CS 336 Lecture 19– 4/6/98

Announcements

- Handout describing simulation project is now online. (If you did not receive a copy of the Feldmeier paper before break, see me.)
- Exercise 5 solution is now available.
- A "lite" written assignment (Exercise 6 is also now available.

IEEE 802.1 Transparent Bridges

1. Before you all went away for break, we were discussing a technique for interconnecting multiple LANS intended to:
   - Enable one to connect moderately incompatible networks (IEEE Ethernets, Fast Ethernets, Token rings).
   - Overcome the length limitations imposed to keep contention protocol behavior reasonable.
   - Provide a way to limit congestion on a LAN by replacing the "everything is broadcast to everyone" approach with an attempt to break the LAN into sub-LANs and limit traffic to the sub-LAN on which it originated whenever possible.
2. If one ignores the concern about congestion, it is simple to construct bridges that solve all the other problems.
   - Each bridge reads in every packet sent (successfully) on any network to which it is connected. called *ports*.
   - Once the packet is received, the bridge retransmits it onto all of the networks to which it is connected except the one from which it was received (following the standard MAC protocols of these networks). This is called *flooding*.
3. It also isn't hard to design a bridge that solves the congestion problem without much help from the stations on connected networks.
   - Each bridge keeps a little table a packets sources and the ports the associated packets arrived on.
     - When a packet is received, look the destination of the packet up in the source/port table.
     - If no entry is found, just flood the packet.
     - If an entry is found:
       * If the port associated with the address is the port on which the packet arrived, ignore the packet.
       * Otherwise, just forward the packet to the network attached through the associated port.
4. Both of these schemes only work if the network is loop free.
   - If there were a cycle, the flooding process would be disastrous.
   - If there were a cycle, packets from a given source might be observed on several different ports of a single bridge.

The IEEE 803.1 Bridge Spanning Tree Algorithm

1. It may be desirable to build networks which contain bridges that form loops for reliability reasons.
   - If a large sub-LAN (like all of Bronfman) is only connected to the rest of a LAN (i.e. the rest of the campus) through a single bridge, that bridge becomes a single point of failure.
   - It would be nice if two bridges could be installed in such a situation. In this case, the bridges somehow have to be designed to be smart enough to deal with the loop.
2. IEEE 802.1 bridges are designed to detect loops and deal with them by making enough ports on enough bridges inactive that no "active" loops exist.
3. If the topology of a LAN is abstracted to form a bipartite graph where the nodes are networks and sub-LANs and the edges correspond to bridge ports, then the IEEE 802.1 approach to avoiding loops can be seen as finding a set of edges that form a spanning tree for this graph.
   - The bridges first use broadcast messages to "elect" a root for this tree.
   - While the election is in progress, the bridges are also exchanging enough information so that when it is over every bridge will no the cost of sending a message from it to the root.
   - For each sub-LAN, the attached bridges then determine which has the least cost path to the root. Those bridges with greater than minimum cost deactivate their ports that connect to the sub-LAN considered.
4. The details of bridge election are fairly simple.
   - Each bridge has a unique "priority" assigned to it actually a non-unique priority with a unique ID appended to it) and each port has a "cost". These can be set by the network administrator or left at default values supplied by the factory.

- When the bridges recognize the need for an election, they all start sending packet announcing the candidate they endorse including:
  - The candidate's priority (Initially this will be their own priority.
  - Their ID number.
  - The cost of reaching the candidate from the sending hub.
- As bridges receive such packets, they look for the candidate with the lowest priority/ID pair and given equal priorities they look for the lowest path cost.

  Each bridge maintains
  - The priority/ID of the best candidate for root it has seen (i.e. the smallest prioirity/ID seen).
  - The cost of and port leading to the best known route to the best candidate for root.
  - For each port attached to the bridge, the contents of the campaign packet received on that port advertising the least cost to reach the root.