

CSE 3300 - Homework 4

Prof. Bing Wang

Nicholas Lambourne - 2749404 - ndl17004

Problem 1

1. 223.1.17.0/26
2. 223.1.17.64/26
3. 223.1.17.128/25

Problem 2

Dijkstra's Algorithm (Working)

Step	N^i (visited)	$D, p(y)$	$D, p(w)$	$D, p(v)$	$D, p(z)$	$D, p(t)$	$D, p(u)$	$D, p(s)$
0	x	6,x	1,x	3,x	∞	∞	∞	∞
1	xw	6,x		2,w	∞	∞	4,w	∞
2	xwv	3,v			∞	11,v	3,v	∞
3	xwvy				17,y	7,y		∞
4	xwvyu				17,y	5,u		7,u
5	xwvyut				7,t			6,t
6	xwvyuts							
7	xwvyutsz							

Shortest Paths From Node x

Node	Shortest Path	Length
x	x	0
y	xwvy	3
w	xw	1
v	xwv	2
z	xwvutz	7
t	xwvut	5
u	XWVU	3
s	xwvuts	6

Problem 3

Node A Table

T = 1

	A	B	C
A	0	5	1
B	∞	∞	∞
C	∞	∞	∞

T = 2

	A	B	C
A	0	5	1
B	5	0	7
C	1	7	0

T = 3

	A	B	C
A	0	5	1
B	5	0	6
C	1	6	0

Node B Table

T = 1

	A	B	C
A	∞	∞	∞
B	5	0	7
C	∞	∞	∞

T = 2

	A	B	C
A	0	5	1
B	5	0	6
C	1	7	0

T = 3

	A	B	C

	A	B	C
A	0	5	1
B	5	0	6
C	1	6	0

Node C Table

T = 1

	A	B	C
A	∞	∞	∞
B	∞	∞	∞
C	1	7	0

T = 2

	A	B	C
A	0	5	1
B	5	0	7
C	1	6	0

T = 3

	A	B	C
A	0	5	1
B	5	0	6
C	1	6	0

Convergent Table (T=3)

	A	B	C
A	0	5	1
B	5	0	6
C	1	6	0

Problem 4

a) Maximum Throughput (Single Node)

- TDMA: $\frac{C}{N}$
- CSMA: C
- Slotted Aloha: C
- Token Passing: C (Assuming zero transmission time of token).

b) Aggregate Throughput (All Nodes)

- TDMA: C is achievable when all nodes are transmitting in all slots.
- CSMA: C is not achievable when there is a non-zero propagation delay between nodes. Maximum throughput is $\frac{1}{1+5P/d_{trans}} \cdot C$. Due to collisions.
- Slotted Aloha: Cannot achieve throughput of C , maximum efficiency limited to $Np(1 - p)^{N-1}$ of C due to collisions.
- Token Passing: C is achievable.

Problem 5

a) Network adapters have been added as red bars on each interface in the image below.

