**Project Report**

By Sowrabh Kumar B

CB.EN.4CSE21058

**Problem Statement:** Packet Flow Visualizer.

* **Objective**

The main objective of this project is to create a visual representation of the packet flow from students' laptops/desktops (hosts) to external networks outside of the college campus.

The project can be divided into two key parts, as outlined below:

* + Network Topology Creation: To begin, students will need to determine the devices present within the college network. They can achieve this by using tools like traceroute or by consulting with the college network administrator. Based on the gathered information, students will then create a network topology using Cisco Packet Tracer. The topology will illustrate the various network devices, network design, and network boundaries, as explained in the Network Essential course, showcasing the path from the host to the external network.
  + Packet Flow Investigation: After establishing the network topology using Cisco Packet Tracer and configuring IPv4 addresses on all layer-3 devices, students will proceed to collect packets at each device using a packet sniffer. They can choose to use either the inbuilt sniffer in Cisco Packet Tracer or a tool like Wireshark. By analyzing the packets captured from different devices (nodes), students can extract relevant information from the packet headers, particularly noting changes occurring in the Ethernet and IP headers. This data will enable them to create a flow diagram illustrating the path of the packet flow from their device (host) to the external network. Any flow chart creator application can be used to create this diagram.

**ABSTRACT**

Computer networks significantly impact an organization's functioning, with universities relying on proper functioning for various purposes such as education, administration, communication, e-library, and automation. An efficient network facilitates systematic and cost-efficient information transfer in messages, files, and resources. The project offers insights into topology design, IP address configuration, and packet-based information transmission in wireless networks across various university areas.

The aim of this project is to create a visual representation of the packet flow from students' laptops/desktops (hosts) to external networks outside of the college campus. This university network consists of the following devices:

1) Router (2911)

2) Multilayer Switches (3560 24PS)

3) Switches (2960 IOS15)

4) Email Server

5) WEB server

6) DNS Server

7) FTP Server

8) Printers

9) Wireless Routers

10) PCs

11) Laptops

12) Smart Phone

**The design includes the following parts of the University:**

* Academic Blocks: AB1, AB2 and AB3
* Cloud for Email Server
* External Network (Outside the Campus)

TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| 1. | Project Report | 1 |
| 2. | Abstract | 2 |
| 3. | Table of Contents | 3 |
| 4. | Literature Review | 4 |
| 6. | Work Done | 7 |
| 7. | Flow diagram and packet Investigation | 29 |
| 8. | Conclusion | 42 |

**LITERATURE REVIEW**

* What is Packet Tracer?

Packet Tracer is a Cisco Systems-designed visual simulation tool that enables users to create network topologies and imitate modern computer networks. It uses a drag-and-drop interface to simulate Cisco routers and switches, allowing users to add and remove devices. Designed for Certified Cisco Network Associate Academy students, the tool is available for free download and use for educational purposes.

* Router

A router is a Network Layer device that routes data packets based on IP addresses. It connects LANs and WANs and has a dynamically updating routing table for decision-making. Routers divide broadcast domains of hosts connected through them.

* Switch

A network switch is a networking hardware that connects devices using packet switching to receive and forward data. It is a multiport network bridge that forwards data at layer 2 of the OSI model using MAC addresses. Some switches can also forward data at layer 3 by incorporating routing functionality, known as layer-3 switches or multilayer switches.

* Network Packet

A network packet is a formatted data unit carrying control information and user data, known as the payload, in a packet-switched network.

* Server

A server is a computer that shares resources, data, services, or programs with clients over a network. There are various types of servers, including web servers, mail servers, and virtual servers.

Many networks contain one or more of the common servers. The servers used in our project are as follows:

* DNS Server

Domain Name System servers (DNS) are application servers that provide a human-friendly naming method for user computers, making IP addresses readable. The DNS system is a widely distributed database of names and other servers that can be used to request unknown computer names. When a user needs a system's address, they send a DNS request to a DNS server, which returns the necessary IP address from its table of names.

* WEB Server

A web server is a widely used application server that hosts programs and data requested by users on the Internet or intranet. It responds to requests from browsers for web pages and other web-based services.

* EMAIL Server

An email server handles and delivers email using standard protocols like SMTP and POP3. These protocols handle outgoing and incoming mail requests, while webmail interfaces or email clients handle connections. These protocols are essential for efficient communication and communication across networks.

* Wireless Network

Wireless networks enable mobility between workstations and PCs, maintaining a secure connection while allowing for room-to-room access. However, they also require additional security measures.

* Ethernet

The backbone of a network is the cabling, which connects computer systems to form a local area network. It uses protocols to control information transmission and prevent simultaneous transmission by multiple systems. Gigabit Ethernet, capable of 1000 Mbps, and fast Ethernet, 100 Mbps, are two types of Ethernet networks. These networks control the transmission of information and prevent simultaneous transmission by multiple systems.

* Computing Device

Computing devices are the electronic devices that take user inputs, process the inputs, and then provide us with the end results. These devices may be Smartphones, PC Desktops, Laptops, printer, and many more.

* Internet Protocol

Internet Protocol (IP) is one of the fundamental protocols that allow the internet to work. IP addresses are a unique set of numbers on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

* Simulation Environment

The simulations of our network topology can be easily achieved using cisco packet tracer. Using a simulation mode, you can see packets flowing from one node to another and can also click on a packet to see detailed information about the OSI layers of the networking. Packet Tracer offers a huge platform to combine realistic simulation and visualize them simultaneously. Cisco Packet Tracer makes learning and teaching significantly easier by supporting multi-user collaboration and by providing a realistic simulation environment for experimenting with projects.

**WORK DONE**

In order to make the project understandable, I have divided the content into steps. They are as follows:

**Network Requirements**

1. **Campus Area**

The Campus area is further divided into various Departments Like Admin, HR, ELC, MECH, CS…etc... Academic Blocks (AB1, AB2 and AB3).

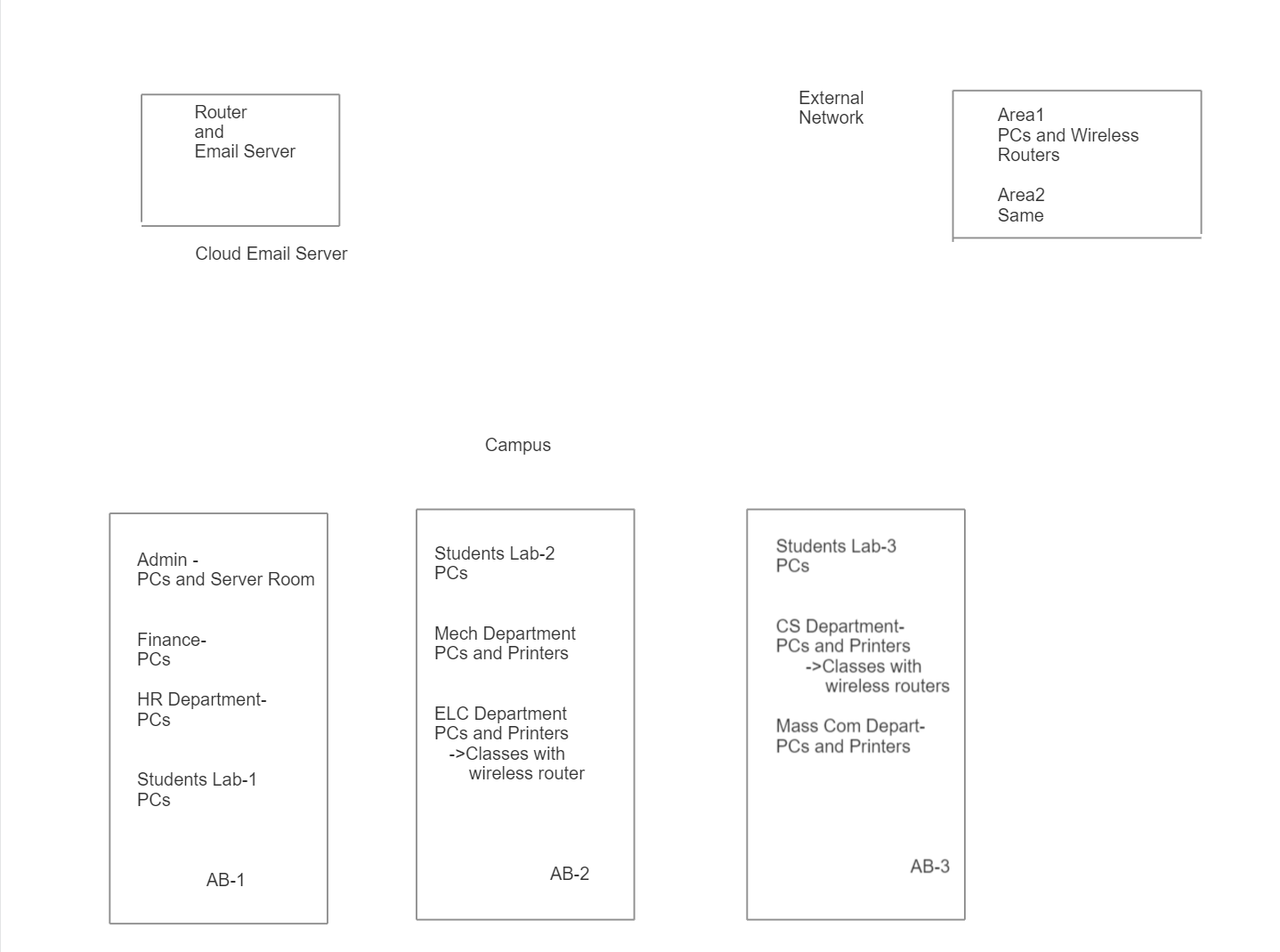
1. **External Network**

Outside the Campus (Area and Home)

1. **Cloud Network for Email Service**

Google Email server

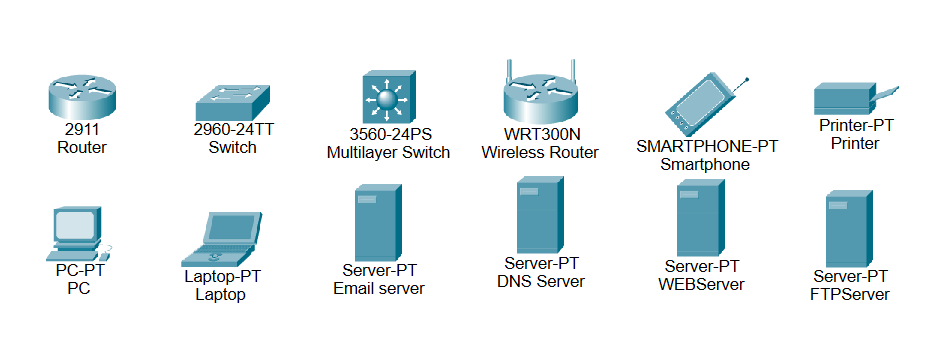
1. **Layout**



Basic layout of university

**Devices Used in The Network**

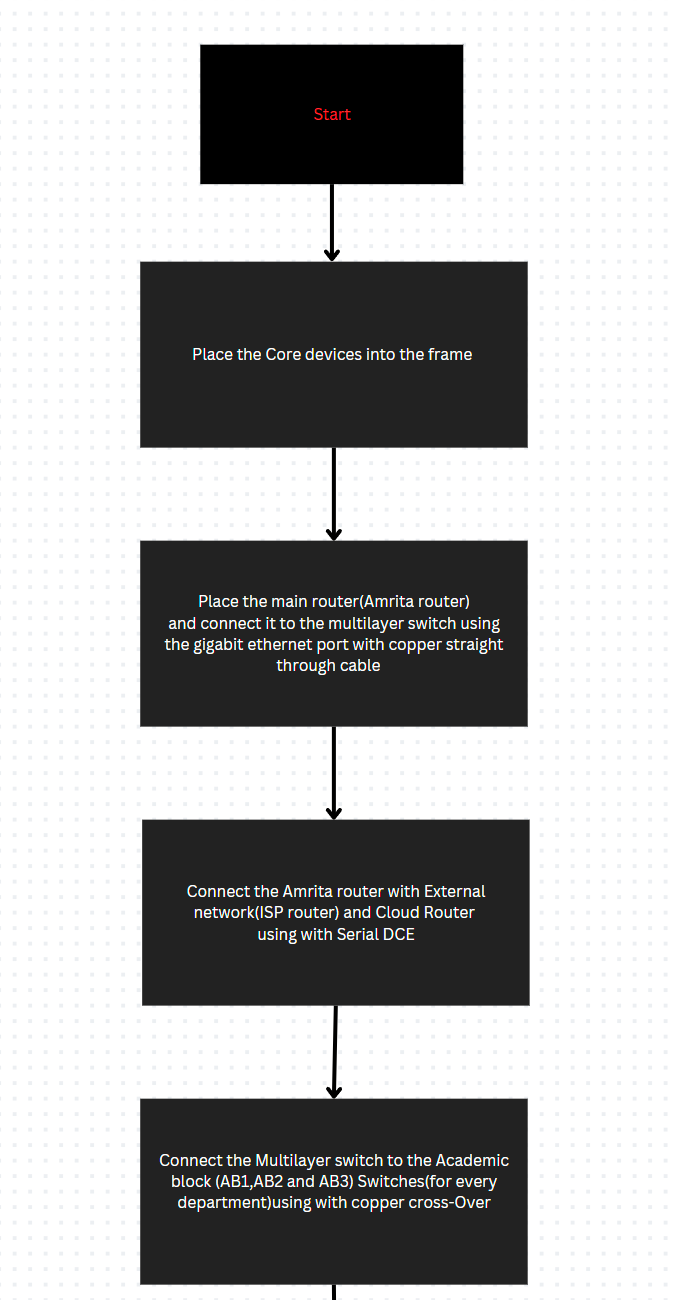
|  |  |
| --- | --- |
| Devices | Quantity |
| 1) Router (2911) | 3 |
| 2) Multilayer Switches (3650-24PS) | 2 |
| 3) Switches (2960-IOS15) | 12 |
| 4) DNS server | 1 |
| 5) WEB server | 2 |
| 6) Email Server | 2 |
| 7) FTP Server | 1 |
| 8) Wireless Routers | 3 |
| 9) PCs | 23 |
| 10)Printers | 8 |
| 11)Laptops | 3 |
| 12)Smart Phone | 3 |

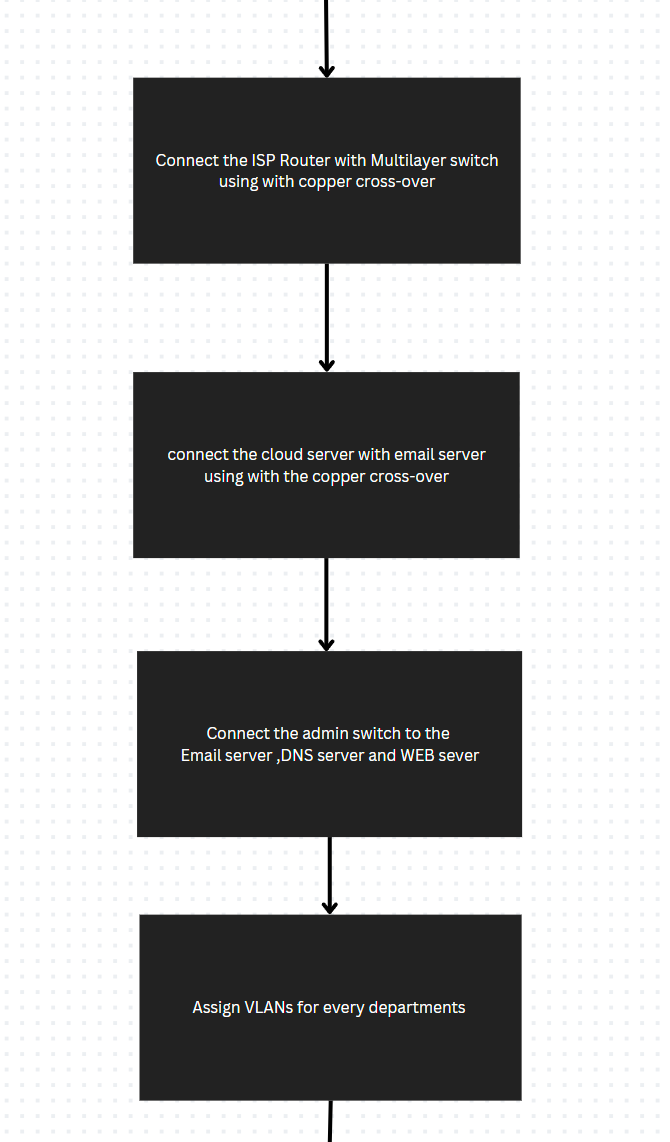


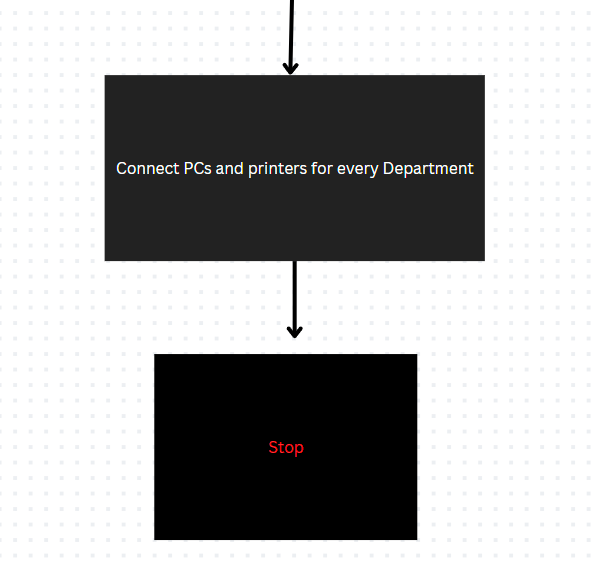
Devices used in the network

**Implementation and Flow Diagram**

* To design the network for university and outside campus. I initially started by placing the core devices (Routers) into the frame as mentioned in the layout.
* Firstly, I placed the **Amrita router** at the center of the university outline, which was further connected to the **Multilayer switch** using the gigabit ethernet port with copper straight-through cable and Switches (For all the Departments**)** using the serial port with serial DCE cable at the External Network and Cloud server router respectively.
* Here, Multilayer Switch is our Distribution Layer
* And further connected switch are Access Layer
* Total of 10 Unique VLANs for the campus Network and 2 Unique for External Network
* Each Department (Switches) have their separate VLANs.
* The Admin switch was further connected to the **EMAIL, DNS, and WEB** servers (as Server Room) respectively.
* Amrita router was connected to the Multilayer switch which was further connected with switches of the academic block (**AB1, AB2 and AB3**).
* Amrita Router connected with ISP router (Internet service provider) and Cloud Router using with Serial DCE
* Similarly, the ISP router was connected to the Area1 switch which was further connected with the wireless Router to Home.
* Also, for Cloud Server its connected with Email Server(google.com).
* All these connections are made through ethernet ports (gigabit ethernet and fast ethernet) using copper straight-through cables.





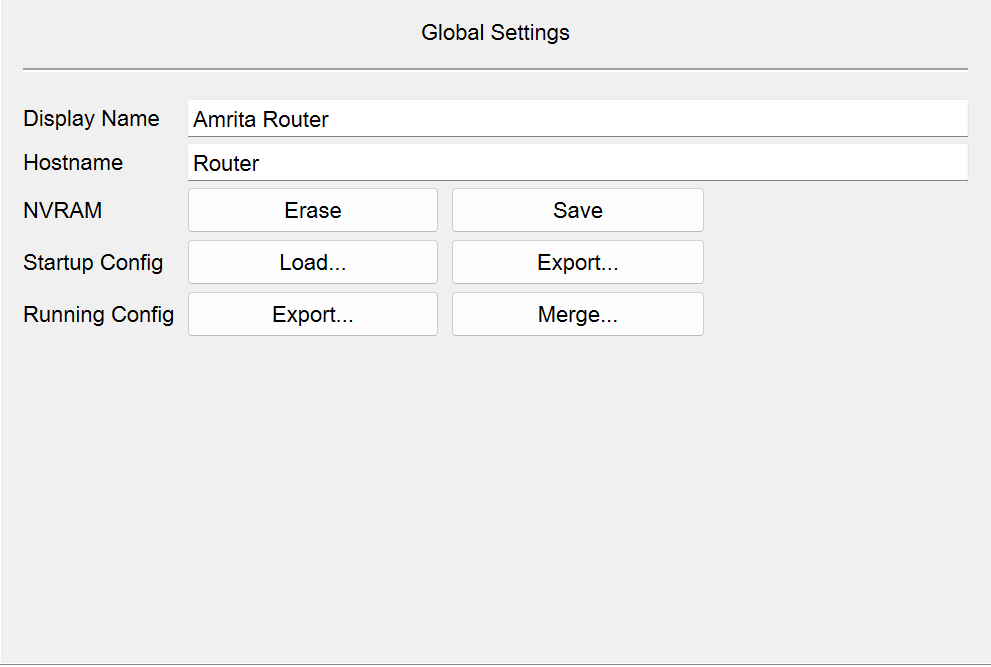


This is the flow diagram for a better understanding of the steps mentioned above.

