CPSC 317 COMPUTER NETWORKING

Module 7: Link Layer – Day 2 – Access Control and ARP

LEARNING GOALS

Link Layer

- Explain the purpose of the link layer, and the four types of services the link layer provides
- Know the general structure of link layer "frames"
- Understand link layer addressing: MAC addresses
- Explain why the link layer may use "error correction"
- Know three techniques for error detection: parity (1D and 2D), checksum, CRC
- Understand the basic types of media (point-to-point, broadcast) and what is meant by "access control"
- Know the basic differences between a switch and a router

LEARNING GOALS

ARP

- Explain the purpose of ARP
- Enumerate the steps to resolve an IP address on a LAN with ARP
- Explain how ARP is implemented at layer two
- Describe the steps to send a datagram from one LAN to another LAN, assuming you need to resolve the IP addresses
- Know how to perform a layer 2 broadcast

READING

- Reading: 6.3 Intro, 6.3.2, 6.3.3, 6.4 Intro, 6.4.1

TERMINOLOGY

- The networks that we have been talking about at the link layer are often called Local Area Networks (LANs)
- Historically, they were limited to a small area and a relatively small number of adapters
- They often use a broadcast medium for communication

ACCESS CONTROL

- Many links are half-duplex
  - Multiple adapters can transmit, but only one at a time
- Some (point to point links) are full-duplex
  - Both sides can transmit at the same time without interference
- When the link is half-duplex, how do you know if someone else is using the link?
- We make two (generally true) assumptions:
  - You can tell if someone else is sending by listening
  - You can tell if your transmission overlapped some other transmission (a *collision* happened) again by listening

RANDOM ACCESS CONTROL

- When you have something to send, just send it
- If a collision is detected, try again after a random delay

CSMA - CARRIER SENSE MULTIPLE ACCESS

- Listen before sending, only send if no one else is
- Matches our human conventions for conversation

CSMA/CD – ADD COLLISION DETECTION

- While sending, listen for a collision
- If so, abort your transmission early
- This wastes less time than continuing to send the whole frame even after a collision is detected
- This also matches our human conventions for conversation
  - If someone else starts talking when you are, you both stop and figure out who should go first

HOW LONG TO WAIT BEFORE TRYING AGAIN?

- If there are only a small number of adapters that are trying to send, we want to wait a little while
- If there are a large number of adapters that are trying to send, we want to wait a long time
- You don't know how many other adapters are trying to send
- Binary Exponential Backoff
  - Choose a random number in the range 1 – 2^n
  - Where n is the number of times you have collided trying to send this frame

TURN-BASED ACCESS CONTROL

- Senders take turns
- If they have nothing to send right now, pass on their turn
- This can be done with either
  - Centralized control
  - Decentralized control

CENTRALIZED CONTROL

- A single node decides whose turn it is
  - Either it polls everyone, or
  - There is a way for an adapter to signal that it wants a turn
- Used in WIFI – the access point is the centralized controller
  - It polls each adapter to see if it wants a turn

DECENTRALIZED CONTROL

- A ‘token’ is passed between senders
- Only send when you have the token
- More complicated
  - What happens if the adapter with the token breaks?
    - Somehow create a new token – who does this?
  - What happens if an adapter thinks that the adapter with the token is broken and creates a new token when there is already a token?
    - Now you have two tokens

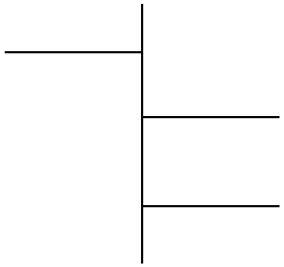
CLICKER QUESTION

Consider CSMA/CD and turn-based access control with a central controller in a network with many hosts. Which of the following statements are true?

A. CSMA/CD will use the network efficiently if there are many hosts sending data
B. CSMA/CD will use the network efficiently if there is just one host sending data
C. Turn based access control will use the network efficiently if there are many hosts sending data
D. Turn based access control will use the network efficiently if there is just one host sending data

SWITCHES (LAYER 2 DEVICES)

Single Broadcast Domain



SWITCHED LINKS

- Each wire has only 2 ends
- If you engineer it right, both sides can be sending at once
  - Full-duplex
- No need for access control
- The central switch implements the broadcast behaviour expected in a LAN
  - Every incoming frame is duplicated to every wire (except the one it came in on)

HOW DOES A SWITCH WORK?

