

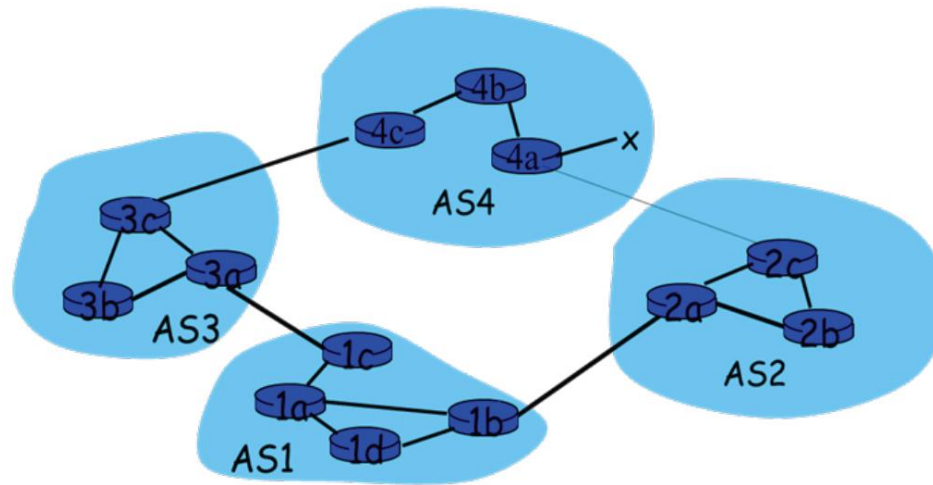
# CSEE 5110 Network Architecture I

## Assignment 3 solution

Sri Harsha Chennavajjala (16210893)

[SC9V9@mail.umkc.edu](mailto:SC9V9@mail.umkc.edu)

- 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.



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

In the figure shown above, the following points can be derived.

- x is present in Autonomous System (AS) 4.
- Router 3c is present in AS3.
- In AS3, 3c is connected as a gateway router for AS4.
- In AS3, 4c is connected as a gateway router for AS3.
- In AS4, router 4c will have the information about x.
- In AS3, router 3c can have the information about 4c.
- Therefore 3c should get the information of x from 4c which is present outside of AS3. So, 3c uses eBGP protocol to learn about x.

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

Router 3a can learn about x from 3c as 3c already has the information of AS4. So, 3a uses iBGP to get the information of x.

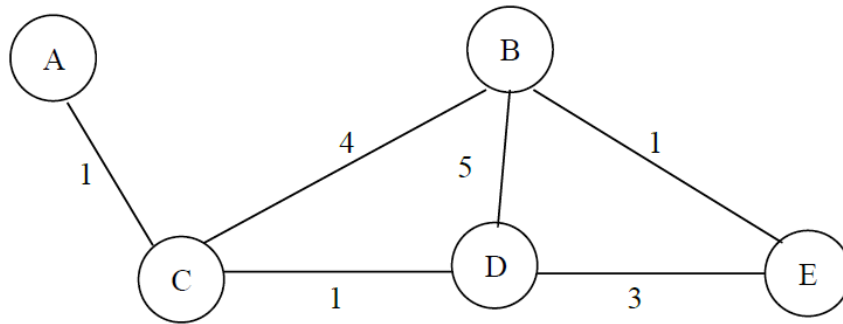
- Router 1c learns about prefix x from which routing protocol?

From the figure it can be observed that 1c is a gateway router for AS1 and 3a is the gateway router for AS3. Also, the router 3a has the information about x (from above problem (b)). Therefore, 1c uses eBGP to learn about x.

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

Router 1d can learn about x from 1c as 1c already has the information about x (from above problem (c)). Therefore 1d learns information about x using iBGP.

