University of Southern California

Viterbi School of Engineering

EE450

Computer Networks

Connecting Devices

Shahin Nazarian

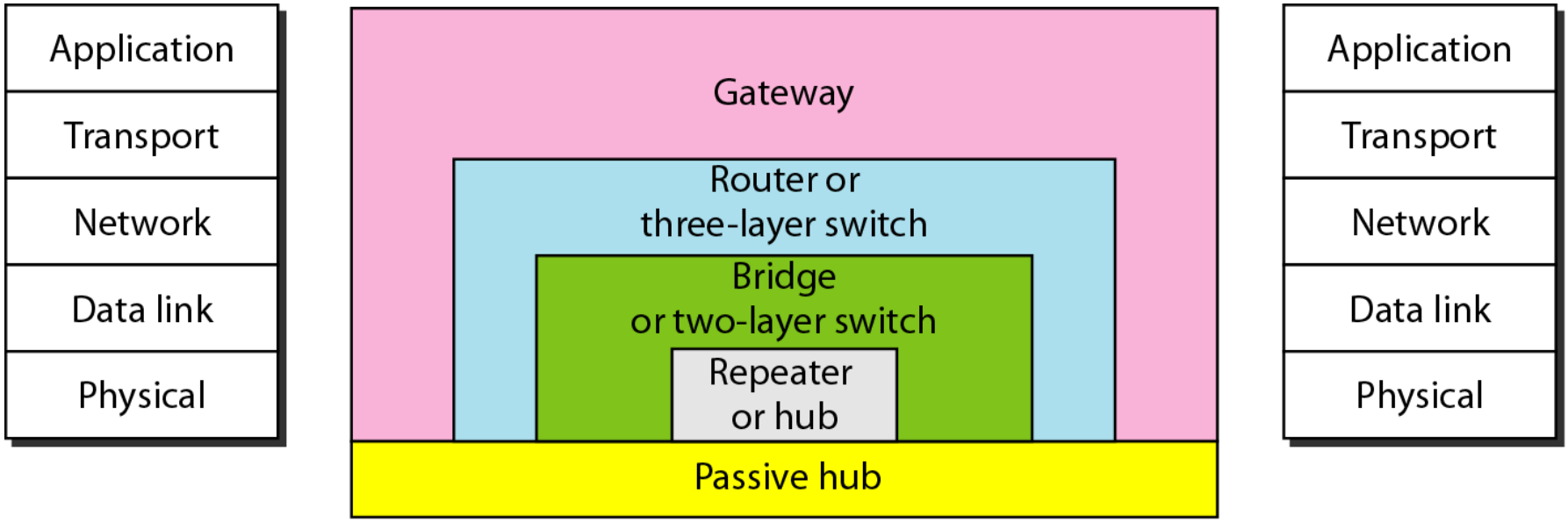
Spring 2013

!


I wonder where
Alice moved to?

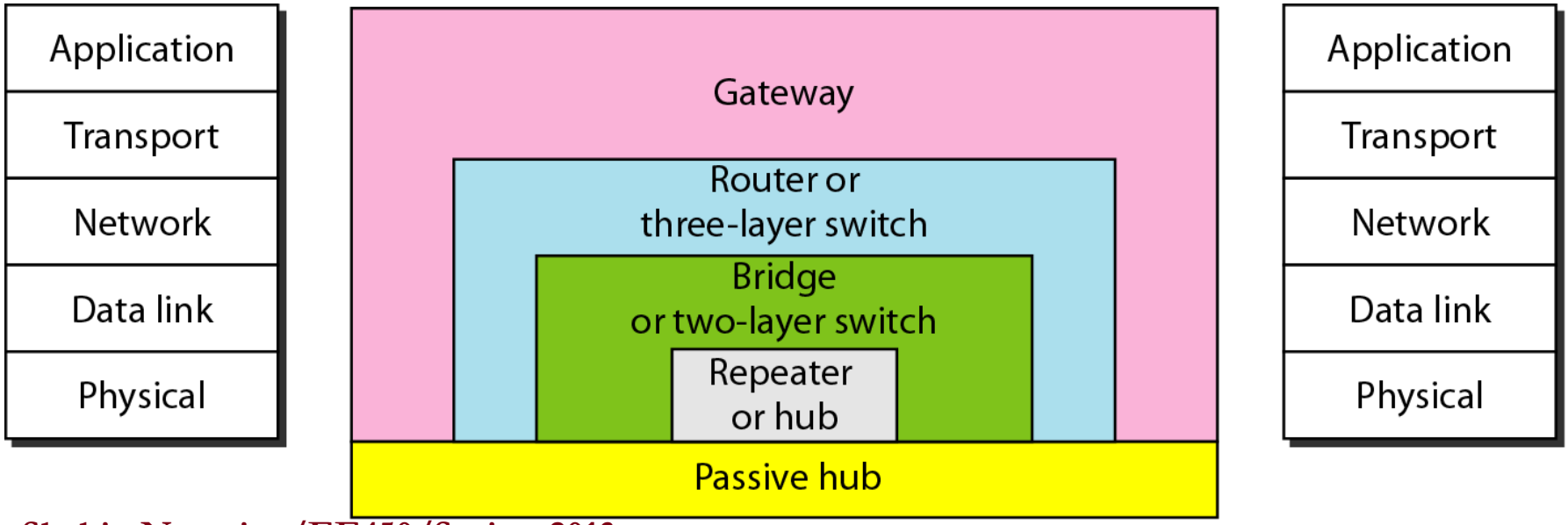
Connecting Devices

- **Connecting devices** are layer1 devices such as hubs, layer2 devices such as bridges, layer 3 devices such as routers and finally gateways with all 5 layers and are used to interconnect two or more networks together
- Connecting devices are classified based on their functionality in the TCP/IP model. User also decides which one to use based on their functionality



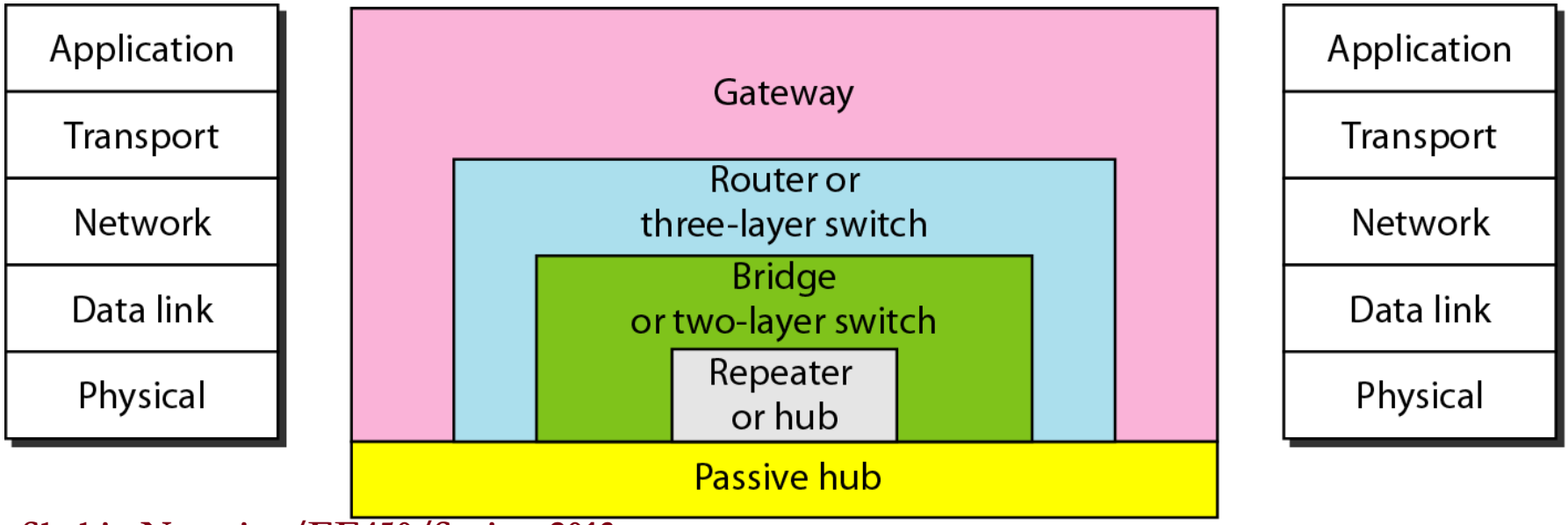
Connecting Devices (Cont.)

- Addressing in
  - Hubs (Layer 1 devices)
  - Bridges (Layer 2 devices)
  - Routers (Layer 3 devices)
  - Gateways (Layer 5 devices)



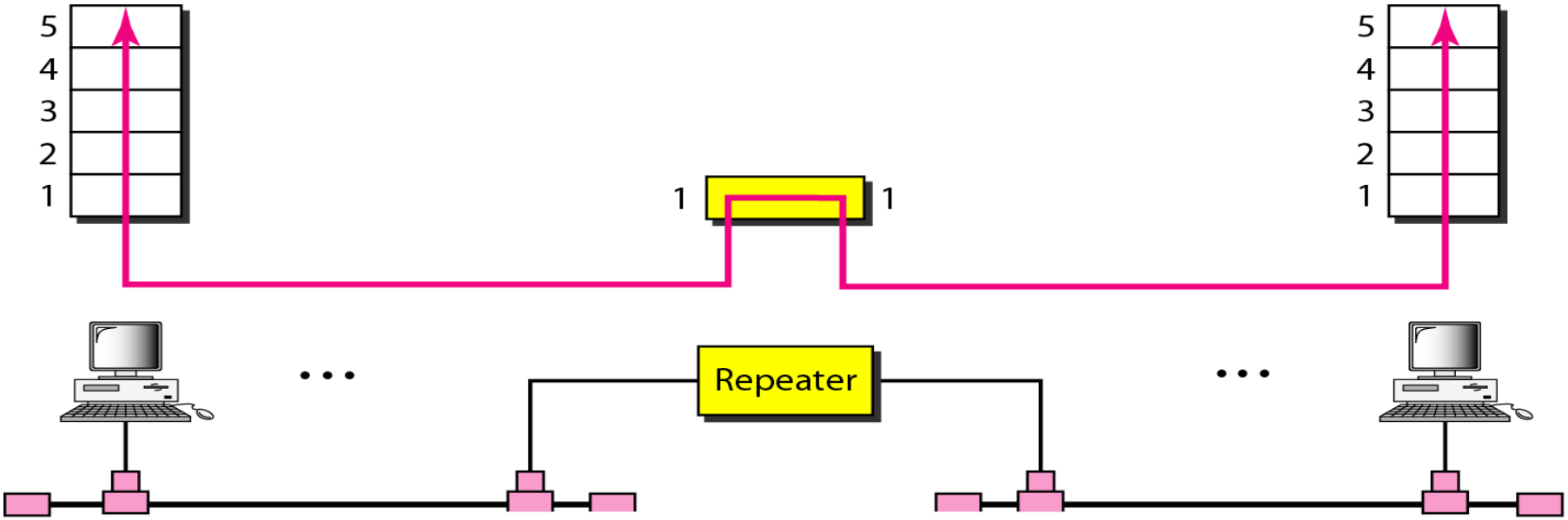
Passive Hubs

- A **passive hub** is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide. This type of the hub is part of the media. Its location in the Internet model is below physical layer



