# Internet Control Message Protocol - ICMP

Introduction

- The Internet Protocol has no error-reporting or error-correcting mechanism.

- The Internet Protocol also lacks a mechanism for host and management queries.

- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies.

- ICMP is a companion to the Internet Protocol .

Types of Messages
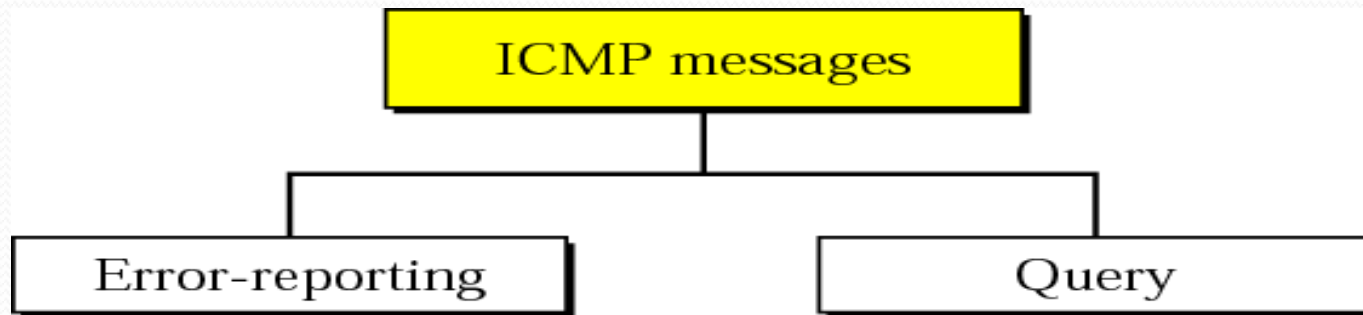
- Error Reporting Messages
  - A router or hosts reports the problems encountered when it processes a packet
- Query Messages
  - Helps a host or a network manager to get specific information from a router or another host
  - Ex: nodes can discover their neighbor

ICMP Message Format

8 byte header

| 8 bits	8 bits	8 bits	8 bits
Type	Code	Checksum	
Rest of the header			
Data section			
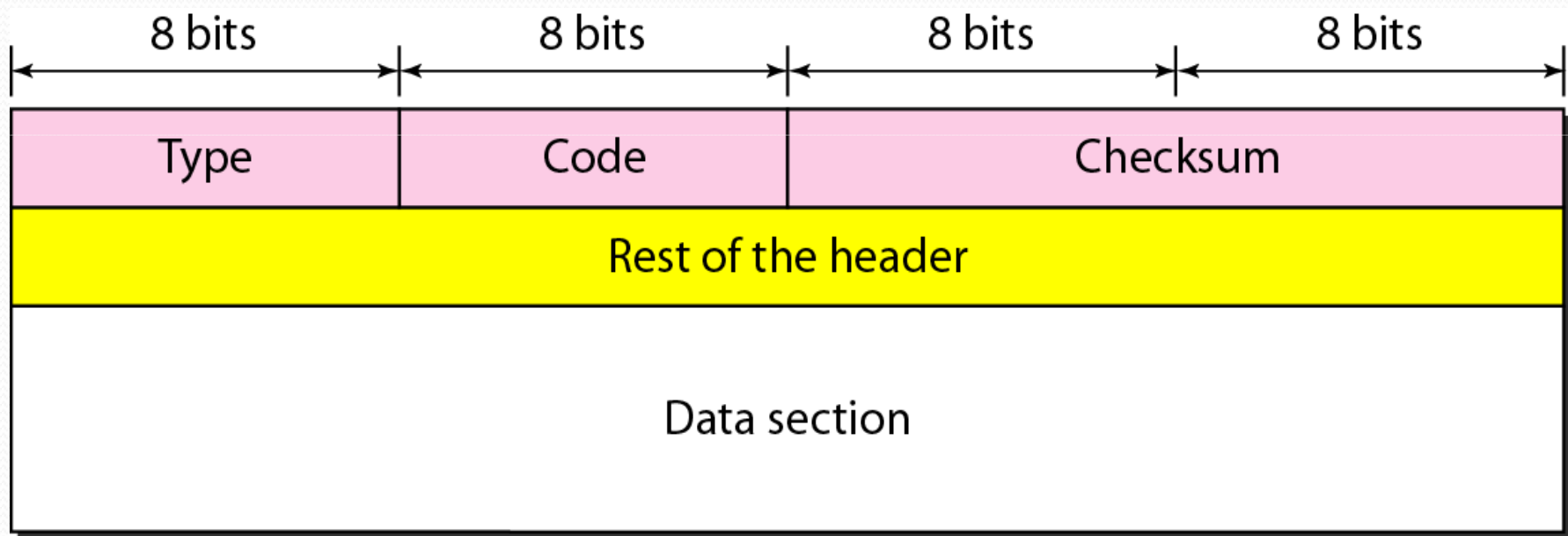
ICMP Message Format

