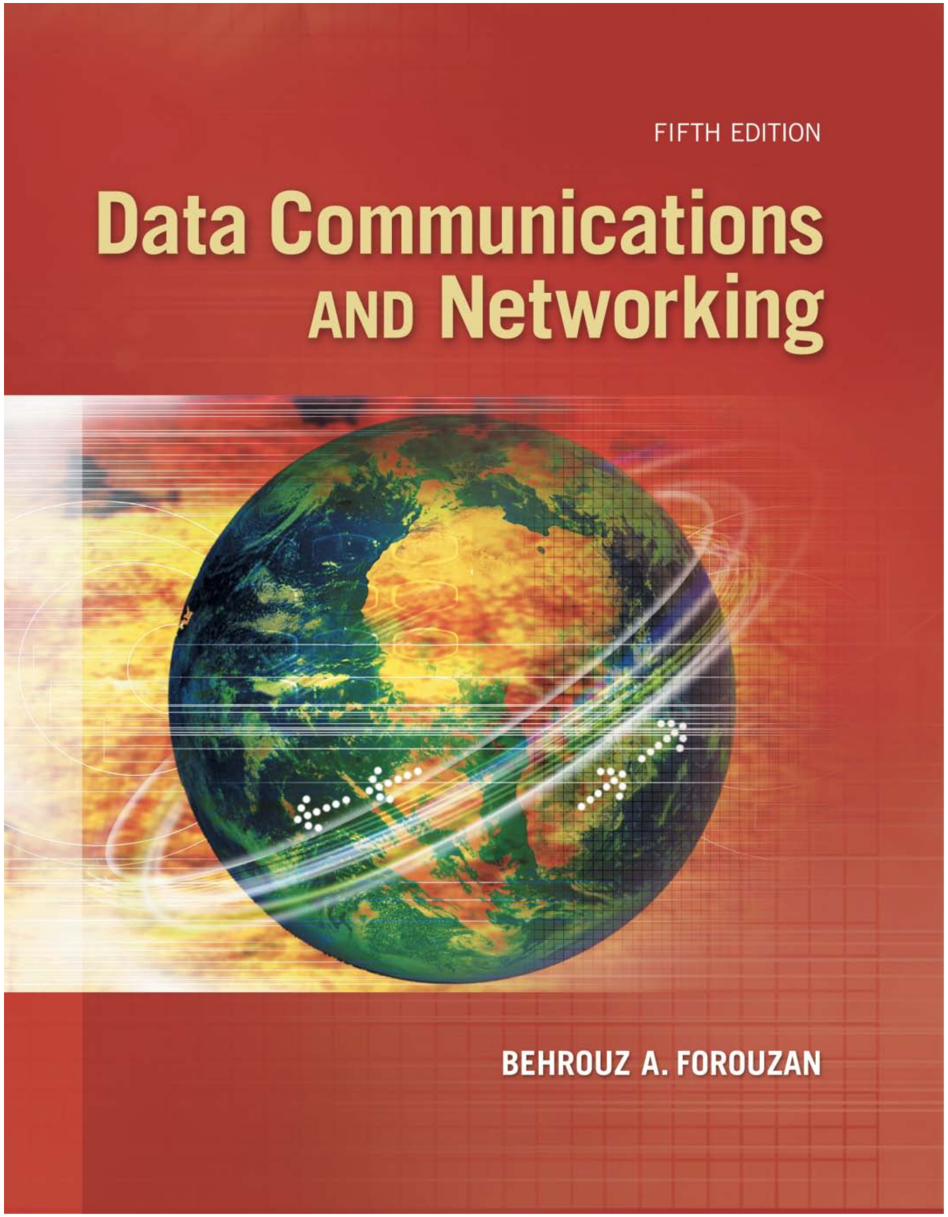
Chapter 17

Connecting Devices And Virtual LANs



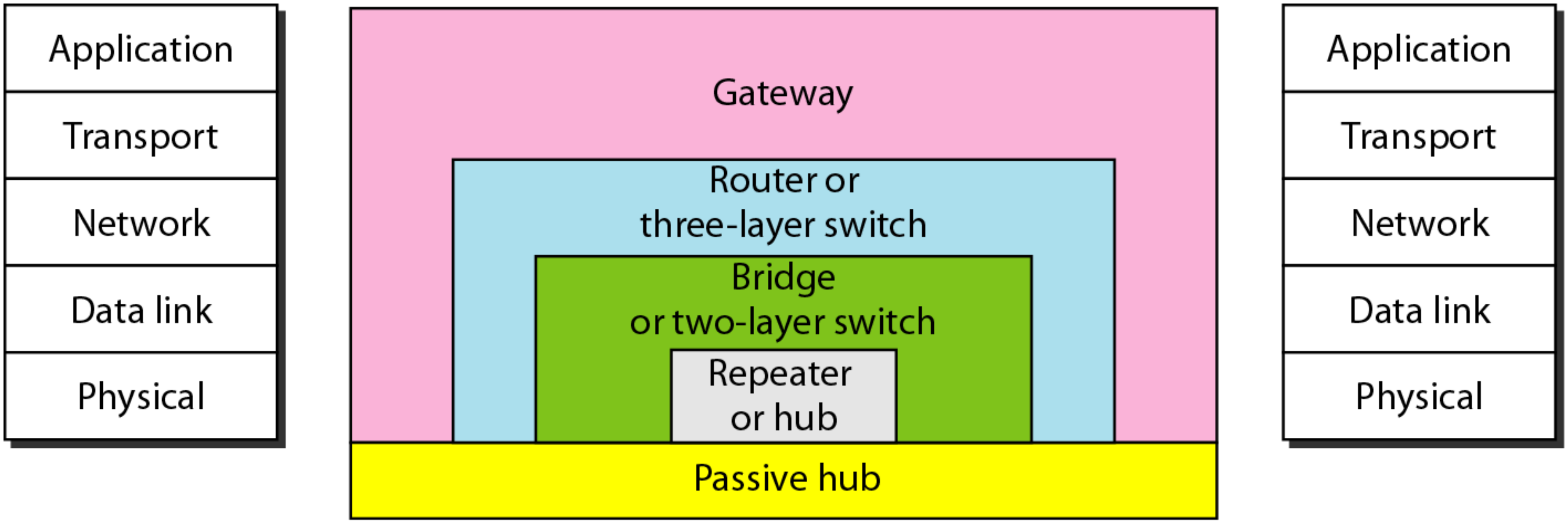
Chapter 17: Objective

- The first section discusses connecting devices. It first describes hubs and their features. The section then discusses link-layer switches (or simply switches, as they are called), and shows how they can create loops if they connect LANs with broadcast domains.

- The second section discusses virtual LANs or VLANs. The section first shows how membership in a VLAN can be defined. The section then discusses the VLAN configuration. It next shows how switches can communicate in a VLAN. Finally, the section mentions the advantages of a VLAN..

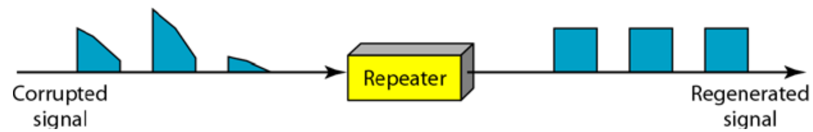
Interconnecting LAN segments

- Repeater or Hubs
- Bridges
- Switches
  - Remark: switches are essentially multi-port bridges.
  - What we say about bridges also holds for switches!
- Router



Interconnecting with Repeaters (or hubs)

- A repeater connects segments of a LAN. (Extends max distance)
- But individual segment collision domains become one large collision domain



  - A repeater is a regenerator, not an amplifier.
  - A repeater forwards every frame; it has no filtering capability.
- Can't interconnect 10BaseT & 100BaseT

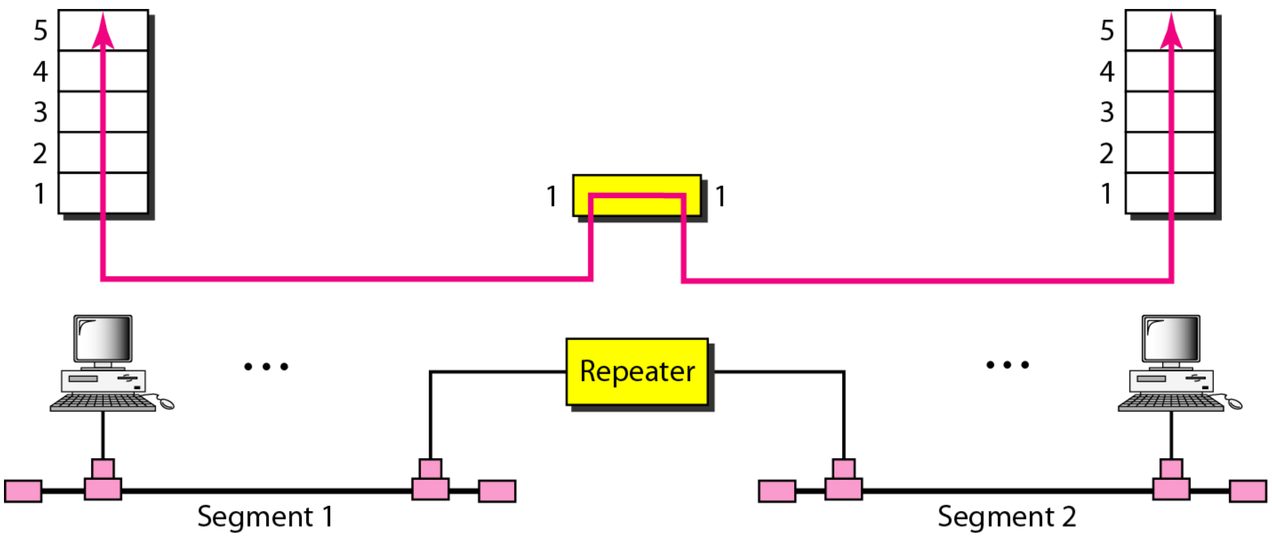
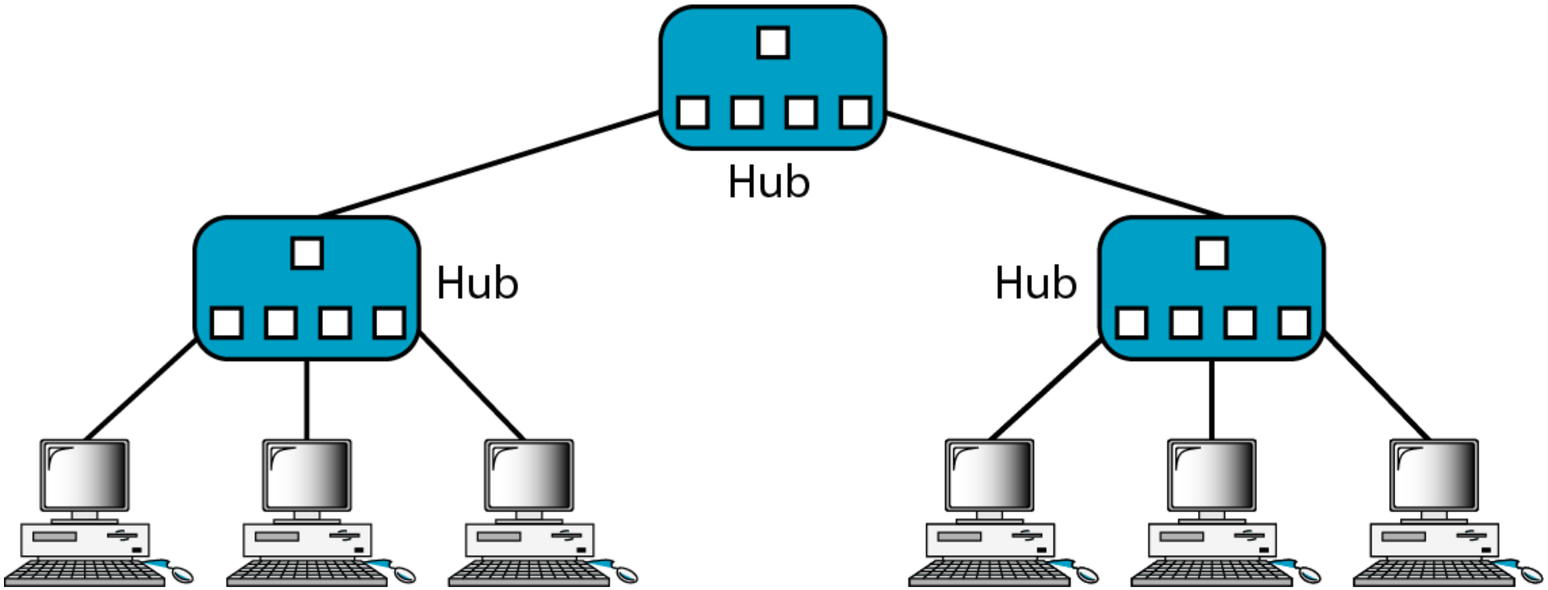
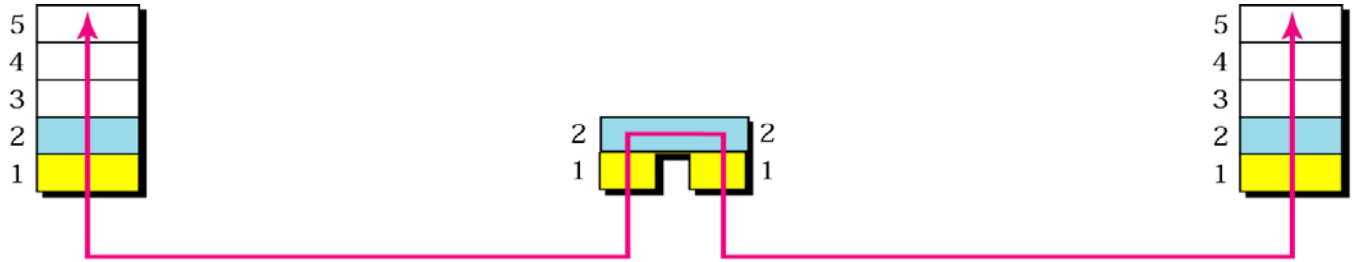


