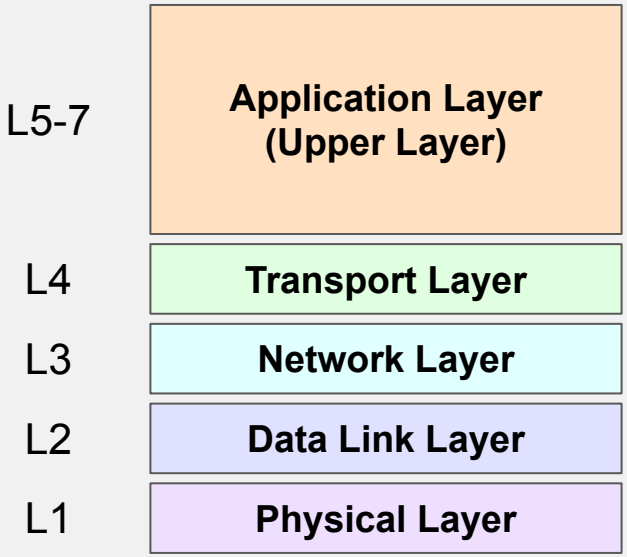
Network Security

LAN, VLAN, War in the LAN?

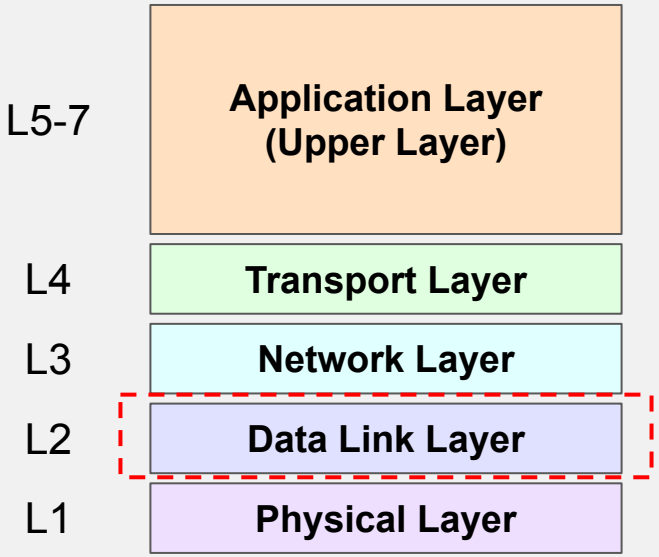
Gwendal Patat
Univ Rennes, CNRS, IRISA
2025/2026

Recall TCP/IP Model



TCP/IP Model

Today's Topic: Link Layer



TCP/IP Model

MAC, CAM, and STP

MAC Addresses

Layer 2 Address: 48 bits unique interface identifier

1234.5678.9ABC

Manufacturer Code

1234.56XX.XXXX

Interface Identifier

XXXX.XX**78.9ABC**

Broadcast

FFFF.FFFF.FFFF

CAM Table

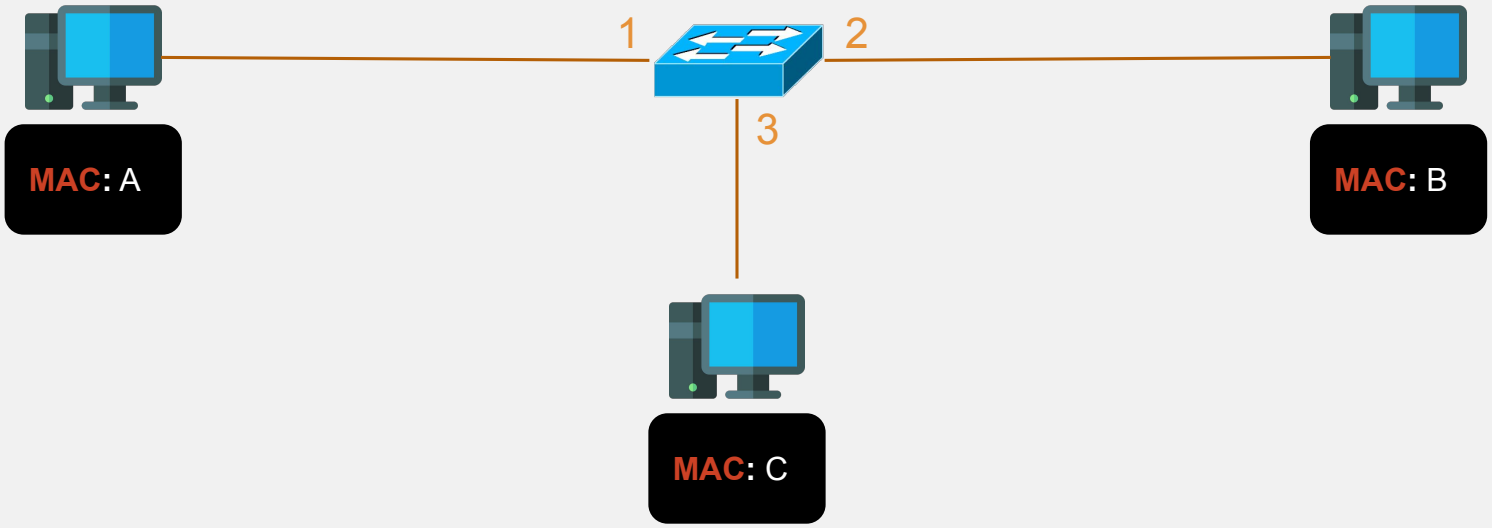
Content Addressable Memory (CAM) Table:

- Here to help the switch memorize MAC addresses for routing.
- Memory table in a switch.
- Used to store MAC addresses linked to a specific port (network interface).
- Fixed size.

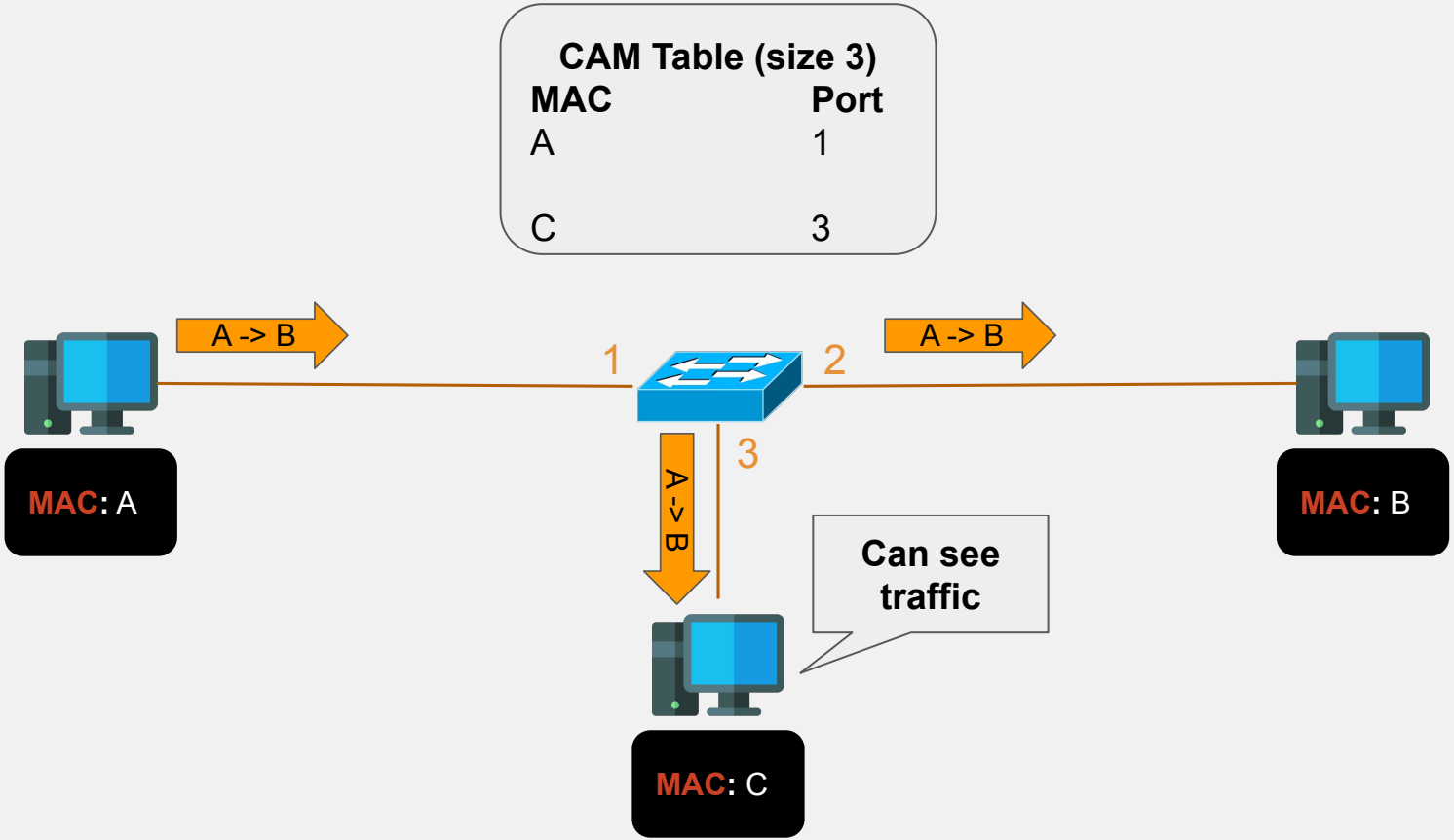
CAM Table Expected Behaviour 1/4

CAM Table (size 3)

