Lecture 7
Connecting LANs, Backbone Networks, and Virtual LANs

CONNECTING DEVICES

In this section, we divide connecting devices into five different categories based on the layer in which they operate in a network.

Passive Hubs
Active Hubs
Bridges
Two-Layer Switches
Routers
Three-Layer Switches
Gateways

Figure 15.1 *Five categories of connecting devices*

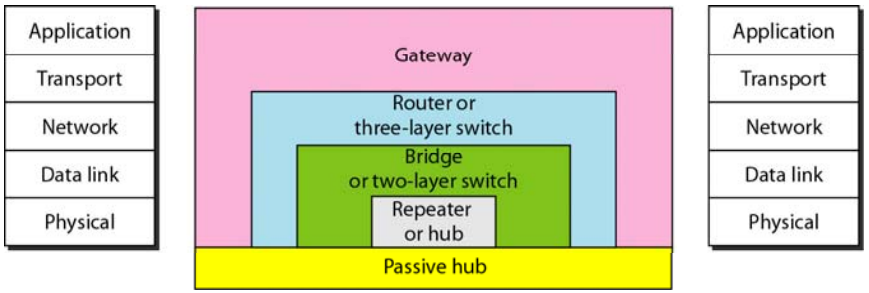
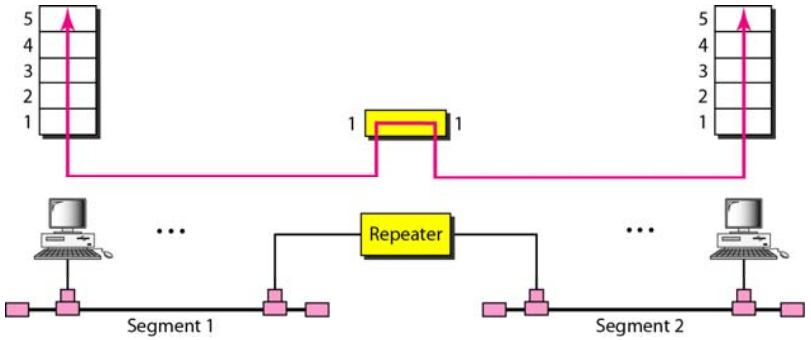


Figure 15.2 *A repeater connecting two segments of a LAN*



Note

A repeater connects segments of a LAN.

Note

A repeater forwards every frame;
it has no filtering capability.

Note

A repeater is a regenerator,
not an amplifier.

Figure 15.3 *Function of a repeater*

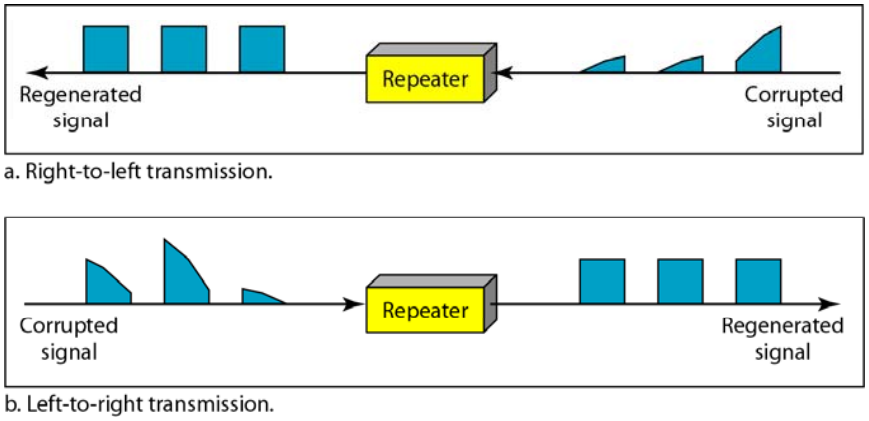
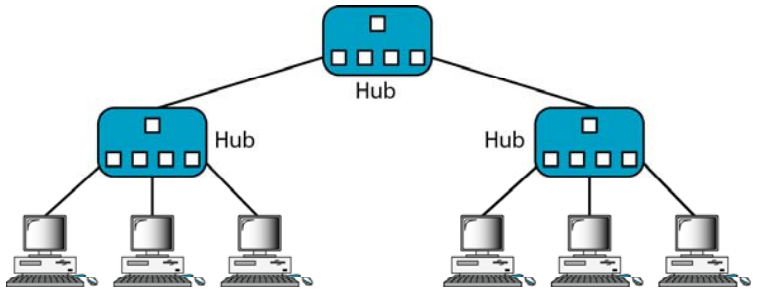


