Data link Layer addressing

Directing data is what addressing is all about. At the Data Link layer, this is done by pointing PDUs to the destination MAC address for delivery of a frame within a LAN. The MAC address is the number that is assigned by the manufacturer of a NIC or a network interface. In Figure below, you can see a group of individuals sharing a physical medium. If Bob needs to send anything to Larry, he simply enters the MAC address (01:bb:04:af:00:1f) that is assigned to the NIC card on Larry's PC in the frame and sends it toward Larry's PC.

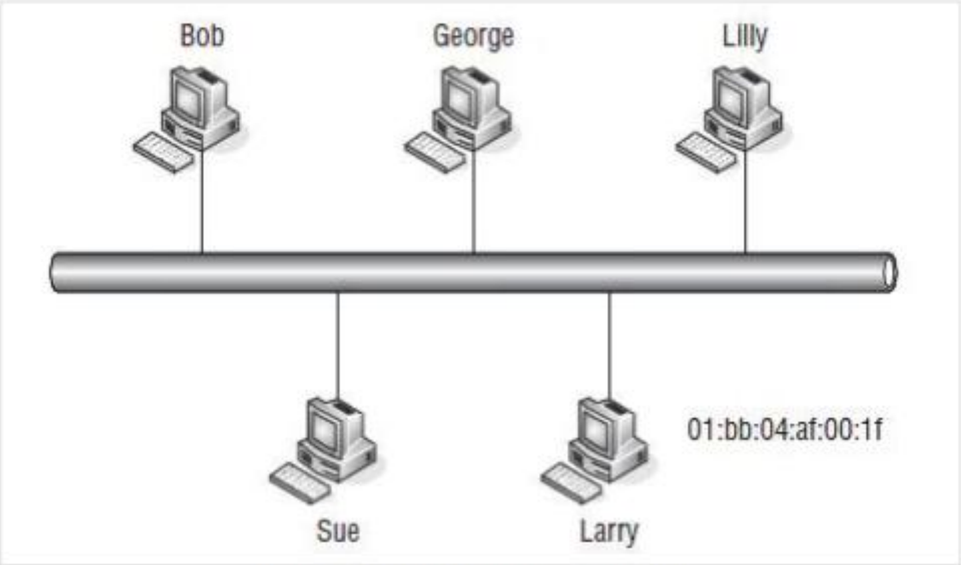
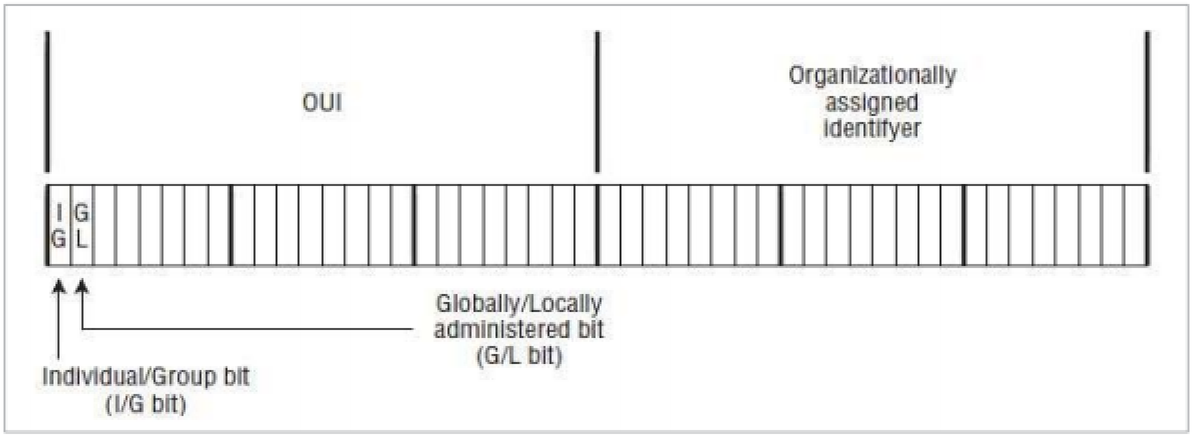


Figure: Data link layer frame delivery

The MAC Address Format

The MAC header of a frame contains the destination and source MAC addresses for the interfaces involved in the communication stream. Figure below shows the 48 bits that make up the MAC address.


