Analysis of a case of the application layer

Networks

1st Félix Rivero Graverán
Electronics engineering
University of los Andes
Bogota, Colombia
f.riverog@uniandes.edu.co

2nd Andres Mateo Chilito Avella
Electronics engineering
University of los Andes
Bogota, Colombia
a.chilitoa@uniandes.edu.co

***Abstract*—In this report we will analyze various protocols of the application layer while observing the packet traffic generated by various applications of this layer, such as FTP or SMTP, we will do so with the Cisco Packet Tracer tool. Using this tool we will develop various capabilities that will allow us to understand the configuration of various servers, as well as various types of communication. On the other hand, we will test and analyze the efficiency between terminal systems and packet switching devices. At the end of this practice we will be able to use all the above mentioned concepts correctly and thus apply them to our daily life, analyzing in a technical way the different situations that are presented to us, such as a web search, a video call, among others.**

***Index Terms*—DNS, HTTP, FTP, SMTP, POP, SNMP, IP, Packet Switch Devices**

I. Introduction

In this report we will go into the application layer, using the Cisco Packet Tracer tool which will allow us to become familiar with several key concepts for understanding the aforementioned layer. In the development of this laboratory we will also familiarize ourselves with the RFC documentation of each concept, this in order to have present and clear the key concepts. At the end we will reflect on the different results we obtained.

II. Theoretical framework

A. DNS:

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. [1]

The primary goal is a consistent name space which will be used for referring to resources. In order to avoid the problems caused by ad hoc encodings, names should not be required to contain network identifiers, addresses, routes, or similar information as part of the name.

The DNS has three major components:

• The DOMAIN NAME SPACE and RESOURCE RECORDS, which are specifications for a tree structured name space and data associated with the names. Conceptually, each node and leaf of the domain name space tree names a set of information, and query operations are attempts to extract specific types of information from a particular set. A query names the domain name of interest and describes the type of resource information that is desired. For example, the Internet uses some of its domain names to identify hosts; queries for address resources return Internet host addresses.

• NAME SERVERS are server programs which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree. Name servers know the parts of the domain tree for which they have complete information; a name server is said to be an AUTHORITY for these parts of the name space. Authoritative information is organized into units called ZONEs, and these zones can be automatically distributed to the name servers which provide redundant service for the data in a zone.

• RESOLVERS are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query directly or pursue the query using referrals to other name servers. A resolver will typically be a system routine that is directly accessible to user programs; hence no protocol is necessary between the resolver and the user program. [2]

B. HTTP:

The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load web pages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. [3]

Each Hypertext Transfer Protocol (HTTP) message is either a request or a response. A server listens on a connection for a request, parses each message received, interprets the message semantics in relation to the identified request target, and responds to that request with one or more response messages. A client constructs request messages to communicate specific intentions, examines received responses to see if the intentions were carried out, and determines how to interpret the

results. This document defines HTTP/1.1 request and response semantics in terms of the architecture defined in [RFC7230]. [4]

C. FTP:

FTP (File Transfer Protocol) is used to communicate and transfer files between computers on a TCP/IP (Transmission Control Protocol/Internet Protocol) network, aka the internet. Users, who have been granted access, can receive and transfer files in the File Transfer Protocol server (also known as FTP host/site). [5]

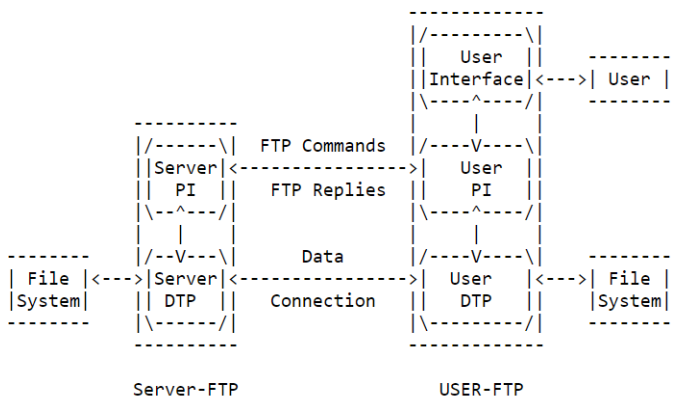


Fig. 1. Model for FTP Use

The user-protocol interpreter initiates the control connection. The control connection follows the Telnet protocol. At the initiation of the user, standard FTP commands are generated by the user-PI and transmitted to the server process via the control connection. (The user may establish a direct control connection to the server-FTP, from a TAC terminal for example, and generate standard FTP commands independently, bypassing the user-FTP process.) Standard replies are sent from the server-PI to the user-PI over the control connection in response to the commands. The FTP commands specify the parameters for the data connection (data port, transfer mode, representation type, and structure) and the nature of file system operation (store, retrieve, append, delete, etc.). The user-DTP or its designate should ”listen” on the specified data port, and the server initiate the data connection and data transfer in accordance with the specified parameters. It should be noted that the data port need not be in File Transfer Protocol the same host that initiates the FTP commands via the control connection, but the user or the user-FTP process must ensure a ”listen” on the specified data port. It ought to also be noted that the data connection may be used for simultaneous sending and receiving. [6]

D. SMTP:

SMTP stands for Simple Mail Transfer Protocol, and it’s an application used by mail servers to send, receive, and/or relay outgoing mail between email senders and receivers.

