# CS183

Instructor: Ali Davanian
(Slides were adopted from Brian Crites and Alireza Abdoli)

# L1 and L2 Networks

# Introduction

- Network devices operate at different levels (layers)
- We use $L_x$ or Lx to denote the level a device operates at
- A device operating at layer $L_x$ can understand layers<x
    - A L3 device often will not understand layer 4 protocols
    - A layer 3 device might understand the lower levels, and provide functionalities for that level.
- In this lecture we will cover L1 and L2 network appliances

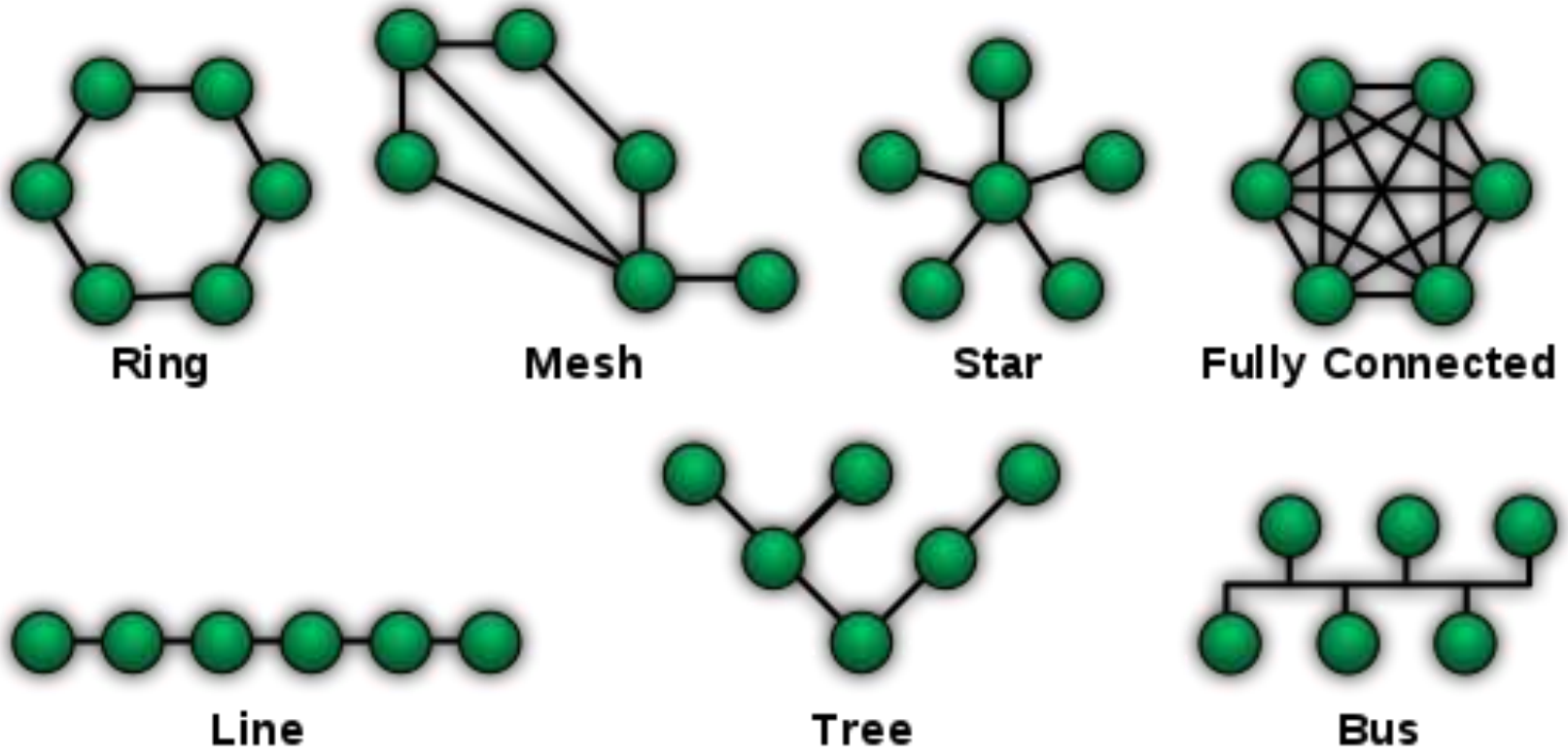
# L1 Network Appliances

- Hardware that functions on the the L1 (physical) layer (though not necessarily exclusively)
  - Routers
  - Switches
  - **Hubs**
  - **Repeaters**
- If it moves traffic but doesn’t make any decisions about it, it’s L1

# L2 Network Appliances

- Hardware that functions on the the L2 (data link) layer (though not necessarily exclusively)
  - Routers
  - **Switches**
- Responsible for sending specific frames through specific ports
- Capable of determining what MAC addresses it is connected to

# Basic Topologies

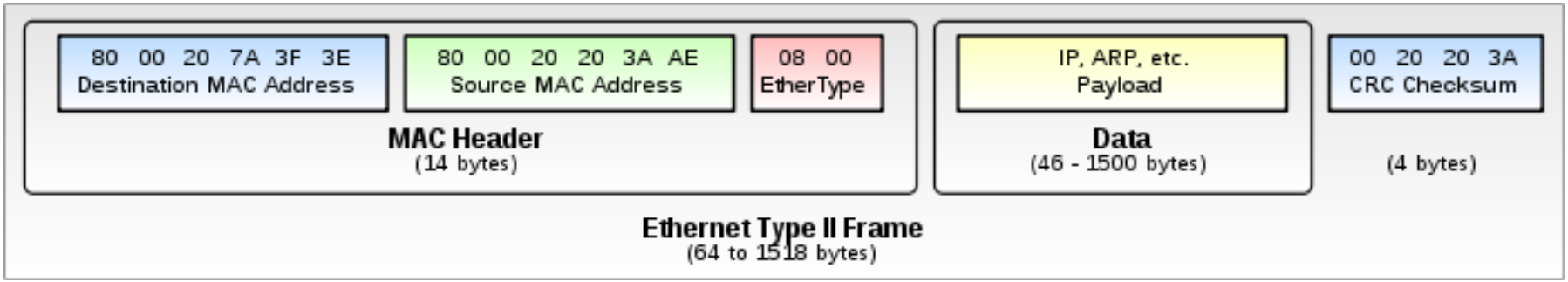


# Data Link Layer (L2) Sublevels

- The data link layer is actually broken down into two sublayers, although we typically discuss them as a single level
  - Logical Link Control (LLC) Layer: responsible for multiplexing, error management, and congestion management (exponential backoff)
  - Media Access Control (MAC) Layer: responsible for addressing data (source and destination) and encapsulation of incoming data in a frame
- The logical link control typically deals with the L1 physical connection below the L2 data link layer while the media access control layer deals with the L3 IP layer (but they interface with each other to perform the L2 functionality)

