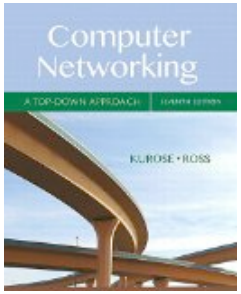
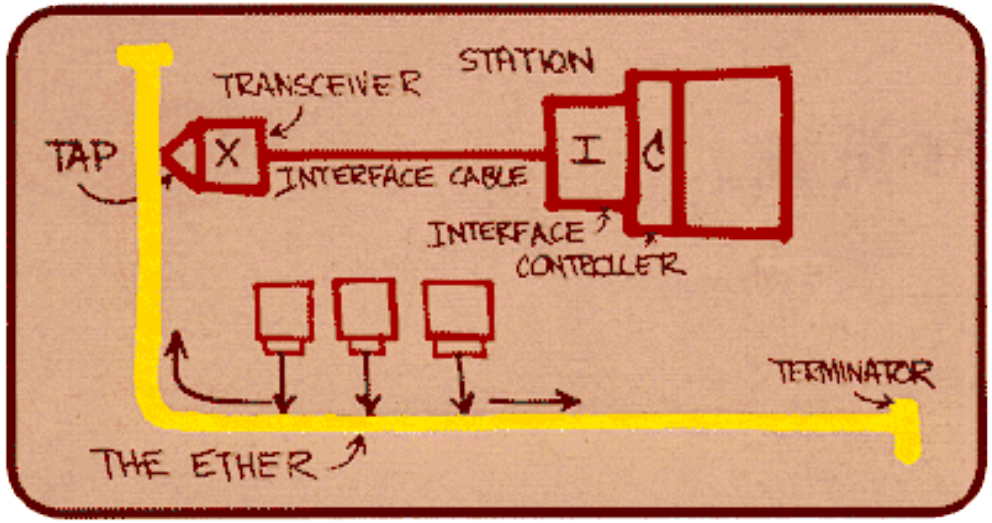
COMP 375: Lecture 38



- **News & Notes:**
  - Project #5 due @ 10PM
  - Quiz #9 in class ~~today~~ Monday
- **Reading (Mon, May 7)**
  - Sections 8.{4,5}

LINK LAYER ADDRESSING

Ethernet is the dominant wired LAN technology today.

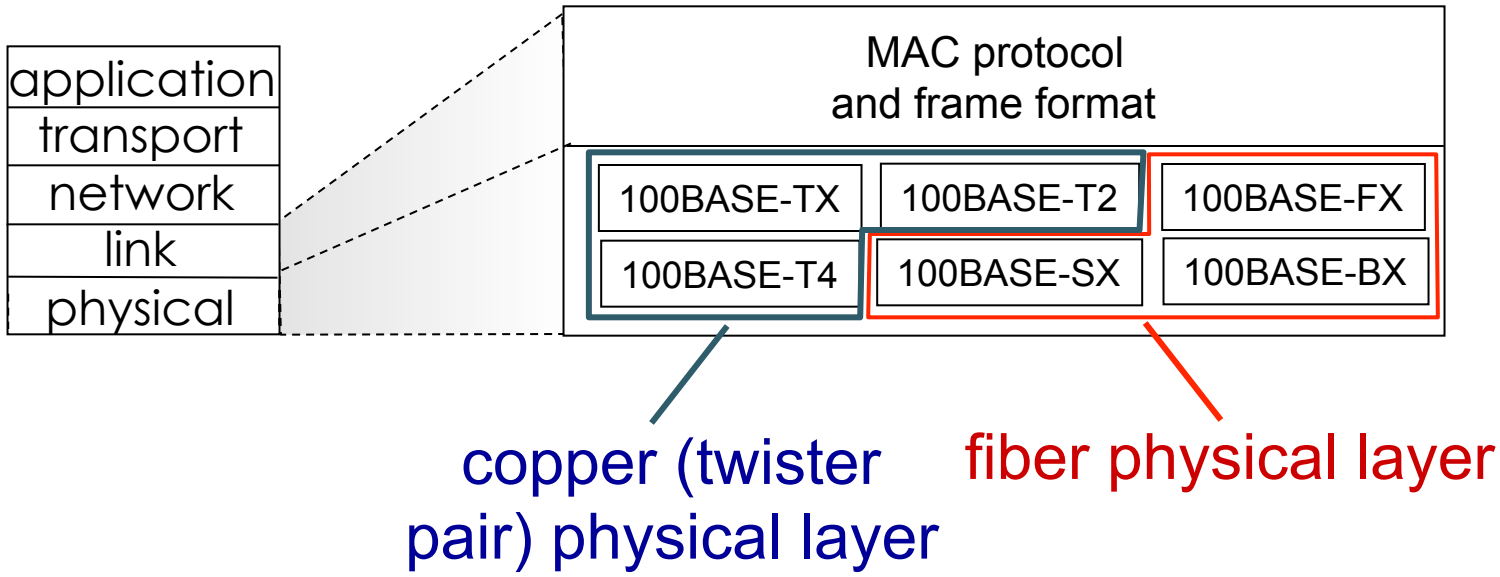


Metcalfe's Ethernet sketch

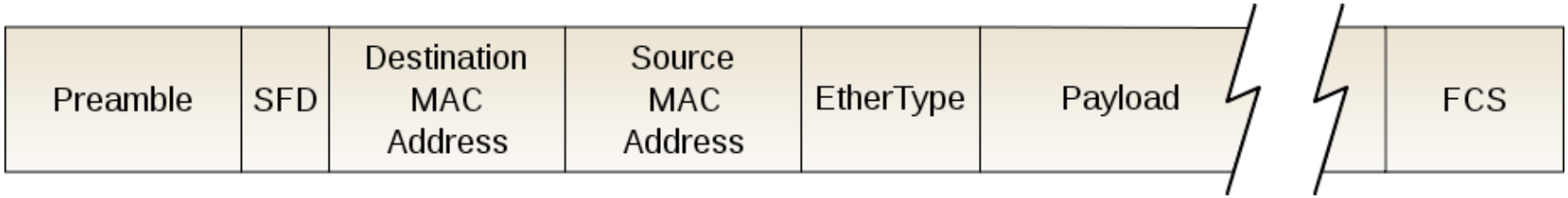
Ethernet provides connectionless, unreliable transmission.

- *What other protocol does Ethernet sound like?*
- *What protocol does Ethernet use for multiple access?*

There are several Ethernet standards, based on the link and physical layer.



