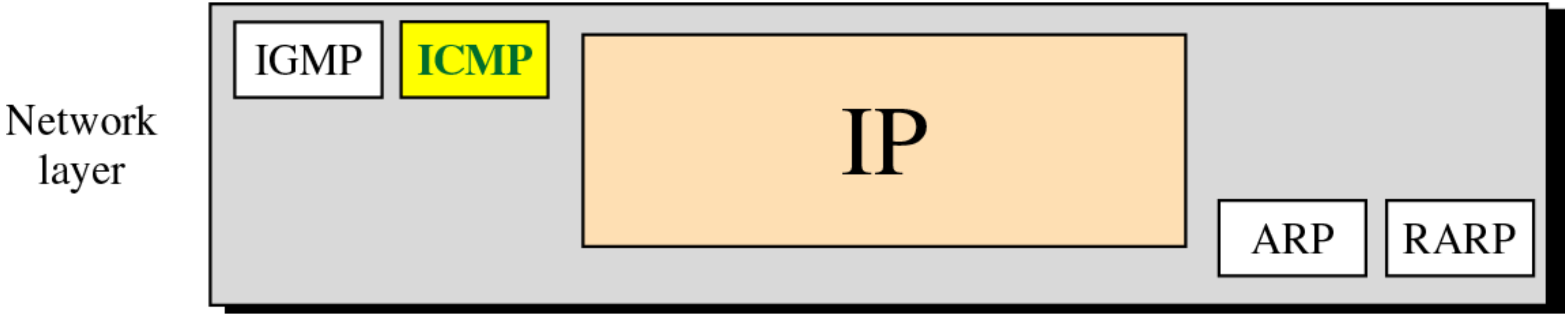
ICMP

Introduction to Internet Control Message Protocol (ICMP)

- IP protocol has no error-reporting or error-correcting mechanism
  - When errors occur, no built-in mechanism to notify the original host
- IP protocol also lacks a mechanism for host and management queries
  - A host sometimes needs to determine if a router or another host is alive
  - Network manager needs information from another host and router

Introduction to ICMP (cont'd)

- Position of ICMP in the network layer

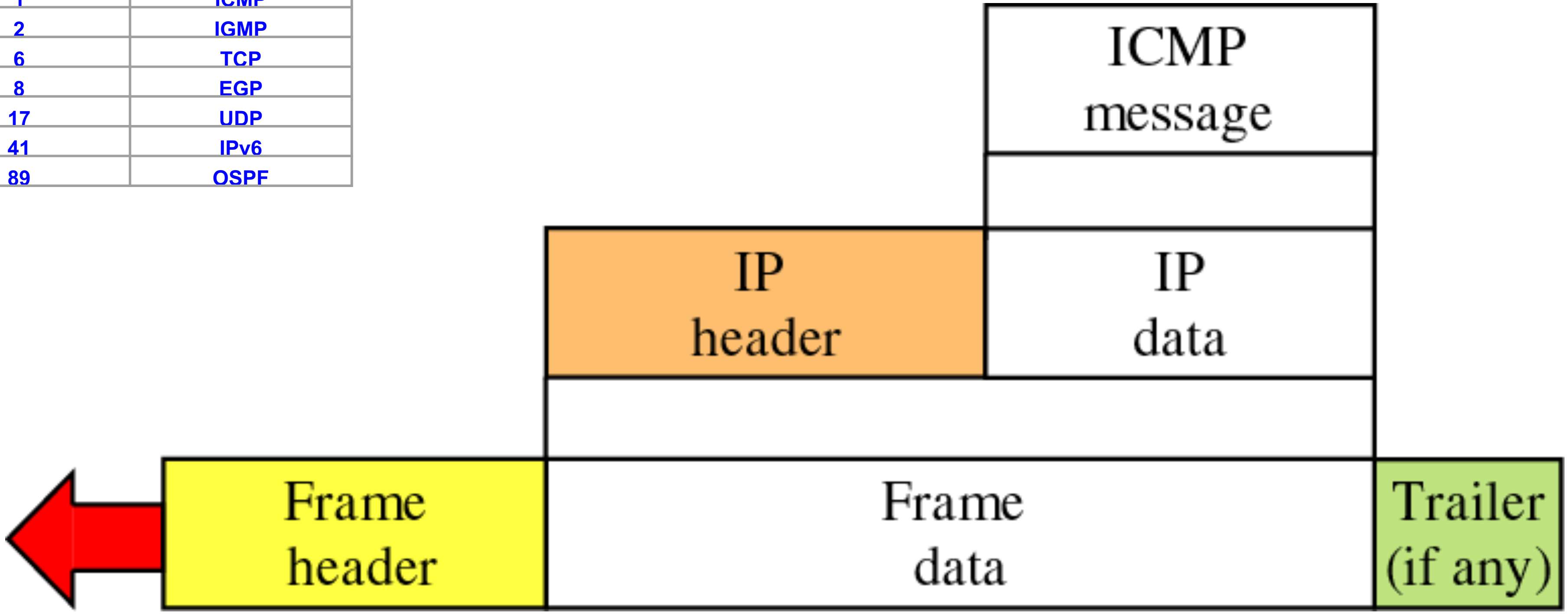


Introduction to ICMP (cont'd)

ICMP encapsulation

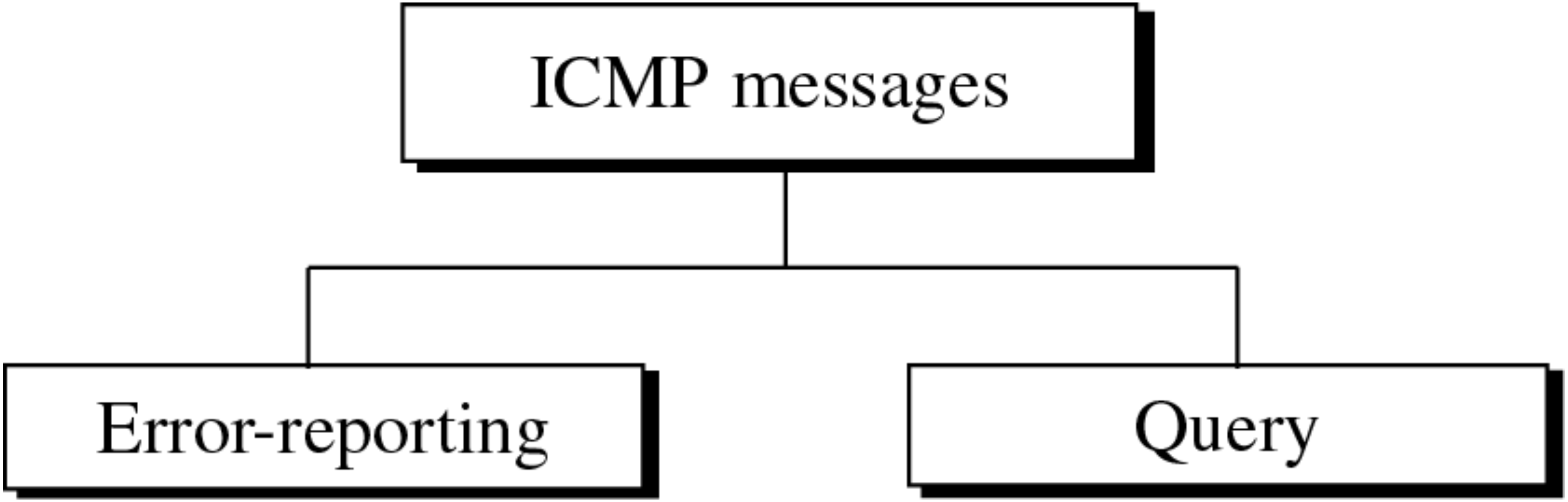
- The value of the protocol field in the IP datagram : 1

