Network Technologies (TCP/IP Suite)

Umar Kalim
Dept. of Communication Systems Engineering

umar.kalim@niit.edu.pk
http://www.niit.edu.pk/~umarkalim

06/04/2007

ARP

Logical vs Physical addresses

- Internetwork addresses
  - Jurisdiction is universal
  - IP addresses
    - All networks understand the addressing scheme
  - Implemented in software
- Physical addresses
  - Jurisdiction is local
  - Implemented in hardware
  - Depends on the technology used at the physical layer (and hence the protocols at MAC layer)

A packet using one logical addressing scheme may pass through networks with different physical layer technologies

---

Thus we need to consider two different and independent addressing schemes; logical and physical

Problem

- Whenever a host needs to send a message to another host, it has the IP address.
- However the IP datagram must be encapsulated in a frame (by the MAC layer) so that it may be delivered over the physical layer
- Hence the need for the physical address
- The only way to get the physical address is to have a mapping scheme

Static mapping

Create a table that associates a logical address with a physical address

Static mapping

- Assumptions
  - Each machine knows the IP of the destination machine
  - In case the machine address is not known, it can be looked up in the table

Drawbacks of static mapping

- A machine could change its NIC
  - Hence a new physical address
- In some physical & data link layer protocols, the machine addresses changes whenever a machine is turned on
- A mobile computer can move from one network to another
  - Hence a change in the physical address (depending upon the underline protocols)

Solution

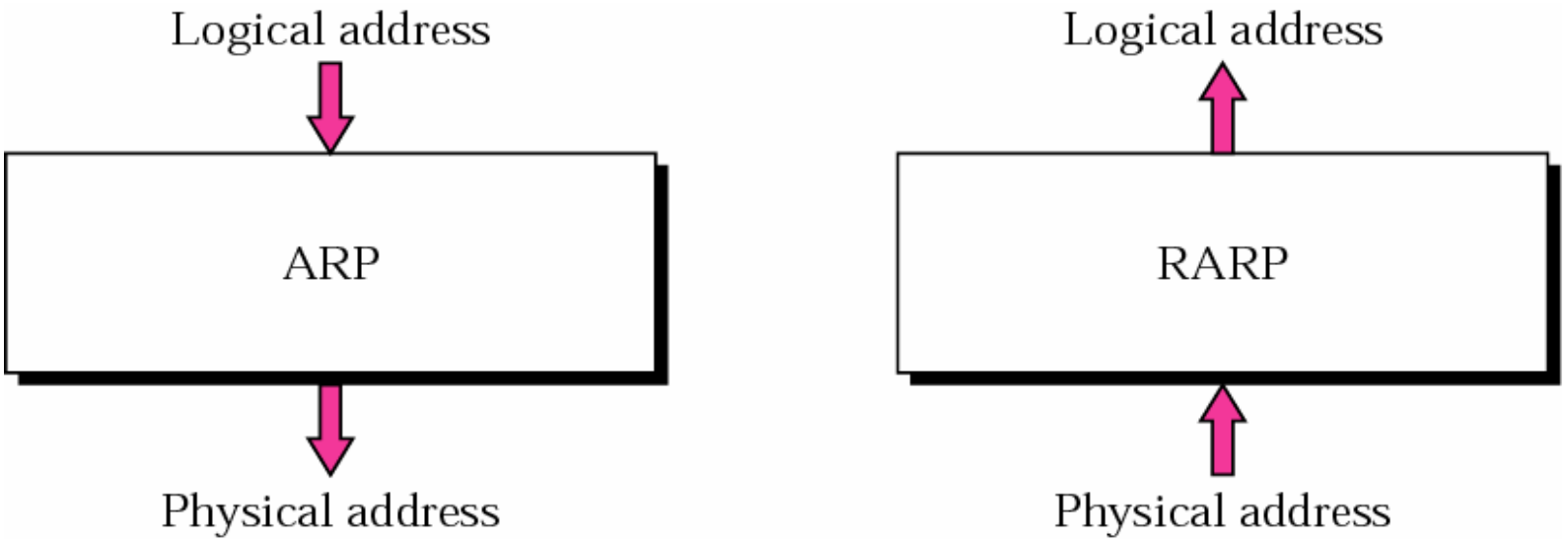
The static mapping table must be updated periodically or whenever the need arises

Dynamic mapping

Each time the machine knows one of the two addresses (physical or logical) it can obtain the other

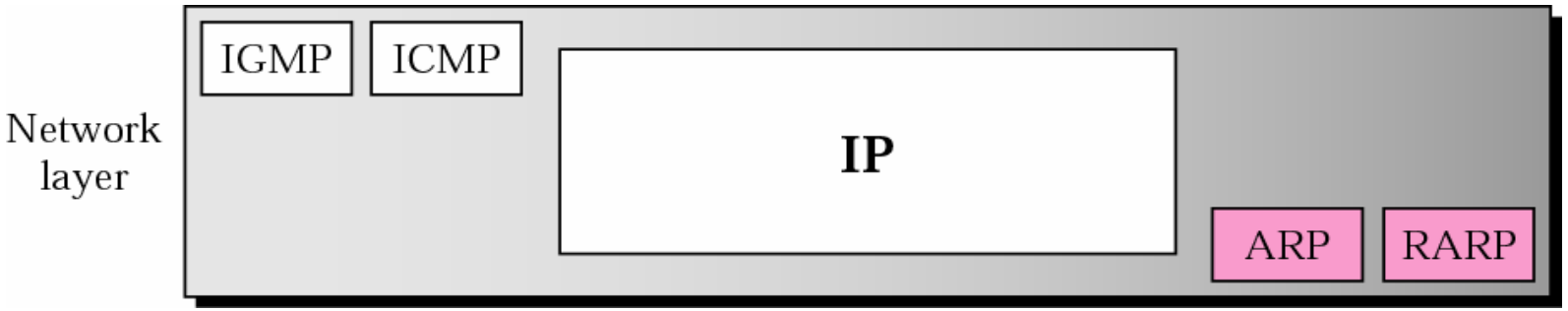
ARP & RARP

- Protocols defined for the dynamic mapping of logical and physical addresses



ARP & RARP

- ARP: Address Resolution Protocol
- RARP: Reverse Address Resolution Protocol
- Use unicast and broadcast physical addresses
- Position of ARP & RARP in the TCP/IP stack



ARP

- Instead of maintaining a static table, we can obtain the physical address at runtime
  - This is where ARP comes in
- ARP associates an IP address with a physical address
- On a typical network, each interface is identified by a physical address