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



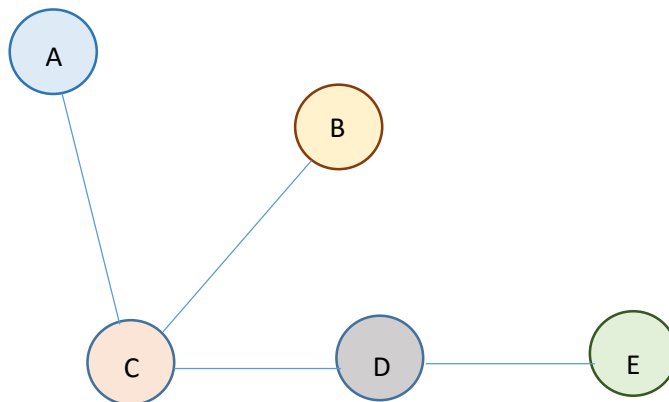
(a) Show the operation of Dijkstra's (Link State) algorithm for computing the shortest path from C to all destinations.

In the above diagram C is directly connected to B, D and A. C is connected to E through B and through D. The shortest cost path from C to E is through D. Suppose  $D(X)$  is the cost of the node  $x$  from source and  $P(Y)$  is the node predecessor to  $Y$ . For e.g.,  $P(D) = C$  or  $B$  if we are going from C to D.

Dijkstra's (Link State) algorithm operation steps:

S. No.	N	D(A), P(A)	D(B), P(B)	D(D), P(D)	D(E), P(E)
1	C	1, C	4, C	1, C	$\infty$
2	CA		4, C	1, C	$\infty$
3	CAD		4, C		4, D
4	CADB				4, D
5	CADBE				

Shortest path diagram:



Forwarding Table:

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

- (b) Show the distance table that would be computed by the distance vector algorithm in C. You don't have to show all the steps of the distance vector algorithm.

The formula for computation of path using distance vector algorithm is

$$dc(E) = \min \{ c(C, B) + dB(E), c(C, D) + dD(E), c(C, A) + dA(E) \}$$

From C To	Onto A	Onto B	Onto D
A	1	9	3
B	6	4	6
D	3	9	1
E	6	5	4

In the next step, the algorithm calculates the minimum value from each column. Therefore the minimum distances are...

From C to A is 1

From C to B is 4

From C to D is 1

From C to E is 4

### Laboratory Homework: Wireshark

In this part of the homework, you investigate the IP protocol, focusing on the IP datagram. You'll do so by analyzing a trace of IP datagrams sent and received by an execution of the traceroute (or pingplotter) program. You will inspect the various fields in the IP datagram, and study IP fragmentation in detail.

*Download a packet trace file of this homework from the Blackboard, Assignment Section. Open the trace file1 on the Wireshark, and answer to the questions below.*

In your trace, you should be able to see the series of ICMP Echo Request (Windows machine) (the UDP segment in the case of Linux/Unix) sent by the user's

computer and the ICMP Time Exceeded messages returned to the user's computer by the intermediate routers.

Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use File->Print, choose selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

*Answer to the questions below.*

## IP Datagram

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?

The image shows a Wireshark packet capture window titled 'ip-wireshark-trace-1'. The packet list on the left shows several ICMP Echo (ping) requests from source 192.168.1.102 to destination 128.59.23.100. The first packet (No. 8) is selected. The packet details pane on the right shows the expanded 'Internet Control Message Protocol' section. The 'Source' field is highlighted with a red box, showing '192.168.1.102'. The 'Destination' field shows '128.59.23.100'. The packet bytes pane at the bottom shows the raw data of the packet.