An SMTP email server will have an address (or addresses) that can be set by the mail client or application that you are using and is generally formatted as smtp.serveraddress.com. For example, the SMTP server Gmail uses is smtp.gmail.com, and Twilio SendGrid’s is smtp.sendgrid.com. You can generally find your SMTP email server address in the account or settings section of your mail client. [7]

When an SMTP client has a message to transmit, it establishes a two- way transmission channel to an SMTP server, and its design is as follows [8]:

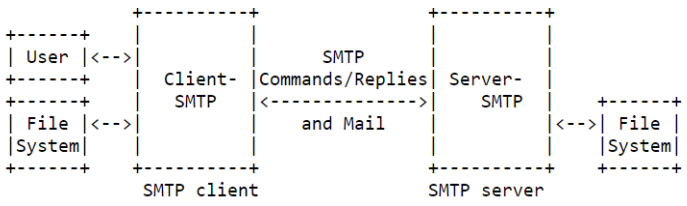


Fig. 2. SMTP design

E. POP:

On the Internet, a point-of-presence (POP) is an access point from one place to the rest of the Internet. (POP also stands for the e-mail Post Office Protocol; see POP3.) A POP necessarily has a unique Internet Protocol (IP) address. Your Internet service provider (ISP) or online service provider (such as AOL) has a point-of-presence on the Internet and probably more than one. [9]

Initially, the server host starts the POP3 service by listening on TCP port 110. When a client host wishes to make use of the service, it establishes a TCP connection with the server host. When the connection is established, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses (respectively) until the connection is closed or aborted. Commands in the POP3 consist of a case-insensitive keyword, possibly followed by one or more arguments. All commands are terminated by a CRLF pair. Keywords and arguments consist of printable ASCII characters. Keywords and arguments are each separated by a single SPACE character. Keywords are three or four characters long. Each argument may be up to 40 characters long. [10]

F. Application layer:

The Application Layer is the seventh layer of the seven-layer OSI model. Application layer interface directly interacts with the application and provides common web application services. The application layer also makes a request to the presentation layer. Application layer is the highest level of open systems, providing services directly for the application process.

Application layer functions

•**Transport access and management** It allows a user to access, retrieve and manage files in a remote computer.

•**Mail services** It provides the basis for email forwarding and storage facilities.

•**Virtual terminal** For various reasons, it can be said that the standardization of terminals has completely failed. The OSI solution to this problem is to define a virtual terminal that is really just an abstract data structure that takes the abstract state of the actual terminal. This abstract data structure can be operated by both the keyboard and the computer and reflects the current state of the data structure on the display. The computer can query this abstract data structure and change this abstract data structure so that the output appears on the screen.

•**Other functions** In addition to the three functions above, there are some other functions: directory services, remote job entry, graphics, information communication and so on. [11]

III. Analysis

In this part of the report we will analyze and answer several questions presented in the lab guide. (To review the topology see annexes).

Which devices in the topology do not require the assignment of an IP address? Why?

Dispositivo	Dirección IP	Puerta de enlace
Router 0	192.168.0.1	N/A
Router 1	192.168.0.10	N/A
Switch 0	N/A	N/A
Server DNS	192.168.0.2	192.168.0.1
Server FTP	192.168.0.4	192.168.0.1
Server HTTP	192.168.0.3	192.168.0.1
Server SMTP/POP3	192.168.0.5	192.168.0.1
Sniffer 0	N/A	N/A
Sniffer 1	N/A	N/A
Sniffer 2	N/A	N/A
PC 0	192.168.0.6	192.168.0.1
PC 1	192.168.0.8	192.168.0.1
Laptop 0	192.168.0.7	192.168.0.1

Fig. 3. IP addresses

A network sniffer "sniffs" or monitors network traffic for information (e.g., where it's coming from, which device, the protocol used, etc.). Network administrators can use this information to help optimize their environment. [12] Bearing in mind the sniffer concept, we know that it does not have an IP address as well as the Switch which, as we have learned in previous labs, does not have an IP address.

What is a default gateway and explain its function in the network?

