COMPSCI 314 S2 T

Data Communications Fundamentals

Lecture Slides, Set #6

Clark Thomborson

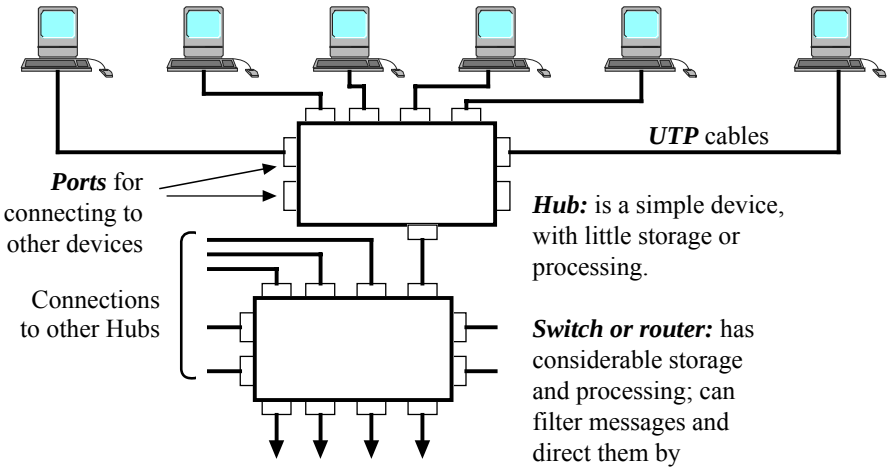
17 September 2007

Review: OSI Layers

1. Physical: Transmit bits from one place to another.
2. Link: Assemble bits into bytes and messages, check for reliable transmission. (The "MAC" sublayer is below the "LLC" sublayer.)
3. Network: Send messages between nodes on different links.
4. Transport: Handle lost packets, broken links, network independence.
5. Session: Handle extended connections.
6. Presentation: Resolve differences between data representation in different computers.
7. Application: Interact with a human.

- These are the seven layers of the "Open Systems Interconnection" (OSI) communications model.

A user connection into a network



Many Types of Connections...

- Additional wire length may be needed on a LAN segment – use ***repeaters*** (also called signal regenerators).
- Additional stations may be needed on a LAN – use ***hubs***.
- A network may have to be subdivided to reduce contention, or to allow more stations – use ***bridges*** or ***switches***.
- Two or more networks may have to be connected together – use ***routers*** (if the networks use the same Network layer protocol) or ***gateways*** (if the networks use different protocol stacks).
- Warning: terminology is **not** standardised.
- Some equipment manufacturers and vendors use the term "router" for what others call a "bridge".
- To add to the confusion… you can buy ***repeater hubs***, ***bridging hubs***, and ***switching hubs***.

Repeaters vs. Hubs; Bridges vs. Switches

- Shay:
  - Hubs have more ports than repeaters. Both work only at L1.
  - Switches have more ports than bridges. Both work at L1 and L2.
- Cisco:
  - A bridge is a "[d]evice that connects and passes packets between **two** network segments that use the same communications protocol. Bridges operate at the data link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame. See also *relay*."
- Most bridges handle just one frame at a time (half-duplex).
- Some switches can handle "wire-speed" frames on all ports simultaneously, even if the frames are minimum-length.
- Read the specification sheets!

Layer Activity of Connectors

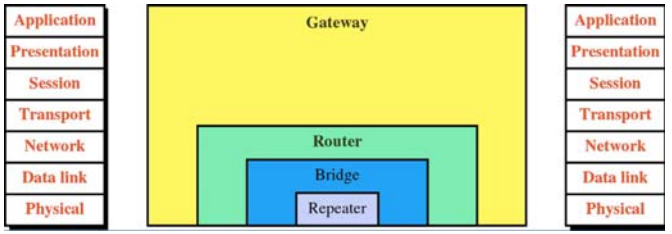
Repeater, Hub – active only at the Physical (L1) layer.

