DOKUZ EYLUL UNIVERSITY

ENGINEERING FACULTY

DEPARTMENT OF COMPUTER ENGINEERING

METROPOLITAN AREA NETWORK SIMULATION PROJECT

by

Ahmet Fevzi BALABAN 2015510016

Doğukan Berk ÖZER 2015510087

Kemalcan ŞİMŞEK 2013510093

8.05.2020

İZMİR

CHAPTER ONE

INTRODUCTION

1.1. Project Definition and Problem Formulation

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network. It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

1.2. The Purpose and Motivation of the Project

MAN allows sending and receiving of local emails in a cheaper and more quicker manner.Due to its use of fiber optics, users can transfer databases and files quickly, as the speed of the network has the capacity of reaching 1000Mbps. This is why telephone companies across the world utilize the structure of MAN and use fiber optics to transfer data in an unprecedented speed.MAN has the feature of allowing network administrators to manage the entire network centrally leading to much more effective and efficient network management. Speaking of effective network management, it is always highly recommended to essential network training beforehand.A MAN is also considered a more secure network in comparison to a WAN[2].

1.3. Term Definitions

Network : This general term refers to all the components involved in getting computers and other types of hardware to talk to each other.

Server : Also called "file server" and "network server" this term refers to the "nerve center" of your network. It typically needs to be much more high-powered than a regular desktop workstation. The server is home to hardware that is networked (allows more than one person to use it simultaneously). All of your data will typically be stored on this machine.

Workstation : This refers to each person's computer. Your front and back office staff computers and the machines in the examination room will be workstations on the network.

Wireless : This refers to a type of network that broadcasts an access signal to the workstations. This allows for transporting laptops and tablet PCs from room to room while maintaining a network connection continuously. A wireless network also presents some additional security requirements.

Ethernet : This is the backbone of our network. It consists of the cabling and is typically able to transfer data at a rate of 100mb/s. What is not shown here are the hubs and switches that are used to connect computers and other devices together.

Router : This is your network's "air traffic controller." It routes all the data on your network to where it is supposed to go. It also assigns unique network addresses to all the computers (IP addresses). Routers can also hide the computer and devices that connect to it from the outside world. To people on the Internet, your entire network looks like one computer (one IP address). This adds another layer of protection to the computers on your network. A router may contain a VPN server and/or a firewall. Read more about hubs, switches and routers.

Architecture: Network architecture is the design of a computer network. It can also be defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.

Switch: Switch is a high-speed device that receives incoming data packets and redirects them to their destination.

Server: Servers manage access to a centralized resource or service in a network.

Packet: Packet is a formatted unit of data carried by a packet-switched network.

Channel: Channel refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel.

Protocol: Protocols define rules of communication between network devices.

DNS : DNS stands for domain name system. It is an application layer protocol used to provide a human-friendly naming mechanism for internet resources. It is what ties a domain name to an IP address and allows you to access sites by name in your browser.

IP : The IP protocol is one of the fundamental protocols that allow the internet to work. IP addresses are unique 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[3].

CHAPTER TWO

METHOD AND SIMULATION

2.1. Simulation and Modelling Concepts

The network requirements, physical and logical needs were calculated. The alternate approach, known as bottom-up, is more commonly employed, but is far from optimal. They have a tendency to begin the design process at this level, leaving applications and services as an afterthought to be considered later. In most cases, taking a bottom-up approach tends to require a less thorough initial analysis, and is easier to implement as a quick fix.

The main approach to the modelling is building workstations (some facilities include the wireless workstation users and to provide a successful connection wireless router were used and their configurations were adjusted) as needed for facilities and connections between each of them. Furthermore, we could call it this method as divide and conquer. It makes the process much easier than the thought.

After building workstations, the IP`s are assigned for each workstation. In deeply, first campus is located on network. Network devices connections between workstations and network devices are analysed. In addition to analyse process, facilities have more than one network devices and they must be connected logically and physically to workstations. Network devices were configured.

In order to connect workstations to the each other to provide essential connection, the physical cable is chosen as automatically by the packet tracer simulation software. In this case, workstations are connected with straight copper cable to the switches.

A facilities which are located in the same campuses are connected each other with a main switch over a fast ethernet port. Router has been used for two different networks which are commonly used same network channel rules/bases. The other significant responsibility of the router is managing the packages; if one of the workstation wants to send something (message/mail or etc.) to another workstation at different network, router ensure the package goes to the other network with the help of static routing.(In packet tracer simulation, router has a option for redirecting the incoming network requests named as static routing configuration).

Finally, to achieve the main requested services; such as sending/receiving mail, browsing the web, sending/receiving files, VoIP Services (sending voice data over an IP between dedicated users/workstations) and lastly database management the servers are essential and needful. Servers are located in second campus, third facility. Servers were configured and connected to the main switch of server farm. This server farm switch is connected to the other switch of second facility.

To sum up, we did not want to mention the structure deeply. All network connections are ended and connected successfully to ensure the achievable accomplished network connection between two distinct campuses.

2.2. Simulation Environment

The simulations done in the project Cisco Packet Tracer was used. Packet Tracer offers a unique combination of realistic simulation and visualization experiences, complex assessment and activity authoring capabilities and opportunities for multi-user collaboration. Cisco Packet Tracer makes learning and teaching significantly easier by supporting multi-user collaboration and by providing a realistic simulation environment for exploration and experimentation.

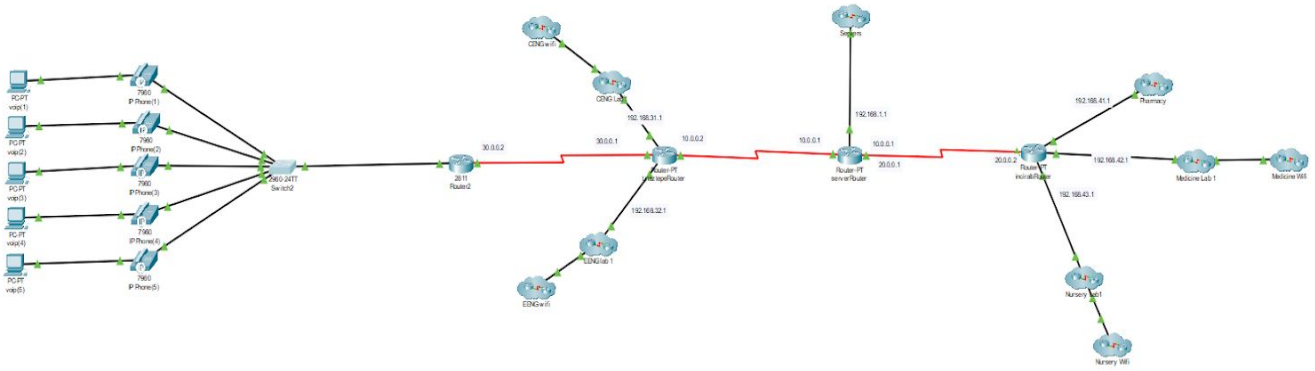
2.3. Network Design Requirements

Server/client architecture was used as the architecture of the network. Seven switches, four access points, four routers and seven servers used for the design. MAIL, DNS, HTTP 2, HTTP 1, FTP 1, FTP 2 and DHCP protocols were used for the communication between devices. LANs contained in the MAN use the star topology so in general our topology can be considered to be a hybrid topology. Logical and physical topology of the network is presented below with the configurations for the servers.

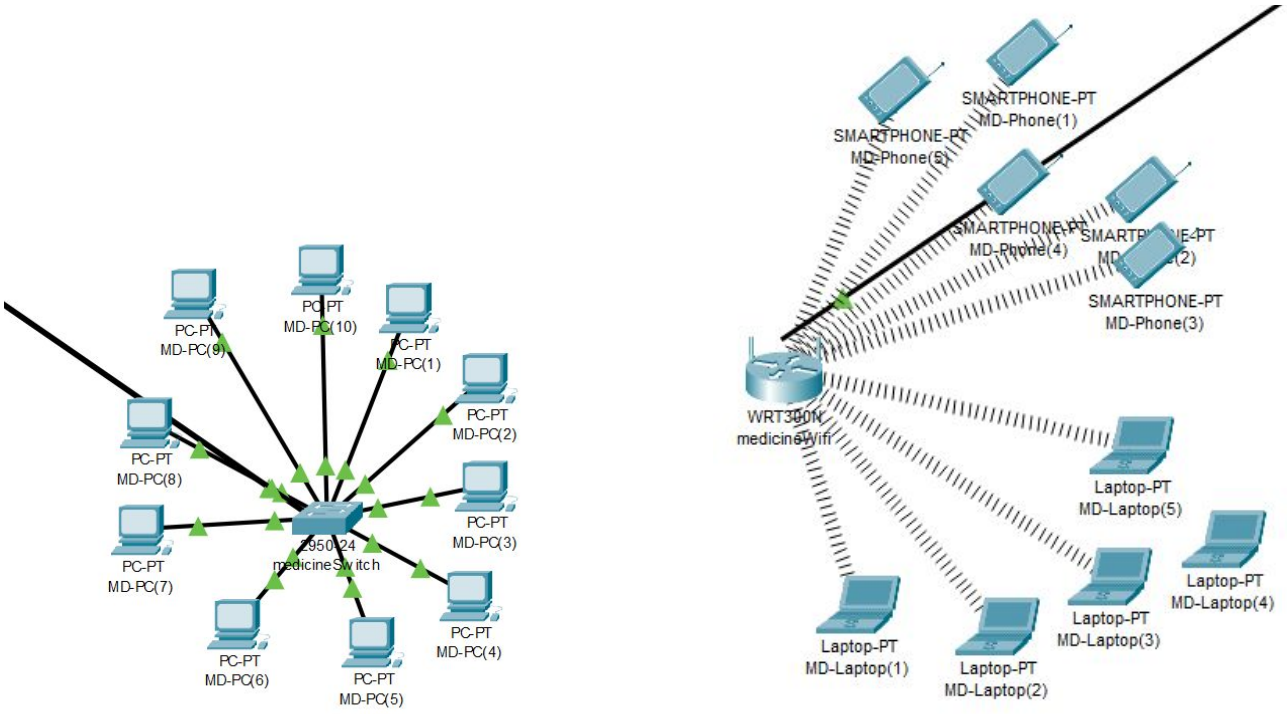
2.4. Requirement Analysis

All workstations in all facilities of the first campus and in the first and second facilities of the second campus have access to web servers located in the third facility of the second campus.
The mail server was authorized to send mail to all workstations in the first and third facilities of the first campus, to receive mail from workstations in the third facility of the first campus, and to use mail applications to the workstations in the first facility of the second campus.
FTP servers were authorized to send files to workstations in the first facility of the first campus, and access to the FTP server to workstations in the second facility.
Workstations at the second facility of the first campus were given the authority to use the database, and workstations at the second facility of the second campus were allowed to organize files and applications.
In addition, the access point was used for the wireless network feature of the workstations in the first facility of the second campus, and only 5 computers from the workstations in the second facility of the second campus were used in that facility for the VoIP protocol router2811 because other routers are not suitable for sending voice.

