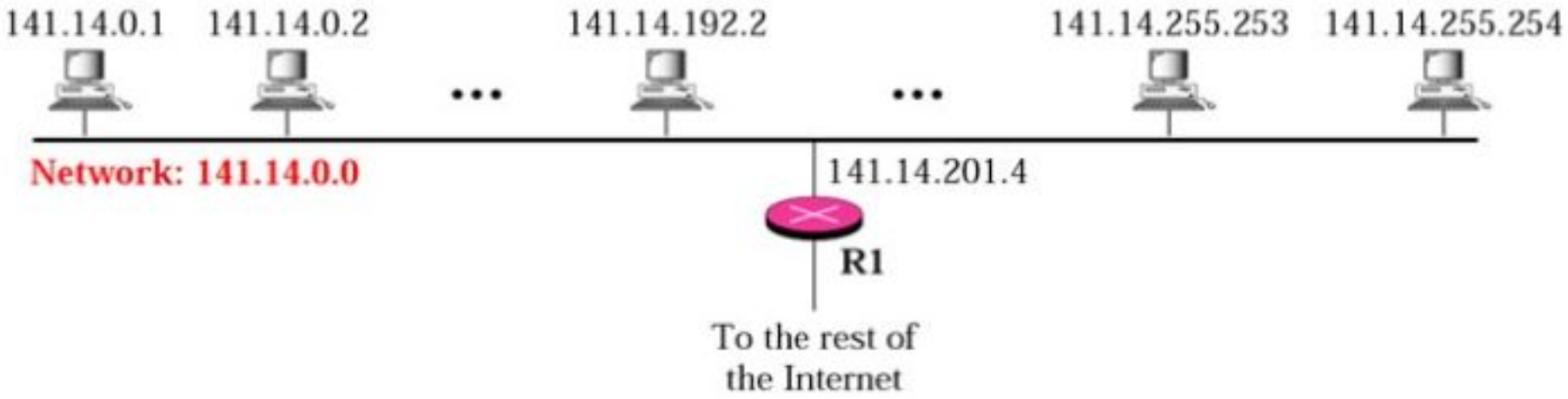
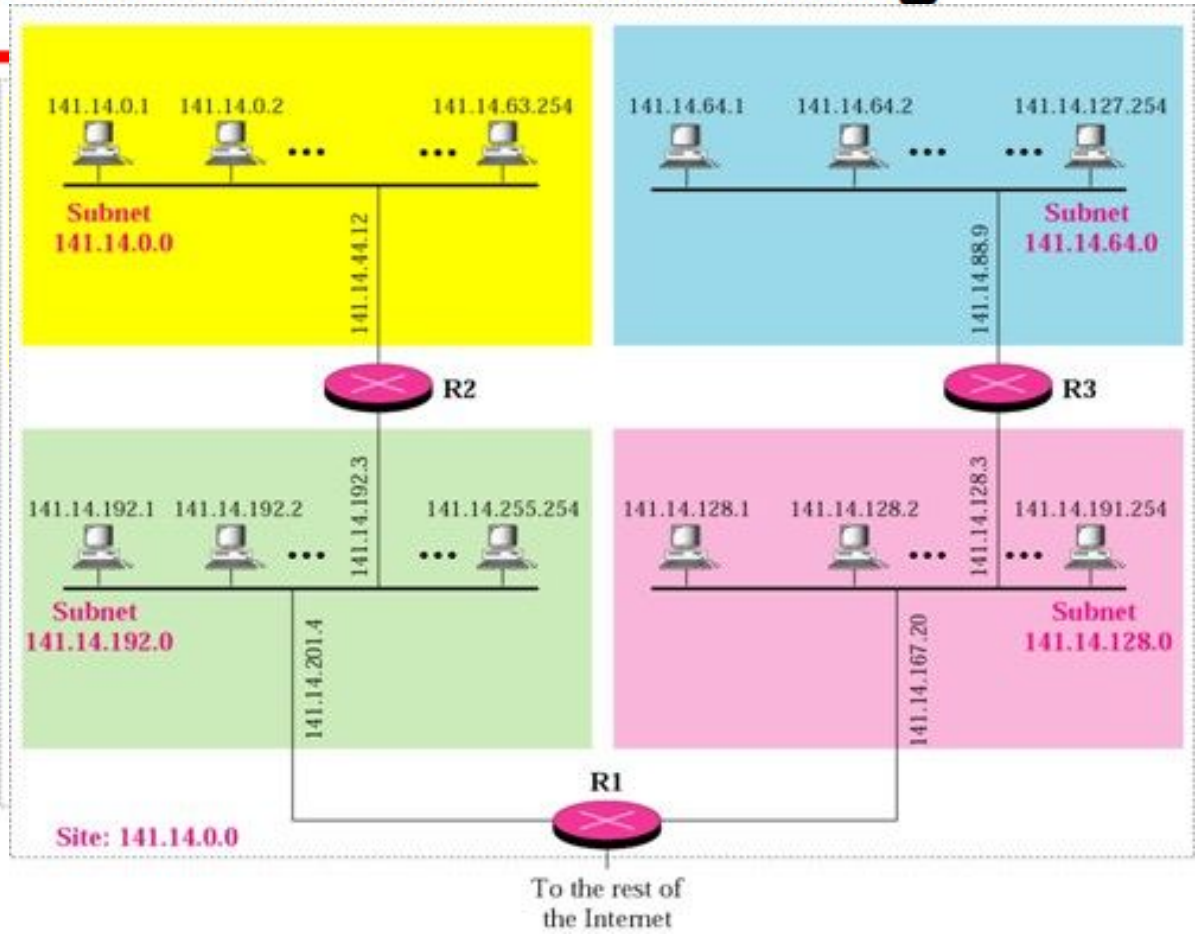
Subnetting

In subnetting, a network is divided into several smaller sub-networks with each subnet having its own subnet address.

A Network Without Subnetting



A Network With Subnetting



Example

As an example, suppose an organization is given the block 17.12.40.0/26, which contains 64 addresses. The organization has three offices and needs to divide the addresses into three sub blocks of 32, 16, and 16 addresses. We can find the new masks by using the following arguments:

First address:17.12.40.0/26

Last address: 17.12.40.63/26

First subnet 32 addresses

Second subnet 16 addresses

Third subnet 16 addresses

Range??

