Computer Networking

COMP 177 | Fall 2020 | University of the Pacific | Jeff Shafer

Virtual LANs (VLANs)

Recap

Past Topics

- Overview of networking and layered architecture
- Wireshark packet sniffer
- Ethernet and WiFi
- IPv4
- ARP

Today's Topics

- Virtual LANs (VLANs)

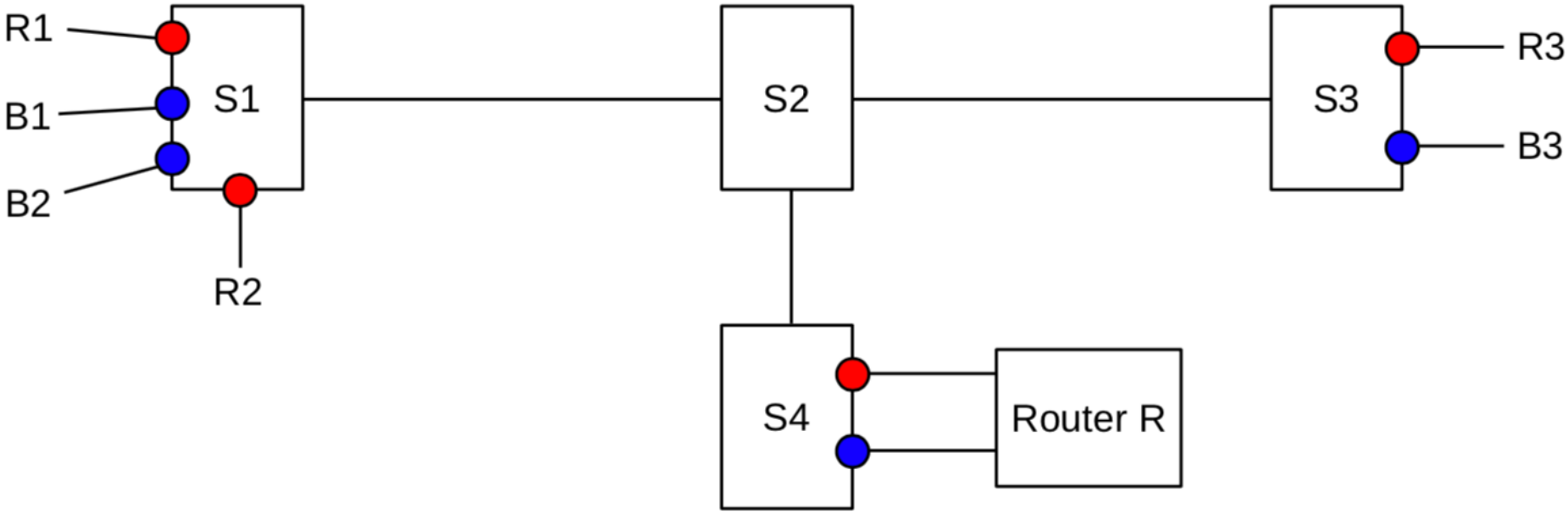
Motivation for VLANs

- Consider a multi-story building of a company
- Each story has its own physical LAN
- All these LANs are connected to each other through a router
- Each team within the company wishes to have their own LAN
  - Isolation / security?
- This means that each team must be assigned to a different story of the building
  - Physical properties of the environment limit the configuration
- Solution: Virtual LANs (VLANs)

VLANs

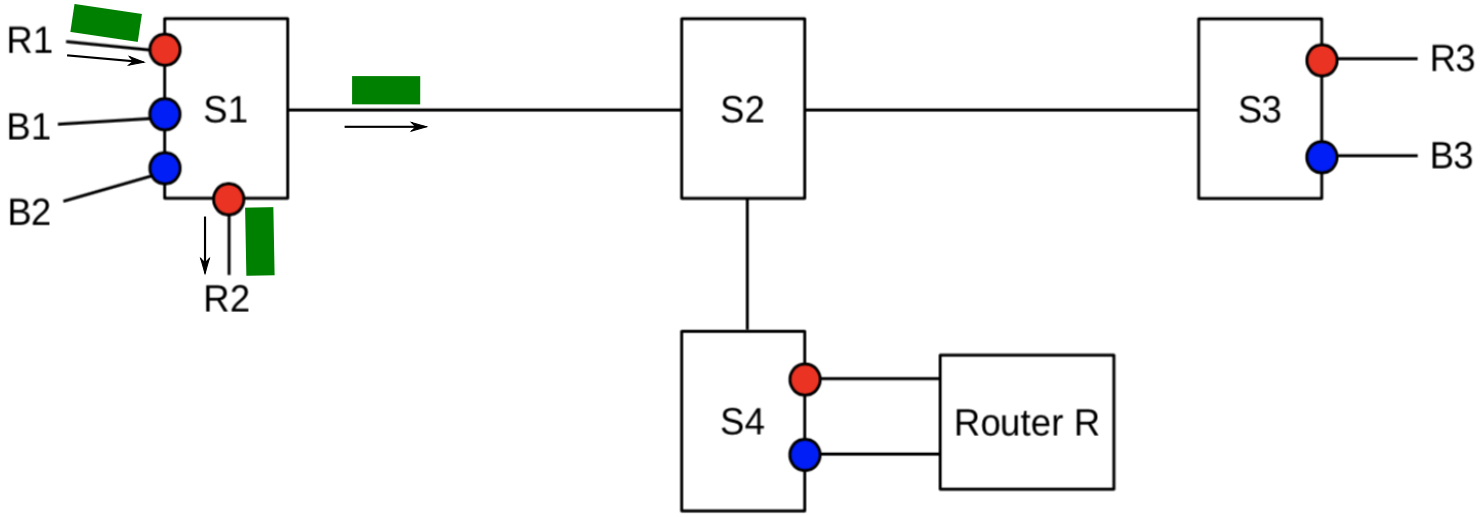
- Virtual LANs have similar features to LANs
  - A VLAN defines a *broadcast domain*
  - A VLAN has a *single IP subnet*
  - The traffic between two VLANs is *routed*
- Multiple VLANs can be defined within a single physical LAN
- VLANs can be visualized and designed by coloring, where each color represents a single VLAN
  - We logically assign all nodes on the same VLAN the same color, and switches forward packets accordingly

