Exploration: MAC addresses and the Address Resolution Protocol

Introduction

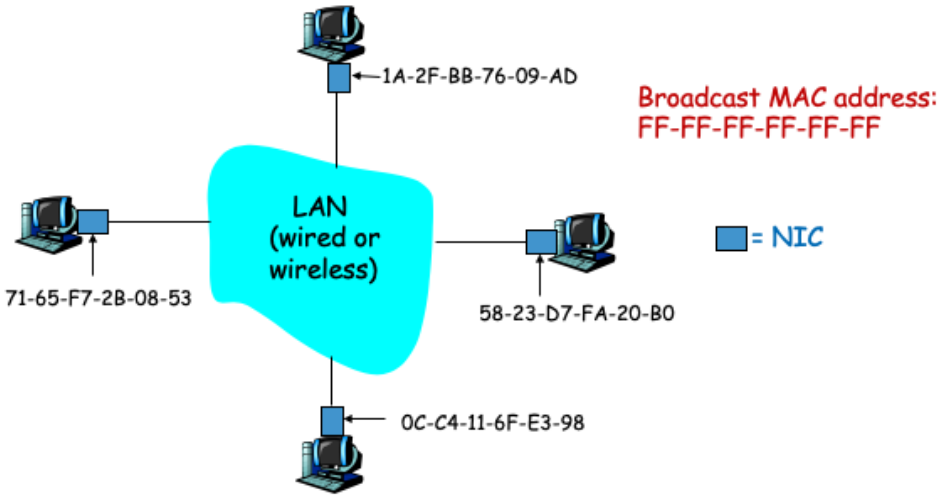
In this lecture we will discuss what hardware addresses really are. We will also answer an important question: How are hardware addresses and IP addresses related? That problem will be answered with the ARP…

MAC addresses

We have talked all along about IP addresses. But IP addresses are a virtual address. IP addresses are used to get the datagram to the destination's subnet. And then that subnet is responsible for moving the datagram to the destination host.

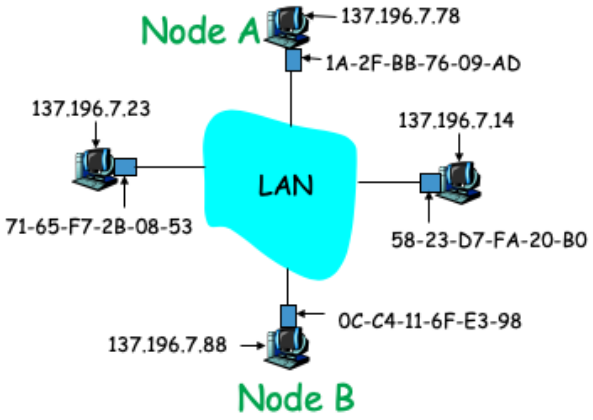
In contrast, the MAC address is a physical network address in the same network as the sender. It is used to communicate to the next node in the path. Every communication at the physical layer is sent to a MAC address. Every NIC card in the world must have a unique MAC address! But how?

A MAC address is 48 bits and is burned into the ROM on the NIC card by the manufacturer. It would be impossible to administer MAC addresses in the same way that IP addresses are administered. IP addresses are hierarchical, unlike MAC addresses, which are only from node to node. Instead, a portion of the MAC address space is allocated by the IEEE to each of the card manufacturers. MAC addresses are plug-and-play portable.



Above we see a diagram of a LAN. The LAN could be wired or wireless. Each NIC card on the LAN has a unique MAC address. They are 48 bits shown here in hexadecimal. The NIC cards also have a broadcast MAC address, that can be used for the ARP. That's a MAC address that is 48 binary 1s, written here in hex.

If you already know a hardware address inside a LAN, communication can take place inside the LAN. All of the nodes are adjacent to each other, so they can communicate by sending frames to that address. But what happens if the address is not known?



In the scenario depicted above, **A** wants to send a frame to **B**. **A** knows **B**'s IP address, but does *not* know **B**'s MAC address. It cannot send the frame, because at this layer, the MAC address must be known in order to send data.

