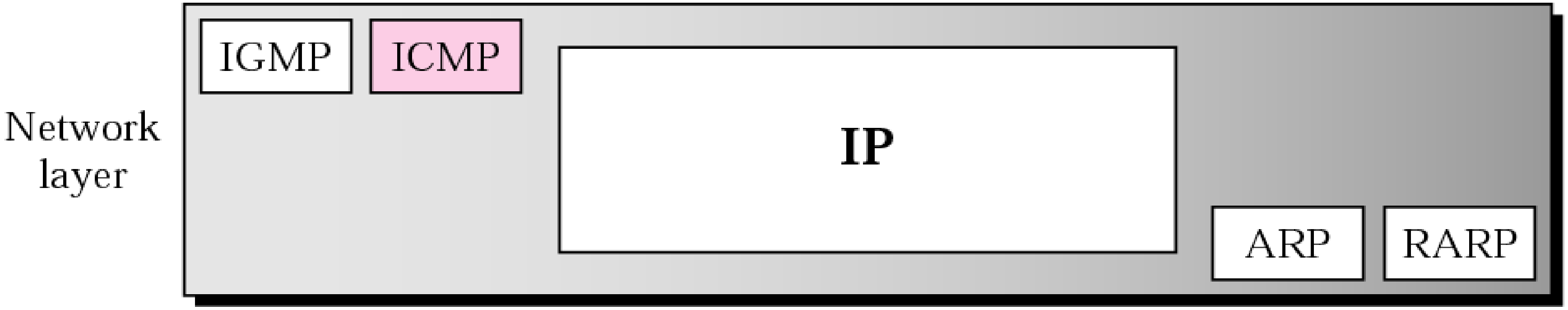
Internet Control Protocols



Internet Control Protocols

- In addition to IP, which is used for data transfer, the Internet has several control protocols used in the network layer, including ICMP, ARP, RARP, BOOTP, and DHCP
- ***ICMP - Internet Control Message Protocol:***
  - The operation of the Internet is monitored closely by the routers.
  - When something unexpected occurs, the event is reported by the ICMP
  - ICMP is also used to test the Internet.
  - About a dozen types of ICMP messages are defined. The most important ones are listed in Fig.
  - Each ICMP message type is encapsulated in an IP packet.

ICMP Messages

a) ICMP messages are divided into two broad categories:

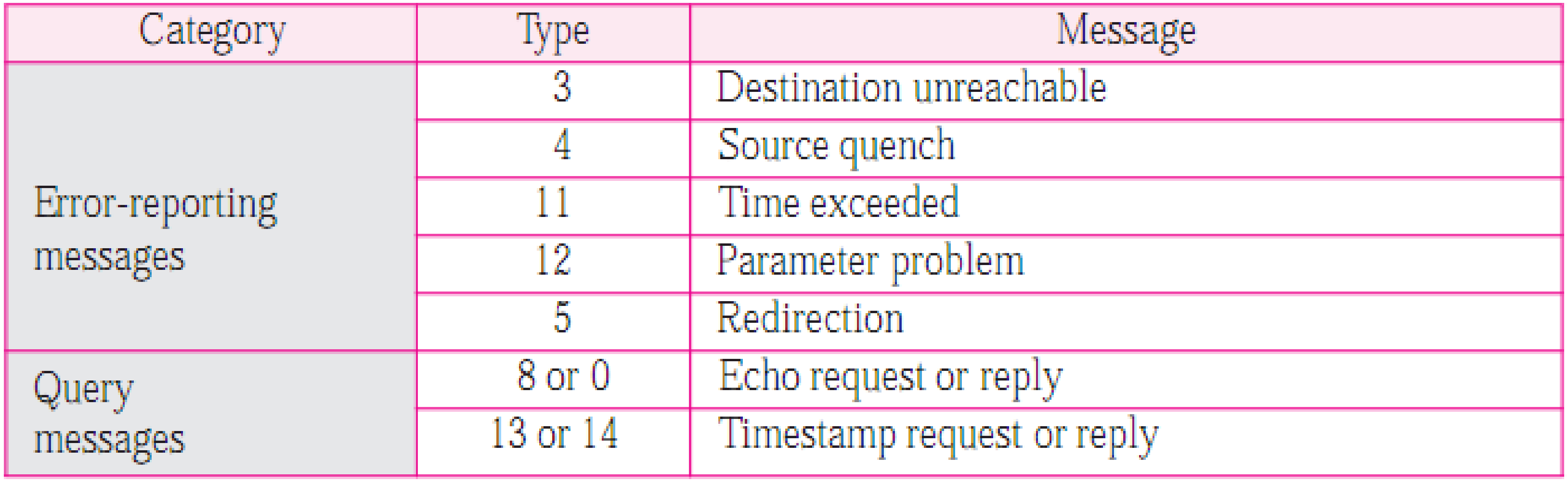
1. Error-reporting messages
   - The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

and

2. Query messages.
   - Occur in pairs, help a host or a network manager get specific information from a router or another host.

