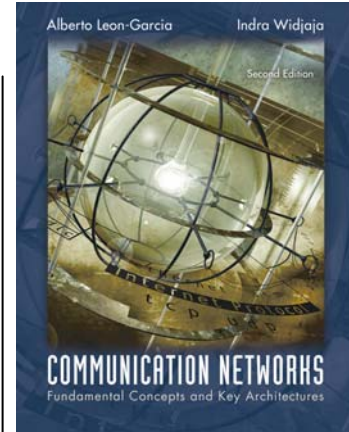
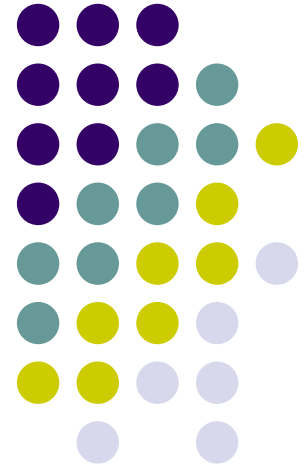


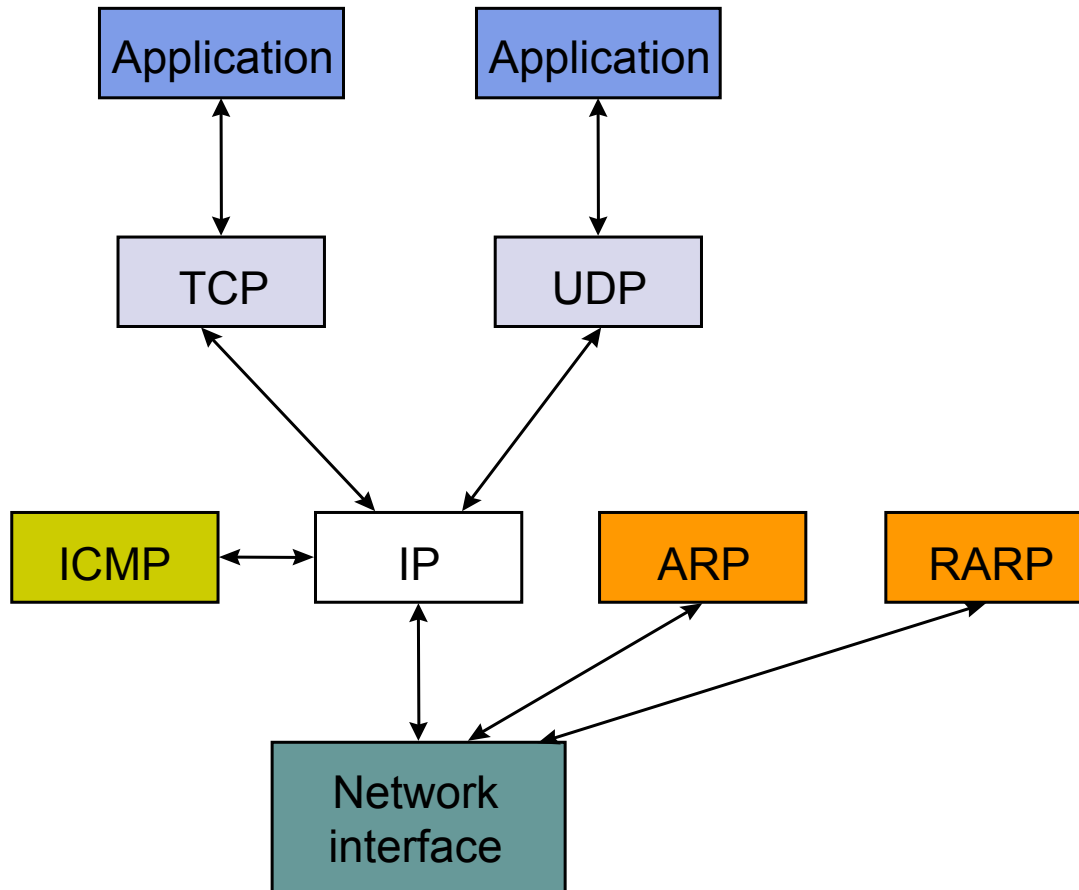
Chapter 8

TCP/IP



Chapter Figures

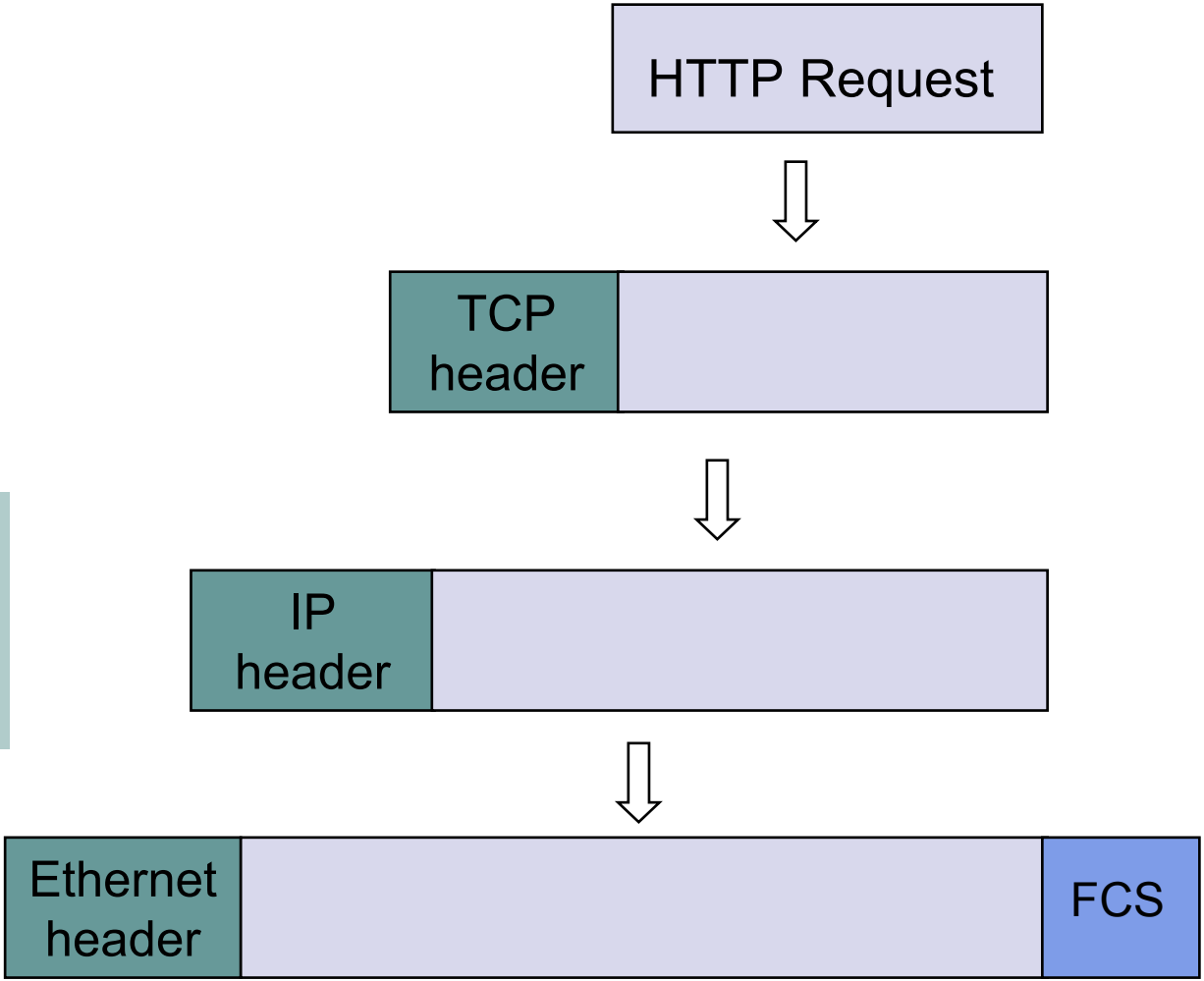


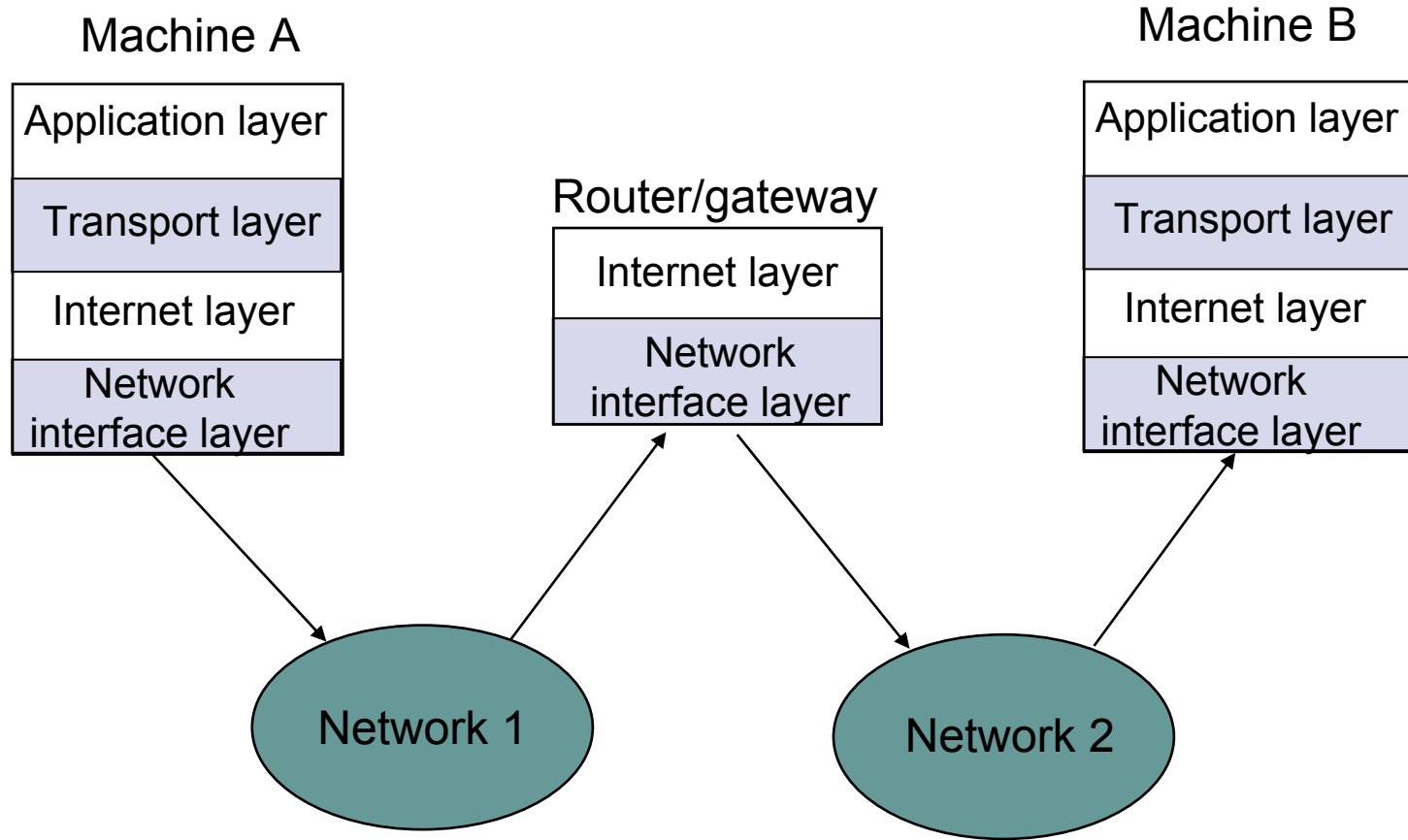


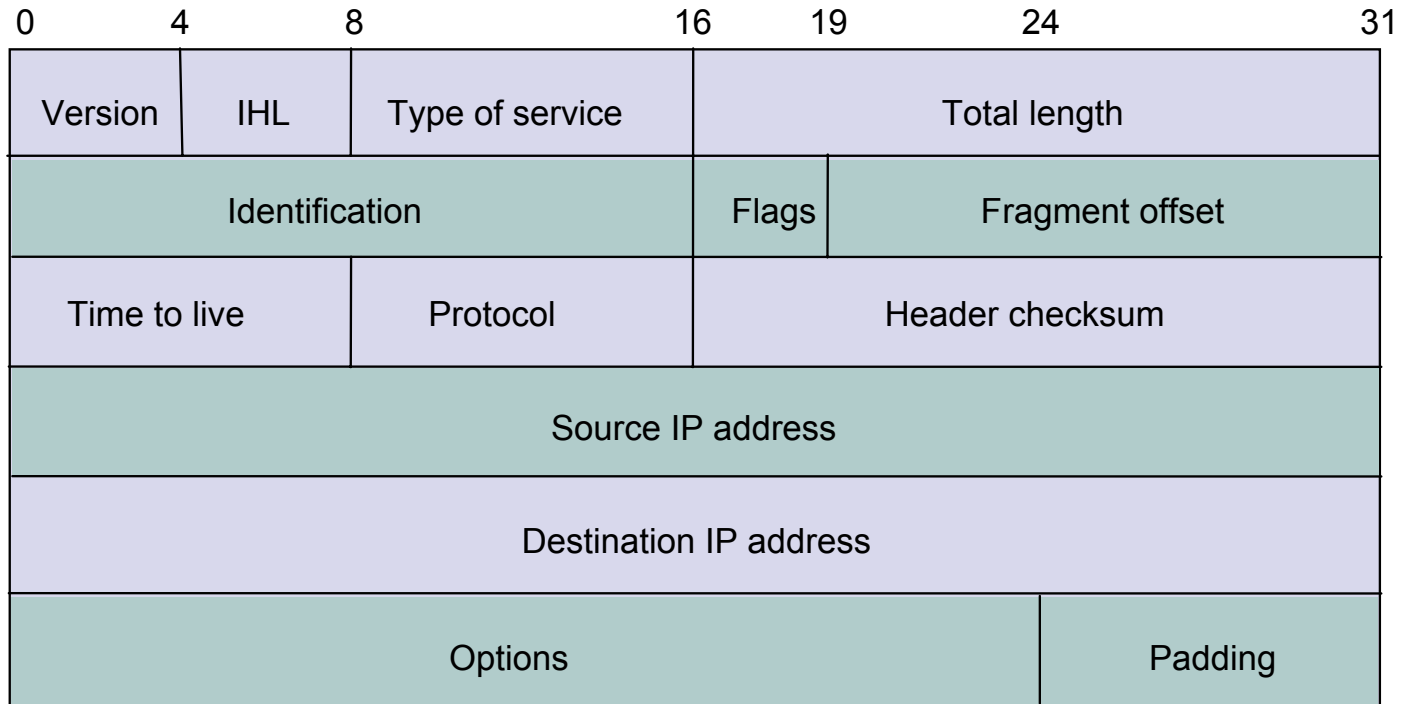
Header contains source & destination port numbers

Header contains source and destination IP addresses; transport protocol type

Header contains source & destination physical addresses; network protocol type







smtplex - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	66.185.95.99	192.168.2.18	SMTP	Response: 220 fep03-mail.bloor.is.net.cable.rogers.com ESMT
2	0.001316	192.168.2.18	66.185.95.99	SMTP	Command: EHLO rogers.com
3	0.041956	66.185.95.99	192.168.2.18	SMTP	Response: 250-fep03-mail.bloor.is.net.cable.rogers.com
4	0.043166	192.168.2.18	66.185.95.99	SMTP	Command: AUTH PLAIN AGTjyXJsewxlQHJvZ2vycy5jb20AY3IwY3VZ
5	0.094338	66.185.95.99	192.168.2.18	SMTP	Response: 235 Authentication successful
6	0.103503	192.168.2.18	66.185.95.99	SMTP	Command: MAIL FROM:[REDACTED]@rogers.com>
7	0.152871	66.185.95.99	192.168.2.18	SMTP	Response: 250 Sender [REDACTED]@rogers.com> ok
8	0.153959	192.168.2.18	66.185.95.99	SMTP	Command: RCPT TO:<alg@accelight.com>
9	0.187072	66.185.95.99	192.168.2.18	SMTP	Response: 250 Recipient <alg@accelight.com> ok
10	0.188325	192.168.2.18	66.185.95.99	SMTP	Command: DATA
11	0.207439	66.185.95.99	192.168.2.18	SMTP	Response: 354 Ok Send data ending with <CRLF>.<CRLF>
12	0.214523	192.168.2.18	66.185.95.99	SMTP	Message Body

.....

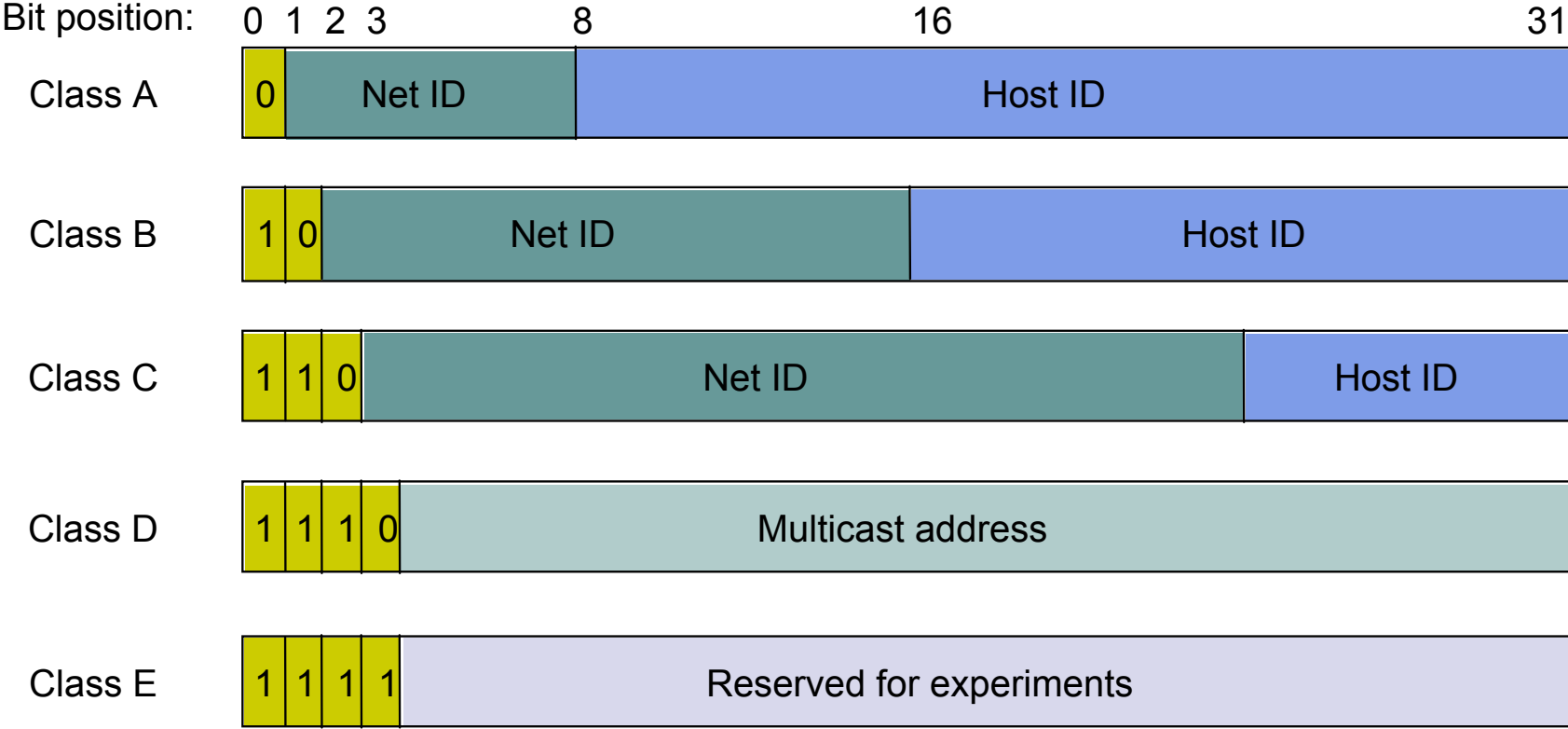
Frame 1 (205 bytes on wire, 205 bytes captured)
 Ethernet II, Src: 00:04:e2:29:b2:3a, Dst: 00:01:03:1d:cc:f7
 Internet Protocol, Src Addr: 66.185.95.99 (66.185.95.99), Dst Addr: 192.168.2.18 (192.168.2.18)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total Length: 191
 Identification: 0x664a
 Flags: 0x04
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 Fragment offset: 0
 Time to live: 53
 Protocol: TCP (0x06)
 Header checksum: 0x7a18 (correct)
 Source: 66.185.95.99 (66.185.95.99)
 Destination: 192.168.2.18 (192.168.2.18)
 Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1187 (1187), Seq: 2389398210, Ack: 9094119, Len: 151
 Simple Mail Transfer Protocol

.....