VLAN Example



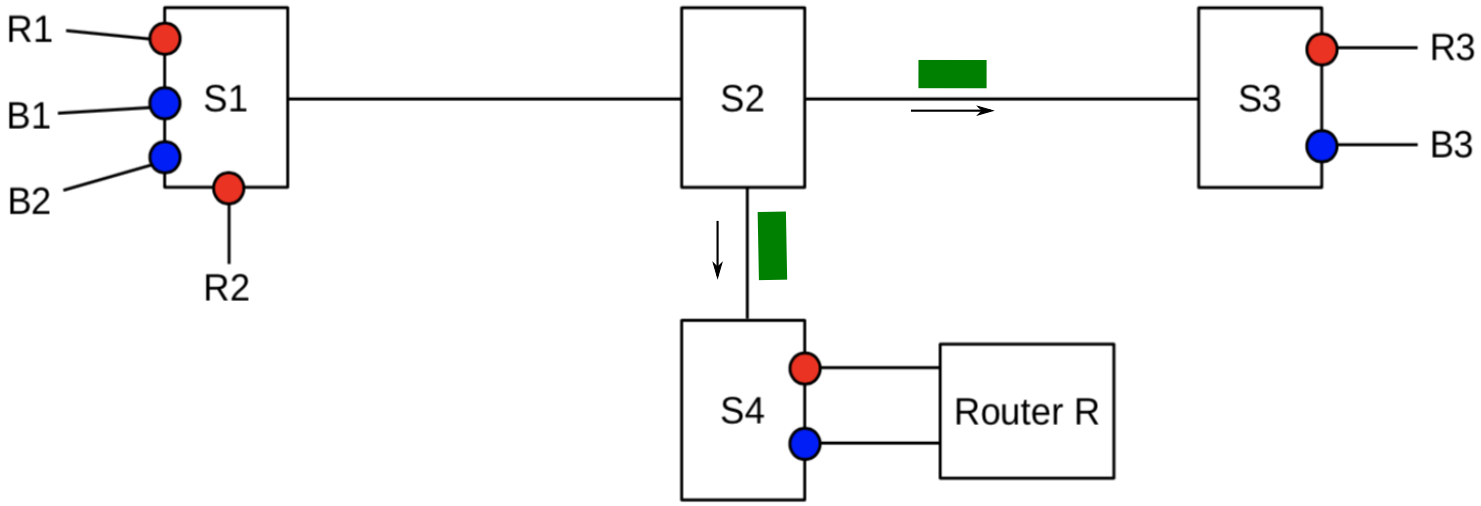
- A single physical switched LAN divided into two VLANs: **Red** and **Blue**
- A switch may physically connect nodes from different VLANs

