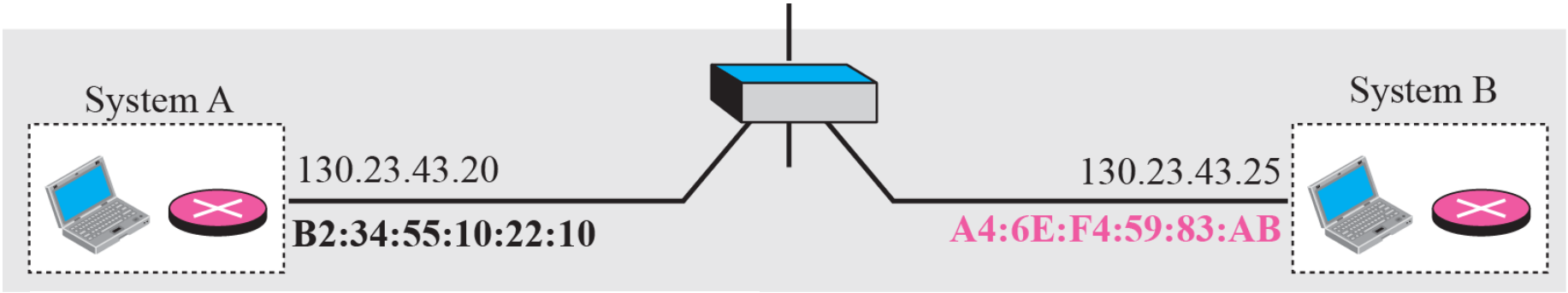
Example

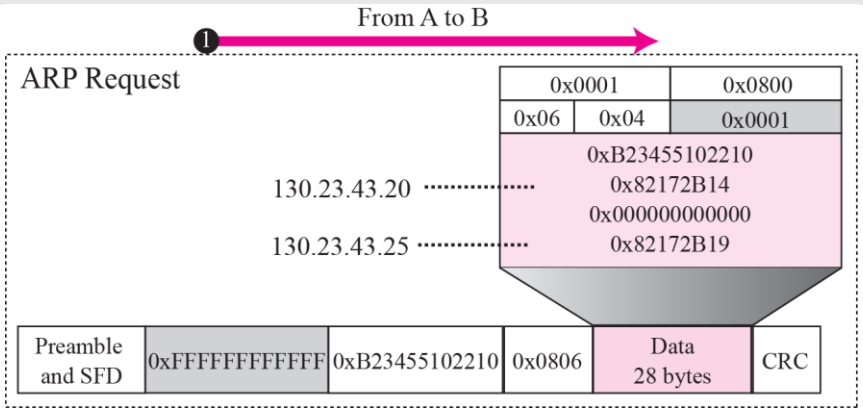
A host with IP address 130.23.43.20 and physical address B2:34:55:10:22:10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

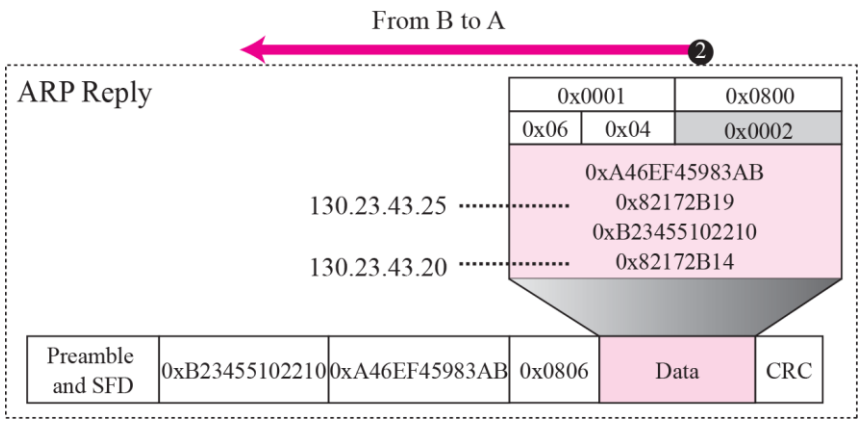
Solution

Figure shows the ARP request and reply packets. Note that the ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why we do not show the regular 4-byte boundaries for these addresses. Also note that the IP addresses are shown in hexadecimal.

Example

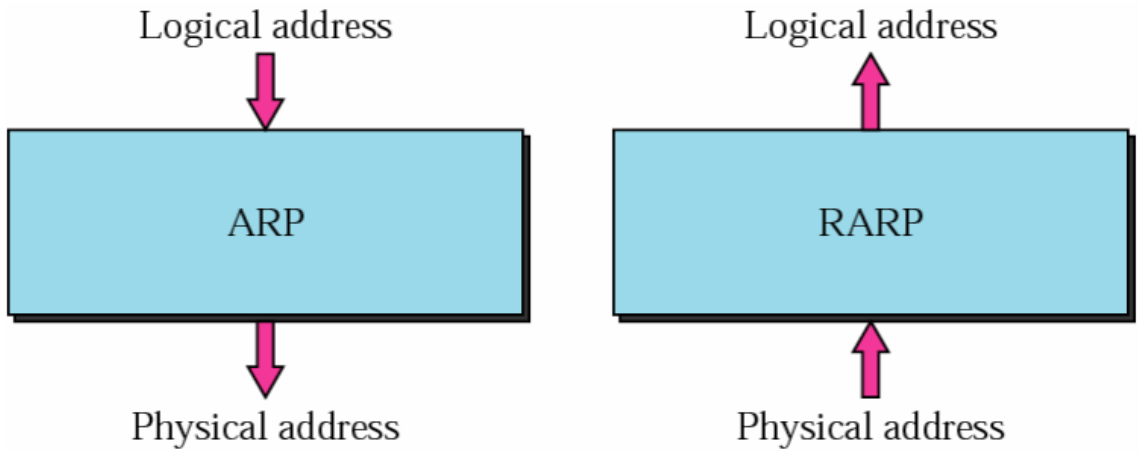

System A
System B
130.23.43.20
130.23.43.25
B2:34:55:10:22:10
A4:6E:F4:59:83:AB


From A to B
1
ARP Request
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
130.23.43.20
130.23.43.25
Preamble and SFD
0xFFFFFFFFFFFF
0xB23455102210
0x0806
Data 28 bytes
CRC

