

network hw4  
dr. arshadi

aeirya mohammadi  
97103779

### سوالات نظری

1]

a)

Dest Addr Range				Link Interface
11100000	00xxxxxx	xxxxxxx	xxxxxxx	0
11100000	01000000	xxxxxxx	xxxxxxx	1
1110000x	xxxxxxx	xxxxxxx	xxxxxxx	2
11100001	1xxxxxxx	xxxxxxx	xxxxxxx	3
otherwise				3

b)

Address				Link Interface
11001000	10010001	01010001	01010101	3
11100001	01000000	11000011	00111100	1
11100001	10000000	00010001	01110111	3

2]

Subnet+Host				[Sub]network
<u>10000000</u>	<u>01110111</u>	<u>00101000</u>	0000000	All
<u>10000000</u>	<u>01110111</u>	<u>00101000</u>	0000000	A
<u>10000000</u>	<u>01110111</u>	<u>00101001</u>	0000000	B
<u>10000000</u>	<u>01110111</u>	<u>00101001</u>	<u>1000000</u>	C
<u>10000000</u>	<u>01110111</u>	<u>00101001</u>	<u>1111100</u>	D
<u>10000000</u>	<u>01110111</u>	<u>00101001</u>	<u>1111110</u>	E
Net ID				Sub-network
128.119.40.0/24				A
128.119.41.0/25				B
128.119.41.127/26				C
128.119.41.252/31				D
128.119.41.254/31				E

3]

a) the packet splits into  $\text{ceil}[(14000-20)/(3300-20)] = 5$  parts, each of maximum size 3300 which are small enough to be also passed by the second router without fragmentation.

total payload:  $14000 - 20 = 13980$

# of parts =  $\text{ceil}(13980/3280) = 5$

last frag size =  $13980 - 3280 * 4 + 20 = 860 + 20$  (overhead) = 880

4 fragment of size 3300, 1 of size 880

5 fragments exiting router 2

b) the first router splits the packet to packets of size 4480 (plus 20 overhead of header), making  $\text{ceil}((14000-20)/4500) = 4$  packets of the following sizes:

last datagram fragment size =  $14000 - 20 - 3*(4500-20) + 20 = 560$

3 of size 4500, 1 of size 560

the former 3 will be dividend again at the router two. into fragments of following size:

packet 1 = 3300  
 packet 2 = (4500 - 20) - (3300 - 20) + 20 = 1220

then the packets exiting router 2 will be:  
 1 of size 560, 3 of size 3300, 3 of size 1220  
 adding up to 7

4]

350 - 20 (header) = 330 Bytes for payload  
 nearest number divisible by 8 -> 328

#. of fragments = 900 / 328 = 2.74 -> 3

last frag size = 900 - 2\*328 + 20 = 244 + 20

part 1 offset = 328/8 = 41

frag #.	1	2	3
length	348	348	264
frag flag	1	1	0
offset	0	41	82

5]

192.168.1.192/28 <-> 11111111 11111111 11111111 11110000 (subnet mask)

NAT translation table

WAN side	LAN side
129.119.112.235: 5010	192.168.1.192: 3000
129.119.112.235: 5011	192.168.1.192: 3001
129.119.112.235: 5020	192.168.1.193: 3000
129.119.112.235: 5021	192.168.1.193: 3001
129.119.112.235: 5030	192.168.1.194: 4000
129.119.112.235: 5031	192.168.1.194: 4001

a sample packet P entering the router from internet:

source ip	source port	destination ip	destination port
176.213.40.12	80	129.119.112.235	5010

P will be forwarded to host A (listening at 192.168.1.192: 3000)

6]

a) not necessarily. there's a chance the broadcast doesn't reach some nodes (and is lost). even if it does, there's always some delay and until the state is updated, packets are sent to "wrong" routers.

b) still some are lost. so the routes aren't **always** correct but most of the time they are. there's still delay.

c) the bigger the network gets there's more chance flooding causes heavy traffic and infinite looping so we can't really have such network (with no loss) but if we did, then this protocol works more correctly but still some bad routing could happen because of change of link states (change of costs/broken links) as we're broadcasting the previous change. but if the broadcast happens immediately (and without other change of network) this would be a usable protocol and there will probably be no need to rebroadcast states.

