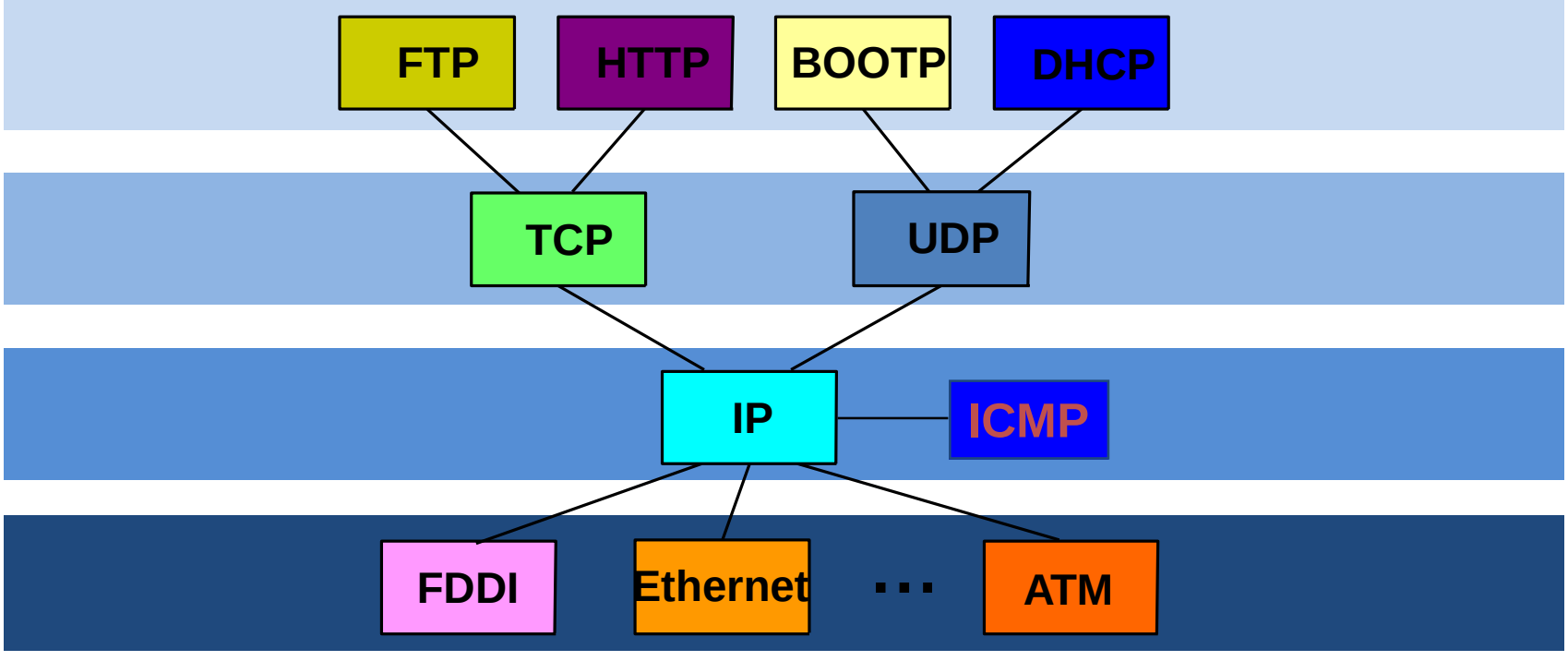
Internet Control Message Protocol (ICMP)



Why ICMP is used?

- IP companion protocol (not necessary)
- Handles error and control messages
- IP is best effort; i.e., packets can be:
  - Lost,
  - delayed,
  - duplicated,
  - delivered out of order
  - corrupted.
- Best-effort, however, does not mean careless;
- IP attempts to avoid/ detect errors (without guarantees)

- ICMP is used for:
- Error reporting
- Information querying

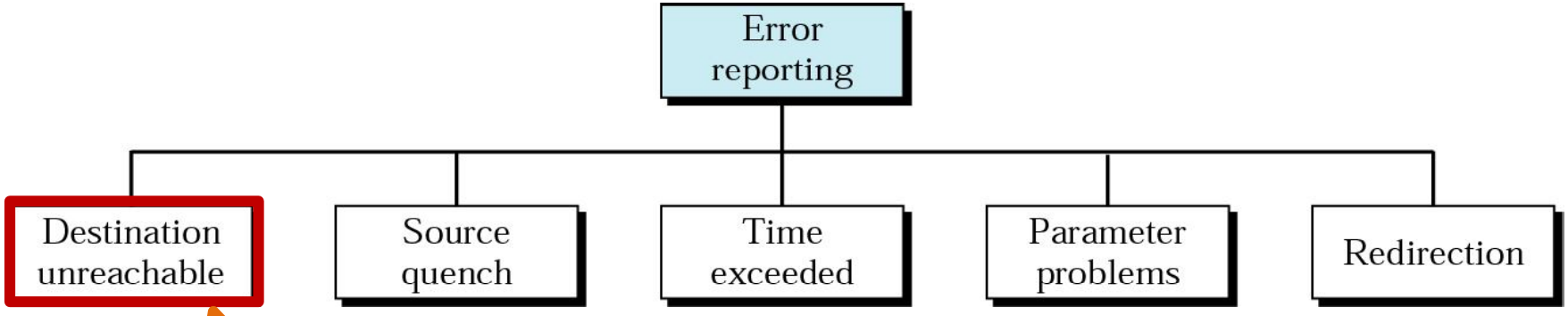
ICMP Message

- The IP protocol has no error-reporting or error-correcting mechanism. Moreover, the IP protocol also lacks a mechanism for host and management queries. The ICMP has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

- **Error messages**
  - Destination unreachable (protocol, port, or host)
  - Reassembly failed
  - IP Checksum failed; or invalid header
  - TTL exceeded (so datagrams don't cycle forever)
  - Cannot fragment

