Metropolitan Area Network Simulation

Project Report

Group 18

Alper Temel - 2017510073

Vedat Özcan - 2016510083

Zeynep Hilal Destebaşı - 2017510024

İzmir

11.06.2021

Table of Content

1. Introduction

1.1. Project Definition and Problem Formulation

A company has two different branches in a city. There are 3 buildings in each branch and various users in each building. These users are divided according to different functions. Each function includes different hardware devices and various configurations between these devices.

1.2. The purpose and motivation of the project

The main purpose of this project is to design a metropolitan area network (MAN) using the Packet Tracer simulation tool. Metropolitan area network is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. With this network model, it is aimed to solve the communication between two different branches of a company in a city in the most efficient way.

Each company has units and employees responsible for different jobs.These employees can send emails to each other, browse the web and attend conferences due to their jobs.

Various principles are considered in this network model, which is designed to find solutions to all these needs of users.

The network should be designed to support maximum hardware devices. Communication between devices connected to the network should be fast and a suitable topology should be selected. There should be no data loss, the data should reach the desired address and users should not see each other's data.

1.3. Term Definitions

Node: The definition of a node depends on the network and protocol layer referred to. A physical network node is an electronic device that is attached to a network, and is capable of creating, receiving, or transmitting information over a communication channel. A passive distribution point such as a distribution frame or patch panel is consequently not a node.[1]

Packet: A packet is a small amount of data sent over a network, such as a LAN or the Internet. Similar to a real-life package, each packet includes a source and destination as well as the content (or data) being transferred. When the packets reach their destination, they are reassembled into a single file or other contiguous block of data. [2]

Channel: A channel is a communication medium, the path that data takes from source to destination. A channel can be comprised of so many different things: wires, free space, and entire networks. Signals can be routed from one type of network to another network with completely different characteristics.[3]

Protocol: There are many protocols while establishing a connection on the internet. According to the type of connection need to be established, the protocols used varies. The protocols define the characteristics of the connection. [4]

Network Protocol: A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.[5]

Transmission Control Protocol (TCP): The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP. [6]

Internet Protocol: The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.[7]

Hypertext Transfer Protocol (HTTP): The HTTP is the foundation of data communication for the World Wide Web. The hypertext is structured text that uses hyperlinks between nodes containing texts. The HTTP is the application protocol for distributed and collaborative hypermedia information systems. The default port of HTTP is 80 and 443 is the secured port.[4]

File Transfer Protocol (FTP): The FTP is the most common protocol used in the file transferring on the Internet and within private networks. The default port of FTP is 20/21.[4]

Domain Name System (DNS): Domain name system is used to convert the domain name to IP address. There are root servers, TLDs and authoritative servers in the DNS hierarchy. The default port of DNS is 53.[4]

Post Office Protocol version 3 (POP 3): The Post Office Protocol version 3 is one of the two main protocols used to retrieve mail from the internet. It is very simple as it allows the client to retrieve complete content from the server mailbox and deletes contents from the server. The default port of POP3 is 110 and secured is 995. [4]

Internet Message Access Protocol (IMAP): IMAP version 3 is another main protocol that is used to retrieve mail from a server. IMAP does not delete the content from the mailbox of the server. The default port of IMAP is 143 and secured is 993. [4]

System: A communication system in telecommunications is a collection of individual communication networks, transmission systems, transfer stations and data terminal equipment that can be interconnected and interoperable, often to form an integrated whole. The basic components of a communication system are information source, input transducer, transmitter, communication channel, receiver, output transducer and destination.[8]

Architecture: Network architecture refers to the way network devices and services are structured to serve the connectivity needs of client devices. Network devices typically include switches and routers. Types of services include DHCP and DNS. Client devices comprise end-user devices, servers, and smart things. [9]

Dynamic Host Configuration Protocol (DHCP): The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.[10]

Server: In computing, a server is a piece of computer hardware or software (computer program) that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device.[11]

Router: A router is a networking device that routes data packets between computer networks. A router can connect networked computers to the Internet, so multiple users can share a connection. Routers help connect networks within an organization or connect the networks of multiple branch locations. And a router works as a dispatcher. It directs data traffic, choosing the best route for information to travel across the network, so that it's transmitted as efficiently as possible.[12]

Switch: Switches facilitate the sharing of resources by connecting together all the devices, including computers, printers, and servers, in a small business network. Thanks to the switch, these connected devices can share information and talk to each other, regardless of where they are in a building or on a campus. Building a small business network is not possible without switches to tie devices together.[13]

Internet Control Message Protocol (ICMP): The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address, for example, an error is indicated when a requested service is not available or that a host or router could not be reached. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).[14]

1.4. Related Work

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Our work is a Metropolitan Area Network (MAN) study and we have not encountered any design project like this in real life.

While doing research, we saw many studies on this subject on the internet. Studies similar to the Metropolitan Area Network (MAN) simulation, which is our own project, were rarely encountered. Because MAN design contains more details when compared to other works. We have encountered network designs that cover a smaller area and use fewer devices, mostly Personal Area Network (PAN) and Local Area Network (LAN). We applied the knowledge gained from these less complex structures in our own design.

2. Method and Simulation

2.1. Simulation and Modeling Concepts

Physical and logical needs were considered. Although it is correct to go from the specific to the general, since some features were reused in our project, a plan was made from general to specific.

This project includes two branches. First, branches were created. Three facilities were set up inside the branches. IPs are assigned to each of these facilities. Some facilities have more than one network device. These devices are configured to connect to different stations differently.

For devices that do not use the internet network, the cable automatically adjusted by the cisco packet tracer is used. Devices are connected to switches with copper cable.

For the first branch, the first two facilities are connected to a router for a faster system. Thanks to this system, sending or receiving transactions such as messages, mail, files etc. can be realized faster. Since the third facility is also used in the second branch, it is connected to a router that connects the two branches. Thus, facilities in other branches using this facility will be able to reach this facility more quickly. This third facility has servers. Thanks to these servers, the processes of sending and receiving mail, messages and files are realized.

The same system used in the first branch was used for the second branch. Devices are connected to switches. Thus, the incoming data can be distributed to all devices. This branch uses VoIP Services (sending voice data over an IP between private users/workstations) in addition to the other branch.

As a result, the whole system was designed and all the desired features were realized. The desired network connection was established between the facilities and the two branches.

2.2. Simulation Environment/Tool

While designing this model, we use Cisco Packet Tracer as a simulation tool. Cisco Packet Tracer is a network simulation program that allows you to study and test how networks work. It provides a visual representation of complex technologies and configurations.

2.3 Network Design Requirements

Seven switches (2950-24), four routers (Router-PT and 2811), four wireless devices (WRT300N), eight servers (servet-PT) were used for the design. MAIL, DNS, HTTP 2, HTTP 1, FTP 1, FTP 2 and DHCP protocols are used for communication between devices. The topology we use is star and hybrid.

2.4 Requirement Analysis

The server in the first branch can be accessed by the allowed facilities in both the first branch and the second branch.

For the first facility in the first branch, web browsing, sending emails and file transfer were requested. For the second facility, web browsing, file transfer and VoIP conference are requested.

For the first facility in the second branch, it was requested to use wireless connection, web browsing and email. Web browsing, editing applications and file transfer were requested for the second branch. The third branch was asked to browse the web and send an email and reply.

As a result, at least 40 workstation users, 15 wireless users, 15 smartphone users, 5 tablet users are expected for these requirements. Protocols are followed in accordance with the desired situations. If a situation is not requested in a facility, that protocol is not applied. The network speed of this project reaches up to 50-150 Mbps according to these specifications.

2.5 Definitions of the System/Model

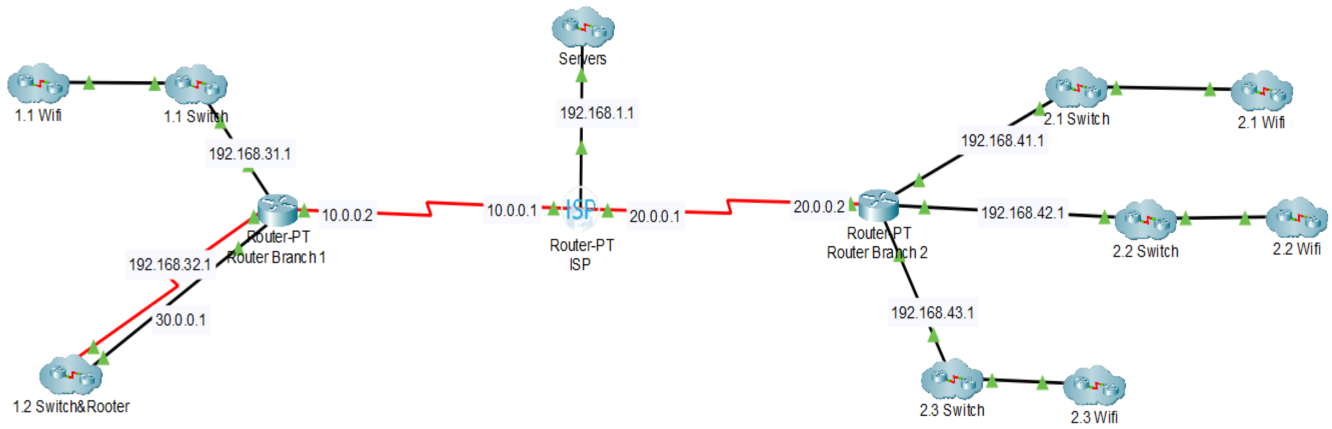
In the system, users can communicate among themselves, connect to the internet, file operations for some users, e-mail transactions for some users and make calls over VoIP.

Two different cable types are used in this system. The first is serial DTE (DTE is typically either a dumb terminal or the serial port on a computer/workstation)[15], and the second is copper straight-through.

In the created network, some operations of some facilities were restricted. This is a security measure. For example, some facilities can receive email, others cannot, or not all facilities can transfer files. Necessary management has been done to ensure this.

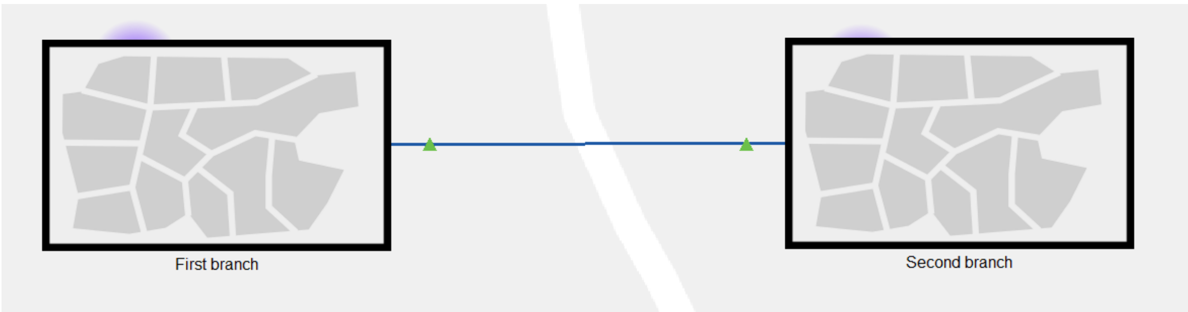
General shape of the system

Logical:

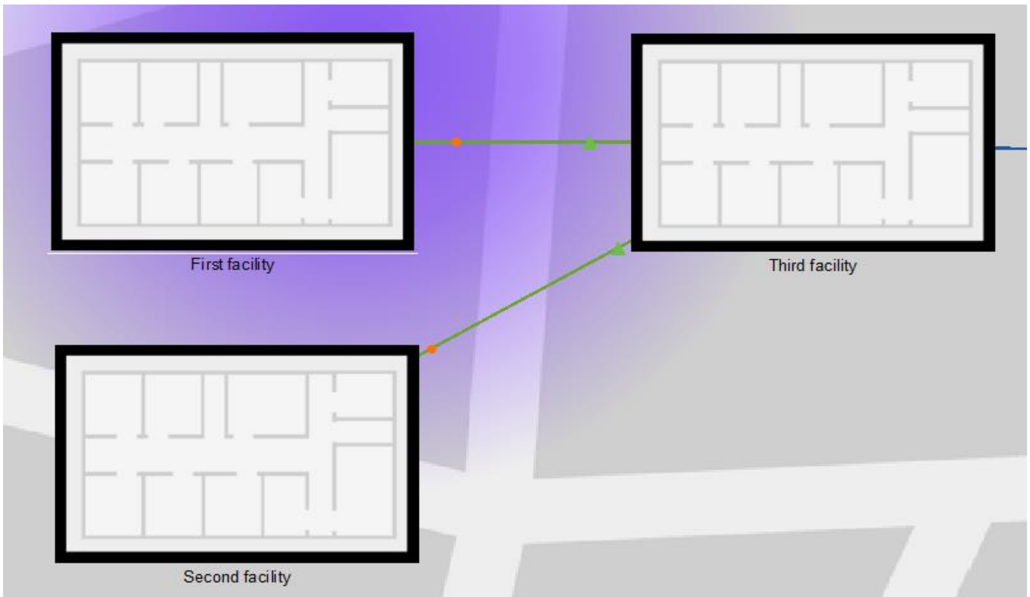


Physical:

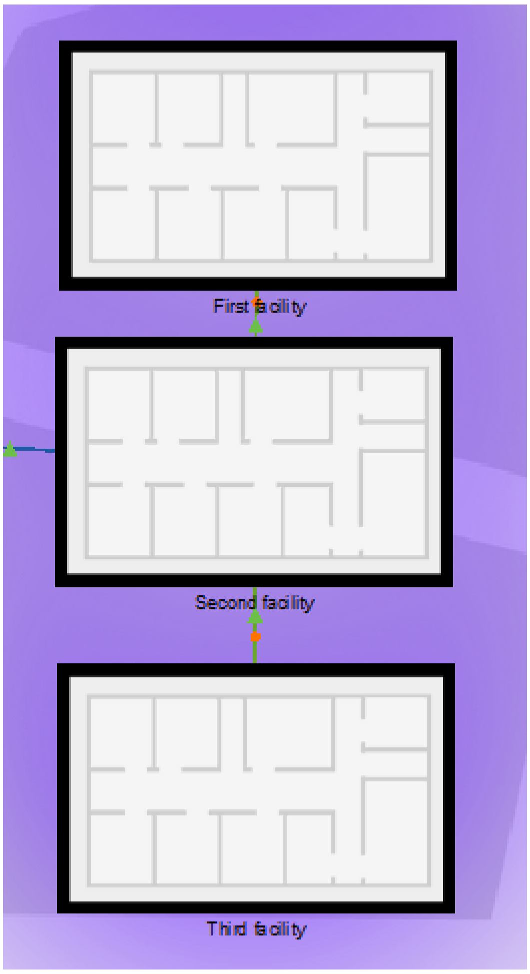
Branches:



First branch:

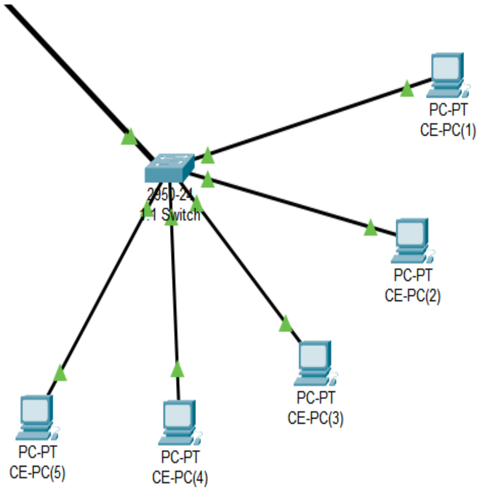


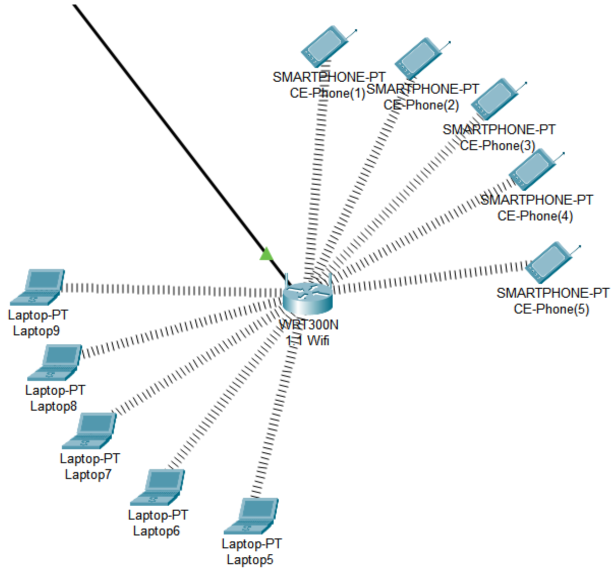
Second branch:



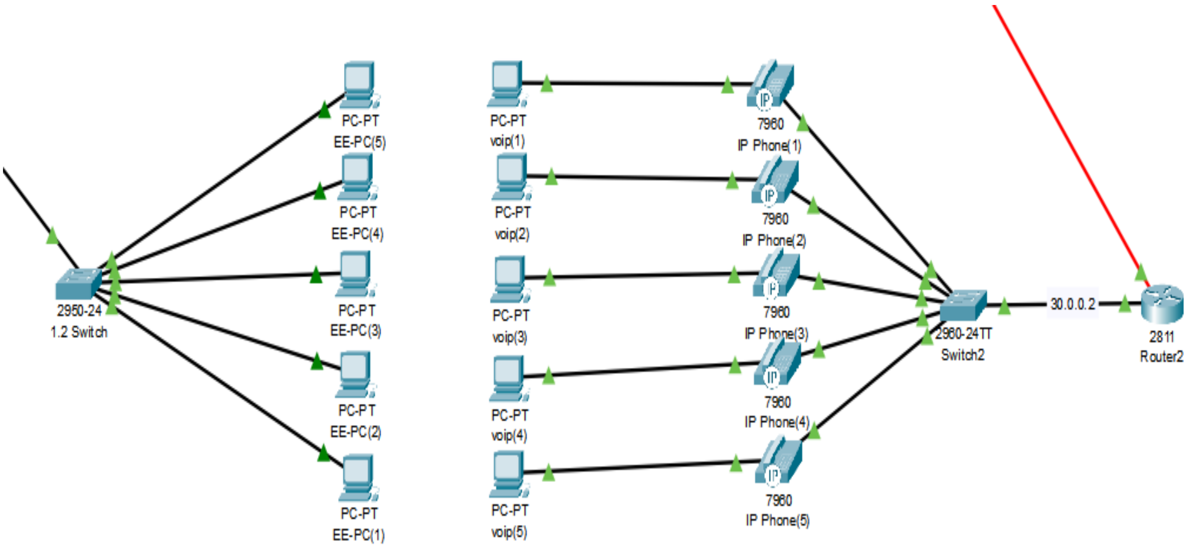
First Branch:

First Facility:

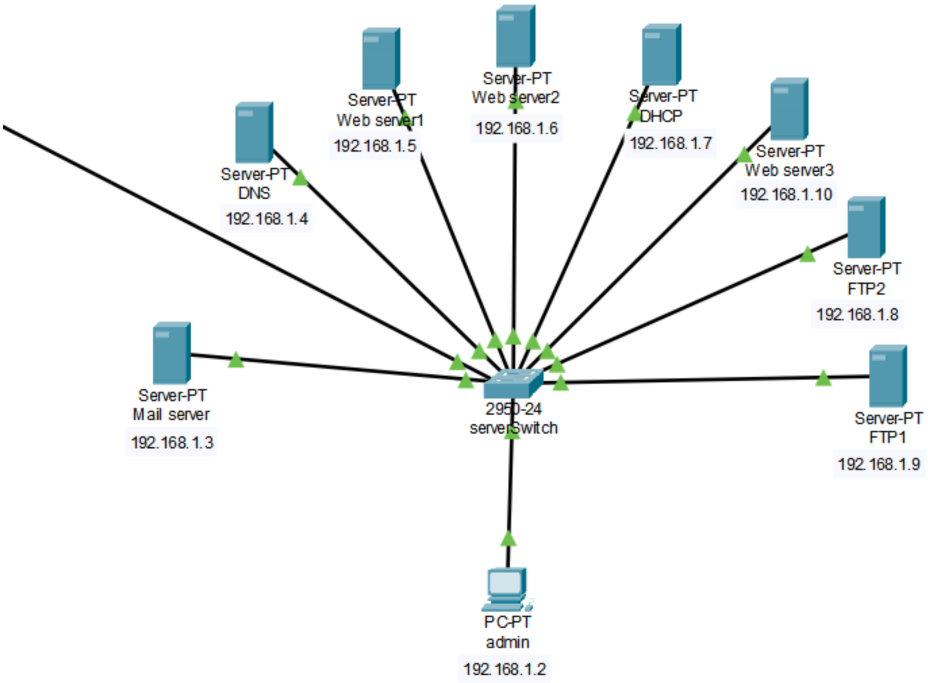




Second Facility:

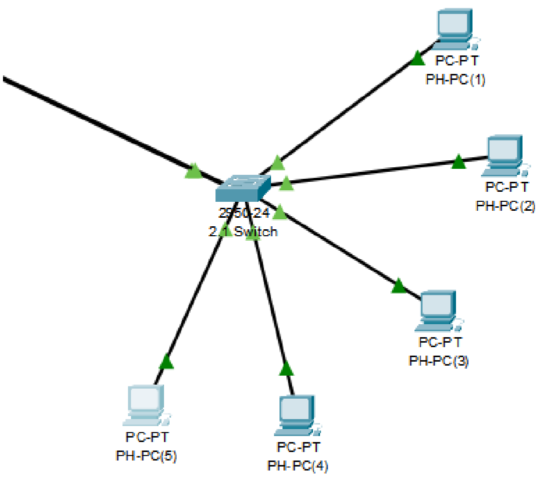


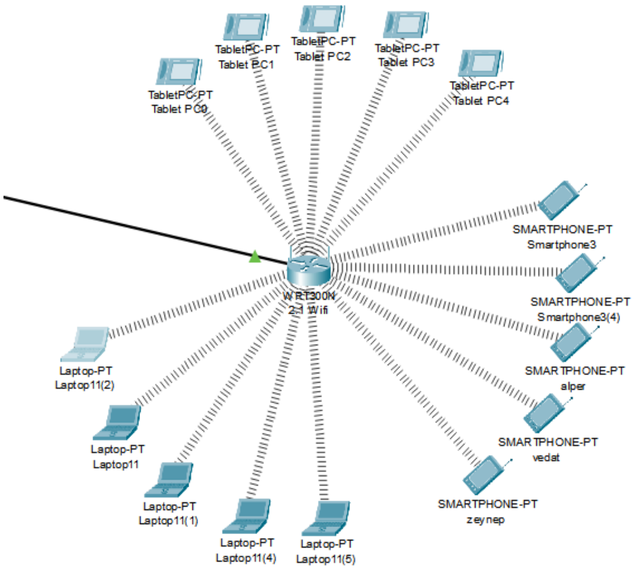
Third Facility:



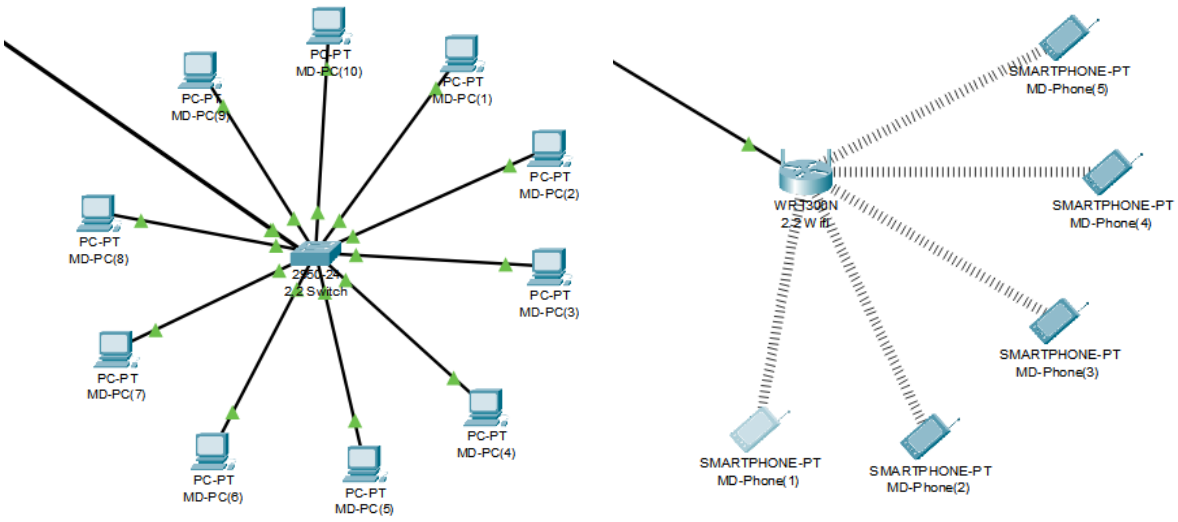
Second Branch:

First Facility:

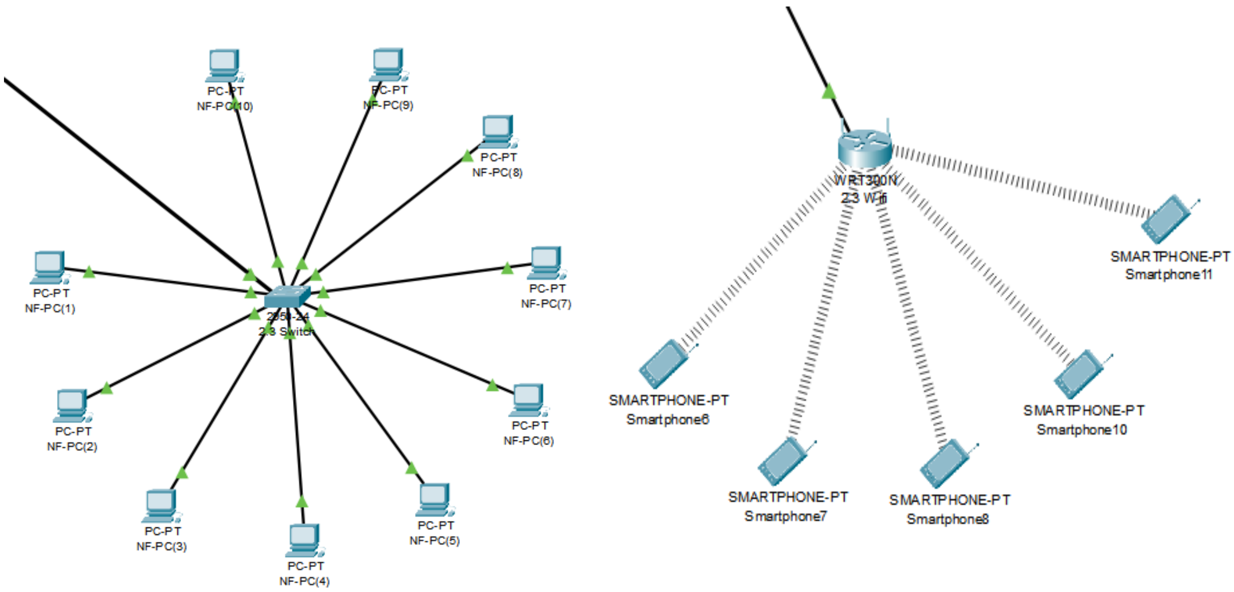




Second Facility:



Third Facility:



2.6 Simulation Elements

In this project, the devices in the Cisco Packet Tracer simulation tool were used and their numbers are as follows:

Network Devices:

- 4 Routers
- 7 Switches
- 4 Wireless Devices

End Devices:

- 41 PCs
- 10 Laptops
- 8 Servers
- 5 IP Phones
- 5 Tablets
- 20 Smartphones

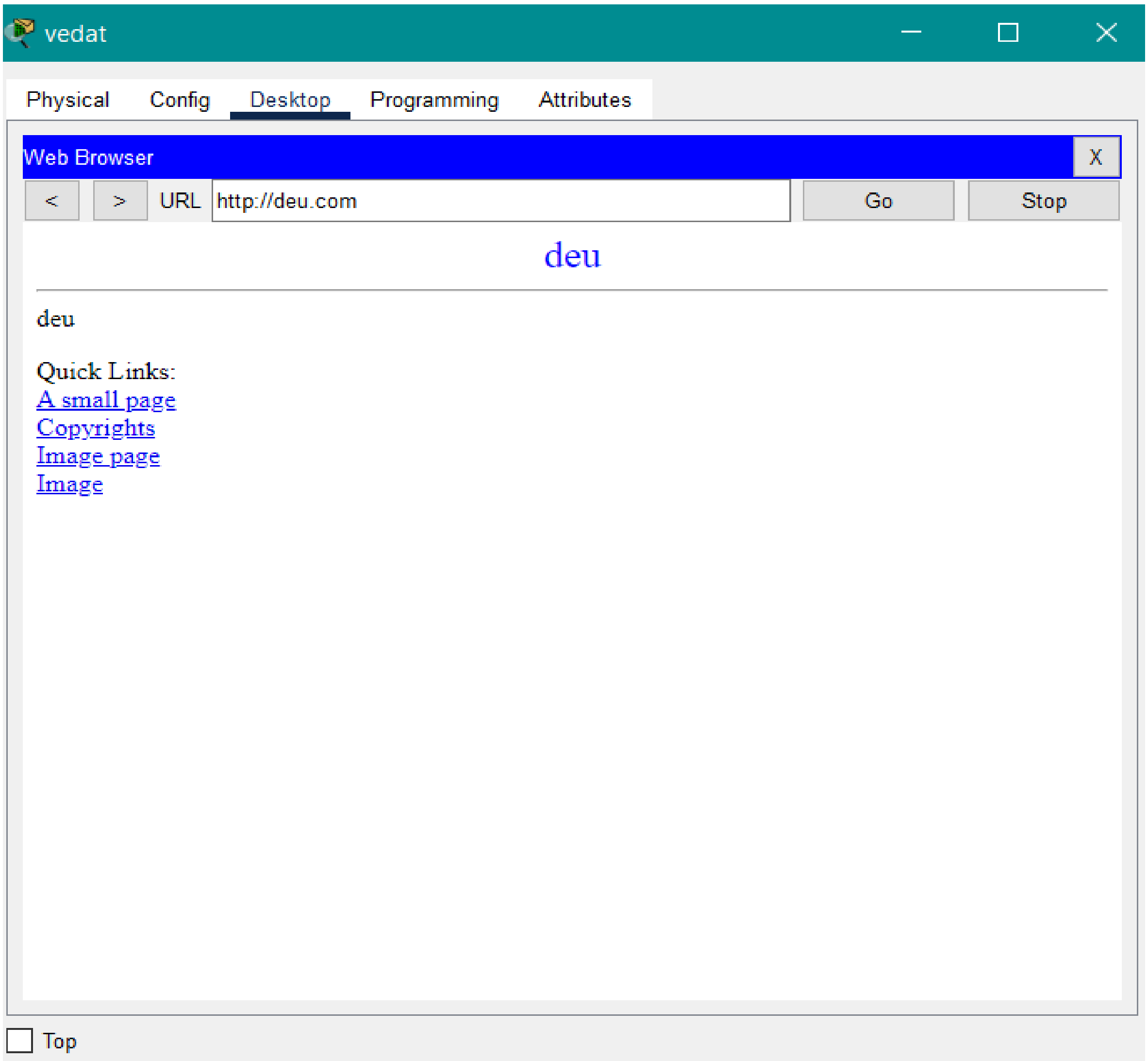
Connection Devices:

- Copper Straight
- Serial DTE

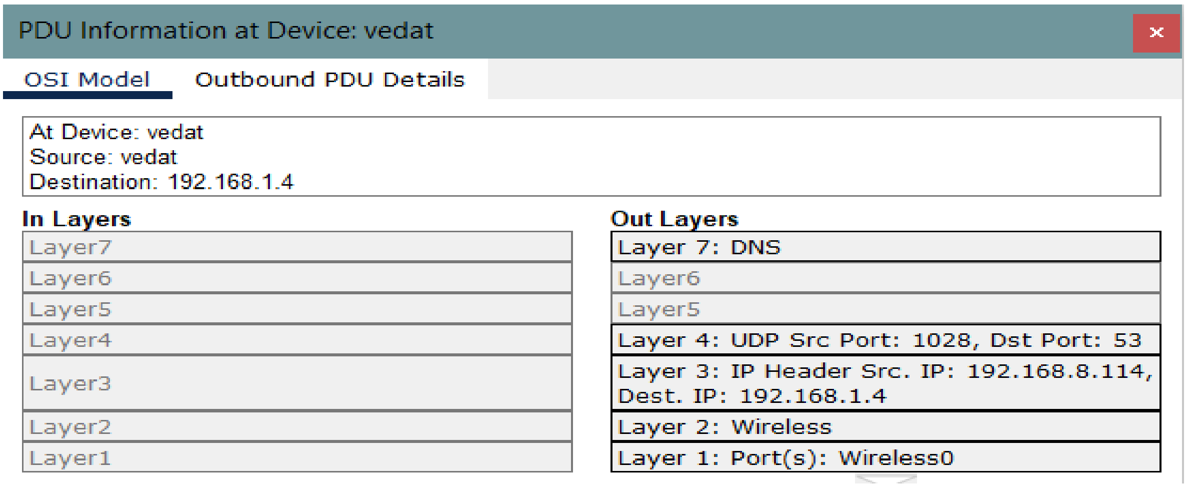
3. Traffic Analysis and Simulation Results

3.1. Network Functionality

Scenario 1: A wireless user from the first facility of the second branch wants to read emails and browse the Web.



We want to surf the internet on Vedat's phone. First we need to go to the DNS server. The layers at this stage are as follows.



Layer 7: The DNS client sends a DNS query to the DNS server.

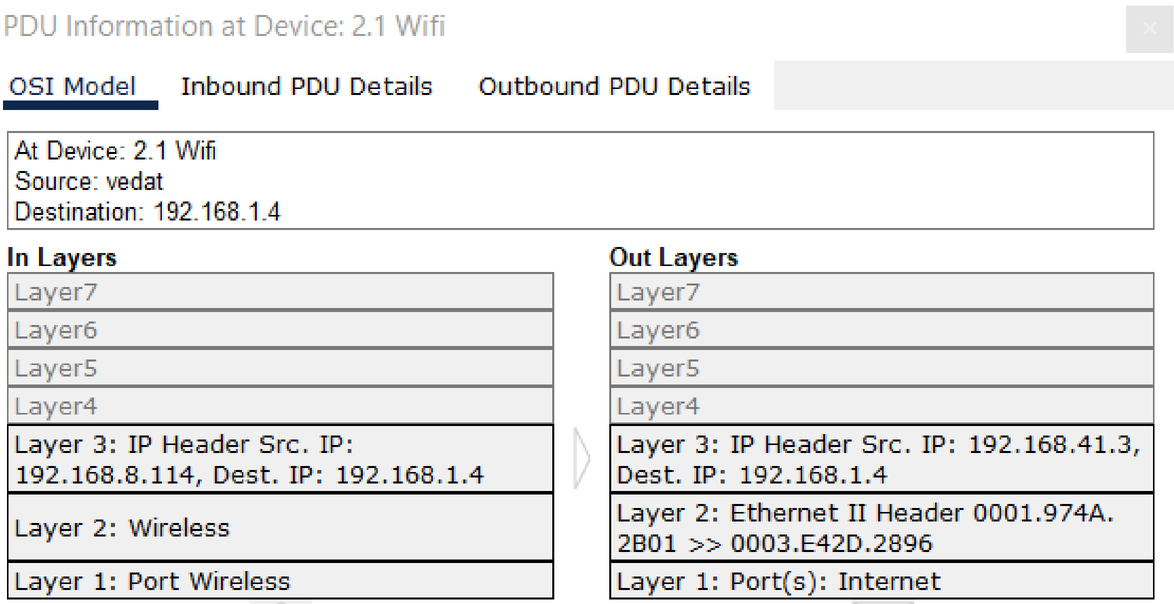
Layer 4: The device encapsulates the PDU into an UDP segment.

Layer 3: The device sets it to the port’s IP address. The destination IP address 192.168.1.4 is not in the same subnet and is not the broadcast address. The device sets the next-hop to default gateway.

Layer 2: The ARP process sets the frame’s destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.

Layer 1: Wireless sends out the frame.

Second, there is a response from DNS. Actions will be initiated based on this response. The layers of this stage are as follows.



In layers;

Layer 3: The device checks the packet against the access-list. The packet is permitted. The device looks up the destination IP address in the CEF table.
Layer 2: The frame source MAC address was found in the MAC table of Wireless Router. The frame destination MAC address matches the MAC address of the active VLAN interface. The device decapsulates the PDU from the Ethernet frame.
Layer 1: Wireless receives the frame.

Out Layers;

Layer 3: The CEF table has an entry for the destination IP address. The device decrements the TTL on the packet. The device looks up its NAT table for necessary translations. The packet matches an inside source list and creates a new entry for the source local address. The device translates the packet from local to global addresses with the matched entry.
Layer 2: The device sets the frame's destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.
Layer 1: The port Wireless is sending another frame at this time. The device buffers the frame to be sent later. The Internet sends out the frame.

After these operations, DNS operation continues 2 more times in the same way. After that, it enters TCP.

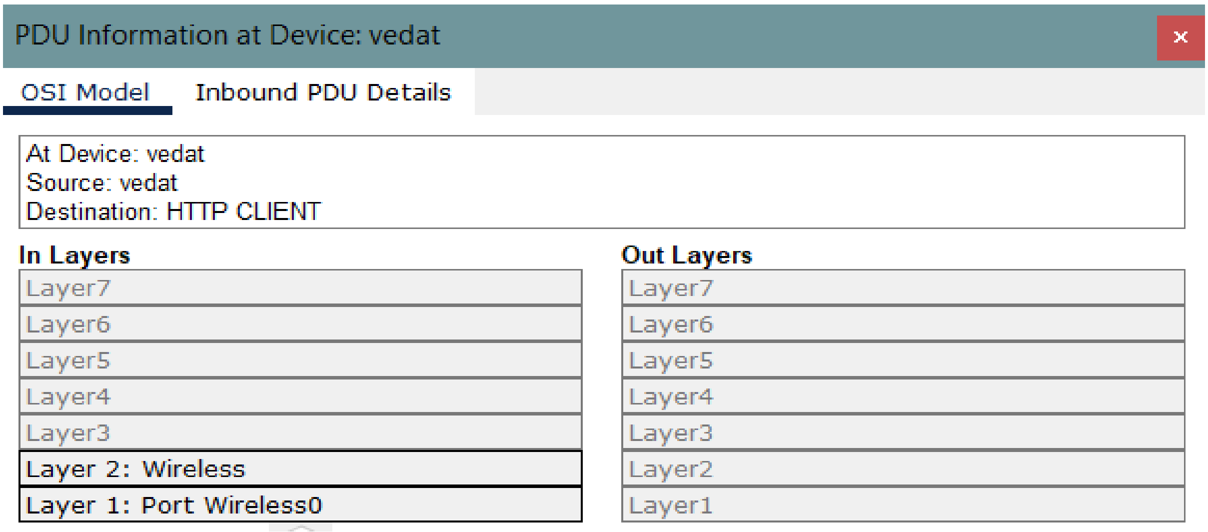
Time(sec)	Last Device	At Device	Type
0.012	--	vedat	TCP
0.014	--	vedat	TCP
0.015	vedat	2.1 Wifi	TCP
0.016	2.1 Wifi	2.1 Switch	TCP
0.020	--	2.1 Wifi	TCP
0.021	2.1 Wifi	Tablet PC4	TCP
0.021	2.1 Wifi	Tablet PC0	TCP
0.021	2.1 Wifi	Tablet PC2	TCP
0.021	2.1 Wifi	Tablet PC3	TCP
0.021	2.1 Wifi	Laptop11(1)	TCP
0.021	2.1 Wifi	Laptop11(4)	TCP
0.021	2.1 Wifi	Laptop11(2)	TCP
0.021	2.1 Wifi	Laptop11(5)	TCP
0.021	2.1 Wifi	Laptop11	TCP
0.021	2.1 Wifi	alper	TCP
0.021	2.1 Wifi	vedat	TCP
0.021	2.1 Wifi	Smartpho...	TCP
0.021	2.1 Wifi	zeynep	TCP
0.021	2.1 Wifi	Smartpho...	TCP
0.021	2.1 Wifi	Tablet PC1	TCP
0.025	2.1 Switch	2.1 Wifi	TCP
0.026	2.1 Wifi	Tablet PC4	TCP
0.026	2.1 Wifi	Tablet PC0	TCP
0.026	2.1 Wifi	Tablet PC2	TCP
0.026	2.1 Wifi	Tablet PC3	TCP
0.026	2.1 Wifi	Laptop11(1)	TCP
0.026	2.1 Wifi	Laptop11(4)	TCP
0.026	2.1 Wifi	Laptop11(2)	TCP
0.026	2.1 Wifi	Laptop11(5)	TCP
0.026	2.1 Wifi	Laptop11	TCP
0.026	2.1 Wifi	alper	TCP
0.026	2.1 Wifi	vedat	TCP

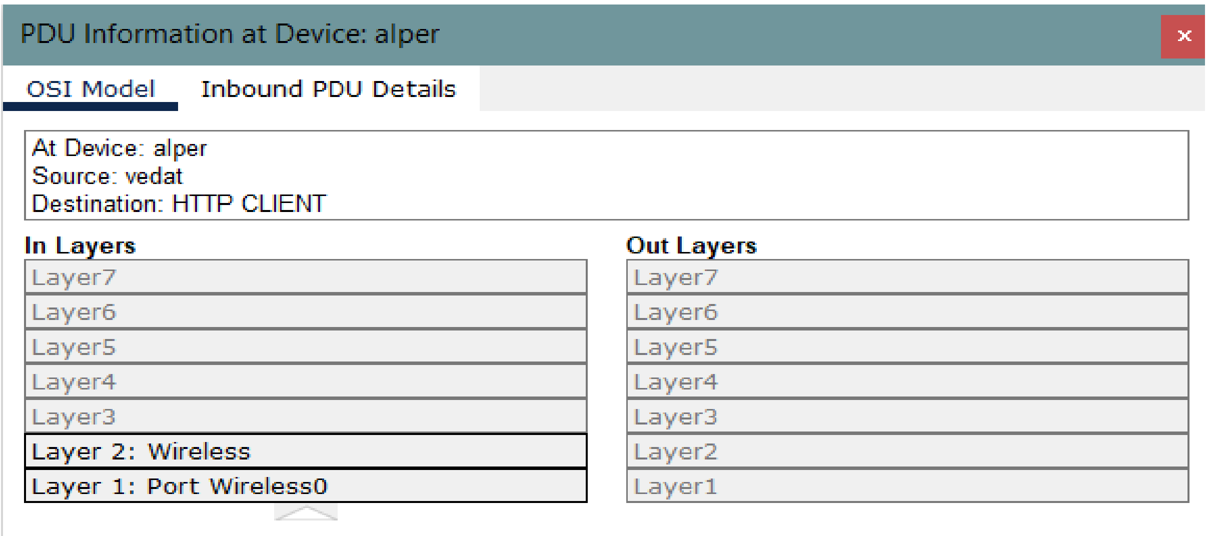
Time(sec)	Last Device	At Device	Type
0.026	2.1 Wifi	Tablet PC1	TCP
0.026	2.1 Wifi	Smartpho...	TCP
0.026	2.1 Wifi	zeynep	TCP
0.026	2.1 Wifi	Smartpho...	TCP
0.026	--	vedat	HTTP
0.029	--	vedat	TCP
0.030	vedat	2.1 Wifi	TCP
0.031	2.1 Wifi	2.1 Switch	TCP
0.031	--	vedat	HTTP
0.032	vedat	2.1 Wifi	HTTP
0.033	2.1 Wifi	2.1 Switch	HTTP
0.035	--	2.1 Wifi	TCP
0.036	2.1 Wifi	Tablet PC4	TCP
0.036	2.1 Wifi	Tablet PC0	TCP
0.036	2.1 Wifi	Tablet PC2	TCP
0.036	2.1 Wifi	Tablet PC3	TCP
0.036	2.1 Wifi	Laptop11(1)	TCP
0.036	2.1 Wifi	Laptop11(4)	TCP
0.036	2.1 Wifi	Laptop11(2)	TCP
0.036	2.1 Wifi	Laptop11(5)	TCP
0.036	2.1 Wifi	Laptop11	TCP
0.036	2.1 Wifi	alper	TCP
0.036	2.1 Wifi	vedat	TCP
0.036	2.1 Wifi	Smartpho	TCP

After the TCP operations, we move on to the HTTP operations, which will bring us the screen.

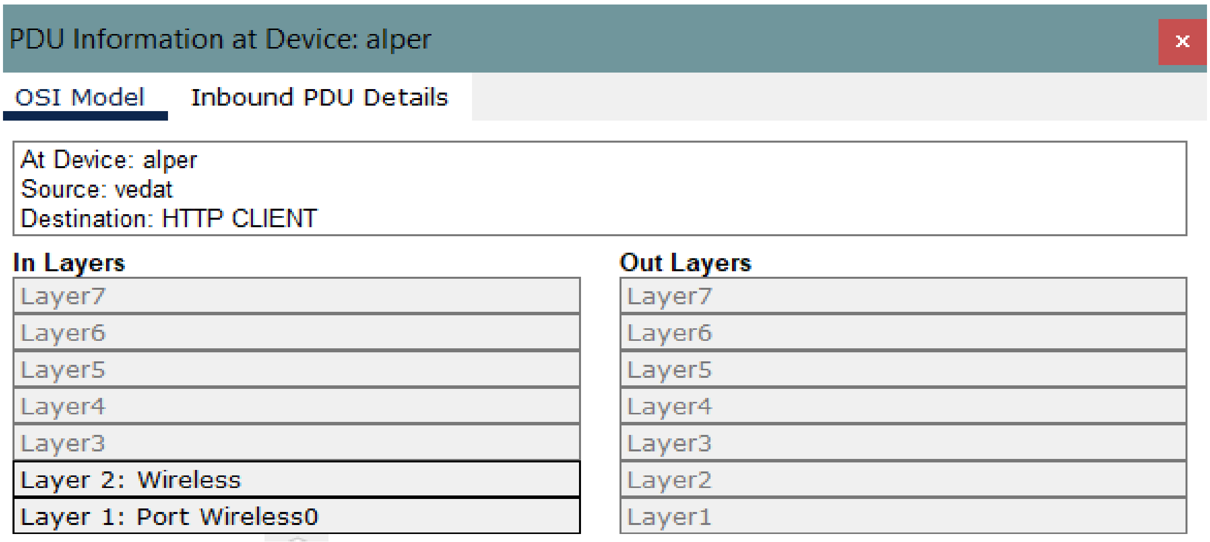
The first HTTP transactions are the same for all devices, but our last HTTP transaction is different from the others on the only phone we want (Vedat). This last HTTP process helps us to see the final version on the screen, and different layers are used compared to the others.

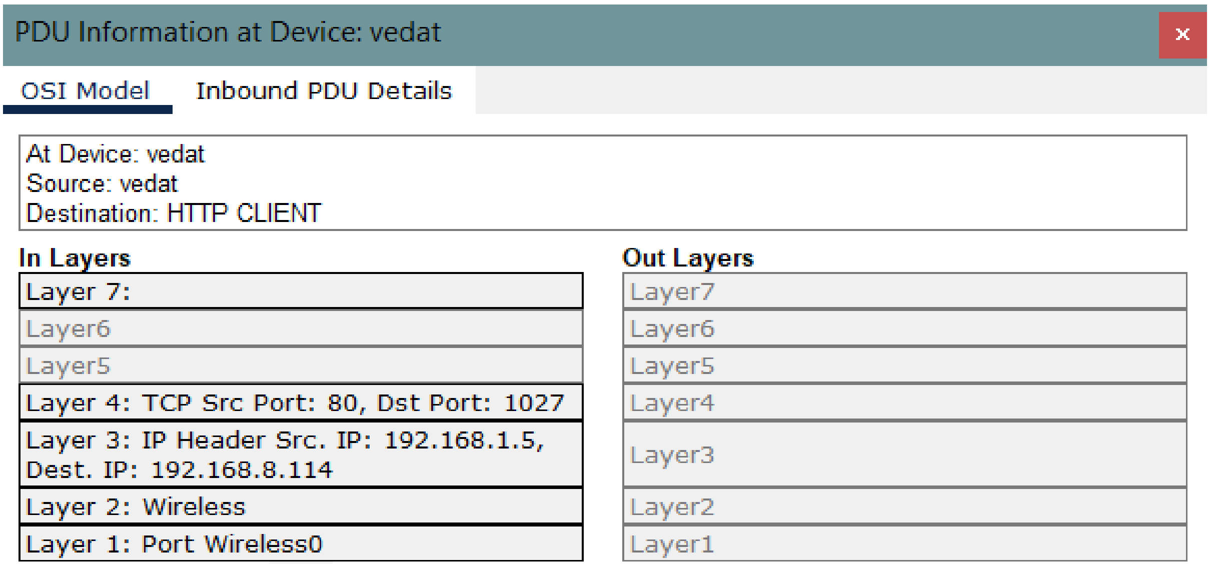
Our layers on two different phones for first-in-come HTTP:





Our layers in the final HTTP transaction:





As seen above, the website is loaded correctly on the device we want. While there is no change in the Alper device we do not want, the Vedat device we want is displayed correctly.

Layer 7: The HTTP client receives a HTTP reply from the server. It displays the page in the web browser.

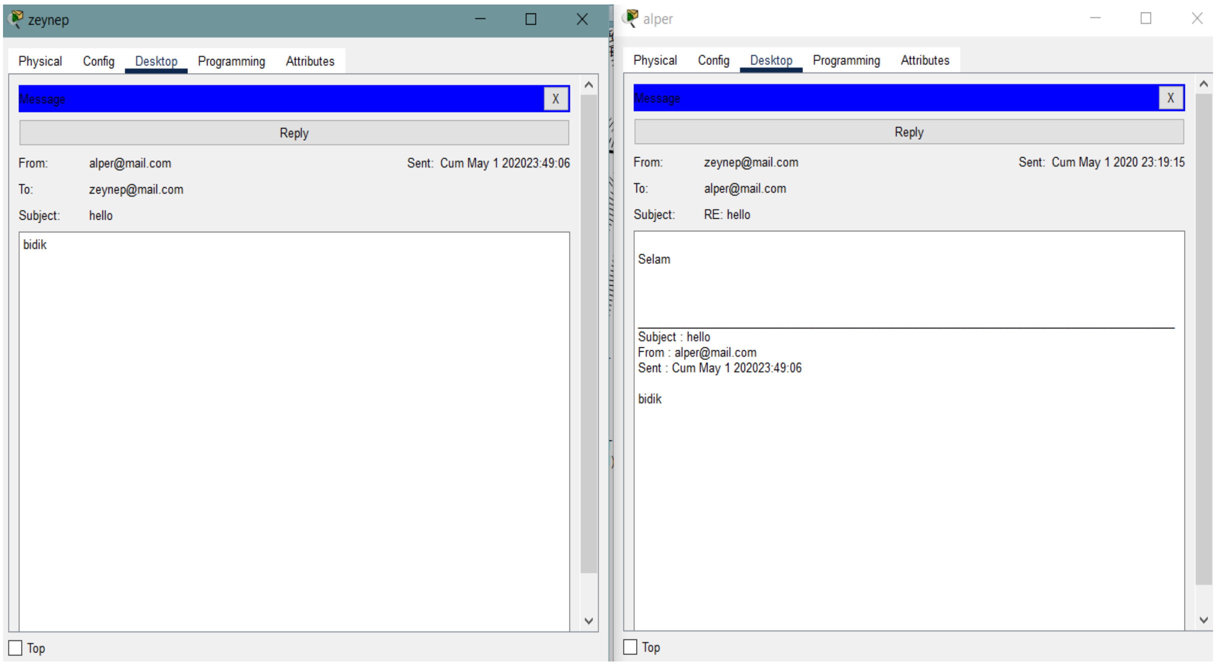
Layer 4: The device receives a TCP PUSH+ACK segment on the connection to 192.168.1.5 on port 80. Received segment information: the sequence number 1, the ACK number 97, and the data length 375. The TCP segment has the expected peer sequence number and ACK number. The device pops the last sent segment from the buffer. TCP processes payload data. TCP reassembles all data segments and passes to the upper layer.

Layer 3: The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.

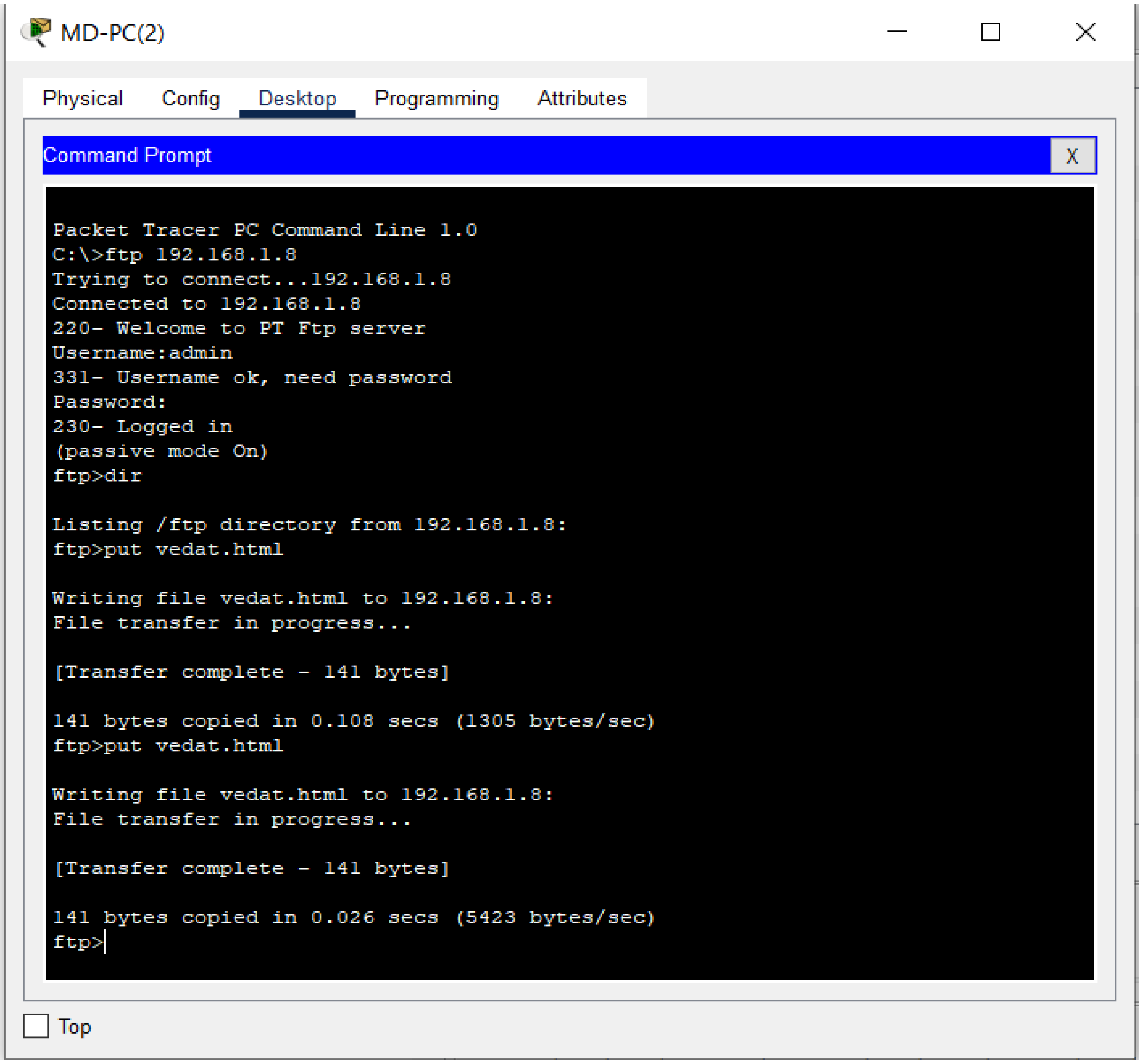
Layer 2: The frame's destination MAC address matches the receiving ports's MAC address, the broadcast address or a multicast address. The device decapsulates the PDU from the Ethernet frame.

