Internet Protocol - IP

2017/18 Q2

Jaime Delgado

DAC – UPC

Contents

- Unit 1: IP.
- Unit 2: Other supporting protocols and services.
- Unit 3: Routing algorithms.
- Unit 4: Security.

Contents Unit 1

IP:

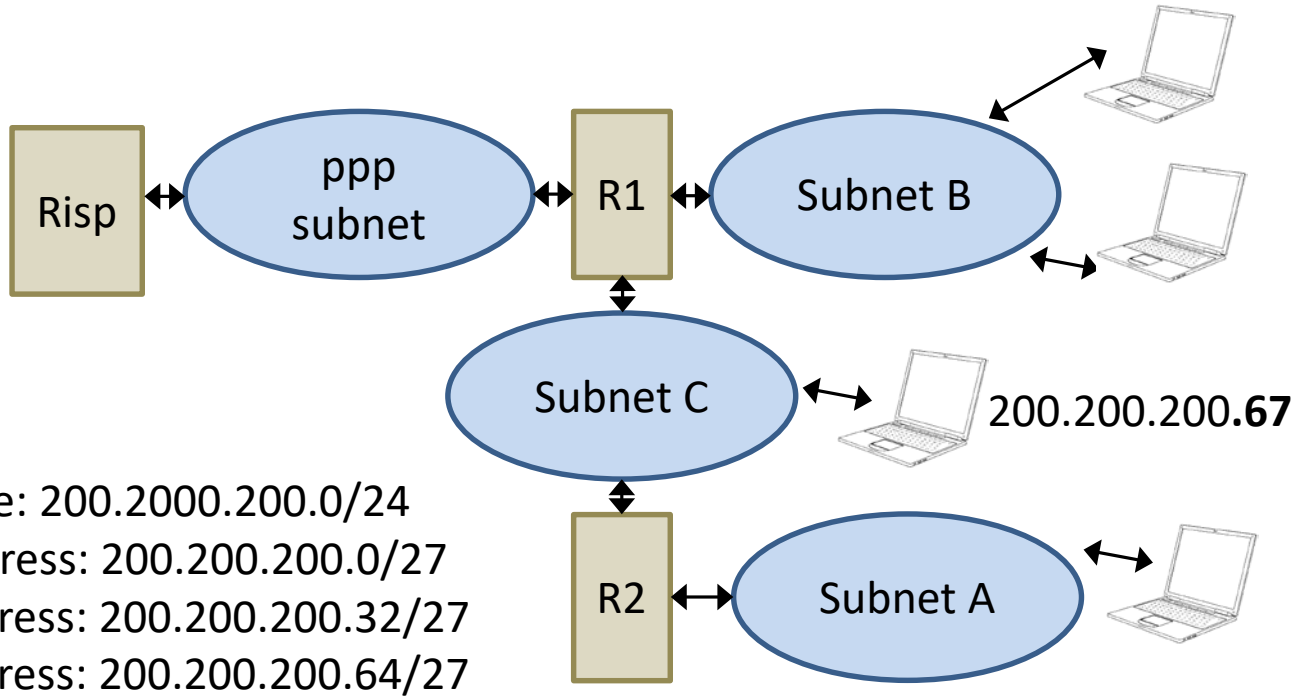
- IP addresses.
- Routing tables.
- Fragmentation.
- IP protocol (header).

Contents Unit 1

IP:

- IP addresses.
- **Routing tables.**
- Fragmentation.
- IP protocol (header).

Subnet example



Address range: 200.2000.200.0/24
Subnet A address: 200.200.200.0/27
Subnet B address: 200.200.200.32/27
Subnet C address: 200.200.200.64/27
ppp subnet address: 200.200.202.0/30

R1 interfaces:
ppp0, e0 (subnet B), e1 (subnet C)
R2 interfaces:
e0 (subnet C), e1 (subnet B)

R1 ppp address: 200.200.**202.1**
Risp ppp address: 200.200.**202.2**
R1 subnet **B** address: 200.200.200.**33**
R1 subnet **C** address: 200.200.200.**66**
R2 subnet **A** address: 200.200.200.**1**
R2 subnet **C** address: 200.200.200.**65**

Routing table 200.200.200.67

Where do I want to go?		How do I get there?	
Destination network	**Mask**	**Gateway**	**Interface**
.64 (my subnet, C)	/27	Direct	E0
.0 (subnet A)	/27	.65 (R2)	E0
.32 (subnet B)	/27	.66 (R1)	E0
0.0.0.0 (rest of the world)	/0	.66 (R1)	E0

Routing table Router R1

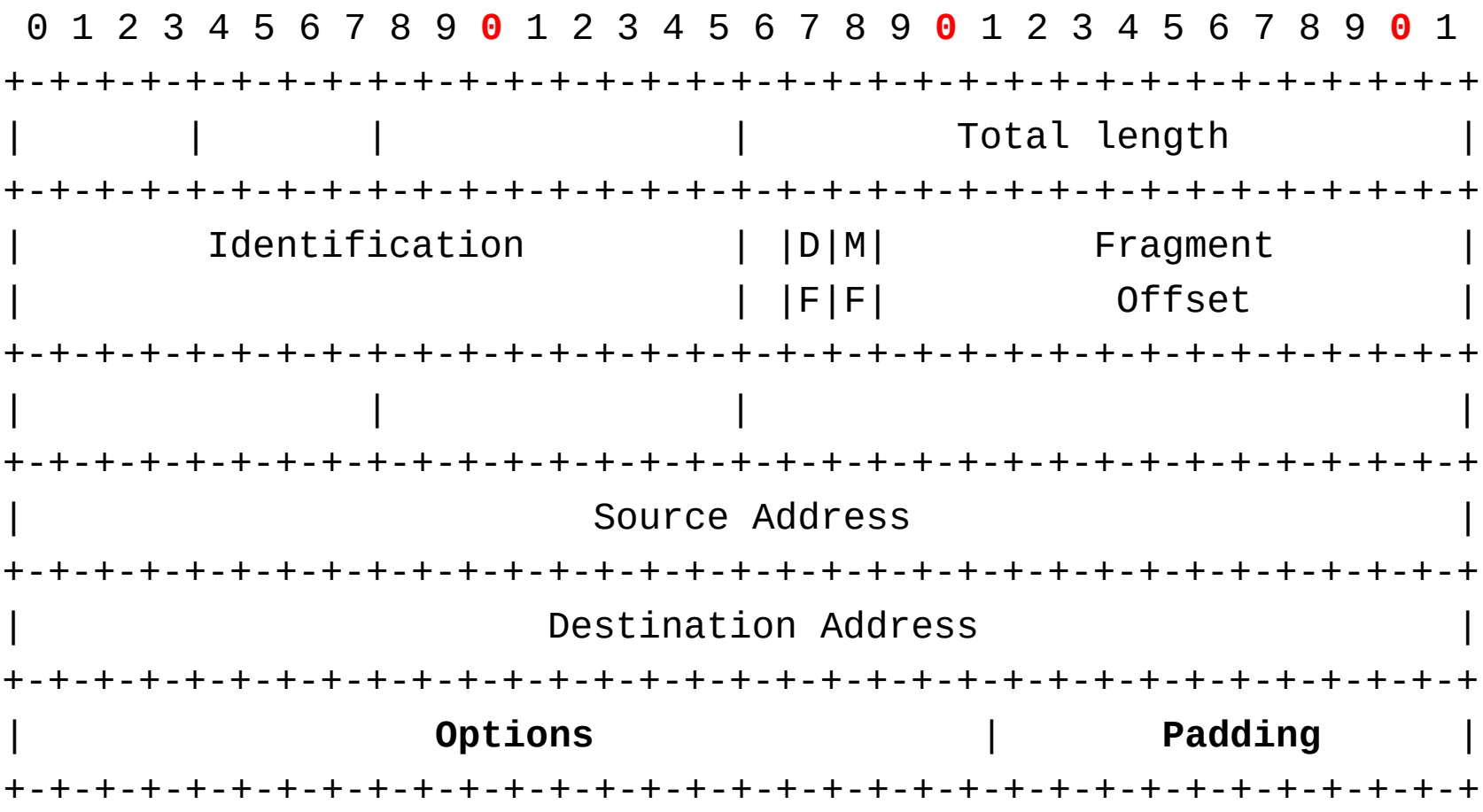
Where do I want to go?		How do I get there?	
Destination network	**Mask**	**Gateway**	**Interface**
.32 (my subnet, B)	/27	Direct	E0
.64 (my subnet C)	/27	Direct	E1
.0 (subnet A)	/27	.65 (R2)	E1
0.0.0.0 (rest of the world)	/0	200.200.202 .2 (Risp)	ppp0

Contents Unit 1

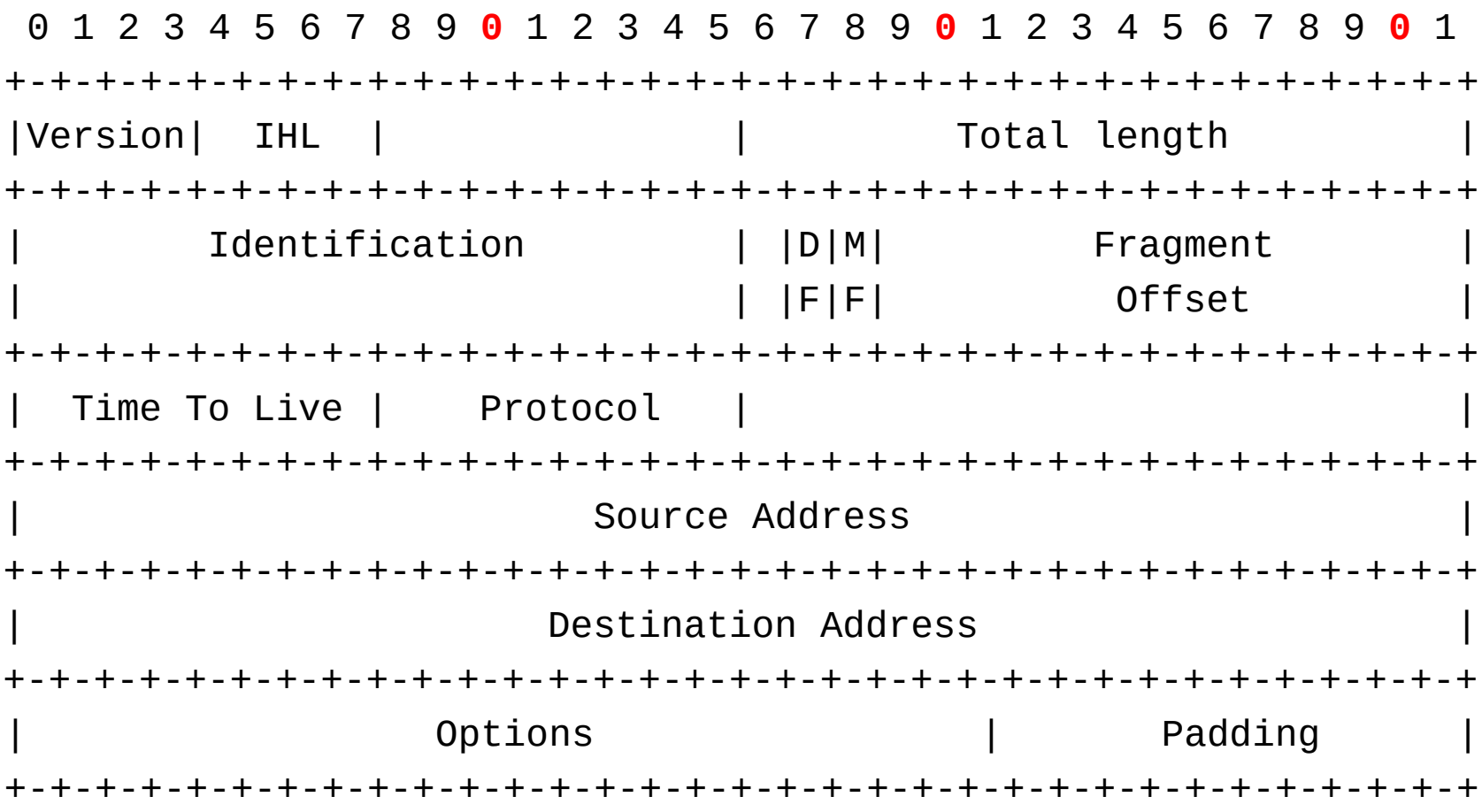
IP:

- IP addresses.
- Routing tables.
- Fragmentation.
- **IP protocol (header).**

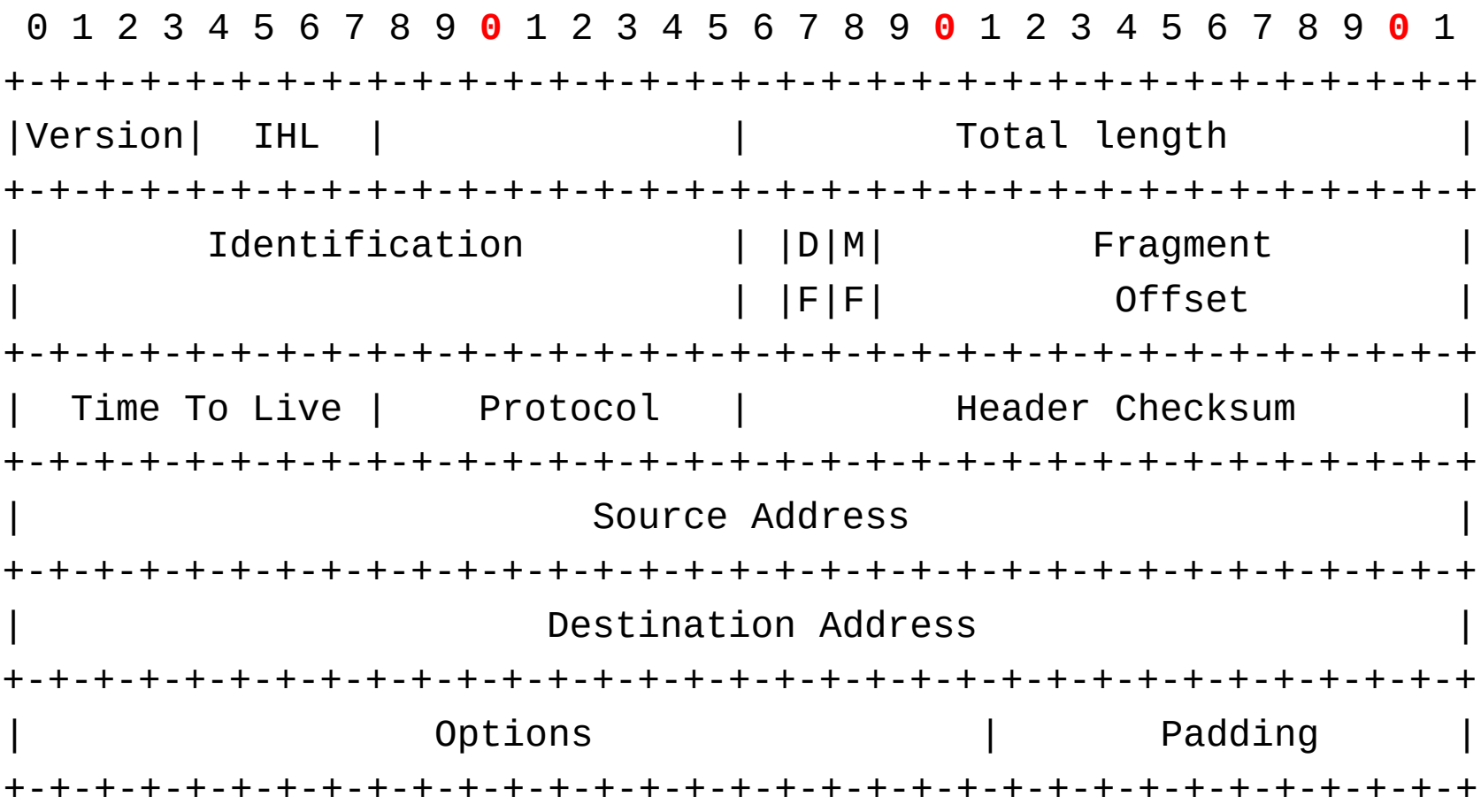
IP Header


0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Total length
Identification
D
M
F
F
Fragment
Offset
Source Address
Destination Address
Options
Padding

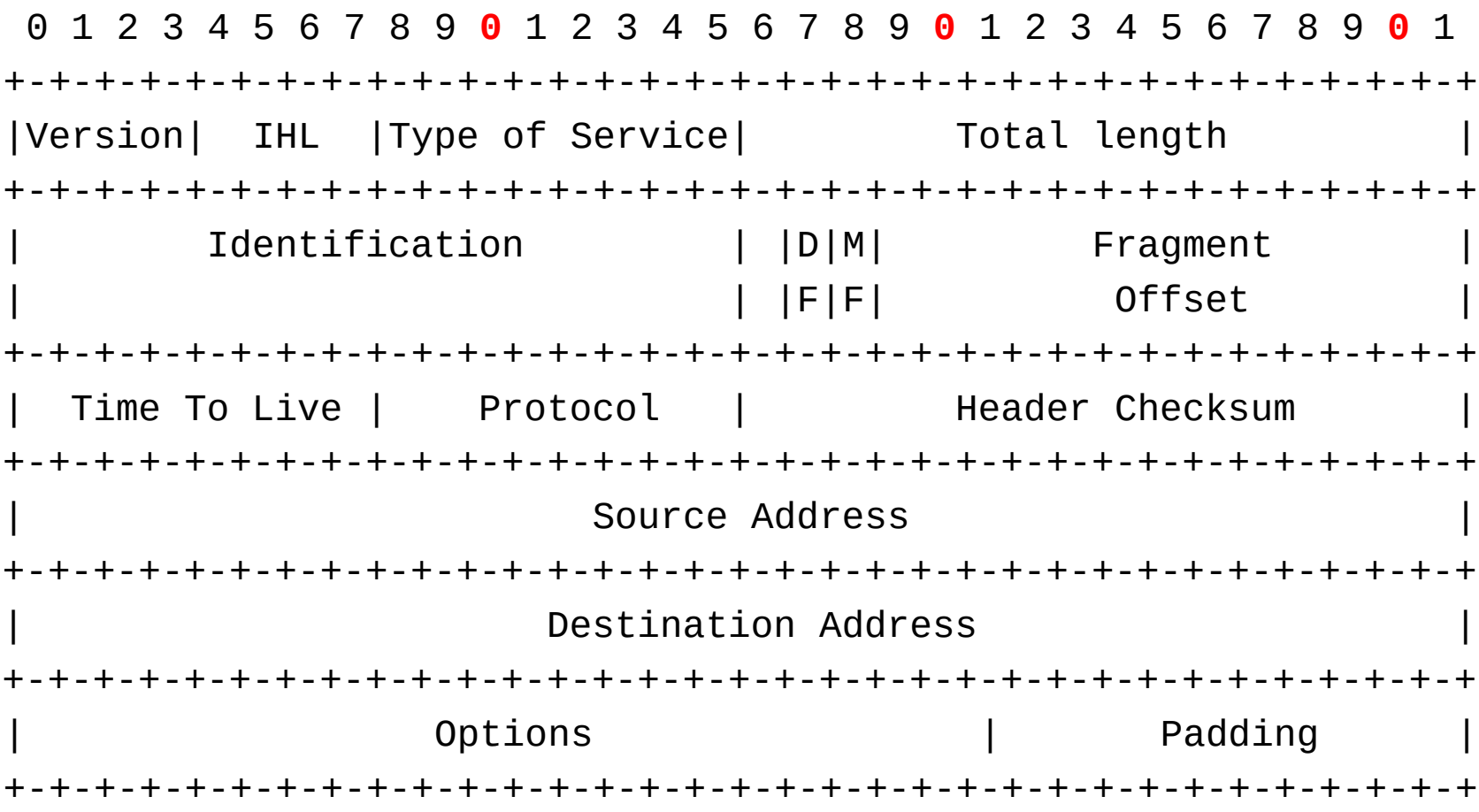
IP Header


0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Total length
Identification
D
M
F
F
Fragment Offset
Time To Live
Protocol
Source Address
Destination Address
Options
Padding

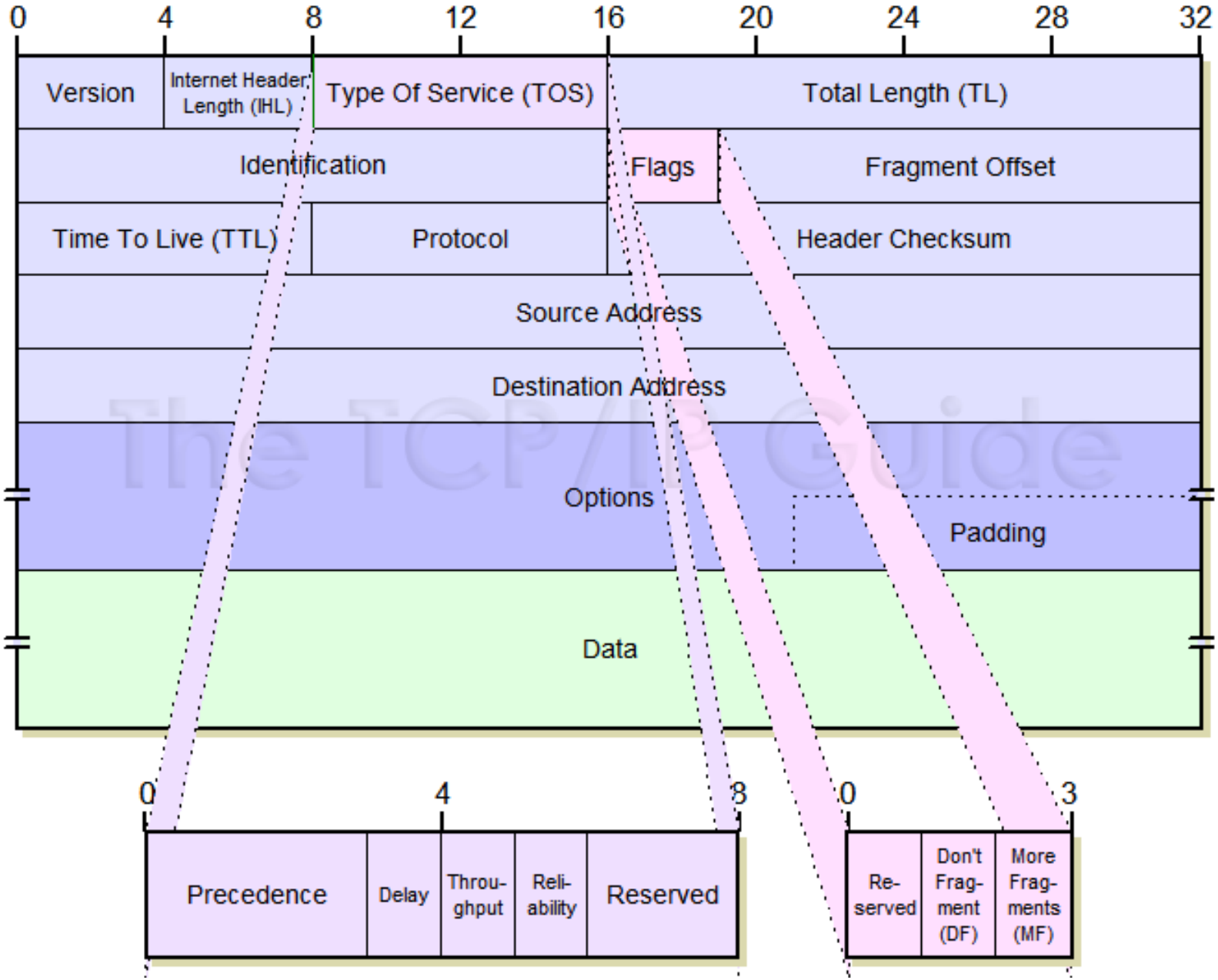
IP Header


0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Total length
Identification
D
M
Fragment Offset
Time To Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding

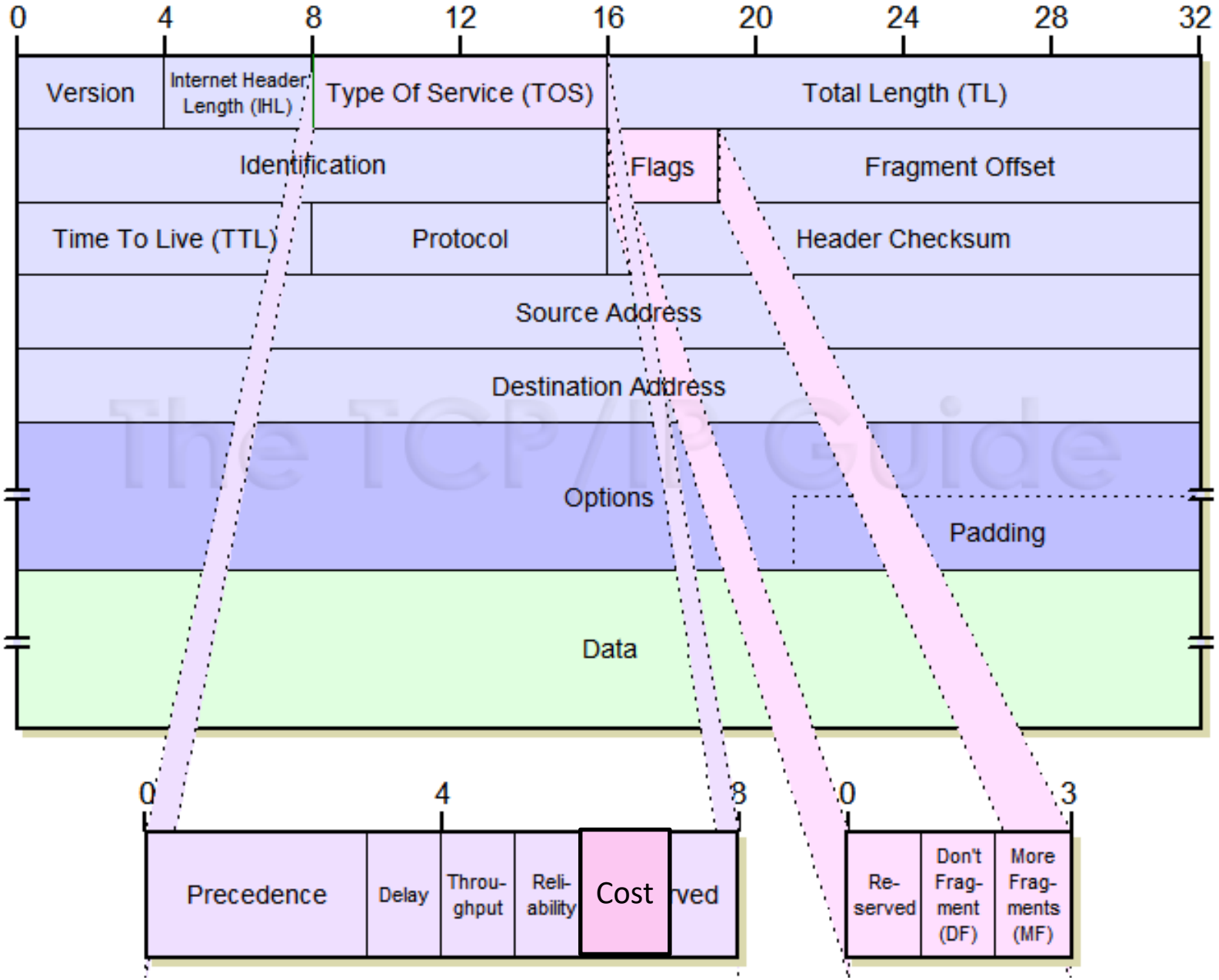
IP Header


0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Type of Service
Total length
Identification
D
M
F
F
Fragment Offset
Time To Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding

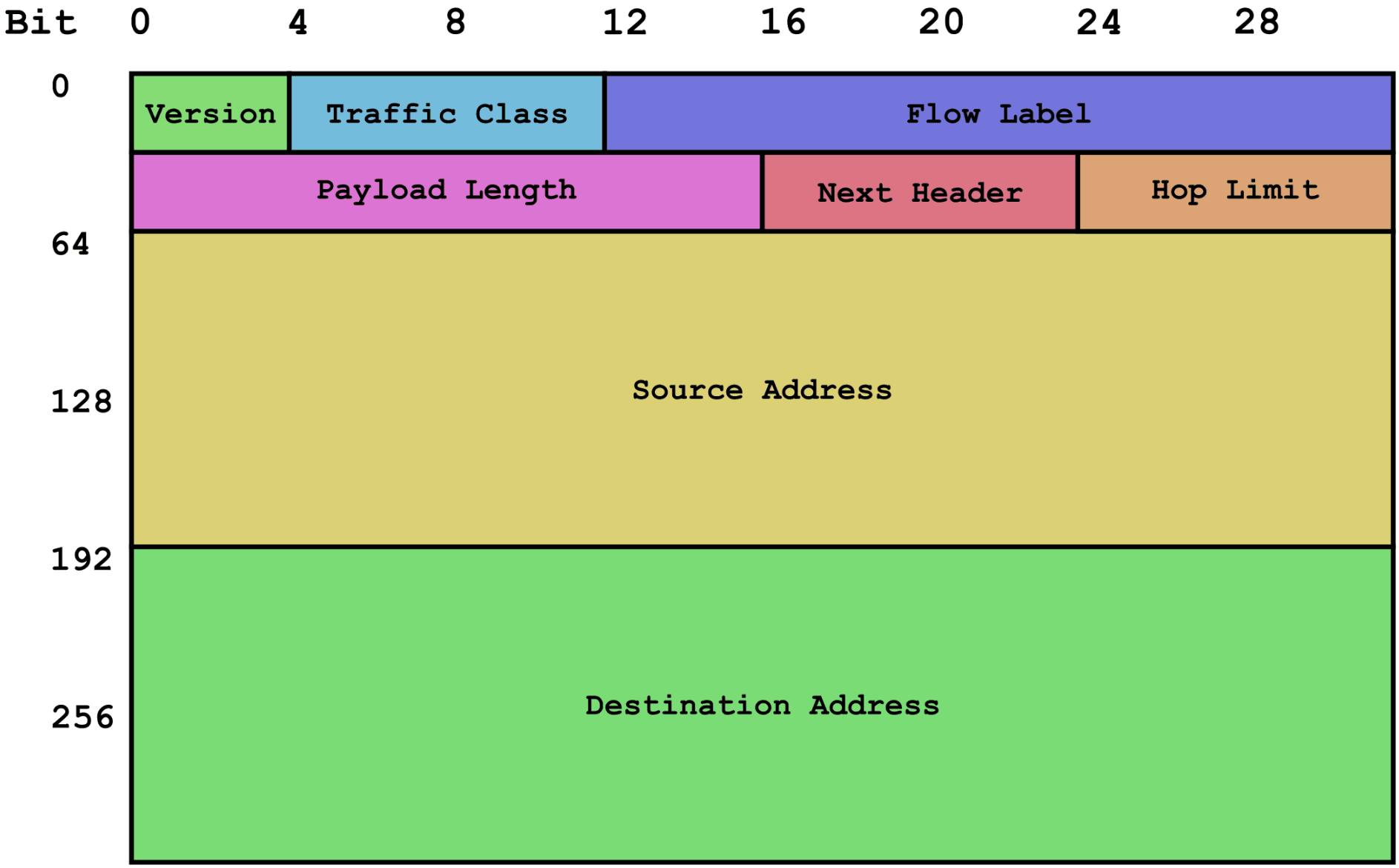
IPv4 Header


0
4
8
12
16
20
24
28
32
Version
Internet Header Length (IHL)
Type Of Service (TOS)
Total Length (TL)
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data
0
4
8
Precedence
Delay
Throu-ghput
Reli-ability
Reserved
0
3
Re-served
Don't Frag-ment (DF)
More Frag-ments (MF)

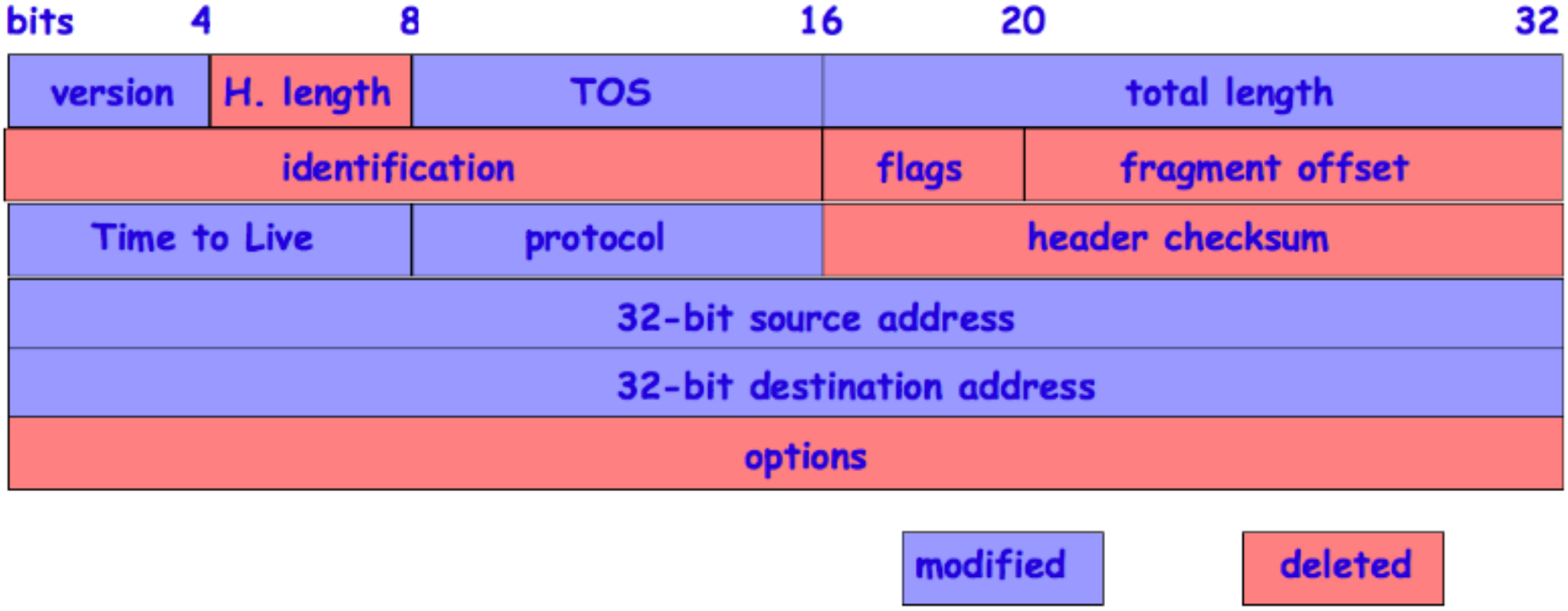
IPv4 Header


0
4
8
12
16
20
24
28
32
Version
Internet Header Length (IHL)
Type Of Service (TOS)
Total Length (TL)
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data
0
4
8
Precedence
Delay
Throu-ghput
Reli-ability
Cost
rved
0
3
Re-served
Don't Frag-ment (DF)
More Frag-ments (MF)

IPv6 Header


Bit
0
4
8
12
16
20
24
28
0
64
128
192
256
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address

IPv4 vs. IPv6 Header



Contents Unit 2

Other supporting protocols and services:

- ARP (Address Resolution Protocol).
- ICMP (Internet Control Message Protocol).
- DHCP (Dynamic Host Configuration Protocol).
- NAT (Network Address Translation).
- DNS (Domain Name System).

Contents Unit 2

Other supporting protocols and services:

- ARP (Address Resolution Protocol).
- ICMP (Internet Control Message Protocol).
- DHCP (Dynamic Host Configuration Protocol).
- **NAT (Network Address Translation).**
- DNS (Domain Name System).

NAT (Network Address Translation)

- Service in Router
- NAT table: Private and (mapped) Public addresses

Private address	Public address

- Static and Dynamic (more efficient)
- IP-address and Port (*transport address*) (other info if other protocols): **NAPT** or **PAT** (P="port")

Private address	Local port	Public address	External port

- If communication starts from outside:
  DNAT (Destination NAT)

Contents Unit 2

Other supporting protocols and services:

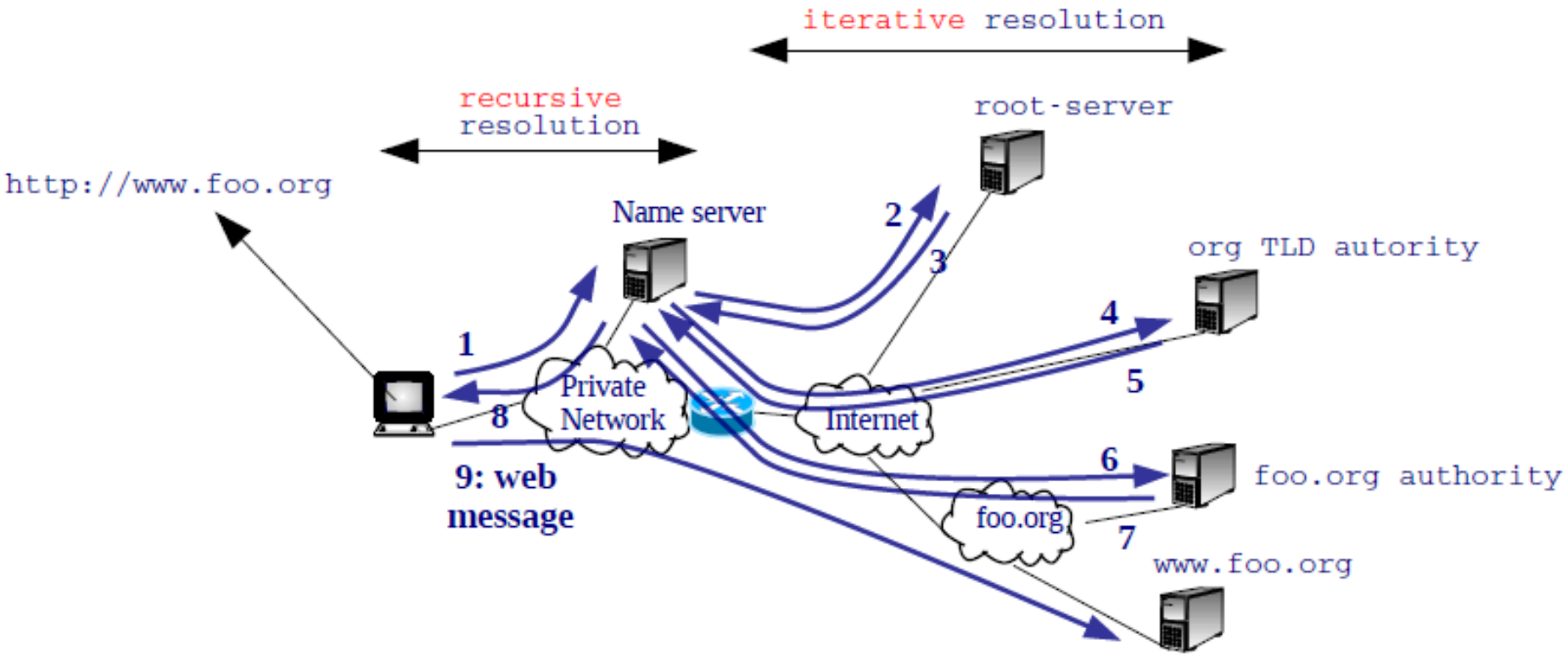
- ARP (Address Resolution Protocol).
- ICMP (Internet Control Message Protocol).
- DHCP (Dynamic Host Configuration Protocol).
- NAT (Network Address Translation).
- **DNS (Domain Name System).**

DNS (Domain Name System)

- Application protocol needed for IP:
  - Obtain IP addresses from “names”.
- Domain/sub-domain/host name:
  - Hierarchical structure: “*myhost.ac.upc.edu*”
  - *.edu* is a TLD (Top Level Domain).
- IP of *myhost.ac.upc.edu* (node/host name) know by local **Name Server** of *ac.upc.edu*
- DNS format & protocol needed.