Ethernet Frame Structure

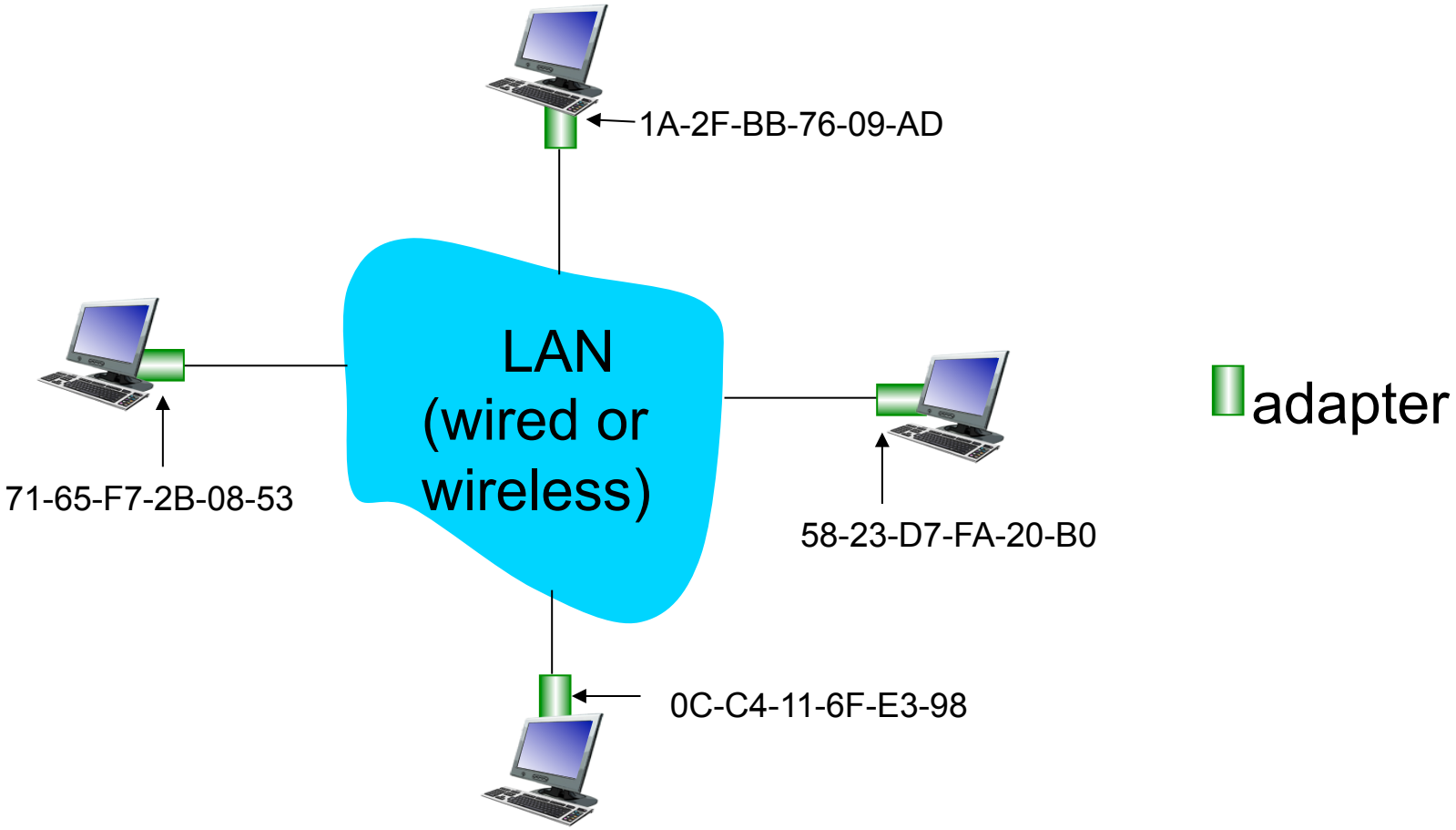


The Link Layer uses MAC Addresses for addressing.

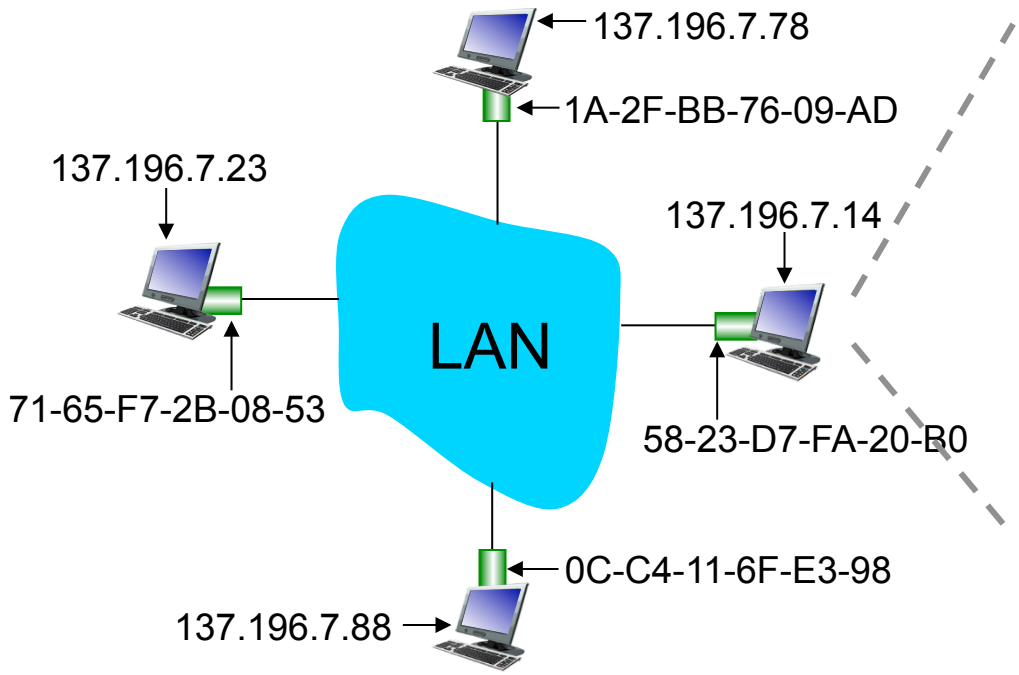
- **IPv4 address:** (e.g. 174.24.11.8)
  - *32-bit*
  - *Network-layer* address for interface
  - Changes as you change networks
  - Used for end-to-end routing

- **MAC address:** (e.g. 1A-2F-BB-76-09-AD)
  - *48-bit*
  - *Link-layer* address for interface
  - Modifiable, but not required to change
  - Used to get data to next hop

Each adapter on LAN has unique MAC address



ARP* is used to convert between IP and MAC addresses.



