Next Generation: IPv6

Introduction

- IPv4 has some deficiencies that make it unsuitable for the fast-growing Internet, including the following:
  - Addressing method has depleted the address space of IPv4, and soon there will not be any addresses left to assign to any new system that wants to be connected to the Internet.
  - The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.
  - The Internet must accommodate encryption and authentication of data for some applications.

Introduction (cont’d)

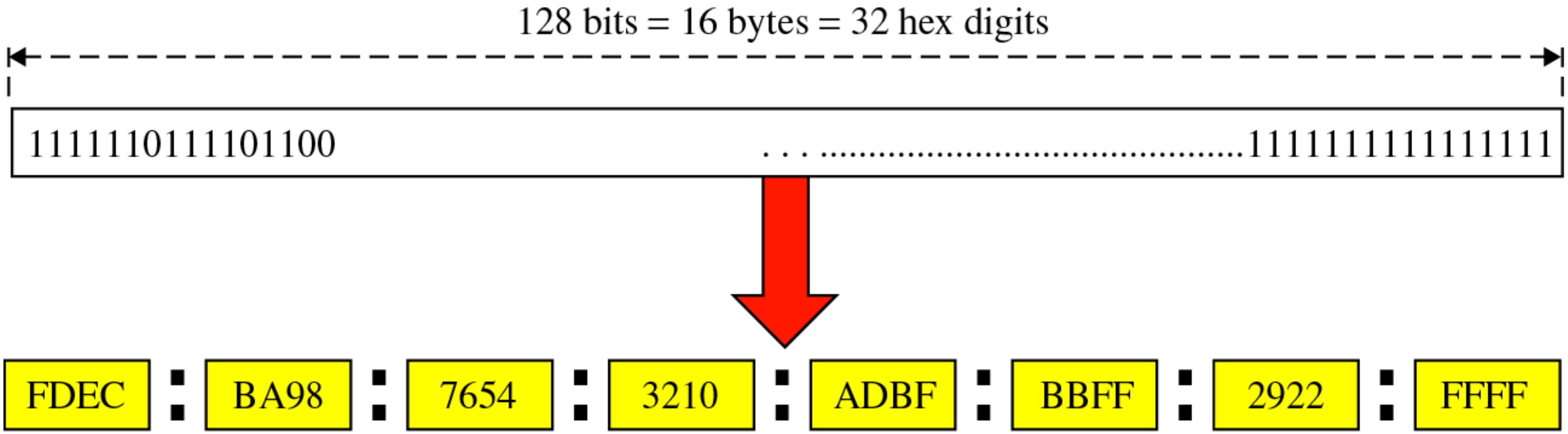
- IPv6 (Internet Protocol, version 6) is also known as IPng (next generation).
- Related protocols, such as ICMP, were also changed.
- Other protocols in the network layer, such as ARP , RARP, and IGMP, were either deleted or included in the ICMP protocol.
- Routing protocols, such as RIP and OSPF, were also slightly modified to accommodate these changes.

IPv6

- Some advantages over IPv4
  - Lager address space
  - Better header format : IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data
    - This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
  - New options : IPv6 has new options to allow additional functionalities
  - Allowance for extensions : allowing the extension of the protocol if required
  - Support for resource allocation : used for real-time audio and video
  - Support for more security

IPv6 Addresses

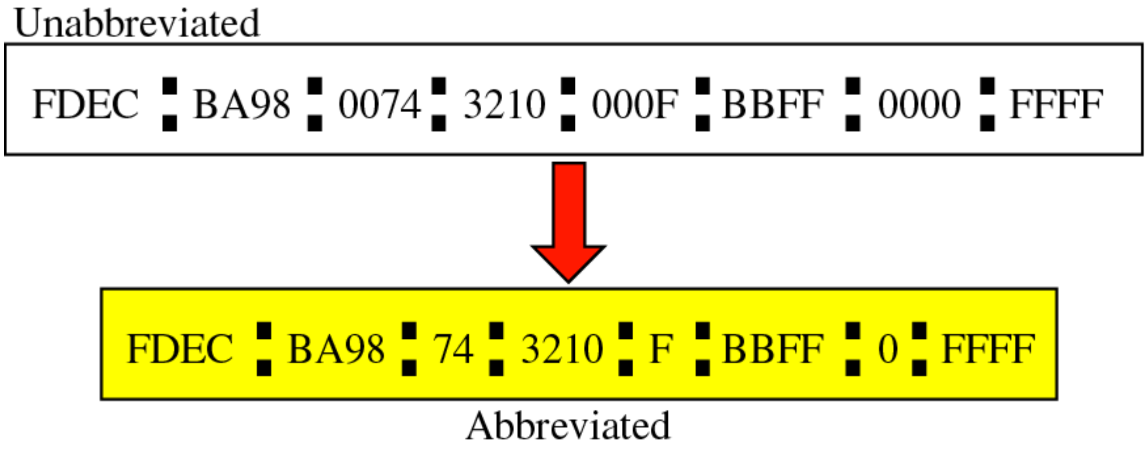
- 16 bytes (octets)


128 bits = 16 bytes = 32 hex digits
1111110111101100 1111111111111111
FDEC : BA98 : 7654 : 3210 : ADBF : BBFF : 2922 : FFFF

- Hexadecimal Colon Notation
  - To make address more readable
  - 128 bits are divided into eight sections, each two bytes in length (4 hexadecimal digits)
  - Therefore, the address consists of 32 hexadecimal digits

IPv6 Addresses

- □ **Abbreviation**



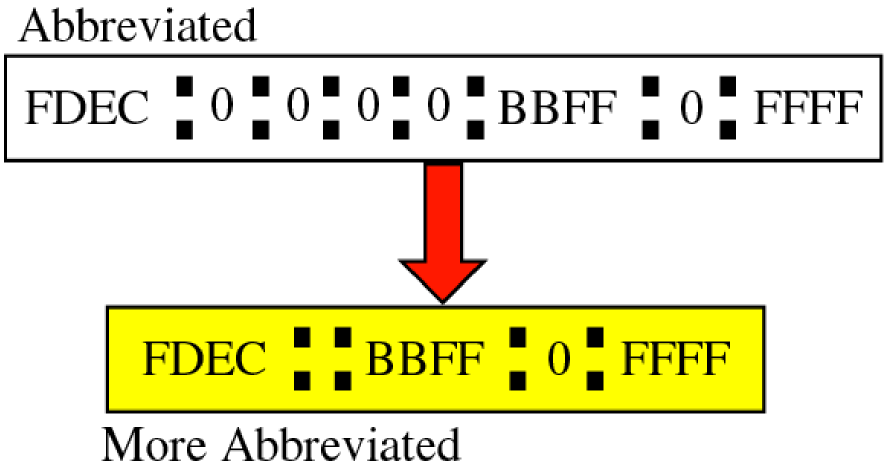
Unabbreviated

FDEC : BA98 : 0074 : 3210 : 000F : BBFF : 0000 : FFFF

FDEC : BA98 : 74 : 3210 : F : BBFF : 0 : FFFF

Abbreviated

- □ **Abbreviated address with consecutive zeros**



Abbreviated

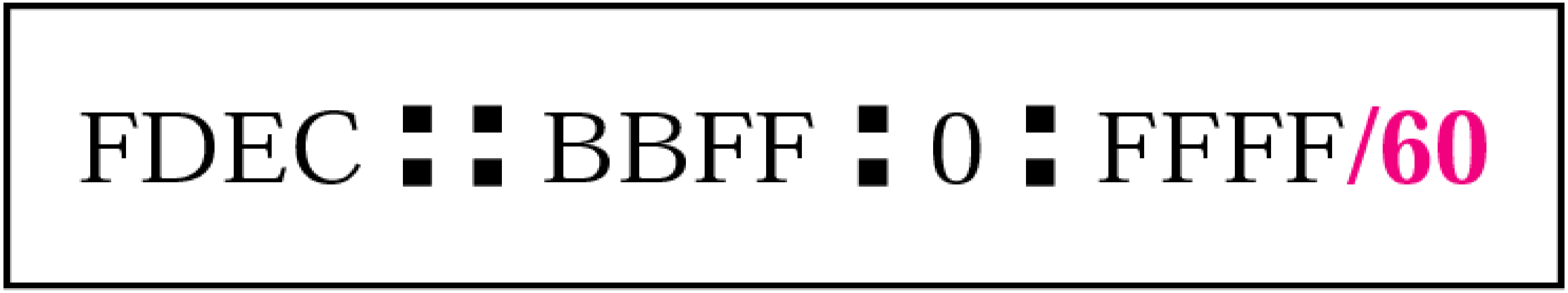
FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF

FDEC : : BBFF : 0 : FFFF

More Abbreviated

IPv6 Addresses (cont'd)

- CIDR (Classless Inter-Domain Routing) Address



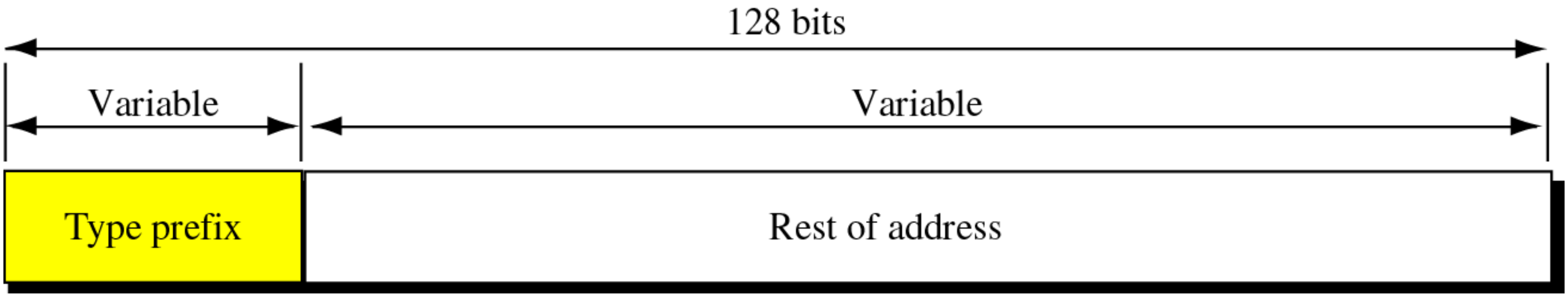
FDEC::BBFF:0:FFFF/60

IPv6 Addresses (cont'd)

- Categories of Address
  - Unicast addresses : defining a single computer
  - Anycast addresses : defining a group of computers whose addresses have the same prefix
    - All the computers connected to the the same physical network share the same prefix address
  - Multicast addresses : defining a group of computers that may or may not share the same prefix and may or may not be connected to the same physical network

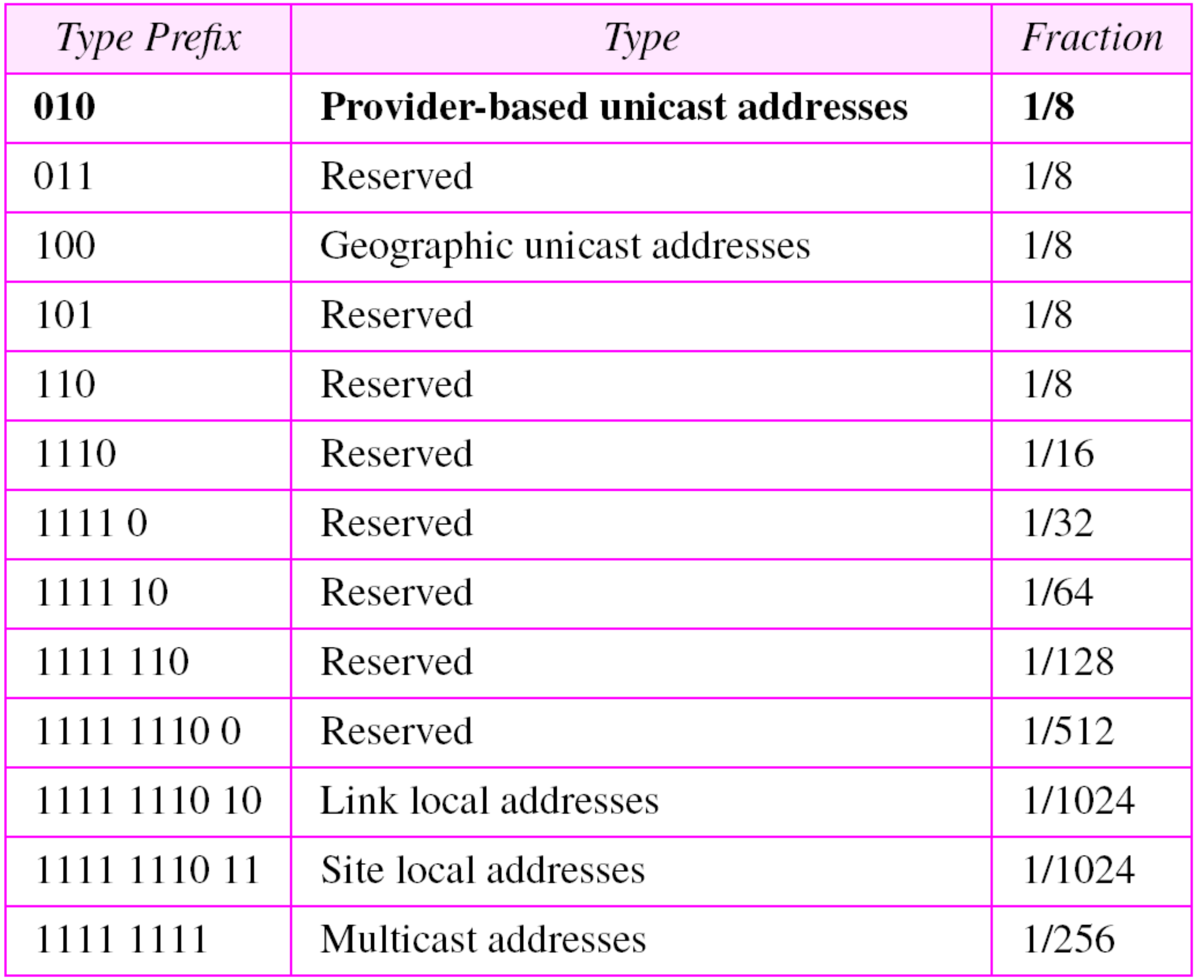
IPv6 Addresses (cont'd)

