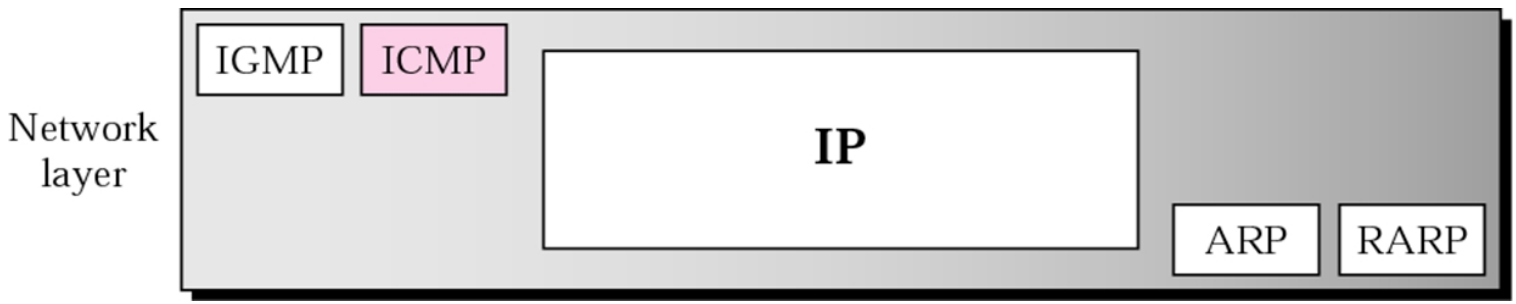
Computer Networks - ICMP

Mridul Sankar Barik

Jadavpur University

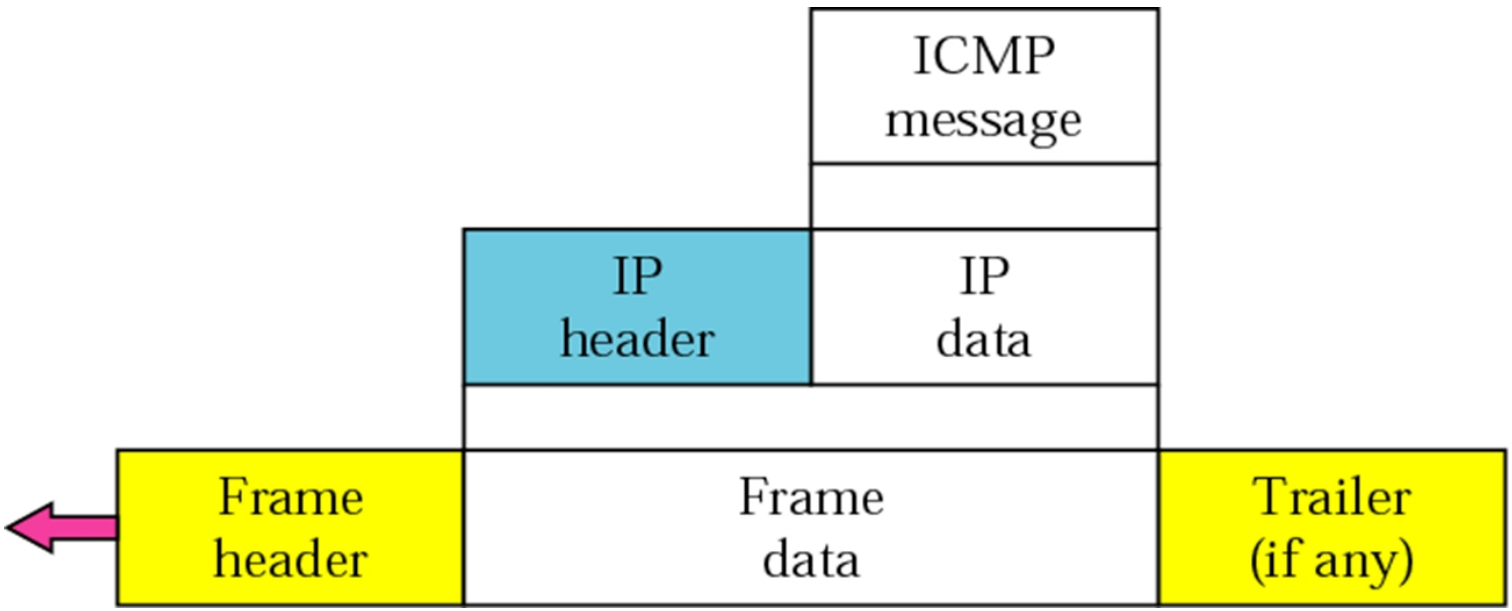
2023

Position of ICMP



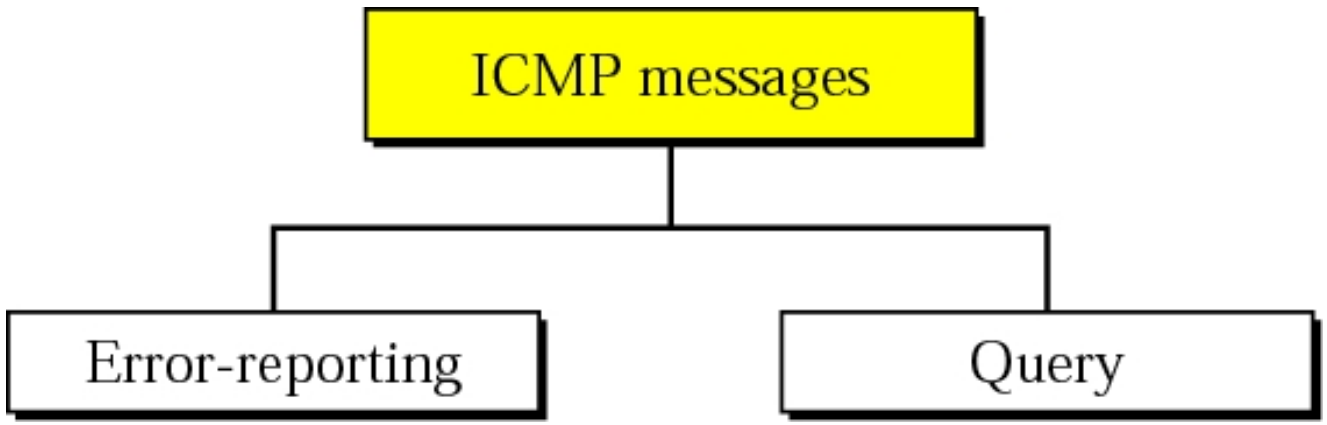
- RFC 792

ICMP Encapsulation

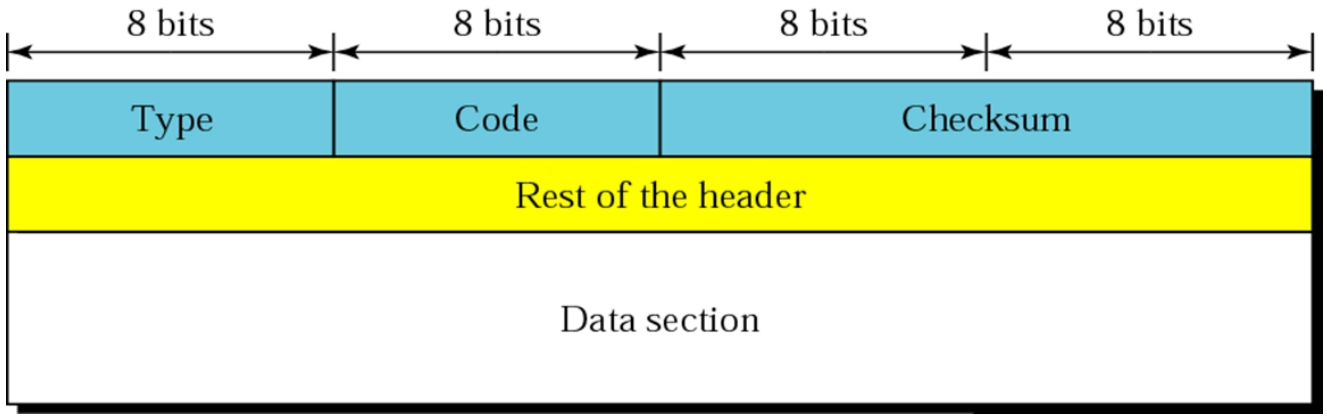


Types of Messages

- ICMP messages are divided into error-reporting messages and query messages
- The error-reporting messages report problems that a router or a host (destination) may encounter
- The query messages get specific information from a router or another host



ICMP Message Format



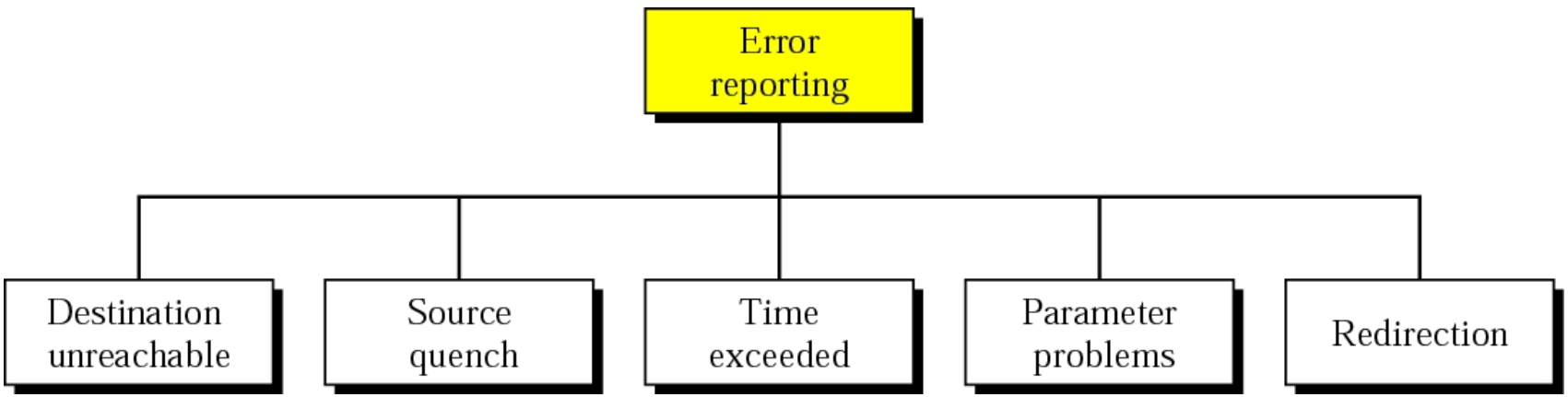
- An ICMP message has an 8-byte header and a variable-size data section
- Although the general format of the header is different for each message type, the first 4 bytes are common to all