Bridge, Switch – most active at the Link layer (usually MAC).

Router – links separate but similar LANs (⇒ Network layer).

Gateway – provides "translation" service between incompatible LANs or applications ⇒ active in all layers.

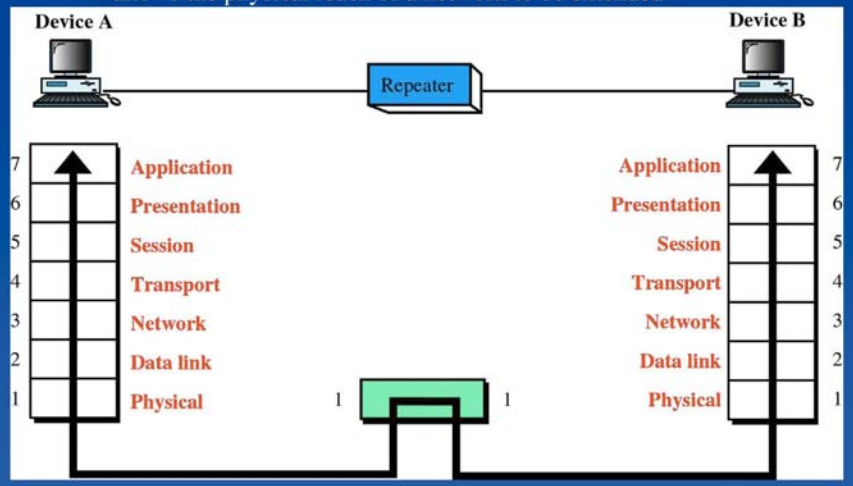
NOTE: each of these devices also operates in all layers **below** the one in which it is most active.



Source: **Dr. Gabriel-Miro Muntean**, http://www.eeng.dcu.ie/~ee210/

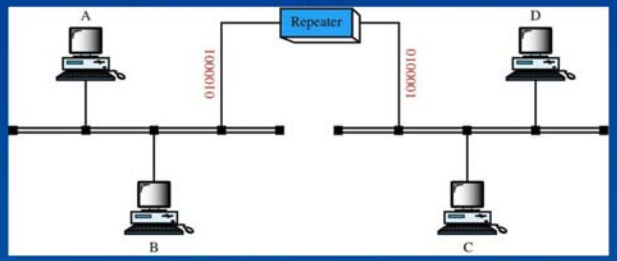
6.1 Internetworking Devices: Repeater

- an electronic device which regenerates ("cleans up") incoming signals
  - allows the physical reach of a network to be extended

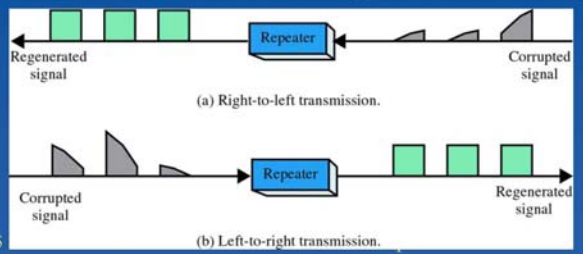


Internetworking Devices: Repeater (cont.)

- a repeater *does not filter* frames, e.g. A's Frame to B also received by C & D