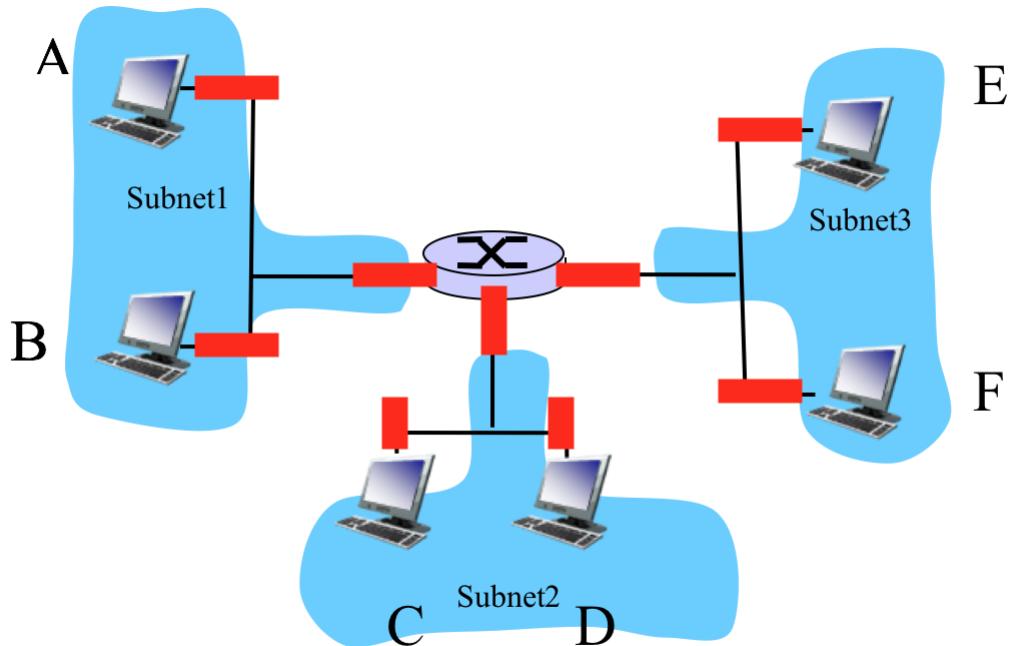


Fig. 3: Three LANs connected by a router.

b) In the image below, the network interfaces have been assigned IP addresses. Note: the addresses specified for subnet 3 are invalid, as each block of an IP address is made of 8 bits, which means a maximum value of 255 ($2^8 - 1$), less than the specified 333.

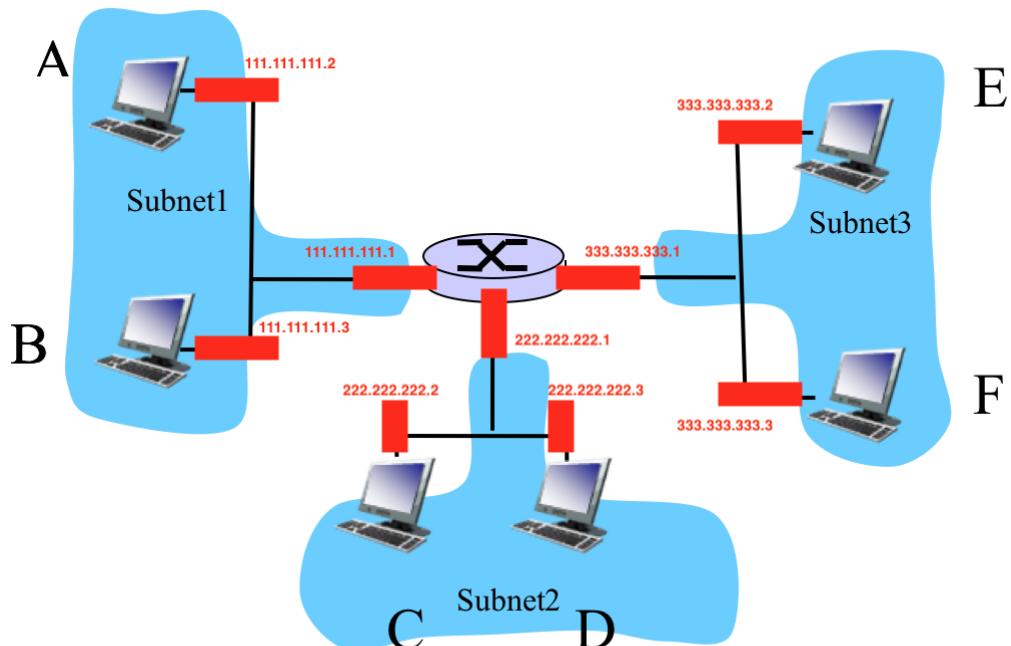


Fig. 3: Three LANs connected by a router.

c) In the image below, each network adapter has been assigned a unique MAC address.