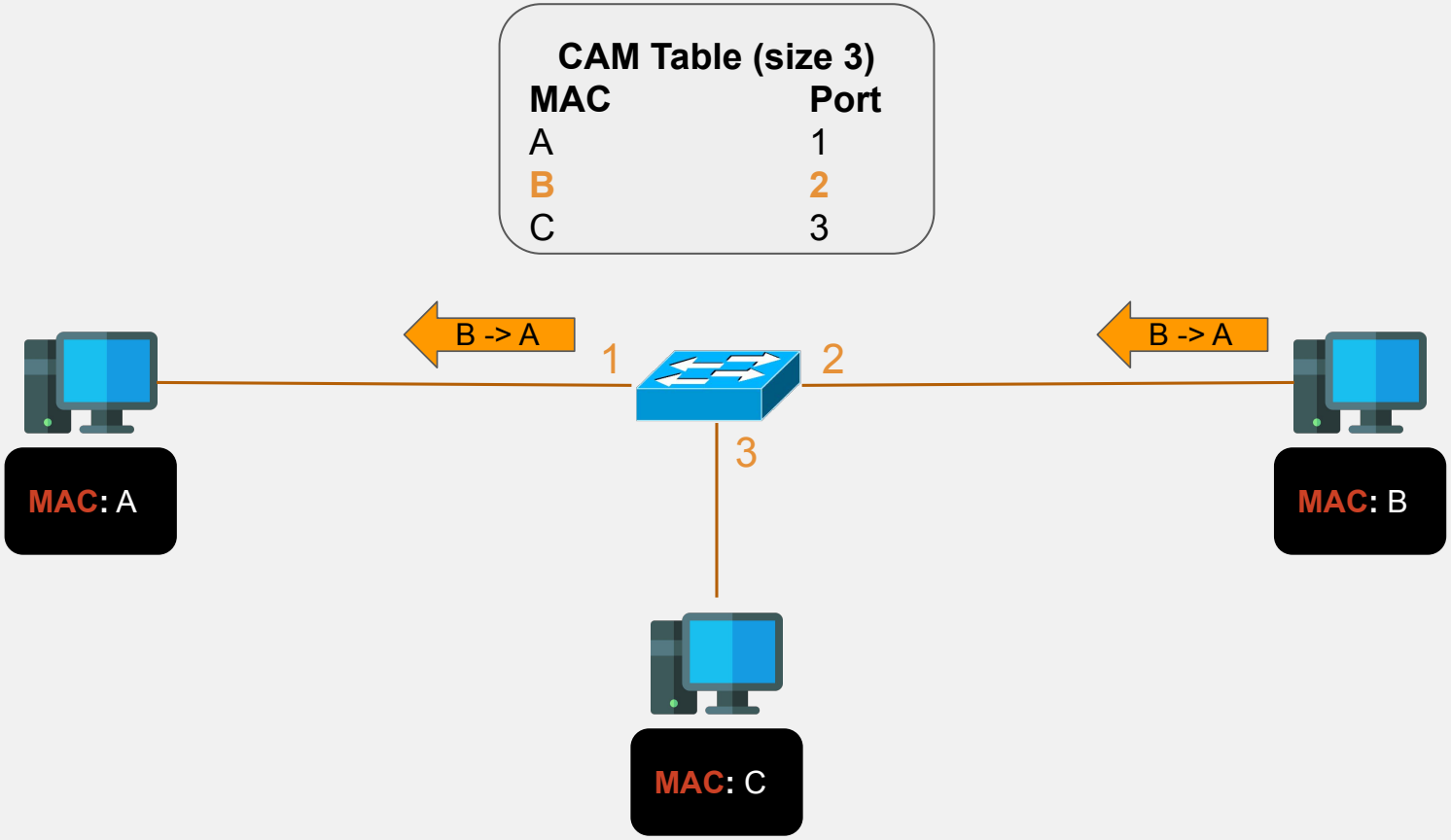
MAC	Port
A	1
C	3



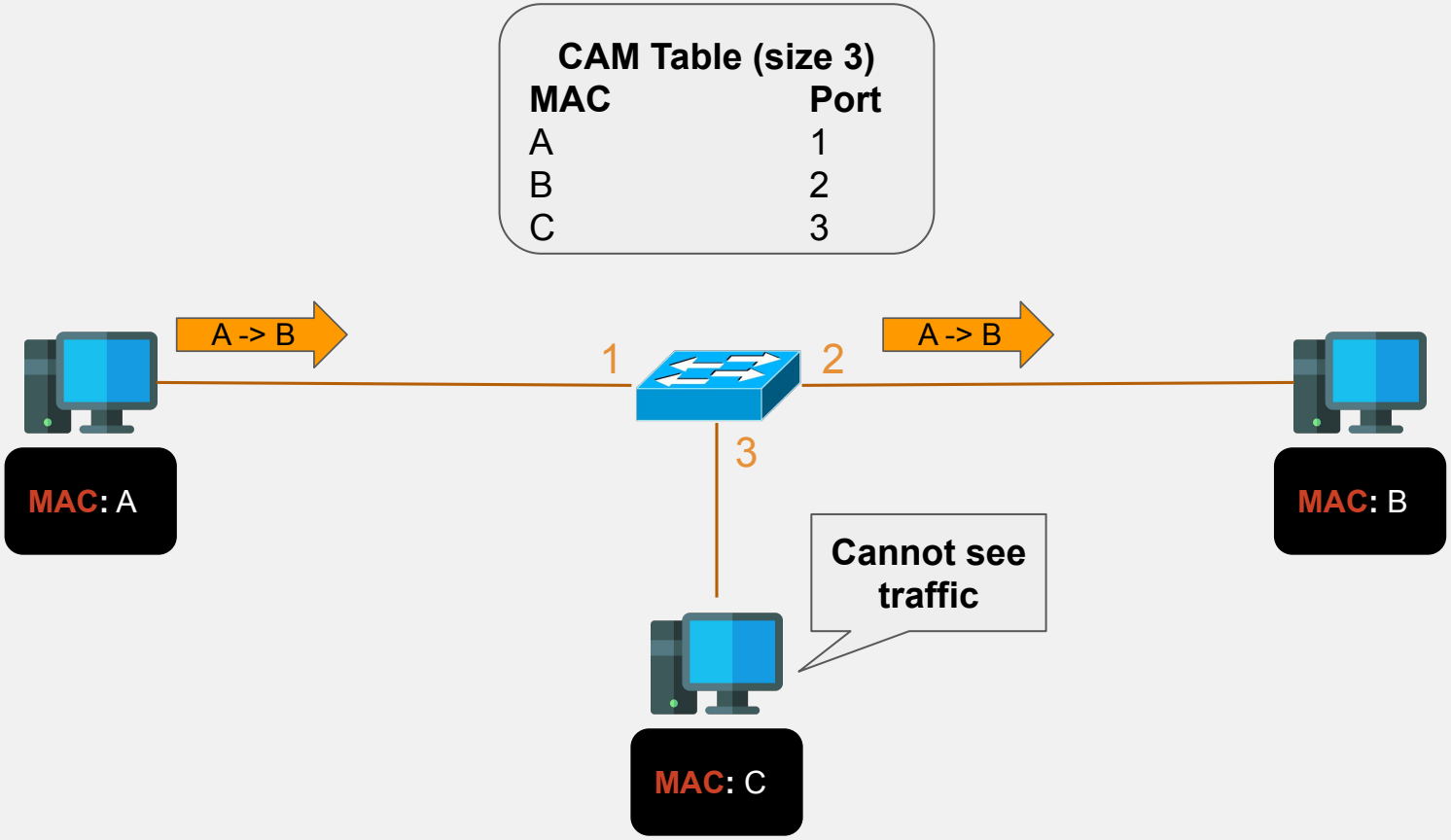
CAM Table Expected Behaviour 2/4



CAM Table Expected Behaviour 3/4



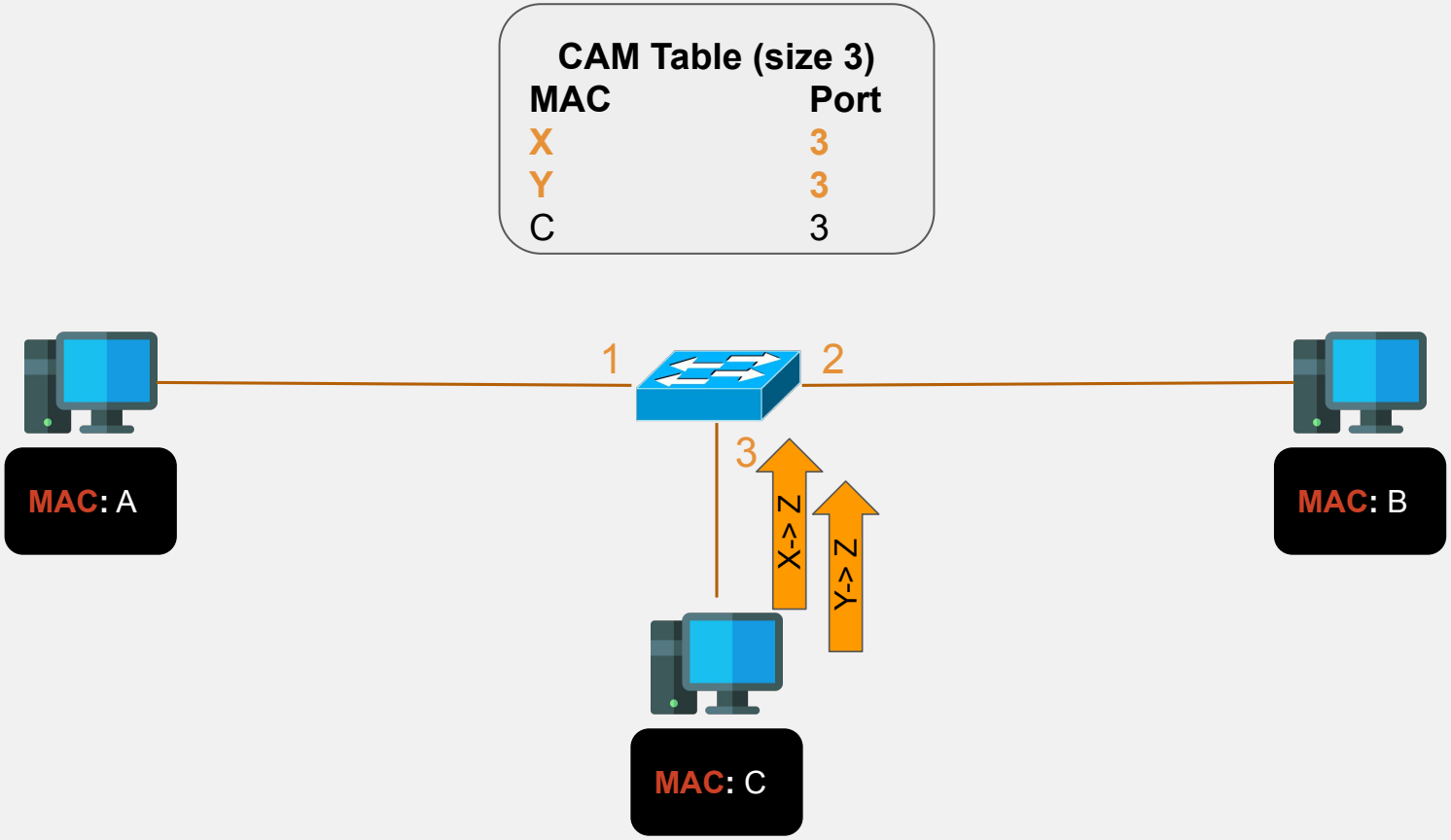
CAM Table Expected Behaviour 4/4



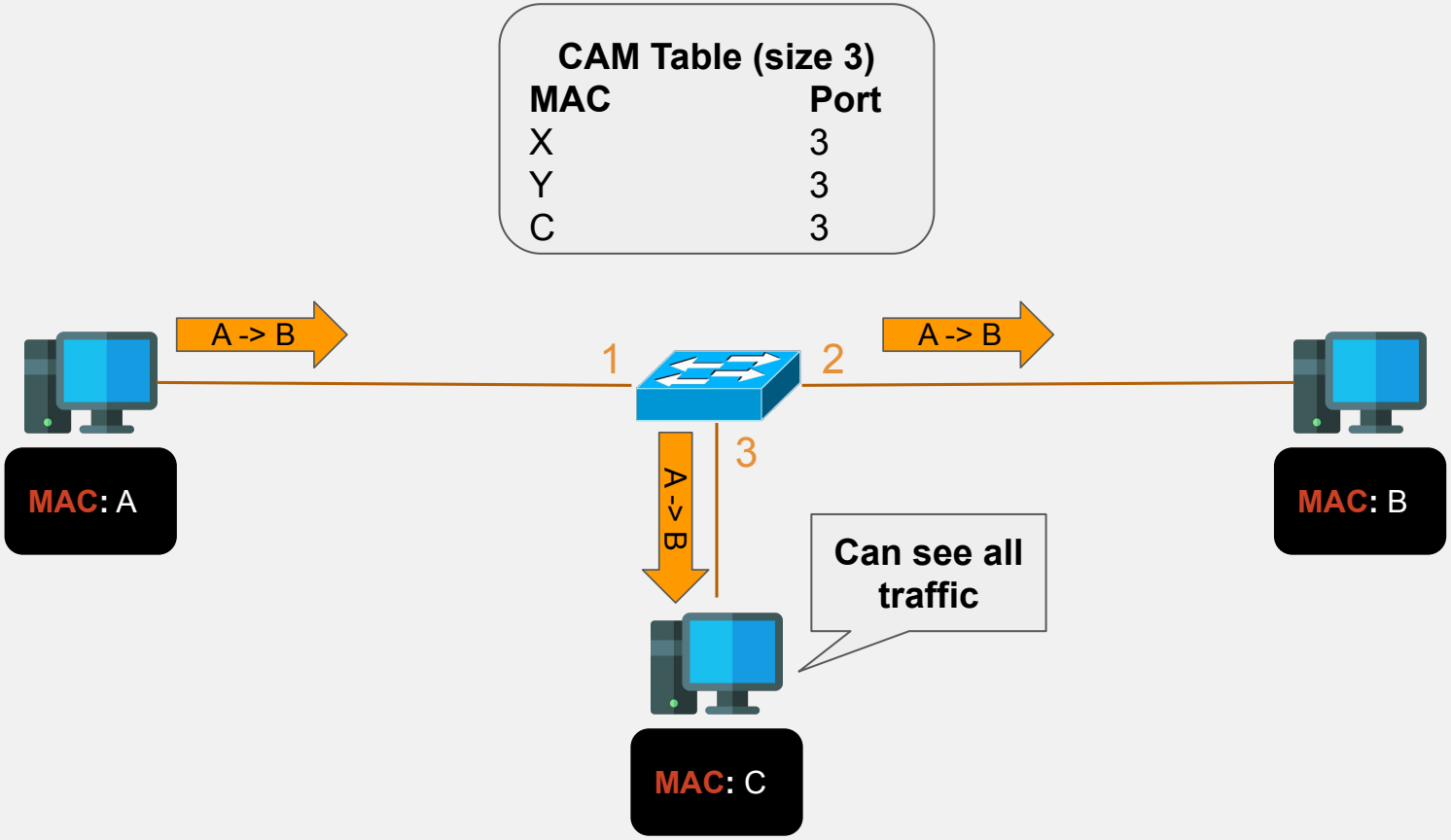
CAM Attack: CAM Overflow

- **Main Issue: Limited Size**

CAM Overflow 1/2



CAM Overflow 2/2



Cisco Catalyst CAM Tables

In the Network lab rooms:

