**EXERCISE 2:**

**1.)**

**HTTP (*Hypertext Transfer Protocol):***

It is a protocol for transmitting data over the internet. It is used to send and receive data between a client (such as a web browser) and a server (such as a web server).

Some of the main functions of HTTP include:

* **Requesting data:** HTTP enables clients to request data from servers using methods such as GET, POST, PUT, and DELETE.
* **Receiving data:** HTTP enables servers to send data to clients in response to requests.
* **Transferring data:** HTTP enables the transfer of data between clients and servers in the form of messages, which consist of a request line, headers, and a message body.
* **Caching:** HTTP enables the caching of responses to requests, which can improve the performance of the system by reducing the need to send the same data repeatedly.
* **Security:** HTTP can be used in conjunction with secure protocols such as HTTPS to provide secure communication between clients and servers.
* **Compression:** HTTP enables the use of compression algorithms to reduce the size of the data being transmitted, which can improve the speed of data transfer.
* **Redirection:** HTTP enables servers to redirect clients to other resources, which can be useful for managing the flow of traffic on a website.

**HTTPS *(Hypertext Transfer Protocol Secure):***

It is a secure version of HTTP, the protocol used to transmit data over the internet. It adds an additional layer of security to the connection between a client (such as a web browser) and a server (such as a web server) by encrypting the data being transmitted.

Some of the main functions of HTTPS include:

* **Encrypting data:** HTTPS uses a secure protocol such as SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt the data being transmitted between a client and a server. This makes it difficult for anyone to intercept and read the data as it is being transmitted.
* **Providing authentication:** HTTPS enables the use of digital certificates to authenticate the identity of the server. This helps to prevent man-in-the-middle attacks, in which an attacker intercepts the communication between a client and a server and masquerades as the server.
* **Ensuring data integrity**: HTTPS uses checksums and other mechanisms to ensure that the data being transmitted has not been modified during transmission.
* **Improving security:** HTTPS helps to improve the security of the internet by enabling secure communication between clients and servers. It is often used to protect sensitive information such as passwords and financial data.
* **Increasing trust:** HTTPS can increase the trust of users in a website by demonstrating that the website is legitimate and secure. Many web browsers display a padlock icon or a green address bar when a website is using HTTPS.

**DHCP *Dynamic Host Configuration Protocol***:

It is a network protocol used to dynamically assign IP addresses and other network configuration information to devices on a network.

DHCP is widely used on networks of all sizes, from small home networks to large enterprise networks. It helps to simplify the management of network configuration and ensure that devices can communicate with each other on the network.

Some of the main functions of DHCP include:

* **Automatically assigning IP addresses:** DHCP enables devices to automatically receive an IP address and other network configuration information when they connect to a network. This eliminates the need for administrators to manually assign IP addresses to each device.
* **Allocating IP addresses efficiently**: DHCP uses a pool of available IP addresses and assigns them to devices as needed, helping to ensure that the addresses are used efficiently.
* **Providing network configuration information:** DHCP can also provide devices with other network configuration information, such as the default gateway, DNS servers, and subnet mask.
* **Managing IP address leases:** DHCP assigns IP addresses to devices for a specific period of time, called a lease. When the lease expires, the device must request a new lease to continue using the same IP address. This enables DHCP to reclaim IP addresses that are no longer in use and assign them to other devices.
* **Facilitating network changes:** DHCP enables administrators to easily make changes to the network configuration, such as adding or removing devices or changing the IP address range, without having to manually reconfigure each device.

**DNS (*Domain Name System):***

It is a protocol used to translate human-readable domain names into numerical IP addresses that computers can understand and use to communicate with each other.

DNS plays a critical role in the operation of the internet by enabling users to access internet resources using human-readable domain names and by mapping those names to the numerical IP addresses that computers use to communicate with each other.