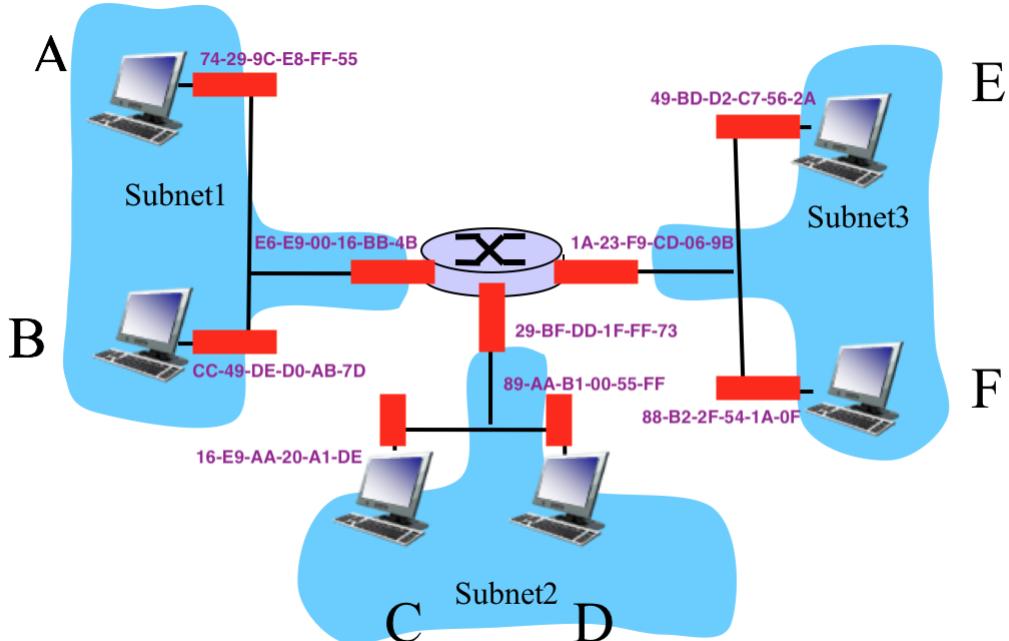


Fig. 3: Three LANs connected by a router.

d) If the ARP tables are up to date then the process for sending an IP datagram from A to F is as follows:

- A creates an IP datagram with IP source A, destination F.
- A creates a link-layer frame with the MAC address of the central router, containing the A-F IP datagram.
- The frame is sent from A to the central router, where the datagram is removed and passed up to the IP layer.
- The central router then takes the IP datagram and includes it as the payload in a new link-layer frame with F's MAC address as the destination (and forwards it to host F).
- When the frame reaches host F, the link-layer frame is stripped off and the datagram is passed to the IP layer.

e) If the ARP tables in the sending host (A) are empty, it will need to conduct additional steps in order to route the IP datagram to host F:

- A broadcasts an ARP query containing B's IP address to all nodes in the LAN.
- It will receive a response from the central router (which has a cached copy of the IP-MAC mapping for host F - if DHCP is being used F gets its IP assigned from the central router) with the MAC for F.
- Then the process will in d (above) will start and continue as described.

Problem 6 - Wireshark IP Lab

- 1) The source IP was 192.168.1.102 (image below).

ip-ethereal-trace-1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Telebit_73:8d..	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no route to host)
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 route to host)
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 route to host)
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 route to host)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

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

- 2) The value in the upper layer protocol field is 0x01 (the code for ICMP - image below).

ip-ethereal-trace-1

Apply a display filter ... <%>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Telebit_73:8d...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no route to host)
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 route to host)
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 route to host)
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 route to host)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

► Ethernet II, Src: PremaxPe_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]

3) The header length was 20 bytes, the payload is the total length minus the header (84-20), 64 bytes (see image below)

ip-ethereal-trace-1

Apply a display filter ... <Expression...>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Telebit_73:8d...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no route to host)
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 route to host)
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 route to host)
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 route to host)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

► Ethernet II, Src: PremaxPe_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