Figure 15.4 *A hierarchy of hubs*

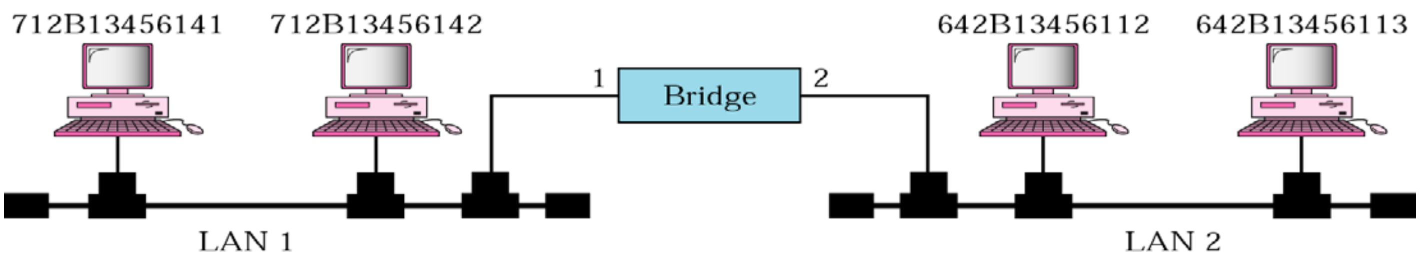


Bridges



Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

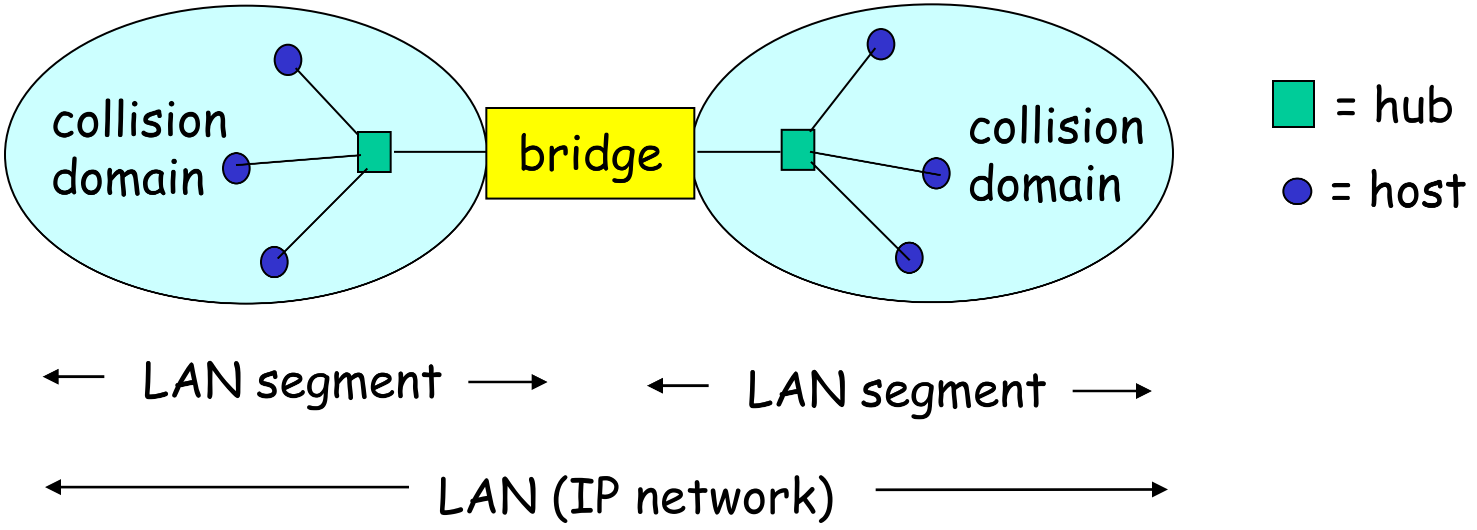
Bridge Table



- **A bridge has a table used in filtering decisions.**
- **A bridge does not change the Physical (MAC) address in a frame.**

Filtering: traffic isolation

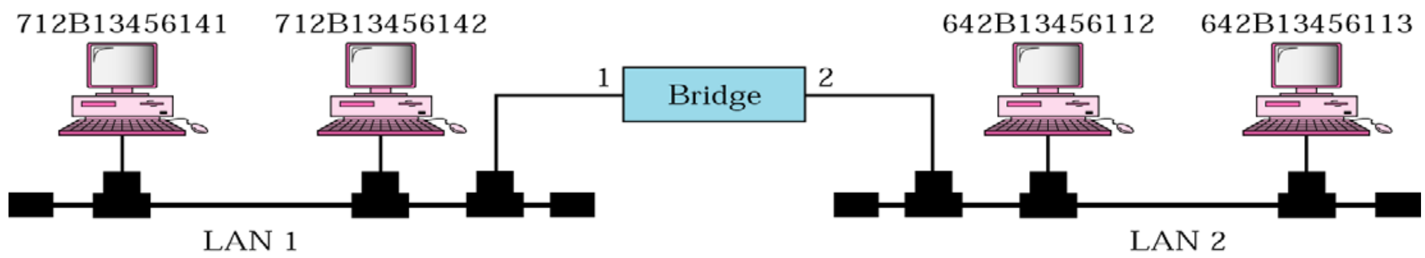
- Bridge installation breaks LAN into LAN segments
- bridges filter packets:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate collision domains



Selectively Forwarding

Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

Bridge Table



- **How do determine to which LAN segment to forward frame?**
  Sol) selectively forwards frame based on MAC dest. address
- **cf. Looks like a routing problem...**

When bridge receives a frame:

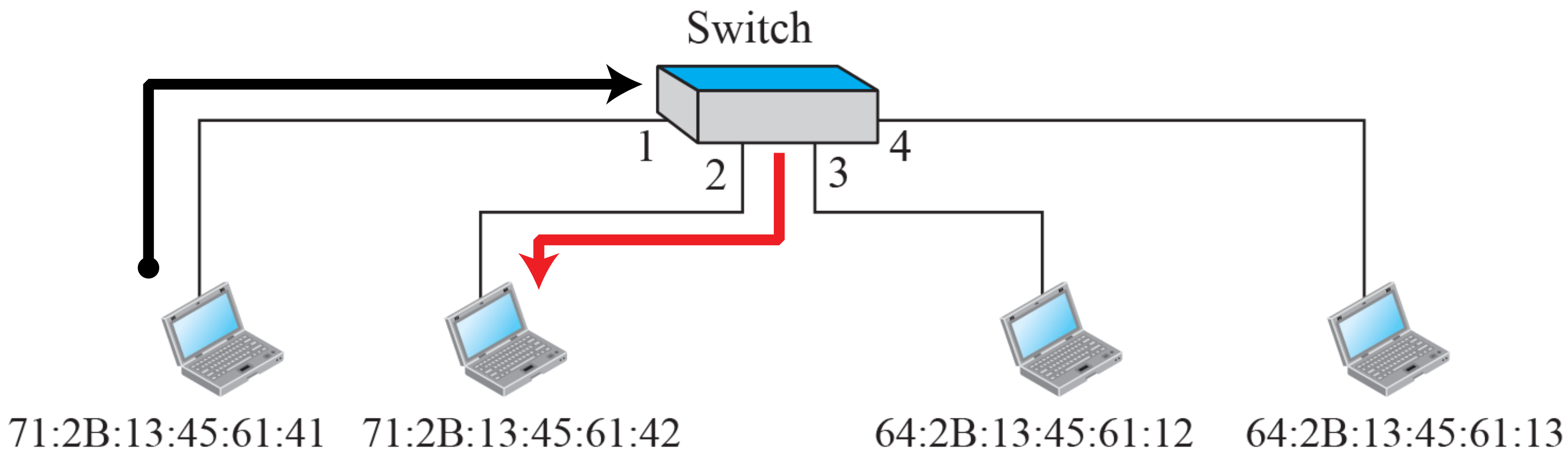
index bridge table using MAC dest address
if **entry found for destination**
then{
  if **dest on segment from which frame arrived**
    then **drop the frame**
      else **forward the frame on interface indicated**
    }
  else **flood**

Flood= forward on all but the interface on which the frame arrived

Figure 17.3: Link-Layer Switch

Switching table

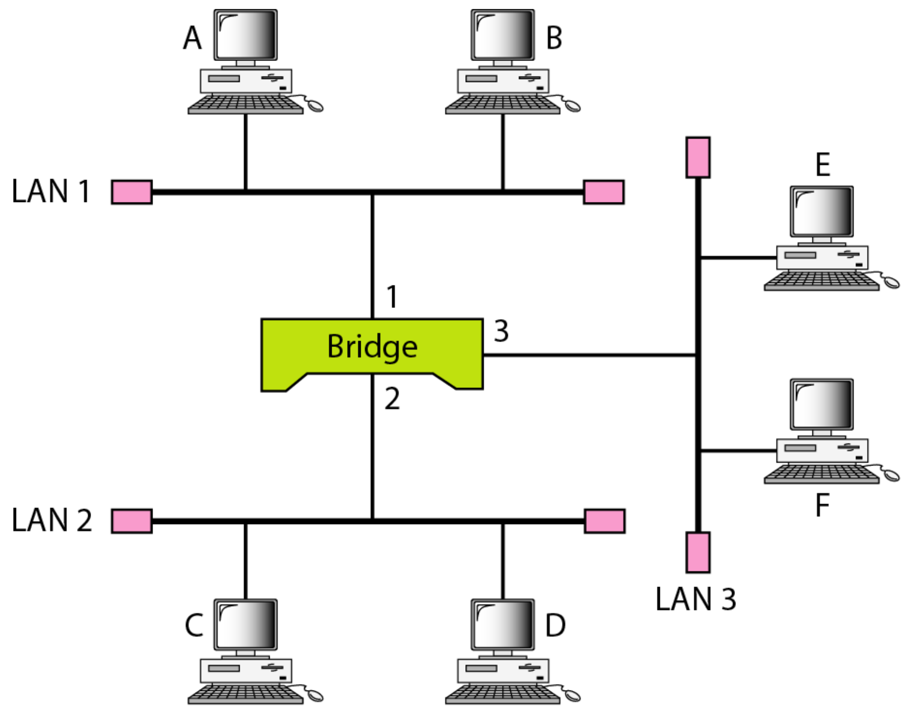
Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4



Self learning

- How does the bridge know where the destinations are?
- Sol) A bridge has a bridge table
- entry in bridge table:
  - (Node LAN Address, Bridge Interface, Time Stamp)
  - stale entries in table dropped (TTL can be 60 min)
- bridges *learn* which hosts can be reached through which interfaces
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender/location pair in bridge table