- It contains a forwarding table with 3 columns

MAC Address	Interface	Time
01-02-03-04-05-06	1	8:23
02-03-04-05-06-07	1	7:56
03-04-05-06-07-08	2	7:59
04-05-06-07-08-09	3	8:01

1. Each time a frame is received on an interface I, the switch looks at both the source and destination MAC address

SOURCE MAC ADDRESS – LEARNING

MAC Address	Interface	Time
01-02-03-04-05-06	1	8:23
02-03-04-05-06-07	1	7:56
03-04-05-06-07-08	2	7:59
04-05-06-07-08-09	3	8:01

2. If the source address appears in the table, update the interface (I) and the time

3. If the source address doesn't appear in the table, add an entry with the address, the interface (I), and the time

DESTINATION MAC ADDRESS – FORWARDING

MAC Address	Interface	Time
01-02-03-04-05-06	1	8:23
02-03-04-05-06-07	1	7:56
03-04-05-06-07-08	2	7:59
04-05-06-07-08-09	3	8:01

4. Destination address not in the table
   - Send to every interface except I
5. Interface for destination in the table is I
   - Discard the frame
6. Interface for destination in the table is I' != I
   - Send the frame to interface I'

TWO MORE RULES

MAC Address	Interface	Time
01-02-03-04-05-06	1	8:23
02-03-04-05-06-07	1	7:56
03-04-05-06-07-08	2	7:59
04-05-06-07-08-09	3	8:01

- Never put the broadcast address (FF-FF-FF-FF-FF-FF) in the table
- Delete entries in the table whose time is too long ago

SWITCH VS ROUTER

- A switch is a link layer device
  - Can send frames only between directly connected interfaces
  - Supports broadcast
- A router is a network layer device
  - Can send datagram to any host in the Internet
  - Does not support broadcast

LEARNING GOALS

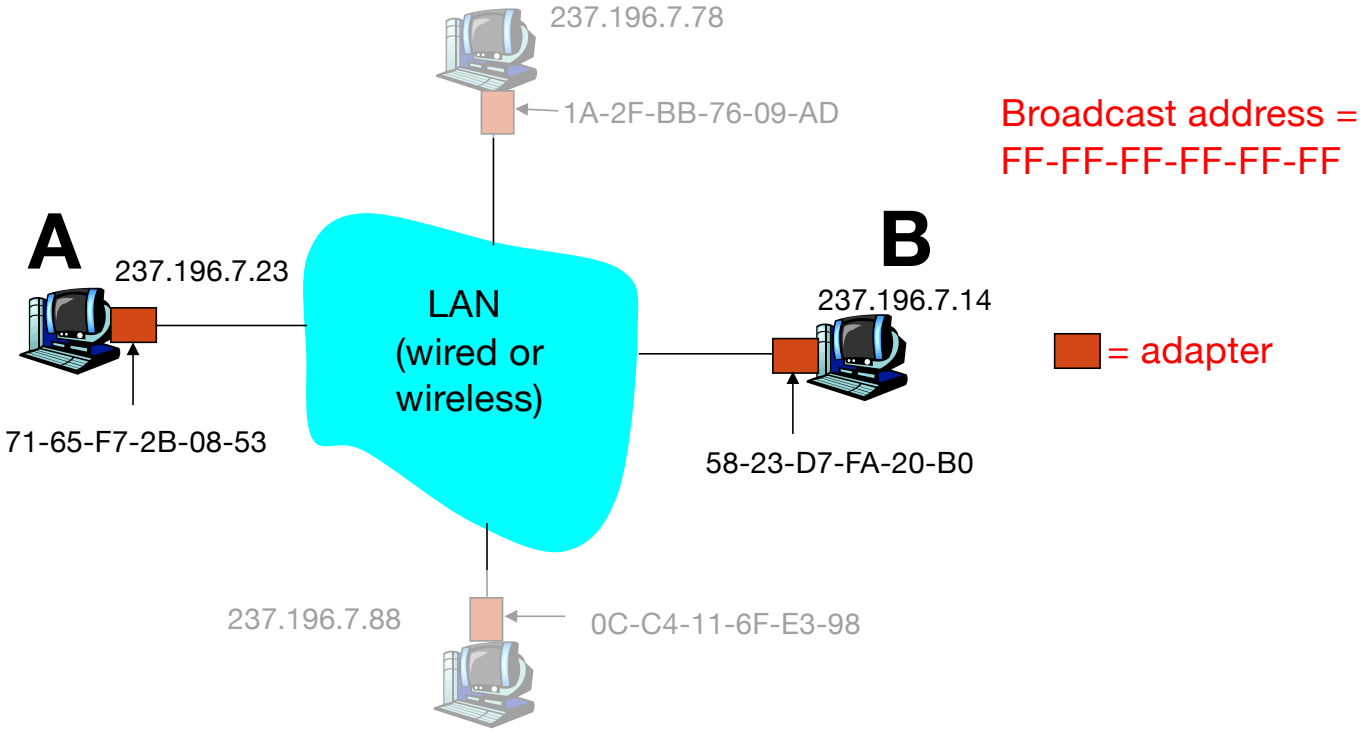
ARP

- Explain the purpose of ARP
- Enumerate the steps to resolve an IP address on a LAN with ARP
- Explain how ARP is implemented at layer two
- Describe the steps to send a datagram from one LAN to another LAN, assuming you need to resolve the IP addresses
- Know how to perform a layer 2 broadcast

