LAN, Legacy Ethernet, Bridging

LAN Introduction, IEEE Standards,
Logical Link Control (LLC), Ethernet Fundamentals,
Bridging Fundamentals, Bridging vs. Routing

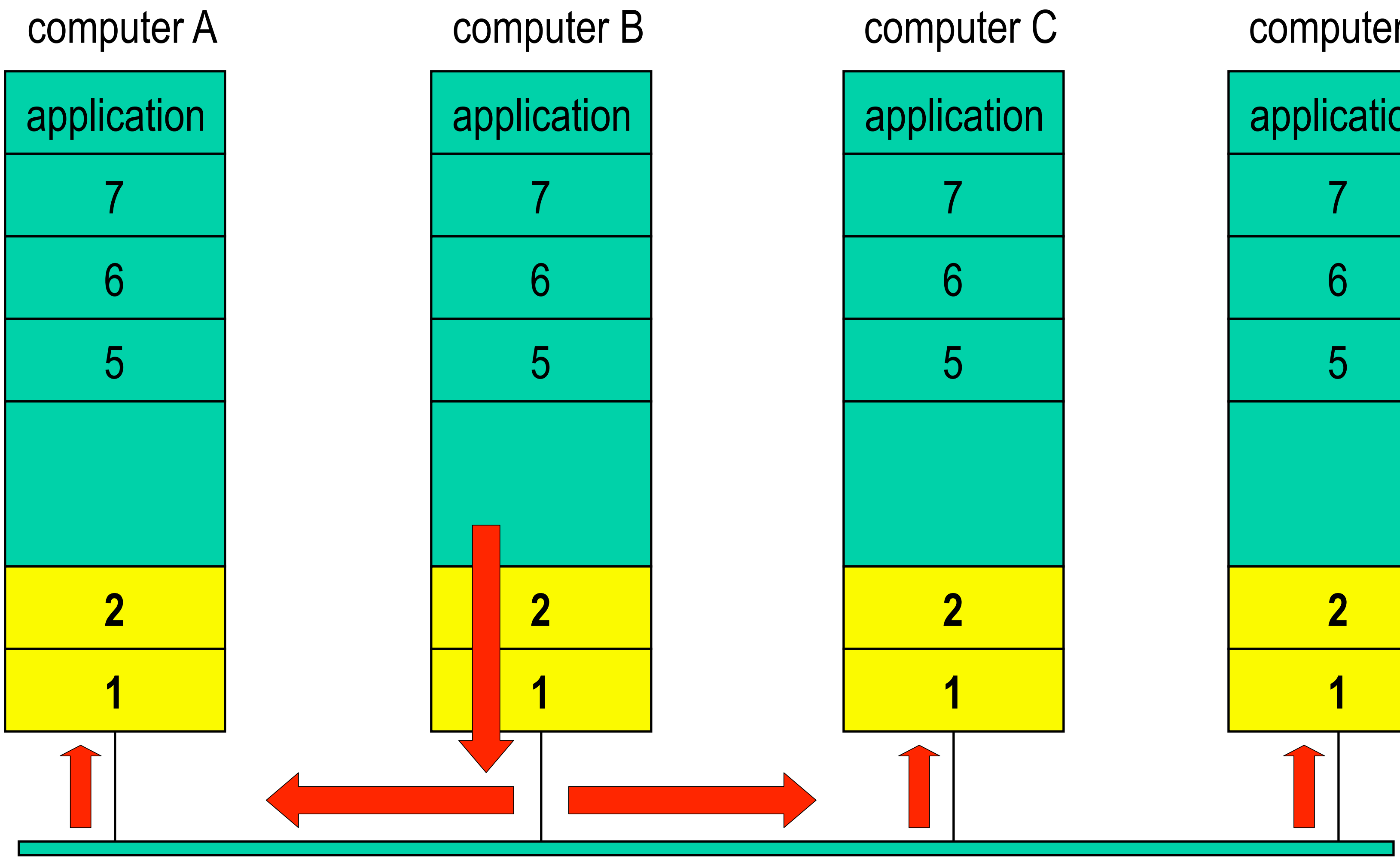
Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

