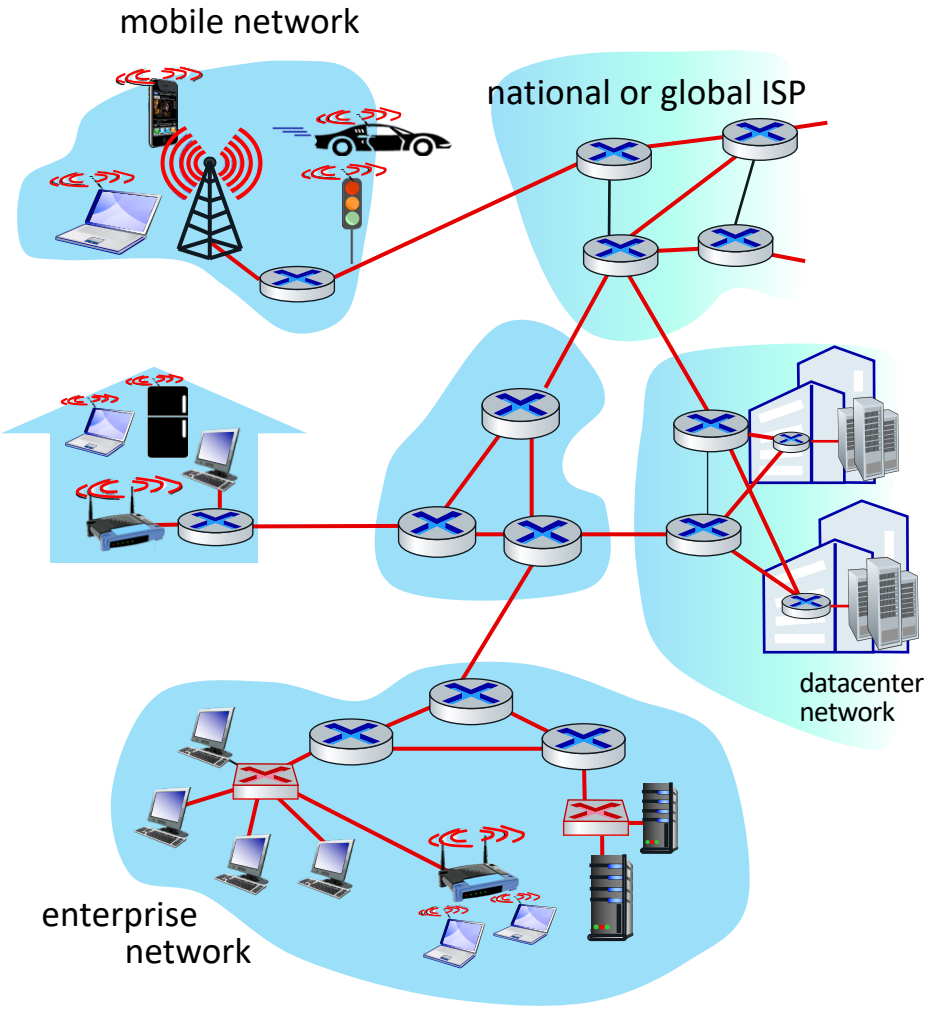
Link Layer Introduction

Link Layer: Introduction

terminology:

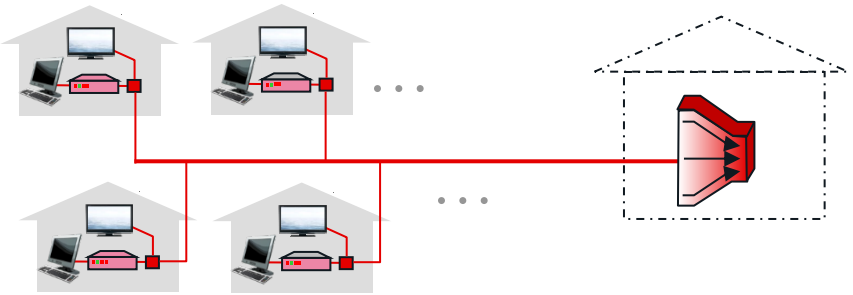
- hosts and routers: nodes
- communication channels that connect adjacent nodes along communication path: links
  - wired
  - wireless
  - LANs
- layer-2 packet: *frame*, encapsulates datagram

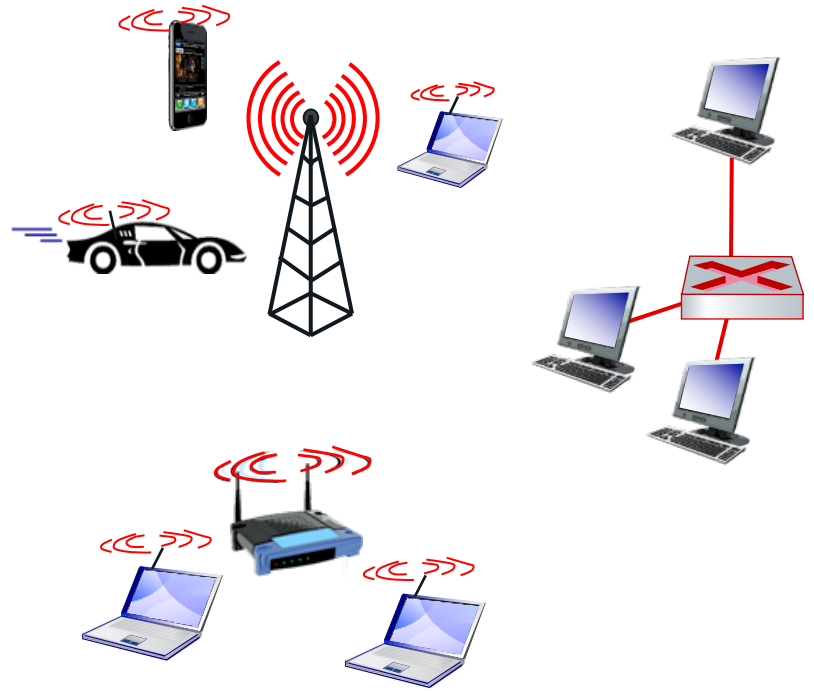
link layer has responsibility of transferring datagram from one node to physically adjacent node over a link



Link Layer: Service

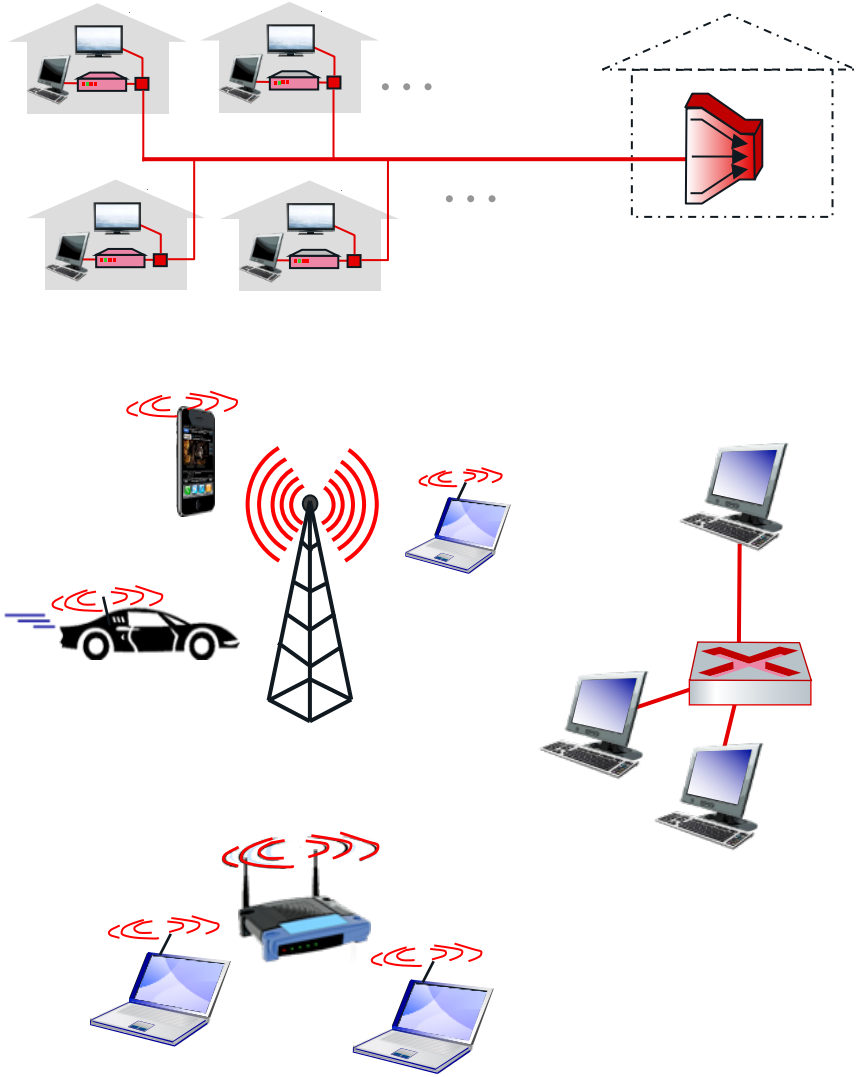
- datagram transferred by different link protocols over different links:
  - e.g., WiFi on first link, Ethernet on next link
- framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - "MAC" addresses in frame headers identify source, destination (different from IP address!)





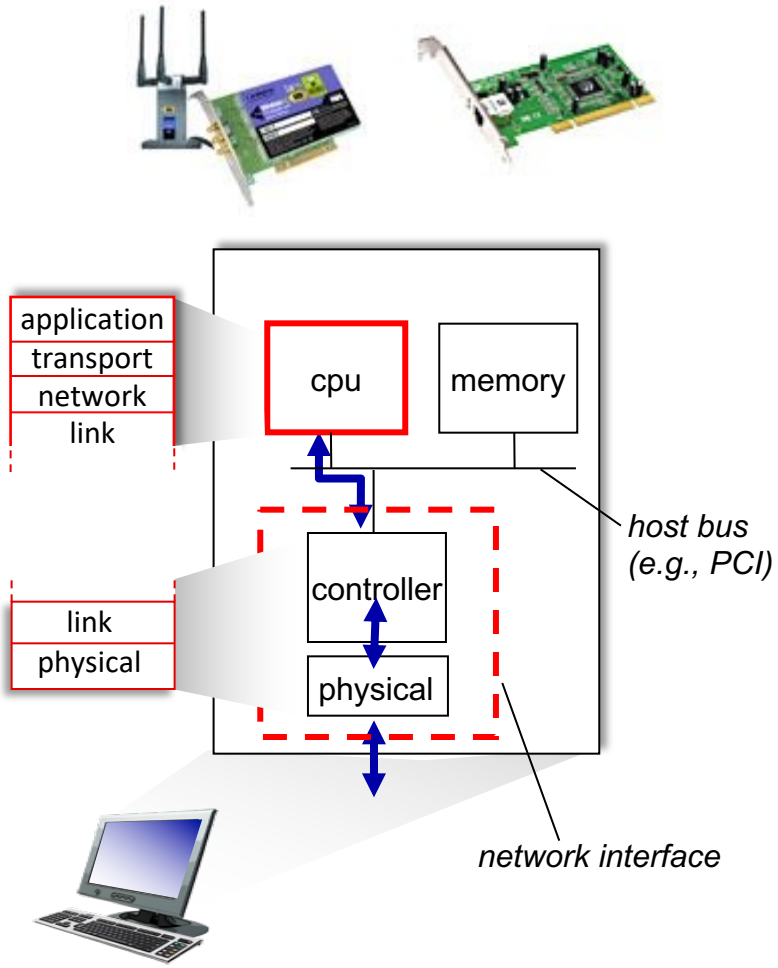
Link Layer: Service

- flow control:
  - pacing between adjacent sending and receiving nodes
- error detection:
  - errors caused by signal attenuation, noise.
  - receiver detects errors, signals retransmission, or drops frame
- error correction:
  - receiver identifies *and corrects* bit error(s) without retransmission
- half-duplex and full-duplex:
  - with half duplex, nodes at both ends of link can transmit, but not at same time