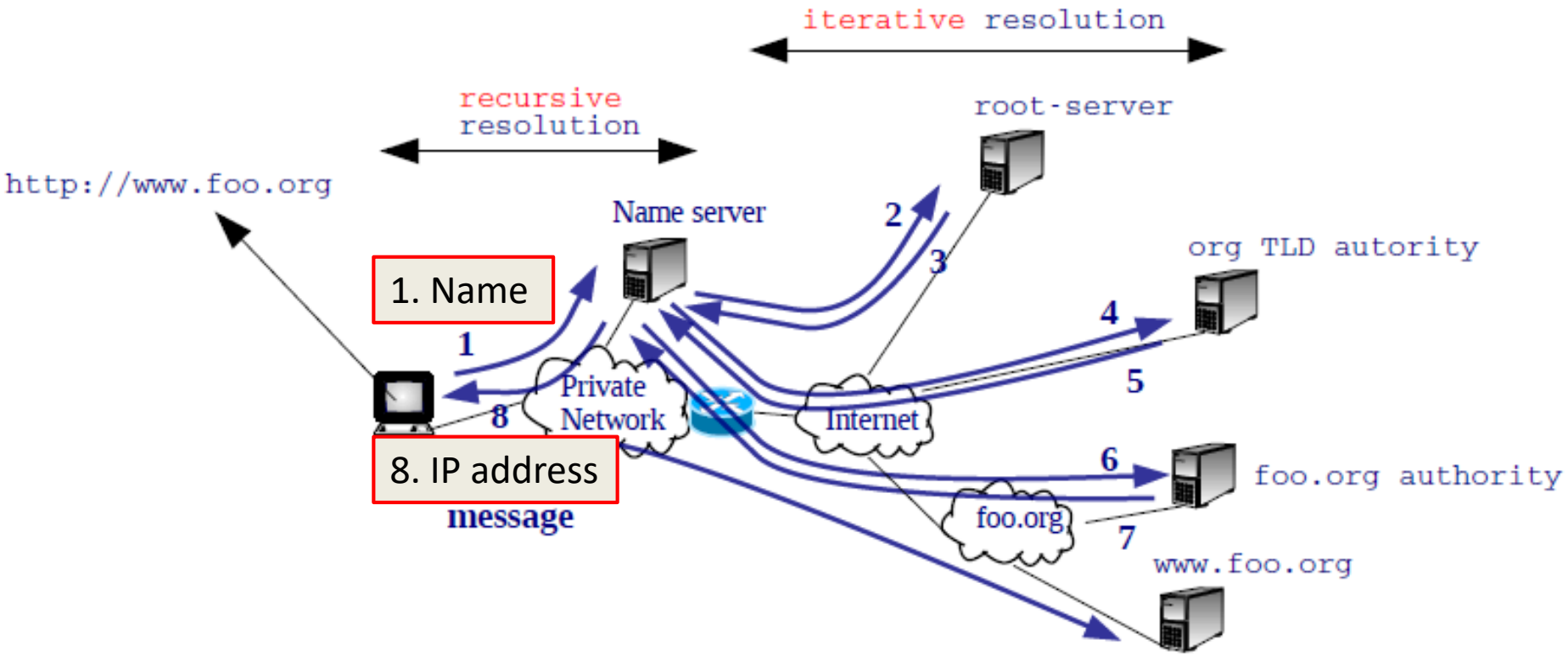
DNS (Domain Name System)

- Application protocol:



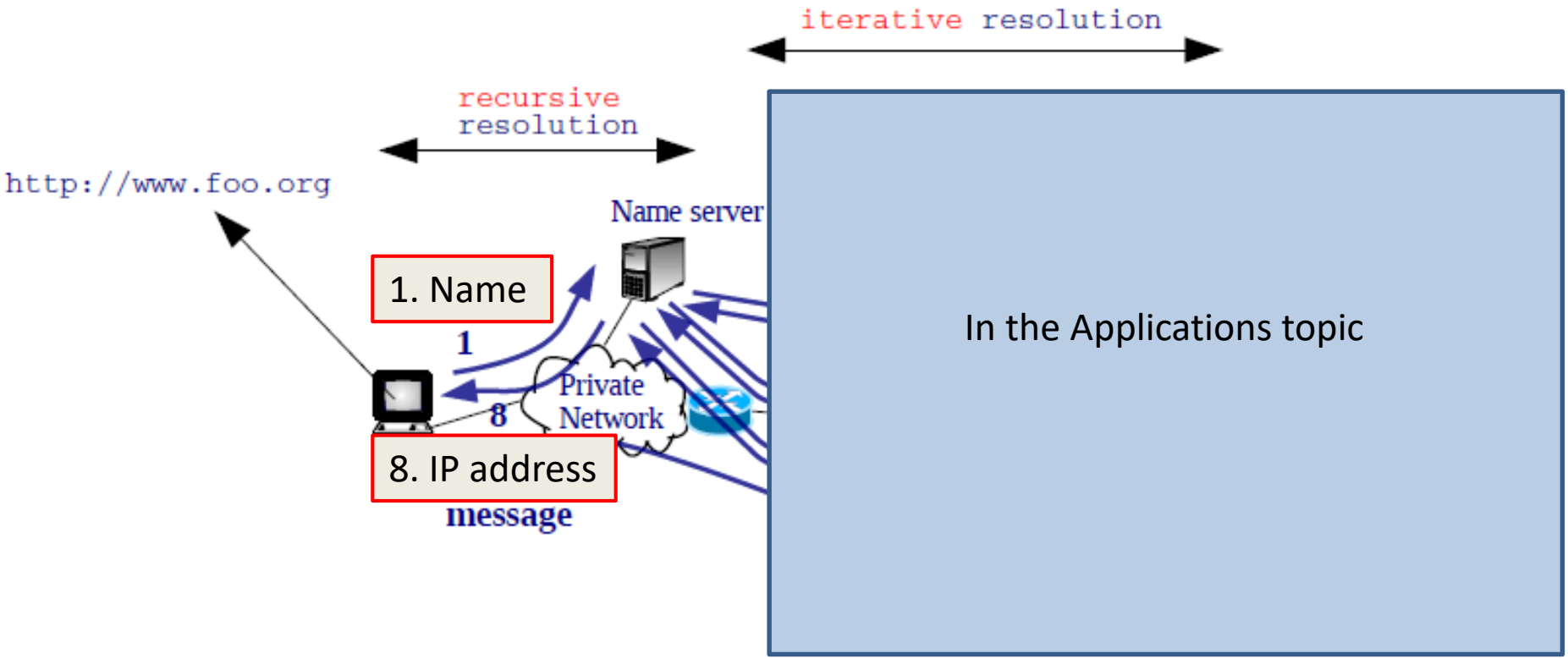
DNS (Domain Name System)

- Application protocol:



DNS (Domain Name System)

- Application protocol:



Unit 2

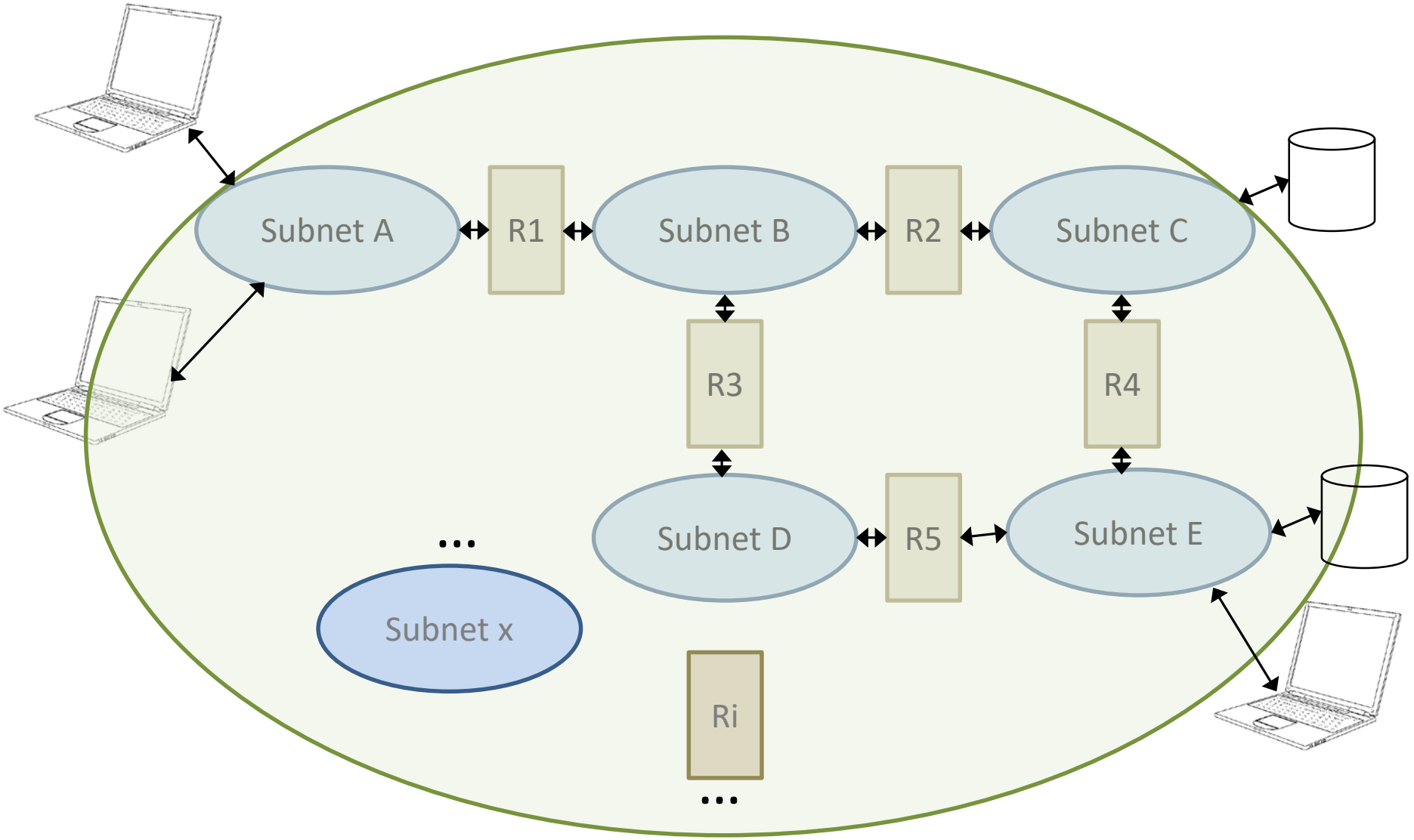
Other supporting protocols and services:

- ARP (Address Resolution Protocol).
- ICMP (Internet Control Message Protocol).
- DHCP (Dynamic Host Configuration Protocol).
- NAT (Network Address Translation).
- DNS (Domain Name System).

