

به نام خدا



درس شبکه های کامپیوتری

تمرین دوم عملی : Wireshark

مدرس : دکتر موحدی

سارا سادات یونسی-۹۸۵۳۳۰۵۳

سؤال ۱

پاسخ درست ۱

B

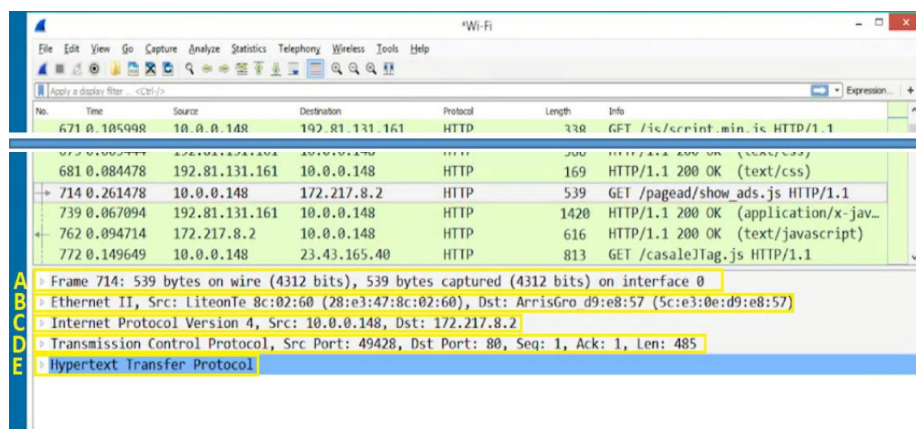
این یک فریم http است و شامل اطلاعات مبدا و مقصد می باشد. src/dest, Ethernet II

چون فریم http توسط پروتکل Ethernet در نتورک راه پیدا می کنند و این هدر شامل اطلاعاتی مانند آدرس MAC مبدا و مقصد و نوع پروتکل استفاده شده یا همان تایپ که HTTP است را نشان می دهد. در نتیجه می توان گفت که هدر اینترنت به هدر فریم HTTP در قسمت اول این شکل است.

توضیحاتی درباره ی این HEADER:

اترنت (Ethernet)، پروتکل استاندارد یا تکنولوژی است از خانواده ی شبکه های کامپیوتری که معمولا در شبکه های LAN (Local area network) و MAN (Metropolitan area network) مورد استفاده قرار می گیرد. تجهیزاتی که از طریق اترنت ارتباط برقرار می کنند داده ها را به قسمت های کوچکتری به اسم قالب (Frame) تبدیل می کنند. با طول مشخص ۶۴ تا ۱۵۱۸ هر استاندارد ممکن است ساختار خاصی را برای فریم تعریف کرده باشد. یک فریم از چندین بخش (field) تشکیل می گردد. و دارای آدرس فرستنده و گیرنده و اطلاعات خطایابی (error-checking) است، هر فیلد نیز از مجموعه ای بایت تشکیل شده است. همچنین در لایه Data link layer قرار می گیرد و شامل اطلاعات کنترلی من جمله چک سام برای اطمینان از درستی آن مجموعه هست.

گزینه A به کل هدر اشاره می کند اما ۱۴ بایت اولیه ی ما توسط B نمایش داده شد.



۱. شکل صورت سوال

سؤال ۲

پاسخ درست ۲

الف)