Catalyst 2960 Series

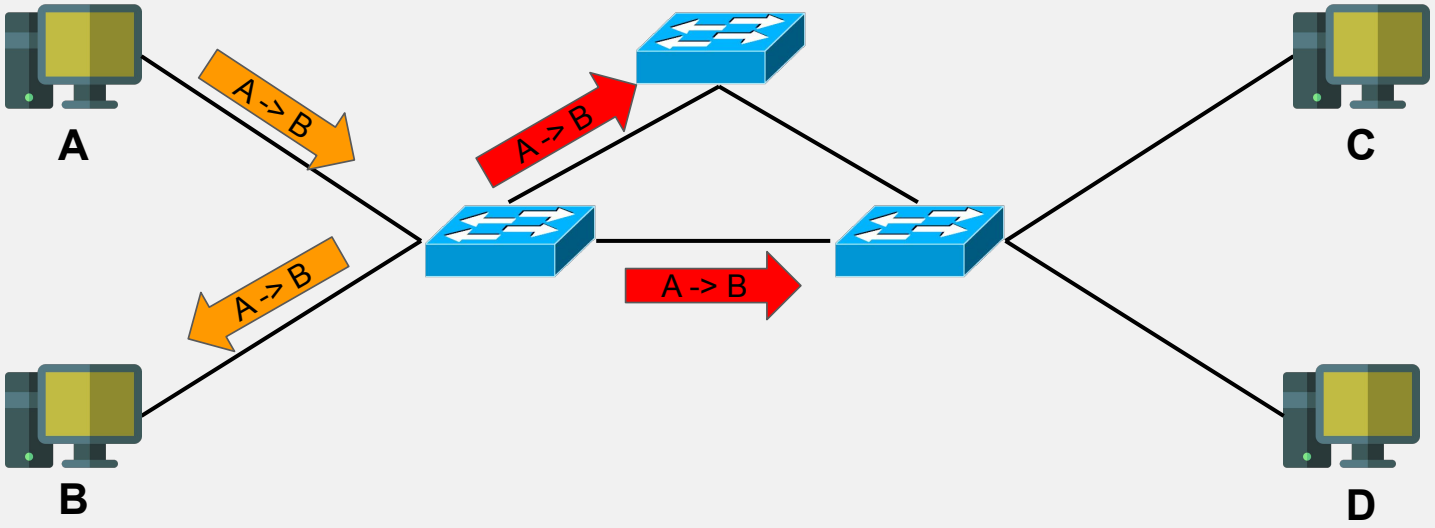
The Catalyst CAM table uses hash functions to store entries. The flooding attack needs to send many frame but can done in under a minute.

Flooding Mitigation: Port Security

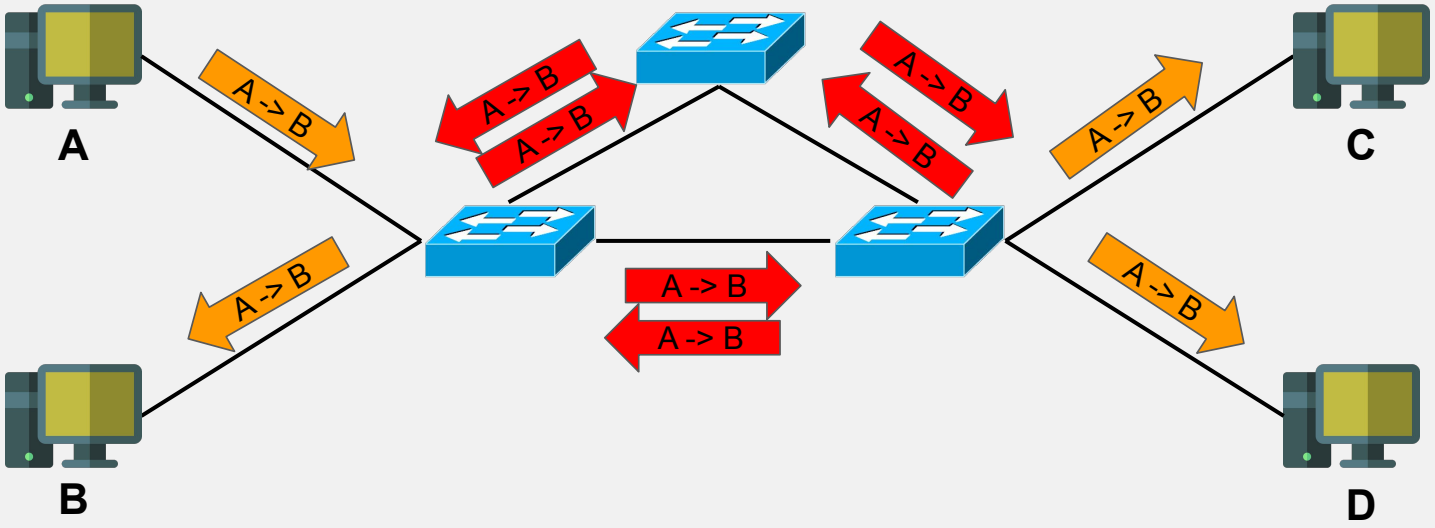
Can be configured directly on the switch:

- Can define the max number of MAC addresses linked to a port.
- Can even shutdown the port if violation are spotted.

Another problem: Broadcast Storm 1/2



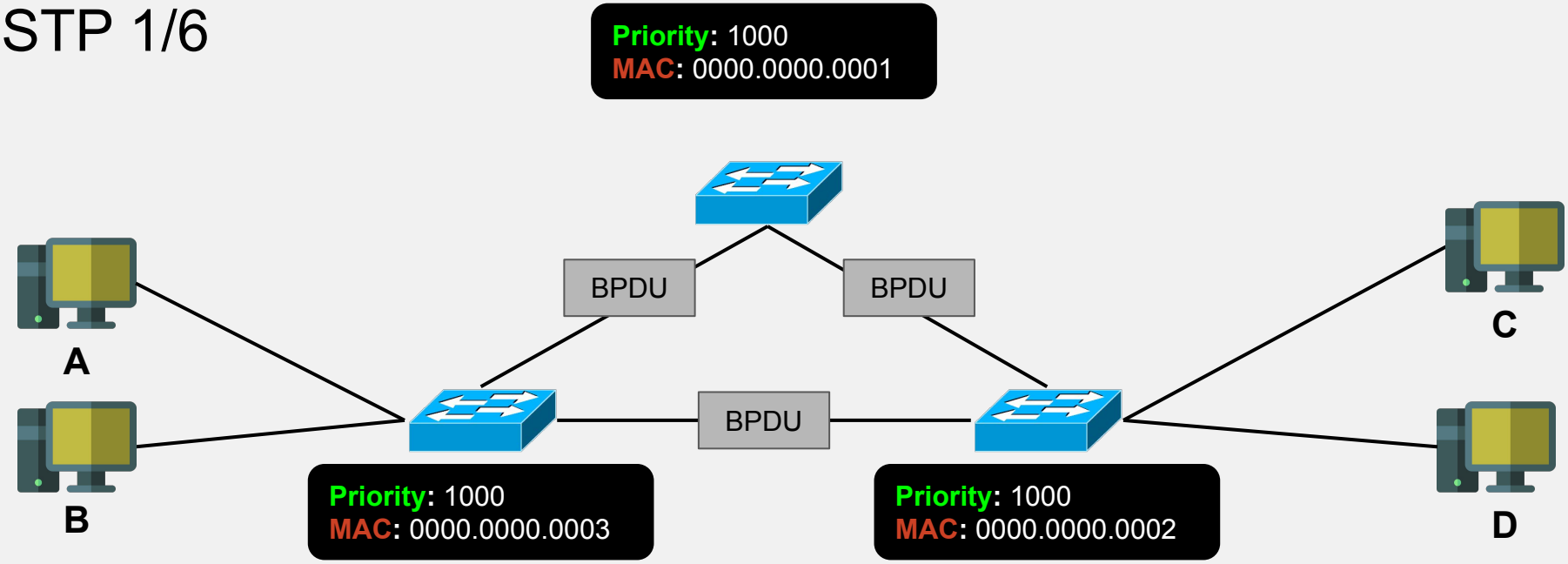
Another problem: Broadcast Storm 2/2



Spanning Tree Protocol (STP)

- **STP**
  - Here to avoid broadcast loop.
  - Define a **root bridge:** the main switch of the tree.
    - Elected by exchanging **Bridge Protocol Data Units** (BPDUs)
  - Calculate which port to block based on **priority** and **speed**.

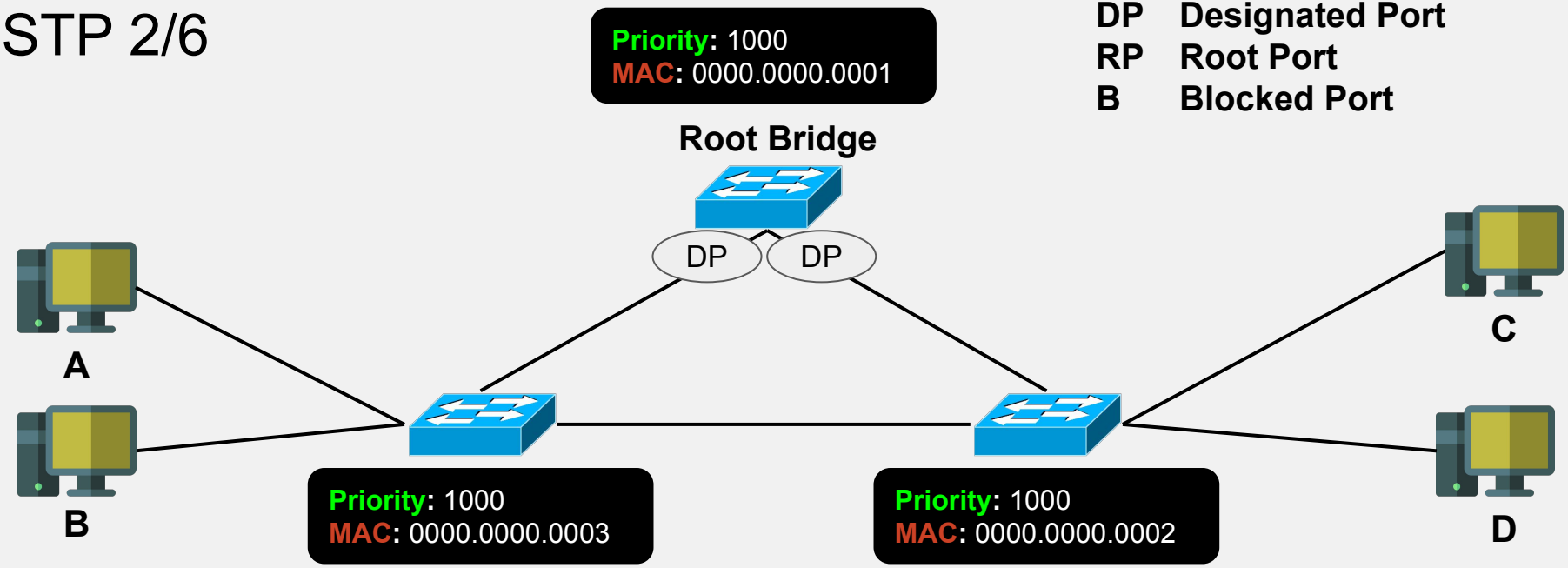
STP 1/6



Switches exchange BPDUs with Bridge ID (BID) inside:
BID = **Priority** + **MAC** (+ VLAN)