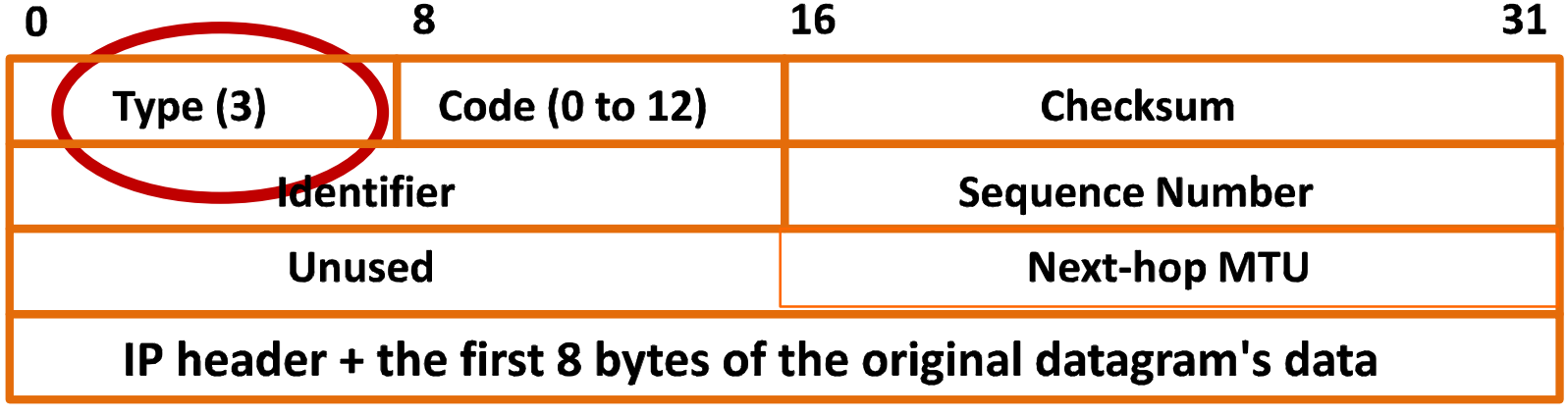
- **Control or information querying messages**
  - Echo (ping) request and reply
  - Redirect (from router to source host, to change route)

ICMP Error Messages

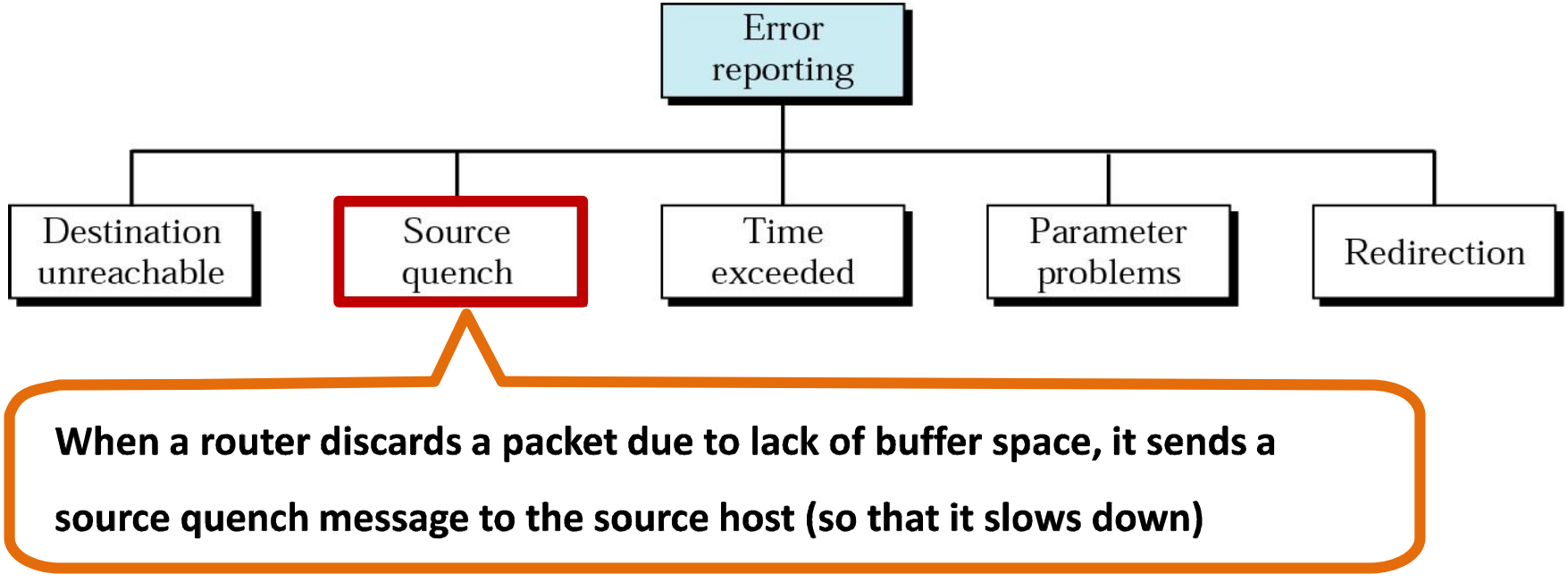


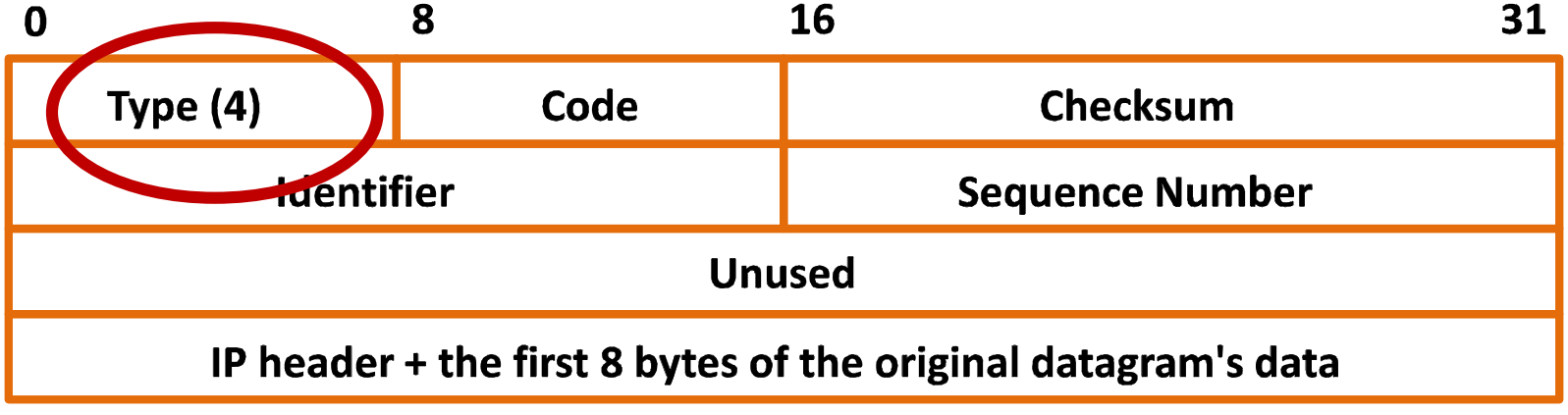
Sent when a router determines that a packet cannot be delivered.