LAN History

- **Local Area Network (LAN), invented late 70s**
  - Initially designed for a common transmission medium
    - Shared media
  - High speed
    - 4 Mbit/s, 10 Mbit/s, 16 Mbit/s, 100 Mbit/s
    - nowadays up to 10 Gbit/s
  - Limited distance
    - Up to some km -> hence local
  - High speed
    - Did not allow any network elements with store and forward behavior
  - Therefore simple topologies
    - Bus, ring, star
  - Base for distributed computing

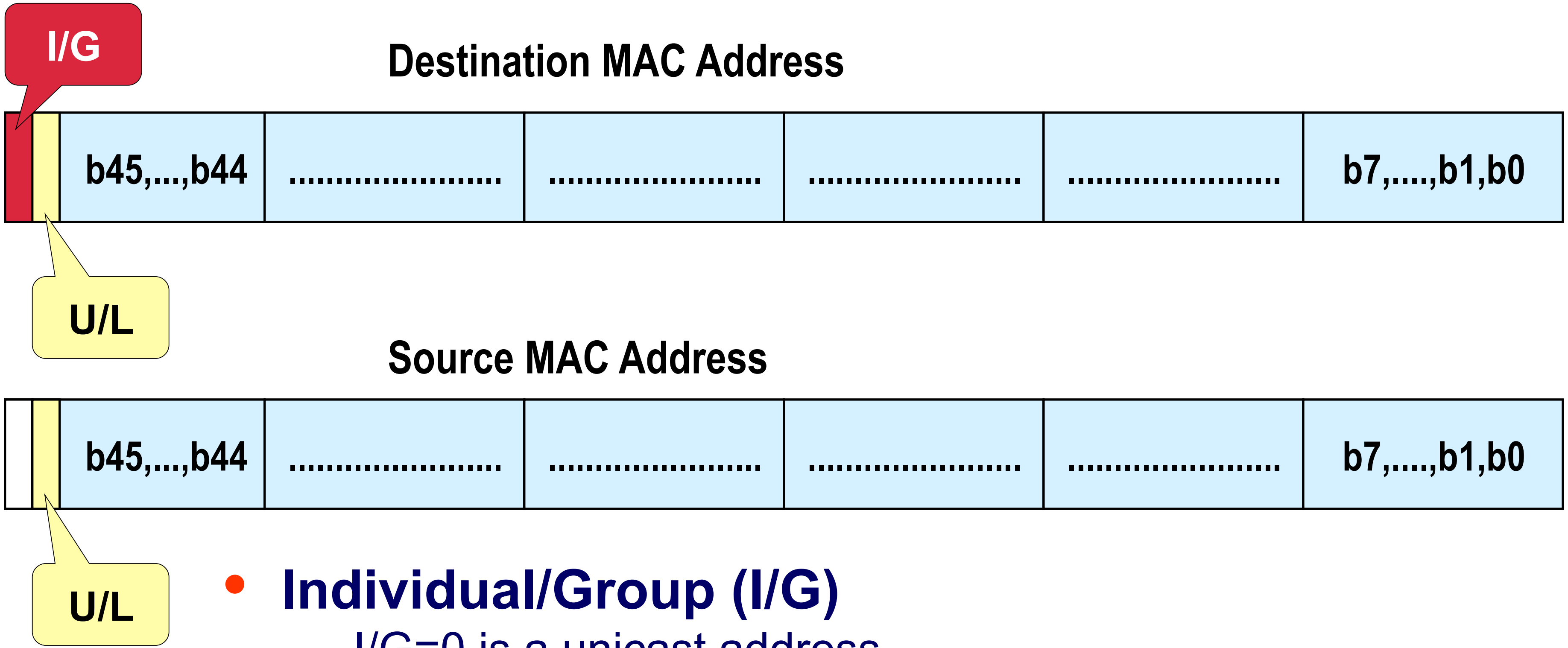
LAN Communication



