# HARDWARE ADDRESSING AND FRAME TYPE IDENTIFICATION

# Physical/Hardware Addressing

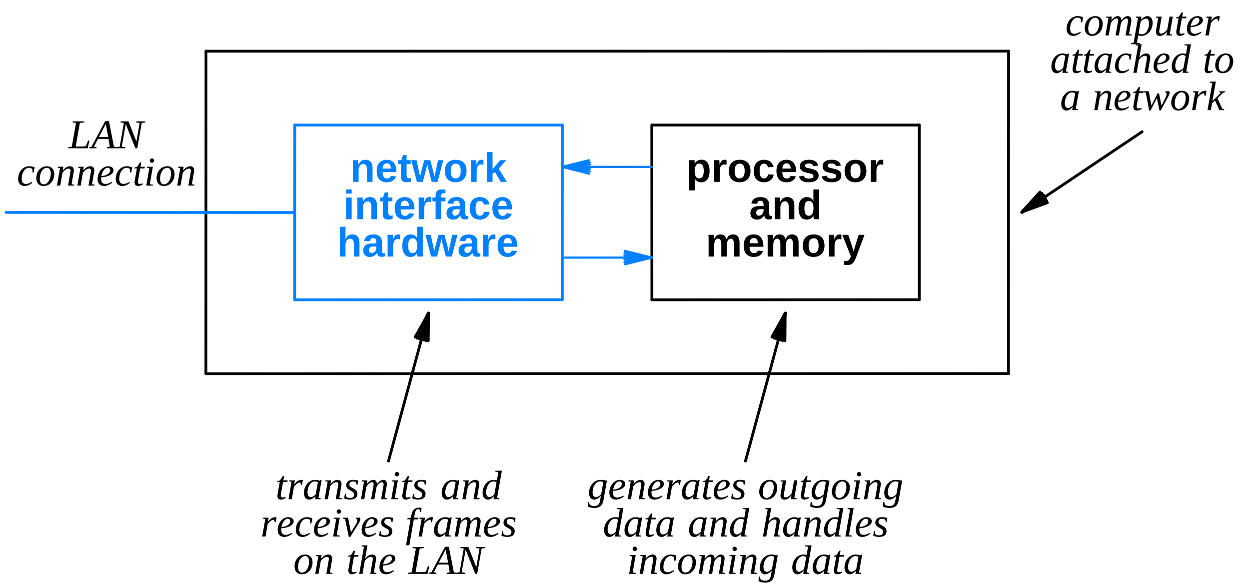
- A LAN provides a physical path from one computer to all other computers
- Complete physical connectivity by itself does not solve the communication problem
- The formats and the rules that govern the communication are as important as the physical connections
- How does a single pair of computers communicate across a LAN without forcing other computers to receive and process a copy of each message?
- An answer: when composing a frame, a sender must specify the recipient(s) of the frame
- Each computer in the LAN is assigned a "*unique*" numeric value called *physical address*, *hardware address*, or *media access address*
- Note that: the IP address is not the physical address

## A Transmitting/Receiving Scenario

- When transmitting a frame across a LAN, the sender includes in the frame the hardware address of the intended recipient, i.e., the *destination address*
- The LAN hardware on each computer checks the address of each incoming frame to determine whether it should accept the frame or not
- The sender also includes its own hardware address in the frame, i.e., the *source address*, to make it easy for the recipient to generate a reply/acknowledge, in case of successful transmission
- How about unsuccessful transmission;
  Should a recipient report this error to the sender?

## How LAN Uses Addresses to Filter Packets

- The LAN hardware in a computer is completely separated from the computer's CPU and memory; in fact the LAN hardware often contains its own CPU, ROM, and RAM
- The LAN interface hardware handles all the details of sending/receiving frames on the shared medium, including:
  - Waiting for an access to the shared medium
  - Transmitting frames
  - Receiving frames
  - Checking the minimum/maximum sizes in the coming frames
  - Checking the CRC
  - Discarding frames that contain errors




Organization of the hardware in a computer attached to a LAN

- The LAN interface hardware uses physical addressing to prevent the computer from receiving all frames that travel across the LAN
  - Once the LAN interface hardware has captured a complete frame, it compares the destination address in the frame to its physical address
  - If addresses match, it accepts the frame and passes it to the operating system
  - If addresses do not match, it discards the frame and waits for the next frame to appear

## Physical Addressing Schemes

- There are three main addressing schemes
  - Static addressing scheme
  - Dynamic addressing scheme
  - Configurable addressing scheme

## Static Addressing Scheme

- A unique 48-bit address
- Unique throughout the world
- Assigned when a Network Interface Card (NIC) manufactured
- Does not change unless the hardware (i.e., the NIC) is replaced
- Standardized by IEEE

## Dynamic Addressing Scheme

- Provides a mechanism that automatically assigns a physical address to a station when the station first boots
- Requires a station to try random numbers until it find a value that no other computer is using it as an address, e.g., a station might choose the current time of day as an initial value
- A computer might obtain a different address each time it restarts
- Depends on which addresses other computers are using when a computer boots
- Uniqueness is only important within a single LAN
- Other computers must learn the new address before they can communicate
- Eliminates the need for hardware manufacturers to coordinate in assigning addresses
- If a network is temporarily disconnected, two booted computers may choose the same physical address (a problem)

## Configurable Addressing Scheme

- Provides a compromise between the static and dynamic schemes
- Allows a customer to set the physical address of the NIC card
- Once selected, it becomes permanent, i.e., remains the same across reboots
- Uniqueness is only important within a single LAN
- Eliminates the need for hardware manufacturers to coordinate in assigning addresses
- Usually, administrators choose to assign configurable addresses sequential values
- In case of hardware failure and replacement is a must, the same physical address can be re-assigned to the new NIC