Example 1: Communication Within VLAN



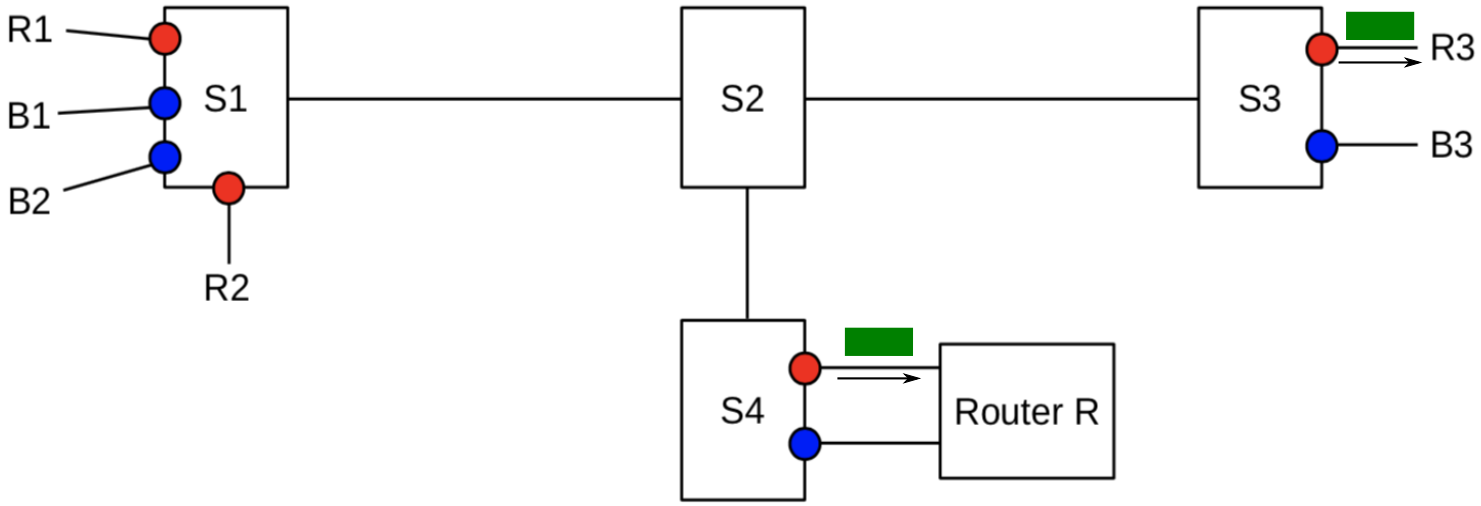
- Switches apply *port-based policy* to deliver *broadcast* packets
- Suppose R1 wants to broadcast a packet. Since R1 is in the **red** VLAN:
  - S1 forwards the packet through the port connected to R2
  - S1 does not forward the packet through the ports connected to B1 and B2
  - S1 forwards the packet through the port connected to S2, since that is not colored

Example 1: Communication Within VLAN



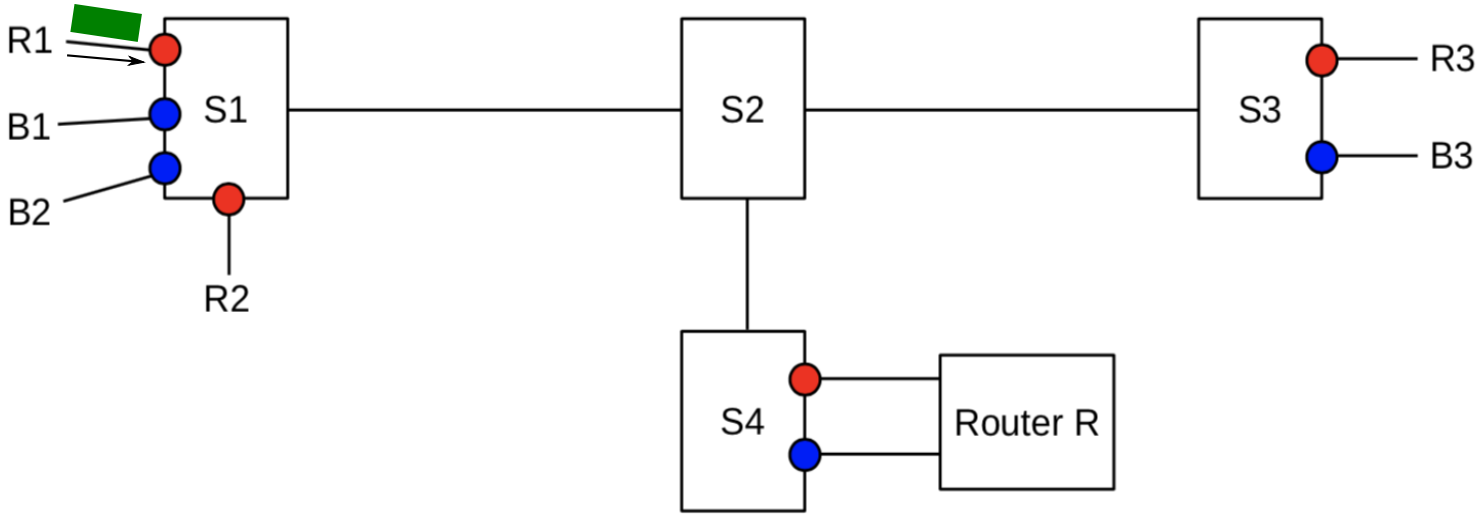
- Switches apply *port-based policy* to deliver *broadcast* packets
- Suppose R1 wants to broadcast a packet. Since R1 is in the **red** VLAN:
  - S2 forwards the packet through the two other ports, since none of them are colored