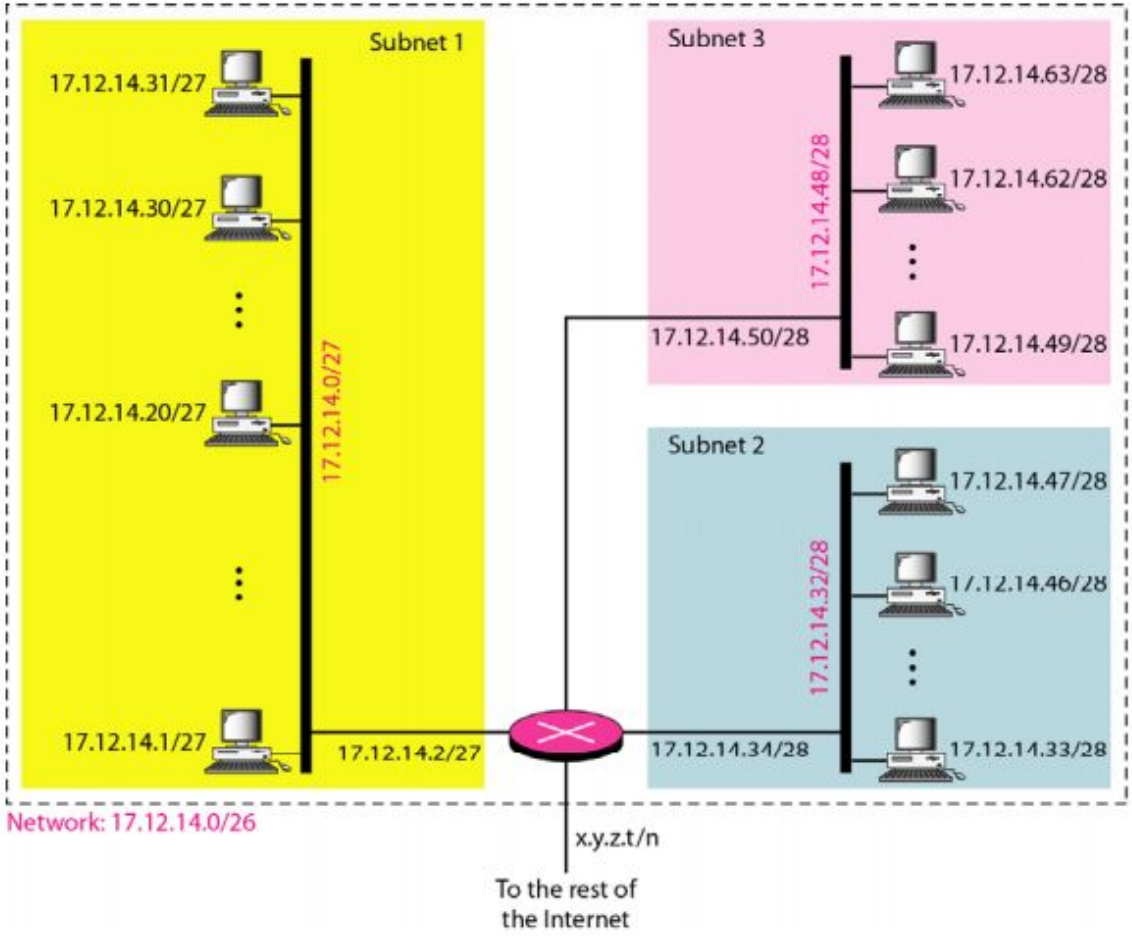
Subnet mask?

Subnet mask.

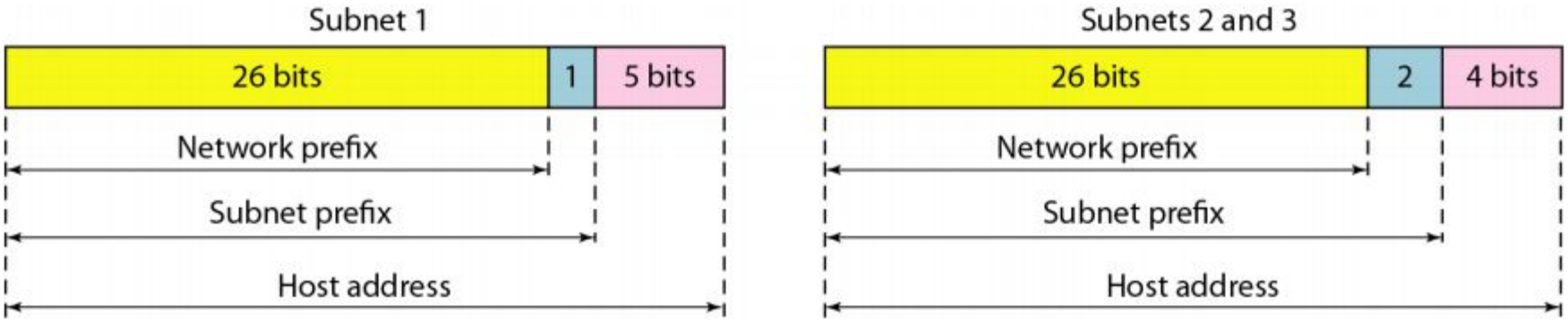
Suppose the mask for the first subnet is n1, then 2^(32- n1) must be 32, which means that n1 =27.

Suppose the mask for the second subnet is n2, then 2^(32- n2) must be 16, which means that n2 = 28.

Suppose the mask for the third subnet is n3, then 2^(32- n3) must be 16, which means that n3 =28


Subnet 1
17.12.14.31/27
17.12.14.30/27
17.12.14.20/27
17.12.14.1/27
17.12.14.0/27
17.12.14.2/27
Subnet 3
17.12.14.63/28
17.12.14.62/28
17.12.14.49/28
17.12.14.48/28
17.12.14.50/28
Subnet 2
17.12.14.47/28
17.12.14.46/28
17.12.14.33/28
17.12.14.32/28
17.12.14.34/28
Network: 17.12.14.0/26
x.y.z.t/n
To the rest of
the Internet

Three-level hierarchy in an IPv4 address



While subnetting things to keep in mind..

Restriction To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.

2. The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ...).

3. The first address must be evenly divisible by the number of addresses.

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a. *The first group has 64 customers; each needs 256 addresses.*
b. *The second group has 128 customers; each needs 128 addresses.*
c. *The third group has 128 customers; each needs 64 addresses.*

Design the subblocks and find out how many addresses are still available after these allocations.

