Chapter 9

Internet Control Message Protocol (ICMP)

CONTENTS

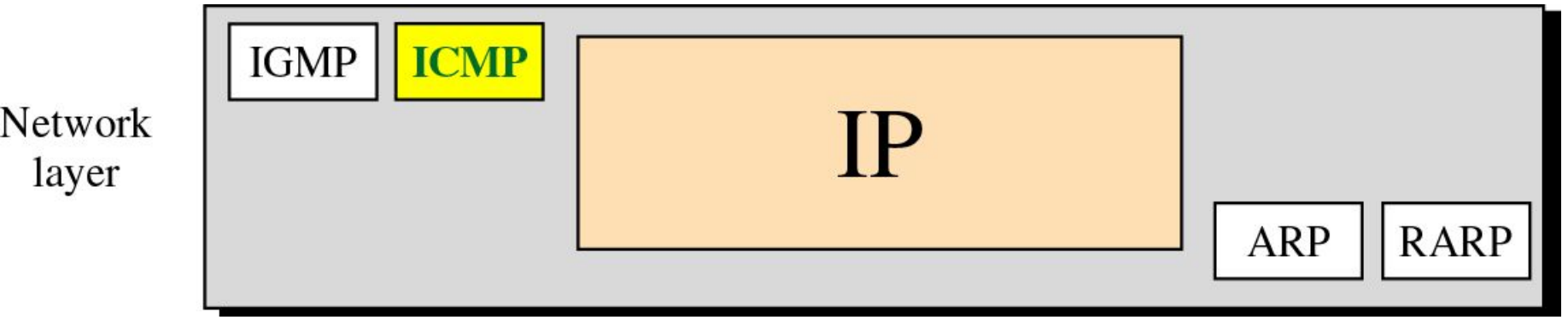
- **TYPES OF MESSAGES**
- **MESSAGE FORMAT**
- **ERROR REPORTING**
- **QUERY**

- The IP protocol has no error-reporting or error-correcting mechanism.
- What happens if a router must discard a datagram because it cannot find a router to the final destination, or because the time-to-live field has a zero value?
- What happens if the final destination host must discard all fragments of a datagram because it has not received all fragments within a predetermined time limit?

- These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host.
- The IP protocol also lacks a mechanism for host and management queries.

Figure 9-1

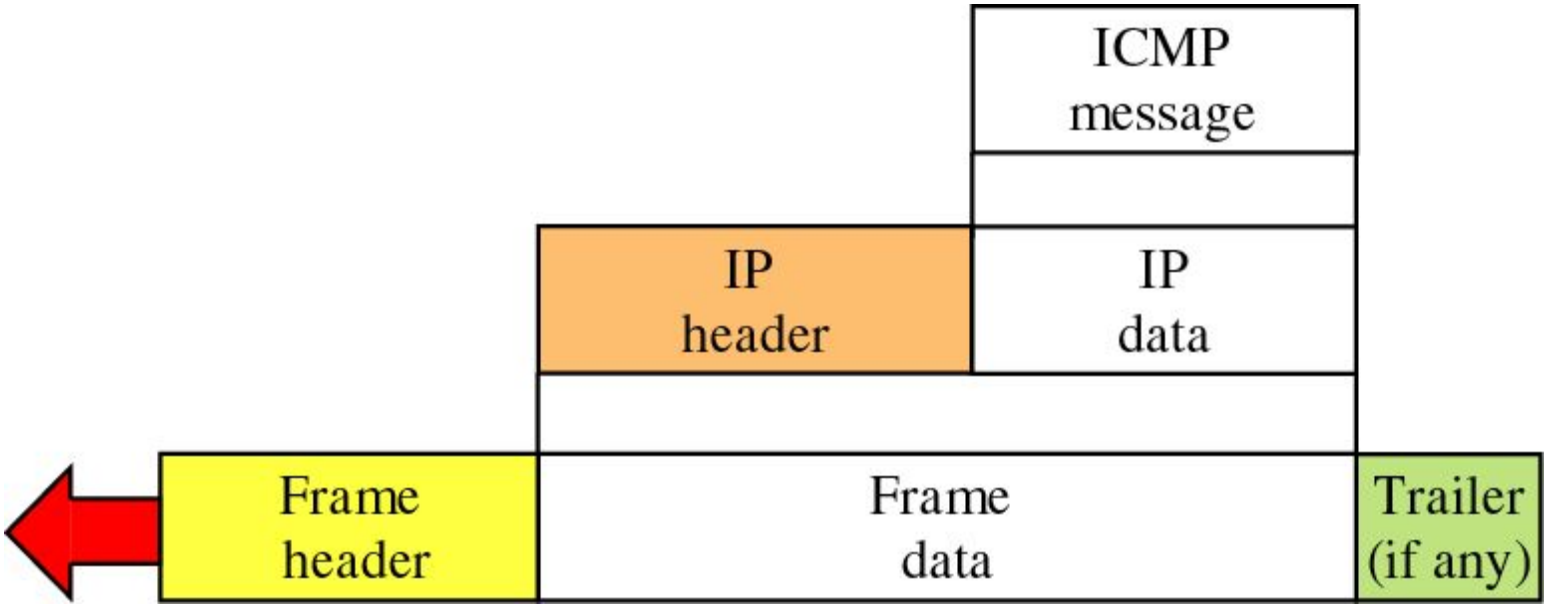
Position of ICMP in the network layer



ICMP itself is a network layer protocol. However, its messages are not passed directly to the data link layer as would be expected. Instead, the messages are first encapsulated inside IP datagrams before going to the lower layer