Example 1: Communication Within VLAN



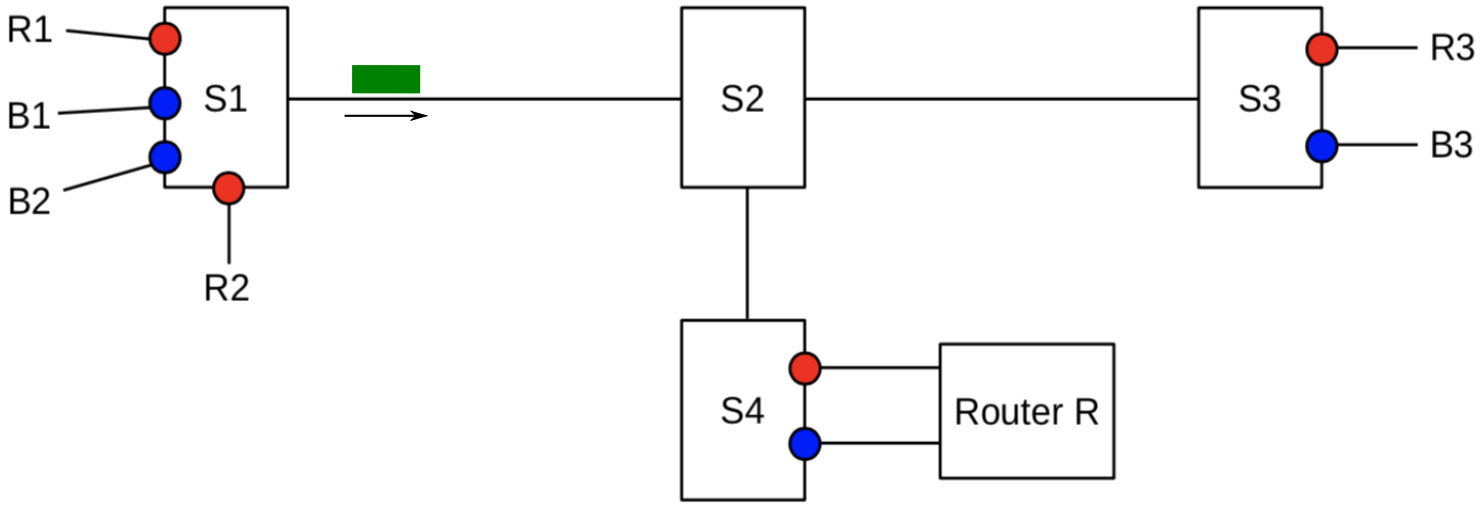
- Switches apply *port-based policy* to deliver *broadcast* packets
- Suppose R1 wants to broadcast a packet. Since R1 is in the **red** VLAN:
  - S3 forwards the packet through the port to R3, but not the port to B3
  - S4 forwards the packet through the red port connected to RouterR, but not the blue port connected to RouterR

Example 2: Communication Within VLAN



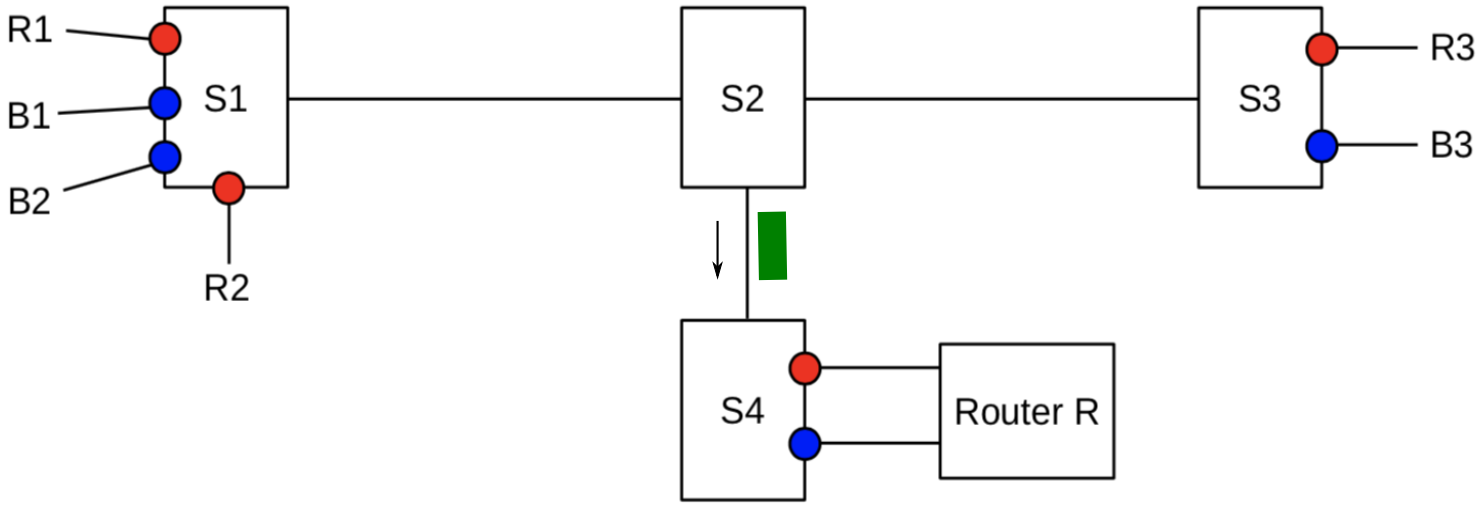
- Switches apply *port-based policy* to deliver *unicast* packets
  - R1, R2, and R3: Default gateway is router port connected to red link
  - B1, B2, and B3: Default gateway is router port connected to blue link
- For example, suppose R1 wants to send a packet to B1
  - R1 sends the packet to S1