ADDRESS RESOLUTION PROTOCOL

Purpose: resolving an IP address to a MAC address

HOW CAN A DETERMINE B'S MAC ADDRESS IF IT KNOWS B'S IP ADDRESS?



ARP SUMMARY

1. A wants to send datagram to B, but A doesn't know B's MAC address

2. A broadcasts ARP query packet, containing B's IP address

- Dest MAC address: FF-FF-FF-FF-FF-FF
- all machines on LAN receive ARP query

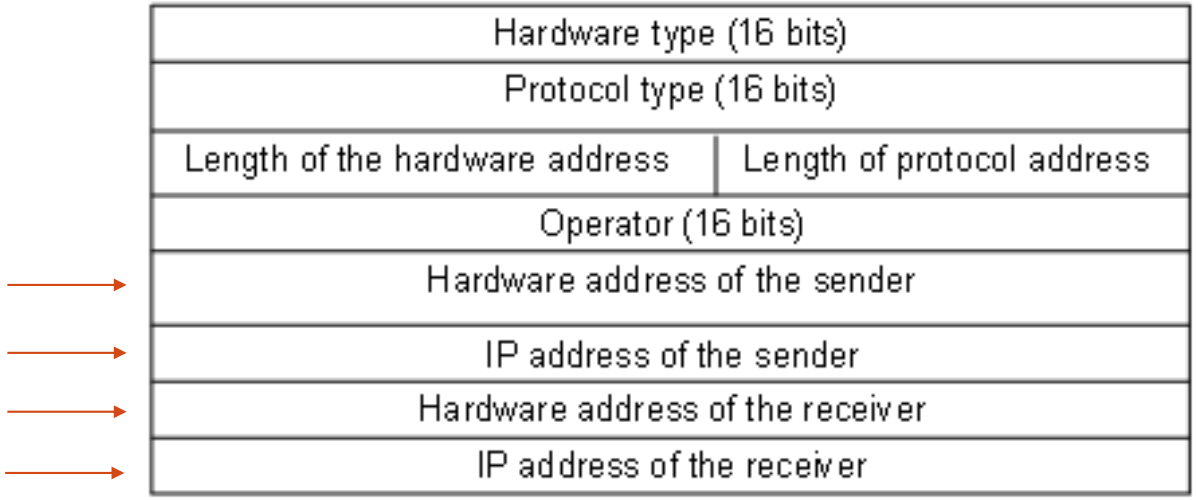
3. B receives ARP query, replies to A with its (B's) MAC address

- frame sent to A's MAC address (unicast)

4. A caches (saves) B's IP and MAC address pair in its ARP table

- The ARP table is soft state: information that goes away unless refreshed
  - Each entry in the table has a time limit
- ARP is "plug-and-play"
  - nodes create their ARP tables without intervention from network administrators

