Link layer, LANs: outline

5.1 introduction, services

5.2 error detection, correction

5.3 multiple access protocols

5.4 LANs

- addressing, ARP
- Ethernet
- switches
- VLANS

5.5 link virtualization: MPLS

5.6 data center networking

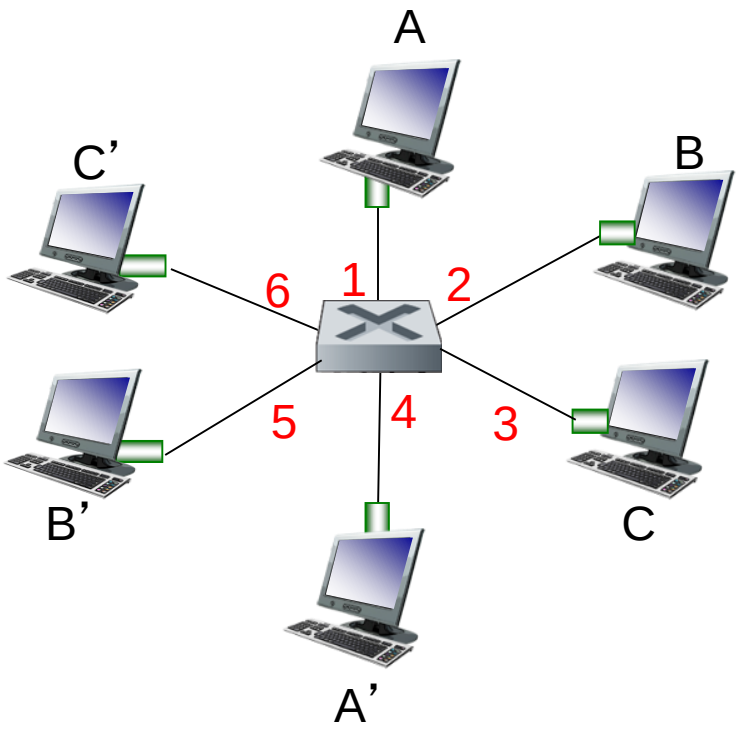
5.7 a day in the life of a web request

Ethernet switch

- link-layer device: takes an *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: *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 (more later)
  - each link is its own collision domain
- *switching:* A-to-A' and B-to-B' can transmit simultaneously, without collisions, either in the switch, or in the line.



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

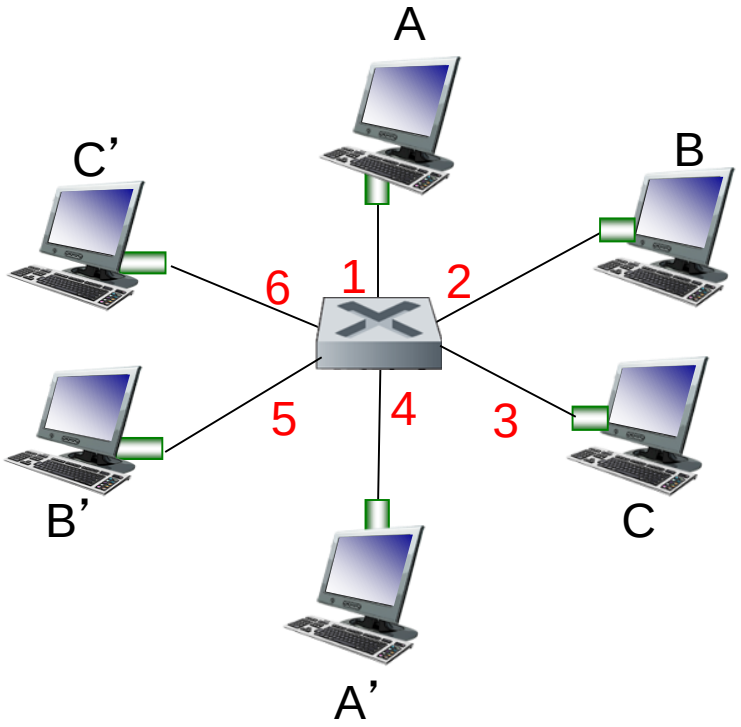
Switch forwarding table

Q: how does switch know 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?

