Internet Control Message Protocol
Part-I

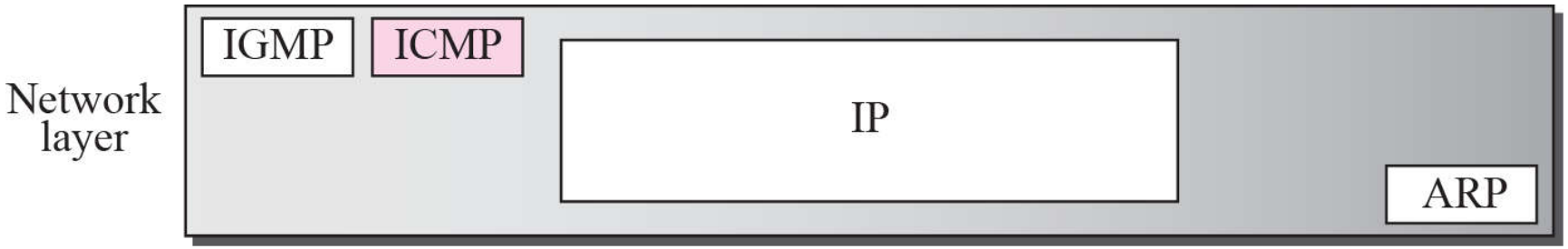
Internet Control Message Protocol (ICMP) (1/2)

- IP is an unreliable method for delivery of network data.
- It has no built-in processes to ensure that data is delivered in the event that problems exist with network communication.
- If an intermediary device such as a router fails, or if a destination device is disconnected from the network, data cannot be delivered.
- Additionally, nothing in its basic design allows IP to notify the sender that a data transmission has failed.

Internet Control Message Protocol (ICMP) (2/2)

- Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP.
- ICMP does not overcome the unreliability issues in IP.
- Reliability must be provided by upper layer protocols if it is needed.

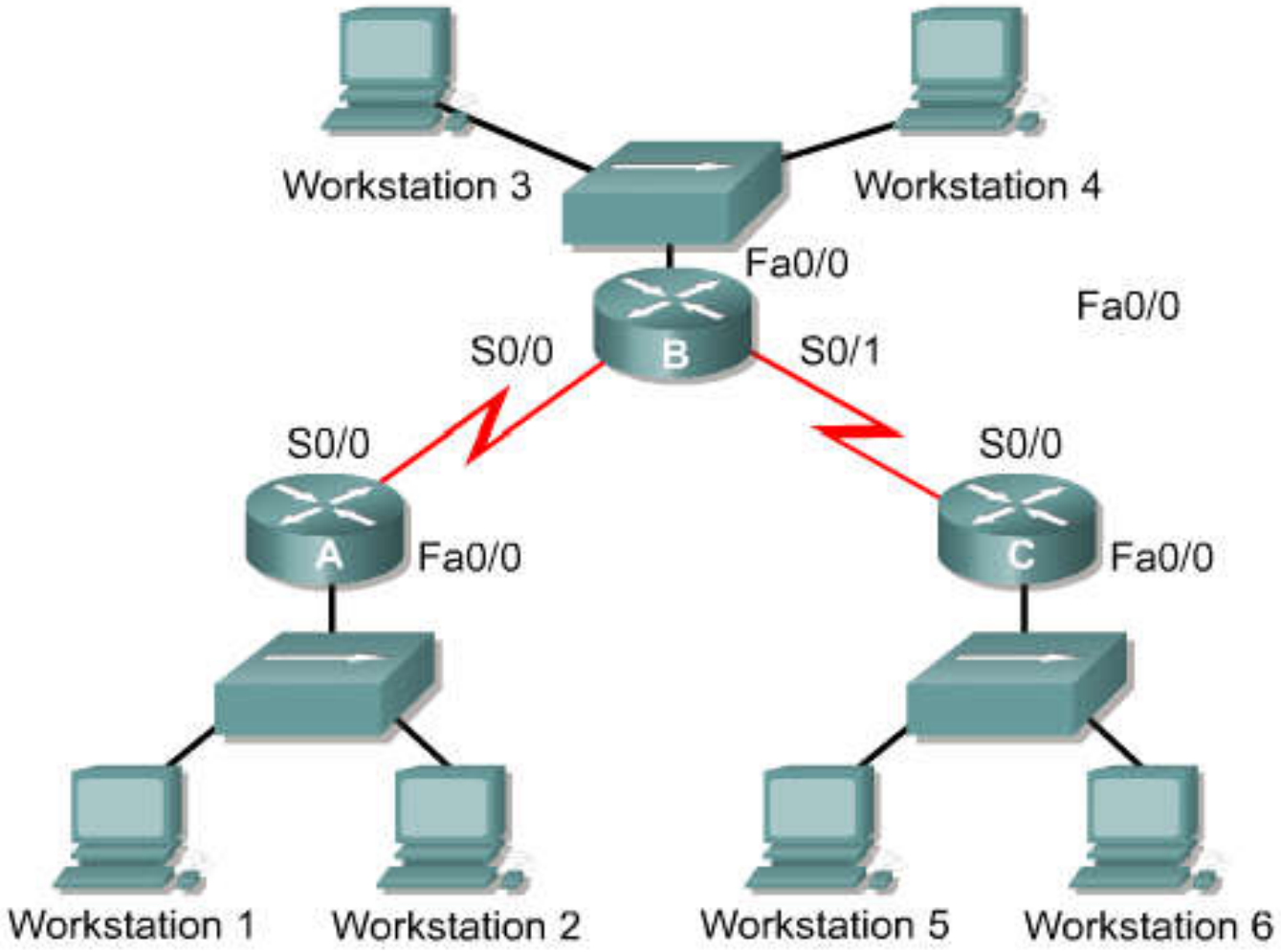
Position of ICMP in the Network Layer



Error Reporting and Error Correction

- ICMP is an error reporting protocol for IP.
- When datagram delivery errors occur, ICMP is used to report these errors back to the source of the datagram.
- ICMP does not correct the encountered network problem; it merely reports the problem.
- ICMP reports on the status of the delivered packet only to the source device.
- *It does not propagate information about network changes to routers.*

A Typical Network with Workstations



ICMP Messages (1/2)

- ICMP messages are divided into two broad categories:
  - error-reporting messages and
  - 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.
- Also, *hosts can discover and learn about routers on their network and routers can help a node redirect its messages*.

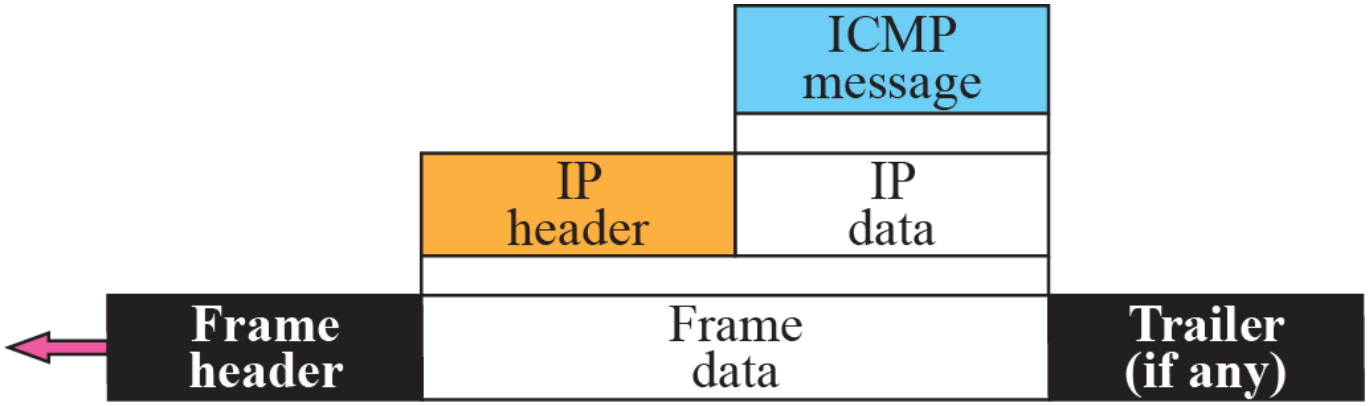
ICMP Messages (2/2)