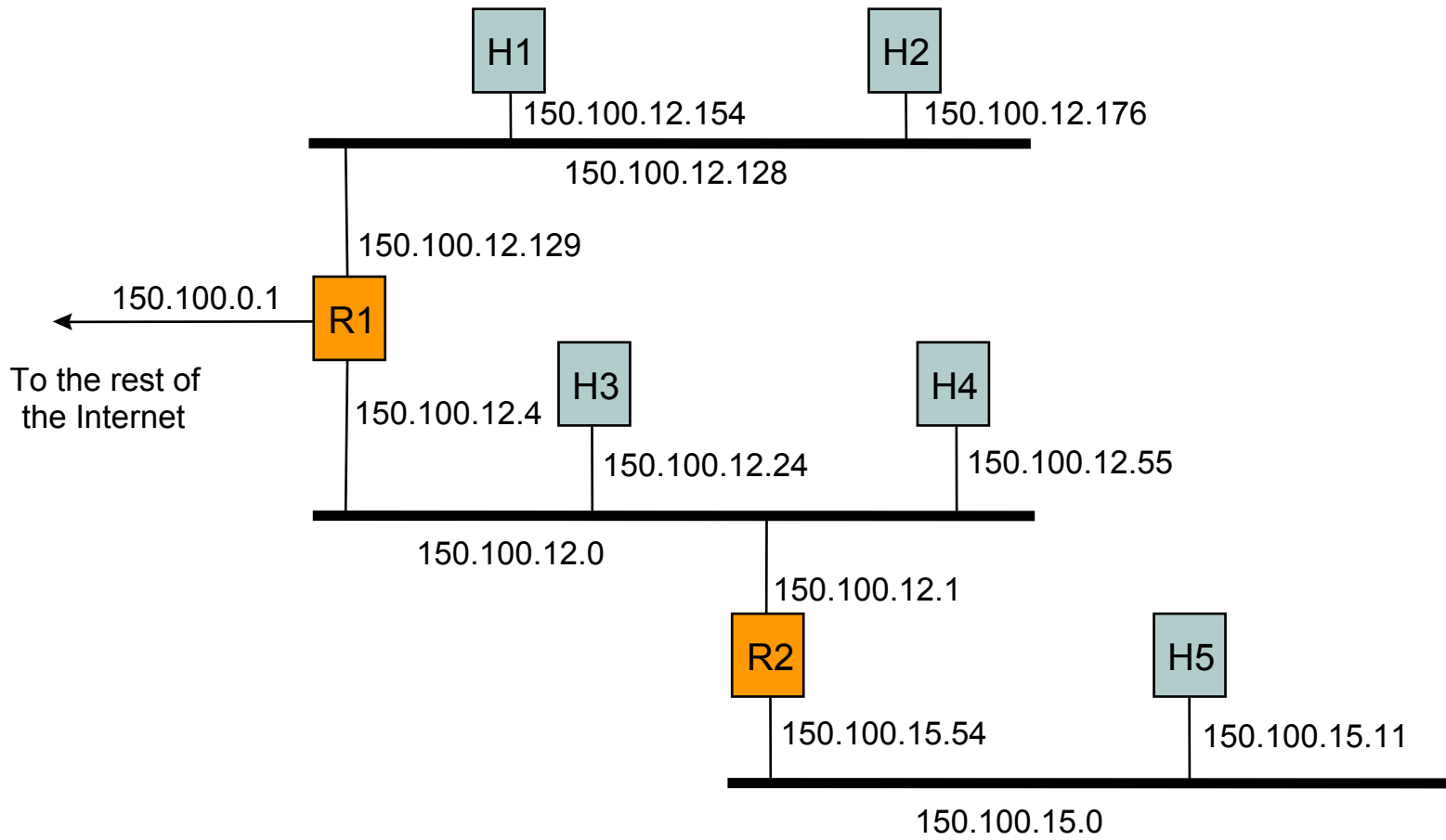
```

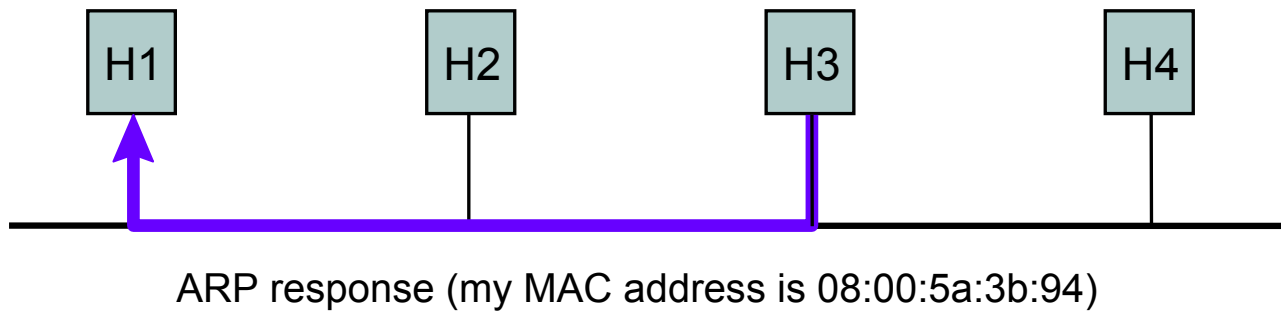
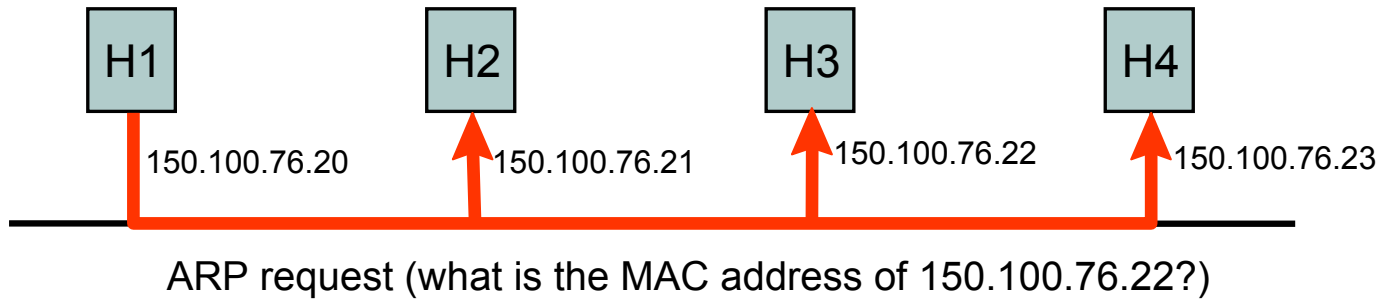
0000  00 01 03 1d cc f7 00 04 e2 29 b2 3a 08 00 45 00  .... .).:..E.
0010  00 bf 66 4a 40 00 35 06 7a 18 42 b9 5f 63 c0 a8  ..fj@.5. z.B._c..
0020  02 12 00 19 04 a3 8e 6b 52 c2 00 8a c3 e7 50 18  ....k R.....P.
0030  f0 00 1d 45 00 00 32 32 30 20 66 65 70 30 33 2d  ...E..22 0 fep03-
0040  6d 61 69 6c 2e 62 6c 6f 6f 72 2e 69 73 2e 6e 65  mail.blo or.is.ne
  
```

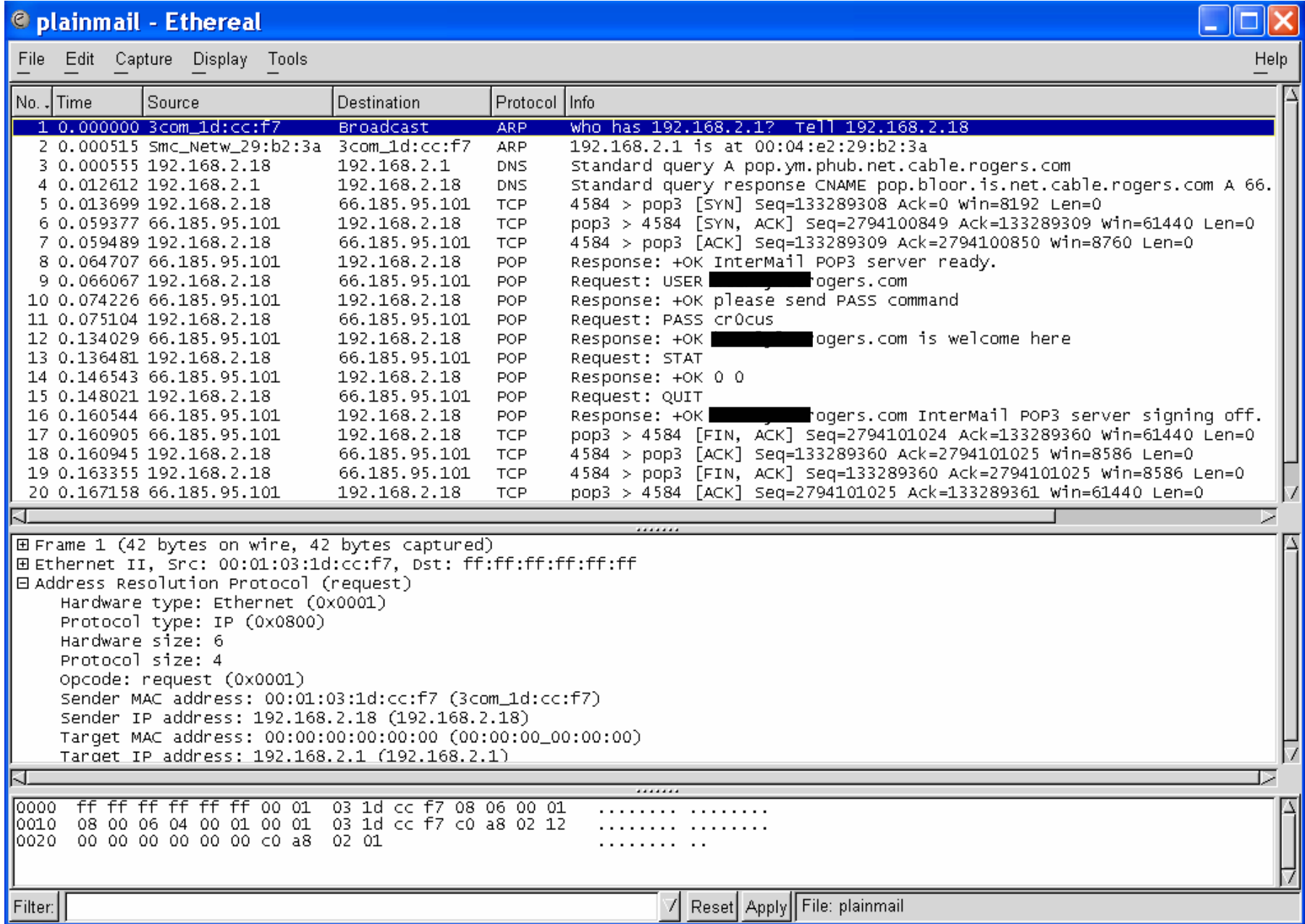
Filter: / Reset Apply File: smtplex

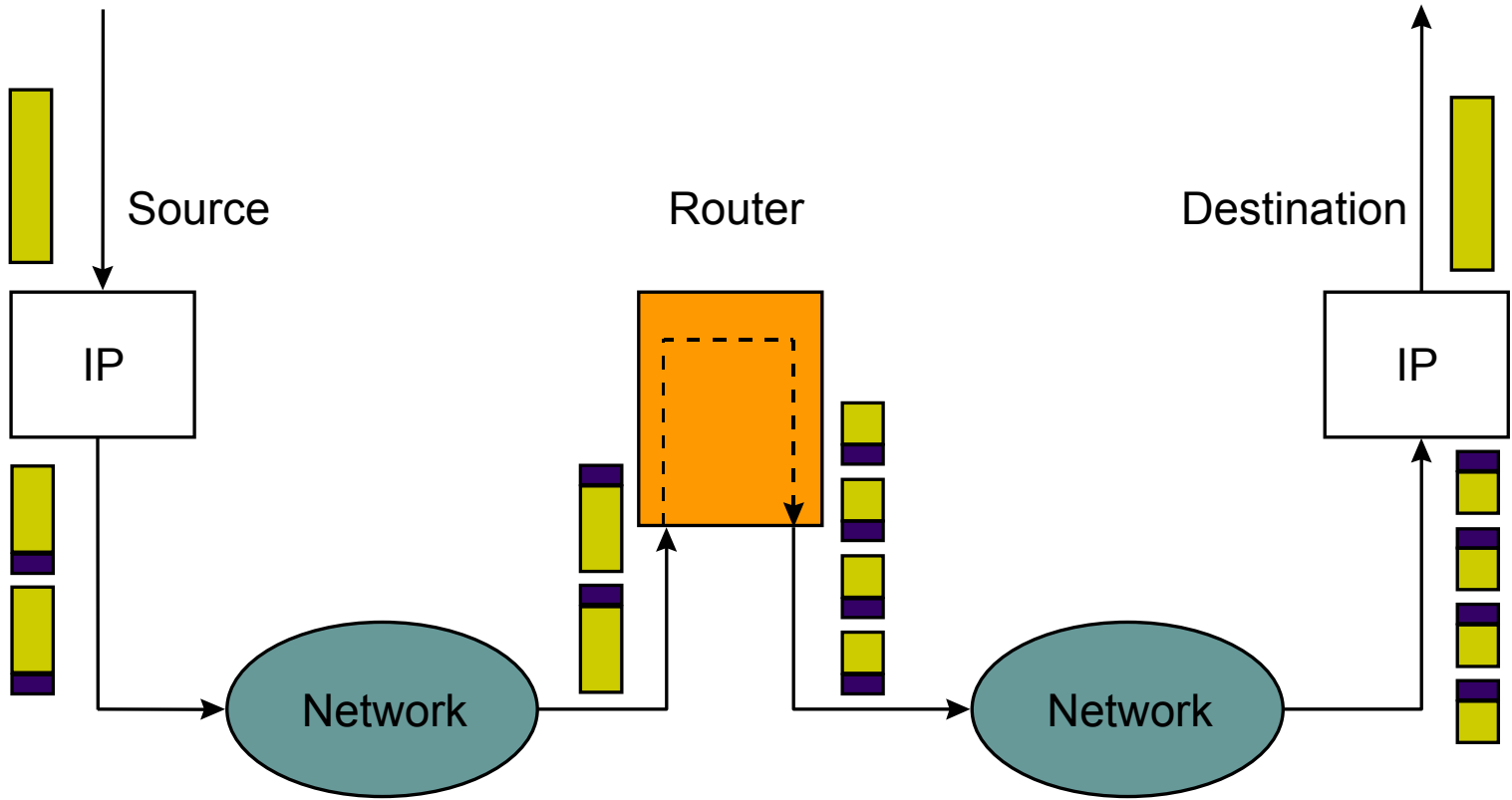


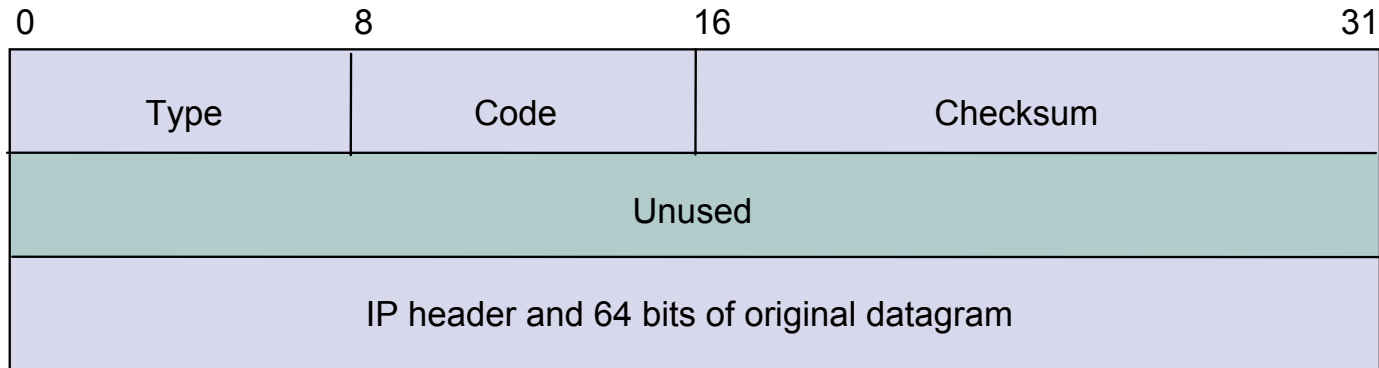


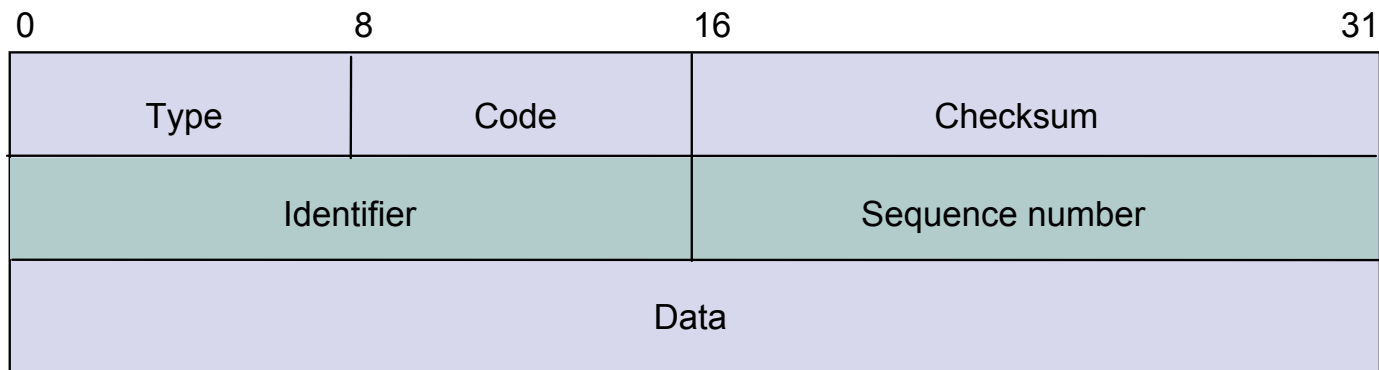












pingtesla - Ethereal

File Edit Capture Display Tools Help

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	00000000.0001031dccf7	00000000.Broadcast	IPX SAP	Nearest Query
2	13.526454	192.168.2.18	192.168.2.1	DNS	Standard query A tesla.comm.utoronto.ca
3	13.534545	192.168.2.1	192.168.2.18	DNS	Standard query response A 128.100.11.1
4	13.541026	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
5	13.555913	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
6	14.542842	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
7	14.567211	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
8	15.547669	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
9	15.586209	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
10	16.552528	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
11	16.565526	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
12	22.941534	192.168.2.18	192.168.2.255	BROWSER	Domain/workgroup Announcement @HOME, windows for wor

.....

Frame 4 (74 bytes on wire, 74 bytes captured)
 Ethernet II, Src: 00:01:03:1d:cc:f7, Dst: 00:04:e2:29:b2:3a
 Internet Protocol, Src Addr: 192.168.2.18 (192.168.2.18), Dst Addr: 128.100.11.1 (128.100.11.1)
 Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xf05b (correct)
 Identifier: 0x0200
 Sequence number: 5b:00
 Data (32 bytes)

.....

0000	00 04 e2 29 b2 3a 00 01 03 1d cc f7 08 00 45 00	...).:... ..E.
0010	00 3c 19 8a 00 00 20 01 33 18 c0 a8 02 12 80 64	.<.... . 3.....d
0020	0b 01 08 00 f0 5b 02 00 5b 00 61 62 63 64 65 66[. [.abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

Filter: Reset Apply File: pingtesla

pingtesla - Ethereal

File Edit Capture Display Tools Help

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	00000000.0001031dccb7	00000000.Broadcast	IPX SAP	Nearest Query
2	13.526454	192.168.2.18	192.168.2.1	DNS	Standard query A tesla.comm.utoronto.ca
3	13.534545	192.168.2.1	192.168.2.18	DNS	Standard query response A 128.100.11.1
4	13.541026	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
5	13.555913	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
6	14.542842	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
7	14.567211	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
8	15.547669	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
9	15.586209	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply
10	16.552528	192.168.2.18	128.100.11.1	ICMP	Echo (ping) request
11	16.565526	128.100.11.1	192.168.2.18	ICMP	Echo (ping) reply

.....