Network address translation

Table 19.3 ***Addresses for private networks***

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

Figure 19.10 *A NAT implementation*

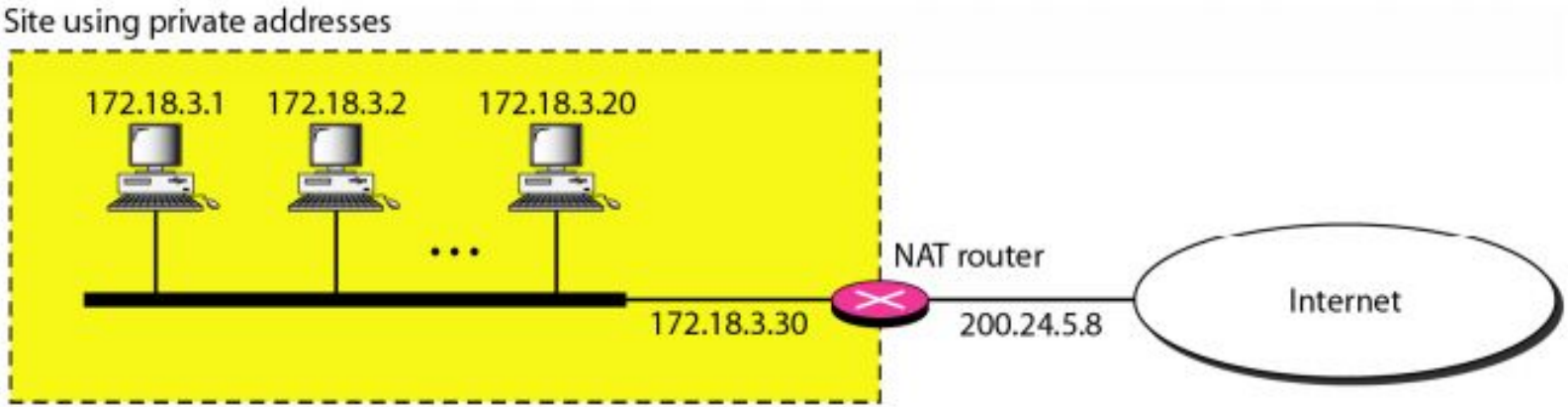


Figure 19.11 *Addresses in a NAT*

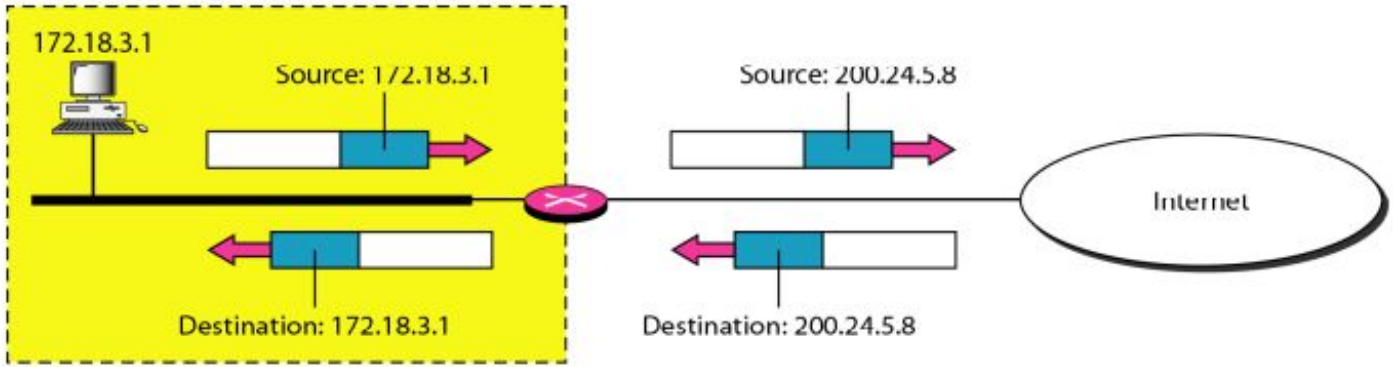
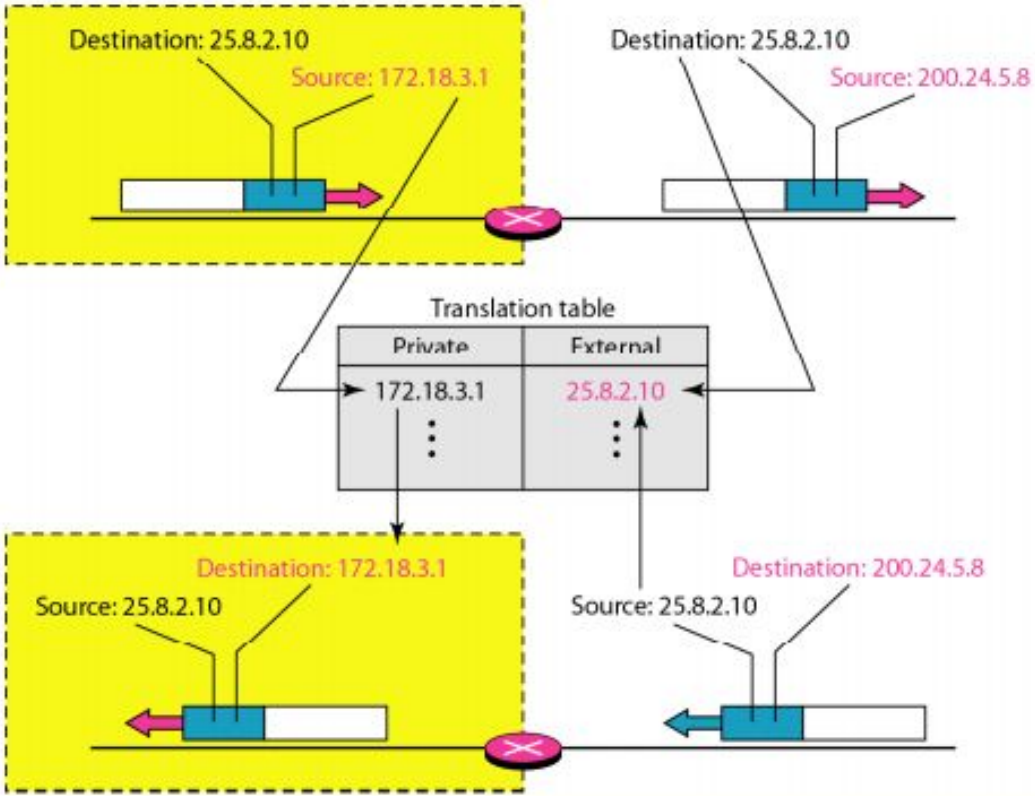
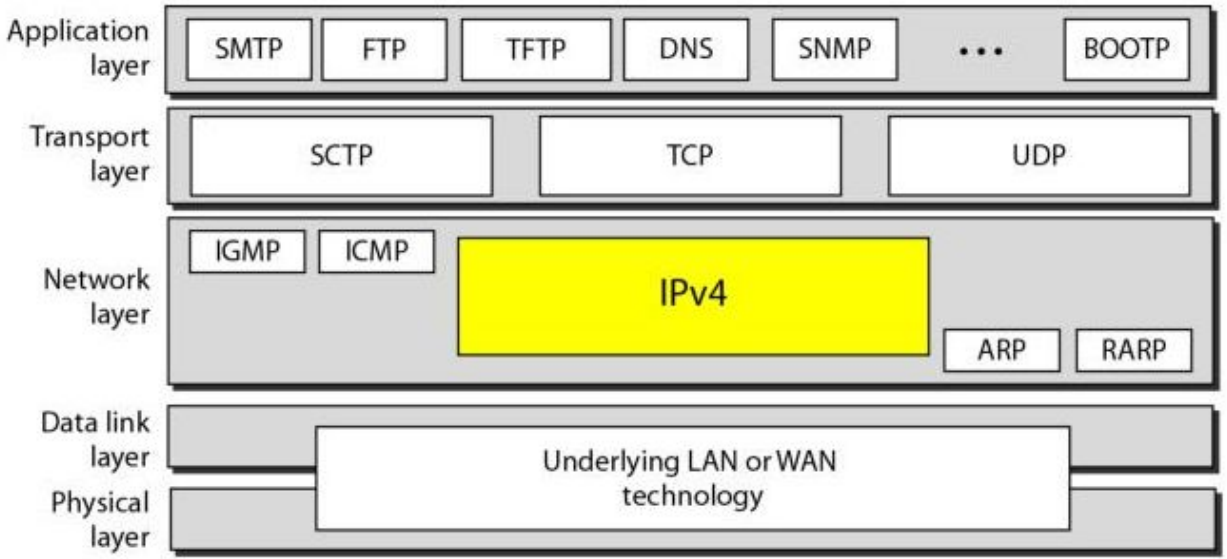