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

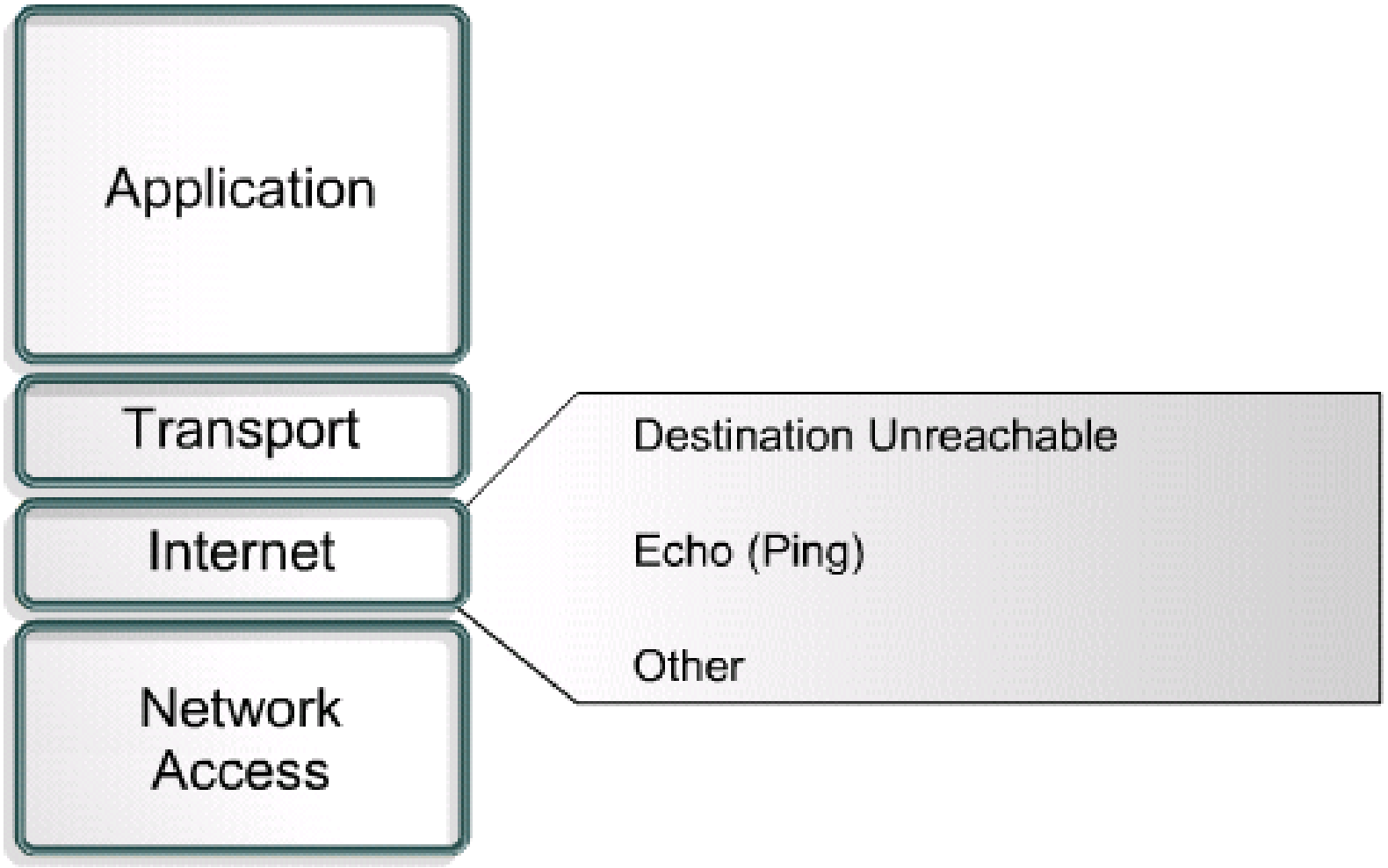
ICMP Message Delivery

- ICMP messages are encapsulated into datagrams in the same way any other data is delivered using IP.
- This creates a scenario where error reports could generate more error reports, causing increased congestion on an already ailing network.
- For this reason, errors created by ICMP messages do not generate their own ICMP messages.
- It is thus possible to have a datagram delivery error that is never reported back to the sender of the data.

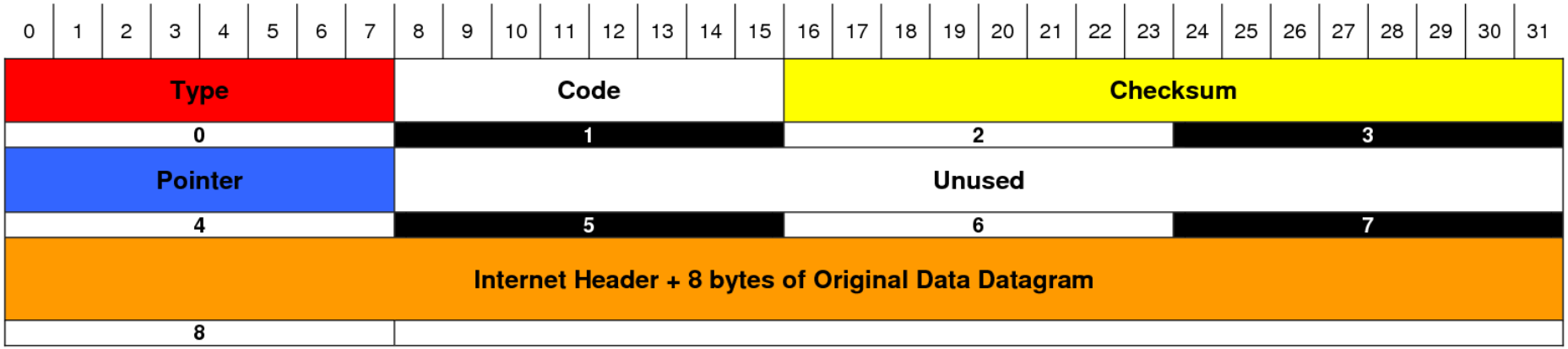
ICMP Encapsulation



TCP/IP Protocol Suite with ICMP



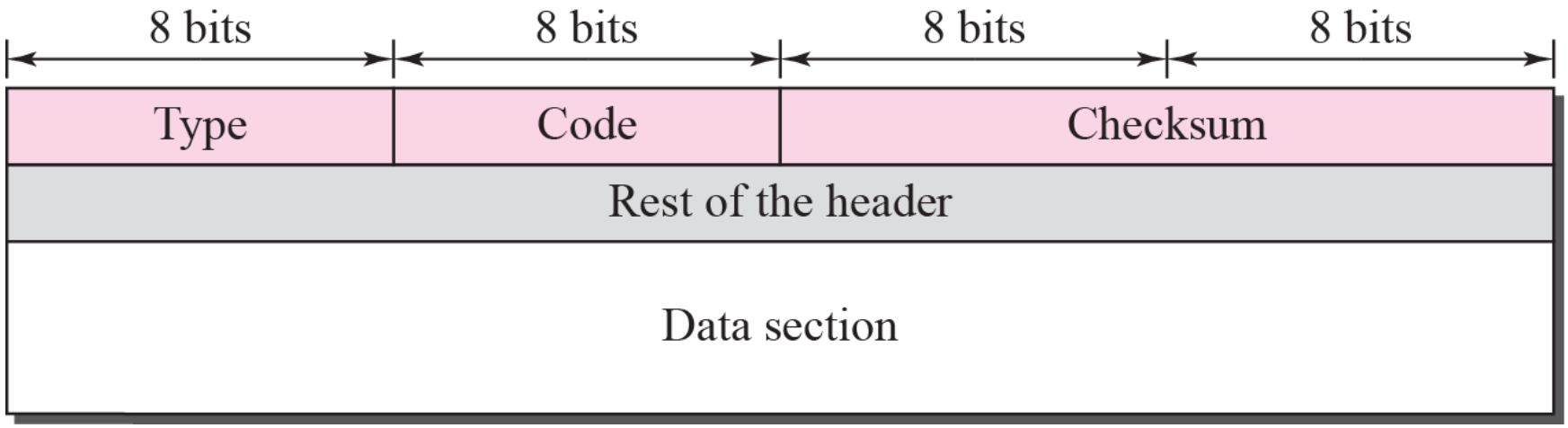
ICMP Parameter Message Format



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)