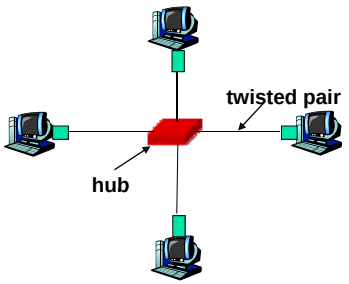
Figure 15.4 *A hierarchy of hubs*



Hubs

... physical-layer ("dumb") repeaters:

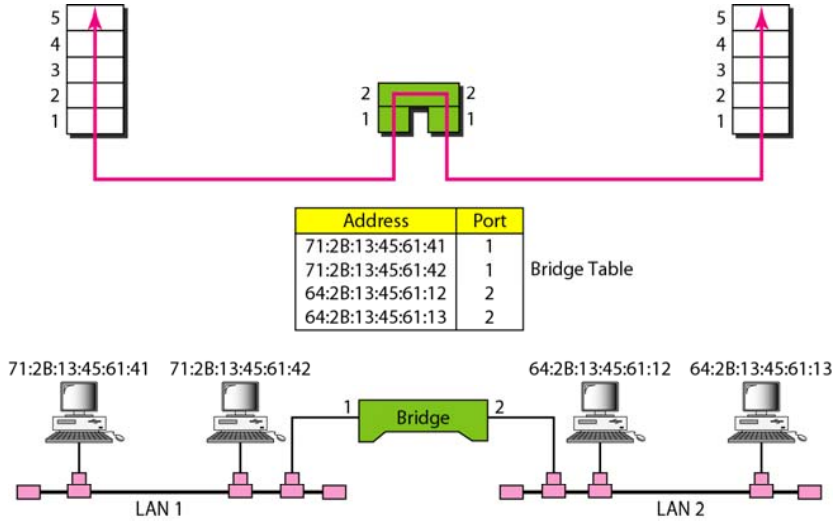
- bits coming in one link go out *all* other links at same rate
- all nodes connected to hub can collide with one another
- no frame buffering
- no CSMA/CD at hub: host NICs detect collisions



Note

A bridge has a table used in filtering decisions.

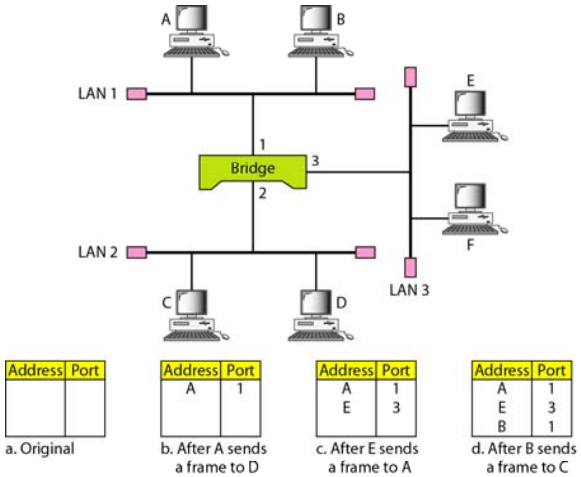
Figure 15.5 *A bridge connecting two LANs*



Note

A bridge does not change the physical (MAC) addresses in a frame.

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

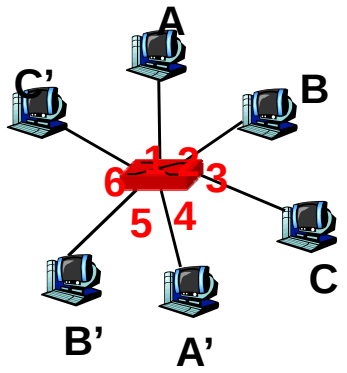


Switch

- link-layer device: smarter than hubs, take *active* role
  - store, forward Ethernet frames
  - examine incoming frame's MAC address, selectively forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
- *transparent*
  - hosts are unaware of presence of switches
- *plug-and-play, self-learning*
  - switches do not need to be configured