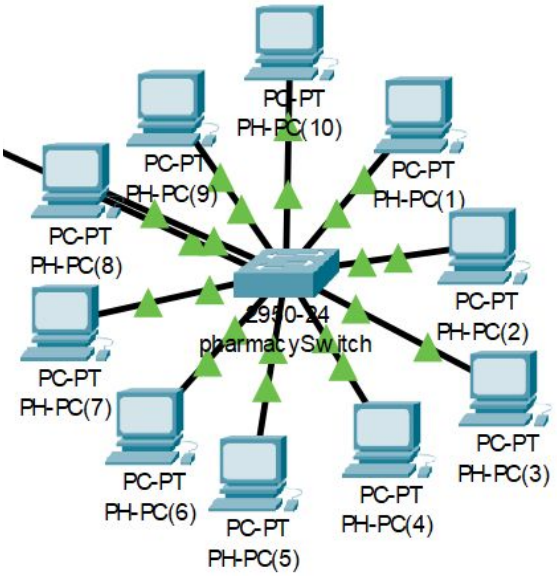
2.5. Definitions of the System/Model



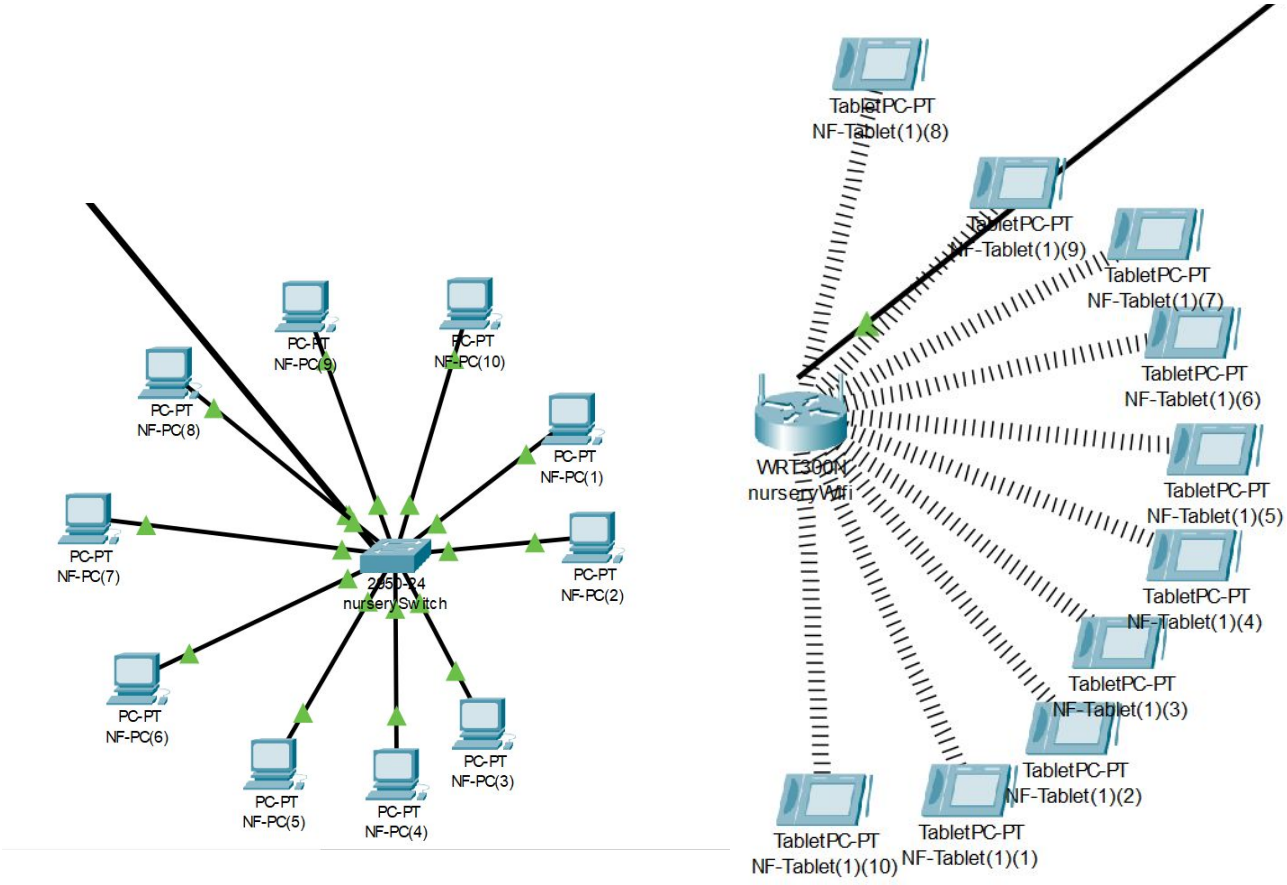
General Shape of The System



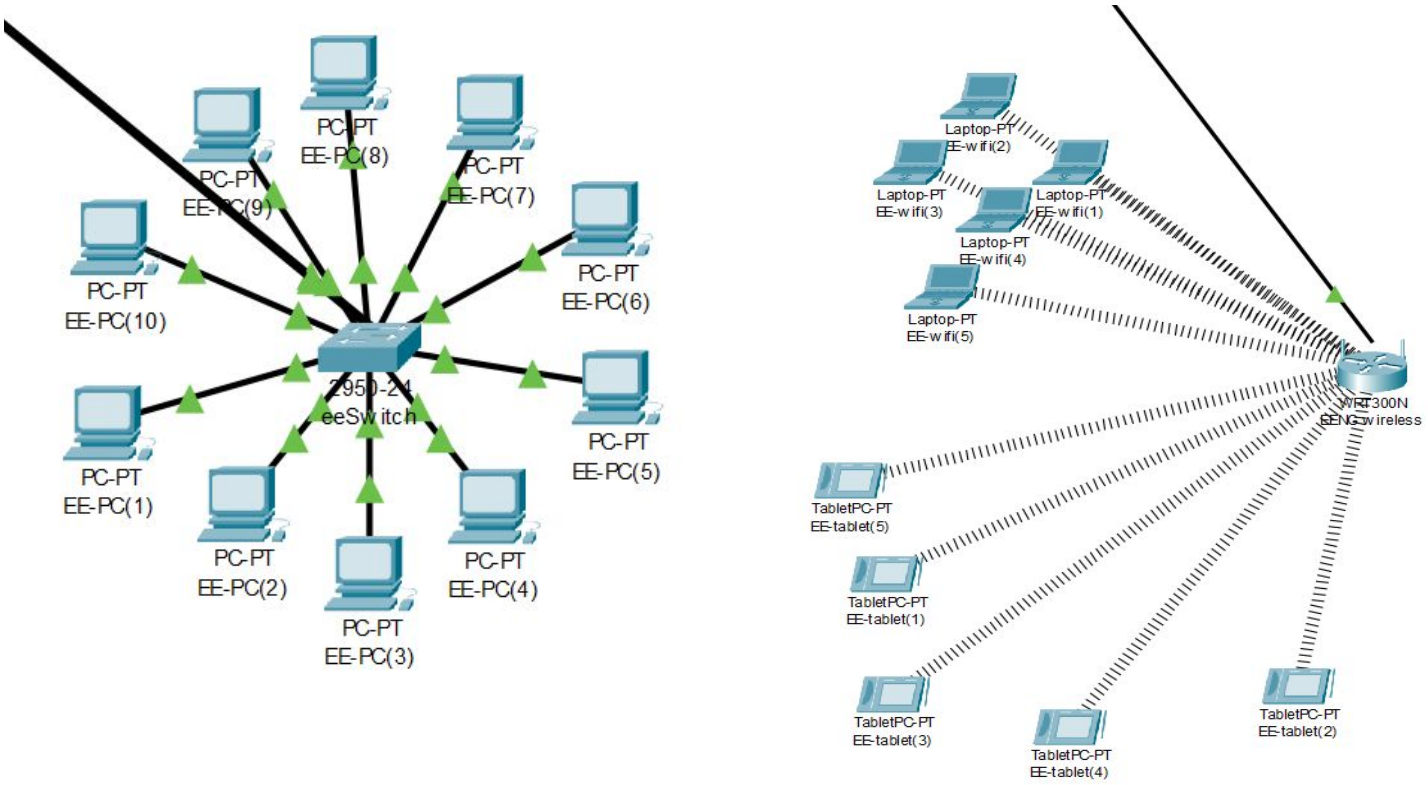
First Campus First Facility



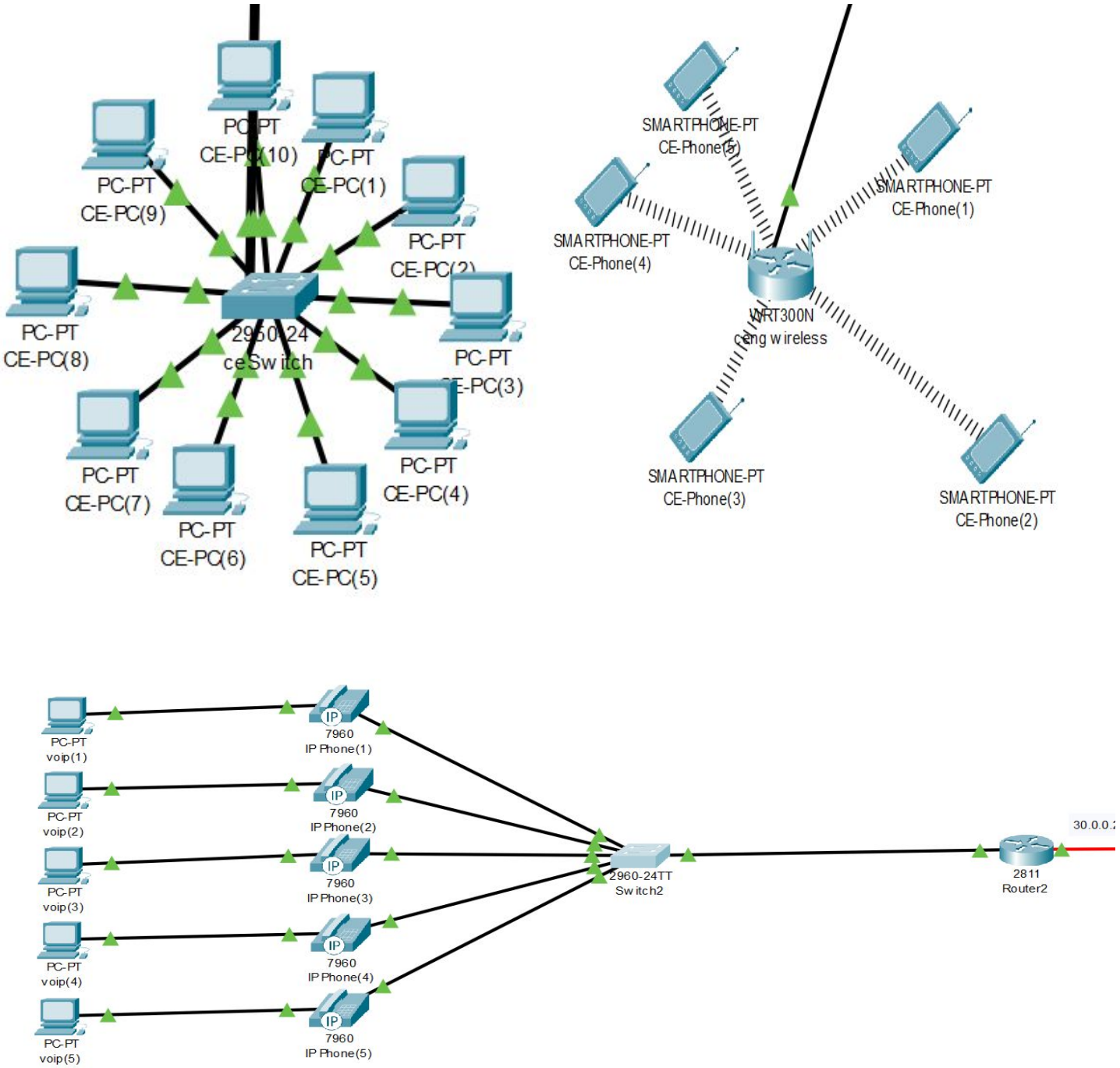
First Campus Second Facility



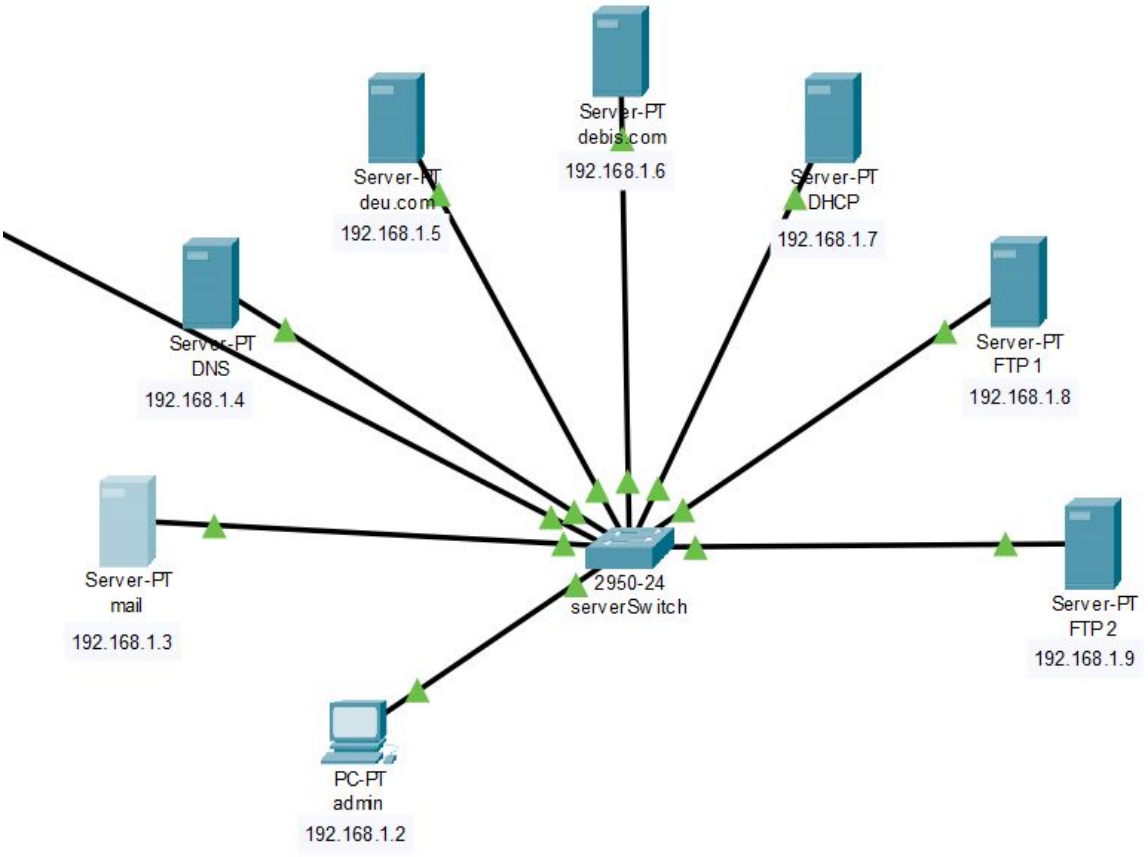
First Campus Third Facility



Second Campus First Facility

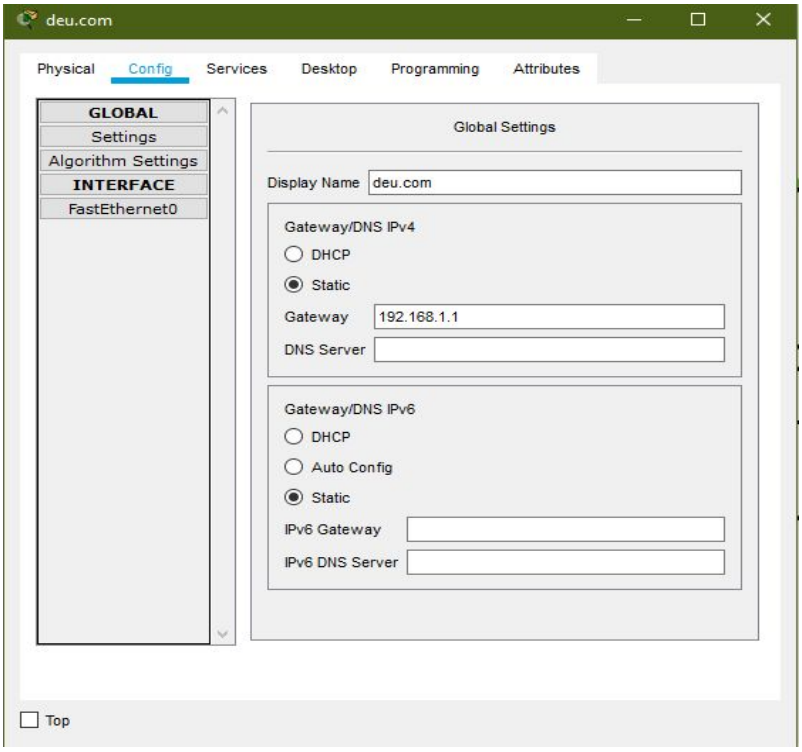


Second Campus Second Facility

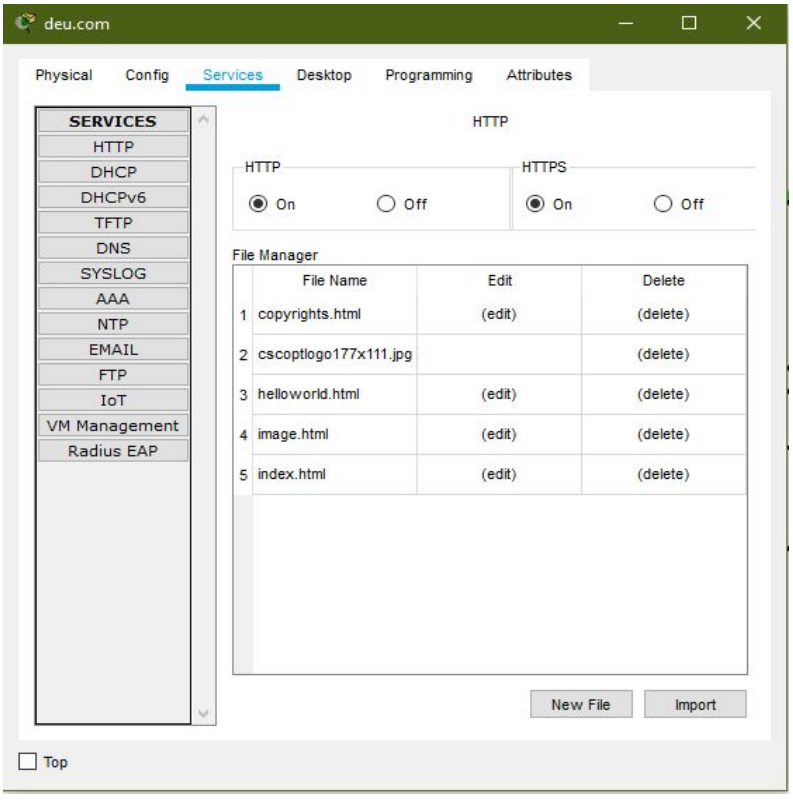


Second Campus Third Facility

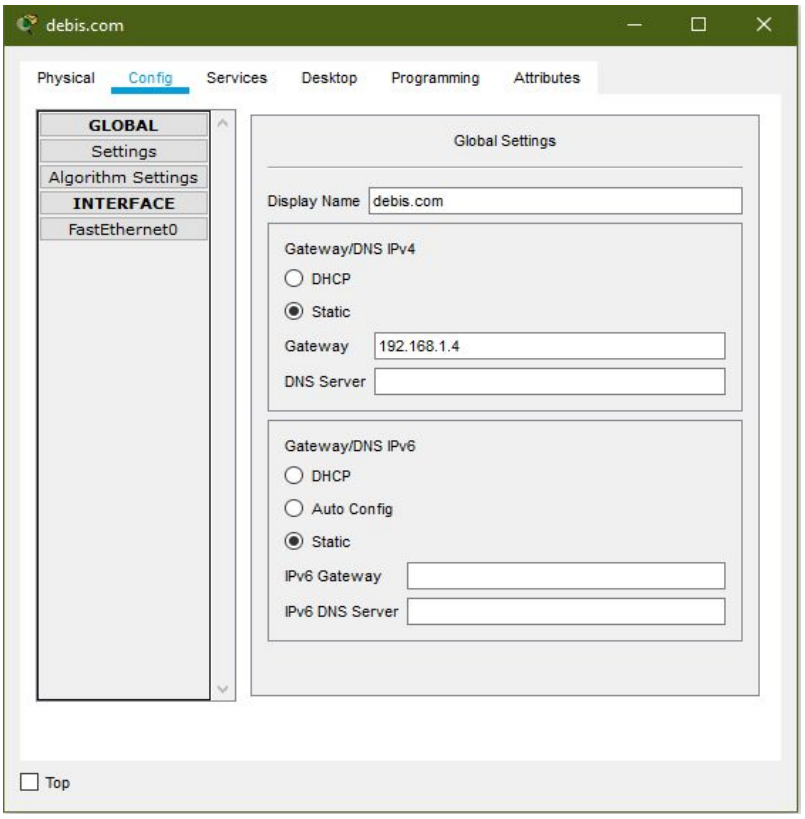
2.6. Simulation Elements



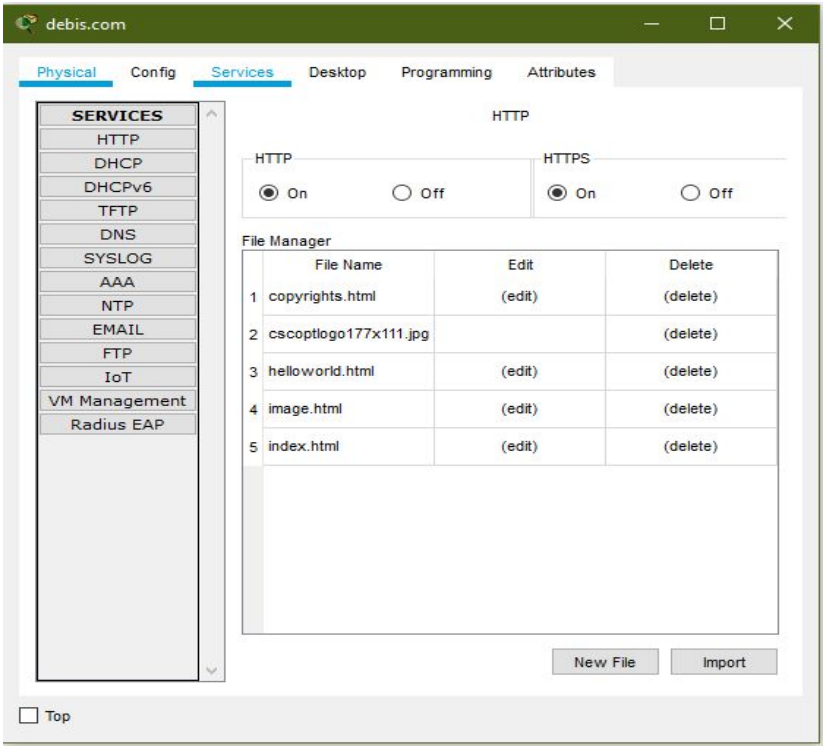
HTTP1 Server Config



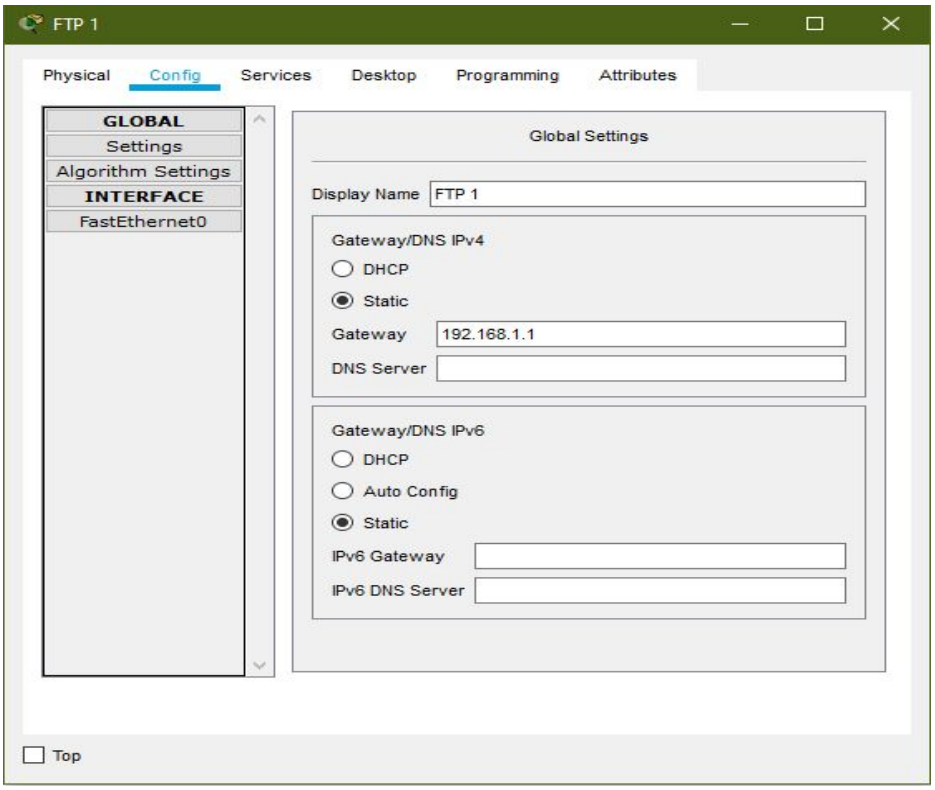
HTTP1 Server Services



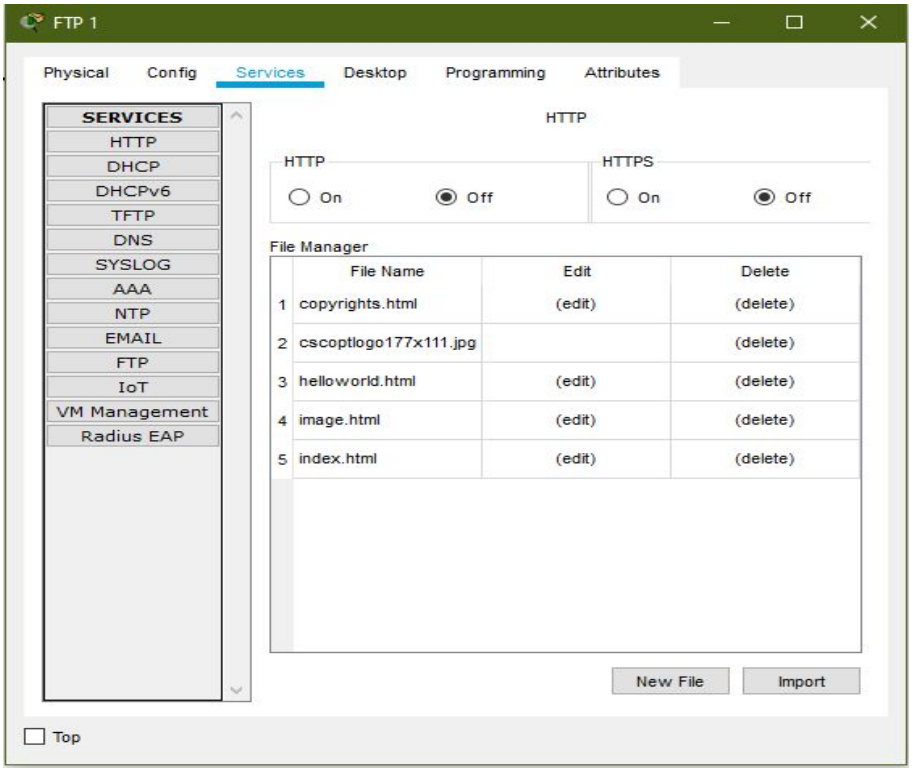
HTTP2 Server Config



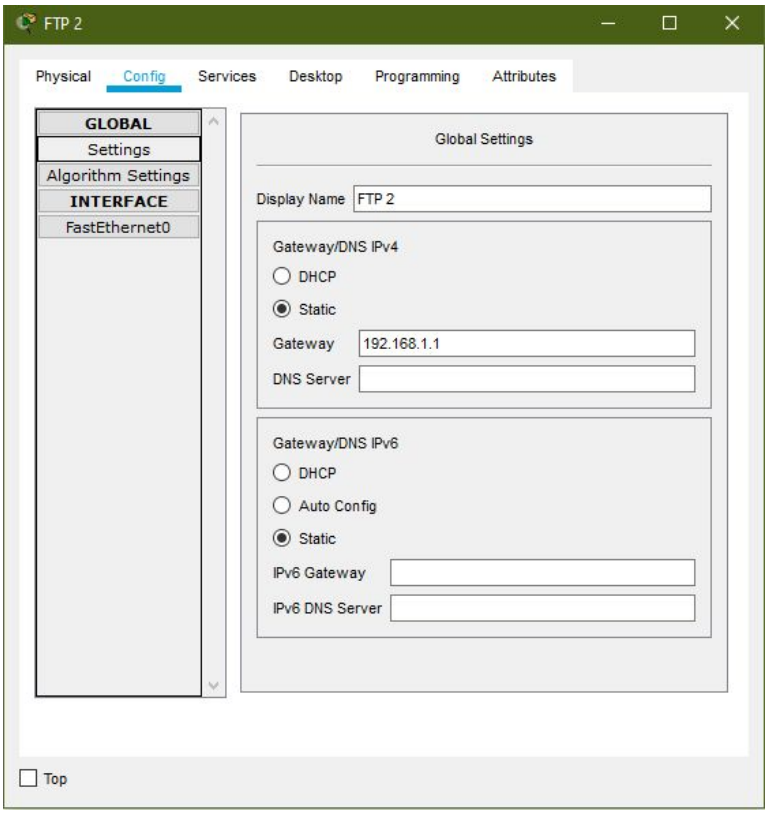
HTTP2 Server Services



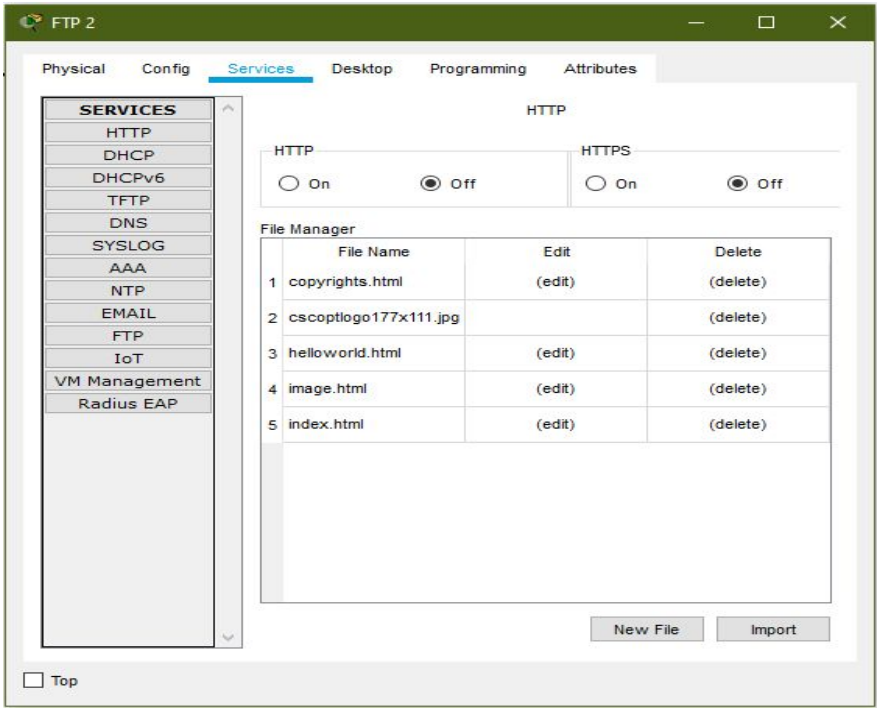
FTP1 Server Config



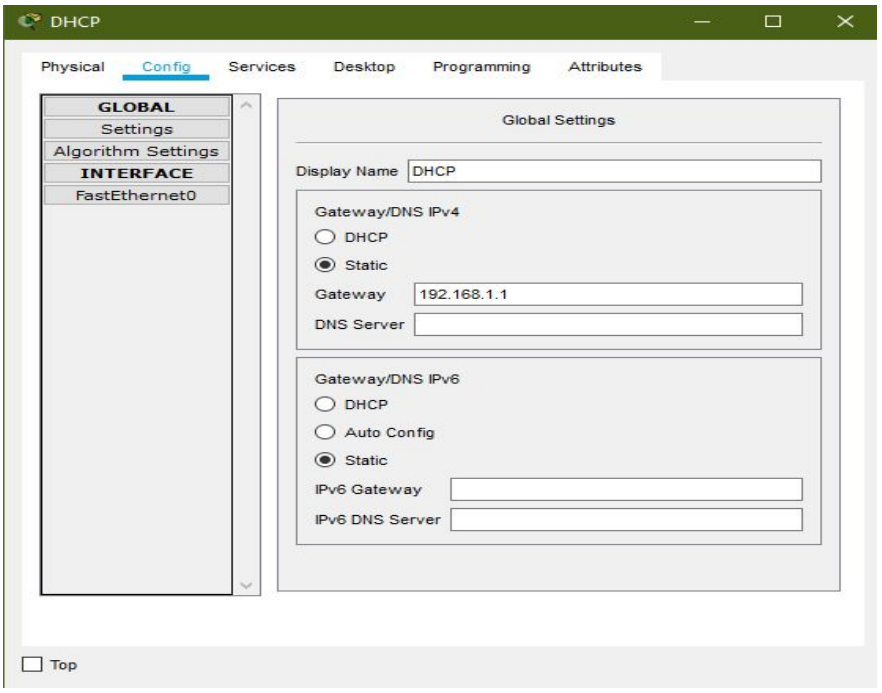
FTP1 Server Service



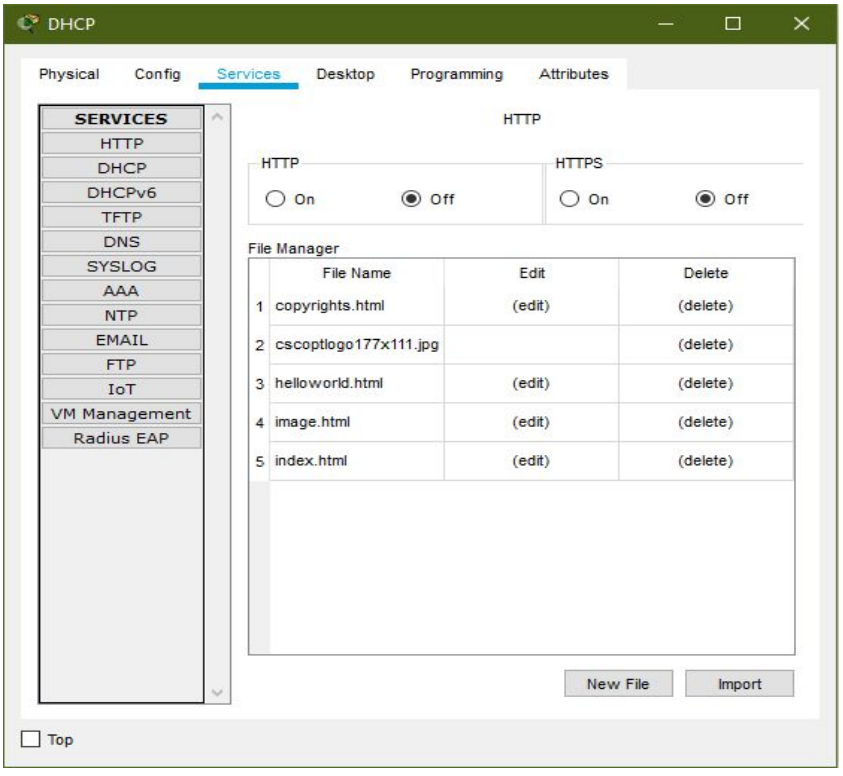
FTP2 Server Config



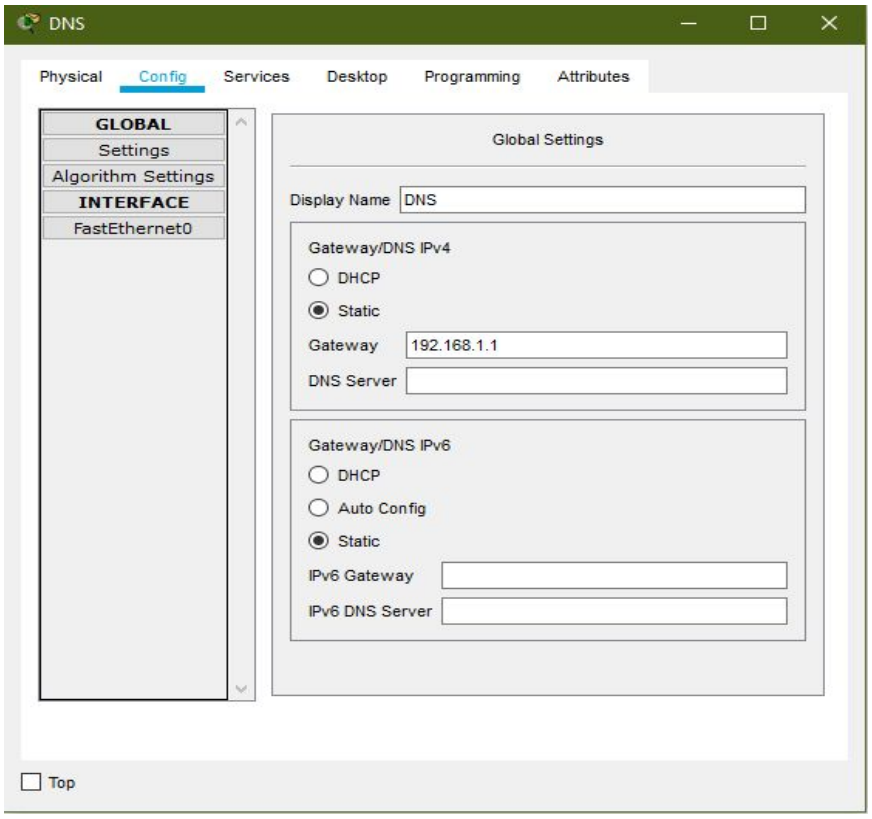
FTP2 Server Service



