COMPSCI 314 S1 C

Data Communications Fundamentals

Lecture Slides, Set #3

Clark Thomborson

27 March 2006

What sort of a student are you?

- "C" student: attends most lectures, reads the textbook only when it seems necessary to do homework, learns terminology and basic concepts.
- "B" student: pays attention during lectures, reads textbook carefully *before* the lecture on that topic, completes homework, develops a competent understanding of the material emphasized in homework and lectures.
- "A" student: asks and answers their own questions, using outside sources if necessary; develops a critical and appreciative understanding of the textbook and the lecturer; works creatively with what they have learned.

Critical and Appreciative Views

- "I think networks, as taught in COMPSCI 314, are a boring and bewildering mess of detail. Where are the underlying scientific concepts?"
- "I want to learn how to set up and administer a network for a small office – or for a large corporation!"
- "I want to learn enough to get hired as a network administrator when I graduate."
- What is your current view of this class? Can you develop a view that will motivate you to be an "A" student?

Layers in a Communication System

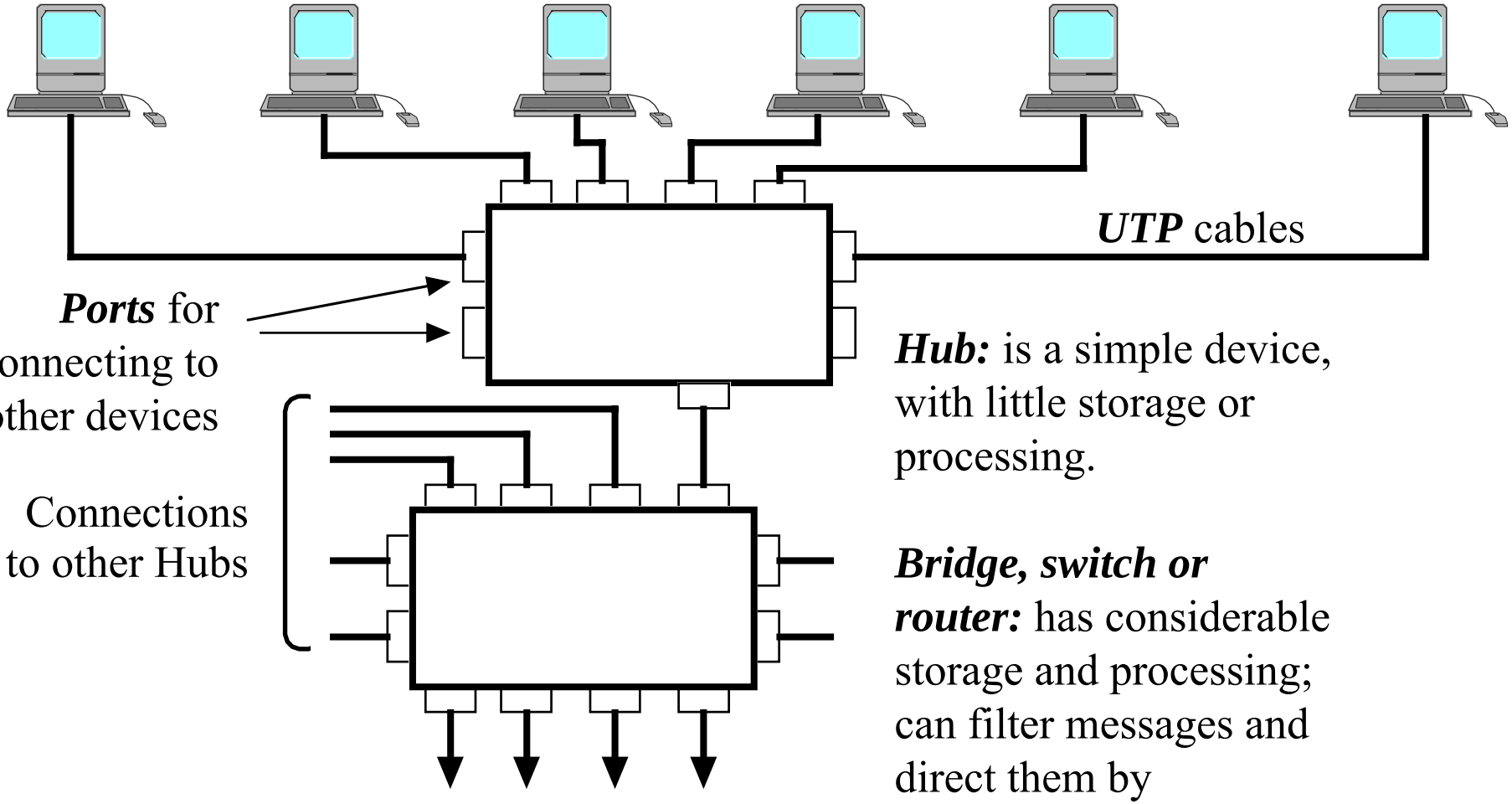
1. Physical: Transmit bits from one place to another.
2. Link: Assemble bits into bytes and messages, check for reliable transmission. (The "MAC" sublayer is below the "LLC" sublayer.)
3. Network: Send messages between nodes on different links.
4. Transport: Handle lost packets, broken links, network 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.

  (Compare with Figure 1.38?)

- We concentrate on levels 1 through 4 in COMPSCI 314.

A user connection into a network



Hub: is a simple device, with little storage or processing.

Bridge, switch or router: has considerable storage and processing; can filter messages and direct them by destination address.

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*** or ***switches***.
- A network may have to be subdivided to reduce contention, or to allow more stations – use ***bridges***.
- 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… we have ***repeater hubs***, ***bridging hubs***, and ***switching hubs***.

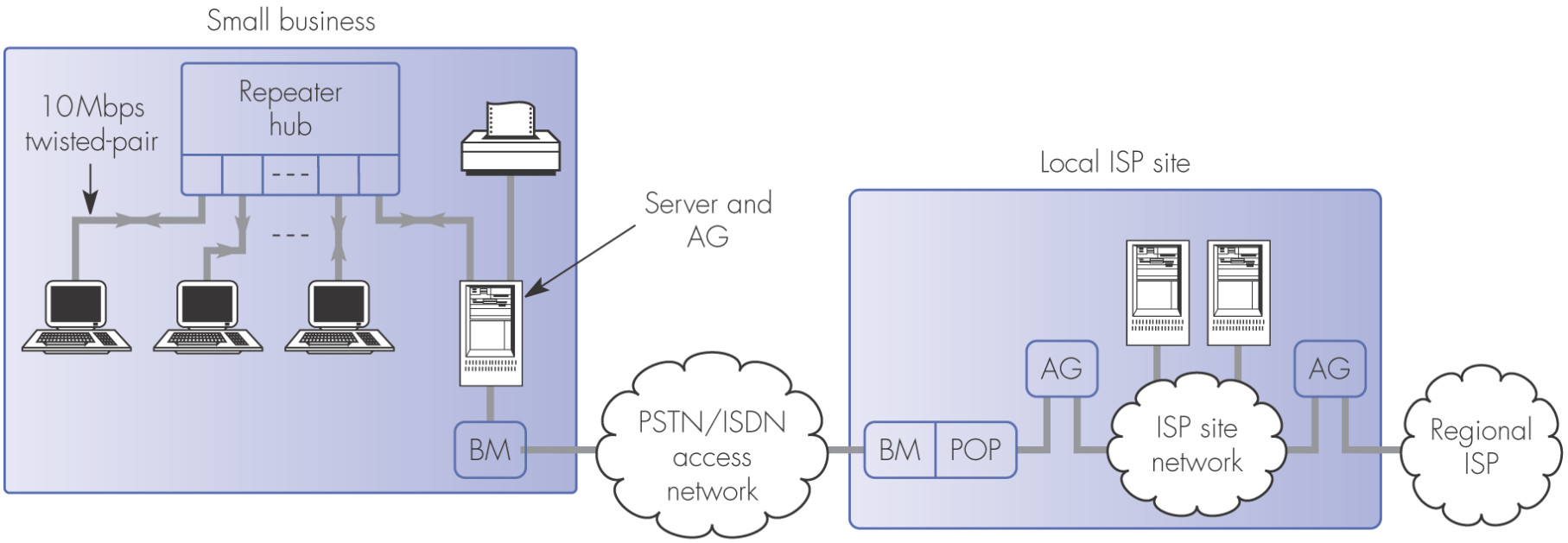


Figure 3.5 Access to the Internet for a small business.
AG = access gateway; IG = interior gateway;
ISP = internet service provider; BM = broadband modem;
POP = point of presence.

What OSI level(s) are handled by each of these devices?

Layer Activity of Connectors

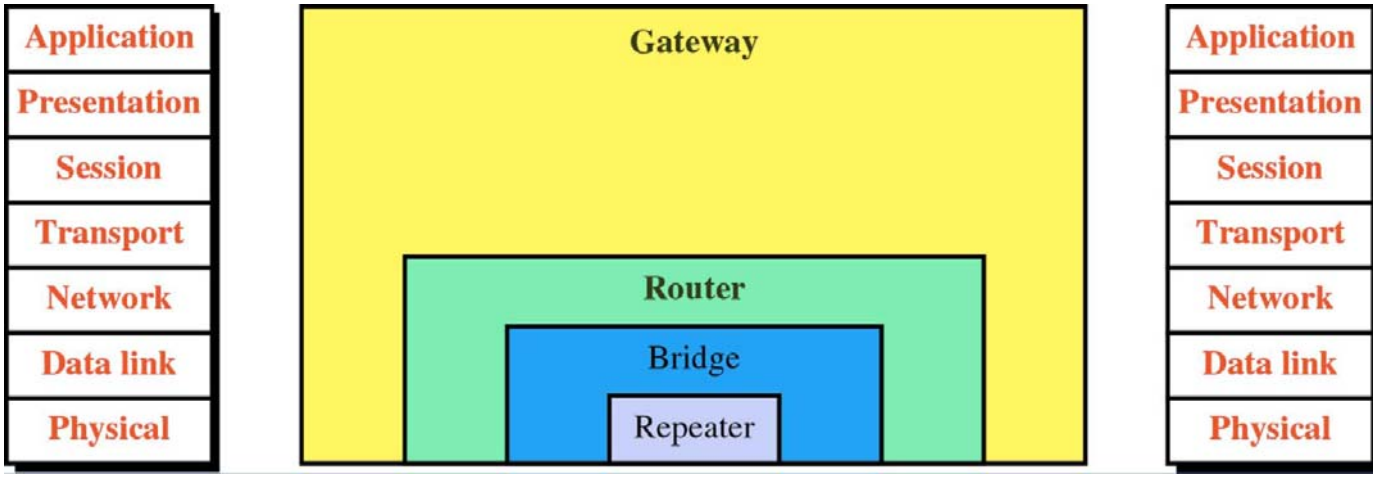
Repeater – active only at the Physical layer.

Hub, Bridge – 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.

