Chapter 9

Internet Control Message Protocol (ICMP)

CONTENTS

- **TYPES OF MESSAGES**
- **MESSAGE FORMAT**
- **ERROR REPORTING**
- **QUERY**
- **CHECKSUM**
- **ICMP PACKAGE**

Figure 9-1

Position of ICMP in the network layer

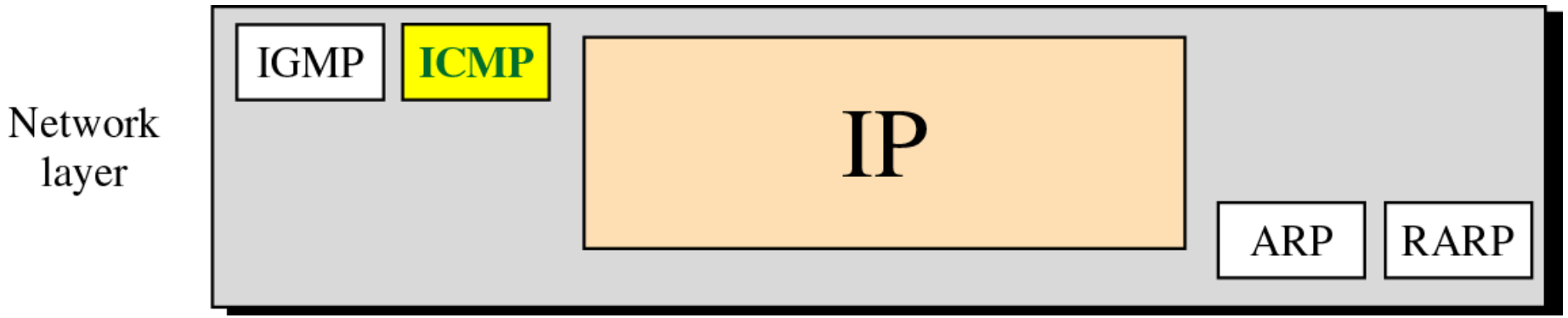
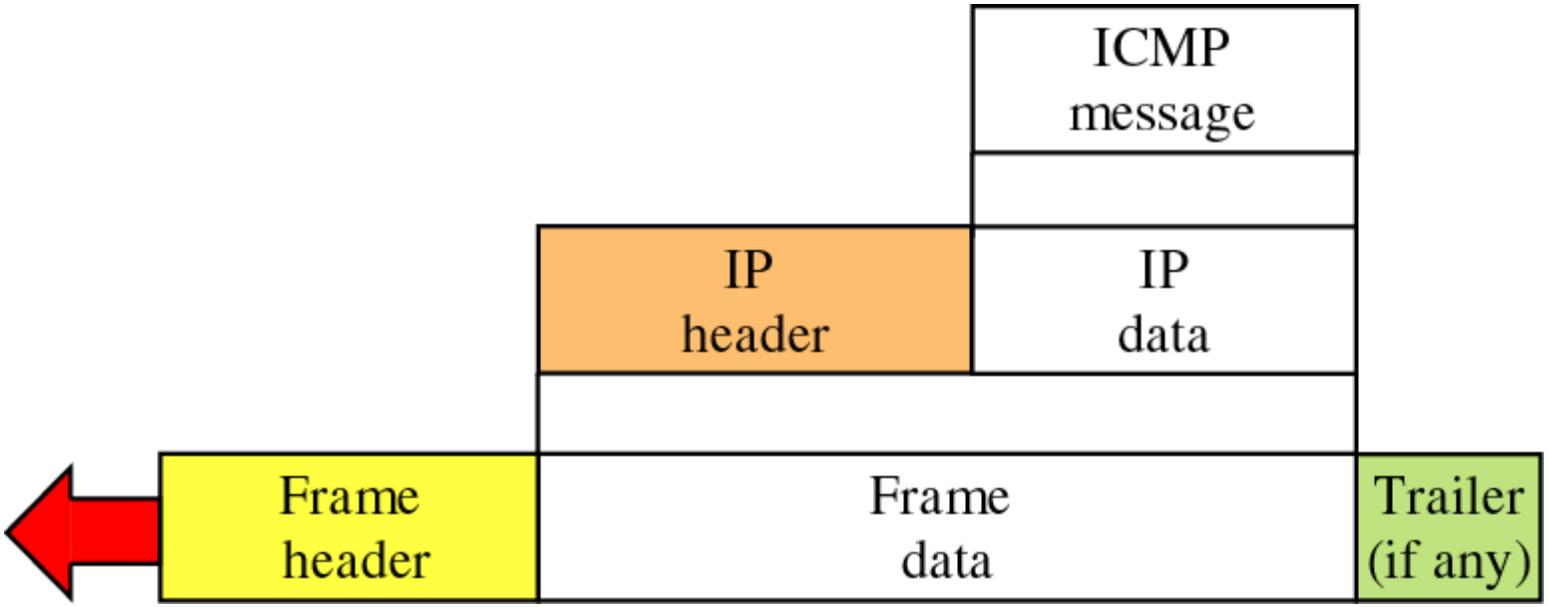