It is specified whether destination host/ network is unreachable

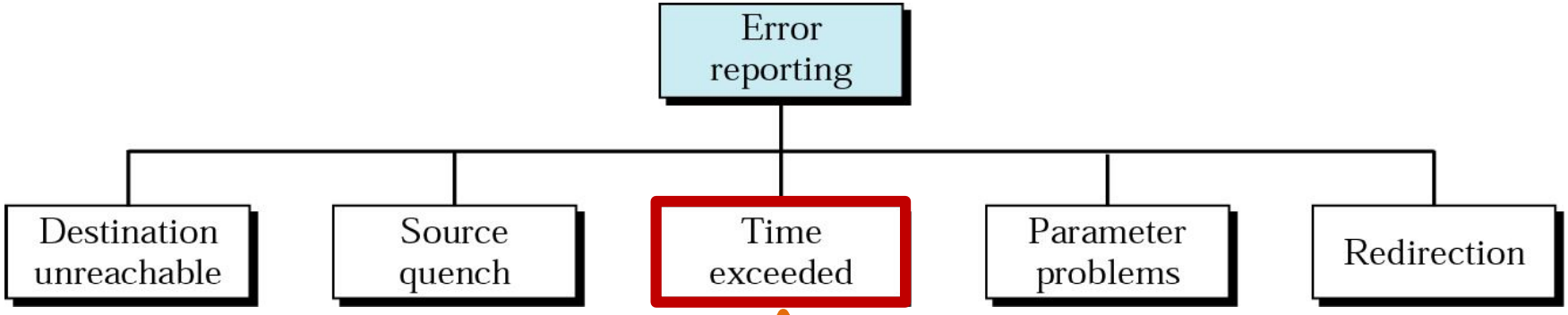


ICMP Error Messages



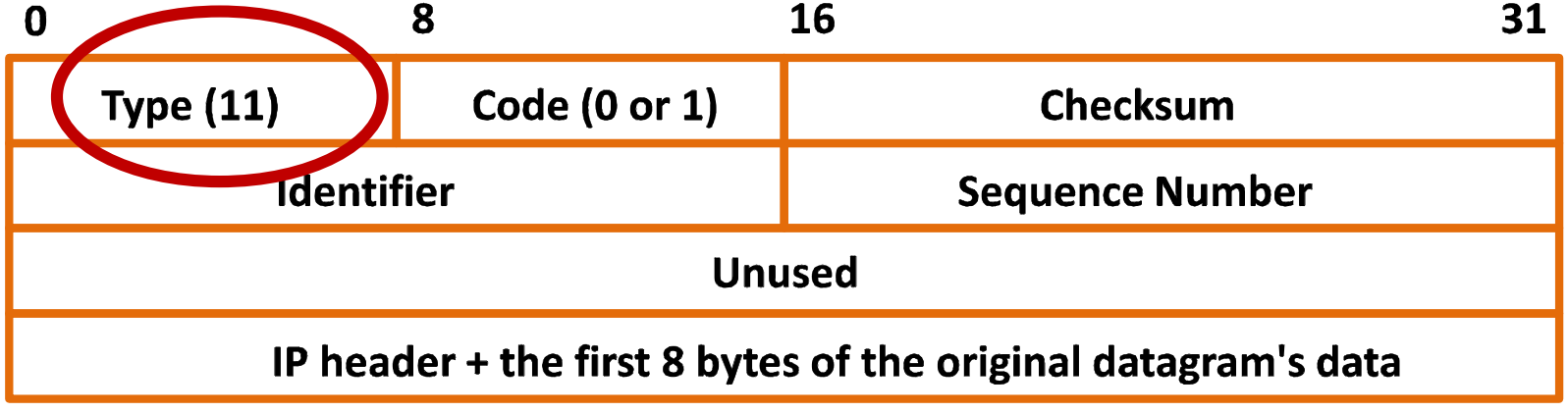


ICMP Error Messages

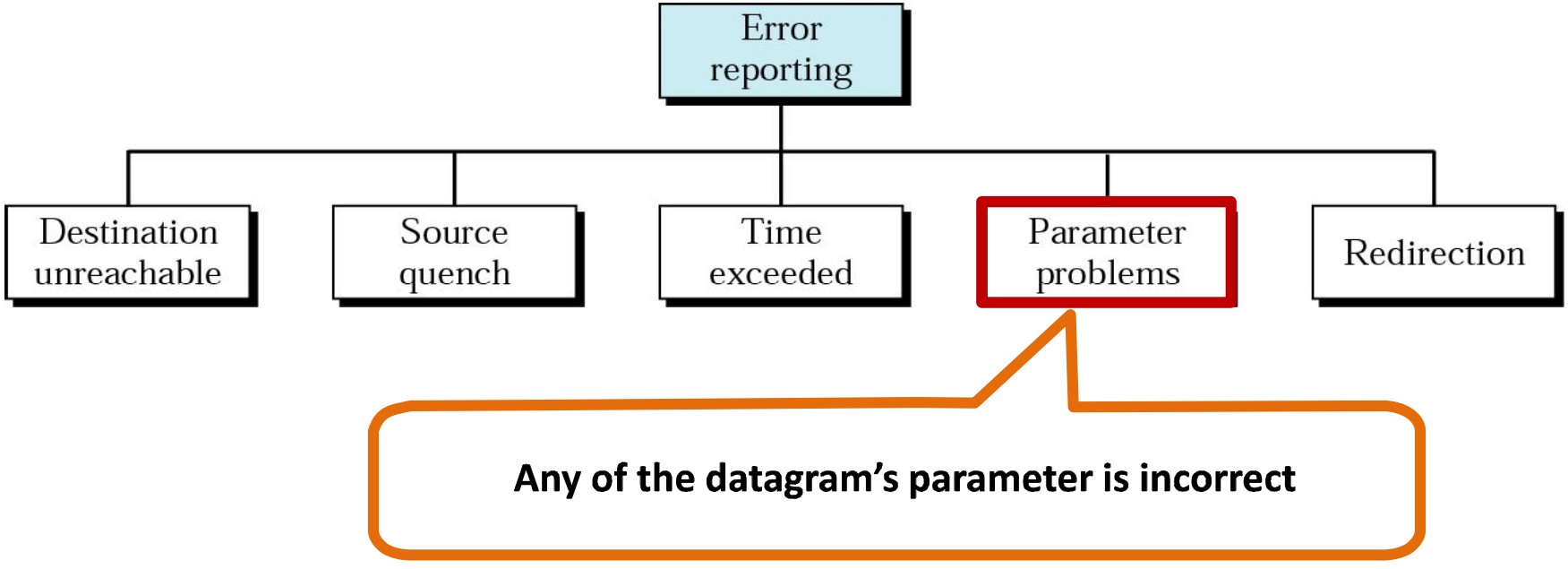


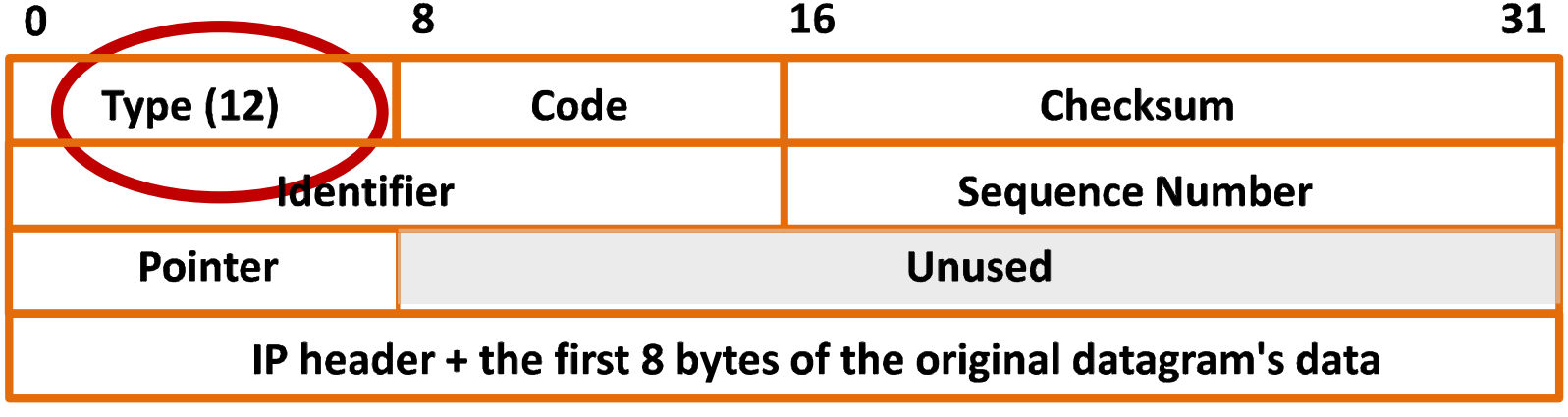
"Time exceeded" ICMP message sent to datagram source in two cases:

1) **When Time to Live (TTL) is decremented to zero,**
2) **When Reassembly timer expires before all fragments arrive at dest.**