The ARP or address resolution protocol is what solves this dilemma. Each IP node on the LAN has an ARP table. The ARP table as you might have guessed, maps the IP and MAC address for some of the LAN nodes. Each table entry has just 3 entries per node: The IP address, MAC address, and Time-to-Live (TTL).

The TTL in this case is a time (usually in min) after which the table entry will be removed (typically 20 min). That is to keep the table simple, and to keep only the most frequently visited nodes in the table. Another reason for expiring table entries is that IP addresses can change, and NIC cards can be swapped out (plug-and-play operation).

Assuming B's MAC address is in the ARP table, the following will happen:

- A looks up B's MAC address in its ARP table
- A encapsulates B's MAC into the frame
- A broadcasts the frame into the medium, and many hosts receive the transmission
- Only B accepts the frame

ARP

What if B's MAC address is not in the ARP table? It is ordinarily very easy to find out what a node's IP address is. A node can run a DNS query and find that out very easily.

In the case where you have the IP address of an adjacent node, but do not know the node's MAC address, the following will happen:

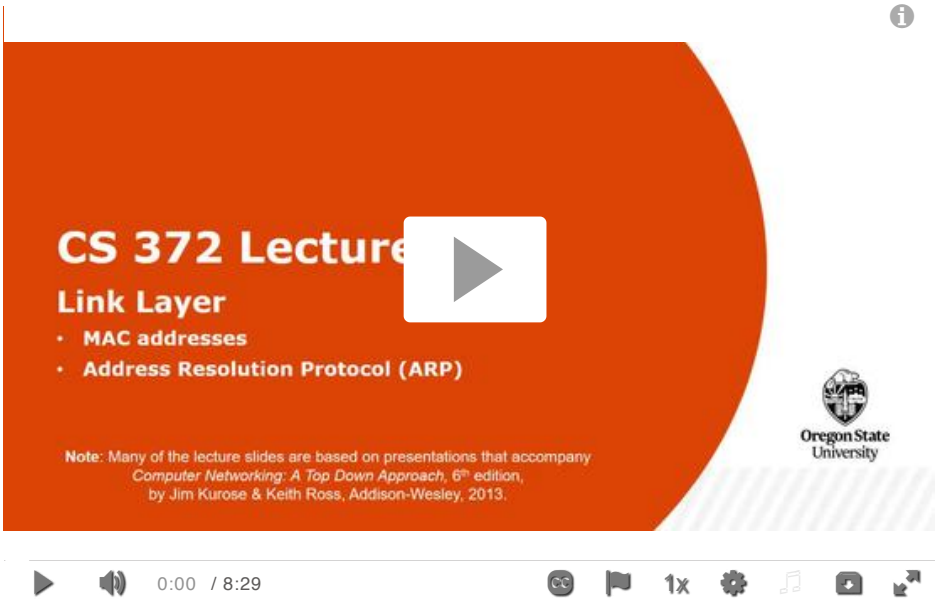
1. In this case, A will broadcast an ARP query packet that contains B's IP address. This broadcast MAC address is FF-FF-FF-FF-FF-FF
2. all machines on LAN receive ARP query
3. B receives ARP packet, replies to A with B's MAC address
4. A sends frame to B since it now knows its MAC address
5. A caches IP-to-MAC address pair in its ARP table until information times out (TTL)
6. Now, with B's MAC address in the ARP table, the sender may send the frame to B.

ARP is plug and play - nodes create their ARP tables without intervention from network administrator!

This concludes our discussion of MAC addresses and ARP. Be sure to watch the video lecture below for more in-depth details on ARP. Then head to the included Self-Check exercises to test your knowledge.

Video Lecture

Link Layer - MAC Addresses



(PDF (https://oregonstate.instructure.com/courses/1798856/files/83165274/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165274/download?wrap=1) |PPT (https://oregonstate.instructure.com/courses/1798856/files/83165135/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165135/download?wrap=1))

Self-Check Exercises

Self-check exercises: **W9E4 - MAC addresses and the ARP.pdf** (https://oregonstate.instructure.com/courses/1798856/files/83165094/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165094/download?wrap=1)

Self-check exercises with solutions: **W9E4 - MAC addresses and the ARP - Solutions.pdf** (https://oregonstate.instructure.com/courses/1798856/files/83165072/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165072/download?wrap=1)