

NETWORKING



CISCO VIRTUAL INTERNSHIP PROGRAM 2022

RITHIKA SRI J
CB.EN.U4CSE19025

PART 1 - To create college network topology

A brief outline of what I did

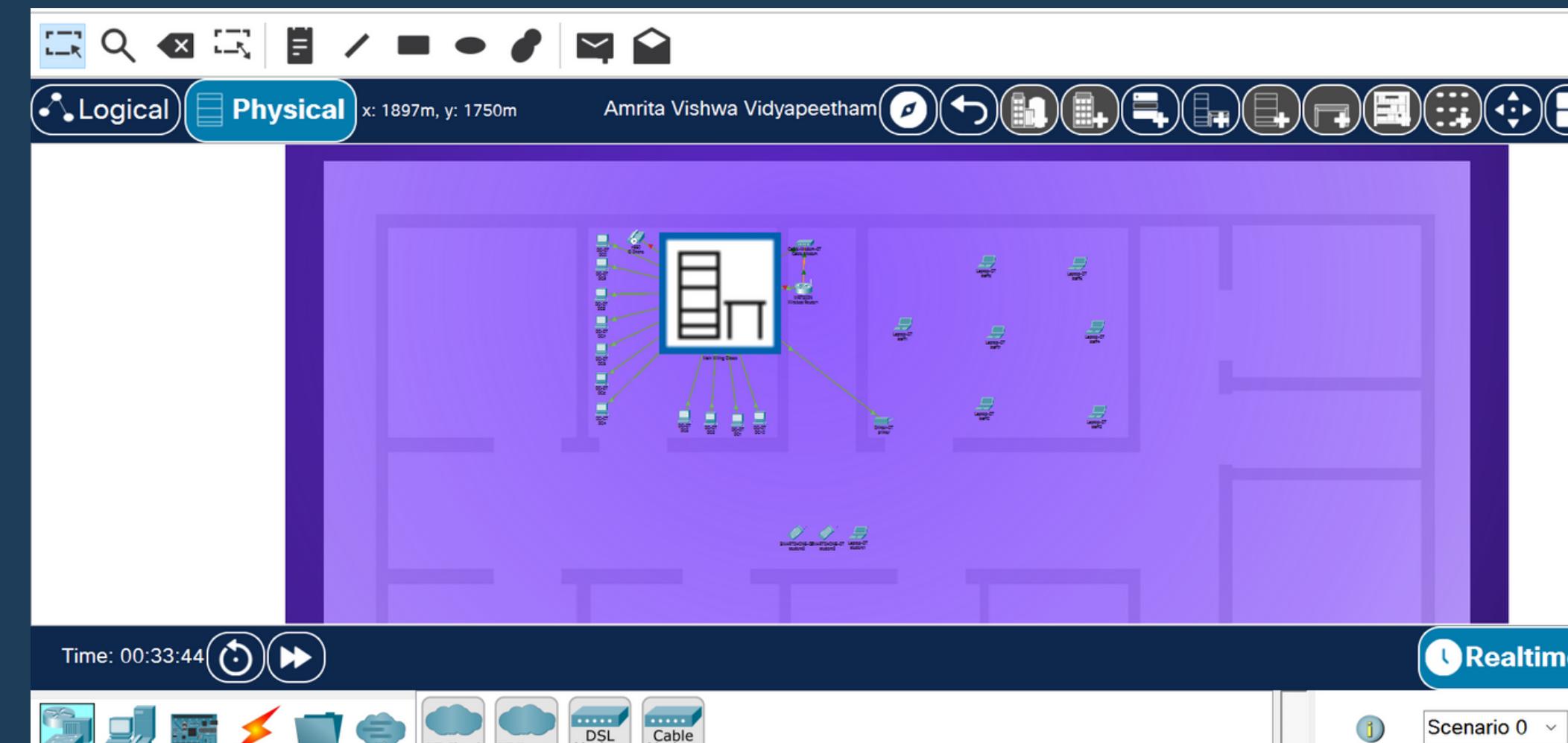
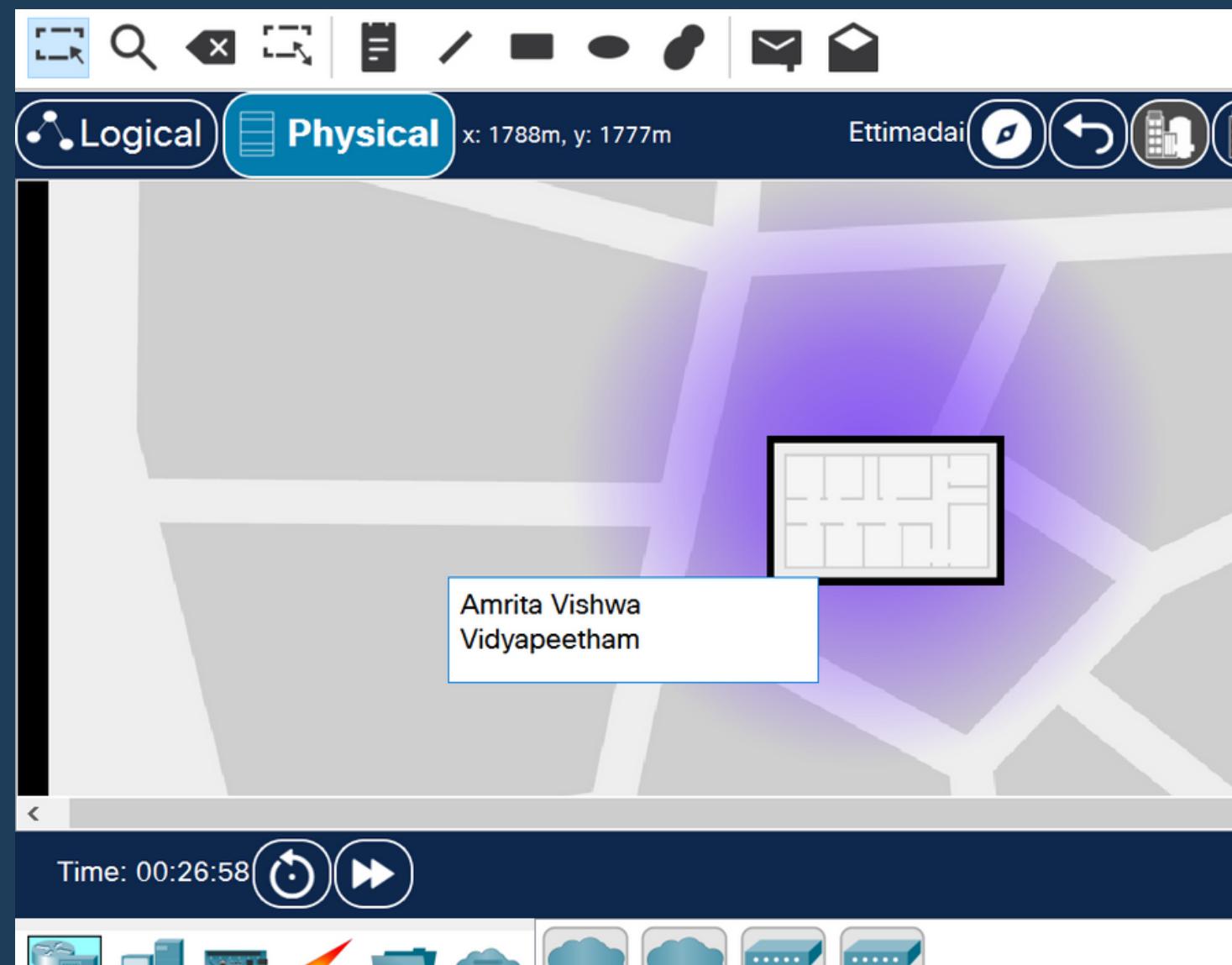