A computer that sits between different networks or applications. The gateway converts information, data or other communications from one protocol or format to another. A router may perform some of the functions of a gateway. An Internet gateway can transfer communications between an enterprise network and the Internet. Because enterprises often use protocols on their local-area networks (LANs) that differ from those of the Internet, a gateway will often act as a protocol converter so that users can send and receive communications over the Internet. [13]

Which DNS record types (record) should you use in each case? Justify

Let us recall the most commonly used types of records:

A (Host address)
AAAA (IPv6 host address)
ALIAS (Auto resolved alias)
CNAME (Canonical name for an alias)
MX (Mail eXchange)
NS (Name Server)
PTR (Pointer)
SOA (Start Of Authority)
SRV (location of service)
TXT (Descriptive text)

Fig. 4. Commonly used record types

For FTP we use Ns and the name server record indicates which DNS server is authoritative for a domain. For HTTP we use CNAME as it is a canonical name. For SMTP/POP3 we use SOA as it is an email address. For PC0, Laptop0 and PC1 we use Type A as it is a Host address, and we join the address with its domain

FIRST

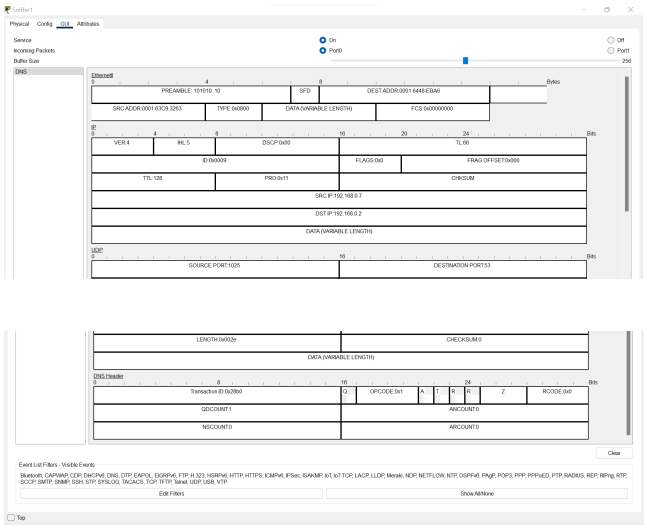


Fig. 5. format

Which source/destination ports are used in the selected frame?

The source port is port 1025 as shown in the image, and the destination port is port 53 (DNS port).

What are the source/destination IP addresses used?

The source IP address is 192.168.0.7 and the destination address is 192.168.0.2.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

SECOND

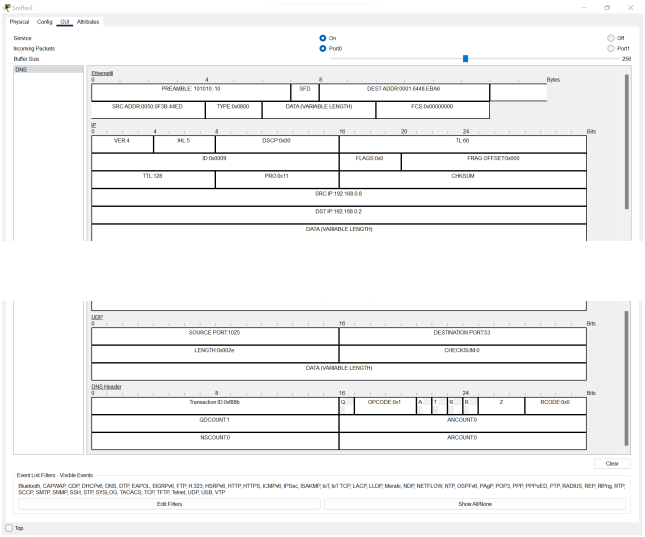


Fig. 6. format

Which source/destination ports are used in the selected frame?

The source port is port 1025 as shown in the image, and the destination port is port 53 (DNS port).

What are the source/destination IP addresses used?

The source IP address is 192.168.0.8 and the destination address is 192.168.0.2.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

THIRD

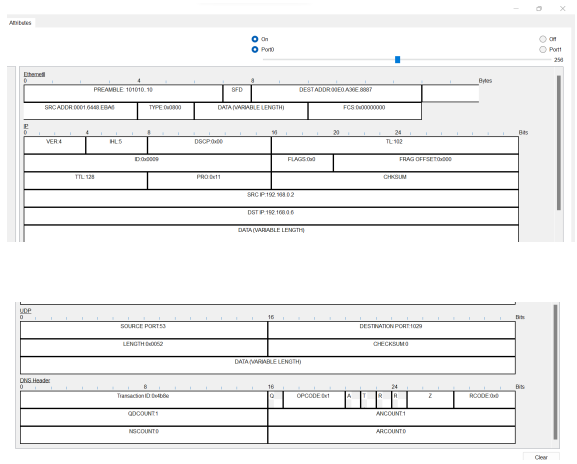


Fig. 7. format

Which source/destination ports are used in the selected frame?