Value	Protocol
1	ICMP
2	IGMP
6	TCP
8	EGP
17	UDP
41	IPv6
89	OSPF



Types of Message

- Category of ICMP messages



Types of Message (cont'd)

- ICMP messages
  - Error reporting messages

Type	Message
3	Destination unreachable
4	Source quench
11	Time Exceeded
12	Parameter problem
5	Redirection

Types of Message (cont'd)

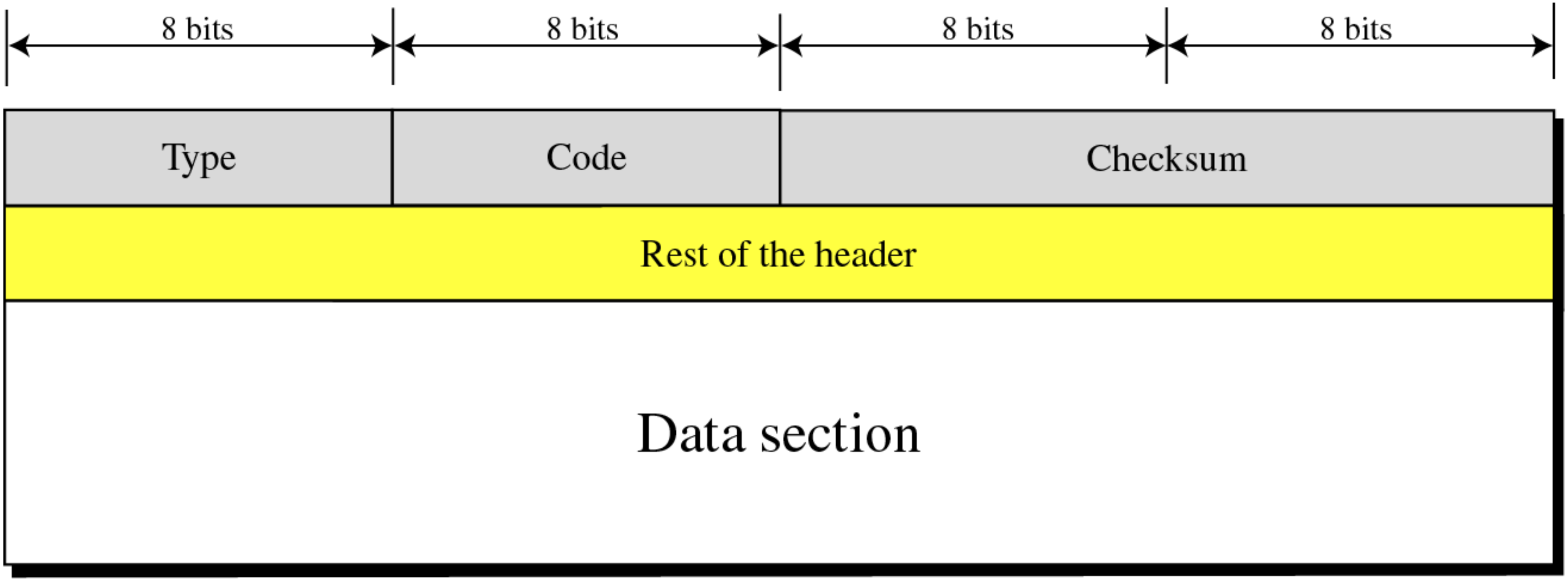
- ICMP messages
  - Query messages

Type	Message
8 or 0	Echo request or reply
13 or 14	Timestamp request and reply
17 or 18	Address mask request and reply
10 or 9	Router solicitation and advertisement

Message Format

- Having 8 byte header and variable-size data section
  - ICMP type : defining the type of the message
  - Code field : specifying the reason for the particular message type
  - Checksum field (for header and message)
  - Data section
    - In error message, carrying information for finding the original packet which caused the error
    - In query message, carrying extra information based on the type of the query

Message Format (cont'd)



8 bits

8 bits

8 bits

8 bits

Type

Code

Checksum

Rest of the header

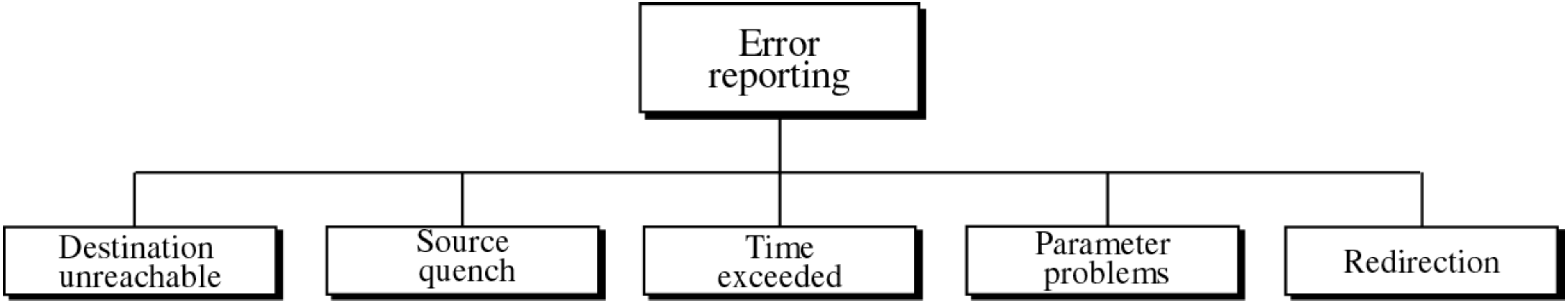
Data section

Error Reporting

- Error checking and control
- Not correcting errors : it is left to the higher level protocols
- Always reporting error messages to the original source

