CSC465 – Computer Networks
Spring 2004

Dr. J. Harrison

These slides were produced from material by Behrouz Forouzan for the text "TCP/IP Protocol Suite (2nd Edition)" and from Kurose & Ross, "Computer Networking; A Top-down Approach Featuring the Internet"

Chapter 3 (Part B)

Underlying Technologies -Continued-

CONNECTING DEVICES

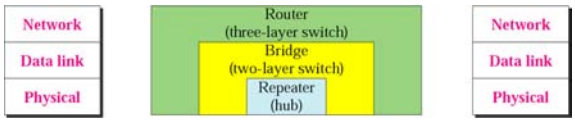
Hubs, Bridges and Switches

- 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

Internet

- Internet is neither single LAN or WAN
- Interconnected WANs and LANs
- Interconnection achieved via ***connecting devices***
- ***Repeaters*** & ***Hubs*** operate in 1st TCP/IP Layer
  - same as 1st ISO/OSI Layer
- ***Bridges*** operate in the first two layers
- ***Routers*** operate in the first three layers
- ***Switches***
  - Sophisticated bridge
  - Sophisticated router

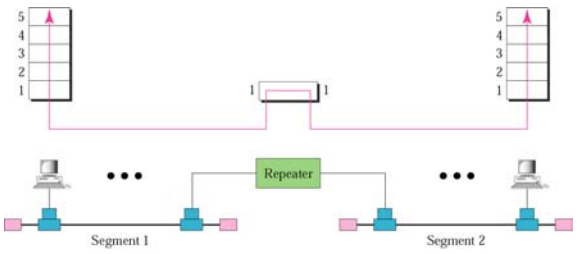
Connecting devices



Repeaters

- Signals attenuate over longer distances
- Before attenuation causes the signal to become too weak or become corrupted, repeater regenerates and transmits the original bit pattern
- Operates only at physical layer
- Simply retransmits bit with more energy
  - no CSMS/CD performed
  - No address filtering capability
- Partitions network into ***segments***
- All segments in same ***collision domain.***

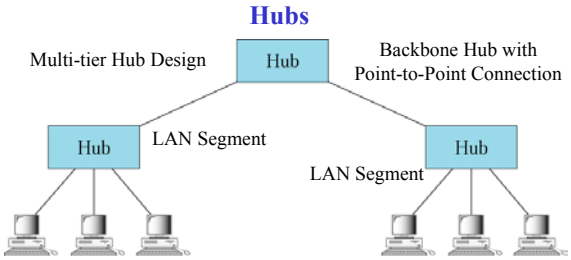
Repeater



Hubs

- Overloaded term but means: ***multiport repeater***
- Used to create connections in a physical star configuration
- All nodes must use same technology
  - Example: 10BASE-T Ethernet LAN
- Hubs can be used to build hierarchies to overcome attenuation limitations

Hubs



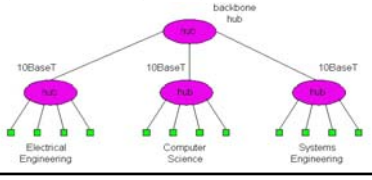
Network still ***one*** LAN with ***logical*** bus topology

Every packet sent is still received by all stations

Hierarchy removes length limitations of 10BASE-T

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
- 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



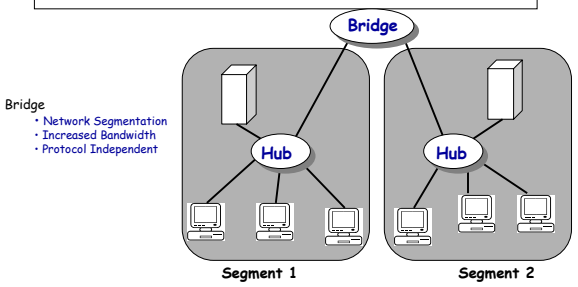
Hubs (Cont.)