Figure 15.6 *A learning bridge and the process of learning*



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

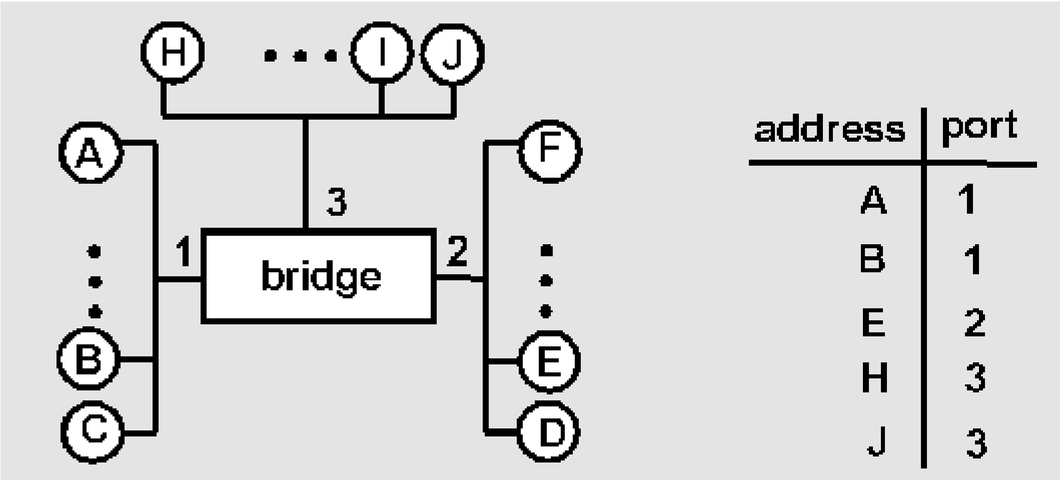
d. After B sends a frame to C

Transparent Bridges

- Bridge = Link layer device
  - stores and forwards Ethernet frames
  - examines frame header and selectively forwards frame based on MAC dest address -> filtering (traffic isolation)
  - The forwarding table is automatically made by learning frame movements (self-learning)
  - Loops in the system must be prevented.
- Transparent Bridge
  - hosts are unaware of presence of bridges
- plug-and-play
  - bridges do not need to be configured

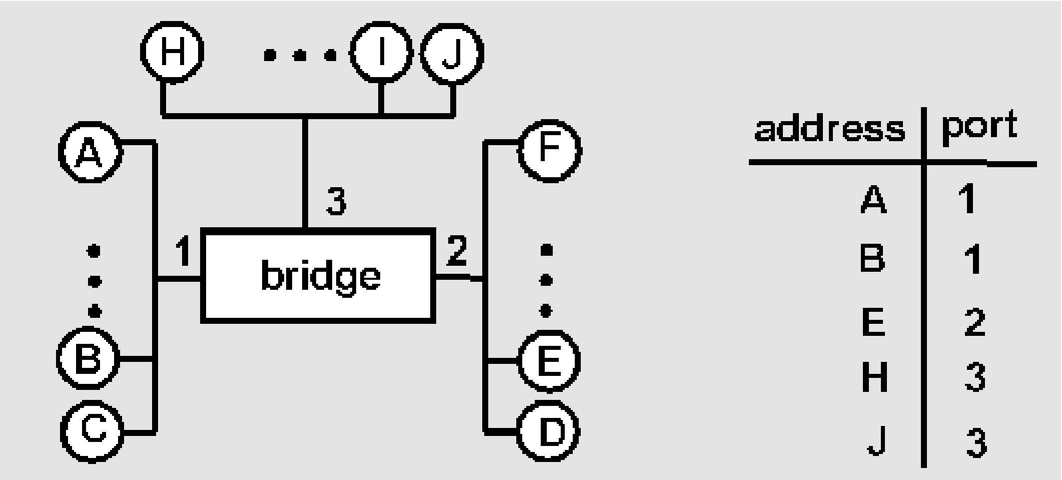
Bridge example

Suppose C sends frame to D and D replies back with frame to C.



- **Bridge receives frame from from C**
  - **notes in bridge table that C is on interface 1**
  - **because D is not in table, bridge sends frame into interfaces 2 and 3**
- **frame received by D**

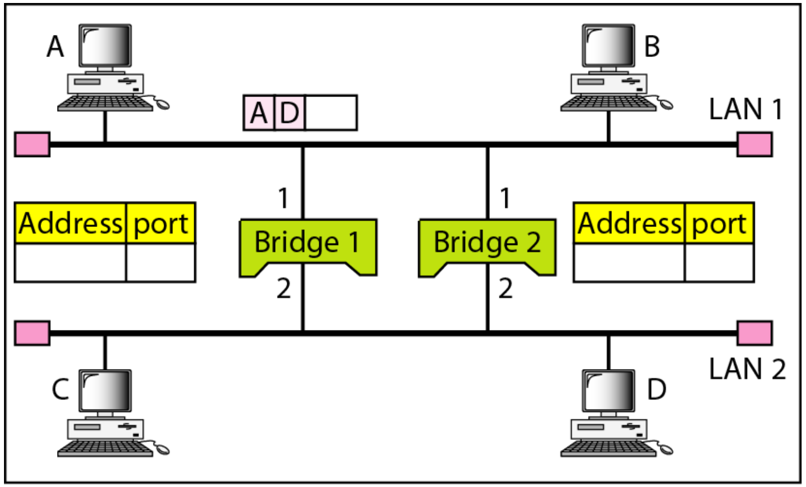
Bridge Learning: example



- D generates frame for C, sends
- bridge receives frame
  - notes in bridge table that D is on interface 2
  - bridge knows C is on interface 1, so *selectively* forwards frame to interface 1

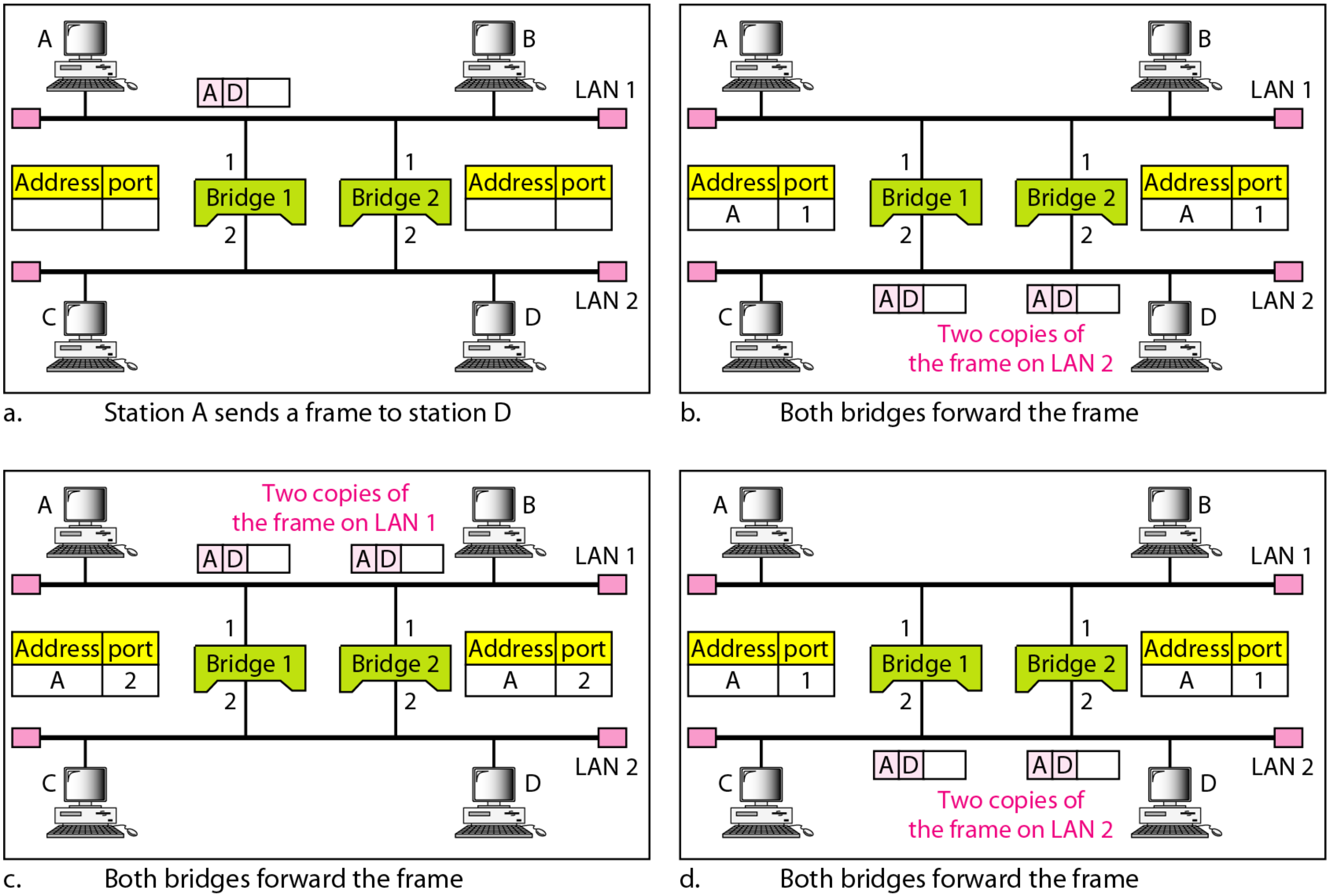
Actual System (Mesh Topology)

- **for increased reliability, desirable to have redundant, alternative paths from source to dest**
- **with multiple paths, cycles result - bridges may multiply and forward frame forever –Loop Problem**
- **solution: organize bridges in a spanning tree by disabling subset of interfaces**



