UNIVERSITY OF WATERLOO

# CS 456/656
# Computer Networks

## Lecture 15: Link Layer – Part 2

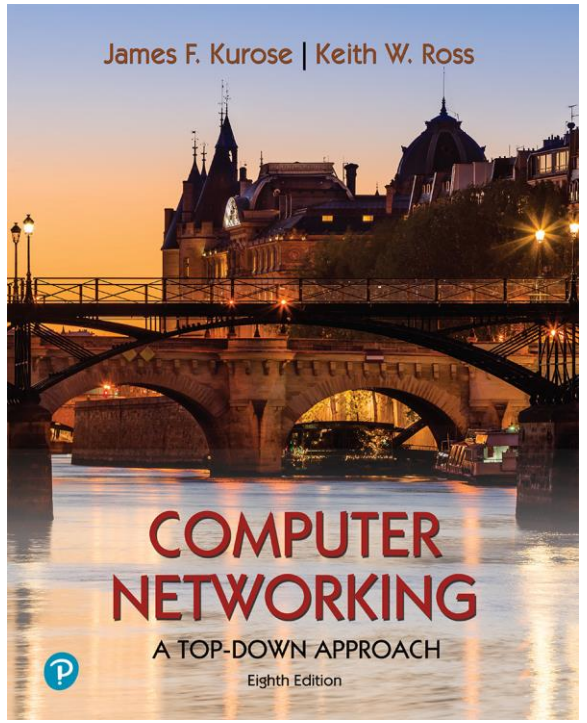
Mina Tahmasbi Arashloo and Bo Sun

Fall 2024

# A note on the slides

Adapted from the slides that accompany this book.



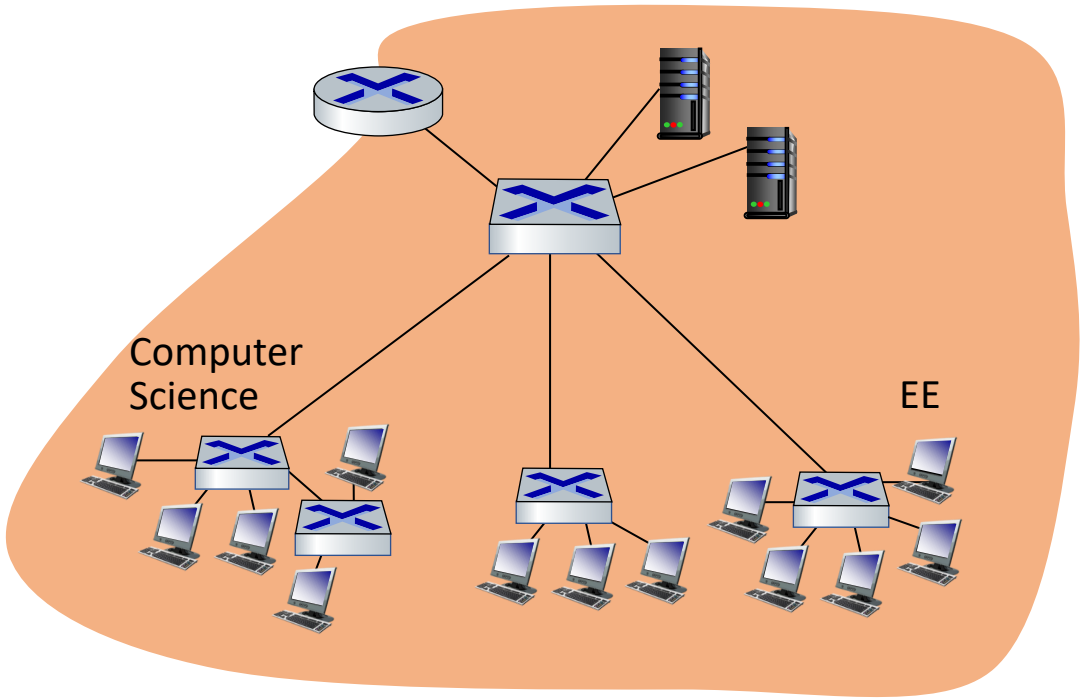



*Computer Networking: A Top-Down Approach*
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

# Link layer: roadmap

- Link layer overview
  - Local Area Networks (LANs)
- Switched LANs
  - Ethernet and Addressing
  - Address Resolution Protocol (ARP)
  - Switches
- Virtual LANs (VLANs)
- Shared LANs and multiple access protocols

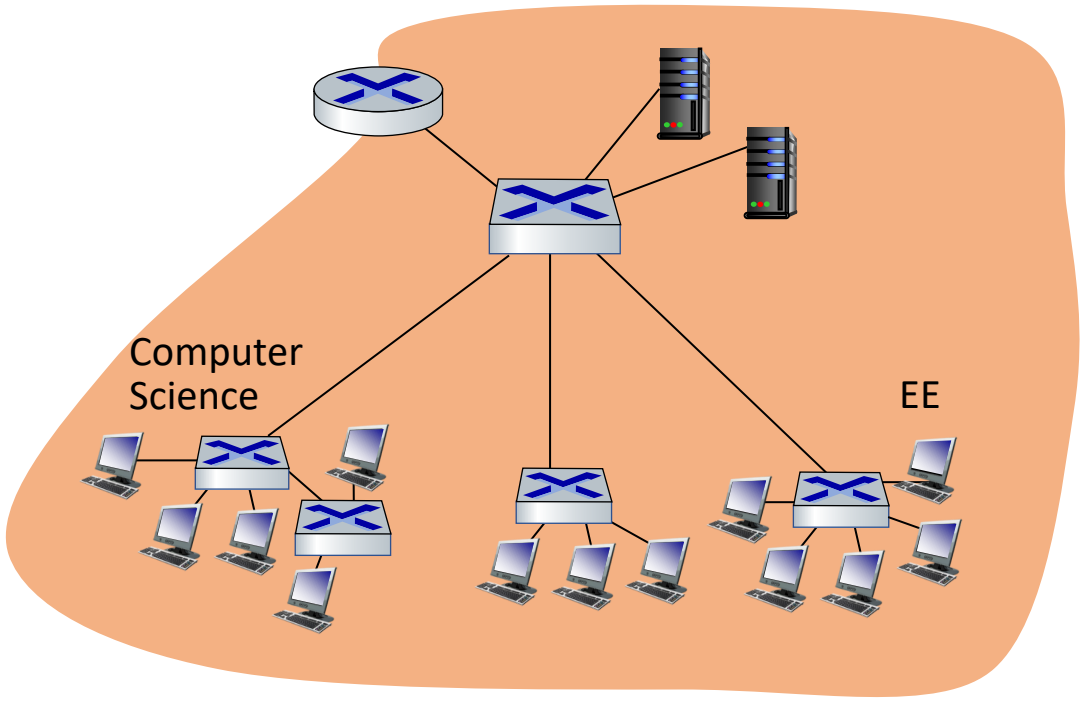
# Virtual LANs (VLANs): motivation




An example institutional network.

- All layer-2 broadcast traffic (ARP, unknown MAC) crosses the entire LAN
- What issues can this cause as the LAN size grows?