The image shows two screenshots of a Wireshark network traffic capture. The top screenshot displays a list of 15 packets. The bottom screenshot shows a detailed view of packet 6, which is an ICMP Echo (ping) request from Cisco_ea:b8:c1 to 192.168.123.1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_ea:b8:c1	Broadcast	ARP	64	Gratuitous ARP for 192.168.123.1 (Reply)
2	0.010948	Cisco_de:57:c1	Broadcast	ARP	64	Gratuitous ARP for 192.168.123.2 (Reply)
3	33.026340	Cisco_de:57:c1	Broadcast	ARP	64	Who has 192.168.123.1? Tell 192.168.123.2
4	33.026654	Cisco_ea:b8:c1	Cisco_de:57:c1	ARP	64	192.168.123.1 is at 00:19:06:ea:b8:c1
5	34.029970	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=0/0, ttl=255 (no response found!)
6	34.030494	Cisco_ea:b8:c1	Broadcast	ARP	64	Who has 192.168.123.2? Tell 192.168.123.1
7	34.030894	Cisco_de:57:c1	Cisco_ea:b8:c1	ARP	64	192.168.123.2 is at 00:18:73:de:57:c1
8	35.028280	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255 (reply in 9)
9	35.029230	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 8)
10	35.029743	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 11)
11	35.030037	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 10)
12	35.030526	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=3/768, ttl=255 (reply in 13)
13	35.030820	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 12)
14	35.031311	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (reply in 15)
15	35.031612	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 14)

Packet 6 Details:

- Frame 6: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
- Ethernet II, Src: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1)
 - Type: 802.1Q Virtual LAN (8x8100)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 123
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1)
 - Sender IP address: 192.168.123.1
 - Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
 - Target IP address: 192.168.123.2

Packet 6 Hex Data:

```
0000 ff ff ff ff ff ff 00 19 06 ea b8 c1 81 00 00 7b .....{
0010 08 06 00 01 08 00 06 04 00 01 00 19 06 ea b8 c1 .....
0020 c0 a8 7b 01 00 00 00 00 00 00 c0 a8 7b 02 00 00 ..{.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..{.....
```

۲. شکل ICMP request

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_ea:b8:c1	Broadcast	ARP	64	Gratuitous ARP for 192.168.123.1 (Reply)
2	0.010948	Cisco_de:57:c1	Broadcast	ARP	64	Gratuitous ARP for 192.168.123.2 (Reply)
3	0.026340	Cisco_de:57:c1	Broadcast	ARP	64	Who has 192.168.123.1? Tell 192.168.123.2
4	0.026654	Cisco_ea:b8:c1	Cisco_de:57:c1	ARP	64	192.168.123.1 is at 00:19:06:ea:b8:c1
5	34.029970	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=0/0, ttl=255 (no response found!)
6	34.030494	Cisco_ea:b8:c1	Broadcast	ARP	64	Who has 192.168.123.2? Tell 192.168.123.1
7	34.030894	Cisco_de:57:c1	Cisco_ea:b8:c1	ARP	64	192.168.123.2 is at 00:18:73:de:57:c1
8	35.028280	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255 (reply in 9)
9	35.029230	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255 (request in 8)
10	35.029743	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=2/512, ttl=255 (reply in 11)
11	35.030037	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 10)
12	35.030526	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=3/768, ttl=255 (reply in 13)
13	35.030820	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=3/768, ttl=255 (request in 12)
14	35.031311	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=4/1024, ttl=255 (reply in 15)
15	35.031612	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=4/1024, ttl=255 (request in 14)

<p>Frame 7: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)</p> <p>Ethernet II, Src: Cisco_de:57:c1 (00:18:73:de:57:c1), Dst: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1)</p> <ul style="list-style-type: none"> Destination: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1) Source: Cisco_de:57:c1 (00:18:73:de:57:c1) Type: 802.1Q Virtual LAN (0x8100) 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 123 Address Resolution Protocol (reply) <ul style="list-style-type: none"> Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: Cisco_de:57:c1 (00:18:73:de:57:c1) Sender IP address: 192.168.123.2 Target MAC address: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1) Target IP address: 192.168.123.1 	<pre> 0000 00 19 06 ea b8 c1 00 18 73 de 57 c1 81 00 e0 7b s.W....{ 0010 08 06 00 01 08 00 06 04 00 02 00 18 73 de 57 c1 s.W....{ 0020 c0 a8 7b 02 00 19 06 ea b8 c1 c0 a8 7b 01 00 00 ..{.....{... 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..{.....{... </pre>
---	--

شکل ۳: ICMP reply

Request :
Source IP address : 192.168.123.1
Destination IP address : 192.168.123.2
Source MAC address : (Cisco_ea:b8:c1)00:19:06:ea:b8:c1
Destination MAC address : Broadcast (ff:ff:ff:ff:ff:ff)

Reply :
Source IP address : 192.168.123.2
Destination IP address : 192.168.123.1
Source MAC address : (Cisco_de:57:c1)00:18:73:de:57:c1
Destination MAC address : (Cisco_ea:b8:c1) 00:19:06:ea:b8:c1

قسمت های نارنجی جداول جواب نهایی و موردنظر هستند.