LAN = Natural Broadcast Medium

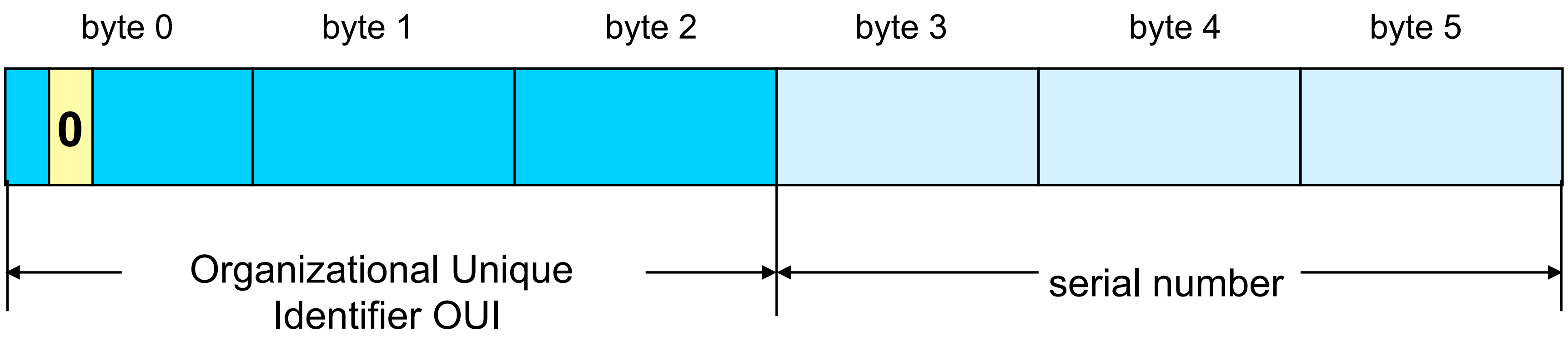
MAC (Media Access Control) and L2 addressing is needed

6 Byte MAC Addresses



- **Individual/Group (I/G)**
  - I/G=0 is a unicast address
  - I/G=1 is a group (broadcast) address
- **Universal/Local (U/L)**
  - U/L=0 is a global, IEEE administered address
  - U/L=1 is a local administered address

MAC Address Structure



- **Each vendor of networking component can apply for an unique vendor code**
- **Administered by IEEE**
- **Called "Burnt In" Address (BIA)**