ICMP Messages

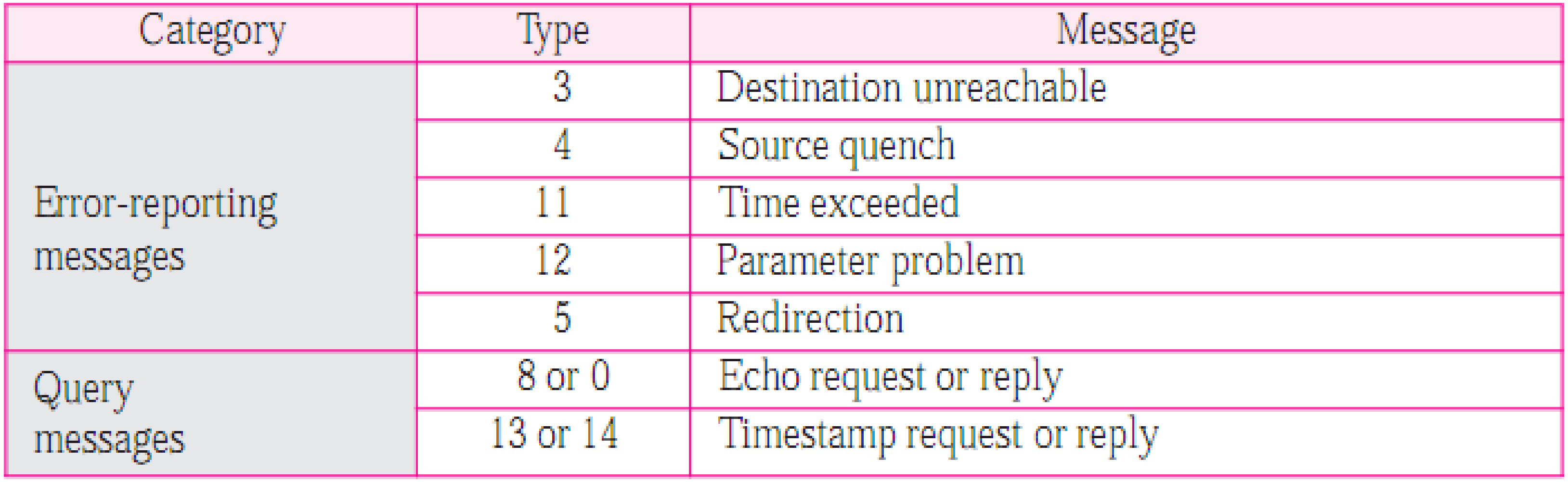
a) ICMP Message Types



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

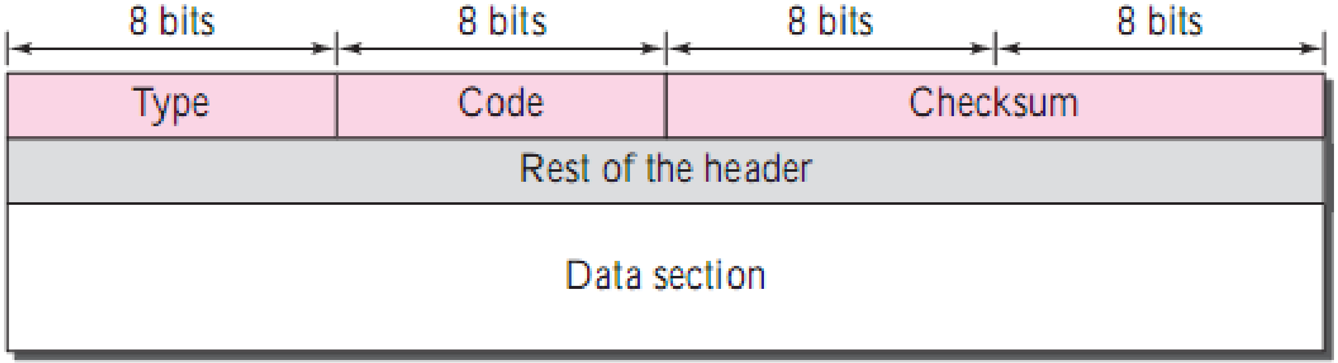
ICMP Messages

- ICMP Message Types



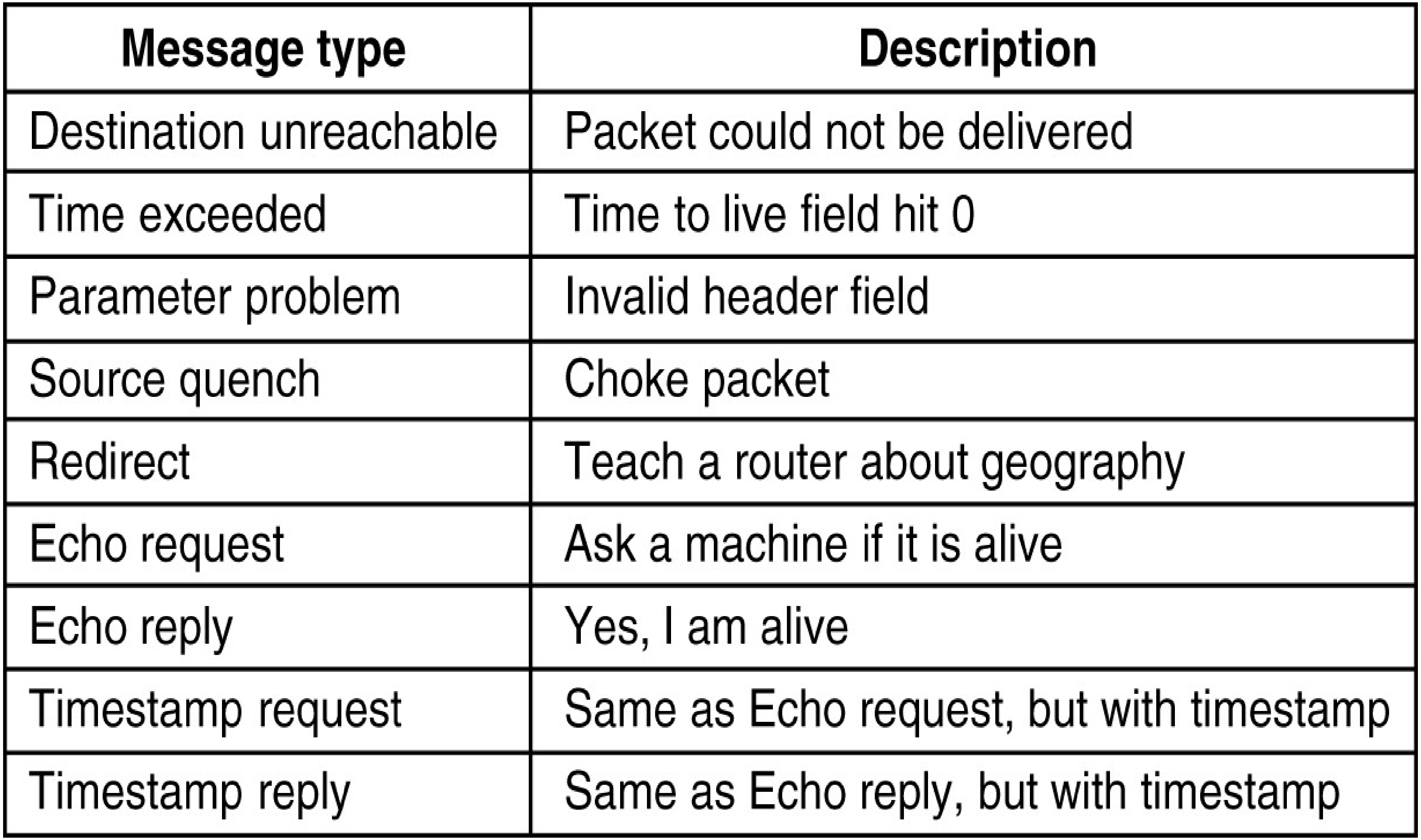
Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

- Message Format



8 bits	8 bits	8 bits	8 bits
Type	Code	Checksum	
Rest of the header			
Data section			

Internet Control Message Protocol

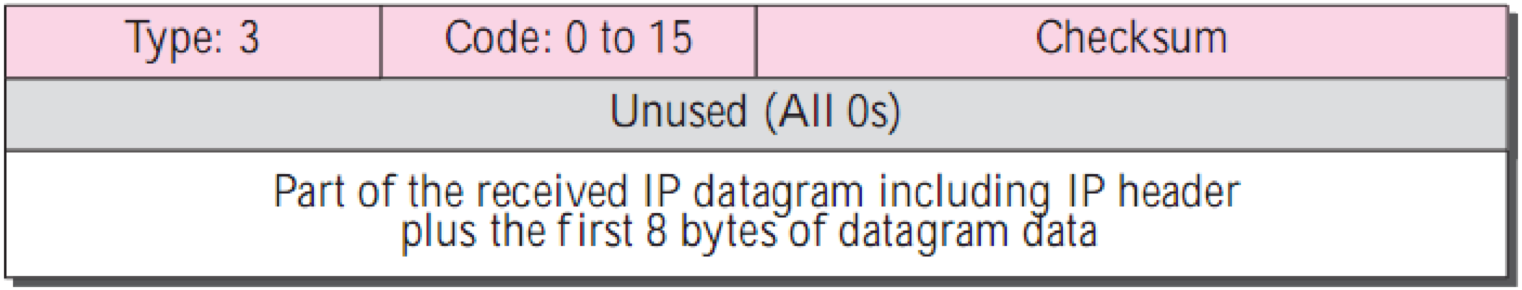


Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

The principal ICMP message types.

Destination Unreachable

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



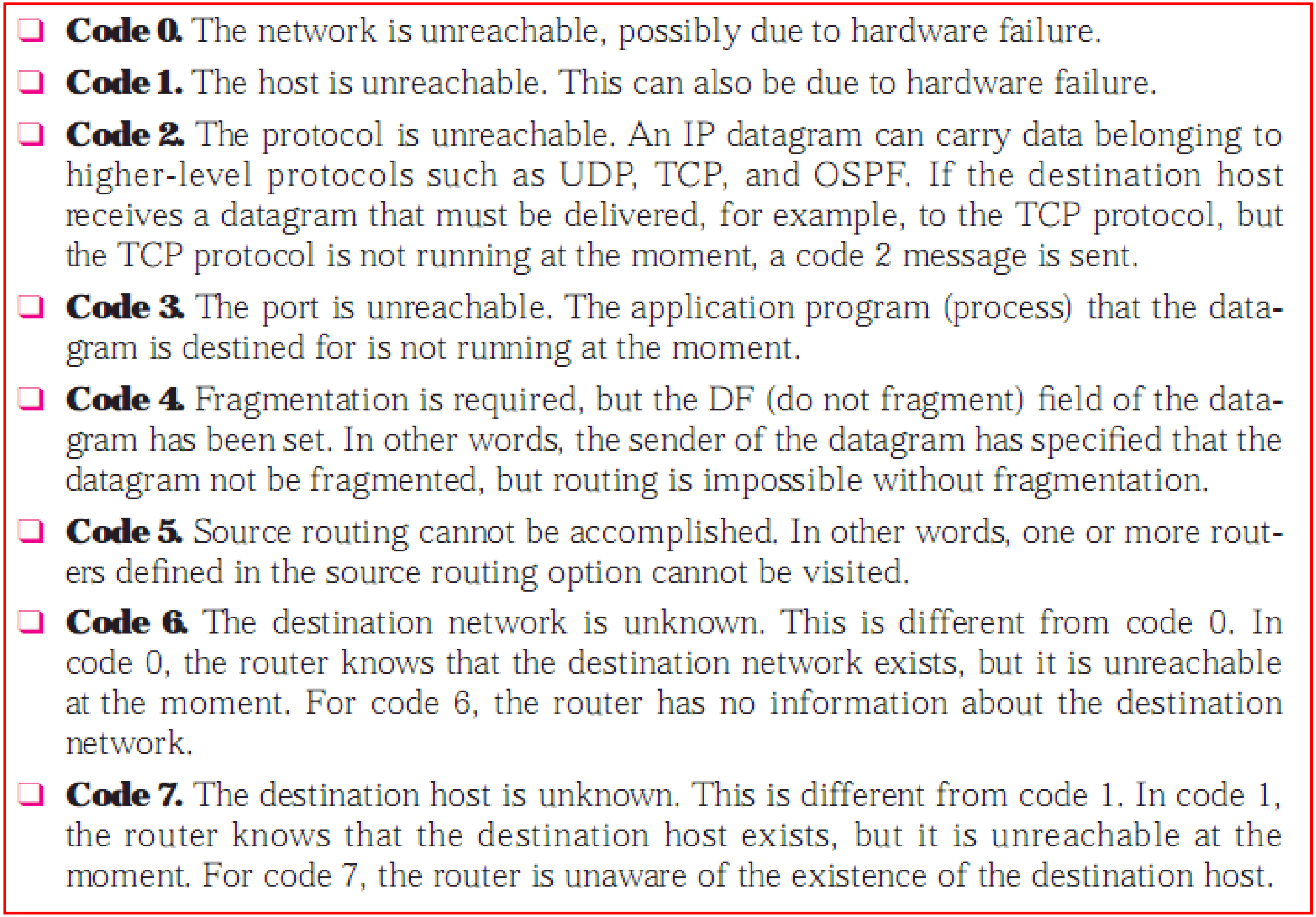
Type: 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