Figure 19.12 *NAT address translation*

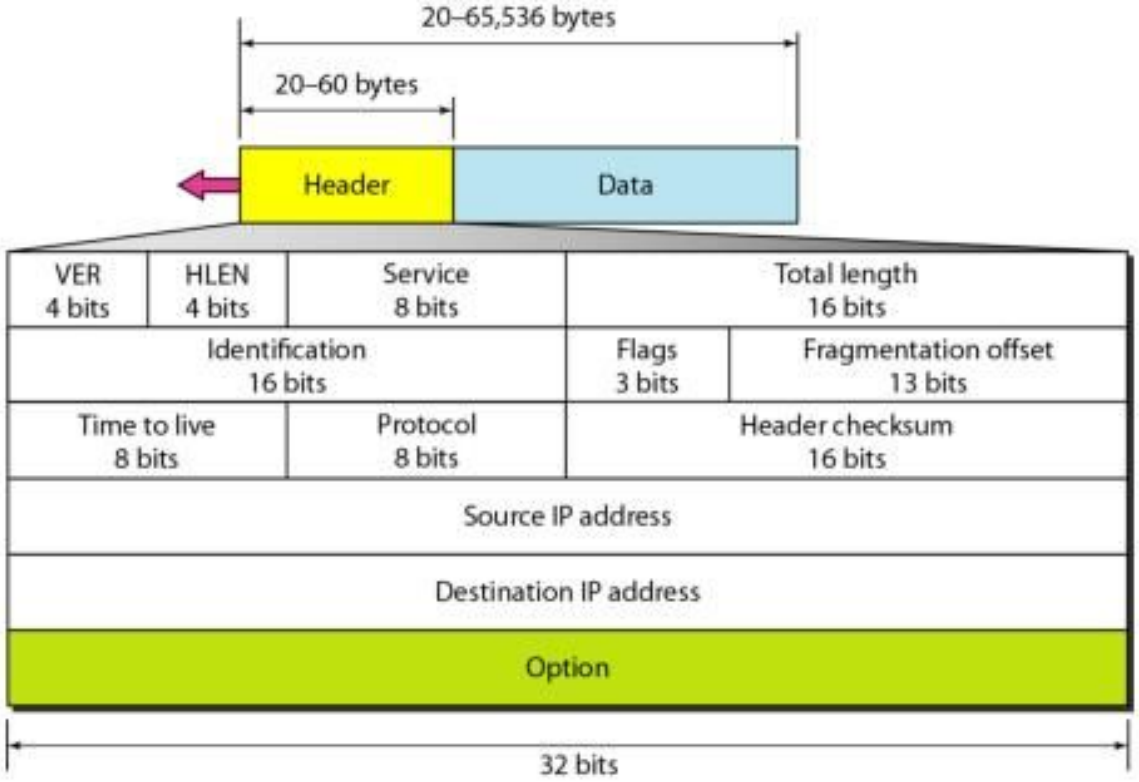


Internet Protocol (IP)

- Switching at the network layer in the Internet uses the ***datagram approach***
- Communication at the network layer in the Internet is ***connectionless***
- Position of IPv4 in TCP/IP protocol suite

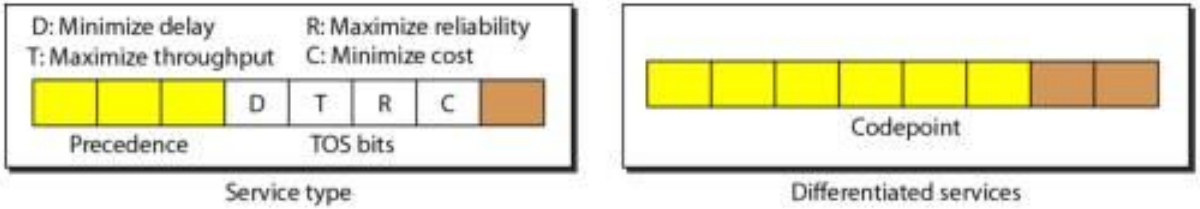


IPv4 Datagram



IPv4 Header

- Version: IPv6, IPv4
- Service type or differentiated services



  - Precedence: never used
  - TOS

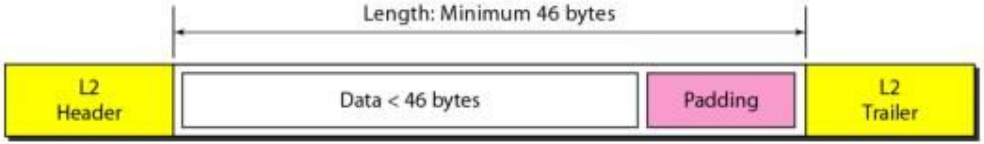
TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Default TOS for Applications