برای یافتن بسته رکوئست از بین broadcast شده ها آن هایی که gratuitous نباشند و با مک ادرس سوال مطابقت داشته باشند را در نظر میگیریم و به بسته مورد نظر می رسیم برای یافتن رپیلای هم دنبال arp های رپیلای دار و آن هایی که address resolution protocol کنار آن ها رپیلای نوشته است می پردازیم که با میدا ما سینک باشد.

و سپس اطلاعات لازم را از آدرس های مک و ای پی های رکوئست و رپیلای پیدا می کنیم .

A source MAC address is the address of the device sending the packet, and you can usually see it in the packet's Ethernet header

When a device is forwarding a message to an Ethernet network, the Ethernet header includes the following: Source MAC address: This is the MAC address of the source device NIC. Destination MAC address: This is the MAC address of the destination device NIC.

ب) براساس icmp فیلتر می کنیم که در نهایت ۵ تا ICMP REQUEST خواهیم داشت.

No.	icmp	icmpv6	Source	Destination	Protocol	Length	Info
8	35.028280	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request	id=0x0001, seq=0/0, ttl=255 (no response found)
9	35.029230	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply	id=0x0001, seq=1/256, ttl=255 (reply in 9)
10	35.029743	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request	id=0x0001, seq=1/256, ttl=255 (request in 8)
11	35.030037	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply	id=0x0001, seq=2/512, ttl=255 (reply in 11)
12	35.030526	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request	id=0x0001, seq=2/512, ttl=255 (request in 10)
13	35.030820	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply	id=0x0001, seq=3/768, ttl=255 (reply in 13)
14	35.031311	192.168.123.2	192.168.123.1	ICMP	118	Echo (ping) request	id=0x0001, seq=3/768, ttl=255 (request in 12)
15	35.031612	192.168.123.1	192.168.123.2	ICMP	118	Echo (ping) reply	id=0x0001, seq=4/1024, ttl=255 (reply in 15)

سؤال ۳

پاسخ درست ۳

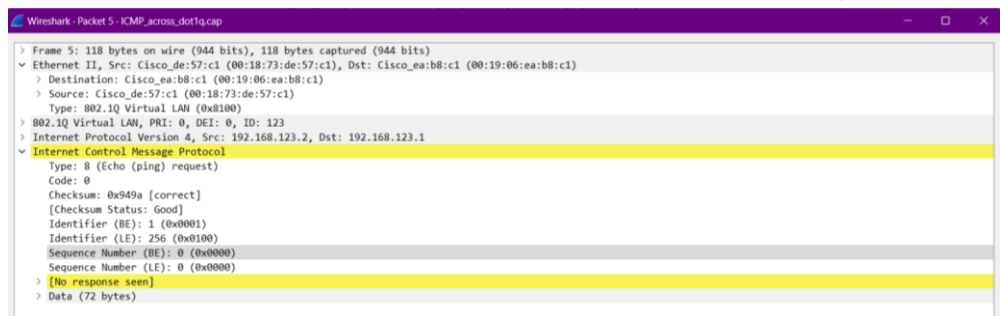
توضیحی درباره ی RTT :

زمان رفت و برگشت (RTT) در شبکه، که به عنوان زمان تأخیر رفت و برگشت (RTD) نیز شناخته می‌شود، معیاری است که برحسب میلی ثانیه (ms) مدت زمان ارسال یک بسته داده، به اضافه مدت زمان دریافت تأییدیه سیگنال آن را نشان می‌دهد. عبارت دیگر، RTT از زمانی که مرورگر درخواستی را به سرور ارسال می‌کند تا زمانی که پاسخی از سرور دریافت می‌کند، محاسبه می‌شود. عدد حاصل از این محاسبه برای برنامه‌های کاربردی وب بسیار مهم است RTT به همراه TTFB از اصلی ترین معیارهای اندازه گیری زمان بارگذاری صفحه و تأخیر شبکه محسوب می‌شود. در این بسته های ICMP نیز به همان معنای ارسال و دریافت یک بسته و یا request و reply زده شده دریافت شده را محسوب می کنیم.

