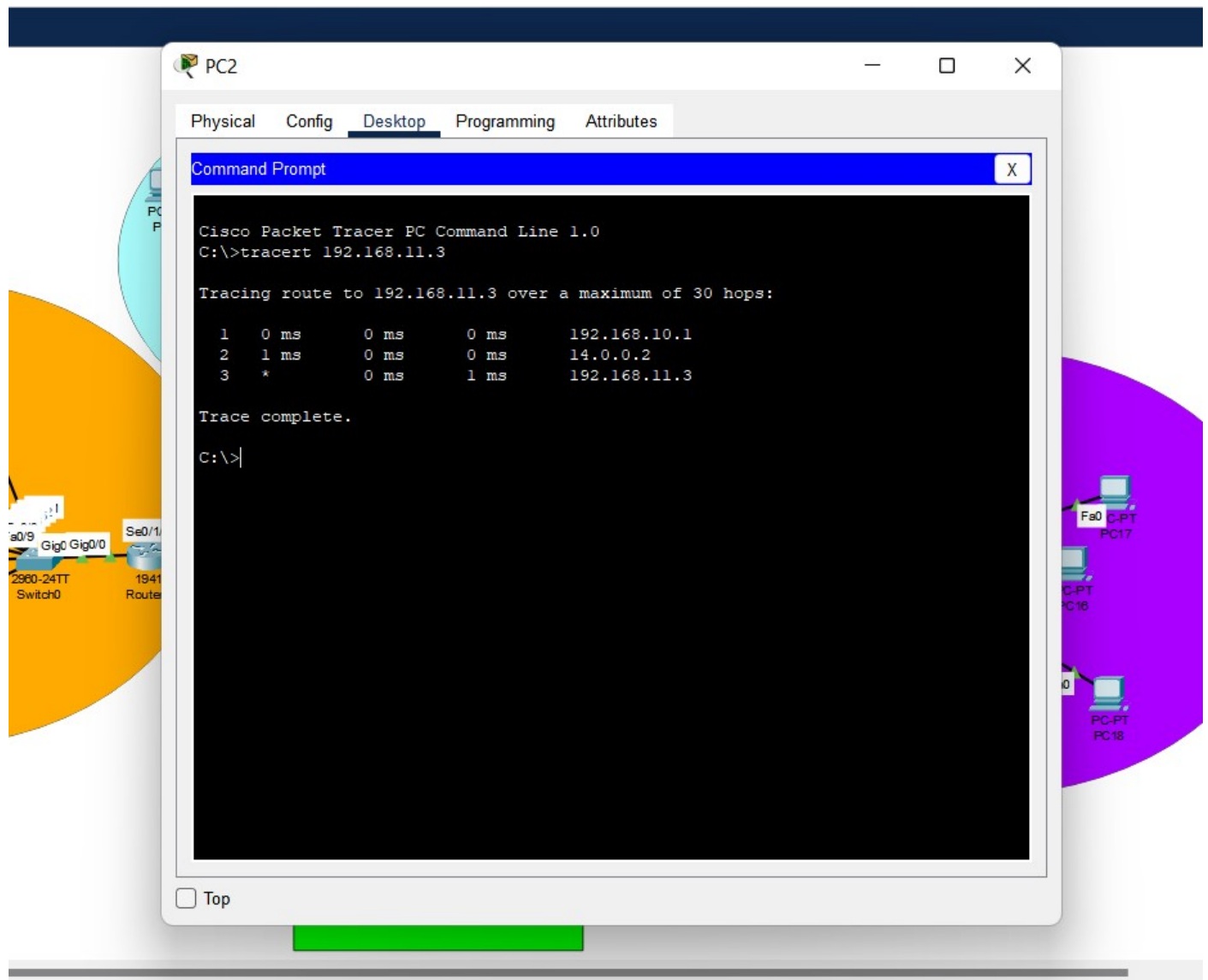
Reply from 192.168.11.2: bytes=32 time=23ms TTL=126
Reply from 192.168.11.2: bytes=32 time=10ms TTL=126
Reply from 192.168.11.2: bytes=32 time=1ms TTL=126
Reply from 192.168.11.2: bytes=32 time=1ms TTL=126

