Transparent Bridging and VLAN

Plug and Play Networking

Algorhyme

I think that I shall never see
a graph more lovely than a tree
a graph whose crucial property
is loop-free connectivity.
A tree which must be sure to span
so packets can reach every lan.
first the root must be selected
by ID it is elected.
least cost paths to root are traced,
and in the tree these paths are place.
mesh is made by folks like me;
bridges find a spanning tree.

Radia Perlman

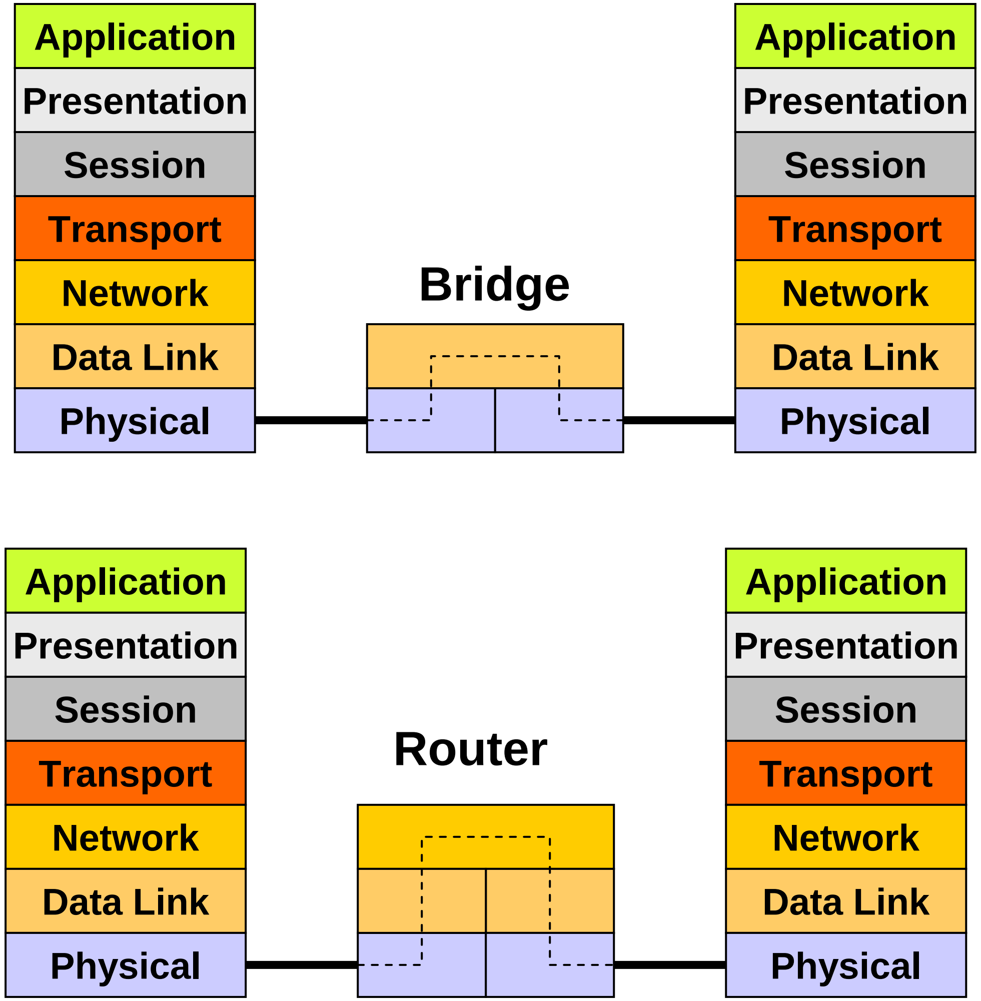
Bridge History

- Bridges came after routers!
- First bridge designed by Radia Perlman
  - Ethernet has size limitations
  - Routers were single protocol and expensive
- Spanning Tree because Ethernet had no hop count
- IEEE 802.1D
  - Bridging and Spanning Tree Protocol

What is Bridging?

- Layer 2 packet forwarding principle
- Separate two (or more) shared-media LAN segments with a bridge
  - Only frames destined to the other LAN segment are forwarded
  - Number of collisions reduced (!)
- Different bridging principles
  - Ethernet: Transparent Bridging
  - Token Ring: Source Route Bridging

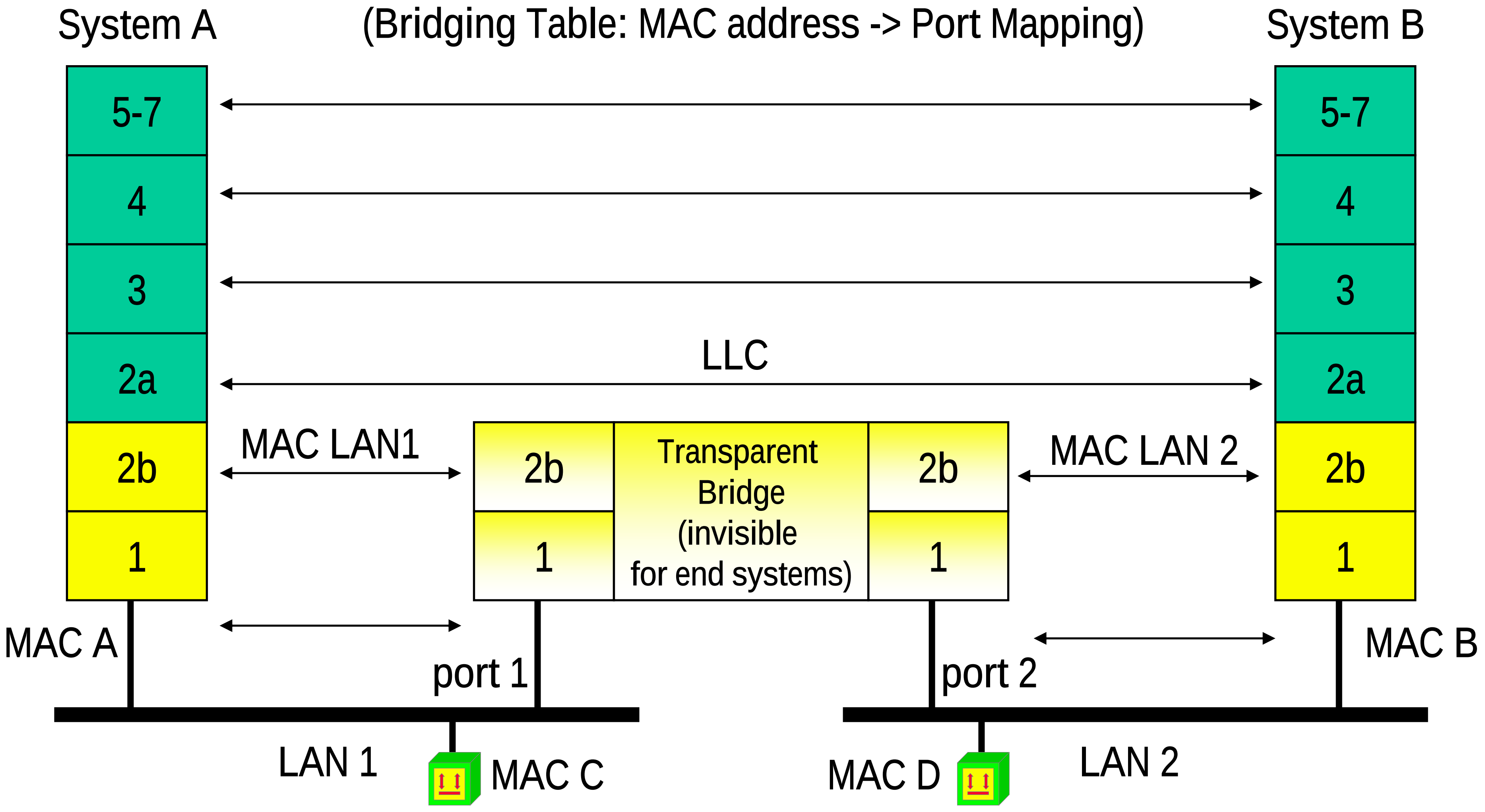
OSI Comparison



- MAC addresses not routable
  - NetBios over NetBEUI not routable (no L3)
- Bridge supports different physical media on each port
  - E.g. 10Mbit/s to 100Mbit/s
- Router supports different layer-2 technologies
  - E.g. Ethernet to Frame Relay

Transparent Bridge = Ethernet Switch

Packet Switching (PS) in Connectionless Service Mode on OSI Layer 2
Routing Table (Signposts) –> Bridging Table (= Ethernet Switch Table)
(Bridging Table: MAC address -> Port Mapping)

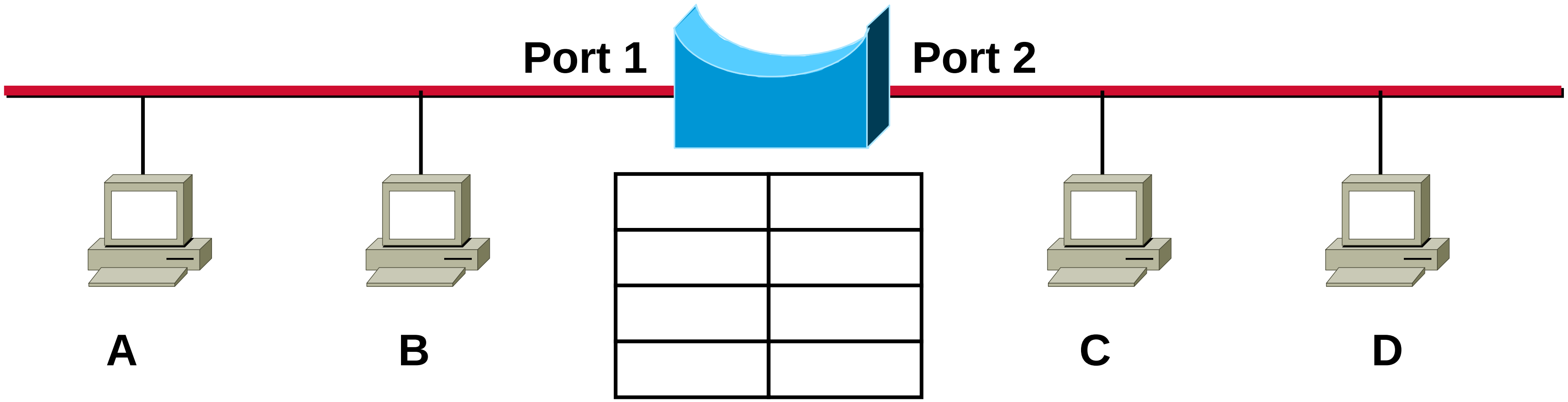


Bridging vs Routing

- Bridging works on OSI layer 2
  - Forwarding of frames
  - Use MAC addresses only
  - Termination of physical layer (!)
- Routing works on OSI layer 3
  - Forwarding of packets
  - Use routable addresses only (e.g. IP)
  - Termination of both layer 1 and 2

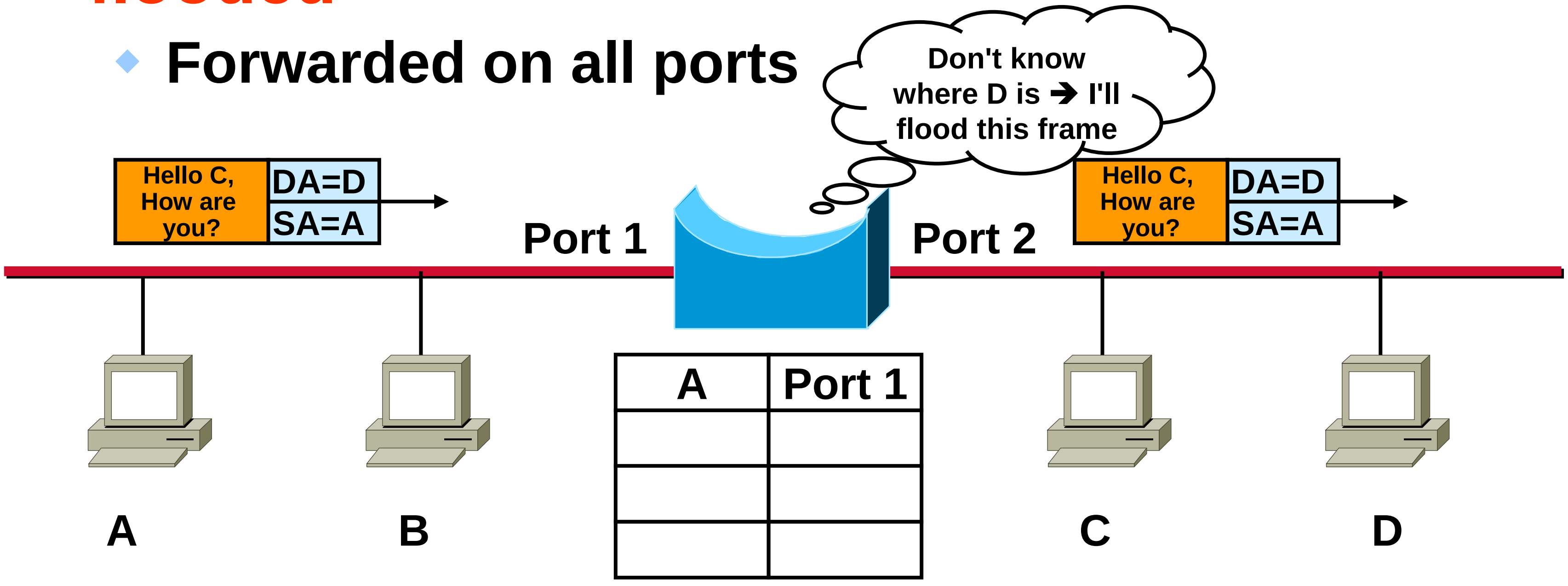
How does it work?

- Transparent bridging is like "plug & play"
- Upon startup a bridge knows nothing
- Bridge is in learning mode



Learning

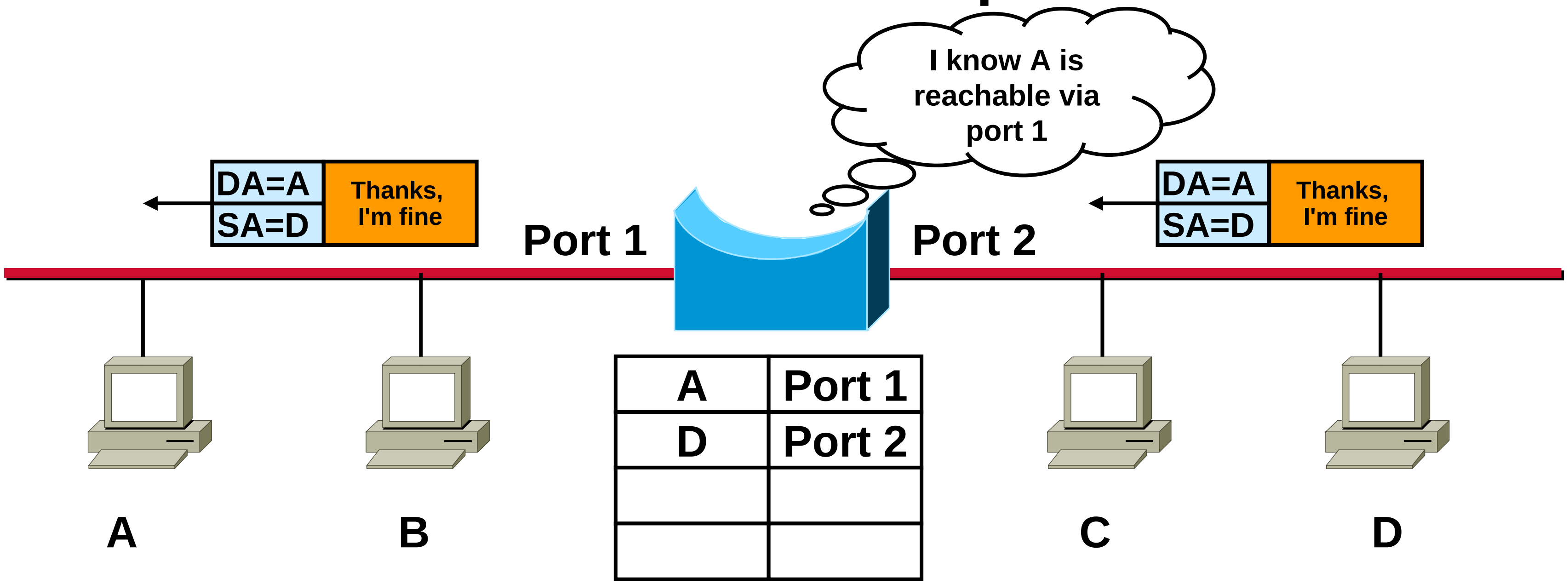
- Once stations send frames the bridge notices the source MAC address
  - Entered in bridging table
- Frames for unknown destinations are flooded
  - Forwarded on all ports



A	Port 1

Learning ➔ Table Filling

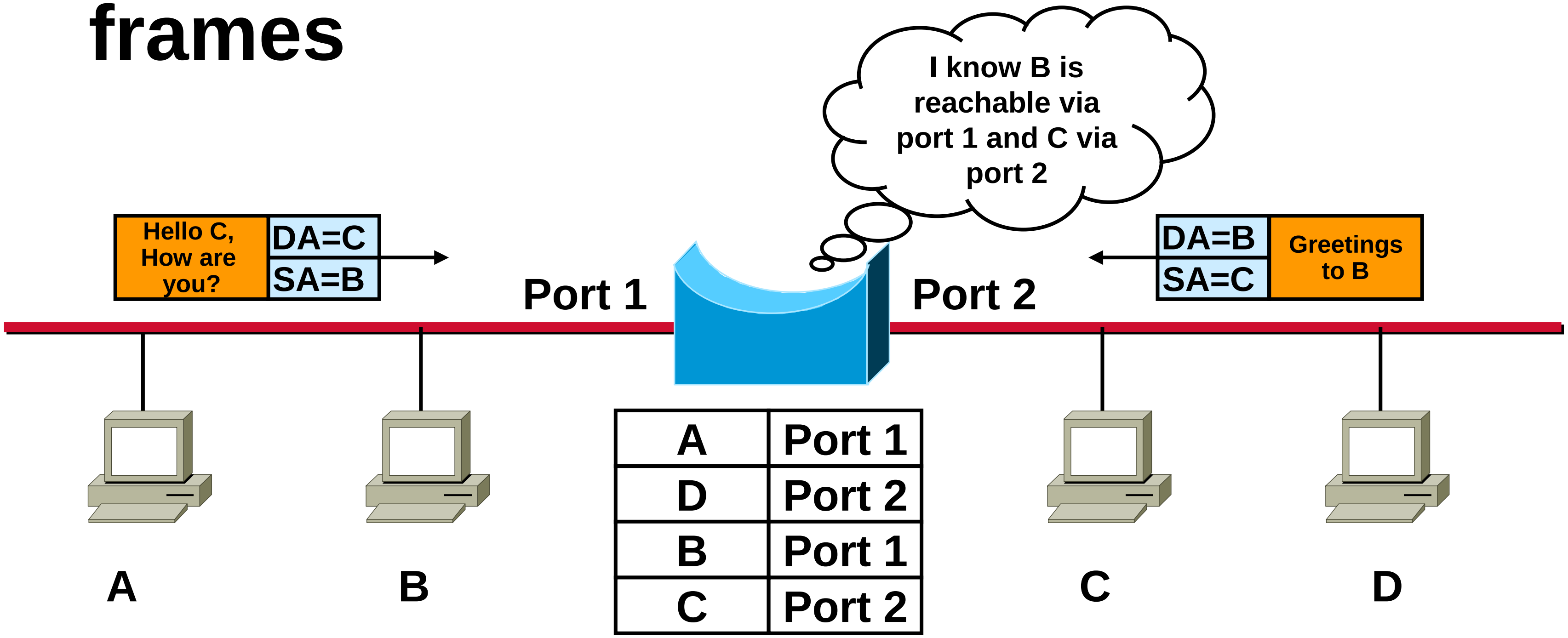
- If the destination address matches a bridging table entry, this frame can be actively
  - **forwarded** if reachable via other port
  - **filtered** if reachable on same port



A	Port 1
D	Port 2

Learning → Table Filling

- After some time the location of every station is known – simply by listening!
- Now only forwarding and filtering of frames

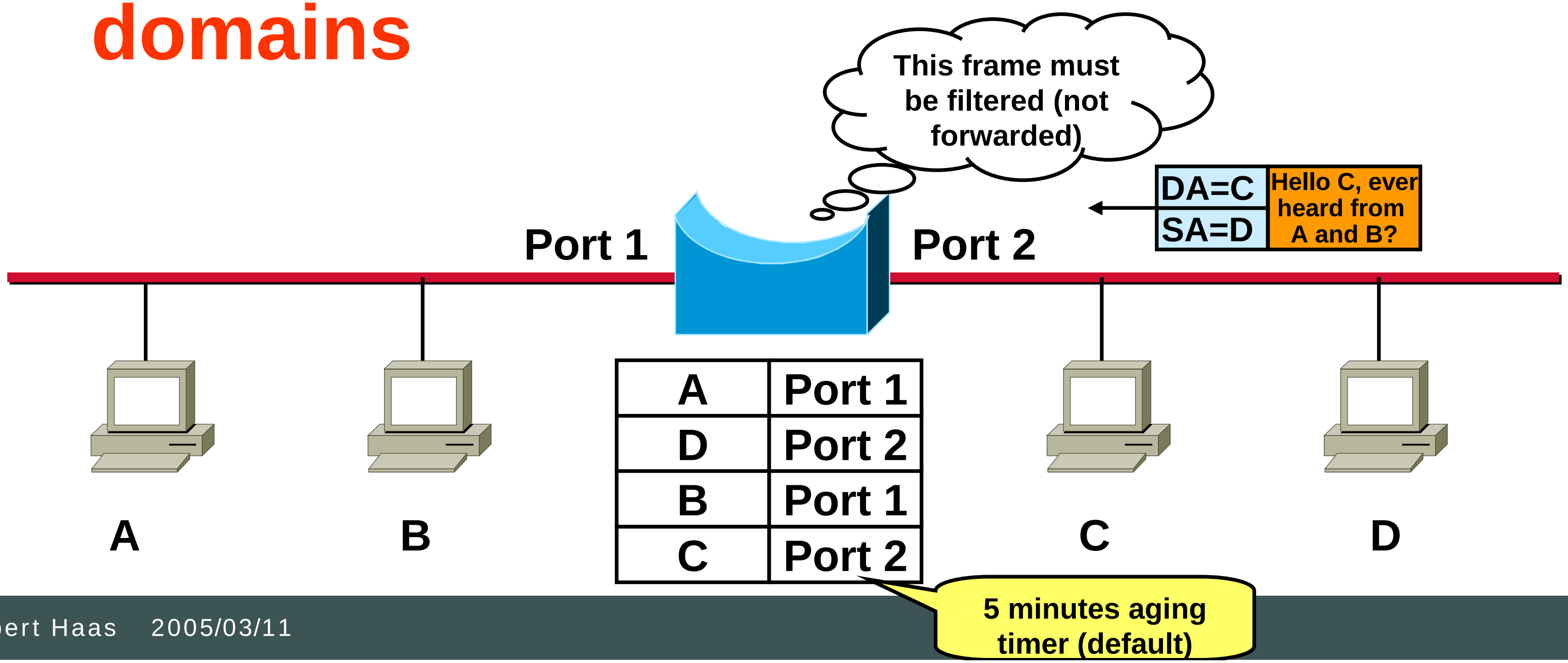


I know B is reachable via port 1 and C via port 2

A	Port 1
D	Port 2
B	Port 1
C	Port 2

Forwarding and Filtering

- Frames whose source and destination address are reachable over the same bridge port are filtered
- LAN separated into two collision domains



This frame must be filtered (not forwarded)
DA=C
SA=D
Hello C, ever heard from A and B?
Port 1
Port 2
A
B
C
D
5 minutes aging timer (default)

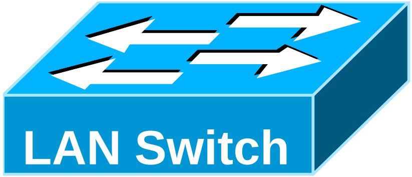
A	Port 1
D	Port 2
B	Port 1
C	Port 2

Most Important !