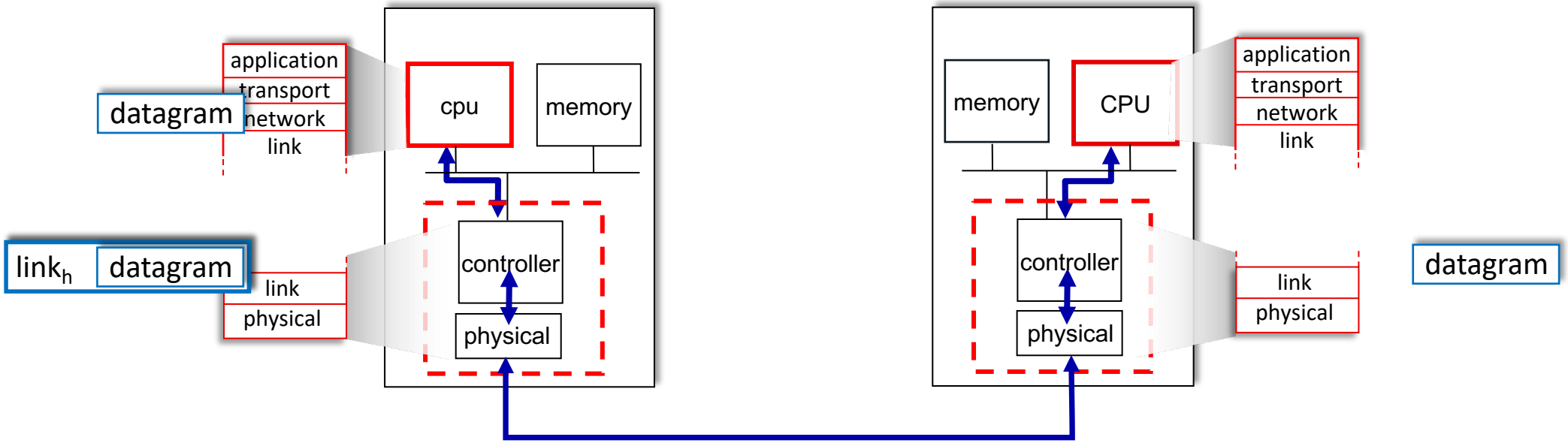


Where is the link layer implemented?

- in each-and-every host
- link layer implemented in *network interface card* (NIC) or on a chip
  - Ethernet, WiFi card or chip
  - implements link, physical layer
- attaches into host's system buses
- combination of hardware, software, firmware



Interfaces Communicating



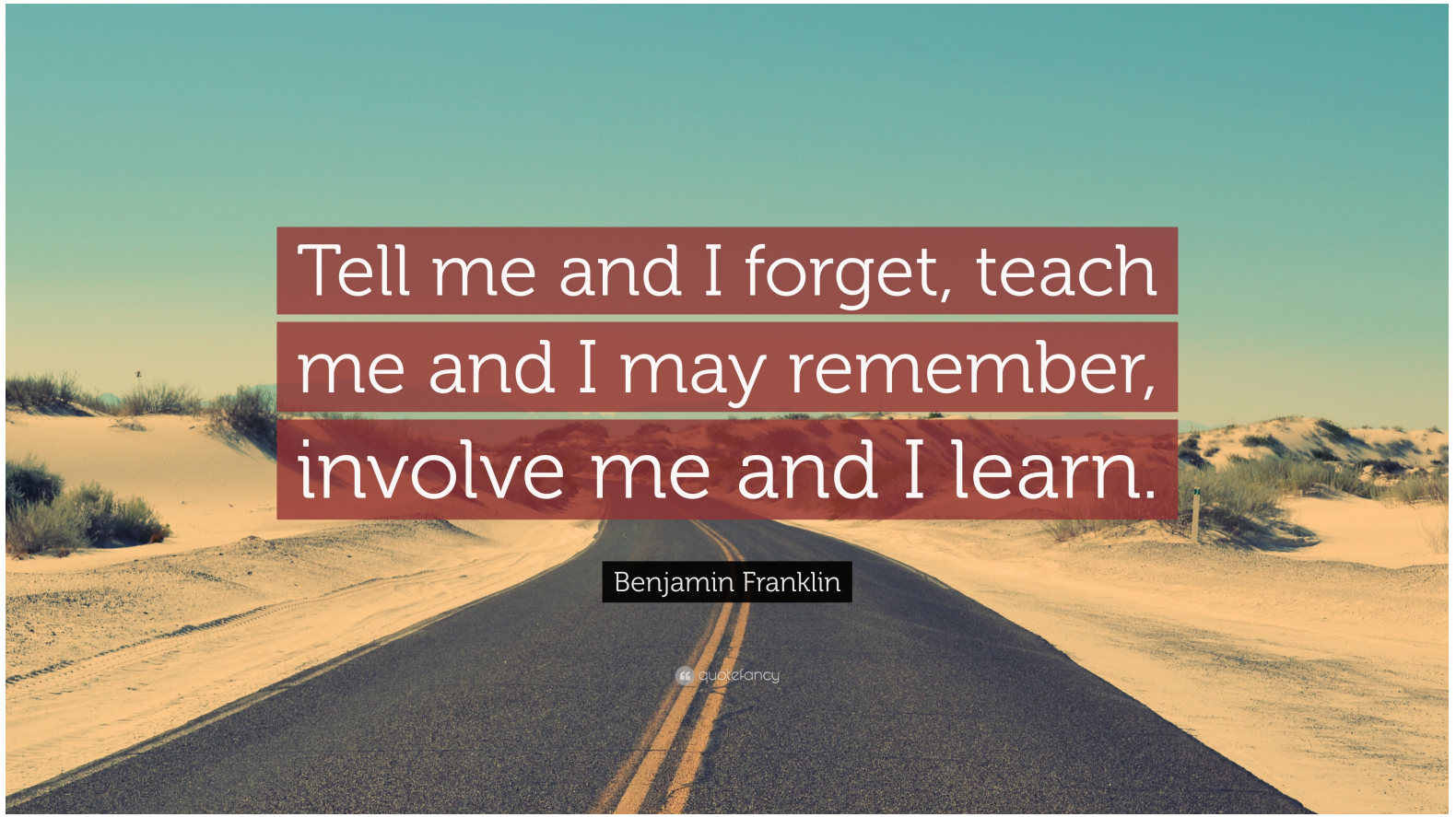
sending side:

- encapsulates datagram in frame
- adds error checking bits, reliable data transfer, flow control, etc.

receiving side:

- looks for errors, reliable data transfer, flow control, etc.
- extracts datagram, passes to upper layer at receiving side

Thank You!

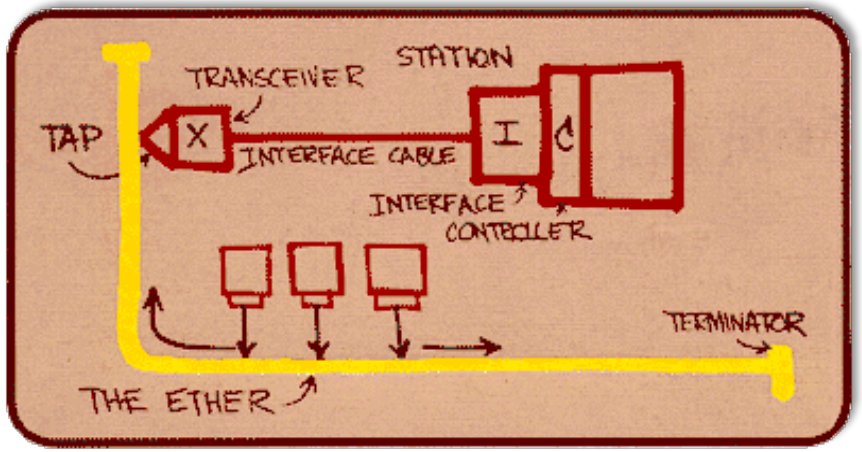

Tell me and I forget, teach
me and I may remember,
involve me and I learn.
Benjamin Franklin
quotefancy

Ethernet

Ethernet

"dominant" wired LAN technology:

- first widely used LAN technology
- simpler, cheap
- kept up with speed race: 10 Mbps – 400 Gbps
- single chip, multiple speeds

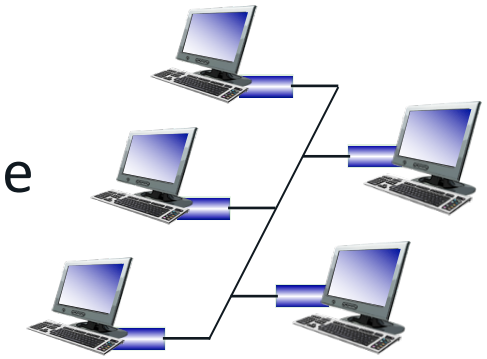


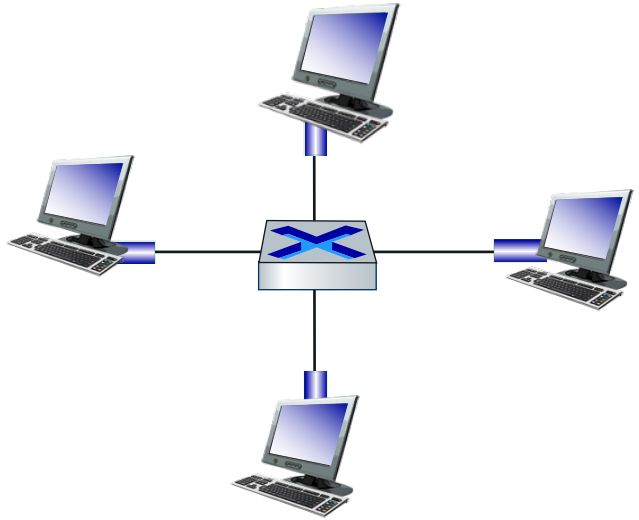
Metcalfe's Ethernet sketch

Ethernet: Physical Topology

- bus: popular through mid 90s
  - all nodes in same collision domain (can collide with each other)
- switched: prevails today
  - active link-layer 2 *switch* in center
  - each “spoke” runs a (separate) Ethernet protocol (nodes do not collide with each other)