As shown in the image, the destination port is port 1029 and the source port is port 53.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.2 and the destination address is 192.168.0.6.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

What is the function of the ¡hr¿ ¡br¿ ¡p¿ and ¡/¿ commands? Why did you have to delete the index.html file, if you later recreated it, why that name?

The ”h1” tag is used to create the title of a page in html, on the other hand ”br” creates a line break in the page we are creating and when we use a tag that begins with ”/” it means that we are closing it. We delete the index file because we create a new one, this refers to the page that our server will have, index is because it is our main page, remember that html is the language for http.

FIRST

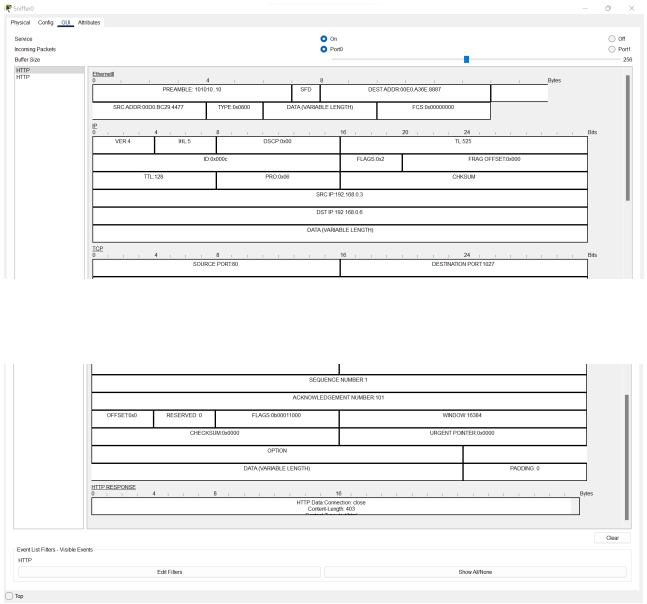


Fig. 8. format http

Which source/destination ports are used in the selected frame?

The source port is port 80 and the destination port is port 1027.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.3 and the destination IP address is 192.168.0.6.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

SECOND

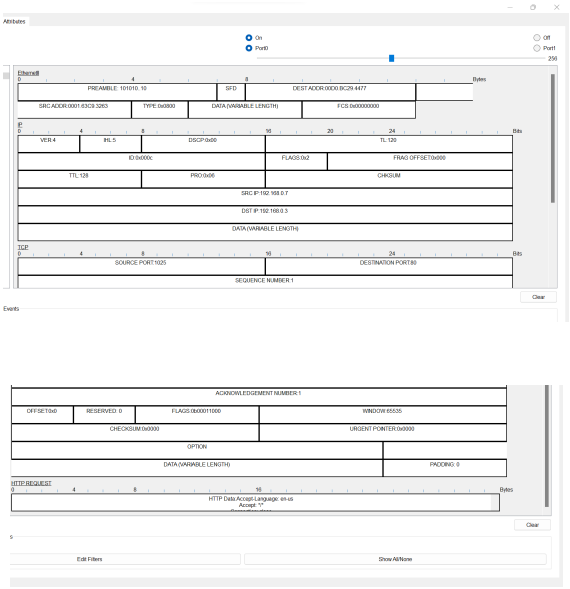


Fig. 9. format http

Which source/destination ports are used in the selected frame?

The source port is port 1025 and the destination port is port 80.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.7 and the destination IP address is 192.168.0.3 .

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

THIRD

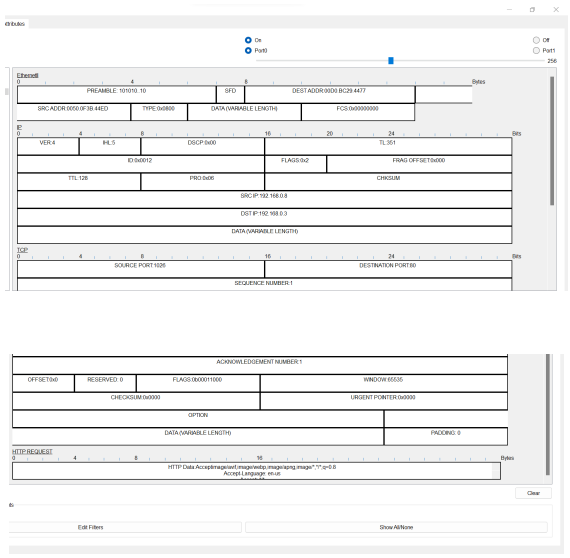


Fig. 10. format http

Which source/destination ports are used in the selected frame?