Layer 1: Wireless receives the frame.

While the mail is reading, there is no movement in the simulation because the operations are already performed.



Scenario 2: A computer engineer from the second facility of the second branch developed a web application and wants to send her code files to the FTP server in the third facility of the first branch.



As seen above, we first prepare the file we will send. Then we connect to the relevant FTP server with the "ftp -ip address" command. After this process, we print the file to the FTP server with the "put -ip address" command.

As seen below in this scenario, the "MD-PC2" computer sends the prepared .html file to the "FTP1" server. While sending the file, it passes through the following network devices in order:

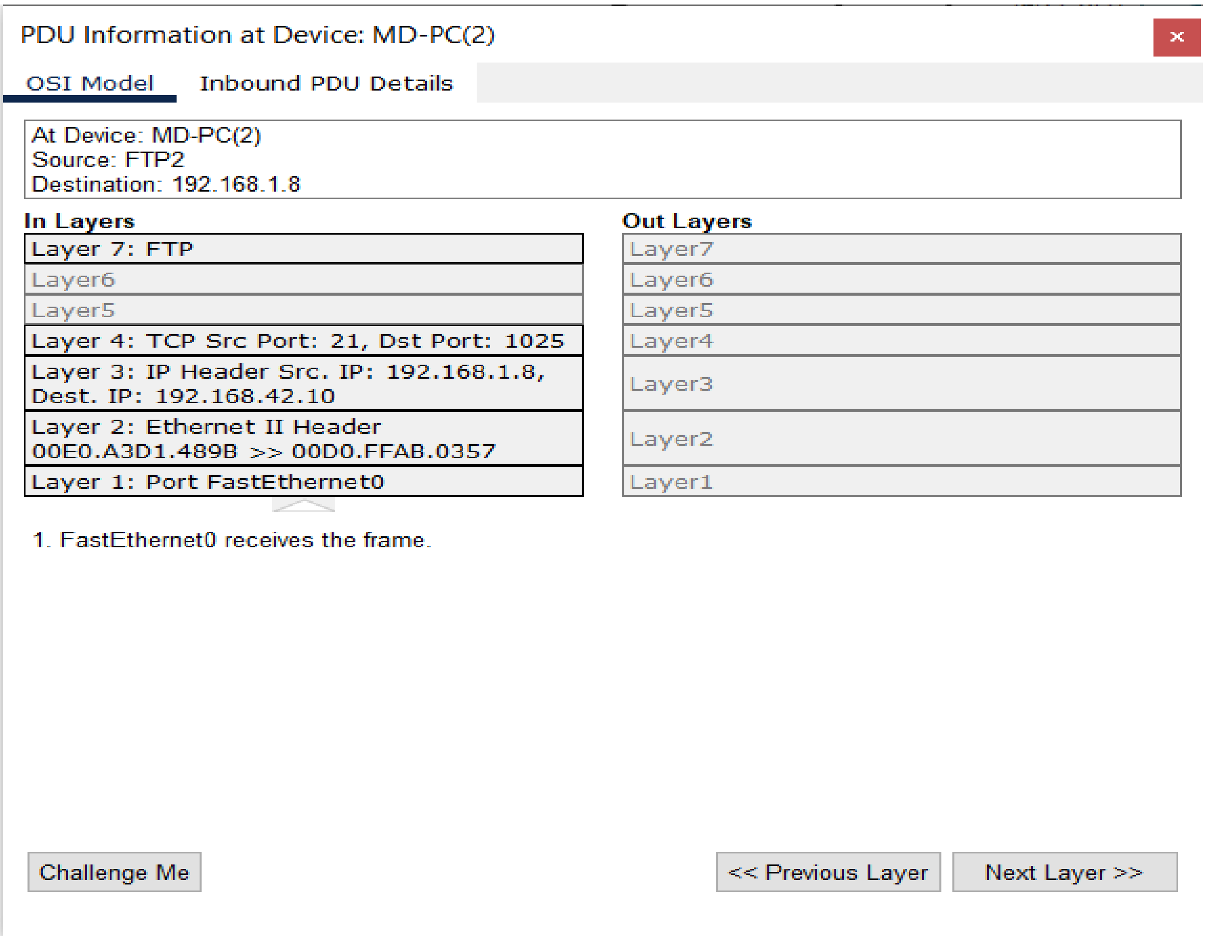
2.2 Switch , Router Branch 2, serverRouter, serverSwitch, FTP1

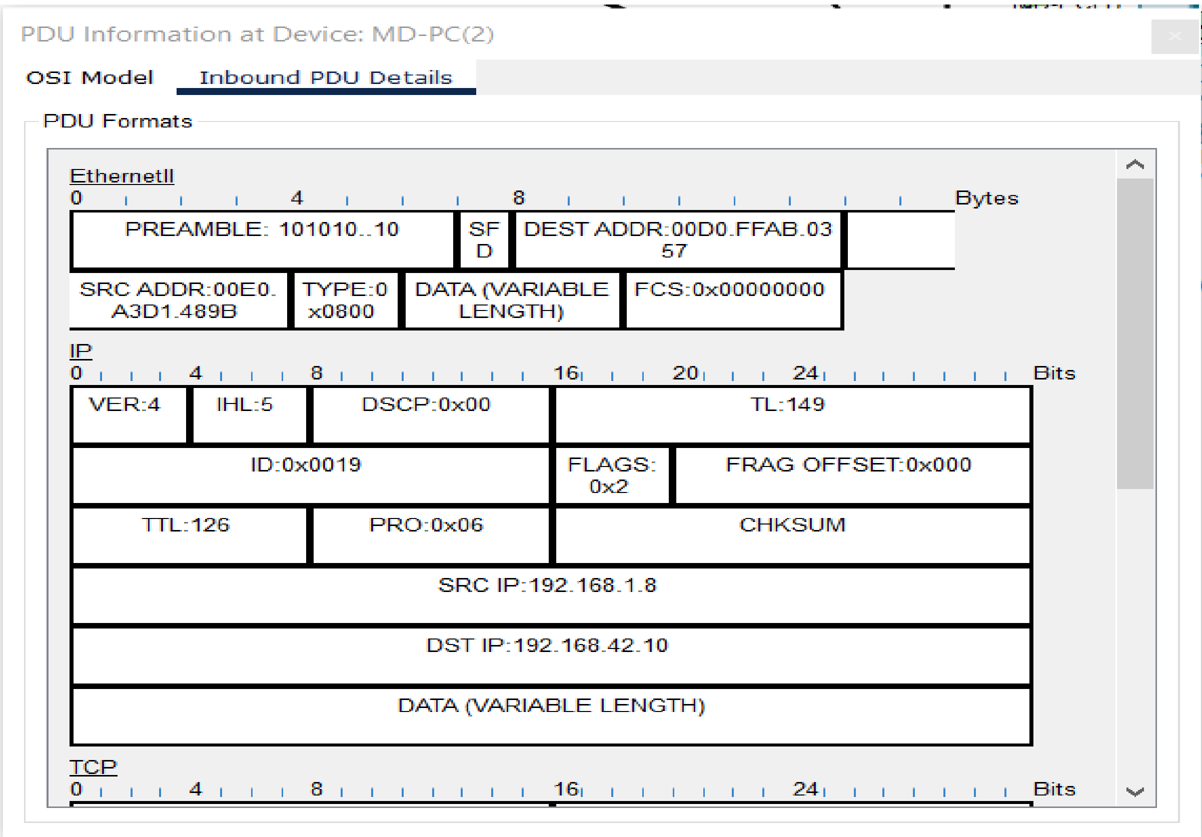
Simulation Panel

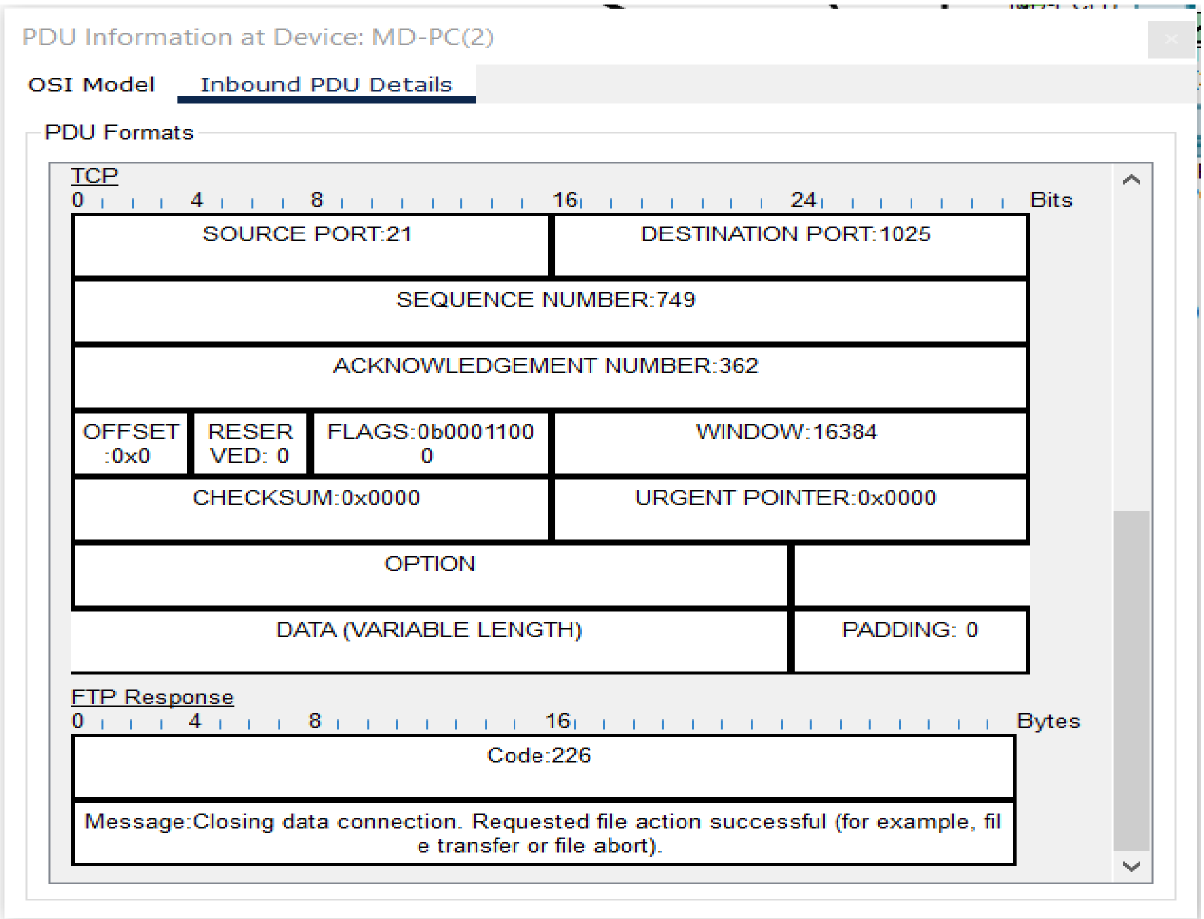
Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	MD-PC(2)	FTP
	0.001	MD-PC(2)	2.2 Switch	FTP
	0.002	2.2 Switch	Router Br...	FTP
	0.009	Router Bran...	2.2 Switch	FTP
	0.010	2.2 Switch	MD-PC(2)	FTP
	0.010	--	MD-PC(2)	FTP
	0.011	MD-PC(2)	2.2 Switch	FTP
	0.012	2.2 Switch	Router Br...	FTP
	0.019	Router Bran...	2.2 Switch	FTP
	0.020	2.2 Switch	MD-PC(2)	FTP
	0.020	--	MD-PC(2)	FTP
	0.021	MD-PC(2)	2.2 Switch	FTP
	0.022	2.2 Switch	Router Br...	FTP
	0.029	Router Bran...	2.2 Switch	FTP
	0.030	2.2 Switch	MD-PC(2)	FTP
	0.030	--	MD-PC(2)	TCP
	0.031	MD-PC(2)	2.2 Switch	TCP
	0.032	2.2 Switch	Router Br...	TCP
	0.039	Router Bran...	2.2 Switch	TCP
	0.040	2.2 Switch	MD-PC(2)	TCP
	0.040	--	MD-PC(2)	FTP
	0.041	MD-PC(2)	2.2 Switch	TCP
	0.041	--	MD-PC(2)	FTP
	0.042	MD-PC(2)	2.2 Switch	FTP
	0.042	2.2 Switch	Router Br...	TCP

	0.042	MD-PC(2)	2.2 Switch	FTP
	0.042	2.2 Switch	Router Br...	TCP
	0.043	2.2 Switch	Router Br...	FTP
	0.046	--	MD-PC(2)	TCP
	0.047	MD-PC(2)	2.2 Switch	TCP
	0.048	2.2 Switch	Router Br...	TCP
	0.050	Router Bran...	2.2 Switch	TCP
	0.051	2.2 Switch	MD-PC(2)	TCP
	0.051	--	MD-PC(2)	TCP
	0.052	MD-PC(2)	2.2 Switch	TCP
	0.053	2.2 Switch	Router Br...	TCP
	0.055	Router Bran...	2.2 Switch	FTP
	0.056	2.2 Switch	MD-PC(2)	FTP
	0.060	Router Bran...	2.2 Switch	TCP
	0.061	2.2 Switch	MD-PC(2)	TCP

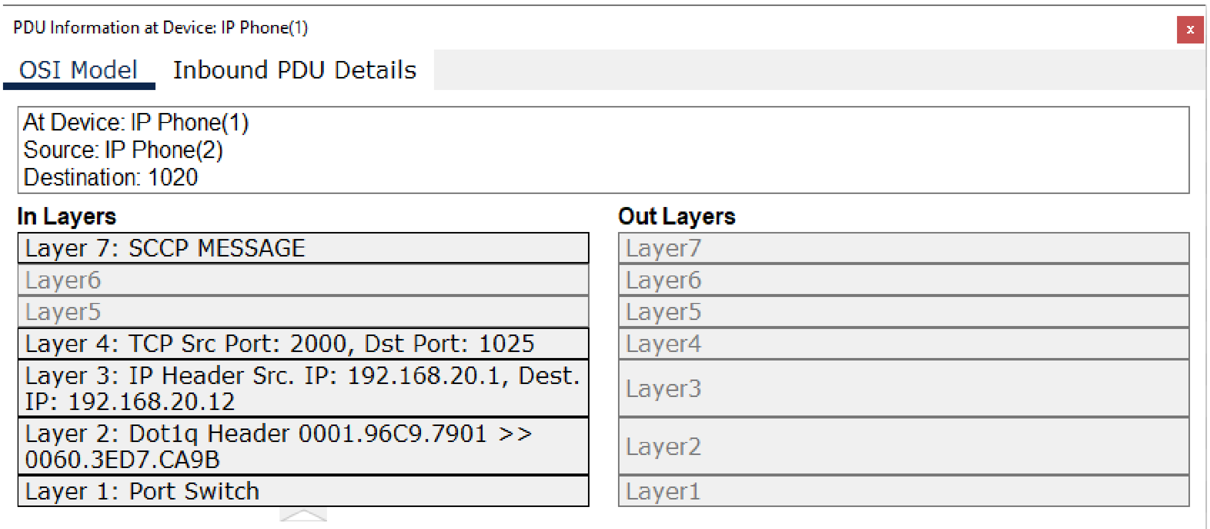

PDU Information at Device: MD-PC(2)
OSI Model
Inbound PDU Details
At Device: MD-PC(2)
Source: FTP2
Destination: 192.168.1.8
In Layers
Layer 7: FTP
Layer6
Layer5
Layer 4: TCP Src Port: 21, Dst Port: 1025
Layer 3: IP Header Src. IP: 192.168.1.8, Dest. IP: 192.168.42.10
Layer 2: Ethernet II Header 00E0.A3D1.489B >> 00D0.FFAB.0357
Layer 1: Port FastEthernet0
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
1. FastEthernet0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: MD-PC(2)
OSI Model
Inbound PDU Details
PDU Formats
EthernetII
0 4 8 Bytes
PREAMBLE: 101010..10
SFD
DEST ADDR:00D0.FFAB.0357
SRC ADDR:00E0.A3D1.489B
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
0 4 8 16 20 24 Bits
VER:4
IHL:5
DSCP:0x00
TL:149
ID:0x0019
FLAGS: 0x2
FRAG OFFSET:0x000
TTL:126
PRO:0x06
CHKSUM
SRC IP:192.168.1.8
DST IP:192.168.42.10
DATA (VARIABLE LENGTH)
TCP
0 4 8 16 24 Bits

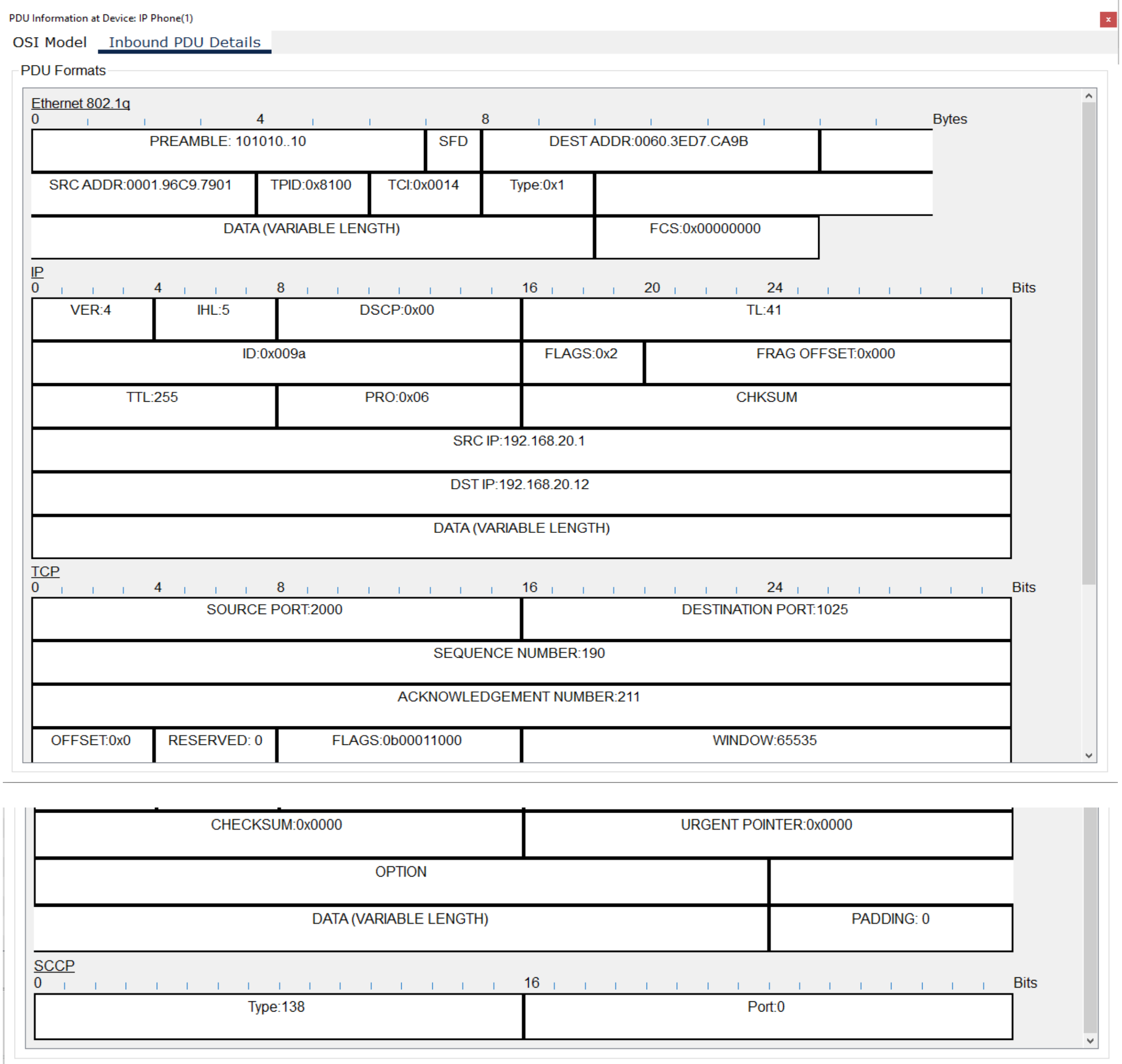

PDU Information at Device: MD-PC(2)
OSI Model
Inbound PDU Details
PDU Formats
TCP
0 4 8 16 24 Bits
SOURCE PORT:21
DESTINATION PORT:1025
SEQUENCE NUMBER:749
ACKNOWLEDGEMENT NUMBER:362
OFFSET :0x0
RESERVED: 0
FLAGS:0b00011000
WINDOW:16384
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0
FTP Response
0 4 8 16 Bytes
Code:226
Message:Closing data connection. Requested file action successful (for example, file transfer or file abort).

Scenario 3: Two users from the second facility of the first branch want to talk via VoIP.

Two users from second facility of second campus want to talk with VoIP in this scenario. "IP Phone(1)" and “Ip Phone(2)” are phones used for these users. “Switch2” and “Router2” are node between "IP Phone(1)" and “IP Phone(2)”. The events that occurs when connecting these phones are shown above.



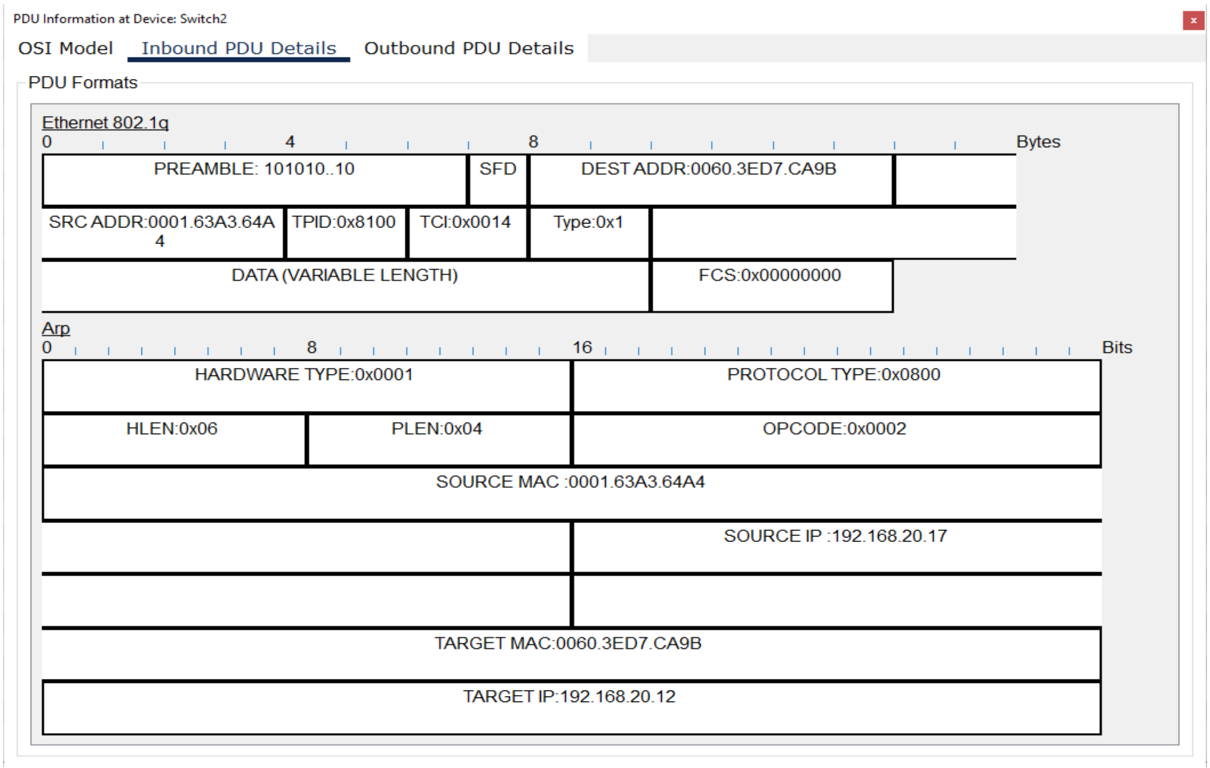
1. Switch receives the frame.



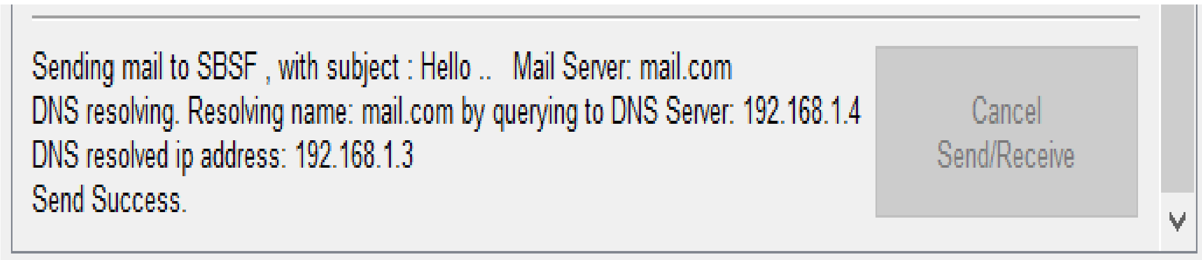
The packet exchange between "Router2", "Switch2" and IP Phones is shown below.These packet exchanges are sorted by events.

