**Chapter 4: The Medium Access Control Sublayer**

Responsible for deciding who sends next on a multi-access link.

An important part of the link layer, especially for LANs.

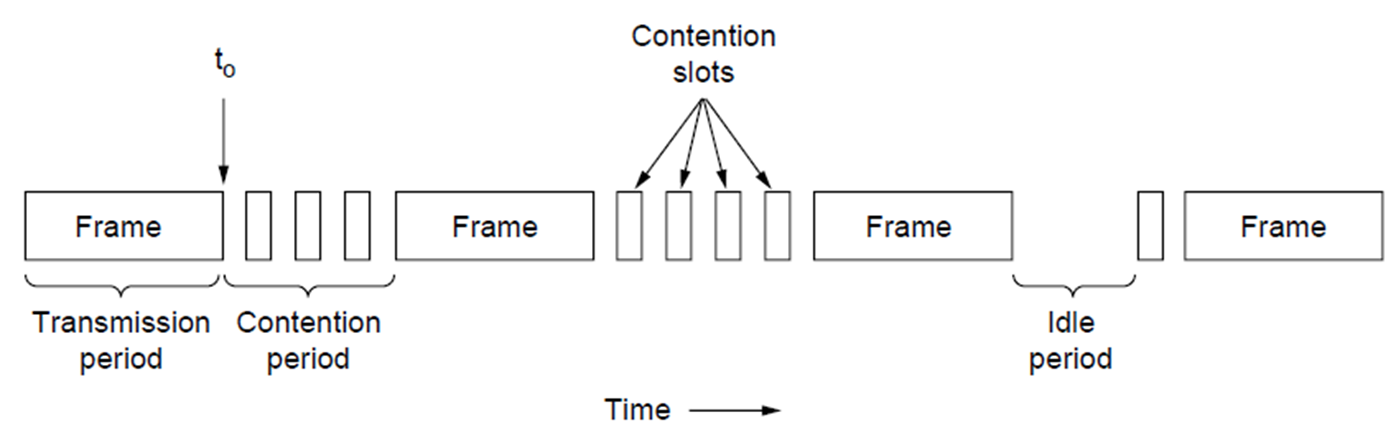
**Contention:** media access method that is used to share a broadcast medium. In contention, any computer in the network can transmit data at any time (first come-first served).This system breaks down when two computers attempt to transmit at the same time. This is a case of collision. To avoid collision, carrier sensing mechanism is used. Here each computer listens to the network before attempting to transmit. If the network is busy, it waits until network quiets down. In carrier detection, computers continue to listen to the network as they transmit. If computer detects another signal that interferes with the signal it is sending, it stops transmitting. Both computers then wait for random amount of time and attempt to transmit. Contention methods are most popular media access control method on LANs.

**CSMA:** Carrier Sense Multiple Access. CSMA improves on ALOHA by sensing the channel, so user doesn’t send if it senses someone else.

Variations on what to do if the channel is busy:

* 1-persistent (greedy) sends as soon as idle
* Nonpersistent waits a random time then tries again
* p-persistent sends with probability p when idle

**CSMA/CD:** CSMA/CD improvement is to detect/abort collisions. Reduced contention times improve performance.



Collision time is much shorter than frame time

**Wireless LANs:**

Wireless has complications compared to wired:

* Nodes may have different coverage regions
  + Leads to hidden and exposed terminals
* Nodes can’t detect collisions, i.e., sense while sending
  + Makes collisions expensive and to be avoided