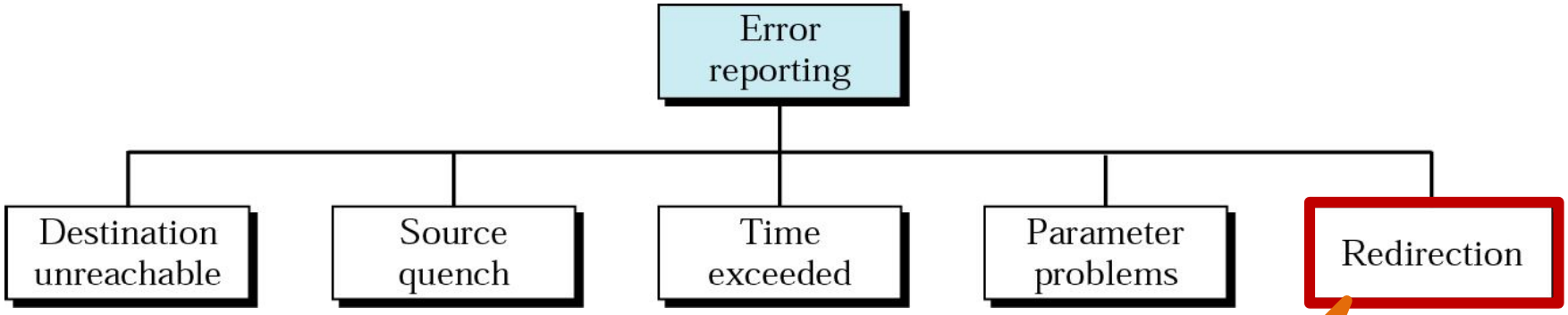


ICMP Error Messages



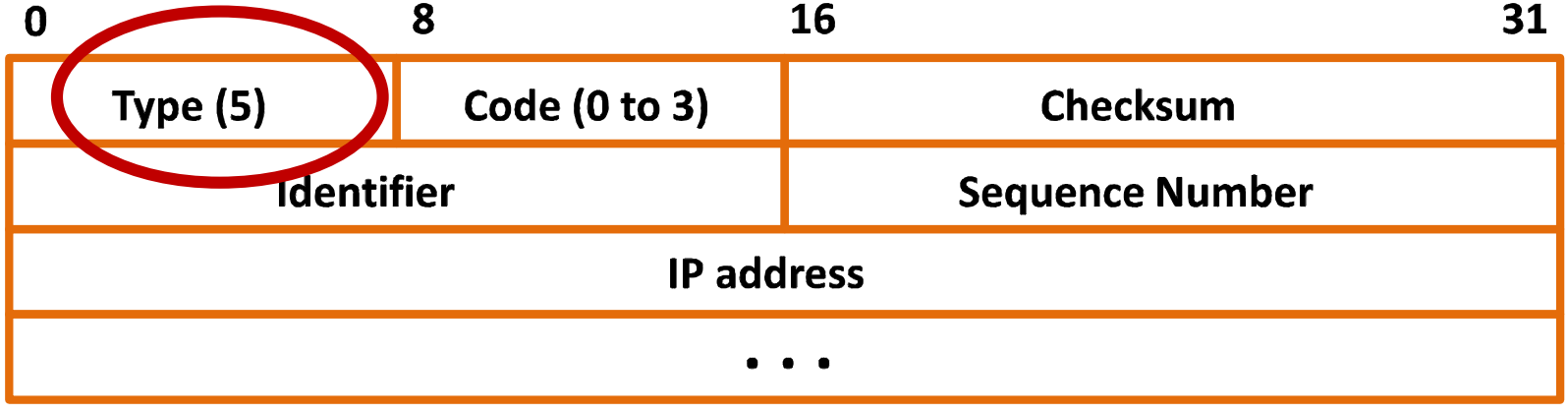


ICMP Error Messages

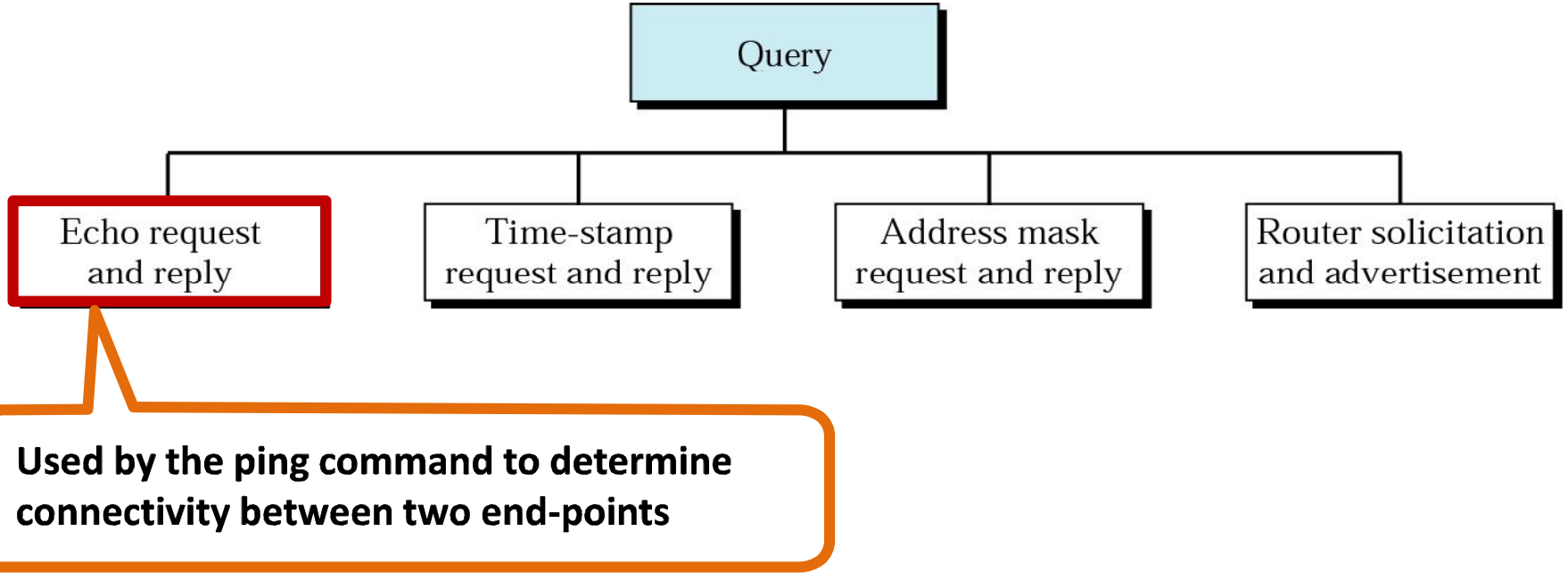


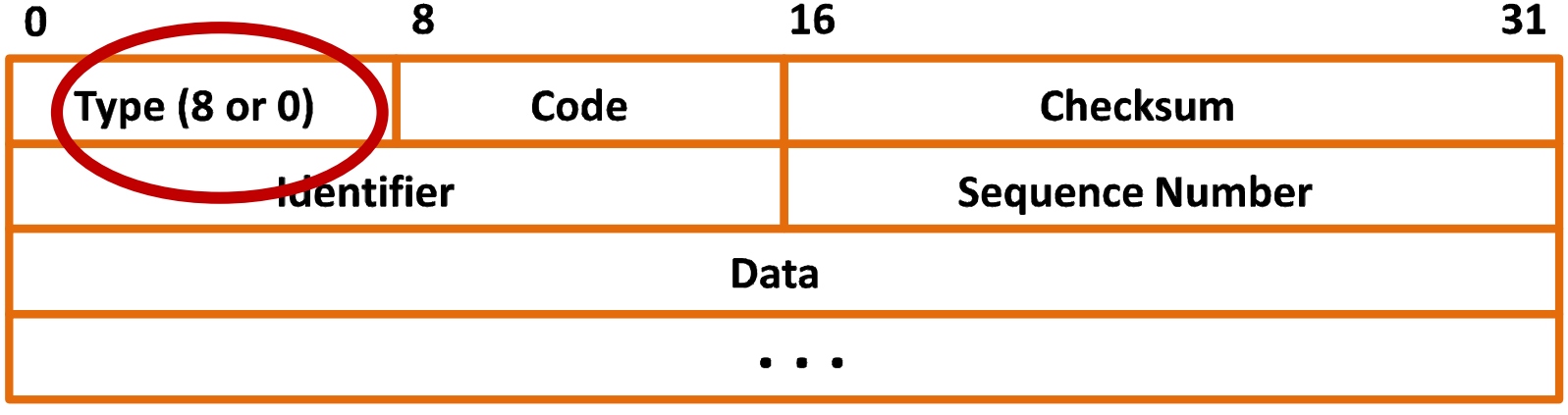
Sent if a router determines that a host has incorrectly sent datagram that should be sent to different router