The source port is port 1026 and the destination port is port 80.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.8 and the destination IP address is 192.168.0.3 .

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

In what environments is FTP protocol used? File Transport Protocol or FTP is a client-initiated transfer where the client can receive a file or can send a file to the server. The specific type of transmission, as well as the level of security, is determined by the server. There are many types of FTP types:

•Active

•Passive

•Simple FTP - SFTP

•Password Protected FTP

•Secure FTP - SFTP

•FTP over SSL

File Transport Protocol or FTP is typically used in business environments to send or receive larger files across a local network or the internet. [14]

What is a super administrator and in which applications does it appear?

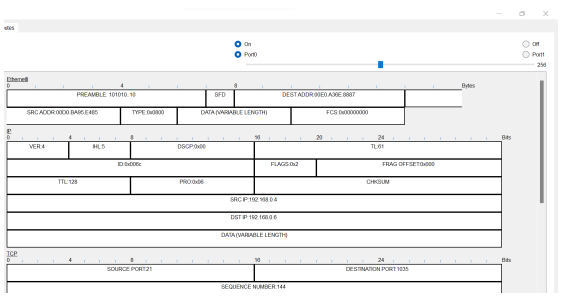
A Super Administrator is a user who has complete access to all objects, folders, role templates, and groups in the system. A deployment can have one or more Super Administrators.

- A Super Administrator can create users, groups, and other super administrators.

- A Super Administrator can delegate administration activities by assigning roles to users through the use of role templates and group administrator permissions.

For example, a Super Administrator can delegate user provisioning functions to other administrators. [15]

FIRST



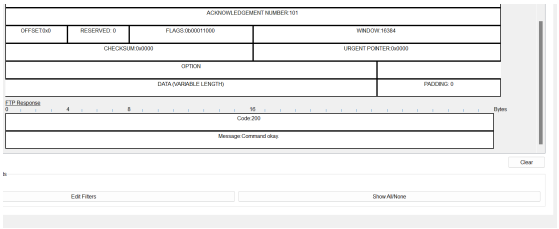


Fig. 11. format FTP

Which source/destination ports are used in the selected frame?

The source port is port 21 and the destination port is port 1035.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.4 and the destination IP address is 192.168.0.6 .

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

SECOND

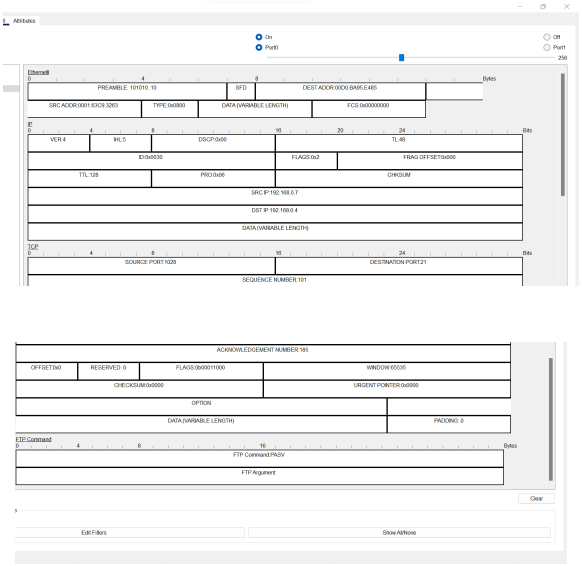


Fig. 12. format FTP

Which source/destination ports are used in the selected frame?

The source port is port 1028 and the destination port is port 21.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.7 and the destination IP address is 192.168.0.4.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

THIRD

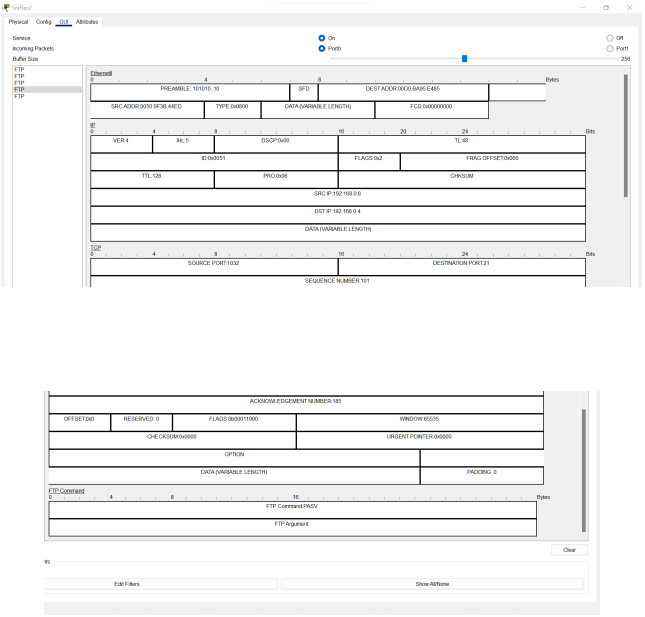


Fig. 13. format FTP

Which source/destination ports are used in the selected frame?

