COMPUTER COMMUNICATION AND NETWORKING LAB (IT205)

ASSIGNMENT 6
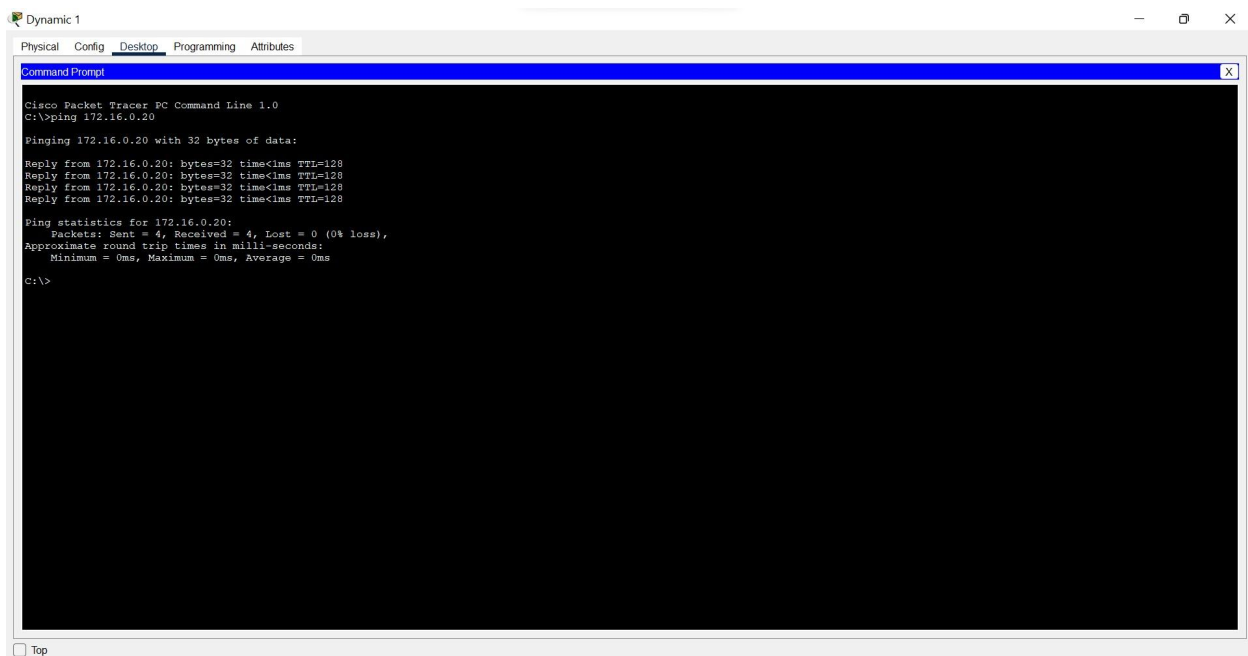
Name: Sachin Prasanna

Roll : 211IT058

1. m)

Verifying the connectivity of the Network:

Ping (ICMP)

Web Browser (HTTP)

Email (SMTP)

Static						– ☐ ✕

Physical Config Desktop Programming Attributes

Message   X

Reply

From: user1@mail.nitk.edu   Sent: Wed Dec 28 2022 00:14:27
To: user3@mail.nitk.edu
Subject: Test Email

This is Dynamic 1 !

☐ Top

PTO

1. n)