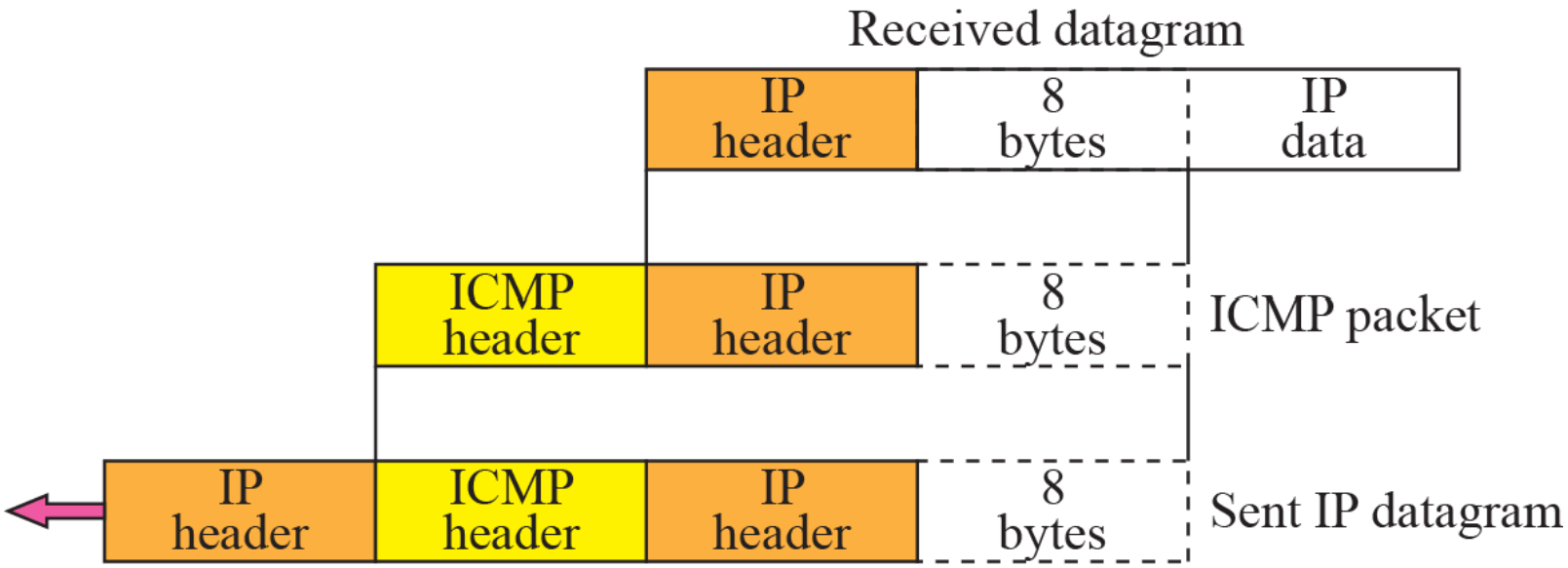
General Format of ICMP messages



Note

ICMP always reports error messages to the original source.

Contents of Data Field for the Error Message



ICMP

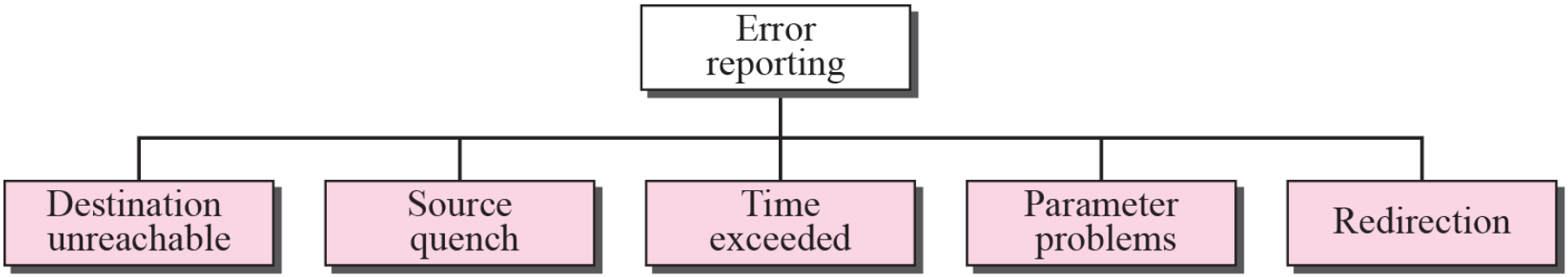
TCP/IP Suite Error and Control Messages

Outline

- **Overview of TCP/IP Error Message**
- **TCP/IP Suite Control Messages**

ICMP
TCP/IP Suite Error Messages

Error Reporting Messages



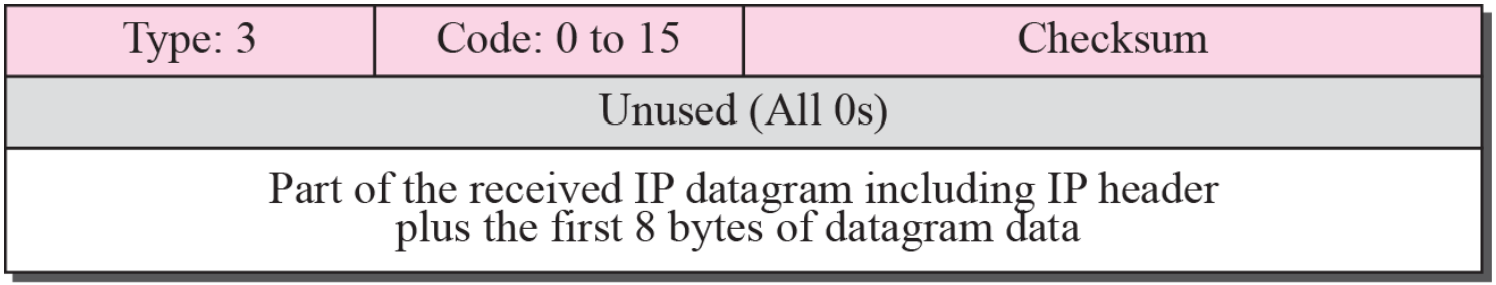
Unreachable Networks (1/2)

- Network communication depends upon certain basic conditions being met.
  - First, the sending and receiving devices must have the TCP/IP protocol stack properly configured.
  - Second, intermediary devices must be in place to route the datagram from the source device and its network to the destination network.

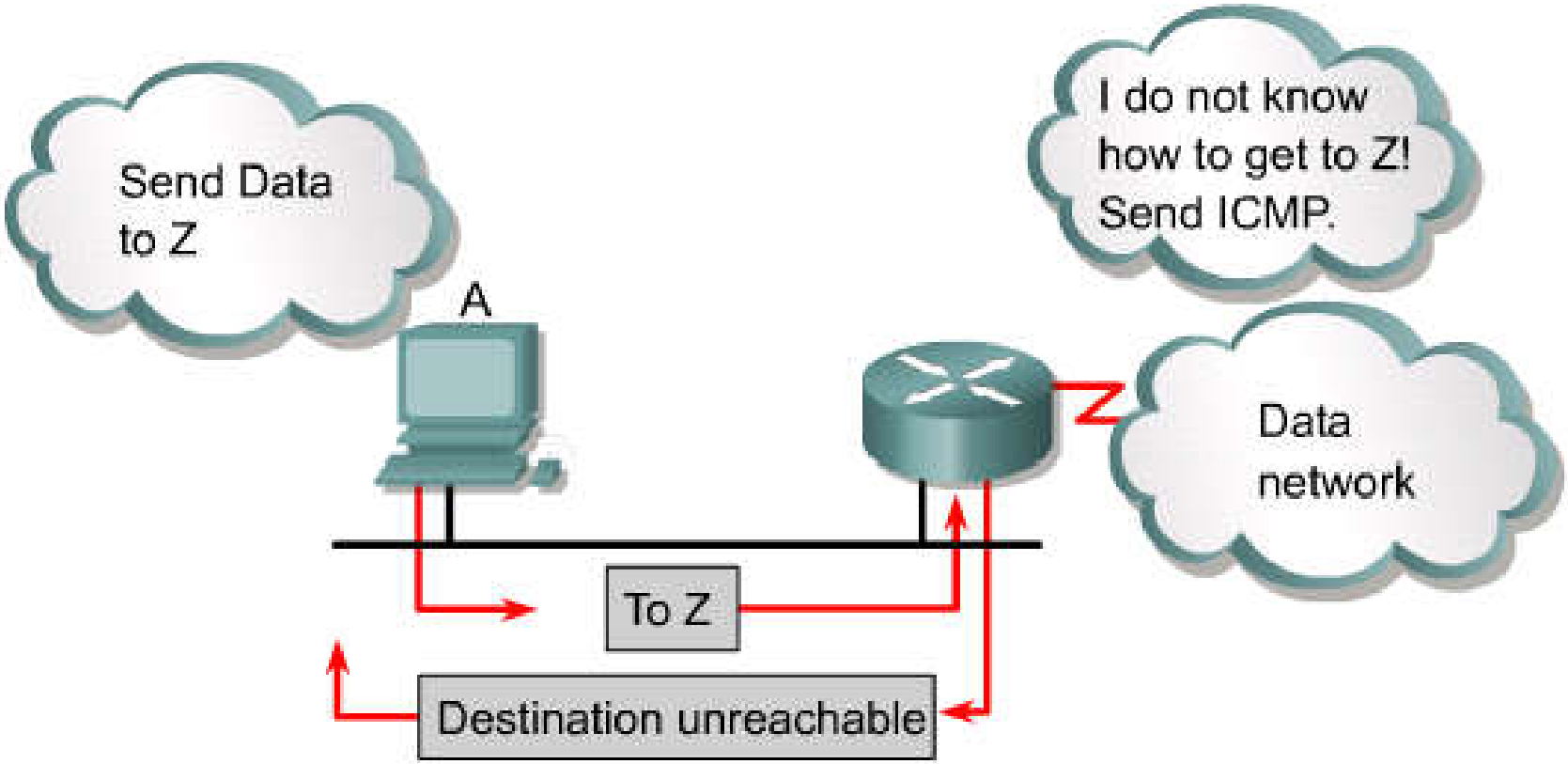
Unreachable Networks (2/2)

- For instance, the sending device may address the datagram to a non-existent IP address or to a destination device that is disconnected from its network.
- Routers can also be points of failure if a connecting interface is down or if the router does not have the information necessary to find the destination network.
- If a destination network is not accessible, it is said to be an unreachable network.