**Hidden terminals** are senders that cannot sense each other but nonetheless collide at intended receiver

* Want to prevent; loss of efficiency

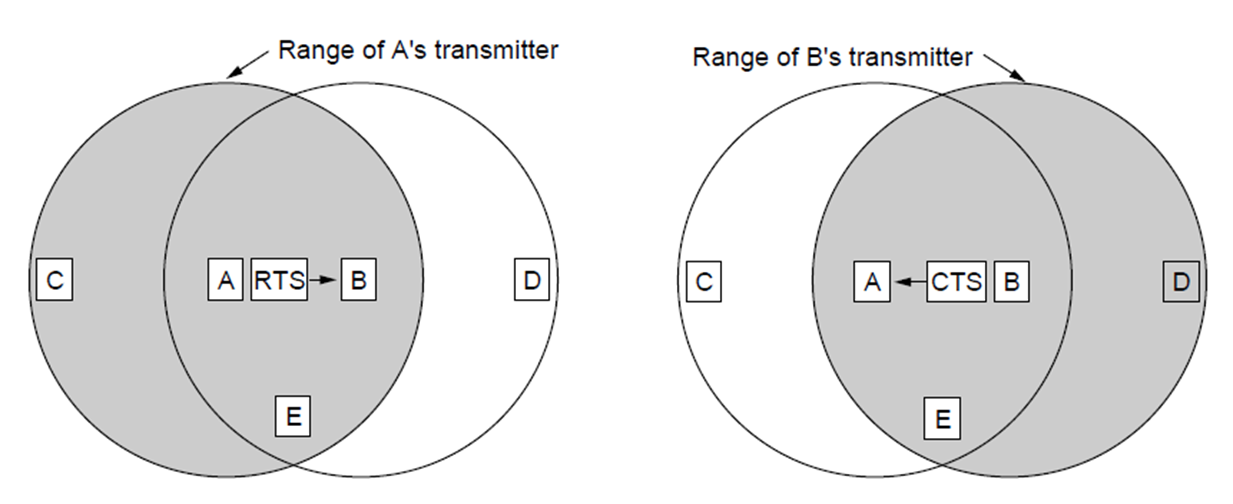
(Hidden = can’t hear each other)

**Exposed terminals** are senders who can sense each other but still transmit safely (to different receivers)

* Concurrency desirably; improves performance

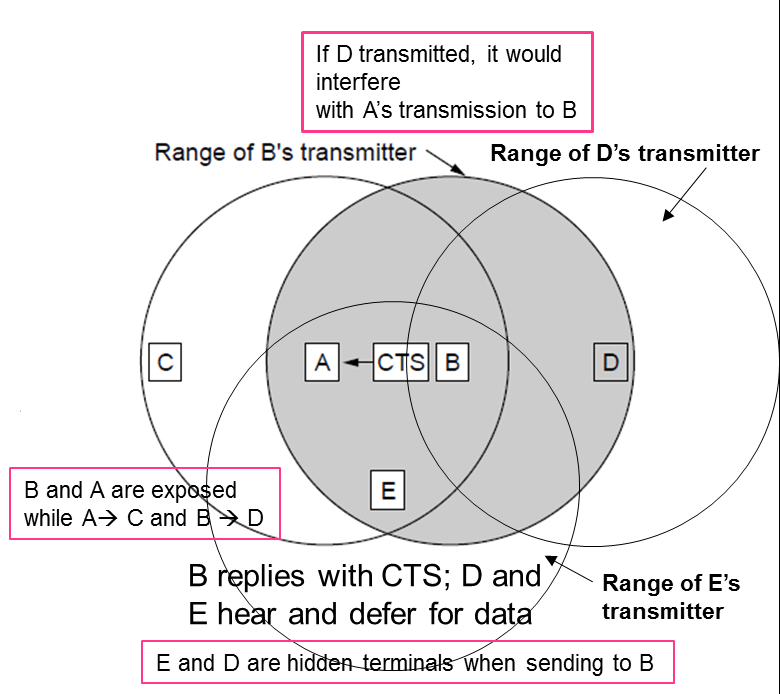
**MACA:** MACA protocol grants access for A to send to B:

* A sends RTS to B [left]; B replies with CTS [right]
* A can send with exposed but not hidden terminals



