Chapter 9

Internet Control Message Protocol Version 4 (ICMPv4)

9-1 INTRODUCTION

The IP protocol has no error-reporting or error correcting mechanism. What happens if something goes wrong? 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? These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host.

Topics Discussed in the Section

- ✓ **The position of ICMP in the TCP/IP suite**
- ✓ **Encapsulation of ICMP Packets**

Figure 9.1 *Position of ICMP in the network layer*

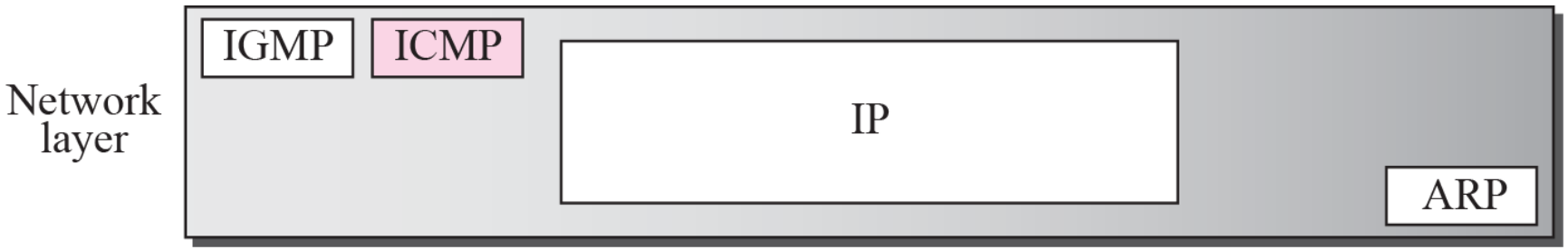
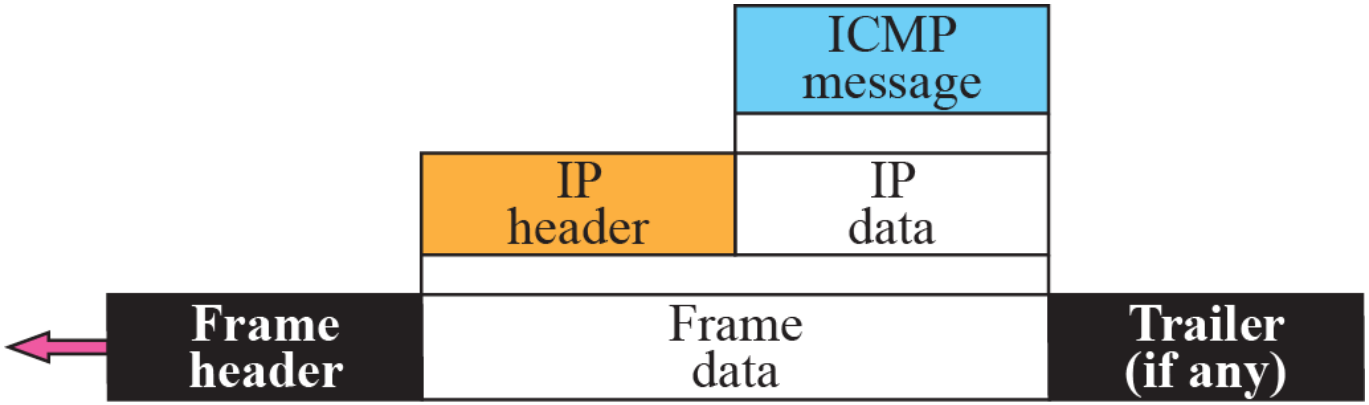


Figure 9.2 *ICMP encapsulation*



9-2 MESSAGES

ICMP messages are divided into two broad categories: error-reporting messages and query messages.

- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

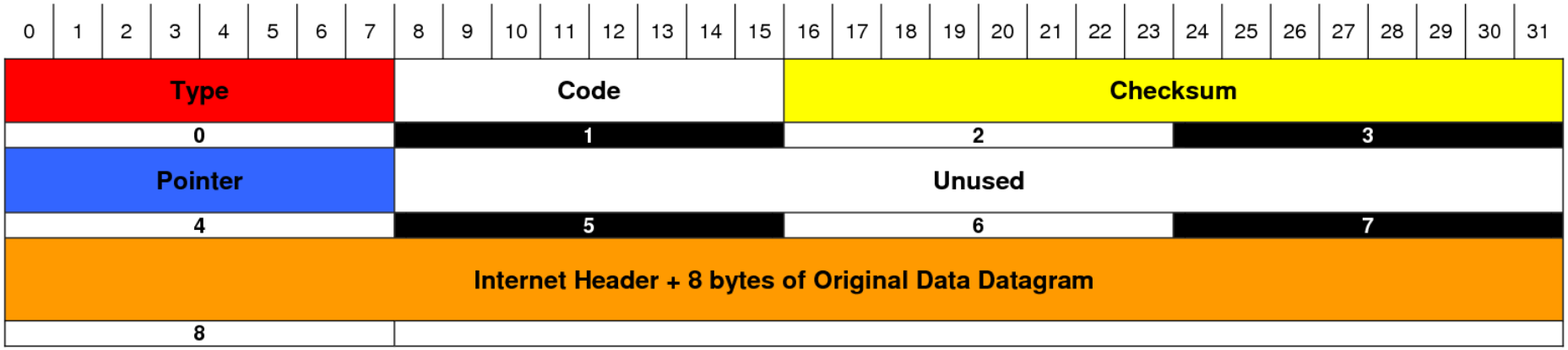
Topics Discussed in the Section

- ✓ **Message Format**
- ✓ **Error Reporting Messages**
- ✓ **Query Messages**
- ✓ **Checksum**

Table 9.1 *ICMP messages*

Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

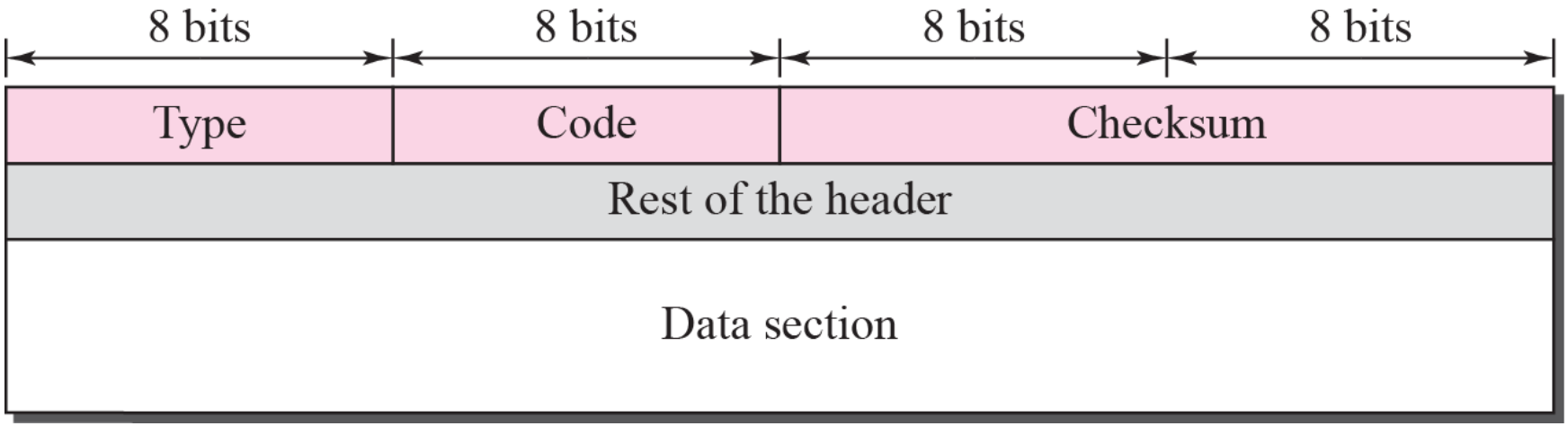
ICMP Parameter Message Format

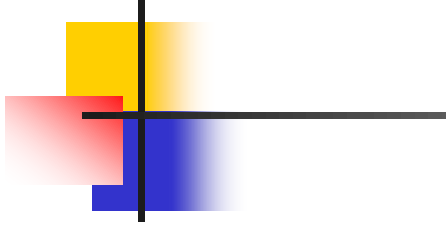


Type	Code	Meaning
0	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication admin prohibited
4	0	Source Quench (Slow down/Shut up)

Type	Code	Meaning
5	0	Redirect datagram for the network
	1	Redirect datagram for the host
	2	Redirect datagram for the TOS & Network
	3	Redirect datagram for the TOS & Host
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	Time To Live exceeded in transit
	1	Fragment reassemble time exceeded
12	0	Pointer indicates the error (Parameter Problem)
	1	Missing a required option (Parameter Problem)
	2	Bad length (Parameter Problem)
13	0	Time Stamp
14	0	Time Stamp Reply
15	0	Information Request
16	0	Informaiton Reply
17	0	Address Mask Request
18	0	Address Mask Reply
30	0	Traceroute (Tracert)

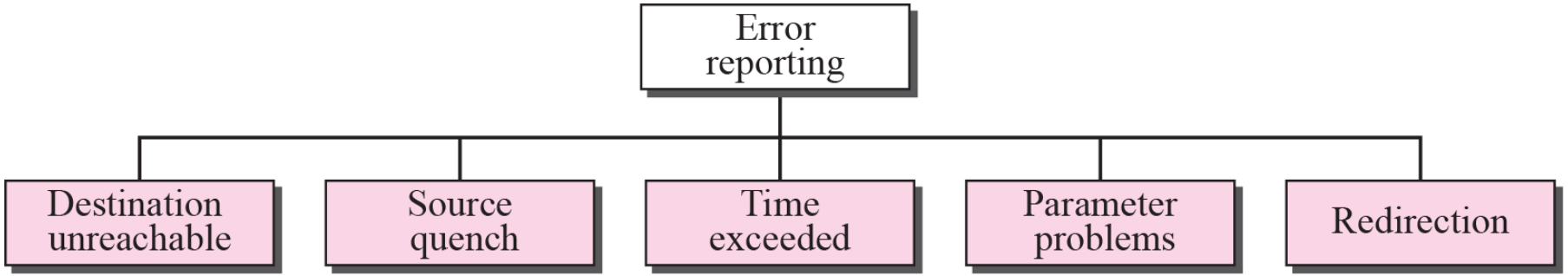
Figure 9.3 *General format of ICMP messages*





ICMP always reports error messages to the original source.

Figure 9.4 *Error-reporting messages*

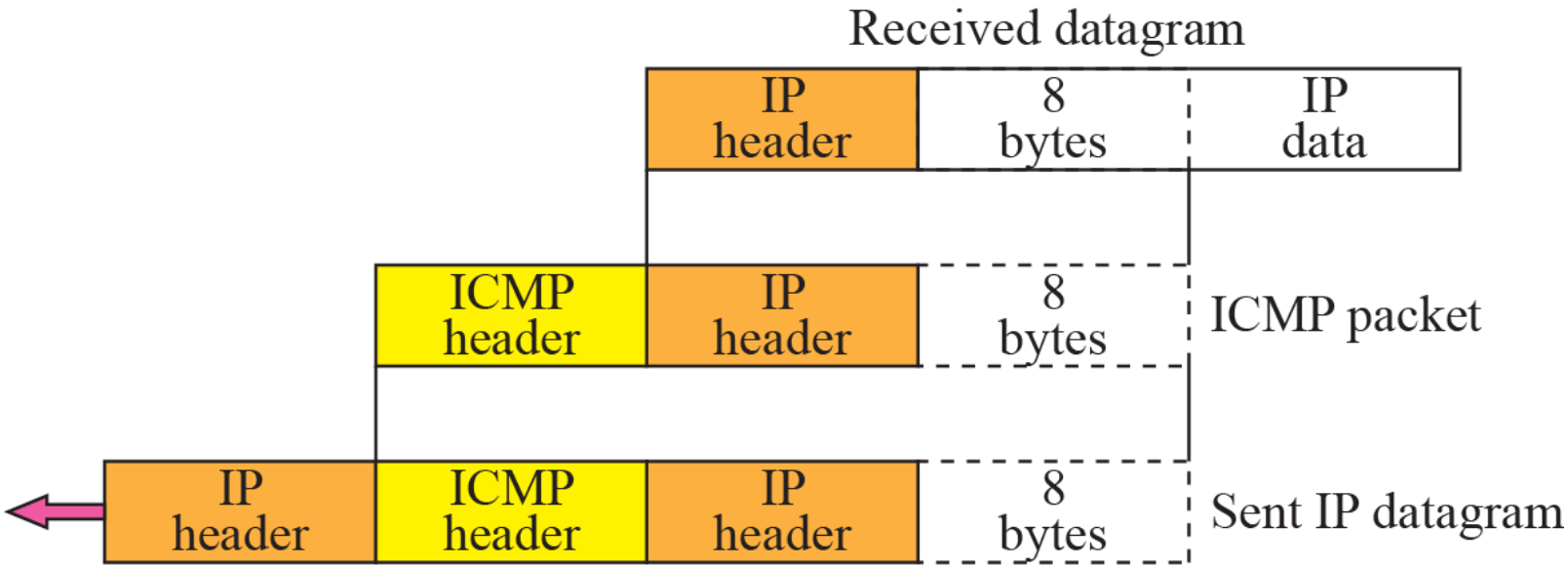


Important Points:

No ICMP error messages are generated for:

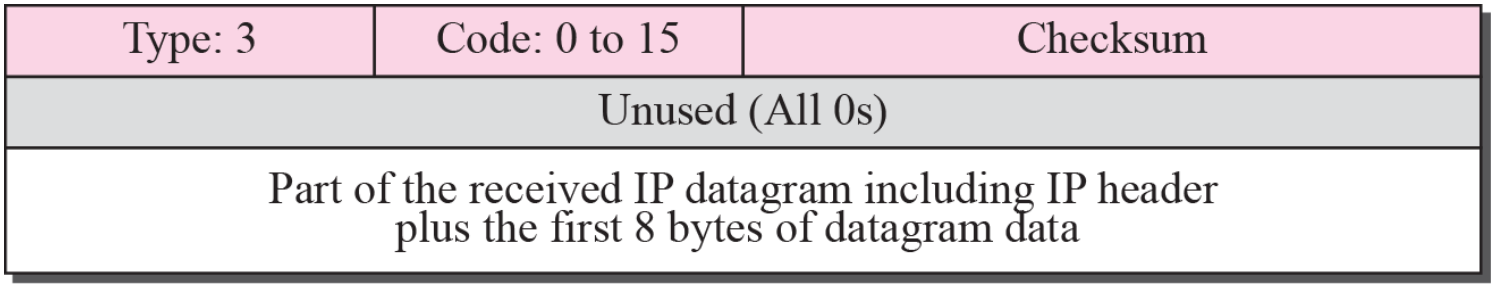
- Datagram carrying a ICMP error message.
- Fragmented datagram that is not the first fragment.
- Multicast address
- Datagram having special address such as loopback or 0.0.0.0

Figure 9.5 *Contents of data field for the error message*



TCP & UDP Header

Figure 9.6 *Destination-unreachable format*



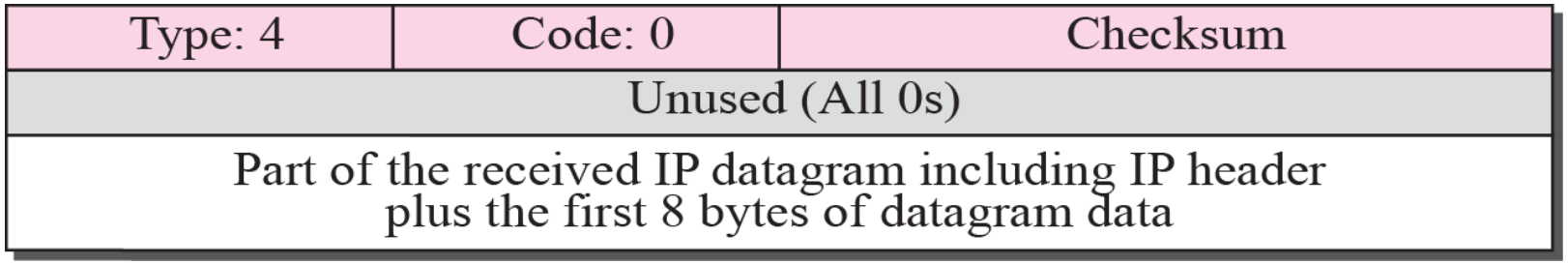
Destination-unreachable messages with codes 2 or 3 can be created only by the destination host.

Other destination-unreachable messages can be created only by routers.

Source Quench

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

Figure 9.7 *Source-quench format*



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.

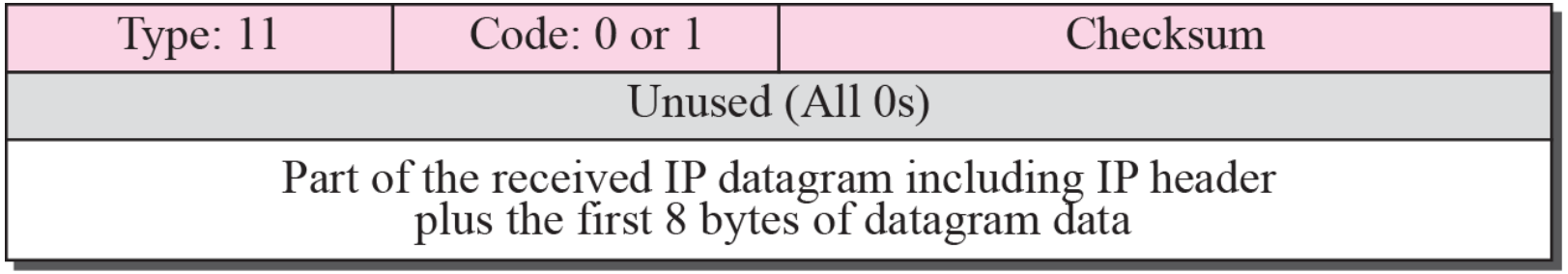
One source-quench message is sent for each datagram that is discarded due to congestion.

Time Exceeded:

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

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.

Figure 9.8 *Time-exceeded message format*



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.

Parameter Problem

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

Figure 9.9 *Parameter-problem message format*

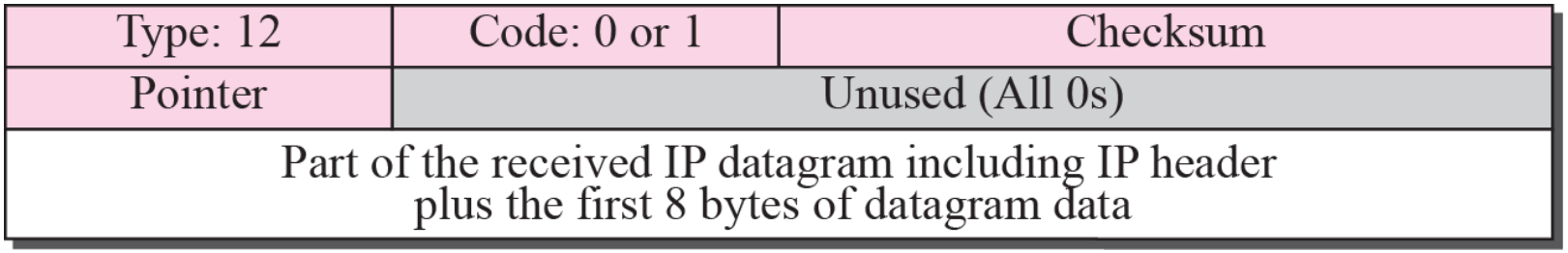
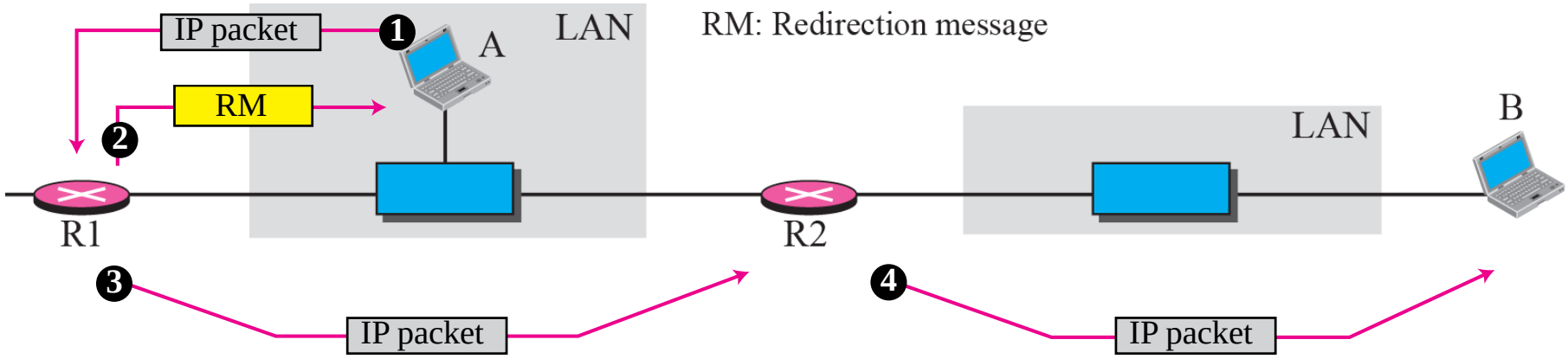


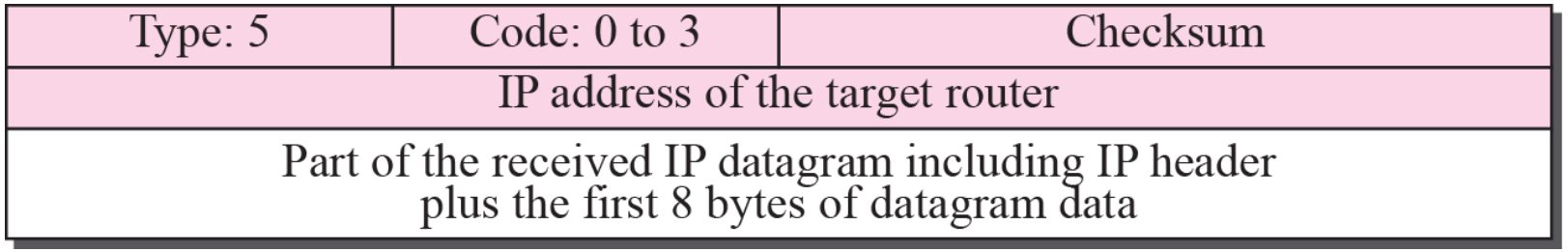
Figure 9.10 *Redirection concept*



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 9.11 *Redirection message format*

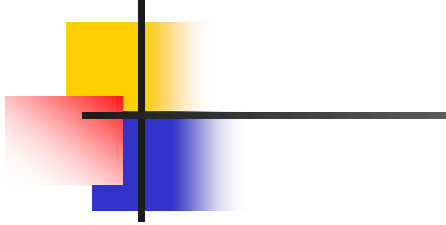


A redirection message is sent from a router to a host on the same local network.

Echo Request and Reply

An echo-request message can be sent by a host or router.

An echo-reply message is sent by the host or router that receives an echo-request message.



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

Echo-request and echo-reply messages can test the reachability of a host.

This is usually done by invoking the ping command.

Figure 9.12 *Echo-request and echo-reply message*

Type 8: Echo request
Type 0: Echo reply

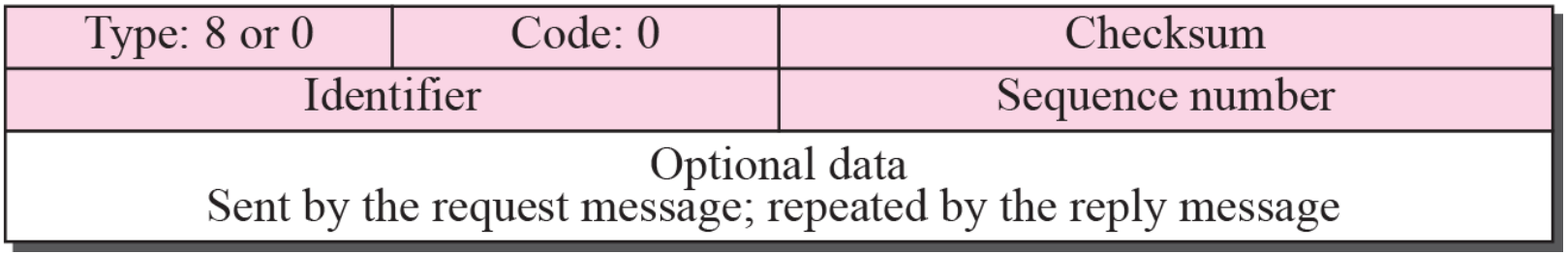
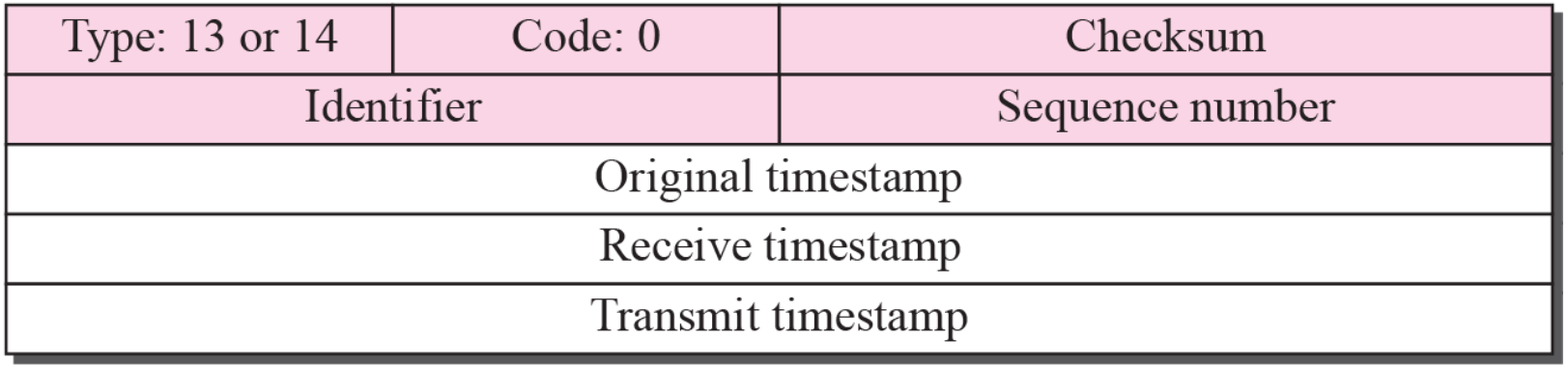


Figure 9.13 *Timestamp-request and timestamp-reply message format*

Type 13: request
Type 14: reply



Timestamp-request and Reply message

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.

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.