OUI
Organizationally assigned identifyer
I G
G L
Globally/Locally administered bit (G/L bit)
Individual/Group bit (I/G bit)

MAC address format

The first bit (the I/G bit) identifies whether the source/destination target is an individual (unicast) or a group (multicast).

The second bit in the source and destination address field indicates whether the address is globally or locally unique. This bit is called the G/L bit and it identifies whether the organizational assigned identifier is globally unique (G/L bit set to 0) or locally unique (G/L bit set to 1). If it is a locally unique identifier, then the address is unique only to the LAN. Unicast Addressing A unicast address is simply the address of a particular node’s interface within the LAN. The unicast address is the MAC address that is assigned to a device or an interface within the LAN.

Unicasting

Unicasting is the act of sending a frame from one source node to a single destination node. Figure below shows an example of unicasting.

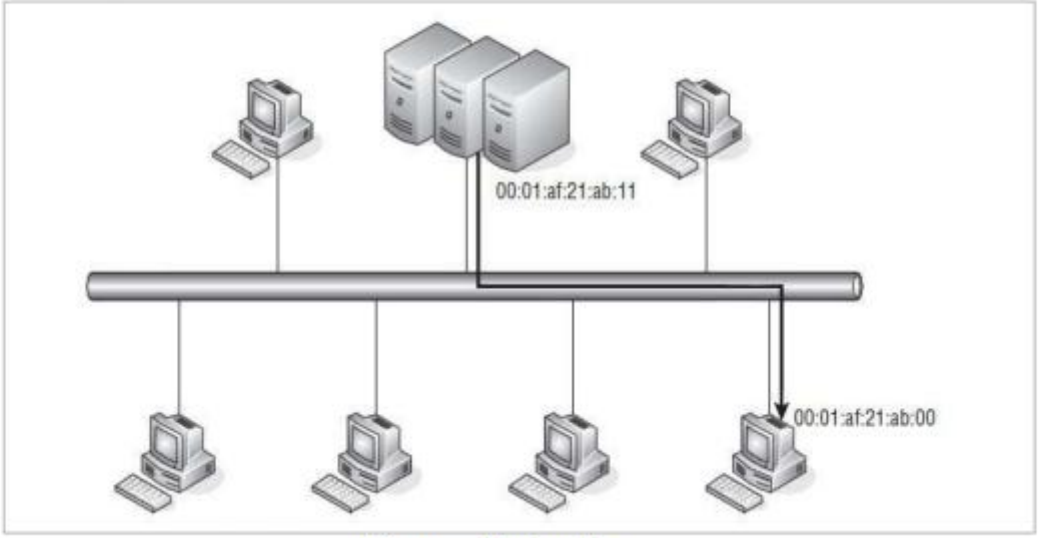
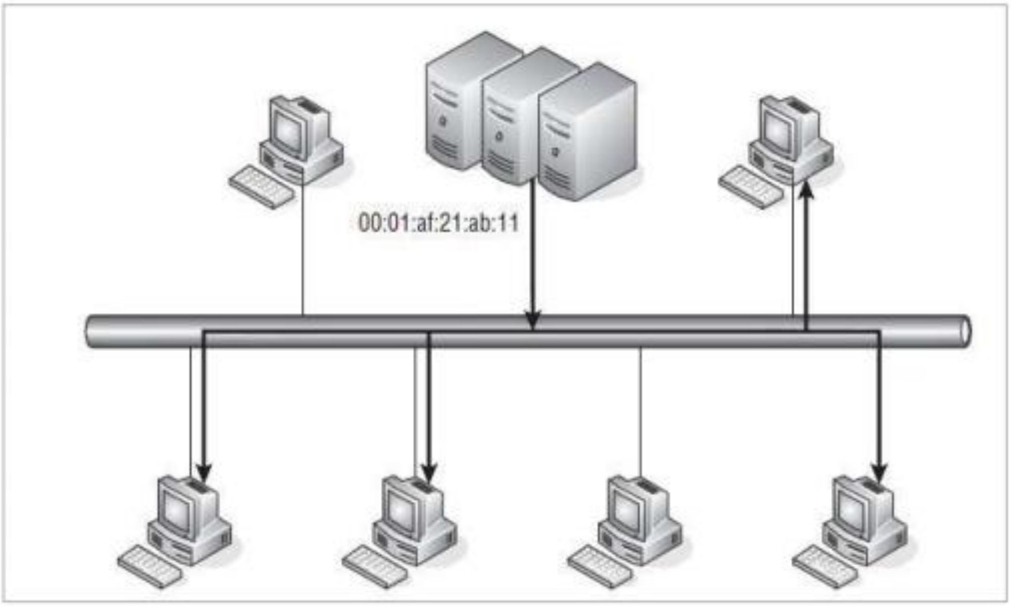