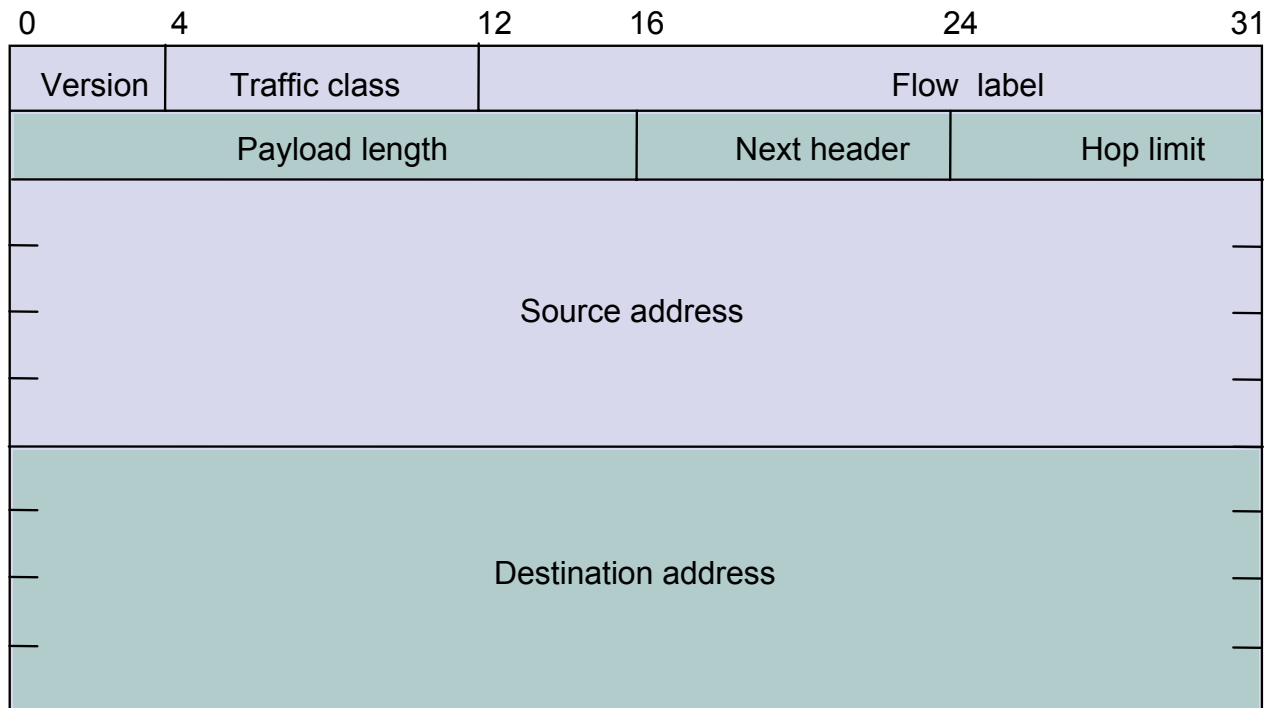
Frame 5 (74 bytes on wire, 74 bytes captured)
 Ethernet II, Src: 00:04:e2:29:b2:3a, Dst: 00:01:03:1d:cc:f7
 Internet Protocol, Src Addr: 128.100.11.1 (128.100.11.1), Dst Addr: 192.168.2.18 (192.168.2.18)
 Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0xf85b (correct)
 Identifier: 0x0200
 Sequence number: 5b:00
 Data (32 bytes)

.....

```

0000  00 01 03 1d cc f7 00 04  e2 29 b2 3a 08 00 45 00  .....  .).:..E.
0010  00 3c 99 88 00 00 f0 01  e3 18 80 64 0b 01 c0 a8  .<.....  ...d....
0020  02 12 00 00 f8 5b 02 00  5b 00 61 62 63 64 65 66  .....[.  [.abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76  ghijklmn  opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                                wabcdefg  hi
  
```

Filter: / Reset Apply File: pingtesla



v6.pcap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
7	6.617560	3ffe:507:0:1:200:86ff:fe05:80da	3ffe:501:4819::42	DNS	Standard query MX www.yahoo.com
8	6.752573	3ffe:501:4819::42	3ffe:507:0:1:200:86ff:fe05:80da	DNS	Standard query response MX 0 mr1.yahoo.com
9	10.364948	3ffe:507:0:1:200:86ff:fe05:80da	3ffe:507:0:1:260:97ff:fe07:69ea	ICMPv6	Neighbor solicitation
10	10.365231	3ffe:507:0:1:260:97ff:fe07:69ea	3ffe:507:0:1:200:86ff:fe05:80da	ICMPv6	Neighbor advertisement
11	10.490052	fe80::260:97ff:fe07:69ea	fe80::200:86ff:fe05:80da	ICMPv6	Neighbor solicitation
12	10.490554	fe80::200:86ff:fe05:80da	fe80::260:97ff:fe07:69ea	ICMPv6	Neighbor advertisement
13	12.297384	fe80::260:97ff:fe07:69ea	ff02::9	RIPng v6	Response

Ethernet II, Src: 00:00:86:05:80:da, Dst: 00:60:97:07:69:ea

Internet Protocol Version 6
 Version: 6
 Traffic class: 0x00
 Flowlabel: 0x00000
 Payload length: 39
 Next header: UDP (0x11)
 Hop limit: 64
 Source address: 3ffe:507:0:1:200:86ff:fe05:80da
 Destination address: 3ffe:501:4819::42

User Datagram Protocol, Src Port: 2397 (2397), Dst Port: domain (53)

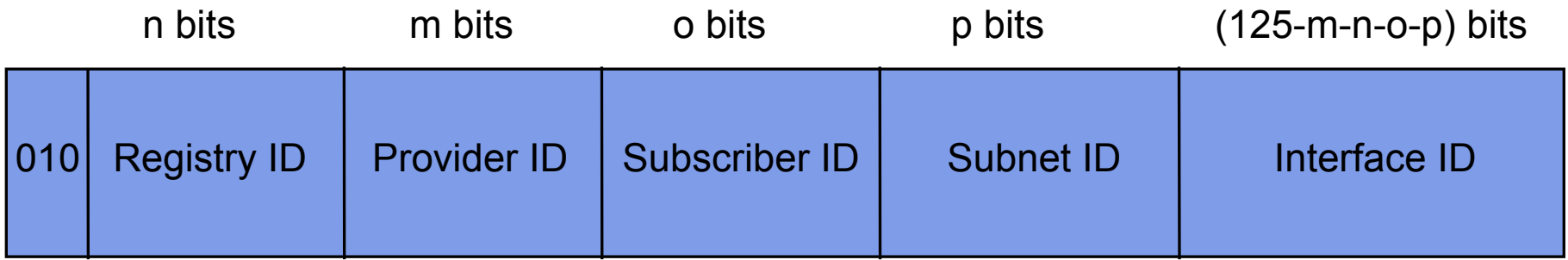
Domain Name System (query)
 Transaction ID: 0x0006
 Flags: 0x0100 (Standard query)
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0

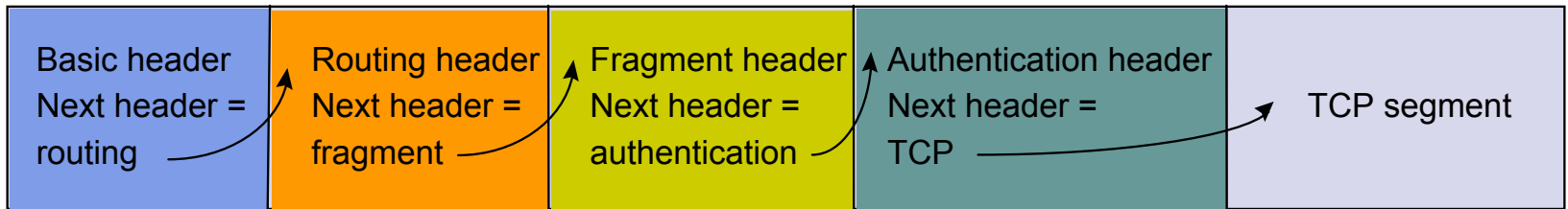
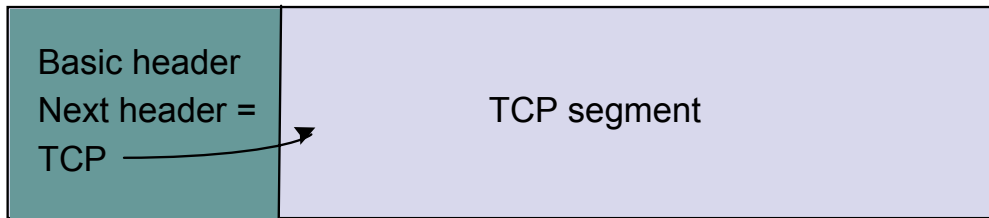
Queries
 www.yahoo.com: type MX, class inet
 Name: www.yahoo.com
 Type: Mail exchange
 Class: inet

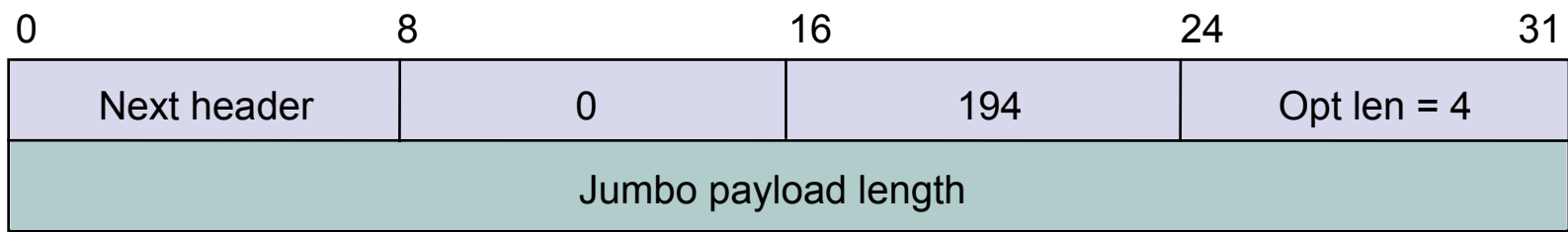
```

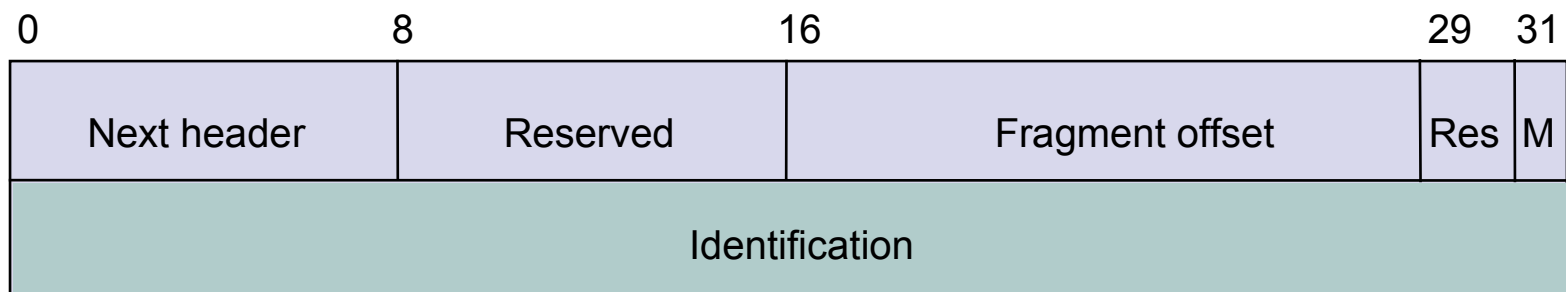
0000  00 60 97 07 69 ea 00 00 86 05 80 da 86 dd 60 00  . . . i . . . . . . . .
0010  00 00 00 27 11 40 3f fe 05 07 00 00 00 01 02 00  . . . . @ ? . . . . . . . .
0020  86 ff fe 05 80 da 3f fe 05 01 48 19 00 00 00 00  . . . . ? . . . H . . . .
0030  00 00 00 00 00 00 42 09 5d 00 35 00 27 46 b7 00 06  . . . . B . ] . 5 . ' F . . .
0040  01 00 00 01 00 00 00 00 00 00 03 77 77 77 05 79  . . . . . . . . . . www . y
0050  61 68 6f 6f 03 63 6f 6d 00 00 0f 00 01          a h o o . c o m . . . . .
  
```

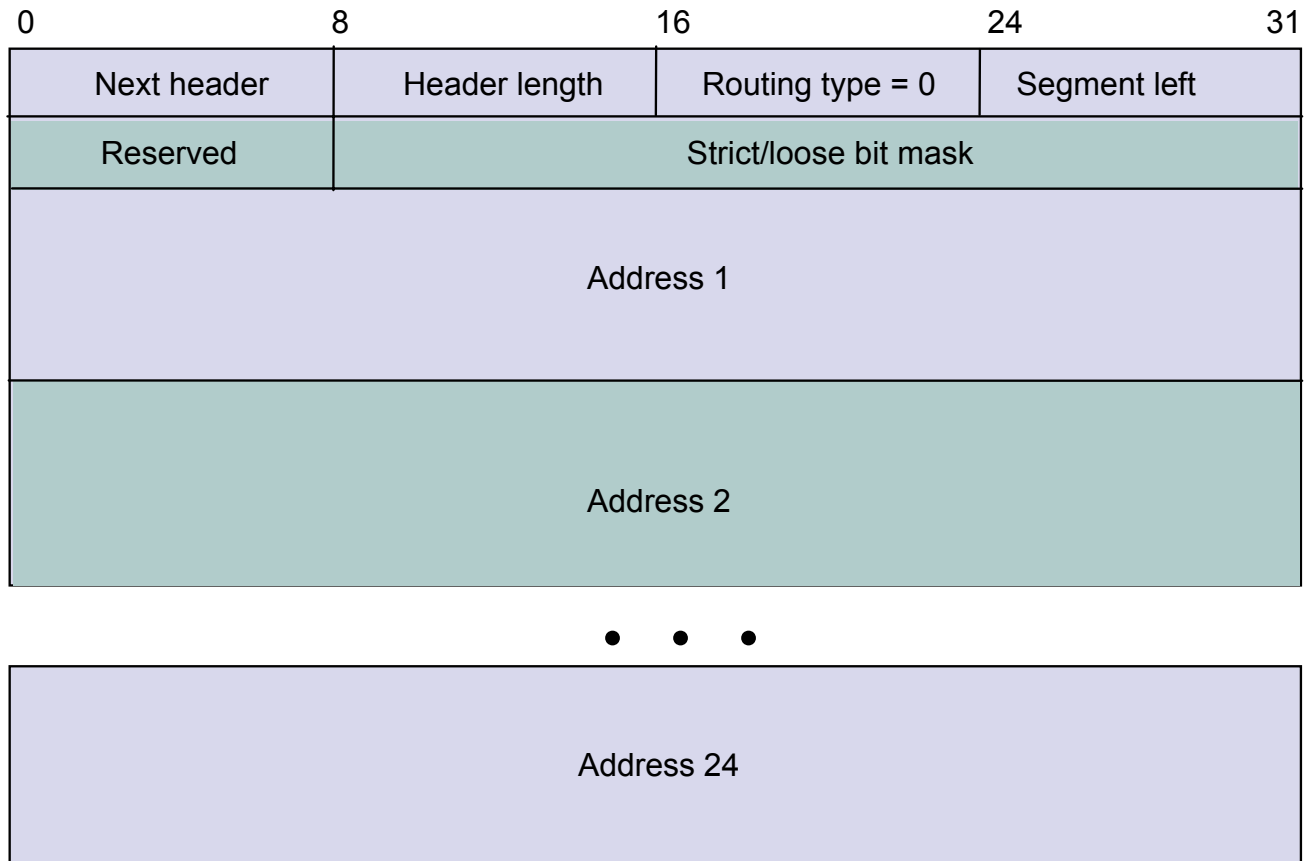
Filter: [] [x] Reset [x] Apply File: v6.pcap

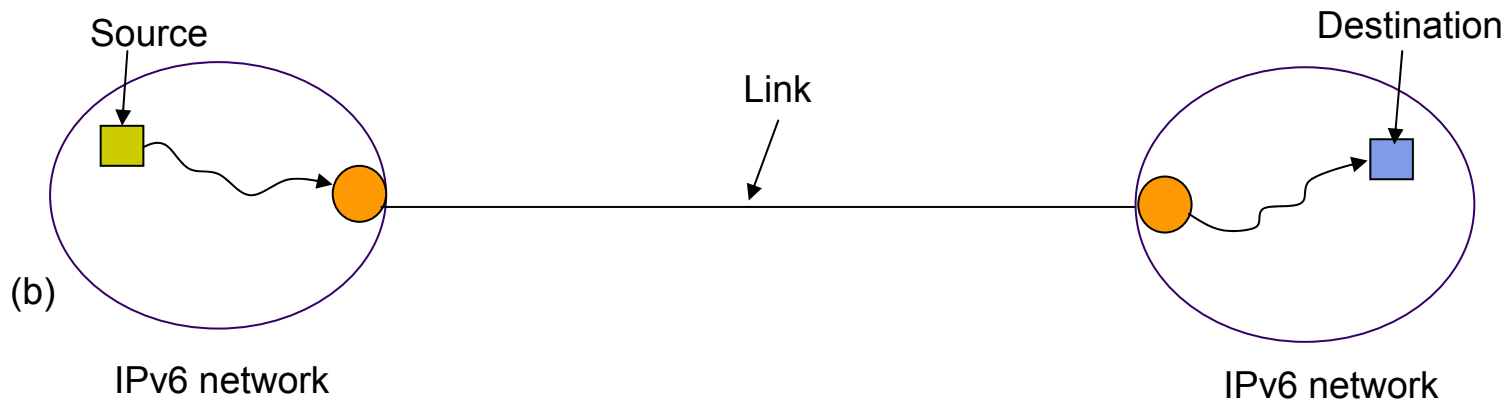
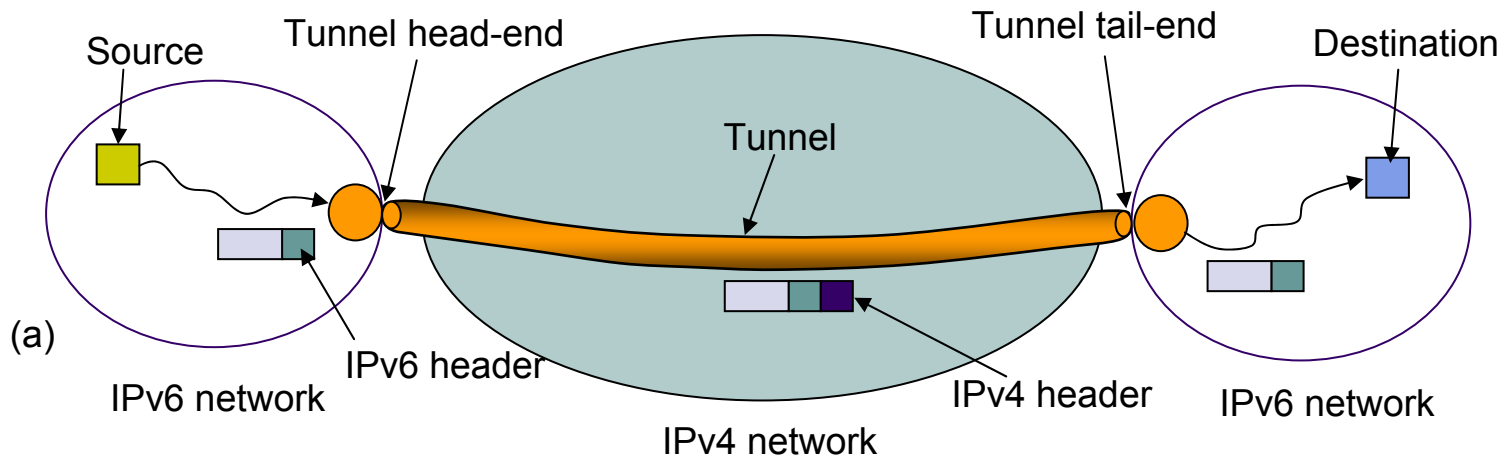


