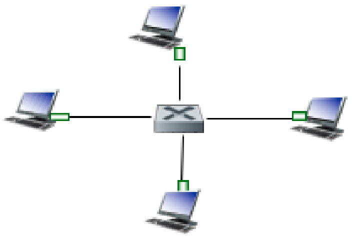
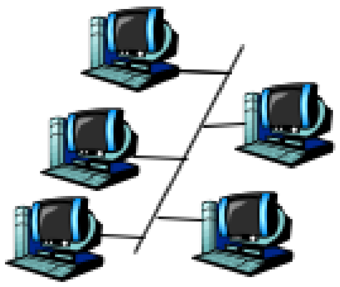
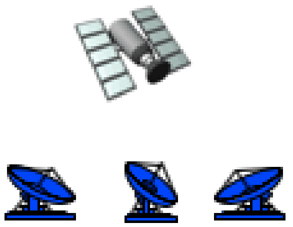
Exploration: Link Layer Multiple Access

Introduction



At the physical layer, we have two types of link. The first kind is point-to-point. With this kind of link, data can go back and forth between the two devices without any kind of interference.





The second kind is called a broadcast link, because a number of computers are connected to some shared medium and any of them could be sending at the same time. The shared medium can be wired or wireless. Interference, or "collisions", would be caused when any two computers try to send at the same time. A multiple access protocol is required to allow communications to occur on a shared medium.

Multiple Access Protocols

There must be some kind of protocol for determining how adjacent nodes can share a channel. This type of protocol is called a multiple access (MA) protocol. The MA protocol will determine when a node can transmit. The protocol itself uses the communication channel to transmit info about sharing (no out-of-band signaling is used).

The "Ideal" multiple access protocol criteria, for a broadcast channel of rate R bps:

1. When only one node wants to transmit, it can send at rate R.
2. When M nodes want to transmit, each can send at average rate R/M
3. The protocol is fully decentralized:
    - no special node is required to coordinate transmissions
4. The protocol should be simple and robust

There are three main approaches to sharing media, none of them ideal:

- Channel Partitioning (discussed in earlier lectures)
    - divide channel into smaller "pieces"
        - TDM (time-division), FDM (frequency-division)
    - allocate piece to node for exclusive use
    - easy to implement, but does not satisfy criterion #1 (above)
- Random Access

  - allow collisions
  - recover from collisions
  - difficult to guarantee criterion #2 (above)
- “Taking turns”
  - nodes with more to send can take longer turns
  - supervisor required, does not satisfy criterion #3 (above)

Random Access Protocols

With Random Access, if a node has a packet to send, it will transmit at the full channel data rate R. There is no supervised coordination among nodes, so two or more nodes transmitting simultaneously will cause a collision. The random access MA protocol specifies:

- How to detect collisions
- How to recover from collisions (e.g., via delayed retransmissions)

Carrier-Sense Multiple Access (CSMA)

CSMA is a type of random-access protocol. CSMA will listen before transmitting. If the channel is sensed idle, the entire frame is transmitted. If the channel is sensed busy, the transmission is deferred.

Collisions can still occur with CSMA. Propagation delay means that two nodes may not sense each other’s transmission in time to avoid collisions. If a collision occurs, the entire packet transmission time is wasted.

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

CSMA/CD is an improvement to CSMA that aims to reduce wasted transmission time. As with pure CSMA, the host that wants to send will sense the medium first, and if free will send. It is possible with hardware to detect a collision within a short time (the CD part of CSMA/CD). If this happens, the colliding transmissions can be aborted, reducing channel wastage. Then the senders can back off and retry later.

The collision detection is easy in wired LANs, where the signal strengths of transmitted and received signals can be easily measured and compared. This is much more difficult in wireless LANs, because the received signal strength is overwhelmed by the local transmission strength. Therefore wireless LANs will often employ other strategies.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

What is used by wireless is called CSMA/CA. With this protocol, the sending computer sends a very short reservation message to the receiver. The receiver responds with a brief slot message reserving a broadcast slot for the sender. This response from the receiver is broadcast to all potential senders within range, so that all are notified of the reservation and will therefore need to wait their turn. We will discuss this in greater depth in our Wireless module.

Taking-turns protocols

Finally we have several types of “Taking-turns” MA protocols: Polling and Token Passing. It should be noted that these protocols are usually associated with legacy networking systems.

With Polling, a master computer invites secondary nodes to transmit in turn. Typically this will be used with dumb terminal. Polling has several issues, including the overhead and latency of polling itself and a single point of failure (the master computer).

With Token Passing, a token message is passed from one node to the next in sequence. If a node has anything to send it must wait for the token, send its data, wait for a response, and then the token can be passed on. Problems with this approach include token loss, in which case no one can send anything, and the overhead and latency involved with token passing..

This concludes our discussion of Multiple Access protocols. Be sure to watch the video lecture below for more details. Then test your knowledge with the included Self-Check exercises.

Video Lecture

Multiple Access

CS 372 Lecture

Multiple Access

- links
- protocols

Note: Many of the lecture slides are based on presentations that accompany *Computer Networking: A Top Down Approach*, 6th edition, by Jim Kurose & Keith Ross, Addison-Wesley, 2013.

(PDF (https://oregonstate.instructure.com/courses/1798856/files/83165298/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165298/download?wrap=1) |PPT (https://oregonstate.instructure.com/courses/1798856/files/83165074/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165074/download?wrap=1))

Self-Check Exercises

What is a multiple access protocol designed to do?

Turn

Card 1 of 3

In link layer terminology, a collision is two or more frames of the same type being received at the same node at different times.

○ True

○ False

Reuse

<> Embed