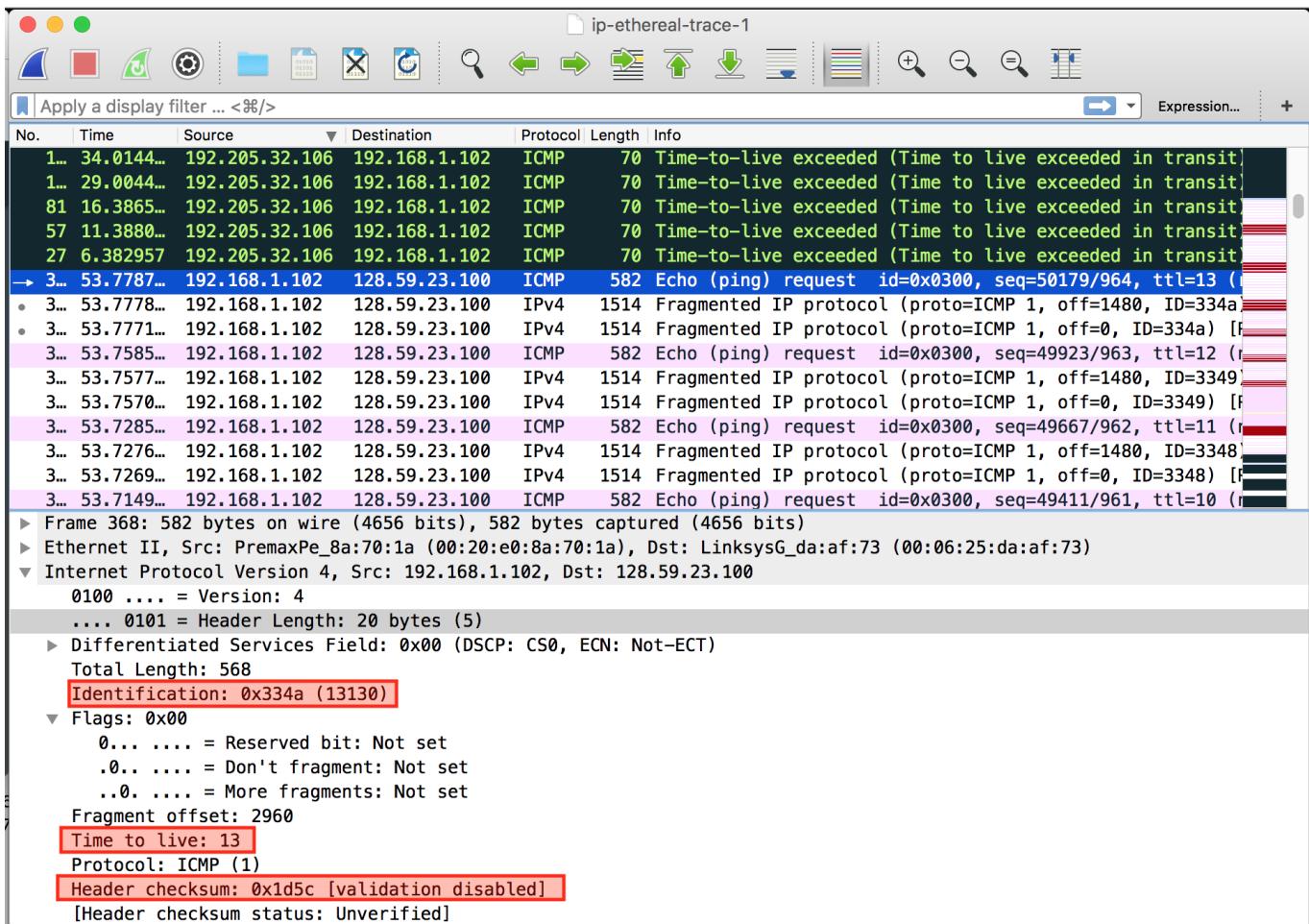
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x32d0 (13008)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0xd2c [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.102
- Destination: 128.59.23.100
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

4) The IP datagram has not been fragmented, this is evidenced by the "More fragments" bit not being set (see image below).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Telebit_73:8d..	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
2	4.866867	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
3	4.868147	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no route to host)
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 route to host)
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 route to host)
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 route to host)
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

► Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 ► Ethernet II, Src: PremaxPe_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
 0.... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 0
 ► Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x2d2c [validation disabled]
 [Header checksum status: Unverified]

5) Between subsequent packets, the Identification, Header Checksum and Time To Live (TTL) always change.