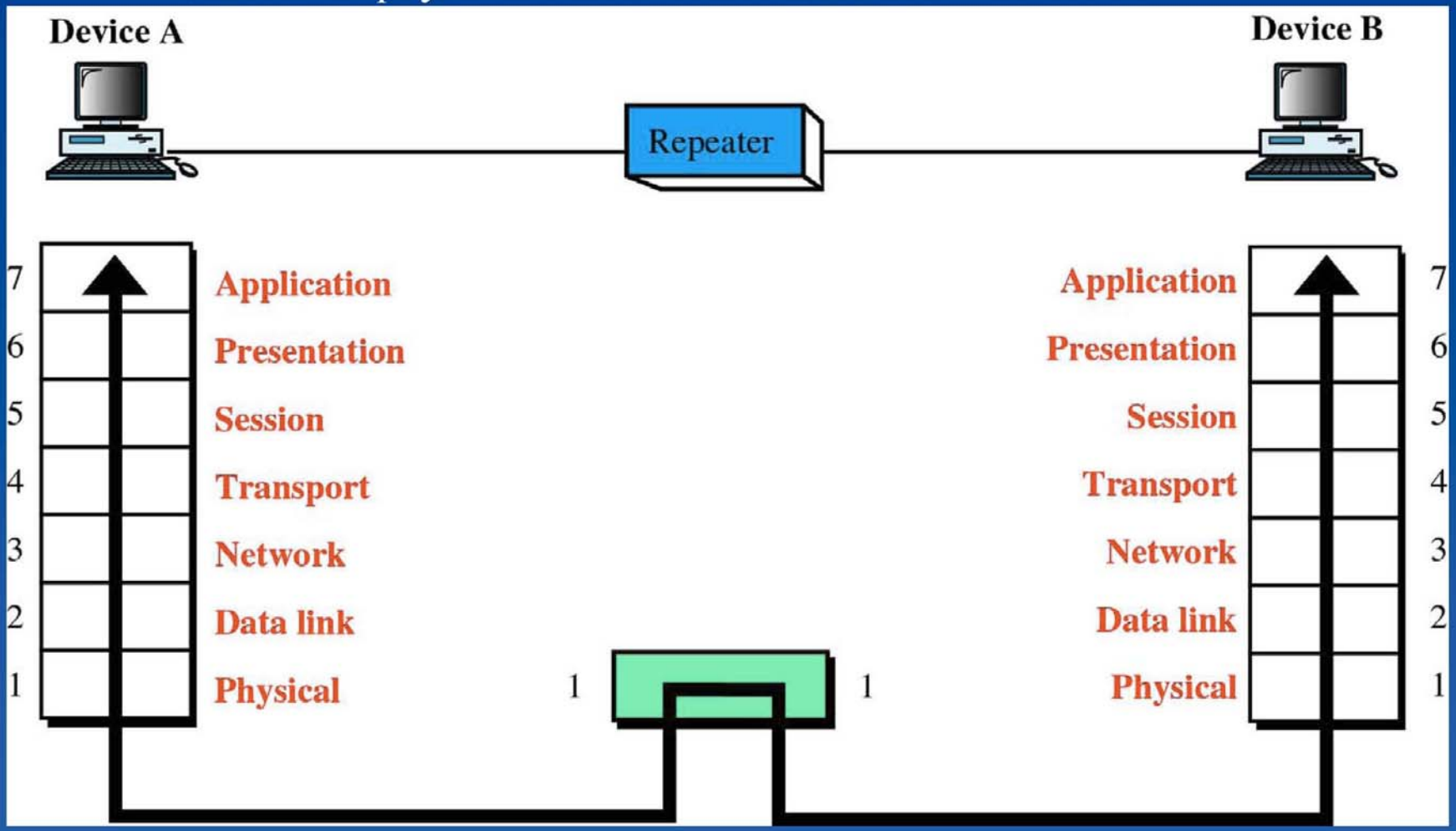
NOTE: each of these devices also operates in all layers **below** the one in which it is most active.



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

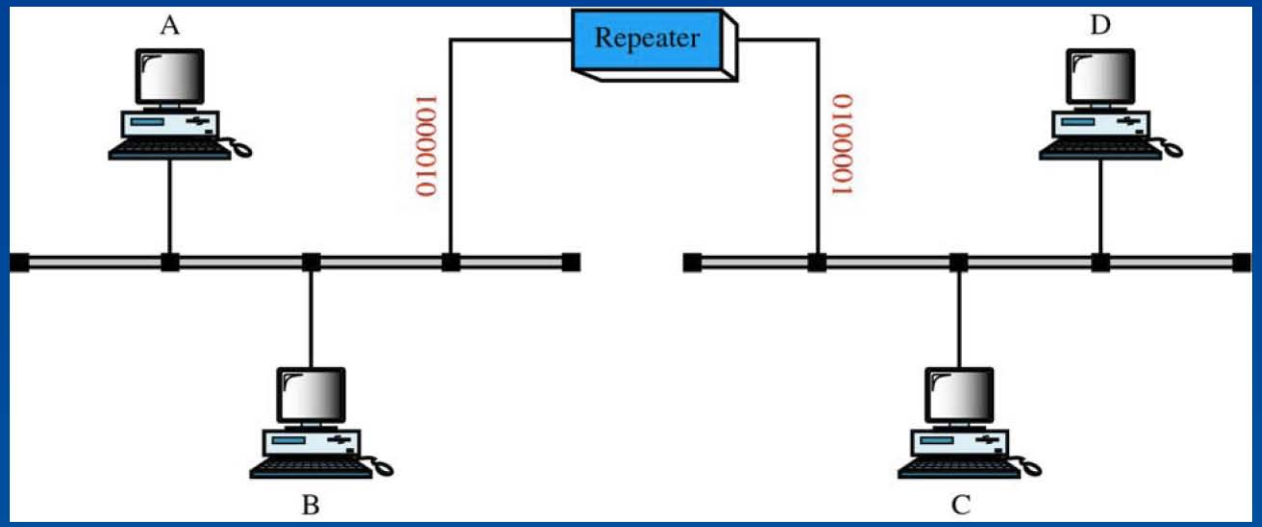
6.1 Internetworking Devices: Repeater

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

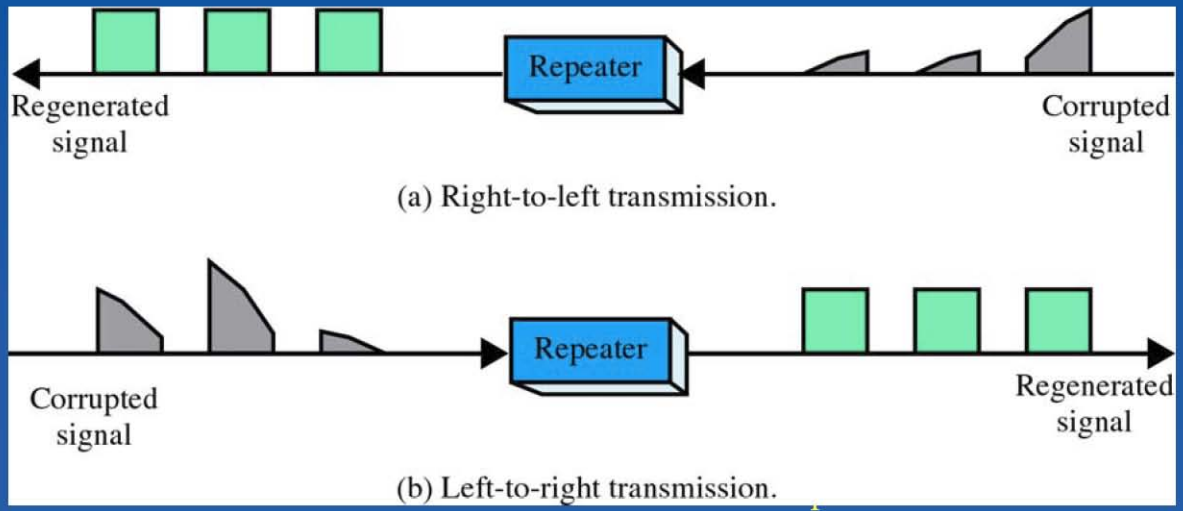


Internetworking Devices: Repeater (cont.)

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

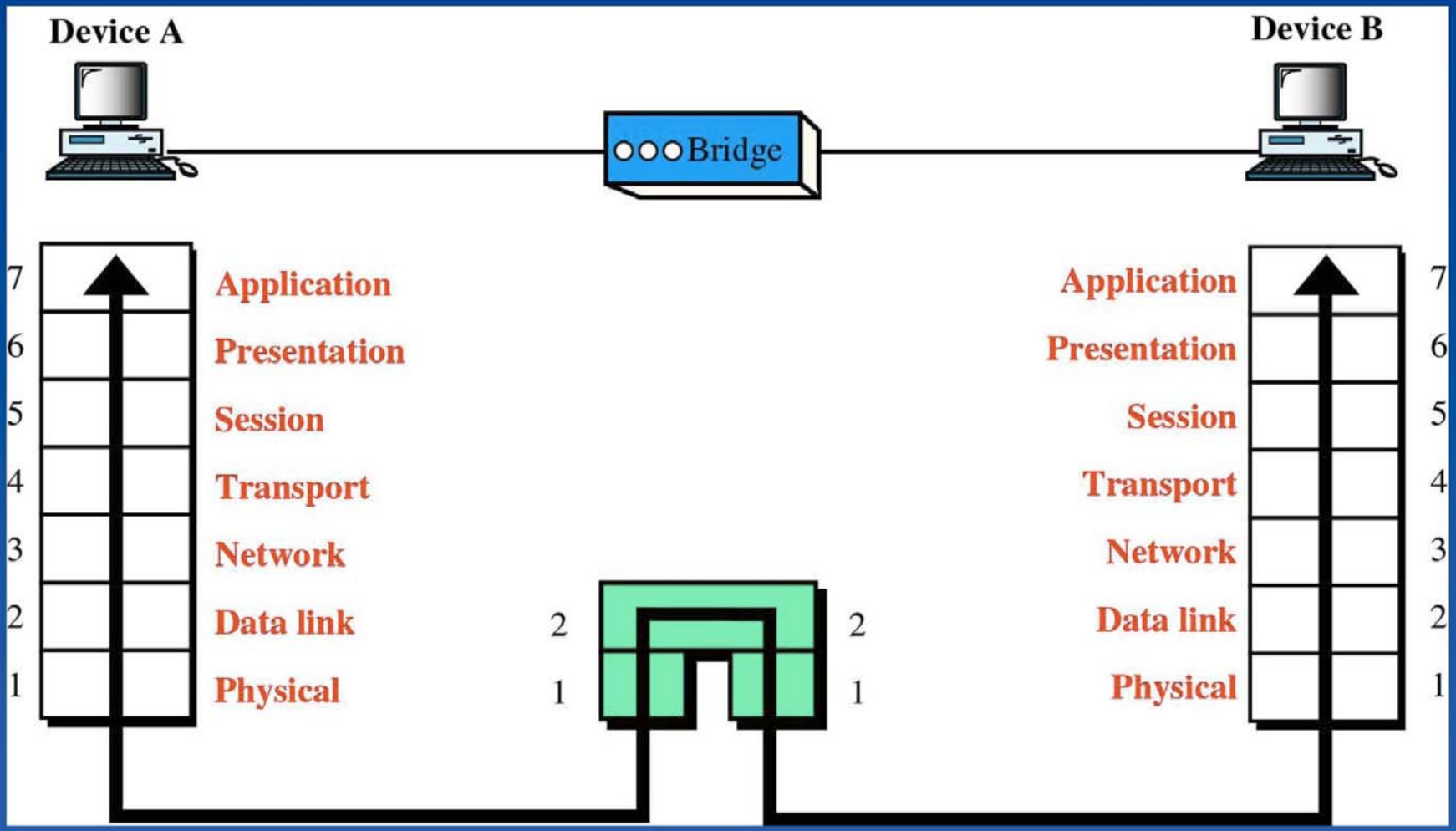


- a repeater copies and "refreshes" incoming bits – it ***does not amplify*** the signal