Switch: allows *multiple* simultaneous transmissions

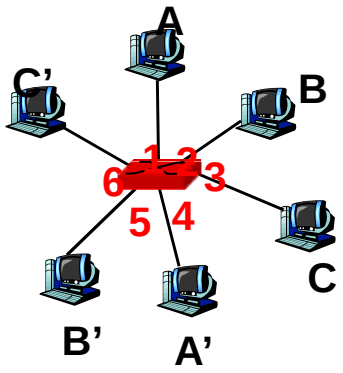
- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, but no collisions; full duplex
  - each link is its own collision domain
- *switching:* A-to-A' and B-to-B' simultaneously, without collisions
  - not possible with dumb hub



switch with six interfac (1,2,3,4,5,6)

Switch Table

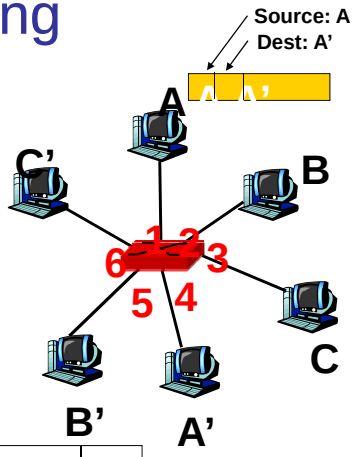
- *Q:* how does switch know that A' reachable via interface 4, B' reachable via interface 5?
- *A:* each switch has a switch table, each entry:
  - (MAC address of host, interface to reach host, time stamp)
- looks like a routing table!
- *Q:* how are entries created, maintained in switch table?
  - something like a routing protocol?



switch with six interfac (1,2,3,4,5,6)

Switch: self-learning

- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table



MAC addr	interface	TTL
A	1	60

Switch table (initially empty)

Switch: frame filtering/forwarding

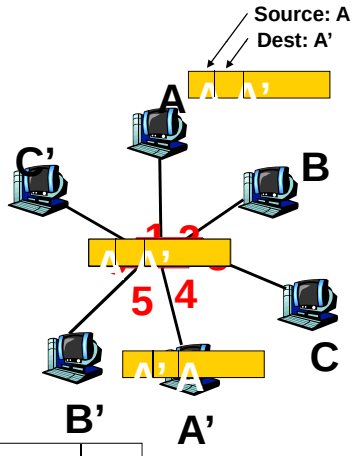
When frame received:

1. record link associated with sending host
2. index switch table using MAC dest address
3. **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

forward on all but the interface on which the frame arrived

Self-learning, forwarding: example

- frame destination unknown: **flood**
- **destination A location known: selective send**



MAC addr	interface	TTL
A	1	60
A'	4	60

Switch table (initially empty)

Figure 15.7 *Loop problem in a learning bridge*

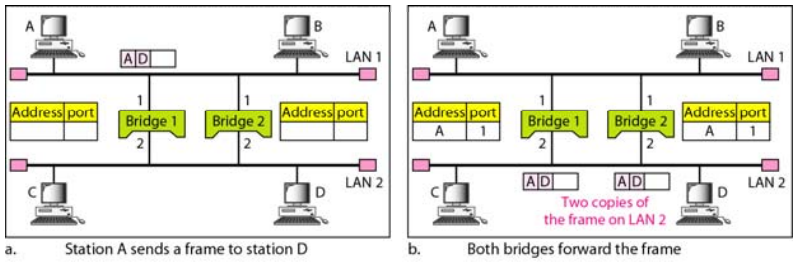


Figure 15.8 *A system of connected LANs and its graph representation*

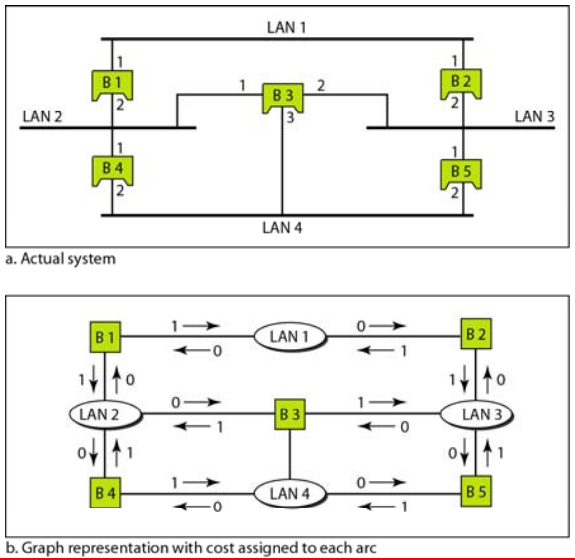


Figure 15.9 *Finding the shortest paths and the spanning tree in a system of bridges*