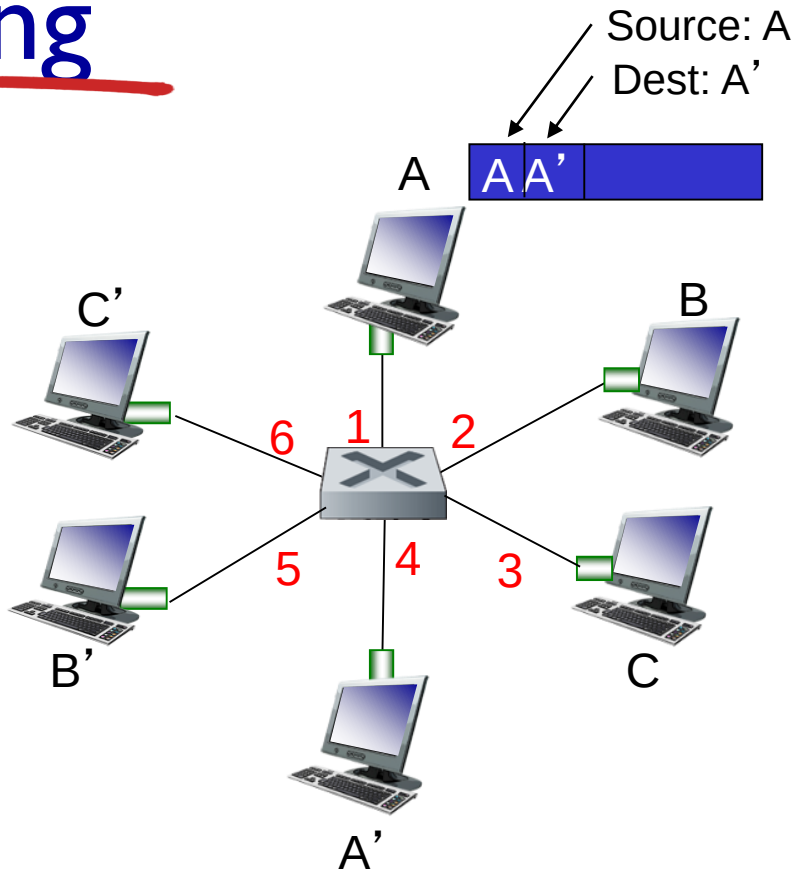
- *something like a routing protocol?*



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

Switch: self-learning

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



Remember: no ACKs when sending Ethernet frames!

MAC addr	interface	TTL
A	*1*	*60*

Switch table (initially empty)

Switch: frame filtering/forwarding

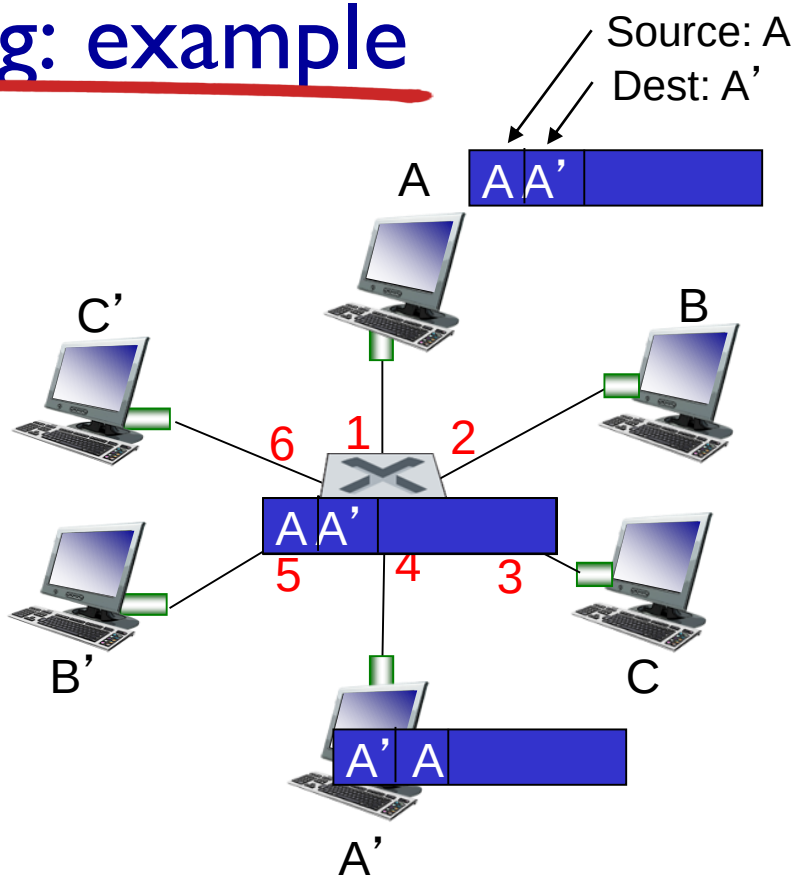
when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination, then

```
{
    if destination on segment from which frame arrived
        then drop frame
    else
        forward frame on interface indicated by entry
}
else flood  // forward on all interfaces except arriving one
```