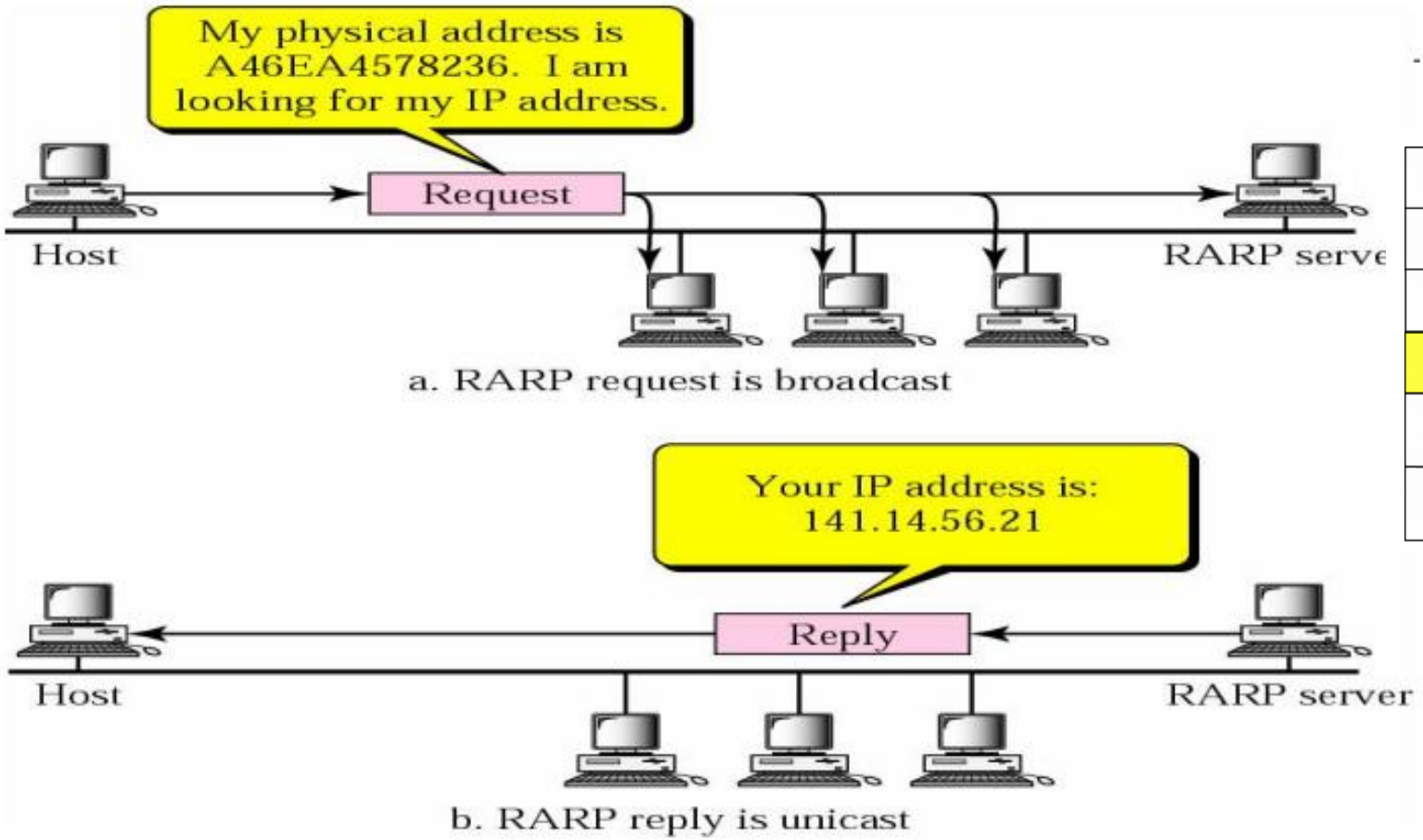

From B to A
2
ARP Reply
0x0001
0x0800
0x06
0x04
0x0002
0xA46EF45983AB
0x82172B19
0xB23455102210
0x82172B14
130.23.43.25
130.23.43.20
Preamble and SFD
0xB23455102210
0xA46EF45983AB
0x0806
Data
CRC

RARP

- Physical address to logical address.
- A diskless machine is usually booted from ROM. RARP is used for diskless machine which can not store the IP address.
- Request Broadcast, reply unicast by RARP server.



RARP Operation



Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

The format of the RARP packet is the same as the ARP packet, Except that the operation field is three for RARP request message and Four for RARP reply message

Alternative Solution to RARP

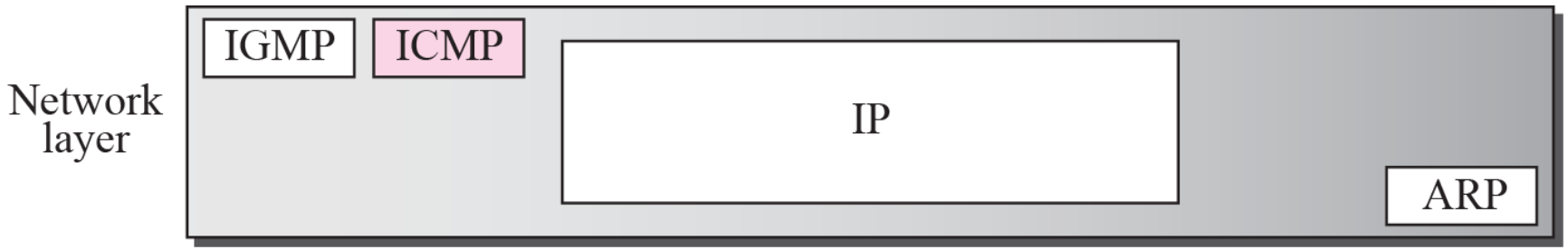
- When a diskless computer is booted, it needs more information in addition to its IP address
  - like subnet mask,
  - default gateway/router,
  - DNS server,
- RARP cannot provide this extra information
- Hence we need something more than RARP i.e., DHCP.