Figure 9-2

Encapsulation of ICMP packet

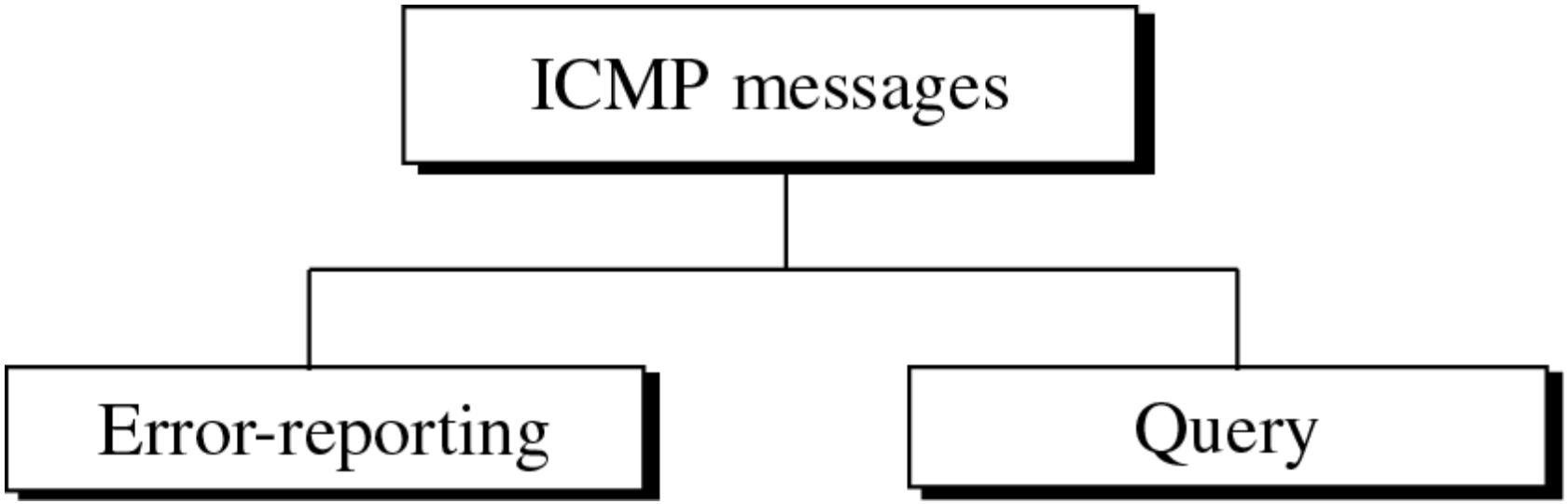


9.1

TYPES OF MESSAGES

Figure 9-3

ICMP messages

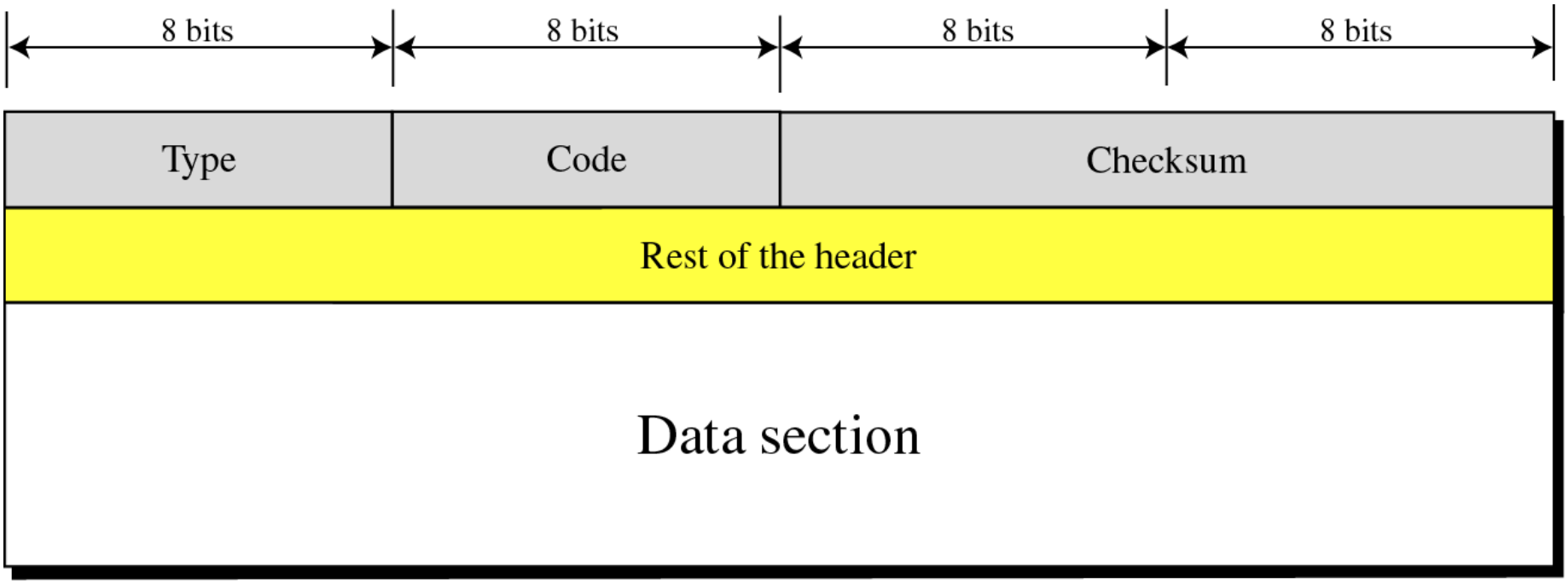


9.2

MESSAGE FORMAT

Figure 9-4

General format of ICMP messages



9.3

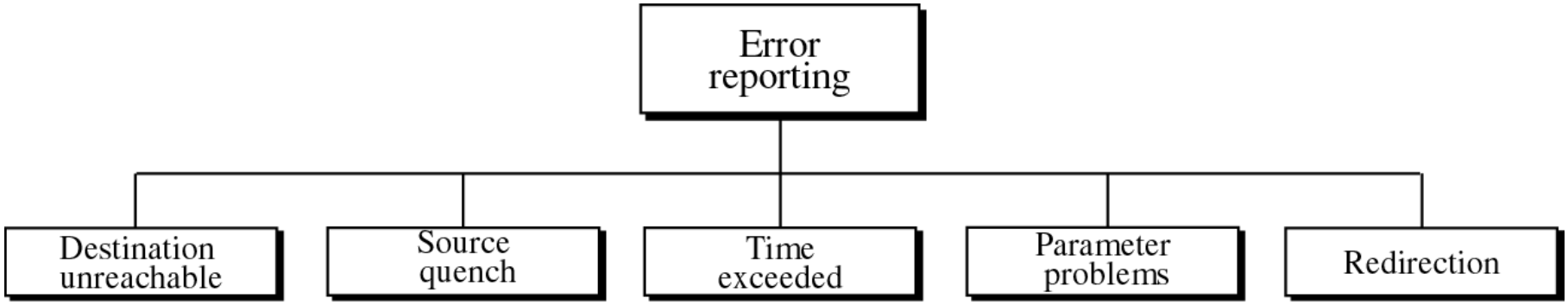
ERROR REPORTING

Note

ICMP always reports error messages to the original source.