Destination Unreachable Format



Destination Unreachable



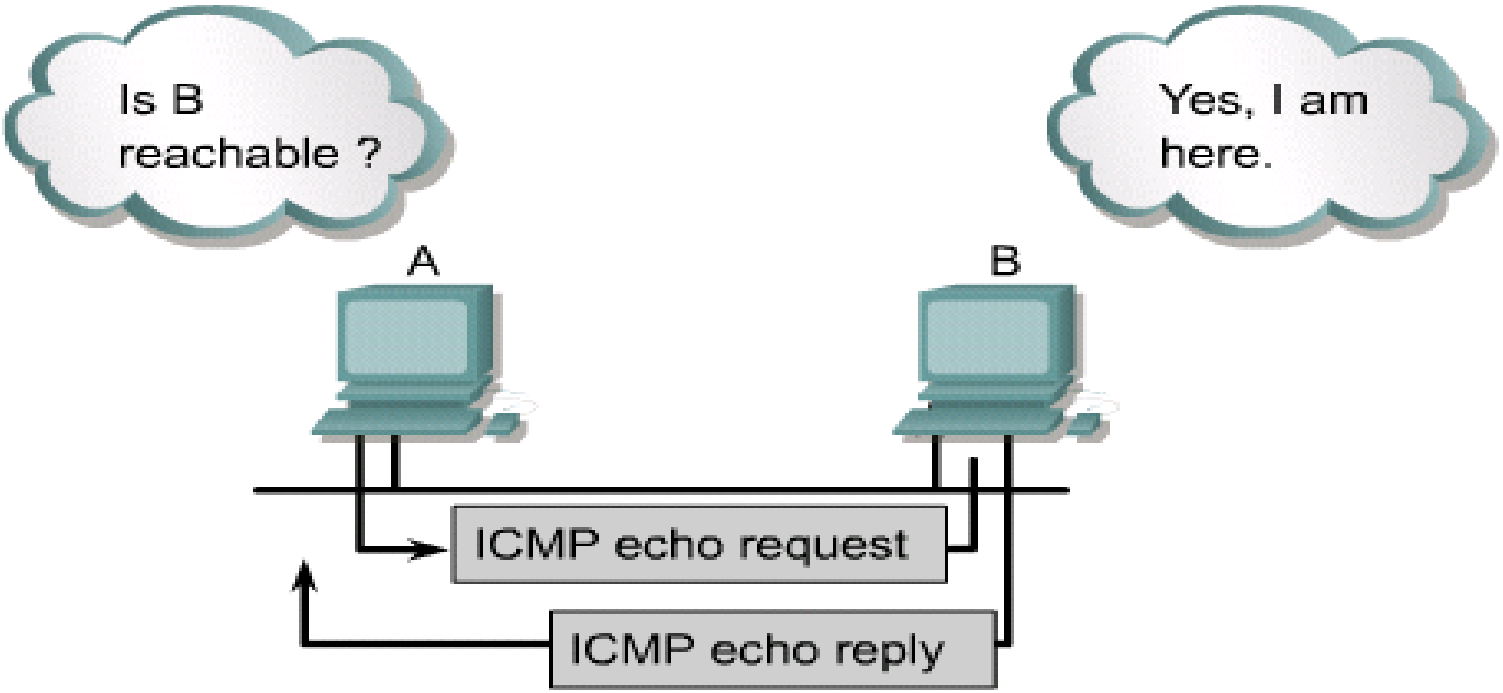
An ICMP destination unreachable meassage is sent if:

- Host or port unreachable
- Network unreachable

Using ping to Test Destination Reachability

- The ICMP protocol can be used to test the availability of a particular destination.
- The following Figure shows ICMP being used to issue an echo request message to the destination device.
- If the destination device receives the ICMP echo request, it formulates an echo reply message to send back to the source of the echo request.
- The echo request message is typically initiated using the **ping** command.

Traffic Generated by the ping Command



Traffic generated by the `ping` command

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.

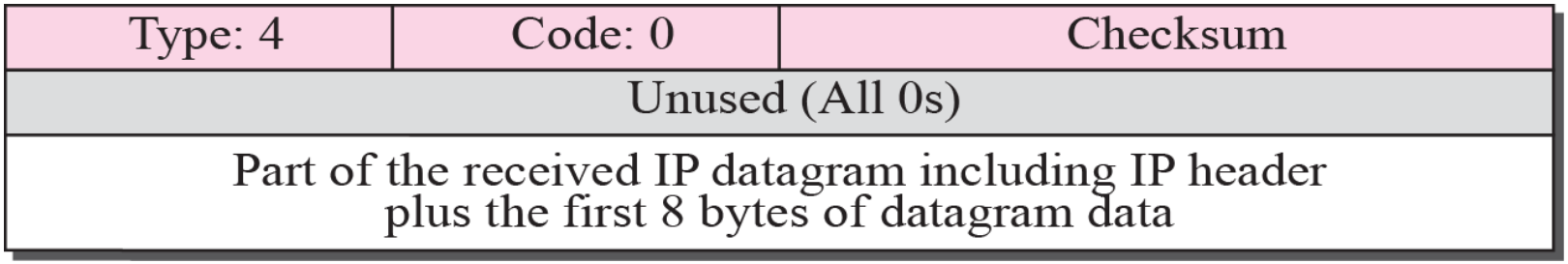
Note

A router cannot detect all problems that prevent the delivery of a packet.

Note

There is no flow-control or congestion-control mechanism in the IP protocol.

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.

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.

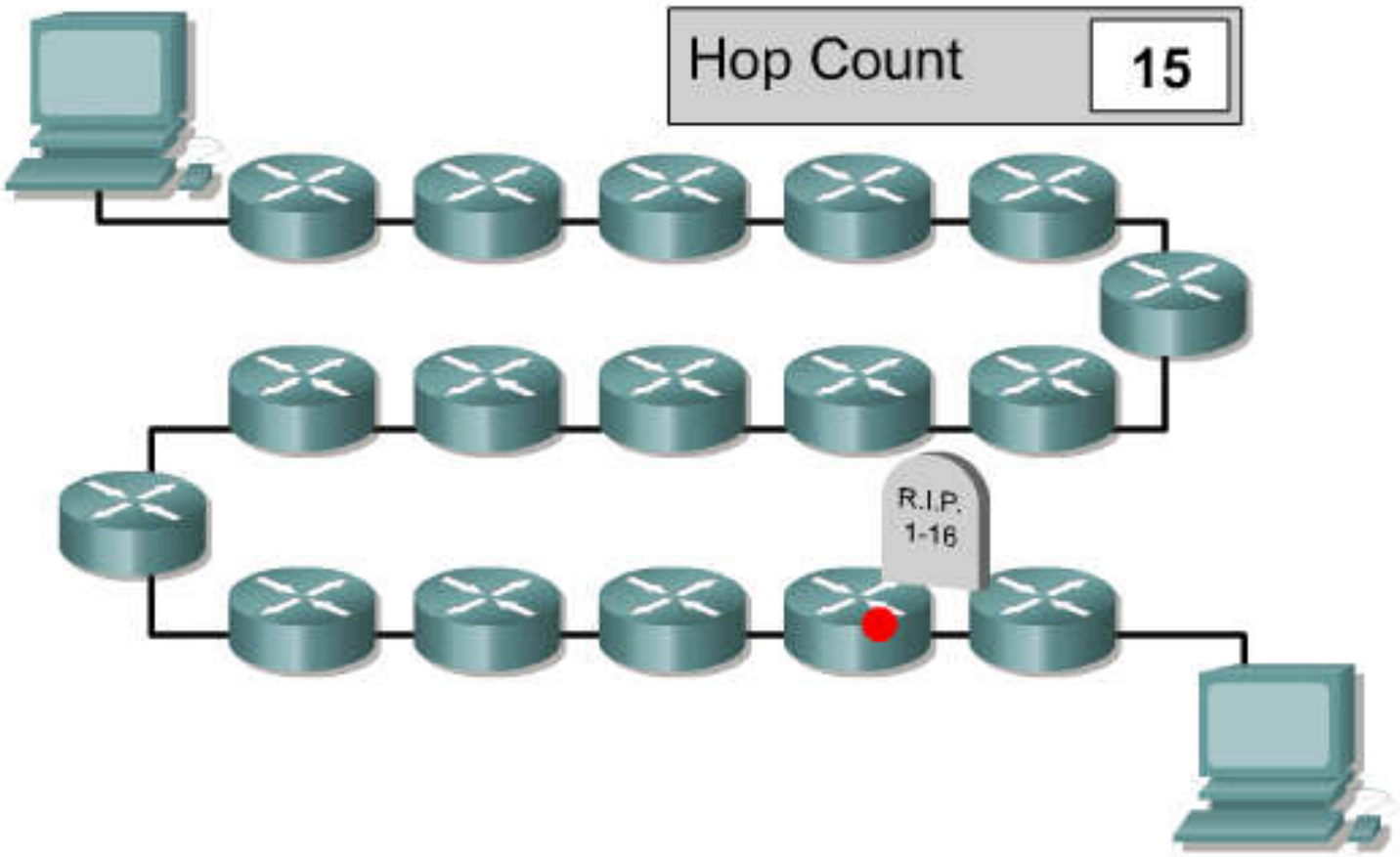
Detecting Excessively Long Routes (1/3)

- The limitations of the routing protocol can result in destinations being unreachable.
- For example, RIP has a limit on the distance a certain routing information is allowed to travel.
- The hop limit of RIP is 15, which means that the packet will only be allowed to pass through 15 routers.