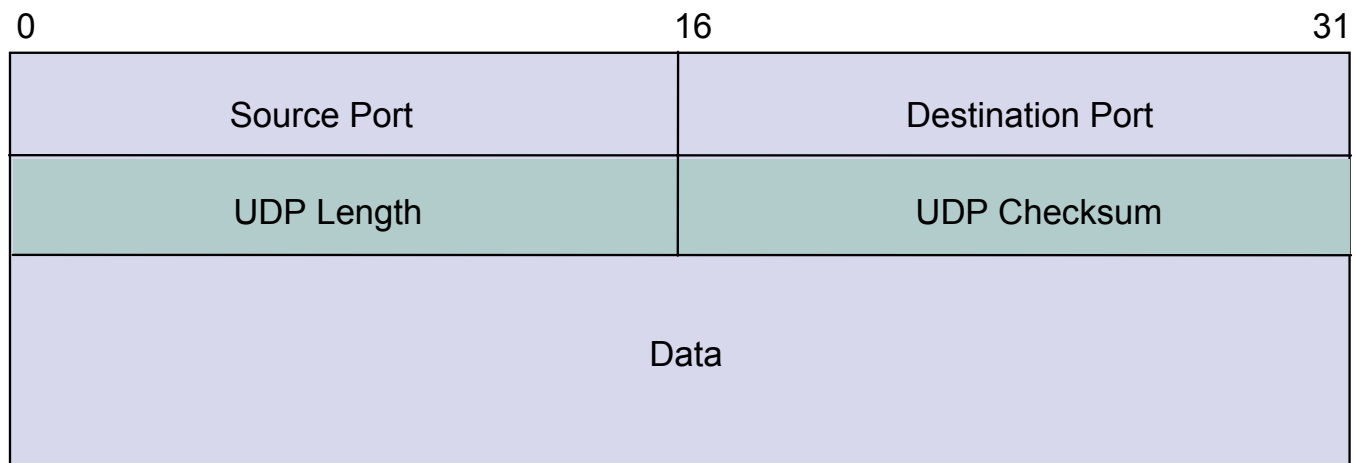


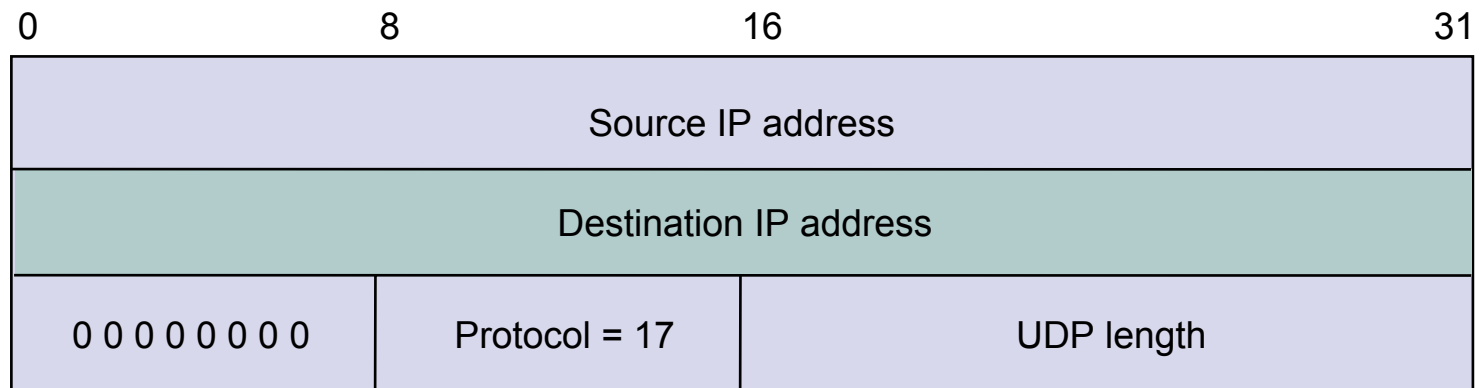


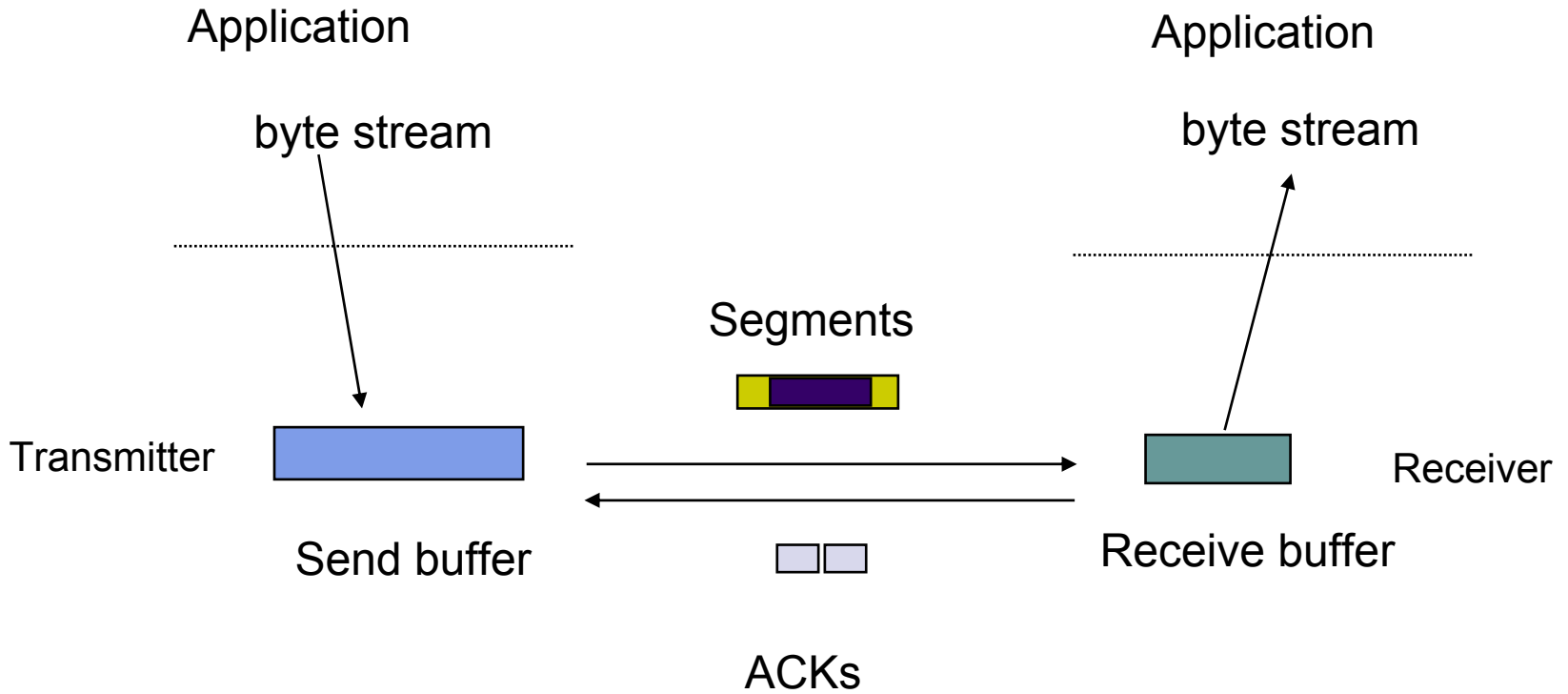


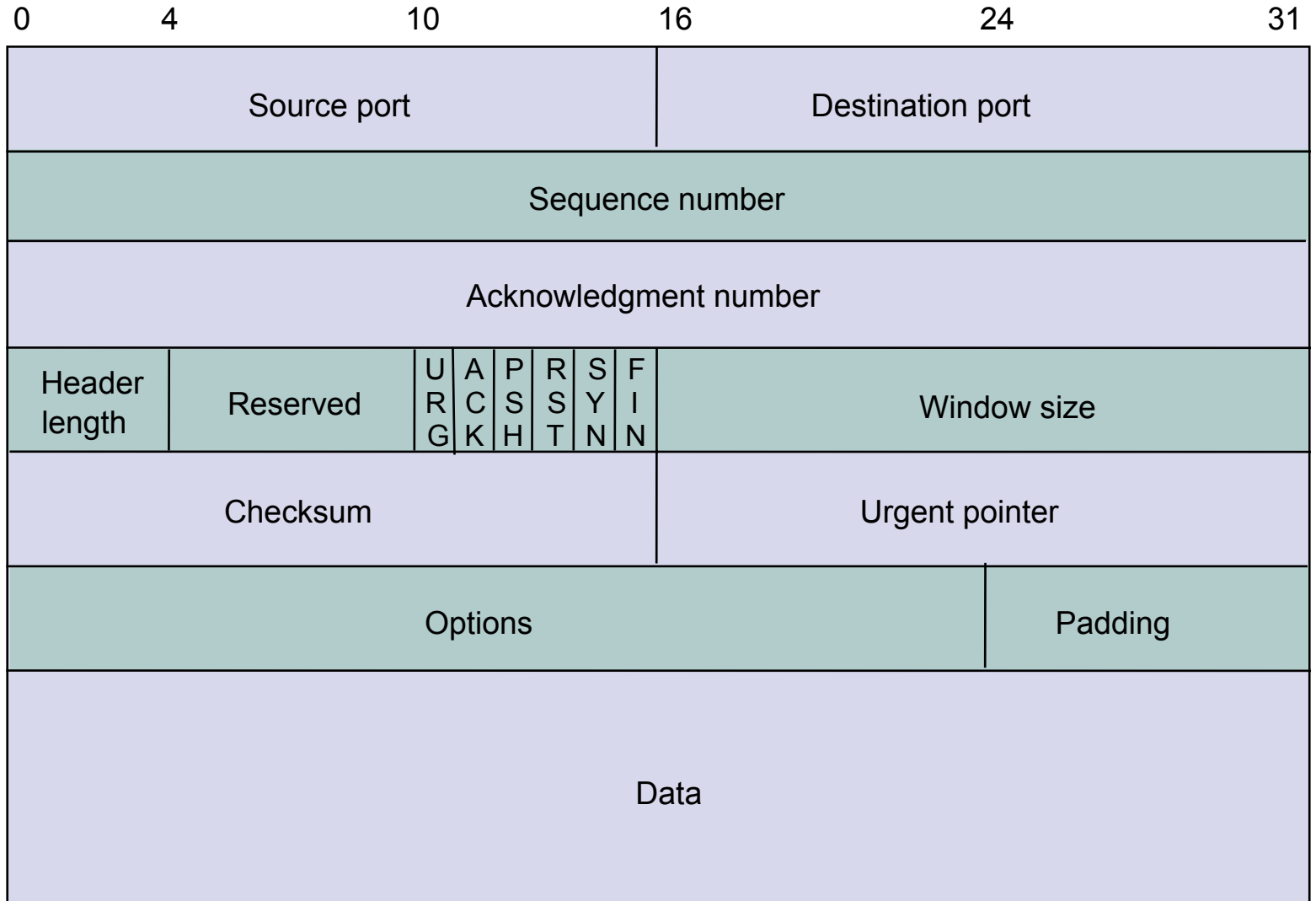


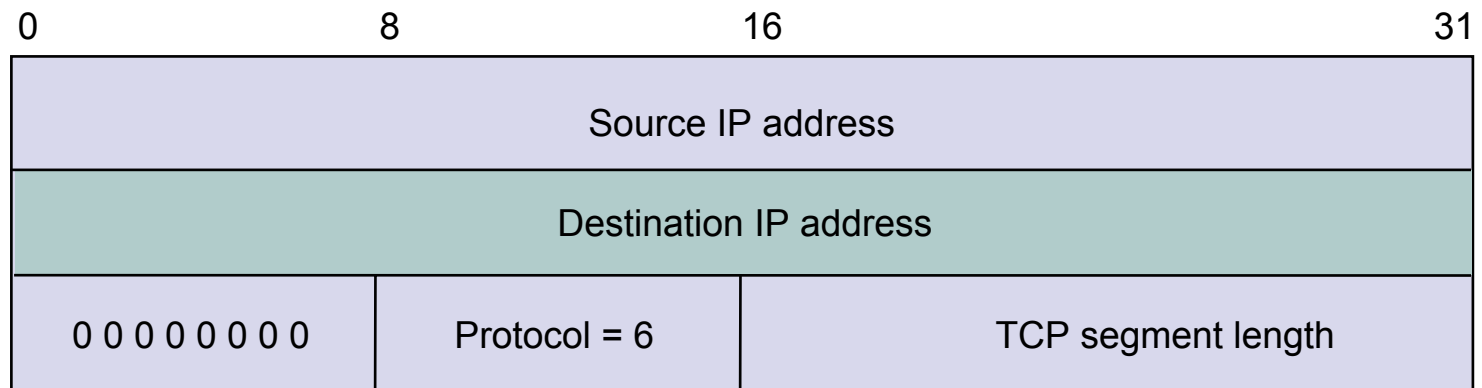






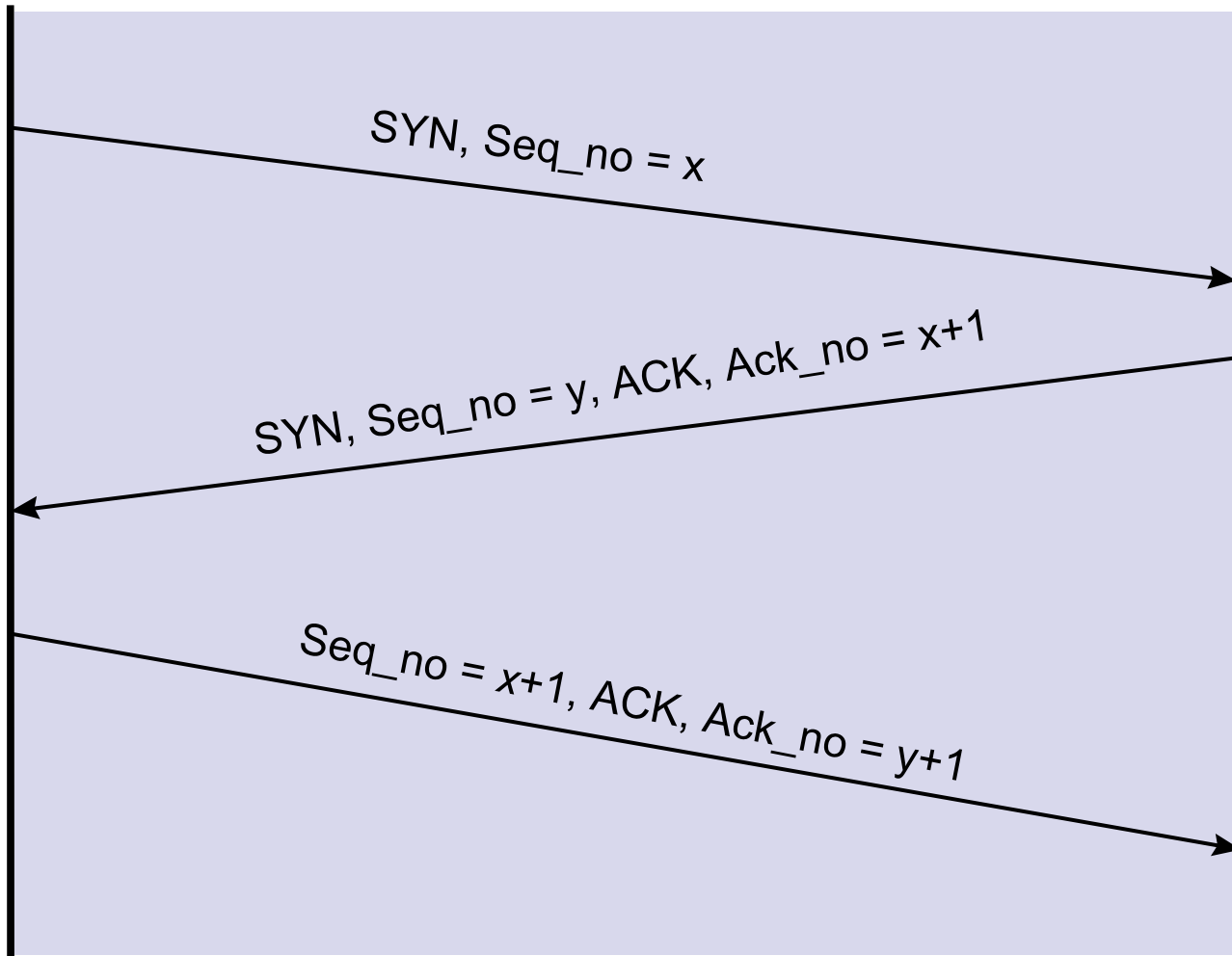


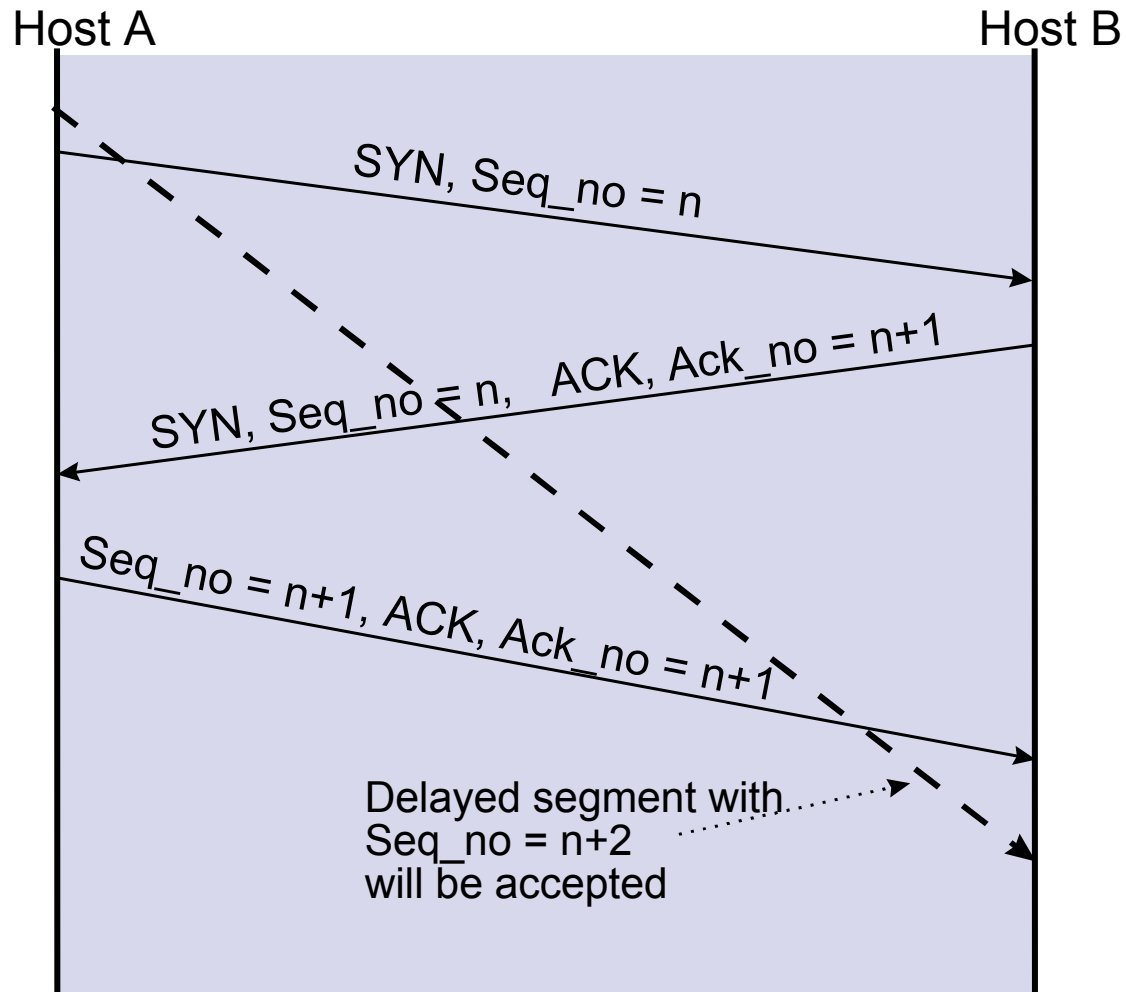




Host A

Host B





TCP Telnet Capture - Ethereal

File Edit Capture Display Tools Help

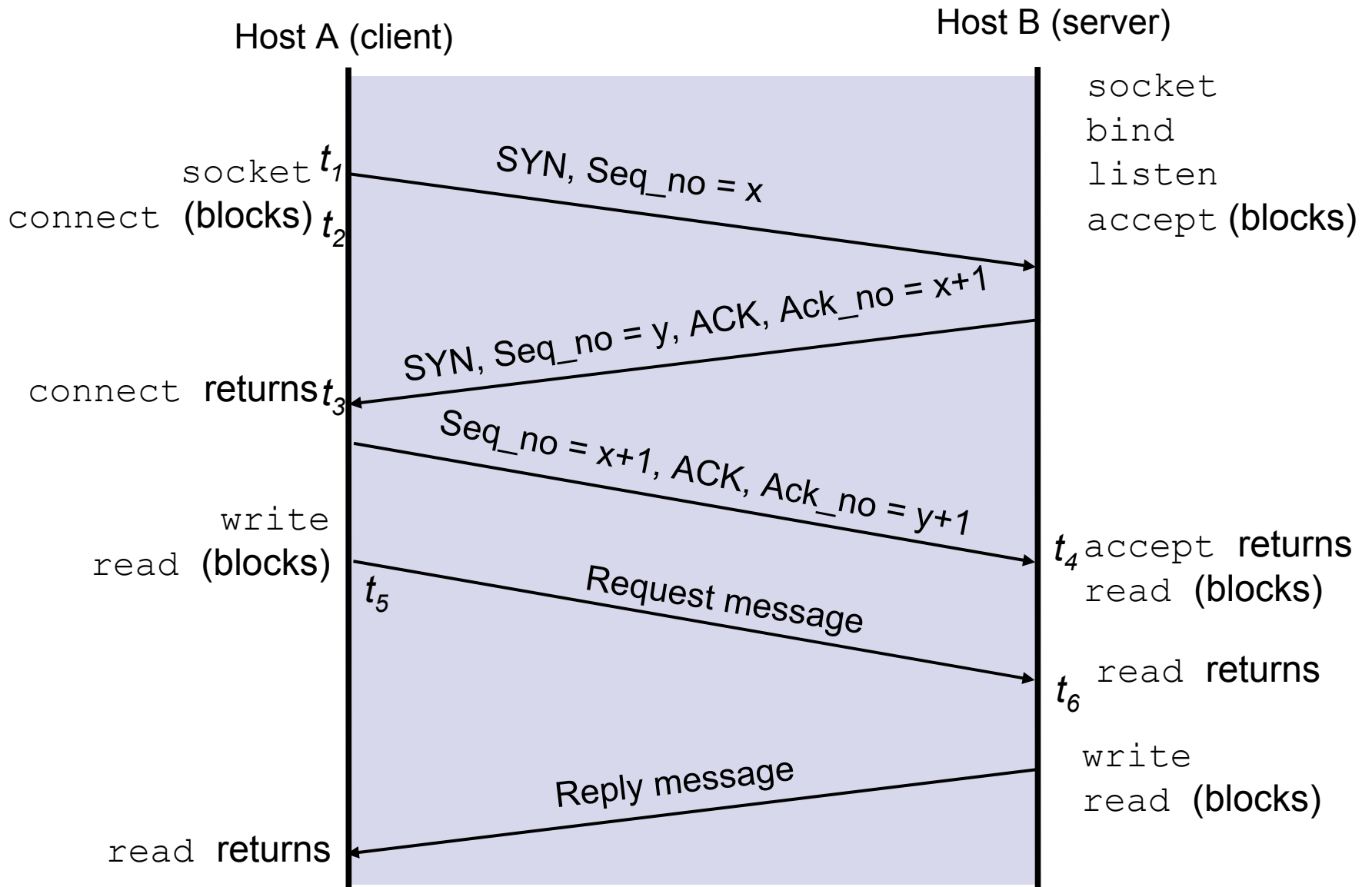
No.	Time	Source	Destination	Protocol	Info
1	0.000000	65.95.113.77	128.113.26.22	TCP	2743 > telnet [SYN] Seq=1839733355 Ack=0 win=31988 Len=0
2	0.144934	128.113.26.22	65.95.113.77	TCP	telnet > 2743 [SYN, ACK] Seq=1877388864 Ack=1839733356 win=49152 Len=0
3	0.145270	65.95.113.77	128.113.26.22	TCP	2743 > telnet [ACK] Seq=1839733356 Ack=1877388865 win=31988 Len=0
4	0.322432	128.113.26.22	65.95.113.77	TELNET	Telnet Data ...
5	0.323617	65.95.113.77	128.113.26.22	TELNET	Telnet Data ...
6	21.606250	65.95.113.77	128.113.26.22	TCP	2743 > telnet [FIN, ACK] Seq=1839733427 Ack=1877389120 win=31733 Len=0
7	21.751944	128.113.26.22	65.95.113.77	TCP	telnet > 2743 [ACK] Seq=1877389120 Ack=1839733428 win=49152 Len=0
8	21.757136	128.113.26.22	65.95.113.77	TCP	telnet > 2743 [FIN, ACK] Seq=1877389120 Ack=1839733428 win=49152 Len=0
9	21.757468	65.95.113.77	128.113.26.22	TCP	2743 > telnet [ACK] Seq=1839733428 Ack=1877389121 win=31733 Len=0