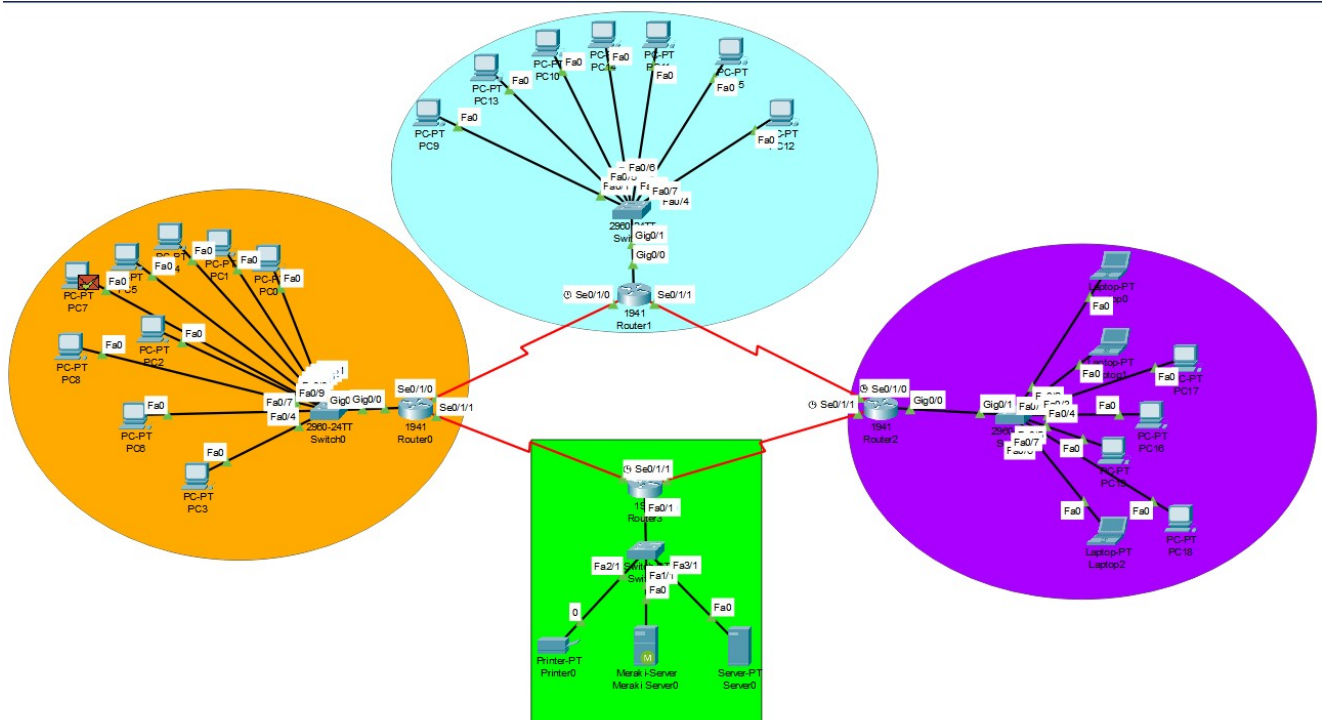
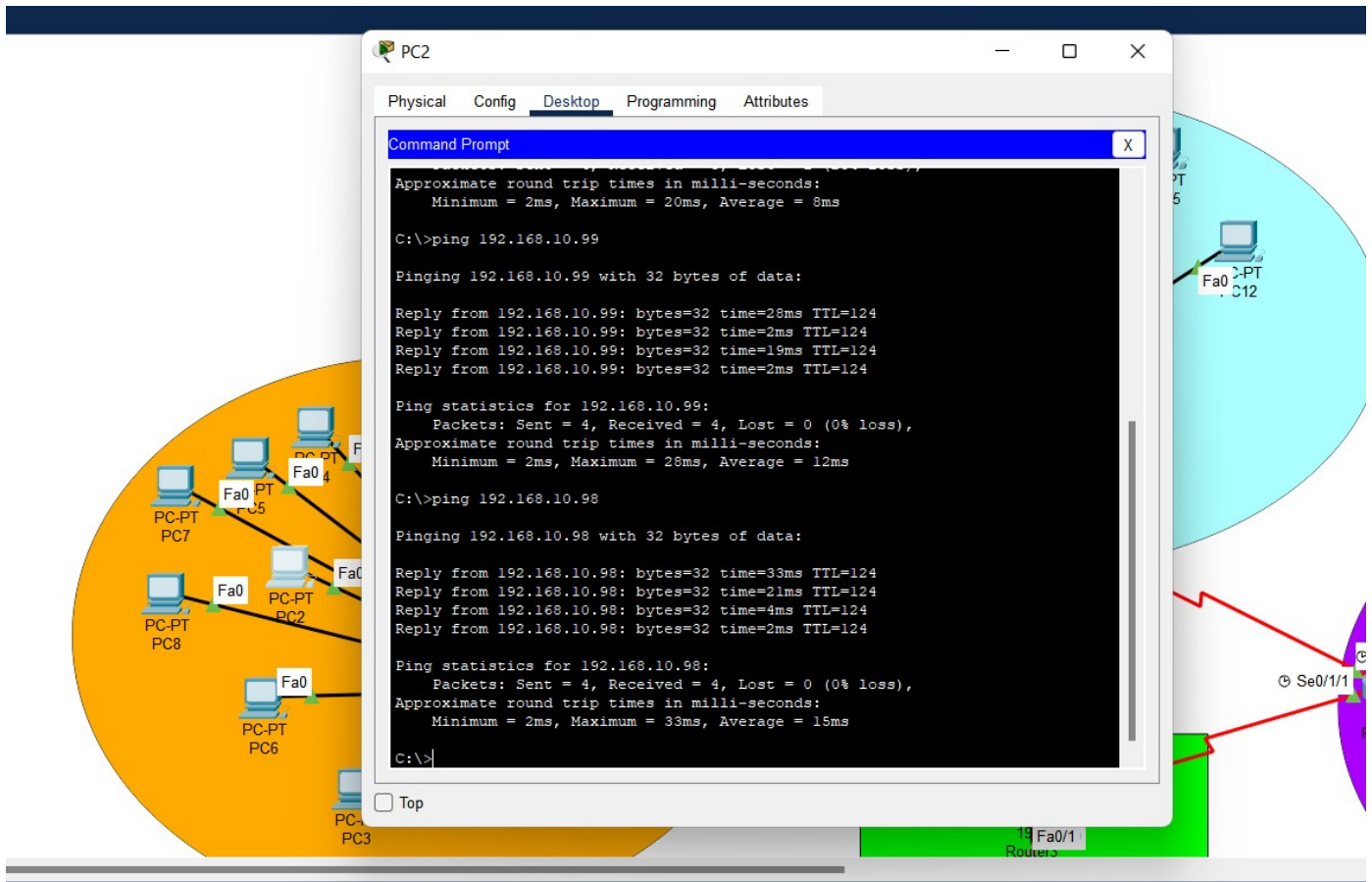
Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 23ms, Average = 8ms