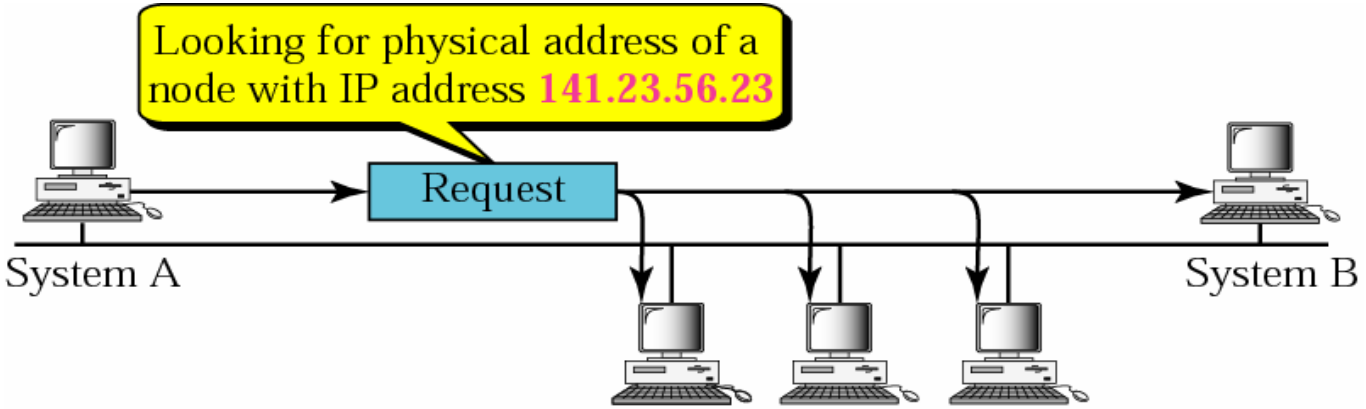
ARP

- Anytime a host needs to find the physical address, it send an ARP query
- The datagram contains the IP and the physical address of the sender as well as the IP address of the intended recipient
- Since the sender does not knows the destinations physical address, the datagram is broadcasted over the network

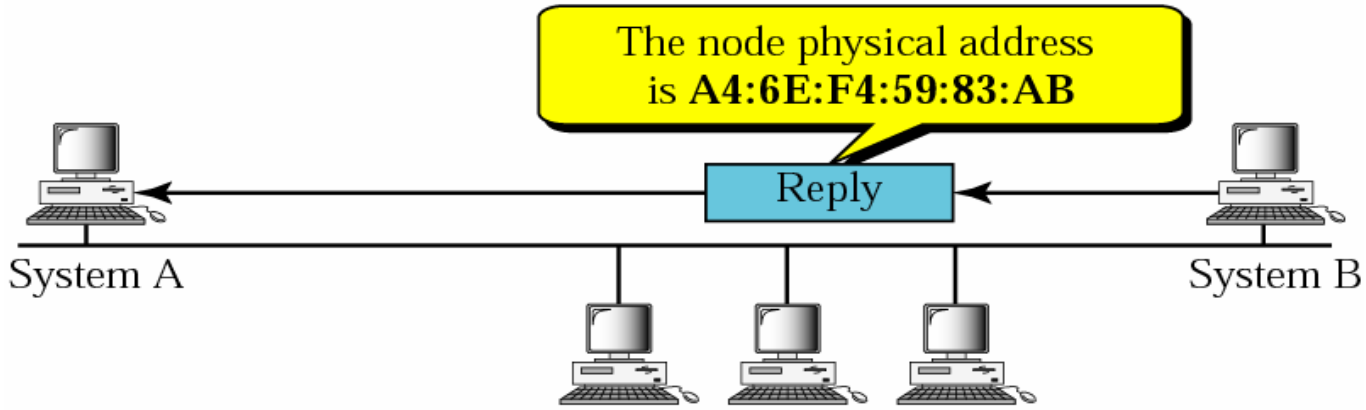
ARP

- Every host receives the query
- However only the intended recipient finds its IP address in the query message and responds
- This response is sent as a unicast