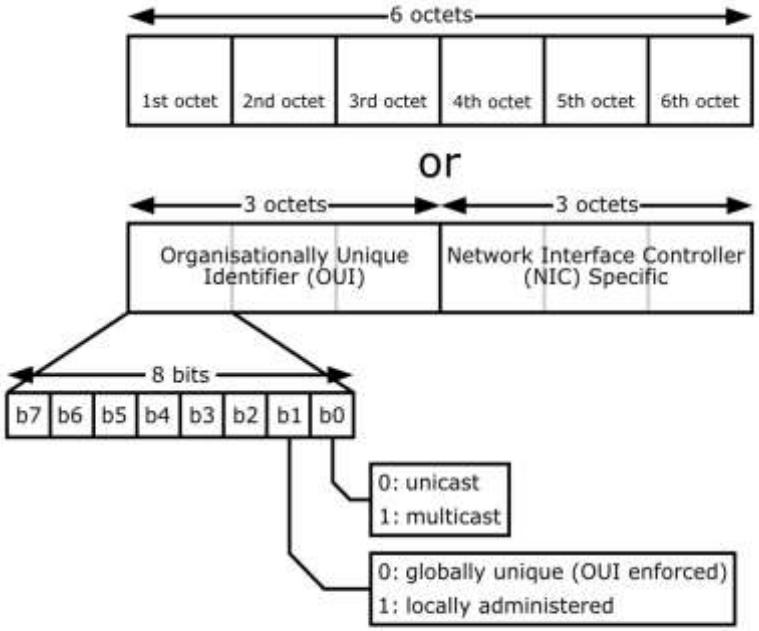
# MAC Address

- “Unique” and “immutable” address for a **network interface** set by the manufacturer used to communicate across the network
- Use the `ifconfig -a` command to find your MAC address on Linux
- Pseudo-immutable and unique because it can usually be modified
- Frames contain both a source MAC address for the device creating the frame and a destination MAC address for where the frame will be sent



# MAC Address

- Specified in six groups of hex pairs separated by colons (C0:3F:0E:23:AA:C2)
- The first three pairs make up the Organizational Unique Identifier (OUI) which identifies the manufacturer (C0:3F:0E)
- The second three pairs make up the Network Interface Controller (NIC) which represents the device (23:AA:C2)



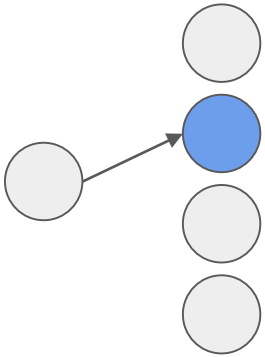
# Anatomy of a Frame

| Preamble | Destination | Source | Type | Data | Frame Check Sequence |
|---|---|---|---|---|---|
| 8 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 46-1500 bytes | 4 Bytes |

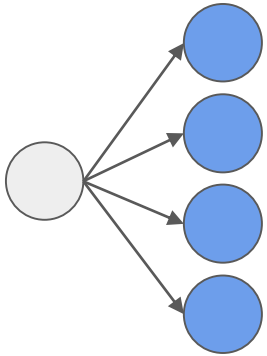
- Preamble: synchronization, delimiter to mark end of timing info
- Destination: 48-bit MAC address of destination
- Source: 48-bit MAC address of source
- Type: which upper layer will receive the data after Ethernet is done
- Data: this is the PDU, encapsulating an IP packet
- FCS: used in error detection to check for damaged frames

# Types of Network Communication

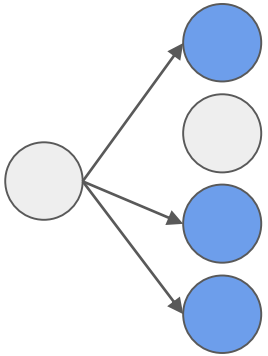
- **Unicast**: direct one-to-one communication between devices on a network



- **Broadcast**: communication to all devices connected to on a network



- **Multicast**: one-to-many communication to a subset of devices on a network



# Switching mechanism at layers 2

How can two devices connected to a switch communicate?

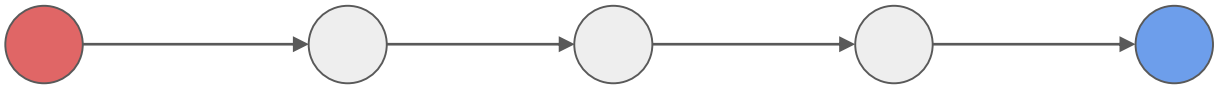
# Switching Table

- L2 communication is possible because each device that works on L2 keeps an internal switching table that lists the different MAC addresses associated with each port on the device
- This allows the device to know who it can communicate with (over L2) and what port it should put the frame on to perform the communication

| Record ID | Port | MAC Address |
|---|---|---|
| 1 | 4 | 0A:5C:44:BB:81:A5 |
| 2 | 7 | 60:AB:1C:43:19:55 |
| 3 | 12 | B9:12:34:56:78:90 |

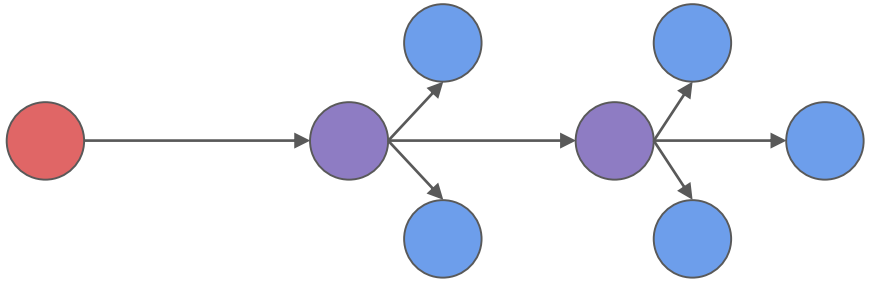
# Unicast

- The host (or appliance) sending the packet signs its own MAC address (which is baked in by the manufacturer) to the frame
- The host (or appliance) uses its internal list of all devices connected over L2 in order to sign the destination MAC address
- Because of the nature of an L2 network, every device connected to the same L2 network knows the MAC addresses of all other devices, and what network interface to use in order to communicate with that device

