COMPUTER NETWORKS

Case Study

COLLEGE NETWORK System

Group Number 16

|  |  |  |
| --- | --- | --- |
| **Registration No** | **Name** | **Email ID** |
| CB.EN.U4CSE21412 | Boya Abhiram | cb.en.u4cse21412@cb.students.amrita.edu |
| CB.EN.U4CSE21430 | K .Mahammad Sami | cb.en.u4cse21430@cb.students.amrita.edu |
| CB.EN.U4CSE21431 | K.Adithya | cb.en.u4cse21431@cb.students.amrita.edu |
| CB.EN.U4CSE21462 | T.Bhargavi | cb.en.u4cse21462@cb.students.amrita.edu |

Table Of Contents

|  |  |
| --- | --- |
| **Content** | **Page no** |
| 1.Introduction | 3 |
| 2.Problem Statement | 4 |
| 3.protocols used | 5 |
| 4.Network devices used | 7 |
| 5.Performance parameters | 8 |
| 6.Ip adressing plan | 10 |
| 7.Architecture design | 13 |
| 8.server room | 14 |
| 9.Implementation | 15 |
| 10.RIP | 17 |
| 11.Departments | 19 |
| 12.Results | 20 |
| 13.Analytical Questions | 24 |
| 14.Table | 25 |

**Importance of Networking in College Environments:**

**1. Interdepartmental Communication:**

Networking fosters seamless communication between different departments, enabling effective collaboration among faculty, staff, and students.

**2. Resource Sharing:**

Facilitates the sharing of resources like printers and storage, optimizing resource utilization and reducing the need for redundant equipment in each department.

**3. Access to Centralized Services:**

Allows access to centralized services such as databases, email servers, and learning management systems, ensuring consistency and efficiency in service delivery.

**4. Course Materials and Information Sharing:**

Enables efficient sharing of course materials, research findings, and academic information, supporting collaborative projects and interdisciplinary studies.

**5. Student Services:**

Supports online registration, access to library resources, communication with professors, and the implementation of e-learning platforms and online assessments.

**6. Security and Access Control:**

Incorporates security measures to control access, ensuring the protection of sensitive data and resources with different levels of access based on roles.

**7. Administrative Functions:**

Streamlines administrative processes such as attendance tracking, grading systems, and student information management.

**8. Distance Learning and Virtual Collaboration:**

Allows for the implementation of distance learning programs and virtual collaboration tools, especially relevant in situations with remote students and faculty.

**Problem statement:**

**Background**: In today's dynamic educational landscape, colleges face the challenge of creating a robust and scalable network infrastructure that can meet the diverse communication and collaboration needs of different departments, students, and faculty members.

**Problem:** The current state of our college network lacks a well-organized and optimized LAN topology. This deficiency leads to inefficiencies in communication, resource sharing, and administrative functions. The absence of a cohesive network design hinders the seamless exchange of data and information between departments, impacting collaboration and the overall efficiency of academic and administrative processes.

**Objective:** The primary goal of this project is to design and implement an optimized LAN topology for our college network, addressing the identified issues. This includes enhancing interdepartmental communication, improving resource sharing, strengthening security measures, streamlining administrative processes.

**How WiFi works ?**

1. Wireless Access Points (APs):

Deploy wireless access points strategically across the college campus to provide coverage in various locations, such as classrooms, labs, offices, and common areas.

Use enterprise-grade access points that support the latest Wi-Fi standards for better performance and security.

1. VLANs (Virtual Local Area Networks):

Implement VLANs to logically segregate Wi-Fi traffic based on different departments, user groups, or purposes.

Assign each VLAN a unique identifier to facilitate efficient network management and security.

1. Router Configuration:

Configure routers to facilitate inter-VLAN routing, allowing communication between different VLANs while maintaining logical separation.

Implement security measures to control and monitor the traffic between VLANs.

1. Security Measures:

Enforce WPA3 (Wi-Fi Protected Access 3) or WPA2 security protocols to secure Wi-Fi communications.

Utilize strong authentication methods, such as WPA3-Enterprise with 802.1X authentication, for user authentication.

**Protocols Used:**

1. Internet Protocol (IP)
2. Routing Information Protocol (RIP)
3. Transmission Control Protocol (TCP)
4. File Transfer Protocol (FTP)
5. Domain Name System (DNS)
6. Hypertext Transfer Protocol (HTTP)

**Software/Operating System used:**

* **Cisco Packet Tracer:**

Cisco Packet Tracer is a widely used network simulation tool for learning and practicing networking concepts. It allows users to design, configure, and simulate network topologies. The report mentions the use of Cisco Packet Tracer in designing and implementing the college network scenario.

* Cisco IOS (Internetwork Operating System):

Cisco IOS is the operating system used on Cisco routers and switches. In the context of the report, the routers and switches in the college network scenario may be running Cisco IOS.

* Windows/Linux for End Devices:

The end devices, such as computers and servers, in the college network may run operating systems like Windows or Linux.

* Web Servers:

The web server mentioned in the report could be running a web server software like Apache, Nginx, or Microsoft IIS. The specific operating system for the web server is not mentioned.

**Programming Languages:**

a) Java

b) C

d) Assembly Language for processors like 8086

e) C++

**Network Requirements**

1: The new system should be able to reduce internet downtime. Download and upload links should be maintained above 5 Mbps speed requirement.

2: Network will be scalable.

3: The system should support remote access.

4: Should comprise of data centers with necessary security features and support.

**Networking devices used :**

* Cisco Catalyst 6509 Switch:

This is a high-performance switch that is part of the Cisco Catalyst 6500 Series. It's equipped with Cisco 720 supervisors and Virtual Switching System (VSS).