C:\>
```

The screenshot shows the main interface of Cisco Packet Tracer. The network topology is visible, featuring three main clusters of devices. The left cluster (orange) includes a switch (2960-24TT Switch0) connected to several PCs and laptops. The middle cluster (light blue) includes a switch (2960-24TT Switch1) connected to several PCs and laptops. The right cluster (purple) includes a switch (2960-24TT Switch2) connected to several PCs and laptops. A central green cluster contains a Meraki-Server and a Server-PT. The interface also shows a 'Logical' tab, a 'Physical' tab, and a 'Realtime' tab. A status bar at the bottom indicates the time is 00:43:38 and the simulation is running.

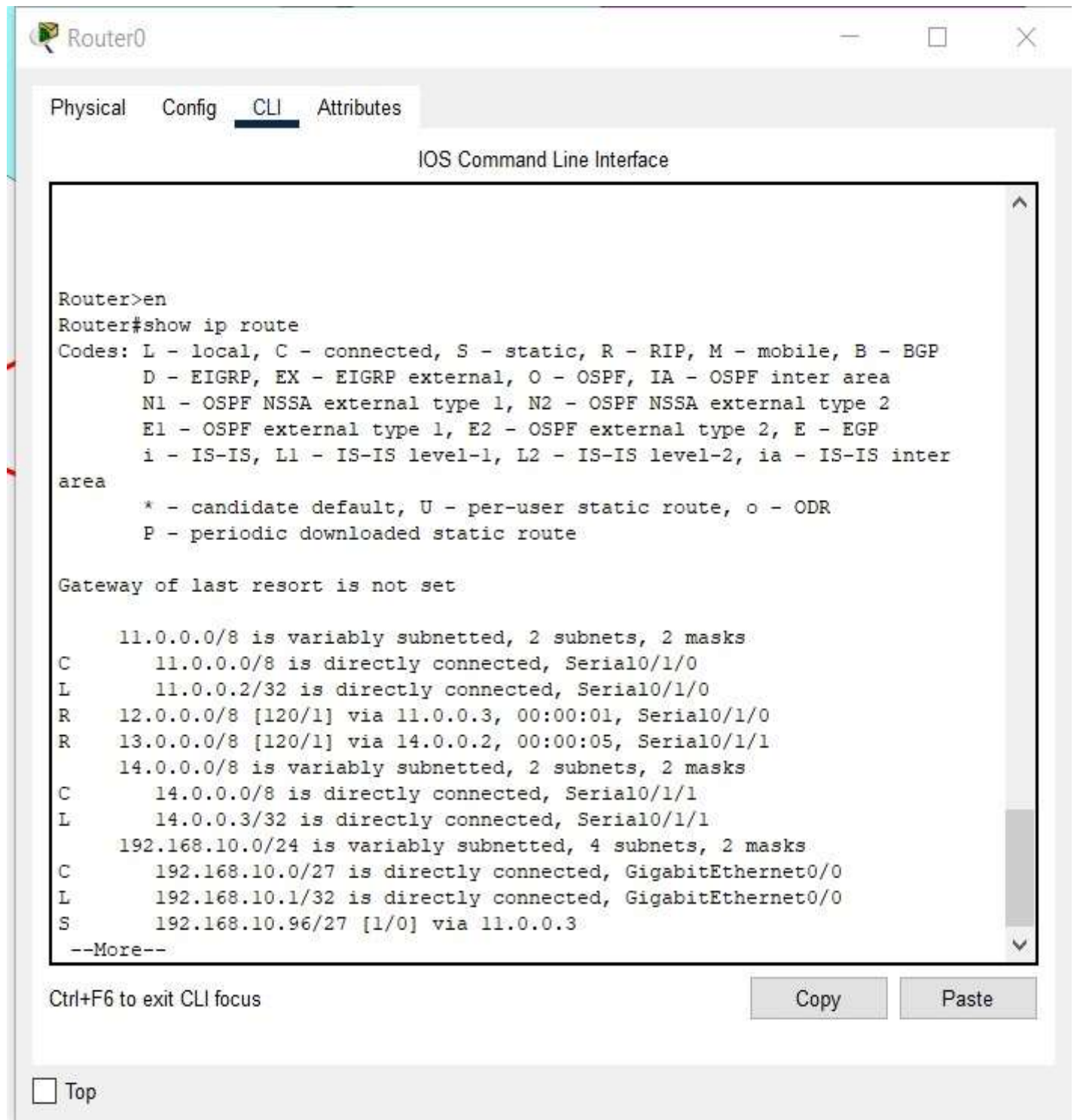
## Finding Route to the Printer Using TRACERT Command





## 10 .Show Commands :-

A. show ip route



The screenshot shows a window titled "Router0" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The command "Router>en" has been entered, followed by "Router#show ip route". The output shows the routing table with various codes and routes. The codes are: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP, i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area, \* - candidate default, U - per-user static route, o - ODR, P - periodic downloaded static route. The output also shows the gateway of last resort is not set. The routes are: 11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks; C 11.0.0.0/8 is directly connected, Serial0/1/0; L 11.0.0.2/32 is directly connected, Serial0/1/0; R 12.0.0.0/8 [120/1] via 11.0.0.3, 00:00:01, Serial0/1/0; R 13.0.0.0/8 [120/1] via 14.0.0.2, 00:00:05, Serial0/1/1; 14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks; C 14.0.0.0/8 is directly connected, Serial0/1/1; L 14.0.0.3/32 is directly connected, Serial0/1/1; 192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks; C 192.168.10.0/27 is directly connected, GigabitEthernet0/0; L 192.168.10.1/32 is directly connected, GigabitEthernet0/0; S 192.168.10.96/27 [1/0] via 11.0.0.3. The output ends with "--More--".