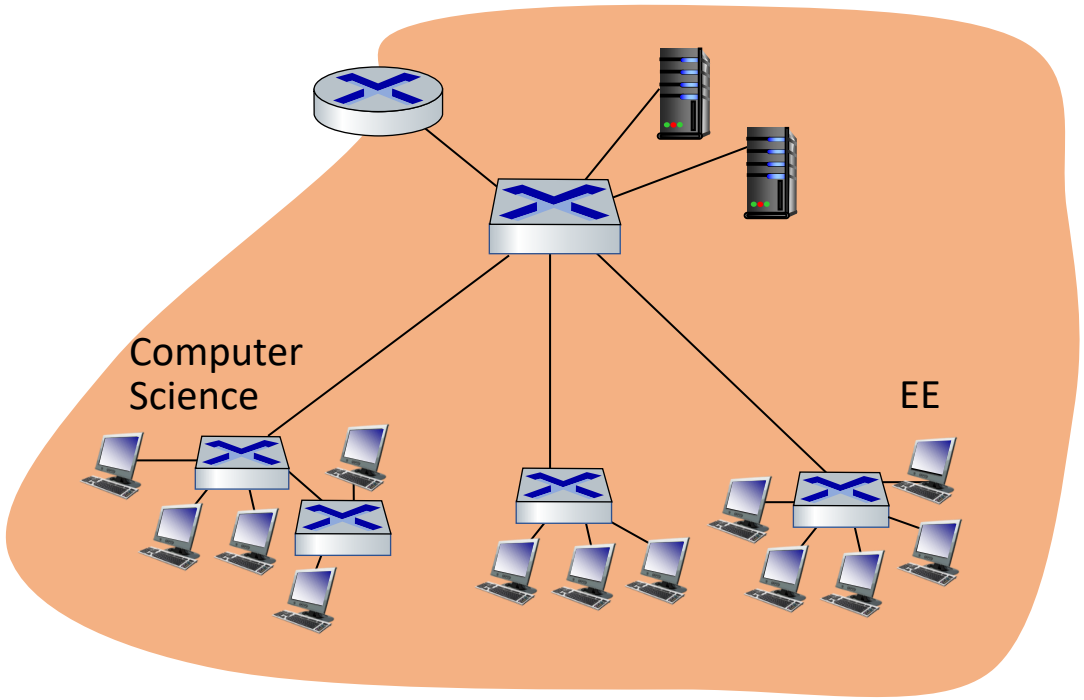
# Virtual LANs (VLANs): motivation




An example institutional network.

- Scalability/efficiency issues
  - Non-trivial overhead from broadcast for larger LANs
- Security/privacy/admin issues
  - Diverse groups of users
  - It may not be okay for different groups to see each other's traffic.

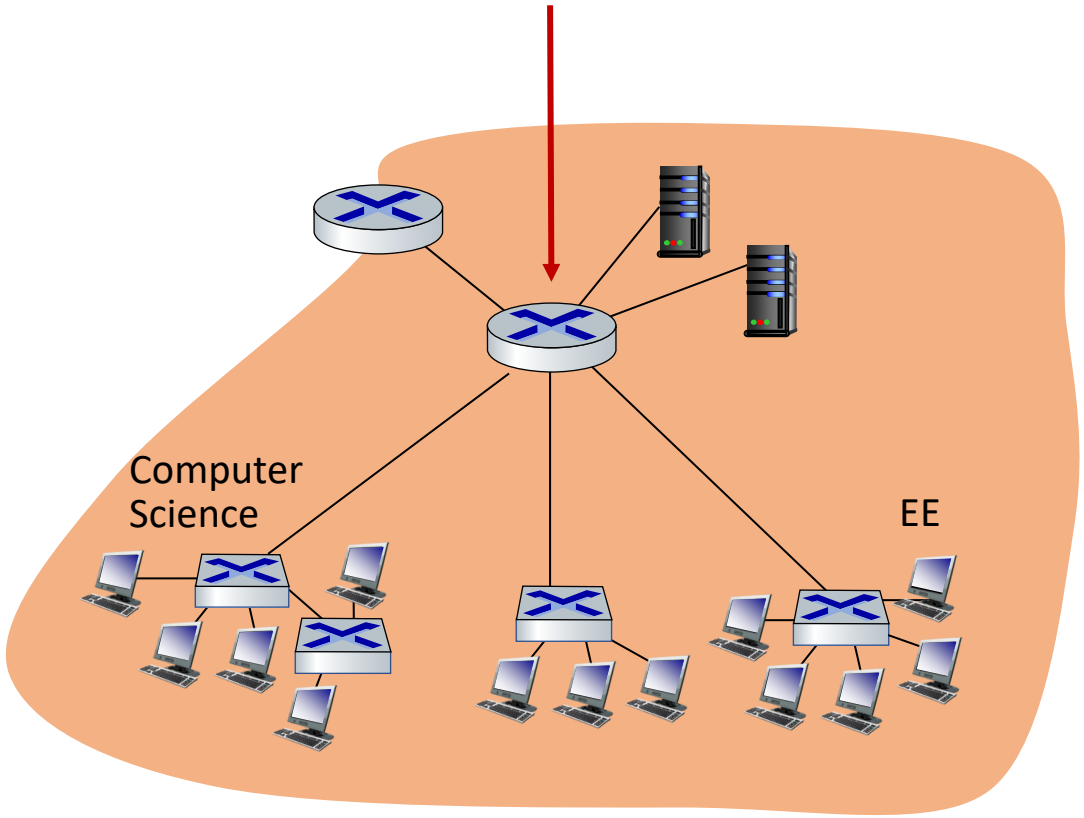
# Virtual LANs (VLANs): motivation




An example institutional network.

- Why not use routers instead?