The code field for this type specifies the reason for discarding the datagram

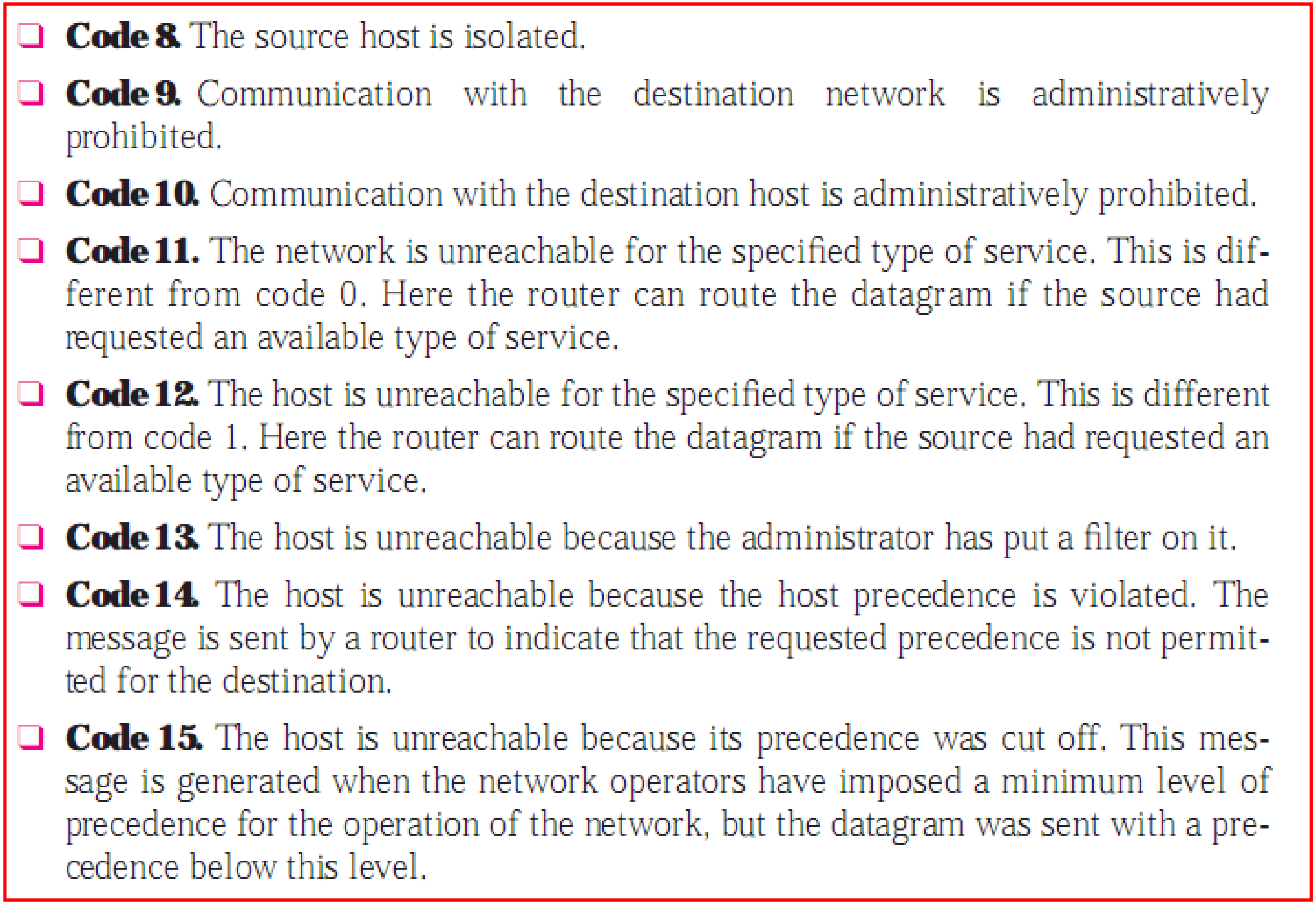
First 8 bytes of data provide information about the port numbers and sequence number

This information is needed so that the source can inform the protocols (TCP or UDP) about the error.

Destination Unreachable - Codes



- **Code 0.** The network is unreachable, possibly due to hardware failure.
- **Code 1.** The host is unreachable. This can also be due to hardware failure.
- **Code 2.** The protocol is unreachable. An IP datagram can carry data belonging to higher-level protocols such as UDP, TCP, and OSPF. If the destination host receives a datagram that must be delivered, for example, to the TCP protocol, but the TCP protocol is not running at the moment, a code 2 message is sent.
- **Code 3.** The port is unreachable. 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 of the datagram has been set. In other words, the sender of the datagram has specified that the datagram not be fragmented, but routing is impossible without fragmentation.
- **Code 5.** Source routing cannot be accomplished. In other words, one or more routers defined in the source routing option cannot be visited.
- **Code 6.** The destination network is unknown. This is different from code 0. In code 0, the router knows that the destination network exists, but it is unreachable at the moment. For code 6, the router has no information about the destination network.
- **Code 7.** The destination host is unknown. This is different from code 1. In code 1, the router knows that the destination host exists, but it is unreachable at the moment. For code 7, the router is unaware of the existence of the destination host.



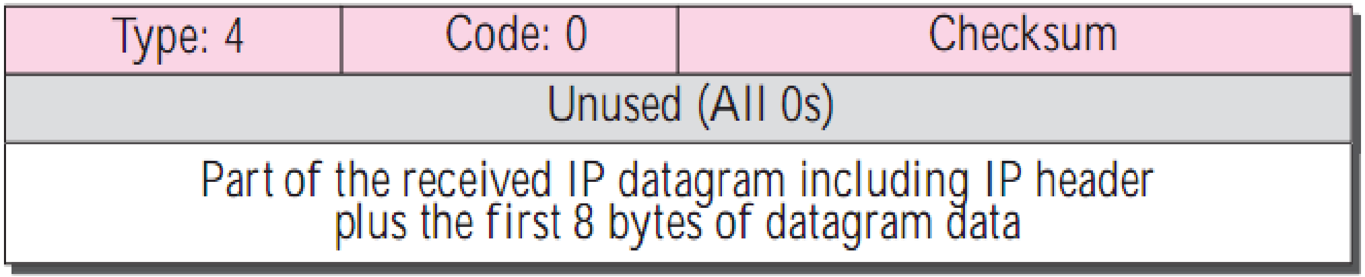
- **Code 8.** The source host is isolated.
- **Code 9.** Communication with the destination network is administratively prohibited.
- **Code 10.** Communication with the destination host is administratively prohibited.
- **Code 11.** The network is unreachable for the specified type of service. This is different from code 0. Here the router can route the datagram if the source had requested an available type of service.
- **Code 12.** The host is unreachable for the specified type of service. This is different from code 1. Here the router can route the datagram if the source had requested an available type of service.
- **Code 13.** The host is unreachable because the administrator has put a filter on it.
- **Code 14.** The host is unreachable because the host precedence is violated. The message is sent by a router to indicate that 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, but the datagram was sent with a precedence below this level.

Source Quench

- There is no flow-control or congestion-control mechanism in the IP protocol.
- The source-quench message in ICMP was designed to add a kind of flow control and congestion control to the IP.
- When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram.
- This message has two purposes.
  - First, it informs the source that the datagram has been discarded.
  - Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.

Source Quench

- Message Format:

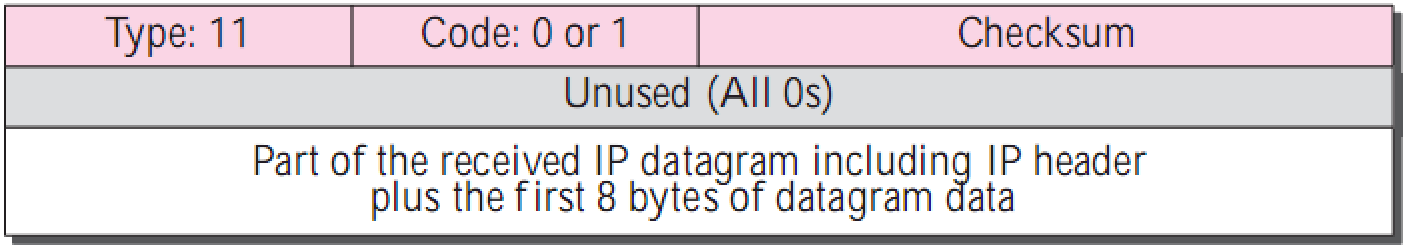


<table>
<tr><td>Type: 4</td><td>Code: 0</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="4">Unused (All 0s)</td></tr>
<tr><td colspan="4">Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data</td></tr>
</table>

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

Time Exceeded

- The time-exceeded message is generated in two cases:
  - 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.
  - 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 m



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		

Code 0 : the value of the TTL field is zero.