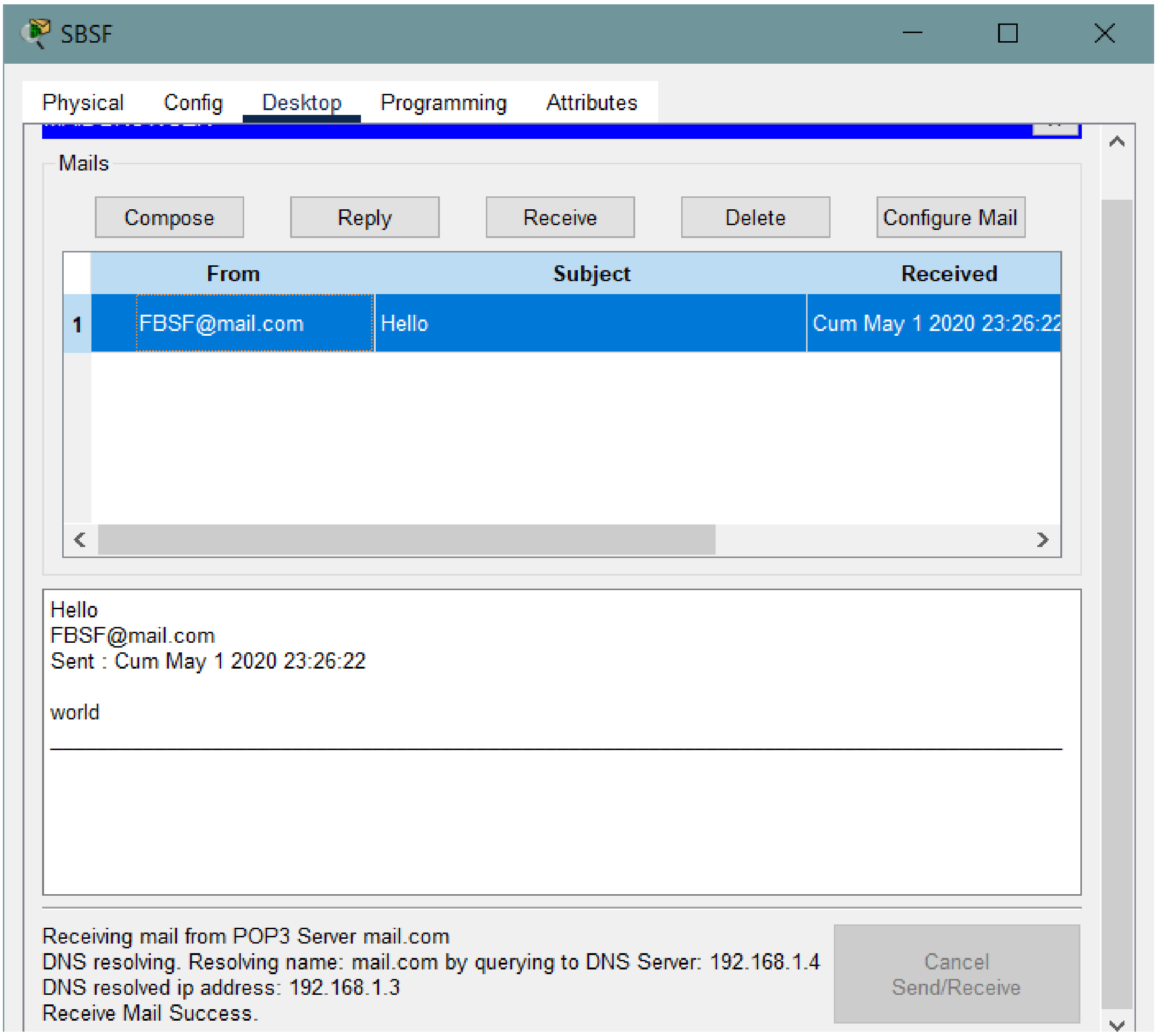
0.027	Switch2	Router2	STP
0.127	--	Switch2	STP
0.128	Switch2	Router2	STP
0.128	--	Switch2	STP
0.129	Switch2	Router2	STP
0.464	Switch2	Router2	STP
0.464	--	IP Phone(1)	SCCP
0.465	IP Phone(1)	Switch2	SCCP
0.466	Switch2	Router2	SCCP
0.467	Router2	Switch2	SCCP
0.468	Switch2	IP Phone(1)	SCCP
0.468	--	IP Phone(1)	SCCP
0.469	IP Phone(1)	Switch2	SCCP
0.470	Switch2	Router2	SCCP
0.471	Router2	Switch2	SCCP
0.471	--	Router2	SCCP
0.472	Router2	Switch2	SCCP
0.472	Switch2	IP Phone(2)	SCCP
0.473	--	Switch2	STP
0.473	Switch2	IP Phone(1)	SCCP
0.473	--	Switch2	STP
0.474	Switch2	Router2	STP
0.474	Switch2	IP Phone(2)	STP
0.474	Switch2	IP Phone(3)	STP
0.474	Switch2	IP Phone(4)	STP
0.474	Switch2	IP Phone(5)	STP
0.474	Switch2	IP Phone(1)	STP
0.474	--	IP Phone(2)	SCCP
0.475	IP Phone(2)	voip(2)	STP
0.475	IP Phone(3)	voip(3)	STP
0.475	IP Phone(4)	voip(4)	STP
0.475	IP Phone(5)	voip(5)	STP
0.475	IP Phone(1)	voip(1)	STP
0.475	IP Phone(2)	Switch2	SCCP
0.476	Switch2	Router2	SCCP

0.477	Router2	Switch2	SCCP
0.477	--	Router2	SCCP
0.478	Router2	Switch2	SCCP
0.478	Switch2	IP Phone(1)	SCCP
0.479	Switch2	IP Phone(2)	SCCP
0.479	IP Phone(1)	Switch2	SCCP
0.480	IP Phone(2)	Switch2	SCCP
0.480	Switch2	Router2	SCCP
0.481	Switch2	Router2	SCCP
0.481	Router2	Switch2	SCCP
0.482	Router2	Switch2	SCCP
0.482	Switch2	IP Phone(2)	SCCP
0.482	--	IP Phone(2)	RTP
0.482	--	IP Phone(2)	ARP
0.483	Switch2	IP Phone(1)	SCCP
0.483	--	IP Phone(1)	RTP
0.483	IP Phone(2)	Switch2	ARP
0.483	--	IP Phone(1)	ARP
0.484	IP Phone(1)	Switch2	ARP
0.484	Switch2	Router2	ARP
0.484	Switch2	IP Phone(1)	ARP
0.484	Switch2	IP Phone(3)	ARP
0.484	Switch2	IP Phone(4)	ARP
0.484	Switch2	IP Phone(5)	ARP
0.485	Switch2	Router2	ARP
0.485	Switch2	IP Phone(2)	ARP
0.485	Switch2	IP Phone(3)	ARP
0.485	Switch2	IP Phone(4)	ARP
0.485	Switch2	IP Phone(5)	ARP
0.485	IP Phone(1)	Switch2	ARP
0.486	IP Phone(2)	Switch2	ARP
0.486	Switch2	IP Phone(2)	ARP



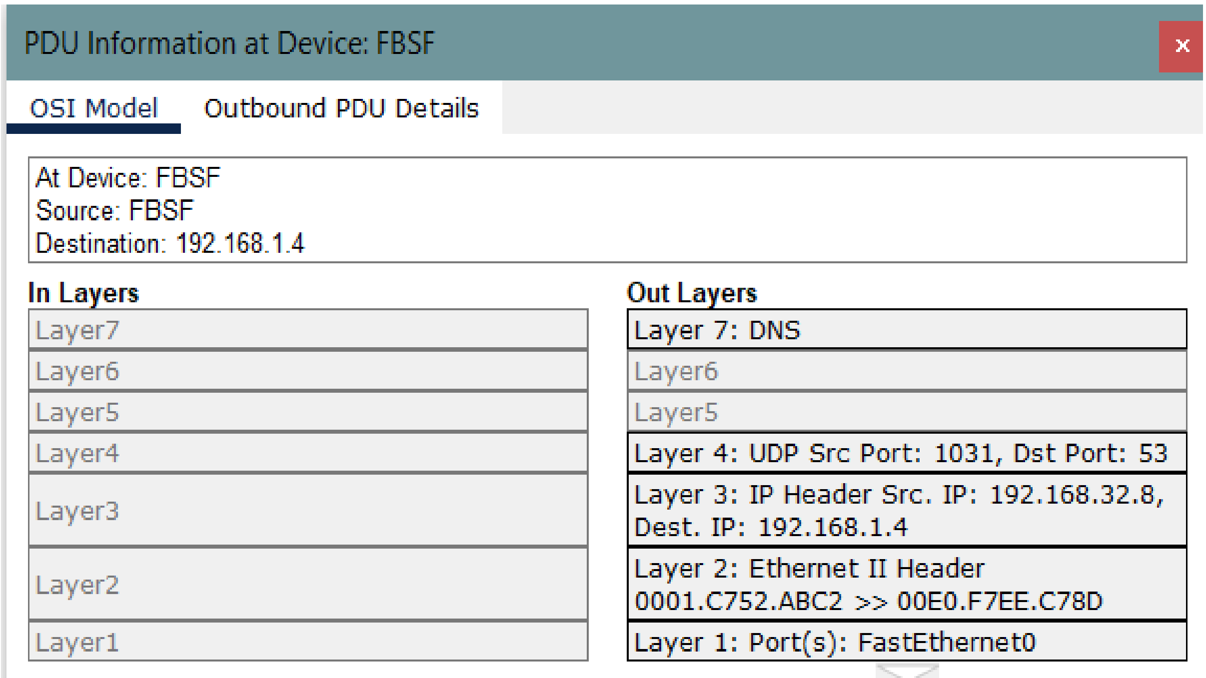
Scenario 4: A user in the second facility of the first branch wants to send an email message to his friend in the second facility of the second branch.





In the first picture, you can see that the mail has been successfully transmitted from the first branch to the second branch. In the second picture, you can see the incoming mail.

First, DNS operation takes place to meet our request.



Layer 7: The DNs client sends a DNS query to the DNS server.

Layer 4: The device encapsulates the PDU into an UDP segment.

Layer 3:The source IP address is not specified. The device sets it to the port's IP address. The destination IP address 192.168.1.4 is not in the same subnet and is not the broadcast address. The default gateway is set. The device sets the next-hop to default gateway.

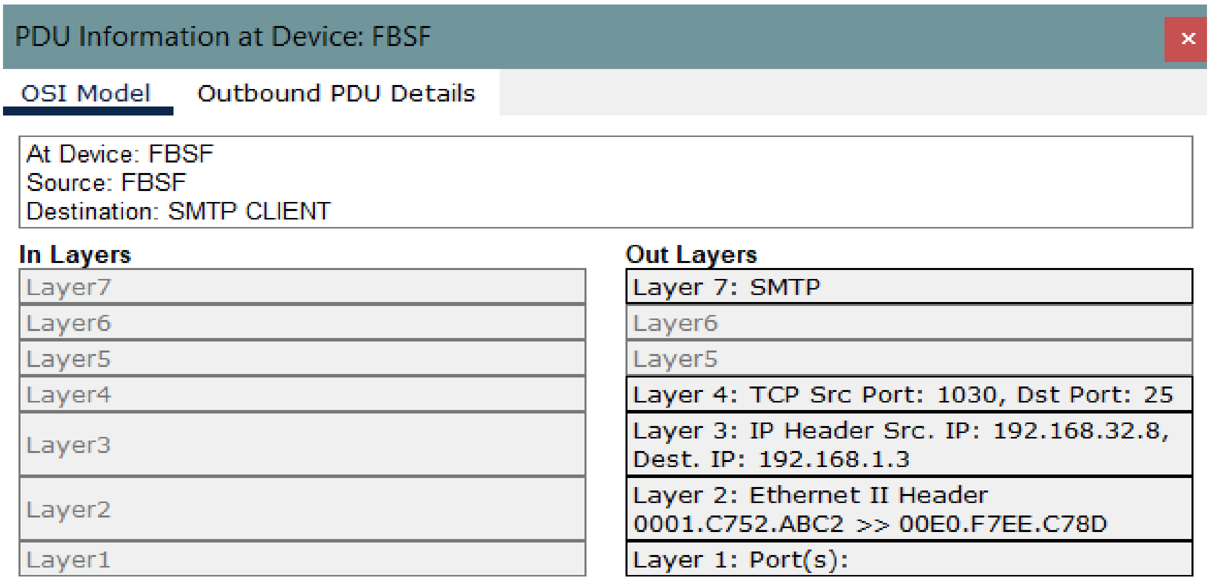
Layer 2: The next-hop IP address is a unicast. The ARP process looks it up in the ARP table. The next-hop IP address is in the ARP table. The ARP process sets the frame's destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.

Layer 1: FastEthernet sends out the frame.

Then the necessary answers about DNS are sent or received. TCP protocols for identity checks take place as follows.

Time(sec)	Last Device	At Device	Type
0.000	--	FBSF	DNS
0.001	FBSF	1.2 Switch	DNS
0.002	1.2 Switch	Router Br...	DNS
0.003	Router Bran...	Server router	DNS
0.004	Server router	serverSwitch	DNS
0.005	serverSwitch	DNS	DNS
0.006	DNS	serverSwitch	DNS
0.007	serverSwitch	Server router	DNS
0.008	Server router	Router Br...	DNS
0.009	Router Bran...	1.2 Switch	DNS
0.010	1.2 Switch	FBSF	DNS
0.010	--	FBSF	TCP
0.011	FBSF	1.2 Switch	TCP
0.012	1.2 Switch	Router Br...	TCP
0.013	Router Bran...	Server router	TCP
0.014	Server router	serverSwitch	TCP
0.015	serverSwitch	Mail server	TCP
0.016	Mail server	serverSwitch	TCP
0.017	serverSwitch	Server router	TCP
0.018	Server router	Router Br...	TCP
0.019	Router Bran...	1.2 Switch	TCP
0.020	1.2 Switch	FBSF	TCP
0.020	--	FBSF	SMTP
0.021	FBSF	1.2 Switch	TCP
0.021	--	FBSF	SMTP

SMTP operations start after TCP operations. SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used when sending and receiving emails between servers.[16]



Layer 7: The device sends out a SMTP packet.

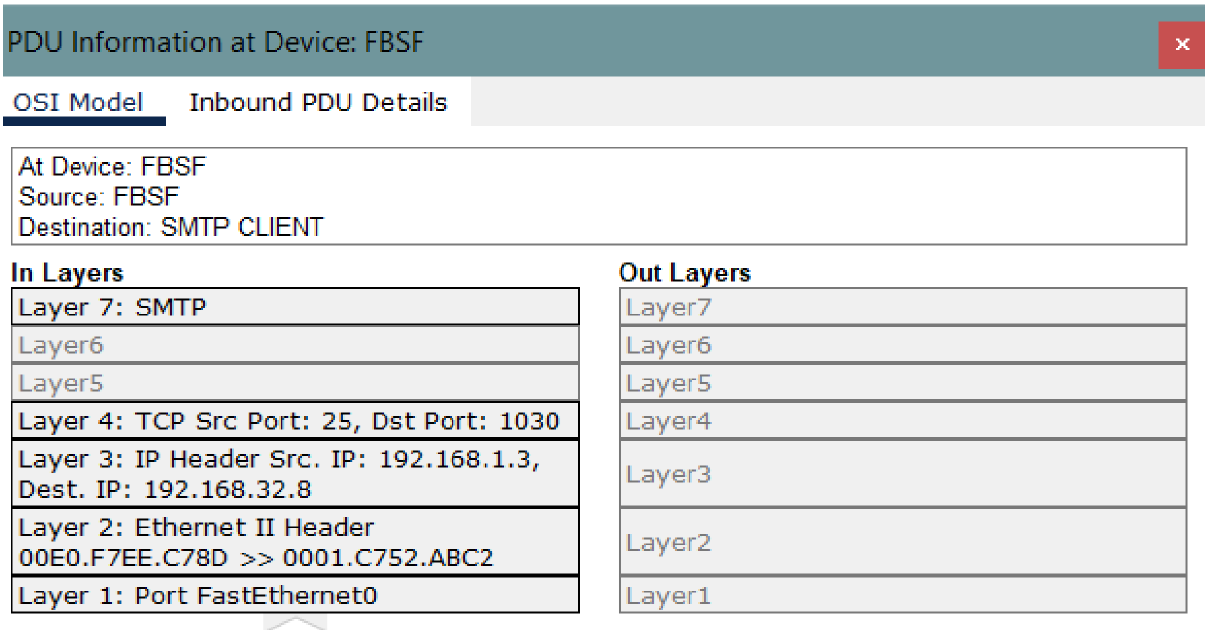
Layer 4: Sent segment information: the sequence number 1, the ACK number 1, and the data length 61.

Layer 3: The destination IP address 192.168.1.3 is not in the same subnet and is not the broadcast address.

Layer 2: The next-hop IP address is a unicast. The ARP process looks it up in the ARP table. The next-hop IP address is in the ARP table. The ARP process sets the frame’s destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.

Layer 1: The port FastEthernet0 is sending another frame at this time. The device buffers the frame to be sent later.

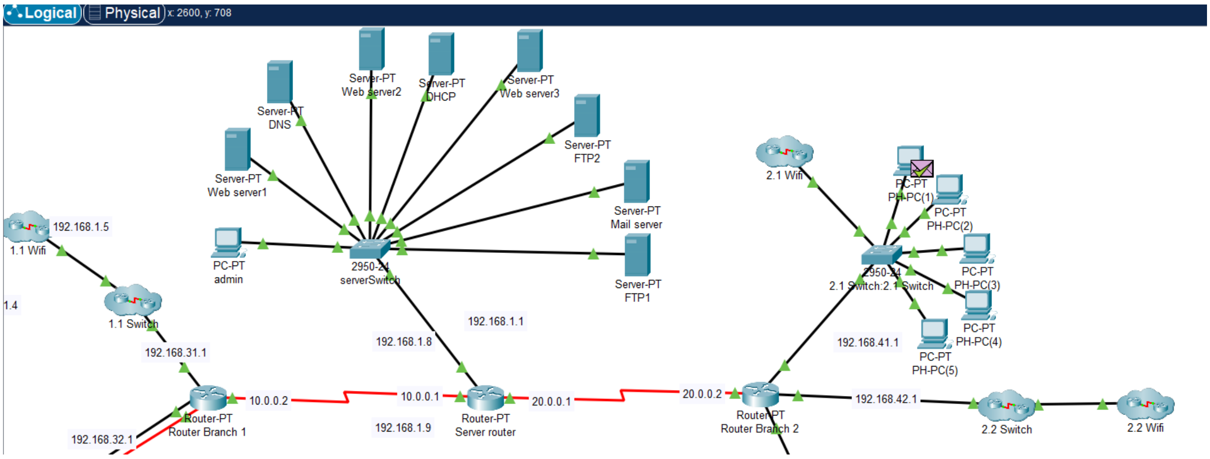
After the necessary TCP and SMTP processes, our final confirmation that we have sent our mail to the other party takes place.



Layer 7: The device receives a SMTP packet.
Layer 4: The device receives a TCP PUSH+ACK segment on the connection to 192.168.1.3 on port 25. Received segment information: the sequence number 1, the ACK number 62, and the data length 24. The TCP segment has the expected peer sequence number. The TCP segment has the expected ACK number. The device pops the last sent segment from the buffer. TCP processes payload data. TCP reassembles all data segments and passes to the upper layer.

Layer 3: The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
Layer 2: The frame's destination MAC address matches the receiving port's MAC address, the broadcast address or a multicast address. The device decapsulates the PDU froö the Ethernet frame.
Layer 1: FastEthernet0 receives the frame.

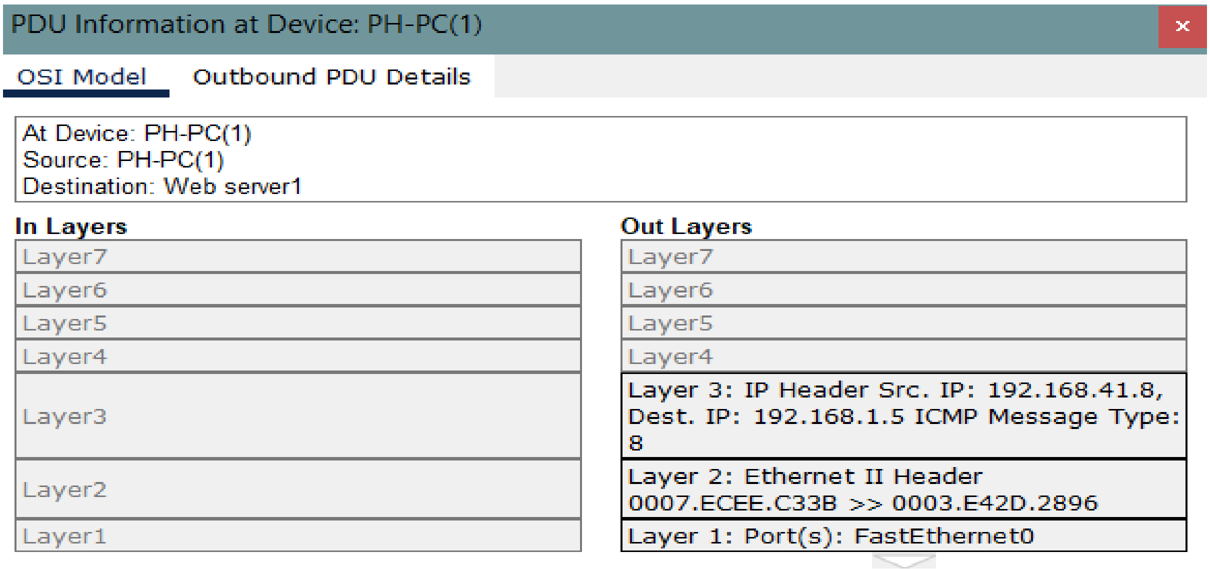
Scenario 5: A user from the first facility of the second branch pings the Web server of the second facility of the first branch.



First, the ping goes from the computer to the switch. It is then connected to the router of the second branch. It goes from that router to the router that connects the two branches. Since our aim is the server facility, it goes to the switch where the servers are located. From there it goes to our target server. After connecting to the server our response goes to our original device and is verified.

s.	Time(sec)	Last Device	At Device	Type
	0.000	--	PH-PC(1)	ICMP
	0.001	PH-PC(1)	2.1 Switch:2.1 Switch	ICMP
	0.002	2.1 Switch:2.1 Switch	Router Branch 2	ICMP
	0.003	Router Branch 2	Server router	ICMP
	0.004	Server router	serverSwitch	ICMP
	0.005	serverSwitch	Web server1	ICMP
	0.006	Web server1	serverSwitch	ICMP
	0.007	serverSwitch	Server router	ICMP
	0.008	Server router	Router Branch 2	ICMP
	0.009	Router Branch 2	2.1 Switch:2.1 Switch	ICMP
	0.010	2.1 Switch:2.1 Switch	PH-PC(1)	ICMP

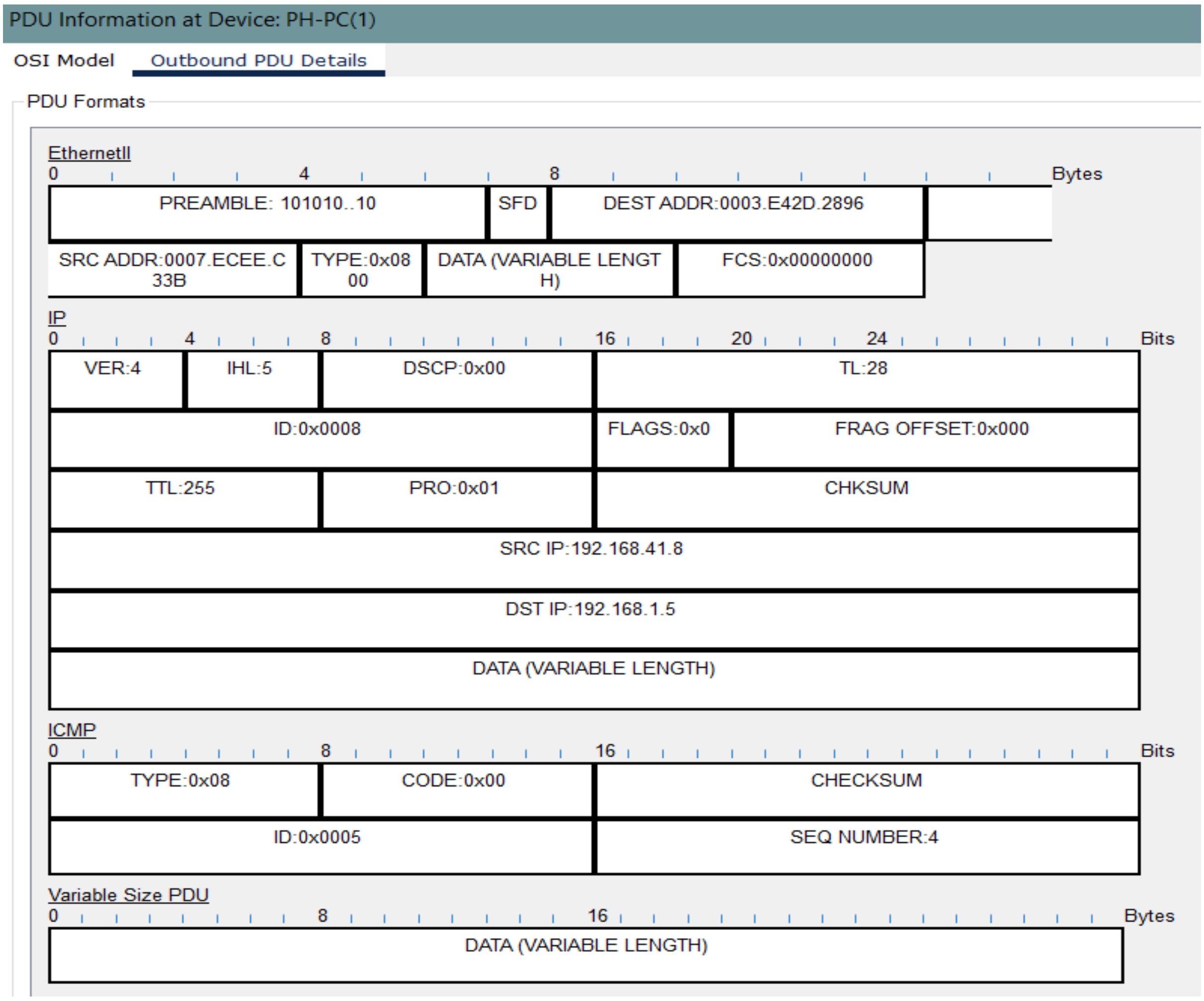
First ICMP operation:



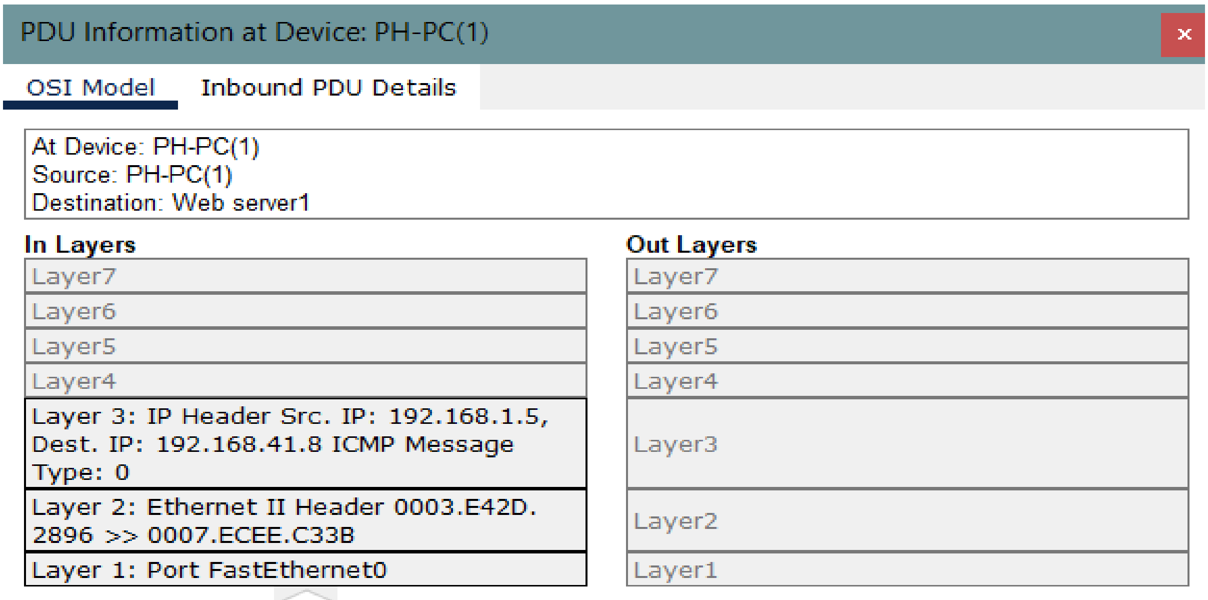
Layer 3: The Ping process starts the next ping request and creates an ICMP Echo Request message and sends it to the lower process. The source IP address is not specified. The device sets TTL in the packet header. The destination IP address 192.168.1.5 is not in the same subnet and is not the broadcast address. The default gateway is set. The device sets the next-hop to default gateway.