- Type: Identifies the ICMP message type
- Code: Identifies the "subtype" of message within each ICMP message Type value
- Checksum: 16-bit checksum field, it provides error detection coverage for the entire ICMP message
  - It is calculated by dividing the ICMP message into words (16 bits) and then adding them together

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
	17 or 18	Address mask request or reply
	10 or 9	Router solicitation or advertisement

ICMP Error Reporting

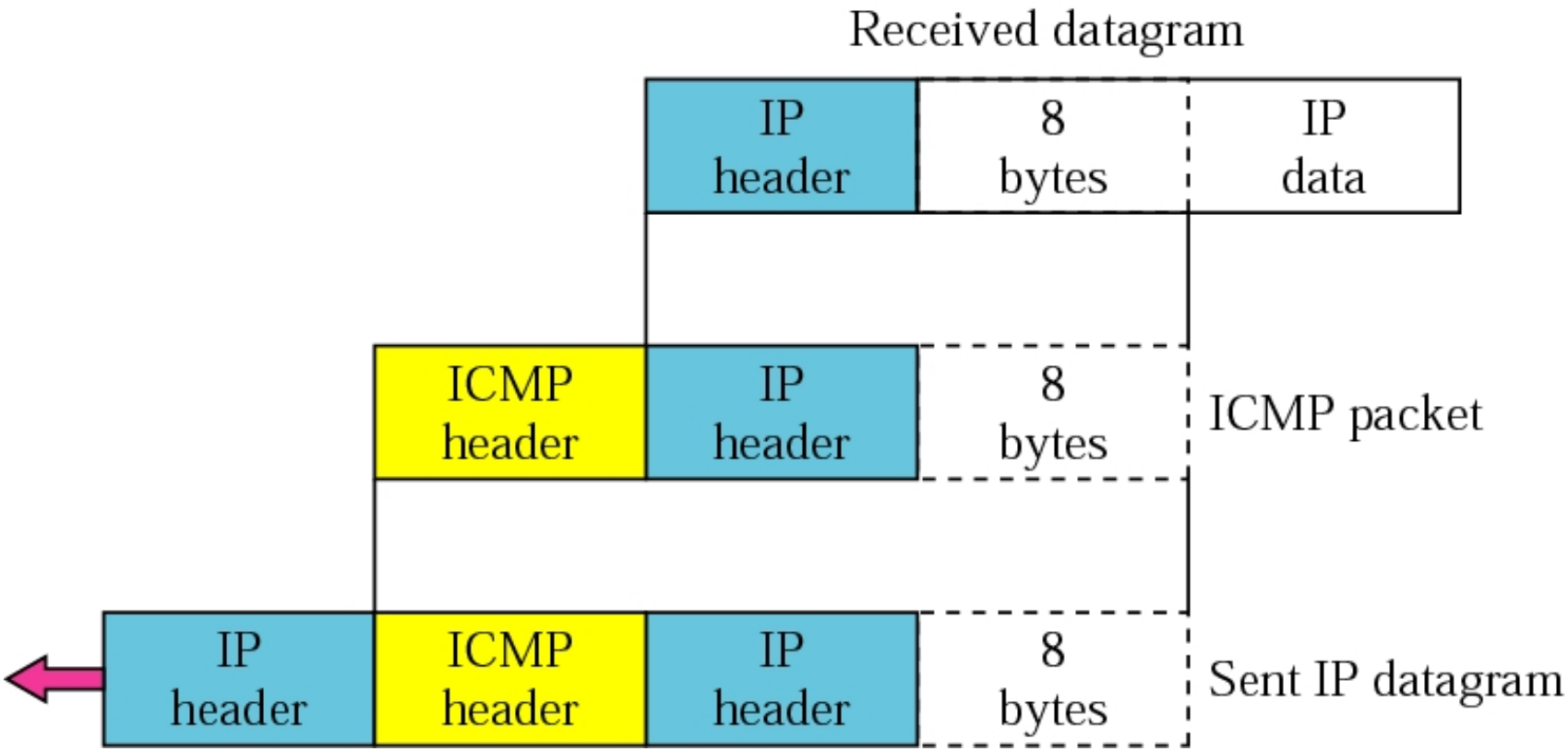
- IP is an unreliable protocol
  - No error checking and error control
- ICMP compensates this shortcoming
- ICMP does not correct errors, it simply reports them
- ICMP always reports error messages to the original source