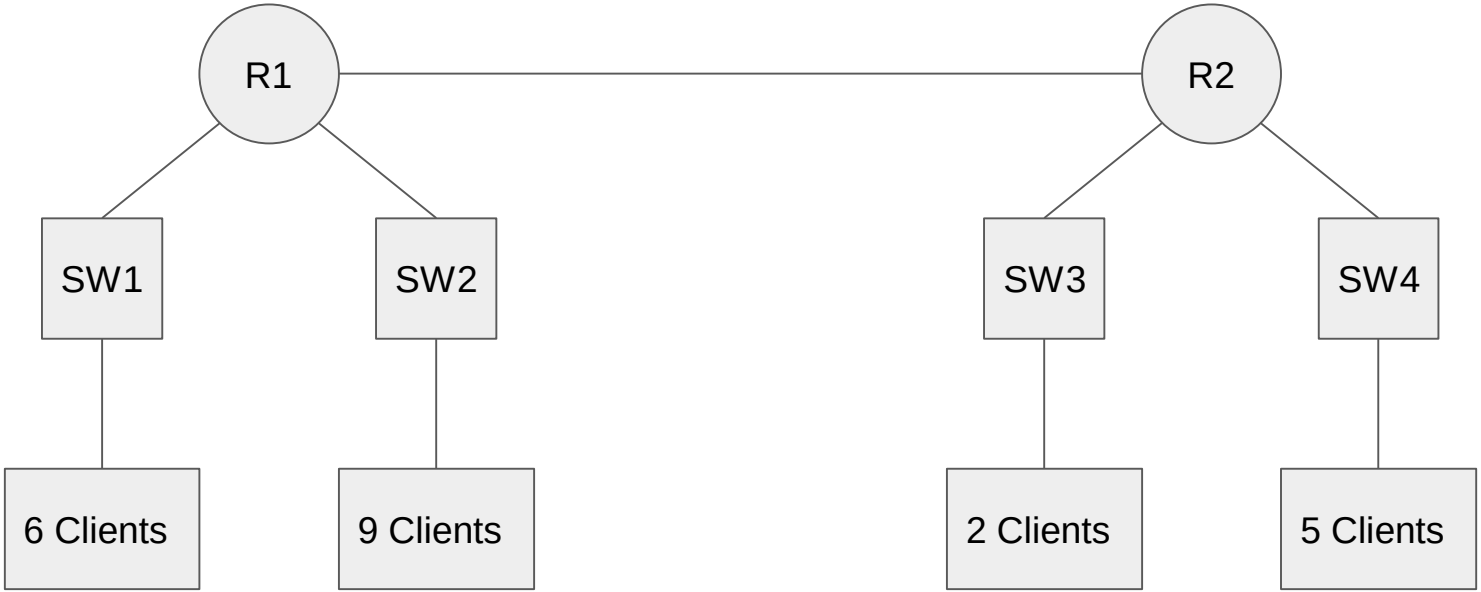


# Broadcast

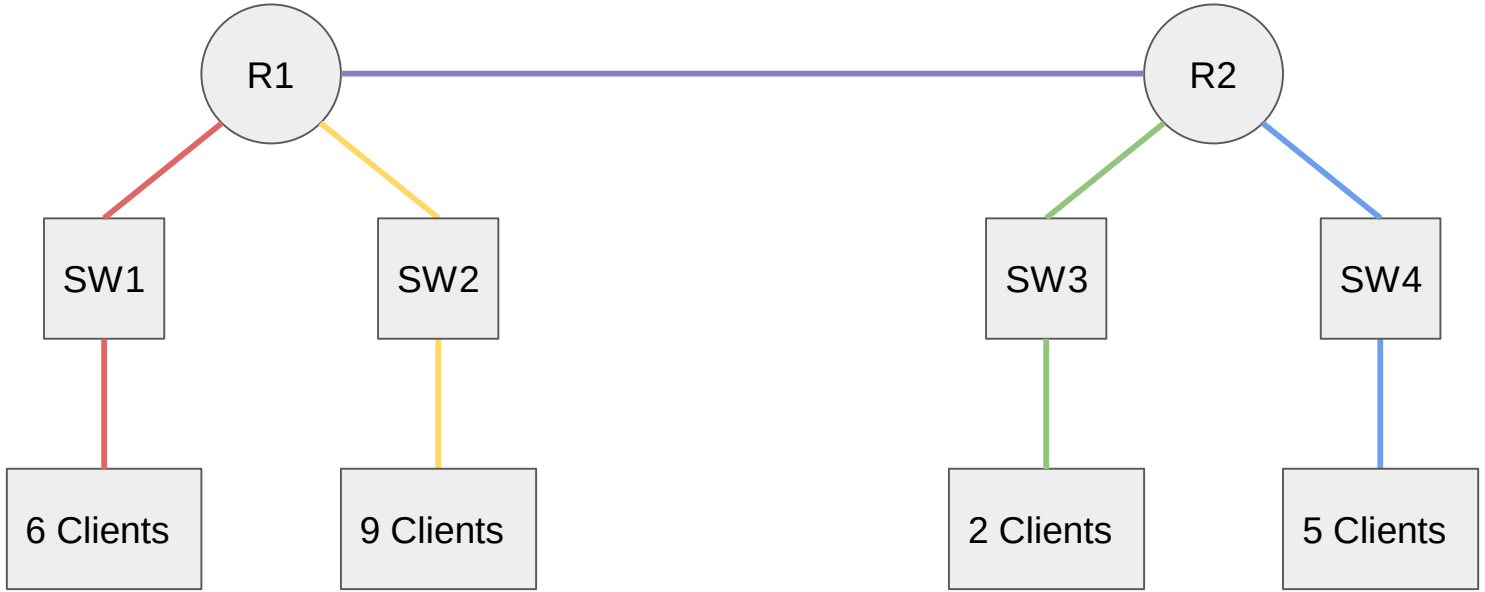
- A method to send out a packet that all devices on the network will respond to (unless otherwise configured)
- Allows for hosts to discover what other devices are attached to the network, their MAC addresses, and what network interface to use to communicate with them (uses special destination FF:FF:FF:FF:FF:FF)
- A **broadcast domain** is a logical division of a computer **network**, in which all nodes can reach each other by broadcast at the data link layer
- Broadcast is used to fill the switching tables of devices connected to the network (that are not connected directly to the device)