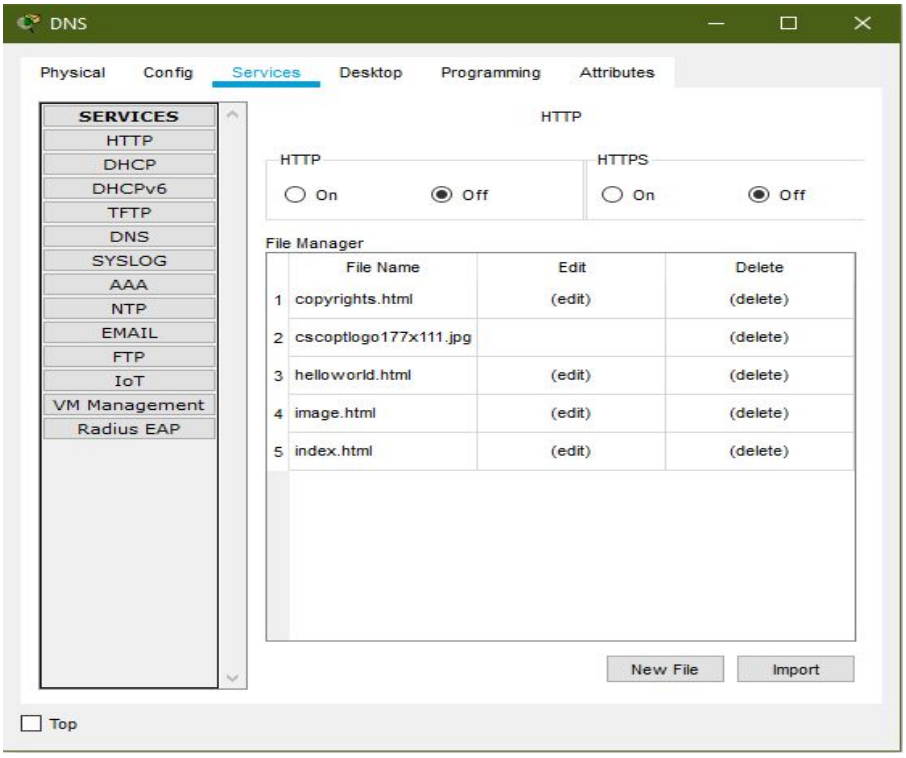
DHCP Server Config



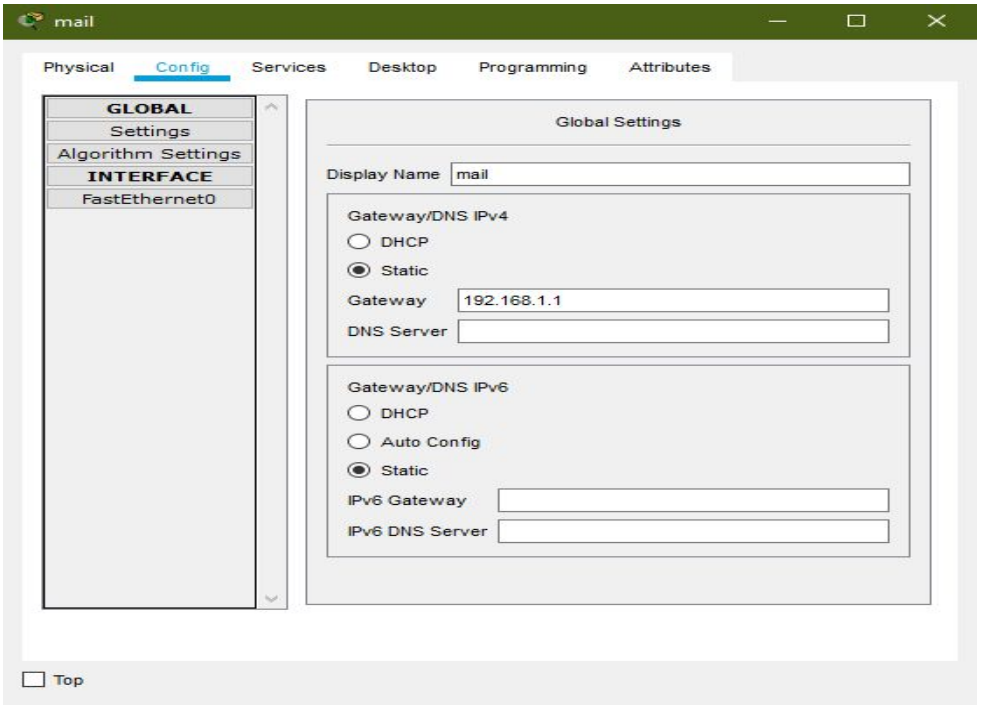
DHCP Server Service



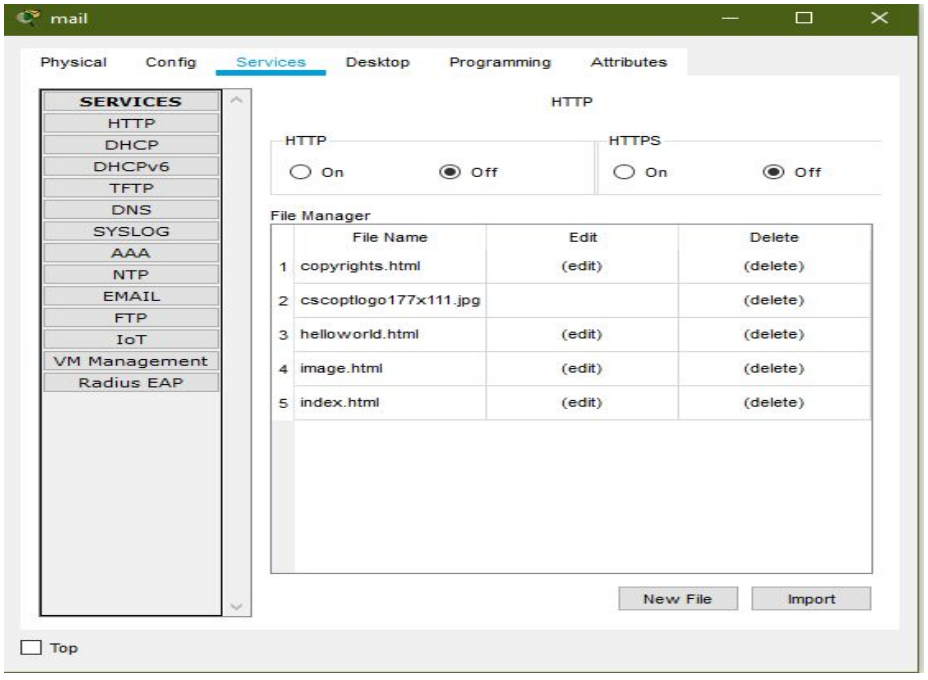
DNS Server Config



DNS Server Service



MAIL Server Config

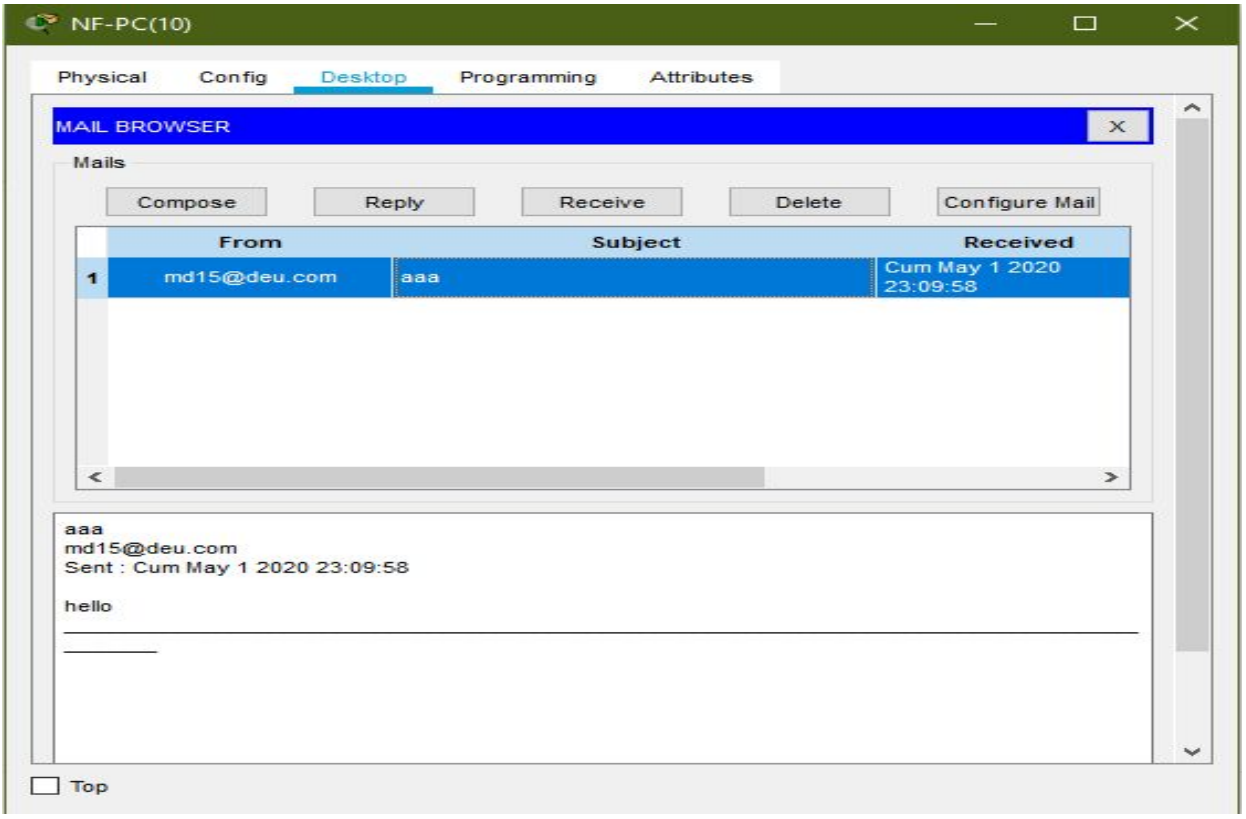


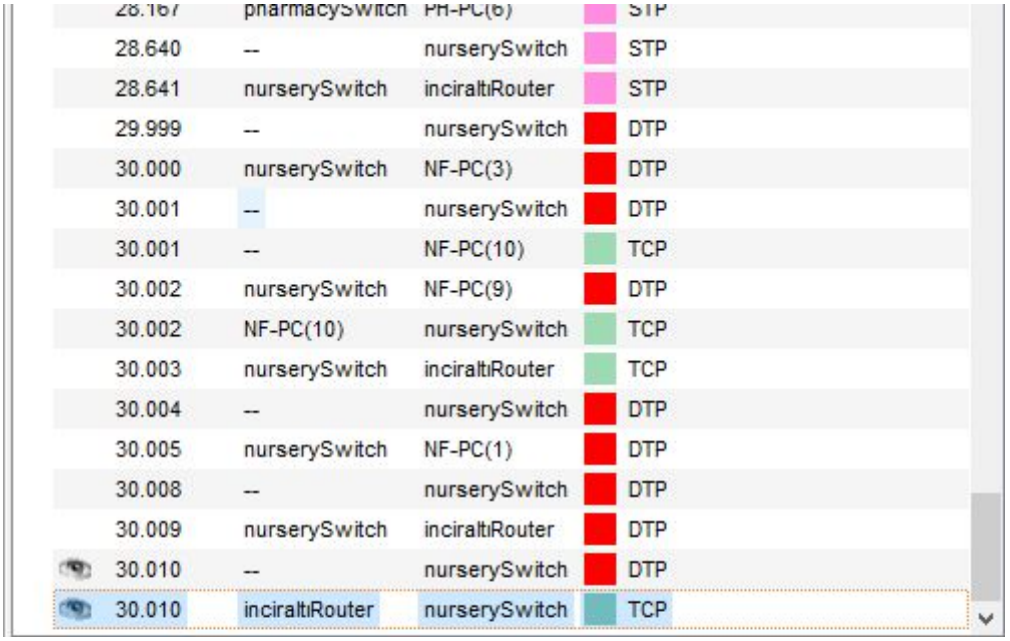
MAIL Server Service

CHAPTER THREE

TRAFFIC ANALYSIS & SIMULATION RESULTS

Scenario 1 : A smartphone user from first facility of first campus wants to send email to her friend in the 3rd facility of first campus.





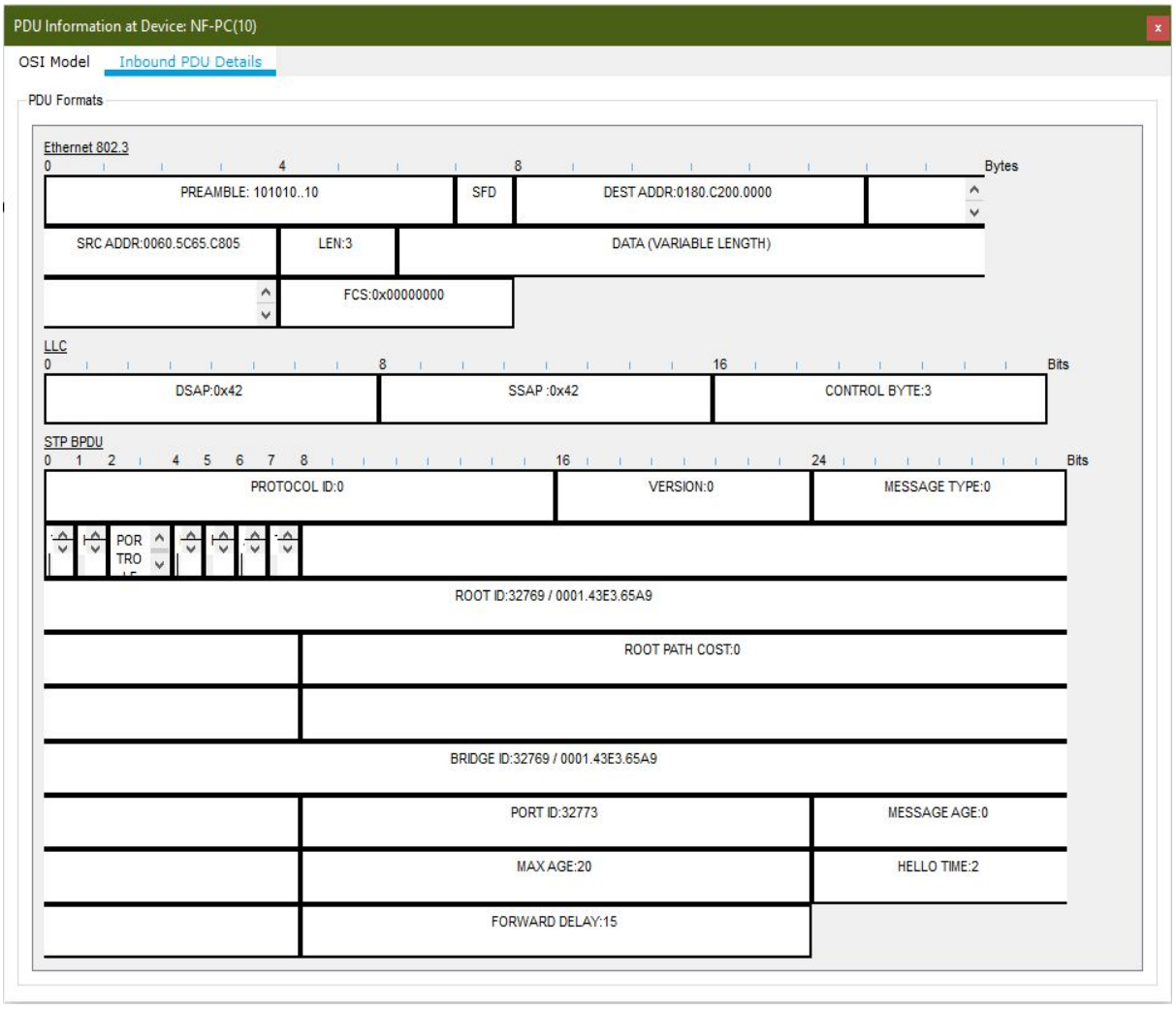
PDU Information at Device: NF-PC(10)

OSI Model | Inbound PDU Details

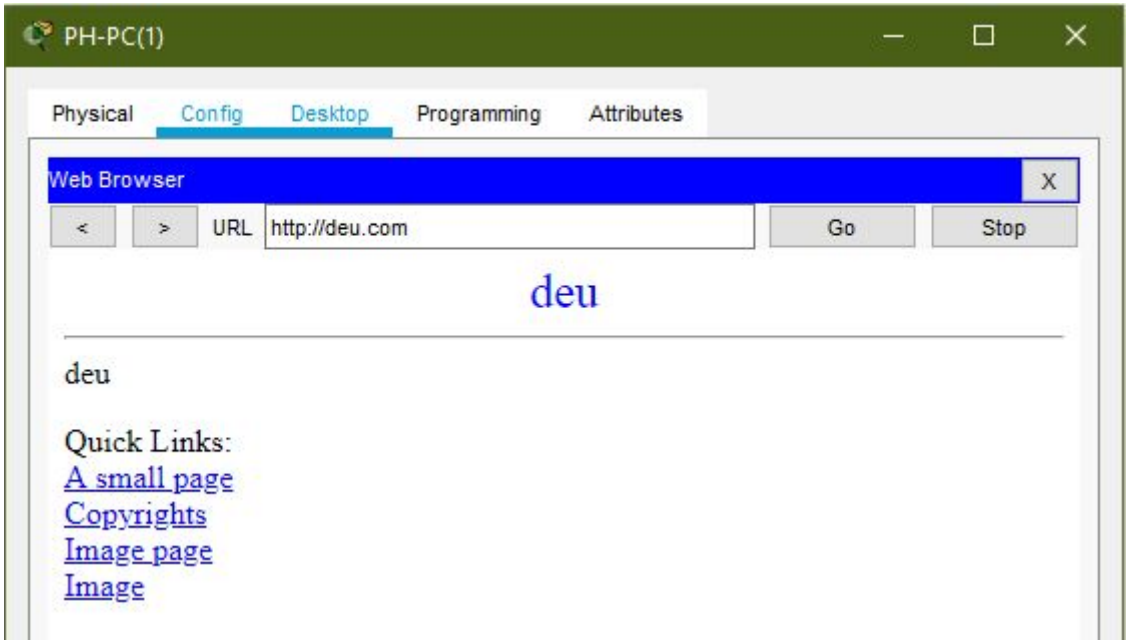
At Device: NF-PC(10)
Source: nurserySwitch
Destination: STP Multicast Address

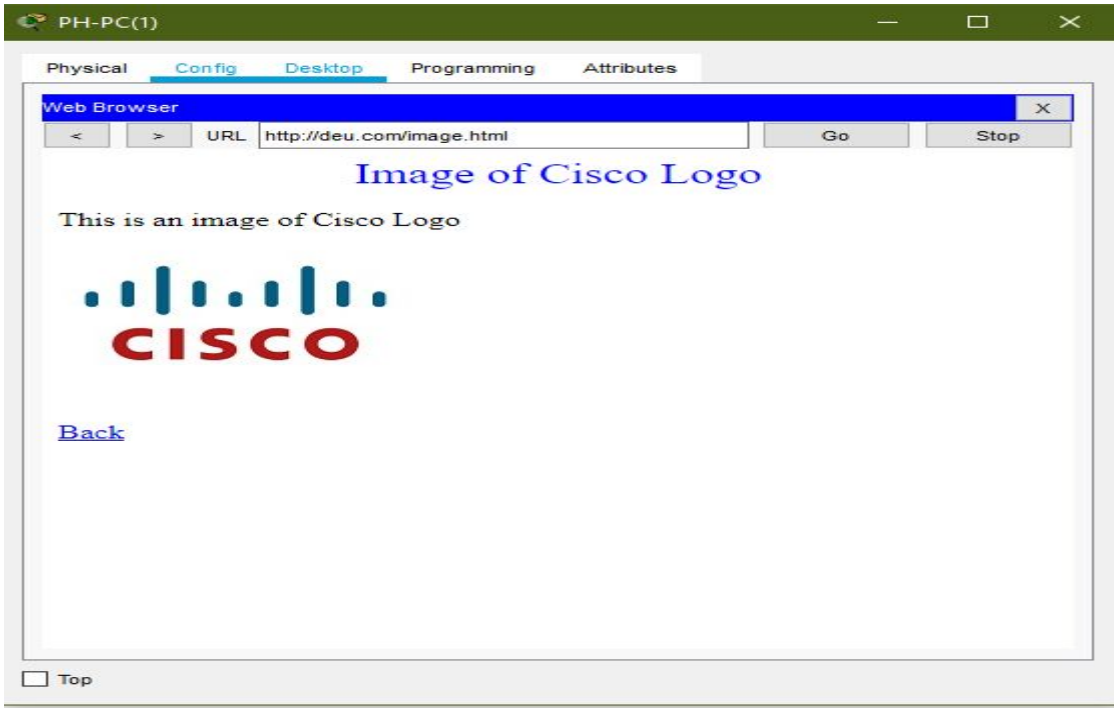
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: IEEE 802.3 Header 0060.5C65.C805 >> 0180.C200.0000 LLC STP BPDU	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.



Scenario 2 : A user from second facility of first campus wants to browse a Web page.





Vis.	Time(sec)	Last Device	At Device	Type
	8.138	pharmacySwitch	PH-PC(6)	STP