The source port is port 1032 and the destination port is port 21.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.8 and the destination IP address is 192.168.0.4.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

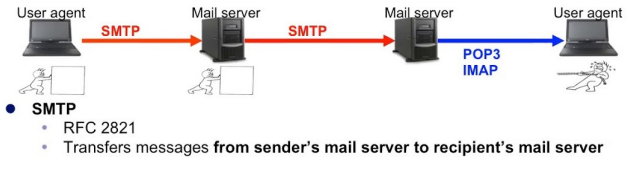


Fig. 14. SMTP and POP3

As we can see SMTP and POP3 work hand in hand, since one is in charge of the output and distribution (SMTP), while the other (POP3) is in charge of the input and organization of the mails, without one of the two the mail service does not work. Likewise, as we explained at the beginning of the report, the domain name is of vital importance to comply with the protocol for sending e-mails by indicating the path to follow.

FIRST

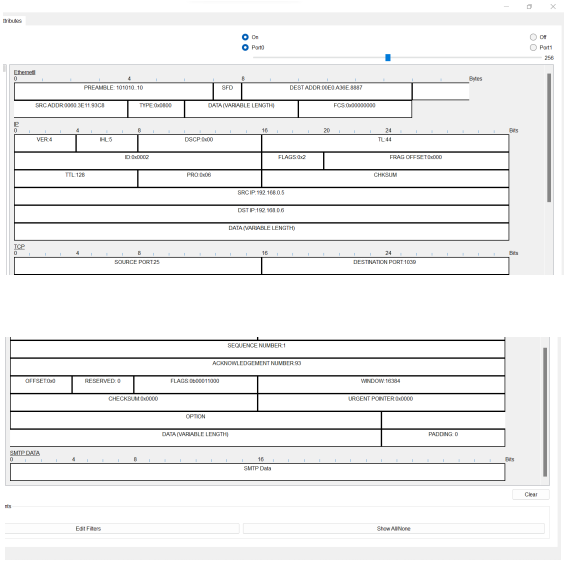


Fig. 15. Format SMTP

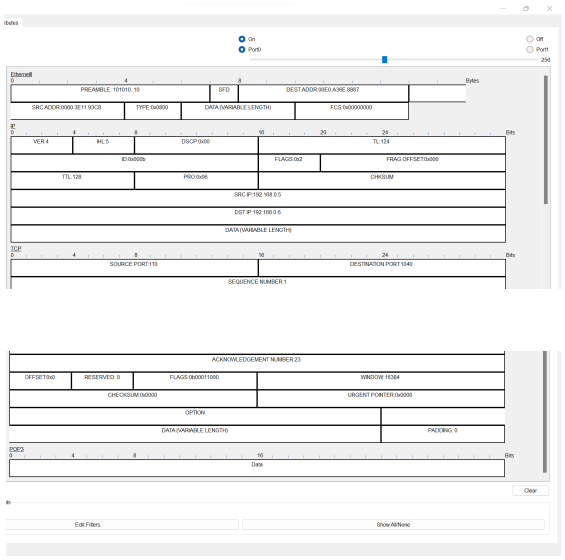


Fig. 16. Format POP3

Which source/destination ports are used in the selected frame?

The source port in the SMTP is 25 and the destination port is 1039. On the other hand, the source port in POP3 is 110 and the destination port is 1040.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.5 and the destination IP address is 192.168.0.6.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