- Type (1 byte)
  - Type of ICMP message
  - Thirteen message type are defined
- Code (1 byte)
  - Subtype of ICMP message
- Checksum (2 bytes)
  - Similar to IP header checksum
  - Checksum is calculated over entire ICMP message
- Additional (4 bytes)
  - If there is no additional data, the 4 bytes set to zero
    → each ICMP messages is at least 8 bytes long

ICMP Message types

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

ICMP Error Message
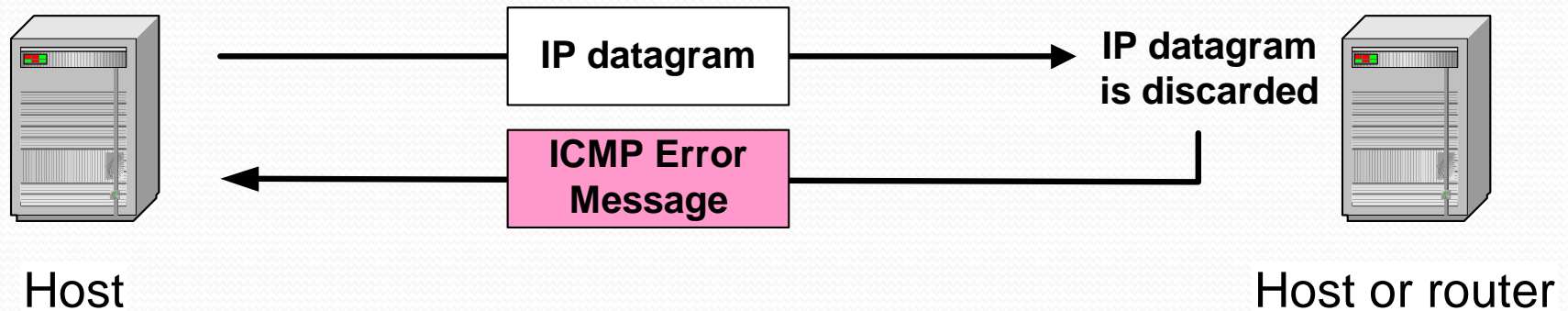
- ICMP error messages report error conditions
- Typically sent when a datagram is discarded
- Error message is often passed from ICMP to the application program

Encapsulation of ICMP error with IP

Received datagram

IP header	8 bytes	Rest of IP data

ICMP header	IP header	8 bytes	ICMP packet

IP header	ICMP header	IP header	8 bytes	Sent IP datagram
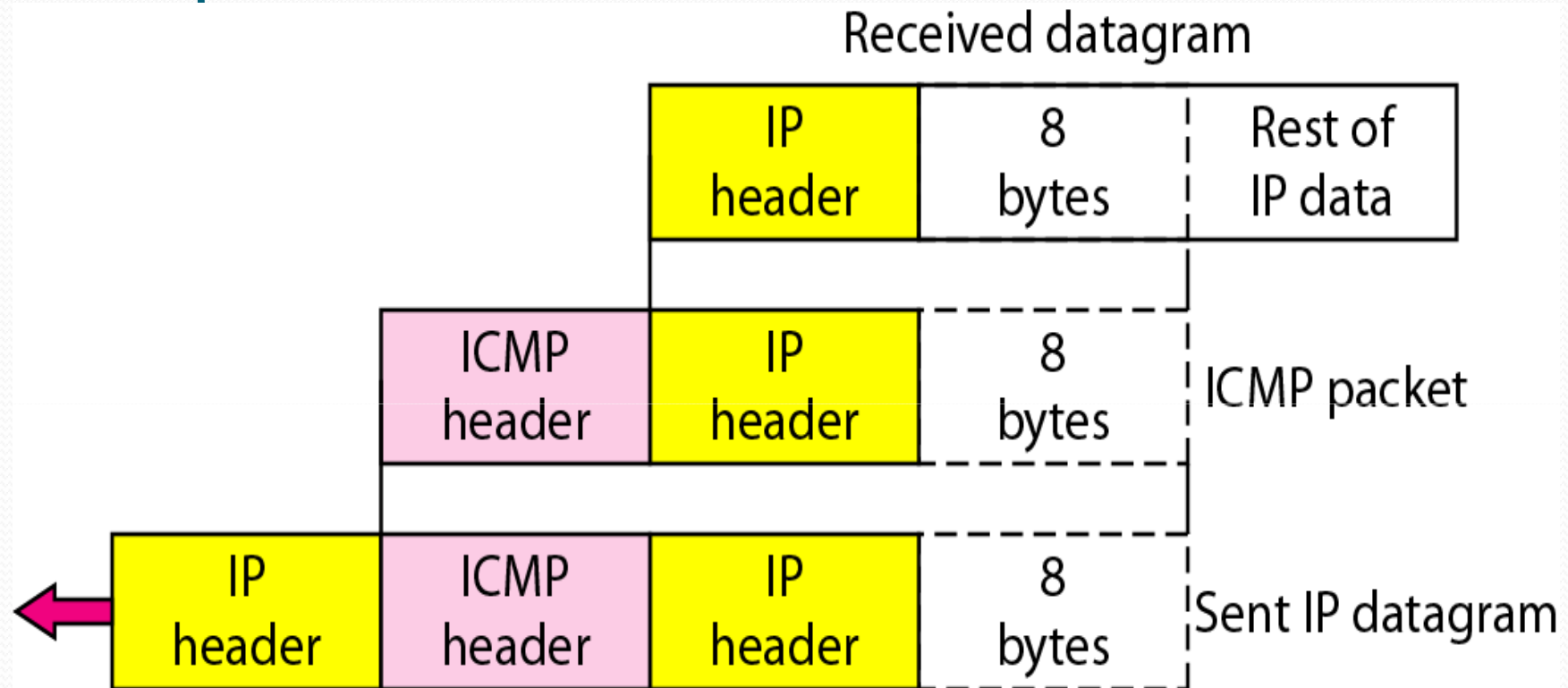
- 8 bytes provide port numbers (UDP & TCP) and sequence numbers (TCP)