In physical view = Intercity -> Ettimadai -> Amrita Vishwa Vidyapeetham

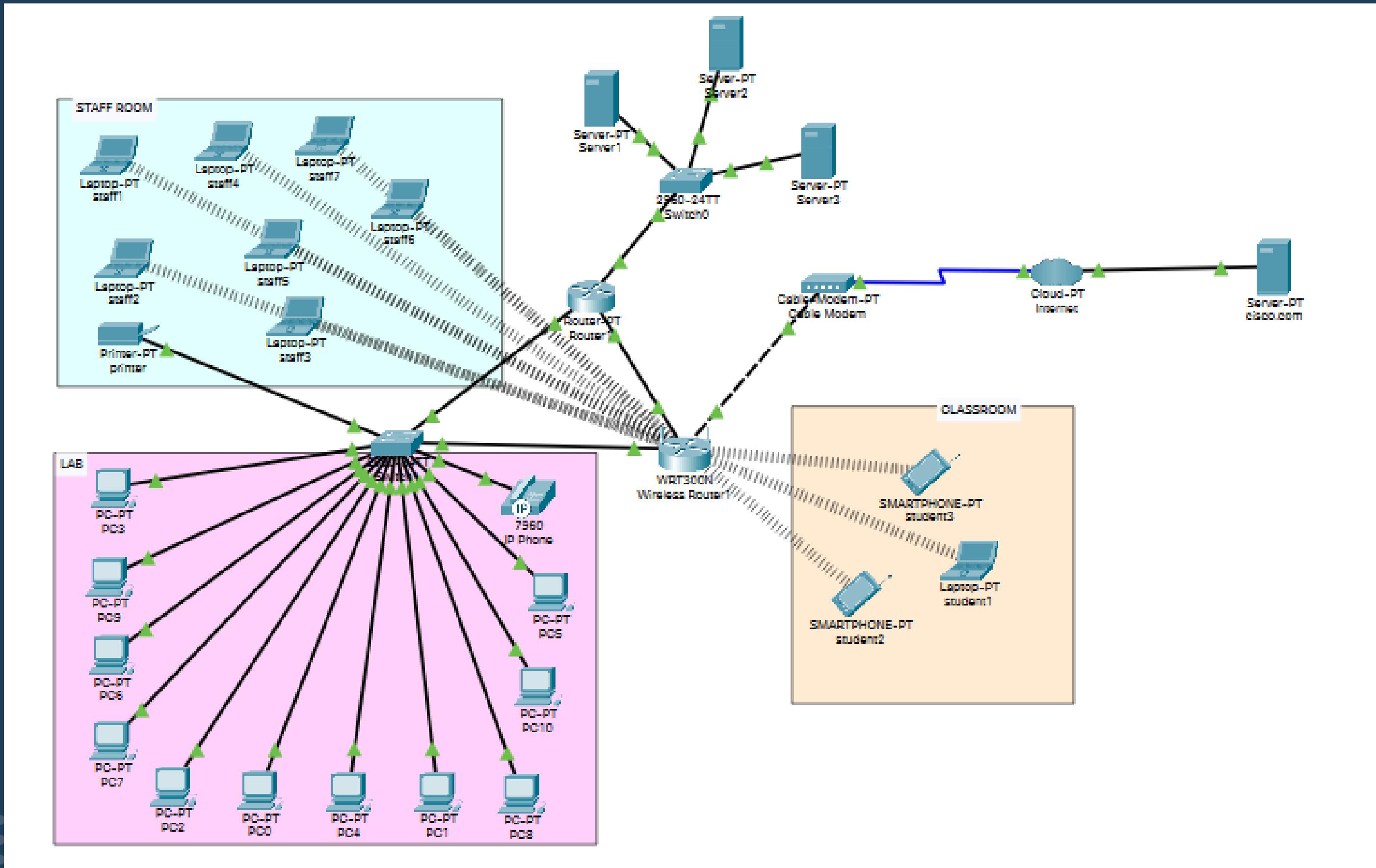
In logical view = 1 staff room, 1 classroom, 1 lab

Networking components = laptops, PCs, personal tablet, IP phone, switch, router(wired+wireless), modem, internet(cloud)

