Internet Control Message Protocol

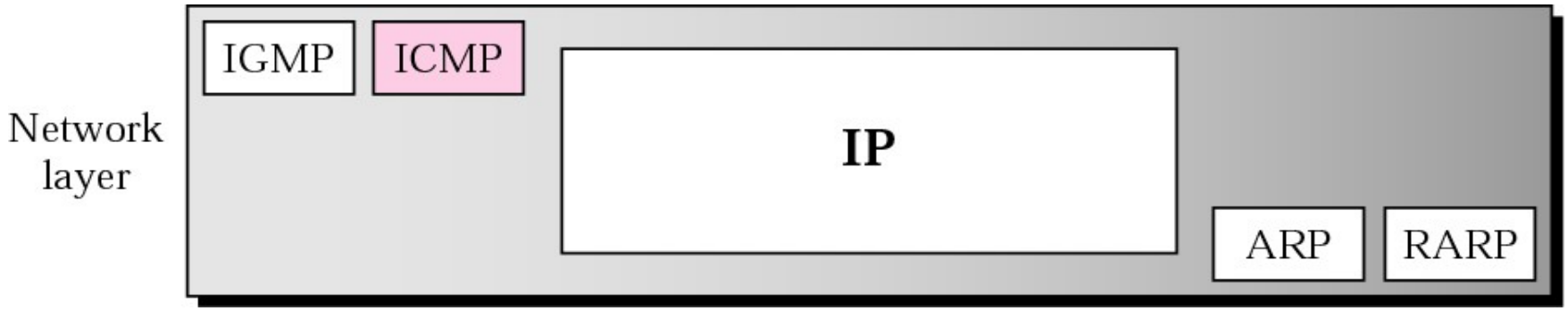
Objectives

Upon completion you will be able to:

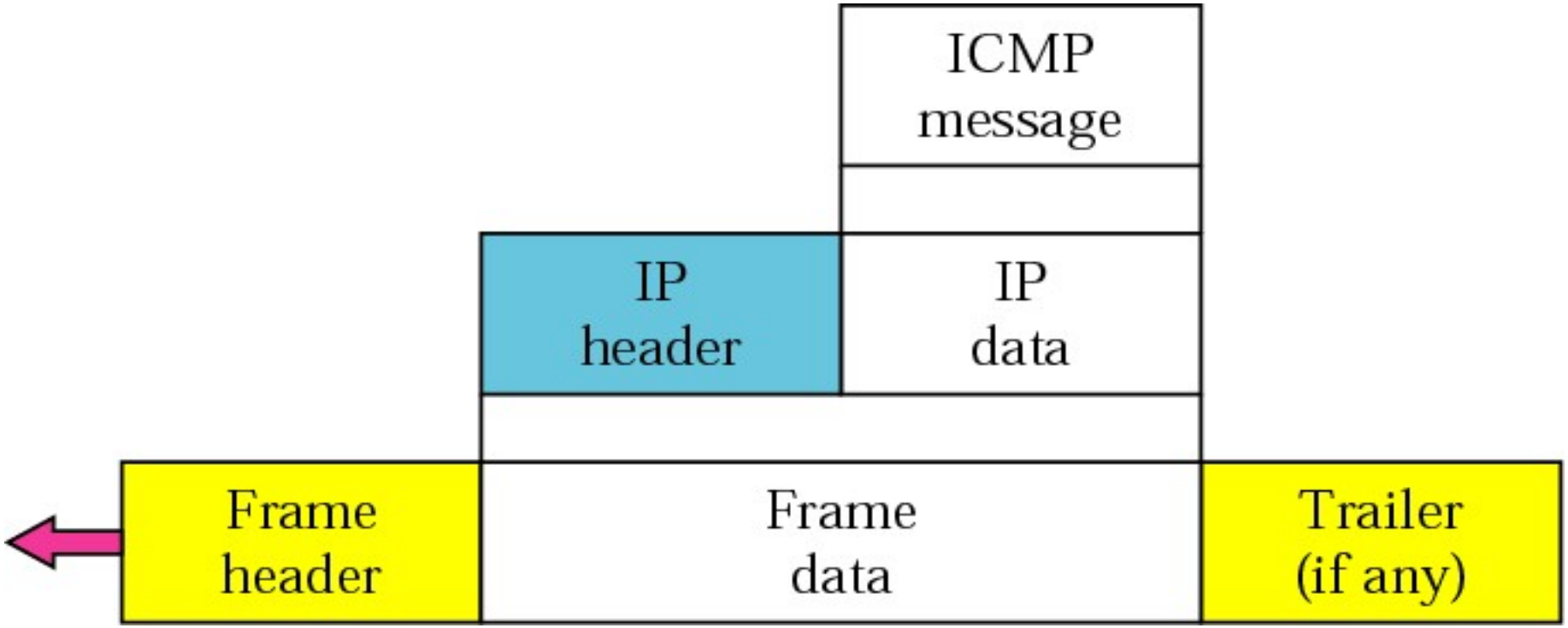
- ***Be familiar with the ICMP message format***
- ***Know the types of error reporting messages***
- ***Know the types of query messages***
- ***Be able to calculate the ICMP checksum***
- ***Know how to use the ping and traceroute commands***
- ***Understand the modules and interactions of an ICMP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

Position of ICMP in the network layer

- IP has no error-reporting or error-correcting mechanism
- IP protocol also lacks a mechanism for host and management queries
- ICMP (Internet Control Message Protocol) has been designed to compensate for the above two deficiencies.
- The Position of ICMP in the network layer is shown below.



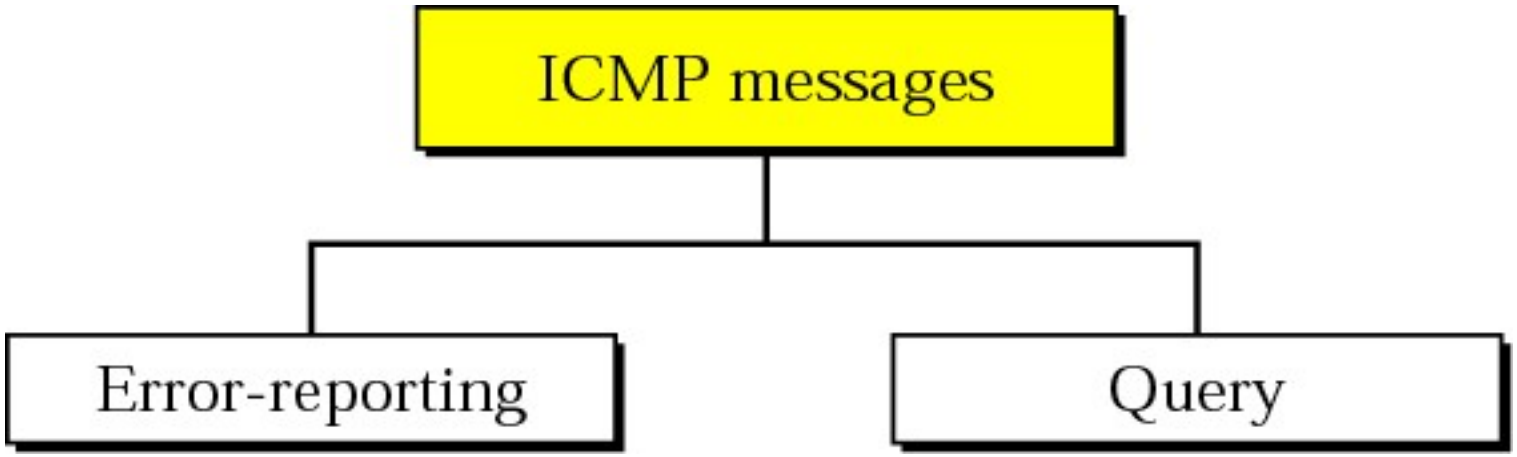
- ICMP Messages are encapsulated in the IP Datagram