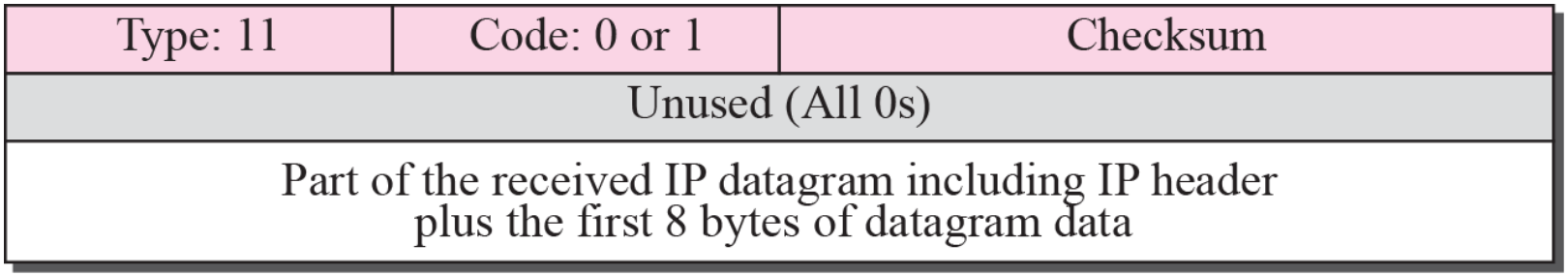
Detecting Excessively Long Routes (2/3)

- Whether the actual path includes a circular routing path or too many hops, the packet will eventually exceed the maximum hop count.
- This is also known as reaching its time-to-live (TTL), because the TTL value typically matches the maximum hop count defined by the routing protocol.
- As each router processes the datagram, it decreases the TTL value by one.
- When the TTL of the datagram value reaches zero, the packet is discarded.
- ICMP uses a time exceeded message to notify the source device that the TTL of the datagram has been exceeded.

Detecting Excessively Long Routes (3/3)



Time Exceeded Message Format



Note

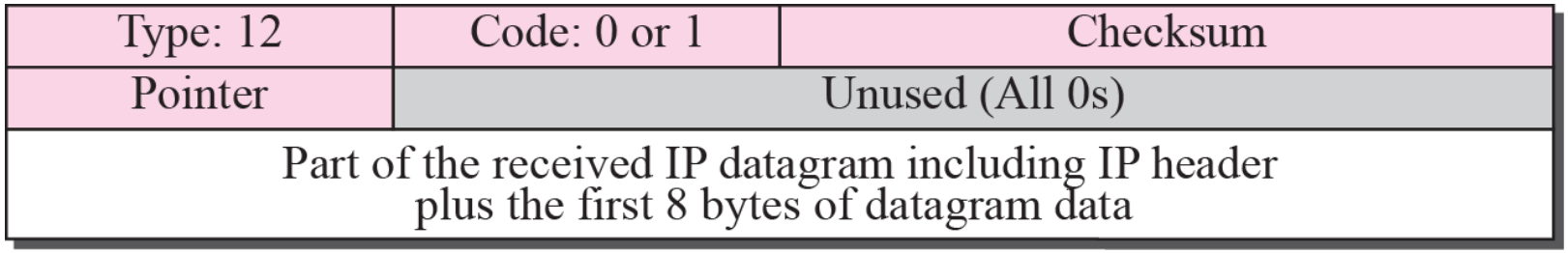
In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero.

Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time.

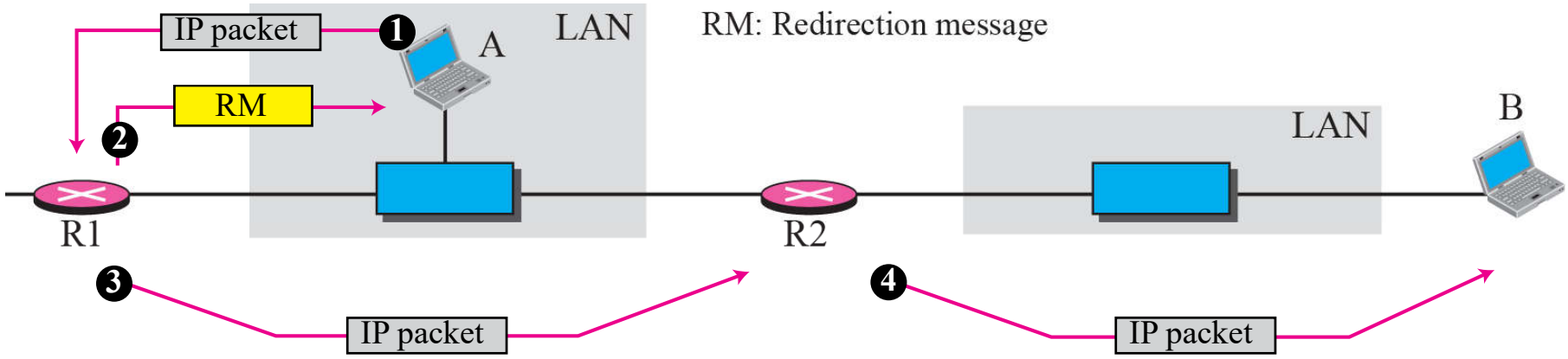
Note

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

Parameter-problem message format



Redirection Concept

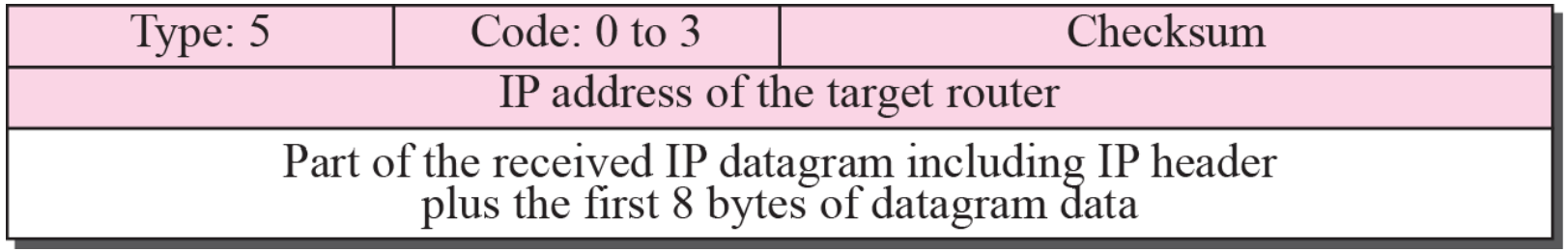


Note

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.

Echo Messages

- ICMP message formats start with these three fields:
  - Type
  - Code
  - Checksum
- The type field indicates the type of ICMP message being sent.
- The code field includes further information specific to the message type.
- The checksum field, as in other types of packets, is used to verify the integrity of the data.

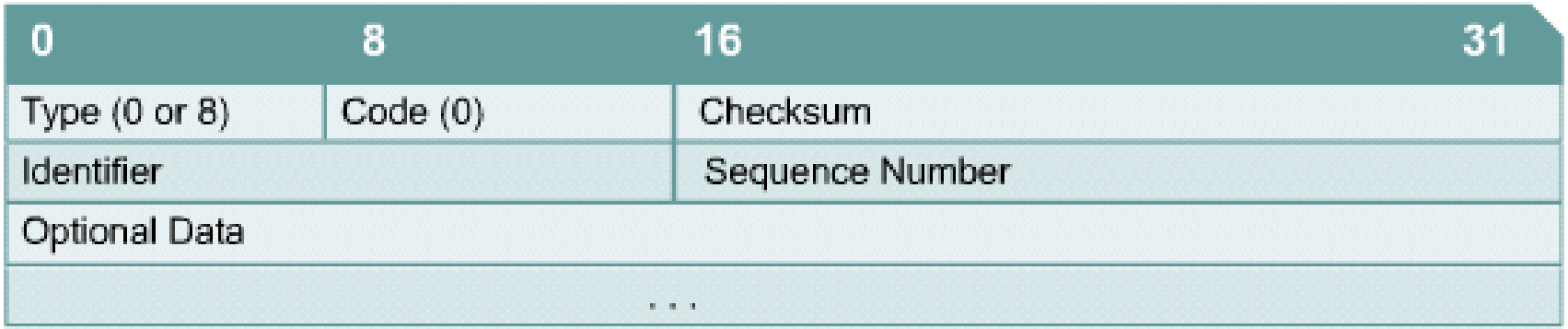
ICMP Message Types

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP Echo Request and Reply Messages (1/2)

- Figure shows the message format for the ICMP echo request and echo reply messages.
- The identifier and sequence number fields are used to match the echo replies to the corresponding echo request.
- The optional data field contains additional information that may be a part of the echo reply or echo request message.