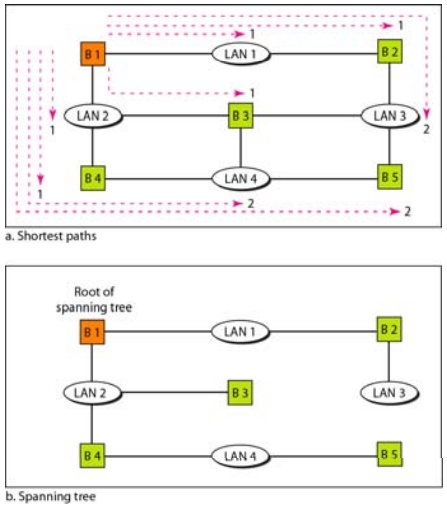
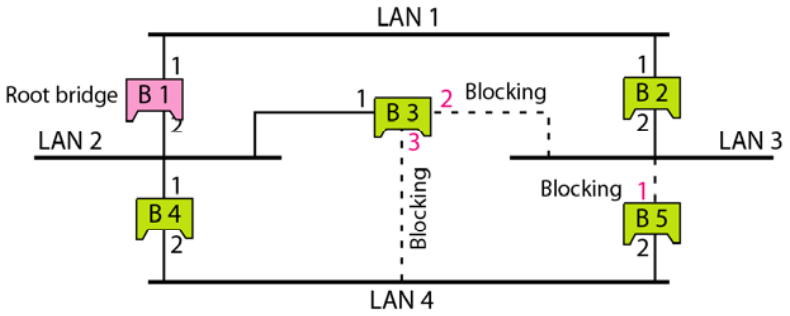


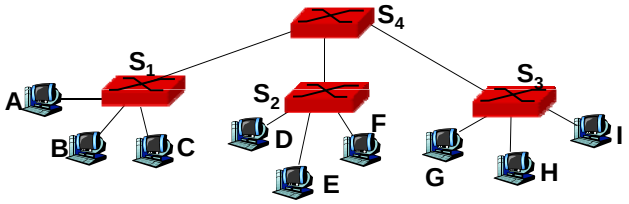
Figure 15.10 *Forwarding and blocking ports after using spanning tree algorithm*



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).

Interconnecting switches

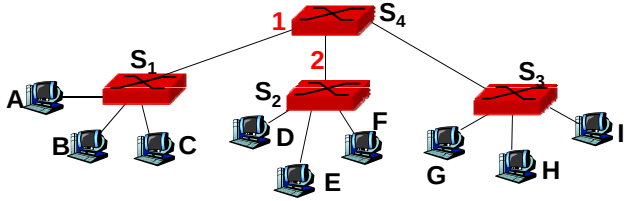
- switches can be connected together



- **Q: sending from A to G - how does S_1 know to forward frame destined to F via S_4 and S_3?**
- **A: self learning! (works exactly the same as in single-switch case!)**