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.*

ICMP messages



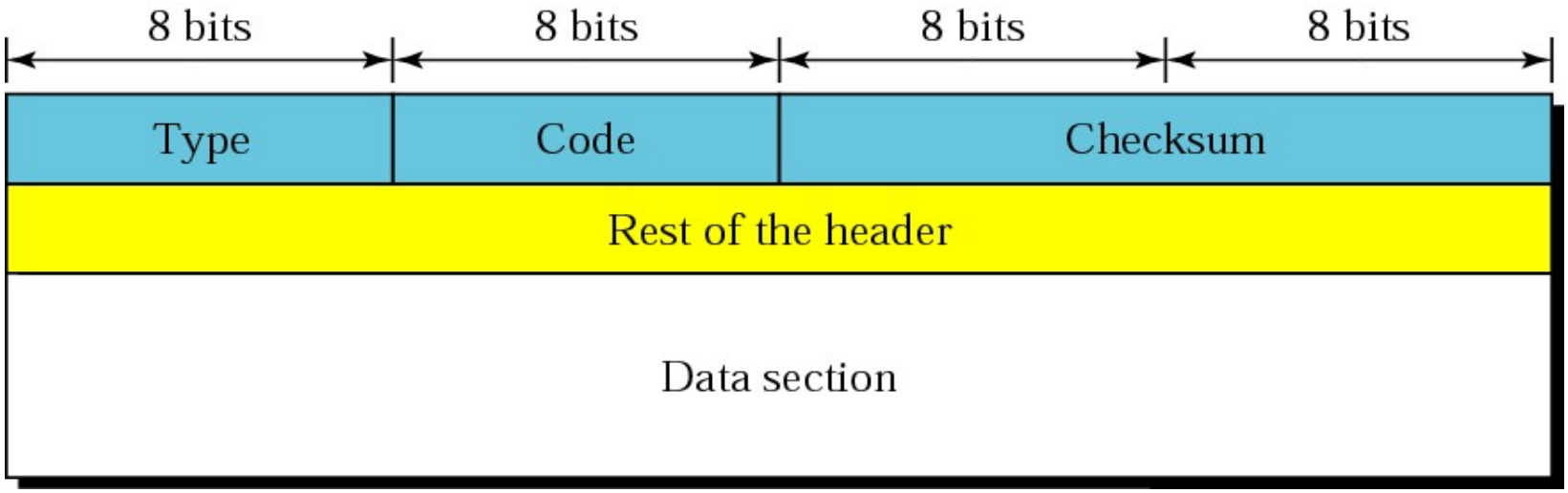
ICMP messages

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

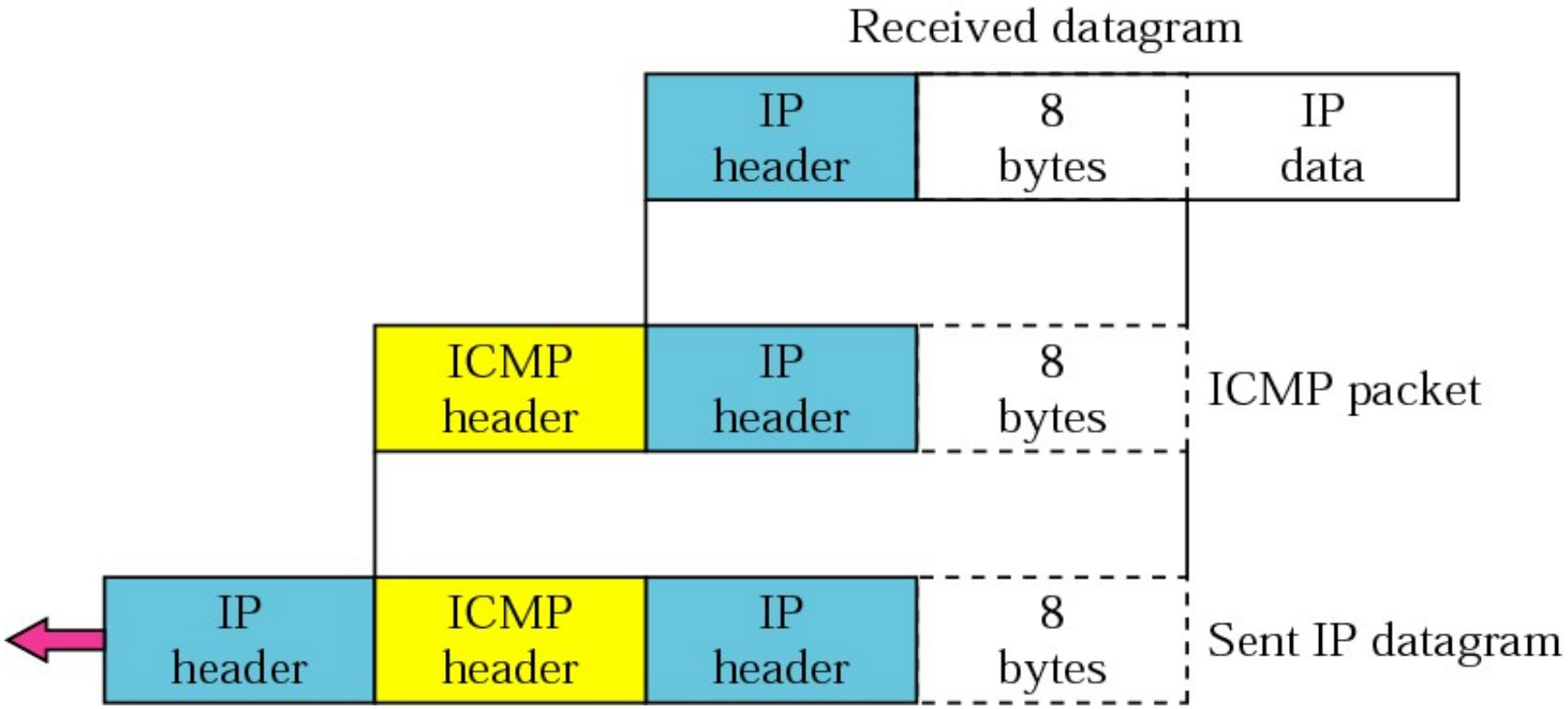
MESSAGE FORMAT

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.