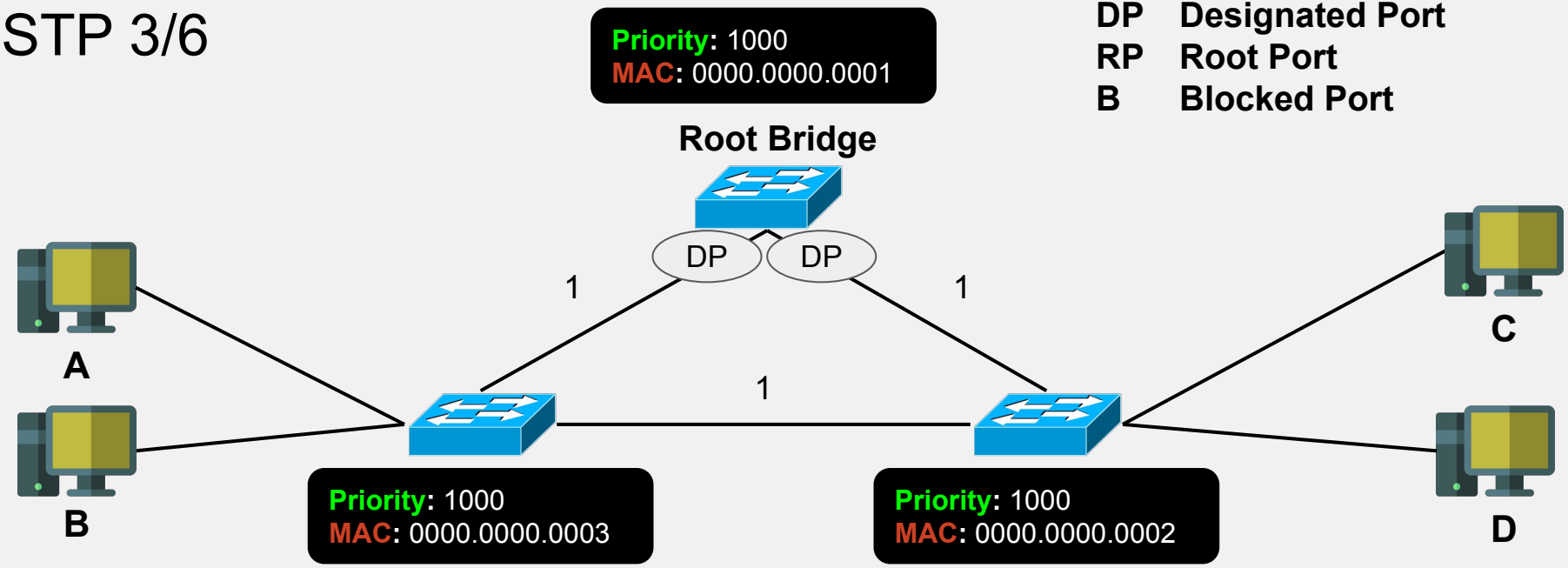
The switch with the **lowest** BID becomes the ***root bridge***.

STP 2/6



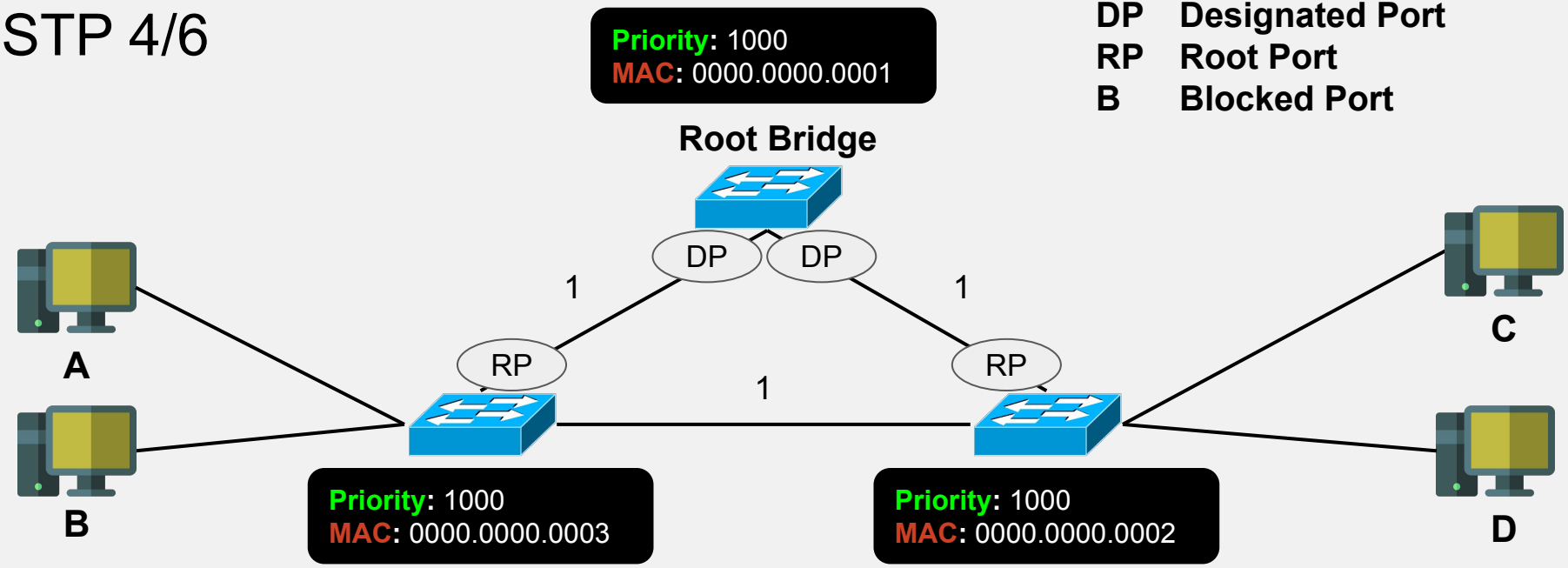
DP Designated Port
RP Root Port
B Blocked Port

STP 3/6



Root ports are defined by the **lowest path cost** to the root bridge.

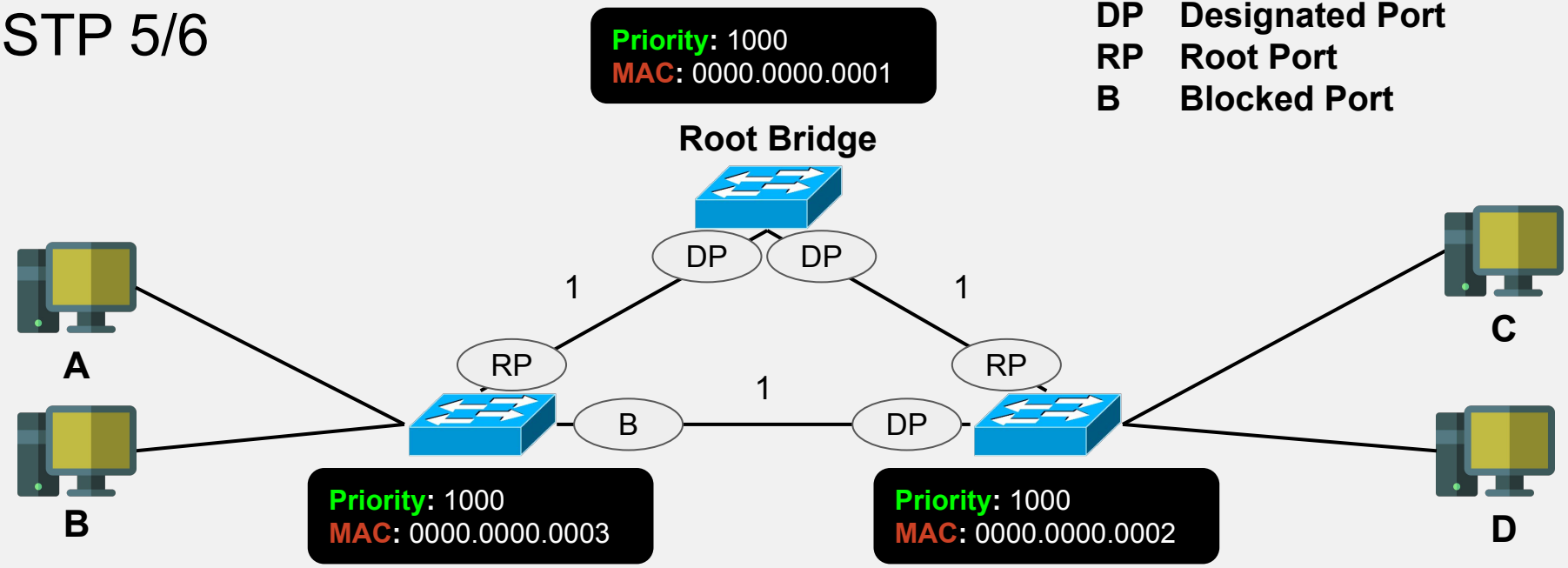
STP 4/6



What about the last two ports?

We keep open the one from the lowest BID.

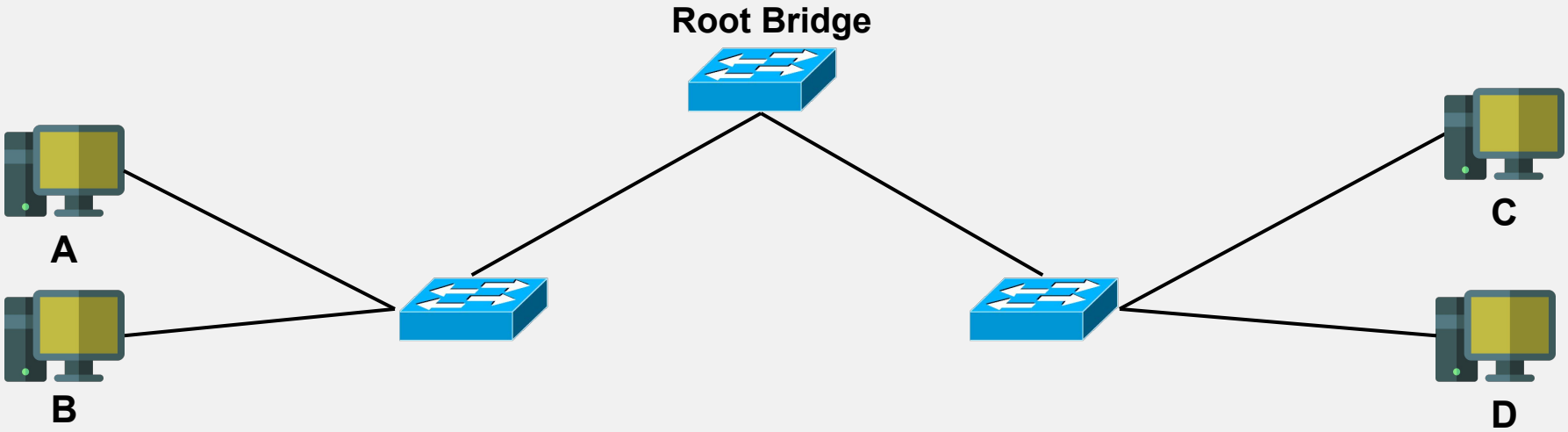
STP 5/6



What about the last two ports?

We keep open the one from the lowest BID.