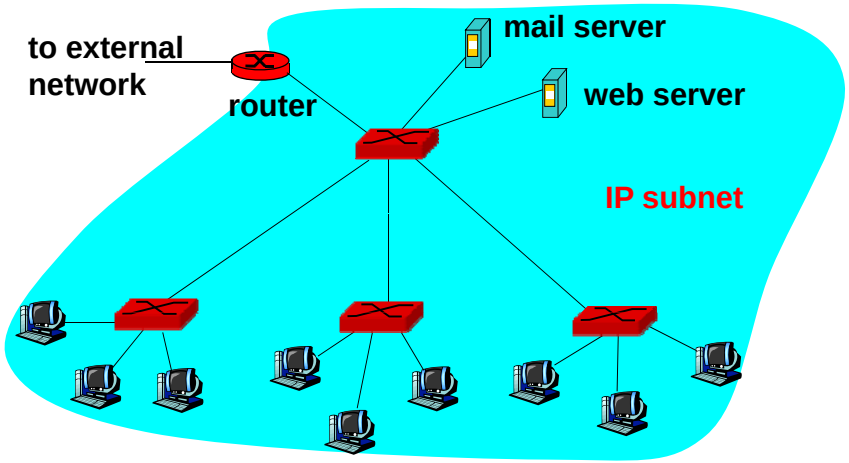
Self-learning multi-switch example

Suppose C sends frame to I, I responds to C



- **Q: show switch tables and packet forwarding in S_1, S_2, S_3, S_4**

Institutional network



Switches vs. Routers

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - switches are link layer devices
- routers maintain routing tables, implement routing algorithms
- switches maintain switch tables, implement filtering, learning algorithms

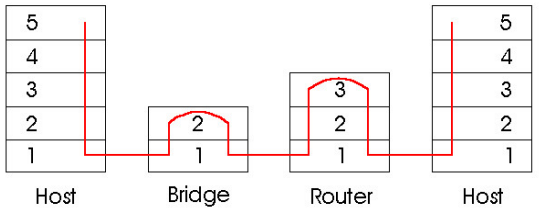
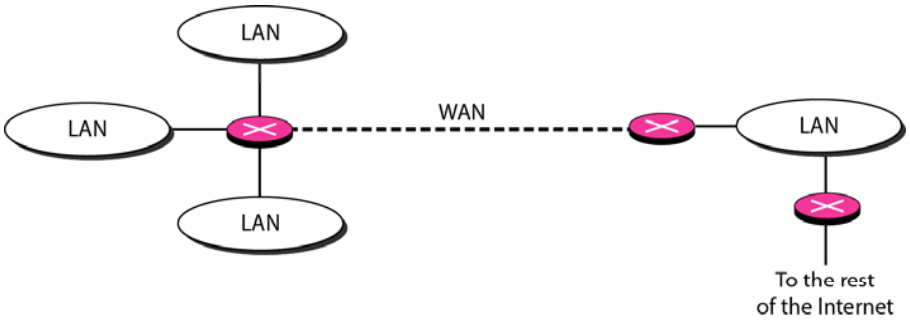


Figure 15.11 *Routers connecting independent LANs and WANs*



BACKBONE NETWORKS

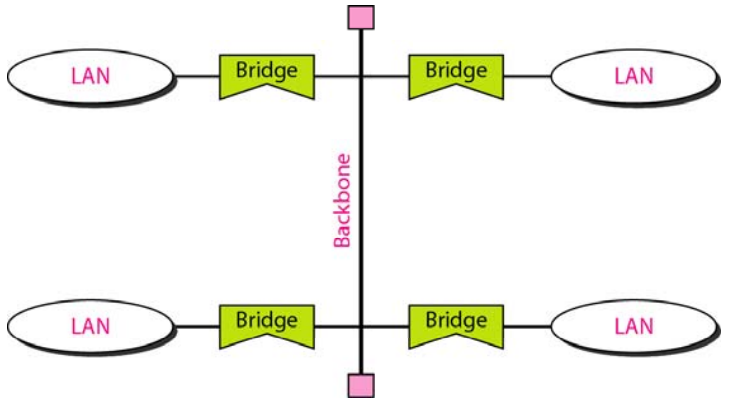
A backbone network allows several LANs to be connected. In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN, and the backbone connects the LANs.