Output of the command ipconfig /renew

```
Dynamic 2                                                          —  □  ✕

Physical   Config   Desktop   Programming   Attributes

Command Prompt                                                         X

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /renew

  IP Address......................: 172.16.0.101
  Subnet Mask.....................: 255.255.0.0
  Default Gateway.................: 172.16.0.1
  DNS Server......................: 172.16.0.11

C:\>

☐ Top
```
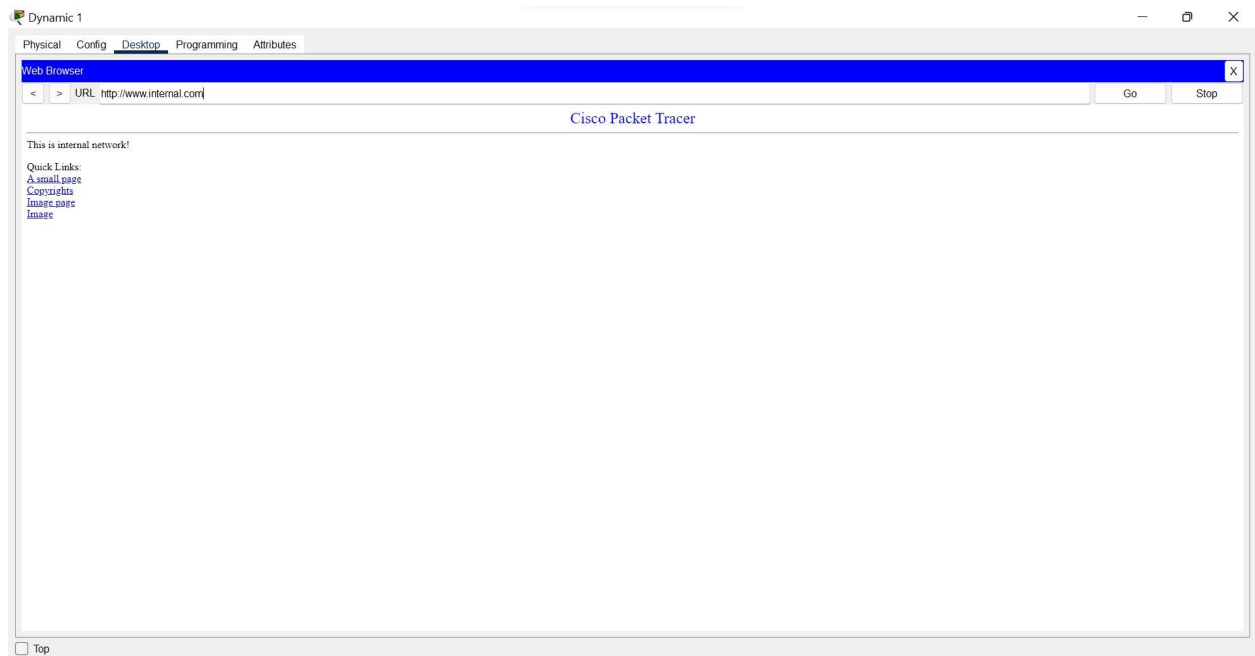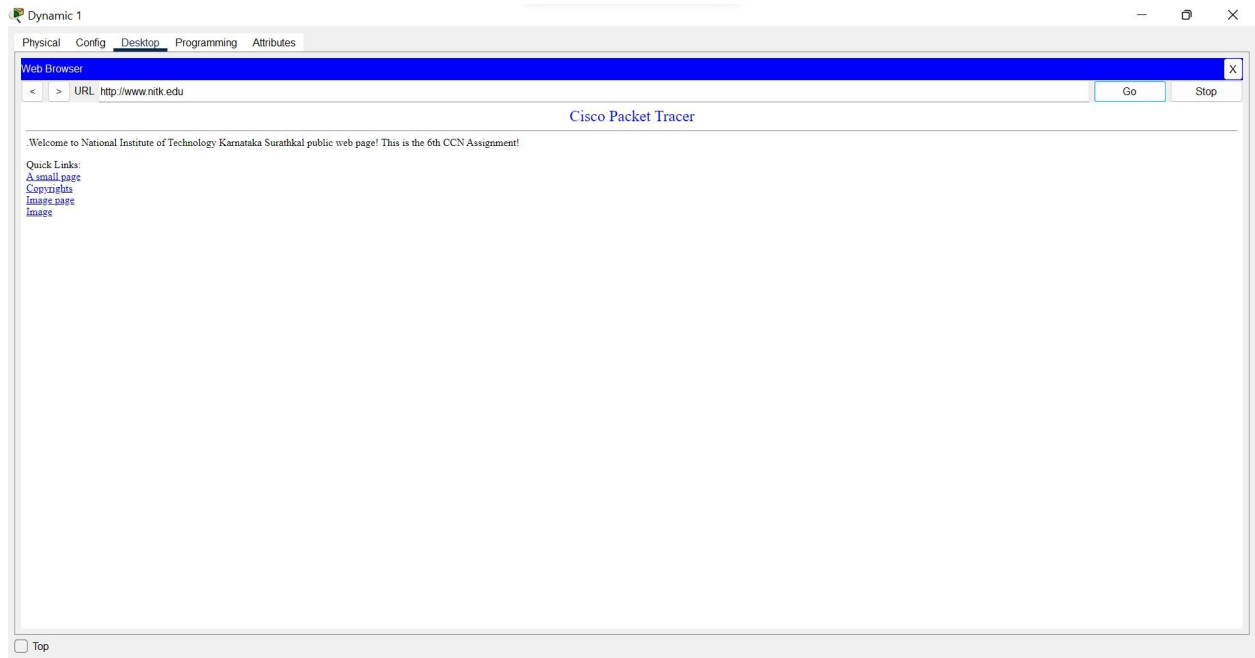
2.
1. a) HTTP (Hypertext Transfer Protocol)

HTTP (Hypertext Transfer Protocol) is a protocol designed for transmitting data over the internet. It is used to send and receive data, basically exchange data between a client and a server.
Some of the main functions of HTTP include:

- **Requesting data:** HTTP enables clients to request data from servers using various methods like GET, POST, DELETE, etc.