Figure 9-5

Error-reporting messages



Note

Important points about ICMP error messages:

1. ***No ICMP error message for a datagram carrying an ICMP error message.***
2. ***No ICMP error message for a fragmented datagram that is not the first fragment.***
3. ***No ICMP error message for a datagram having a multicast address.***
4. ***No ICMP error message for a datagram with a special address such as 127.0.0.0 or 0.0.0.0.***

Figure 9-6

Contents of data field for error messages

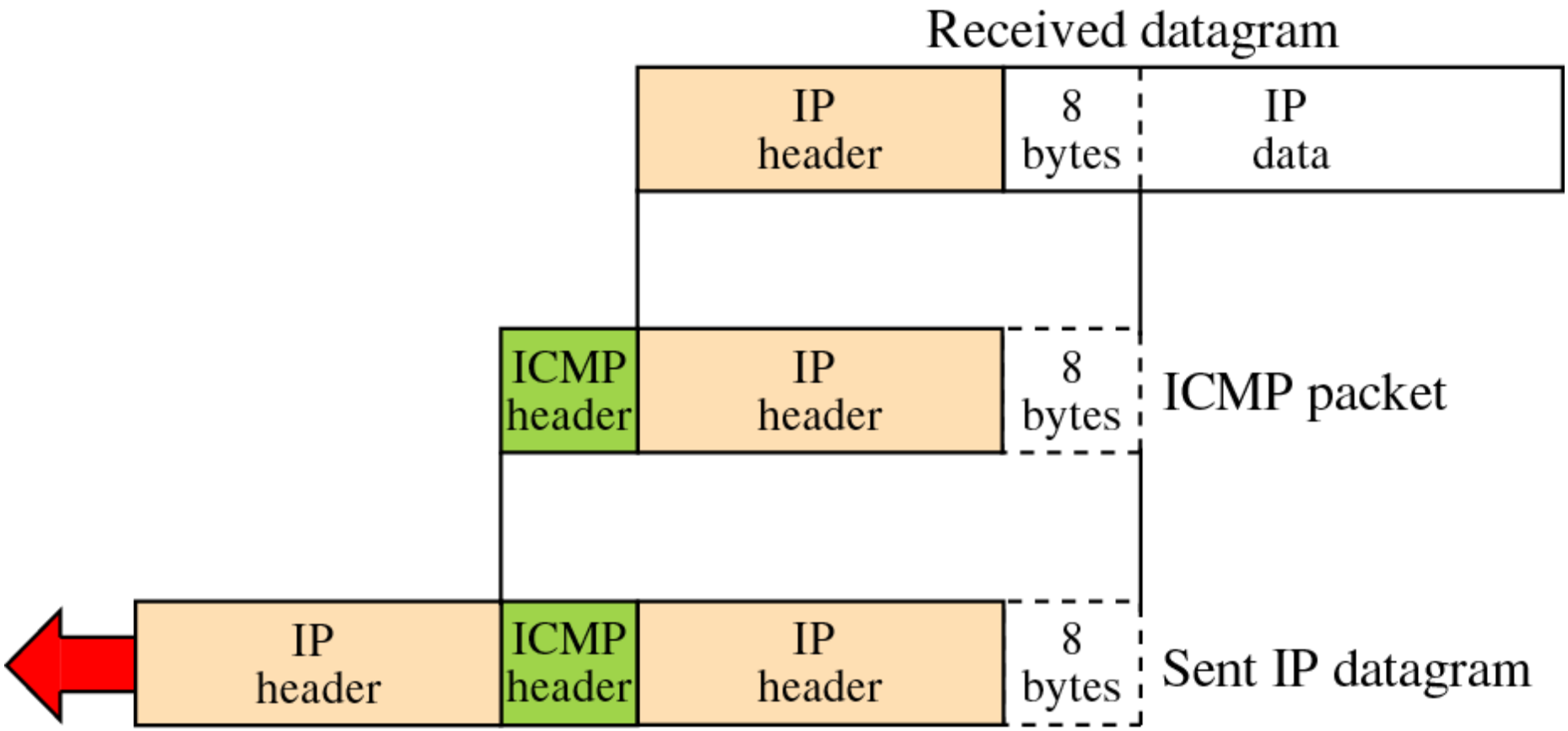
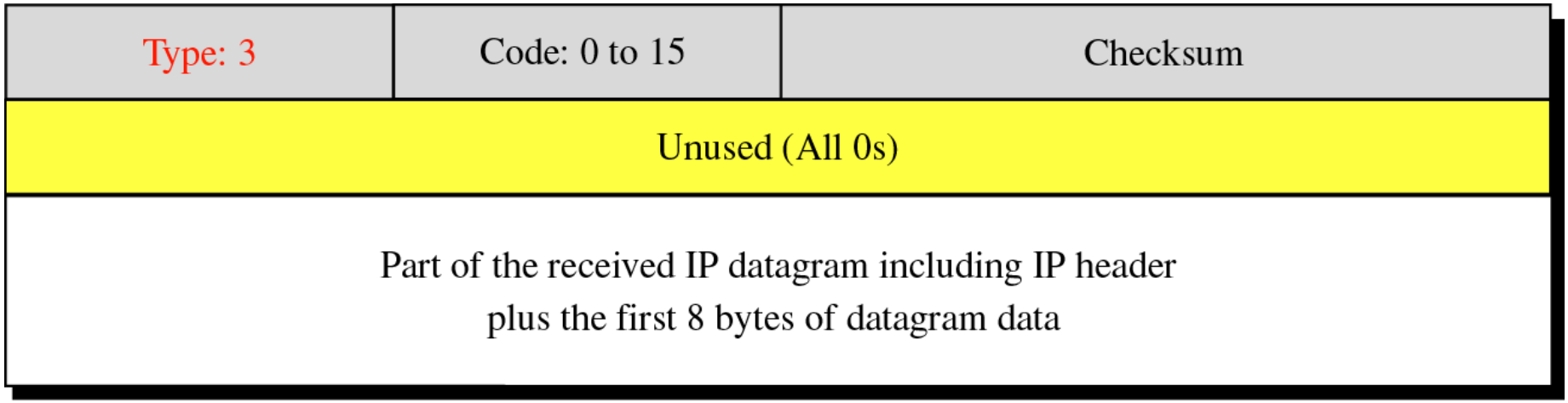


Figure 9-7

Destination-unreachable format



Destination-unreachable different codes

- Code 0: the network is unreachable
- Code 1: the host is unreachable
- Code 2: the protocol is unreachable
- Code 3: the port is unreachable
- Code 4: fragmentation is required but the DF flag is set
- Code 5: source routing can not be accomplished
- Code 6: the destination network is unknown
- Code 7: the destination host is unknown
- Code 9: communication with destination network is administratively prohibited
- Code 10: communication with destination host is administratively prohibited
- Code 11: the network is unreachable for specified type of service
- Code 12: the host is unreachable for specified type of service
- Code 14: the host is unreachable because the precedence is violated
- Code 15: the host is unreachable because the precedence was cut off

Note

Destination-unreachable messages with codes 2 or 3 can be created only by the destination host. Other destination-unreachable messages can be created only by routers.

