



NETWORK ARCHITECTURE-1
HOMEWORK-3

Submitted by:

Moulika Chadalavada

16234180

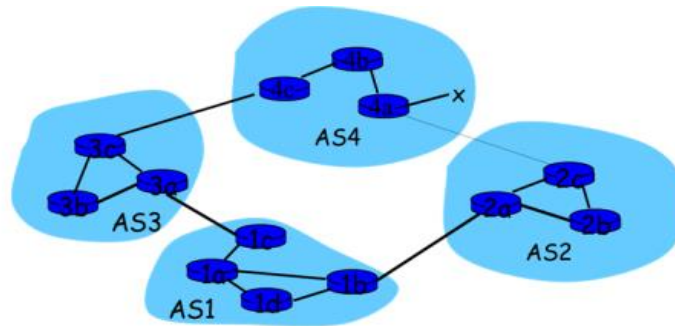
NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 2 of 15

Question 1: Consider the network shown below. Suppose AS2 and AS3 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.

- (a) Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP or iBGP?
- (b) Router 3a learns about prefix x from which routing protocol?
- (c) Router 1c learns about prefix x from which routing protocol?
- (d) Router 1d learns about prefix x from which routing protocol?



Solution:

- (a) Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP or iBGP?

In above diagram, Router 3c is in AS3 terminal and it learns about the destination x which is connected to 4a of AS4 by using inter-AS routing protocol i.e. **eBGP**. So **Router 3c learns about prefix x from eBGP routing protocol**.

- (b) Router 3a learns about prefix x from which routing protocol?

In above diagram, Router 3a in AS3 learns about destination x through 3c using **iBGP** inter-AS routing protocol. Router 3c is in AS3 gateway and it learns about the destination x connected to 4a of AS4 by using inter-AS routing protocol i.e. eBGP. So **Router 3a learns about prefix x from iBGP routing protocol**.

- (c) Router 1c learns about prefix x from which routing protocol?

In above diagram, Router 1c is in AS1 gateway and it learns about destination x that is connected to Router 4a of AS4 by using inter-AS routing protocol that is **eBGP**. So **Router 1c learns about prefix x from eBGP routing protocol**.

- (d) Router 1d learns about prefix x from which routing protocol?

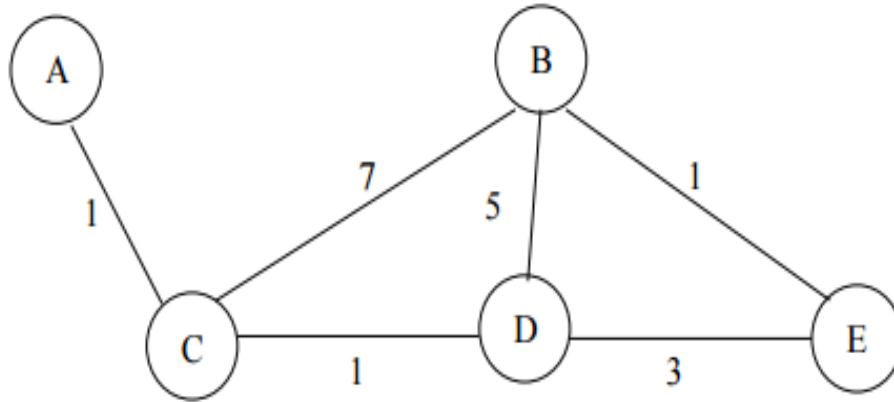
In above diagram, Router 1c is in AS1 and it learns about destination x that is connected to 4a of AS4 by using inter-AS routing protocol that is eBGP. **Router 1d learns about x through 1c using iBGP inter-AS routing protocol**.

NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 3 of 15

Question 2: Consider the network shown below (the labels are the delay on the links).



(a) Show the operation of Dijkstra's (Link State) algorithm for computing the shortest path from C to all destinations.

Solution:

Dijkstra's algorithm is used for finding the shortest paths between nodes in a graph

The below table shows different paths from C to other nodes which is calculated using Dijkstra's algorithm.

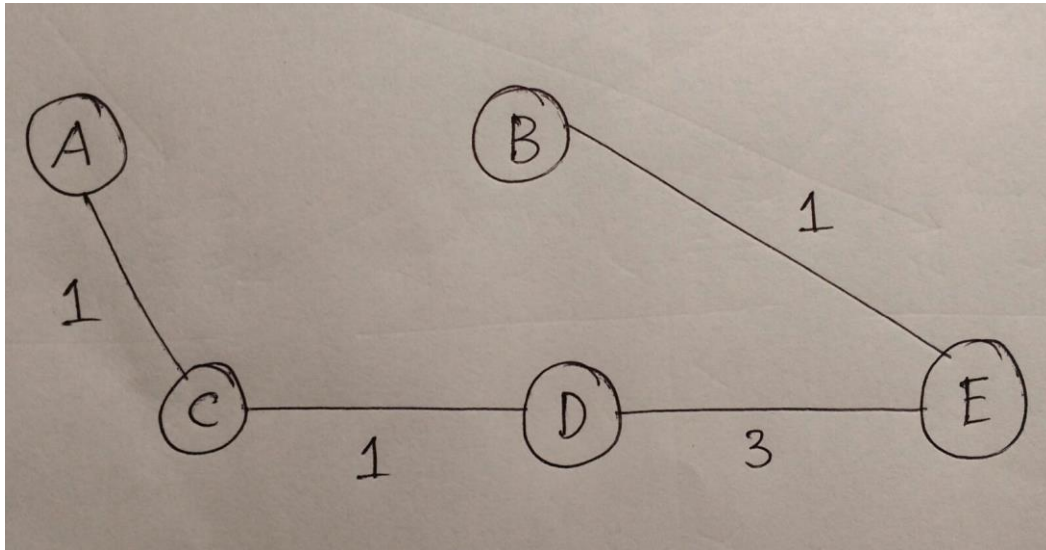
STEP	N'	D(A)=P(A)	D(B)=P(B)	D(D)=P(D)	D(E)=P(E)
0	C	1, A	7, B	1, D	∞
1	CD	1, A	6, D	—	4, D
2	CDA	—	6, D	—	4, D
3	CDAE	—	5, E	—	—
4	CDAEB	—	—	—	—

NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 4 of 15

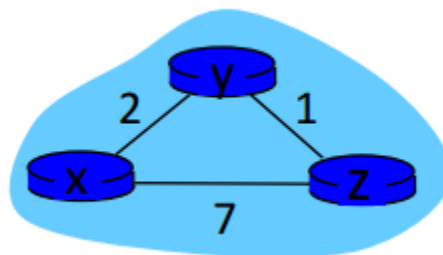
The below diagram shows the shortest path from C to all destinations.



