

CS118 Discussion 1A, Week 8

Yunqi Guo

Boelter Hall 5422, Friday 10:00—11:50 p.m.

Outline

- Lecture review:
 - Link layer
- Project 2 questions

Link layer: introduction

- understand principles behind link layer services:
 - data framing
 - error detection, correction — CRC (cyclic redundancy check)
 - sharing a broadcast channel: multiple access
 - link layer addressing
- local area networks: Ethernet, VLANs

Delivering packet at link layer

- Basic communication models
 - Unicast
 - Broadcast
 - Multicast
- What, how, why?

Broadcast

- Replicate at source, or in-network
- Flooding (FYI)
 - Reverse path forwarding (RPF)
- Spanning tree

Multicast (FYI)

- Address range
 - class-D IP: 224.0.0.0 — 239.255.255.255
- Protocols:
 - IGMP
 - DVMRP, PIM

Medium Access Links and Protocols

- Two types: point-to-point, broadcast
- **Broadcast** channel shared by multiple hosts
 - What if we only have unicast channel?
 - What's the pros and cons for a broadcast channel?
- Three classes of Multiple Access Control (MAC) protocols
 - Channel partitioning: FDMA, TDMA, CDMA
 - Random access: Aloha, CSMA/CD, Ethernet
 - Taking turns: Token ring/passing
 - **Pros and cons for each class of protocol?**

Random access: slotted ALOHA

- Assumptions:
 - all frames same size
 - time divided into equal size slots (time to transmit 1 frame)
 - nodes start to transmit only slot beginning
 - nodes are synchronized
 - if 2 or more nodes transmit in slot, all nodes detect collision

Random access: slotted ALOHA

- suppose: N nodes with many frames to send, each transmits in slot with probability p
- $\text{Pr}(\text{given node has success in a slot}) = p(1-p)^{(N-1)}$
- $\text{Pr}(\text{any node has a success}) = Np(1-p)^{(N-1)}$
- max efficiency: find p^* that maximizes $Np(1-p)^{(N-1)}$
- Take the limit of $Np^*(1-p^*)^{(N-1)}$ as N goes to infinity, yields:
 - max efficiency = $1/e = .37$

Random access: ALOHA efficiency

- Slotted ALOHA max efficiency = $1/e = .37$
- Unslotted ALOHA max efficiency = $1/2e = .18$

CSMA (carrier sense multiple access)

- Listen before transmit:
 - if channel sensed idle: transmit entire frame
 - if channel sensed busy, defer transmission
 - “don’t interrupt others!”
- Channel busy?
 - 1-persistent CSMA: retry immediately
 - p-persistent CSMA: retry immediately with probability p
 - Non-persistent CSMA: retry after a random interval
- Collision?
 - hidden terminal problem

CSMA/CD (collision detection)

- CSMA/CD: carrier sensing, deferral as in CSMA
 - collisions detected within short time
 - colliding transmissions aborted, reducing channel wastage
- collision detection:
 - easy in wired LANs: measure signal strengths, compare transmitted, received signals
 - difficult in wireless LANs: received signal strength overwhelmed by local transmission strength

CSMA/CD (collision detection)

- A: sense channel, wait if necessary, when channel is idle, transmit and monitor the channel
- If detect collision then {
 - abort and send jam signal;
 - update collision-count ($n++$);
 - delay for K slots (1 slot = 512bits transmission time) goto A
- } else {finish sending the frame; reset collision-count ($n = 0$)}
- collision detection: compare transmitted, received signal strengths