Error Reporting (cont’d)

- Error-reporting messages



Error Reporting (cont’d)

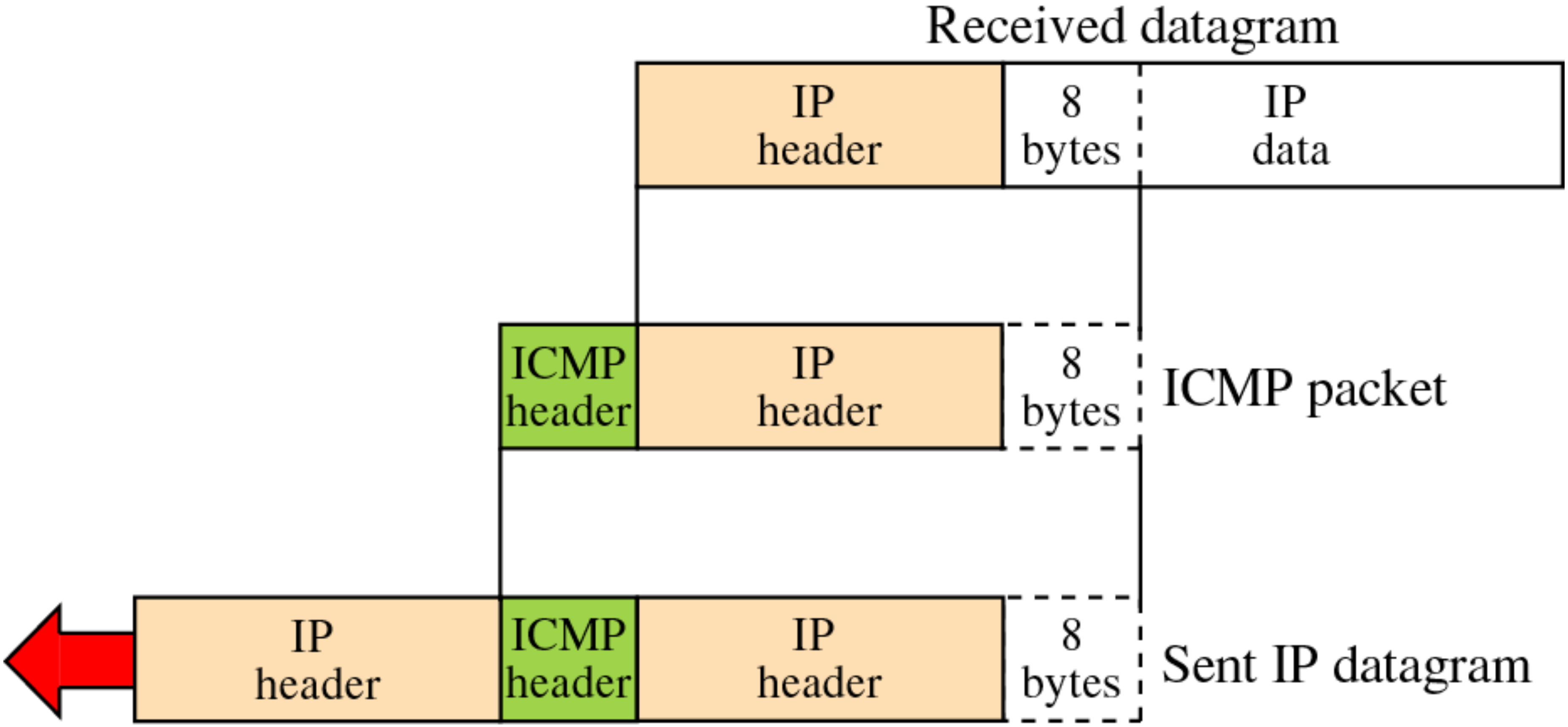
- Important points about ICMP error messages
  - No ICMP error message will be generated in response to a datagram carrying an ICMP error message
  - No ICMP error message will be generated for a fragmented datagram that is not the first fragment
  - No ICMP error message will be generated for a datagram 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 (cont'd)

- All error messages
  - containing a data section that includes the IP header of the original datagram + the first 8 bytes of data in that IP datagram
    - 8 bytes of data : port # (UDP and TCP) and sequence # (TCP)
      - Used for informing to the protocols (TCP or UDP) about the error situation

Error Reporting (cont'd)

- Contents of data field for the error messages



Error Reporting (cont'd)

❑ Destination Unreachable

- When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded.
- Then, the router or the host sends a destination unreachable message back to the source that initiated the datagram.
- Destination unreachable format

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		

Error Reporting (cont'd)

- **Code 0 :** network is unreachable, due to hardware failure, can only be generated by a router
- **Code 1 :** host is unreachable, due to hardware failure, can only be generated by a router
- **Code 2 :** protocol such as UDP, TCP or OSPF is not running at the moment.
  - generated only by the destination
- **Code 3 :** 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 has been set
- **Code 5 :** Source routing cannot be accomplished
- **Code 6 :** The destination network is unknown.
  - A router has no information about the destination network

Error Reporting (cont'd)

- **Code 7 :** The destination host is unknown.
  - the router is unaware of the existence of the destination
- **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
- **Code 12 :** The host is unreachable for the specified type of service

Error Reporting (cont'd)

- **Code 13 :** The host is unreachable because the administration has put a filter on it

- **Code 14 :** The host is unreachable because the host precedence is violated. 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