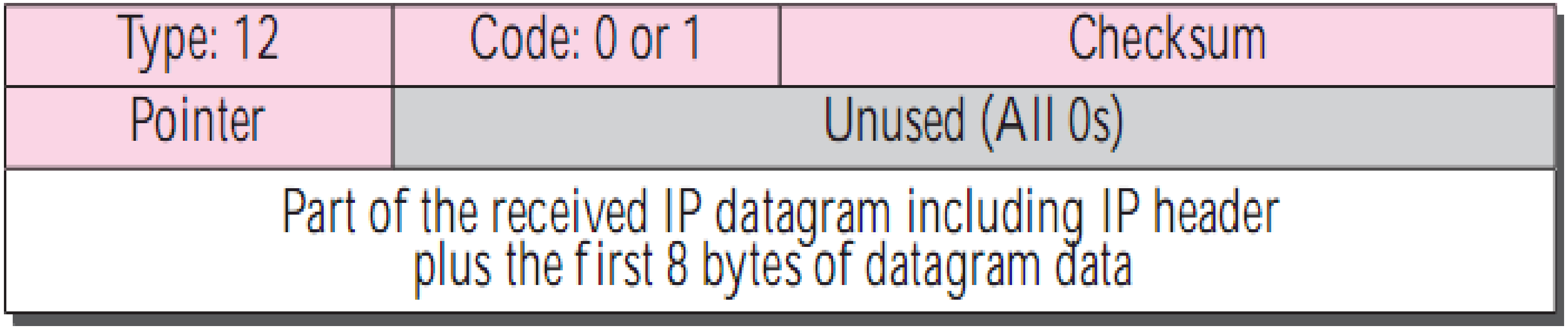
- Code 1 : not all of the fragments have arrived within a set time.

Parameter Problem

- If a router or the destination host discovers
  - an ambiguous value or
  - missing value in any field of the datagram,

it discards the datagram and sends a parameter-problem message back to the source.

Parameter Problem



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		

- The code field in this case specifies the reason for discarding the datagram:
  - Code 0: There is an error or ambiguity in one of the header fields. In this case, the value in the pointer field points to the byte with the problem.
    - For example, if the value is zero, then the first byte is not a valid field.
  - Code 1:The required part of an option is missing. In this case, the pointer is not used

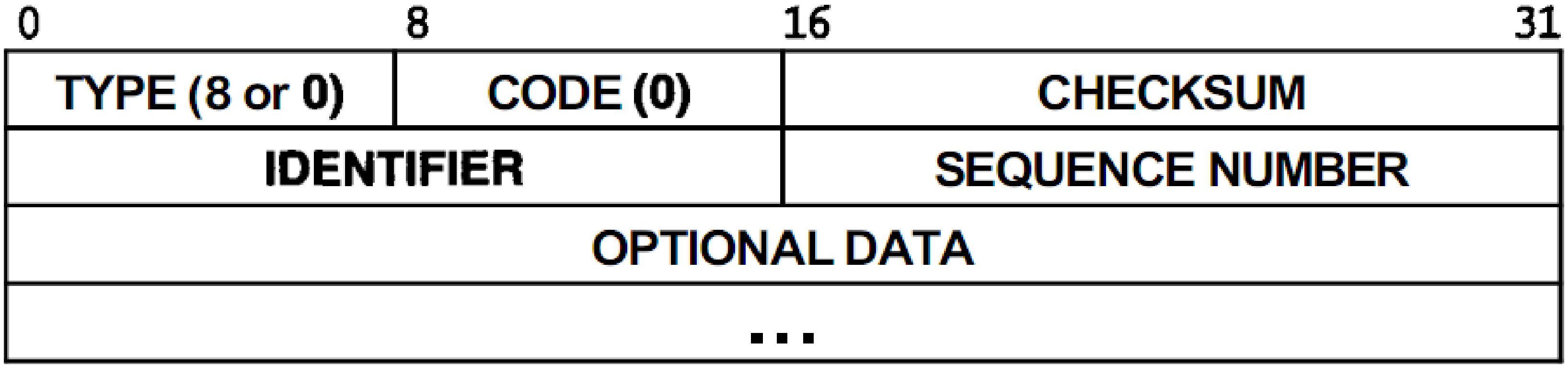
Query Messages

- ICMP can also diagnose some network problems.
  - accomplished through the query messages.
- A group of five different pairs of messages have been designed for this purpose, but three of these pairs are commonly used.
  1. Echo request and reply and
  2. Timestamp request and reply
  3. Subnet Mask request and reply

Echo Request & Reply Message

- Network managers and users utilize this pair of messages to identify network problems.
- The combination of echo-request and echo-reply messages determines whether two 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 that receives an echo-request message.
- Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol.
- Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command.

Echo Request & Reply Message



<table>
<tr><td>0</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td>TYPE (8 or 0)</td><td>CODE (0)</td><td colspan="2">CHECKSUM</td></tr>
<tr><td colspan="2">IDENTIFIER</td><td colspan="2">SEQUENCE NUMBER</td></tr>
<tr><td colspan="4">OPTIONAL DATA</td></tr>
<tr><td colspan="4">...</td></tr>
</table>

- OPTIONAL DATA is a variable length field that contains data to be returned to the sender. An echo reply always returns exactly the same data as was received in the request.

- IDENTIFIER and SEQUENCE NUMBER are used by the sender to match replies to requests.

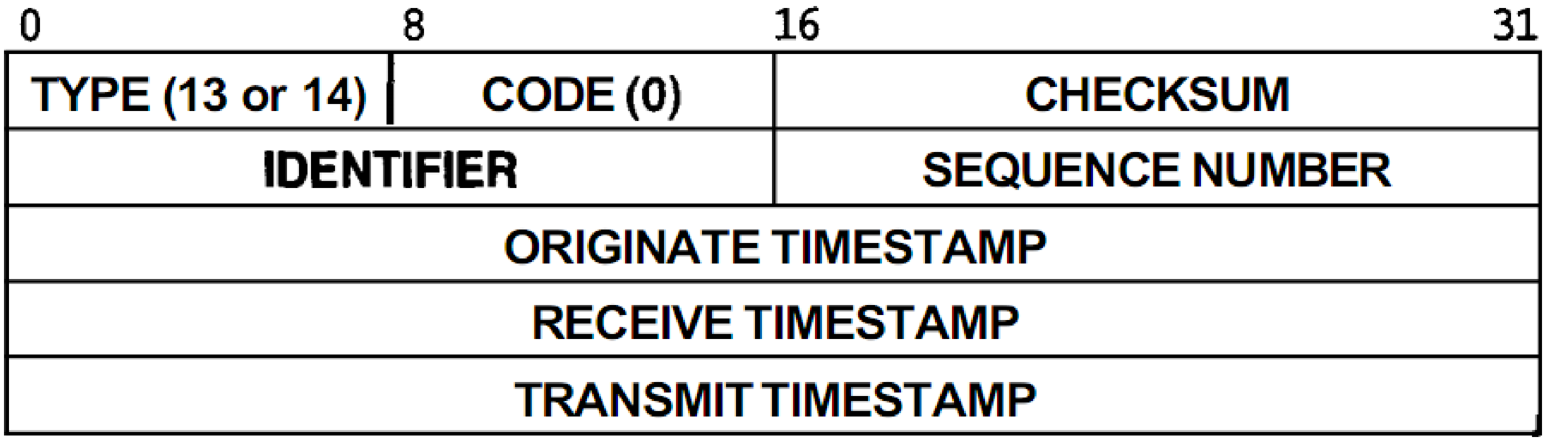
- TYPE field specifies whether the message is a request (8) or a reply (0)

2.2 Time Stamp Request- Reply Message

- A requesting machine sends an ICMP timestamp request message to another machine, asking the current value for the time of day on the second machine.

- The receiving machine returns a timestamp reply back to the machine making the request.