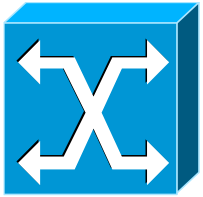
- Bridge separates LAN into multiple collision domains !
- A bridged network is still one broadcast domain !
  - Broadcast frames are always flooded
- A router separates the whole LAN into multiple broadcast domains

What is a Switch?

- A switch *is* basically a bridge, differences are only:



  - Faster because implemented in HW
  - Multiple ports
  - Improved functionality
- Don't confuse it with WAN Switching!
  - Completely different !
  - Connection oriented (stateful) VCs



In Principle (Logically)

Bridge = Switch

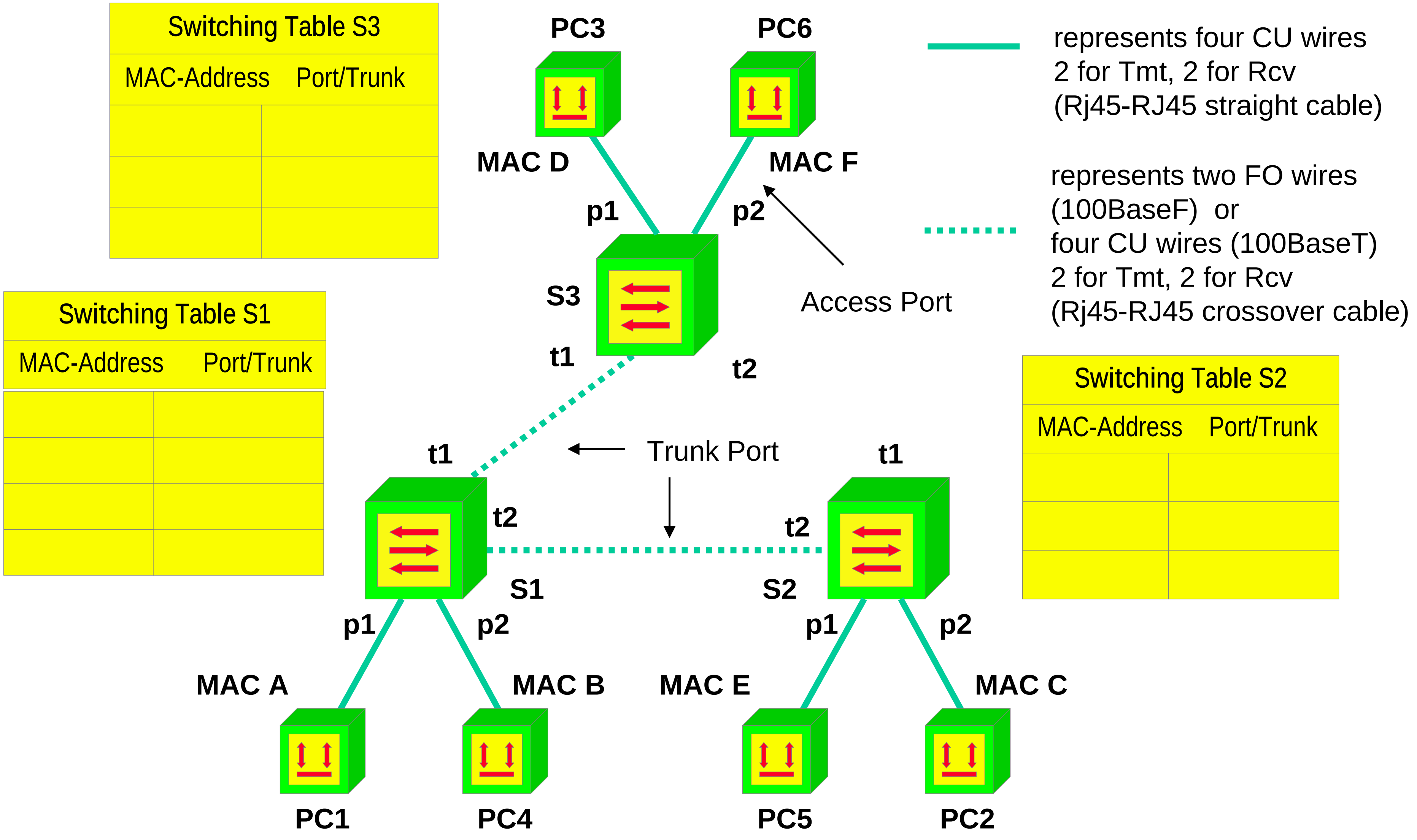
Since we use only switches today, let's talk about them…

Modern Switching Features

- Different data rates supported simultaneously
  - 10, 100, 1000, 10000 Mbit/s depending on switch
- Full duplex operation
- QoS
  - Queuing mechanisms
  - Flow control
- Security features
  - Restricted static mappings (DA associated with source port)
  - Port secure (Limited number of predefined users per port)
- Different forwarding
  - Store & Forward
  - Cut-through
  - Fragment-Free
- VLAN support (Trunking)
- Spanning Tree

Ethernet Switch Table - Power On

(MAC Address Table - Empty)



Switching Table S3	
MAC-Address	Port/Trunk

Switching Table S1	
MAC-Address	Port/Trunk

Switching Table S2	
MAC-Address	Port/Trunk

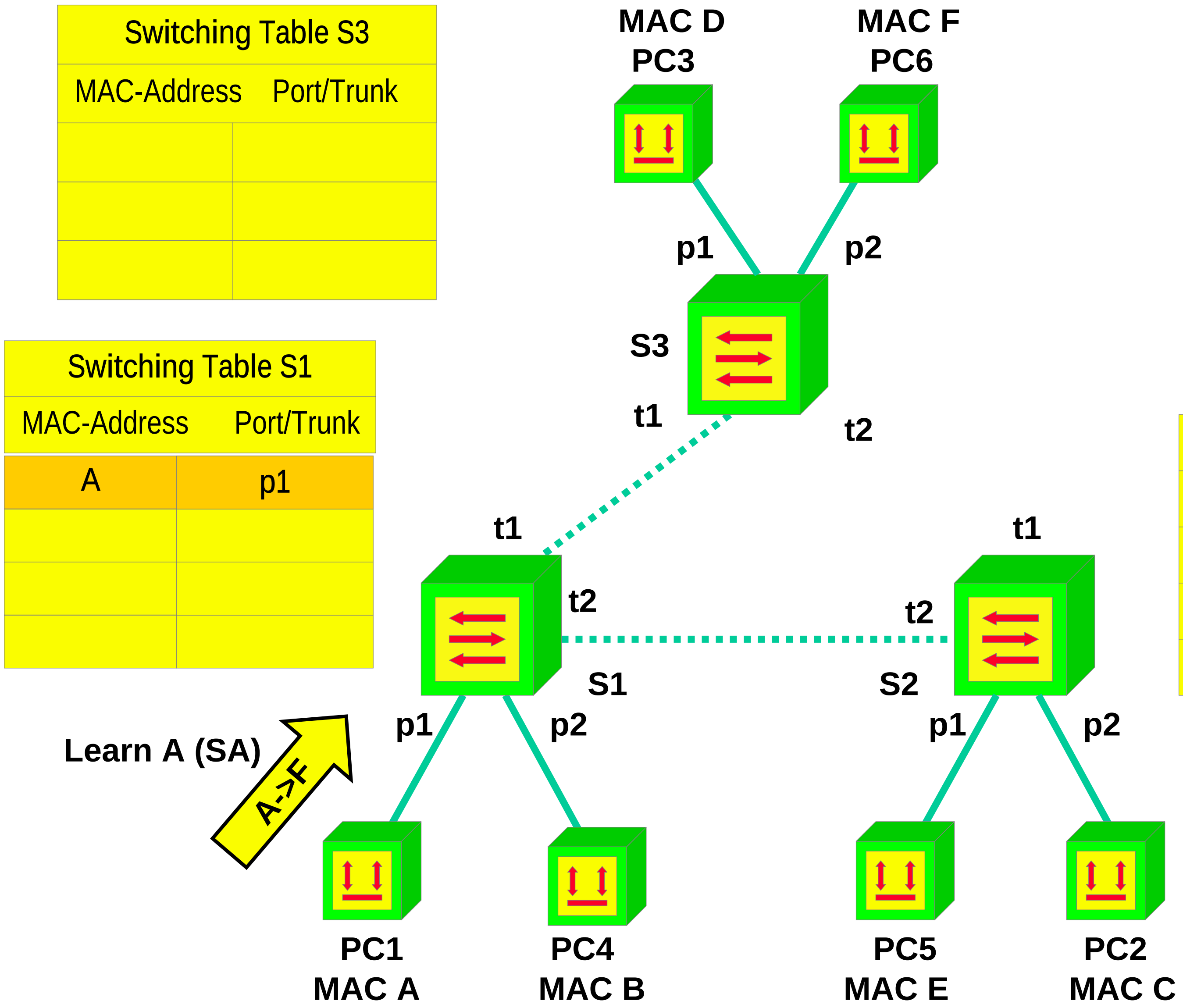
represents four CU wires
2 for Tmt, 2 for Rcv
(Rj45-RJ45 straight cable)

represents two FO wires
(100BaseF) or
four CU wires (100BaseT)
2 for Tmt, 2 for Rcv
(Rj45-RJ45 crossover cable)

Table Building for Ethernet Frame MAC-A to MAC-F 1

Switching Table S3	
MAC-Address	Port/Trunk

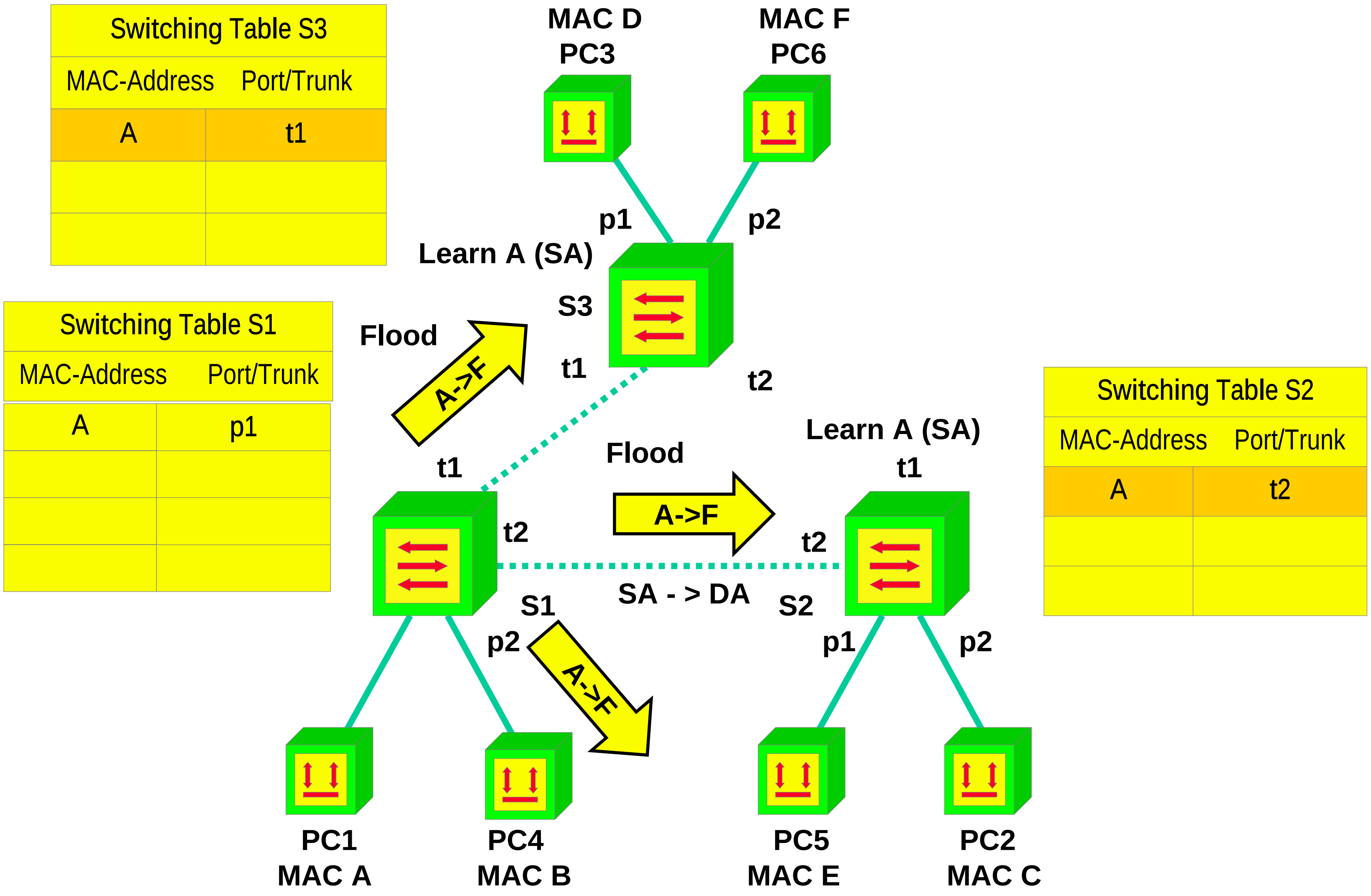
Switching Table S1	
MAC-Address	Port/Trunk
A	p1



Learn A (SA)

Switching Table S2	
MAC-Address	Port/Trunk

Table Building for Ethernet Frame MAC-A to MAC-F 2



Switching Table S3

MAC-Address	Port/Trunk
A	t1

Switching Table S1

MAC-Address	Port/Trunk
A	p1

Switching Table S2

MAC-Address	Port/Trunk
A	t2

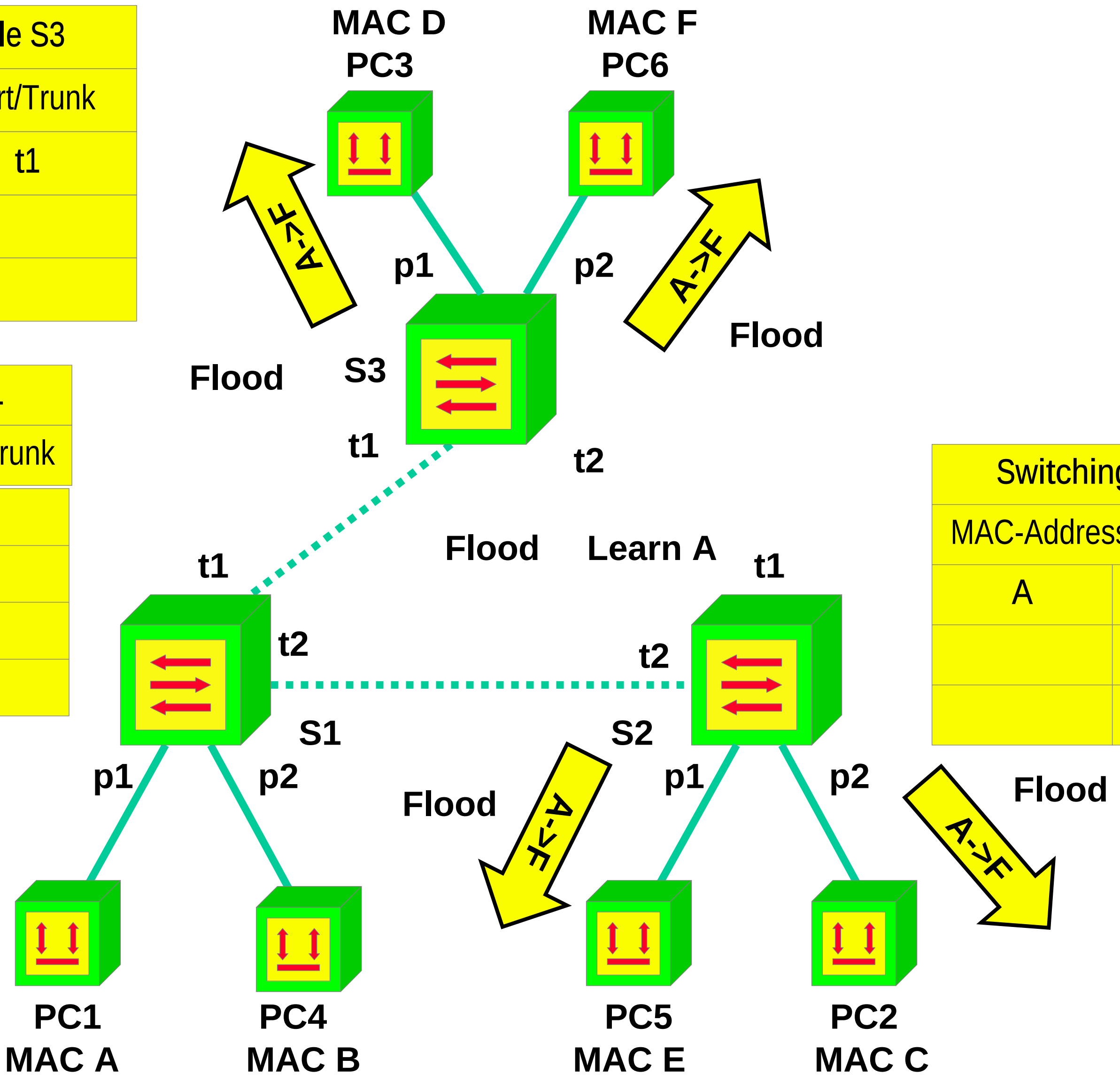
Table Building for Ethernet Frame MAC-A to MAC-F 3