Example 2: Communication Within VLAN



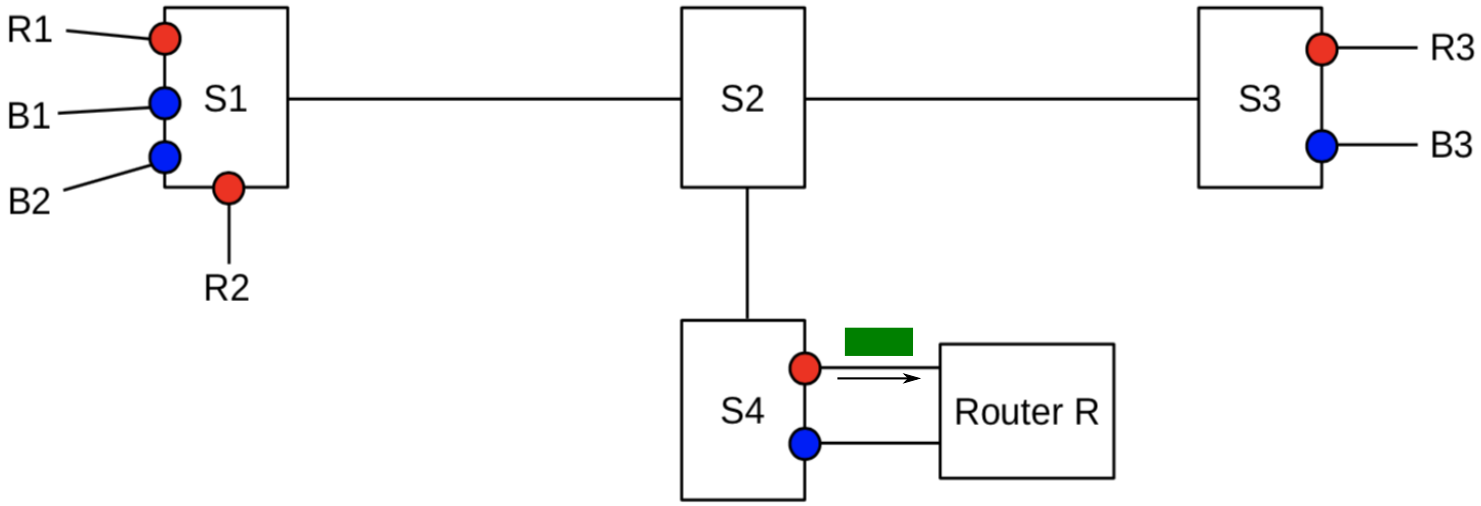
- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - S1 forwards the packet to S2

Example 2: Communication Within VLAN



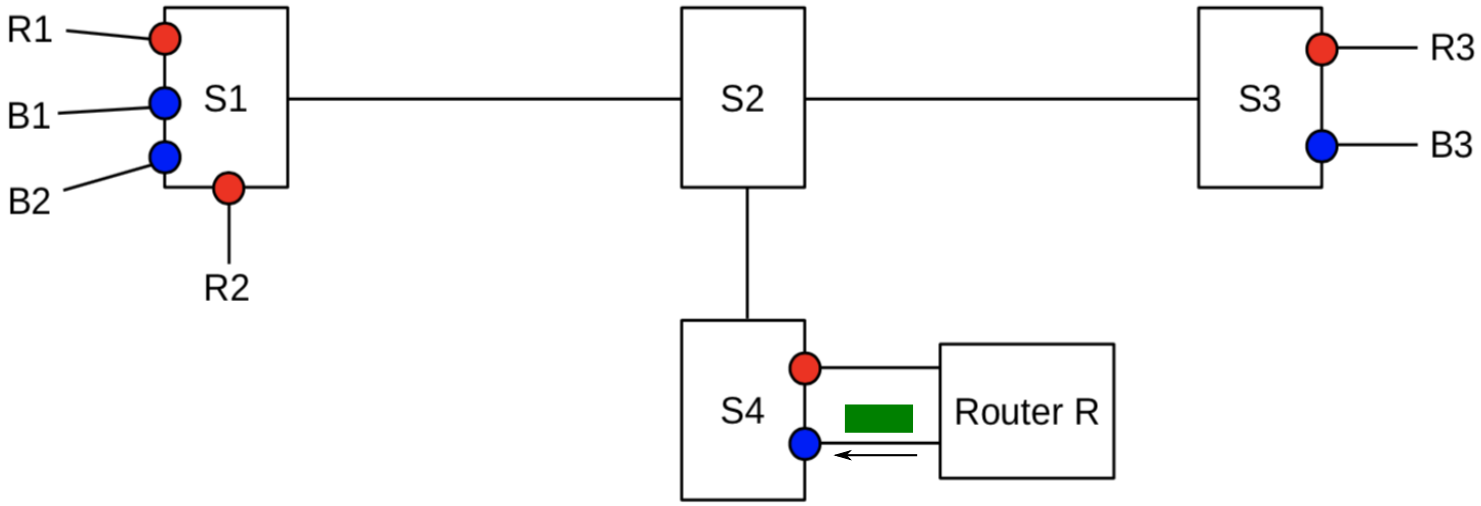
- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - S2 forwards the packet to S4