6) The following fields all (must) stay constant (blue) between all datagrams:

- IP Version: the IP is always version 4.
- Header Length: the header itself does not change.
- Destination IP: the destination is always the same (though not all packets get to it - by design).
- Source IP: the source never changes, every packet is sent from the same requesting machine.
- Upper Layer Protocol (ICMP): every datagram is an ICMP request.

The fields that must change between datagrams (red) are:

- ID
- Header Checksum
- TTL

7) With each ICMP echo request, the IP datagram Identification field increments by one in hexadecimal (two examples are included below).

Identification: 0x3349 (13129)

Identification: 0x334a (13130)

8) The value in the ID field is always different (by nature, e.g. 0x9d7c = 40316) and the TTL value is always 255 (see image below).

Screenshot of Wireshark showing network traffic analysis. The main pane displays a list of captured frames, with frame 9 selected. Frame 9 is an ICMP message with the following details:

- 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: PremaxPe_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 (5)**
 - Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)**
 - Total Length: 56**
 - Identification: 0x9d7c (40316)**
 - Flags: 0x00**
 - 0... = Reserved bit: Not set**
 - .0.. = Don't fragment: Not set**
 - ..0. = More fragments: Not set**
 - Fragment offset: 0**
 - Time to live: 255**
 - Protocol: ICMP (1)**
 - Header checksum: 0x6ca0 [validation disabled]**
 - [Header checksum status: Unverified]**
- Hex dump:**

0000	00 20 e0 8a 70 1a 00 06	25 da af 73 08 00 45 c0	. . . p . . . % . . s . . E .
0010	00 38 9d 7c 00 00 ff 01	6c a0 0a d8 e4 01 c0 a8	. 8 l
0020	01 66 0b 00 d9 46 00 00	00 00 45 00 00 54 32 d0	. f . . F E . . T2 . .
0030	00 00 01 01 f6 16 c0 a8	01 66 80 3b 17 64 08 00 f ; . d
0040	f7 ca 03 00 50 03	 p
- Don't fragment (ip.flags.df), 1 byte**
- Packets: 380 · Displayed: 380 (100.0%) · Load time: 0:0.15 · Profile: Default**

9) The TTL always stays the same for the nearest hop router, because the number of hops to it is always the same. The identification value is always different because it uniquely identifies the response (the same ID for two datagrams indicates that they are both fragments of the same message).

10) Yes, the message has been fragmented across two IP datagrams (see image below).

ip-ethereal-trace-1

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
84	16.4180...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (n)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (n)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (n)
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [F]
93	28.4421...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (n)
94	28.4622...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [F]
96	28.4713...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (n)
97	28.4906...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [F]
98	28.4913...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (n)

Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: PremaxPe_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: 1500
Identification: 0x32f9 (13049)
Flags: 0x01 (More Fragments)
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..1.... = More fragments: Set
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x077b [validation disabled]
[Header checksum status: Unverified]

11) The fact that the 'More Fragments' bit has been set signifies that it has been fragmented. The fact that this is the first fragment is signified by the fact that the fragment offset is 0. This IP datagram is 1500 bytes in length (see image below).

ip-ethereal-trace-1

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
84	16.4180...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (n)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (n)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (n)
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [F]
93	28.4421...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (n)
94	28.4622...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [F]
96	28.4713...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (n)
97	28.4906...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [F]
98	28.4913...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (n)

Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: PremaxPe_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: 1500
Identification: 0x32f9 (13049)
Flags: 0x01 (More Fragments)
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..1.... = More fragments: Set
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x077b [validation disabled]
[Header checksum status: Unverified]

12) The fact there is a non-zero (1480) Fragment Offset indicates that this is not the first datagram fragment. There are no more fragments because the 'More Fragments' bit is not set (see image below).