فریم های مورد بررسی :

Arrival time دو بسته ی رکوئست و رپلای فریم را از هم کم می کنیم و حاصل را پیدا می کنیم یا می توانیم از عددی که

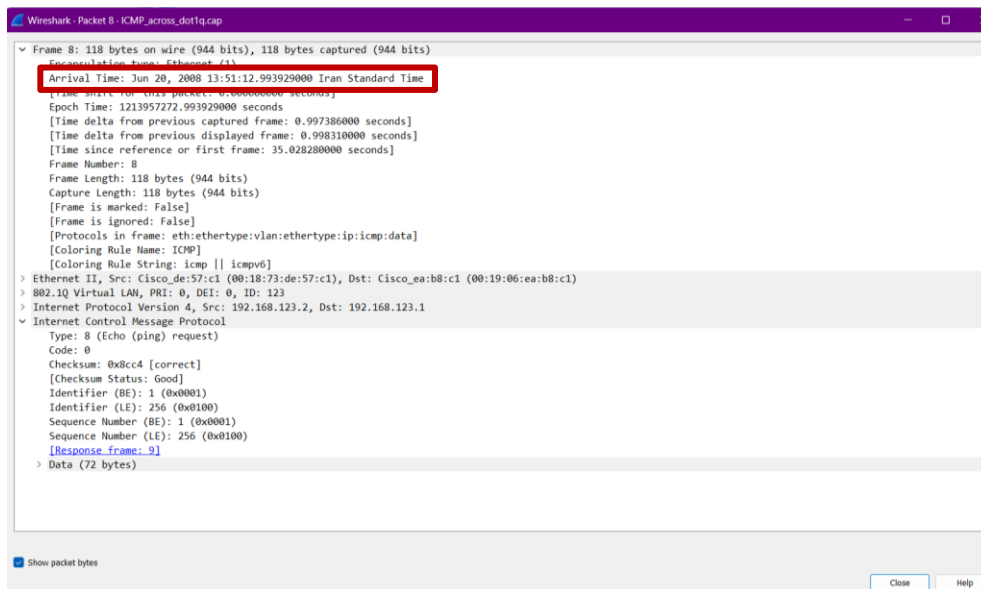
برای ریسپانس تایم گذاشته شده استفاده کنیم .. برای بسته ی ۵ محاسبه نمی شود چون فاقد رپلای است.