Figure 9-2

Encapsulation of ICMP packet

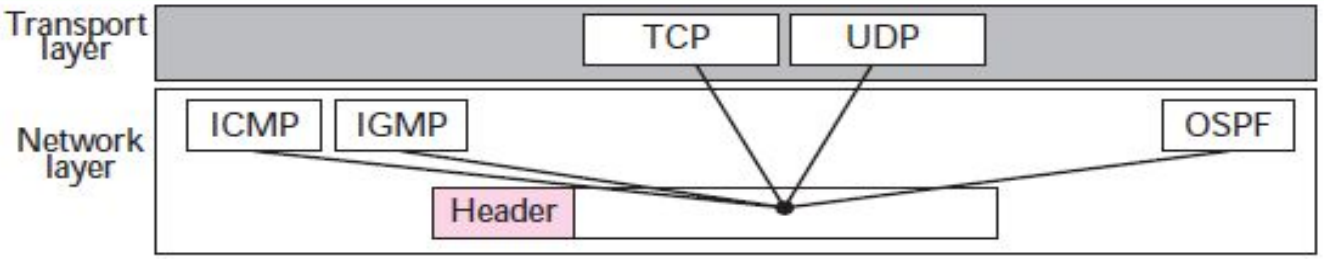


The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message.

example

- **Protocol.** This 8-bit field defines the higher-level protocol that uses the services of the IP layer. An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IP datagram should be delivered. In other words, since the IP protocol multiplexes and demultiplexes data from different higher-level protocols, the value of this field helps in the demultiplexing process when the datagram arrives at its final destination (see Figure 7.5).

Figure 7.5 *Multiplexing*



Some of the value of this field for different higher-level protocols is shown in Table 7.2.

Table 7.2 *Protocols*

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

Figure 9-3

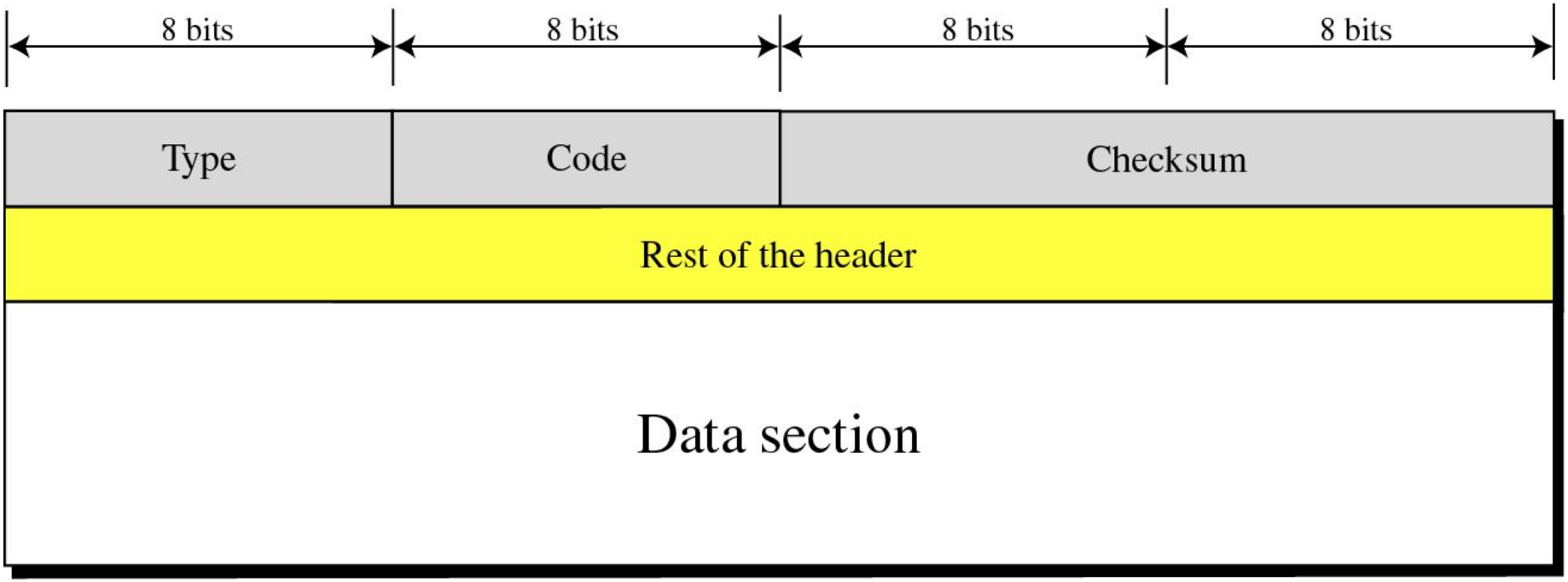
ICMP messages

9.2

MESSAGE FORMAT

Figure 9-4

General format of ICMP messages



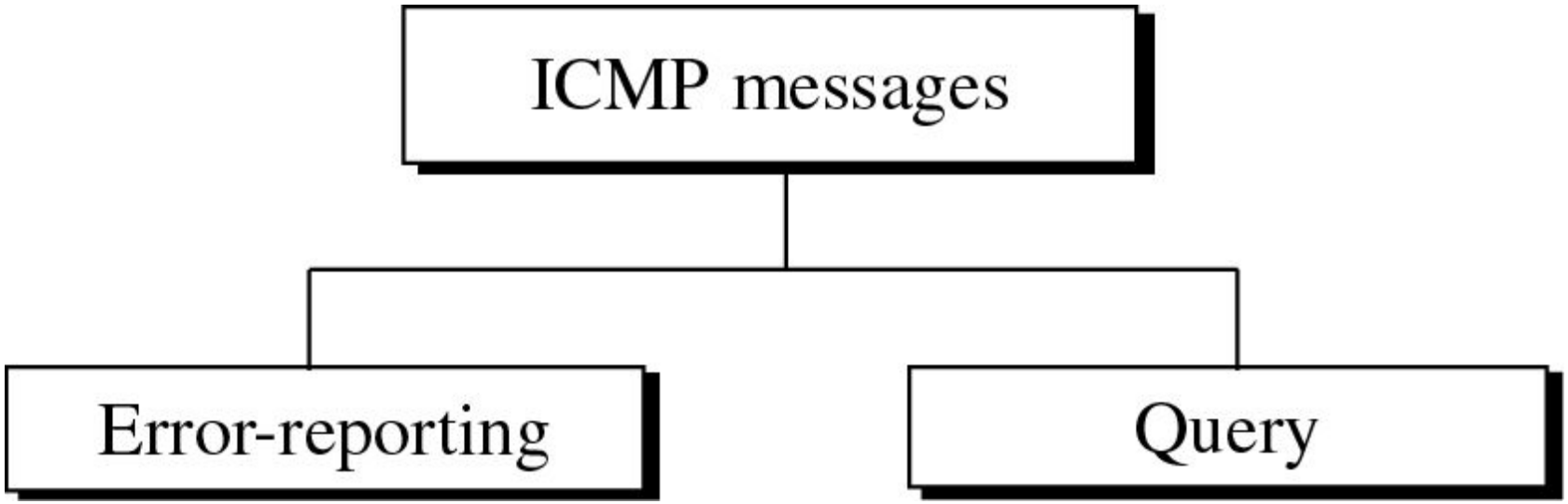
- An ICMP message has an 8-byte header and a variable-size data section.
- Data section in error messages carries information for finding the original packet that had the error.
- In query messages, the data section carries extra information based on the type of the query