- Address Space Assignment



IPv6 Addresses (cont'd)

- □ Type prefixes for IPv6 addresses

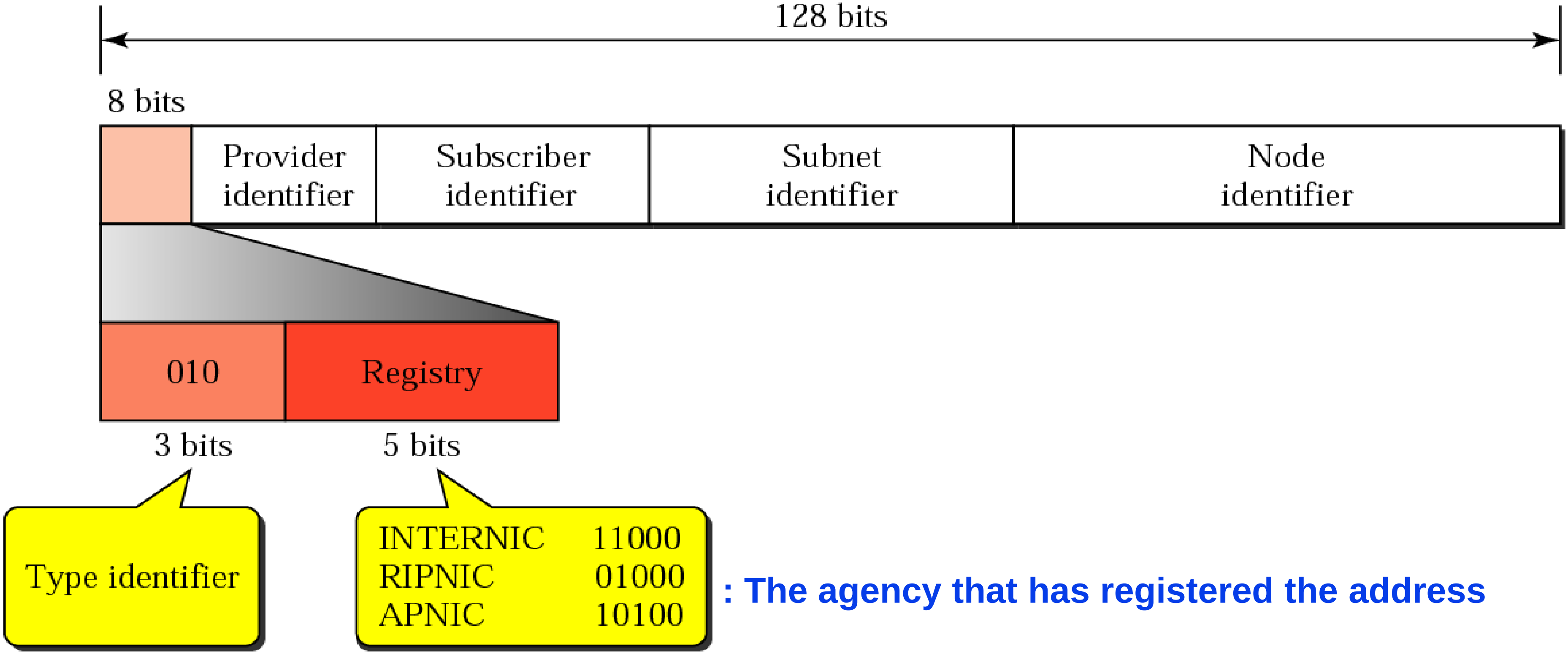


Type Prefix	*Type*	*Fraction*
010	**Provider-based unicast addresses**	**1/8**
011	Reserved	1/8
100	Geographic unicast addresses	1/8
101	Reserved	1/8
110	Reserved	1/8
1110	Reserved	1/16
1111 0	Reserved	1/32
1111 10	Reserved	1/64
1111 110	Reserved	1/128
1111 1110 0	Reserved	1/512
1111 1110 10	Link local addresses	1/1024
1111 1110 11	Site local addresses	1/1024
1111 1111	Multicast addresses	1/256

IPv6 Addresses (cont'd)

□ Provider-Based Unicast Address

- generally used by a normal host as a unicast address



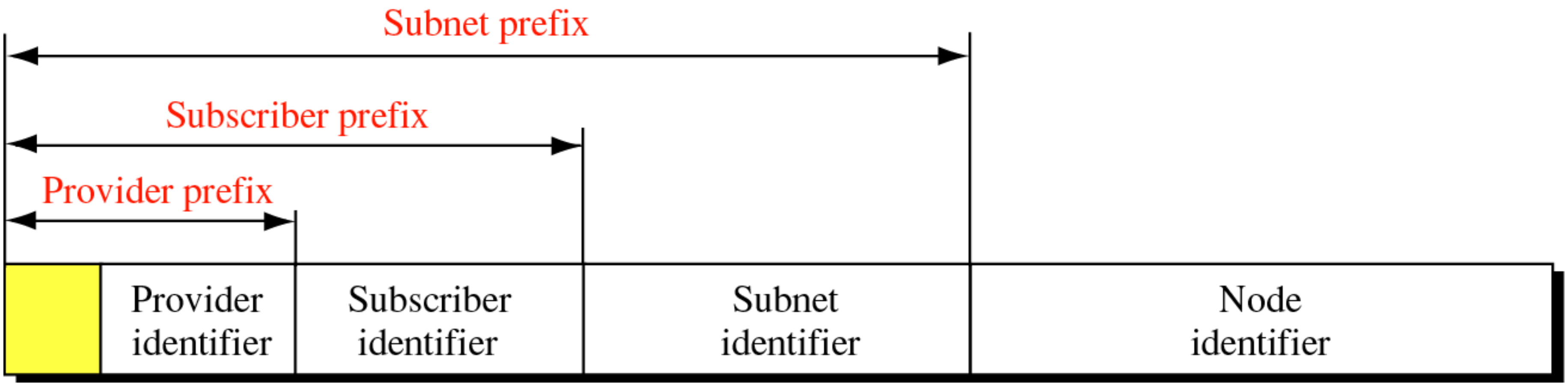
: The agency that has registered the address

IPv6 Addresses (cont'd)

- Type identifier : defining the address as a provider-based address
- Registry identifier : indicating the agency that has registered the address.
  - INTERNIC (code 11000) : the center for North America
  - RIPNIC (code 01000) : the center for European registration
  - APNIC (code 10100) : the center for Asian and Pacific countries
- Provider identifier : identifying the provider for Internet access
- Subscriber identifier : 24-bit length is recommended for this field
- Subnet identifier : each subscriber can have many different subnetworks and each network can have different identifiers. The subnet identifier defines a specific network under the territory of the subscriber. A 32-bit length is recommended for this field.
- Node identifier : defining the identity of the node connected to a subnet. A length of 48bits is recommended for this field to make it compatible with the 48-bit link (physical) address used by Ethernet.

IPv6 Addresses (cont'd)

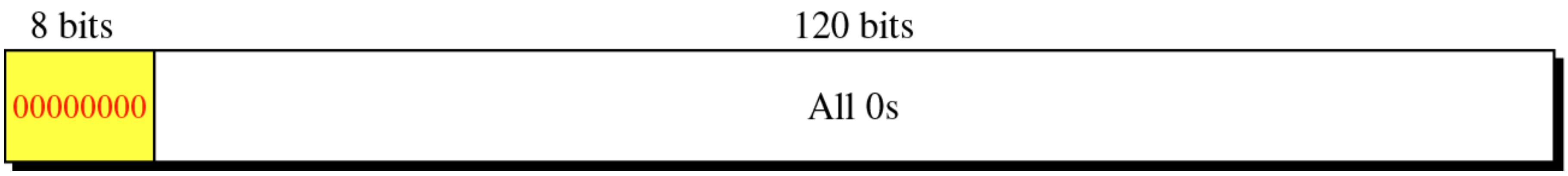
- Address Hierarchy



IPv6 Addresses (cont'd)

□ Reserved addresses

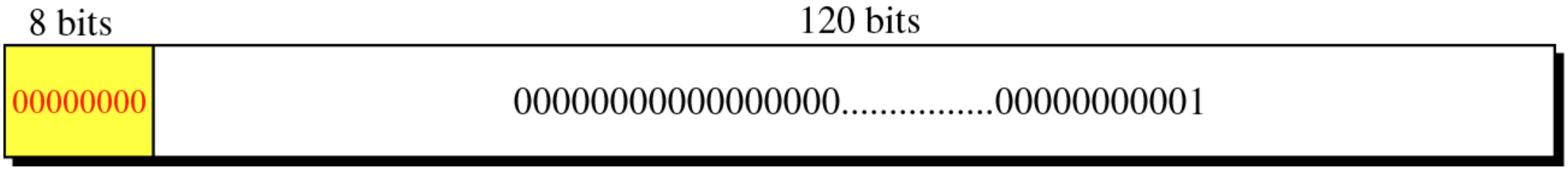
- <u>Reserved prefix (0000 0000)</u>
- Unspecified address
  - this address is used when a host does not know its own address and sends an inquiry to find its address. So, it can be used as a source address



8 bits	120 bits
00000000	All 0s

IPv6 Addresses (cont'd)

- Loopback address
  - used by a host to test itself without going into the network



8 bits

120 bits

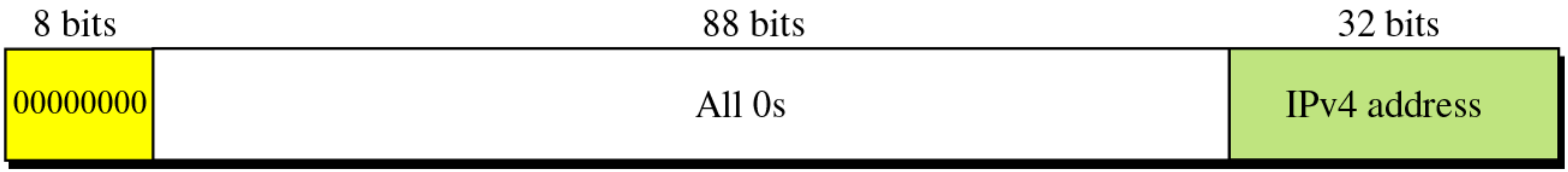
00000000

00000000000000000................00000000001

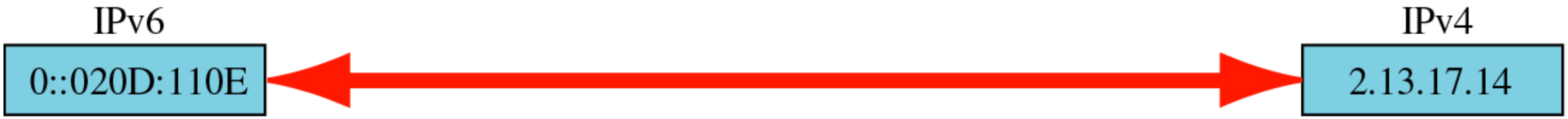
  - is useful for testing the functions of software packages in layers before even connecting the computer to the network
  - 00000000 followed by 119 zero bits and 1 one bit
- IPv4 addresses
  - transition from IPv4 to IPv6 hosts can use their IPv4 addresses embedded in IPv6 addresses
  - end-to-end computers having IPv6 addresses, but used in the case that passes the networks of IPv4

IPv6 Addresses (cont'd)

- Two formats for this purpose : compatible and mapped
- compatible address : 96 bits of zero followed by 32 bits of IPv4 addresses
  - Networks are still using IPv4 addresses



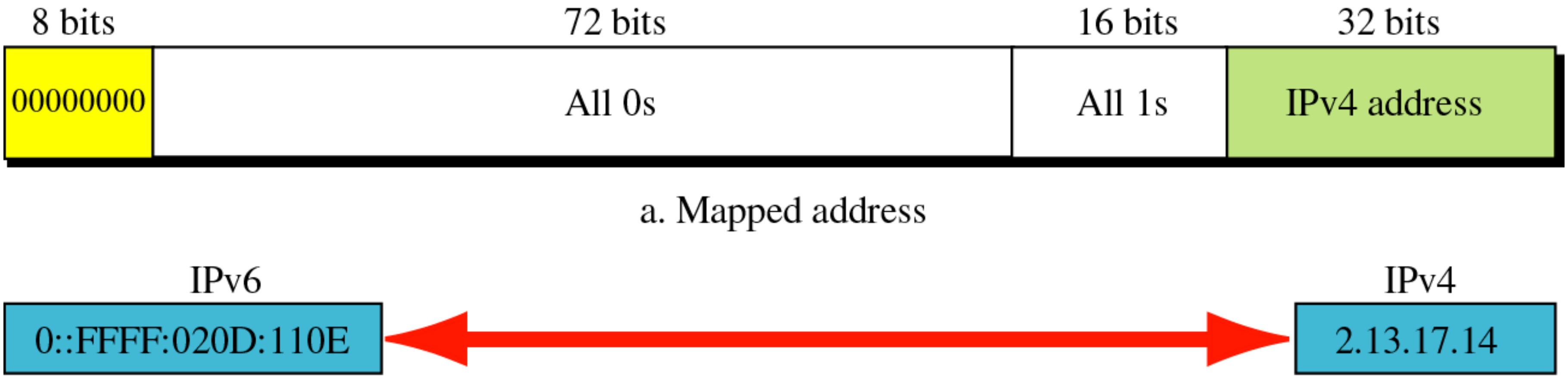
a. Compatible address



b. An example of address transformation

IPv6 Addresses (cont'd)