PHYSICAL TOPOLOGY



LOGICAL TOPOLOGY



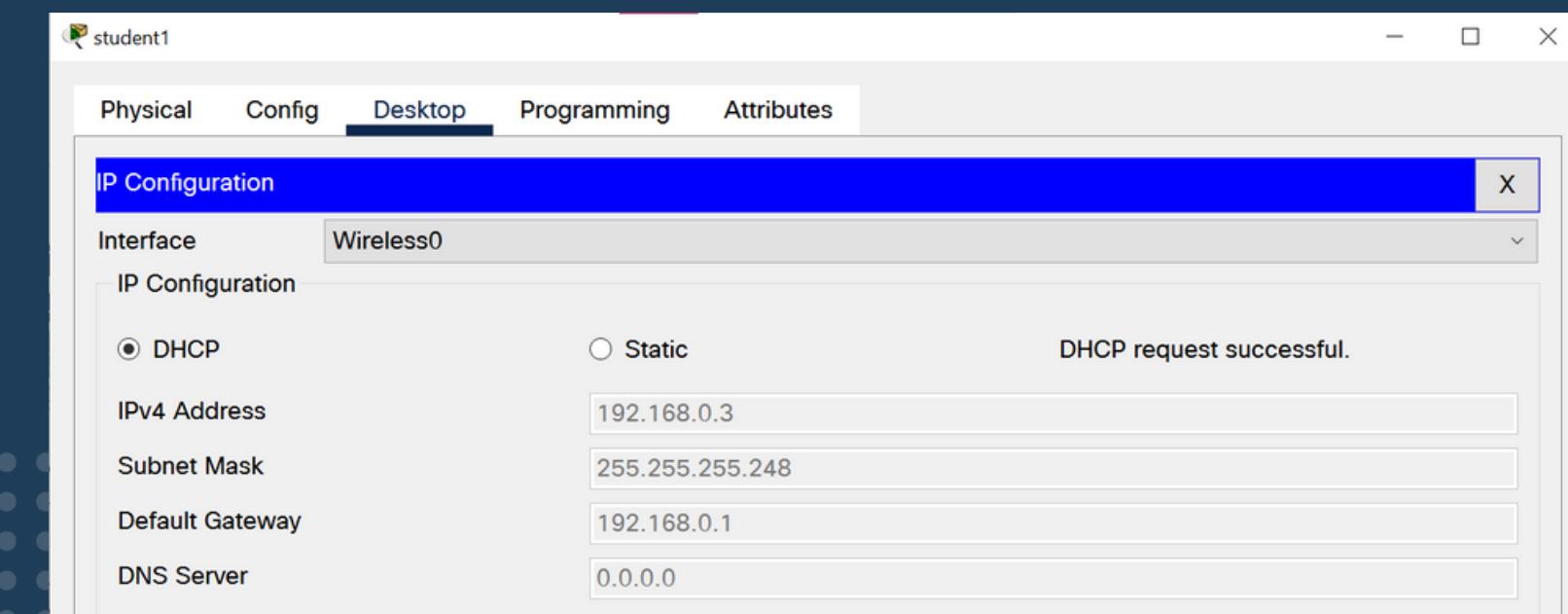
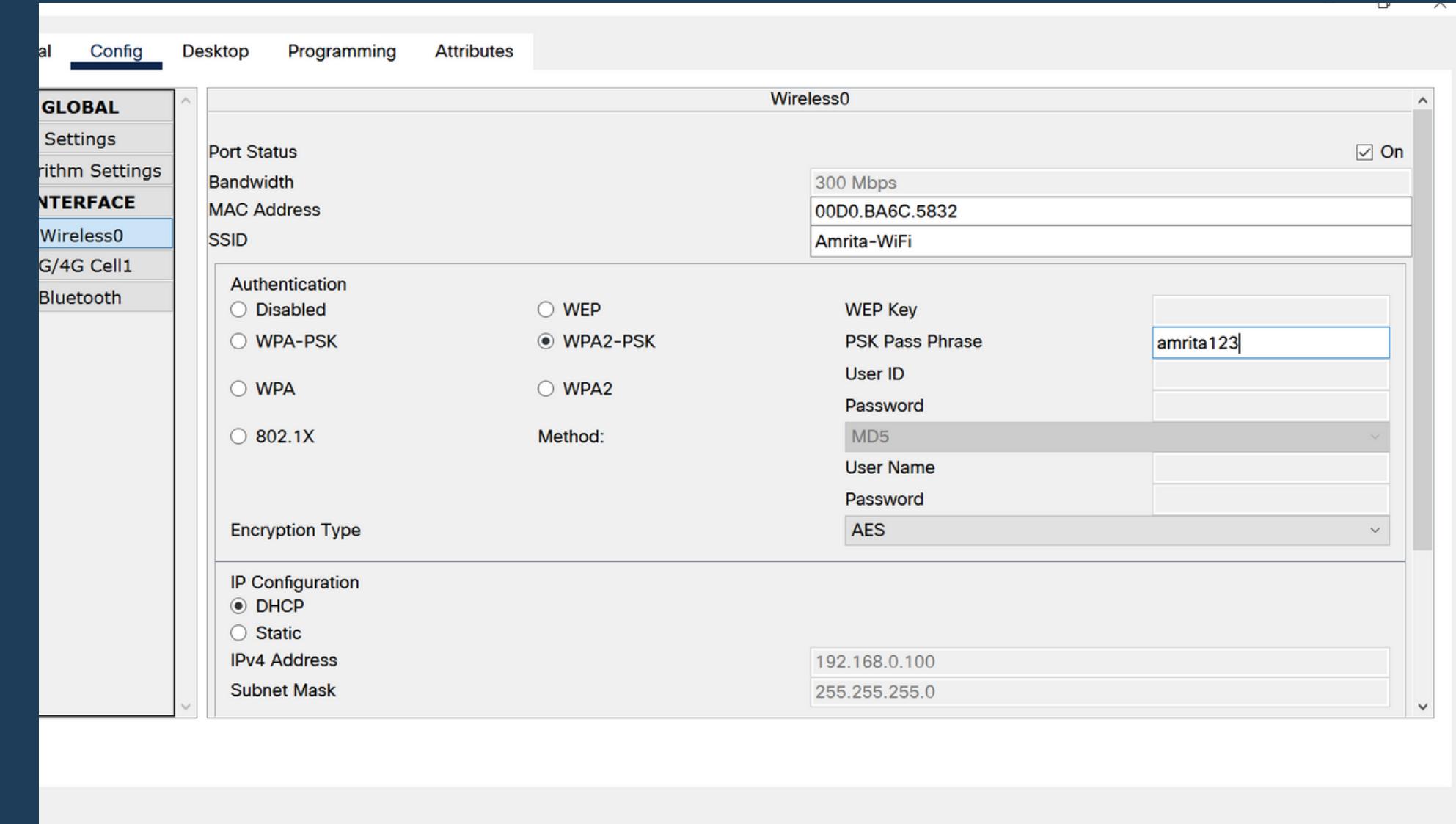
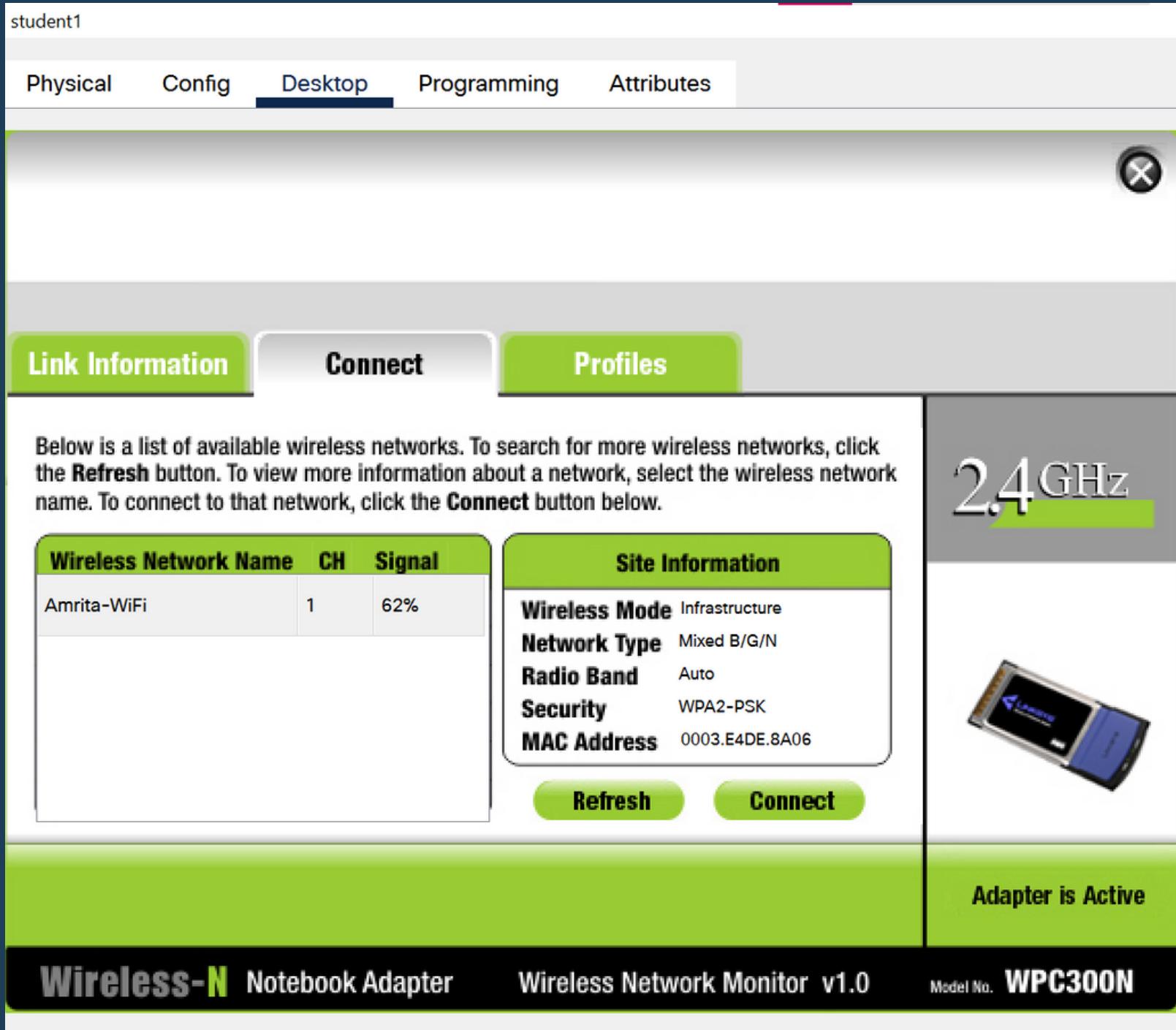
IP ADDRESS, NETWORK, SUBNET AND HOST CONFIGURATION

IP Address:	169.231.0.0
Network Address:	169.231.0.0
Usable Host IP Range:	169.231.0.1 - 169.231.0.62
Broadcast Address:	169.231.0.63
Total Number of Hosts:	64
Number of Usable Hosts:	62
Subnet Mask:	255.255.255.192
Wildcard Mask:	0.0.0.63
Binary Subnet Mask:	1111111.1111111.1111111.11000000
IP Class:	C
CIDR Notation:	/26
IP Type:	Public

IMPLEMENTED 3 SUBNETS.
 1ST SUBNET - STAFFROOM & CLASSROOM
 2ND SUBNET - DATA CENTER (SERVERS)
 3RD SUBNET - LAB

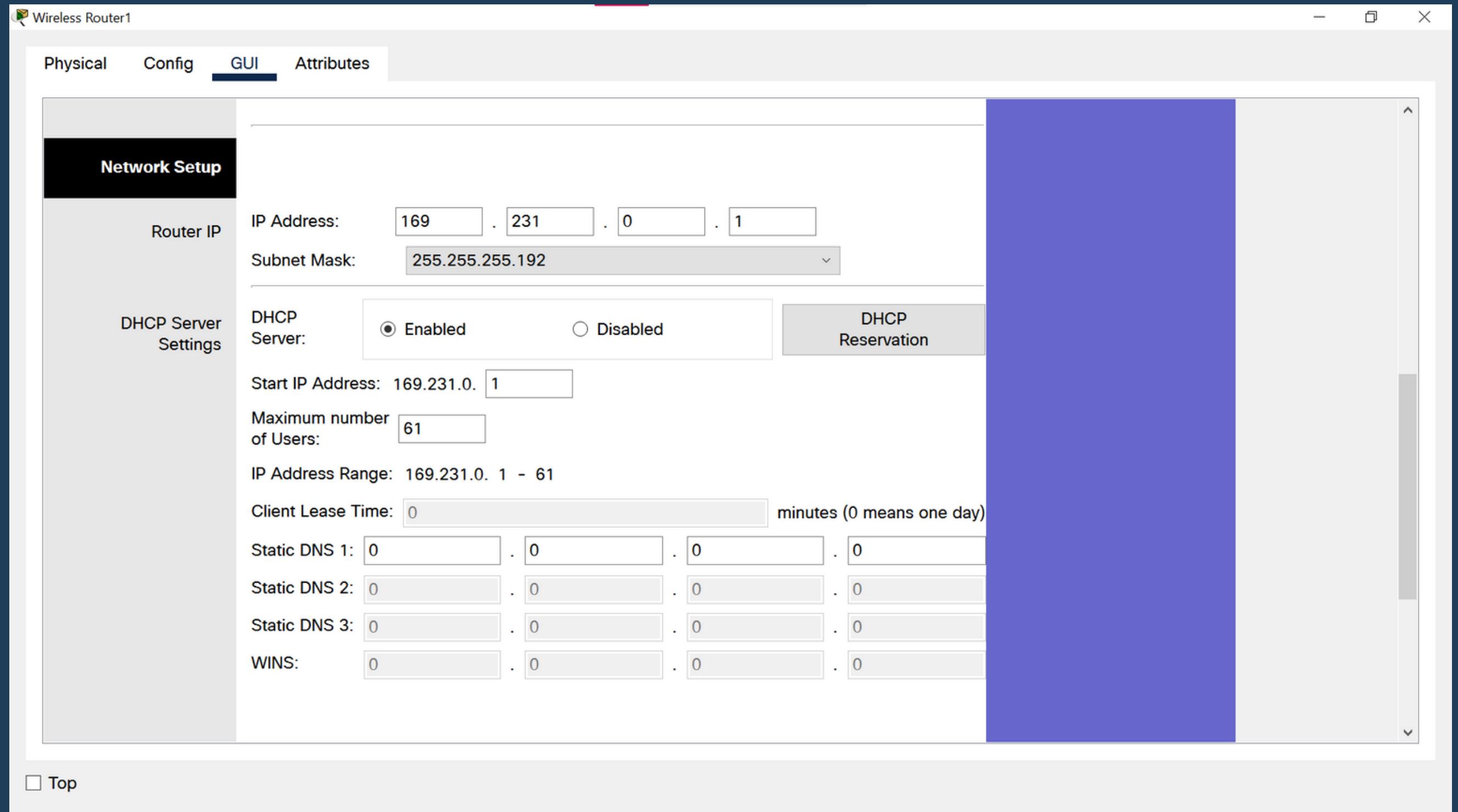
	Network Address	Usable Host Range	Broadcast Address:
	169.231.0.0	169.231.0.1 - 169.231.0.62	169.231.0.63
	169.231.0.64	169.231.0.65 - 169.231.0.126	169.231.0.127
	169.231.0.128	169.231.0.129 - 169.231.0.190	169.231.0.191
	169.231.0.192	169.231.0.193 - 169.231.0.254	169.231.0.255