Internet Control Message Protocol (ICMP)

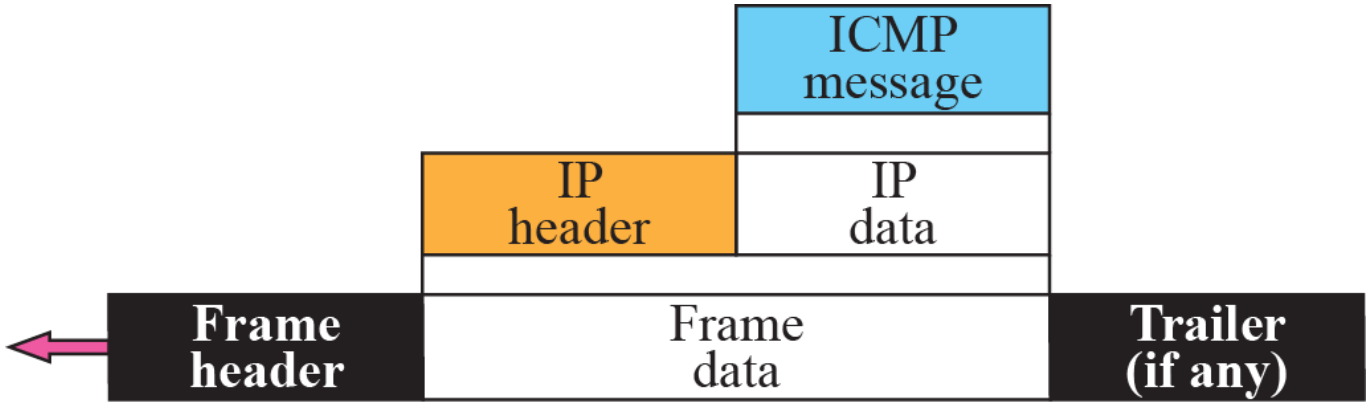
Introduction

- The IP protocol has no error-reporting or error correcting mechanism.
- What happens if something goes wrong? What happens if a router must discard a datagram because it cannot find a router to the final destination, or because the time-to-live field has a zero value?
- These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host.

Position of ICMP in the network layer



ICMP encapsulation



ICMP

- ICMP messages are divided into two broad categories:
  - error-reporting messages
  - query messages.

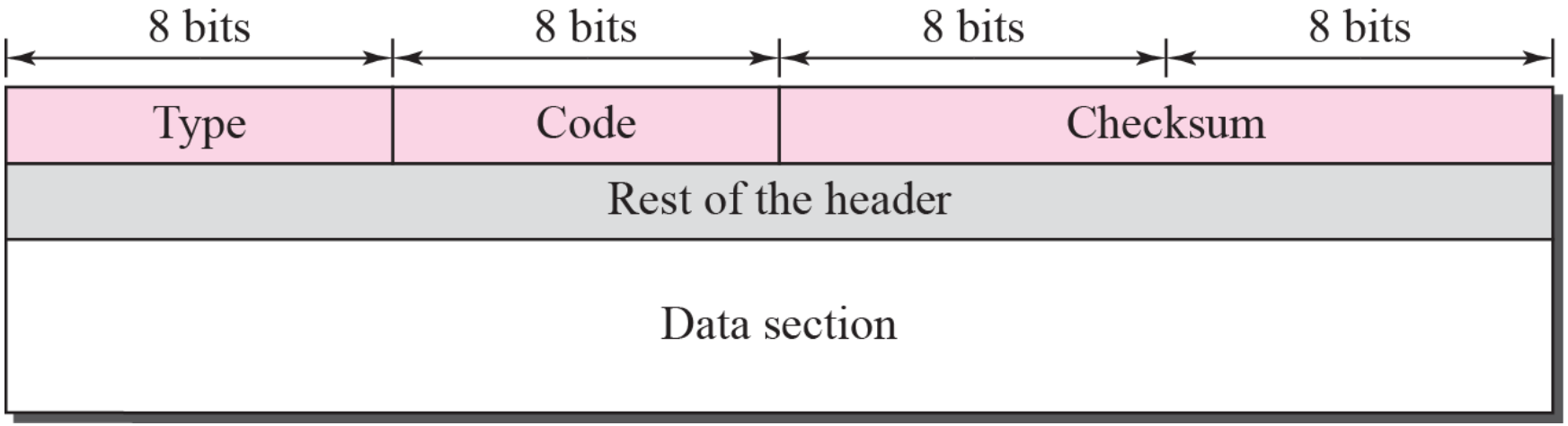
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