- 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)
- 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
  - Cannot 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
- 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

Segmenting Ethernet



Bridges

- Operates in physical and data link layers
- Physical layer: regenerates signal it receives
- Data Link Layer: filtering and forwarding
  - Examines the physical addresses in the packet
  - Decides if packet should be forwarded
  - If forwarded, decides which interface and places frame in that interface's buffer
- Decision based on table that map addresses to interfaces

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 could be 60 minutes

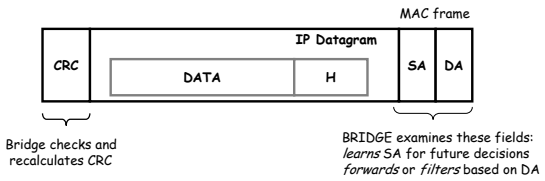
Bridge Table

Contains tuples:

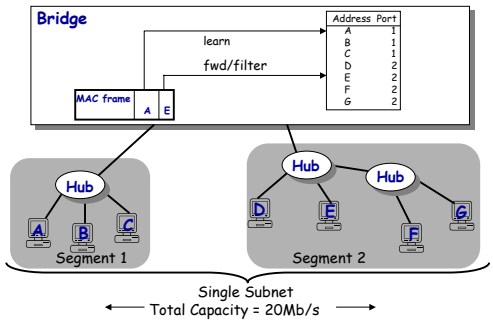
1. LAN address of node (62-AE-F7-23-45-B4)
2. Bridge interface of node
3. Timestamp of table entry

- Bridge will "learn" physical addresses
- Examines traffic and builds bridge table
- Simplifies the work of the network admin
- "Self-learning" bridge also called "transparent" bridge

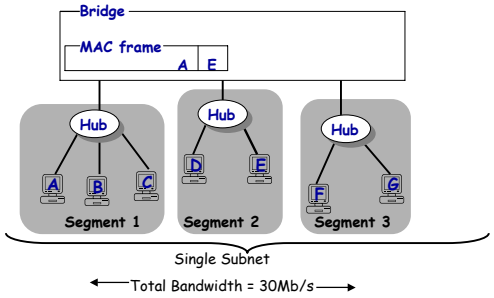
Primary Functions of Bridge



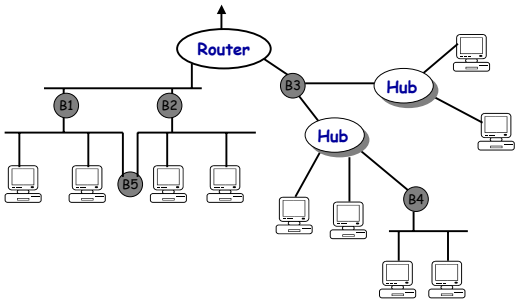
Primary Functions of a Bridge



Further Segmenting: Multiport Bridges



Typical Network topology with Bridges



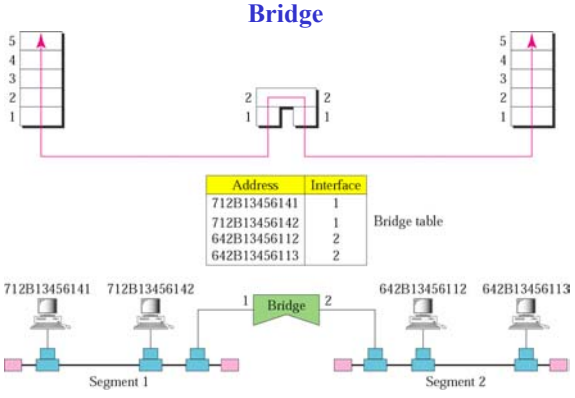
Self-learning Bridge

- Bridge table initially empty
- If a frame arrives and the destination is not in the table, the frame is copied to output buffers of all interfaces
- Each interfaces sends frame using CSMA/CD
- If every node eventually sends a frame, every node will eventually get recording in the table
- Bridge table removes entries after the ***aging time*** has elapsed (like e-mail)
- If PC gets new adapter, physical address of old adapter will eventually be purged from table

Bridges

- Unlike a hub, bridge runs the CSMA/CD algorithm
  - Refrains from sending if it hears traffic and employs exponential backoff
- Like a NIC except there are no addresses
  - Does not insert a physical address into the packet
- Can be used to combine Ethernet segments that use different technologies (10BASE-T,10BASE2)