Note

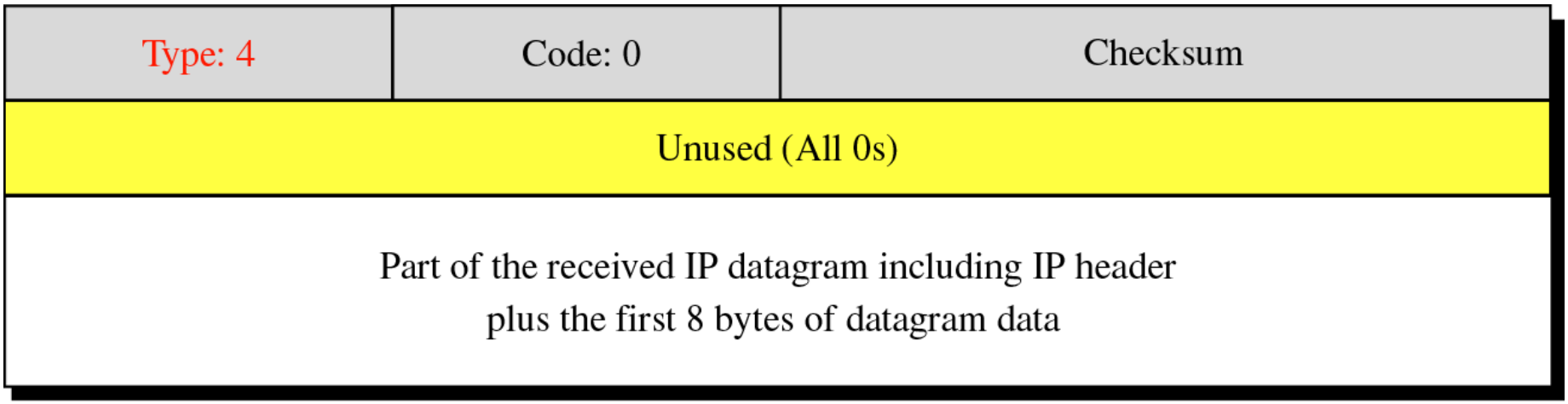
A router cannot detect all problems that prevent the delivery of a packet.

Note

There is no flow-control mechanism in the IP protocol.

Figure 9-8

Source-quench format



Note

A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host.

The source must slow down the sending of datagrams until the congestion is relieved.

Note

One source-quench message should be sent for each datagram that is discarded due to congestion.

Note

Whenever a router receives a datagram with a time-to-live value of zero, it discards the datagram and sends a time-exceeded message to the original source.

Note

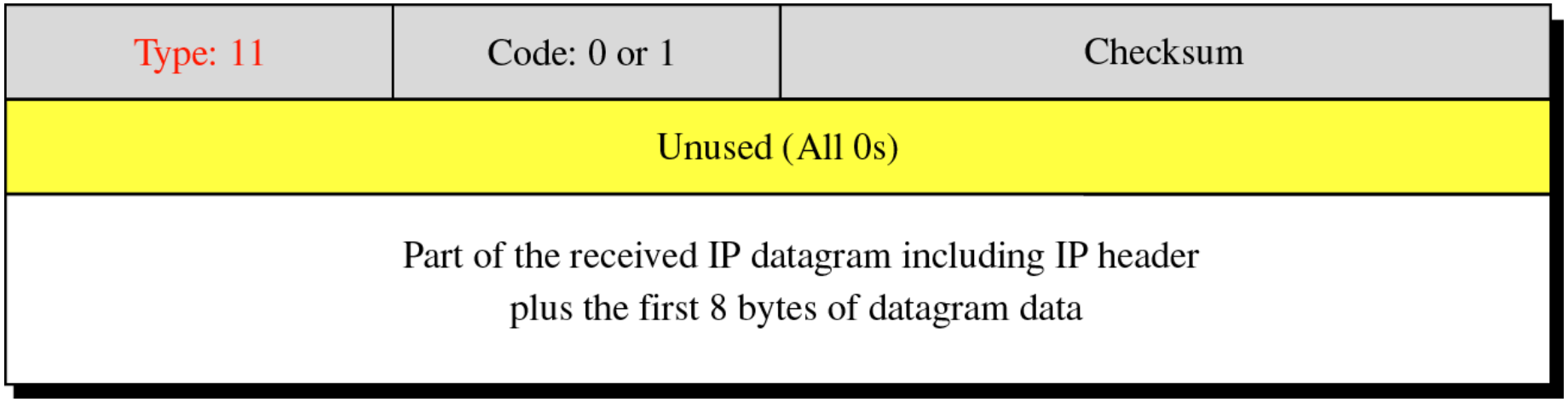
When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.

Note

In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero. Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time.

Figure 9-9

Time-exceeded message format



Code 0: Time to live

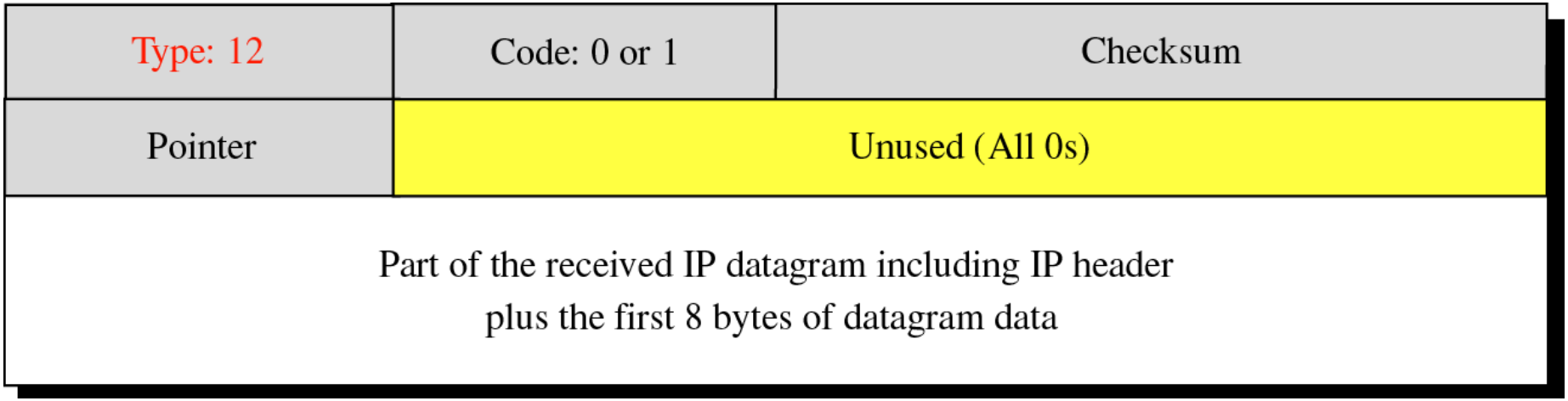
Code 1: Fragmentation

Note

A parameter-problem message can be created by a router or the destination host.