25-Feb-15   Unit II   8
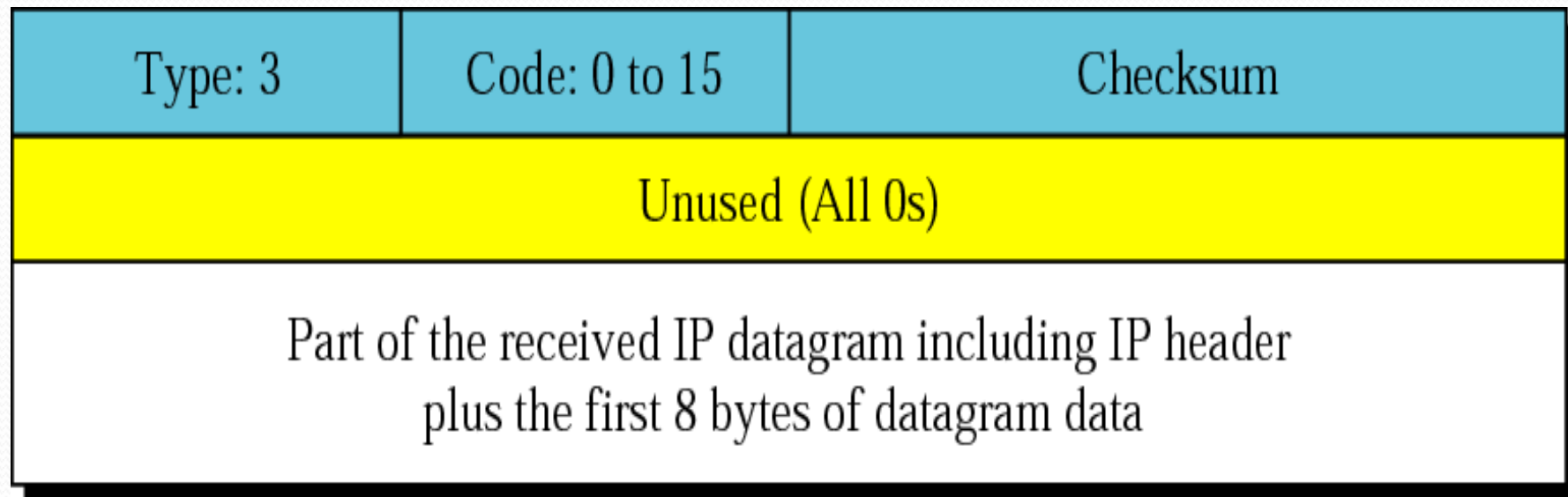
Types of Errors handled
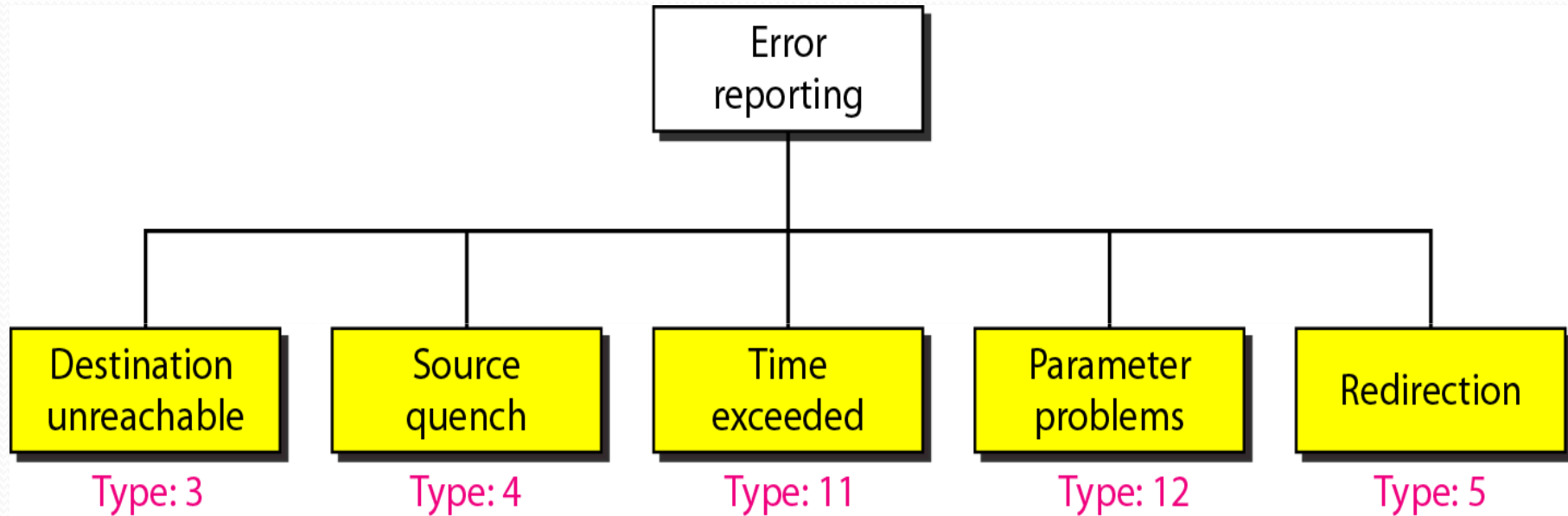
Points to note