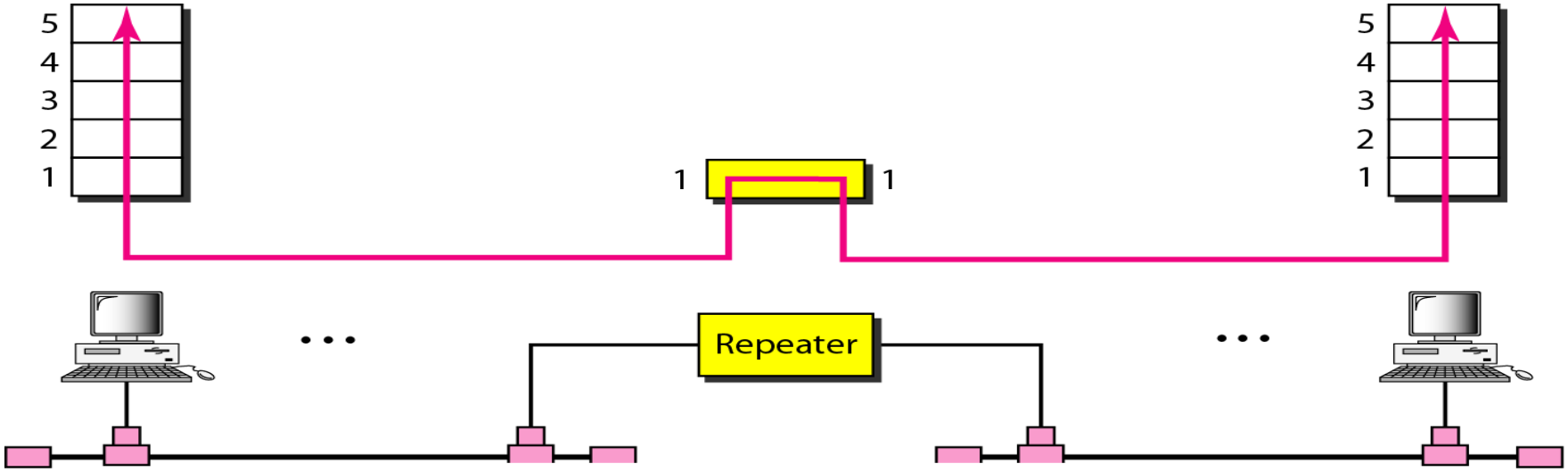
Hub or Repeater

- The functionality of a repeater is to regenerate the signal
- It is basically to extend the network coverage
- A repeater looks at the signal as a group of 0s and 1s
- An active hub is usually a multiport repeater



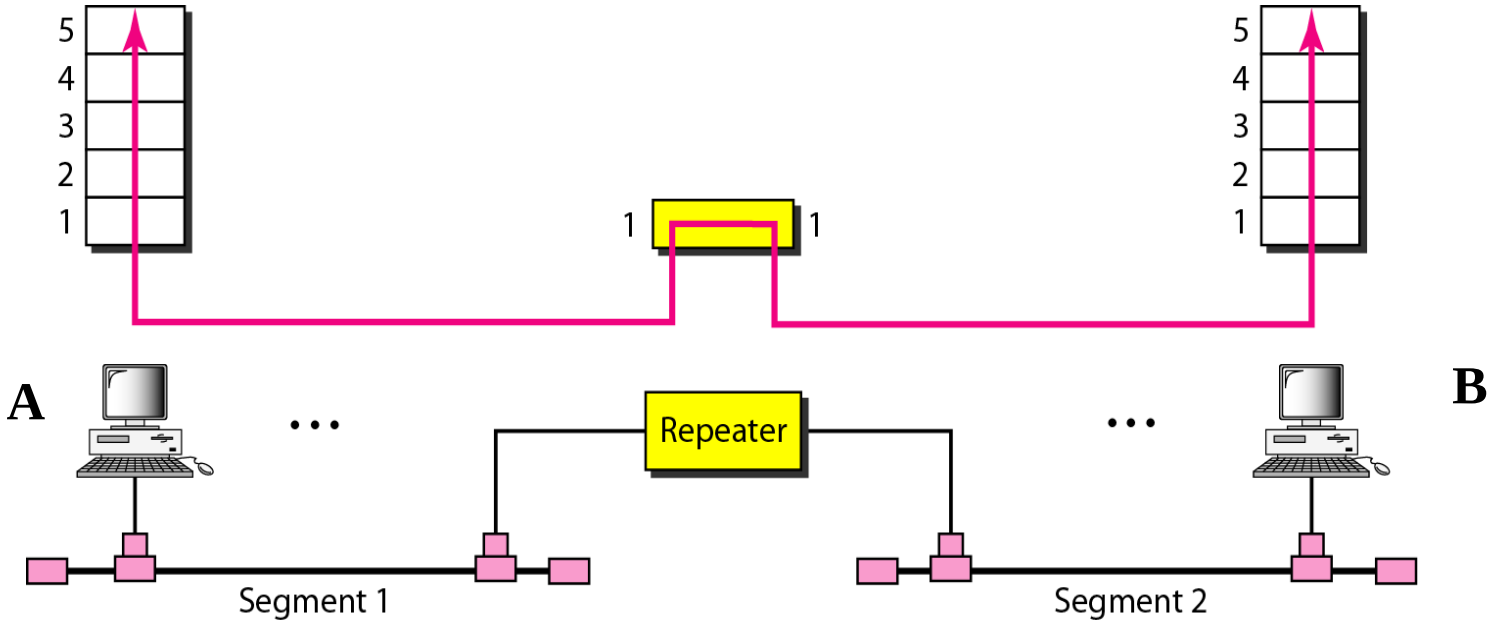
Collision Domain and Broadcast Domain

- **Collision domain** is defined as a set of nodes that compete to access the channel
- **Broadcast domain** is defined as the set of nodes that receive a broadcast transmission
- A repeater or hub can isolate neither broadcast domain nor collision domain. This is not desirable



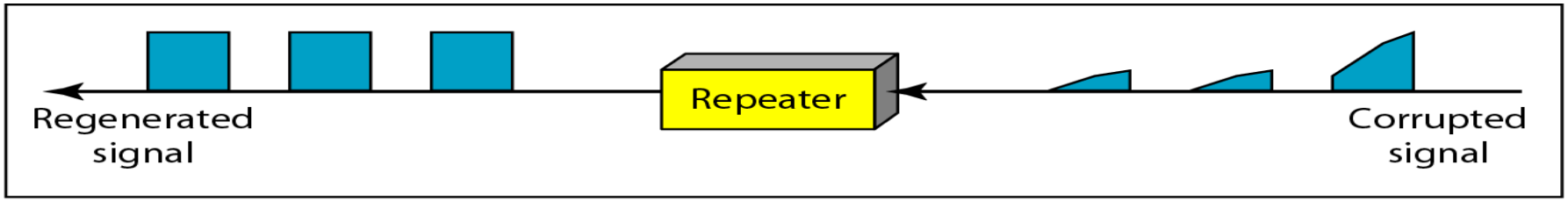
Collision and Broadcast Domains (Cont.)

- Networks are distinguished by the network address
- Let's assume networks are both Ethernet: A is sending a frame to B. The repeater and all the nodes connected to the network will receive the frame

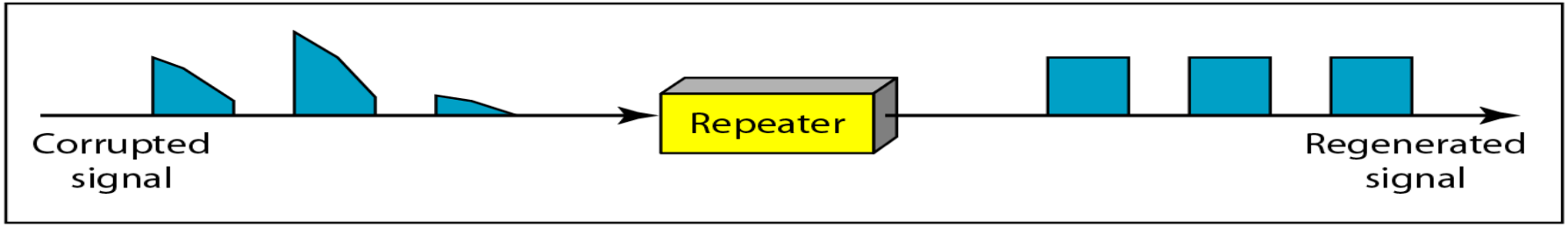


Hub or Repeater (Cont.)

- Repeater is a regenerator; it is a two way device. It is not an amplifier (amplifier is a one way device)
- When signal travels through the medium it gets distorted/corrupted but when it goes through the repeater, it is cleaned and regenerated and then transmitted to all the nodes connected to hub except the transmitter node
- Nodes have CSMA/CD layer 2 protocol. All nodes compete with each other to access the channel



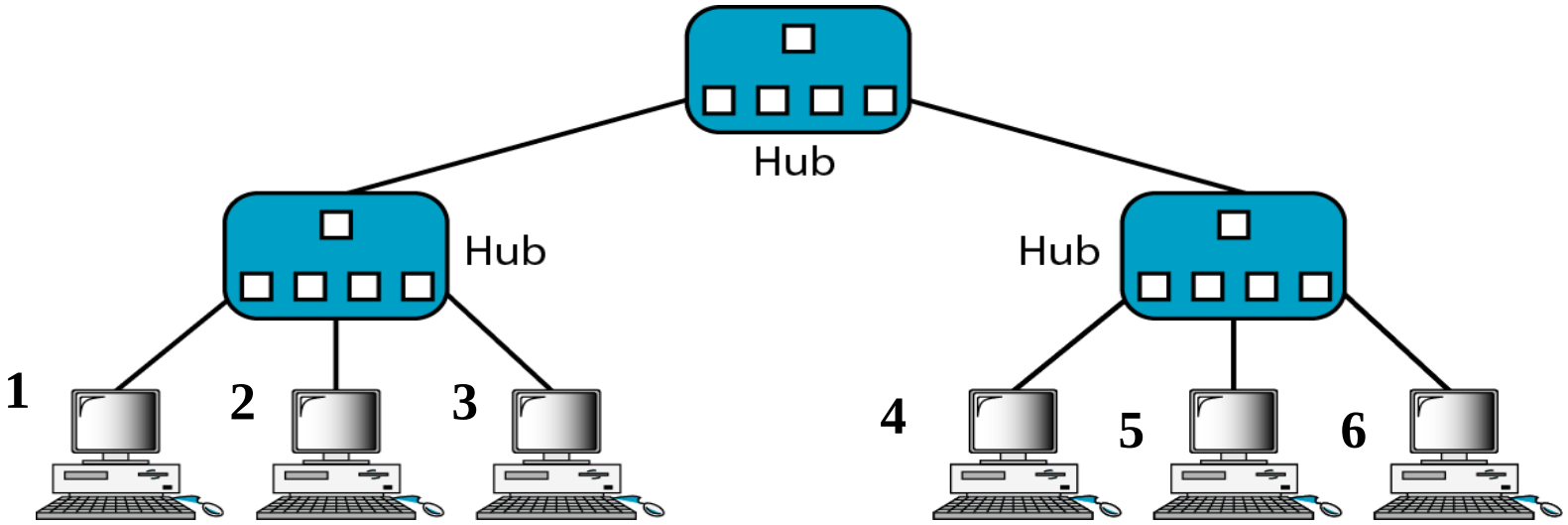
a. Right-to-left transmission.



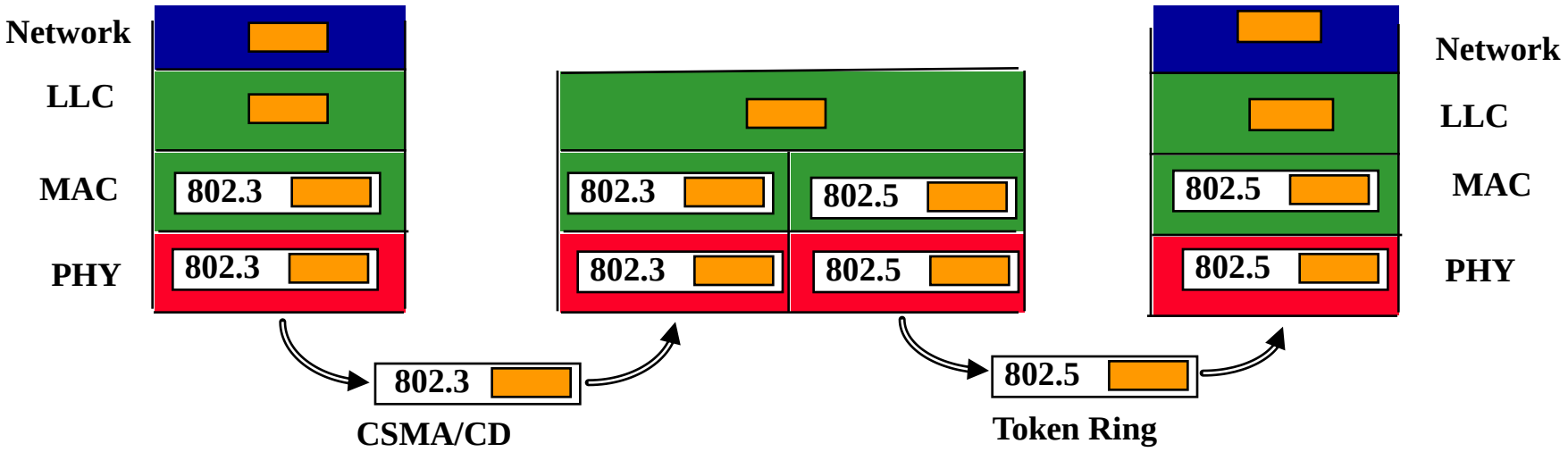
b. Left-to-right transmission.