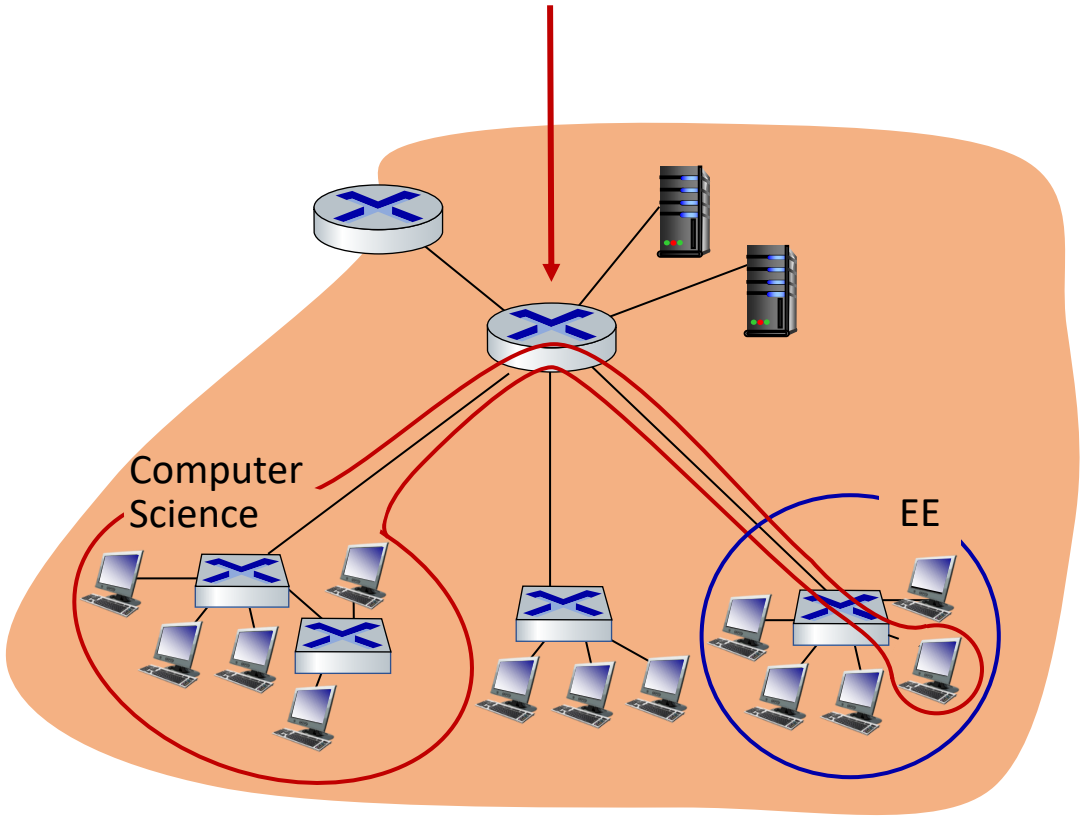
# Virtual LANs (VLANs): motivation




An example institutional network.

- Why not use routers instead?

# Virtual LANs (VLANs): motivation




An example institutional network.

- Why not use routers instead?
- Makes mobility difficult.
- E.g., a CS user moves office to EE, but still belongs to the CS “group” in terms of the properties of its network connectivity.

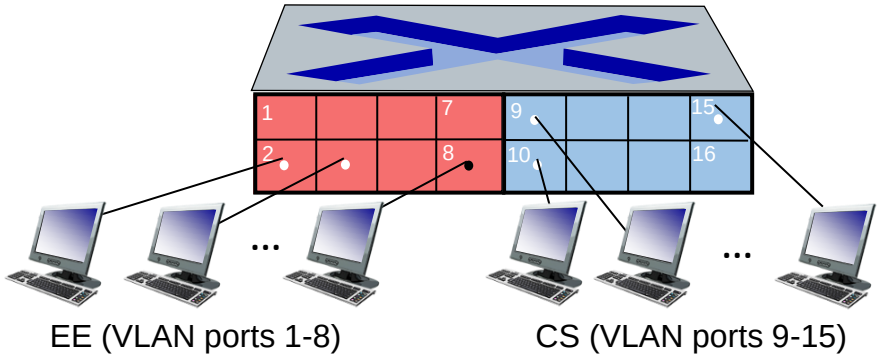
# Virtual LAN (VLANs)

- Define the set of “users” that belong in the same LAN
  - i.e., users for whom it is ok for them to share a broadcast domain.
- Each will become one virtual LAN (VLAN).
- Configure the physical switches so that they can act as a virtual switch for each VLAN.
- So, you’ll have multiple VLANs over a single physical LAN infrastructure.

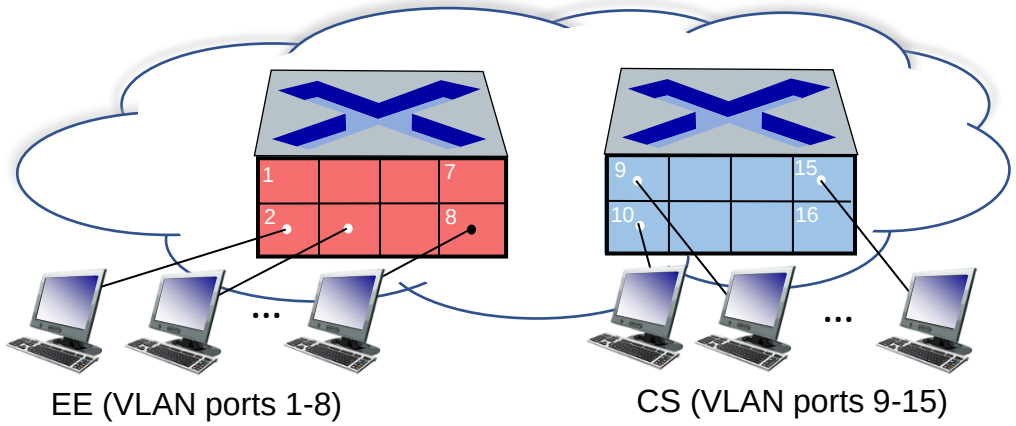
# Port-based VLANs

- VLAN defined based on ports:
  - The operator will specify which switch ports belong to a specific VLAN
    - 1-8 for EE, 9-15 for CS
  - Any endpoint connected to that port will be part of that VLAN
- traffic isolation:
  - frames to/from ports 1-8 (EE VLAN) can *only* reach ports 1-8.
- dynamic membership: ports can be dynamically assigned among VLANs