	10.138	--	pharmacyS...	STP
	10.139	pharmacySwitch	PH-PC(3)	STP
	10.139	pharmacySwitch	PH-PC(4)	STP
	10.139	pharmacySwitch	PH-PC(2)	STP
	10.139	pharmacySwitch	inciraltıRouter	STP
	10.139	pharmacySwitch	PH-PC(8)	STP
	10.139	pharmacySwitch	PH-PC(7)	STP
	10.139	pharmacySwitch	PH-PC(9)	STP
	10.139	pharmacySwitch	PH-PC(10)	STP
	10.139	pharmacySwitch	PH-PC(1)	STP
	10.139	pharmacySwitch	PH-PC(5)	STP
	10.139	pharmacySwitch	PH-PC(6)	STP
	12.137	--	pharmacyS...	STP
	12.138	pharmacySwitch	PH-PC(3)	STP
	12.138	pharmacySwitch	PH-PC(4)	STP
	12.138	pharmacySwitch	PH-PC(2)	STP
	12.138	pharmacySwitch	inciraltıRouter	STP
	12.138	pharmacySwitch	PH-PC(8)	STP
	12.138	pharmacySwitch	PH-PC(7)	STP
	12.138	pharmacySwitch	PH-PC(9)	STP
	12.138	pharmacySwitch	PH-PC(10)	STP
	12.138	pharmacySwitch	PH-PC(1)	STP
	12.138	pharmacySwitch	PH-PC(5)	STP
	12.138	pharmacySwitch	PH-PC(6)	STP

PDU Information at Device: PH-PC(1)

OSI Model | Inbound PDU Details

PDU Formats

Ethernet 802.3

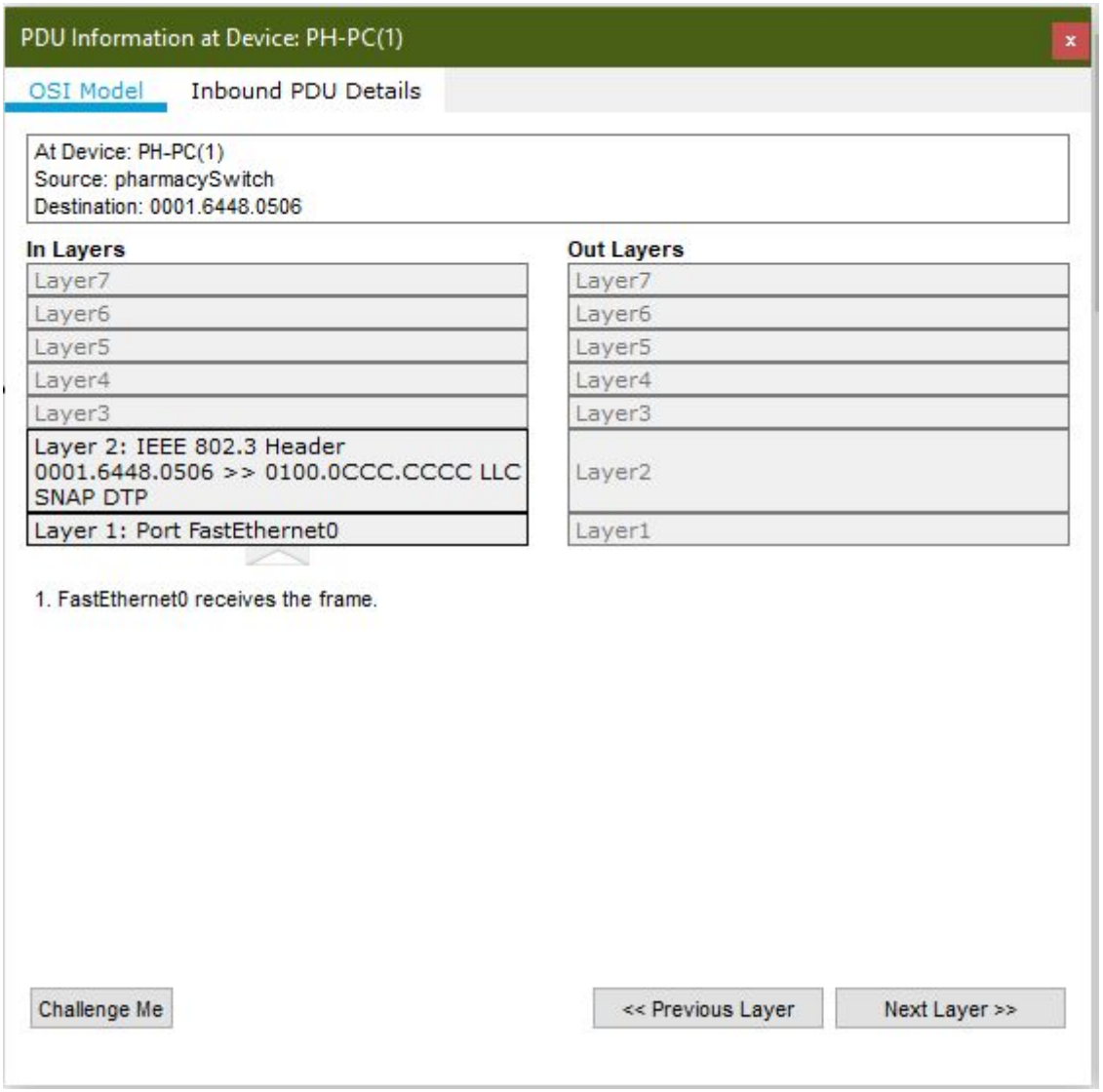
0	4	8	Bytes
PREAMBLE: 101010..10	SFD	DEST ADDR:0100.0CCC.CCCC	
SRC ADDR:0001.6448.0506	LEN:8	DATA (VARIABLE LENGTH)	
	FCS:0x00000000		

