Chapter 27

Next Generation: IPv6 and ICMPv6

Objectives

Upon completion you will be able to:

- *Understand the shortcomings of IPv4*
- *Know the IPv6 address format, address types, and abbreviations*
- *Be familiar with the IPv6 header format*
- *Know the extension header types*
- *Know the differences between ICMPv4 and ICMPv6*
- *Know the strategies for transitioning from IPv4 to IPv6*

27.1 IPv6

IPv6 has these advantages over IPv4:

1. *larger address space*
2. *better header format*
3. *new options*
4. *allowance for extension*
5. *support for resource allocation*
6. *support for more security*

The topics discussed in this section include:

IPv6 Addresses
Address Space Assignment
Packet Format
Comparison between IPv4 and IPv6

Figure 27.1 *IPv6 address*

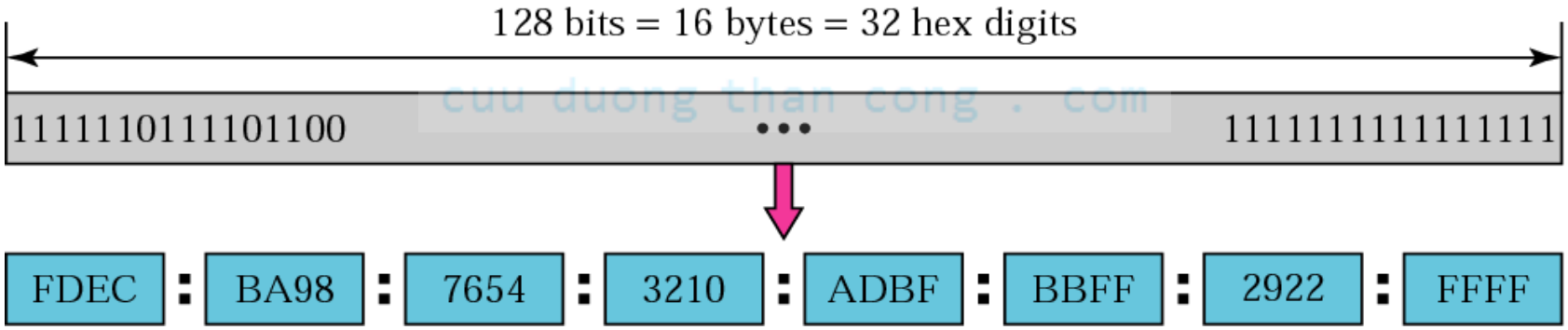


Figure 27.2 *Abbreviated address*

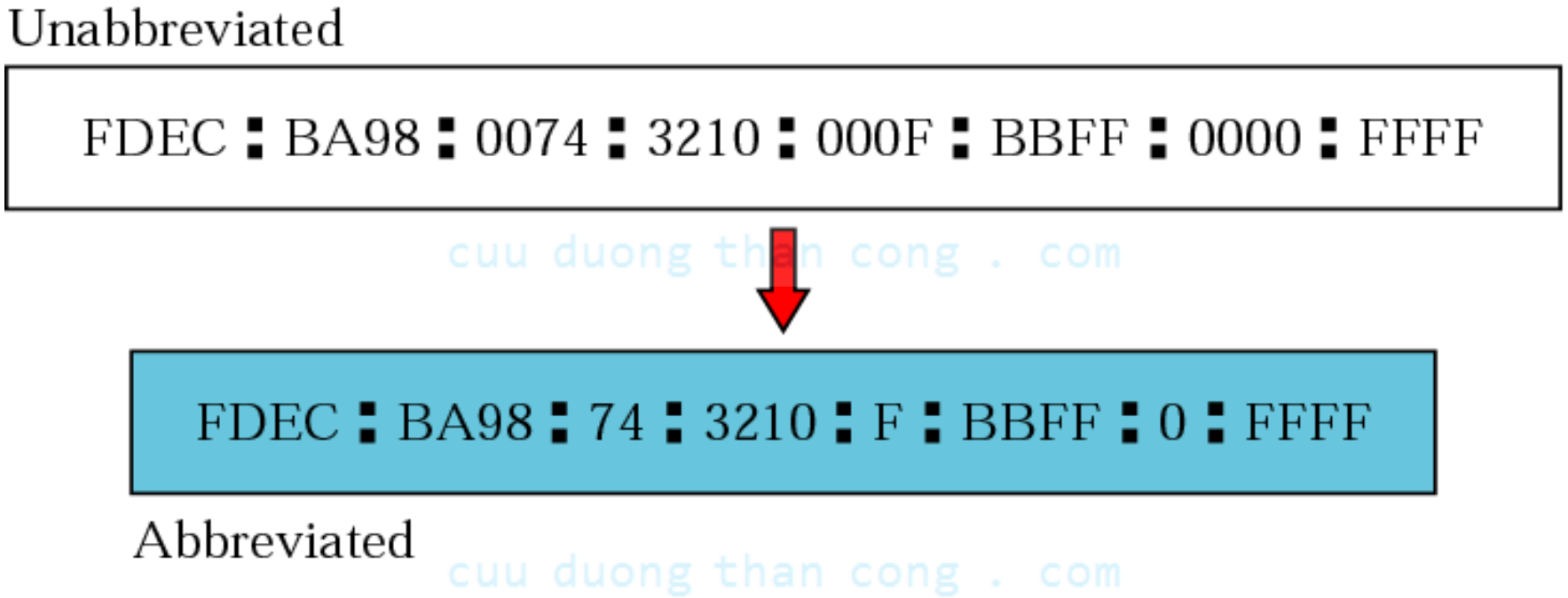


Figure 27.3 *Abbreviated address with consecutive zeros*

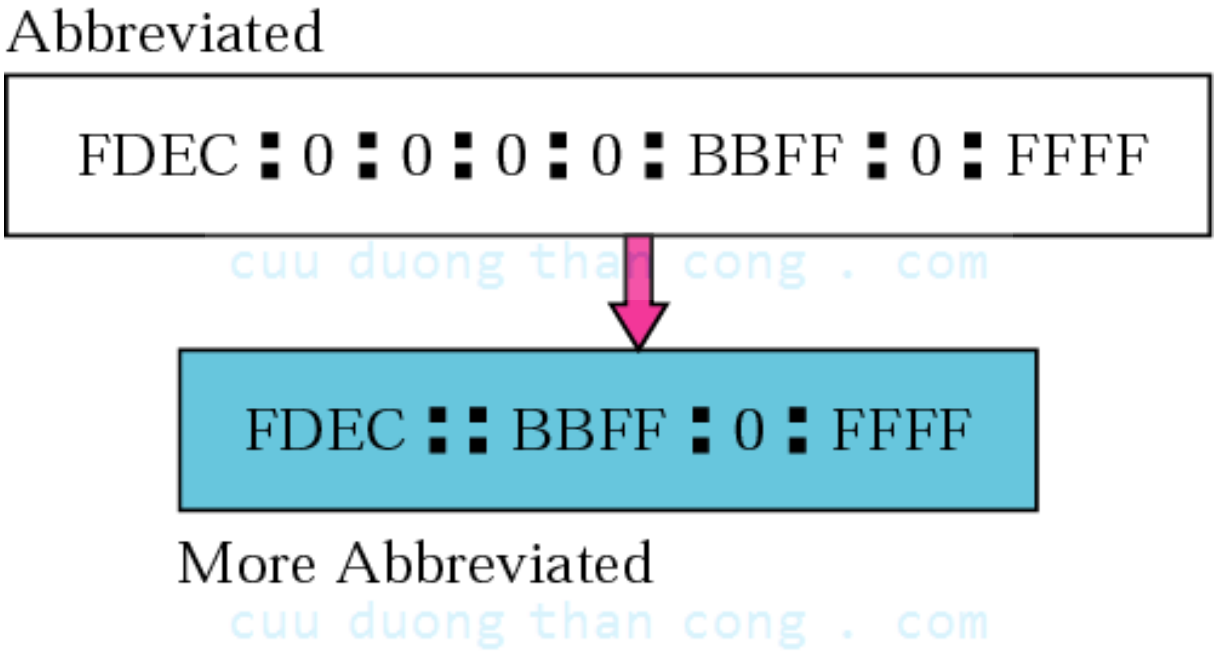


Figure 27.4 *CIDR address*

FDEC : : BBFF : 0 : FFFF/60

Figure 27.5 *Address structure*

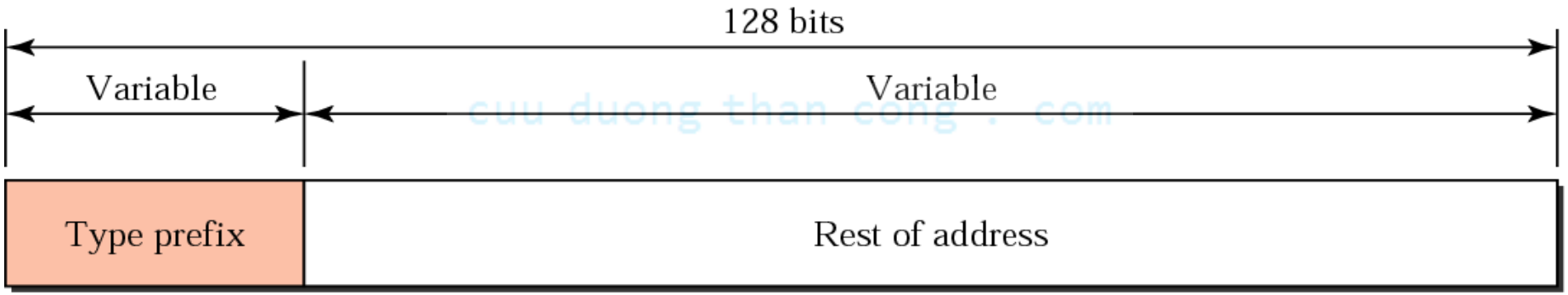


Table 27.1 Type prefixes for IPv6 addresses

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

Figure 27.6 *Provider-based address*