Figure: Unicasting

The figure shows the server sending data to a single node on the LAN. The unicast address of the source is 00:01:af:21:ab:11, which is the MAC address of the interface on the source side of the transmission. The destination unicast address is the MAC address of the interface used by the destination node —in this case, 00:01:af:21:ab:00. All transmitted frames during the session will use the same destination and source unicast addresses.

Multicast Addressing

Multicasting is the act of sending a message to multiple nodes. Multicasting can be handled at the Layer 3 level (IP multicasting) or at Layer 2 (Ethernet multicasting). Multicasting provides the ability for multiple nodes to receive data sent from a single transmission. Figure below shows an example of multicasting.



Notice that in the figure not all nodes are receiving the transmission that is being sourced from the server. This is because not all of the nodes are in the same multicast group. Also notice that the source address for the originator will be a unicast address. When a node decides to join a multicast group, it needs to determine if a received frame is a unicast or a multicast frame. NIC cards are configured to recognize when a frame is unicast and when it is not. This is the bit that identifies if the frame is a unicast (I/G bit set to 0) or multicast (I/G bit set to 1).

- **Broadcasting**

  Broadcasting is really nothing more than multicasting to everyone in the LAN.

Error Detection

Frames are either fixed-length PDUs or bit-oriented. Regardless of the frame type, errors can occur in the LAN, and frames can disappear, duplicate, and even become corrupted on their way to a destination. An error in a length-type frame can cause the frame to terminate and skew the beginning of a new frame. Likewise, a bit can be set incorrectly in a bit-oriented type frame, which can cause duplication and even deletion of the frame. Errors can be caused by numerous reasons, environmental as well as traffic related. Electrical interference can cause noise on the physical medium, which can corrupt the bits in the frame. **Other causes of transmission errors include:**

- Signal distortion
- Synchronization issues
- Crosstalk

There are two methods of error detection used at Layer 2,

- parity check and
- cyclic redundancy check (CRC)

Parity check —the simplest of the error-checking methods. This method adds a bit to a string of bits to ensure that the total number of 1s in the string is equal to an even or an odd number. For example: Odd parity— 01010101 + 1 parity bit = 010101011. Notice that the total number of 1s is an odd number. An odd parity bit is always set to 1 if the total number of 1s in the string (before the parity bit is considered) is an even number. By adding 1 to the even number, it ensures that the number is odd, which matches the type of parity in use in this case. Figure below shows an example of data transmission using odd parity.