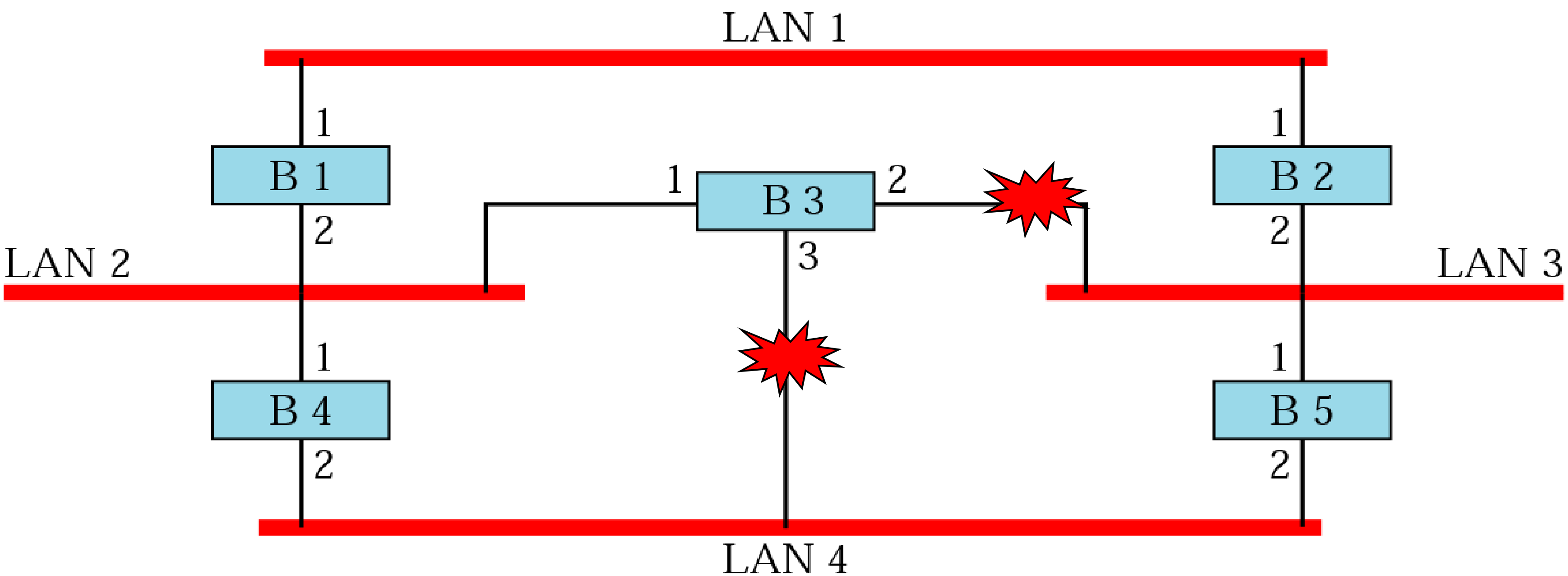
a. Station A sends a frame to station D

A Loop Problem (Figure 15.7 *Loop problem in a learning bridge)*



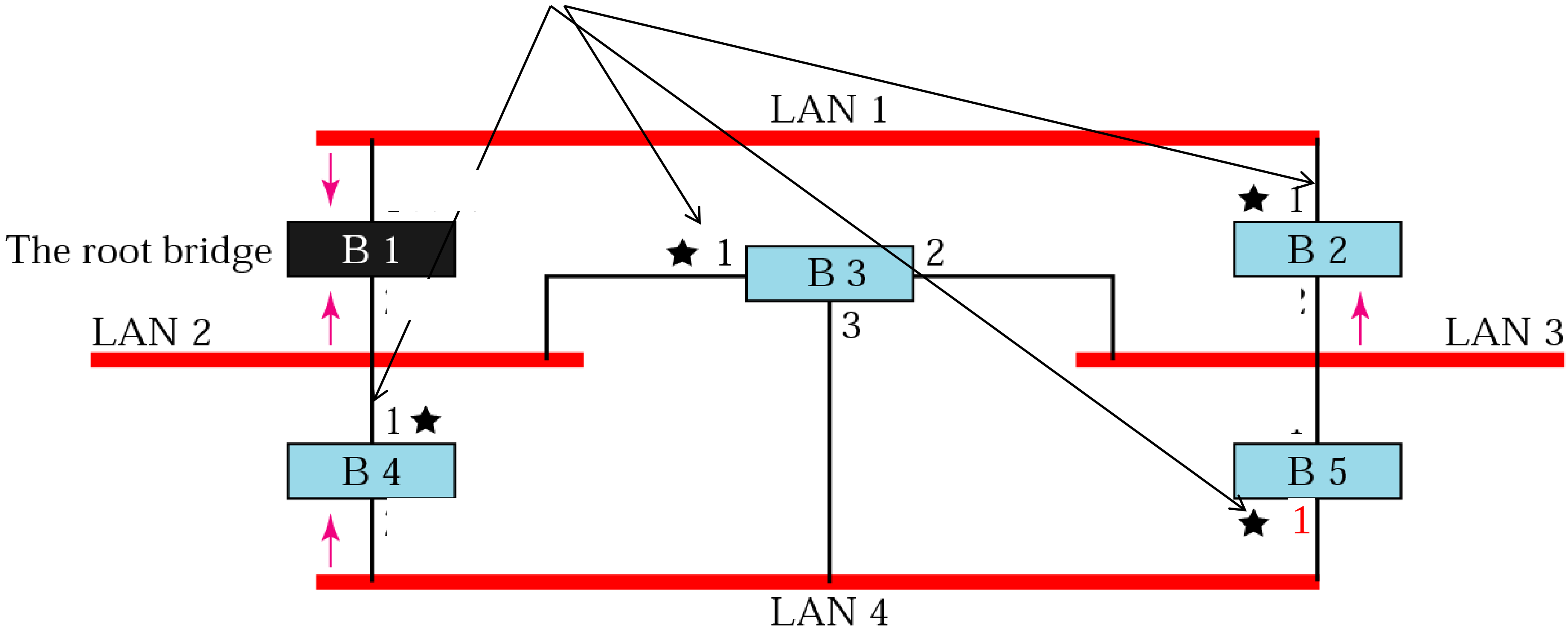
An example - Spanning Tree

- **Based on graph theory: nodes (LANs) and edges (bridges)**
  - *For any connected graph there is a spanning tree of edges connecting pairs of nodes, that maintains the connectivity of the graph but contains no closed loops*
  - **The algorithm is dynamic – hello messages every t seconds between bridges maintain topology information about the network:**
    - i.e. which bridge is down or which LAN is down
    - After 3 consecutive missed hello's the LAN/bridge is "down"



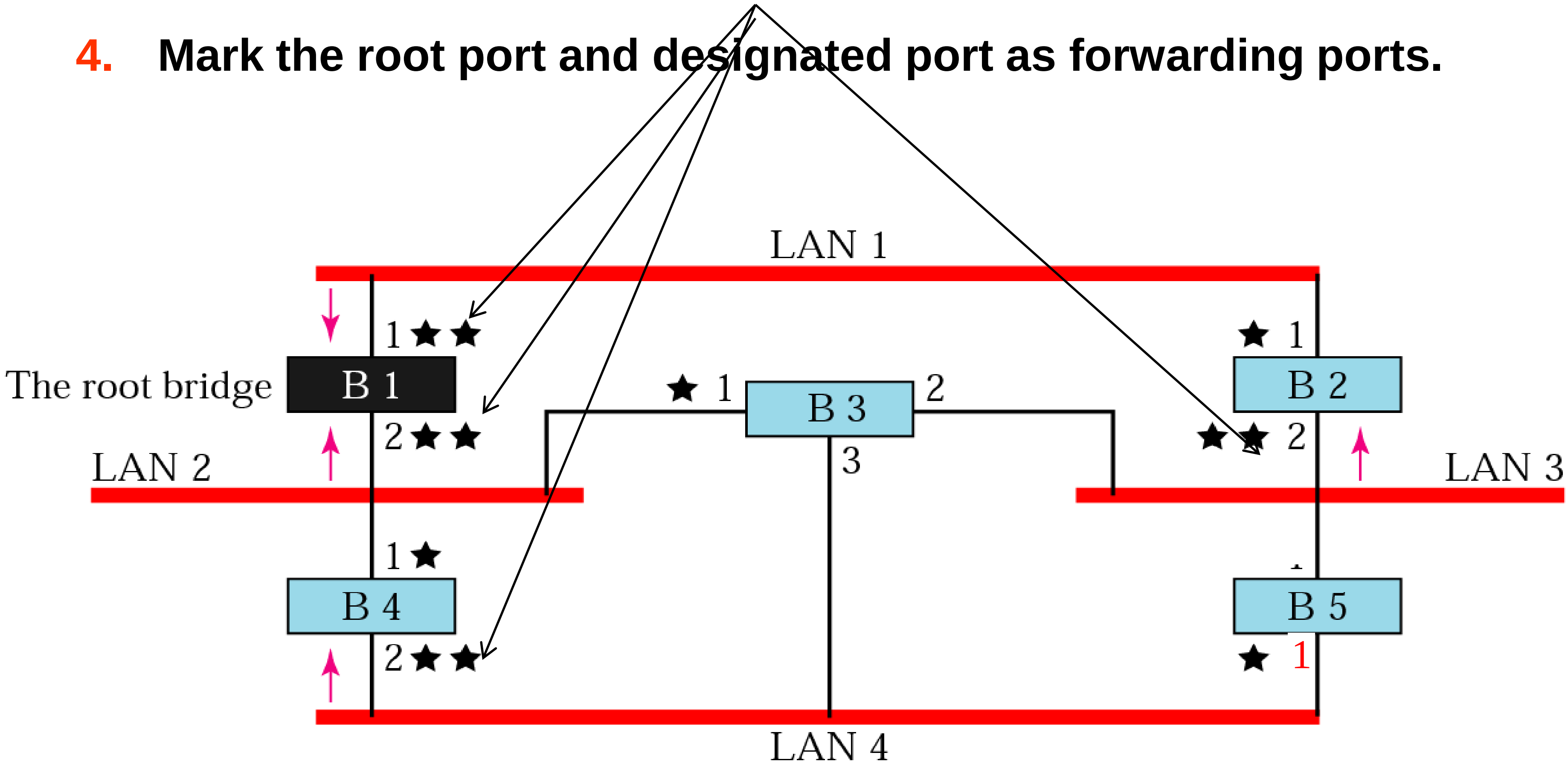
Example of Bridges Spanning Tree

1. The smallest ID is selected as the root bridge
2. Mark one port of each bridge except for the root (the cheapest path to the root bridge)



Example of Bridges Spanning Tree

3. Choose a designated bridge for each LAN
4. Mark the root port and designated port as forwarding ports.



Example of Bridges Spanning Tree

5. **Remove all other ports.**

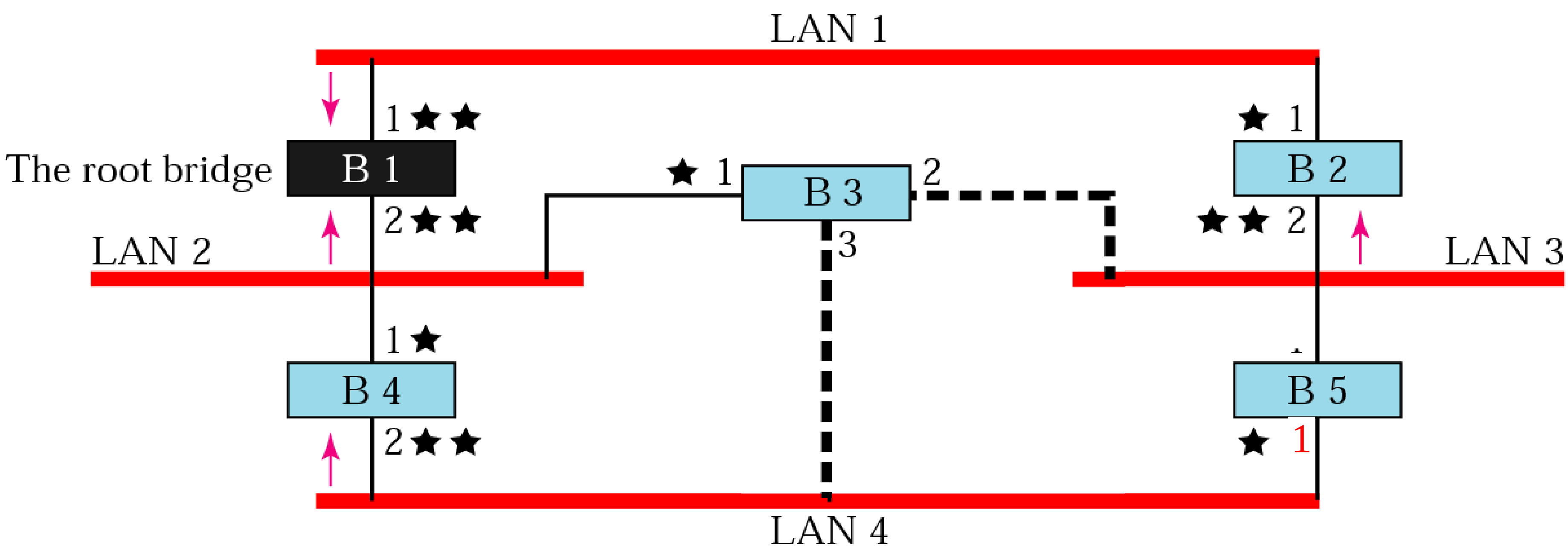
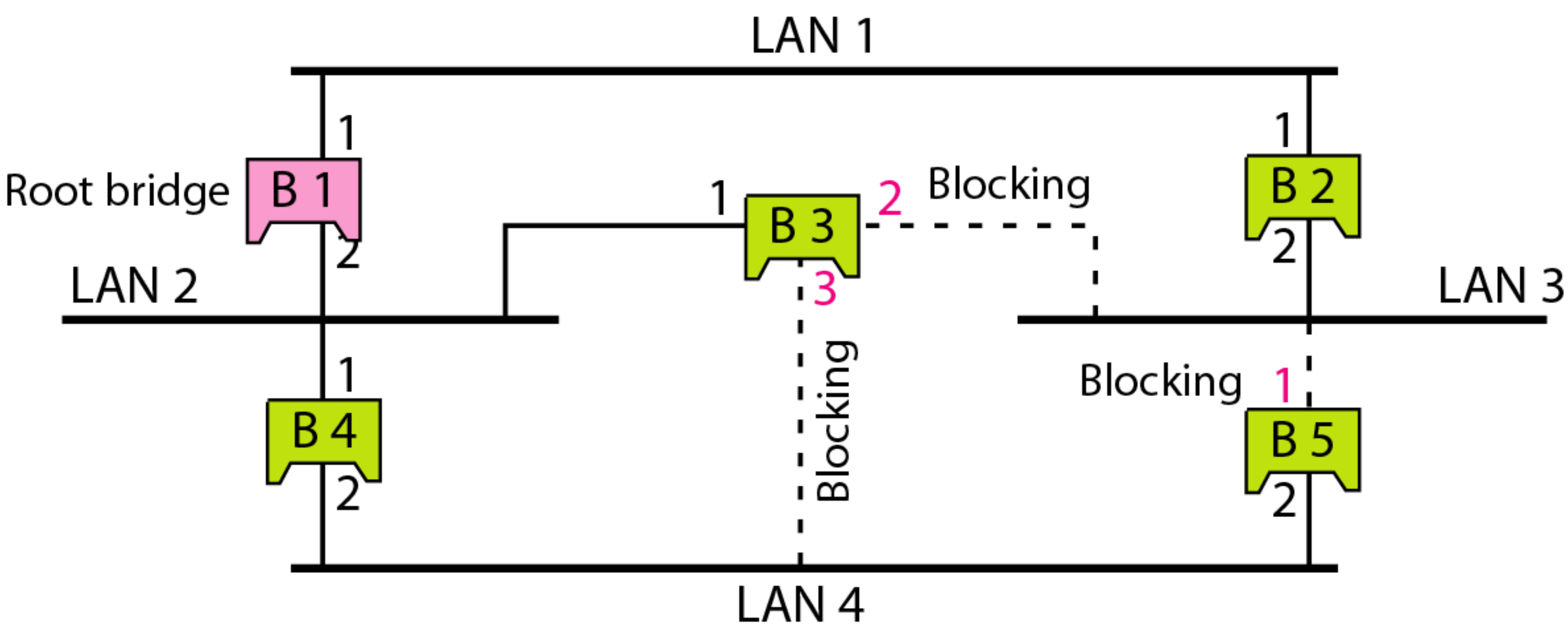


Figure 15.10 *Forwarding and blocking ports after using spanning tree algorithm*

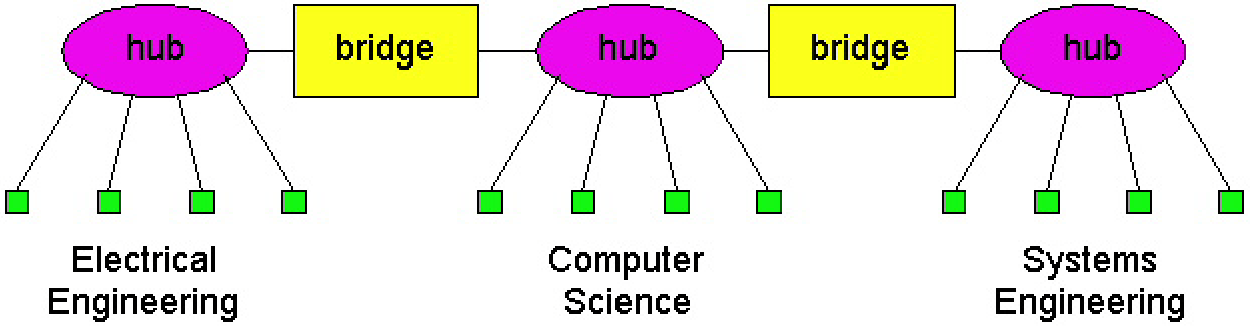


Ports 2 and 3 of bridge B3 are blocking ports (no frame is sent out of these ports).
Port 1 of bridge B5 is also a blocking port (no frame is sent out of this port).