Hub Hierarchy

- Here the whole system is only one network. Note that networks are distinguished among each other by the network address
- All hosts here have the same network address, so this is one network with 6 nodes (hubs are not considered nodes as far as network is concerned)
- Hub hierarchy is useful. In case a hub goes down there is still a a chance that part of the network still operates
- Example: Host 1 wants to email 6. The email frames will go through all hubs, and are received by all nodes



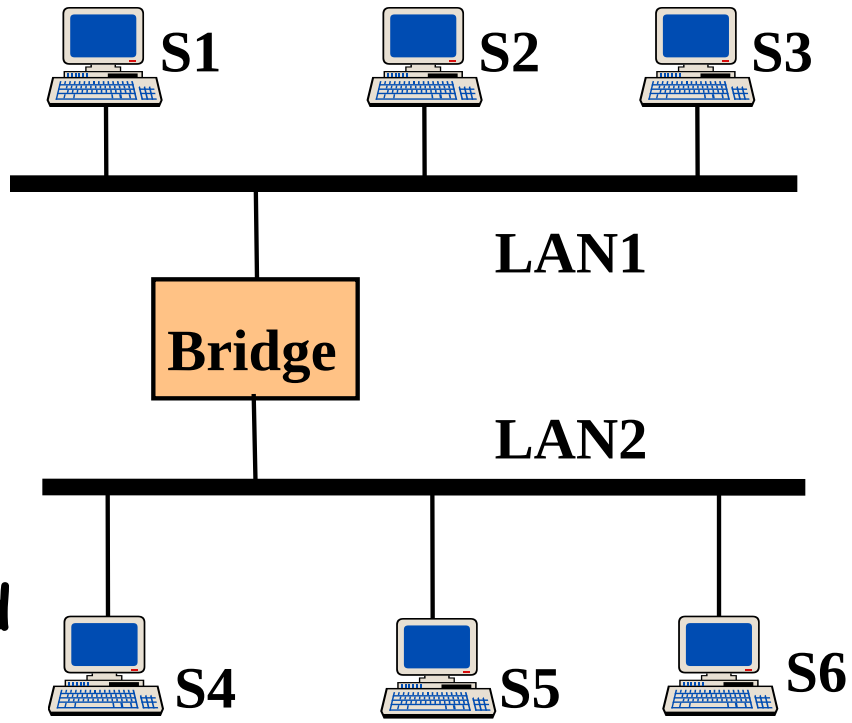
Bridge in General



- In general bridge operations at data link level implies capability to work with multiple network layers
- However, must deal with
  - Difference in MAC formats
  - Difference in data rates; buffering; timers
  - Difference in maximum frame length

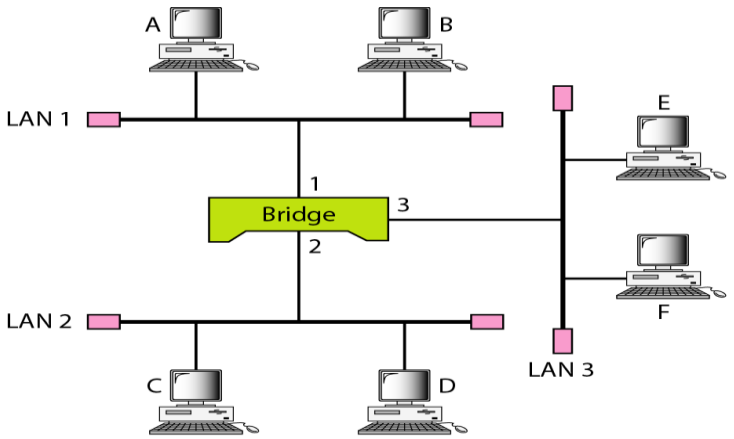
Transparent Bridges

- Interconnection of IEEE LANs with complete transparency
- Use table lookup, and
  - discard frame, if source & destination in same LAN
  - forward frame, if source & destination in different LAN
  - use flooding, if destination unknown
- Use backward learning to build table
  - observe source address of arriving LANs
  - handle topology changes by removing old entries



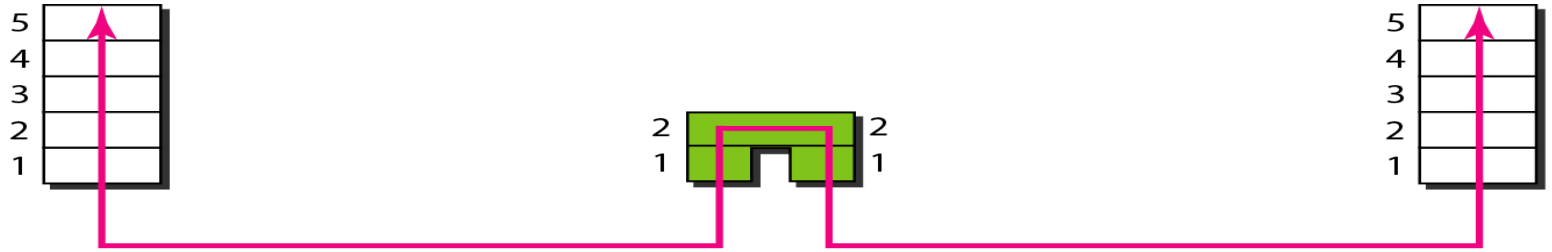
Bridge

- Bridges are usually used to connect the same type of network, e.g., Ethernet with Ethernet or wireless with wireless. Such bridges are called transparent
- Transparent bridges do not introduce large delays, because no frame translation is required (from one type to another)
- One other reason bridges are called transparent is that hosts do not know bridges exist
- We know that routers are not transparent, because hosts know about them, and the IP address of the router is configured in them

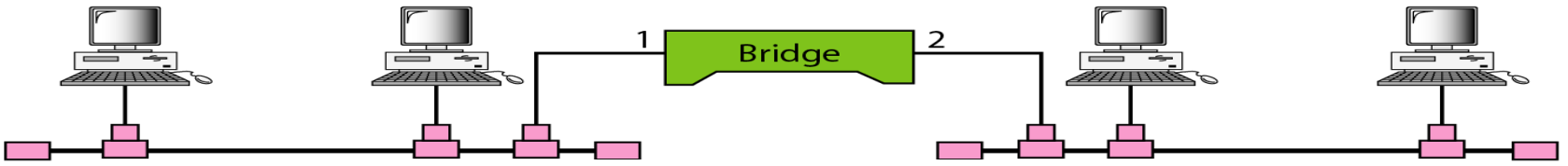


Bridge (Cont.)

- The separation of the physical layers in the bridge implies that the physical layer in each segment does not need to be the same; one side can be cable, and the other side fiber
- However layer 2 is identical on both sides and both use the same MAC procedure



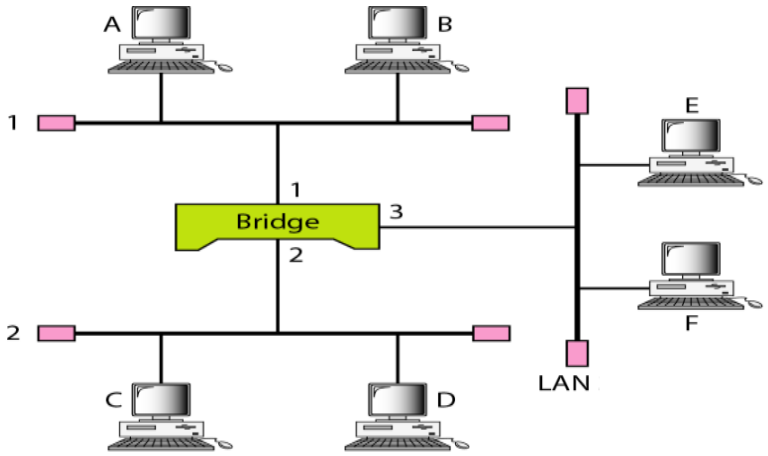
- Unlike routers, bridges do not change the physical (MAC) addresses in a frame (hint: later on, review filtering, flooding, and forwarding; none will change the MAC addresses)



Bridge Table

- Removing the bridge there are 3 networks, 3 collision domains and 3 broadcast domains. 3 networks means that their network addresses are different

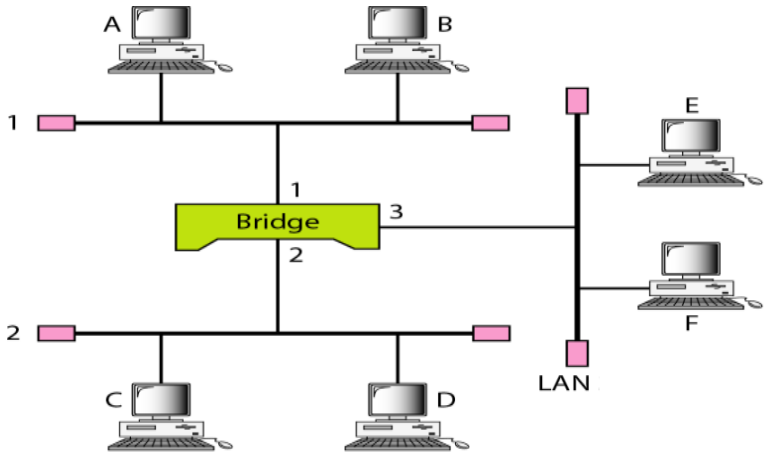
- However adding the bridge back, we have to reconfigure the nodes' IP addresses to let them all have the same network address. To not go through this hassle, one solution is to use a router instead of a bridge



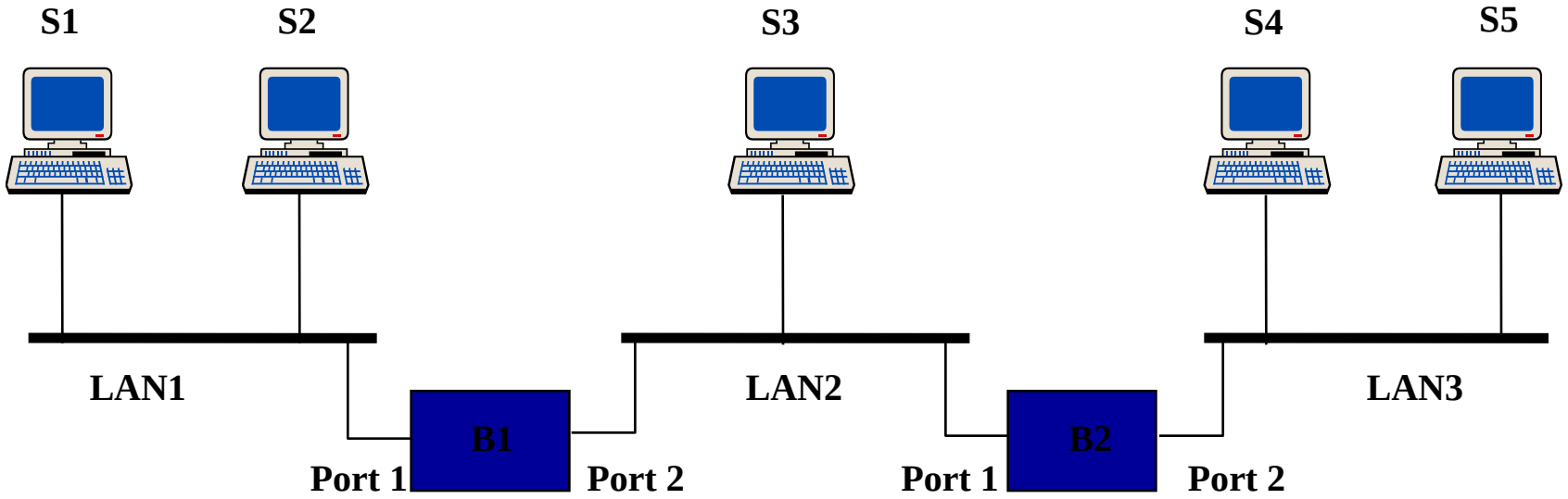
Bridge Table (Cont.)