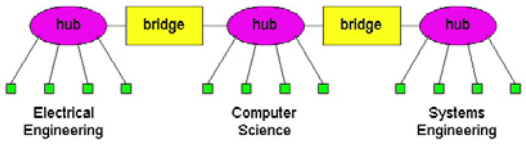
Bridge



Backbone Bridge

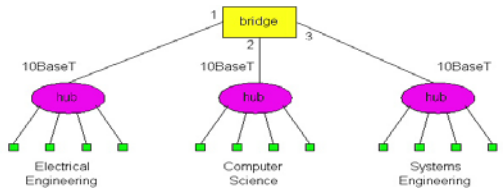
- LAN segments should be connected with a backbone
- Backbone: network that has direct connection to LAN segments
- Each pair of LAN segments can communicate without passing through a third LAN segment

Interconnection Without Backbone Bridge



- Two disadvantages:
  - Single point of failure at Computer Science hub
  - All traffic between EE and SE must path over CS segment

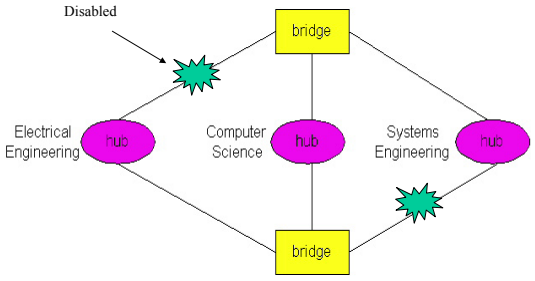
Interconnection with Backbone Bridge



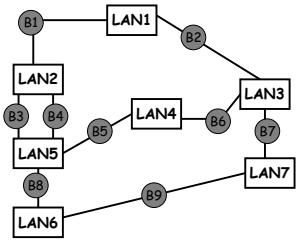
Bridges Spanning Tree

- 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

Bridges Spanning Tree

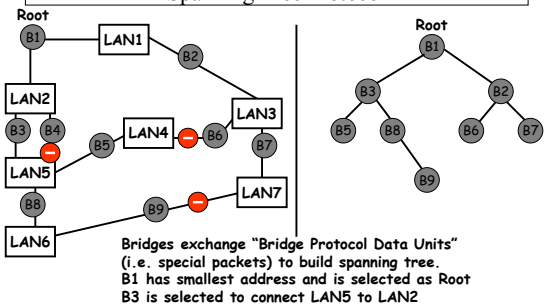


Preventing Loops: Spanning Tree Protocol



Preventing Loops

Spanning Tree Protocol



Bridges exchange "Bridge Protocol Data Units" (i.e. special packets) to build spanning tree.
B1 has smallest address and is selected as Root
B3 is selected to connect LAN5 to LAN2

Note

A bridge connects segments of a LAN together.

All segments connected to bridge are still part of the one LAN

Bridge does not change the physical addresses contained in packet

Switches

Two (network-related) meanings

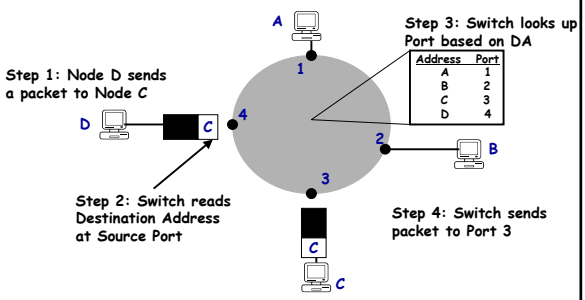
- Two-layer switch
  - Bridge with many interfaces
  - Each interface to a new segment with one station
  - No competing traffic on segments (no collisions)
  - Like bridges, vulnerable to broadcast storms
- Three-layer switch
  - Application specific ICs for better performance
  - Customized for specific network layer protocols (IP)
  - In some cases, learn routing tables from routers

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 sense the medium as idle
- Ethernet Switches provide a combinations of shared/dedicated, 10/100/1000 Mbps connections
- Some Ethernet 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