The below is the Forwarding table in C:

Destination	Link
A	(C,A)
B	(C,D)
D	(C,D)
E	(C,D)

Question 3: Consider the network shown below (the labels are the delay on the links)



NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 5 of 15

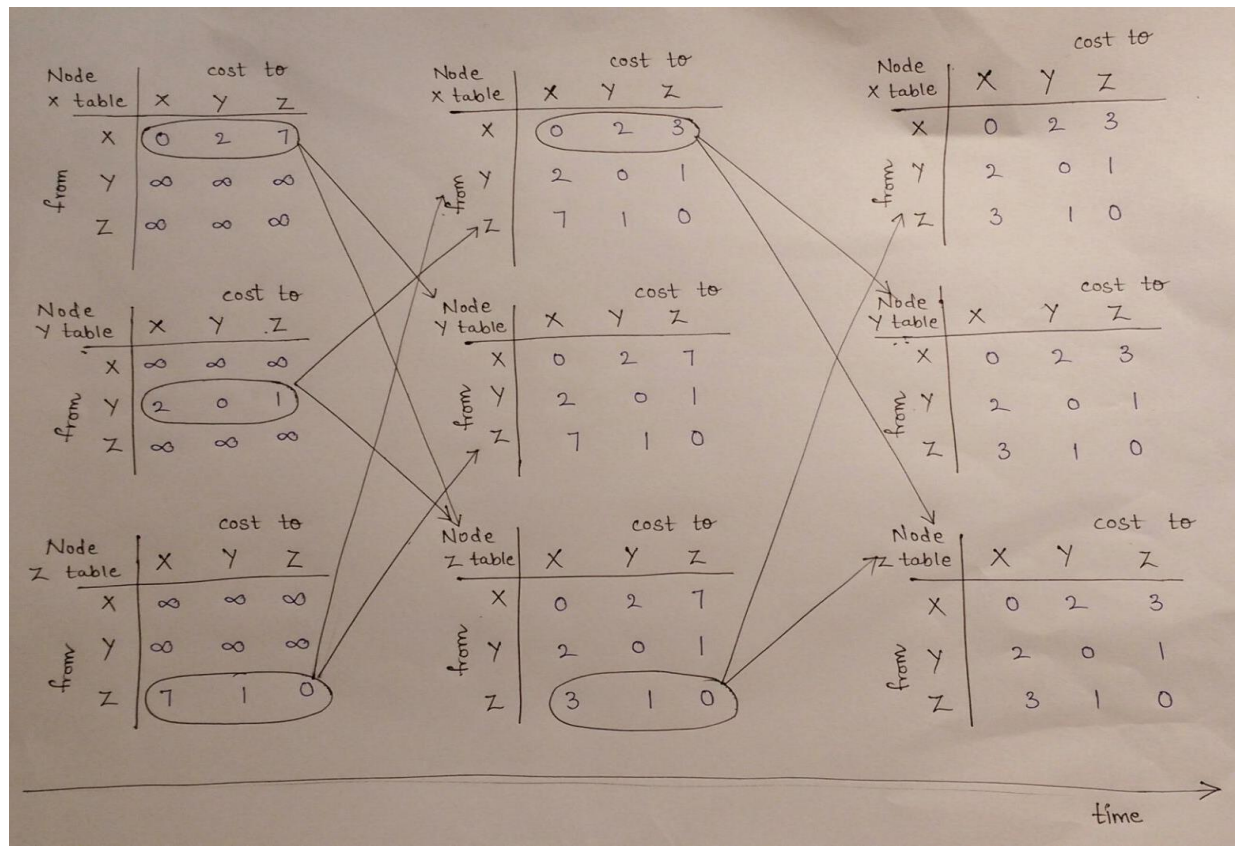
(a) Show the operation of Distance Vector algorithm for computing the shortest path from node X, node Y, node Z to all destinations.

Solution:

We know that,

$$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\} = \min\{2+0, 7+1\} = 2$$

$$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\} = \min\{2+1, 7+0\} = 3$$



(b) Show the distance table that would be computed by the distance vector algorithm.

Solution:

Node	To x	To y	To z
From x	0	2	3
From y	2	0	1
From z	3	1	0

NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

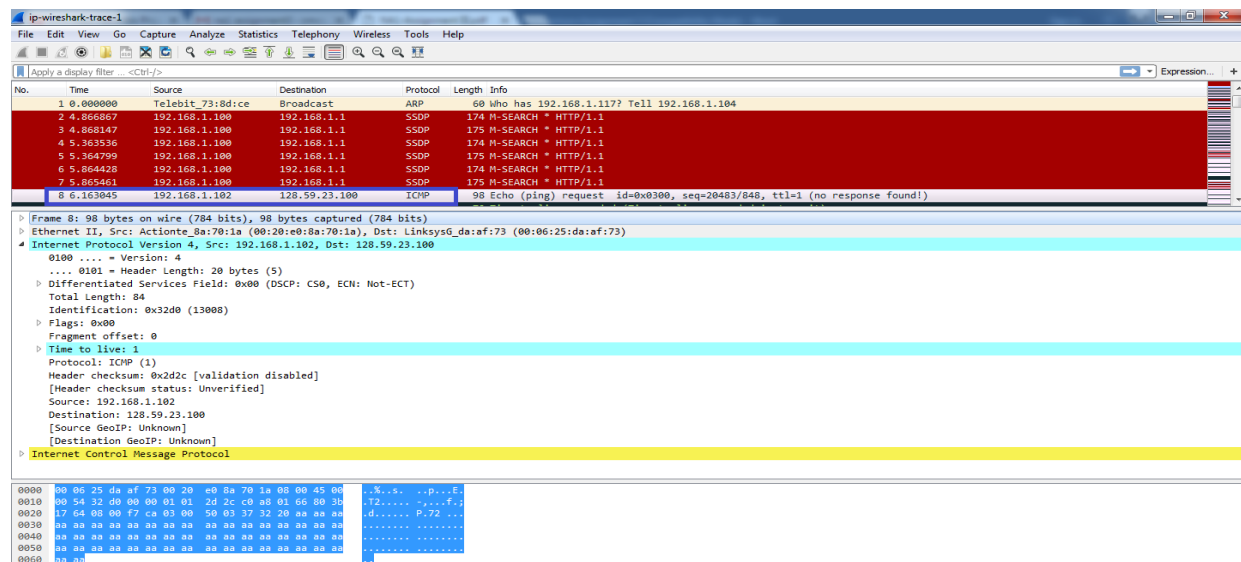
Page 6 of 15

Laboratory Homework: Wireshark

1. Select the first ICMP Echo Request message sent by the computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of the user's computer?

Solution:

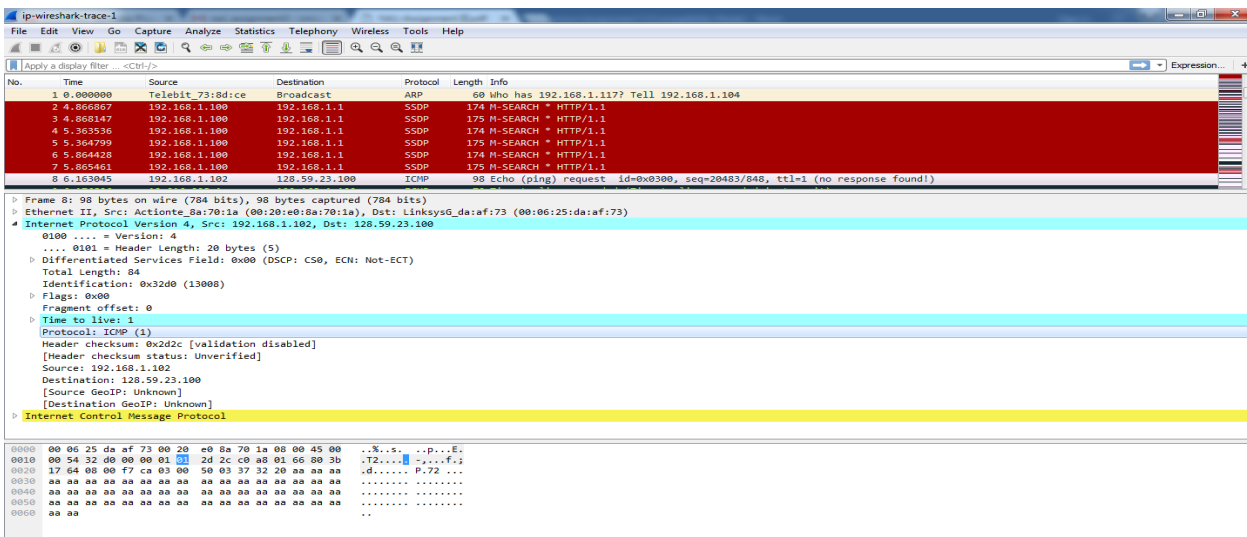
The below image shows the Wireshark screen of first ICMP Echo Request. IP address of user's computer is **192.168.1.102**