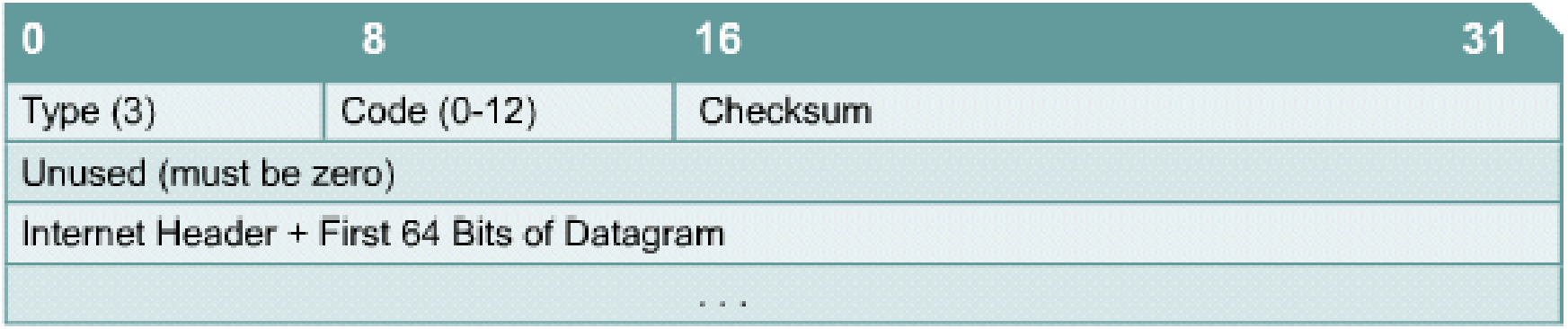
ICMP Echo Request and Reply Messages (2/2)



Destination Unreachable Message

- Figure shows an ICMP destination unreachable message header.
- The value of 3 in the type field indicates it is a destination unreachable message.
- The code value indicates the reason the packet could not be delivered.

Destination Unreachable Message



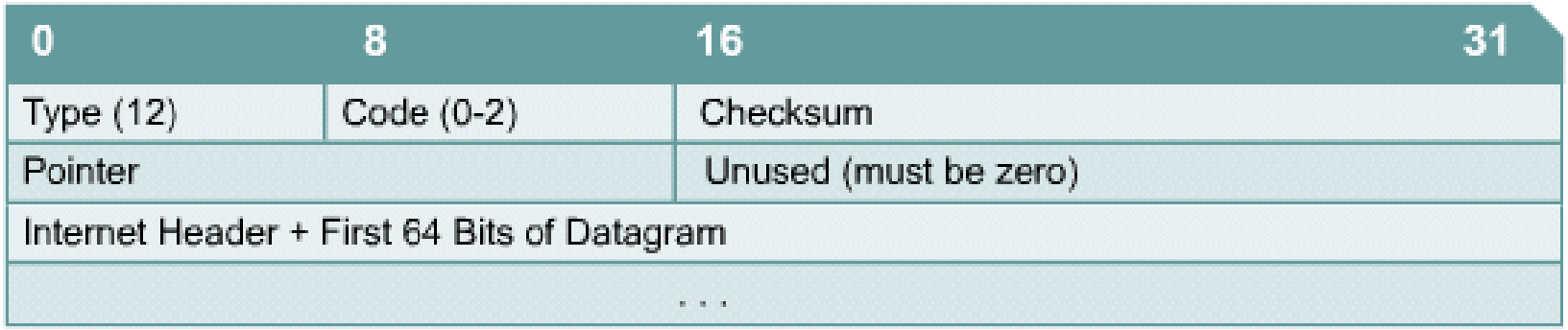
ICMP Code Types

0 = net unreachable
1 = host unreachable
2 = protocol unreachable
3 = port unreachable
4 = fragmentation needed and DF set
5 = source route failed
6 = destination network unknown
7 = destination host unknown
8 = source host isolated
9 = communication with destination network administratively prohibited
10 = communication with destination host administratively prohibited
11 = network unreachable for type device
12 = host unreachable for type of service

Miscellaneous Error Reporting (1/2)

- Devices that process datagrams may not be able to forward a datagram due to some type of error in the header.
- *This error does not relate to the state of the destination host or network but still prevents the datagram from being processed and delivered*.
- In this case, an ICMP type 12 parameter problem message is sent to the source of the datagram.

Miscellaneous Error Reporting (2/2)



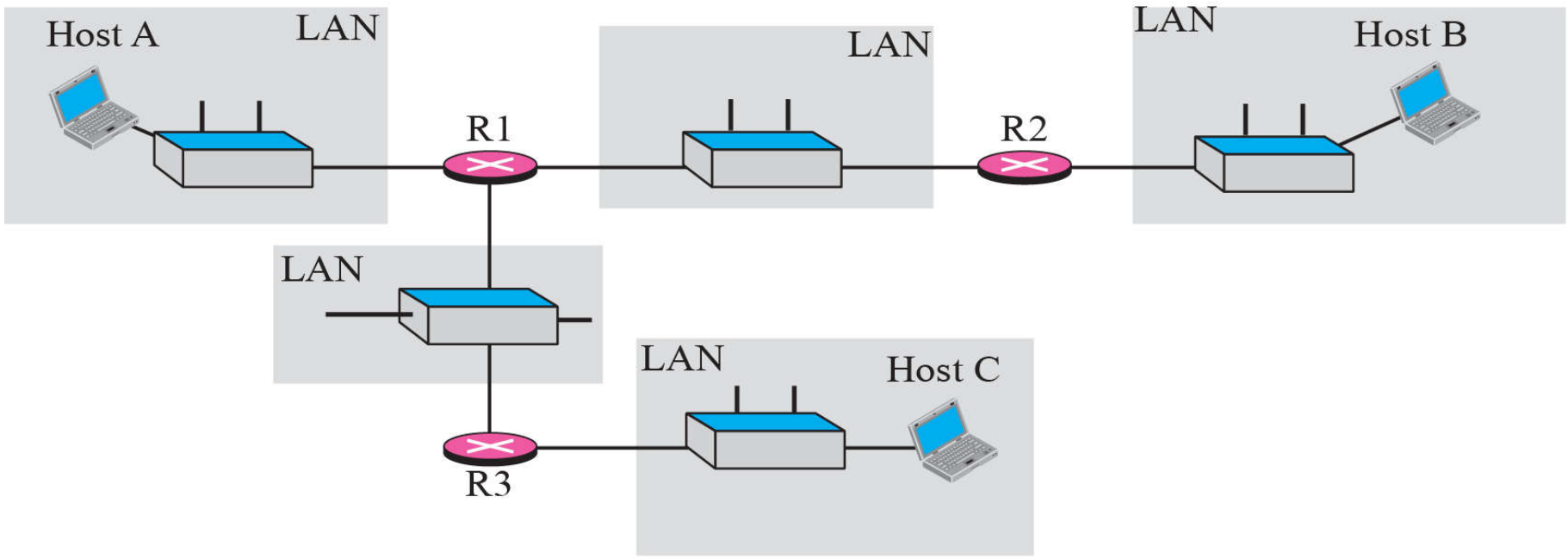
Debugging Tools

- There are several tools that can be used in the Internet for debugging.
- We can find if a host or router is alive and running.
- We can trace the route of a packet.
- We introduce two tools that use ICMP for debugging: ping and traceroute.

Topics Discussed in the Section

- ✓ ping
- ✓ traceroute

The traceroute Program Operation



Example 1: traceroute

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 2: traceroute

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
```

Example 3: traceroute

An interesting point is that a host can send a traceroute packet to itself. This can be done by specifying the host as the destination. The packet goes to the loopback address as we expect.

```
$ traceroute voyager.deanza.edu
traceroute to voyager.deanza.edu  (127.0.0.1), 30 hops max, 38 byte packets
1  voyager          (127.0.0.1)          0.178 ms          0.086 ms          0.055 ms
```

Example 4: traceroute

Finally, we use the traceroute program to find the route between fhda.edu and mhhe.com (McGraw-Hill server). We notice that we cannot find the whole route. When traceroute does not receive a response within 5 seconds, it prints an asterisk to signify a problem (not the case in this example), and then tries the next hop.