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

IPv4 Header

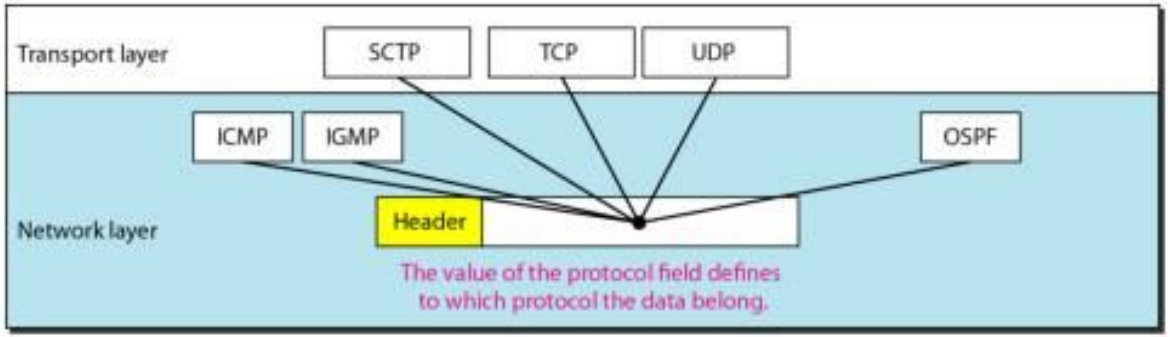
- Total length: Length of data = total length – header length
  - Maximum 65535 ($2^{16} - 1$) bytes
  - Encapsulation of a small datagram in an Ethernet frame



- Identification: used in fragmentation
- Flag : used in fragmentation
- Fragmentation offset
- Time to live
- Checksum
- Source and destination address

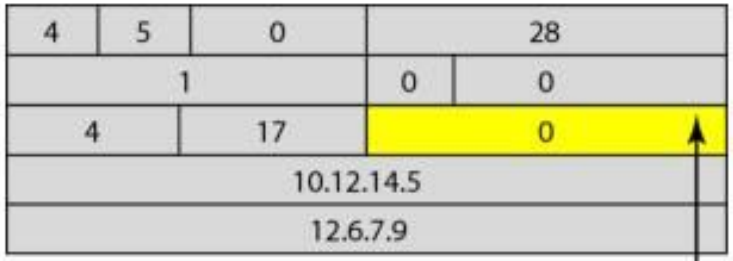
IPv4 Header

- Protocol field for higher-level protocol



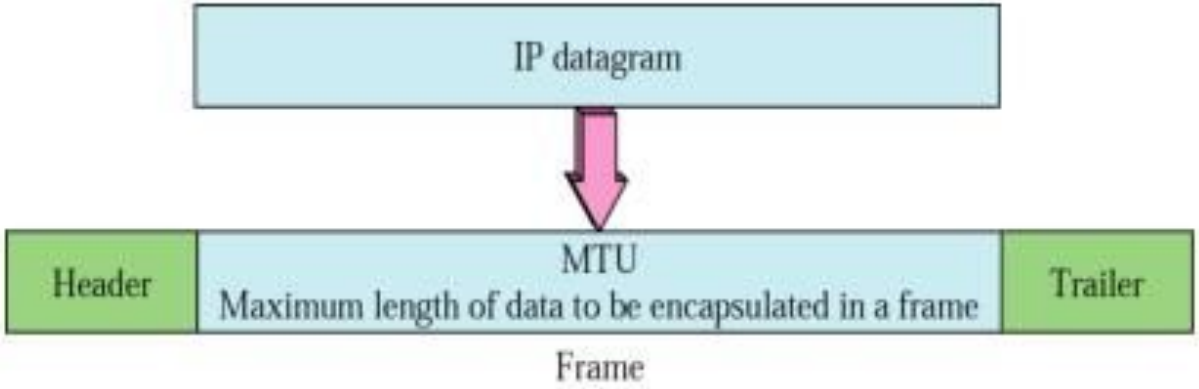
Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Checksum



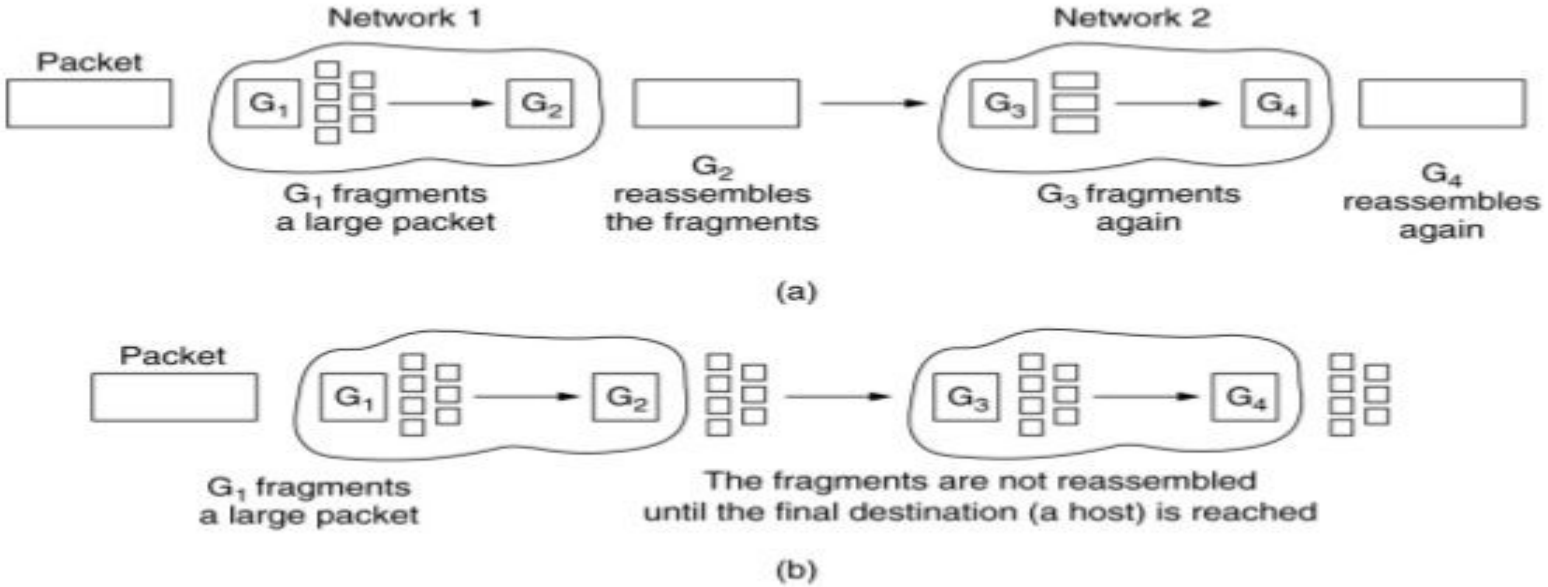
4, 5, and 0 →	4	5	0	0
28 →	0	0	1	C
1 →	0	0	0	1
0 and 0 →	0	0	0	0
4 and 17 →	0	4	1	1
0 →	0	0	0	0
10.12 →	0	A	0	C
14.5 →	0	E	0	5
12.6 →	0	C	0	6
7.9 →	0	7	0	9
Sum →	7	4	4	E
Checksum →	8	B	B	1