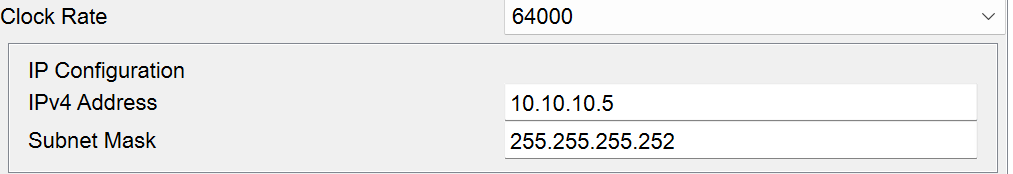
**Configuring IP Addresses**

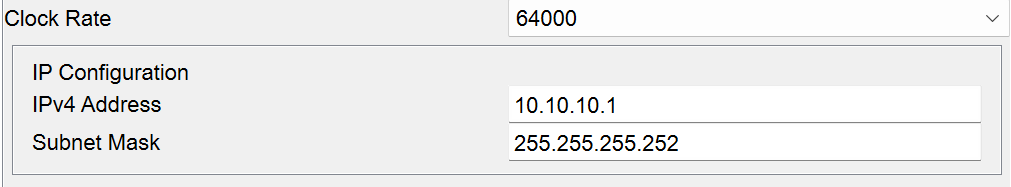
I have attached the screenshots of all the IP configuration below:

* Amrita Router configuration

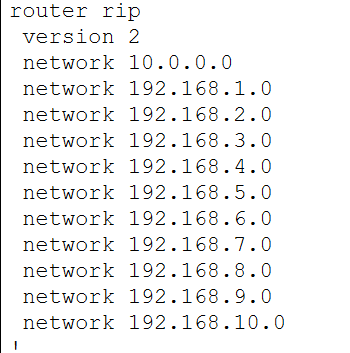


Serial0/0/0

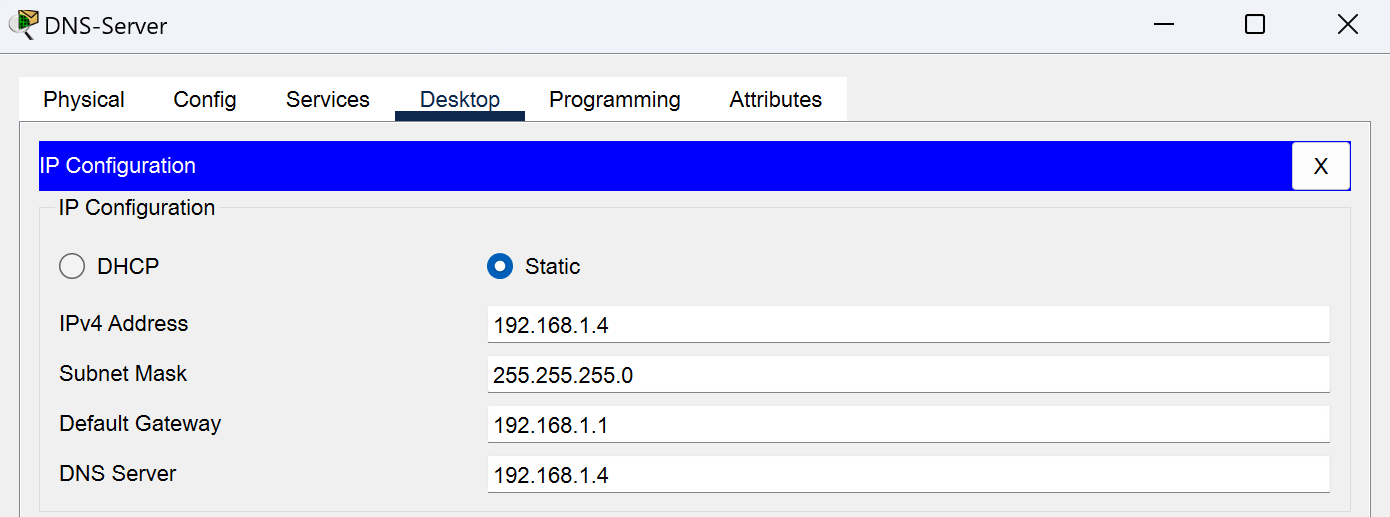


Serial0/0/1

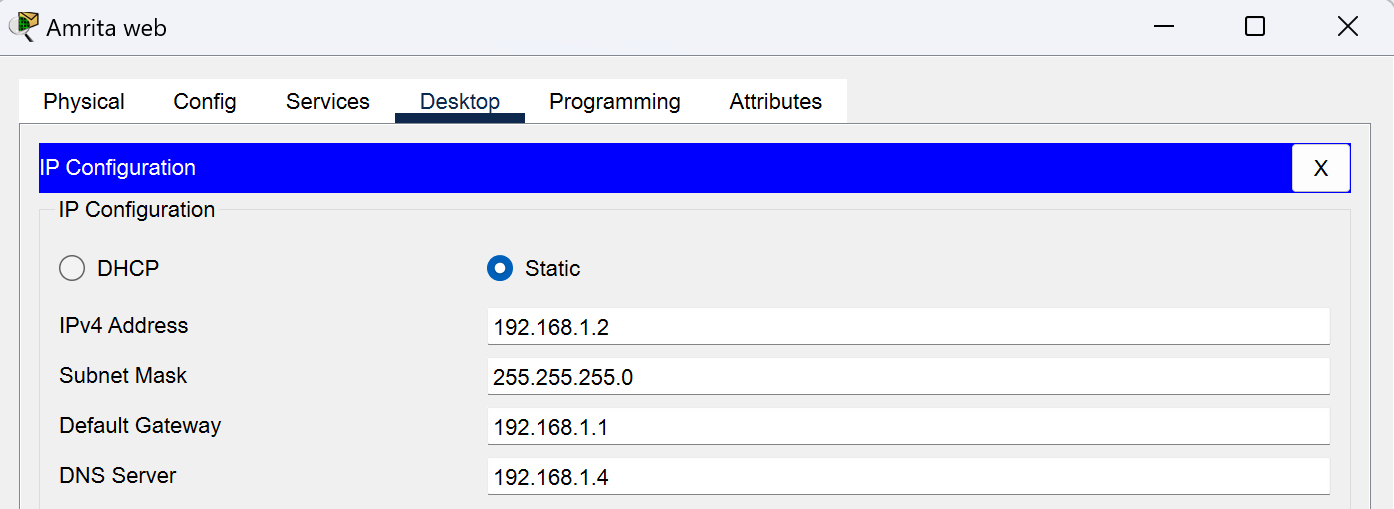
RIP V2



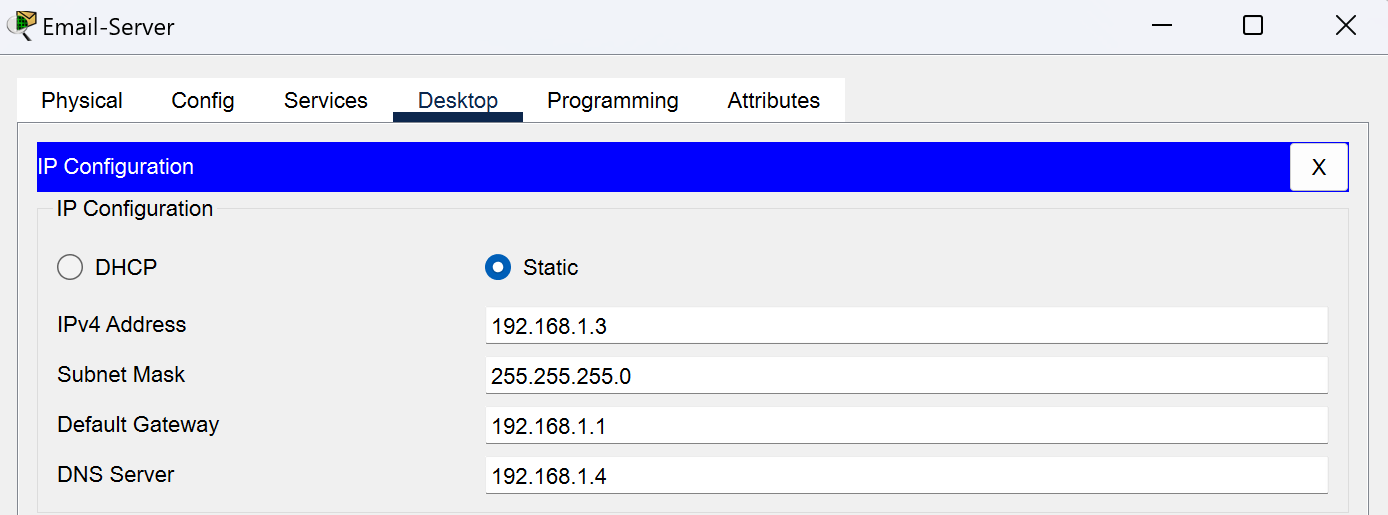
* Amrita DNS SERVER



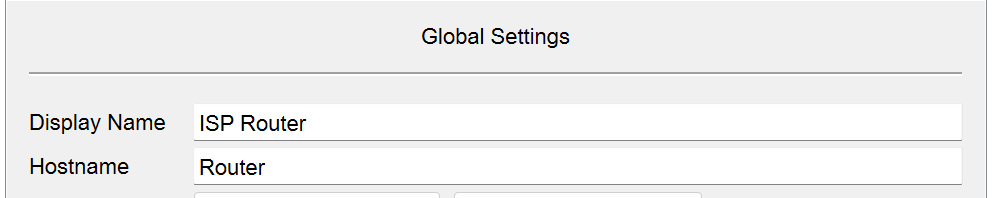
* Amrita WEB SERVER



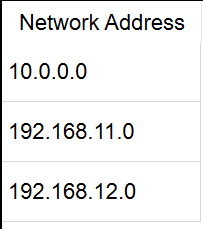
* Amrita EMAIL SERVER



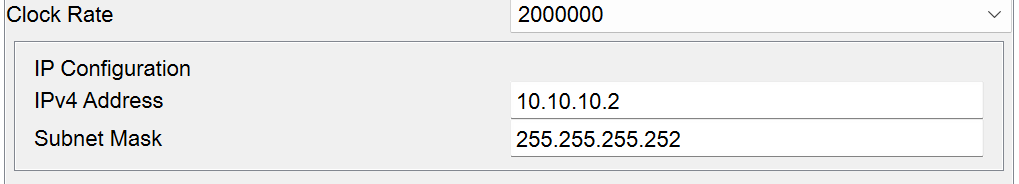
* ROUTER



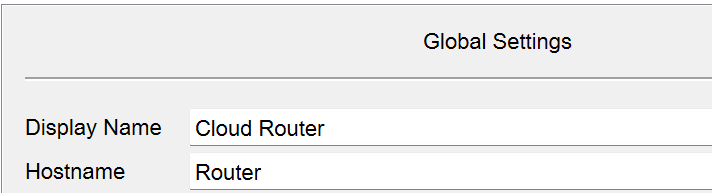
RIP V2



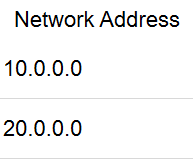
Serial0/1/0



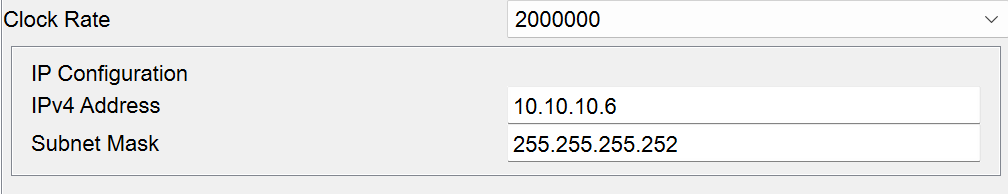
* Cloud Router



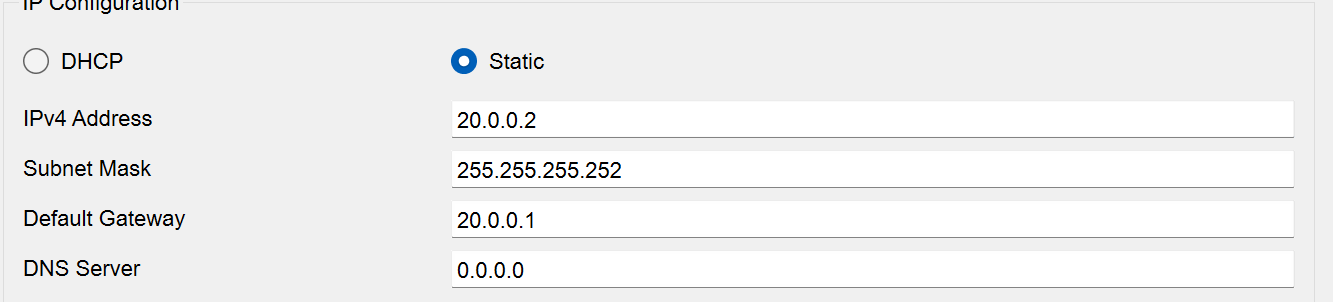
RIP V2



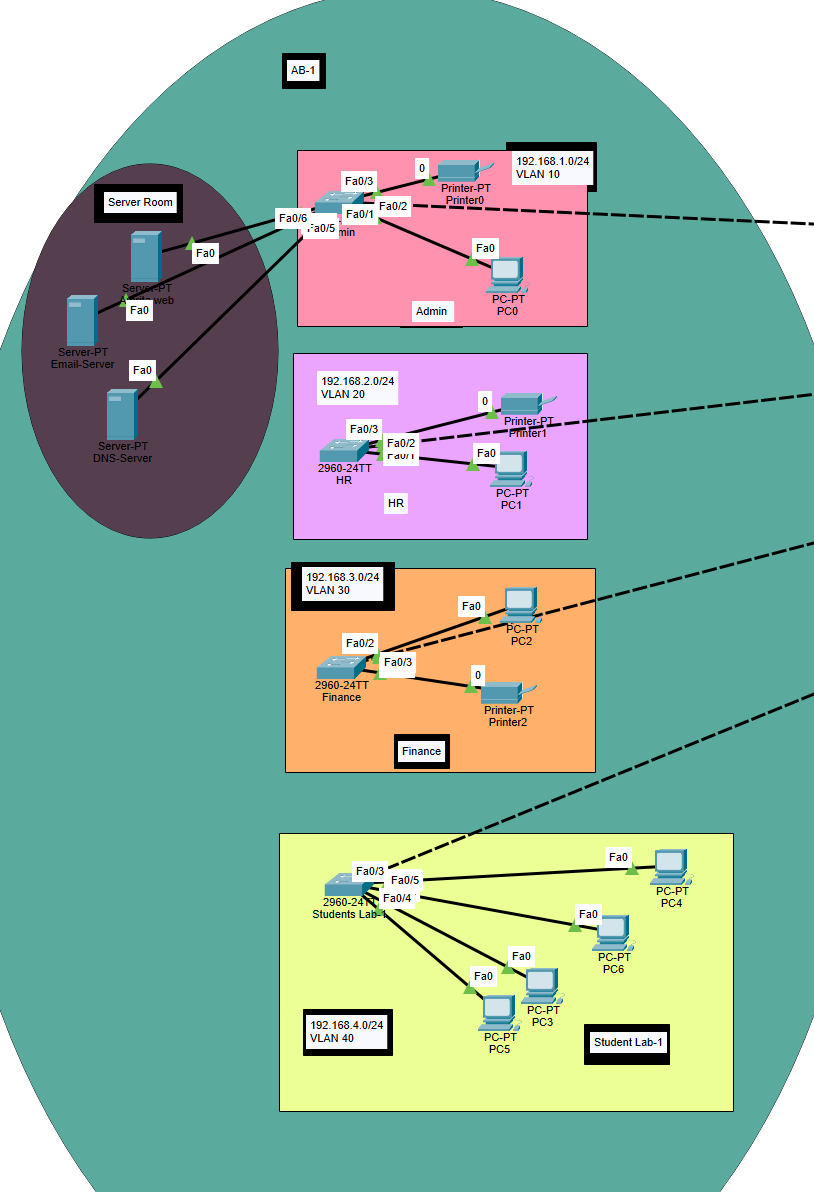
Serial0/0/0



Cloud Email Server



* ACADEMIC BLOCK 1



Admin – 192.168.1.0/24

VLAN-10

HR – 192.168.2.0/24

VLAN-20

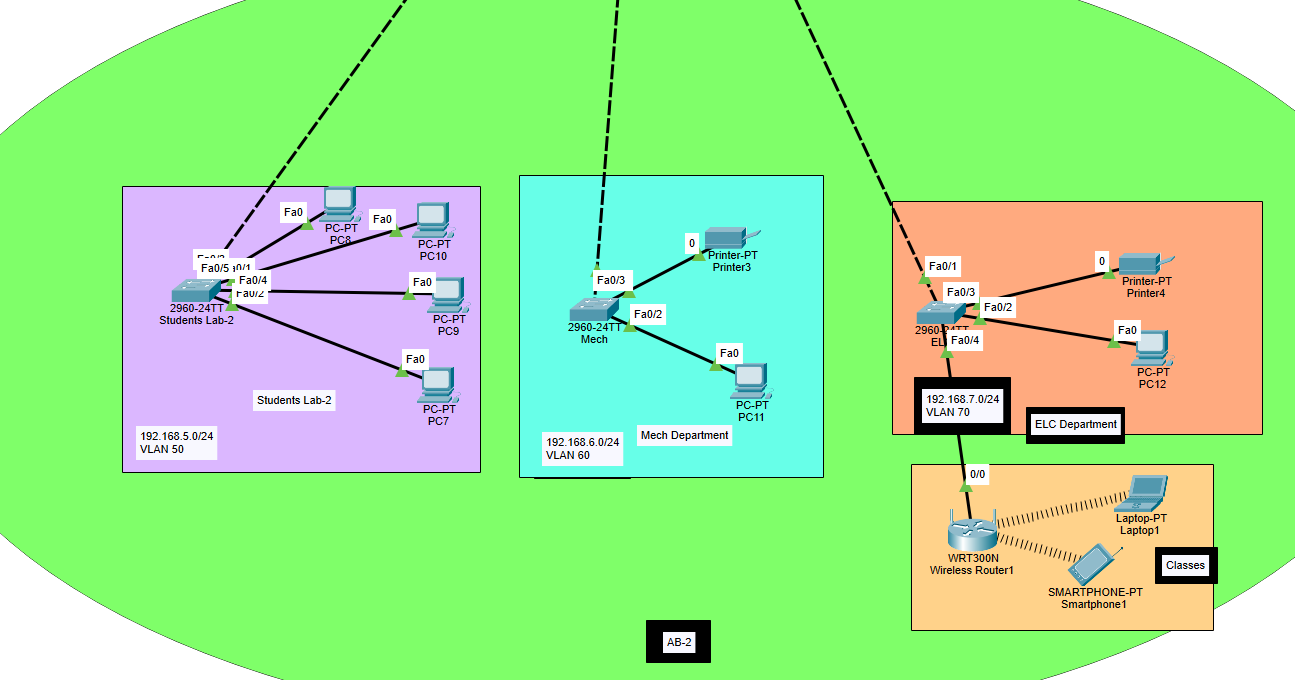
Finance – 192.168.3.0/24

VLAN-30

Students Lab-1 - 192.168.4.0/24

VLAN-40

* Each Department is connected with a computer and a printer and Students Lab is connected with 4 computers
* Admin Switch is connected to servers is called server room
* Server Room which consists of Web , DNS and Email server
* ACADEMIC BLOCK 2



Students Lab-2 – 192.168.5.0/24

VLAN-50

Mech Department – 192.168.6.0/24

VLAN-60

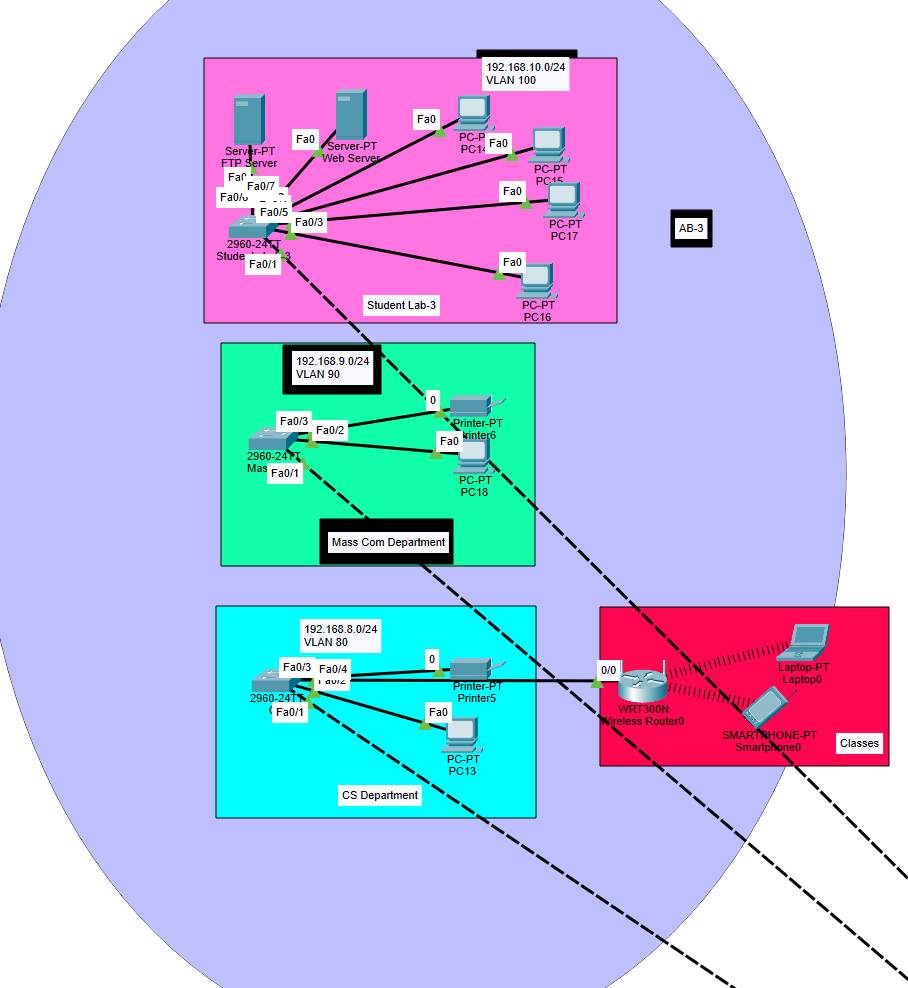
ELC Department – 192.168.7.0/24

VLAN-70

Just for Demonstration purpose I have connected a wireless router for a class which is under ELC Department and further laptop and smart devices are connected

Each Department can have multiple classes so they can connect to their respective switch and it will be easy to differentiate where this IP address belongs to.