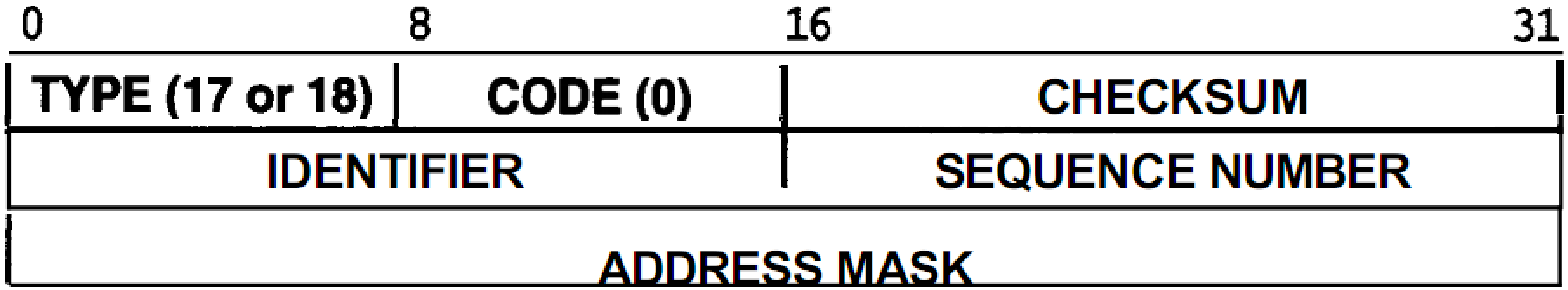
Time Stamp Request- Reply Message



0	8	16	31
TYPE (13 or 14)	CODE (0)	CHECKSUM	
IDENTIFIER		SEQUENCE NUMBER	
ORIGINATE TIMESTAMP			
RECEIVE TIMESTAMP			
TRANSMIT TIMESTAMP			

- The TYPE field identifies the message as a request (13) or a reply (14);
- IDENTIFIER and SEQUENCE NUMBER fields are used by the source to associate replies with requests.
- Remaining fields specify times
  - ORIGINATE TIMESTAMP field is filled in by the original sender just before the packet is transmitted,
  - RECEIVE TIMESTAMP field is filled immediately upon receipt of a request, and
  - TRANSMIT TIMESTAMP field is filled immediately before the reply is transmitted.

Subnet Mask Request- Reply Message



<table>
<tr><td>0</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td>TYPE (17 or 18)</td><td>CODE (0)</td><td colspan="2">CHECKSUM</td></tr>
<tr><td colspan="2">IDENTIFIER</td><td colspan="2">SEQUENCE NUMBER</td></tr>
<tr><td colspan="4">ADDRESS MASK</td></tr>
</table>

- The TYPE field in an address mask message specifies whether the message is a request (17) or a reply (18).

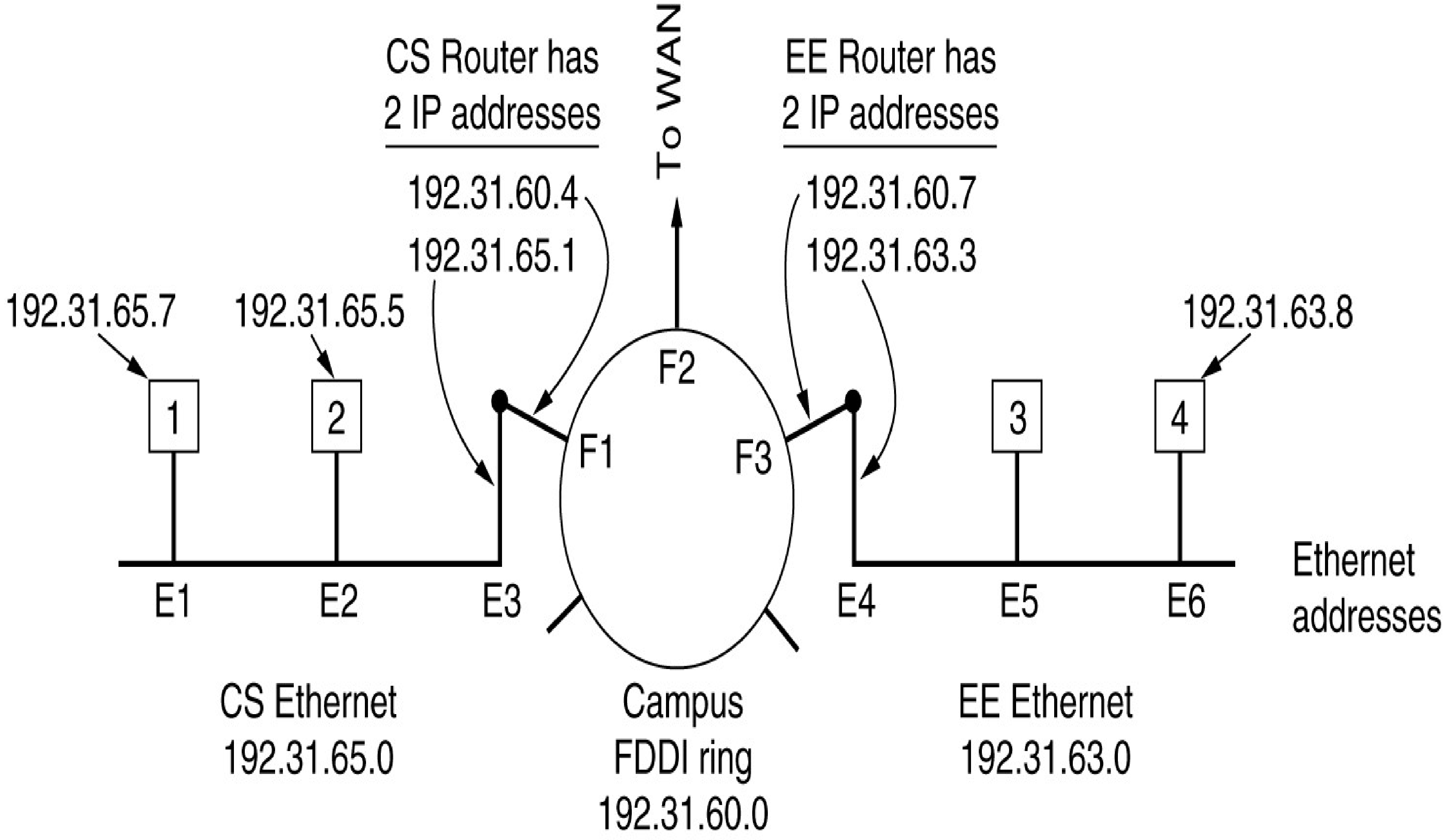
- A reply contains the network's subnet address mask in the ADDRESS MASK field.

- IDENTIFIER and SEQUENCE NUMBER fields allow a machine to associate replies with requests.

Internet Control Protocols

- ***ARP - The Address Resolution Protocol***
  - IP address alone is not enough for sending packets
  - because the data link layer hardware does not understand Internet addresses.
  - most hosts at companies and universities are attached to a LAN by an interface board that only understands LAN addresses.
  - For example, every Ethernet board comes equipped with a 48-bit Ethernet address. Eg: 14.04.05.18.01.25.
  - Manufacturers of Ethernet boards request a block of addresses from a central authority to ensure that no two boards have the same address
  - The boards send and receive frames based on 48-bit Ethernet addresses.
  - They know nothing at all about 32-bit IP addresses.

ARP - The Address Resolution Protocol



Three interconnected /24 networks: two Ethernets and an FDDI ring.

Internet Control Protocols

- how a user on host 1 sends a packet to a user on host 2.
  - Let us assume the sender knows the name of the intended receiver, possibly something like xyz@cs.uni.edu
  - The first step is to find the IP address for host 2, known as cs.uni.edu.
  - This lookup is performed by the Domain Name System (DNS) which returns the IP address for host 2 (192.31.65.5).
  - upper layer software on host 1 now builds a packet with 192.31.65.5 in the Destination address field and gives it to the IP software to transmit.
  - The IP software can look at the address and see that the destination is on its own network
  - but it needs some way to find the destination's Ethernet address

Internet Control Protocols

- One solution
  - to have a configuration file somewhere in the system that maps IP addresses onto Ethernet addresses.
  - While this solution is certainly possible, for organizations with thousands of machines, keeping all these files up to date is an error-prone, time-consuming job.
- Better solution
  - to output a broadcast packet onto the Ethernet asking: Who owns IP address 192.31.65.5?
  - The broadcast will arrive at every machine on Ethernet 192.31.65.0, and each one will check its IP address.
  - Host 2 alone will respond with its Ethernet address (E2).
  - The protocol used for asking this question and getting the reply is called **ARP (Address Resolution Protocol)**
  - Almost every machine on the Internet runs it.