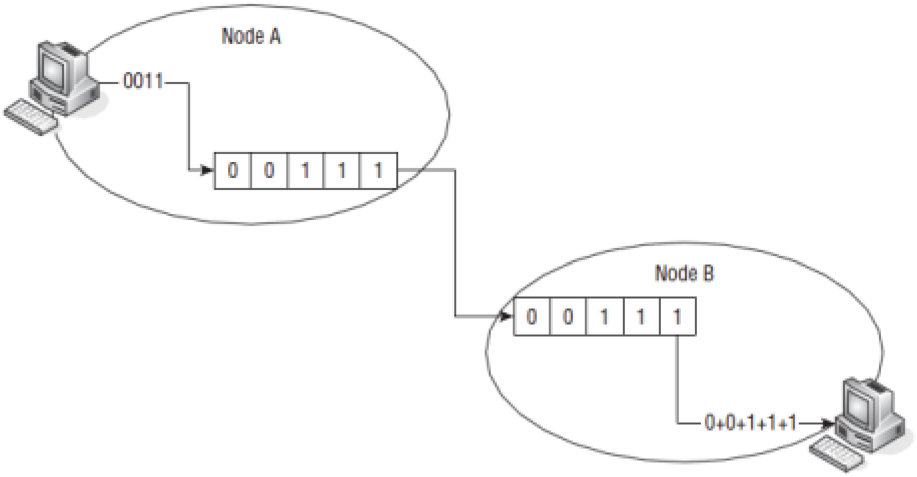


Figure: Odd Parity

In Figure above, node A wants to send the data stream 0011 to node B. Node A computes the value of the data stream (0+0+1+1)21 and because odd parity checking is being used, node A turns the parity bit on to 1 before it transmits the data. Node B then receives the data and computes the overall value (0+0+1+1+1), which is an odd value. Odd Parity is in use, so node B reports a good frame received. Even parity— 01010100 + 1 parity bit = 010101001. Notice that the total number of 1s is an even number. An even parity bit is always set to 1 if the total number of 1s in the string (before the parity bit is considered) is an odd number. By adding 1 to the odd number, it ensures that the number is even, which matches the type of parity in use in this case. Figure shows an example of data transmission using even parity.

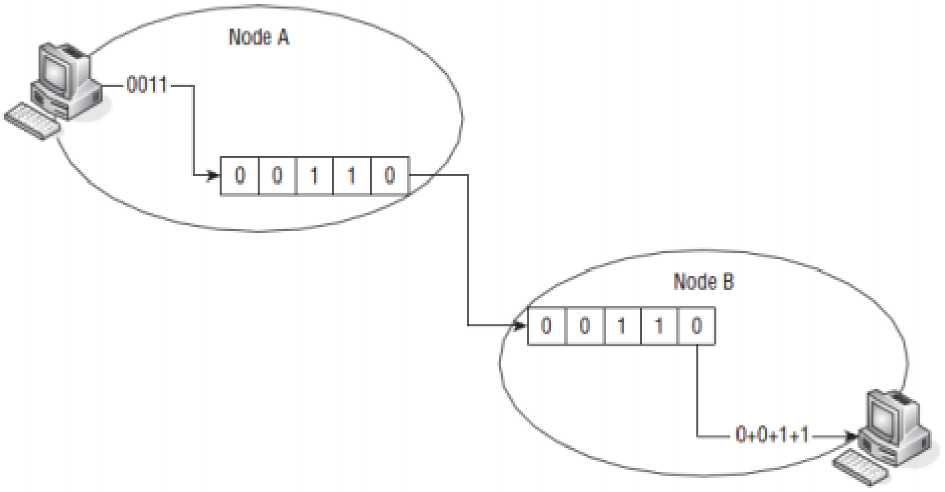


Figure: Even Parity

In the Figure, node A wants to send the data stream 0011 to node B. Node A computes the value of the data stream (0+0+1+1) and because even parity checking is being used, node A does not turn on the parity bit before it transmits the data. Node B then receives the data and computes the overall value (0+0+1+1+0), which is an even value. Even parity is in use, so node B reports a good frame received. Finally, let's take a look at the parity check when an error has occurred. Figure below shows an example of a data stream that is being sent using even parity. Notice that an error occurs before the stream reached the destination. When node B receives the data, it counts the number of 1s and notices that there is an odd number, therefore realizing that an error has occurred.