Figure 9-10

Parameter-problem message format

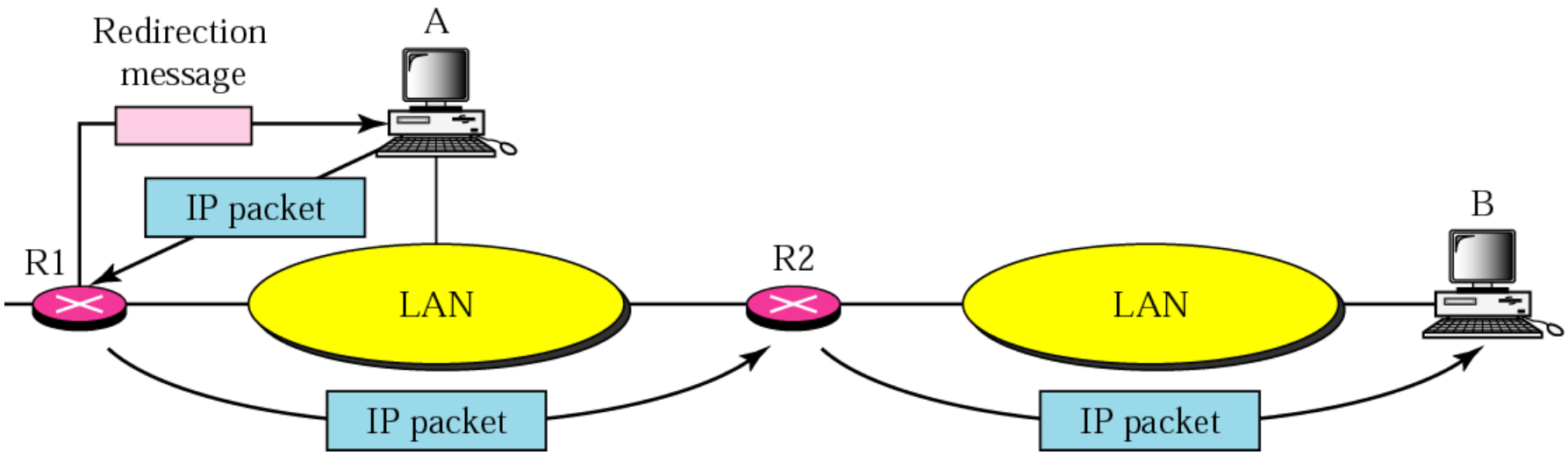


Code 0: Main header problem

Code 1: Problem in the option field

Figure 9-11

Redirection concept

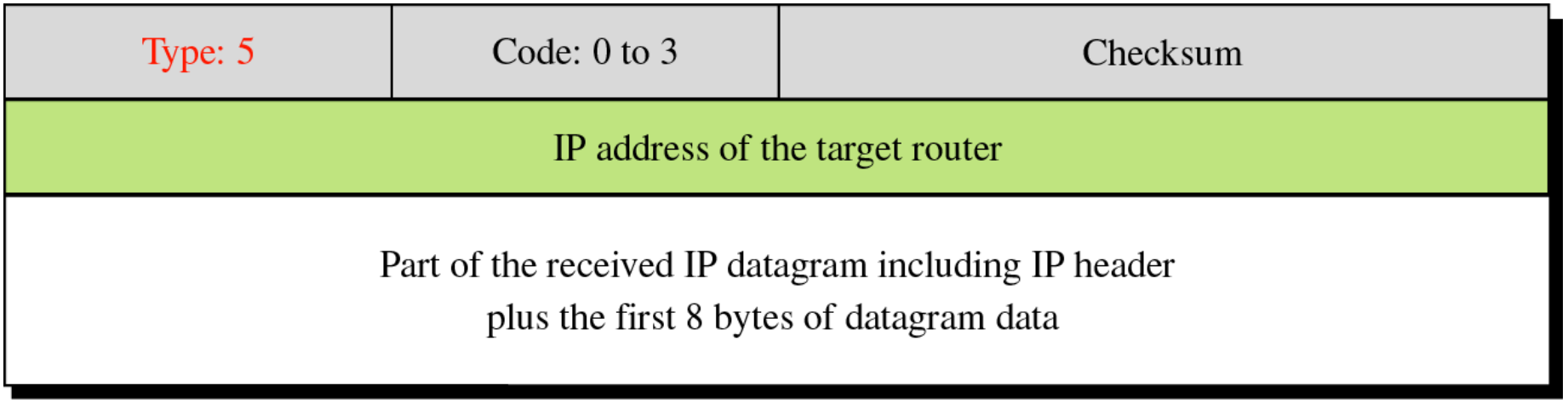


Note

A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.

Figure 9-12

Redirection message format



Code 0: Network specific
Code 1: Host specific
Code 2: Network specific (specified service)
Code 3: Host specific (specified service)

Note

A redirection message is sent from a router to a host on the same local network.