ARP

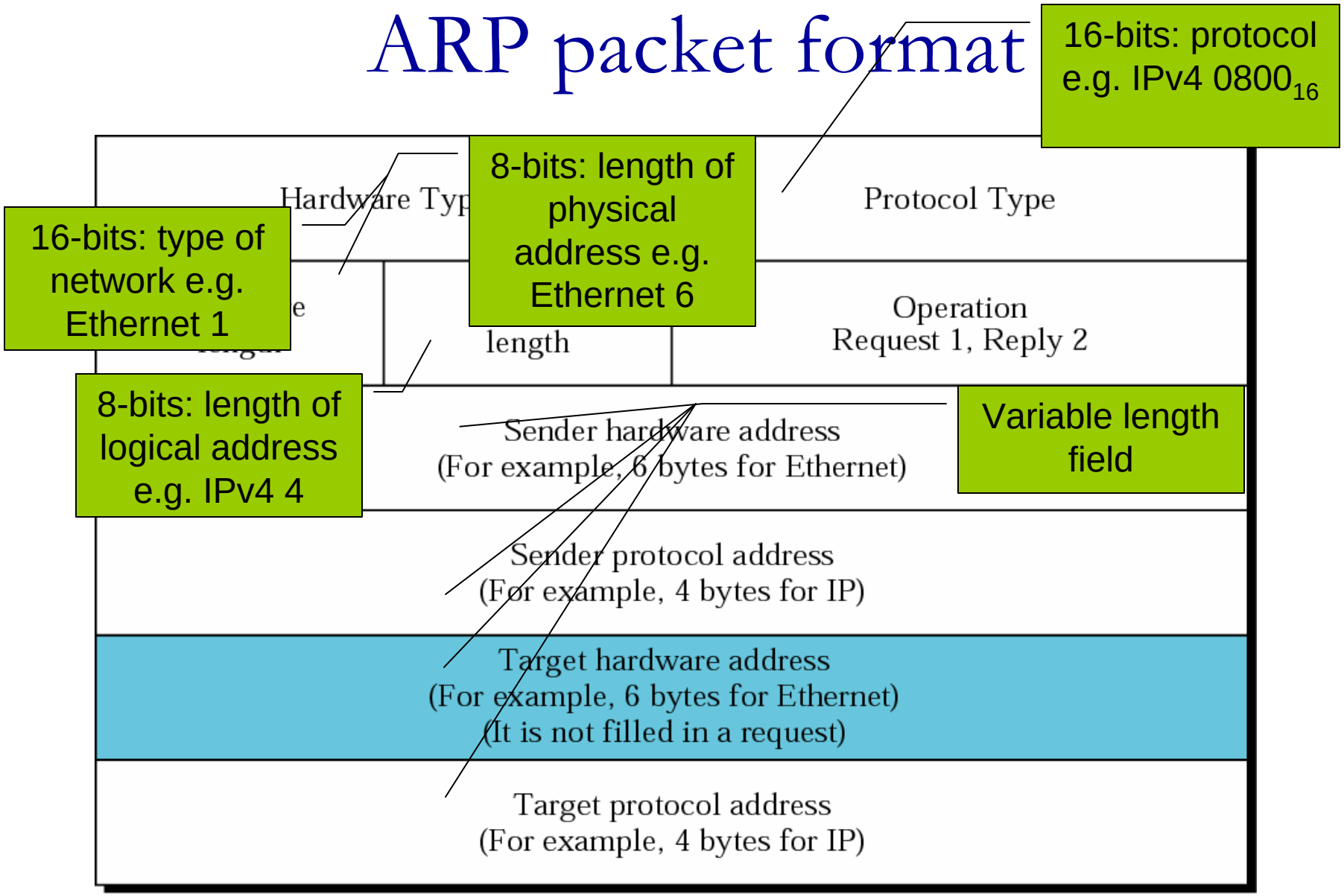


a. ARP request is broadcast



b. ARP reply is unicast

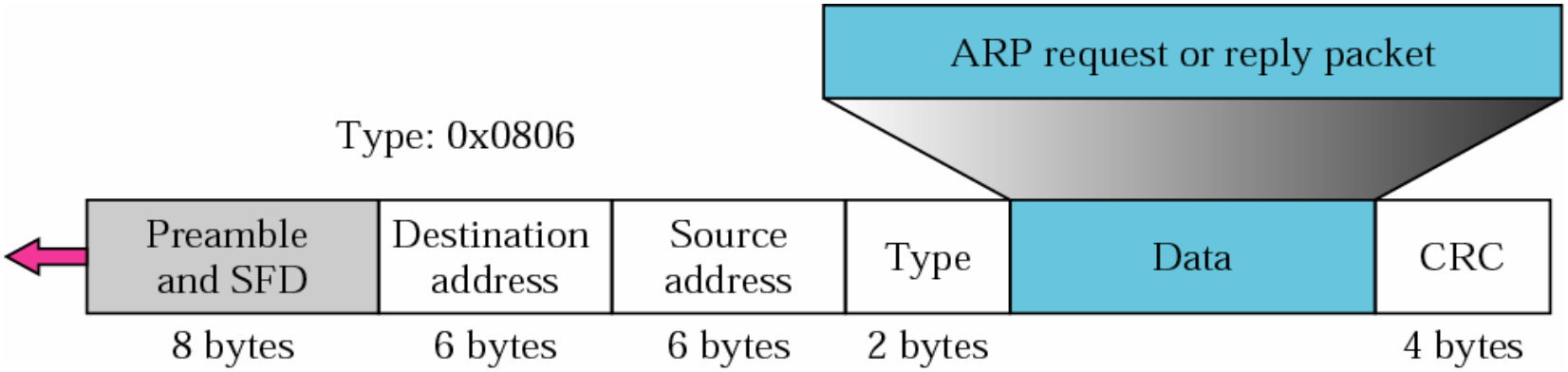
ARP packet format



Encapsulation

- ARP packet is encapsulated into a data-link frame

- Ethernet frame



Steps

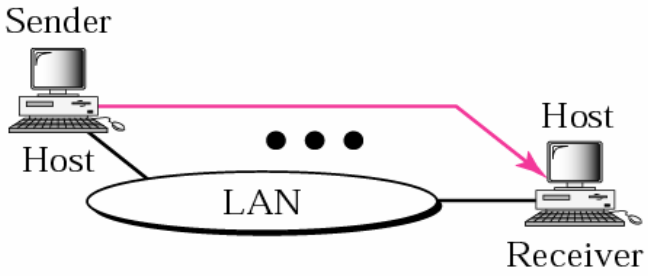
1. Sender knows the IP of the destination
2. IP asks ARP to create a request
3. Message is passed to the data-link layer and after encapsulation, the frame is transmitted
4. Every host receives the frame and pass it to ARP as the "type" field has the ARP code. All machines drop the packet, since the IP of the intended recipient do not match with their IP

Steps …

5. The host then replies with another ARP message (response) that contains the physical address. This response is transmitted as a unicast message.
6. The sender receives the reply
7. The sender then compiles and transmits the required datagrams using the physical address

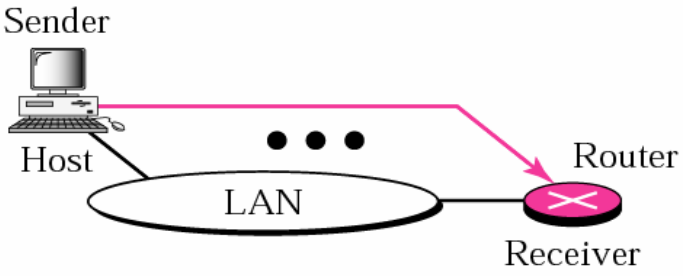
Four cases

Target IP address:
Destination address in the IP datagram



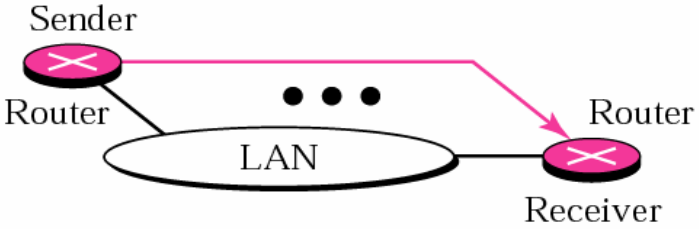
Case 1. A host has a packet to send to another host on the same network.

Target IP address:
IP address of a router



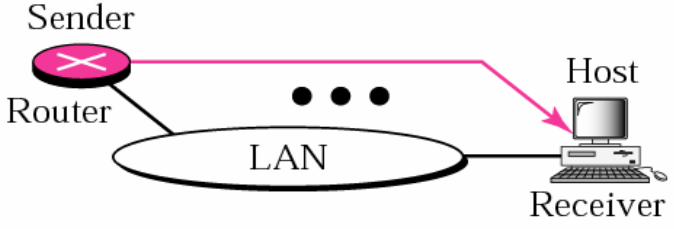
Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.

Target IP address:
IP address of the appropriate router found in the routing table

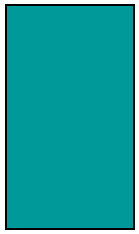


Case 3. A router receives a packet to be sent to a host on another network.
It must first be delivered to the appropriate router.

Target IP address:
Destination address in the IP datagram



Case 4. A router receives a packet to be sent to a host on the same network.



EXAMPLE 1

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 (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