* Cisco 4500 Switch:

We have used Cisco 4500 switches, which are likely part of the Cisco Catalyst 4500 Series. These switches are often used in campus networks.

* Mobility Services Engine (MSE) and Cisco Aironet 1140 Access Points:

The Mobility Services Engine (MSE) and Cisco Aironet 1140 access points are part of the Cisco Unified Wireless Network. They are used for wireless connectivity within the college network.

* Routers (Router0, Router1, Router2):

The project outlines the routing protocol plans for three routers: Router0, Router1, and Router2. These routers are crucial for routing data between different departments or segments within the college network.

* Web Server:

A web server is used in the proje t, indicating the presence of a server that hosts web content, potentially used for the college website or other web applications.

* FTP Server:

An FTP server is mentioned, which could be used for file transfer purposes within the college network.

* DNS Server:

A DNS server is mentioned, indicating the presence of a Domain Name System server that resolves domain names to IP addresses.

* End Devices (Computers, Laptops, Printers):

The report mentions various end devices, such as computers, laptops, and printers, connected to different departments in the college.

* Firewall

Used for server side as only ip protocols are enabled and others are disabled

For security reasons.

**SECURITY DEVICES**

1. ACCESS CONTROL LISTS (ACLS)

- Implemented for controlling user access to the external site using ACLs.

2. FIREWALL RULES

- Firewalls for securing the network and controlling traffic

**Performance parameters:**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Meaning** | **Formula** |
| **Bandwidth** | Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time | Expressed as [bits](https://web.archive.org/web/20190816003233/https:/whatis.techtarget.com/definition/bit-binary-digit) per second ([bps](https://web.archive.org/web/20190816003233/https:/searchnetworking.techtarget.com/definition/bits-per-second)), modern network links have greater capacity, which is typically measured in millions of bits per second ([megabits per second](https://web.archive.org/web/20190816003233/https:/searchnetworking.techtarget.com/definition/Mbps), or Mbps) or billions of bits per second ([gigabits per second](https://web.archive.org/web/20190816003233/https:/whatis.techtarget.com/definition/Gbps-billions-of-bits-per-second), or Gbps). |
| **Throughput** | Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again. |  |
| **Packet Loss** | Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.Due to network congestion | Efficiency = 100% \* (transferred - retransmitted) / transferred  Network Loss = 100 - Efficiency |
| **Transmission time** | The time required for transmission of a message depends on the size of the message and the bandwidth of the channel. | Transmission time=Message size / Bandwidth |
| **Propagation Time** | Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed. | Propagation time = Distance /Propagation speed |
| **Processing Delay** | Time taken by the processor to process the data packet is called processing delay. |  |
| **Queuing Delay** | Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay. |  |
| **Jitter** | Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network | Latency=sum of all delays    To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1). |

**IP Addressing Plan**

**1.IT DEPARTMENT:**

|  |  |
| --- | --- |
| **IT DEPARTMENT (192.168.1.0)** | |
| HOD CABIN | 192.168.1.2 |
| IT LAB 1 | 192.168.1.3 |
| IT LAB 2 | 192.168.1.4 |
| IT LAB 3 | 192.168.1.5 |
| IT LAB 4 | 192.168.1.6 |
| Printer 0 | 192.168.1.7 |

|  |  |
| --- | --- |
| **COMPUTER DEPARTMENT (192.168.2.0)** | |
| CS HOD CABIN | 192.168.2.2 |
| CS LAB 1 | 192.168.2.3 |
| CS LAB 2 | 192.168.2.4 |
| CS LAB 3 | 192.168.2.5 |
| CS LAB 4 | 192.168.2.6 |
| Printer 7 | 192.168.2.7 |

**2.Computer Department:**

**3.OTHERS :**

|  |  |
| --- | --- |
| **OTHERS (192.168.3.0)** | |
| OFFICE | 192.168.3.2 |
| Printer 2 | 192.168.3.6 |
| EXAM CELL | 192.168.3.3 |
| Printer 3 | 192.168.3.7 |
| ENQUIRY | 192.168.3.4 |
| TPO | 192.168.3.5 |
| Printer 4 | 192.168.3.8 |

**4..SERVER ROOM :**

|  |  |
| --- | --- |
| **SERVER ROOM (1.0.0.0)** | |
| FTP SERVER | 1.0.0.4 |
| PC1 | 1.0.0.5 |
| DNS SERVER | 1.0.0.2 |
| WEB SERVER | 1.0.0.3 |

