CCNA Study Group Week 1

Preview

- Subnetting
- VLANs
- Switching Concepts
- How computers talk to each other
- Spanning Tree
- Link Aggregation
- Routing Concepts
- OSPF

What do we use to send messages?

Binary Addressing

More bits = More hosts you can address

1 bit = 1 or 0

2 bits = 00, 01, 10, 11

3 bits = 000, 001, 010, 011, 100, 101, 110, 111

4 bits = 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, etc.

Grouping based on bits

We could say 00|01 is in the 00 group

00|10 is also in the 00 (0) group

01|01 is in a different group (group 1)

10|01 is in the 10 group (group 2)

Grouping based on bits (Continued)

We can change the bits that determine what group its in.

0|101 would be in group 0

1|001 would be in group 1

More bits = more groups you can address, but the less hosts you can address.

IP Address Subnetting

The first and last IP of a subnet are reserved

IP Address: 172.20.0.1
Subnet Mask: 255.255.255.0 or /24

Group/Network portion: 172.20.0
Host portion: .1

How many hosts can you address inside this subnet?

What is subnetting used for?

Hosts look at three things to see if destination is in the same VLAN:

1. Sending IP Address
2. Sending Subnet Mask
3. Destination IP Address

If the destination is in the same LAN, the host is reachable over layer 2.

if the destination is outside, the host is only reachable over layer 3.

Broadcast domain

Broadcast Domain, VLAN/LAN, and subnet refer to different parts of the same thing.

Subnet: a smaller group of a network

(V)LAN: all hosts that you can reach over layer 2

Broadcast domain: all hosts that you can broadcast to over layer 2

Original Layer 2 Design

Hosts were connected to each other with a hub.

When someone wanted to send data, the Network Interface Card (NIC) would send electricity into the hub.

The hub would repeat the electric signal on all ports, whether someone was also sending data at the same time or not.

This creates a lot of collisions since people are talking at the same time.

Original Layer 2 Design (Cont.)

Everyone would receive the frame, but only process it if the frame belonged to them.

The destination would respond in the same way, causing more collisions.

Broadcast Domain vs. Collision Domain

A collision domain is a place where two hosts can send electricity at the exact same time.

Switches avoid this by waiting/buffering.

Switches wait until the host connected to it is done talking.

Buffering means that it keeps the frames in a buffer, waiting for the opportunity to send them over the port.

Switch Operations: Forwarding Table

Forwarding table

1. Every time a host sends a frame, the switch reads the MAC Address and creates an entry. The entry has the port received on and the source MAC Address.
2. When forwarding, the switch looks for the entry with the destination MAC Address and sends it on the port in the entry.
3. After a few minutes (5 minutes default on Cisco IOS), the entry is taken out.
4. Each VLAN has its own forwarding table.
5. Multiple entries with different MACs can be on one port (trunk ports).

Switch Operations: Trunking and Flooding

Trunks

1. Trunks are used to share VLANs between switches.
2. Trunks send frames in 802.1Q format; each frame has its VLAN ID.
3. When a switch receives a frame on a VLAN that has to go to another switch, it tags that frame with its VLAN ID.
4. The switch on the other side will read the VLAN ID and look at it's forwarding table for that VLAN.

Flooding

1. If the switch does not have an entry for the destination MAC Address, it will flood and send the frame out on all ports.

Packets and Frames

Frames encapsulate packets.

Frames are destined to the next Layer 2 hop.

Packets are destined to the Layer 3 destination.

If the destination is in the same VLAN, the Layer 2 destination and Layer 3 destination are the same.