Some of the main functions of DNS include:

* **Resolving domain names:** DNS enables users to access websites and other internet resources using easy-to-remember domain names, rather than having to remember and enter the numerical IP addresses of those resources.
* **Mapping domain names to IP addresses:** DNS maintains a database of domain names and their corresponding IP addresses, and it uses this database to resolve domain names and return the correct IP address to clients.
* **Improving the scalability of the internet:** It enables the internet to scale to a large number of devices and resources by allowing domain names to be used instead of IP addresses. This helps to make it easier for users to access the internet and for administrators to manage internet resources.
* **Enhancing security:** It can be used to enhance security by allowing administrators to control which resources are available to users and by enabling the use of secure protocols such as DNSSEC (Domain Name System Security Extensions) to authenticate DNS responses and protect against certain types of attacks.
* **Providing redundancy:** DNS servers are distributed across the internet, and each domain name has multiple servers that can resolve it. This helps to ensure that the system is highly available and can continue to function even if some servers are unavailable.

**SMTP *(Simple Mail Transfer Protocol)*:**

It is a protocol used for transmitting email messages between servers. Most email systems use SMTP to send messages from one server to another, and to deliver messages to local mail clients.

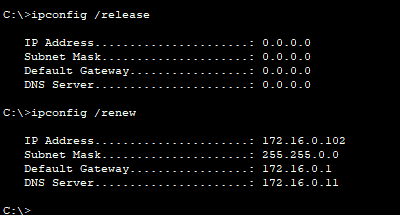
SMTP is an essential part of the email infrastructure of the internet, enabling the transmission of messages between servers and the delivery of those messages to local mail clients.

*Some of the main functions of SMTP include:*

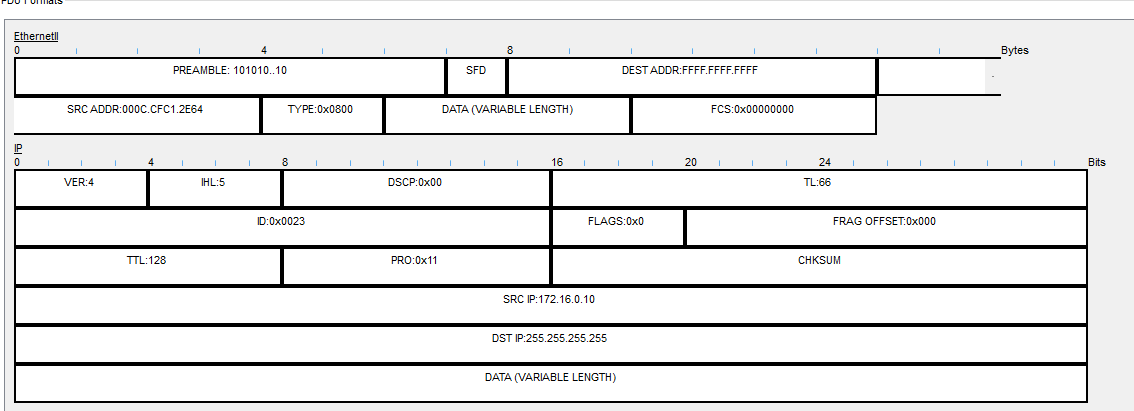
* **Sending email:** Allows email servers to send messages to other servers and to local mail clients.
* **Receiving email:** SMTP enables email servers to receive messages from other servers and to deliver them to local mail clients.
* **Relaying email:** SMTP enables email servers to relay messages to other servers, which can be useful when sending email to recipients on different networks or domains.
* **Authenticating users**: SMTP can be configured to require authentication before allowing a client to send email, which helps to prevent spam and unauthorized use of the email system.
* **Enabling the use of attachments:** SMTP enables the use of attachments in email messages, allowing users to send files and other types of data along with their messages.
* **Providing delivery notifications:** SMTP enables the use of delivery notifications, which allow senders to receive notifications when their messages are delivered or when there are problems with delivery.