ADDRESS RESOLUTION PROTOCOL PACKET



Usually Ethernet

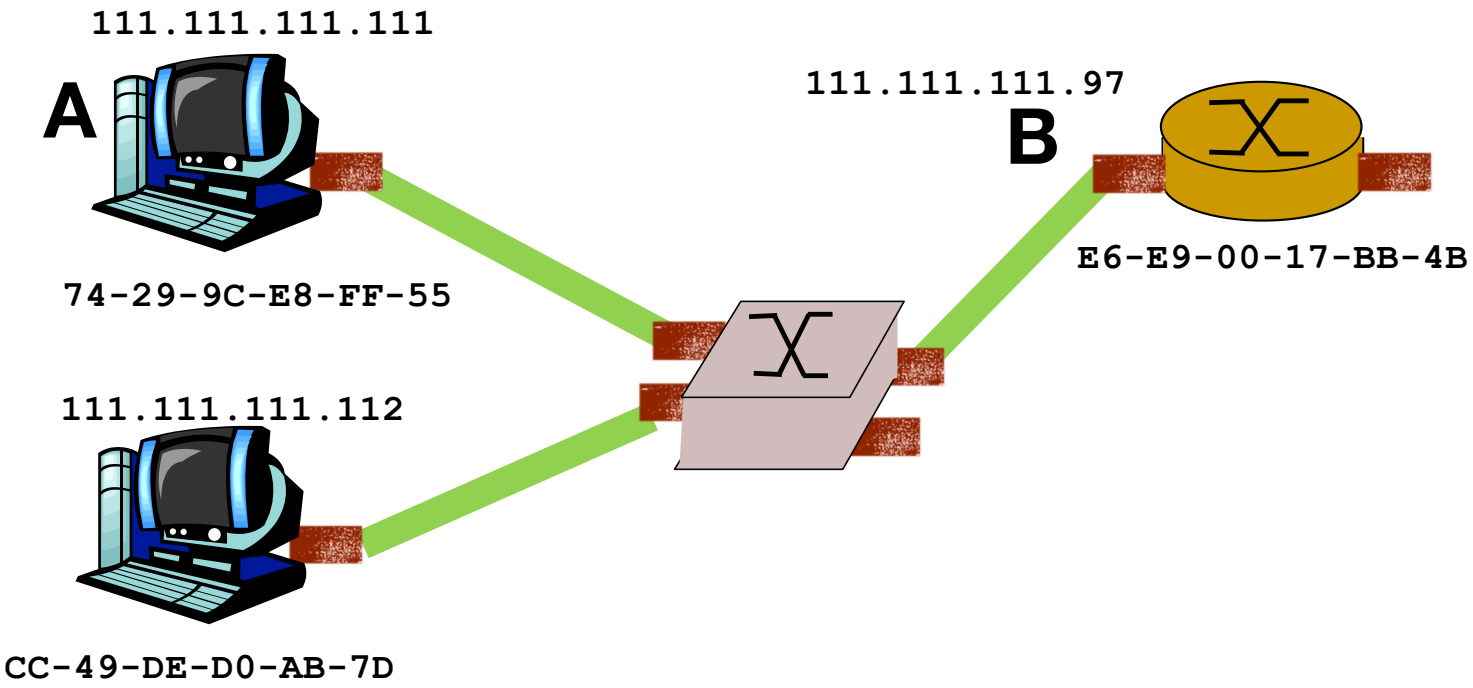
Usually IP

6 byte | 4 byte (for Eth|IP)

1: request, 2:reply

What do we do with it?