ARP Table

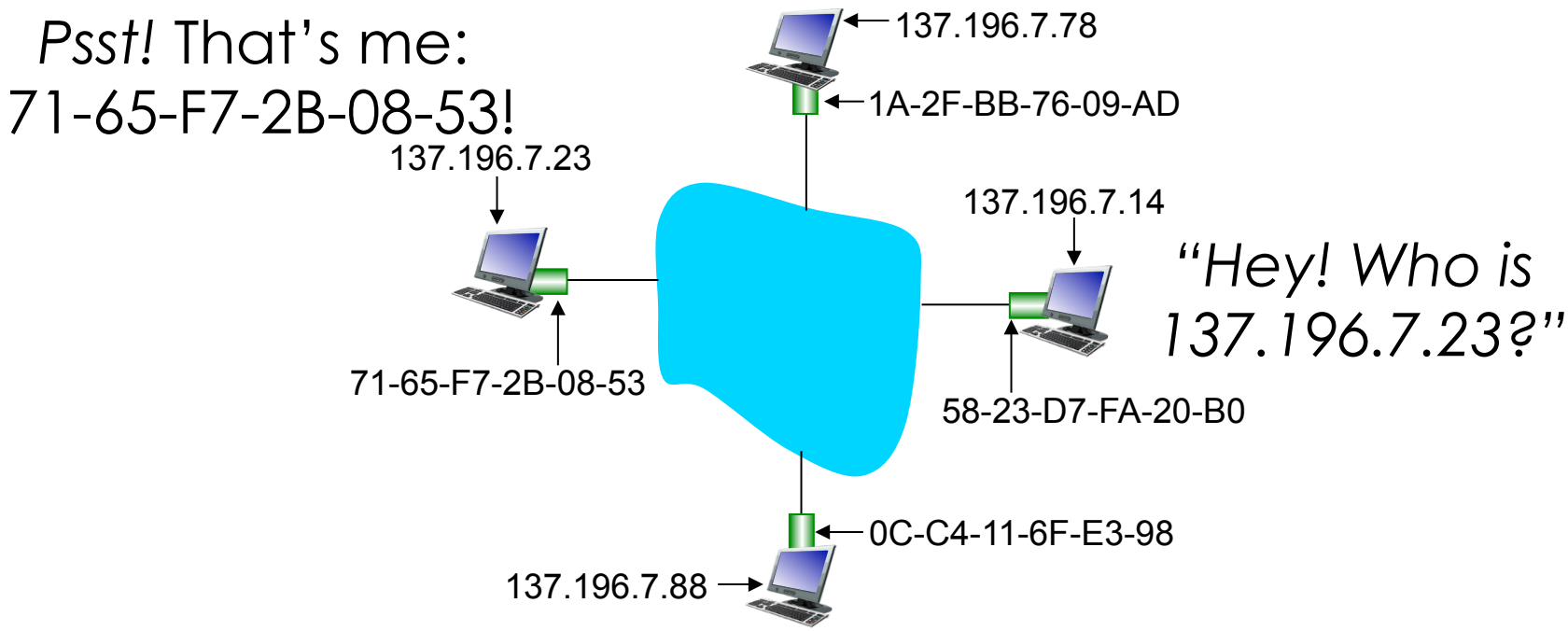
MAC	IP	TTL
1A-2F-BB-76-09-AD	137.196.7.78	10 min
0C-C4-11-6F-E3-98	137.196.7.88	15 min
…	…	

**Address Resolution Protocol*

What's the best way to handle filling in a host's ARP table?

A.	Each host periodically broadcasts its IP address.
B.	Each host will periodically ask everyone for their IP address.
C.	A host will ask another host for its IP address.
D.	A host will ask who has a specific IP address.
E.	None of the above.

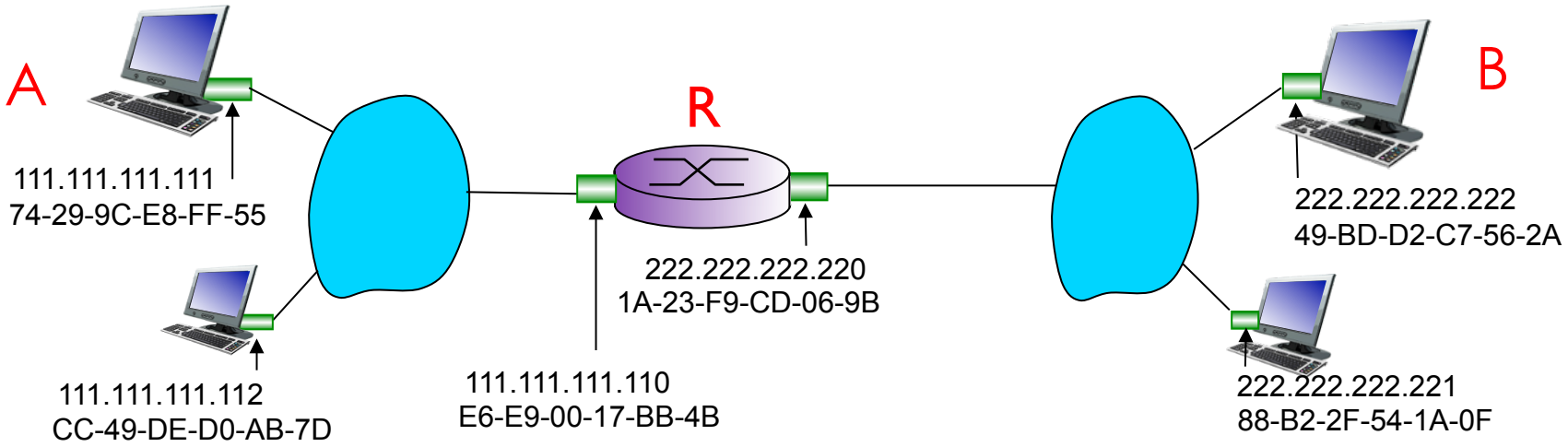
Hosts broadcast requests to all other hosts; only the host in question responds.



What happens when we want to **send** a datagram **from A to B, via R**?

