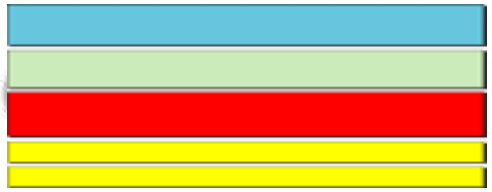


Internet Control Message Protocol

Objectives

Upon completion you will be able to:

- *Be familiar with the ICMP message format*
- *Know the types of error reporting messages*
- *Know the types of query messages*
- *Be able to calculate the ICMP checksum*
- *Know how to use the ping and traceroute commands*
- *Understand the modules and interactions of an ICMP package*

Figure 1 *Position of ICMP in the network layer*

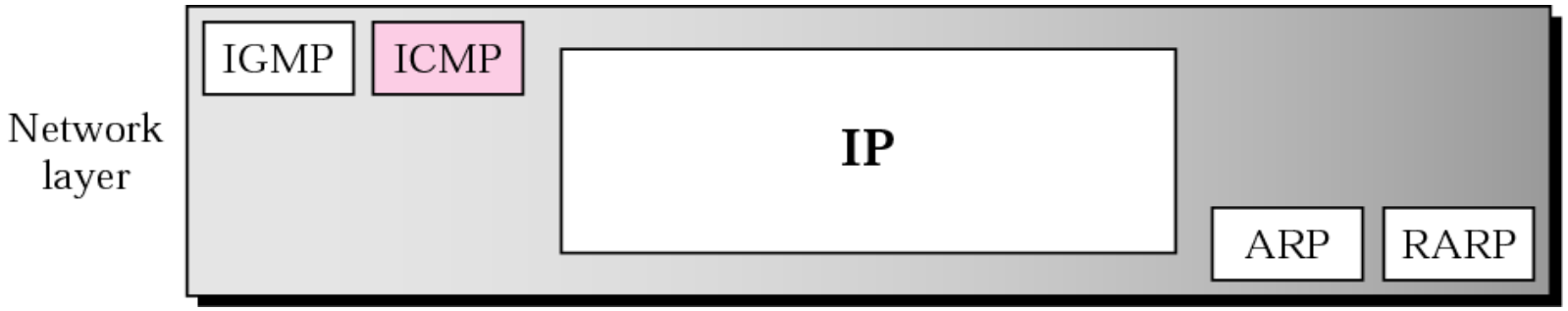
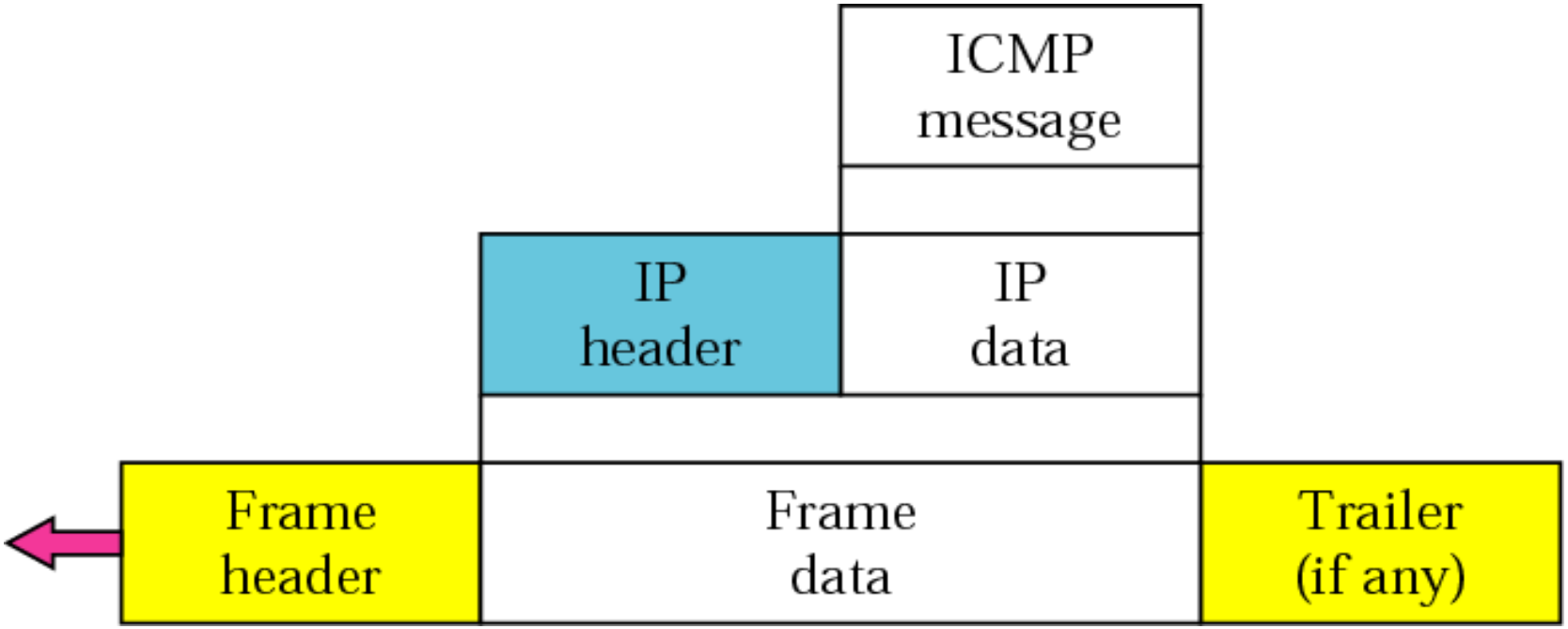


Figure 9.2 *ICMP encapsulation*



9.1 TYPES OF MESSAGES

ICMP messages are divided into error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter. The query messages get specific information from a router or another host.