Internet Control Protocols

Advantages

Simplicity-system manager does not have to do much except assign each machine an IP address and decide about subnet mask

Optimizations

- Arp cache-Once a machine has run ARP, it caches the result in case it needs to contact the same machine shortly.
- No need for a second broadcast
- Mostly second host will need to send back a reply ie it need the Ethernet address of first host
- ARP broadcast can be avoided by having host1 include its IP-to-Ethernet mapping in the ARP packet
- When the ARP broadcast arrives at host2,the pair (IP,EI)is entered into second host’s ARP cache for future use
- All machines on the Ethernet can enter this mapping into their ARP caches

Internet Control Protocols

- When mappings change
  - When Ethernet board breaks and is replaced with a new one, entries in the ARP cache should time out after a few minutes

Suppose host1 wants to send a packet to host4(192.31.63.8)

- Since destination is on a remote network send all such traffic to a default Ethernet address that handles all remote traffic here E3
- The packet routed to host4 should pass through router 192.31.60.7
- When it reaches the router, its ARP cache contains the Ethernet address of Host4(E6) and it is delivered

Internet Control Protocols

- ***RARP*** **- Reverse Address Resolution Protocol**
  - Given an Ethernet address, what is the corresponding IP address?
  - this problem occurs when a diskless workstation is booted.
  - Such a machine will normally get the binary image of its OS from a remote file server.
  - But how does it learn its IP address?
  - RARP allows a newly-booted workstation to broadcast its Ethernet address and say: My 48-bit Ethernet address is 14.04.05.18.01.25.
  - Does anyone out there know my IP address?
  - The RARP server sees this request, looks up the Ethernet address in its configuration files, and sends back the corresponding IP address.

Internet Control Protocols

- .
- Disadvantage of RARP
  - uses a destination address of all 1s (limited broadcasting) to reach the RARP server.
  - Such broadcasts are not forwarded by routers
  - So, a RARP server is needed on each network
  - To overcome this problem, **BOOTP** was invented

Internet Control Protocols

- **BOOTP - bootstrap protocol**
  - BOOTP uses UDP messages, which are forwarded over routers.
  - It also provides a diskless workstation with additional information, including
    - IP address of the file server holding the memory image,
    - IP address of the default router, and
    - subnet mask to use.

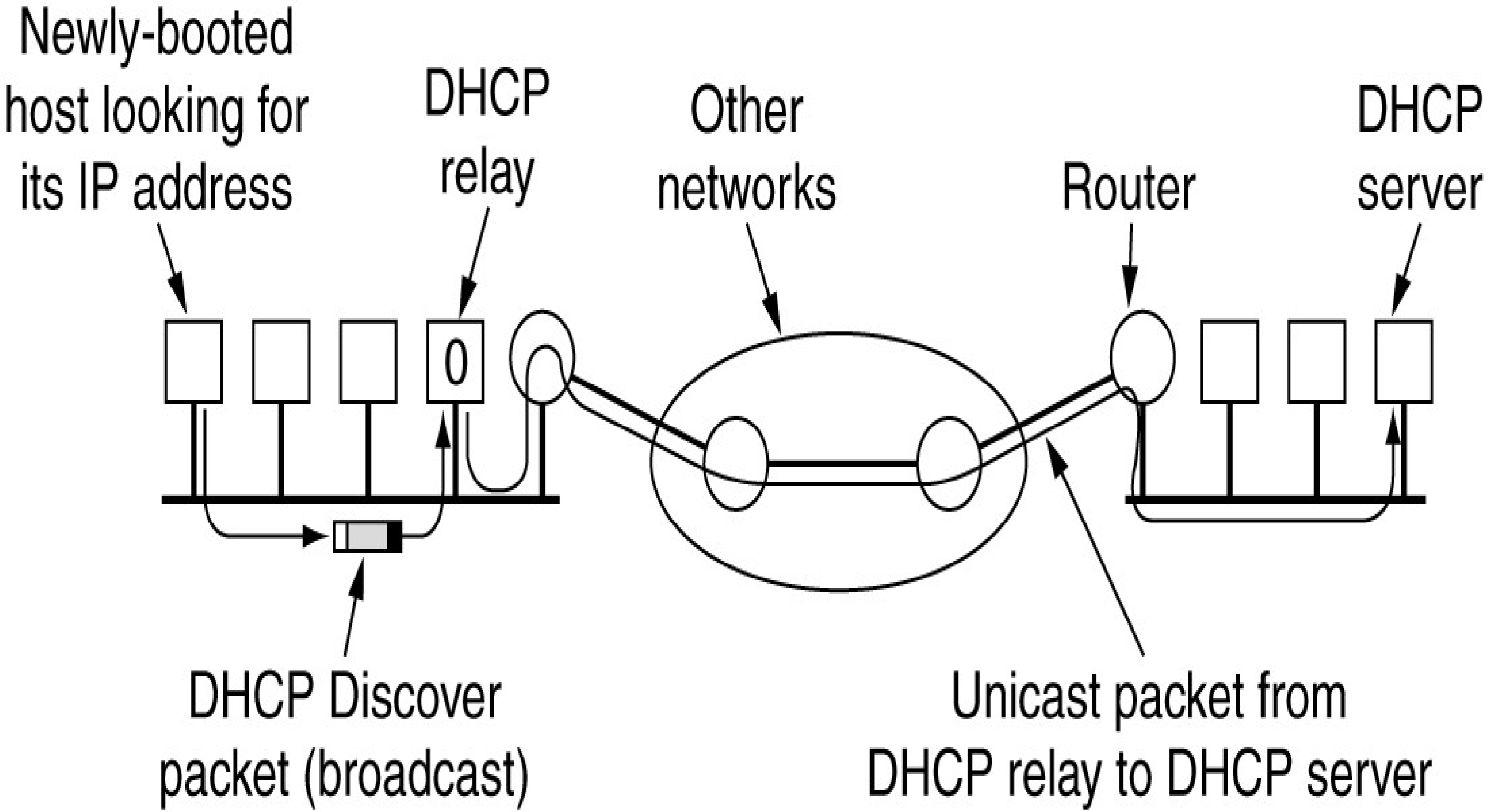
Internet Control Protocols

- Serious problem with BOOTP
  - requires manual configuration of tables mapping IP address to Ethernet address.
  - When a new host is added to a LAN, it cannot use BOOTP until an administrator has assigned it an IP address and entered its (Ethernet address, IP address) into the BOOTP configuration tables by hand.
  - To eliminate this error-prone step, BOOTP was extended and given a new name: **DHCP (Dynamic Host Configuration Protocol)**

Internet Control Protocols

- **DHCP - Dynamic Host Configuration Protocol**
  - DHCP allows both manual IP address assignment and automatic assignment.
  - In most systems, it has largely replaced RARP and BOOTP.
  - Like RARP and BOOTP, DHCP is based on the idea of a special server that assigns IP addresses to hosts asking for one.
  - This server need not be on the same LAN as the requesting host.
  - Since the DHCP server may not be reachable by broadcasting, a **DHCP relay agent** is needed on each LAN

Dynamic Host Configuration Protocol


Newly-booted host looking for its IP address
DHCP relay
0
Other networks
Router
DHCP server
DHCP Discover packet (broadcast)
Unicast packet from DHCP relay to DHCP server

Operation of DHCP.

Internet Control Protocols

- To find its IP address, a newly-booted machine broadcasts a DHCP DISCOVER packet.
- The DHCP relay agent on its LAN captures all DHCP broadcasts.
- When it finds a DHCP DISCOVER packet, it sends the packet as a unicast packet to the DHCP server, possibly on a distant network.
- The only piece of information the relay agent needs is the IP address of the DHCP server.

Internet Control Protocols

- Issue that arises with automatic assignment of IP addresses from a pool
  - how long an IP address should be allocated.
  - If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost.
  - After a period of time, many addresses may be lost.
  - To prevent that from happening, IP address assignment may be for a fixed period of time, a technique called **leasing**.
  - Just before the lease expires, the host must ask the DHCP for a renewal.
  - If it fails to make a request or the request is denied, the host may no longer use the IP address it was given earlier.

Internet Multicasting

- Ability to send to a large number of receivers simultaneously
- Eg:
  - updating replicated, distributed databases
  - transmitting stock quotes to multiple brokers and
  - handling digital conference telephone calls
- IP supports multicasting using class D addresses
- Each class D address identifies a group of hosts
- 28 bits are available for identifying groups, so over 250 million groups can exist at the same time.
- When a process sends a packet to a class D address, a best-efforts attempt is made to deliver it to all the members of the group addressed, but no guarantees are given
- some members may not get the packet

Internet Multicasting

- Two kinds of group addresses are supported:
  - permanent addresses and
  - temporary addresses .
- permanent group is always there and does not have to be set up.
- Each permanent group has a permanent group address
- Some examples of permanent group addresses are:
  - 224.0.0.1 All systems on a LAN
  - 224.0.0.2 All routers on a LAN
  - 224.0.0.5 All OSPF routers on a LAN
  - 224.0.0.6 All designated OSPF routers on a LAN

Internet Multicasting

- Temporary groups must be created before they can be used.
- A process can ask its host to join a specific group.
- It can also ask its host to leave the group.
- When the last process on a host leaves a group, that group is no longer present on the host.
- Each host keeps track of which groups its processes currently belong to.
- Multicasting is implemented by special multicast routers
- About once a minute, each multicast router sends a hardware (i.e., data link layer) multicast to the hosts on its LAN (address 224.0.0.1) asking them to report back on the groups their processes currently belong to.
- Each host sends back responses for all the class D addresses it is interested in.