- With bridge there one network and one broadcast domain
- Bridges have advantage over hubs
- We will see that Bridges have a bridge table of MAC addresses and their respective segment numbers aka the bridge port numbers
- Note: port number here refers to the network segment number and has nothing to do with the application port number in layer 4

Bridge has 3 modes of operations, filtering, forwarding & flooding



Learning Bridge Example

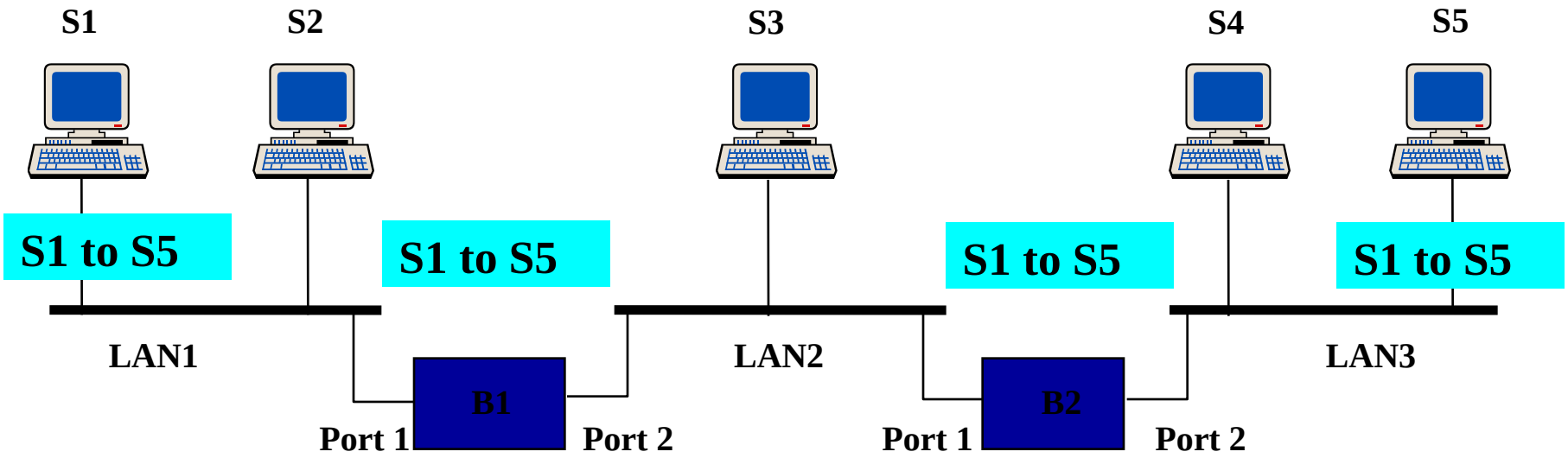


Address	Port

Address	Port

Learning Bridge Example (Cont.)

S1→S5

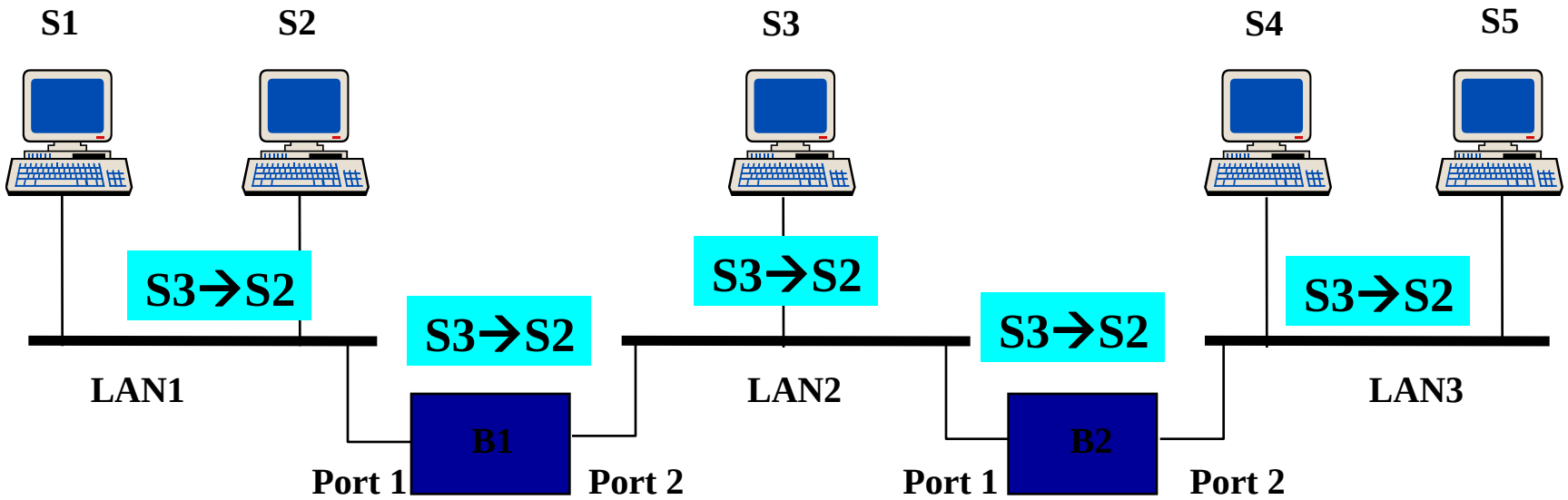


Address	Port
S1	1

Address	Port
S1	1

Learning Bridge Example (Cont.)

S3→S2

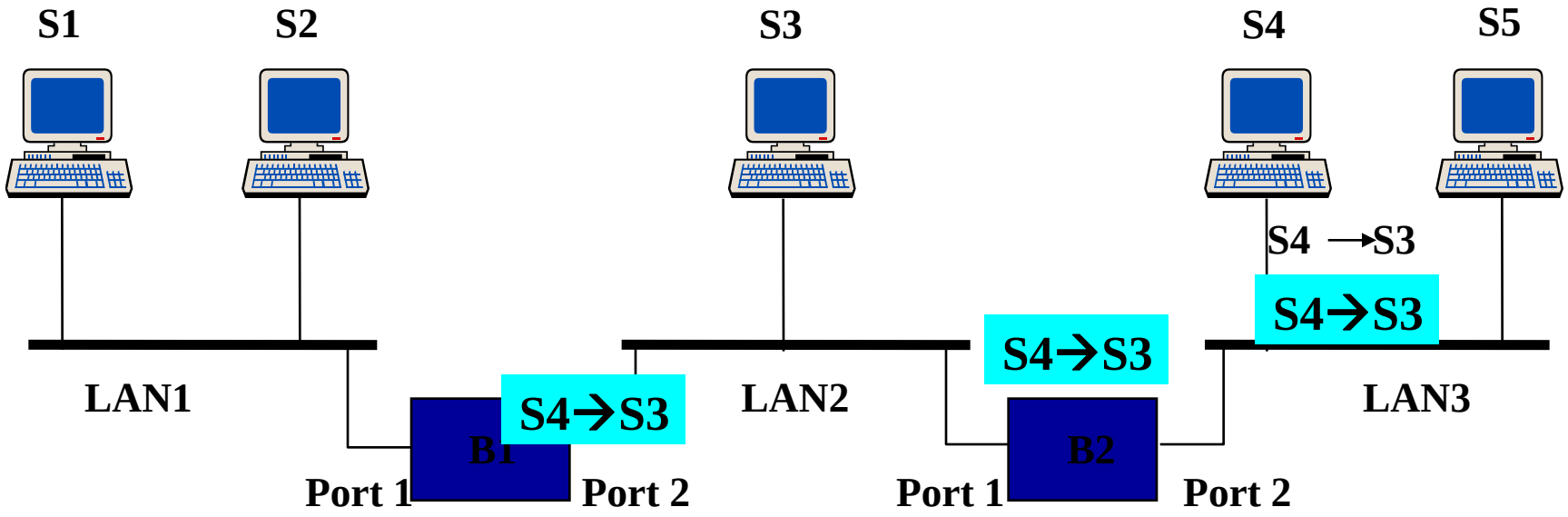


Address	Port
S1	1
S3	2

Address	Port
S1	1
S3	1

Learning Bridge Example (Cont.)

S4→S3

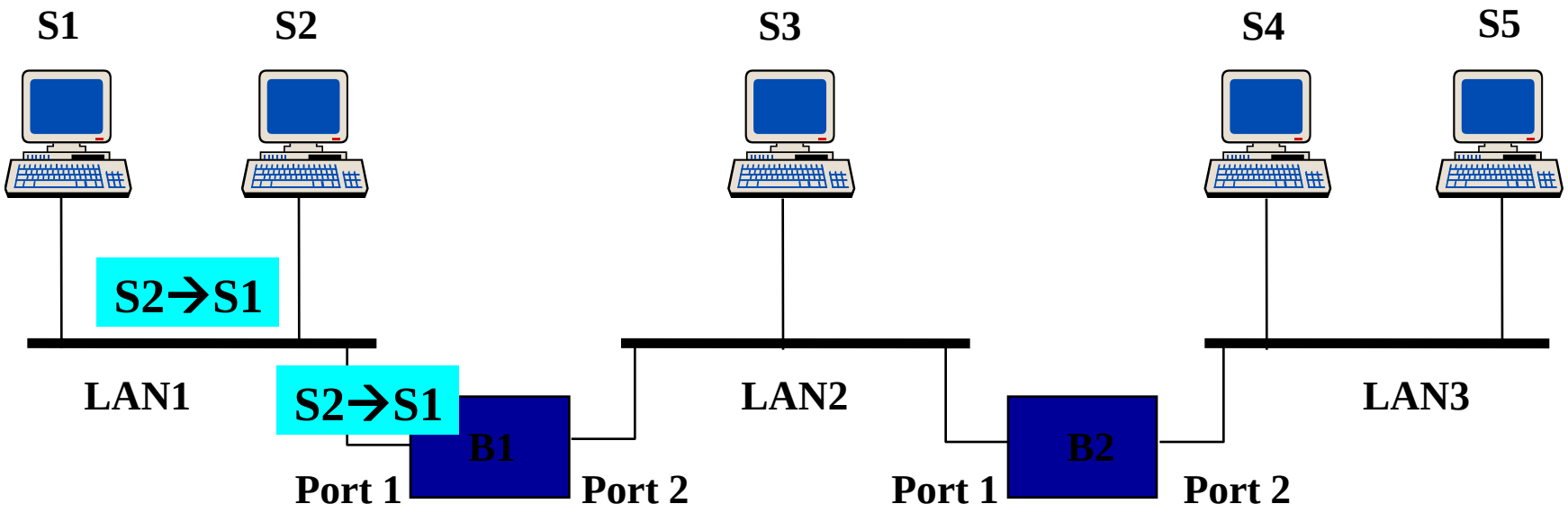


Address	Port
S1	1
S3	2
S4	2

Address	Port
S1	1
S3	1
S4	2

Learning Bridge Example (Cont.)