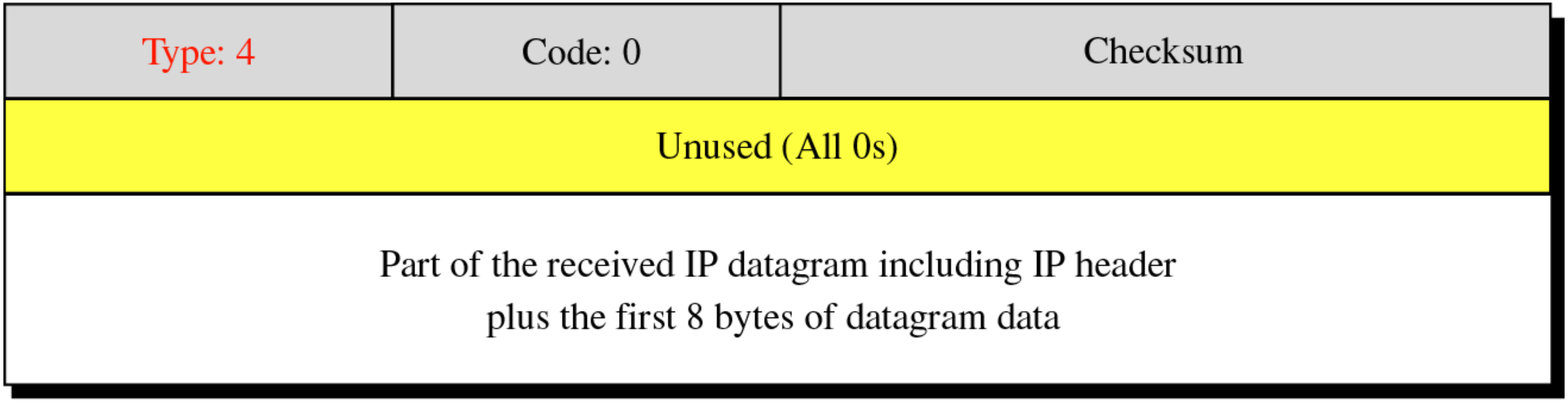
Error Reporting (cont'd)

- Destination-unreachable messages with codes 2 or 3 can be created only by the destination host. Other destination-unreachable message can be created only by routers.

- A router can not detect all problems that prevent the delivery of a packet.
  - The case that a datagram is traveling through an Ethernet network.
  - Ethernet does not provide any acknowledgement mechanism.

Error Reporting (cont'd)

- Source Quench
  - is designed to add a kind of flow control to the IP
    - IP does not have a flow-control mechanism embedded in the protocol
  - when a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram
    - making slow down the sending process



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		

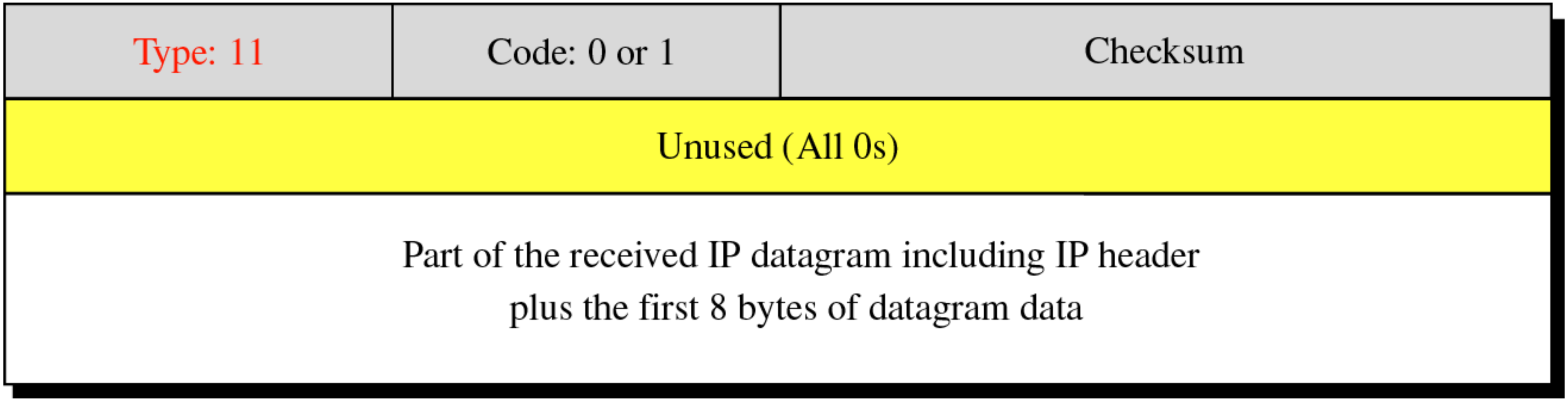
Error Reporting (cont’d)

- Time exceeded
  - Whenever a router receives a datagram whose time-to-live field has the value of zero, it discards the datagram and sends a time-exceeded message to the original source
  - 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

Error Reporting (cont'd)

- 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



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

Error Reporting (cont'd)

Parameter-problem

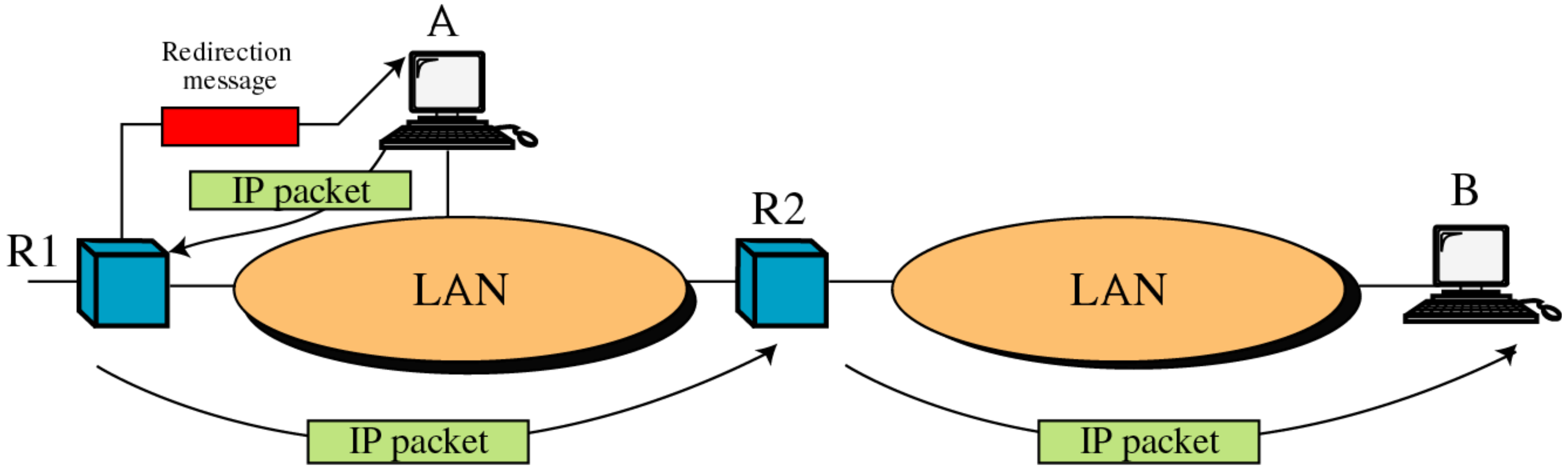
- A parameter-problem message caused by ambiguity in the header part can be created by a router or the destination host
- Code 0 : error or ambiguity in one of the header fields
  - the value in the pointer field points to the byte with the problem
- Code 1 : the required part of an option is missing. In this case, pointer is not used

