

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.

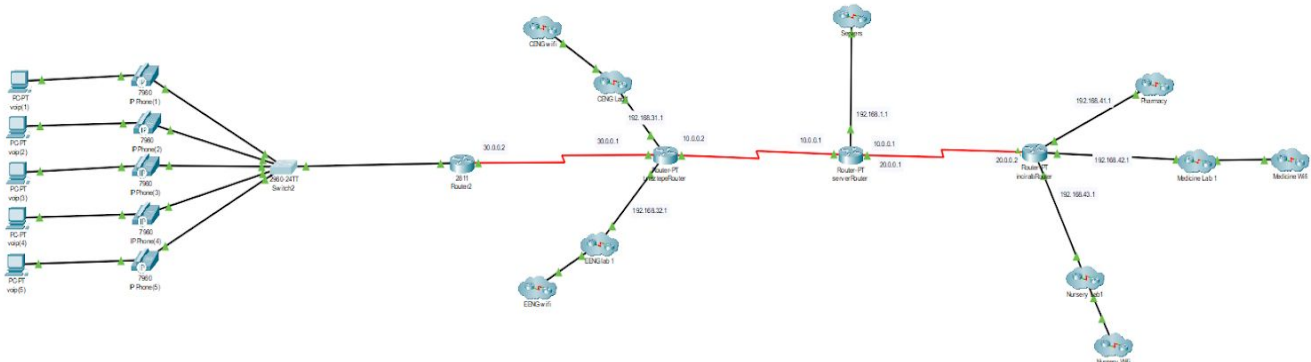
The mail server was authorized to send mail to all workstations in the first and third facilities of the first campus, to receive mail from workstations in the third facility of the first campus, and to use mail applications to the workstations in the first facility of the second campus.

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.

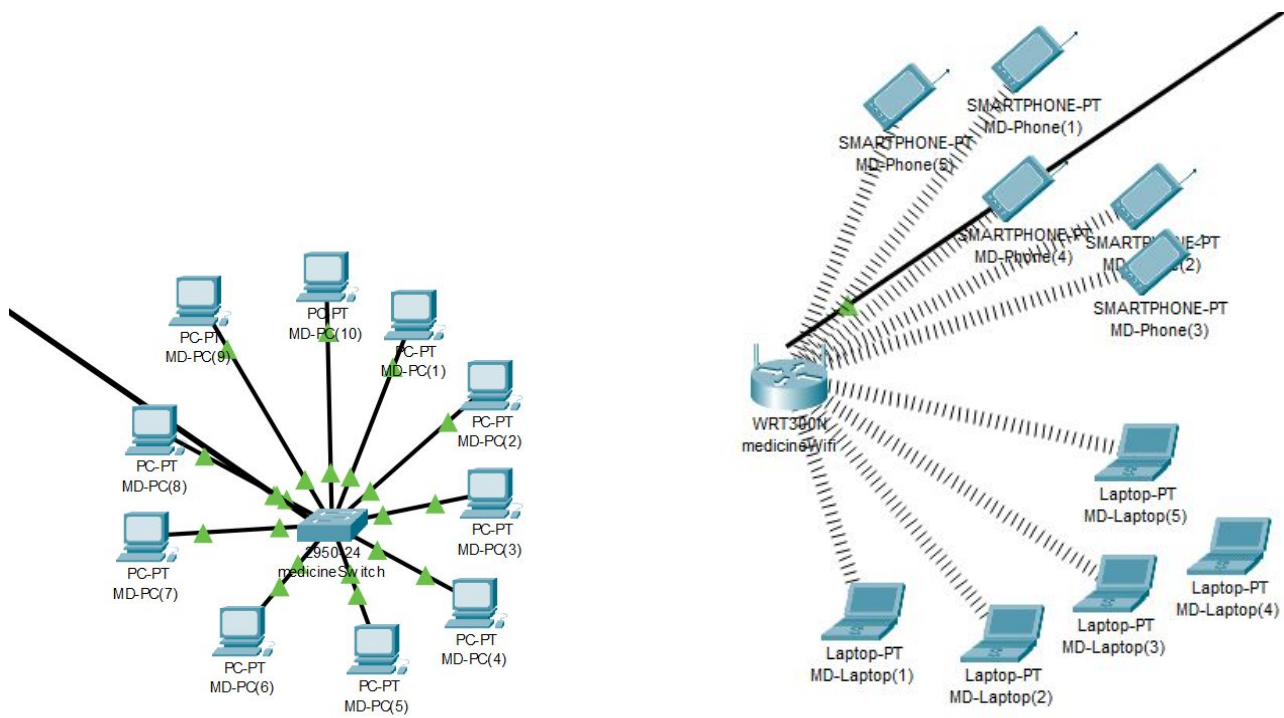
Workstations at the second facility of the first campus were given the authority to use the database, and workstations at the second facility of the second campus were allowed to organize files and applications.

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.