- Mapped address : comprising 80 bits of zero, followed by 16 bits of one, followed by the 32-bit IPv4 address.
  - used when a computer that has migrated to IPv6 wants to send a packet to a computer still using IPv4
  - The packet travels mostly through IPv6 networks but is finally delivered to a host that uses IPv4

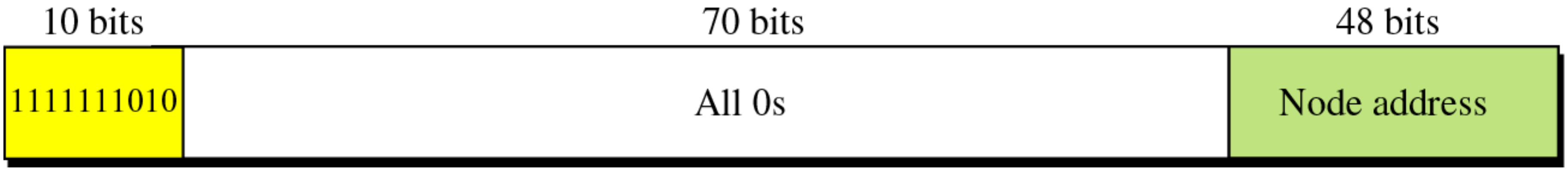


a. Mapped address

b. An Example of address transformation

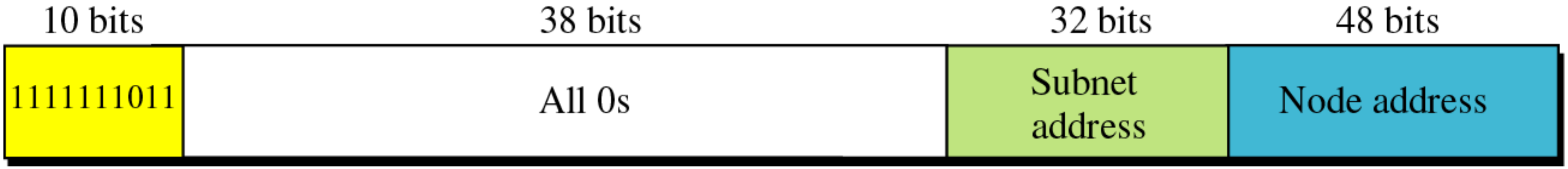
IPv6 Addresses (cont'd)

- Local addresses
  - reserved prefix (11111110)
  - Link local address : used if a LAN is to use the Internet protocols but is not connected to the Internet for security reasons.



10 bits	70 bits	48 bits
1111111010	All 0s	Node address

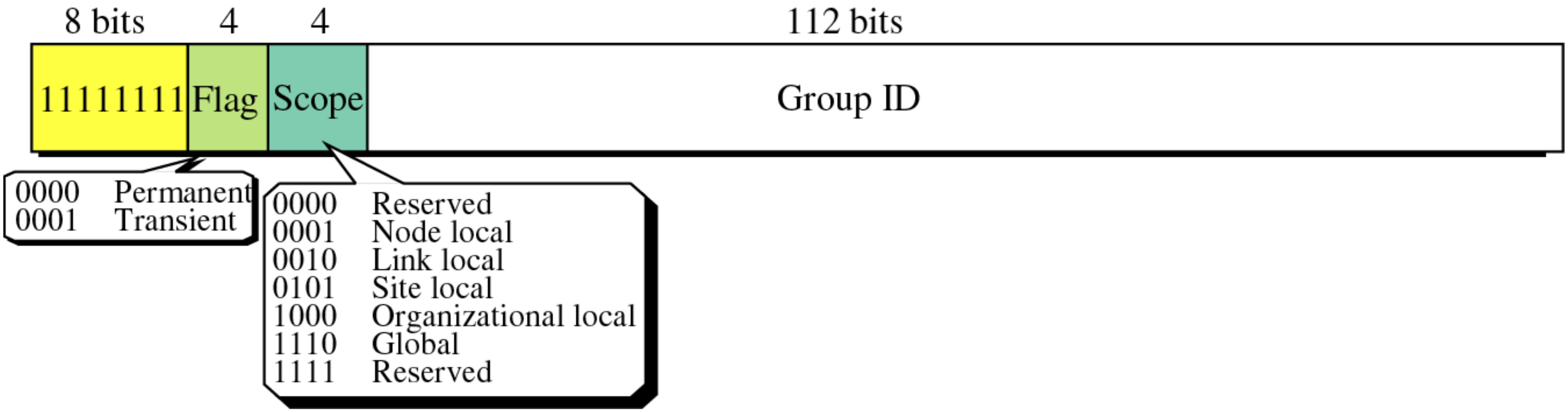
  - Site local address : used if a site having several networks uses the Internet protocols but is not connected to the Internet, also for security reasons.



10 bits	38 bits	32 bits	48 bits
1111111011	All 0s	Subnet address	Node address

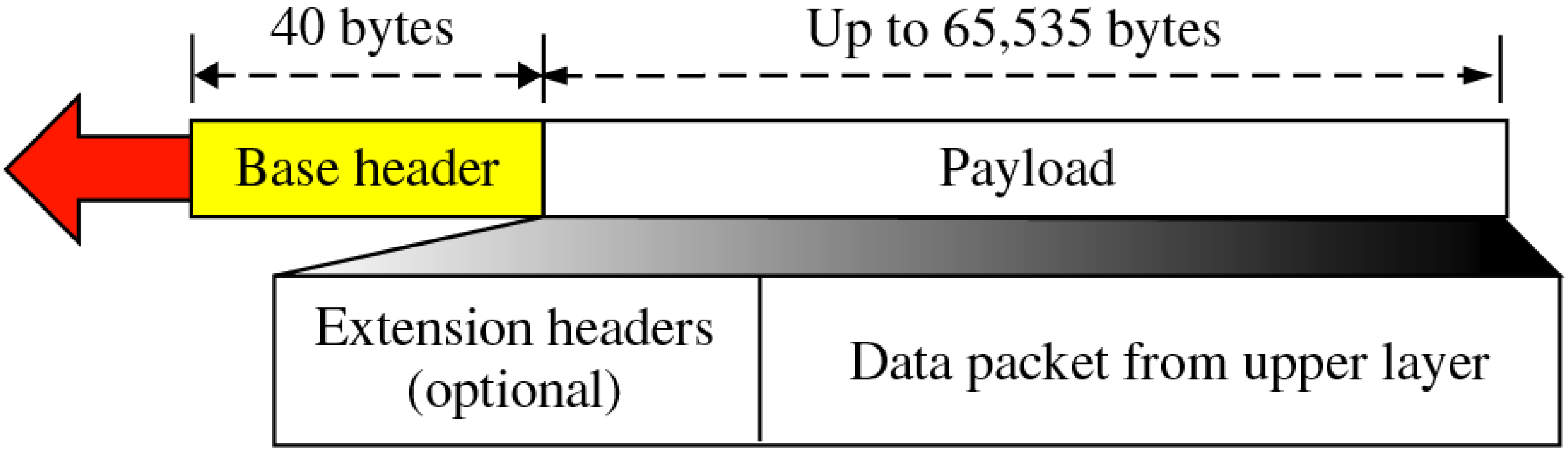
IPv6 Addresses (cont'd)

- Multicast Addresses
  - used to define a group of hosts instead of just one
  - The second field
    - permanent group address : defined by Internet authorities and can be accessed at all times
    - transient group address : used only temporarily. For example, used in a teleconference



IPv6 Packet Format

- is composed of a mandatory base header followed by the payload
-

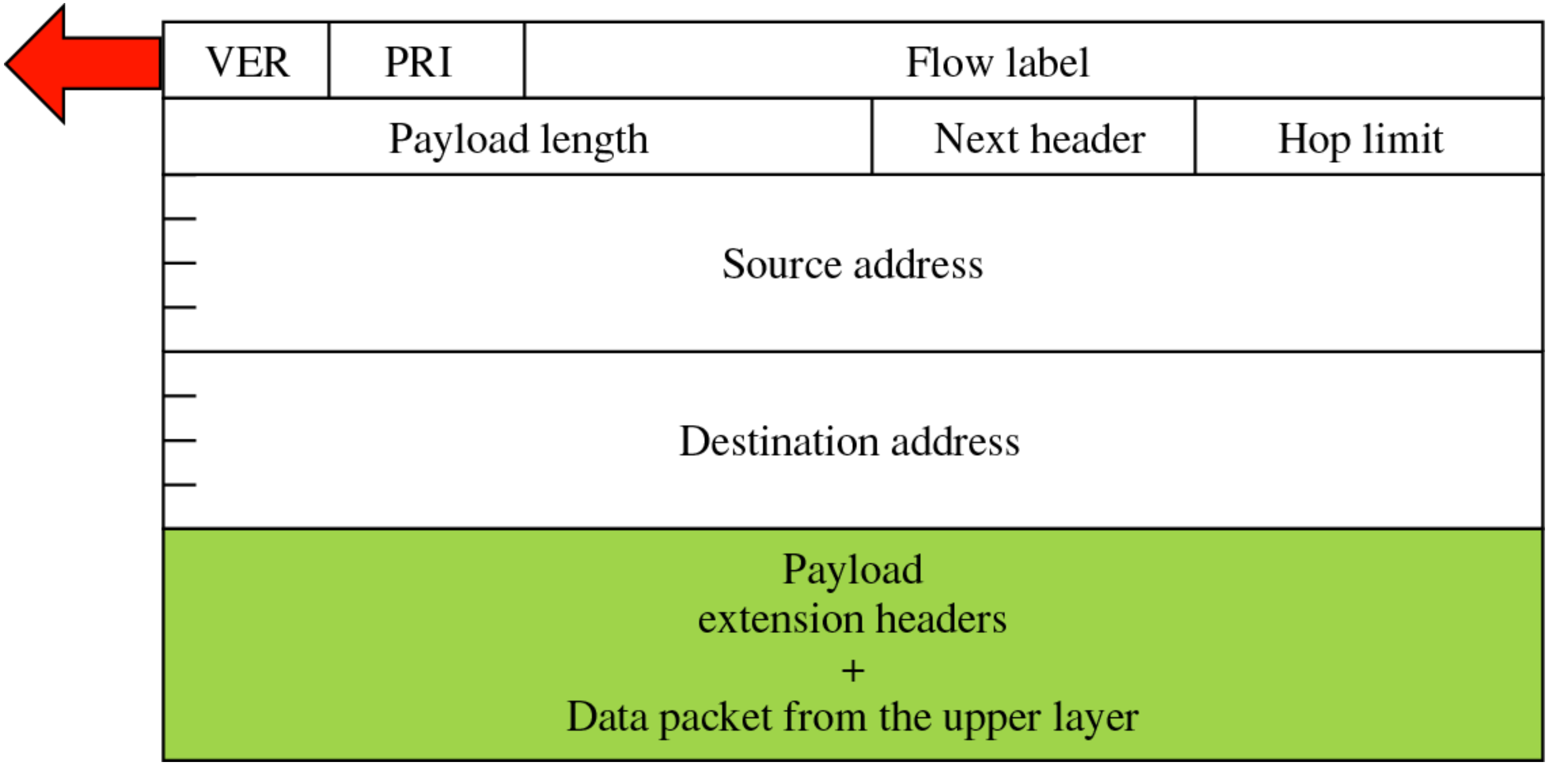


IPv6 Packet Format (cont'd)

- Base header
  - Version : for IPv6, the value is 6 (4 bits)
  - Priority : defining the priority of the packet with respect to traffic congestion (4 bits)
  - Flow label : designed to provide special handling for a particular flow of data (24 bits)
  - Payload length : defining the total length of the IP datagram excluding the base header (2 bytes)

IPv6 Packet Format (cont’d)

- Next header : defining the header that follows the base header in the datagram (8 bits)
  - either one of the optional extension headers used by IP or the header for an upper layer protocol such as UDP or TCP