- The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

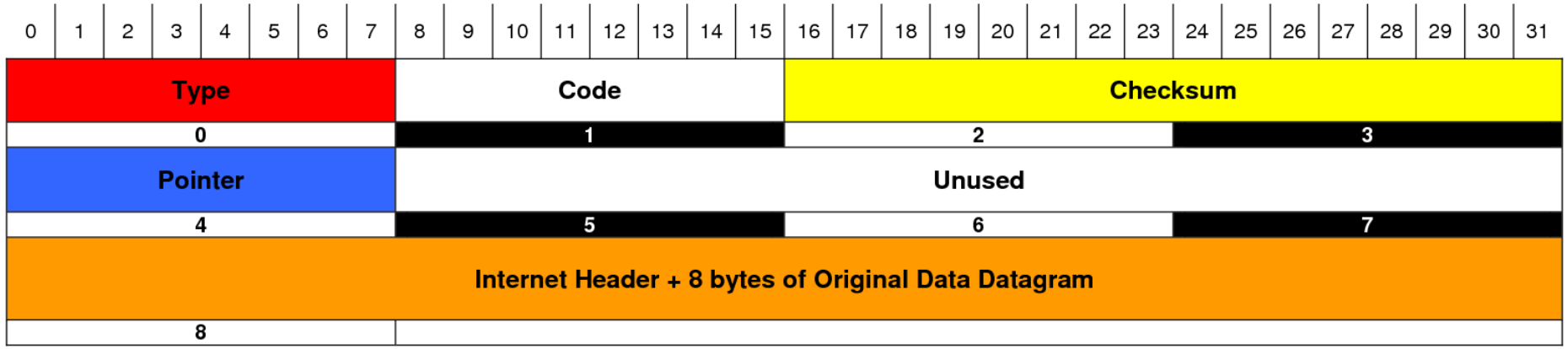
Table 9.1 *ICMP messages*

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

General format of ICMP messages



ICMP Parameter Message Format



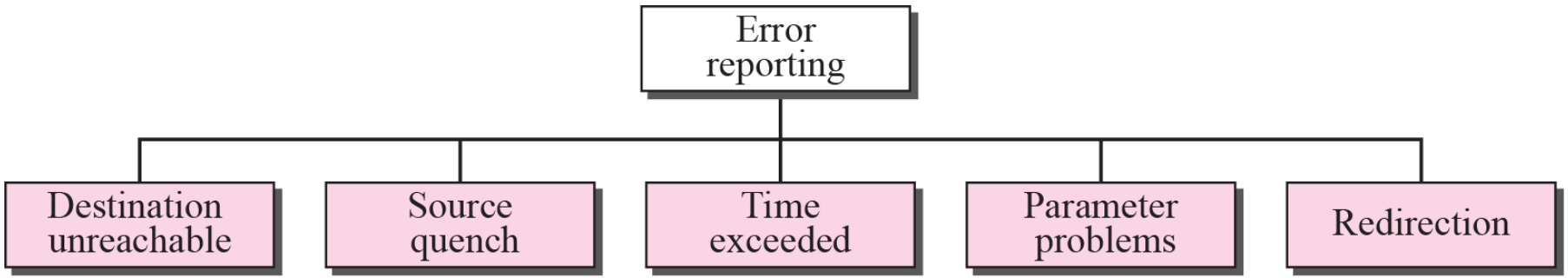
Type	Code	Meaning
0	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication admin prohibited
4	0	Source Quench (Slow down/Shut up)

Type	Code	Meaning
5	0	Redirect datagram for the network
	1	Redirect datagram for the host
	2	Redirect datagram for the TOS & Network
	3	Redirect datagram for the TOS & Host
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	Time To Live exceeded in transit
	1	Fragment reassemble time exceeded
12	0	Pointer indicates the error (Parameter Problem)
	1	Missing a required option (Parameter Problem)
	2	Bad length (Parameter Problem)
13	0	Time Stamp
14	0	Time Stamp Reply
15	0	Information Request
16	0	Informaiton Reply
17	0	Address Mask Request
18	0	Address Mask Reply
30	0	Traceroute (Tracert)

