Hubs, Bridges, and Switches (oh my)

- Used for extending LANs in terms of geographical coverage, number of nodes, administration capabilities, etc.
- Differ in regards to:
  - collision domain isolation
  - layer at which they operate
- Different than routers
  - plug and play
  - don't provide optimal routing of IP packets

Hubs

- Physical Layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or multi-tier design), with a backbone hub at its top
Hubs (more)

- Each connected LAN is referred to as a LAN segment
- Hubs do not isolate collision domains: a node may collide with any node residing at any segment in the LAN

Hub Advantages:
- Simple, inexpensive device
- Multi-tier provides graceful degradation: portions of the LAN continue to operate if one of the hubs malfunction
- Extends maximum distance between node pairs (100m per Hub)

Hubs (more)

Hub Limitations:
- Single collision domain results in no increase in max throughput: the multi-tier throughput same as the the single segment throughput
- Individual LAN restrictions pose limits on the number of nodes in the same collision domain (thus, per Hub); and on the total allowed geographical coverage
- May not connect different Ethernet types (e.g., 10BaseT and 100baseT)
Bridges

- **Link Layer devices**: they operate on Ethernet frames, examining the frame header and selectively forwarding a frame based on its destination.

- **Bridge isolates collision** domains since it buffers frames.

- When a frame is to be forwarded on a segment, the bridge uses CSMA/CD to access the segment and transmit.

Bridges (more)

- **Bridge advantages**:
  - Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage.
  - Can connect different type Ethernet since it is a store and forward device.
  - Transparent: no need for any change to hosts LAN adapters.
Backbone Bridge

![Diagram of a backbone bridge setup with hubs and bridges connecting Electrical Engineering, Computer Science, and Systems Engineering.

Interconnection Without Backbone

- **Not recommended** for two reasons:
  - Single point of failure at Computer Science hub
  - All traffic between EE and SE must path over CS segment
**Bridge Filtering**

- Bridges learn which hosts can be reached through which interfaces and maintain filtering tables
- A filtering table entry: (Node LAN Address, Bridge Interface, Time Stamp)
- Filtering procedure:
  - if destination is on LAN on which frame was received
    - then drop the frame
  - else (lookup 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**

- When a frame is received, the bridge “learns” from the source address and updates its filtering table (Node LAN Address, Bridge Interface, Time Stamp)
- Stale entries in the Filtering Table are dropped (TTL can be 60 minutes)
**Bridges Spanning Tree**

- For increased reliability, it is desirable to have redundant, alternate paths from a source to a destination.
- With multiple simultaneous paths however, cycles result on which bridges may multiply and forward a frame forever.
- Solution is organizing the set of bridges in a spanning tree by disabling a subset of the interfaces in the bridges.

![Diagram of Bridges Spanning Tree]

**WWF Bridges vs. Routers Smackdown**

- Both are store-and-forward devices, but Routers are Network Layer devices (examine network layer headers) and Bridges are Link Layer devices.
- Routers maintain routing tables and implement routing algorithms, bridges maintain filtering tables and implement filtering, learning and spanning tree algorithms.

![Diagram comparing Host and Router connections]
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 offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge)

- Routers + and -
  - Arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)
  - Provide firewall protection against broadcast storms
  - Require IP address configuration (not plug and play)
  - Require higher processing bandwidth

- Bridges do well in small (few hundred hosts) while routers are required in large networks (thousands of hosts)
**Ethernet Switches**

- A switch is a device that incorporates bridge functions as well as point-to-point 'dedicated connections'
- A host attached to a switch via a dedicated point-to-point connection; will always sense the medium as idle; no collisions ever!
- Ethernet Switches provide a combinations of shared/dedicated, 10/100/1000 Mbps connections

**Ethernet**

- Some E-net switches support cut-through switching: frame forwarded immediately to destination without awaiting for assembly of the entire frame in the switch buffer; slight reduction in latency
- Ethernet switches vary in size, with the largest ones incorporating a high bandwidth interconnection network
Ethernet Switches (more)

IEEE 802.11 Wireless LAN

- Wireless LANs are becoming popular for mobile Internet access
- Applications: nomadic Internet access, portable computing, ad hoc networking (multihopping)
- IEEE 802.11 standards defines MAC protocol; unlicensed frequency spectrum bands: 900Mhz, 2.4Ghz
- Basic Service Sets + Access Points => Distribution System
- Like a bridged LAN (flat MAC address)
Ad Hoc Networks

- IEEE 802.11 stations can dynamically form a group without AP
- Ad Hoc Network: no pre-existing infrastructure
- Applications: "laptop" meeting in conference room, car, airport; interconnection of "personal" devices (see bluetooth.com); battlefield; pervasive computing (smart spaces)
- IETF MANET (Mobile Ad hoc Networks) working group

IEEE 802.11 MAC Protocol

CSMA Protocol:
- sense channel idle for DISF sec (Distributed Inter Frame Space)
  - transmit frame (no Collision Detection)
  - receiver returns ACK after SIFS (Short Inter Frame Space)

- if channel sensed busy then binary backoff

NAV: Network Allocation Vector
(min time of deferral)
**Hidden Terminal effect**

- CSMA inefficient in presence of hidden terminals
- Hidden terminals: A and B cannot hear each other because of obstacles or signal attenuation; so, their packets collide at B
- Solution? CSMA/CA
- CA = Collision Avoidance

![Diagram of hidden terminals and collision avoidance]

**Collision Avoidance: RTS-CTS exchange**

- **CTS** “freezes” stations within range of receiver (but possibly hidden from transmitter): this prevents collisions by hidden station during data
- **RTS** and **CTS** are very short: collisions during data phase are thus very unlikely (the end result is similar to Collision Detection)

- Note: IEEE 802.11 allows **CSMA**, **CSMA/CA** and “polling” from AP
**Point to Point protocol (PPP)**

- Point to point, wired data link easier to manage than broadcast link: no Media Access Control
- Several Data Link Protocols: PPP, HDLC, SDLC, Alternating Bit protocol, etc
- PPP (Point to Point Protocol) is very popular: used in dial up connection between residential Host and ISP; on SONET/SDH connections, etc
- PPP is extremely simple (the simplest in the Data Link protocol family) and very streamlined

**PPP Requirements**

- Pkt framing: encapsulation of packets
- bit transparency: must carry any bit pattern in the data field
- error detection (no correction)
- multiple network layer protocols
- connection liveness
- Network Layer Address negotiation: Hosts/nodes across the link must learn/configure each other’s network address
## Not Provided by PPP

- error correction/recovery
- flow control
- sequencing
- multipoint links (e.g., polling)

## PPP Data Frame

- Flag: delimiter (framing)
- Address: does nothing (only one option)
- Control: does nothing; in the future possible multiple control fields
- Protocol: upper layer to which frame must be delivered (e.g., PPP-LCP, IP, IPCP, etc)
Byte Stuffing

- For "data transparency", the data field must be allowed to include the pattern <01111110>; i.e., this must not be interpreted as a flag
- To alert the receiver, the transmitter "stuff"s an extra <01111110> byte after each <01111110> data byte
- The receiver discards each 01111110 followed by another 01111110, and continues data reception

PPP Data Control Protocol

- PPP-LCP establishes/releases the PPP connection; negotiates options
- Starts in DEAD state
- Options: max frame length; authentication protocol
- Once PPP link established, IPCP (Control Protocol) moves in (on top of PPP) to configure IP network addresses etc.