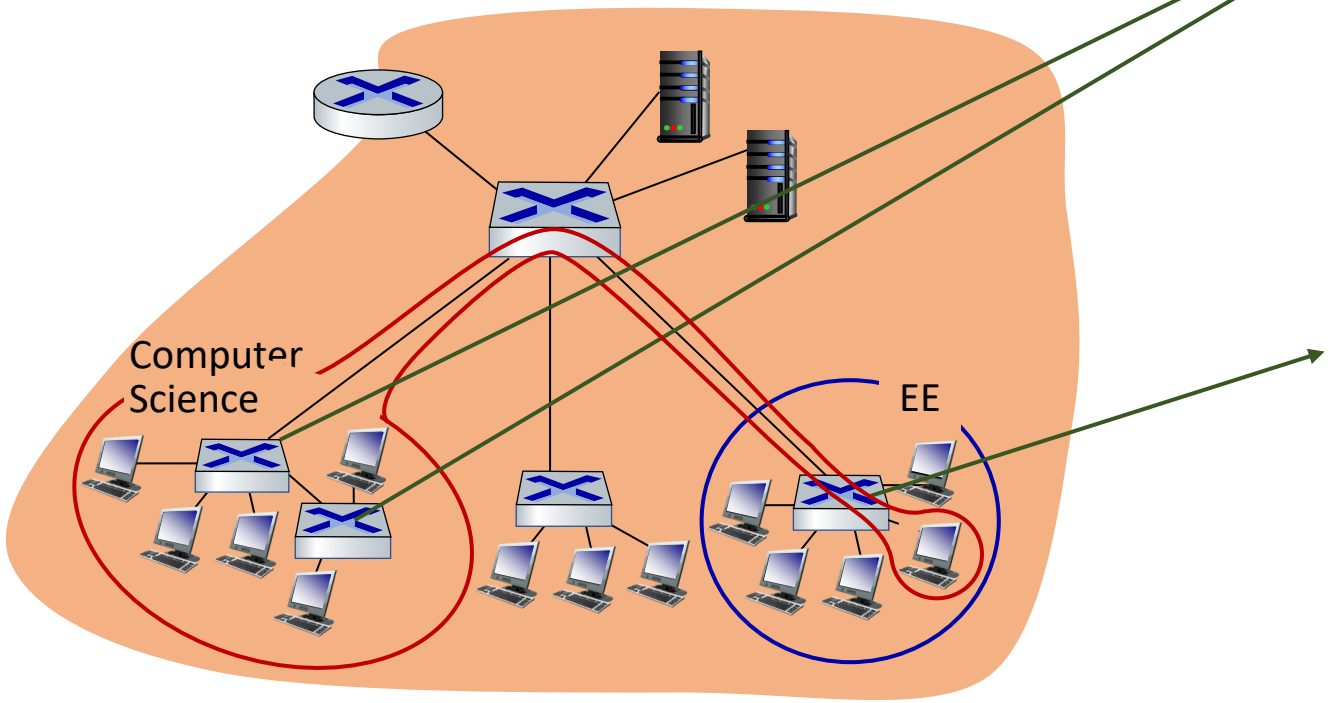
a *single* physical switch ……




… operates as multiple virtual switches



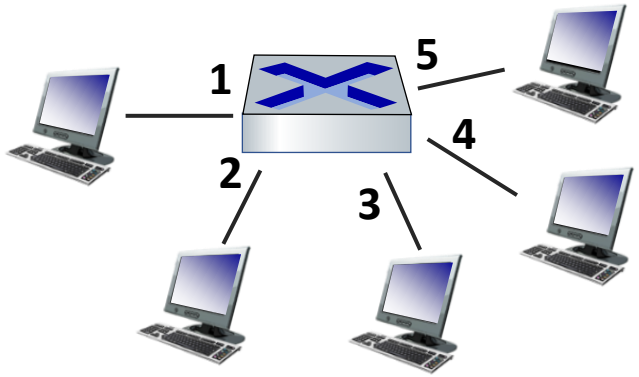
# Port-based VLANs




An example institutional network.

All ports belong to the CS VLAN

Ports 1,2, 3, 5 belong to the EE VLAN
Port 4 belongs to the CS VLAN



# Sidenote: Other VLAN definition criteria

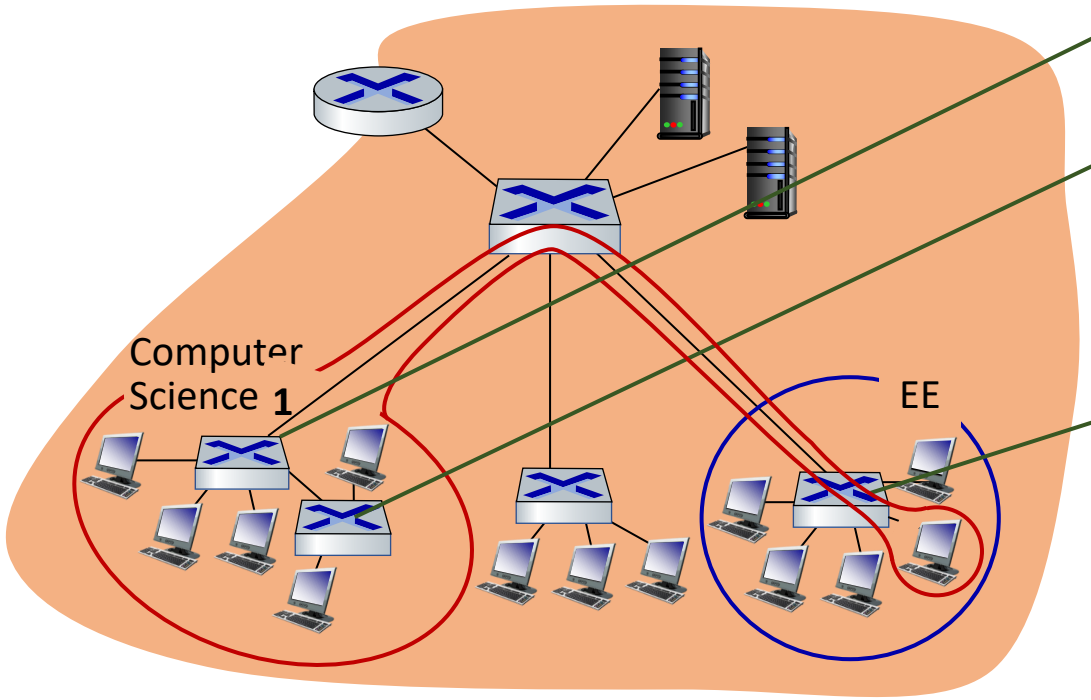
- We can also define VLAN based on MAC addresses of endpoints, rather than switch port
  - whenever a device attaches to a port, the port is connected into the appropriate VLAN based on the MAC address of the device

# Make sure you know

- The motivation behind VLANs
- What a port-based VLAN mean and how it provides traffic isolation.

# Port-based VLANs

How do we forward traffic between A and B?

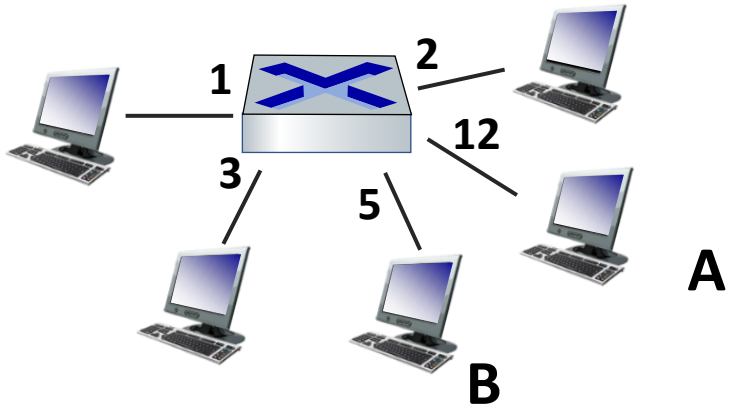



An example institutional network.