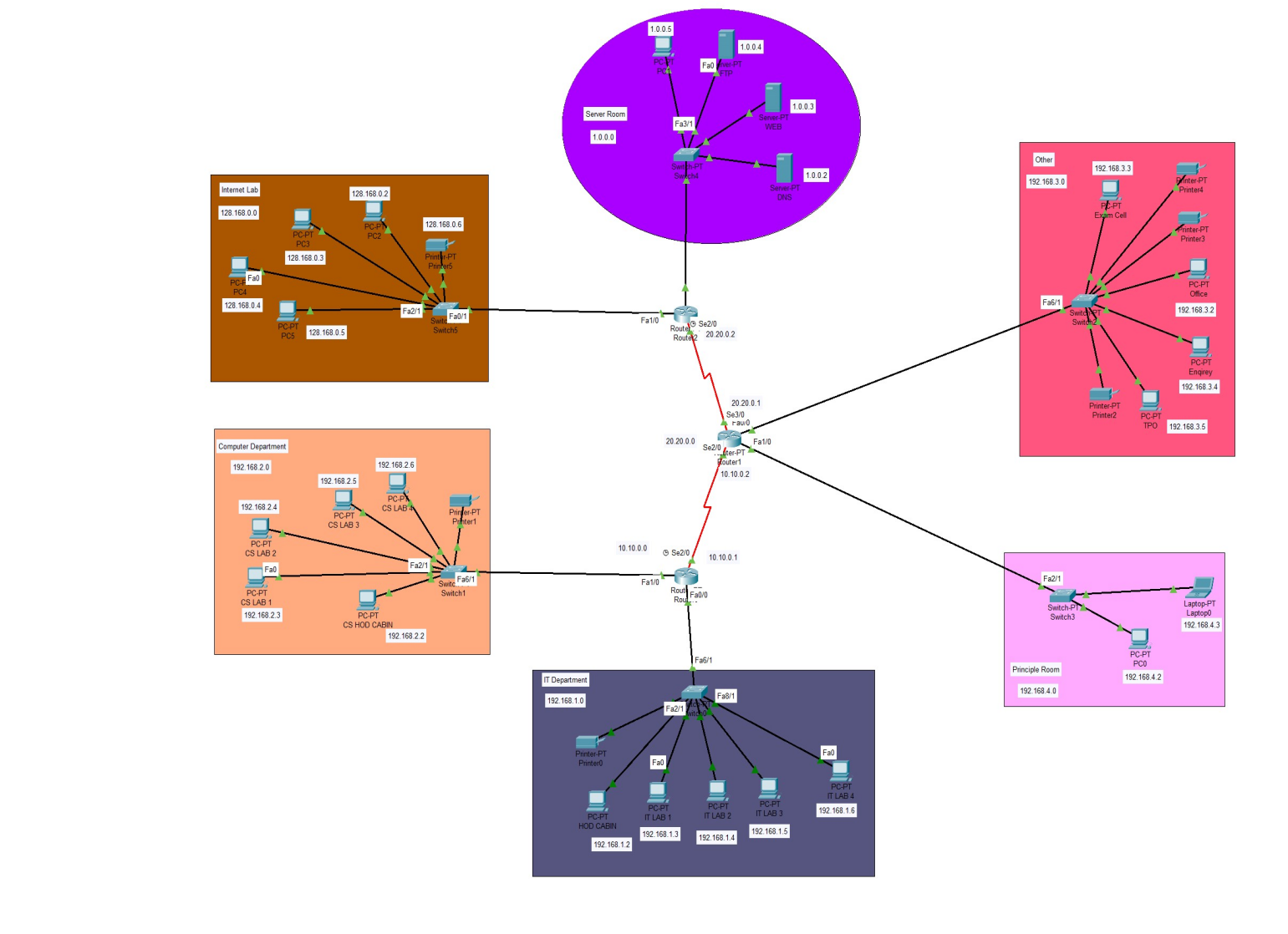
**5.INTERNET LAB :**

|  |  |
| --- | --- |
| **INTERNET LAB (128.168.0.0)** | |
| PC2 | 128.168.0.2 |
| PC3 | 128.168.0.3 |
| PC4 | 128.168.0.4 |
| PC5 | 128.168.0.5 |
| Printer 5 | 128.168.0.6 |

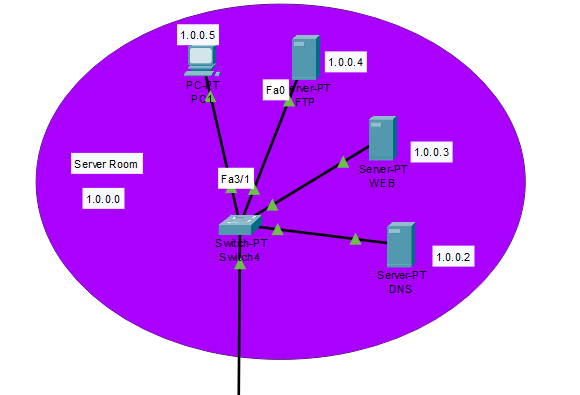
**6.PRINCIPLE ROOM**

|  |  |
| --- | --- |
| **PRINCIPLE ROOM (192.168.4.0)** | |
| PC 0 | 192.168.4.2 |
| LAPTOP 0 | 192.168.4.3 |

**Architecture diagram:**



1. **server room**



Contains dns,web,ftp servers with the subnet ip 1.0.0.0

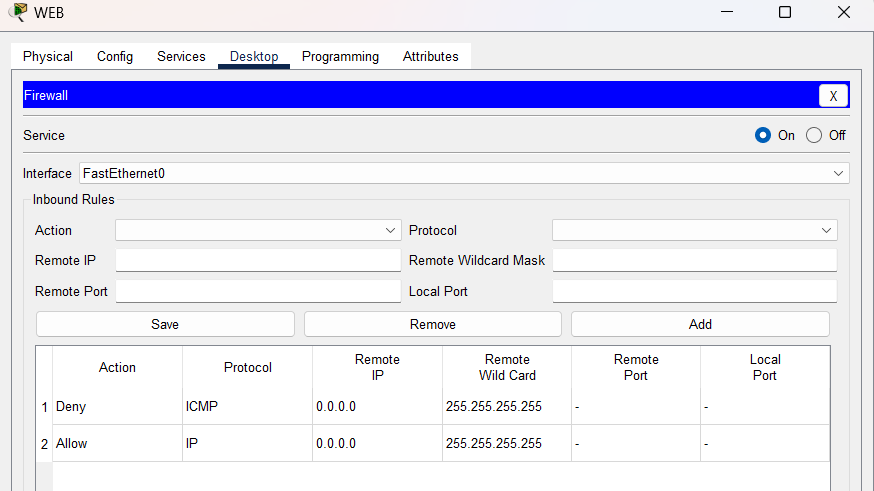
` firewall configured for the web server (only ip is allowed)

Users can access web browser,dns ,ftp by ips

Implementation

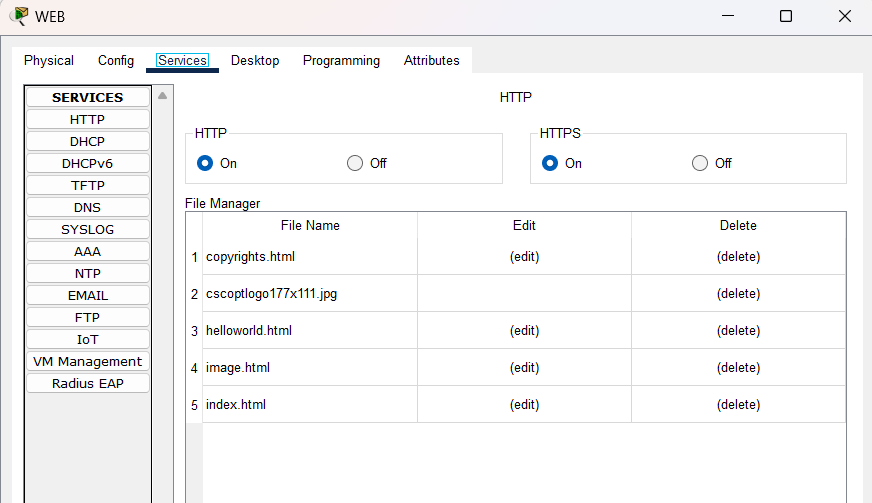
1. firewall blocking

ICMP protocol blocked for all ips



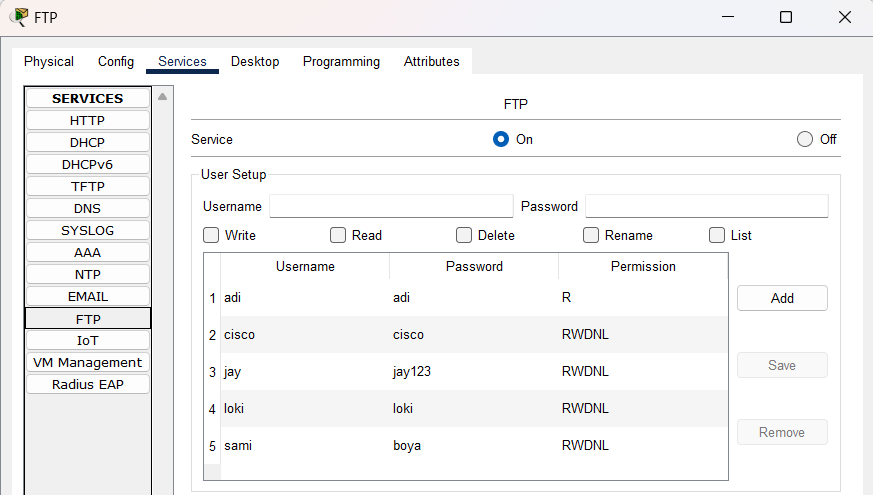
1. Web page

We have made a webpage users can acess



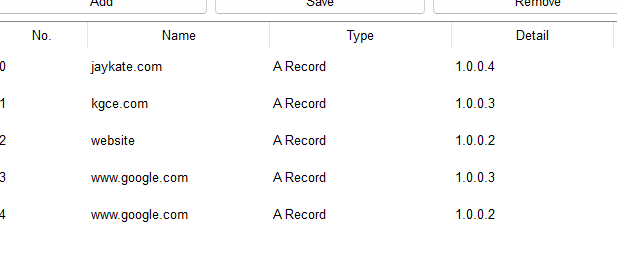
1. FTP

Created ftp users with password so that one can access ftp from their pcs

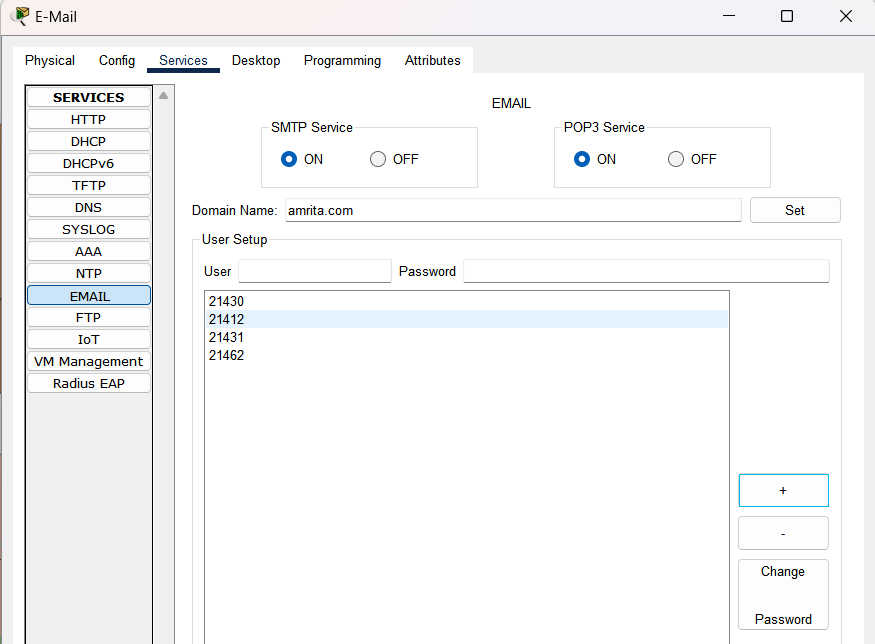


Ex:username-sami password-boya

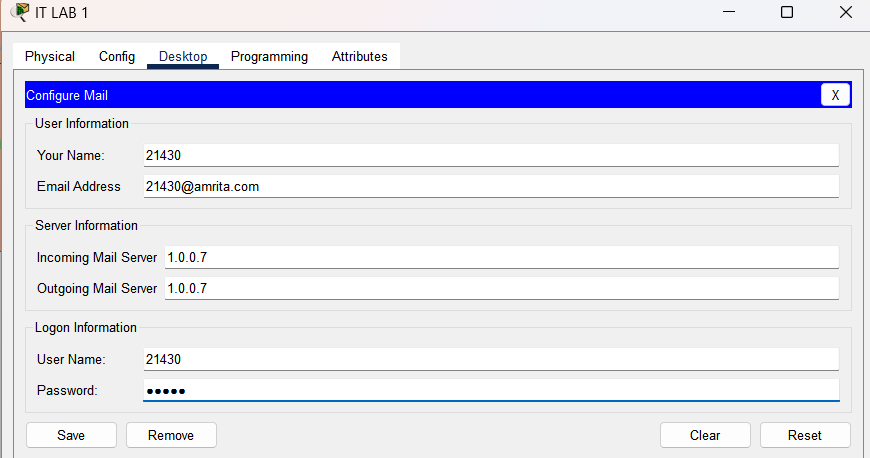
1. similarly for DNS



1. Email:



Configuring mail in any pc



Here we have taken domain name as amrita.com and created student ids as per their respective reg nos now from any dept students can use the mail server and send/receive mails

RIP (Routing Information Protocol):

What is it?

RIP is a way for routers in a network to talk to each other and figure out the best paths for sending data from one place to another.

How does it work?

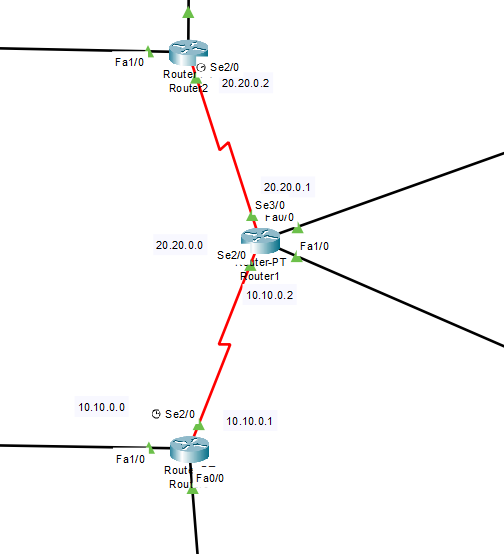
Routers share information about the networks they know. They decide the best way to reach a destination based on the number of routers (hops) involved.