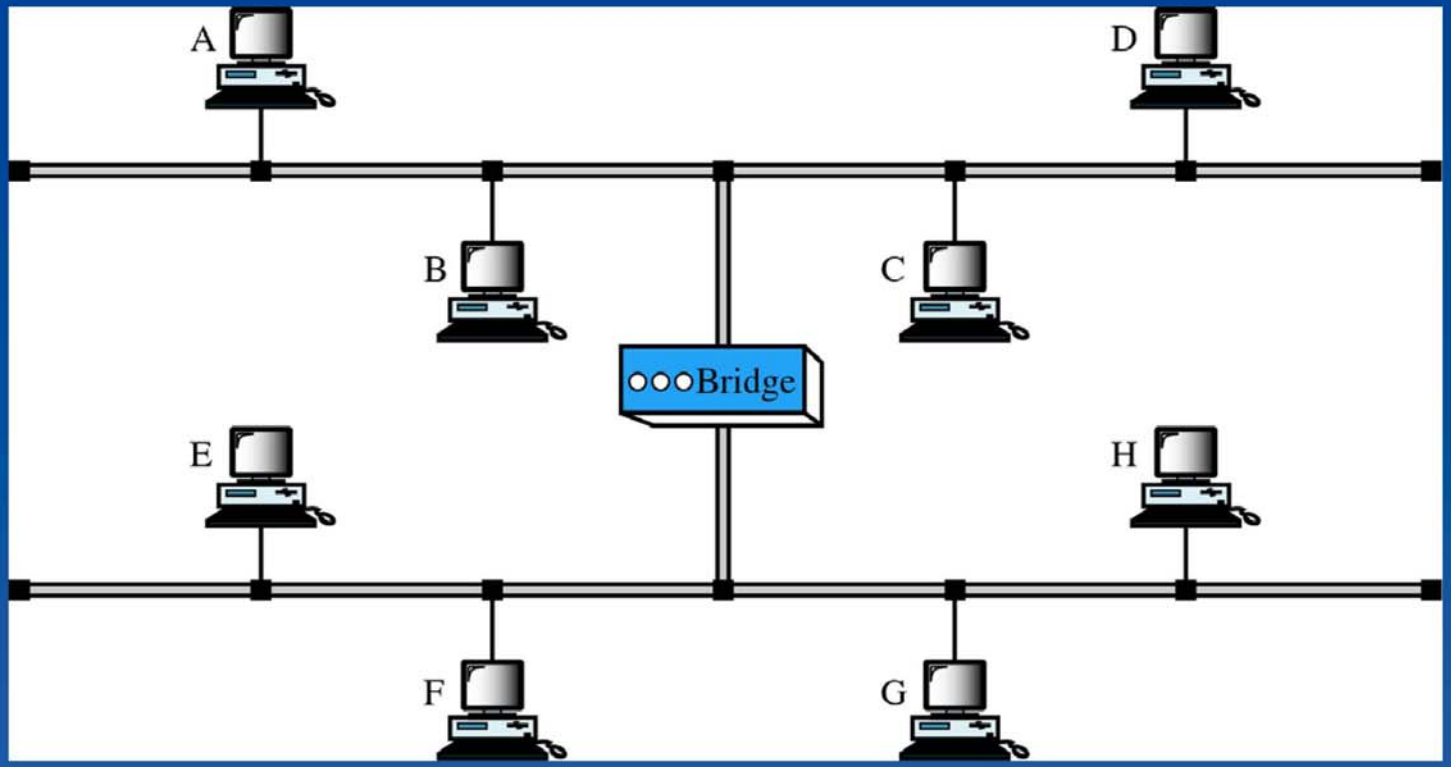
6.2 Internetworking Devices: Bridge

- 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:

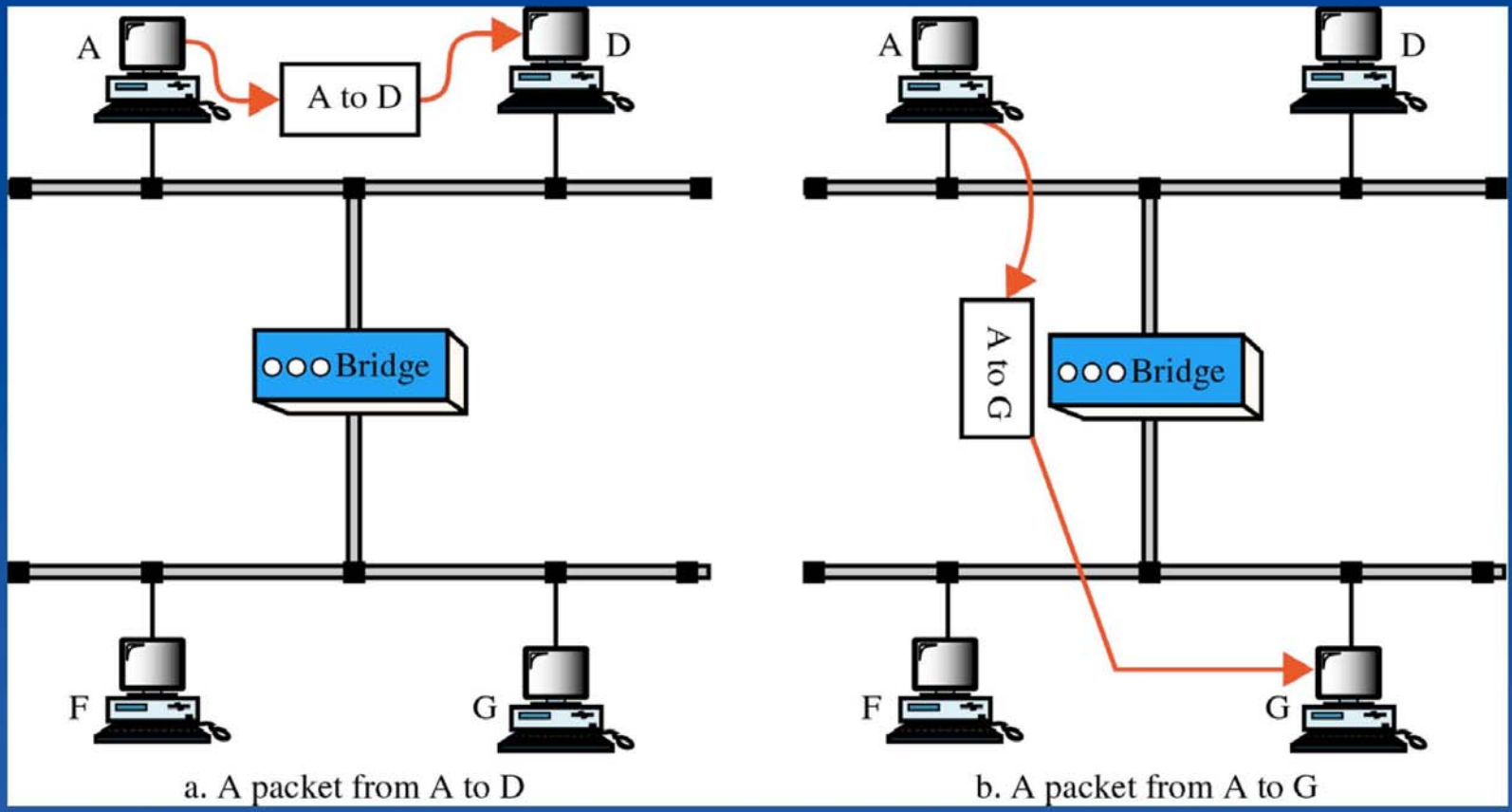


• unlike a repeater, a bridge contains logic which allows it to keep traffic for each segment separate ⇒ ***bridge can filter traffic***

  • 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:

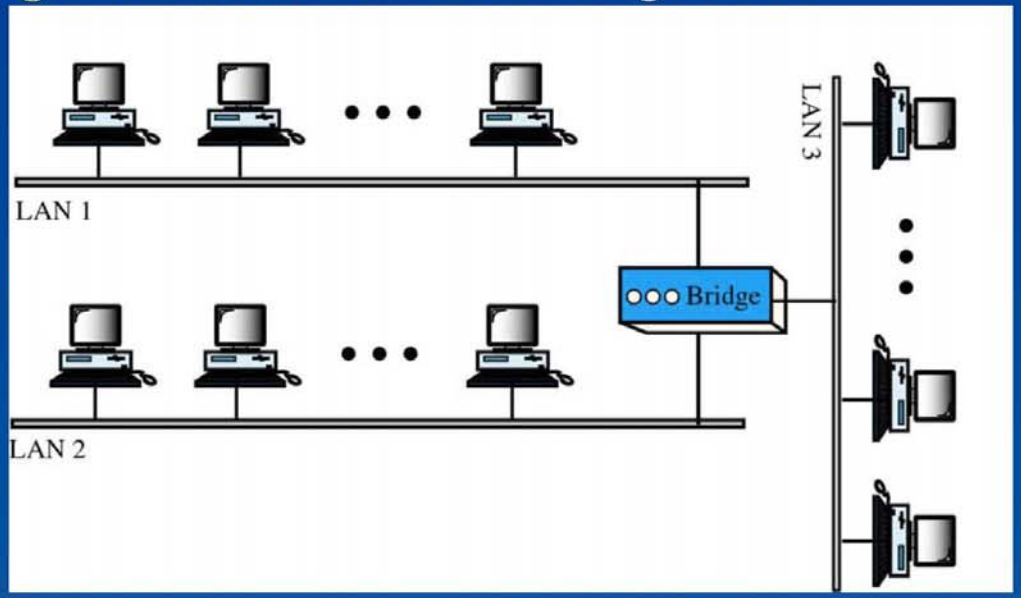


Frame relayed to entire upper segment

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.