LOCAL AREA NETWORK 111.111.111.96/27



ARP REQUEST

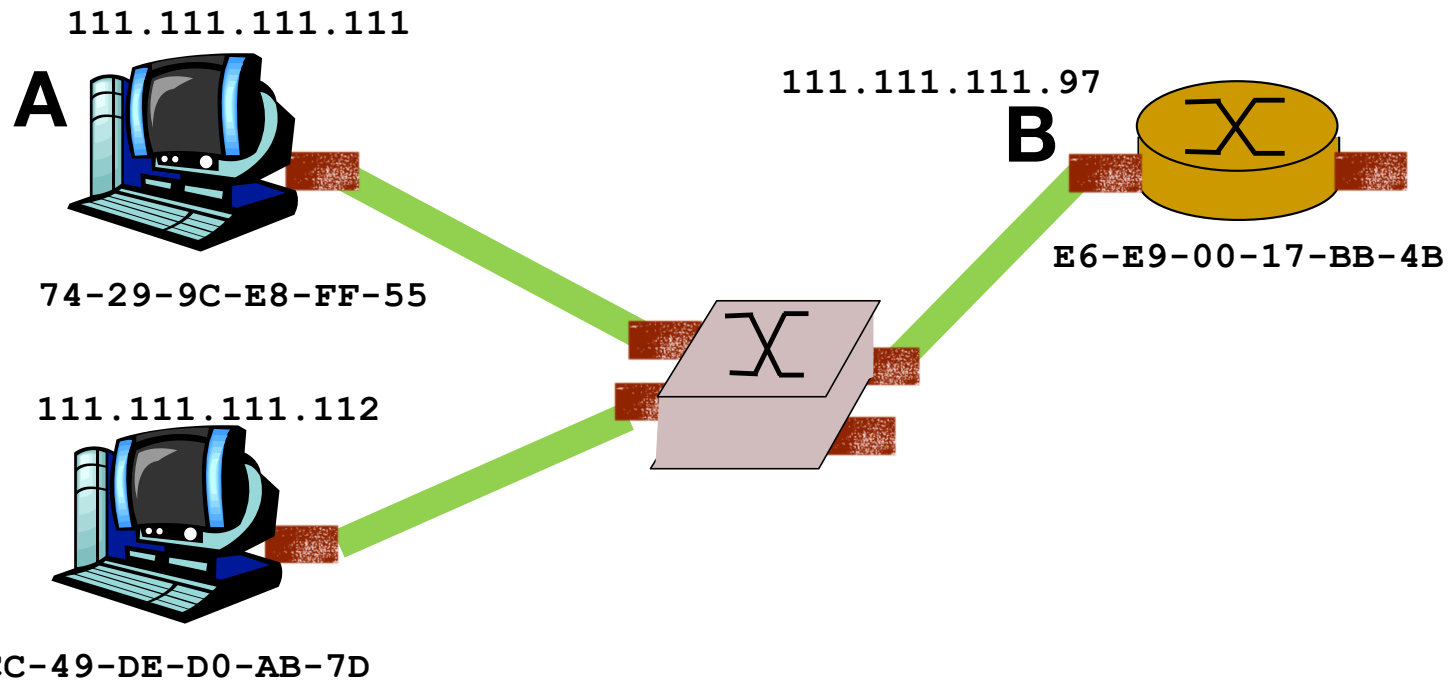
Destination: BCAST Source: A's MAC

FF:FF:FF:FF:FF:FF	74:29:9C:E8:FF:55	ARP