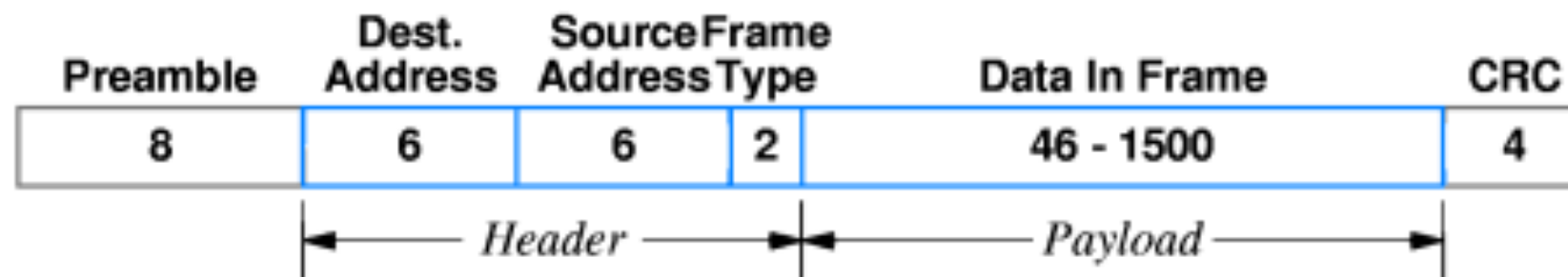
Ethernet

- Connectionless and unreliable protocol
 - Why doesn't Ethernet provide reliable data transfer?
- MAC protocol: CSMA/CD + exponential backoff
 - Can we use CSMA/CD in wireless network?
- Switch-based Ethernet
 - No real broadcast channel anymore
 - Self-learning algorithm: support plug-and-play
 - **Differences between routing table, switch table and ARP table?**

MAC address

- MAC address allocation by IEEE (who assigns IP?)
- MAC address is flat -> portability (IP address is ____?)
- Format: 48 bit address
 - AA-BB-CC-DD-EE-FF
 - Broadcast address: FF-FF-FF-FF-FF-FF

Ethernet Frame



- Min frame size: 64 Bytes
 - why? (to reliably detect collisions)
- Max frame size: 1514 Bytes
 - why? (to fair share the media)

Ethernet CSMA/CD

- 1. NIC receives datagram from network layer, creates frame
- 2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
- 3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !
- 4. If NIC detects another transmission while transmitting, aborts and sends jam signal
- 5. After aborting, NIC enters binary exponential backoff:

Switch

- Examine each incoming frame's MAC address, forward to the destination LAN if dest. host is on a different LAN
- store-and-forward
- switch table: self-learning algorithm
 - (MAC address of host, interface to reach host, timestamp)