- **Receiving data:** HTTP lets servers send data to clients in response to requests.
- **Transferring data:** HTTP is the protocol behind data between clients and servers in the form of messages, which consist of a request line, headers, and a message body.
- **Security:** HTTP can be used along with more secure protocols such as HTTPS to provide more security.
- **Redirection:** HTTP enables servers to redirect clients to other resources, which is useful for managing traffic.

b) HTTPS (Hypertext Transfer Protocol Secure)

HTTPS (Hypertext Transfer Protocol Secure) 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 and a server by adding a layer of encryption in the data being transmitted.

Some of the main functions of HTTPS include:

- **Encrypting data:** HTTPS uses secure protocols 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 harder for the hackers to track and intercept any data 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.
- **Ensuring data integrity:** HTTPS uses checksums and other error checking mechanisms to ensure that the data being transmitted has not been modified or errored during transmission.

- **Improving security:** HTTPS helps to improve the security of the internet by enabling secure communication between clients and servers. Due to this extra protection, personal information like passwords stay protected.

c) DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically assign IP addresses and other network configuration information to the various devices on a network.It is widely used on networks of all sizes. 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 and not wasted
- **Providing network configuration information:** DHCP can also provide devices with other network configuration information, such as the Subnet mask, default gateway, etc.
- **Managing IP address leases:** DHCP assigns IP addresses to devices for a specific period of time, this is called a lease. When this lease expires, the device must request a new lease to

continue using the same IP address. Thus DHCP can retake other IP addresses that are no longer in use and assign them to other devices.

d) DNS (Domain Name System)

DNS (Domain Name System) is a protocol used to translate 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 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:

- **Enhancing security:** DNS can be used to enhance security by allowing administrators to control which resources are available to users and also by enabling the use of secure protocols such as DNSSEC, etc to authenticate DNS responses and protect against attacks.
- **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. It finally uses this database to resolve domain names and return the correct IP address to the clients.
- **Improving the scalability of the internet:** DNS 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.

e) SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol) is a protocol used to transmit email messages between servers. Most email systems use SMTP (PoP is also used nowadays) to send messages from one server to another, and to deliver messages to local mail clients.

Some of the main functions of SMTP include:

- **Sending email and Receiving email:** SMTP enables email servers to send and receive messages to other servers and to local mail clients.
- **Relaying email:** SMTP enables email servers to relay messages to other servers.
- **Authenticating users:** SMTP can be configured to require authentication before allowing a client to send email, which helps in spam detection.
- **Providing delivery notifications:** SMTP enables the use of delivery notifications, which allow senders to receive notifications when their messages are delivered or if it has not been delivered owing to some problems in the mail.

2.

The information as seen in the outbound PDU tab are filled in the following table:

	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

a)

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

b)

The three application protocols using TCP services are:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- SMTP (Simple Mail Transfer Protocol)

3.

a)

Before the interaction of the client using HTTP and HTTPS, **DNS protocol was used first**, along with **TCP** and **ARP** being used subsequently after it.

b)

Source Port used by HTTP servers is **80**
Source Port used by HTTP servers is **443**

c)

4.

a)

Before the interaction of the clients using SMTP, the **DNS protocol was used first,** along with **TCP** protocol being used subsequently after it.

b)

The Source Port used by servers running SMTP is **25**

5.

After identification, it is found that,

The protocols serviced by TCP are **HTTP**, **HTTPS** and **SMTP**.
The protocols serviced by UDP are **DNS** and **DHCP**.

Fields used in TCP are:
Source Port, Destination Port, Sequence Number, AcK Number, Data offset, Reserved, Control bit, Window, Urgent Pointer, Options, Padding and CheckSum

Fields in UDP are:
Source Port, Destination Port, CheckSum, Length

Hence, 3 fields present in TCP that are not found in UDP are:
Data offset, Reserved, Control bit

6.

a)

Before the interaction of the clients with ping, **ARP** (Address Resolution Protocol) **protocol was used first**.

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