No.	Time	Source	Destination	Protocol	Length	Info
84	16.4180...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no payload)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (no payload)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (no payload)
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
• 92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Frag 1/1]
• 93	28.4421...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no payload)
94	28.4622...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Frag 2/1]
96	28.4713...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no payload)
97	28.4906...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Frag 3/1]
98	28.4913...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no payload)

Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: PremaxPe_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: 548
 Identification: 0x32f9 (13049)
 Flags: 0x00
 0.... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 1480
 Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x2a7a [validation disabled]
[Header checksum status: Unverified]

13) The length, the more fragments bit, the fragment offset and the header checksum change between the first and second fragments (see images below).

ip-ethereal-trace-1

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
84	16.4180...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no payload)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (no payload)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (no payload)
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Frag 1/3]
93	28.4421...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no payload)
94	28.4622...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Frag 2/3]
96	28.4713...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no payload)
97	28.4906...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Frag 3/3]
98	28.4913...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no payload)

▶ Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
 ▶ Ethernet II, Src: PremaxPe_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: 1500
 Identification: 0x32f9 (13049)
 ▶ Flags: 0x01 (More Fragments)
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..1.... = More fragments: Set
 Fragment offset: 0
 ▶ Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x077b [validation disabled]
 [Header checksum status: Unverified]

ip-ethereal-trace-1

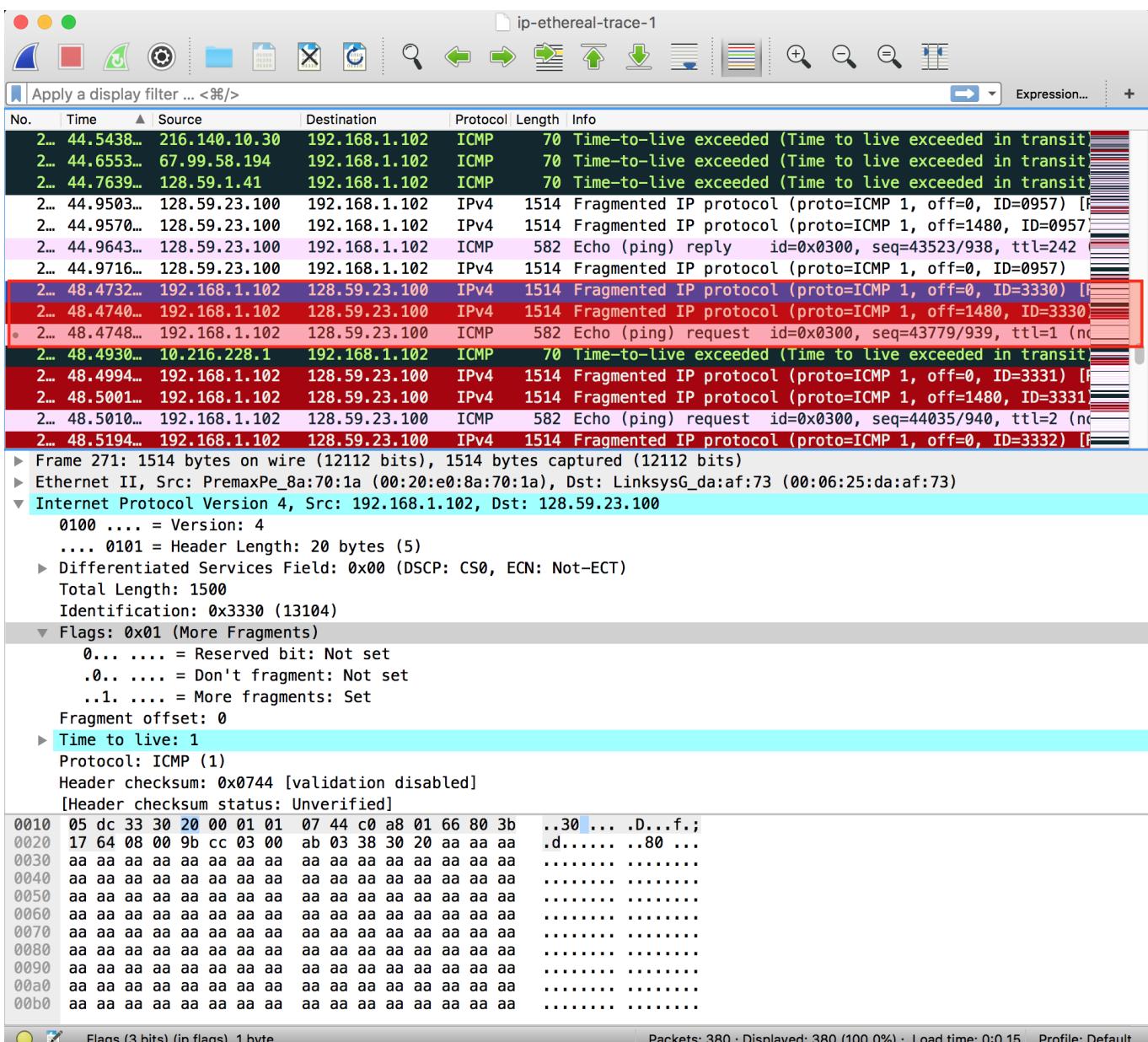
Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
84	16.4180...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	16.4382...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	16.4433...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=29955/885, ttl=12 (no payload)
87	16.4633...	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=30211/886, ttl=13 (no payload)
88	16.4686...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	16.4999...	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, seq=30211/886, ttl=242 (no payload)
90	22.9280...	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.9527...	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0
92	28.4415...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Frag 1/3]
93	28.4421...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no payload)
94	28.4622...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	28.4706...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Frag 2/3]
96	28.4713...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no payload)
97	28.4906...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Frag 3/3]
98	28.4913...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no payload)