Key Points:

RIP uses the "hop count" to measure distance. Fewer hops mean a better path.

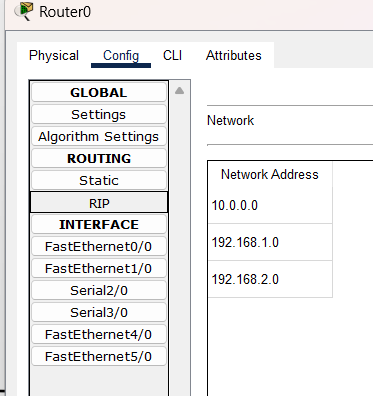
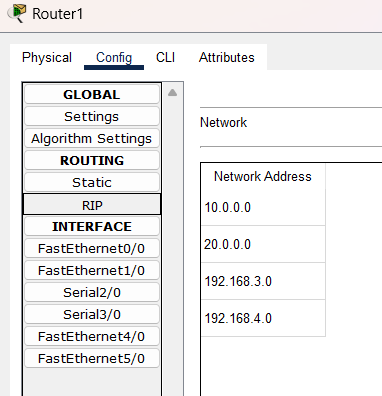
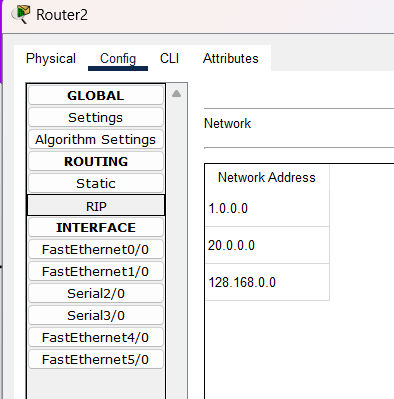
Routers tell each other about the networks they know by broadcasting updates.

To avoid confusion, routers don't share information back through the same path they received it (split horizon).



RIP CONFIGURING IN ROUTERS:

For r1,r2,r0



###code

Router#

Router#show ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 2 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

FastEthernet1/0 12 1

Serial2/0 12 1

FastEthernet0/0 12 1

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

192.168.1.0

192.168.2.0

Passive Interface(s):

Routing Information Sources:

Gateway Distance Last Update

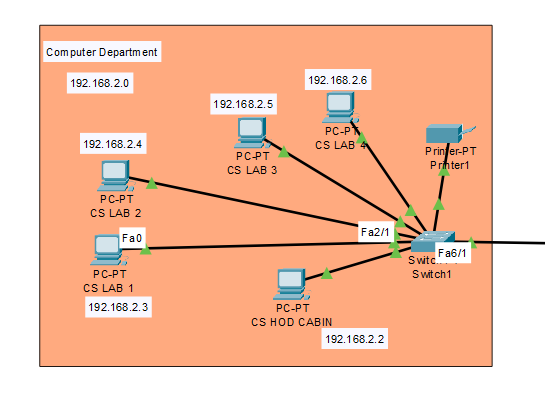
10.10.0.2 120 00:00:04

Distance: (default is 120)

Router#

%SYS-5-CONFIG\_I: Configured from console by console

Departments Info:

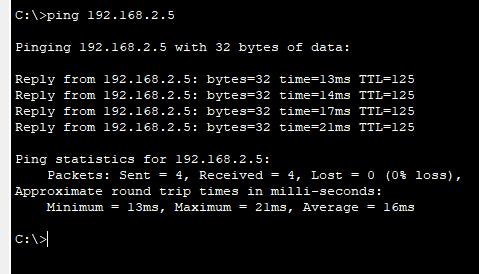


Like the computer department we have 4 more rooms/departments where we have one switch connected with the pcs,printers etc with the dedictaed ips for the respective subnets connected with the same vlan as we have to transfer files across the whole college so same vlan is reqd if possible we can changa vlan and use access list to restrict the packet sending to private networks in our side we have used firewall in the web server

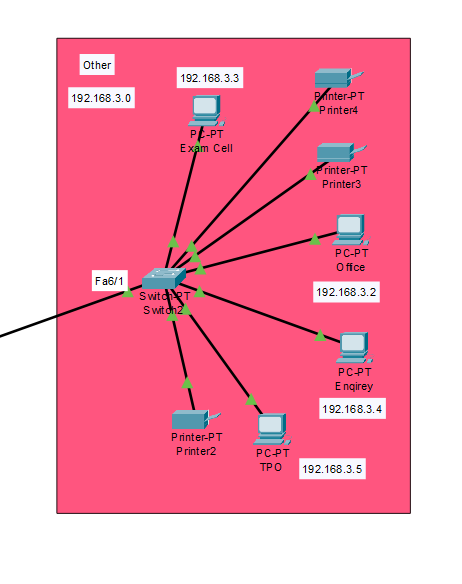
**Results for all configurations:**

Basic vlan config:

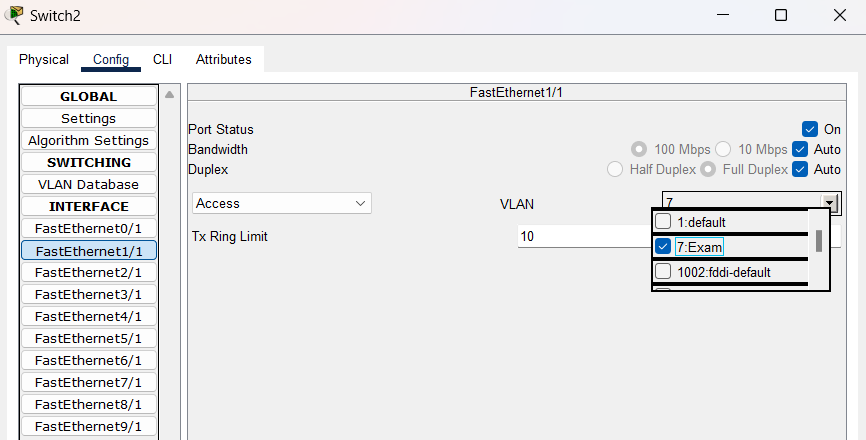
Same vlan so packets transferred successfully



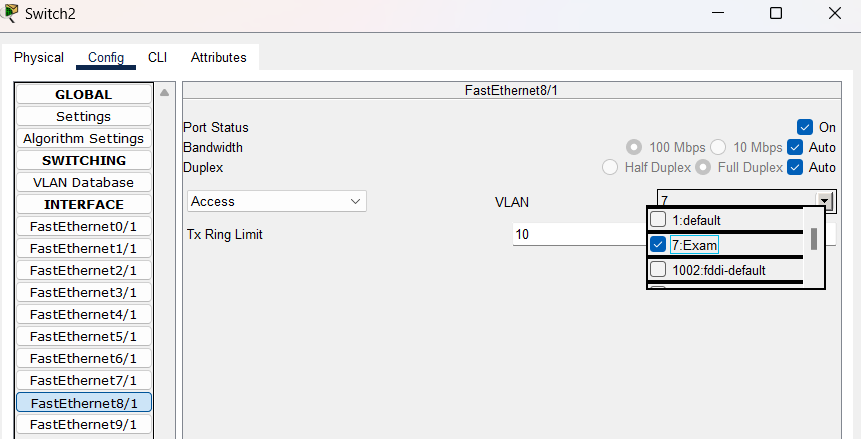
Here in Others in Exam Cell lets define new vlan 7 with name Exam and add the Exam-cell pc and printer 3 and others on default vlan so no others can access the exam cell and printer other than themselves this is the concept of vlan



For PC



For Printer:

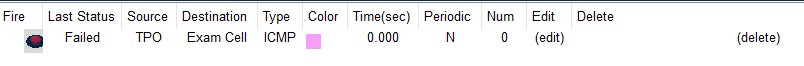


Results:

Pc to printer:

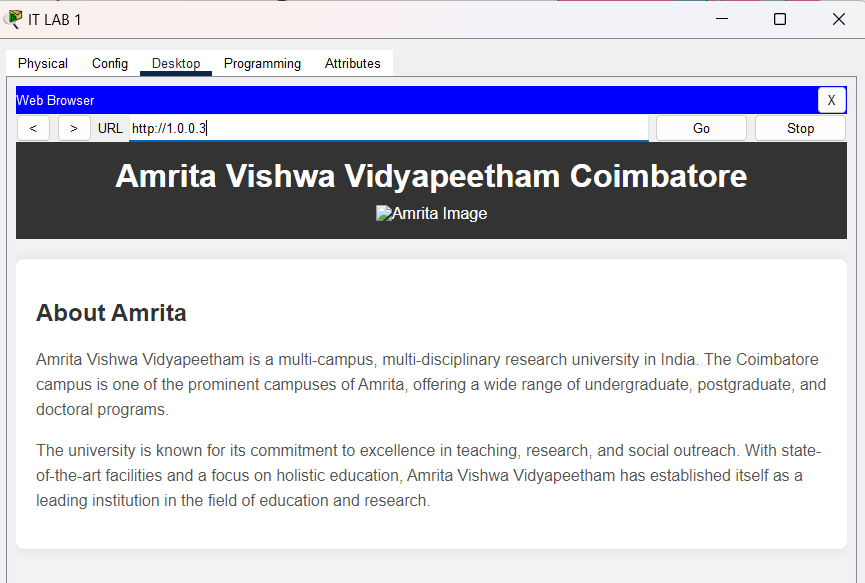


Other case:



**Accessing Web Browser:**

1. lets say from it dept I want to access the web browser



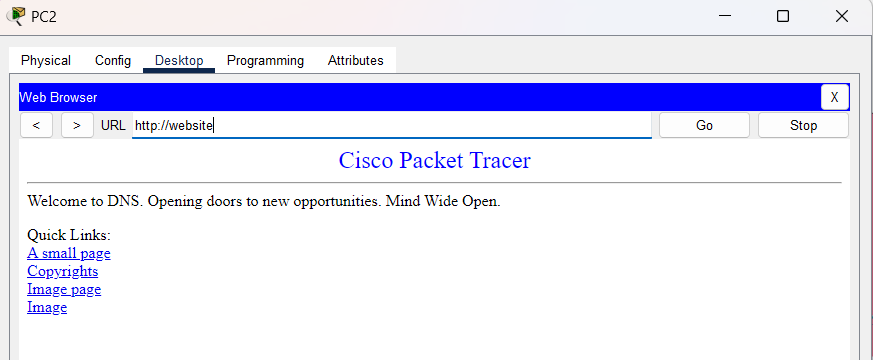
Firewall check:

Lets check whether firewall is working or not as firewall is included for the wen server as no icmp protocols are accessed



Its failed as firewall protects the server

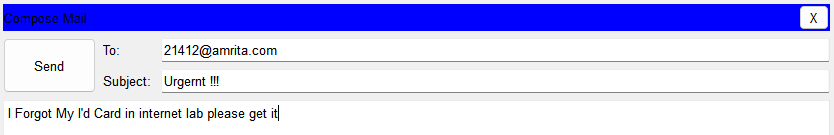
DNS:Results:

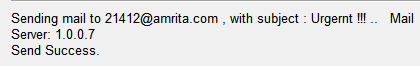


Email-results:

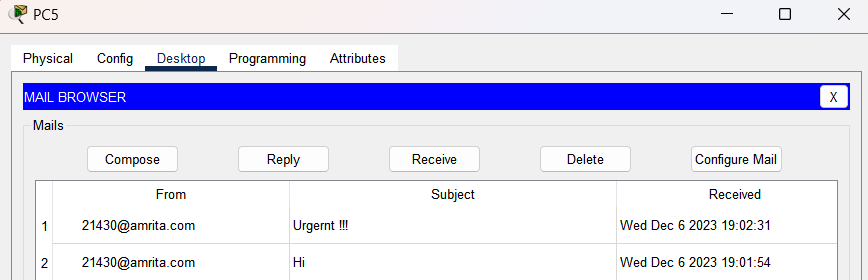
Lets say 21430 is in it lab wants to send the mail to 21412 in internet lab

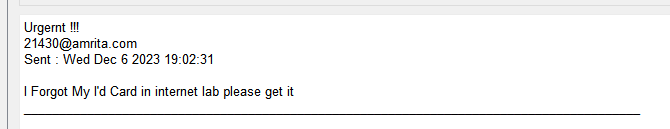
21430-mail side



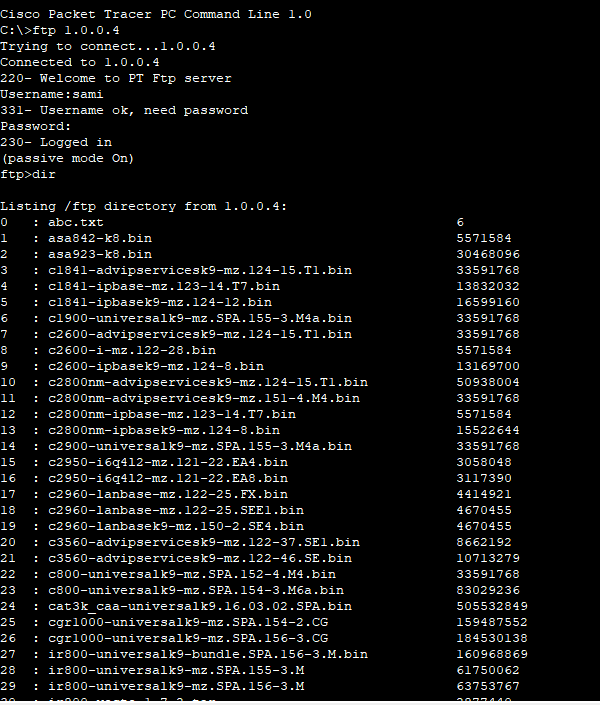


21412-mail side in internet lab





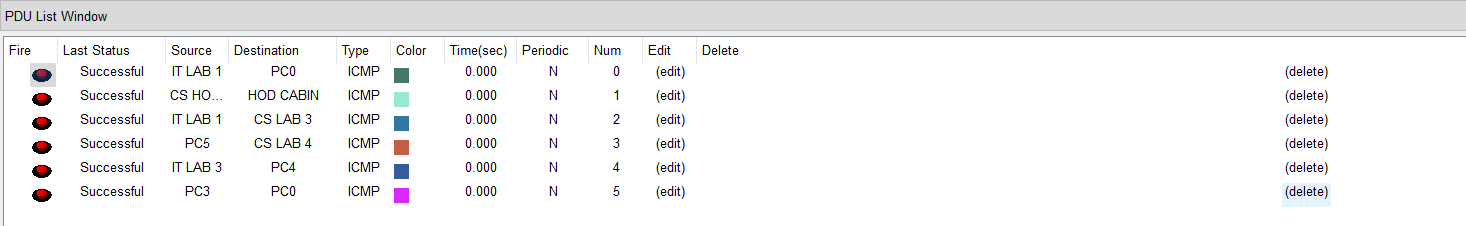
FTP:resullts



We can put files in the ftp and store there as per the users permissions given for the user name as per the ftp server