## Destination Addressing Types

- Network destination addresses can be classified into three basic types:
  - Addresses correspond to a single computer each *(unicast)*
    - Only one computer, if any, will accept the frame; all other network hardware interface will reject it
    - Efficient for interactions between two computers
  - One address for all computers *(broadcast)*
    - No additional hardware is needed, this is because all station connect directly to the shared medium
    - Needs a special reserved address known as *broadcast address*
    - Efficient when you want to send a message to all computers
    - If it is not carefully used, it leads to wasting the computer CPU time to reject frames, i.e., accepted by the network hardware and then rejected by the computer (e.g., junk mails)

- Addresses correspond to a set of computers each *(multicast)*
  - Takes advantage of the broadcast capabilities without wasting the CPUs on other computers
  - The network interface hardware must be programmed with the specifications of which multicast frames to accept and which to reject; i.e., the network interface hardware takes the decision and filter out the unwanted junk mail
    - If an application on the computer wishes to receive multicast frames, it must inform the network interface which multicast address to use
    - The interface adds the address to the set it will recognize, and begins accepting frames sent to that address
  - Efficient for transmitting to a subset of computers

## When Does A Frame Get Accepted And Sent To The CPU?

- A conventional network interface must examine the destination address of each frame that is sent over the network
- The interface passes a copy of the frame to the local system for processing if, and only if, the CRC check is Ok, and the destination address in the frame matches
  - The computer's address
  - The special broadcast address
  - One of the pre-approved multicast addresses

  Otherwise, the interface discards the frame without using the computer's CPU

# Network Analyzers

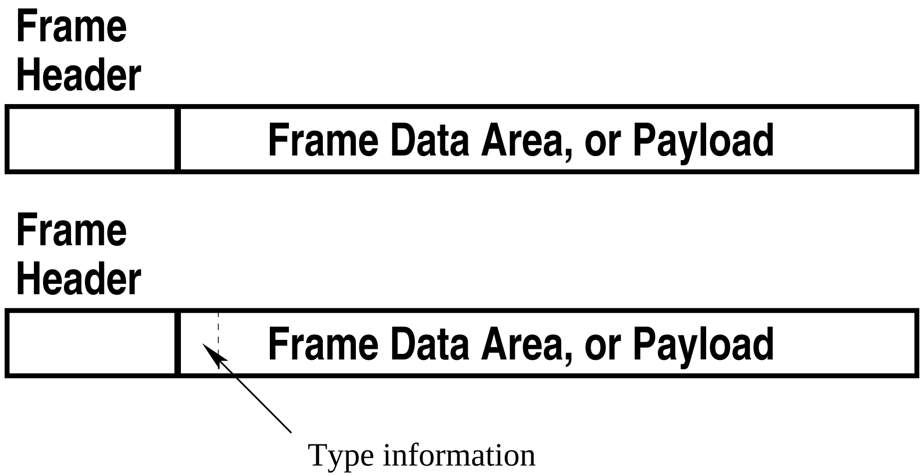
- A network analyzer, a.k.a. network monitor, is a device that can be configured to read and then count, display, or analyze frames as they pass across a shared network
- To do so, the NIC card of this device must be placed into *promiscuous mode*
- When being in a promiscuous mode an NIC connected to a shared network captures all frames, including frames destined for other computers
- Almost all commercially available NIC supports promiscuous reading
- Switching an NIC into promiscuous mode is usually trivial
- Promiscuous mode is useful for network monitoring, however, it presents a security risk
- in General, messages sent over a LAN are not guaranteed to be private

## Identifying Packet Contents

- To inform the receiver about the frame content, each frame should contain additional information that specifies the type of the contents
- Using this additional information, the network software may reject frames, or pass the frame to the correct software module
- There are two possibility
  - Explicit frame type
    - Included in the frame header (frame-type field)
    - Its values and its meaning are identified by the network hardware designers
  - Implicit frame type
    - Not included in the frame header
    - The sender and receiver must agree
      - On the contents of a frame (seldom used)
      - To use the first few bytes of the data field to store the frame-type information

# General Frame Format

- A frame consists of two parts
  - Header
    - Contains addresses
    - May contain the frame-type information
    - Has a fixed layout
  - Data area, a.k.a. payload
    - Contains the data being sent
    - Might start with few bytes to represent the frame-type information




Two possible formats of a frame sent across a LAN

# An Example Of A Frame Format

| Preamble | Dest. Address | Source Address | Frame Type | Data In Frame | CRC |
|---|---|---|---|---|---|
| 8 | 6 | 6 | 2 | 46 - 1500 | 4 |
| | *Header* | | | *Payload* | |

Illustration of the original frame format used with Ethernet

- The 64-bit preamble contains alternating 1s and 0s that allow the receiver's hardware to synchronize with the incoming signal
- The 64-bit preamble is not a part of the header
- The first two field of the header contain physical addresses
- Ethernet uses a 48-bit static addressing type, in which each device is assigned a unique address by the manufacturer
- The third field of the header is a 16-bit frame-type
- The payload field is a variable length field from 46 to 1500 bytes
- The 32-bit CRC field comes after the frame; (it is a part of the header)

- This Example, in fact, is the original DIX (Digital Intel Xerox) Ethernet standard
- IEEE 802.3 standard (IEEE, 1985) suggested a format similar to the DIX Ethernet standard format, except
  - The third field of the header is a 16-bit length of data, instead of frame-type
  - The frame-type is added to the first few bytes of the payload