S2→S1

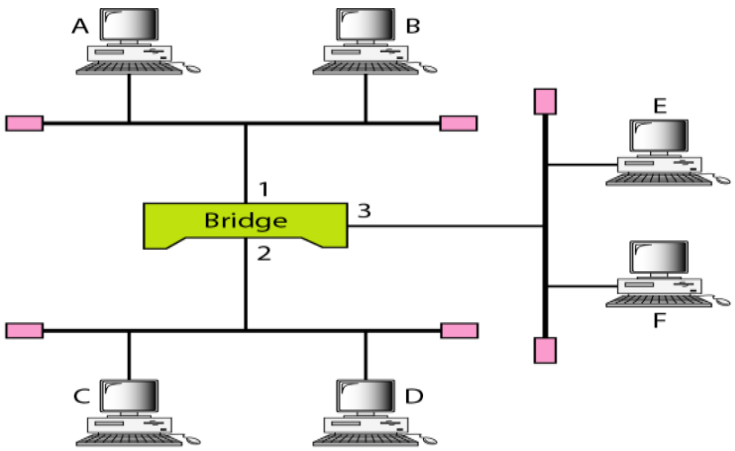


Address	Port
S1	1
S3	2
S4	2
S2	1

Address	Port
S1	1
S3	1
S4	2

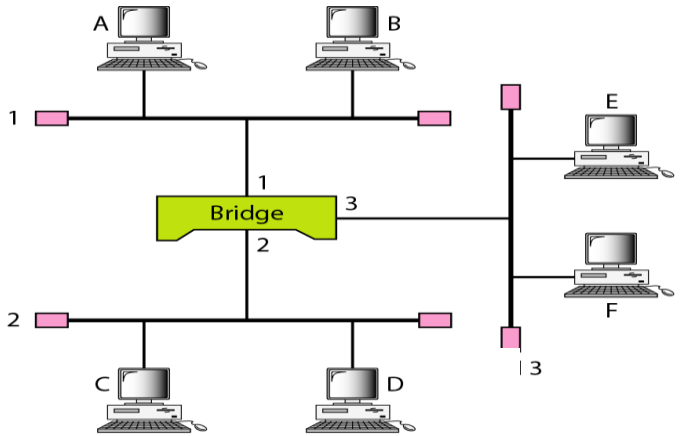
Bridge Operation Modes – Filtering

- Assume A sends a frame to B. Bridge recreates the frame in its second layer and recognizes B's MAC address as the destination address
- The bridge uses its bridge table and finds out that the message is confined in segment 1, because both A and B are in segment 1. Bridge will filter the frame
- Note: Bridge will operate in filtering mode if both source and destination MAC address are in the same segment
- A can send to B, E can send to F, and C can send to D at the same time. There won't be a collision, because bridge will do filtering properly



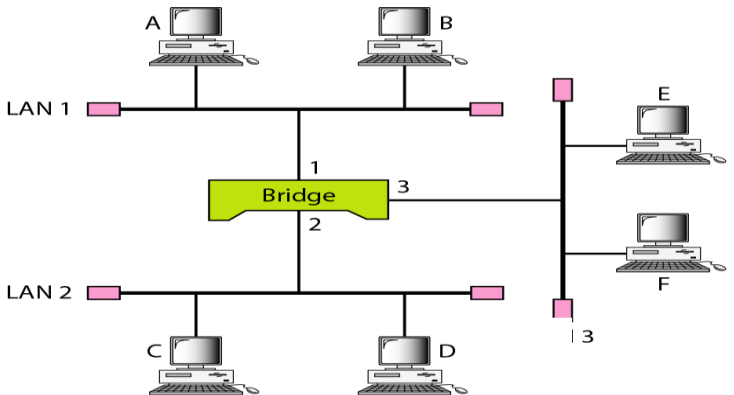
Bridge Operation Modes – Forwarding

- Assume A wants to send a frame to F
- B and bridge receive the frame
- B drops it
- Bridge looks at its bridge table and finds out that F is connected to port 3 and A to port 1, so it forwards the frame to port 3
- It also filters the frame from port 2



Bridge Forwarding Mode (Cont.)

- Bridge needs a buffer for each port. Because while checking the frame and trying to figure out what mode to operate, it needs to keep the frame
- Here bridge gets the frame from buffer of port 1 and forwards it to the buffer of port 3
- This is Ethernet and the bridge, as a layer 2 device, needs to play by the rules of CSMA/CD, so before putting the frame from buffer of port 3 to channel, it needs to sense the channel …
- Note: repeaters (hubs) don't do any frame processing, so they do not need a buffer

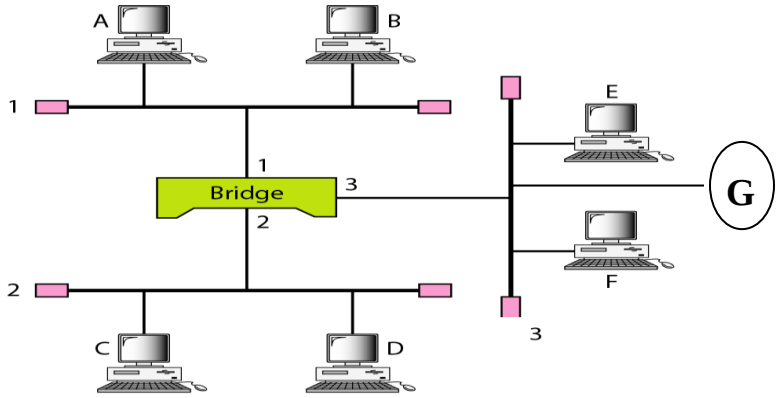


Bridge: 1) Buffer 2) FDX Support

- If buffer overflows, the bridge will drop the frame. In networking there is no guarantee that everything will go smoothly with no problem
- However buffer overflow is rare here, because the frames are bursty, and when the bridge becomes idle, it will go back and deal with the backlog
- Network admin will monitor this, and in case of frequent frame dropping by bridge, the buffer size of the bridge should be increased
- Note that a repeater or hub relays the transmitted bits from a segment to all other segments, so __ buffering is needed for hub
- Bridges can support not only simultaneous connections, but also full duplex (FDX) connection. Bridges can also support multiple port rates, e.g., a bridge with notation 100/1000 means that it can support 100Mbps and 1000Mbps
- A repeater or hub cannot support FDX, because it will have collision

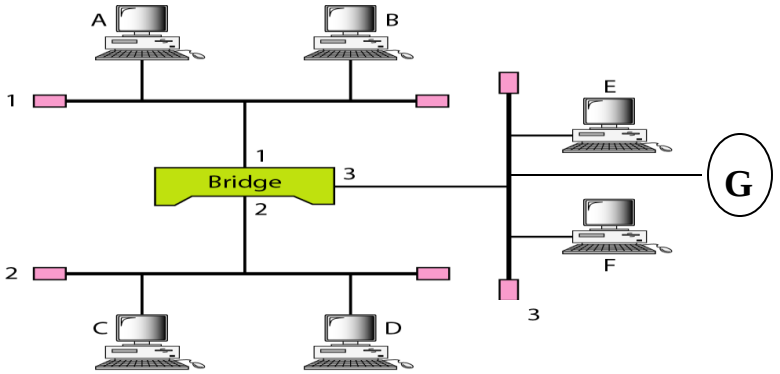
Bridge Operation Modes – Flooding

- Suppose a new node G is added to the network. G gets its IP through DHCP or manually by network admin, however bridge has not included G's MAC address and it's port number (3) in its table [either network admin has not put it yet, or bridge did not get a chance to learn this]
- A wants to send a message to G. Bridge looks for the destination MAC address (G's MAC address) in the table and does not find it, so it goes to flooding mode and broadcasts the frame to all its ports except the sender port (here port 1)
- Flooding is not desired, because this is exactly what repeaters do
- G cannot inform bridge that it just joined port 3, because to G, bridge is transparent and does not exist
- In reality learning bridges are typically used



Learning Bridges

- The original bridges had static tables, meaning the system admin would manually enter each table entry during bridge setup
- Bridges that complete their table dynamically, without the help of the network admin are called plug and play bridges
- Assume A moves to port 2 and happens to not transmit for a while, so bridge does not know A moved and it's table is not updated. It still shows A's port number as 1



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

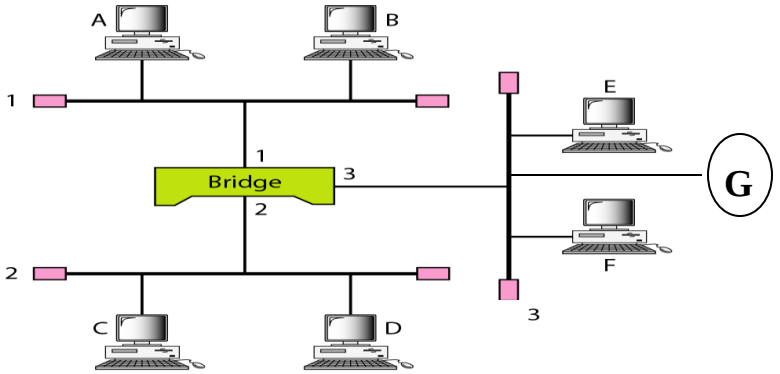
c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

Learning Bridges (Cont.)

- Now B wants to transmit a frame to A. Bridge goes to filtering mode and filter the frame from port 2 and 3, believing that A is on the same port as B is (port 1) whereas A is in another port. To address this problem the bridge table has another column called TTL (Time To Live)
- If the bridge timer expires for TTL, bridge removes A's entry in table
- If A sends a frame before timer expires, bridge resets the timer
- A, B, and bridge compete with each other to access the channel (Also E, F, and bridge and C, D and bridge



a. Original

Address	Port

b. After A sends a frame to D

Address	Port
A	1

c. After E sends a frame to A

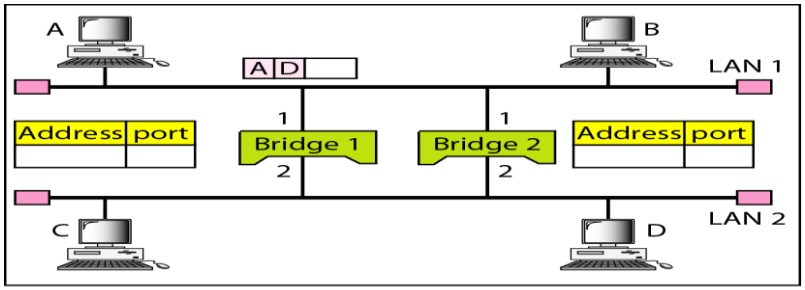
Address	Port
A	1
E	3

d. After B sends a frame to C

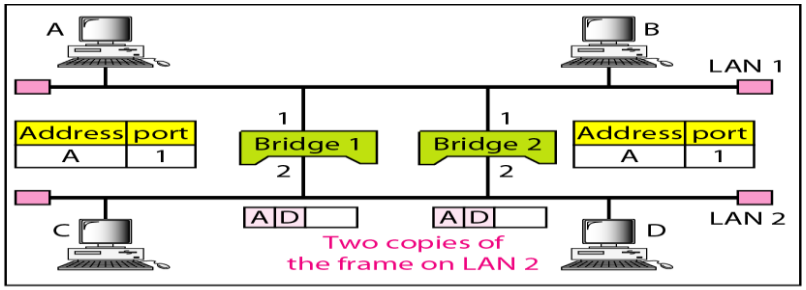
Address	Port
A	1
E	3
B	1

Loop Problem in Learning Bridges

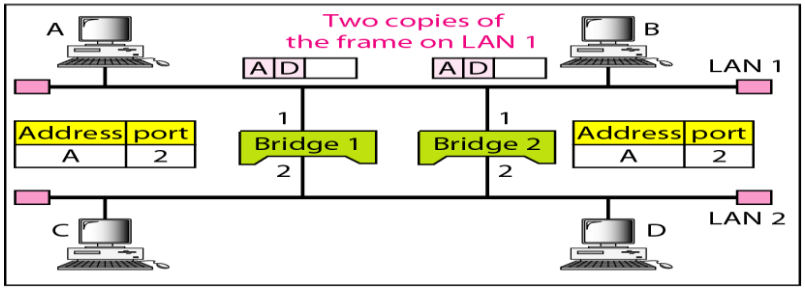
- In bridge network there should not be more than one path from each segment to any other segment
- The loop problem is avoided by dynamic monitoring of the bridges and the paths and making sure no loop exists (next page)
- However remember that in general the main disadvantage of bridges are the single broadcast domain: All 1s are not in the table, so bridge goes into flooding mode (which is similar to what hub does)