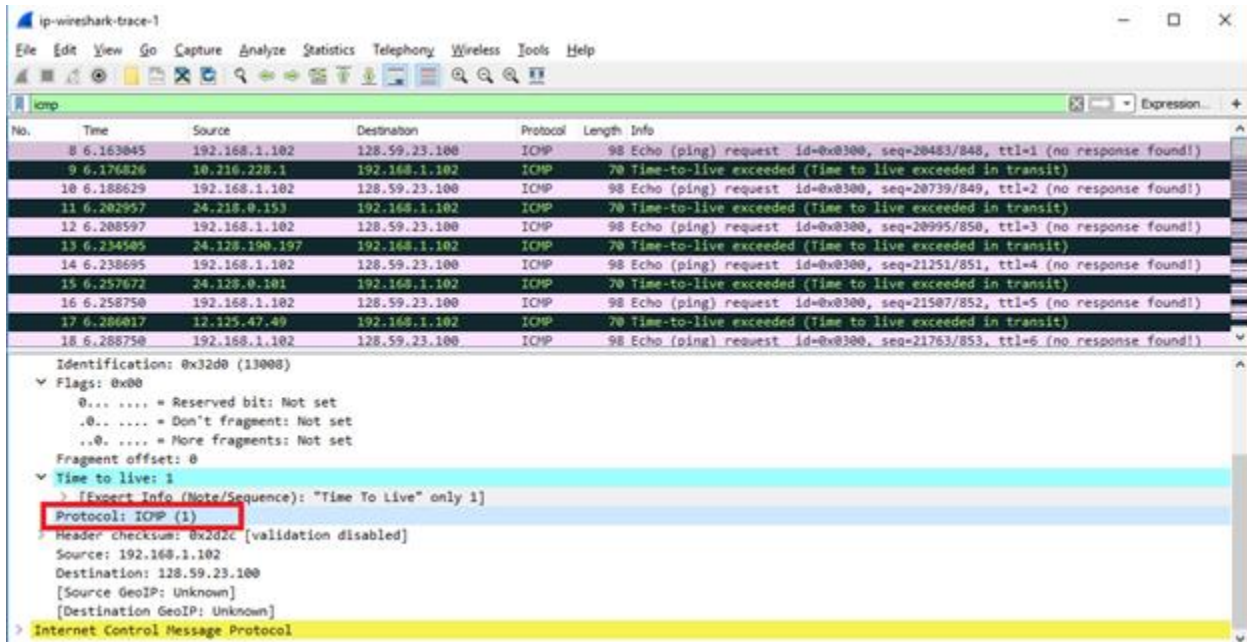
No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	6.286017	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)

Identification: 0x32d0 (13008)  
▼ Flags: 0x00  
0... .. = Reserved bit: Not set  
.0.. .... = Don't fragment: Not set  
..0. .... = More fragments: Not set  
Fragment offset: 0  
▼ Time to live: 1  
> [Expert Info (Note/Sequence): "Time To Live" only 1]  
Protocol: ICMP (1)  
> Header checksum: 0x2d2c [validation disabled]  
Source: 192.168.1.102  
Destination: 128.59.23.100  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]  
> Internet Control Message Protocol