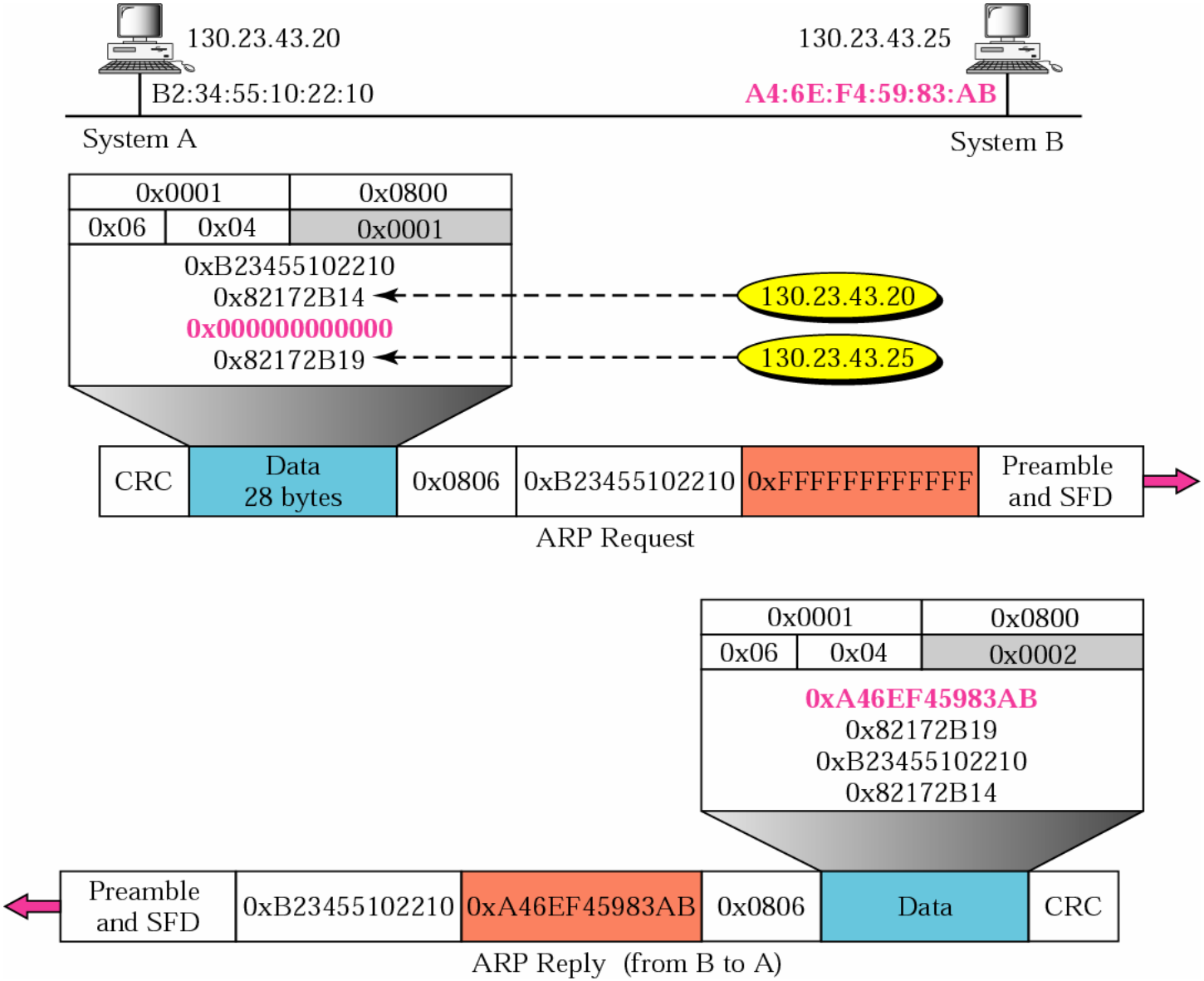
See Next Slide

EXAMPLE 1 (CONTINUED)

Solution

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. For information on binary or hexadecimal notation see Appendix B.

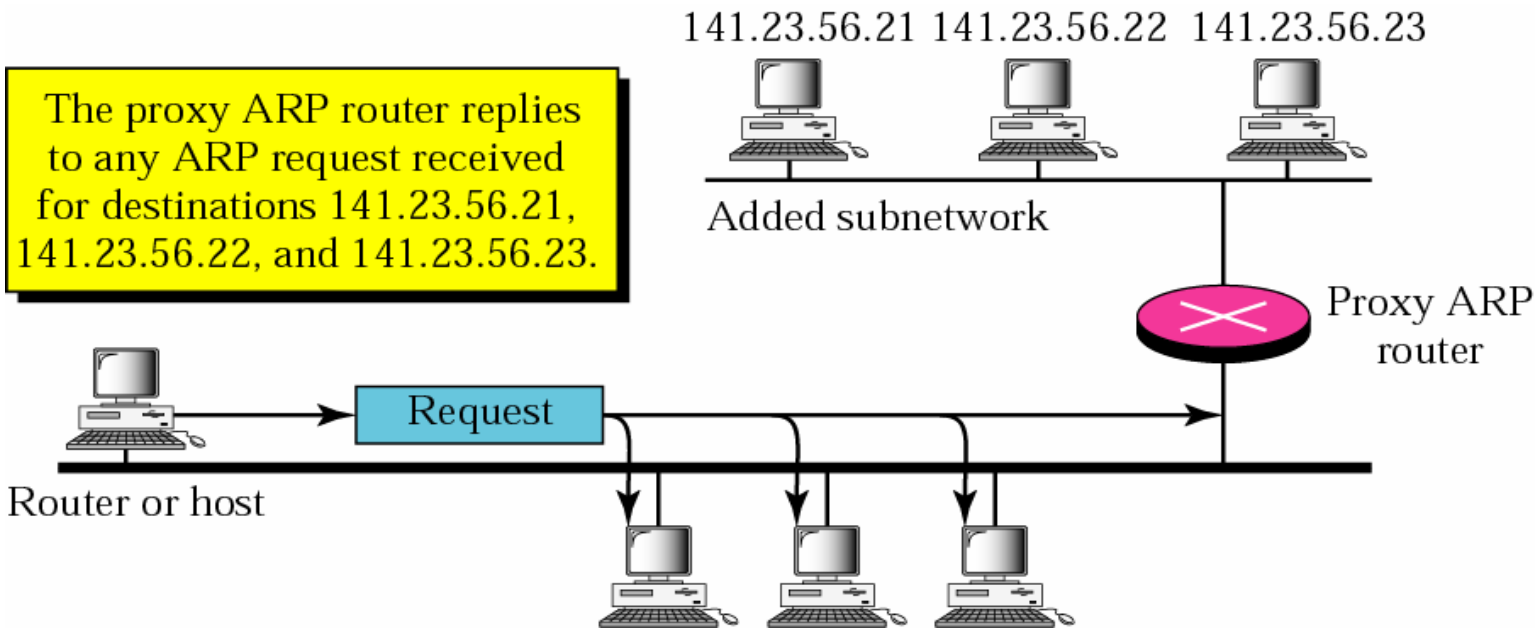
See Next Slide


130.23.43.20
B2:34:55:10:22:10
System A
130.23.43.25
A4:6E:F4:59:83:AB
System B
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
130.23.43.20
130.23.43.25
CRC
Data
28 bytes
0x0806
0xB23455102210
0xFFFFFFFFFFFF
Preamble
and SFD
ARP Request
0x0001
0x0800
0x06
0x04
0x0002
0xA46EF45983AB
0x82172B19
0xB23455102210
0x82172B14
Preamble
and SFD
0xB23455102210
0xA46EF45983AB
0x0806
Data
CRC
ARP Reply (from B to A)

Proxy ARP

- Proxy ARP is used to create subnetting effect
- Proxy ARP: An ARP that acts on behalf of a set of hosts
  - Whenever a router receives an ARP request which asks for the physical address of any one of the hosts it is representing, the router responds with its own physical address

Proxy ARP


141.23.56.21 141.23.56.22 141.23.56.23
The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.
Added subnetwork
Proxy ARP router
Request
Router or host

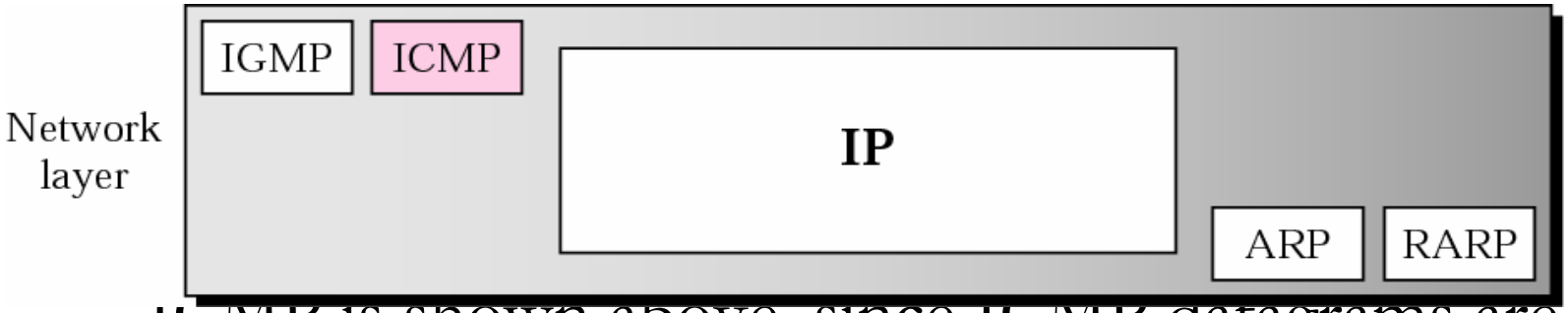
ICMP

Why ICMP?

