

CET2032 - Computer Networks & Network Security - Practicum 02

Task 2

1. What were the protocols used? (select any THREE) What do each of these protocols do, generally? (12 marks)

A: Address Resolution Protocol (ARP) is a communication protocol for resolving an ever-changing network-layer address such as the IP address to a fixed MAC address. In other words, it is used to find an unknown MAC address by mapping it to the corresponding known IP address. To send data to the correct IP address, the sender must have the MAC address of the destination. If the sender's ARP table has an entry for the destination, it will have the MAC address of the destination. However, if the ARP table does not have that entry, an ARP query packet is sent out to the subnet and once there is a match to the IP address in that ARP packet a response ARP packet containing the corresponding MAC address is sent back to the sender who can now update its ARP table and send its data out to the correct MAC address.

Transmission Control Protocol (TCP) offers transport layer addressing for application processes in the form of TCP ports and enables computers to communicate with one another over these ports. It establishes a connection between two apps, i.e., it constructs a temporary virtual circuit during the connecting process. This is a complete duplex circuit; data is sent in both directions concurrently and independently. To establish a connection a three-way handshake is carried out by utilising the SYN and ACK flag. To close a connection, it utilises the FIN and ACK flag.

Hypertext Transfer Protocol (HTTP) is an application-layer protocol, is the underlying protocol of the Web. HTTP messages are used to communicate between the client and server programs running on separate end systems. The protocol describes the structure of these messages and the way they are exchanged between the client and server. In general, when a user requests a web page the browser will send HTTP request messages for the objects in the page to the server. The server receives the requests and replies with HTTP response messages containing the objects.

2. What was the user's device's MAC address? (2 marks)

A: 02:42:ac:11:00:02

3. What was the user's device's IP address on the local network? (2 marks)

A: 172.17.0.2

4. What was the IP address/addresses of the server which responded to the HTTP request? (4 marks)

A: 172.217.26.68 and 151.101.129.67

5. What was the domain name/s that resolved to those IP address/addresses in Q4? (4 marks)

A: www.google.com and edition.cnn.com

6. What TCP/IP Transport layer protocol did the DNS query use? (2 marks)

A: The DNS query used User Datagram Protocol (UDP)

7. What was the port of the user's device that sent information to www.google.com (HTTP request/response)? (2 marks)

A: Port 33610 and 33614

8. What was the port of the server serving www.google.com that sent information to the user's device (HTTP request/response)? (2 marks)

A: Port 80