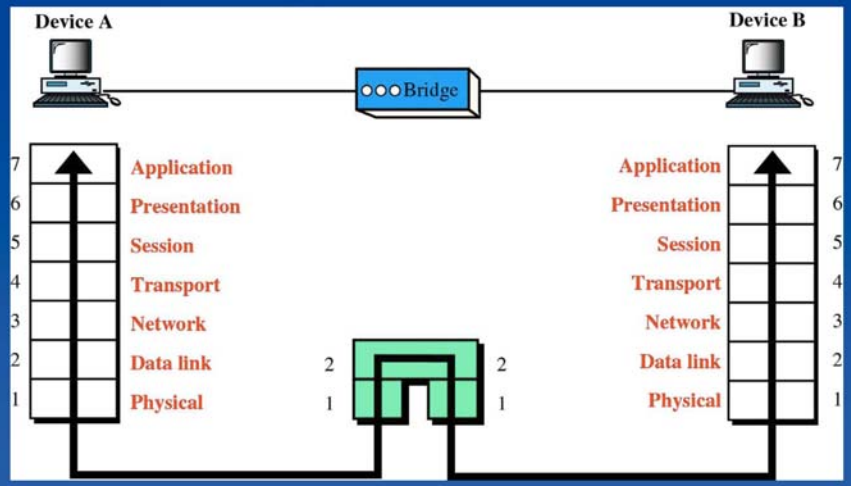


- a repeater copies and "refreshes" incoming bits – it *does not amplify* the signal



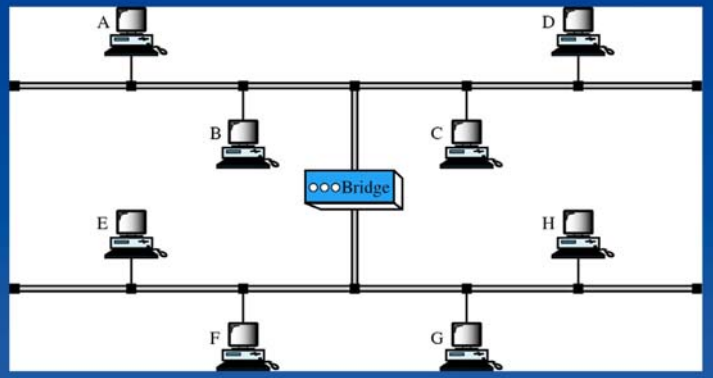
6.2 Internetworking Devices: Bridge

- operates in both the Physical and Datalink layers
  - a bridge knows the physical addresses of the connected nodes



Internetworking Devices: Bridge (cont.)

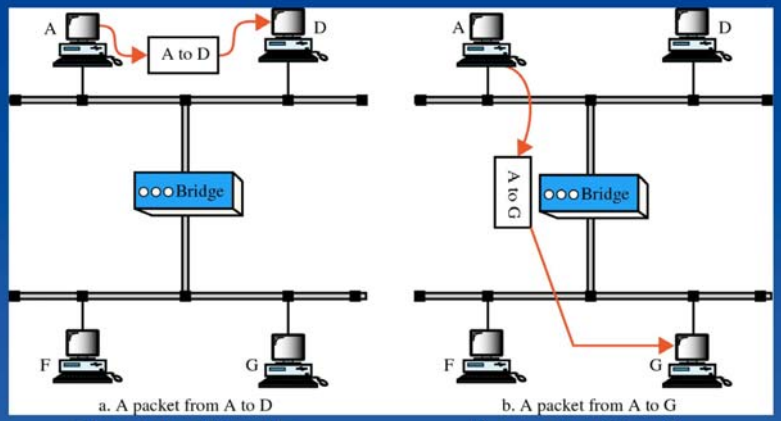
- a bridge can divide a large network into smaller segments, or relay Frames between 2 originally unconnected LANs:



- unlike a repeater, a bridge contains logic which allows it to keep traffic for each segment separate ⇒ ***bridge can filter traffic***
  - helps in controlling traffic congestion, isolating problems, security…

Internetworking Devices: Bridge traffic filtering

- when a Frame arrives, the bridge not only regenerates the signal but also checks the destination address, and only forwards the Frame to the segment to which this address belongs:



a. A packet from A to D

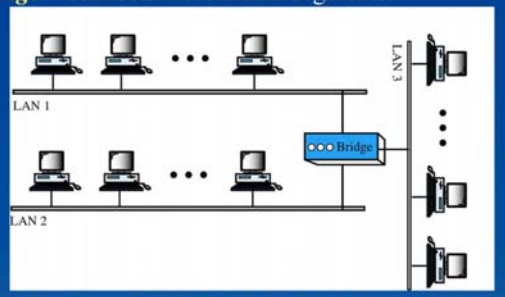
Frame relayed to entire upper segment

b. A packet from A to G

Frame relayed to entire lower segment

Internetworking Devices: Bridge types

- ***simple bridge*** – links 2 segments; node addresses entered manually in bridge table
- ***multi-port bridge*** – connects more than 2 segments:



- ***transparent bridge*** (also called a ***learning bridge***) – builds its tables of addresses automatically as it relays Frames (by noting the source address in each Frame)
  - if more than one bridge connects 2 LANs, a loop could be formed in the bridges' forwarding tables ⇒ Frames could circulate forever
  - transparent bridges learn the topology and build a loop-free **spanning tree**
- ***source routing bridge*** – each sender learns the topology (using *Discovery Frames*) and decides the **exact path** of segments and bridges each of its Frames will take

How Transparent Bridges Learn

- A bridge maintains a ***forwarding database***, or ***routing directory***, so that it can properly route the frames it receives.
- Initially the database is empty.
  - **CREATE TABLE database (address INTEGER, port INTEGER);**
- When a bridge receives a frame it looks for the correct port:
  - **SELECT port FROM database WHERE database.address=DA;**
  - Of course we don't use a relational database system!
  - A hash table will do the trick.
- If no match is found in the database, then the bridge broadcasts the frame on all its other ports ("flooding").
- This bridge may have learned something!
  - **INSERT INTO database VALUES (SA, IN-PORT);**

What Happens When a Machine is Moved?

- The forwarding database should be changed whenever machines and bridges are powered up or down, moved around, links are broken, etc.
- Whenever a hash table entry is updated, its ***inactivity timer*** is reset to some fixed value $T \approx 3$ minutes.
- The bridge purges all records that have been inactive for more than T minutes.

Routing Procedure for a Transparent Bridge

1. If the destination and source ports are the same, discard the frame.
2. If the destination and source ports are different, forward the frame.
3. If the destination port is unknown, use flooding.

Problems:

1. This doesn't scale. Imagine a network with 1000 bridges, 1001 segments, and 10000 nodes. There will be (10000)(1000) = 10 million flood frames!
2. What if there are redundant links (= loops)?
   - Should use IEEE 802.1d (minimum spanning tree).
3. What about stations that rarely send frames, *e.g.* printers?
   - Should statically configure these addresses to avoid repeated floods.

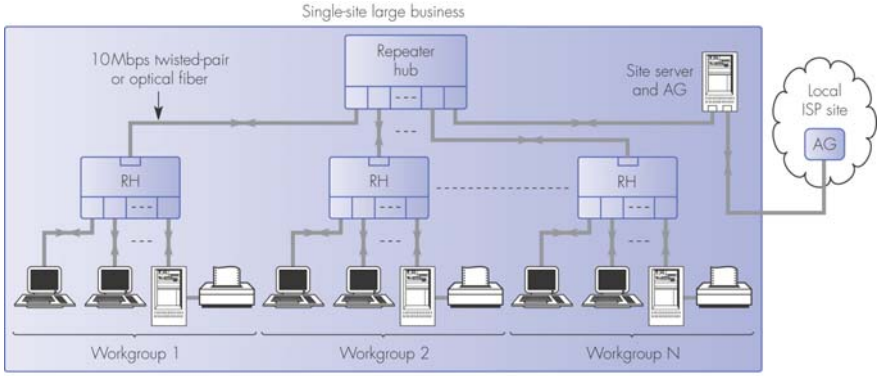


Figure 3.6 (Halsall) Access to the Internet for a single-site large business using repeater hubs only. RH = repeater hub (repeats each frame onto all ports); AG = access gateway; IG = interior gateway.

Can you see any security issues here?