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		

Error Reporting (cont'd)

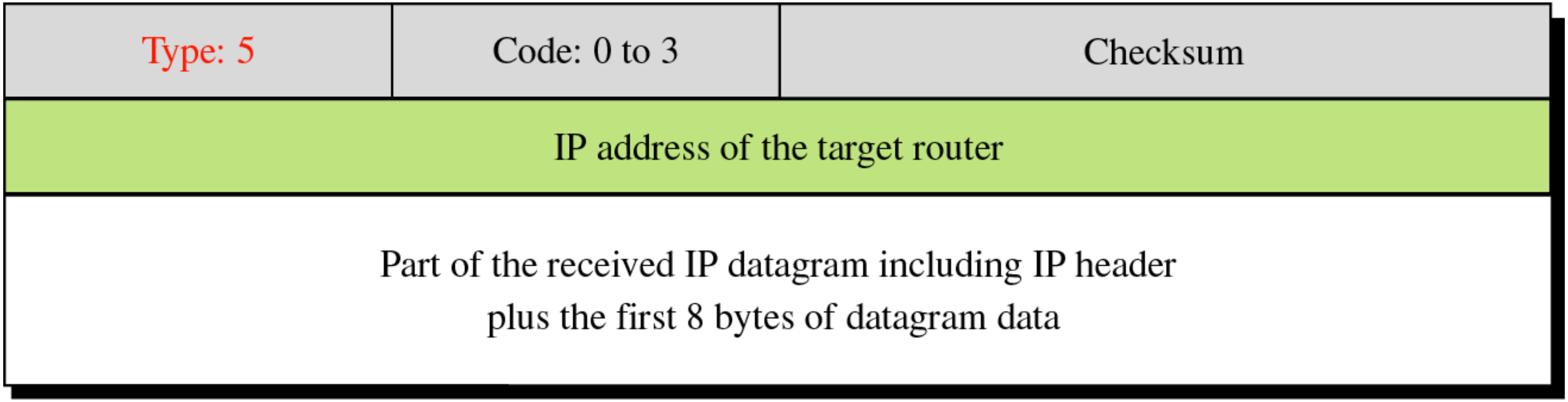
Redirection

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



Error Reporting (cont'd)

- Redirection message format



Type: 5

Code: 0 to 3

Checksum

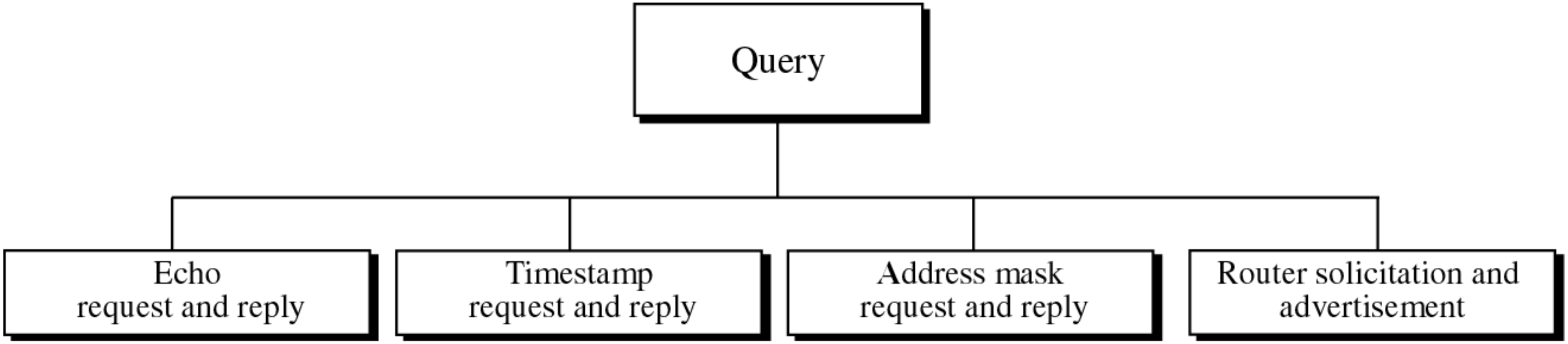
IP address of the target router

Part of the received IP datagram including IP header plus the first 8 bytes of datagram data

- **Code 0 : redirection for the network-specific route**
- **Code 1 : redirection for the host-specific route**
- **Code 2 : redirection for network-specific route based on specific type of service**
- **Code 3 : redirection for the host-specific route based on the specified type of service**

Query

- Diagnosing some network problems
- 4 different pairs of messages


Query
Echo request and reply
Timestamp request and reply
Address mask request and reply
Router solicitation and advertisement

Query (cont'd)

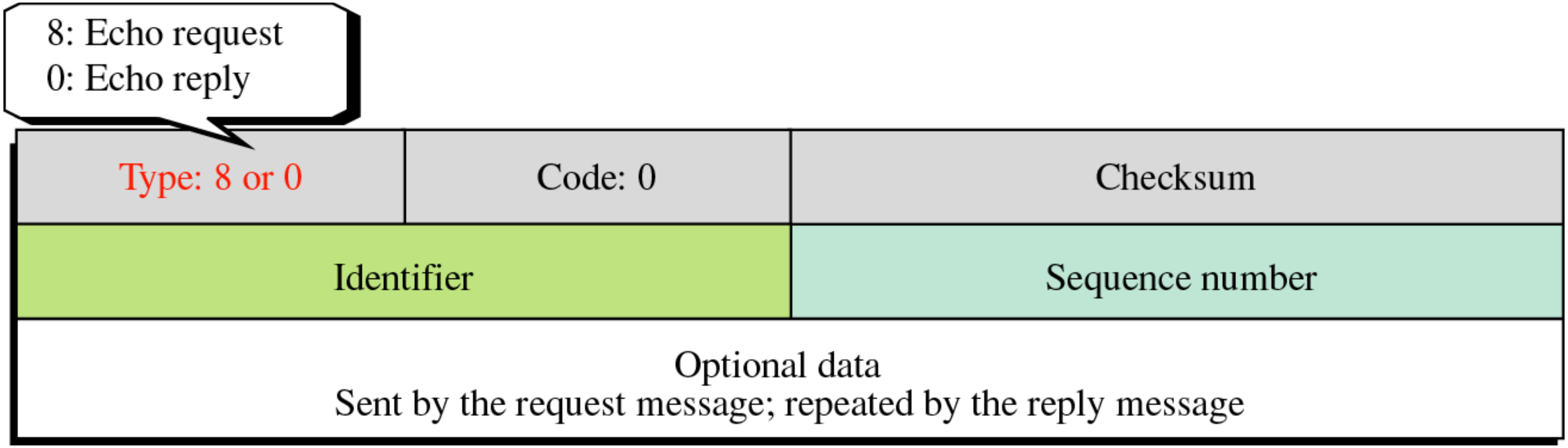
- Echo Request and Reply messages
  - designed for diagnostic purpose
  - the combination of echo-request and echo-reply messages determines whether 2 systems (hosts or routers) can communicate with each other
  - An echo-request message can be sent by a host or router. An echo-reply message is sent by the host or router which receives an echo-request message
  - Echo-request and echo-reply message can be used by network managers to check the operation of the IP protocol