IP address of source user's computer is 192.168.1.102

IP address of destination user's computer is 128.59.23.100

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

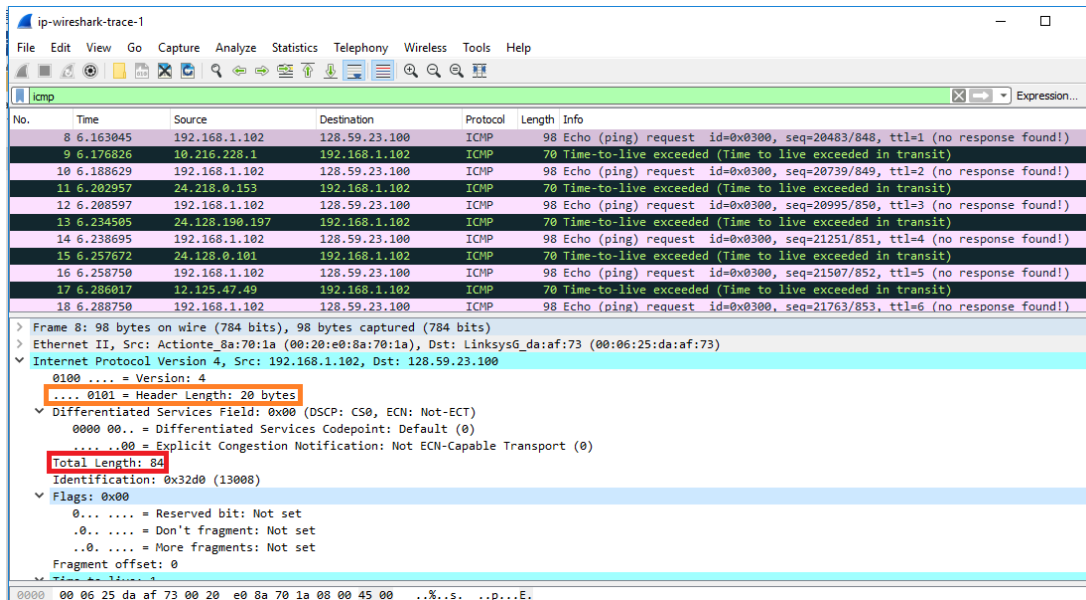


Within the IP packet header, the value in the upper layer protocol field is 1. It is highlighted in the above figure in red box.

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.

IP header contains 20 bytes (annotated in the below figure).

From the figure, it can be observed that the total length is 84 bytes. Therefore payload length is  $84 - 20 = 64$  bytes.



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

The datagram was not fragmented. From the below figure, we can identify that the flag bits are set to 0x00 (annotated in red box). Therefore, we can conclude that the datagram was not fragmented.

ip-wireshark-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
17	6.286017	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21763/853, ttl=6 (no response found!)

0000 00.. = Differentiated Services Codepoint: Default (0)  
.... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)  
Total Length: 84  
Identification: 0x32d0 (13008)  
Flags: 0x00  
0... .... = Reserved bit: Not set  
.0.. .... = Don't fragment: Not set  
..0. .... = More fragments: Not set  
Fragment offset: 0  
Time to live: 1  
> [Expert Info (Note/Sequence): "Time To Live" only 1]  
Protocol: ICMP (1)  
> Header checksum: 0x2d2c [validation disabled]

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by the computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent other protocols running on the computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by the computer.

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?

The first datagram sent by user 192.168.1.102 is of No. 8. So, let's observe the datagrams 8, 10, and 12 of this user.

ip-wireshark-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, ttl=242 (request in 368)
324	49.970589	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=46851/951, ttl=242 (request in 312)
269	44.964332	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ttl=242 (request in 257)
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
172	34.305470	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=36867/912, ttl=242 (request in 163)
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)

Identification: 0x32d0 (13008)

Flags: 0x00

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0... .. = More fragments: Not set

Fragment offset: 0

Time to live: 1

[Expert Info (Note/Sequence): "Time To Live" only 1]

["Time To Live" only 1]

[Severity level: Note]

[Group: Sequence]

Protocol: ICMP (1)

Header checksum: 0x2d2c [validation disabled]

[Good: False]

[Bad: False]

## Datagram 8

ip-wireshark-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, ttl=242 (request in 368)
324	49.970589	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=46851/951, ttl=242 (request in 312)
269	44.964332	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ttl=242 (request in 257)
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
172	34.305470	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=36867/912, ttl=242 (request in 163)
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 84

Identification: 0x32d1 (13009)

Flags: 0x00

0... .. = Reserved bit: Not set

.0... .. = Don't fragment: Not set

..0... .. = More fragments: Not set

Fragment offset: 0

Time to live: 2

[Expert Info (Note/Sequence): "Time To Live" only 2]

["Time To Live" only 2]

[Severity level: Note]

[Group: Sequence]

Protocol: ICMP (1)

Header checksum: 0x2d2c [validation disabled]

## Datagram 10



No.	Time	Source	Destination	Protocol	Length	Info
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=5 (no response found!)
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=4 (no response found!)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, ttl=242 (request in 368)
324	49.970589	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=46851/951, ttl=242 (request in 312)
269	44.964332	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ttl=242 (request in 257)
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
172	34.305470	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=36867/912, ttl=242 (request in 163)
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=242 (request in 122)

