COMP9121 Main

● Graded

Student

Lihang Shen

Total Points

71.5 / 100 pts

Question 1

Question 1.1

3 / 3 pts

✔ **+ 3 pts** Correct

− 1 pt Wrong 1

− 1 pt Wrong 2

− 1 pt Wrong 3

+ 0 pts All wrong

Question 2

Question 1.2

2.5 / 3 pts

✔ **+ 3 pts** Correct

✔ **− 1 pt** 0s wrong

− 1 pt 1s wrong

− 1 pt rest wrong

+ 0 pts all wrong

💬 **+ 0.5 pts** Point adjustment

Question 3

Question 1.3

2 / 3 pts

✔ **+ 3 pts** Correct

✔ **− 1 pt** not 16 bits

+ 0 pts all wrong

Question 4

Question 1.4

3 / 3 pts

✔ **+ 3 pts** Correct

+ 1 pt not 32 bits, but 20 1s, or 12 0s

+ 1 pt Wrong answer, but 1s before 0s, and 32 bits

+ 0 pts Wrong answer

Question 5

Question 1.5

3 / 3 pts

✔ **+ 3 pts** Correct

+ 2 pts 1 mistake

+ 1 pt two mistakes

+ 0 pts three or more mistakes or blank

Question 6

Question 2.1

1.5 / 3 pts

+ 3 pts X_2 and X_1 (or X_1 and X_2)

+ 0 pts No answer of wrong answer

+ 1.5 pts X_1 is destination MAC address

✔ **+ 1.5 pts** X_2 is source MAC address

Question 7

Question 2.2

0 / 3 pts

+ 3 pts $Y_1$and Y_2 (or $Y_2$and Y_1)

✔ **+ 0 pts** No answer of wrong answer

+ 1.5 pts Y_1 is the source IP address

+ 1.5 pts Y_2 is the destination IP address

Question 8

Question 2.3

1.5 / 3 pts

+ 1.5 pts X_3 is CRC

✔ **+ 1.5 pts** Error detection

+ 0 pts No answer of wrong answer

Question 9

Question 2.4

0 / 3 pts

+ 2 pts Sequence number and ACK number. (ACK and sequence number is also regarded as correct)

+ 1 pt For reliable data transfer/detect packet loss.

✔ **+ 0 pts** No answer of wrong answer

+ 1 pt Z_3 is sequence number

+ 1 pt Z_4 is ACK number

Question 10

Question 2.5

0 / 3 pts

+ 1.5 pts A. flow control/not overflowing receiver buffer

+ 1.5 pts B. prevent packets transmitted infinitely in a loop.
OR Each time it is forwarded, the value is reduced by one and it is dropped when TTL is zero

✔ **+ 0 pts** No answer of wrong answer

Question 11

Question 3

15 / 16 pts

– 0 pts Correct

✔ **– 1 pt** Final answer is 52/53/53.63, rounding error.

– 2 pts 3N calculation incorrect.

– 3 pts Efficiency calculation incorrect.

– 3 pts Transmission delay calculation incorrect.

– 3 pts Propagation delay calculation incorrect.

– 4 pts Longest distance calculation incorrect.

– 16 pts No answer has been provided.

Question 12

Question 4.1

1.5 / 3 pts

– 0 pts Correct

– 0.5 pts The source IP address is incorrect.

✔ **– 0.5 pts** The destination IP address is incorrect.

– 0.5 pts The source MAC address is incorrect.

✔ **– 0.5 pts** The destination MAC address is incorrect.

– 0.5 pts The source port number is incorrect.

✔ **– 0.5 pts** The destination port number is incorrect.

– 3 pts No answer has been provided.

Question 13

Question 4.2

1.5 / 3 pts

– **0 pts** Correct

– **0.5 pts** The source IP address is incorrect.

✔ – **0.5 pts** The destination IP address is incorrect.

– **0.5 pts** The source MAC address is incorrect.

✔ – **0.5 pts** The destination MAC address is incorrect.

– **0.5 pts** The source port number is incorrect.

✔ – **0.5 pts** The destination port number is incorrect.

– **3 pts** No answer has been provided.

Question 14

Question 4.3

1 / 3 pts

– **0 pts** Correct

– **0.5 pts** The source IP address is incorrect.

✔ – **0.5 pts** The destination IP address is incorrect.

✔ – **0.5 pts** The source MAC address is incorrect.

✔ – **0.5 pts** The destination MAC address is incorrect.

– **0.5 pts** The source port number is incorrect.

✔ – **0.5 pts** The destination port number is incorrect.

– **3 pts** No answer has been provided.

– **3 pts** The answer provided is incorrect.

Question 15

Question 4.4

1 / 3 pts

– **0 pts** Correct

– **0.5 pts** The source IP address is incorrect.