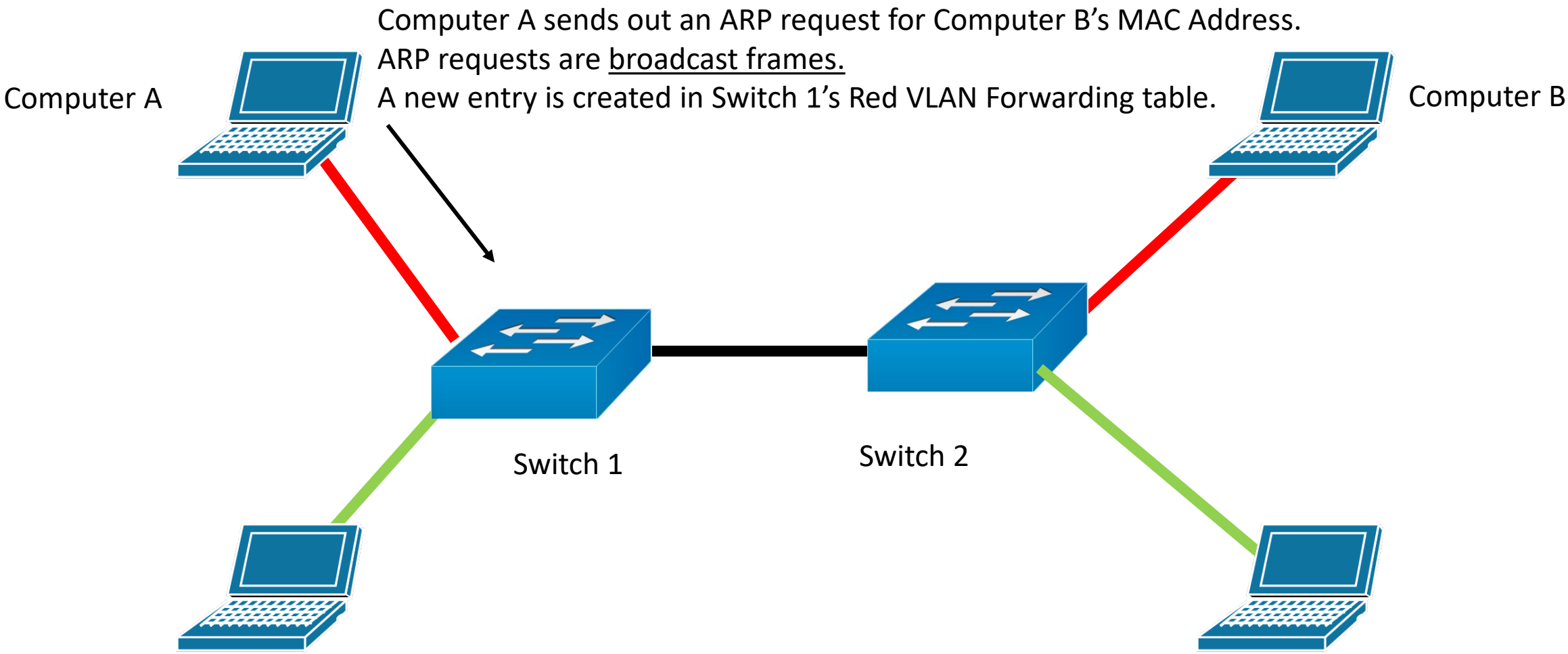
Packets and Frames (Cont.)

To send a packet to a neighbor on the LAN, the device must know the neighbor's MAC Address.

The packet contains the data, but the host needs to address the frame to the neighbor to send the packet.

If a host knows the neighbor's IP Address, but not its MAC Address, it will use Address Resolution Protocol (ARP).