Example 2: Communication Within VLAN



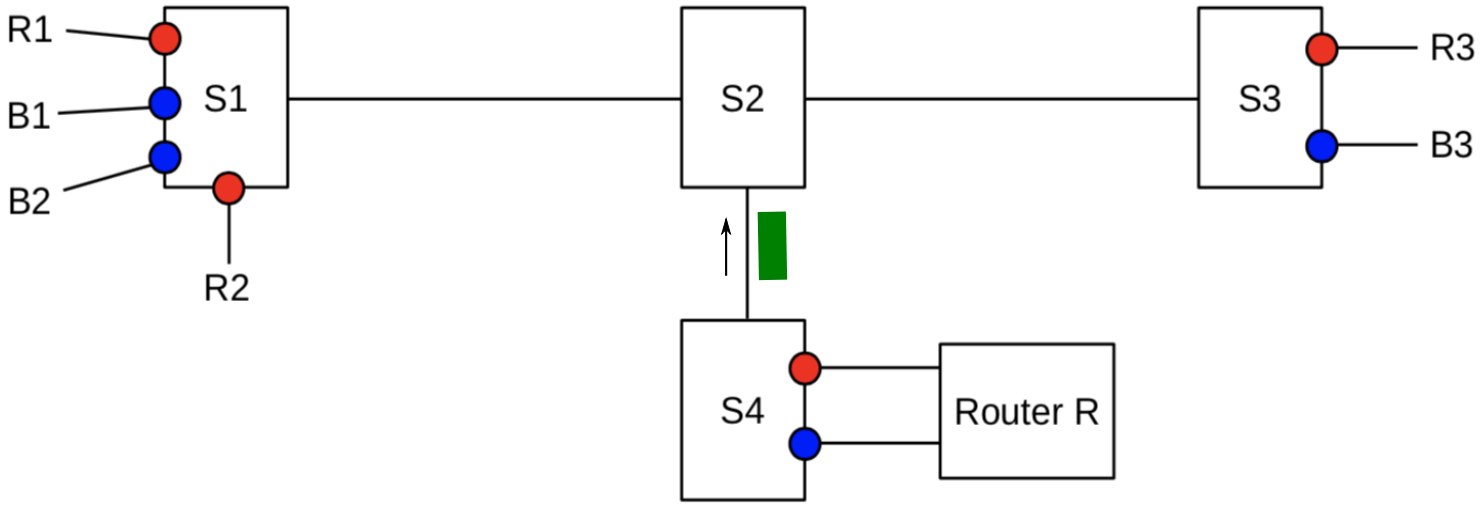
- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - S4 forwards the packet to RouterR through the red port

Example 2: Communication Within VLAN



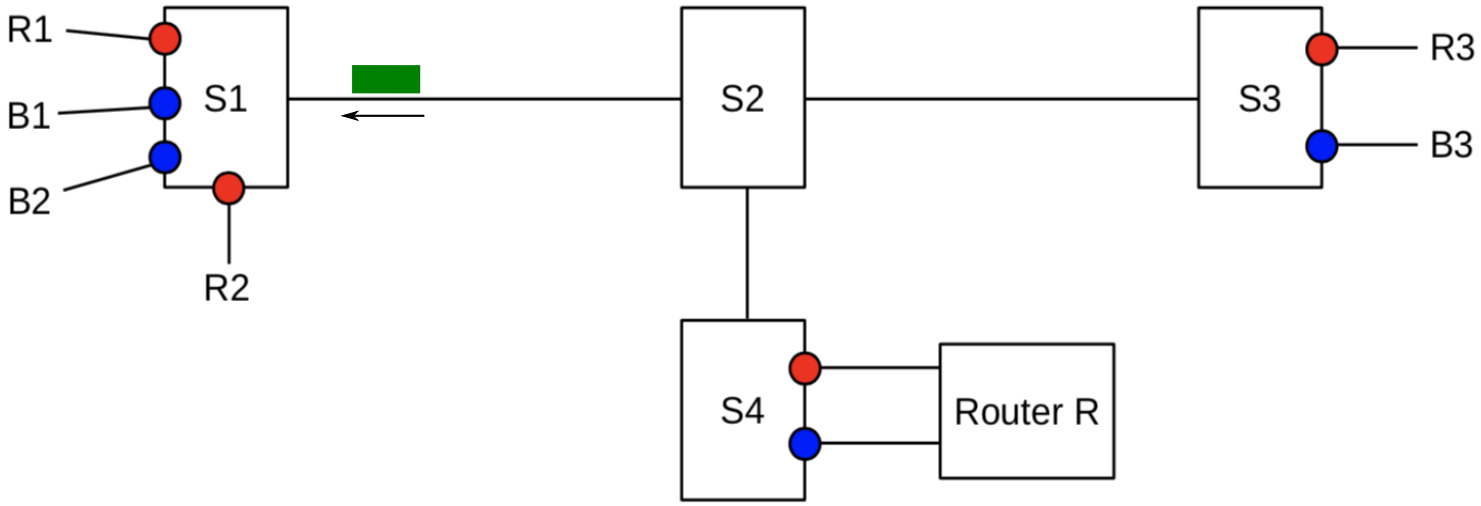
- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - RouterR routes the packet to the other VLAN, i.e., blue VLAN