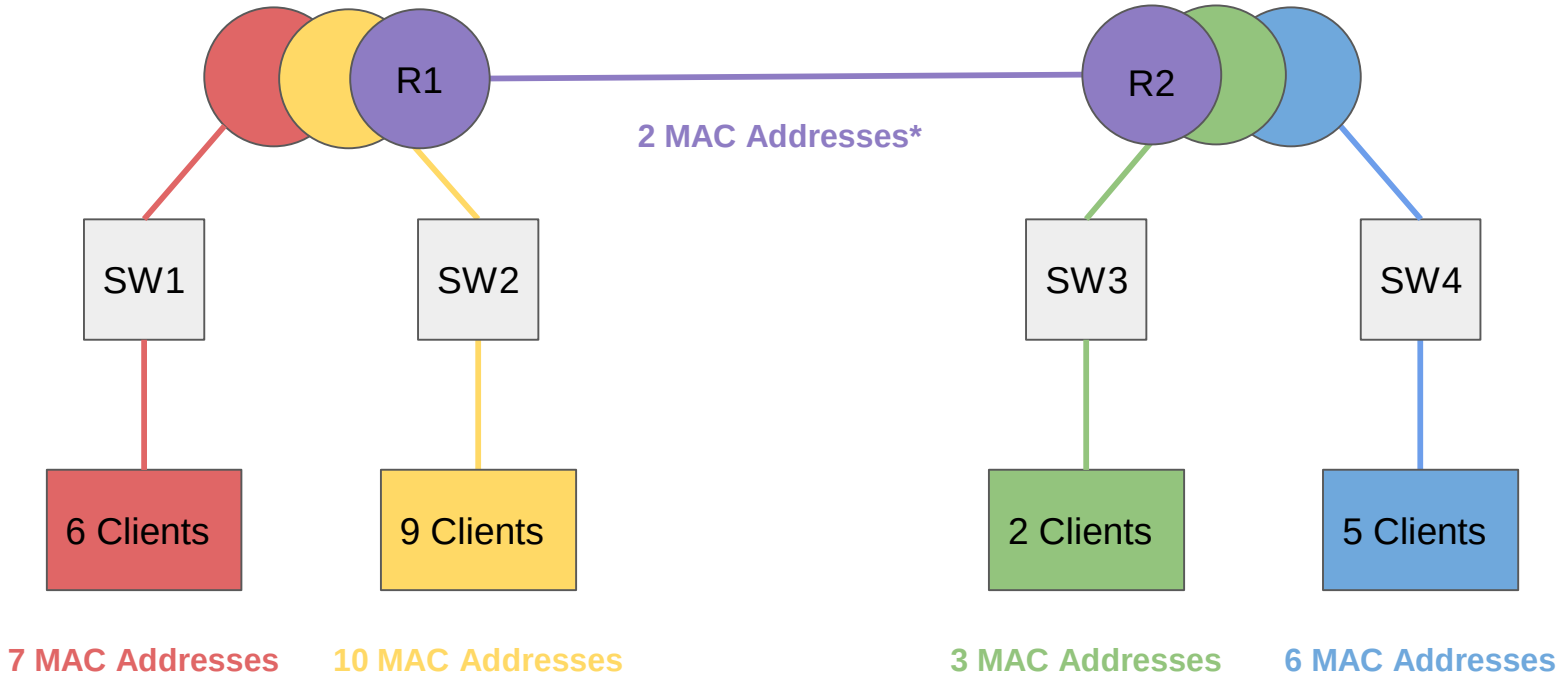
# Count the Broadcast Domains



# Count the MACs per domain



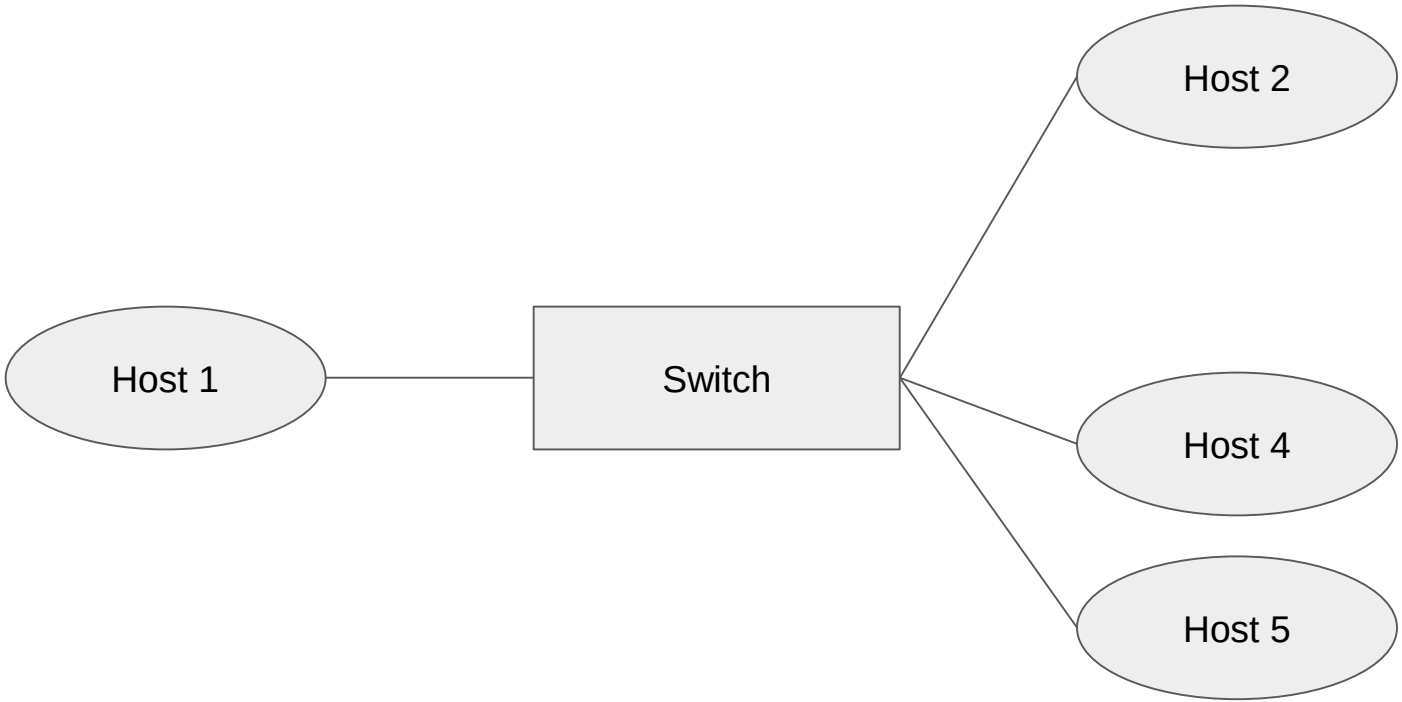
# Count the MACs per domain



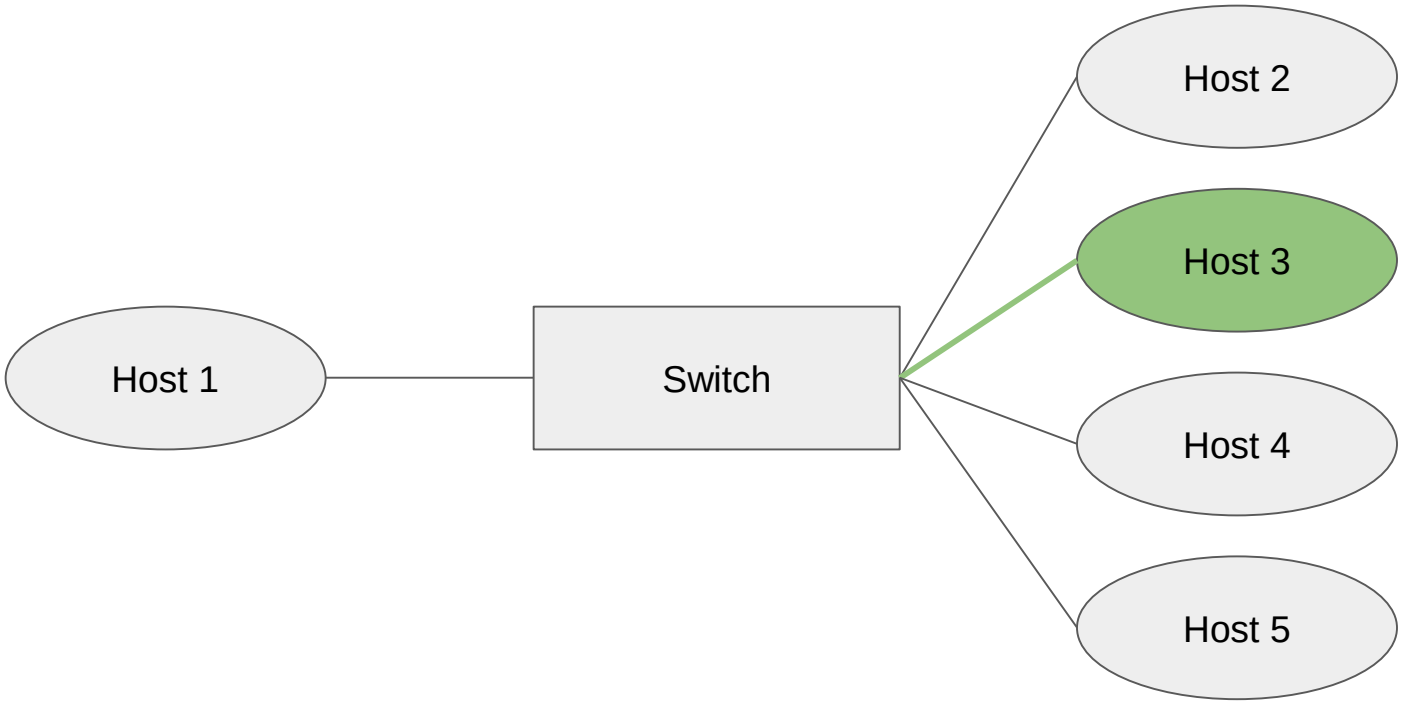
# Address Resolution Protocol (ARP)