✔ – **0.5 pts** The destination IP address is incorrect.

✔ – **0.5 pts** The source MAC address is incorrect.

✔ – **0.5 pts** The destination MAC address is incorrect.

– **0.5 pts** The source port number is incorrect.

✔ – **0.5 pts** The destination port number is incorrect.

– **3 pts** No answer has been provided.

– **3 pts** The provided answer is incorrect or fails to address the question appropriately.

Question 16

Question 4.5

2 / 3 pts

– **0 pts** Correct

– **1 pt** The source IP address is incorrect.

– **1 pt** The destination IP address is incorrect.

– **1 pt** The source port number is incorrect.

– **1 pt** The destination port number is incorrect.

✔ – **1 pt** The question did not require a MAC address, but one was provided.

– **3 pts** No answer has been provided.

– **3 pts** The provided answer is incorrect or fails to address the question appropriately.

Question 17

Question 4.6

1 / 3 pts

– **0 pts** Correct

– **1 pt** The source IP address is incorrect.

– **1 pt** The destination IP address is incorrect.

– **1 pt** The source port number is incorrect.

✔ – **1 pt** The destination port number is incorrect.

✔ – **1 pt** The question did not require a MAC address, but one was provided.

– **3 pts** No answer has been provided.

– **3 pts** The provided answer is incorrect and fails to address the question appropriately

Question 18

Question 5.1

10 / 10 pts

+ **2 pts** 1 row correct

+ **4 pts** 2 rows correct

+ **6 pts** 3 rows correct

+ **8 pts** 4 rows correct

✔ + **10 pts** 5 rows correct

+ **0 pts** 0 rows correct

Question 19

Question 5.2

10 / 10 pts

✔ + **2 pts** correct round trip: x-local

✔ + **2 pts** correct round trip: local-root

✔ + **2 pts** correct round trip: local-TLD

✔ + **2 pts** correct round trip: local-authoritive

✔ + **2 pts** correct trip order

+ **0 pts** 0 correct round trip

− **1 pt** IP resolve time is needed (correct but not explictly writen).

− **2 pts** wrong number of RTTs

+ **0 pts** wrong center at x

Question 20

Question 6.1

4 / 4 pts

✔ + **4 pts** Correct

+ **2 pts** Mostly correct

+ **0 pts** Incorrect or no answer

Question 21

Question 6.2

4 / 4 pts

✔ + **2 pts** (a) Bob can use his private key to decrypt session key Ks.

✔ + **1 pt** (b) Ks can decrypt the message.

✔ + **1 pt** (c) Trudy cannot decrypt the session key Ks and cannot decrypt the message.

+ **0 pts** Incorrect or no answer.

Question 22

Question 6.3

4 / 4 pts

✔ **+ 4 pts** Correct

+ 2 pts Mostly Correct

+ 0 pts Incorrect or no answer

Question 23

Question 6.4

0 / 4 pts

+ 4 pts Correct

+ 2 pts Mostly Correct

✔ **+ 0 pts** Incorrect or no answer

Question 24

Additional space

0 / 0 pts

✔ **– 0 pts** Correct

THE UNIVERSITY OF SYDNEY

Room Number ISL

Seat Number 11

Student Number 490351481

ANONYMOUSLY MARKED

(Please do not write your name on this exam paper)

CONFIDENTIAL EXAM PAPER

This paper is not to be removed from the exam venue

Computer Science

EXAMINATION

Semester 2 - Final, 2024

COMP9121 Design of Networks and Distributed Systems

EXAM WRITING TIME: 2 hours

READING TIME: 10 minutes

EXAM CONDITIONS:
This is a CLOSED book exam - no material permitted

MATERIALS PERMITTED IN THE EXAM VENUE:
(No electronic aids are permitted e.g. laptops, phones)

Calculator - non-programmable

MATERIALS TO BE SUPPLIED TO STUDENTS:
Blank scratch paper (3 sheets)

INSTRUCTIONS TO STUDENTS:
There are six questions. For question 1, only the final result is required. For questions 2 to 6, please show all steps of your work.

If you require additional space, please use the last two pages of the exam paper, and clearly specify which question you are answering.

Please tick the box to confirm that your examination paper is complete. ☑

For Examiner Use Only

Q	Mark
1	
2	
3	
4	
5	
6	

Total _____

88

1. Binary numbers. (15 points, 3 points each)
In this question, only the final result is required. If your final answer has more than 8 bits, please separate each 8-bit with a comma ",".

(1) Convert the IPv4 address 129.78.46.135 into binary form.

1000 0001 . 0100 1110 . 0010 1110 . 1000 0111

(2) Convert the IPv6 address ::ffff:814e:2e87 into binary form.