CONNECTION CONFIGURATION (WIRED & WIRELESS)



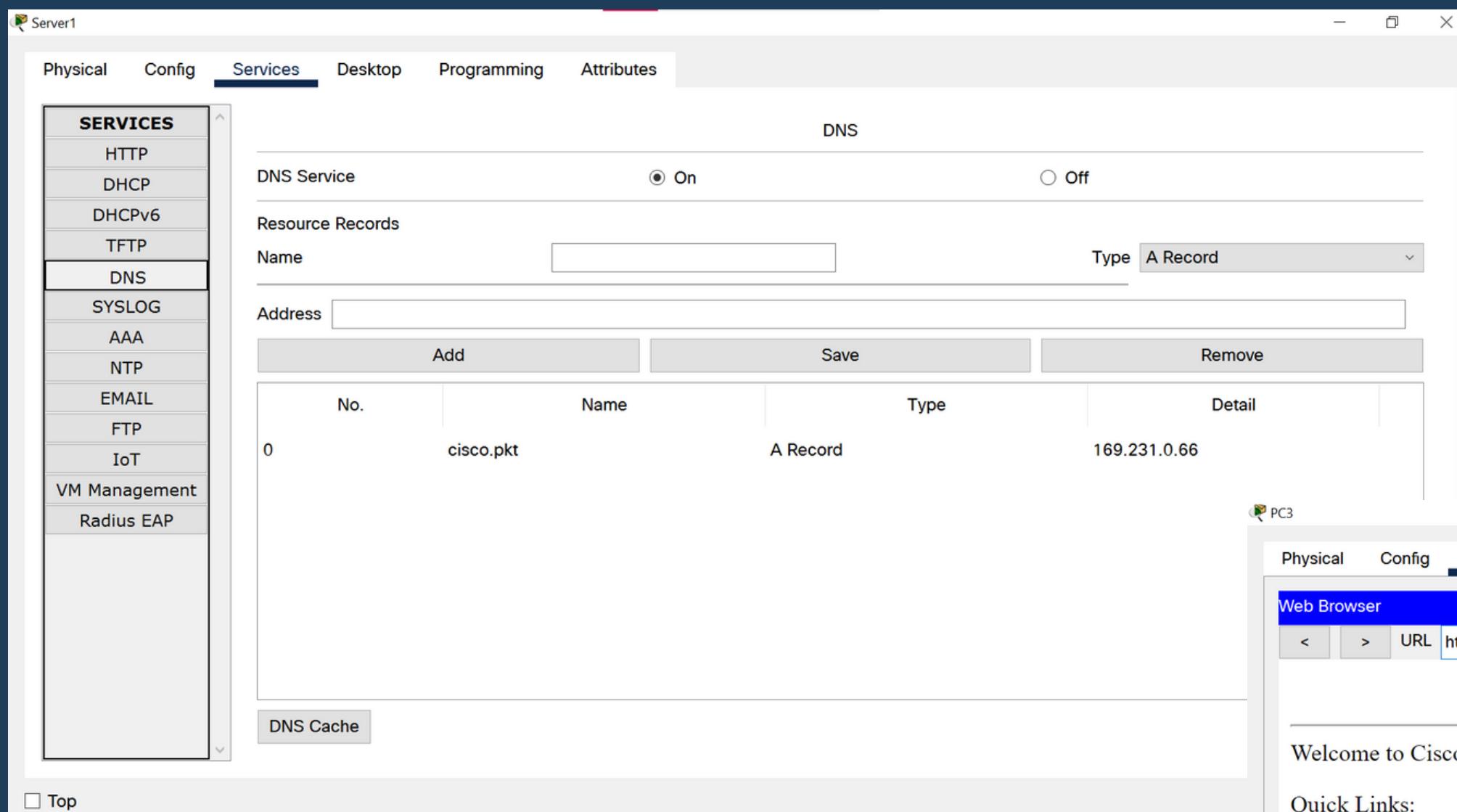
CONNECTION BETWEEN ALL THE SUBNETS
CONFIGURED AND WORKING. THUS
COMMUNICATION BETWEEN ANY TWO END
DEVICES ENABLED.

