CS 315: Computer Networks Lab
Spring 2025, IIT Dharwad

End-semester Exam
April 26, 2025

09:30 AM to 12:30 PM
Total Marks: 85.5

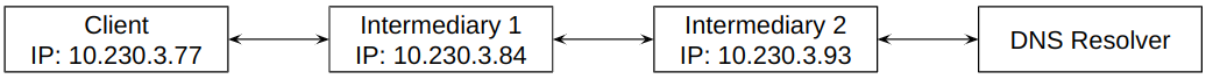
Name: _____ **Roll No.** _____

Instructions

- This is a question paper-cum-answer sheet, which must be submitted to the invigilator at the end of the exam.
- Answers are to be written exclusively in the space provided after each question.
- Extra sheets may be used for rough work, which need not be submitted.
- No notes, books, cheat-sheet, etc. are allowed in this exam.
- To answer each question, please refer to the corresponding trace file.

Part 1 [25 marks]: DNS, IP, and Transport Layer

Scenario: Four nodes involved in a DNS resolution path, namely, `client`, `intermediary1`, `intermediary2`, and the `DNS resolver`, as shown below:



On the client's system, we execute the following commands:

- `dig www.google.com @10.230.3.84`
- `dig iitdh.ac.in @10.230.3.84`

which means that the `client` is forwarding the DNS requests to the `intermediary1`, which does not resolve but only forwards the request to `intermediary2`, which in turn requests the `DNS resolver` to resolve the domains. Wireshark is executed on the `client`, `intermediary1`, and `intermediary2` nodes to capture the packet traces, which are saved as `Part_1_client_trace.pcapng`, `Part_1_inter1_trace.pcapng`, and `Part_1_inter2_trace.pcapng`, respectively. Answer the following questions using these trace files.

Q1. [5 marks] State the IP addresses of all nodes involved along the DNS resolution path.

Ans.
Client: 10.230.3.77
Intermediary 1 (Inter#1): 10.230.3.84
Intermediary 2 (Inter#2): 10.230.3.93
Public Resolver: 8.8.8.8 and 1.1.1.1

Q2. [3 marks] List the MAC addresses of the `client`, `intermediary1`, and `intermediary2` nodes.

Ans.
Client: d8:5e:d3:54:2f:1c
Intermediary 1: ac:1f:6b:87:49:d2
Intermediary 2: 3c:ec:ef:a2:e6:1e

Q3. [2 marks] What are the resolved IP addresses for the queried domains?

Ans.
www.google.com: 142.250.205.228
iitdh.ac.in: 103.120.31.124, 14.139.150.68, and 117.205.73.165

Q4. [2 marks] From the client's perspective, what is each domain's total DNS resolution time?

Ans.
www.google.com: 17.3775 - 17.3360 = 0.0415 sec (~42 msec)

iitdh.ac.in: 26.7883 - 26.5273 = 0.261 sec (~261msec)

Q5. [6 marks] For each of the two domains, identify the source and destination port numbers used in the DNS resolution from the client to the DNS resolver.

Ans.

	www.google.com		iitdh.ac.in	
Connection	**Source port**	**Destination Port**	**Source port**	**Destination Port**
Client -> Inter#1	54538	53	47536	53
Inter#1 -> Inter#2	44259	53	51564	53
Inter#2 -> DNS resolver	54919	53	51887	53

Q6. [1 mark] Given the destination port number observed in the DNS request from client to the resolver, what can you infer about the nature of the DNS message – was it transmitted in plaintext or was it encrypted?

Ans. Plaintext

Q7. [1 mark] Which Transport layer protocol is used for DNS queries and responses in this scenario?

Ans. UDP

Q8. [3 marks] Are the DNS response sizes for both domains significantly different from the client's end? Explain why.

Ans.
Response size for www.google.com is 59 bytes
Response size for iitdh.ac.in is 88 bytes
Because of the number of A records returned in the response, the domain iitdh.ac.in has three A records in its Answer field.

Q9. [2 marks] Investigate the difference in DNS query lengths observed at each hop. You observe the following DNS query sizes for each domain.

www.google.com	
Hop	**DNS Query Length**
Client → Inter#1	55 bytes
Inter#1 → Inter#2	43 bytes
Inter#2 → 8.8.8.8	43 bytes

iitdh.ac.in	
Hop	**DNS Query Length**
Client → Inter#1	52 bytes
Inter#1 → Inter#2	40 bytes
Inter#2 → 1.1.1.1	40 bytes

What are the additional bytes in the client-originated DNS queries compared to intermediary queries?