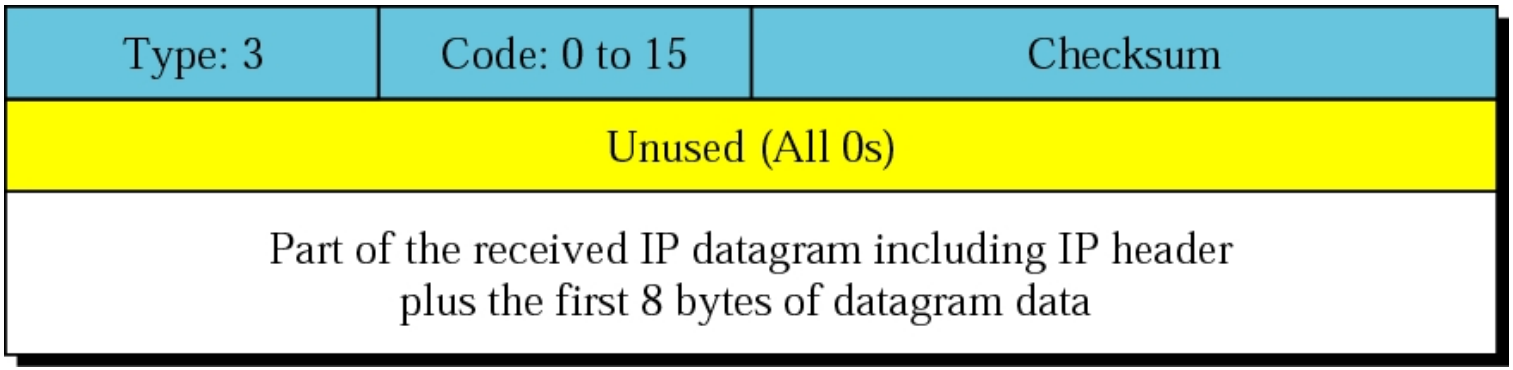
ICMP Error Messages

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

ICMP Error Messages

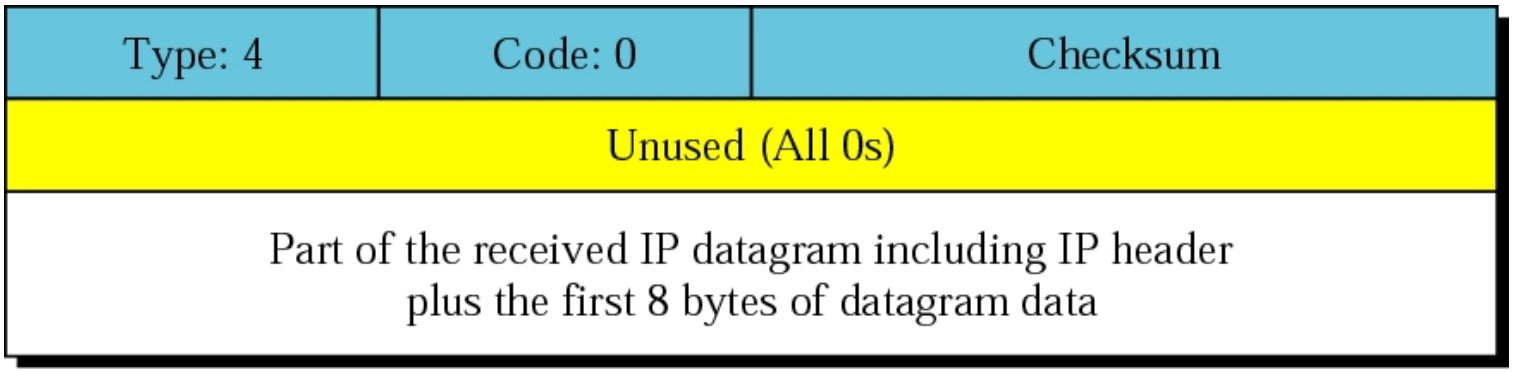


ICMP Error Messages: Destination Unreachable Format



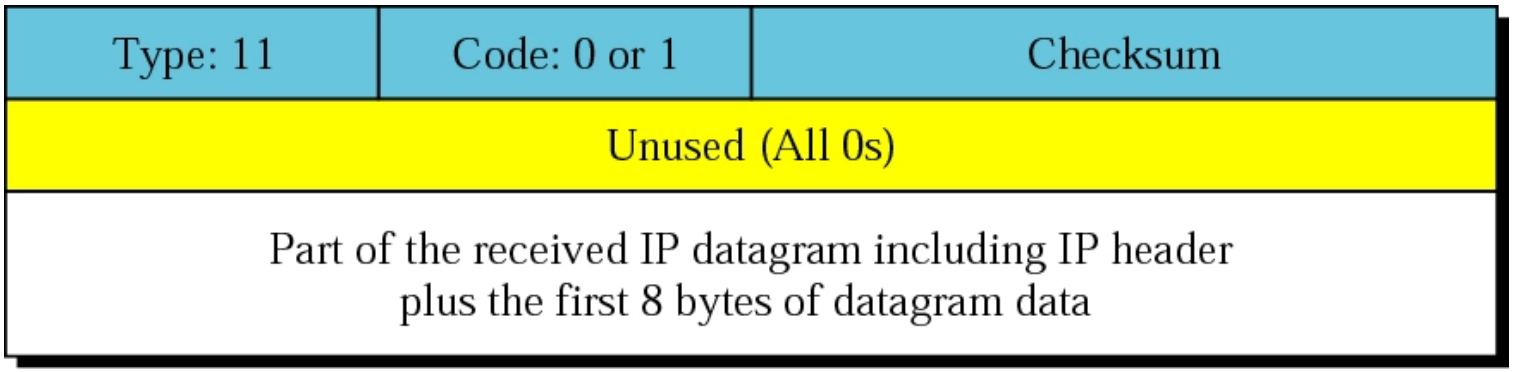
- Generated by a router/gateway
  - To inform the source host that the destination unicast address is unreachable
  - When a datagram must be fragmented to be forwarded yet the Don't Fragment flag is on
- Generated by a destination host
  - If the IP module cannot deliver the datagram because the indicated protocol module or process port is not active