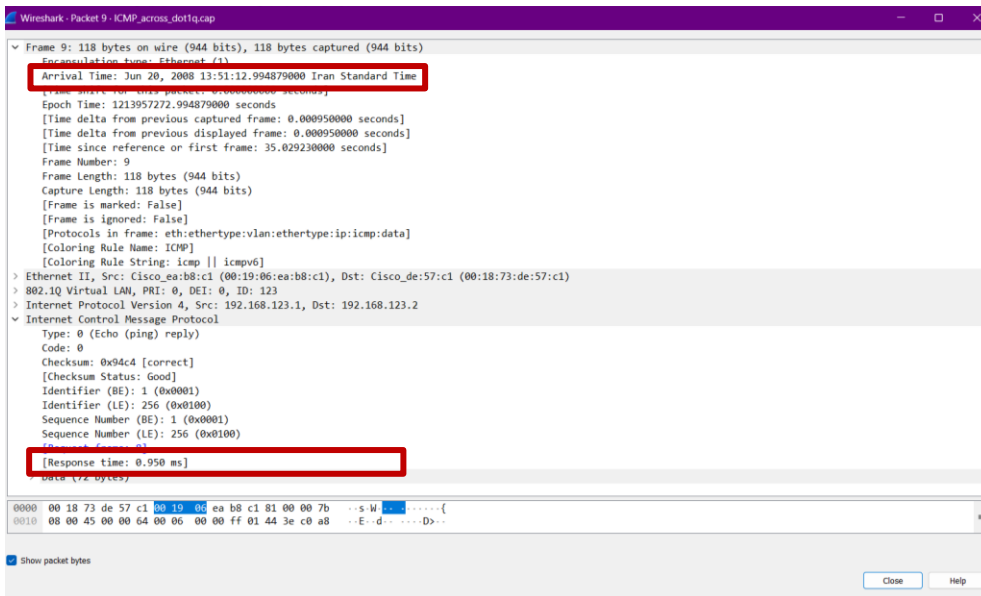
۴. شکل فریم ۵

برای

Request :8 → Reply :9 $0.994879-0.993929=0.950\text{ms}$



۵. شکل فریم ۸ درخواست



۶. شکل فریم ۹ پاسخ

Request : 10 → Reply : 11 $0.995686 - 0.995392 = 0.294\text{ms}$

```
Wireshark - Packet 10 - ICMP_across_dot1q.cap

▼ Frame 10: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
  Encapsulation type: Ethernet (1)
  Arrival Time: Jun 20, 2008 13:51:12.995392000 Iran Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1213957272.995392000 seconds
  [Time delta from previous captured frame: 0.000513000 seconds]
  [Time delta from previous displayed frame: 0.000513000 seconds]
  [Time since reference or first frame: 35.029743000 seconds]
  Frame Number: 10
  Frame Length: 118 bytes (944 bits)
  Capture Length: 118 bytes (944 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:vlan:ethertype:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
  > Ethernet II, Src: Cisco_de:57:c1 (00:18:73:de:57:c1), Dst: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 123
  > Internet Protocol Version 4, Src: 192.168.123.2, Dst: 192.168.123.1
  ▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x8cc3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 2 (0x0002)
    Sequence Number (LE): 512 (0x0200)
    [Response frame: 11]
  > Data (72 bytes)
```

۷. شکل فریم ۱۰ درخواست

```
Wireshark - Packet 11 - ICMP_across_dot1q.cap

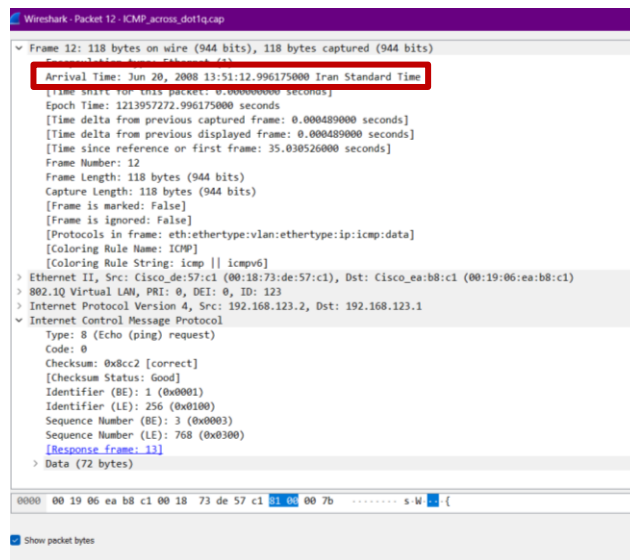
▼ Frame 11: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
  Encapsulation type: Ethernet (1)
  Arrival Time: Jun 20, 2008 13:51:12.995686000 Iran Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1213957272.995686000 seconds
  [Time delta from previous captured frame: 0.000294000 seconds]
  [Time delta from previous displayed frame: 0.000294000 seconds]
  [Time since reference or first frame: 35.030037000 seconds]
  Frame Number: 11
  Frame Length: 118 bytes (944 bits)
  Capture Length: 118 bytes (944 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:vlan:ethertype:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
  > Ethernet II, Src: Cisco_ea:b8:c1 (00:19:06:ea:b8:c1), Dst: Cisco_de:57:c1 (00:18:73:de:57:c1)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 123
  > Internet Protocol Version 4, Src: 192.168.123.1, Dst: 192.168.123.2
  ▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x94c3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 2 (0x0002)
    Sequence Number (LE): 512 (0x0200)
    [Request frame: 10]
    [Response time: 0.294 ms]
  > Data (72 bytes)
```