Example with DHCP, DNS, ARP

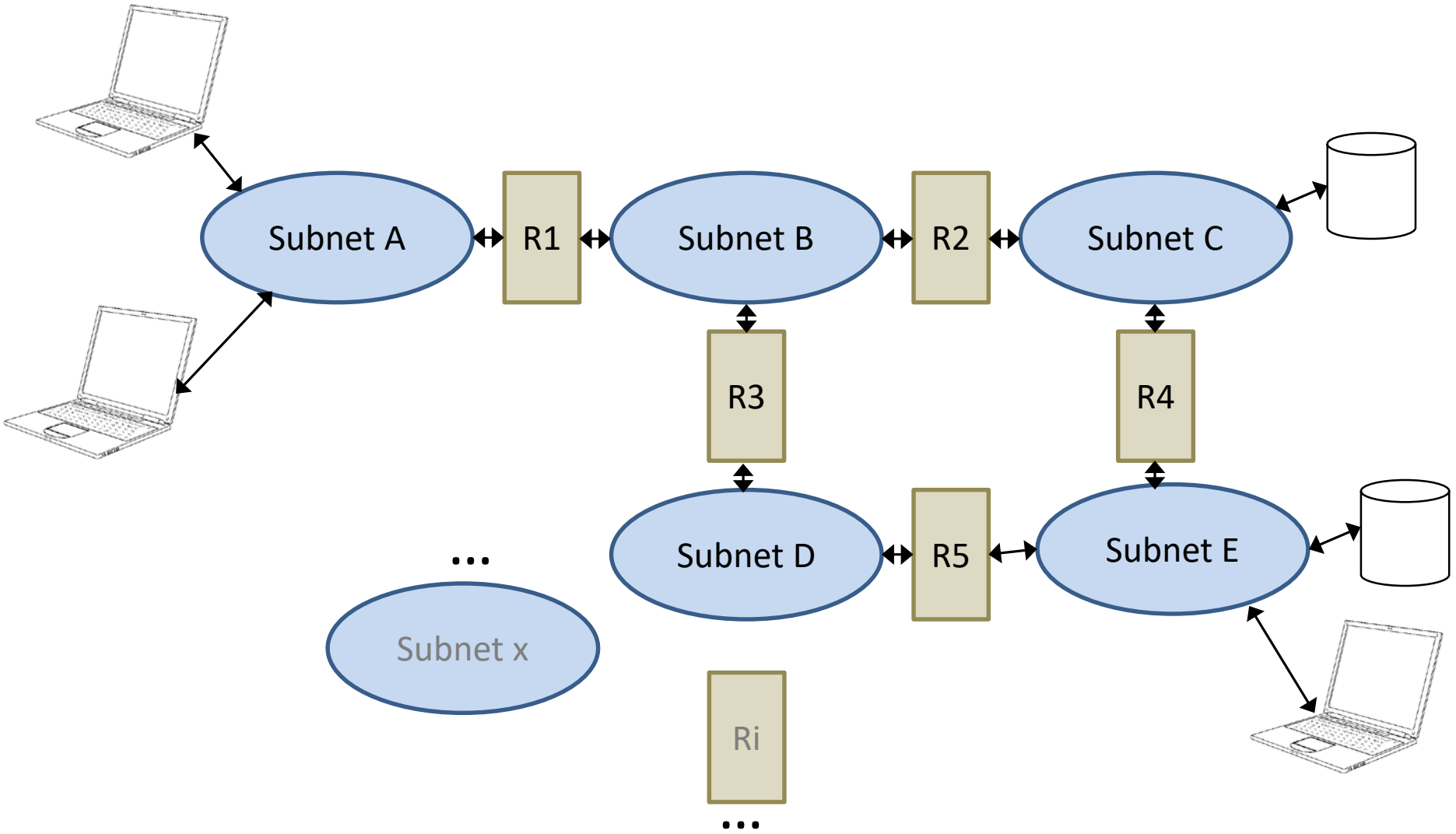
The Internet

Ri: Router



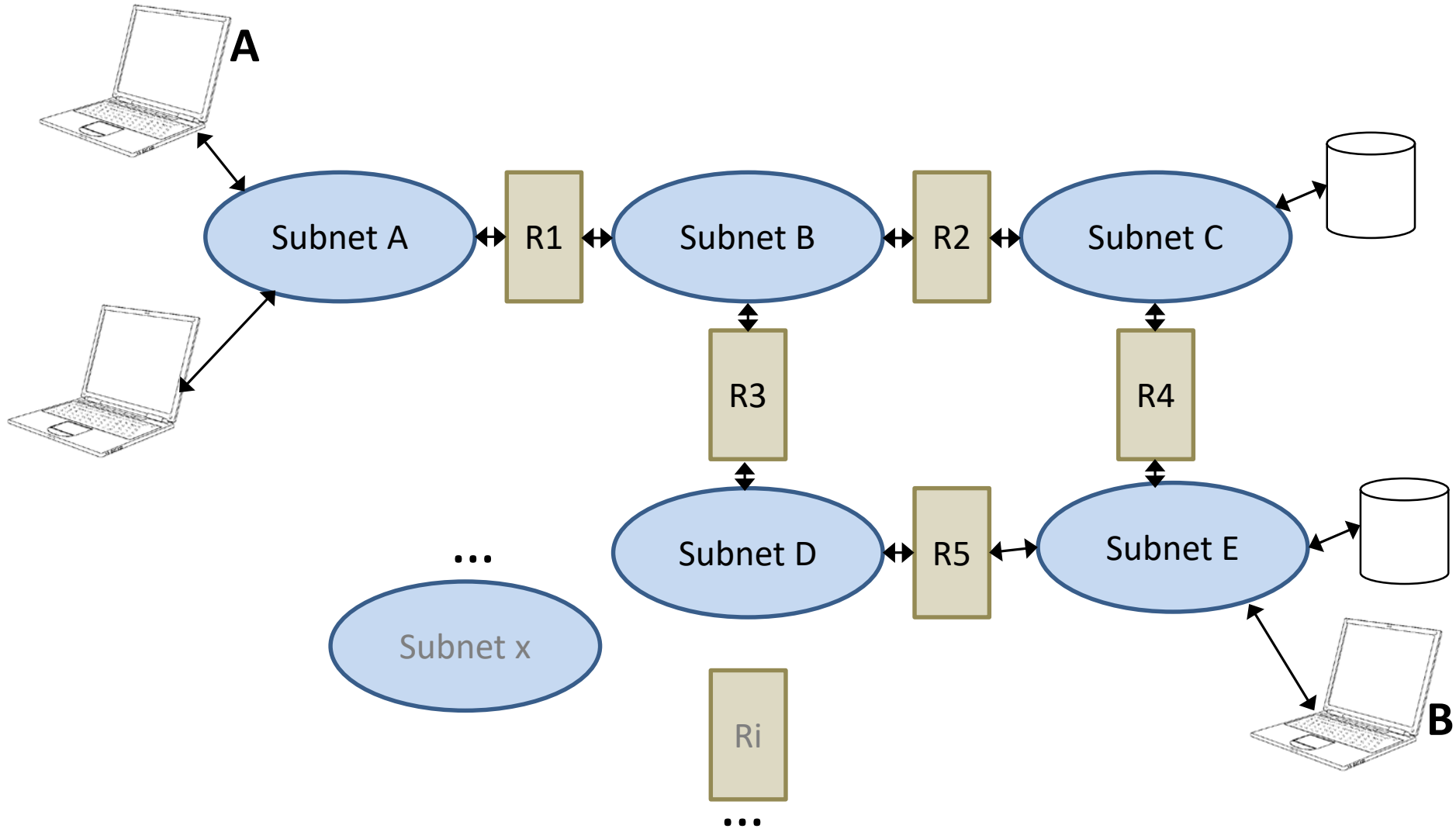
The Internet

Ri: Router

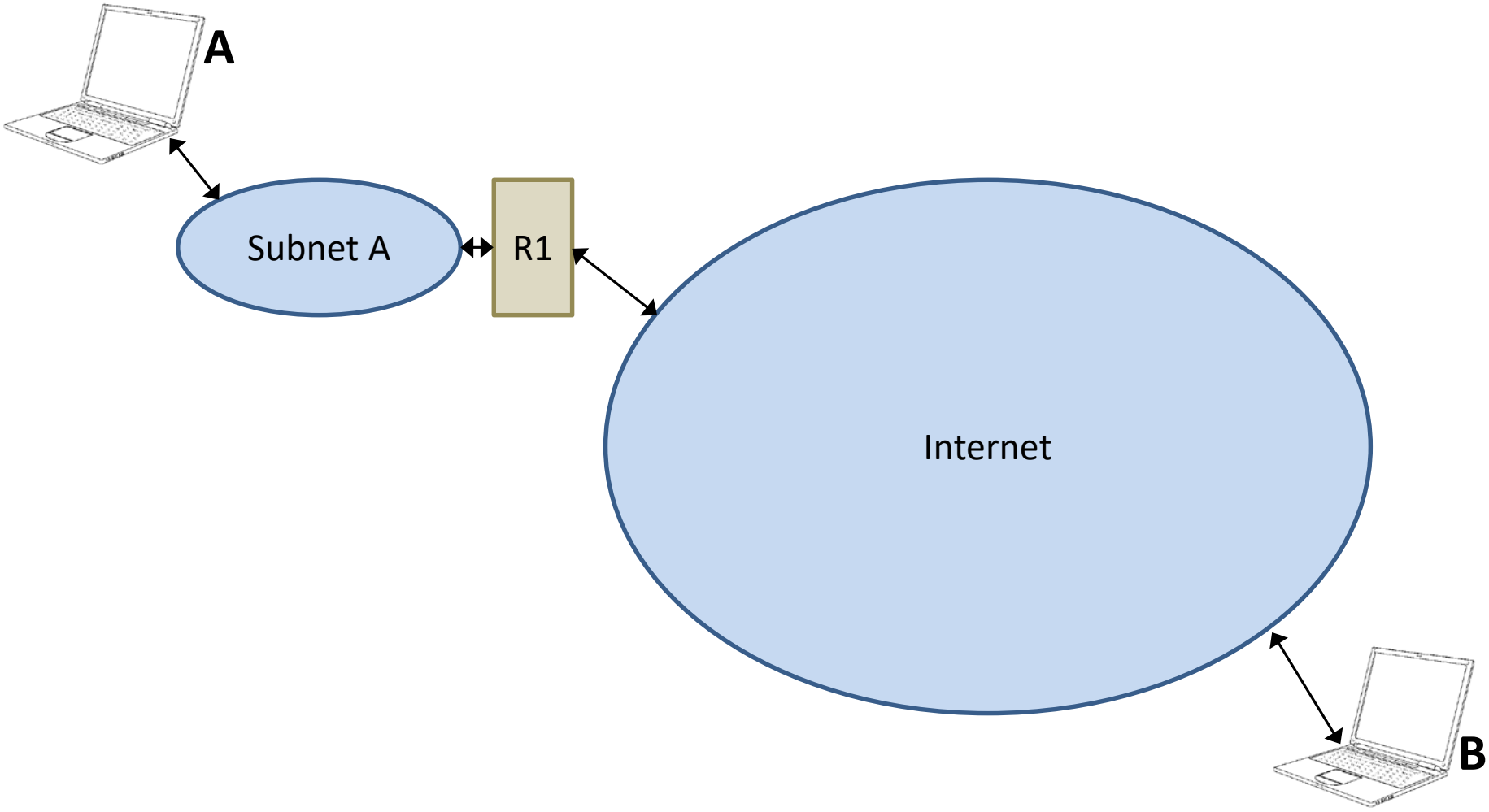


The Internet

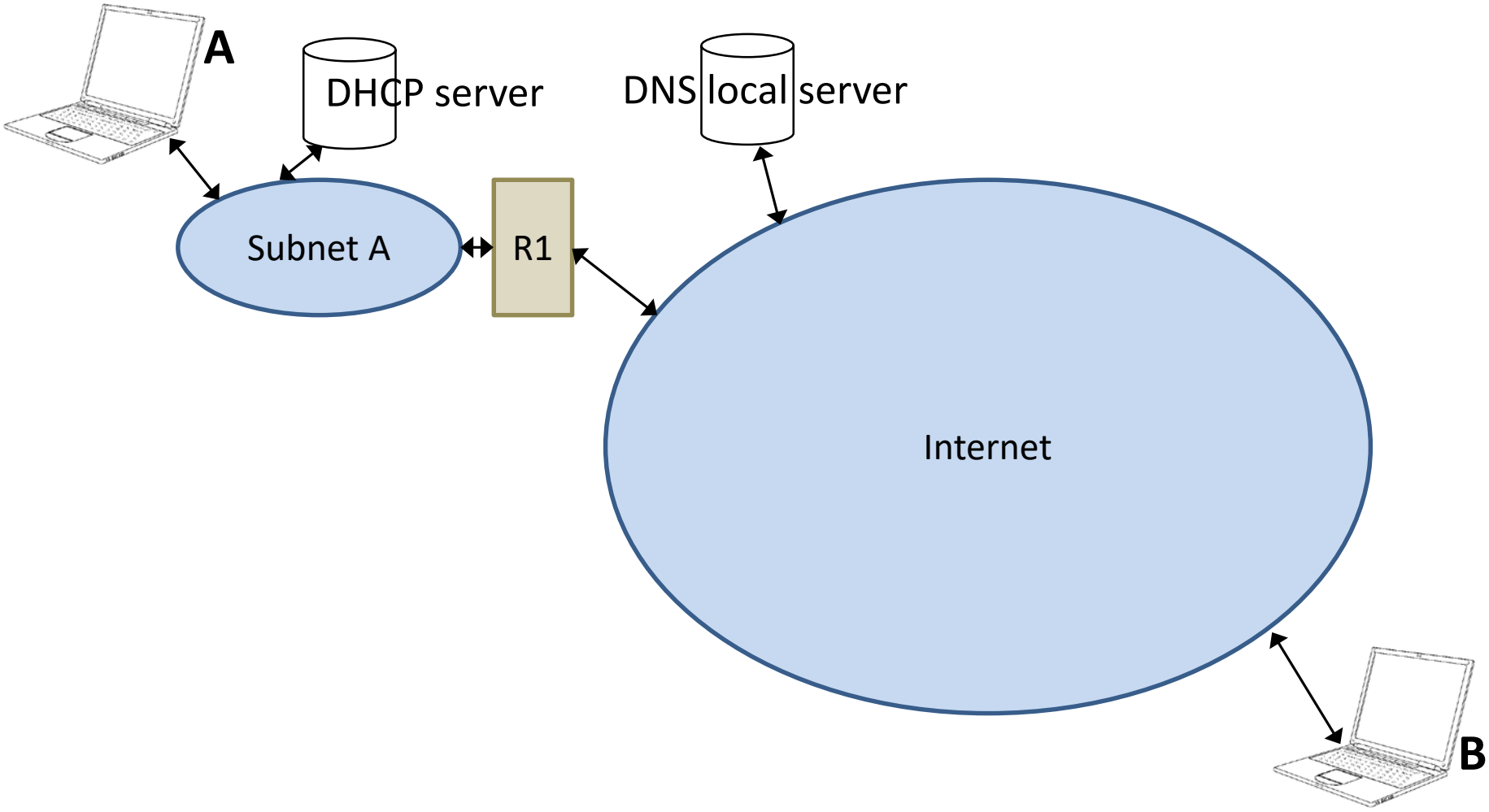
Ri: Router



A wants to send a datagram to B



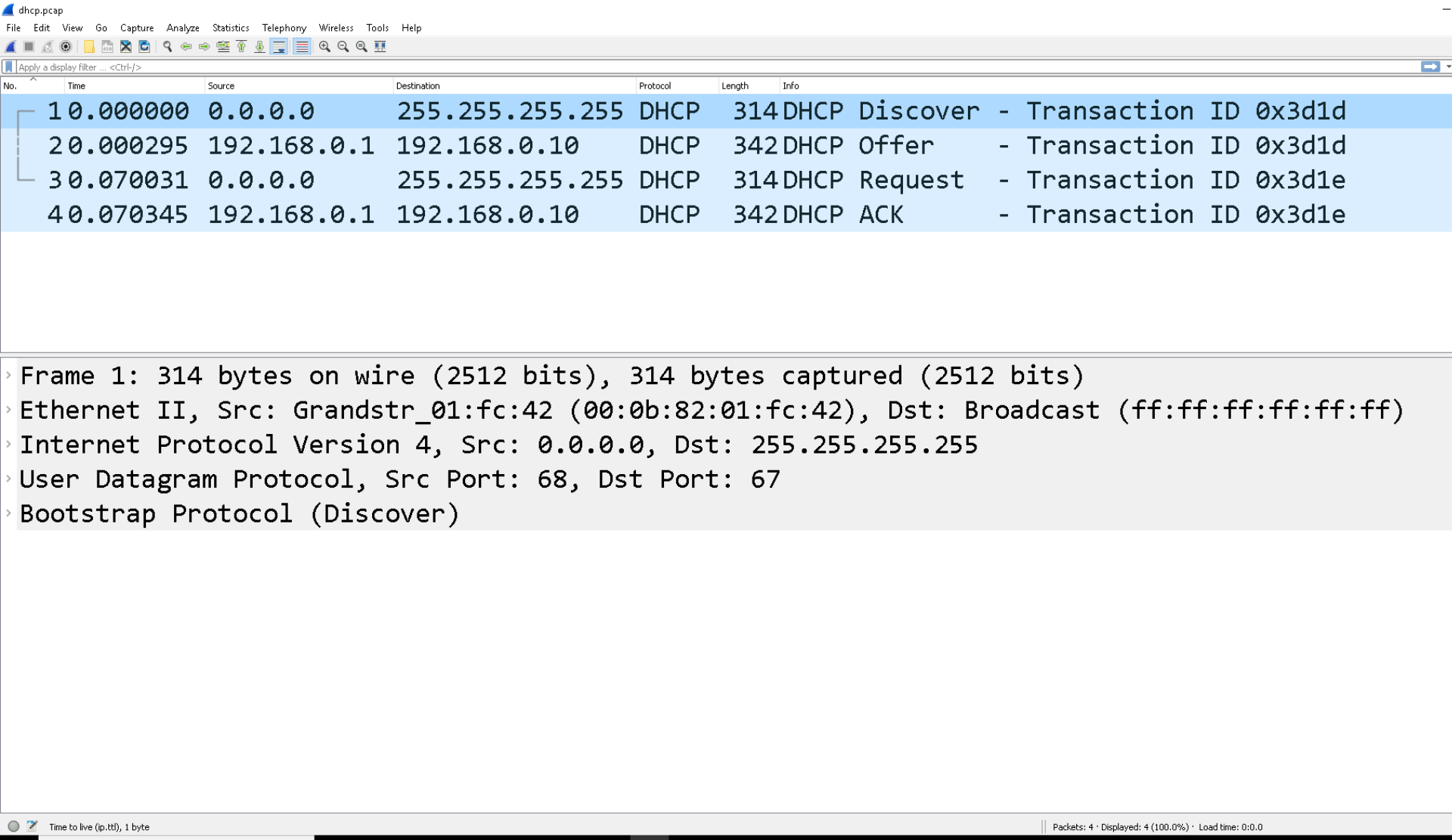
A wants to send a datagram to B



Protocols sequence

- A wants to send a datagram to B
- Host A starts → **DHCP**
- A needs to ask **DNS** for IP of host B (domain name)
- A checks *Routing Table* to know where to send DNS request (DNS server) → to R1
- A needs to find R1 → **ARP**
- A sends **DNS** Request to R1
- Once IP address of Host B known, datagram is sent to R1, after checking Routing Table.

DHCP