bus: coaxial cable



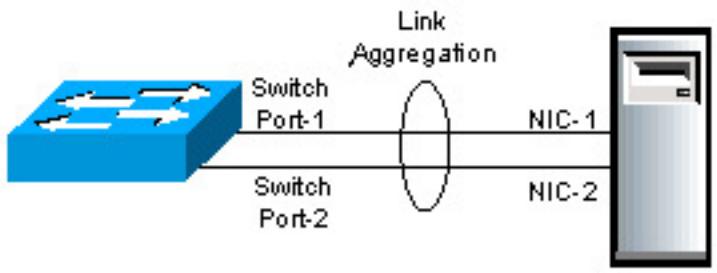


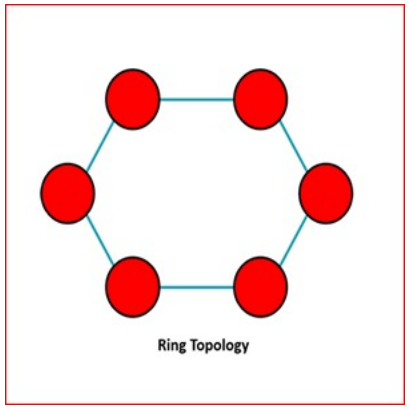
switched

Ethernet Redundancy

Two types of redundancy

- Link redundancy on full-duplex connections
  - Multiple links between two devices via link aggregation (LAG)
  - Logical bundling to provide failover for one or more links
- Redundant topology
  - Multiple paths to reach the same destination
  - Provides protection for path failures where ports/devices fail





Link Redundancy - LAG

Based on IEEE 802.3ad standard

- Benefits
  - increased performance by providing incremental bandwidth between two devices
  - increased resiliency by providing automatic, point-to-point redundancy between two devices if one or more links in the LAG should fail
- Statically configured or formed dynamically with LACP
- Failover time less than one second

Redundant Topology

Redundancy

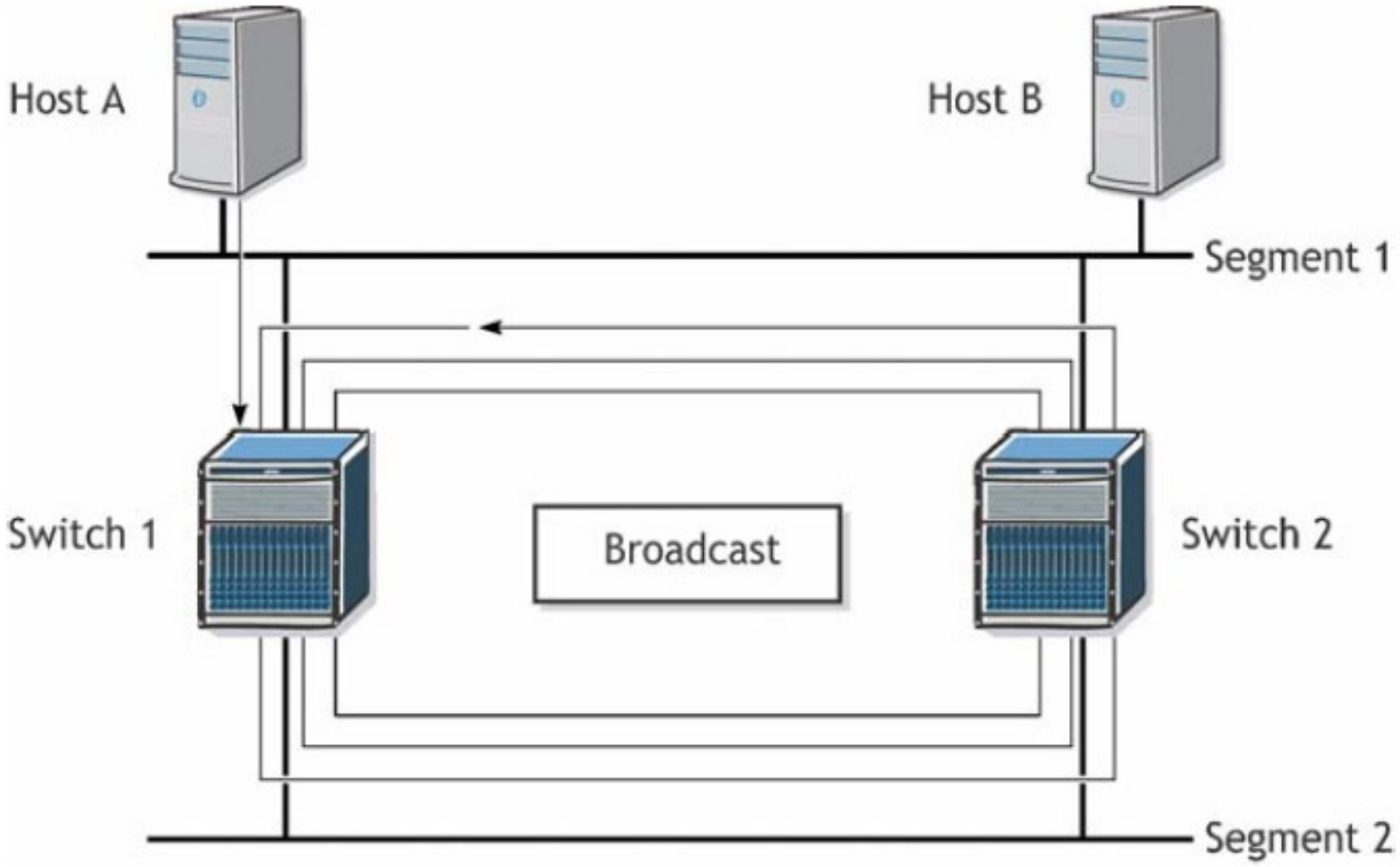
- Advantages
  - Protection when an entire switch fails, rather than just link protection
  - Load balancing across switches rather than just across links of the same switch
- Disadvantages
  - May cause broadcast storms if not designed correctly
  - May cause forwarding table instability
- Frame looping problems
  - Layer 2 has no mechanism to stop looping as Layer 3 has with TTL

Broadcast Storms (Looping)

Networks that are designed with redundancy and no Spanning Tree Protocol (STP) are vulnerable to broadcast storms because as the switch receives multiple copies of a frame, it further replicates each frame and transmits them out one or more ports on the switch.

Because of the Layer 2 loop, the transmitted frames are received back and replicated again. This results in an exponential increase in Layer 2 traffic in the looped network.

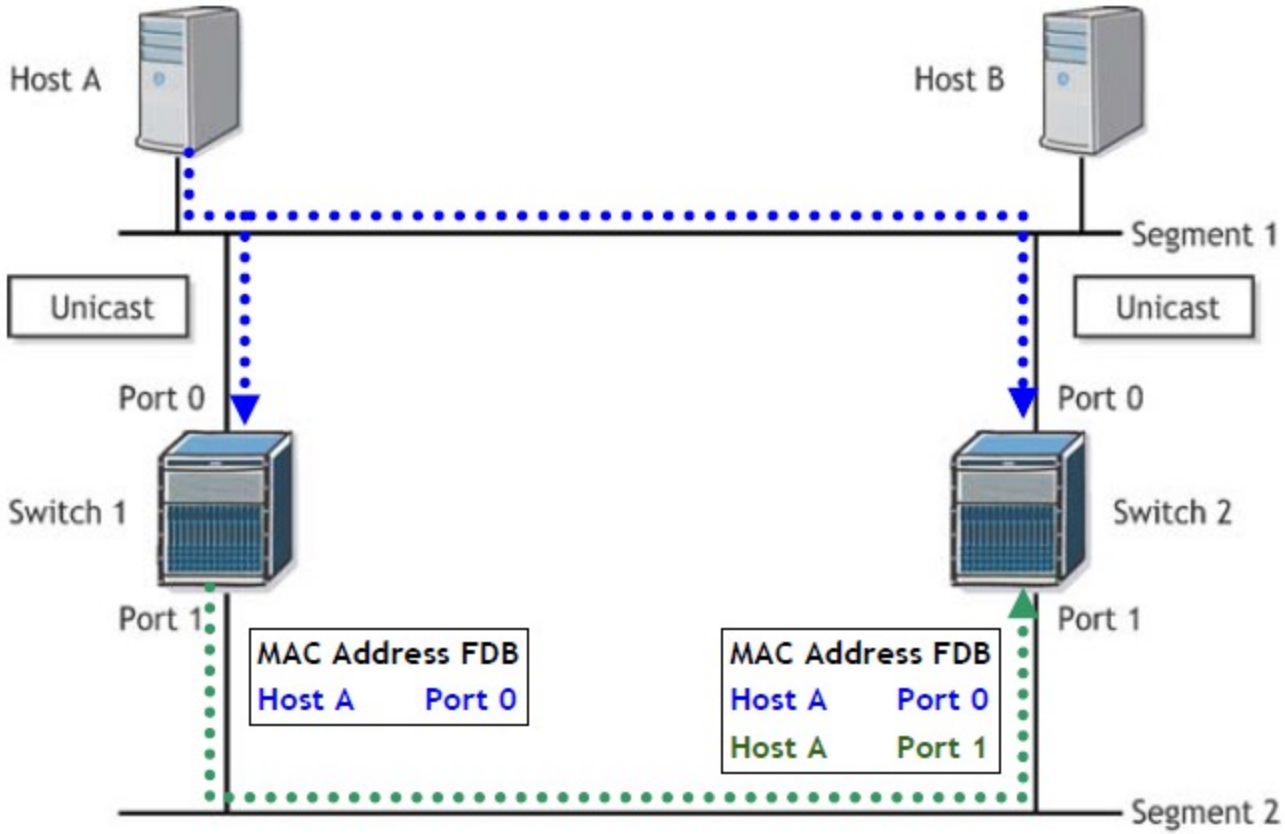
Because there is no time to live (TTL) in Layer 2, this frame is copied and transmitted repeatedly until the switch gets overwhelmed with activity and possibly resets or locks up.