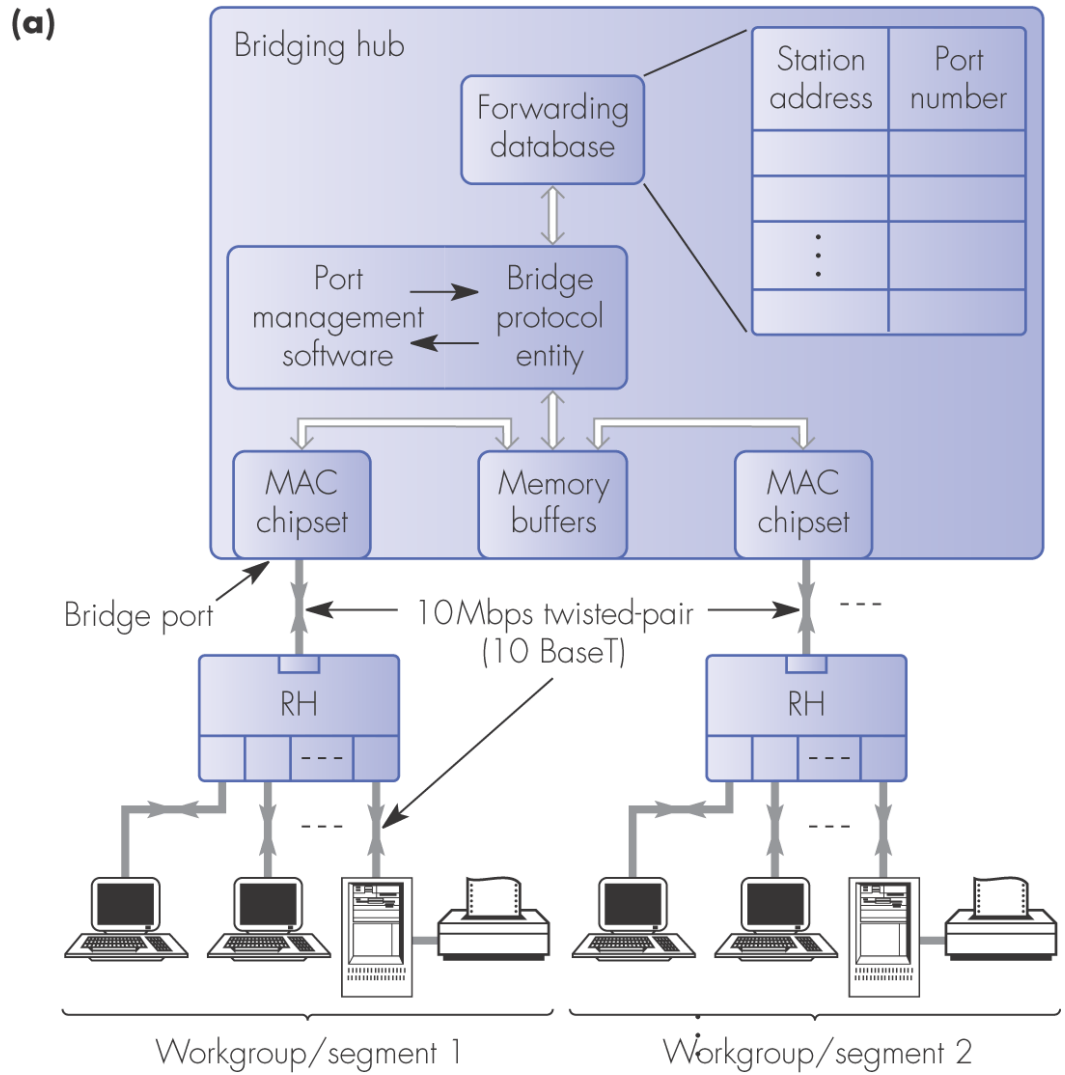


Figure 3.7 Transparent bridging hub schematic: (a) general topology. (Why might this be preferable to using repeaters?)

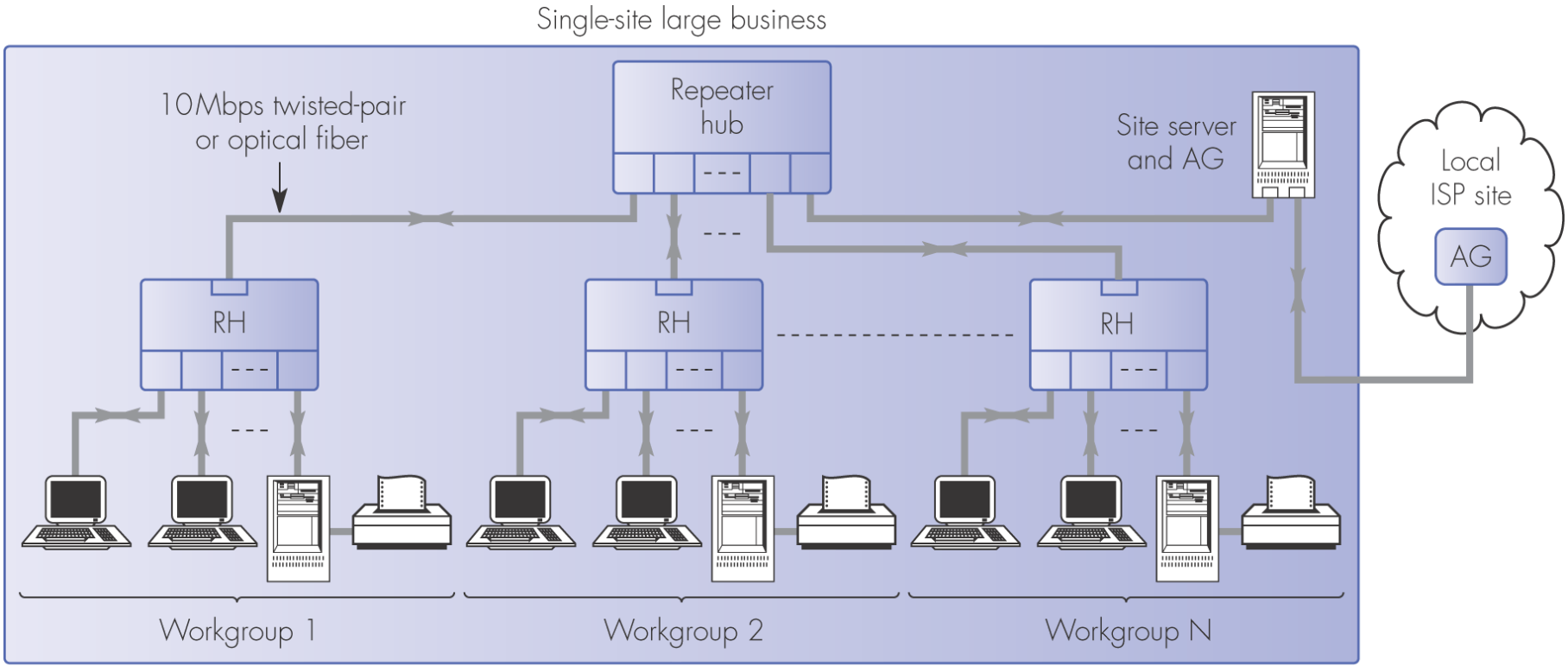


Figure 3.6 Access to the Internet for a single-site large business using repeater hubs only. RH = repeater hub (repeats each frame onto all ports); AG = access gateway; IG = interior gateway.

Can you see any security issues here?