LAN communication



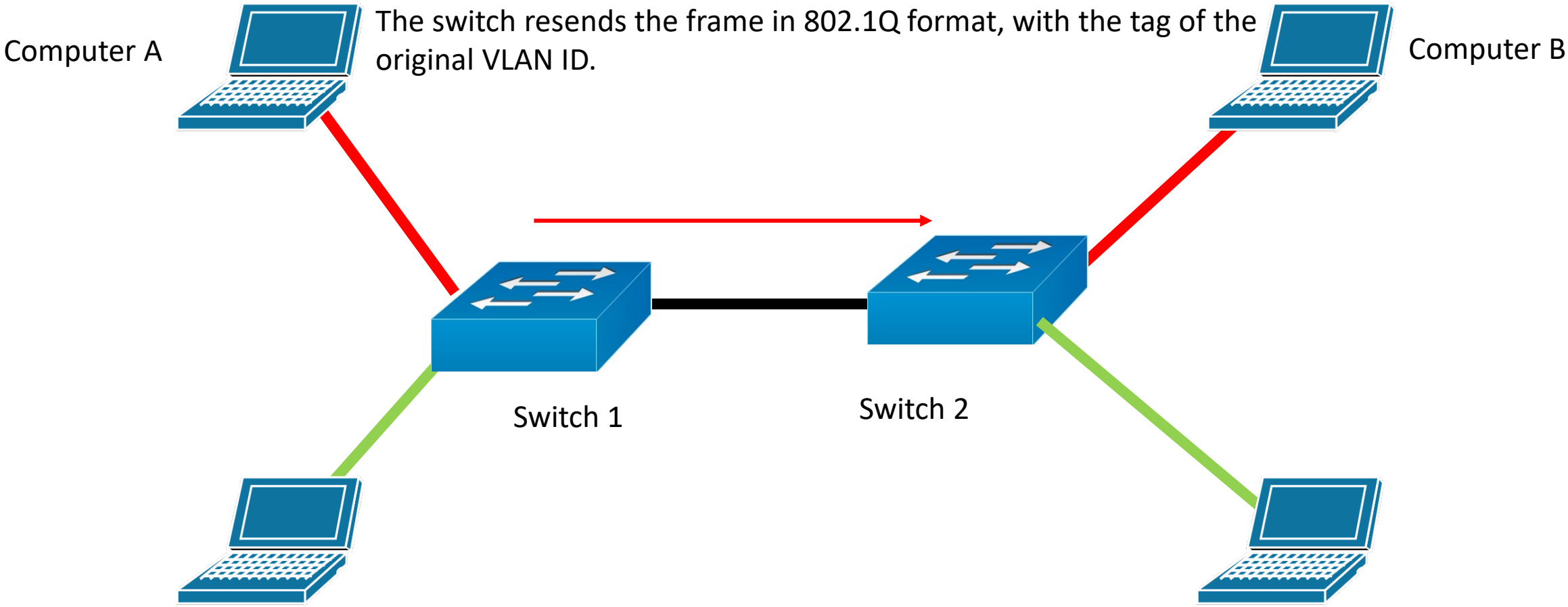
ARP Request Anatomy

Source MAC: Requester MAC Address

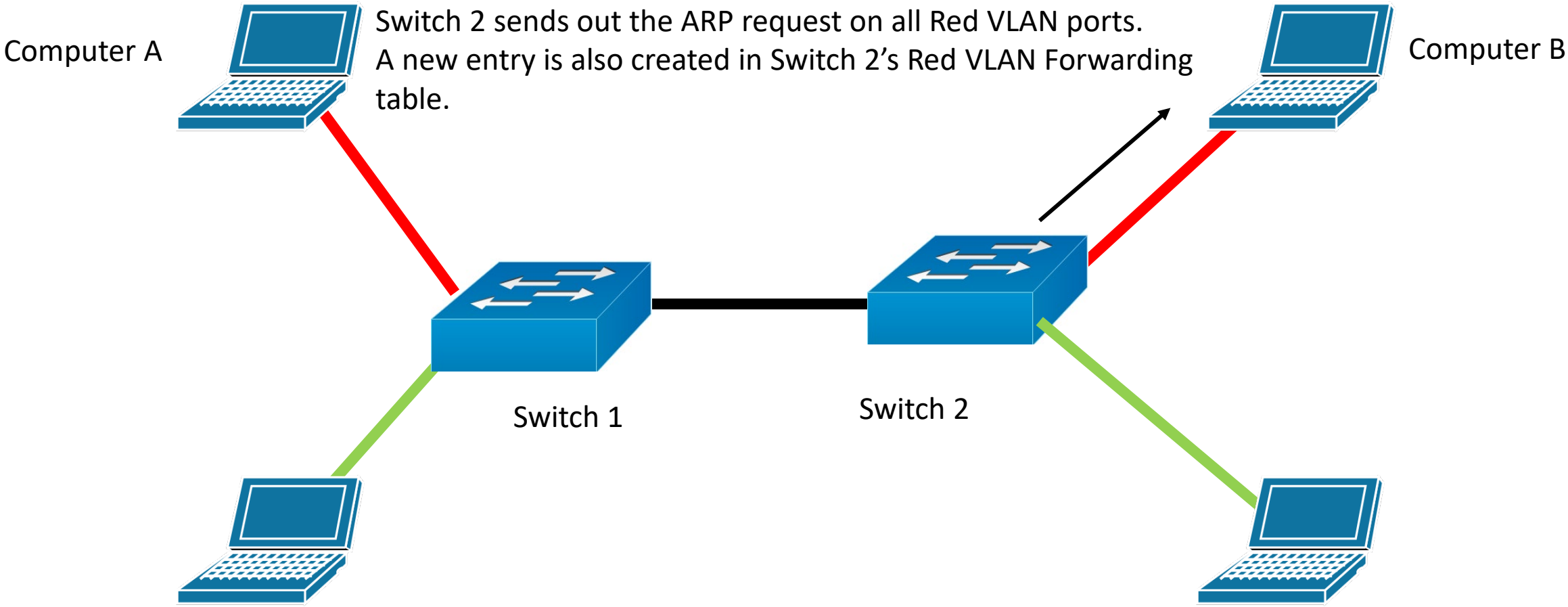
Dest MAC: FF:FF:FF:FF:FF:FF (broadcast)