Switching Table S3

MAC-Address	Port/Trunk
A	t1

Switching Table S1

MAC-Address	Port/Trunk
A	p1



Switching Table S2

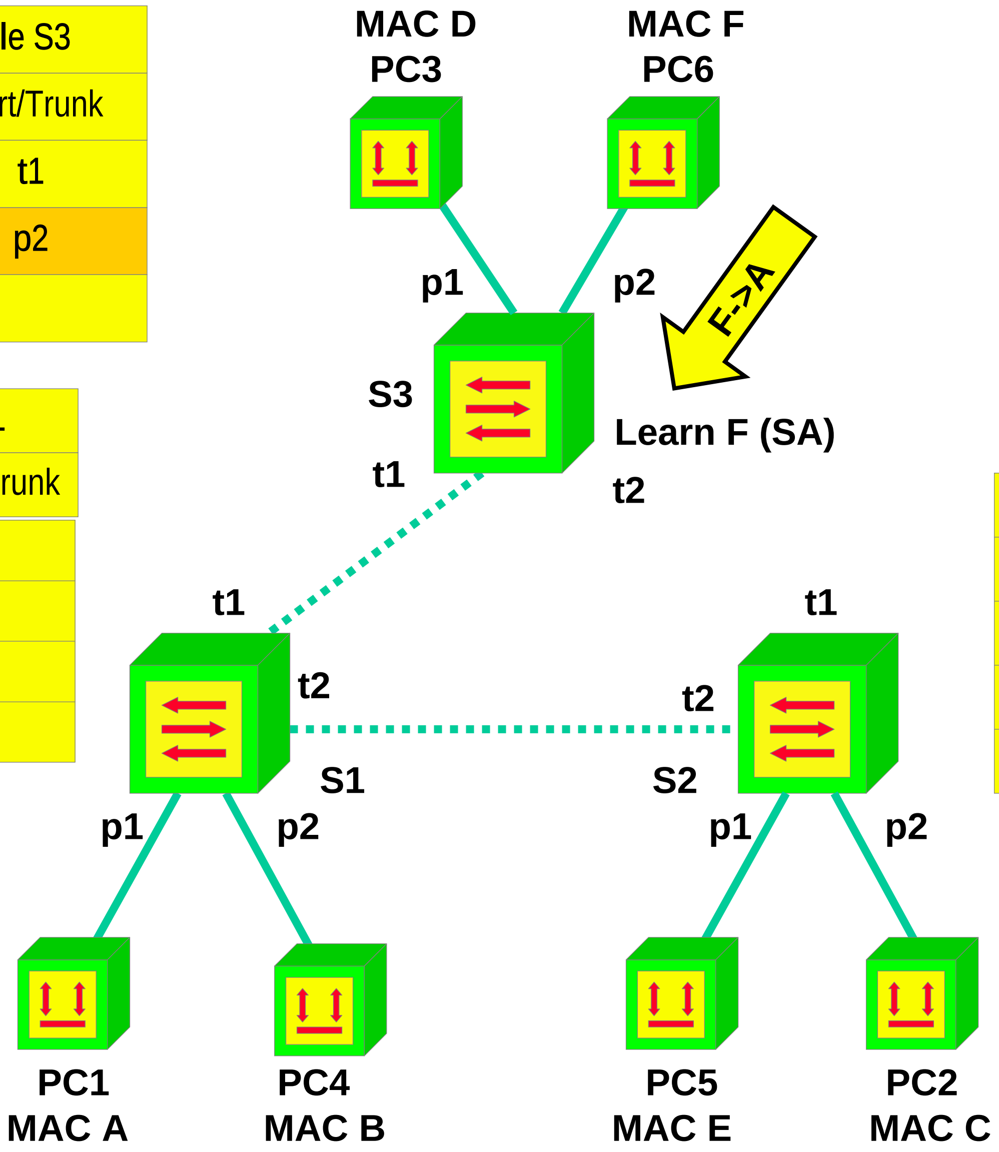
MAC-Address	Port/Trunk
A	t2

Table Building / Table Usage for Ethernet Frame MAC-F to MAC-A

1

Switching Table S3	
MAC-Address	Port/Trunk
A	t1
F	p2

Switching Table S1	
MAC-Address	Port/Trunk
A	p1

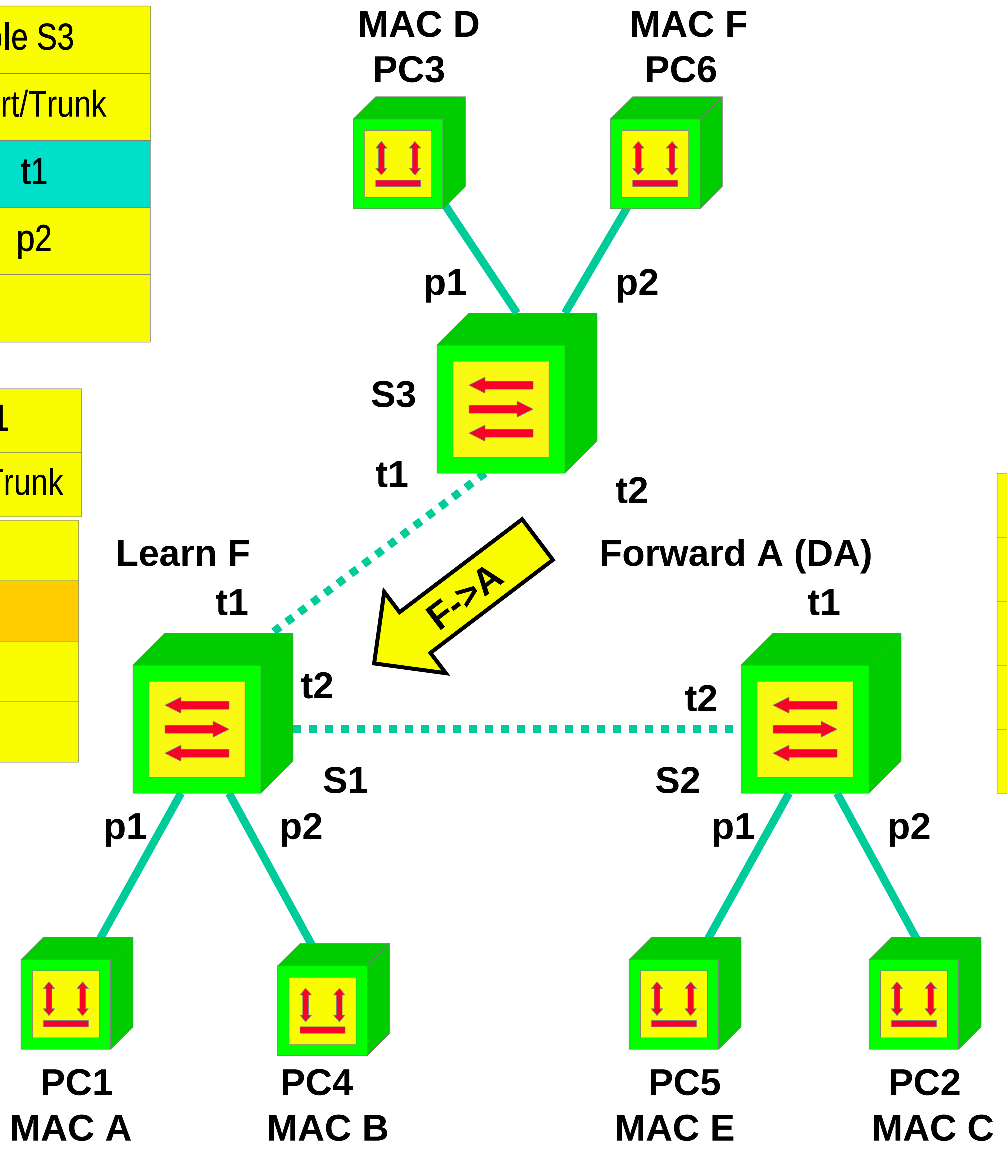


Switching Table S2	
MAC-Address	Port/Trunk
A	t2

Table Building / Table Usage (Forwarding Decision) for Ethernet Frame MAC-F to MAC-A 2

Switching Table S3	
MAC-Address	Port/Trunk
A	t1
F	p2

Switching Table S1	
MAC-Address	Port/Trunk
A	p1
F	t1



Switching Table S2	
MAC-Address	Port/Trunk
A	t2

Table Building / Table Usage (Forwarding Decision) for Ethernet Frame MAC-F to MAC-A 3

Switching Table S3

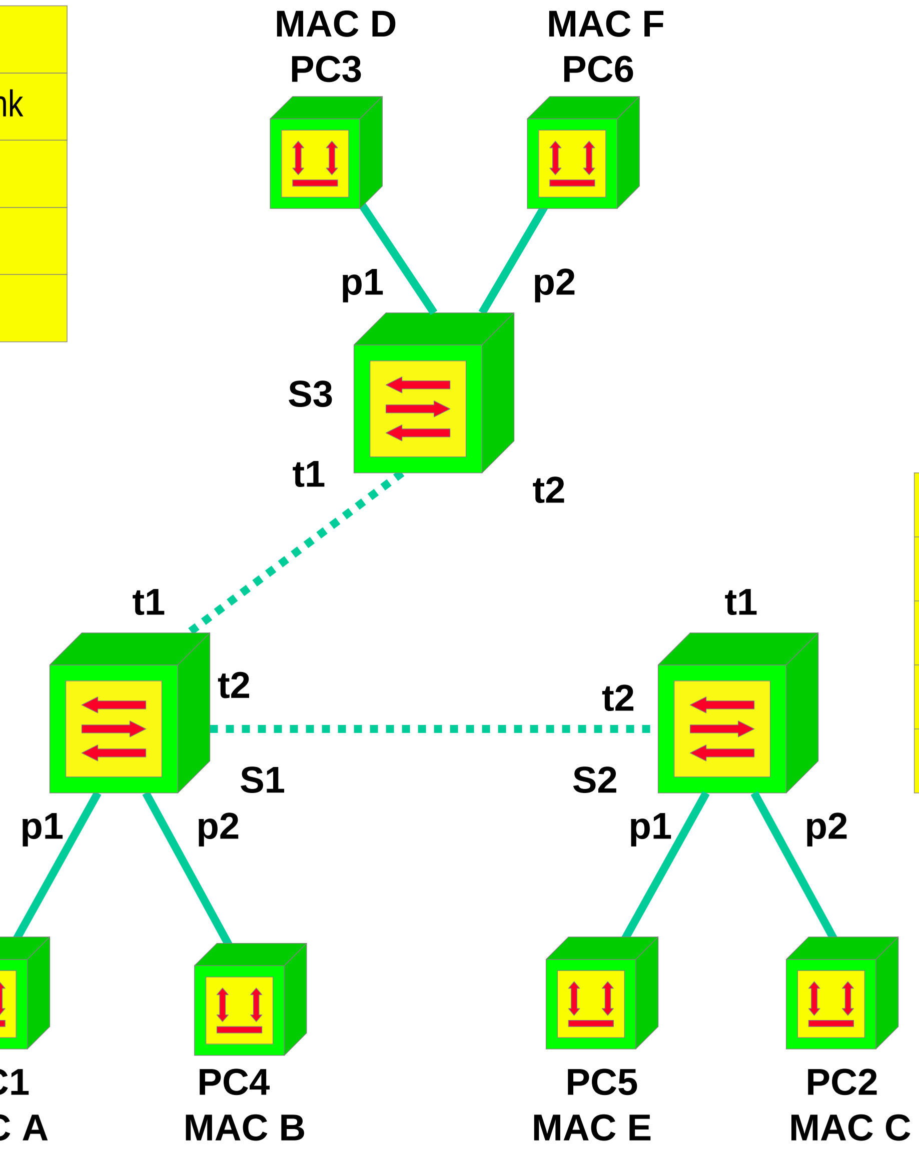
MAC-Address	Port/Trunk
A	t1
F	p2

Switching Table S1

MAC-Address	Port/Trunk
A	p1
F	t1

Switching Table S2

MAC-Address	Port/Trunk
A	t2



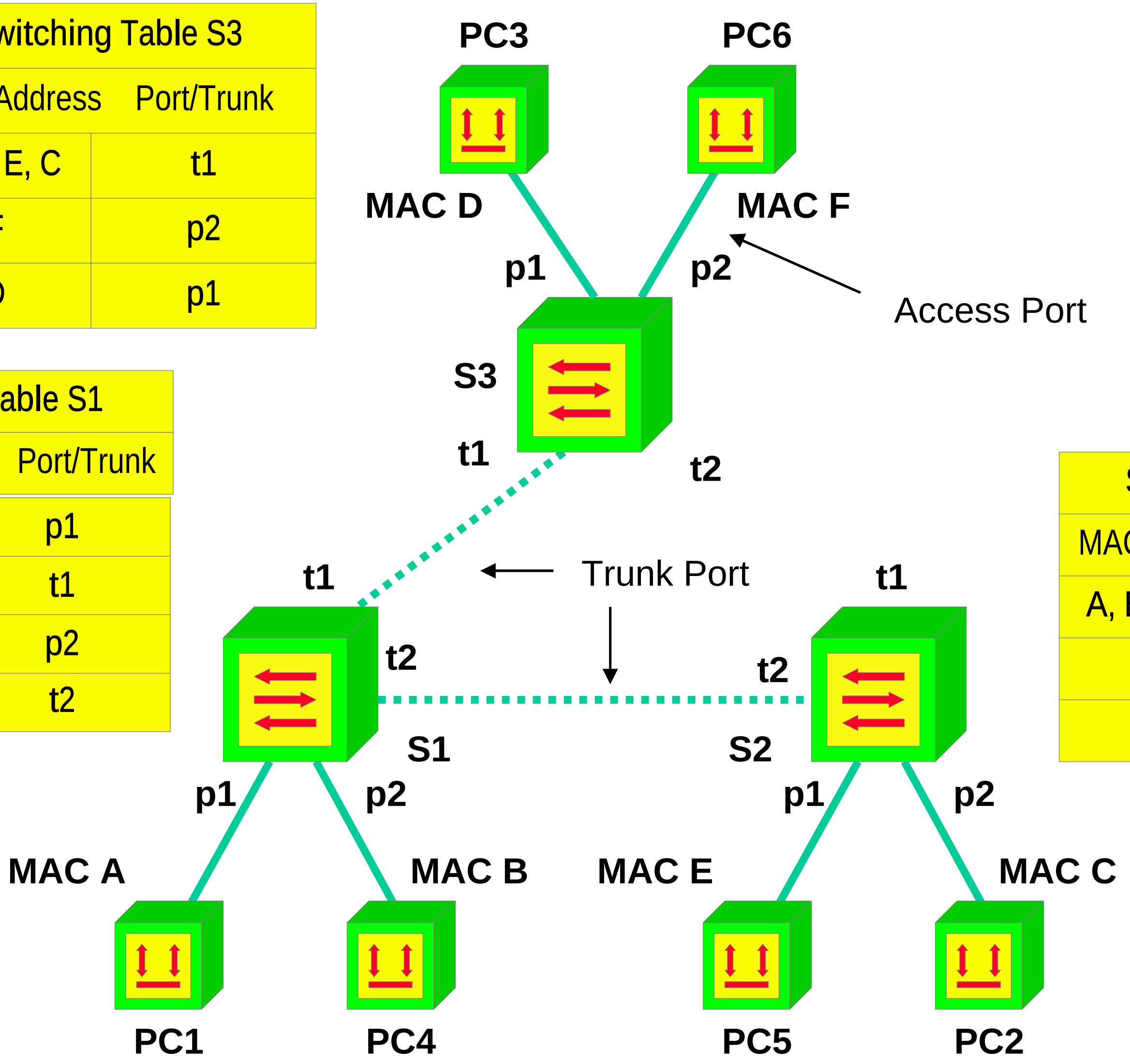
Forward A (DA)

F->A

Ethernet Switch Table – Final State
(All MAC addresses learned)

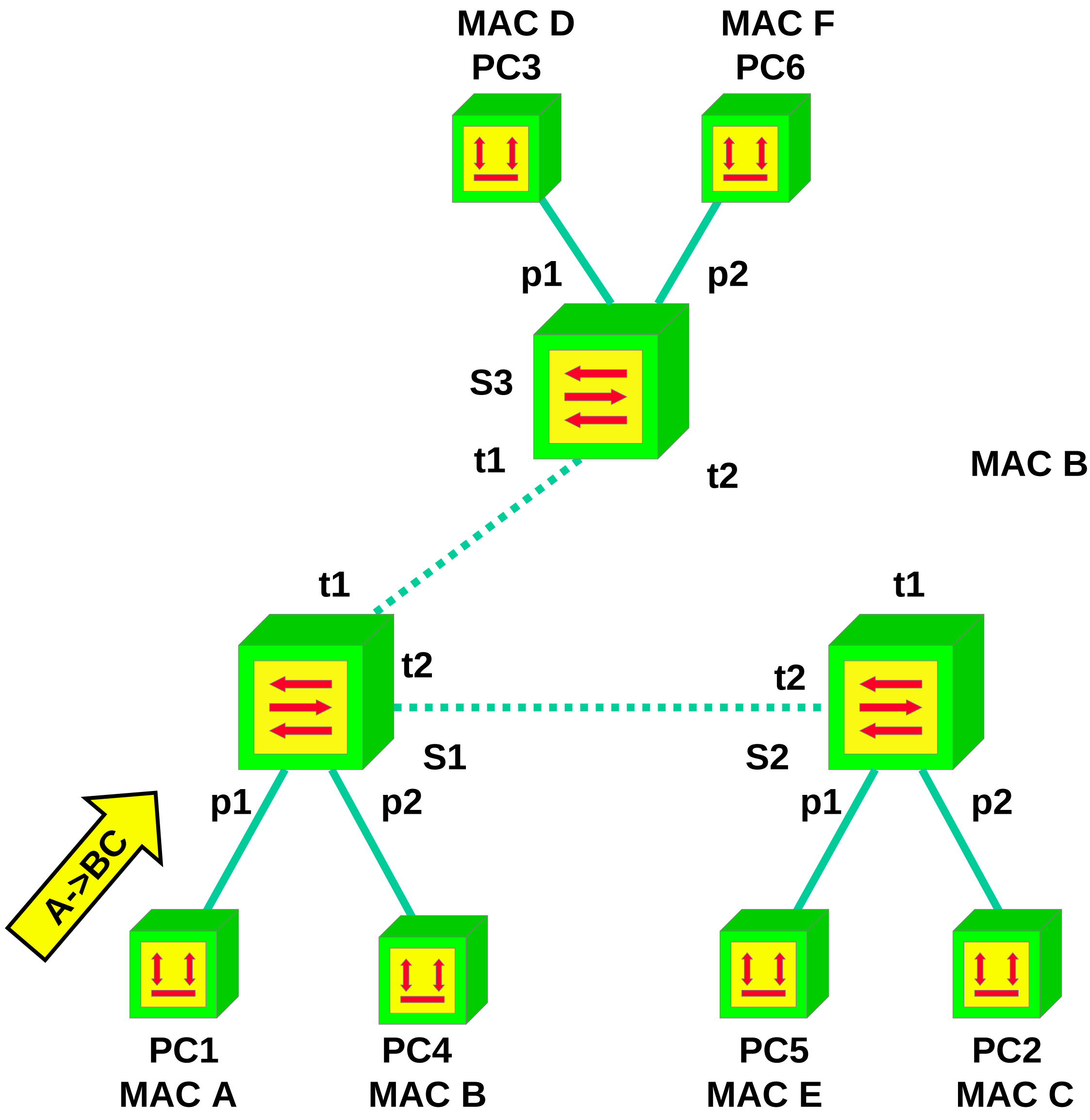
Switching Table S3	
MAC-Address	Port/Trunk
A, B, E, C	t1
F	p2
D	p1

Switching Table S1	
MAC-Address	Port/Trunk
A	p1
F, D	t1
B	p2
E, C	t2



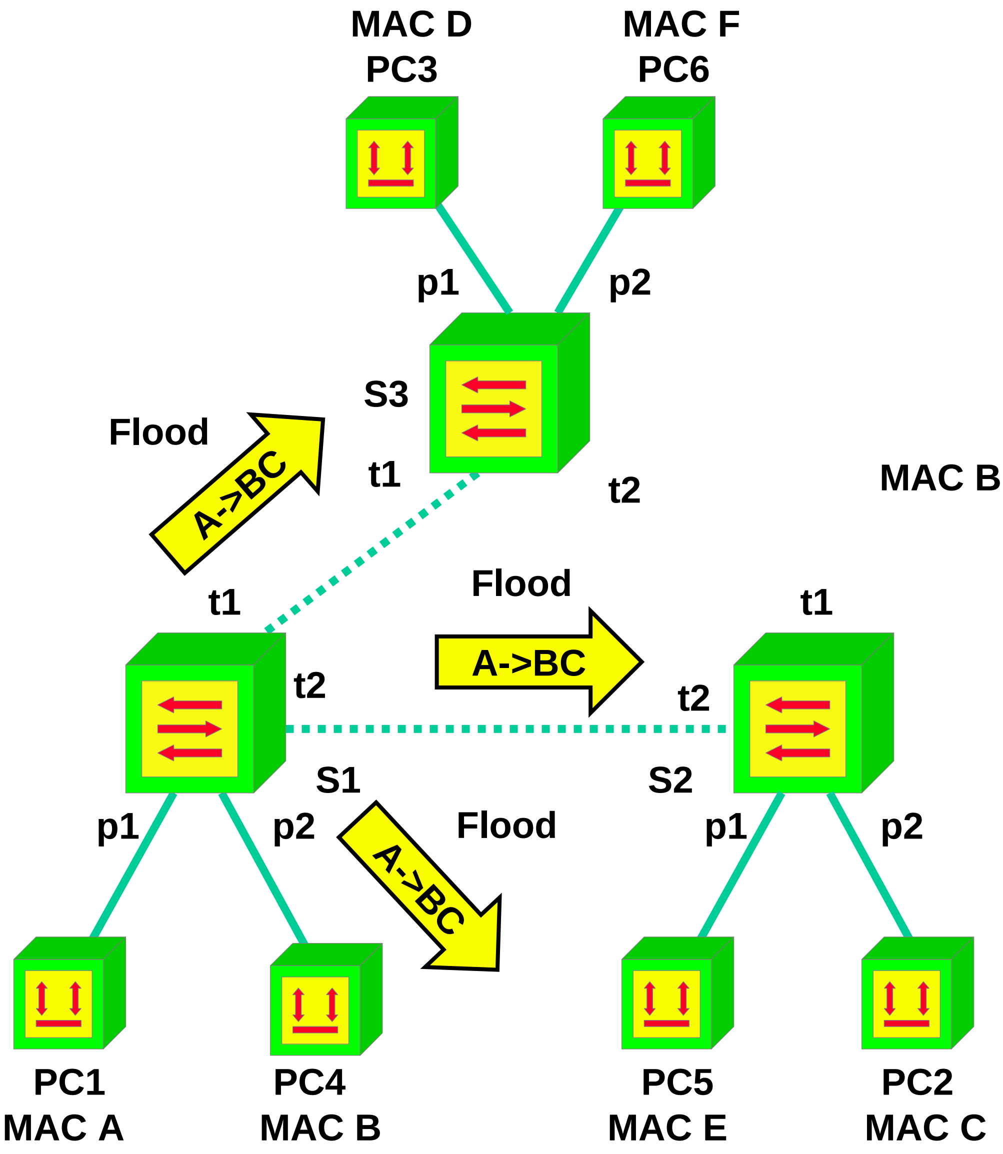
Switching Table S2	
MAC-Address	Port/Trunk
A, B, D, F	t2
E	p1
C	p2