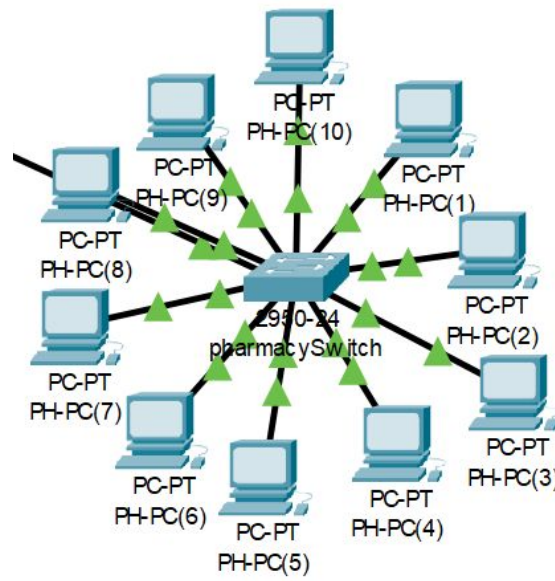
2.5. Definitions of the System/Model



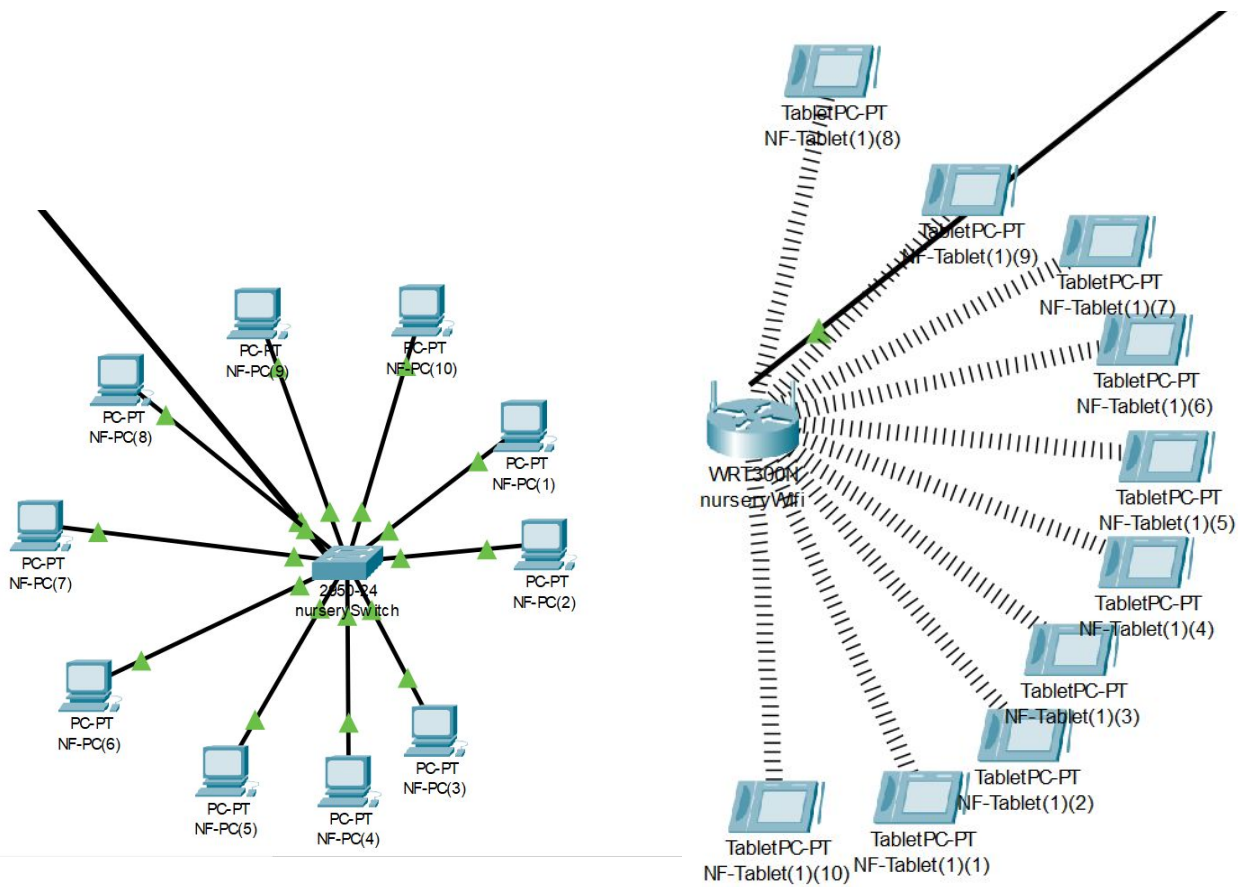
General Shape of The System



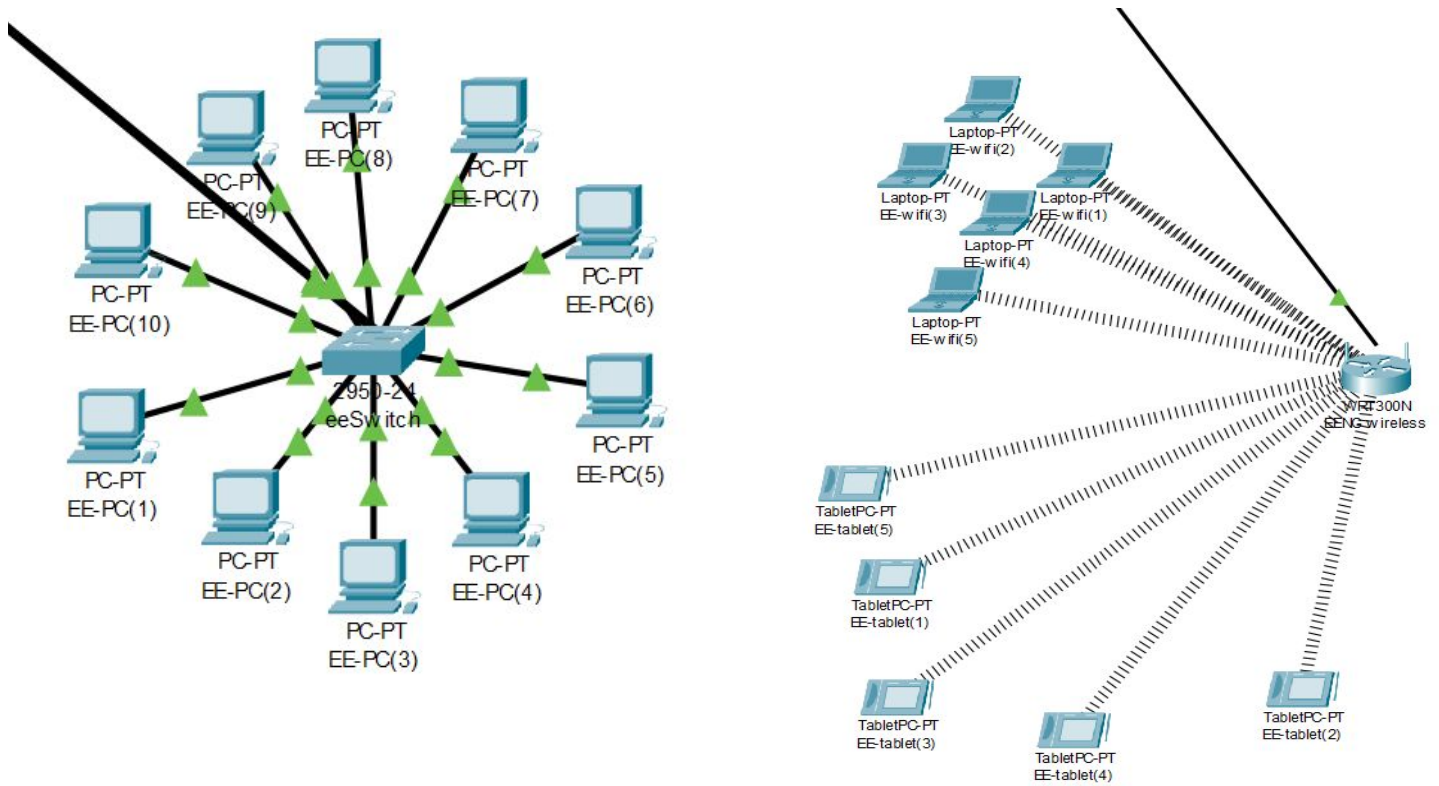
First Campus First Facility



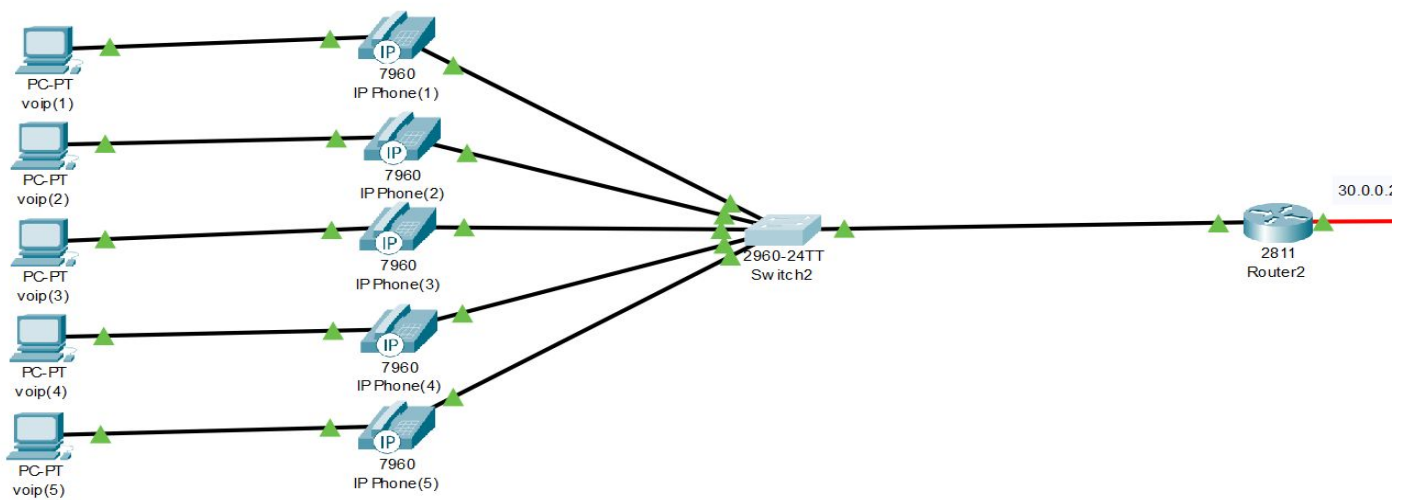
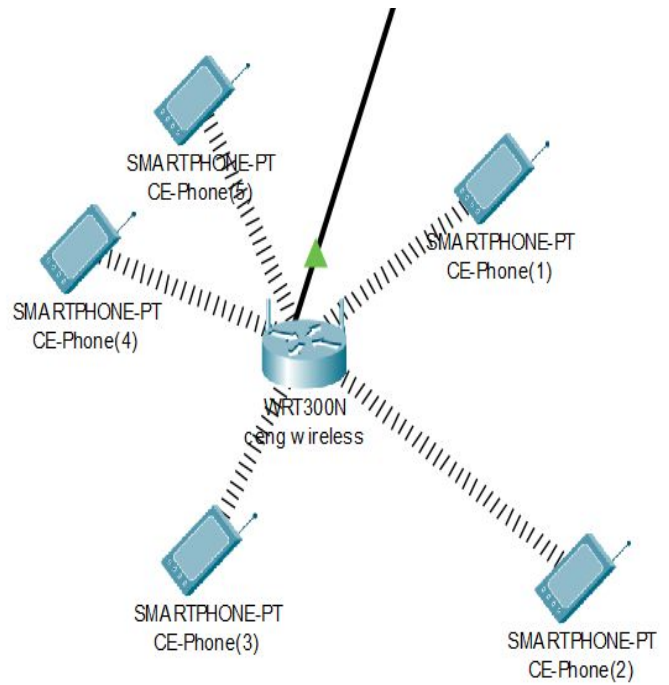
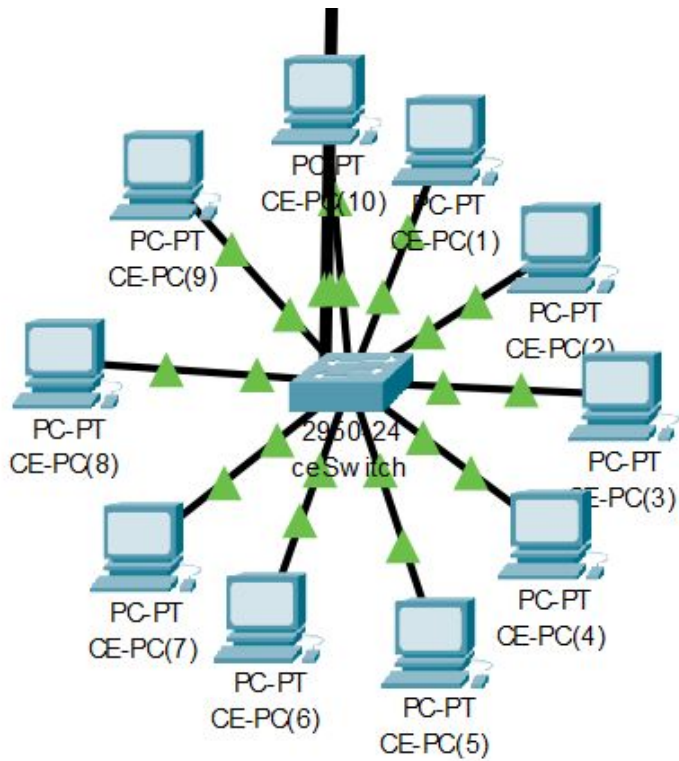
First Campus Second Facility