- IP provides connectionless & unreliable (best-effort) datagram delivery
- IP has deficiencies
  - Lack of error control/correction
    - What if something goes wrong?
      - Router drops a packet, how to know?
      - TTL is decremented by one at each hop, how will the source know that TTL has reached 0
  - Lack of host and management queries
    - Host is alive or not? Misc information is required, how to fetch?

ICMP w.ref.t Network layer

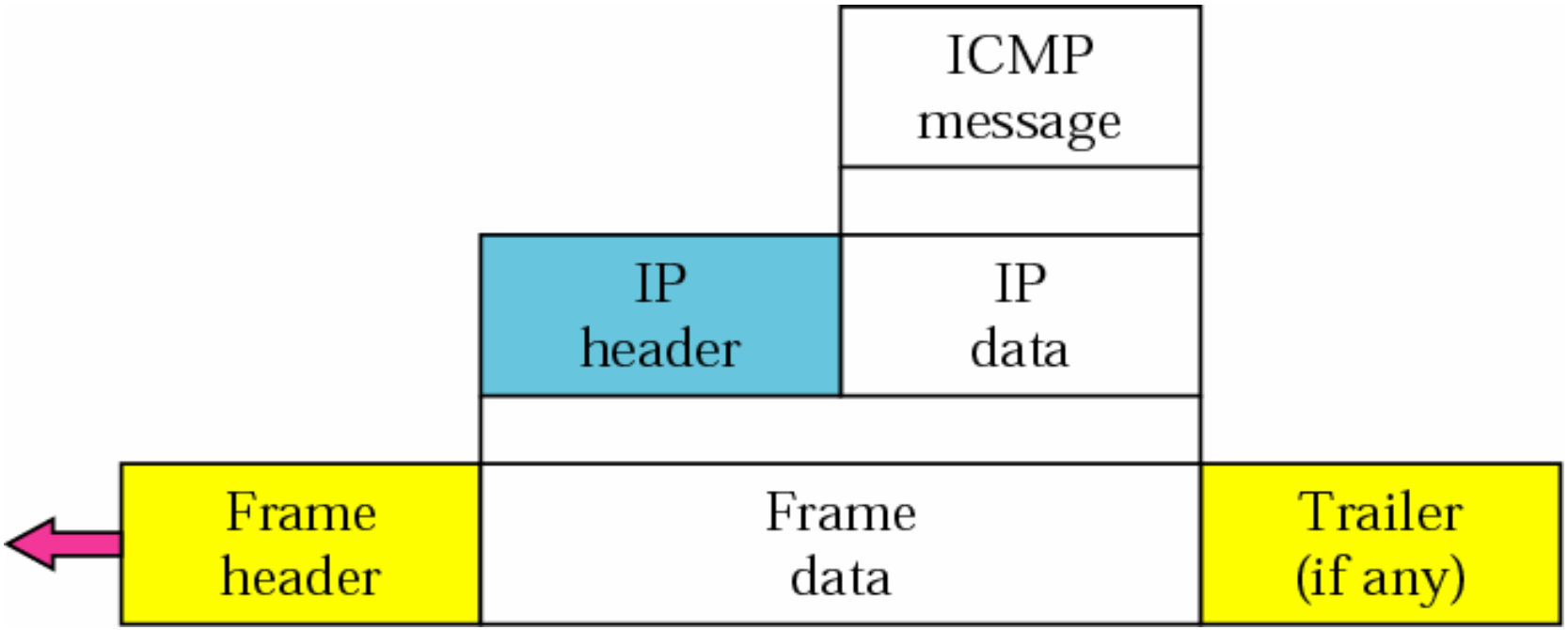
- Supporting protocol for IP
  - As is ARP and RARP



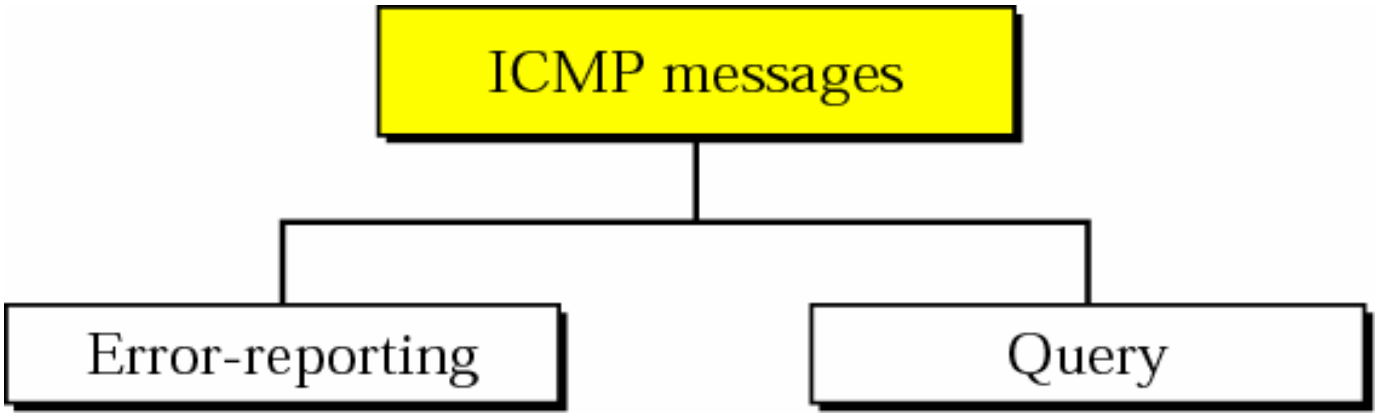
  - ICMP is shown above, since ICMP datagrams are not sent to the data-link layer directly. They are encapsulated in IP datagrams and then forwarded