All ports (except 1) belong to the CS VLAN

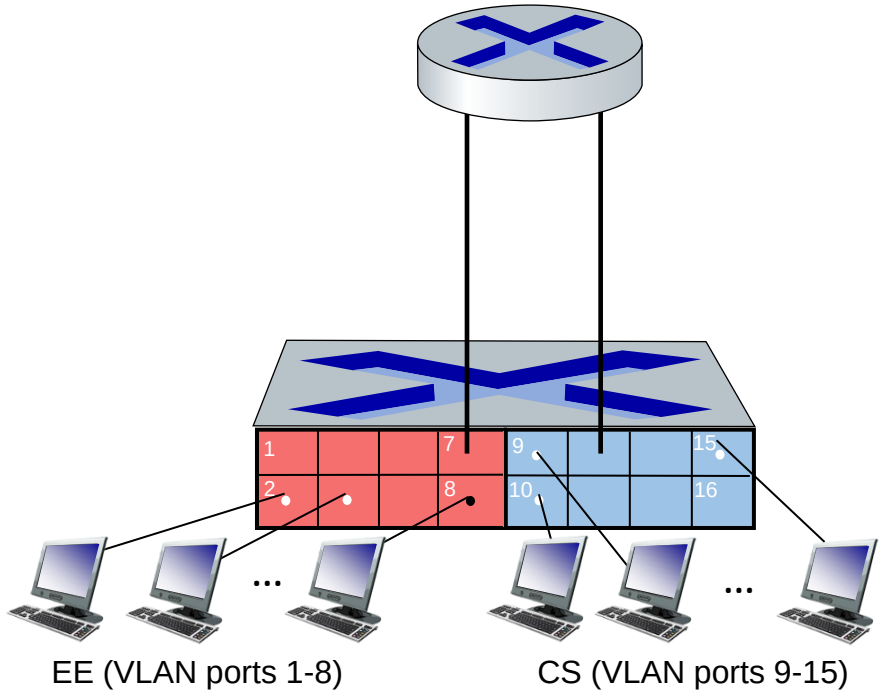
All ports belong to the CS VLAN

Ports 1-8 belong to the EE VLAN
Ports 9-15 belong to the CS VLAN



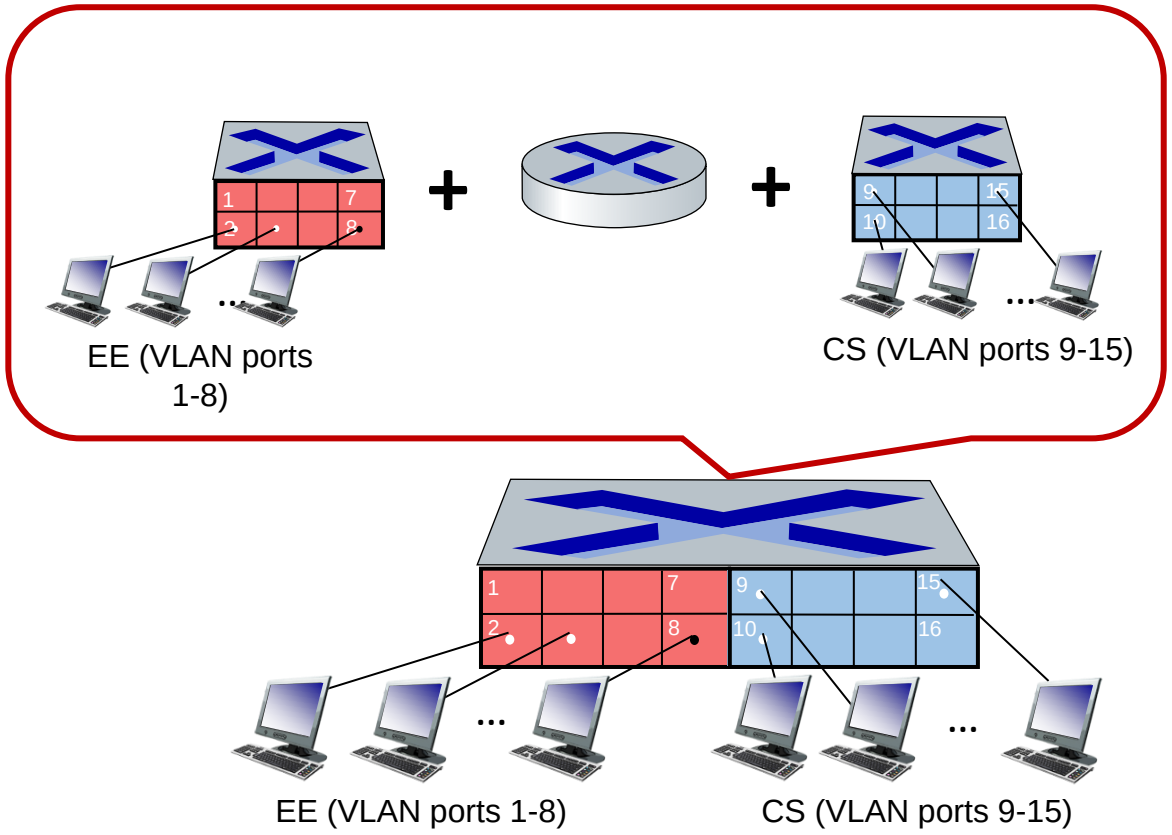
# Forwarding between VLANs

- VLANs are separate L2 networks
- So, traffic forwarding between them happens via routing
  - just as with separate switches



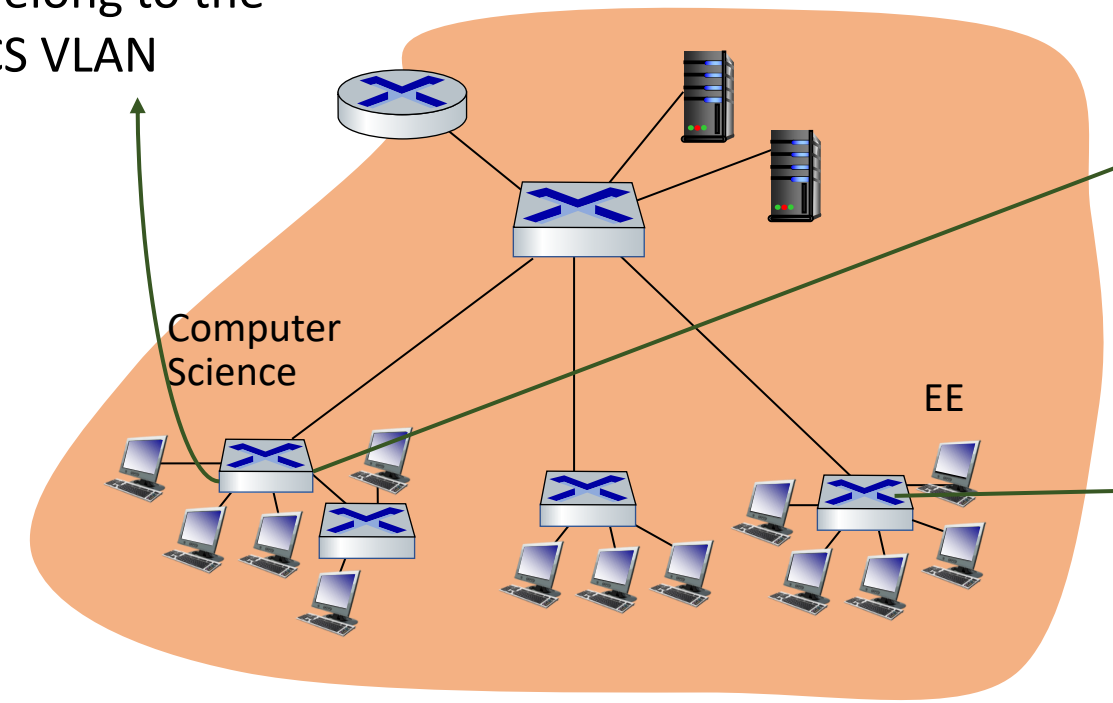
# Forwarding between VLANs

- In practice, there is not a separate physical router
- The vendors sell combined switches plus routers.
- So, traffic going between different VLANs will be processed by a “L3 router” within the same device.