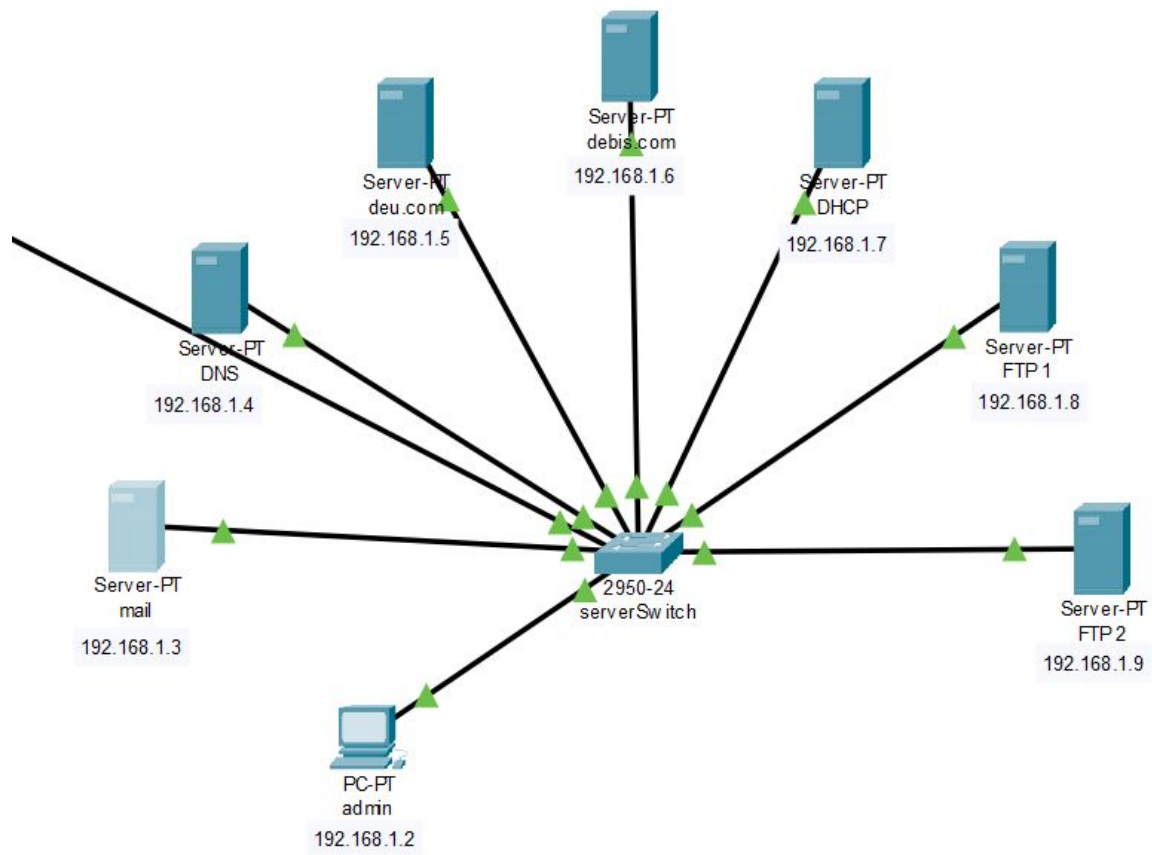
First Campus Third Facility



Second Campus First Facility

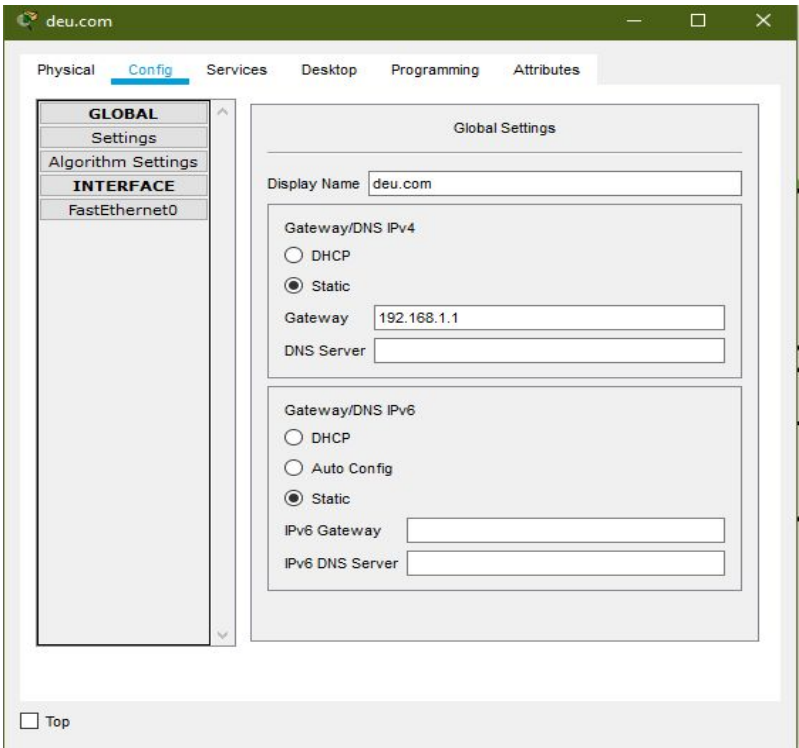


Second Campus Second Facility

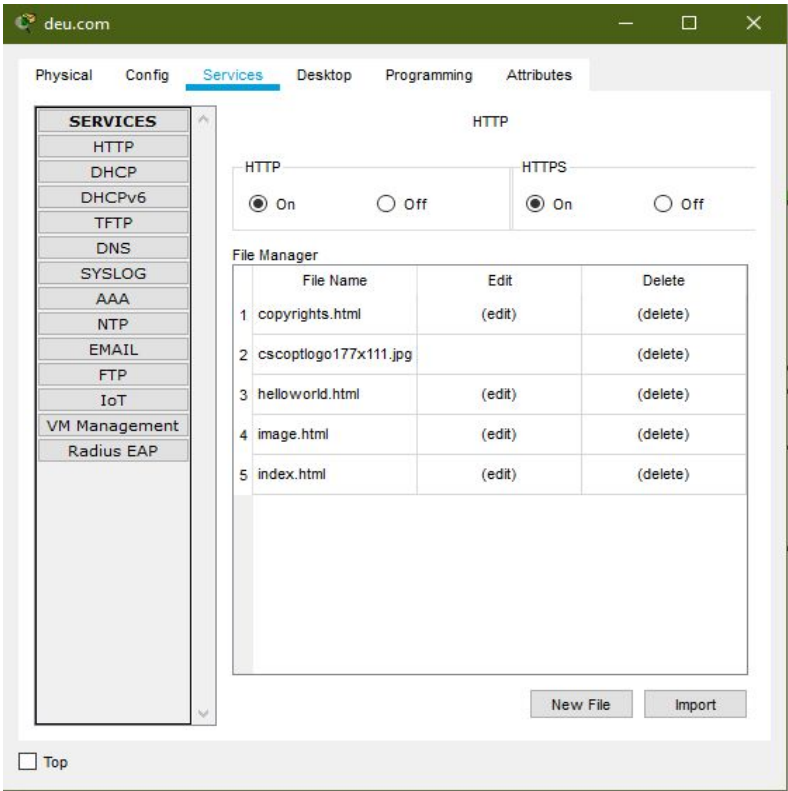


Second Campus Third Facility

2.6. Simulation Elements



HTTP1 Server Config



HTTP1 Server Services

debis.com

Physical **Config** Services Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Global Settings

Display Name

Gateway/DNS IPv4

☐ DHCP

☒ Static

Gateway

DNS Server

Gateway/DNS IPv6

☐ DHCP

☐ Auto Config

☒ Static

IPv6 Gateway

IPv6 DNS Server

☐ Top

HTTP2 Server Config

debis.com

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

HTTP

HTTP ☒ On ☐ Off

HTTPS ☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoplogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

☐ Top

HTTP2 Server Services

FTP 1

Physical **Config** Services Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Global Settings

Display Name

Gateway/DNS IPv4

☐ DHCP

☒ Static

Gateway

DNS Server

Gateway/DNS IPv6

☐ DHCP

☐ Auto Config

☒ Static

IPv6 Gateway

IPv6 DNS Server

☐ Top

FTP1 Server Config

FTP 1

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

HTTP

HTTP ☐ On ☒ Off

HTTPS ☐ On ☒ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

☐ Top

FTP1 Server Service

Physical **Config** Services Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings
- INTERFACE**
- FastEthernet0

Global Settings

Display Name:

Gateway/DNS IPv4

☐ DHCP

☒ Static

Gateway:

DNS Server:

Gateway/DNS IPv6

☐ DHCP

☐ Auto Config

☒ Static

IPv6 Gateway:

IPv6 DNS Server:

☐ Top

FTP2 Server Config

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

HTTP

HTTP: ☐ On ☒ Off

HTTPS: ☐ On ☒ Off

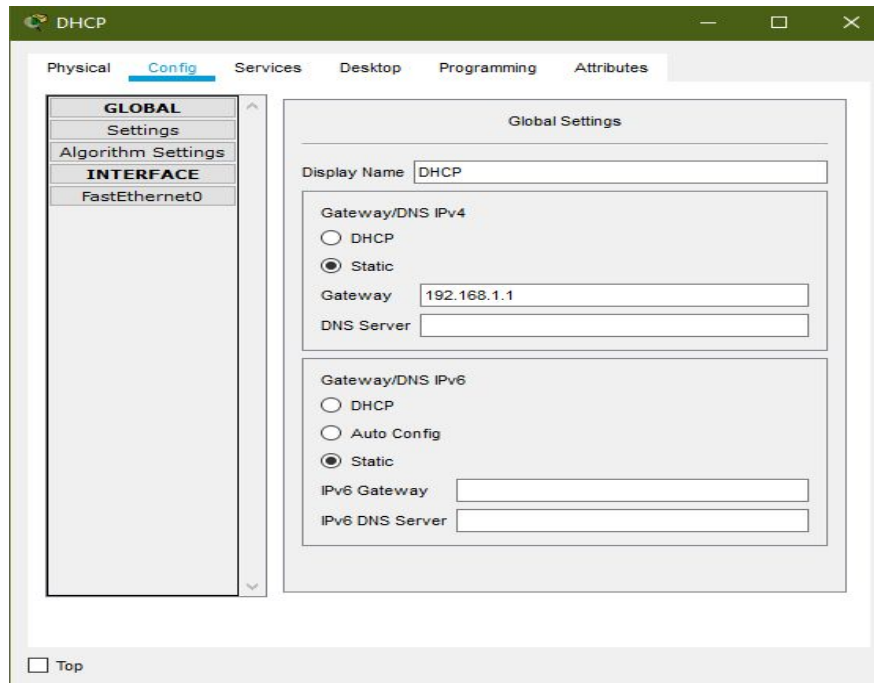
File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

☐ Top

New File Import

FTP2 Server Service

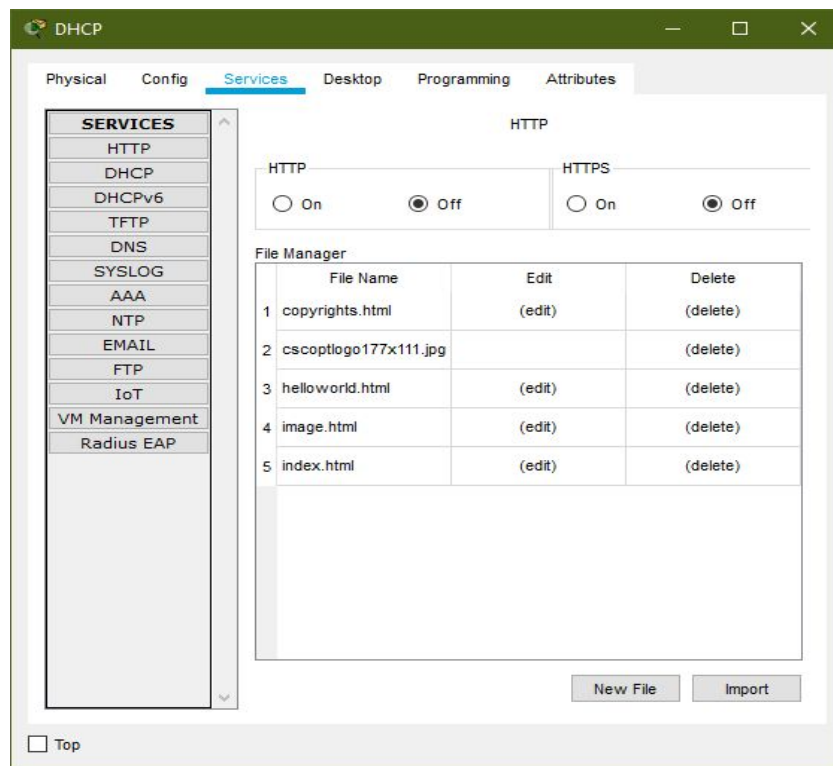


The screenshot shows the DHCP configuration window with the 'Config' tab selected. The left sidebar lists 'GLOBAL' settings, including 'Settings', 'Algorithm Settings', and 'INTERFACE' (FastEthernet0). The main area is titled 'Global Settings' and contains the following fields:

- Display Name:** DHCP
- Gateway/DNS IPv4:**
 - ☐ DHCP
 - ☒ Static
 - Gateway:** 192.168.1.1
 - DNS Server:** (empty field)
- Gateway/DNS IPv6:**
 - ☐ DHCP
 - ☐ Auto Config
 - ☒ Static
 - IPv6 Gateway:** (empty field)
 - IPv6 DNS Server:** (empty field)

At the bottom left, there is a 'Top' button.

DHCP Server Config



The screenshot shows the DHCP configuration window with the 'Services' tab selected. The left sidebar lists 'SERVICES' including HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'HTTP' and contains the following fields:

- HTTP:** ☐ On ☒ Off
- HTTPS:** ☐ On ☒ Off
- File Manager:**

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

At the bottom right, there are 'New File' and 'Import' buttons. At the bottom left, there is a 'Top' button.

DHCP Server Service

The screenshot shows the 'DNS' configuration window with the 'Config' tab selected. The left sidebar has a tree view with 'GLOBAL' expanded, showing 'Settings' and 'Algorithm Settings'. Below 'GLOBAL' is the 'INTERFACE' section with 'FastEthernet0' selected. The main area is titled 'Global Settings' and contains the following fields:

- Display Name:** DNS
- Gateway/DNS IPv4:**
 - ☐ DHCP
 - ☒ Static
 - Gateway:** 192.168.1.1
 - DNS Server:** (empty field)
- Gateway/DNS IPv6:**
 - ☐ DHCP
 - ☐ Auto Config
 - ☒ Static
 - IPv6 Gateway:** (empty field)
 - IPv6 DNS Server:** (empty field)

At the bottom left, there is a 'Top' button.