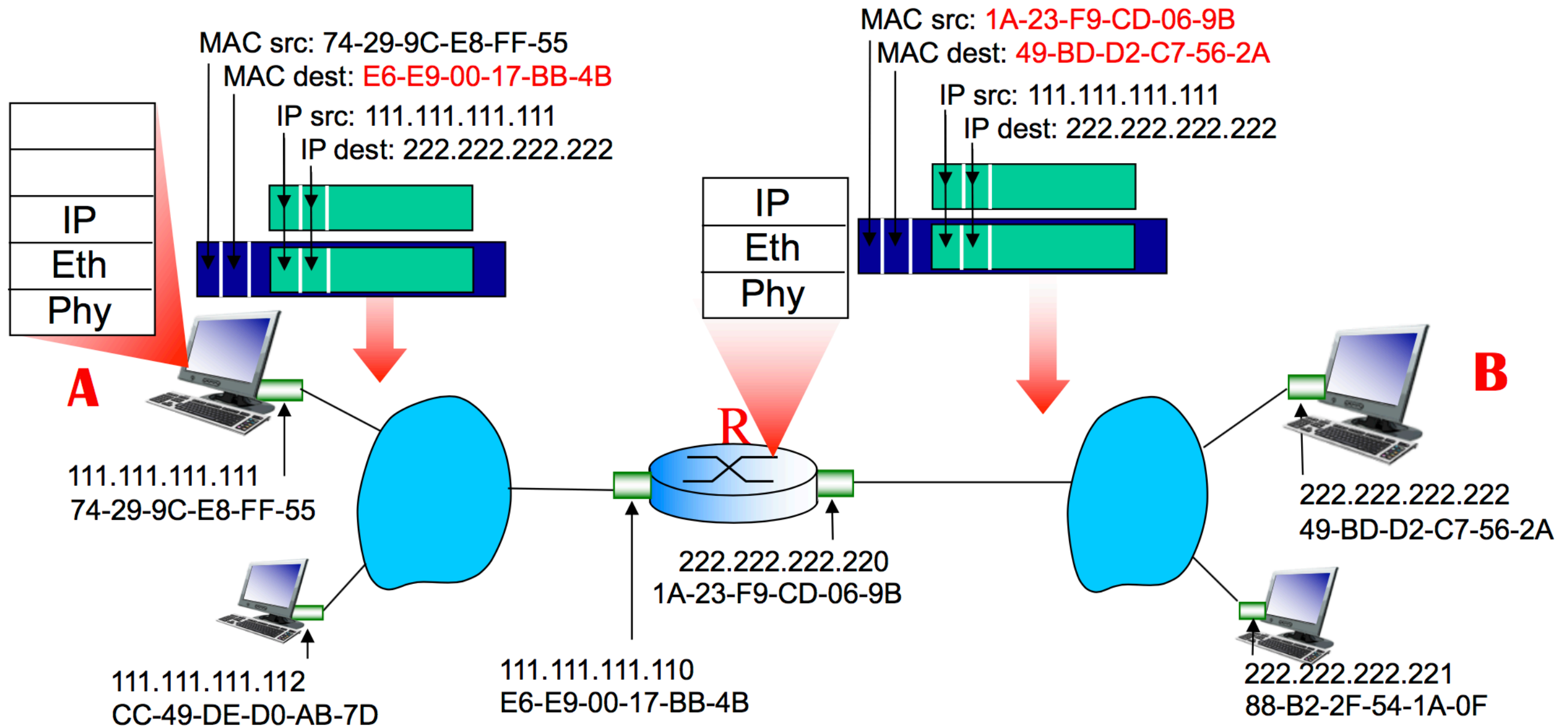
ARP: address resolution protocol

- How to determine interface's MAC address, knowing its IP address?
- ARP table: each IP node (host, router) on LAN has table
 - IP/MAC address mappings for some LAN nodes:
 - <IP address; MAC address; TTL>
 - called PnP (plug-and-play)
- soft-state design: information deletes itself after certain time unless being refreshed

ARP: send an IP packet in the same subnet

- A wants to send IP packet to B, but B's MAC address not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address (all nodes on LAN receive ARP query)
 - dest MAC address = FF-FF-FF-FF-FF-FF
- B receives ARP packet, replies to A with its (B's) MAC address
 - frame sent to A's MAC address (unicast)
- A caches IP-to-MAC address pair in its ARP table until information becomes old (times out)

ARP: send an IP packet across subnets



ARP: send an IP packet across subnets

- Find an entry in the **routing table**
- If entry is saying that packet can be sent directly
 - Lookup MAC for destination IP in **ARP table**
- If entry is saying that packet should be set to the gateway
 - Lookup MAC for the gateway's IP in **ARP table**
- Create frame with the found MAC and original IP packet as a payload
- Send the frame

ARP: send an IP packet across subnets (cont'd)

- Router or node receives the frame, as it is destined to it
- Router removes Ethernet header, finds IP destination address
 - If IP is itself, deliver to transport layer and higher layers
 - If IP is not self and node is router, repeat the previous steps (lookup routing table, lookup ARP, ...)

Router vs. Switch

- Both are store-and-forward devices
 - routers: network layer devices (examine IP headers)
 - switches: link layer devices (examine Ethernet headers)
- Circuit-switch network: connection should be established before forwarding the data
 - At each hop, the circuit path is marked as a label
 - Data forwarding is based on label: **$O(1)$ complexity**
 - **Vulnerable to link/node failures**
- Packet-switched network: connectionless, packets are forwarded based on IP header
 - Longest prefix matching: **$O(N)$ complexity**
 - **Robust to link/node failures**
- **Can we take advantage of both, while preventing any vulnerabilities?**

Network devices

- Repeater: PHY layer
 - bits coming in one link go out all other links at same rate
- Hub: link layer
 - packets coming in one port/link, go out all other ports/links
- Switch: link layer