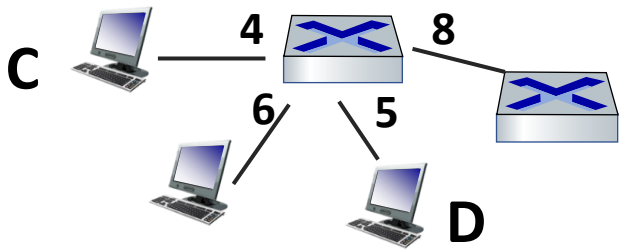


- How do we forward traffic between A and C?
  - Both belong to CS VLAN, not attached to the same switch
- How about between B and D?

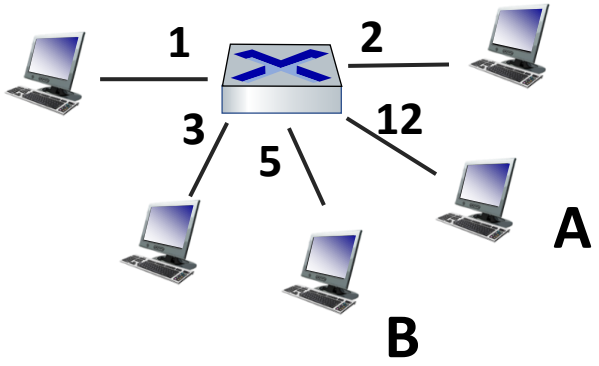
All ports belong to the CS VLAN




Ports 4, 6, 7, 8 belong to CS VLAN
Ports 2, 3, 5 belong to EE VLAN




Ports 1-8 belong to the EE VLAN
Ports 9-15 belong to the CS VLAN

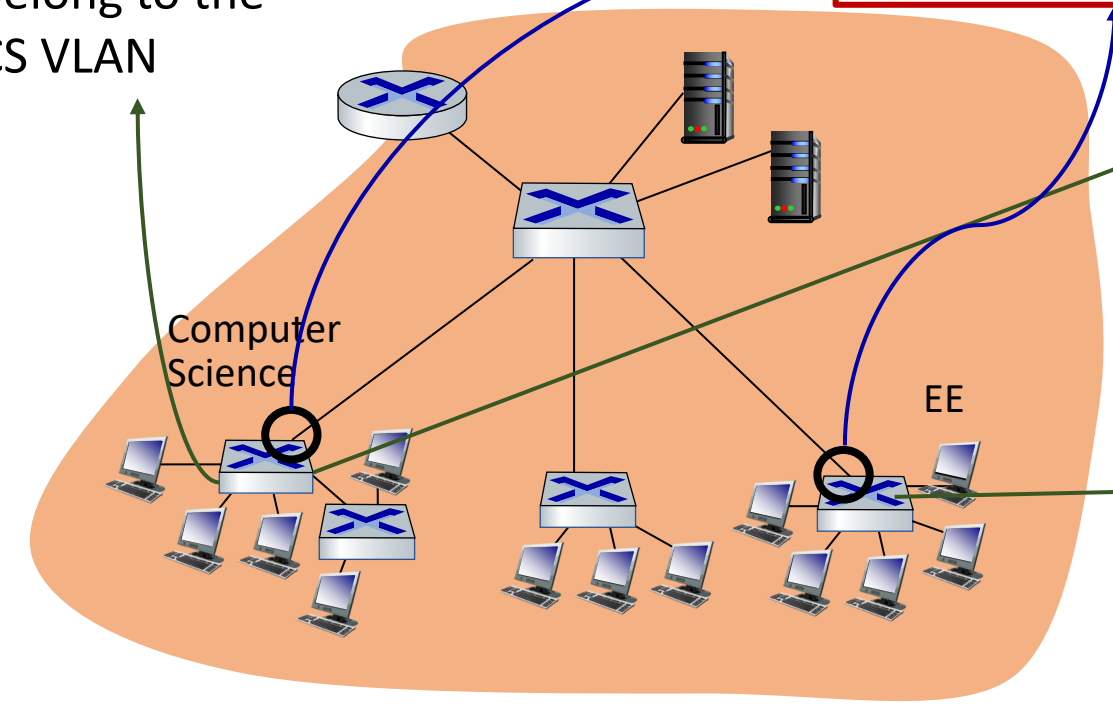



An example institutional network.

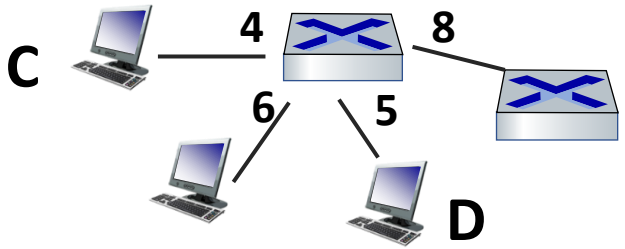
- How do we forward traffic between A and C?
  - Both belong to CS VLAN, not attached to the same switch
- How about between B and D?

All ports belong to the CS VLAN

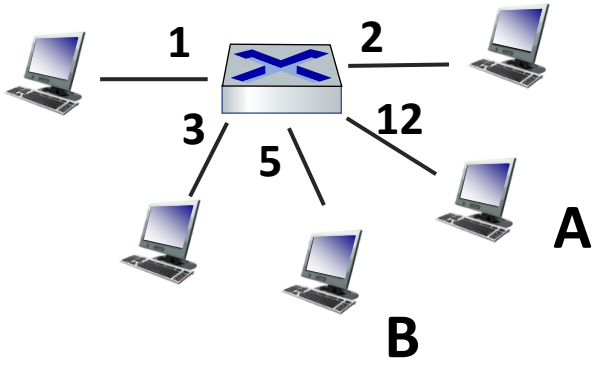
Traffic on these ports can be from multiple VLANs