**2.)**

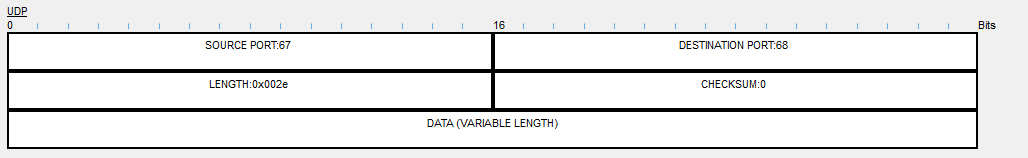
**-Performing ipconfig /release then ipconfig /renew**

****

|  |  |
| --- | --- |
|  | Answer |
| Preamble | 101010..10 |
| Source MAC Address | 000C.CfC1.2E64 |
| Destination MAC address | FFFF.FFFF.FFFF |
| Type Field Value | 0x0800 |
| Source IP address | 172.16.0.10 |
| Destination IP address | 255.255.255.255 |

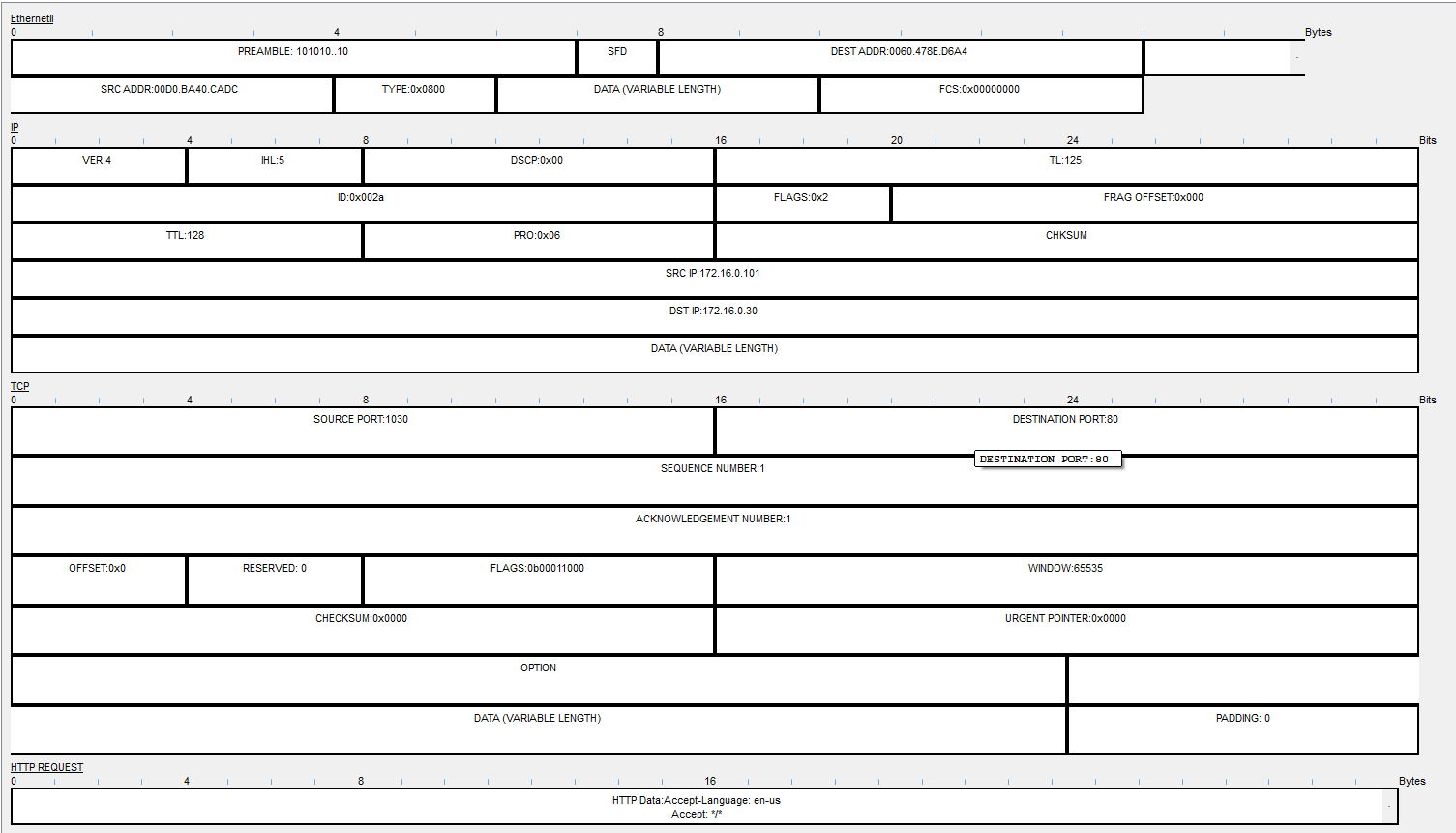
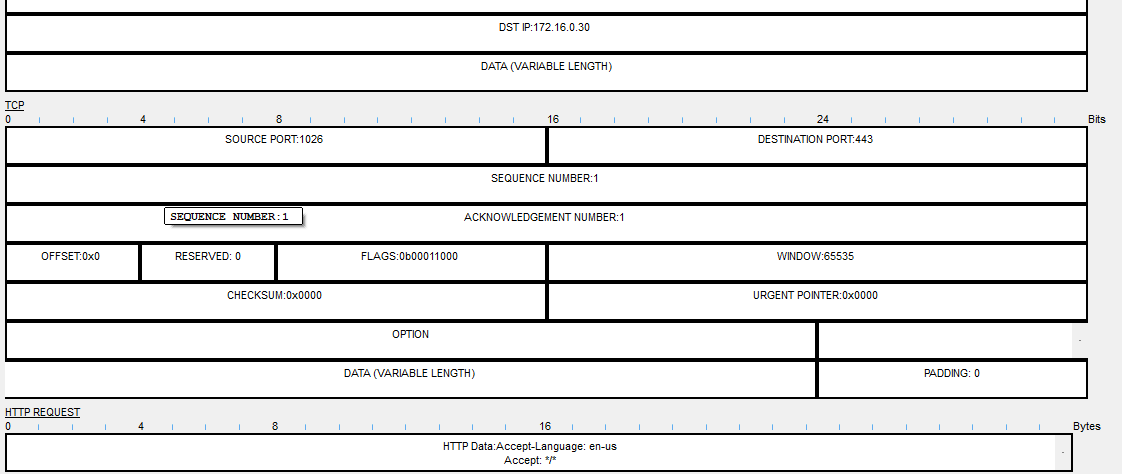
**(screenshot of the PDU information) **