Ethernet Broadcast (BC) 1



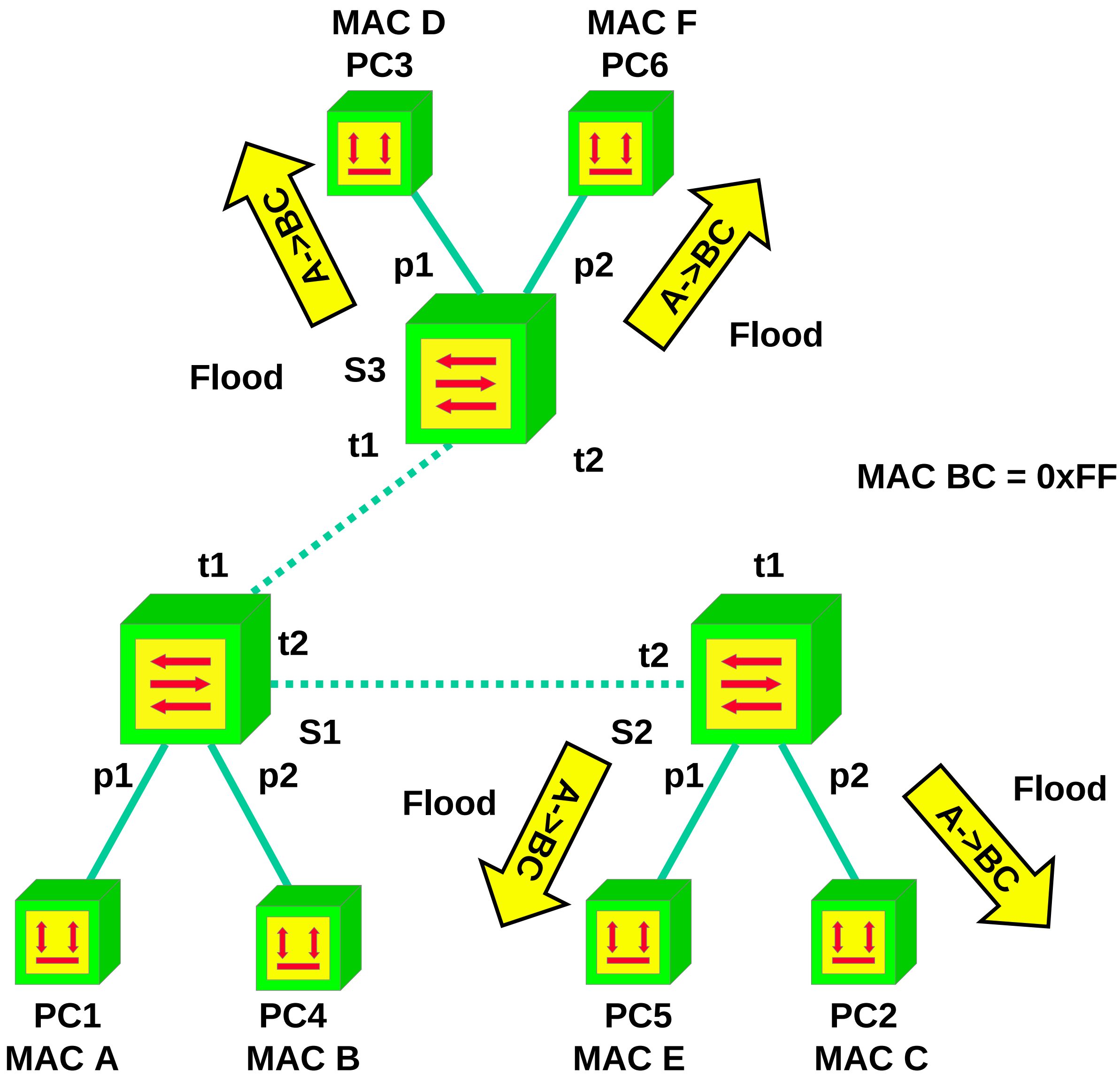
MAC BC = 0xFFFF.FFFF.FFFF

Ethernet Broadcast (BC) 2



MAC BC = 0xFFFF.FFFF.FFFF

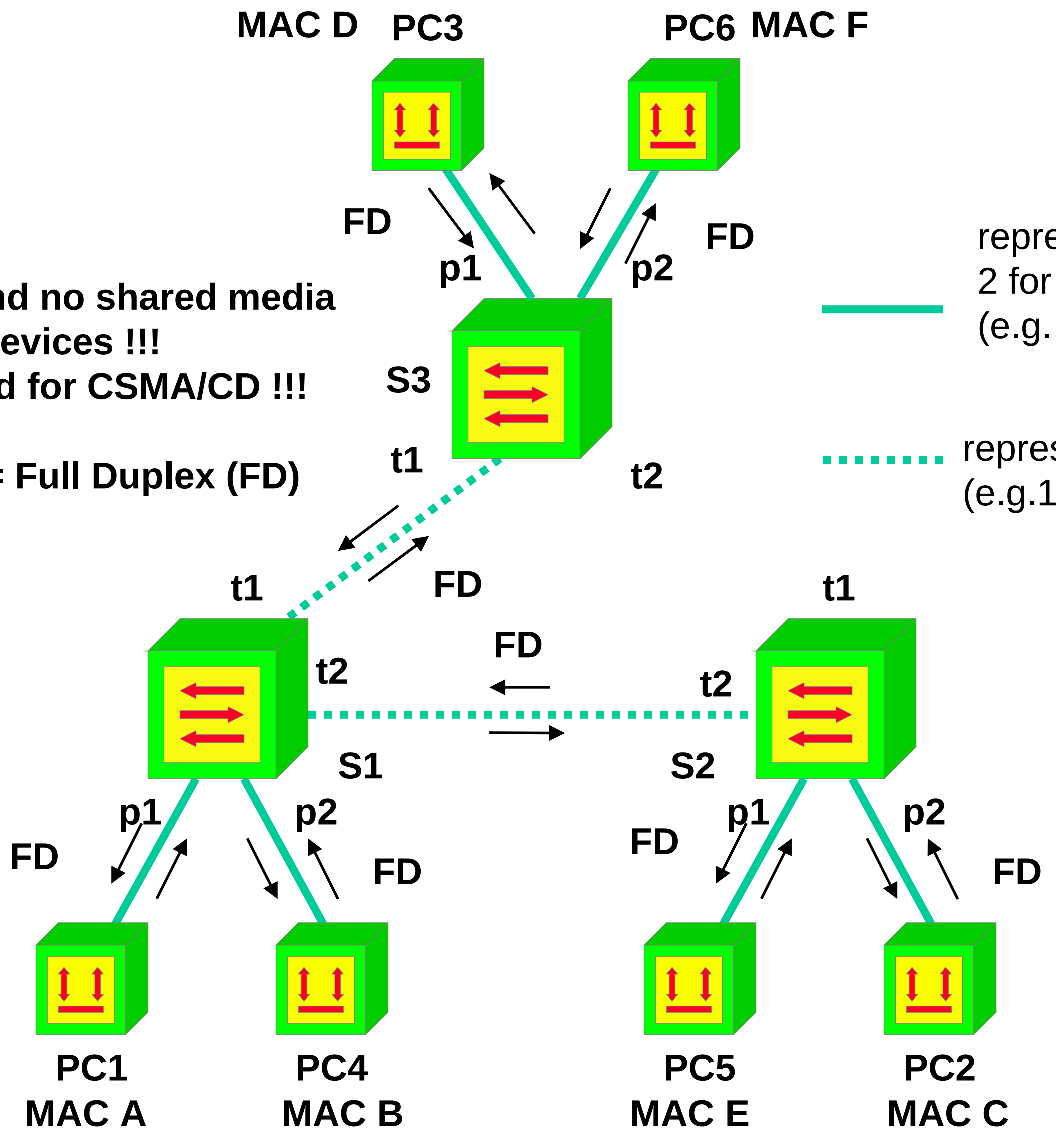
Ethernet Broadcast (BC) 3



MAC BC = 0xFFFF.FFFF.FFFF

Ethernet Switching – Full Duplex (FD)

(Point-to-Point Links and FD Everywhere)



Only PTP links and no shared media for more than 2 Devices !!!
Therefore no need for CSMA/CD !!!

CSMA/CD OFF == Full Duplex (FD)

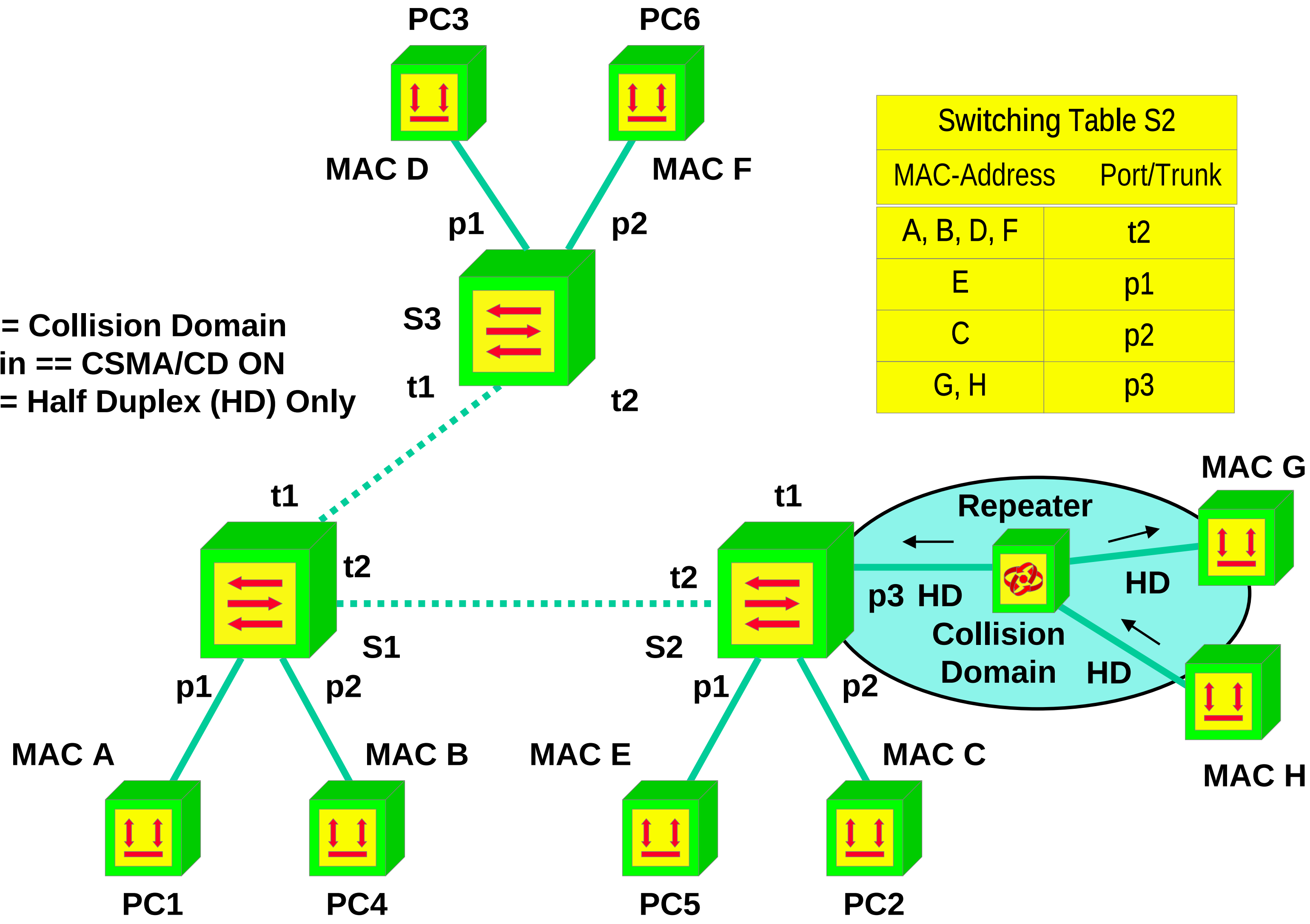
represents four CU wires
2 for Tmt, 2 for Rcv
(e.g. 100BaseT)

represents two FO wires
(e.g.100BaseF)

Ethernet Switching – Repeater (Hub)

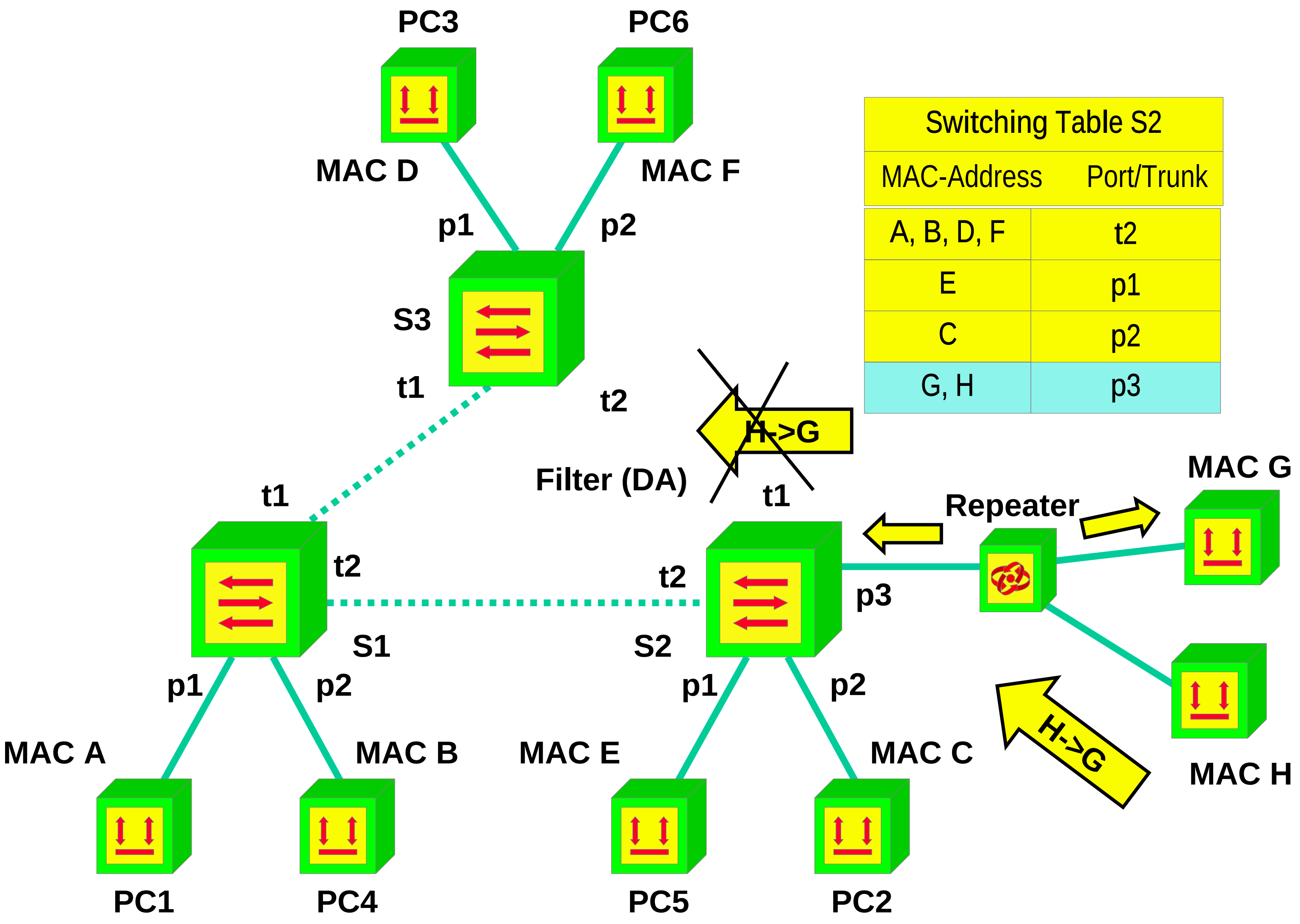
(Point-to-Point Links Everywhere but on Shared Media – Half Duplex)

Shared Media == Collision Domain
Collision Domain == CSMA/CD ON
CSMA/CD ON == Half Duplex (HD) Only



Switching Table S2	
MAC-Address	Port/Trunk
A, B, D, F	t2
E	p1
C	p2
G, H	p3

Table Usage (Filtering Decision) for Ethernet Frame MAC-H to MAC-G

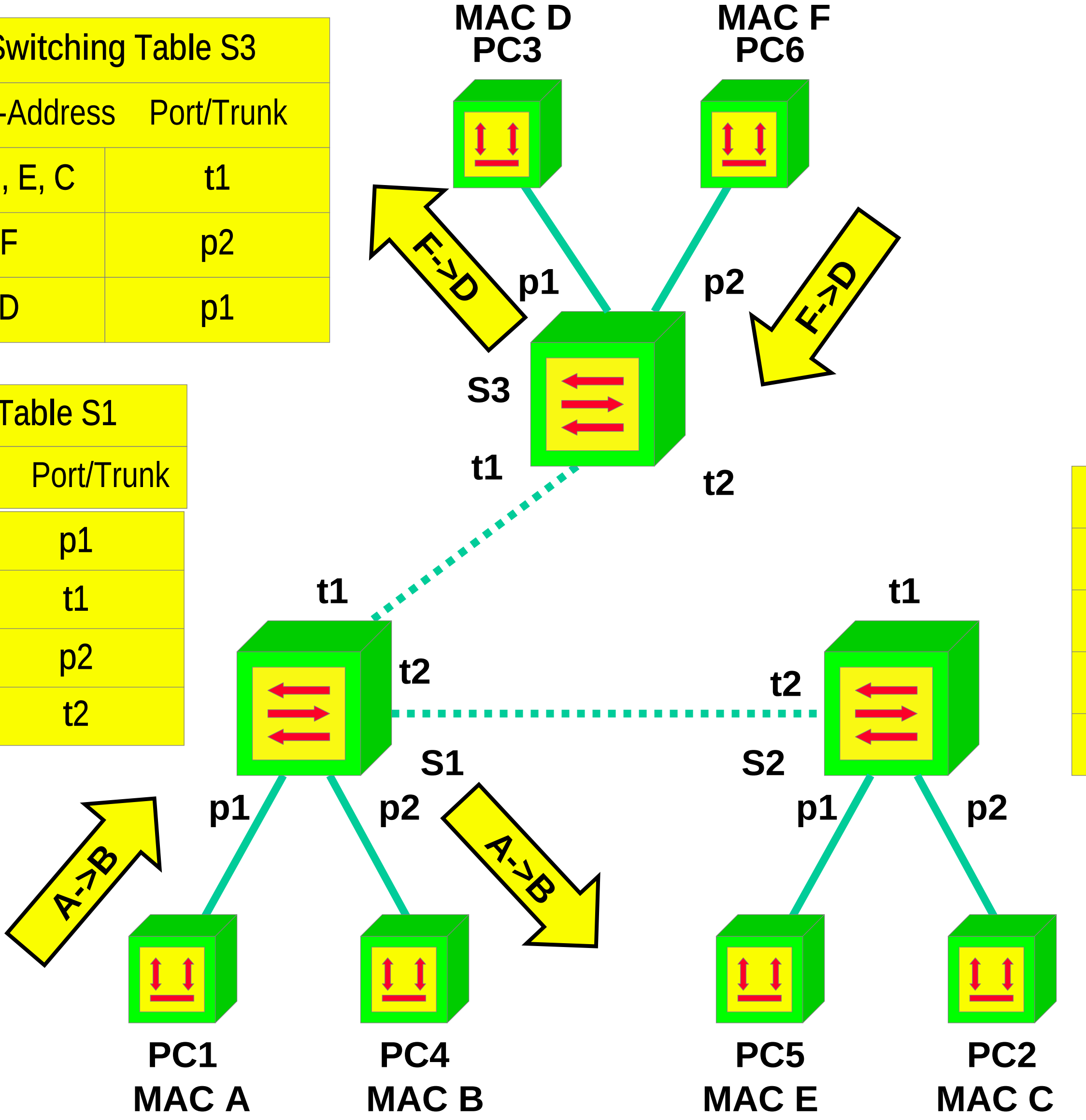


Switching Table S2	
MAC-Address	Port/Trunk
A, B, D, F	t2
E	p1
C	p2
G, H	p3

Ethernet Switch Table – Decoupling (Improving Performance <-> Collision Domains)

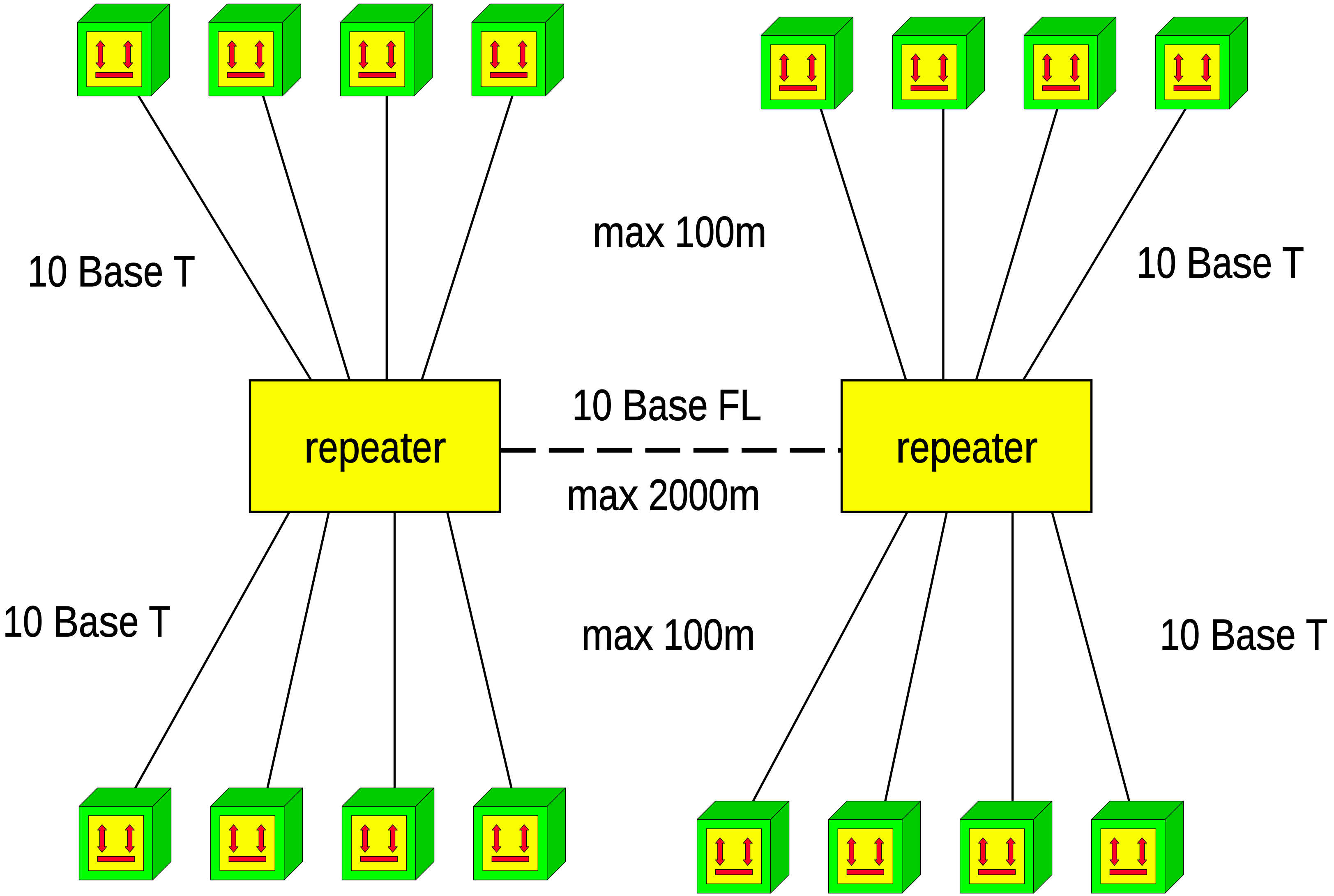
Switching Table S3	
MAC-Address	Port/Trunk
A, B, E, C	t1
F	p2
D	p1