Figure 9.3 *ICMP messages*

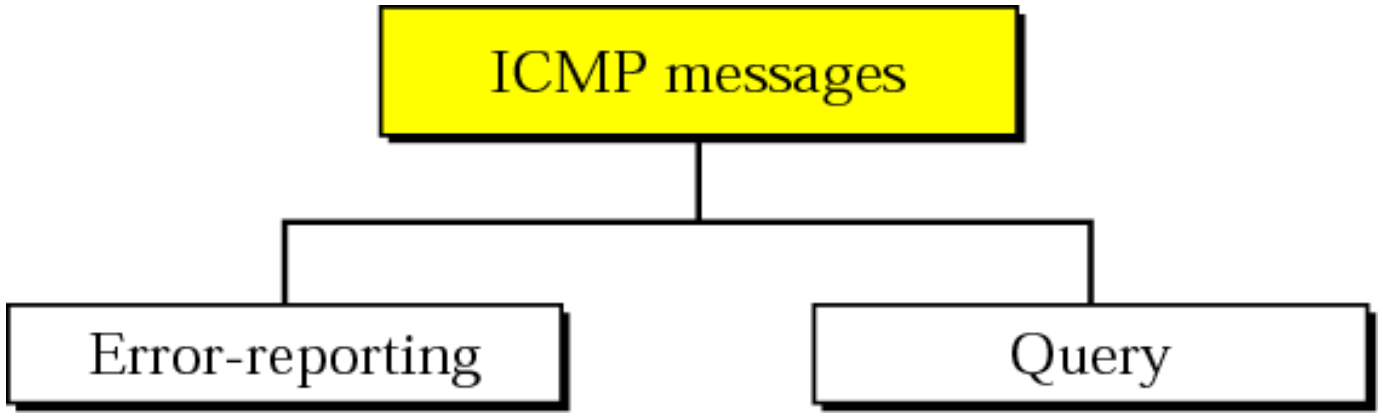


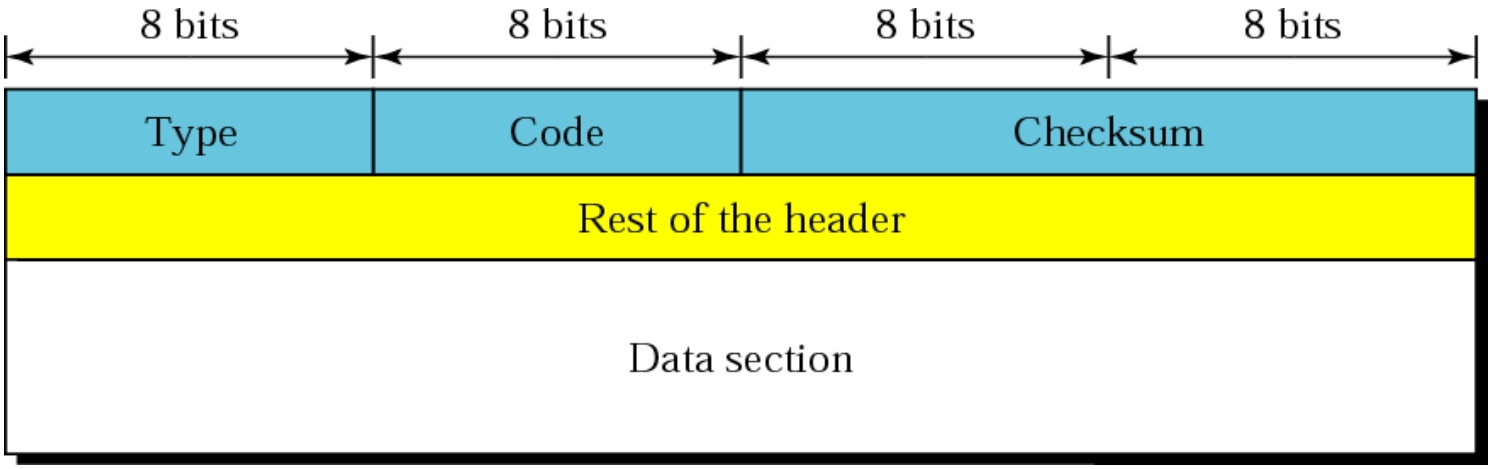
Table 9.1 ICMP messages

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
	17 or 18	Address mask request or reply
	10 or 9	Router solicitation or advertisement

9.2 MESSAGE FORMAT

An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all.

Figure 9.4 *General format of ICMP messages*



9.3 ERROR REPORTING

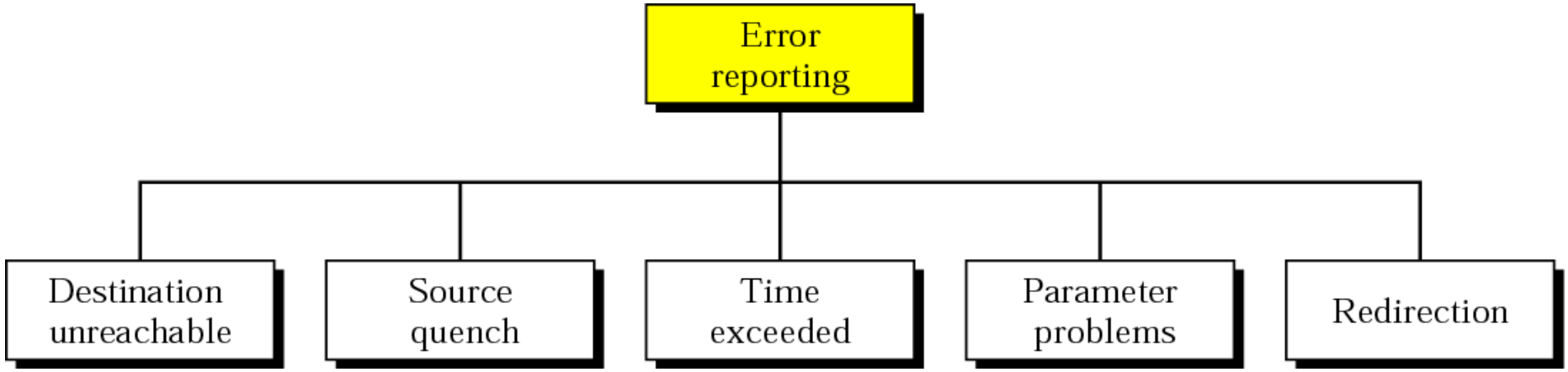
IP, as an unreliable protocol, is not concerned with error checking and error control. ICMP was designed, in part, to compensate for this shortcoming. ICMP does not correct errors, it simply reports them.