ICMP Error Messages: Source Quench



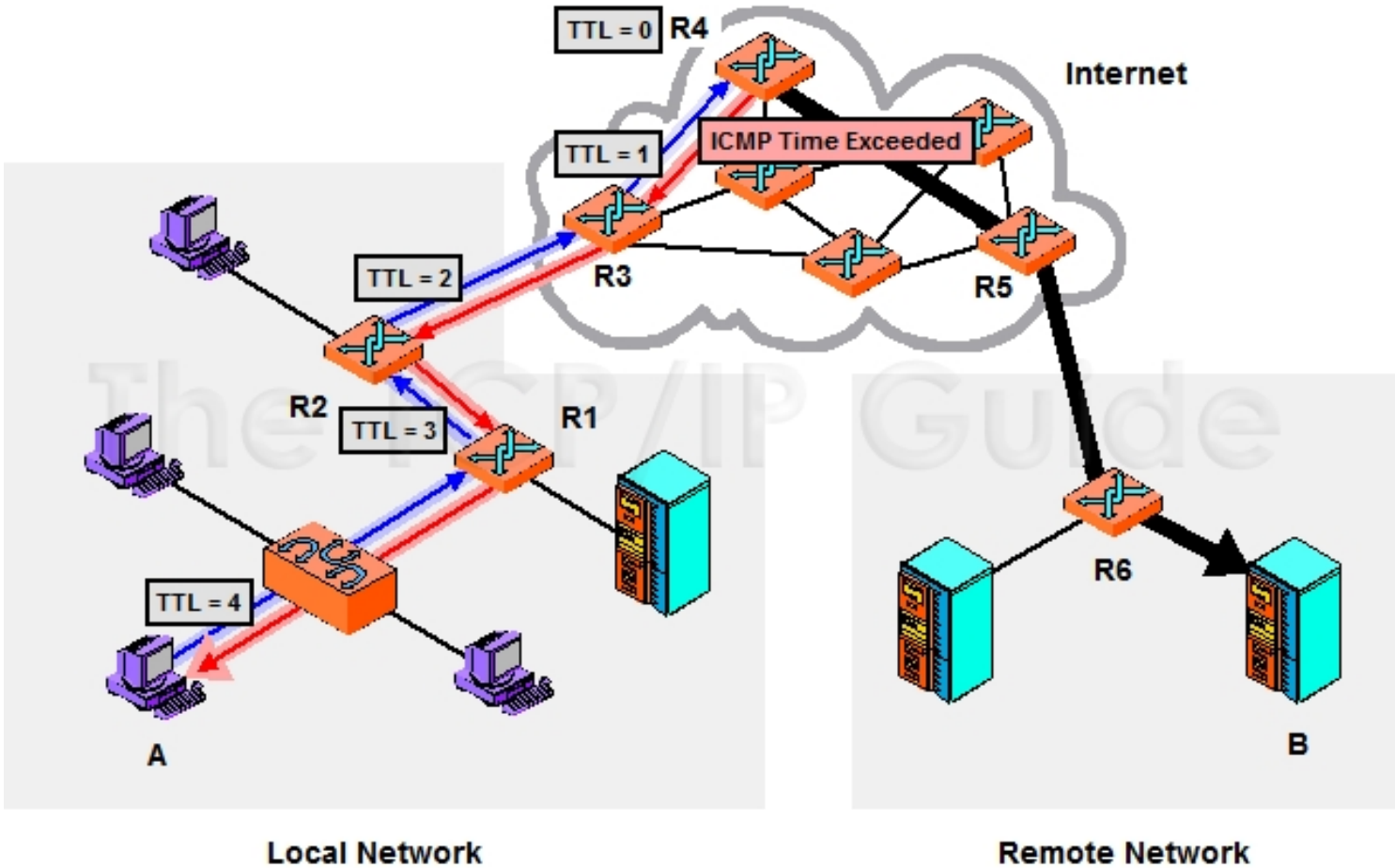
- A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host
- The source must slow down the sending of datagrams until the congestion is relieved
- One source-quench message is sent for each datagram that is discarded due to congestion

ICMP Error Messages: Time Exceeded Message

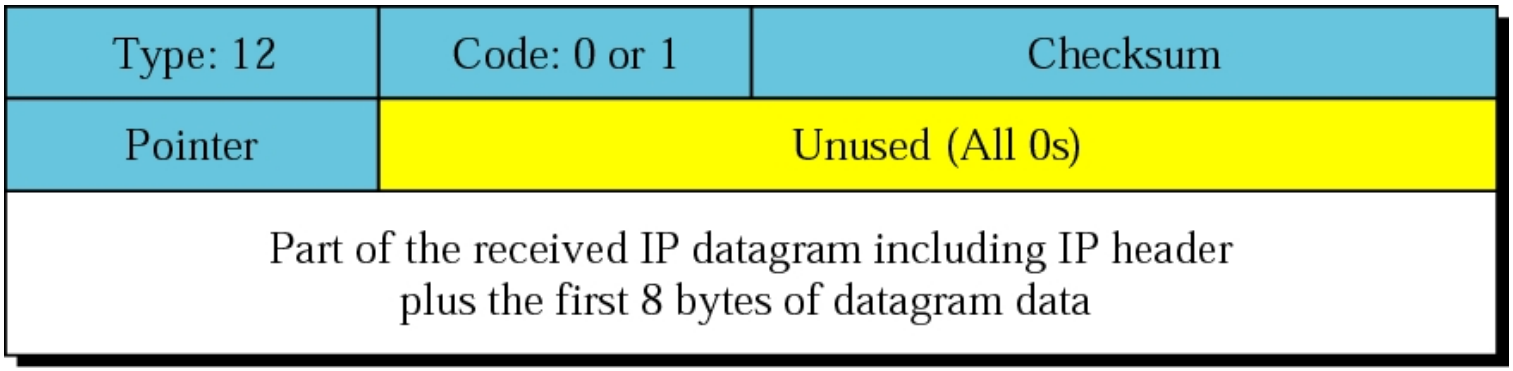


- Sent by a router, when the TTL value reaches zero, it discards the datagram and sends a time-exceeded message to the original source: Code 0
- Sent by a final destination if it does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source: Code 1