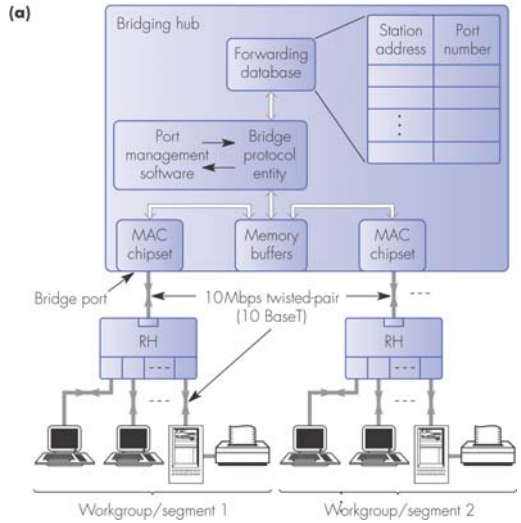


Figure 3.7a (Halsall) Transparent bridging hub schematic. (Why might this system be preferable to using only repeaters? What would Shay call the top device?)

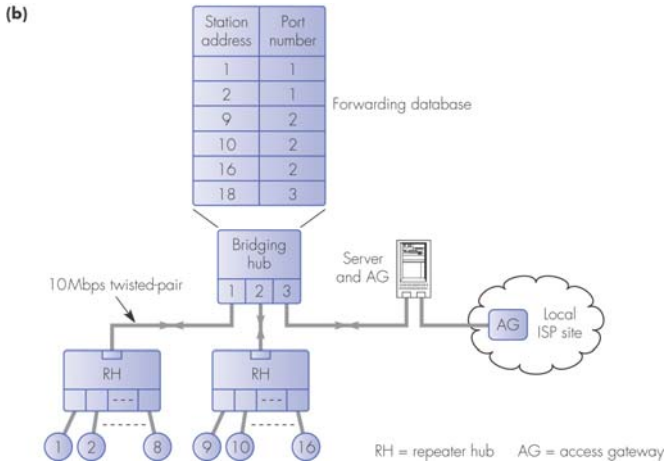


Figure 3.7b (Halsall) Transparent bridging hub schematic. (Is the routing table correct?)

What would **you** call a device with...

- 24 RJ-45, 10/100 Mbps Ethernet LAN ports
- Maximum Bandwidth:
  - Full duplex: 200 Mbps (for 100BASE-TX), 20 Mbps (for 10BASE-T)
  - Half duplex: 100 Mbps (for 100BASE-TX), 10 Mbps (for 10BASE-T)
- Operates at maximum forwarding rate and provides frame filtering and forwarding functions for each port
  - 14,880 packets per second for 10 Mbps ports
  - 148,800 packets per second for 100 Mbps ports
- Store-and-forward scheme to forward packets
- MAC address table: 4096 entries
- Packet buffer: 256 KB
- IEEE 802.3x Flow Control
  - Half-duplex: Back pressure
  - Full-duplex: Pause frame

USRobotics:
"24 Port 10/100 Mbps Switch"

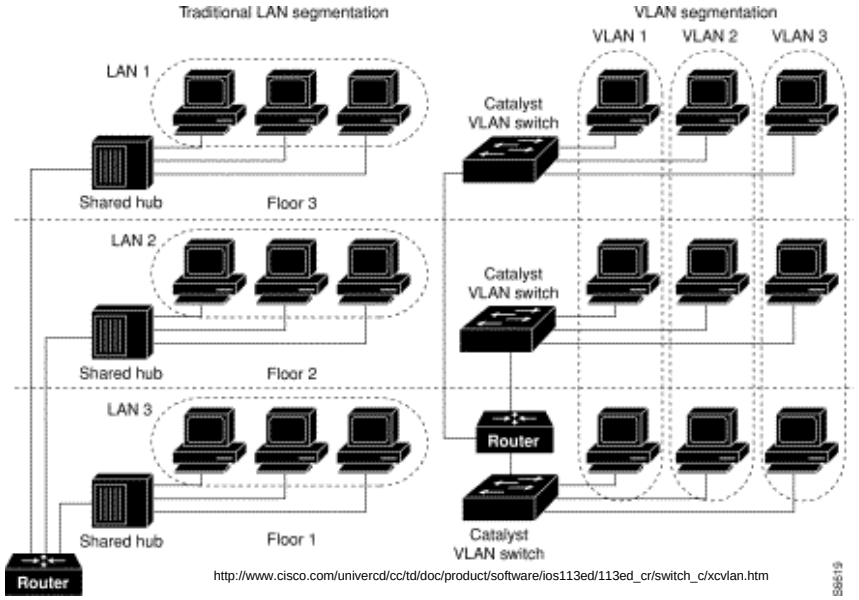
Is this a repeater, hub, bridge, or switch?