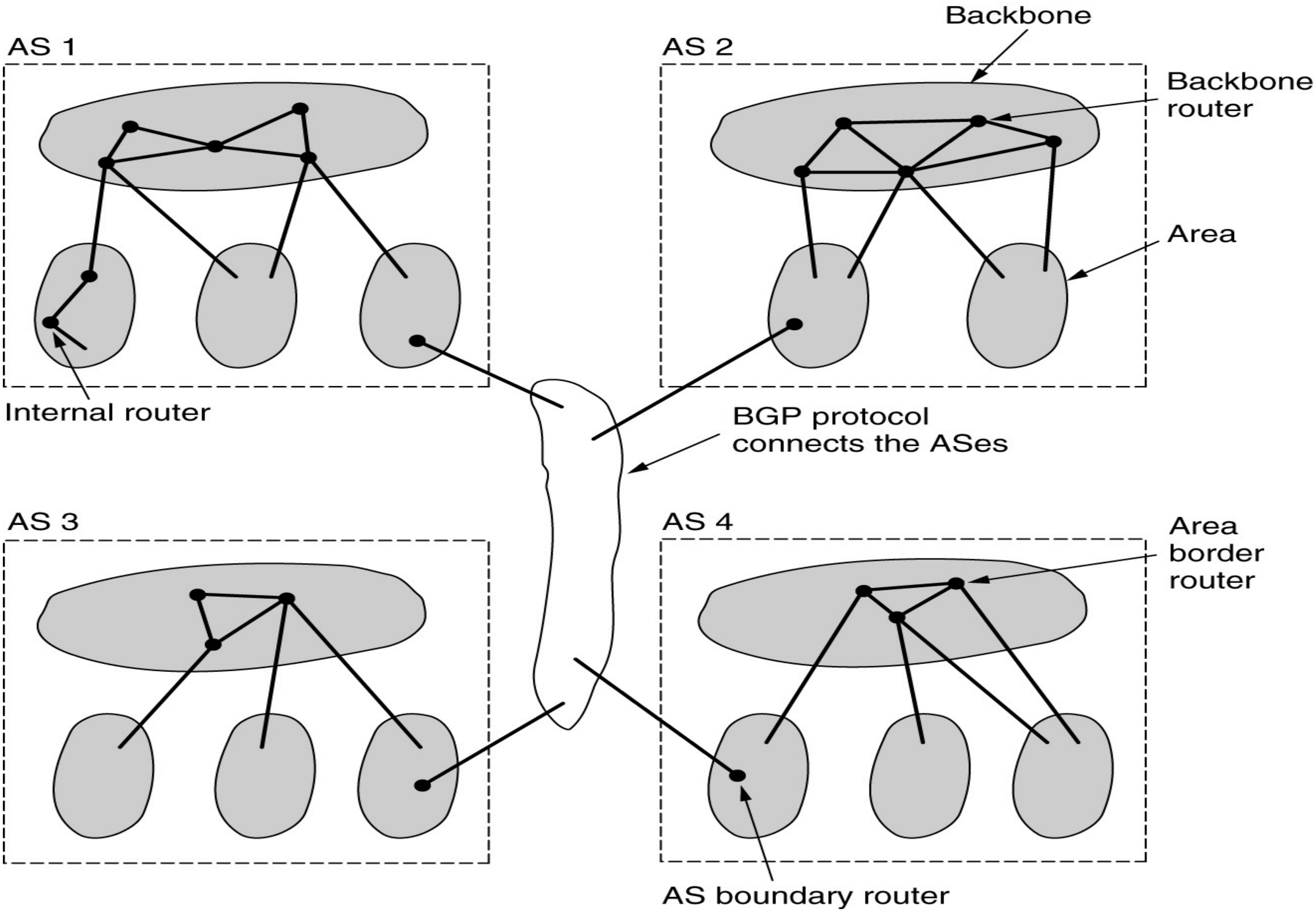
Internet Multicasting

- These query and response packets use a protocol called **IGMP (Internet Group Management Protocol),**
  - which is vaguely analogous to ICMP.
- It has only two kinds of packets:
  - query and response
    - each with a simple, fixed format containing some control information in the first word of the payload field and a class D address in the second word.
- Multicast routing is done using spanning trees.
  - **spanning tree** of a connected, undirected graph, G is a tree that includes all of the vertices and some of the edges of *G* such that it becomes a tree, i.e, it contains no more cycles.

Internet Multicasting

- Each multicast router exchanges information with its neighbors, using a modified distance vector protocol
- in order for each one to construct a spanning tree per group covering all group members.
- Various optimizations are used to prune the tree to eliminate routers and networks not interested in particular groups.
- The protocol makes heavy use of tunneling to avoid bothering nodes not in a spanning tree.

Exterior Gateway Routing Protocol - BGP



Exterior Gateway Routing Protocol - BGP

- For routing between ASes, **BGP (Border Gateway Protocol)** is used
- Exterior gateway protocol routers have to worry about politics
- For example, a corporate AS might want the ability to send packets to any Internet site and receive packets from any Internet site.
- However, it might be unwilling to carry transit packets originating in a foreign AS and ending in a different foreign AS, even if its own AS was on the shortest path between the two foreign ASes ("That's their problem, not ours").
- Telephone companies, for example, might be happy to act as a carrier for their customers, but not for others.

Exterior Gateway Routing Protocol - BGP

- Exterior gateway protocols in general, and BGP in particular, have been designed to allow many kinds of routing policies to be enforced in the interAS traffic
- Typical policies involve political, security, or economic considerations.
- A few examples of routing constraints are
  - ✓ No transit traffic through certain ASes
  - ✓ Traffic starting or ending at IBM should not transit Microsoft
  - ✓ Never put Iraq on a route starting at the Pentagon
- From the point of view of a BGP router, the world consists of ASes and the lines connecting them

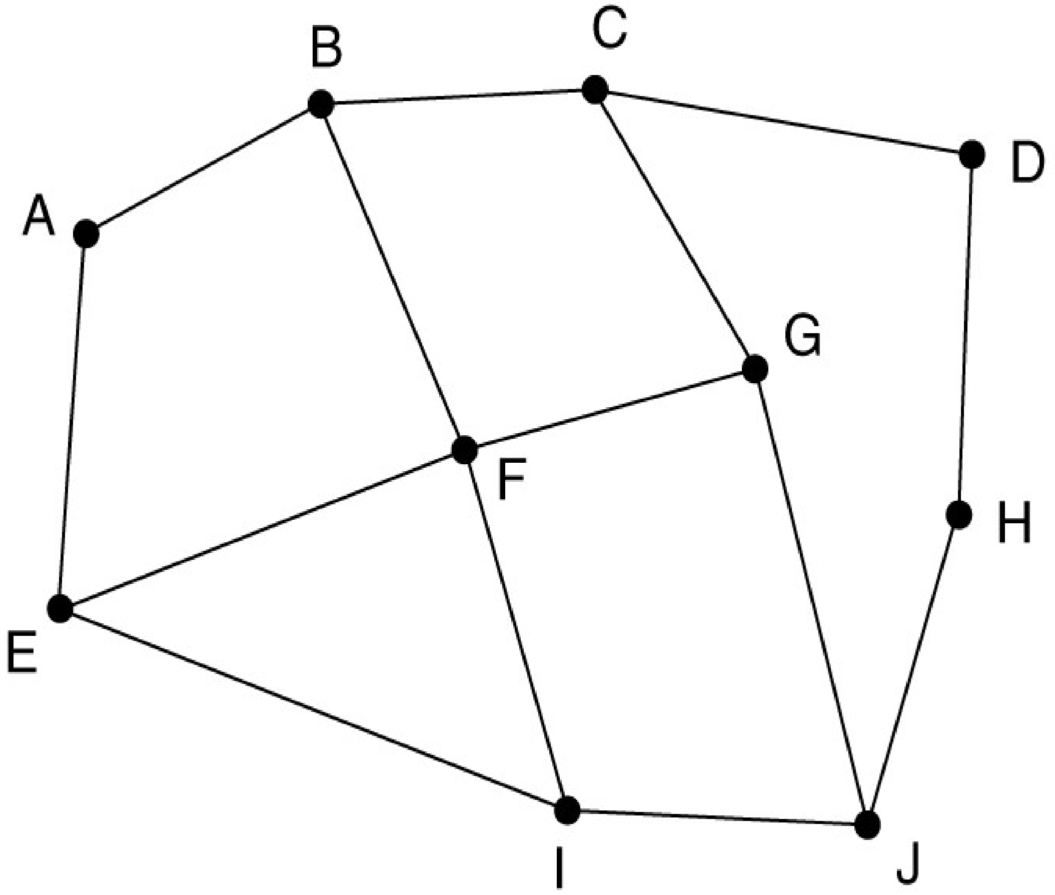
Exterior Gateway Routing Protocol - BGP

- Given BGP's special interest in transit traffic, networks are grouped into one of 3 categories.
- Category 1: **stub networks**
  - which have only one connection to the BGP graph.
  - cannot be used for transit traffic because there is no one on the other side.
- Category 2: **multiconnected networks**
  - could be used for transit traffic, except that they refuse.
- Category 3: **transit networks**
  - such as backbones, which are willing to handle third-party packets
  - possibly with some restrictions, and usually for pay

Exterior Gateway Routing Protocol - BGP

- Pairs of BGP routers communicate with each other by establishing TCP connections.
- Operating this way provides reliable communication and hides all the details of the network being passed through.
- BGP is fundamentally a distance vector protocol
- Instead of maintaining just the cost to each destination, each BGP router keeps track of the path used.
- Similarly, instead of periodically giving each neighbor its estimated cost to each possible destination, each BGP router tells its neighbors the exact path it is using
- Eg is illustrated in the next slide figure

BGP – The Exterior Gateway Routing Protocol



(a)

Information F receives
from its neighbors about D

From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"

(b)

(a) A set of BGP routers. (b) Information sent to F.