```
$ traceroute mhhe.com
traceroute to mhhe.com (198.45.24.104), 30 hops max, 38 byte packets
```

1	Dcore.fhda.edu	(153.18.31.254)	1.025 ms	0.892 ms	0.880 ms
2	Ddmz.fhda.edu	(153.18.251.40)	2.141 ms	2.159 ms	2.103 ms
3	Cinic.fhda.edu	(153.18.253.126)	2.159 ms	2.050 ms	1.992 ms
4	cenic.net	(137.164.32.140)	3.220 ms	2.929 ms	2.943 ms
5	cenic.net	(137.164.22.59)	3.217 ms	2.998 ms	2.755 ms
6	SanJose1.net	(209.247.159.109)	10.653 ms	10.639 ms	10.618 ms
7	SanJose2.net	(64.159.2.1)	10.804 ms	10.798 ms	10.634 ms
8	Denver1.Level3.net	(64.159.1.114)	43.404 ms	43.367 ms	43.414 ms
9	Denver2.Level3.net	(4.68.112.162)	43.533 ms	43.290 ms	43.347 ms
10	unknown	(64.156.40.134)	55.509 ms	55.462 ms	55.647 ms
11	mcleodusa1.net	(64.198.100.2)	60.961 ms	55.681 ms	55.461 ms
12	mcleodusa2.net	(64.198.101.202)	55.692 ms	55.617 ms	55.505 ms
13	mcleodusa3.net	(64.198.101.142)	56.059 ms	55.623 ms	56.333 ms
14	mcleodusa4.net	(209.253.101.178)	297.199 ms	192.790 ms	250.594 ms
15	eppg.com	(198.45.24.246)	71.213 ms	70.536 ms	70.663 ms
16	...	...	...	...	...

ICMP
TCP/IP Suite Control Messages

Introduction to Control Messages (1/2)

- The Internet Control Message Protocol (ICMP) is an integral part of the TCP/IP protocol suite.
- Unlike error messages, control messages are not the results of lost packets or error conditions which occur during packet transmission.
- Instead, they are used to inform hosts of conditions such as network congestion or the existence of a better gateway to a remote network.

Introduction to Control Messages (2/2)

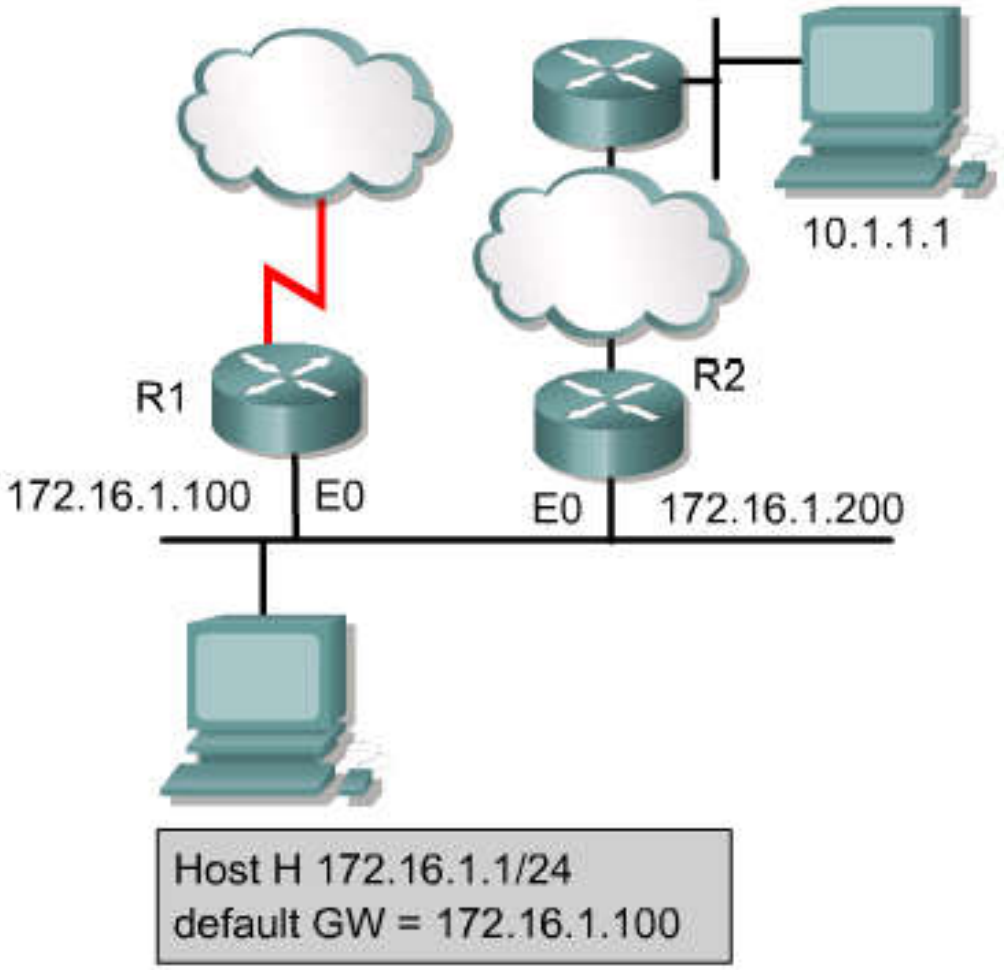
- Like all ICMP messages, ICMP control messages are encapsulated within an IP datagram.
- ICMP uses IP datagrams in order to traverse multiple networks.
- Multiple types of control messages are used by ICMP.

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP Redirect/Change Requests (1/4)

- This type of message can only be initiated by a gateway.
- However, in some circumstances, a host connects to a segment that has two or more directly connected routers.
- In this case, the default gateway of the host may need to use a redirect/change request to inform the host of the best path to a certain network.

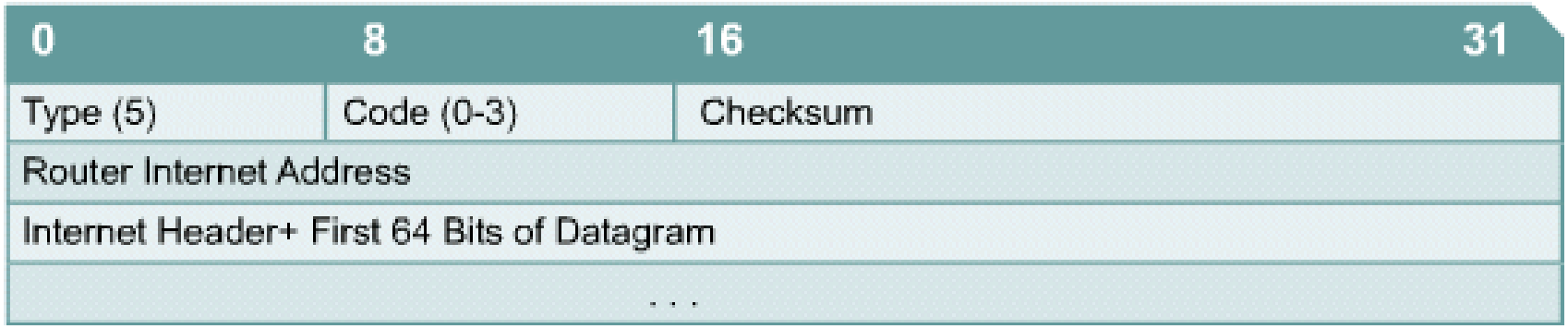
ICMP Redirect/Change Requests (2/4)



ICMP Redirect/Change Requests (3/4)

- Default gateways only send ICMP redirect/change request messages if the following conditions are met:
  - The interface on which the packet comes into the router is the same interface on which the packet gets routed out.
  - The subnet/network of the source IP address is the same subnet/network of the next-hop IP address of the routed packet.
  - The datagram is not source-routed.
  - The route for the redirect is not another ICMP redirect or a default route.
  - The router is configured to send redirects. (By default, Cisco routers send ICMP redirects. The interface subcommand **no ip redirects** will disable ICMP redirects.)

ICMP Redirect/Change Requests (4/4)



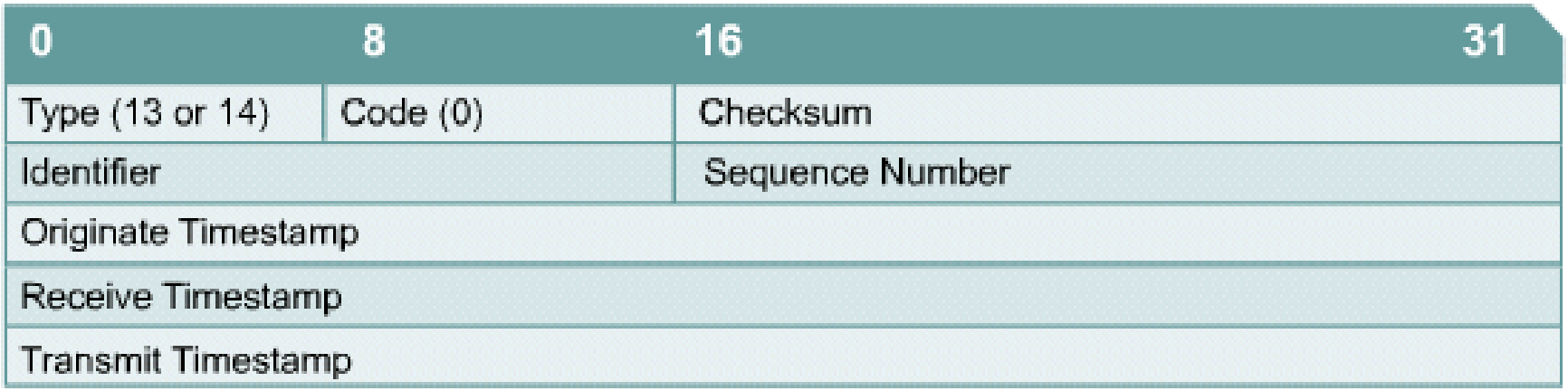
0	8	16	31
Type (5)	Code (0-3)	Checksum	
Router Internet Address			
Internet Header+ First 64 Bits of Datagram			
. . .			

Code Value	Required Action
0	Redirected datagrams for the network.
1	Redirected datagrams for the host.
2	Redirected datagrams for the type of services and networks.