Wanted MAC Address for IP: 172.20.3.5

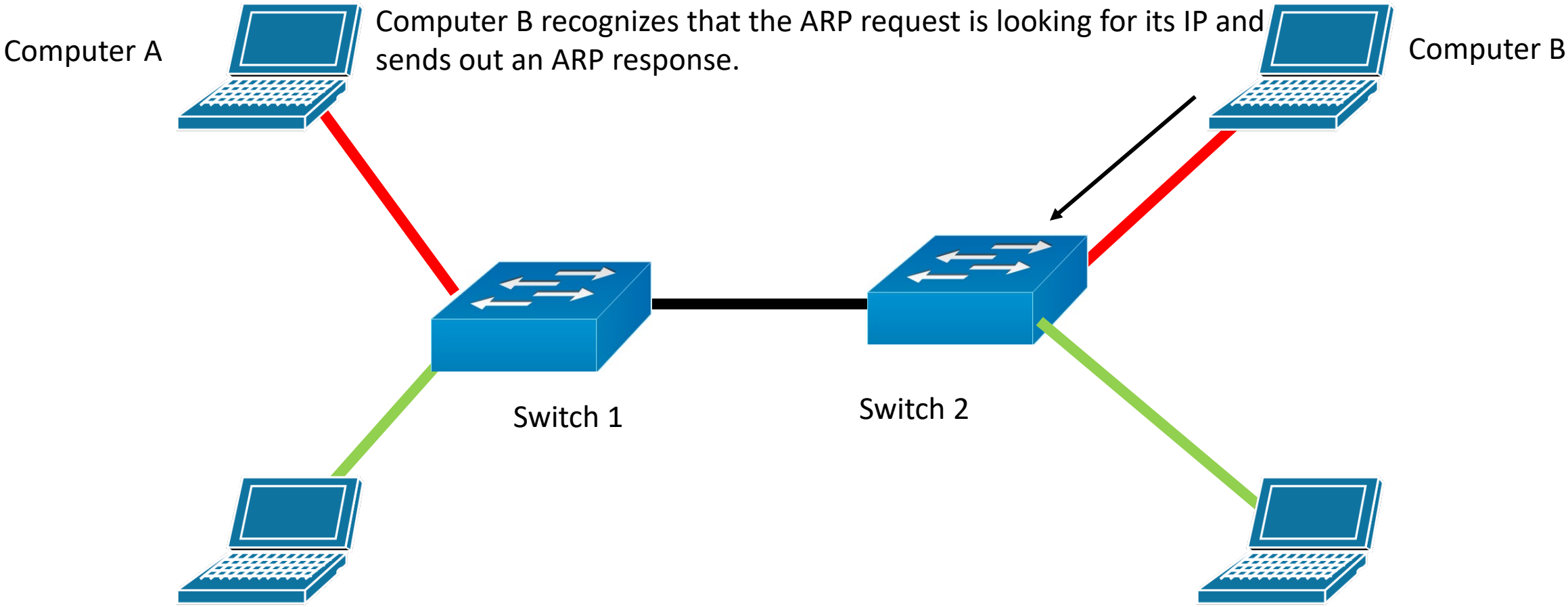
LAN communication



LAN communication



LAN communication



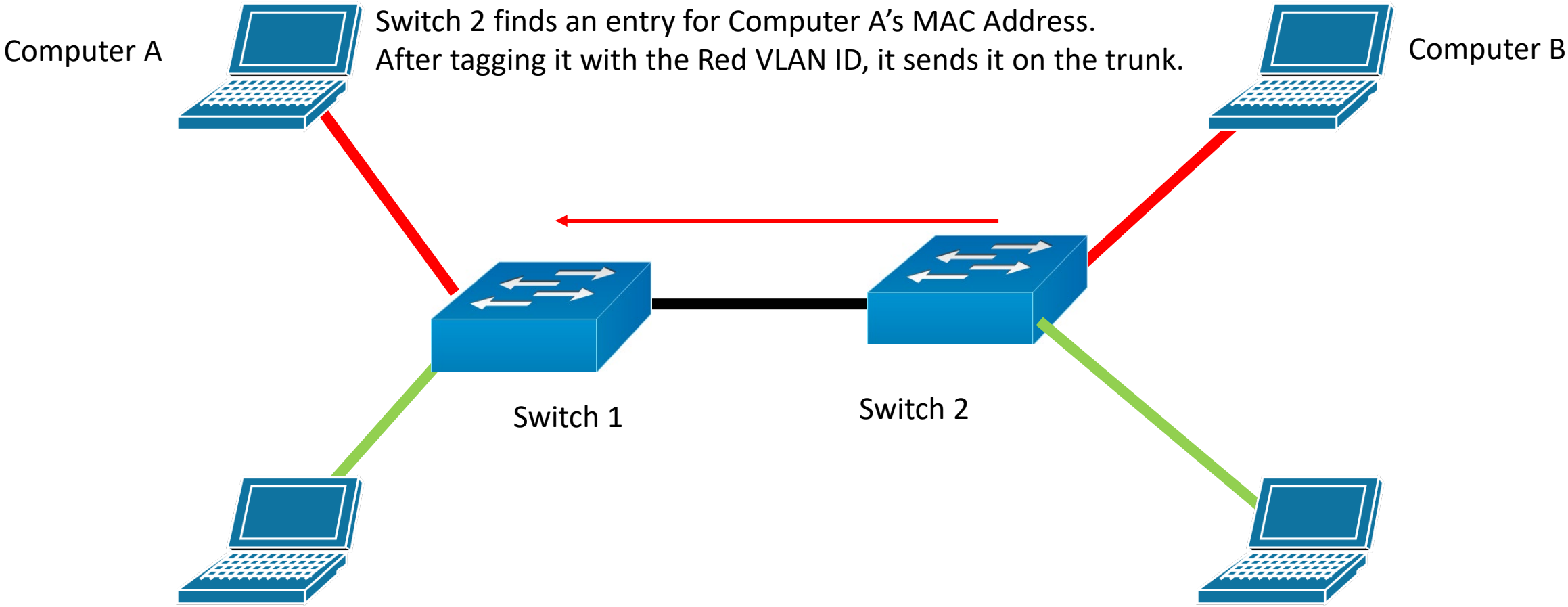
ARP Response Anatomy

Source MAC: Responder MAC Address

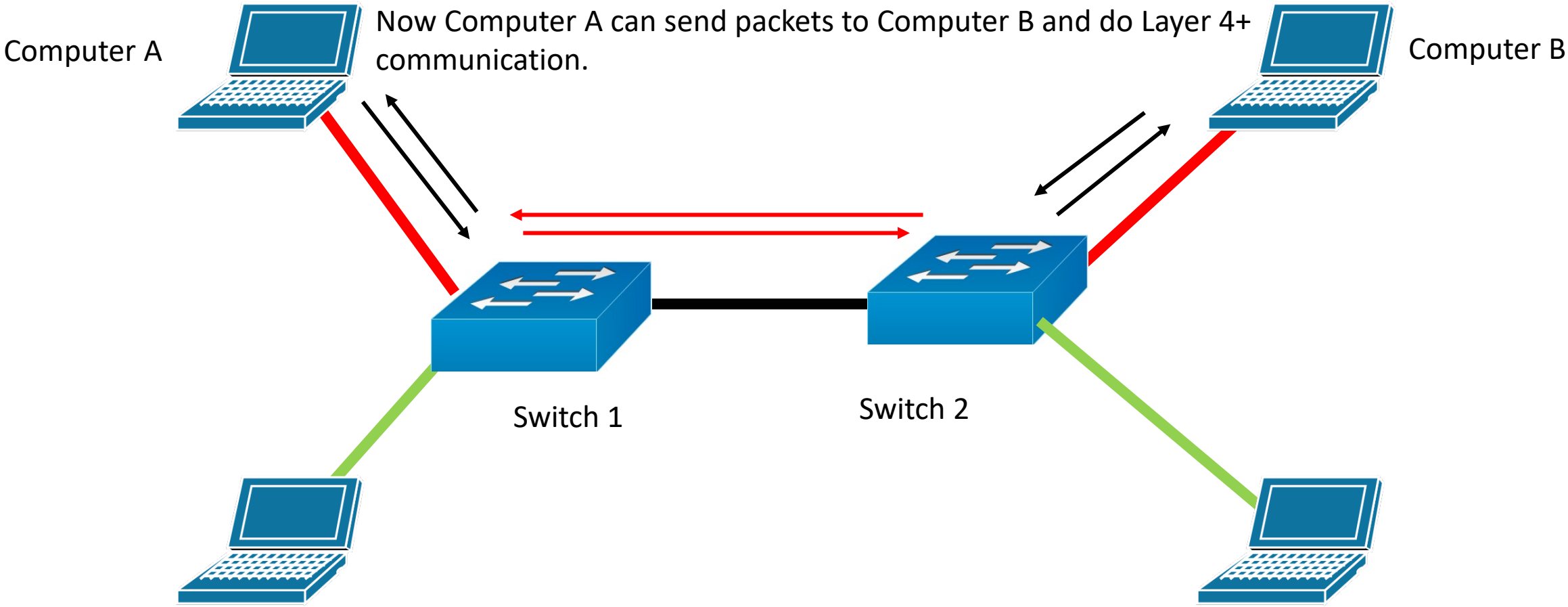
Dest MAC: Requester MAC Address

MAC Adddress for 172.20.3.5: 12:34:56:78:90:12

LAN communication



LAN communication



Sending packets outside the subnet

If a host decides that the destination address it wants to reach is outside its subnet, it will send the packet to its default gateway.

Frame Addressed to Default Gateway

Packet Addressed to End Destination

Storms

When a packet is forwarded, the router decreases its Time To Live (TTL)

If a router decreases a packet's TTL to zero, the router does not forward the packet.