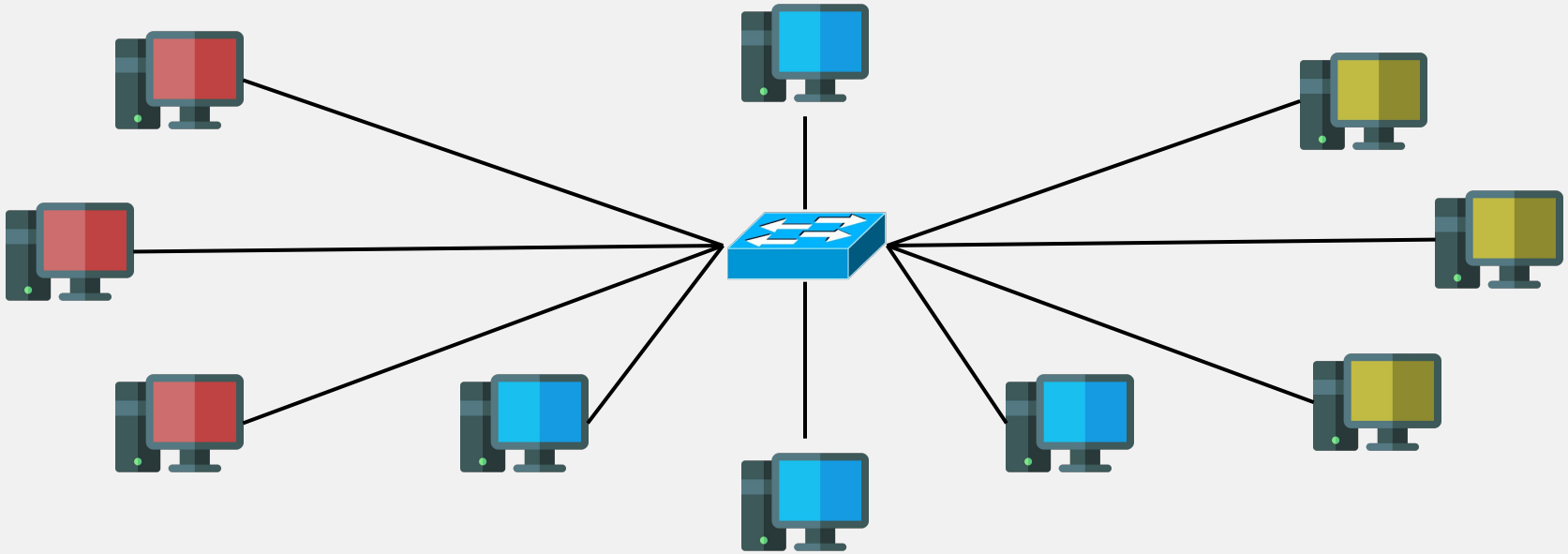
STP 6/6



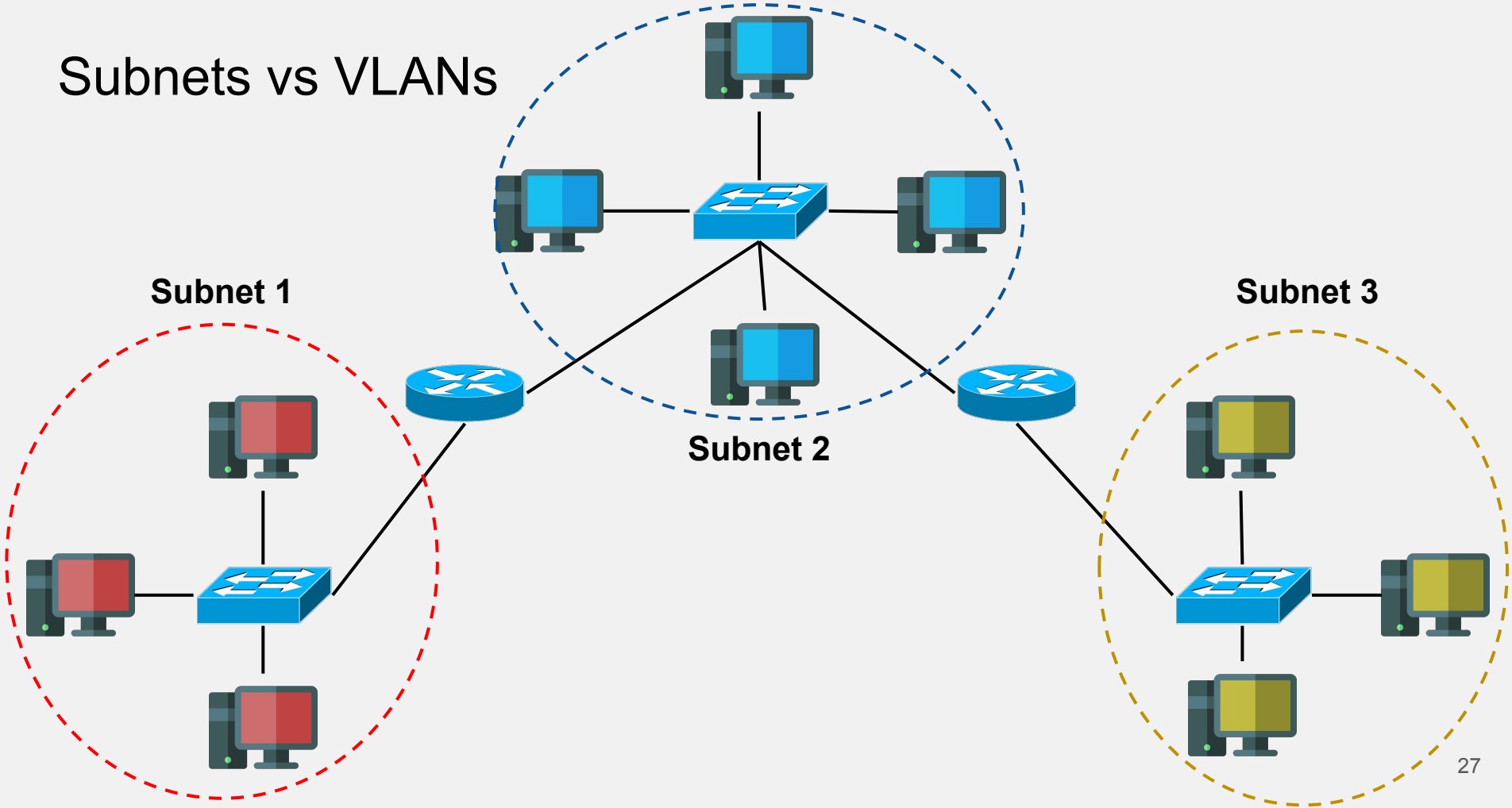
Logical route at the end.

VLANs

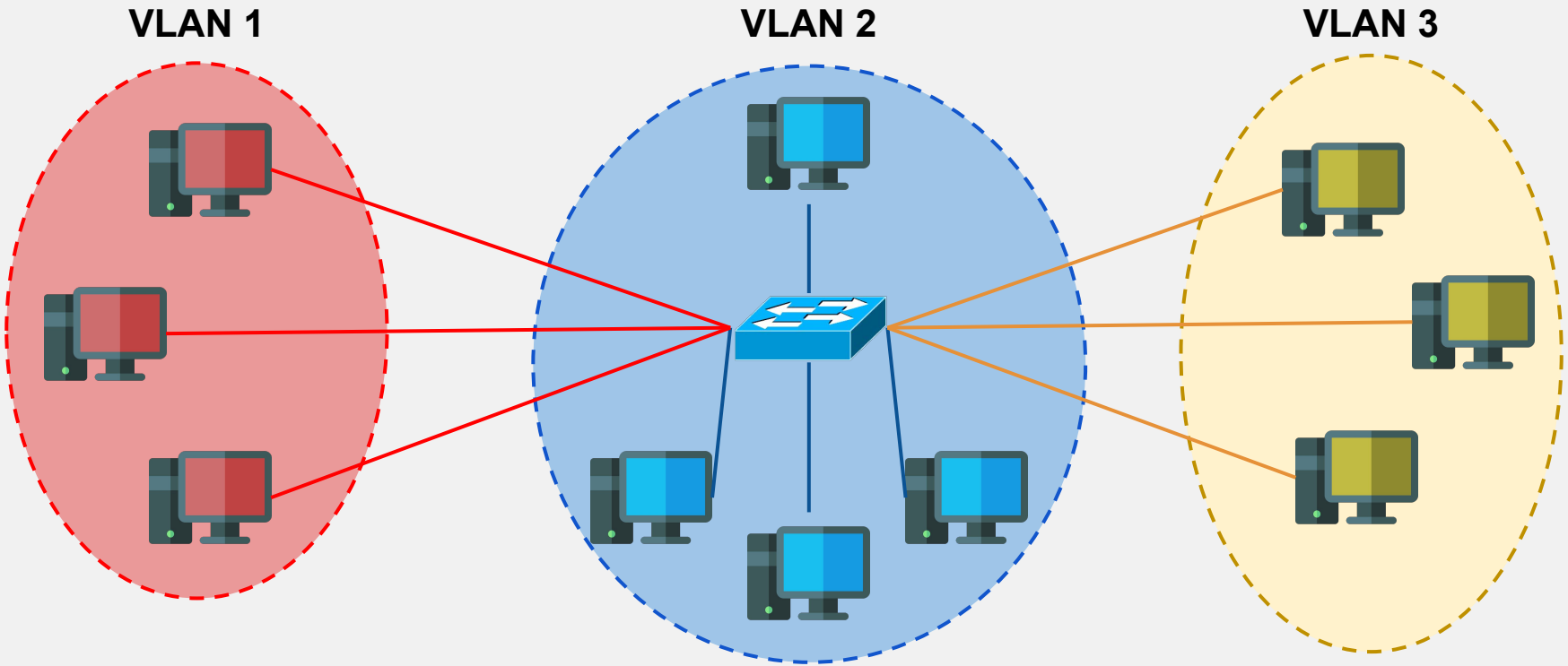
Subnets vs VLANs



Subnets vs VLANs



Subnets vs VLANs

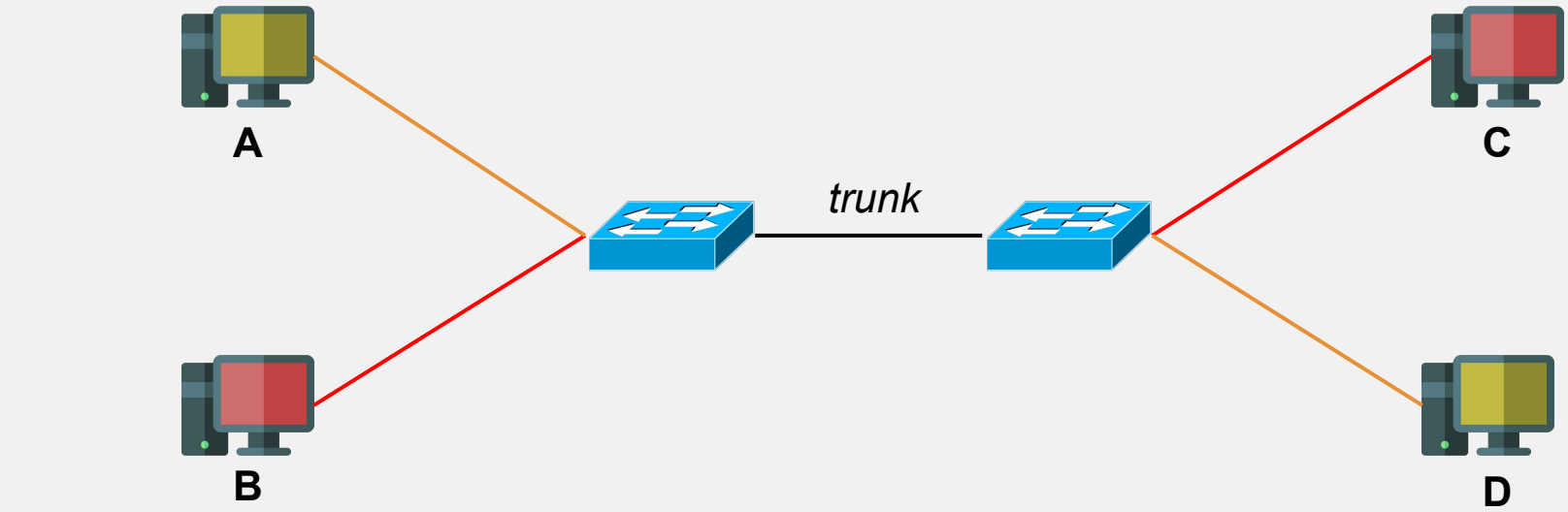


Virtual LAN (VLAN)

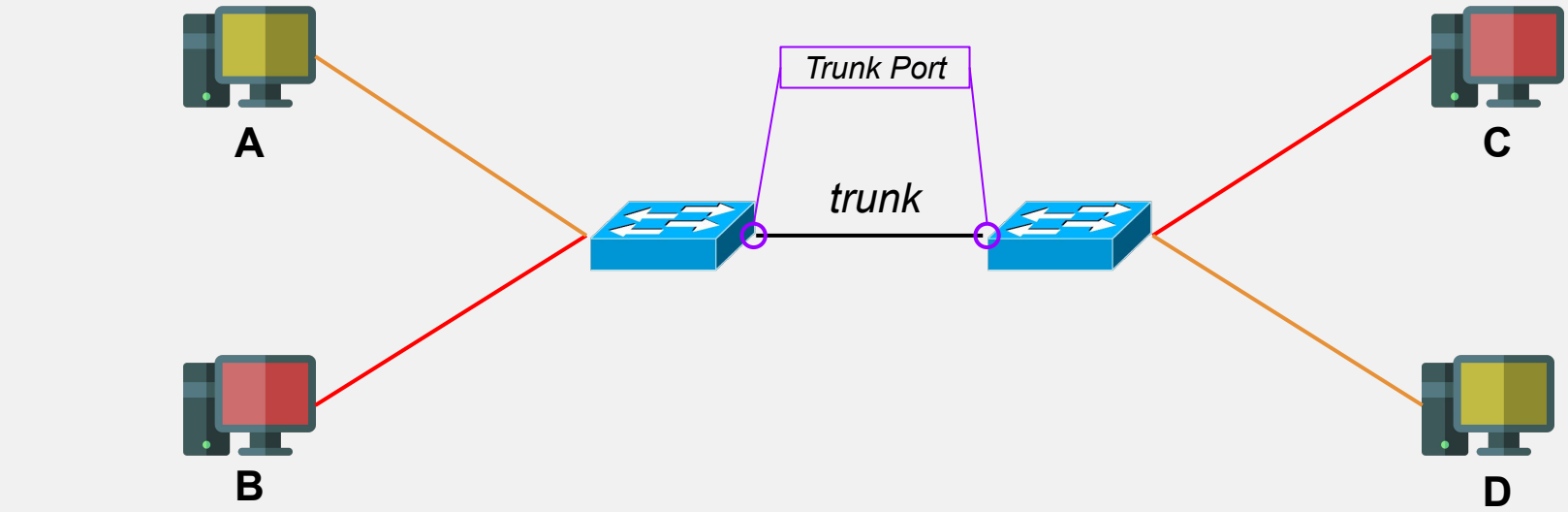
VLAN:

- Defined in IEEE 802.1Q, also known as Dot1Q.
- Logical separation of broadcast domain.
- Can also be used between switches.