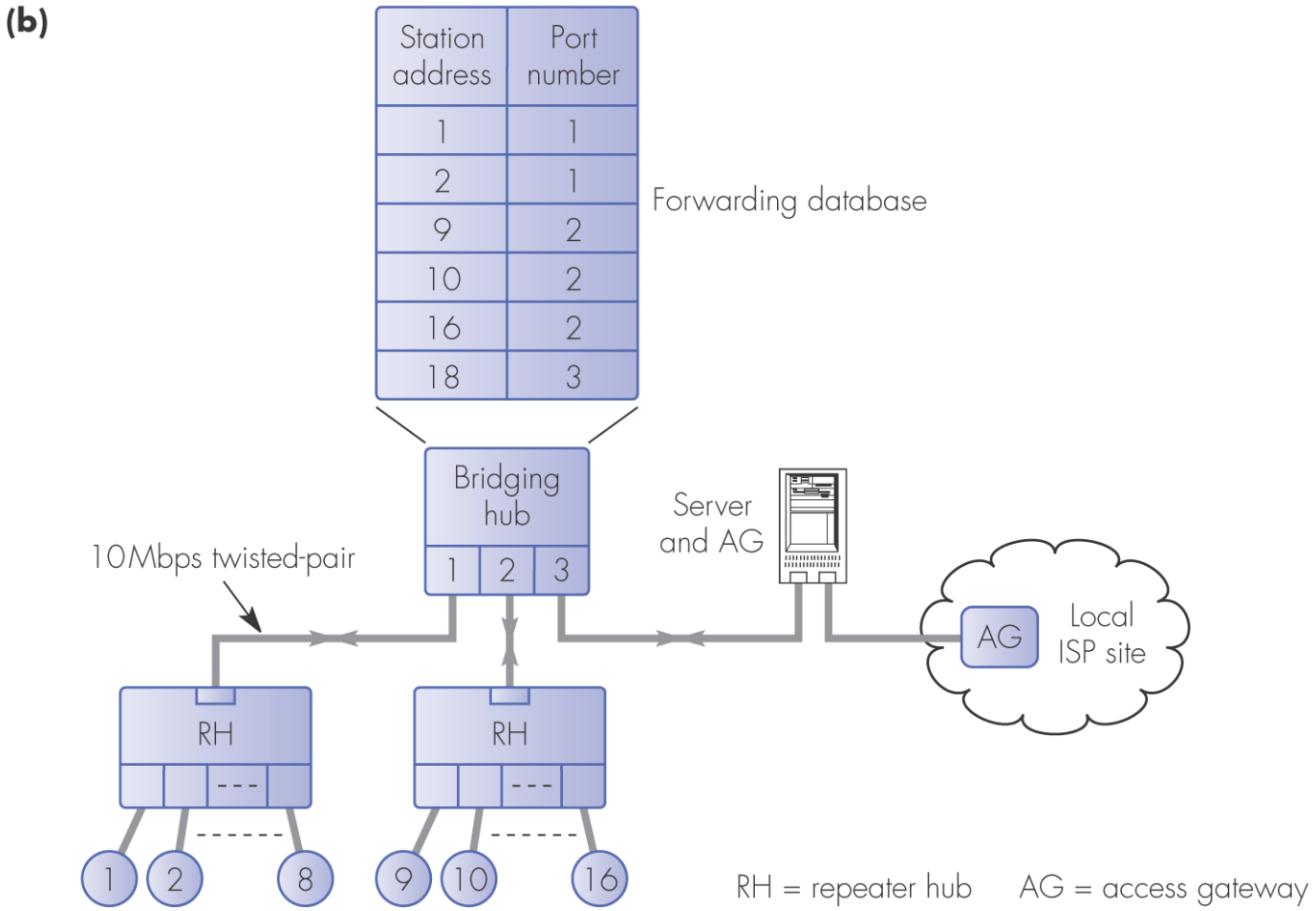


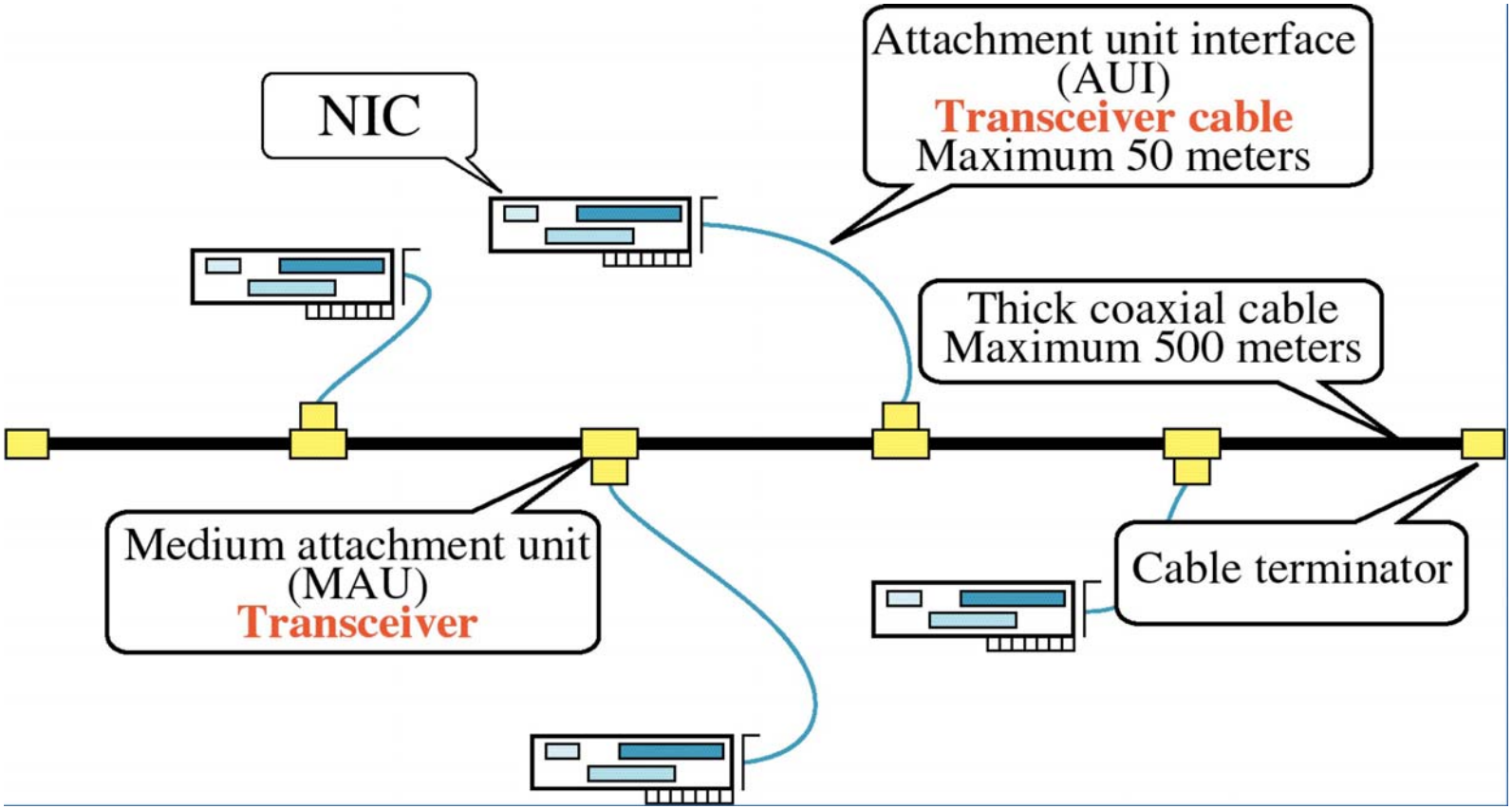
Figure 3.7 Transparent bridging hub schematic: (b) multiport bridge example. (Is the routing table correct?)

Switching Hubs versus Bridging Hubs

- 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.
- Switches may have more ports than bridges, e.g. 16 vs. 4.
  - 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*."
- According to your textbook, switches route any-to-any, whereas a bridge will discard frames that would be routed to the same link.
- Read the specification sheets!

Review: 10Base5 “Thick Ethernet”

- **10 Mbps, Baseband (digital encoding), maximum channel length = 500 metres, 0.5” diameter coax.**

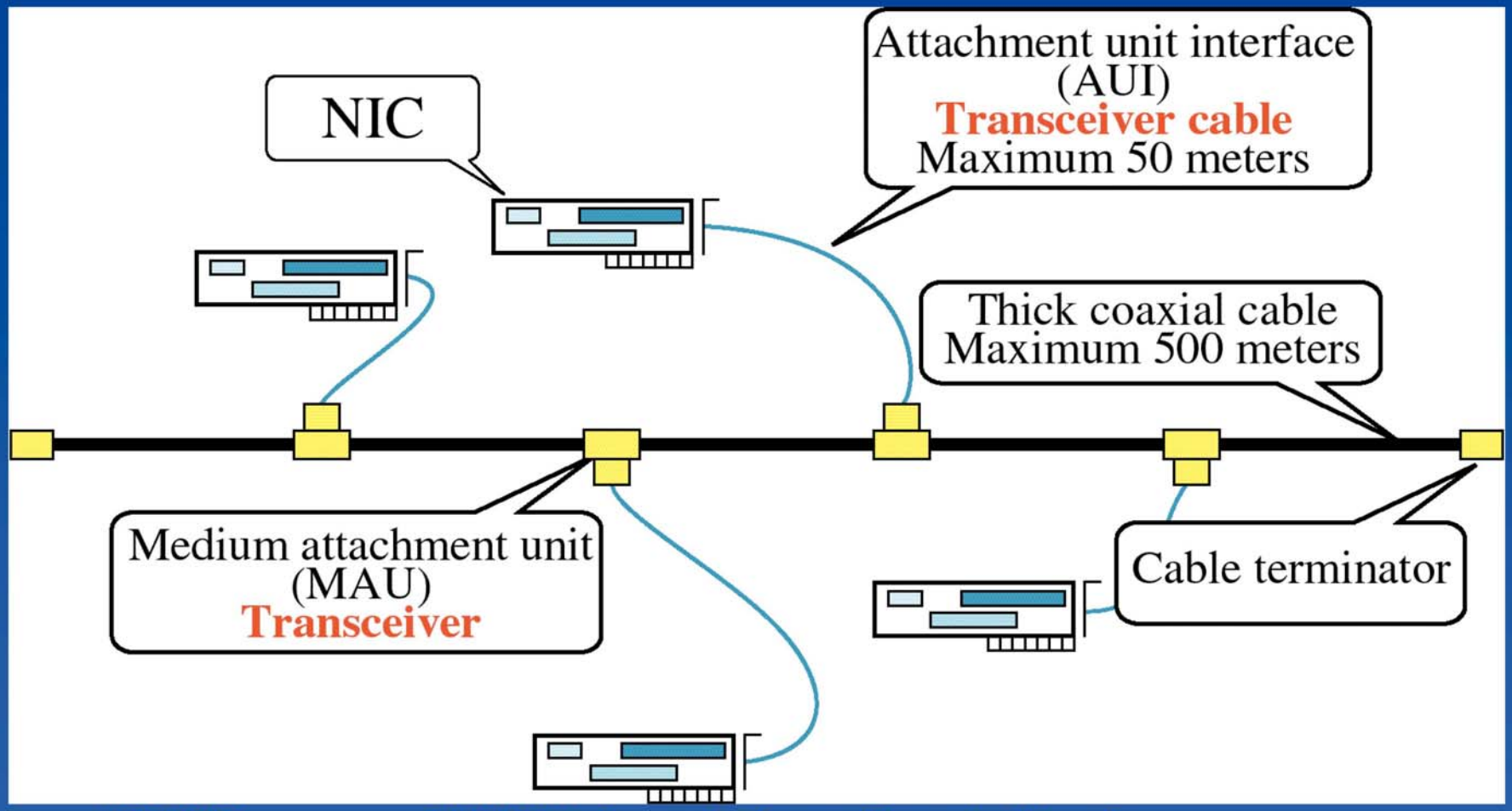


Source: **Dr. Gabriel-Miro Muntean**, http://www.eeng.dcu.ie/~ee210/

Datalink layer: Ethernet Implementations (1)

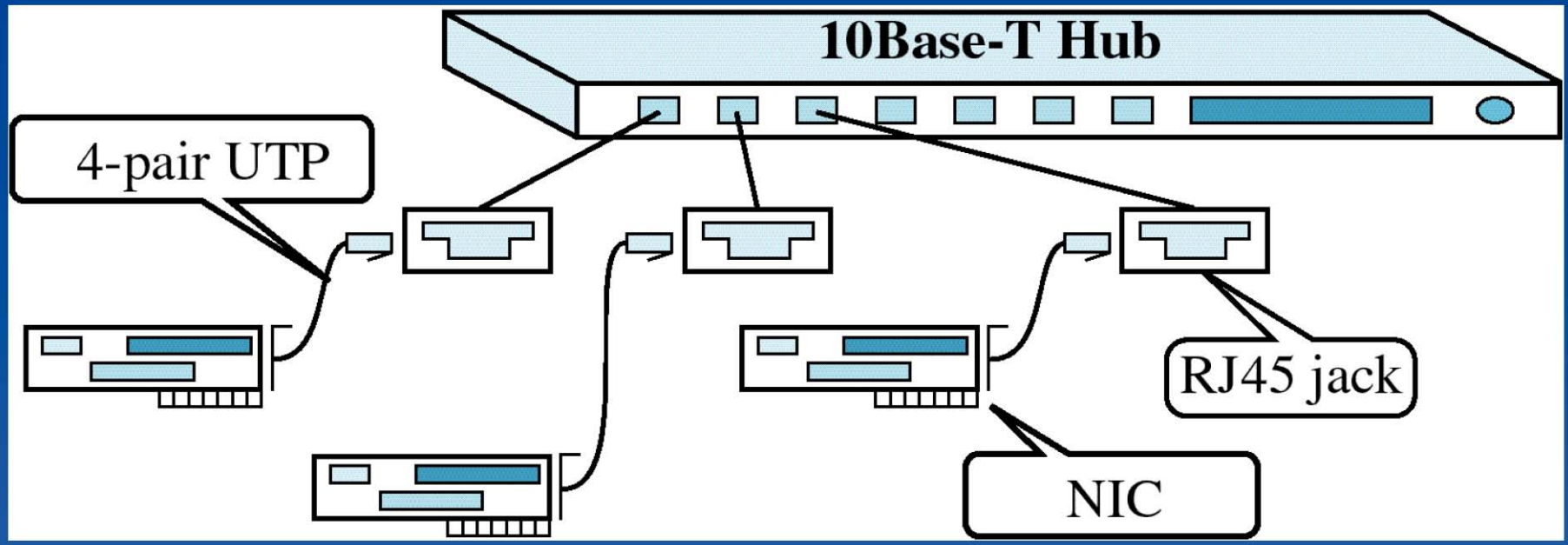
10Base5: 10 Mbps, Baseband (digital encoding), maximum channel length = 500 metres

(also called "Thick Ethernet")



Datalink layer: Ethernet Implementations (3)