- Maximum length of the IPv4 datagram: 65,535 bytes



Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

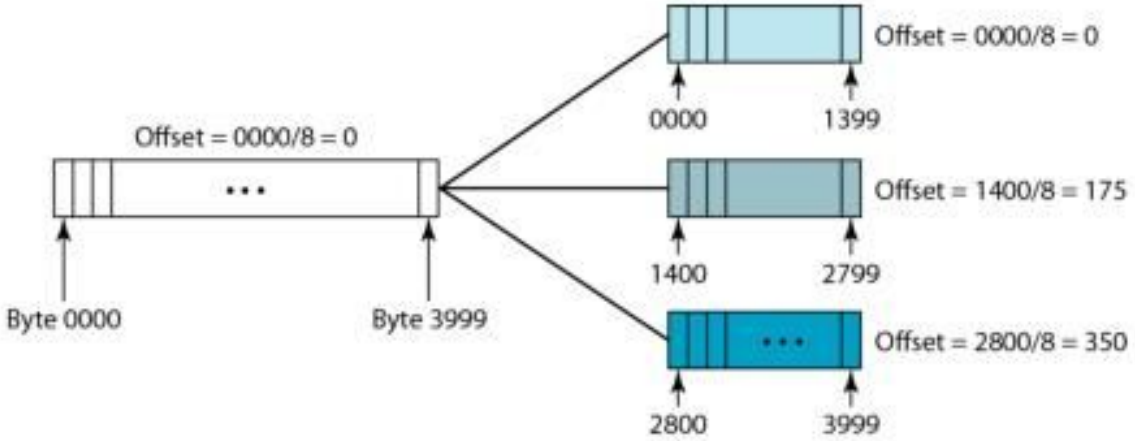
Transparent and non transparent fragmentation



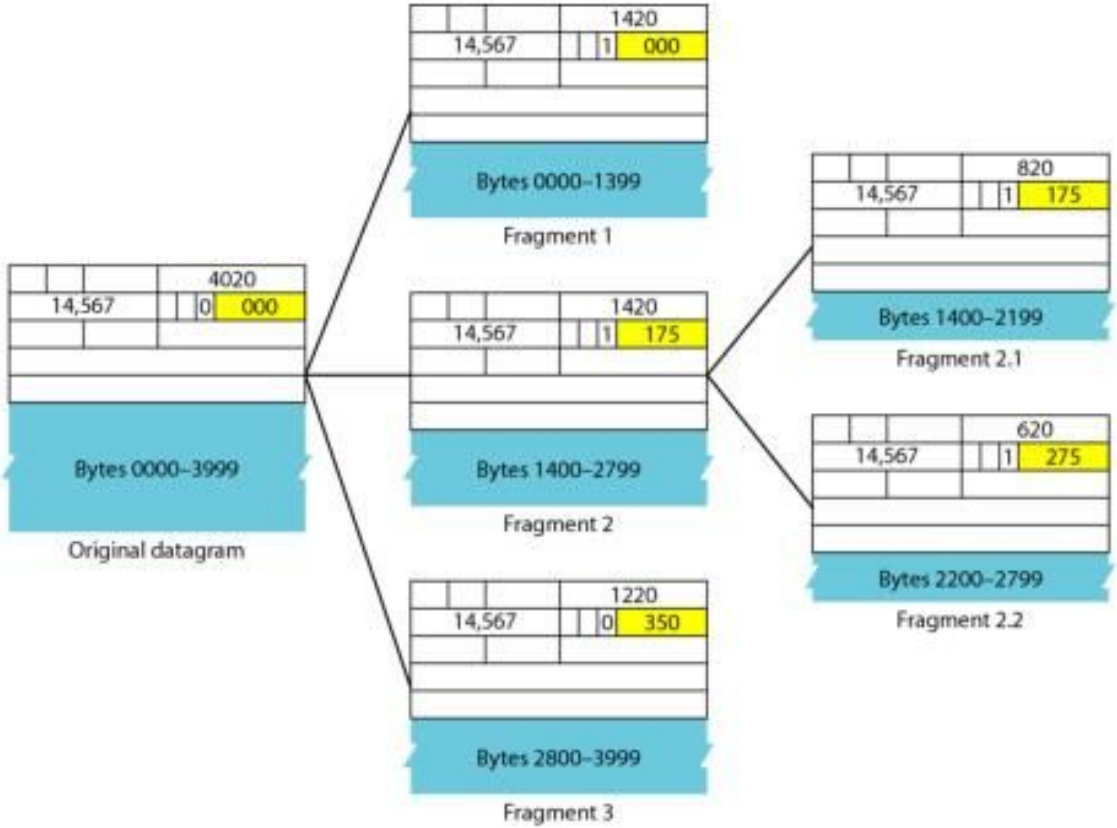
(a) Transparent fragmentation. (b) Nontransparent fragmentation.