No.: 11 • Time: 35.030037 • Source: 192.168.123.1 • Destination: 192.168.123.2 • Protocol: ICMP • Length: 118 • Info: Echo (ping) reply id=0x0001, seq=2/512, ttl=255 (request in 10)

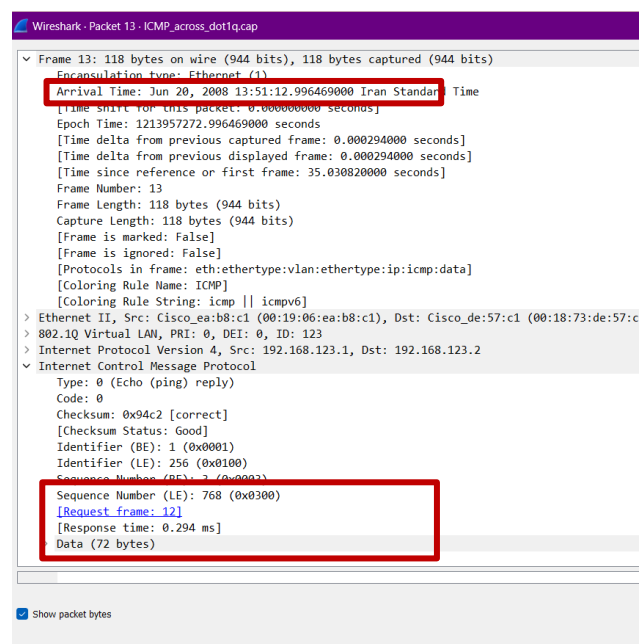
☒ Show packet bytes

۸. شکل فریم ۱۱ پاسخ

Request : 12 → Reply : 13 $0.996469 - 0.996175 = 0.294\text{ms}$

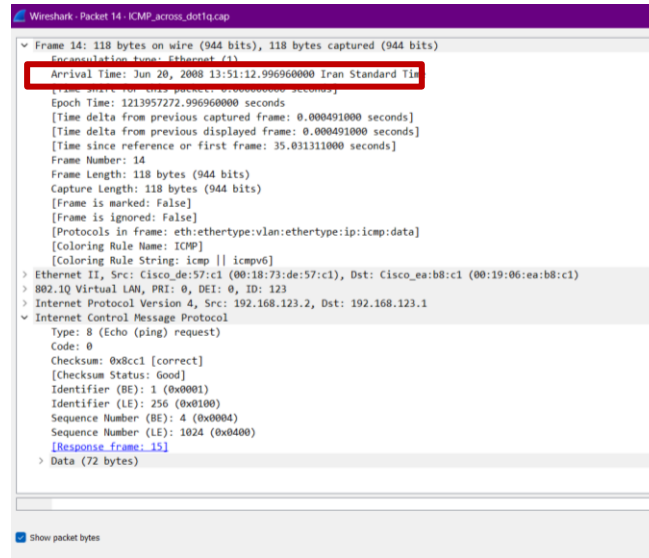


۹. شکل فریم ۱۲ درخواست

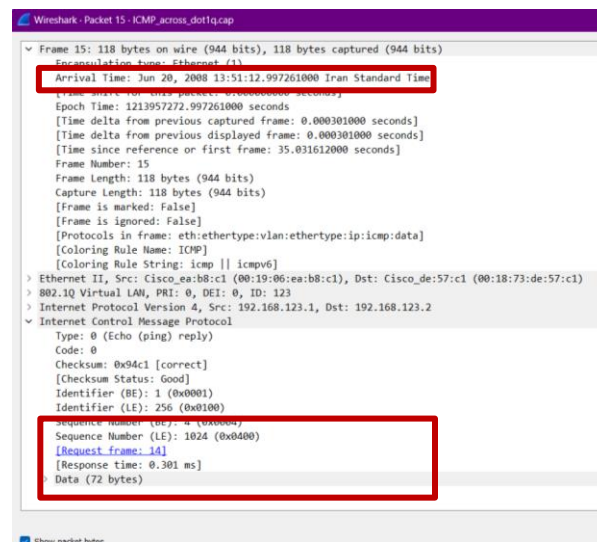


۱۰. شکل فریم ۱۳ پاسخ

Request : 14 → Reply : 15 $0.997261 - 0.996960 = 0.301\text{ms}$



۱۱. شکل فریم ۱۴ درخواست



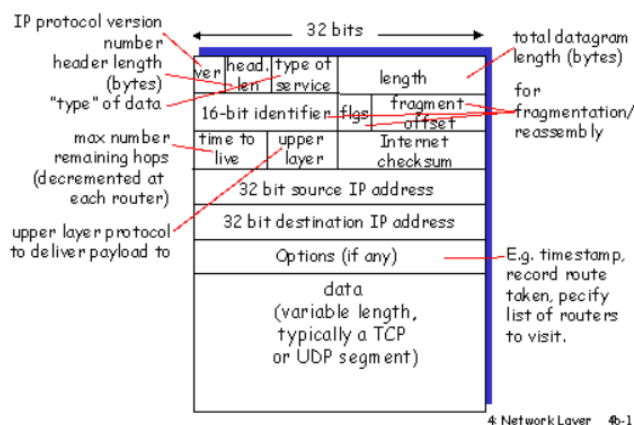
۱۲. شکل فریم ۱۵ پاسخ

A) Min = 0.294 ms

B) Max = 0.950 ms

C) Avg = 0.45975 ms

IP datagram format



Note: for each packet, the first 14 Bytes are the Ethernet header.

01 00 5e 00 00 fc 60 eb 69 4d 97 3f 08 00 46 00
00 20 07 32 00 00 01 02 33 d7 ac 11 5c c1 e0 00
00 fc 94 04 00 00 16 00 09 03 e0 00 00 fc 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Header : 14 bit

ip source address : ac 11 5c c1 → 172.17.92.193

ip destination address: e0 00 00 fc → 224.0.0.252

ip protocol : 02 → IGMP

فیلد پروتوکل در بایت ۲۴ ام قرار دارد که همانطور که مشاهده می کنیم ۰۲ است که نماد پروتوکل Internet Group Management Protocol