Self-learning, forwarding: example

- frame destination, A', locaton unknown: *flood*
- destination A location known: *selectively send on just one link*

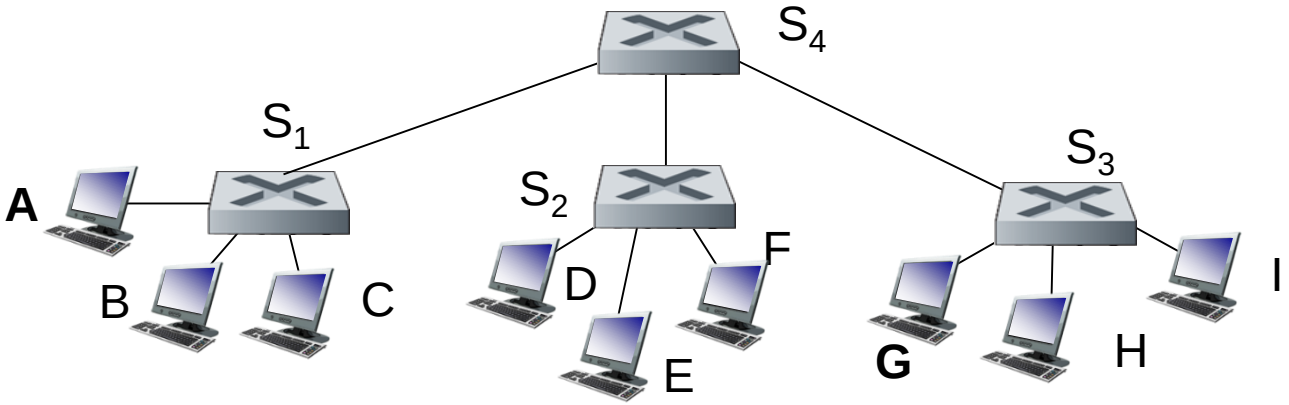


MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

Interconnecting switches

- switches can be connected together

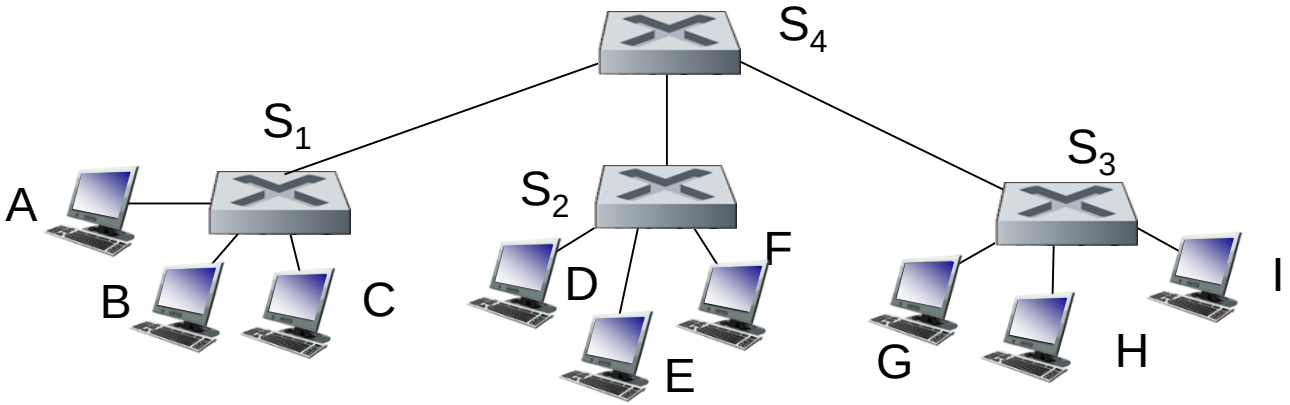


Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

- A: self learning! (works *exactly* the same as in single-switch case!)