B replies with CTS; D and E hear and defer for data

A sends RTS to B; C and E hear and defer for CTS



**Classic (non-switched) Ethernet:**

One shared coaxial cable (bus) to which all hosts attach

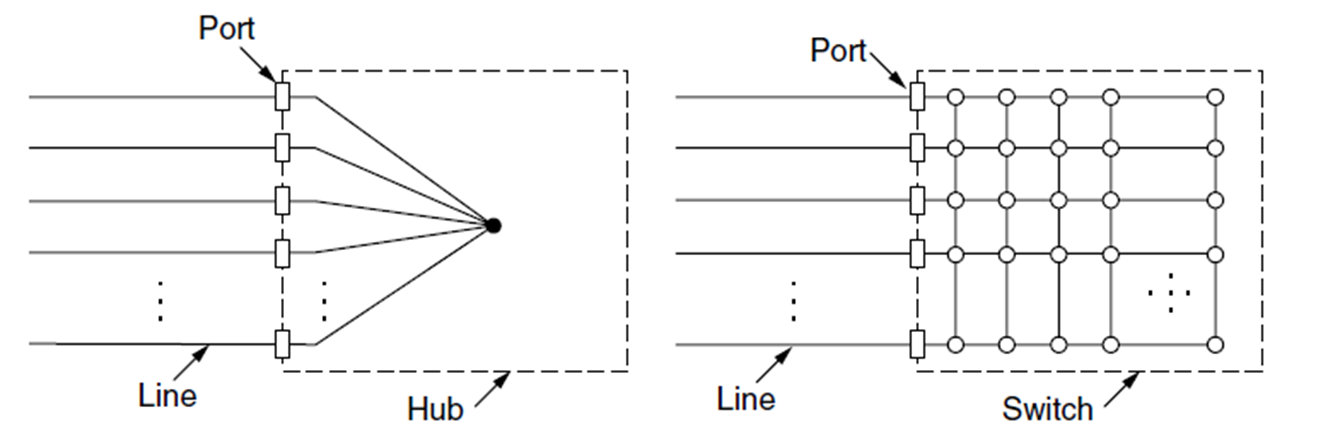
* Up to 10 Mbps, with Manchester encoding
* Hosts ran the classic Ethernet protocol for access
* Efficient for large frames, even with many senders
* Degrades for small frames (and long LANs)

MAC protocol is 1-persistent CSMA/CD (greedy)

* Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)
* Collisions can occur and take as long as 2τ to detect
  + (τ is the time it takes to propagate over the Ethernet)

**Switched/Fast Ethernet:**

* Hubs wire all lines into a single star-wired CSMA/CD domain
  + Hubs concentrate traffic from computers
* Switches isolate each port to a separate domain
  + Switches can be wired to computers, hubs and switches
* Much greater throughput for multiple ports
* No need for CSMA/CD when using full-duplex lines
* Fast Ethernet extended Ethernet from 10 to 100 Mbps



Hub is a logical bus which repeats (copies) any bits it sees on one port to all of the other ports

**What happens to the minimum frame size when we upgrade from 10 Mbps Ethernet to Fast Ethernet, and why.**

The worst-case situation occurs when the two most-distant stations on the network both need to send a frame and when the second station does not begin transmitting until just before the frame from the first station arrives. The collision will be detected almost immediately by the second station, but it will not be detected by the first station until the corrupted signal has propagated all the way back to that station. The maximum time that is required to detect a collision (the collision window, or "slot time") is approximately equal to twice the signal propagation time between the two most-distant stations on the network.

This means that both the minimum frame length and the maximum collision diameter are directly related to the slot time. Longer minimum frame lengths translate to longer slot times and larger collision diameters; shorter minimum frame lengths correspond to shorter slot times and smaller collision diameters.

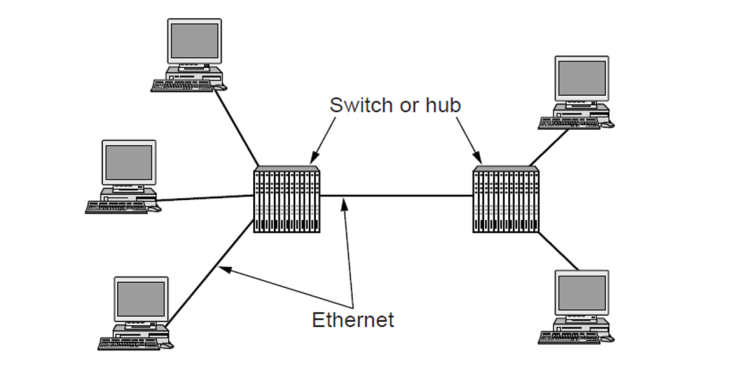
The trade-off was between the need to reduce the impact of collision recovery and the need for network diameters to be large enough to accommodate reasonable network sizes. The compromise was to choose a maximum network diameter (about 2500 meters) and then to set the minimum frame length long enough to ensure detection of all worst-case collisions.