Redirect can specify either a change for a host or complete network

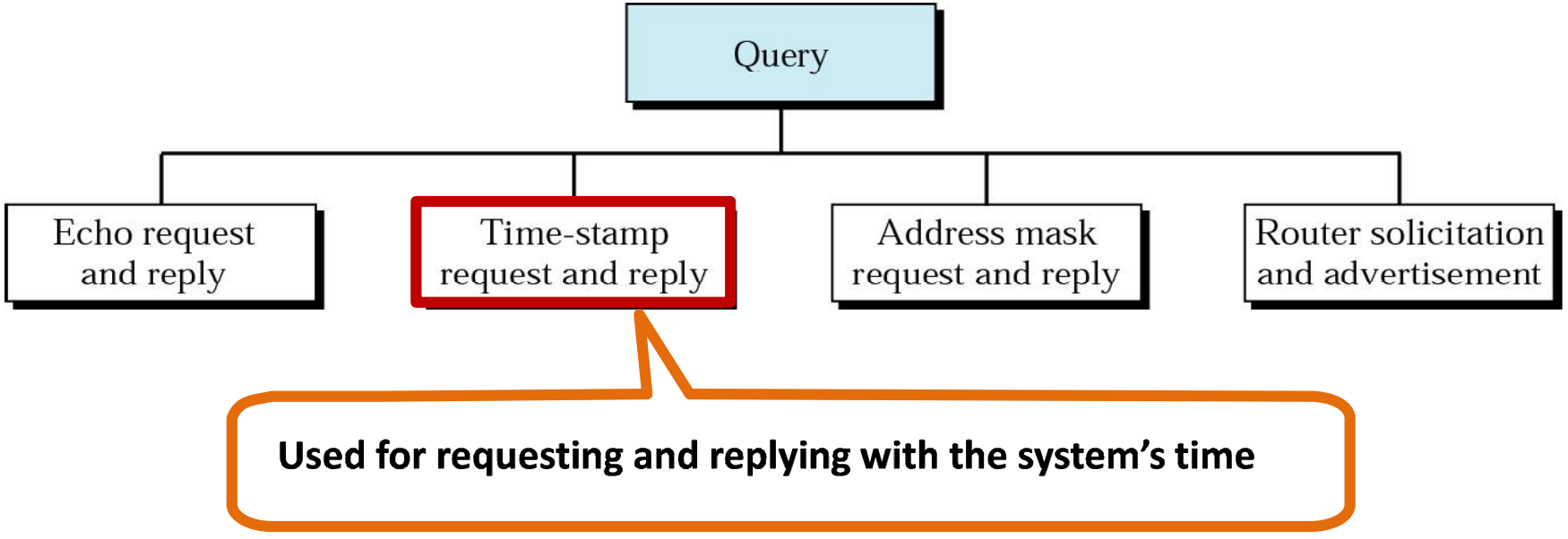


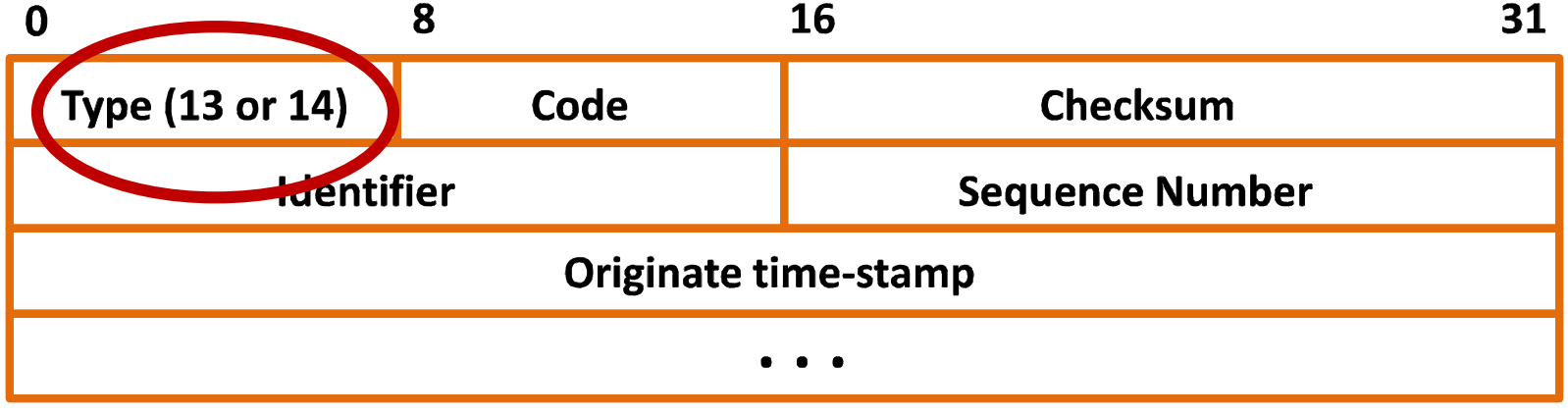
ICMP Control or Information Querying Messages