0000 0000 0000 0000 : 0000 0000 0000 0000 : 1111 1111 1111 1111 : 1000 0001 0100 1110 :

0010 1110 1000 0111

(3) Convert the port number 1001 (one thousand and one) into binary form.

1111 1010 01

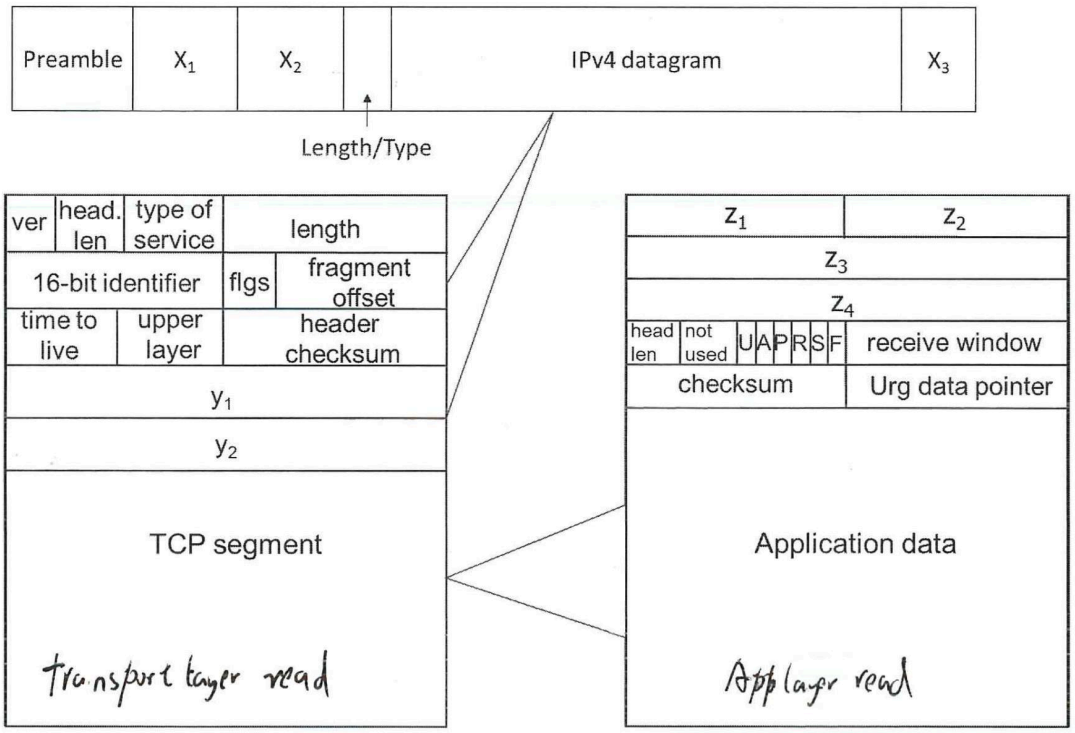
(4) Convert the subnet mask 255.255.240.0 into binary form.

1111 1111 . 1111 1111 . 1111 0000 . 00000000

(5) Convert the MAC address 00:15:5D:67:6E:07 into binary form.

0000 0000 : 0001 0101 : 0101 1101 : 0110 0111 : 0110 1110 : 0000 0111

2. Packet Header. (15 points, 3 points each). The figure below shows a TCP segment encapsulated in an IPv4 datagram encapsulated in an Ethernet frame. Most of the header fields are labeled but some fields are labelled as X, Y, or Z.



(1) Where are the source MAC address and destination MAC address?

~~X_2~~ represent MAC address (should inside network layer)

(2) Where are the source IP address and destination IP address?

~~X_1 other X~~ represent those IP address (should inside network layer)

X_1

(3) What is the field X_3? What is it used for?

It's the Error field. Used to check whether there is an Error during transfer such as bit flip.

(4) What are the fields Z_3 and Z_4? What are they used for?

It's the source port/socket and dest port/socket. Used for application to communicate with application. (Inside App layer)

I don't remember we call it port or socket in the lecture, but it's just used to receive TCP for each Applications.