- Uses broadcasts to request the MAC address for other network interfaces on the network (usually occurring when a device knows the IP address of another machine on the network, but not its MAC address)
- Sends out a broadcast request which is only responded to by the network interface specified in the request (all others ignore the request)
- When network interfaces are added to the network, it can also send out an ARP announcement which is a broadcast with the broadcasters MAC address which is intended to update the switching tables of all other network interfaces on the network

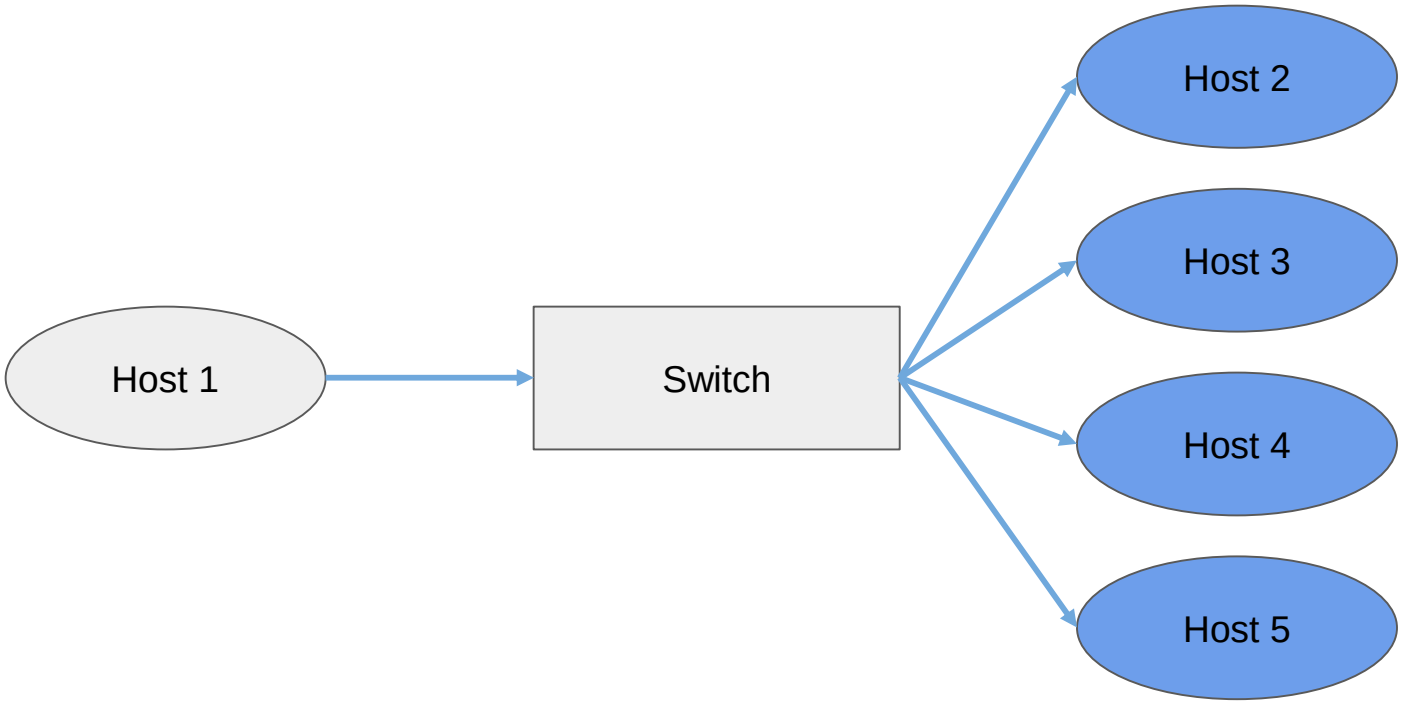
# ARP Resolution



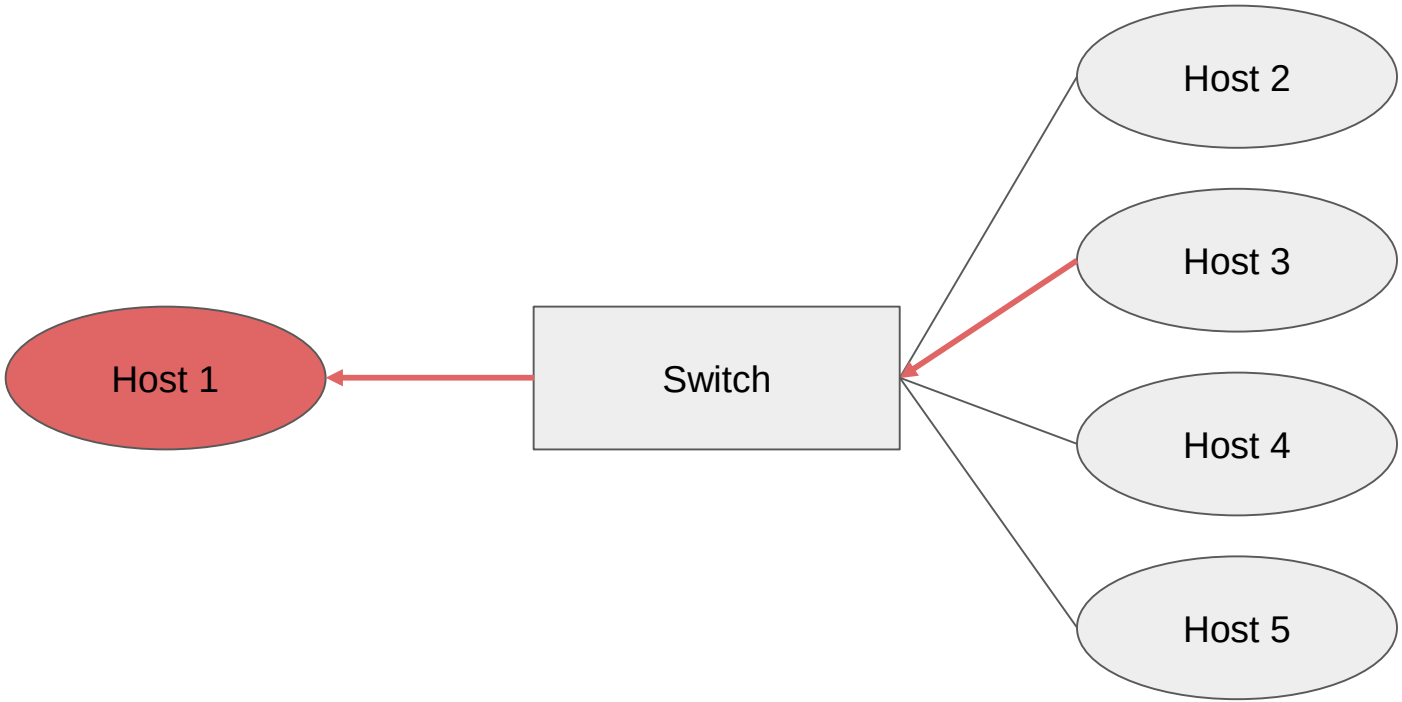
# ARP Resolution



# ARP Resolution



# ARP Resolution



# L2 Loops and Broadcast Storms

- By default frames do not time out; they can live forever unless they reach their destination!
    - In contrast, packets have time to live (TTL) that would destroy them after sometime
- Because of this any loops that exist in your L2 network can lead to broadcasts which create yet more broadcasts, think of what will happen if two switches are connected together in a loop and receive a broadcast request
- These events where a single broadcast uses a loop to create a cascade of more broadcasts is known as a “broadcast storm”