**Final Check:**

Lets check the transfer of packets from departments



So as seen all possible cases are successful

**Analytical questions:**

* Question 1: What factors influenced the choice of the RIP routing protocol for this network project?

Answer: The choice of RIP was influenced by the project's simplicity requirements and the size of the network. RIP's ease of configuration and low resource requirements made it suitable for the project's context.

* Question: How does the implementation of VLANs contribute to network security in this college network scenario?

Answer: VLANs enhance network security by logically segmenting the network, isolating departments or groups. This segmentation helps control access, contain potential security breaches, and improve network performance.

* Question: What security measures were implemented in the project to protect against unauthorized access and potential threats?

Answer: The project includes the implementation of VLANs, access control lists (ACLs), and the use of a firewall. These measures collectively enhance network security by controlling traffic, isolating segments, and preventing unauthorized access.

* Question: Describe how the RIP routing protocol adapts to changes in the network topology, and discuss any potential drawbacks.

Answer: RIP adapts to changes through periodic updates and route poisoning. Drawbacks include slower convergence times, potential routing loops during changes, and a limited maximum hop count of 15.

* Question: Explain the role of a firewall in the college network and how it enhances security.

Answer: A firewall controls incoming and outgoing traffic, acting as a barrier between the internal network and the internet, preventing unauthorized access and protecting against cyber threats.

* Question: Explain the significance of the ICMP protocols in the context of network troubleshooting and diagnostics.

Answer: ICMP protocols, such as Echo Request (ping) and Destination Unreachable, are crucial for network troubleshooting. They provide feedback on network reachability, errors, and performance, aiding administrators in diagnosing and resolving network issues.

Table

|  |  |  |  |
| --- | --- | --- | --- |
| Computer Dept | CMP-SW | Number of nodes:6  Range of IP address:  192.168.2.1  To  192.168.2.6  Subnet address:  192.168.2.0  Subnet mask:  "255.255.255.0"  Protocols configured  IP,DNS,RIP | Purpose-  The Computer Department's network serves as a vital connectivity and communication hub, fostering seamless interaction and data exchange across various computing resources. With a strategic allocation of IP addresses and implementation of essential protocols such as IP, DNS, and RIP, the network ensures efficient resource management and a secure environment. The design caters to the specific needs of computer labs, offering an interconnected platform for collaborative work, research, and shared access to resources like printers. This holistic approach contributes to an optimized and productive learning environment within the Computer Department, supporting the diverse computing needs of students and faculty alike. |
| IT Dept | IT-SW | Number of nodes:6  Range of IP address:  192.168.1.0  To  192.168.1.6  Subnet address:  192.168.1.0  Subnet mask:  "255.255.255.0"  Protocols configured  IP,DNS,RIP | Purpose:  The IT Department's network is designed to foster seamless communication and collaboration through strategically planned IP addressing and essential protocols like IP, DNS, and RIP. It prioritizes reliability, scalability, and security to support the diverse activities within the department, ensuring efficient information exchange and technology services. The network serves as a robust foundation for IT-related functions, promoting a conducive environment for research, innovation, and academic endeavors. |
| Internet Lab | IL-SW | Number of nodes:5  Range of IP address:  128.168.0.0  To  128.168.1.5  Subnet address:  192.168.0.0  Subnet mask:  "255.255.255.0"  Protocols configured  IP,DNS,RIP | Purpose  The Internet Lab serves as a hands-on space for students to explore and experiment with real-world internet applications and services. With a dedicated IP address range and essential protocols like IP, it enhances practical learning in web hosting, FTP servers, and other internet-related functionalities within the secure college network environment. |
| Principle Room | Principle-sw | Number of nodes:3  Range of IP address:  192.168.4.0  To  192.168.4.4  Subnet address:  192.168.0.0  Subnet mask:  "255.255.255.0"  Protocols configured  IP,DNS,RIP | Purpose-  The Principal's Room in the college network scenario serves as the administrative hub for the college principal. It functions as a space for decision-making, communication, meetings, and record-keeping. It is used for administrative tasks, discussions with faculty, decision-making processes, and private workspace for the principal. Additionally, the room may be utilized for counseling sessions, visitor reception, and strategic planning for the college's development. |
| Other | Exam | Number of nodes:7  Range of IP address:  192.168.3.0  To  192.168.3.6  Subnet address:  192.168.3.0  Subnet mask:  "255.255.255.0"  Protocols configured  IP,DNS,RIP | Purpose-  Exam Cell:  Manages and coordinates the examination process.  Handles exam scheduling, question paper preparation, and result declaration.  Ensures the integrity and security of the examination process.  Enquiry Department:  Addresses inquiries from prospective students, parents, and the community.  Provides information about courses, admissions, and general college details. |
| Server | FTP | Cat:FTP  Adress:  1.0.0.4 | For reliable file transfer |
| Server | Web,dns | Cat:web  Firewall,access list  Adress:  1.0.0.3 for web  1.0.0.5 for dns | For accessing IP protocols over the network |