DHCP SERVICE

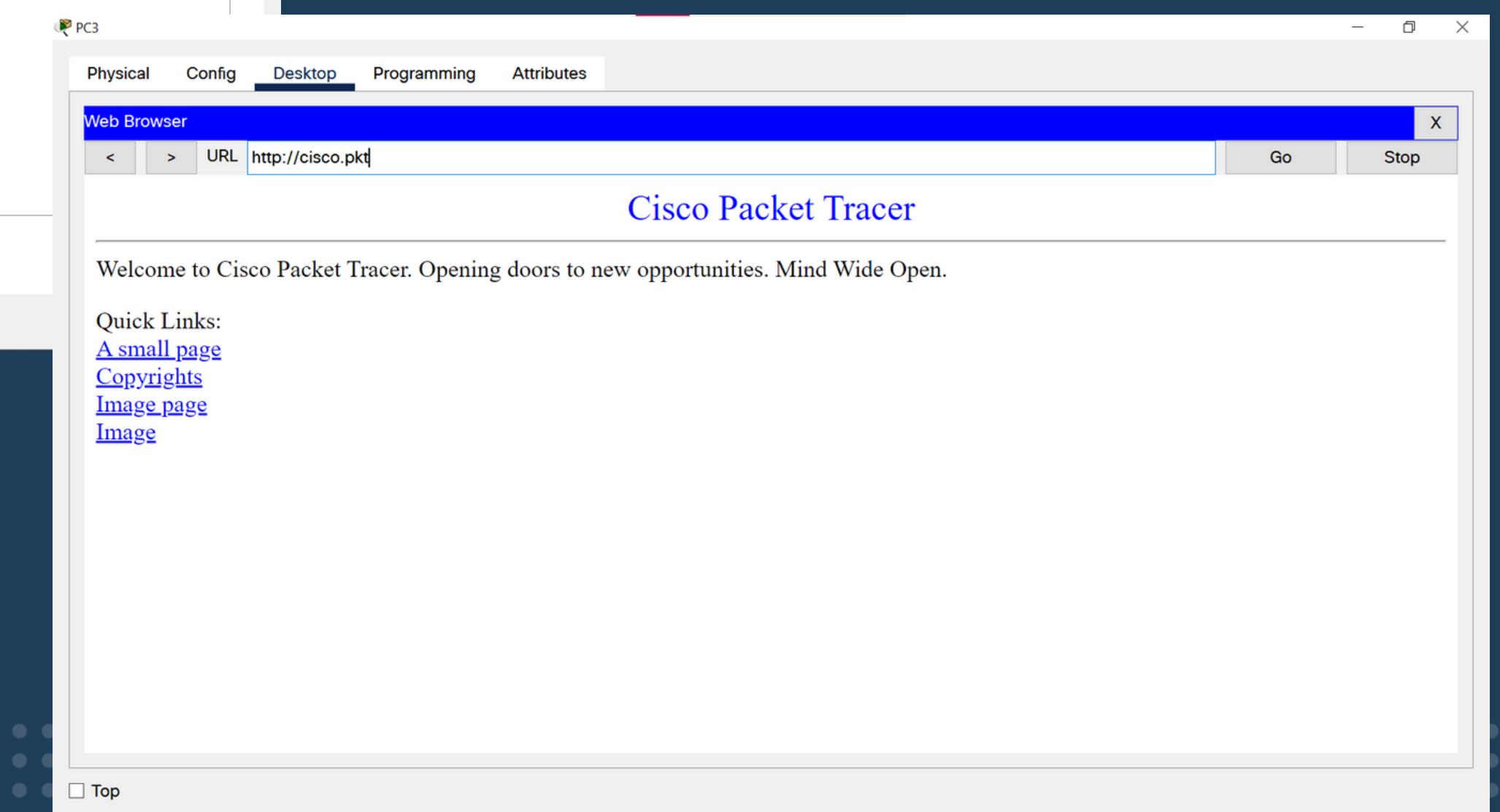


**DHCP SERVICE
CONFIGURED.
WIRELESS END DEVICES
ACQUIRE IP ADDRESS
THROUGH DHCP WHEN
CONNECTED TO THE
WIRELESS ROUTER.**

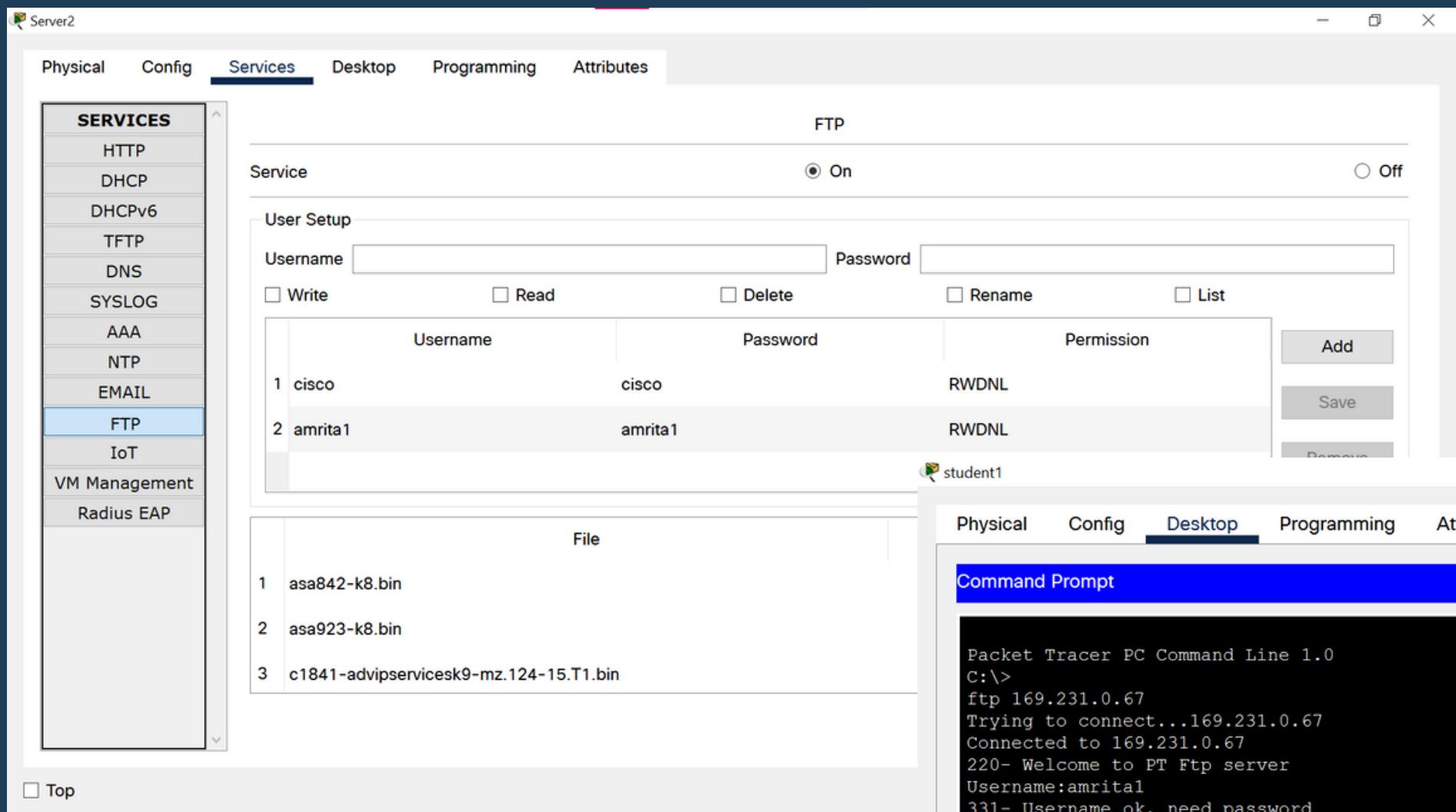
DNS SERVICE



DNS SERVICE CONFIGURED.
REGISTERED THE HOSTNAME AND
ITS CORRESPONDING IP ADDRESS.
THE PAGE IS ACCESSED THROUGH
THE HOSTNAME IS SHOWN IN THE
SCREENSHOT



FTP SERVICE

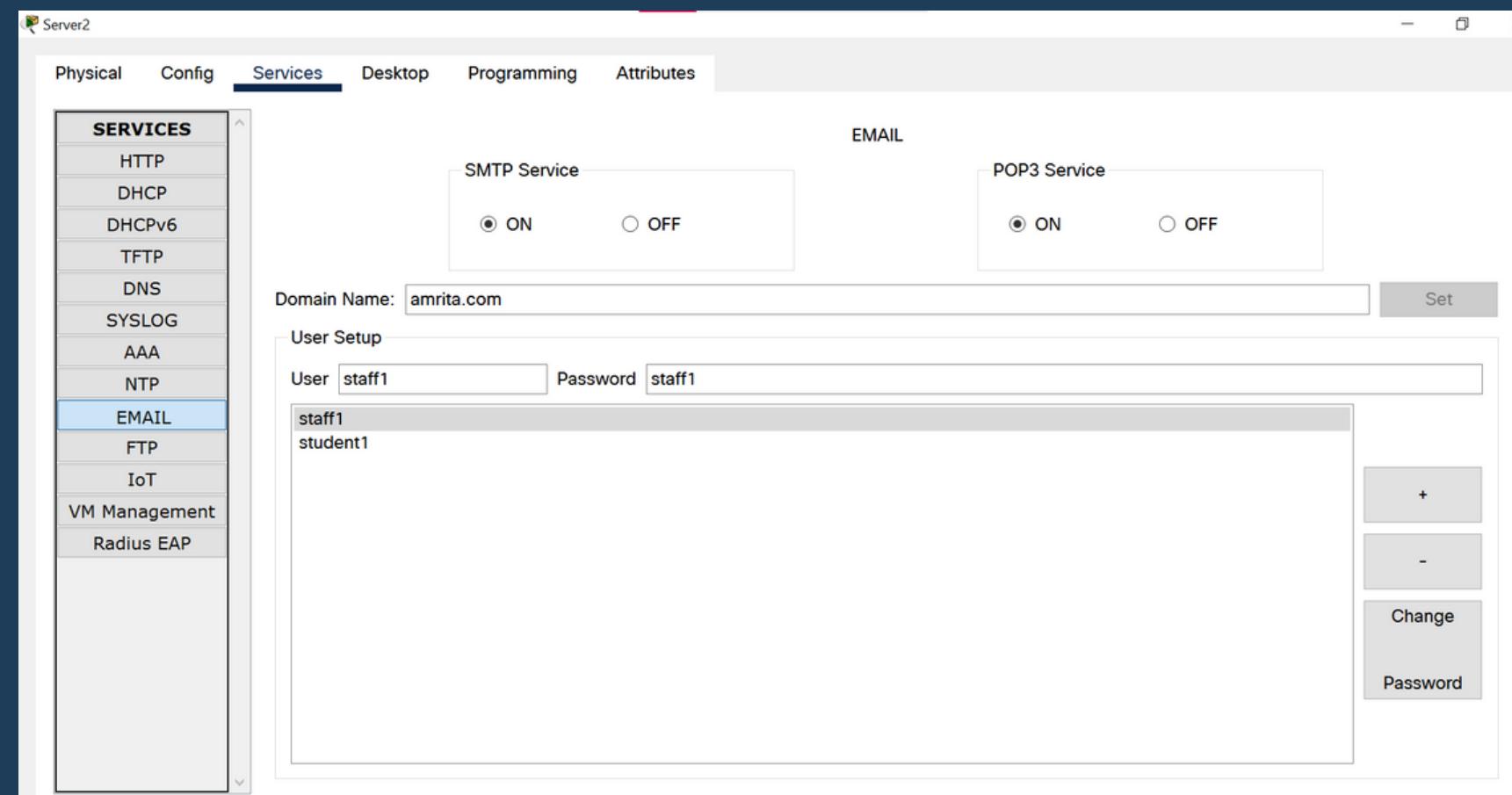


**FTP SERVER CONFIGURED.
CREATED USERNAME AND PASSWORD FOR A
AMRITA USER.
THE AMRITIAN ACCESS THE FILE USING HIS
ACCOUNT IS SHOWN IN THE BELOW
SCREENSHOT.**