SNAP

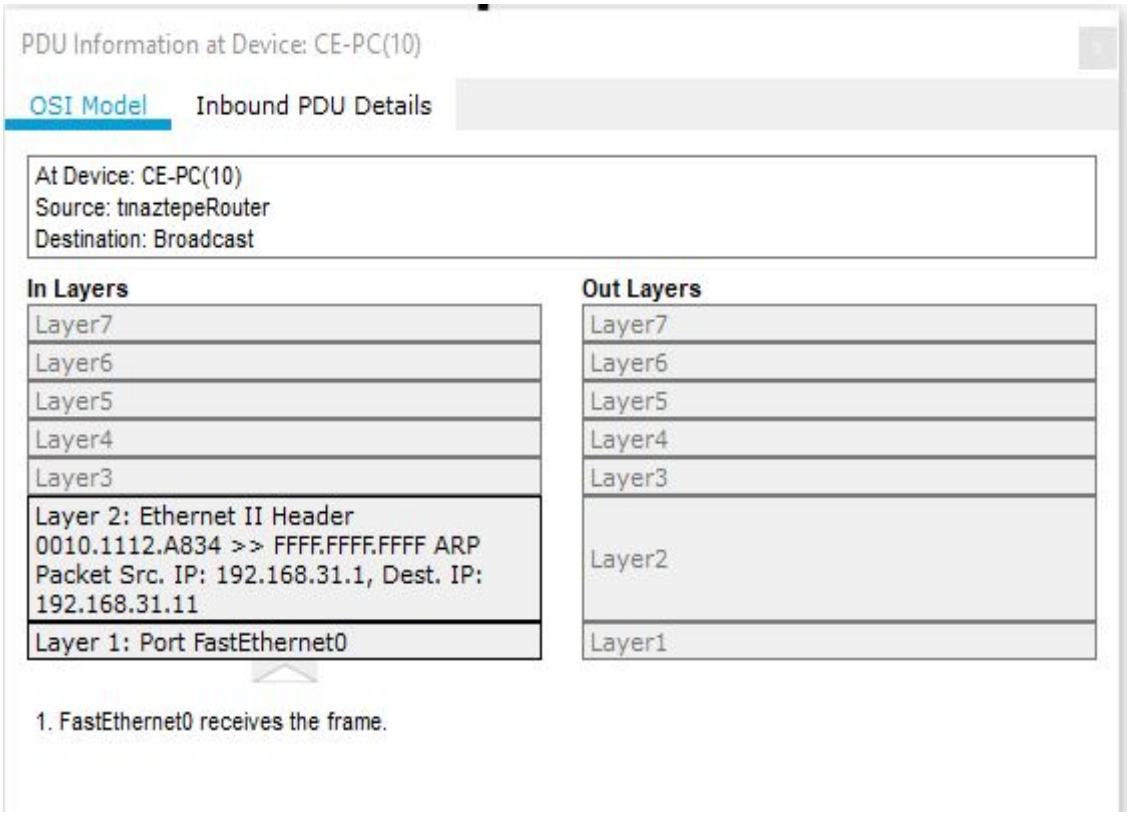
0	24	Bits
DSAP:0xaa	SSAP :0xaa	CONTROL BYTE:3
OUI:0x00000c	PID:0x2004	

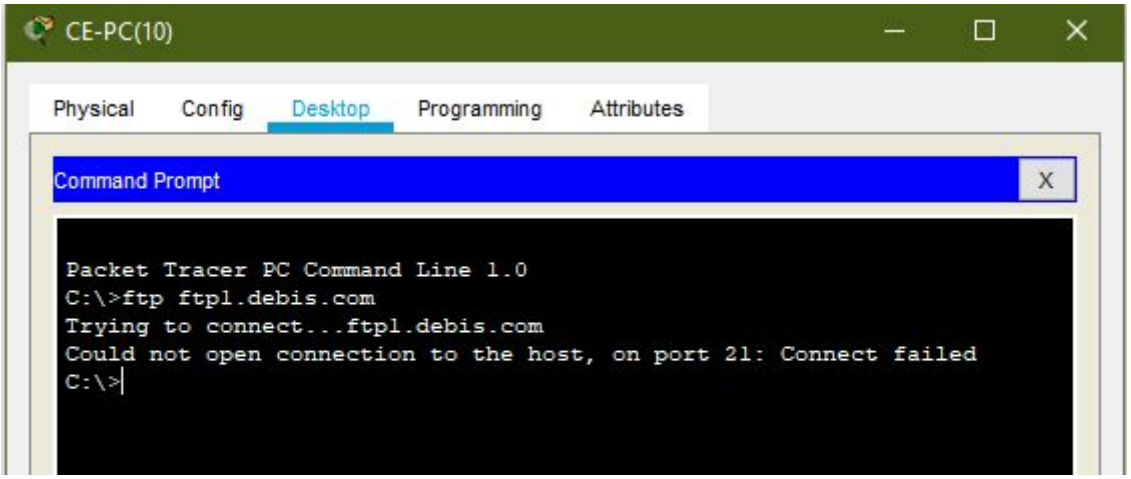
DTP

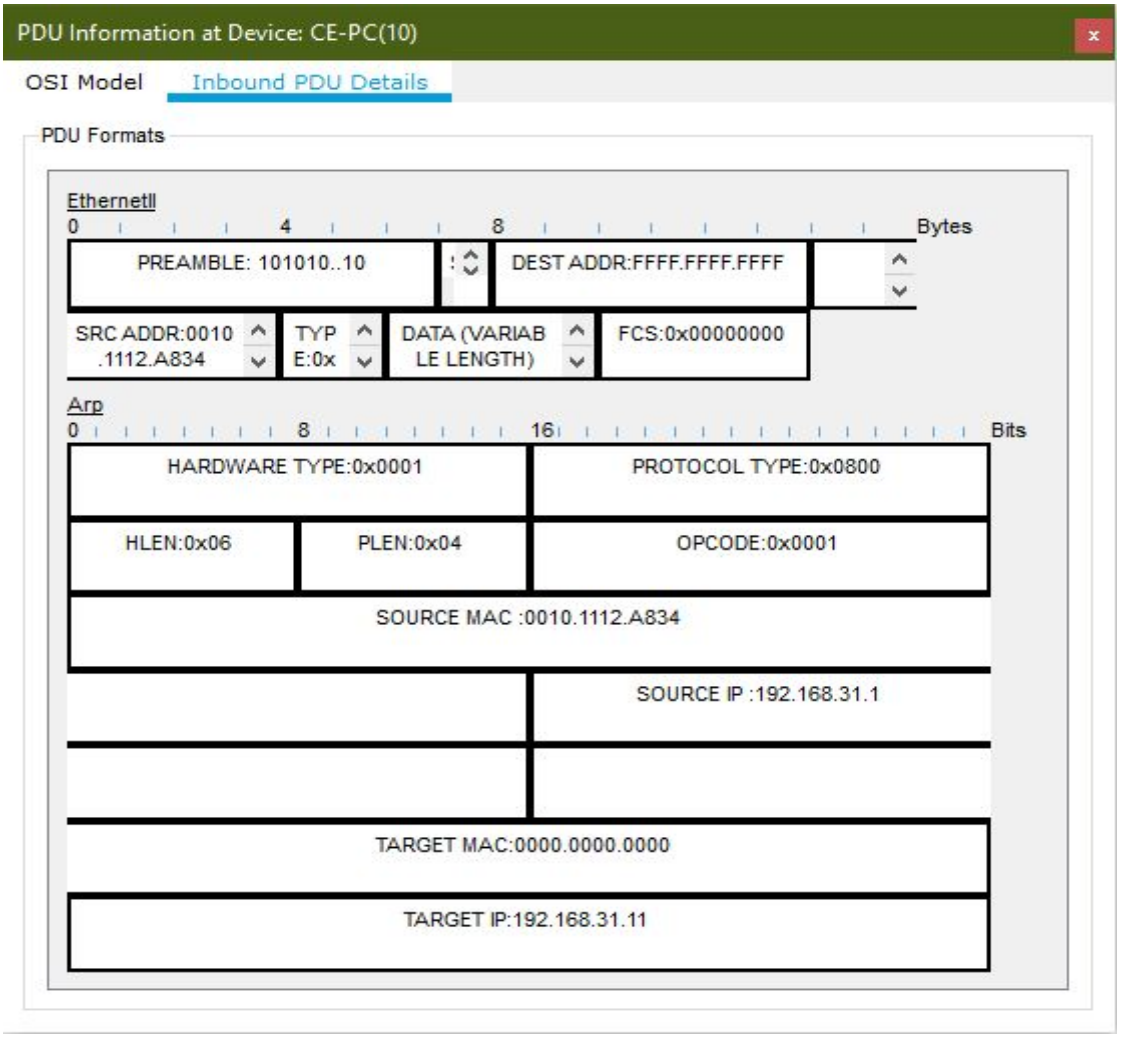
0	1	2	Bytes
VERSION:1	TYPE: 1	LENGTH:5	
	DOMAIN NAME:	TYPE: 2	
LENGTH: 5	STATUS:Dynamic Auto		
TYPE: 3	LENGTH: 5		
TRUNK:0	TYPE: 4		
LENGTH: 10			
SENDER ID:0001.6448.0506			


PDU Information at Device: PH-PC(1)
OSI Model
Inbound PDU Details
At Device: PH-PC(1)
Source: pharmacySwitch
Destination: 0001.6448.0506
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: IEEE 802.3 Header
0001.6448.0506 >> 0100.0CCC.CCCC LLC
SNAP DTP
Layer 1: Port FastEthernet0
Layer2
Layer1
1. FastEthernet0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>

Scenario 3 : A computer engineer from second facility of second campus developed a web application and wants to send her code files to FTP server in the third facility of second campus.





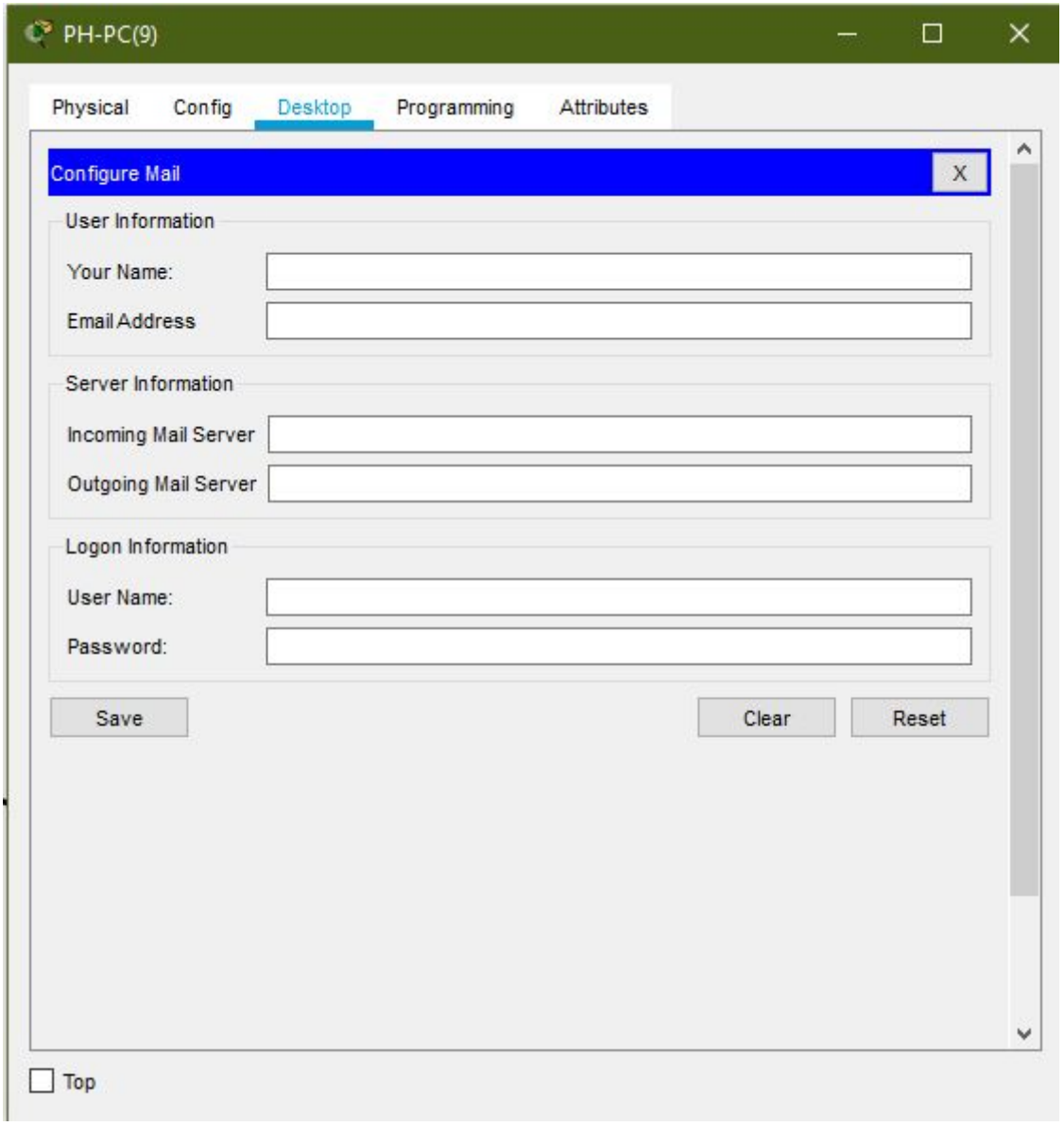


	0.005	tinaztepeRouter	ceSwitch		ARP
	0.006	ceSwitch	CE-PC(8)		ARP
	0.006	ceSwitch	CE-PC(10)		ARP
	0.006	ceSwitch	CE-PC(9)		ARP
	0.006	ceSwitch	CE-PC(1)		ARP
	0.006	ceSwitch	CE-PC(7)		ARP
	0.006	ceSwitch	CE-PC(6)		ARP
	0.006	ceSwitch	CE-PC(5)		ARP
	0.006	ceSwitch	CE-PC(4)		ARP
	0.006	ceSwitch	CE-PC(3)		ARP

Scenario 4 : Two users from second facility of second campus want to talk with VoIP.

	0.023	--	IP Phone(5)	TCP
	0.024	IP Phone(5)	Switch2	TCP
	0.024	Switch2	Router2	TCP
	0.025	Switch2	Router2	TCP
	0.027	--	pharmacyS...	STP
	0.028	pharmacySwitch	inciraltiRouter	STP
	0.043	--	Switch2	STP
	0.044	Switch2	IP Phone(1)	STP
	0.044	Switch2	Router2	STP
	0.044	Switch2	IP Phone(4)	STP
	0.044	Switch2	IP Phone(2)	STP
	0.044	Switch2	IP Phone(5)	STP
	0.044	Switch2	IP Phone(3)	STP
	0.045	IP Phone(1)	voip(1)	STP
	0.045	IP Phone(4)	voip(4)	STP
	0.045	IP Phone(2)	voip(2)	STP
	0.045	IP Phone(5)	voip(5)	STP
	0.045	IP Phone(3)	voip(3)	STP
	0.105	--	IP Phone(1)	SCCP
	0.106	IP Phone(1)	Switch2	SCCP
	0.107	Switch2	Router2	SCCP
	0.137	Switch2	Router2	STP
	0.139	--	Router2	TCP
	0.140	Router2	Switch2	TCP
	0.141	Switch2	IP Phone(1)	TCP

Scenario 5 : A user in the second facility of first campus wants to send an email message to his friend in the second facility of second campus.