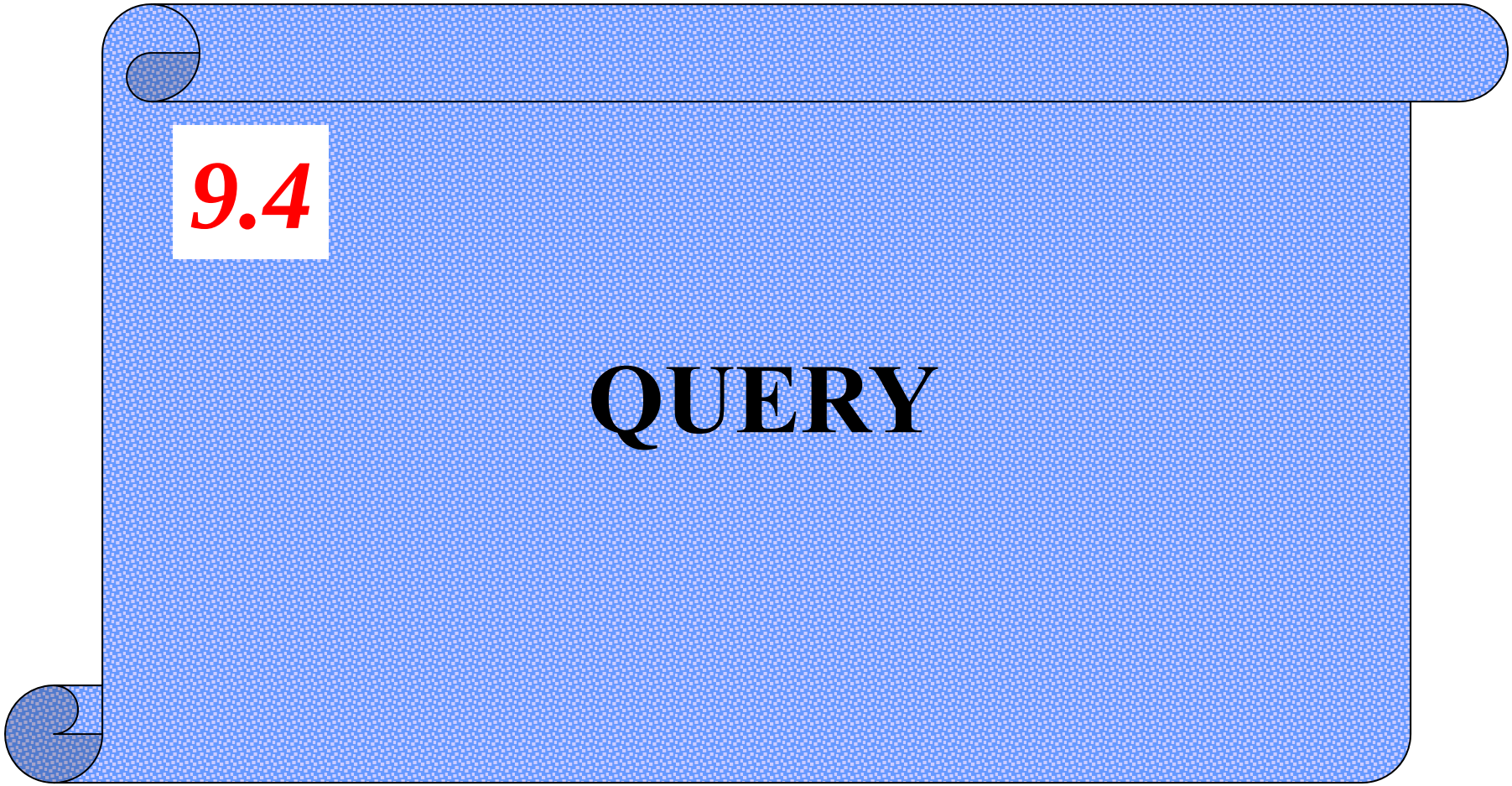
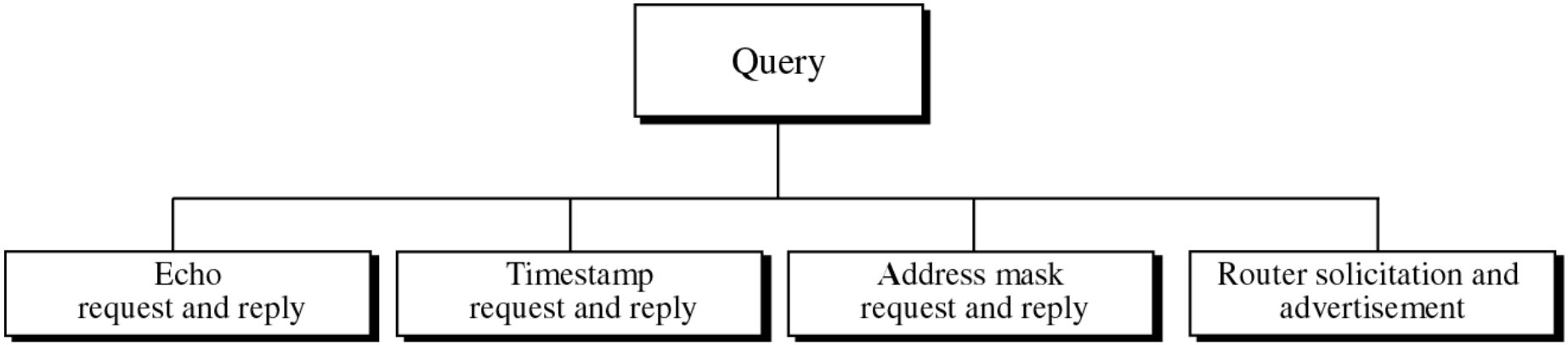


Figure 9-13

Query messages



Note

An echo-request message can be sent by a host or router. An echo-reply message is sent by the host or router which receives an echo-request message.

Note

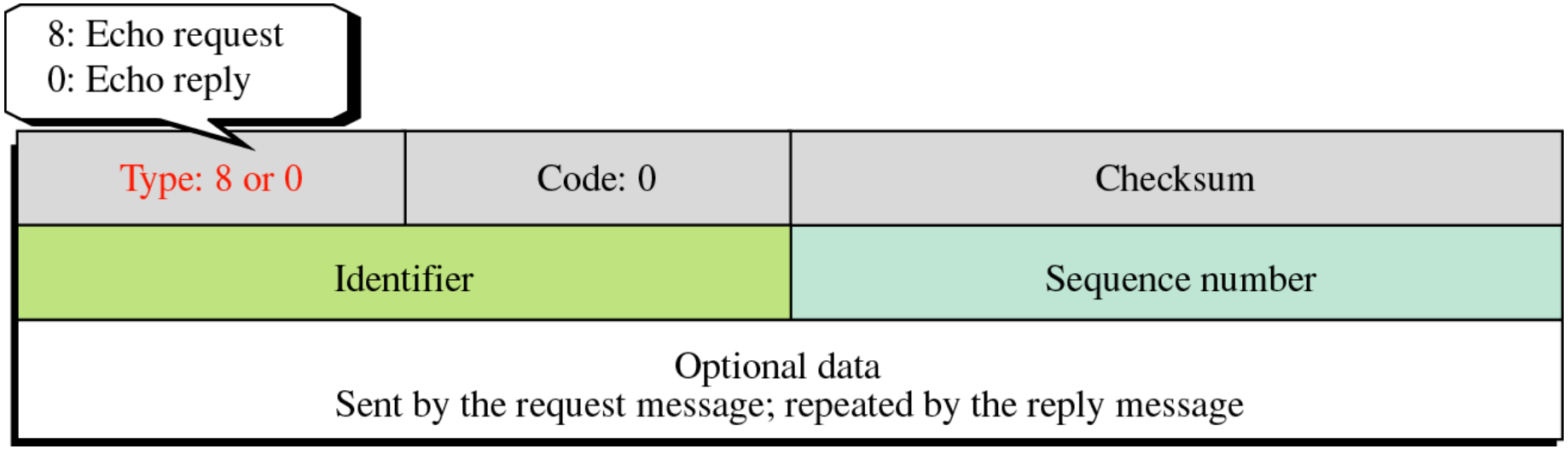
Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol.

Note

Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command.

Figure 9-14

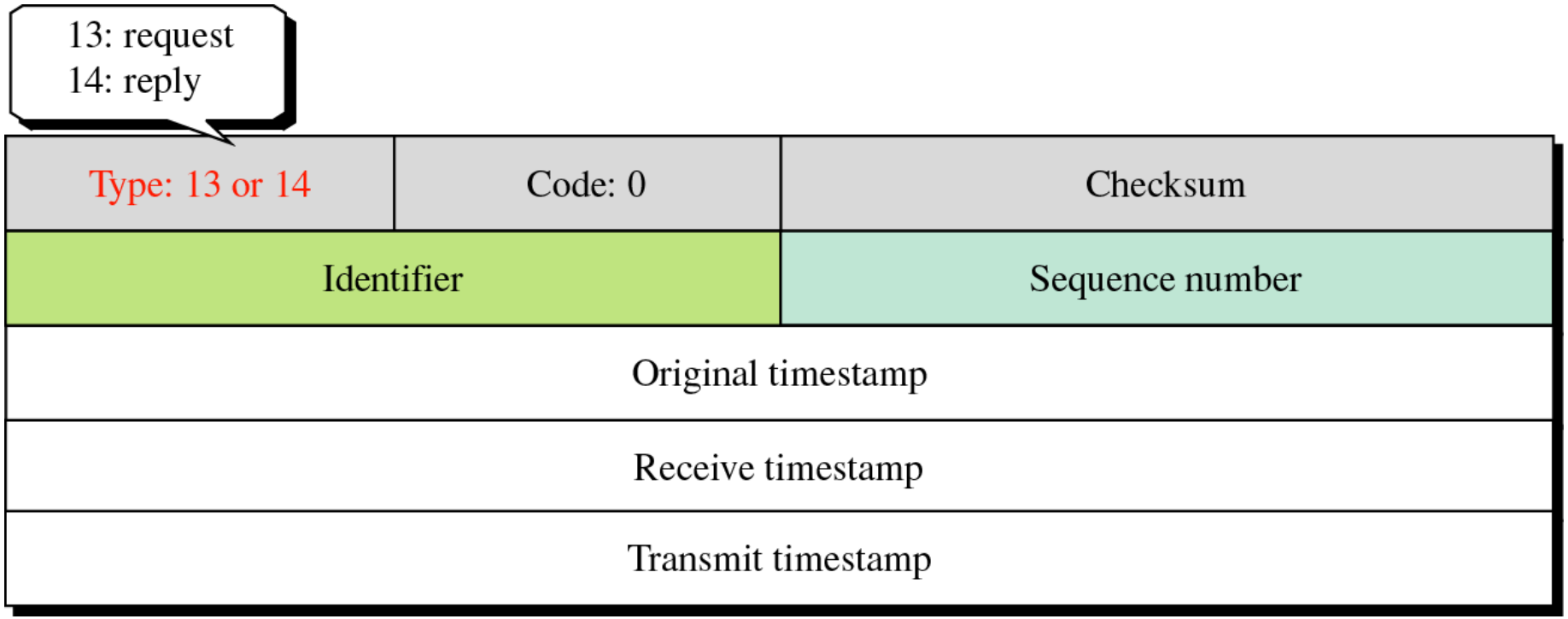
Echo-request and echo-reply message format



Ping command can use theses messages.

Figure 9-15

Timestamp-request and timestamp-reply message format



Sending time = value of receive timestamp –
value of original timestamp

Receiving time = time the packet returned –
value of transmit timestamp

Round-trip time = sending time +
receiving time

Note

Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine even if their clocks are not synchronized.

Given the following information:

Value of original timestamp: 46

Value of receive timestamp: 59

Value of transmit timestamp: 60

Time the packet arrived: 67

We can calculate:

Sending time = 59 – 46 = 13 milliseconds

Receiving time = 67 – 60 = 7 milliseconds

Round-trip time = 13 + 7 = 20 milliseconds

Given the actual one-way time,

Time difference = receive timestamp –

(original timestamp field
+ one-way time duration)

We have:

$$\text{Time difference} = 59 - (46 + 10) = 3$$

Note

The timestamp-request and timestamp-reply messages can be used to synchronize two clocks in two machines if the exact one-way time duration is known.