Example 2: Communication Within VLAN



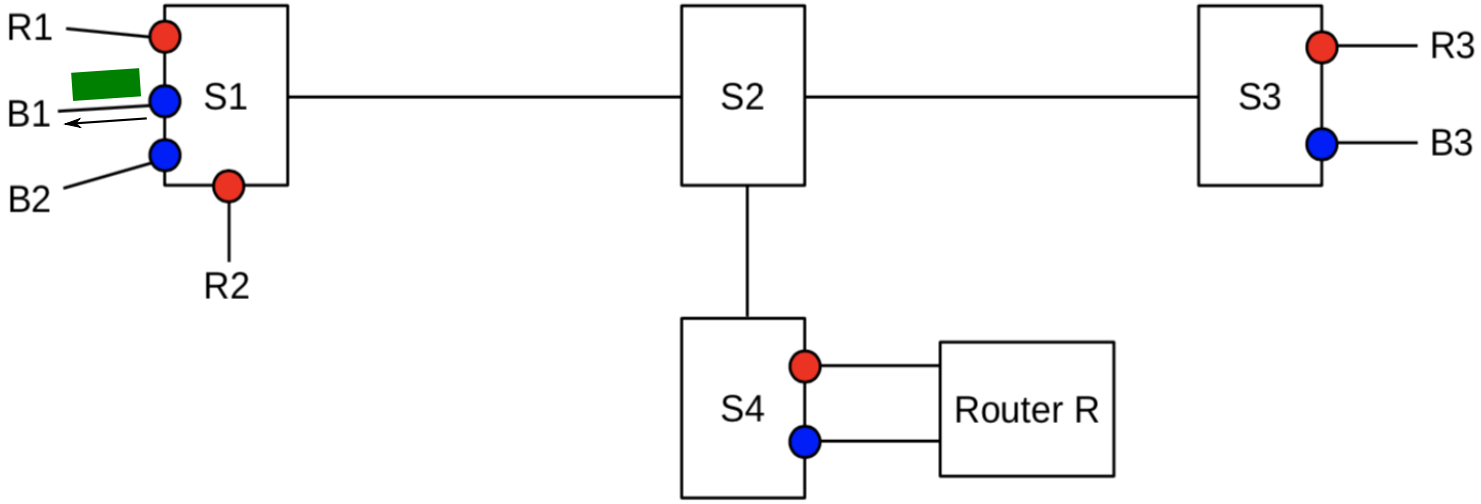
- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - S4 forwards the packet to S2

Example 2: Communication Within VLAN



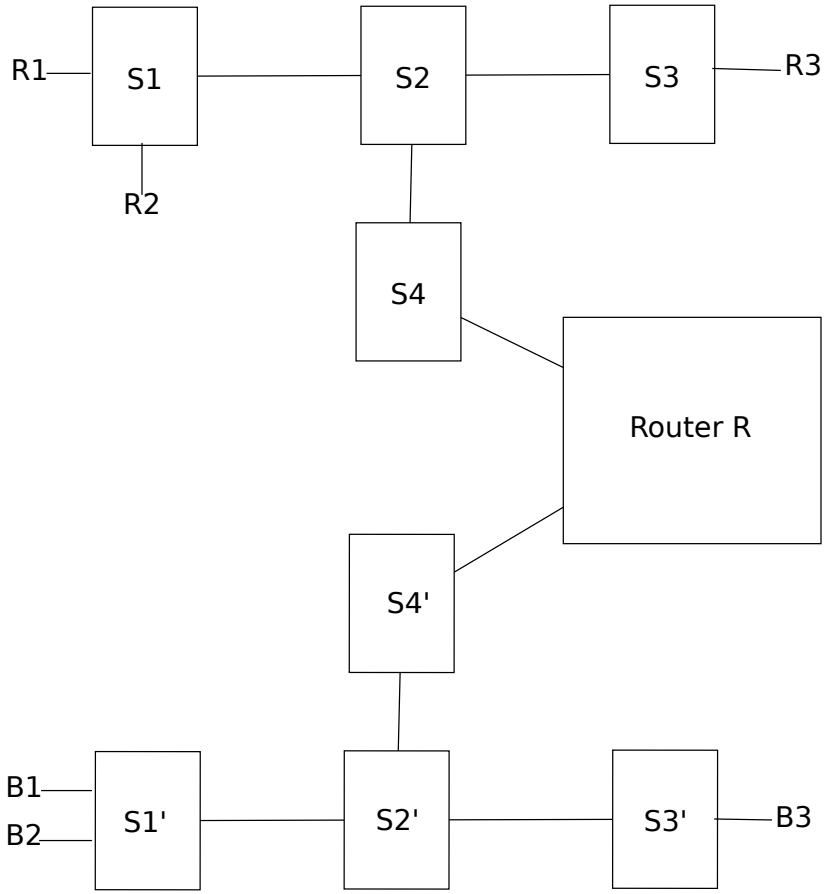
- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - S2 forwards the packet to S1