DNS Server Config

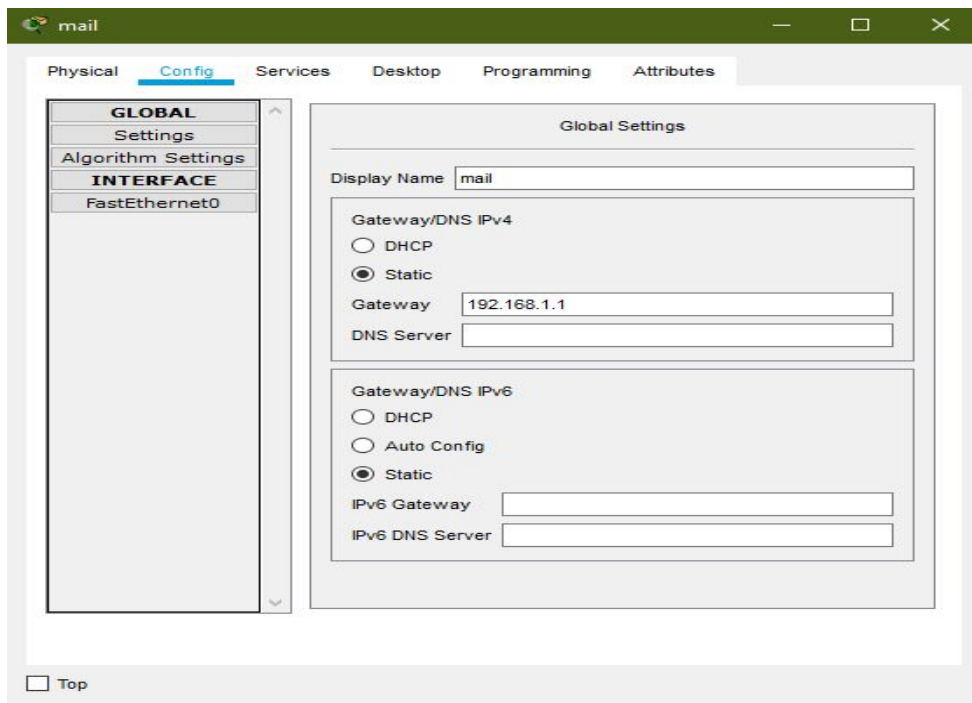
The screenshot shows the 'DNS' configuration window with the 'Services' tab selected. The left sidebar has a tree view with 'SERVICES' expanded, showing a list of services: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'HTTP' and contains the following fields:

- HTTP:**
 - ☐ On
 - ☒ Off
- HTTPS:**
 - ☐ On
 - ☒ Off
- File Manager:**

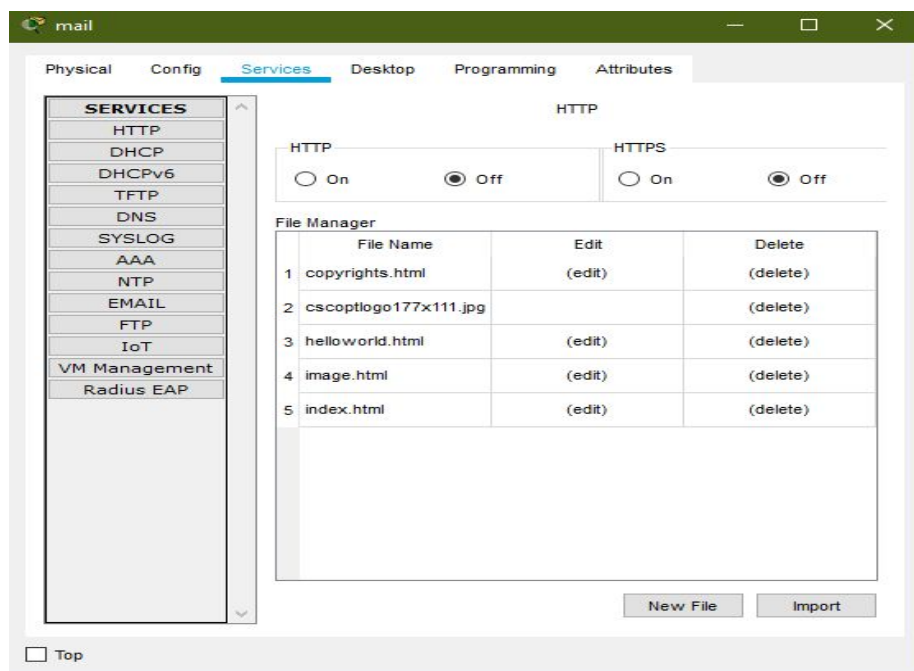
	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

At the bottom right, there are 'New File' and 'Import' buttons. At the bottom left, there is a 'Top' button.

DNS Server Service



MAIL Server Config

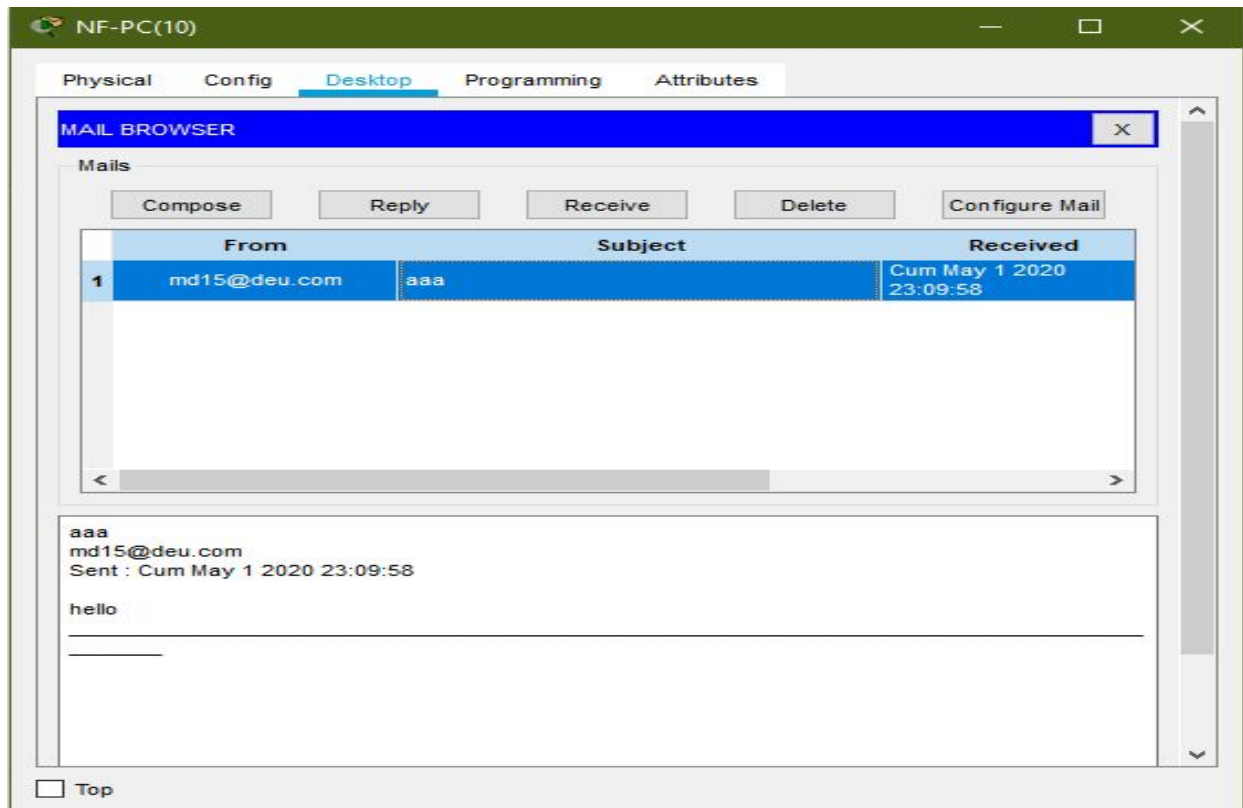


MAIL Server Service

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.



28.167	pharmacySwitch	PH-PC(6)	STP
28.640	--	nurserySwitch	STP
28.641	nurserySwitch	inciraltiRouter	STP
29.999	--	nurserySwitch	DTP
30.000	nurserySwitch	NF-PC(3)	DTP
30.001	--	nurserySwitch	DTP
30.001	--	NF-PC(10)	TCP
30.002	nurserySwitch	NF-PC(9)	DTP
30.002	NF-PC(10)	nurserySwitch	TCP
30.003	nurserySwitch	inciraltiRouter	TCP
30.004	--	nurserySwitch	DTP
30.005	nurserySwitch	NF-PC(1)	DTP
30.008	--	nurserySwitch	DTP
30.009	nurserySwitch	inciraltiRouter	DTP
30.010	--	nurserySwitch	DTP
30.010	inciraltiRouter	nurserySwitch	TCP

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

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

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

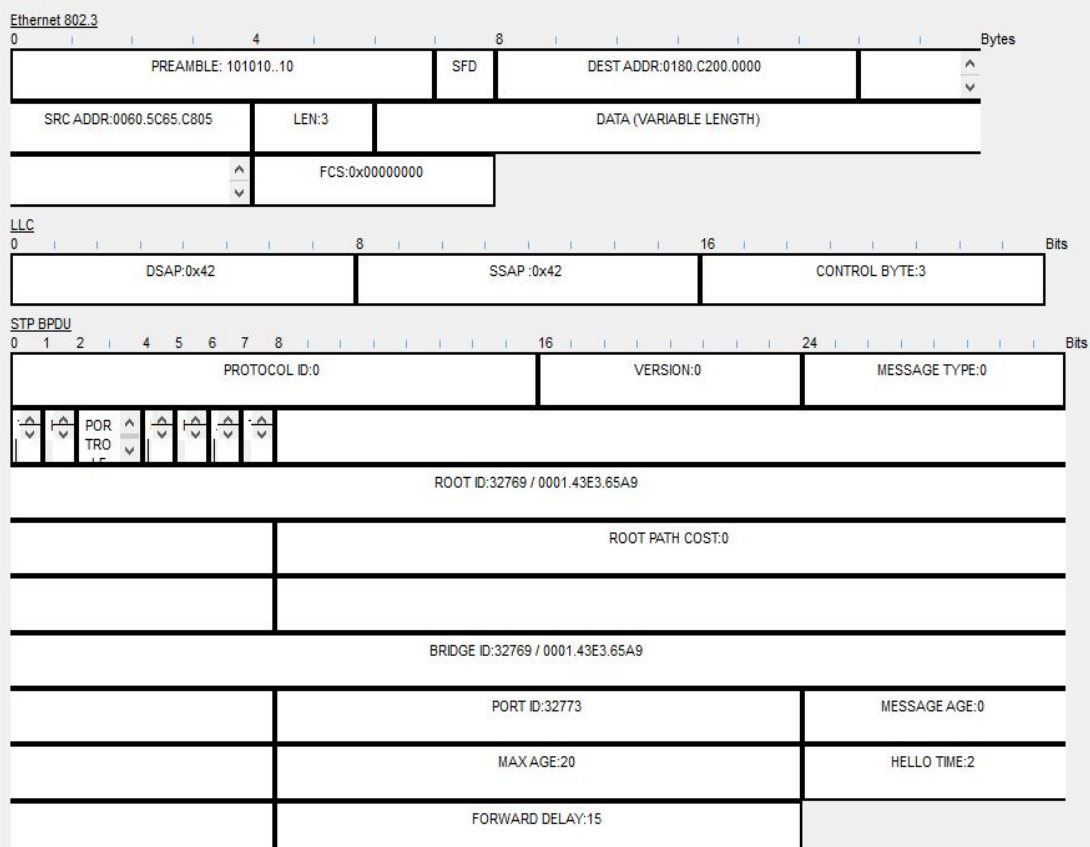
1. FastEthernet0 receives the frame.