The topics discussed in this section include:

Destination Unreachable
Source Quench
Time Exceeded
Parameter Problem
Redirection

ICMP always reports error messages to the original source.

Figure 9.5 *Error-reporting messages*



Note:

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 9.6 *Contents of data field for the error messages*

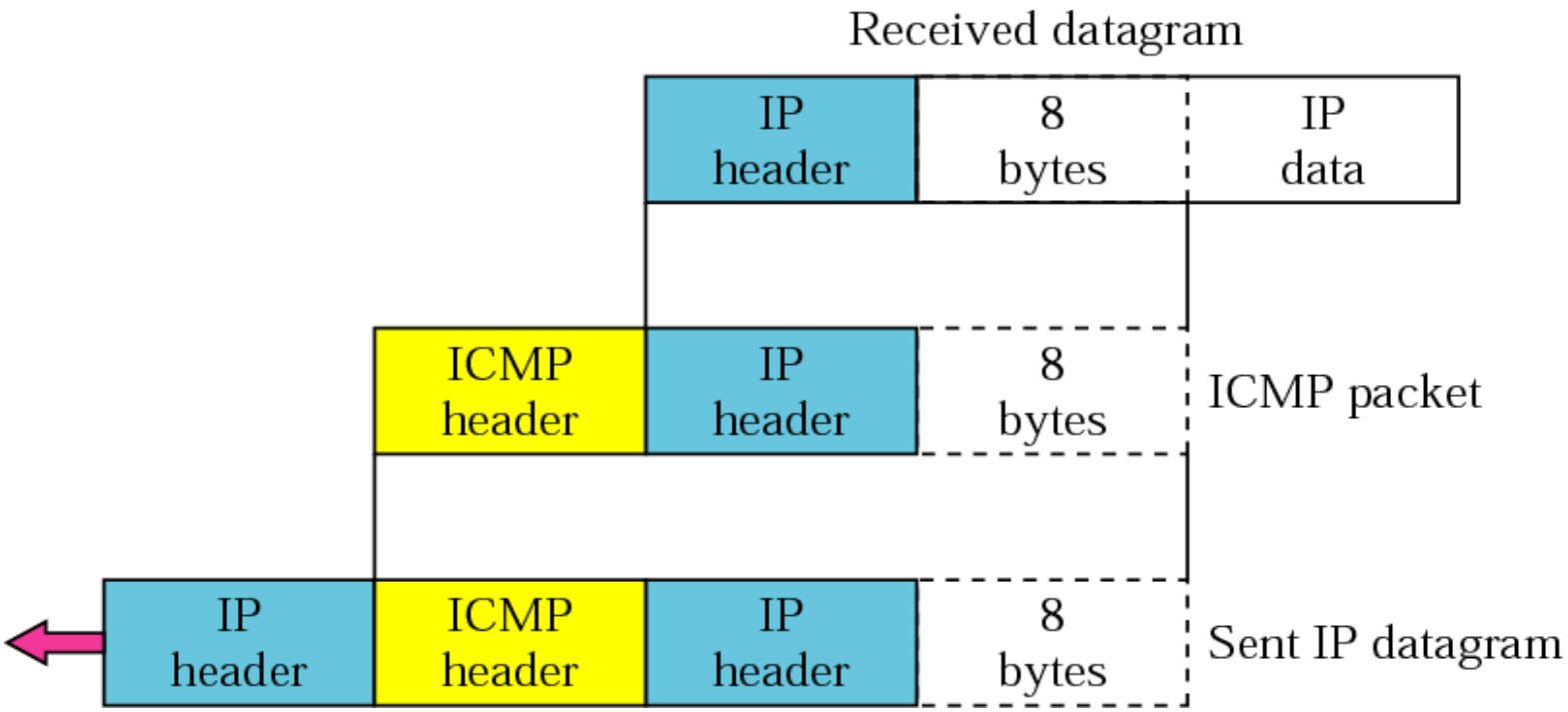
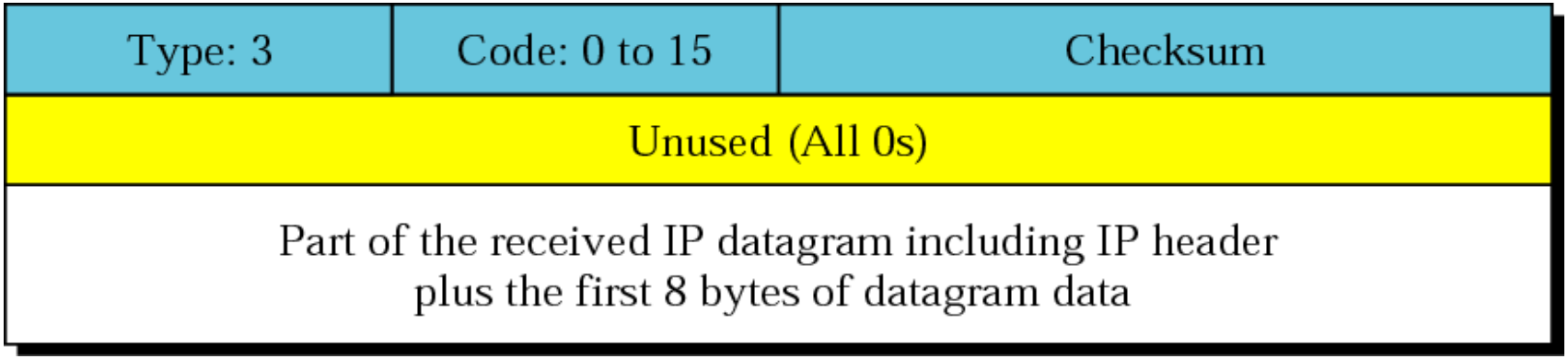


Figure 9.7 *Destination-unreachable format*



Note:

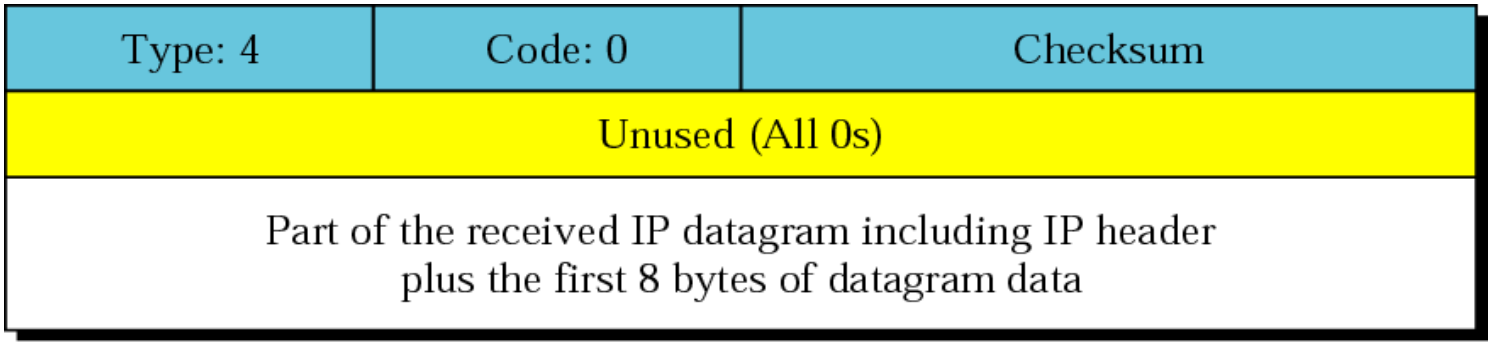
Destination-unreachable messages with codes 2 or 3 can be created only by the destination host.

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

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

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.

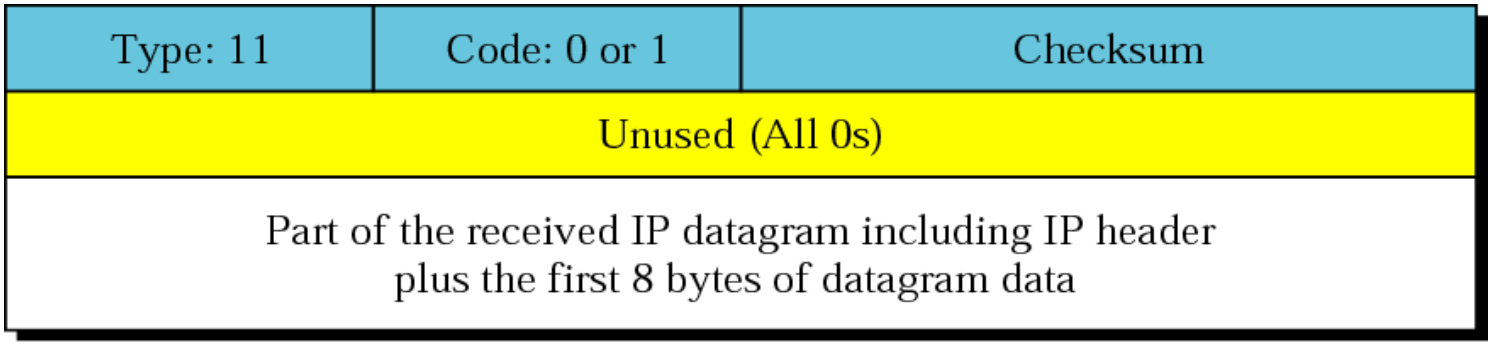
One source-quench message is sent for each datagram that is discarded due to congestion.

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.