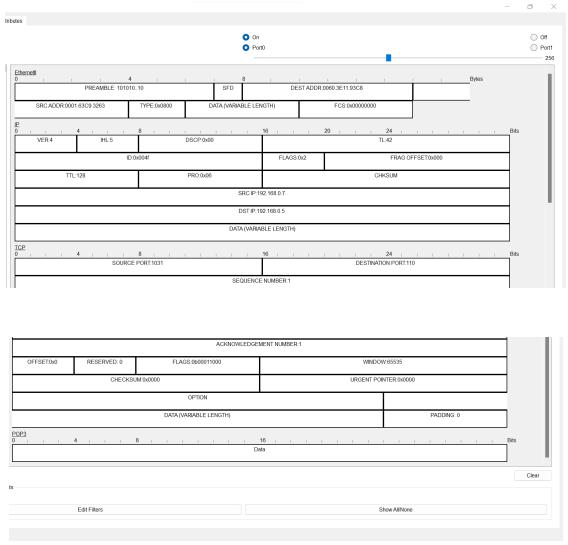


Fig. 17. Format POP3

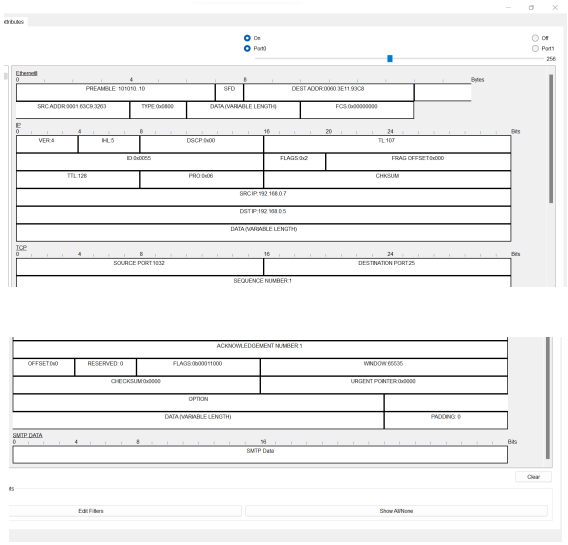


Fig. 18. Format SMTP

SECOND

Which source/destination ports are used in the selected frame?

The source port in the SMTP is 1032 and the destination port is 25. On the other hand, the source port in POP3 is 1031 and the destination port is 110.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.7 and the destination IP address is 192.168.0.5.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

THIRD

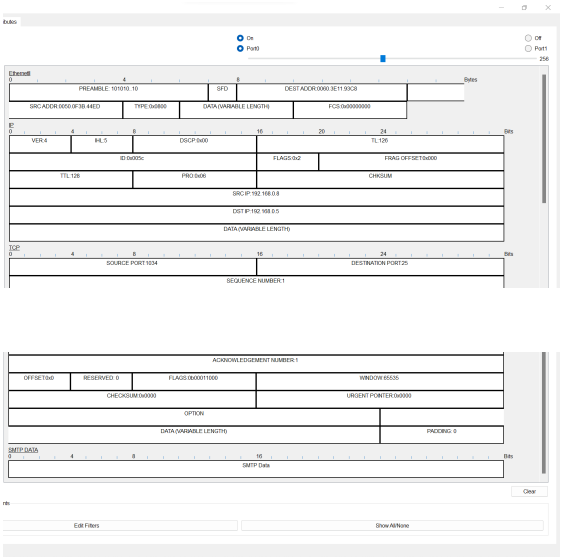


Fig. 19. Format SMTP

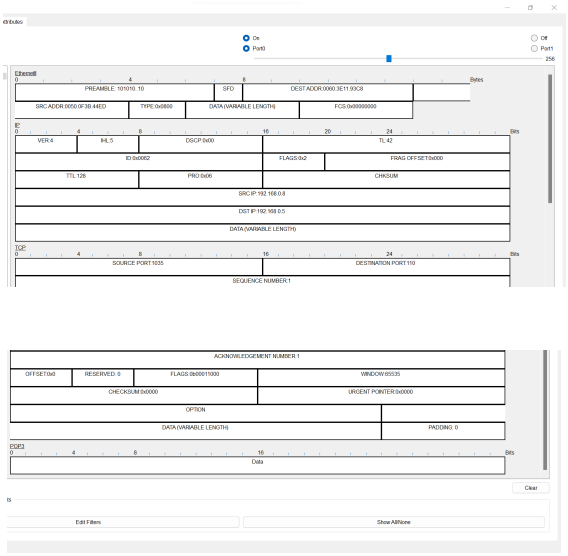


Fig. 20. Format POP3

Which source/destination ports are used in the selected frame?

The source port in the SMTP is 1034 and the destination port is 25. On the other hand, the source port in POP3 is 1035 and the destination port is 110.

What are the source/destination IP addresses used?

The source IP address is 192.168.0.8 and the destination IP address is 192.168.0.5.

Is there information on the net size of the data carried in the frame?

The net size in this case we do not know, it is variable as shown by the format

What is the advantage of using the SNMP protocol on a data network? What limitations does Cisco Packet Tracer have with respect to MIB objects? If you ran it on a desktop client on a real network, would you get the same or different information presented in the simulator? information presented in the simulator or a different one?