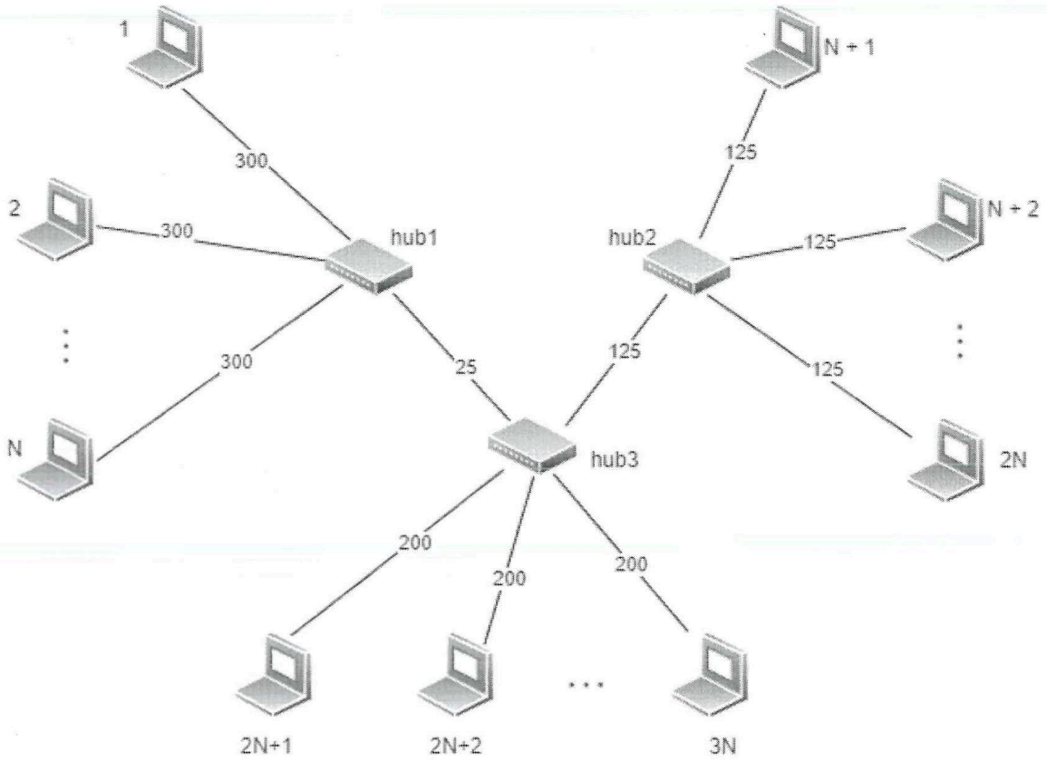
(5) What are the following fields used for? (A) receive window. (B) time to live.

(A) Indicate how many segment do we received with specific sequence number

(B) time to live (TTL) means the existing time of this datagram. (count when it was generated by sender)

3. Link Layer. (16 points)

3N computers have been connected in a network as illustrated. N computers are on the left side, connected to hub 1. Another N computers are on the right side, connected to hub 2, and N computers are on the bottom side, connected to hub 3. Hub 1 is connected to hub 3, and hub 3 is connected to hub 2. The length of each link is measured in meters, labelled in the figure. Each computer generates 1000 packets per second, with each packet being 500 bytes. The maximum link rate is 1 Gbps, and the propagation speed through the medium is 2×10^8 meters per second.



What is the maximum number of nodes supported in the network if CSMA-CD is used on the shared medium? Hint: $\frac{1}{1+5\frac{t_{prop}}{t_{trans}}}$

$t_{prop} = \frac{\text{max length}}{\text{prop speed}} = \frac{600\,m}{2 \times 10^8\,m/s} = 3 \times 10^{-6}$

$t_{trans} = \frac{500 \times 8\ bits}{1 \times 10^9\ bps} = 4 \times 10^{-6}\ s$