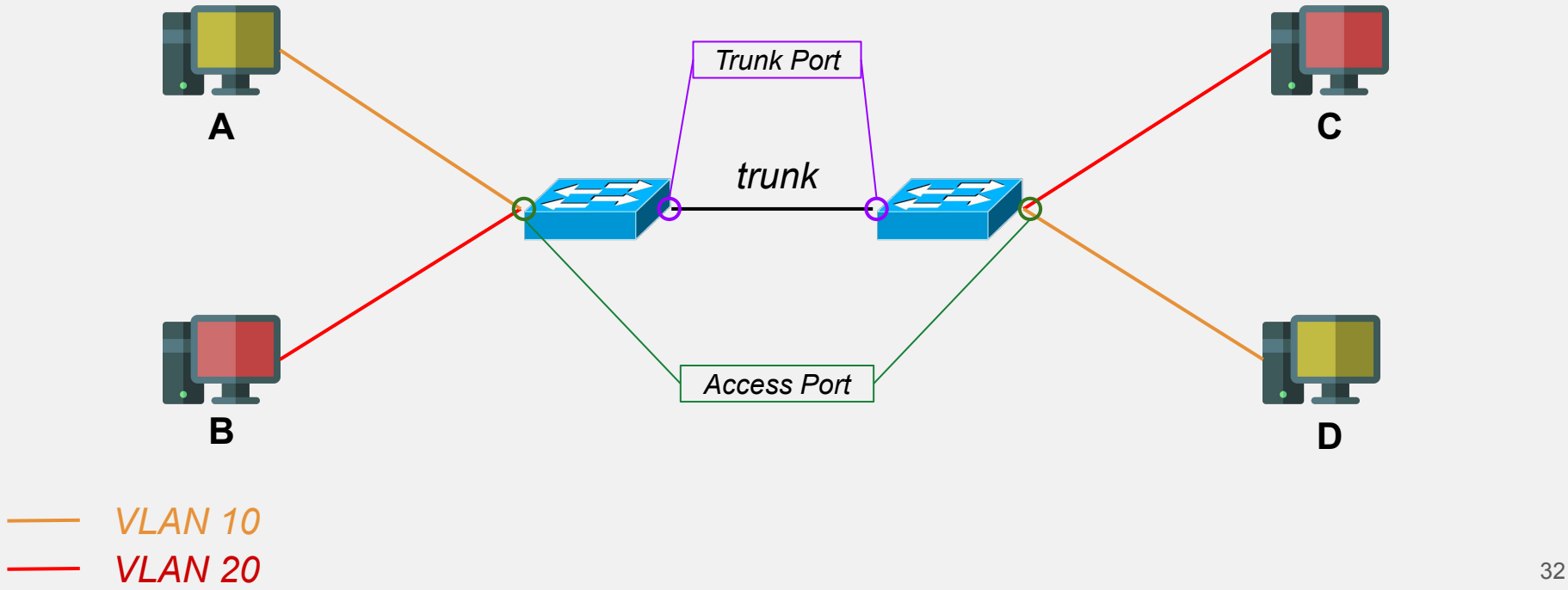
VLAN: Trunking 1/6



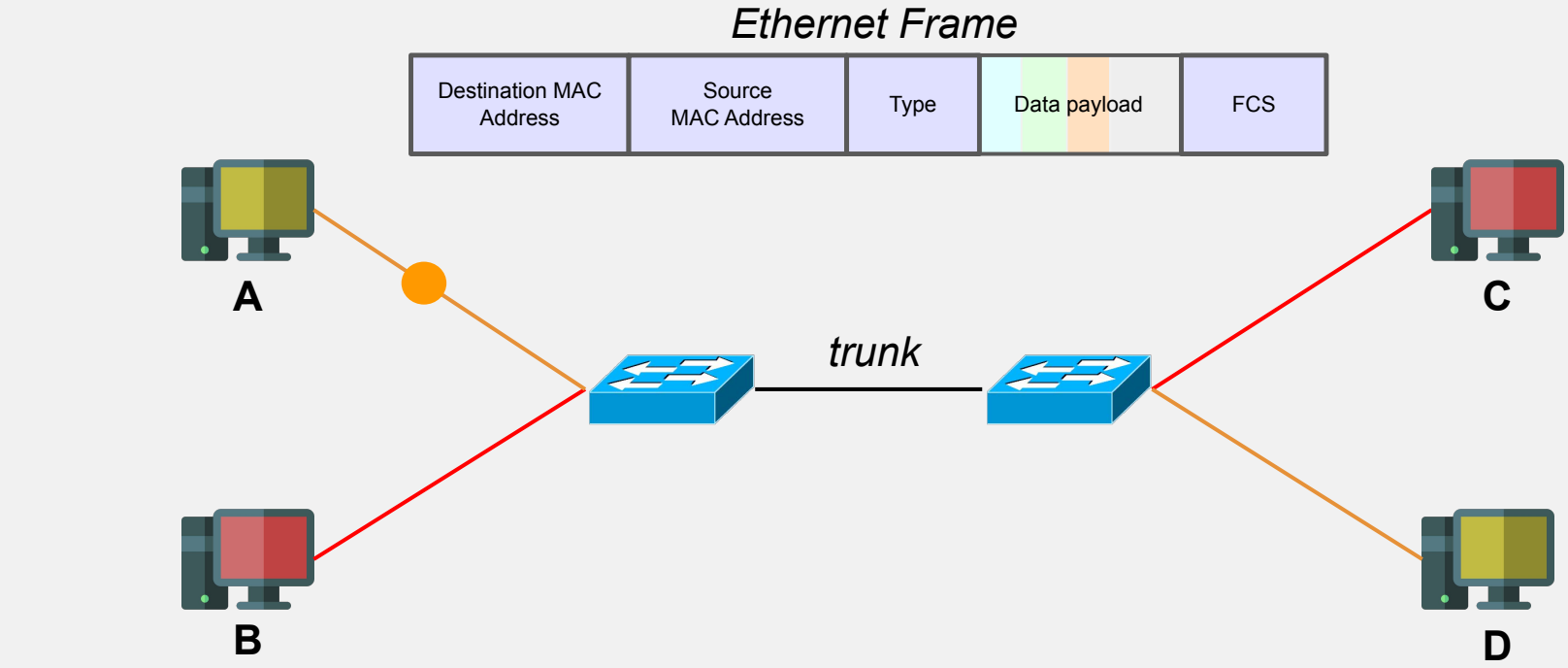
VLAN: Trunking 2/6



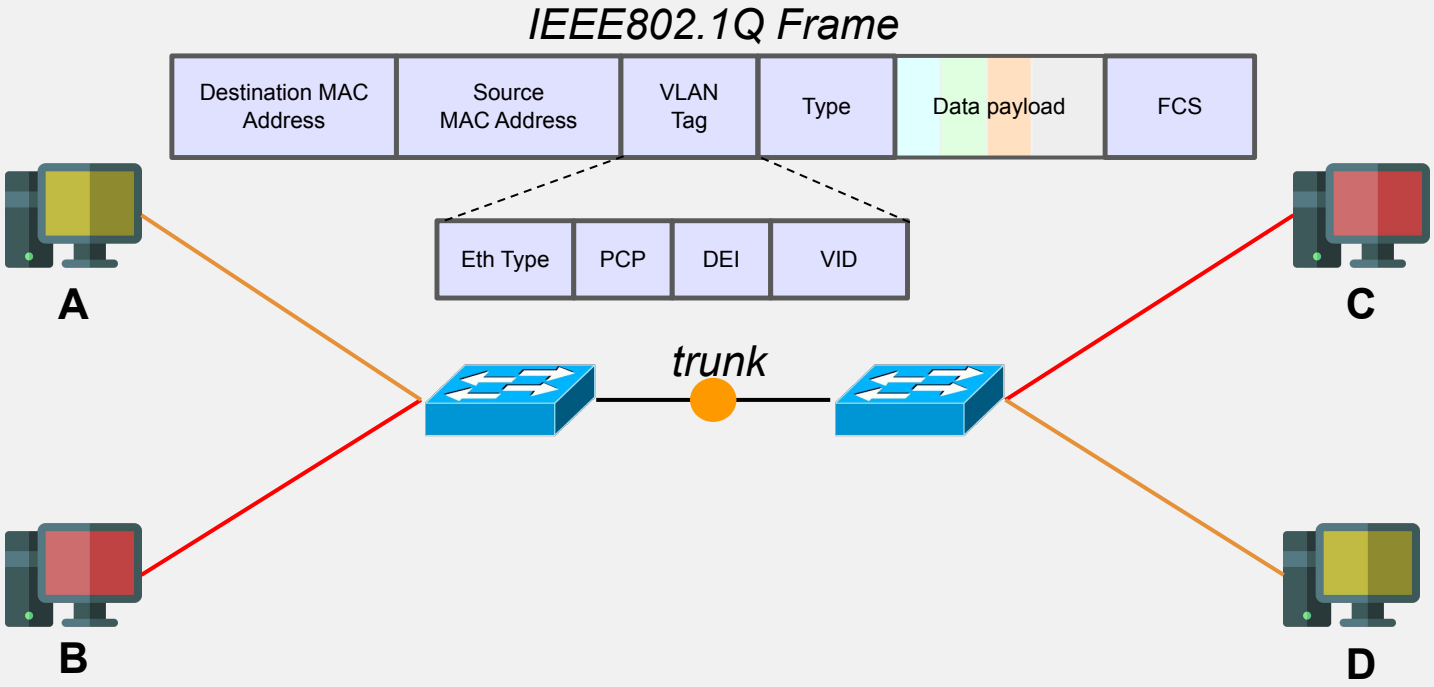
VLAN: Trunking 3/6



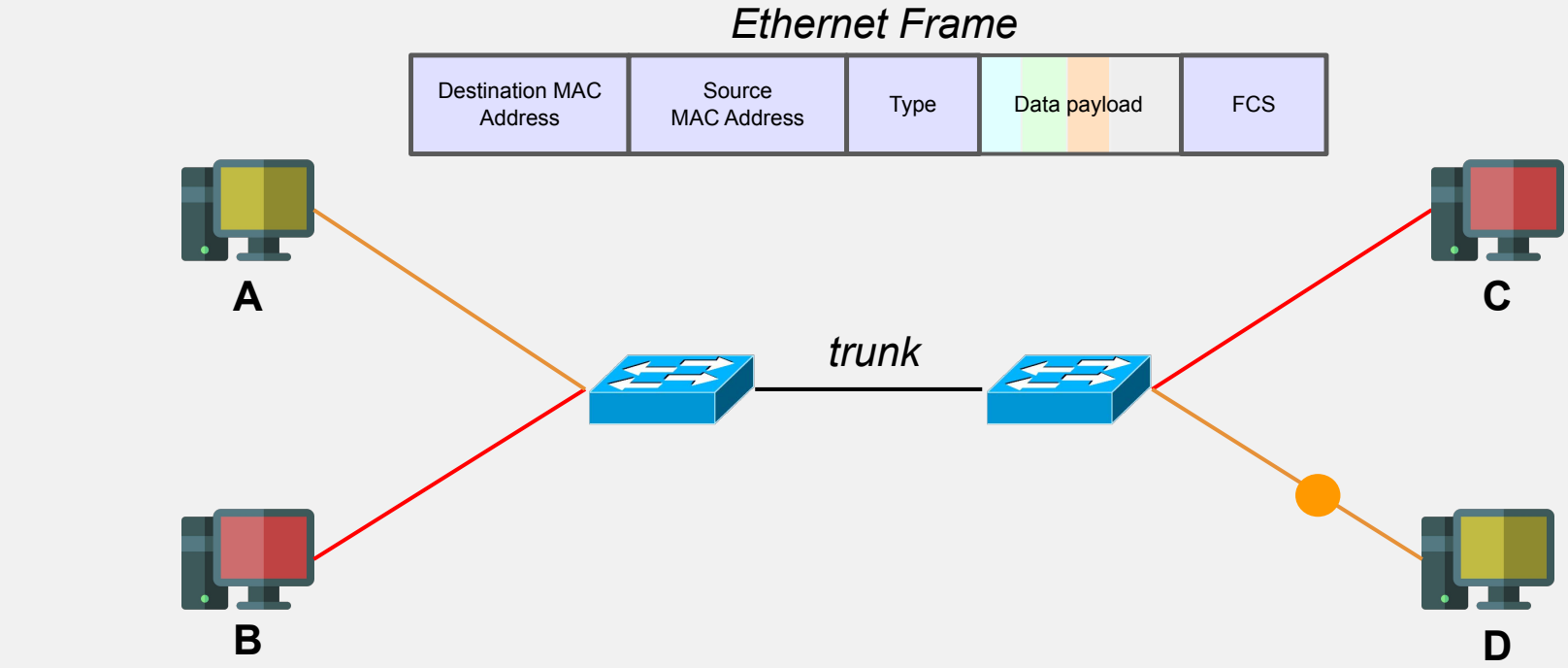
VLAN: Trunking 4/6



VLAN: Trunking 5/6



VLAN: Trunking 6/6



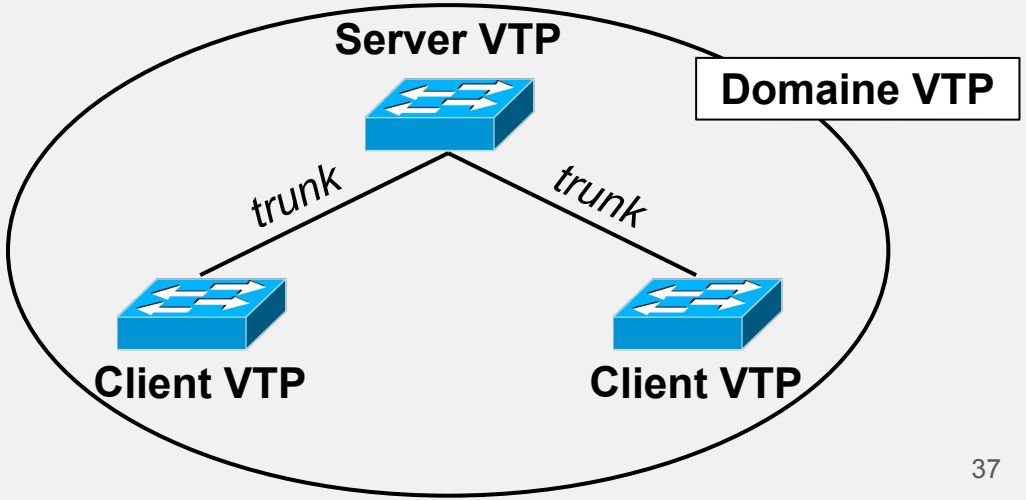
Default VLAN vs Native VLAN

- **Default VLAN:**
  - All non configured port will be assigned to the default VLAN (**VLAN1**).
- **Native VLAN:**
  - By default set to the default VLAN.
  - **Untagged traffic** between switches through a trunk link.
  - Backward compatibility for non-VLAN switches.
  - Control and management protocol traffic (e.g. STP, VTP, DTP).

VLAN Trunking Protocol (VTP)

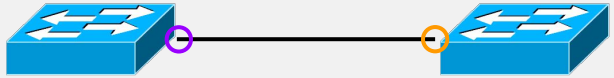
- **VTP**
  - Proprietary protocol of Cisco.
- Allow VLAN configurations to be propagated to nearby switches.

- **Server:**
  - Create, modify, delete VLANs.
  - Sync configurations.
- **Client:**
  - Cannot change VLANs.
  - Sync configurations.



Dynamic Trunking Protocol (DTP) 1/2