9.1

TYPES OF MESSAGES

Figure 9-3

ICMP messages



9.3

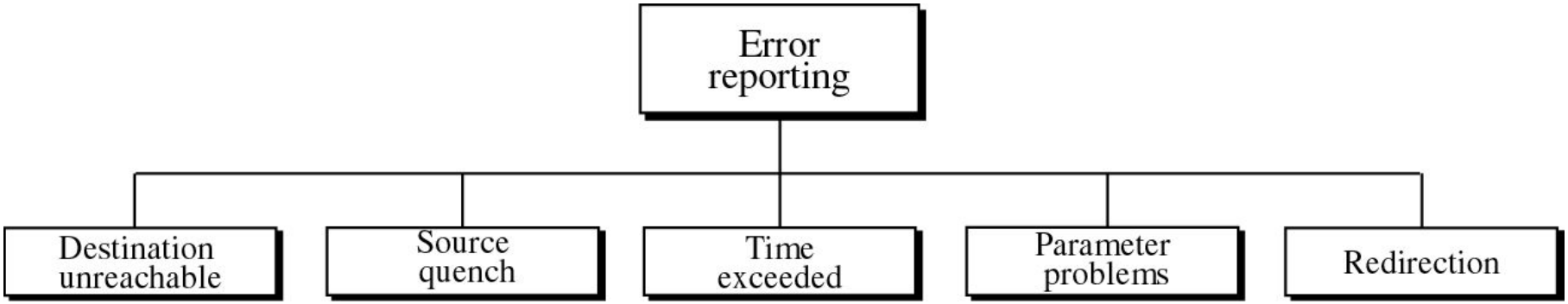
ERROR REPORTING

Note

ICMP always reports error messages to the original source.

Figure 9-5

Error-reporting messages

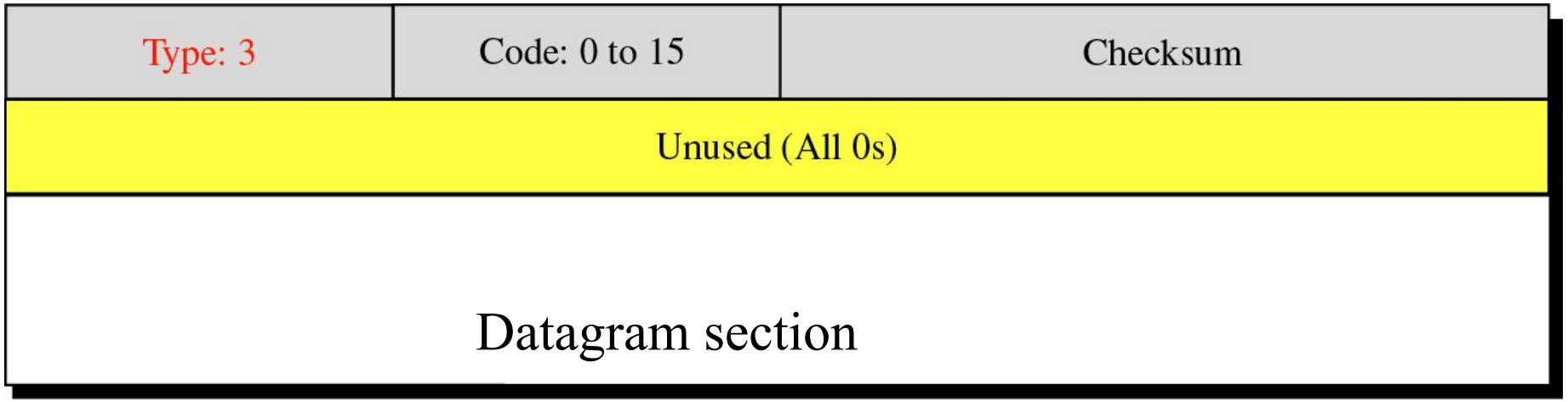


The following are important points about ICMP error messages:

- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Figure 9-7

Destination-unreachable format



Code specifies the reason for (type of msg)discarding the datagram

Destination Unreachable CODE Field

Code Value	Meaning
0	Network Unreachable due to h/w failure
1	Host Unreachable due to h/w failure
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation needed
5	Source Route Failed
6	Destination Network unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Comm. Administratively prohibited (network)
10	Comm. Administratively prohibited (host)
11	Network unreachable for type of service
12	Host unreachable for type of service
13	host is unreachable bcos the admin has put a filter
14	host is unreachable bcos the host precedence is violated
15	host is unreachable bcos its precedence is 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