- Eight RJ-45, 10/100 Mbps Fast Ethernet LAN ports
  - Crossover cable detection on each port
- Maximum Bandwidth:
  - Full-duplex: 200 Mbps (for 100BASE-TX), 20 Mbps (for 10BASE-T)
  - Half-duplex: 100 Mbps (for 100BASE-TX), 10 Mbps (for 10BASE-T)
- No other functional specs
- USRobotics: "8 Port 10/100 Ethernet Switching Hub"

Virtual LANs

- Imagine a workplace with a hundred computers on a 100BaseT Ethernet
  - Fourteen 8-port hubs, at $50 apiece: $700.
  - Five 24-port transparent switches, at $400 apiece: $2000.
  - Do you see any advantage to the transparent switch architecture, which might justify its 3x cost? (Explain.)
- A network manager might try to be clever when connecting computers to switches.
  - If most of the network traffic stays within a workgroup,
  - If each workgroup has its own transparent switch, and
  - If the routing tables are static, then ...
  - There won't be much traffic through the centre switch.
  - This is a ***lot of work*** for the network manager!

LANs versus VLANs



Advantages of VLANs over LANs

- Scalability
  - Broadcasts (e.g. floods) and multicasts stay within a VLAN
- Security
  - High-security users can be put on the same physical link. Their VLAN traffic doesn't go outside the link, but they can still communicate with other users, servers and printers on the local network.
- Network management
  - Low-security users can be put on any low-security link. They can be organised into workgroups depending on their job description, rather than by their physical location.
  - When a user is moved to a new physical address, they can use their old VLAN address.

Can you see any disadvantages?

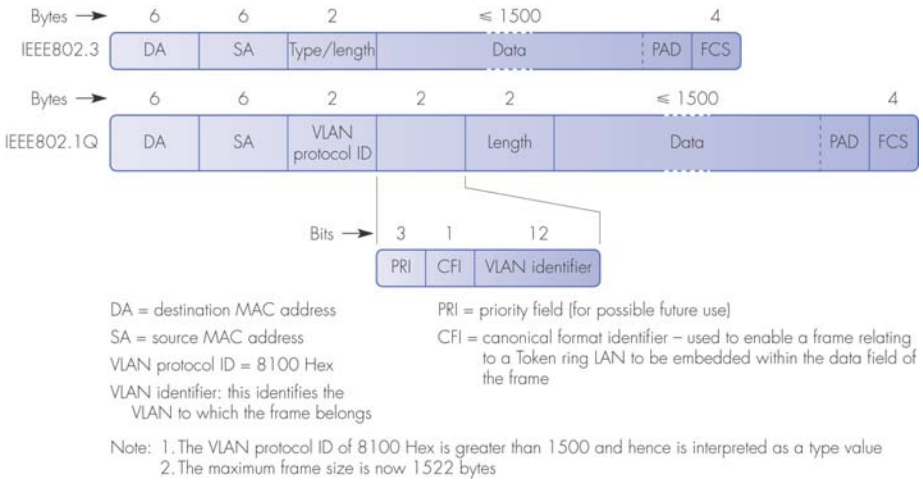


Figure 3.15 IEEE802.1Q frame format and field descriptions.

Will a 802.3 repeater or bridge correctly handle 802.1Q frames?