- ICMP error messages will not be generated
  - in response to a datagram carrying an ICMP error message.
  - For a fragmented datagram that is not the first fragment.
  - For a datagram having a multicast address.
  - For a datagram having a special address such as 127.0.0.0 or 0.0.0.0

a. Destination unreachable

- Notification that an IP datagram could not be forwarded and was dropped
- Some Destination-unreachable messages can be created only by the destination host. Others can be created only by routers.

| 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		

a. Destination unreachable

- Codes:
  - 0 - net unreachable ; 1 - host unreachable
  - 2 - protocol unreachable ; 3 - port unreachable
    - sent by destination host IP module
  - 4 - fragmentation needed DF set ; 5 source route failed
  - 6 - destination network unknown ;
  - 7 destination host unknown
  - 8 - source host isolated ;
  - 9 - comm. with destn network prohibited
  - 10 - comm. With dest host prohibited ;
  - 11 - network unreachable for service
  - 12 - host unreachable for service

Example: ICMP Port Unreachable

Request a service
at a port 80

Client

No process is
waiting at port
80

Server

Port
Unreachable
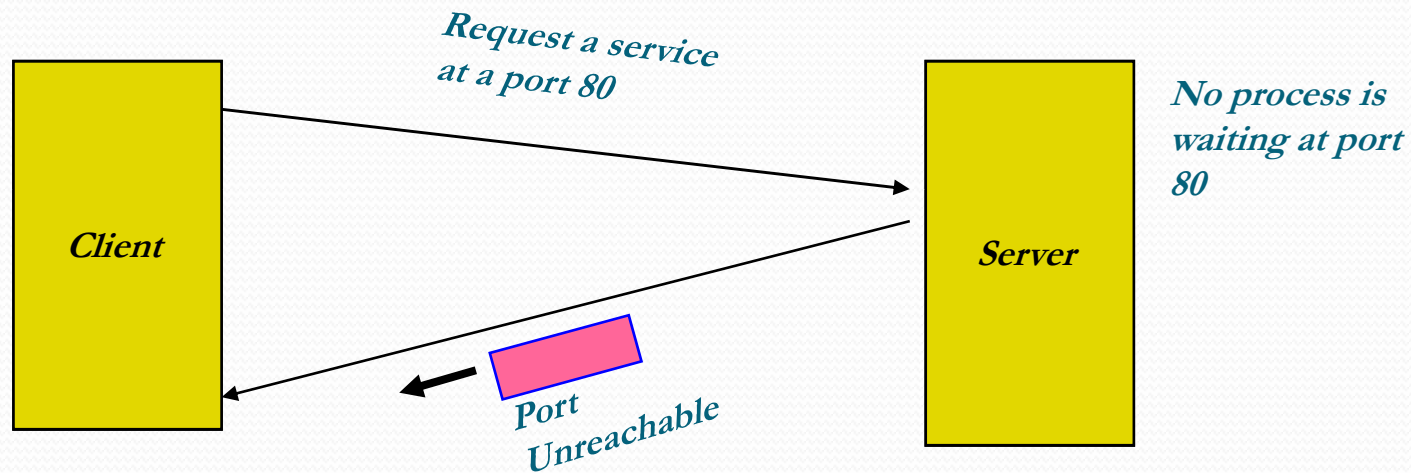
b. Source Quench

- 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		
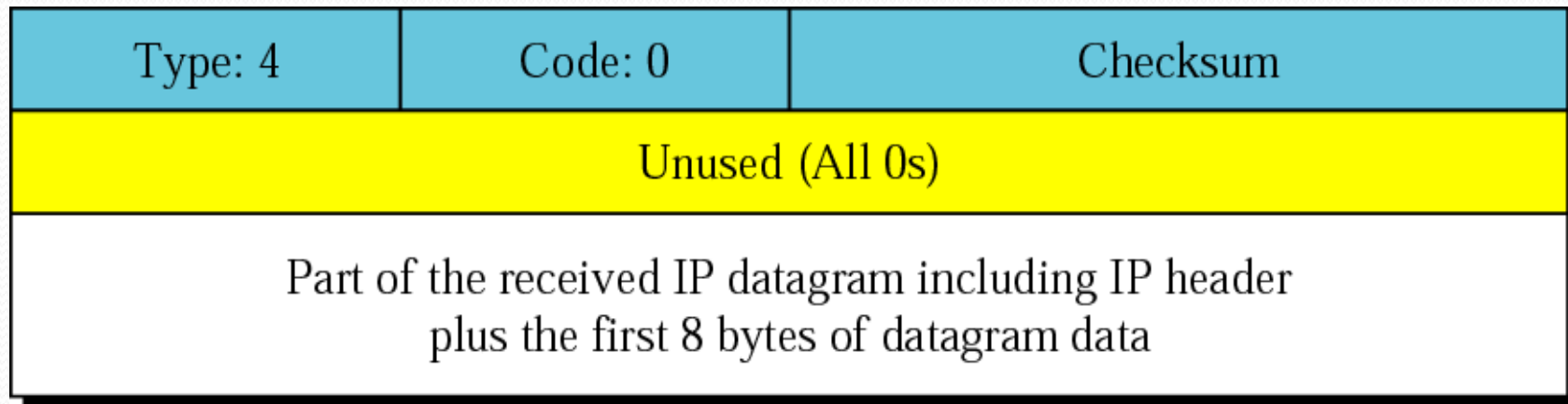
c. Time Exceeded

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		

d. Parameter Problem

- The ICMP Parameter problem message is generated as a response for any error not specifically covered by another ICMP message

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

| 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		

e. Redirection

- A router sends a message to a host when it determines a datagram that originated from the host must be forwarded to router that can be directly reached

- Code:
  - 0 - redirect datagrams for the network
  - 1 - redirect datagrams for the host
  - 2 - redirect datagrams for the type of service and the network
  - 3 - redirect datagrams for the type of service and host