Exterior Gateway Routing Protocol - BGP

- consider F's routing table.
- Suppose that it uses the path FGCD to get to D.
- When the neighbors give it routing information, they provide their complete paths
- After all the paths come in from the neighbors, F examines them to see which is the best.
- It quickly discards the paths from I and E, since these paths pass through F itself.
- The choice is then between using B and G.
- Every BGP router contains a module that examines routes to a given destination and scores them, returning a number for the "distance" to that destination for each route.

Exterior Gateway Routing Protocol - BGP

- Any route violating a policy constraint automatically gets a score of infinity.
- The router then adopts the route with the shortest distance.
- The scoring function is not part of the BGP protocol and can be any function the system managers want.
- BGP easily solves the count-to-infinity problem
- For example, suppose G crashes or the line FG goes down.
- F then receives routes from its three remaining neighbors. These routes are BCD, IFGCD, and EFGCD.
- It can immediately see that the two latter routes are pointless, since they pass through F itself, so it chooses FBCD as its new route.

IPv6

Major goals were:

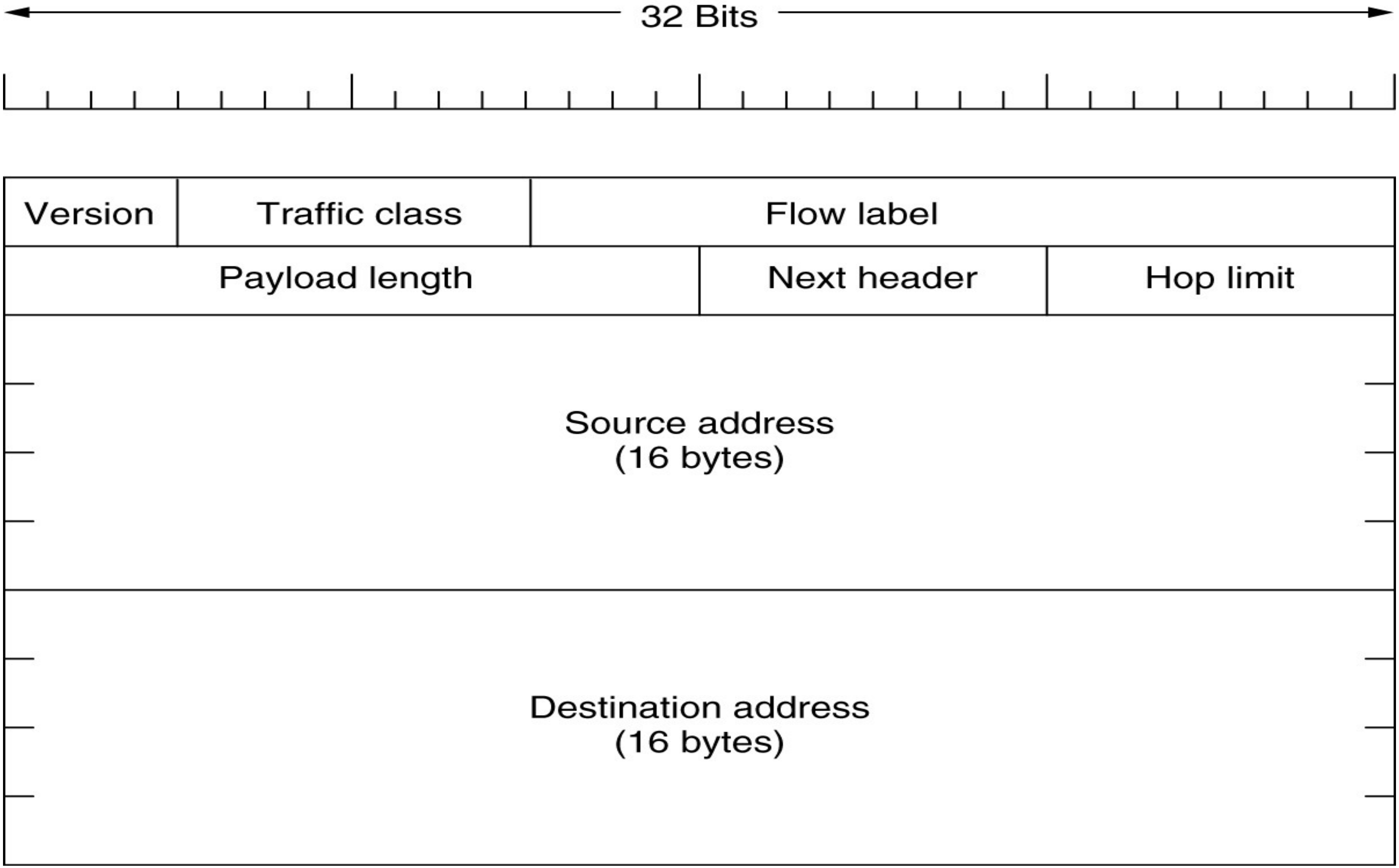
1. Support billions of hosts, even with inefficient address space allocation.
2. Reduce the size of the routing tables.
3. Simplify the protocol, to allow routers to process packets faster.
4. Provide better security (authentication and privacy) than current IP.
5. Pay more attention to type of service, particularly for real- time data.
6. Aid multicasting by allowing scopes to be specified.
7. Make it possible for a host to roam without changing its address.
8. Allow the protocol to evolve in the future.
9. Permit the old and new protocols to coexist for years.

IPv6

- IPv6 represents a big advance is in security.
  - Authentication and privacy are key features of new IP.
  - These were later added to IPv4
- more attention has been paid to quality of service
  - with the growth of multimedia on the Internet, the sense of urgency is greater

- Main IPv6 Header is shown in the next slide
  - Version field is always 6 for IPv6 (4 for IPv4)
    - During the transition period from IPv4, router will be able to examine this field to tell what kind of packet they have

The Main IPv6 Header



32 Bits

Version

Traffic class

Flow label

Payload length

Next header

Hop limit

Source address
(16 bytes)

Destination address
(16 bytes)

The IPv6 fixed header (required).

IPv6

- Traffic class field
  - used to distinguish between packets with different real-time delivery requirements.
  - A field designed for this purpose has been in IP since the beginning, but it has been only periodically implemented by routers.
  - Experiments are now underway to determine how best it can be used for multimedia delivery

- Flow label field
  - also still experimental
  - but will be used to allow a source and destination to set up a pseudo-connection with particular properties and requirements.

IPv6

- Payload length field
  - tells how many bytes follow the 40-byte main header
  - The name was changed from the IPv4 Total length field because the meaning was changed slightly:
    - the 40 header bytes are no longer counted as part of the length

IPv6

- Next header field
  - there can be additional (optional) extension headers.
  - This field tells which of the (currently) six extension headers follow this one.
  - If this header is the last IP header, the Next header field tells which transport protocol handler (e.g., TCP, UDP) to pass the packet to.
- Hop limit field
  - used to keep packets from living forever.
  - same as the Time to live field in IPv4, namely, a field that is decremented on each hop.
  - In theory, in IPv4 it was a time in seconds, but no router used it that way
  - so the name was changed to reflect the way it is actually used

IPv6

- Source address and Destination address fields
  - 16-byte addresses
  - They are written as eight groups of four hexadecimal digits with colons between the groups

    8000:0000:0000:0000:0123:4567:89AB:CDEF

IPv6

- Compare the IPv4 header with the IPv6 header
  - IHL field is gone because the IPv6 header has a fixed length.
  - Protocol field was taken out because the Next header field tells what follows the last IP header (e.g., a UDP or TCP segment).
  - All the fields relating to fragmentation were removed because IPv6 takes a different approach to fragmentation
    - hosts are expected to dynamically determine the datagram size to use.
    - router that is unable to forward it sends back an error message
    - This message tells the host to break up all future packets to that destination
  - Checksum field is gone because calculating it greatly reduces performance (data link layer and transport layers normally have their own checksums)