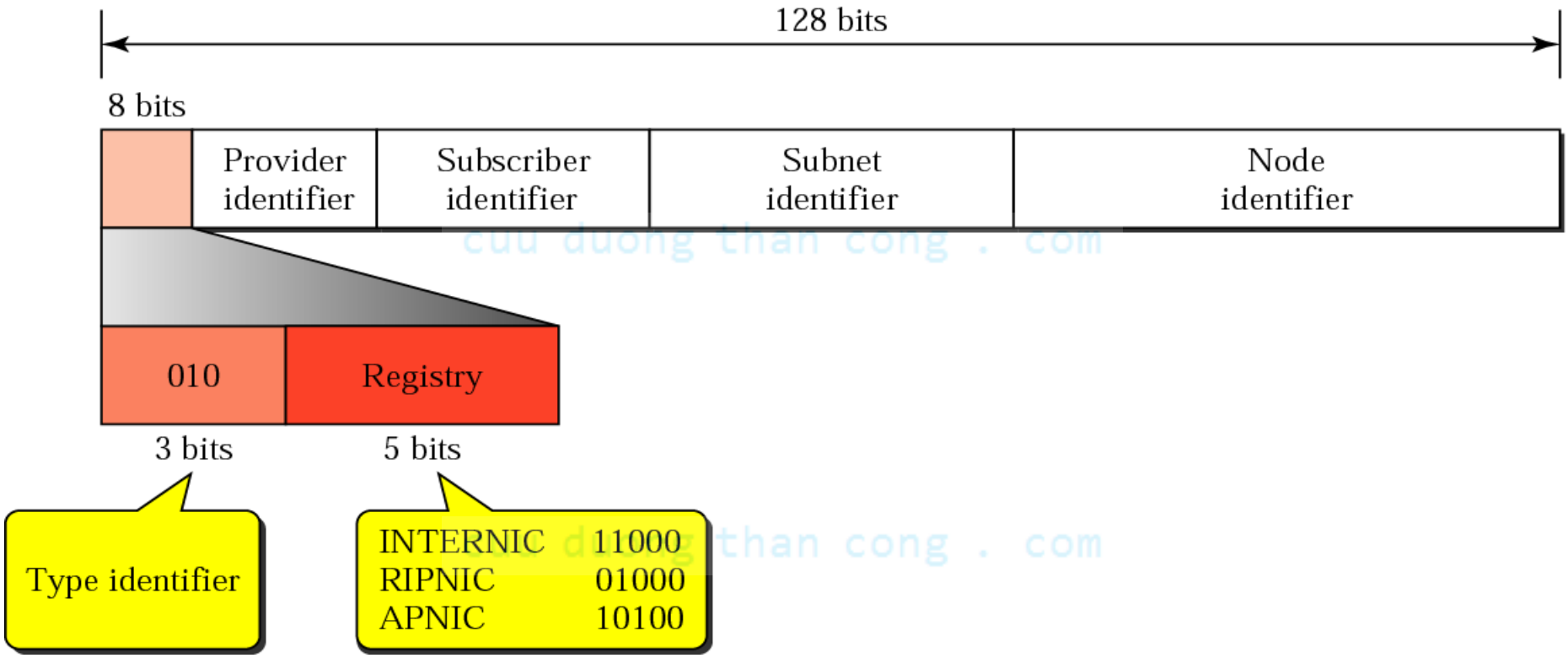


Figure 27.7 *Address hierarchy*

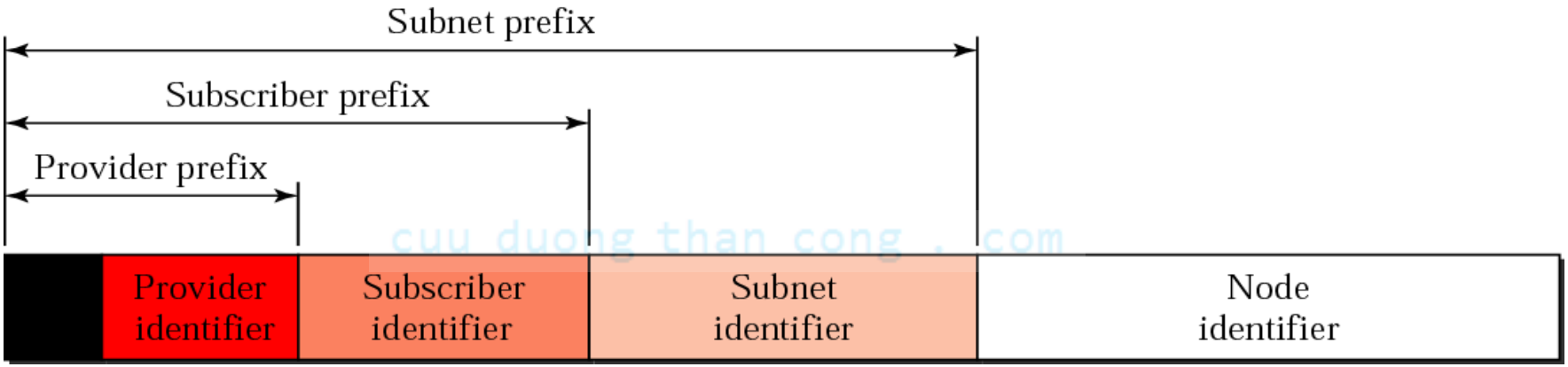


Figure 27.8 *Unspecified address*

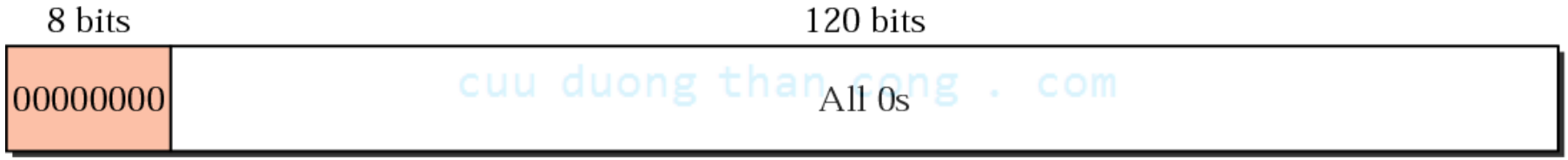


Figure 27.9 *Loopback address*

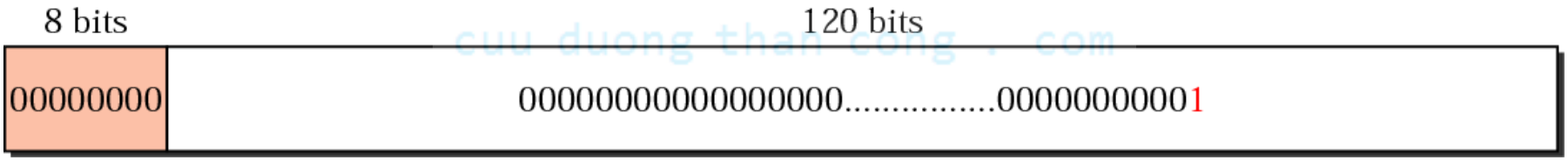


Figure 27.10 *Compatible address*

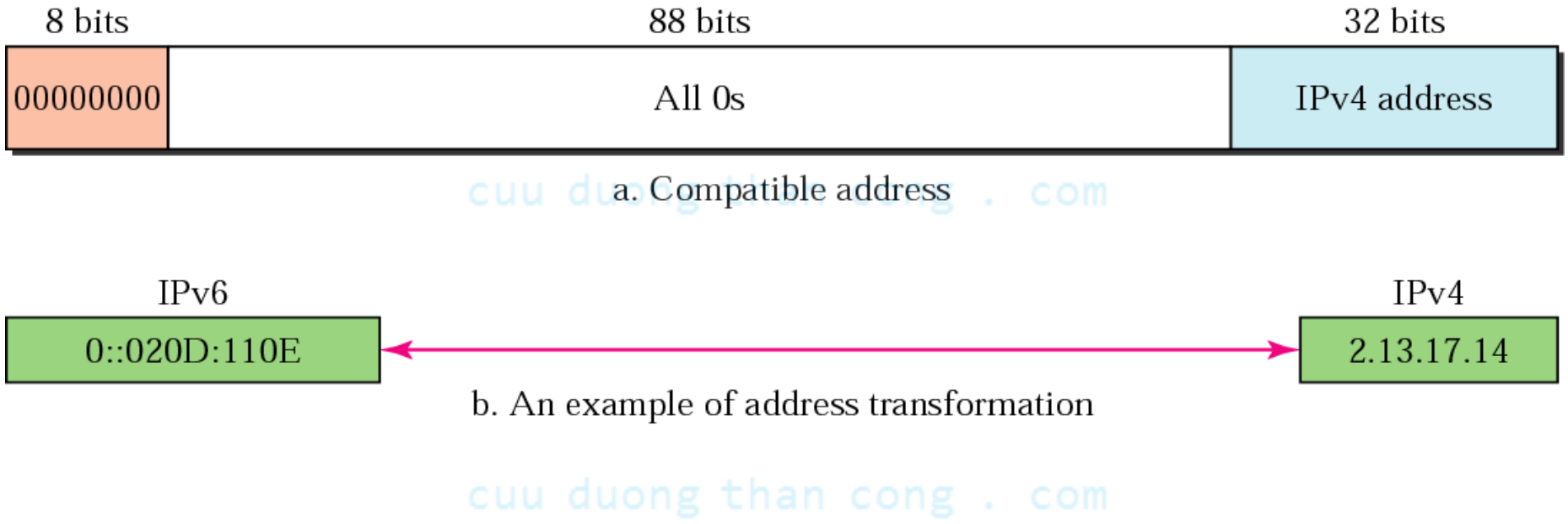


Figure 27.11 *Mapped address*

a. Mapped address

b. An example of address transformation

Figure 27.12 *Link local address*

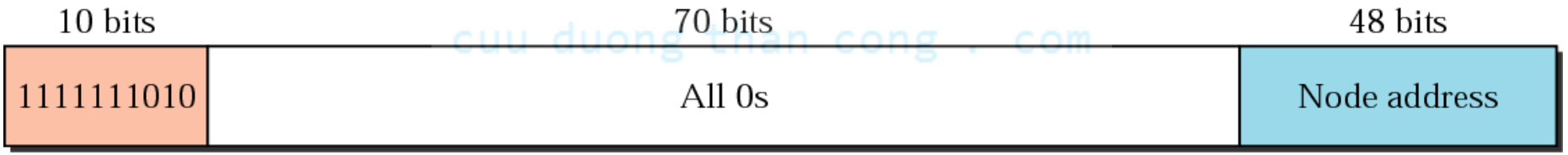


Figure 27.13 *Site local address*

Figure 27.14 *Multicast address*

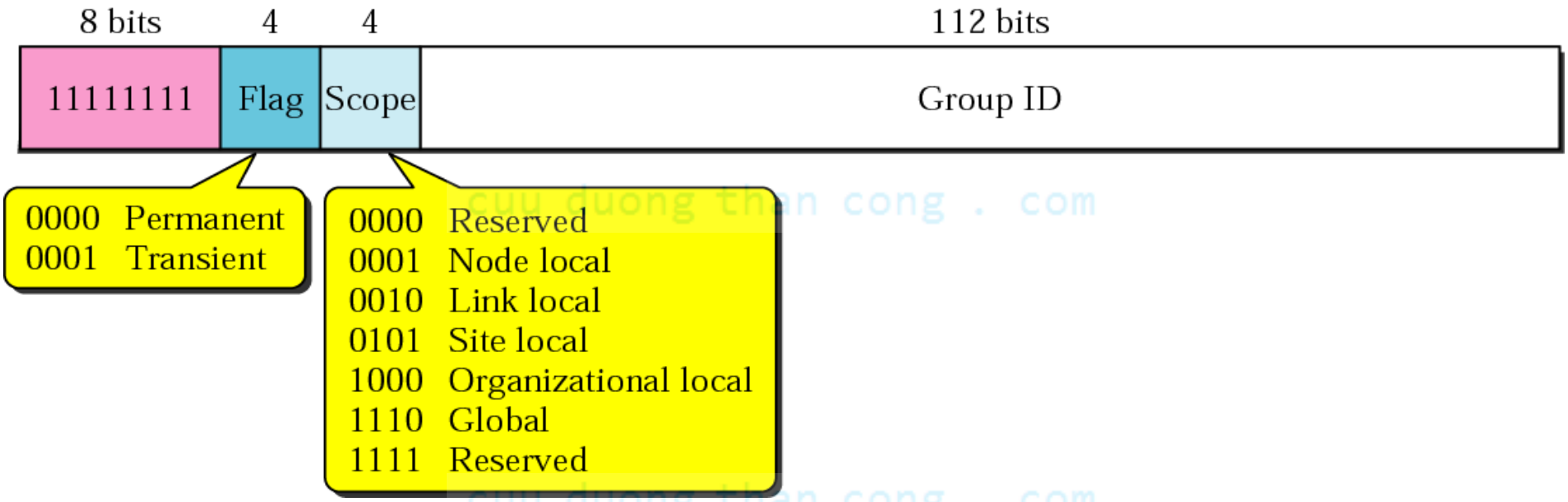


Figure 27.15 *IPv6 datagram*

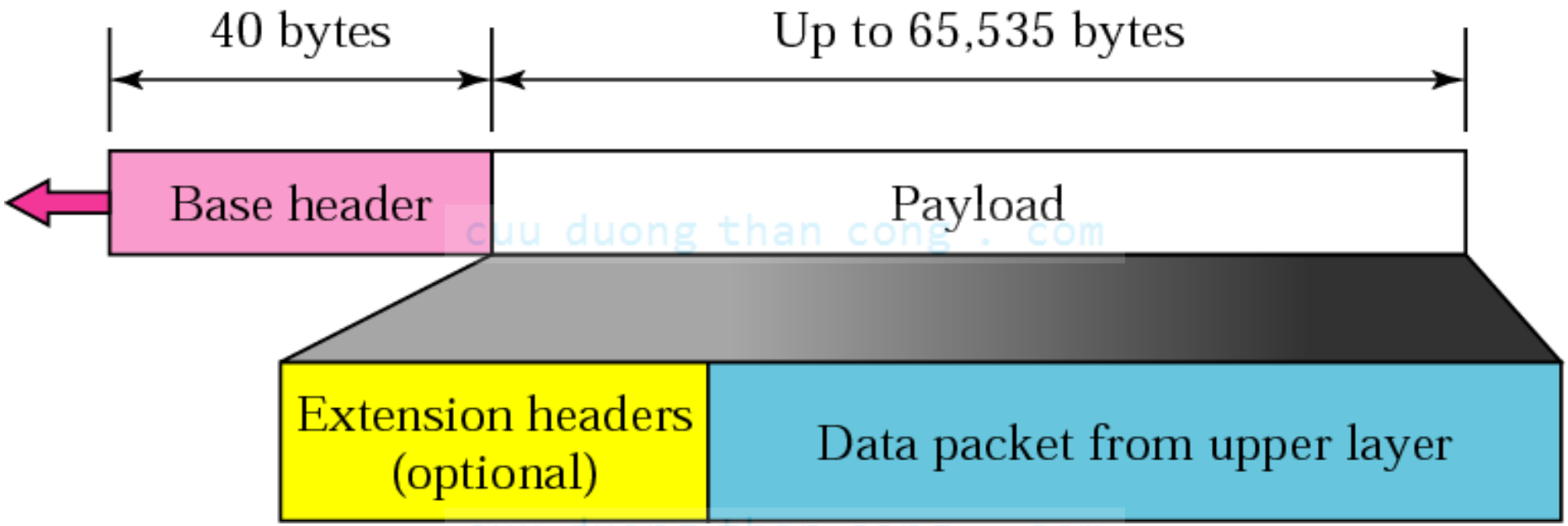


Figure 27.16 *Format of an IPv6 datagram*

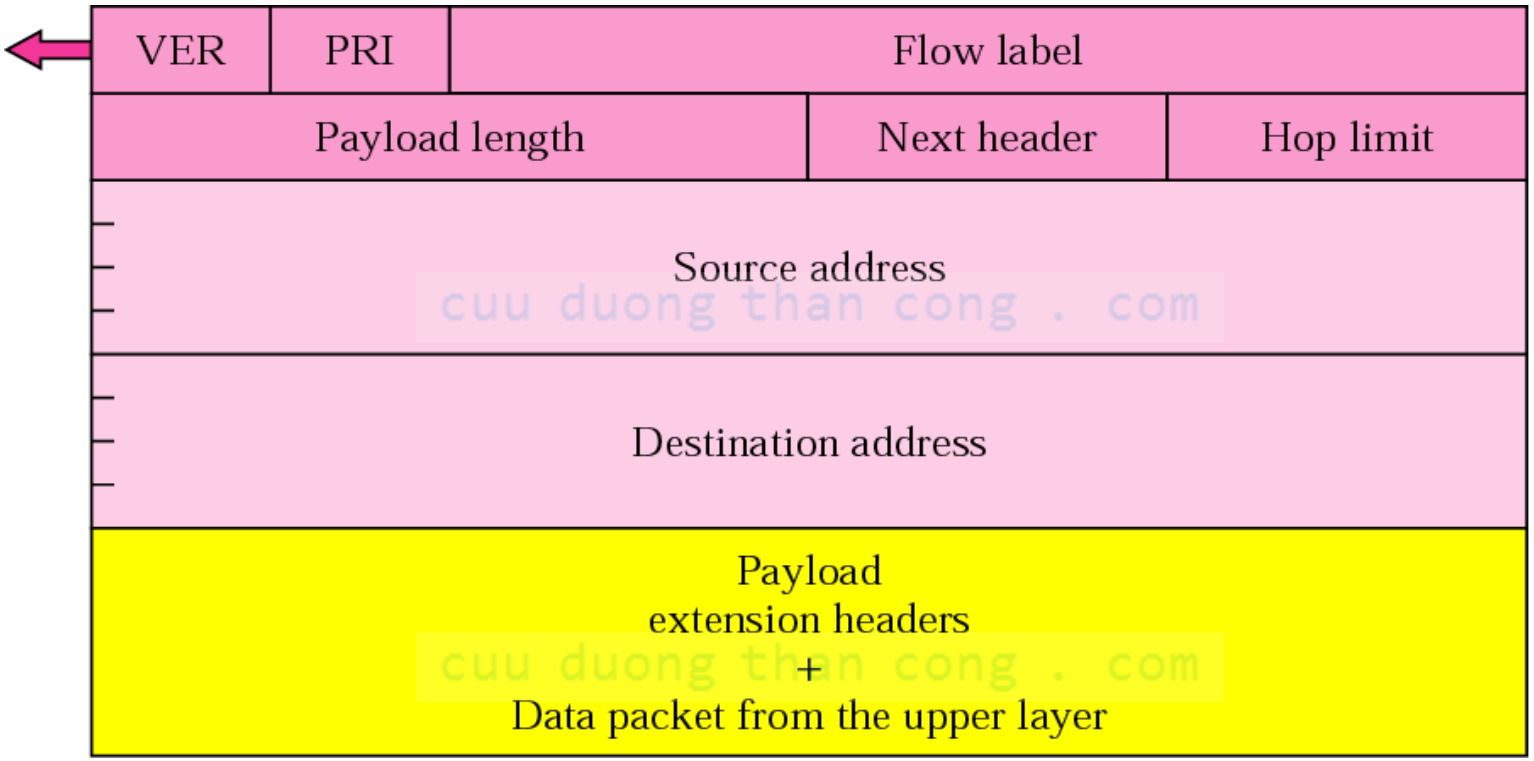


Table 27.2 *Next header codes*

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

Table 27.3 *Priorities for congestion-controlled traffic*

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

Table 27.4 *Priorities for noncongestion-controlled traffic*

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

Table 27.5 Comparison between IPv4 and IPv6 packet header

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 27.17 *Extension header format*