Layer 2: The next-hop IP address is a unicast. The ARP process looks it up in the ARP table. The next-hop IP address is in the ARP table. The ARP process sets the frame’s destination MAC address to the one found in the table. The device encapsulates the PDU into an Ethernet frame.

Layer 1: FastEthernet0 sends out the frame.



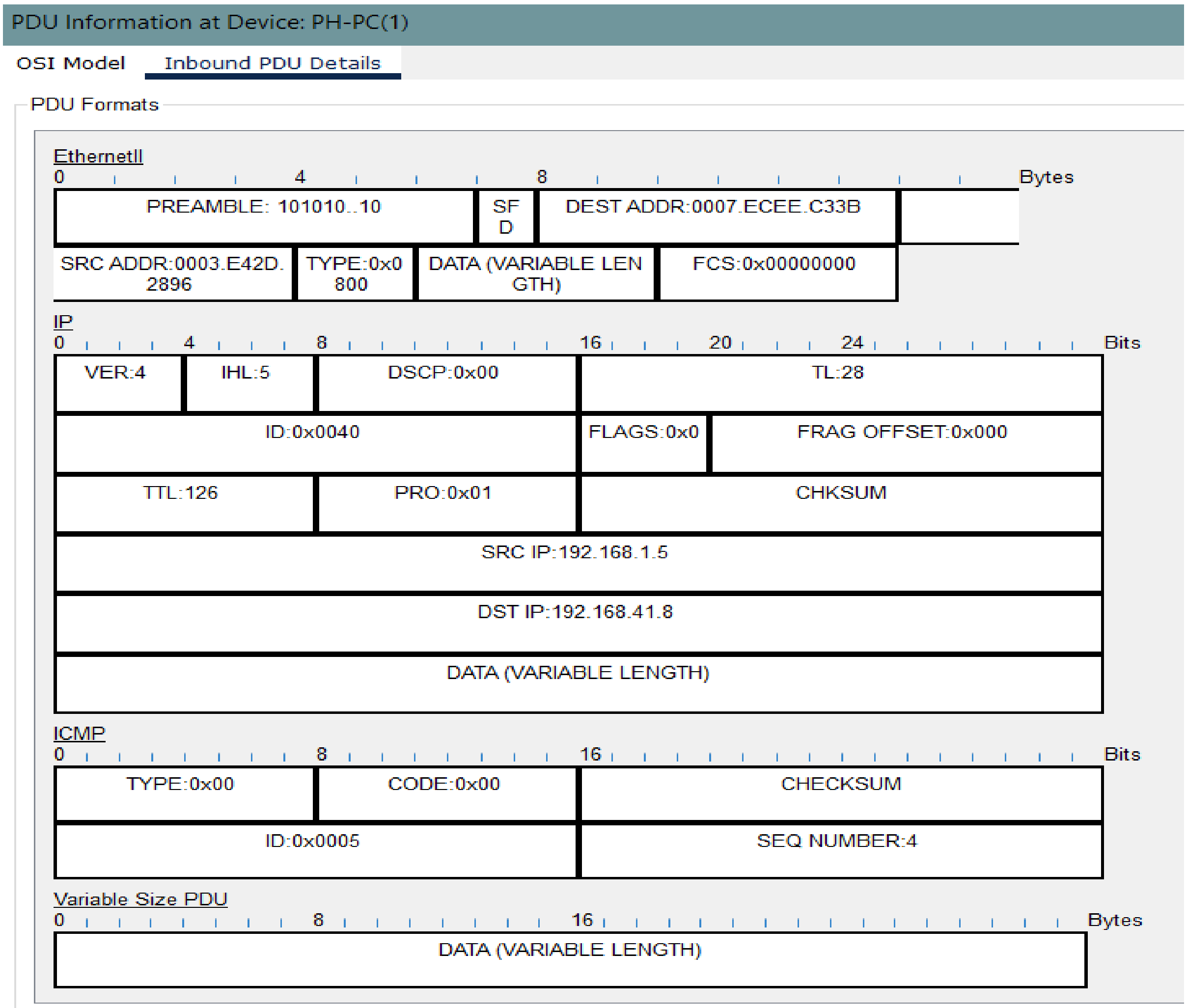
Last ICMP operation:



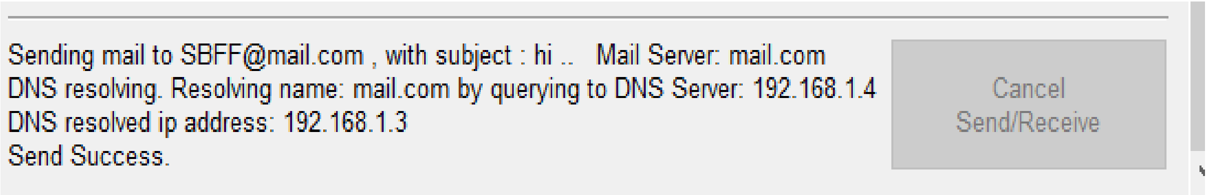
Layer 3: The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet. The packet is an ICMP packet. The ICMP process processes it. The ICMP process received an Echo Reply message. The ping process received an Echo Reply message.

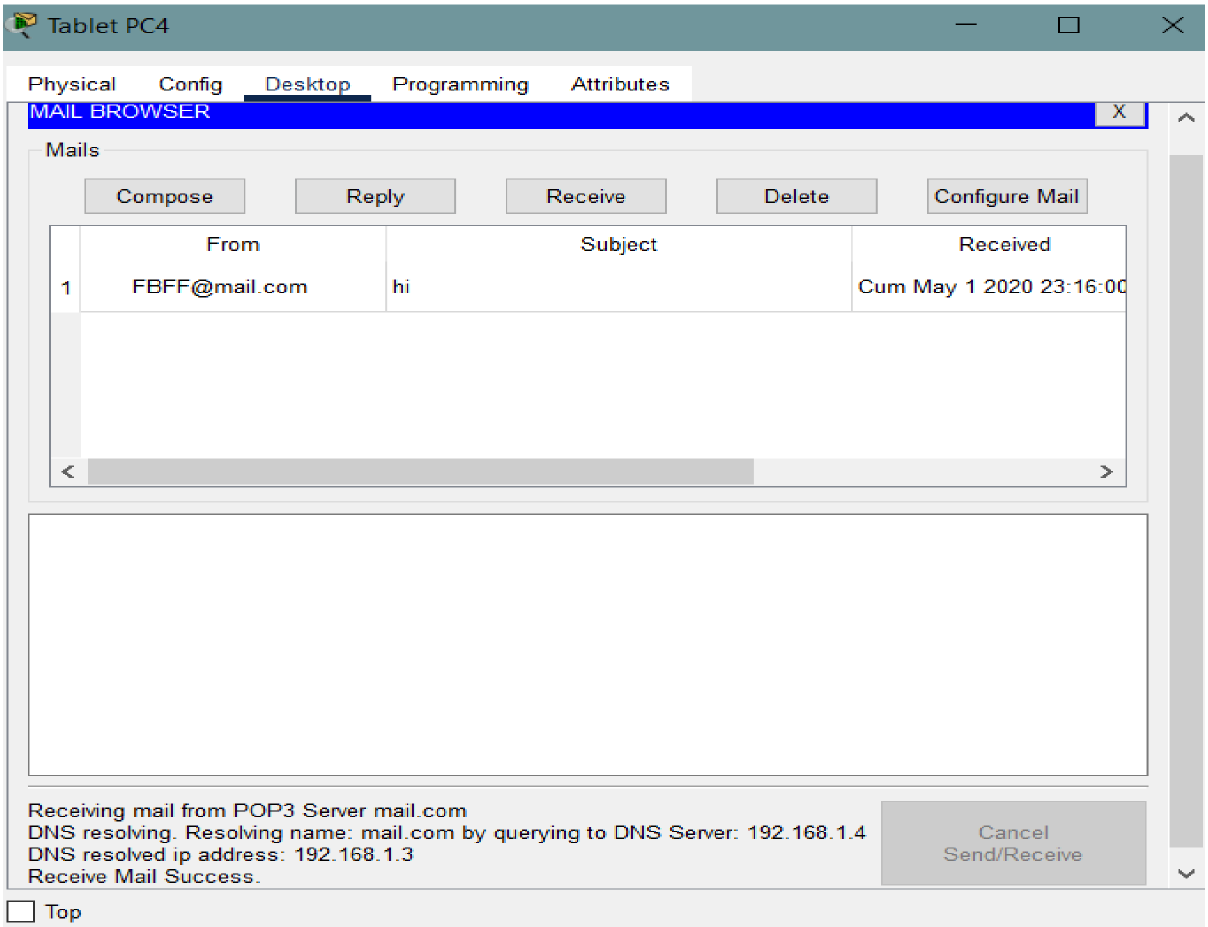
Layer 2: The frame's destination MAC address matches the receiving port's MAC address, the broadcast address or a multicast address. The device decapsulates the PDU from the Ethernet frame.

Layer 1: FastEthernet0 receives the frame.



Scenario 6: A laptop user from the first facility of the first branch office wants to send email to her friend in the first facility of the second branch office.





This scenario is similar to scenario 4. It goes through the same layers and stages as in scenario 4. However, in this scenario, different devices are also shown in the simulation as they visit different branches and different facilities. The simulation of this scenario is as follows.

First, DNS operations are performed, then TCP operations for identity control, and then SMTP operations for mail operations.

Simulation Panel

Event List

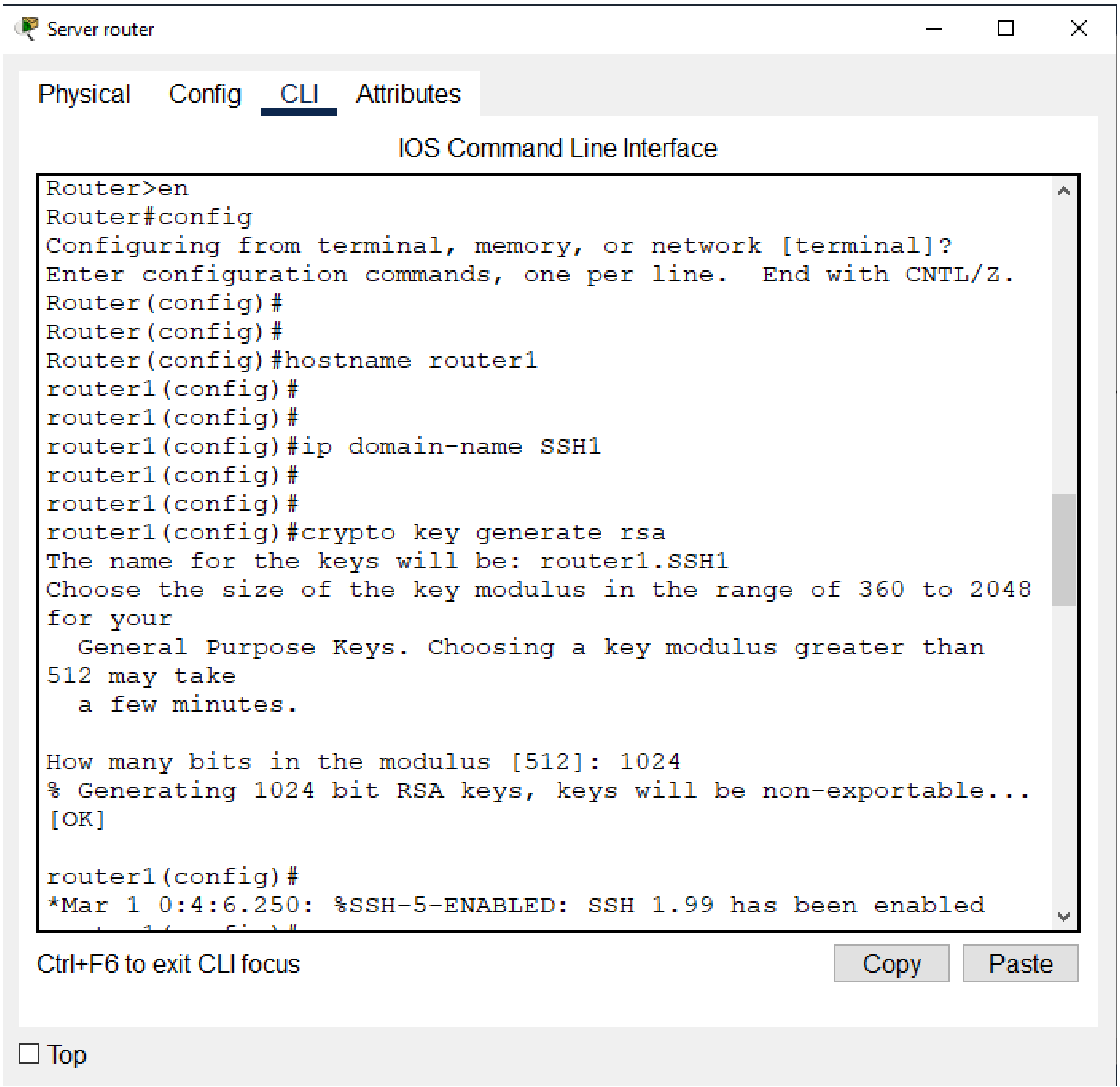
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop5	DNS
	0.001	Laptop5	1.1 Wifi:1....	DNS
	0.002	1.1 Wifi:1.1 ...	1.1 Switch	DNS
	0.003	1.1 Switch	Router Br...	DNS
	0.003	--	1.1 Wifi:1....	DNS
	0.004	1.1 Wifi:1.1 ...	CE-Phone(1)	DNS
	0.004	1.1 Wifi:1.1 ...	CE-Phone(2)	DNS
	0.004	1.1 Wifi:1.1 ...	CE-Phone(4)	DNS
	0.004	1.1 Wifi:1.1 ...	CE-Phone(5)	DNS
	0.004	1.1 Wifi:1.1 ...	Laptop6	DNS
	0.004	1.1 Wifi:1.1 ...	CE-Phone(3)	DNS
	0.004	1.1 Wifi:1.1 ...	Laptop8	DNS
	0.004	1.1 Wifi:1.1 ...	Laptop5	DNS
	0.004	1.1 Wifi:1.1 ...	Laptop9	DNS
	0.004	1.1 Wifi:1.1 ...	Laptop7	DNS
	0.004	Router Bran...	Server router	DNS
	0.005	Server router	serverSwitch	DNS
	0.006	serverSwitch	DNS	DNS
	0.007	DNS	serverSwitch	DNS
	0.008	serverSwitch	Server router	DNS
	0.009	Server router	Router Br...	DNS
	0.010	Router Bran...	1.1 Switch	DNS
	0.011	1.1 Switch	1.1 Wifi:1....	DNS
	0.012	1.1 Wifi:1.1 ...	CE-Phone(1)	DNS
	0.012	1.1 Wifi:1.1 ...	CE-Phone(2)	DNS
	0.012	1.1 Wifi:1.1 ...	CE-Phone(4)	DNS
	0.012	1.1 Wifi:1.1 ...	CE-Phone(5)	DNS
	0.012	1.1 Wifi:1.1 ...	Laptop6	DNS
	0.012	1.1 Wifi:1.1 ...	CE-Phone(3)	DNS
	0.012	1.1 Wifi:1.1 ...	Laptop8	DNS
	0.012	1.1 Wifi:1.1 ...	Laptop5	DNS
	0.012	1.1 Wifi:1.1 ...	Laptop7	DNS
	0.012	1.1 Wifi:1.1	Laptop9	DNS
	0.012	--	Laptop5	TCP
	0.014	--	Laptop5	TCP
	0.015	Laptop5	1.1 Wifi:1....	TCP
	0.016	1.1 Wifi:1.1 ...	1.1 Switch	TCP
	0.017	1.1 Switch	Router Br...	TCP
	0.018	Router Bran...	Server router	TCP
	0.019	Server router	serverSwitch	TCP
	0.020	serverSwitch	Mail server	TCP
	0.020	--	1.1 Wifi:1....	TCP
	0.021	1.1 Wifi:1.1 ...	CE-Phone(1)	TCP
	0.021	1.1 Wifi:1.1 ...	CE-Phone(2)	TCP
	0.021	1.1 Wifi:1.1 ...	CE-Phone(4)	TCP
	0.021	1.1 Wifi:1.1 ...	CE-Phone(5)	TCP
	0.021	1.1 Wifi:1.1 ...	Laptop6	TCP
	0.021	1.1 Wifi:1.1 ...	CE-Phone(3)	TCP
	0.021	1.1 Wifi:1.1 ...	Laptop8	TCP
	0.021	1.1 Wifi:1.1 ...	Laptop5	TCP
	0.021	1.1 Wifi:1.1 ...	Laptop9	TCP
	0.021	1.1 Wifi:1.1 ...	Laptop7	TCP
	0.021	Mail server	serverSwitch	TCP
	0.022	serverSwitch	Server router	TCP
	0.023	Server router	Router Br...	TCP
	0.024	Router Bran...	1.1 Switch	TCP
	0.025	1.1 Switch	1.1 Wifi:1....	TCP
	0.026	1.1 Wifi:1.1 ...	CE-Phone(1)	TCP
	0.026	1.1 Wifi:1.1 ...	CE-Phone(2)	TCP
	0.026	1.1 Wifi:1.1 ...	CE-Phone(4)	TCP
	0.026	1.1 Wifi:1.1 ...	CE-Phone(5)	TCP
	0.026	1.1 Wifi:1.1 ...	Laptop6	TCP
	0.026	1.1 Wifi:1.1 ...	CE-Phone(3)	TCP
	0.026	1.1 Wifi:1.1 ...	Laptop8	TCP
	0.026	1.1 Wifi:1.1 ...	Laptop5	TCP
	0.026	1.1 Wifi:1.1	Laptop7	TCP

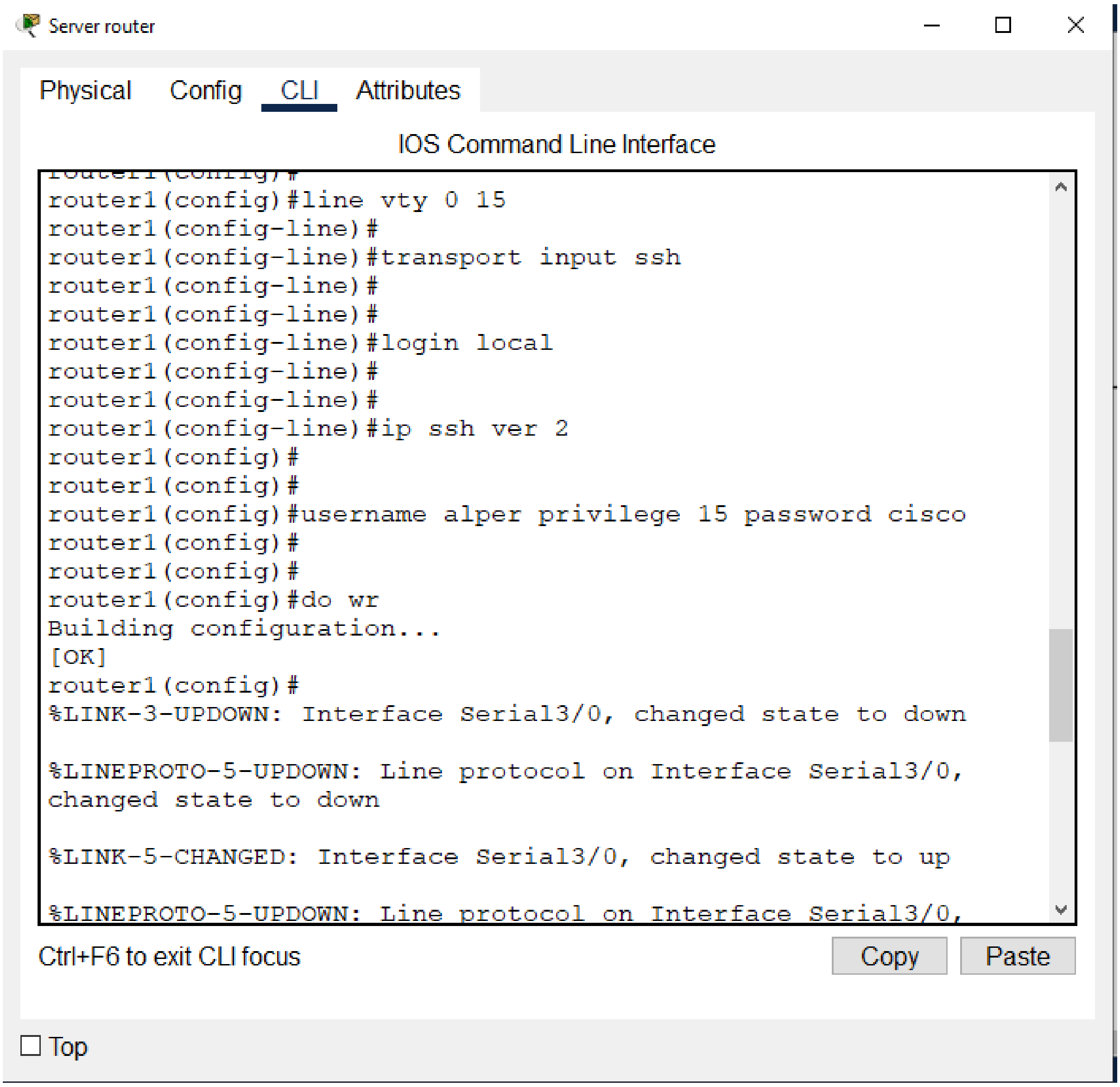
Event List

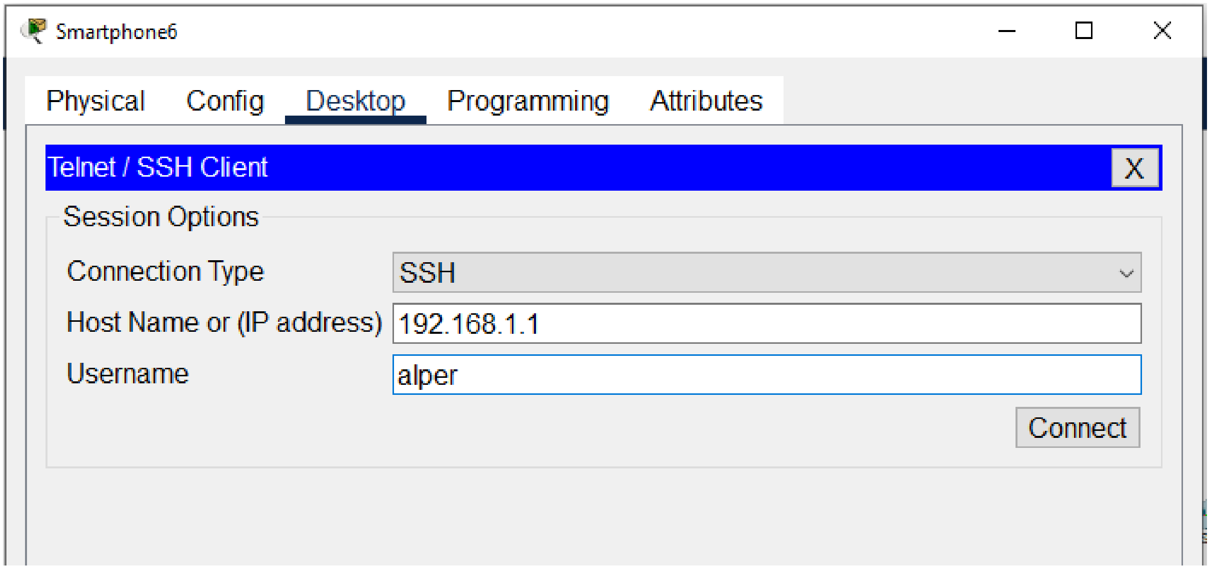
Vis.	Time(sec)	Last Device	At Device	Type
	0.026	1.1 Wifi:1.1 ...	Laptop7	TCP
	0.026	1.1 Wifi:1.1 ...	Laptop9	TCP
	0.026	--	Laptop5	SMTP
	0.030	--	Laptop5	TCP
	0.031	Laptop5	1.1 Wifi:1....	TCP
	0.032	1.1 Wifi:1.1 ...	1.1 Switch	TCP
	0.033	1.1 Switch	Router Br...	TCP
	0.034	Router Bran...	Server router	TCP
	0.034	--	Laptop5	SMTP
	0.035	Laptop5	1.1 Wifi:1....	SMTP
	0.035	Server router	serverSwitch	TCP
	0.036	1.1 Wifi:1.1 ...	1.1 Switch	SMTP
	0.036	serverSwitch	Mail server	TCP
	0.036	--	1.1 Wifi:1....	TCP
	0.037	1.1 Wifi:1.1 ...	CE-Phone(1)	TCP
	0.037	1.1 Wifi:1.1 ...	CE-Phone(2)	TCP
	0.037	1.1 Wifi:1.1 ...	CE-Phone(4)	TCP
	0.037	1.1 Wifi:1.1 ...	CE-Phone(5)	TCP
	0.037	1.1 Wifi:1.1 ...	Laptop6	TCP
	0.037	1.1 Wifi:1.1 ...	CE-Phone(3)	TCP
	0.037	1.1 Wifi:1.1 ...	Laptop8	TCP
	0.037	1.1 Wifi:1.1 ...	Laptop5	TCP
	0.037	1.1 Wifi:1.1 ...	Laptop9	TCP
	0.037	1.1 Wifi:1.1 ...	Laptop7	TCP
	0.037	1.1 Switch	Router Br...	SMTP
	0.038	Router Bran...	Server router	SMTP
	0.039	Server router	serverSwitch	SMTP
	0.040	serverSwitch	Mail server	SMTP
	0.041	Mail server	serverSwitch	SMTP
	0.041	--	1.1 Wifi:1....	SMTP
	0.042	1.1 Wifi:1.1 ...	CE-Phone(1)	SMTP
	0.042	1.1 Wifi:1.1 ...	CE-Phone(2)	SMTP
	0.042	1.1 Wifi:1.1	CE-Phone(4)	SMTP
	0.042	1.1 Wifi:1.1 ...	CE-Phone(4)	SMTP
	0.042	1.1 Wifi:1.1 ...	CE-Phone(5)	SMTP
	0.042	1.1 Wifi:1.1 ...	Laptop6	SMTP
	0.042	1.1 Wifi:1.1 ...	CE-Phone(3)	SMTP
	0.042	1.1 Wifi:1.1 ...	Laptop8	SMTP
	0.042	1.1 Wifi:1.1 ...	Laptop5	SMTP
	0.042	1.1 Wifi:1.1 ...	Laptop9	SMTP
	0.042	1.1 Wifi:1.1 ...	Laptop7	SMTP
	0.042	serverSwitch	Server router	SMTP
	0.043	Server router	Router Br...	SMTP
	0.044	Router Bran...	1.1 Switch	SMTP
	0.045	1.1 Switch	1.1 Wifi:1....	SMTP
	0.046	1.1 Wifi:1.1 ...	CE-Phone(1)	SMTP
	0.046	1.1 Wifi:1.1 ...	CE-Phone(2)	SMTP
	0.046	1.1 Wifi:1.1 ...	CE-Phone(4)	SMTP
	0.046	1.1 Wifi:1.1 ...	CE-Phone(5)	SMTP
	0.046	1.1 Wifi:1.1 ...	Laptop6	SMTP
	0.046	1.1 Wifi:1.1 ...	CE-Phone(3)	SMTP
	0.046	1.1 Wifi:1.1 ...	Laptop8	SMTP
	0.046	1.1 Wifi:1.1 ...	Laptop5	SMTP
	0.046	1.1 Wifi:1.1 ...	Laptop7	SMTP
	0.046	1.1 Wifi:1.1 ...	Laptop9	SMTP
	0.046	--	Laptop5	TCP

Scenario 7: A smartphone user from the third facility of the second branch office wants to use ssh to connect to a Web server in the third facility of the first branch office.