VER

PRI

Flow label

Payload length

Next header

Hop limit

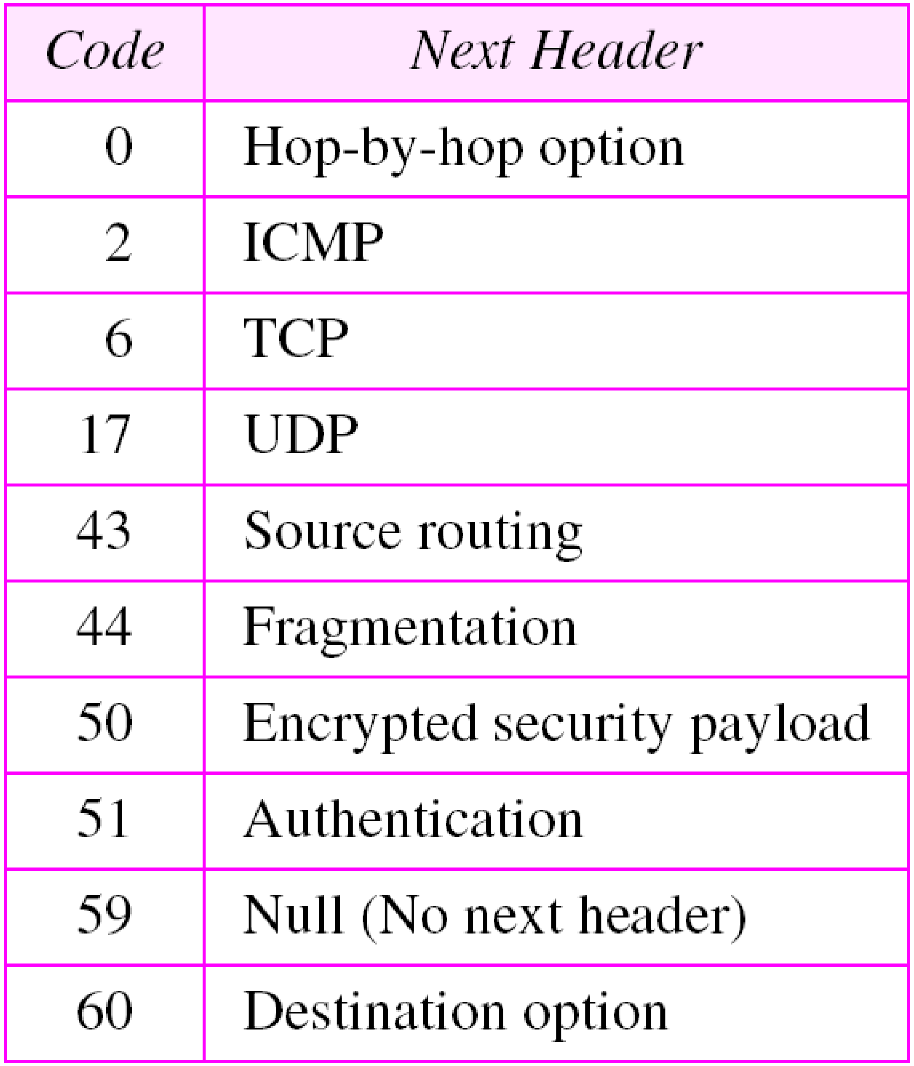
Source address

Destination address

Payload
extension headers
+
Data packet from the upper layer

IPv6 Packet Format (cont'd)

□ **Next header codes**



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

IPv6 Packet Format (cont’d)

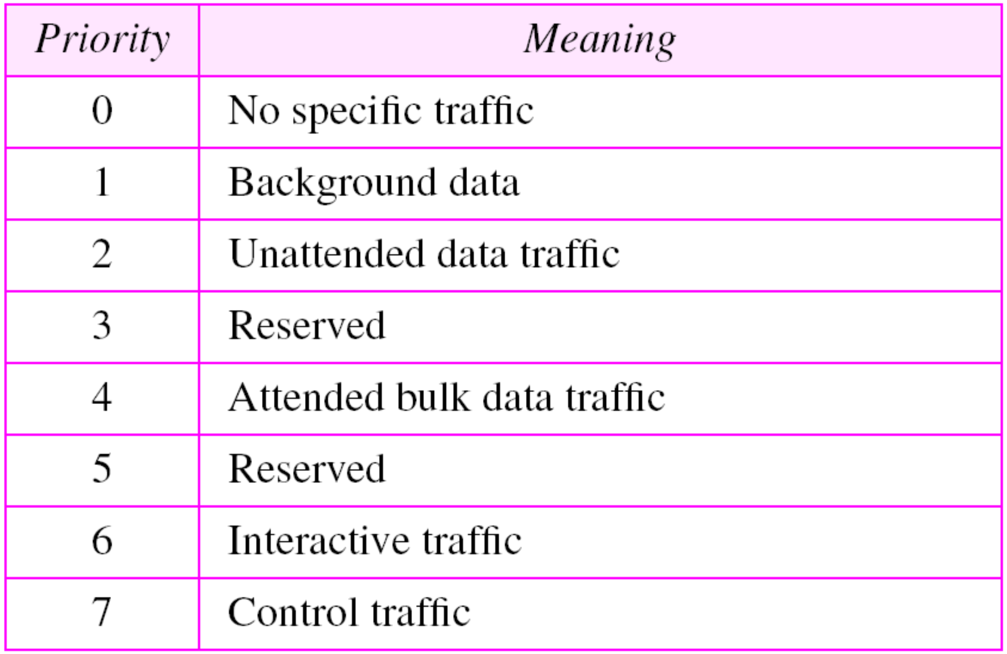
- Hop limit : serving the same purpose as the TTL field in IPv4 (8 bits)
- Source address : the original source of the datagram
- Destination addresses : the final destination of the datagram. But, if source address routing is used, this field contains the address of the next router

IPv6 Packet Format (cont'd)

- Priority
  - IPv6 divides traffic into two broad categories : congestion-controlled and non-congestion-controlled.
- Congestion-Controlled Traffic
  - If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as *congestion-controlled traffic*. (0 ~ 7 priorities)
    - No specific traffic
    - Background data : usually delivered in the background. Delivery of the news is a good example
    - Unattended data traffic : If the user is not waiting (attending) for the data to be received, the packet will be given priority 2. E-mail belongs to this group.

IPv6 Packet Format (cont’d)

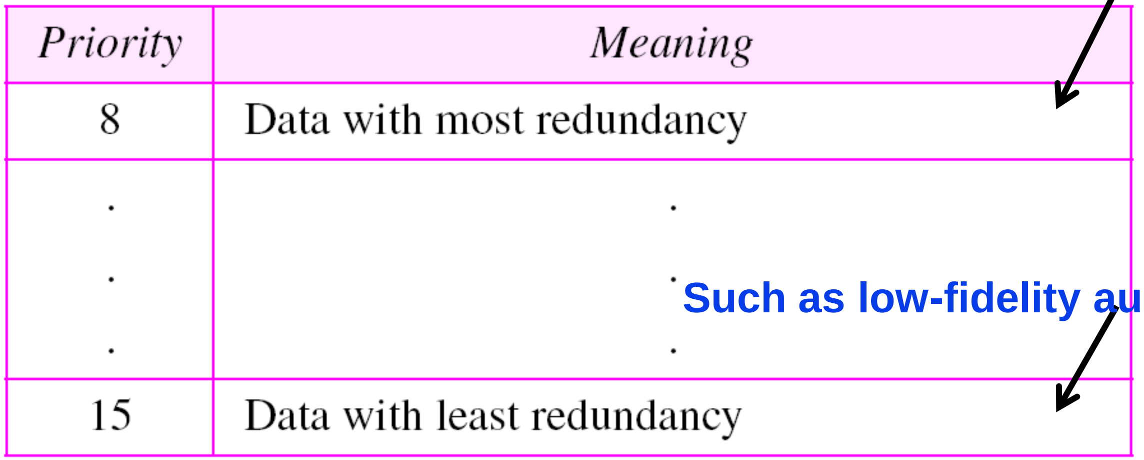
- **Attended bulk data traffic : the protocol that transfers the bulk of data while the user is waiting (attending) to receive the data (possibly with delay) is given priority 4. FTP and HTTP belong to this group.**
- **Interactive traffic : Protocols such as TELNET that need interaction with the user are assigned priority 6**
- **Control traffic : Priority 7 is assigned for routing protocol such as OSPF and RIP and management protocols such as SNMP**



Priority	*Meaning*
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

IPv6 Packet Format (cont'd)

- Noncongestion-Controlled Traffic
  - Referring to a type of traffic that expects minimum delay
  - Discarding of packets is not desirable.
  - Retransmission in most cases is impossible.
  - Real-time audio and video are good examples of this type of traffic
  - Priority 8 ~ 15 (the higher priority)



Priority	*Meaning*
8	Data with most redundancy
.	.
.	.
.	.
15	Data with least redundancy

Such as high-fidelity audio or video

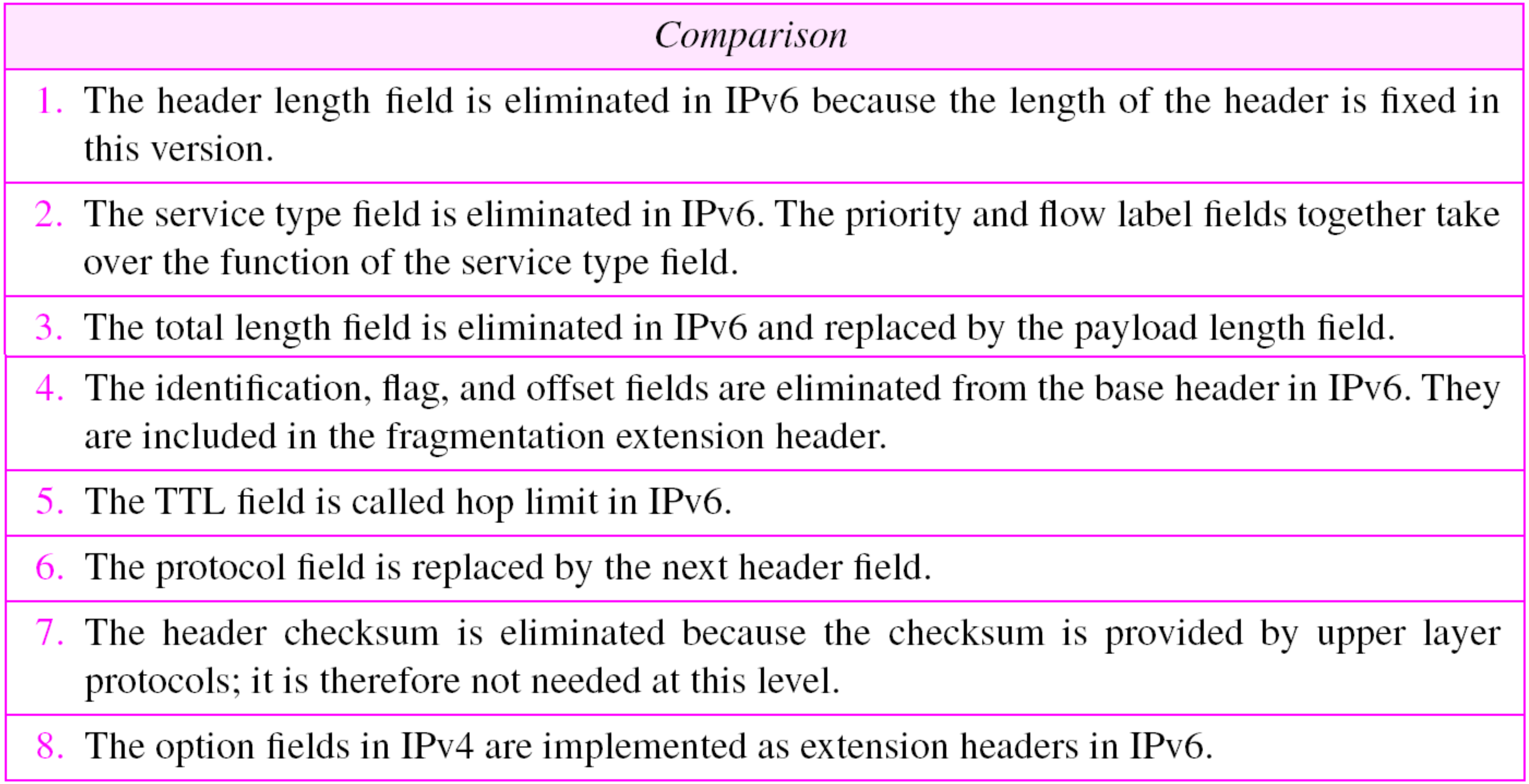
Such as low-fidelity audio or video

IPv6 Packet Format (cont’d)

- **Flow label**
  - **the combination of the source address and the value of the** *flow label* **uniquely defines a flow of packets**
  - **To a router, a flow is a sequence of packets that share the same characteristics, such as traveling the same path, using the same resources, having the same kind of security.**
  - **When the router receives a packet, it consults its flow label table to find the corresponding entry for the flow label value defined in the packet**

IPv6 Packet Format (cont'd)