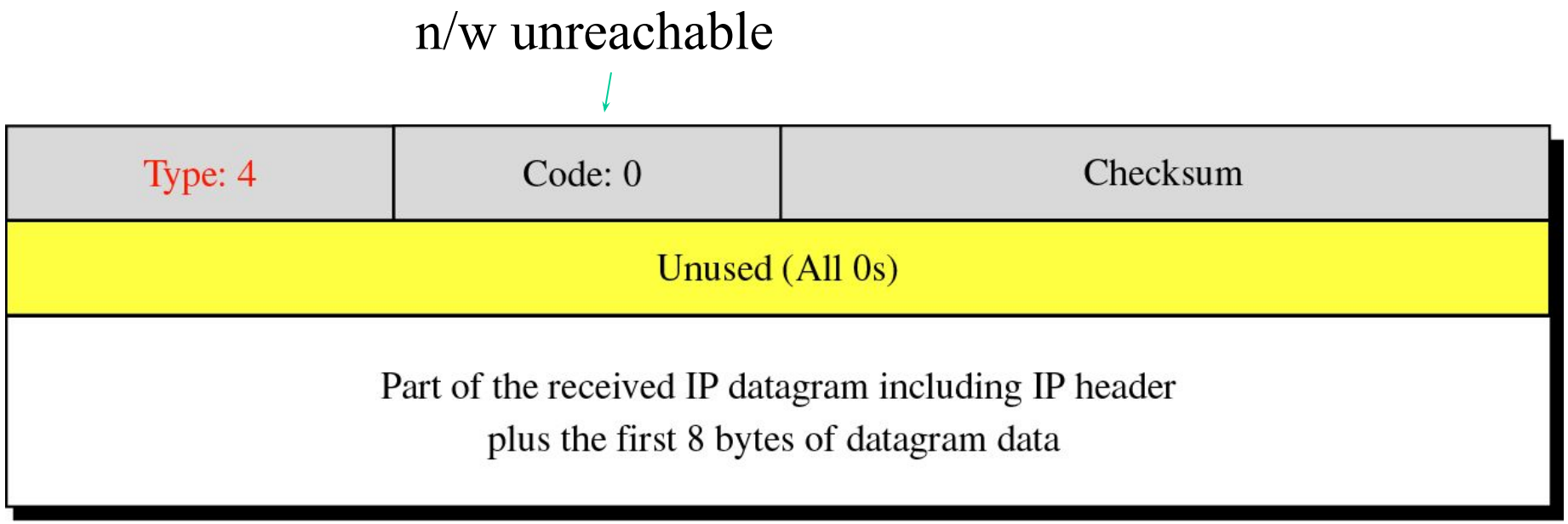
A router cannot detect all problems that prevent the delivery of a packet.

Source quench

- The IP protocol is a connectionless protocol. There is no communication between the source host, which produces the datagram, the routers, which forward it, and the destination host, which processes it. One of the ramifications of this absence of communication is the lack of *flow control and congestion control.*

Figure 9-8

Source-quench format



It is used to add flow and congestion control

Note

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

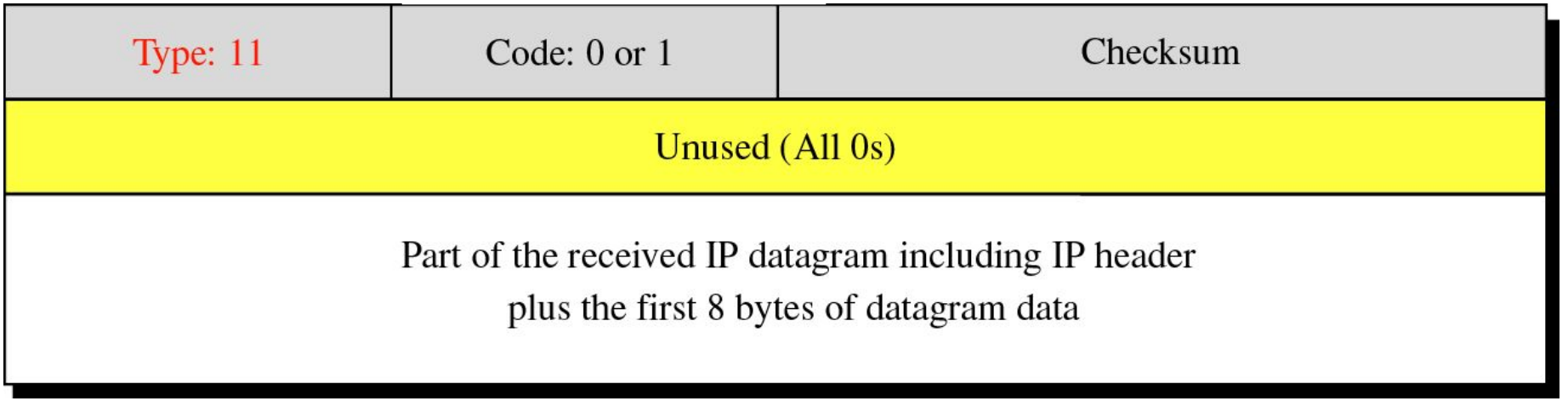
The source must slow down the sending of datagrams until the congestion is relieved.

Note

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

Figure 9-9

Time-exceeded message format



Code 0: Time to live

Code 1: Fragmentation

- Routers use routing tables to find the next hop (next router) that must receive the packet.
- If there are errors in one or more routing tables, a packet can travel in a loop or a cycle, going from one router to the next or visiting a series of routers endlessly.
- each datagram contains a field called *time to live that controls this situation.*
- *When a datagram visits a* router, the value of this field is decremented by 1.
- When the time-to-live value reaches 0, the router discards the datagram.
- However, when the datagram is discarded, a time-exceeded message must be sent by the router to the original source.

Time-exceeded message

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.

- a time-exceeded message is also generated when all fragments that make up a message do not arrive at the destination host within a certain time limit.
- When the first fragment arrives, the destination host starts a timer. If all the fragments have not arrived when the time expires, the destination discards all the fragments and sends a time-exceeded message to the original sender.

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.