- To avoid this network crippling issue you need to create networks which don’t introduce any L2 loops

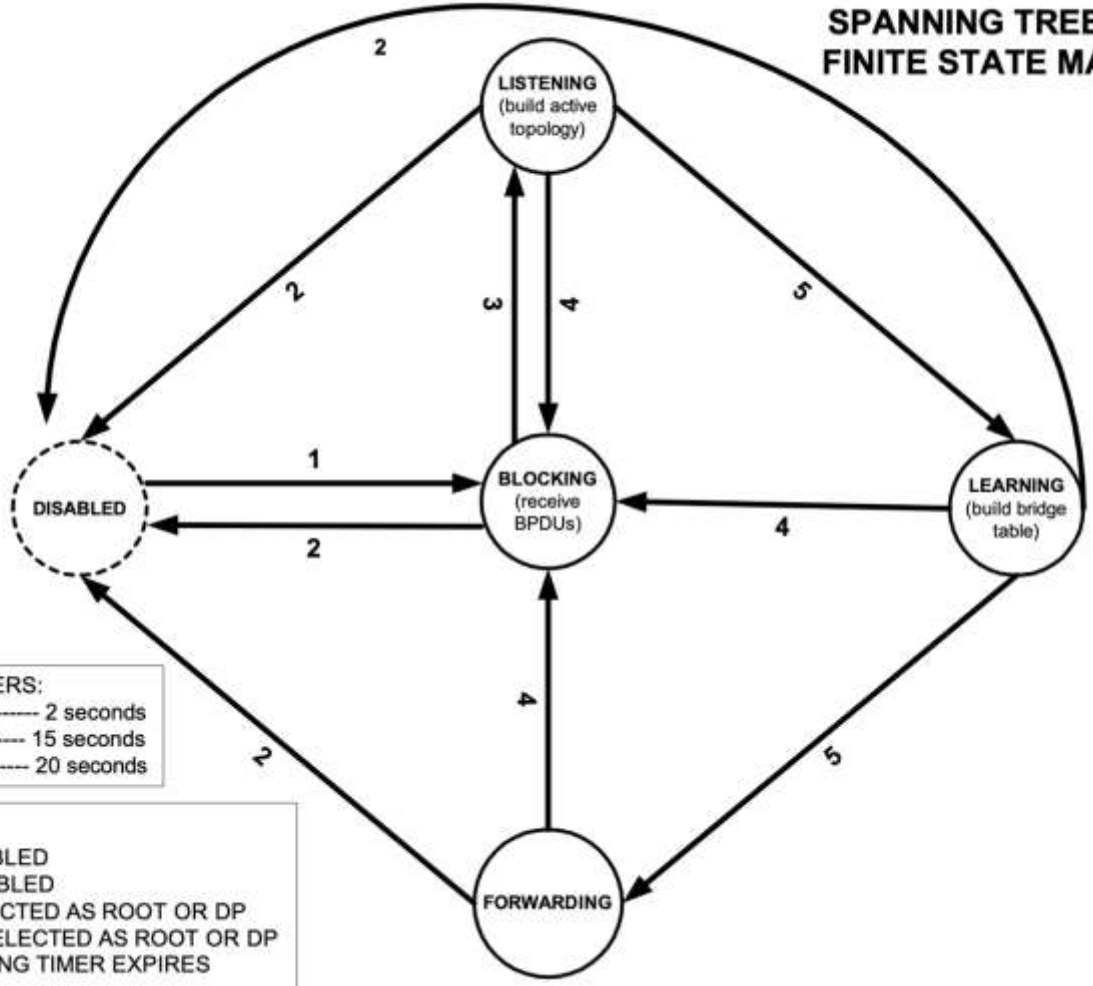
# Spanning Tree Protocol (STP)

- STP is a protocol for identifying and removing loops from a network and creating efficient paths for traffic to flow through
- The protocol works across all L2 devices and has the following steps:
  1. Elect a root node (configured or lowest MAC address)
  2. Calculate the cost between each node and the root
  3. Disable the least efficient redundant paths
- Cost calculated by sending out special Bridge Protocol Data Units (BPDU) which record information about the path and cost based on throughput
- Redundant paths are disabled but can become re-enabled if data can no longer use the most efficient path, allowing for redundancy

# STP States of Ports

- State changes typically happen when a faster path is identified or a path through the network fails
  - Forwarding: normal port operation
  - Blocking: no user traffic allowed, only BPDU traffic traverses this state
  - Learning: learns source addresses from frame, populates switching table, but no forwarding of frames through the network
  - Listening: processes BPDU and decides if it should move back to blocking or learning state, no population of the switching table
  - Disabled: not being governed by STP, set by administrator

