Computer Networks - CS 204

Rishit Saiya - 180010027, Summary

April 17, 2020

1 Random Access MAC Protocols

These protocols are taken into considerations when transmission is at full channel data rate. Moreover, there is no coordination between prior nodes and current nodes. From previous literature, it is clear that 2 or more nodes transmitting at the same time will lead to collision in the network.

These protocols specify and lead us to detect collisions and how to mitigate and recover from the collisions. Examples of Random Access Protocols are ALOHA, Slotted ALOHA, CSMA & CSMA/CD.

2 ALOHA

The crude idea of the ALOHA protocol was as follows:

Whenever the sender is ready, it transmits the packet. Receiver then sends a ACK back to the sender. There is timings maintained for each ACK. This idea is in resemblance with the Congestion Control detection with timings attached to ACKs. Next here, collision are detected with timings of the ACKs. Recovery from the collision is by trying after random delay (Backoff Approach).

When the implementation of ALOHA was shifted from pure to slotted, we had rise in utilization with 36% from 18%.

It is depicted in Figure 1.

2.1 Slotted ALOHA

The working of Slotted ALOHA is as follows:

- The packet transmission time is divided into equal size slots.
- A node transmits the packet at the beginning of the next slot.
- If a collision occurs, the node retransmits the packet in future slots with probability ‘p’ until we have a successful transmission.

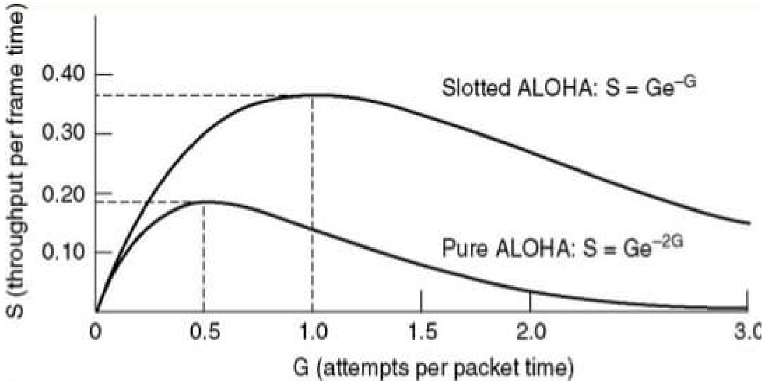


Figure 1: Throughput Vs. Offered Traffic for Pure ALOHA and Slotted ALOHA

2.2 Pure ALOHA

This is basically unslotted, just the quite opposite of Slotted ALOHA. The working in Pure ALOHA is as follows:

- The packet is transmitted without awaiting for beginning of the slot.
- It is natural that in these cases, the chances of collisions increase tremendously. A simple collision example can be explained as follows:
  Consider a packet sent at a certain time t_0 will collide with the packets sent at the times $[t_0 - 1\ ,\ t_0 + 1]$ because the packet at time t_0 will have an overlap with the packets of times $[t_0 - 1\ ,\ t_0 + 1]$ in the time frames.

3 Ethernet

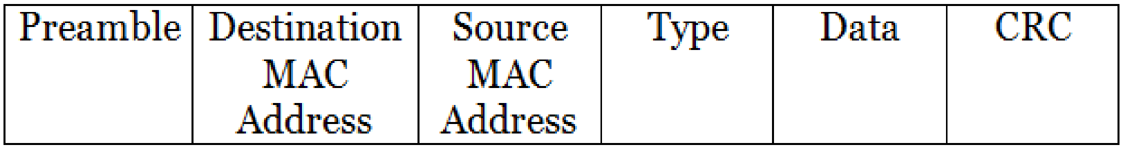
This first practical LAN (Local Area Network) was the Ethernet.

The basic idea was remains the same. It had to listen to the wire before transmission. If a collision is detected, it is avoided in the active transmission time.

3.1 Ethernet MAC Protocols

In ALOHA, decisions to transmit are made irrespective of other nodes' involvement in the network. Ethernet uses CSMA/CD and listens to line before or during the process of transmission.

If the line is idle, the condition is said to be no carrier sensed. In this case, we send packet immediately. It is to be noted that the upper bound message size of ***1500 bytes*** and the line in the network has to wait for ***9.6*** *μsec.*



Preamble	Destination MAC Address	Source MAC Address	Type	Data	CRC

Figure 2: Ethernet MAC Frame Format

If the line is busy, the condition is said to be carrier sensed. We wait until the line is idle again and transmit the packet immediately afterwards.

If collision is detected, we stop sending packets due to the jam signal. We try again later.