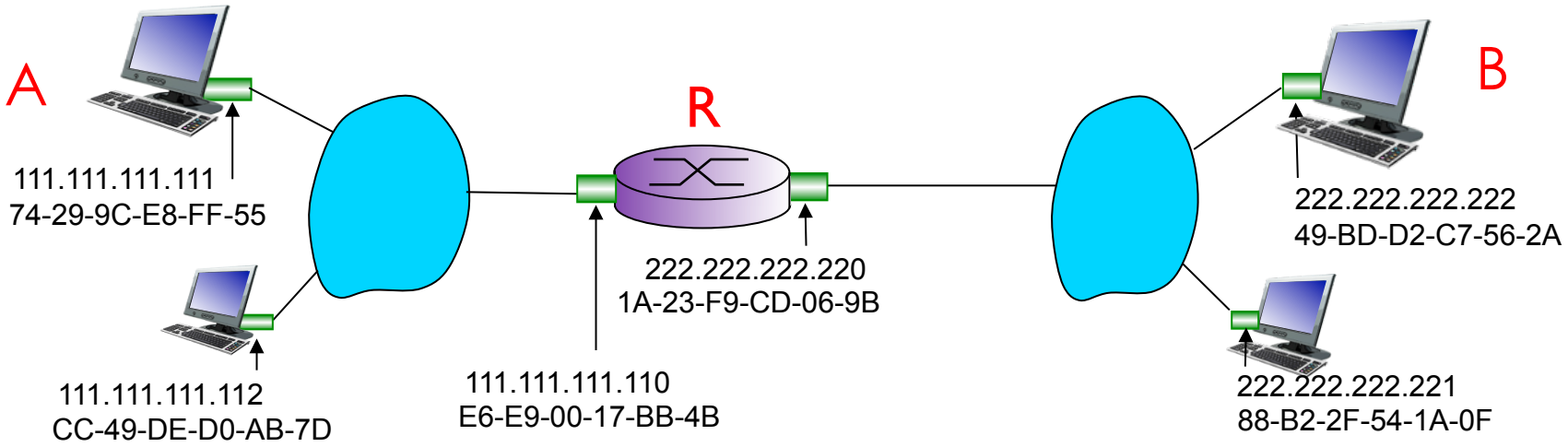
Assume A knows B's IP address.

(DNS, FTW!)



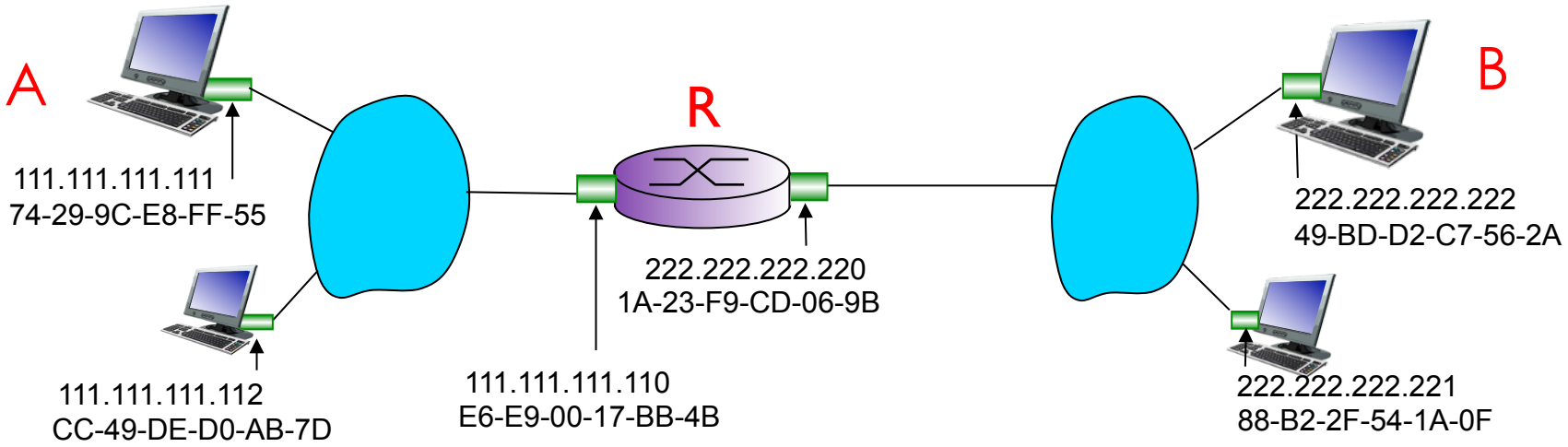
A couple important questions…

1. *Who do we address the datagram to (IP destination)?*
2. *Who do we forward it to on the first hop?*