Database Instability

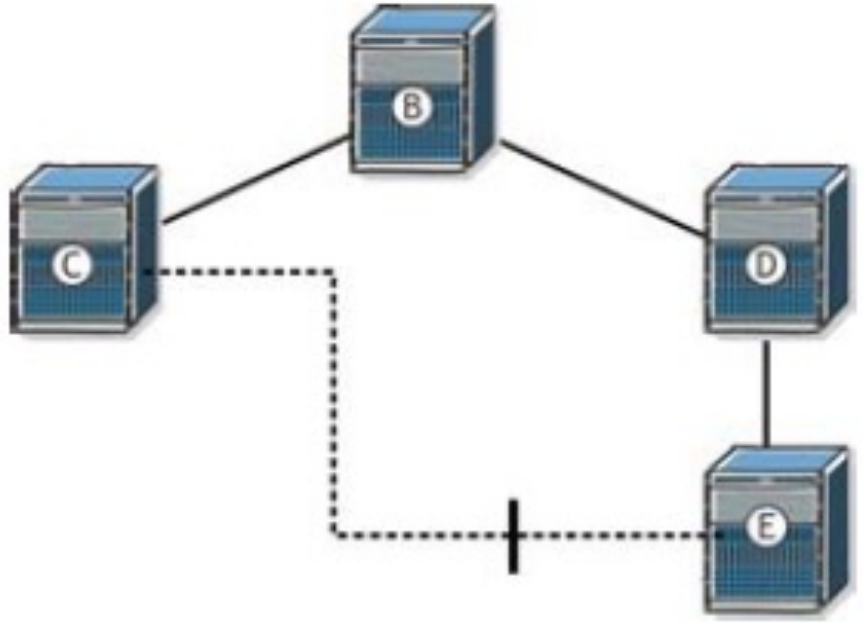
Redundant networks without STP can also cause database instability.

In this slide, Switch 1 and Switch 2 will map the MAC address of Host A to Port 0. Later, when the copy of the frame arrives at Port 1 of Switch 2, Switch 2 must remove its original entry for Host A and replace it with the new entry for Host A, mapping it to Port 1. This activity causes an unstable database as Switch 2 tries to keep up with the perceived location of Host A.



How to Fix the problems? -> STP

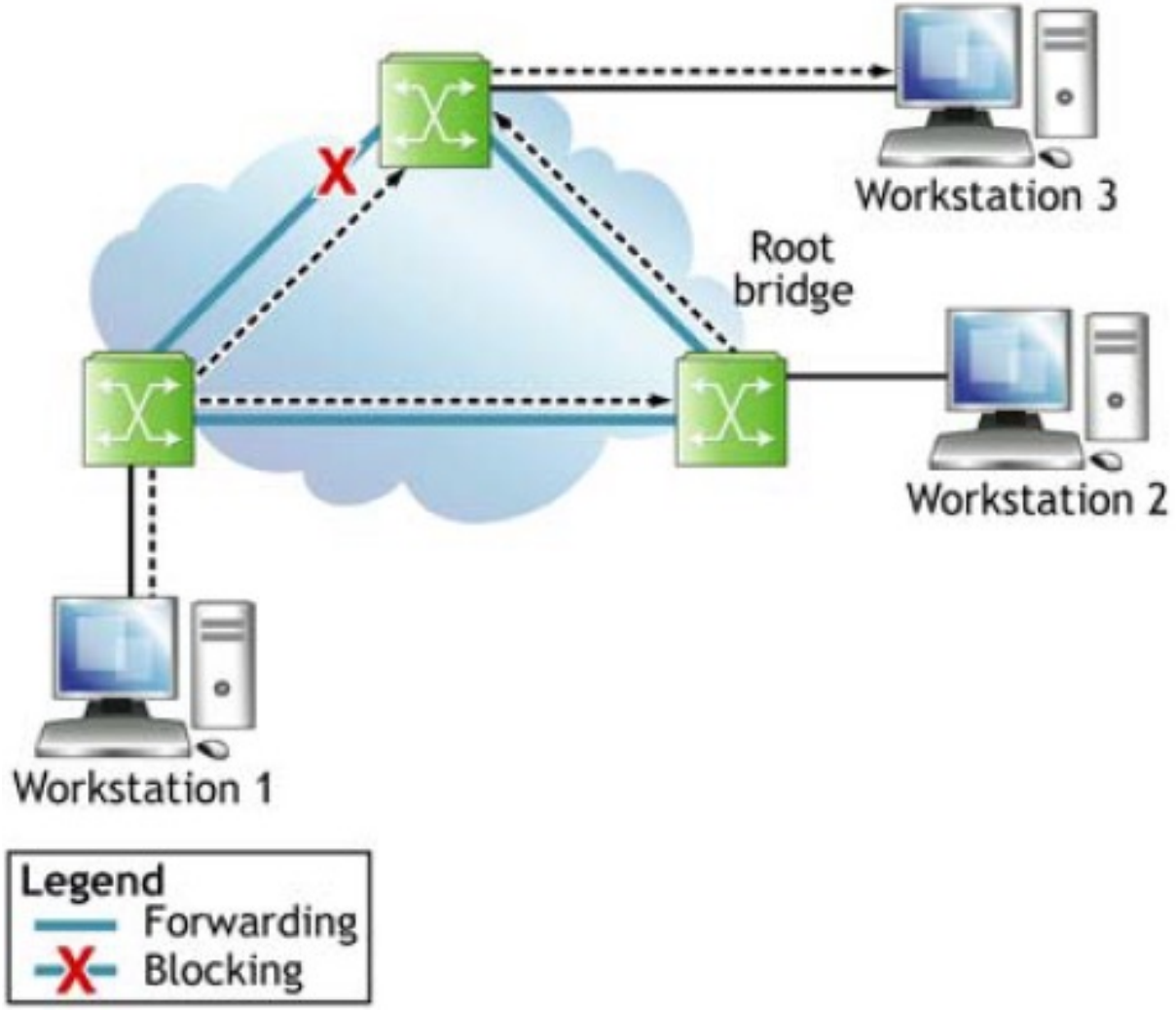
- Standardized by IEEE in 1990 as 802.1d, for Ethernet link management
- Designed to prevent loops and therefore allow path redundancy to be designed into Ethernet bridge/ switch based networks
- STP uses a root/branch/leaf model, which determines one path to each leaf spanning the entire L2 network
- STP will selectively block ports to remove L2 loops
- End hosts (for example, PCs) are oblivious to STP and instead see one LAN segment



- Main purpose of the STP is building loop-free active topologies
- Our ring topology will be converted into a spanning tree active topology with the root on top

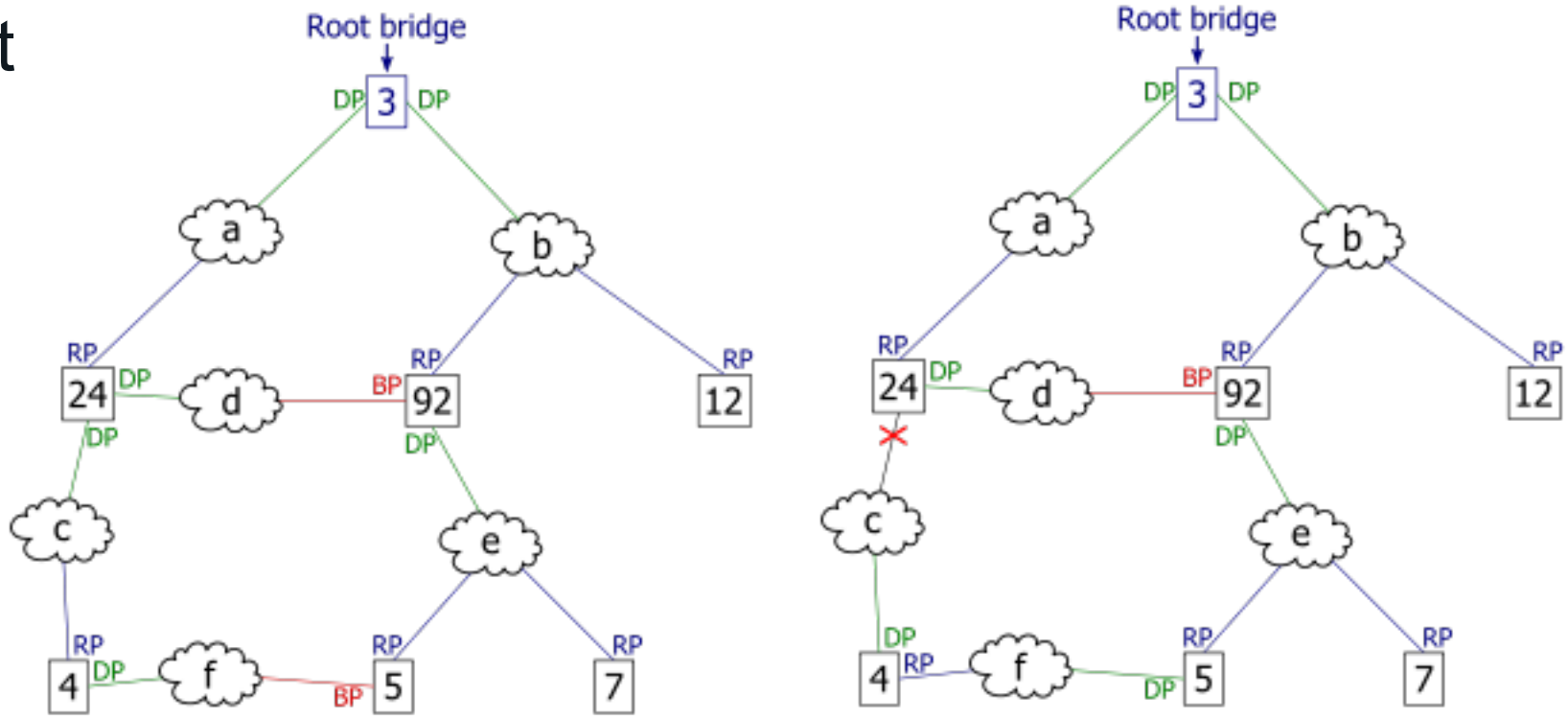
Loop Prevention using Spanning Tree Protocol

- STP removes loops by blocking redundant links.
- Topology changes result in long outages
- STP does not efficiently use all available bandwidth.