Storage Format of 802.3 MAC-Address

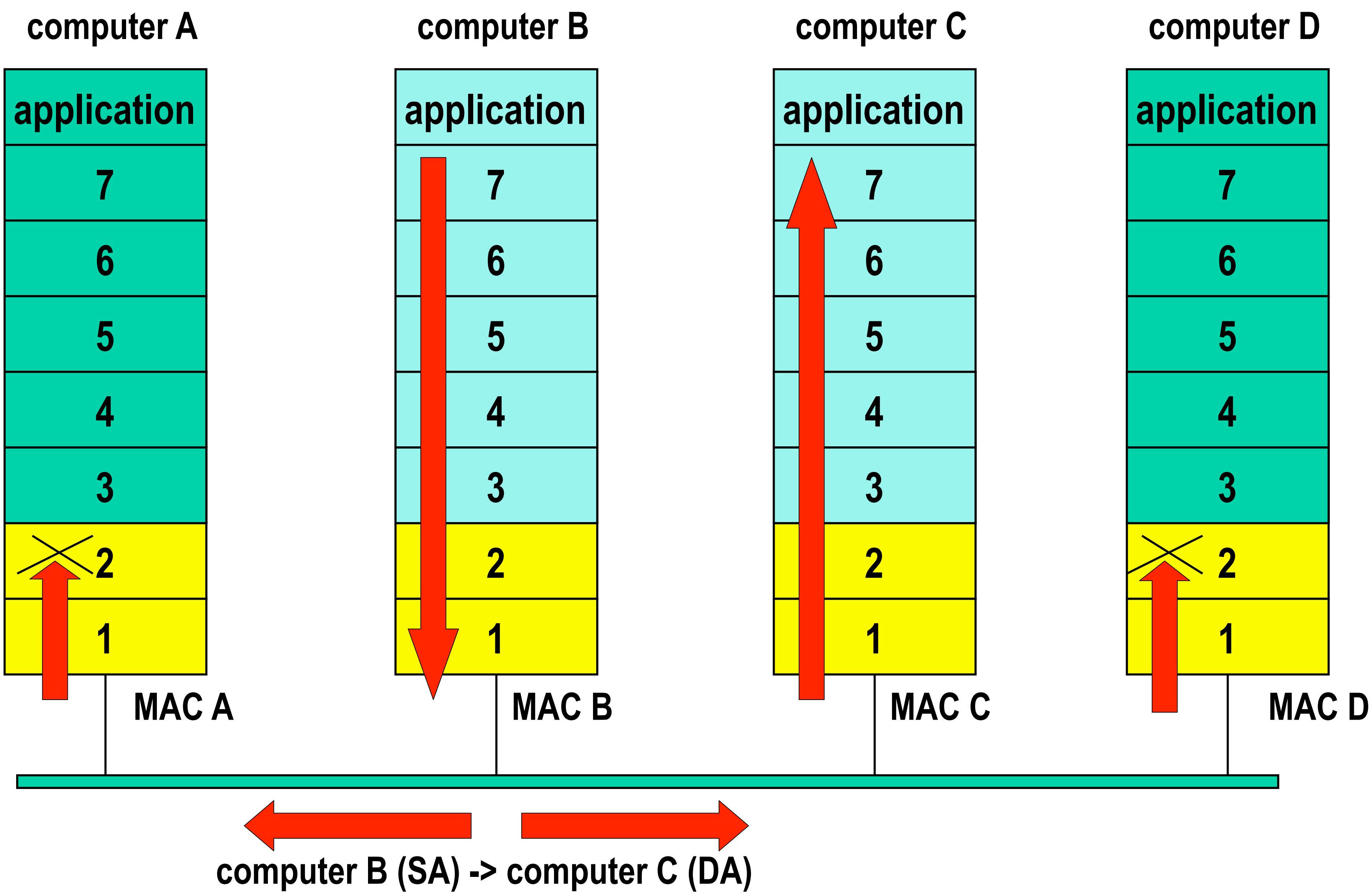
- **Basic rule:**
  - I/G bit must be the first bit on the medium, so the transmitted address must have the following format:

I/G	U/L	b45, ..., b40	b39, ..., b32	...	b15, ..., b8	b7, ..., b1, b0
0	1	00 1000	0000 0000	....	0000 0000	1100 0001