Query (cont'd)

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

- Identifier and sequence number fields are not formally defined by the protocol and can be used by the sender

- Echo-request and echo-reply message



8: Echo request
0: Echo reply

Type: 8 or 0

Code: 0

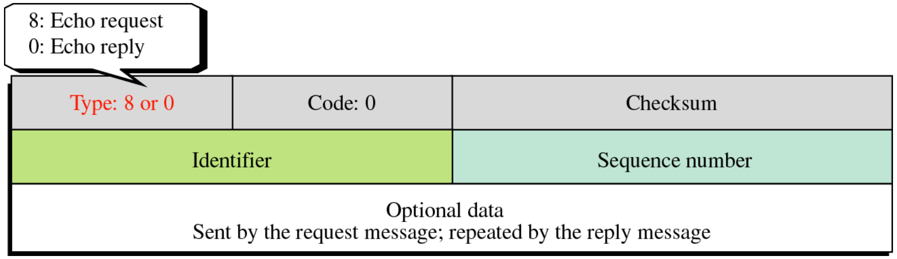
Checksum

Identifier

Sequence number

Optional data
Sent by the request message; repeated by the reply message

Query (cont'd)



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

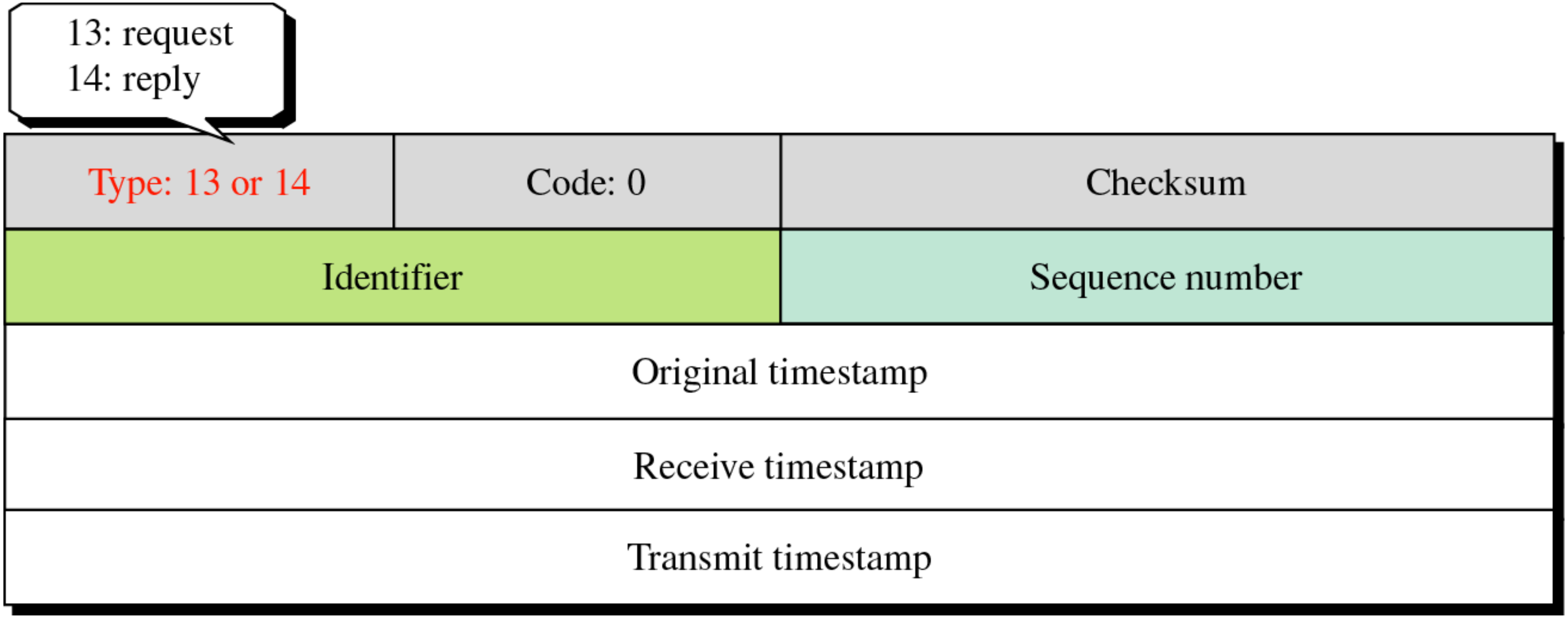
- The identifier field
  - defines a group of problems
  - ex) process ID that originated the request
- The sequence number field
  - keeps track of the particular echo request messages sent
- At the user level
  - Invoking the packet Internet groper (ping) command

Query (cont'd)

- Timestamp Request and Reply
  - 2 machines (routers or hosts) can use the timestamp-request and timestamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them
  - can used to synchronize the clocks in two machines
  - Three timestamp fields are each 32 bits long
    - holding a number representing time measured in milliseconds from midnight in Universal Time
      - Cannot exceed 86,400,000 = 24 x 60 x 60 x 1,000

Query (cont'd)

- Timestamp-request and reply message format



13: request
14: reply

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

- original timestamp field : clock at departure time
- receive timestamp field : at the time the request was received
- transmit timestamp field : at the time the reply message departs

Query (cont'd)

- The formulas for computing the one-way or round-trip time required for a datagram to go from a source to a destination and then back again.
  - Sending time = value of receive timestamp – value of original time stamp
  - Receiving time = time the packet returned – value of transmit timestamp
  - Round-trip time = sending time + receiving time

Query (cont’d)

- Timestamp-request and timestamp reply message can be used to measure the round-trip time between a source and a destination machine even if their clocks are not synchronized
  - Example
    - Value of original timestamp : 46
    - Value of receive timestamp : 59
    - Value of transmit timestamp : 60
    - Time the packet arrived : 67