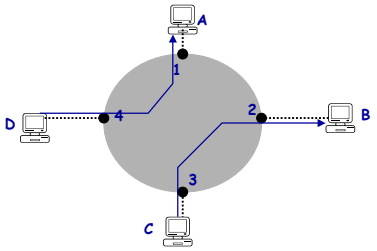
Switched Ethernet

An example of a switch



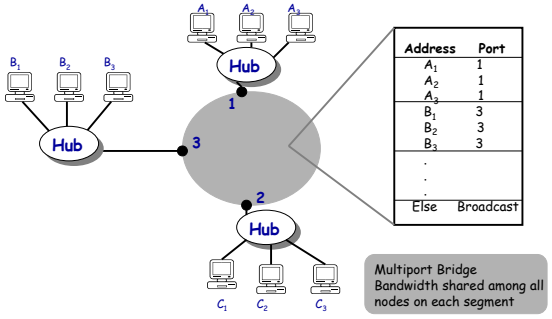
Switched Ethernet

Multiple transactions in a switch

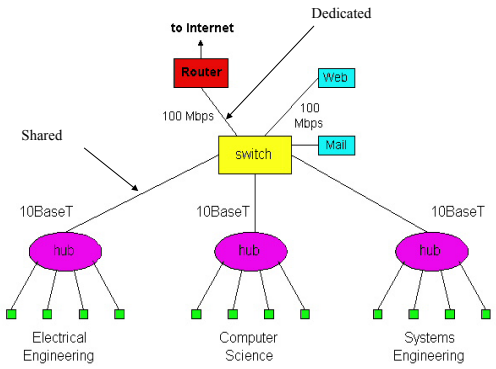


Increased throughput needs increased forwarding capability

Switched Ethernet



Ethernet Switches (Cont)

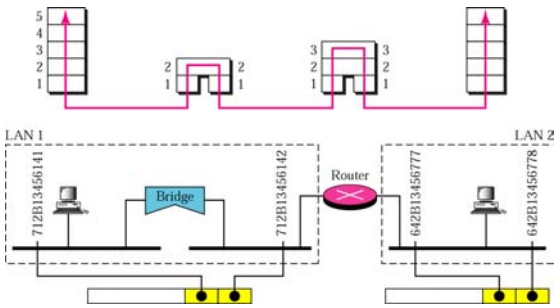


Routers

- 3-layer device (physical, data link & network)
- Physical: regenerates signal it receives
- Data link: examines physical addresses in packet
- Network layer: checks the network layer addresses (IP)
- Router is an internetworking device:
  - Can connect 2 LANs together
  - Can connect 2 WANs together
  - Can connect a LAN and WAN together

A repeater or a bridge connects segments of a LAN.
A router connects independent LANs or WANs to create an internetwork (internet).

Routing example

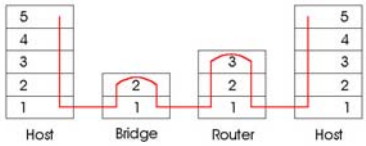


Note

A router changes the physical addresses in a packet.

Bridges Vs. Routers

- 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



Bridges Pros and Cons:

+ Bridge operation is simpler requiring less processing bandwidth, i.e., faster
- 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 Pros and Cons:

+ Arbitrary topologies can be supported, cycling is limited by TTL counters
+ Can provide firewall protection against broadcast storms
- Often requires IP address configuration
  - not plug and play; DHCP is exception
- Require higher processing bandwidth
- Bridges do well in small (few hundred hosts) while routers are required in large networks (thousands of hosts)

Routers vs. Repeaters/Bridges (con't)

- A router has both a ***physical*** and ***logical*** (IP) address for each of its interfaces
- A router acts only on those packets in which the destination address matches the address of the interface at which the packet arrives
  - True for unicast, multicast and broadcast
- A router changes the physical address of the packet (both source and destination) when forwarding the packet

Routers vs. Repeaters/Bridges (con't)

- A router separates collision domains
  - Can improve performance
  - But 3-layer processing more time consuming than 2-layer processing
- Transparent bridges are "*plug-and-play*"
- Routers require configuration (more admin)
- Bridges implement spanning tree over nodes to eliminate cycles
  - Implemented by virtually disconnecting nodes
  - Results in self-imposed traffic increases
  - Frames concentrated on spanning tree links when it could be spread on all links in original topology

Routers vs. Repeaters/Bridges

- If failure in a link, new spanning tree is created automatically
- Bridges offer no protection from layer-2 broadcast storms
- Bridges increase traffic flow and require no manual IP configuration
- Routers provide better isolation of traffic, control broadcast storms and can use more intelligent routes among hosts

Switches

Two (network-related) meanings

- Two-layer switch
  - Bridge with many interfaces
  - Each interface to a new segment with one station
  - No competing traffic on segments (no collisions)
  - Like bridges, vulnerable to broadcast storms
- Three-layer switch
  - Application specific ICs for better performance
  - Customized for specific network layer protocols (IP)
  - In some cases, learn routing tables from routers