The screenshot shows a 'Command Prompt' window with a blue header bar. The terminal session starts with 'Packet Tracer PC Command Line 1.0' and 'C:\>'. The user enters 'ftp 169.231.0.67' and receives a response: 'Trying to connect...169.231.0.67' and 'Connected to 169.231.0.67'. The user logs in with 'Username:amrita1' and '331- Username ok, need password'. They then enter their password 'amrita1'. The server responds with '230- Logged in (passive mode On)'. The user runs the command 'ftp>dir' to list the files in the directory. The output shows the following file list:

File Name	Size
0 : asa842-k8.bin	5571584
1 : asa923-k8.bin	30468096
2 : c1841-advipsericesk9-mz.124-15.T1.bin	33591768
3 : c1841-ipbasek9-mz.123-14.T7.bin	13832032
4 : c1841-ipbasek9-mz.124-12.bin	16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin	33591768
6 : c2600-advipsericesk9-mz.124-15.T1.bin	33591768
7 : c2600-i-mz.122-28.bin	5571584
8 : c2600-ipbasek9-mz.124-8.bin	13169700
9 : c2800nm-advipsericesk9-mz.124-15.T1.bin	50938004
10 : c2800nm-advipsericesk9-mz.151-4.M4.bin	33591768
11 : c2800nm-ipbasek9-mz.123-14.T7.bin	5571584
12 : c2800nm-ipbasek9-mz.124-8.bin	15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin	33591768
14 : c2950-i6q412-mz.121-22.EA4.bin	3058048

EMAIL SERVICE

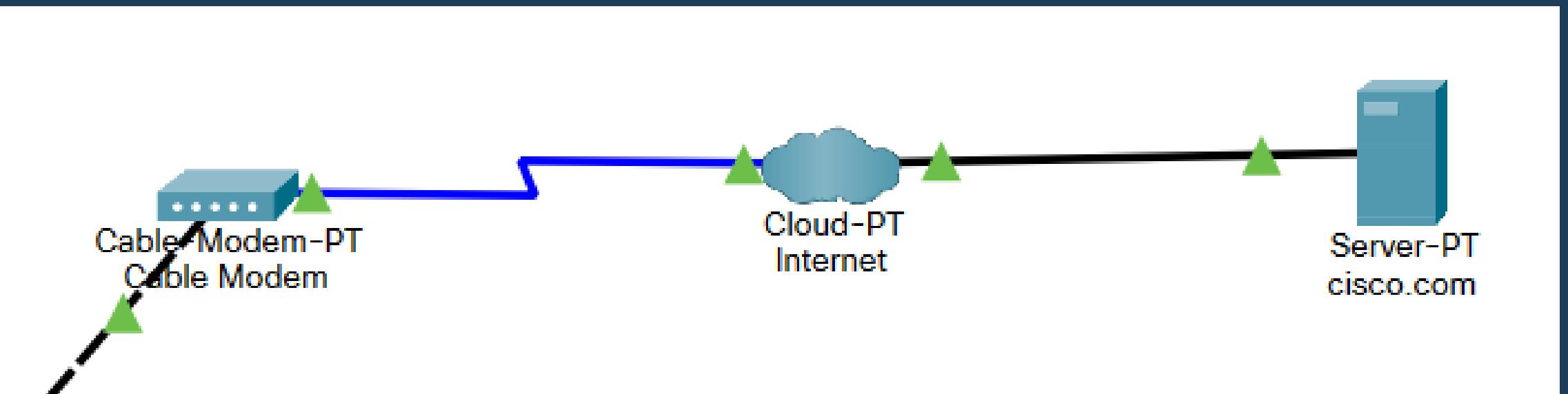


MAIL SERVER CONFIGURED.
CREATED DOMAIN AND AN ACCOUNT FOR A
STAFF AND A STUDENT.
COMMUNICATION THROUGH MAIL BETWEEN A
STAFF AND A STUDENT.
SCREENSHOT SHOWS THE INBOX OF BOTH.

The top screenshot shows the 'MAIL BROWSER' window for 'staff1'. It displays an incoming email from 'student1@amrita.com' with the subject 'RE: meeting - reg'. The message body contains 'Yes,ma'am'. Below the message, the original email header is shown: 'Subject : meeting - reg' and 'From : staff1@amrita.com'. The bottom screenshot shows the 'MAIL BROWSER' window for 'student1'. It displays an outgoing email from 'staff1@amrita.com' with the subject 'meeting - reg'. The message body contains 'Today meeting scheduled @3pm.'

CONNECTING TO EXTERNAL INTERNET

STAFF6 CONNECTED
TO EXTERNAL
SERVER CISCO.COM
SUCCESSFULLY.



staff6

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ipconfig /release
IP Address.....: 0.0.0.0
Subnet Mask....: 0.0.0.0
Default Gateway.: 0.0.0.0
DNS Server.....: 0.0.0.0

C:\>ipconfig /renew
IP Address.....: 208.67.220.1
Subnet Mask....: 255.255.255.0
Default Gateway.: 0.0.0.0
DNS Server.....: 208.67.220.220

C:\>ping cisco.com
Pinging 208.67.220.220 with 32 bytes of data:
Reply from 208.67.220.220: bytes=32 time=43ms TTL=128
Reply from 208.67.220.220: bytes=32 time=6ms TTL=128
Reply from 208.67.220.220: bytes=32 time=11ms TTL=128
Reply from 208.67.220.220: bytes=32 time=21ms TTL=128

Ping statistics for 208.67.220.220:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 43ms, Average = 20ms