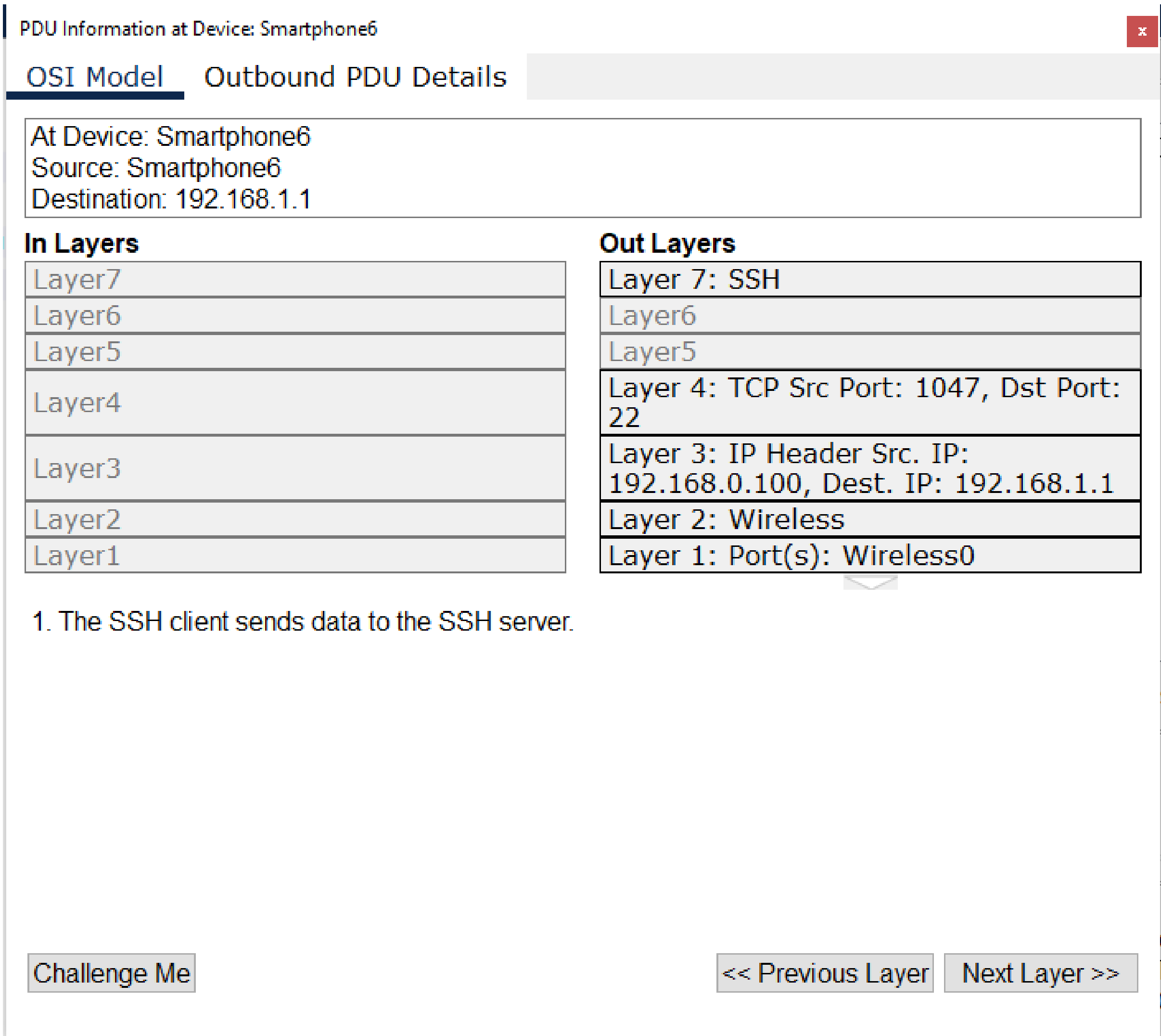
Server router ssh configuration is done as shown below.

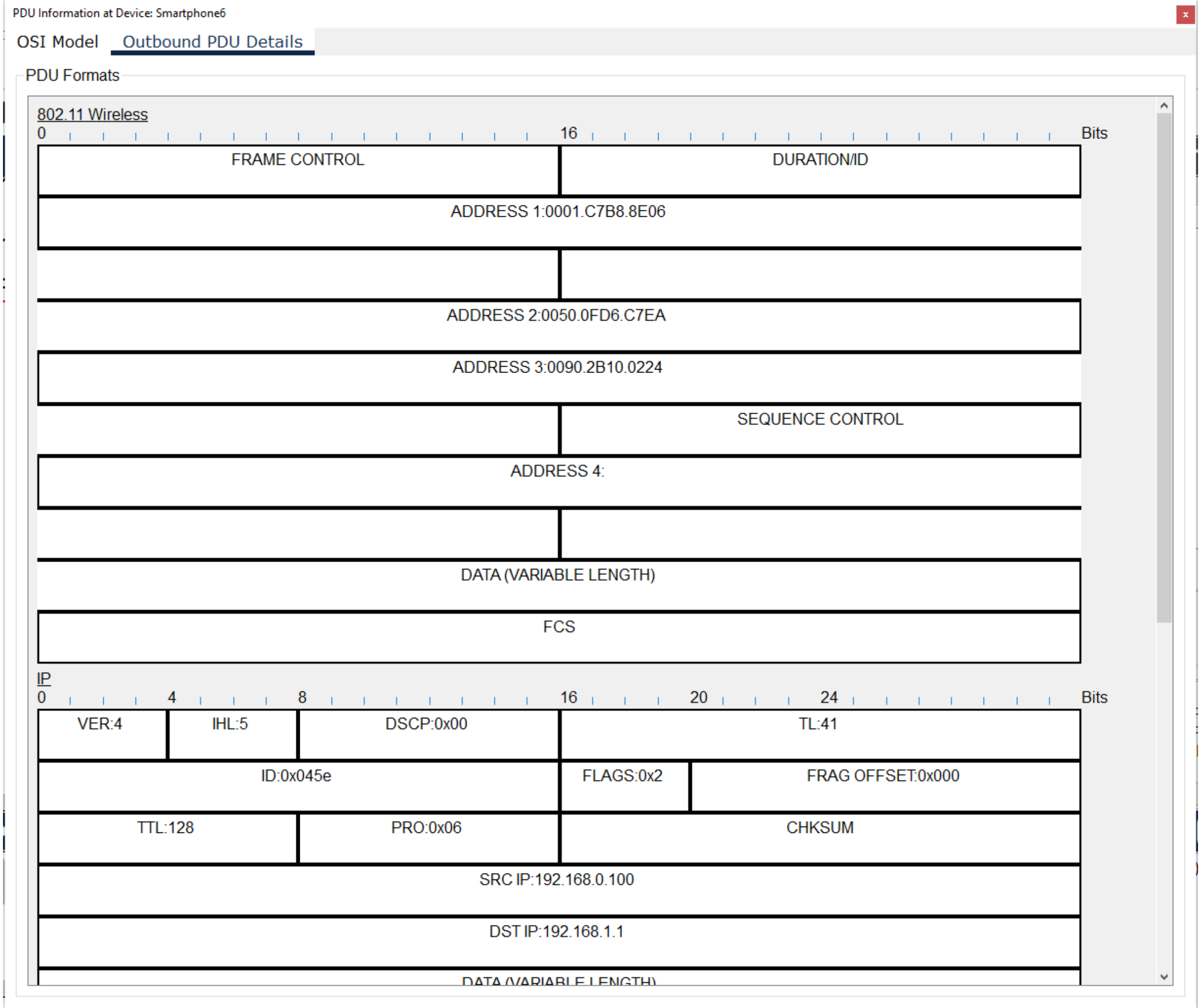


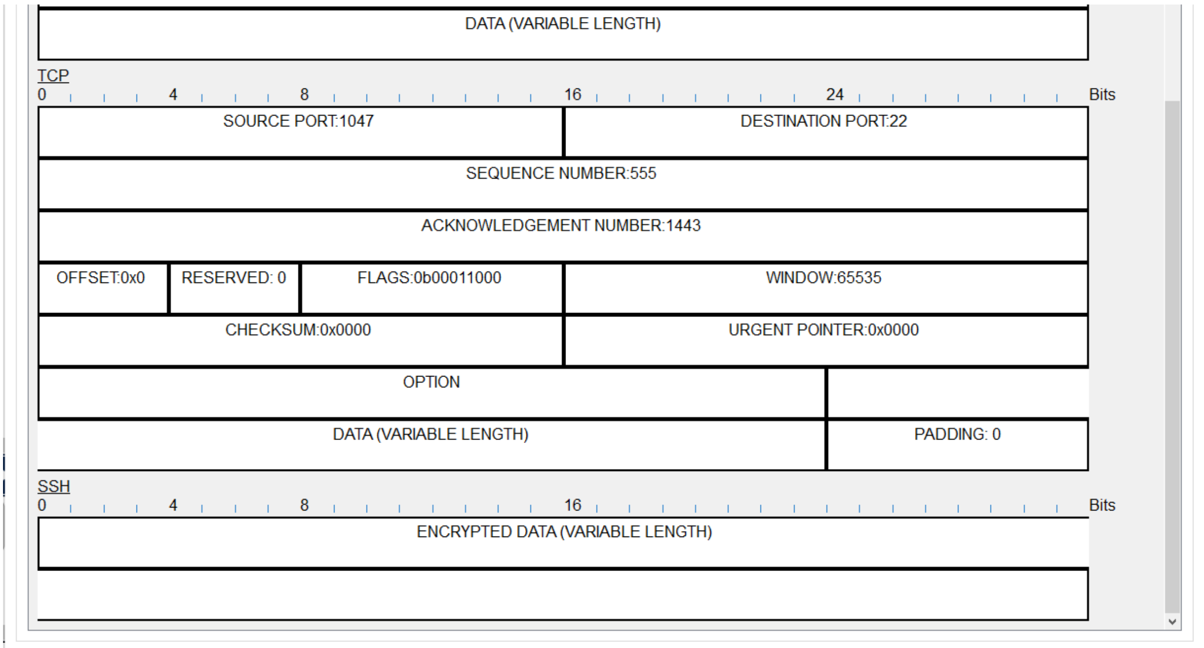

Server router
Physical
Config
CLI
Attributes
IOS Command Line Interface
router1(config)#line vty 0 15
router1(config-line)#
router1(config-line)#transport input ssh
router1(config-line)#
router1(config-line)#
router1(config-line)#login local
router1(config-line)#
router1(config-line)#
router1(config-line)#ip ssh ver 2
router1(config)#
router1(config)#
router1(config)#username alper privilege 15 password cisco
router1(config)#
router1(config)#
router1(config)#do wr
Building configuration...
[OK]
router1(config)#
%LINK-3-UPDOWN: Interface Serial3/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to down
%LINK-5-CHANGED: Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0,
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



According to the OSI reference model, the layer information is as follows.




PDU Information at Device: Smartphone6
OSI Model
Outbound PDU Details
PDU Formats
802.11 Wireless
0
16
Bits
FRAME CONTROL
DURATION/ID
ADDRESS 1:0001.C7B8.8E06
ADDRESS 2:0050.0FD6.C7EA
ADDRESS 3:0090.2B10.0224
SEQUENCE CONTROL
ADDRESS 4:
DATA (VARIABLE LENGTH)
FCS
IP
0
4
8
16
20
24
Bits
VER:4
IHL:5
DSCP:0x00
TL:41
ID:0x045e
FLAGS:0x2
FRAG OFFSET:0x000
TTL:128
PRO:0x06
CHKSUM
SRC IP:192.168.0.100
DST IP:192.168.1.1


DATA (VARIABLE LENGTH)
TCP
0
4
8
16
24
Bits
SOURCE PORT:1047
DESTINATION PORT:22
SEQUENCE NUMBER:555
ACKNOWLEDGEMENT NUMBER:1443
OFFSET:0x0
RESERVED: 0
FLAGS:0b00011000
WINDOW:65535
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0
SSH
0
4
8
16
Bits
ENCRYPTED DATA (VARIABLE LENGTH)

In this scenario, transactions go through the ssh layer.

SSH: The Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. This document describes the SSH transport layer protocol, which typically runs on top of TCP/IP. The protocol can be used as a basis for a number of secure network services.[18]

is.	Time(sec)	Last Device	At Device	Type
	0.000	--	Smartphone6	SSH
	0.001	Smartphone6	2.3 Wifi:2.3 Wifi	SSH
	0.002	2.3 Wifi:2.3 Wifi	2.3 Switch	SSH
	0.003	2.3 Switch	Router Branch 2	SSH
	0.004	Router Branch 2	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	SSH
	0.004	--	Server router	ICMP
	0.005	--	2.3 Wifi:2.3 Wifi	SSH
	0.005	Server router	Router Branch 2	SSH
	0.005	Server router	serverSwitch	ICMP

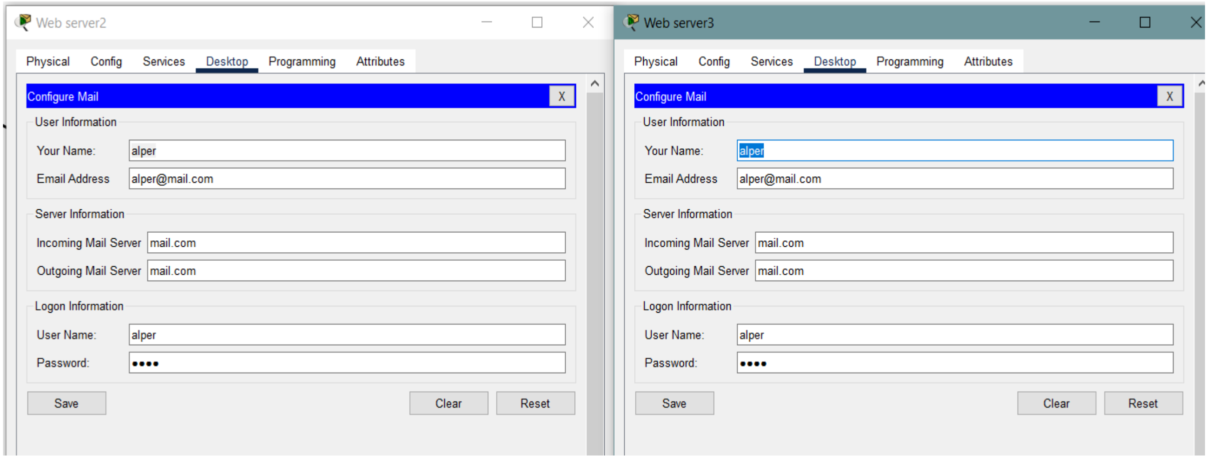
s.	Time(sec)	Last Device	At Device	Type
	0.005	Server router	serverSwitch	ICMP
	0.005	--	Server router	SSH
	0.006	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.006	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.006	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.006	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.006	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.006	Server router	Router Branch 2	SSH
	0.006	Router Branch 2	2.3 Switch	SSH
	0.006	serverSwitch	Web server1	ICMP
	0.006	--	Server router	SSH
	0.007	Server router	Router Branch 2	SSH
	0.007	Router Branch 2	2.3 Switch	SSH
	0.007	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.007	Web server1	serverSwitch	ICMP
	0.007	--	Server router	SSH
	0.008	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.008	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.008	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.008	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.008	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.008	Server router	Router Branch 2	SSH
	0.008	Router Branch 2	2.3 Switch	SSH
	0.008	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.008	serverSwitch	Server router	ICMP
	0.008	--	Server router	SSH
	0.009	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.009	2.3 Wifi:2.3 Wifi	Smartphone11	SSH

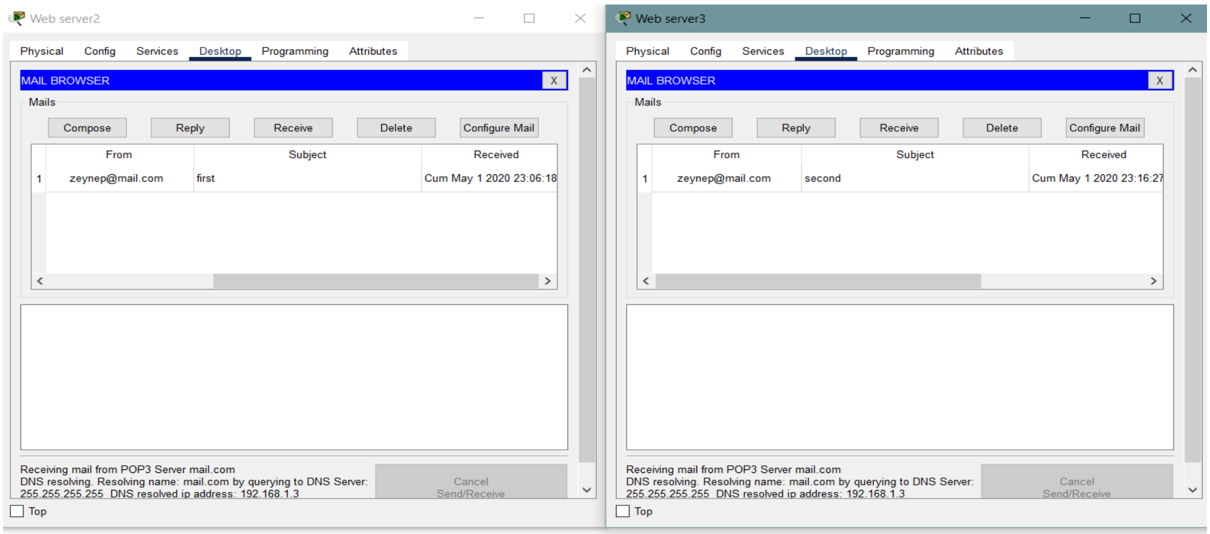
is.	Time(sec)	Last Device	At Device	Type
	0.009	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.009	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.009	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.009	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.009	Server router	Router Branch 2	SSH
	0.009	Router Branch 2	2.3 Switch	SSH
	0.009	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.009	--	Server router	SSH
	0.010	--	Server router	SSH
	0.010	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.010	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.010	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.010	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.010	--	Server router	SSH
	0.010	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.010	Server router	Router Branch 2	SSH
	0.010	Router Branch 2	2.3 Switch	SSH
	0.010	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.010	--	Smartphone6	TCP
	0.011	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.011	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.011	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.011	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.011	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.011	Server router	Router Branch 2	SSH
	0.011	Router Branch 2	2.3 Switch	SSH
	0.011	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.011	--	Server router	SSH

s.	Time(sec)	Last Device	At Device	Type
	0.012	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.012	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.012	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.012	Server router	Router Branch 2	SSH
	0.012	Router Branch 2	2.3 Switch	SSH
	0.012	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.012	--	Server router	SSH
	0.013	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.013	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.013	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.013	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.013	--	Server router	SSH
	0.013	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.013	Server router	Router Branch 2	SSH
	0.013	Router Branch 2	2.3 Switch	SSH
	0.013	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.013	--	Smartphone6	TCP
	0.014	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.014	2.3 Wifi:2.3 Wifi	Smartphone11	SSH
	0.014	2.3 Wifi:2.3 Wifi	Smartphone10	SSH
	0.014	2.3 Wifi:2.3 Wifi	Smartphone6	SSH
	0.014	2.3 Wifi:2.3 Wifi	Smartphone8	SSH
	0.014	Server router	Router Branch 2	SSH
	0.014	Router Branch 2	2.3 Switch	SSH
	0.014	2.3 Switch	2.3 Wifi:2.3 Wifi	SSH
	0.014	--	Server router	SSH
	0.015	2.3 Wifi:2.3 Wifi	Smartphone7	SSH
	0.015	2.3 Wifi:2.3 Wifi	Smartphone11	SSH

Scenario 8: It is desired to send mail from one server to two servers with the same email information.

Web server1 and Web server2 have the same mail features. If mail is sent from another server, the servers are queued and the next mail goes to the next server. The priority server is the one with the smaller IP address.

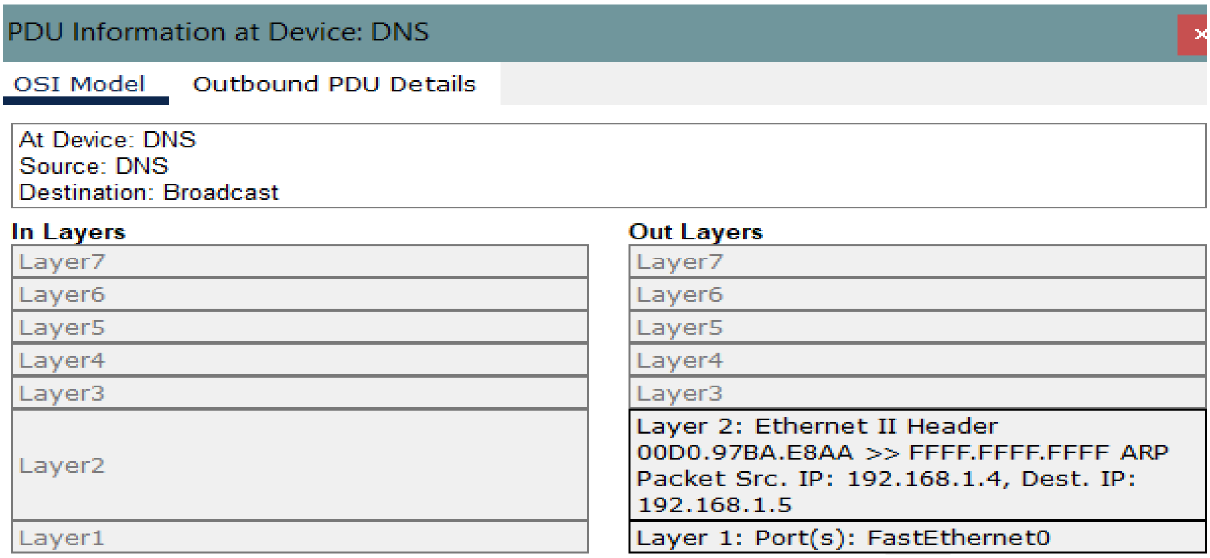




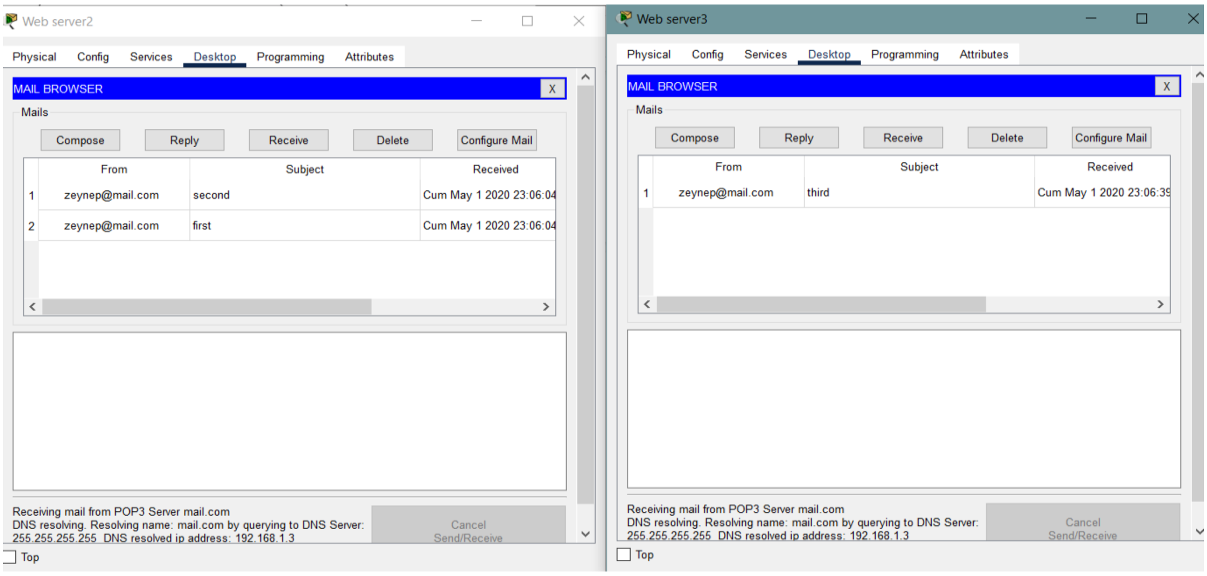
nt List

Time(sec)	Last Device	At Device	Type
0.000	--	Web server1	DNS
0.001	Web server1	serverSwitch	DNS
0.002	serverSwitch	Server router	DNS
0.002	serverSwitch	FTP2	DNS
0.002	serverSwitch	DNS	DNS
0.002	serverSwitch	DHCP	DNS
0.002	serverSwitch	Mail server	DNS
0.002	serverSwitch	FTP1	DNS
0.002	serverSwitch	Web server2	DNS
0.002	serverSwitch	admin	DNS
0.002	serverSwitch	Web server3	DNS
0.002	--	DNS	ARP
0.003	DNS	serverSwitch	ARP
0.004	serverSwitch	Server router	ARP
0.004	serverSwitch	FTP2	ARP
0.004	serverSwitch	DHCP	ARP
0.004	serverSwitch	Web server1	ARP
0.004	serverSwitch	Mail server	ARP
0.004	serverSwitch	FTP1	ARP
0.004	serverSwitch	Web server2	ARP
0.004	serverSwitch	admin	ARP
0.004	serverSwitch	Web server3	ARP
0.005	Web server1	serverSwitch	ARP
0.006	serverSwitch	DNS	ARP
0.006	--	DNS	DNS
0.007	DNS	serverSwitch	DNS
0.008	serverSwitch	Web server1	DNS
0.008	--	Web server1	TCP
0.008	--	Web server1	ARP
0.009	Web server1	serverSwitch	ARP
0.010	serverSwitch	Server router	ARP
0.010	serverSwitch	FTP2	ARP
0.010	serverSwitch	DNS	ARP
0.010	serverSwitch	DHCP	ARP
0.010	serverSwitch	Mail server	ARP
0.010	serverSwitch	FTP1	ARP
0.010	serverSwitch	Web server2	ARP
0.010	serverSwitch	admin	ARP
0.010	serverSwitch	Web server3	ARP
0.011	Mail server	serverSwitch	ARP
0.012	serverSwitch	Web server1	ARP
0.012	--	Web server1	TCP
0.013	Web server1	serverSwitch	TCP
0.014	serverSwitch	Mail server	TCP
0.015	Mail server	serverSwitch	TCP
0.016	serverSwitch	Web server1	TCP
0.016	--	Web server1	SMTP
0.017	Web server1	serverSwitch	TCP
0.017	--	Web server1	SMTP
0.018	Web server1	serverSwitch	SMTP
0.018	serverSwitch	Mail server	TCP
0.019	serverSwitch	Mail server	SMTP
0.020	Mail server	serverSwitch	SMTP
0.021	serverSwitch	Web server1	SMTP
0.021	--	Web server1	TCP
0.021	--	Web server1	DNS
0.022	Web server1	serverSwitch	TCP
0.022	--	Web server1	DNS
0.023	Web server1	serverSwitch	DNS
0.023	serverSwitch	Mail server	TCP
0.024	serverSwitch	Server router	DNS
0.024	serverSwitch	FTP2	DNS
0.024	serverSwitch	DNS	DNS
0.024	serverSwitch	DHCP	DNS
0.024	serverSwitch	Mail server	DNS
0.024	serverSwitch	FTP1	DNS
0.024	serverSwitch	Web server2	DNS
0.024	serverSwitch	admin	DNS
0.024	serverSwitch	Web server3	DNS
0.024	Mail server	serverSwitch	TCP
0.025	DNS	serverSwitch	DNS
0.025	serverSwitch	Web server1	TCP
0.026	serverSwitch	Web server1	DNS
0.026	Web server1	serverSwitch	TCP
0.026	--	Web server1	TCP
0.027	Web server1	serverSwitch	TCP
0.027	serverSwitch	Mail server	TCP
0.028	serverSwitch	Mail server	TCP
0.029	Mail server	serverSwitch	TCP
0.030	serverSwitch	Web server1	TCP
0.030	--	Web server1	SMTP
0.031	Web server1	serverSwitch	TCP
0.031	--	Web server1	SMTP
0.032	Web server1	serverSwitch	SMTP
0.032	serverSwitch	Mail server	TCP
0.033	serverSwitch	Mail server	SMTP
0.034	Mail server	serverSwitch	SMTP
0.035	serverSwitch	Web server1	SMTP
0.035	--	Web server1	TCP
0.035	--	Web server2	DNS

Unlike other mail operations, Address Resolution Protocol is also applied during this process. The layers during this protocol are as follows.