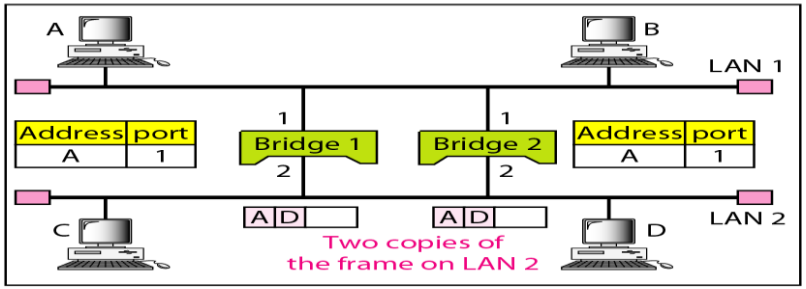
a. Station A sends a frame to station D



b. Both bridges forward the frame



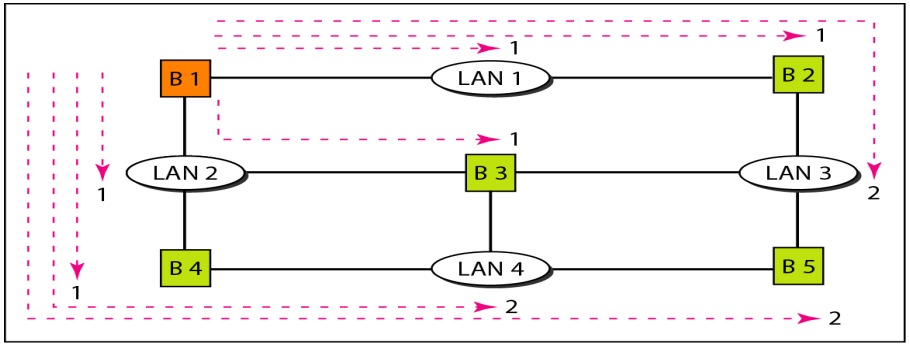
c. Both bridges forward the frame



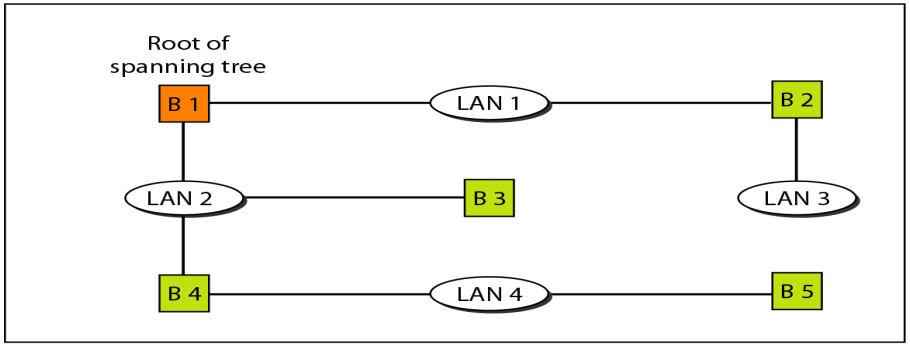
d. Both bridges forward the frame

Loop Problem Solution – SPT

- With more segments in the network the chances of loops being created are higher
- Removing the loops manually is infeasible
- There must be a solution (not a static solution) that does not need anyone such as the network admin (i.e., a dynamic solution is required)



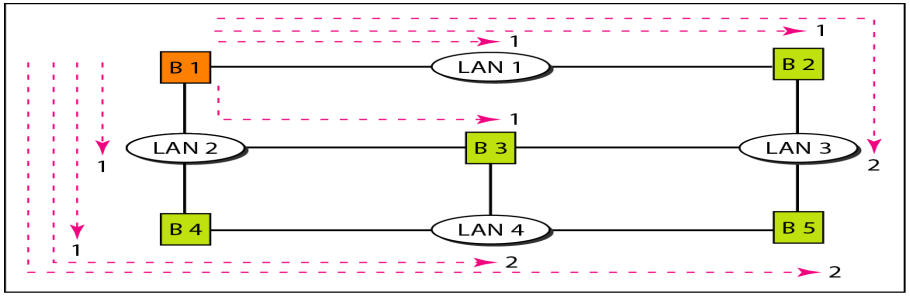
a. Shortest paths



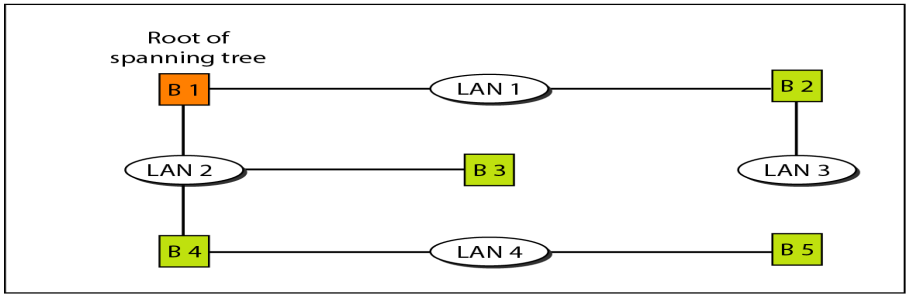
b. Spanning tree

SPT Generation

- A spanning tree (SPT) of the network must be generated to reach out every bridge with no loop and the rest of the paths must be inactive to avoid the loop problem
- In case a path becomes disconnected due to a problem, the inactive paths are going to be used to restore connection
- Spanning tree generation algorithms are based on a cost definition, e.g., delay, distance, throughput, etc



a. Shortest paths



b. Spanning tree

SPT – Root Bridge

- Bridges must first choose one bridge to be the root of the SPT. To do so, they each include an identifier based on their MAC address in the configuration message, as well as the identifier of the bridge they believe to be the root (remember that MAC addresses are globally unique, so identifiers are convenient and unique)
- Then a tree of shortest paths from the root to every bridge is built. To do so, bridges use their distance from root in their configuration message. Each bridge remembers the shortest path it finds to the root. Bridges will then turn off the ports that are not part of the shortest path
- Even if SPT is now established, the algorithm will continue to run during normal operation to check whether any update is necessary (because of a change in topology of the network)

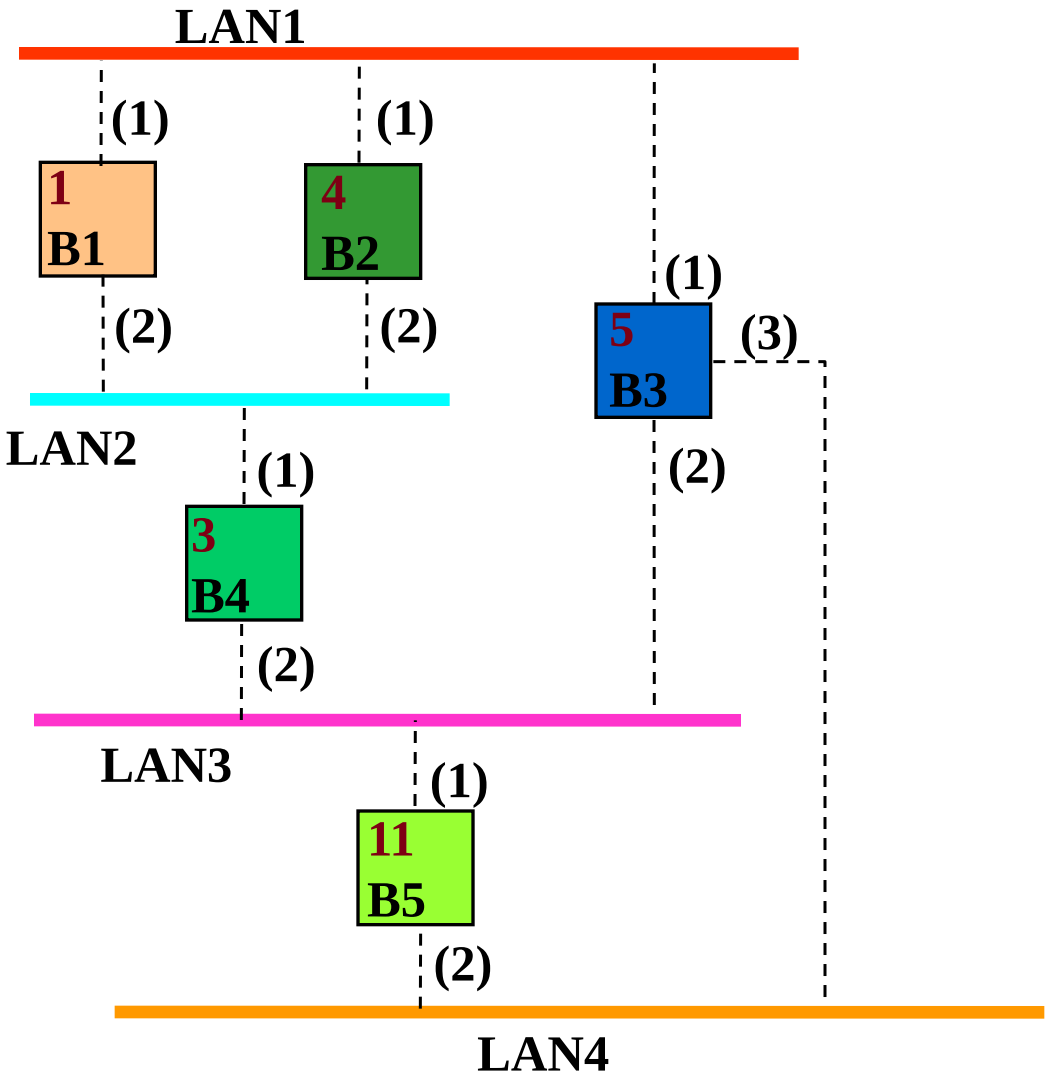
SPT Algorithm by Radia Perlman

1. Select a *root bridge* among all the bridges
   - root bridge = the lowest bridge ID
2. Determine the *root port* for each bridge except the root bridge
   - root port = port with the least-cost path to the root bridge
3. Select a *designated bridge* for each LAN
   - designated bridge = bridge has least-cost path from the LAN to the root bridge
   - *designated port* connects the LAN and the designated bridge
4. All root ports and all designated ports are placed into a "forwarding" state. These are the only ports that are allowed to forward frames. The other ports are placed into a "blocking" state

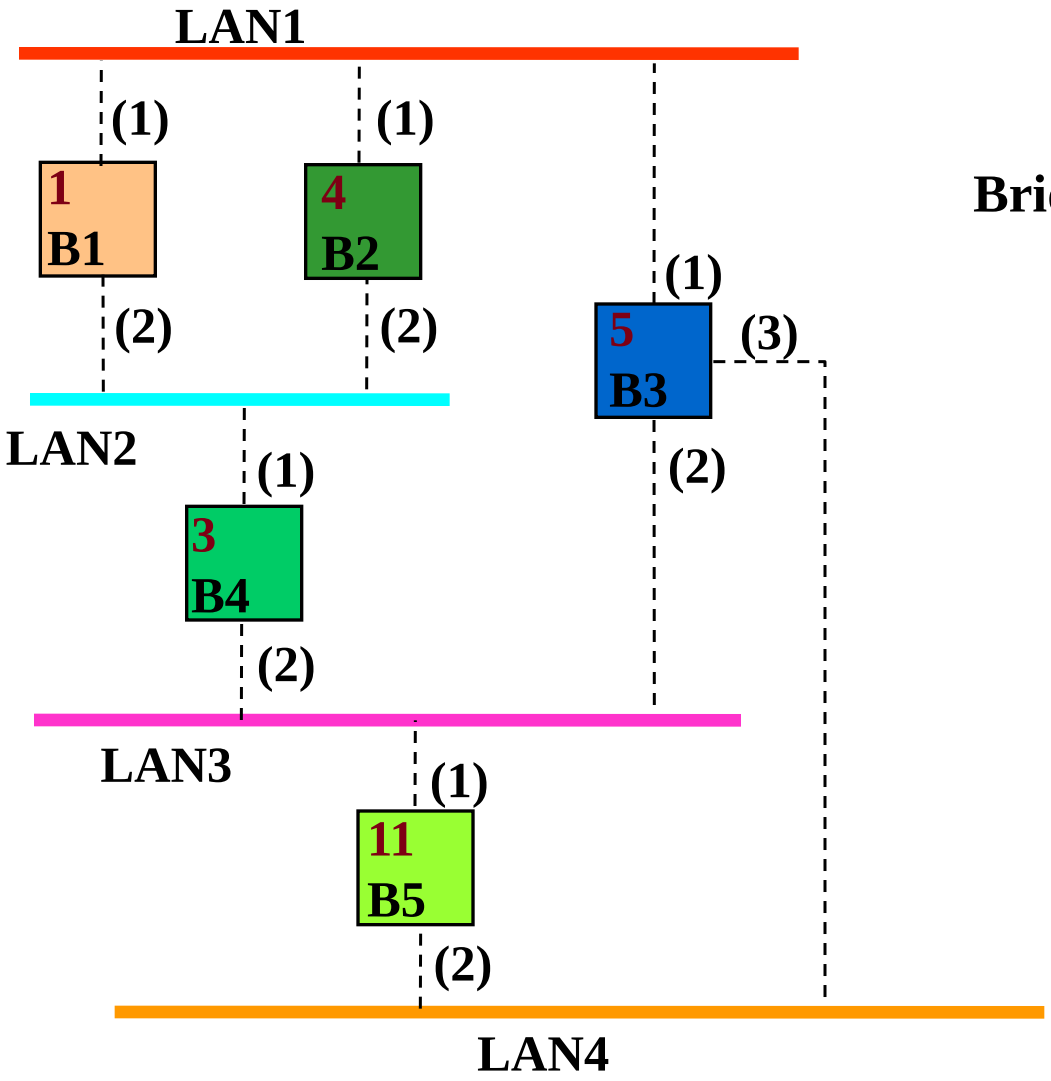
Radia Perlman's Poem (1985)