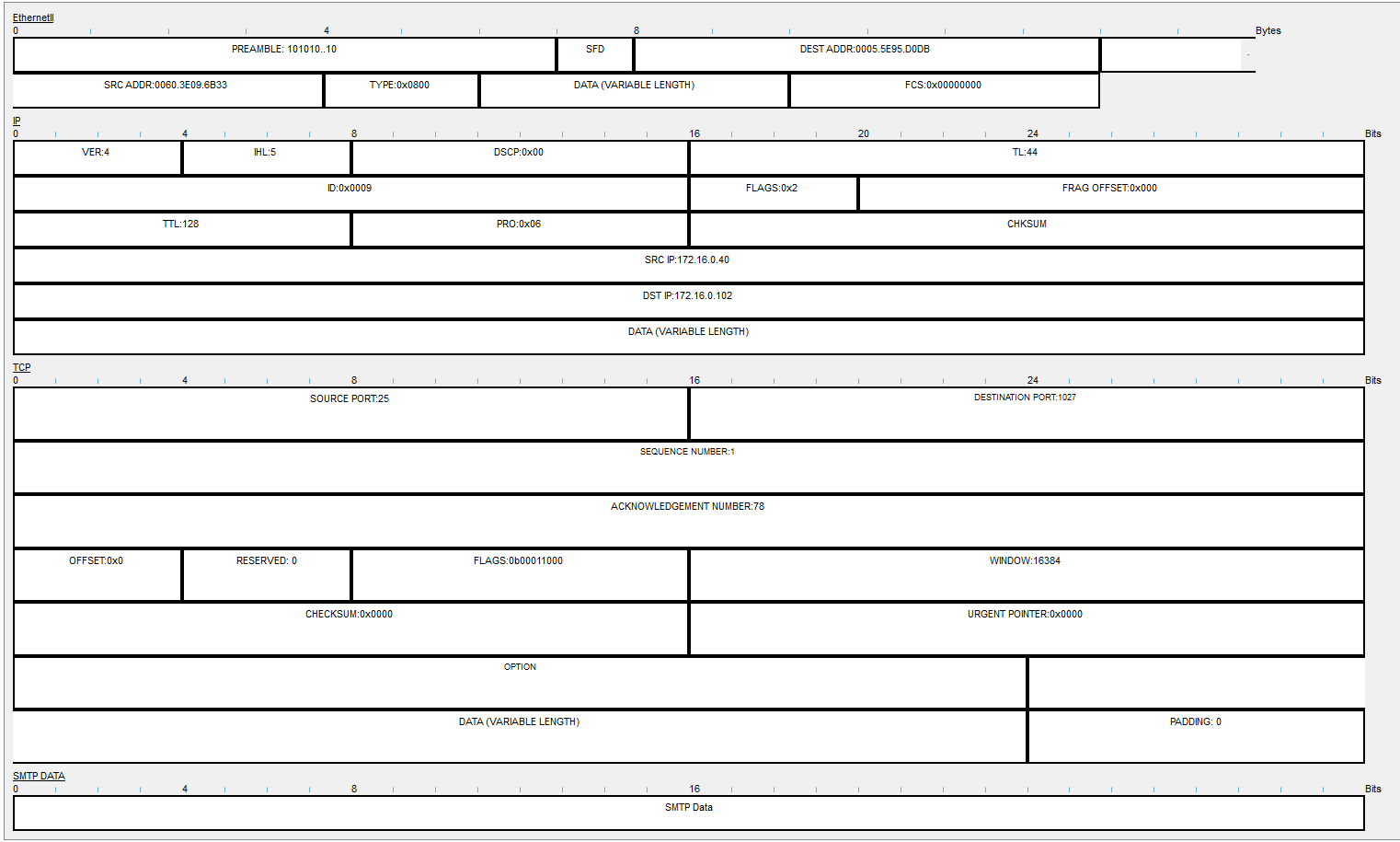
**a.)**

**DHCP** is running **UDP** services.  **Source** Port of **DHCP** servers is **67**.  
**Destination** port of **DHCP** servers is **68**.

**b.)**

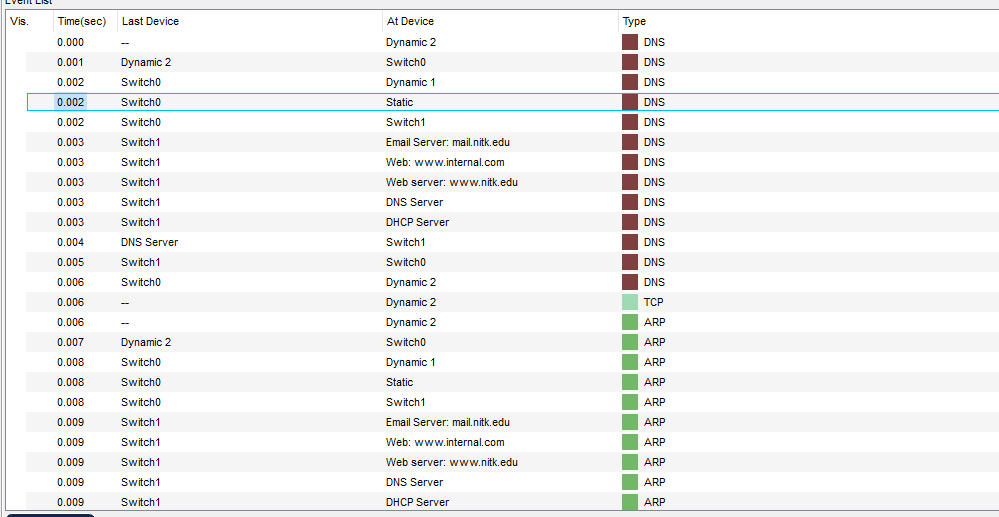
Three application protocols using TCP services are:

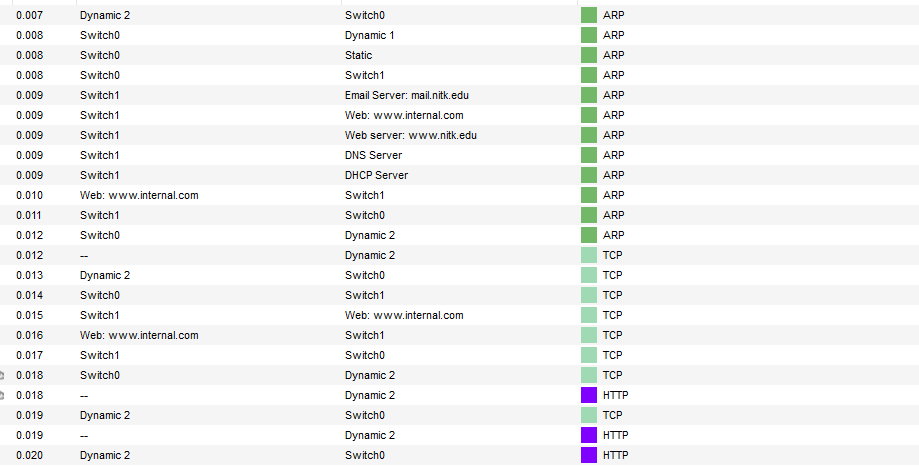
* **HTTP**
* 
* **HTTPS**
* 

SMTP  


**3.)**

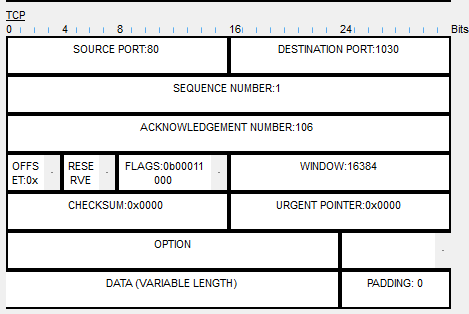
**a.) Before the interaction of client using HTTP AND HTTPS; DNS, TCP and ARP were used.**