Some bridge features

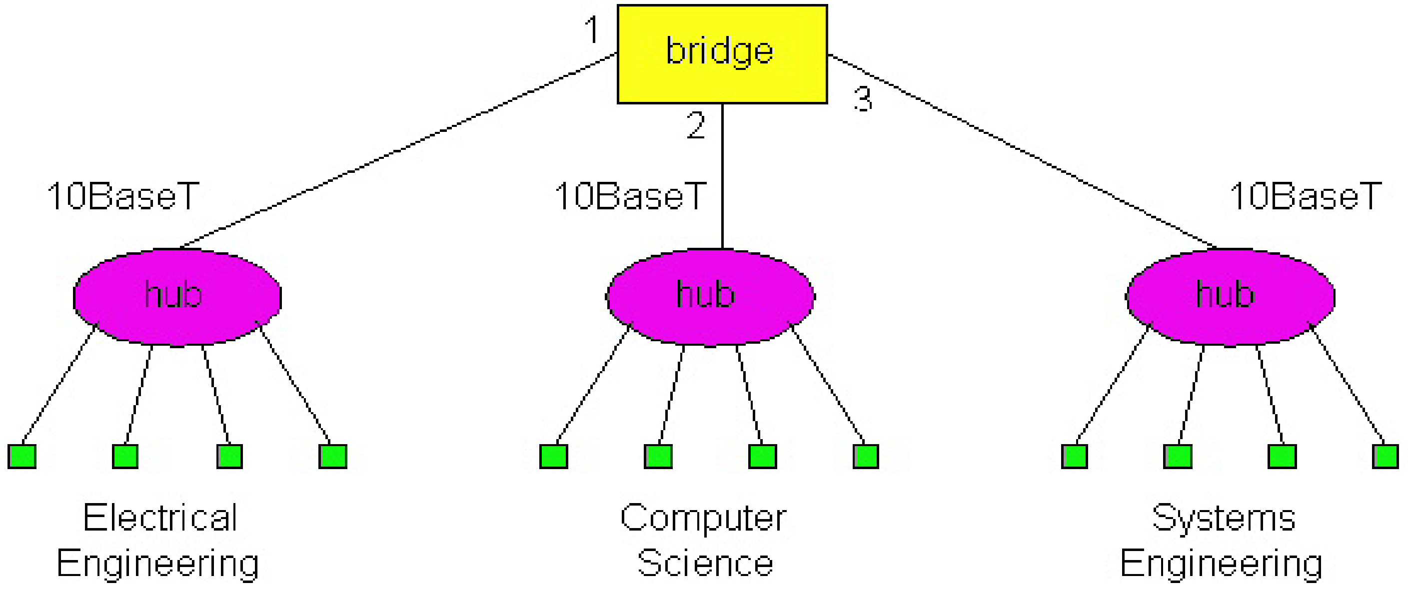
- Isolates collision domains resulting in higher total max throughput
- limitless number of nodes and geographical coverage
- Can connect different Ethernet types
  - Frame format conversion (Ethernet → Wireless LAN)
  - Compensate for the difference of data rate (Store & Forward)
  - Cannot support different MAX Data size (not allow the frag/reassembly)
  - Different Security measures (decrypt message before forwarding)
- Transparent ("plug-and-play"): no configuration necessary

An example of Bridge Interconnection



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

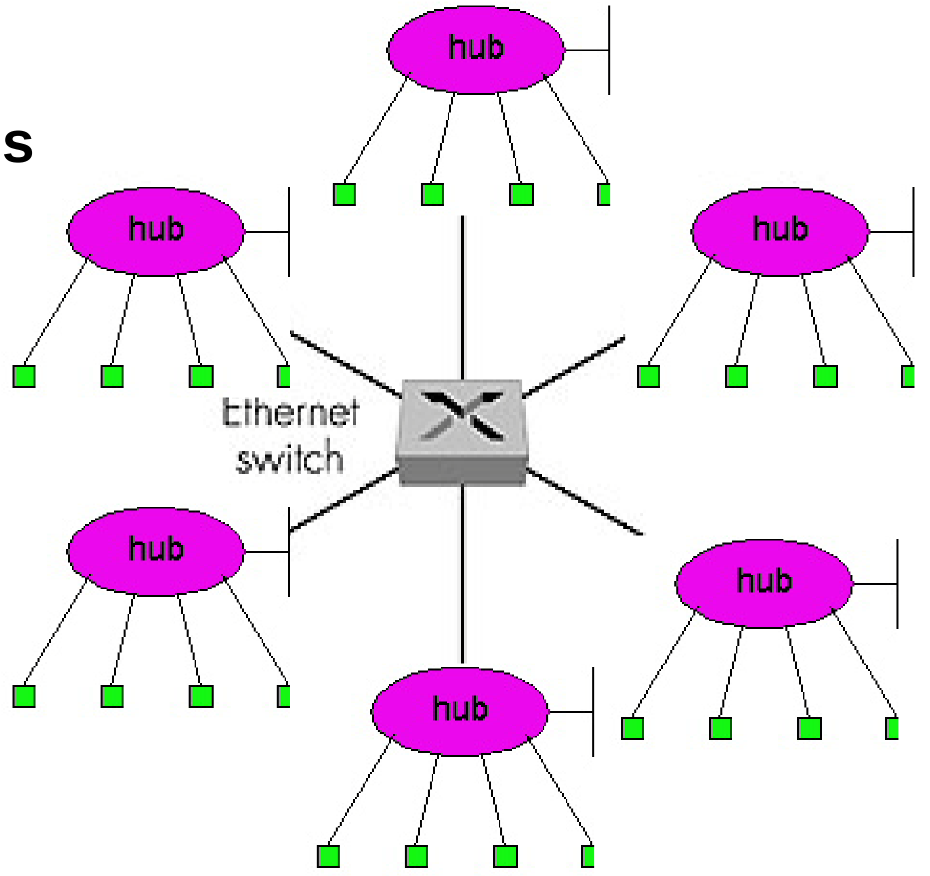
Another example of Bridge Interconnection



Recommended !

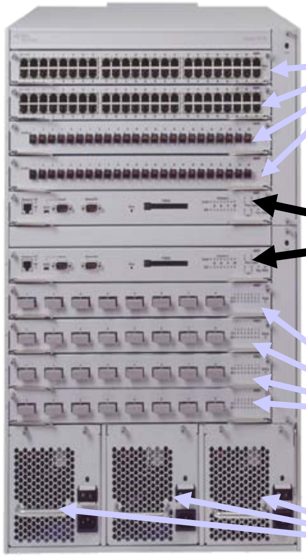
Switches

- Essentially a multi-interface bridge
- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-A' and B-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!



Special Switches

- **cut-through switching:** **frame forwarded from input to output port without awaiting for assembly of entire frame**
  - **slight reduction in latency**
- **combinations of shared/dedicated, 10/100/1000 Mbps interfaces**



High density 10/100BaseT and 100BaseFX ports (up to 96*100BaseT is typical per linecard)

High capacity switching cards (duplicated) (typical capacity is 64Gbps or greater for this size of box)

Gigabit Ethernet ports – typically 8 ports per linecard

Redundant Power Supply Units (PSU)

Router

- **Three-layer device**
  - **Limited broadcasting vs. Unknow-broadcasting**
  - **Shortest path vs. Spanning tree**

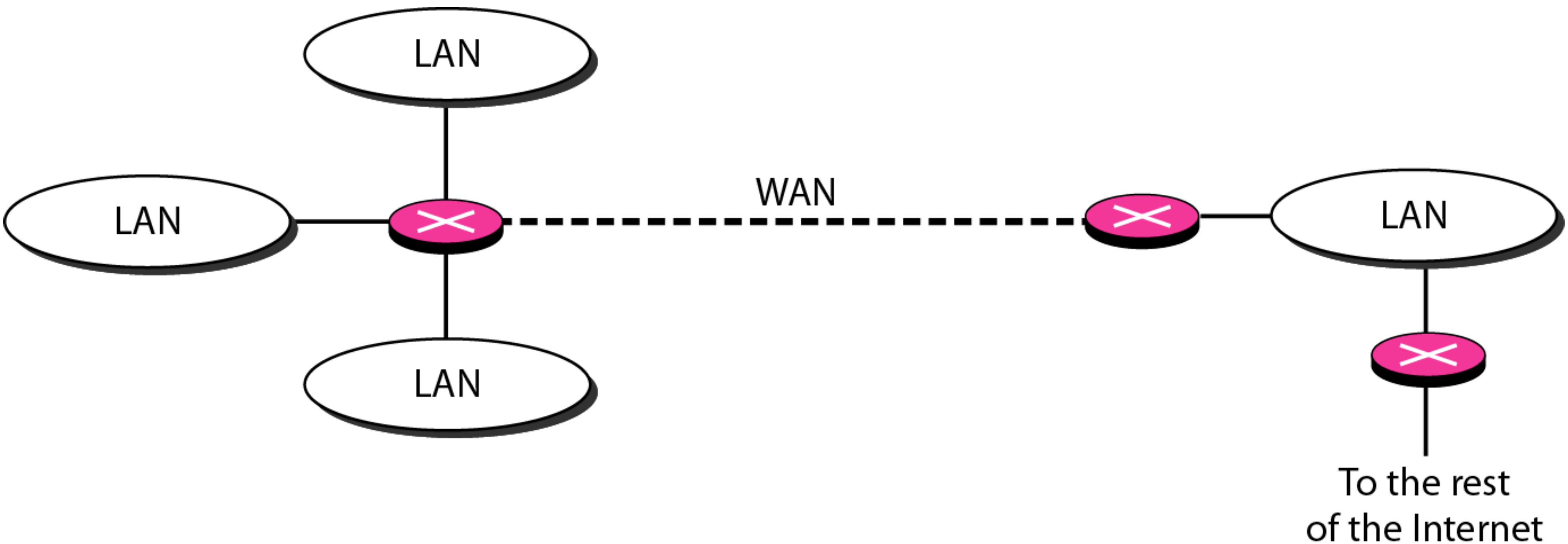
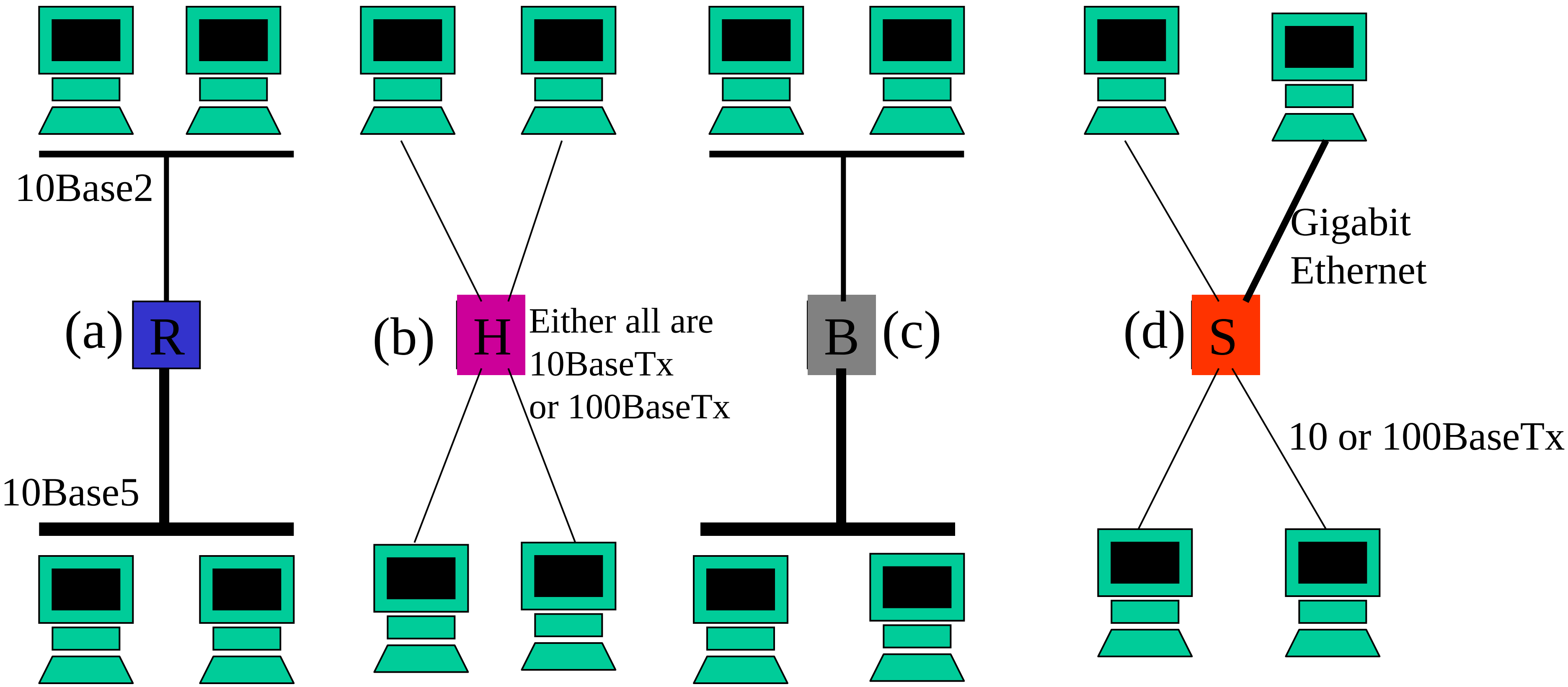