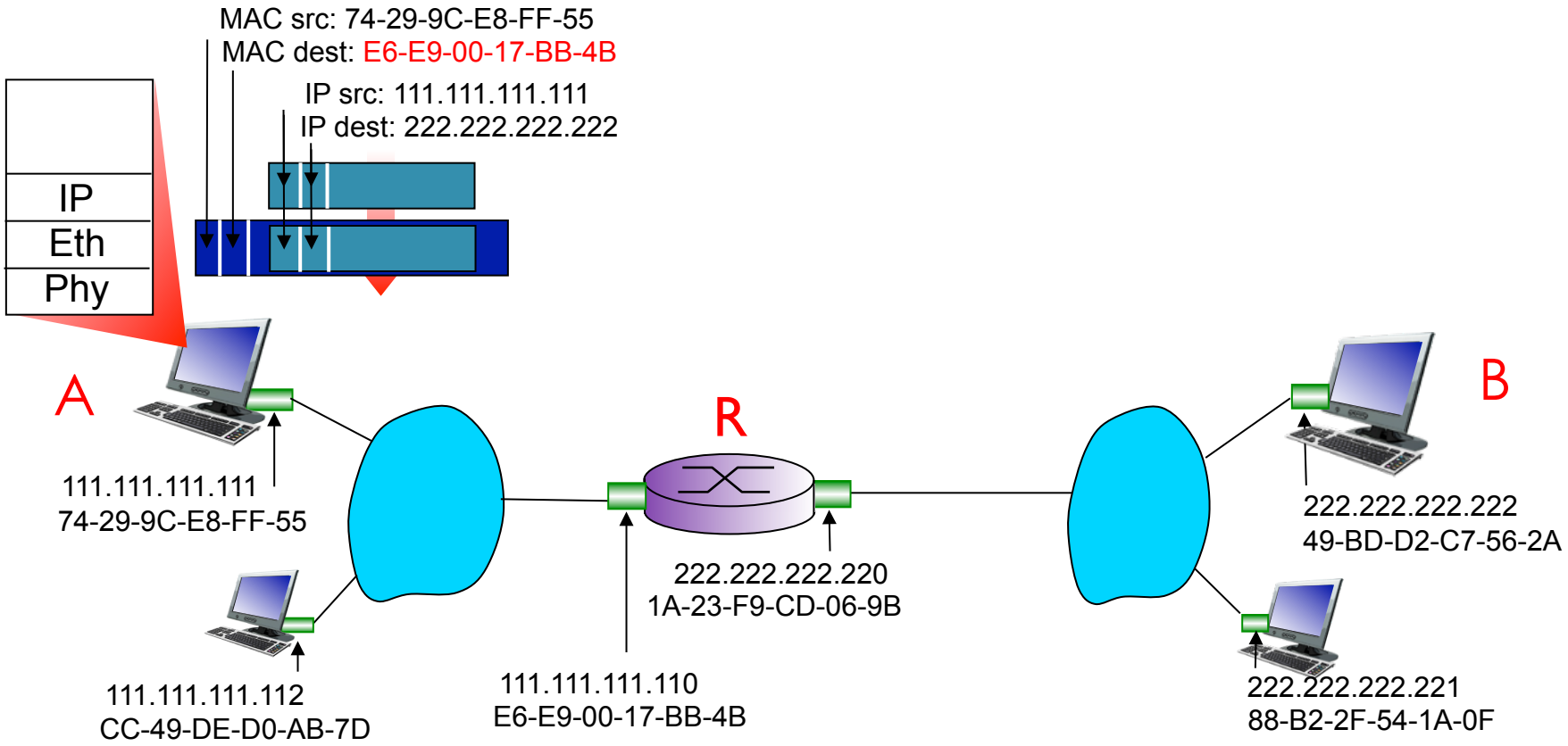


How does **A** learn **R's IP address**?