C:\>
```

Top

Display Name

Gateway/DNS IPv4

DHCP

Static

Default Gateway

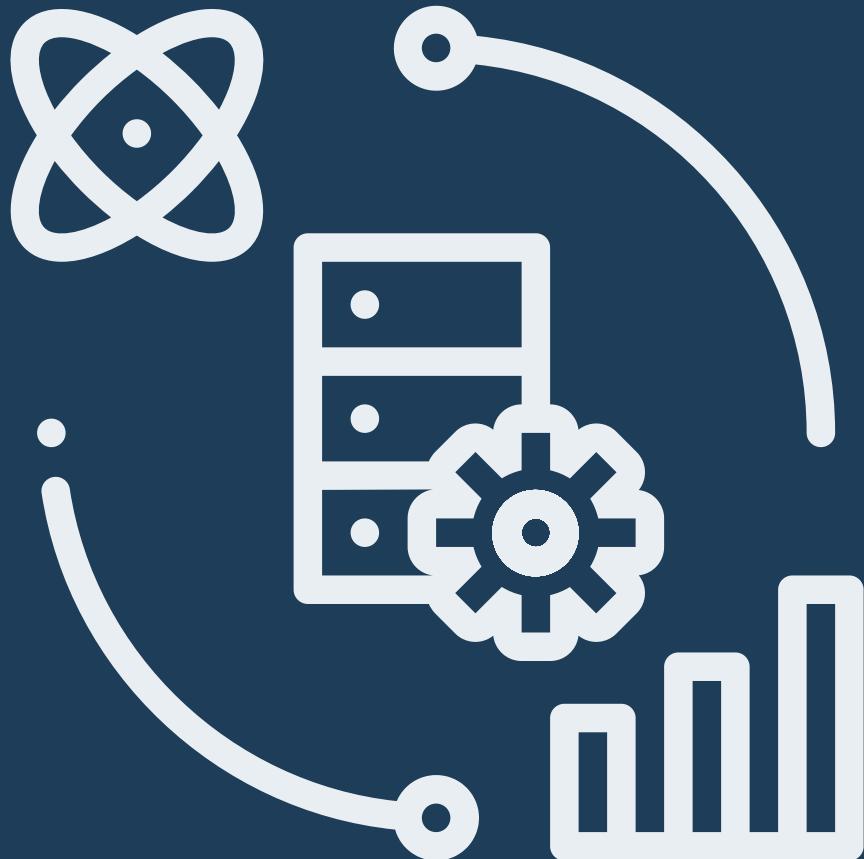
DNS Server

PART 2 - To investigate packet flow

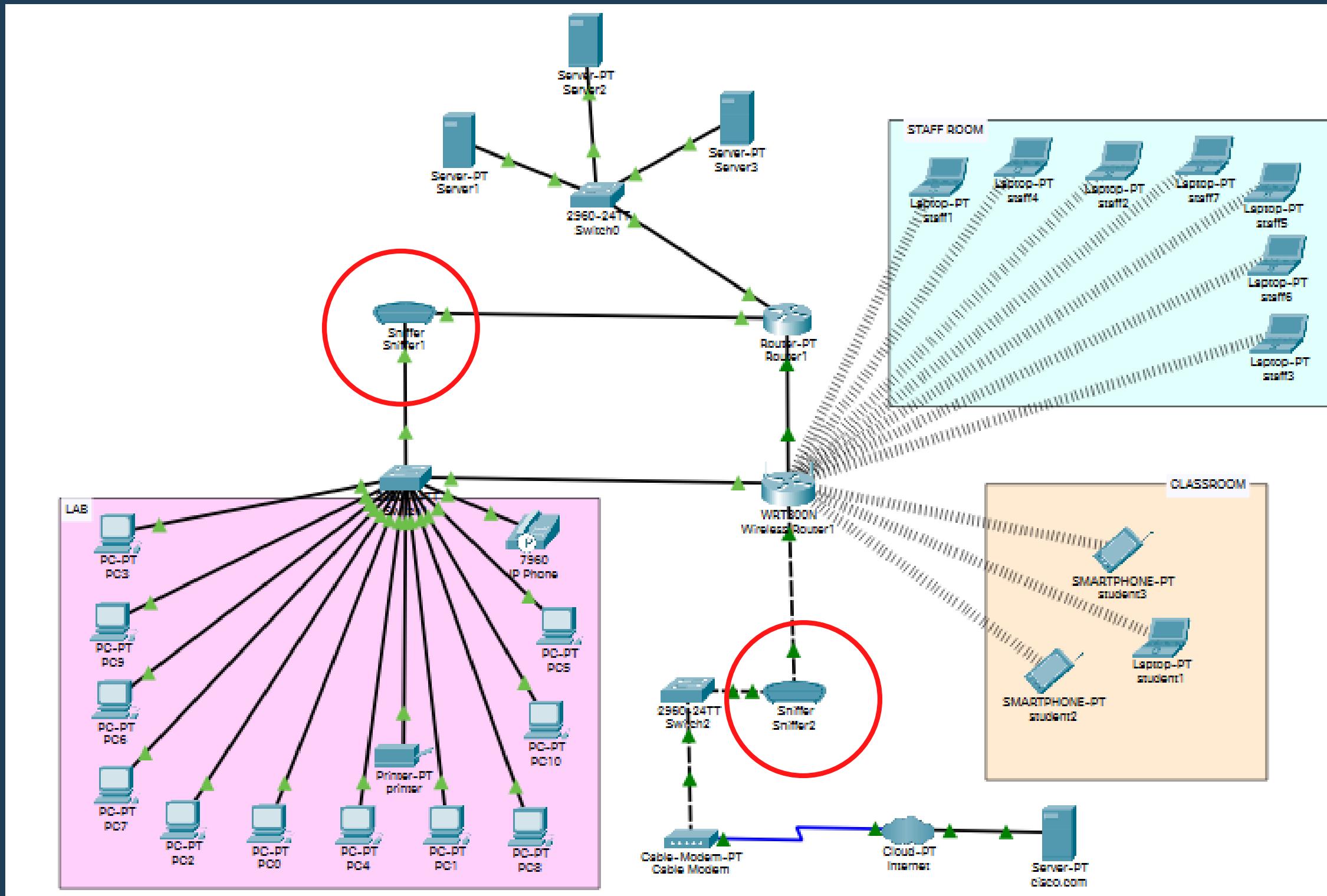
A BRIEF OUTLINE OF WHAT I DID

INTERNAL NETWORK - SNIFFING PACKET FLOW FROM PCS
FROM LAB TO SMARTPHONE IN CLASSROOM.

EXTERNAL NETWORK - SNIFFER PACKET FLOW FROM
EXTERNAL NETWORK SERVER TO INTERNAL END
SYSTEMS,



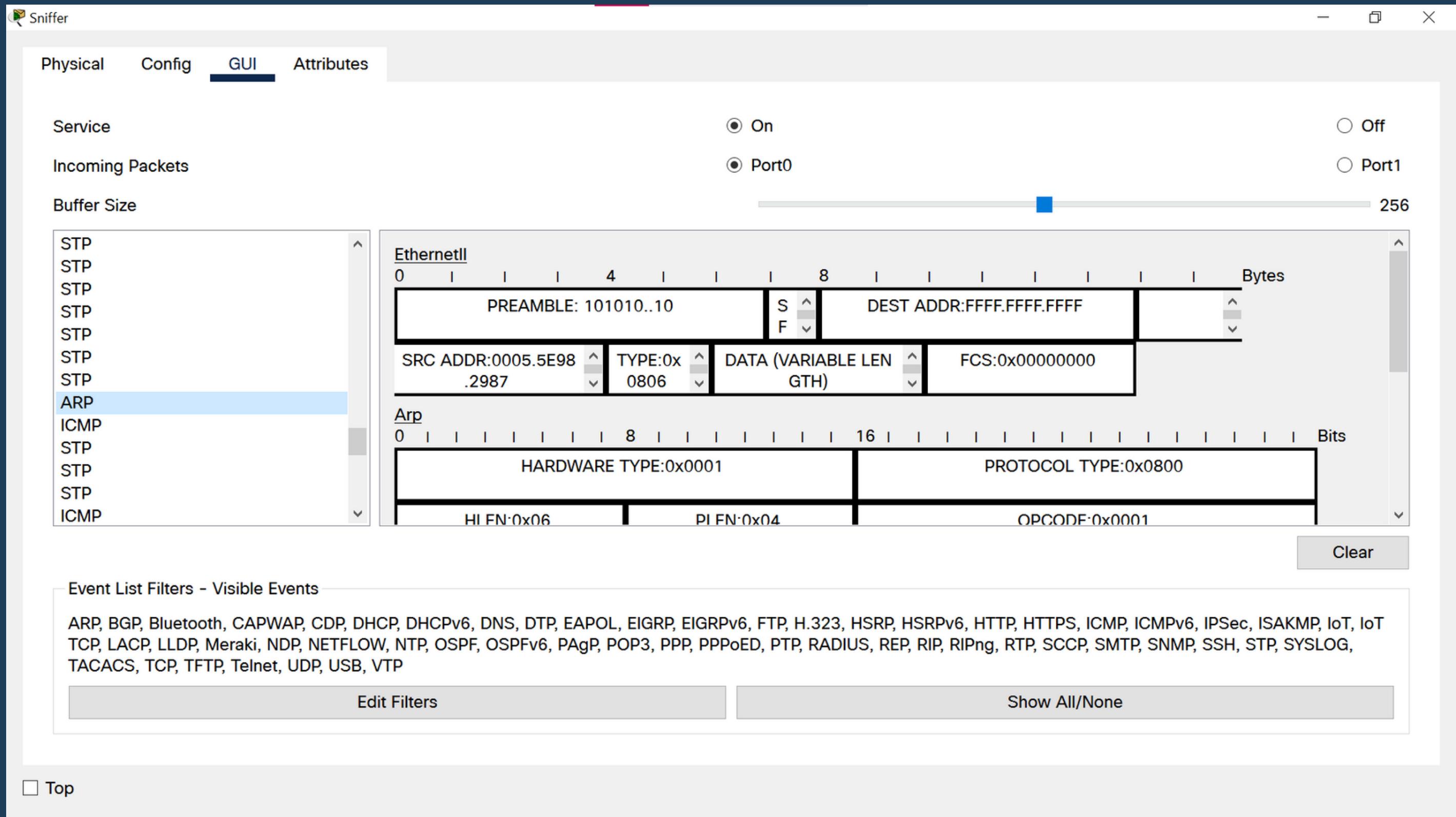
INSTALLATION OF SNIFFERS



SNIFFER1 INSTALLED BETWEEN THE LAB SWITCH AND ROUTER TO CAPTURE PACKETS FLOWING THROUGH THEM (INTERNAL NETWORK).

SNIFFER2 INSTALLED BETWEEN THE SWITCH AND ROUTER TO CAPTURE PACKETS FLOWING THROUGH THEM (EXTERNAL NETWORK).