ICMP Error Messages: Time Exceeded Message

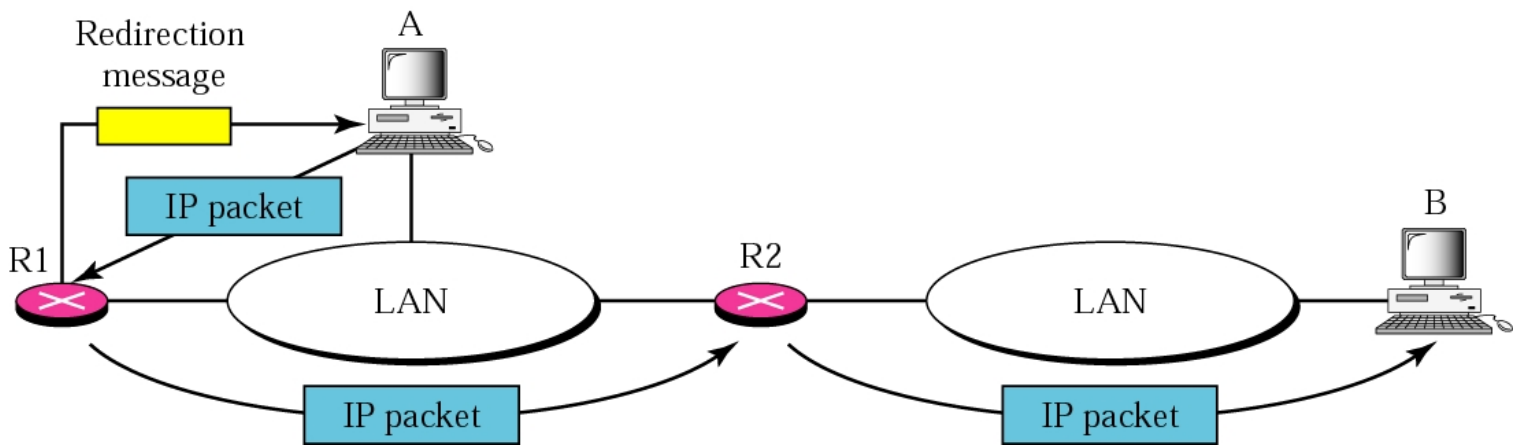


ICMP Error Messages: Parameter Problem Message



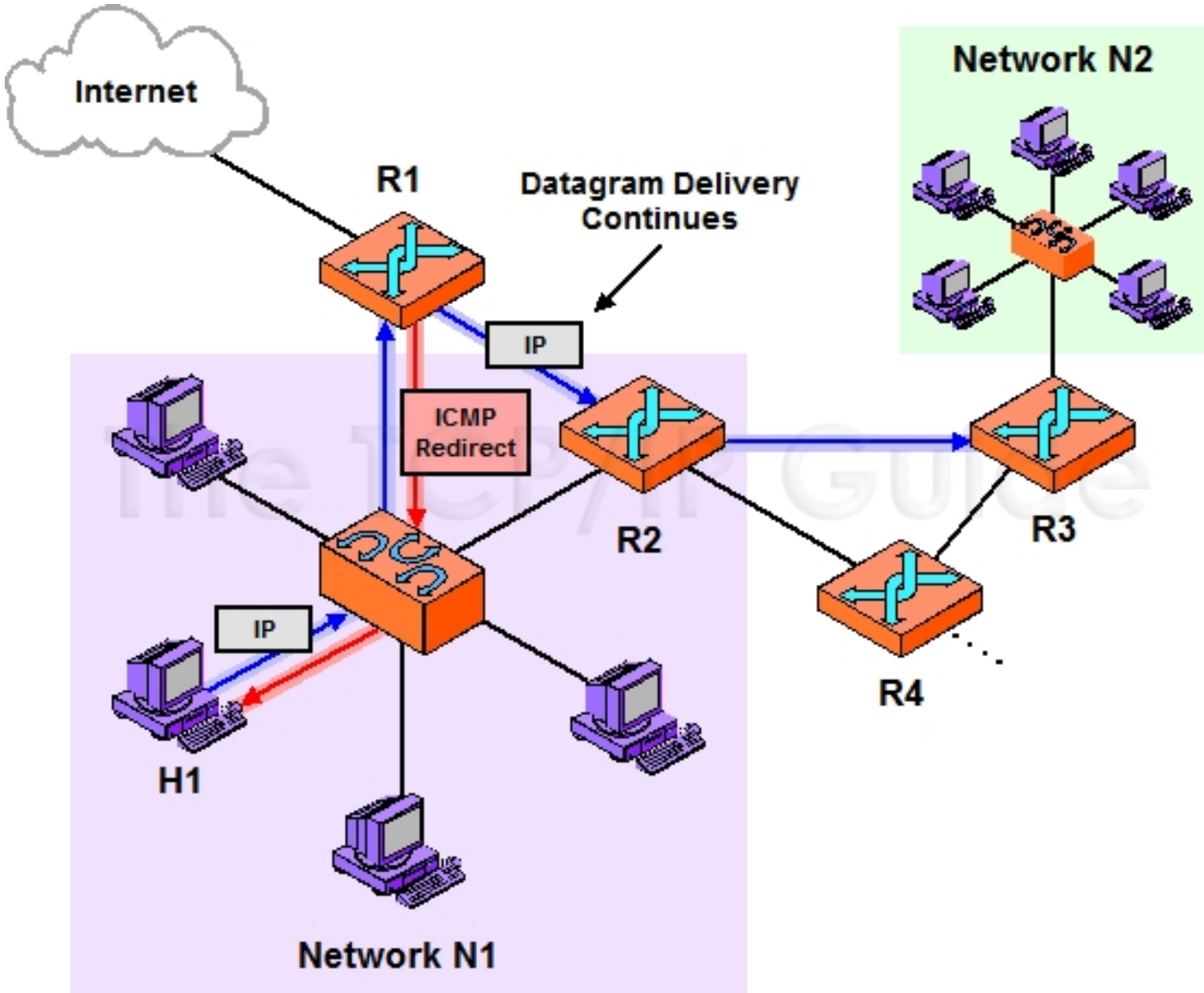
- A parameter-problem message can be created by a router or the destination host
- Sent by a device when it finds problem with any of the parameters in an IP datagram header so that it cannot complete processing the header and it must discard the datagram