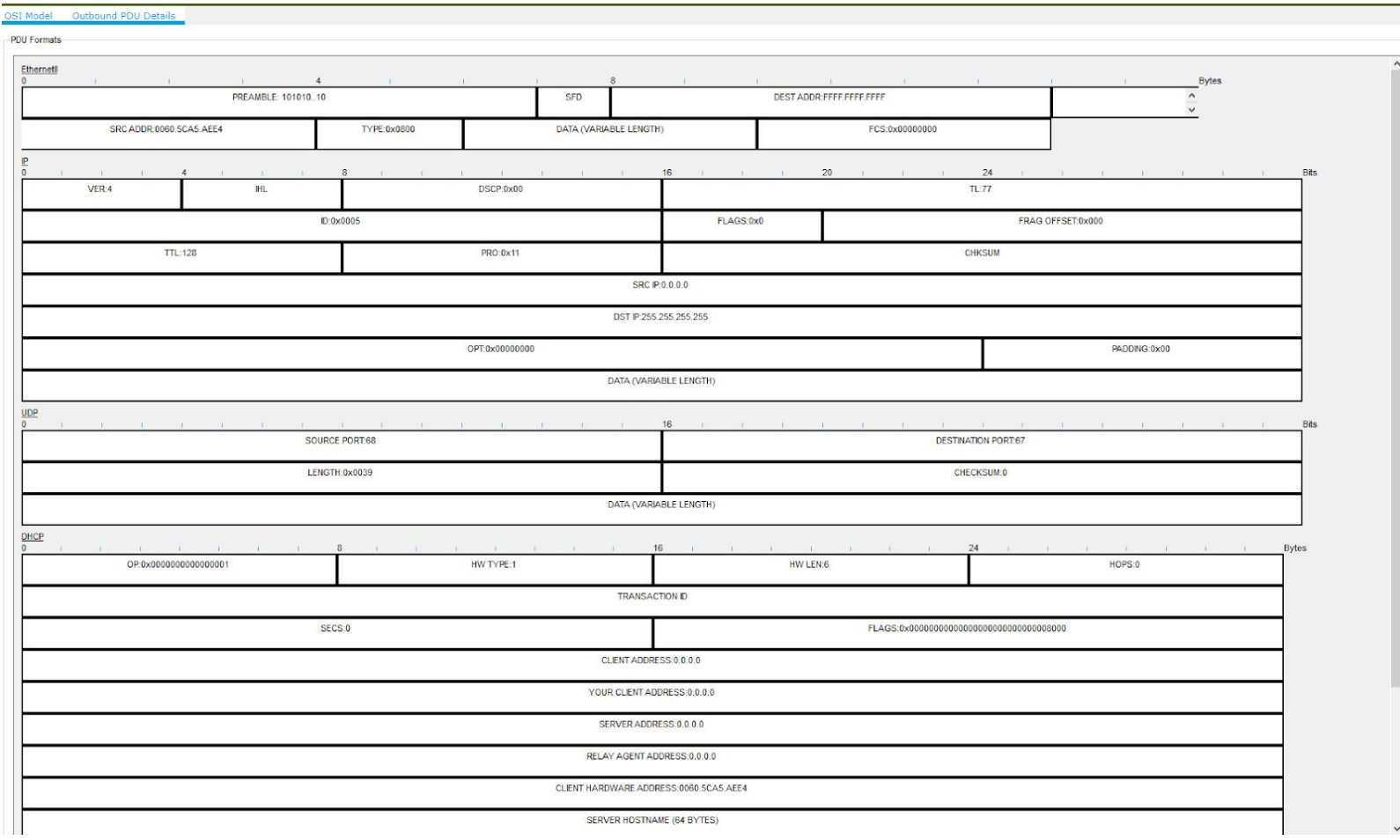
PDU Information at Device: PH-PC(9)

OSI Model | Outbound PDU Details

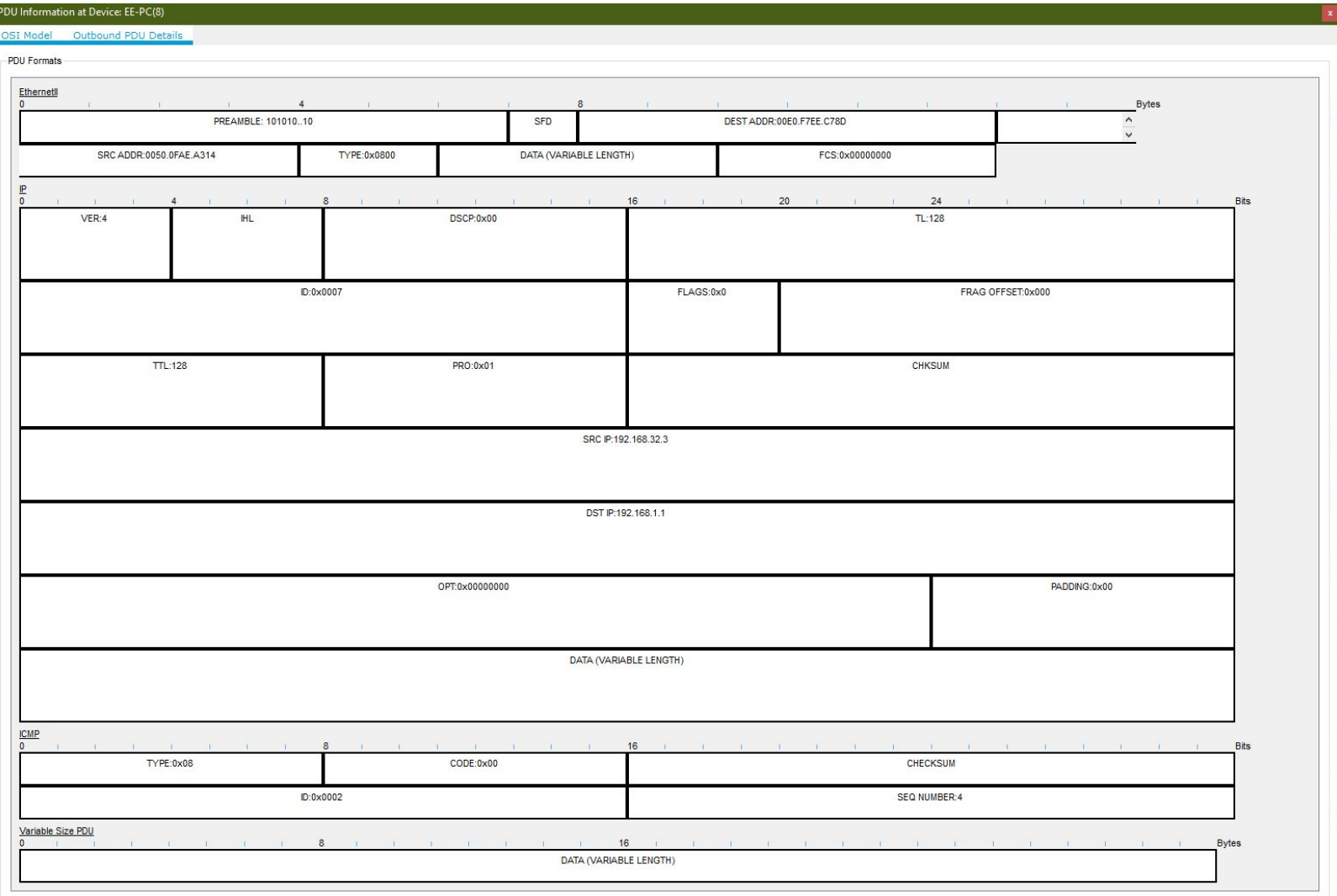
At Device: PH-PC(9)
Source: PH-PC(9)
Destination: 255.255.255.255

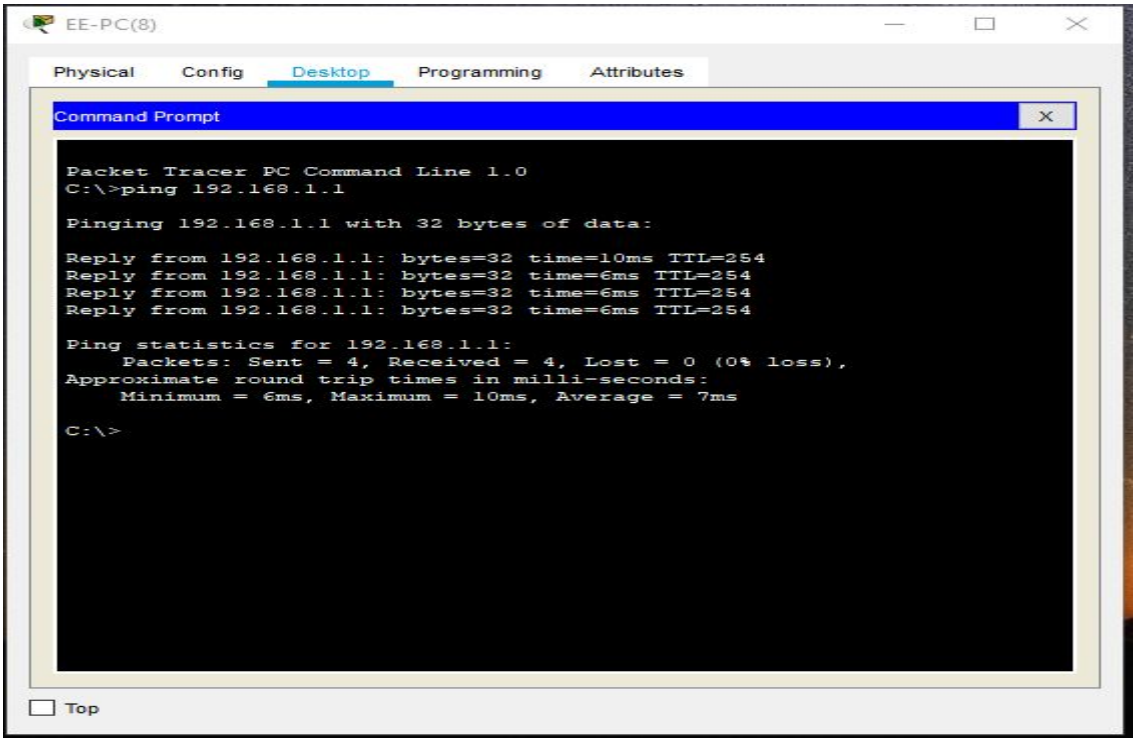
In Layers	Out Layers
Layer7	Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 68, Dst Port: 67
Layer3	Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255
Layer2	Layer 2: Ethernet II Header 0060.5CA5.AEE4 >> FFFF.FFFF.FFFF
Layer1	Layer 1: Port(s):

1. The DHCP client constructs a Discover packet and sends it out.



Scenario 6 : A user from first facility of second branch pings Web server of third facility of second campus.





	0.010	eeSwitch	EE-PC(8)	ICMP
	0.217	--	eeSwitch	STP
	0.218	eeSwitch	EE-PC(2)	STP
	0.218	eeSwitch	tınaztepeRo...	STP
	0.218	eeSwitch	EE-PC(7)	STP
	0.218	eeSwitch	EE-PC(3)	STP
	0.218	eeSwitch	EE-PC(6)	STP
	0.218	eeSwitch	EE-PC(8)	STP
	0.218	eeSwitch	EE-PC(5)	STP
	0.218	eeSwitch	EE-PC(4)	STP
	0.218	eeSwitch	EE-PC(10)	STP
	0.218	eeSwitch	EE-PC(1)	STP
	0.218	eeSwitch	EE-PC(9)	STP
	0.218	eeSwitch	EENG wireless	STP
	1.012	--	EE-PC(8)	ICMP
	1.013	EE-PC(8)	eeSwitch	ICMP
	1.014	eeSwitch	tınaztepeRo...	ICMP
	1.017	tınaztepeRouter	eeSwitch	ICMP
	1.018	eeSwitch	EE-PC(8)	ICMP
	2.021	--	EE-PC(8)	ICMP
	2.022	EE-PC(8)	eeSwitch	ICMP
	2.023	eeSwitch	tınaztepeRo...	ICMP
	2.026	tınaztepeRouter	eeSwitch	ICMP
	2.027	eeSwitch	EE-PC(8)	ICMP
	2.223	--	eeSwitch	STP

PDU Information at Device: EE-PC(8)

OSI Model | Outbound PDU Details

At Device: EE-PC(8)
Source: EE-PC(8)
Destination: 192.168.1.1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 192.168.32.3, Dest. IP: 192.168.1.1 ICMP Message Type: 8
Layer2	Layer 2: Ethernet II Header 0050.0FAE.A314 >> 00E0.F7EE.C78D
Layer1	Layer 1: Port(s): FastEthernet0

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address 192.168.1.1 is not in the same subnet and is not the broadcast address.
5. The default gateway is set. The device sets the next-hop to default gateway.

Scenario 7 : A tablet user from first facility of second campus wants to read her emails.

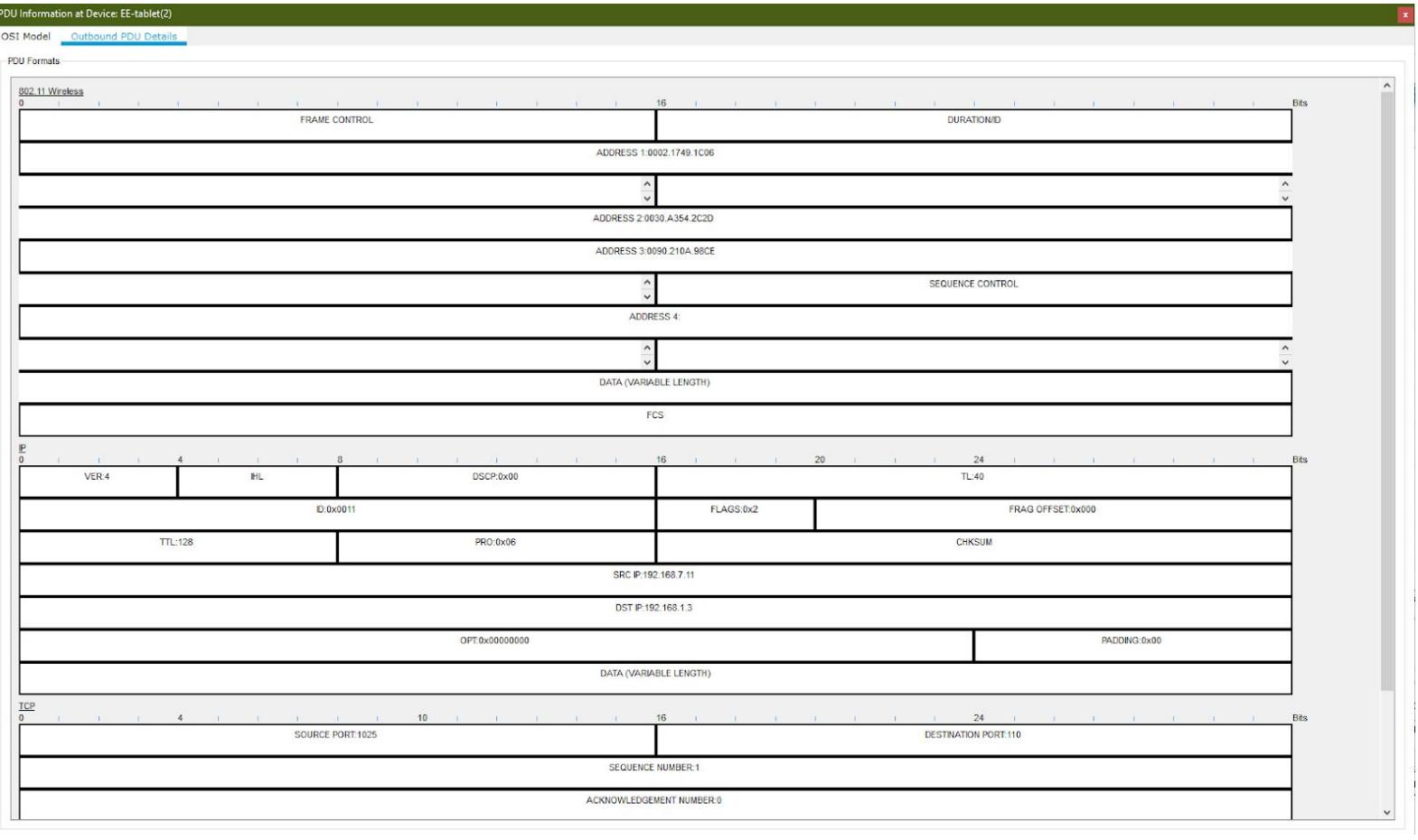
PDU Information at Device: EE-tablet(2)