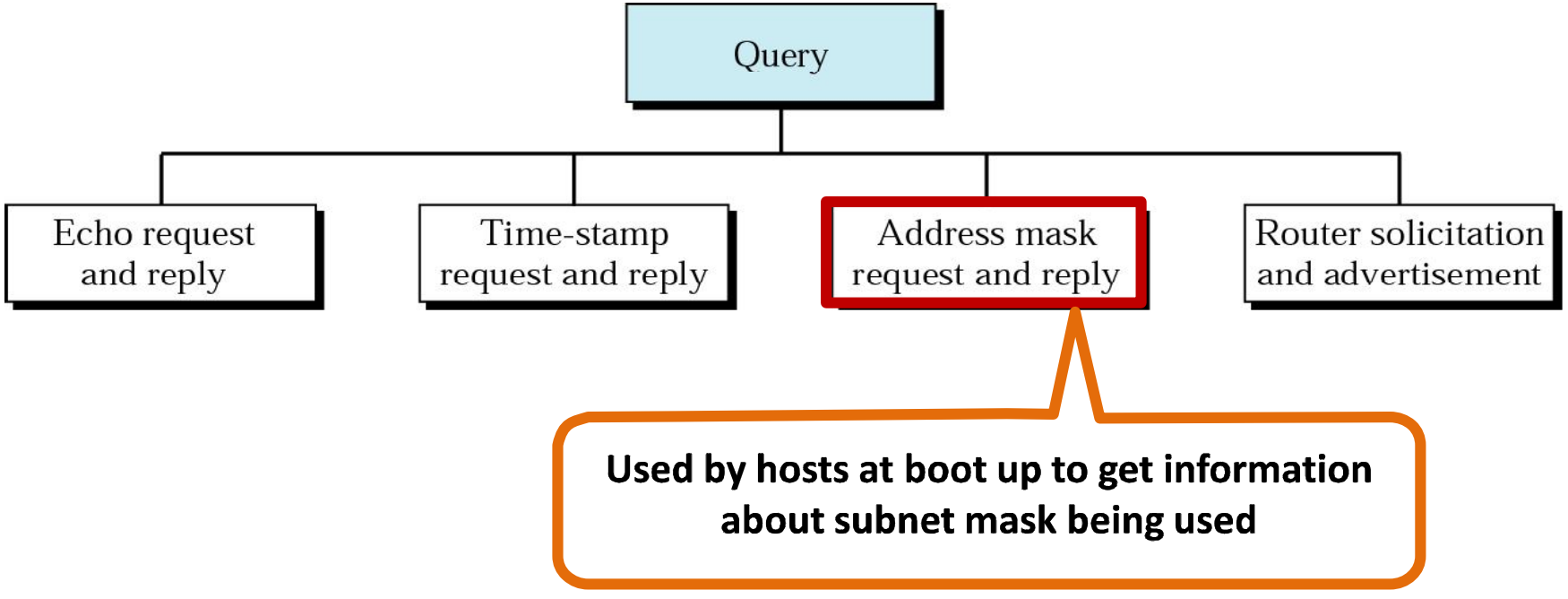


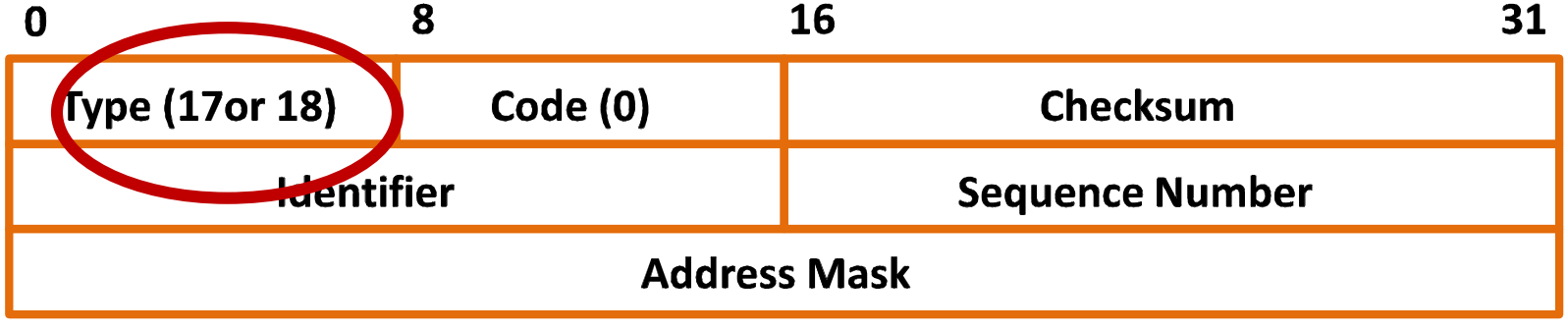
ICMP Control or Information Querying Messages