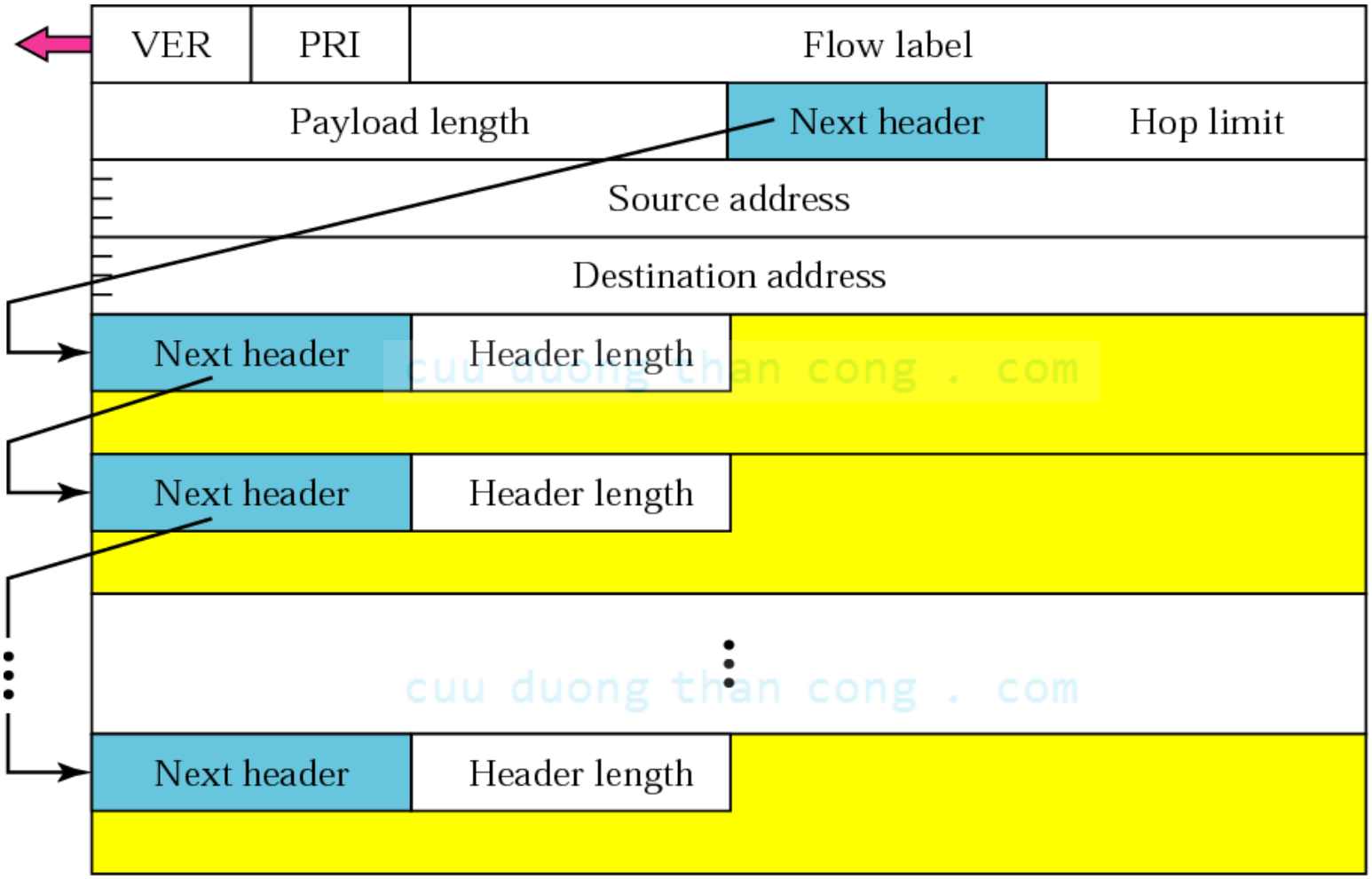


Figure 27.18 *Extension header types*

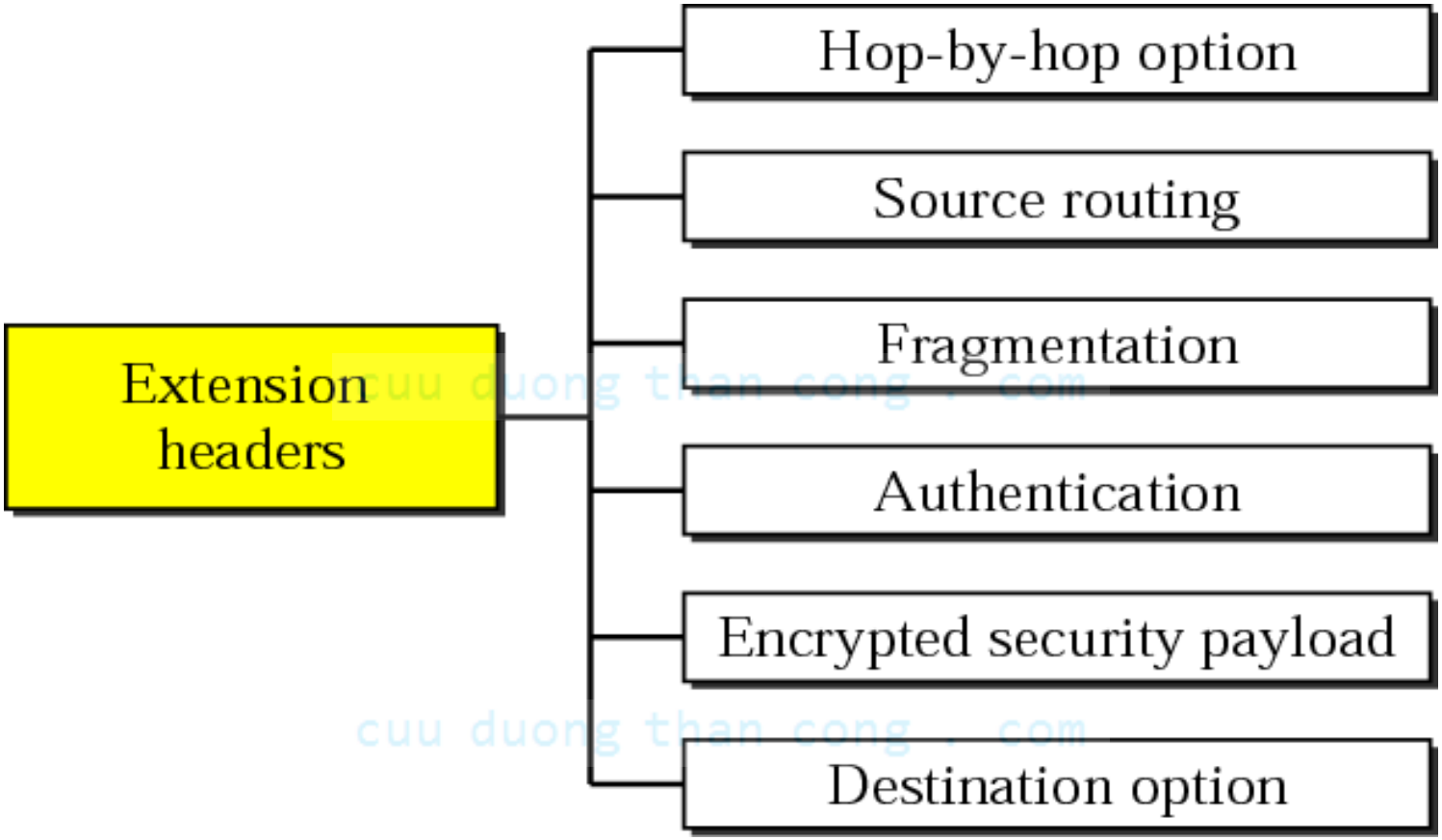


Figure 27.19 *Hop-by-hop option header format*

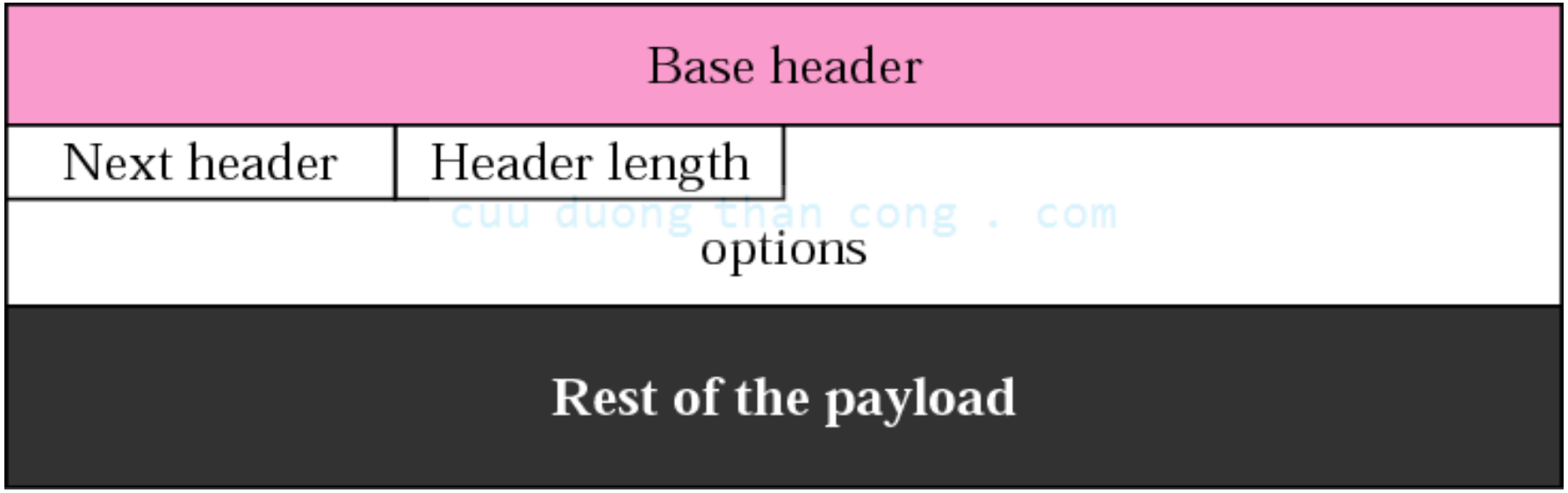
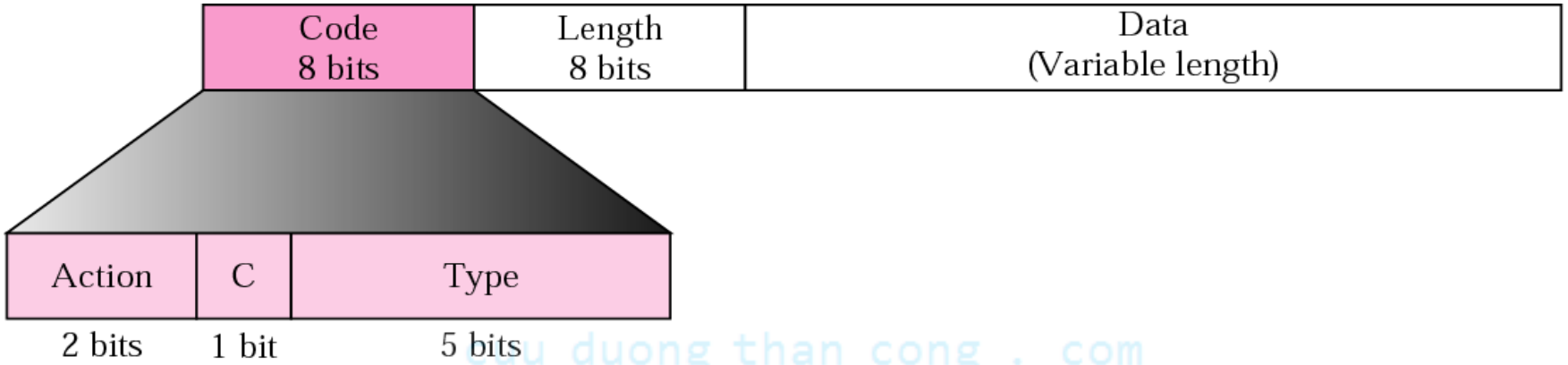


Figure 27.20 *The format of options in a hop-by-hop option header*



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

Type

00000 Pad1
00001 PadN
00010 Jumbo payload

C: Change in option value

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

Figure 27.21 *Pad1*

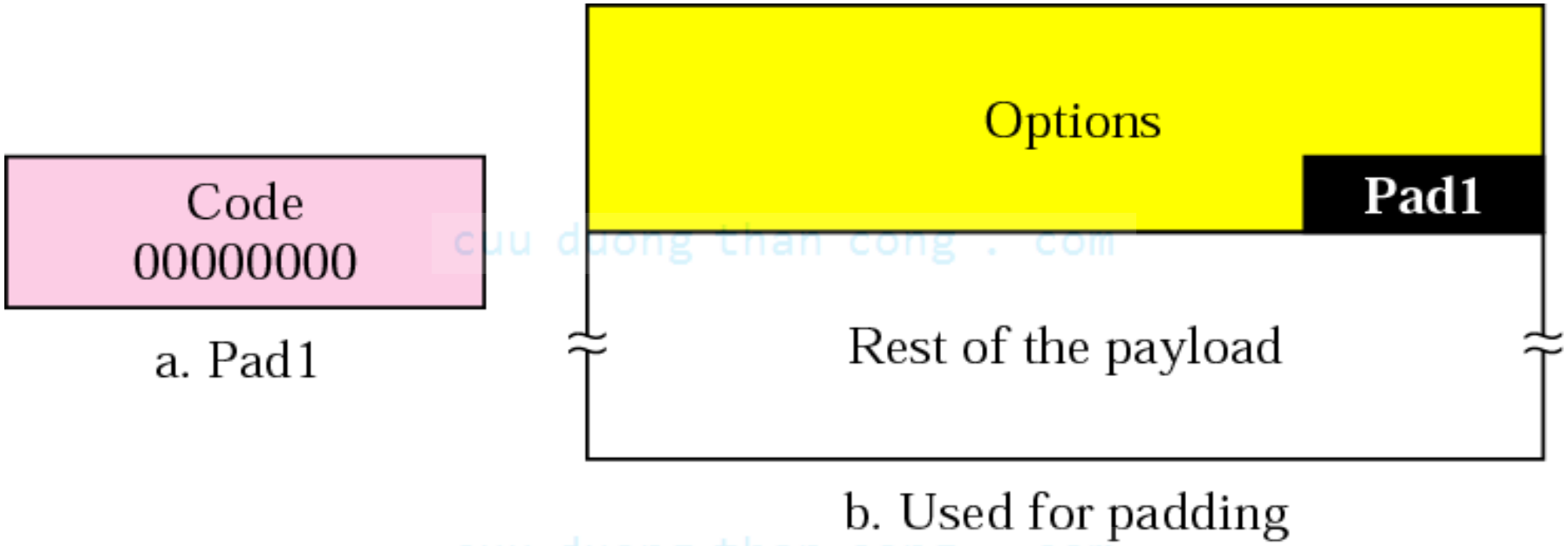


Figure 27.22 *PadN*

Figure 27.23 *Jumbo payload*

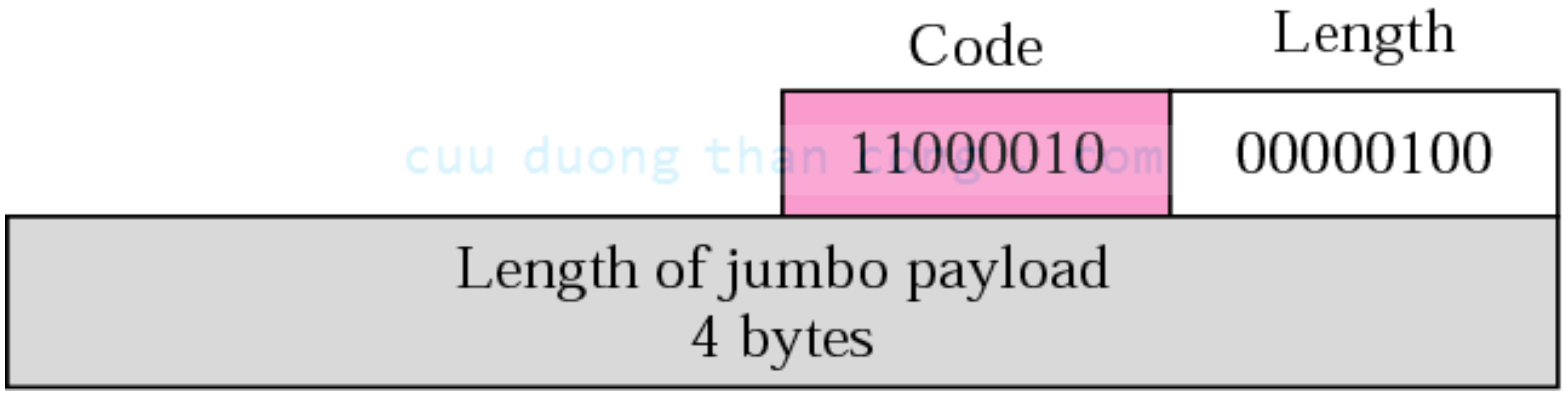


Figure 27.24 *Source routing*

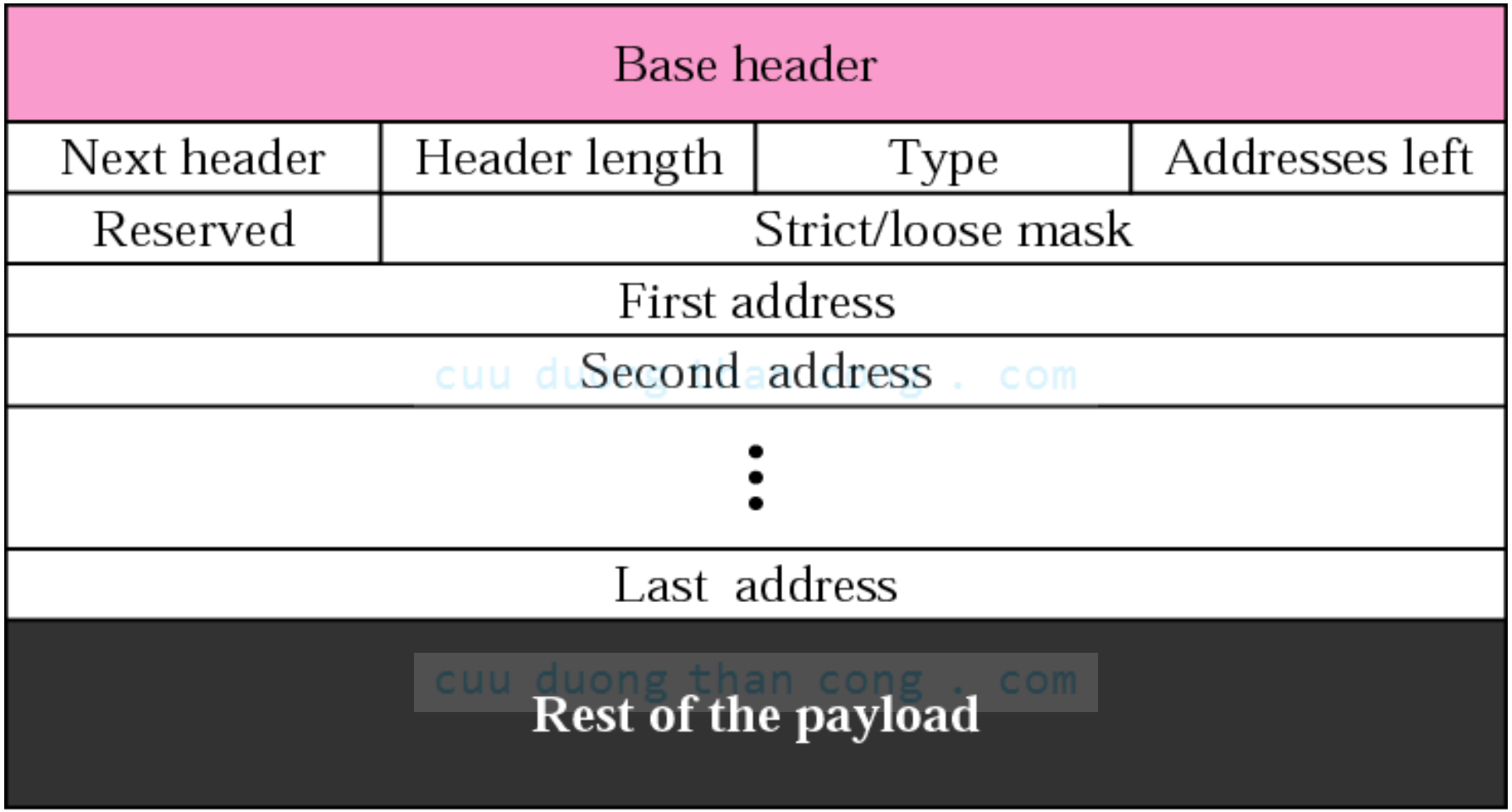


Figure 27.25 *Source routing example*

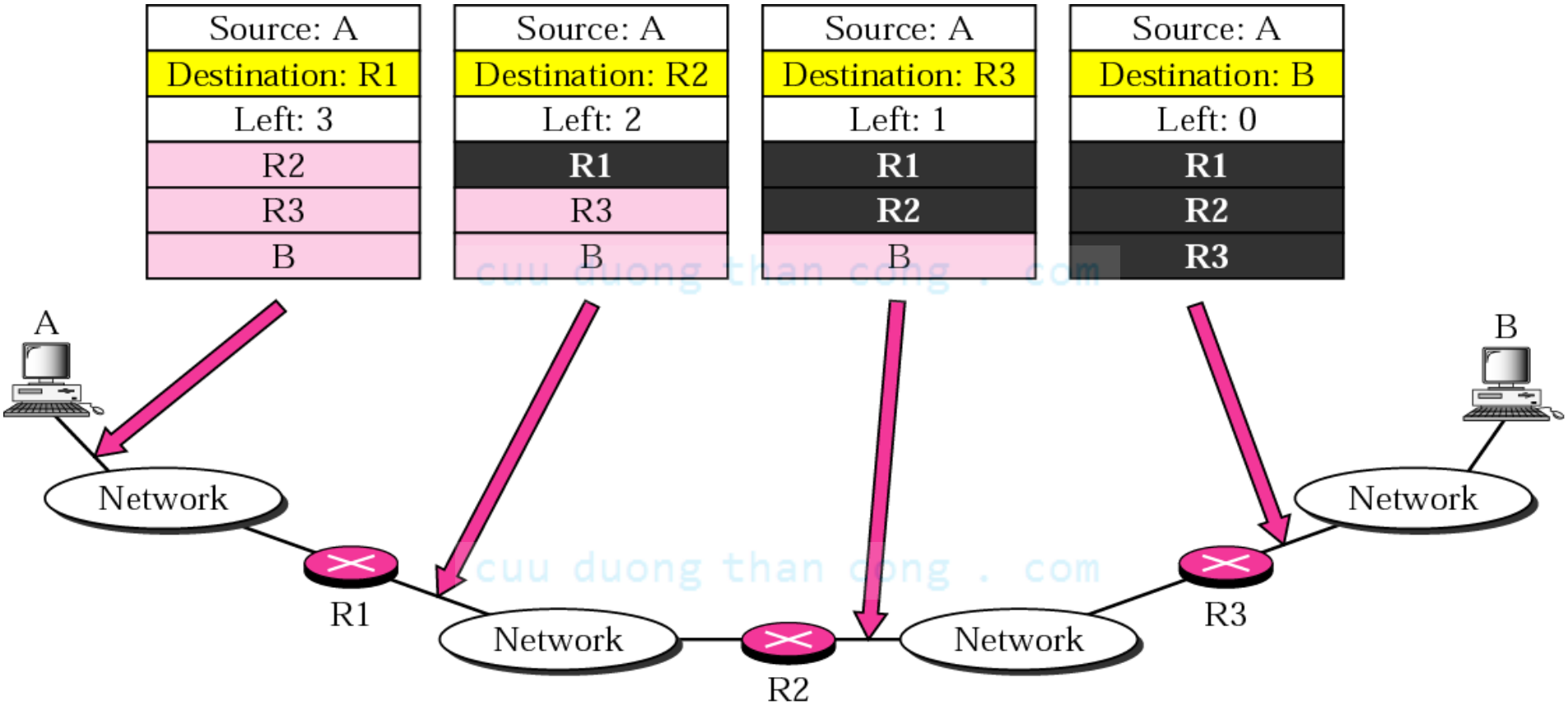


Figure 27.26 *Fragmentation*

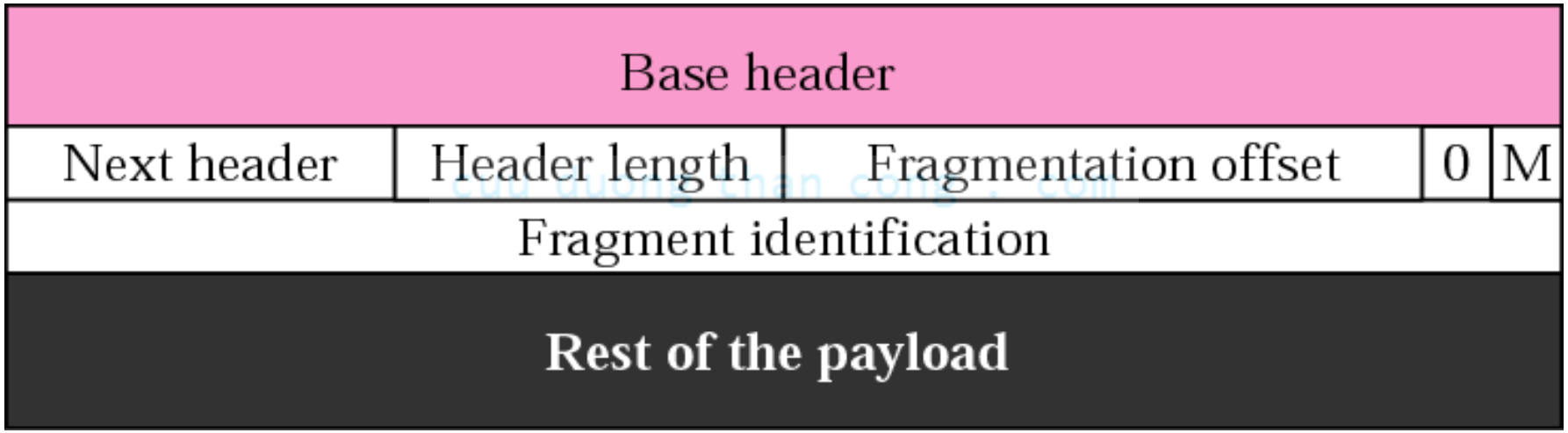


Figure 27.27 *Authentication*

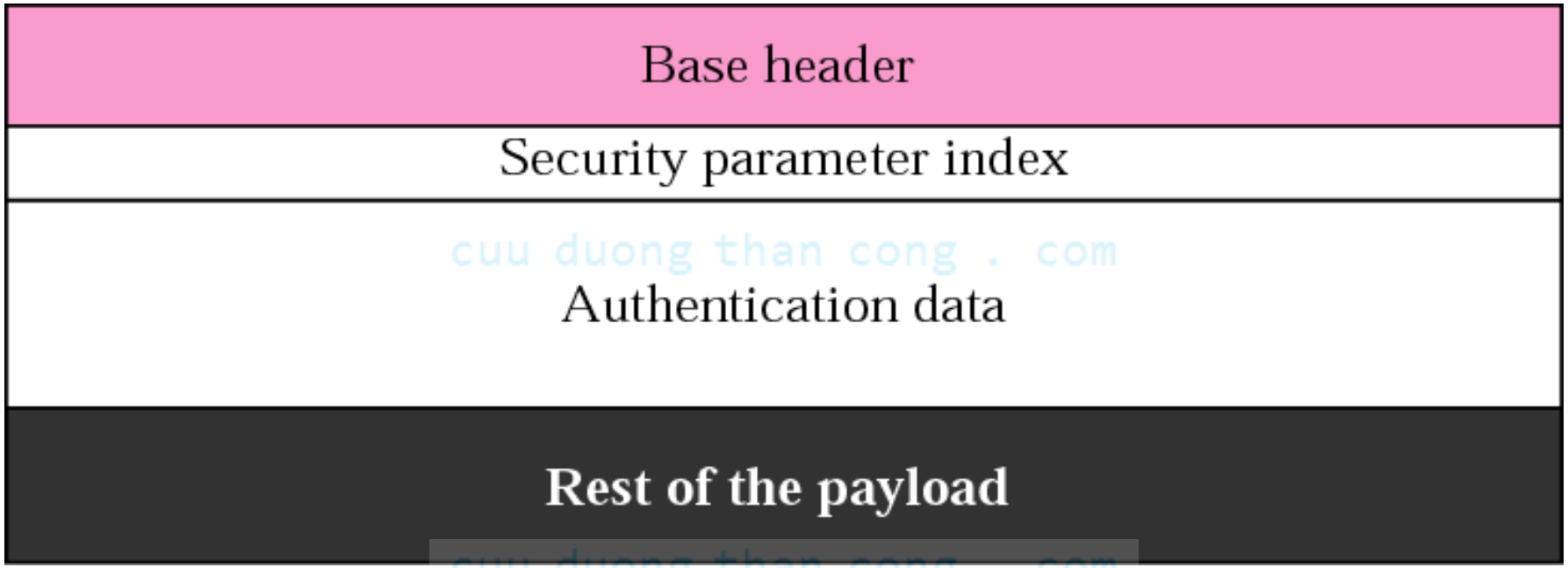