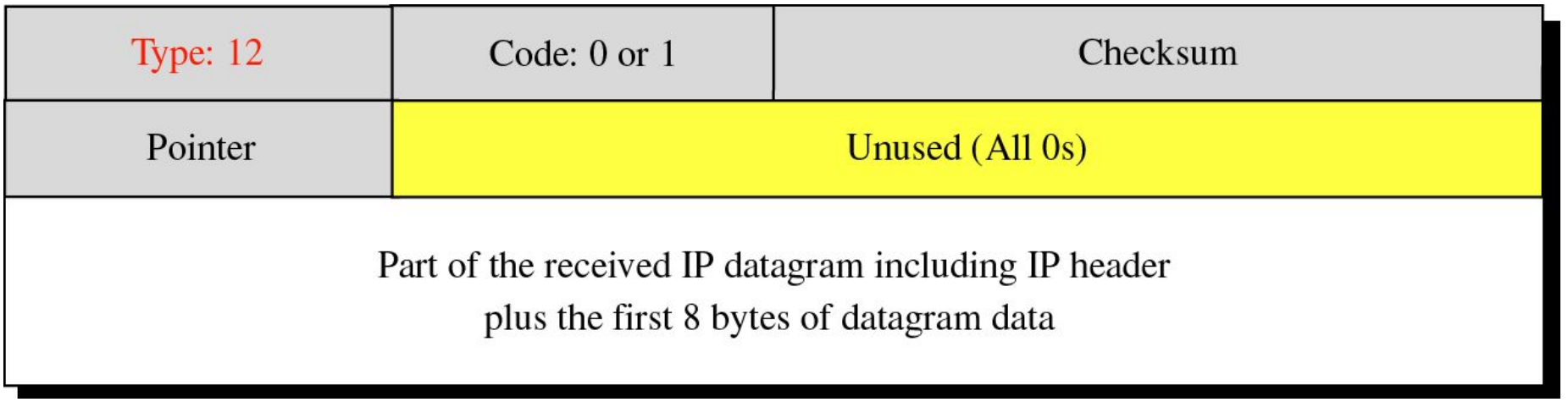
Note

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 9-10

Parameter-problem message format



Code 0: Main header problem

Code 1: Problem in the option field

- Any ambiguity in the header part of a datagram can create serious problems as the datagram travels through the Internet.
- If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.

- The code field in this case specifies the reason for discarding the datagram:

❑ **Code 0. There is an error or ambiguity in one of the header fields.**

In this case, the value in the pointer field points to the byte with the problem.

❑ **Code 1. The required part of an option is missing.**

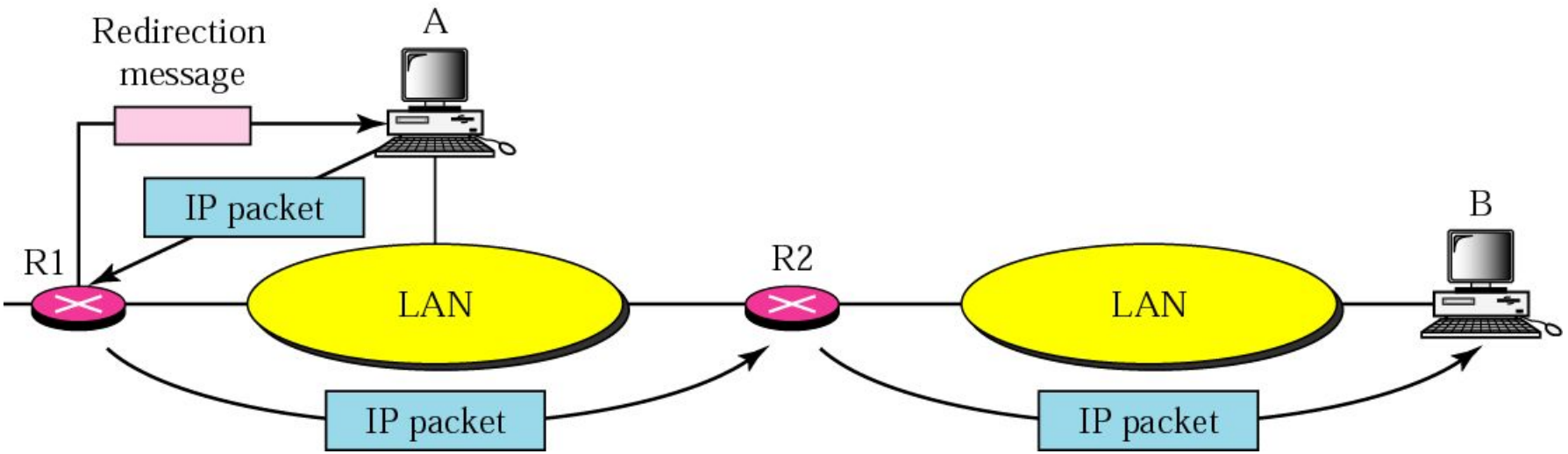
In this case, the pointer is not used.

Note

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

Figure 9-11

Redirection concept

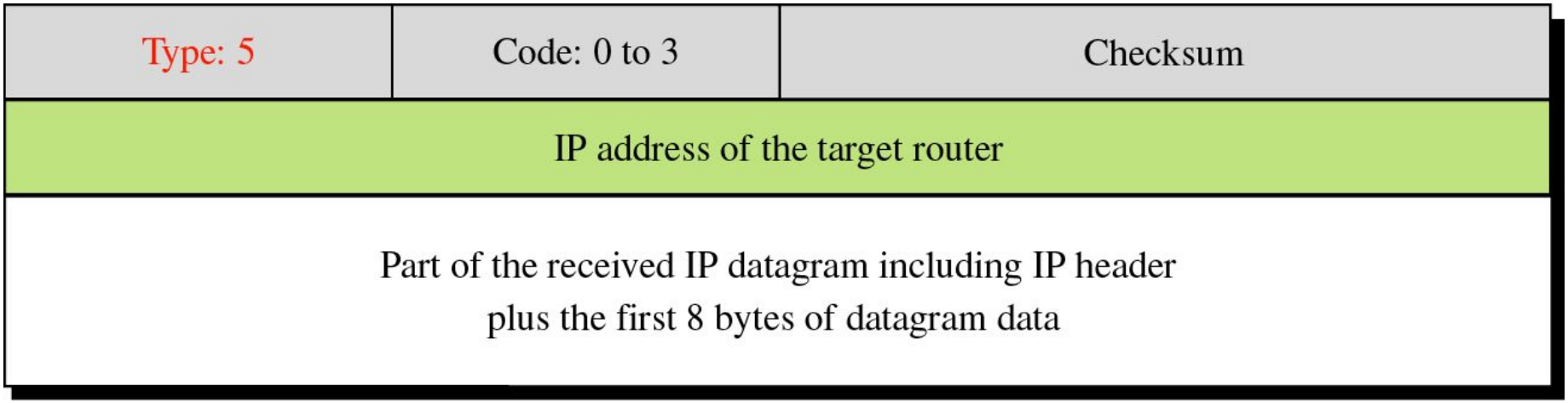


Note

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



- Although the redirection message is considered an error-reporting message, it is different from other error messages.
- The router does not discard the datagram in this case; it is sent to the appropriate router.
- The code field for the redirection message:
- ❑ **Code 0. Redirection for a network-specific route.**
- ❑ **Code 1. Redirection for a host-specific route.**
- ❑ **Code 2. Redirection for a network-specific route based on a specified type of service.**
- ❑ **Code 3. Redirection for a host-specific route based on a specified type of service.**

Note

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

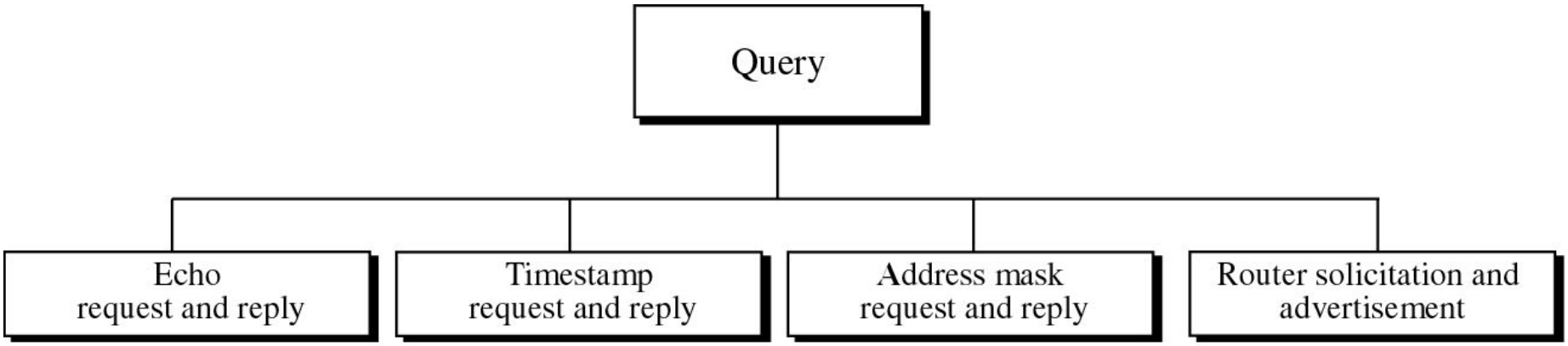
9.4

QUERY

- In addition to error reporting, ICMP can also diagnose some network problems.
- This is accomplished through the query messages.
- A group of five different pairs of messages have been designed for this purpose, but three of these pairs are deprecated today, as we discuss later in the section. Only two pairs are used today: echo request and reply and timestamp request and reply.
- In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node.

Figure 9-13

Query messages



Echo request and echo reply msg

The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.

A host or router can send an echo-request message to another host or router. The host or router that receives an echo-request message creates an echo-reply message and returns it to the original sender.

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.

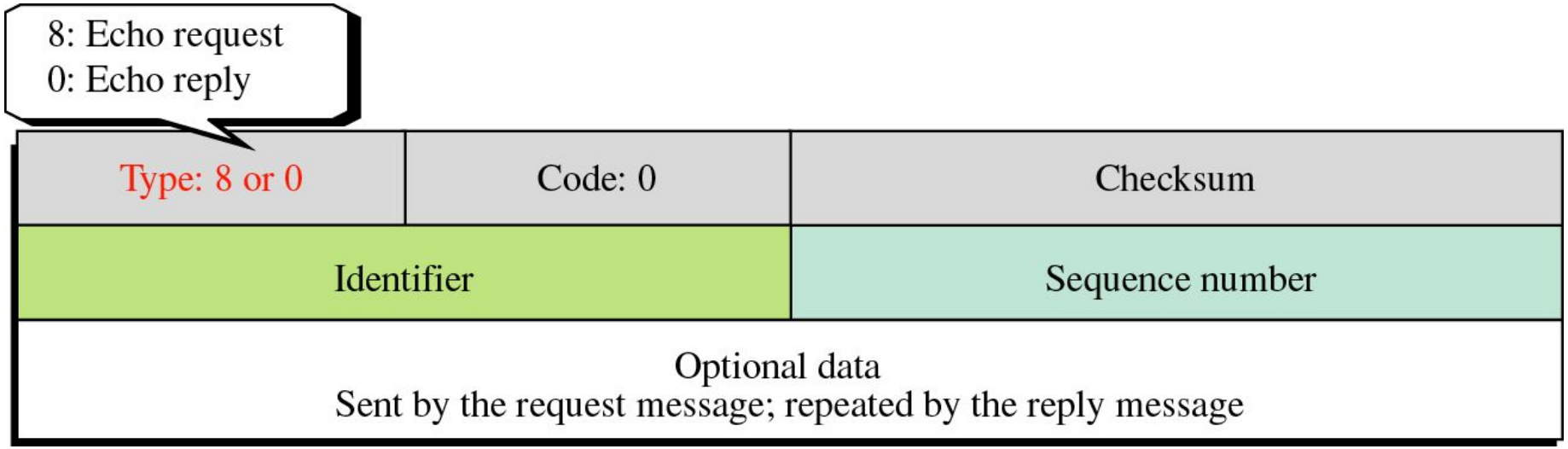
- The echo-request and echo-reply messages can be used to determine if there is communication at the IP level.
- Because ICMP messages are encapsulated in IP datagrams, the receipt of an echo-reply message by the machine that sent the echo request is proof that the IP protocols in the sender and receiver are communicating with each other using the IP datagram.