I think I shall never see
A graph more lovely than a tree
A tree whose crucial property
Is loop-free connectivity
A tree which must be sure to span
So packets can reach every LAN
First the Root must be selected
By ID it is selected
Least cost paths from Root are traced
In the tree these paths are placed
A mesh is made by folks like me
Then bridges find a spanning tree

Generalized SPT Algorithm – Example

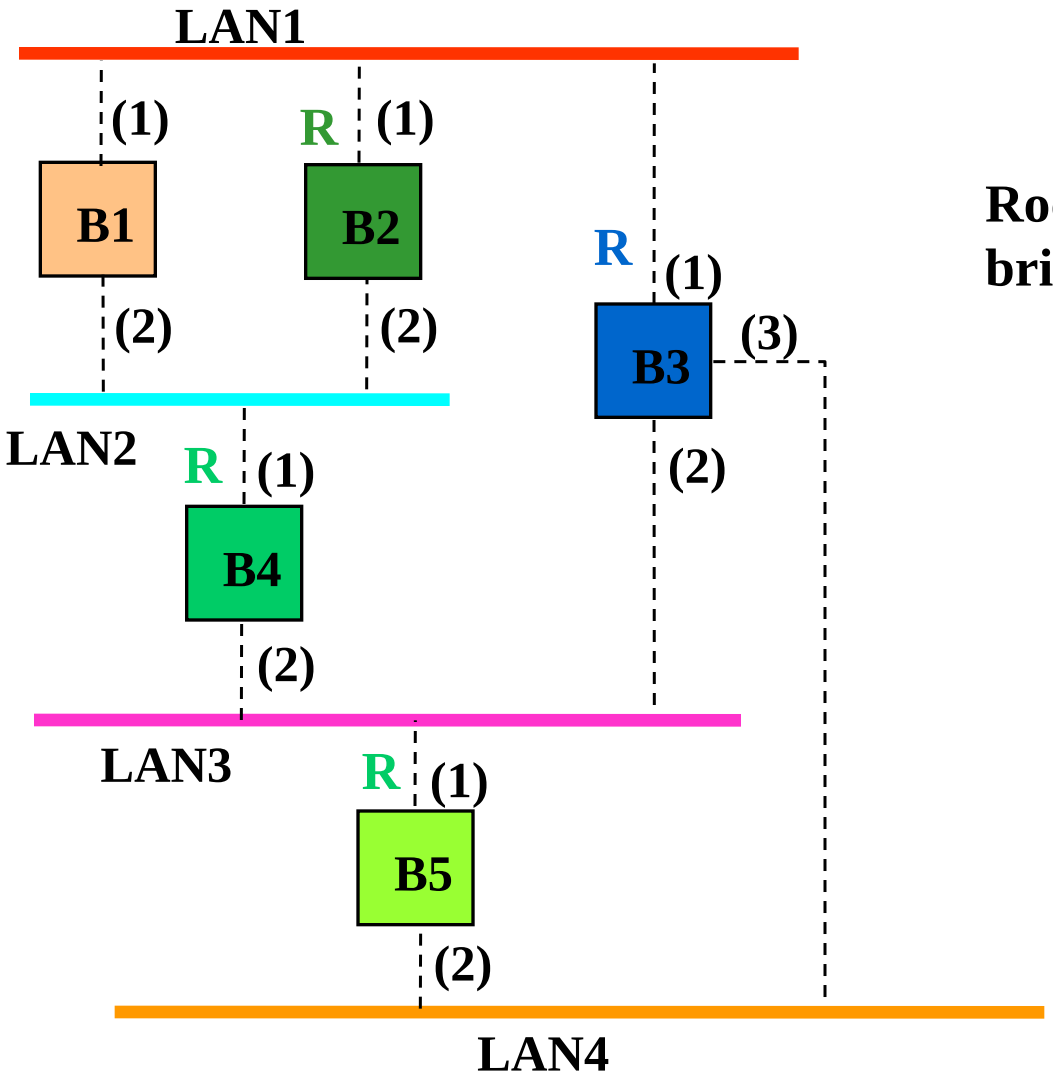


Generalized SPT Algorithm – Example (Cont.)



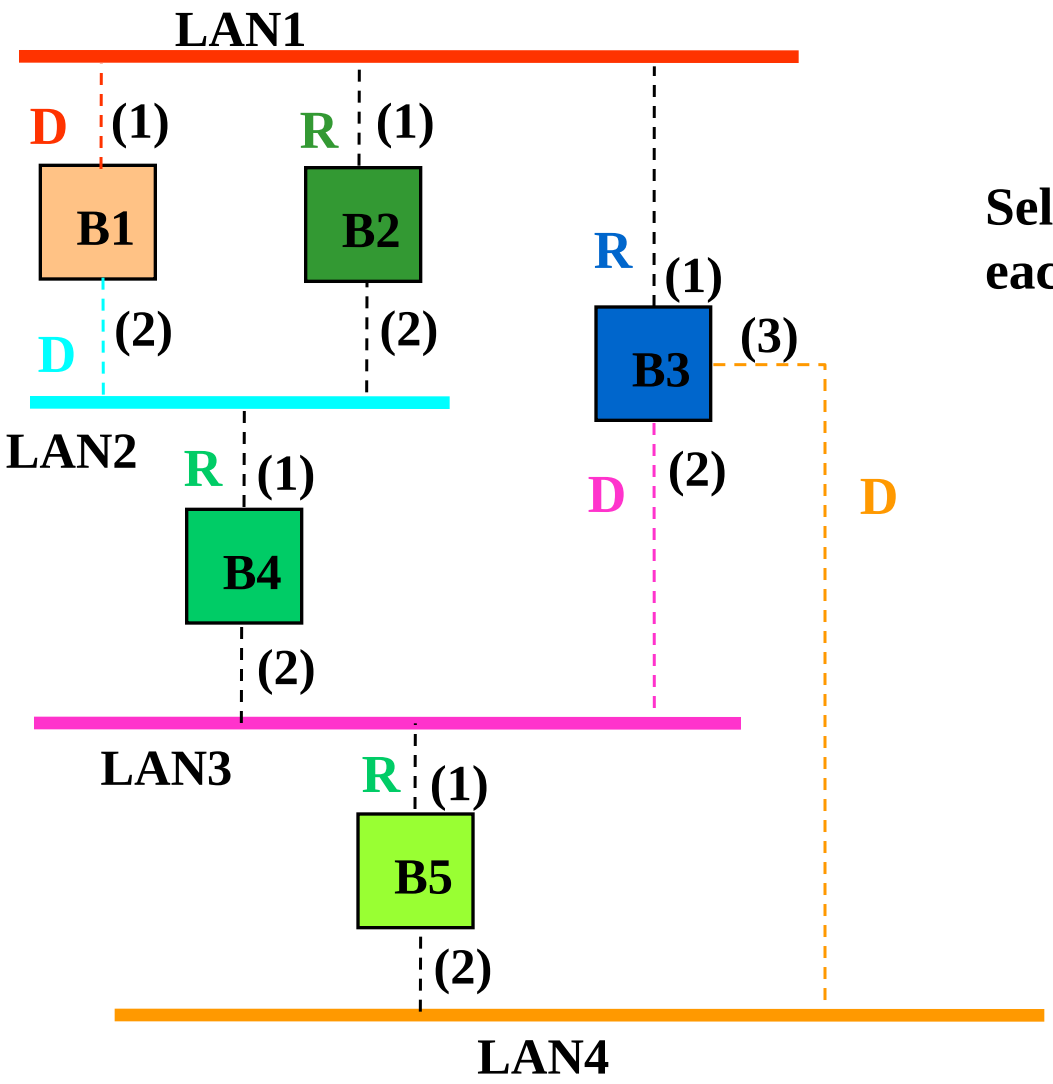
Bridge 1 selected as root bridge

Generalized SPT Algorithm – Example (Cont.)



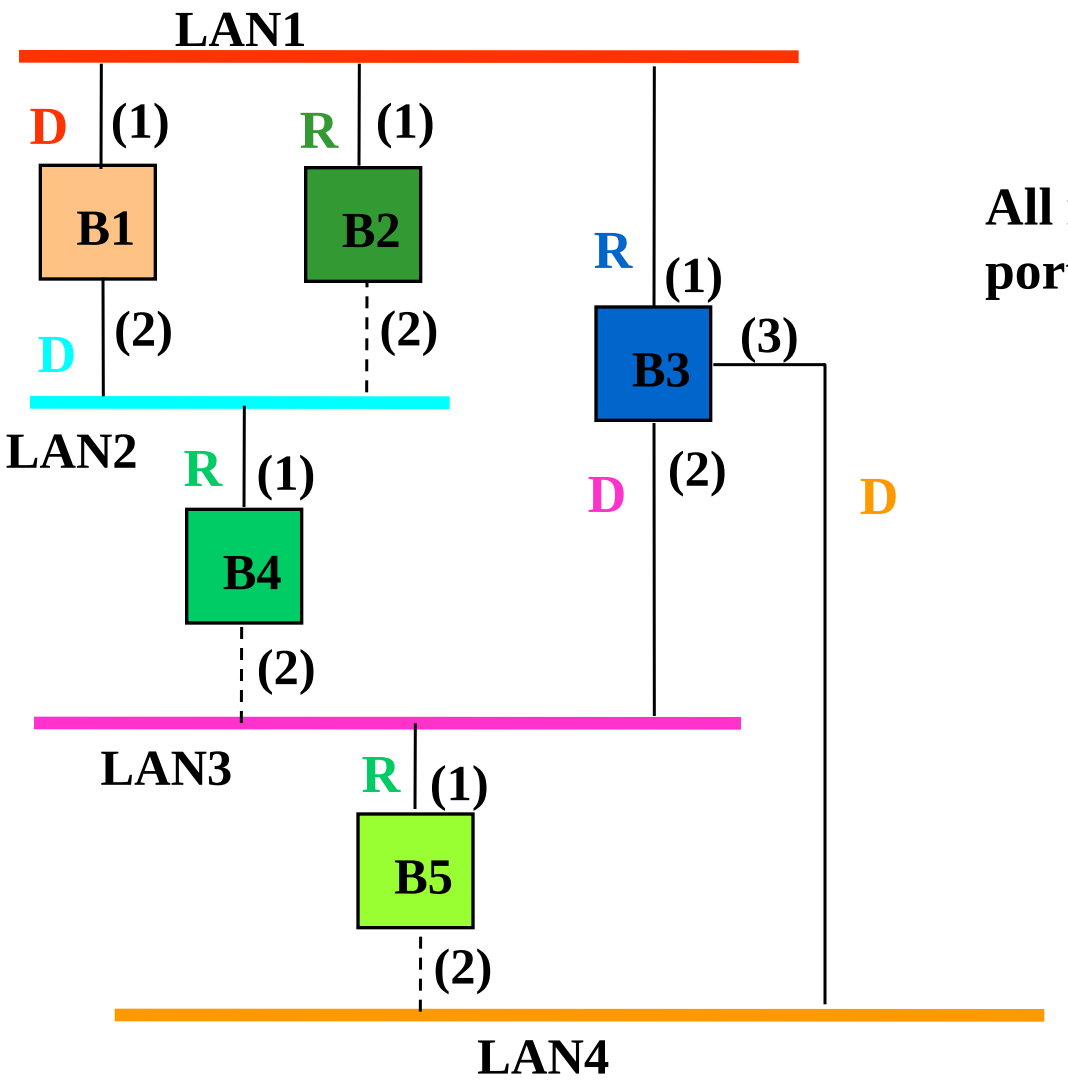
Root port selected for every bridge except root port

Generalized SPT Algorithm – Example (Cont.)



Select designated bridge for each LAN

Generalized SPT Algorithm – Example (Cont.)