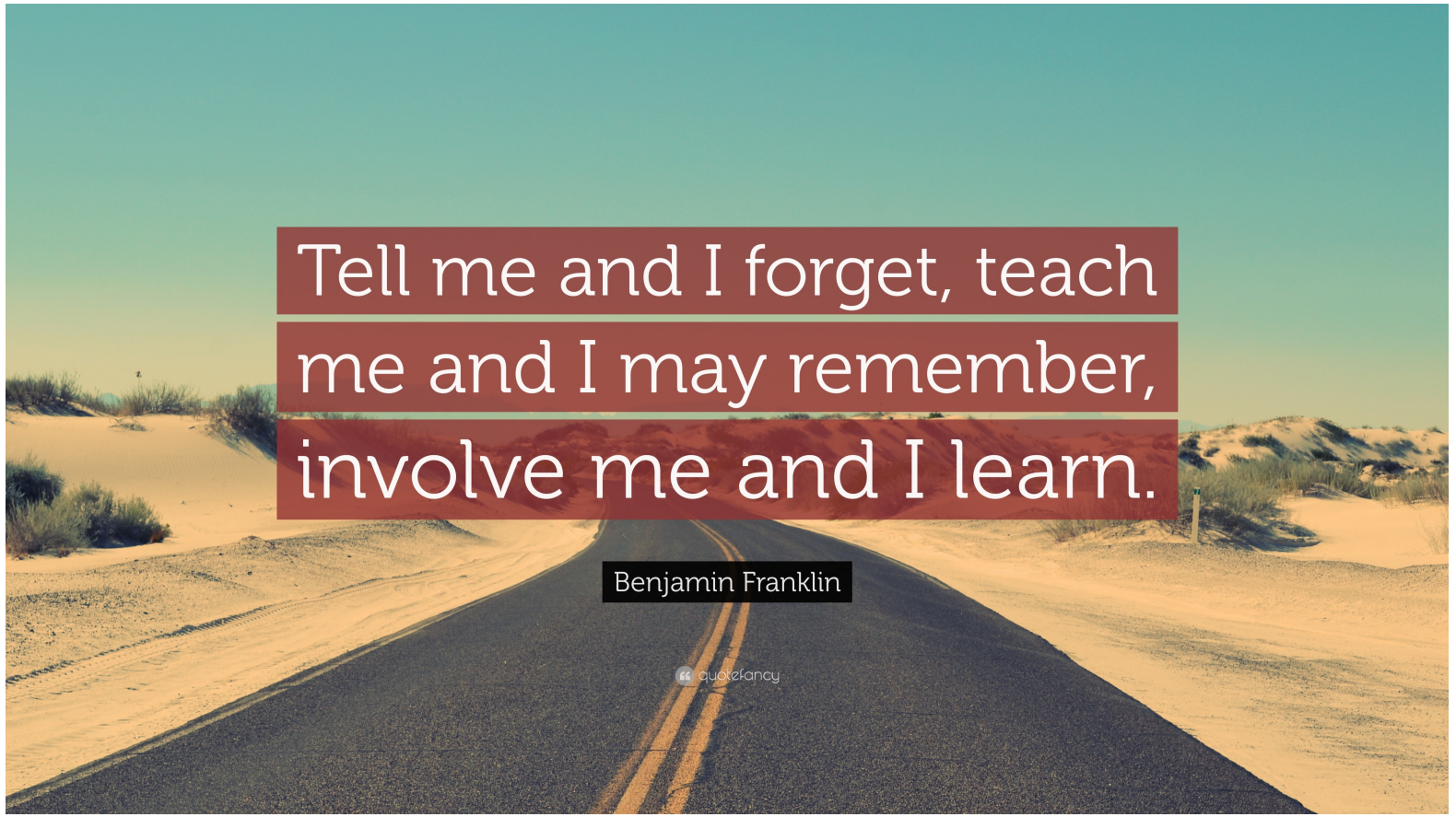


Loop Prevention using Spanning Tree Protocol

- RP: Root port
- DP: Designated port
- BP: Blocked port



Thank You!


Tell me and I forget, teach
me and I may remember,
involve me and I learn.
Benjamin Franklin
quotefancy

Ethernet Frame

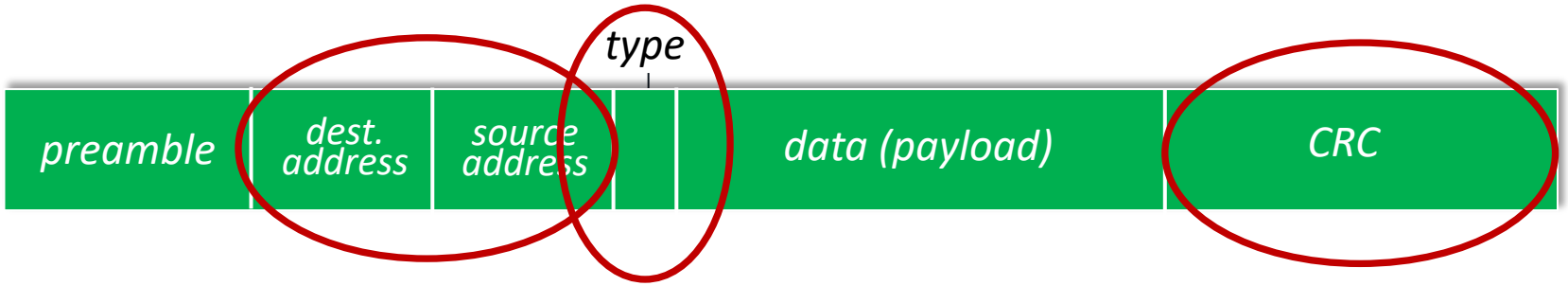
Ethernet Frame Structure

sending interface encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

preamble:

- used to synchronize receiver, sender clock rates
- 7 bytes of 10101010 followed by one byte of 10101011

Ethernet Frame Structure



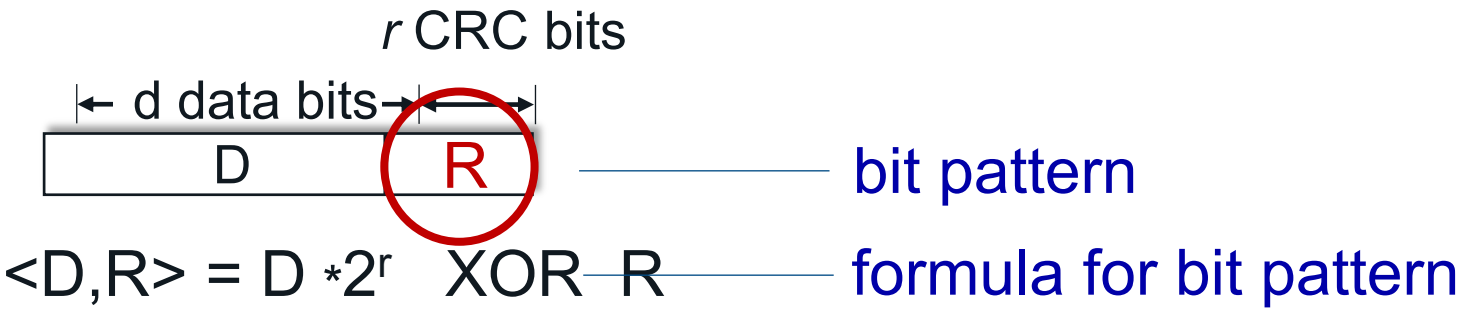
- addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- type: indicates higher layer protocol
  - mostly IP but others possible, e.g., Novell IPX, AppleTalk
  - used to demultiplex up at receiver
- CRC: cyclic redundancy check at receiver
  - error detected: frame is dropped

Ethernet: Unreliable and Connectionless

- connectionless: no handshaking between sending and receiving NICs
- unreliable: receiving NIC doesn't send ACKs or NAKs to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted CSMA/CD with binary backoff

Cyclic Redundancy Check (CRC)

- more powerful error-detection coding
- D: data bits (given, think of these as a binary number)
- G: bit pattern (generator), of *r+1* bits (given)



goal: choose *r* CRC bits, R, such that <D,R> exactly divisible by G (mod 2)

- receiver knows G, divides <D,R> by G. If non-zero remainder: error detected!
- can detect all burst errors less than r+1 bits
- widely used in practice (Ethernet, 802.11 WiFi)

Cyclic Redundancy Check (CRC)

We want:

$D \cdot 2^r$ XOR $R = nG$

or equivalently:

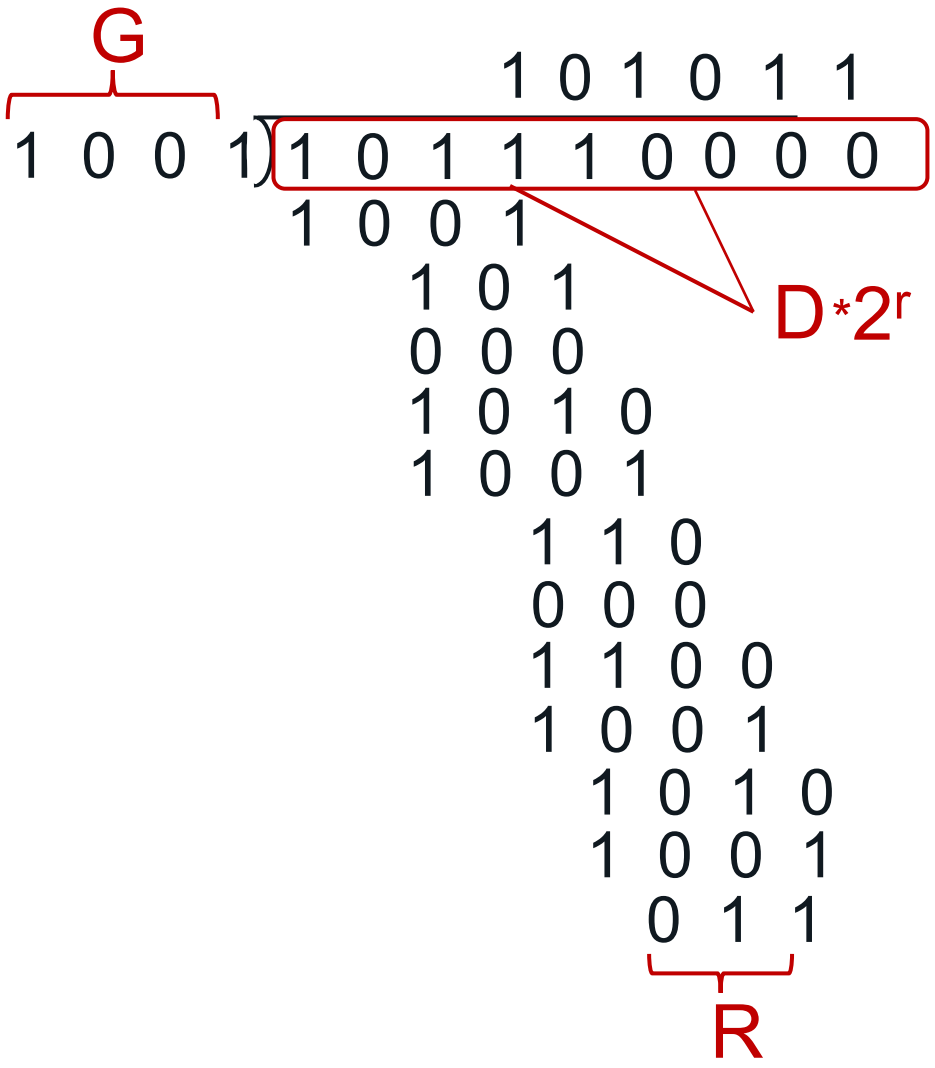
$D \cdot 2^r = nG$ XOR R

or equivalently:

if we divide $D \cdot 2^r$ by G, want remainder R to satisfy:

$$R = \text{remainder}\left[\frac{D \cdot 2^r}{G}\right]$$

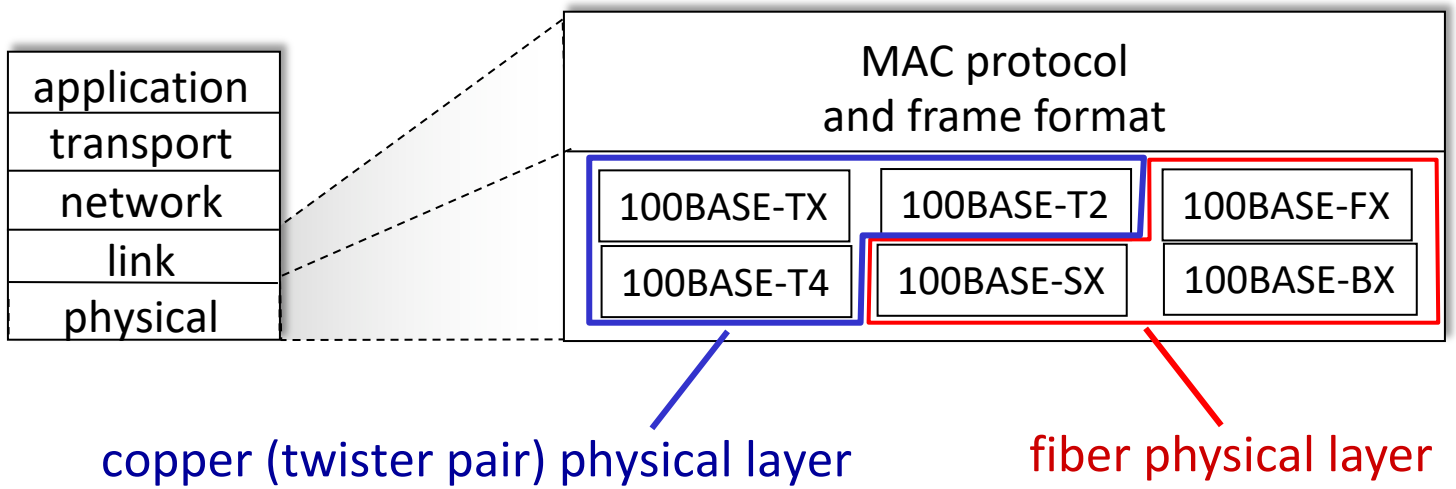
Transmitted frame: 101110011



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

802.3 Standards: Link & Physical Layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps
  - different physical layer media: fiber, cable



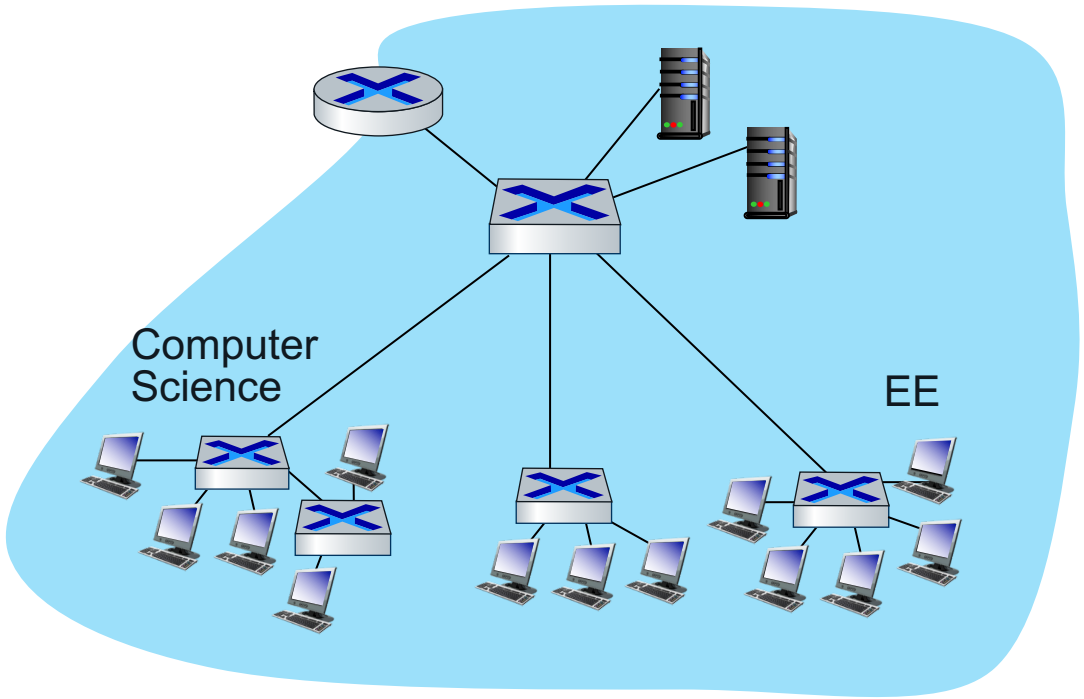
Thank You!


Tell me and I
forget. Teach me
and I remember.
Involve me and I
learn.
~ Benjamin Franklin

Virtual LAN

Virtual LAN: Motivations

Q: what happens as LAN sizes scale, users change point of attachment?

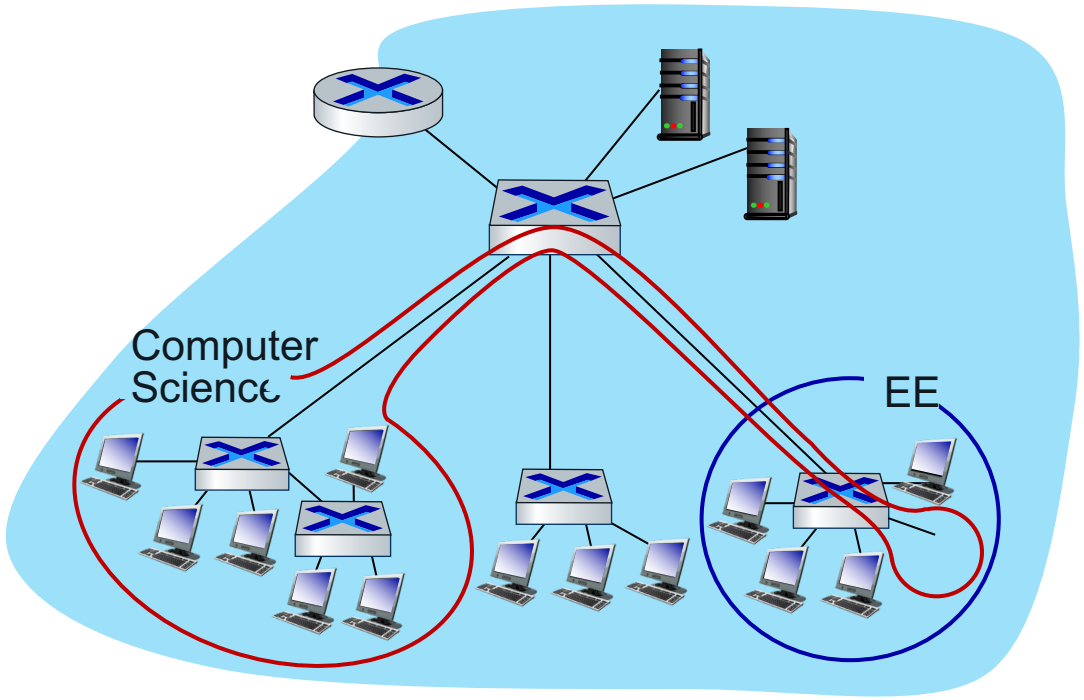


single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy issues

Virtual LAN: Motivations

Q: what happens as LAN sizes scale, users change point of attachment?



single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy, efficiency issues

administrative issues:

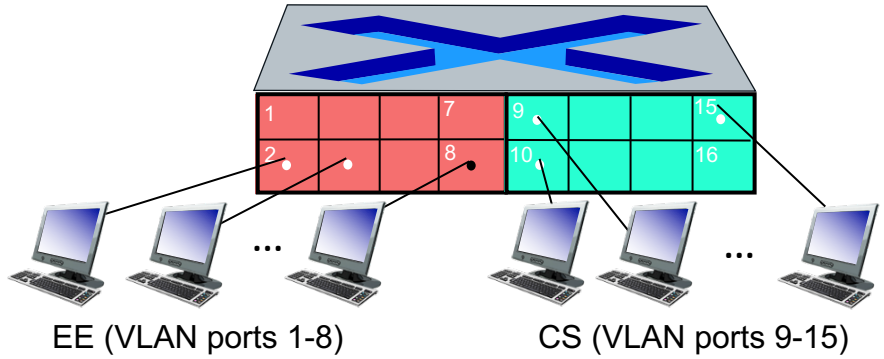
- CS user moves office to EE - *physically* attached to EE switch, but wants to remain *logically* attached to CS switch

Port-Based VLAN

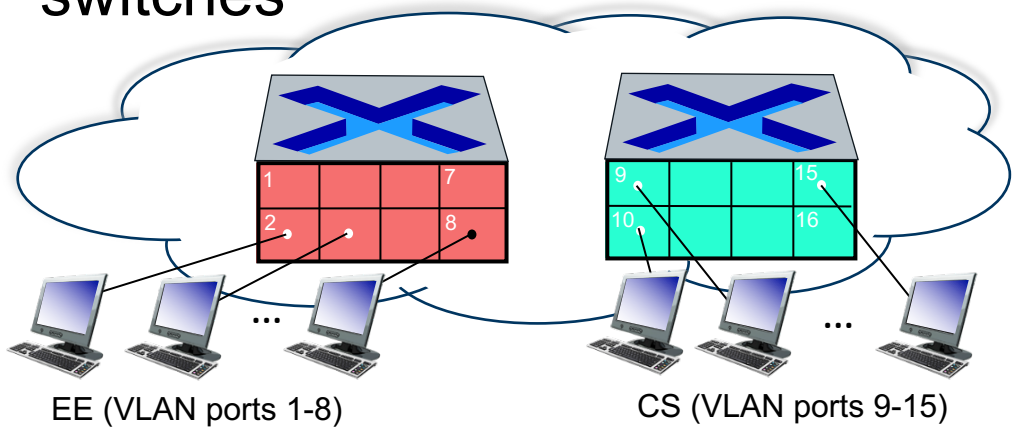
Virtual Local Area Network (VLAN)