Figure 27.28 *Calculation of authentication data*

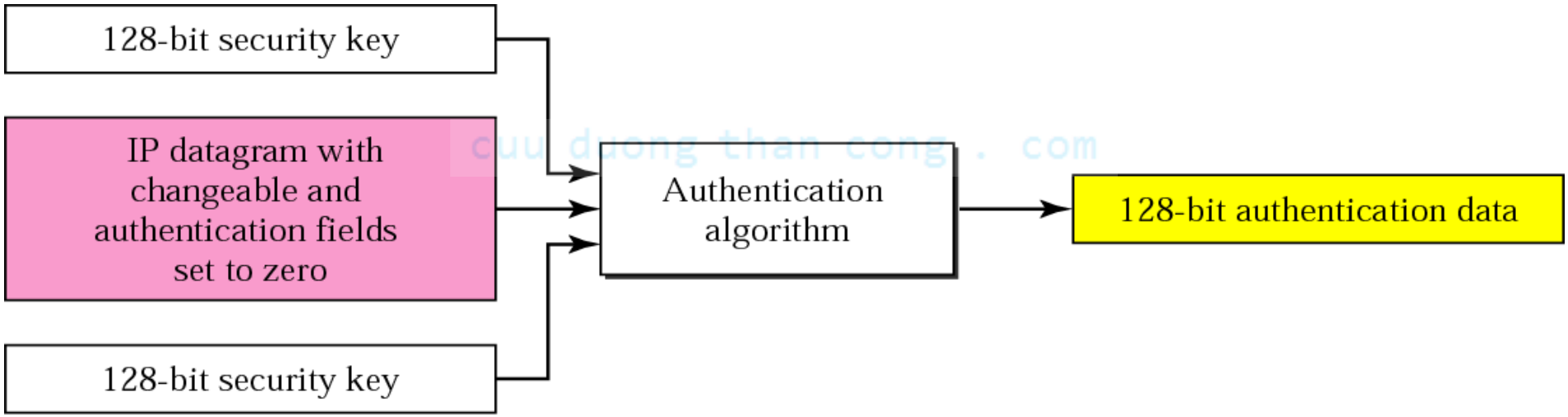


Figure 27.29 *Encrypted security payload*

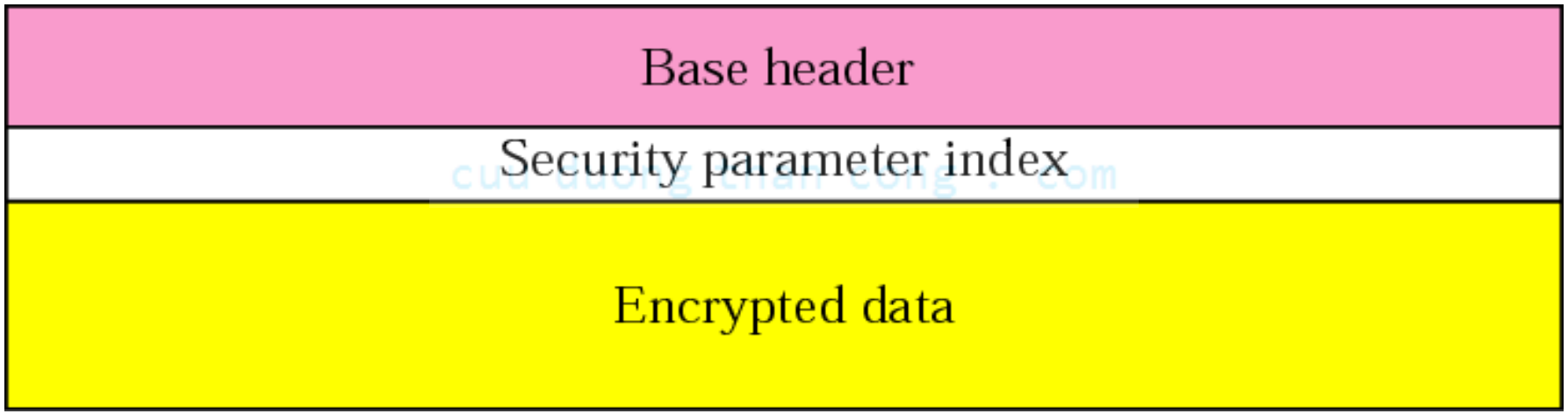


Figure 27.30 *Transport mode encryption*

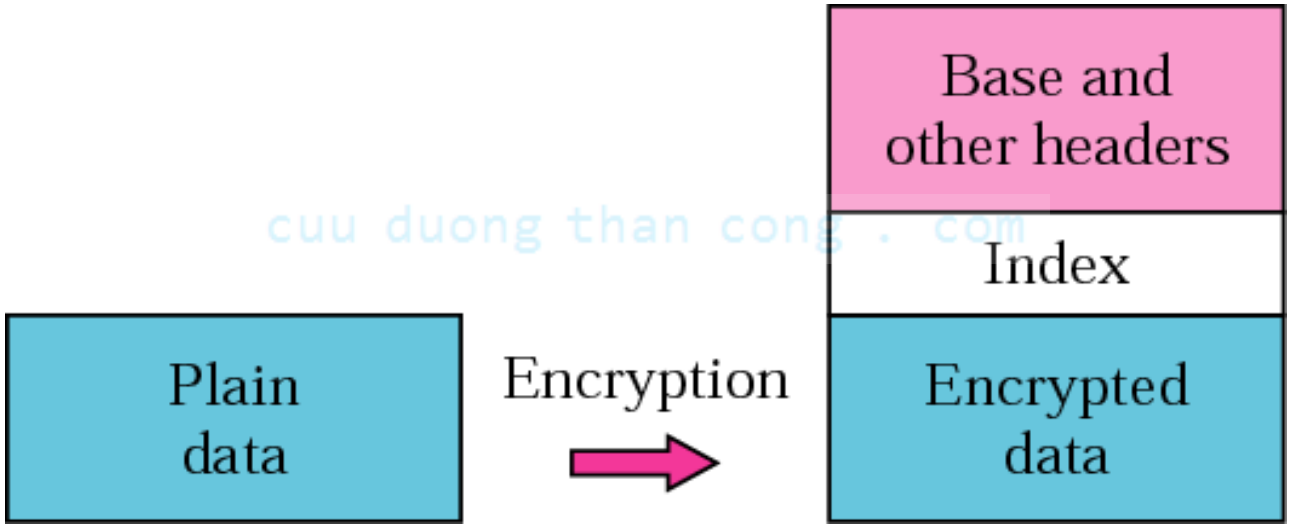


Figure 27.31 *Tunnel-mode encryption*

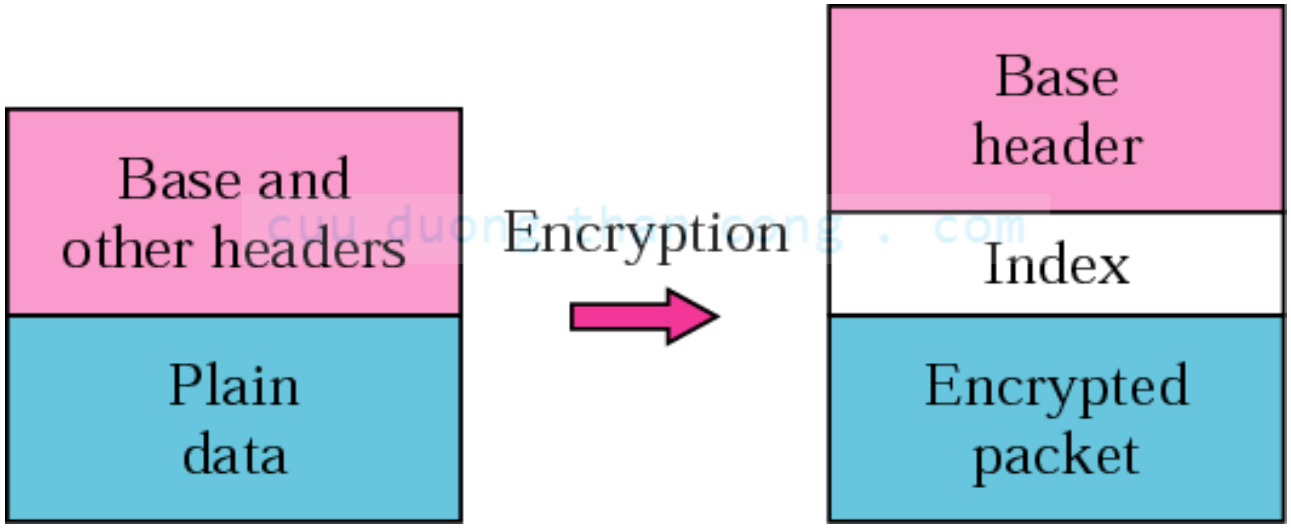


Table 27.6 Comparison between IPv4 options and IPv6 extension headers

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.

27.2 ICMPv6

ICMPv6, while similar in strategy to ICMPv4, has changes that makes it more suitable for IPv6. ICMPv6 has absorbed some protocols that were independent in version 4.

The topics discussed in this section include:

Error Reporting
Query

Figure 27.32 *Comparison of network layers in version 4 and version 6*

Network layer in version 4

Network layer in version 6

Figure 27.33 *Categories of ICMPv6 messages*

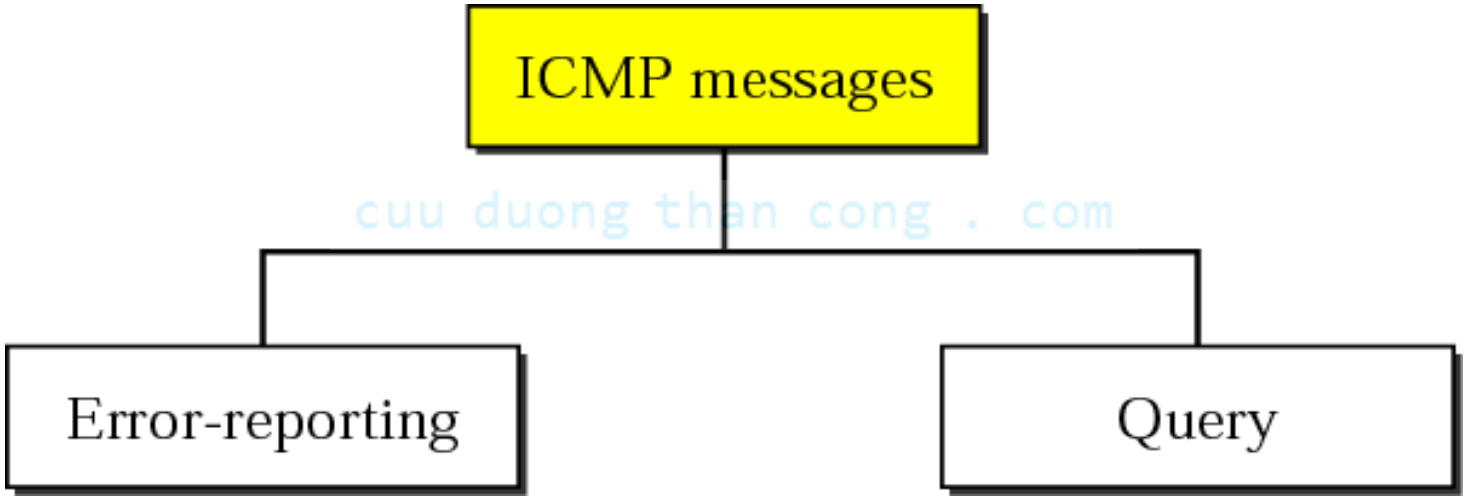


Figure 27.34 *General format of ICMP messages*

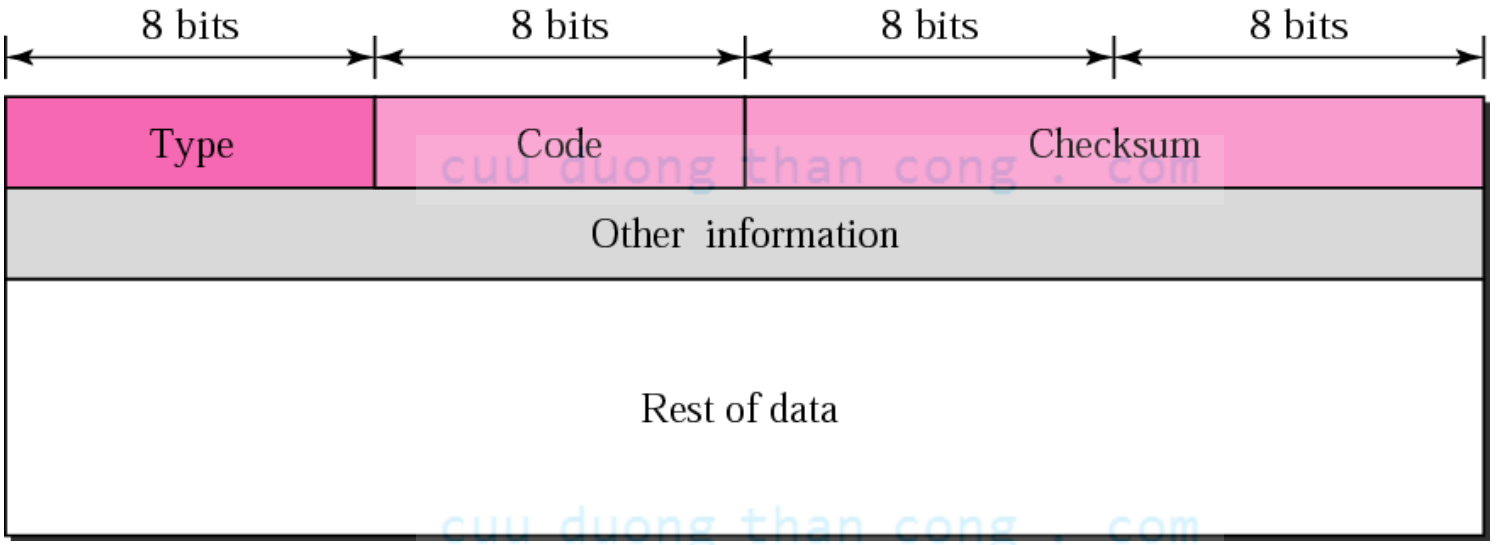


Figure 27.35 *Error-reporting messages*

Table 27.7 Comparison of error-reporting messages in ICMPv4 and ICMPv6

Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes

Figure 27.36 *Destination-unreachable message format*

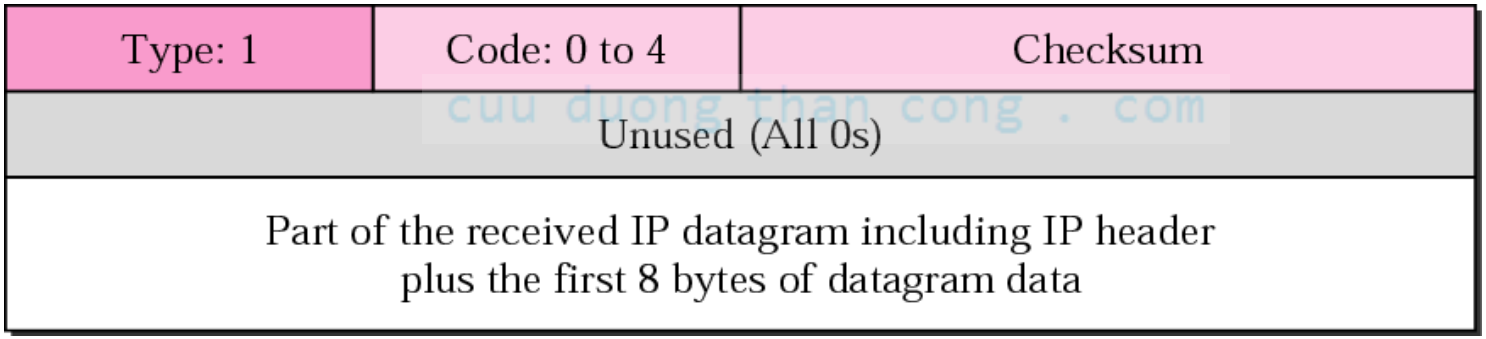


Figure 27.37 *Packet-too-big message format*

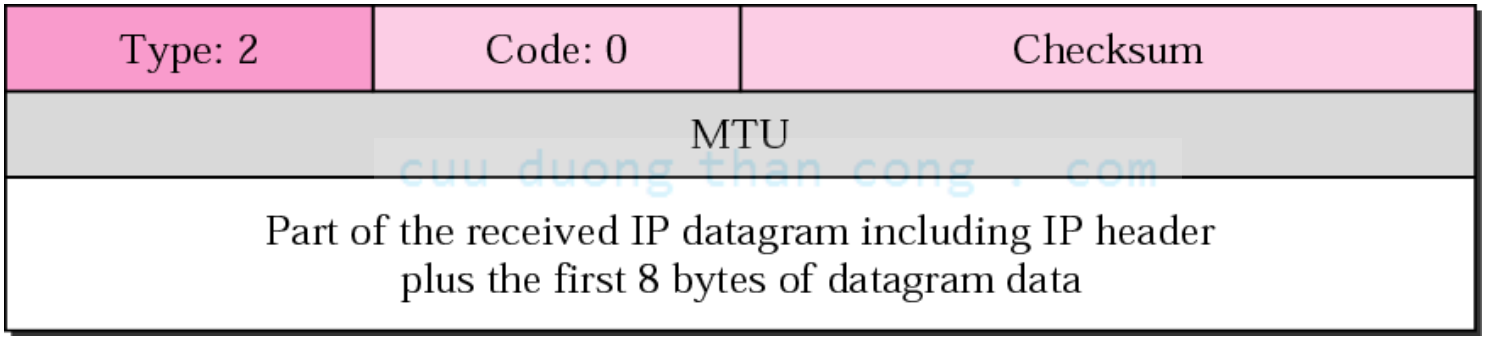


Figure 27.38 *Time-exceeded message format*

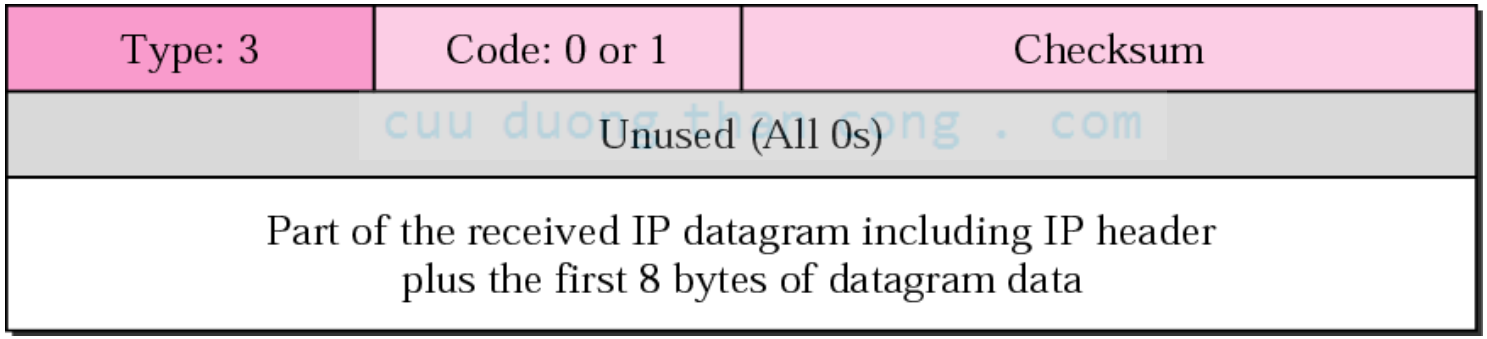


Figure 27.39 *Parameter-problem message format*

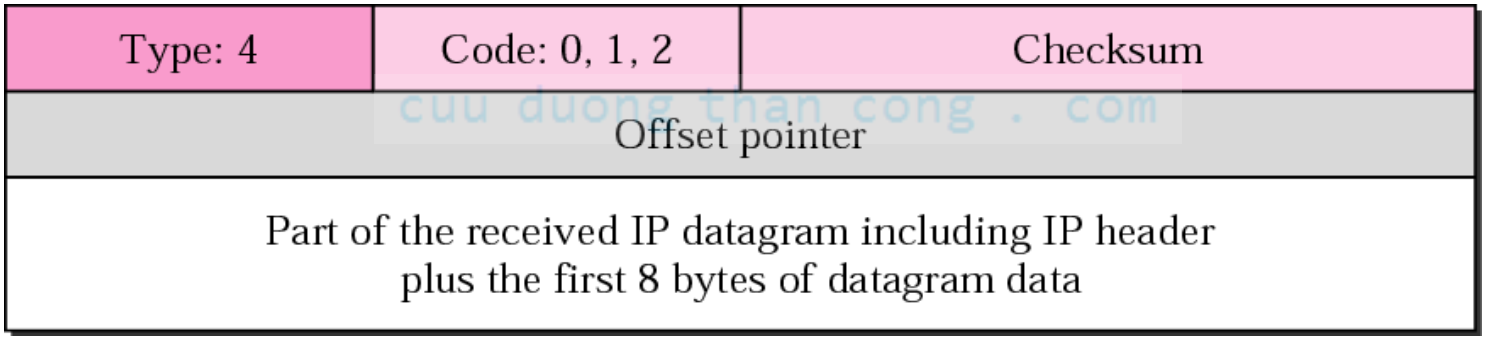


Figure 27.40 *Redirection message format*

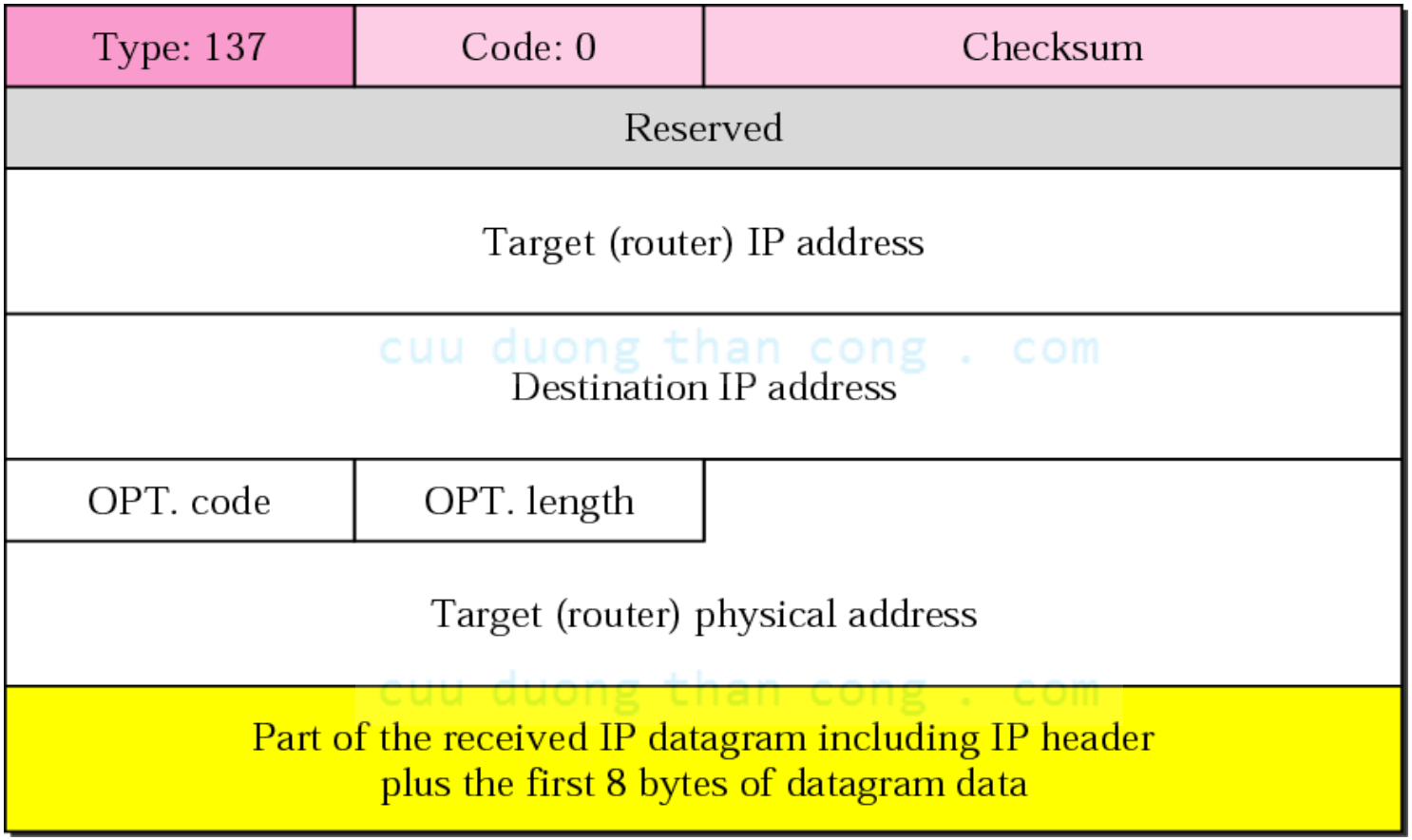


Figure 27.41 *Query messages*

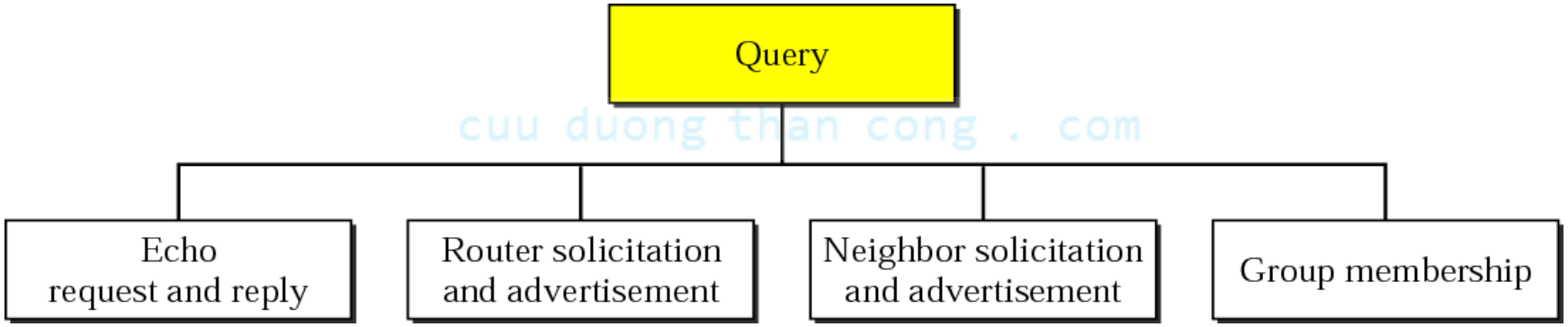


Table 27.8 Comparison of query messages in ICMPv4 and ICMPv6

Type of Message	*Version 4*	*Version 6*
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes

Figure 27.42 *Echo request and reply messages*

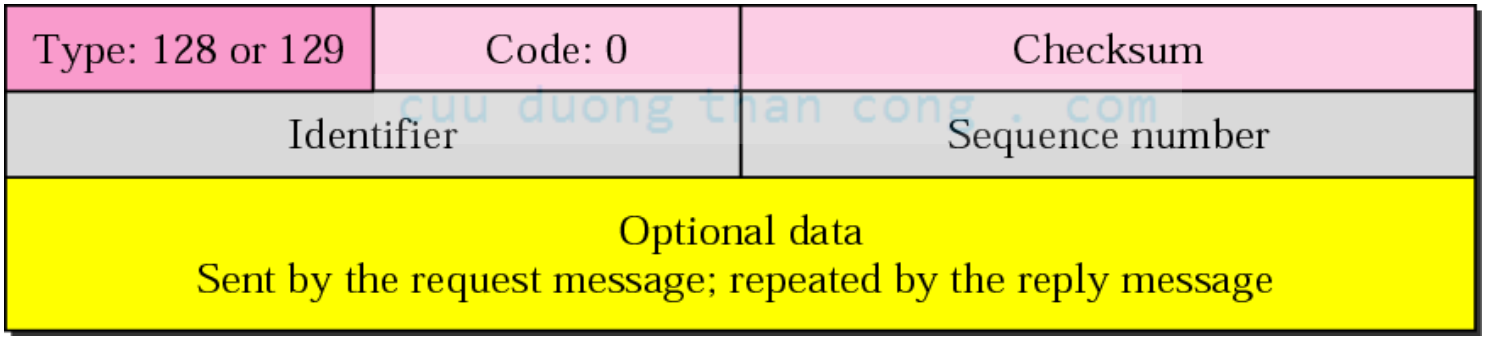
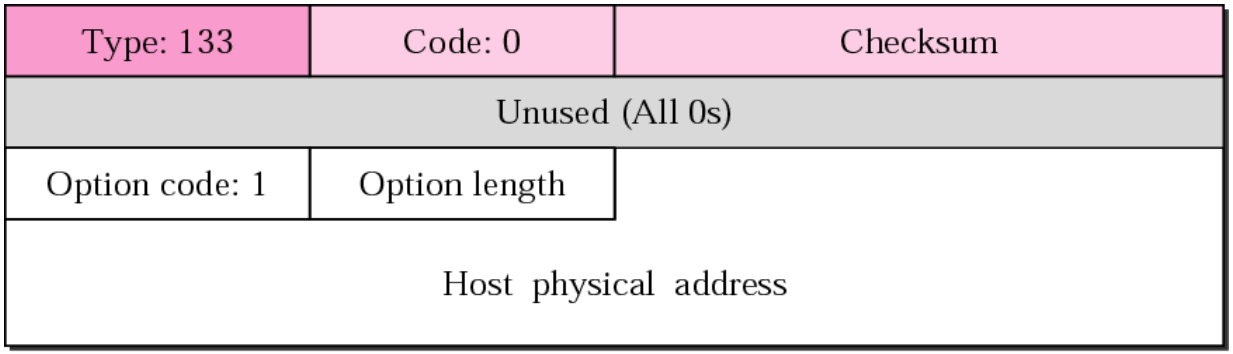
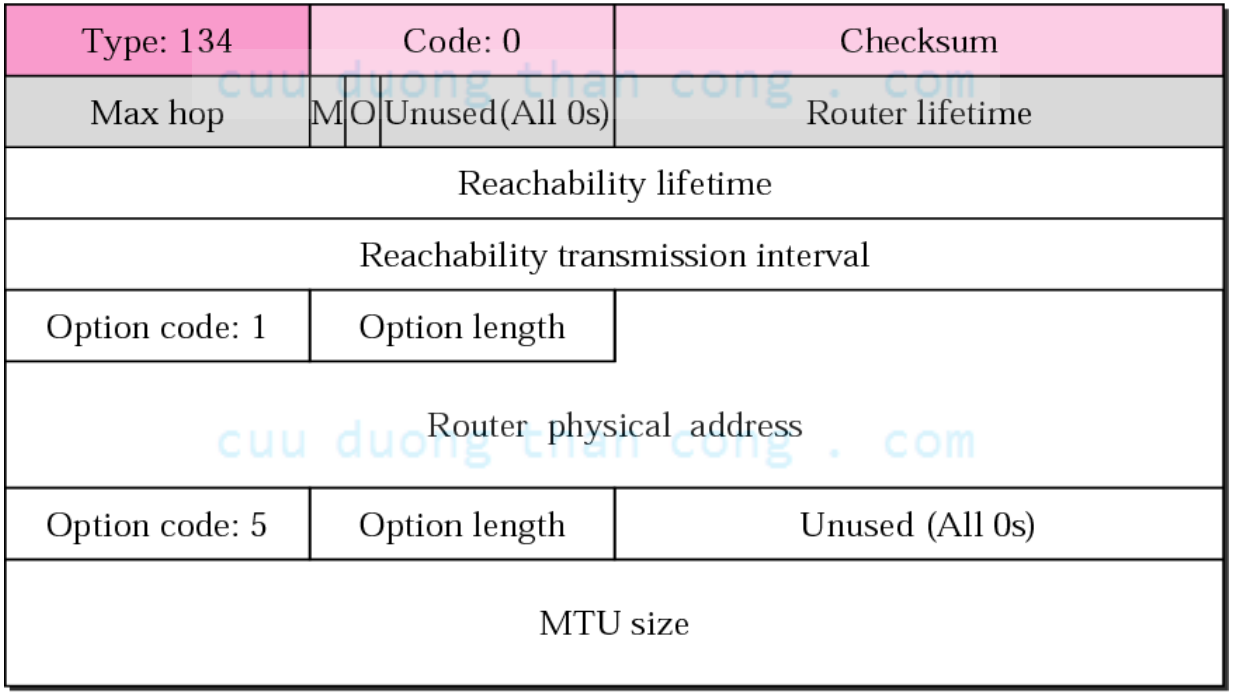