General format of ICMP messages



Contents of data field for the error messages

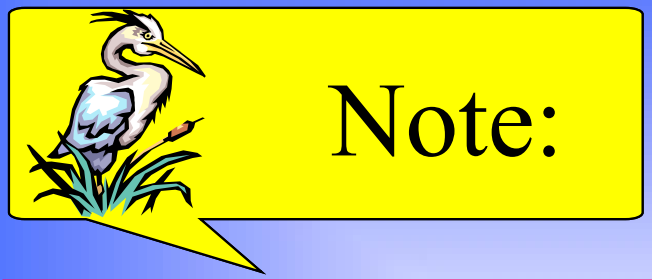


ERROR REPORTING

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.

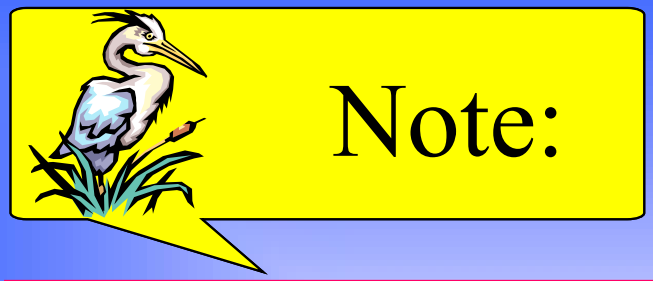
The topics discussed in this section include:

Destination Unreachable
Source Quench
Time Exceeded
Parameter Problem
Redirection



ICMP always reports error messages to the original source but does not correct errors.

Error Messages are always sent to the original source because this is the only information available in the datagram

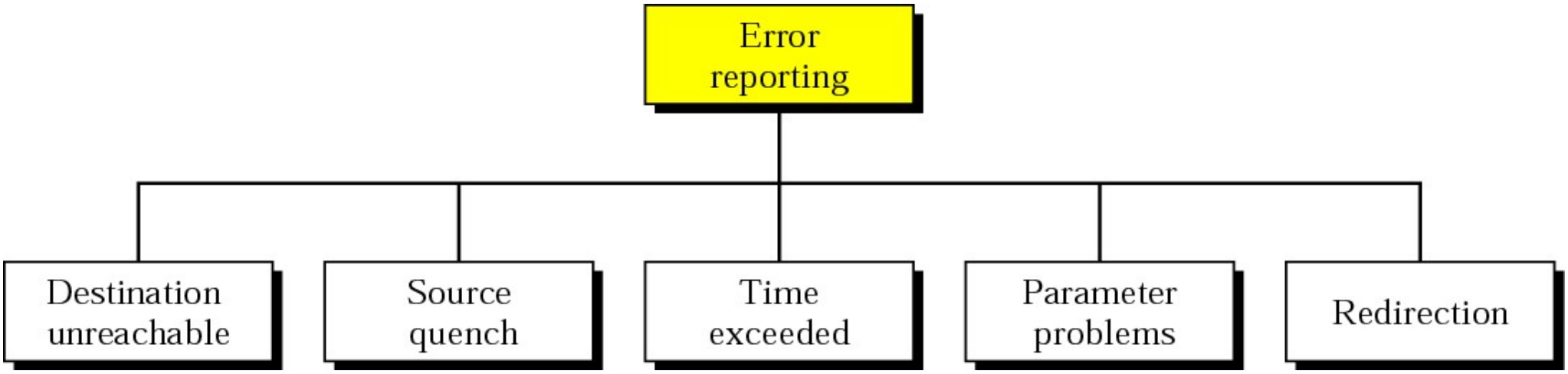


Note:

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.***

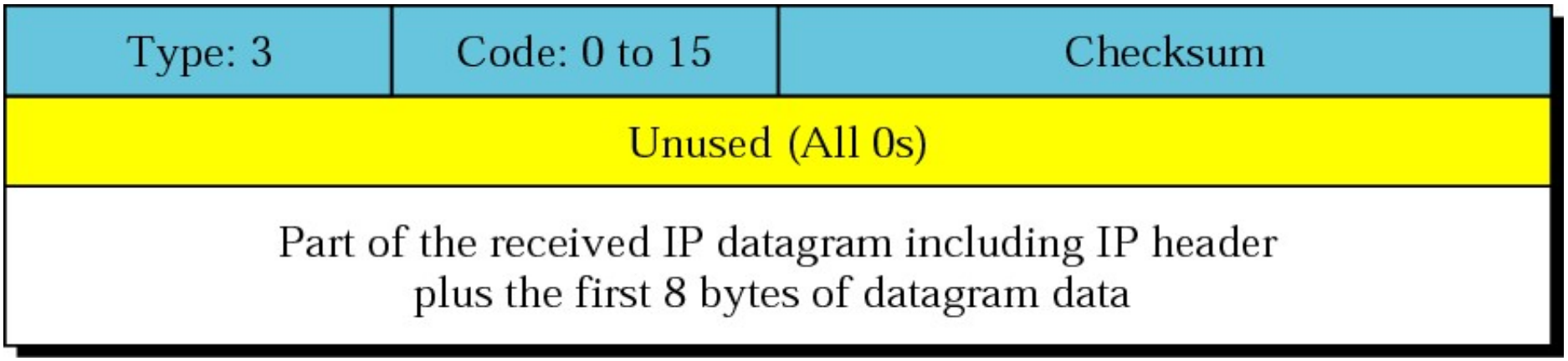
Error-reporting messages



Destination Unreachable

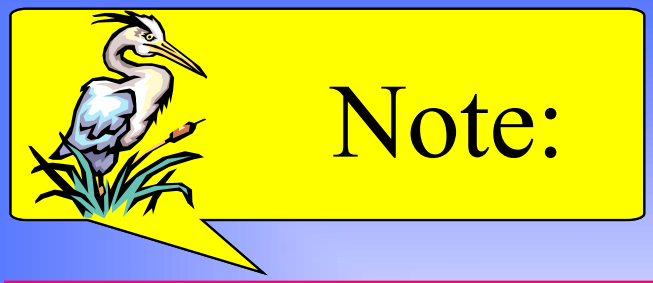
- When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a **destination-unreachable message** back to the source host that initiated the datagram

Destination-unreachable format



- **Code 0.** The network is unreachable, possibly due to hardware failure.
- **Code 1.** The host is unreachable. This can also be due to hardware failure.
- **Code 2.** The protocol is unreachable. An IP datagram can carry data belonging to higher-level protocols such as UDP, TCP, and OSPF
- **Code 3.** The port is unreachable. The application program (process) that the datagram is destined for is not running at the moment.
- **Code 4.** Fragmentation is required, but the DF (do not fragment) field of the datagram has been set. In other words, the sender of the datagram has specified that the datagram not be fragmented, but routing is impossible without fragmentation.
- **Code 5**. Source routing cannot be accomplished. In other words, one or more routers defined in the source routing option cannot be visited.
- **Code 6.** The destination network is unknown.
- **Code 7.** The destination host is unknown.