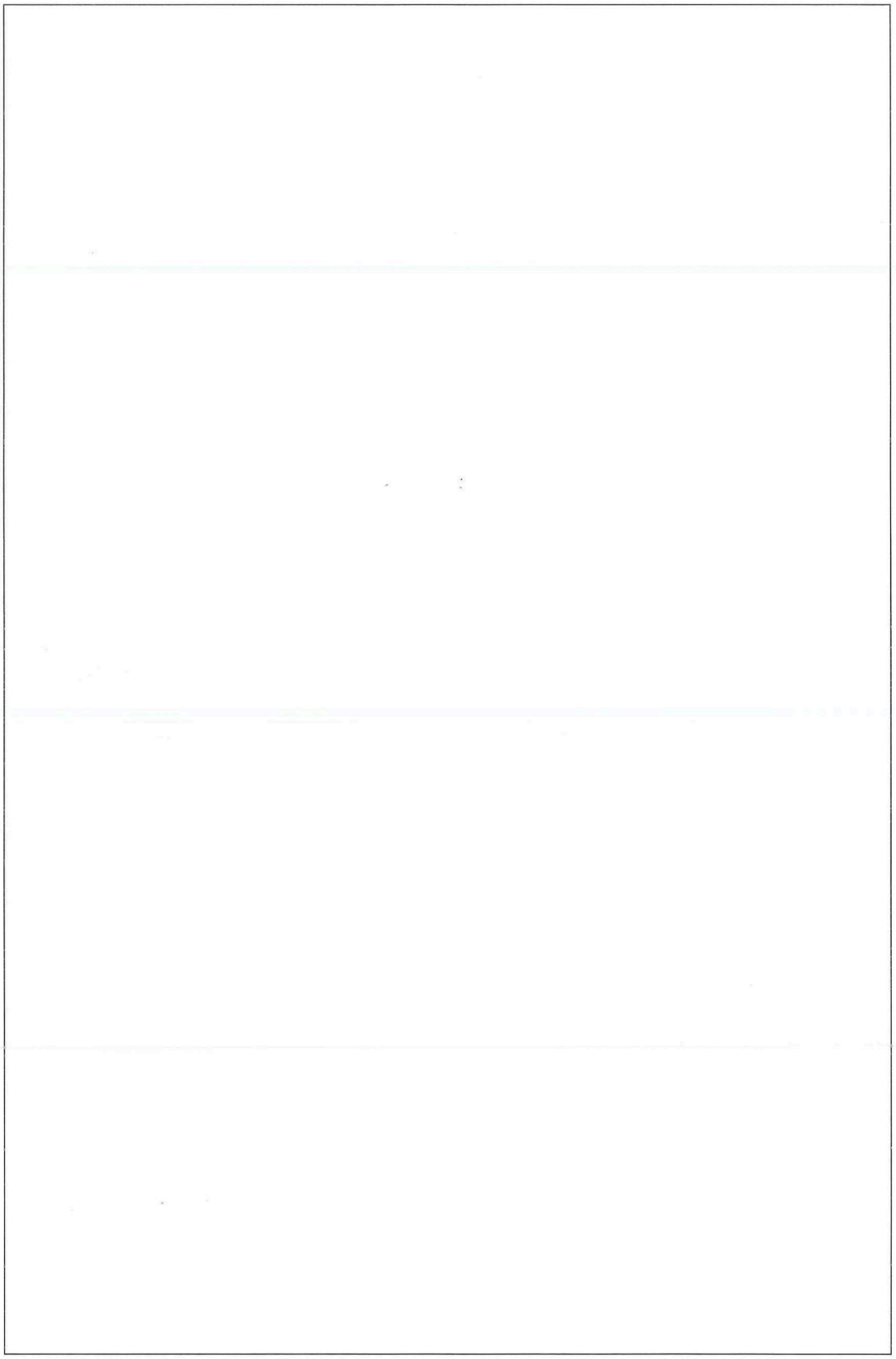
$\text{Efficiency} = \frac{1}{1+5\frac{t_{prop}}{t_{trans}}} = \frac{1}{1+5\frac{3 \times 10^{-6}}{4 \times 10^{-6}}} = \frac{4}{19}$

$$\text{Max \# of Nodes} = \frac{\text{Efficiency} \times \text{chanel rate}}{\text{Computer throughput}}$$

$$= \frac{\frac{4}{19} \times 10^9}{1000 \times 500 \times 8} = 52.6 \approx 52$$

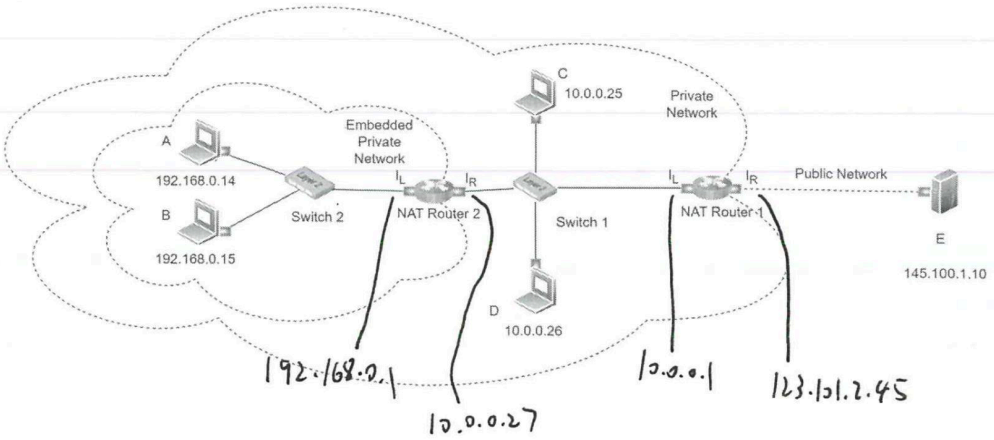
So the max computer this network can afford is

52



4. Network Layer (18 points, 3 points each)

NAT routers can be used in an embedded way. The figure below shows a network consisting of a public network, a private network, and an embedded private network located within the private network. A, B, C, D, and E are hosts; Switch 1 and Switch 2 are two switches; NAT Router 1 and NAT Router 2 are two NAT routers. The embedded private network can be regarded as the private network's private network. Both NAT routers are standard: They will generate the NAT translation table and change the IP address and port number when there is a packet passing the router. There is no NAT router in the public network. The IP addresses of the hosts are labelled in the figure.