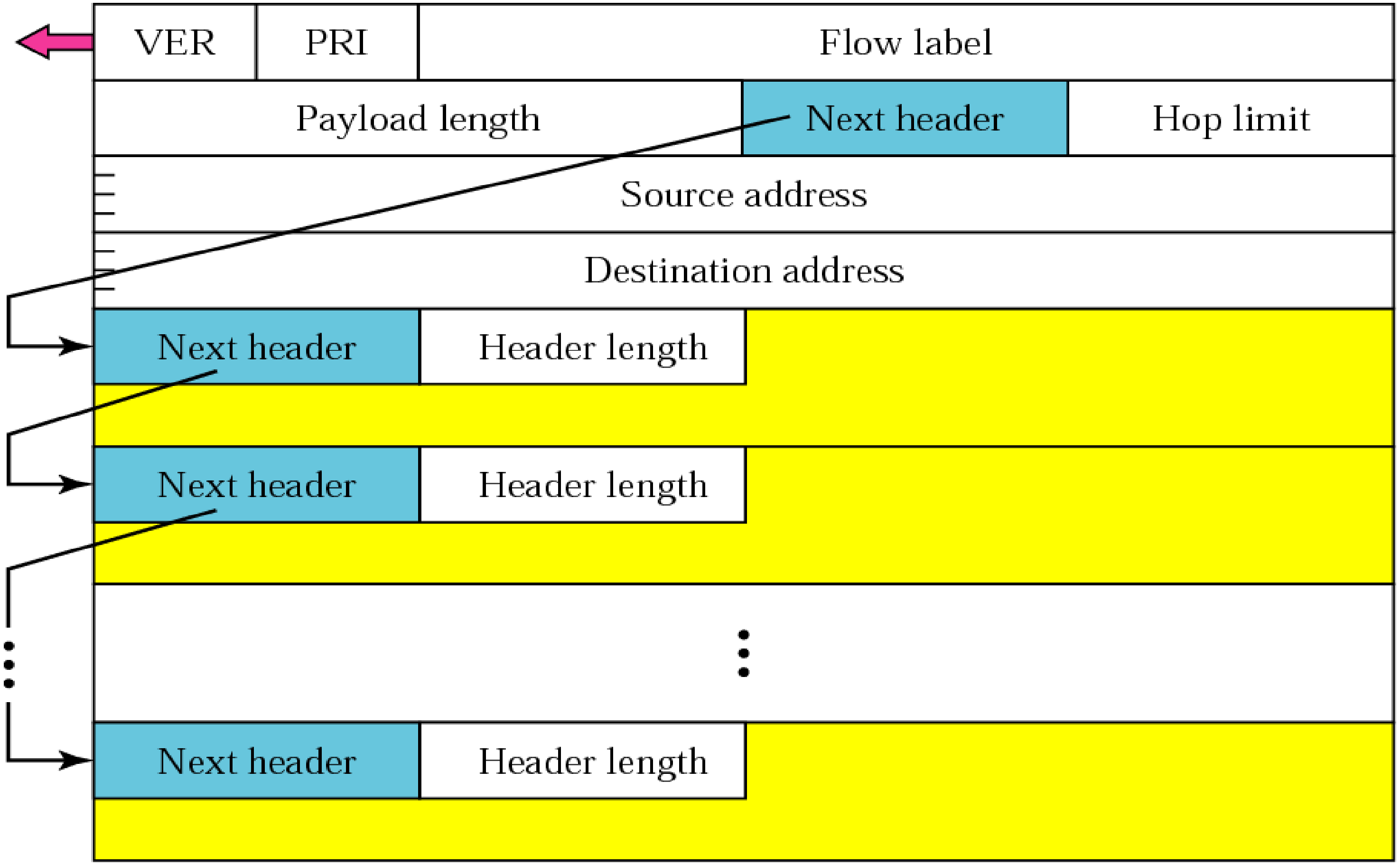
□ **Comparison between IPv4 and IPv6 Headers**



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.

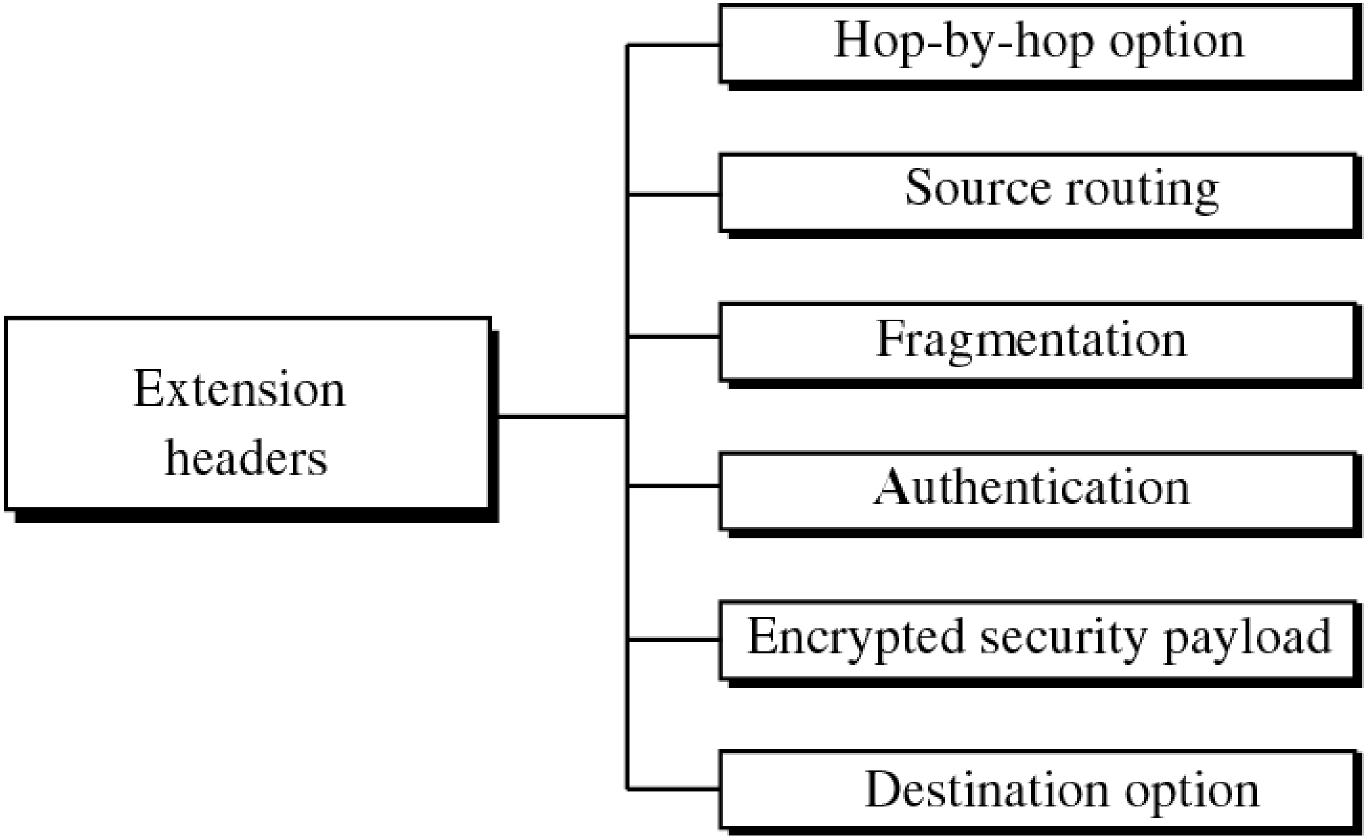
IPv6 Packet Format (cont'd)

- Extension Headers
  - the base header can be followed by up to six extension headers



IPv6 Packet Format (cont'd)

- Extension header types



Extension headers

Hop-by-hop option

Source routing

Fragmentation

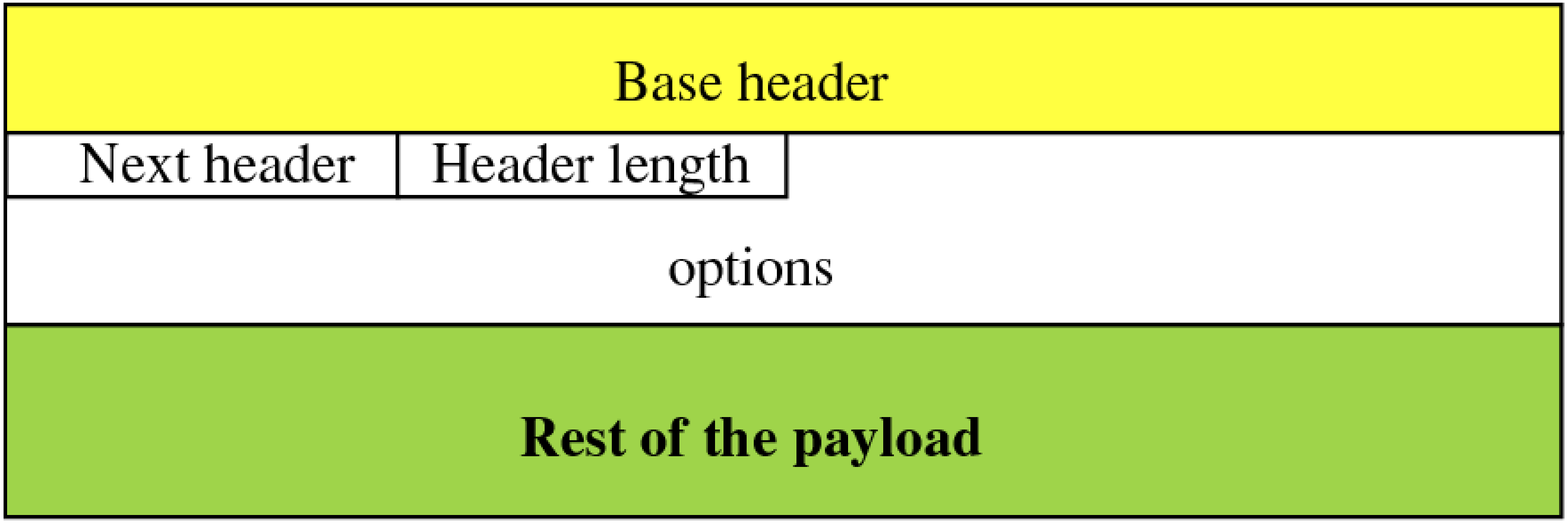
Authentication

Encrypted security payload

Destination option

IPv6 Packet Format (cont'd)

- **Hop-by-Hop Option**
  - **The hop-by-hop option is used when the source needs to pass information to all routers visited by the datagram.**
  - **For example, perhaps routers must be informed about certain management, debugging, or control functions.**



Base header

Next header

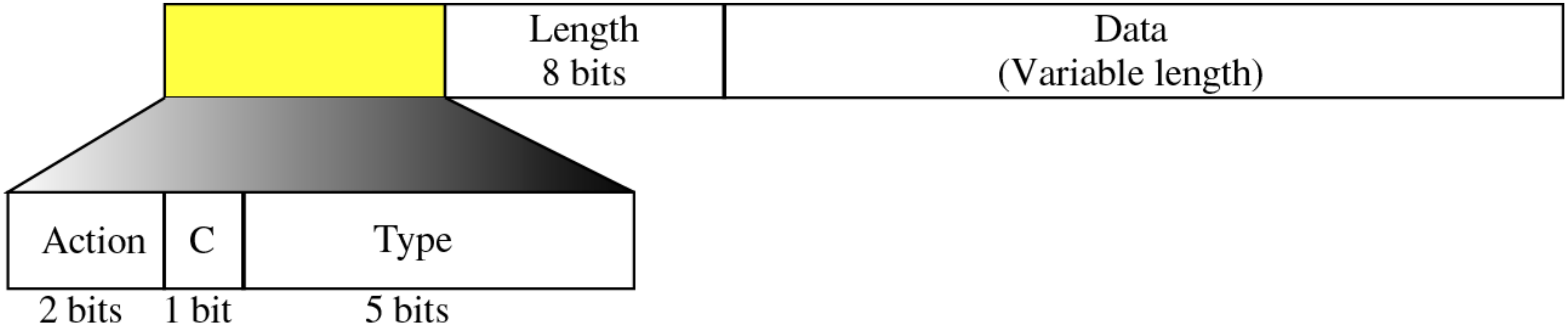
Header length

options

Rest of the payload

IPv6 Packet Format (cont'd)

□ **The format of options in a hop-by-hop option header**



Action: To be taken if the option is not recognized

00 Skip over this option
01 Discard the datagram, no more action
10 Discard the datagram and send an error message
11 Same as 10, but only if the destination is not a multicast address

C: Change in option value

0 Does not change in transit
1 May be changed in transit

Type

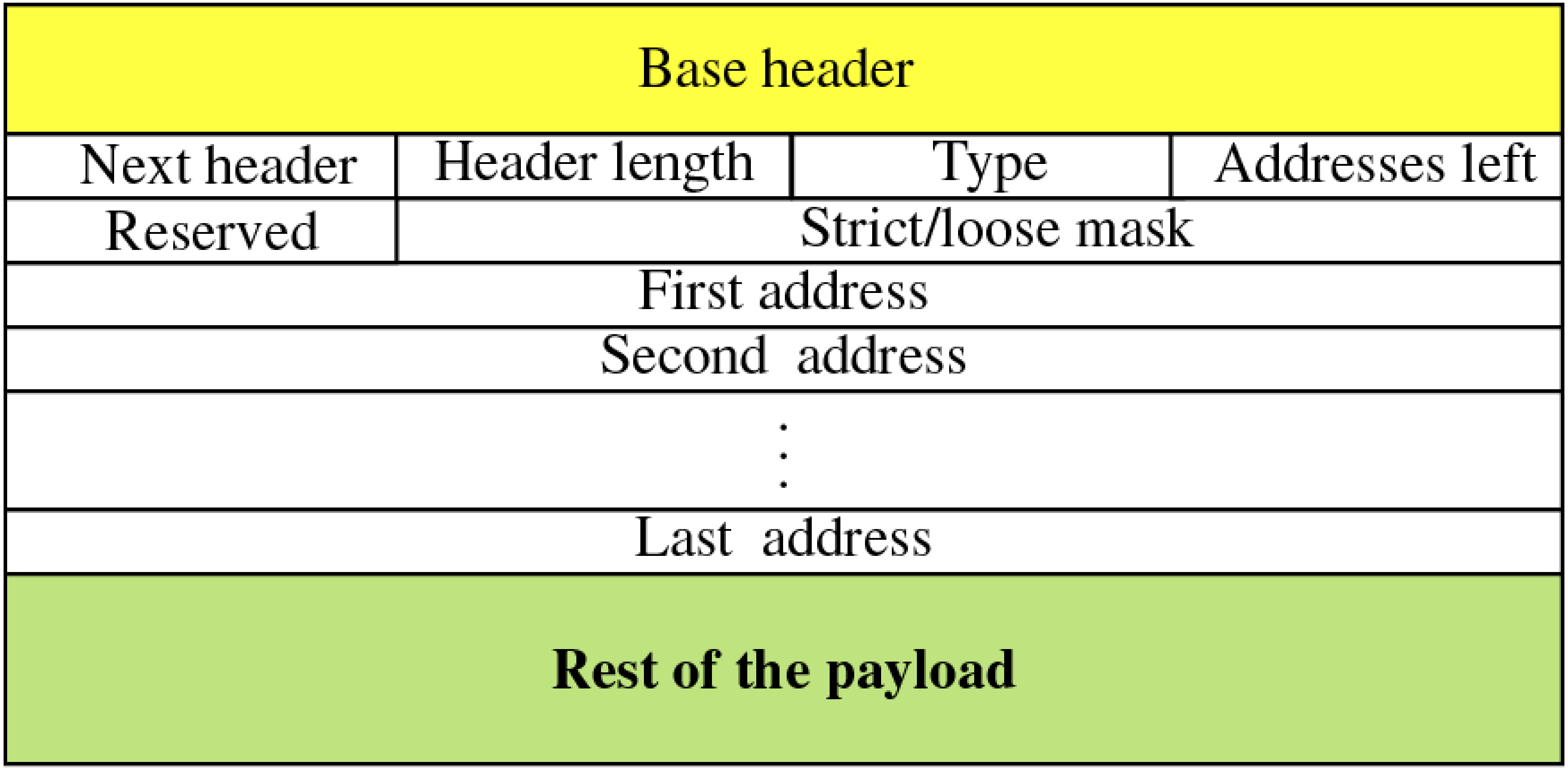
00000	Pad1
00001	PadN
00010	Jumbo payload