- Code 8. The source host is isolated.
- Code 9. Communication with the destination network is administratively prohibited.
- Code 10. Communication with the destination host is administratively prohibited.
- Code 11. The network is unreachable for the specified type of service. This is different from code 0. Here the router can route the datagram if the source had requested an available type of service.
- Code 12. The host is unreachable for the specified type of service. This is different from code 1. Here the router can route the datagram if the source had requested an available type of service.
- Code 13. The host is unreachable because the administrator has put a filter on it.
- Code 14. The host is unreachable because the host precedence is violated. The message is sent by a router to indicate that the requested precedence is not permitted for the destination.
- Code 15. The host is unreachable because its precedence was cut off.



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:

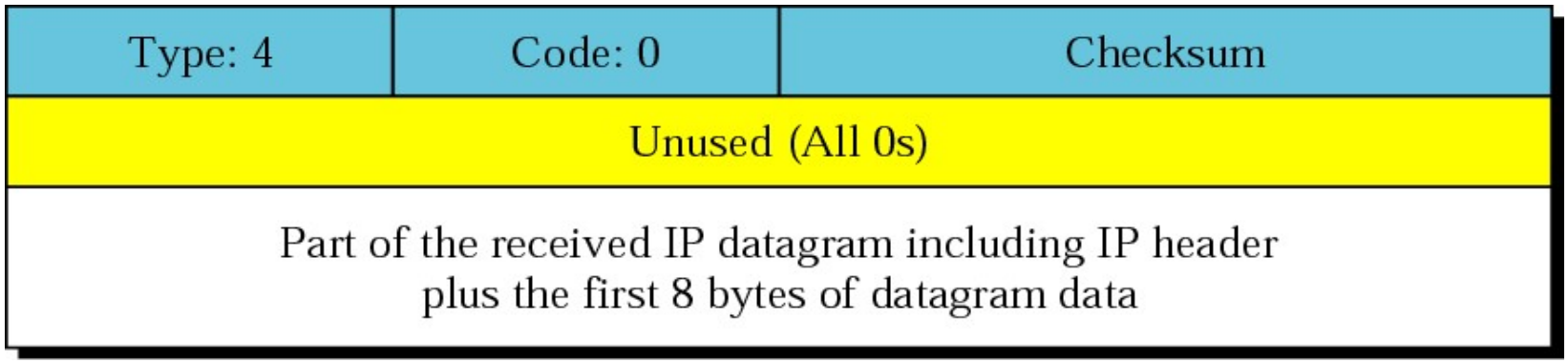
Even if a router does not report a destination unreachable message, it does not necessarily mean that the datagram has been delivered.

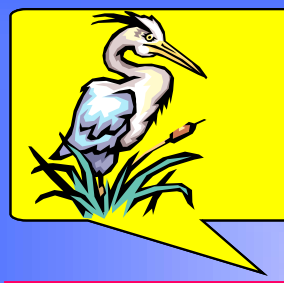
A router cannot detect all problems that prevent the delivery of a packet.

Source Quench

- There is no flow-control mechanism in the IP protocol.
- The **source-quench message in ICMP was designed to add a kind of flow control** and congestion control to the IP.
- When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram.
- This message has two purposes.
  - First, it informs the source that the datagram has been discarded.
  - Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.

Source-quench format

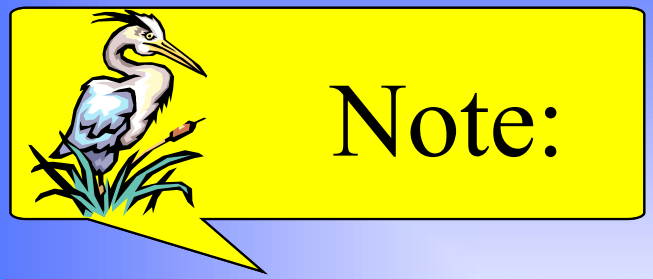




Note:

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

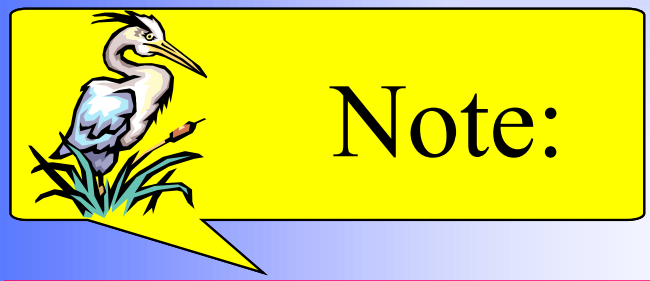
The source must slow down the sending of datagrams until the congestion is relieved.



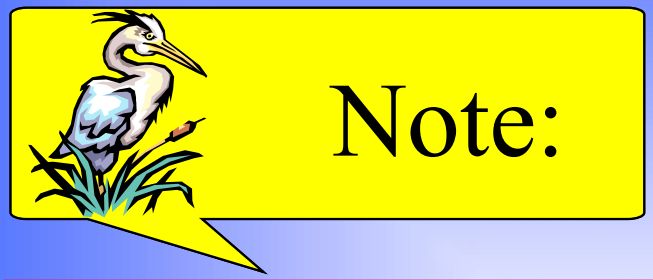
Note:

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

Time Exceeded

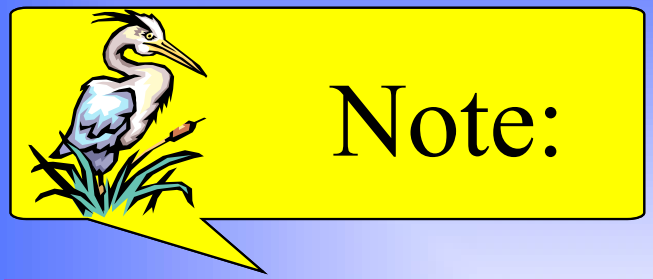


Whenever a router decrements a datagram with a time-to-live value to zero, it discards the datagram and sends a time-exceeded message to the original source.