## سوالات عملی

### 1- IPv4

- 1] source ip: 192.168.43.29
- 2] TTL: 1  
protocol: UDP (17)
- 3] header len: 20 bytes  
payload len: 56-20 = 36 bytes
- 4] no, it is exactly 56 bytes (datagram size)
- 6] TTL changes (incrementally) and that's to let the packet traverse further into internet (hop one more router each time). Dest port may vary. Identification value and checksum (obviously) also differ. Other labels stay the same since all sent packets (which are of the same size and content) are supposed to reach 'sharif.ir'.
- 7] starting from 50889 and going up by one for each UDP packet sent.
- 9] protocol: ICMP (1)
- 10] no, since they are probably sent by different routers.
- 11] no, neither they share the same identification as the sent datagram nor they necessarily follow up each other numerically (though it's increasing, but not by one).

26	4.116013	8.8.4.4	192.168.43.29	DNS	85	Standard query response 0x9abf A sharif.ir A 81.31.186.54	53	57443	5744
27	4.117148	192.168.43.29	81.31.186.54	UDP	70	50888 → 33435 Len=28	50888	33435	3343
28	4.118526	192.168.43.29	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	55476	1900	1900
29	4.118787	192.168.43.1	192.168.43.29	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)	50888	33435	3343
30	4.119501	192.168.43.29	8.8.4.4	DNS	85	Standard query 0x1f38 PTR 1.43.168.192.in-addr.arpa	59337	53	53
31	4.189984	8.8.4.4	192.168.43.29	DNS	85	Standard query response 0x1f38 No such name PTR 1.43.168...	53	59337	5933
32	4.190789	192.168.43.29	81.31.186.54	UDP	70	50888 → 33436 Len=28	50888	33436	3343
33	4.192532	192.168.43.1	192.168.43.29	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)	50888	33436	3343
34	4.192736	192.168.43.29	81.31.186.54	UDP	70	50888 → 33437 Len=28	50888	33437	3343
35	4.194348	192.168.43.1	192.168.43.29	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)	50888	33437	3343
36	4.194556	192.168.43.29	81.31.186.54	UDP	70	50888 → 33438 Len=28	50888	33438	3343
37	4.525865	192.168.43.41	224.0.0.251	MDNS	439	Standard query 0x0000 PTR _airport._tcp.local, "QM" ques...	5353	5353	5353
38	4.530263	fe80::10c4:a65...	ff02::fb	MDNS	459	Standard query 0x0000 PTR _airport._tcp.local, "QM" ques...	5353	5353	5353
39	4.686270	192.168.43.29	224.0.0.251	MDNS	208	Standard query response 0x0000 TXT, cache flush NSEC, ca...	5353	5353	5353

  

Frame 27: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0

Ethernet II, Src: Apple\_42:f1:94 (3c:22:fb:42:f1:94), Dst: be:a5:8b:d0:e5:df (be:a5:8b:d0:e5:df)

Internet Protocol Version 4, Src: 192.168.43.29, Dst: 81.31.186.54

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 56

Identification: 0xc6c9 (50889)

Flags: 0x00

Fragment Offset: 0

Time to Live: 1

Protocol: UDP (17)

Header Checksum: 0xfbd0 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.43.29