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*



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

Figure 9.10 *Parameter-problem message format*

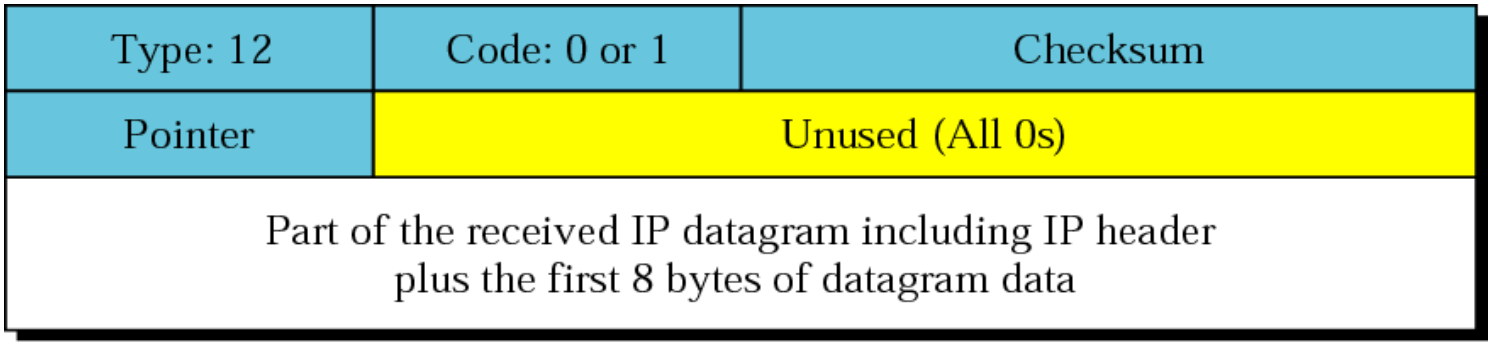
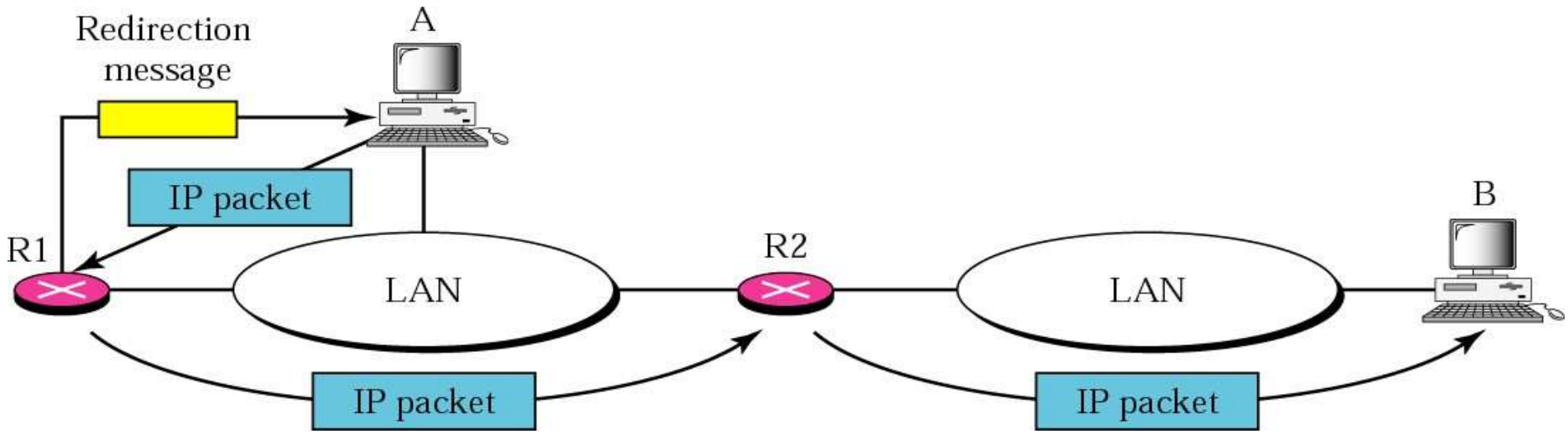
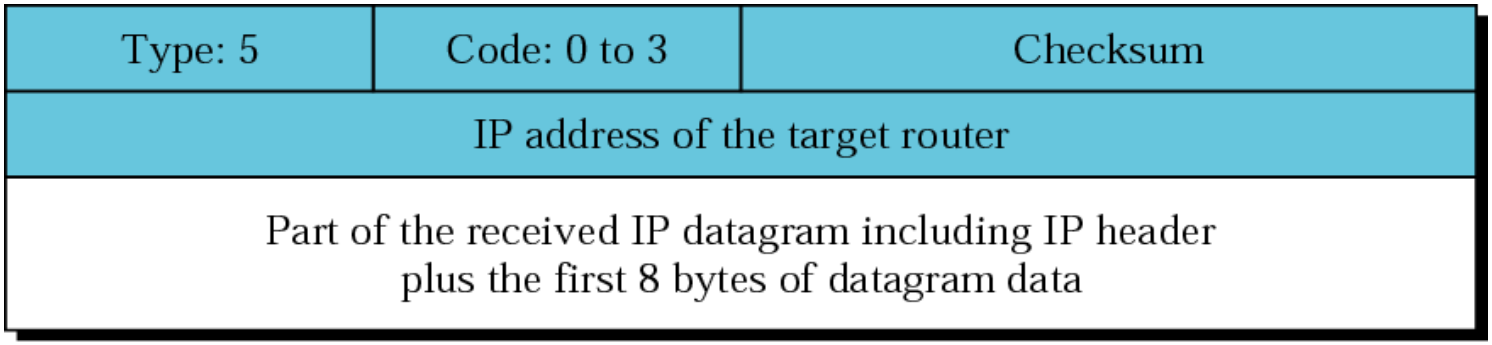


Figure 9.11 *Redirection concept*



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 9.12 *Redirection message format*



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

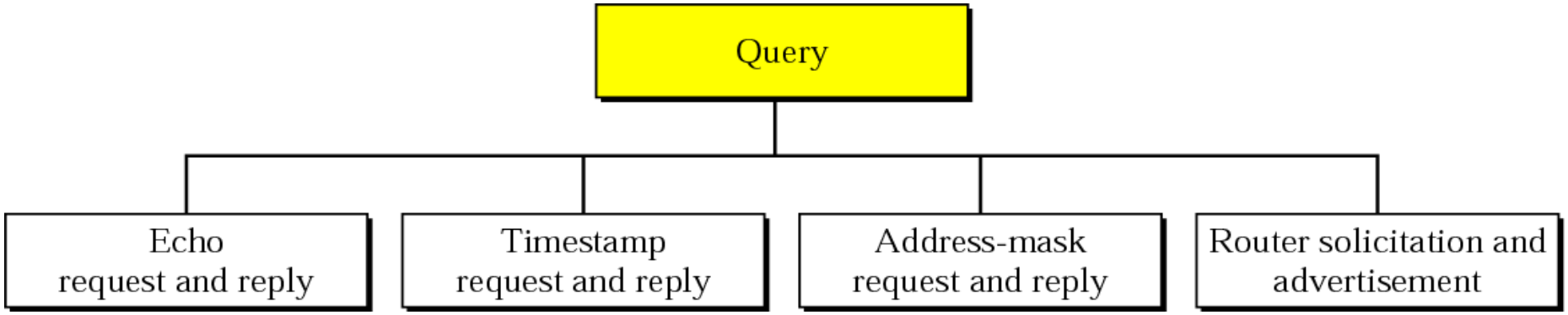
9.4 QUERY

ICMP can also diagnose some network problems through the query messages, a group of four different pairs of messages. In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node.

The topics discussed in this section include:

Echo Request and Reply
Timestamp Request and Reply
Address-Mask Request and Reply
Router Solicitation and Advertisement

Figure 9.13 *Query messages*



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.