Bus Backbone
Star Backbone
Connecting Remote LANs

Note

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

Figure 15.12 *Bus backbone*



Note

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

Figure 15.13 *Star backbone*

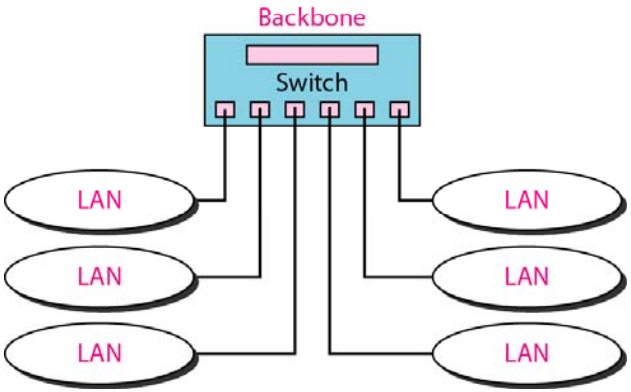
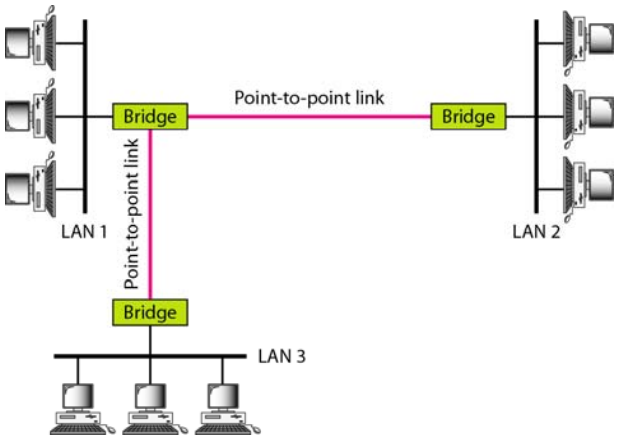


Figure 15.14 *Connecting remote LANs with bridges*



Note

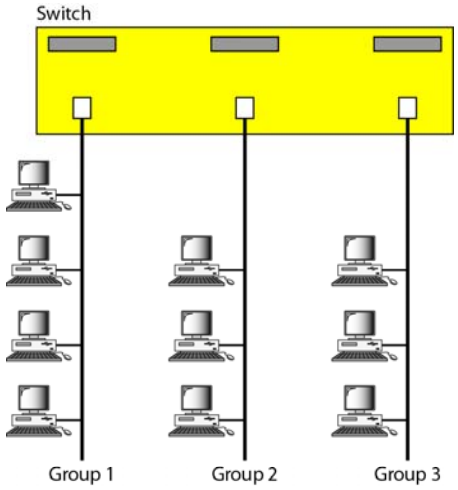
A point-to-point link acts as a LAN in a remote backbone connected by remote bridges.

VIRTUAL LANs

We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

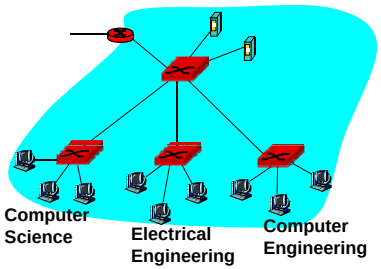
Membership
Configuration
Communication between Switches
IEEE Standard
Advantages

Figure 15.15 *A switch connecting three LANs*



VLANs: motivation

What's wrong with this picture?



What happens if:

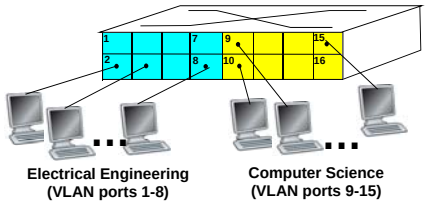
- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP) crosses entire LAN (security/privacy, efficiency issues)
- each lowest level switch has only few ports in use

VLANs

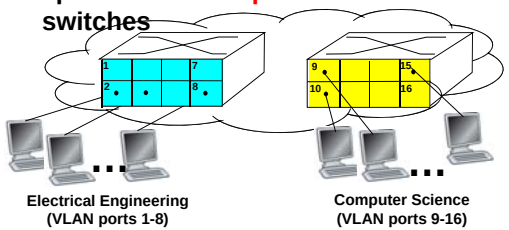
Virtual Local Area Network

Switch(es) supporting VLAN capabilities can be configured to define multiple virtual LANS over single physical LAN infrastructure.

Port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch .....