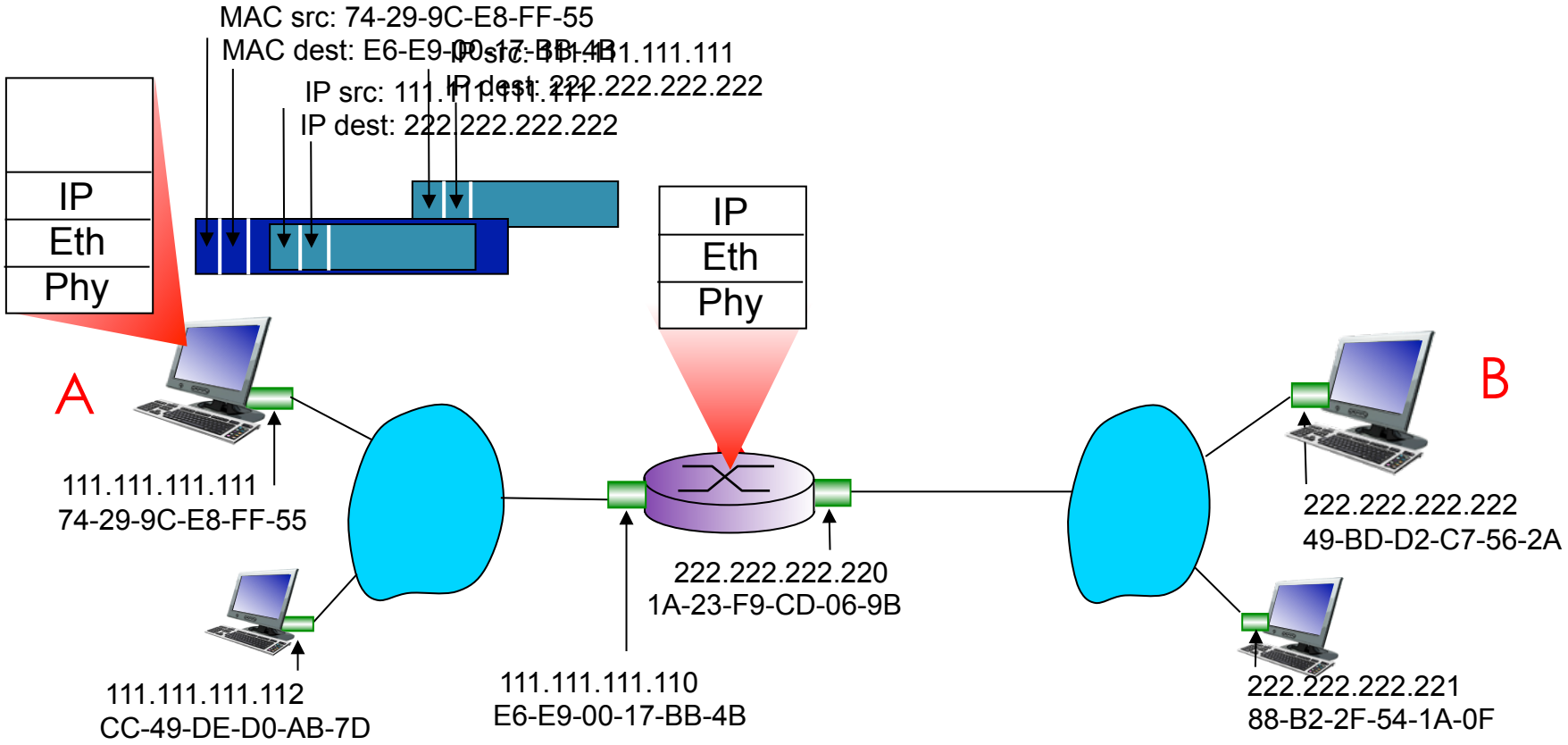
A.	ARP
B	DHCP
C.	IP
D.	Routing protocol



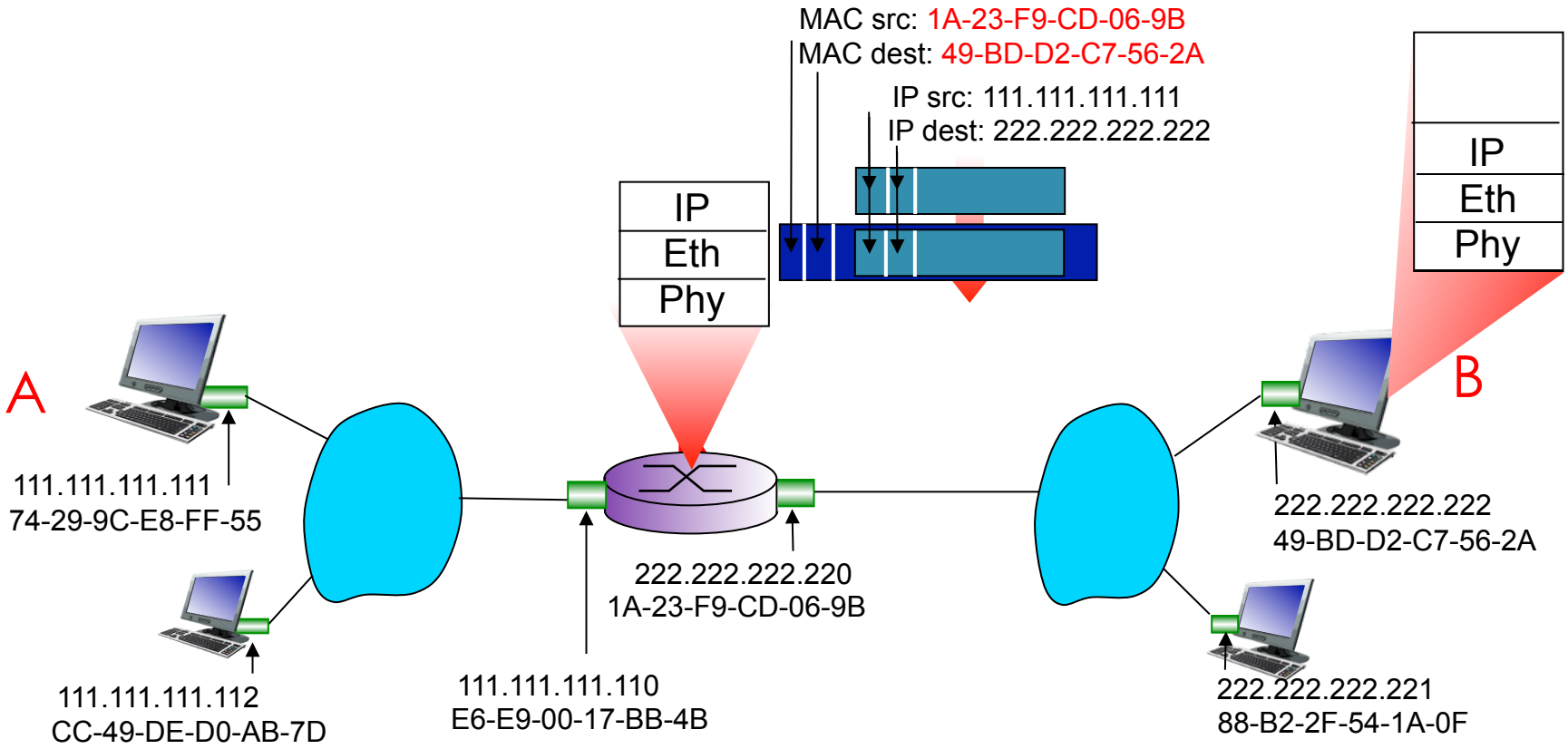
A's datagram destined to B is wrapped in a link-layer frame with R as destination.



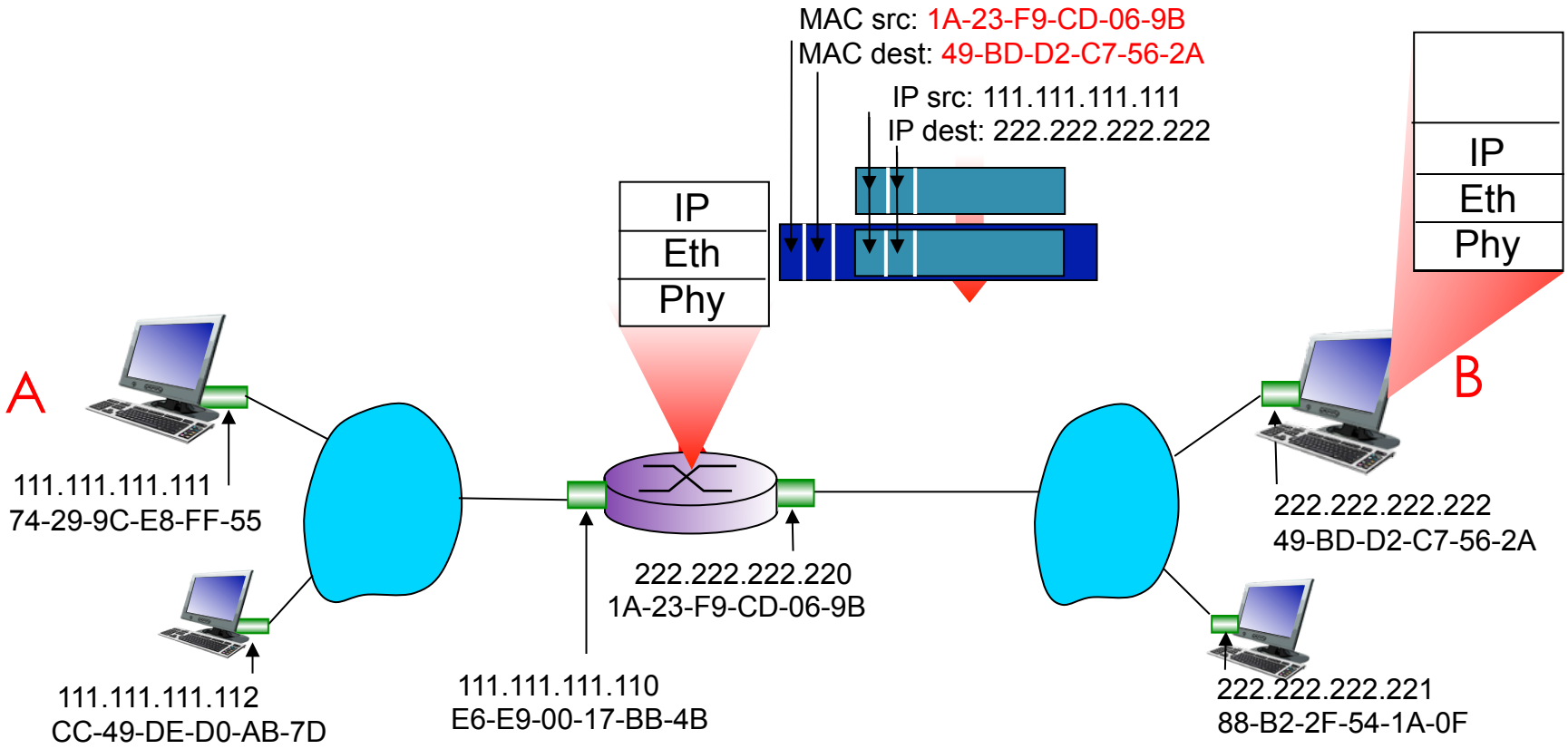
The frame is sent to R, which sends payload to the network layer.