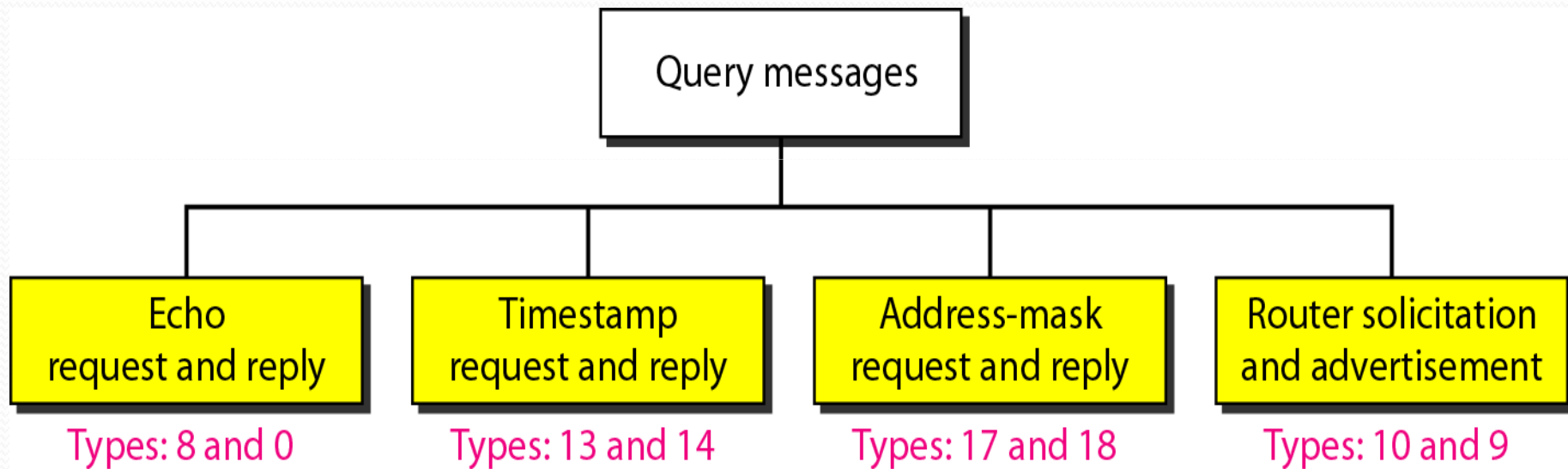| Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		
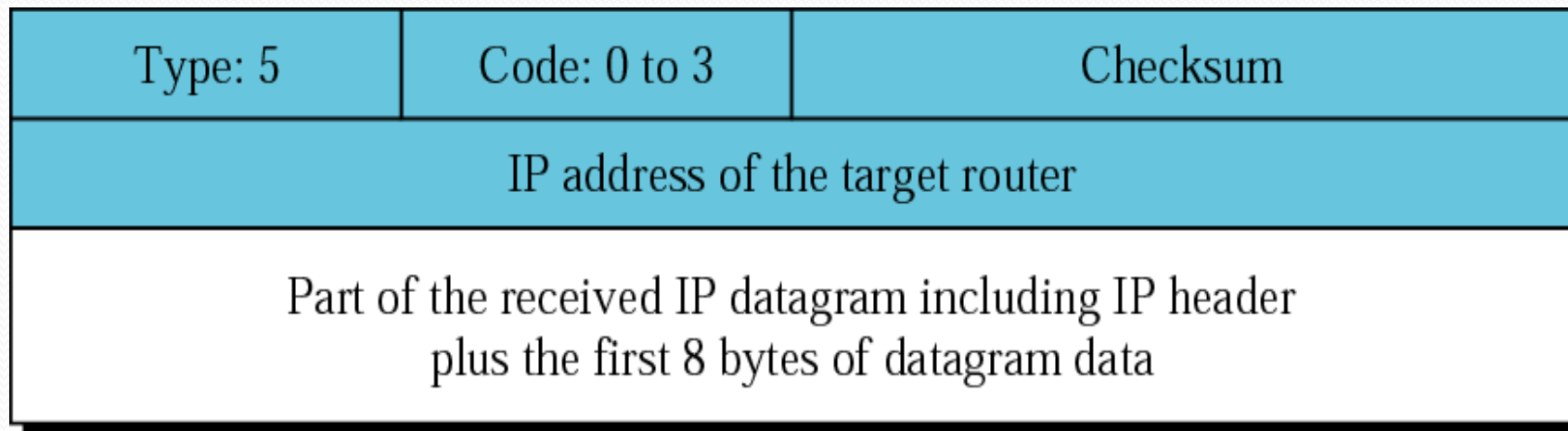