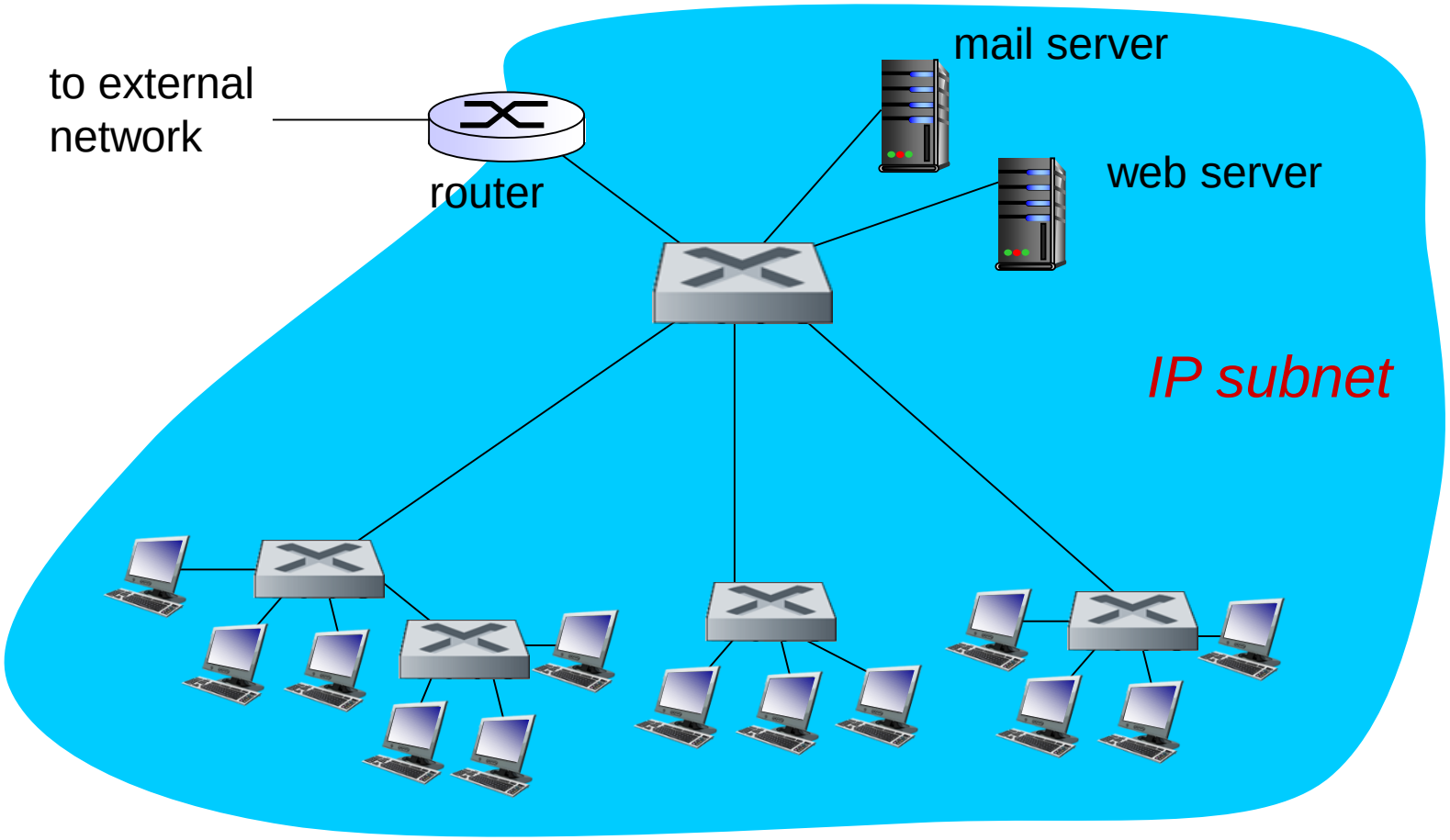
Self-learning multi-switch example

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



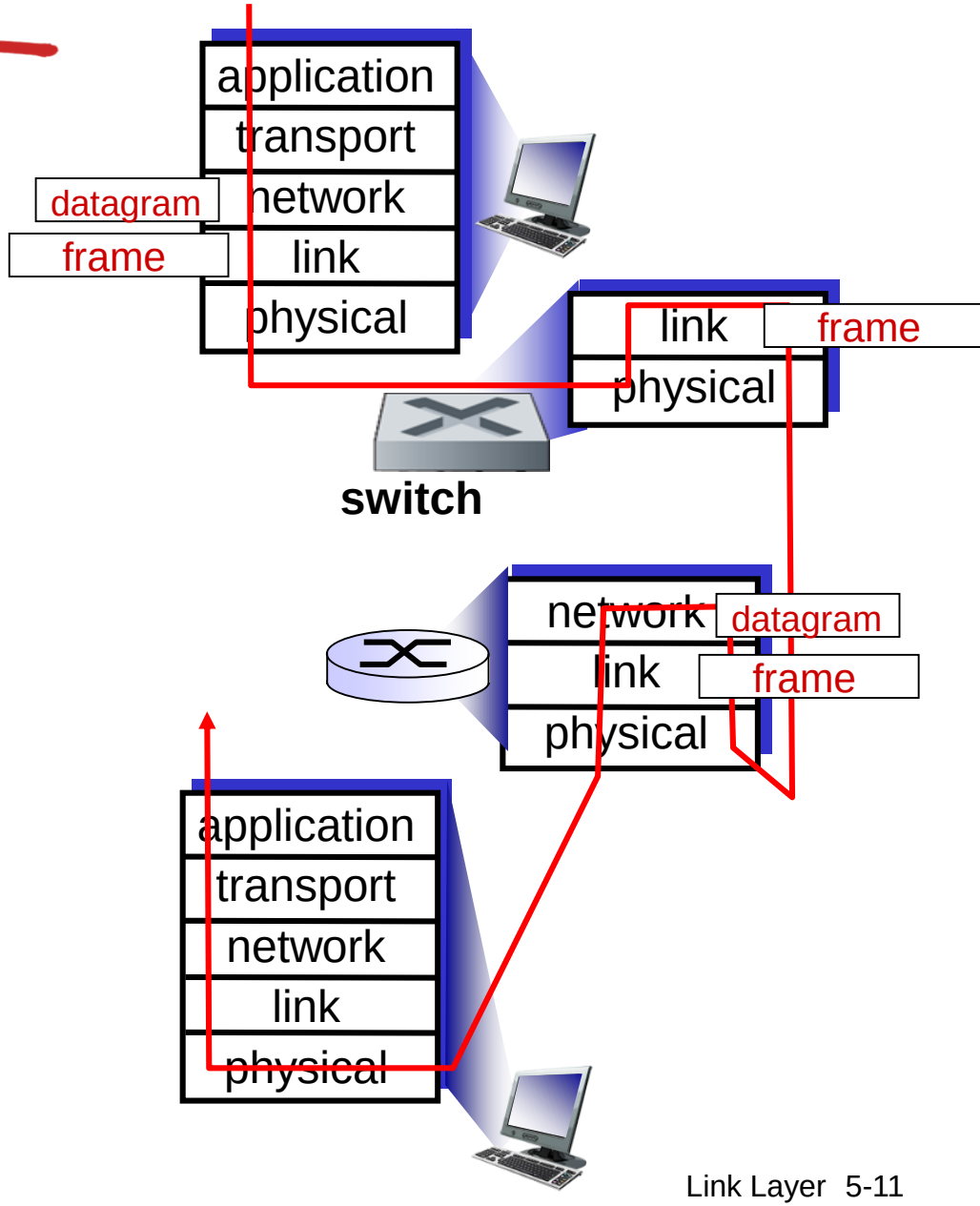
Switches vs. routers

both are store-and-forward:

- *routers:* network-layer devices (examine network-layer headers)
- *switches*: link-layer devices (examine link-layer headers)

both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses

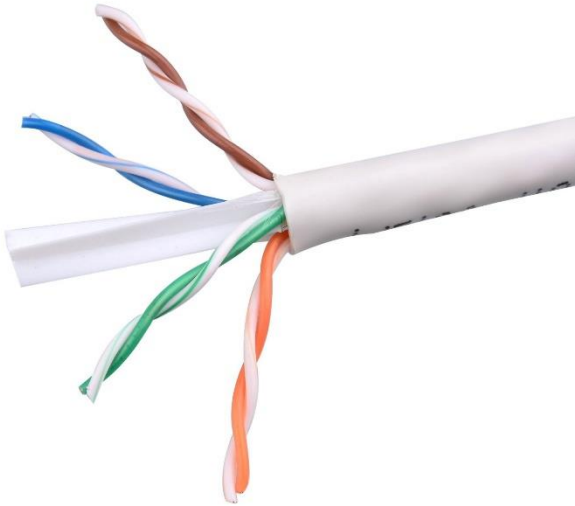


Collisions and MAC Protocols

- Remember that MAC protocols involve both controlling multiple access needs and addressing

- Why use MAC protocols with a switch?
  - How many devices are communicating on each "link"?
  - Are collisions possible on a link?
  - Are they full duplex?