ICMP Error Messages: Redirection Messages

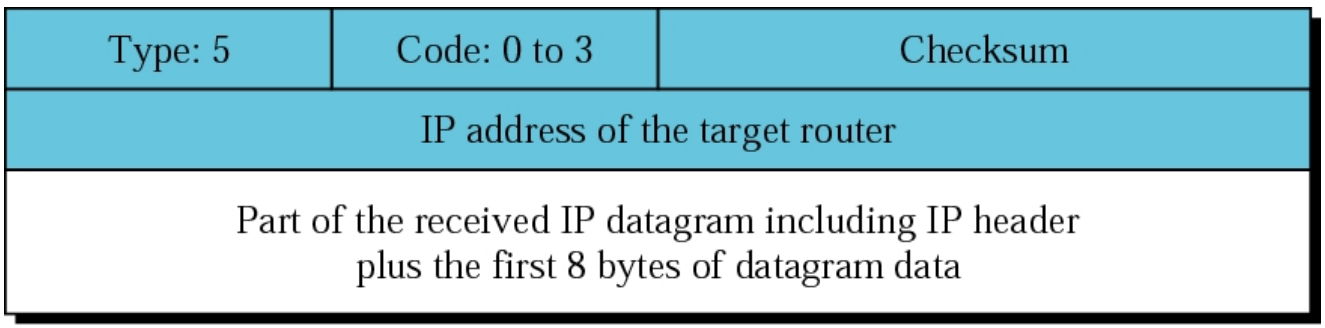


- A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message

ICMP Error Messages: Redirection Messages



ICMP Error Messages: Redirection Messages



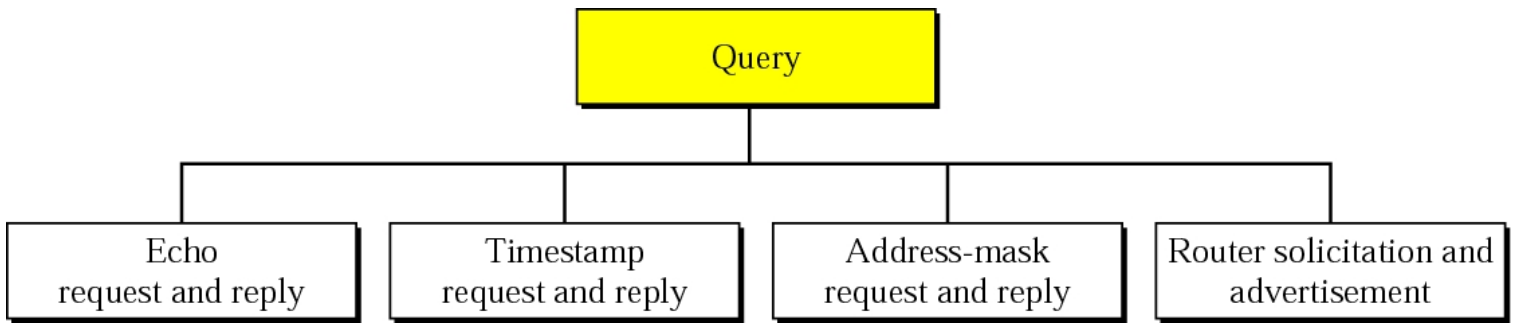
- A redirection message is sent from a router to a host on the same local network

ICMP Error Messages: Redirection Messages

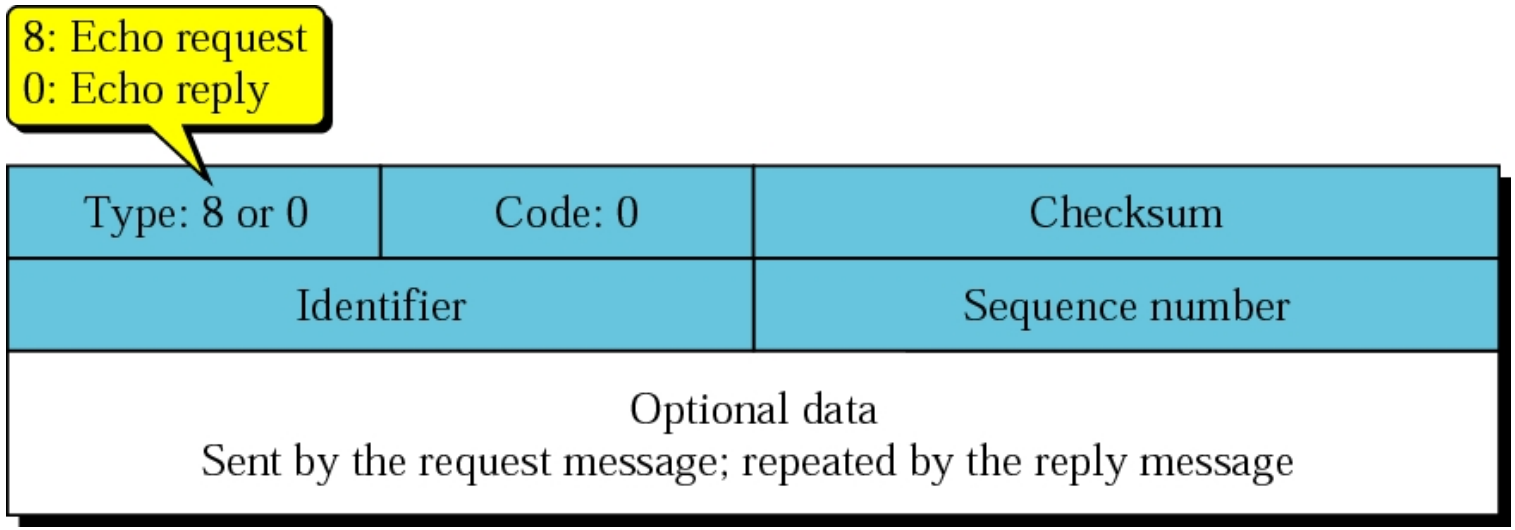
- A convenient way for hosts to be given information about routes by local routers
- Not used to communicate route information between routers

ICMP Query Messages

- ICMP can also diagnose some network problems through the query messages, a group of four different pairs of messages. In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node