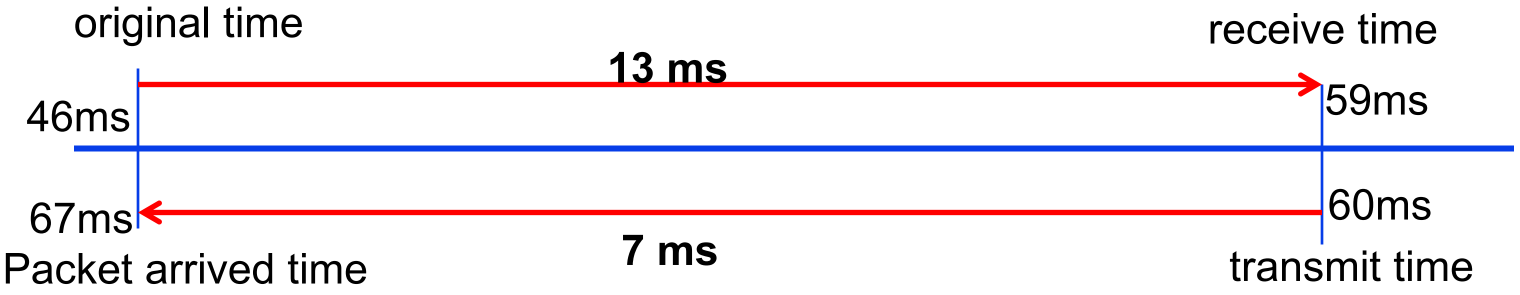
    Sending time = 13 ms

    Receiving time = 7 ms

    Round-trip time = 20 ms

Query (cont'd)

- Synchronizing clocks between two machines
  - Time difference = receive timestamp – (original timestamp field + oneway time duration)
  - In previous example,
    - Time difference = 59 – (46 + 10) = 3



Query (cont'd)

- ❑ **Address Mask Request and Reply**

  - **for differentiating among network address, subnetwork address and host ID**
  - **example, a host may know its 32-bit IP address as**

    10011111.00011111.11100010.10101011

  - **left 20 bits are network and subnetwork addresses and remaining 12 bits are Host ID. In this case, following mask**

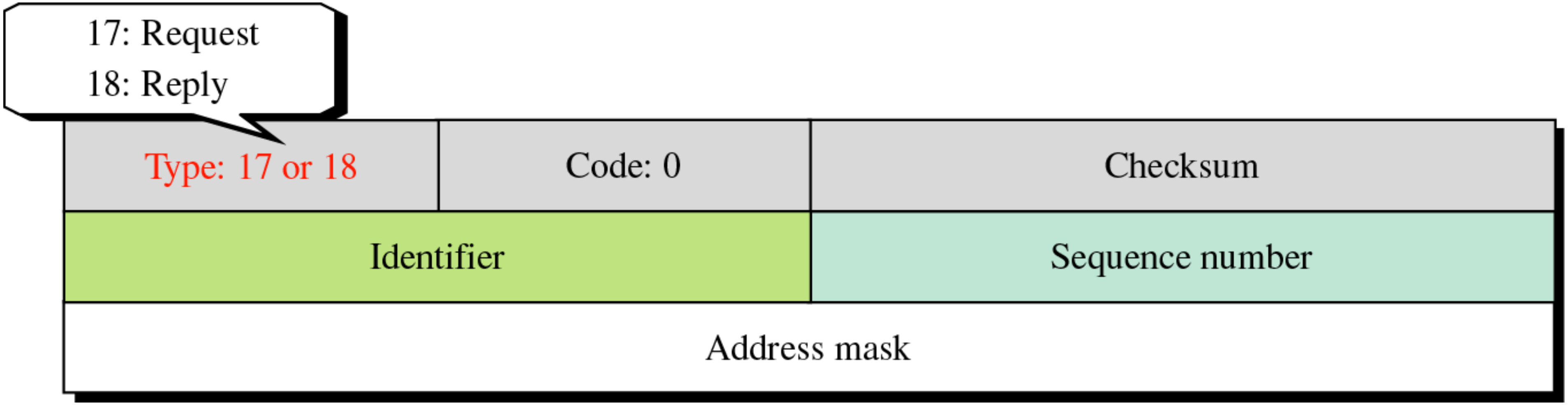
    11111111.11111111.11110000.00000000

NetId and subnetid → 10011111.00011111.1110

Host ID → 0010.10101011

Query (cont'd)

- To obtain its mask,
  - A host sends an address-mask-request message to a router on the LAN. (unicast or broadcast)
  - If the host knows the address of the router, it sends the request directly to the router, if not, it broadcasts the message.



17: Request
18: Reply

Type: 17 or 18	Code: 0	Checksum

Identifier	Sequence number

Address mask

Query (cont'd)

- Masking is needed for diskless stations at start-up time.

- When a diskless station comes up for the first time
  - it may ask for its full IP address using RARP protocol
  - after receiving its IP address, it may use the address mask request and reply to find out which part of the address defines the subnet

Query (cont'd)

Router Solicitation and Advertisement

- A host that wants to send data to a host on another network needs to know the address of routers connected to its own network.
  - the host should know if the routers are alive and functioning
  - A host can broadcast (or multicast) a router-solicitation message.
  - The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message.
    - A router can also periodically advertise router-advertisement messages even if no host has solicited

Query (cont’d)

- Router-solicitation message format

Type: 10	Code: 0	Checksum
Identifier		Sequence number

Query (cont'd)