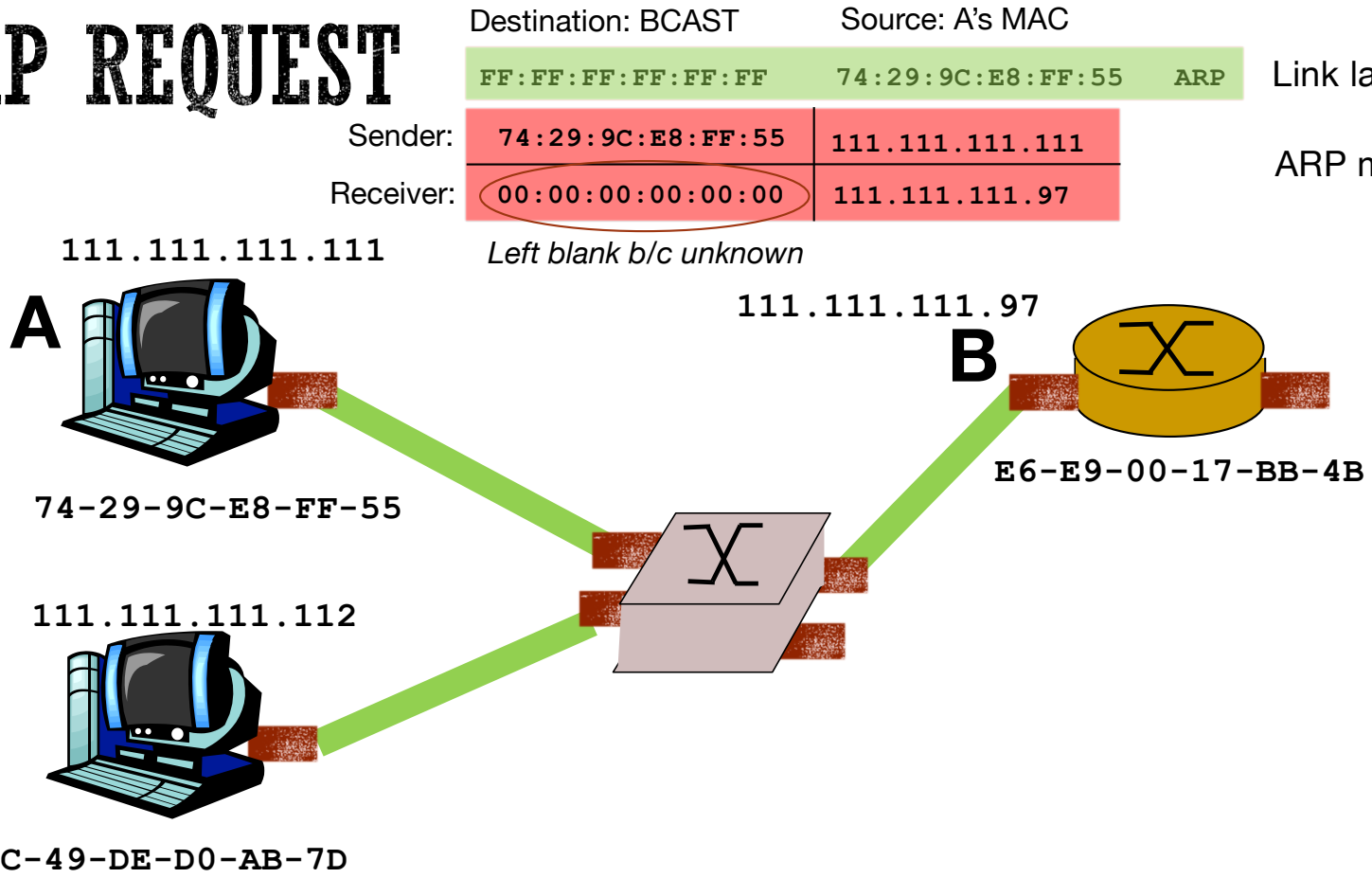
Link layer header

Sender:	74:29:9C:E8:FF:55	111.111.111.111
Receiver:	00:00:00:00:00:00	111.111.111.97