3.2 10Base2 Ethernet Technology

The **10** represents the 10 Mbps and **2** represents the ($\sim$ 200 meters) cable length. The cable is coaxial in nature and is used in Bus Topology. Repeaters are used to connect to multiple segments. The physical layer device, Repeater repeats bits it receives on one interface onto the other interfaces.

3.3 10BaseT Ethernet Technology

The **10** represents the 10 Mbps and **T** stands for the Twisted Pair. The hubs are connected by Twisted Pair Facility in a Star Network Topology given that the distance between any node to hub is less than 100m.

3.4 100BaseT Ethernet Technology

The **100** represents the 100 Mbps and **T** stands for the Twisted Pair. The hubs are connected by Twisted Pair Facility in a Star Network Topology given that the distance between any node to hub is less than 100m.

3.5 Ethernet Frame Format

The Ethernet Frame Format is divided into 2 types based on the guidelines and compliance it was set in. They are explained as follows.

1. **The Ethernet MAC Frame Format**
   The Ethernet MAC Frame Format is as given in Figure 2.

   The components in the Ethernet Frame are explained as follows:

   - ***Preamble***
     It is used to synchronize the receiver before actual data is sent. It consists of a sequence of 7 bytes, each set to 1010101.

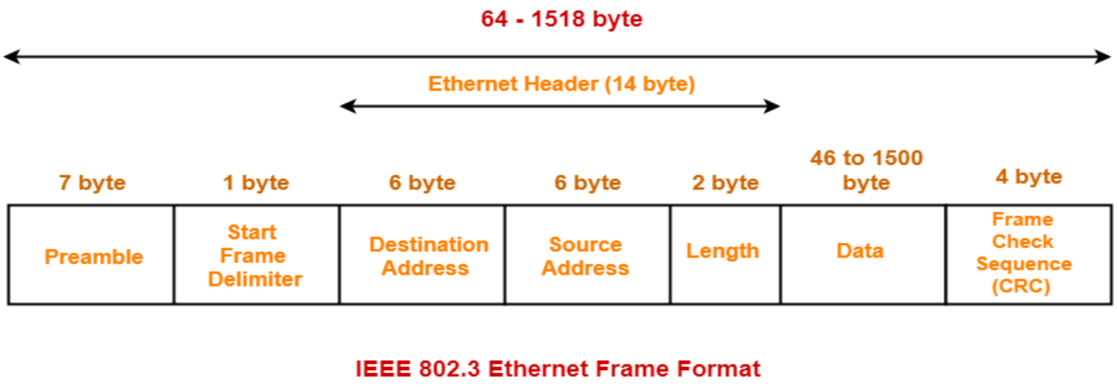


Figure 3: Ethernet IEEE 802.3 Frame Format

- ***MAC Addresses (Source and Destination)***
  It is a unique, 48-bit unicast address assigned to each adapter. Example: D4-3B-04-67-16-AE.
- ***Type***
  This field is a demultiplexing key used to determine which higher level protocol the frame should be delivered to.
- ***Body***
  The body is the field which has the capacity to contain upto 1500 bytes of data.

2. **The Ethernet IEEE 802.3 Frame Format**

   The Ethernet IEEE 802.3 Frame Format is as given in Figure 3.

   The components in the Ethernet Frame are explained as follows:

   - ***Preamble***
     It informs the receiving system that a frame is starting and enables synchronization.
   - ***SFD (Start Frame Delimiter)***
     It signifies that the destination MAC Address field begins with the next byte. This is a 1-Byte field which is always set to 10101011.
   - ***Destination MAC Address***
     It identifies the receiving system.
   - ***Source MAC Address***
     It identifies the sending system.
   - ***Type***
     This field defines the type of protocol such as IPv4 or IPv6 inside the frame.
   - ***Data***
     It contains the payload data. Padding Data is added to meet the minimum length requirement for this field (46 bytes).

- ***FCS (Frame Check Sequence)***
  It contains a 32-bit ***Cyclic Redundancy Check (CRC)*** which allows detection of malicious data.

4 Collision Detection

A **Collision** is caused when two adapters transmit at the same time. The adapters in the network sense collision based on the voltage differences.

So far, all the things have been explained on how the protocols work when a collision is detected. But we also need to firmly understand how the collision is actually detected.

Consider two hosts, **A** & **B**, who belong to a certain network. Suppose A sends a packet which takes T time to reach B. WLOG, we can say that B's packet will also take T time to reach A. So if A is still transmitting at 2T, a collision is detected. This mechanism is in general used to detect collisions.

Using IEEE 802.3 standards, we specify maximum value of 2T to ***51.2*** μsec

5 Exponential Backoff

From previous literature, we are aware that if a collision is detected, we make a delay in the next sending packet and try again till it is successfully transmitted.