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 ……

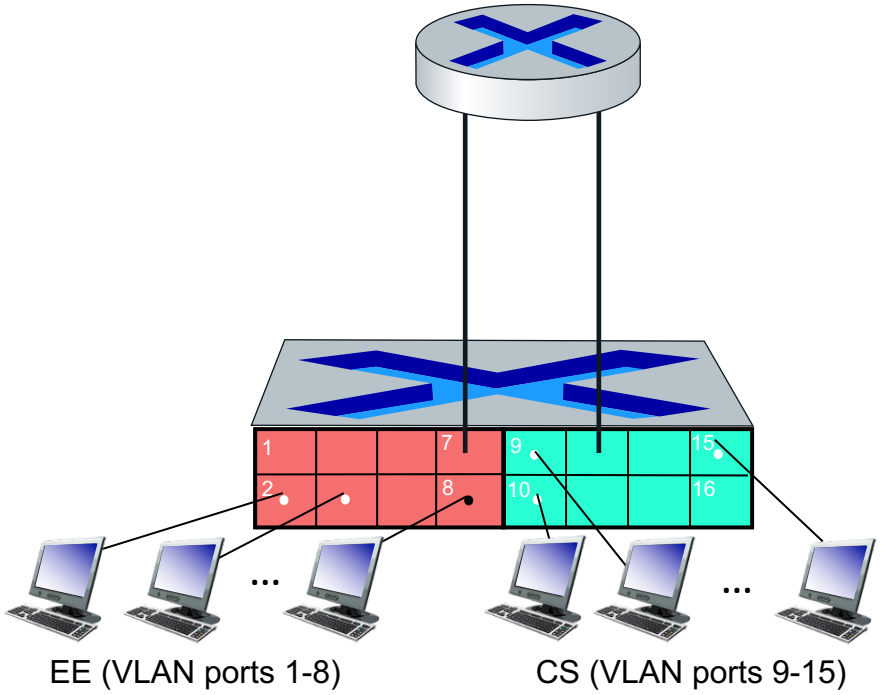


… operates as multiple virtual switches



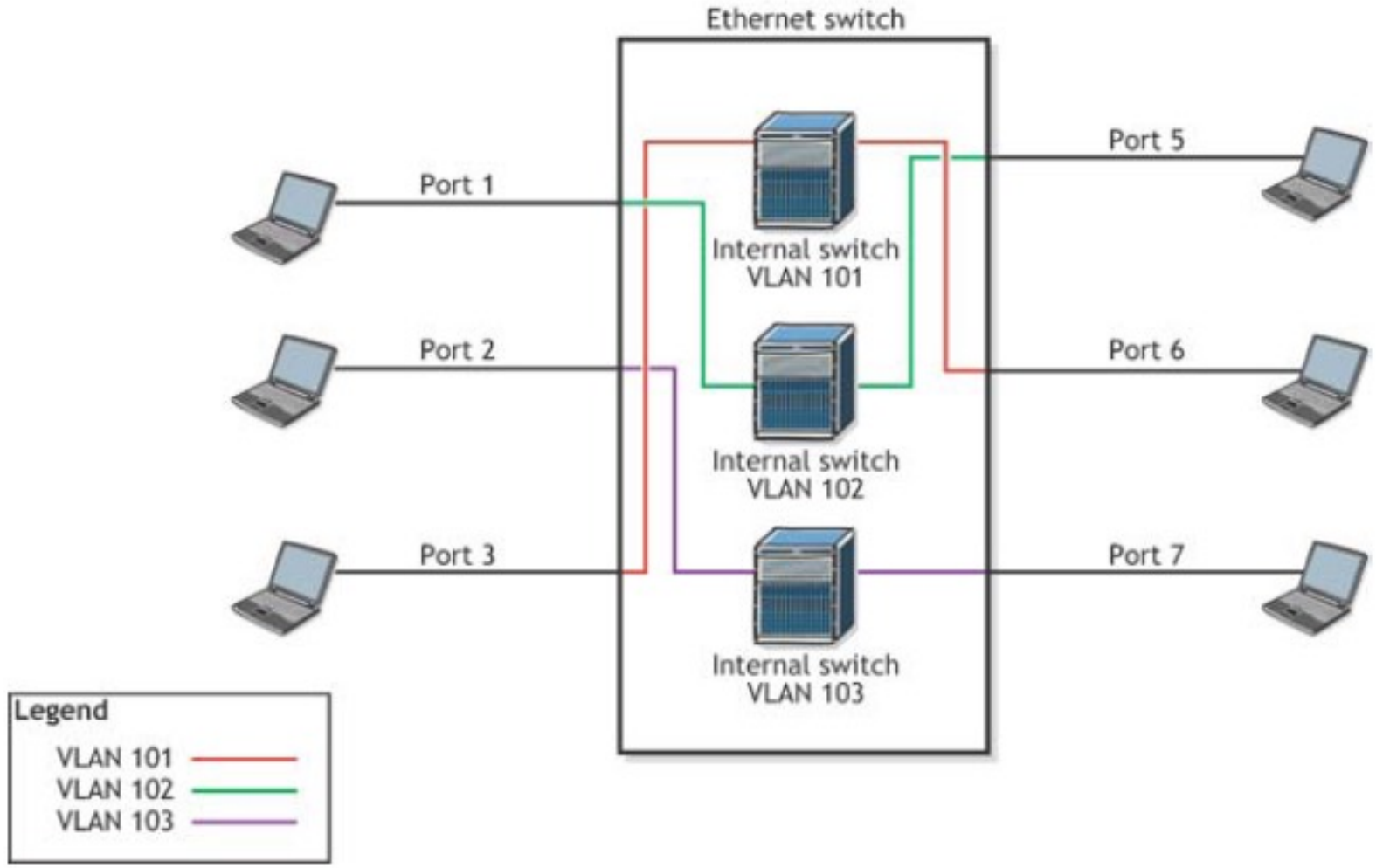
Port-Based VLAN

- 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

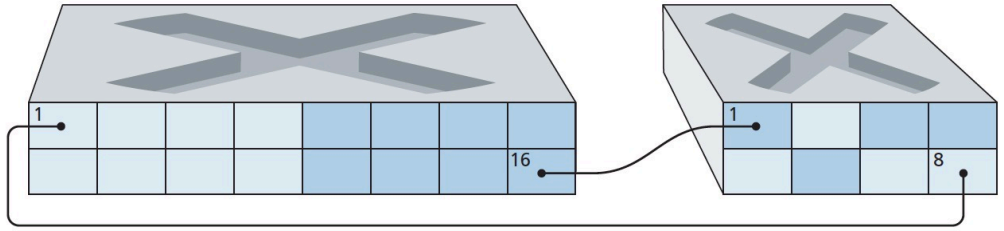


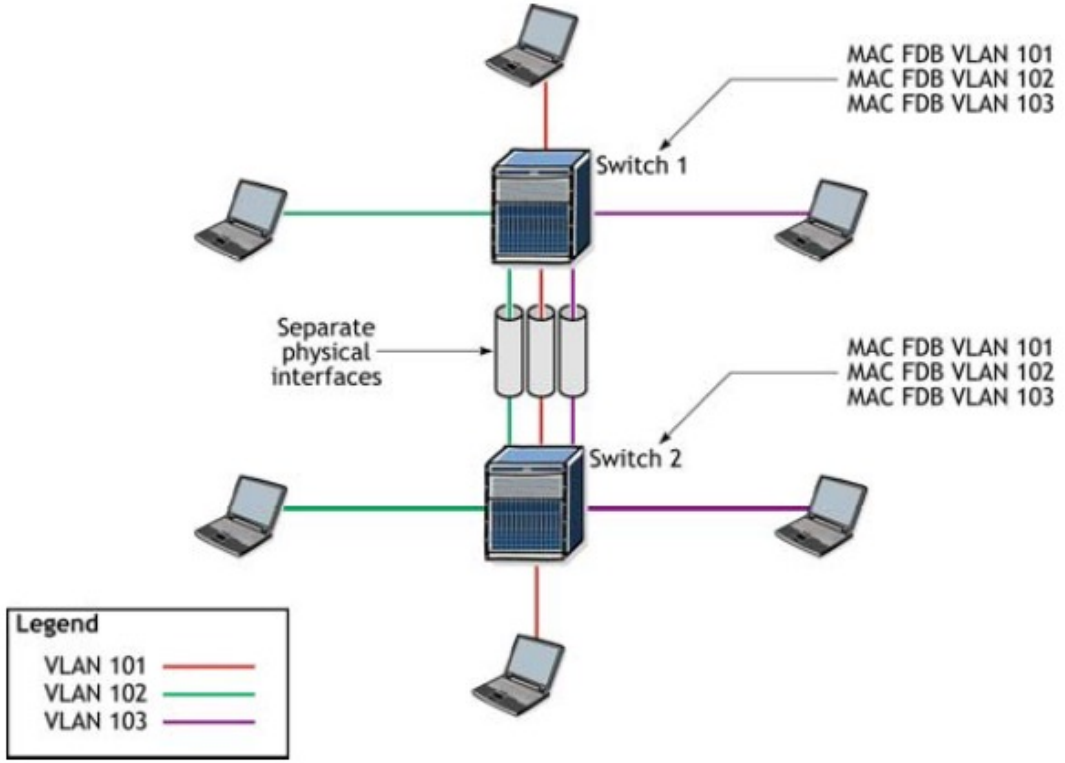
VLAN - Switches and VLANs

- A VLAN permits a group of ports to share a common broadcast domain regardless of physical location
- A VLAN can reside on one switch or on many switches
- Each VLAN is identified by a VLAN ID
- Devices in different VLANs can only communicate with each other if the frame is first sent to a Layer 3 device such as a router



VLAN Spanning Multiple Switches

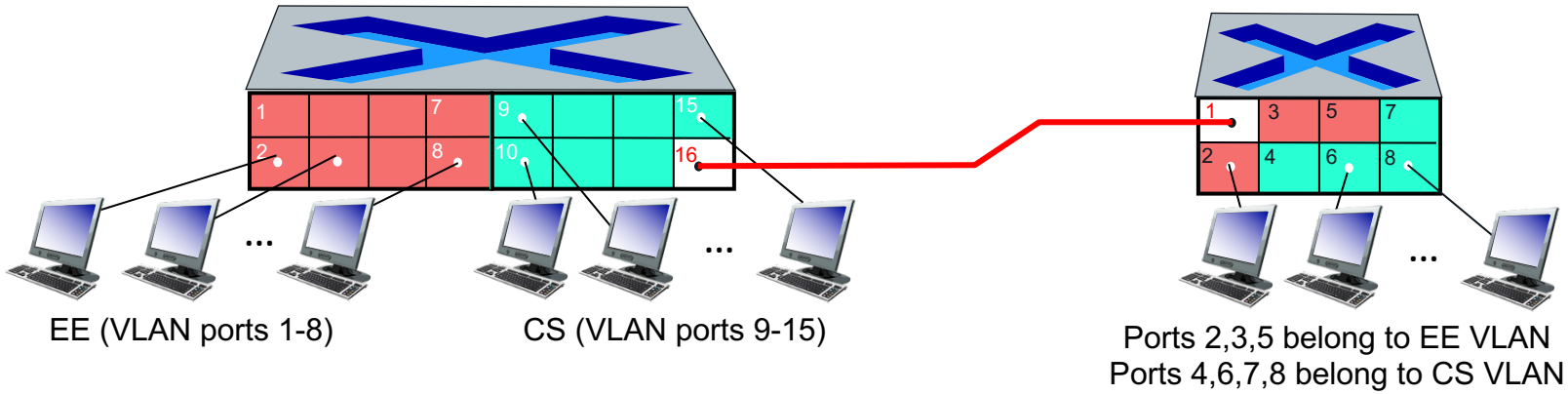




Physical port: carries frames between VLANS defined over multiple physical switches

- Requires 1 physical port for each switch
- Does not scale if the number of switches increases