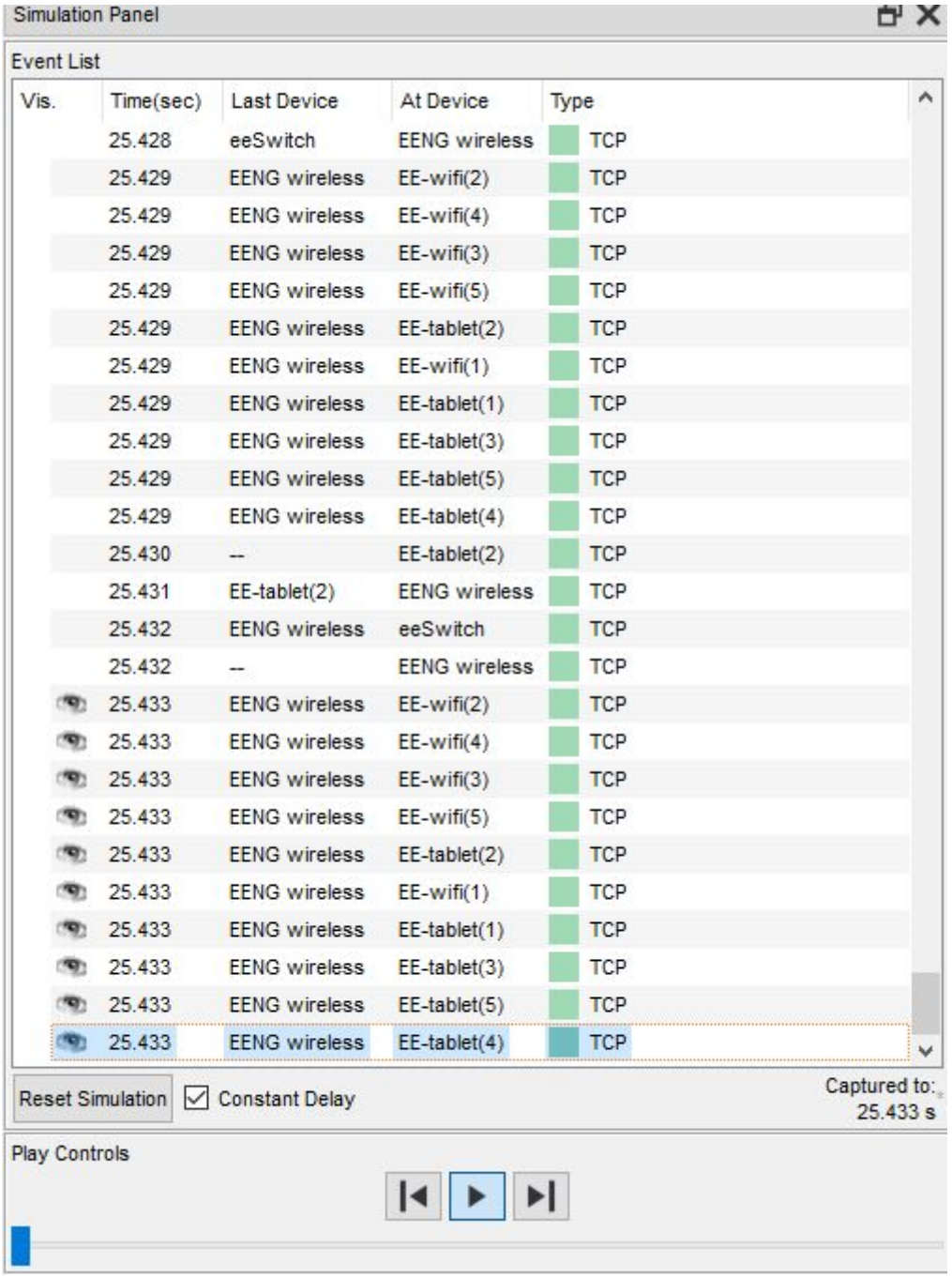
OSI Model | Outbound PDU Details

At Device: EE-tablet(2)
Source: EE-tablet(2)
Destination: 192.168.1.3

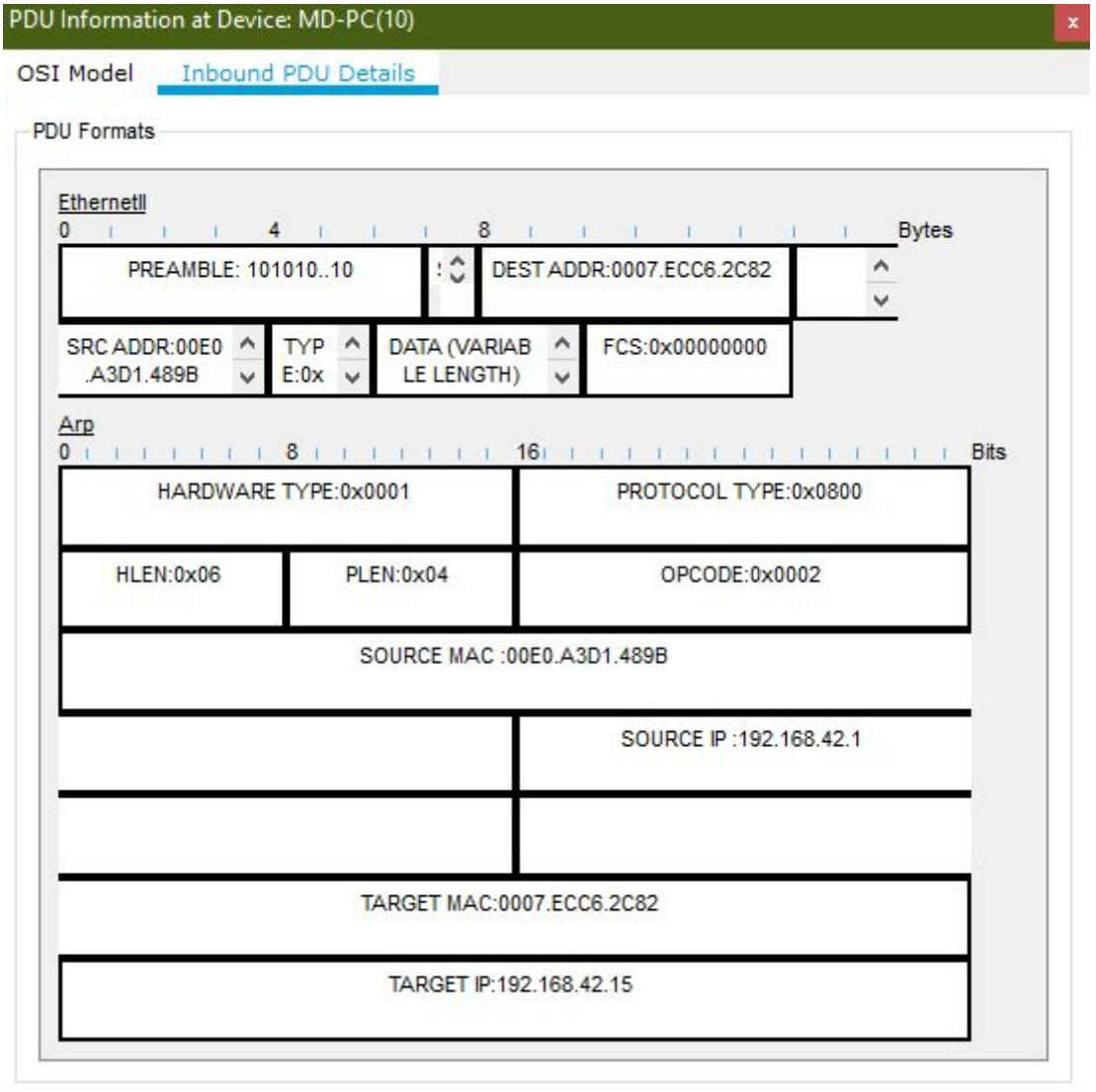
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1025, Dst Port: 110
Layer3	Layer 3: IP Header Src. IP: 192.168.7.11, Dest. IP: 192.168.1.3
Layer2	Layer 2: Wireless
Layer1	Layer 1: Port(s):

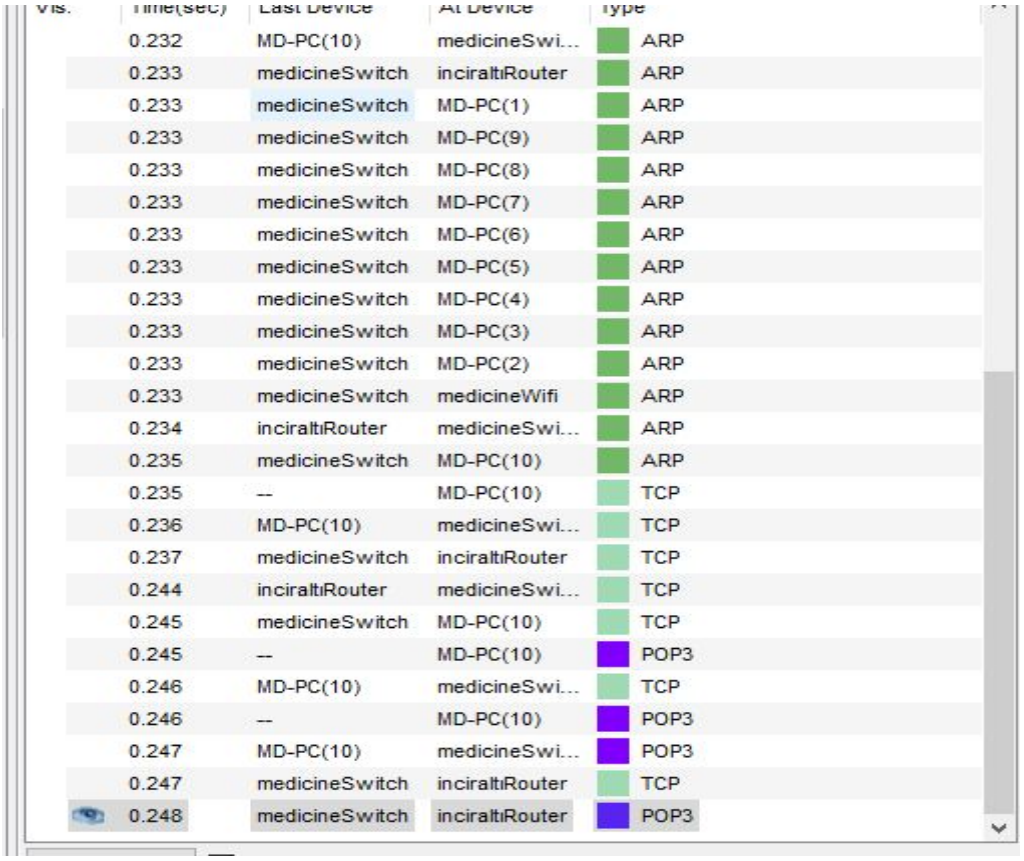
1. The device closes the TCP connection to 192.168.1.3 on port 110.
2. The device sets the connection state to FIN_WAIT_1.
3. The device sends a TCP FIN+ACK segment.
4. Sent segment information: the sequence number 1, the ACK number 0, and the data length 20.




Simulation Panel
Event List
Vis.
Time(sec)
Last Device
At Device
Type
25.428 eeSwitch EENG wireless TCP
25.429 EENG wireless EE-wifi(2) TCP
25.429 EENG wireless EE-wifi(4) TCP
25.429 EENG wireless EE-wifi(3) TCP
25.429 EENG wireless EE-wifi(5) TCP
25.429 EENG wireless EE-tablet(2) TCP
25.429 EENG wireless EE-wifi(1) TCP
25.429 EENG wireless EE-tablet(1) TCP
25.429 EENG wireless EE-tablet(3) TCP
25.429 EENG wireless EE-tablet(5) TCP
25.429 EENG wireless EE-tablet(4) TCP
25.430 -- EE-tablet(2) TCP
25.431 EE-tablet(2) EENG wireless TCP
25.432 EENG wireless eeSwitch TCP
25.432 -- EENG wireless TCP
25.433 EENG wireless EE-wifi(2) TCP
25.433 EENG wireless EE-wifi(4) TCP
25.433 EENG wireless EE-wifi(3) TCP
25.433 EENG wireless EE-wifi(5) TCP
25.433 EENG wireless EE-tablet(2) TCP
25.433 EENG wireless EE-wifi(1) TCP
25.433 EENG wireless EE-tablet(1) TCP
25.433 EENG wireless EE-tablet(3) TCP
25.433 EENG wireless EE-tablet(5) TCP
25.433 EENG wireless EE-tablet(4) TCP
Reset Simulation
Constant Delay
Captured to:
25.433 s
Play Controls

Scenario 8 : Sending email from third facility of first campus to first facility of first campus.





Vis.	Time(sec)	Last Device	At Device	Type
	0.232	MD-PC(10)	medicineSwi...	ARP
	0.233	medicineSwitch	inciraltiRouter	ARP
	0.233	medicineSwitch	MD-PC(1)	ARP
	0.233	medicineSwitch	MD-PC(9)	ARP
	0.233	medicineSwitch	MD-PC(8)	ARP
	0.233	medicineSwitch	MD-PC(7)	ARP
	0.233	medicineSwitch	MD-PC(6)	ARP
	0.233	medicineSwitch	MD-PC(5)	ARP
	0.233	medicineSwitch	MD-PC(4)	ARP
	0.233	medicineSwitch	MD-PC(3)	ARP
	0.233	medicineSwitch	MD-PC(2)	ARP
	0.233	medicineSwitch	medicineWifi	ARP
	0.234	inciraltiRouter	medicineSwi...	ARP
	0.235	medicineSwitch	MD-PC(10)	ARP
	0.235	--	MD-PC(10)	TCP
	0.236	MD-PC(10)	medicineSwi...	TCP
	0.237	medicineSwitch	inciraltiRouter	TCP
	0.244	inciraltiRouter	medicineSwi...	TCP
	0.245	medicineSwitch	MD-PC(10)	TCP
	0.245	--	MD-PC(10)	POP3
	0.246	MD-PC(10)	medicineSwi...	TCP
	0.246	--	MD-PC(10)	POP3
	0.247	MD-PC(10)	medicineSwi...	POP3
	0.247	medicineSwitch	inciraltiRouter	TCP
	0.248	medicineSwitch	inciraltiRouter	POP3

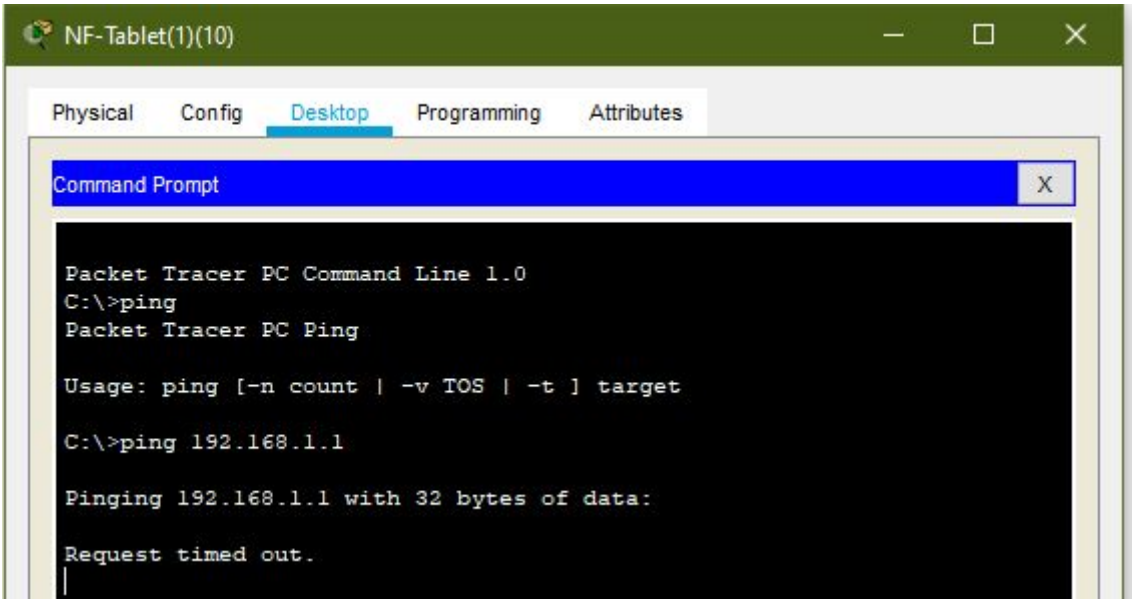
PDU Information at Device: MD-PC(10)

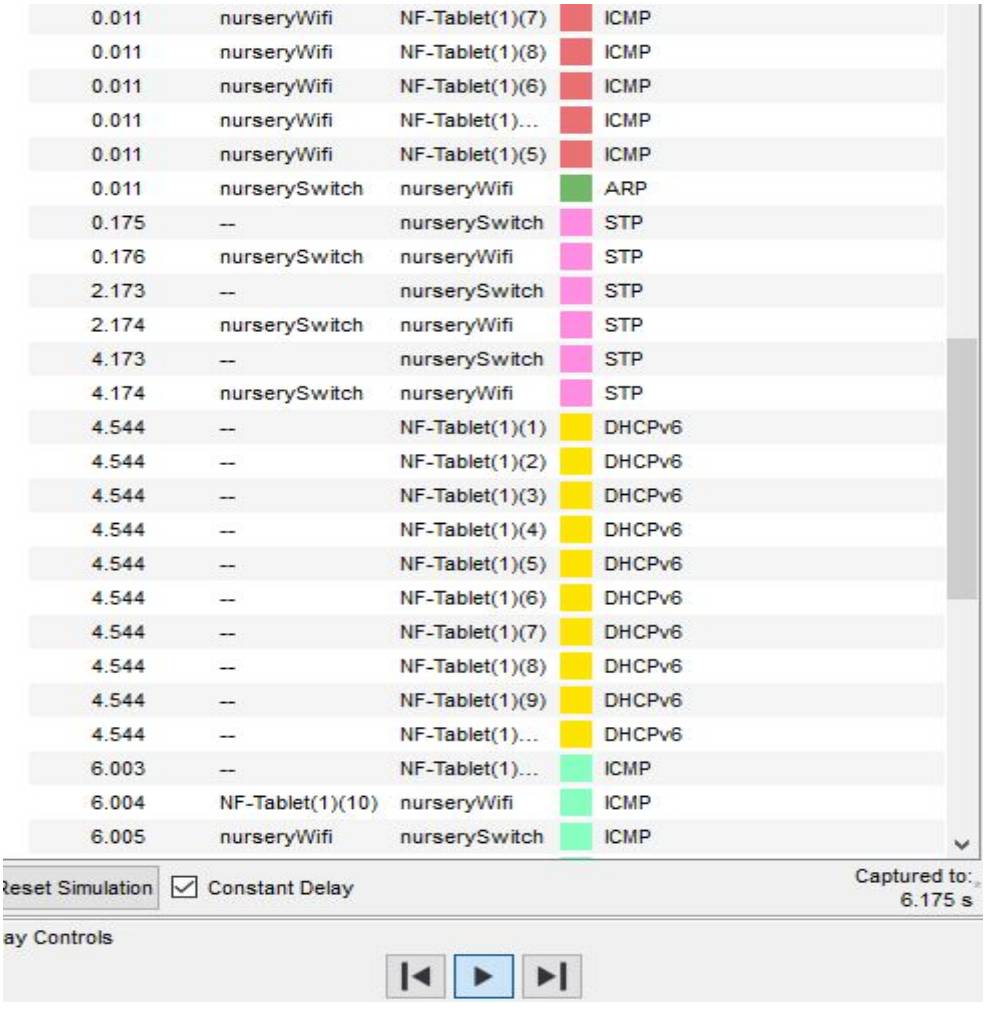
OSI Model | Inbound PDU Details

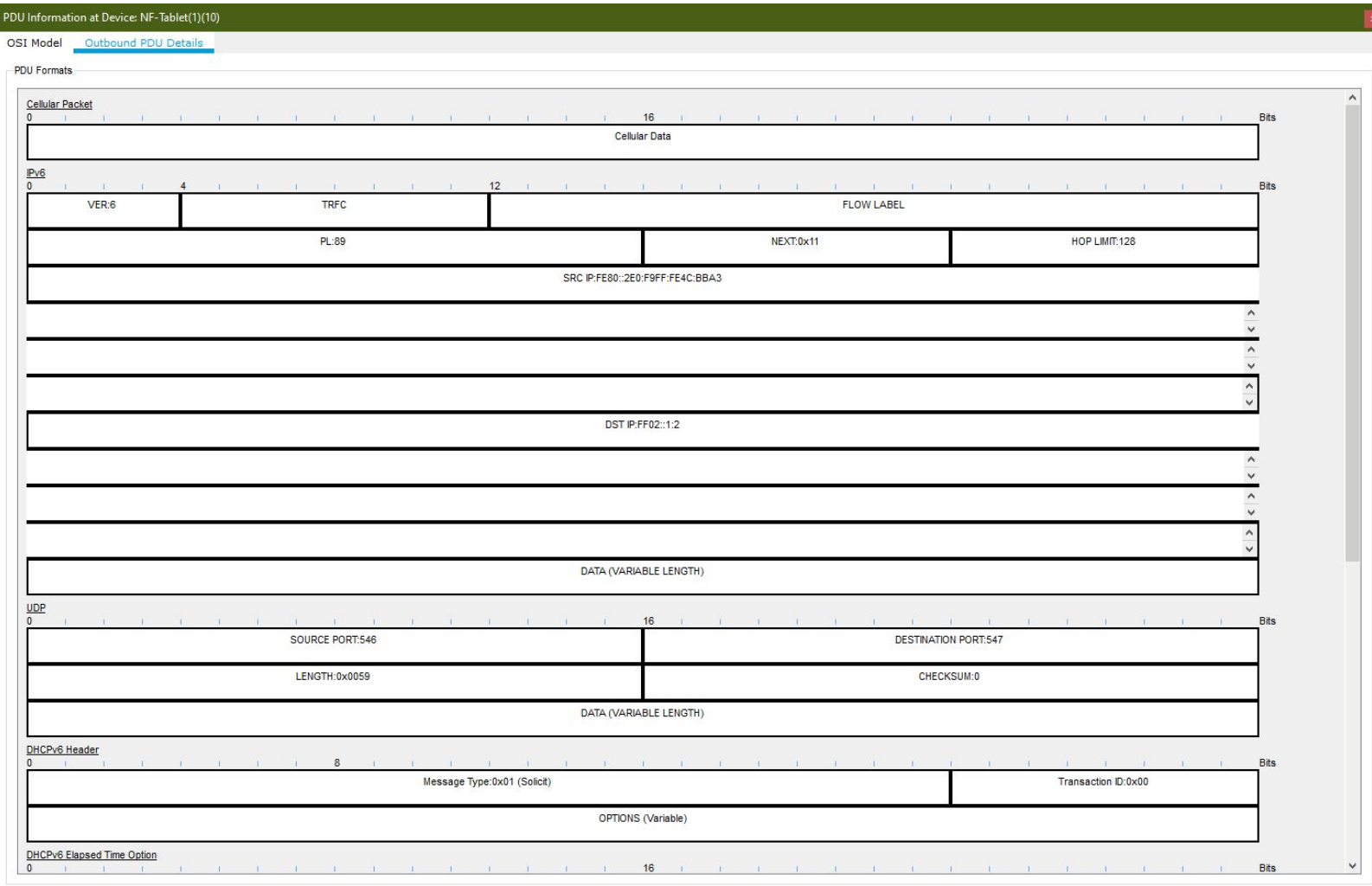
At Device: MD-PC(10)
Source: MD-PC(10)
Destination: Broadcast