ICMP Encapsulation

- IPheader.protocol = 1



Types of ICMP Messages



Errors which a router or a host (destination) may encounter

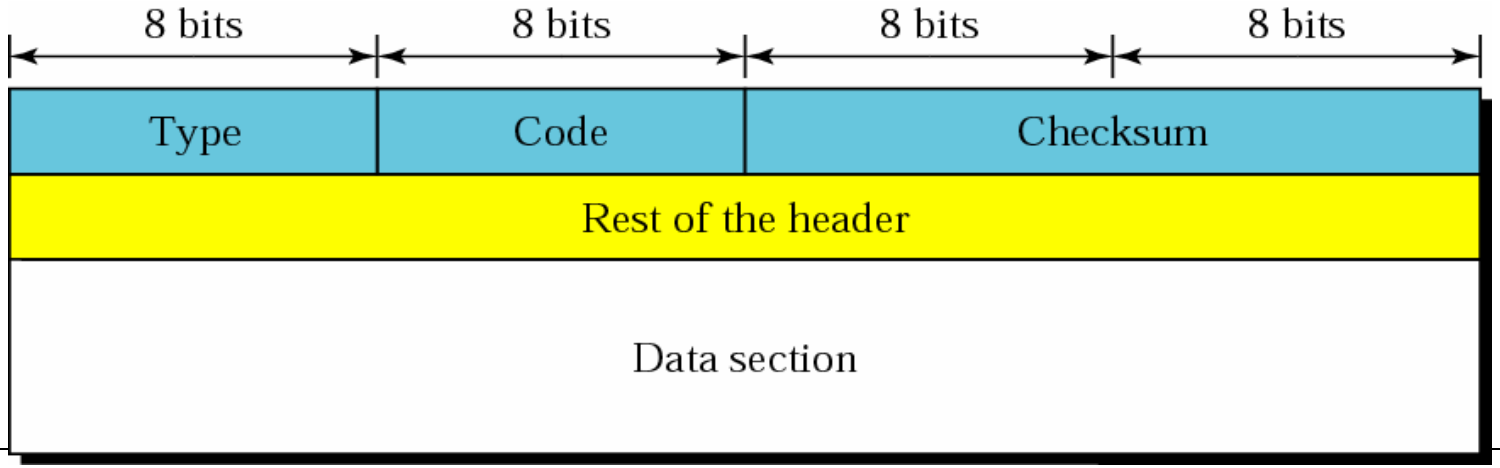
Query messages to get specific information from a router or a host. Always occur in pairs

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

Message Format

- An ICMP message has an 8-byte header and a variable-size data section
- The general format of the header is different for each message type yet the first 4 bytes are common to all

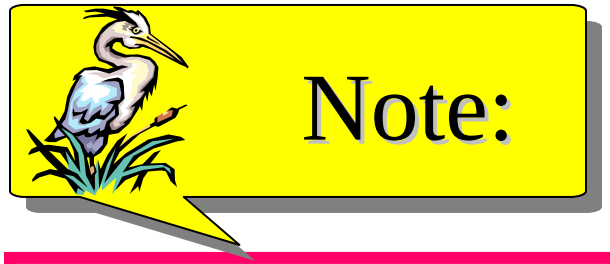


Error Messages

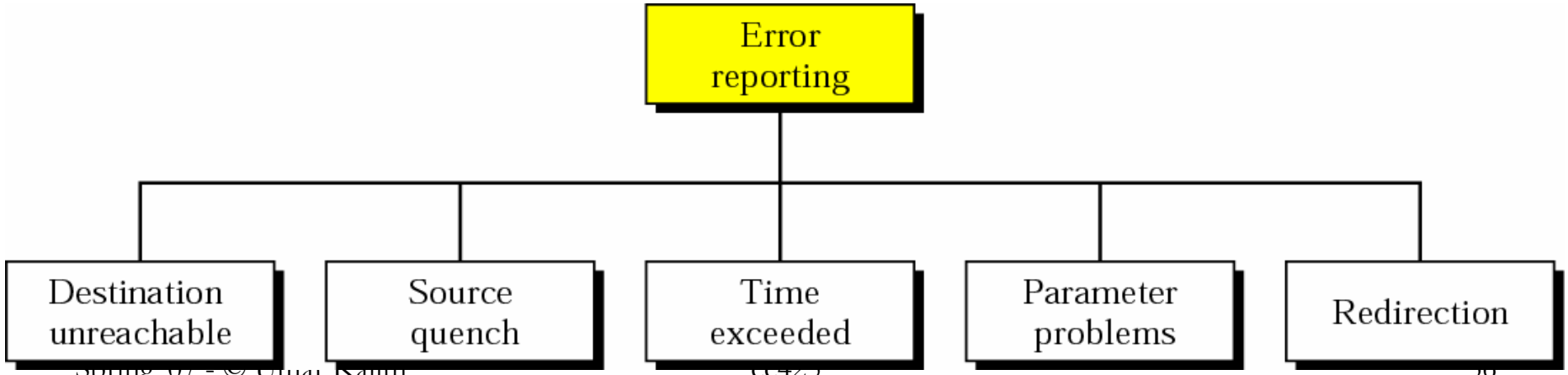
Error Reporting vs Error Correction

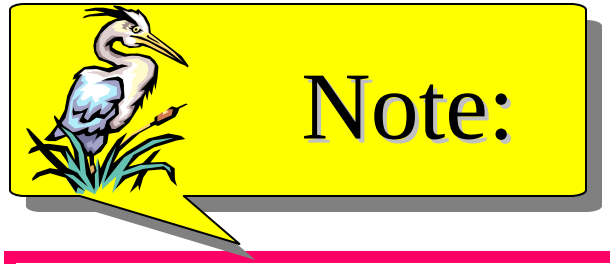
- ICMP does not
  - Provide interaction between a router and the source of trouble
  - Maintain state information (each packet is handled independently)
- When a datagram causes an error, ICMP can only report the error condition back to the original source of the datagram

Error Reporting



ICMP always reports error messages to the original source.



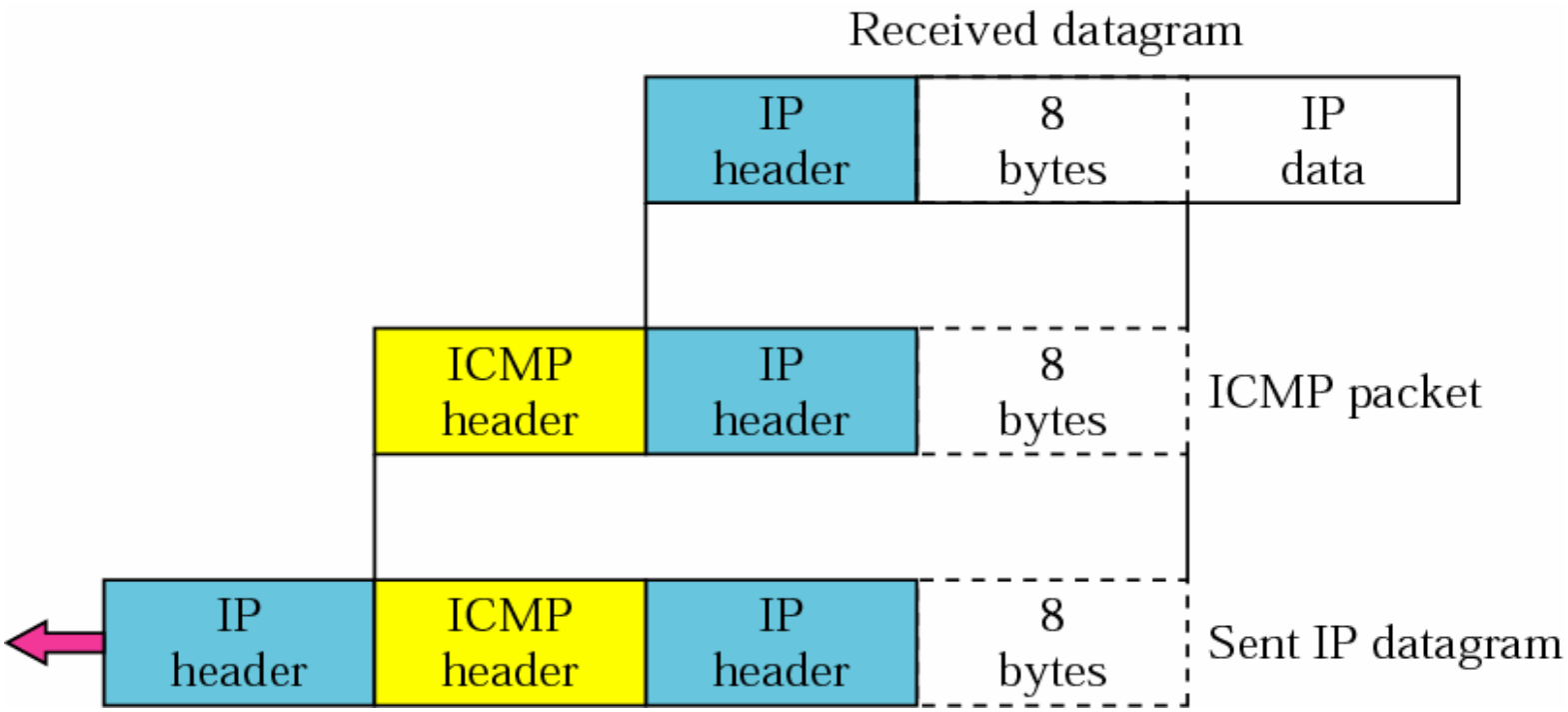


Note:

The following are important points about ICMP error messages:

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

Error Messages

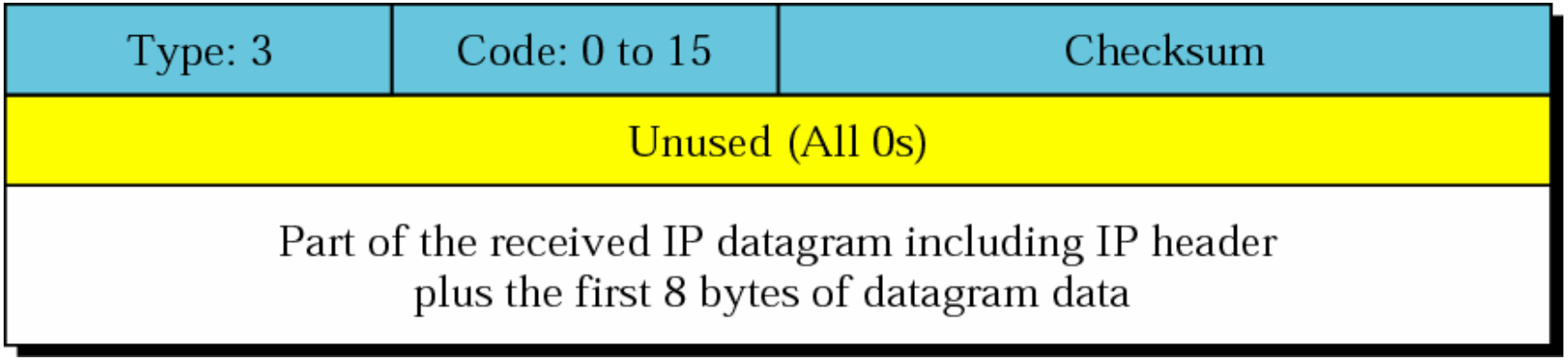


Destination unreachable ~ 3

- Generated by the router to inform the client that the destination host is unreachable
- Reasons for this message may include the
  - physical connection to the host does not exist (distance is infinite),
  - the indicated protocol or port is not active, or
  - the data must be fragmented but the 'don't fragment' flag is on
- http://en.wikipedia.org/wiki/ICMP_Destination_Unreachable

Destination unreachable ~ 3

- Defined codes for each type of failure
  - Refer to the book for the values



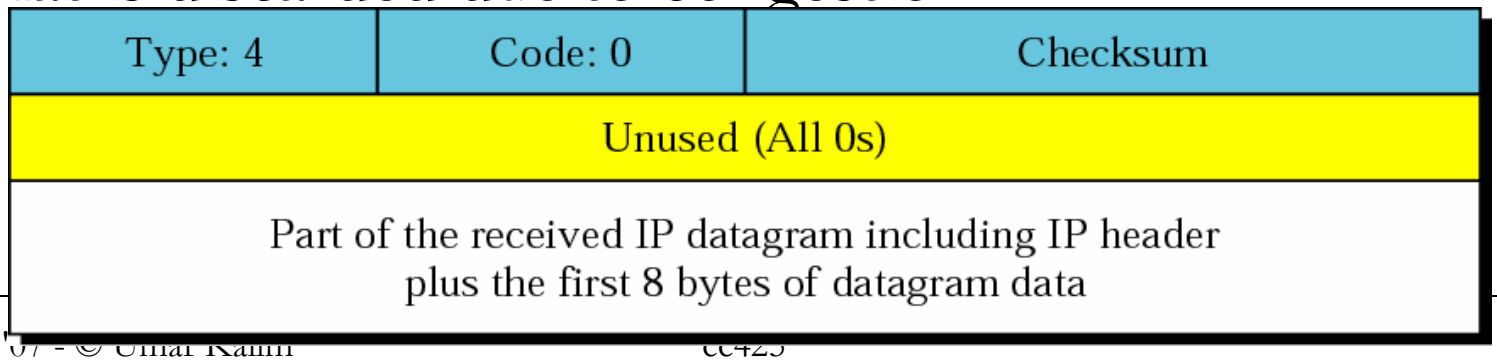
Source Quench ~ 4

- Message which requests the sender to decrease the traffic rate of messages to a router or host
- Generated if the router or host does not have sufficient buffer space to process the request,
- or may occur if the router or host's buffer is approaching its limit

- http://en.wikipedia.org/wiki/ICMP_Source_Quench

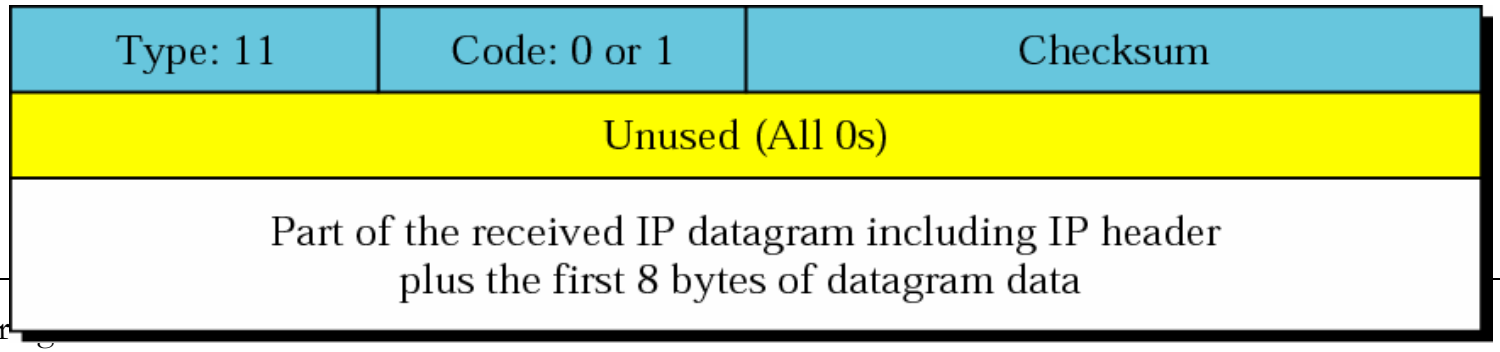
Source Quench ~ 4

- No mechanism for Flow-control in IP
- 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