3	Redirected datagrams for the type of services and host.

Clock synchronization and transit time estimation (1/2)

- Hosts on different networks who are trying to communicate using software that requires time synchronization can sometimes encounter problems.
- The ICMP timestamp message type is designed to help alleviate this problem.
- The ICMP timestamp request message allows a host to ask for the current time according to the remote host.
- The remote host uses an ICMP timestamp reply message to respond to the request.

Clock synchronization and transit time estimation (2/2)



0	8	16	31
Type (13 or 14)	Code (0)	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

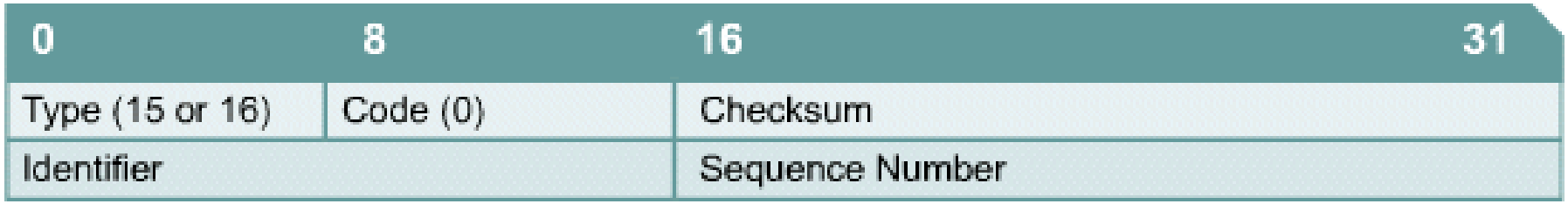
Network Time Protocol (NTP)

- More robust protocols such as Network Time Protocol (NTP) at the upper layers of the TCP/IP protocol stack perform clock synchronization in a more reliable manner.

Information requests and reply message formats (1/2)

- The ICMP information requests and reply messages were originally intended to allow a host to determine its network number.
- Type 15 signifies an information request message, and type 16 identifies an information reply message.
- This particular ICMP message type is considered obsolete.
- Other protocols such as BOOTP and Dynamic Host Configuration Protocol (DHCP) are now used to allow hosts to obtain their network numbers.

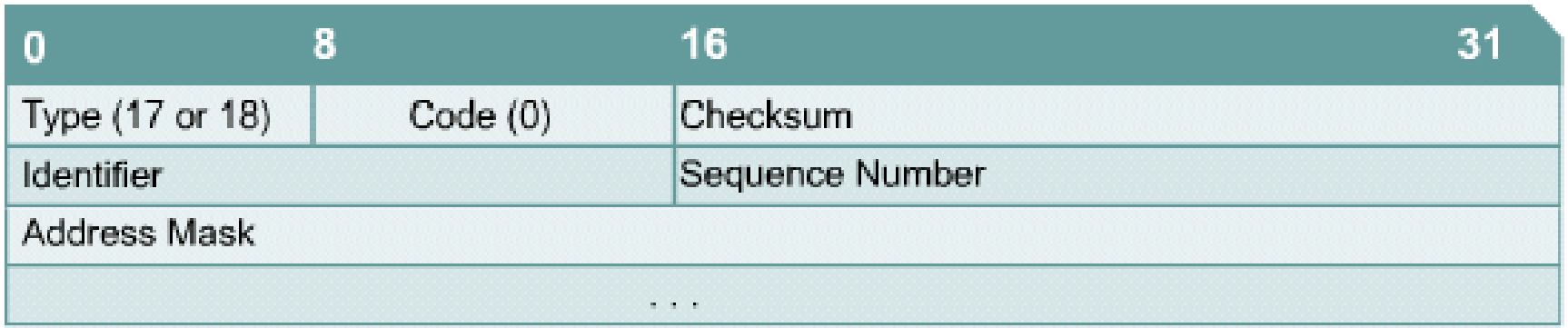
Information requests and reply message formats (2/2)



Address mask requirements (1/2)

- If a host does not know the subnet mask, it may send an address mask request to the local router.
- If the address of the router is known, this request may be sent directly to the router. Otherwise, the request will be broadcast.
- When the router receives the request, it will respond with an address mask reply.

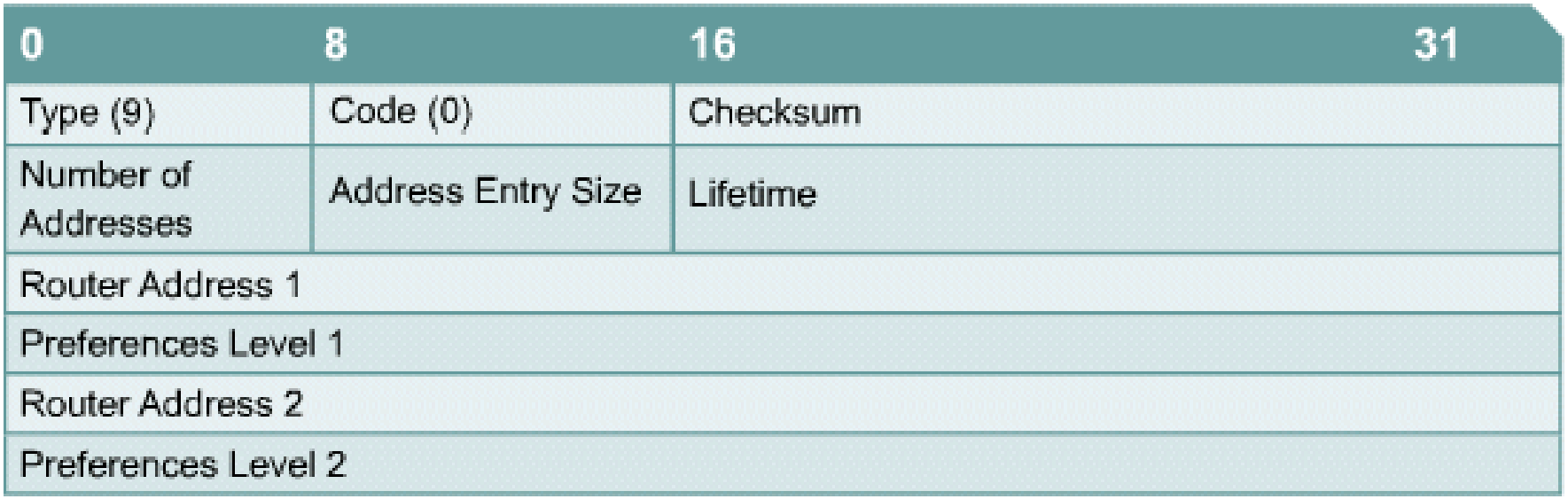
Address mask requirements (2/2)



Router discovery message (1/2)

- When a host on the network boots, and the host has not been manually configured with a default gateway, it can learn of available routers through the process of router discovery.
- This process begins with the host sending a router solicitation message to all routers, using the multicast address 224.0.0.2 as the destination address.
- When a router that supports the discovery process receives the router discovery message, a router advertisement is sent in return.

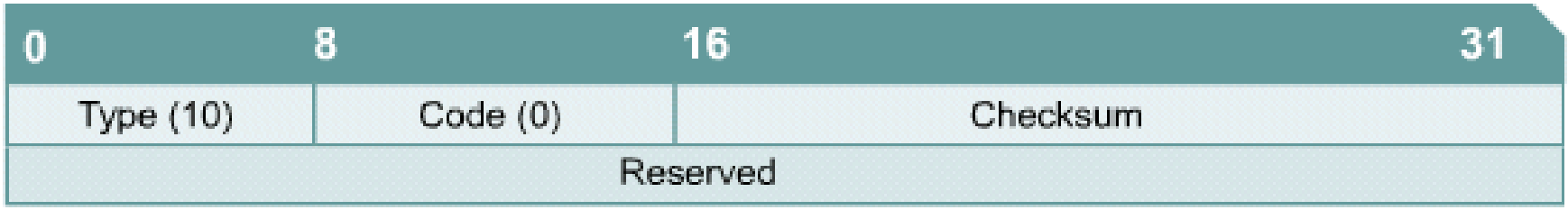
Router discovery message (2/2)



Router solicitation message (1/2)

- A host generates an ICMP router solicitation message in response to a missing default gateway.
- This message is sent via multicast and it is the first step in the router discovery process.
- A local router will respond with a router advertisement identifying the default gateway for the local host.

Router solicitation message (2/2)



Congestion and flow control messages

- Dropped packets occur when there is too much congestion on a network.
- ICMP source-quench messages are used to reduce the amount of data lost.
- The source-quench message asks senders to reduce the rate at which they are transmitting packets.
- Most Cisco routers do not send source-quench messages by default, because the source-quench message may itself add to the network congestion.