# SPANNING TREE PORT FINITE STATE MACHINE

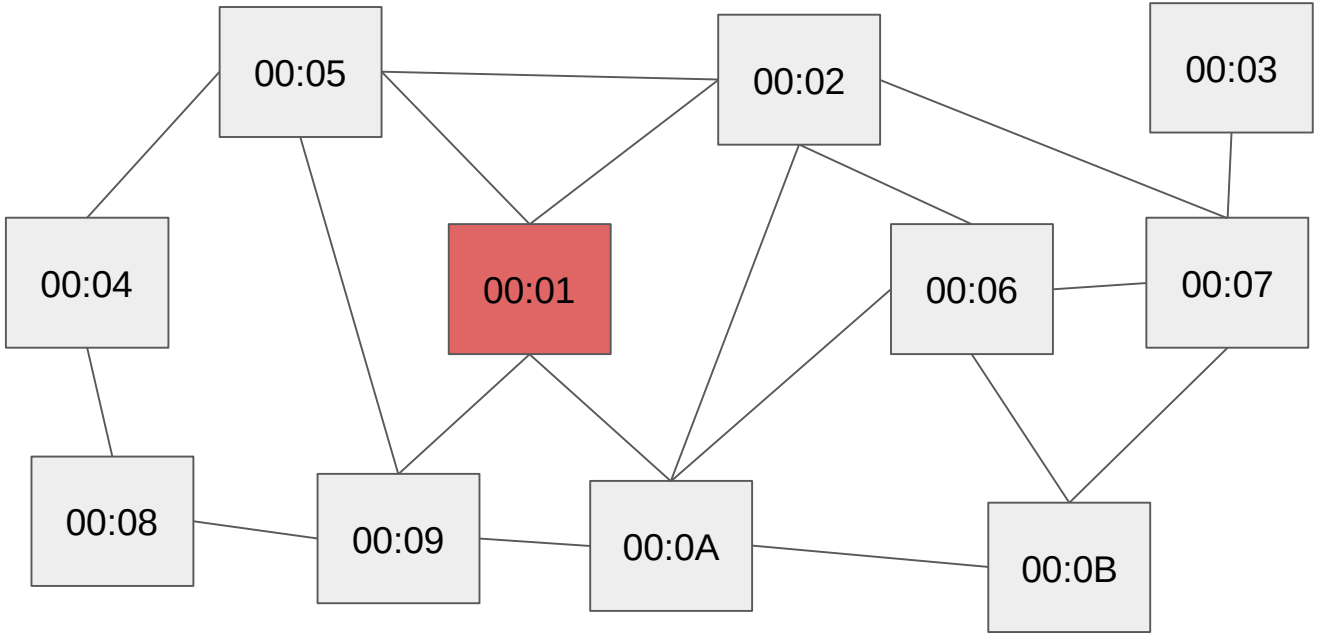



DEFAULT TIMERS:
Hello Timer ---------- 2 seconds
Forward Delay ---- 15 seconds
Max Age ---------- 20 seconds

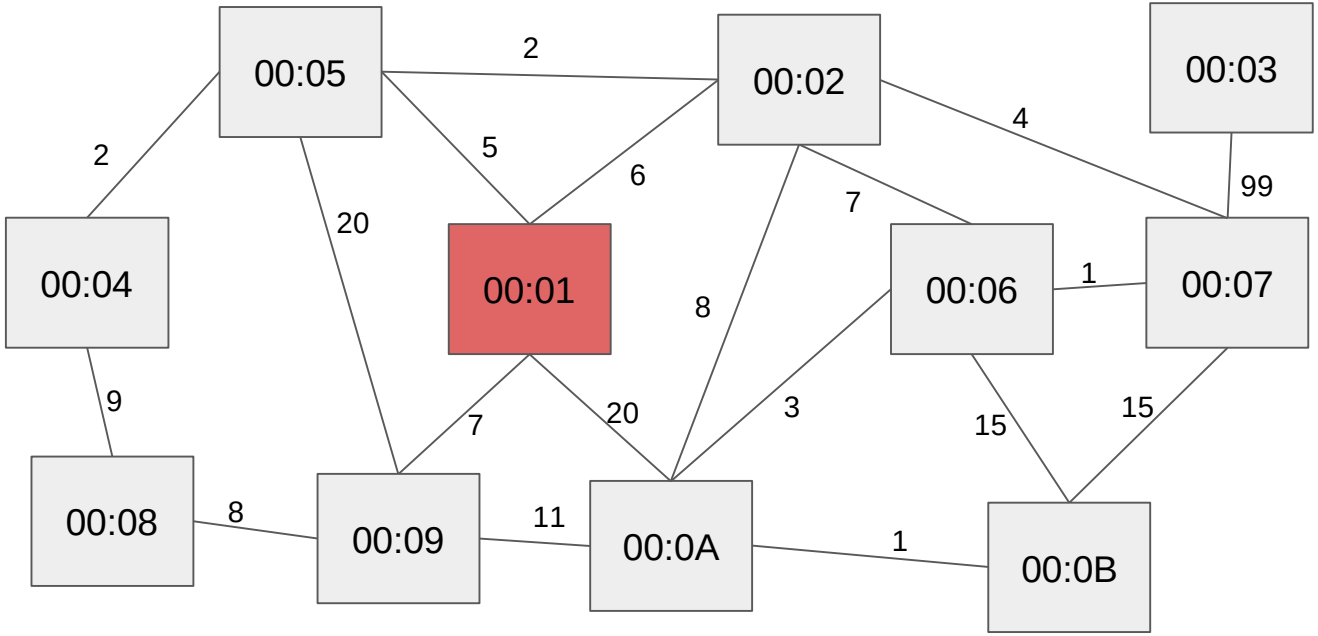
KEY:
1. PORT ENABLED
2. PORT DISABLED
3. PORT SELECTED AS ROOT OR DP
4. PORT UNSELECTED AS ROOT OR DP
5. FORWARDING TIMER EXPIRES