▶ Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
 ▶ Ethernet II, Src: PremaxPe_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: 548
 Identification: 0x32f9 (13049)
 ▶ Flags: 0x00
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0.... = More fragments: Not set
 Fragment offset: 1480
 ▶ Time to live: 1
 Protocol: ICMP (1)
 Header checksum: 0x2a7a [validation disabled]
 [Header checksum status: Unverified]

14) For a packet size of 3500, there are three fragments made from the original datagram (see image below).



- 15) The the fragment offset and the header checksum change between the first and second fragments (see images below). The length, more fragments bit, the fragment offset bit change between the second and third fragments.

ip-ethereal-trace-1

Apply a display filter ... <%>/ Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
2...	44.5438...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	44.6553...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	44.7639...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	44.9503...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957) [F]
2...	44.9570...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0957) [F]
2...	44.9643...	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ttl=242
2...	44.9716...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957)
2...	48.4732...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3330) [F]
2...	48.4740...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3330) [F]
2...	48.4748...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=43779/939, ttl=1 (no route to host)
2...	48.4930...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	48.4994...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3331) [F]
2...	48.5001...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3331) [F]
2...	48.5010...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=44035/940, ttl=2 (no route to host)
2...	48.5194...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3332) [F]

Frame 271: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: PremaxPe_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: 1500
Identification: 0x3330 (13104)
Flags: 0x01 (More Fragments)
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..1.... = More fragments: Set
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0744 [validation disabled]
[Header checksum status: Unverified]

ip-ethereal-trace-1

Apply a display filter ... <%>/ Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
2...	44.5438...	216.140.10.30	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	44.6553...	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	44.7639...	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2...	44.9503...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957) [F]
2...	44.9570...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0957) [F]
2...	44.9643...	128.59.23.100	192.168.1.102	ICMP	582	Echo (ping) reply id=0x0300, seq=43523/938, ttl=242
2...	44.9716...	128.59.23.100	192.168.1.102	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=0957)
2...	48.4732...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3330) [F]
2...	48.4740...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3330) [F]
2...	48.4748...	192.168.1.102	128.59.23.100	ICMP	582	Echo (ping) request id=0x0300, seq=43779/939, ttl=1 (no route to host)

In []: