Internet Control Message Protocol Version 4 (ICMPv4)

Hayder Al-Ghanimi

Objectives

❑ To discuss the rationale for the existence of ICMP.

❑ To show how ICMP messages are divided into two categories: error reporting and query messages.

❑ To discuss the purpose and format of error-reporting messages.

❑ To discuss the purpose and format of query messages.

BRIFE DISCRIPTION

- ***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? 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?

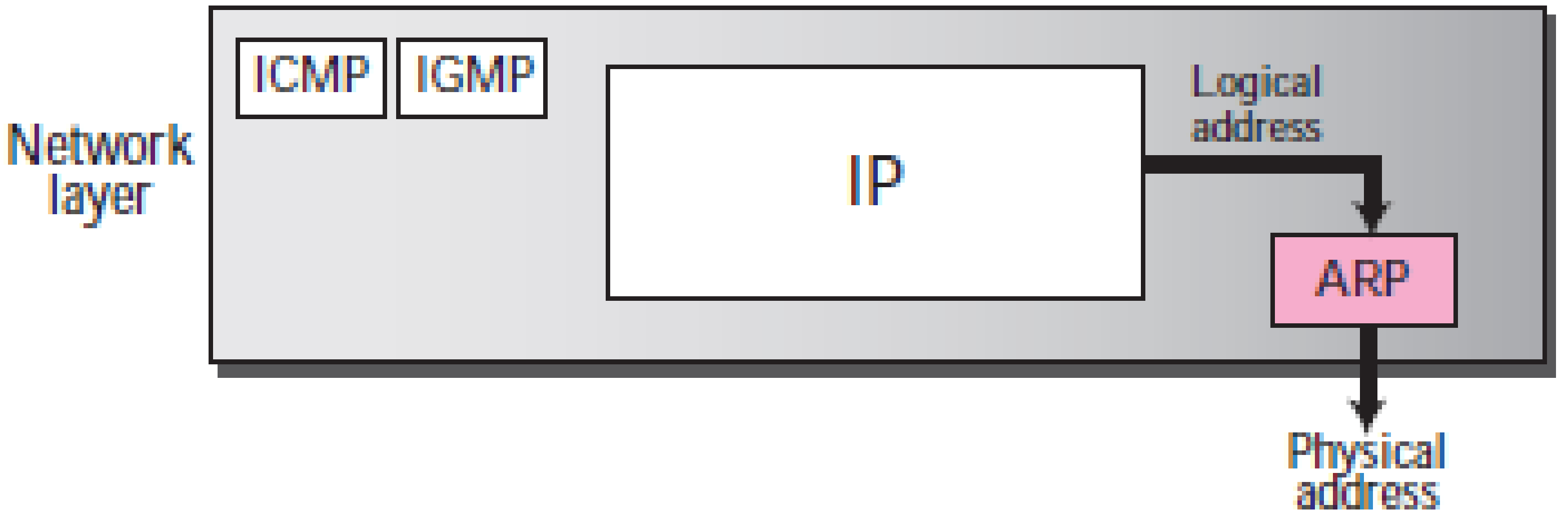
- These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host

- Solution is by using ***ICMP***

ICMP

The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

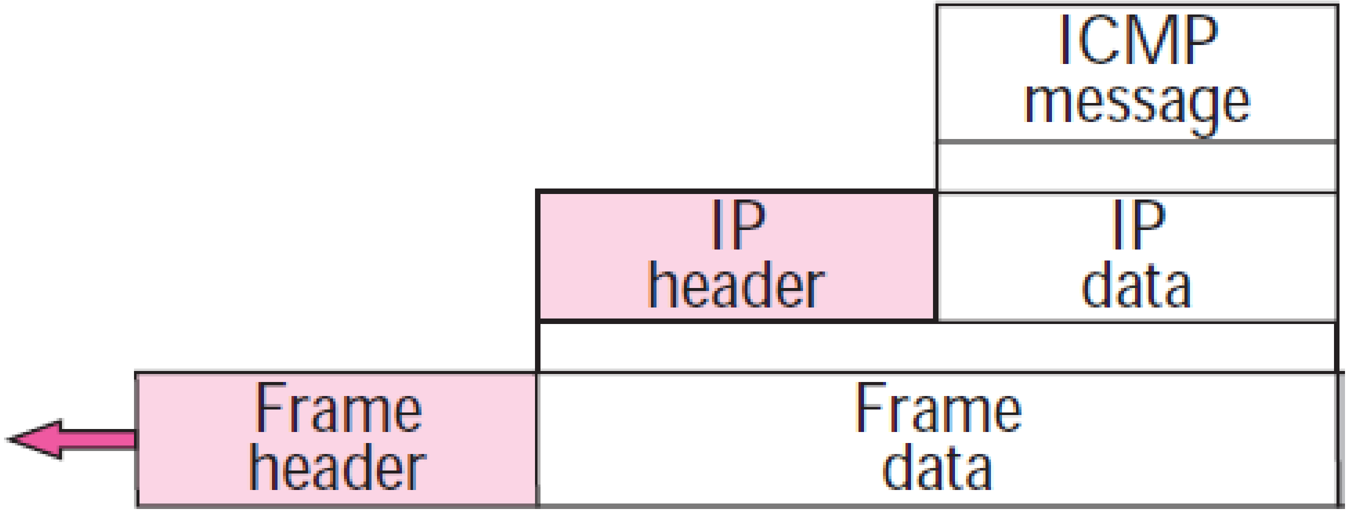
Position of ICMP in the network layer



shows the position of ICMP in relation to IP and other protocols in the network layer.

ICMP Encapsulation

- 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

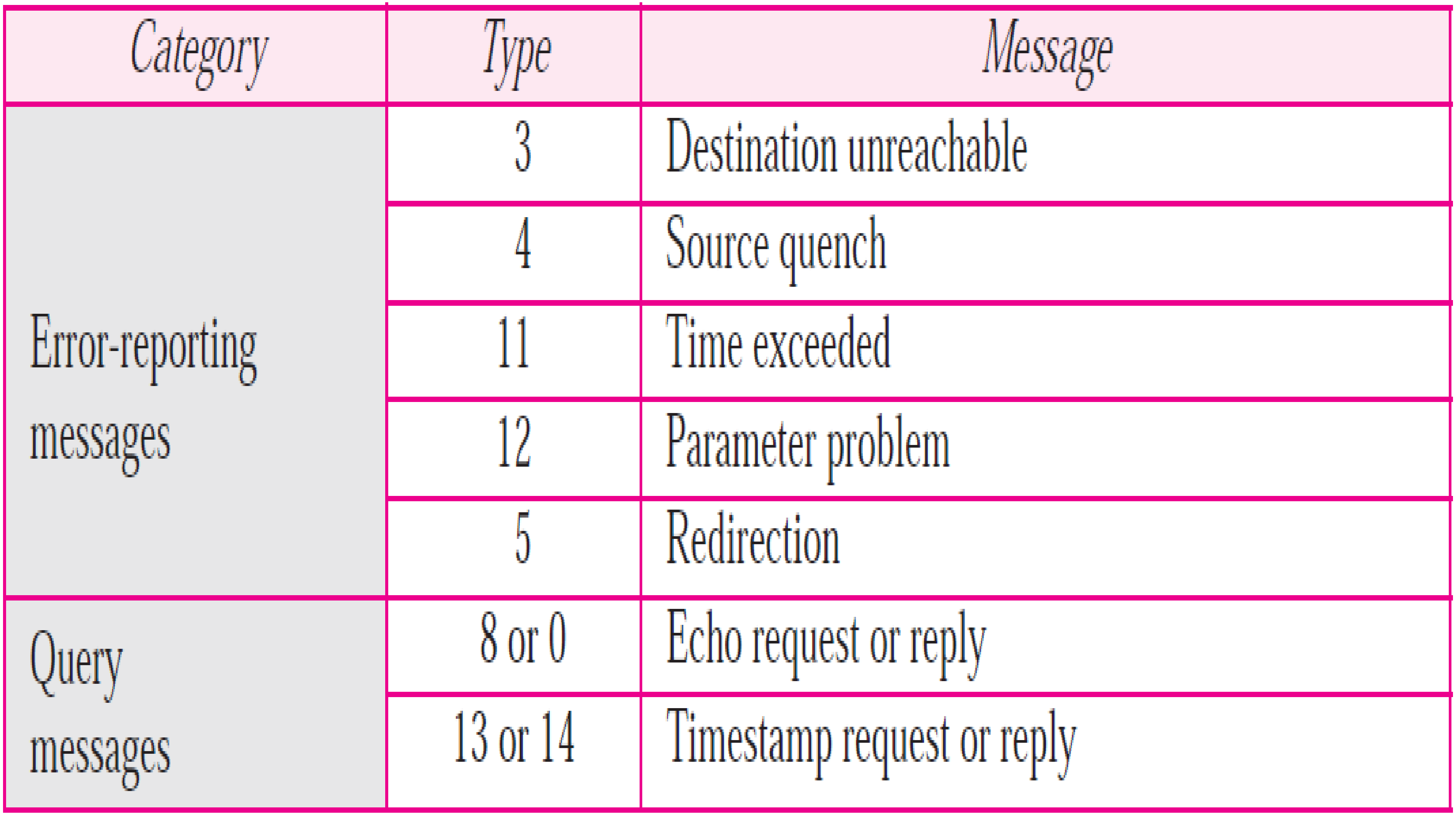


Messages

- **Types**:
  I. **Error-reporting messages:** reports problems that a router or a host (destination) may encounter when it processes an IP packet.

  II. **Query messages**: which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

ICMP messages

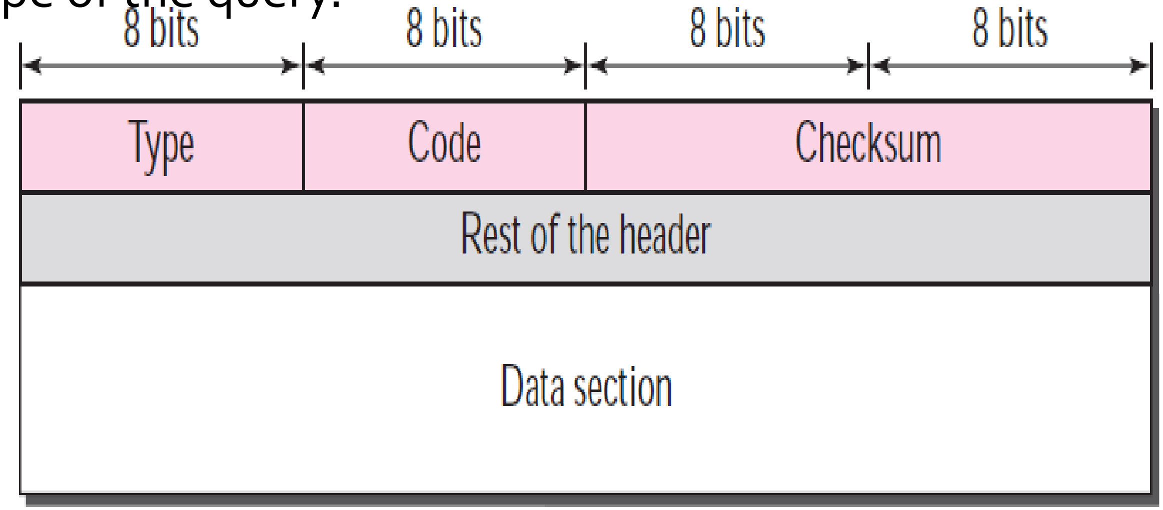


Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

General format of ICMP messages

- 8-byte header ***AND*** a variable-size data section
- The first 4 bytes are common
- The first field defines the type of the message.
- The code field specifies the reason for the particular message type
- The last common field is the checksum field
- The rest of the header is specific for each message type
- The 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.

ICMP always reports error messages to the original source



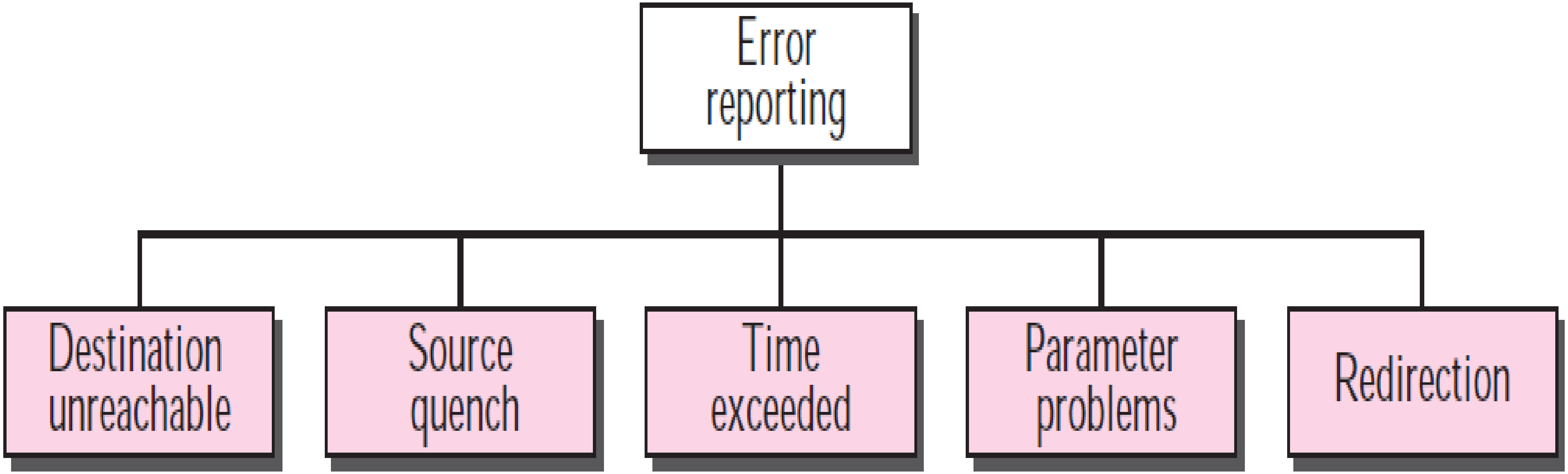
8 bits 8 bits 8 bits 8 bits

Type | Code | Checksum

Rest of the header

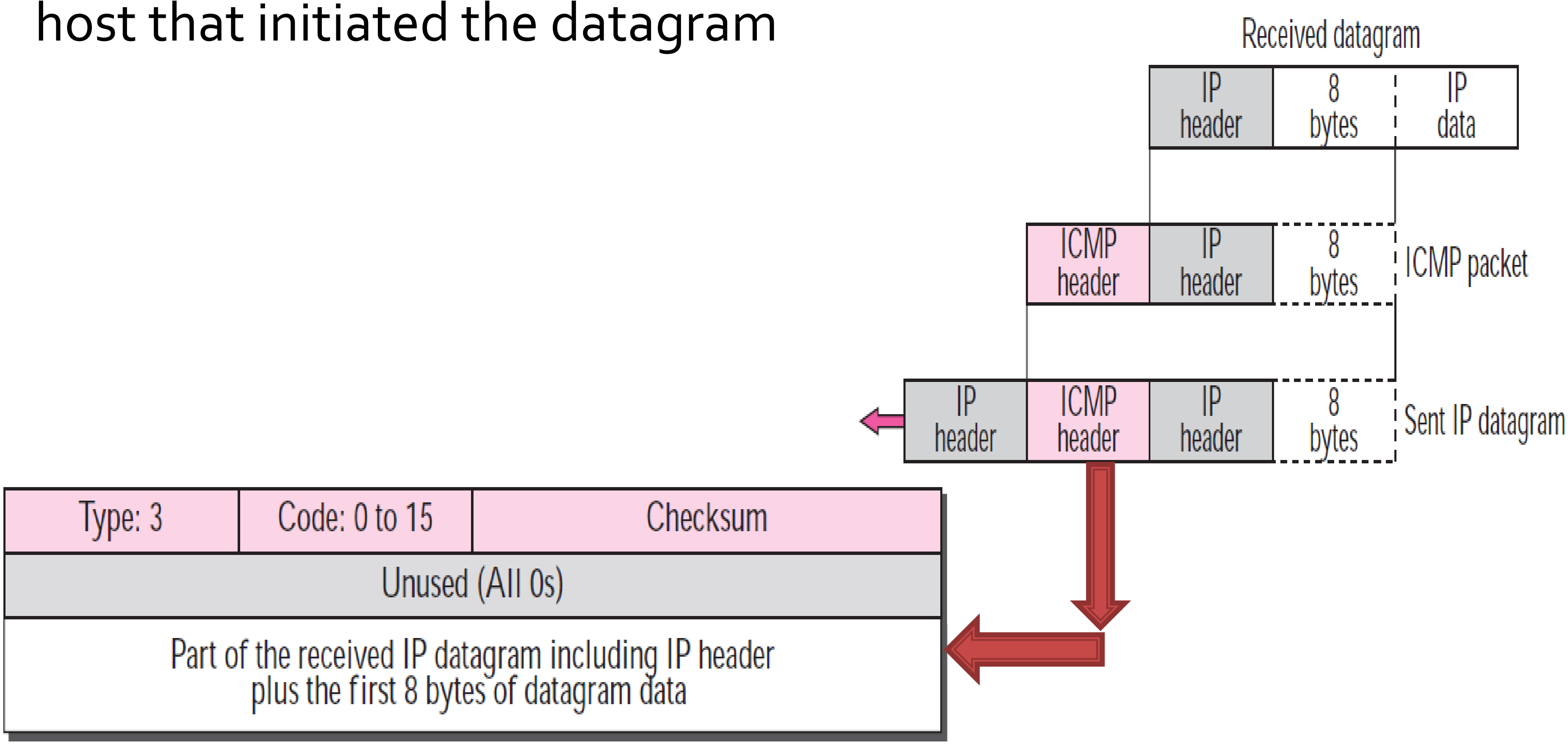
Data section

Error-reporting messages [1]



[1] 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



Type: 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Codes [0 .. 15]

- **The code field specifies the reason for discarding the datagram:**

1. **Code 0**. The network is unreachable, possibly due to hardware failure.
2. **Code 1.** The host is unreachable. This can also be due to hardware failure.
3. **Code 2**. The protocol is unreachable. An IP datagram can carry data belonging to higher-level protocols such as UDP, TCP, and OSPF. If the destination host receives a datagram that must be delivered, for example, to the TCP protocol, but the TCP protocol is not running at the moment, a code 2 message is sent.
4. **Code 3.** The port is unreachable. The application program (process) that the datagram is destined for is not running at the moment.
5. **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.
6. **Code 5**. one or more routers defined in the source routing option cannot be visited.
7. **Code 6.** The destination network is unknown. This is different from code 0. In code 0, the router knows that the destination network exists, but it is unreachable at the moment. For code 6, the router has no information about the destination network.

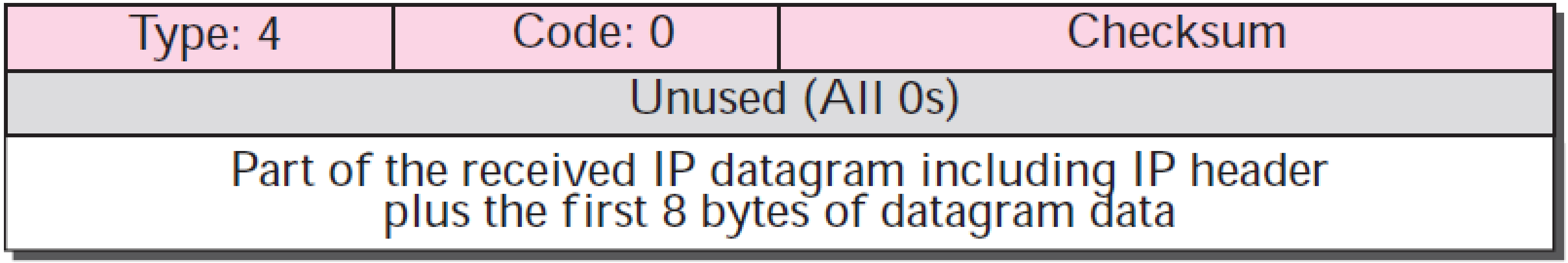
More

8. **Code 7.** The destination host is unknown. This is different from code 1. In code 1, the router knows that the destination host exists, but it is unreachable at the moment. For code 7, the router is unaware of the existence of the destination host.
9. **Code 8.** The source host is isolated.
10. **Code 9.** Communication with the destination network is administratively prohibited.
11. **Code 10.** Communication with the destination host is administratively prohibited.
12. **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.
13. **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.
14. **Code 13.** The host is unreachable because the administrator has put a filter on it.
15. **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.
16. **Code 15.** The host is unreachable because its precedence was cut off. This message is generated when the network operators have imposed a minimum level of precedence for the operation of the network, but the datagram was sent with a precedence below this level.

Source Quench

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

- **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.**



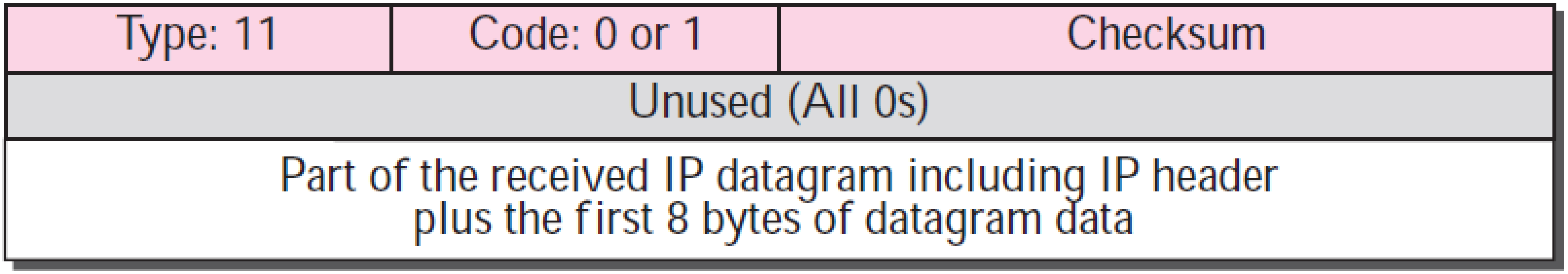
Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Time Exceeded

- The **time-exceeded message** is generated in two cases:

1. 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.

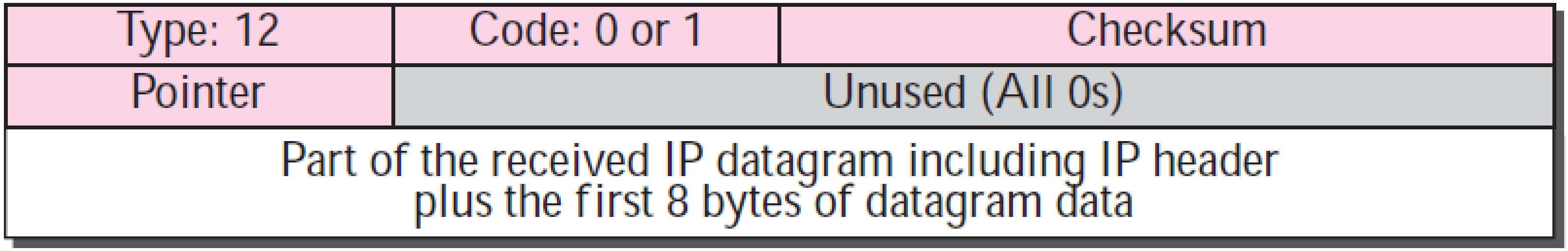
2. When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.



Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Parameter Problem

- A parameter-problem message can be created by a router or the destination host. Whenever find missing value in any filed.



Type: 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

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. For example, if the value is zero, then the first byte is not a valid field.