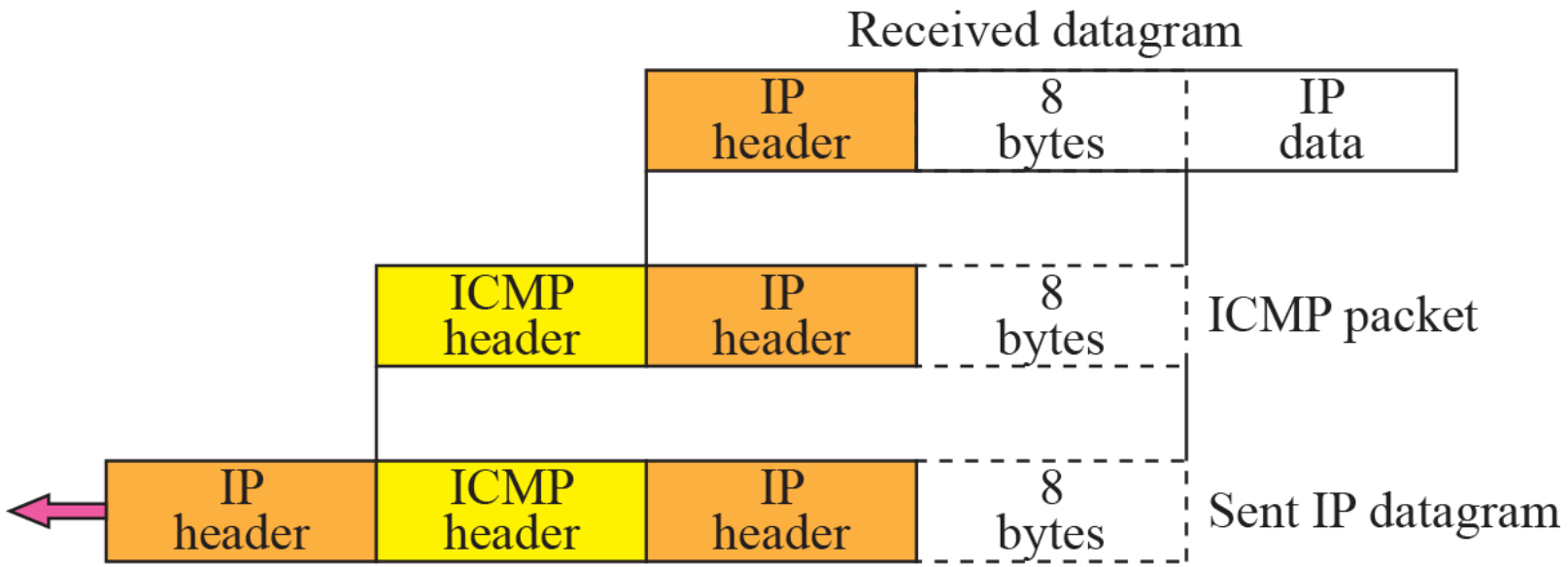
Note

ICMP always reports error messages to the original source.

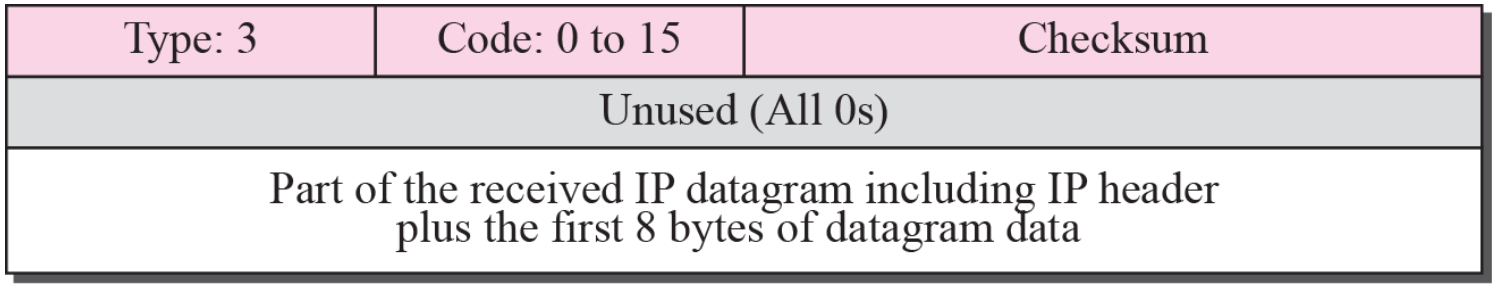
Error-reporting messages



Contents of data field for the error message



Destination-unreachable format

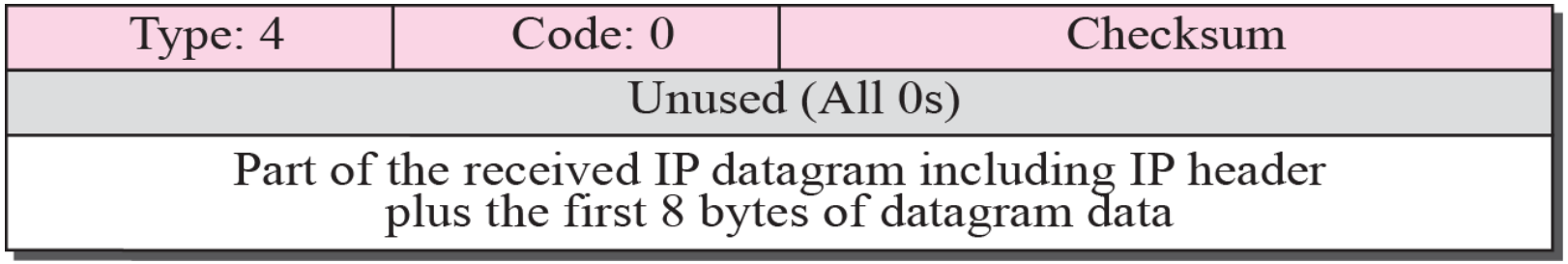


Note

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

Other destination-unreachable messages can be created only by routers.

Source-quench format



Note

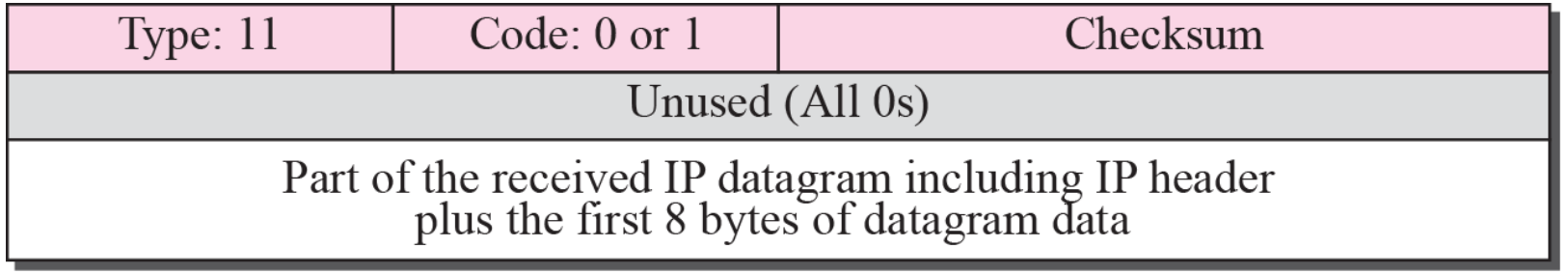
A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host.

The source must slow down the sending of datagrams until the congestion is relieved.

Note

One source-quench message is sent for each datagram that is discarded due to congestion.

Time-exceeded message format



Note

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.