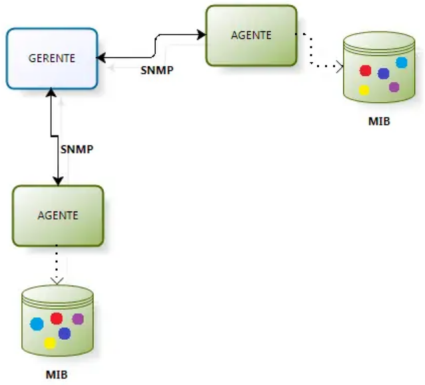


Fig. 21. SNMP management model

SNMP helps the network manager to locate possible problems and errors in your network. Through an SNMP manager (e.g. SLAview), graphs of traffic statistics can be displayed. In addition to the SNMP manager, it is necessary for each device to be monitored to have an SNMP agent. The agent will receive requests from the manager and return with the information. A MIB (Management Information Base) is a database that describes the properties of each component in a network device, for example a tape library. MIBs are stored in the SNMP manager. When data is sent from the device to an SNMP manager, the manager's compiler uses the MIB to convert the data to a user-readable format. [16] Cisco does not present all the expected data, so we would see limited data, while a customer with a real-life network would have many other objects and possibilities that Cisco does not show.

IV. CONCLUSIONS

In this lab we observed various application layer protocols. This was achieved thanks to Cisco Packet Tracer, the tool that allowed us to analyze each packet with the sniffers in the various cases that were presented to us, as well as the topology implemented helped us to have a clearer understanding of the technical concepts. On the other hand, the study of the RFCs of each protocol and various concepts helped us to understand each protocol in depth. It was very enriching the process that we had in this laboratory since the practical part made us reflect and analyze with each small step that we took in the construction of the requirements such as having correctly configured the SMTP/POP3 server so that the message arrived in a proper way. Now we are able to analyze situations of daily life and reflect on the technical concepts involved in actions such as sending an email.

REFERENCES

[1] ”Cloudflare - The Web Performance Security Company”. Cloudflare. https://www.cloudflare.com/ (accedido el 2 de octubre de 2022).

[2] ”RFC 1034: Domain names - concepts and facilities”. RFC Editor. https://www.rfc-editor.org/rfc/rfc1034 (accedido el 2 de octubre de 2022).

[3] ”Home · Cloudflare Docs”. Home · Cloudflare Docs. https://developerscloudflare.com (accedido el 2 de octubre de 2022).

[4] ”RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”. RFC Editor. https://www.rfc-editor.org/rfc/rfc7231section-1 (accedido el 2 de octubre de 2022).

[5] ”What is FTP: FTP Explained for Beginners”. Hostinger Tutorials. https://www.hostinger.com/tutorials/what-is-ftpWhatIsFTP (accedido el 2 de octubre de 2022).

[6] RFC-es - Grupo de Traducción de RFC al español. https://www.rfc-es.org/rfc/rfc0959-es.txt (accedido el 2 de octubre de 2022).

[7] ”What Is an SMTP Server? — Twilio SendGrid”. SendGrid. https://sendgrid.com/blog/what-is-an-smtp-server/ (accedido el 2 de octubre de 2022).

[8] ”RFC 5321: Simple Mail Transfer Protocol”. RFC Editor. https://www.rfc-editor.org/rfc/rfc5321section-2 (accedido el 2 de octubre de 2022).

[9] T. Contributor. ”What is point-of-presence (POP)? - Definition from WhatIs.com”. SearchNetworking.https://www.techtarget.com/ searchnetworking/definition/point-of-presence-POP: :text=On20the20Internet, 20a20point,Internet20Protocol20(IP)20address. (accedido el 2 de octubre de 2022).

[10] RFC Editor. https://www.rfc-editor.org/rfc/rfc1939.txt (accedido el 2 de octubre de 2022).

[11] ”2022 Sourcing Season - Router-Switch.com”. Cisco Router, Cisco Switch, New Used Cisco Prices Comparison. https://www.router-switch.com/faq/what-is-application-layer-the-functions-and-examples-of-application-layer.html (accedido el 2 de octubre de 2022).

[12] ”Network Sniffers: What Are They and How Can I Use Them?” PagerDuty. https://www.pagerduty.com/resources/learn/what-are-network-sniffers/ (accedido el 3 de octubre de 2022).

[13] ”Definition of Gateway - Gartner Information Technology Glossary”. Gartner. https://www.gartner.com/en/information-technology/glossary/ gateway: :text=A20computer20that20sits20between,enterprise20network20and 20the20Internet. (accedido el 3 de octubre de 2022).

[14] https://study.com/academy/lesson/what-is-file-transfer-protocol -ftp-definition-lesson-quiz.html: :text=File20Transport20Protocol20orFTP, local20network20o20the20internet. (accedido el 3 de octubre de 2022).

[15] ”IBM Documentation”. IBM - Deutschland — IBM. https://www.ibm.com/docs/en/opw/8.1.0?topic=domains-super-administrator (accedido el 3 de octubre de 2022).

[16] ”IBM Documentation”. IBM - Deutschland — IBM. https://www.ibm.com/docs/es/ts4500-tape-library?topic=library-management-information-base-mib-files (accedido el 3 de octubre de 2022).

V. ANNEXES

Topology