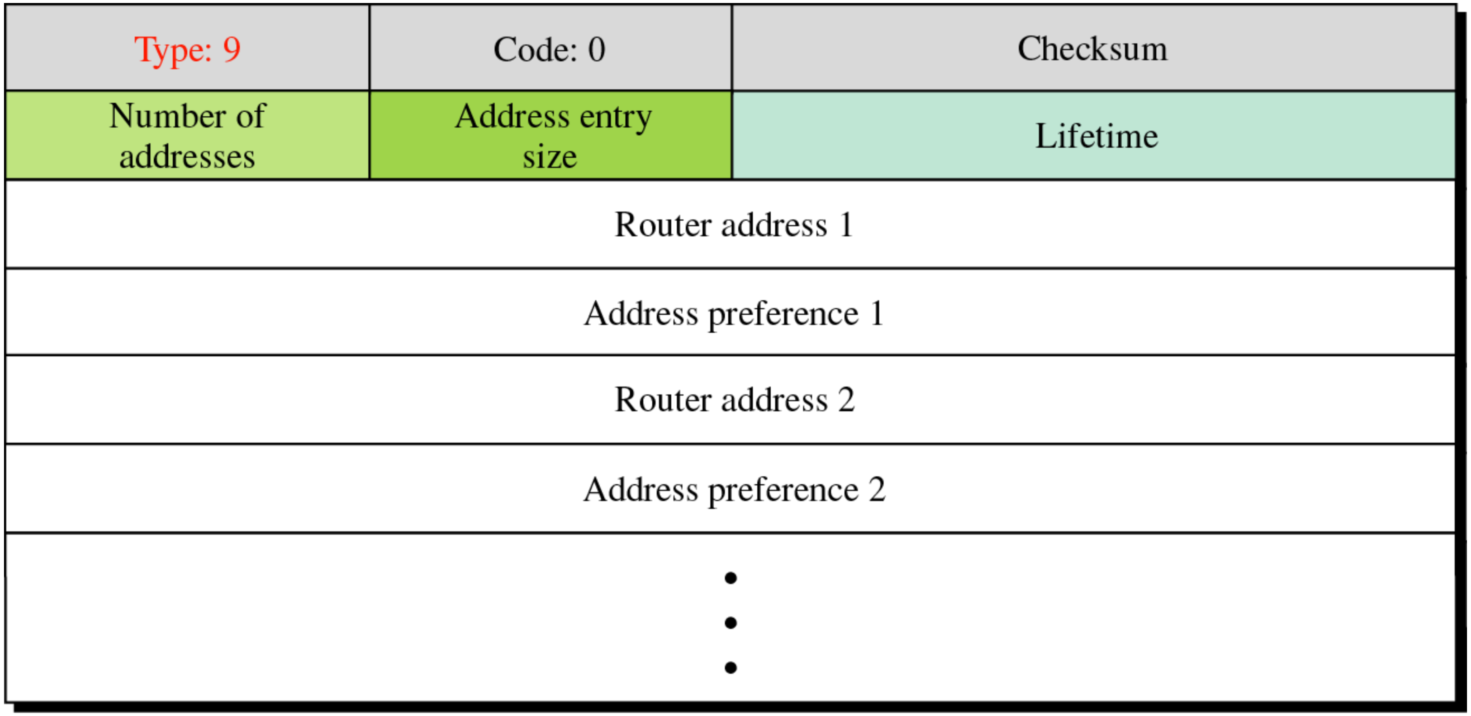
- Router-advertisement message format

  - lifetime field : showing the number of seconds that entries are considered to be valid

  - address preference level defines the ranking of the router

    - preference level 0 : default router

    - preference level 80000000_{16} : the router should never be selected as the default router



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

Checksum

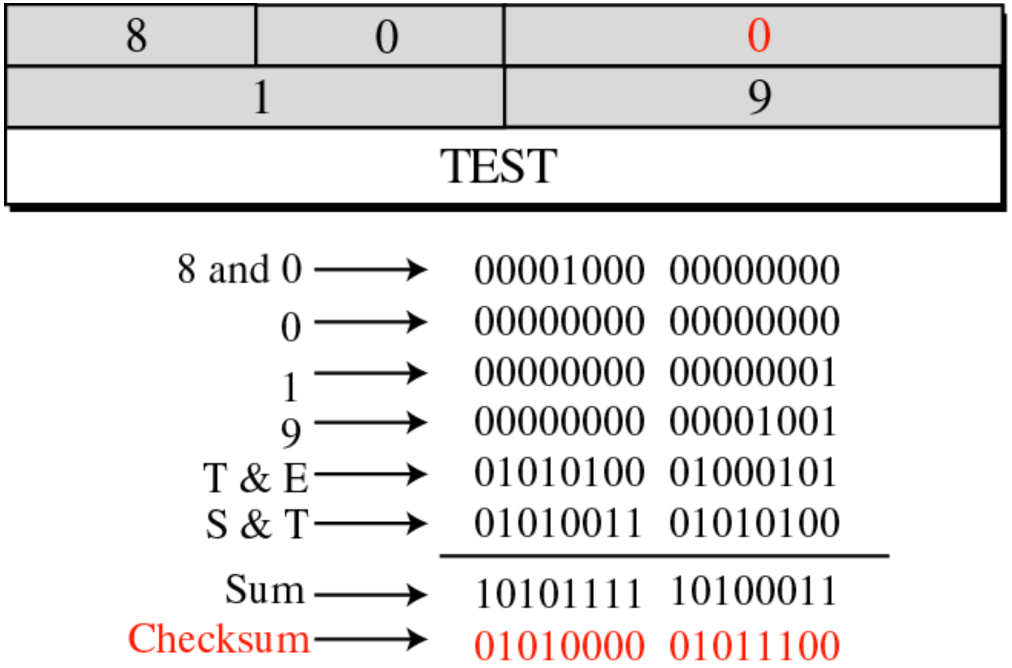
- Checksum
  - calculating over the entire message (header and data)
- Checksum calculation
  1. Checksum field is set to zero
  2. Sum of all the 16-bit words (header and data) is calculated
  3. Sum is complemented to get the checksum
  4. Checksum is stored in the checksum field

Checksum (cont'd)

Checksum testing

1. the sum of all words (header and data) is calculated
2. the sum is completed
3. if the result obtained in step 2 is 16 0s, the message is accepted; otherwise, it is rejected.

- Example,



8	0	0
1		9
TEST		

```
8 and 0 ──→  00001000  00000000
      0 ──→  00000000  00000000
      1 ──→  00000000  00000001
      9 ──→  00000000  00001001
  T & E ──→  01010100  01000101
  S & T ──→  01010011  01010100
             ──────────────────
    Sum ──→  10101111  10100011
Checksum──→  01010000  01011100
```

Summary(1)

- The Internet Control Message Protocol (ICMP) sends five types of error reporting messages and four pairs of query messages to support the unreliable and connectionless Internet Protocol (IP).
- ICMP messages are encapsulated in IP datagrams.
- The destination-unreachable error message is sent to the source host when a datagram is undeliverable.
- The source-quench error message is sent in an effort to alleviate congestion.
- The time-exceeded message notifies a source host that (1) the time-to-live field has reached zero, or (2) fragments of a message have not arrived in a set amount of time.
- The parameter-problem message notifies a host that there is a problem in the header field of a datagram.
- The redirection message is sent to make the routing table of a host more efficient.

Summary(2)

- The echo-request and echo-reply messages test the connectivity between two systems.
- The timestamp-request and timestamp-reply messages can determine the round-trip time between two systems or the difference in time between two systems.
- The address-mask-request and address-mask-reply messages are used to obtain the subnet mask.
- The router-solicitation and router-advertisement messages allow hosts to update their routing tables.
- The checksum for ICMP is calculated using both the header and the data fields of the ICMP message.
- Packet InterNet Groper (ping) is an application program that uses the services of ICMP to test the reachability of a host.
- A simple ICMP design can consist of an input module that handles incoming ICMP packets and an output module that handles demands for ICMP services.