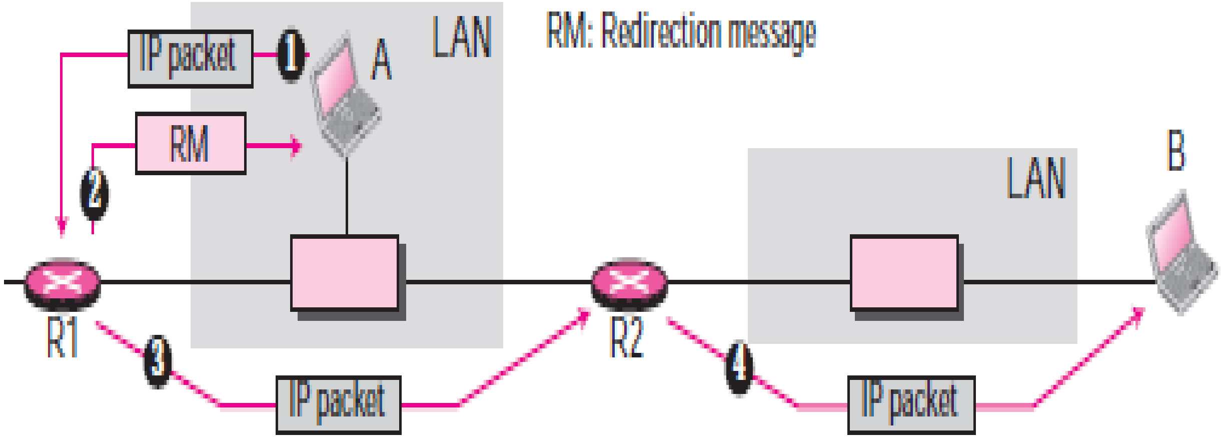
Code 1. The required part of an option is missing. In this case, the pointer is not used.

Redirection

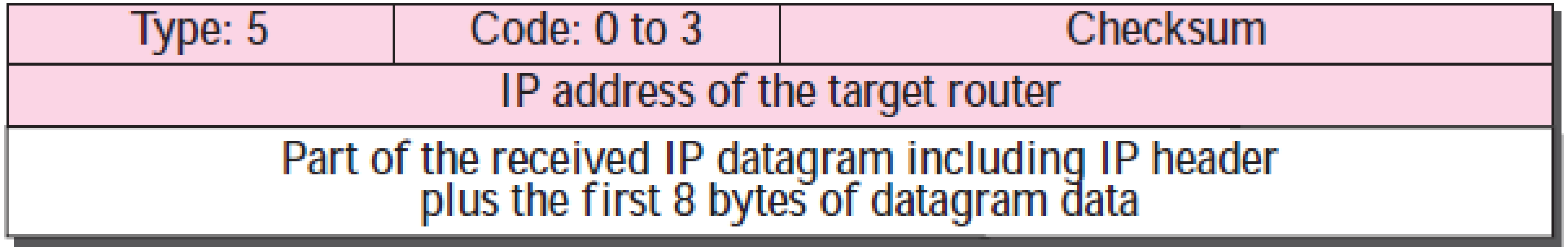
When a router needs to send a packet destined for another network, it must know the IP address of the next appropriate router. Both routers and hosts then must have a routing table to find the address of the router or the next router. Routers take part in the routing update process. Routing is dynamic. However, for efficiency, hosts do not take part in the routing update process because there are many more hosts in an internet than routers. Updating the routing tables of hosts dynamically produces unacceptable traffic. The hosts usually use static routing. When a host comes up, its routing table has a limited number of entries. It usually knows only the IP address of one router, the default router. For this reason, the host may send a datagram, which is destined for another network, to the wrong router. In this case, the router that receives the datagram will forward the datagram to the correct router. However, to update the routing table of the host, it sends a redirection message to the host. This concept of redirection is shown.

Redirection

- Host A wants to send a datagram to host B. Router R2 is obviously the most efficient routing choice, but host A did not choose router R2. The datagram goes to R1 instead. R1, after consulting its table, finds that the packet should have gone to R2. It sends the packet to R2 and, at the same time, sends a redirection message to host A. Host A's routing table can now be updated.