2. Within the IP packet header, what is the value in the upper layer protocol field?

Solution:

As show in below image, within the IP packet header the value in the upper layer protocol field is '1'



NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 7 of 15

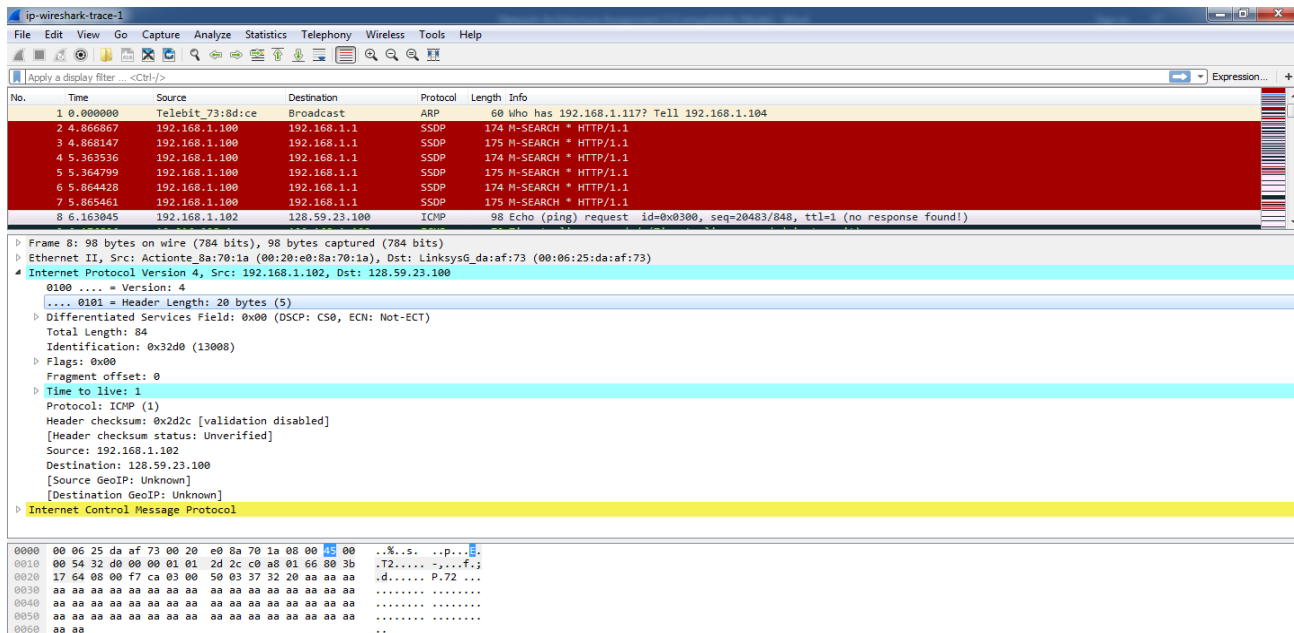
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Solution:

As shown in below image, the header length is **20 bytes**.

The payload of IP datagram is of length **84 bytes**.

The number of payload bytes is given by the difference between the payload of IP datagram and the header length = $84 - 20 = 64$ bytes.



4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Solution:

As shown in below diagram IP datagram is **not fragmented**.

It is not fragmented as it is known by flags value i.e. **0x00**.

NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA

Page 8 of 15

STUDENT ID: 16234180

The image shows a Wireshark capture of network traffic. The packet list pane shows several SSDP (Simple Service Discovery Protocol) packets and one ICMP Echo (ping) request. The selected packet is an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The packet details pane shows the following information:

- Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x32d0 (13008)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x2d2c [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the ICMP Echo (ping) request, including the IP header and the ICMP header.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by the computer?

Solution:

To analyze the changes from one datagram to another datagram let's consider datagrams 368,365,361,358

Datagram 368

The image shows a Wireshark capture of network traffic. The packet list pane shows several IP fragments and one ICMP Echo (ping) request. The selected packet is an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The packet details pane shows the following information:

- Frame 368: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 560
- Identification: 0x334a (13130)
- Flags: 0x00
- Fragment offset: 2960
- Time to live: 13
- Protocol: ICMP (1)
- Header checksum: 0x1d5c [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- [3 IPv4 Fragments (3508 bytes): #366(1480), #367(1480), #368(548)]
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the ICMP Echo (ping) request, including the IP header and the ICMP header.

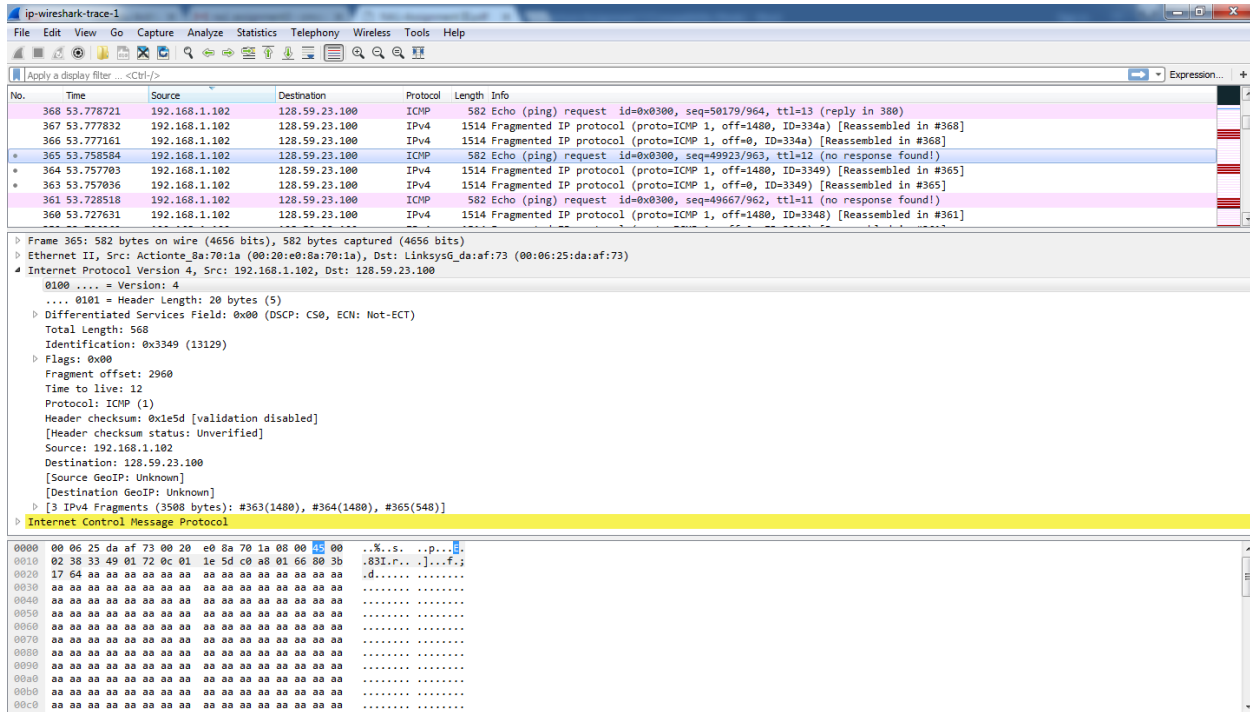
NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA

Page 9 of 15

STUDENT ID: 16234180

Datagram 365

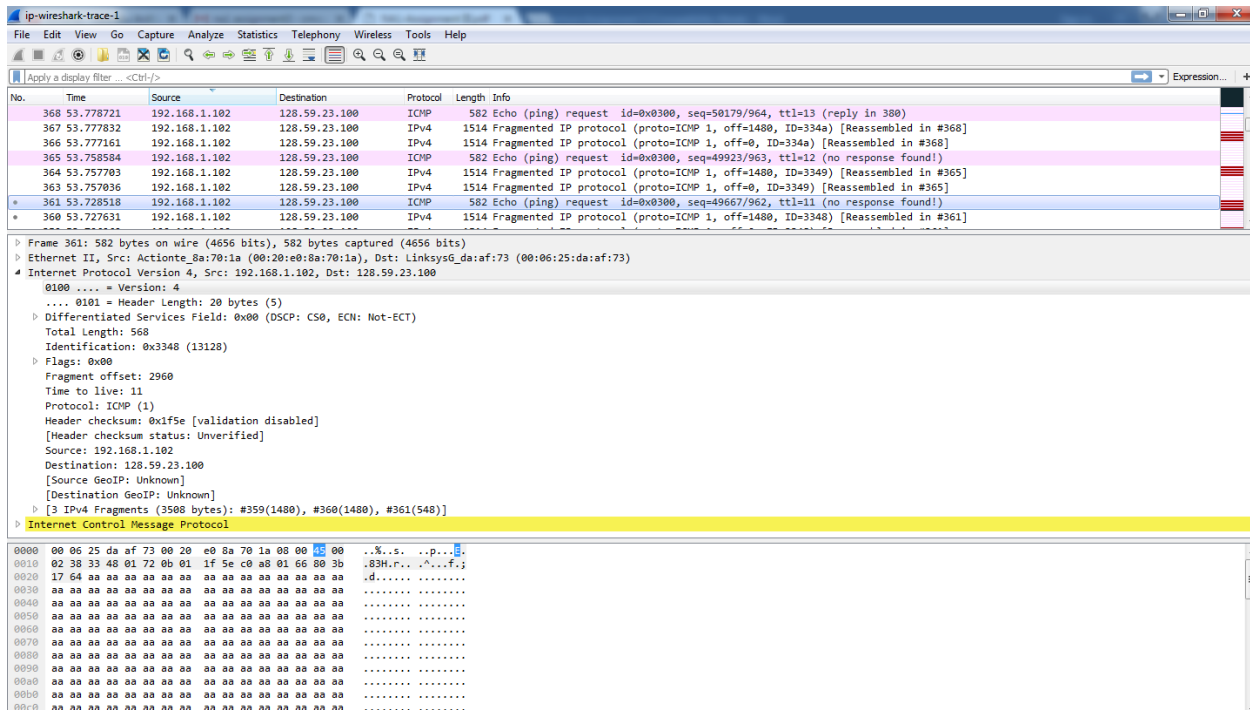


The image shows a Wireshark capture of Datagram 365. The packet list pane on the left shows several ICMP Echo (ping) requests and responses. The selected packet, Datagram 365, is an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The packet details pane shows the following information:

- Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 568
- Identification: 0x3349 (13129)
- Flags: 0x00
- Fragment offset: 2960
- Time to live: 12
- Protocol: ICMP (1)
- Header checksum: 0x1e5d [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- [3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)]
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and ICMP Echo request data.

Datagram 361



The image shows a Wireshark capture of Datagram 361. The packet list pane on the left shows several ICMP Echo (ping) requests and responses. The selected packet, Datagram 361, is an ICMP Echo (ping) request from 192.168.1.102 to 128.59.23.100. The packet details pane shows the following information:

- Frame 361: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 568
- Identification: 0x3348 (13128)
- Flags: 0x00
- Fragment offset: 2960
- Time to live: 11
- Protocol: ICMP (1)
- Header checksum: 0x1f5e [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- [3 IPv4 Fragments (3508 bytes): #359(1480), #360(1480), #361(548)]
- Internet Control Message Protocol

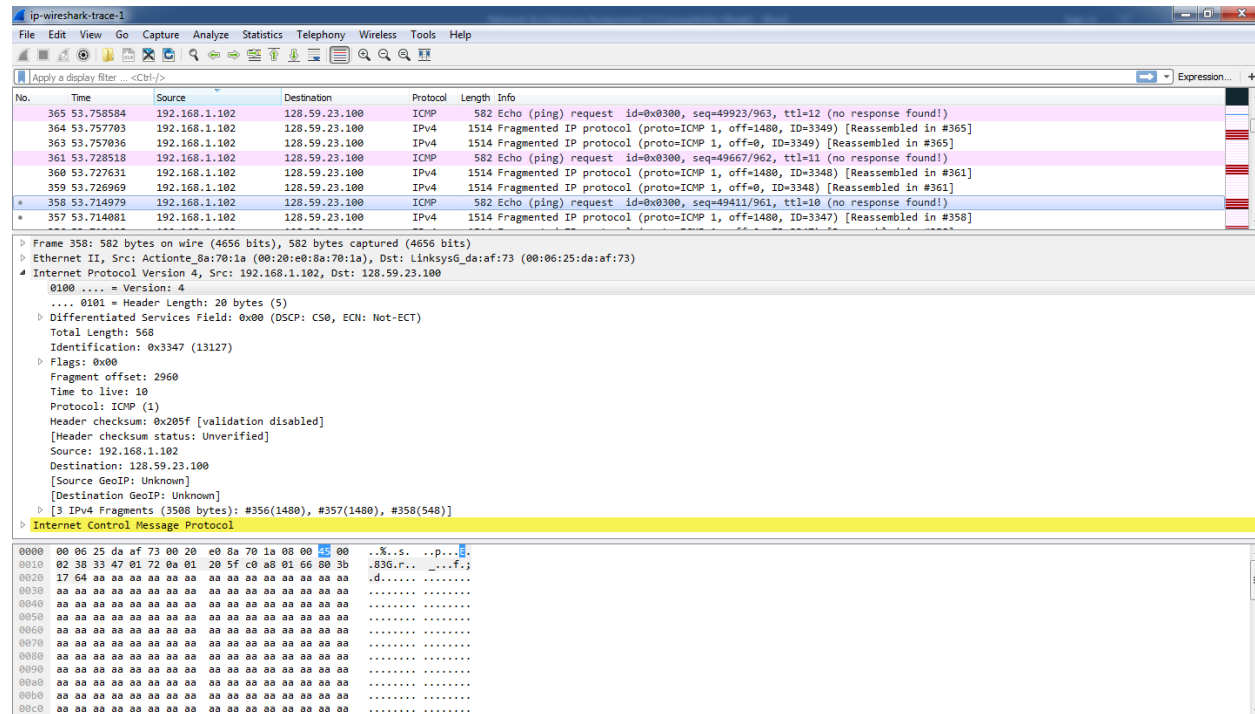
The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and ICMP Echo request data.

NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 10 of 15

Datagram 358



The below table shows the fields that always change from different datagrams.

Fields Type	Datagram 368	Datagram 365	Datagram 361	Datagram 358
Identification	0x334a (13130)	0x3349 (13129)	0x3348 (13128)	0x3347 (13127)
Time to Live	13	12	11	10
Header Checksum	0x1d5c	0x1e5d	0x1f5e	0x205f

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Solution:

Fields like version, header length, flags, fragment offset, total length, source address, and destination address field stay constant as the webpage being accessed is same.

Fields like identification, time to live, header checksum fields change because each packet has unique identification and factors like time to live and checksum are generated for individual elements.

The below table shows various field types which has constant and inconstant values based on the images in question 5 of Datagram 368,365,361,358.

NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 11 of 15

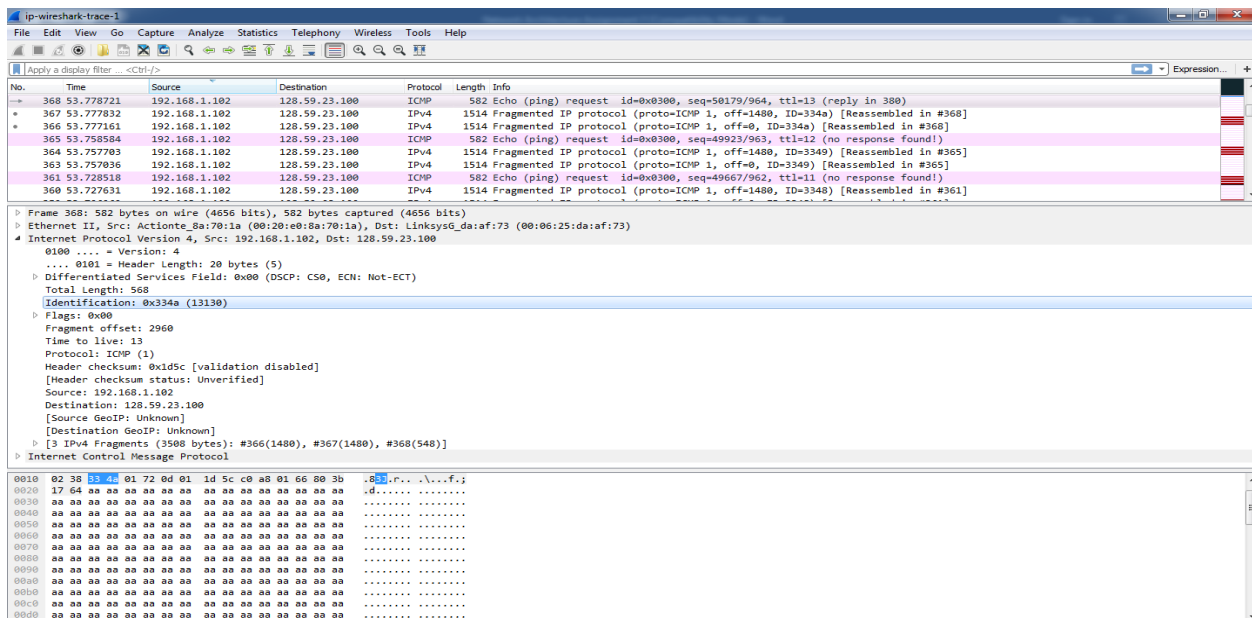
Fields Type	Datagram 368	Datagram 365	Datagram 361	Datagram 358
Identification	0x334a (13130)	0x3349 (13129)	0x3348 (13128)	0x3347 (13127)
Time to Live	13	12	11	10
Header Checksum	0x1d5c	0x1e5d	0x1f5e	0x205f
Version	4	4	4	4
Header Length	20 bytes	20 bytes	20 bytes	20 bytes
Source Address	192.168.1.102	192.168.1.102	192.168.1.102	192.168.1.102
Destination Addr	128.59.23.100	128.59.23.100	128.59.23.100	128.59.23.100
Flags	0x00	0x00	0x00	0x00
Fragment Offset	2960	2960	2960	2960

7. Describe the pattern you see in the values in the Identification field of the IP datagram Next (with the packets still sorted by source address) find the series of ICMP TTLexceeded replies sent to the computer by the nearest (first hop) router.

Solution:

The value in the identification field of the IP datagram decreases by 1 as we move down.

Datagram 368: 13130

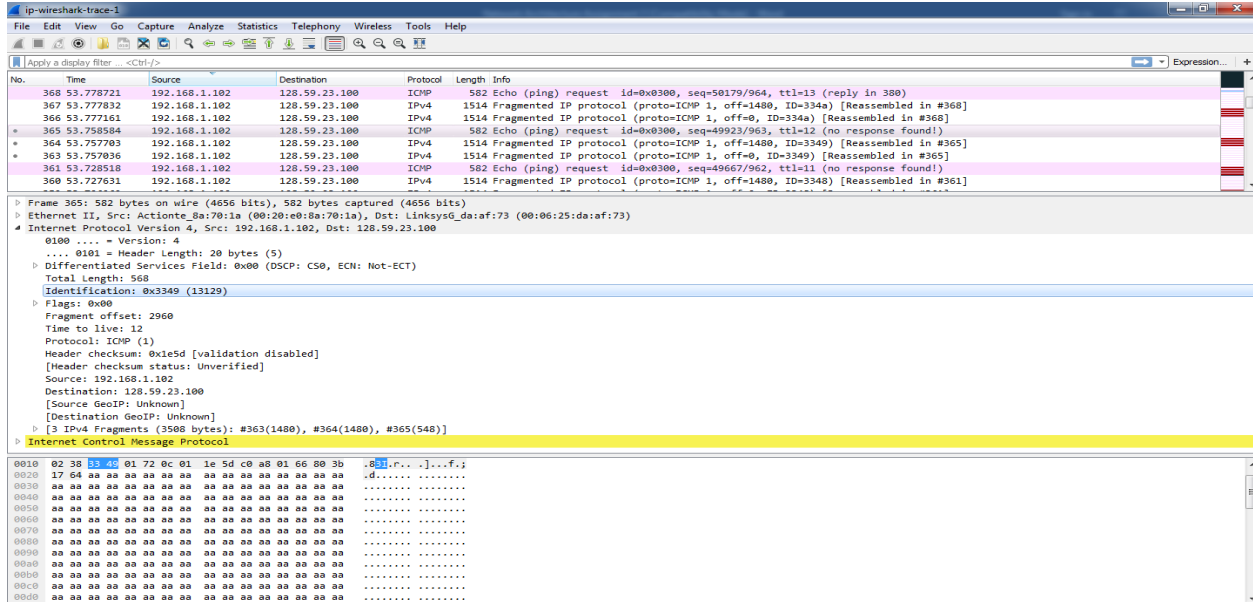


NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 12 of 15

Datagram 365: 13129



The image shows a Wireshark capture of a network packet. The packet list pane shows a list of packets, with packet 365 selected. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) header. The packet bytes pane shows the raw data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
368	53.778721	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367	53.777832	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366	53.777161	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365	53.758584	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
364	53.757703	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
363	53.757036	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
361	53.728518	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
360	53.727631	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]