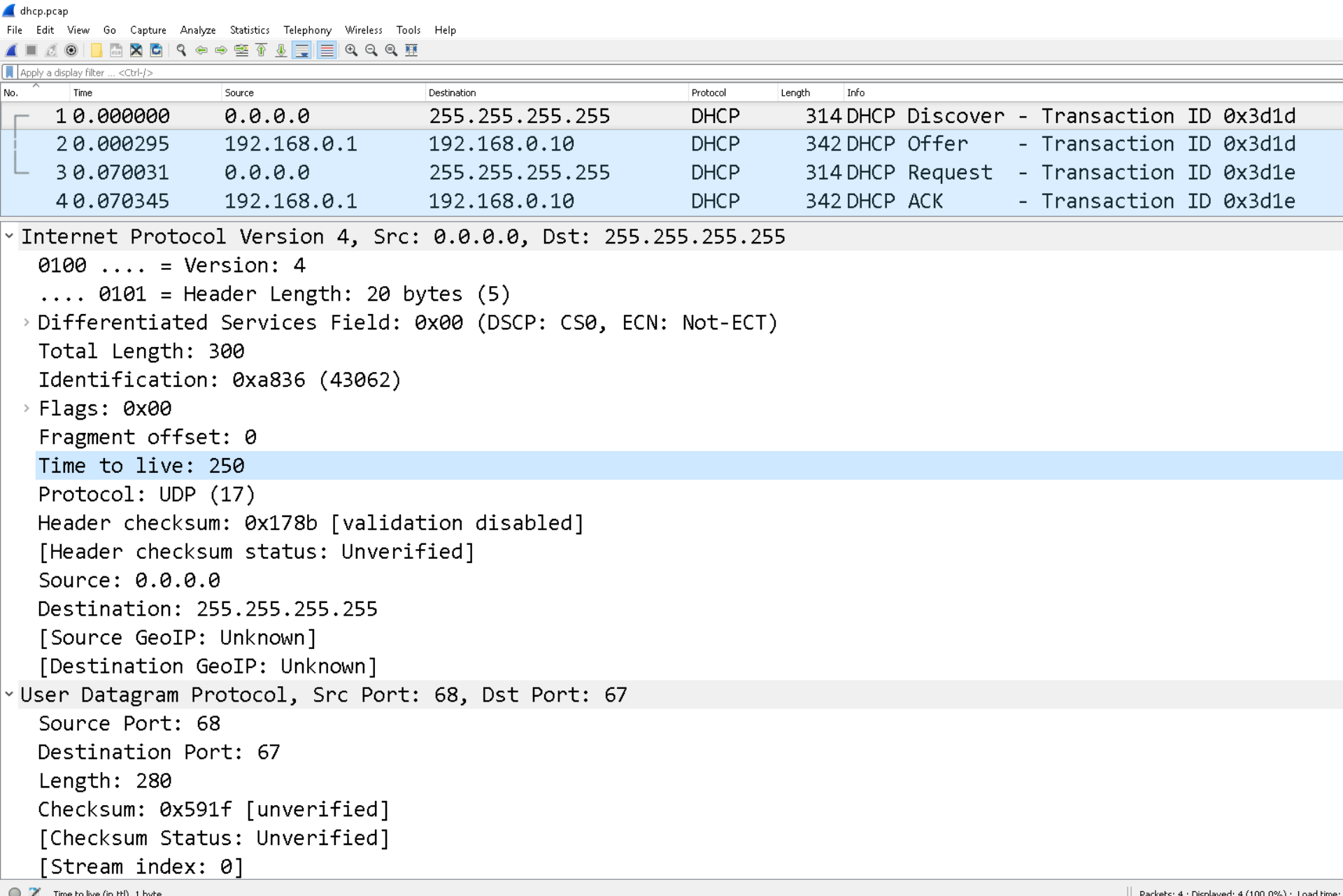

dhcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 314 DHCP Discover - Transaction ID 0x3d1d
2 0.000295 192.168.0.1 192.168.0.10 DHCP 342 DHCP Offer - Transaction ID 0x3d1d
3 0.070031 0.0.0.0 255.255.255.255 DHCP 314 DHCP Request - Transaction ID 0x3d1e
4 0.070345 192.168.0.1 192.168.0.10 DHCP 342 DHCP ACK - Transaction ID 0x3d1e
Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Discover)
Time to live (ip.ttl), 1 byte
Packets: 4 · Displayed: 4 (100.0%) · Load time: 0:0.0

DHCP Discover

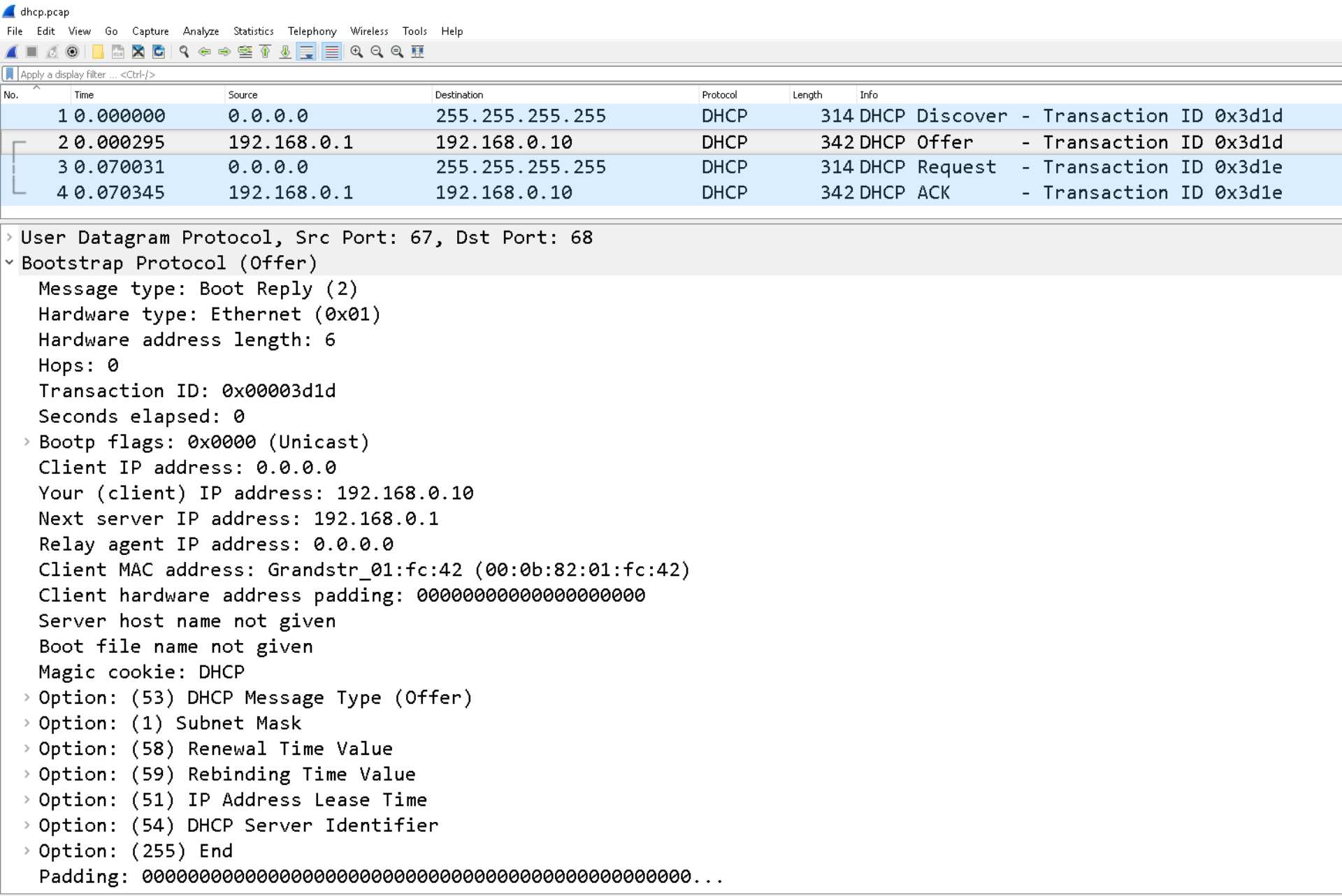
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

```
> Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00003d1d
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 00000000000000
```