SNIFFING - ARP (WITHIN INTERNAL NETWORK)



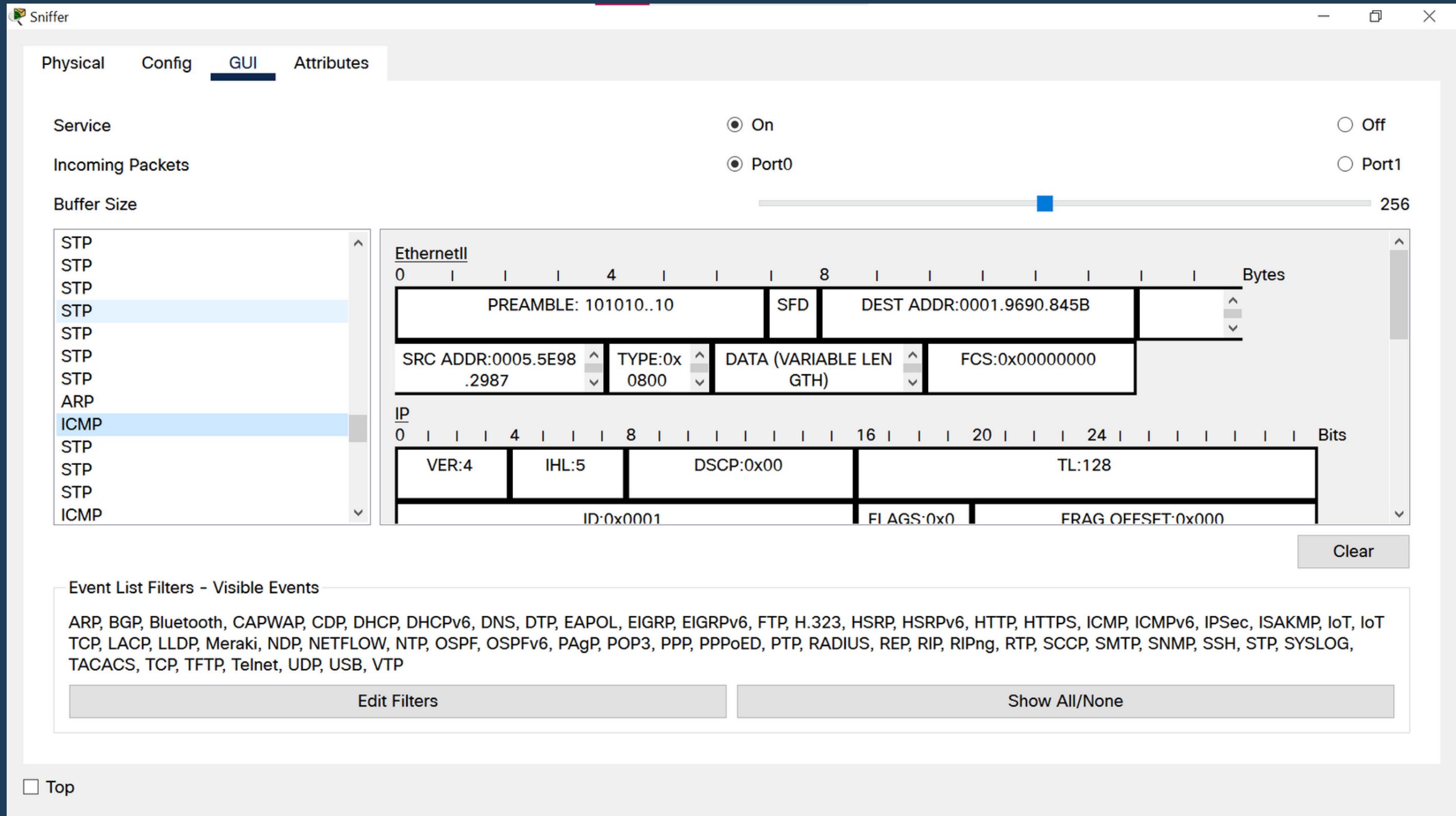
ARP PACKET

DEST MAC ADDR :
BROADCAST

SRC MAC ADDR :
PC2 (FROM LAB)

ARP - TO FIND THE MAC
ADDR WHEN THE
DESTINATION IP
ADDRESS IS KNOWN.

SNIFFING- ICMP (WITHIN INTERNAL NETWORK)



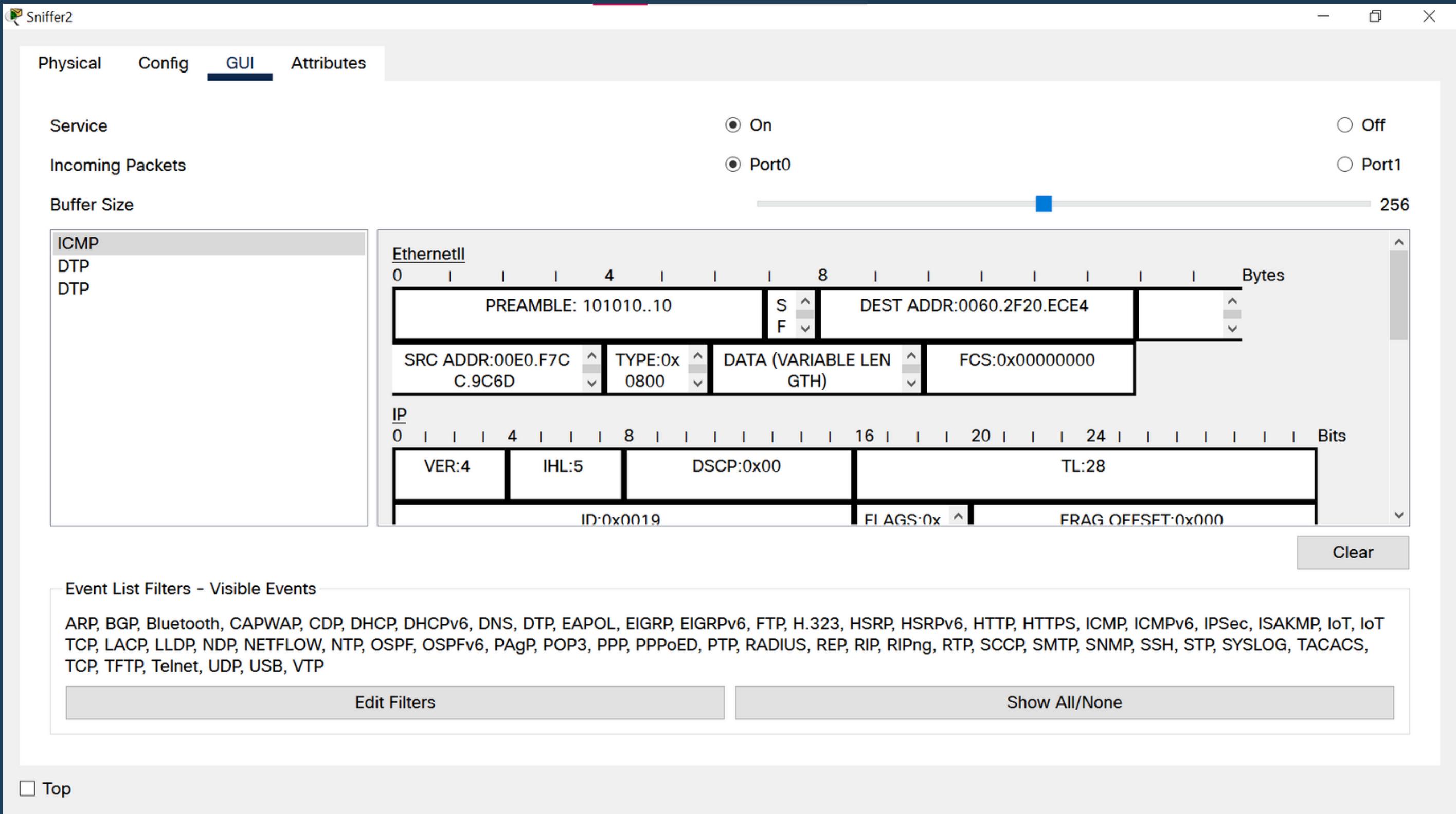
ICMP PACKET

DEST MAC ADDR :
ROUTER1

SRC MAC ADDR:
PC2 FROM LAB

SNIFFER CAPTURES
THE INCOMING
PACKET FROM PC2 TO
ROUTER1

SNIFFING- ICMP(FROM EXTERNAL NETWORK)



ICMP PACKET

DEST MAC ADDR :
STAFF5

SRC MAC ADDR:
CISCO.COM SERVER
FROM EXTERNAL
NETWORK

SNIFFER CAPTURES
THE INCOMING
PACKET FROM THE
EXTERNAL NETWORK.

PACKET FLOW