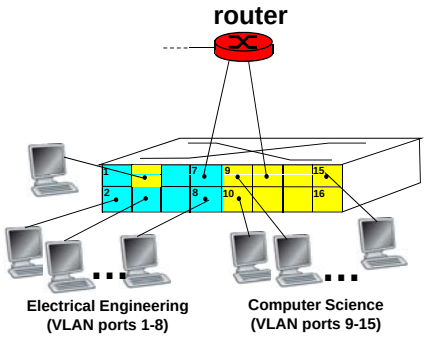


... operates as multiple virtual switches

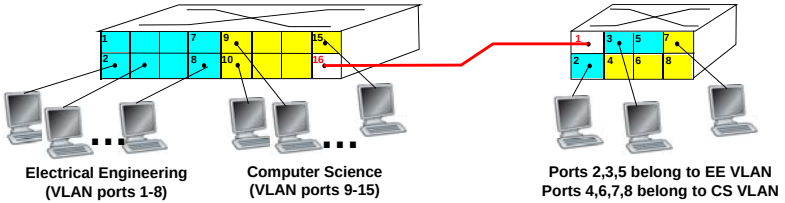


Port-based VLAN

- *traffic isolation:* frames to/from ports 1-8 can *only* reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- **dynamic membership: ports can be dynamically assigned among VLANs**
- **forwarding between VLANS: done via routing (just as with separate switches)**
  - **in practice vendors sell combined switches plus routers**



VLANS spanning multiple switches



- *trunk port:* carries frames between VLANS defined over multiple physical switches
  - frames forwarded within VLAN between switches can't be vanilla 802.1 frames (must carry VLAN ID info)
  - 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

Figure 15.16 *A switch using VLAN software*

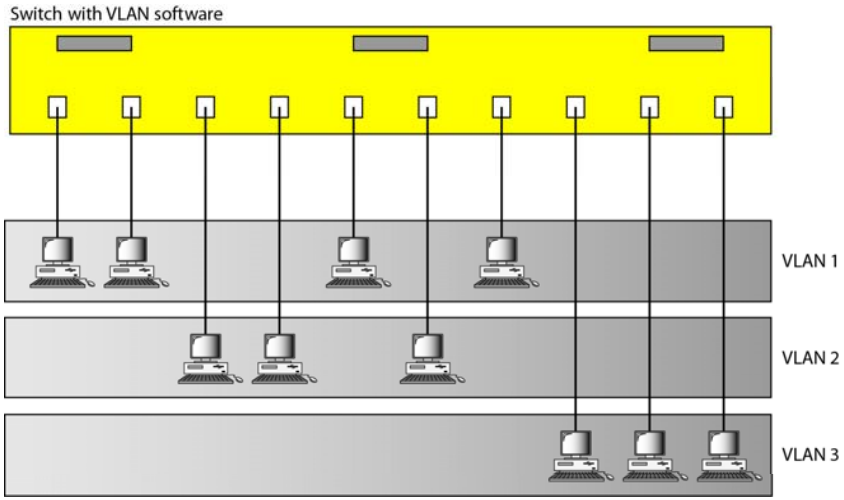
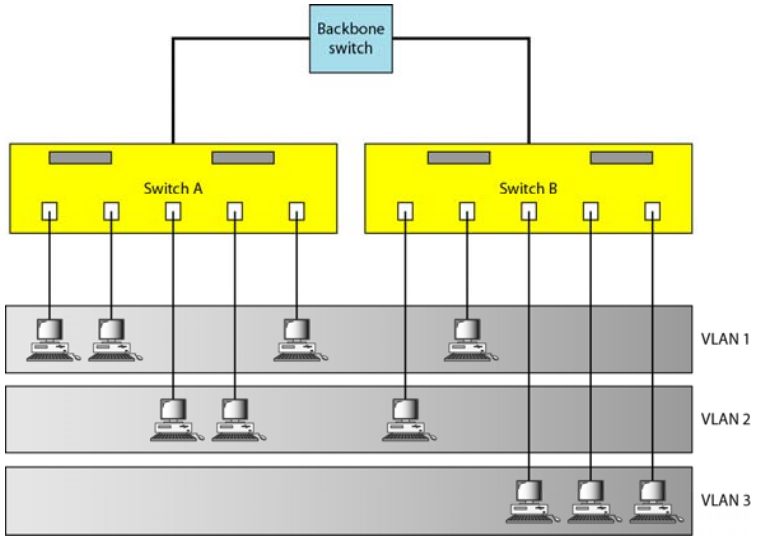


Figure 15.17 *Two switches in a backbone using VLAN software*



Note

VLANs create broadcast domains.