Ports 4, 6, 7, 8 belong to CS VLAN
Ports 2, 3, 5 belong to EE VLAN

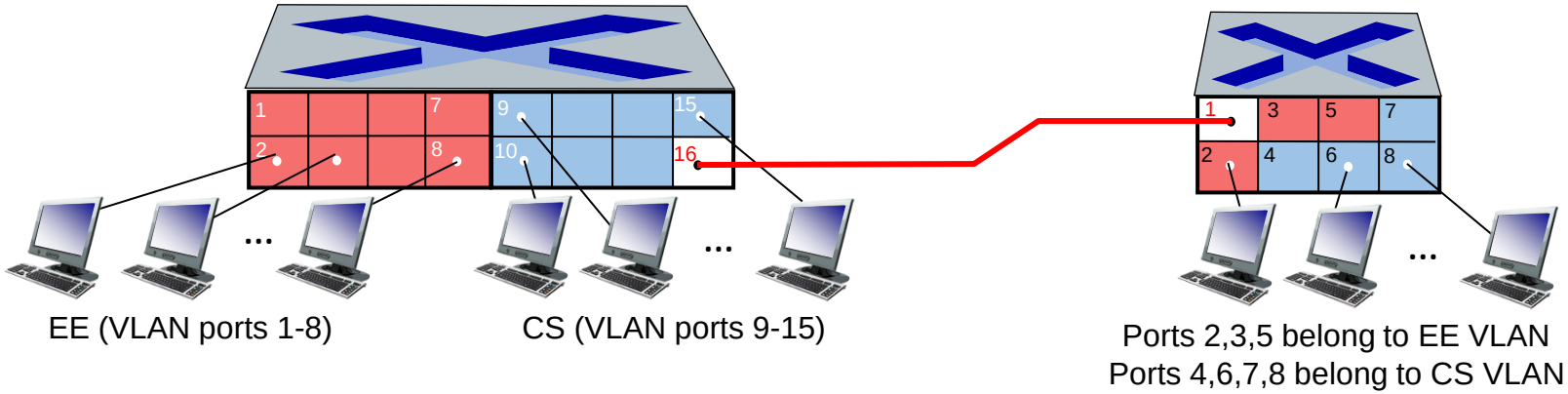



Ports 1-8 belong to the EE VLAN
Ports 9-15 belong to the CS VLAN




An example institutional network.

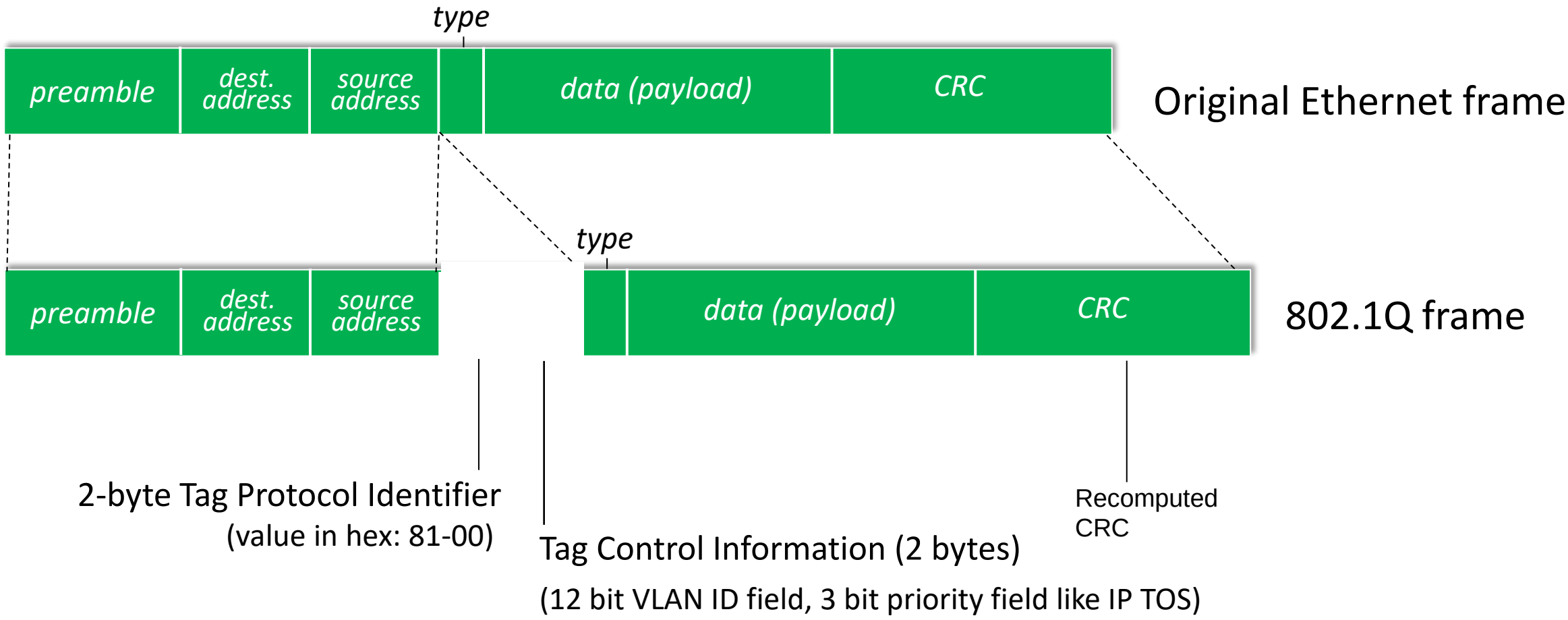
# VLANS spanning multiple switches



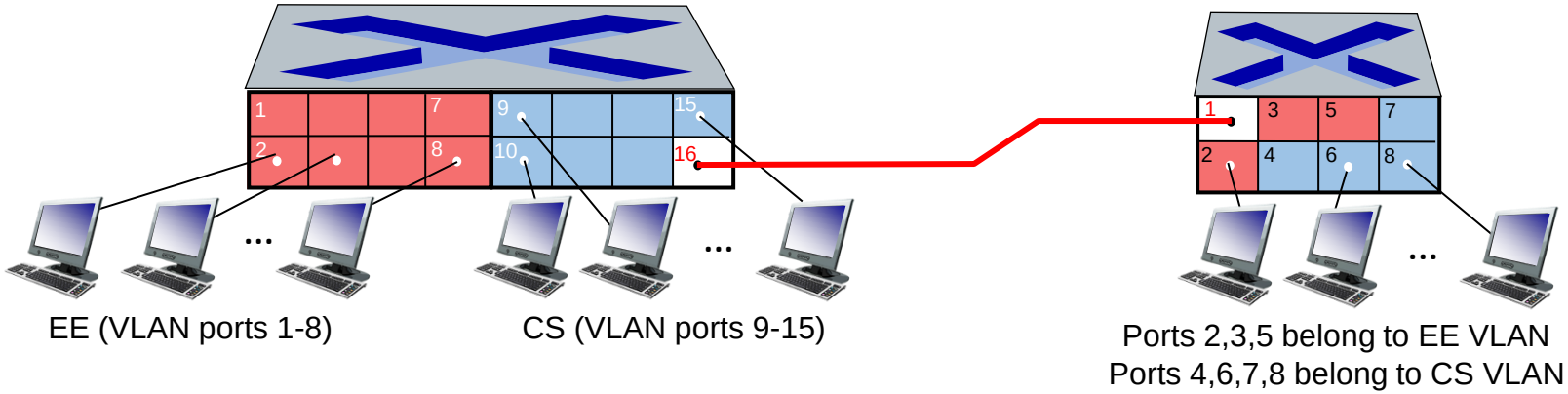

trunk port: carries frames from multiple VLANs

- So, it can help carry frames between users of a VLAN defined over multiple physical switches.
- How do we know which frame belongs to which VLAN?
  - We need extra information in the link layer header.