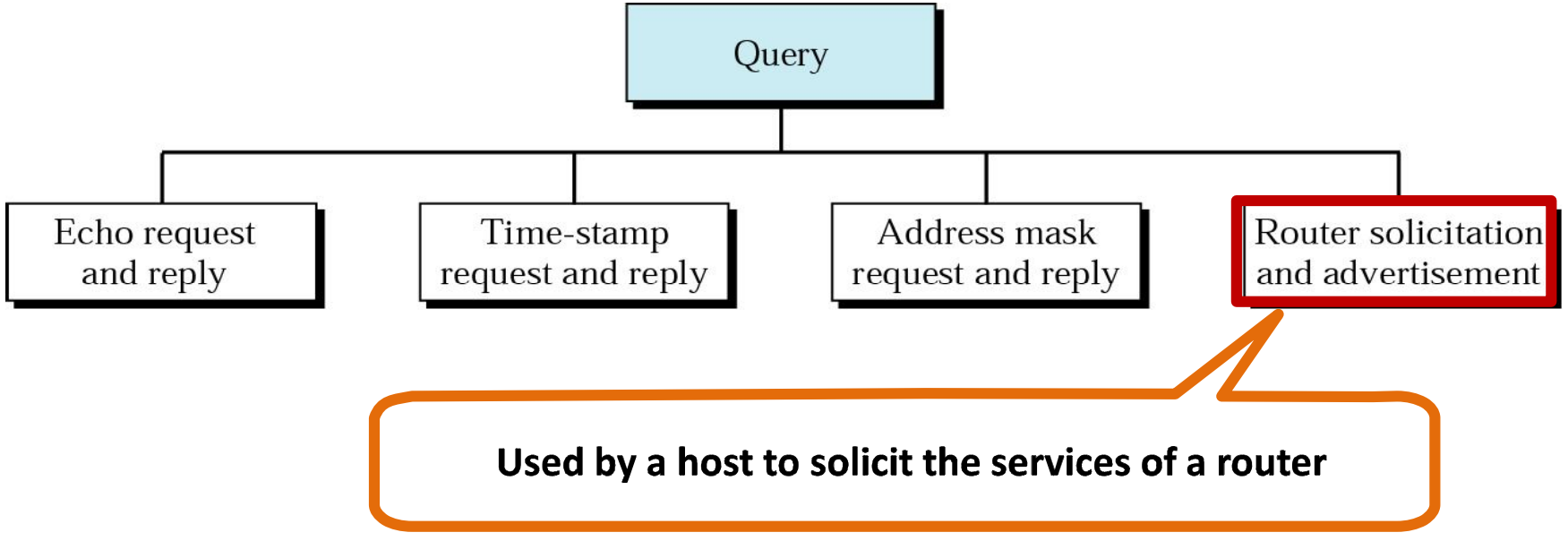


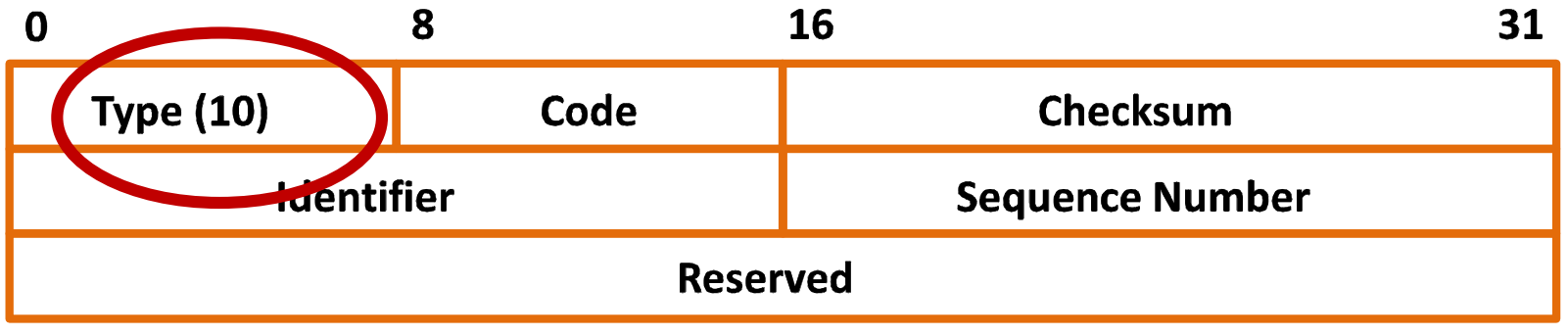
ICMP Control or Information Querying Messages