The compromise worked well for 10 Mbps, but it was a problem for higher data-rate Ethernet developers. Fast Ethernet was required to provide backward compatibility with earlier Ethernet networks, including the existing IEEE 802.3 frame format and error-detection procedures, plus all applications and networking software running on the 10-Mbps networks.

Although signal propagation velocity is essentially constant for all transmission rates, the time required to transmit a frame is inversely related to the transmission rate. At 100 Mbps, a minimum-length frame can be transmitted in approximately one-tenth of the defined slot time, and any collision that occurred during the transmission would not likely be detected by the transmitting stations. This, in turn, meant that the maximum network diameters specified for 10-Mbps networks could not be used for 100-Mbps networks. The solution for Fast Ethernet was to reduce the maximum network diameter by approximately a factor of 10 (to a little more than 200 meters)

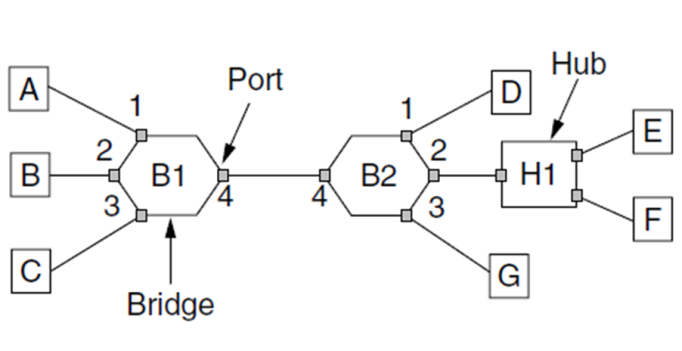
**Gigabit Ethernet:**

* Switched Gigabit Ethernet is now the garden variety
* With full-duplex lines between computers/switches
* Gigabit Ethernet is commonly run over twisted pair



**Data link layer switching;**

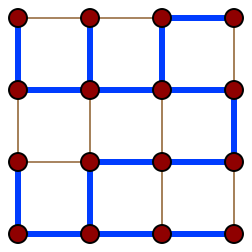
**Bridges:**  A bridge operates as a switched LAN (not a hub). Computers, bridges, and hubs connect to its ports. Bridges extend the Link layer. They use but don’t remove Ethernet header/addresses and do not inspect Network header.



**Backward learning:** algorithm used to pick the output port.

* Associates source address on frame with input port
* Frame with destination address sent to learned port
* Unlearned destinations are flooded (sent to all other ports)
* Needs no configuration
  + Table entries time-stamped
  + Stale table entries dropped to allow changes
* Bandwidth efficient for two-way traffic

**The spanning tree algorithm:**



Bridge topologies with loops and only backward learning will cause frames to circulate for ever

Need spanning tree support to solve problem

**VLANs:** (Virtual LANs) splits one physical LAN into multiple logical LANs to ease management tasks

**Full-duplex Ethernet:** Legacy Ethernet is half-duplex, meaning information can move in only one direction at a time. In a totally switched network, nodes only communicate with the switch and never directly with each other. Switched networks also employ either twisted pair or fiber optic cabling, both of which use separate conductors for sending and receiving data. In this type of environment, Ethernet stations can forgo the collision detection process and transmit at will, since they are the only potential devices that can access the medium. This allows end stations to transmit to the switch at the same time that the switch transmits to them, achieving a **collision-free** environment.

**Collision domain:** a section of a network where data packets can collide with one another when being sent on a shared medium or through repeaters, particularly when using early versions of Ethernet.

**Collision window:** The initial part of its transmission.

**Repeaters:** an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. These can be found at the physical layer.

**Flooding:** overwhelming of a destination receiver

**Promiscuous mode:** a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN.

**Transparent bridges:** is a common type of bridge that observes incoming network traffic to identify media access control (MAC) addresses. These bridges operate in a way that is transparent to all the network's connected hosts. A transparent bridge records MAC addresses in a table that is much like a routing table and evaluates that information whenever a packet is routed toward its location. A transparent bridge may also combine several different bridges to better inspect incoming traffic. Transparent bridges are implemented primarily in Ethernet networks.

**segments and LANs:**

**Frame structure:**

**Lab 2**