IPv6 Packet Format (cont’d)

- Source Routing
  - the source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4
  - Type field : strict or loose routing
  - Addresses left : number of hops still to be needed to reach the destination

IPv6 Packet Format (cont'd)

□ **Source Routing**



Base header

Next header | Header length | Type | Addresses left

Reserved | Strict/loose mask

First address

Second address

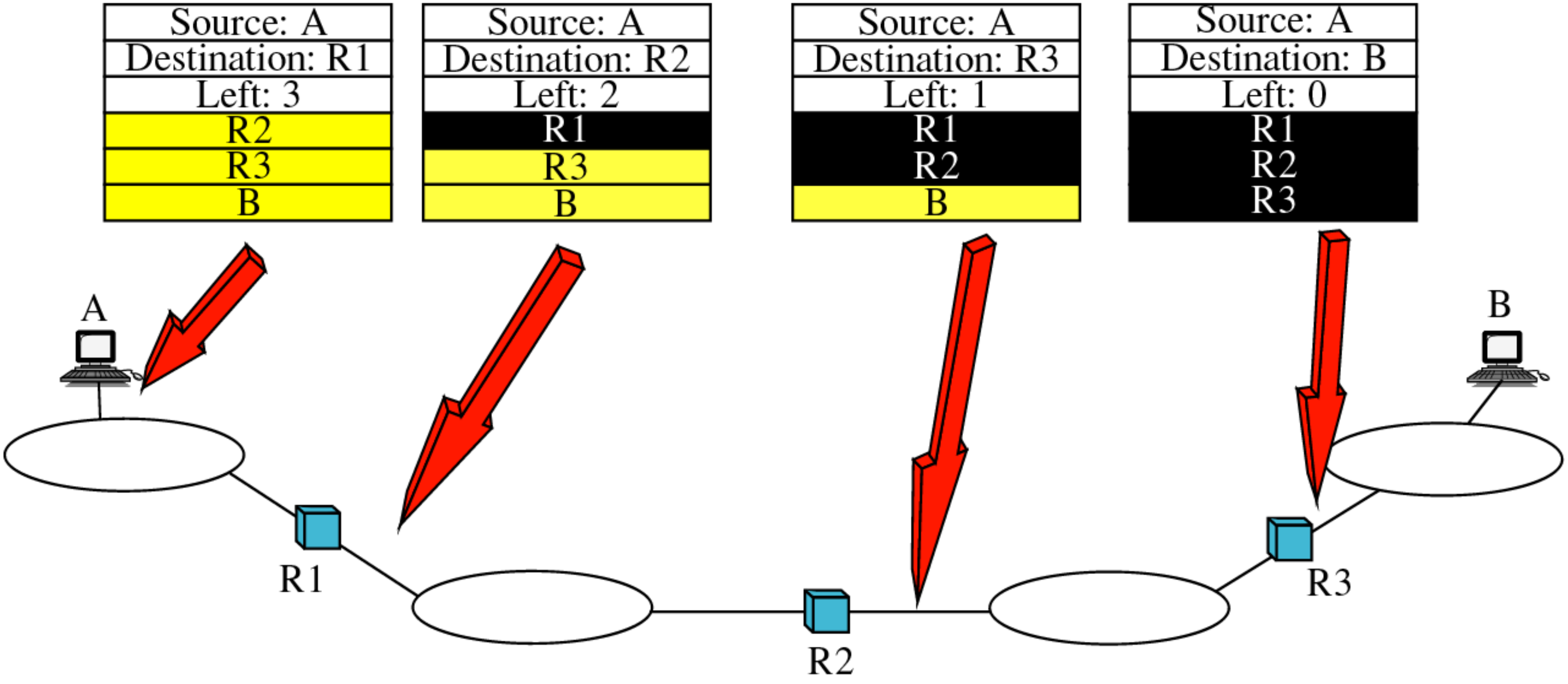
⋮

Last address

Rest of the payload

IPv6 Packet Format (cont'd)

□ **Source routing example**



Source: A
Destination: R1
Left: 3
R2
R3
B

Source: A
Destination: R2
Left: 2
R1
R3
B

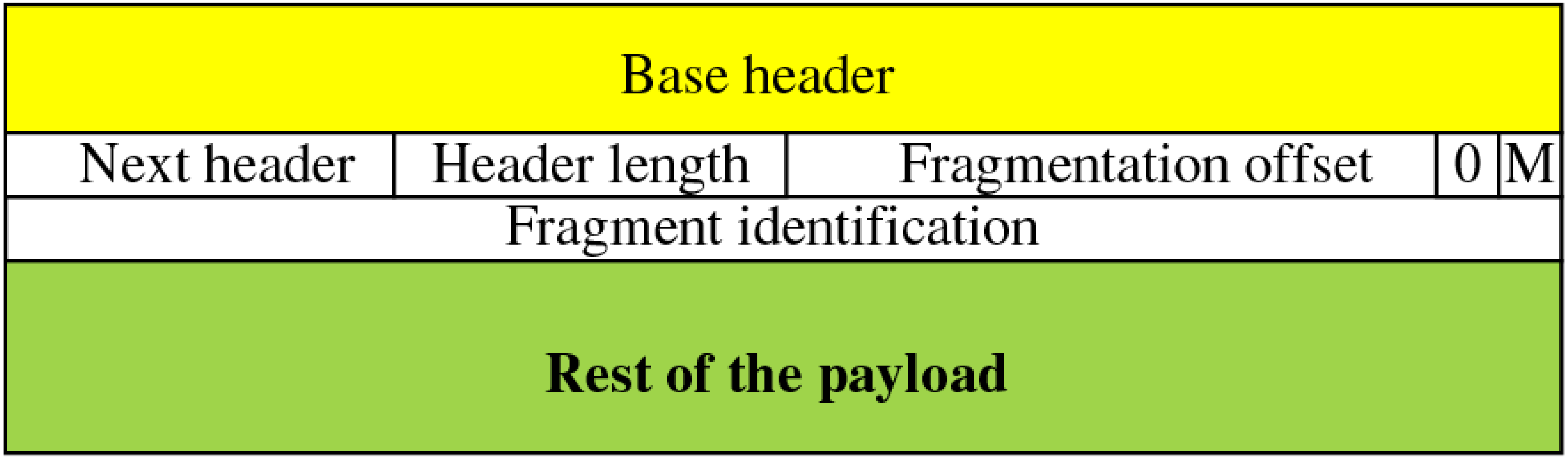
Source: A
Destination: R3
Left: 1
R1
R2
B

Source: A
Destination: B
Left: 0
R1
R2
R3

IPv6 Packet Format (cont'd)

□ Fragmentation

- In IPv6, only the original source can fragment
- A source must use a Path MTU Discovery technique to find the smallest MTU supported by any network on the path. The source then fragments using this knowledge.
- If the source does not use the Path MTU Discovery technique, it should fragment the datagram to a size of 576 bytes or smaller.



Base header

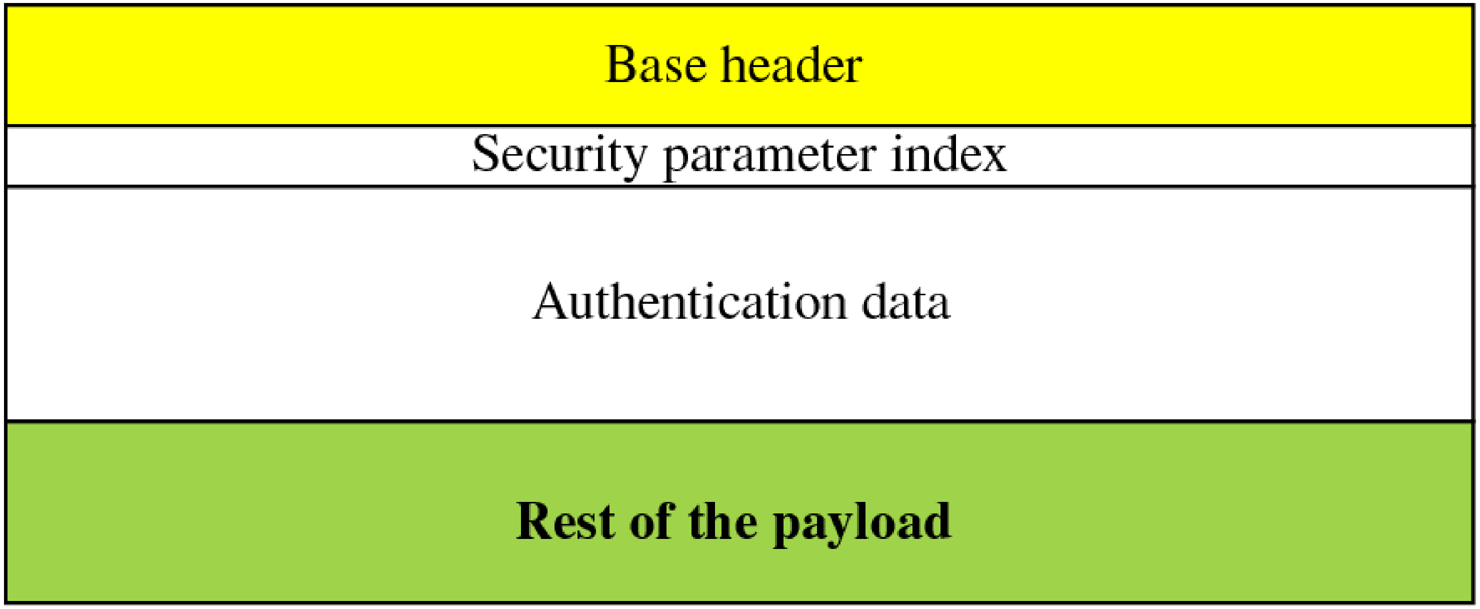
Next header | Header length | Fragmentation offset | 0 | M

Fragment identification

Rest of the payload

IPv6 Packet Format (cont’d)

- **Authentication**
  - **The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.**
  - **The security parameter index field defines the algorithm used for authentication**



Base header

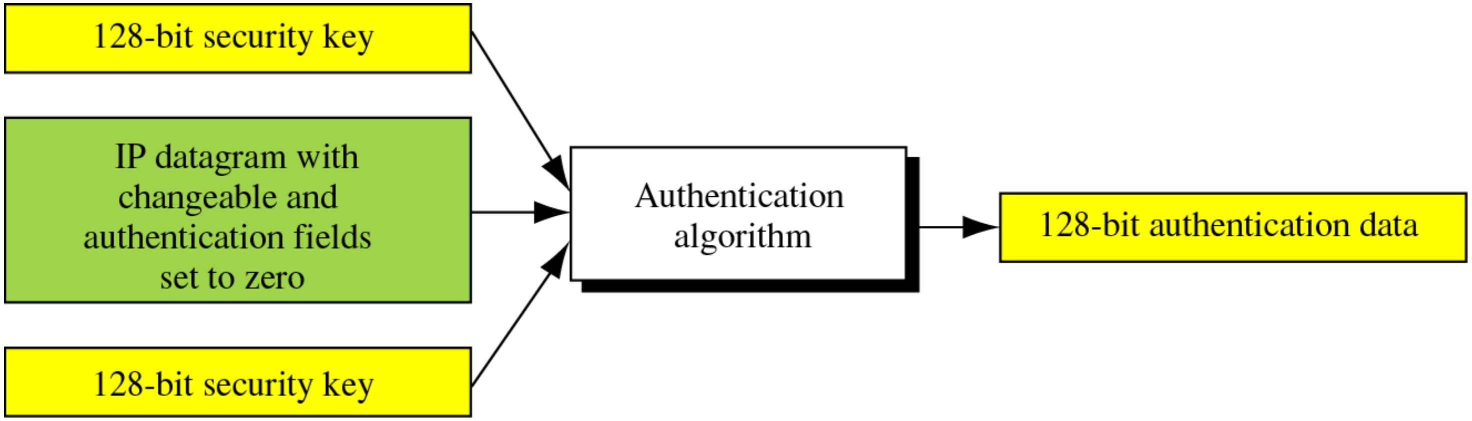
Security parameter index

Authentication data

Rest of the payload

IPv6 Packet Format (cont'd)