  - 2
  - No, because 2 wires are used for each node out of 8 in the cable (so 4 total)
  - Yes, because collisions aren't possible!

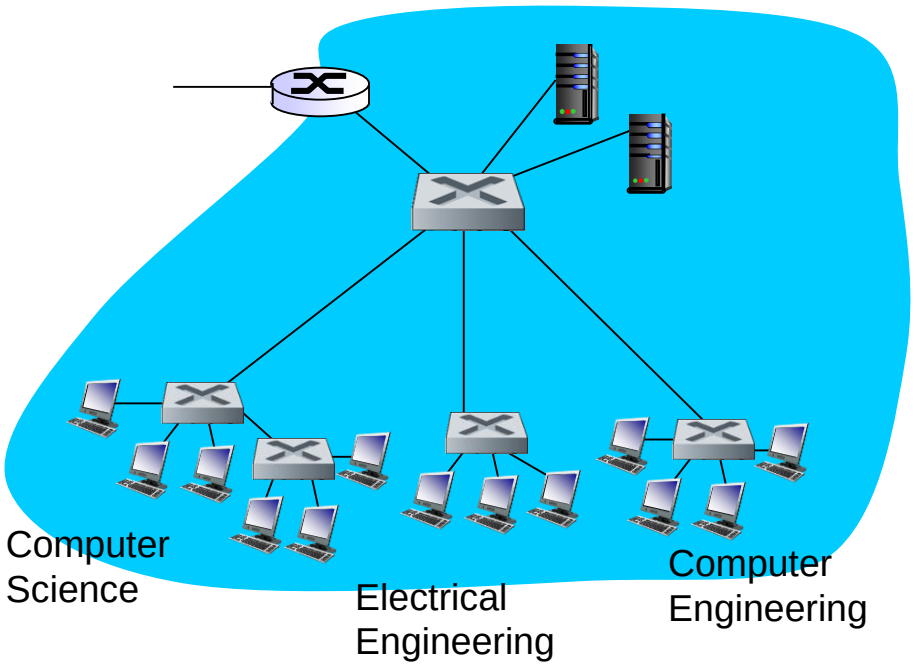


http://www.securitymayor.com/imgcatalog/Security-Mayor-Cable-Matters-Cat6-Ethernet-Cable-D.jpg

Collisions and MAC Protocols

- Why use MAC protocols with a switch?
  - Not necessary!
  - But, the frame format hasn't changed, and the protocol works equally well with wired as well as wireless

VLANs: motivation



consider:

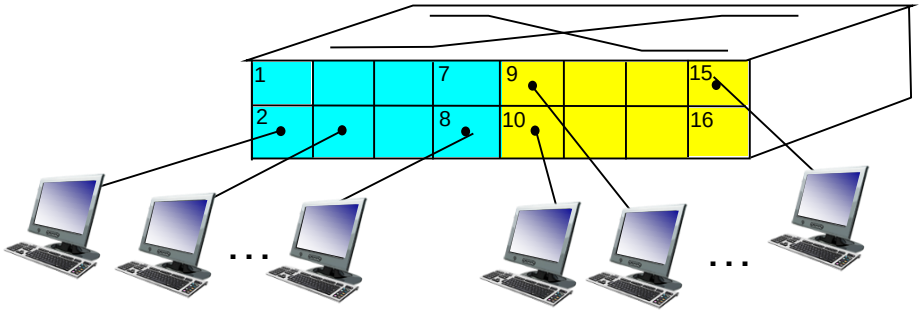
- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
  - security/privacy, efficiency issues