Note:

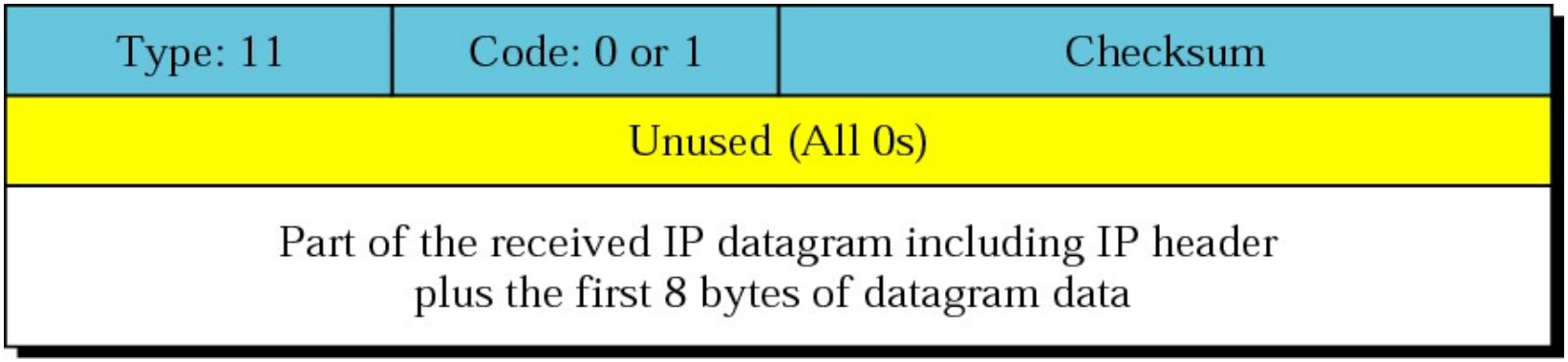
When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.

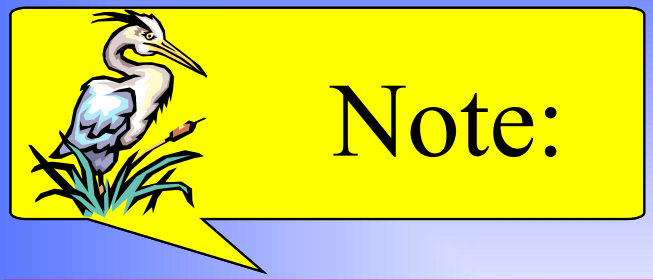


Note:

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.

Time-exceeded message format



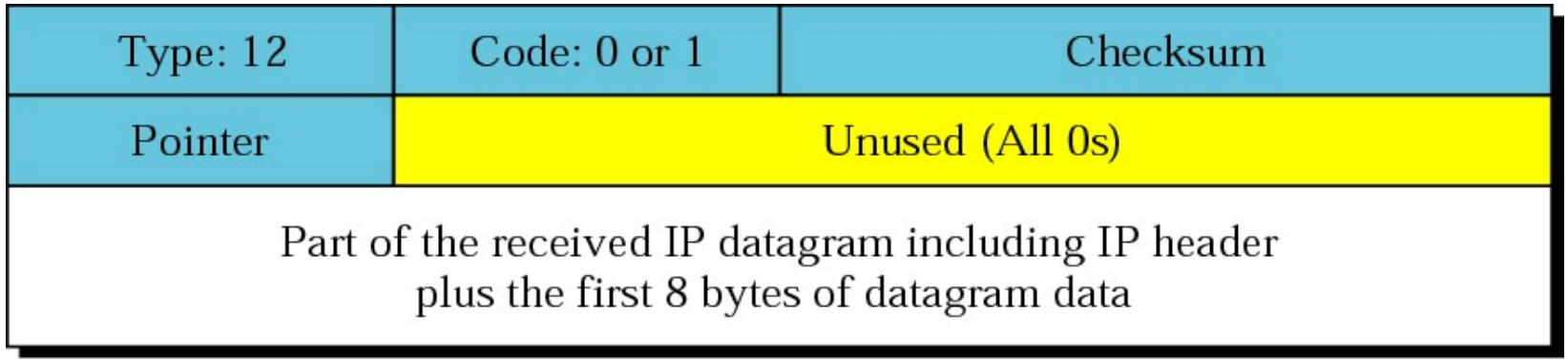


Note:

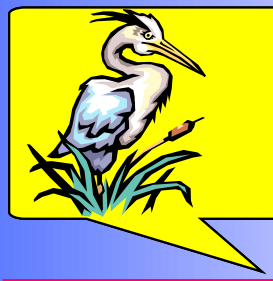
A parameter-problem message can be created by a router or the destination host.

Parameter-problem message format

- 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. In this case, the value in the pointer field points to the byte with the problem. For example, if the value is zero, then the first byte is not a valid field.
- **Code 1.** The required part of an option is missing. In this case, the pointer is not used.