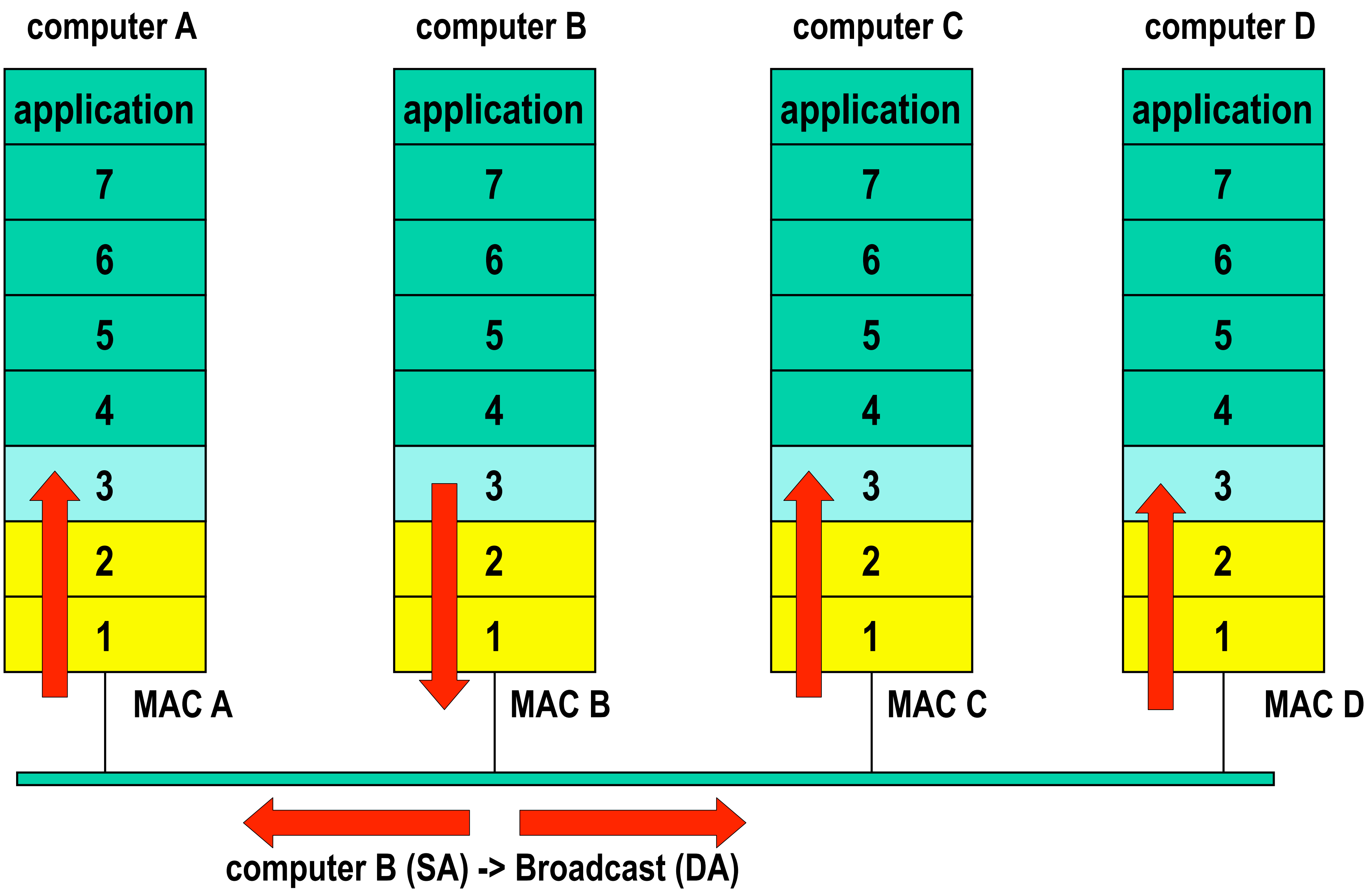
  - <u>802.3 sends the least significant bit of each octet at first</u>
    - So 802.3 must store each octet in memory in reverse order:
    - also called <u>**"Canonical" Format**</u>

b40, ..., b45	U/L	I/G	b32, ..., b39	...	b8, ..., b15	b0, b1, ..., b7
0001 00	1	0	0000 0000	....	0000 0000	1000 0011

