Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP)

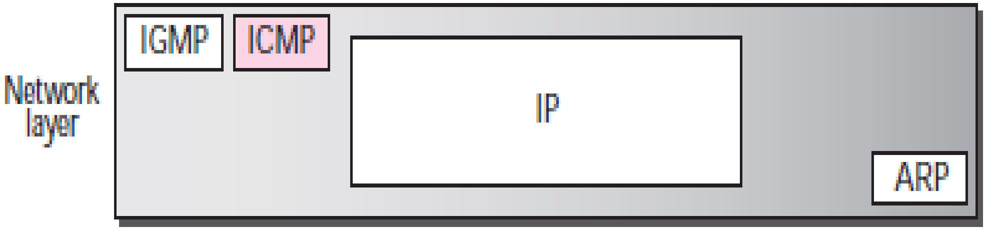
ICMP– An Introduction

- Why ICMP?
  - IP has no error – reporting or error correcting mechanism
- Scenarios in which the error occurs..
  - ✓ What happens if something goes wrong?
  - ✓ What happens if a router must discard a datagram but it cannot find a router to the final destination.
  - ✓ because the time-to-live field has a zero value
  - ✓ What happens if the final destination host must discard all fragments of a datagram due to time limit?

Internet Control Message Protocol (ICMP)

ICMP– An Introduction

- The above are some examples situations where an error has occurred and the IP has no built-in mechanism to notify the original host.
- It depends on Internet Control Message Protocol(ICMP) to provide an error control.
- ICMP –Internet Control Message Protocol
- It is a companion to the IP protocol

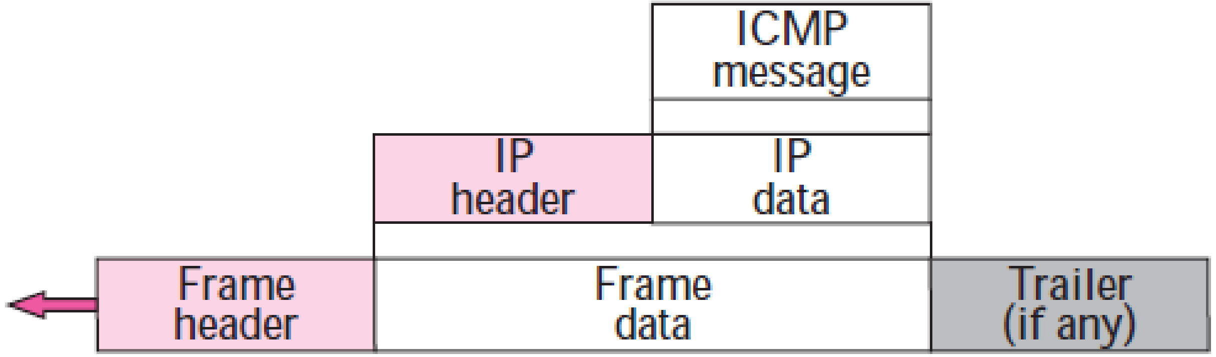


Position of ICMP in the network layer

Internet Control Message Protocol (ICMP)

ICMP– An Introduction

- ICMP -network layer protocol.
- messages are not passed directly to the data link layer.
- The messages encapsulated inside IP datagrams before going to the lower layer .
- The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message



ICMP Encapsulation

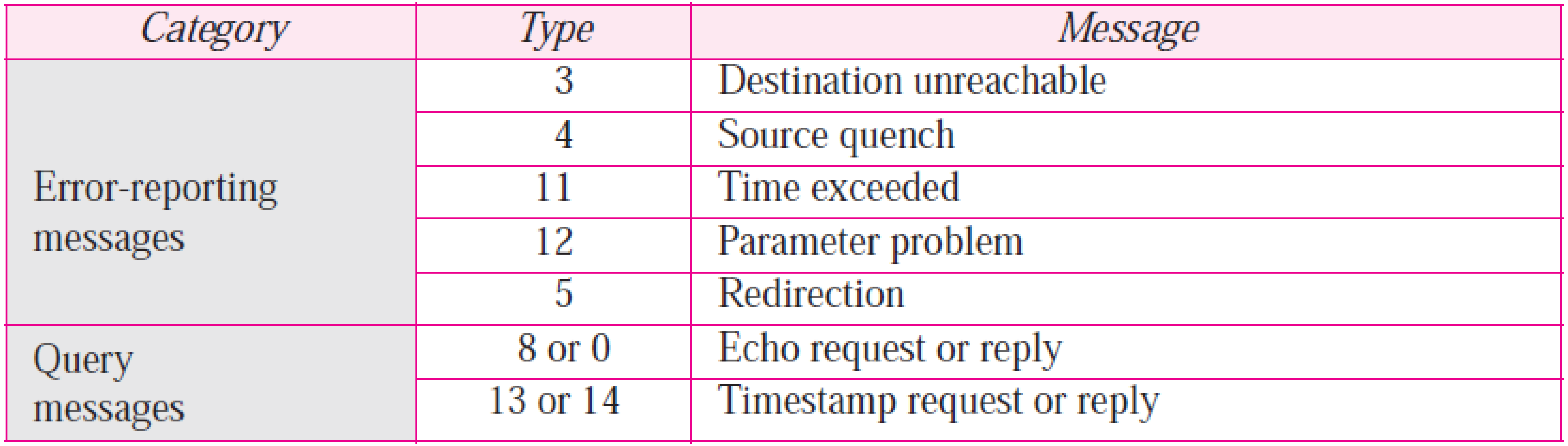
Internet Control Message Protocol (ICMP)

ICMP– Message

- ➢ ICMP message is of Two categories:
  - ➢ Error-reporting Messages
    - ✓ This report problems that a router or a host may encounter when it processes an IP packet.
  - ➢ The query messages
    - ✓ helps network manager get specific information from a router or another host.
- ✓ For example, nodes can discover their neighbors.

Internet Control Message Protocol (ICMP)

ICMP– Message



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 Messages

Internet Control Message Protocol (ICMP)

ICMP– Message format

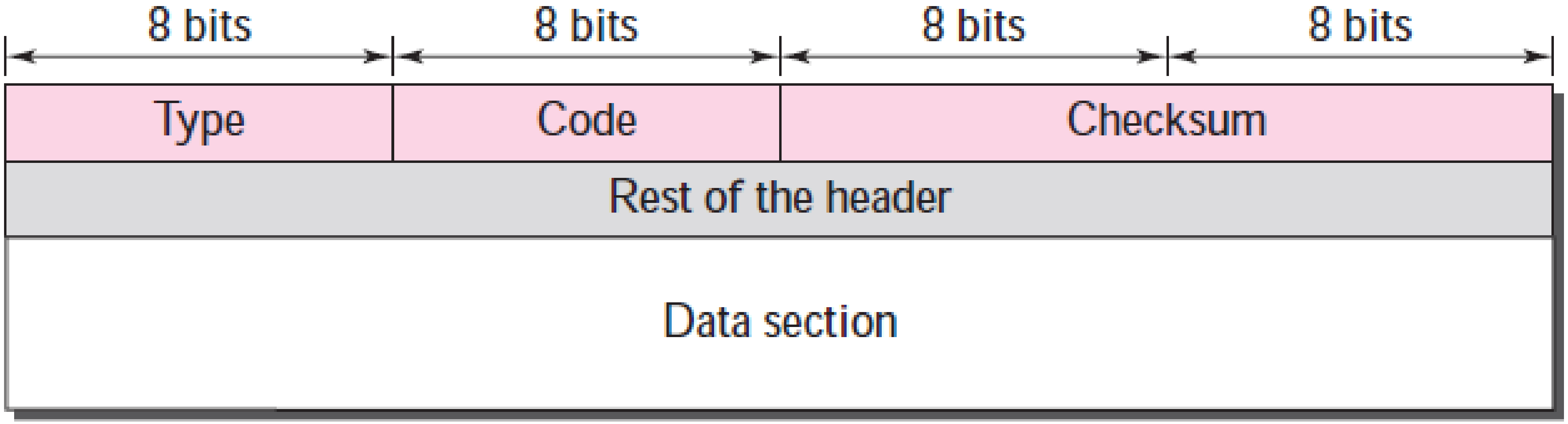
- 8-byte header
- variable-size data section.
- The first field, ICMP type, defines the type of the

message.

- The code specifies the reason for the particular message type.
- 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

Internet Control Message Protocol (ICMP)

ICMP– Message format



8 bits	8 bits	8 bits	8 bits
Type	Code	Checksum	
Rest of the header			
Data section			

General format of ICMP MESSAGE

Internet Control Message Protocol (ICMP)

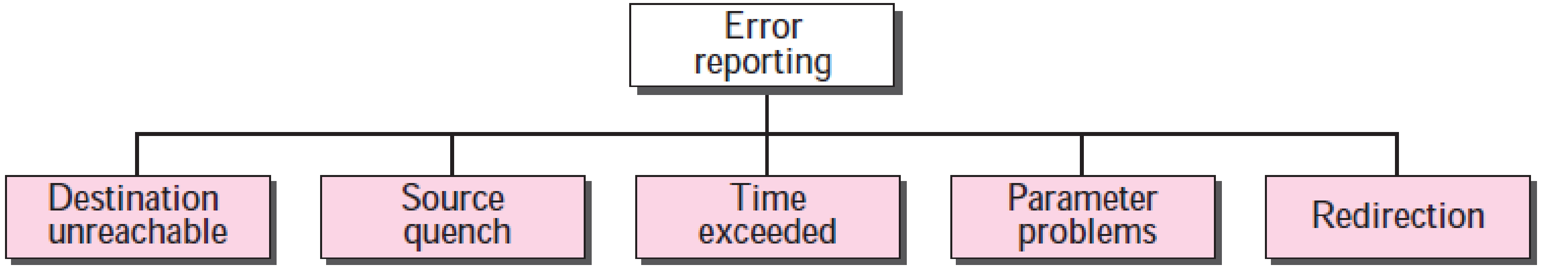
ICMP– MESSAGE FORMAT

Error Reporting Messages

- One of the main responsibilities of ICMP is to report errors.
- IP is an unreliable protocol, error checking and error control are not a concern of IP.
- **ICMP always reports error messages to the original source.**
- Error correction is left to the higher-level protocols.
- Error messages are always sent to the original source

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT



Error-reporting messages

Important ICMP error messages:

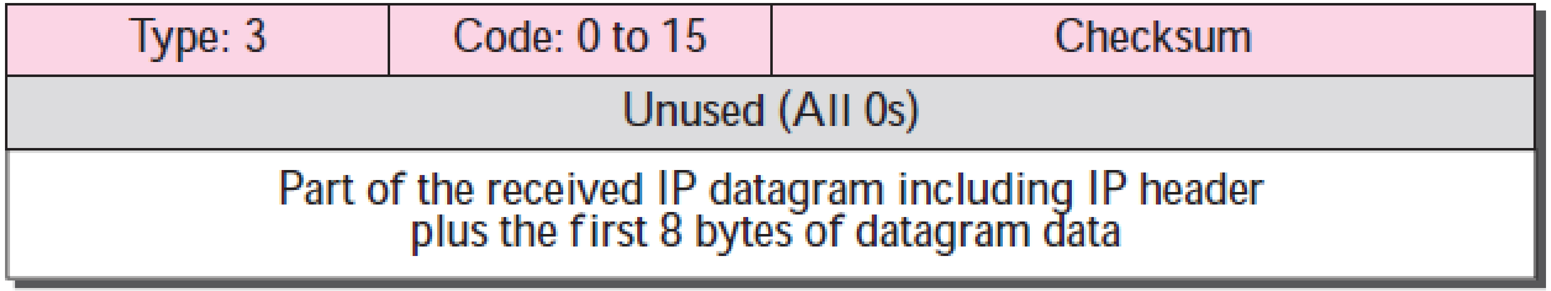
- ➢ No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- ➢ No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- ➢ No ICMP error message will be generated for a datagram having a multicast address.
- ➢ No ICMP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

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable

- A router cannot route a datagram or a host cannot deliver a datagram then the datagram is discarded
- The router or the host sends a **destination-unreachable message** back to the source host



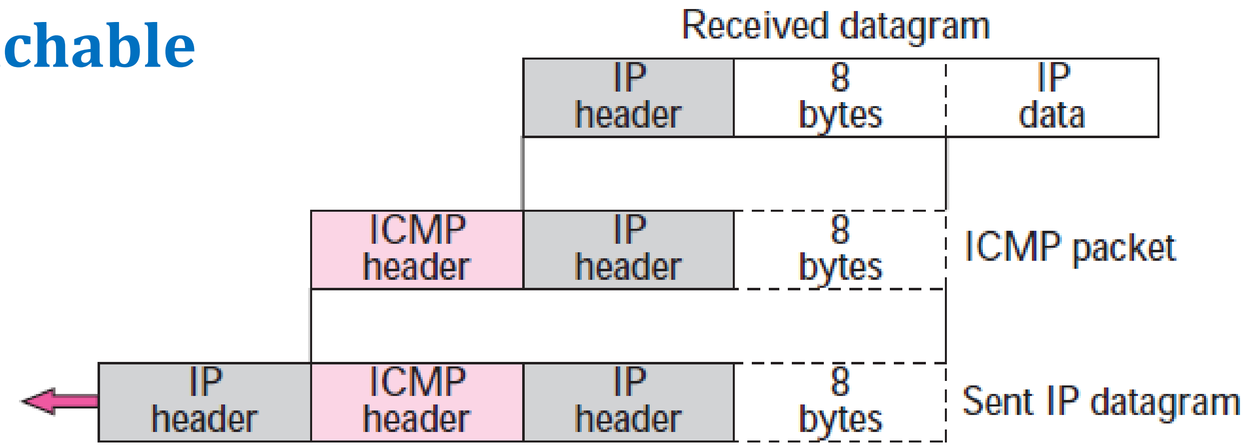
Type: 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Destination-unreachable format

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable



Contents of data field for the error messages

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

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable

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.

Code 3. The port is unreachable. The application program (process) that the datagram is destined for is not running at the moment.

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable

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. 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.

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable

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.

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.

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable

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.

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Destination Unreachable

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.

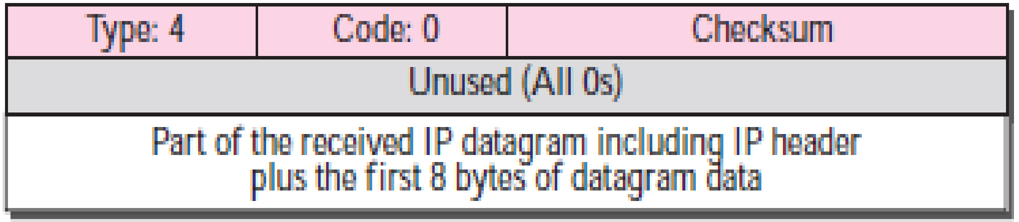
Code 15. The host is unreachable because its precedence was cut off. This message is generated when the network operators have imposed a minimum level of precedence for the operation of the network, but the datagram was sent with a precedence below this level.

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Source Quench

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



<table>
<tr><td>Type: 4</td><td>Code: 0</td><td>Checksum</td></tr>
<tr><td colspan="3">Unused (All 0s)</td></tr>
<tr><td colspan="3">Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data</td></tr>
</table>

Source Quench Format

ICMP– MESSAGE FORMAT

Time Exceeded

- The time-exceeded message is generated in two forms:

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.

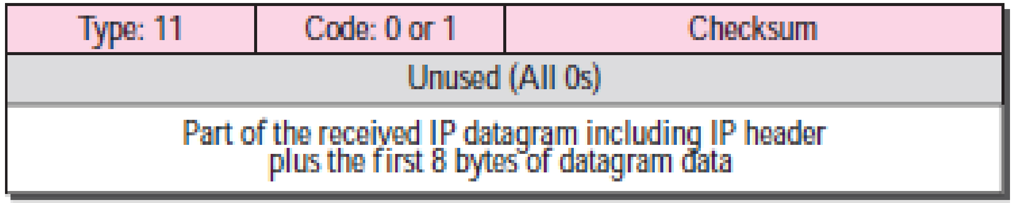
2. When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original Source

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Time Exceeded

- 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.

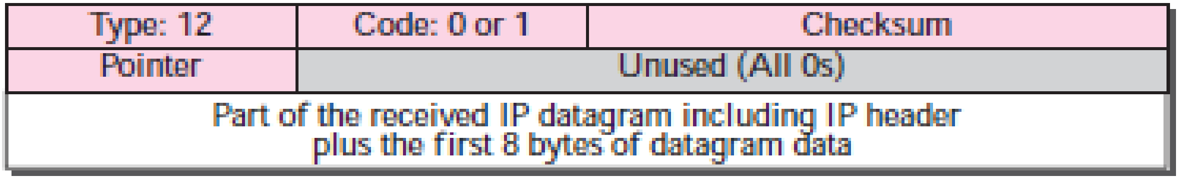


<table>
<tr><td>Type: 11</td><td>Code: 0 or 1</td><td>Checksum</td></tr>
<tr><td colspan="3">Unused (All 0s)</td></tr>
<tr><td colspan="3">Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data</td></tr>
</table>

Time Exceeded format

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT



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		

Parameter Problem

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.

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.

Internet Control Message Protocol (ICMP)

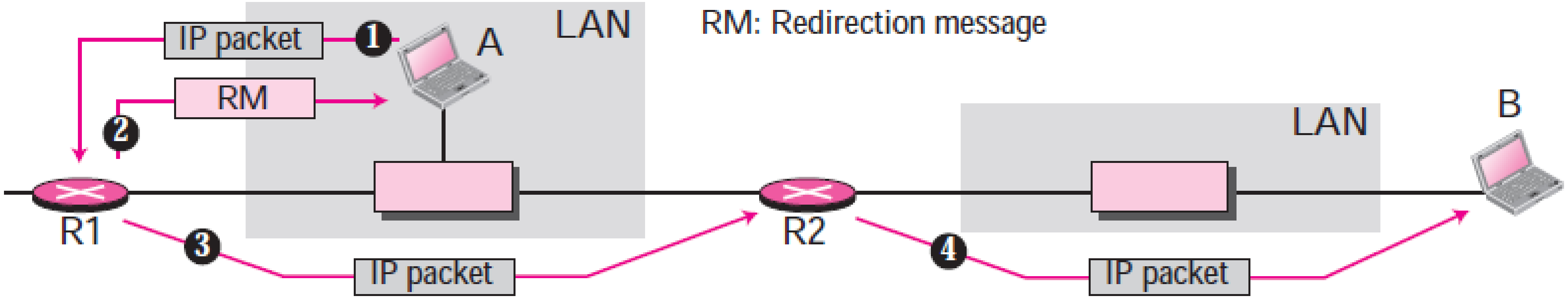
ICMP– MESSAGE FORMAT

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..

- 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
- 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.

Internet Control Message Protocol (ICMP)

ICMP– 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		

Internet Control Message Protocol (ICMP)

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.

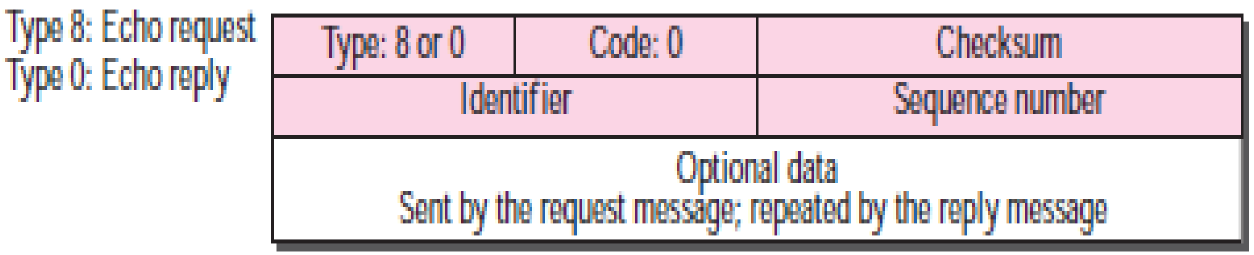
Internet Control Message Protocol (ICMP)

Timestamp Request and Reply

- The **timestamp-request** and **timestamp-reply messages** to determine the round-trip time needed for an IP datagram to travel between them

sending time = receive timestamp − original timestamp
receiving time = returned time − transmit timestamp
round-trip time = sending time + receiving time

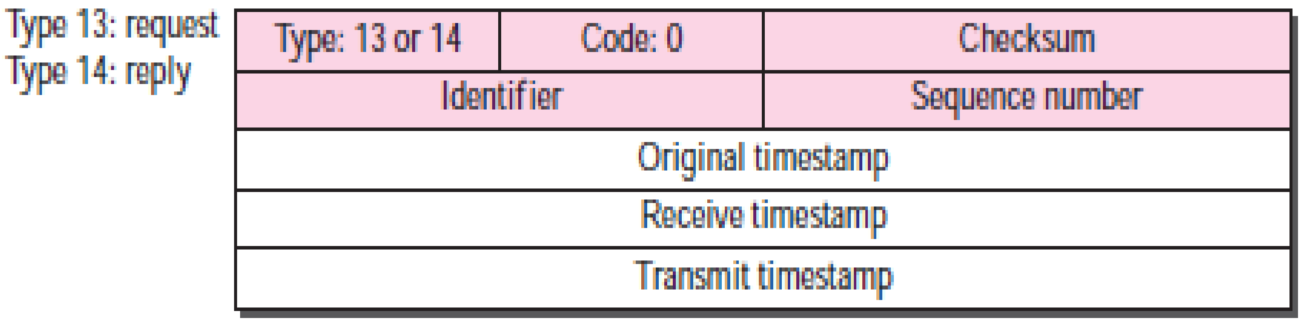
- Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine even if their clocks are not synchronized.
- The timestamp-request and timestamp-reply messages can be used to synchronize two clocks in two machines if the exact one-way time duration is known.



Type 8: Echo request
Type 0: Echo reply

Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

Echo-request and echo-reply messages



Type 13: request
Type 14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		

Timestamp-request and timestamp-reply message format

Internet Control Message Protocol (ICMP)

Timestamp Request and Reply

- ❑ 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 = receive timestamp – (original timestamp field + one-way time duration)
- ❑ Time difference = 59 – (46 + 10) = 3

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Checksum Calculation

The sender follows these steps using one's complement arithmetic:

1. The checksum field is set to zero.

2. The sum of all the 16-bit words (header and data) is calculated.

3. The sum is complemented to get the checksum.

4. The checksum is stored in the checksum field.

Internet Control Message Protocol (ICMP)

ICMP– MESSAGE FORMAT

Checksum Testing

The receiver follows these steps using one’s complement arithmetic:

1. The sum of all words (header and data) is calculated.

2. The sum is complemented.

3. If the result obtained in step 2 is 16 0s, the message is accepted; otherwise, it is rejected.

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

- To check whether host or router is alive and running
- To trace the route of a packet.
- Two tools that use ICMP for debugging: *ping* and *traceroute*

Ping

- The **ping** program to find if a host is alive and responding.
- ***Command : ping the ip of the host.***(ping 152.18.1.3)
- The source host sends ICMP echo request messages (type: 8, code: 0);
- The destination, if alive, responds with ICMP echo reply messages.

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

Ping cont…

- Starts the sequence number from 0; this number is incremented by one each time a new message is sent.
- *ping* can calculate the round-trip time.
- Inserts the sending time in the data section of the message.
- When packet arrives it subtracts the arrival time from the departure time to get the **Round-Trip Time** (RTT).
- The TTL (time to live) field is encapsulates an ICMP message as 62, which means the packet cannot travel more than 62 hops

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

Example : $ ping fhda.edu

```
PING fhda.edu (153.18.8.1) 56 (84) bytes of data.
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=0 ttl=62 time=1.91 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=1 ttl=62 time=2.04 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=2 ttl=62 time=1.90 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=3 ttl=62 time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=4 ttl=62 time=1.93 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=5 ttl=62 time=2.00 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=6 ttl=62 time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=7 ttl=62 time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=8 ttl=62 time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=9 ttl=62 time=1.89 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=10 ttl=62 time=1.98 ms
--- fhda.edu ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10103 ms
rtt min/avg/max = 1.899/1.955/2.041 ms
```

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

Ping cont…

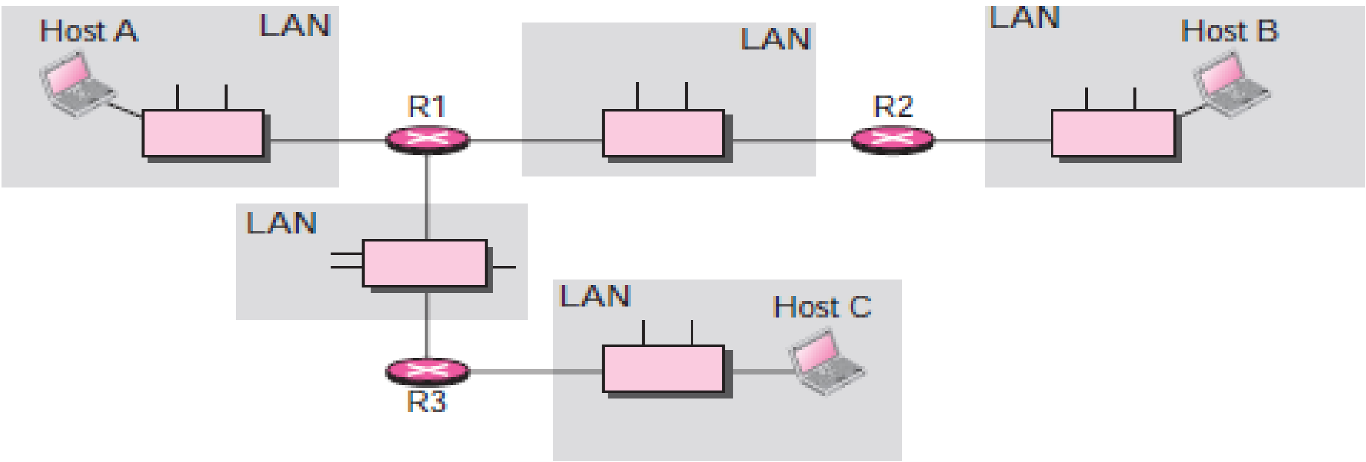
- ➢ Ping data bytes as 56 and the total number of bytes as 84.
- ➢ 8 bytes ICMP header+ 20 bytes of IP header to 56 =84
- ➢ *ping* defines the number of bytes as 64(56 + 8).
- ➢ Interrupts message ctrl+c.
- ➢ it prints the statistics of the probes
  - ✓ number of packets sent,
  - ✓ the number of packets received.
  - ✓ the total time
  - ✓ the RTT minimum, maximum, and average.

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

TRACE ROUTE

- The ***traceroute*** program in UNIX or ***tracert*** in Windows.
- It is used to route the packets from source to destination.
- Example Scenario



The Traceroute Program Operation

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

Trace route cont….

- *In above example* Given the topology, A packet from host A to host B travels through routers R1 and R2.
- The traceroute program find the address of router R1 & RTT between host A and router R1.
- The program repeats steps a to c three times to get a better average round-trip time.

a. Host A sends a packet to destination B using UDP the message is encapsulated in an IP packet with a TTL value of 1. The program notes the time the packet is sent

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

Trace route cont…..

b. Router R1 receives the packet and decrements the value of TTL to 0. It then discards the packet (because TTL is 0).

c. In receiver the ICMP messages uses the source address of the IP packet to find the IP address of router R1 and also makes note of the time the packet has arrived.

- The traceroute program repeats the previous steps to find the address of router R2 and the round-trip time between host A and router R2.
- The round-trip time between host A and host B.

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

Trace route cont.....

Example: The traceroute program to find the route from the computer voyager.deanza.edu to the server fhda.edu. The following shows the result.

```
 $ traceroute fhda.edu
traceroute to fhda.edu (153.18.8.1), 30 hops max, 38 byte packets
1 Dcore.fhda.edu (153.18.31.25) 0.995 ms 0.899 ms 0.878 ms
2 Dbackup.fhda.edu (153.18.251.4) 1.039 ms 1.064 ms 1.083 ms
3 tiptoe.fhda.edu (153.18.8.1) 1.797 ms 1.642 ms 1.757 ms
```

- In the above example the destination is 153.18.8.1.
- TTL value is 30 hops.
- The packet contains 38 bytes: 20 bytes of IP header, 8 bytes of UDP header, and 10 bytes of application data.

Internet Control Message Protocol (ICMP)

ICMP– DEBUGGING TOOL

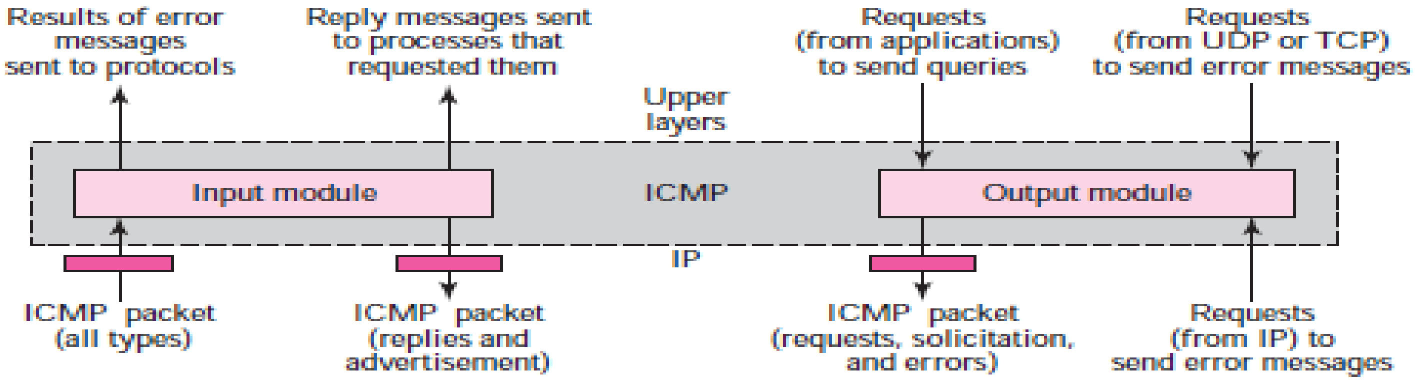
Trace route cont.....

- The router is named Dcore.fhda.edu with IP address 153.18.31.254.
- The Round Trip Time
  - 1. 0.995 milliseconds,
  - 2. 0.899 milliseconds
  - 3. 0.878 milliseconds
- The router is named Dbackup.fhda.edu with IP address 153.18.251.4.
- The third line shows the destination host.

Internet Control Message Protocol (ICMP)

ICMP– Package

- To handle the ICMP sending and receiving messages
- ICMP package made of two modules:
  - input module
  - output module


Results of error messages sent to protocols
Reply messages sent to processes that requested them
Requests (from applications) to send queries
Requests (from UDP or TCP) to send error messages
Upper layers
Input module
ICMP
Output module
IP
ICMP packet (all types)
ICMP packet (replies and advertisement)
ICMP packet (requests, solicitation, and errors)
Requests (from IP) to send error messages

ICMP package

Internet Control Message Protocol (ICMP)

ICMP– Package

Package cont..

Input Module

- ➢ Handles all received ICMP messages.
- ➢ Invoked when an ICMP packet is delivered from the IP layer.
- ➢ If the received packet is a
  - ✓ request - the module creates a reply and sends it out.
  - ✓ redirection message - Uses the information to update the routing table.
  - ✓ error message - It informs the protocol about the situation that caused the error.

Input Module Pseudo code

```
ICMP_Input_module (ICMP_Packet)
 {
    If (the type is a request)
    {
        Create a reply
        Send the reply
    }
    If (the type defines a redirection)
    {
    Modify the routing table
}
 If (the type defines other error messages)
    {
    Inform the appropriate source protocol
     }
 Return
}
```

Internet Control Message Protocol (ICMP)

ICMP– Package

Package cont..

Output Module

- ➢ Responsible for creating request, solicitation, or error messages requested by a higher level or the IP protocol.
- ➢ receives a demand from IP,UDP, or TCP to send one of the ICMP error messages.
- ➢ IP request is first allowed

- ➢ An ICMP message cannot be created for four situations:
  - ✓ an IP packet carrying an ICMP error message.
  - ✓ a fragmented IP packet.
  - ✓ A multicast IP packet.
  - ✓ an IP packet having IP address 0.0.0.0 or 127.X.Y. Z.

Output Module Pseudo code

```
ICMP_Output_Module (demand)
 {
         If (the demand defines an error message)
        {
                If (demand comes from IP AND is forbidden)
                {
                        Return
                 }
         If (demand is a valid redirection message)
         {
                 Return
         }
Create an error message
If (demand defines a request)
        {
                Create a request message
        }
Send the message
 Return
}
```