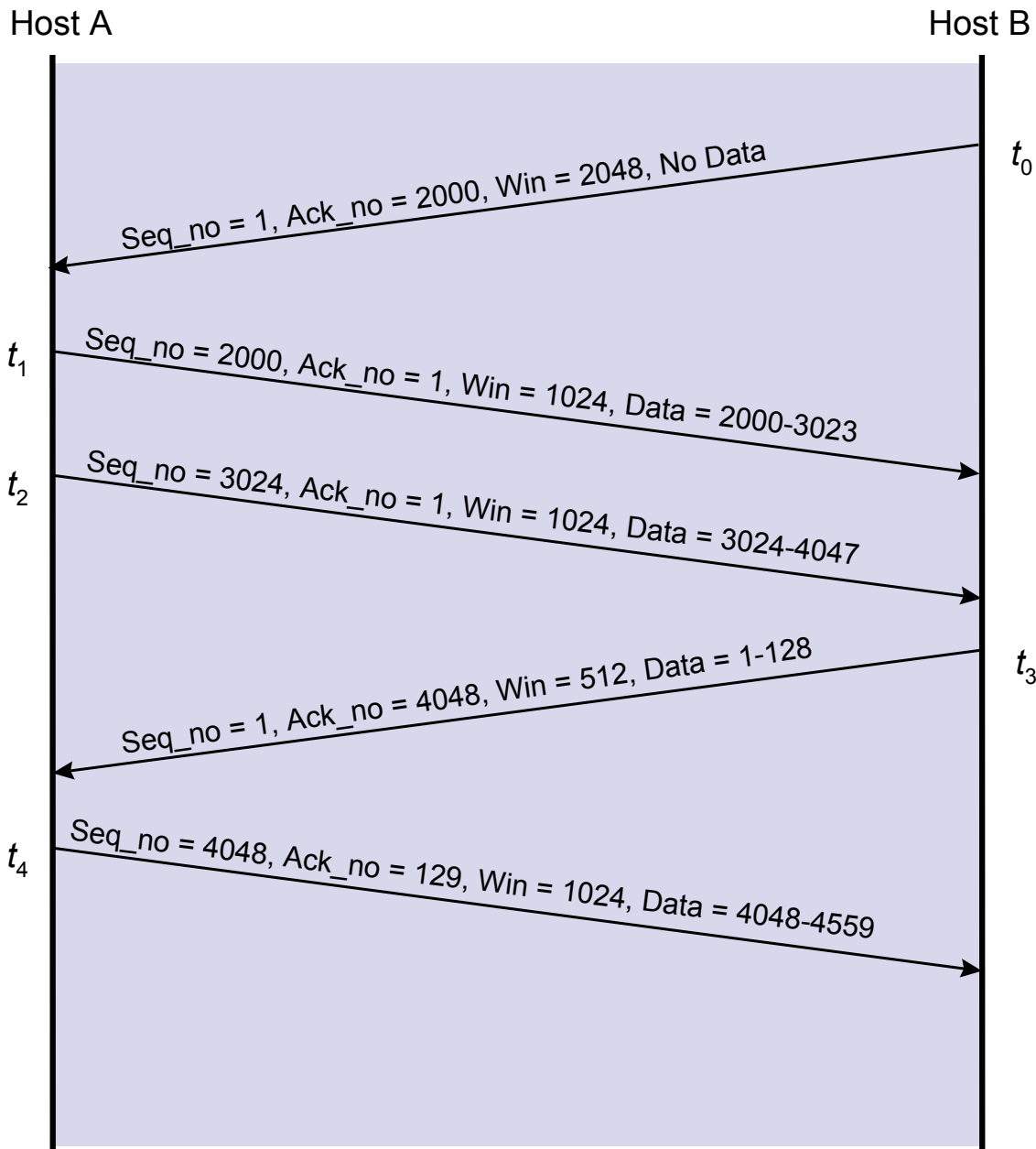
Ethernet II, Src: 00:90:1a:40:1d:17, Dst: 00:80:c6:e9:fe:08
 PPP-over-Ethernet Session
 Point-to-Point Protocol
 Internet Protocol, Src Addr: 128.113.26.22 (128.113.26.22), Dst Addr: 65.95.113.77 (65.95.113.77)
 Transmission Control Protocol, Src Port: telnet (23), Dst Port: 2743 (2743), Seq: 1877388864, Ack: 1839733356, Len: 0
 Source port: telnet (23)
 Destination port: 2743 (2743)
 Sequence number: 1877388864
 Acknowledgement number: 1839733356
 Header length: 24 bytes
 Flags: 0x0012 (SYN, ACK)
 window size: 49152
 checksum: 0xd9d8 (correct)
 options: (4 bytes)
 Maximum segment size: 1460 bytes

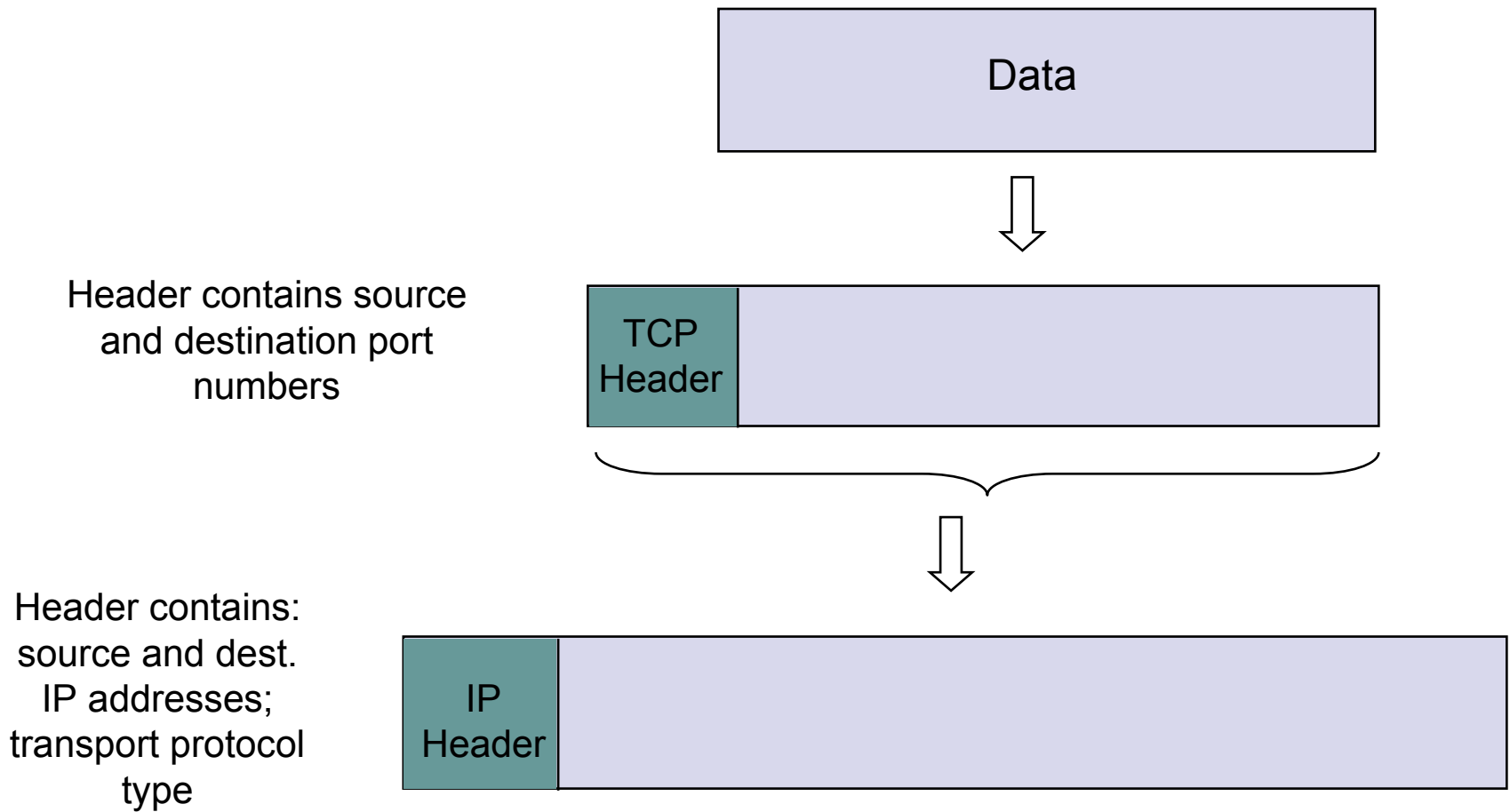
```

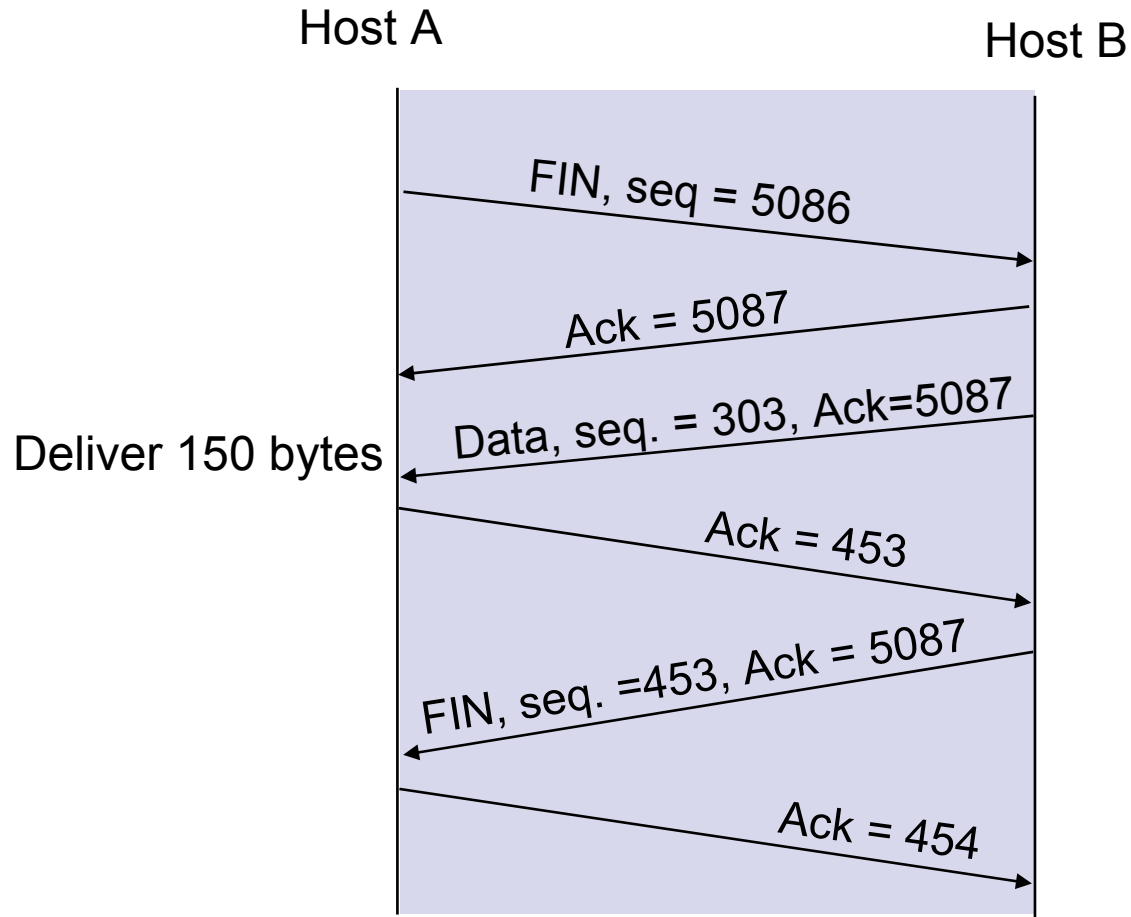
0000  00 80 c6 e9 fe 08 00 90 1a 40 1d 17 88 64 11 00  .....@...d..
0010  15 97 00 2e 00 21 45 00 00 2c c9 1c 40 00 33 06  .....!E. ....@.3.
0020  31 7c 80 71 1a 16 41 5f 71 4d 00 17 0a b7 6f e6  1|.q..A_ qM....o.
0030  ae 40 6d a8 1a 6c 60 12 c0 00 d9 d8 00 00 02 04  .@m..l`. ....
0040  05 b4  ..
  
```

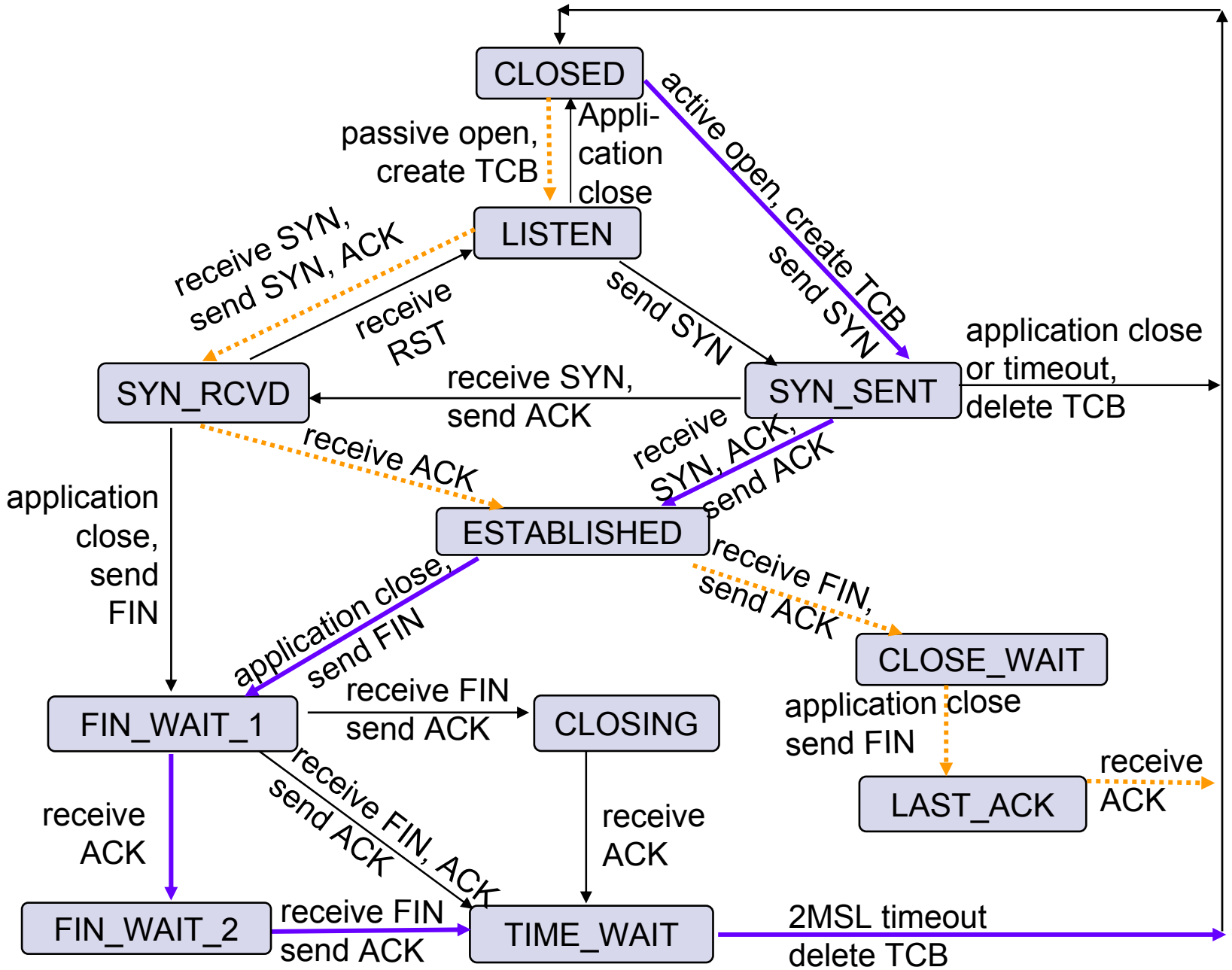
Filter: Reset Apply File: TCP Telnet Capture