NAT Router 1 serves as the gateway between the private network and the public network, with IP addresses 10.0.0.1 (private IP, left interface) and 123.101.2.45 (public IP, right interface). From the public network's view, all the packets in the private network use only one IP address: 123.101.2.45.

NAT Router 2 serves as the gateway between the embedded private network and the private network, with IP addresses 192.168.0.1 (embedded private IP, left interface) and 10.0.0.27 (private IP, right interface). From the private network's view, all the packets in the embedded private network use only one IP address: 10.0.0.27.

The MAC addresses of the interfaces are as follows
Host A: AA-11-11-11-11-AA.
Host B: BB-11-11-11-11-BB.
Host C: CC-11-11-11-11-CC,
Host D: DD-11-11-11-11-DD,
Host E: EE-11-11-11-11-EE.

App1 : 10001

NAT Router 1 (left interface): EE-11-11-11-11-11.
NAT Router 1 (right interface): EE-11-11-11-11-22.
NAT Router 2 (left interface): EE-11-11-11-11-33.
NAT Router 2 (right interface): EE-11-11-11-11-44.
Assume application 1 is running on port 10001 on all hosts A, B, C, and D. Application 1 in "A" sends a packet to server "E" (145.100.1.10, 80). It is successfully delivered to E.

88

The NAT tables for both NAT Router 1 and NAT Router 2 have been already created.

Router 1 NAT Table	
Private Network (left)	Public Network (right)
10.0.0.25, 10001	123.101.2.45, 10001
10.0.0.26, 10001	123.101.2.45, 10002
10.0.0.27, 10001	123.101.2.45, 10003
10.0.0.27, 10002	123.101.2.45, 10004

Router 2 NAT Table	
Embedded Private Network (left)	Private Network (right)
192.168.0.14, 10001	10.0.0.27, 10001
192.168.0.15, 10001	10.0.0.27, 10002

(1) When this packet (mentioned above, sent from A to E) is being delivered on the hop A—Switch 2, specify the source IP address, destination IP address, source MAC address, destination MAC address, source port number, and destination port number of the packet.

	IP	MAC	Port
S	192.168.0.14	AA:::::AA	10001
D	192.168.0.1	EE:::::EE	1000

(2) When this packet is being delivered on the hop Switch 2—NAT Router 2, specify the source IP address, destination IP address, source MAC address, destination MAC address, source port number, and destination port number of the packet.

	IP	MAC	Port
S	192.168.0.14	AA:::::AA	10001
D	192.168.0.1	EE:::::EE	1000

(3) When this packet is being delivered on the hop NAT Router 2—Switch 1, specify the source IP address, destination IP address, source MAC address, destination MAC address, source port number, and destination port number of the packet.

	IP	MAC	Port
S	10.0.0.27	AA:::::::AA	1000
D	10.0.0.1	EE:::::::EE	1000

(4) When this packet is being delivered on the hop Switch 1—NAT Router 1, specify the source IP address, destination IP address, source MAC address, destination MAC address, source port number, and destination port number of the packet.

	IP	MAC	Port
S	10.0.0.27	AA:::::::AA	1000
D	10.0.0.1	EE:::::::EE	1000

(5) When this packet is being delivered on the path from NAT Router 1 to E, specify the source IP address, destination IP address, source port number, and destination port number of the packet.