Switching Table S1	
MAC-Address	Port/Trunk
A	p1
F, D	t1
B	p2
E, C	t2



Switching Table S2	
MAC-Address	Port/Trunk
A, B, D, F	t2
E	p1
C	p2

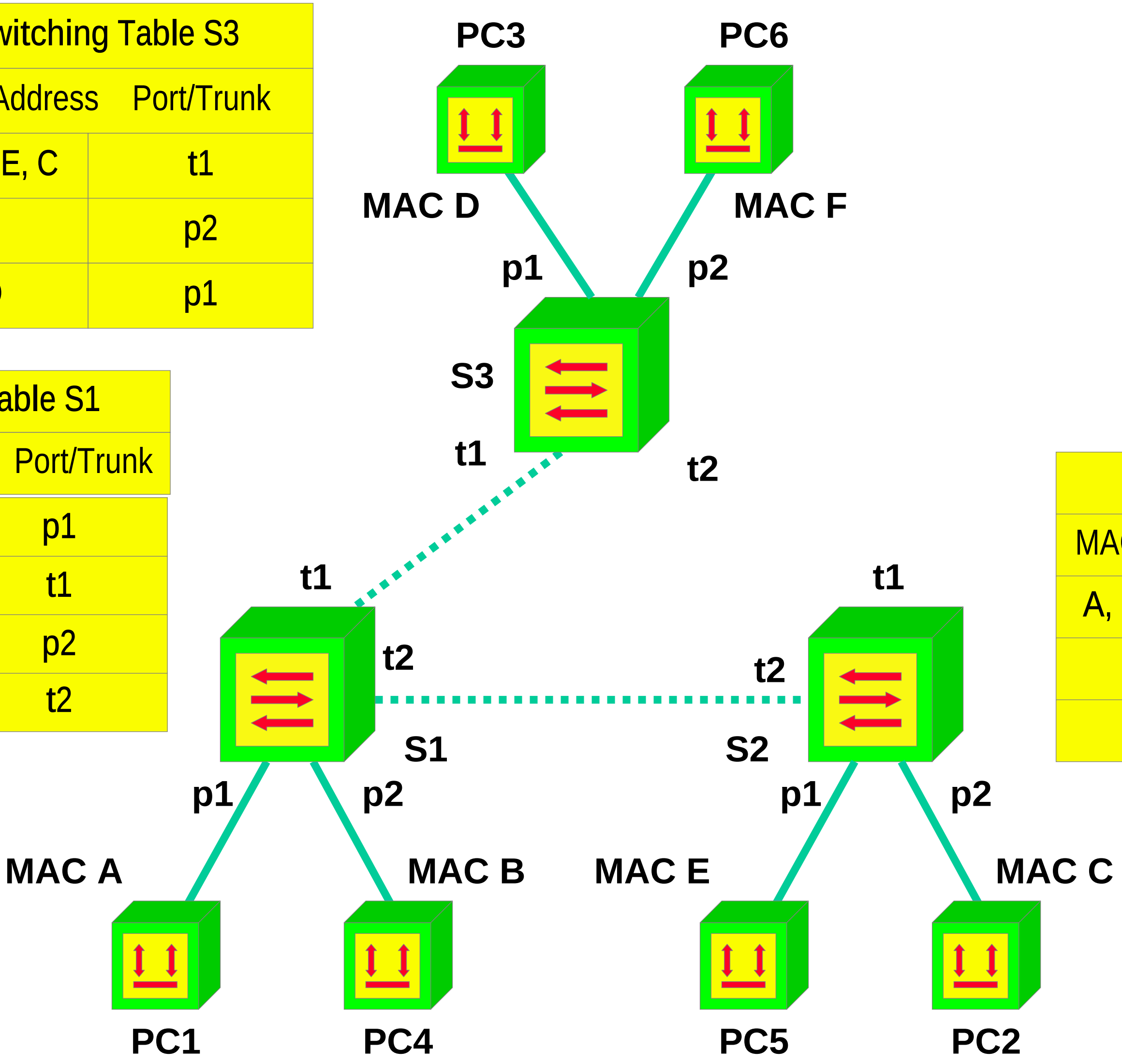
Ethernet with Repeater: Network Sniffing? Yes -> Ethernet Card -> Promiscuous Mode



Ethernet with Switches: Network Sniffing? Not so easy -> Because of Inherent Filtering

Switching Table S3	
MAC-Address	Port/Trunk
A, B, E, C	t1
F	p2
D	p1

Switching Table S1	
MAC-Address	Port/Trunk
A	p1
F, D	t1
B	p2
E, C	t2

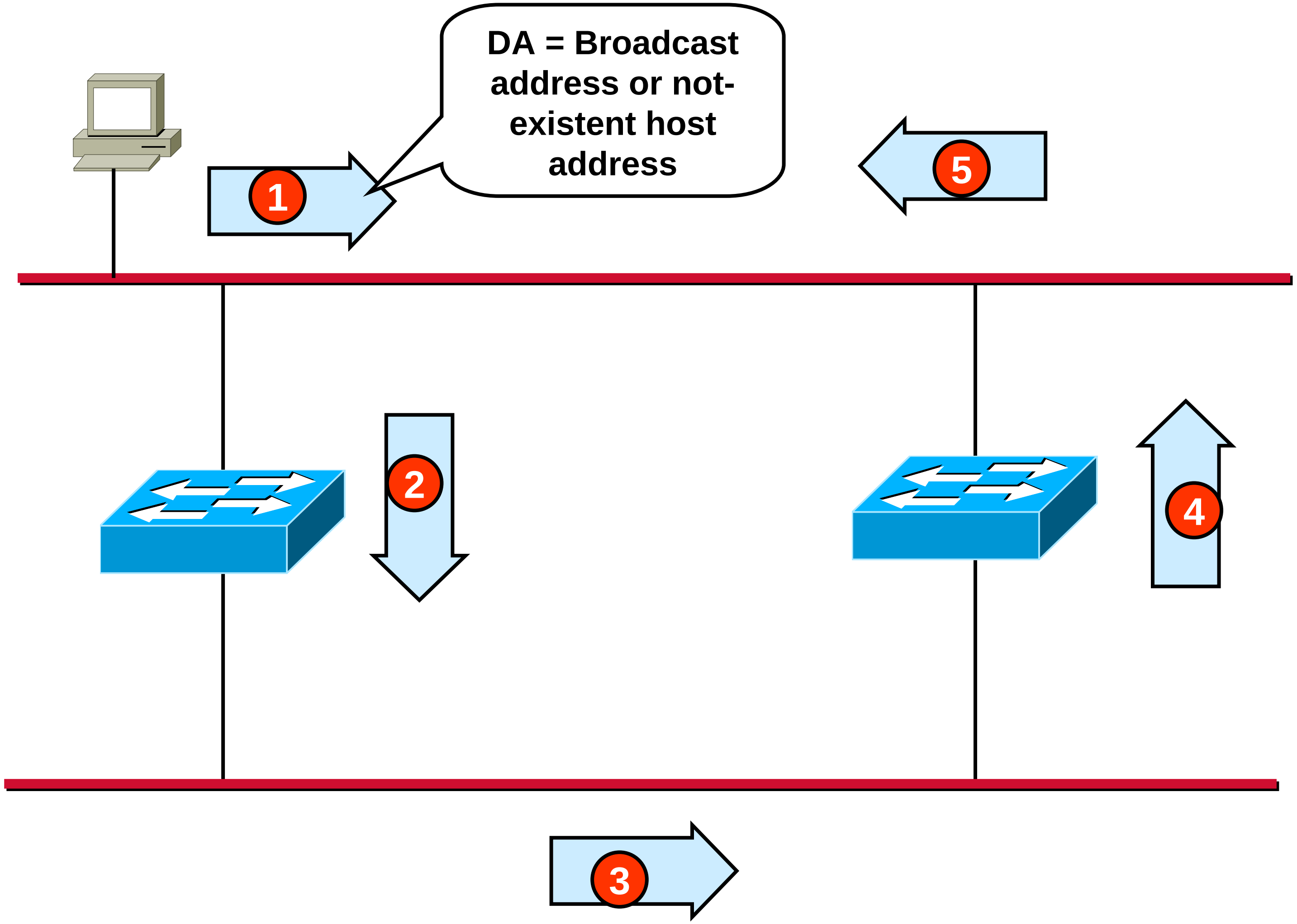


Switching Table S2	
MAC-Address	Port/Trunk
A, B, D, F	t2
E	p1
C	p2

Bridging Problems

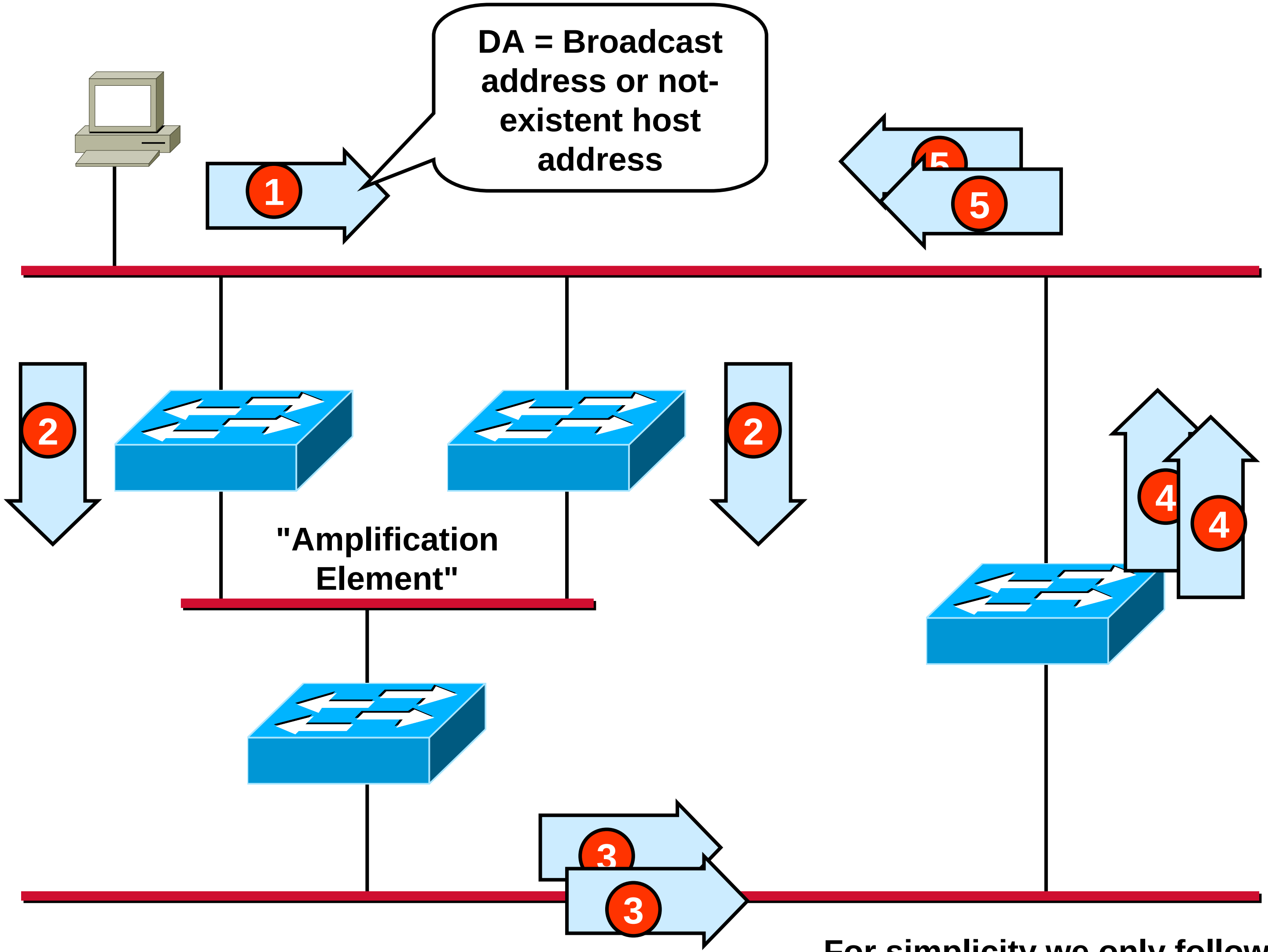
- Redundant paths lead to
  - Broadcast storms
  - Endless cycling
  - Continuous table rewriting
- No load sharing possible
- No ability to select best path
- Frame may be stored for 4 seconds (!)
  - Although rare cases
  - But only little acceptance for realtime and isochronous traffic – might change!

Endless Circling


DA = Broadcast address or not-existent host address

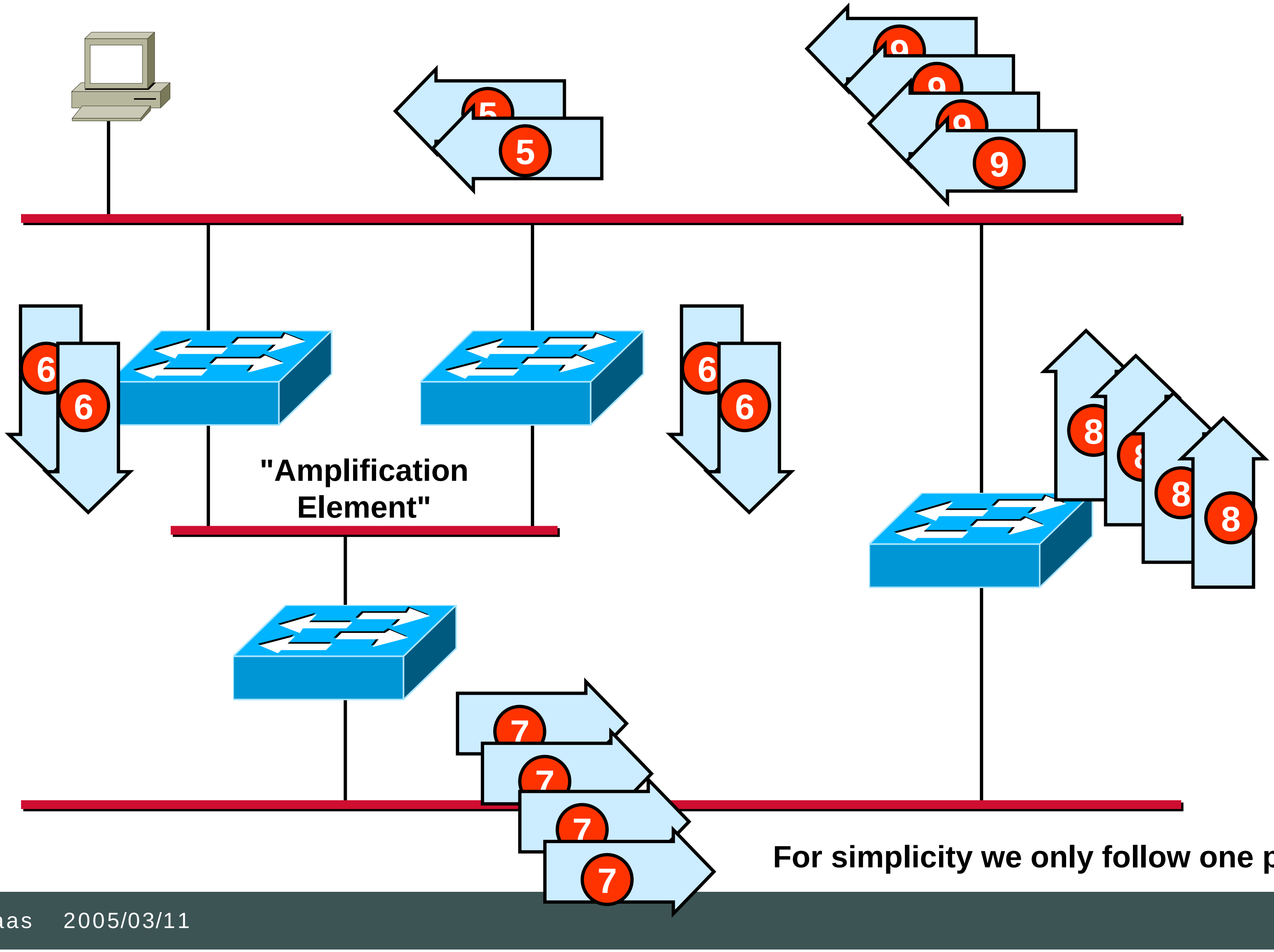
For simplicity we only follow one path

Broadcast Storm (1)



For simplicity we only follow one path

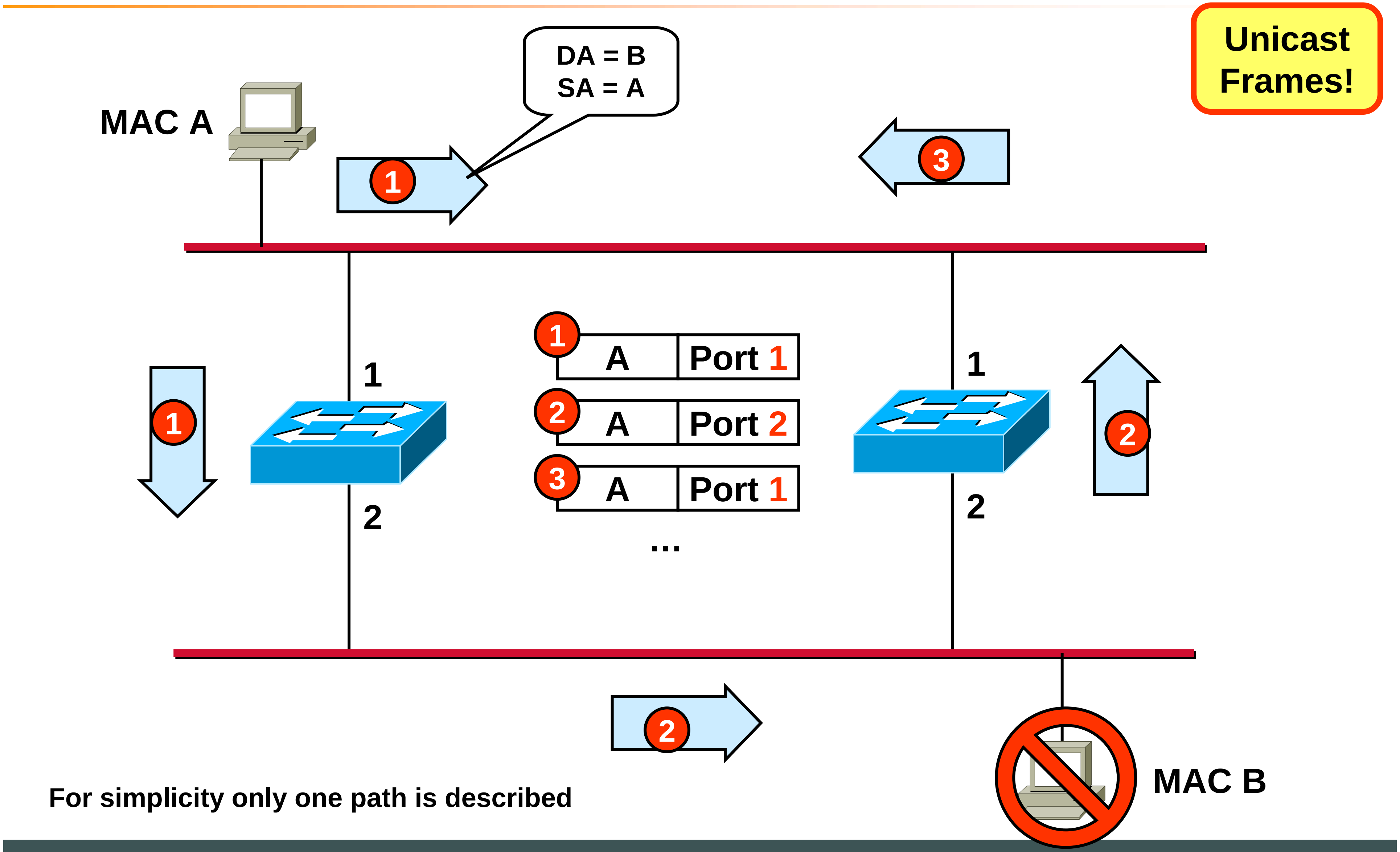
Broadcast Storm (2)



"Amplification Element"

For simplicity we only follow one path

Mutual Table Rewriting



Unicast Frames!

1	A	Port 1
2	A	Port 2
3	A	Port 1
	…	

For simplicity only one path is described

Spanning Tree

- Invented by *Radia Perlman* as general "mesh-to-tree" algorithm
- A must in bridged networks with redundant paths
- Only one purpose:
  cut off redundant paths with highest costs

Algorhyme

I think that I shall never see
a graph more lovely than a tree
a graph whose crucial property
is loop-free connectivity.
A tree which must be sure to span
so packets can reach every lan.
first the root must be selected
by ID it is elected.
least cost paths to root are traced,
and in the tree these paths are place.
mesh is made by folks like me;
bridges find a spanning tree.

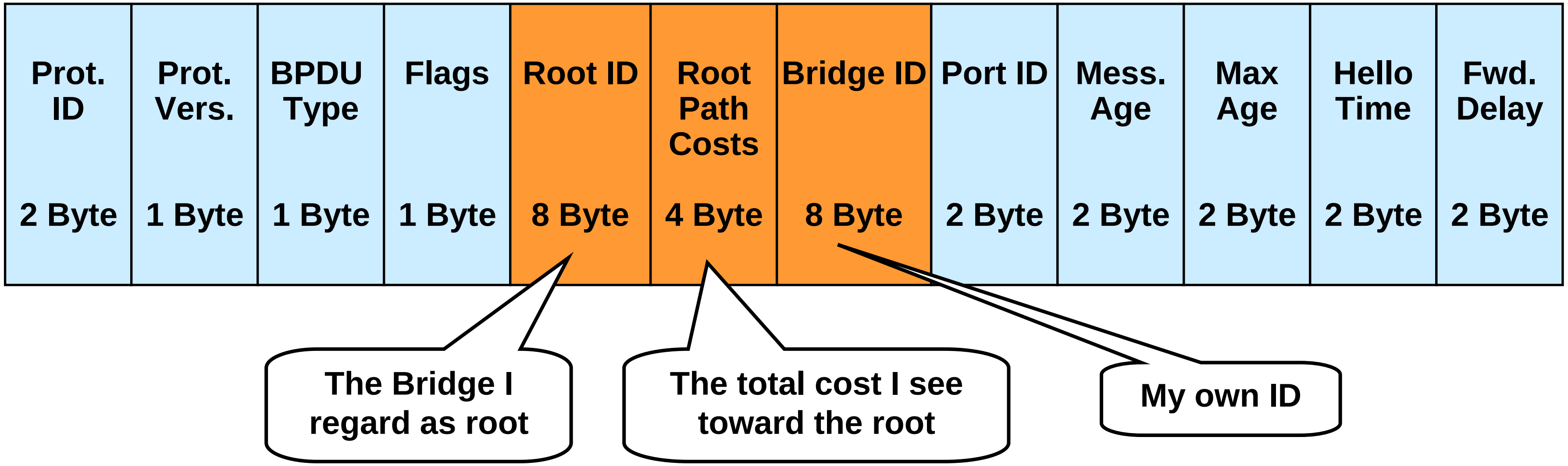
Radia Perlman

STP Ingredients

- Special STP frames: "Bridge Protocol Data Units" (**BPDU**s)
- A **Bridge-ID** for each bridge
  - Priority value (16 bit, default 32768)
  - (Lowest) MAC address
- A **Port Cost** for each port
  - Default 1000/Mbits (can be changed)
  - E.g. 10 Mbit/s → C=100

BPDU Format

- Each bridge sends periodically BPDUs carried in Ethernet multicast frames
  - Hello time default: 2 seconds
- Contains all information necessary for building Spanning Tree