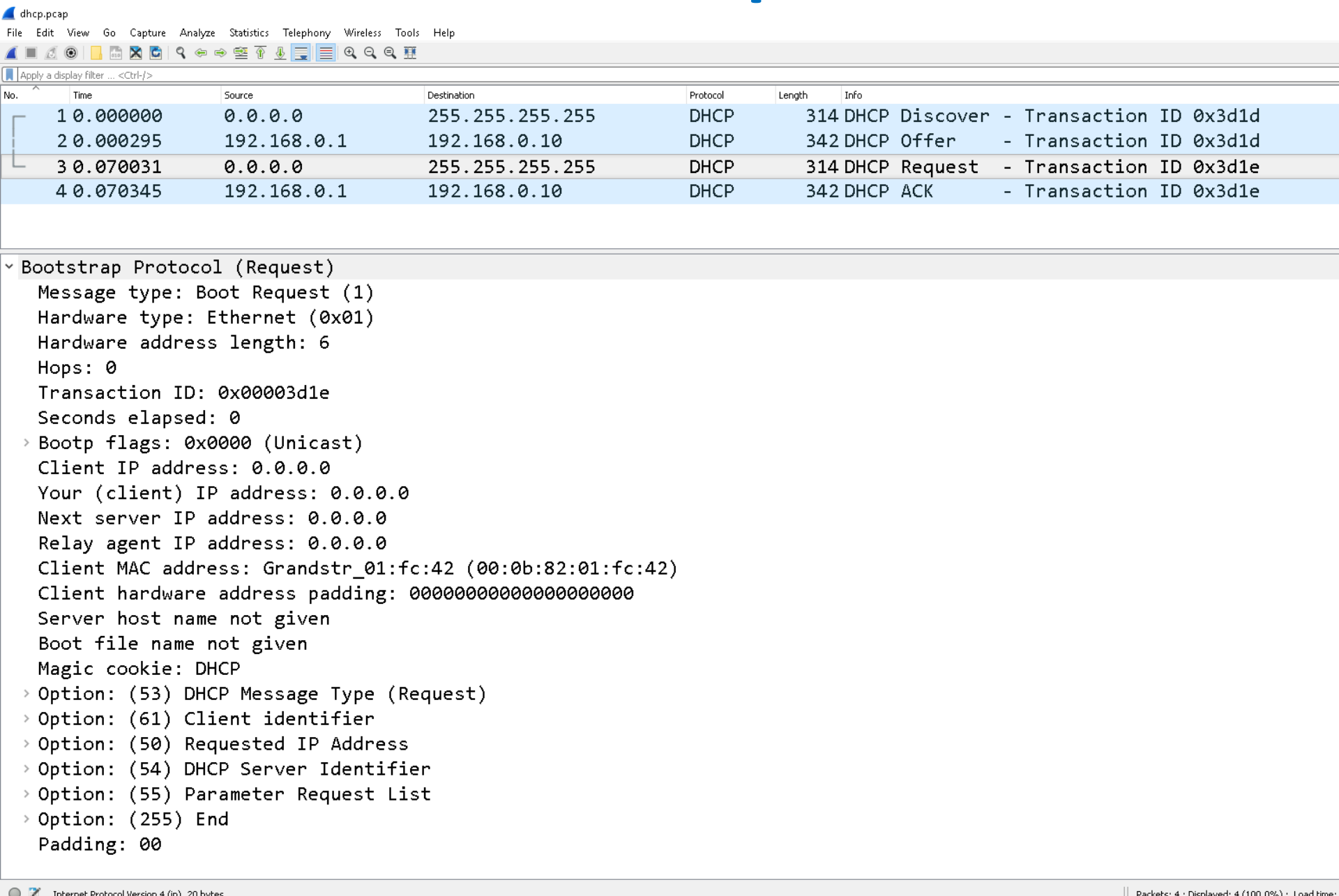
DHCP Discover – IP/UDP



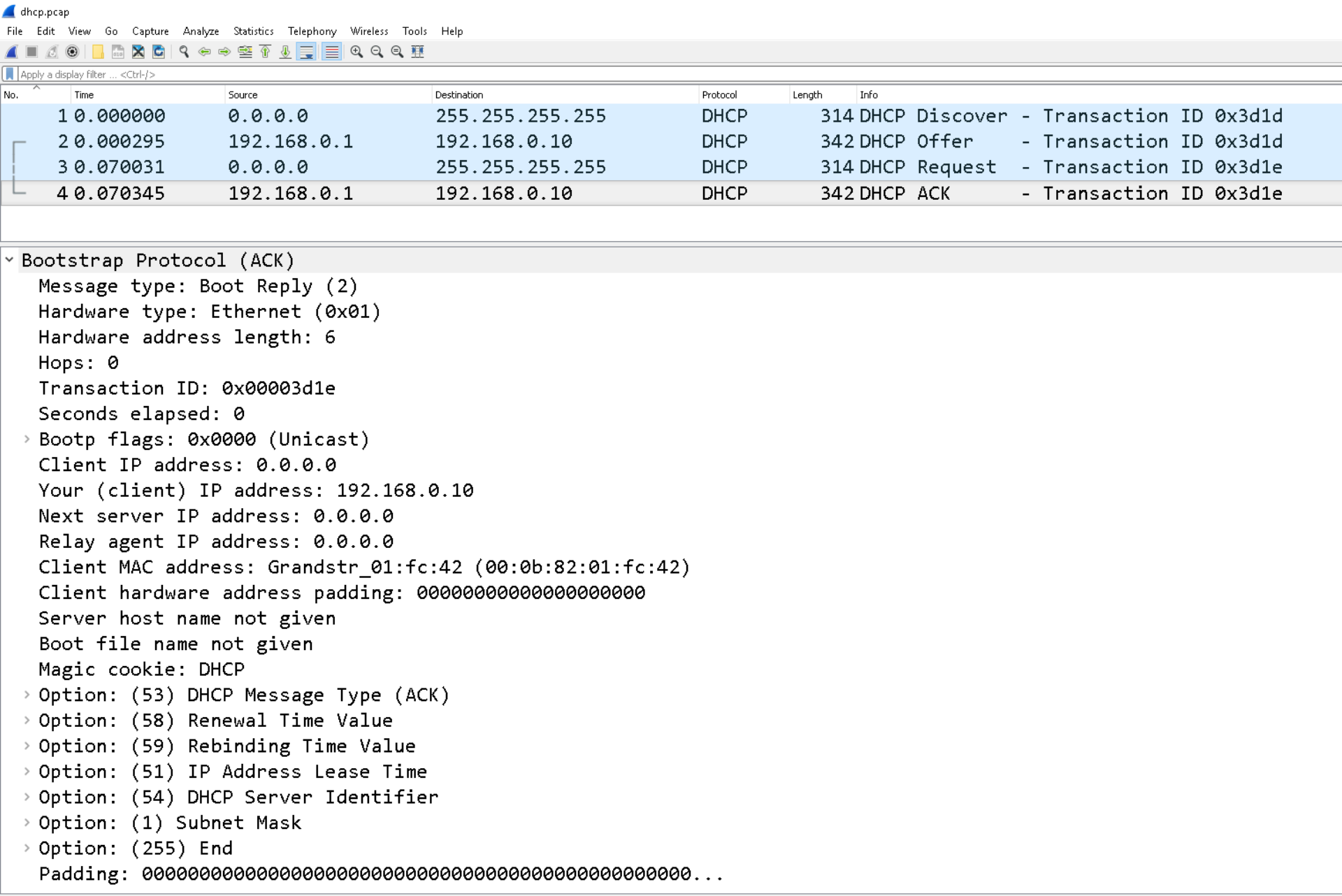
DHCP Offer


dhcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 314 DHCP Discover - Transaction ID 0x3d1d
2 0.000295 192.168.0.1 192.168.0.10 DHCP 342 DHCP Offer - Transaction ID 0x3d1d
3 0.070031 0.0.0.0 255.255.255.255 DHCP 314 DHCP Request - Transaction ID 0x3d1e
4 0.070345 192.168.0.1 192.168.0.10 DHCP 342 DHCP ACK - Transaction ID 0x3d1e
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (Offer)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00003d1d
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.0.10
Next server IP address: 192.168.0.1
Relay agent IP address: 0.0.0.0
Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Offer)
Option: (1) Subnet Mask
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (51) IP Address Lease Time
Option: (54) DHCP Server Identifier
Option: (255) End
Padding: 000000000000000000000000000000000000000000000000...

DHCP Request



DHCP Ack


dhcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 314 DHCP Discover - Transaction ID 0x3d1d
2 0.000295 192.168.0.1 192.168.0.10 DHCP 342 DHCP Offer - Transaction ID 0x3d1d
3 0.070031 0.0.0.0 255.255.255.255 DHCP 314 DHCP Request - Transaction ID 0x3d1e
4 0.070345 192.168.0.1 192.168.0.10 DHCP 342 DHCP ACK - Transaction ID 0x3d1e
Bootstrap Protocol (ACK)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00003d1e
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.0.10
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (51) IP Address Lease Time
Option: (54) DHCP Server Identifier
Option: (1) Subnet Mask
Option: (255) End
Padding: 0000000000000000000000000000000000000000000000...

DNS

captura 1 portátil.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
171	44.703751	192.168.1.63	80.58.61.250	DNS	74	Standard query 0xdf3c A www.google.com
172	44.709958	80.58.61.250	192.168.1.63	DNS	90	Standard query response 0xdf3c A www.google.com A 216.58.214.164
174	44.717829	192.168.1.63	80.58.61.250	DNS	74	Standard query 0xdc91 A www.google.com
175	44.724166	80.58.61.250	192.168.1.63	DNS	90	Standard query response 0xdc91 A www.google.com A 216.58.211.196
178	44.736042	192.168.1.63	80.58.61.250	DNS	74	Standard query 0xdc53 AAAA www.google.com
180	44.741684	80.58.61.250	192.168.1.63	DNS	102	Standard query response 0xdc53 AAAA www.google.com AAAA 2a00:1450:4003:801::2004

```
Frame 171: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
    Interface id: 0 (\Device\NPF_{EF1318FF-F69D-48B1-87F6-F2D3DB77C5B7})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2017 23:09:29.047821000 Hora estándar romance
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1485295769.047821000 seconds
    [Time delta from previous captured frame: 0.508059000 seconds]
    [Time delta from previous displayed frame: 0.508059000 seconds]
    [Time since reference or first frame: 44.703751000 seconds]
    Frame Number: 171
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a), Dst: Mitrasta_3d:35:90 (e0:41:36:3d:35:90)
  > Destination: Mitrasta_3d:35:90 (e0:41:36:3d:35:90)
  > Source: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 80.58.61.250
> User Datagram Protocol, Src Port: 57619, Dst Port: 53
> Domain Name System (query)
```

DNS - ARP

No.	Time	Source	Destination	Protocol	Length	Info
2	0.554532	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
4	0.556282	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
22	8.381676	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
23	8.381696	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
26	10.581077	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
28	10.583178	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
51	20.598894	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
53	20.600845	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
78	30.633732	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
80	30.635448	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
150	40.660490	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
152	40.664348	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
523	47.181598	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
524	47.181617	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
1593	50.691356	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
1594	50.693206	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
12608	60.758095	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
12609	60.760331	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
13504	70.804026	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
13505	70.805997	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
13843	80.825163	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
13846	80.826847	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
14496	86.062337	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
14497	86.062362	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
14498	86.409500	WistronN_f2:c3:21	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.58 (Request)
14499	86.411352	WistronN_f2:c3:21	Broadcast	ARP	60	Who has 192.168.1.58? Tell 0.0.0.0

```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a)
    Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

DNS - ARP Request

No.	Time	Source	Destination	Protocol	Length	Info
2	0.554532	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
4	0.556282	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
22	8.381676	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
23	8.381696	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
26	10.581077	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
28	10.583178	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
51	20.598894	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
53	20.600845	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
78	30.633732	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
80	30.635448	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
150	40.660490	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
152	40.664348	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
523	47.181598	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
524	47.181617	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
1593	50.691356	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
1594	50.693206	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
12608	60.758095	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
12609	60.760331	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
13504	70.804026	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
13505	70.805997	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
13843	80.825163	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
13846	80.826847	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
14496	86.062337	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
14497	86.062362	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
14498	86.409500	WistronN_f2:c3:21	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.58 (Request)
14499	86.411352	WistronN_f2:c3:21	Broadcast	ARP	60	Who has 192.168.1.58? Tell 0.0.0.0

```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a)
    Sender IP address: 192.168.1.63
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

DNS - ARP Reply

No.	Time	Source	Destination	Protocol	Length	Info
2	0.554532	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
4	0.556282	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
22	8.381676	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
23	8.381696	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
26	10.581077	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
28	10.583178	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
51	20.598894	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
53	20.600845	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
78	30.633732	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
80	30.635448	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
150	40.660490	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
152	40.664348	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
523	47.181598	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
524	47.181617	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
1593	50.691356	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
1594	50.693206	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
12608	60.758095	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
12609	60.760331	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
13504	70.804026	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
13505	70.805997	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
13843	80.825163	IntelCor_3a:04:3a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.63
13846	80.826847	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	192.168.1.1 is at e0:41:36:3d:35:90
14496	86.062337	Mitrasta_3d:35:90	IntelCor_3a:04:3a	ARP	42	Who has 192.168.1.63? Tell 192.168.1.1
14497	86.062362	IntelCor_3a:04:3a	Mitrasta_3d:35:90	ARP	42	192.168.1.63 is at 5c:e0:c5:3a:04:3a
14498	86.409500	WistronN_f2:c3:21	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.58 (Request)
14499	86.411352	WistronN_f2:c3:21	Broadcast	ARP	60	Who has 192.168.1.58? Tell 0.0.0.0

```
> Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: Mitrasta_3d:35:90 (e0:41:36:3d:35:90), Dst: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Mitrasta_3d:35:90 (e0:41:36:3d:35:90)
    Sender IP address: 192.168.1.1
    Target MAC address: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a)
    Target IP address: 192.168.1.63
```