* ACADEMIC BLOCK 3



CS Department – 192.168.8.0/24

VLAN-80

Mass Com Department – 192.168.9.0/24

VLAN-90

Students Lab-3 – 192.168.10.0/24

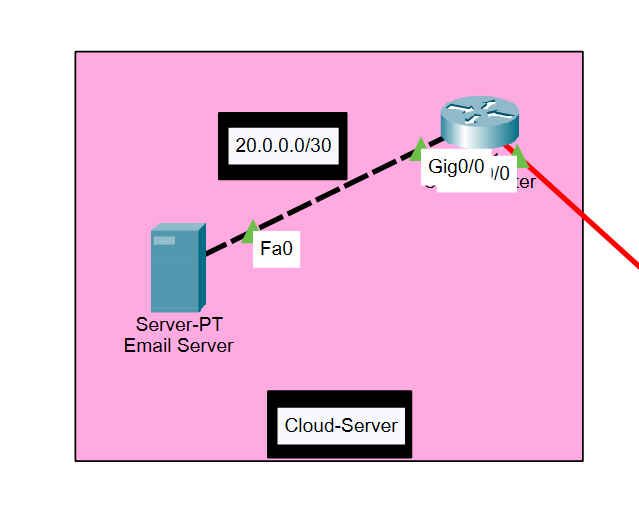
VLAN-100

In the Students lab-3 I have added two Servers (FTP and Web Server)

The question paper can be uploaded through FTP Server

And for demonstration purpose I have added wireless router for CS Department

* Cloud Server



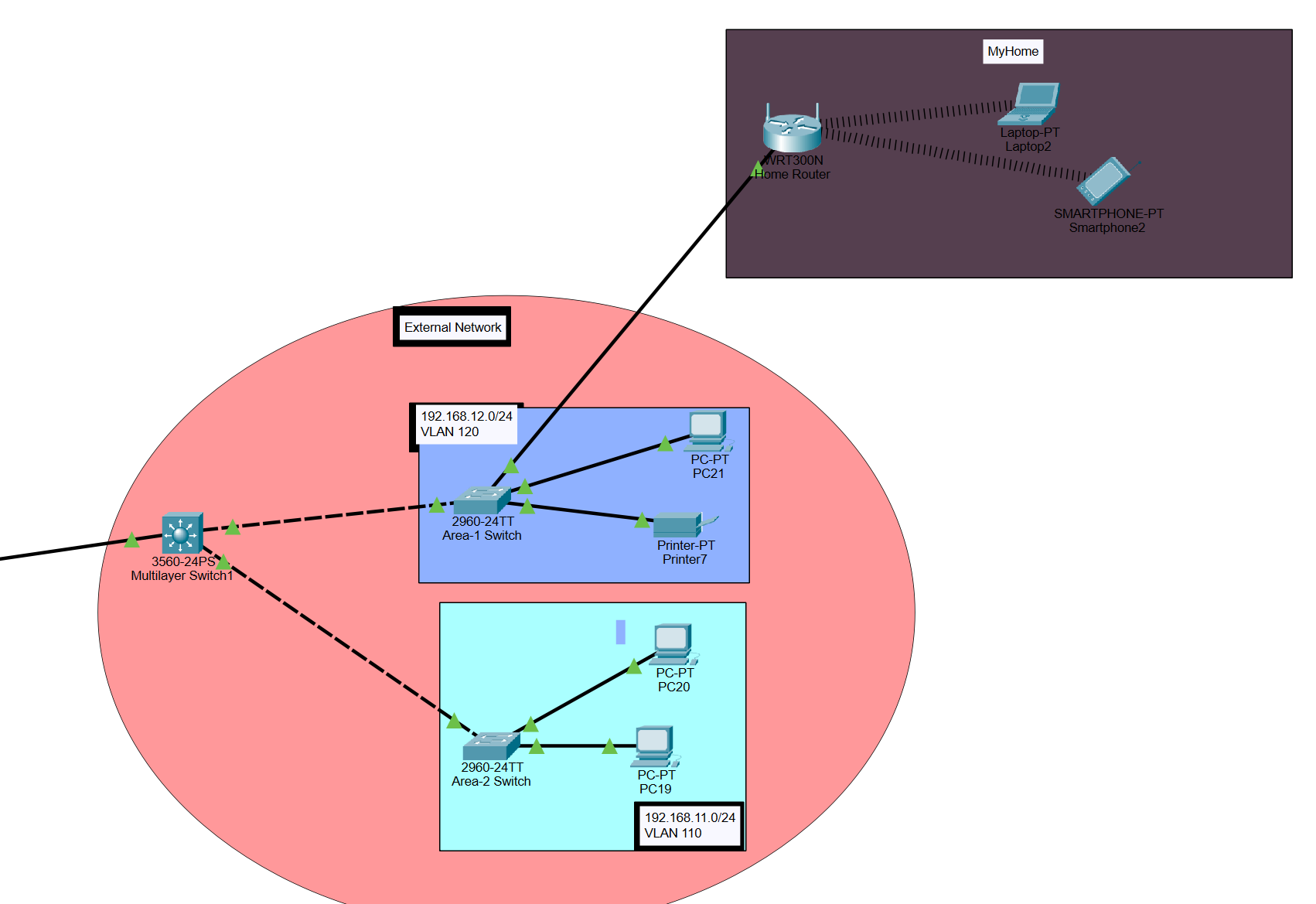
* Cloud Server Consists of email server which can be communicated outside the college

Email server – 20.0.0.2

Subnet Mask - 255.255.255.252

Default Gateway - 20.0.0.1

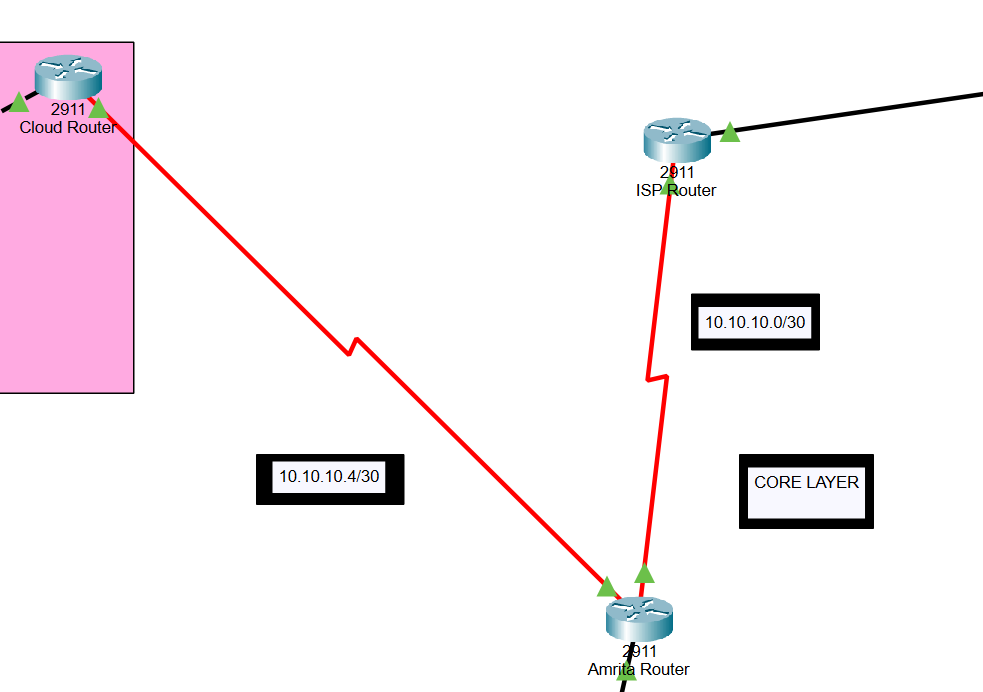
* ISP Router (Outside the College)



* Two Areas are connected to the Multilayer switch
* The Area1 which is further connected to a wireless router

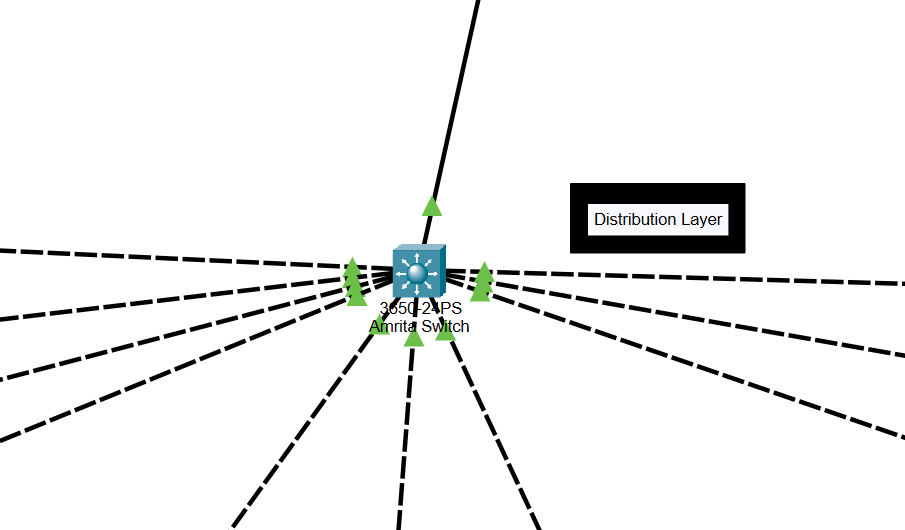
Differentiation between layers

**Core Layer**



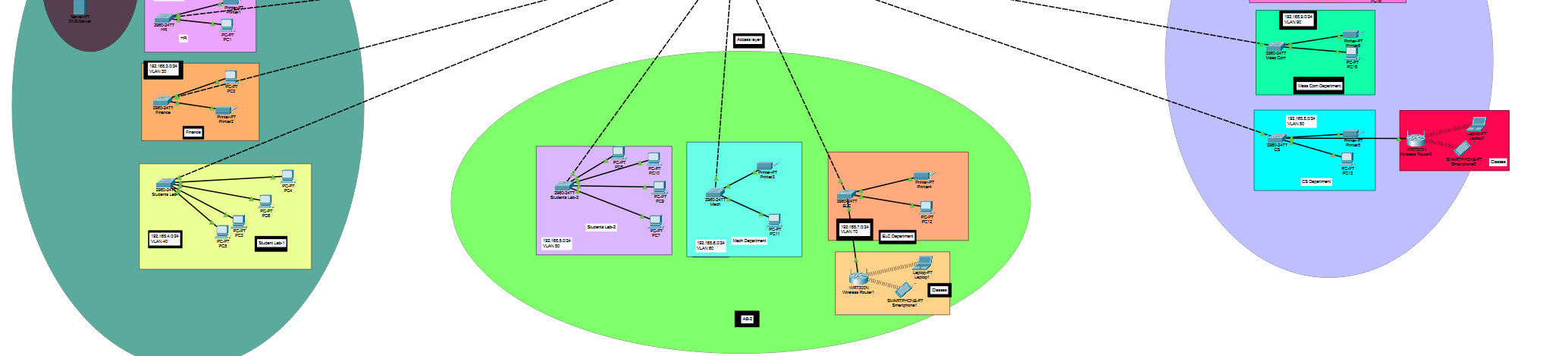
The core layer is a high-speed backbone that should be designed to switch packets as quickly as possible to optimize communication transport within the network.

**Distribution Layer**



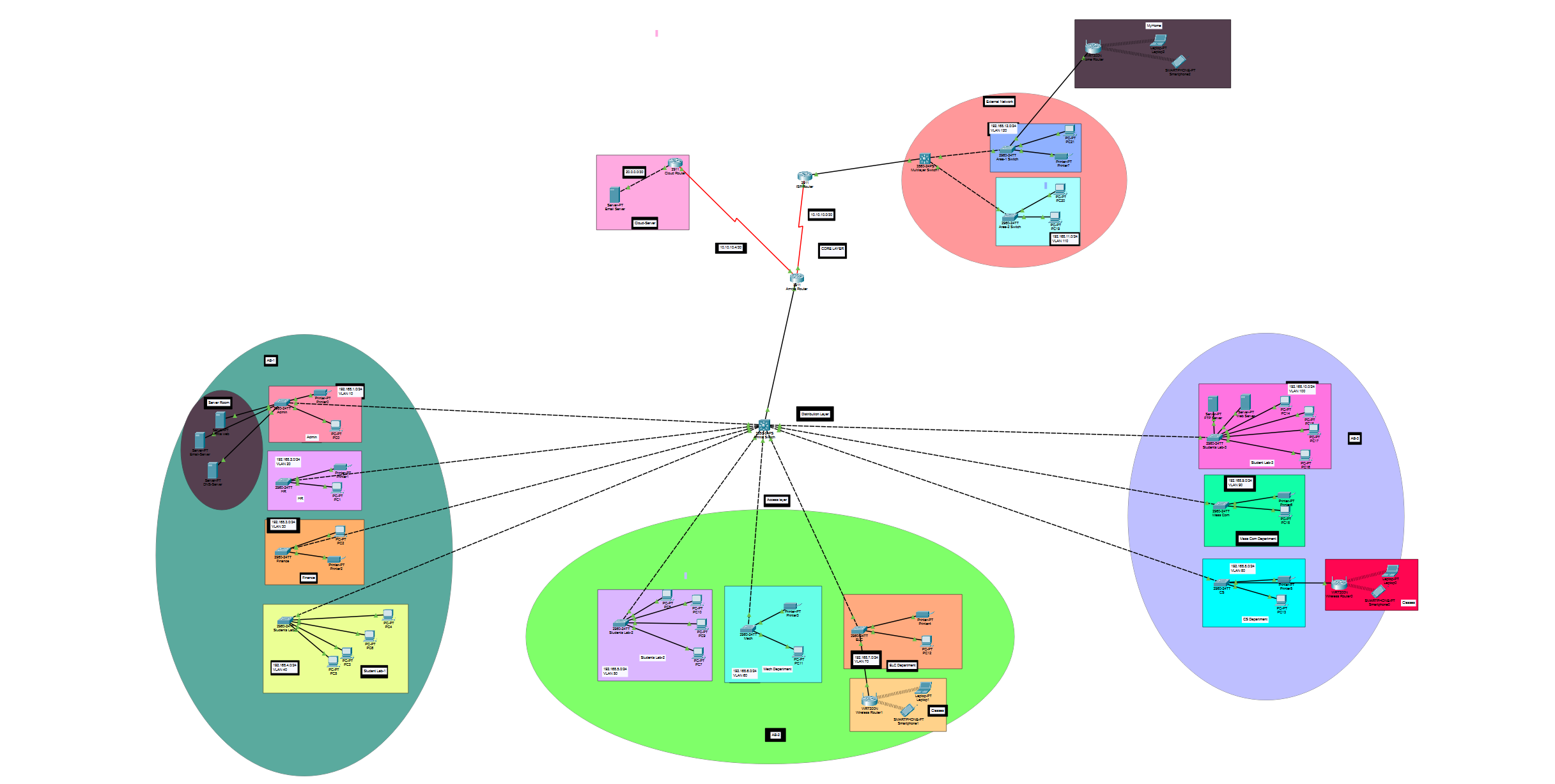
The switch working in the distribution layer is called distribution switch which receives traffic from the access layer and forwarding it to the core layer, determining the workgroup access as well as providing policy-based connectivity.

**Access Layer**



An access layer switch is usually a Layer 2 switch and facilitates the connection of end node devices to the network. In generally, it is not a high-powered switch when compared with those at the distribution layer

Complete University And Outside Campus



**Securing the network**

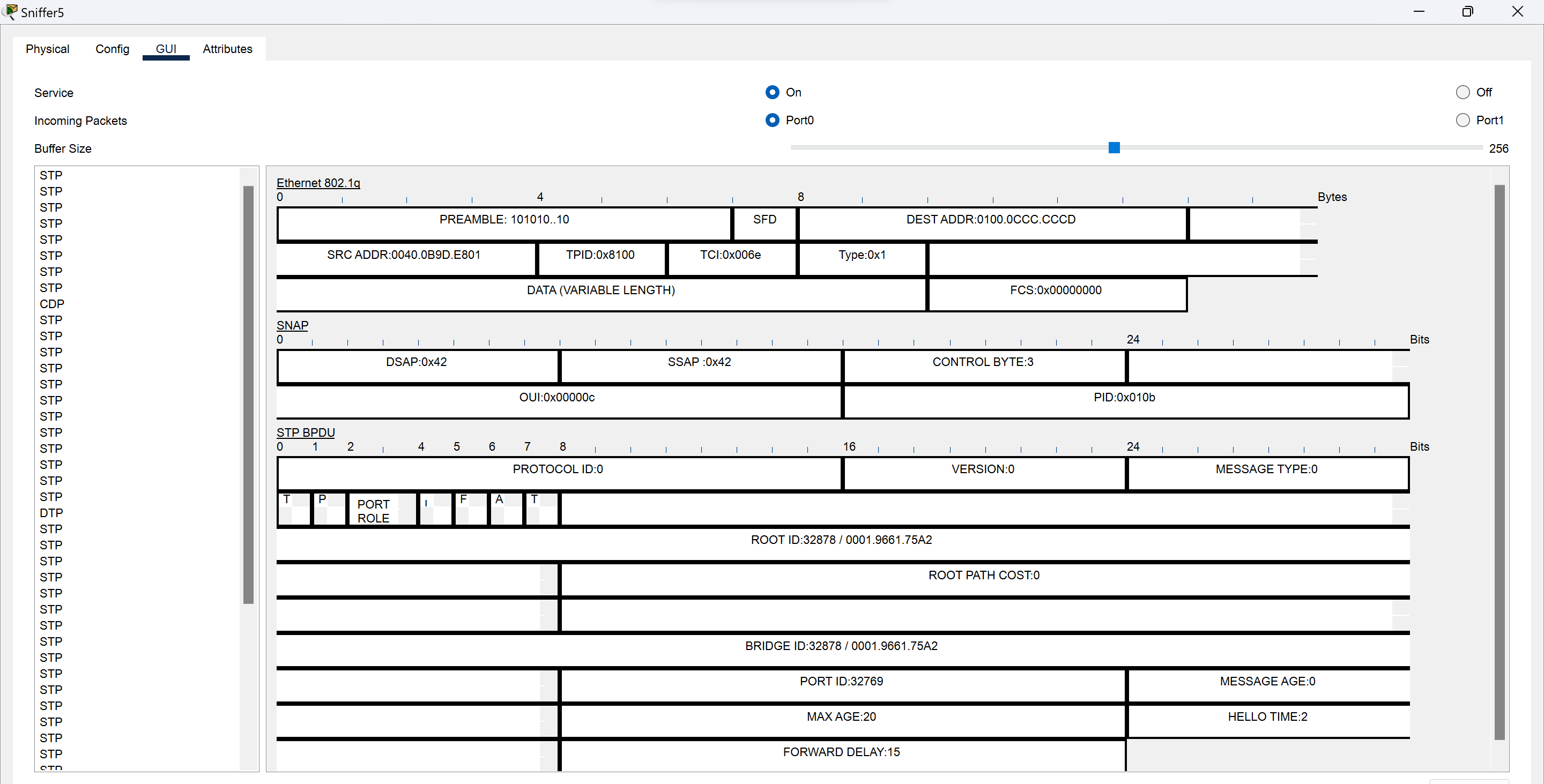
Passwords are used in accessing the router

|  |  |
| --- | --- |
| Router Name | Passwords |
| 1)Amrita Router | Console password: Amrita |
| 2)ISP Router (outside the college) | Console password: sowrabh |
| 3)Cloud Router (Email Servers) | Console password: cloud |