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 9.14 *Echo-request and echo-reply messages*

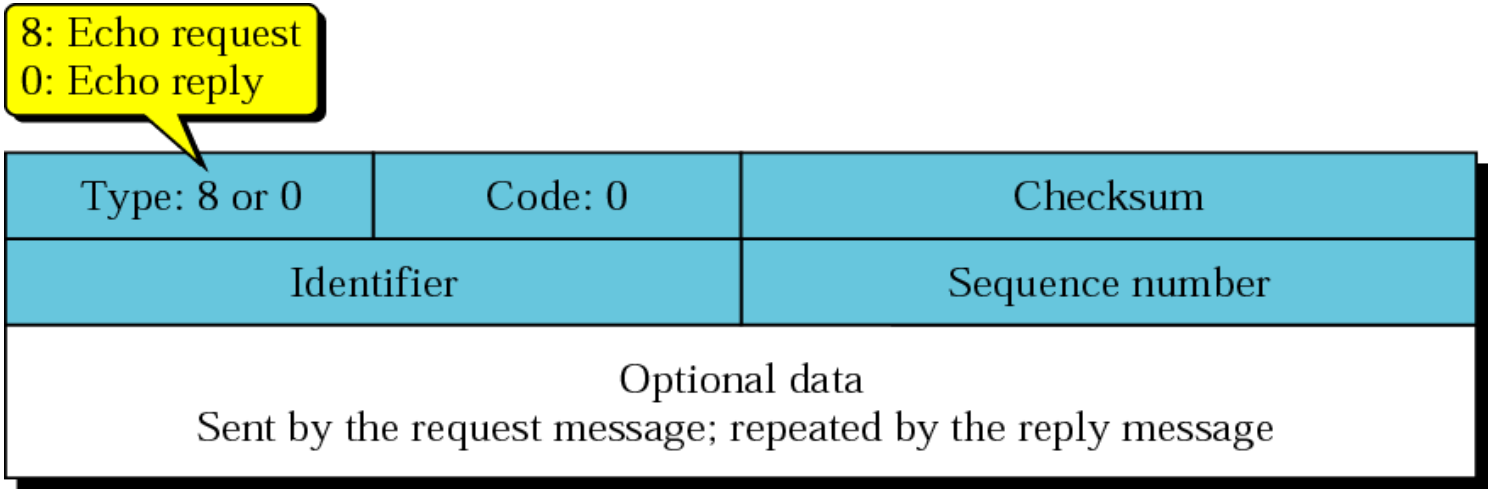
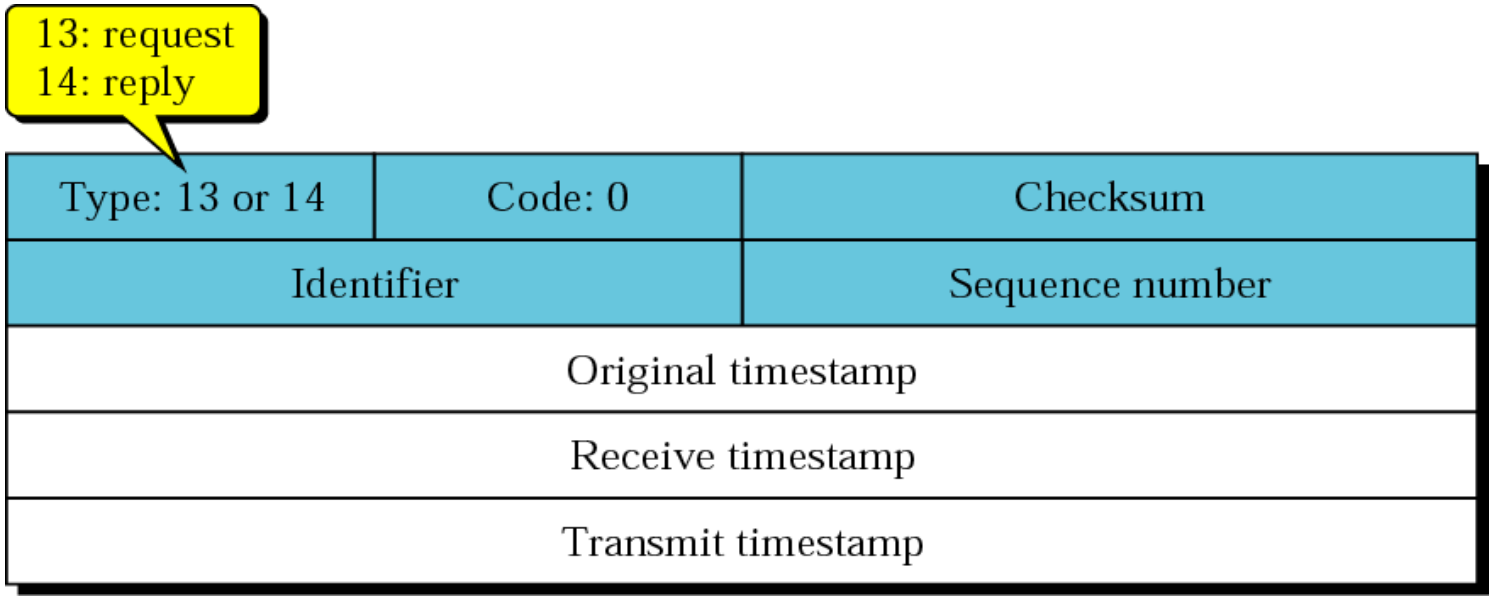


Figure 9.15 *Timestamp-request and timestamp-reply message format*



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.