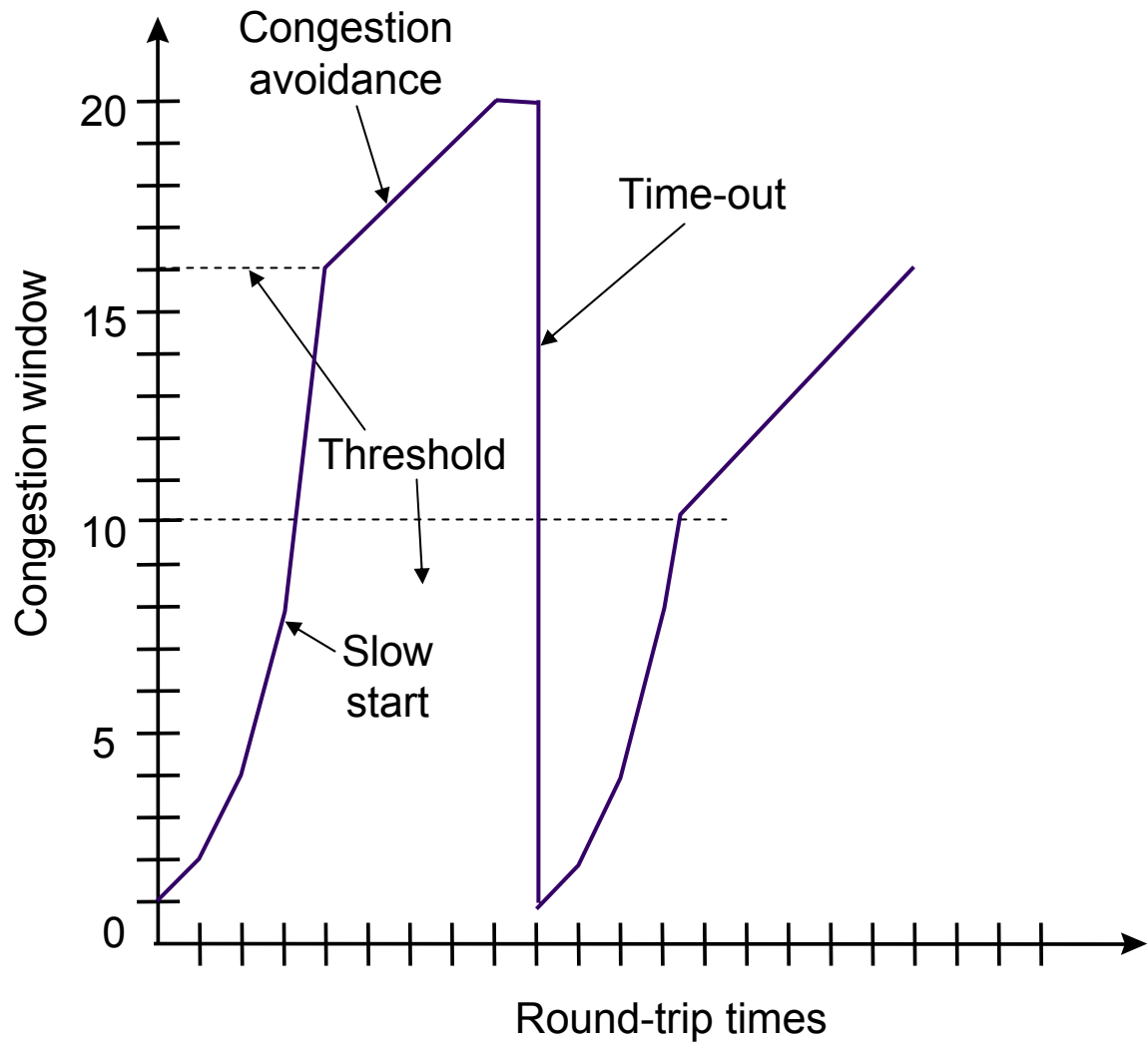


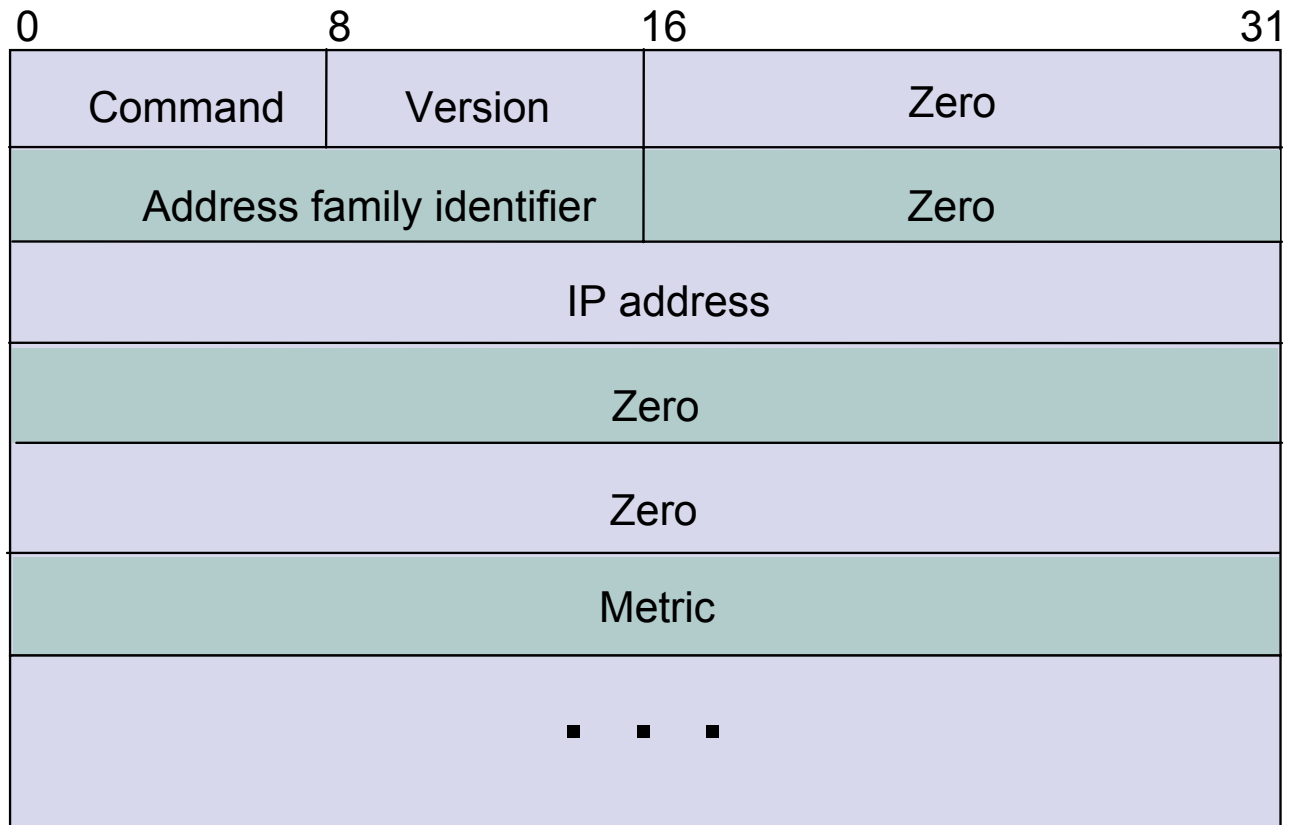


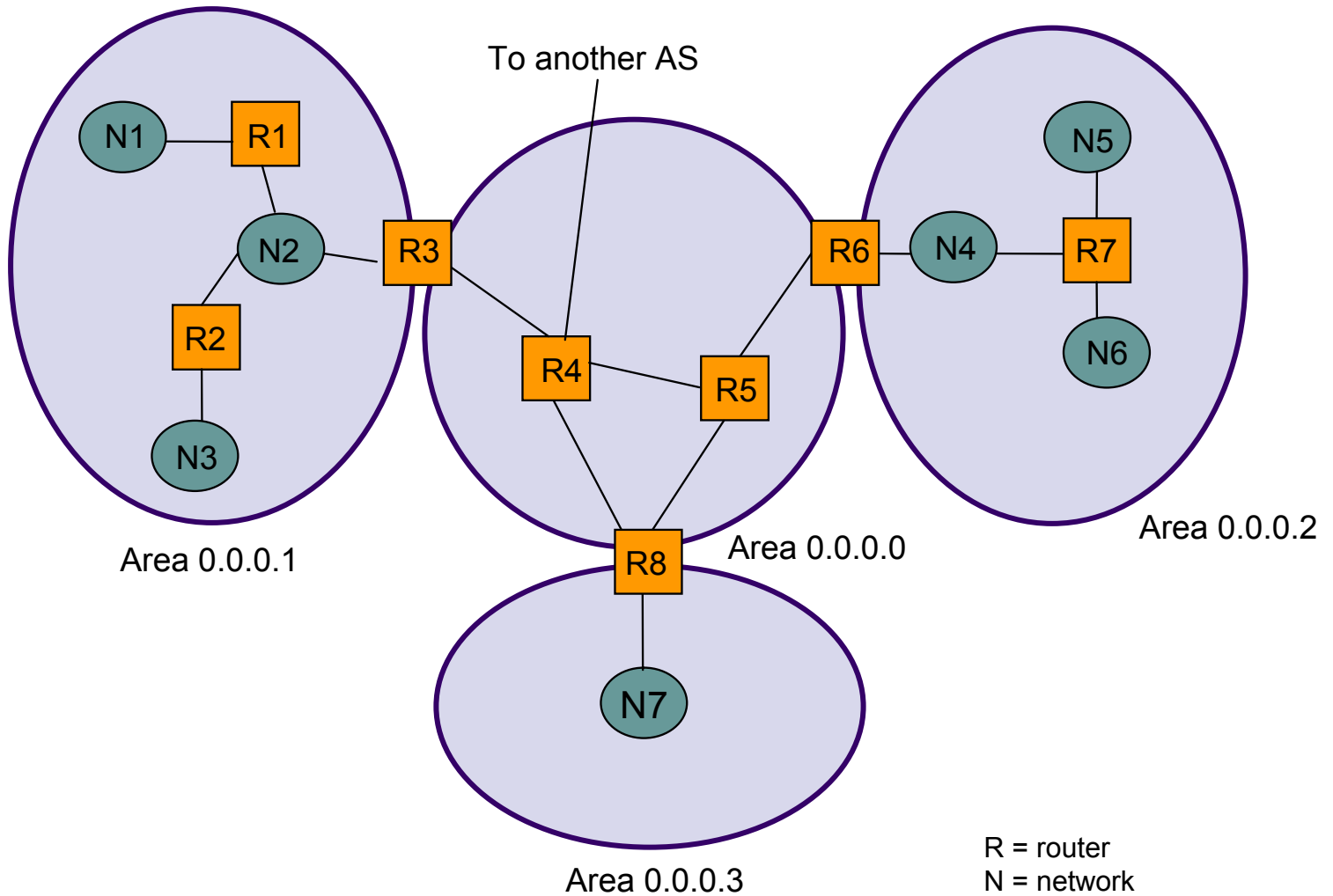


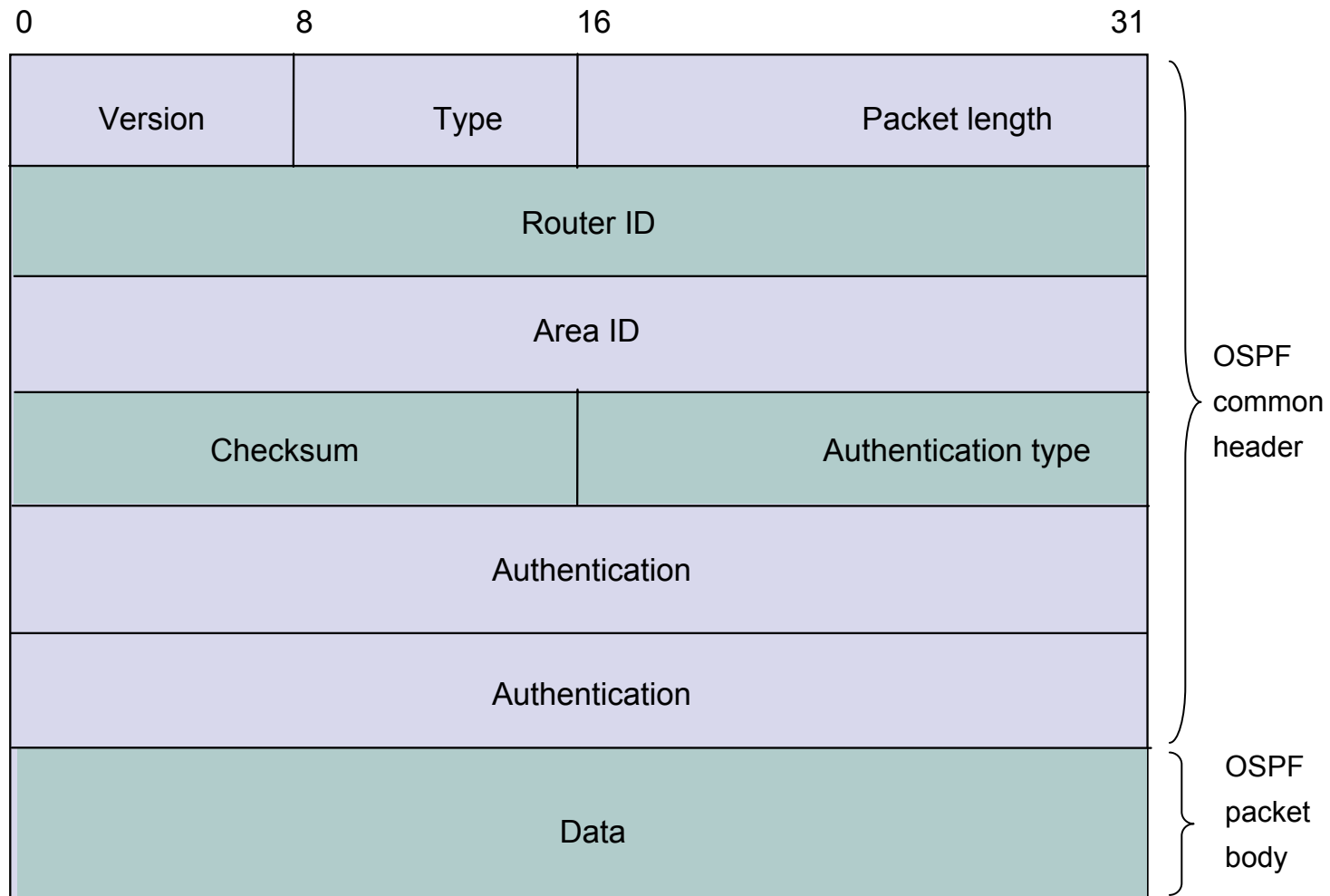


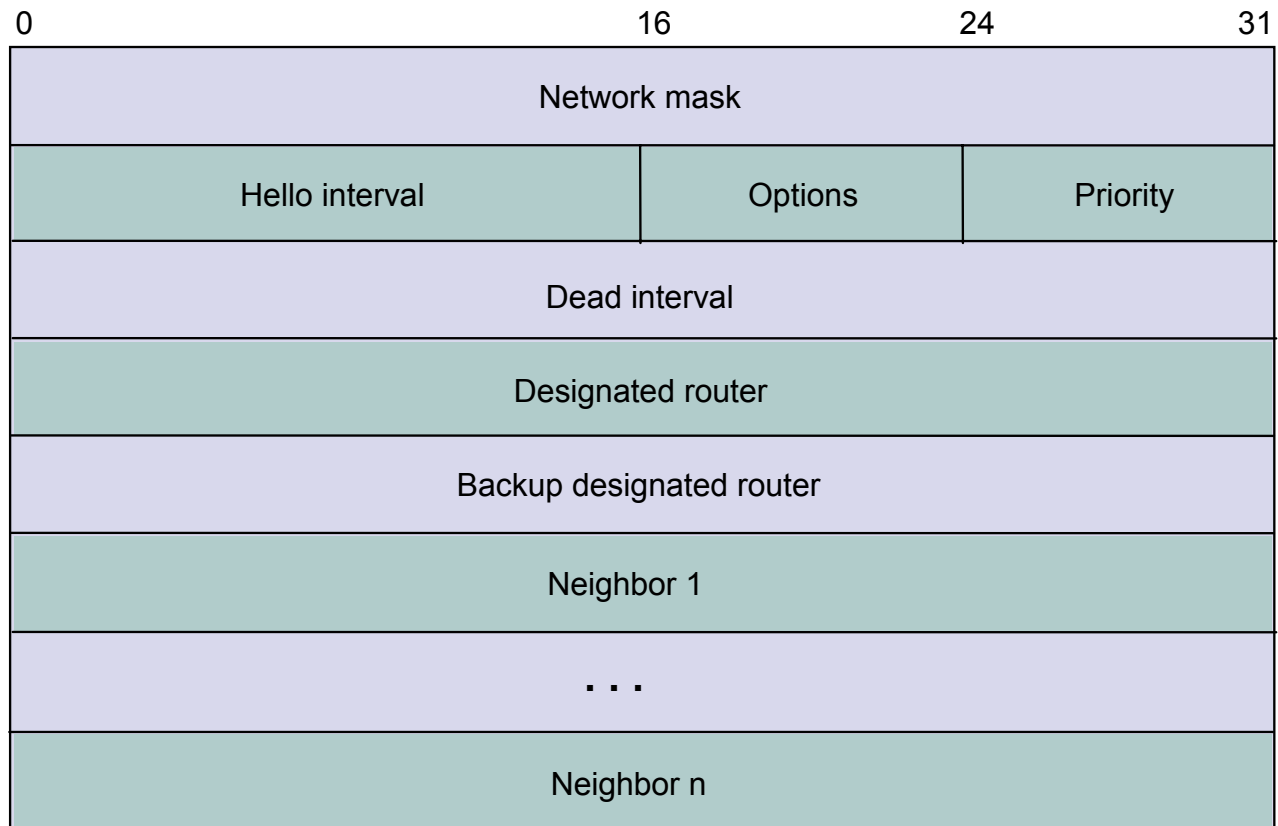


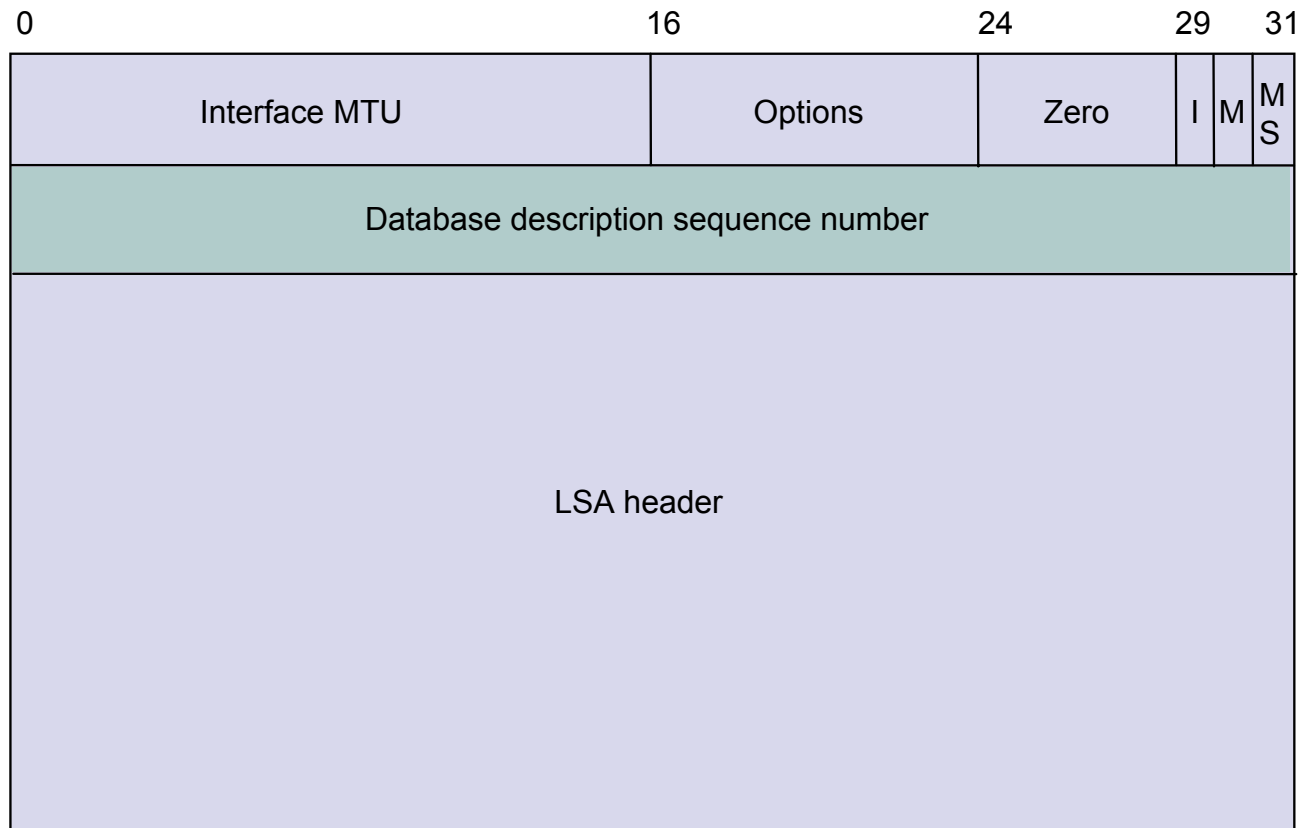


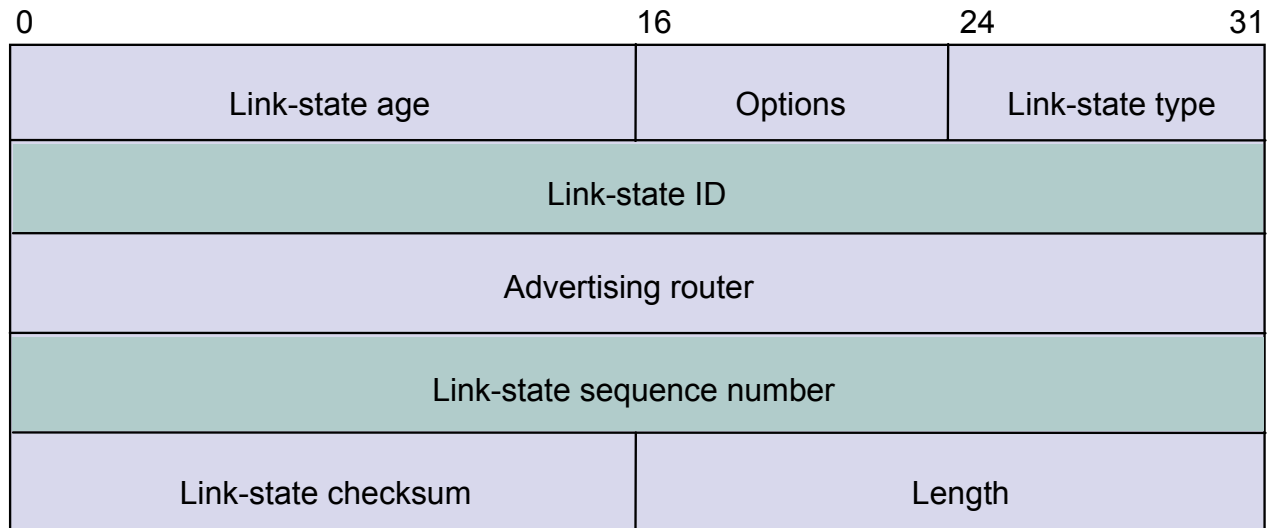


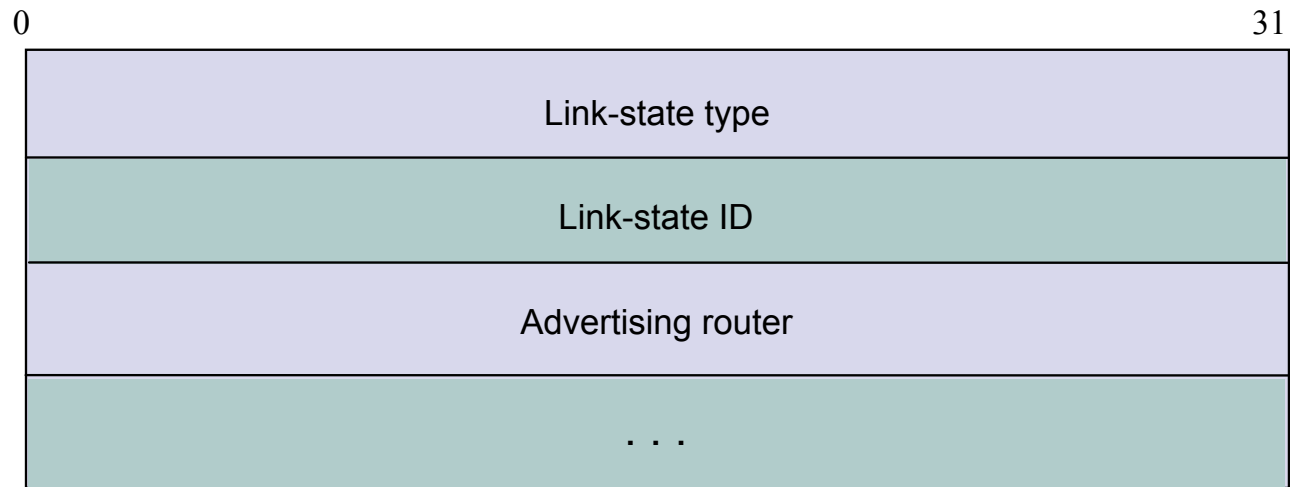


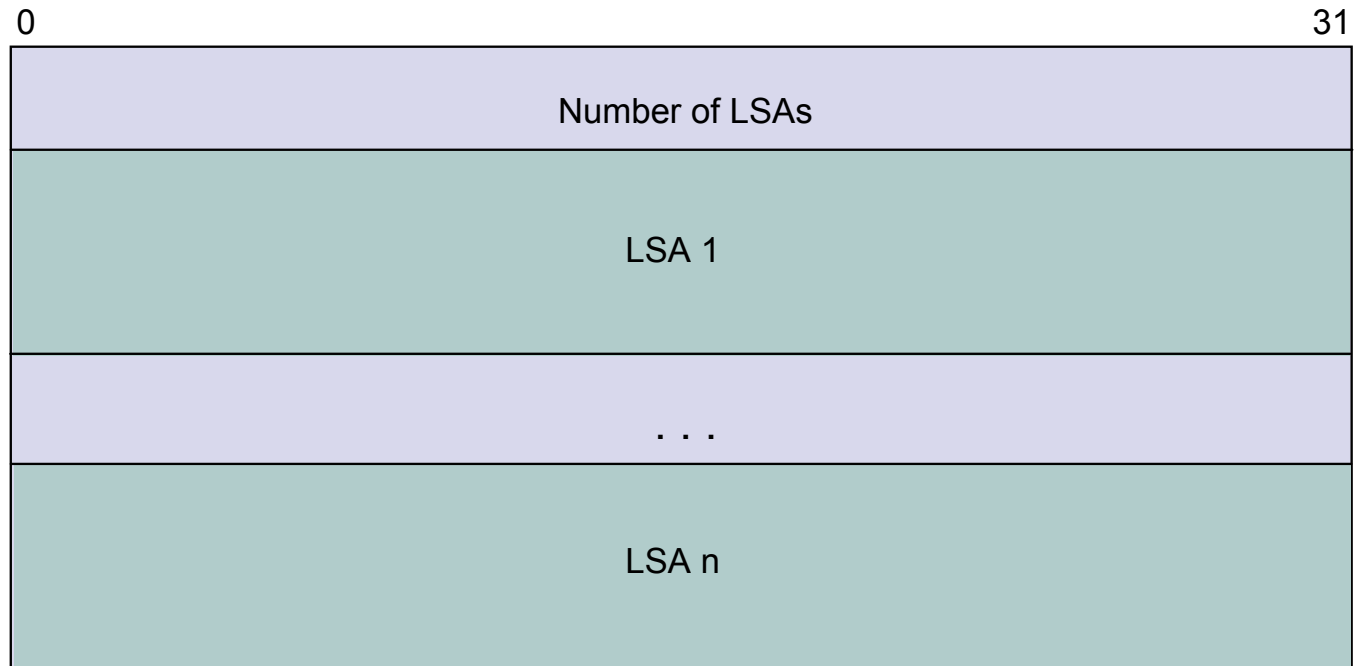












ospfcap - Ethereal

File Edit Capture Display Tools Help

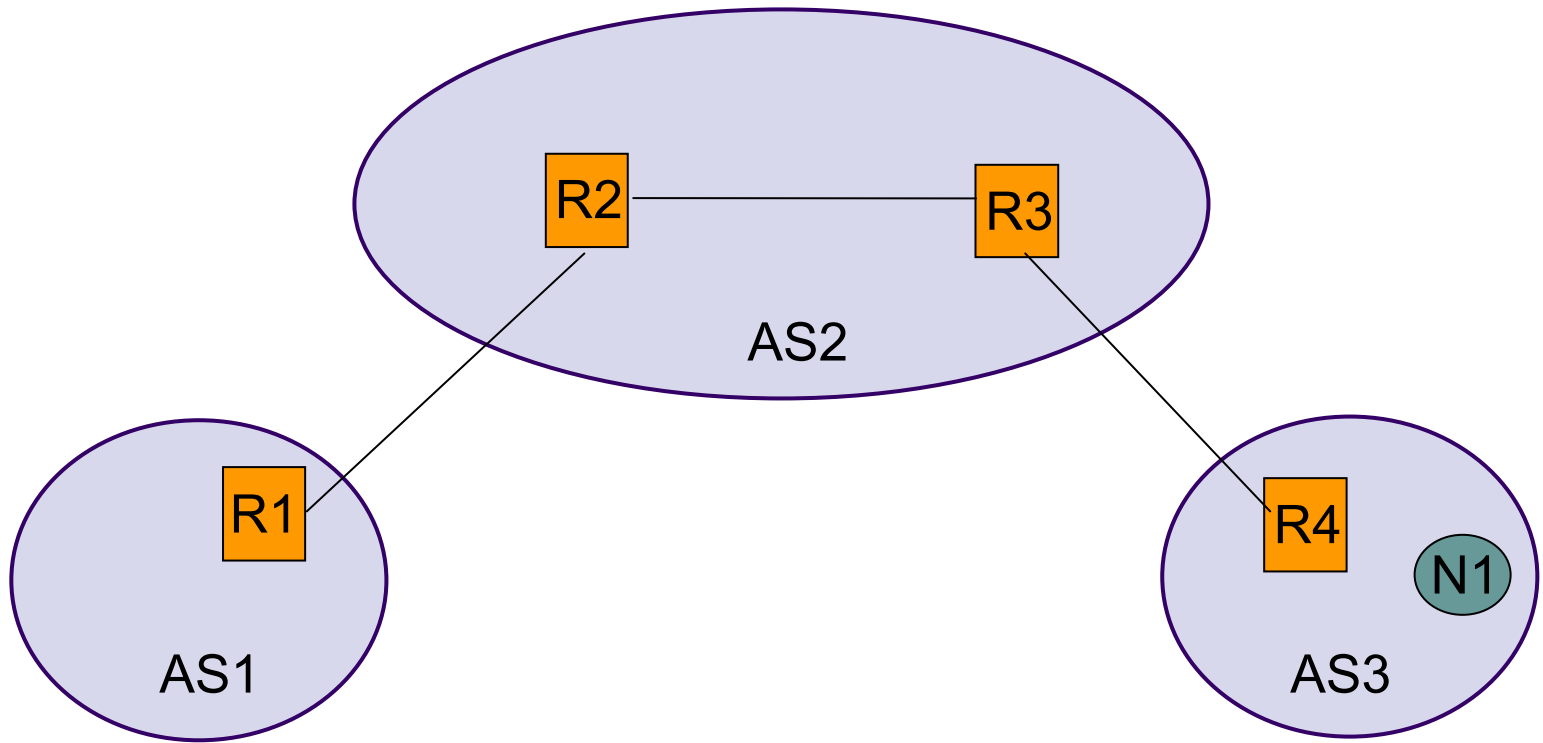
No.	Time	Source	Destination	Protocol	Info
3	3.682599	20.1.1.1	224.0.0.5	OSPF	Hello Packet
6	6.189717	20.1.1.2	224.0.0.5	OSPF	Hello Packet
10	10.495667	20.1.1.1	224.0.0.5	OSPF	Hello Packet
11	11.264514	20.1.1.1	224.0.0.5	OSPF	LS Update
12	11.766168	20.1.1.2	224.0.0.5	OSPF	LS Update
13	11.775527	20.1.1.1	224.0.0.5	OSPF	LS Update
15	13.731086	20.1.1.2	224.0.0.5	OSPF	LS Acknowledge
16	13.740725	20.1.1.1	224.0.0.5	OSPF	LS Acknowledge
19	16.188992	20.1.1.2	224.0.0.5	OSPF	Hello Packet
21	19.018319	20.1.1.1	224.0.0.5	OSPF	LS Acknowledge
22	19.145138	20.1.1.2	224.0.0.5	OSPF	LS Acknowledge
24	20.493778	20.1.1.1	224.0.0.5	OSPF	Hello Packet
28	26.103357	20.1.1.2	224.0.0.5	OSPF	Hello Packet