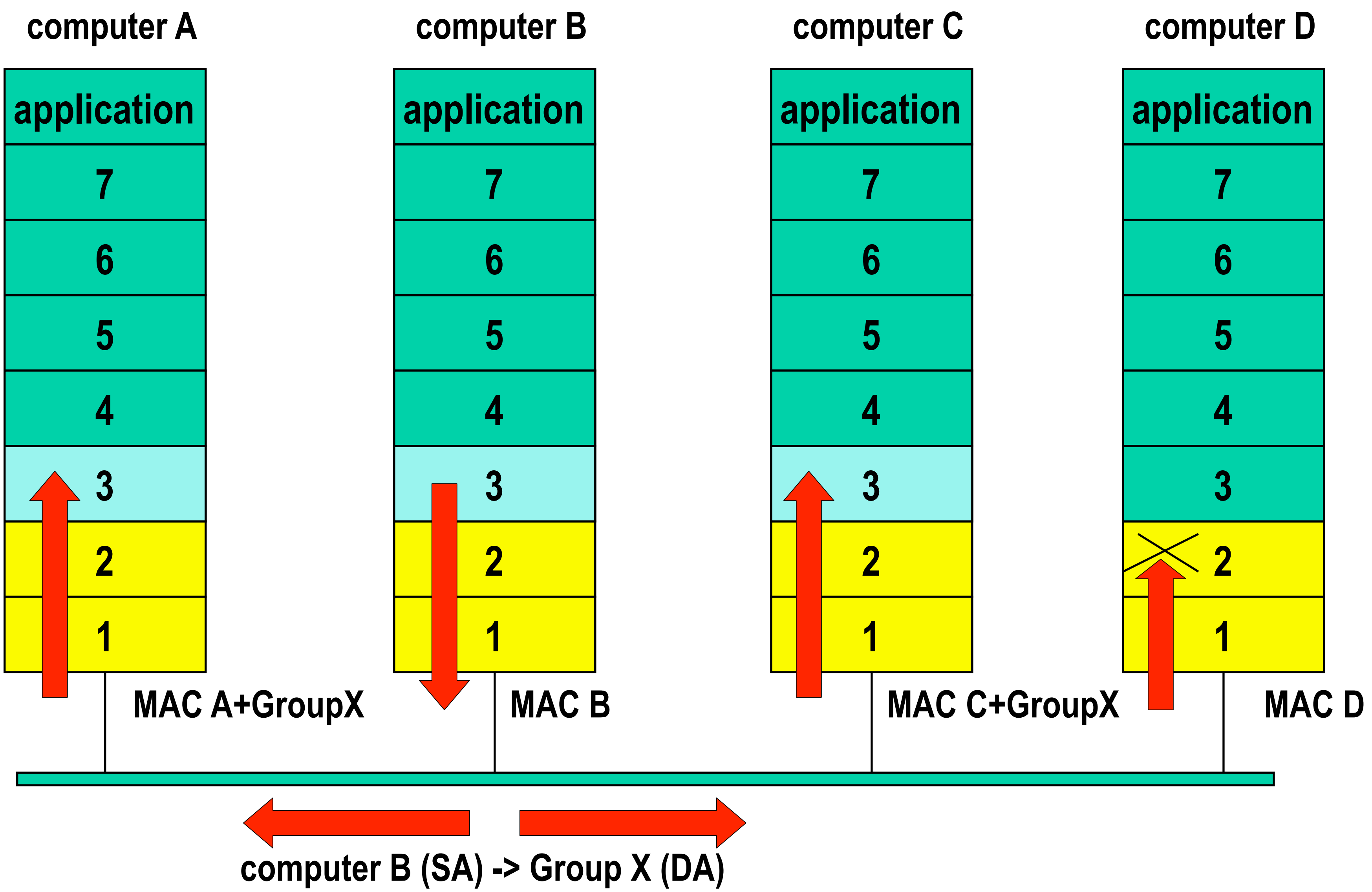
LAN: Only OSI Layer 1, 2 Needed
L2 Unicast Communication