	IP	MAC	Port
S	123.101.245	AA:::::::AA	10003
D	145.100.1.10	EE:::::::EE	80

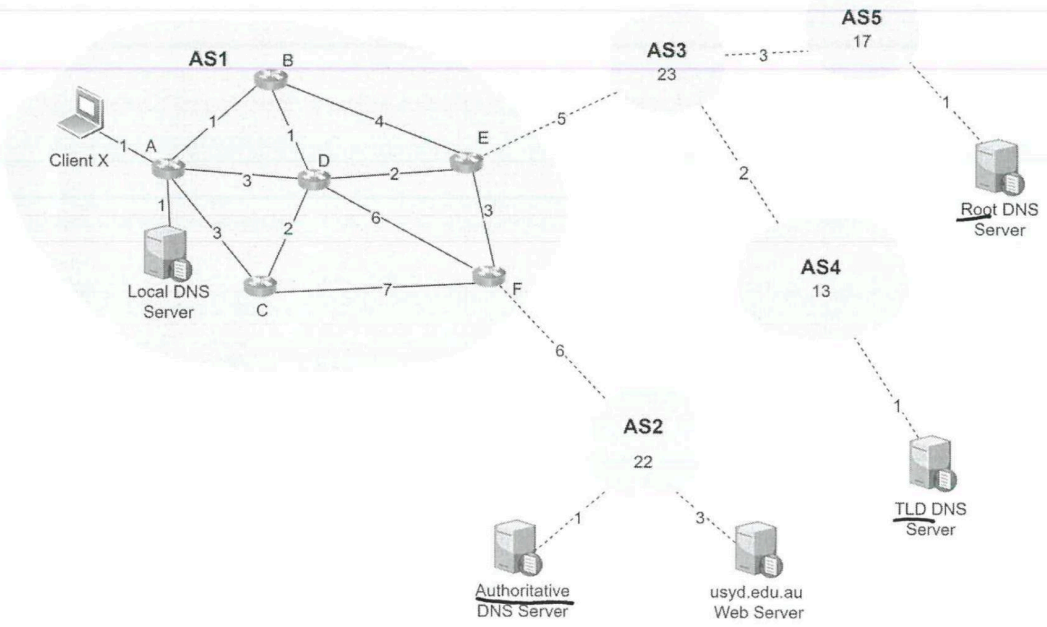
(6) When E sends a packet back to Application A of host C, specify the source IP address, destination IP address, source port number, and destination port number of the packet (when the packet just leaves E).

	IP	MAC	Port
~~S~~	145.100.1.10	EEIIIIIIEE	'80'
D	123.101.2045	AAIIIIIIAA	10003

5. Distance vector algorithm, Inter-AS and DNS. (20 points, 10 points each)

Consider the network topology below, consisting of multiple ASes. The Root DNS Server is connected to AS5; the TLD DNS Server is connected to AS4; the Authoritative DNS Server is connected to AS2; and the Web Server is connected to AS2. The one-way delay through each link inside AS1, is labeled in the figure in ms. The labeled delays are used as link costs to calculate shortest path within AS1. There is 1 ms delay from Client X to A and from local DNS to A. BGP is used among the ASes. The following inter-AS paths are all allowed: AS1-AS3-AS5; AS1-AS3-AS4; and AS1-AS2.

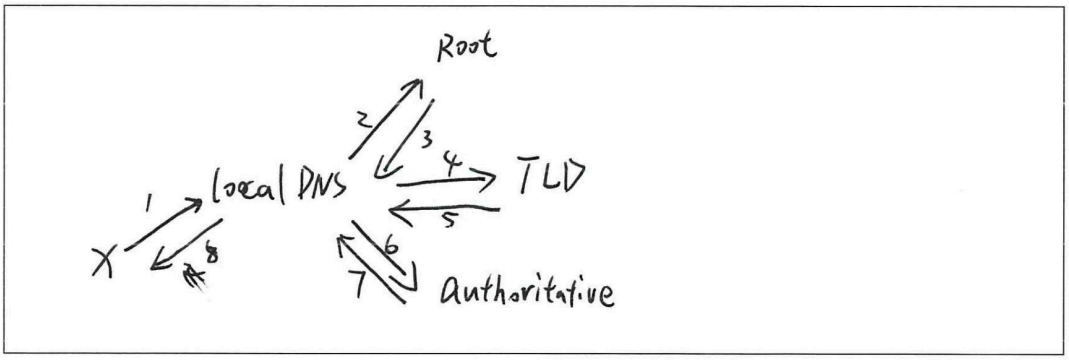
Routers E and F are gateway routers. The delays outside AS1 are also labeled in the figure. The number on the dashed line shows the delay (in ms) on that link, and the number in each AS shows the delay passing through the AS. For example, the one-way delay from Router E to the Root DNS Server is 5+23+3+17+1=49 ms.



(1) Use the distance vector algorithm to find the shortest distances from all routers to router A within AS1 by filling in the table below (assume that exchanges of routing information and routing table updates are synchronous). The table allows up to 12 iterations, but you can stop whenever the algorithm converges.

	B	C	D	E	F
Initial	$-1,\infty$	$-1,\infty$	$-1,\infty$	$-1,\infty$	$-1,\infty$
1	A, 1	A, 3	A, 3	-1, ∞	-1, ∞
2	A, 1	A, 3	B, 2	D, 5	D, 9
3	A, 1	A, 3	B, 2	D, 4	D, 8
4	A, 1	A, 3	B, 2	D, 4	E, 7
5	A, 1	A, 3	B, 2	D, 4	E, 7
6					
7					
8					
9					
10					
11					
12					

(2) Client X, connected to Router A, wants to resolve the IP address of usyd.edu.au. The local DNS server, which serves Client X, is also connected to Router A. The one-way delay between Client X and Router A is 1 ms; and the one-way delay between the local DNS server and Router A is also 1 ms. The IP address of usyd.edu.au is not cached on Client X, but at the authoritative DNS. Assume that the DNS query follows the Iterative approach, so that Root, TLD, and Authoritative DNS servers are all visited. How long, in total, will it take for Client X to successfully resolve the IP address of usyd.edu.au?