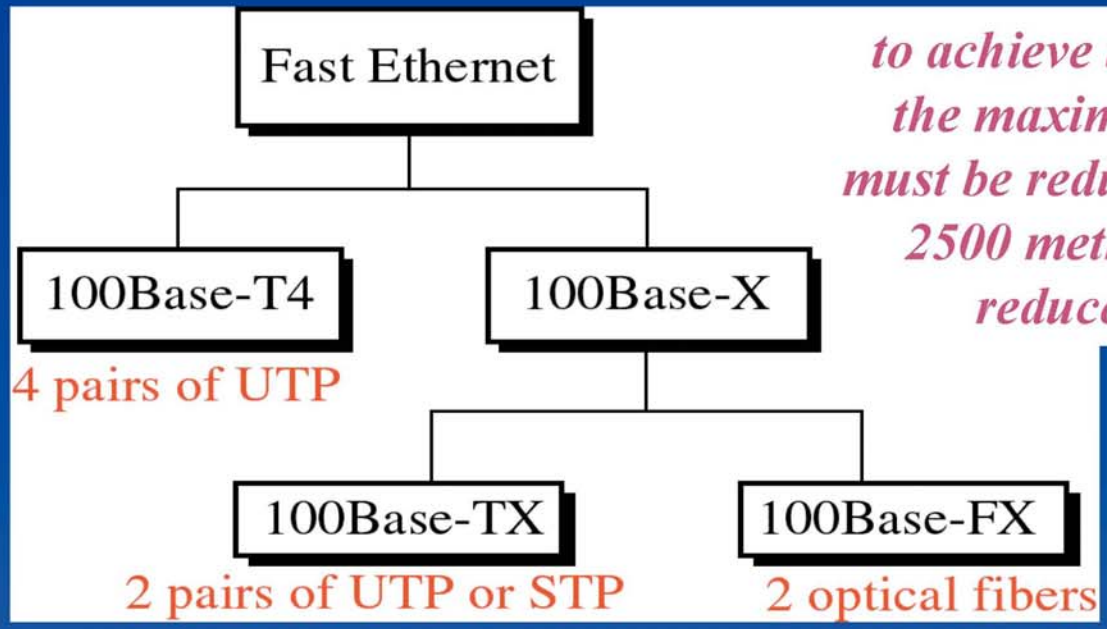
10BaseT: 10 Mbps, Baseband (digital encoding), twisted pair wiring, maximum length hub-to-node = 100 metres



logically still a bus topology, although physical topology is a star

Datalink layer: Ethernet Implementations (5)

Fast Ethernet: increase channel bandwidth to 100 Mbps

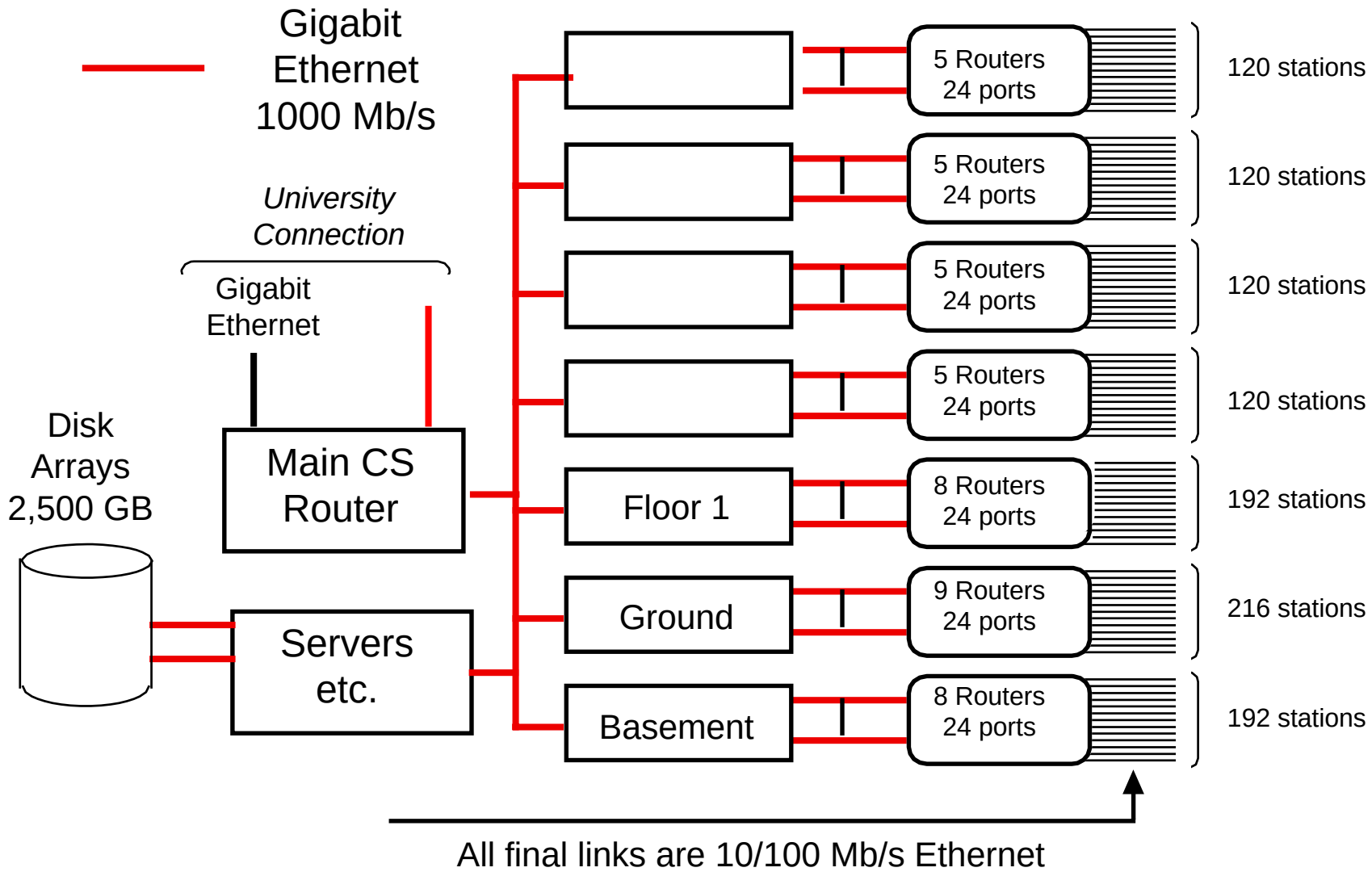


to achieve this 10-fold speedup, the maximum channel length must be reduced by a factor of 10: 2500 metres (with repeaters) reduced to 250 metres

Gigabit Ethernet: increase channel bandwidth to 1000 Mbps = 1 Gbps

- **mainly intended for use with optical fibres**
- **maximum channel length reduced to 25 metres**
- **usually for backbone connection between Fast Ethernet networks**

Simple view of Computer Science Network, 2003



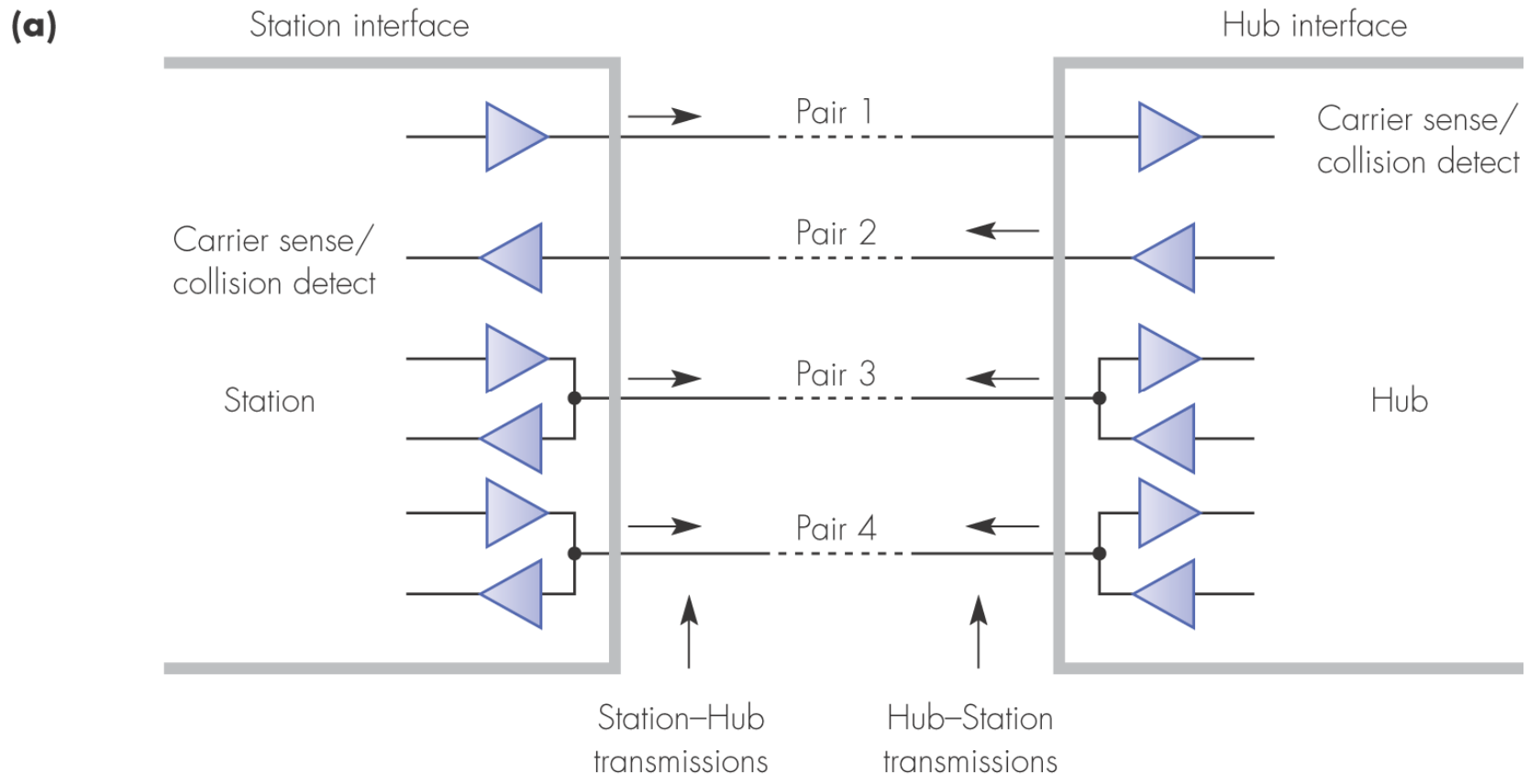


Figure 3.9 100Base4T: (a) use of wire pairs.

Why is this relevant information?