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



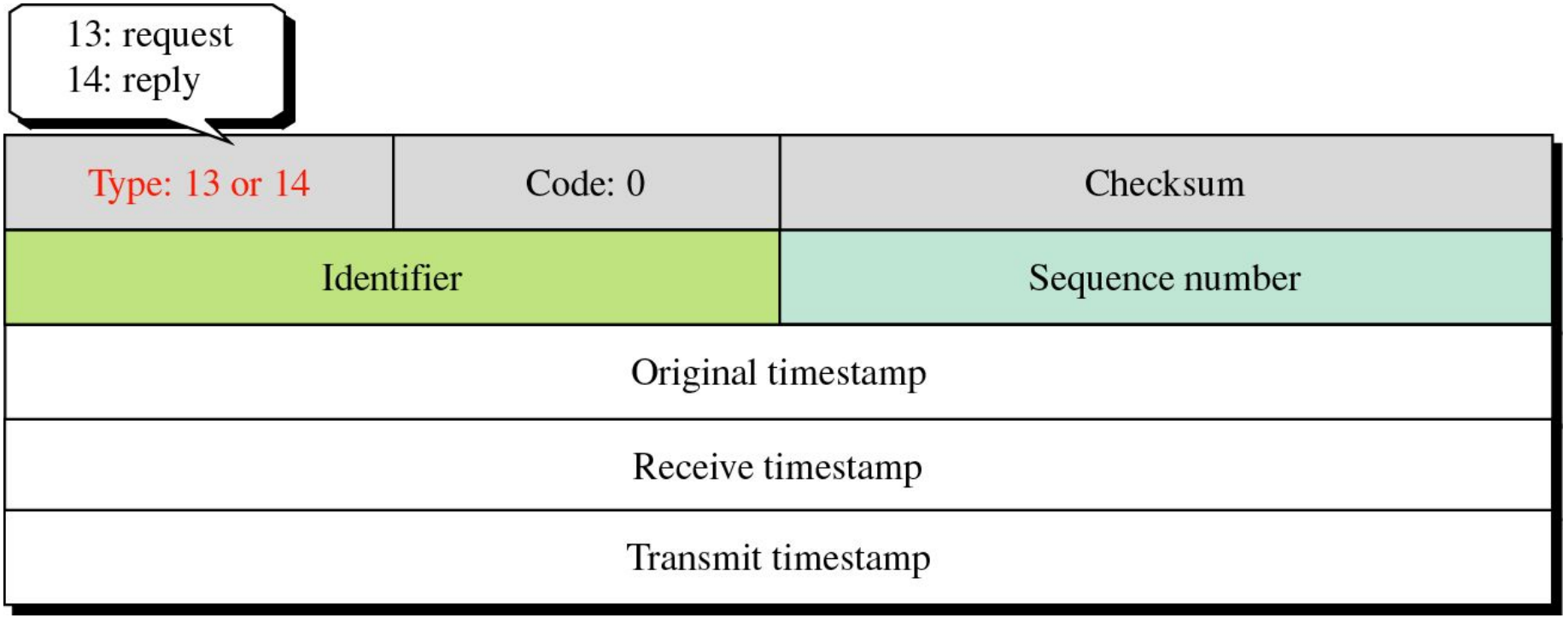
Timestamp request and reply

Note

Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time for an IP datagram to travel between a source and a destination machine.

Figure 9-15

Timestamp-request and timestamp-reply message format



- The source creates a timestamp-request message. The source fills the *original timestamp field with departure time*. *The other* two timestamp fields are filled with zeros.

- The destination creates the timestamp-reply message. The destination copies the original timestamp value from the request message into the same field in its reply message.

- It then fills the *receive timestamp field with* the time the request was received.

- Finally, it fills the *transmit timestamp field* with time at which the reply message departs.

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

Given the following information:

Value of original timestamp: 46

Value of receive timestamp: 59

Value of transmit timestamp: 60

Time the packet arrived: 67

- Calculate ::::::
- sending time ,
- recvng time,
- round trip time

We can calculate:

Sending time = 59 − 46 = 13 milliseconds

Receiving time = 67 − 60 = 7 milliseconds

Round-trip time = 13 + 7 = 20 milliseconds

the timestamp-request and timestamp-reply messages can also be used to synchronize the clocks in two machines using the following formula:

$$\text{Time difference} = \text{receive timestamp} - (\text{original timestamp field} + \text{one-way time duration})$$

For example, we can tell that the two clocks in the previous example are 3 milliseconds out of synchronization because

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

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

Address-Mask Request and Reply

A host may know its IP address, but it may not know the corresponding mask. For example, a host may know its IP address as 159.31.17.24, but it may not know that the corresponding mask is /24.

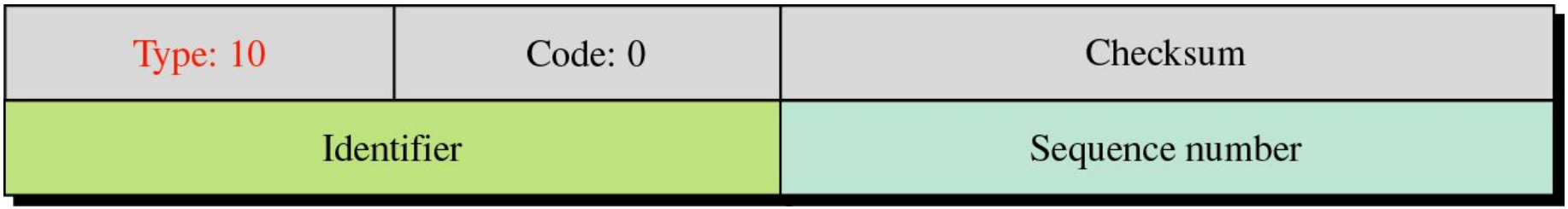
To obtain its mask, a host sends an **address-mask-request message** to a router on the LAN. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message. The router receiving the address-mask-request message responds with an **address-mask-reply message,** providing the necessary mask for the host. This can be applied to its full IP address to get its subnet address.

The format of the address-mask request and address-mask reply is shown in Figure 9.16. The address-mask field is filled with zeros in the request message. When the router sends the address-mask reply back to the host, this field contains the actual mask (1s for the netid and subnetid and 0s for the hostid).

Masking is needed for diskless stations at start-up time. When a diskless station comes up for the first time, it may ask for its full IP address using the RARP protocol (see Chapter 7); after receiving its IP address, it may use the address-mask request and reply to find out which part of the address defines the subnet.

Figure 9-17

Router solicitation message format



Router Solicitation and Advertisement

As we discussed in the redirection message section, a host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. The **router-solicitation and router-advertisement messages** can help in this situation. A host can broadcast (or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message. A router can also periodically send router-advertisement messages even if no host has solicited. Note that when a router sends out an advertisement, it announces not only its own presence but also the presence of all routers on the network of which it is aware. Figure 9.17 shows the format of the router-solicitation message.

Figure 9-18

Router advertisement message format

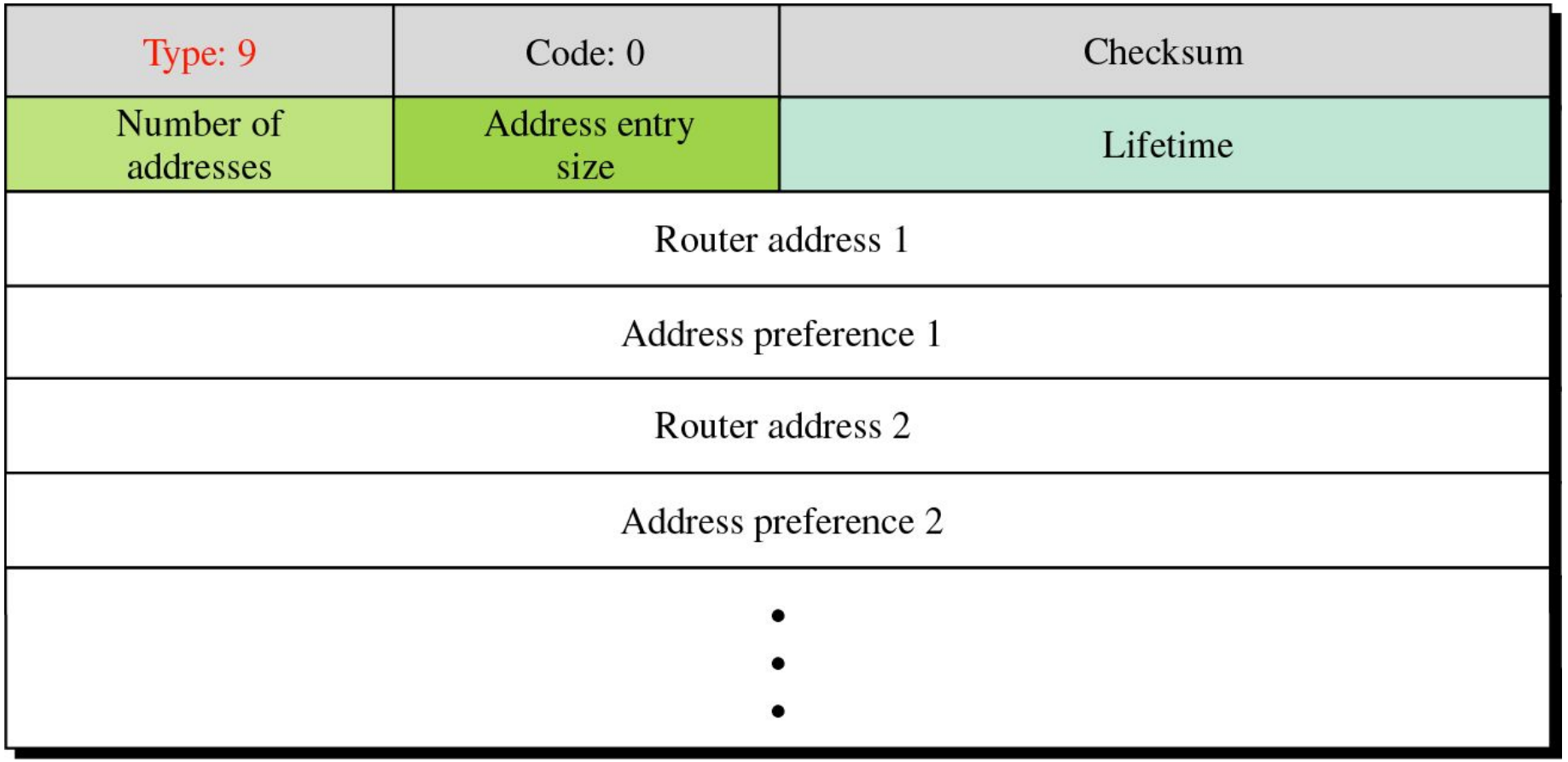


Figure 9.18 shows the format of the router-advertisement message. The lifetime field shows the number of seconds that the entries are considered to be valid. Each router entry in the advertisement contains at least two fields: the router address and the address preference level. The address preference level defines the ranking of the router. The preference level is used to select a router as the default router. If the address preference level is zero, that router is considered the default router. If the address preference level is 80000000_{16}, the router should never be selected as the default router.