Figure 15.11 *Routers connecting independent LANs and WANs*

Repeaters, Hubs, Bridges, Switches, Routers



What is the available bandwidth per network? Per station?
What is the growth capacity of each network? How could they be extended/expanded?
What congestion/contention characteristics does each network exhibit?

HUB vs. SWITCH

- **Hub**
  - **Implements a logical bus or ring topology within a single device.**
- **Switch**
  - **Device that creates a true star network.**
  - **Data is delivered to the appropriate user based on the destination address.**
  - **No other devices on the network hear or interfere with the data transmission.**
- **Connections to hubs/switches usually over twisted pair in a physical star configuration.**

Switching vs Bridging

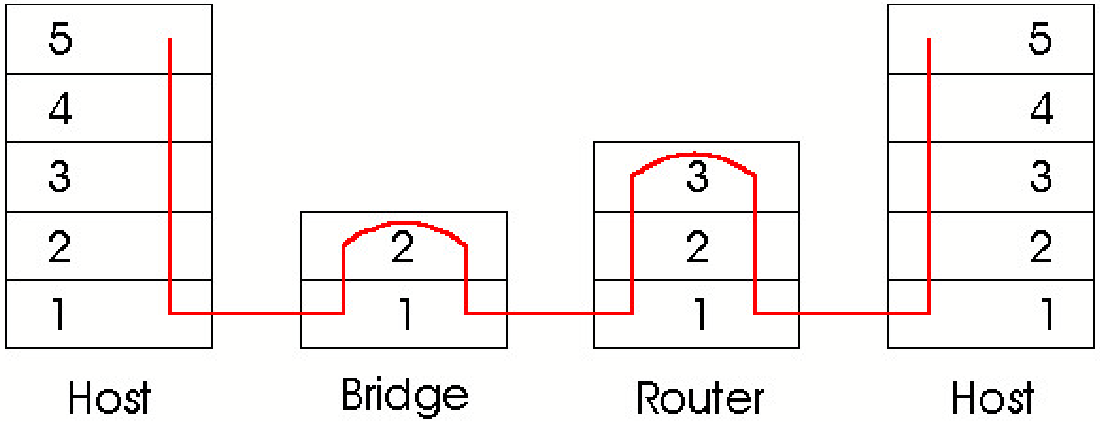
- Switching: information based on next hop address (label)
  - a data link layer relay per connection basis
  - Indexing operation based on circuit numbers (label) in Connection-oriented network
  - Fast and Scalable hardware based forwarding for large networks and large address spaces
  - A data link layer should be designed to carry a packet across networks
  - Complexity~O(1)

- **Bridging: forwarding based on link address**
  - **a data link layer relay Per-packet basis**
  - **an exact match (link-layer addressing) address lookup in datagram network**
  - **software based forwarding in shared media LANs.**
  - **A data link layer should be designed to carry a link layer frame across a single hop**
  - **Complexity~O(1)**

❖**Bridging is often equated with switching.**

Bridges vs. Routers

- **both store-and-forward devices**
  - **routers: network layer devices (examine network layer headers)**
  - **bridges are link layer devices**
- **routers maintain routing tables, implement routing algorithms**
- **bridges maintain bridge tables, implement filtering, learning and spanning tree algorithms**



Routers vs. Bridges

Bridges + and -

+ Bridge operation is simpler requiring less packet processing

+ Bridge tables are self learning

- All traffic confined to spanning tree, even when alternative bandwidth is available

- Bridges do not offer protection from broadcast storms

Routers vs. Bridges

Routers + and -

+ arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)

+ provide protection against broadcast storms

- require IP address configuration (not plug and play)

- require higher packet processing

- bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)

Routing vs Switching

- **Routing: forwarding based on destination address,**
  - **a Network layer relay**
  - **Per-packet basis address lookup - Max prefix match (a best-fit or longest-match)**
  - **Complexity~O(log2n)**
  - ❖ **Address indicates the uniqueness within the network**
  - ❖ **These distinctions apply on all data links: ATM, Ethernet, SONET (forwarding)**

- Switching: information based on next hop address (label)
  - a data link layer relay
  - Indexing operation based on circuit numbers (label) in Connection-oriented network
  - Fast and Scalable for large networks and large address spaces
  - Complexity~O(1)
  - ❖ Circuit number (label) indicates the link identification among multiplexed links. It reduces the time it takes to match the code using a shorter one that exactly matches a code associated with an individual route entry.

Bridging vs Routing

Attribute	Bridging	Routing
Connection-mode	Connection-less	Connection-less
Exchange-mode	Packet routing	Packet forwarding
Packet size	Variable (60-1500B)	Variable (60-1500B)
Forwarding complexity	Low (spanning tree)	High (time to live)
Information	Data, voice and video	Data, voice, and video
Path determination	Per packet	Per packet
Forwarding state		

- **Router.**

Summary

- **Switching virtual Circuit-based networks**
  - **Layer 2 forwarding based on circuit**
  - **Data transfer in Switch hardware**
  - **Connection oriented model for forwarding look-up**
  - **no topology discover**
  - **Eg.: ATM label switching**

- Routing Datagram networks
  - Layer 3 forwarding based on destination address
  - Processor (Software) involved in Data transfer
  - Datagram model for forwarding look-up
  - Discover the network topology
  - Eg.: IP Router

- Bridging in broadcast network
  - Layer 2 forwarding based on an exact match (link-layer addressing)
  - Processor (Software) involved in Data transfer
  - Datagram model for forwarding look-up
  - Discover the end-system
  - Eg. LAN Bridge

Summary comparison

	hubs	bridges	routers	switches
traffic isolation	no	yes	yes	yes
plug & play	yes	yes	no	yes
optimal routing	no	no	yes	no
cut through	yes	no	no	yes

17-2 VIRTUAL LANS

A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic. What happens if we need a virtual connection between two stations belonging to two different physical LANs? We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

17-2 VIRTUAL LANS

- **LAN이 커지면 무엇이 문제인가?**
  - **LAN에 연결된 PC는 수신된 브로드캐스트 프레임을 처리하기 위해 CPU 시간을 소모해야 함**
  - **크기가 커지면 더 많은 브로드캐스트 프레임을 처리해야 함**
    - 따라서 적절한 크기로 유지하는 것이 좋다.
  - **관련 없는 다른 사람이 프레임을 복사해서 엿볼 수 있다.**

- **해결책**
  - **적절한 크기의 여러 개 LAN으로 구성**
    - 동일한 지역에서도 서로 다른 그룹이 독립적인 활동 보장
    - 서로 다른 subnet의 구성을 위해 서로 다른 LAN의 사용
    - 서로 지역적으로 다른 사람들을 동적으로 묶을 수 있음
      - **하나의 장비로 추가 하드웨어 구입 없이 다수의 LAN 구성**