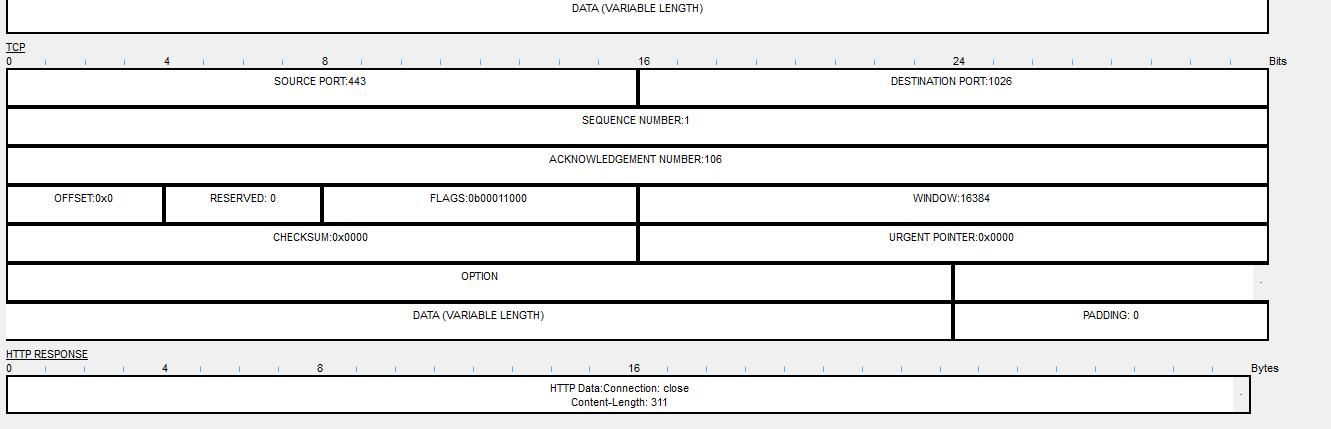




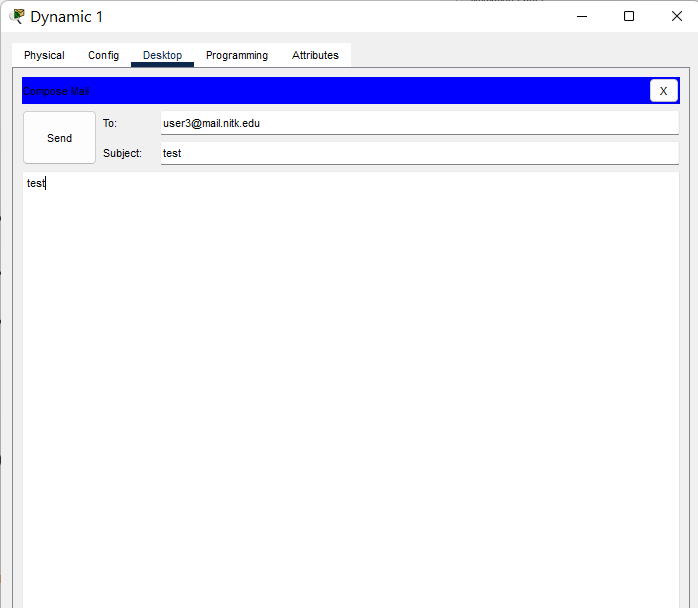
**b. )**

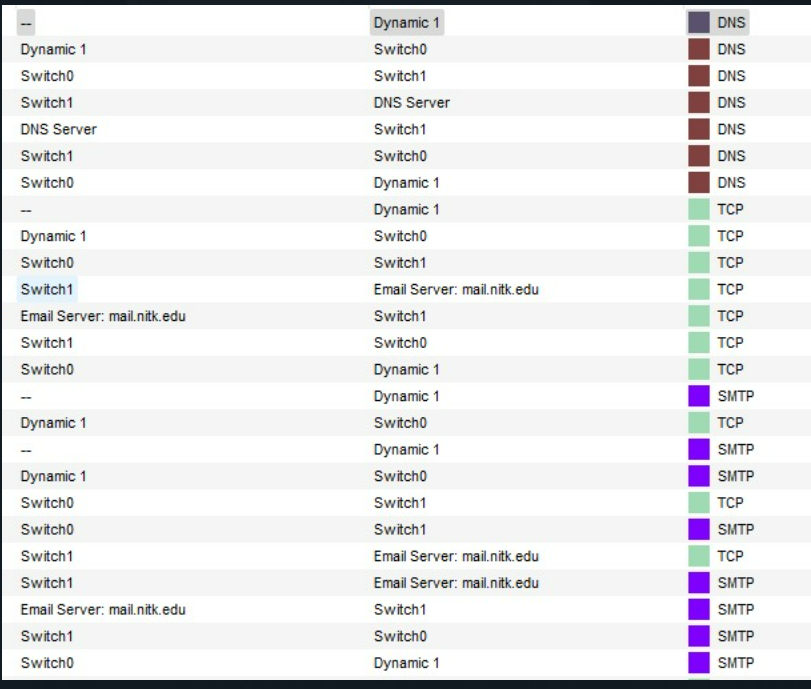