Redirection message format



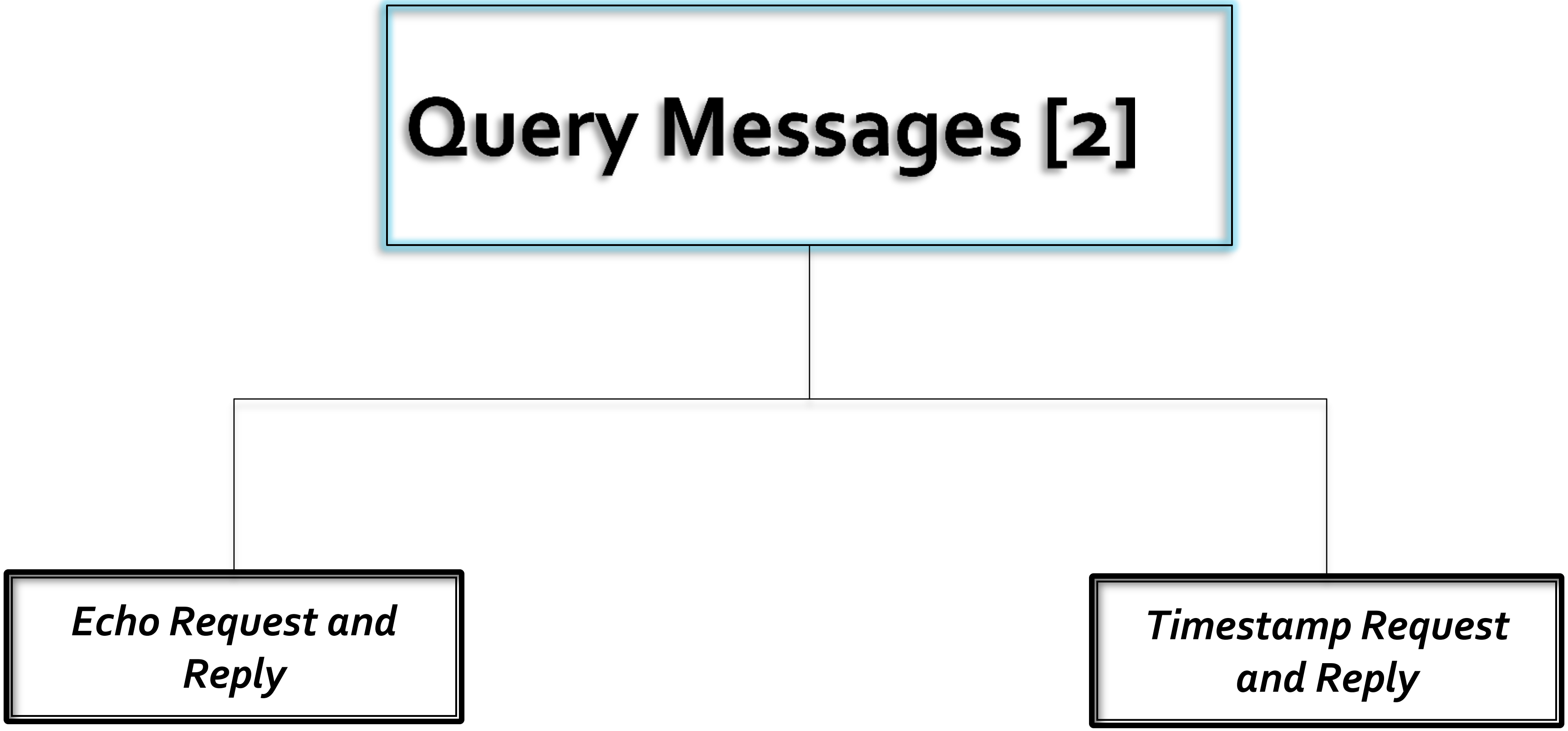
Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

- **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.



Query Messages [2]

Echo Request and Reply

Timestamp Request and Reply

Echo Request and Reply

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

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

- Note: 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.

Timestamp Request and Reply

- Two machines (hosts or routers) can use the timestamp-request and timestamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.