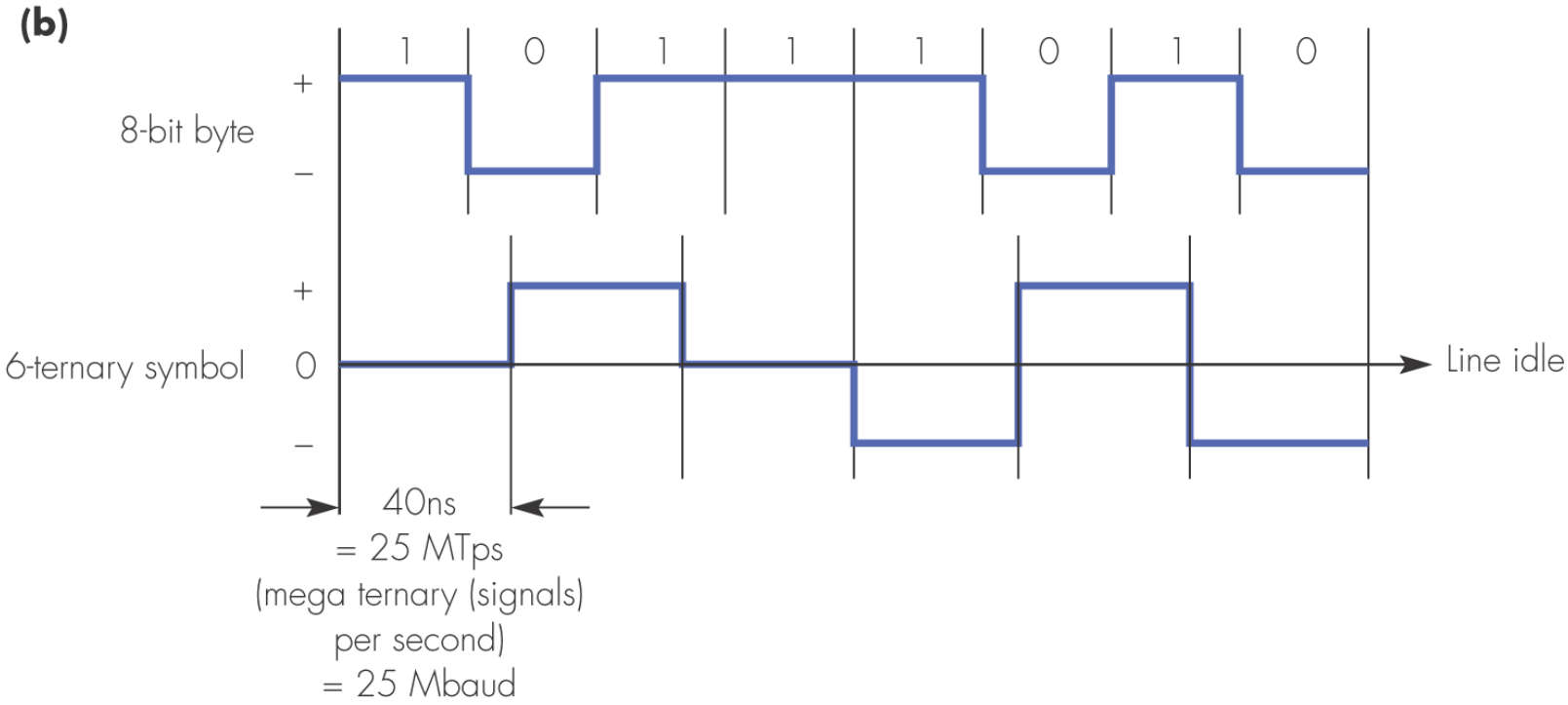


Figure 3.9 100Base4T: (b) 8B6T encoding.

What are the desirable properties of this code?

Have you learned anything interesting about coding theory from this example?

Might coding theory ever be relevant to you again?

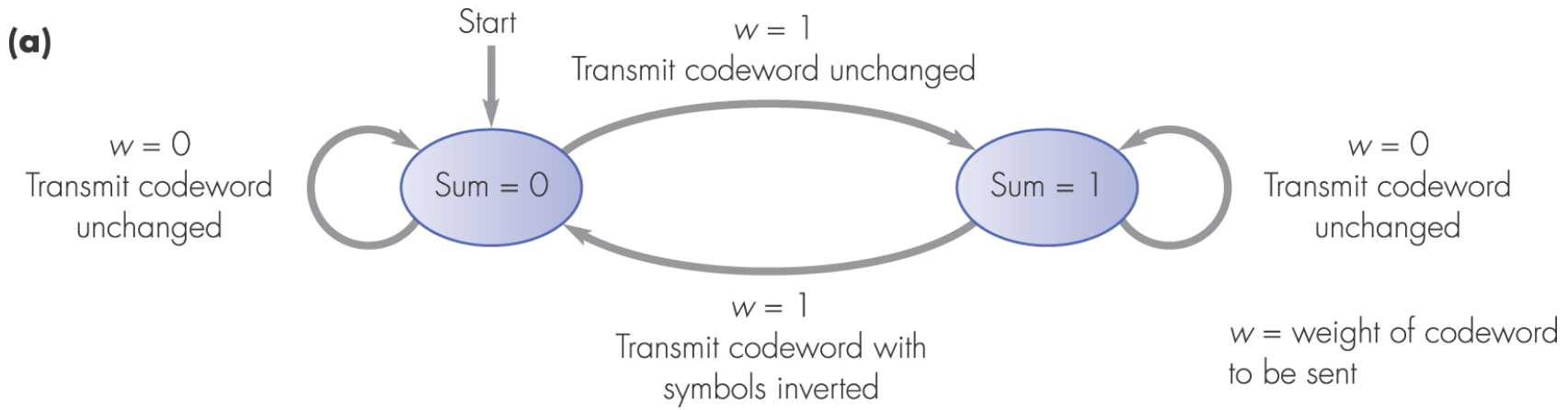


Figure 3.10 100Base4T transmission detail: (a) DC balance transmission rules.

Can you “hand-execute” this finite state machine?

Isn’t this a clever way to ensure DC balance?

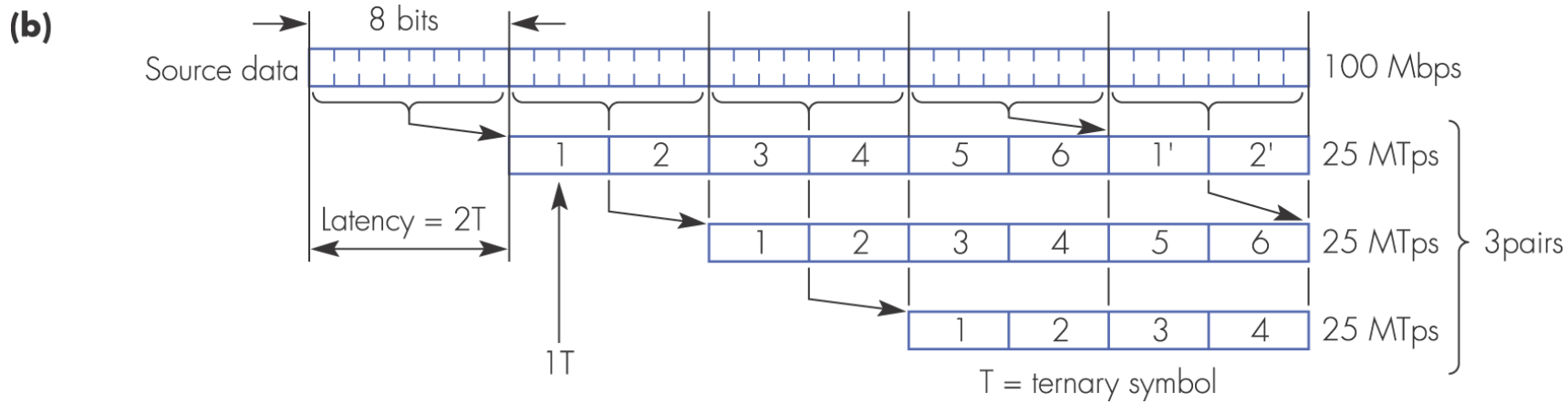
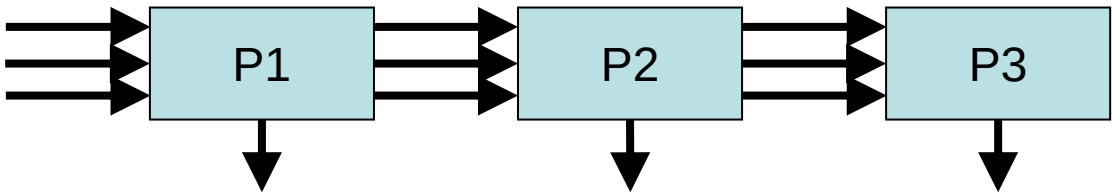


Figure 3.10 100Base4T transmission detail: (b) 8B6T encoding sequence.

Your textbook says "This means that the sequence of symbols received on each pair can be decoded independently. Also the frame can be processed immediately after the last symbol is received." Do you understand this?



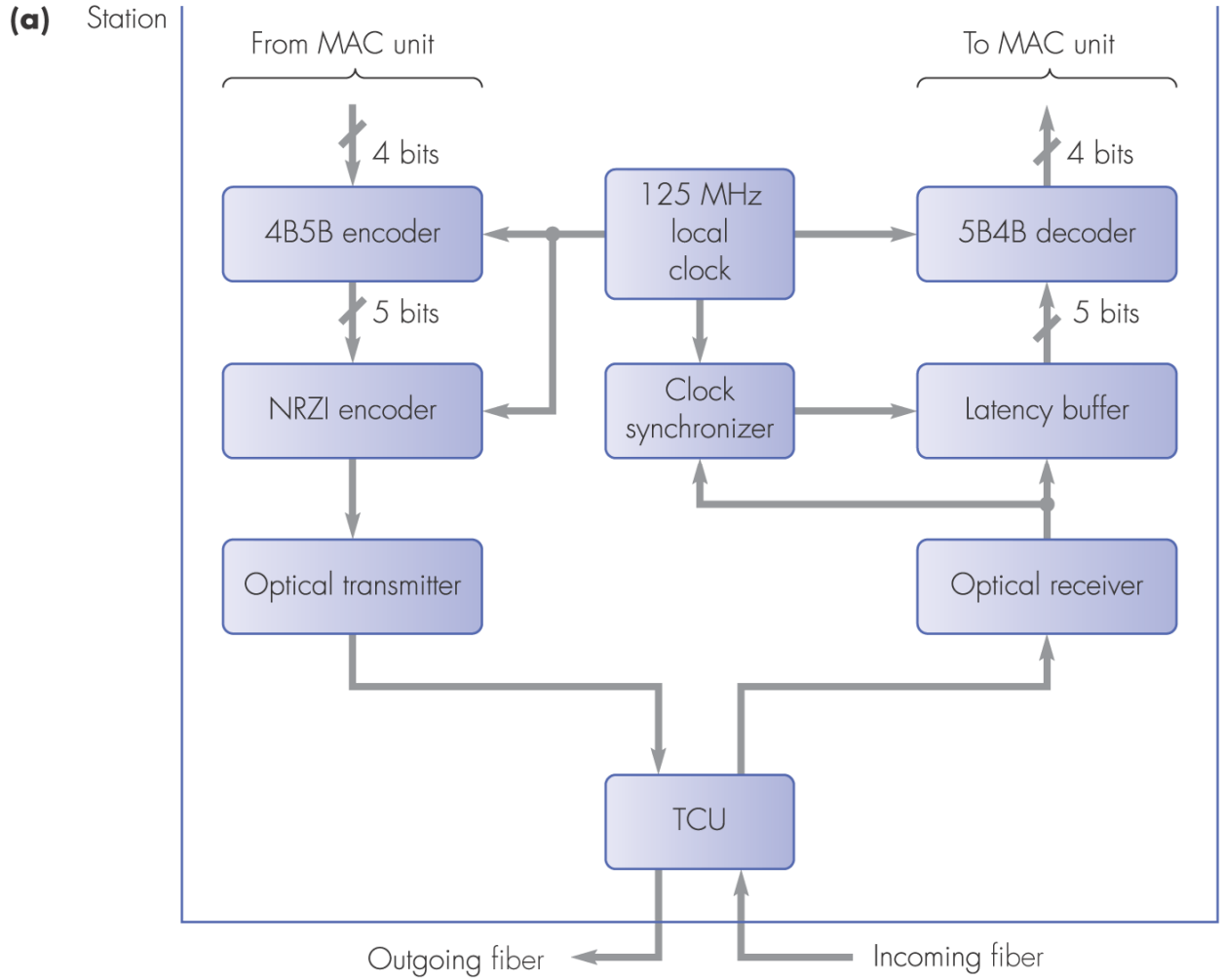


Figure 3.12 100BaseFX: (a) physical interface schematic.