ARP message

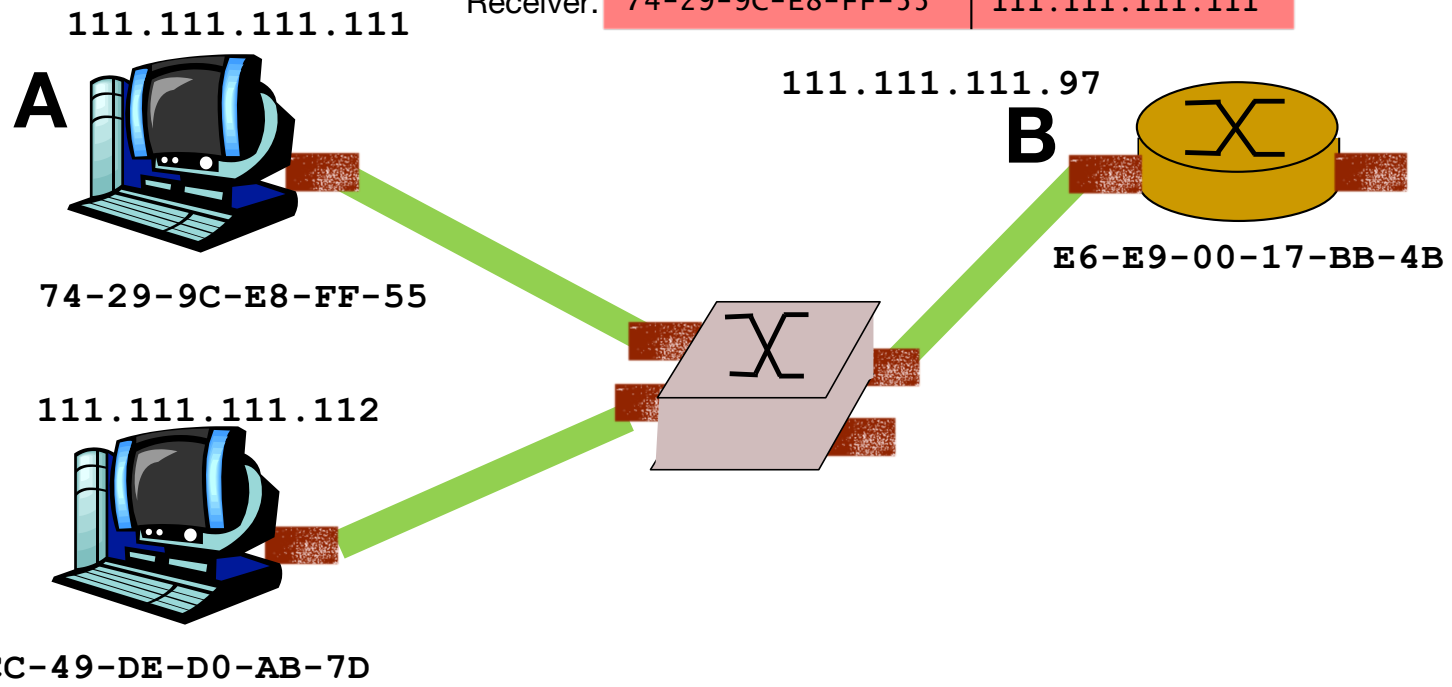


ARP REQUEST

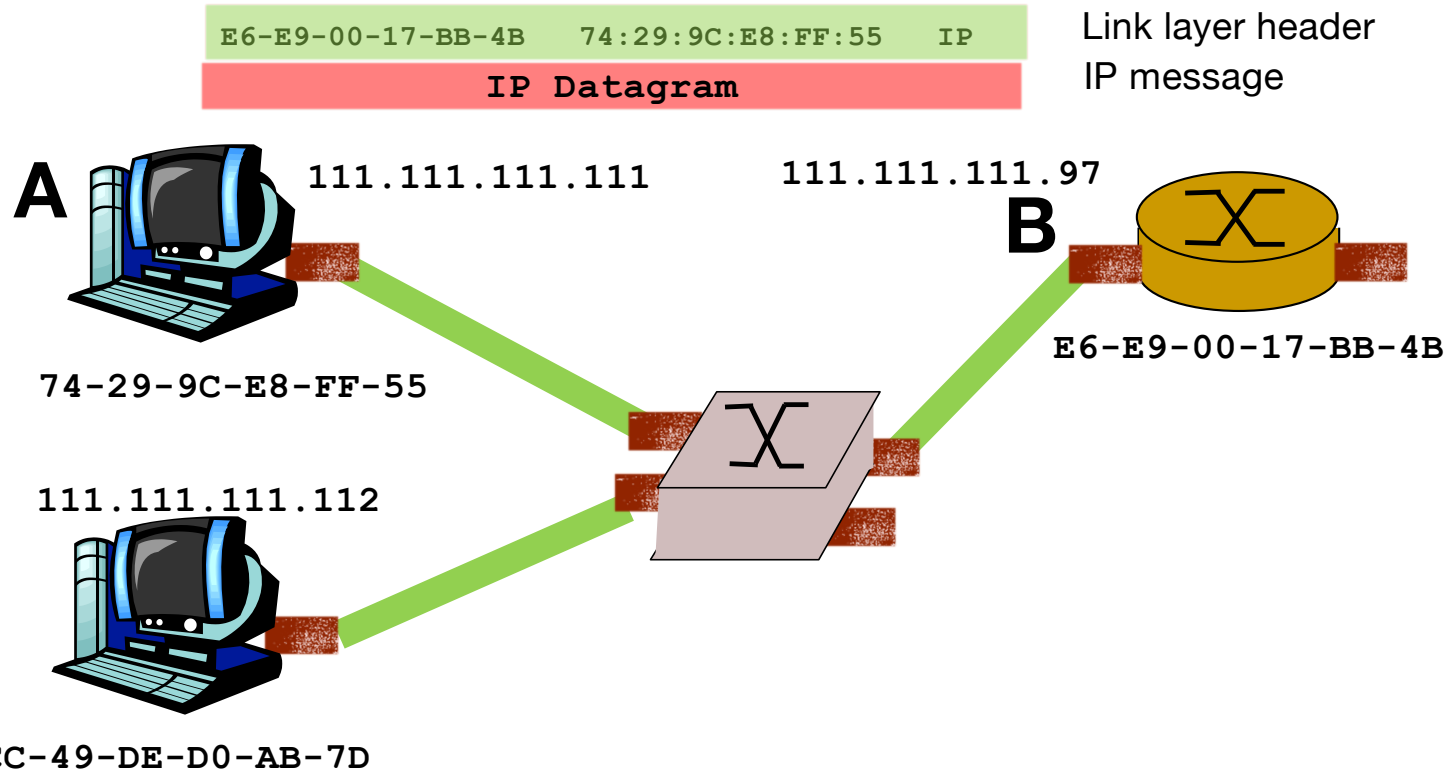

Destination: BCAST
Source: A's MAC
FF:FF:FF:FF:FF:FF
74:29:9C:E8:FF:55
ARP
Link layer header
Sender:
74:29:9C:E8:FF:55
111.111.111.111
Receiver:
00:00:00:00:00:00
111.111.111.97
ARP message
Left blank b/c unknown
111.111.111.111
A
74-29-9C-E8-FF-55
111.111.111.97
B
E6-E9-00-17-BB-4B
111.111.111.112
CC-49-DE-D0-AB-7D