Source Port used by HTTP is **80**

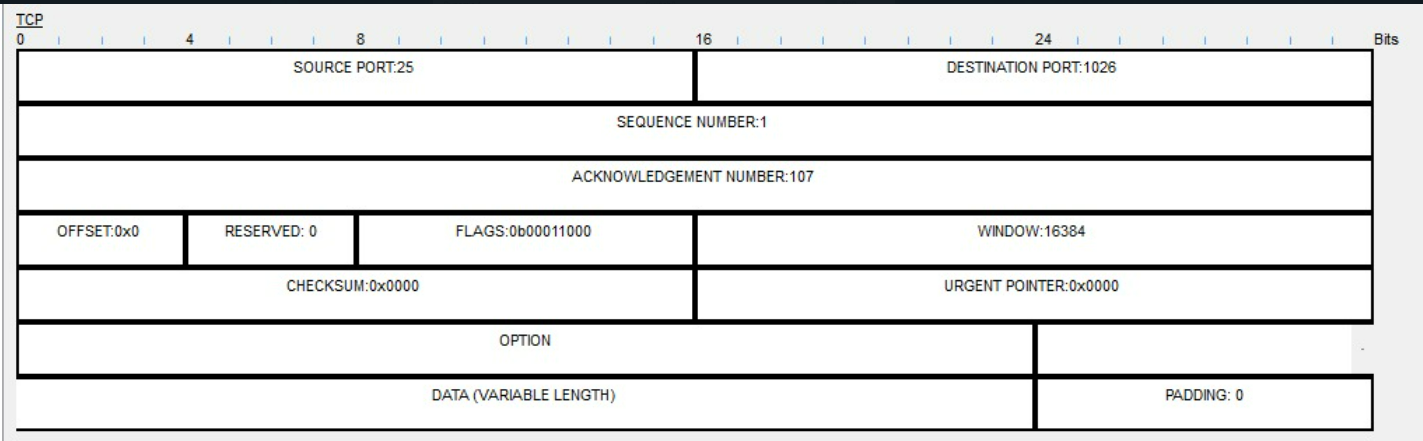
  
Source Port used by HTTPS is **443**



c.)