Do you understand how the clock signal is retrieved? Do you remember what NRZI means?

(b)

Data symbols

4-bit data group	5-bit symbol
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Control symbols

IDLE	11111
J	11000
K	10001
T	01101
R	00111
S	11001
QUIET	00000
HALT	00100

Figure 3.12 100BaseFX: (b) 4B/5B codes.

Which 5-bit codes were not chosen for this code, and why?

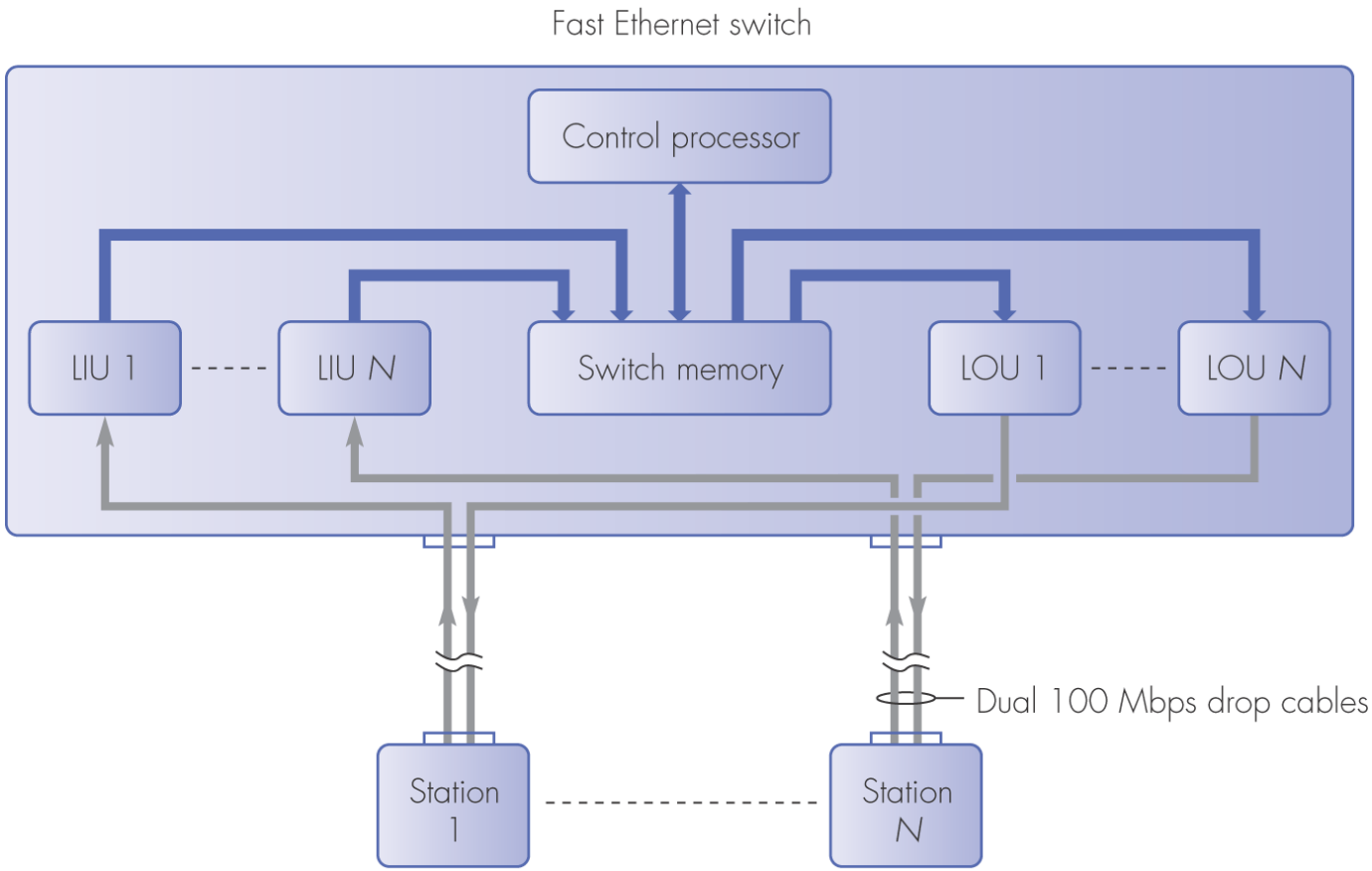
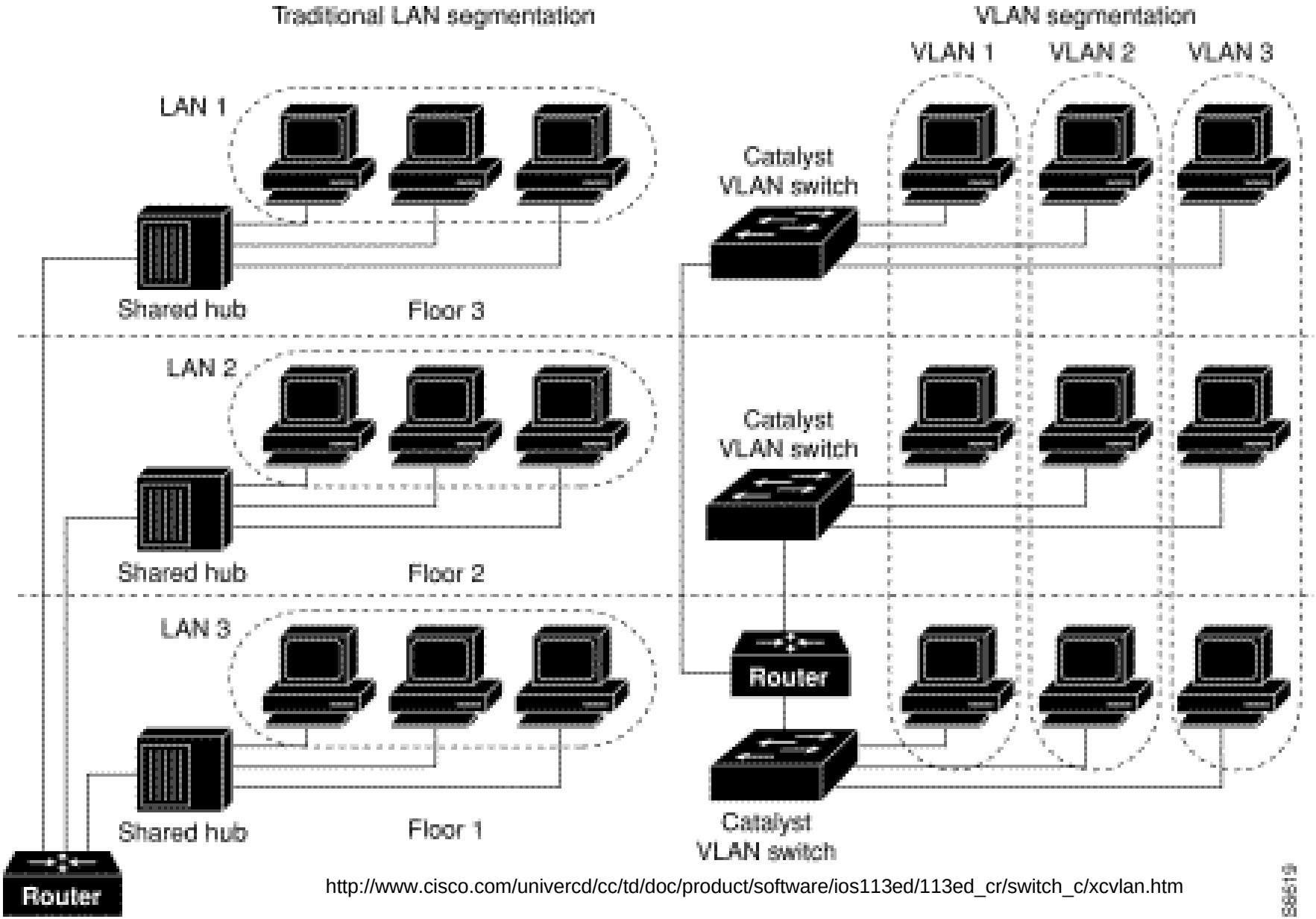


Figure 3.13 Fast Ethernet switch schematic. LIU = Line Input Unit; LOU = Line Output Unit.

Is this a trivial diagram?

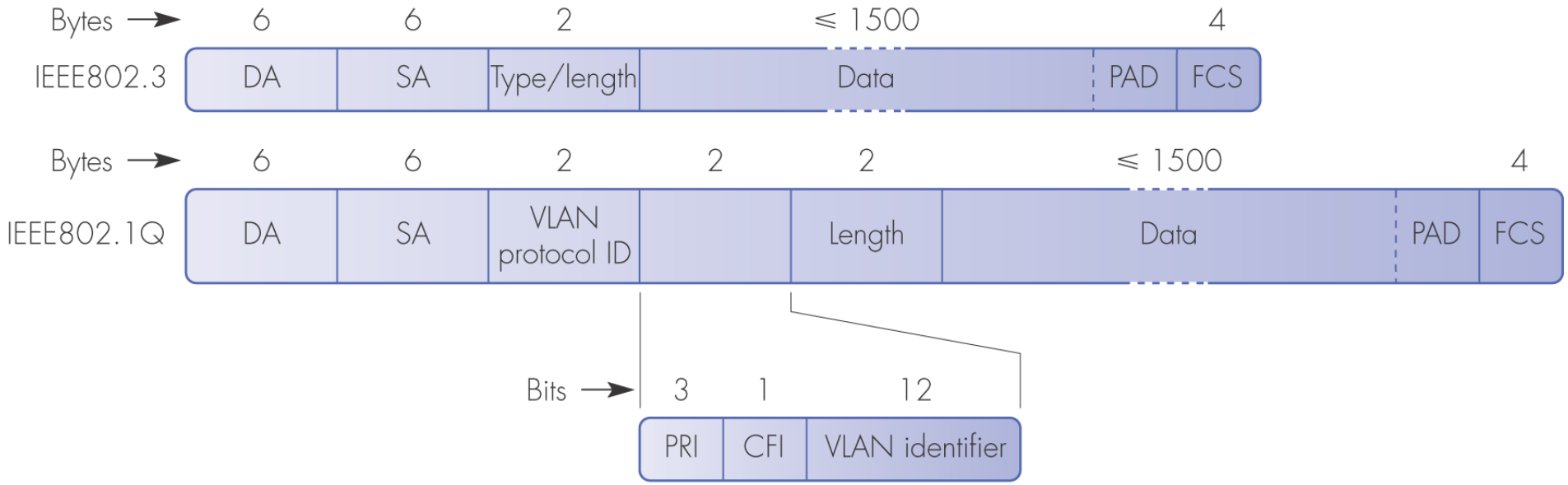
LANs versus VLANs



http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm

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.



DA = destination MAC address

SA = source MAC address

VLAN protocol ID = 8100 Hex

VLAN identifier: this identifies the VLAN to which the frame belongs

PRI = priority field (for possible future use)

CFI = canonical format identifier – used to enable a frame relating to a Token ring LAN to be embedded within the data field of the frame

Note: 1. The VLAN protocol ID of 8100 Hex is greater than 1500 and hence is interpreted as a type value
2. The maximum frame size is now 1522 bytes

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

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