① X → A → local : 1+1 = 2 ms
(1) (1)

② Local → A → B → D → E → AS3 → AS5 → Root :
1 + 1 + 1 + 2 + 5 + 23 + 3 + 17 + 1 = 54 ms

③ same as ② 54 ms

④ Local → A → B → D → E → AS3 → AS4 → TLD
1 + 1 + 1 + 2 + 5 + 23 + 2 + 13 + 1 = 49 ms

⑤ same as ④ 49 ms

⑥ Local → A → B → D → E → F → AS2 → Authoritive
1 + 1 + 1 + 2 + 3 + 6 + 22 + 1 = 37 ms

⑦ same as ⑥ 37 ms

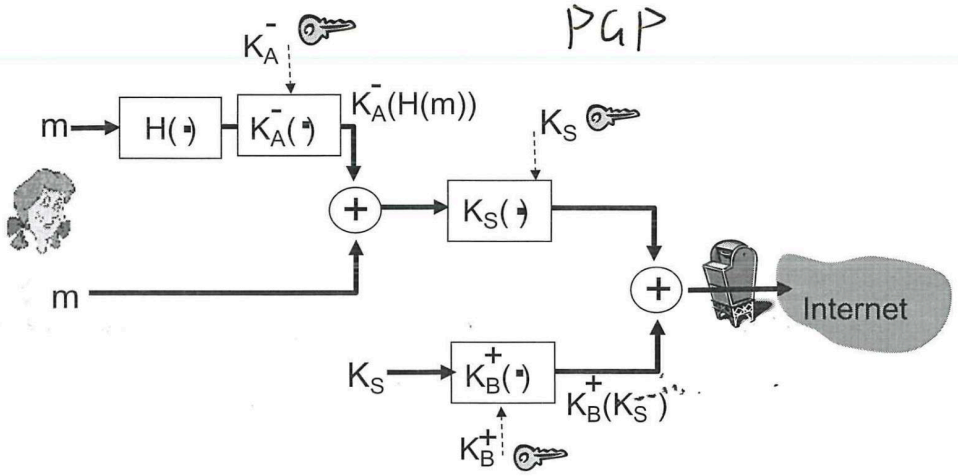
⑧ same as ① 2 ms

In total we have

2 x 2 + 54 x 2 + 49 x 2 + 37 x 2 = 284 ms

6. Security. (16 points, 4 points each)

In the following figure, Alice sends a message to Bob using symmetric key cryptography, public key cryptography, a cryptographic hash function, and a digital signature to provide secrecy, sender authentication, and message integrity. In this example, m is the message to be sent; $H(\cdot)$ is a hash function known by Alice and Bob; $K_A^-(\cdot)$ is Alice's private key; $K_S(\cdot)$ is a symmetric session key selected by Alice; $K_B^+(\cdot)$ is Bob's public key.



(1) When Bob receives the message, how does Bob know that Alice, rather than Trudy, sends the message?

Alice uses her secret key K_A^- to encrypt the message digest. It can be used as a signature of Alice, and Trudy does not have K_A^- so she cannot have that signature

(2) How does Alice ensure that Bob knows the meaning of the message, but Trudy cannot, even if she eavesdrops on the message?

Alice uses a symmetric key K_S to encrypt the message m. And she also use Bob's public key K_B^+ to encrypt the symmetric key. Without Bob's private key K_B^-, Trudy need to take huge amount of time (namely impossible) to decrypt $K_B^+(K_S)$. Hence Trudy cannot use K_S to understand $K_S(\cdot)$ (which include signing and message)

(3) If Trudy alters a part of the message, how can Bob detect it?

Bob can compare $K_A^+(K_A^-(H(m)))$ and $H(m)$. (if equal, then no change; not equal then changed)

Bob will get $K_A^-(H(m))$ after use K_S

Bob will also get m after use K_S

• Key idea is hash function is impossible to traverse back, that's you cannot know $H(m)$ when you only know m. Apparently Trudy does not know the hash function H, so she can not change $H(m)$ correspondingly

(4) The figure above is still vulnerable to playback attack. Find a way to address this issue.

Use goverment or other authoritive organization provided signature is a good choice. Rather than just use K_A^-

Additional Space

Additional Space

END OF EXAMINATION