*Handwritten notes:* Payload: 56 - 20 = 36 bytes

## 2- fragmentation

12] datagram length: 1500

13] “more fragments” flag

14] fragment offset being 0

15] 1500 bytes

No.	Time	Source	Destination	Protocol	Length	Info
4895	10.77.214030	192.168.43.29	81.31.215.122	TCP	60	61900 → 443 [ACK] Seq=42627 Ack=206129 Win=130800 Len=0
4896	10.78.834675	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33435 Len=2972
4897	10.78.834676	192.168.43.29	81.31.186.54	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1488, ID=c73b)
4898	10.78.834676	192.168.43.29	81.31.186.54	IPv4	54	Fragmented IP protocol (proto=UDP 17, off=2968, ID=c73b)
4899	10.78.865125	192.168.43.1	192.168.43.29	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
4900	10.78.865125	192.168.43.29	8.8.4.4	DNS	85	Standard query response 0x36c0 PTR 1.43.168.192.in-addr.arpa
4901	10.78.930213	8.8.4.4	192.168.43.29	DNS	85	Standard query response 0x36c0 No such name PTR 1.43.168.53
4902	10.78.930980	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33435 Len=2972
4903	10.78.930981	192.168.43.29	81.31.186.54	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1488, ID=c73b)
4904	10.78.930982	192.168.43.29	81.31.186.54	IPv4	54	Fragmented IP protocol (proto=UDP 17, off=2968, ID=c73b)
4905	10.78.933214	192.168.43.1	192.168.43.29	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
4906	10.78.933225	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33437 Len=2972
4907	10.78.933226	192.168.43.29	81.31.186.54	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1488, ID=c73d)
4908	10.78.933226	192.168.43.29	81.31.186.54	IPv4	54	Fragmented IP protocol (proto=UDP 17, off=2968, ID=c73d)
4909	10.78.935429	192.168.43.1	192.168.43.29	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
4910	10.78.935514	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33438 Len=2972

Frame 4896: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_42:f1:94 (3c:22:fb:42:f1:94), Dst: bea5:0b:d0:e5:df (bea5:0b:d0:e5:df)  
Internet Protocol Version 4, Src: 192.168.43.29, Dst: 81.31.186.54  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 1500  
Identification: 0xc73b (51003)  
Flags: 0x20, More fragments  
Fragment Offset: 0  
Time to Live: 1  
Protocol: UDP (17)  
Header Checksum: 0xf9fc (validation disabled)

16] fragment offset = 1480 > 0  
(which means the first byte of data is not the first byte of the assembled packet's payload)

17] fragment offset and header checksum

18] because of “more fragments” flag being equal to “not set”.

No.	Time	Source	Destination	Protocol	Length	Info
4894	10.77.213972	63.33.215.122	192.168.43.29	TLSv1.3	206	Application Data
4895	10.77.214030	192.168.43.29	63.33.215.122	TCP	60	61900 → 443 [ACK] Seq=42627 Ack=206129 Win=130800 Len=0
4896	10.78.834675	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33435 Len=2972
4897	10.78.834676	192.168.43.29	81.31.186.54	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1488, ID=c73b)
4898	10.78.834676	192.168.43.29	81.31.186.54	IPv4	54	Fragmented IP protocol (proto=UDP 17, off=2968, ID=c73b)
4899	10.78.865125	192.168.43.1	192.168.43.29	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
4900	10.78.865125	192.168.43.29	8.8.4.4	DNS	85	Standard query response 0x36c0 PTR 1.43.168.192.in-addr.arpa
4901	10.78.930213	8.8.4.4	192.168.43.29	DNS	85	Standard query response 0x36c0 No such name PTR 1.43.168.53
4902	10.78.930980	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33436 Len=2972
4903	10.78.930981	192.168.43.29	81.31.186.54	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1488, ID=c73c)
4904	10.78.930982	192.168.43.29	81.31.186.54	IPv4	54	Fragmented IP protocol (proto=UDP 17, off=2968, ID=c73c)
4905	10.78.933214	192.168.43.1	192.168.43.29	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
4906	10.78.933225	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33437 Len=2972
4907	10.78.933226	192.168.43.29	81.31.186.54	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1488, ID=c73d)
4908	10.78.933226	192.168.43.29	81.31.186.54	IPv4	54	Fragmented IP protocol (proto=UDP 17, off=2968, ID=c73d)
4909	10.78.935429	192.168.43.1	192.168.43.29	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
4910	10.78.935514	192.168.43.29	81.31.186.54	UDP	1514	51002 → 33438 Len=2972

Frame 4898: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0  
Ethernet II, Src: Apple\_42:f1:94 (3c:22:fb:42:f1:94), Dst: bea5:0b:d0:e5:df (bea5:0b:d0:e5:df)  
Internet Protocol Version 4, Src: 192.168.43.29, Dst: 81.31.186.54  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 40  
Identification: 0xc73b (51003)  
Flags: 0x20, More fragments  
Fragment Offset: 0  
Time to Live: 1  
Protocol: UDP (17)  
Header Checksum: 0xf9fc (validation disabled)



## 4- ICMP, Ping

26]

source ip: 192.168.43.29      dest ip: 81.31.186.54

27]

since ICMP is a network layer protocol and unlike TCP and UDP it doesn't need ports to functions.