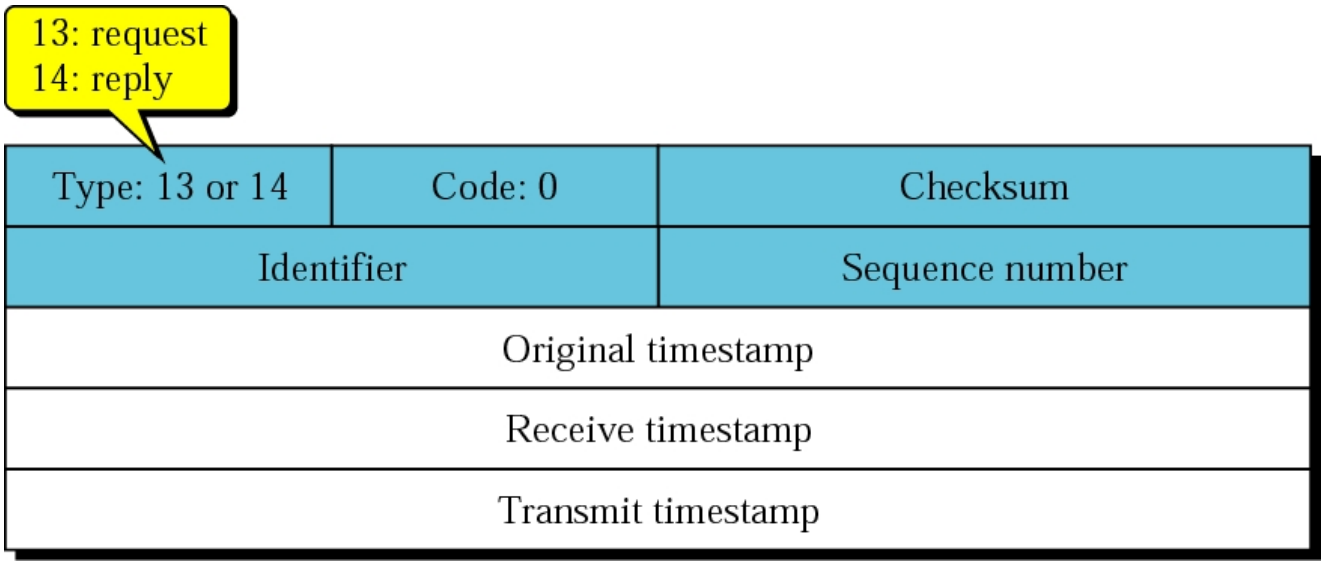


ICMP Query Messages: Echo Request and Echo Reply Messages



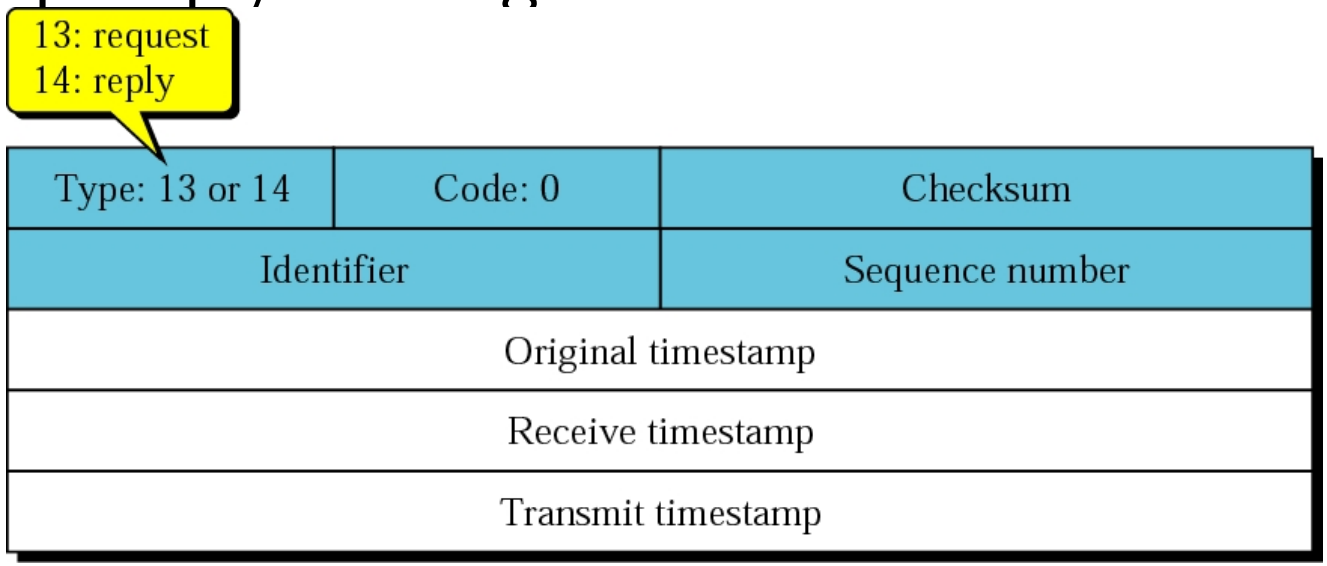
- An echo-request message can be sent by a host or router
- An echo-reply message is sent by the host or router which receives an echo-request message
- Can be used by network managers to check the operation of the IP protocol
- Can be used to test the reachability of a host (ping command)

ICMP Query Messages: Timestamp Request and Timestamp Reply Messages I



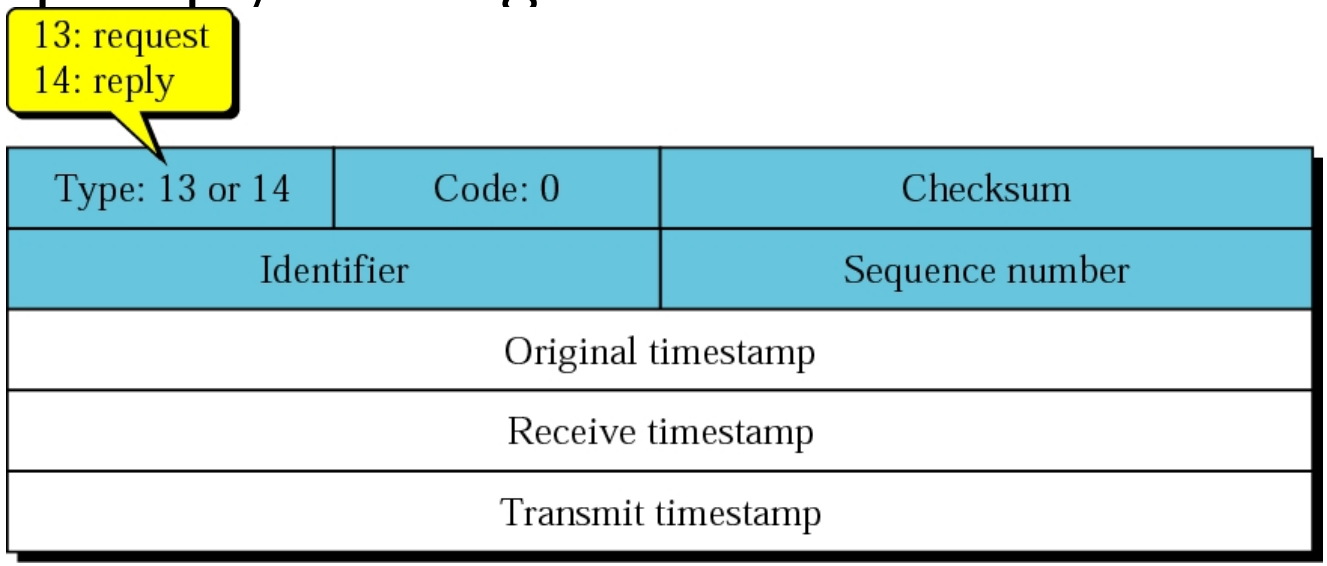
- Allows a system to request another for the current time
- Returned value is number of milliseconds since midnight
- Requester fills the original timestamp
- Replying system fills the receive timestamp when it receives the request
- Replying system fills the transmit timestamp when it sends the reply

ICMP Query Messages: Timestamp Request and Timestamp Reply Messages II



- Can be used to calculate the round-trip time between a source and a destination machine even if their clocks are not synchronized
- Can be used to synchronize two clocks in two machines if the exact one-way time duration is known

ICMP Query Messages: Timestamp Request and Timestamp Reply Messages III

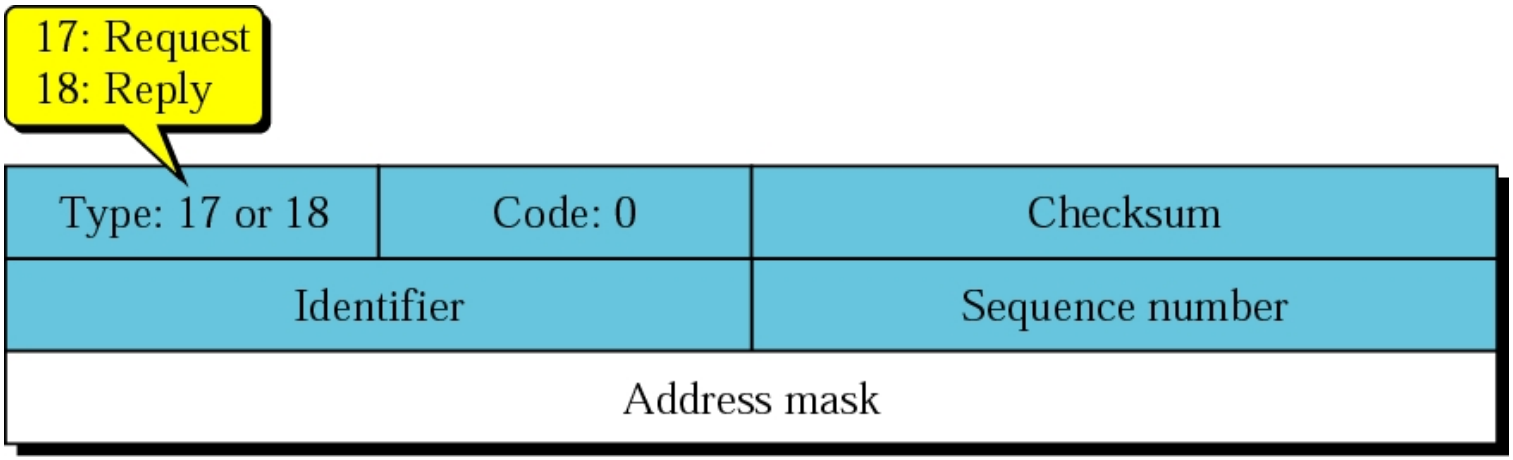


- Requester can calculate
  - Round Trip Time (RTT) = time the reply is received – time the request is send
  - difference = receive timestamp – original timestamp