4.)  






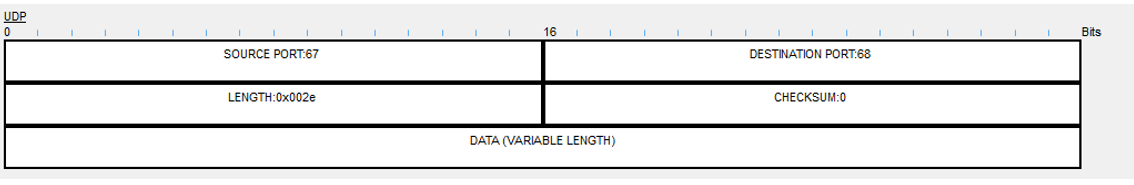
The protocols used before setting up SMTP are:

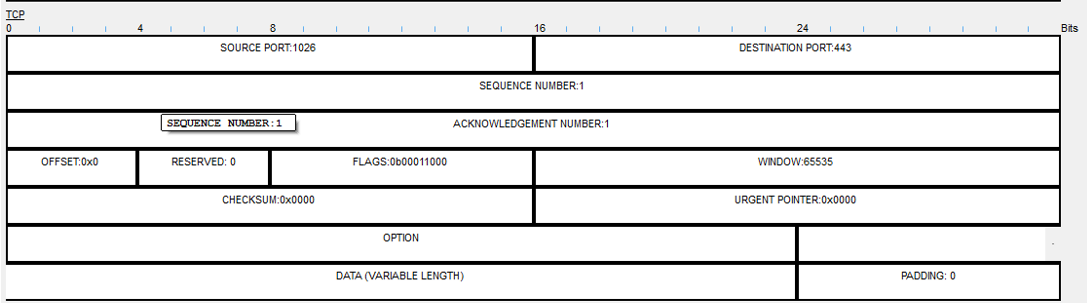
* DNS
* TCP
* ARP

b.)

The source port used by servers running **SMTP** is **25**.

5.)





Protocols serviced by TCP are as follows:

* HTTP
* HTTPs
* SMTP

Protocols serviced by UDP are as follows:

* DNS
* DHCP

Fields used by TCP are:

* Sequence Number
* AcK number
* Data offset
* Reserved
* Control bit
* Window
* Urgent Pointer
* Options
* Padding
* Check Sum
* Source port
* Destination port

Fields used by UDP are:

* source port
* destination port
* check sum
* Length

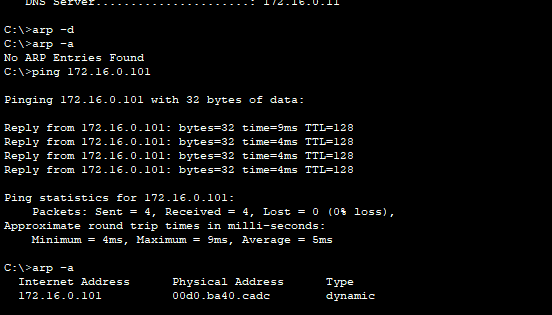
**6.)**

**a.)** Before interaction of the clients using ping; ARP was used.

**b.)**

**Internet Address:** 172.16.0.101

**Physical Address:** 00d0.ba40.cadc

****

**c.)**

|  |  |
| --- | --- |
|  | Answer |
| Source IP address | 172.16.0.102 |
| Destination IP address | 172.16.0.101 |
| ICMP Type value | 0x08 |
| ICMP code value | 0x00 |
| Source Ethernet Address | 0005.5E95.D0DB |
| Destination Ethernet Address | 00D0.8A40.CADC |
| Internet Protocol version | 4 |
| Time to Value | 128 |