VLAN Spanning Multiple Switches

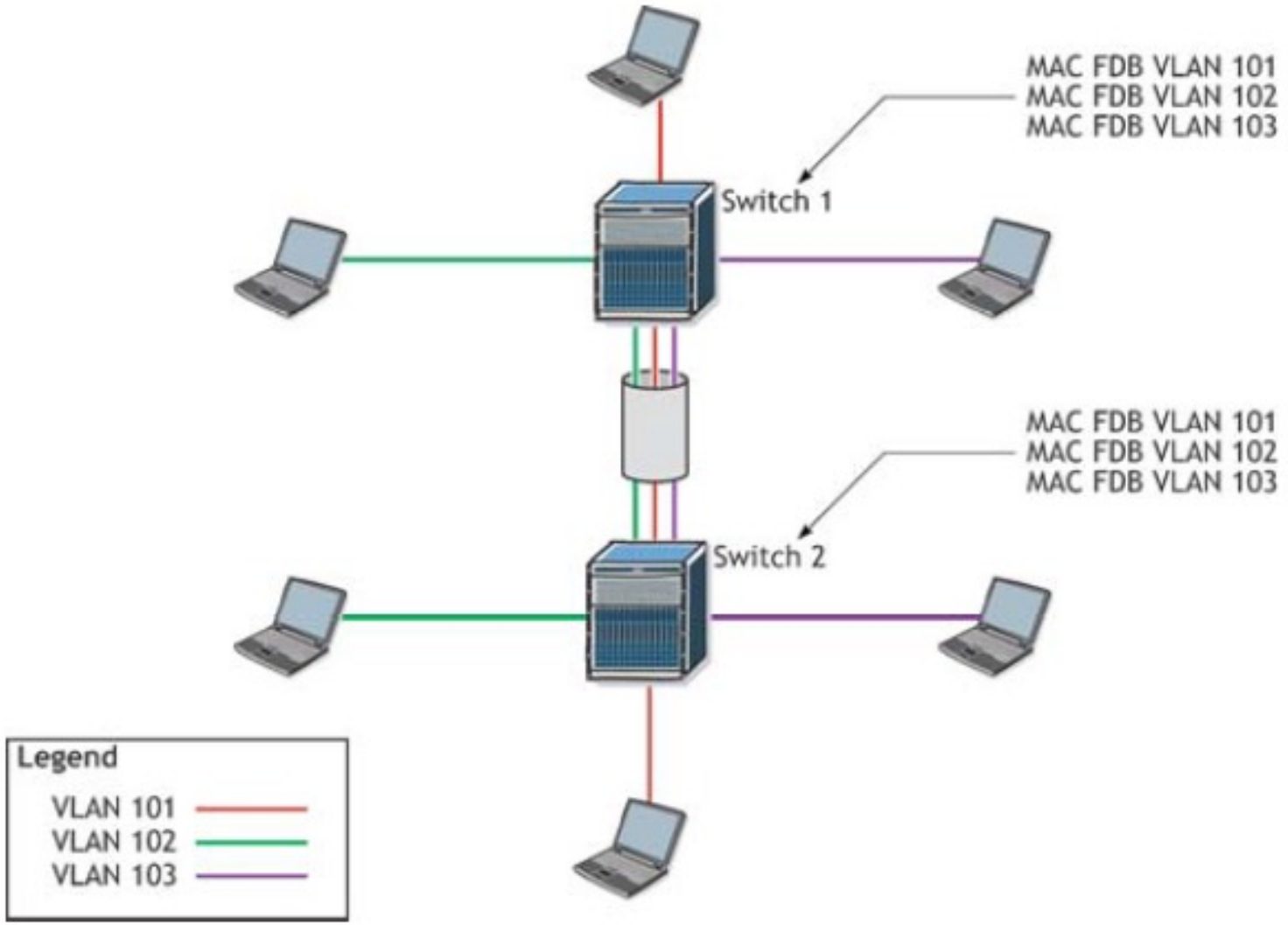


Trunk Port: carries frames between VLANS defined over multiple physical switches

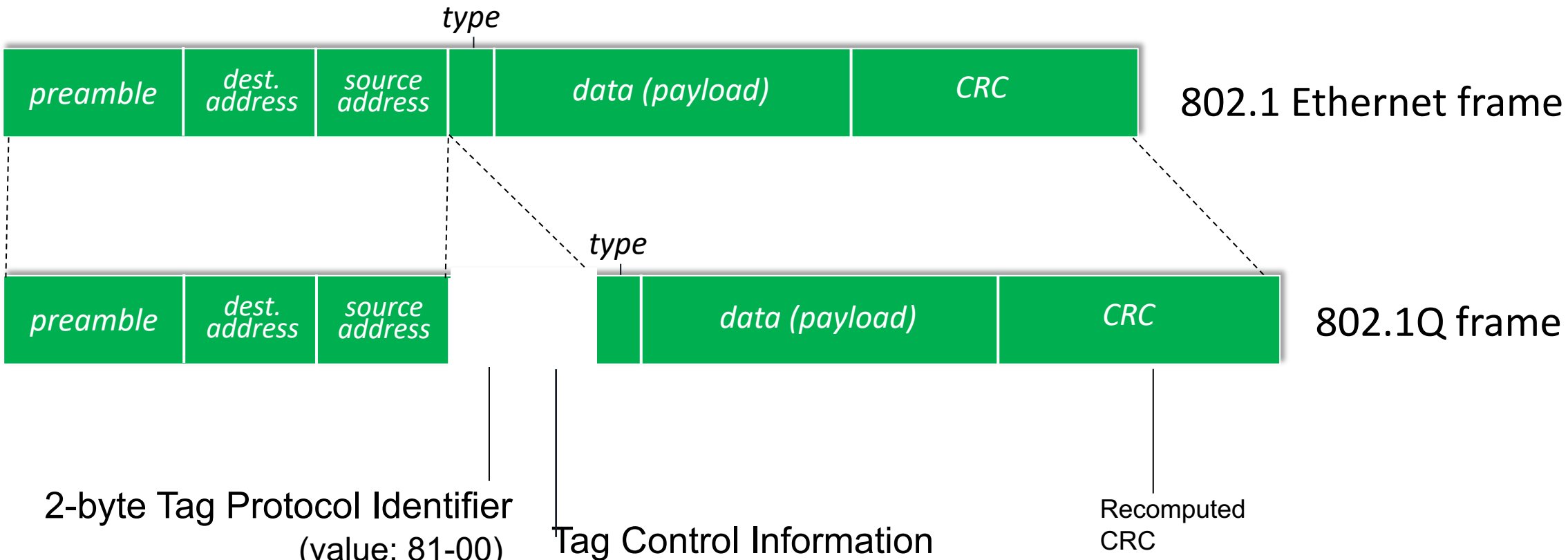
- frames forwarded within VLAN between switches cannot be the same as 802.1 frames (must carry VLAN ID info)
- 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

VLAN Trunking

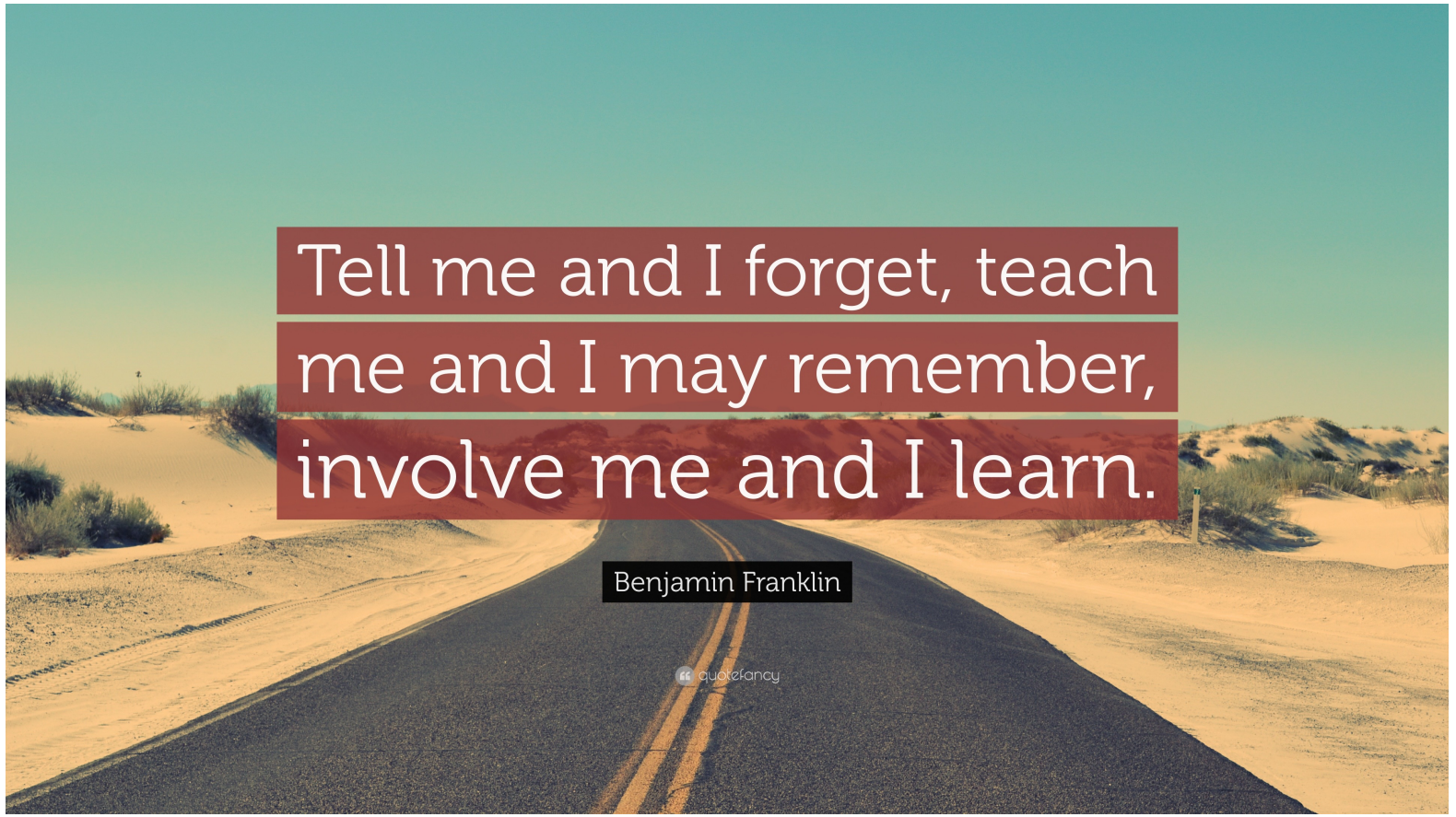
VLAN trunking allows one Ethernet port to carry frames from multiple VLANs. This allows the use of one high-bandwidth port, such as a gigabit(?) Ethernet port, to carry the VLAN traffic between switches instead of multiple fast Ethernet ports. VLANs are separated within the trunk based on their VLAN IDs (Q tags). The FDB at the destination switch designates the destination VLAN for the traffic on the VLAN trunk.



VLAN Spanning Multiple Switches



Thank You!


Tell me and I forget, teach
me and I may remember,
involve me and I learn.
Benjamin Franklin
quotefancy