Figure 9-16

Mask-request and mask-reply message format

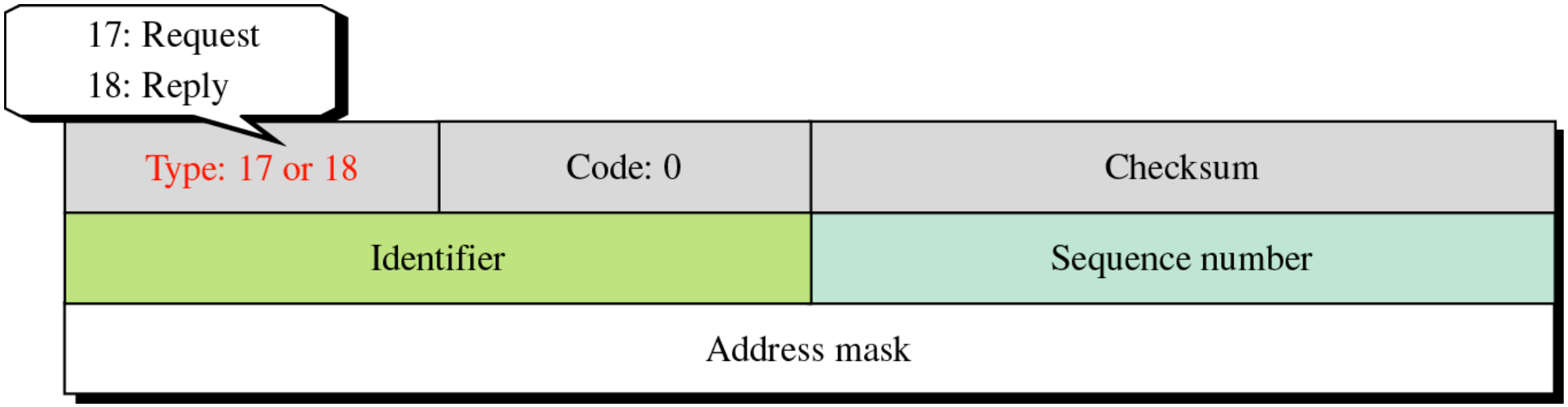


Figure 9-17

Router solicitation message format

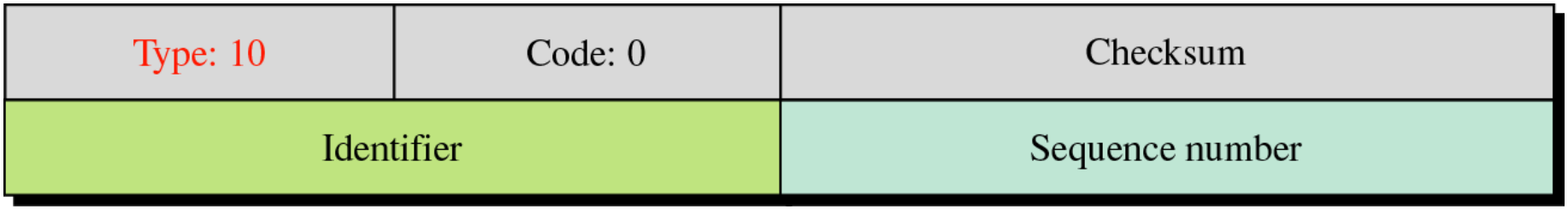
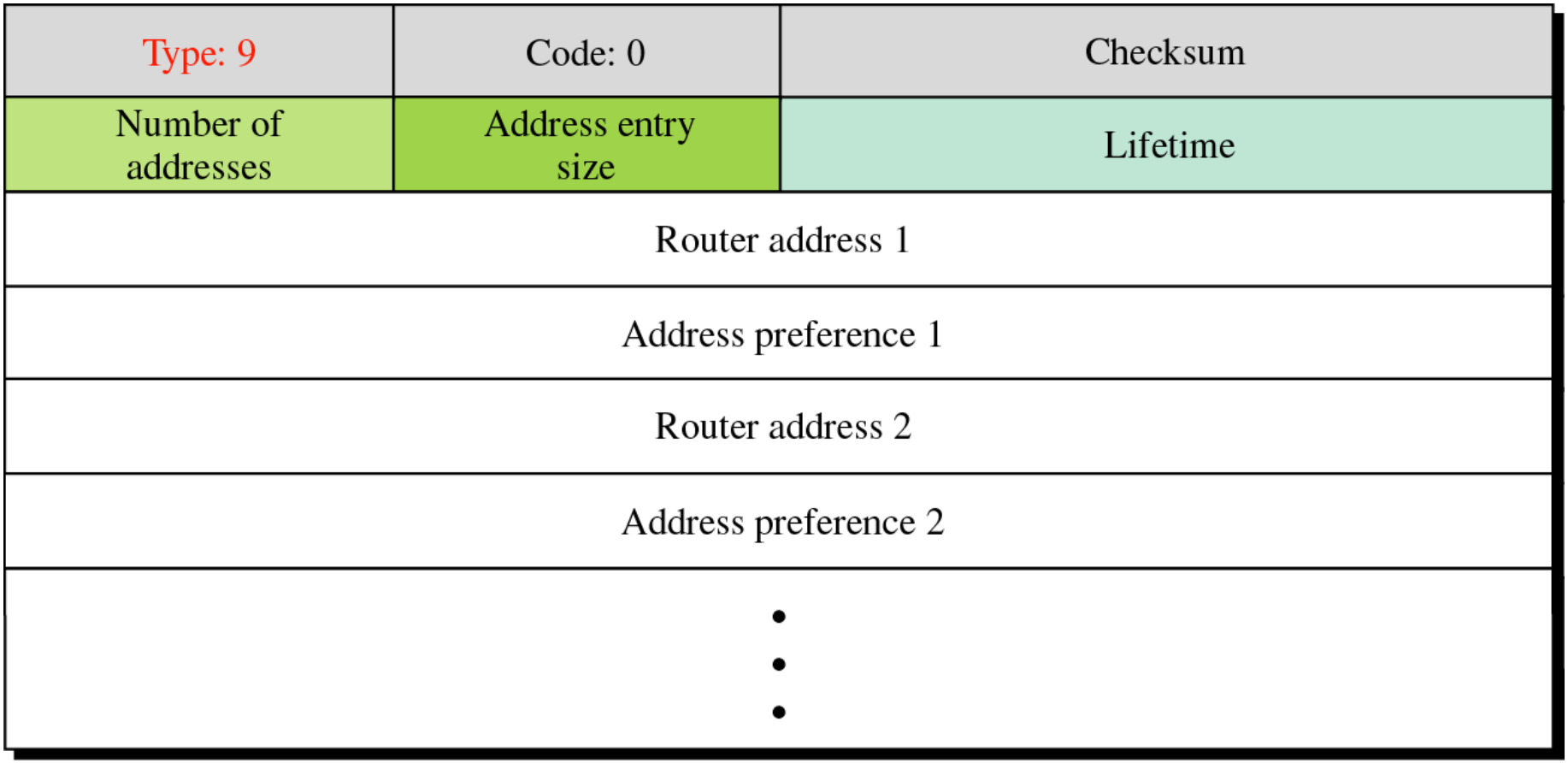


Figure 9-18

Router advertisement message format

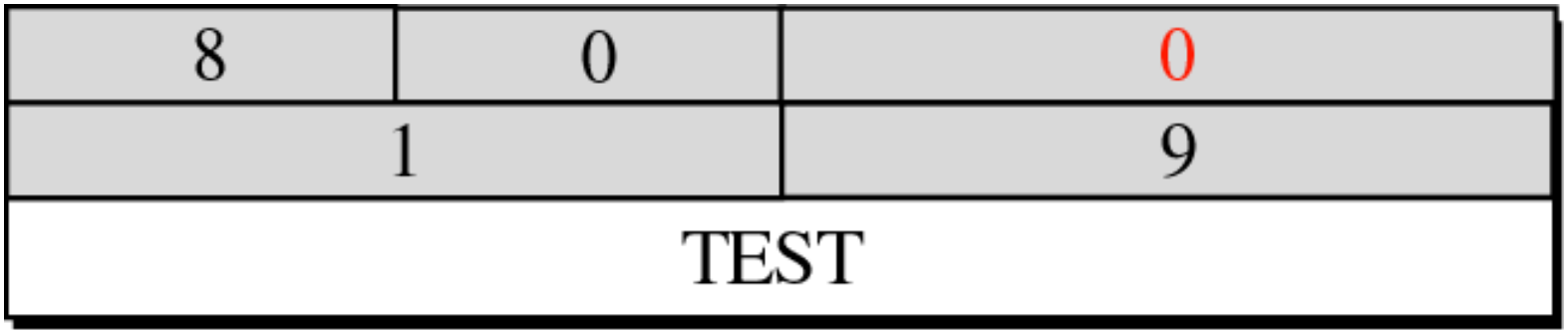


9.5

CHECKSUM

Figure 9-19

Example of checksum calculation



8 and 0 →	00001000	00000000
0 →	00000000	00000000
1 →	00000000	00000001
9 →	00000000	00001001
T & E →	01010100	01000101
S & T →	01010011	01010100
Sum →	10101111	10100011
Checksum →	01010000	01011100

9.6

ICMP PACKAGE

Figure 9-20

ICMP package