ARP REPLY

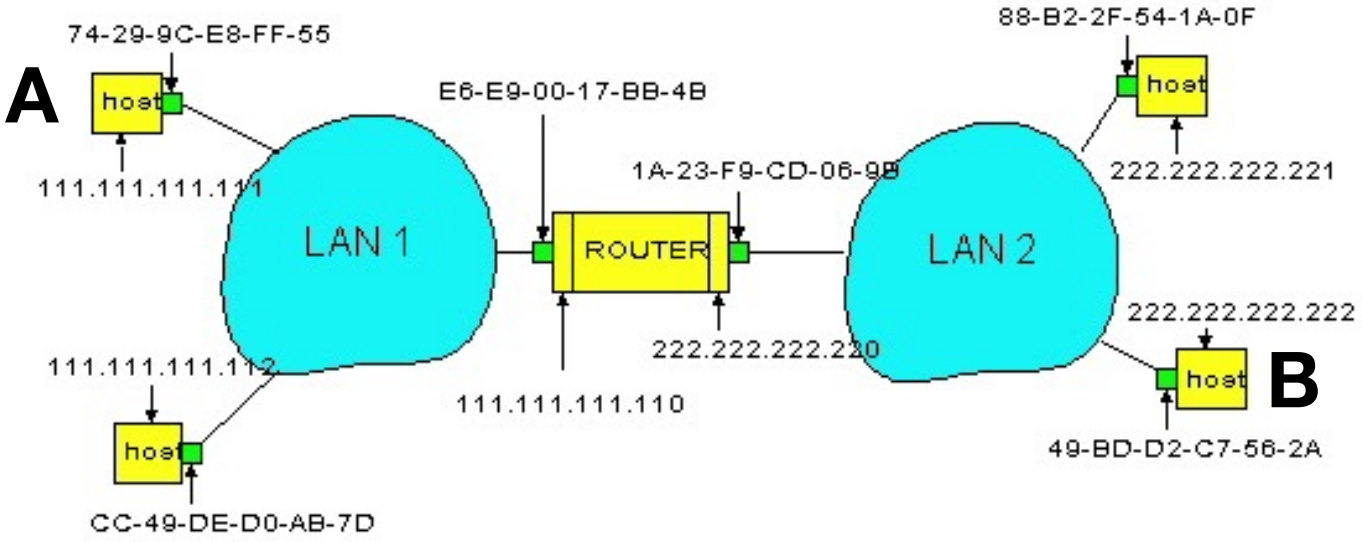
	Destination: A's MAC	Source: B's MAC	
	74-29-9C-E8-FF-55	E6-E9-00-17-BB-4B	ARP
Sender:	E6-E9-00-17-BB-4B	111.111.111.97	
Receiver:	74-29-9C-E8-FF-55	111.111.111.111	



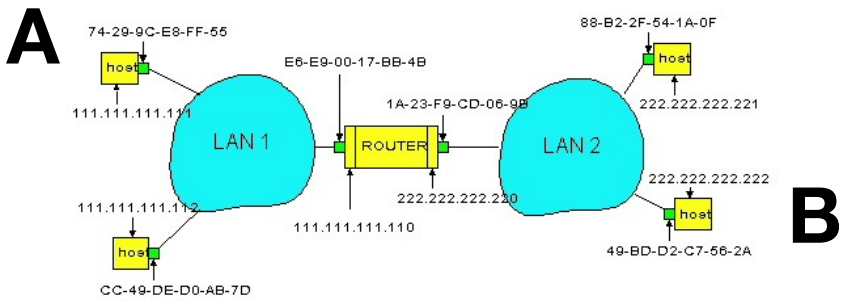
SENDING THE IP DATAGRAM

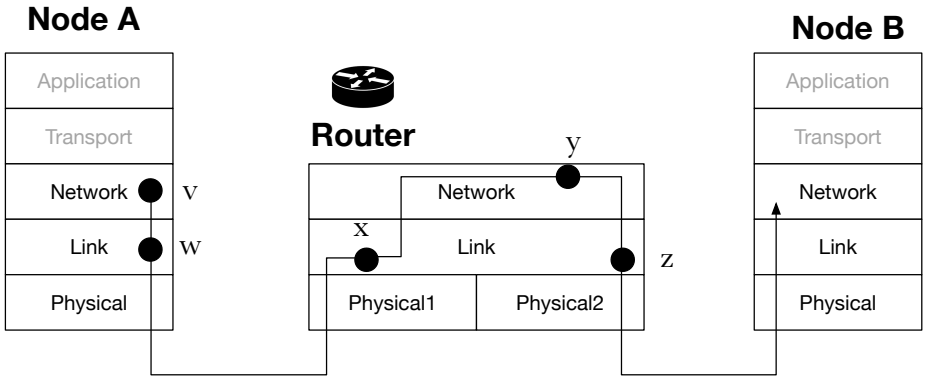


HOW DOES THIS WORK WITH IP ROUTING?



HOW DOES THIS WORK WITH IP ROUTING?





FUN FACTS ABOUT ARP

- ARP is stateless, always read a response even if it didn't make a request
- ARP is not authenticated, anyone can ARP
- ARP can be spoofed – I can attempt to "hijack" another host's IP address by responding to ARP requests, or sending replies that no one asked for
- ARP works in a single "broadcast domain"
- Reverse-ARP used to be used to get an IP address but is now obsolete. We use DHCP instead.

IN-CLASS

- ICA72