Figure 17.10: A switch connecting three LANs

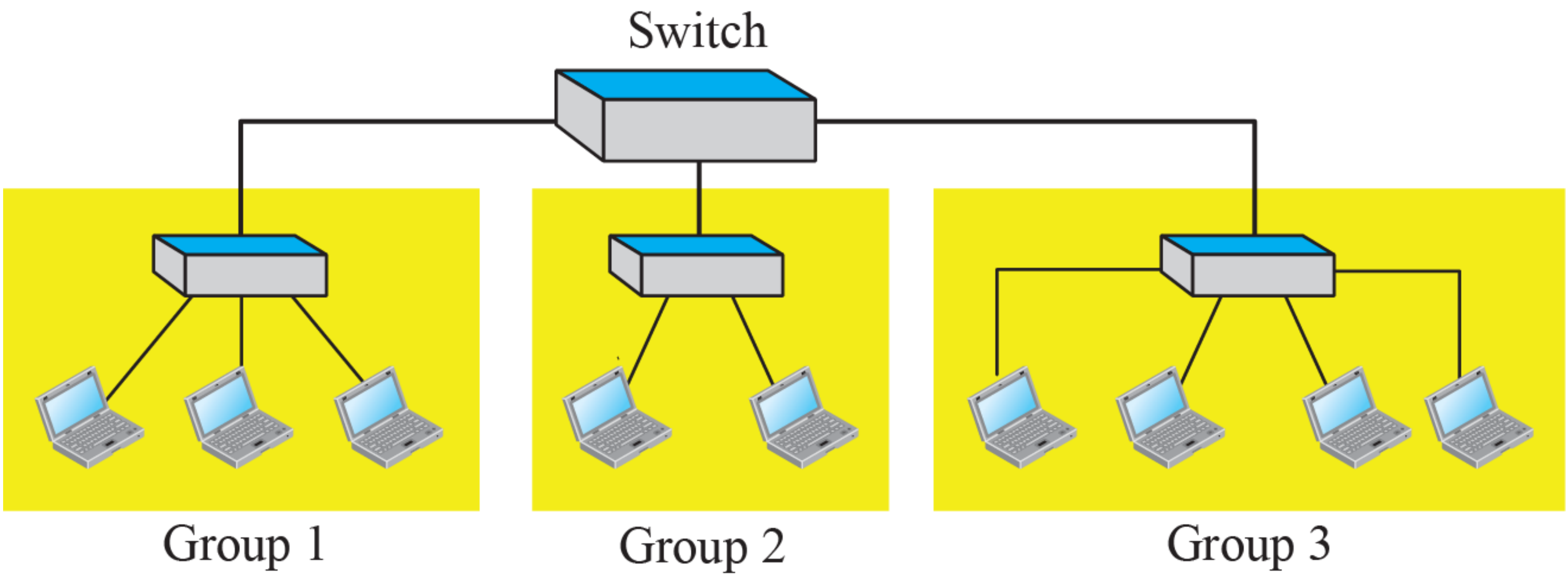


Figure 17.11: A switch using VLAN software

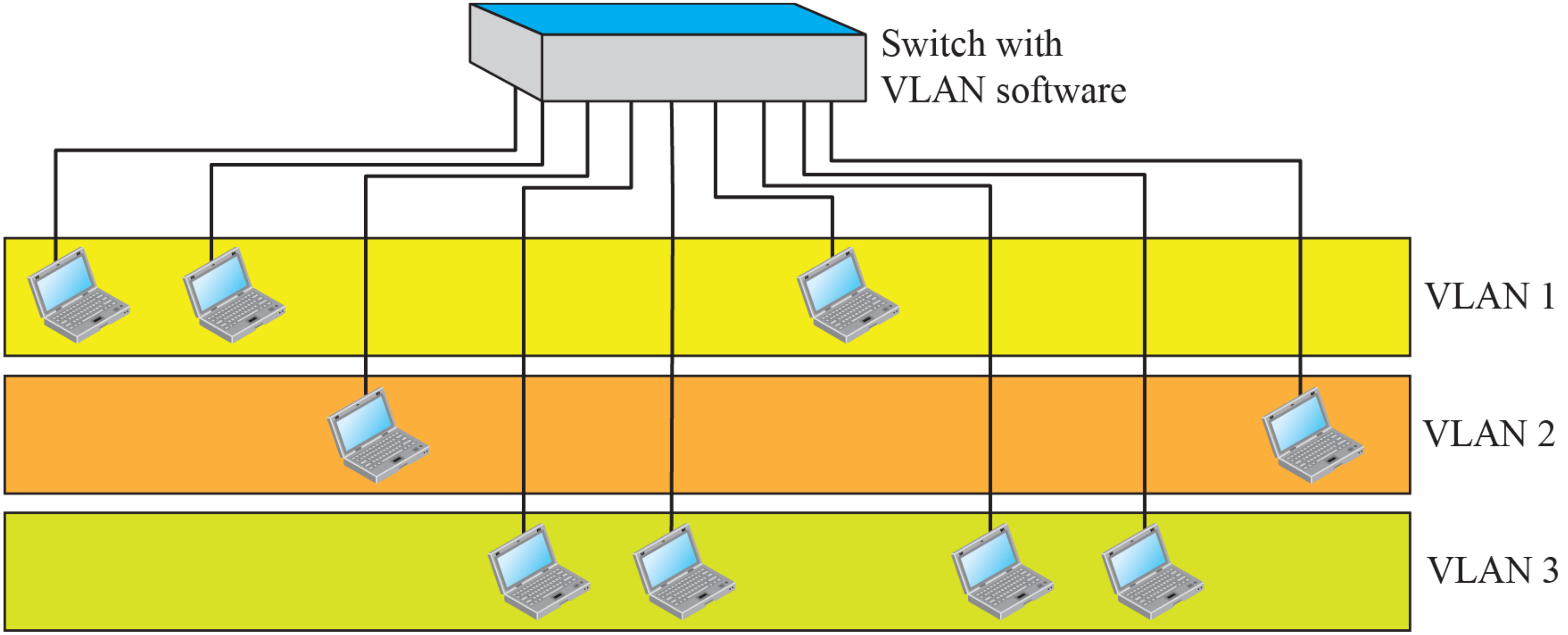
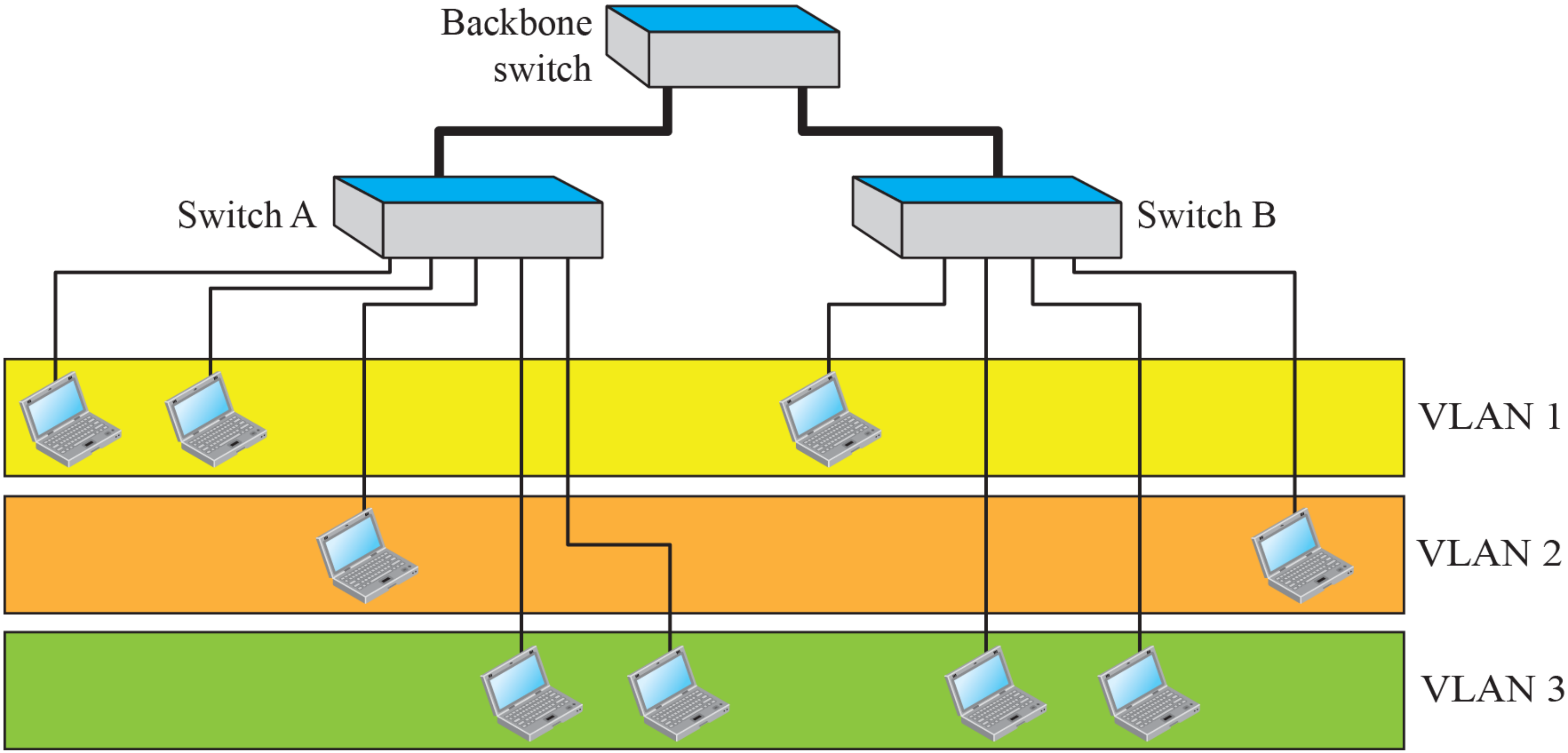
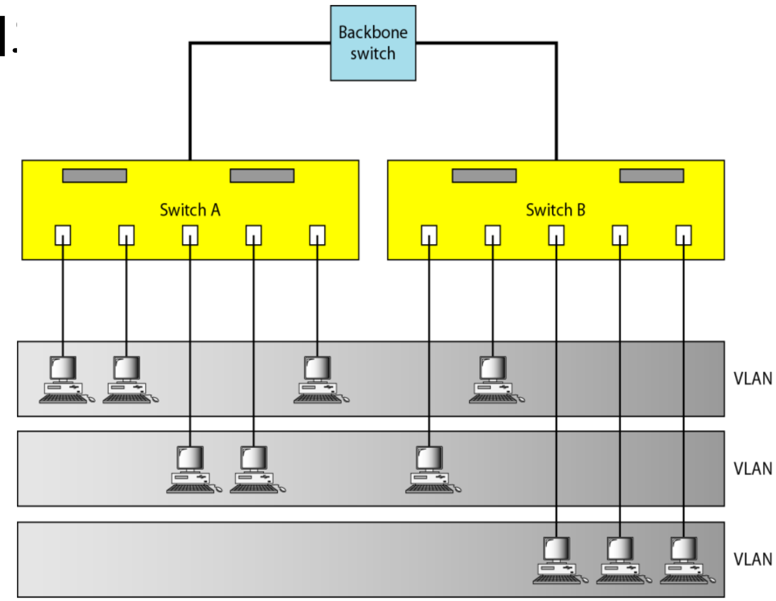


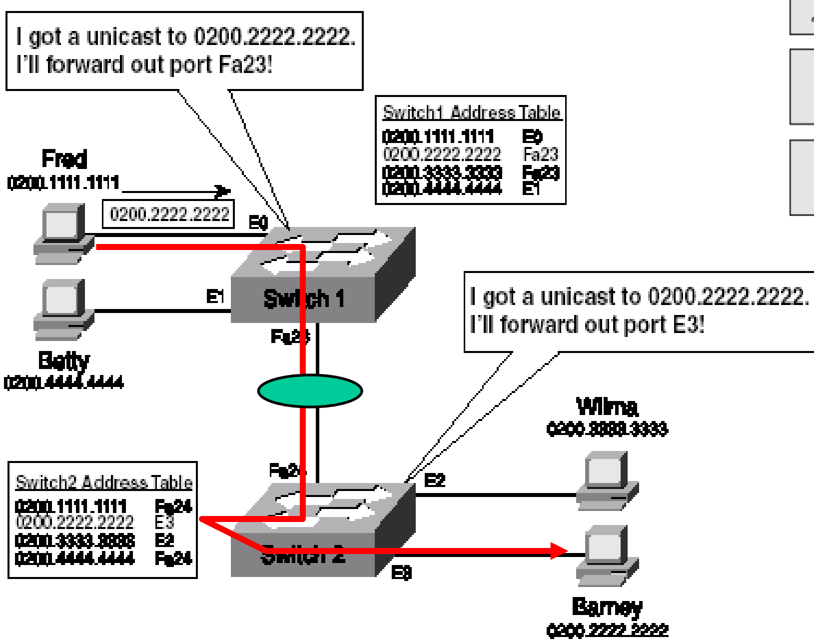
Figure 17.12: Two switches in a backbone using VLAN software



예) VLAN에서의 트렁킹

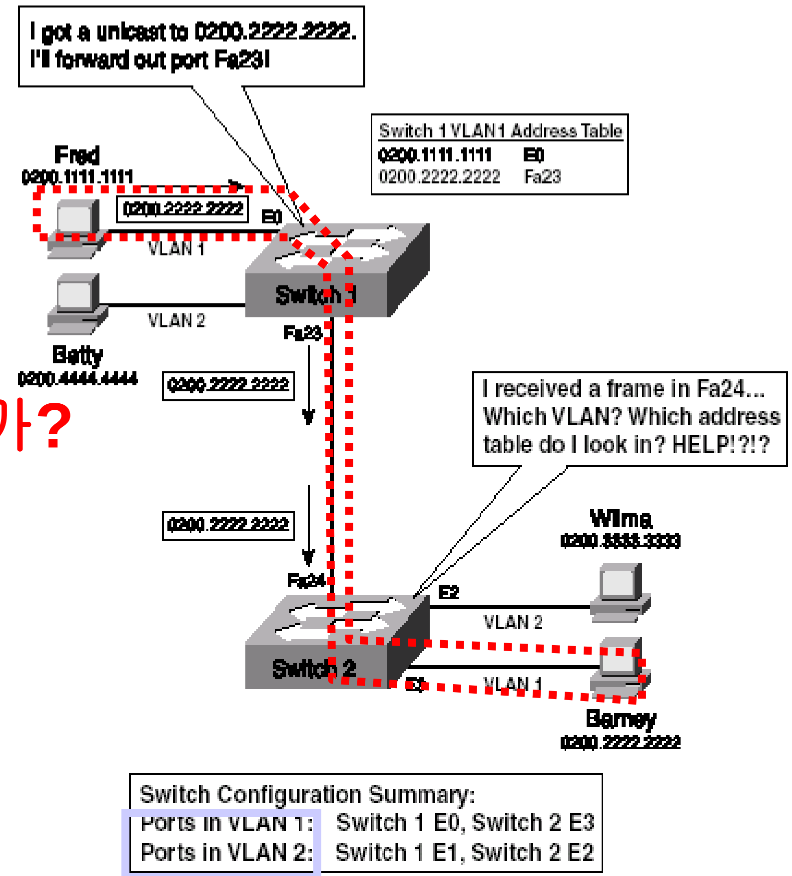
- 여러 개의 스위치를 이용한 LAN





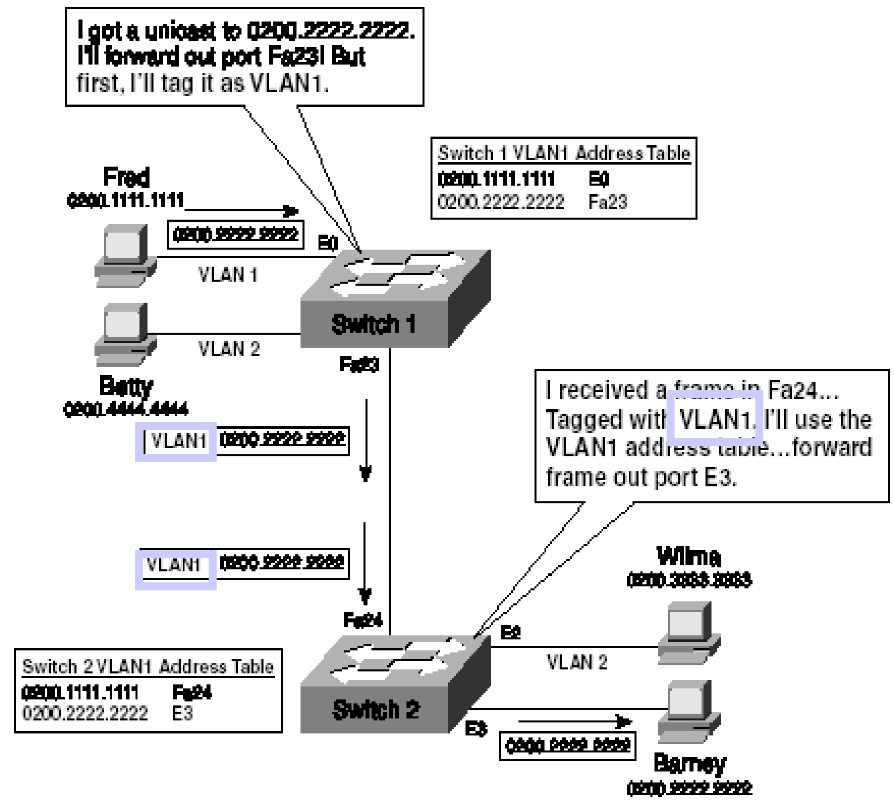
VLAN에서의 트렁킹

- 여러 개의 스위치를 사용한 **VLAN**의 구성
  - 스위치 **1**과 스위치 **2**사이의 케이블 조각 통과= 트렁킹
  - 트렁크를 통해 프레임을 수신할 경우
    - 스위치 2는 프레임 전달을 위해 두개의 테이블 검사
    - 특정 VLAN에 속한 것으로 가정
- 스위치 **2**의 딜레마: 어떤 **VLAN**인가?
  - 트렁크를 통해 수신한 프레임이 어느 **VLAN**인가 구분해야 함
  - 트렁킹의 경우 어느 **VLAN**에 속한 것인가를 구별하기 위한 **VLAN** 태그의 추가