Figure 27.43 *Router-solicitation and advertisement message formats*

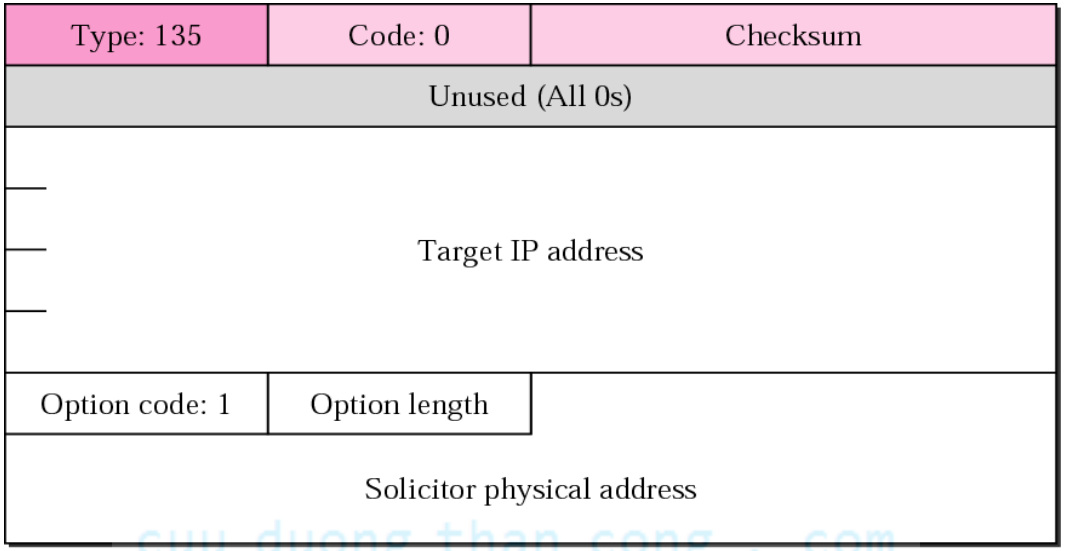


a. Router solicitation format

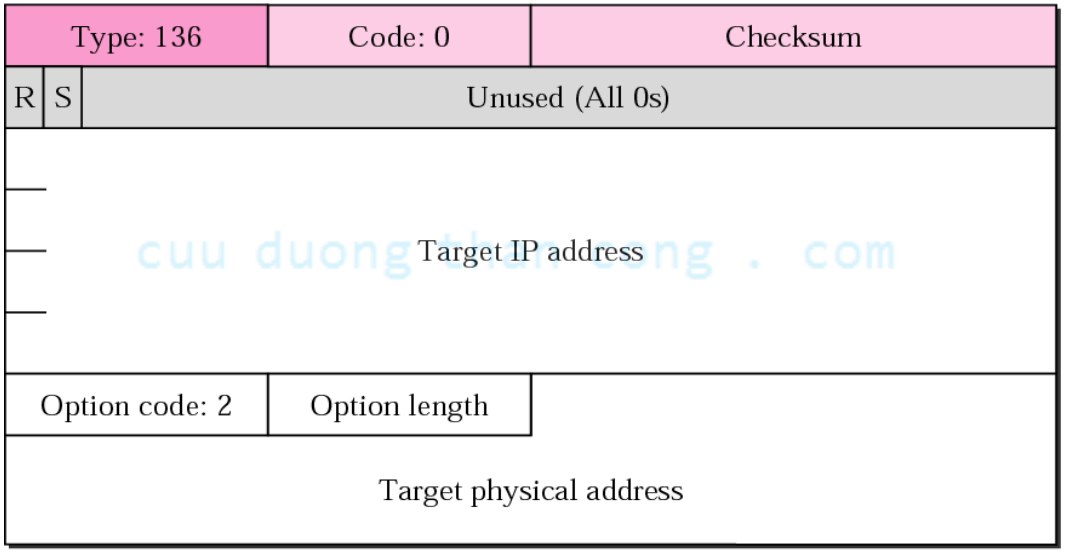


b. Router advertisement format

Figure 27.44 *Neighbor-solicitation and advertisement message formats*



a. Neighbor solicitation



b. Neighbor advertisement

Figure 27.45 *Group-membership messages*

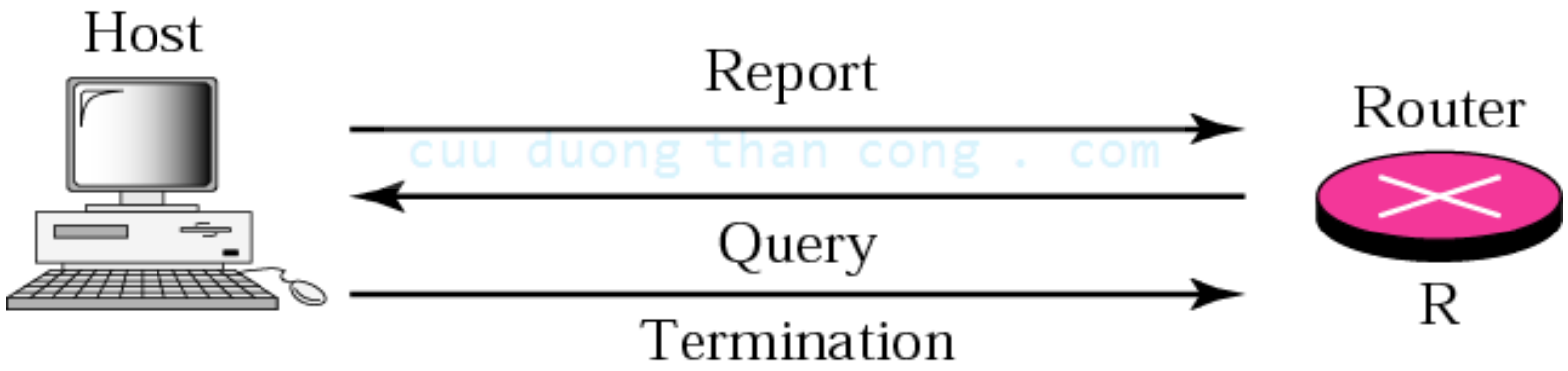
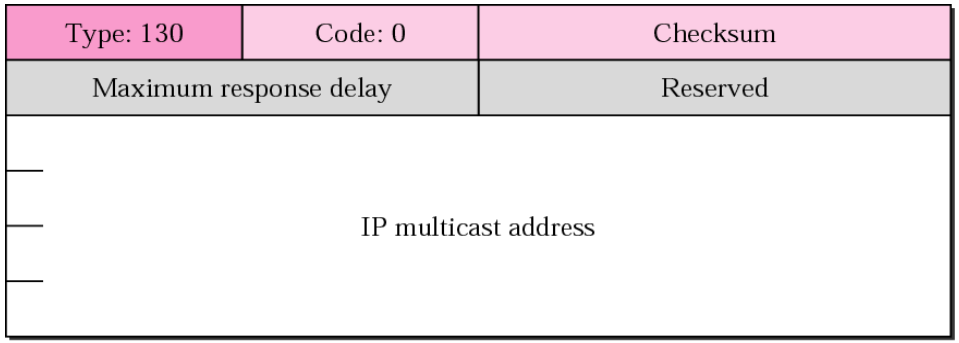
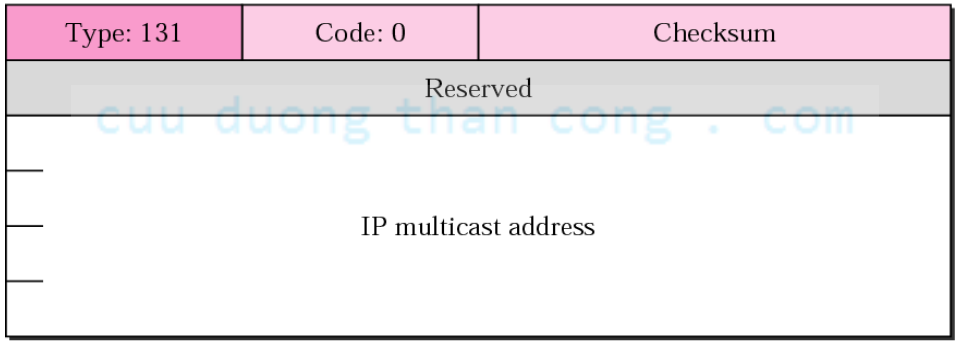


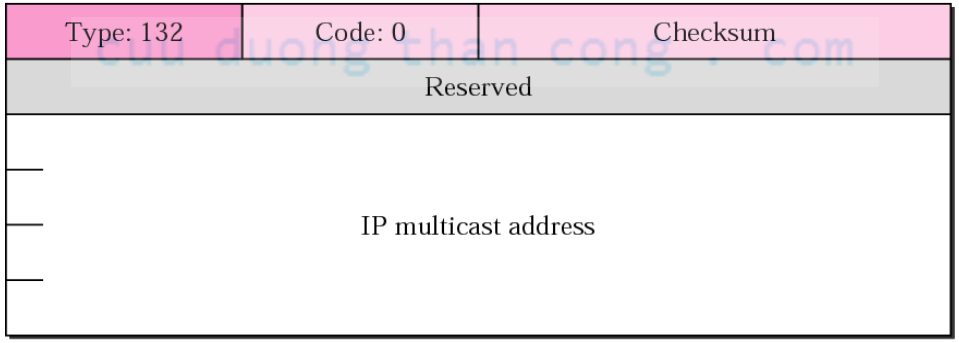
Figure 27.46 *Group-membership message formats*



a. Query

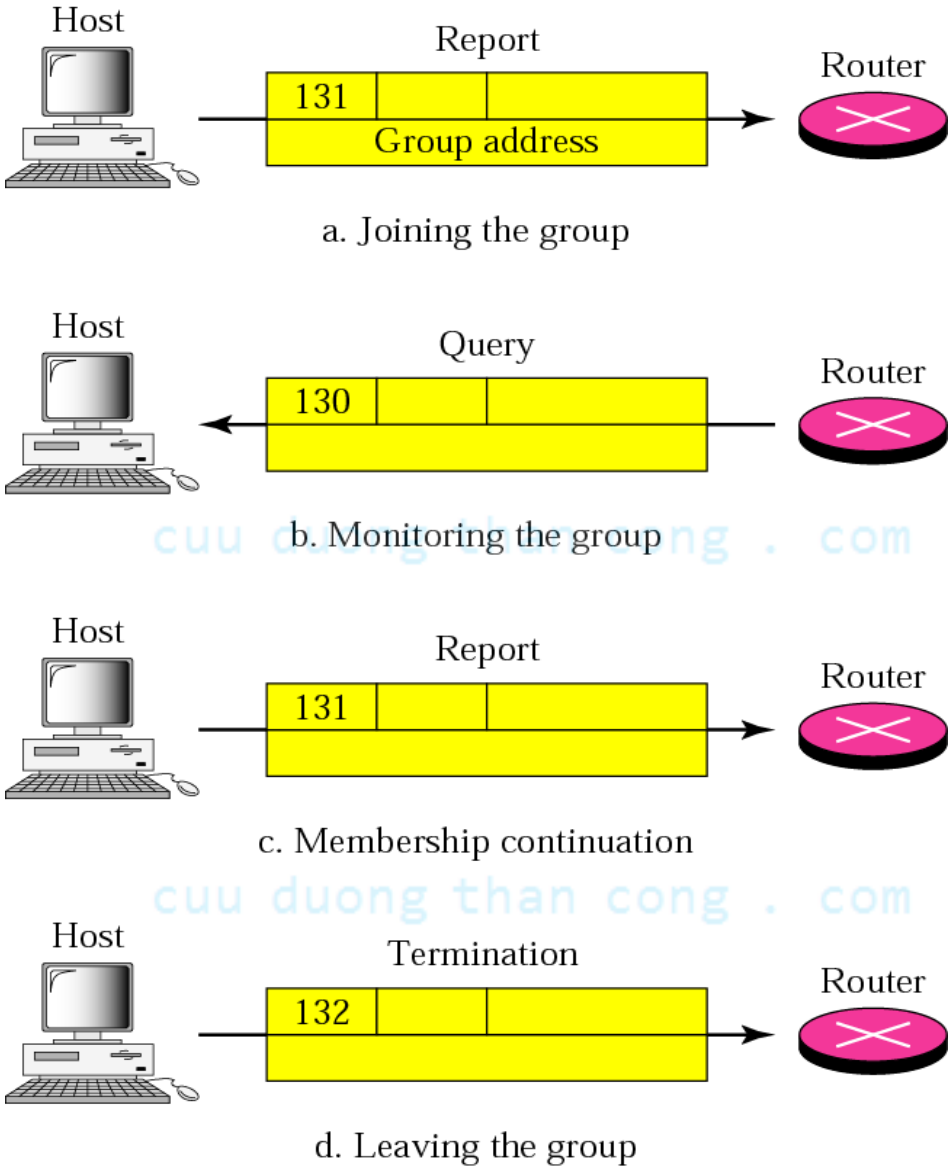


b. Report



c. Termination

Figure 27.47 *Four situations of group-membership operation*



27.3 TRANSITION FROM IPv4 TO IPv6

Three strategies have been devised by the IETF to provide for a smooth transition from IPv4 to IPv6.