Ans. The additional bytes are for the Option: Cookie
Option: COOKIE
Option Code: COOKIE (10)
Option Length: 8
Option Data: 5f725aa0ef3e8284
Client Cookie: 5f725aa0ef3e8284
Server Cookie: <MISSING>

Part 2 [9 marks]: HTTP

`Part_2_Retriving_Long_Document.pcapng` was captured at a client (with IP Address 10.230.3.68) while accessing `http://www.textfiles.com/etext/AUTHORS/SHAKESPEARE/shakespeare-macbeth-46.txt`. Answer the following questions based on this packet capture.

Q10. [2 Marks] List the number of `GET` request(s) sent by the client browser. State the response and the status code for the `GET` request.

Ans. Two `GET` Requests. The response and status code for each `GET` request is `200 OK`.

Q11. [1 Mark] What is the destination IP address for the requested webpage to retrieve the document?

Ans. 208.86.224.90

Q12. [1 Mark] What is the total size of the .txt file requested by the client from the web server?

Ans. 105202 bytes (as can be viewed from the `Content-Length` field of the HTTP Response.

Q13. [1 Mark] What is the Round Trip Time (RTT) required to complete the TCP handshake before retrieving the document?

Ans. 0.253513562 seconds

Q14. [4 Marks] How many TCP segments are retrieved for the document and list all unique segment sizes (in bytes).

Ans. [0.5 mark each]: 27 segments with sizes: 1448, 2896, 4344, 5792, 7053, 7240, 8688

Part 3 [10 Marks]: DHCP

In this scenario, a client is trying to obtain an IP address by requesting a DHCP server. Answer the following questions by referring to the `Part_3_DHCP.pcap` file

Q15. [2 marks] What is/are the transaction ID(s) in the DHCP messages?

Ans. `0x3d1d` and `0x3d1e` are the two transaction IDs

Q16. [4 marks] Fill in the blanks in the following table.

Ans.

DHCP Message	Source IP	Destination IP	Source Port	Destination Port
DHCP Discover	0.0.0.0	255.255.255.255	68	67
DHCP Offer	192.168.0.1	192.168.0.10	67	68
DHCP Request	0.0.0.0	255.255.255.255	68	67
DHCP ACK	192.168.0.1	192.168.0.10	67	68

Q17. [2 marks] What is the IP address requested by the client to the DHCP server, and in which DHCP message do you observe this?

Ans. 192.168.0.10 requested in DHCP Request message

Q18. [2 marks] Provide the rebinding and lease time set by the DHCP server?

Ans.
Rebinding time: 52 minutes 30 seconds (3150 seconds)
Lease time: 1 hour (3600 seconds)

Part 4 [6.5 Marks]: ICMP

`Part_4_ICMP_trace.pcapng` was captured by executing the following command in the terminal of a client with IP Address 10.230.3.68.

```
traceroute -I -q 5 sharetechnote.com
```

Answer the following questions based on this packet capture.

Q19. [1.5 Marks] What type(s) of ICMP messages is/are observed in packet trace?

Ans.
[0.5 mark] a) ICMP Echo Request (Type 8)
[0.5 mark] b) ICMP Time Exceeded (Type 11) — from intermediate routers
[0.5 mark] c) ICMP Echo Reply (Type 0) — from the destination to the echo request.

Q20. [1 Mark] Using the given traceroute command, how many probe(s) is/are transmitted to each hop, and what is the default number of probe(s) is/are transmitted to each hop if no such parameter is specified?

Ans.
[0.5 mark] 5 probes
[0.5 mark] Default- 3 probes

Q21. [1 Mark] How does traceroute determine that it has reached the final destination?

Ans. When it receives an ICMP Echo Reply (Type 0) from the destination IP instead of a Time Exceeded message.

Q22. [3 Marks] List any six IP addresses across the path packets take from the client to the destination host.

Ans. [0.5 mark] for each IP address:
10.230.0.1
10.240.240.1
14.139.150.65
10.255.222.33
61.246.99.85
62.115.162.62
62.115.119.90
62.115.140.222
80.239.167.103
62.115.140.225
69.195.64.105
162.144.240.23

Part 5 [9 Marks]: Ethernet and ARP

`Part_5_Ethernet_and_ARP_trace.pcapng` was captured while fetching `http://pageometry.weebly.com` on the web browser of a client with IP Address 10.230.3.68. Answer the following questions based on this packet capture.

Q23. [1 mark] What is the MAC address of the client interface from which the above webpage was requested?

Ans. e0:73:e7:0a:49:d3

Q24. [1 mark] What is the MAC address of the web server interface from which the web page was sent?

Ans. We will not be able to find it from this trace.