L2 Broadcast Communication



L2 Multicast Communication



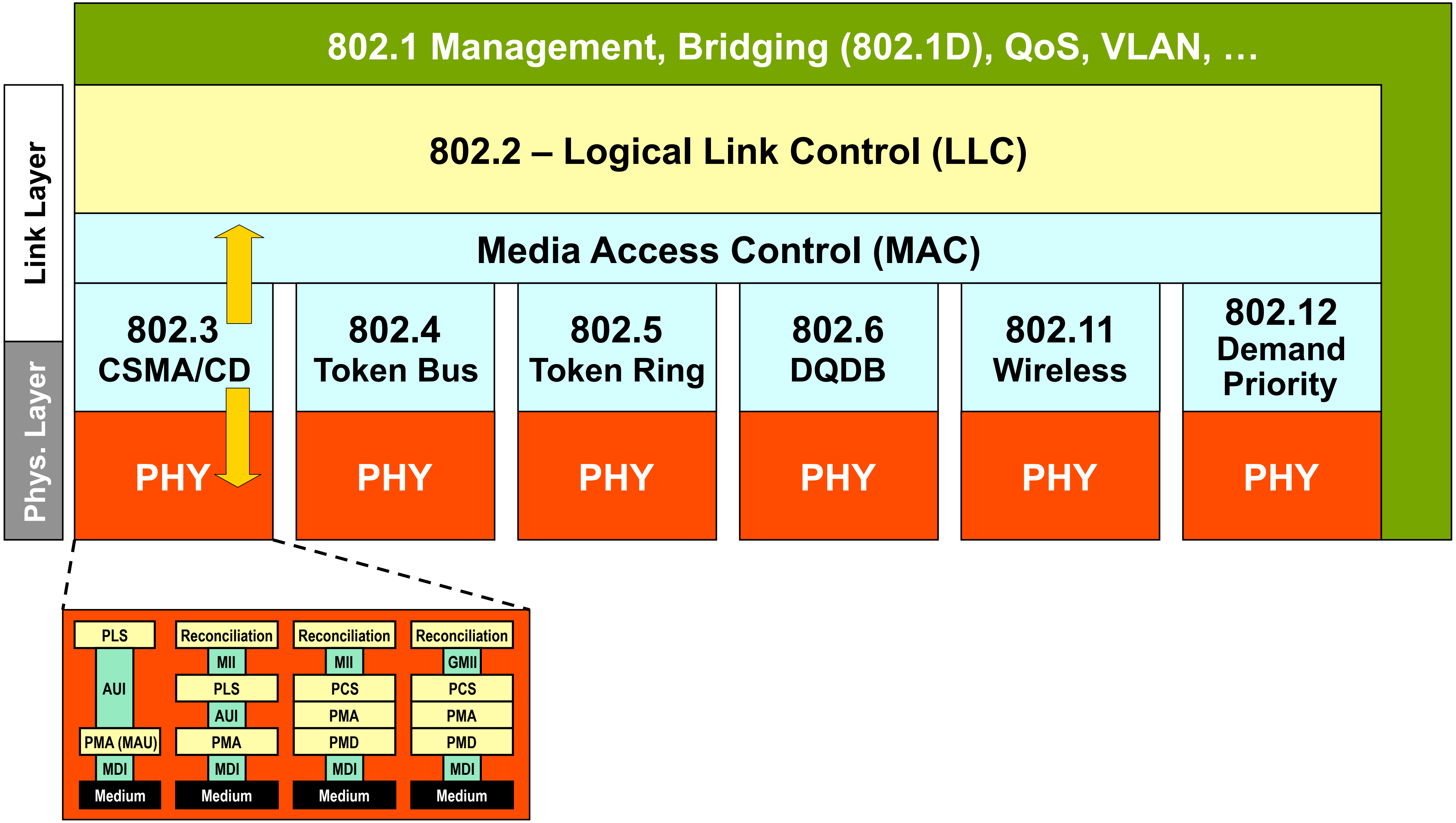
Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

IEEE 802

- **LAN Standardization is done**
  - By IEEE (Institute of Electrical and Electronics Engineers)
  - Workgroup 802 (Start: February 1980)
- **OSI Data Link Layer (Layer 2)**
  - Was originally designed for point-to-point line
  - But LAN = multipoint line, shared media
- **Therefore OSI Layer 2 was split into two sublayers**
  - Logical Link Control
  - Media Access Control

IEEE 802 Layer Model



The IEEE Working Groups

- 802.1 Higher Layer LAN Protocols
- 802.2 Logical Link Control
- 802.3 Ethernet
- 802.4 Token Bus
- 802.5 Token Ring
- 802.6 Metropolitan Area Network (DQDB, MAN)
- 802.7 Broadband TAG
- 802.8 Fiber Optic TAG
- 802.9 Isochronous LAN
- 802.10 Security
- 802.11 Wireless LAN (WLAN)
- 802.12 Demand Priority (VGAnyLAN)
- 802.13 Not Used
- 802.14 Cable Modem
- 802.15 Wireless Personal Area Network (Bluetooth)
- 802.16 Broadband Wireless Access
- 802.17 Resilient Packet Ring

Superstition?