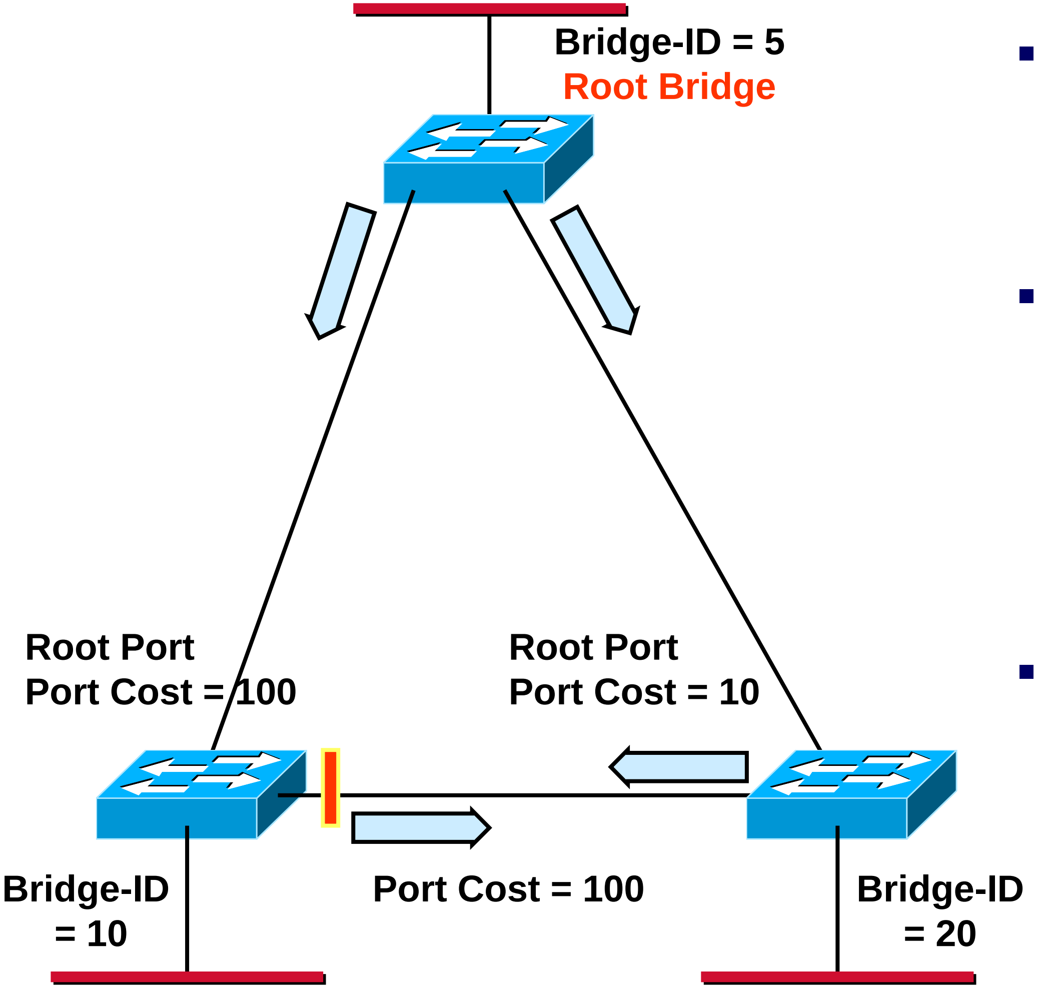
Prot. ID	Prot. Vers.	BPDU Type	Flags	Root ID	Root Path Costs	Bridge ID	Port ID	Mess. Age	Max Age	Hello Time	Fwd. Delay
2 Byte	1 Byte	1 Byte	1 Byte	8 Byte	4 Byte	8 Byte	2 Byte	2 Byte	2 Byte	2 Byte	2 Byte

The Bridge I regard as root

The total cost I see toward the root

My own ID

STP Principle

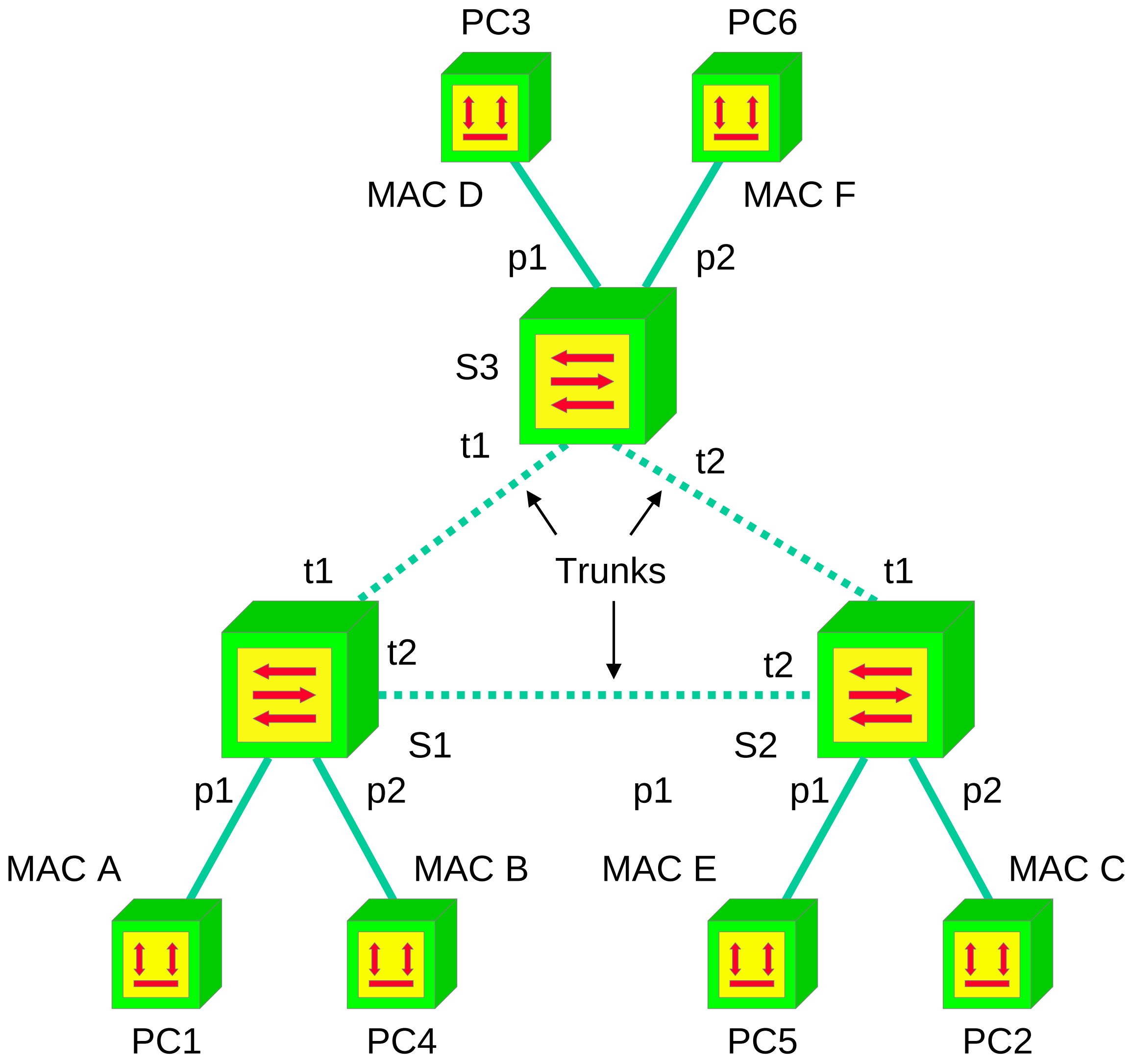


- First a Root Bridge is determined
  - Initially every bridge assumes itself as root
  - The bridge with lowest Bridge-ID wins
- Then the root bridge triggers BDPU sending (hello time intervals)
  - Received at "Root Ports" by other bridges
  - Every bridge adds its own port cost to the advertised cost and forwards the BPDU
- On each LAN segment one bridge becomes Designated Bridge
  - Having lowest total root path cost
  - Other bridges set redundant ports in blocking state

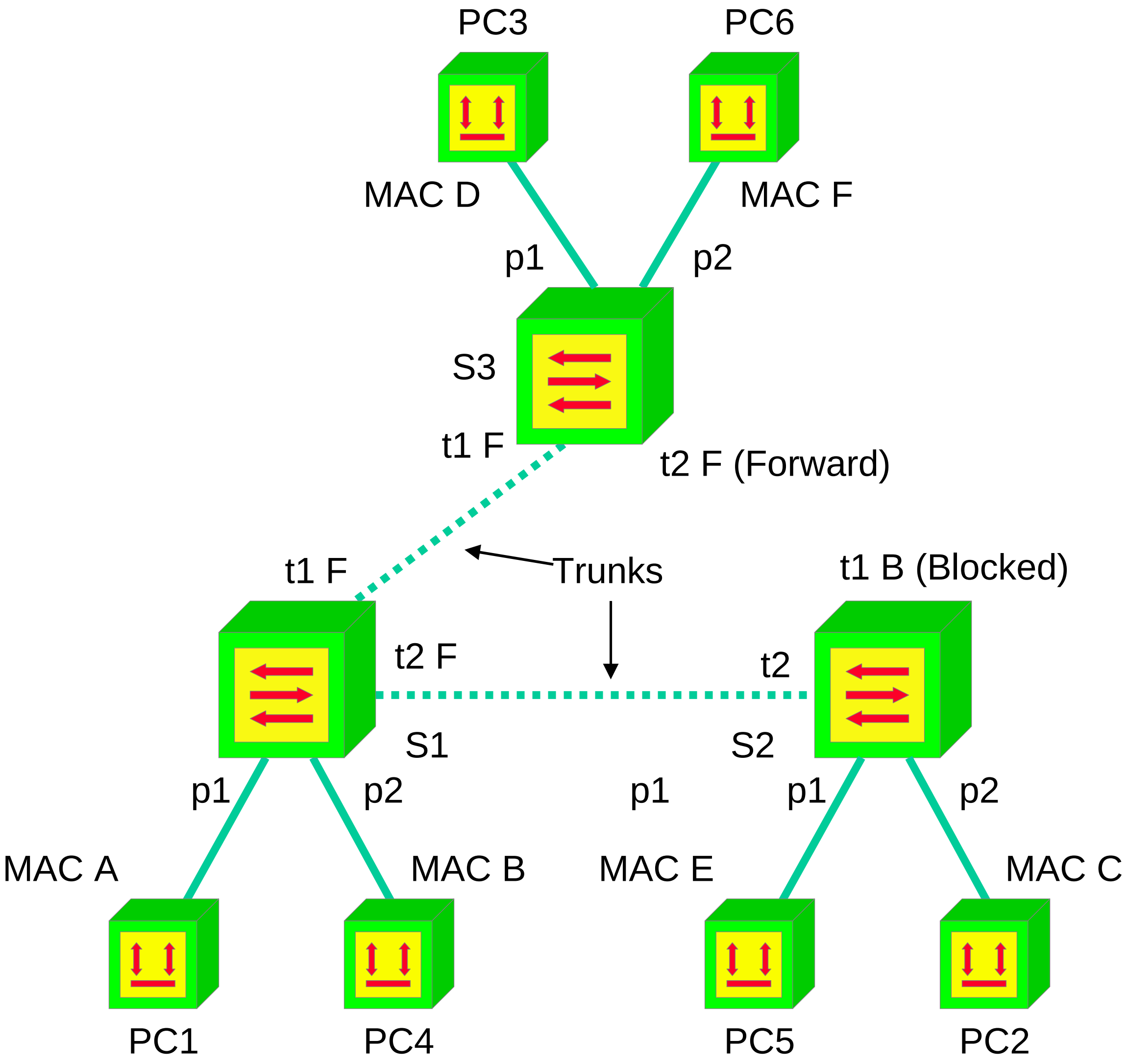
Note

- Redundant links remain in active stand-by mode
  - If root port fails, other root port becomes active
- Low-price switches might not support STP
  - Don't use them in meshed configurations
- Only 7 bridges per path allowed according standard (!)

Redundant Topology L2 Switching

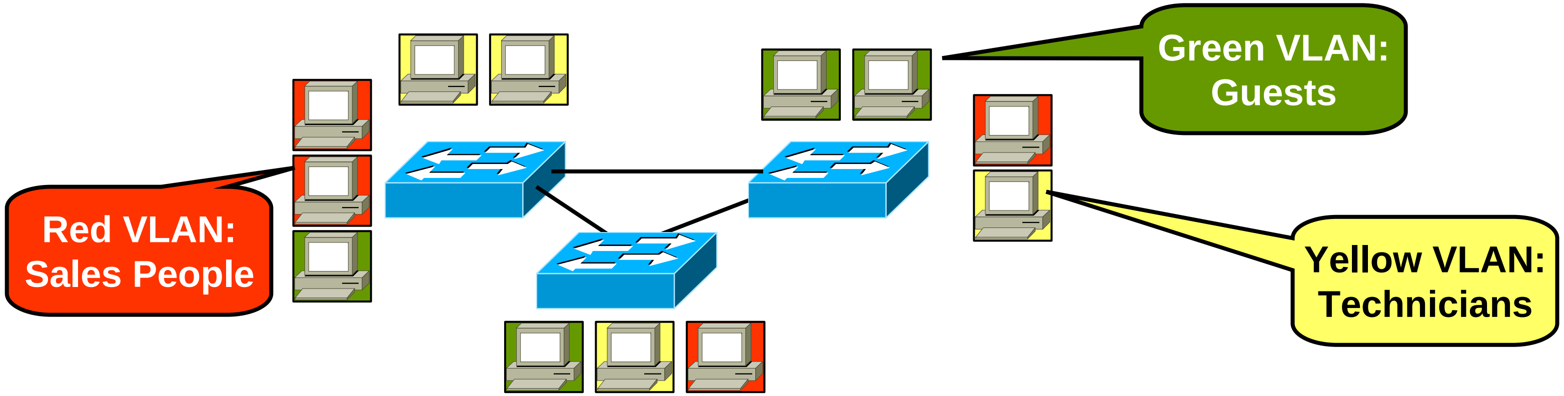


Spanning Tree Applied



Virtual LANs

- Separate LAN into multiple broadcast domains
  - No global broadcasts anymore
  - For security reasons
- Assign users to "VLANs"



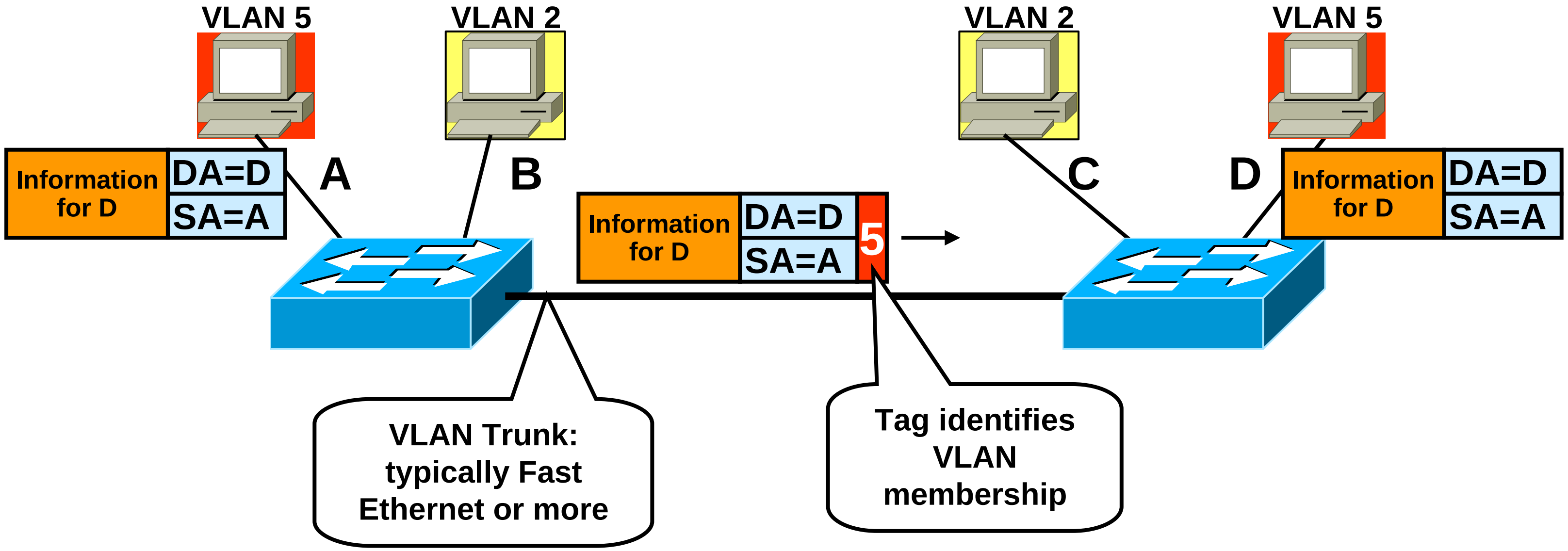
Virtual LANs

- **Base idea of VLAN:**
  - **multiplexing of several LANs via same infrastructure (switches and connection between switches)**
- **Today's switches got the ability to combine several network-stations to so-called "Virtual LANs“**
  - **separate bridging/switching table maintained for every single VLAN**
  - **separate broadcast handling for every single VLAN**
    - **each Virtual LAN is its own broadcast domain**
  - **separate Spanning Tree for every single VLAN in case of Cisco equipment (PVST+)**
    - **note: IEEE 802.1w specifies a method to share one Rapid Spanning Tree among all VLANs**

Host to VLAN Assignment

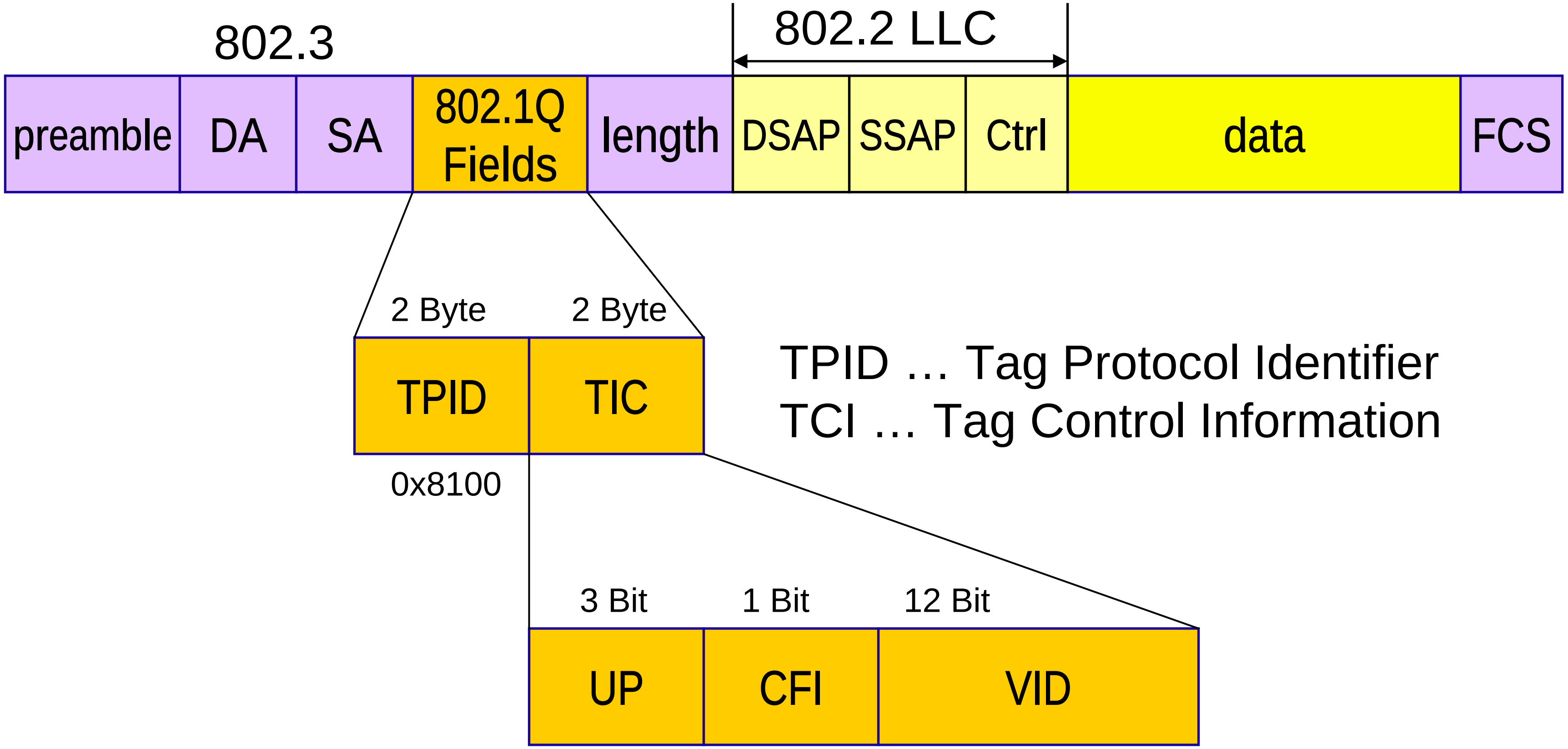
- Different solutions
  - Port based assignment
  - Source address assignment
  - Protocol based
  - Complex rule based
- Bridges are interconnected via VLAN trunks
  - IEEE 802.1q (New: 802.1w, 802.1s)
  - ISL (Cisco)

VLAN Trunking Example



- Inter-VLAN communication not possible
- Packets across the VLAN trunk are tagged
  - Either using 802.1q or ISL tag
  - So next bridge is able to constrain frame to same VLAN as the source