- Calculation of authentication data



128-bit security key

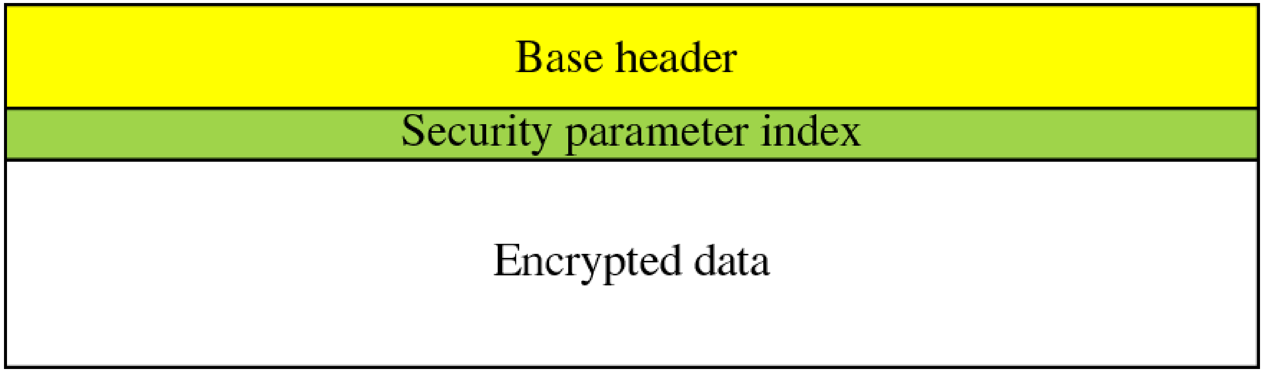
IP datagram with changeable and authentication fields set to zero

128-bit security key

Authentication algorithm

128-bit authentication data

- Encrypted Security Payload (ESP)



Base header

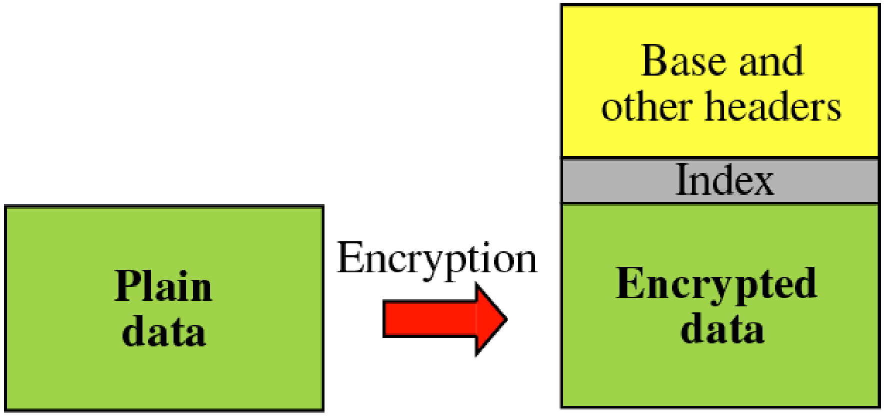
Security parameter index

Encrypted data

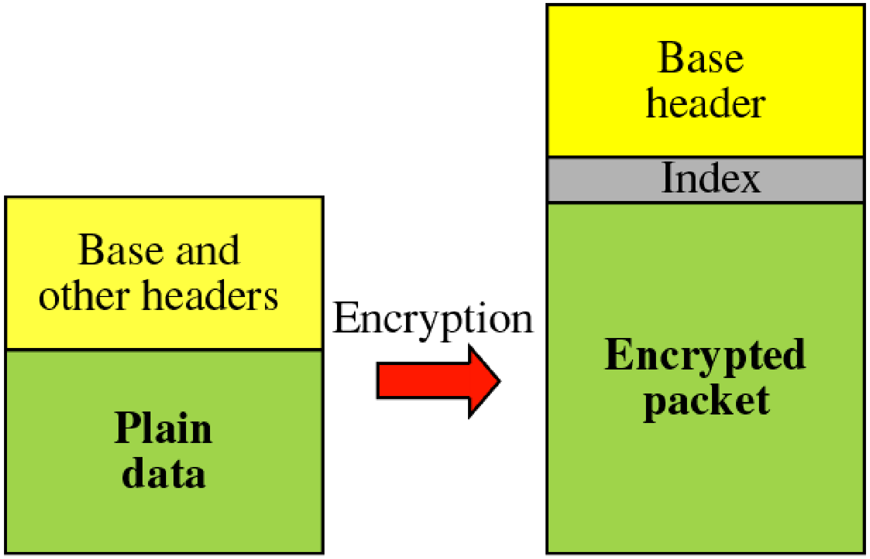
  - Security parameter index : Defining the algorithm used for authentication

IPv6 Packet Format (cont'd)

- Encryption
  - Transport Mode

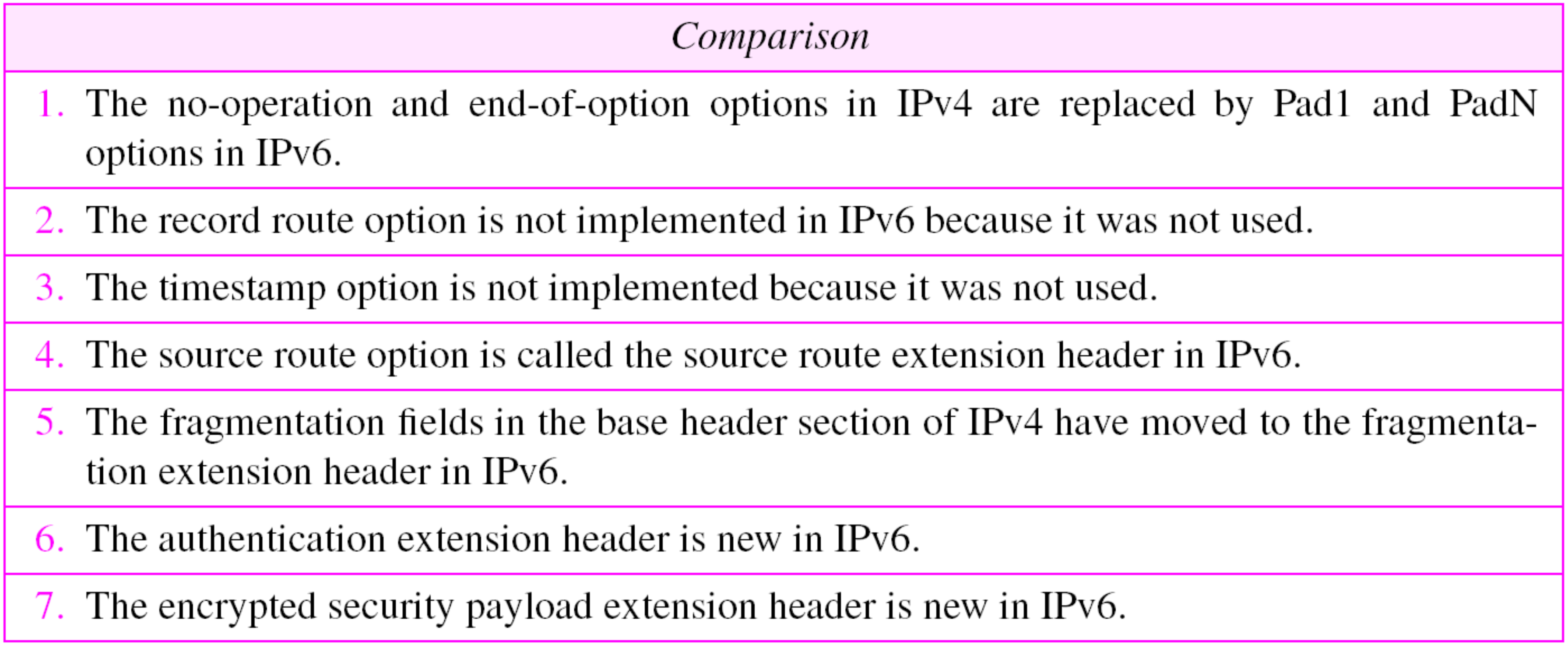


  - Tunnel Mode



IPv6 Packet Format (cont'd)

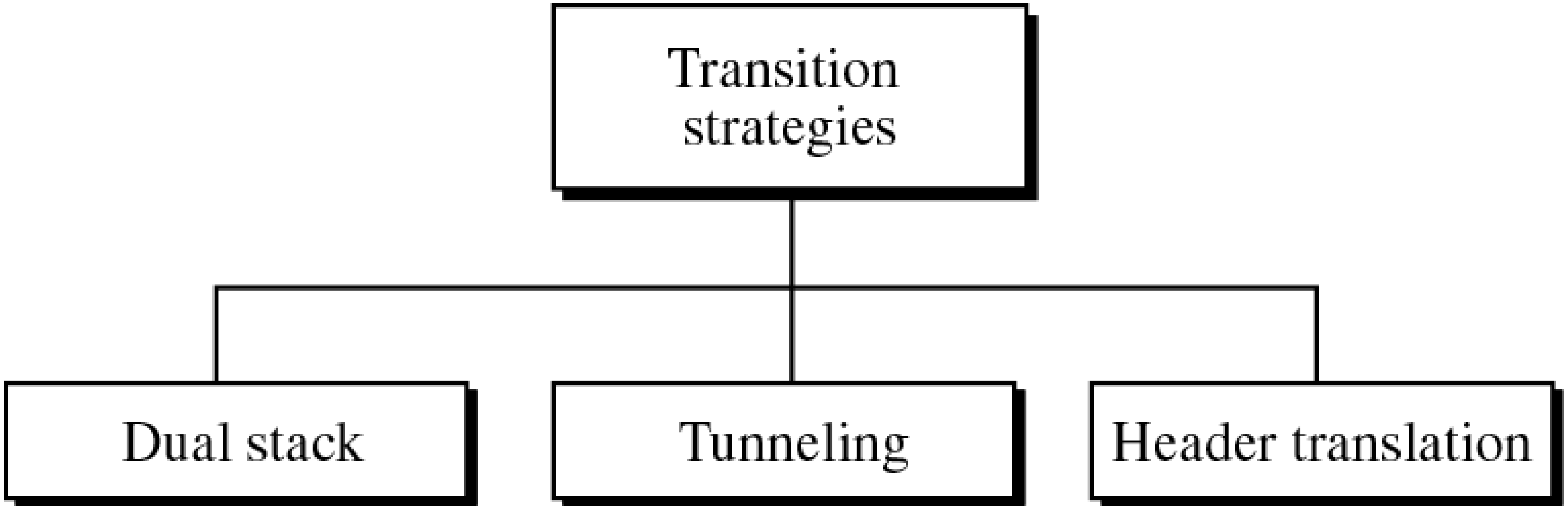
- Comparison between IPv4 and IPv6



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.

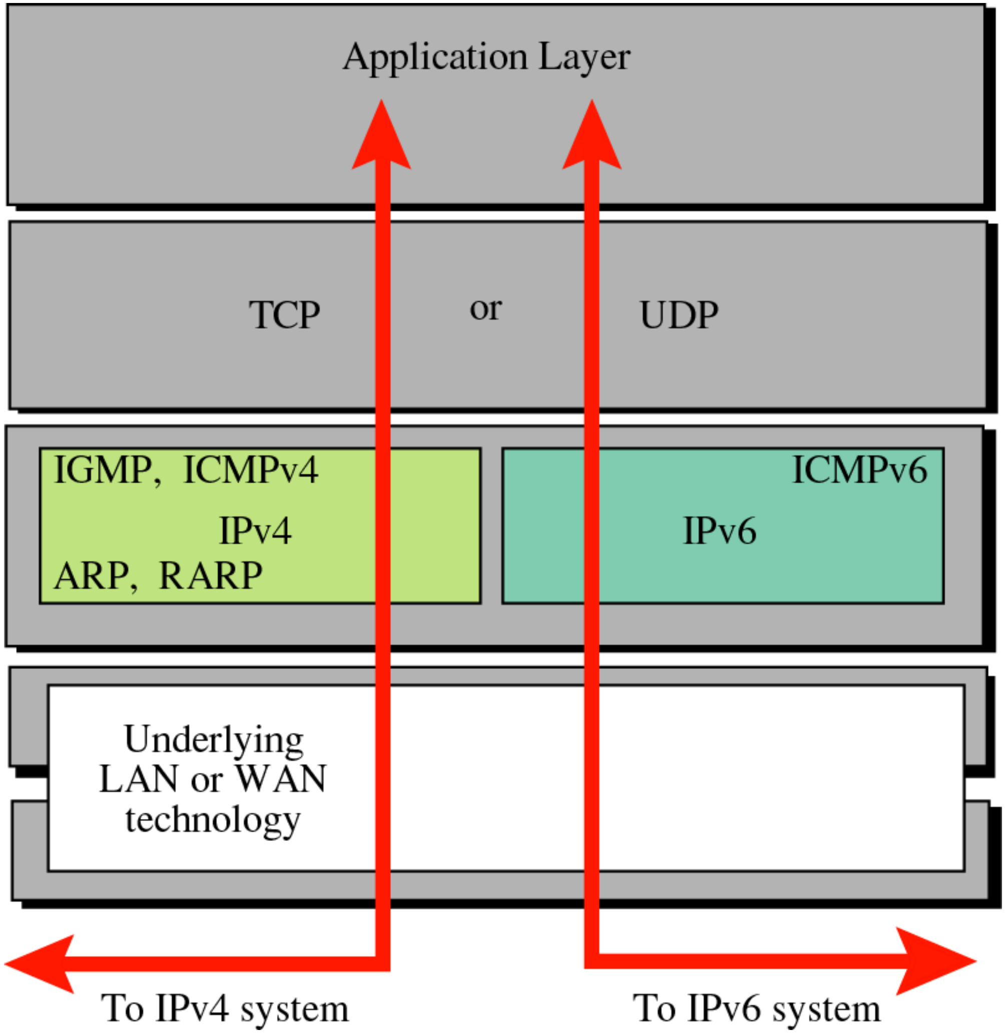
Translation from IPv4 to IPv6

- Three translation strategies



Translation from IPv4 to IPv6 (cont'd)

- Dual Stack



Translation from IPv4 to IPv6 (cont'd)

- It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols.