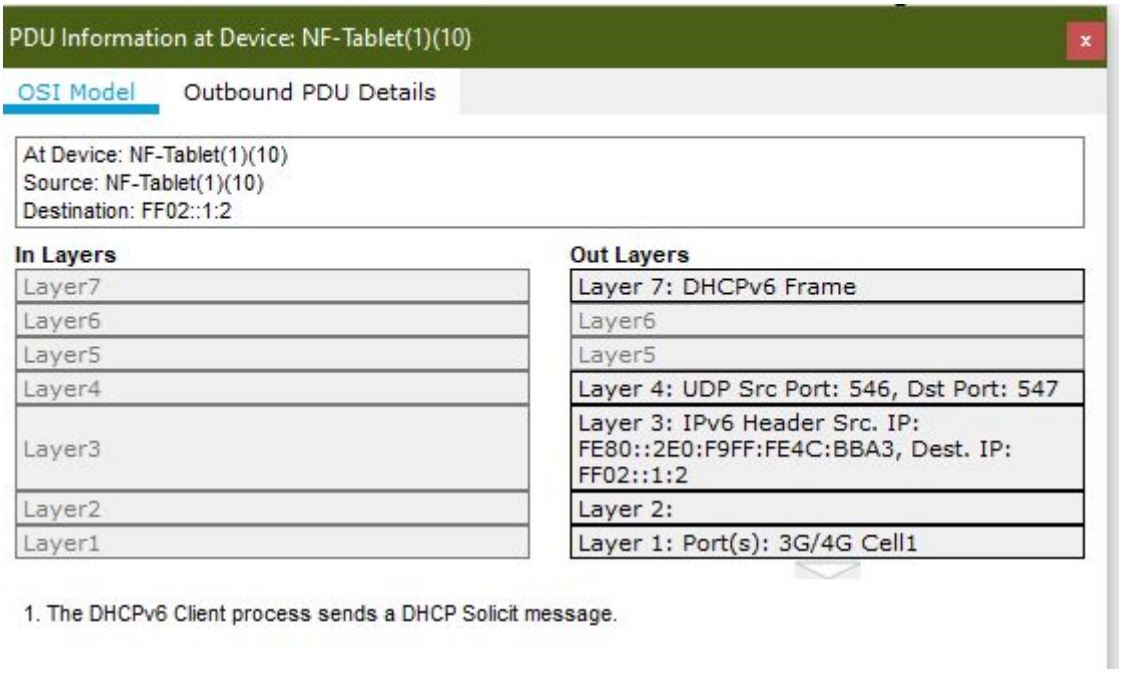
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 00E0.A3D1.489B >> 0007.ECC6.2C82 ARP Packet Src. IP: 192.168.42.1, Dest. IP: 192.168.42.15	Layer2
Layer 1: Port FastEthernet0	Layer1

Scenario 9 : Pinging the pc that is in the third facility of second campus from a tablet which is in the third facility of first campus.

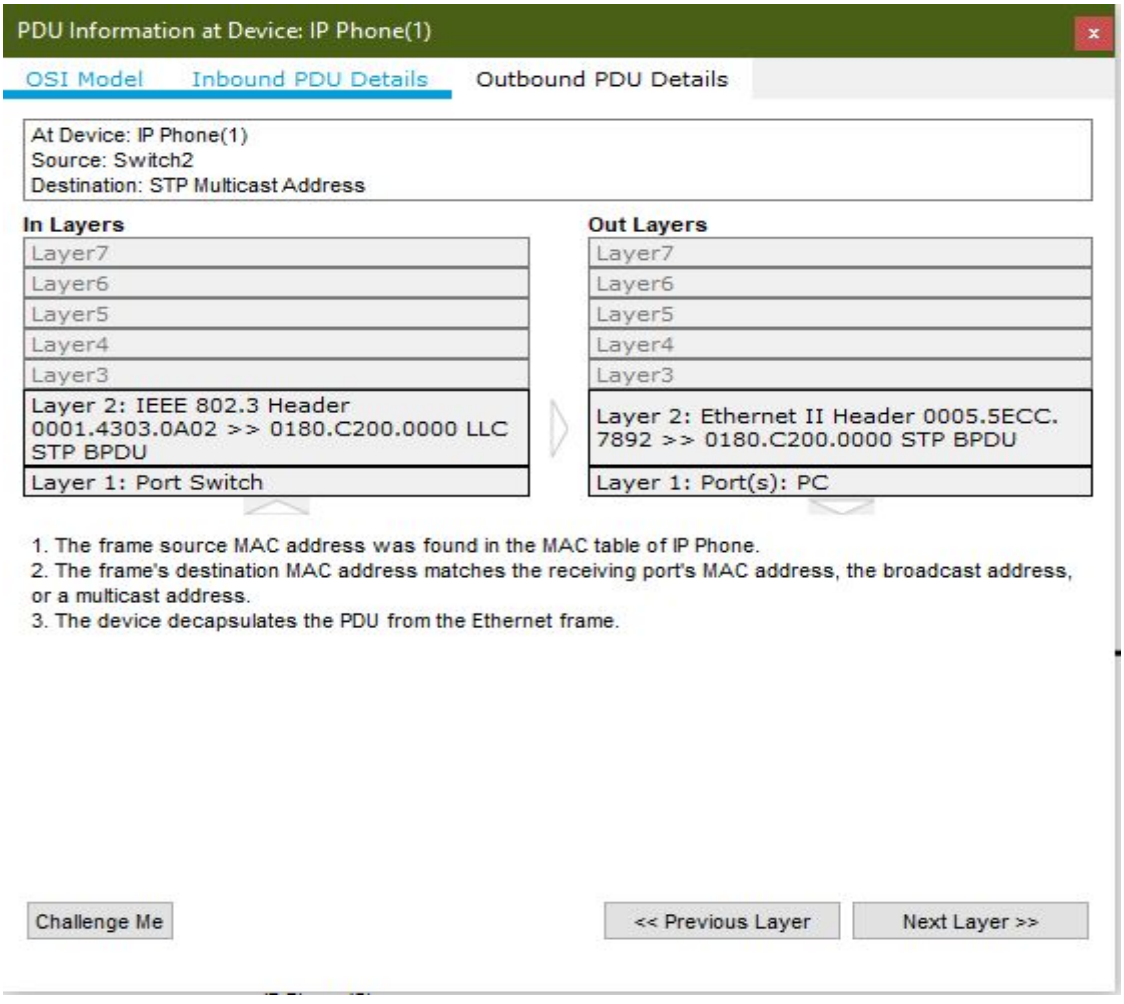





PDU Information at Device: NF-Tablet(1)(10)
OSI Model
Outbound PDU Details
PDU Formats
Cellular Packet
0
16
Bits
Cellular Data
IPv6
0
4
12
Bits
VER:6
TRFC
FLOW LABEL
PL:89
NEXT:0x11
HOP LIMIT:128
SRC IP:FE80::2E0:F9FF:FE4C:BBA3
DST IP:FF02::1:2
DATA (VARIABLE LENGTH)
UDP
0
16
Bits
SOURCE PORT:546
DESTINATION PORT:547
LENGTH:0x0059
CHECKSUM:0
DATA (VARIABLE LENGTH)
DHCPv6 Header
0
8
Bits
Message Type:0x01 (Solicit)
Transaction ID:0x00
OPTIONS (Variable)
DHCPv6 Elapsed Time Option
0
16
Bits


PDU Information at Device: NF-Tablet(1)(10)
OSI Model
Outbound PDU Details
At Device: NF-Tablet(1)(10)
Source: NF-Tablet(1)(10)
Destination: FF02::1:2
In Layers
Out Layers
Layer7
Layer 7: DHCPv6 Frame
Layer6
Layer6
Layer5
Layer5
Layer4
Layer 4: UDP Src Port: 546, Dst Port: 547
Layer3
Layer 3: IPv6 Header Src. IP: FE80::2E0:F9FF:FE4C:BBA3, Dest. IP: FF02::1:2
Layer2
Layer 2:
Layer1
Layer 1: Port(s): 3G/4G Cell1
1. The DHCPv6 Client process sends a DHCP Solicit message.

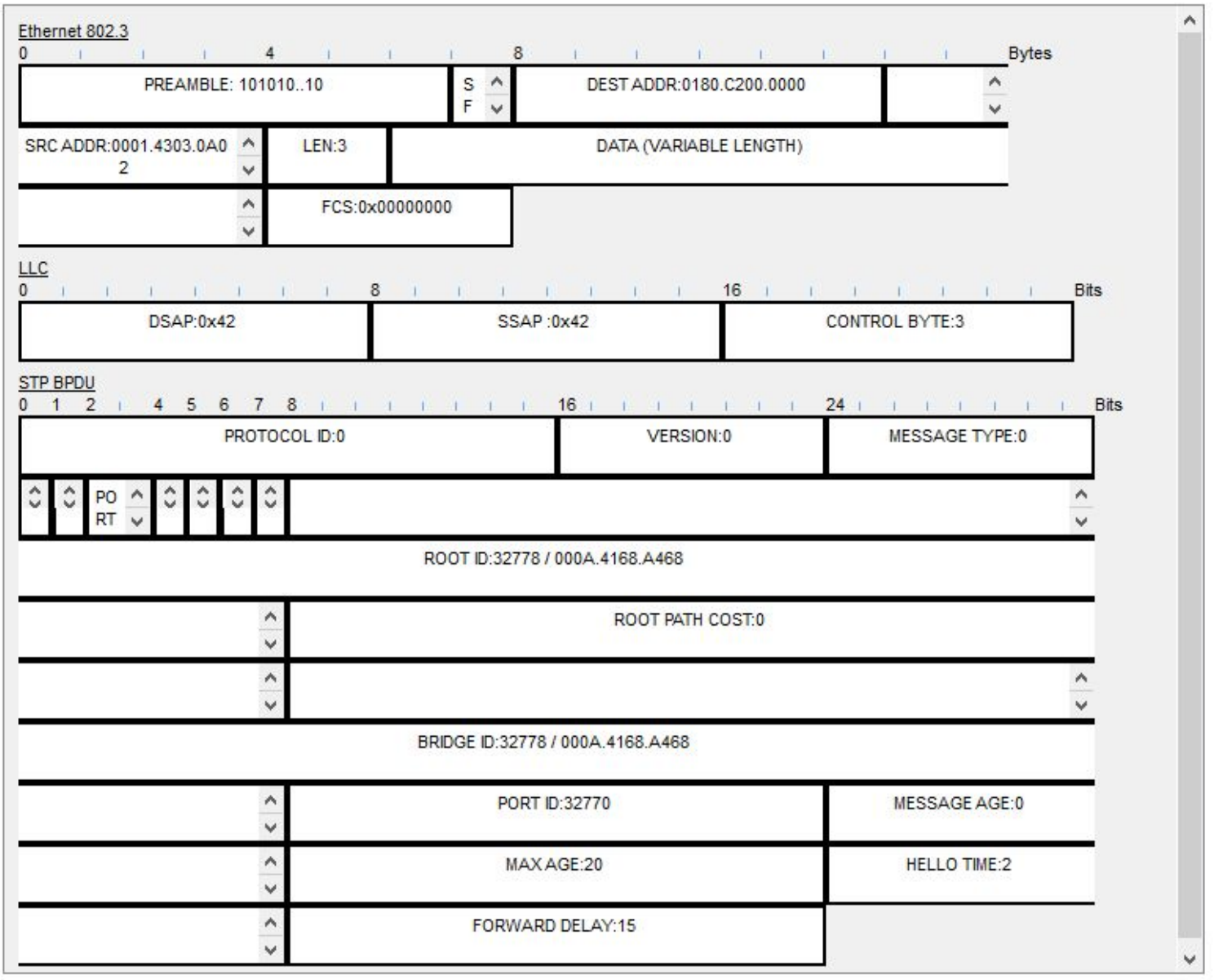
Scenario 10 : Using VoIP protocol of a workstation that is in the second facility of second campus.

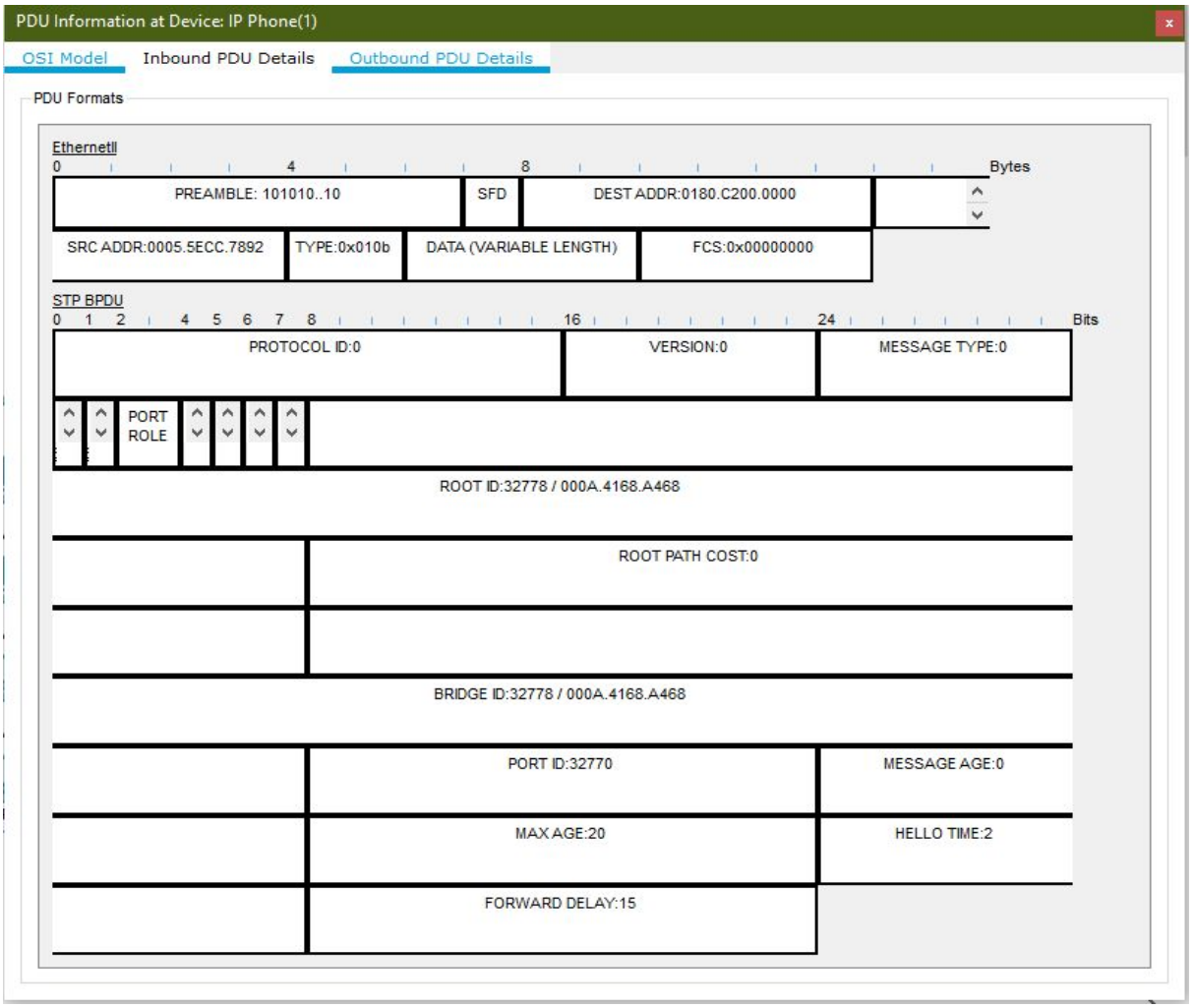


PDU Information at Device: IP Phone(1)

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats





5.987	IP Phone(1)	voip(1)		STP
5.987	IP Phone(4)	voip(4)		STP
5.987	IP Phone(2)	voip(2)		STP
5.987	IP Phone(5)	voip(5)		STP
5.987	IP Phone(3)	voip(3)		STP
6.041	--	Switch2		STP
6.042	Switch2	IP Phone(1)		STP
6.042	Switch2	Router2		STP
6.042	Switch2	IP Phone(4)		STP
6.042	Switch2	IP Phone(2)		STP
6.042	Switch2	IP Phone(5)		STP
6.042	Switch2	IP Phone(3)		STP
6.043	IP Phone(1)	voip(1)		STP
6.043	IP Phone(4)	voip(4)		STP
6.043	IP Phone(2)	voip(2)		STP
6.043	IP Phone(5)	voip(5)		STP
6.043	IP Phone(3)	voip(3)		STP
6.056	Switch2	Router2		STP
6.088	--	Switch2		STP
6.089	Switch2	Router2		STP
6.089	--	Switch2		STP
6.090	Switch2	Router2		STP
6.151	--	nurserySwitch		STP
6.152	nurserySwitch	inciraltiRouter		STP

Reset Simulation | Constant Delay | Capturing...

CHAPTER FOUR

CONCLUSION

Analysis and tests on simulation show that topology and architecture selection is done correctly according to requirements. Using the metropolitan area network instead of the wide area network provided the desired security and speed. The network was successful in providing the desired services using the protocols specified in the report. As a result, networks created between the two campuses of the university and within the campuses themselves were successful. The project team has gained insights into the network design and the challenges it brings.

CHAPTER FIVE

REFERENCES

[1]https://en.wikipedia.org/wiki/Metropolitan_area_network

[2]https://www.ibm.com/cloud/learn/networking-a-complete-guide

[3]https://www.digitalocean.com/community/tutorials/an-introduction-to-networking-terminology-interfaces-and-protocols