28]

request:

type: 8              code: 0

field	type	code	checksum	identifier	seq. #	timestamp
size(B)	1	1	2	2	2	8

29]

reply:

type: 0              code: 0

not only the reply packet's ICMP header shares the same fields as the request but it also has the same field values (except for type). meaning that the only difference between ICMP header of a request message and its reply would be the "type" value (either 0 or 8) and checksum.

No.	Time	Source	Destination	Protocol	Length	Info
19	0.722396	192.168.43.29	81.31.186.54	ICMP		98 Echo (ping) request id=0xcfd2, seq=0/0, ttl=64 (reply in 20)
20	0.785223	81.31.186.54	192.168.43.29	ICMP		98 Echo (ping) reply id=0xcfd2, seq=0/0, ttl=51 (request in 19)
38	1.723653	192.168.43.29	81.31.186.54	ICMP		98 Echo (ping) request id=0xcfd2, seq=1/256, ttl=64 (reply in 39)
39	1.764209	81.31.186.54	192.168.43.29	ICMP		98 Echo (ping) reply id=0xcfd2, seq=1/256, ttl=51 (request in 38)
55	2.727736	192.168.43.29	81.31.186.54	ICMP		98 Echo (ping) request id=0xcfd2, seq=2/512, ttl=64 (reply in 56)
56	2.807176	81.31.186.54	192.168.43.29	ICMP		98 Echo (ping) reply id=0xcfd2, seq=2/512, ttl=51 (request in 55)
57	3.292637	192.168.43.29	8.8.8.8	ICMP		98 Echo (ping) request id=0x7a66, seq=0/0, ttl=64 (reply in 63)
63	3.368112	8.8.8.8	192.168.43.29	ICMP		98 Echo (ping) reply id=0x7a66, seq=0/0, ttl=109 (request in 57)
99	3.728941	192.168.43.29	81.31.186.54	ICMP		98 Echo (ping) request id=0xcfd2, seq=3/768, ttl=64 (reply in 100)
100	3.755007	81.31.186.54	192.168.43.29	ICMP		98 Echo (ping) reply id=0xcfd2, seq=3/768, ttl=51 (request in 99)

  

▶ Frame 55: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_42:f1:94 (3c:22:fb:42:f1:94), Dst: be:a5:8b:d0:e5:df (be:a5:8b:d0:e5:df)
▶ Internet Protocol Version 4, Src: 192.168.43.29, Dst: 81.31.186.54
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x0fcc [correct]
[Checksum Status: Good]
Identifier (BE): 53202 (0xcfd2)
Identifier (LE): 53967 (0xd2cf)
Sequence Number (BE): 2 (0x0002)
Sequence Number (LE): 512 (0x0200)
[Response frame: 56]
Timestamp from icmp data: May 24, 2021 01:23:13.527344000 +0430
[Timestamp from icmp data (relative): 0.000081000 seconds]
▶ Data (48 bytes)

  

▶ Frame 56: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
▶ Ethernet II, Src: be:a5:8b:d0:e5:df (be:a5:8b:d0:e5:df), Dst: Apple_42:f1:94 (3c:22:fb:42:f1:94)
▶ Internet Protocol Version 4, Src: 81.31.186.54, Dst: 192.168.43.29
▼ Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x17cc [correct]
[Checksum Status: Good]
Identifier (BE): 53202 (0xcfd2)
Identifier (LE): 53967 (0xd2cf)
Sequence Number (BE): 2 (0x0002)
Sequence Number (LE): 512 (0x0200)
[Request frame: 55]
[Response time: 79.440 ms]
Timestamp from icmp data: May 24, 2021 01:23:13.527344000 +0430
[Timestamp from icmp data (relative): 0.079521000 seconds]
▶ Data (48 bytes)