Traffic Through Multilayer Switch to ISP router

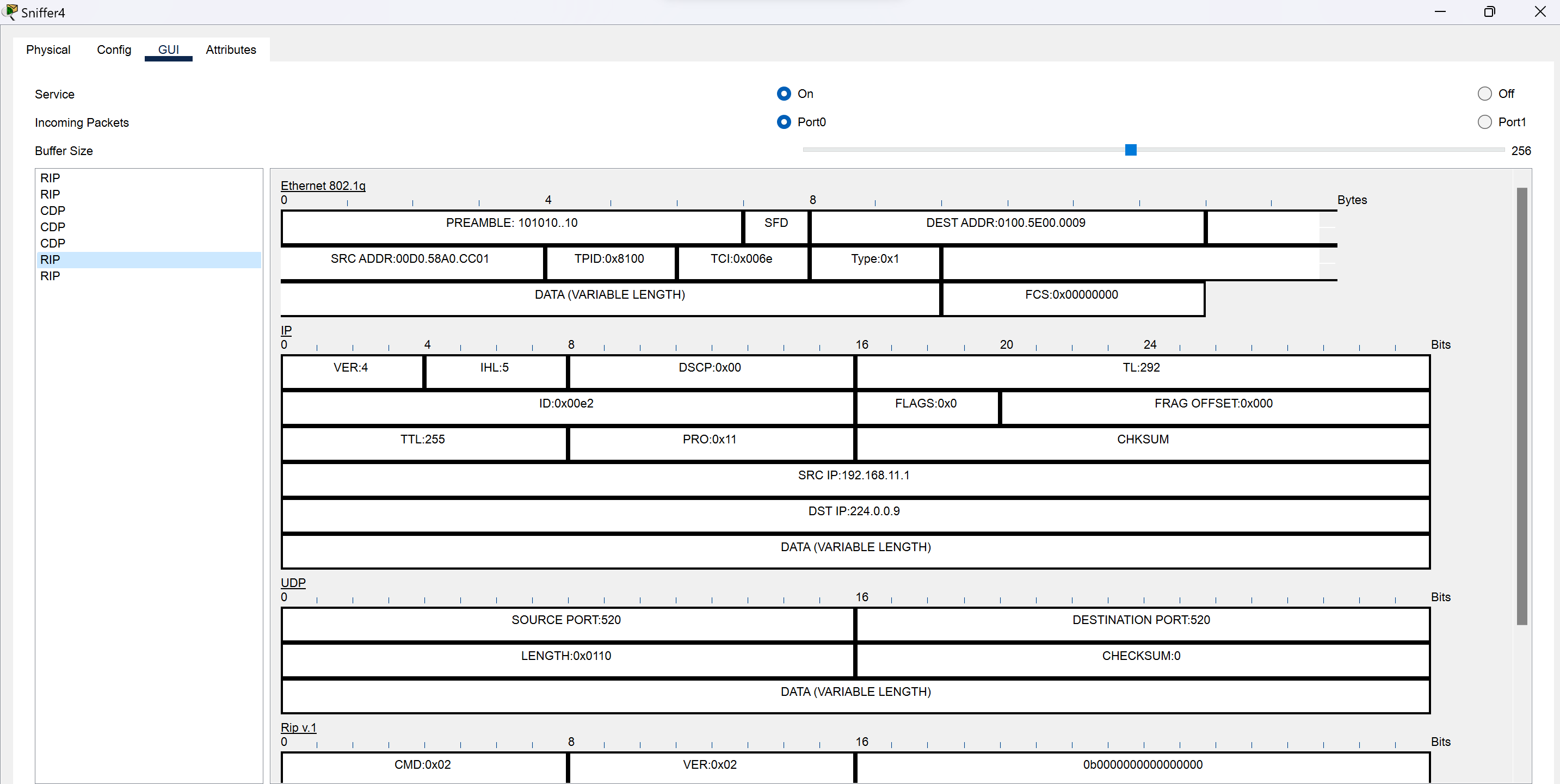


Multilayer switch(outside the campus)



1. Spanning Tree Protocol (STP) ensures a loop-free network by monitoring links and shutting down redundant ones. A root bridge distributes BPDUs and blocks the least redundant port in a single VLAN or topology, according to the STP standard.
2. With standard 802.1Q, only one instance of STP runs only over the native VLAN, and that one STP topology is used for all VLANs. Although using only one STP instance reduces the STP messaging overhead, it does not allow load balancing by using multiple STP instances
3. The Cisco CDP is a layer 2 network protocol that automatically detects connected Cisco devices and efficiently inspects them without physically inspecting them. Enabled by default, it helps in network discovery and efficient device inspection.
4. Dynamic Trunking Protocol is a CISCO proprietary protocol for negotiating trunk links between switches using either 802.1q or ISL encapsulation types.

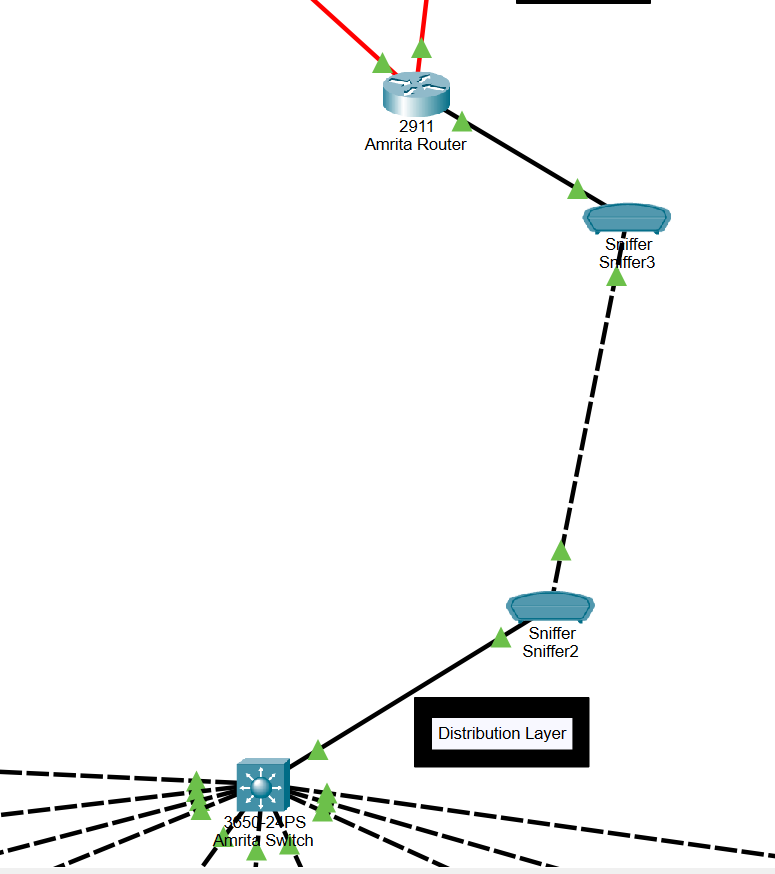
ISP Router (Outside the campus)



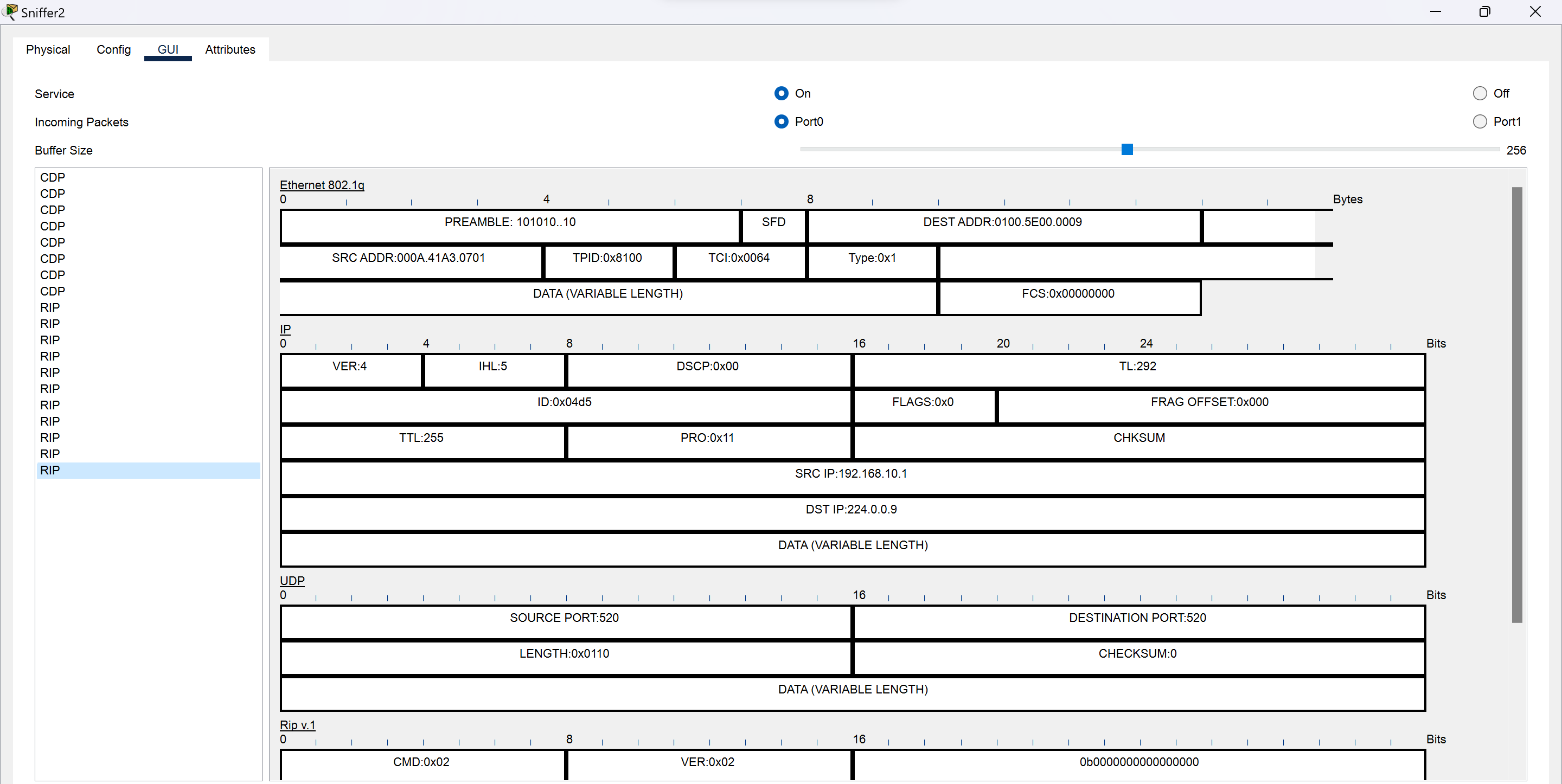
* RIP is a dynamic routing protocol using hop count as a metric to determine the best path between sources and destinations. It is a distance-vector protocol with an AD value of 120 and works on the OSI model's Network layer. It uses port number 520.
* RIP features periodic network updates, broadcasting routing information, sending full routing tables, and routers trust neighbor routers' routing information, known as routing on rumors.
* As I’m using the RIP V2 it sends update as multicast (Multicast at 224.0.0.9)

You can in the image DST IP 224.0.0.9

Traffic Through Amrita router to Multilayer switch (Inside the campus)



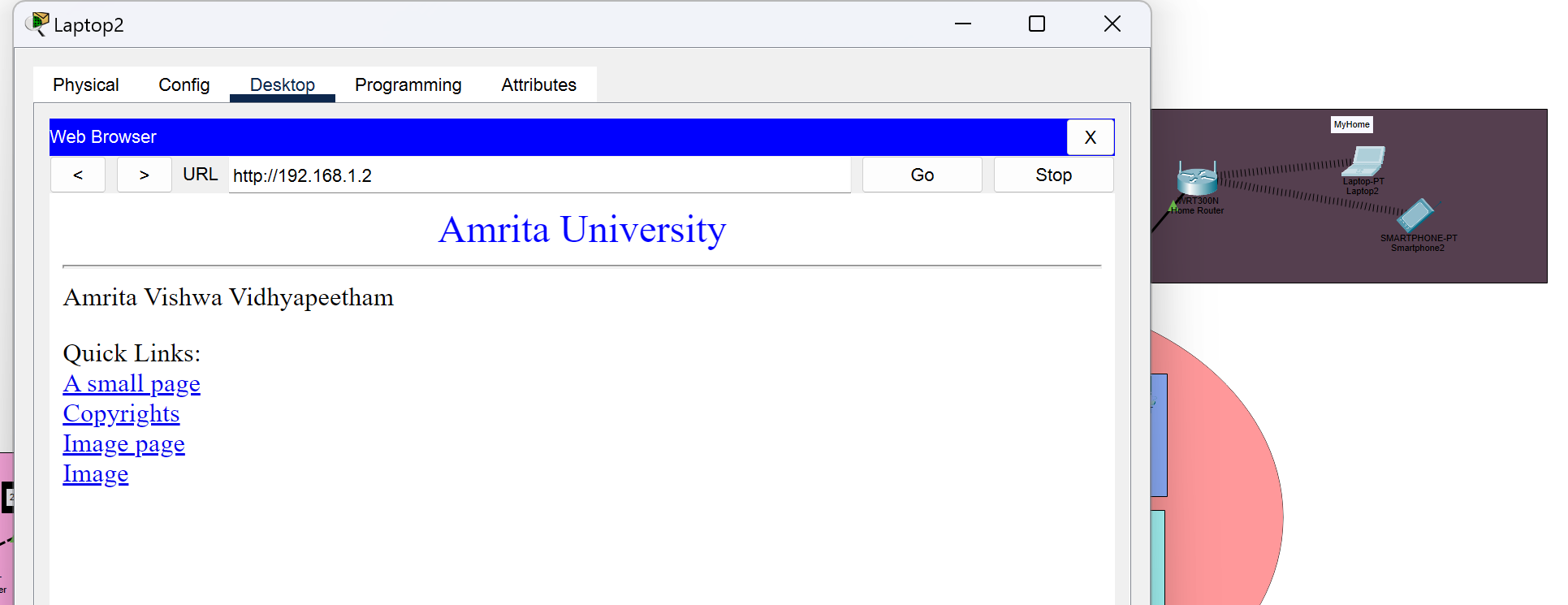
Multilayer Switch (inside the campus)

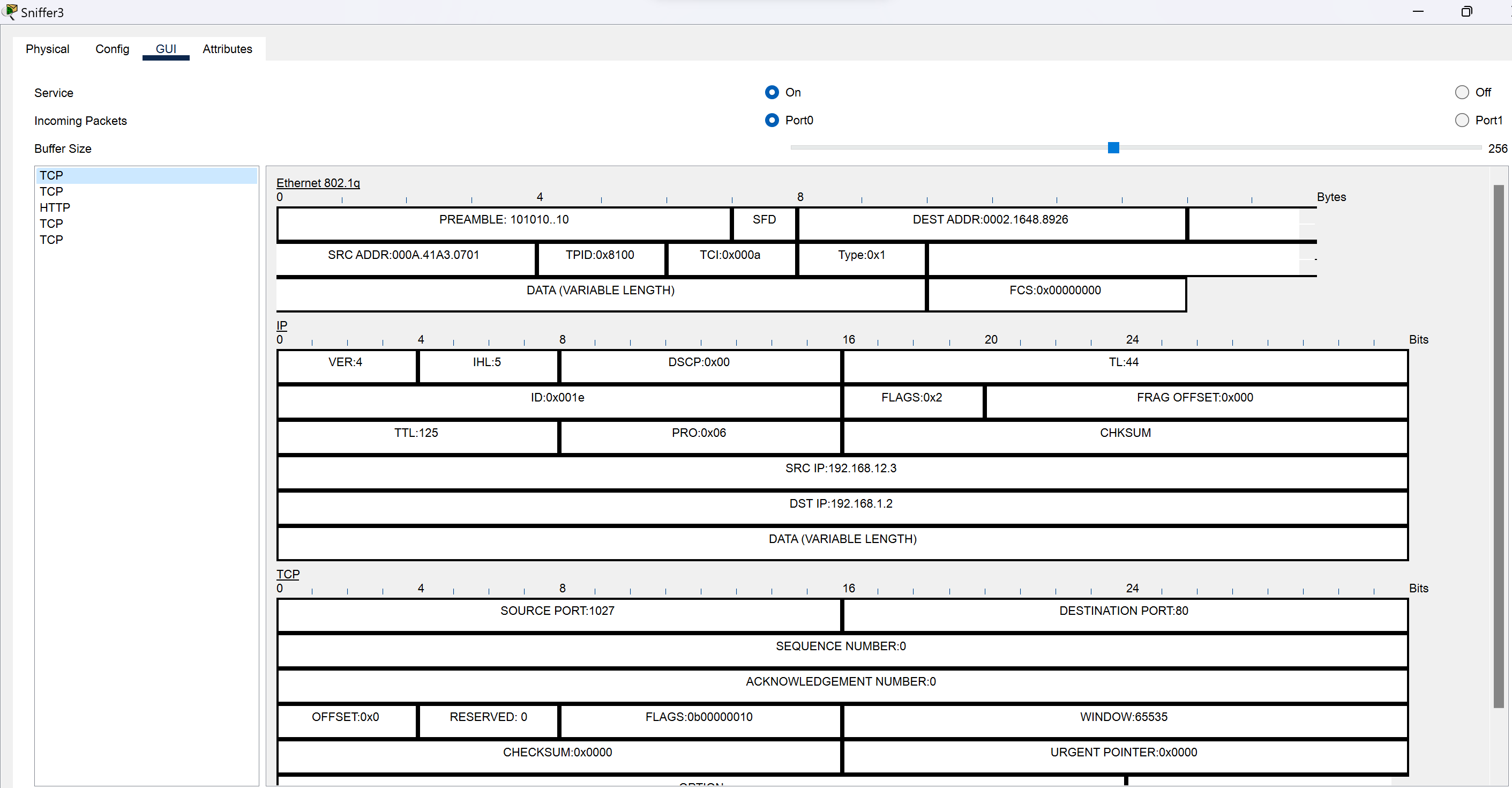


* RIP requests are more frequent on campus due to 10 departments and limited area assignment, while outside campus multilayer switches have fewer requests due to limited area allocation.

Amrita Router

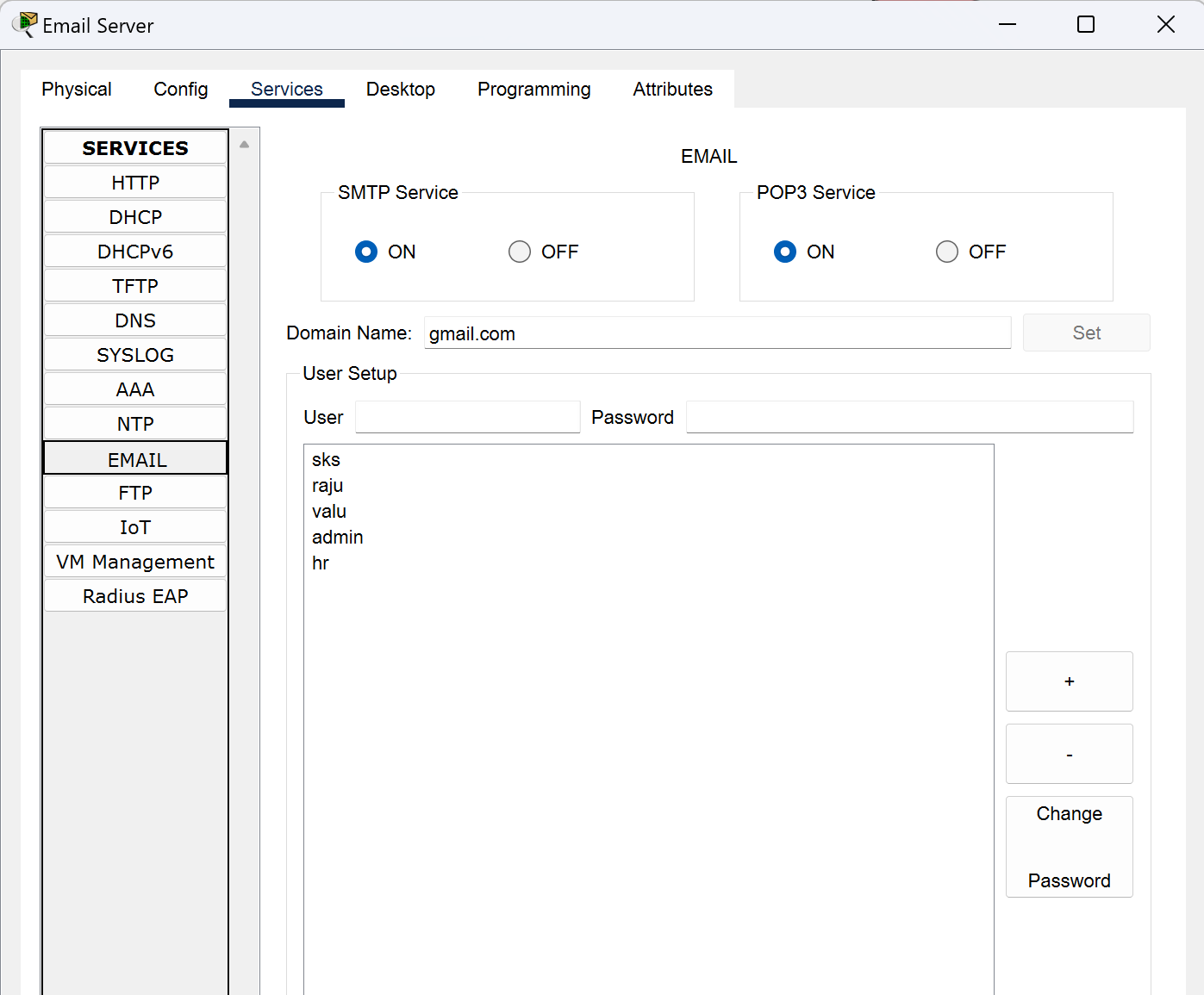
Let’s request for Amrita Web from outside the campus and see what packets are flowing through the amrita router