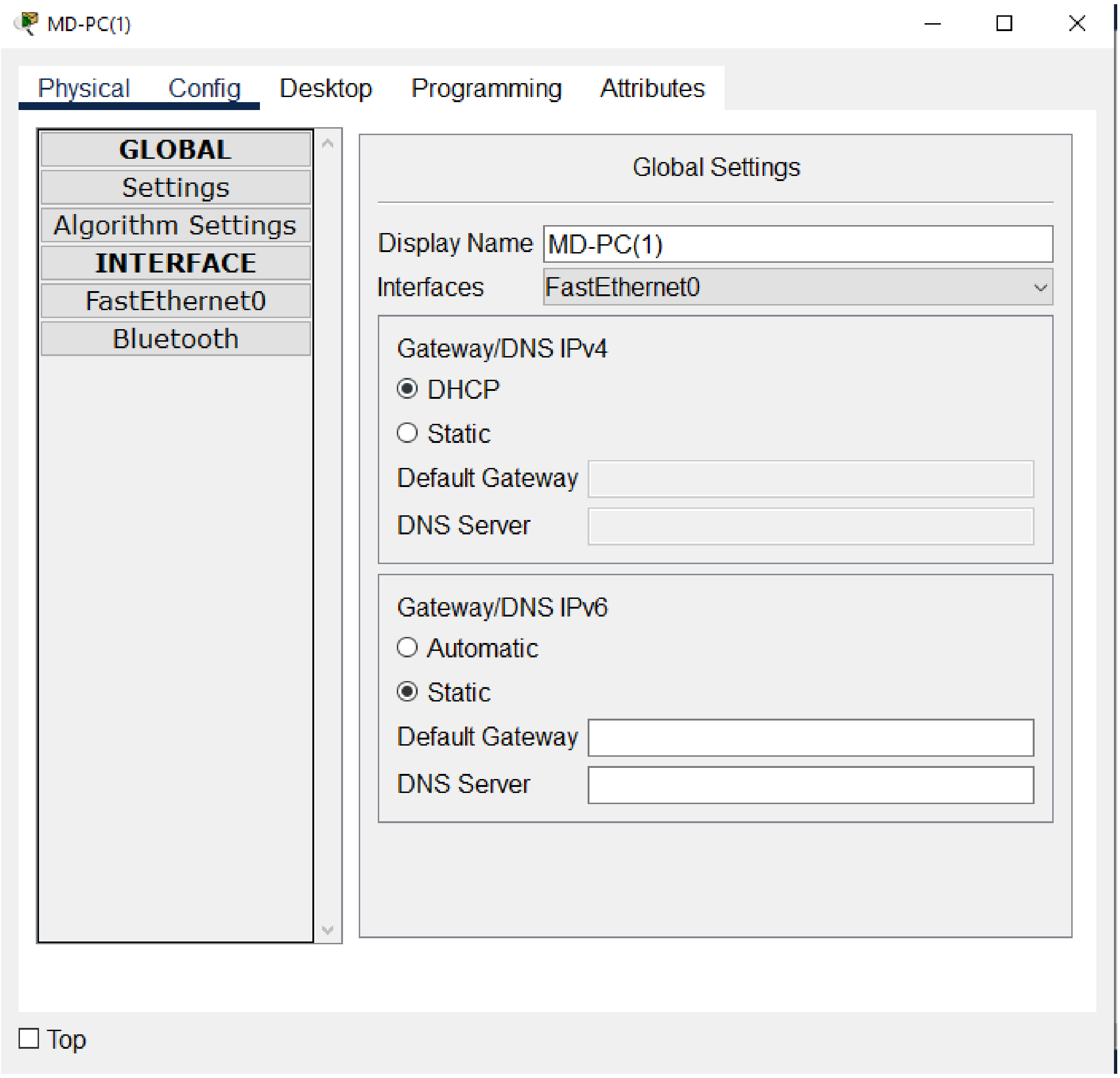
In this scenario, processes work differently during Simulation and in Real Time. While transactions cannot be queued during simulation, transactions can be queued during Real Time. Simulation screenshots are as follows.



The first two mails were sent during Simulation. That's why the first two mails went to Web server2. After the simulation was closed, the third email was sent. The third mail went to the Web server3 because the mail was queued during Real Time.

Scenario 9: A user in the second facility of second branch wants to assign IP address automatically through DHCP server. MD-PC(1) is this user's computer.Events that occur while assigning the IP address automatically are shown below.

The configuration of the MD-PC(1) computer before automatic ip assignment is as shown below.



ent List

s.	Time(sec)	Last Device	At Device	Type
	0.001	--	MD-PC(1)	DHCP
	0.002	MD-PC(1)	2.2 Switch:2.2 Swi...	DHCP
	0.002	2.2 Switch:2.2 Switch	Router Branch 2	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(9)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(8)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(10)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(7)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(6)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(5)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(4)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(3)	DHCP
	0.002	2.2 Switch:2.2 Switch	MD-PC(2)	DHCP
	0.002	2.2 Switch:2.2 Switch	2.2 Wifi	DHCP
	0.003	2.2 Switch:2.2 Switch	Router Branch 2	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(9)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(8)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(10)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(7)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(6)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(5)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(4)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(3)	DHCP
	0.003	2.2 Switch:2.2 Switch	MD-PC(2)	DHCP
	0.003	2.2 Switch:2.2 Switch	2.2 Wifi	DHCP
	0.003	Router Branch 2	Server router	DHCP
	0.004	Router Branch 2	Server router	DHCP
	0.004	Server router	serverSwitch	DHCP
	0.005	Server router	serverSwitch	DHCP
	0.005	serverSwitch	DHCP	DHCP

s.	Time(sec)	Last Device	At Device	Type
	0.006	serverSwitch	DHCP	DHCP
	0.006	--	DHCP	ICMP
	0.007	DHCP	serverSwitch	ICMP
	0.008	serverSwitch	Server router	ICMP
	0.028	--	Router Branch 2	IPSec
	0.029	Router Branch 2	2.1 Switch	IPSec
	0.029	--	Router Branch 2	IPSec
	0.030	Router Branch 2	2.2 Switch:2.2 Swi...	IPSec
	0.030	--	Router Branch 2	IPSec
	0.031	Router Branch 2	2.3 Switch	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(1)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(9)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(8)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(10)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(7)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(6)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(5)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(4)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(3)	IPSec
	0.031	2.2 Switch:2.2 Switch	MD-PC(2)	IPSec
	0.031	2.2 Switch:2.2 Switch	2.2 Wifi	IPSec
	0.031	--	Router Branch 2	IPSec
	0.032	Router Branch 2	2.1 Switch	IPSec
	0.032	MD-PC(8)	2.2 Switch:2.2 Swi...	IPSec
	0.032	2.1 Switch	Router Branch 2	IPSec
	0.032	--	Router Branch 2	IPSec
	0.033	--	Server router	ICMP
	0.033	Router Branch 2	2.2 Switch:2.2 Swi...	IPSec
	0.033	--	Router Branch 2	IPSec

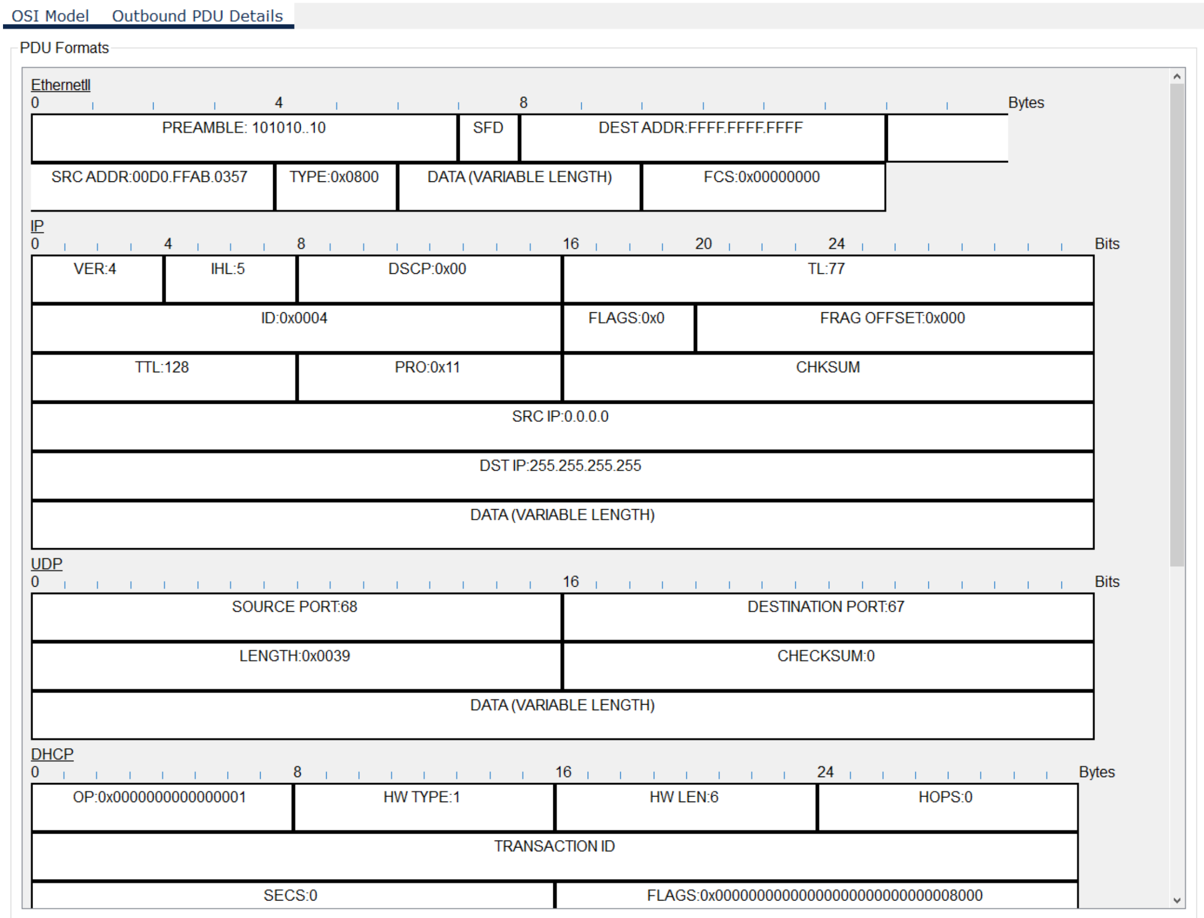
According to the OSI reference model, the layer information is as follows.

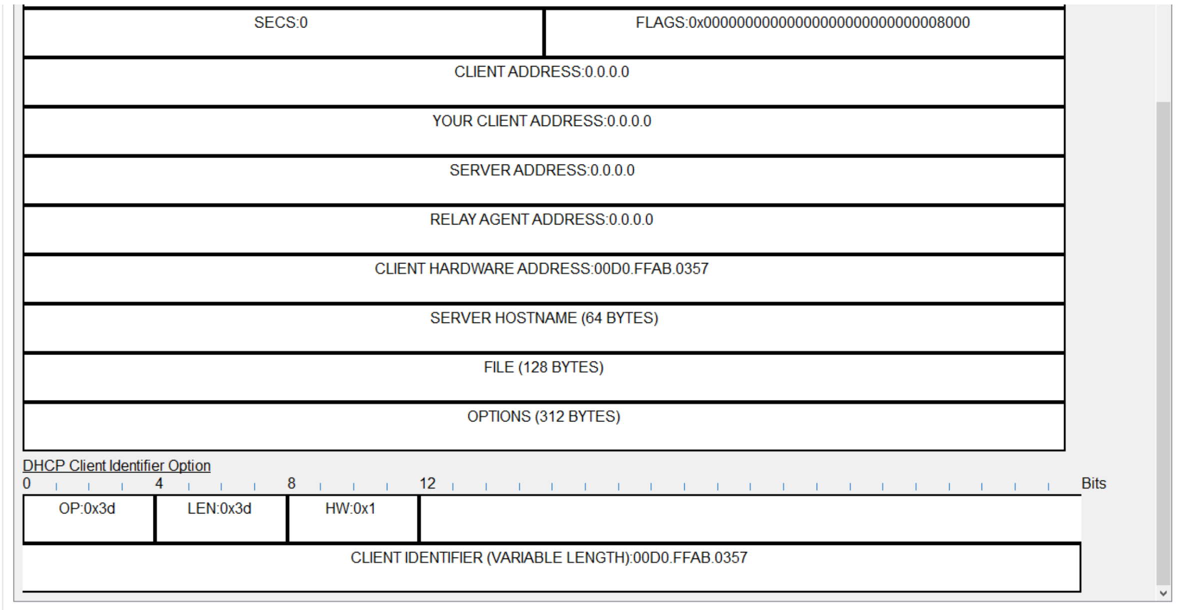
OSI Model   Outbound PDU Details

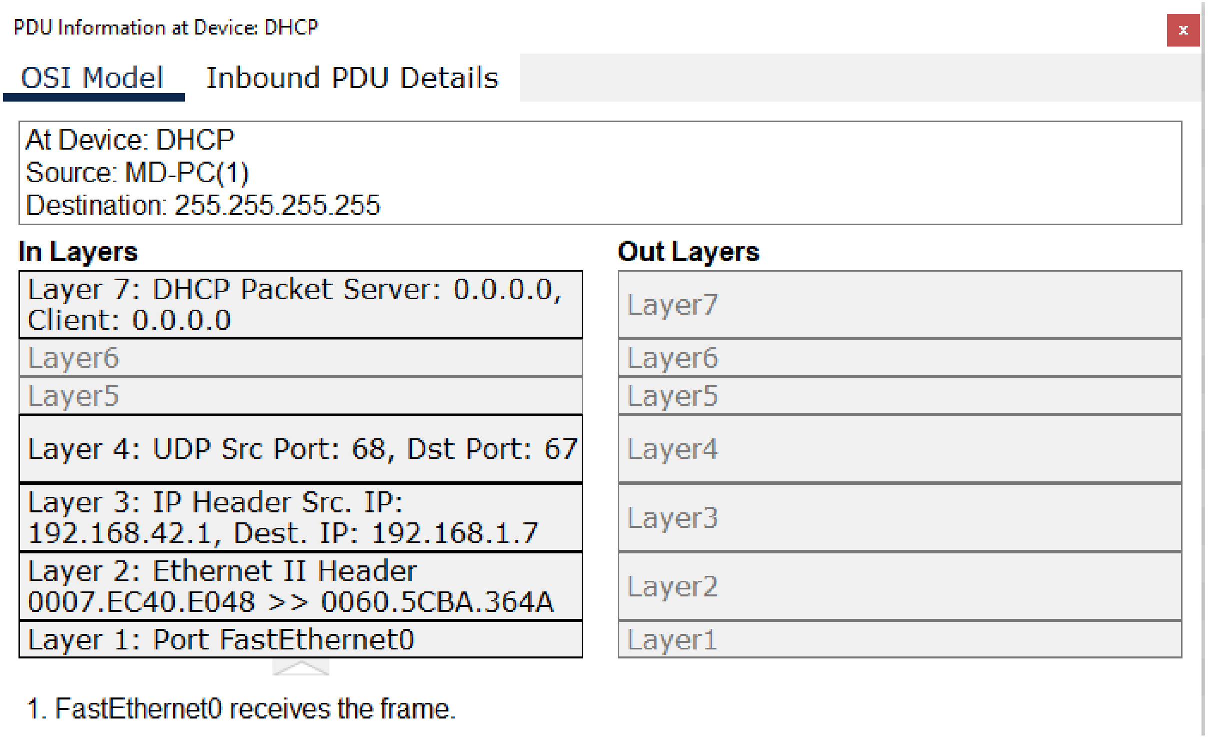
At Device: MD-PC(2)
Source: MD-PC(2)
Destination: 255.255.255.255

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 00D0.FFAB.0357 >> FFFF.FFFF.FFFF
Layer1	Layer 1: Port(s):

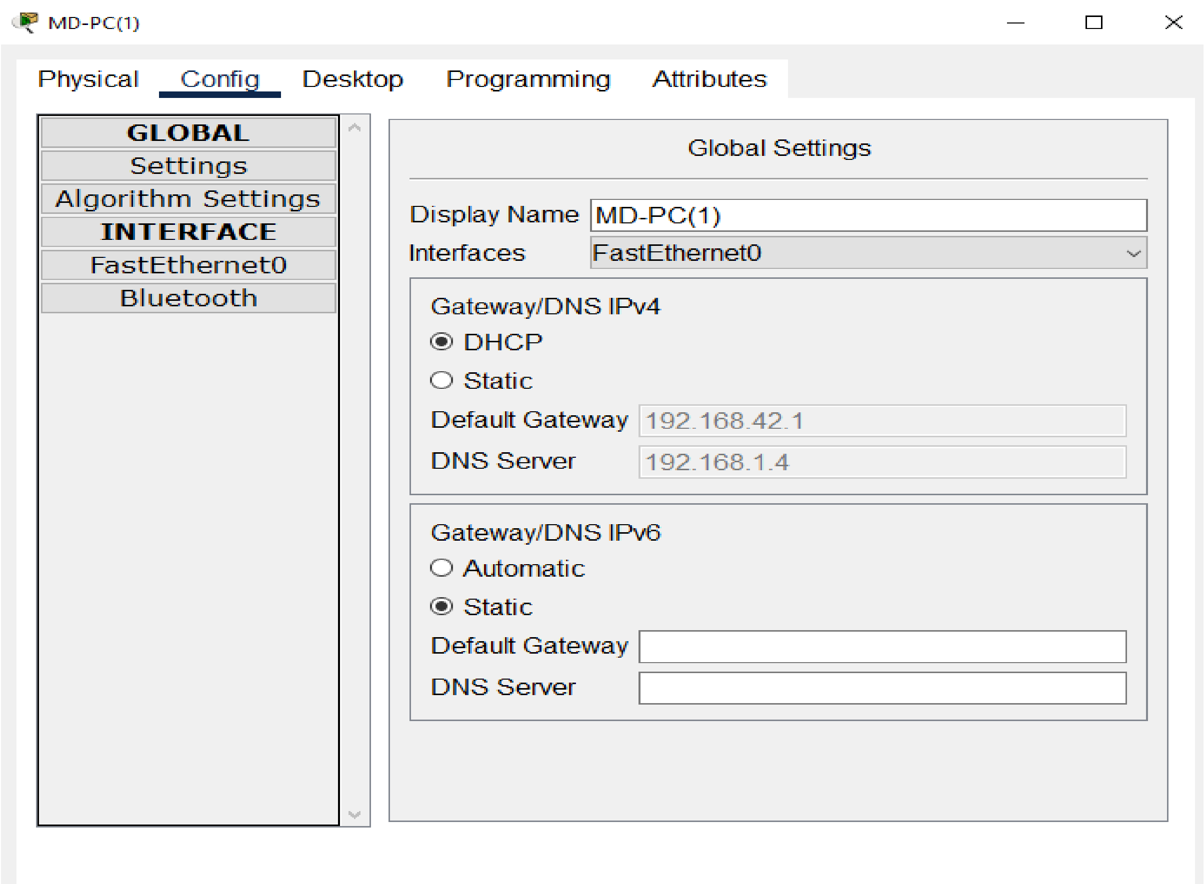
1. The DHCP client constructs a Discover packet and sends it out.


OSI Model
Outbound PDU Details
PDU Formats
EthernetII
0 4 8 Bytes
PREAMBLE: 101010..10
SFD
DEST ADDR:FFFF.FFFF.FFFF
SRC ADDR:00D0.FFAB.0357
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
0 4 8 16 20 24 Bits
VER:4
IHL:5
DSCP:0x00
TL:77
ID:0x0004
FLAGS:0x0
FRAG OFFSET:0x000
TTL:128
PRO:0x11
CHKSUM
SRC IP:0.0.0.0
DST IP:255.255.255.255
DATA (VARIABLE LENGTH)
UDP
0 16 Bits
SOURCE PORT:68
DESTINATION PORT:67
LENGTH:0x0039
CHECKSUM:0
DATA (VARIABLE LENGTH)
DHCP
0 8 16 24 Bytes
OP:0x0000000000000001
HW TYPE:1
HW LEN:6
HOPS:0
TRANSACTION ID
SECS:0
FLAGS:0x0000000000000000000000000000008000


SECS:0
FLAGS:0x0000000000000000000000000000008000
CLIENT ADDRESS:0.0.0.0
YOUR CLIENT ADDRESS:0.0.0.0
SERVER ADDRESS:0.0.0.0
RELAY AGENT ADDRESS:0.0.0.0
CLIENT HARDWARE ADDRESS:00D0.FFAB.0357
SERVER HOSTNAME (64 BYTES)
FILE (128 BYTES)
OPTIONS (312 BYTES)
DHCP Client Identifier Option
0 4 8 12 Bits
OP:0x3d
LEN:0x3d
HW:0x1
CLIENT IDENTIFIER (VARIABLE LENGTH):00D0.FFAB.0357

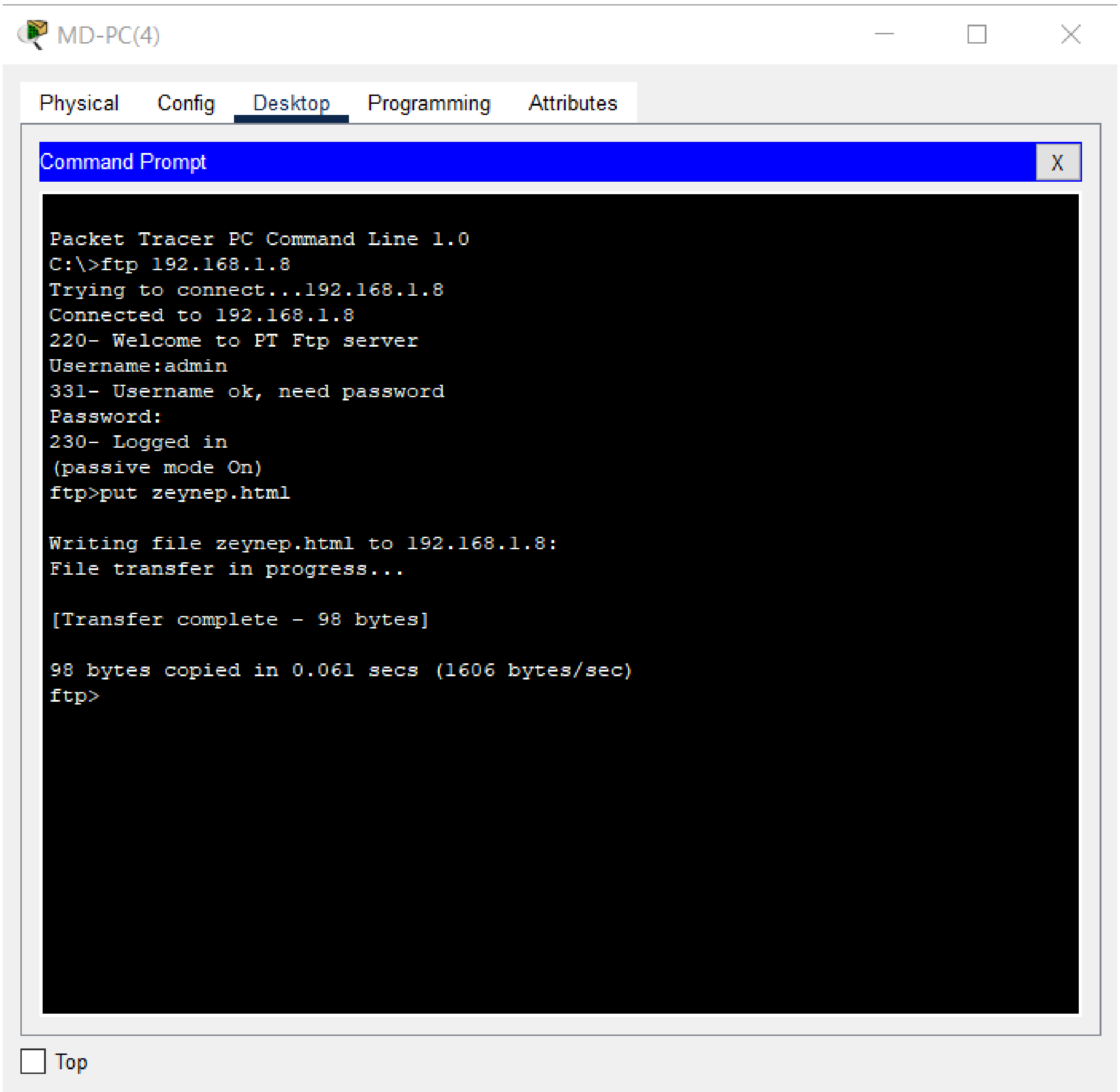


The configuration of the MD-PC(1) computer after automatic ip assignment is as shown below.