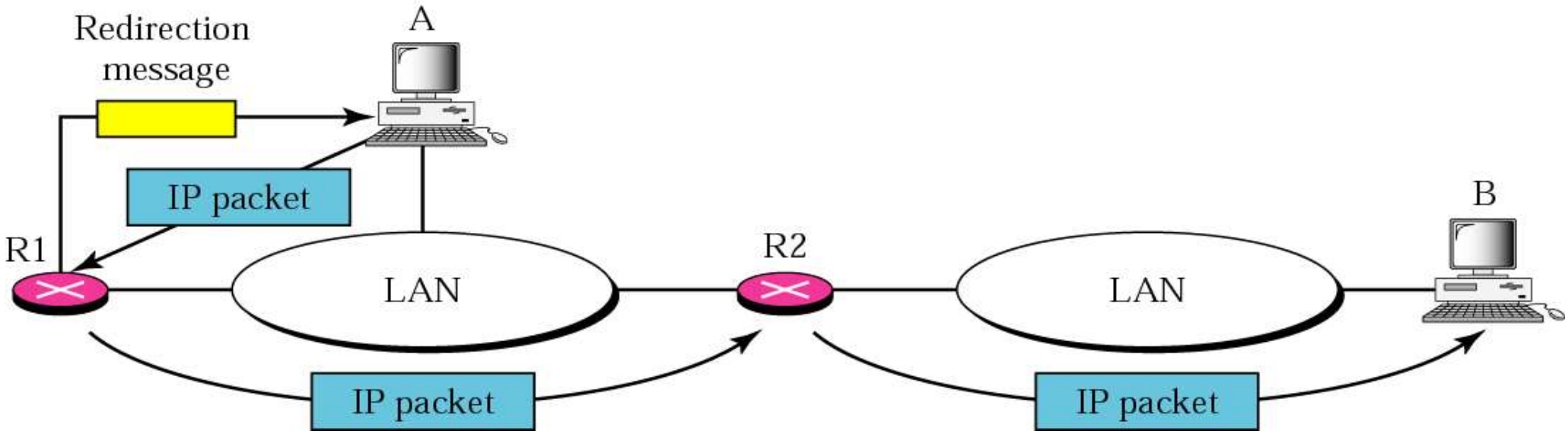
Redirection



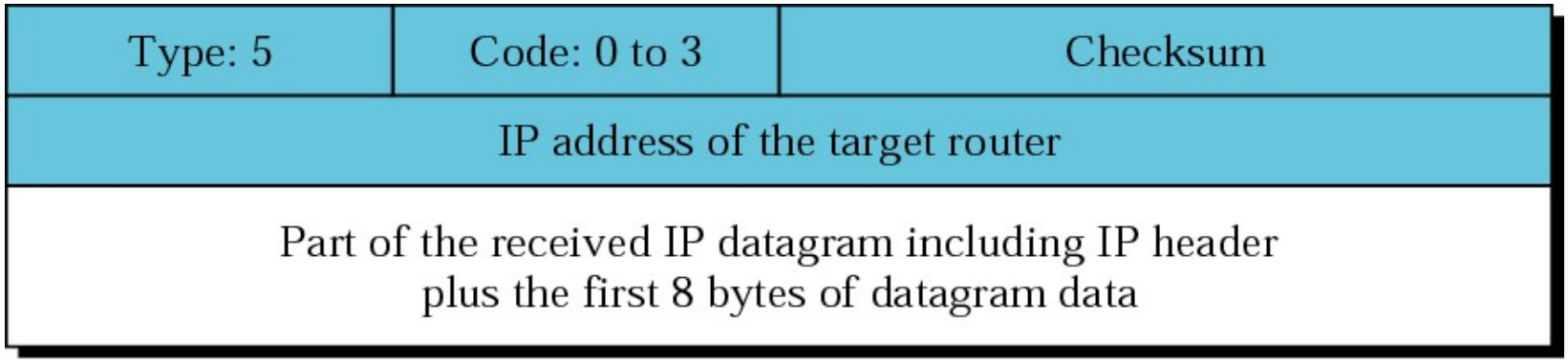
Note:

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.

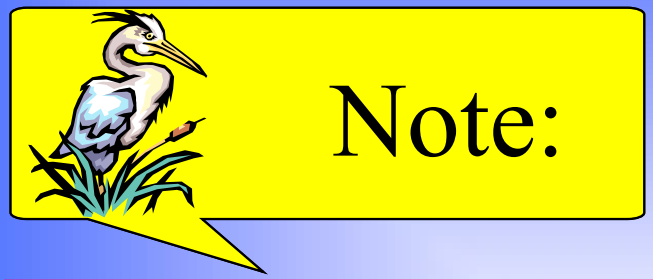
Redirection concept



Redirection message format



- 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.



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

CHECKSUM

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

The topics discussed in this section include:

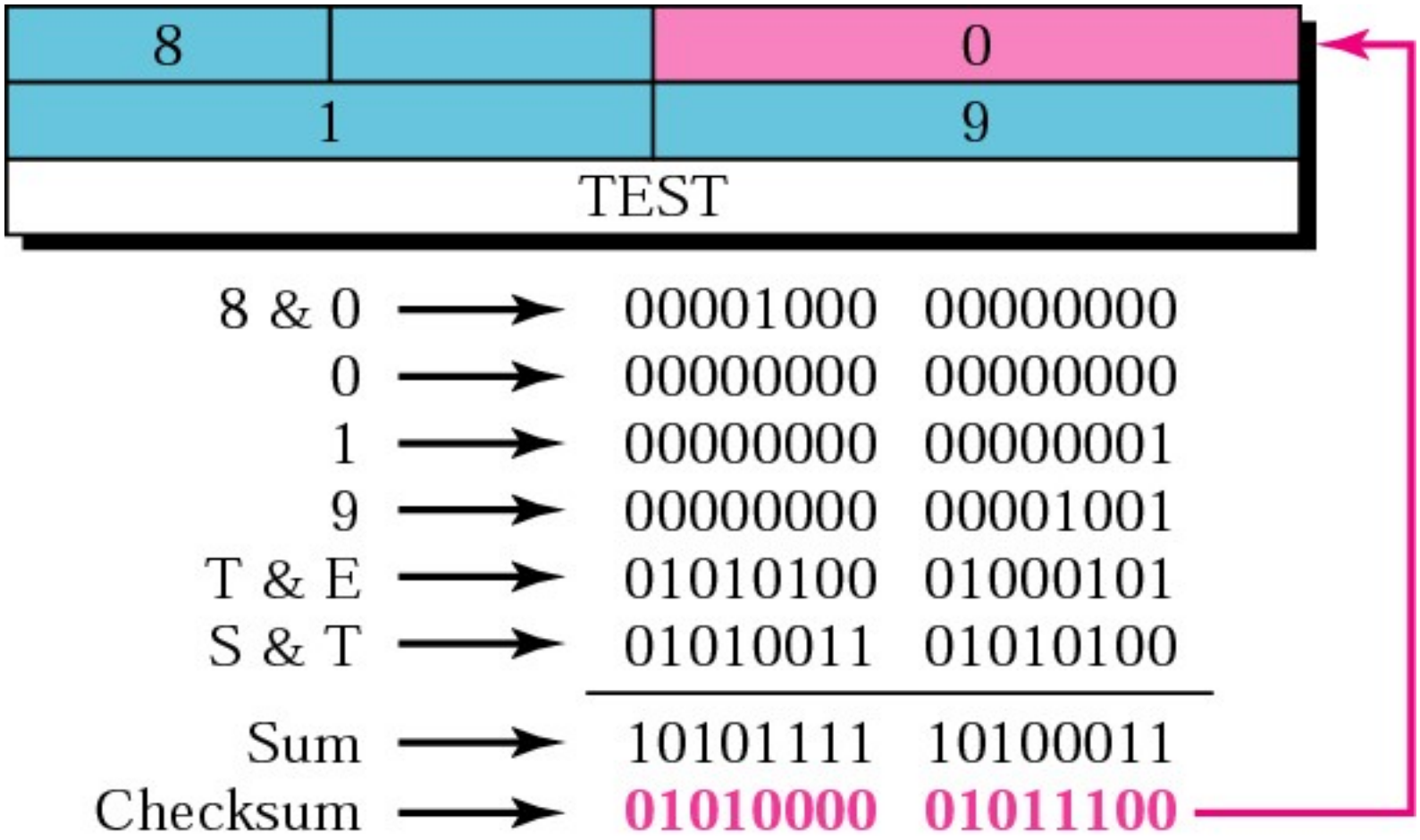
Checksum Calculation
Checksum Testing

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*



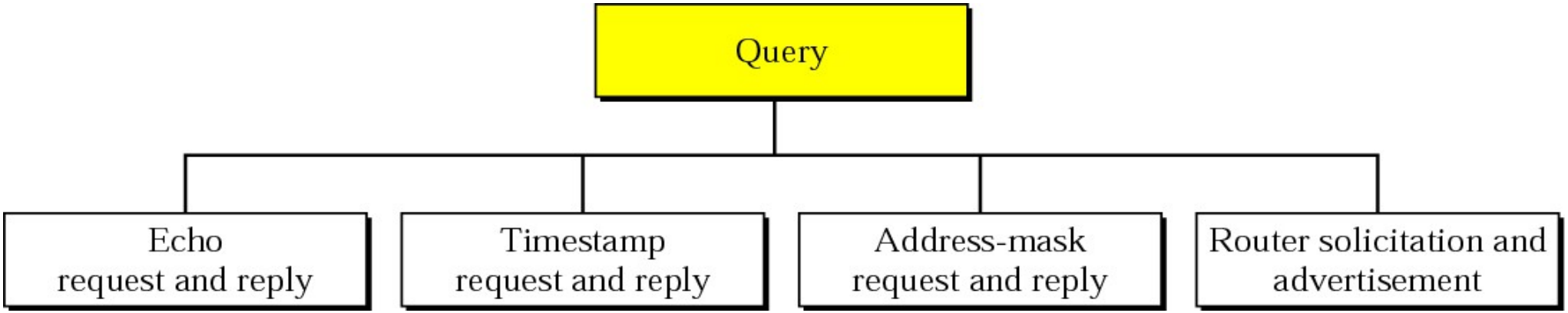
QUERY

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:

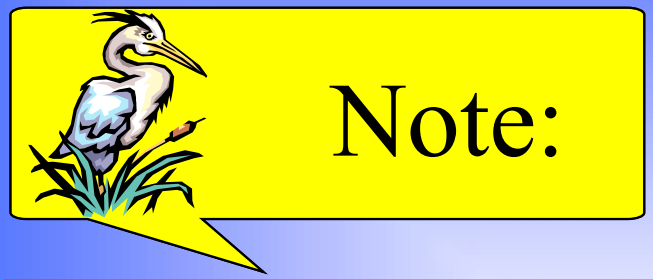
Echo Request and Reply
Timestamp Request and Reply
Address-Mask Request and Reply
Router Solicitation and Advertisement

Query messages



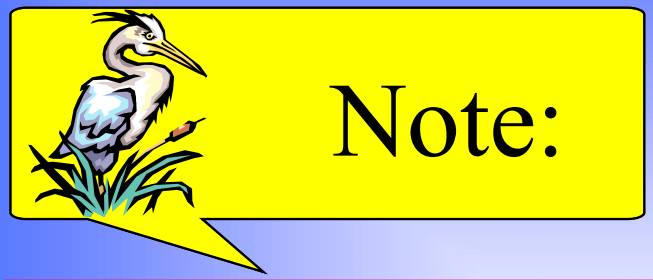
Echo Request and Echo Reply

- The **echo-request** and **echo-reply messages** are designed for diagnostic purposes.
- Network managers and users utilize this pair of messages to identify network problems.
- The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.

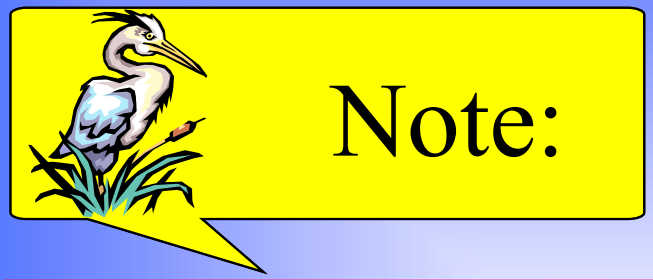


Note:

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.



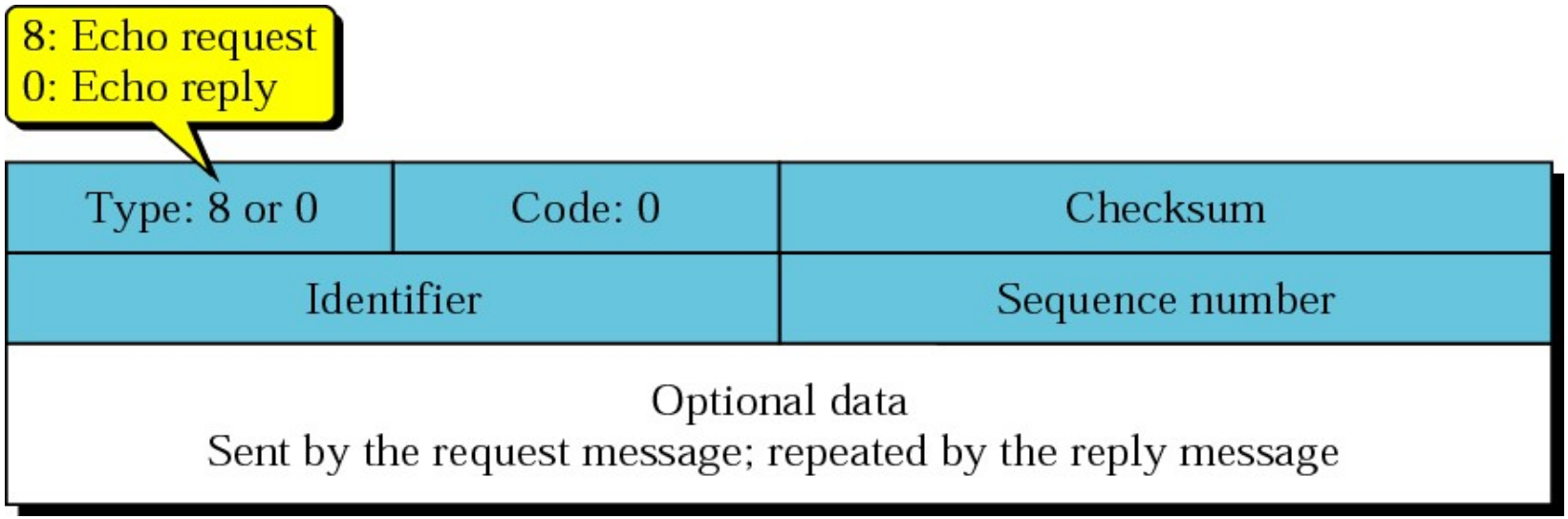
Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol.