The delay time is decided using *Binary Exponential Backoff*. Based upon the number of delays, the delay time is selected as follows:

- If checking 1^{st} time for transmission is leading to collision, then the delay time is calculated by, K × 51.2 μsec, where K is chosen from {0,1}.

- If checking 2^{nd} time for transmission is leading to collision, then the delay time is calculated by, K × 51.2 μsec, where K is chosen from {0,1,2,3}.

- If checking n^{th} time for transmission is leading to collision, then the delay time is calculated by, K × 51.2 μsec, where K is chosen from $\{0,1,2,3,...2^n - 1\}$. Note: $K_{max} = 1023$.

- After several tries, host reports a transmit error.

Given all this, if the delay is not random, then there is a chance that sources would retransmit in the lock step. WLOG, we can say that this works for small number of hosts. It is natural that large number of hosts manifest to large number of collisions.

6 Ethernet Issues

We need to understand the issues regarding the Ethernet so as to mitigate the collisions and try to upgrade the number of transmissions in a given time frame. The general issues are as follows:

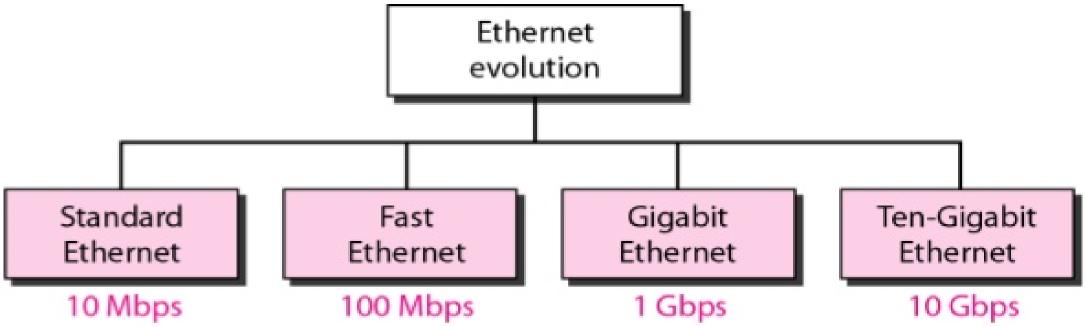


Figure 4: Ethernet Evolution

- Ethernet's peak utilization is pretty low. This is due to the bandwidth used in the recoveries from the collisions, etc.
- The peak throughput/utilisation is worst with more number of hosts. It is natural that more number of hosts lead to more number of collisions.
- The peak throughput is worst with small packets size. This is because the recoveries for collisions would have to be frequent and that would lead to a huge loss in the bandwidth.
- Longer Links can result one more drawback in the peak throughput of Ethernet because the collision detection will take a lot time to reach to the hosts in the network resulting in late recoveries and wastage of bandwidth.

7 Evolution of Ethernet

With the motive of resolving above issues and advancing towards better Ethernet technologies, we have evolved towards various types of Ethernet based on bandwidth.

A picture depicting the evolution is in the Figure 4.

The different types of modified Ethernet are:

- **Bridged Ethernet**
  In bridged LANs, LAN is divided using bridges. This resulted in increased bandwidth and seperated the collision domains. As we can see in the Figure 5, if a collision occurs in a LAN in which bridge isn't present, it jams the whole LAN. On the other hand, if the collision occurs in the LAN with a bridge in it, it only happens only in a particular segment of the LAN and essentially jams only those stations where the collision has occurred, keeping other stations active for transmission.
- **Switched Ethernet**
  This is basically extension of Bridged Ethernet. It is 2-way communication provider.