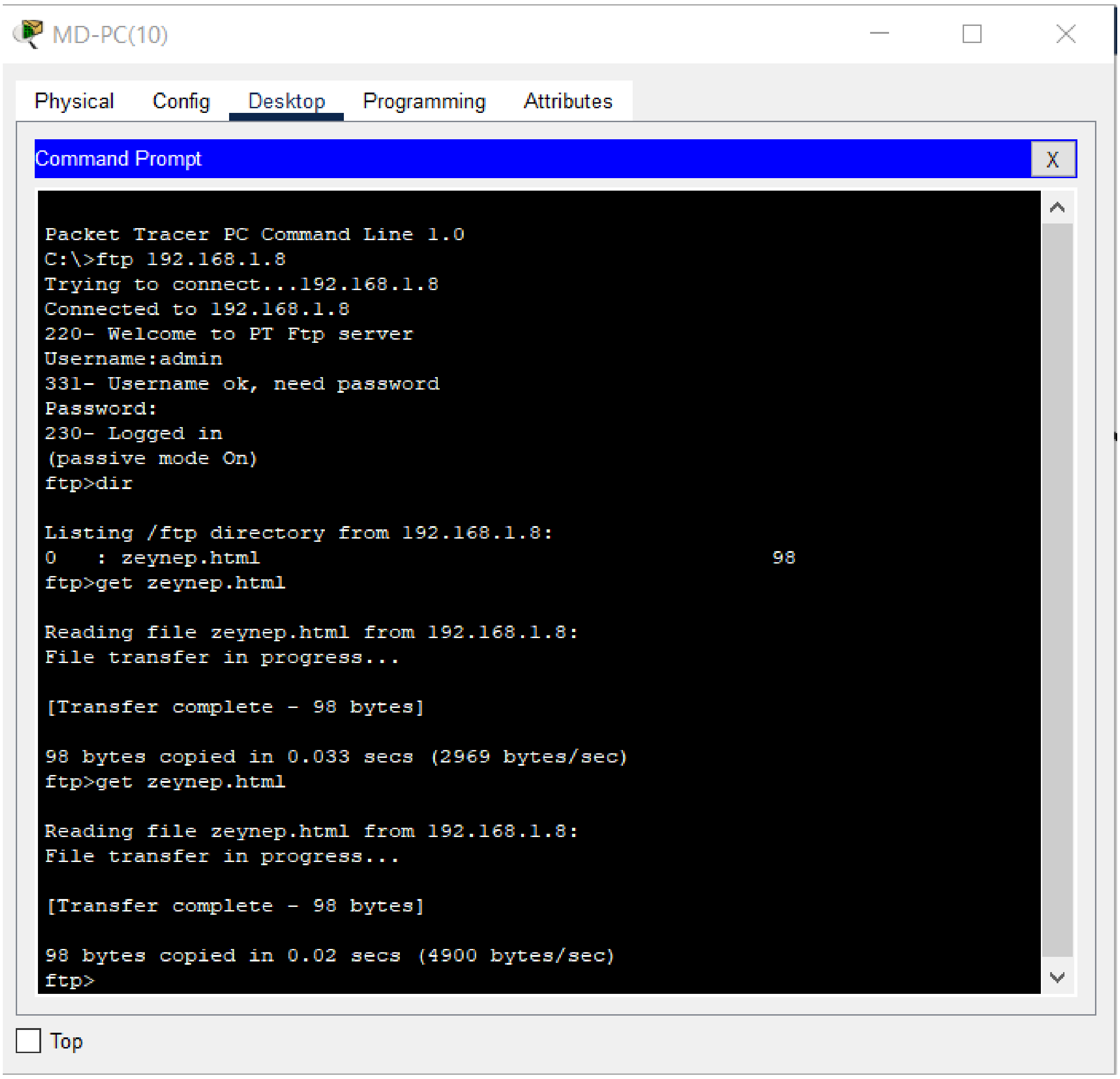


Scenario 10: A computer engineer from the second facility of the second branch developed a web application and wants to get code files from the FTP server in the third facility of the first branch.

In this scenario, we first connect to FTP2 server with the computer named MD-PC(4) and send the zeynep.html file that we created earlier on this computer to this server.



Then, as seen below, computers named MD-PC(10) connect to FTP2 server with "ftp -ip address" command. After this process, we download the zeynep.html file from the FTP2 server with the "get -ip address" command.



In this scenario, as seen below, the "MD-PC(10)" computer downloads the zeynep.html file located on the FTP2 server. The devices working in the download process are shown in the simulation panel, respectively.

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.002	2.2 Switch	Router Br...	FTP
	0.003	Router Bran...	Server router	FTP
	0.004	Server router	serverSwitch	FTP
	0.007	serverSwitch	Server router	FTP
	0.008	Server router	Router Br...	FTP
	0.009	Router Bran...	2.2 Switch	FTP
	0.012	2.2 Switch	Router Br...	FTP
	0.013	Router Bran...	Server router	FTP
	0.014	Server router	serverSwitch	FTP
	0.017	serverSwitch	Server router	FTP
	0.018	Server router	Router Br...	FTP
	0.019	Router Bran...	2.2 Switch	FTP
	0.022	2.2 Switch	Router Br...	FTP
	0.023	Router Bran...	Server router	FTP
	0.024	Server router	serverSwitch	FTP
	0.027	serverSwitch	Server router	FTP
	0.028	Server router	Router Br...	FTP
	0.029	Router Bran...	2.2 Switch	FTP
	0.032	2.2 Switch	Router Br...	TCP
	0.033	Router Bran...	Server router	TCP
	0.034	Server router	serverSwitch	TCP
	0.037	serverSwitch	Server router	TCP
	0.038	Server router	Router Br...	TCP
	0.039	Router Bran...	2.2 Switch	TCP
	0.042	2.2 Switch	Router Br...	TCP

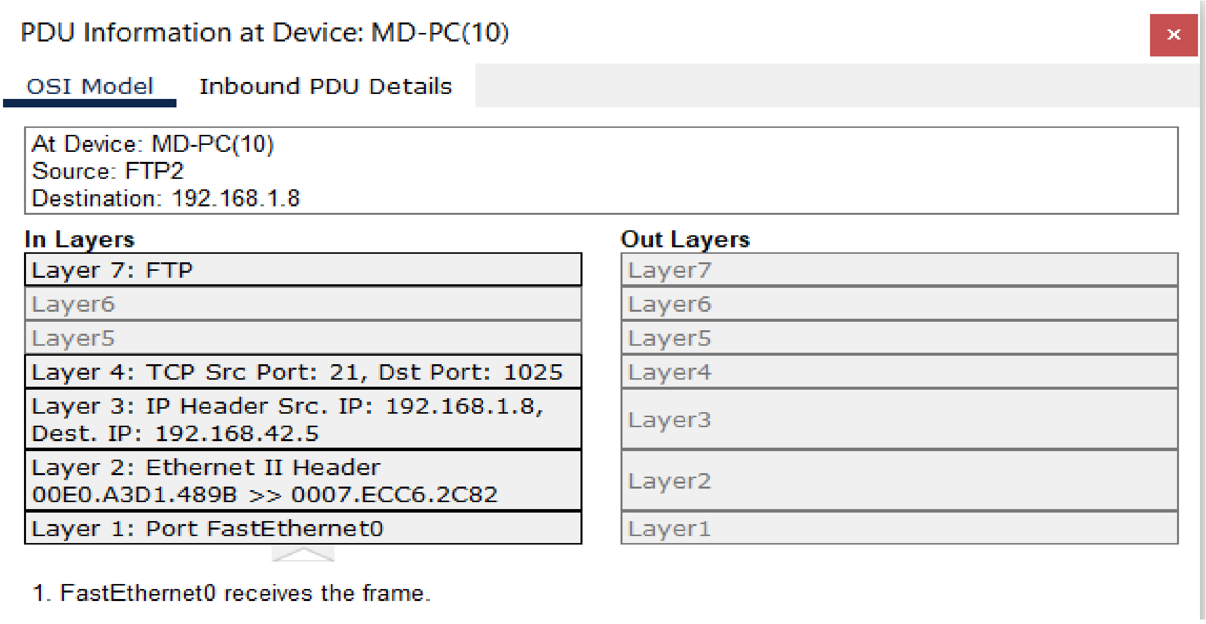
Reset Simulation ☑ Constant Delay

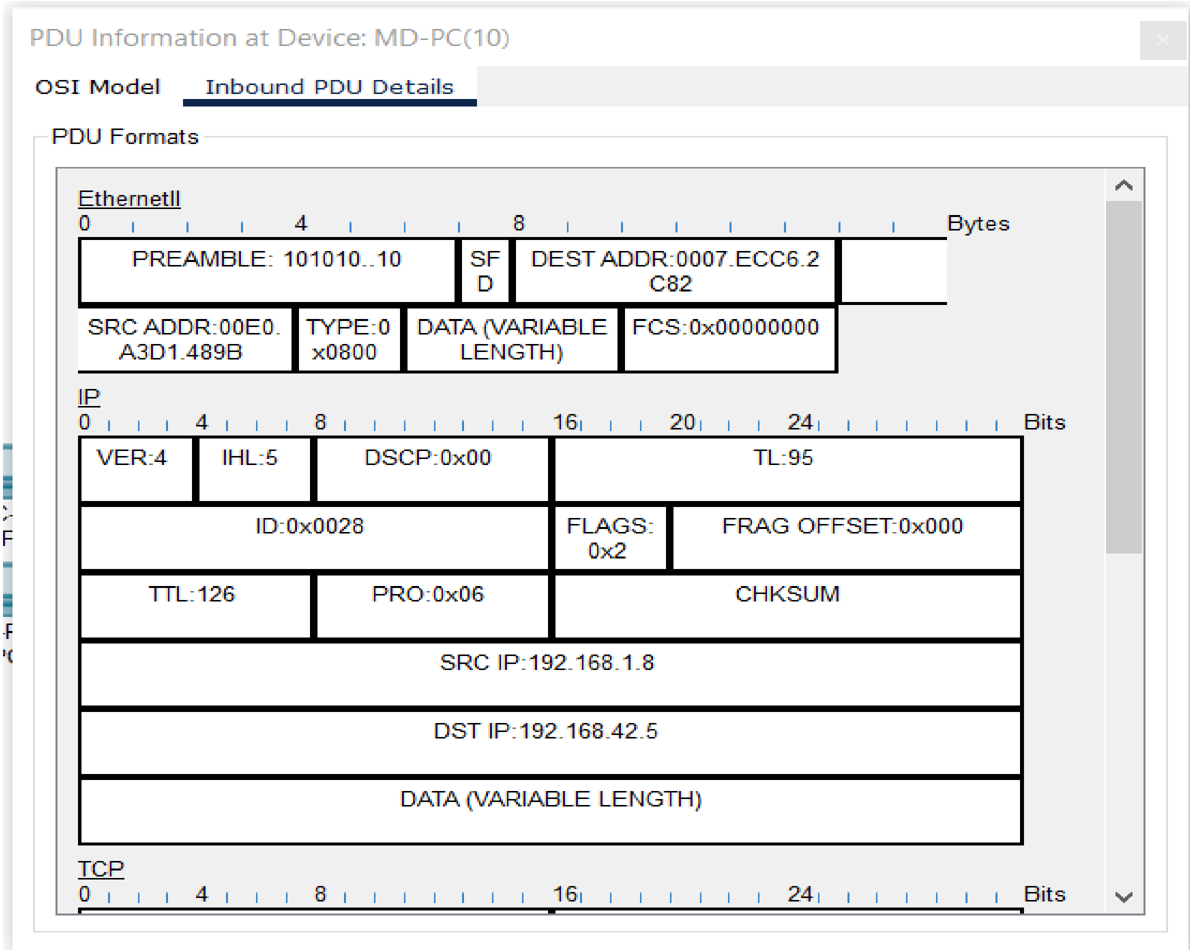
	0.042	2.2 Switch	Router Br...	TCP
	0.043	Router Bran...	Server router	TCP
	0.044	Server router	serverSwitch	TCP
	0.045	MD-PC(10)	2.2 Switch	TCP
	0.046	2.2 Switch	Router Br...	TCP
	0.046	FTP2	serverSwitch	FTP
	0.047	Router Bran...	Server router	TCP
	0.047	serverSwitch	Server router	FTP
	0.048	Server router	serverSwitch	TCP
	0.048	Server router	Router Br...	FTP
	0.049	Router Bran...	2.2 Switch	FTP
	0.051	MD-PC(10)	2.2 Switch	TCP
	0.052	2.2 Switch	Router Br...	TCP
	0.053	Router Bran...	Server router	TCP
	0.054	Server router	serverSwitch	TCP

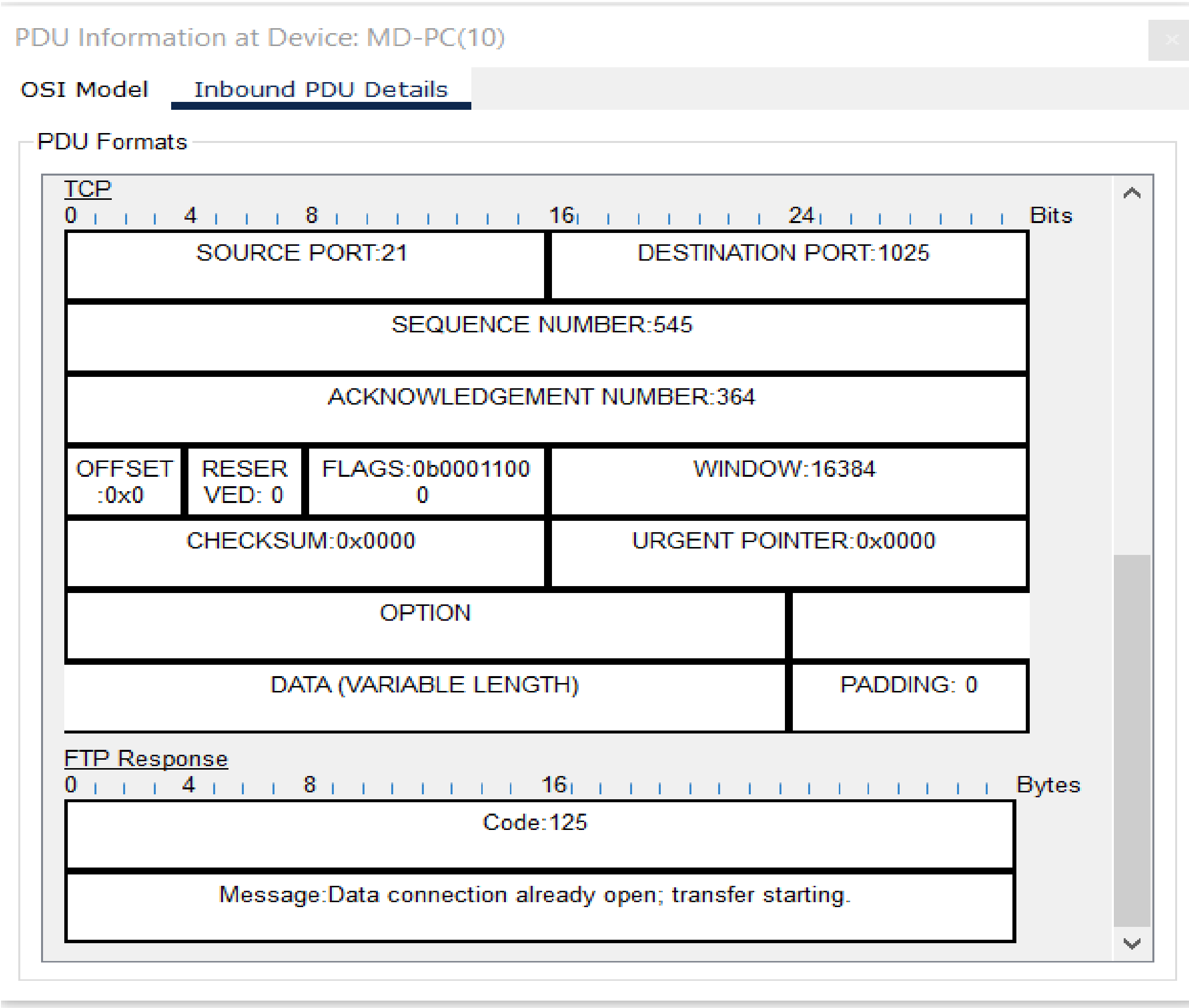
Reset Simulation ☑ Constant Delay

Play Controls

According to the OSI reference model, the layer information is as follows.



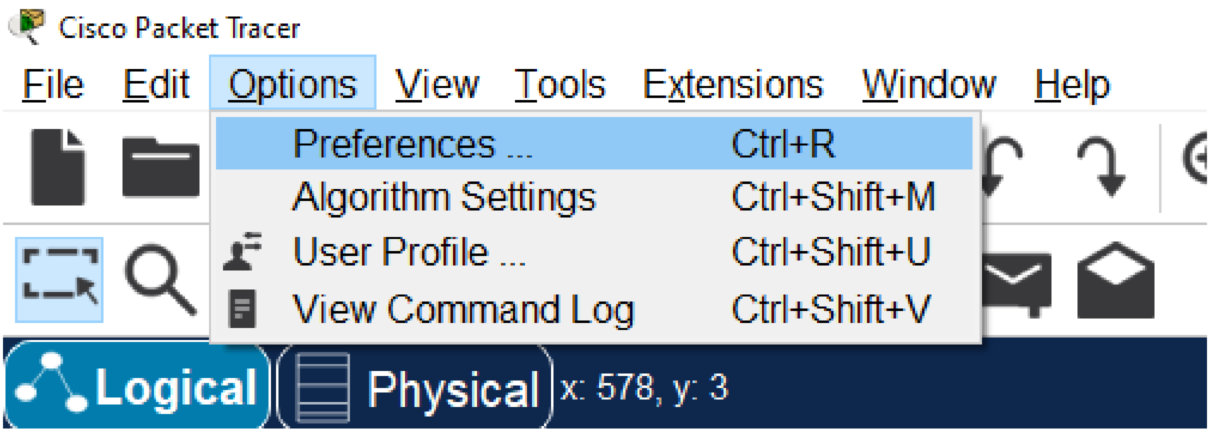


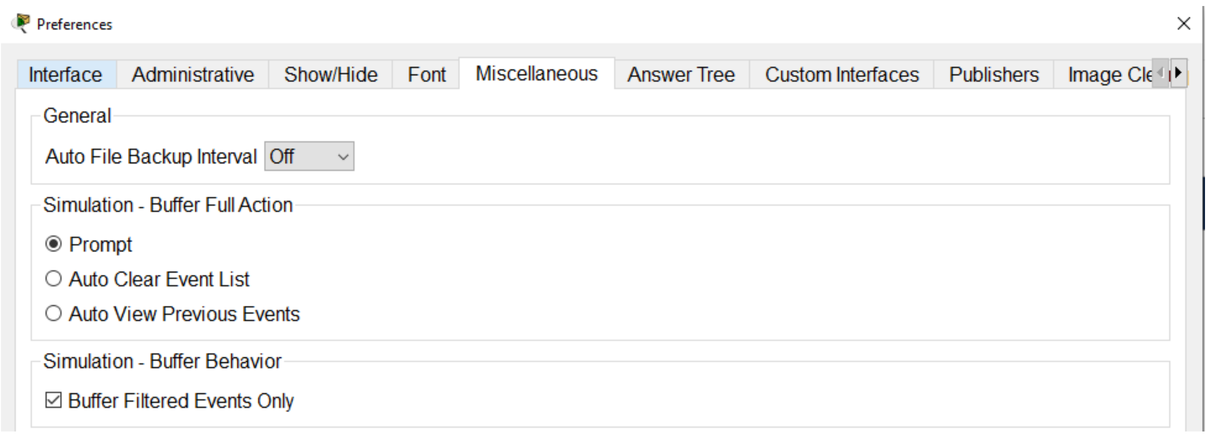

PDU Information at Device: MD-PC(10)
OSI Model
Inbound PDU Details
PDU Formats
TCP
0 4 8 16 24 Bits
SOURCE PORT:21
DESTINATION PORT:1025
SEQUENCE NUMBER:545
ACKNOWLEDGEMENT NUMBER:364
OFFSET :0x0
RESER VED: 0
FLAGS:0b0001100 0
WINDOW:16384
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0
FTP Response
0 4 8 16 Bytes
Code:125
Message:Data connection already open; transfer starting.

4. Encountered Issues

Stopped Cisco Tracer working in the simulation - BUFFER FULL:

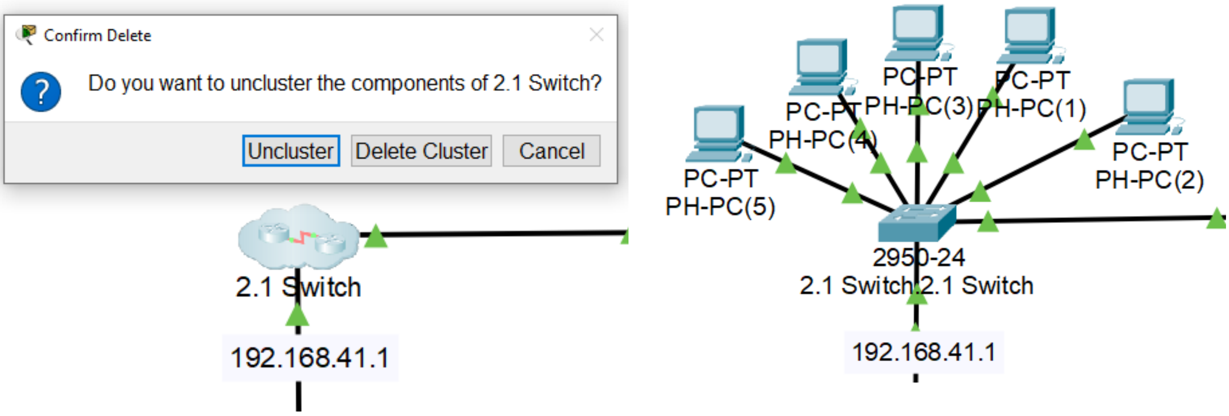
Cisco packet tracer is crashed when running some simulation cases. We have researched this situation on the internet and we have seen that it is also an issue for some people. For the solution, you should click options in the upper bar then click preferences. Then open the Miscellaneous tab and tick Buffer Filtered Events Only. It's solved.





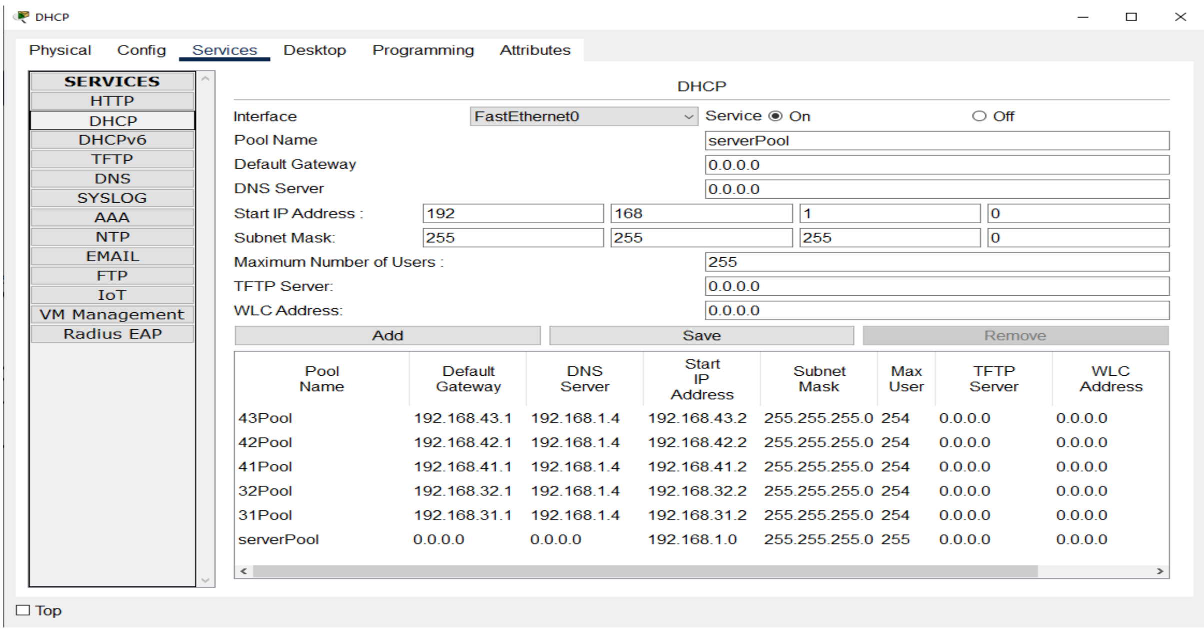
Not Listing Correct Layers in the Simulation Mode:

When we ran simulation scenarios, The output of layers was not correct. After a little research We realized that we must uncluster groups which are used in simulation scenarios. so that the layers for the simulation were done correctly. Devices had been clustered to have a non complex appearance.



Manually Ip Configuration to Automatic:

When we first started we were giving the IPs to each device manually. Although this is not a problem, it is a very time consuming process (A time problem). With a short research, we learned to automatically give the ip to devices by DHCP. Also, this was used in simulation scenarios we wrote ourselves. Server IPs is selected manually but most of devices in facilities are selected automatically and different IPs were given according to their facilitie



5. Conclusion

In this project, the project team used some network models, many network devices and cable type in the desired format according to the connection type. The network structure suitable for the hardware devices used by the users in the two branches and the topology of this network were determined and then successfully implemented. Configuration of hardware devices has been done successfully. As a result, the communication between the branches was carried out successfully with the determined network model by using the Packet Tracer simulation tool effectively.

6. References

[1] https://en.wikipedia.org/wiki/Node_(networking) (23.05.2021)

[2] https://techterms.com/definition/packet (23.05.2021)

[3] https://en.wikibooks.org/wiki/Communication_Networks/Channels (24.05.2021)

[4] https://www.interserver.net/tips/kb/common-network-protocols-ports/ (24.05.2021)

[5] https://www.comptia.org/content/guides/what-is-a-network-protocol (24.05.2021)

[6] https://en.wikipedia.org/wiki/Transmission_Control_Protocol (26.05.2021)

[7] https://www.cloudflare.com/learning/network-layer/internet-protocol/ (27.05.2021)

[8] https://en.wikipedia.org/wiki/Communications_system (27.05.2021)

[9] https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-architecture.html (29.05.2021)

[10] https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol (01.06.2021)

[11] https://en.wikipedia.org/wiki/Server_(computing) (01.06.2021)

[12] https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-how.html#~network-hubs (01.06.2021)

[13] https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html (02.06.2021)

[14] https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol (02.06.2021)

[15] https://ftp1.digi.com/support/cabling/dte_vs_dce.pdf (02.06.2021)

[16] https://www.hosting.com.tr/bilgi-bankasi/smtp-nedir/ (03.06.2021)