در لایه سوم مدل tcp / ip قرار دارد

IGMP (Internet Group Management Protocol) پروتکلی است که عضویت هاست در گروه های IP multicast موجود در یک بخش (Segment) از شبکه مدیریت میکند. یک گروه IP Multicast که با نام یک host group هم شناخته میشود، مجموعه ای از هاستها است که به ترافیک های آدرس دهی شده با آدرس IP multicast در شبکه گوش میدهند. ترافیک IP multicast در واقع به یک آدرس MAC فرستاده اما توسط چندین هاست پردازش میشود.

01 00 5e 00 00 01 64 31 50 0e 0a 2f 08 00 45 00
00 3c 2c a3 00 00 80 01 25 77 ac 11 5c 94 e0 00
00 01 08 00 2d de 00 01 0a 90 42 69 74 44 65 66
65 6e 64 65 72 20 46 69 72 65 77 61 6c 6c 20 42
72 6f 61 64 63 61 73 74 00 00

ip source address : ac 11 5c 94 → 172.17.92.148

ip destination address: e0 00 00 01 → 224.0.0.1

ip protocol : 01 → ICMP

فیلد پروتوکل در بایت ۲۴ ام قرار دارد که همانطور که مشاهده می کنیم ۰۱ است که نماد پروتوکل Internet Control Message Protocol

از پروتوکل های اصلی بسته پروتکل های اینترنت

پروتکل icmp که مخفف عبارت internet control message protocol است که در فارسی آن را پروتکل کنترل پیام های اینترنتی ترجمه می کنند. icmp جهت خطایابی در کامپیوترها ، روترها و هاست، بررسی وجود سیگنال و به طور کلی بررسی وضعیت ارتباطی بین روتر و سرور ها مورد استفاده قرار می گیرد.