33	30.407765	20.1.1.1	224.0.0.5	OSPF	Hello Packet

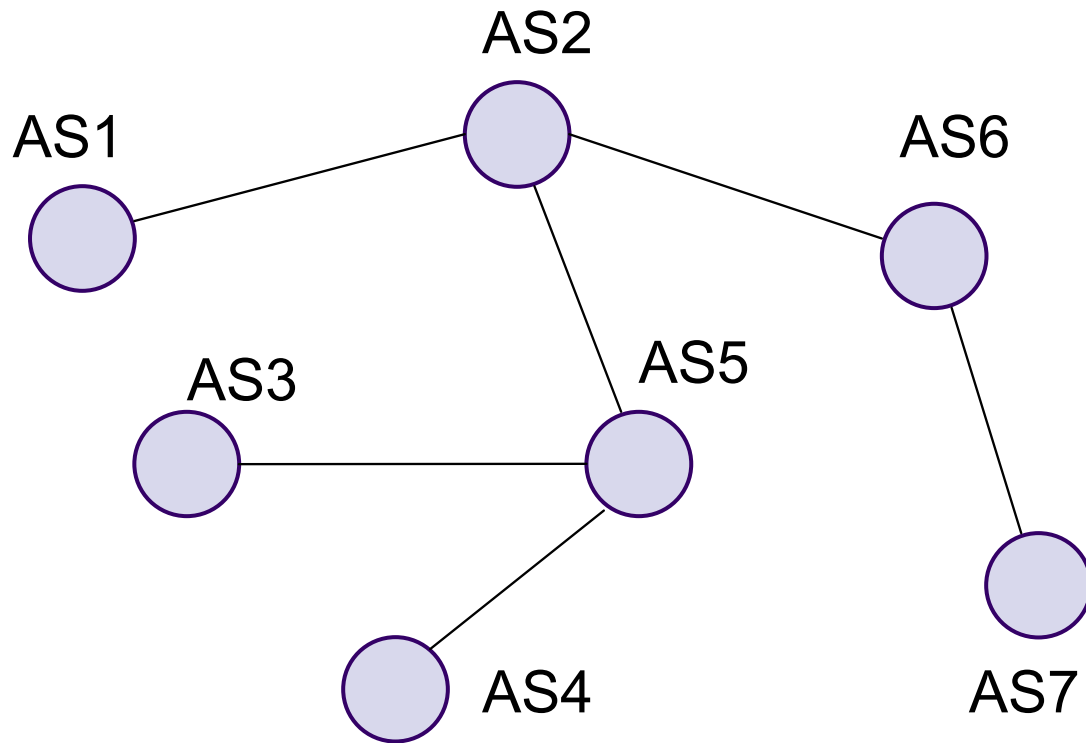
Frame 11 (226 bytes on wire, 226 bytes captured)
 Ethernet II, Src: 00:10:7b:39:ab:42, Dst: 01:00:5e:00:00:05
 Internet Protocol, Src Addr: 20.1.1.1 (20.1.1.1), Dst Addr: 224.0.0.5 (224.0.0.5)
 Open Shortest Path First
 OSPF Header
 LS Update Packet
 Number of LSAs: 5
 LS Type: Summary-LSA (IP network)
 LS Age: 1 seconds
 Options: 0x22 (E/DC)
 Link-State Advertisement Type: Summary-LSA (IP network) (3)
 Link State ID: 172.16.16.0
 Advertising Router: 200.1.1.1 (200.1.1.1)
 LS Sequence Number: 0x80000004
 LS Checksum: abb5
 Length: 28
 Netmask: 255.255.255.0
 Metric: 64
 LS Type: Summary-LSA (IP network)
 LS Type: AS-External-LSA (ASBR)
 LS Type: AS-External-LSA (ASBR)
 LS Type: AS-External-LSA (ASBR)

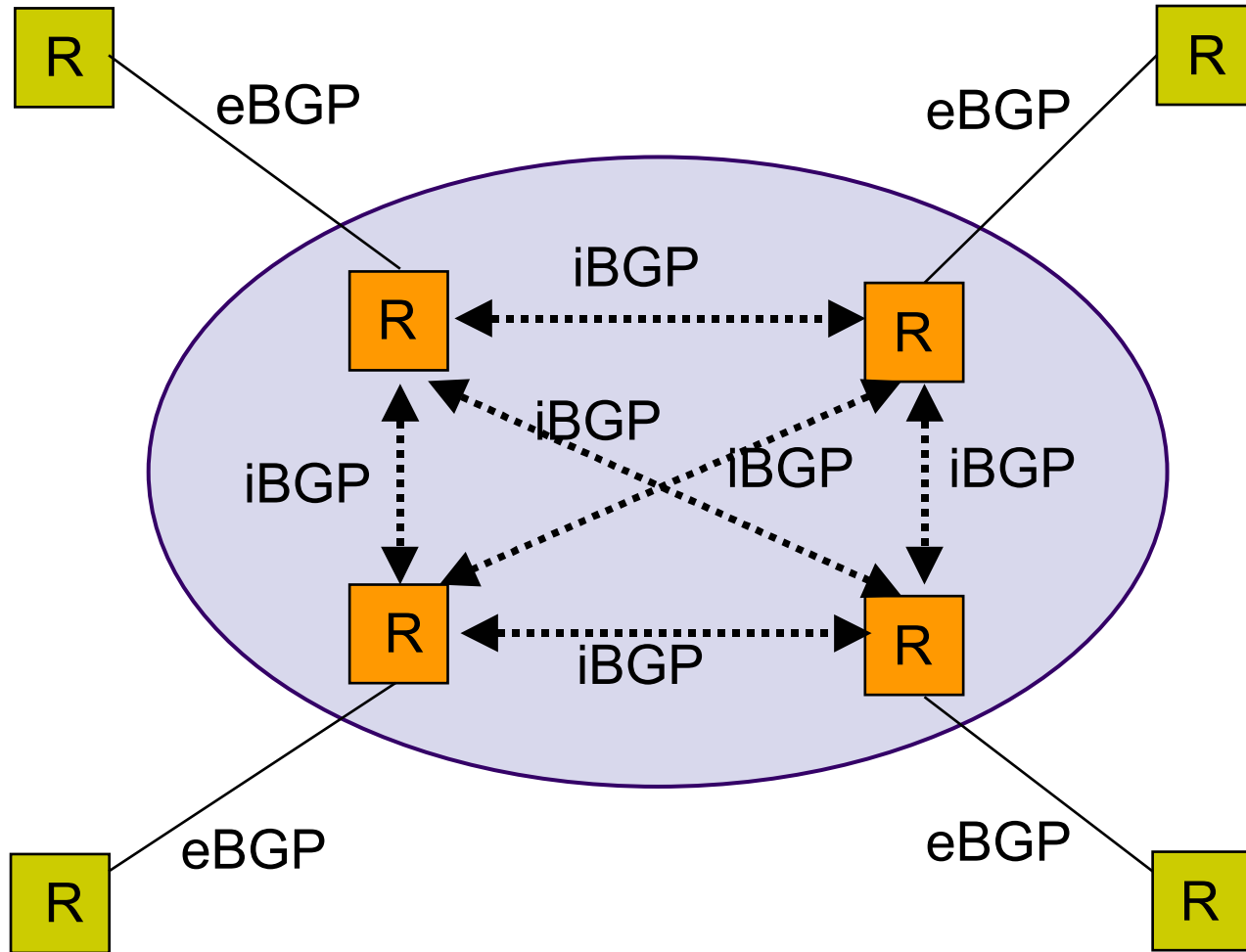
```

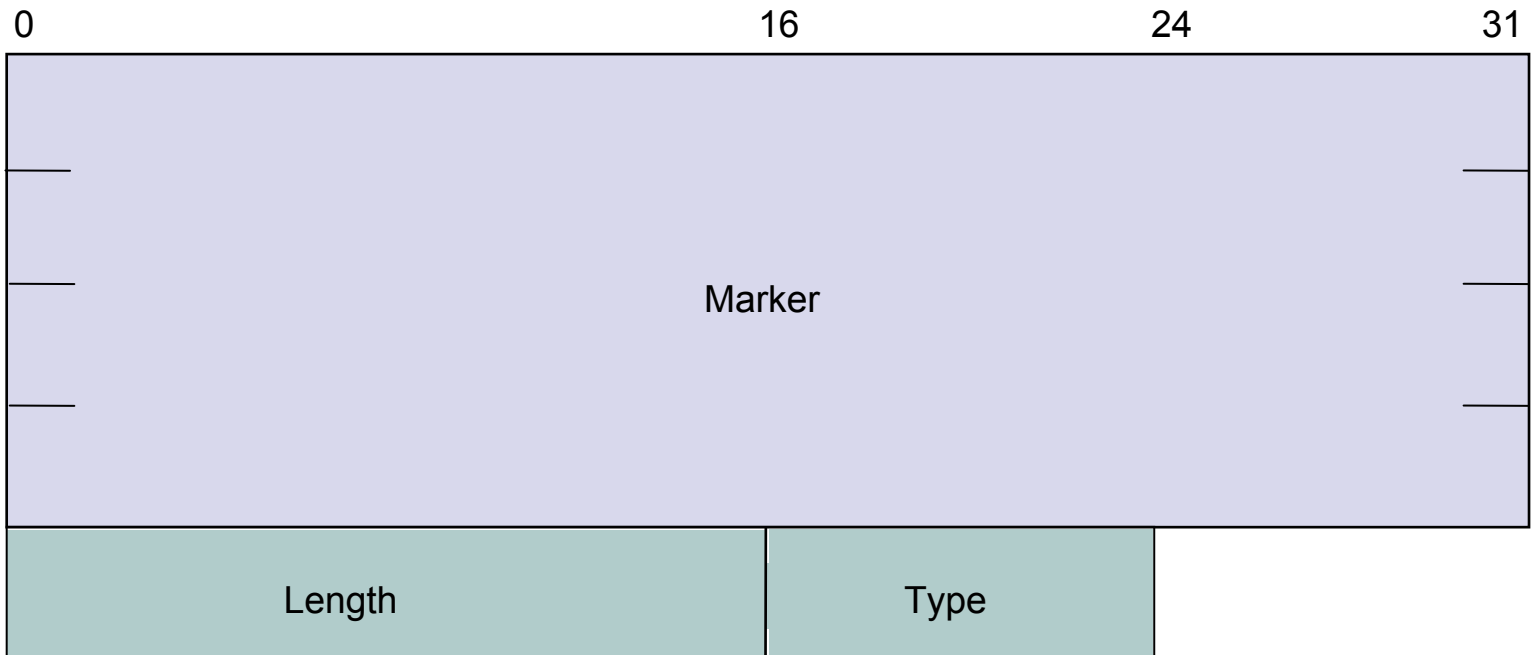
0000  01 00 5e 00 00 05 00 10 7b 39 ab 42 08 00 45 c0  ..A.....{9.B..E.
0010  00 d4 fa e9 00 00 01 59 c8 20 14 01 01 01 e0 00  .....Y. ....
0020  00 05 02 04 00 c0 c8 01 01 01 00 00 00 00 cc 96  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 01  .....
0040  22 03 ac 10 10 00 c8 01 01 01 80 00 00 04 ab b5  ".....
  