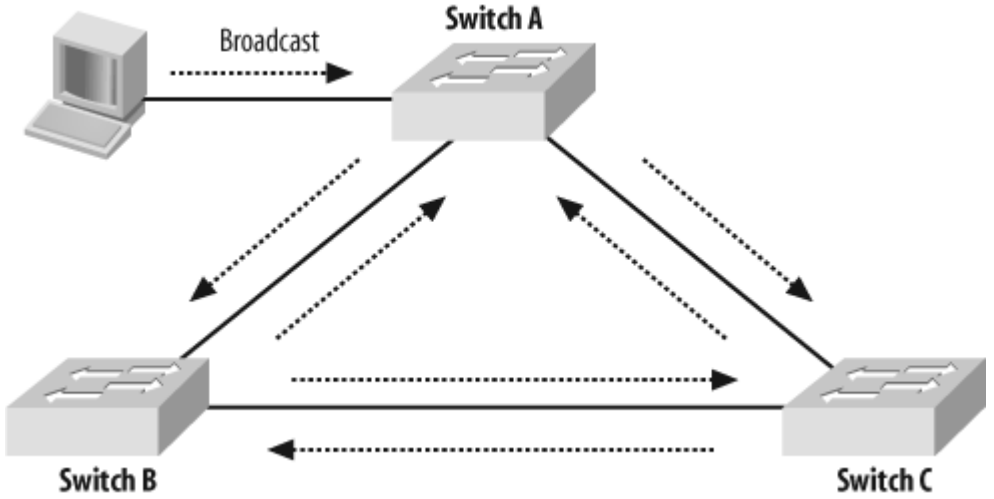
Frames can be forwarded indefinitely because they do not have a TTL.

When frames are forwarded indefinitely, they eat up a lot of CPU on switches and hosts.

Broadcast Storms

Broadcast storms occur when there is a loop in the Layer 2 topology.

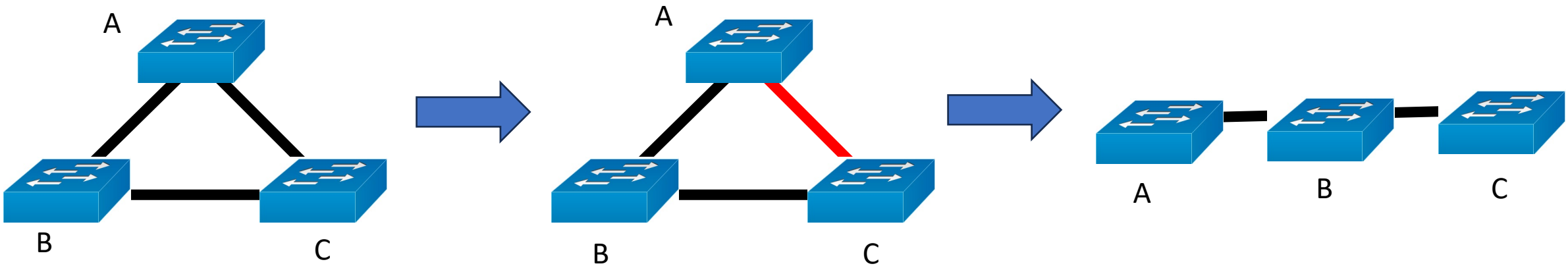
One switch will send out a broadcast, the next switch will forward that broadcast, and the third switch will send that broadcast back to the first switch.



Spanning Tree: Overview

Spanning Tree attempts to fix this by making the Layer 2 topology into a logical tree.

Trees don’t loop (for the most part) in real life, so forcing the topology into a tree fixes switching loops.



Spanning Tree: Port Roles & States

Port State: What is the port doing currently

1. Blocking (20 seconds)
2. Listening (15 seconds)
3. Learning (15 seconds)
4. Forwarding

Port Role: What role is the port filling

- Root
- Designated
- Blocked

Spanning Tree: Port Roles

Designated Port

- Port pointing down the tree.
- Can have multiple.

Root Port

- Port pointing up the tree.
- Can have one.

Blocked Port

- Port pointing down the tree.
- Can have multiple.

Spanning Tree: The TWO Combinations

You will either have:

1. Root + Designated
2. Blocked + Designated

You will never ever have any other combination of port roles on a link.

Link Aggregation

Spanning Tree stops looping by closing links.

What if we combined them instead?

Link Aggregation is when we logically combine two or more interfaces to be one big interface.

Aggregated links are called Port Channels or EtherChannels.

Link Aggregation Cont.

Three ways to do link aggregation:

1. Static
2. Link Aggregation Control Protocol (LACP) – Vendor Neutral
3. Port Aggregation Protocol (PAGP) – Cisco only

Keywords:

LACP – active/passive

PAGP – auto/desirable