Bridge Filtering

- Bridges learn which hosts can be reached through which interfaces: maintain filtering tables
  - When a frame is received, the bridge "learns" the location of the sender: incoming LAN segment
  - Records sender location in the filtering table
- Filtering table entry:
  - (Node LAN Address, Bridge Interface, Time Stamp)
  - Stale entries in the Filtering Table dropped (TTL can be 60 minutes)

 Filtering procedure:

```
if destination is on LAN on which frame was received
then drop the frame
else { lookup dest in filtering table
      if entry found for destination
      then forward the frame on interface indicated;
      else flood; /* forward on all but the interface on which the frame arrived */
    }
```

Bridge Learning: example

Suppose C sends frame to D and D replies back with frame to C

- C sends frame, bridge has no info about D, so floods to both LANs
  - Bridge notes that C is on port 1
  - Frame ignored on upper LAN
  - Frame received by D

- D generates reply to C, sends
  - Bridge sees frame from D
  - Bridge notes that D is on interface 2
  - Bridge knows C on interface 1, so selectively forwards frame out via interface 1
**Bridges Spanning Tree**
- for increased reliability, desirable to have redundant, alternate paths from source to dest
- with multiple simultaneous paths, cycles result - bridges may multiply and forward frame forever
- solution: organize bridges in a spanning tree by disabling subset of interfaces

**Bridges vs. Routers**
- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are Link Layer devices
- routers maintain routing tables, implement routing algorithms
- bridges maintain filtering tables, implement filtering, learning and spanning tree algorithms

**Routers vs. Bridges**
- Bridges + and -
  + Bridge operation is simpler requiring less processing bandwidth
  - Topologies are restricted with bridges: a spanning tree must be built to avoid cycles
  - Bridges do not isolate broadcast domains
    - All hosts see all broadcasts
- Routers + and -
  + arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)
  + isolate broadcast domains
    + reduce broadcast traffic seen by each host
  - require IP address configuration (not plug and play)
  - require higher processing bandwidth
- bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)