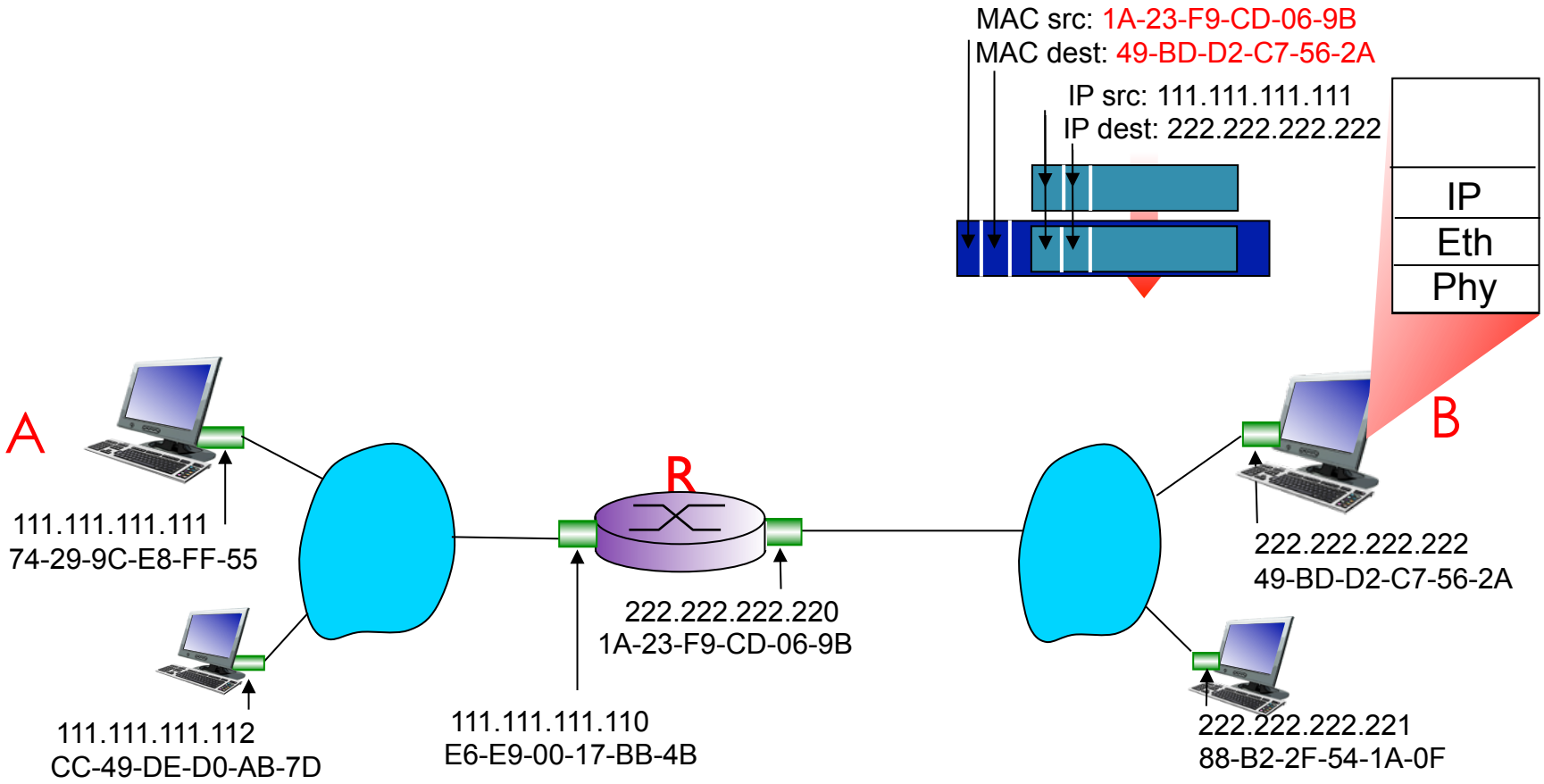
R forward's A's datagram, creating a new link-layer frame with B's MAC.



R forward's A's datagram, creating a new link-layer frame with B's MAC.



At it's final destination, the frame is sent up the network stack.



Chapter 8

SECURITY IN COMPUTER NETWORKS

Why did early Internet protocol designers not integrate security?

A.	They were idealistic and assumed everyone would be trustworthy.
B.	They did not have the knowledge to integrate security.
C.	They were too busy with other things.
D.	They were hindered by laws.
E.	They were hindered by limited CPU performance.