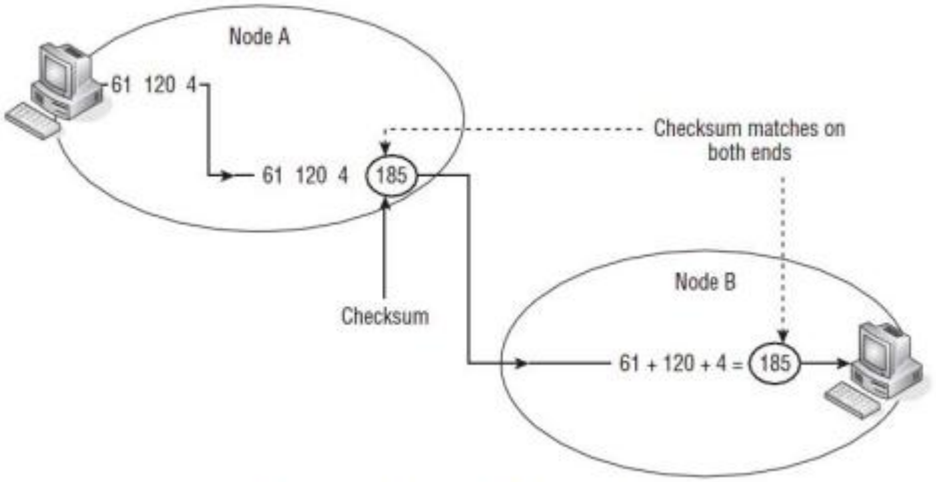


Figure: A simple checksum

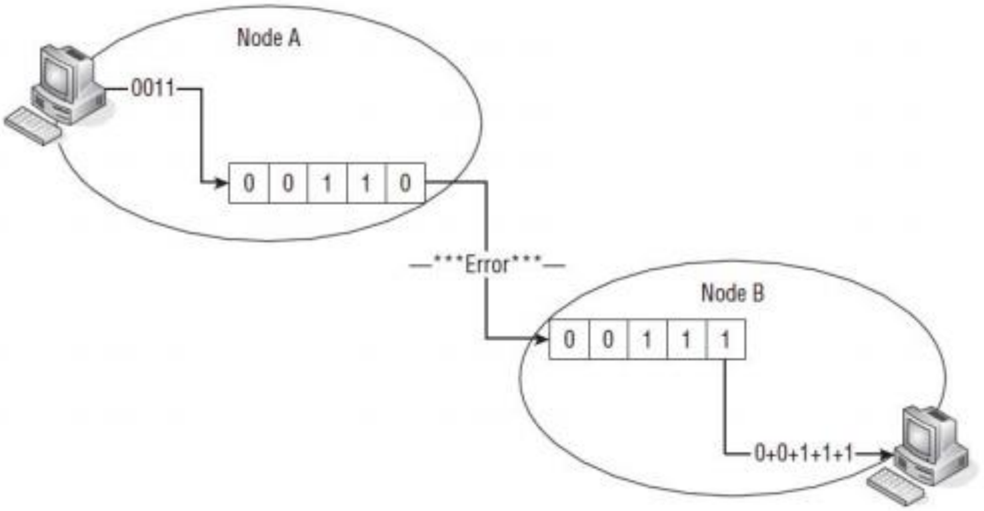


Figure: A parity Error

Error control

Another function of the Data Link layer is error detection. Error detection is the process of detecting whether errors occurred during the transmission of the bits across the wire. The Data Link layer uses a calculated value called the CRC (Cyclic Redundancy Check) that's placed into the Data Link trailer that's added to the message frame before it's sent to the Physical layer. The receiving computer recalculates the CRC and compares it to the one sent with the data. If the two rules are equal, it's assumed that the data arrived without errors. Otherwise, the message frame may need to be retransmitted under control of an upper layer. Although the Data Link layer implements error detection, it does not include a function to perform error recovery. This is left for the upper layers to deal with, primarily on the Transport layer.

Media access control (MAC) sublayer:

- Multiple access protocols for channel-access control, for example CSMA/CD protocols for collision detection and retransmission in Ethernet bus networks and hub networks, or the CSMA/CA protocol for collision avoidance in wireless networks. o Physical addressing (MAC addressing)
- LAN switching (packet switching) including MAC filtering and spanning tree protocol o Data packet queueing or scheduling
- Store-and-forward switching or cut-through switching
- Quality of Service (QoS) control
- Virtual LANs (VLAN)

MAC

The MAC sublayer carries the physical address of each device on the network. This address is more commonly called a device's MAC address. The MAC address is a 48-bit address that's encoded on each network device by its manufacturer. It's the MAC address that the Physical layer uses to move data between nodes of the network.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

CSMA/CD is the method used in Ethernet networks for controlling access to the physical media by network nodes. CSMA/CD process can be described as follows: Listen to see whether the wire is being used.

- If the wire is busy, wait.
- If the wire is quiet, send.
- If a collision occurs while sending, stop wait a specific amount of time, and send again.