DNS Request IP/UDP

No.	Time	Source	Destination	Protocol	Length	Info
171	44.703751	192.168.1.63	80.58.61.250	DNS	74	Standard query 0xdf3c A www.google.com
172	44.709958	80.58.61.250	192.168.1.63	DNS	90	Standard query response 0xdf3c A www.google.com A 216.58.214.164
174	44.717829	192.168.1.63	80.58.61.250	DNS	74	Standard query 0xdc91 A www.google.com
175	44.724166	80.58.61.250	192.168.1.63	DNS	90	Standard query response 0xdc91 A www.google.com A 216.58.211.196
178	44.736042	192.168.1.63	80.58.61.250	DNS	74	Standard query 0xdc53 AAAA www.google.com
180	44.741684	80.58.61.250	192.168.1.63	DNS	102	Standard query response 0xdc53 AAAA www.google.com AAAA 2a00:1450:4003:801::2004

```
> Ethernet II, Src: IntelCor_3a:04:3a (5c:e0:c5:3a:04:3a), Dst: Mitrasta_3d:35:90 (e0:41:36:3d:35:90)
v Internet Protocol Version 4, Src: 192.168.1.63, Dst: 80.58.61.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x04ab (1195)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xe5ea [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.63
    Destination: 80.58.61.250
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v User Datagram Protocol, Src Port: 57619, Dst Port: 53
    Source Port: 57619
    Destination Port: 53
    Length: 40
    Checksum: 0x6055 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
v Domain Name System (query)
    [Response In: 172]
    Transaction ID: 0xdf3c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

Contents

- Unit 1: IP.
- Unit 2: Other supporting protocols and services.
- **Unit 3: Routing algorithms.**
- Unit 4: Security.

Routing algorithms

- *Exterior* vs. *Interior* algorithms.
- Dynamic process of completing Routing Tables.
- Objective: Minimize number of Hops (metrics).
- Routers “talk” with neighbors to learn best routes.
- **RIP: Routing Information Protocol.**

- Exercise 2, dated 3/11/2016.

Routing Information Protocol

- RIP updates every 30”. Down if no update in 180”.
- RIP update: Destination + Metrics.
- Triggered updates when changes occur.
- Infinite metric = 16.
- Count to infinity → Split horizon
  (with Poisoned Reverse).
- RIPv2: Send masks;
  Multicast address 224.0.0.9 (All RIPv2 routers).
- Protocol over UDP.

Routing algorithms – Test question

Control 3/11/2016 – Test. Pregunta 8

En relació a RIP

- ❑ El Count to Infinity permet superar la mètrica 16
- ❑ Si un router està connectat a la mateixa xarxa d'un altre router, a RIP la mètrica entre ells és 0
- ❑ L'Split Horizon permet enviar en els Updates entrades referides al gateway que estigi a la interface per on s'envia el Update
- ❑ Els missatges RIP Updates utilitzen UDP

Open Shortest Path First (OSPF)

- *Link State* protocol:
  - Routers monitor neighbors and send information to all OSPF routers (*Link State Advertisements*, LSA).
- LSA encapsulated into IP datagrams with multicast destination address 224.0.0.5, and routed using *flooding.*
- LSA only sent when changes occur, or when a LSA Request is received.
- Neighbor routers are monitored using a *hello protocol*.
- OSPF routers maintain a LS database. *Shortest Path First algorithm* to build routing table entries.
- Metric computed with link bitrates, delays, etc.

Contents

- Unit 1: IP.
- Unit 2: Other supporting protocols and services.
- Unit 3: Routing algorithms.
- **Unit 4: Security.**

Security - Introduction

- **Threats**
  - External vs. Internal
  - Access: Internal vs. External, Authorized vs. Non
  - Actions: Read, Copy, Modify, Delete, Add, …
  - Data introduction: virus, hoax, … malware
  - Denial of service
  - Communications: Interception, Manipulation, Impersonation (“suplantación”), Repudiation

- **Threats and their protection mechanisms:**
  - *Physical, Technical, Organizational (policies).*

Security - Introduction

- **Protection mechanisms**
  - Preventive, Detective, Corrective
  - External attacks protection (firewalls, …)
  - *Availability*
  - Communication services:
    Confidentiality, Integrity,
    Authentication, No repudiation
  - Basic mechanism: CRYPTOGRAPHY

IP Security

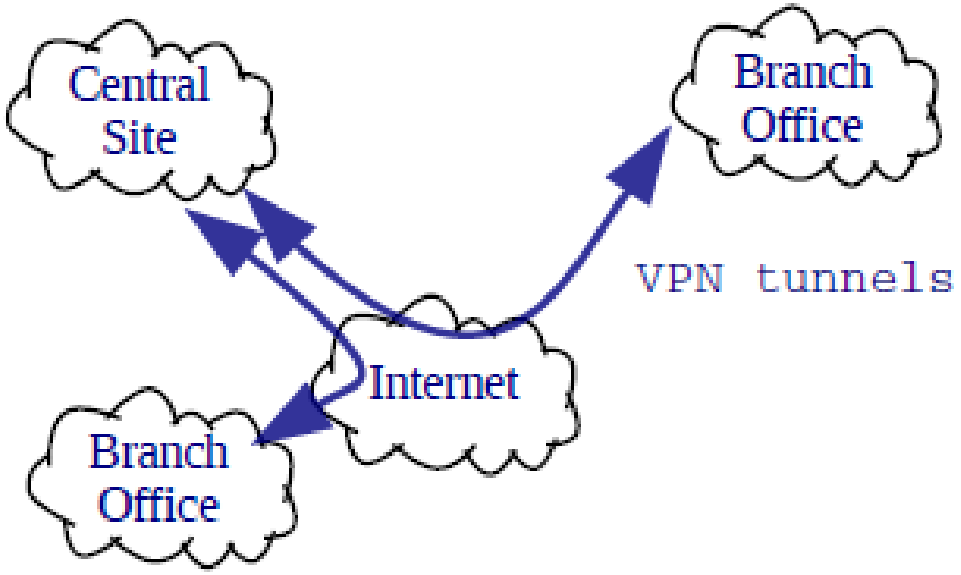
- Handling of Security:
  - Different communications levels.
  - Protocol and information format.
  - User application process.
- Mechanisms at IP level:
  - Firewalls
  - VPN (Virtual Private Networks)

IP Security - Firewalls

- **Firewalls**
  - Implement network access control → ***ACL (Access Control Lists)***
  - Software or Hardware. In Routers.
  - "Filtering" on:
    - IP header information.
    - Transport, Application information.

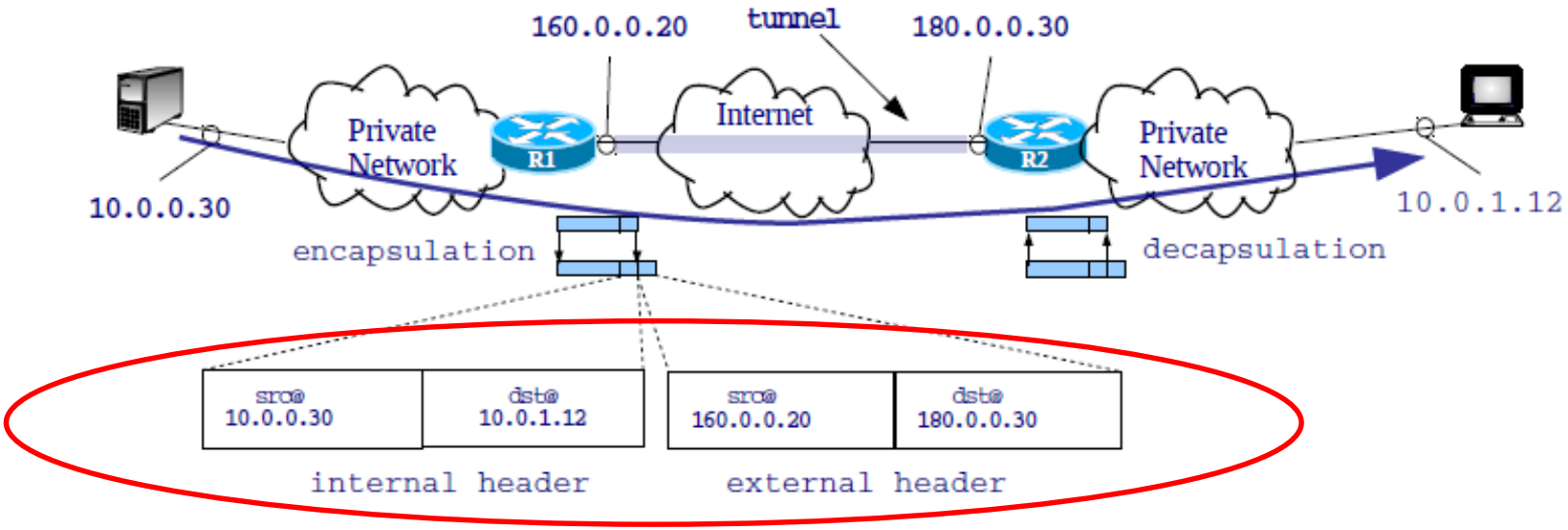
IP Security - VPN

- **VPN (Virtual Private Networks)**
  - Through the open Internet

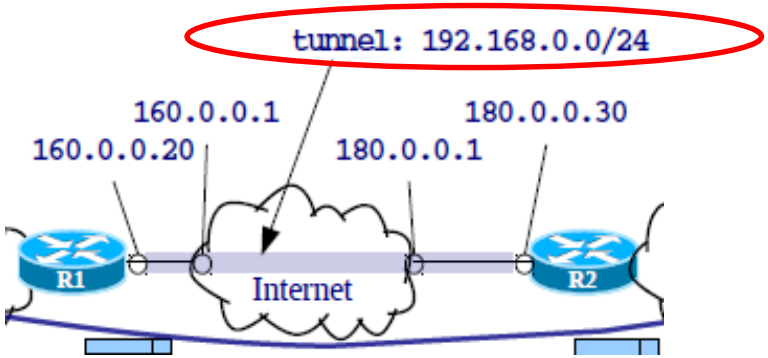


  - Implemented with *Tunneling*

IP Security - VPN

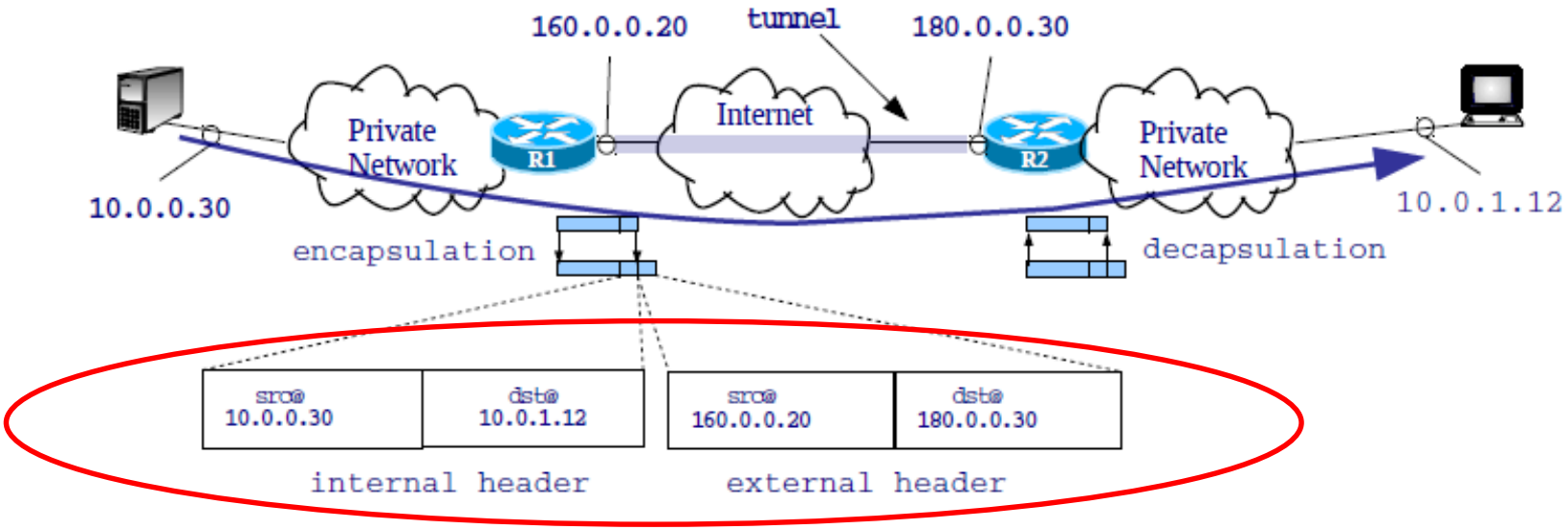


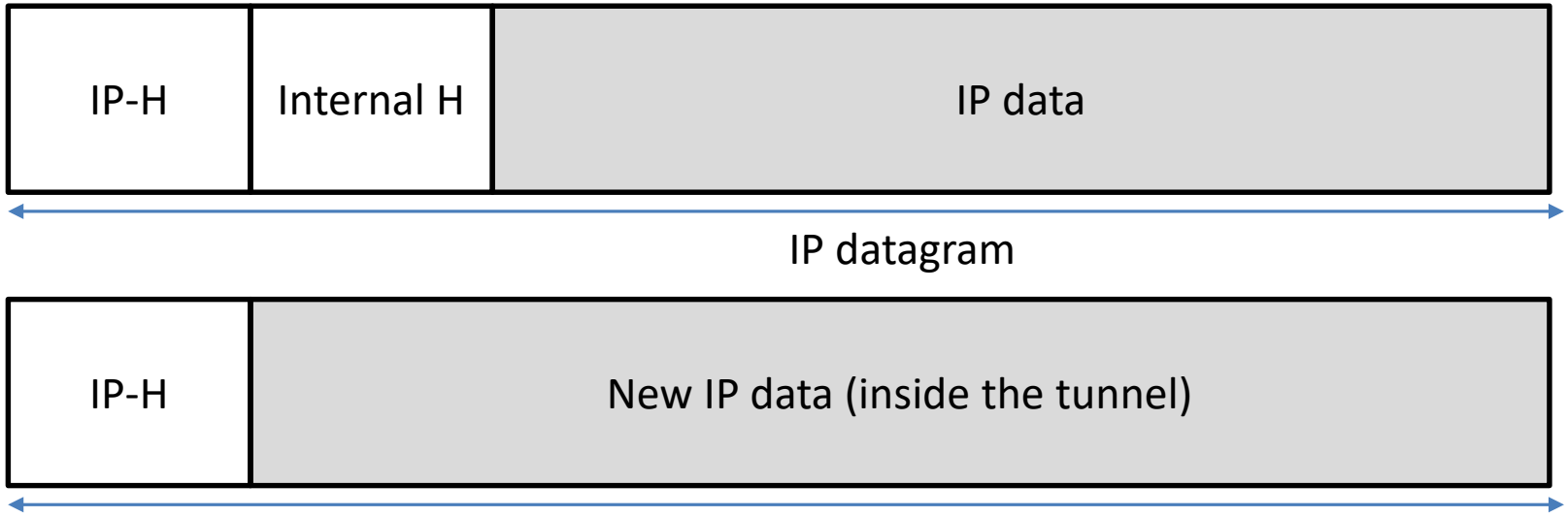
- **Tunnelling**
  - **IP over IP**.
  - IPSec.
  - …



Tunnel as a private address subnetwork

IP Security - VPN





IP Security

- Exercise 1, question “f”, dated 20/1/2017.
  - Firewalls (ACL)
- Exercise 1, question “f”, dated 3/11/2016.
  - Firewalls (ACL)
- Exercise 1, question “h”, dated 3/11/2016.
  - VPN (tunnels)