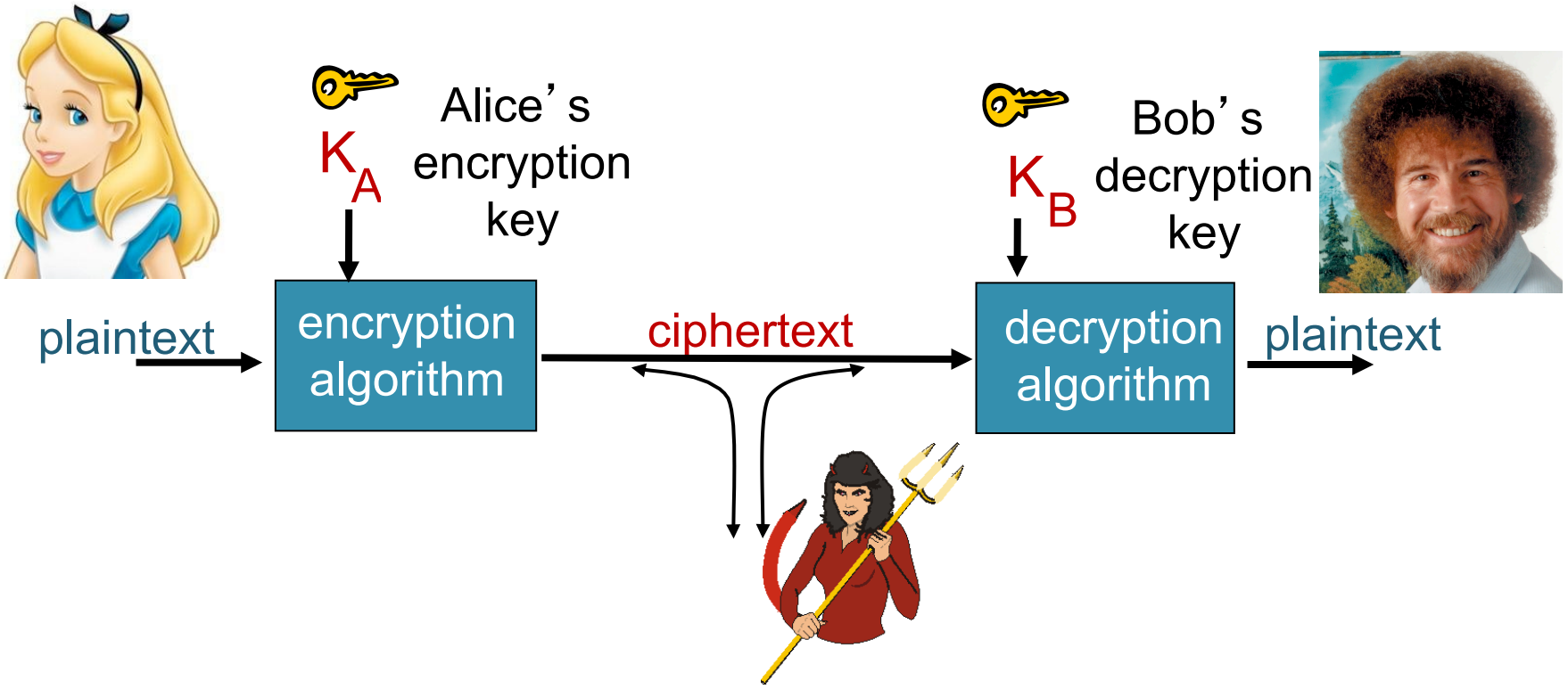
There are four desirable properties for secure communication.

1. Confidentiality
2. Message Integrity
3. End-point authentication
4. Operational Security

Section 8.2

PRINCIPLES OF CRYPTOGRAPHY

The goal is to allow Alice and Bob to securely communicate, despite evil Trudy!

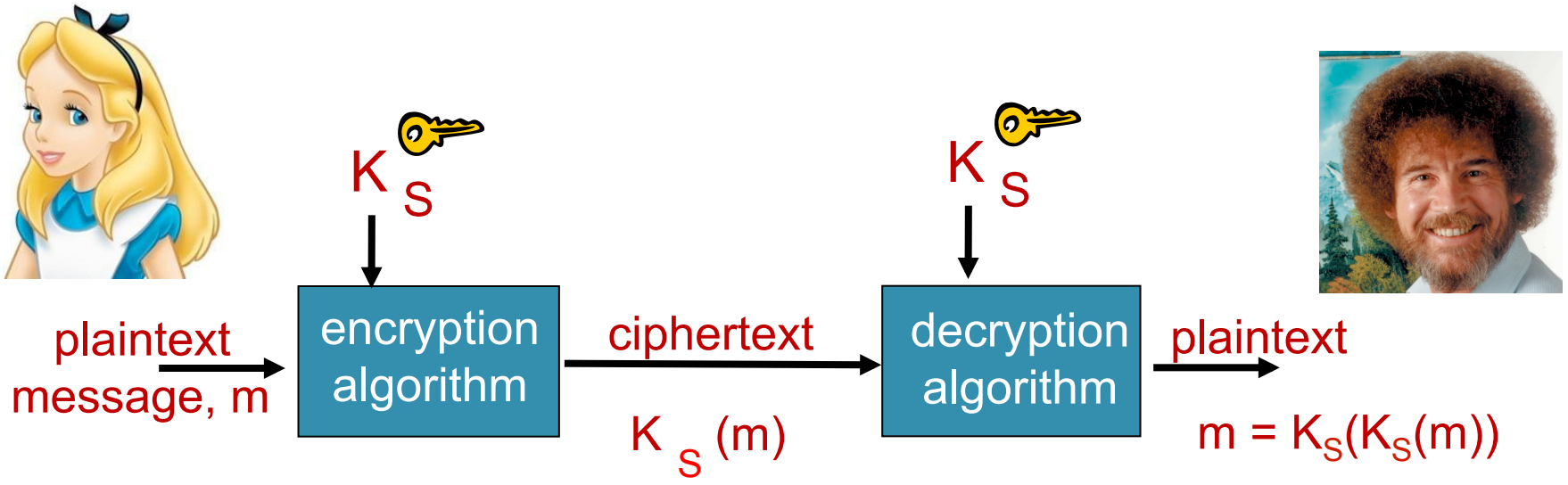


m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

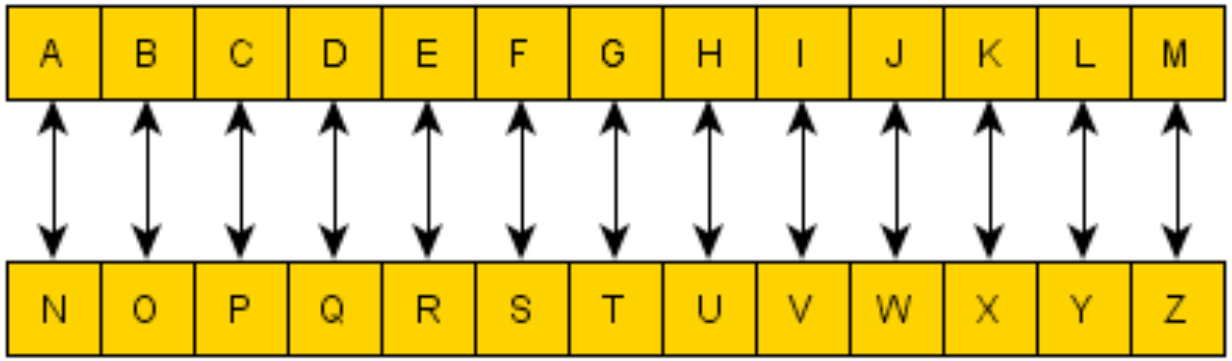
In symmetric key cryptography, Alice and Bob share a secret key, K_S.



Can you decode the following message?

V YVXR PF

ROT13 Encryption:



What if I used a completely random mapping from one letter to another?

How might you decipher the message?