0000 00.. = Differentiated Services Codepoint: Default (0)  
 .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)  
 Total Length: 84  
 Identification: 0x32d2 (13010)  
 Flags: 0x00  
 0... .. = Reserved bit: Not set  
 .0.. .. = Don't fragment: Not set  
 ..0. .. = More fragments: Not set  
 Fragment offset: 0  
 Time to live: 3  
 [Expert Info (Note/Sequence): "Time To Live" only 3]  
 ["Time To Live" only 3]  
 [Severity level: Note]  
 [Group: Sequence]  
 Protocol: ICMP (1)

## Datagram 12

From the above figures, we can find that the fields Identification, Checksum and Time To Live are changing from one datagram to the next datagram.

- Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Below are the screenshots of the packets 8, 10 and 12 of the user 192.168.1.102.

## Datagram 8:

No.	Time	Source	Destination	Protocol	Length	Info
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, t
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, t
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, t
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, t
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, t
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, t
324	49.970589	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=46851/951, t
269	44.964332	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, t
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, t
172	34.305470	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=36867/912, t
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, t

> 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  
 > 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: 0xd2c [validation disabled]  
 Source: 192.168.1.102  
 Destination: 128.59.23.100  
 [Source GeoIP: Unknown]  
 [Destination GeoIP: Unknown]

## Datagram 10:

ip-wireshark-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ttl=...
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ttl=...
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=...
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=...
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=...
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, ttl=...
324	49.970589	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=46851/951, ttl=...
269	44.964332	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ttl=...
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ttl=...
172	34.305470	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=36867/912, ttl=...
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ttl=...

> Frame 10: 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

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

Total Length: 84

Identification: 0x32d1 (13009)

> Flags: 0x00

Fragment offset: 0

> Time to live: 2

Protocol: ICMP (1)

> Header checksum: 0x2c2b [validation disabled]

Source: 192.168.1.102

Destination: 128.59.23.100

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

## Datagram 12:

ip-wireshark-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21507/852, ...
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=21251/851, ...
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ...
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ...
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ...
380	54.973666	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=50179/964, ...
324	49.970589	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=46851/951, ...
269	44.964332	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ...
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=40195/925, ...
172	34.305470	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=36867/912, ...
131	29.299545	128.59.23.100	192.168.1.102	ICMP	562	Echo (ping) reply id=0x0300, seq=33539/899, ...

> Frame 12: 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

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

Total Length: 84

Identification: 0x32d2 (13010)

> Flags: 0x00

Fragment offset: 0

> Time to live: 3

Protocol: ICMP (1)

> Header checksum: 0x2b2a [validation disabled]

Source: 192.168.1.102

Destination: 128.59.23.100

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Here the user is sending request to the same destination and the type of requests is same. Therefore the fields like version, header length, fragment offset, source address, destination address, total length, flags must remain same for all the datagrams.

Frame number, identification, time to live, header checksum fields should be changed for each datagram because each packet will have different identifications, time to live and also the checksums are generated based on the datagram content.

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 TTL exceeded replies sent to the computer by the nearest (first hop) router.

Identification field value of IP datagram is being increased by 1.

Below is the screenshot of the datagram that has Time To Live Exceeded replies sent to the user's computer.

ip-wireshark-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
330	53.501082	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
274	48.493073	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
179	38.491817	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
135	33.470548	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
65	16.179649	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
40	11.174495	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