```

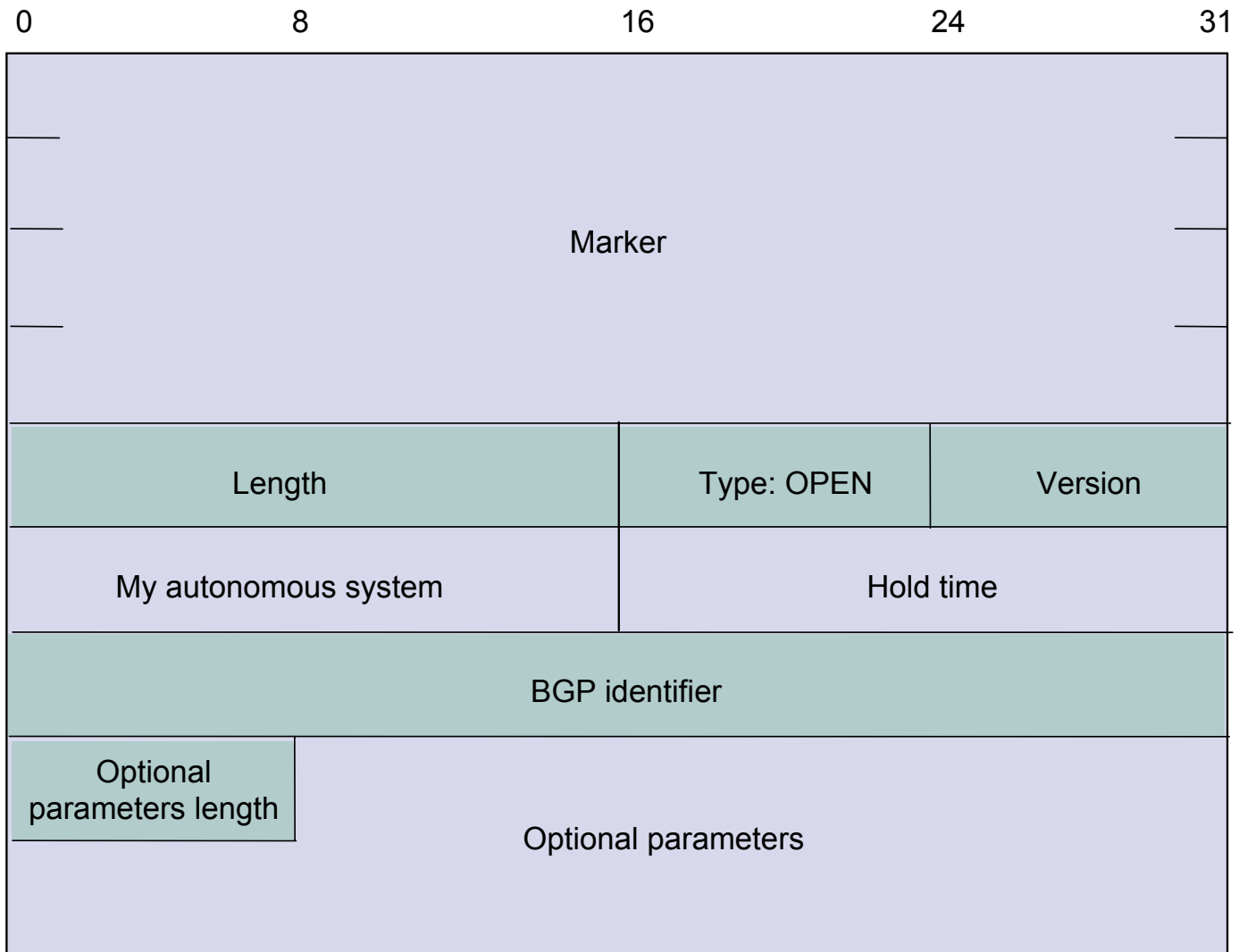
Filter: [Reset] [Apply] File: ospfcap

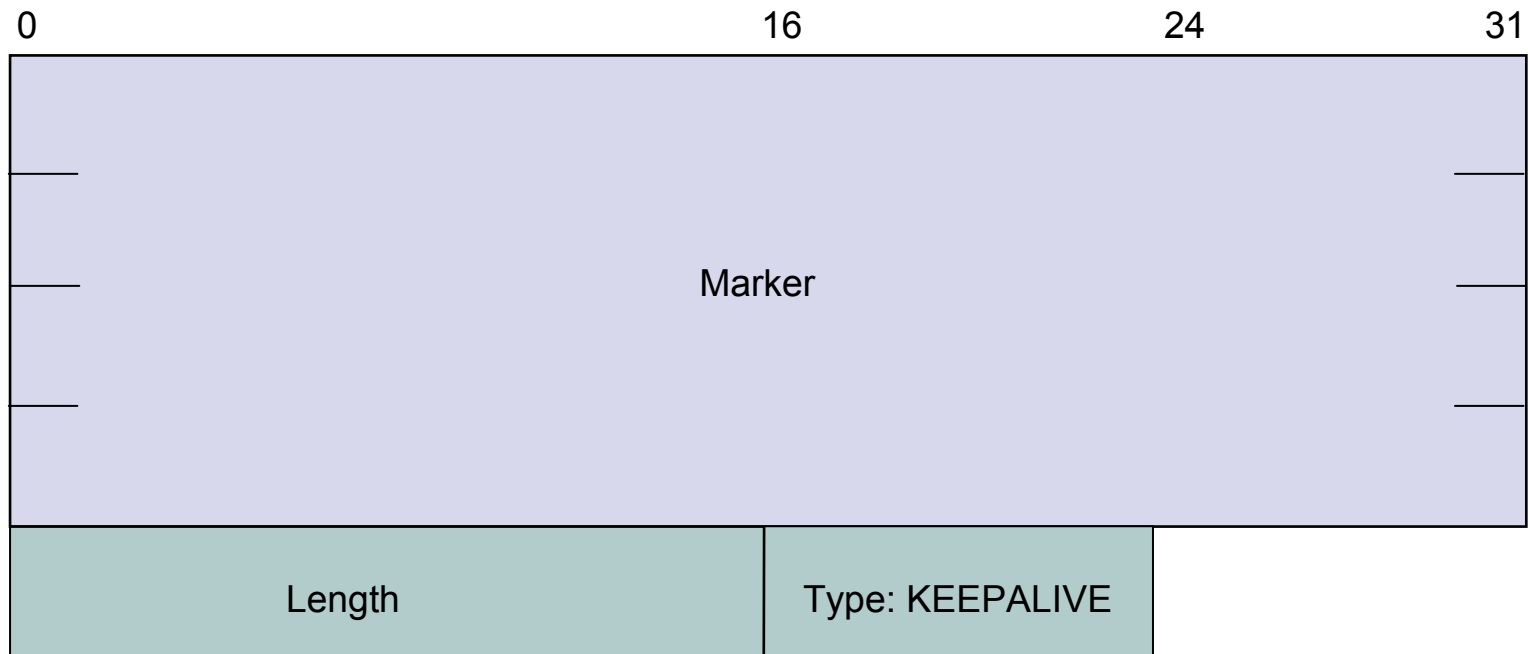


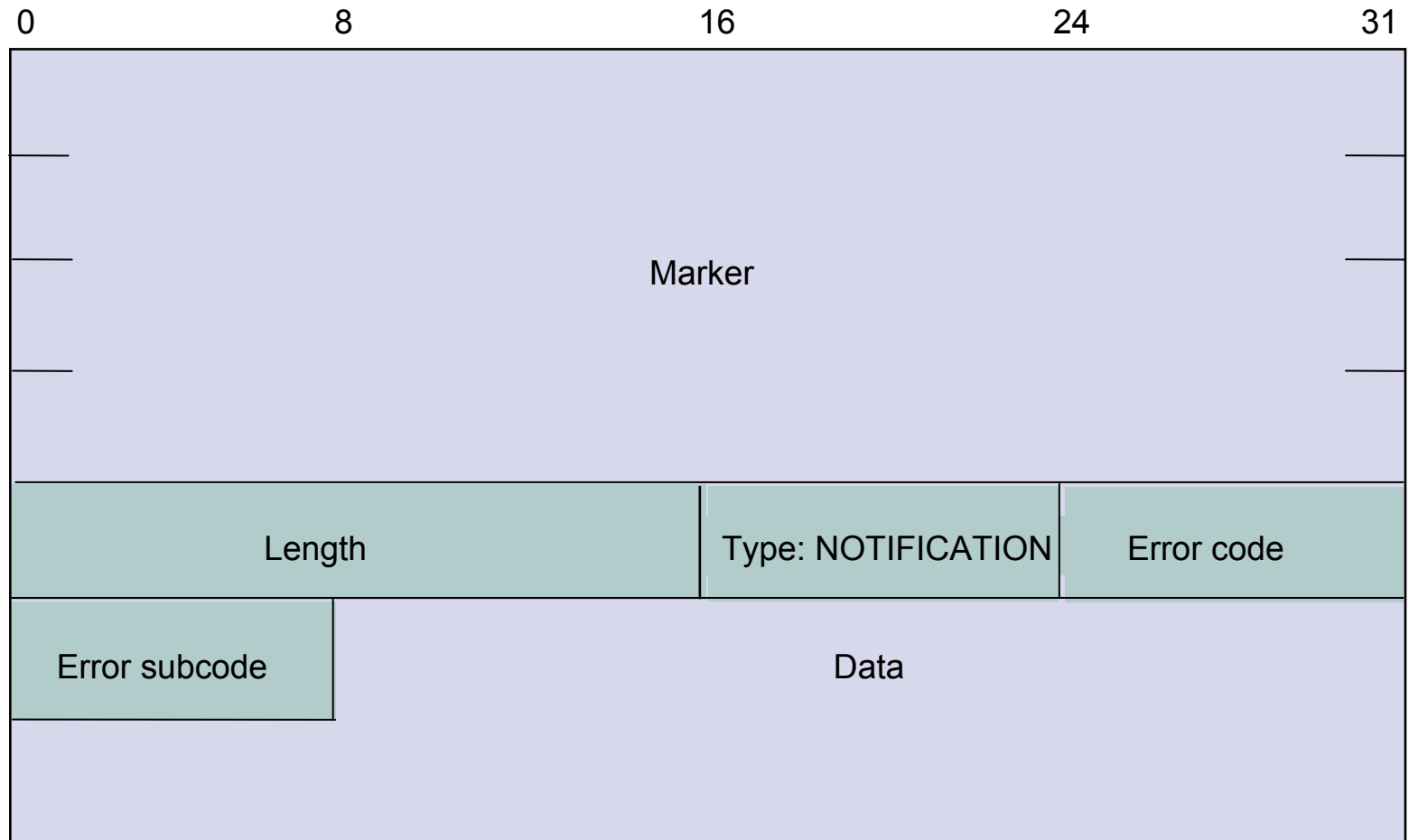




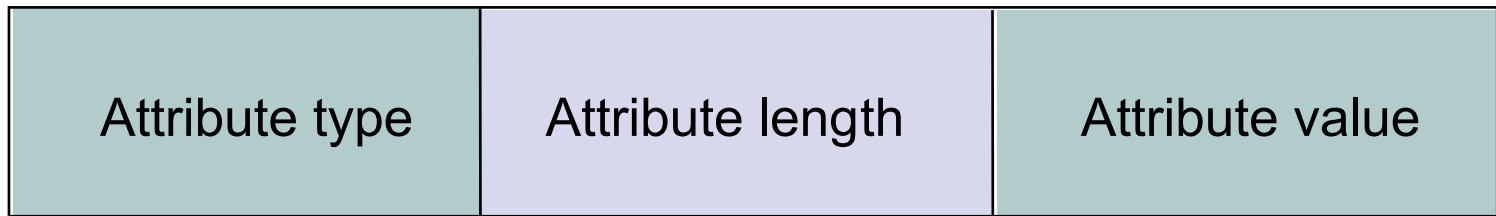


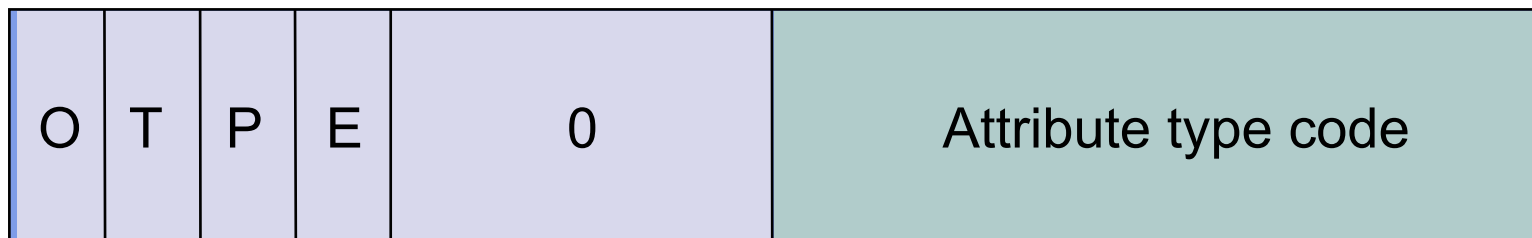


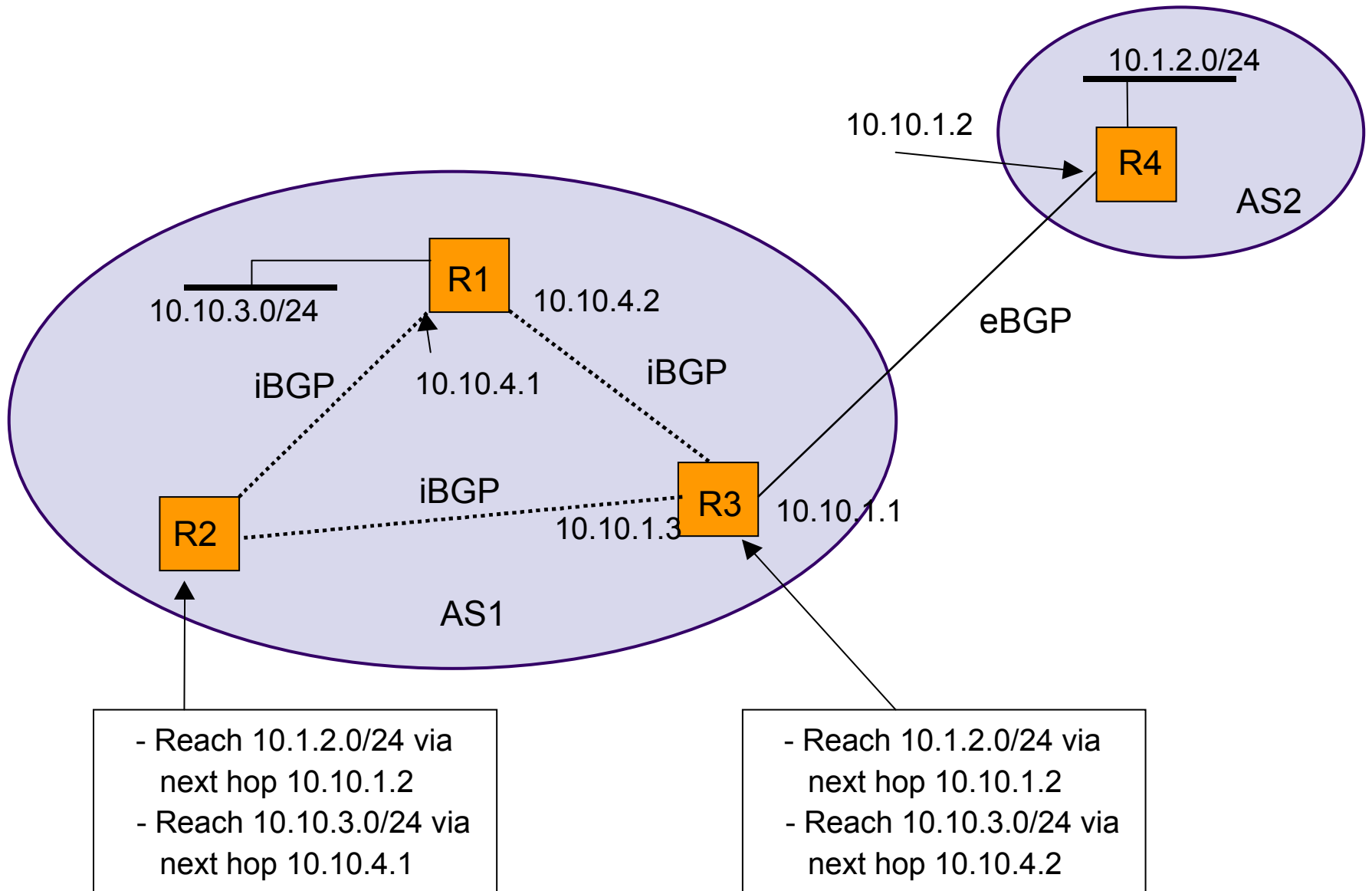


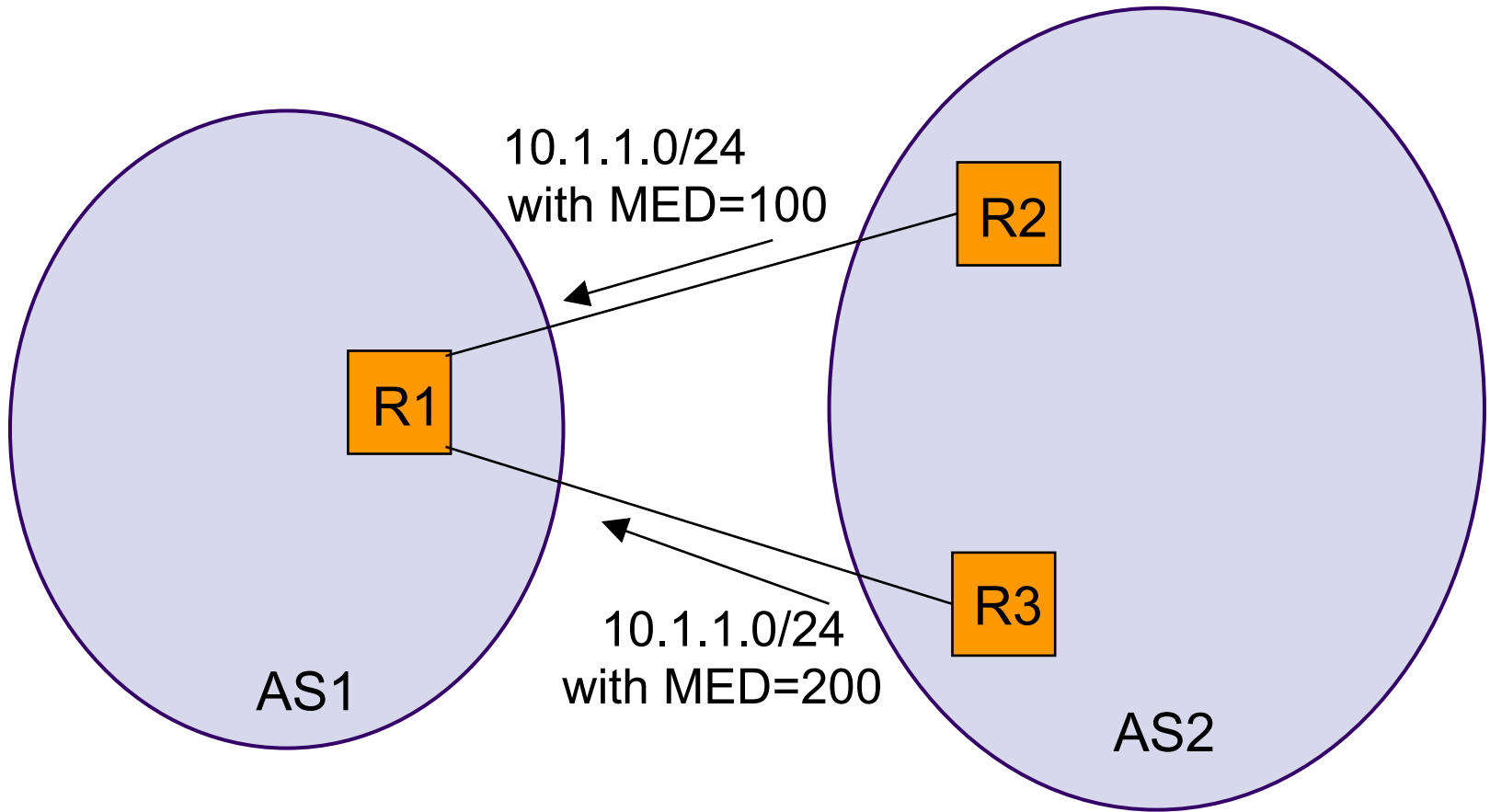


Unfeasible routes length (two octets)
Withdrawn routes (variable)
Total path attribute length (two octets)
Path attributes (variable)
Network layer reachability information (variable)









bgp.pcap.gz - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
12	8.338115	192.168.0.15	192.168.0.33	BGP	KEEPALIVE Message
13	8.342206	192.168.0.33	192.168.0.15	BGP	KEEPALIVE Message
16	8.544149	192.168.0.15	192.168.0.33	BGP	KEEPALIVE Message, UPDATE Message,
17	8.549476	192.168.0.33	192.168.0.15	BGP	UPDATE Message
19	8.562733	192.168.0.33	192.168.0.15	BGP	KEEPALIVE Message

Frame 17 (118 bytes on wire, 118 bytes captured)

- Ethernet II, Src: 00:00:0c:35:0e:1c, Dst: 00:c0:4f:23:c5:95
- Internet Protocol, Src Addr: 192.168.0.33 (192.168.0.33), Dst Addr: 192.168.0.15 (192.168.0.15)
- Transmission Control Protocol, Src Port: 179 (179), Dst Port: 2124 (2124), Seq: 2051072118, Ack: 35
- Border Gateway Protocol
 - UPDATE Message
 - Marker: 16 bytes
 - Length: 64 bytes
 - Type: UPDATE Message (2)
 - Unfeasible routes length: 0 bytes
 - Total path attribute length: 39 bytes
 - Path attributes
 - ORIGIN: EGP (4 bytes)
 - AS_PATH: empty (3 bytes)
 - NEXT_HOP: 192.168.0.33 (7 bytes)
 - MULTI_EXIT_DISC: 0 (7 bytes)
 - LOCAL_PREF: 100 (7 bytes)
 - COMMUNITIES: 65033:500 65033:600 (11 bytes)
 - Network layer reachability information: 2 bytes
 - 10.0.0.0/8

```

0000  00 c0 4f 23 c5 95 00 00 0c 35 0e 1c 08 00 45 c0  ..O#.... .5....E.
0010  00 68 00 05 00 00 ff 06 39 4a c0 a8 00 21 c0 a8  .h..... 9J...!..
0020  00 0f 00 b3 08 4c 7a 40 e0 76 d6 33 9e 6a 50 18  .....Lz@ .v.3.jP.
0030  3e f8 1d 7e 00 00 ff ff ff ff ff ff ff ff ff ff  >...~.... ....
0040  ff ff ff ff ff ff 00 40 02 00 00 00 27 40 01 01  .....@ ....'@..

```

Filter: [] [Reset] [Apply] File: bgp.pcap.gz