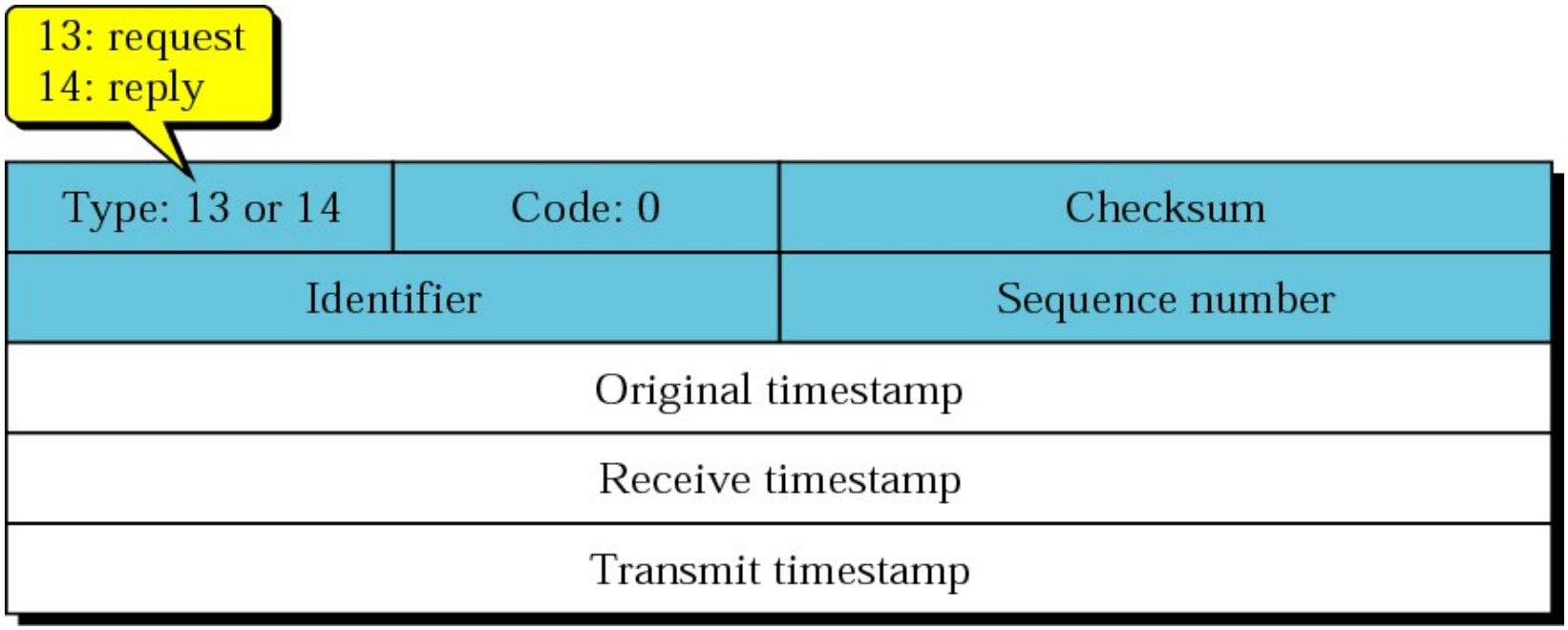
Note:

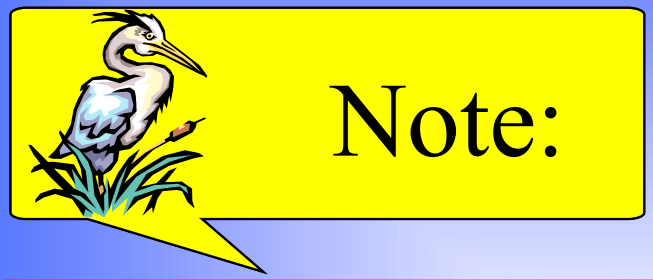
Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command.

Echo-request and echo-reply messages



Timestamp-request and timestamp-reply message format



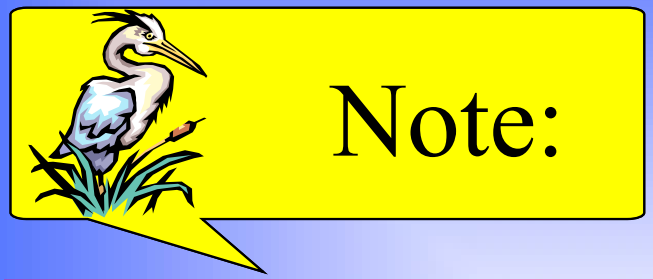


Note:

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.

- The timestamp-request and timestamp-reply messages can be used to compute the one-way or round-trip time required for a datagram to go from a source to a destination and then back again. The formulas are
- **sending time** = **receive timestamp** − **original timestamp**
- **receiving time** = **returned time** − **transmit timestamp**
- **round-trip time** = **sending time** + **receiving time**

- Note that the sending and receiving time calculations are accurate only if the two clocks in the source and destination machines are synchronized.
- However, the round-trip calculation is correct even if the two clocks are not synchronized because each clock contributes twice to the round-trip calculation, thus canceling any difference in synchronization.



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.

- Given the actual one-way time, the timestamp-request and timestamp-reply messages can also be used to synchronize the clocks in two machines using the following formula:
- **Time difference = receive timestamp – (original timestamp field + one-way time duration)**

- For example, given the following information:
- **original timestamp: 46**
- **receive timestamp: 59**
- **transmit timestamp: 60**
- **return time: 67**
  - **sending time = 59 − 46 = 13 milliseconds**
  - **receiving time = 67 − 60 = 7 milliseconds**
  - **round-trip time = 13 + 7= 20 milliseconds**
  - **Time difference = 59 − (46 + 10) = 3**

- A computer receives a timestamp request from another computer at 2:34:20 P.M. The value of the original timestamp is 52,453,000. If the sender clock is 5 ms slow, what is the one-way time?

- To convert 2:34:20 P.M into milliseconds = 14 x 60 x 60 + 34 x 60 + 20 = 52460000 ms
- Original time stamp is 52,453,000.
- Receive time stamp is 52,460,000
- Time difference = -5 ms
- **Time difference = receive timestamp – (original timestamp field + one-way time duration)**
- -5 = 52460000 – 52453000 – one way time duration
- One way time duration = 7000 + 5 = 7005 ms.

- A computer sends a timestamp request to another computer. It receives the corresponding timestamp reply at 3:46:07 A.M. The values of the original timestamp, receive timestamp, and transmit timestamp are 13,560,000, 13,562,000, and 13,564,300, respectively. What is the sending trip time? What is the receiving trip time? What is the round-trip time? What is the difference between the sender clock and the receiver clock?