802.1Q VLAN Tagging 1

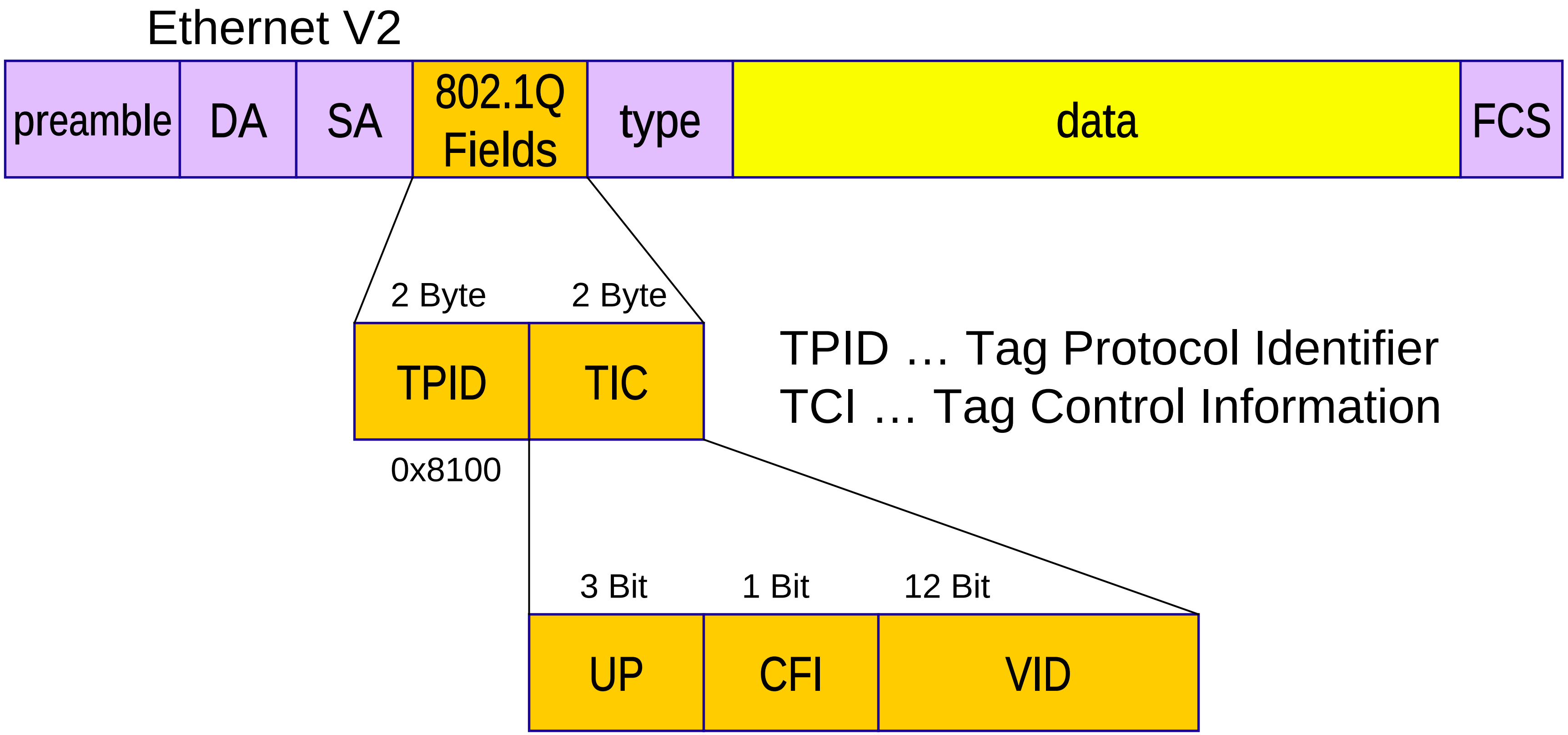


TPID … Tag Protocol Identifier
TCI … Tag Control Information

UP … User Priority
CFI … Canonical Format Identifier
VID … VLAN Identifier

note: With tagging Ethernets maximal frame length = 1522, minimal frame length = 68

802.1Q VLAN Tagging 2



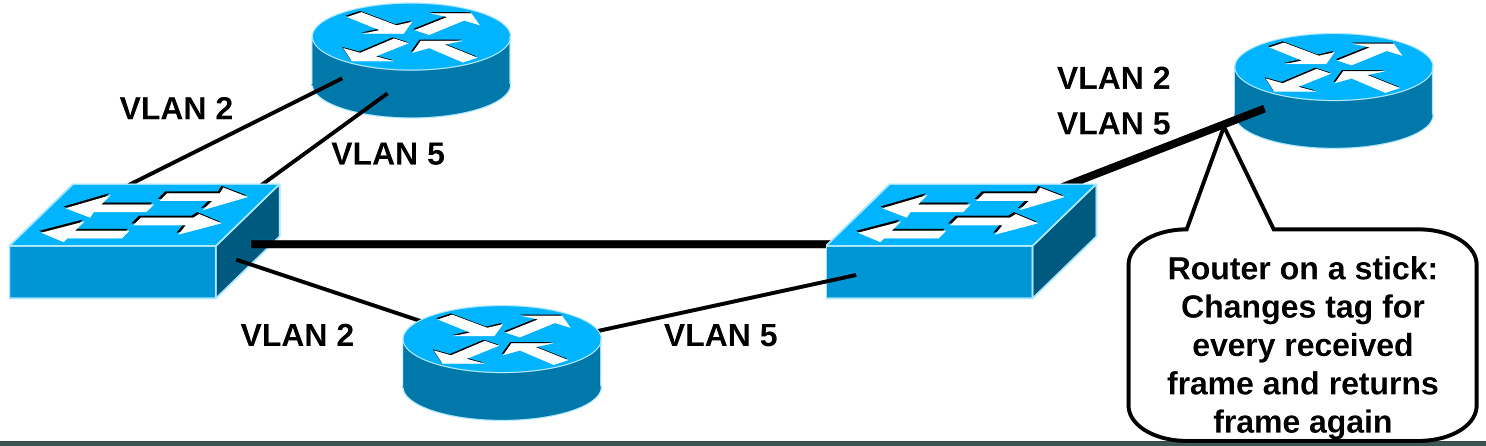
TPID … Tag Protocol Identifier
TCI … Tag Control Information

UP … User Priority
CFI … Canonical Format Identifier
VID … VLAN Identifier

note: With tagging Ethernets maximal frame length = 1522, minimal frame length = 68

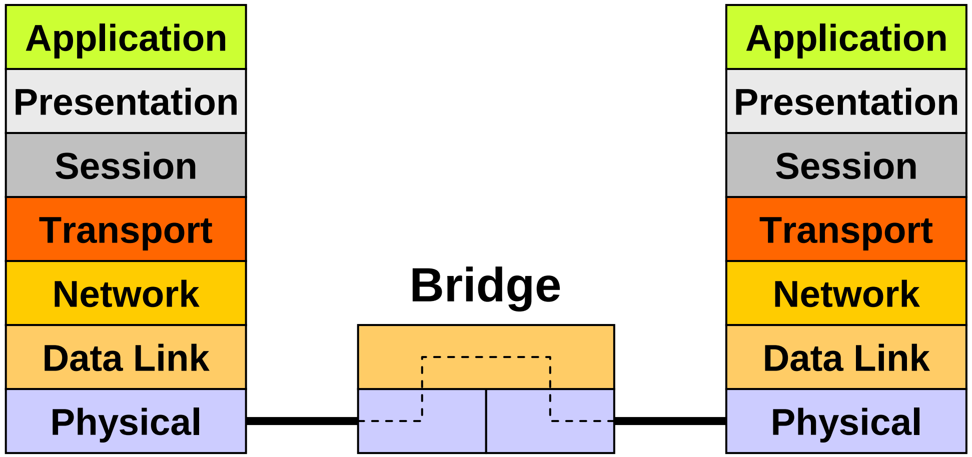
Inter-VLAN Traffic

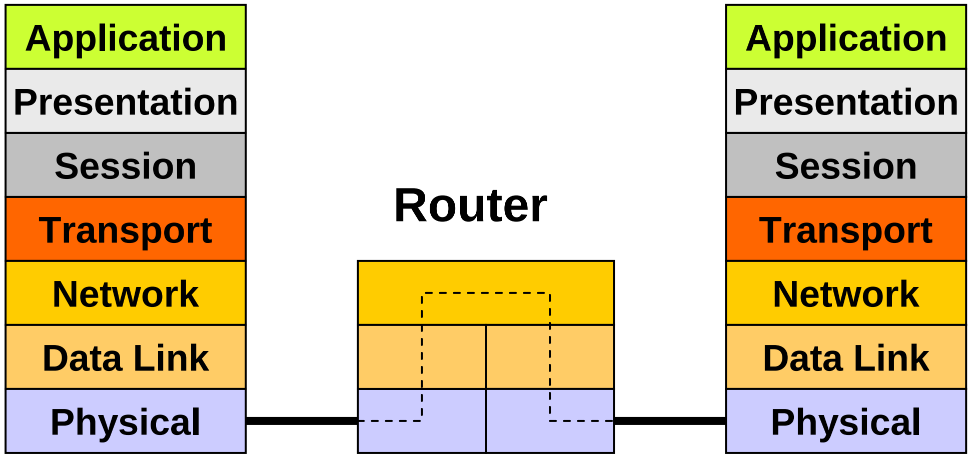
- Router can forward inter-VLAN traffic
  - Terminates Ethernet links
  - Requirement: Each VLAN in other IP subnet !
- Two possibilities
  - Router is member of every VLAN with one link each
  - Router attached on VLAN trunk port ("Router on a stick")



Router on a stick: Changes tag for every received frame and returns frame again

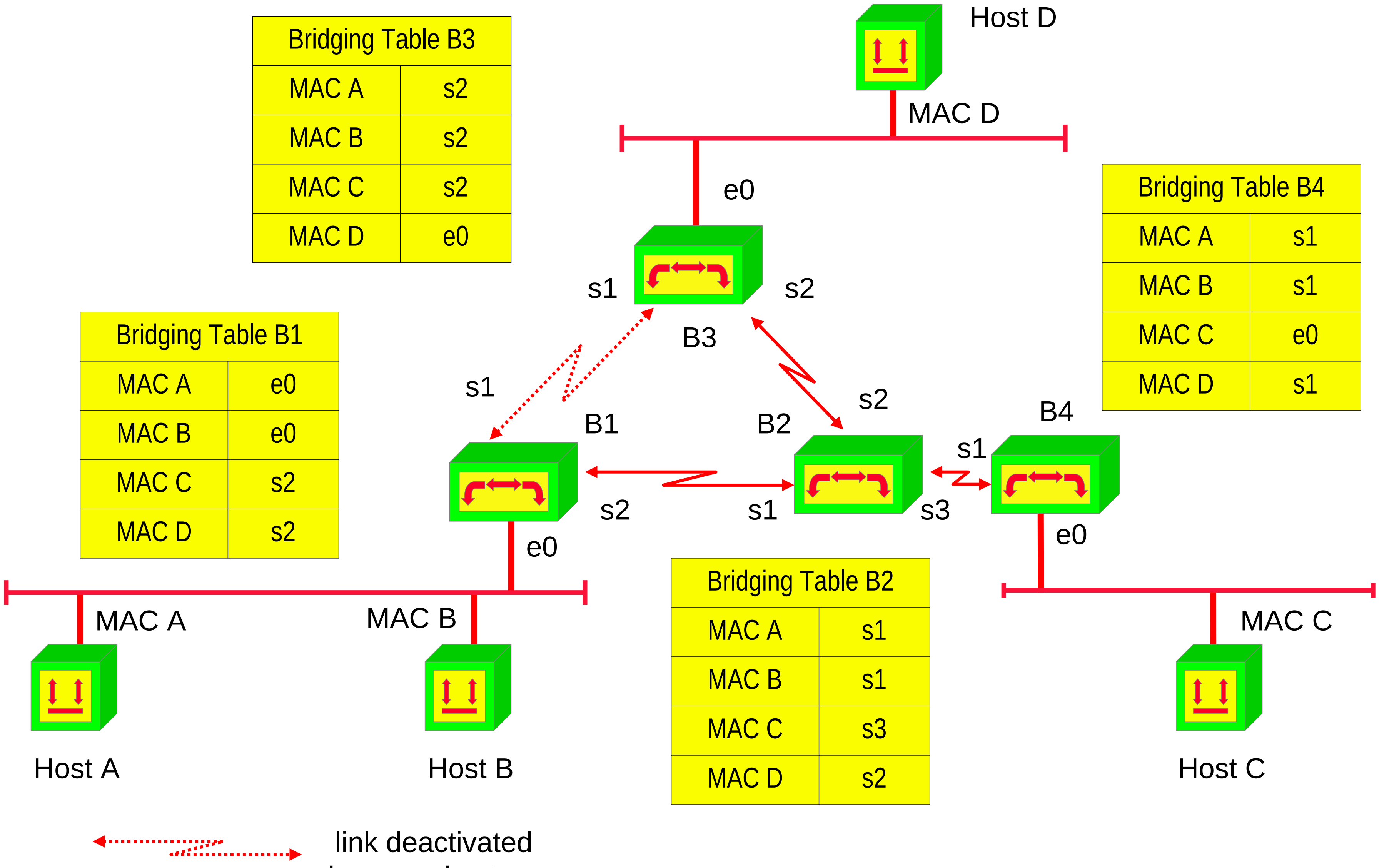
OSI Comparison





- **MAC addresses not routable**
  - NetBIOS over NetBEUI not routable (no L3)
- **Bridge supports different physical media on each port**
  - E.g. 10Mbit/s to 100Mbit/s
- **Router supports different layer-2 technologies**
  - E.g. Ethernet to Frame Relay

Example Topology: Bridging



Bridging Table B3	
MAC A	s2
MAC B	s2
MAC C	s2
MAC D	e0

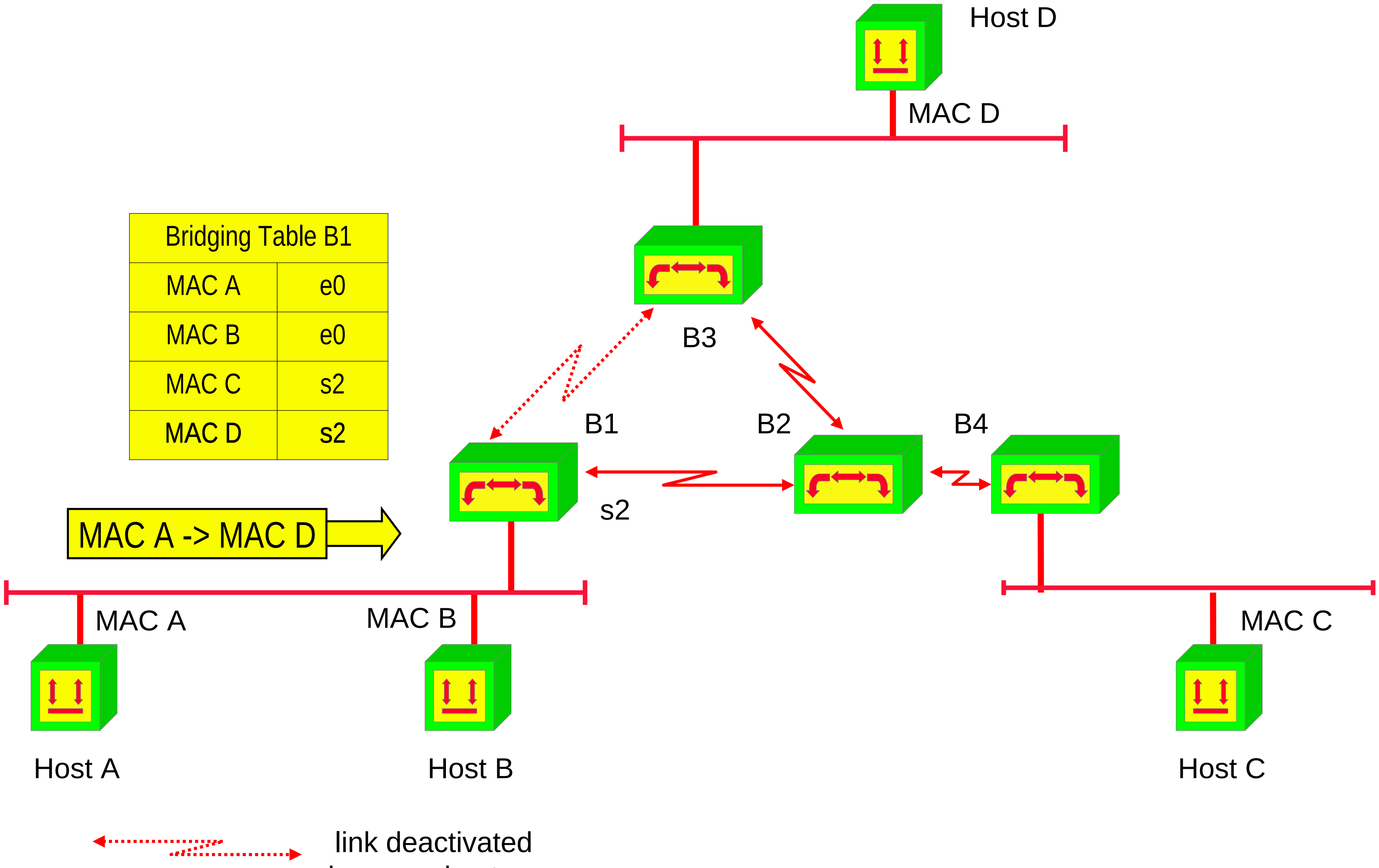
Bridging Table B1	
MAC A	e0
MAC B	e0
MAC C	s2
MAC D	s2

Bridging Table B2	
MAC A	s1
MAC B	s1
MAC C	s3
MAC D	s2

Bridging Table B4	
MAC A	s1
MAC B	s1
MAC C	e0
MAC D	s1

link deactivated
by spanning tree

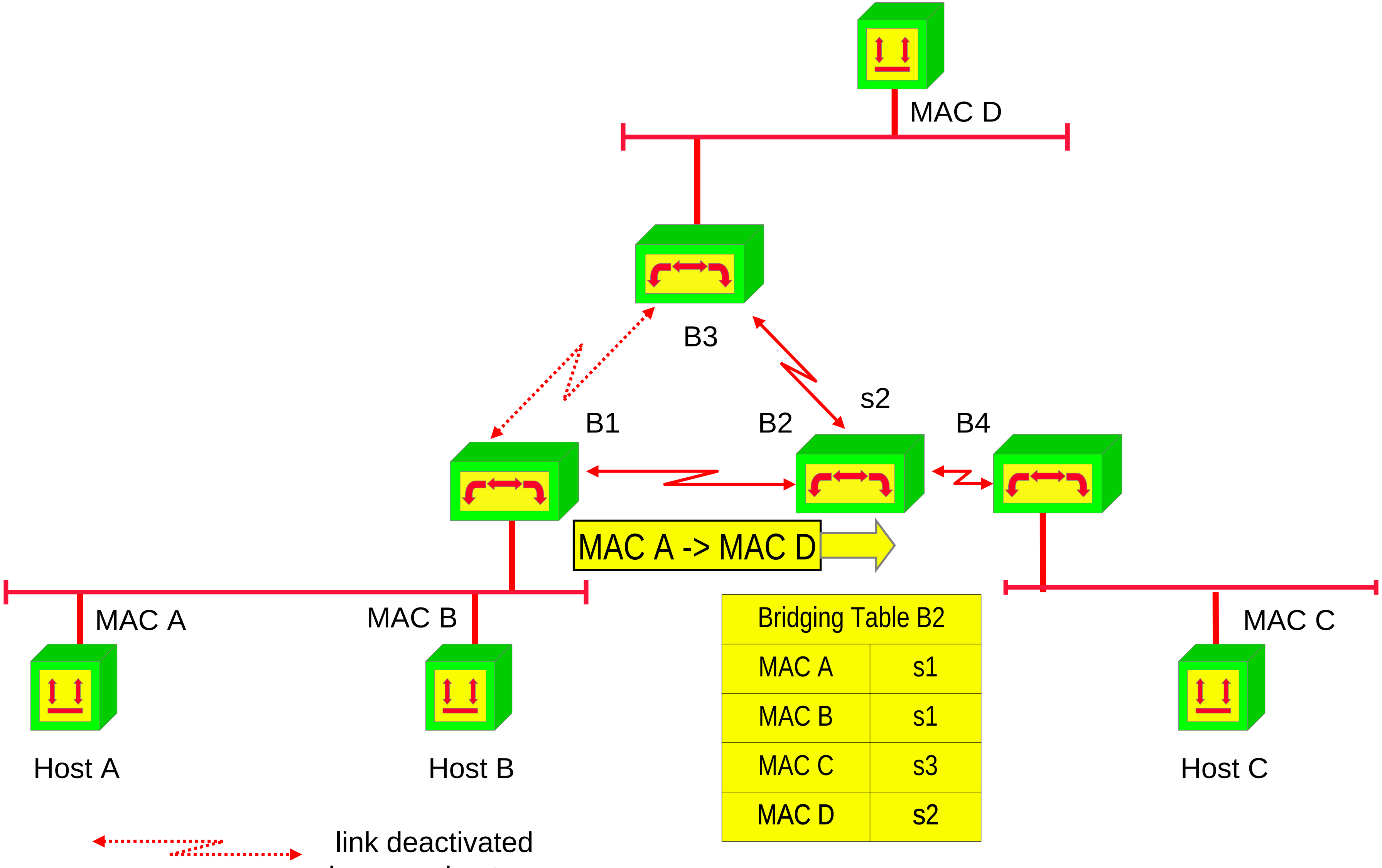
Frame MAC A to MAC D (1)



Bridging Table B1	
MAC A	e0
MAC B	e0
MAC C	s2
MAC D	s2

link deactivated
by spanning tree

Frame MAC A to MAC D (2)