# 802.1Q VLAN frame format



# VLANS spanning multiple switches



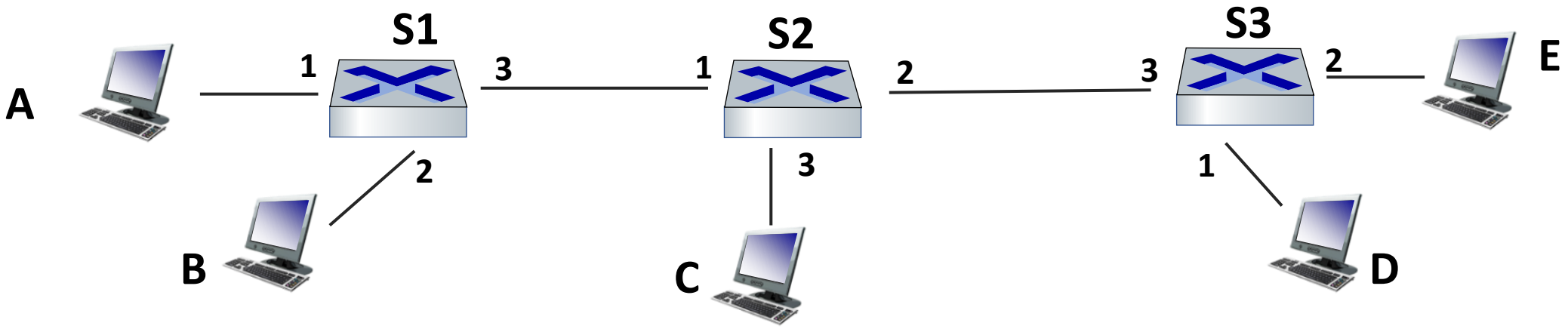

trunk port: carries frames from multiple VLANs

- 802.1q protocol adds/removed additional header fields (i.e., the VLAN tag) for frames forwarded between trunk ports.
- The sending switch will add the tag when sending frames on the trunk port (e.g., switch on the left when sending out of port 16).
- The receiving switch will read (parse) the information and then remove it from the frame (e.g., switch on the right when receiving on port 1).

# Make sure you know

- How traffic is forwarded between endpoints in different VLANs
- How traffic is forwarded between endpoints in the same VLAN
  - When they are attached to the same switch
  - When they are attached to different switches

# VLAN Exercise




- A, C, and D are in VLAN 1, B and E are in VLAN 2.
- For S1, port 1 belong to VLAN 1, port 2 belongs to VLAN 2, port 3 is a trunk port.
- For S2, port 1 is a trunk port, port 2 is a trunk port, port 3 belongs to VLAN 1.
- For S3, port 3 is a trunk port, port 1 belongs to VLAN 1, port 2 belongs to VLAN 2.
- A sends an ARP request to find the MAC address for a certain IP address. For every switch port, find out if the ARP request will be sent out of that port or not, and if yes, does it include a VLAN tag. If yes, include which VLAN the tag represents.
- Do the same exercise for the scenario in which B sends out an ARP request.

# Answer (for A)

- A's ARP request is a broadcast frame. It will enter S1 from port 1.
- S1 will send it only out of port 3
  - Port 2 belongs to a different VLAN. Broadcast frames are not sent to their incoming port.
  - Port 3 is a trunk port, so there will be a VLAN tag for VLAN 1 on the frame.
- S2 receives the ARP request and removes the VLAN tag.
  - It will send it on port 3 as it belongs to VLAN 1. There will be no tag (it is not a trunk port).
  - It will also send it on port 2, with a tag for VLAN 1.
- S3 receives the ARP request and removes the VLAN tag.
  - It will send it on port 1, without a tag.

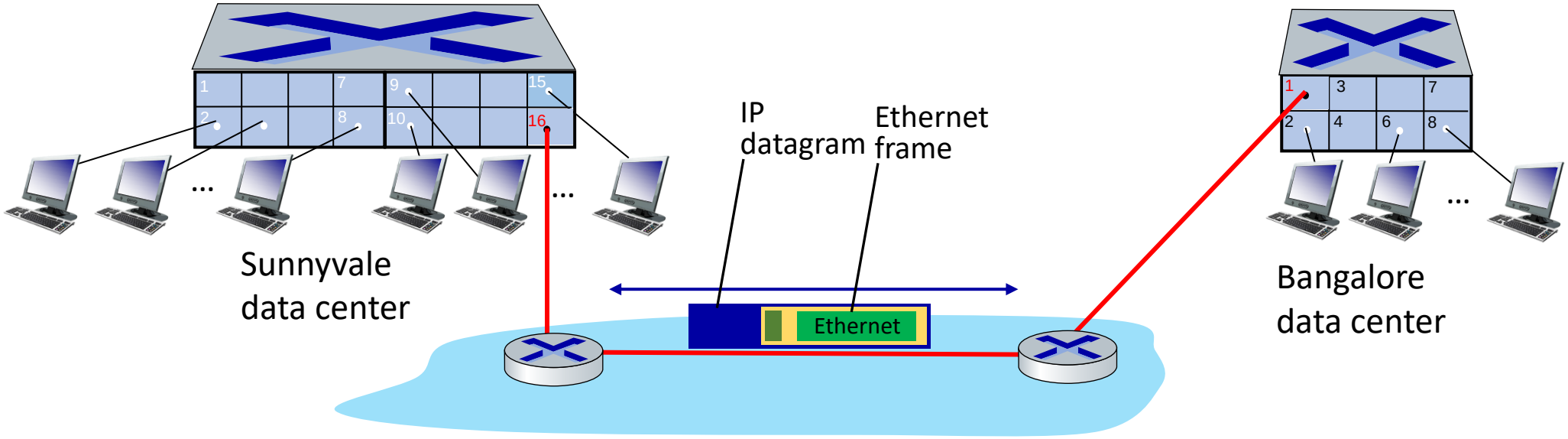
# Answer (for B)

- B's ARP request is a broadcast frame. It will enter S1 from port 2.
- S1 will send it only out of port 3
  - Port 1 belongs to a different VLAN.
  - Broadcast frames are not sent to their incoming port.
  - Port 3 is a trunk port, so there will be a VLAN tag for VLAN 2 on the frame.
- S2 receives the ARP request and removes the VLAN tag.
  - It will only send it on port 2, with a tag for VLAN 2.
- S3 receives the ARP request and removes the VLAN tag.
  - It will send it on port 2, without a tag.

# EVPN: Ethernet VPNs (aka VXLANs)

- In our example institutional network, a CS user could move to a different buildings *inside* the campus and, using VLANs, still have the "illusion" of being part of the CS L2 network.
- What if the user goes home and still wants to be part of the CS L2 network?
  - Why? E.g., if you want to access some server on campus, you need to be "inside" the campus network.

# EVPN: Ethernet VPNs (aka VXLANs)




Layer-2 Ethernet switches *logically* connected to each other (e.g., using IP as an *underlay*)

- Ethernet frames carried *within* IP datagrams between sites
- "*tunneling* scheme to *overlay Layer 2 networks on top of Layer 3 networks* ... runs over the existing networking infrastructure and provides a means to "stretch" a Layer 2 network." [RFC 7348]

# What you need to know about EVPNs

- Nothing for exam purposes ☺