Note

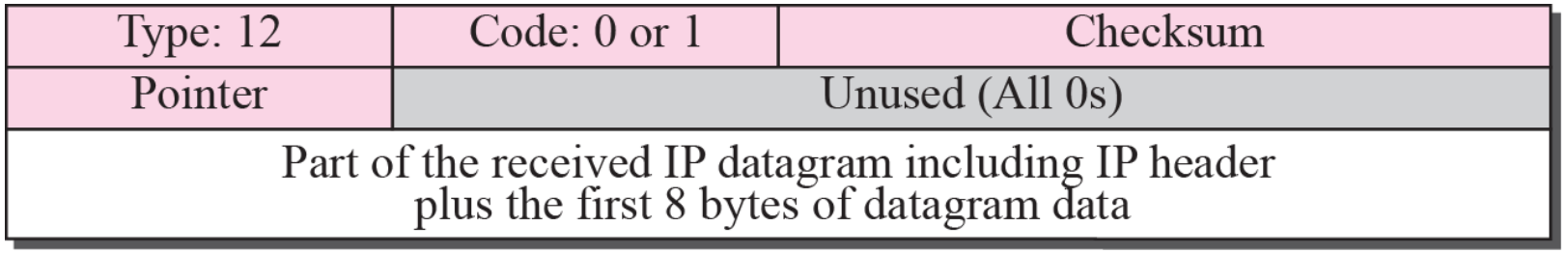
When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.

Note

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.

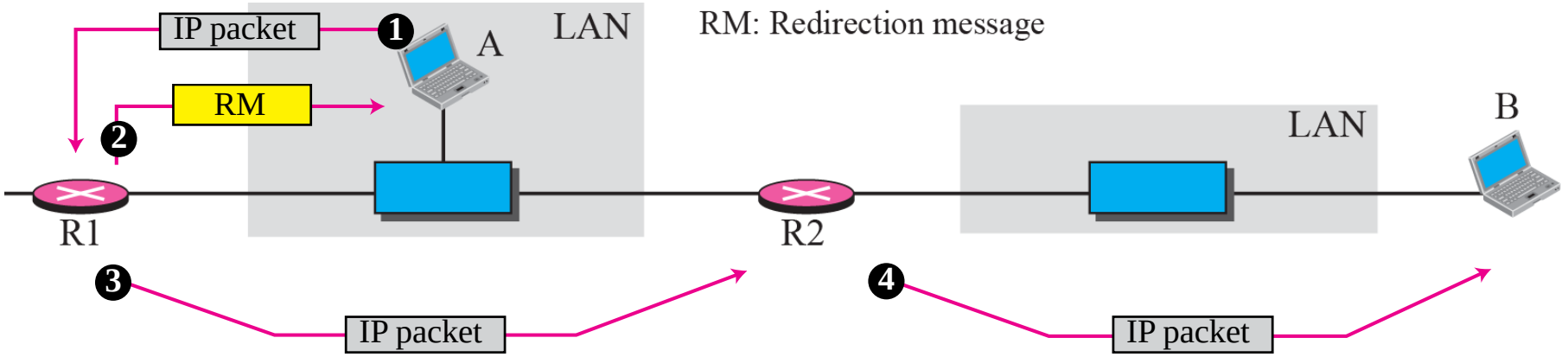
Parameter-problem message format



Note

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

Redirection concept

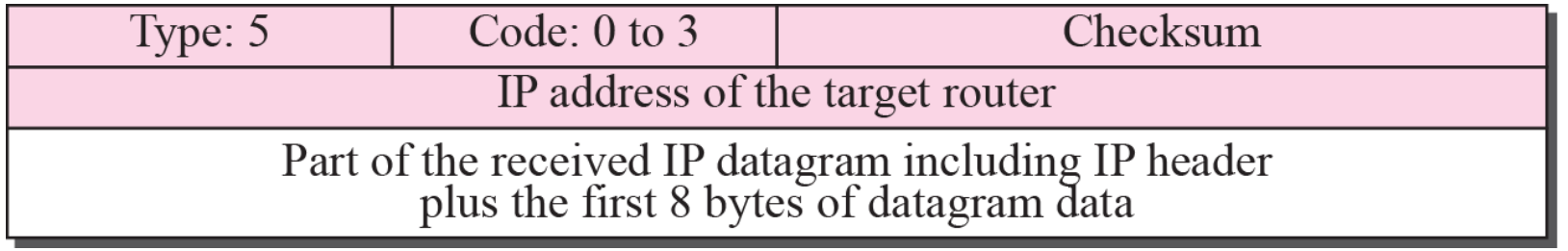


Note

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.

Redirection message format



Note

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

Table 9.1 *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

Note

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.

Note

Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol.

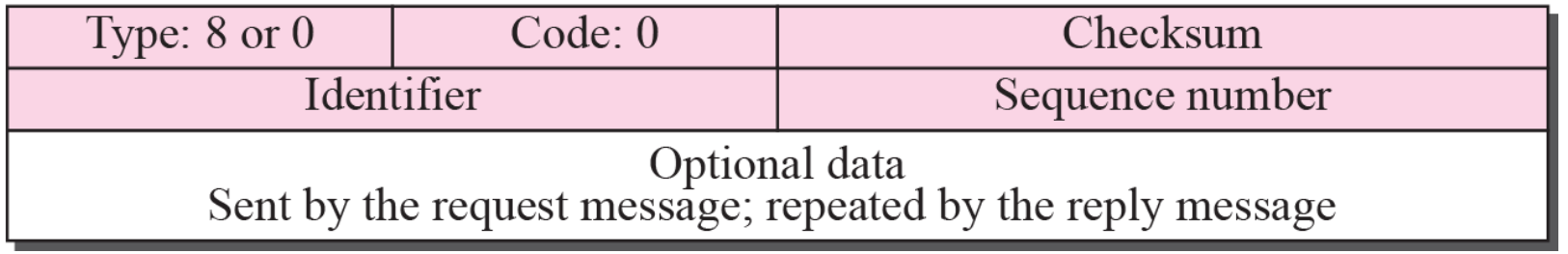
Note

Echo-request and echo-reply messages can test the reachability of a host.