span-fsm.vsd 17-Oct-2000 R.Curci

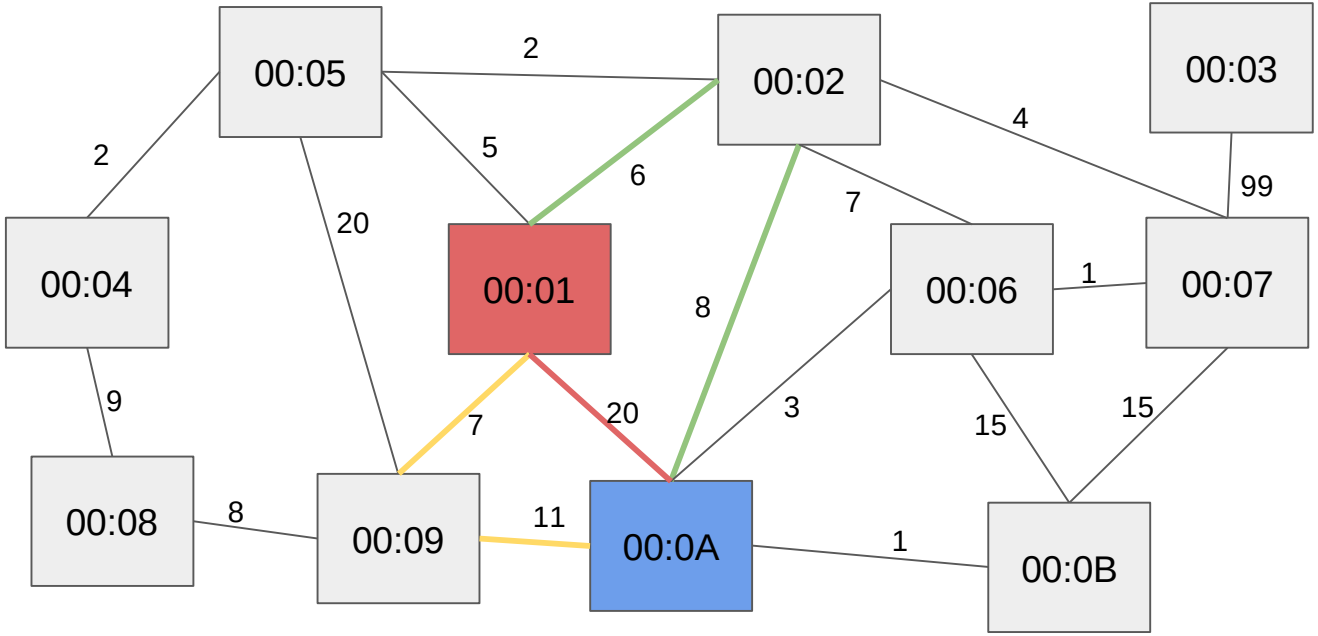
# STP - Root Node Election



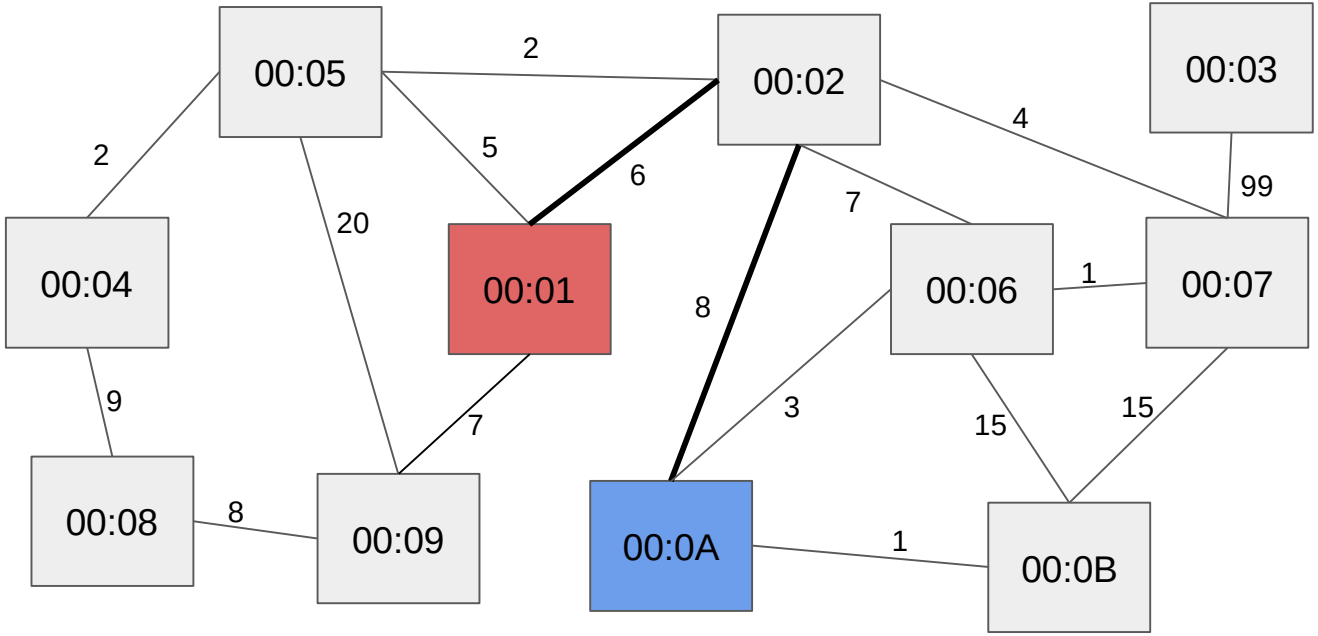
# STP - Calculate Costs



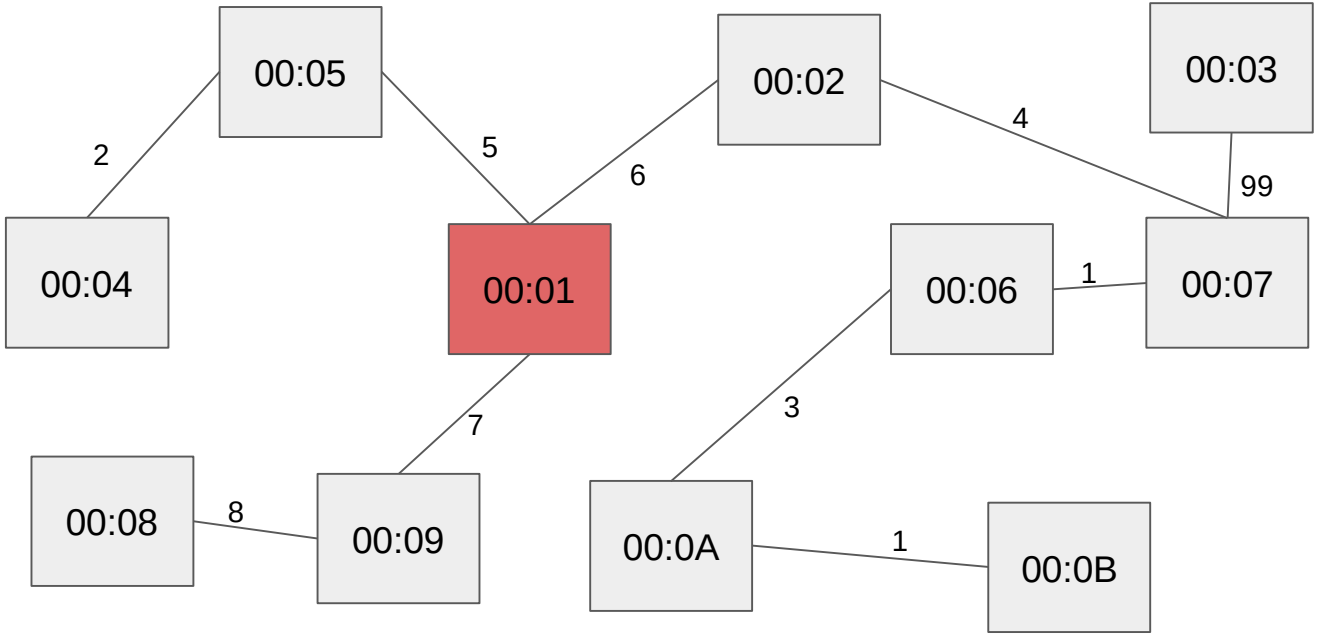
# STP - Disable Redundant Paths



# STP - Disable Redundant Paths



# STP - Final Topology



Questions?

# Additional Resources

Collision and Broadcast Domains

Address Resolution Protocol Wiki

L2 Basics: Spanning-tree Protocol

How does a switch learn MAC Addresses (Video)