Example 2: Communication Within VLAN



- Switches apply *port-based policy* to deliver *unicast* packets
- For example, suppose R1 wants to send a packet to B1
  - S1 forwards the packet to B1

Example 2: Communication Within VLAN



- The two VLANs are imitating this physical network

VLAN ID

- Colors denote identifiers for VLANs
- In a virtual LAN network, this VLAN ID needs to be communicated as part of the data link frame header to facilitate the communication between
  - Two nodes on different VLANs (Example 2)
  - Two nodes on the same VLAN, but connected to different switches (Example 1)
- This way, the switch can determine whether the packet should be forwarded
  - Through a router
  - Through switch
  - To its destination

IEEE 802.1Q

- The protocol for virtual LANs is specified in protocol IEEE 802.1Q as an *extension* to link layer protocols, like 802.3 and 802.11.
- IEEE 802.1Q adds an additional 32-bit collection of header fields:

IEEE 802.1Q

- **Tag Protocol ID** (TPID), 16 bits: The protocol that is used for tagging
  - For IEEE 802.1Q the value is 0x8100, asserting that tagging is for VLAN identifier.

IEEE 802.1Q

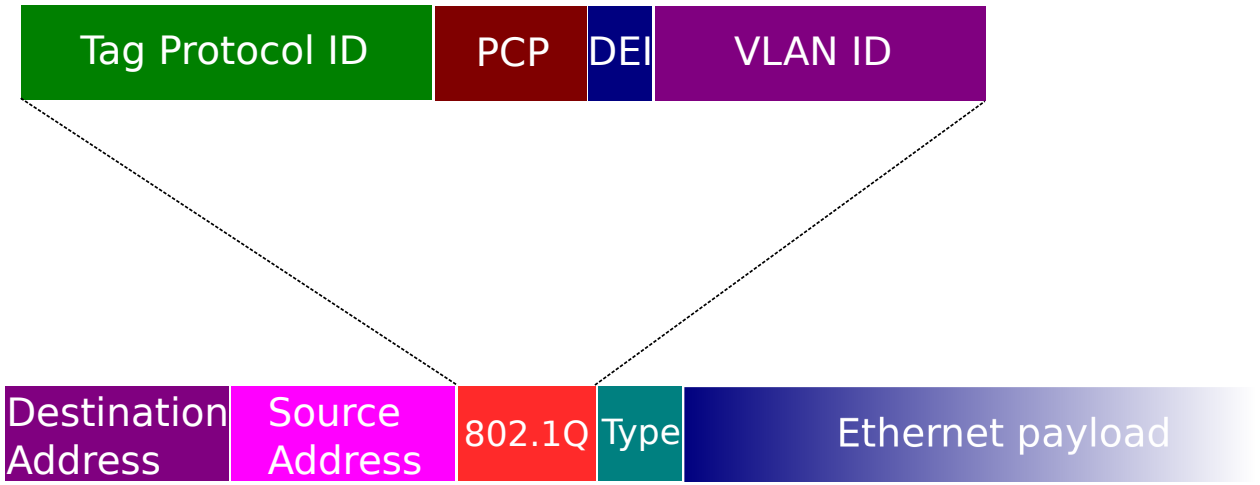
- **Priority Code Pointer (PCP)**, 3 bits: A priority value that switch can use in order to forward the frame
  - Theoretically, different types of traffic can have different priority values
  - The default priority level is 0, which is the lowest of 8 possible levels

IEEE 802.1Q

- **Drop Eligible Indicator (DEI),** 1 bit: indicates that the frame can be dropped in case of congestion
- **VLAN ID**, 12 bits: Each VLAN has its own identifier
  - There are two specific VLAN IDs:
    - 0x000: the frame does not belong to any VLAN
    - 0xFFF: reserved
  - $2^{12} - 2 = 4094$ VLANs within a physical LAN

VLAN in Ethernet

- The VLAN tag is inserted into the Ethernet header between the Source MAC and the type field
  - Tag Protocol ID field of the 802.1Q becomes the type for 802.3, and thus specifies the payload of Ethernet frame as 0x8100
  - The original type field of Ethernet now specifies the payload for 802.1Q, e.g., it can be 0x0800 for IP datagrams



Closing Thoughts

Recap

- Today we discussed VLANs
  - Why we need them
  - How they work
  - 802.1Q header format

Next Class

- ICMP

Class Activity

CA.10 – VLANs & Wireshark

Due tonight at 11:59pm

Homework 2

Due Oct 2nd at 11:59pm

Project 1

Due Sept 30th at 11:59pm