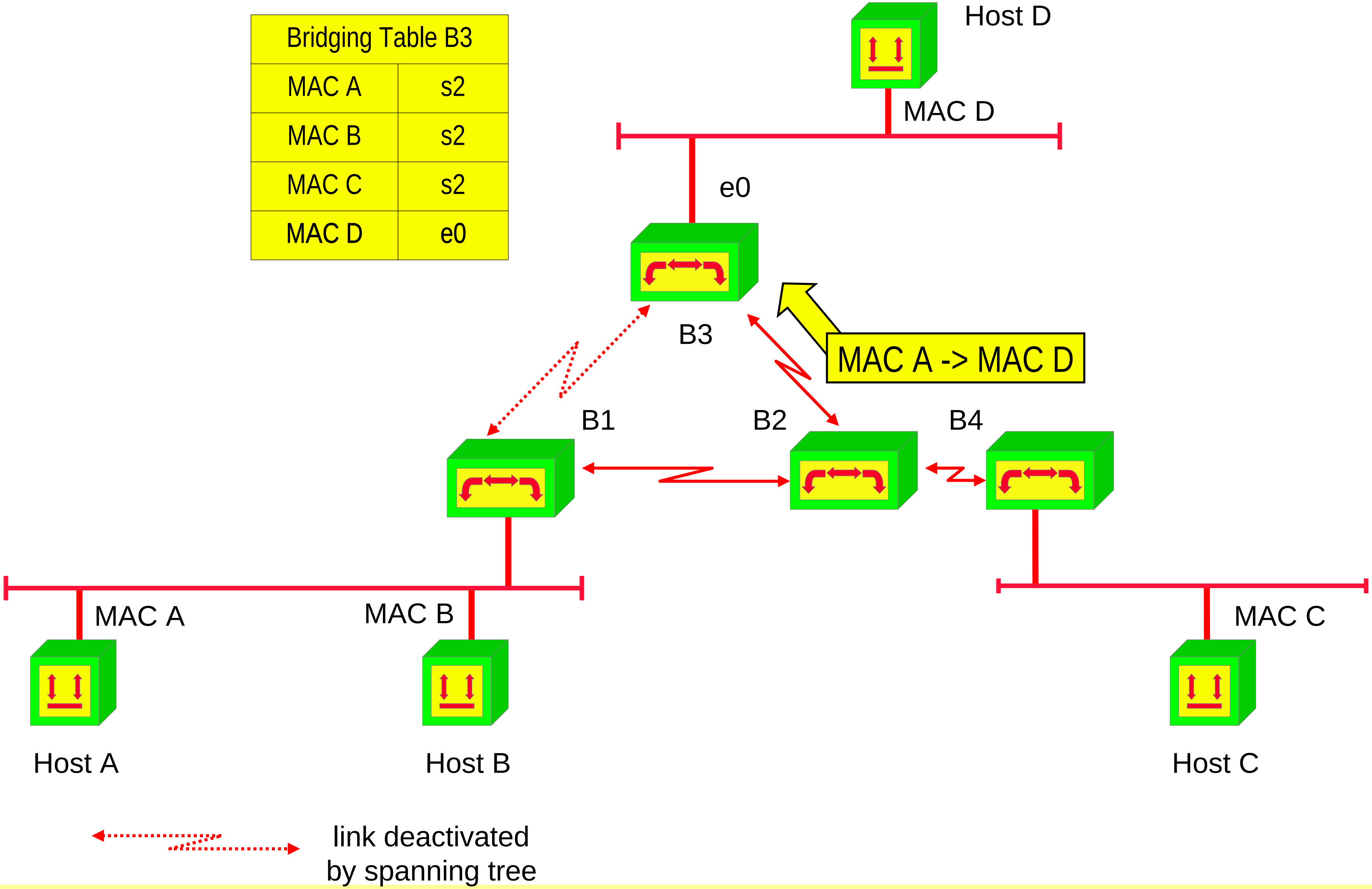


Bridging Table B2	
MAC A	s1
MAC B	s1
MAC C	s3
MAC D	s2

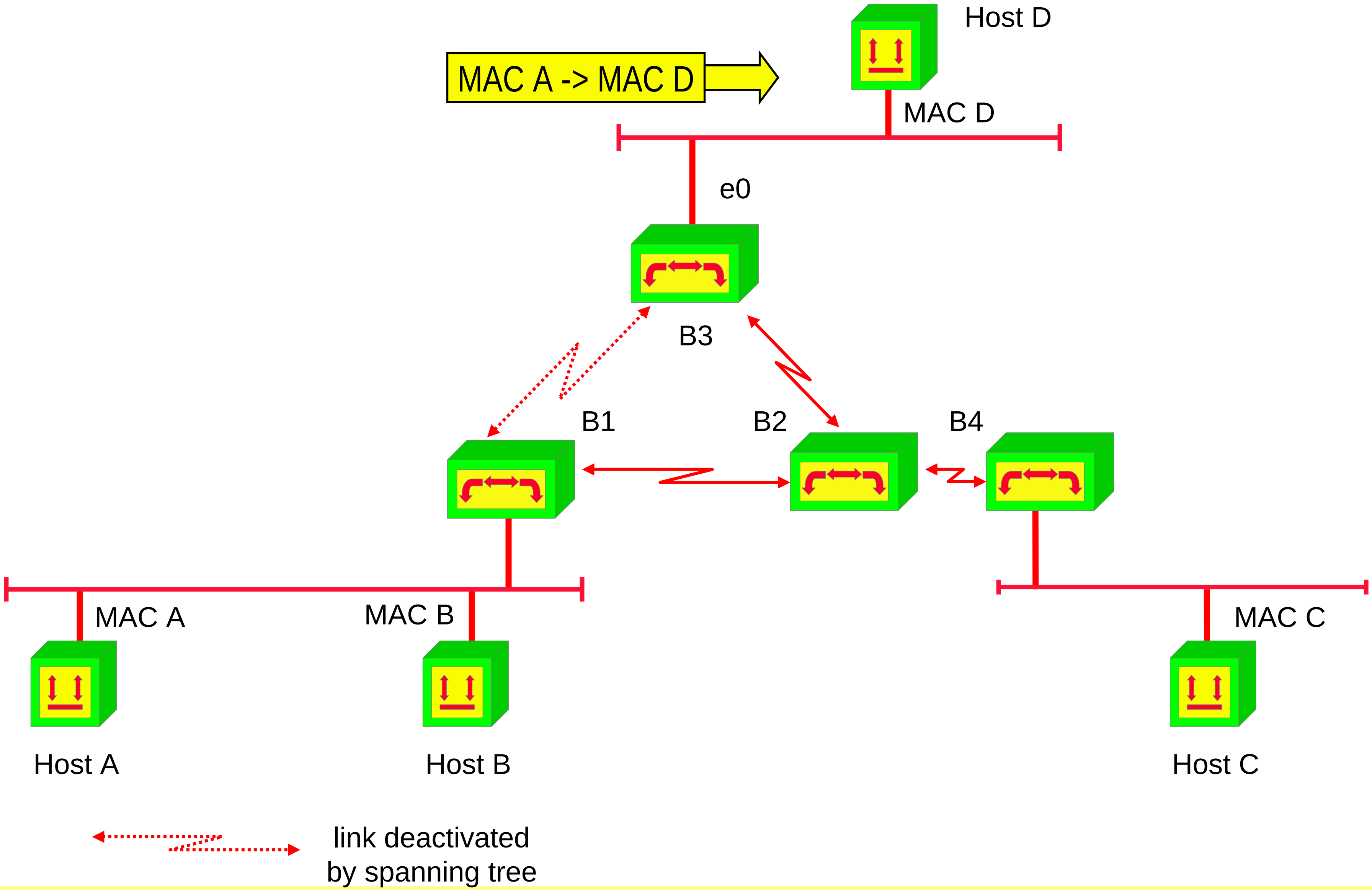
link deactivated
by spanning tree

Frame MAC A to MAC D (3)

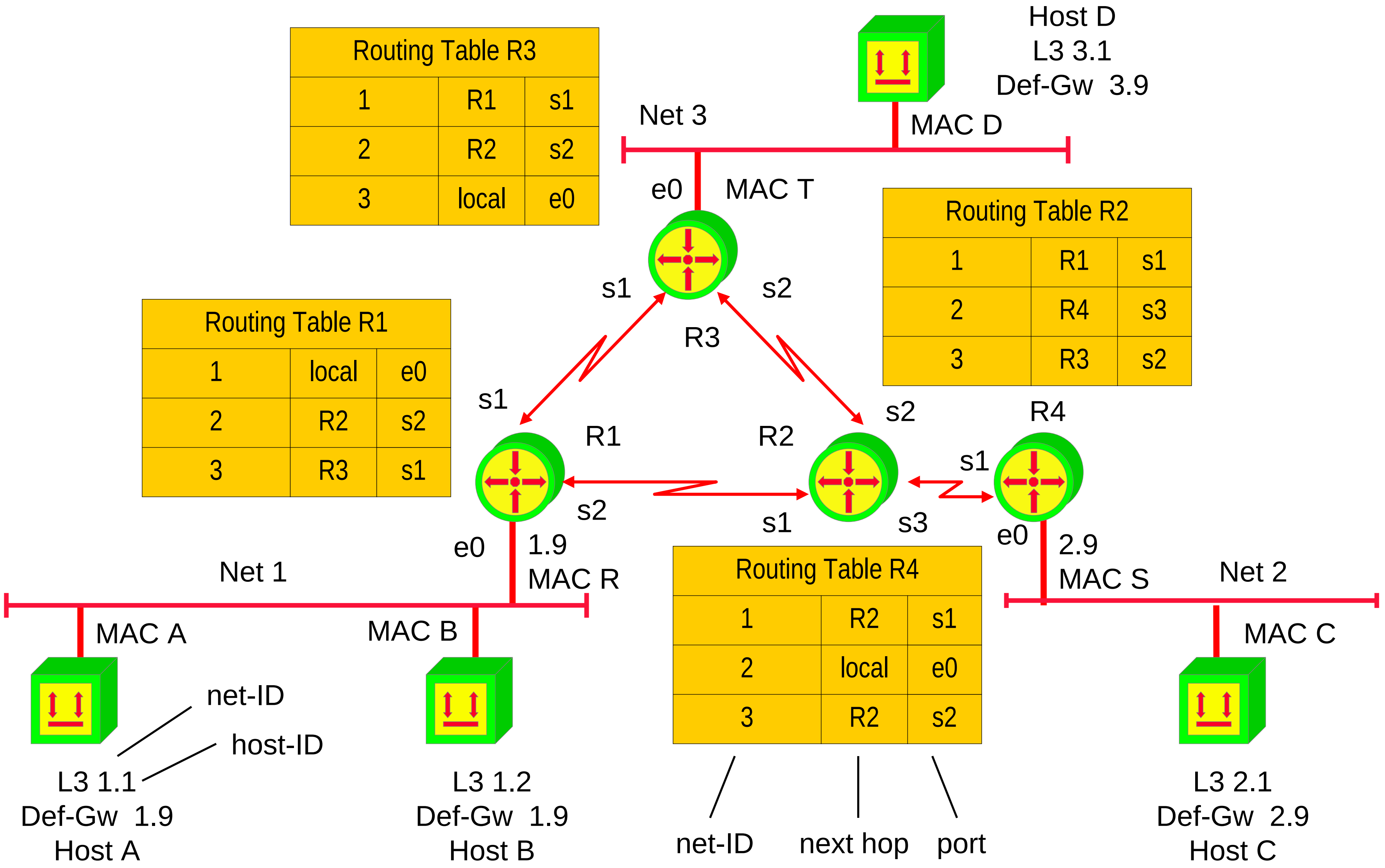
Bridging Table B3	
MAC A	s2
MAC B	s2
MAC C	s2
MAC D	e0



Frame MAC A to MAC D (4)



Example Topology: Generic Routing



Routing Table R3		
1	R1	s1
2	R2	s2
3	local	e0

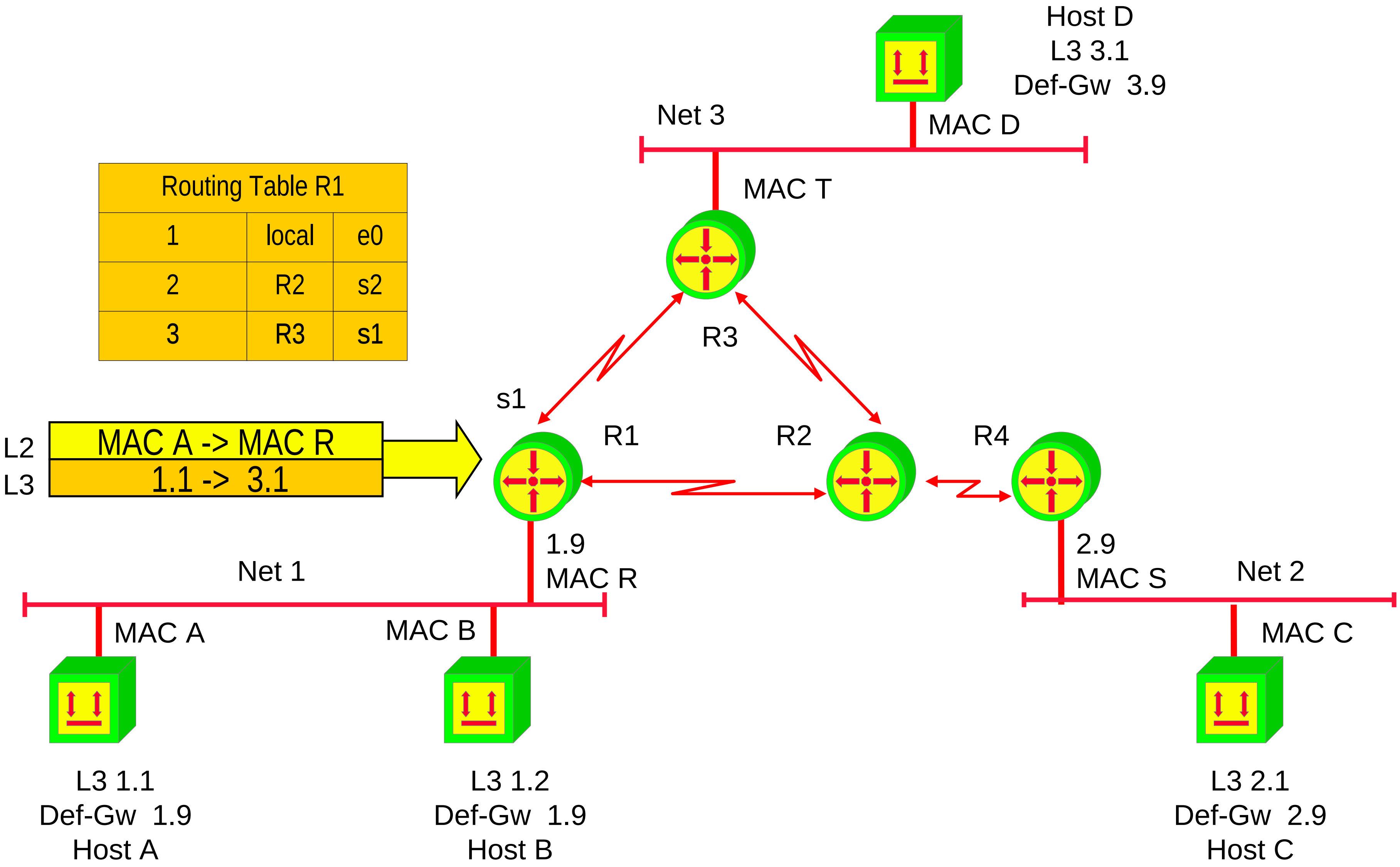
Routing Table R1		
1	local	e0
2	R2	s2
3	R3	s1

Routing Table R2		
1	R1	s1
2	R4	s3
3	R3	s2

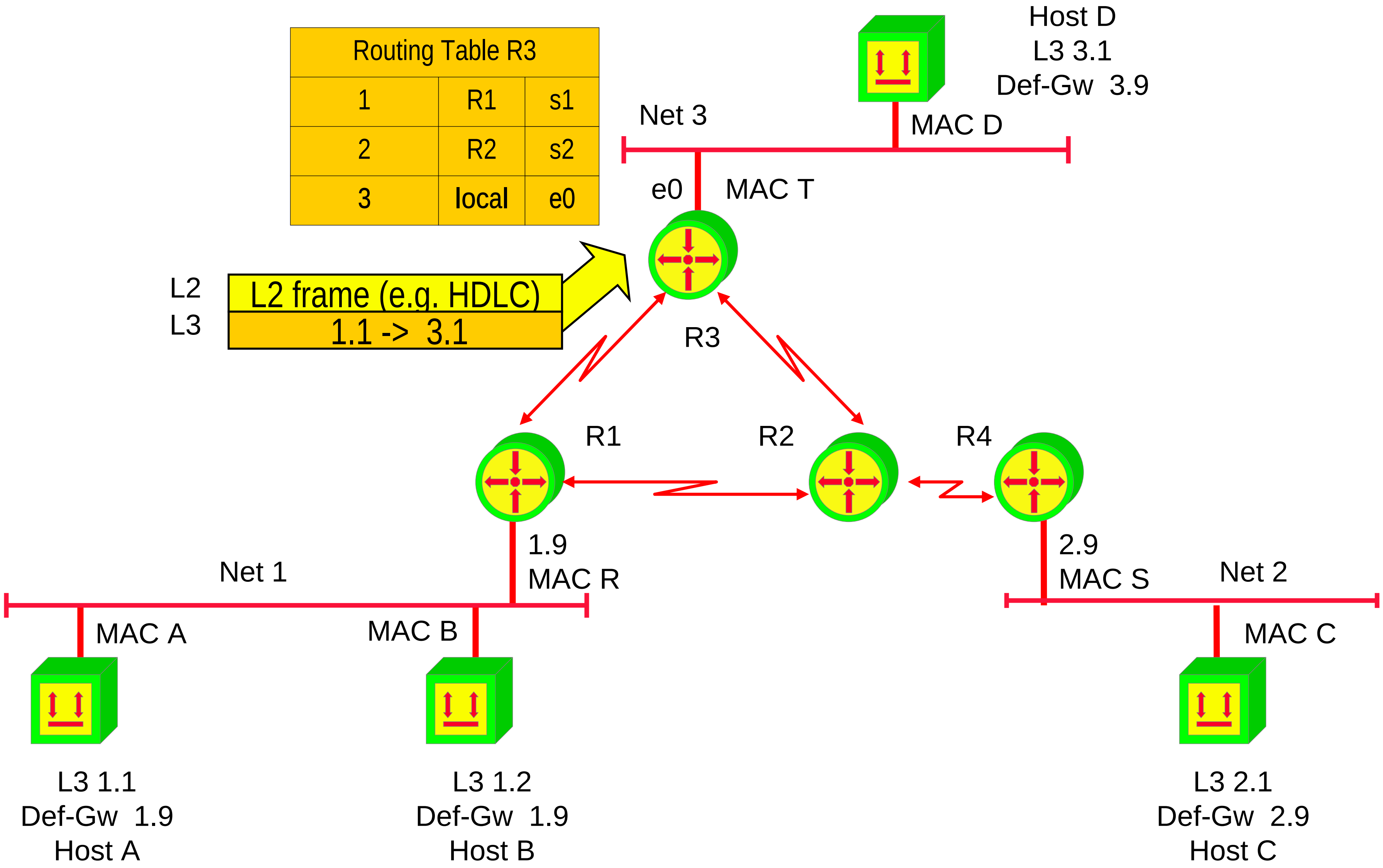
Routing Table R4		
1	R2	s1
2	local	e0
3	R2	s2

Frame 1.1 to 3.1 (1)

Routing Table R1		
1	local	e0
2	R2	s2
3	R3	s1



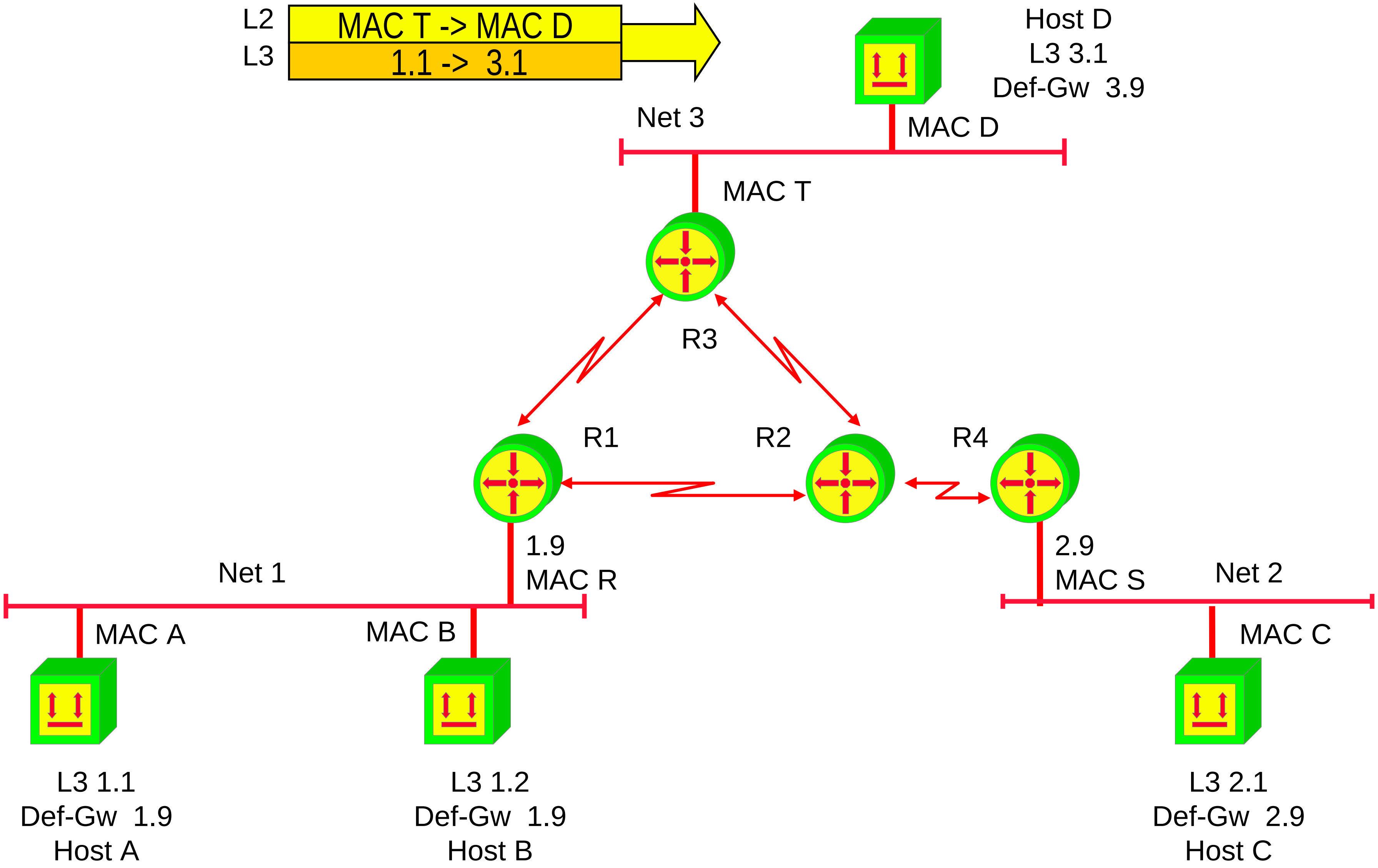
Frame 1.1 to 3.1 (2)



Routing Table R3		
1	R1	s1
2	R2	s2
3	local	e0

L2 L2 frame (e.g. HDLC)
L3 1.1 -> 3.1

Frame 1.1 to 3.1 (3)



Bridging versus Routing

	Bridging		Routing
⊕	Depends on MAC addresses only	⊖	Requires structured addresses (must be configured)
⊕	Invisible for end-systems; transparent for higher layers	⊖	End system must know its default-router
⊖	Must process every frame	⊕	Processes only frames addressed to it
⊖	Number of table-entries = number of all devices in the whole network	⊕	Number of table-entries = number of subnets only
⊖	Spanning Tree eliminates redundant lines; no load balance	⊕	Redundant lines and load balance possible
⊖	No flow control	⊕	Flow control is possible (router is seen by end systems)

Bridging versus Routing

Bridging	Routing
⊖ No LAN/WAN coupling because of high traffic (broadcast domain!)	⊕ Does not stress WAN with subnet's broad- or multicasts; commonly used as "gateway"
⊖ Paths selected by STP may not match communication behaviour/needs of end systems	⊕ Router knows best way for each frame
⊕ Faster, because implemented in HW; no address resolution	⊖ Slower, because usually implemented in SW; address resolution (ARP) necessary
⊕ Location change of an end-system does not require updating any addresses	⊖ Location change of an end-system requires adjustment of layer 3 address
⊖ Spanning tree necessary against endless circling of frames and broadcast storms	⊖ Routing-protocols necessary to determine network topology

Summary

- Ethernet Bridging is "Transparent Bridging"
  - Hosts do not "see" bridges
  - Plug & Play
- 1 Collision domain ➔ 1 Broadcast domain
- Switches increase network performance !
- Redundant paths are dangerous
  - Broadcast storm is most feared
  - Solution: Spanning Tree Protocol
- VLANs create separated broadcast domains
  - Port based or address based VLANing
  - Routers allow inter-VLAN traffic

Quiz

- Can I bridge from Ethernet to Token Ring?
- How is flow control implemented?
- Which bridge should be root bridge?
- What are main differences between 802.1q and ISL?
- What are Layer-3, Layer-4, and Layer-7 switches ?