ICMP Control or Information Querying Messages





tracert: An Example of ICMP

C:\Windows\system32\cmd.exe

```
C:\Users\Azhar>tracert www.jinnah.edu.pk

Tracing route to jinnah.edu.pk [67.23.182.70]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2    35 ms    38 ms    36 ms  39.32.0.1
  3    36 ms    36 ms    50 ms  10.80.80.6
  4    36 ms    34 ms    34 ms  10.0.2.5
  5    37 ms    36 ms    35 ms  10.0.1.2
  6    62 ms    60 ms    60 ms  203.99.170.250
  7    63 ms    62 ms    63 ms  rwp44.pie.net.pk [221.120.253.25]
  8    63 ms    59 ms    63 ms  rwp44.pie.net.pk [221.120.254.30]
  9    61 ms    62 ms    63 ms  static.khi77.pie.net.pk [202.125.128.171]
 10   160 ms   160 ms   159 ms  pos0-0-0.palermo1.pal.seabone.net [195.22.198.20
6]
 11   304 ms   285 ms   327 ms  ge0-0.newark4.new.seabone.net [195.22.216.239]
 12   349 ms   305 ms   273 ms  te-4-2.car3.Newark1.Level3.net [4.71.148.9]
 13   291 ms   343 ms   289 ms  ae-32-52.ebr2.Newark1.Level3.net [4.69.156.62]
 14   289 ms   288 ms   287 ms  ae-4-4.ebr2.Washington1.Level3.net [4.69.132.101
]
 15   386 ms   289 ms   289 ms  ae-62-62.csw1.Washington1.Level3.net [4.69.134.1
46]
 16   342 ms   306 ms   306 ms  ae-61-61.ebr1.Washington1.Level3.net [4.69.134.1
29]
 17   327 ms   306 ms   306 ms  ae-2-2.ebr3.Atlanta2.Level3.net [4.69.132.85]
 18   327 ms   289 ms   288 ms  ae-73-73.ebr2.Atlanta2.Level3.net [4.69.148.254]

 19   311 ms   339 ms   305 ms  4.69.159.53
 20   332 ms   306 ms   306 ms  IMMEDION-LL.edge5.Atlanta2.Level3.net [4.71.254.
78]
 21   316 ms   306 ms   290 ms  67.23.161.143
 22   354 ms   291 ms   320 ms  67.23.161.133
 23   292 ms   292 ms   374 ms  core13.hostingmadeeasy.com [67.23.182.70]

Trace complete.

C:\Users\Azhar>_
```

ping: An Example of ICMP

```
D:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\jq> ping 192.168.15.1

Pinging 192.168.15.1 with 32 bytes of data:

Reply from 192.168.15.1: bytes=32 time=3ms TTL=255
Reply from 192.168.15.1: bytes=32 time<1ms TTL=255
Reply from 192.168.15.1: bytes=32 time<1ms TTL=255
Reply from 192.168.15.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.15.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

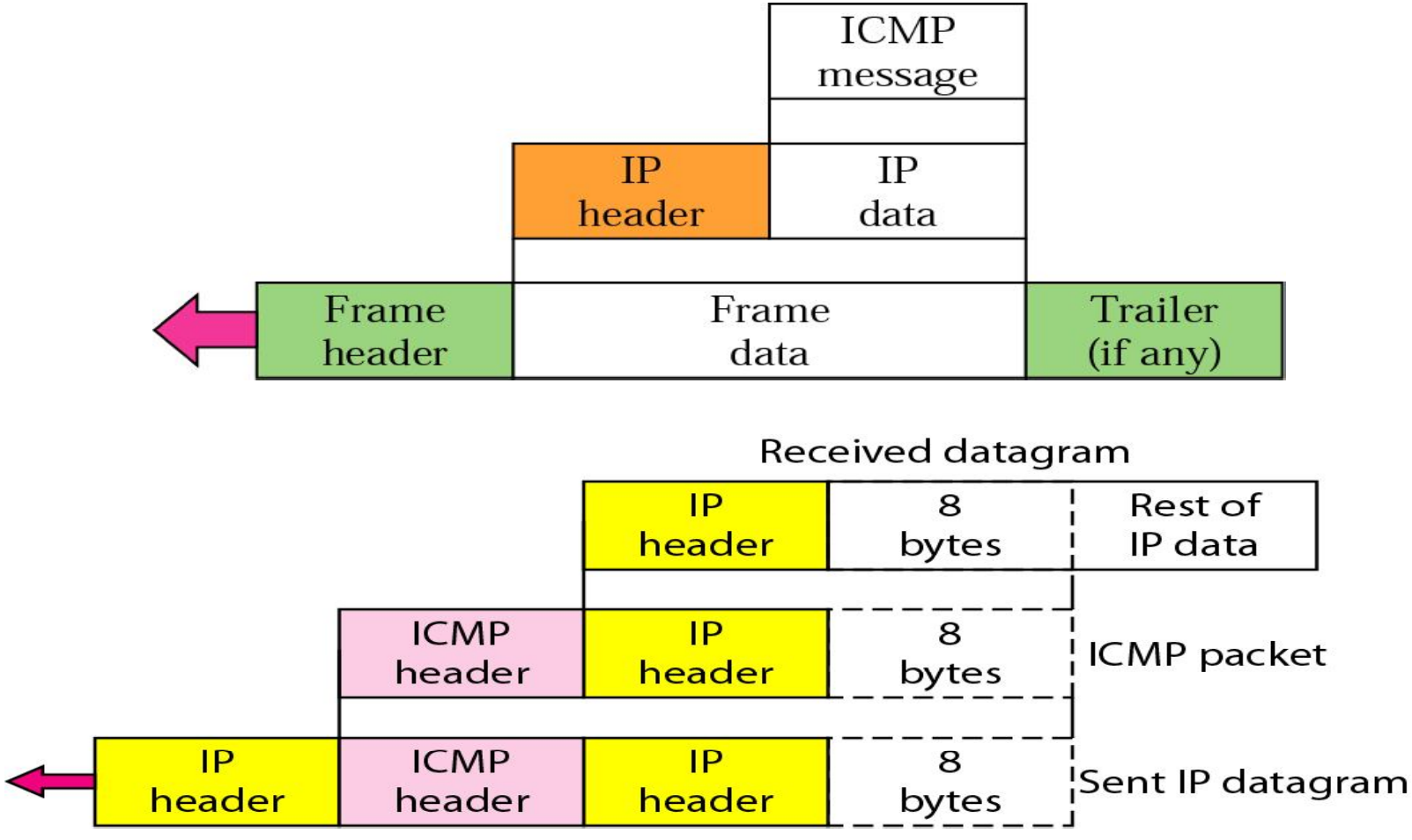
If ICMP reply is received, network connectivity is present

Important 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.

Where is ICMP Encapsulated?

- ICMP message included as part of IP data



ICMP Message Types

Type Field	ICMP Message Type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
6	Alternate Host Address
8	Echo Request
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Type Field	ICMP Message Type
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris

Douglas Comer's book