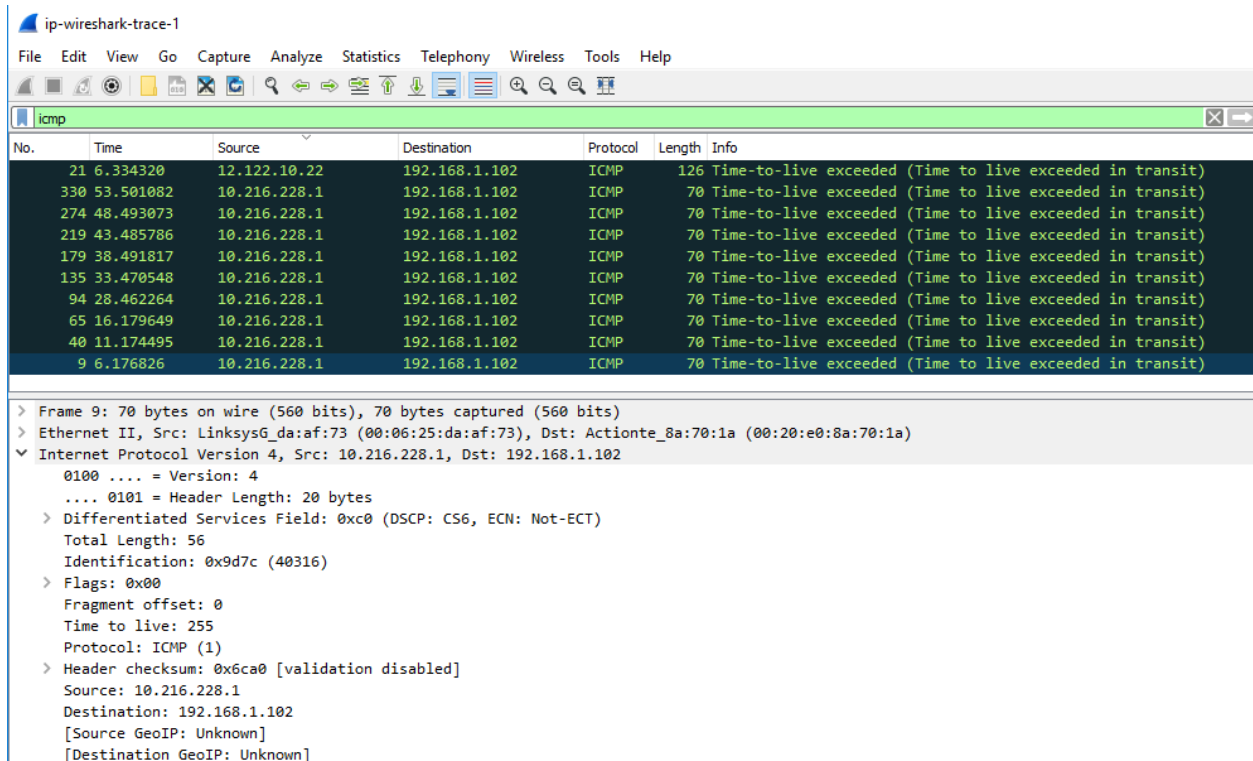
> Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Ethernet II, Src: LinksysG\_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: 10.216.228.1, Dst: 192.168.1.102

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes
- > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
- Total Length: 56
- Identification: 0x9d7c (40316)
- > Flags: 0x00
- Fragment offset: 0
- Time to live: 255
- Protocol: ICMP (1)
- > Header checksum: 0x6ca0 [validation disabled]
- Source: 10.216.228.1
- Destination: 192.168.1.102
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

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



The image shows a Wireshark capture of ICMP messages. The packet list pane displays several ICMP messages, all with the 'Time-to-live exceeded' status. The packet details pane for the selected packet (No. 9) shows the following fields:

- Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
- Ethernet II, Src: Linksys6\_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: 10.216.228.1, Dst: 192.168.1.102
  - Version: 4
  - Header Length: 20 bytes
  - Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  - Total Length: 56
  - Identification: 0x9d7c (40316)
  - Flags: 0x00
  - Fragment offset: 0
  - Time to live: 255
  - Protocol: ICMP (1)
  - Header checksum: 0x6ca0 [validation disabled]
  - Source: 10.216.228.1
  - Destination: 192.168.1.102
  - [Source GeoIP: Unknown]
  - [Destination GeoIP: Unknown]

Value in identification field: 0x9d7c (40316)

Time to Live: 255

## 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?

Time To Live field remains unchanged and the Identification field values changes for all the ICMP messages that have TTL exceeded replies sent to the user's computer. This is because the router did not receive any datagram.