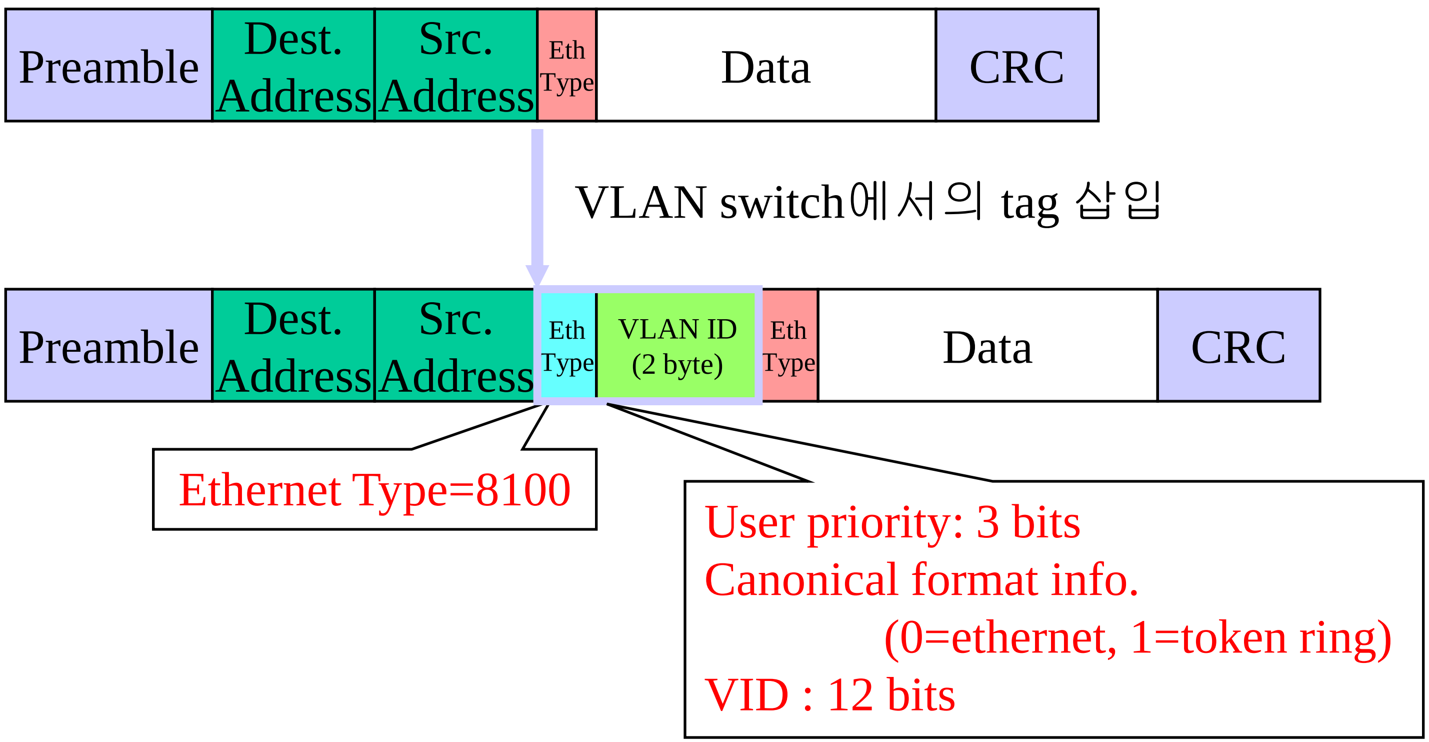
VLAN에서의 트렁킹 방법

- 트렁킹의 경우 어느 VLAN에 속한 것인가를 구별하기 위한 **VLAN**
  태그의 추가
  - 스위치 **2**는 수신된 프레임을
    어떻게 처리할지 알 수 있음
  - **VLAN** 트렁킹은 새로운
    표준 **(IEEE 802.1Q)**



VLAN에서의 태깅 방법

- **VLAN 을 위한 태그의 추가**
  - **VLAN ID 전송**
  - **MAC 주소형식 사용**
  - **Priority 정보 전달**



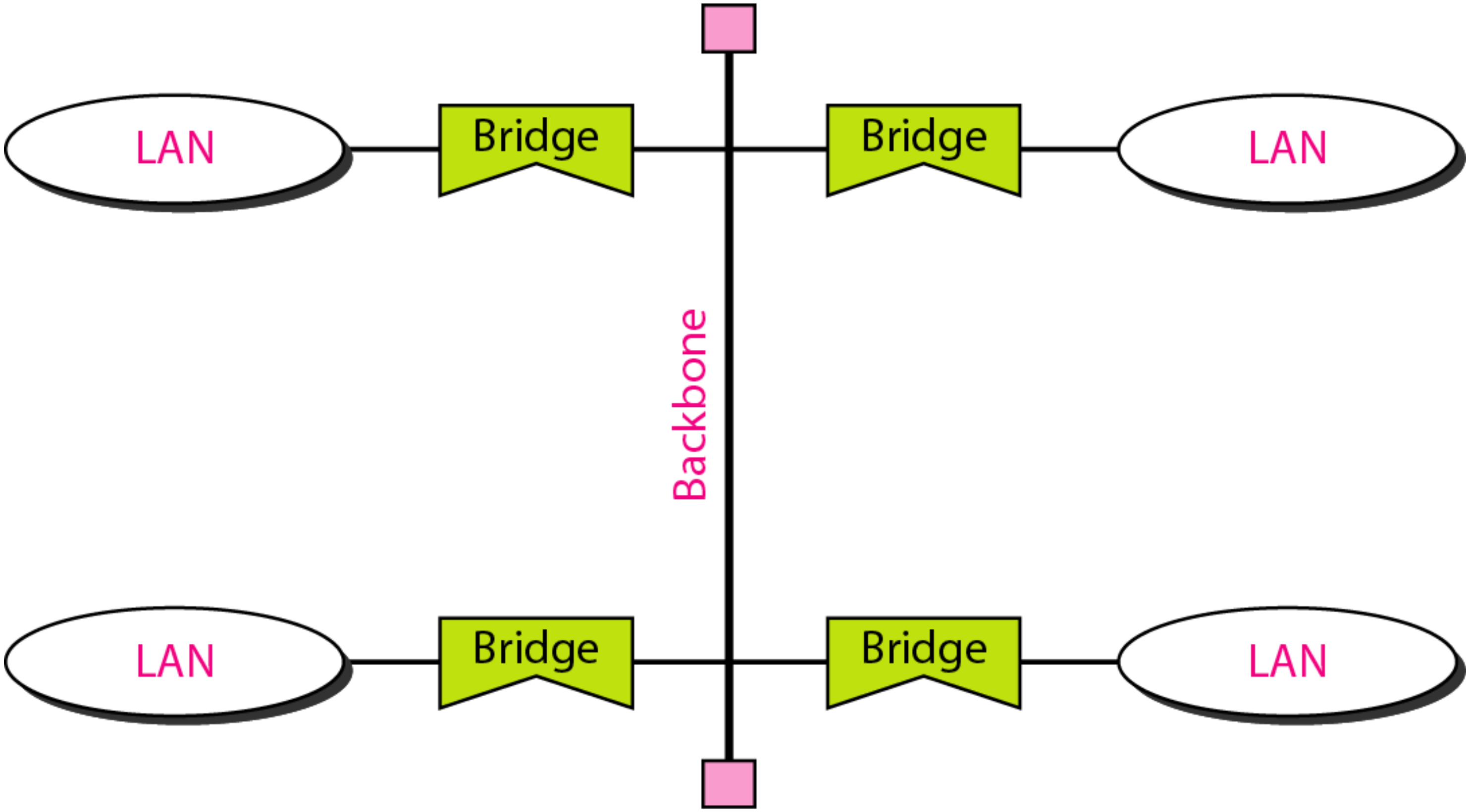
BACKBONE NETWORKS

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.

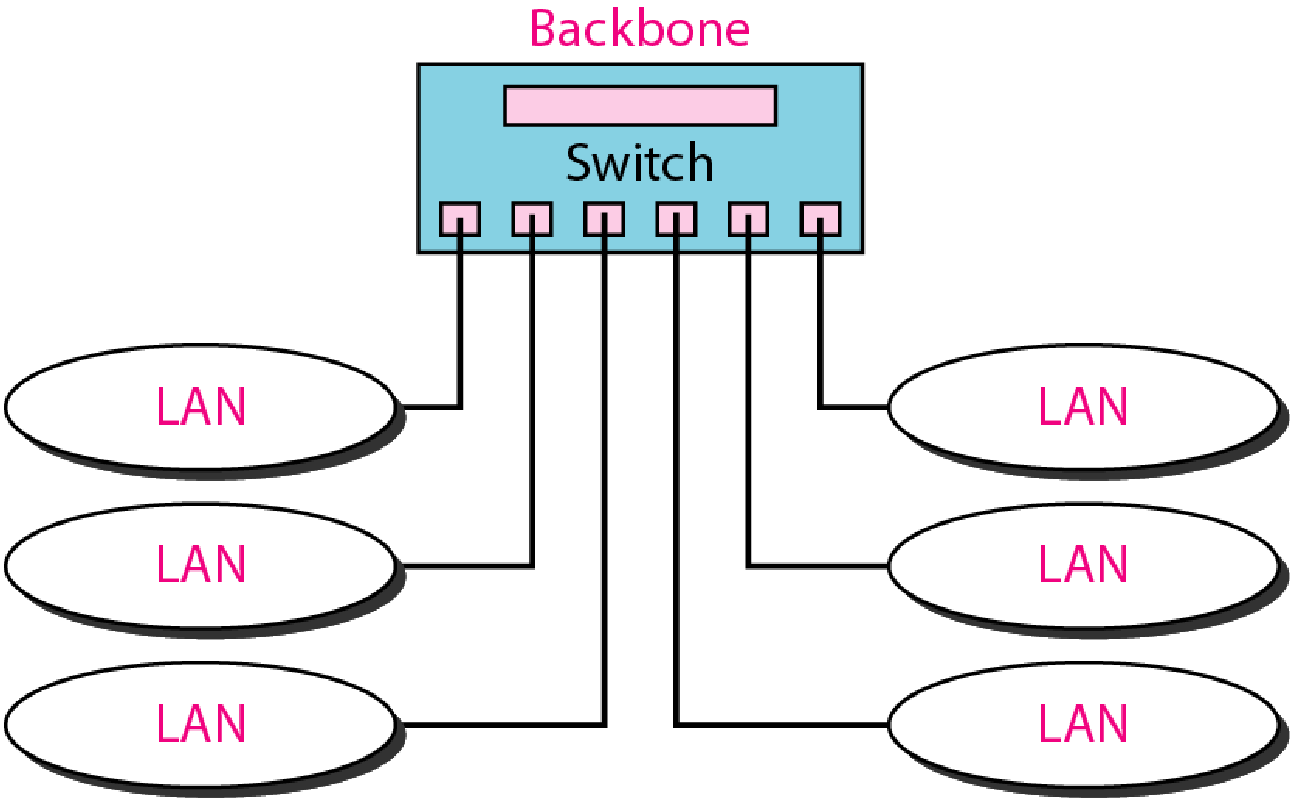
Topics discussed in this section:

Bus Backbone
Star Backbone
Connecting Remote LANs

In a bus backbone, the topology of the backbone is a bus.



In a star backbone, the topology of the backbone is a star; the backbone is just one switch.



A point-to-point link acts as a LAN in a remote backbone connected by remote bridges.