Q25. [2 Marks] Determine the total size (in bytes) of the Ethernet frame encapsulating the first HTTP GET request. State the client's network interface id on which this trace was captured.

Ans. `Frame 1111: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface eno1, id 0`

[1 mark] 415 bytes
[1 mark] eno1

Q26. [3 Marks] What are the target MAC and IP addresses for the ARP request initiated by the client interface? Also, state the total number of ARP requests the client interface sends.

Ans.
Target MAC address: 00:00:00:00:00:00
Target IP address: 10.230.0.1
Number of ARP requests: 1

Q27. [1 Mark] What are the sender MAC and IP addresses for the ARP reply, if observed in the trace?

Ans.
Sender MAC address: `bc:d2:95:13:e0:82`
Sender IP address: 10.230.0.1

Q28. [1 Mark] How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin for the client's request?

Ans. After 20 Bytes

Part 6 [11.5 marks]: TLS

A client establishes a TLS handshake with a server, and immediately after ending its first connection with the server, it connects with another server with the same domain name but with a different TLD. Answer the following questions considering the `Part_6_TLS_Handshake.pcapng` file.

Q29. [2 marks] What is the client and server's IP address? How many TLS handshakes are performed between the client and the server?

Ans.
[0.5 marks] Client IP: 10.9.0.2,
[0.5 marks] Server IP: 93.184.216.34
[1 mark] Two TLS handshakes

Q30. [1 mark] Which TLS version has the server agreed on to set the TLS handshake?

Ans. TLS v1.2

Q31. [2.5 marks] List the different types of TLS messages exchanged between the client and the server?

Ans. [0.5 mark each]
`ClientHello`
`ServerHello`
`Certificate, Server Key Exchange, Server Hello Done`
`Client Key Exchange, Change Cipher Spec, Finished`
`Change Cipher Spec, Finished`

Q32. [2 marks] Which TLS message type contains the server name the client is trying to make a request? And, what is the domain name is it trying to connect to?

Ans.
[1 mark] `ClientHello` message
[1 mark] Domain is `example.com`

Q33. [2 marks] List the count of all the cipher suites the client offers the server to choose from for further communication. Which cipher suite has the server agreed on for further communication?

Ans.
[1 mark] 28 cipher suites
[1 mark] Server agrees on the Cipher Suite: `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` (`0xc02f`)

Q34. [1 mark] Which Certificate Algorithm was agreed upon for the communication?

Ans. `sha256WithRSAEncryption`

Q35. [1 mark] Which handshake protocol is used in the Server Key Exchange message?

Ans. `EC Diffie-Hellman`

Part 7 [10.5 Marks]: WiFi

Use the `Part_7_Wifi_trace.pcap` trace file to answer the following questions. This trace was captured at the interface with MAC address `00:01:e3:41:bd:6e` of a WiFi Access Point.

Q36. [3 Marks] What is/are the client interface's MAC address(s)? List the tagged parameters included in its request.

Ans.
[1 Mark] `NokiaDan_3d:aa:57` (`00:16:bc:3d:aa:57`)
Tagged Parameters: [0.5 Mark each]
- Tag: SSID parameter set: martinet3
- Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
- Tag: DS Parameter set: Current Channel
- Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]

Q37. [4.5 Marks] What are the WiFi Access Point's source and destination MAC addresses that responded to the client's request? List the tagged parameters included in the Access Point's response.

Ans.
[0.5 Mark] Source address: `Siemens_41:bd:6e` (`00:01:e3:41:bd:6e`)
[0.5 Mark] Destination address: `NokiaDan_3d:aa:57` (`00:16:bc:3d:aa:57`)
[3.5 Mark] The tagged parameters included in the Access Point's response are:
- Tag: SSID parameter set: martinet3
- Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
- Tag: DS Parameter set: Current Channel: 11
- Tag: ERP Information
- Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
- Tag: Vendor Specific: Broadcom
- Tag: Vendor Specific: Microsoft Corp.: WPA Information Element

Q38. [1 Mark] Does the host want the authentication to require a key or be open?

Ans. Open System

Q39. [2 Marks] Do you see an `AUTHENTICATION` and `DISASSOCIATION` to/from the `Siemens_41:bd:6e` AP in the trace?

Ans.
[1 mark] Yes
[1 mark] No

Part 8 [4 Marks]: NS-3 Questions

Q40. [1.5 Marks] List any three tracing mechanisms used in NS3 to log the packets in transmission.

Ans. [0.5 mark each]: Wireshark, Flow Monitor, NetAnim, Trace metrics

Q41. [2.5 Marks] What are the key abstraction objects/components in NS3?

Ans. [0.5 mark each] Nodes, Application, Channels, Network Devices, Topology helpers