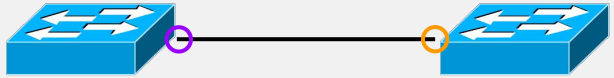
- **DTP**
  - Proprietary protocol of Cisco.
- Allow auto port configuration between switches for trunking.



- **Per port configuration:**
  - **Access**: force port to be an access port.
  - **Trunk**: force port to be a trunk port.
  - **Dynamic desirable**: Tell the connected port that it would like to be a trunk port.
  - **Dynamic**: Adapt to the connected port.

Dynamic Trunking Protocol (DTP) 2/2

- **DTP**
  - Proprietary protocol of Cisco.
- Allow auto port configuration between switches for trunking.



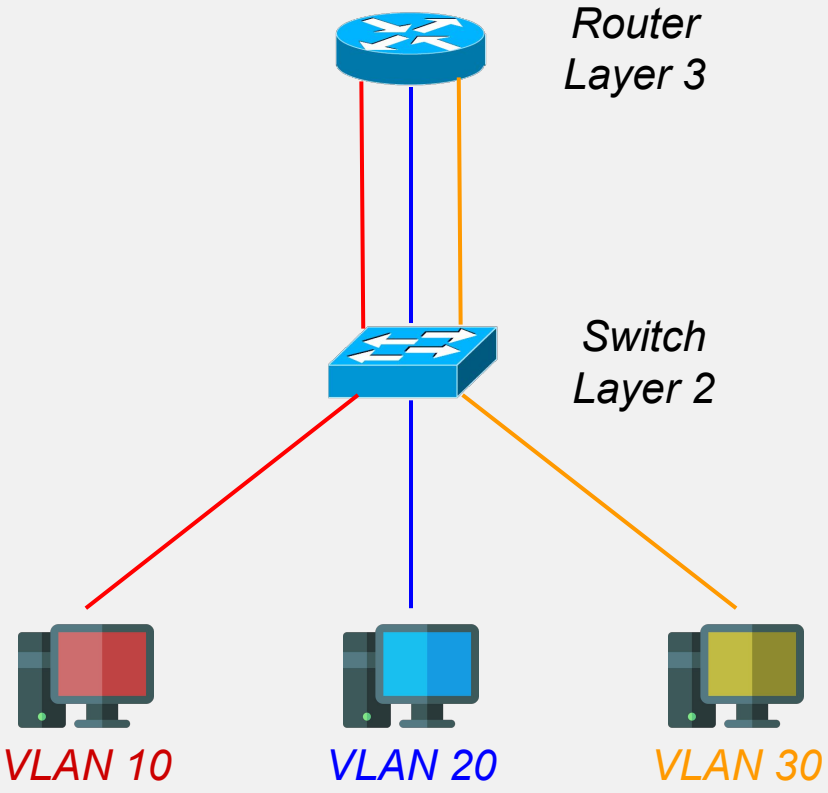
	Access	**Trunk**	**Dynamic Desirable**	**Dynamic auto**
Access	Access	*Limited*	Access	Access
Trunk	*Limited*	Trunk	Trunk	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk
Dynamic auto	Access	Trunk	Trunk	Access

InterVLAN Routing

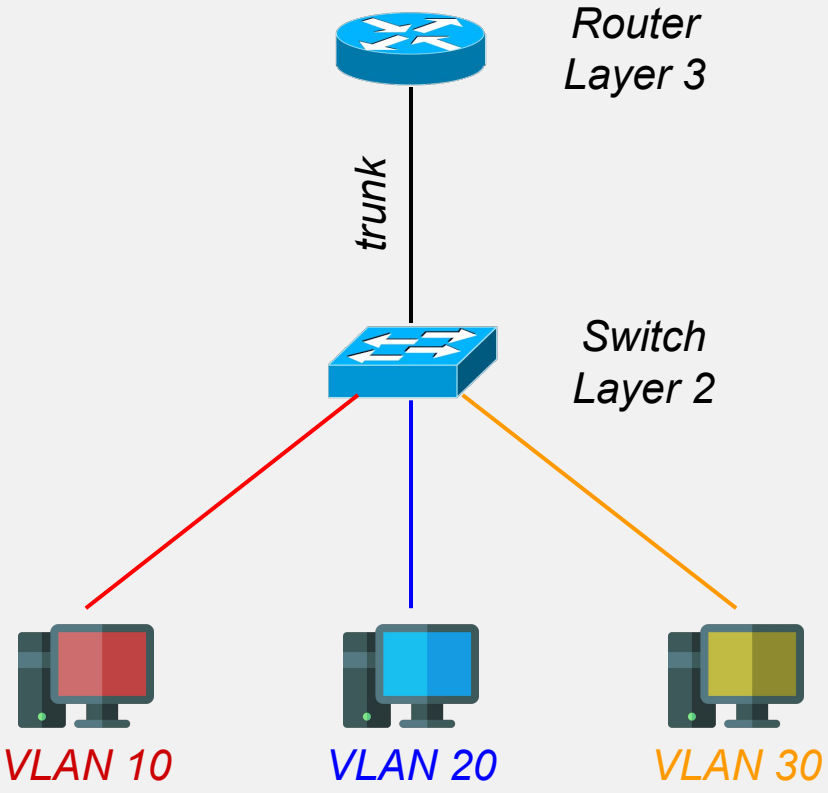
InterVLAN communication

- VLANs are logically isolated from each other in the LAN.
- To communicate they need to a gateway:
  - Using a router.
  - Using a router with trunk.
  - Using a multilayer switch.