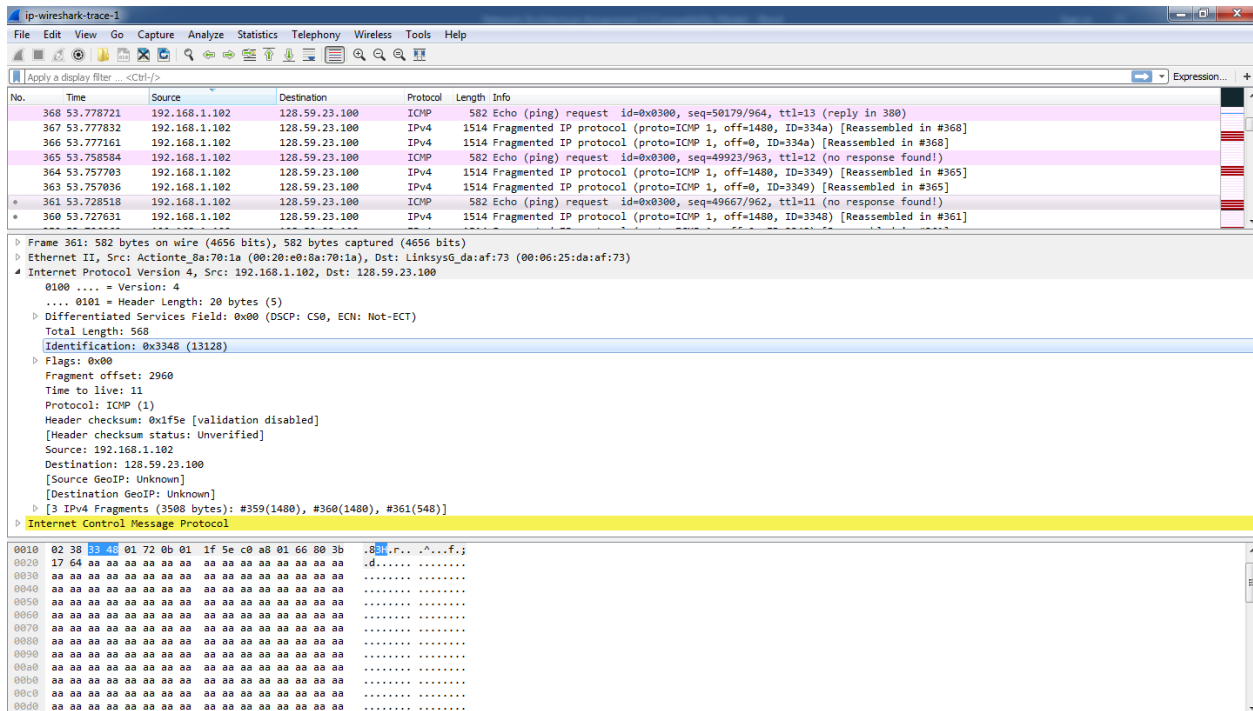
Packet Details:

- Frame 365: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 568
 - Identification: 0x3349 (13129)
 - Flags: 0x00
 - Fragment offset: 2960
 - Time to live: 12
 - Protocol: ICMP (1)
 - Header checksum: 0x1e5d [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.102
 - Destination: 128.59.23.100
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
 - 3 IPv4 Fragments (3508 bytes): #363(1480), #364(1480), #365(548)
- Internet Control Message Protocol

Packet Bytes:

0010 02 38 13 46 01 72 0c 01 1e 5d c0 a0 01 66 80 3b .800(r...f...
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .d.....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0070 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0080 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0090 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00a0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00b0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00c0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00d0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

Datagram 361: 13128



The image shows a Wireshark capture of a network packet. The packet list pane shows a list of packets, with packet 361 selected. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) header. The packet bytes pane shows the raw data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
368	53.778721	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367	53.777832	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366	53.777161	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365	53.758584	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49923/963, ttl=12 (no response found!)
364	53.757703	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
363	53.757036	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
361	53.728518	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=49667/962, ttl=11 (no response found!)
360	53.727631	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3348) [Reassembled in #361]

Packet Details:

- Frame 361: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 568
 - Identification: 0x3348 (13128)
 - Flags: 0x00
 - Fragment offset: 2960
 - Time to live: 11
 - Protocol: ICMP (1)
 - Header checksum: 0x1f5e [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.102
 - Destination: 128.59.23.100
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
 - 3 IPv4 Fragments (3508 bytes): #359(1480), #360(1480), #361(548)
- Internet Control Message Protocol

Packet Bytes:

0010 02 38 13 46 01 72 0b 01 1f 5e c0 a0 01 66 80 3b .800(r...^...f...
0020 17 64 aa aa aa aa aa aa aa aa aa aa aa aa aa aa .d.....
0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0040 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0050 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0060 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0070 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0080 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
0090 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00a0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00b0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00c0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa
00d0 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa

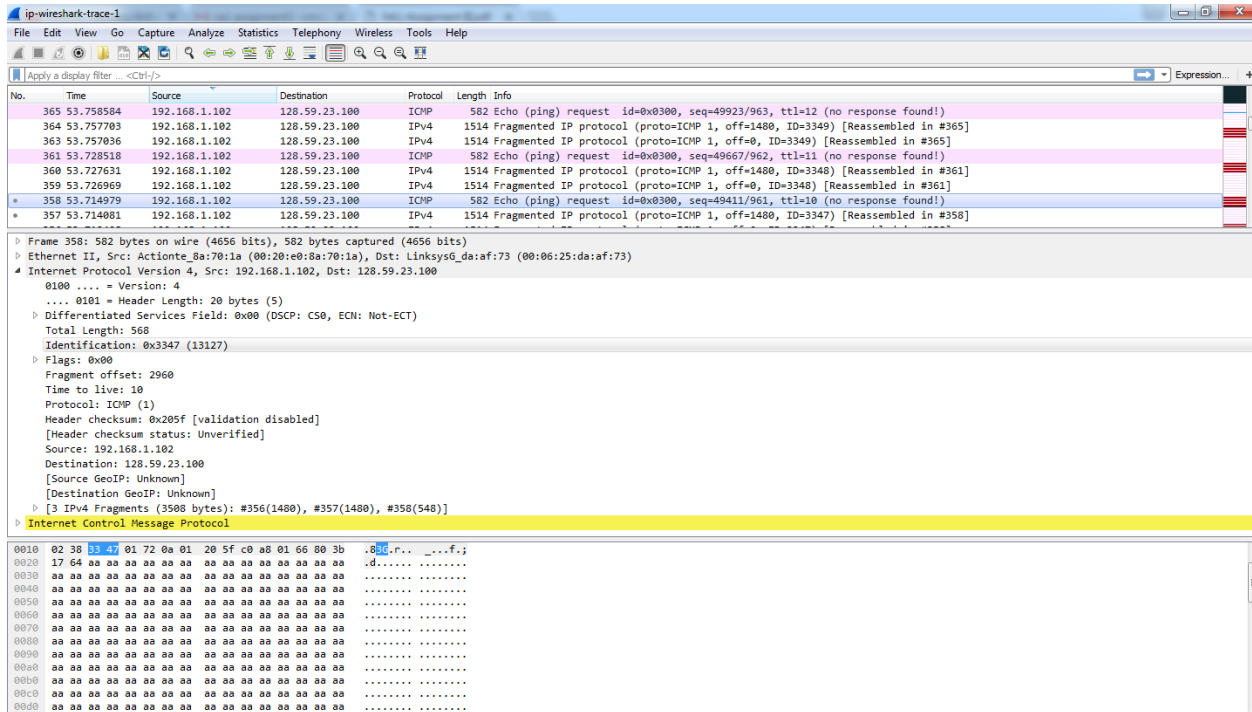
NETWORK ARCHITECTURE-1 HOMEWORK 3

STUDENT NAME: MOULIKA CHADALAVADA

STUDENT ID: 16234180

Page 13 of 15

Datagram 358: 13127

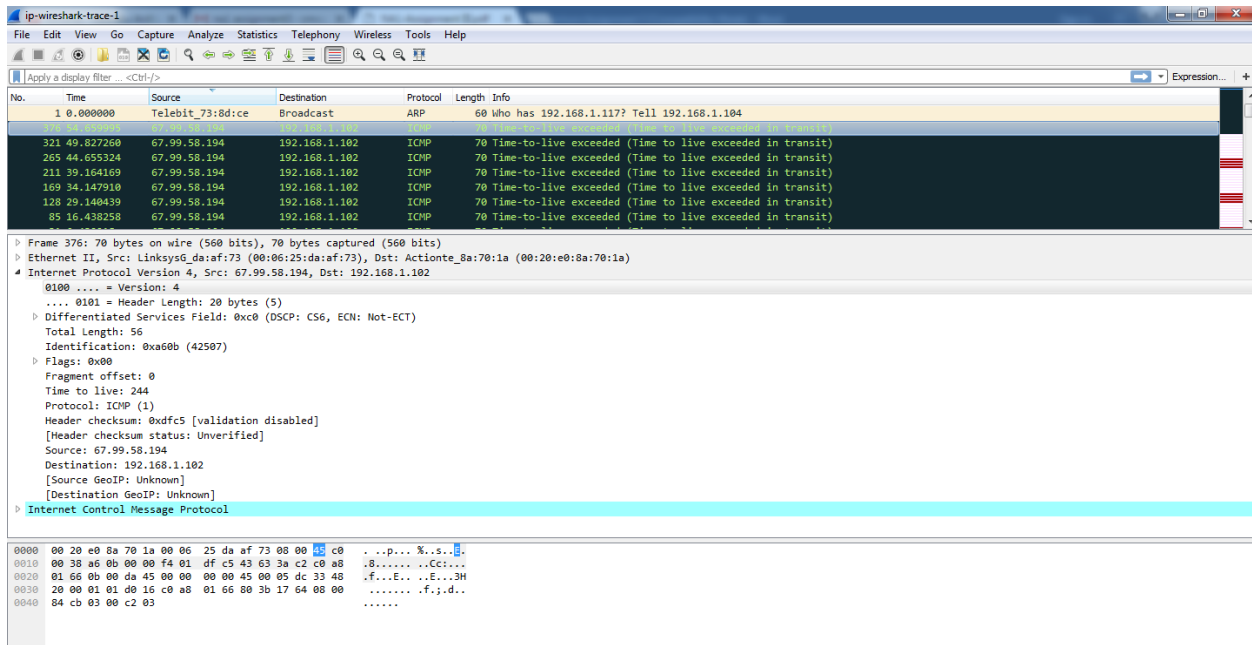


The image shows a Wireshark capture of a network packet. The packet list pane shows a series of ICMP Echo (ping) requests and responses. The packet details pane for packet 358 (13127) shows the following information:

- Frame 358: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits)
- Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys0_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 568
- Identification: 0x3347 (13127)
- Flags: 0x00
- Fragment offset: 2960
- Time to live: 10
- Protocol: ICMP (1)
- Header checksum: 0x205f [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- 3 IPv4 Fragments (3508 bytes): #356(1480), #357(1480), #358(548)
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, including the ICMP Echo request.

The below image shows Series of ICMP TTL exceeded replies sent to the computer.



The image shows a Wireshark capture of a network packet. The packet list pane shows a series of ICMP Time-to-live exceeded (TTL exceeded) replies. The packet details pane for packet 376 (42507) shows the following information:

- Frame 376: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
- Ethernet II, Src: Linksys0_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
- Internet Protocol Version 4, Src: 67.99.58.194, Dst: 192.168.1.102
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
- Total Length: 56
- Identification: 0xa60b (42507)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 244
- Protocol: ICMP (1)
- Header checksum: 0xdfc5 [validation disabled]
- [Header checksum status: Unverified]
- Source: 67.99.58.194
- Destination: 192.168.1.102
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, including the ICMP Time-to-live exceeded reply.

NETWORK ARCHITECTURE-1 HOMEWORK 3

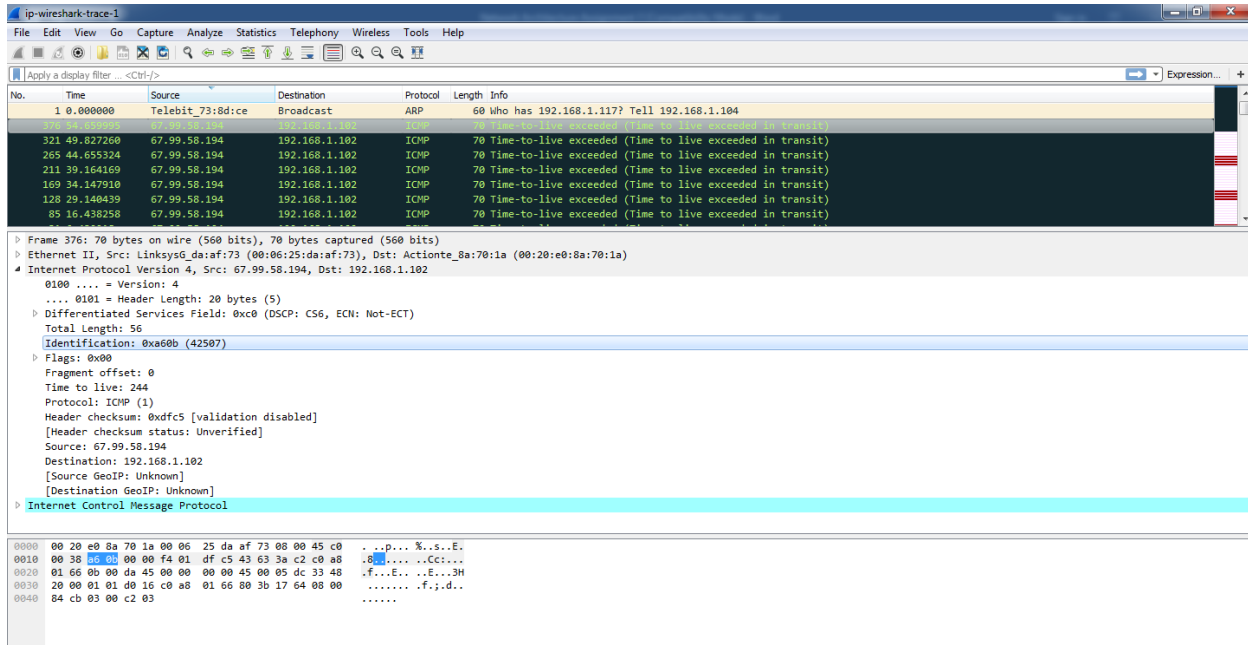
STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 14 of 15

8. What is the value in the Identification field and the TTL field?

Solution:

From the below image Identification field is **0xa60b (42507)** and Time to Live is **244**

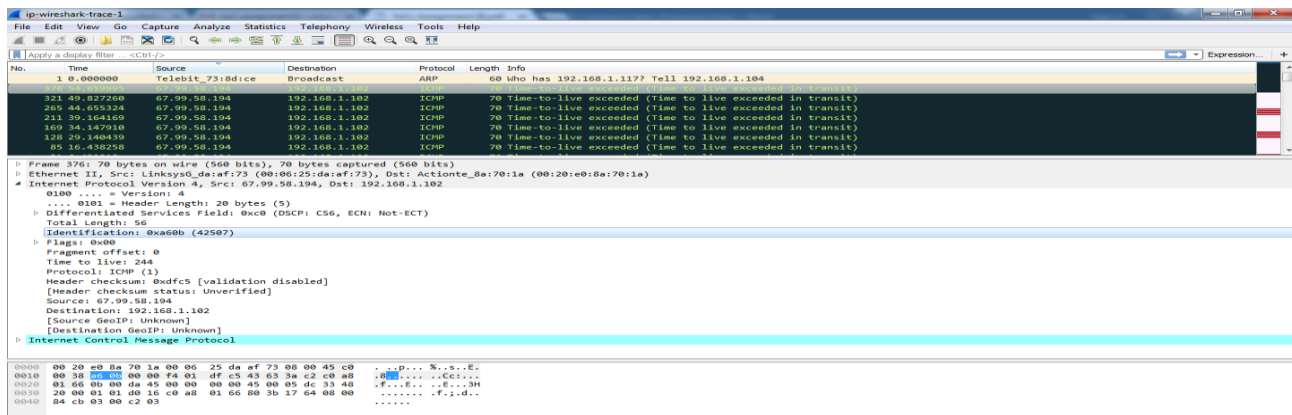


9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to the computer by the nearest (first hop) router? Why?

Solution:

TTL field remains unchanged but Identification field value changes for all the ICMP-TTL exceeded replies sent to the computer because no datagram is sent to router. If datagram is sent to router, then TTL might have changed.

Datagram 376

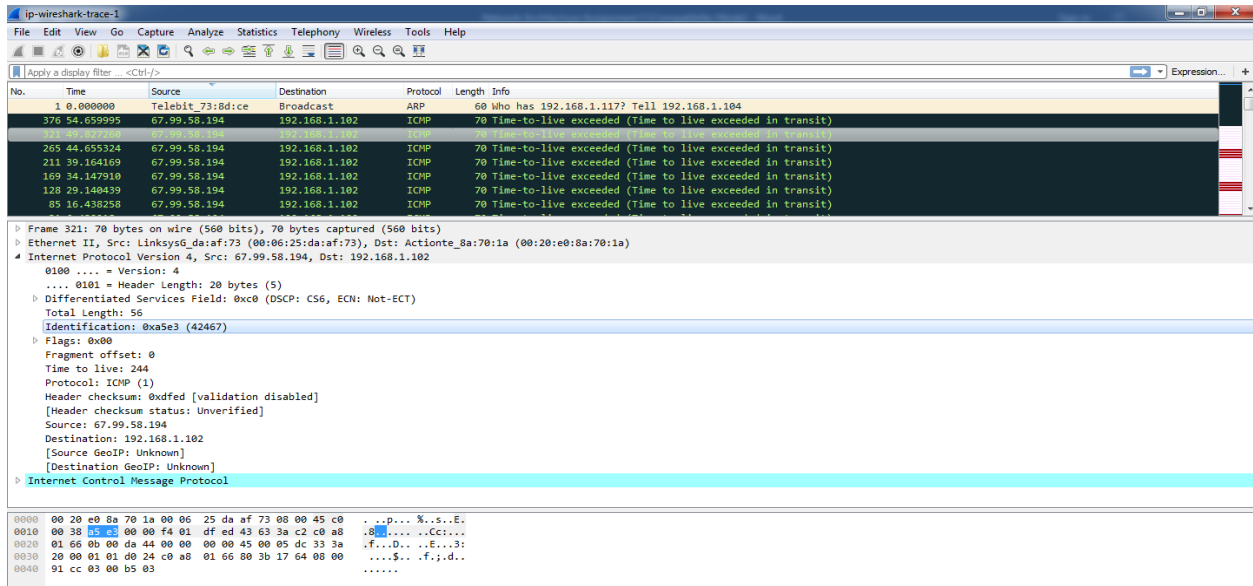


NETWORK ARCHITECTURE-1 HOMEWORK 3

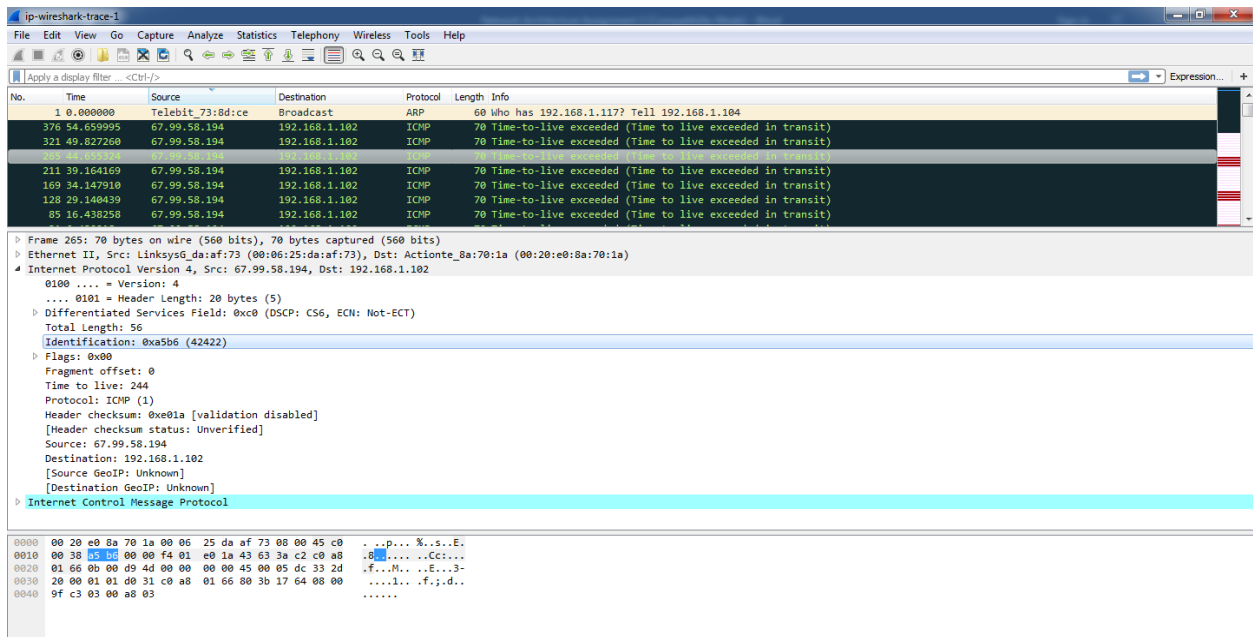
STUDENT NAME: MOULIKA CHADALAVADA
STUDENT ID: 16234180

Page 15 of 15

Datagram 321



Datagram 265



Fields Type	Datagram 376	Datagram 321	Datagram 265
Identification	0xa60b (42507)	0xa5e3 (42467)	0xa5b6 (42422)
Time to Live	244	244	244