ICMP Query Messages: Timestamp Request and Timestamp Reply Messages IV

- At any time instant local time at H1 is 1000 and at H2 is 1100
- H1 wants to synchronize its clock with H2
- H1 sends an ICMP Timestamp Request message at its local time 1000 and receives the corresponding reply at local time 1100
- H2 receives the reply at its local time 1150 and sends the reply immediately at local time 1150
  - Original timestamp = 1000
  - Receive timestamp = 1150
  - Transmit timestamp = 1150
- H1 calculates
  - RTT = time the reply is received – time the request is send = 1100 – 1000 = 100
  - difference = receive timestamp – original timestamp = 1150 – 1000 = 150
  - H1 adjusts its clock by (difference – one half of RTT) = 150 – 100/2 = 100

ICMP Query Messages: Mask Request and Mask Reply Message

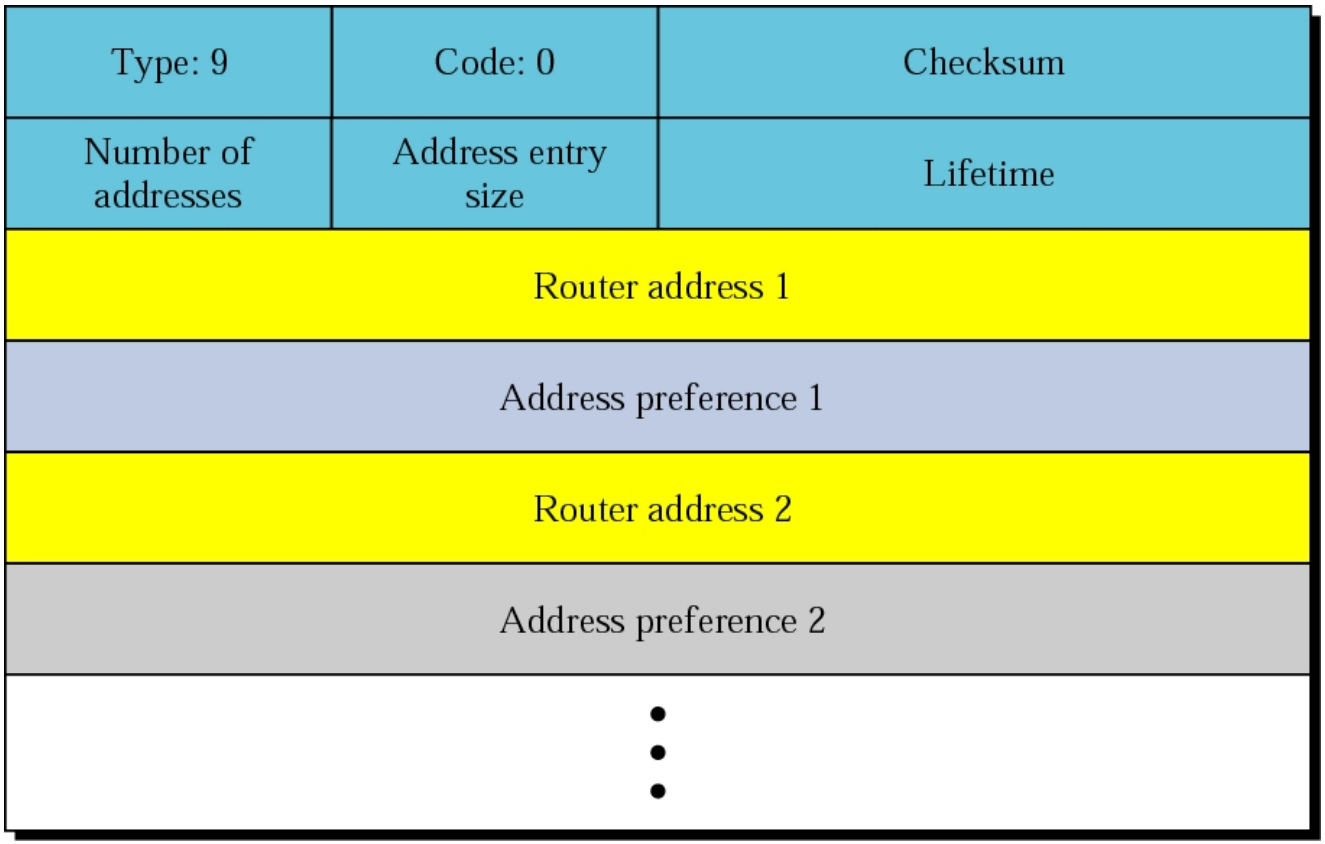


- Used by a diskless system to obtain its subnet mask at bootstrap time
- Mask request is a broadcast message
- The identifier and sequence number field can be anything chosen by the sender; these values and the address mask are returned in the reply

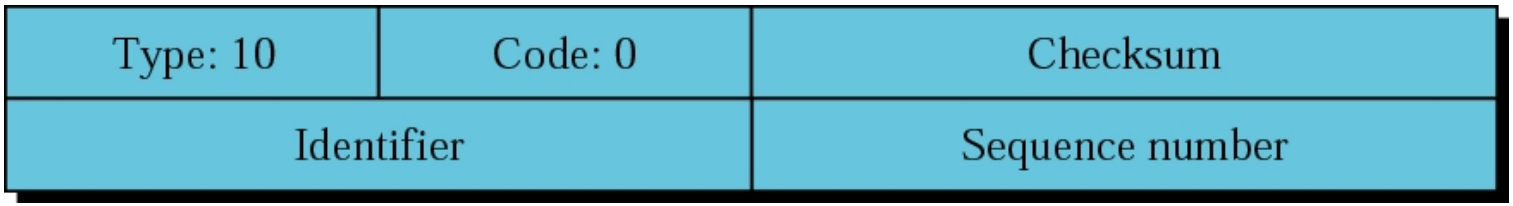
ICMP Query Messages: Router Advertisement Message

- Routers are responsible for sending Router Advertisement messages
- These messages tell listening devices that the router exists, and provide important information about the router
  - Its address (or addresses, if it has more than one)
  - How long the host should retain information about the router
- Routine Router Advertisement messages are sent on a regular basis
  - Usually between 7 and 10 minutes

ICMP Query Messages: Router Advertisement Message



ICMP Query Messages: Router Solicitation Message



- Hosts without manually-configured routing information
  - Have no knowledge of routers when it first powers on
  - It has to sit for many minutes looking for a routine Router Advertisement message is inefficient
- Instead of waiting, the host may send a Router Solicitation message on its local network(s)
  - Prompts any router that hears it to immediately send out an extra Router Advertisement message directly to that host

ICMP Checksum

- In ICMP the checksum is calculated over the entire message (header and data)