PDU Information at Device: NF-PC(10)



OSI Model Inbound PDU Details

PDU Formats



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	inciraltiRouter	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	inciraltiRouter	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

At Device: PH-PC(1)
Source: pharmacySwitch
Destination: 0001.6448.0506

In 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

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
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.

PDU Information at Device: CE-PC(10)

OSI Model Inbound PDU Details

At Device: CE-PC(10)
Source: tinaztepeRouter
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0010.1112.A834 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.31.1, Dest. IP: 192.168.31.11	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

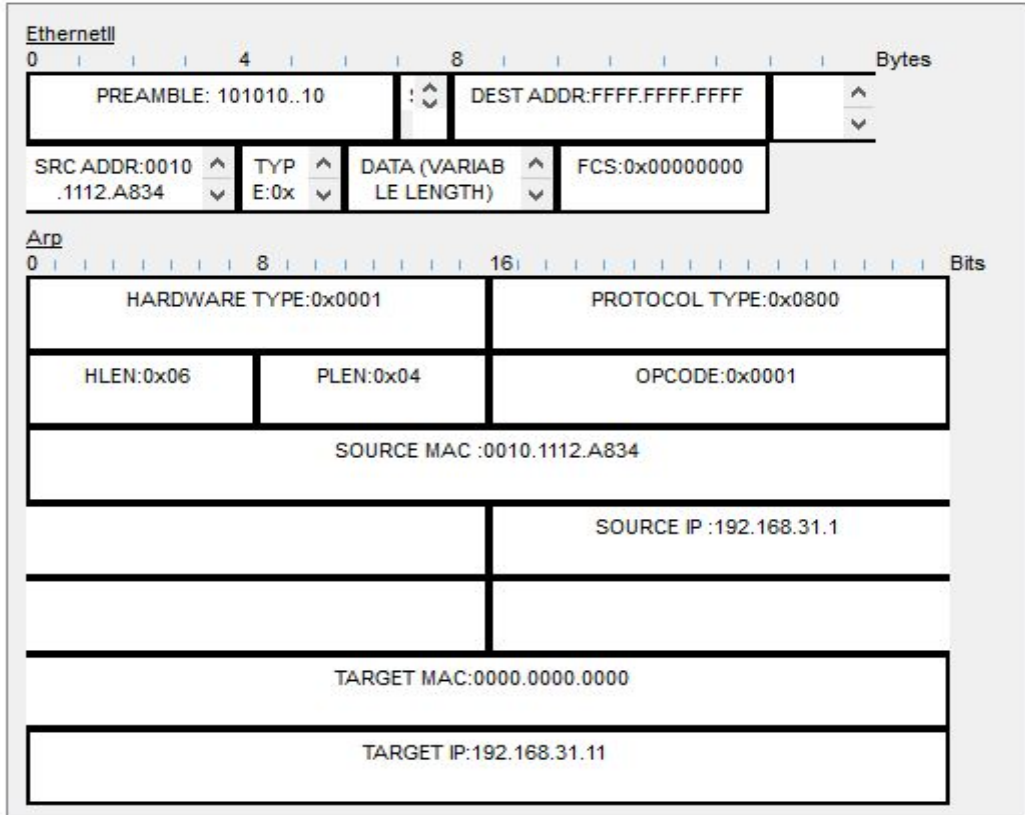
CE-PC(10)