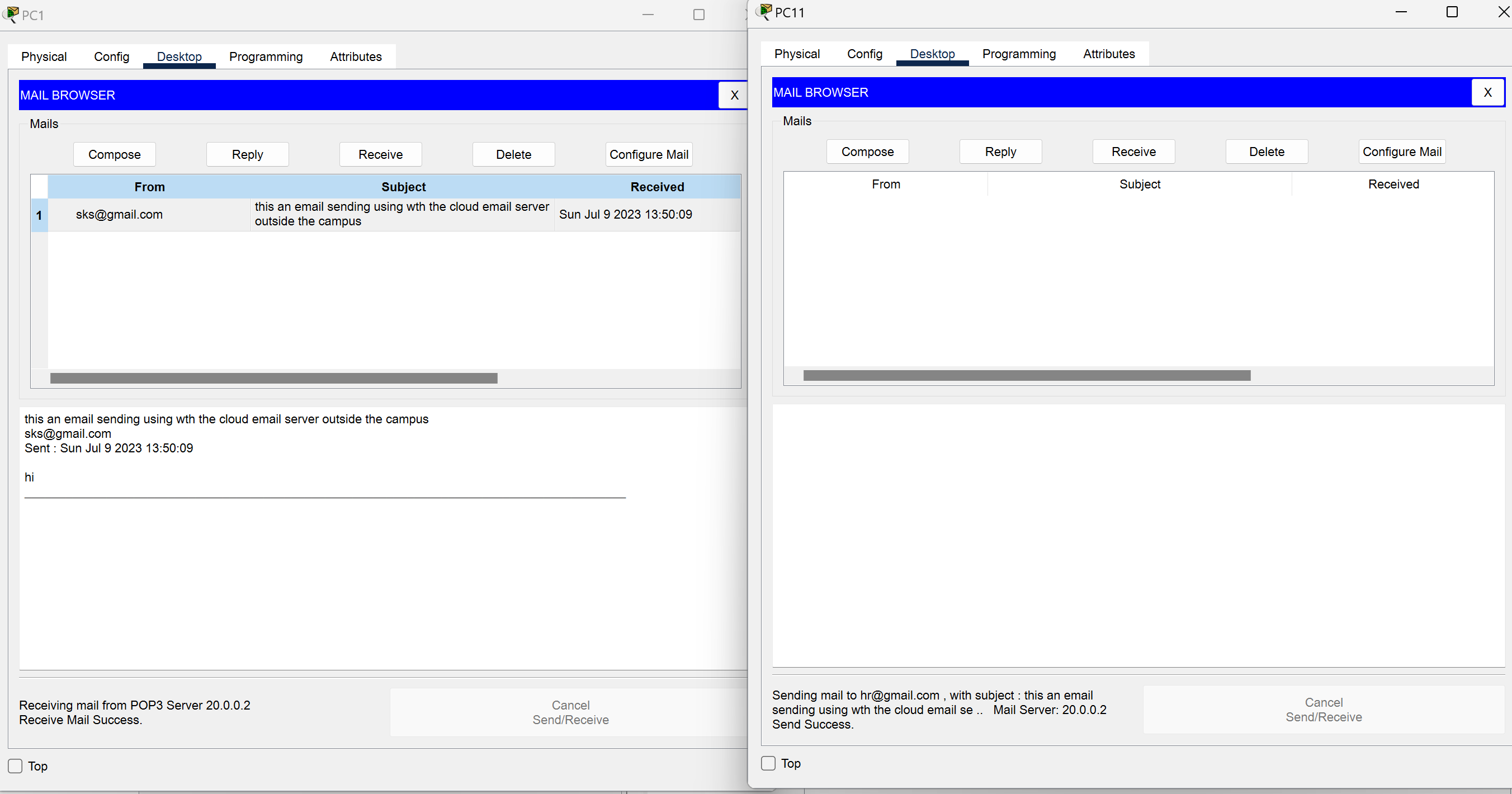


* As you can see HTTP and TCP Packets are flowing
* When you request a website, your browser communicates with the web server using two main protocols: DNS for initial domain-to-IP resolution, and TCP for establishing a reliable connection. Once connected, the browser sends an HTTP request to the server, specifying the desired resource. The server responds with an HTTP response containing the requested data, which is delivered back to the browser via the established TCP connection. This seamless interaction between TCP and HTTP enables the successful retrieval and rendering of web pages

This the cloud email server (Domain: gmail.com)



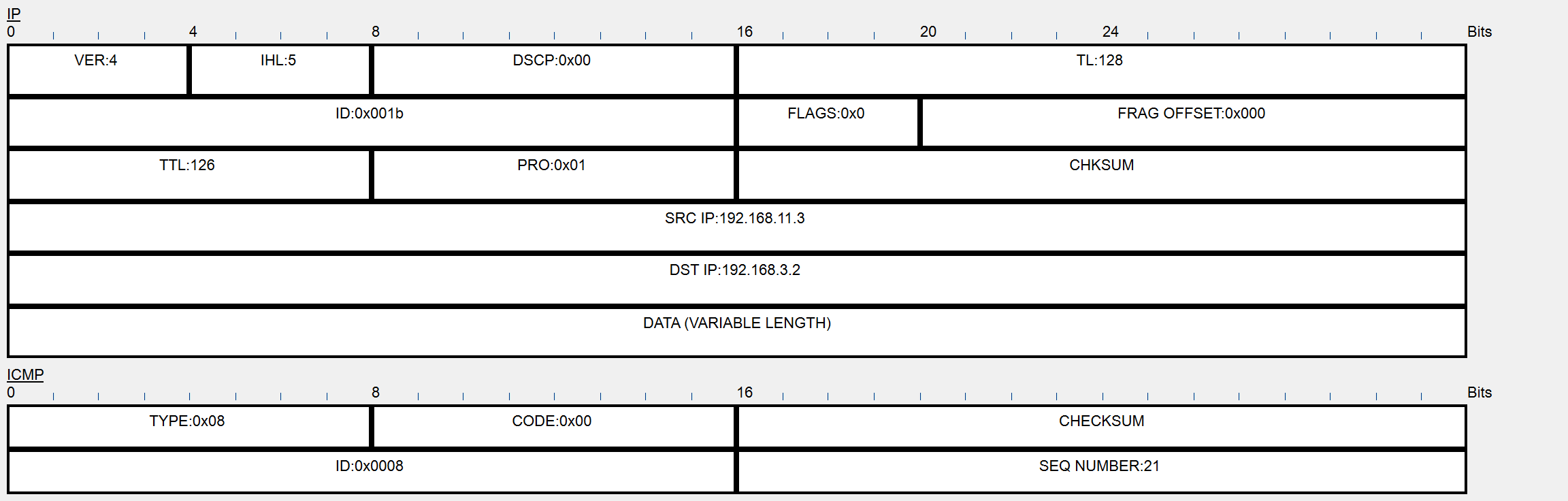
The email server from outside campus (gmail.com) displays the number of users added, I will be sending email from user: sks.



ICMP Packet (Ping)

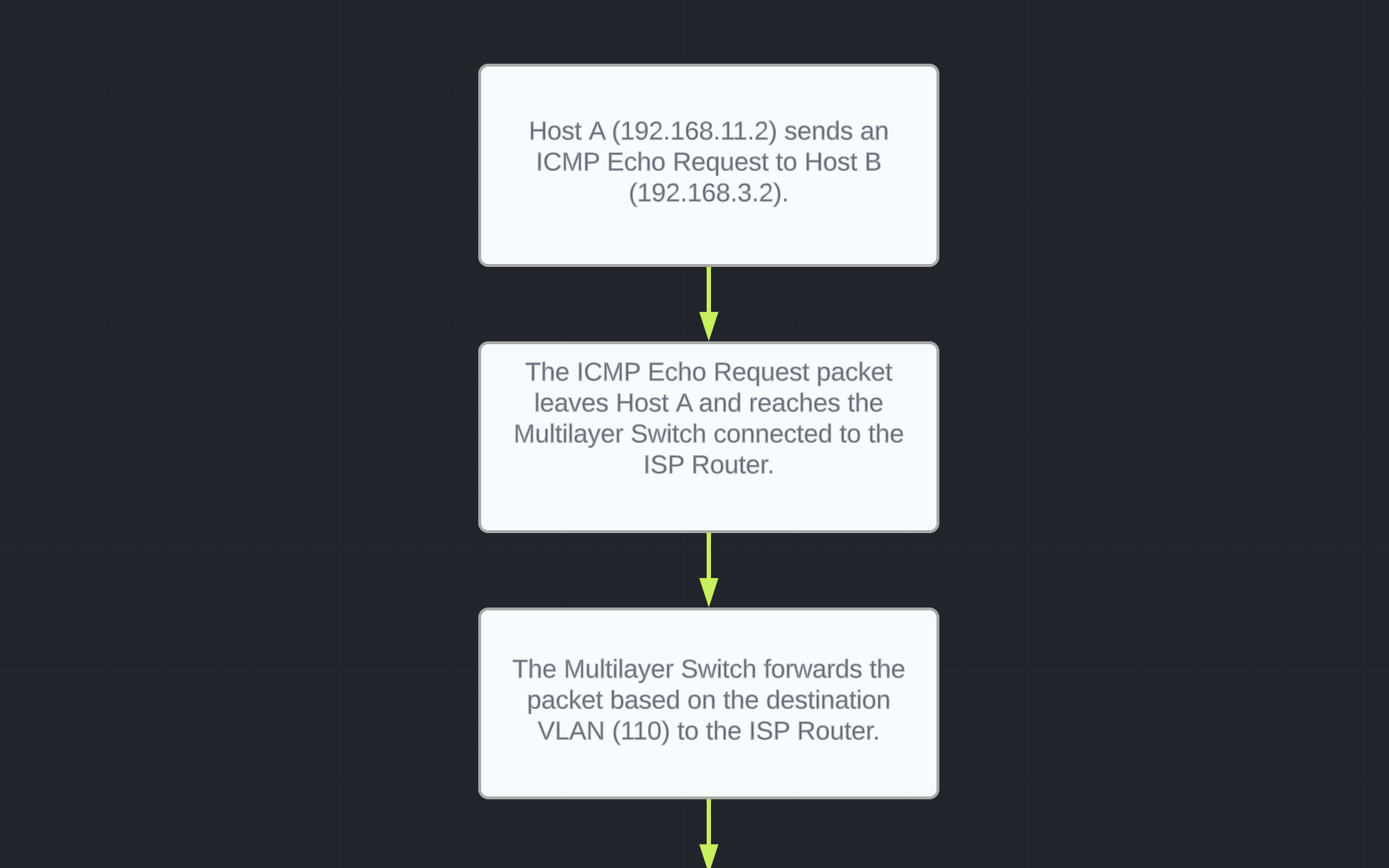


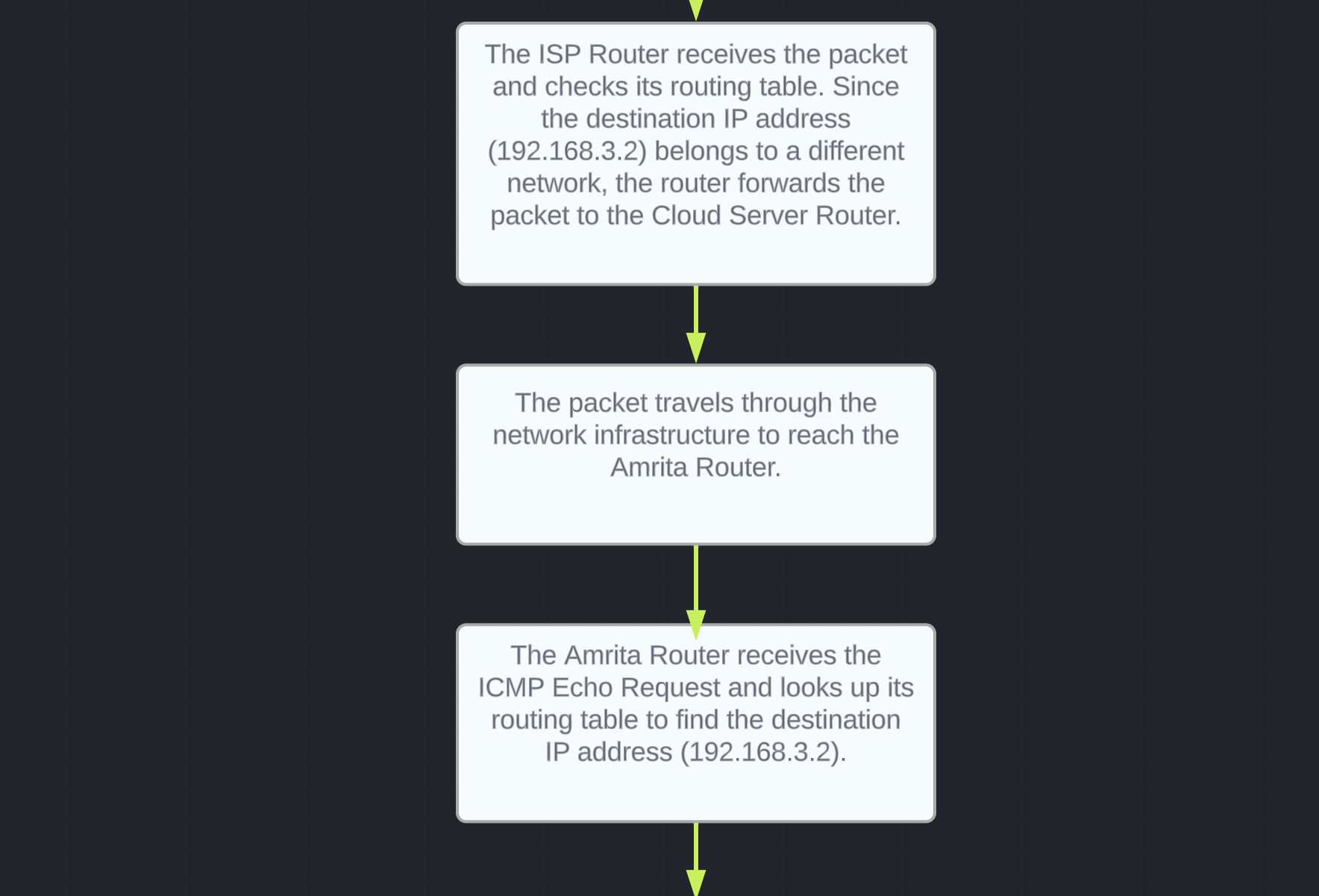
1. Ping command sends ICMP requests to destination IP for device requests, ensuring device communication.
2. In the image which I have provided above there are 4 ICMP requests, we know that usually in cisco packet tracer it sends only 4 packets when use the ping command