```
Router>en
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set


  11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.0.0.0/8 is directly connected, Serial0/1/0
L       11.0.0.2/32 is directly connected, Serial0/1/0
R       12.0.0.0/8 [120/1] via 11.0.0.3, 00:00:01, Serial0/1/0
R       13.0.0.0/8 [120/1] via 14.0.0.2, 00:00:05, Serial0/1/1
  14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       14.0.0.0/8 is directly connected, Serial0/1/1
L       14.0.0.3/32 is directly connected, Serial0/1/1
  192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.10.0/27 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
S       192.168.10.96/27 [1/0] via 11.0.0.3
--More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

## B. Show ip interface brief

 Router0

Physical Config CLI Attributes

IOS Command Line Interface

Press RETURN to get started.

Router>en  
Router#show ip interface brief

Interface	IP-Address	OK?	Method	Status
Protocol				
GigabitEthernet0/0	192.168.10.1	YES	manual	up
GigabitEthernet0/1	unassigned	YES	manual	down
FastEthernet0/0/0	unassigned	YES	unset	up
FastEthernet0/0/1	unassigned	YES	unset	down
FastEthernet0/0/2	unassigned	YES	unset	down
FastEthernet0/0/3	unassigned	YES	unset	down
Serial0/1/0	11.0.0.2	YES	manual	up
Serial0/1/1	14.0.0.3	YES	manual	up
Vlan1	unassigned	YES	unset	administratively down

Router#


Ctrl+F6 to exit CLI focus

CopyPaste

☐ Top



## C. Show ip protocol

 Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#show ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 28 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  GigabitEthernet0/0  12  1
  Serial0/1/1         12  1
  Serial0/1/0         12  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  11.0.0.0
  14.0.0.0
  192.168.10.0
Passive Interface(s):
Routing Information Sources:
  Gateway           Distance      Last Update
  11.0.0.3           120          00:00:02
  14.0.0.2           120          00:00:04
--More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

**11.CONCLUSION :-**To Design the network outlook for the community college network scenario produces the substructure for all other exposure in the service framework such as security of the network, wireless area network, mobility as well as putting the justification to provide safety and security, operational efficiencies, virtual learning environments, and secure classrooms. This paper describes the network design scenario approved by Cisco, as well as where we can apply these scenario within the various locations of a community Office network. Finally, key network foundation services such as switching, routing, multicast, and high availability are given for the full college network scenario.

**REFERENCES :-**1)Cisco Certified Network Associate Study Guide fifth edition by Todd Lammle

2)<http://www.ciscopress.com/articles/article.asp?p=328773&seqNum=3>

3)Interconnecting Cisco Devices Part 1 by Cisco

4)Interconnecting Cisco Devices Part 2 by Cisco

5)[www.wikipedia.com](http://www.wikipedia.com)

6)Computer Networks-A top-down approach by Kurose and Ross.

7)[http://www.cisco.com/en/US/products/hw/routers/ps214/products\\_tech\\_note09186a00801f5d85.shtml](http://www.cisco.com/en/US/products/hw/routers/ps214/products_tech_note09186a00801f5d85.shtml)

8)<http://www.symantec.com/connect/forums/sep-client-switch-computer-mode-user-mode-automatically-and-moving-other-group>.

9)[http://en.wikipedia.org/wiki/Router\\_\(computing\)](http://en.wikipedia.org/wiki/Router_(computing)).

10)[https://documentation.meraki.com/Architectures\\_and\\_Best\\_Practices/Cisco\\_Meraki\\_Best\\_Practice\\_Design/Meraki\\_Cloud\\_Architecture#:~:text=The%20Meraki%20cloud%20solution%20is,web%20interface%20or%20via%20APIs](https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Meraki_Cloud_Architecture#:~:text=The%20Meraki%20cloud%20solution%20is,web%20interface%20or%20via%20APIs).