The topics discussed in this section include:

Dual Stack
Tunneling
Header Translation

Figure 27.48 *Three transition strategies*

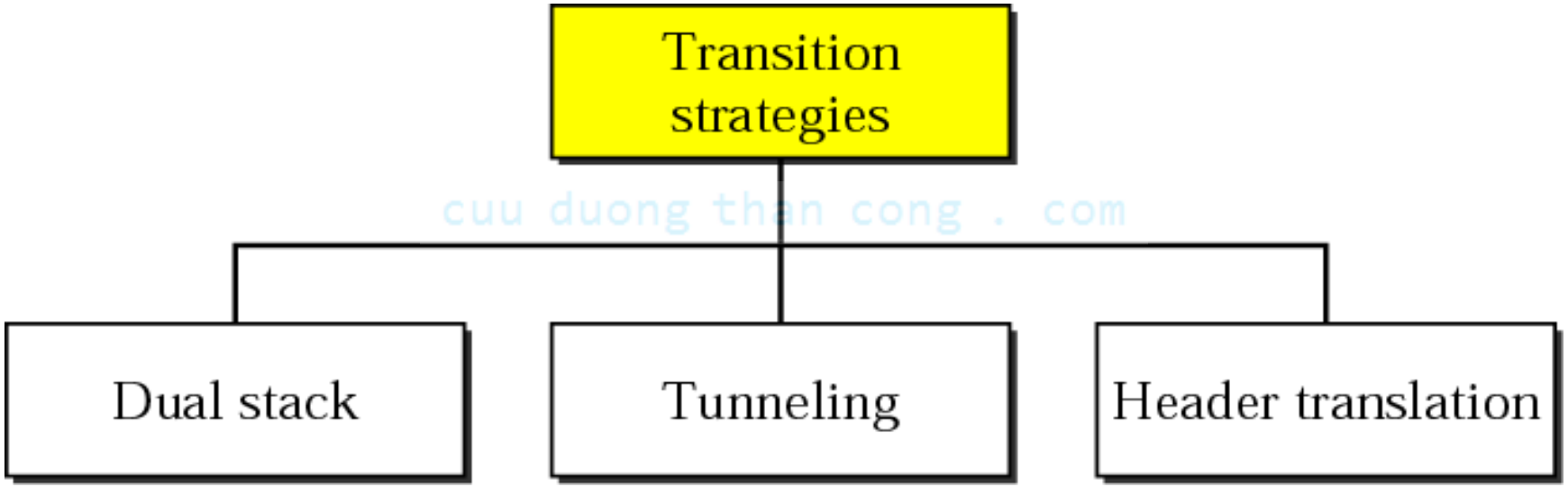


Figure 27.49 *Dual stack*

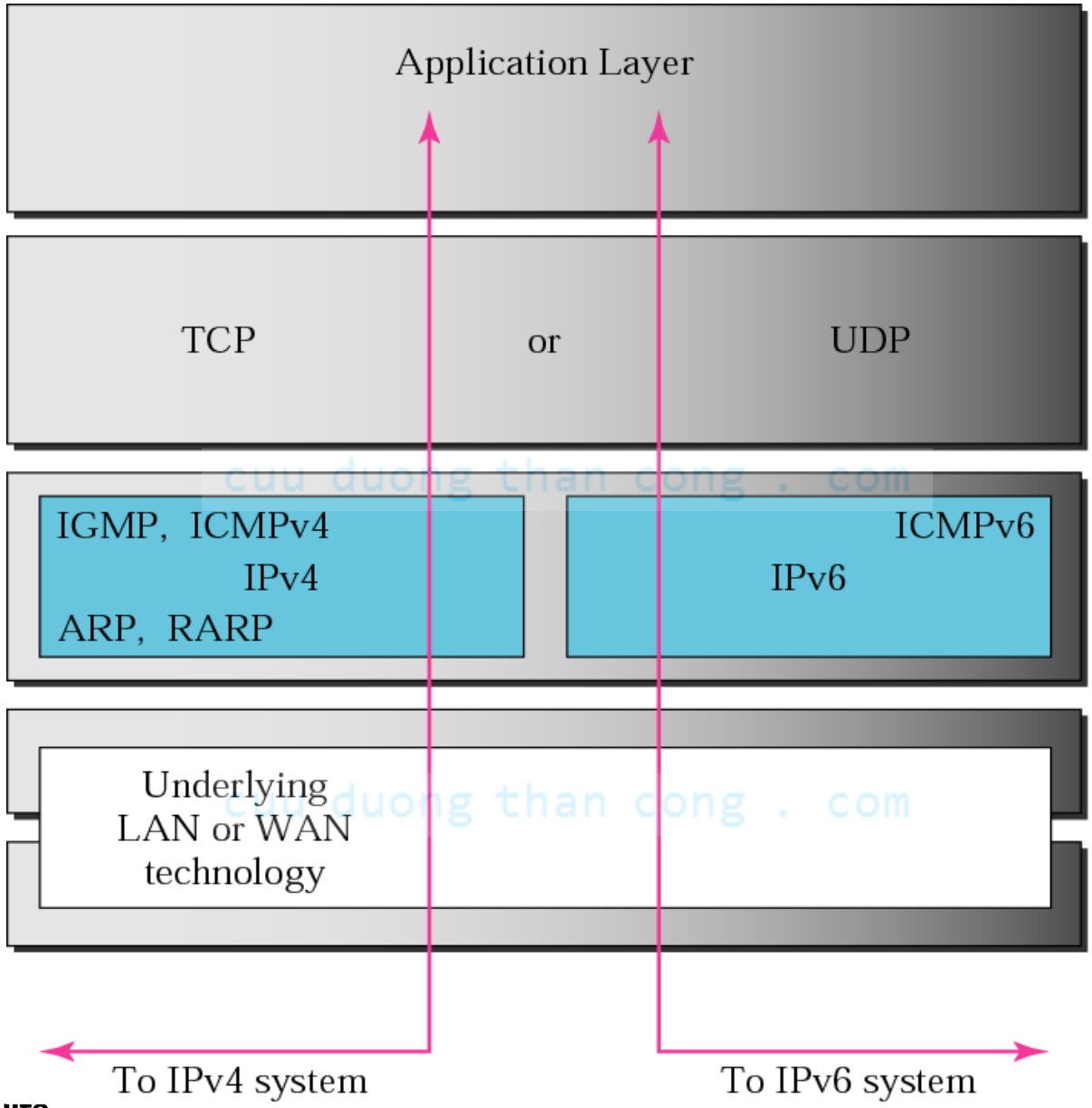


Figure 27.50 *Automatic tunneling*

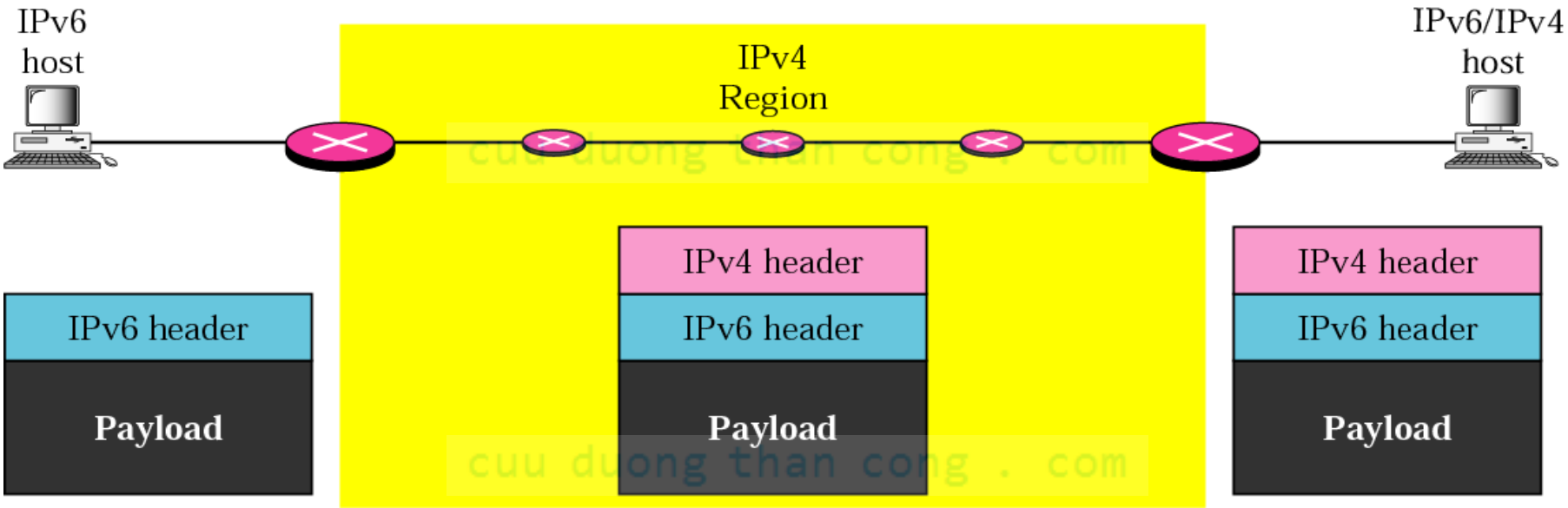


Figure 27.51 *Configured tunneling*

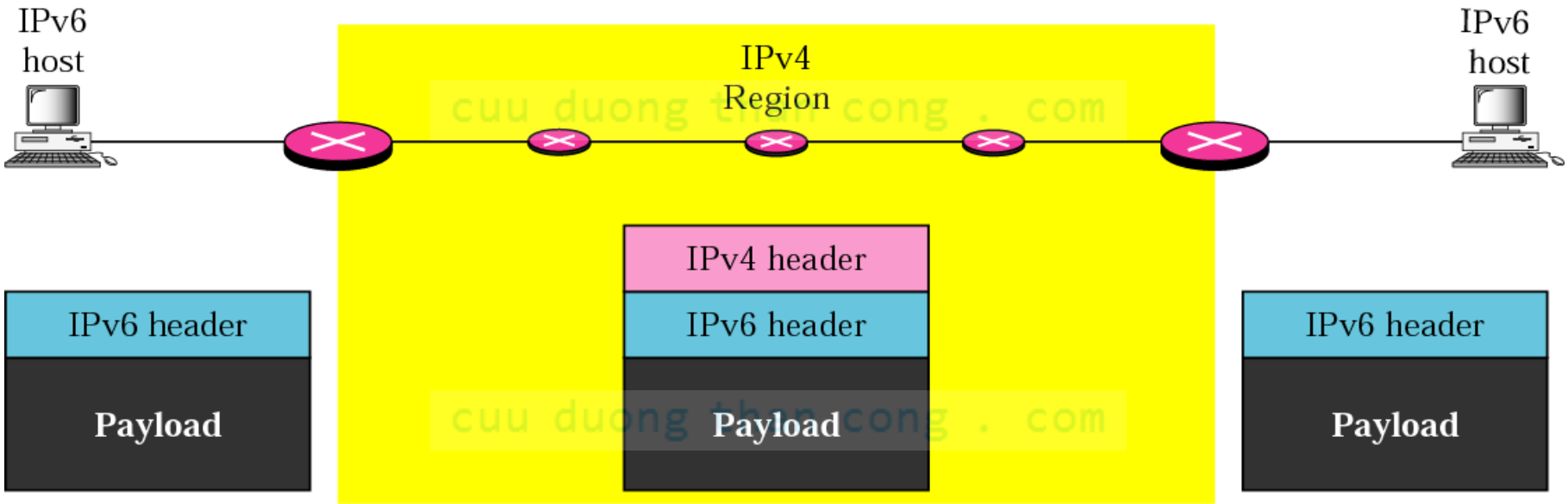


Figure 27.52 *Header translation*

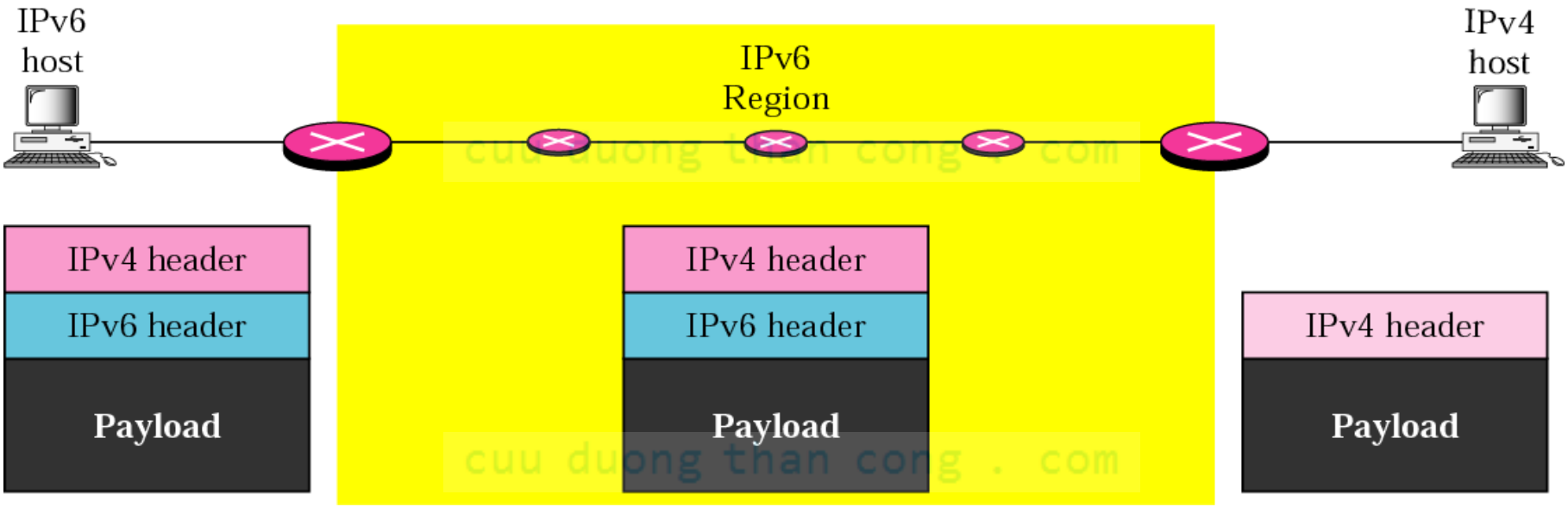


Table 27.9 Header translation

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.