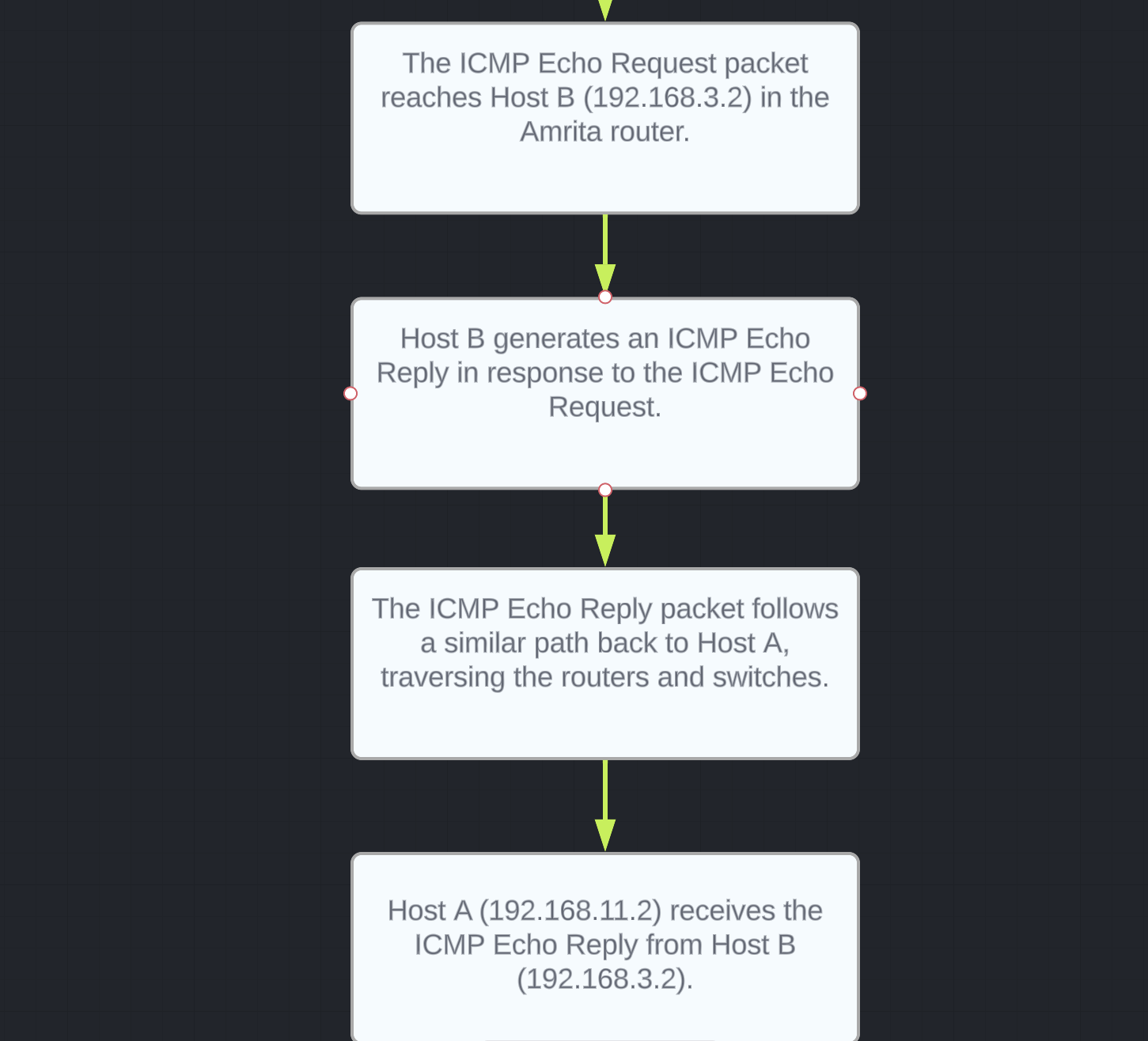


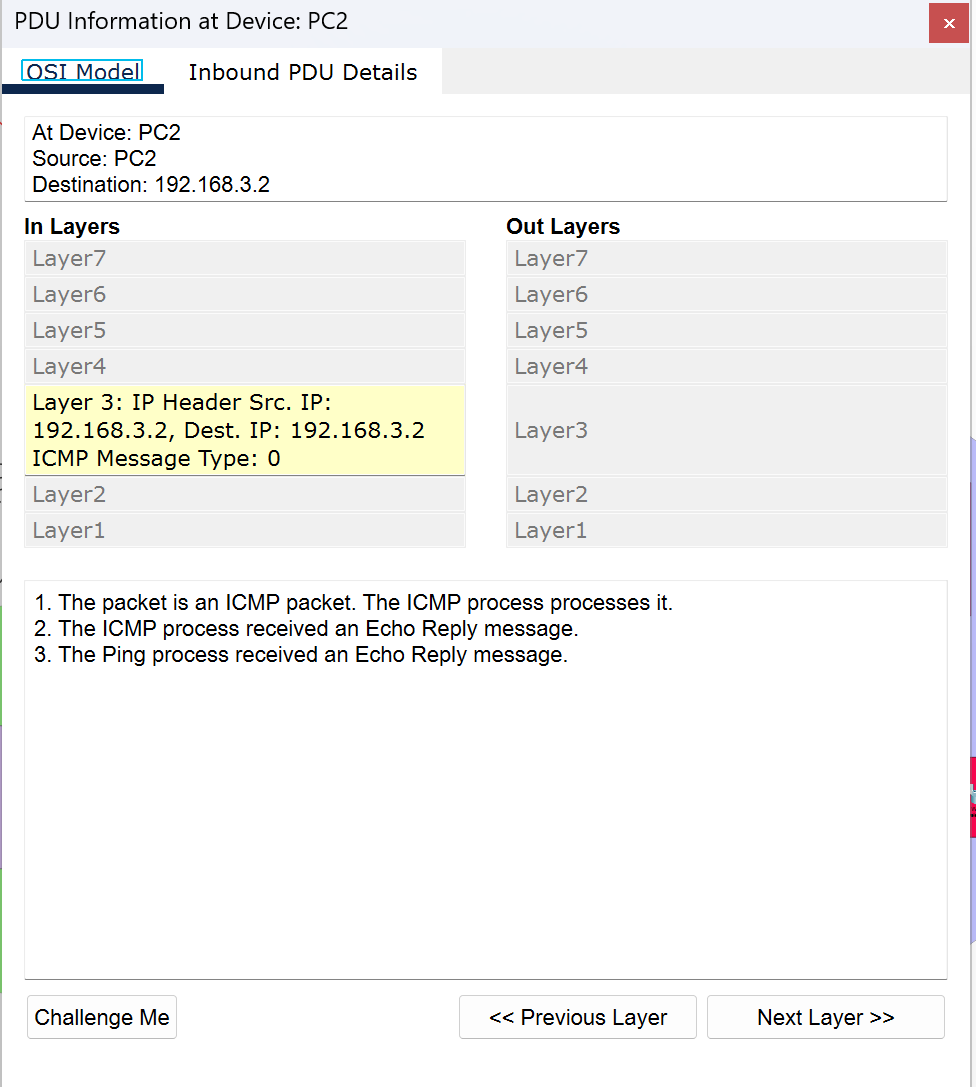
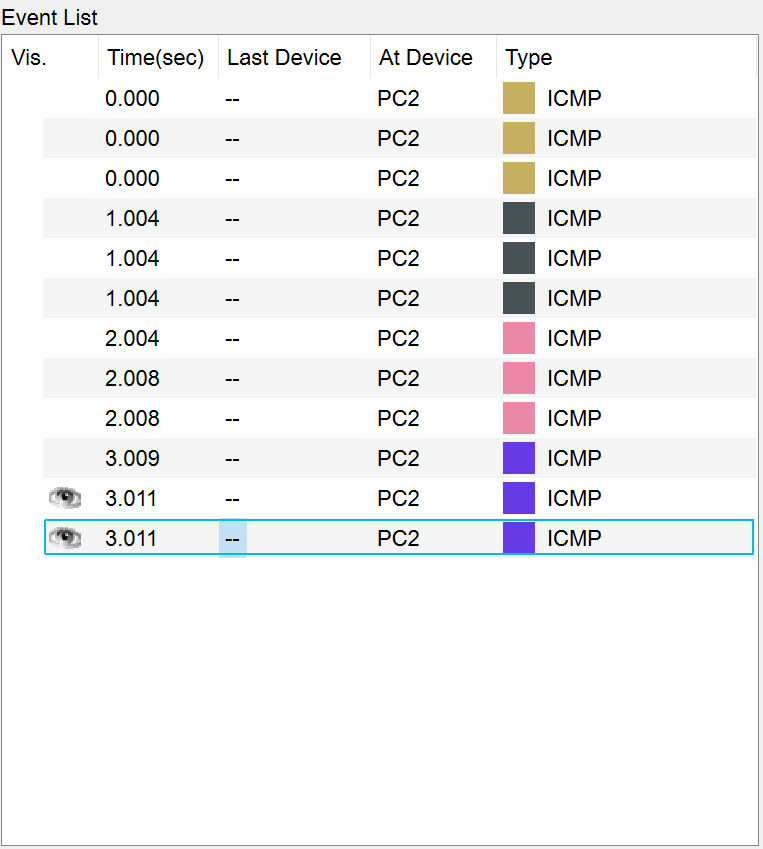
The "ID" field in the IP header assigns a unique identifier to each IP packet, allowing devices to differentiate between different packets, even if they share the same source and destination IP addresses. In the ICMP header, the "Sequence Number" field serves a different purpose. When a device sends an ICMP Echo Request (ping) message to another device, it includes a Sequence Number in the header. The receiving device then copies the same Sequence Number back into the ICMP Echo Reply, helping match the received response with the corresponding Echo Request. This is crucial in situations where multiple ICMP Echo Requests are sent in rapid succession, and the sender needs to track which Echo Request each reply corresponds to. By using these fields together, network administrators can gain better insights into the flow and behavior of ICMP packets and network connectivity.

Flow Chart (ICMP)



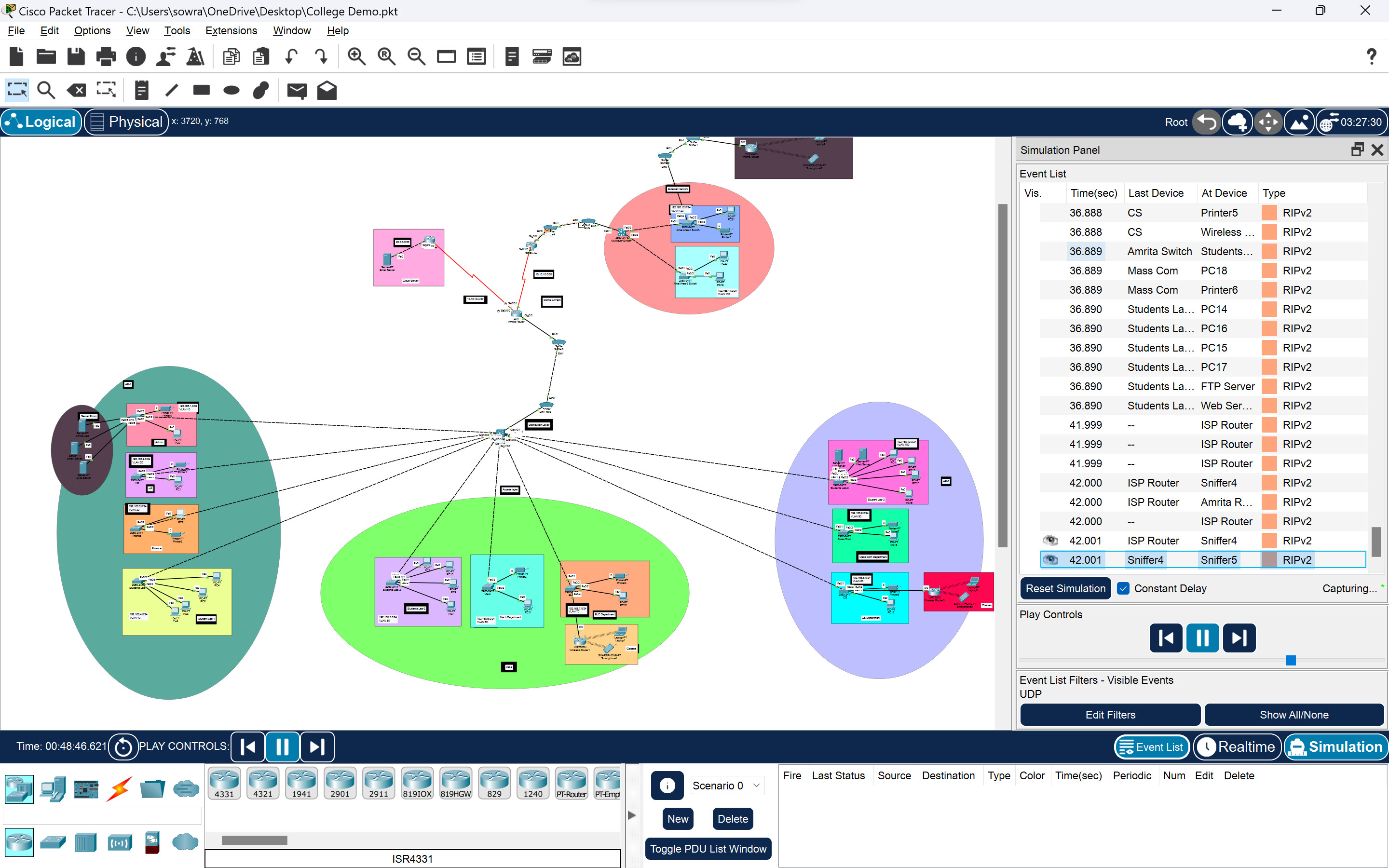






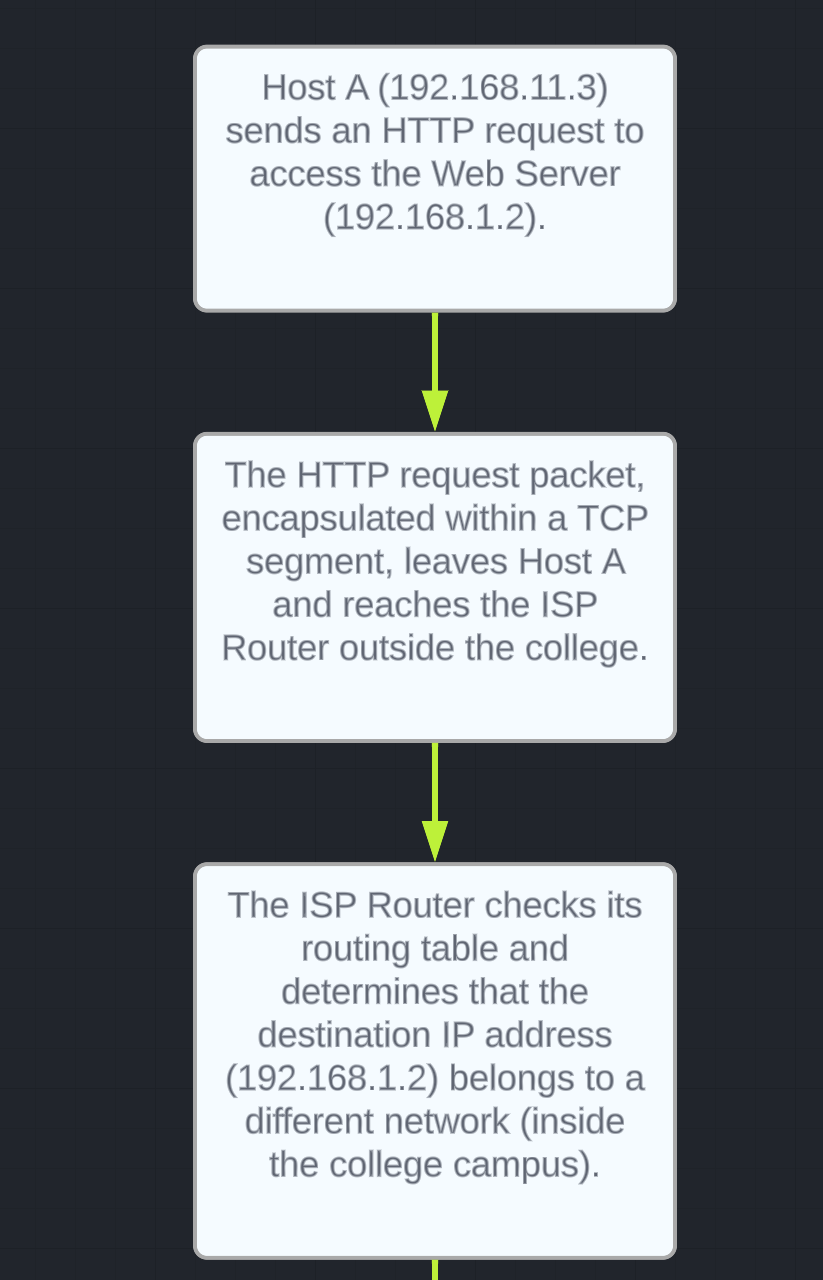
All the four colors represent the four ICMP requests

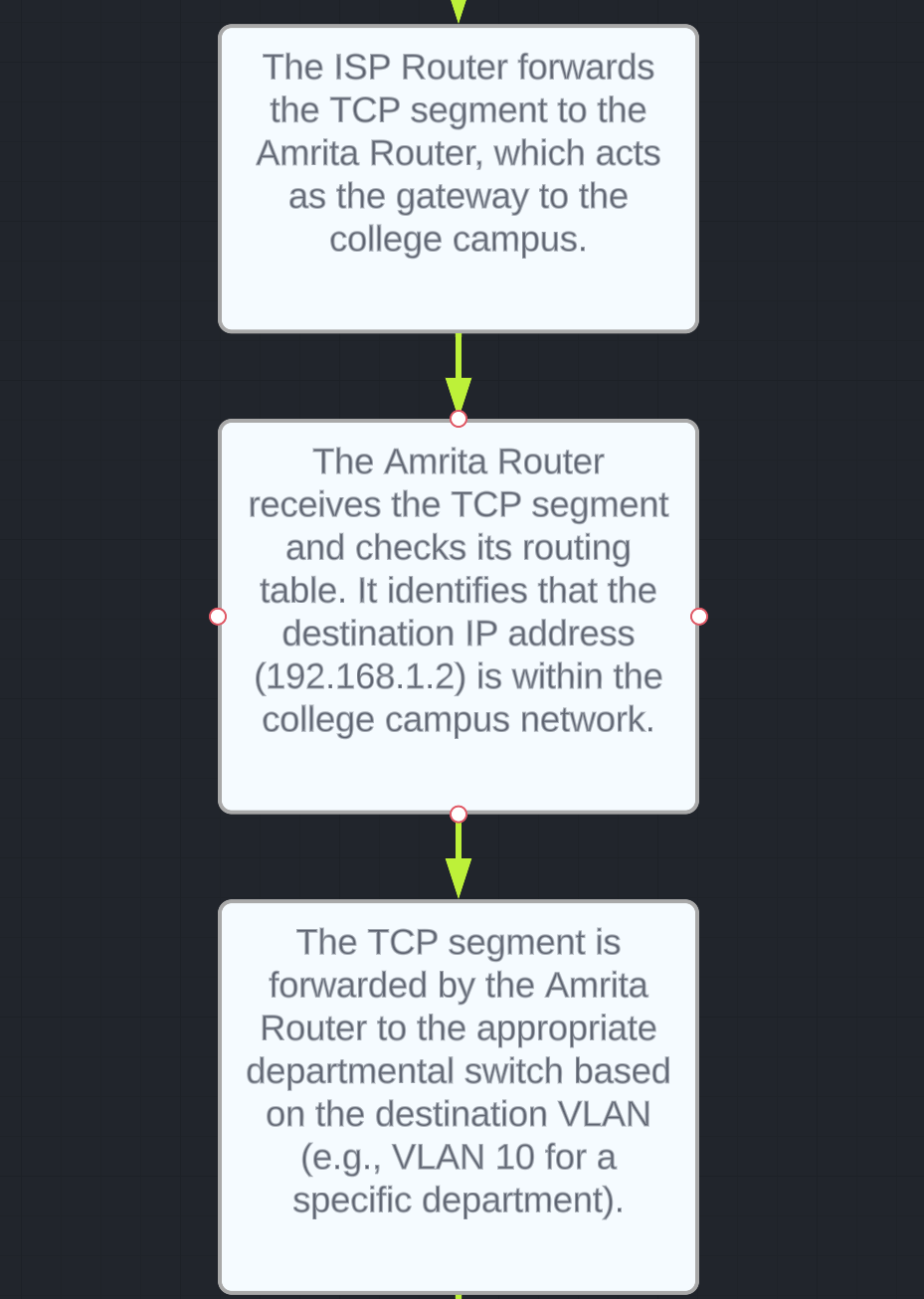
RIP V2

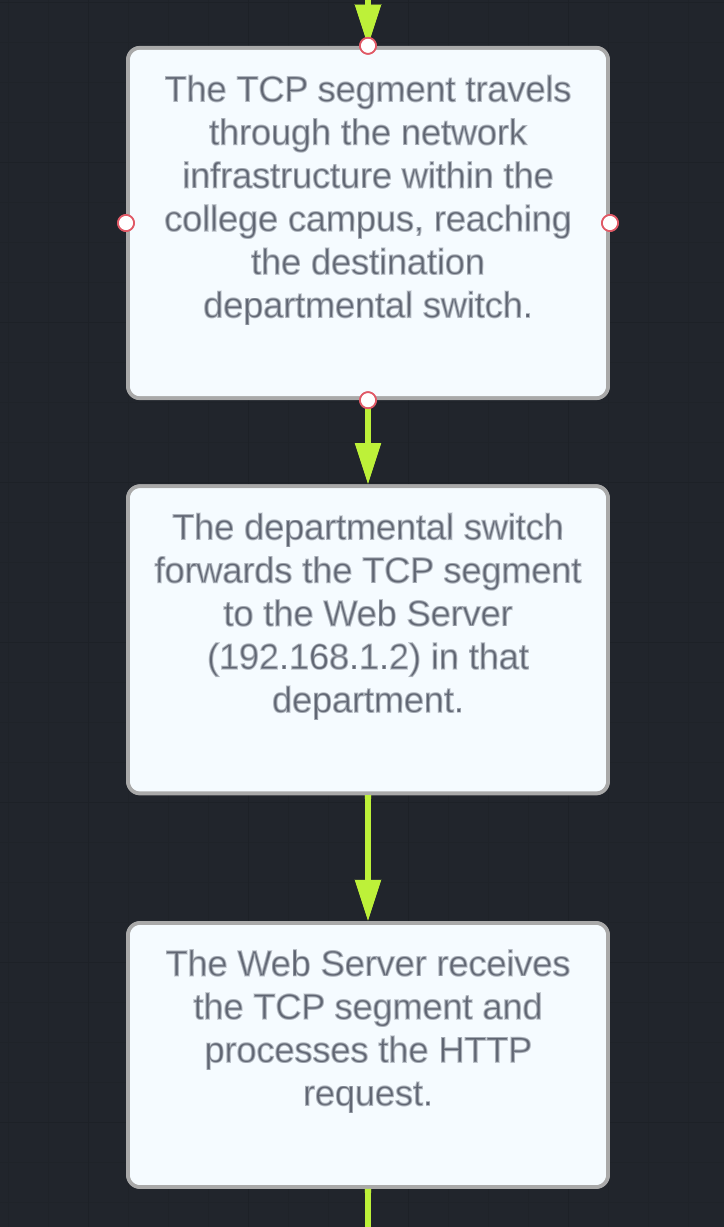


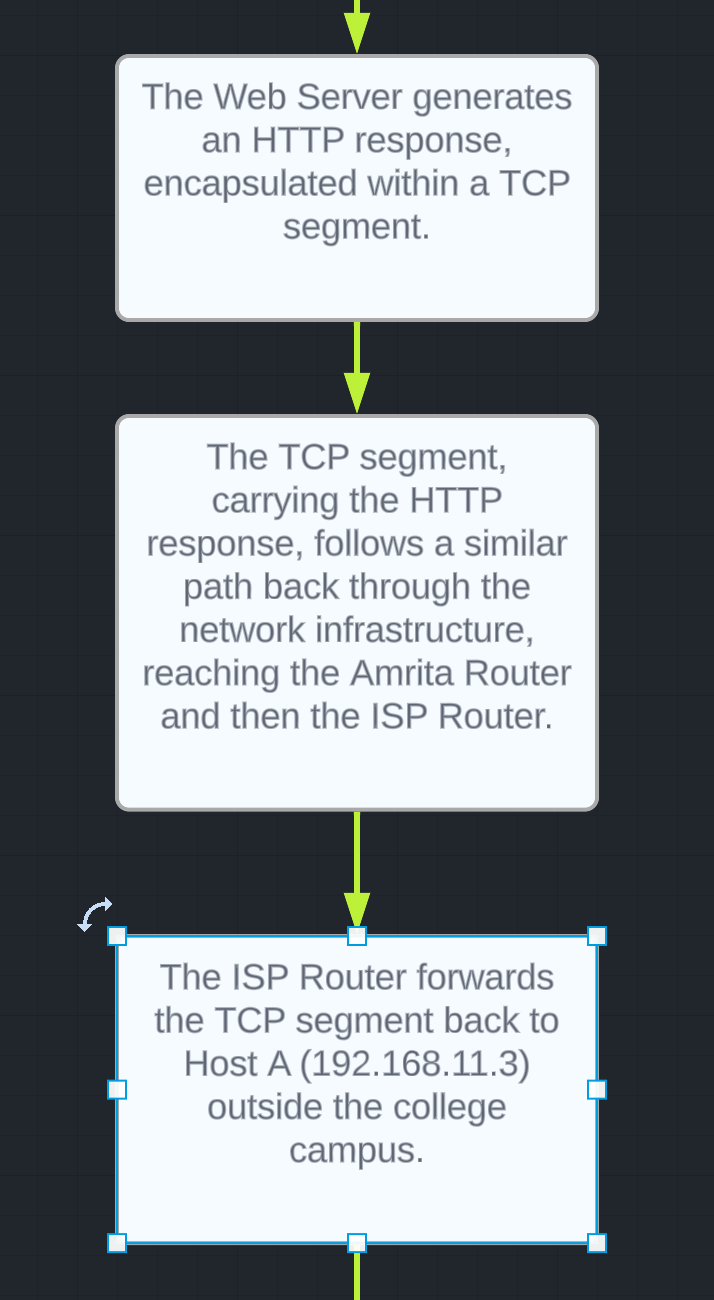
In the above image you can see the RIP V2 is always finding for the best possible path from source to the destination

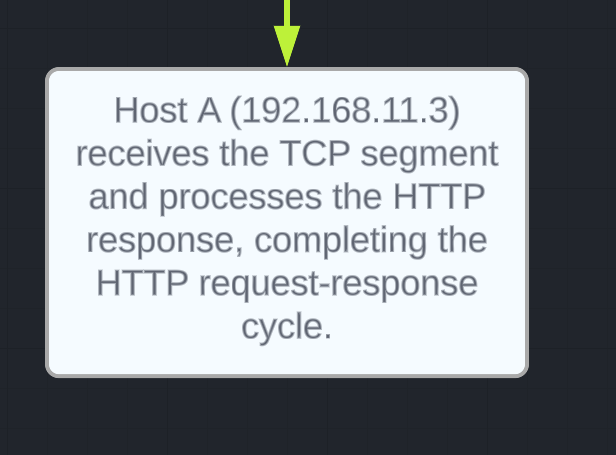
Flow chart (HTTP AND TCP)