- To determine which version to use when sending a packet to a destination, the source queries the DNS. If the DNS returns an IPv4 address, the source sends an IPv4 packets. If the DNS returns an IPv6 address, the source host sends an IPV6 packet.

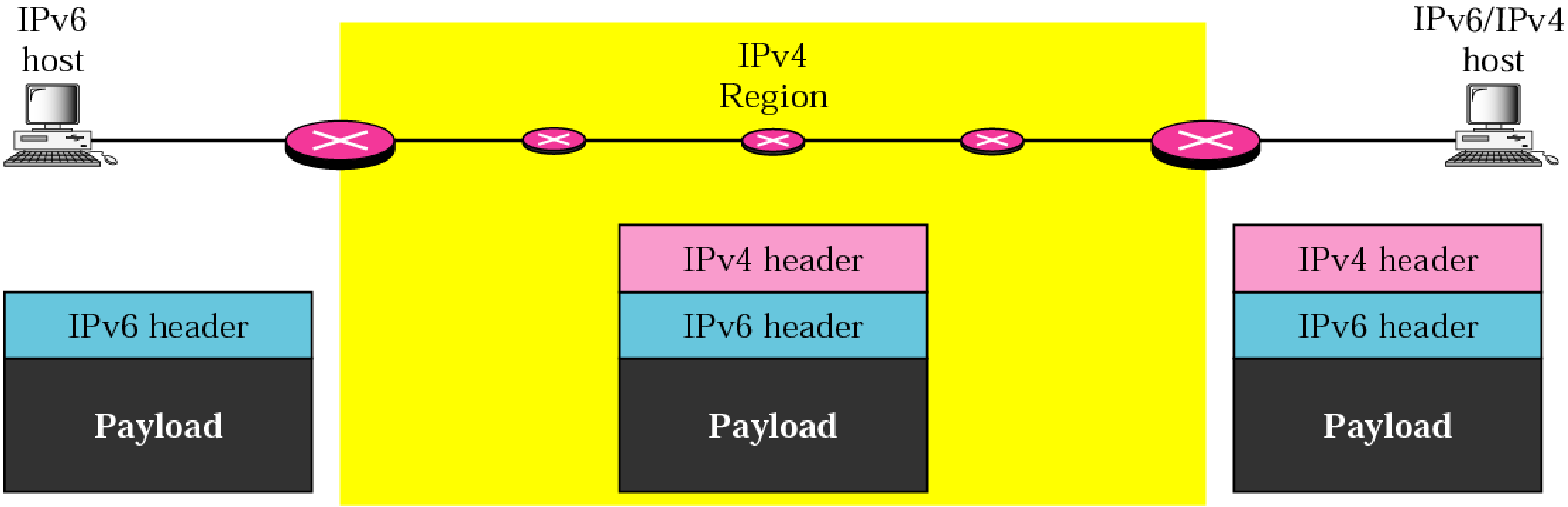
Translation from IPv4 to IPv6 (cont’d)

- Tunneling
  - A strategy used when two computers using IPv6 want to communicate with each other when the packet must pass through a region that uses IPv4.
  - IPv6 packet is encapsulated in an IPv4 packet when it enters the region
  - Use of compatible address

Translation from IPv4 to IPv6 (cont'd)

- Automatic Tunneling

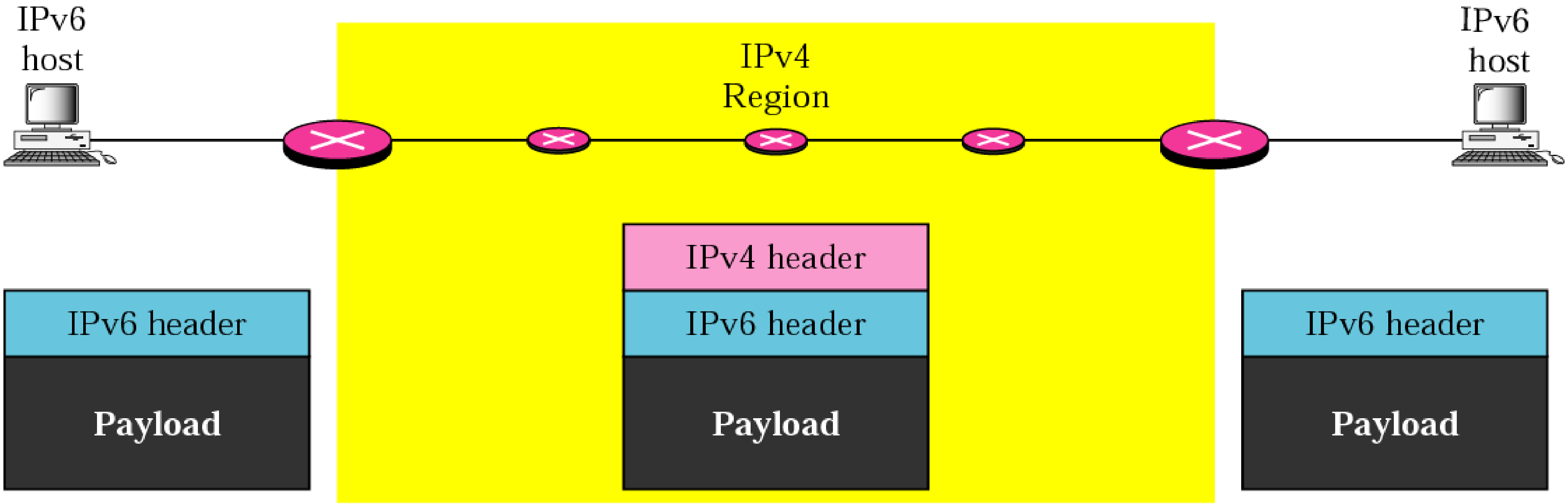
  - The destination host recognizes an IPv4 packet. Recognizing its IPv4 address, it reads the header, and finds (through protocol field value) that the packet is carrying an IPv6 packet



Translation from IPv4 to IPv6 (cont'd)

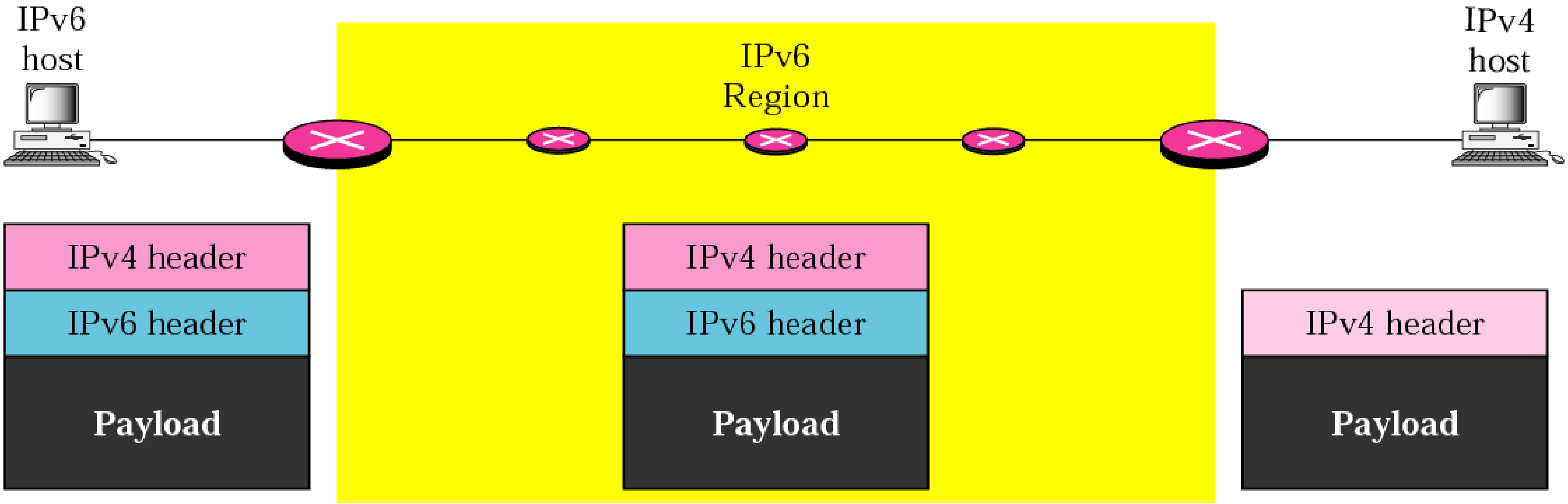
Configured Tunneling

- If the receiving host does not support an IPv6-compatible address, the sender receives a noncompatible IPv6 address from the DNS.



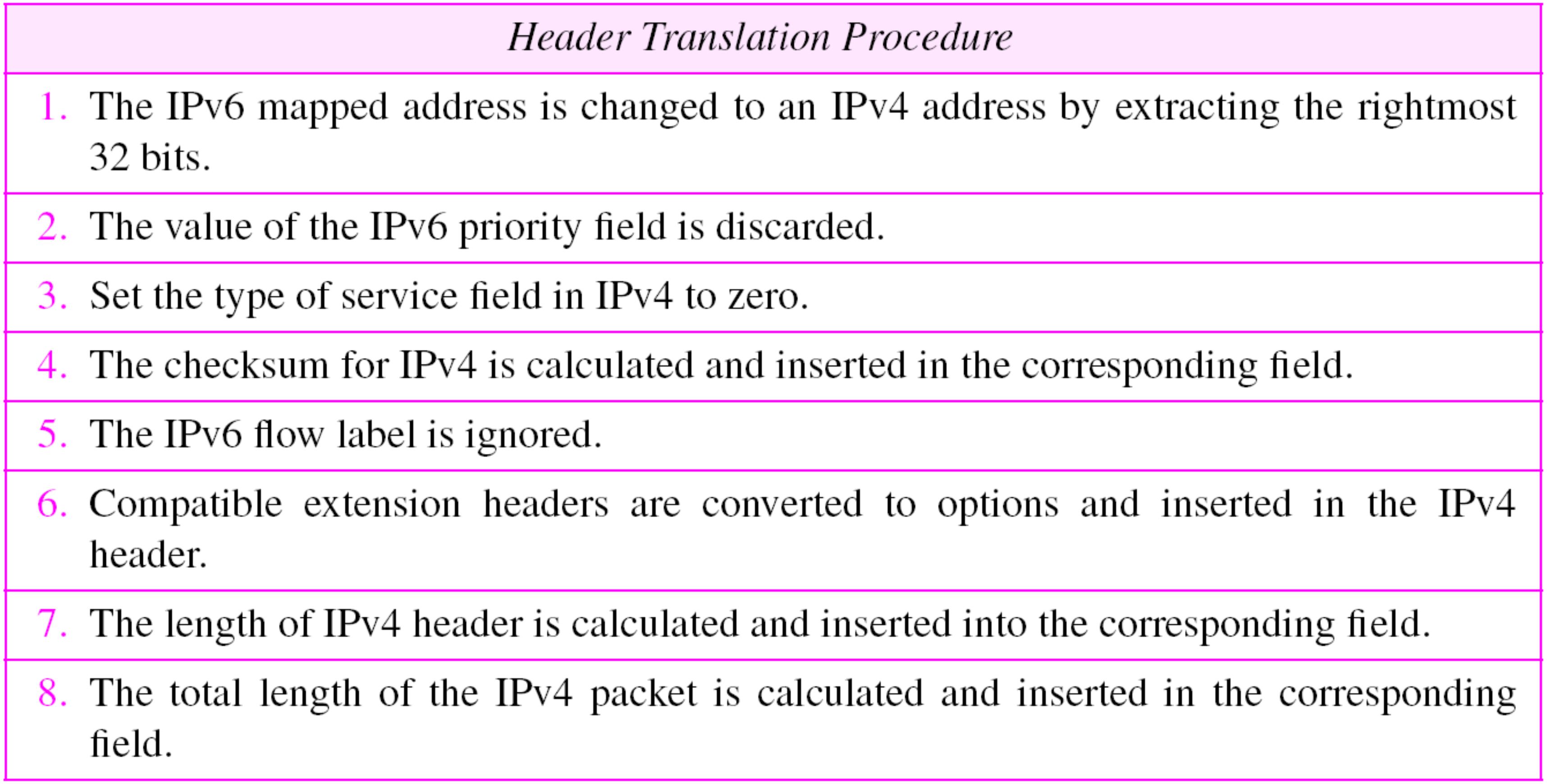
Translation from IPv4 to IPv6 (cont'd)

- Header Translation
  - is necessary when the majority of the Internet has moved to IPv6 but some system still use IPv4.



Translation from IPv4 to IPv6 (cont’d)

□ **Header translation**



Header Translation Procedure

1. The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2. The value of the IPv6 priority field is discarded.
3. Set the type of service field in IPv4 to zero.
4. The checksum for IPv4 is calculated and inserted in the corresponding field.
5. The IPv6 flow label is ignored.
6. Compatible extension headers are converted to options and inserted in the IPv4 header.
7. The length of IPv4 header is calculated and inserted into the corresponding field.
8. The total length of the IPv4 packet is calculated and inserted in the corresponding field.