Figure 9.16 *Mask-request and mask-reply message format*

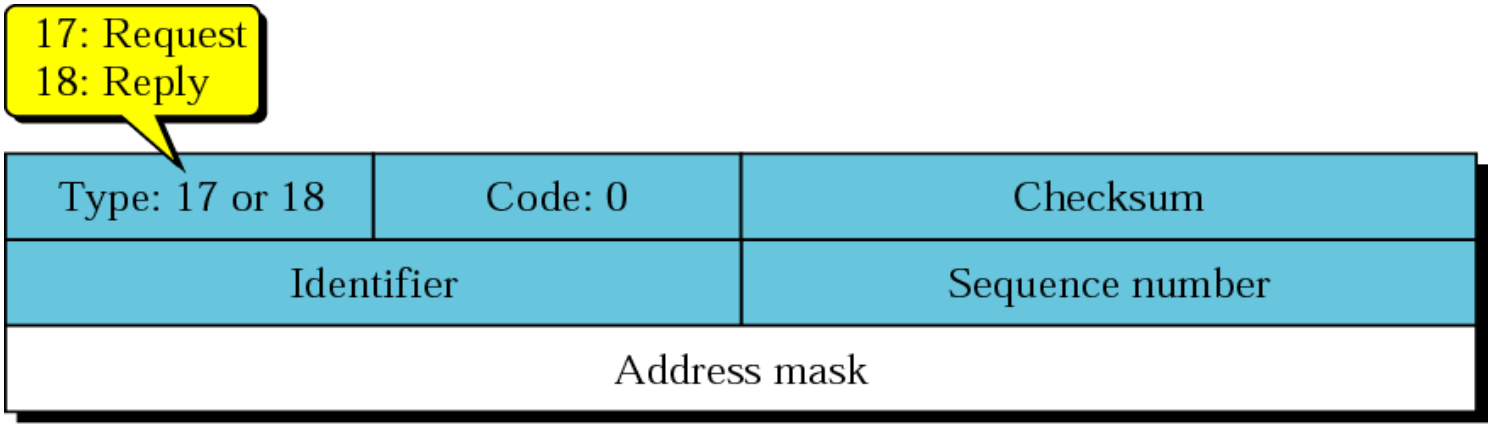
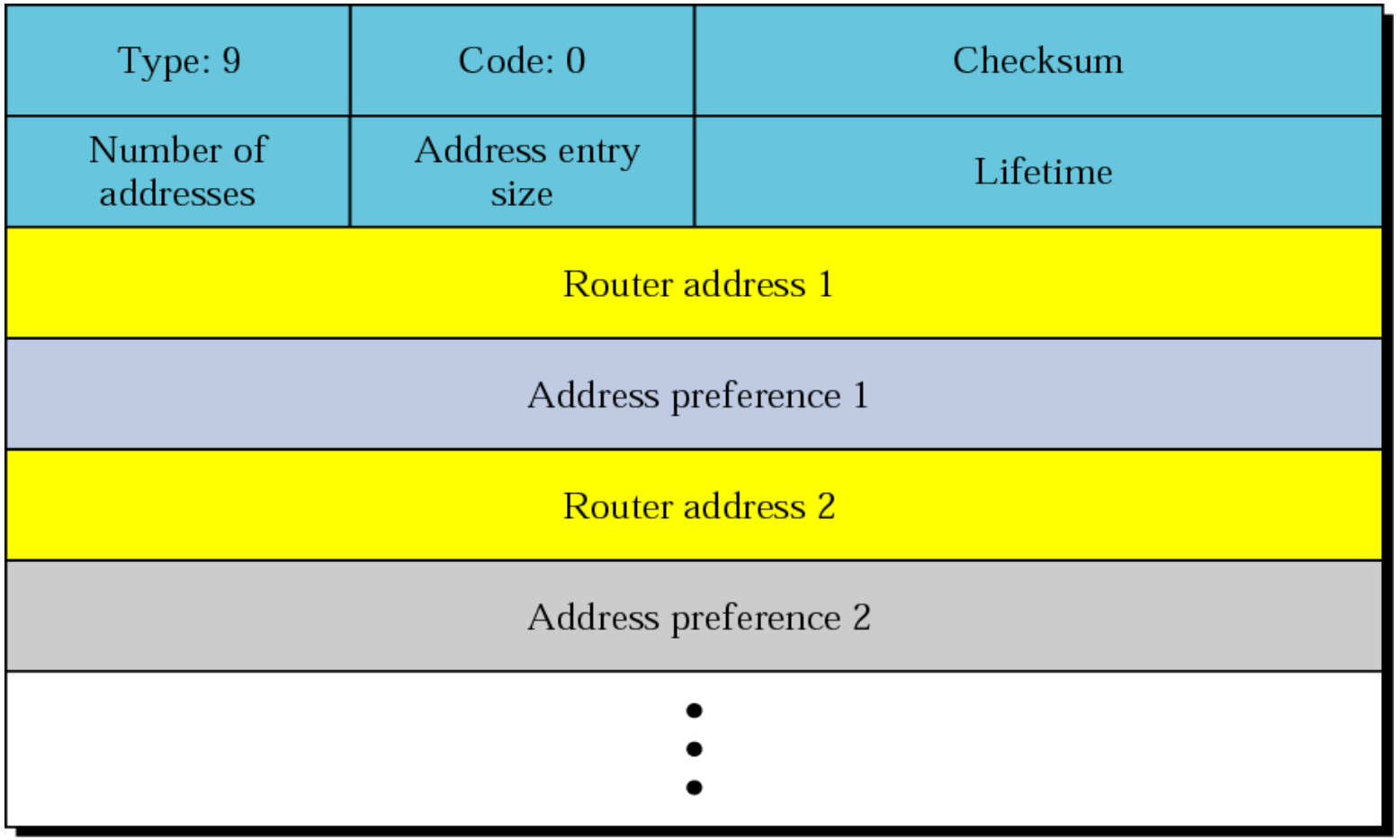


Figure 9.17 *Router-solicitation message format*

Figure 9.18 *Router-advertisement message format*



9.5 CHECKSUM

In ICMP the checksum is calculated over the entire message (header and data).

The topics discussed in this section include:

Checksum Calculation

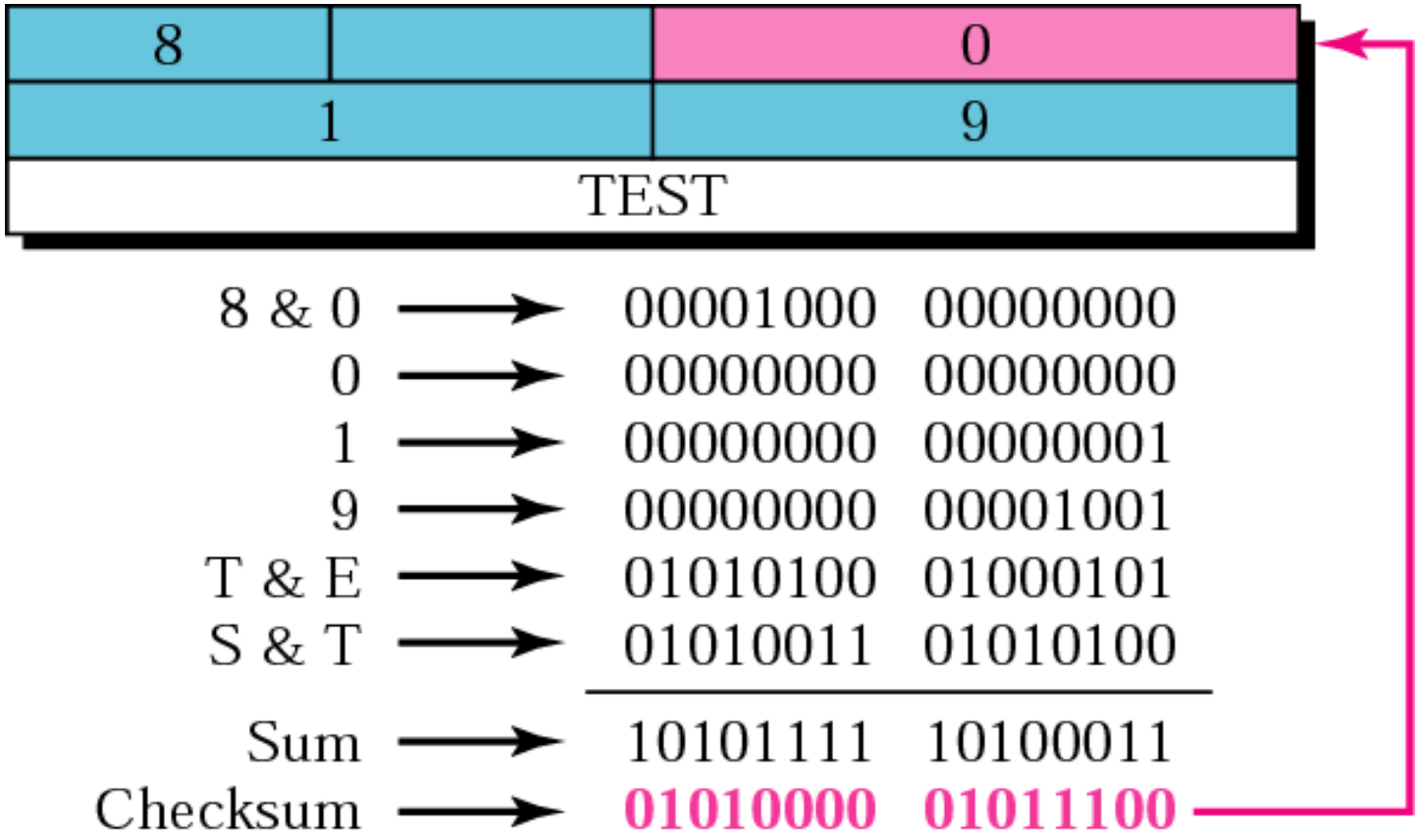
Checksum Testing

EXAMPLE 1

Figure 9.19 shows an example of checksum calculation for a simple echo-request message (see Figure 9.14). We randomly chose the identifier to be 1 and the sequence number to be 9. The message is divided into 16-bit (2-byte) words. The words are added together and the sum is complemented. Now the sender can put this value in the checksum field.

See Next Slide

Figure 9.19 *Example of checksum calculation*



9.6 DEBUGGING TOOLS

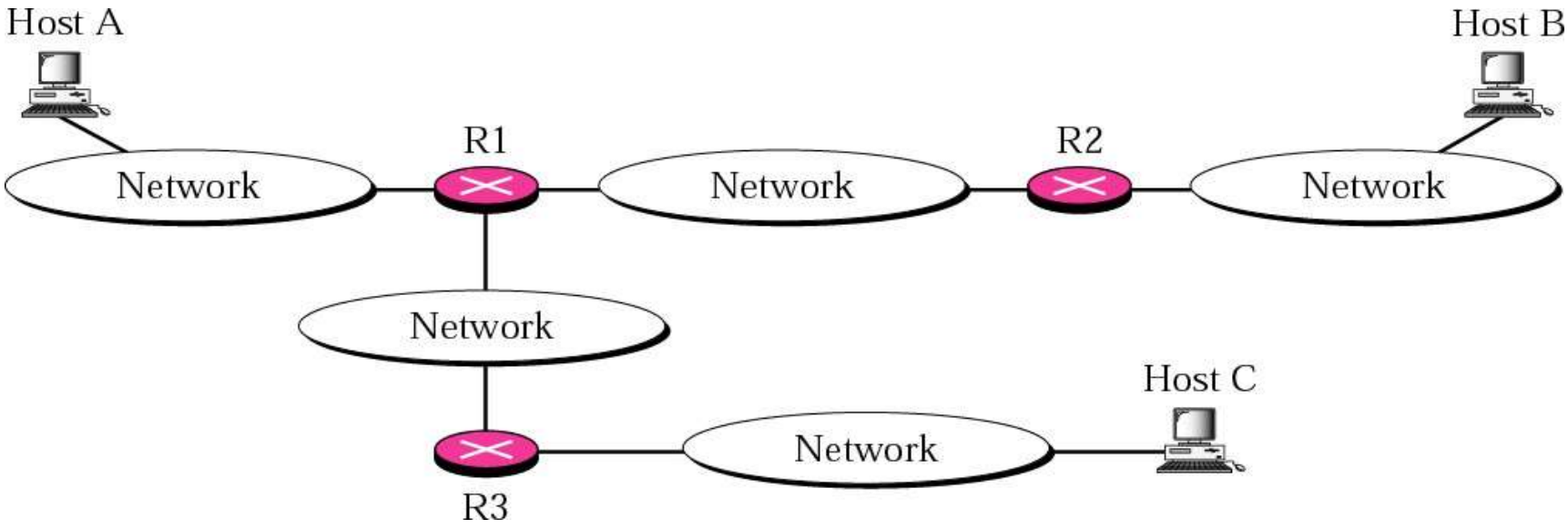
We introduce two tools that use ICMP for debugging: ping and traceroute.

The topics discussed in this section include:

Ping

Traceroute

Figure 9.20 *The traceroute program operation*



9.7 ICMP PACKAGE

To give an idea of how ICMP can handle the sending and receiving of ICMP messages, we present our version of an ICMP package made of two modules: an input module and an output module.

The topics discussed in this section include:

Input Module
Output Module

Figure 9.21 *ICMP package*