All root ports & designated ports put in forwarding state

Bridge Types – Store & Fwd vs. Cut-through

- **Store & fwd**: The bridge processor receives the whole frame, processes that, meaning it does error detection using FCS and if no errors detected, the processor sets up the connection between source and destination ports
- **Cut-through**: When the sender is transmitting the frame, the bridge does not wait for the whole frame, instead as soon as it receives the header, it checks its table and sets up the connection between source and destination ports
  - This implies that the processor does not process the frame (i.e., does not check for error), instead the destination node does the checking
  - This also means cut-through is faster, however if frame is in fact erroneous, this would be a waste of resources
- Some bridges or L2 switches can work based on cut-through and network admin monitors the frames, if too many are erroneous, then the switch can dynamically change to store and forward

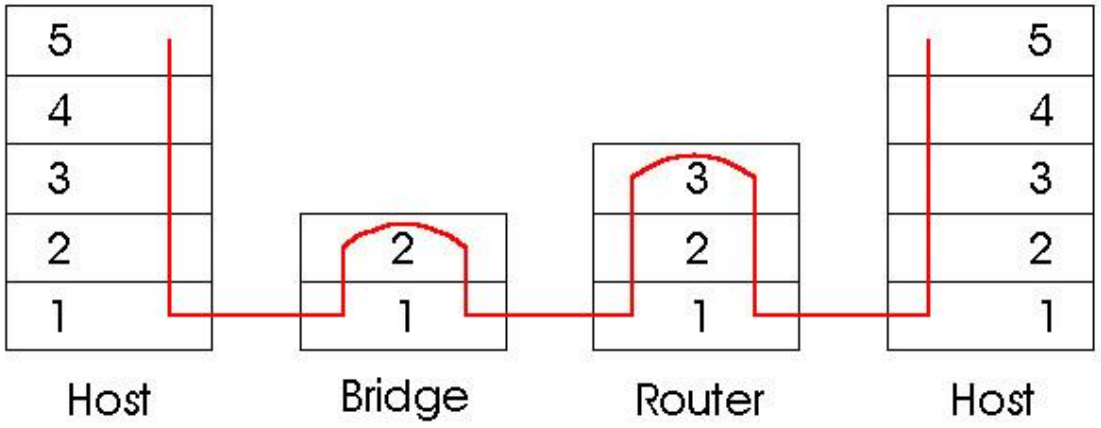
Two-Layer and Three-Layer Switches

- A two-layer switch (Layer 2 switch) is a bridge with many ports
- If each port is allocated to only one station no collision would exist
- A bridge with a few ports may be used to connect a few LANs together
- A layer 2 switch can have more sophisticated design and functionality to allow better performance

- The relation between a router and a layer 3 switch is similar to that between a bridge and a layer 2 switch in the sense that a layer 3 switch is similar to a router however it may be more sophisticated and faster

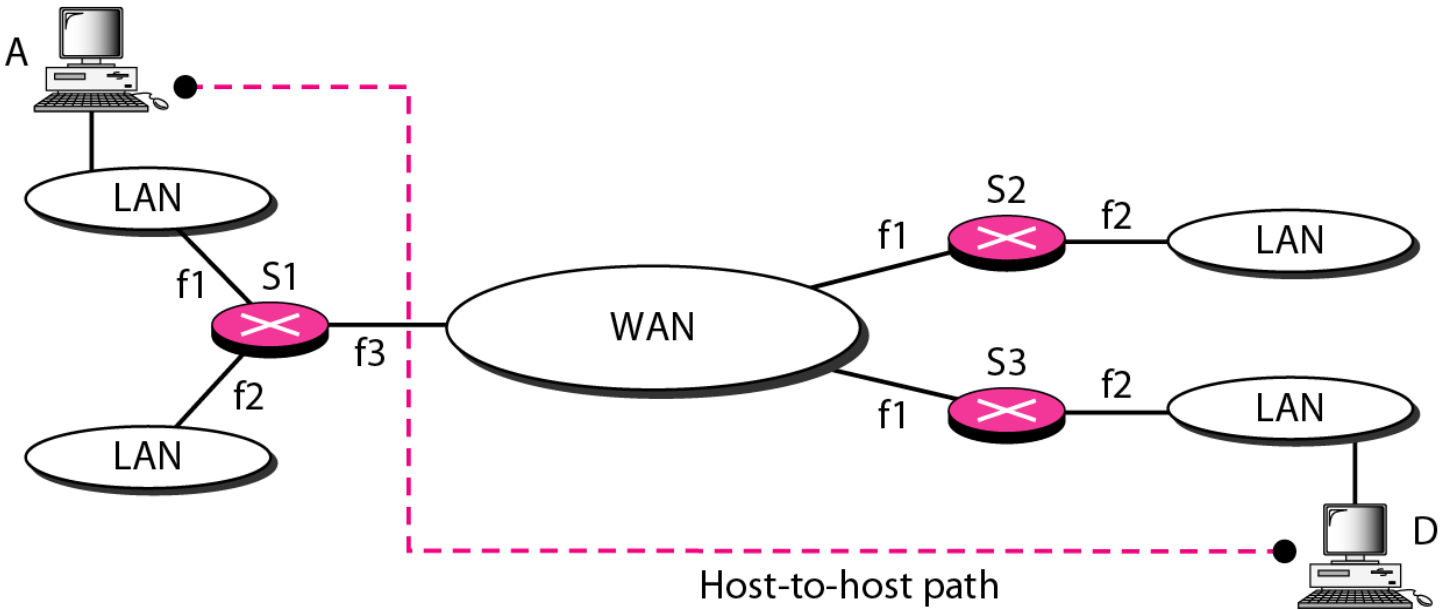
Bridges vs. or Routers

- Store-and-forward devices (bridges can be)
  - Routers or layer 3 switches: network layer devices (examine network layer headers)
  - Bridges or layer 2 switches are link layer devices
- Routers maintain routing tables, implement routing algorithms
- Layer 2 switches maintain switch tables, implement filtering, learning algorithms



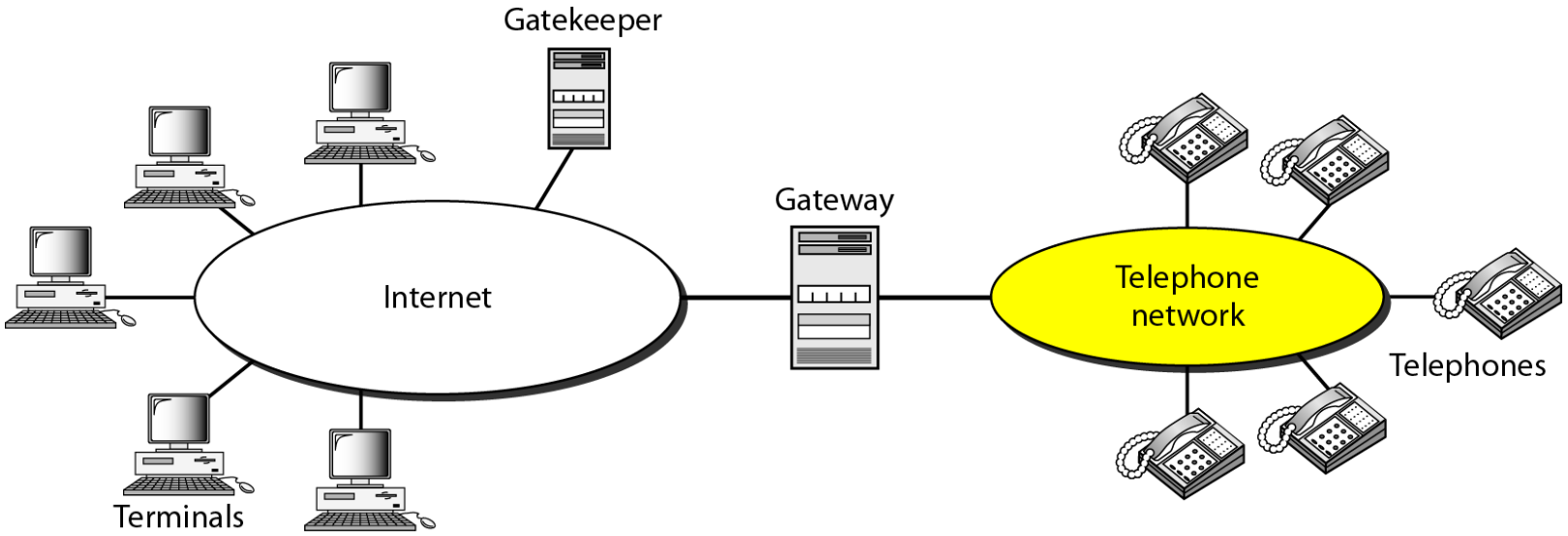
Routers – Broadcast Domain

- Bridges or L2 Switches do not see all 1s in their bridge or switch table (all entries are unicast) therefore they will flood in case of all 1s, i.e., they cannot isolate the broadcast domain



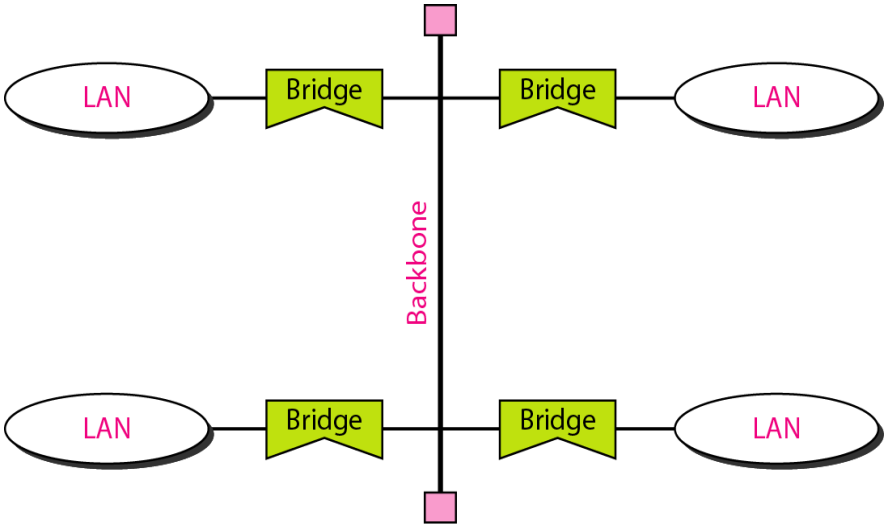
Gateway

- Aka **protocol converters**, can operate at any layer and their job is much more complex than that of routers or switches
- A gateway is typically a 5-layer device that must convert message from one protocol stack into another
- There are gateways that operate at network layer, however they are more complex than routers in the sense that they need to interface among more dissimilar networks

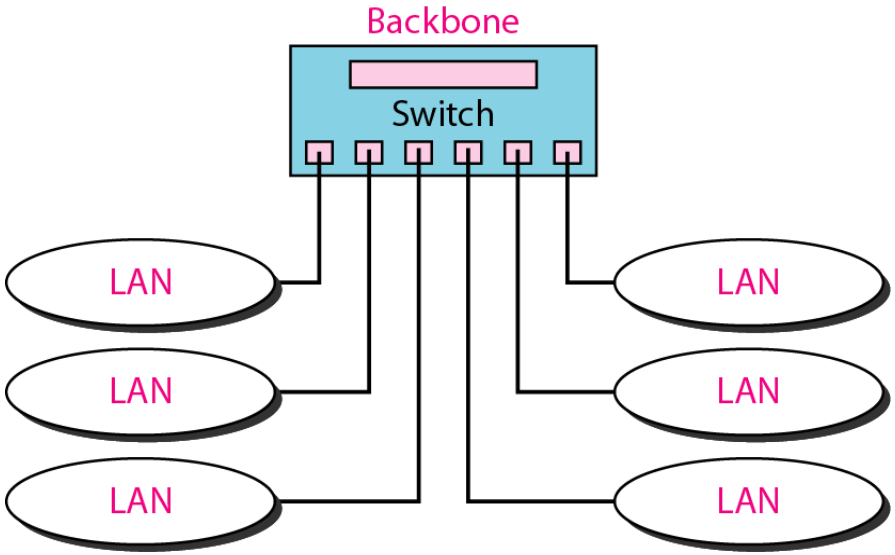


Backbone Networks

- A backbone network allows several LANs to be connected. In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN, and the backbone connects the LANs
- Example: In a bus (star) backbone, the topology of the backbone is a bus (star)



Bus Backbone



Star Backbone

Connecting Remote LANs

- A point-to-point link acts as a LAN in a remote backbone connected by bridges (aka remote bridges)
- Note that the point-to-point links can be considered as a LAN with no station and can use a Point-to-Point protocol such as PPP