e. Redirection Concept
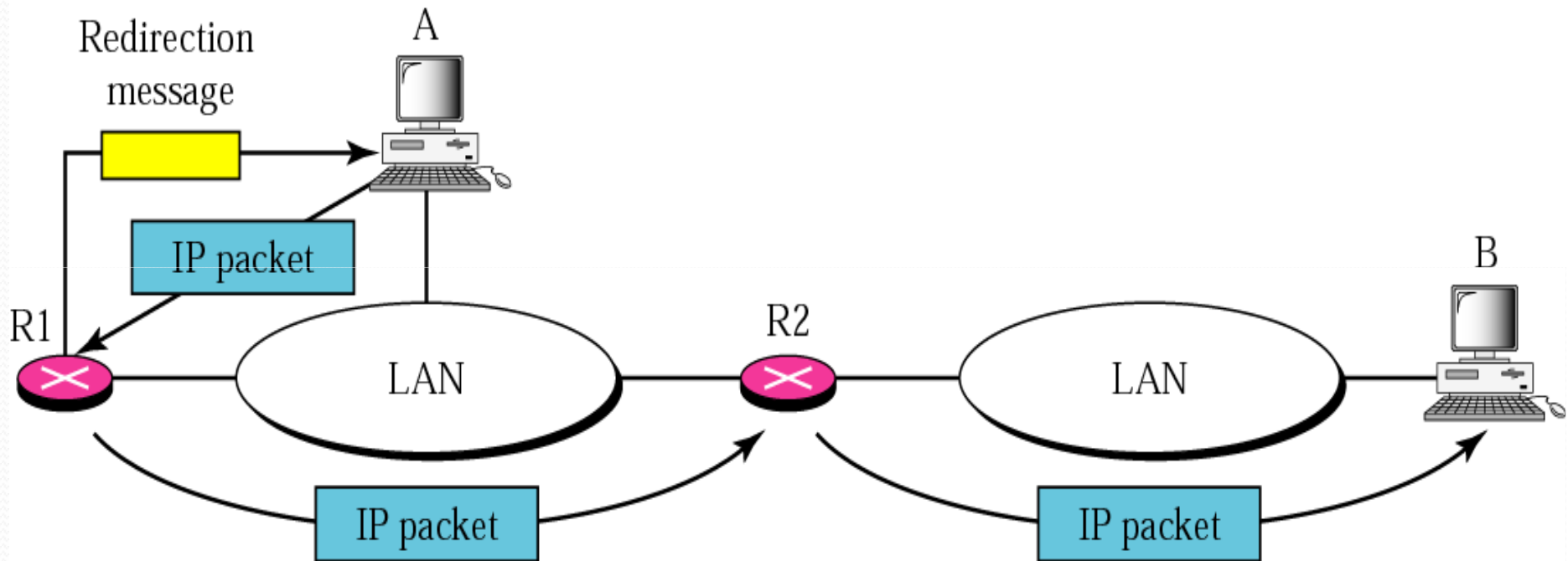
ICMP Query message
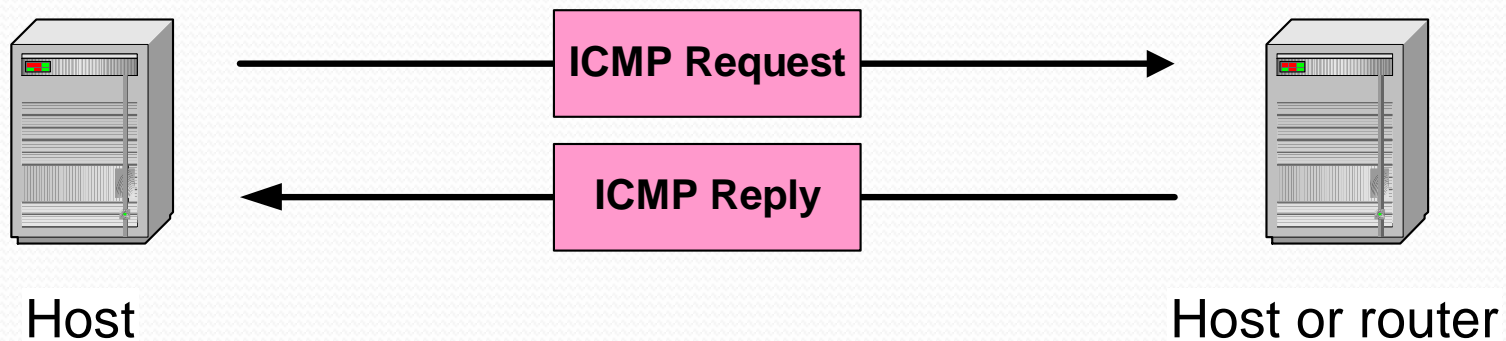
ICMP query:

- Request sent by host to a router or host
- Reply sent back to querying host

25-Feb-15   Unit II

Types of Query


```
                    ┌──────────────────┐
                    │  Query messages  │
                    └──────────────────┘
                             │
     ┌───────────────┬───────────────┬───────────────┐
┌──────────┐   ┌──────────┐    ┌──────────┐    ┌──────────┐
│  Echo    │   │Timestamp │    │Address-  │    │  Router  │
│ request  │   │ request  │    │mask      │    │solicit.  │
│and reply │   │and reply │    │request   │    │and adver.│
└──────────┘   └──────────┘    └──────────┘    └──────────┘
Types: 8 and 0  Types: 13 and 14  Types: 17 and 18  Types: 10 and 9
```

Echo request and reply — Types: 8 and 0

Timestamp request and reply — Types: 13 and 14

Address-mask request and reply — Types: 17 and 18

Router solicitation and advertisement — Types: 10 and 9

25-Feb-15   Unit II   20

Encapsulation of ICMP query with IP
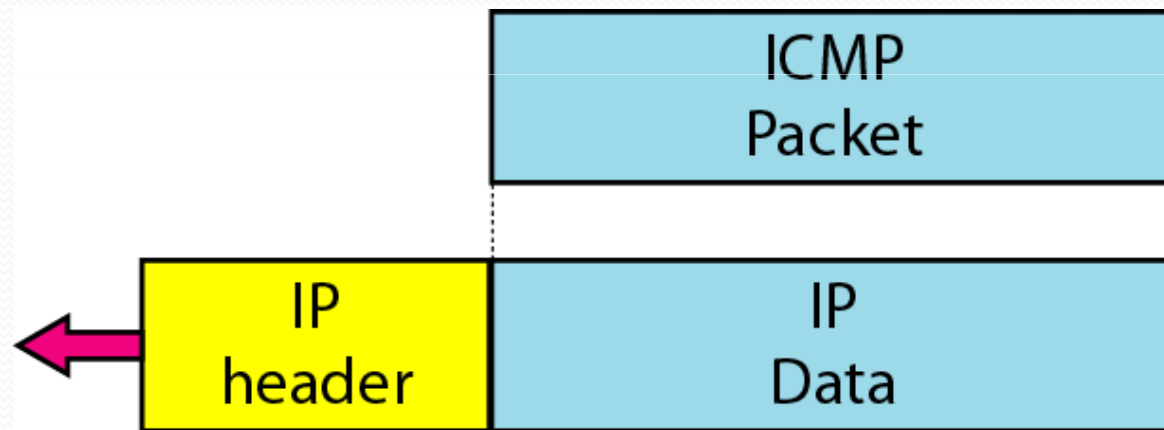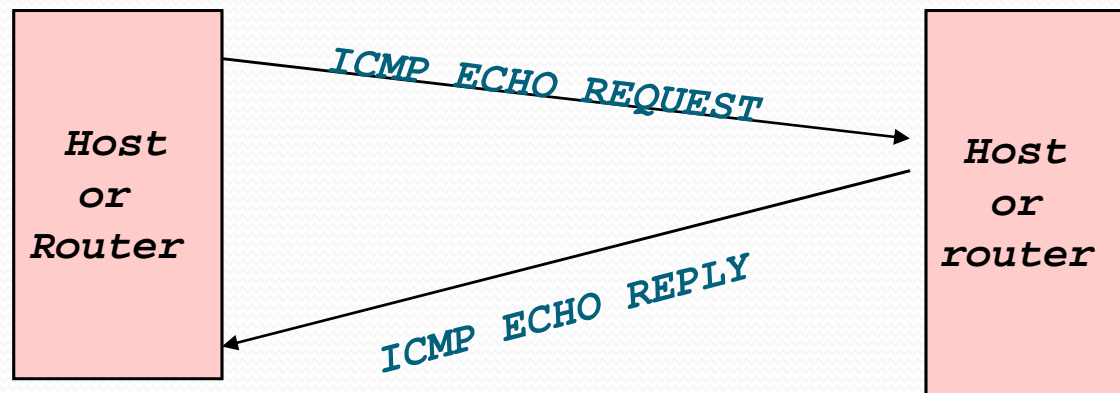
a. Echo Request and Reply