This is usually done by invoking the ping command.

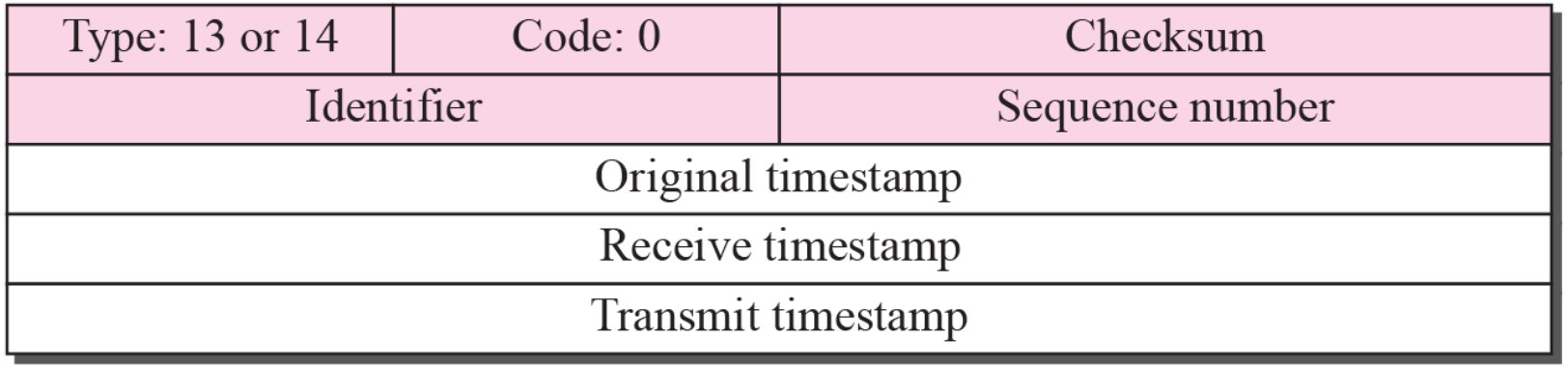
Echo-request and echo-reply message

Type 8: Echo request
Type 0: Echo reply



Timestamp-request and timestamp-reply message format

Type 13: request
Type 14: reply



Note

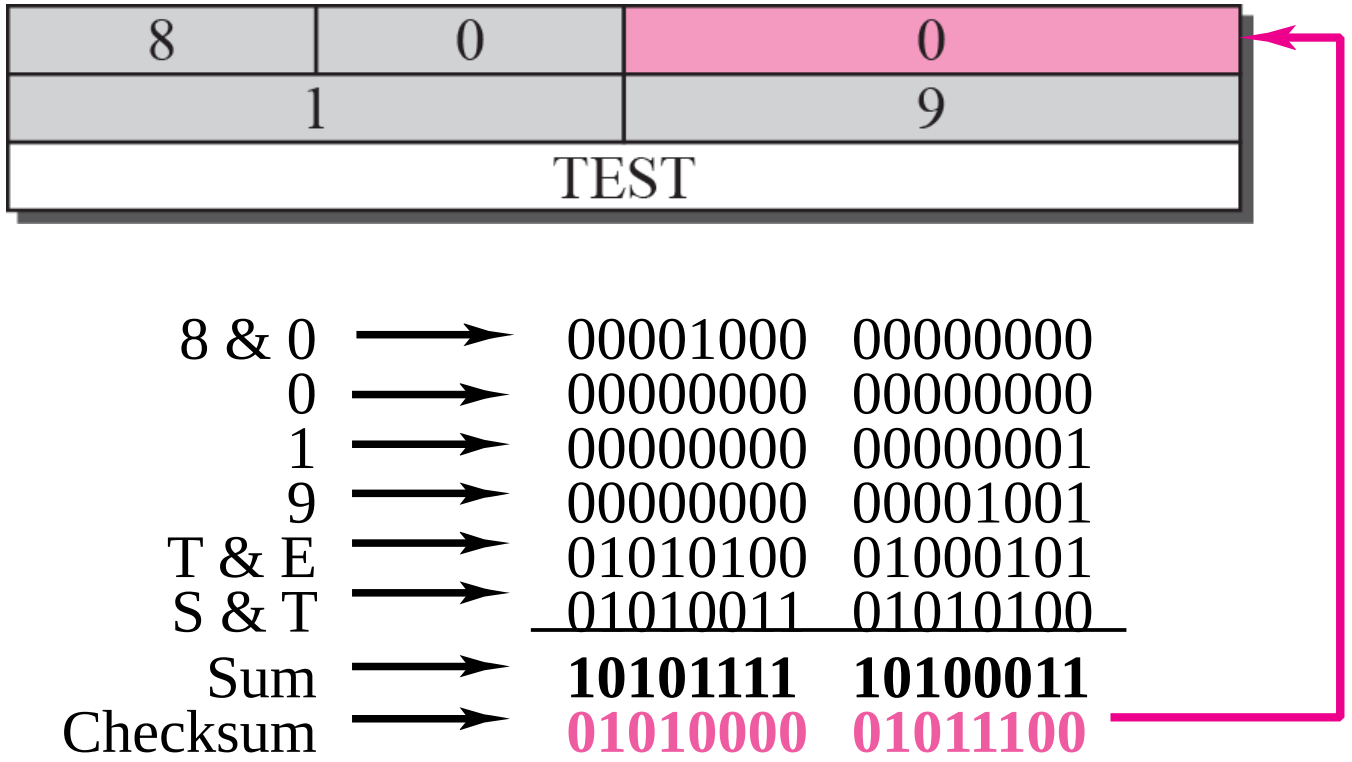
Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine even if their clocks are not synchronized.