در مدل ۵ لایه ای شبکه، این پروتکل همانند پروتکل ip در لایه ی network (شبکه) قرار می گیرد، اما نوع کارکرد آن شبیه پروتکل های لایه ی transport (انتقال) می باشد.

سؤال ۵

پاسخ درست ۵

الف) بسته ICMP دارای پورت مبدا و مقصد نیست زیرا برای network-layer information طراحی شده است.

و این دیتا ها بین روتر و هاست جا به جا می شوند نه برای فرایند های applications layer

هر بسته ICMP یک "نوع" و یک "کد" دارد. ترکیب نوع/کد پیام خاص در حال دریافت را مشخص می کند. از آنجایی که خود نرم افزار شبکه همه چیز را تفسیر می کند پیام های ICMP، برای هدایت پیام ICMP به یک لایه برنامه application layer ، به شماره پورتی نیاز نیست

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

request(ب)

ping request: type: 8 code number: 0

Data section با سائز متغیر خواهیم داشت و دیتای خالص را به ما نشان می دهد و هدر ۸ بایتی که این هدر شامل ایتام های زیر می باشد:

Type : مشخص کننده ی نوع پیام ICMP و یک بایت را شامل می شود در اینجا برابر ۸

Code : در اینجا برابر با صفر اطلاعات بیش تری درباره ی تایپ پیام در اختیار ما می گذارد و در اینجا جزئیاتی همچون زیر نوع ها و خطاها را مشخص می کند که در اینجا به معنای فرستادن یک پینگ مشخص و درخواست ارسال پاسخ است. شامل یک بایت

Checksum : 2 بایت برای اطمینان از درستی پکت

Identifier : ۲ بایت برای بایند کردن رکوئست به ریپلای

Sequence number : شماره توالی خام مقدار واقعی تخصیص داده شده به بسته است. WireShark جلسات TCP را گروه بندی می کند و به آنها اعداد توالی نسبی (و تایید) اختصاص می دهد که از ۰ شروع می شود (و به نظر می رسد برای هر بسته بعدی ۱ افزایش می یابد) تا کاربر بتواند توالی رویدادها را شناسایی کند.

2بایت

ث)reply

type: 0 code number: 0

Type : مشخص کننده ی نوع پیام ICMP و یک بایت را شامل می شود در اینجا برابر 0

نوع پیام ICMP اینجا اکو ریپلای و برابر صفر و کد آن هم برابر صفر می باشد.

Code : در اینجا برابر با صفر اطلاعات بیش تری درباره ی تایپ پیام در اختیار ما می گذارد و در اینجا جزئیاتی همچون زیر نوع ها و خطاها را مشخص می کند که در اینجا به معنای فرستادن یک پینگ مشخص و درخواست ارسال پاسخ است. شامل یک بایت

Checksum : 2 بایت برای اطمینان از درستی پکت

Identifier : ۲ بایت برای بایند کردن رکوئست به ریپلای

Sequence number : شماره توالی خام مقدار واقعی تخصیص داده شده به بسته است. WireShark جلسات TCP را گروه بندی می کند و به آنها اعداد توالی نسبی (و تایید) اختصاص می دهد که از ۰ شروع می شود (و به نظر می رسد برای هر بسته بعدی ۱ افزایش می یابد) تا کاربر بتواند توالی رویدادها را شناسایی کند.

2بایت

```
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xde69 [correct]
[Checksum Status: Good]
Identifier (BE): 2 (0x0002)
Identifier (LE): 512 (0x0200)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
```

رکوئست

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xe669 [correct]
  [Checksum Status: Good]
  Identifier (BE): 2 (0x0002)
  Identifier (LE): 512 (0x0200)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
```

ریپلای