Field related to fragmentation

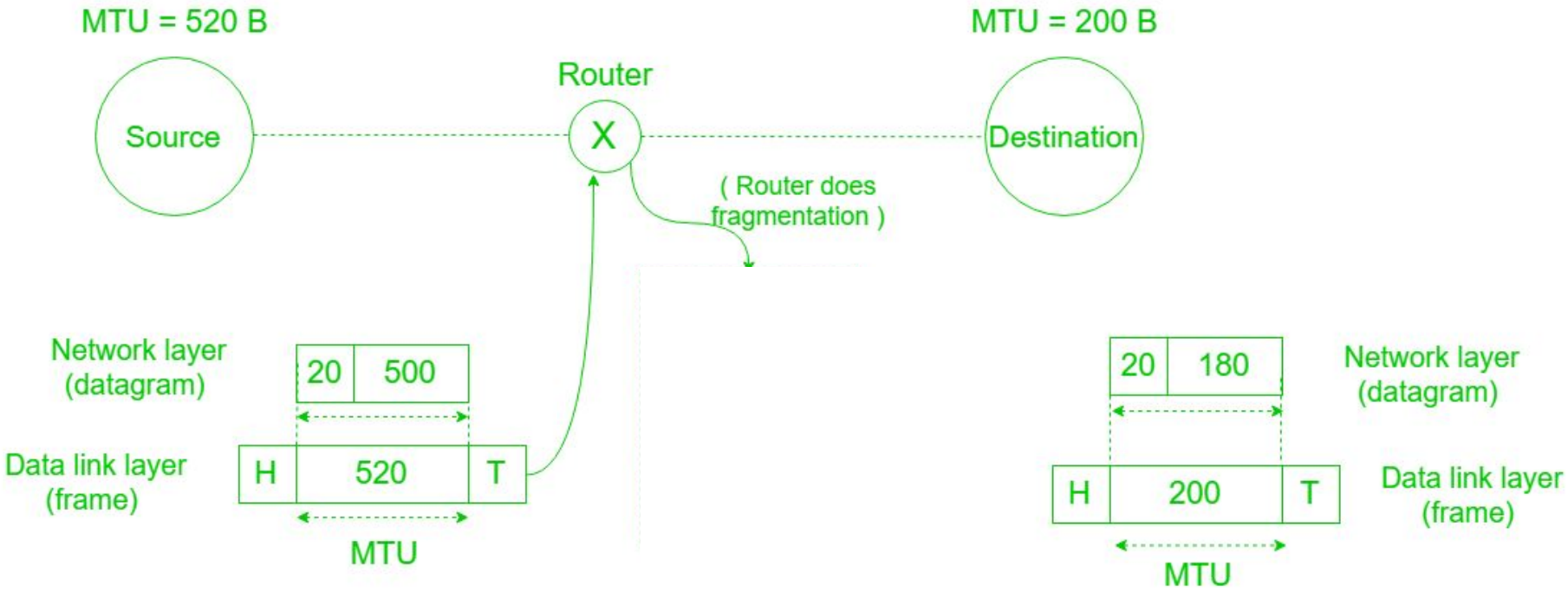
- Identification: identifies a datagram originating form the source host
- Flags: the first bit (reserved), the second bit (do not fragment bit), the third bit (more fragment bit, 0 means this is the last or only fragment)
- Fragmentation offset: (13 bits cannot represent a sequence of bytes greater than 8191



Detailed Fragmentation Example



Fragmentation



	20 | 176	20 | 176	20 | 148
Fragment Offset	0	22	44
MF	1	1	0
Header length	5	5	5
Total length	196	196	168

Options

- IPv4 header is made of two part: a fixed part and a variable part
- Fixed part: 20 bytes long
- Variable part comprises the options that can be a maximum of 40 bytes

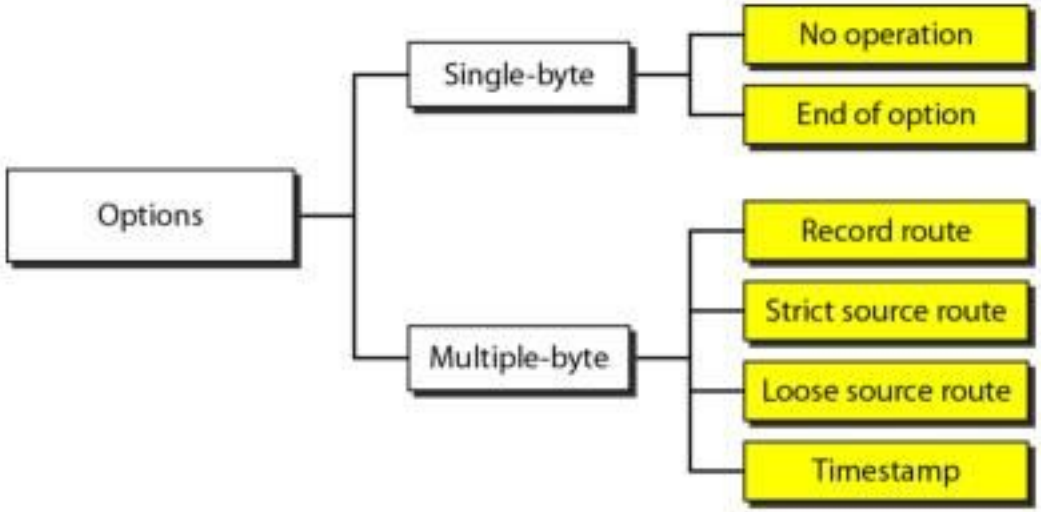
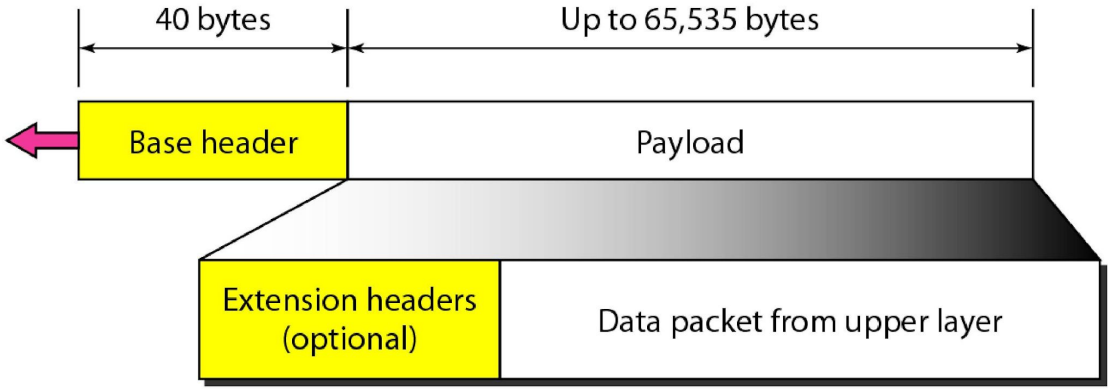