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ftp ftpl.debis.com
Trying to connect...ftpl.debis.com
Could not open connection to the host, on port 21: Connect failed
C:\>
```


PDU Formats



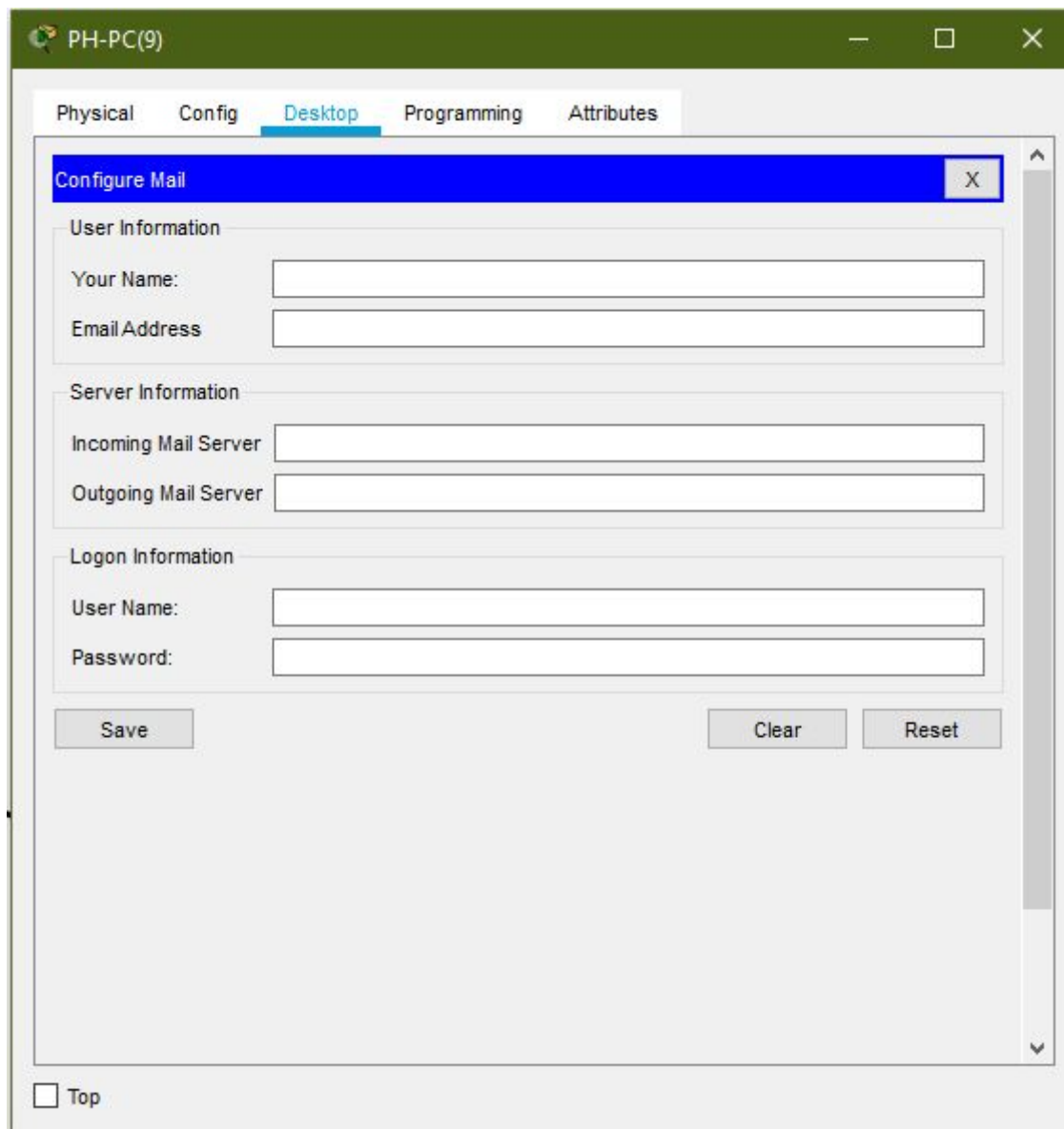
0.005	tinaztepeRouter	ceSwitch	ARP
0.006	ceSwitch	CE-PC(8)	ARP
0.006	ceSwitch	CE-PC(10)	ARP
0.006	ceSwitch	CE-PC(9)	ARP
0.006	ceSwitch	CE-PC(1)	ARP
0.006	ceSwitch	CE-PC(7)	ARP
0.006	ceSwitch	CE-PC(6)	ARP
0.006	ceSwitch	CE-PC(5)	ARP
0.006	ceSwitch	CE-PC(4)	ARP
0.006	ceSwitch	CE-PC(3)	ARP
0.006	ceSwitch	CE-PC(2)	ARP

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



Time(sec)	Left Device	Right Device	Type
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	inciraltRouter	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.



The image shows a screenshot of a web-based configuration interface for a device labeled "PH-PC(9)". The interface has a green header bar with the device name and standard window controls (minimize, maximize, close). Below the header, there are four tabs: "Physical", "Config", "Desktop" (which is selected and highlighted in blue), "Programming", and "Attributes".

The "Desktop" tab contains a "Configure Mail" dialog box. The dialog box has a blue title bar with the text "Configure Mail" and a close button (X). It is divided into three sections:

- User Information:** Contains two text input fields: "Your Name:" and "Email Address".
- Server Information:** Contains two text input fields: "Incoming Mail Server" and "Outgoing Mail Server".
- Logon Information:** Contains two text input fields: "User Name:" and "Password:".

At the bottom of the dialog box, there are three buttons: "Save", "Clear", and "Reset".

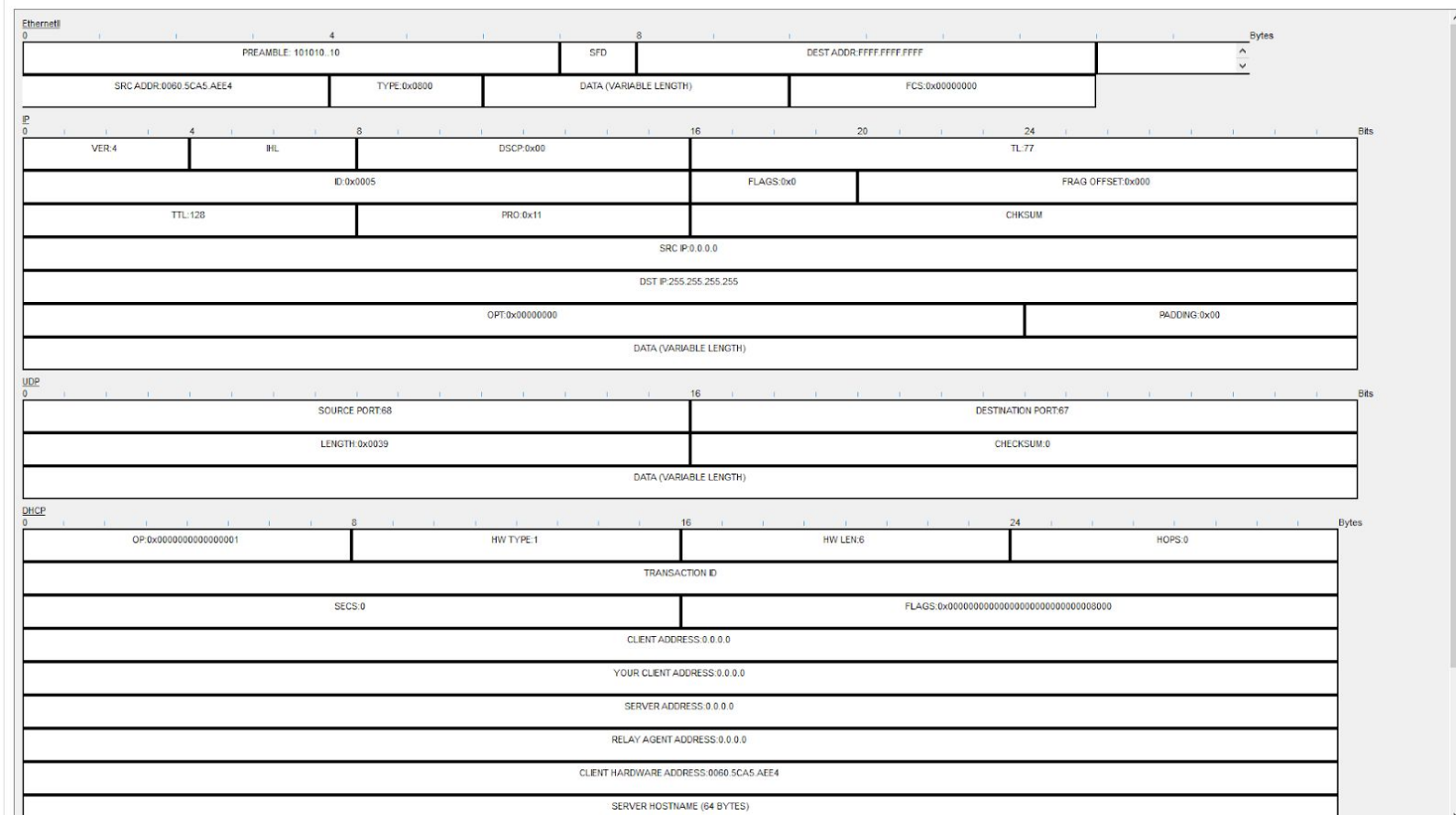
Below the dialog box, there is a checkbox labeled "Top".

x

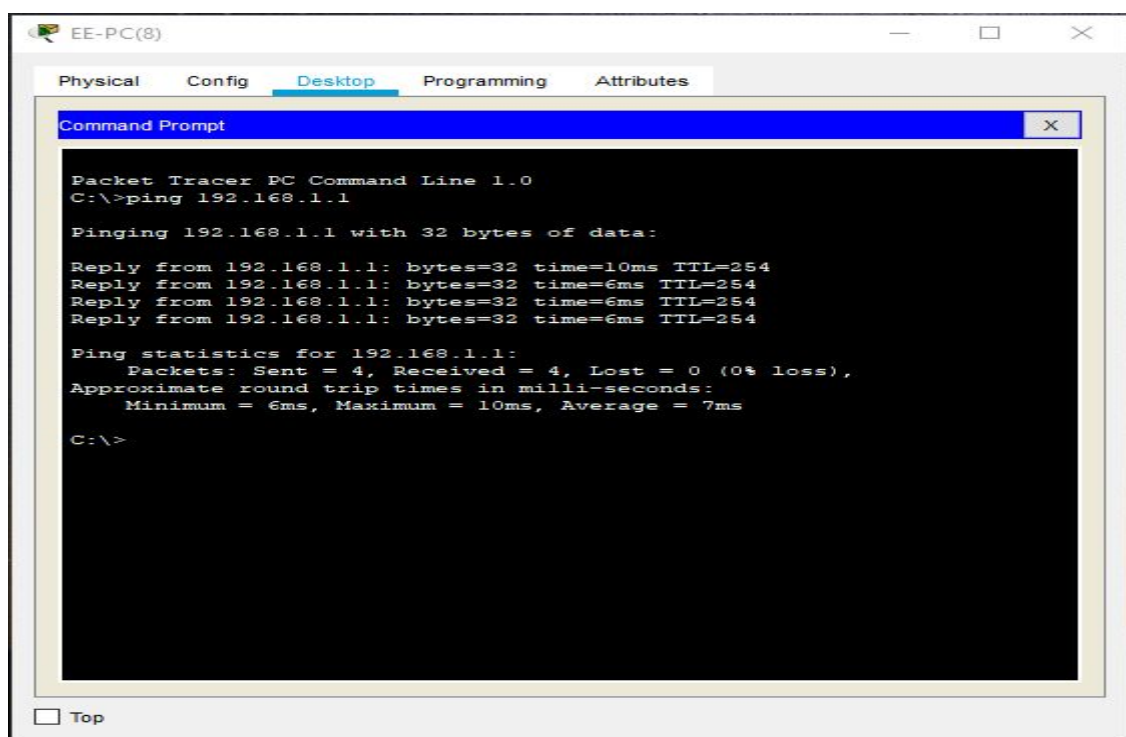
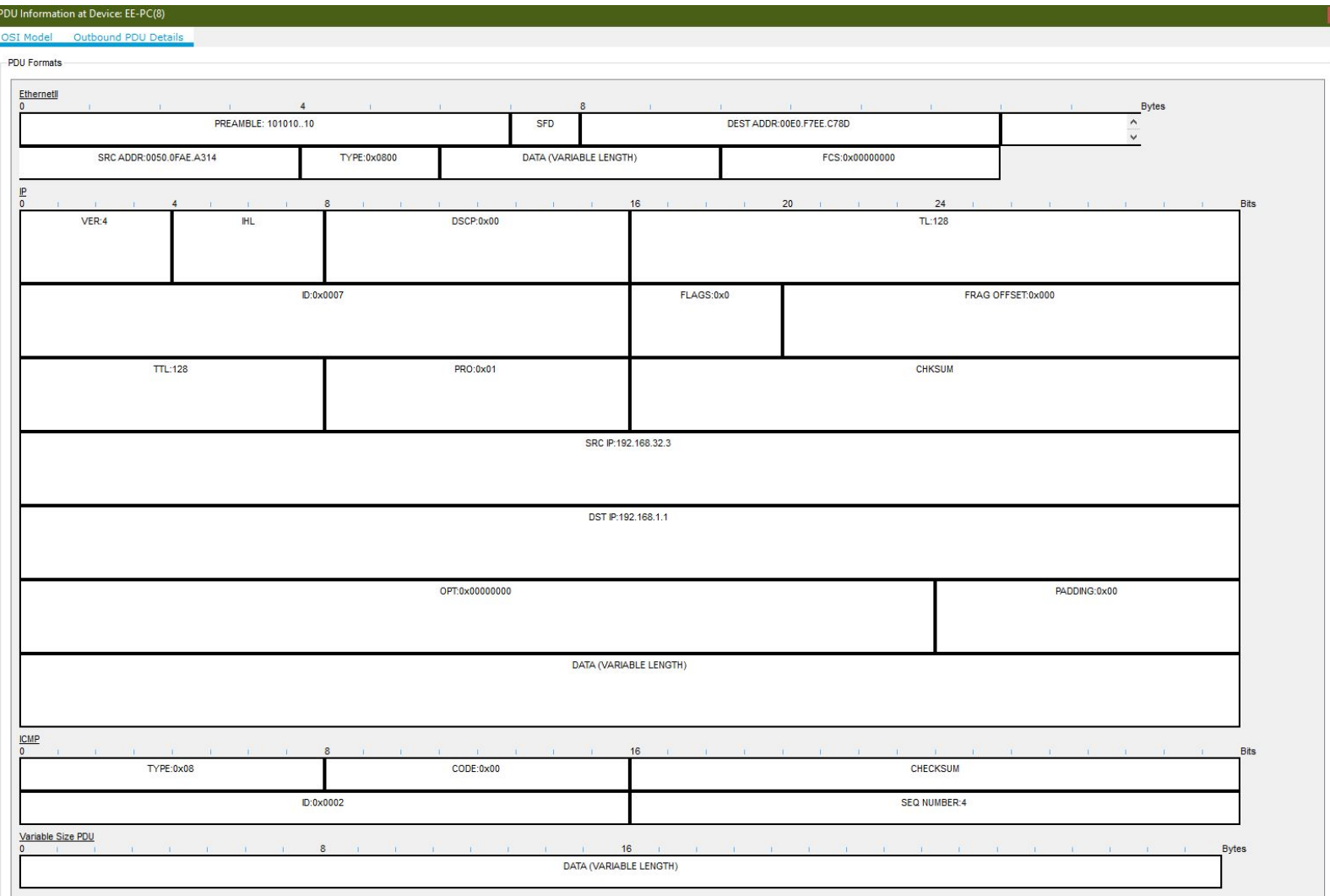
Outbound PDU Details

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

PDU Formats



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



Time	Time(sec)	Last Device	Next Device	Type
0.010	0.010	eeSwitch	EE-PC(8)	ICMP
0.217	0.217	--	eeSwitch	STP
0.218	0.218	eeSwitch	EE-PC(2)	STP
0.218	0.218	eeSwitch	tinaztepeRo...	STP
0.218	0.218	eeSwitch	EE-PC(7)	STP
0.218	0.218	eeSwitch	EE-PC(3)	STP
0.218	0.218	eeSwitch	EE-PC(6)	STP
0.218	0.218	eeSwitch	EE-PC(8)	STP
0.218	0.218	eeSwitch	EE-PC(5)	STP
0.218	0.218	eeSwitch	EE-PC(4)	STP
0.218	0.218	eeSwitch	EE-PC(10)	STP
0.218	0.218	eeSwitch	EE-PC(1)	STP
0.218	0.218	eeSwitch	EE-PC(9)	STP
0.218	0.218	eeSwitch	EENG wireless	STP
1.012	1.012	--	EE-PC(8)	ICMP
1.013	1.013	EE-PC(8)	eeSwitch	ICMP
1.014	1.014	eeSwitch	tinaztepeRo...	ICMP
1.017	1.017	tinaztepeRouter	eeSwitch	ICMP
1.018	1.018	eeSwitch	EE-PC(8)	ICMP
2.021	2.021	--	EE-PC(8)	ICMP
2.022	2.022	EE-PC(8)	eeSwitch	ICMP
2.023	2.023	eeSwitch	tinaztepeRo...	ICMP
2.026	2.026	tinaztepeRouter	eeSwitch	ICMP
2.027	2.027	eeSwitch	EE-PC(8)	ICMP
2.223	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

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.32.3, Dest. IP: 192.168.1.1 ICMP Message Type: 8
Layer 2: Ethernet II Header 0050.0FAE.A314 >> 00E0.F7EE.C78D
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)

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

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer7