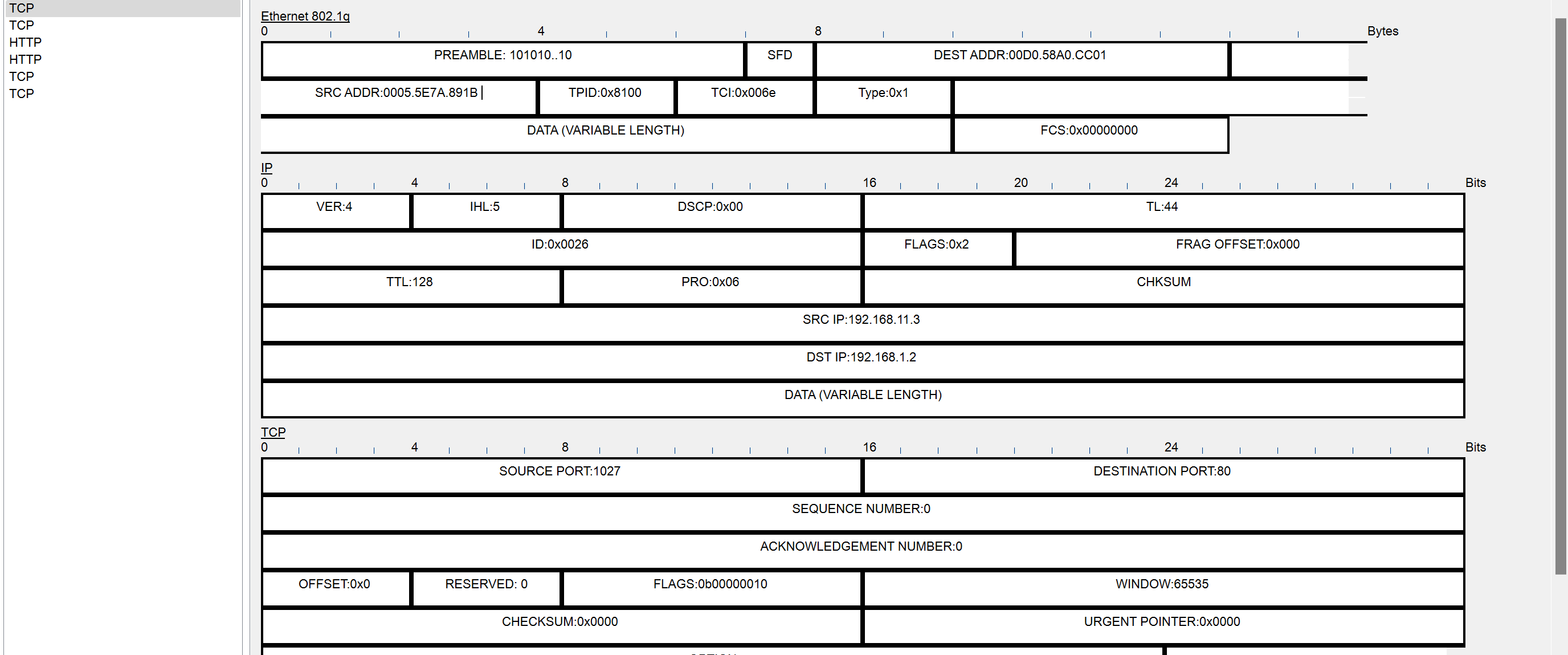




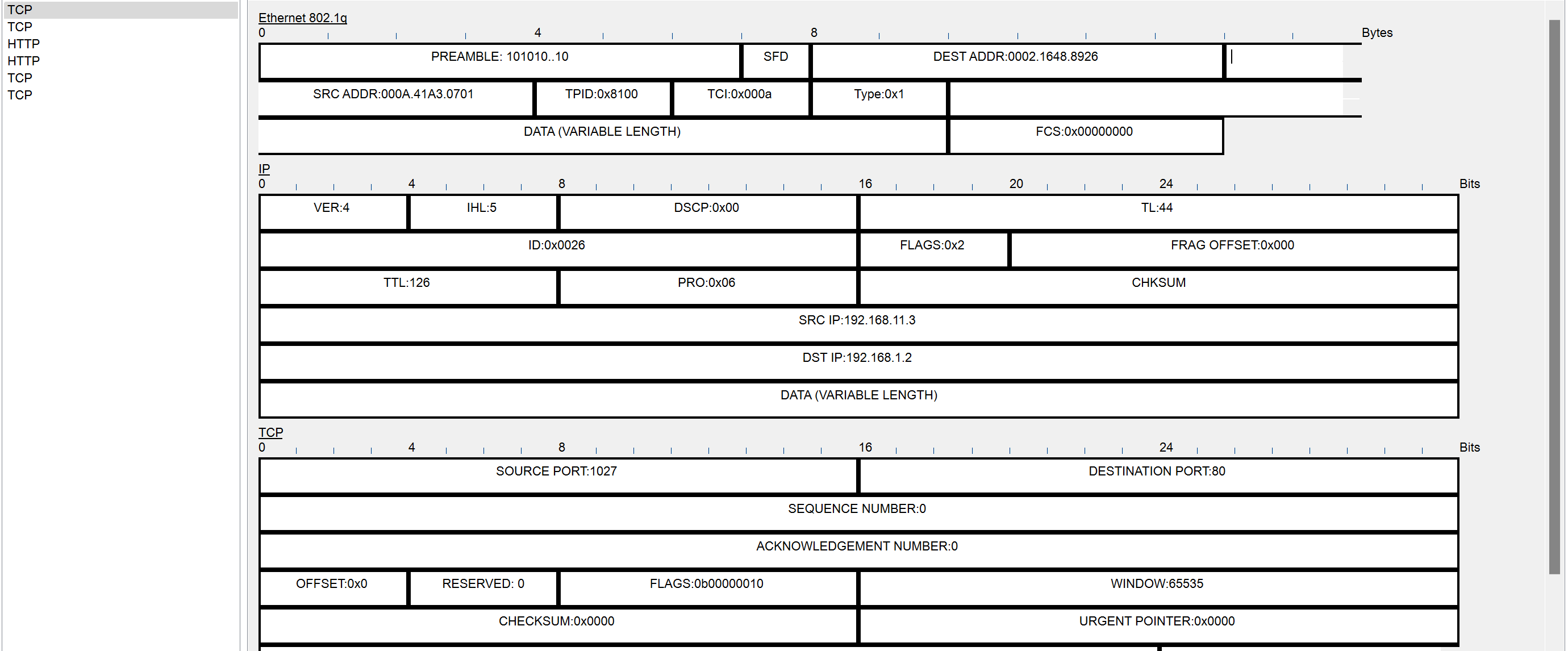


HTTP AND TCP Request

Outside the campus



Inside the campus



Host A sends an HTTP request to access the Web Server, which is then forwarded to the ISP Router outside the college. The ISP Router replaces the source MAC address with its own, and the Amrita Router receives the packet with its destination MAC address. The Amrita Router checks its routing table and forwards the packet to the Web Server. The packet travels through the campus network infrastructure, reaching the departmental switch connected to the Web Server. The departmental switch replaces the destination MAC address with the Web Server's MAC address before forwarding the packet to the Web Server. The Web Server processes the HTTP request and generates an HTTP response. The response is sent back through the network infrastructure, reaching the ISP Router and then Host A. At each hop, the MAC addresses in the Ethernet header are updated to ensure proper delivery to the next hop.

Outside the campus (First request)

TCP Header Details:

Source Mac: 0005.5E7A.891B

Destination mac: 00D0.58A0.CC01

Source Port:

Destination Port: 80 (80 for HTTP)

Sequence Number: 0

Acknowledgment Number: 0

TCP Flags: 0b00000010

Window Size: 65535

HTTP Header Details:

Method: GET (e.g., GET for requesting a web page)

Host: 192.168.1.2

HTTP Data: Accept-Language: en-us  
 Accept: \*/\*

Inside the campus (First request)

TCP Header Details:

Source mac: 000A.41A3.0701

Destination mac: 0002.1648.8926

Source Port: 1027

Destination Port: 80 (80 for HTTP)

Sequence Number: 0

Acknowledgment Number: 0

TCP Flags: 0b00000010

Window Size: 65535

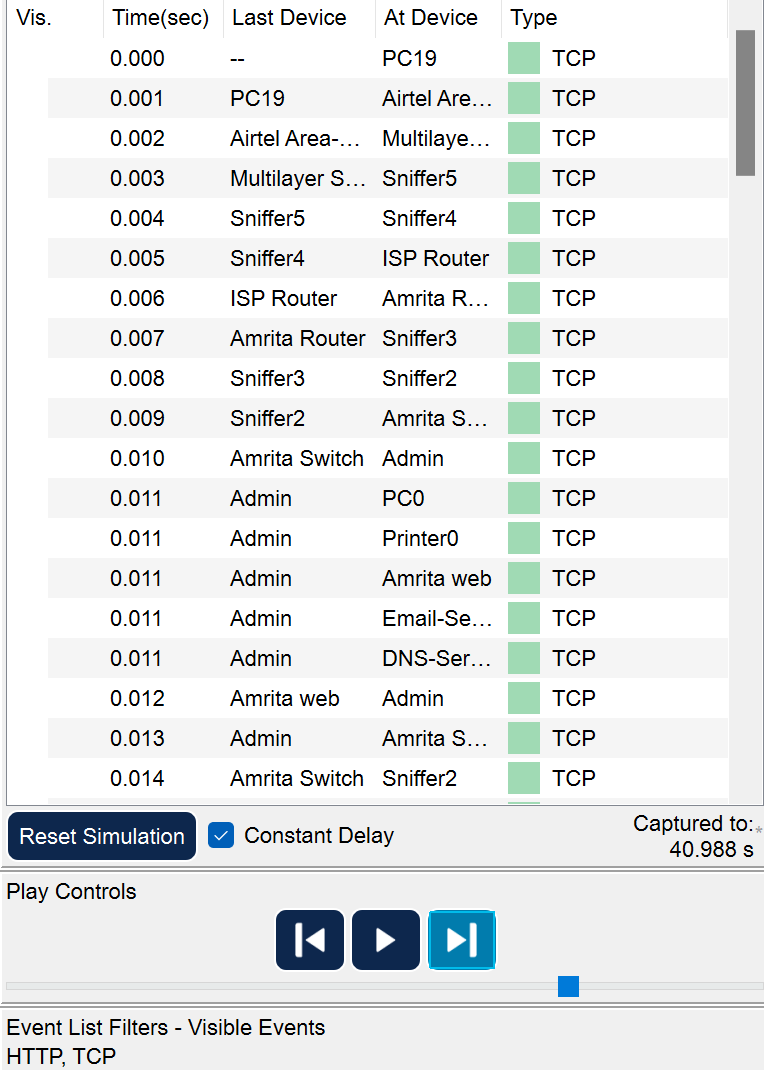
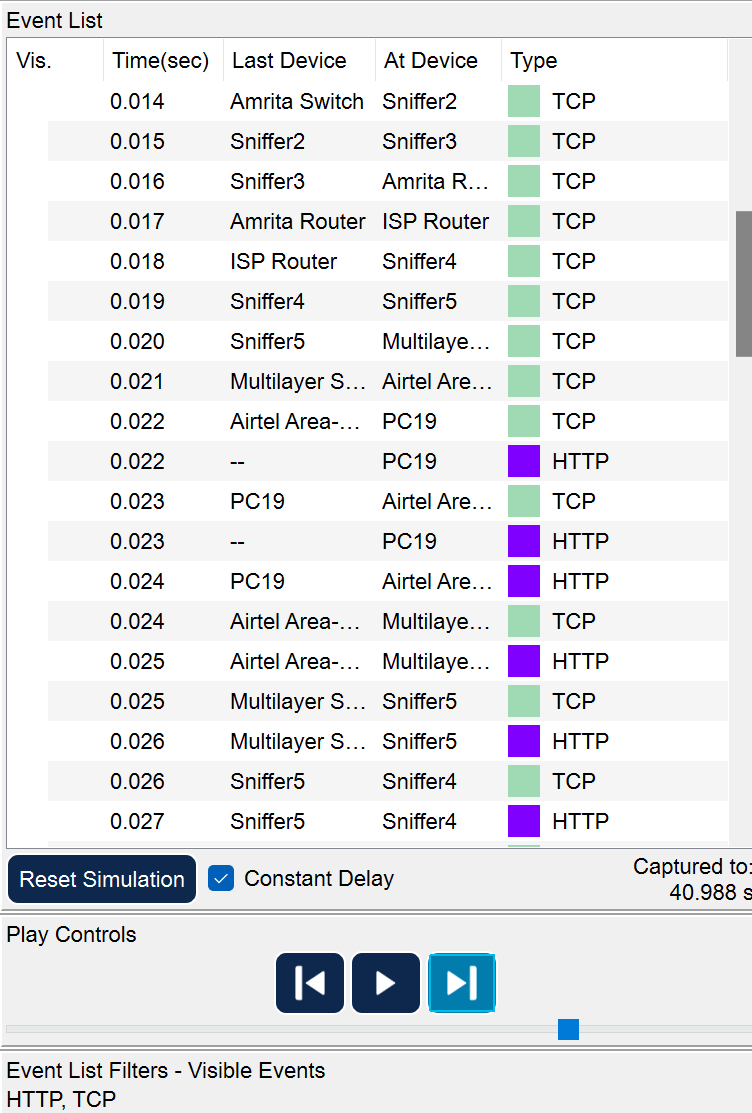
HTTP Header Details:

Method: GET (e.g., GET for requesting a web page)