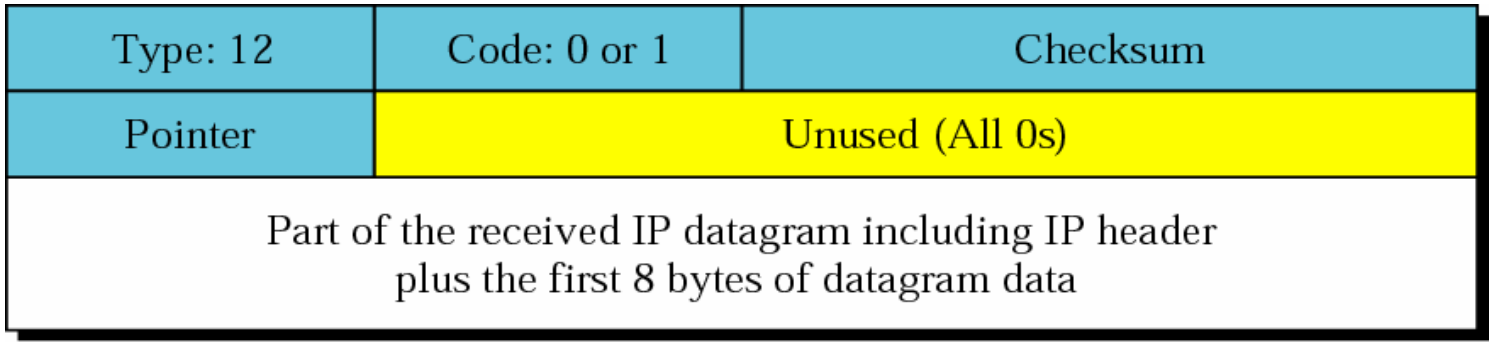
Time exceeded ~ 11

- Generated by a gateway to inform the source of a datagram that the datagram has been discarded due to the time to live field reaching zero
- message may also be sent by a host if it fails to reassemble a fragmented datagram
- http://en.wikipedia.org/wiki/ICMP_Time_Exceeded

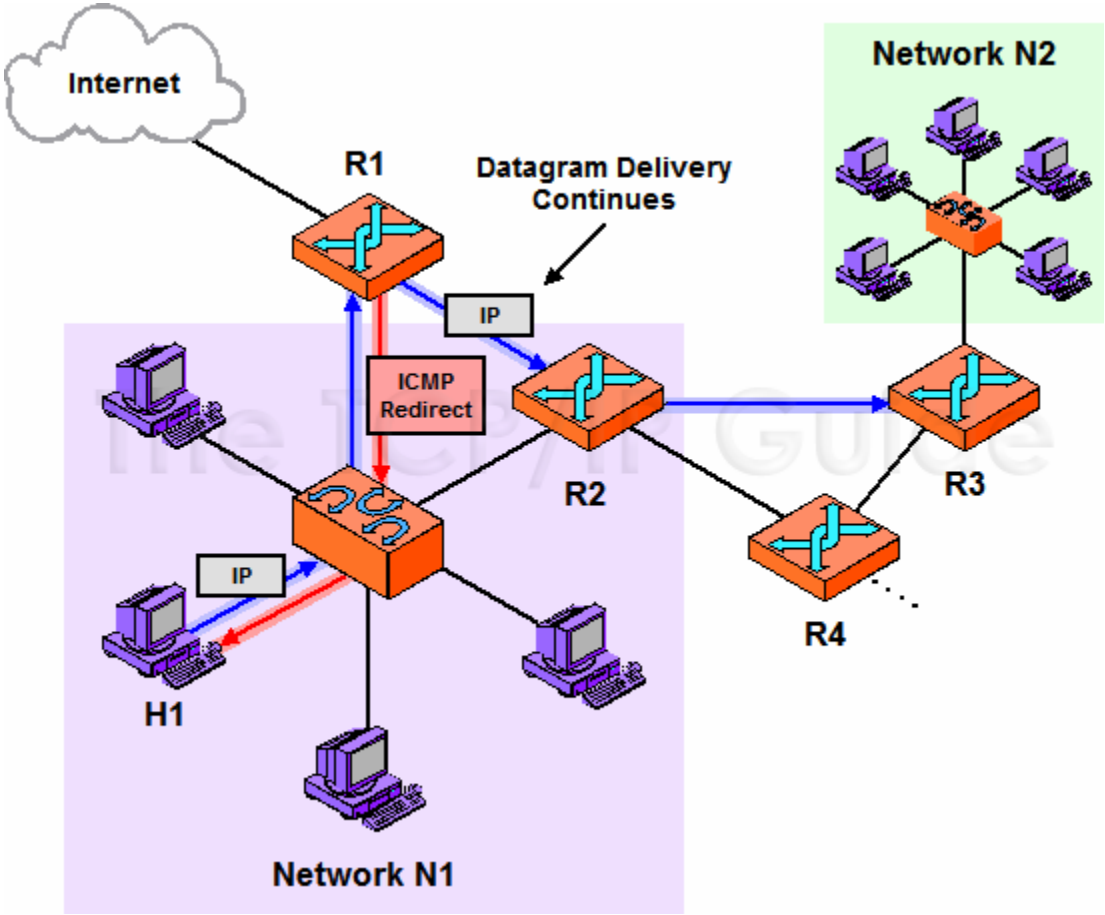


Parameter Problem ~ 12

- Sent to the source host for any problem not specifically covered by another ICMP message
  - 0 ~ ambiguous
  - 1 ~ missing option field

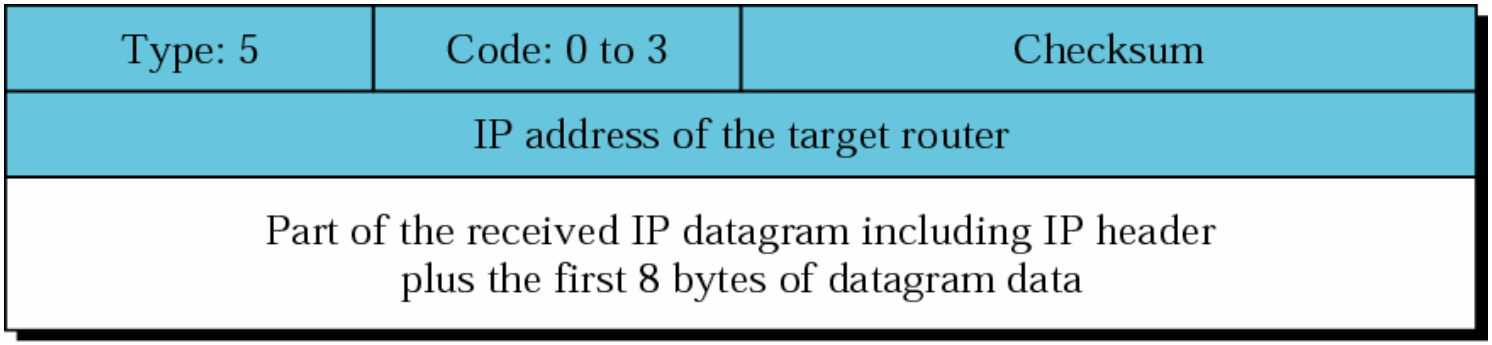


Redirection ~ 5



http://www.tcpipguide.com/free/t_ICMPv4RedirectMessages.htm

Redirection ~ 5



Questions?

That's all folks!