Note

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.

Example of checksum calculation

Figure shows an example of checksum calculation for a simple echo-request message. We randomly chose the identifier to be 1 and the sequence number to be 9. The message is divided into 16-bit (2-byte) words. The words are added together and the sum is complemented. Now the sender can put this value in the checksum field.



DEBUGGING TOOLS

We introduce two tools that use ICMP for debugging: ping and traceroute.

- ✓ Ping
- ✓ Traceroute

Example

We use the ping program to test the server fhda.edu. The result is shown below:

```
$ 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
```

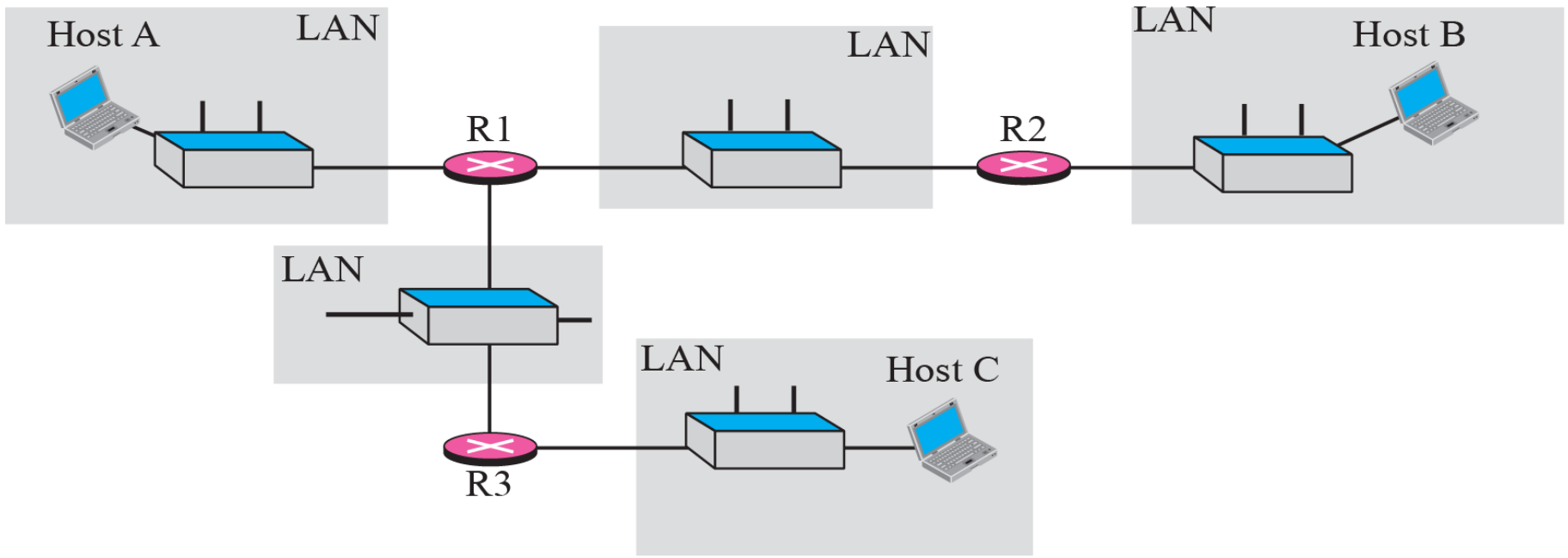
Example

For the second example, we want to know if the adelphia.net mail server is alive and running. The result is shown below: Note that in this case, we sent 14 packets, but only 13 have been returned. We may have interrupted the program before the last packet, with sequence number 13, was returned.

```
$ ping mail.adelphia.net
PING mail.adelphia.net (68.168.78.100) 56(84) bytes of data.
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=0    ttl=48    time=85.4 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=1    ttl=48    time=84.6 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=2    ttl=48    time=84.9 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=3    ttl=48    time=84.3 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=4    ttl=48    time=84.5 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=5    ttl=48    time=84.7 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=6    ttl=48    time=84.6 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=7    ttl=48    time=84.7 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=8    ttl=48    time=84.4 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=9    ttl=48    time=84.2 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=10   ttl=48    time=84.9 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=11   ttl=48    time=84.6 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=12   ttl=48    time=84.5 ms

--- mail.adelphia.net ping statistics ---
14 packets transmitted, 13 received, 7% packet loss, time 13129 ms
rtt min/avg/max/mdev = 84.207/84.694/85.469
```

The traceroute program operation



Example

We use 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
```

Example

In this example, we trace a longer route, the route to xerox.com. The following is a partial listing.

```
$ traceroute xerox.com
traceroute to xerox.com (13.1.64.93), 30 hops max, 38 byte packets
1  Dcore.fhda.edu      (153.18.31.254)     0.622 ms    0.891 ms    0.875 ms
2  Ddmz.fhda.edu       (153.18.251.40)     2.132 ms    2.266 ms    2.094 ms
3  Cinic.fhda.edu      (153.18.253.126)    2.110 ms    2.145 ms    1.763 ms
4  cenic.net           (137.164.32.140)    3.069 ms    2.875 ms    2.930 ms
5  cenic.net           (137.164.22.31)     4.205 ms    4.870 ms    4.197 ms
6  cenic.net           (137.164.22.167)    4.250 ms    4.159 ms    4.078 ms
7  cogentco.com        (38.112.6.225)      5.062 ms    4.825 ms    5.020 ms
8  cogentco.com        (66.28.4.69)        6.070 ms    6.207 ms    5.653 ms
9  cogentco.com        (66.28.4.94)        6.070 ms    5.928 ms    5.499 ms
```