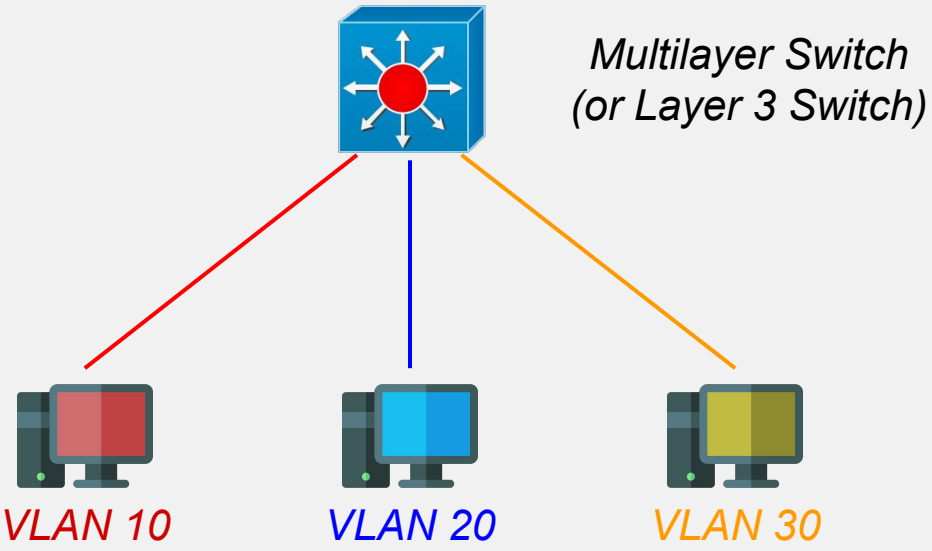
InterVLAN: Router



InterVLAN: Router on stick



InterVLAN: Multilayer Switch

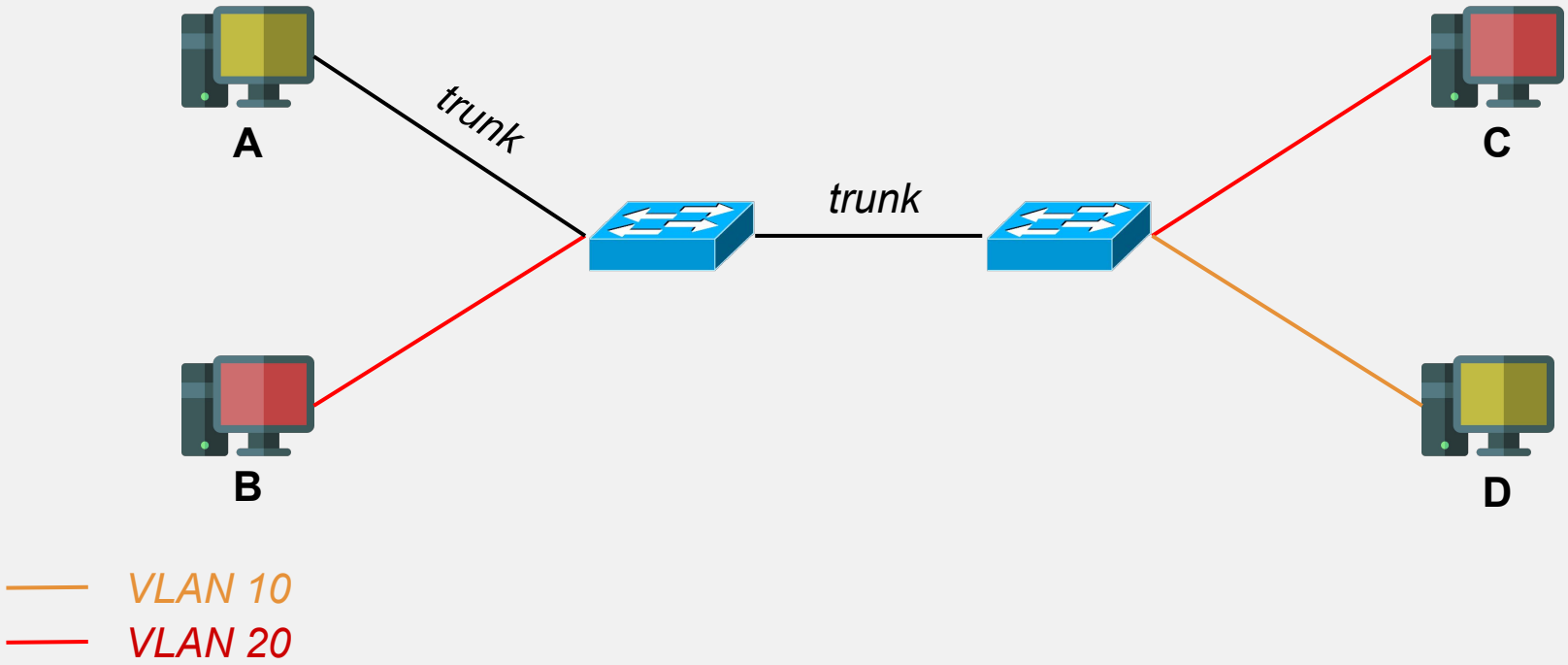


VLAN Hopping Attacks

VLAN Hopping: Switch Spoofing 1/3

- DTP used to create a trunk line between the attacker and a switch.
- The attacker is now part of all VLANs.

VLAN Hopping: Switch Spoofing 2/3



VLAN Hopping: Switch Spoofing 3/3

- Mitigation:
  - Disable trunking on all access ports.
  - Disable auto trunking on all trunk lines.

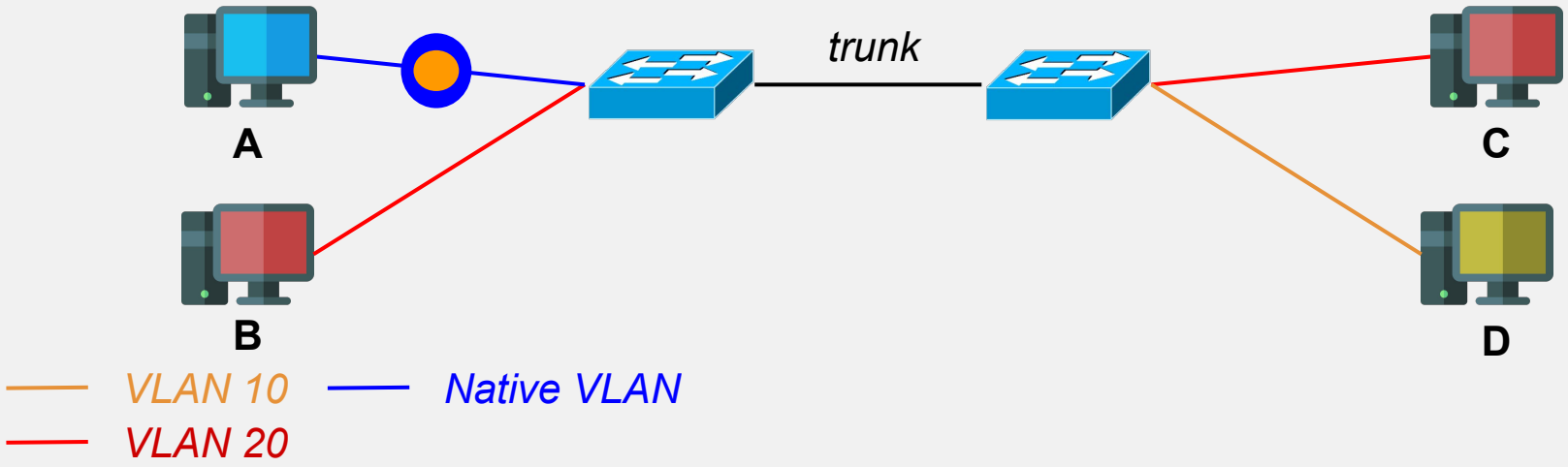
VLAN Hopping: Double Tagging 1/5

- Attacker port is connected to the native VLAN on Switch 1.
- Attacker sends a frame with two VLAN tags:
  - Outer tag = Native VLAN ID.
  - Inner tag = Victim VLAN ID.
- Switch 1 receives the frame:
  - Removes the outer native VLAN tag (frames in the native VLAN are sent untagged).
  - Forwards the now single-tagged frame over the trunk link.
- Switch 2 receives the frame on the trunk:
  - Sees the VLAN tag for the victim VLAN and forwards it into that VLAN.
  - Attacker’s traffic now reaches the victim VLAN without direct membership.

VLAN Hopping: Double Tagging 2/5

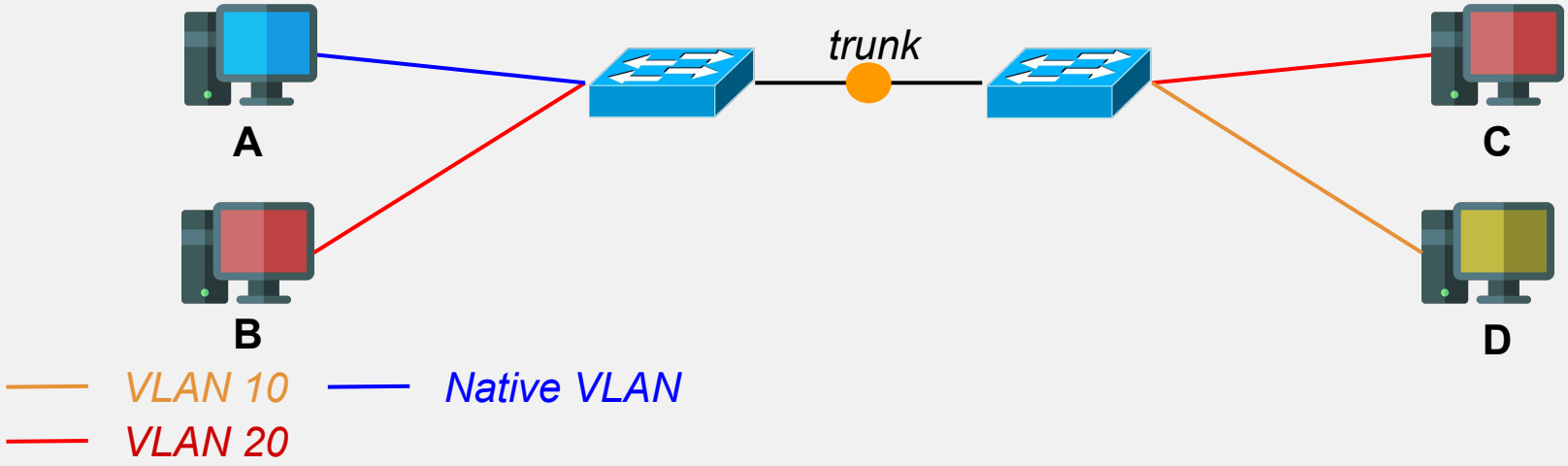
IEEE802.1Q Frame

Destination MAC Address	Source MAC Address	**Native VLAN Tag**	**Target VLAN Tag**	Type	Data payload	FCS

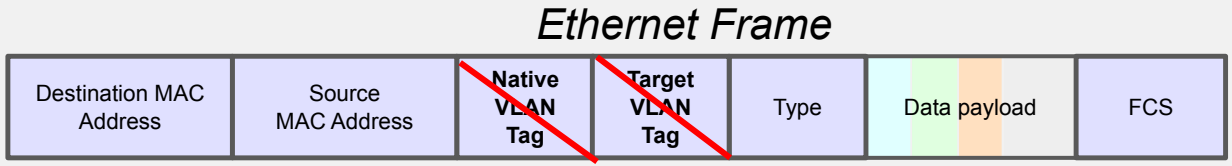


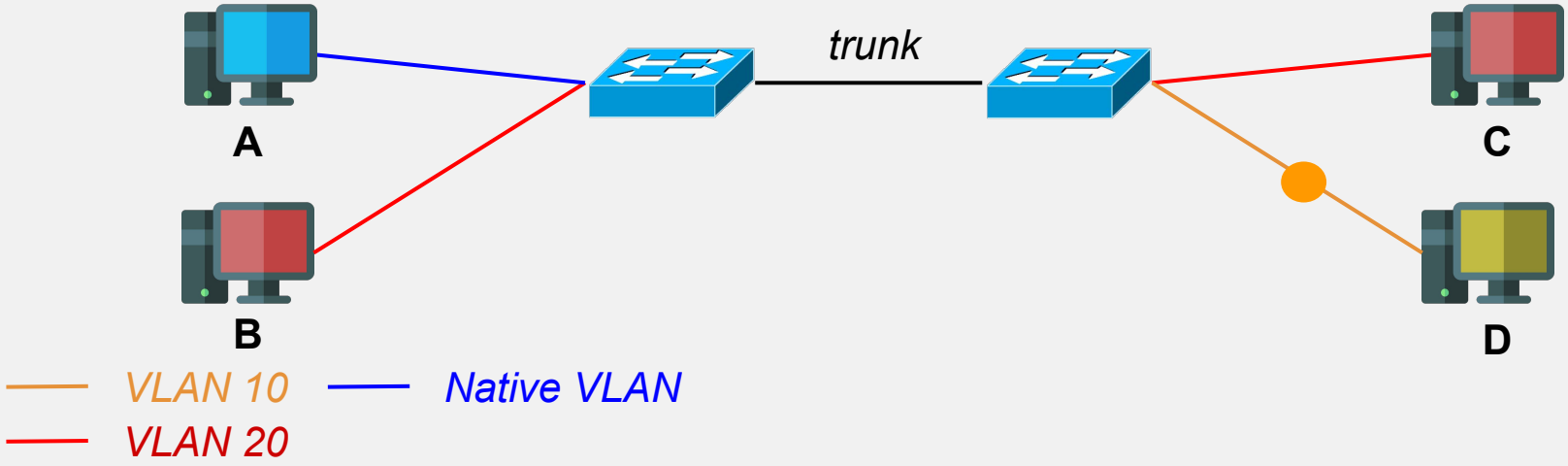
VLAN Hopping: Double Tagging 3/5

IEEE802.1Q Frame



VLAN Hopping: Double Tagging 4/5





VLAN Hopping: Double Tagging 5/5

- Limitation:
  - One way communication: the victim will not answer with a double tag.
- Mitigation:
  - Change the native VLAN to be different than the default one (VLAN1).
  - Disable unused ports and put them in an unused VLAN (e.g., 1234, 666).
  - Disable trunking on all access ports.

Resources and Acknowledgements

- Cisco Documentation
- Computer Networking: A Top-down Approach by James F. Kurose, Keith W. Ross