VLANs

Virtual Local Area Network

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

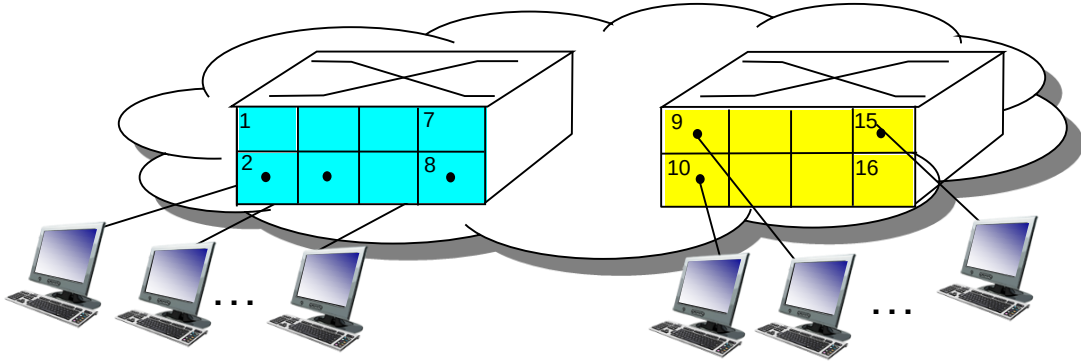
port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-15)

… operates as *multiple* virtual switches

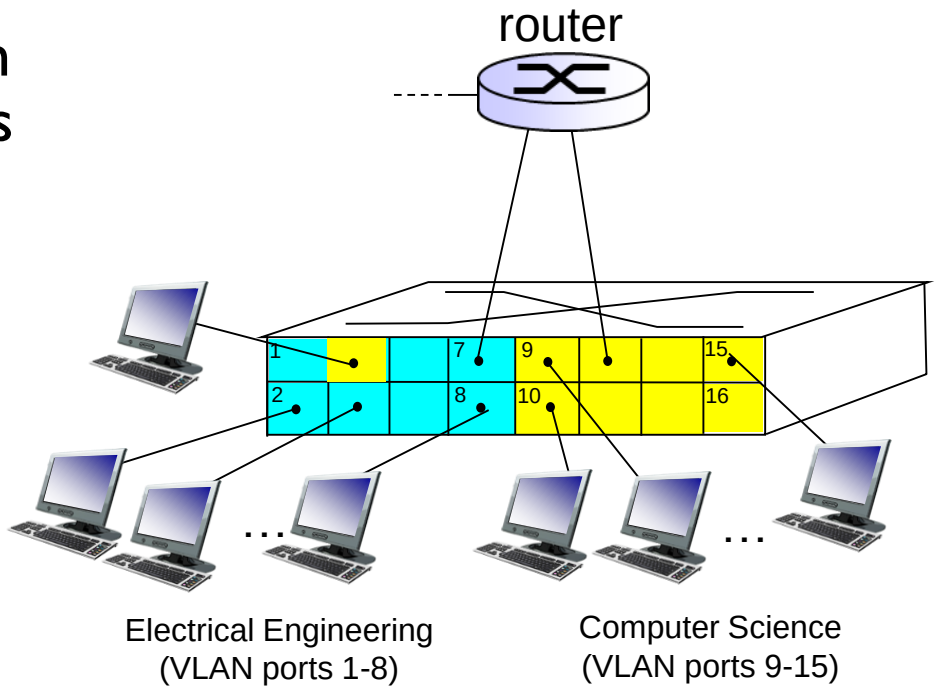


Electrical Engineering (VLAN ports 1-8)

Computer Science (VLAN ports 9-16)