Layer6
Layer5
Layer 4: TCP Src Port: 1025, Dst Port: 110
Layer 3: IP Header Src. IP: 192.168.7.11, Dst. IP: 192.168.1.3
Layer 2: Wireless
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.

802.11 Wireless

0 16 32 48 64 80 96 112 128 144 160 176 192 208 224 240 256 272 288 304 320 336 352 368 384 400 416 432 448 464 480 496 512 528 544 560 576 592 608 624 640 656 672 688 704 720 736 752 768 784 800 816 832 848 864 880 896 912 928 944 960 976 992 1008 1024 Bits

FRAME CONTROL DURATION/ID

ADDRESS 1:0002:1749:1C06

ADDRESS 2:0030:A354:2C2D

ADDRESS 3:0090:210A:98CE

SEQUENCE CONTROL

ADDRESS 4:

DATA (VARIABLE LENGTH)

FCS

IP

0 4 8 16 20 24 28 32 36 40 44 48 52 56 60 64 68 72 76 80 84 88 92 96 100 104 108 112 116 120 124 128 132 136 140 144 148 152 156 160 164 168 172 176 180 184 188 192 196 200 204 208 212 216 220 224 228 232 236 240 244 248 252 256 260 264 268 272 276 280 284 288 292 296 300 304 308 312 316 320 324 328 332 336 340 344 348 352 356 360 364 368 372 376 380 384 388 392 396 400 404 408 412 416 420 424 428 432 436 440 444 448 452 456 460 464 468 472 476 480 484 488 492 496 500 504 508 512 516 520 524 528 532 536 540 544 548 552 556 560 564 568 572 576 580 584 588 592 596 600 604 608 612 616 620 624 628 632 636 640 644 648 652 656 660 664 668 672 676 680 684 688 692 696 700 704 708 712 716 720 724 728 732 736 740 744 748 752 756 760 764 768 772 776 780 784 788 792 796 800 804 808 812 816 820 824 828 832 836 840 844 848 852 856 860 864 868 872 876 880 884 888 892 896 900 904 908 912 916 920 924 928 932 936 940 944 948 952 956 960 964 968 972 976 980 984 988 992 1000 1004 1008 1012 1016 1020 1024 Bits

VER:4 IHL:6 DSCP:0x00 TL:40

ID:0x0011 FLAGS:0x2 FRAG OFFSET:0x000

TTL:128 PRO:0x06 CHKSUM:

SRC IP:192.168.7.11

DST IP:192.168.1.3

OPT:0x00000000 PADDING:0x00

DATA (VARIABLE LENGTH)

TCP

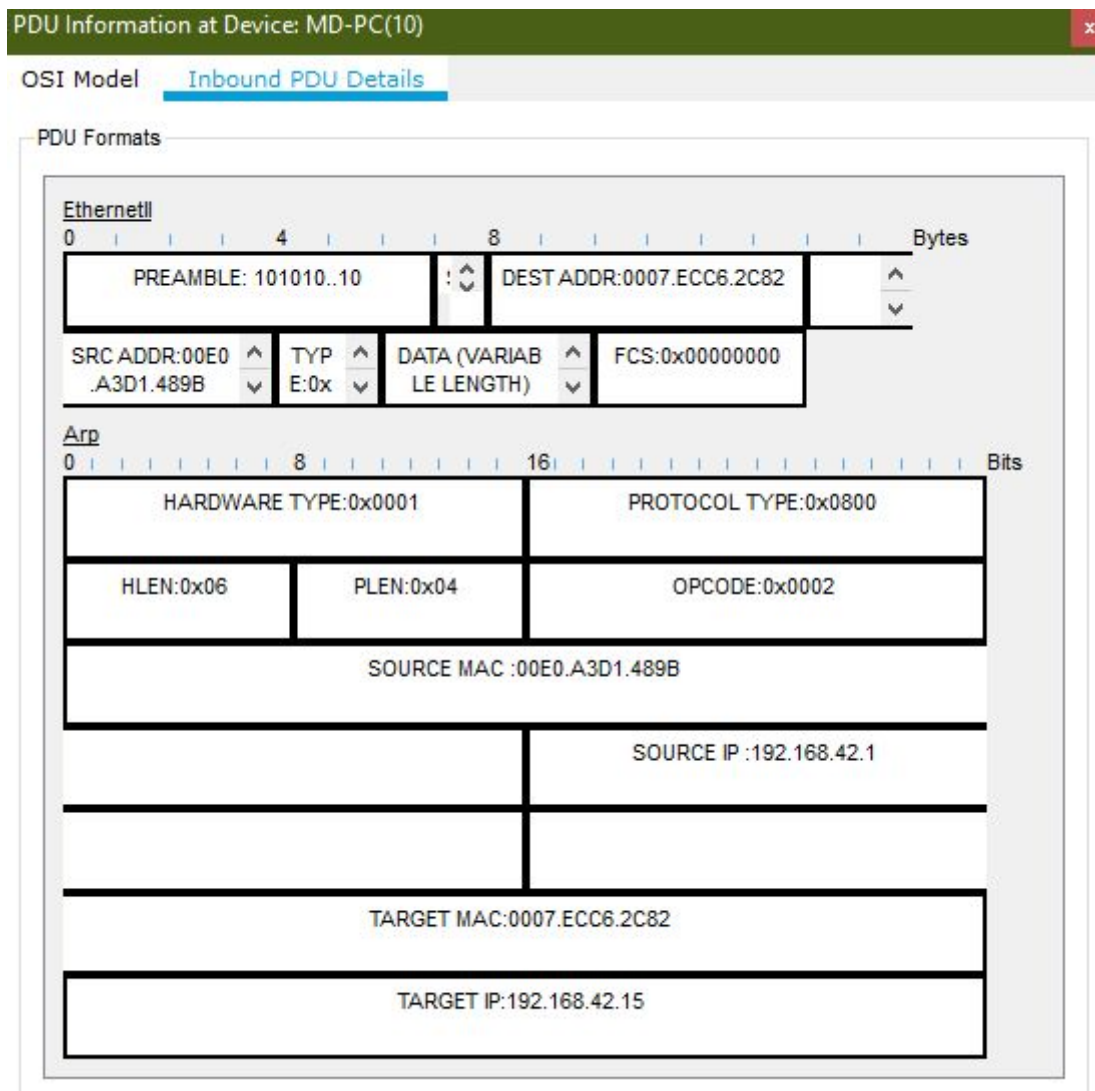
0 4 8 12 16 20 24 28 32 36 40 44 48 52 56 60 64 68 72 76 80 84 88 92 96 100 104 108 112 116 120 124 128 132 136 140 144 148 152 156 160 164 168 172 176 180 184 188 192 196 200 204 208 212 216 220 224 228 232 236 240 244 248 252 256 260 264 268 272 276 280 284 288 292 296 300 304 308 312 316 320 324 328 332 336 340 344 348 352 356 360 364 368 372 376 380 384 388 392 396 400 404 408 412 416 420 424 428 432 436 440 444 448 452 456 460 464 468 472 476 480 484 488 492 496 500 504 508 512 516 520 524 528 532 536 540 544 548 552 556 560 564 568 572 576 580 584 588 592 596 600 604 608 612 616 620 624 628 632 636 640 644 648 652 656 660 664 668 672 676 680 684 688 692 696 700 704 708 712 716 720 724 728 732 736 740 744 748 752 756 760 764 768 772 776 780 784 788 792 796 800 804 808 812 816 820 824 828 832 836 840 844 848 852 856 860 864 868 872 876 880 884 888 892 896 900 904 908 912 916 920 924 928 932 936 940 944 948 952 956 960 964 968 972 976 980 984 988 992 1000 1004 1008 1012 1016 1020 1024 Bits

SOURCE PORT:1025 DESTINATION PORT:110

SEQUENCE NUMBER:1

ACKNOWLEDGEMENT NUMBER:0

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	inciraltRouter	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	inciraltRouter	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	inciraltRouter	TCP
	0.244	inciraltRouter	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	inciraltRouter	TCP
	0.248	medicineSwitch	inciraltRouter	POP3