- An echo-request message can be sent by a host or router.
- An echo-reply message is sent by the host or router which receives an echo-request message.

8: Echo request
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		

Example of a Query: Echo Request and Reply

- Ping's are handled directly by the kernel
- Each Ping is translated into an ICMP Echo Request
- The Ping'ed host responds with an ICMP Echo Reply

```
Host          ICMP ECHO REQUEST          Host
or            ─────────────────▶         or
Router                                   router
              ◀─────────────────
              ICMP ECHO REPLY
```

b. Time stamp Request & Reply

- 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.

13: request
14: reply

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

c. Address Mask Request & Reply

- Hosts and routers can request the subnet address mask for the network they reside on at boot time.
    - Host or router broadcasts it on the local network
    - A receiving router should return it in a reply message

Type: 17 or 18	Code: 0	Checksum	
Identifier		Sequence number	
Address mask			

17: Request
18: Reply
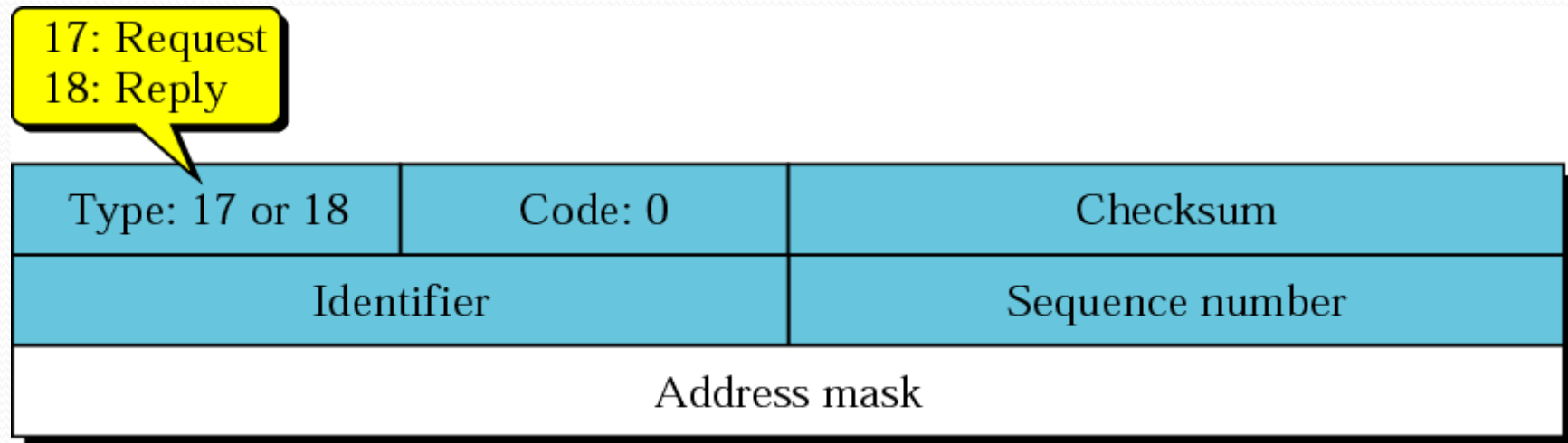
d. Router-solicitation & advertisement

Type: 10	Code: 0	Checksum
Identifier		Sequence number

Type: 9	Code: 0	Checksum
Number of addresses	Address entry size	Lifetime
Router address 1		
Address preference 1		
Router address 2		
Address preference 2		
⋮		