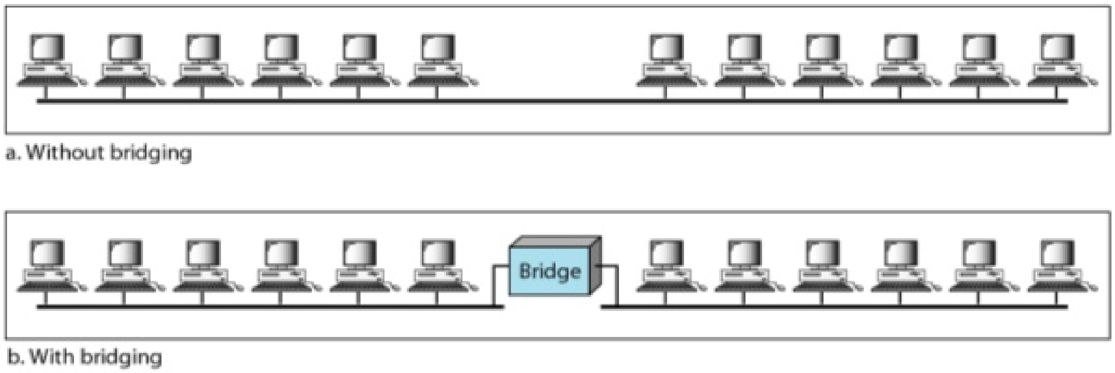


Figure 5: Bridged vs. Non Bridged Ethernet

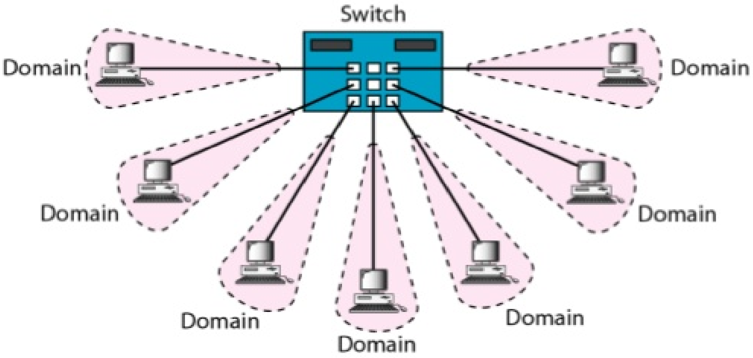


Figure 6: Switched Ethernet

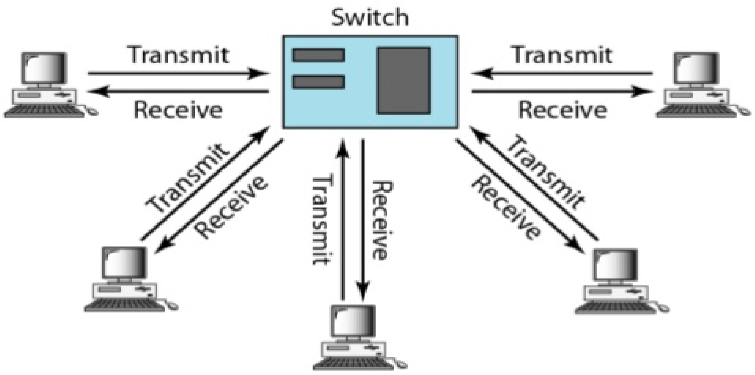


Figure 7: Full-Duplex Switched Ethernet

Here a switch is provided to each domain in the LAN, so this acts as a mitigation to the incoming collisions as well as reduces the loss in the bandwidth.

- **Full-Duplex Switched Ethernet**
  The 2 way communication with the switches and bridges gives a full-duplex switch ethernet. The 10BaseT Ethernet is a full-duplex switch ethernet whilst the 10Base5 and 10Base2 is half-duplex switch ethernet. The advantages of Full-Duplex Ethernet are as follows:
  - Eradicating CSMA/CD
    In Full-Duplex Switch Ethernet, each station is connected to the switch via 2 separate links. Each link is point-to-point dedicated path between the station and the switch.
  - Addition of MAC Control Layer
    To provide a flow and error control in full-duplex switched ethernet, a new sublayer, called MAC Control Layer is introduced between LLC & MAC sublayers. This is because Standard Ethernet was designed as a connectionless protocol at the MAC layer.
- **Fast Ethernet**
  The fast Ethernet is just with the goal of increasing the internet speed providing upto 100 Mbps.
- **Gigabit Ethernet**
  The Gigabit Ethernet is just with the goal of increasing the internet speed providing upto 1000 Mbps.

8 Ethernet Addressing

Each network device/station on an Ethernet network has its own Network Interface Card (NIC). All the devices connected to the network are manufactured in such a way that NIC is fitted inside the station and provides the station with a 6-byte physical address.

For example: D3-3B-10-06-16-AE

According to the scheme at Data Link Layer, the Ethernet Addresses have been divided as follows:

- ***Unicast Address***
  A source address is always a unicast address because the frame comes only from 1 station. When destination address is considered, if the last bit (or Least Significant Bit) of 1^{st} byte of Ethernet Address in binary form is 0, then it is classified under Unicast Address.

- ***Multicast Address***
  In the destination Address, if the last bit (or Least Significant Bit) of 1^{st} byte of Ethernet Address in binary form is **not** 0, then it is classified under Multicast Address.

- ***Broadcast Address***
  A special case of Multicast Address is Broadcast Address, where all the bits in the 1^{st} byte are 1s.

Example: D3-3B-10-06-16-AE
The binary form of above address is 1101001$\underline{\mathbf{1}}$-00111011-00010000-00000110-00010110-10101110
The last bit of 1^{st} byte is underlined above. Since it is 1, it is classified under Multicast Address.