Host: 192.168.1.2

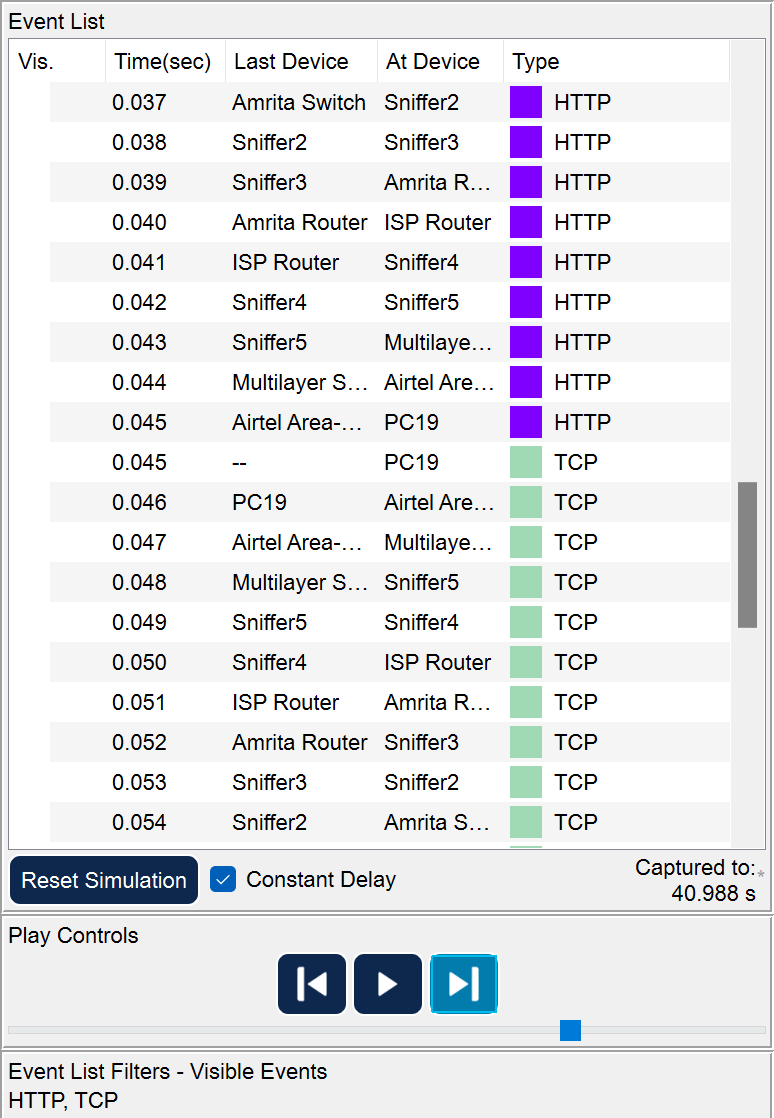
HTTP Data: Accept-Language: en-us

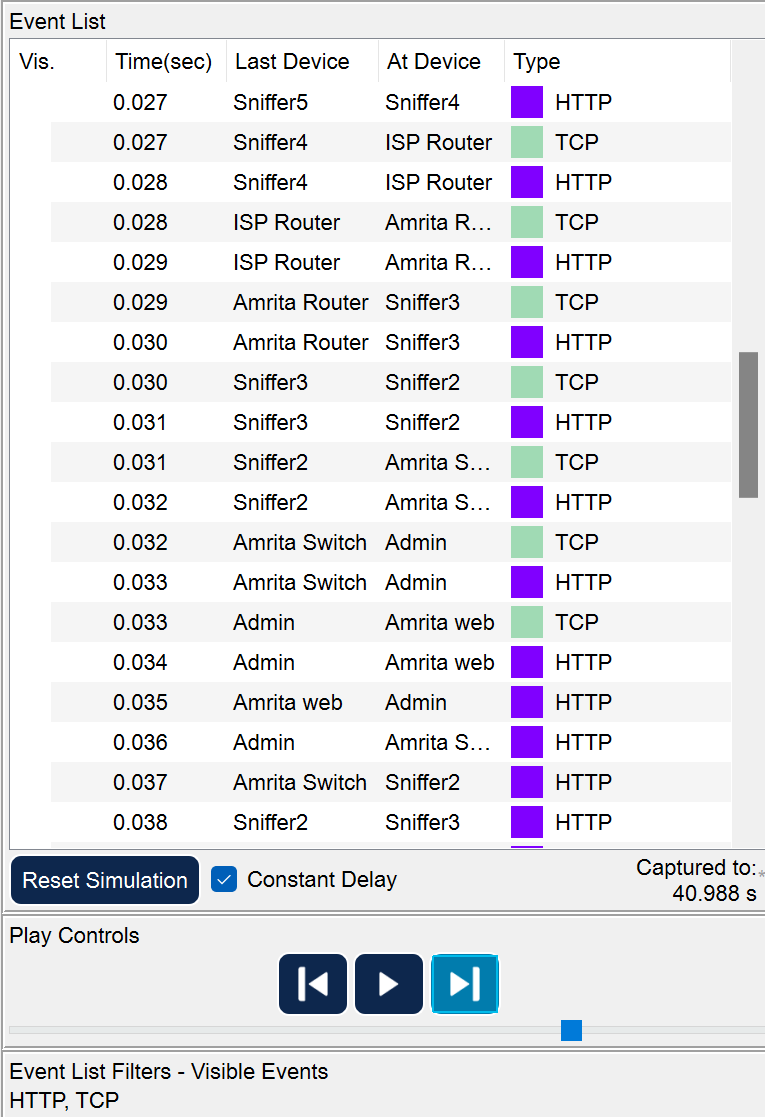
Accept: \*/\*



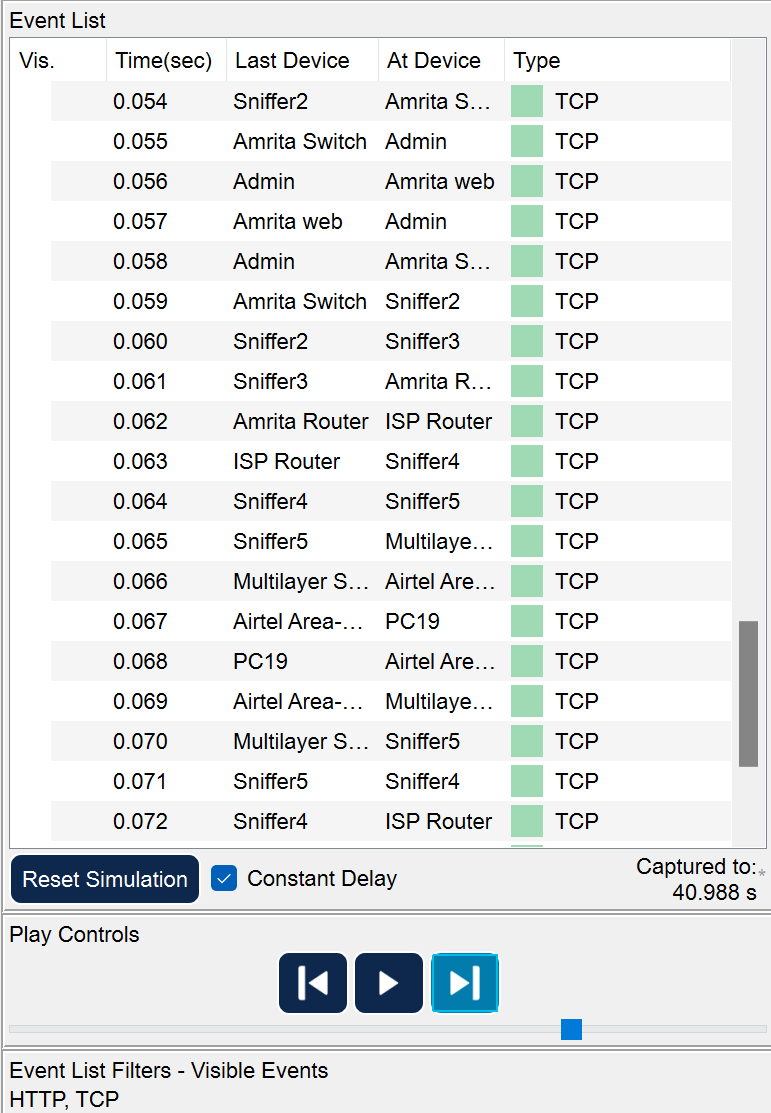
→

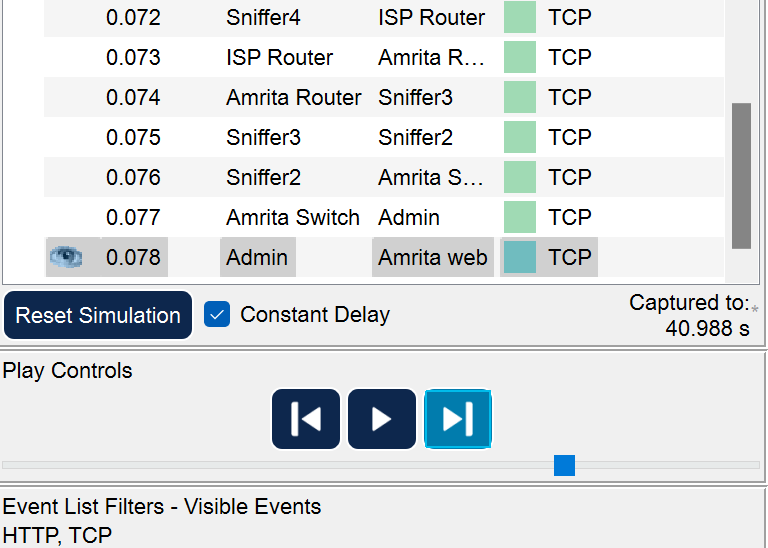
↓



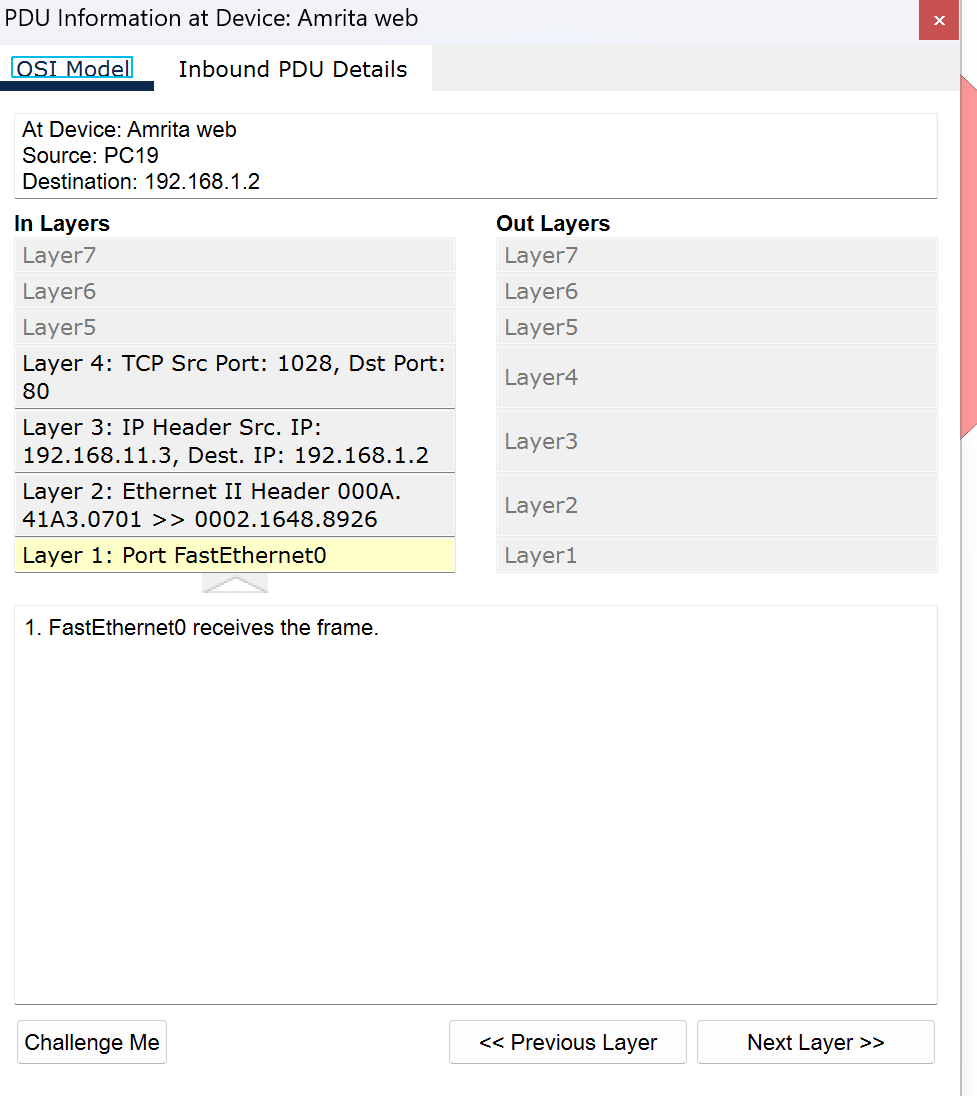


←

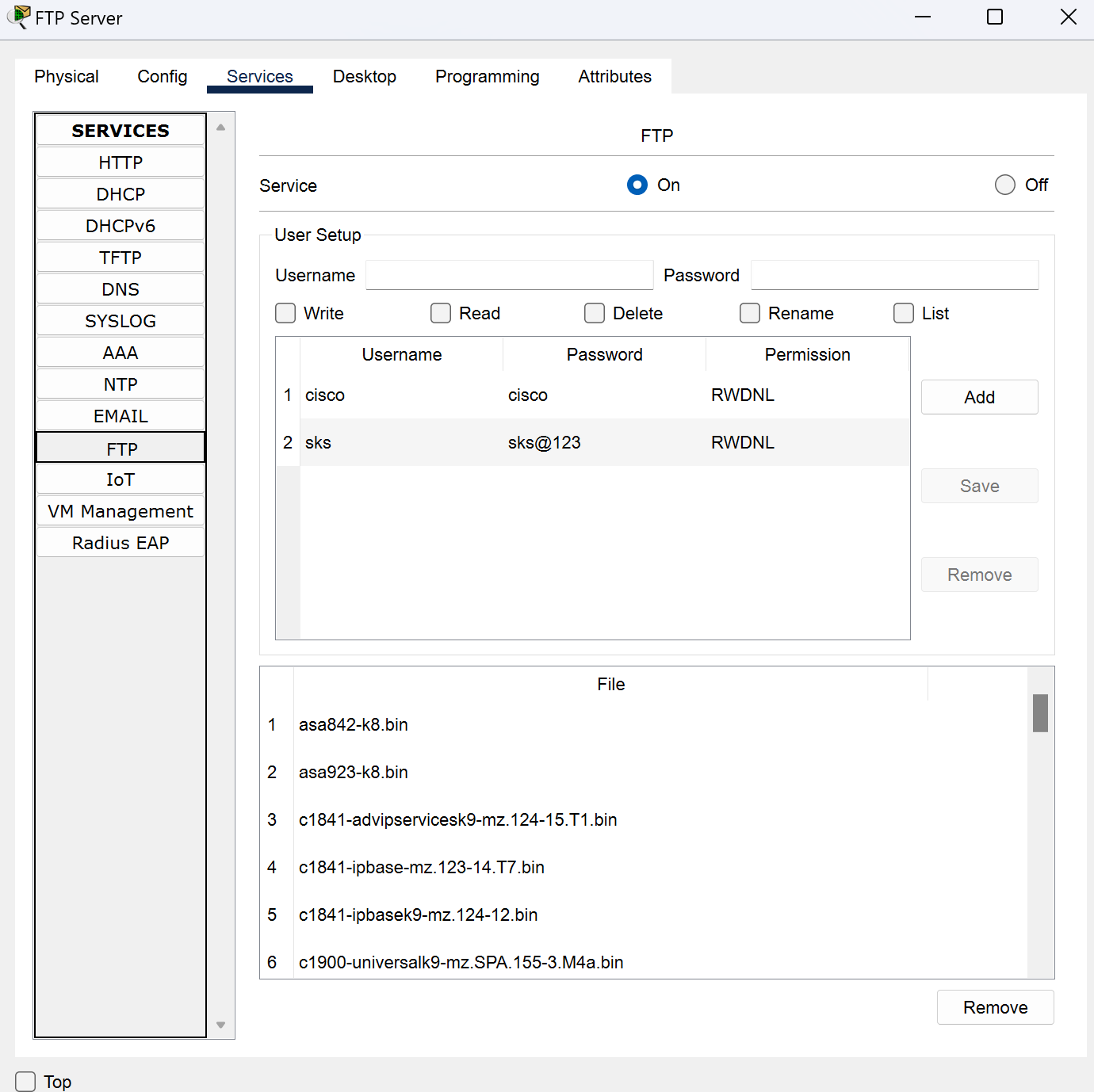


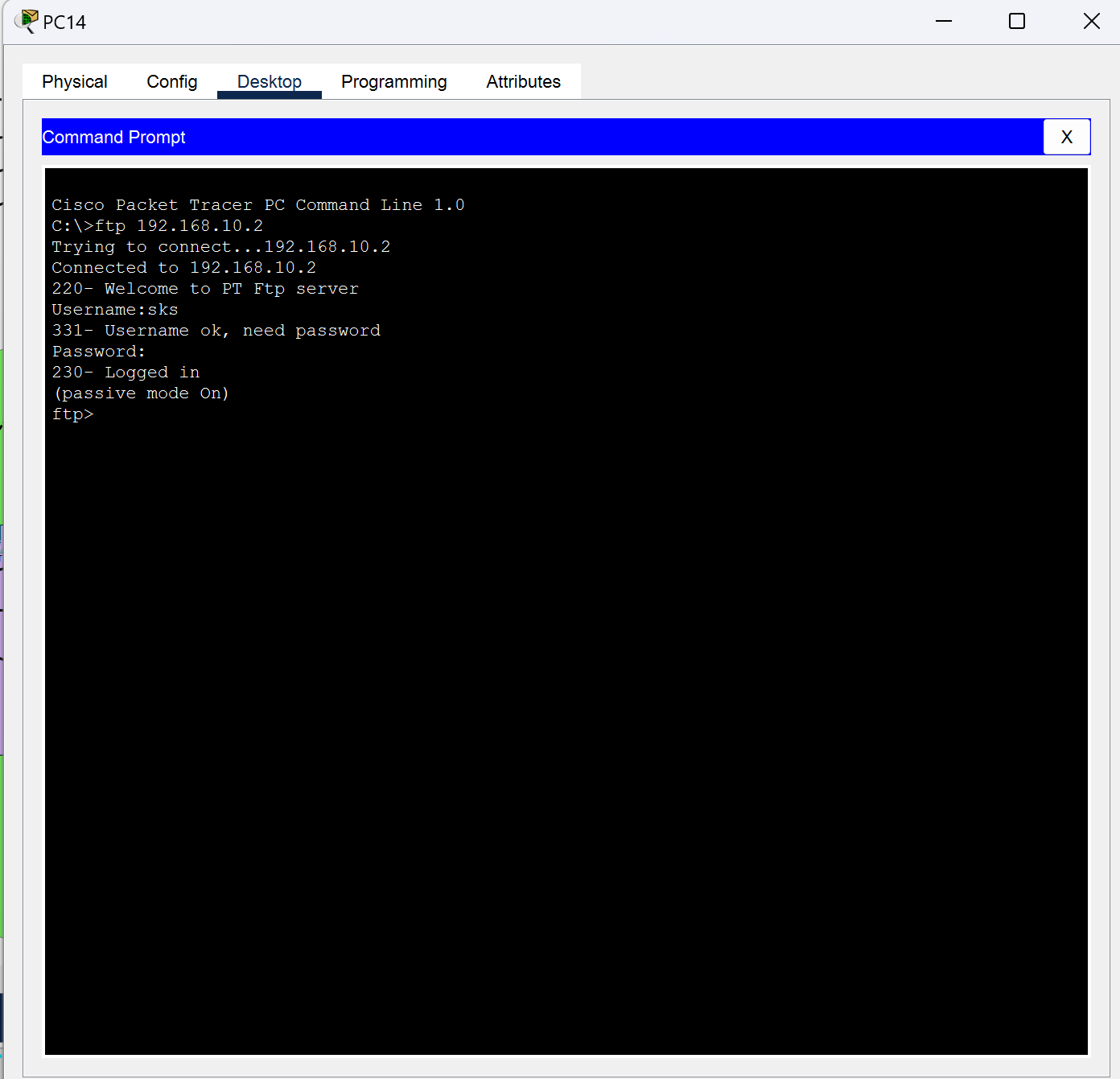
 ↓

Simulation for the TCP and HTTP request (the trace from outside campus to the inside campus)

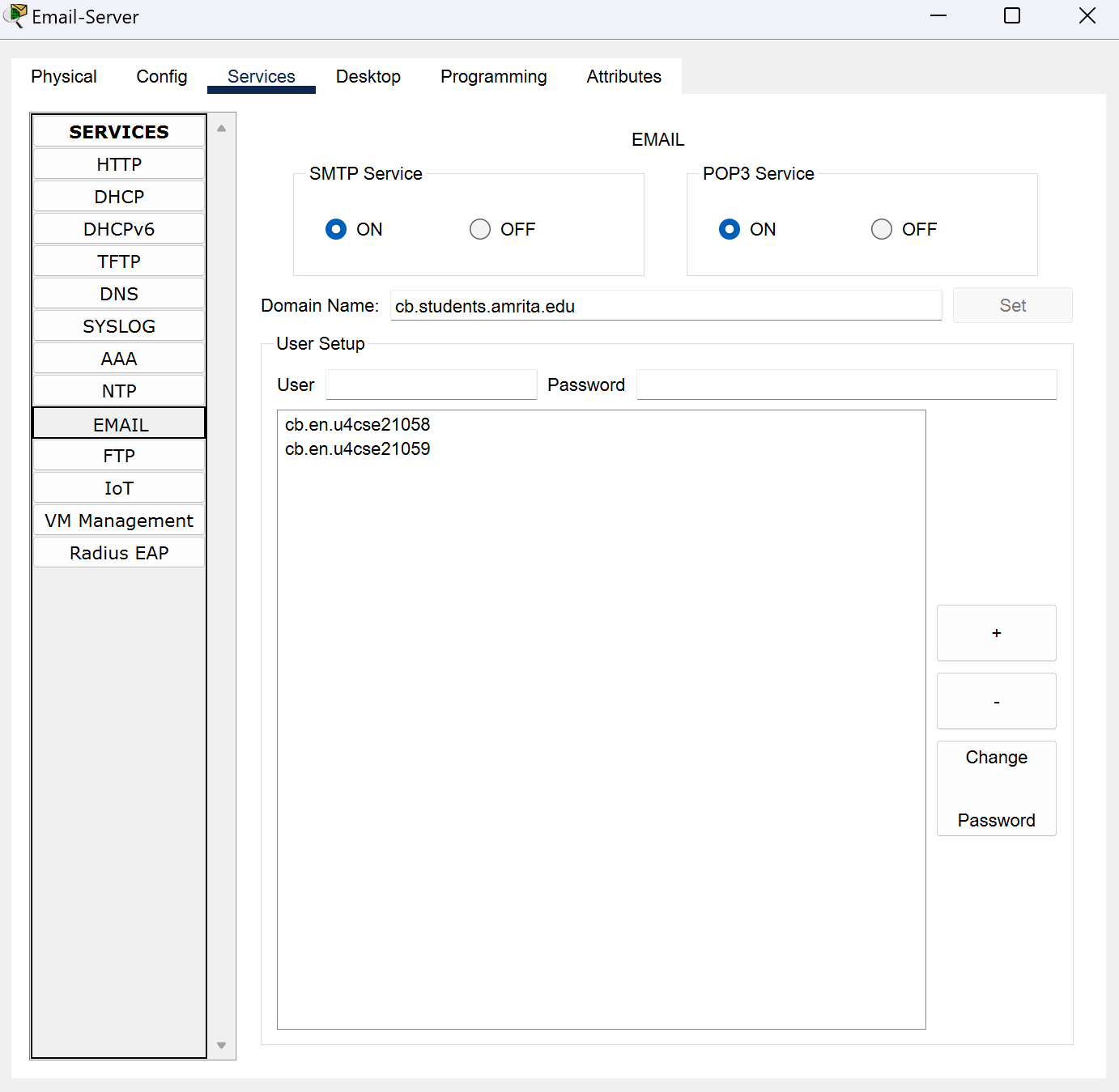


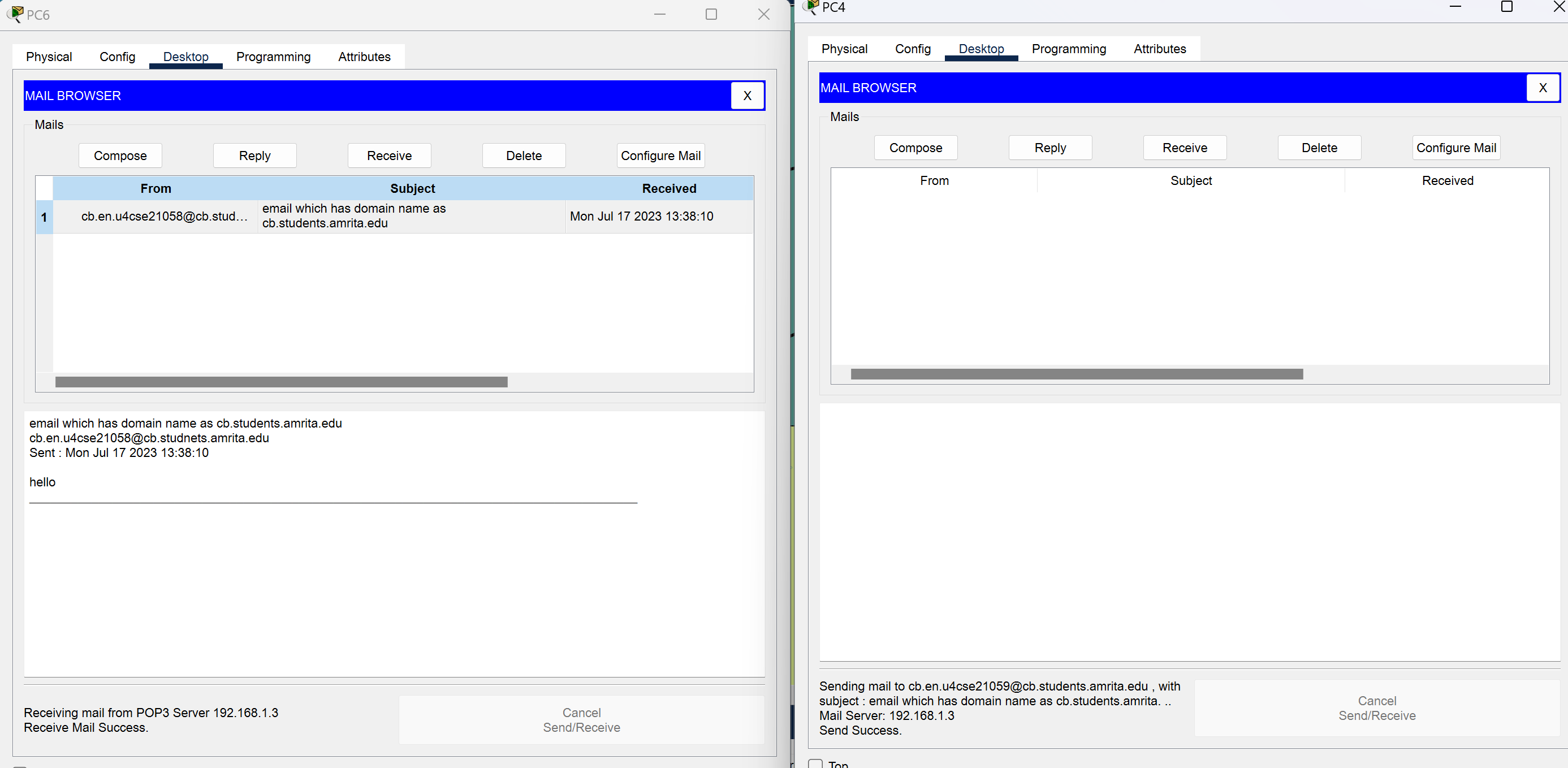
FTP Connection





Email Server (Inside the campus)

 Domain Name: cb.students.amrita.edu



Conclusion

The "Packet Flow Visualizer" project aimed to create a visual representation of packet flow from students' laptops/desktops to external networks outside of the college campus. The project was divided into two key parts: network topology creation and packet flow investigation. During the network topology creation phase, devices were identified using tools like traceroute and consultation with the college network administrator. Cisco Packet Tracer was used to design a network topology, showcasing devices, design, and boundaries. In the packet flow investigation phase, IPv4 addresses were configured on all layer-3 devices, and packet sniffing was performed using Cisco Packet Tracer's built-in sniffer. The collected data served as the foundation for creating a flow diagram, visually illustrating the packet flow from students' devices to external networks. The packet sniffing process provided deeper insight into network communication and data packet behavior, allowing knowledge about various network protocols, including TCP, UDP, ICMP, and HTTP. The flow diagram created during the investigation provided an effective visual representation of complex networking concepts and offered insights into potential network optimizations and troubleshooting. The project provided a practical and hands-on experience in network analysis and visualization, contributing to a better understanding of real-world network scenarios within and beyond the college campus. The combination of network topology creation and packet flow investigation strengthened network management proficiency and problem-solving skills for network-related issues.