Figure 20.15 *IPv6 datagram header and payload*



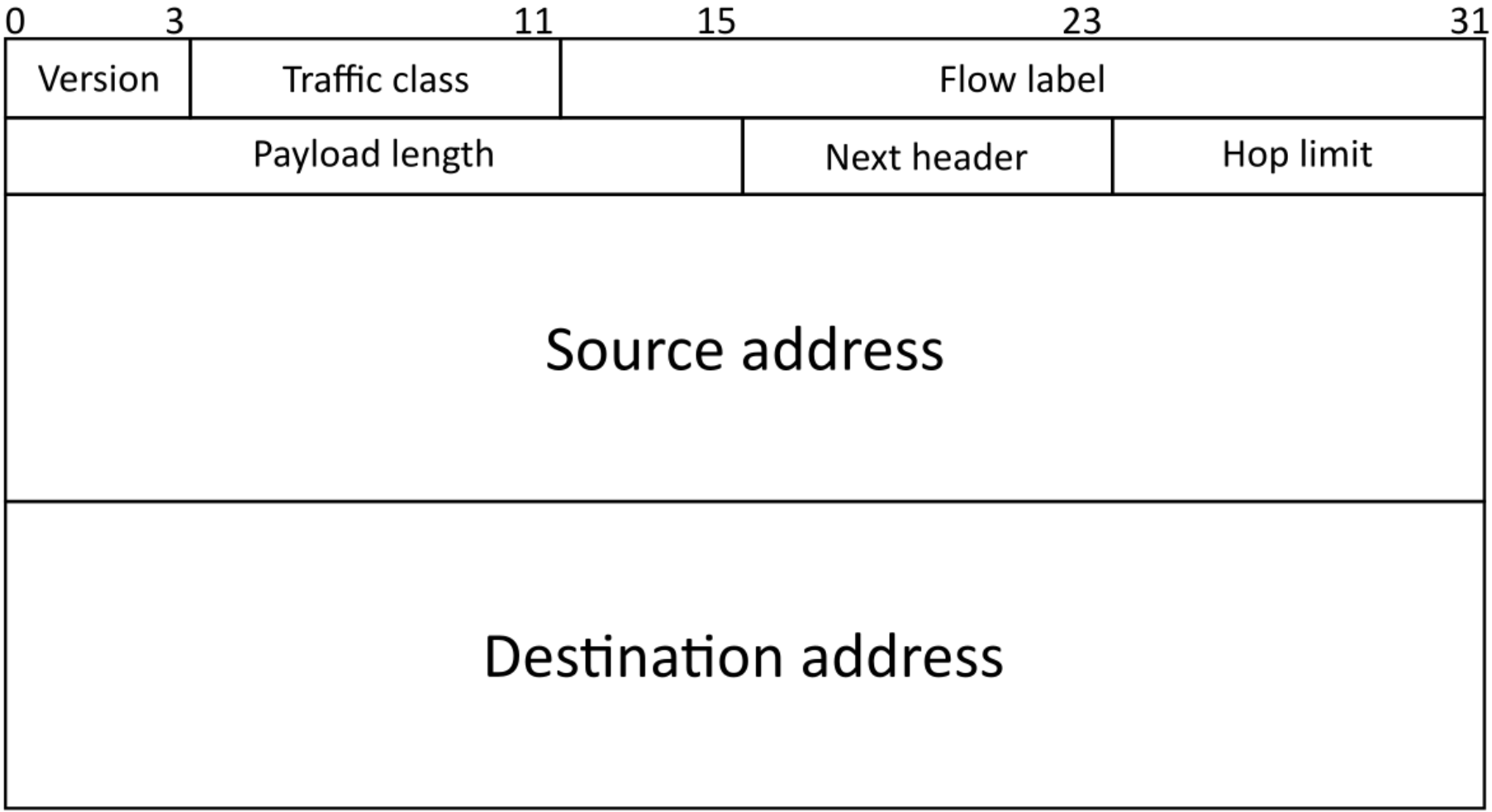

0
3
11
15
23
31
Version
Traffic class
Flow label
Payload length
Next header
Hop limit
Source address
Destination address

Table 20.6 *Next header codes for IPv6*

Code	*Next Header*
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

Table 20.9 *Comparison between IPv4 and IPv6 packet headers*

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Figure 20.17 *Extension header types*

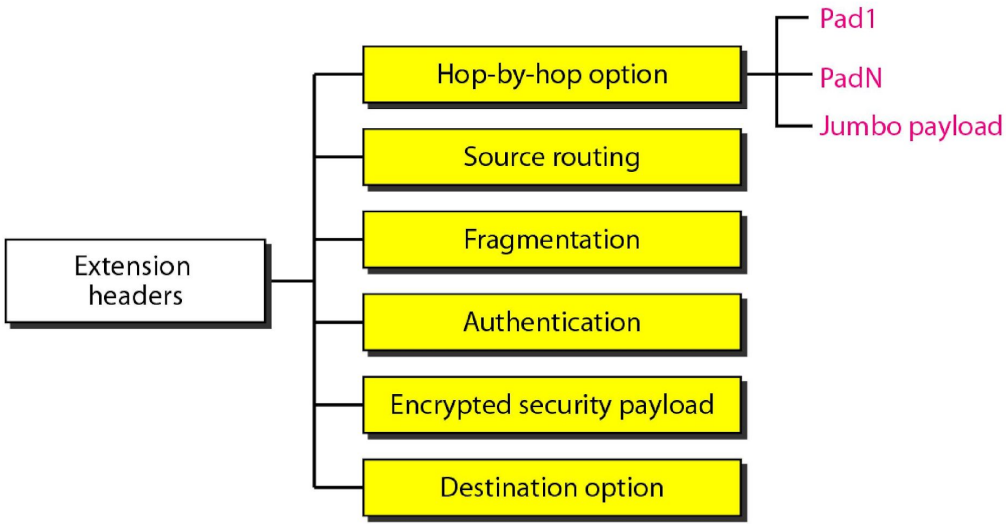


Table 20.10 *Comparison between IPv4 options and IPv6 extension headers*

Comparison
1. The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
2. The record route option is not implemented in IPv6 because it was not used.
3. The timestamp option is not implemented because it was not used.
4. The source route option is called the source route extension header in IPv6.
5. The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
6. The authentication extension header is new in IPv6.
7. The encrypted security payload extension header is new in IPv6.