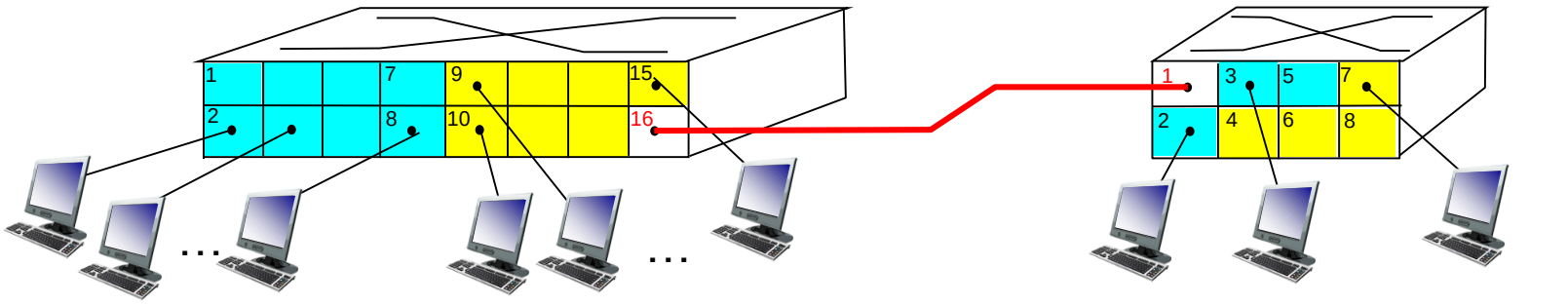
Port-based VLAN

- *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



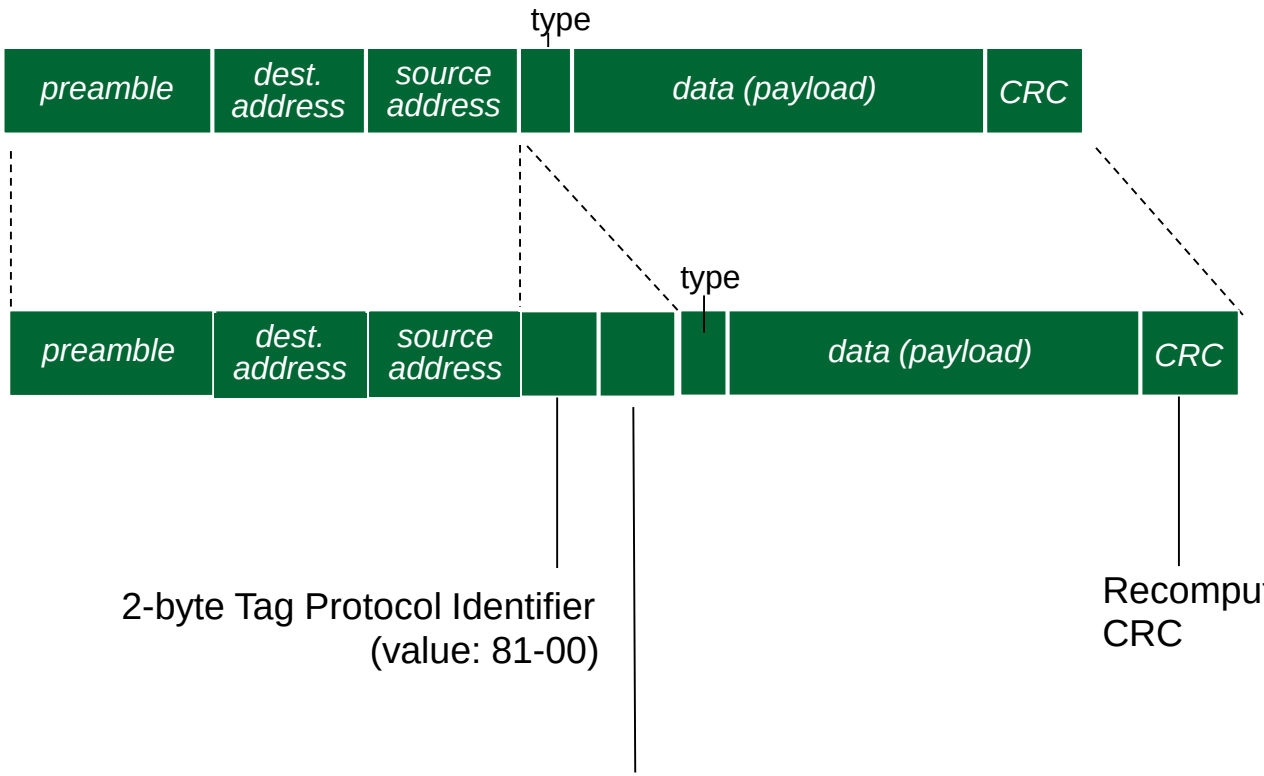
- *forwarding between VLANS:* done via routing (just as with separate switches)
  - in practice vendors sell combined switches+routers

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/removes additional header fields for frames forwarded between trunk ports
  - Behavior of non-VLAN-aware switches when receiving VLAN tagged frames is undefined(!), and could include dropping, forwarding as-is, forwarding with tag removed (i.e. no longer "secure"), forwarding mangled packets, or crashing!

802.1q VLAN frame format



Note the shifted field locations: this is what can cause mangled packets, etc.! How well does your switch or router handle a mangled packet?

Link layer, LANs: outline

5.1 introduction, services

5.2 error detection, correction

5.3 multiple access protocols

5.4 LANs

- addressing, ARP
- Ethernet
- switches
- VLANS

5.5 link virtualization: MPLS

5.6 data center networking

5.7 a day in the life of a web request