PDU Information at Device: MD-PC(10)

OSI Model

Inbound PDU Details

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

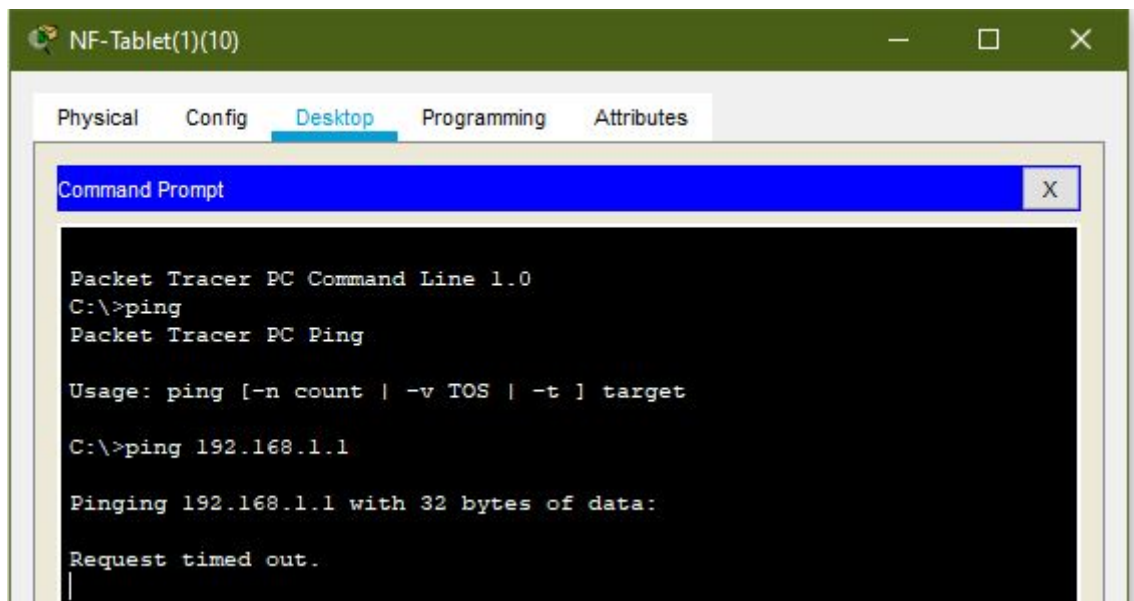
In Layers

Layer7
Layer6
Layer5
Layer4
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
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
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.

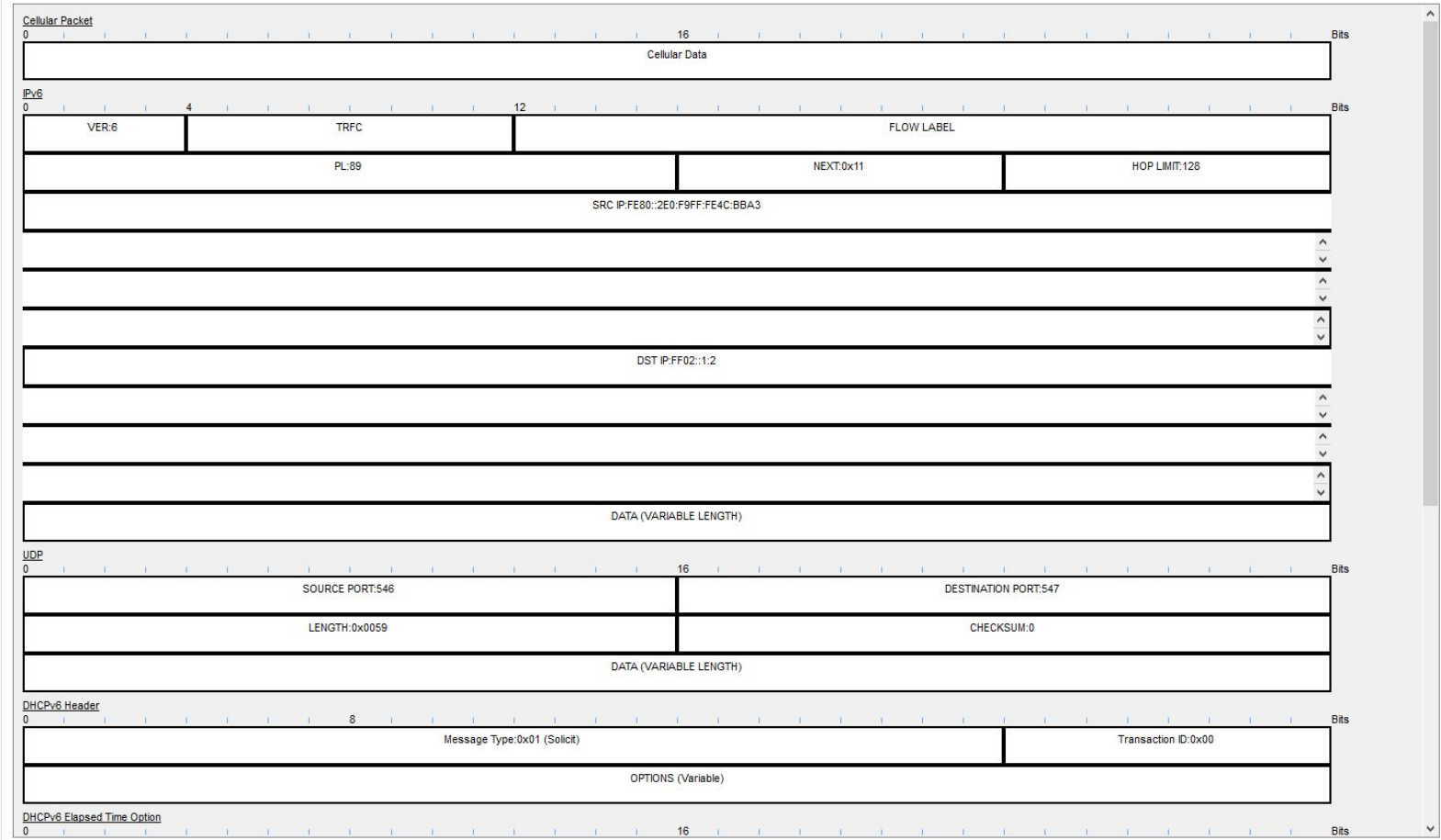


0.011	nurseryWifi	NF-Tablet(1)(7)	ICMP
0.011	nurseryWifi	NF-Tablet(1)(8)	ICMP
0.011	nurseryWifi	NF-Tablet(1)(6)	ICMP
0.011	nurseryWifi	NF-Tablet(1)...	ICMP
0.011	nurseryWifi	NF-Tablet(1)(5)	ICMP
0.011	nurserySwitch	nurseryWifi	ARP
0.175	--	nurserySwitch	STP
0.176	nurserySwitch	nurseryWifi	STP
2.173	--	nurserySwitch	STP
2.174	nurserySwitch	nurseryWifi	STP
4.173	--	nurserySwitch	STP
4.174	nurserySwitch	nurseryWifi	STP
4.544	--	NF-Tablet(1)(1)	DHCPv6
4.544	--	NF-Tablet(1)(2)	DHCPv6
4.544	--	NF-Tablet(1)(3)	DHCPv6
4.544	--	NF-Tablet(1)(4)	DHCPv6
4.544	--	NF-Tablet(1)(5)	DHCPv6
4.544	--	NF-Tablet(1)(6)	DHCPv6
4.544	--	NF-Tablet(1)(7)	DHCPv6
4.544	--	NF-Tablet(1)(8)	DHCPv6
4.544	--	NF-Tablet(1)(9)	DHCPv6
4.544	--	NF-Tablet(1)...	DHCPv6
6.003	--	NF-Tablet(1)...	ICMP
6.004	NF-Tablet(1)(10)	nurseryWifi	ICMP
6.005	nurseryWifi	nurserySwitch	ICMP

Reset Simulation ☒ Constant Delay Captured to: 6.175 s

Play Controls

PDU Formats



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

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer 7: DHCPv6 Frame
Layer6
Layer5
Layer 4: UDP Src Port: 546, Dst Port: 547
Layer 3: IPv6 Header Src. IP: FE80::2E0:F9FF:FE4C:BBA3, Dest. IP: FF02::1:2
Layer 2:
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

At Device: IP Phone(1)

Source: Switch2

Destination: STP Multicast Address

In Layers

Layer7

Layer6

Layer5

Layer4

Layer3

Layer 2: IEEE 802.3 Header
0001.4303.0A02 >> 0180.C200.0000 LLC
STP BPDU

Layer 1: Port Switch

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer3

Layer 2: Ethernet II Header 0005.5ECC.
7892 >> 0180.C200.0000 STP BPDU

Layer 1: Port(s): PC

1. The frame source MAC address was found in the MAC table of IP Phone.

2. The frame's destination MAC address matches the receiving port's MAC address, the broadcast address, or a multicast address.

3. The device decapsulates the PDU from the Ethernet frame.

Challenge Me

<< Previous Layer

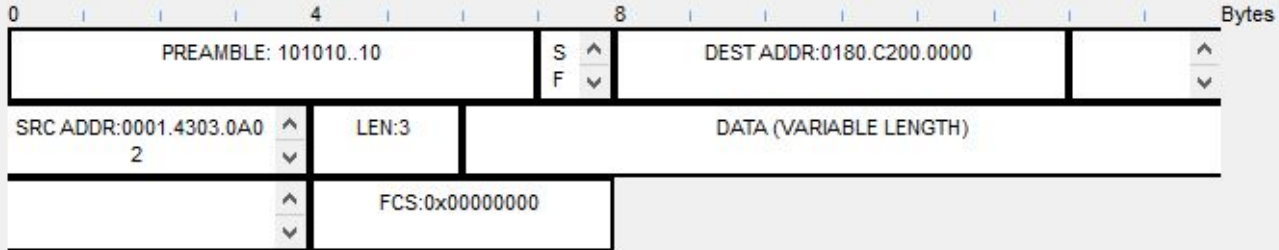
Next Layer >>

PDU Information at Device: IP Phone(1)

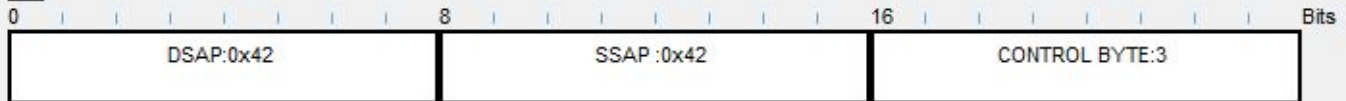
OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

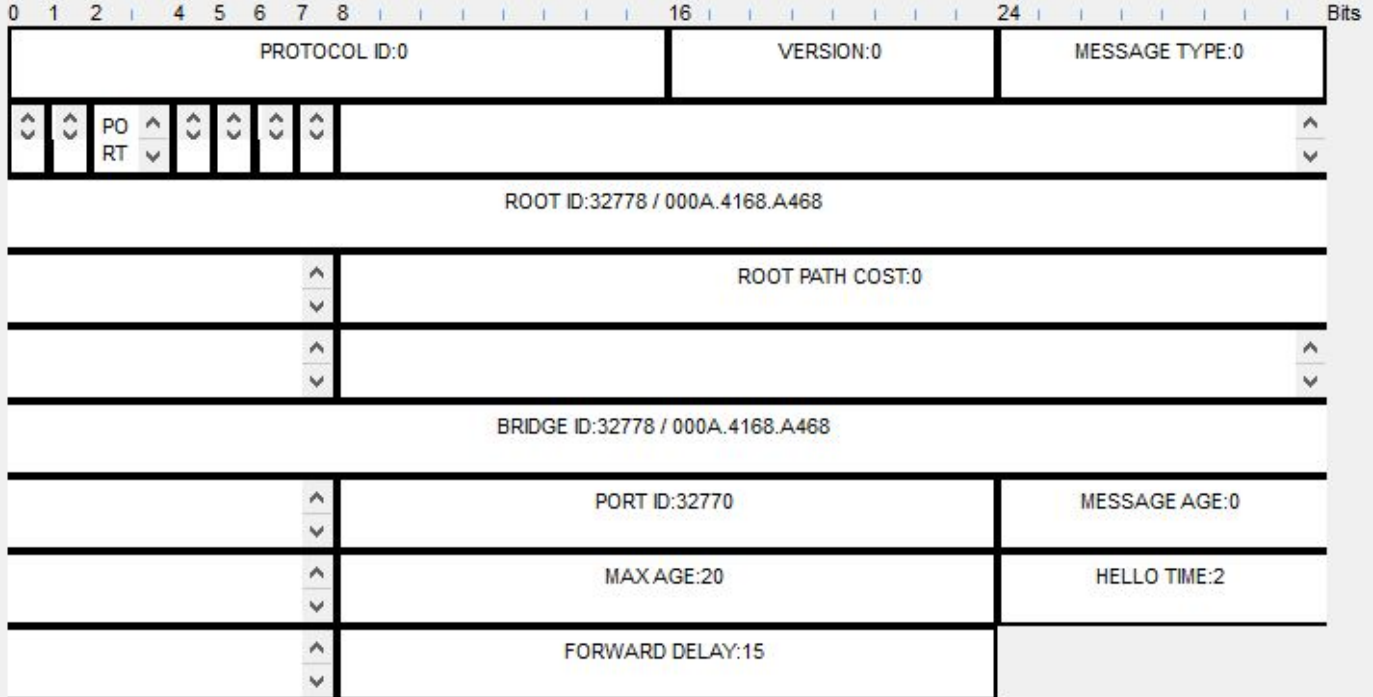
Ethernet 802.3



LLC



STP BPDU



PDU Information at Device: IP Phone(1)

OSI Model Inbound PDU Details **Outbound PDU Details**

PDU Formats

EthernetII

PREAMBLE: 101010..10				SFD	DEST ADDR: 0180.C200.0000			
SRC ADDR: 0005.5ECC.7892		TYPE: 0x010b		DATA (VARIABLE LENGTH)		FCS: 0x00000000		

STP BDPDU

PROTOCOL ID: 0								VERSION: 0								MESSAGE TYPE: 0							
PORT ROLE																							
ROOT ID: 32778 / 000A.4168.A468																							
												ROOT PATH COST: 0											
BRIDGE ID: 32778 / 000A.4168.A468																							
												PORT ID: 32770								MESSAGE AGE: 0			
												MAX AGE: 20								HELLO TIME: 2			
												FORWARD DELAY: 15											

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>