Tasks of LAN Layers 1

- Physical layer (PHY) specifies actual transmission technique
- Provides
  - Electrical/optical specification
  - Mechanical interface
  - Encoding
  - Bit synchronisation
- Consists of
  - MAU (Medium Attachment Unit)
  - AUI (Attachment Unit Interface)
  - PLS (Physical Layer Signalling)
  - Later expanded by PCS, PMA, PMD

Tasks of LAN Layers 2

- MAC (Media Access Control) takes care for medium access algorithms, framing, addressing and error detection
  - Avoid collisions
  - Grant fairness
  - Handle priority frames

- LLC (Logical Link Control) provides original services of data link layer
  - “HDLC on LAN”
  - Connection-oriented services with error-recovery
  - Connection-less service (best-effort)
  - SAPs (Service Access Points) for the higher layers

IEEE 802.1 Standards

- **Specifies a common framework for all 802.x LANs**
  - Addressing rules, relations to the OSI model
  - Subnet addressing, Bridging Ethernetv2 to 802.2 LANs
  - Management (802.1B)
  - Bridging (802.1D-1998) including STP (Spanning Tree Protocol)
    - Single STP in case of VLANs
  - System Load Protocol (802.1E)
  - Virtual (V) LANs (802.1Q)
    - Tagging
  - STP Rapid Configuration (802.1w or 802.1D-2004)
  - Multiple STP (802.1Q-2003)
    - Multiple STP instances in case of VLANs
  - EAP Authentication (802.1x)
    - Extensible Authentication Protocol

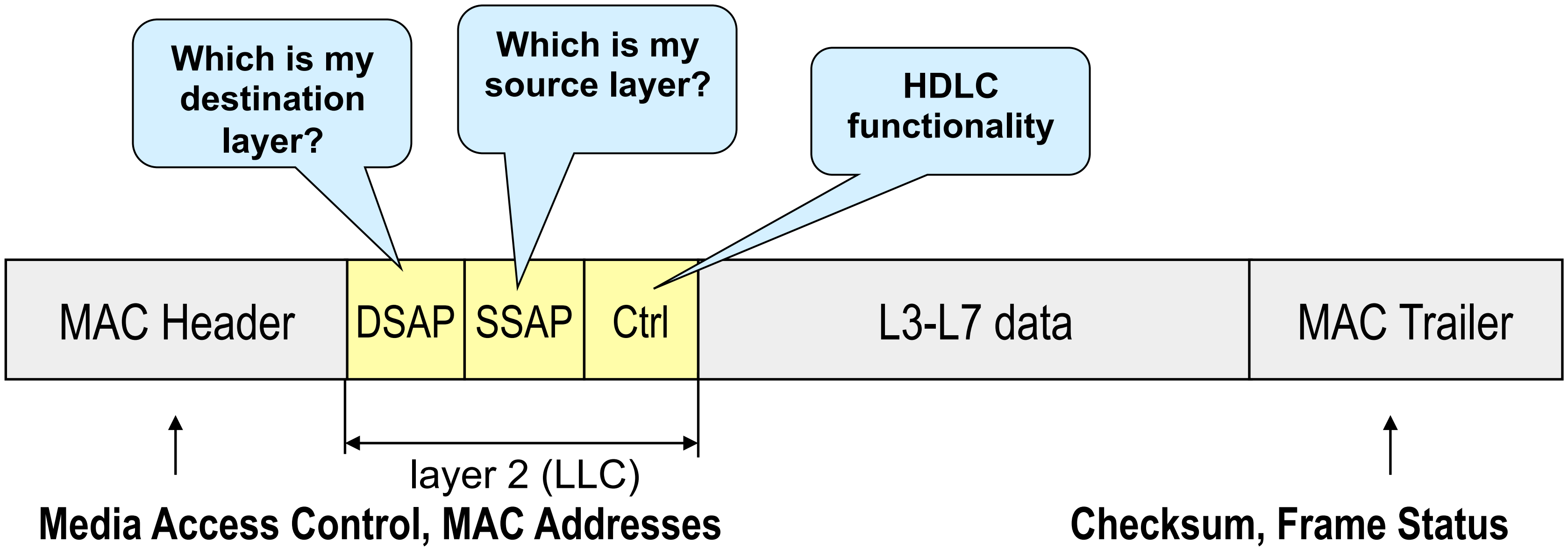
Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

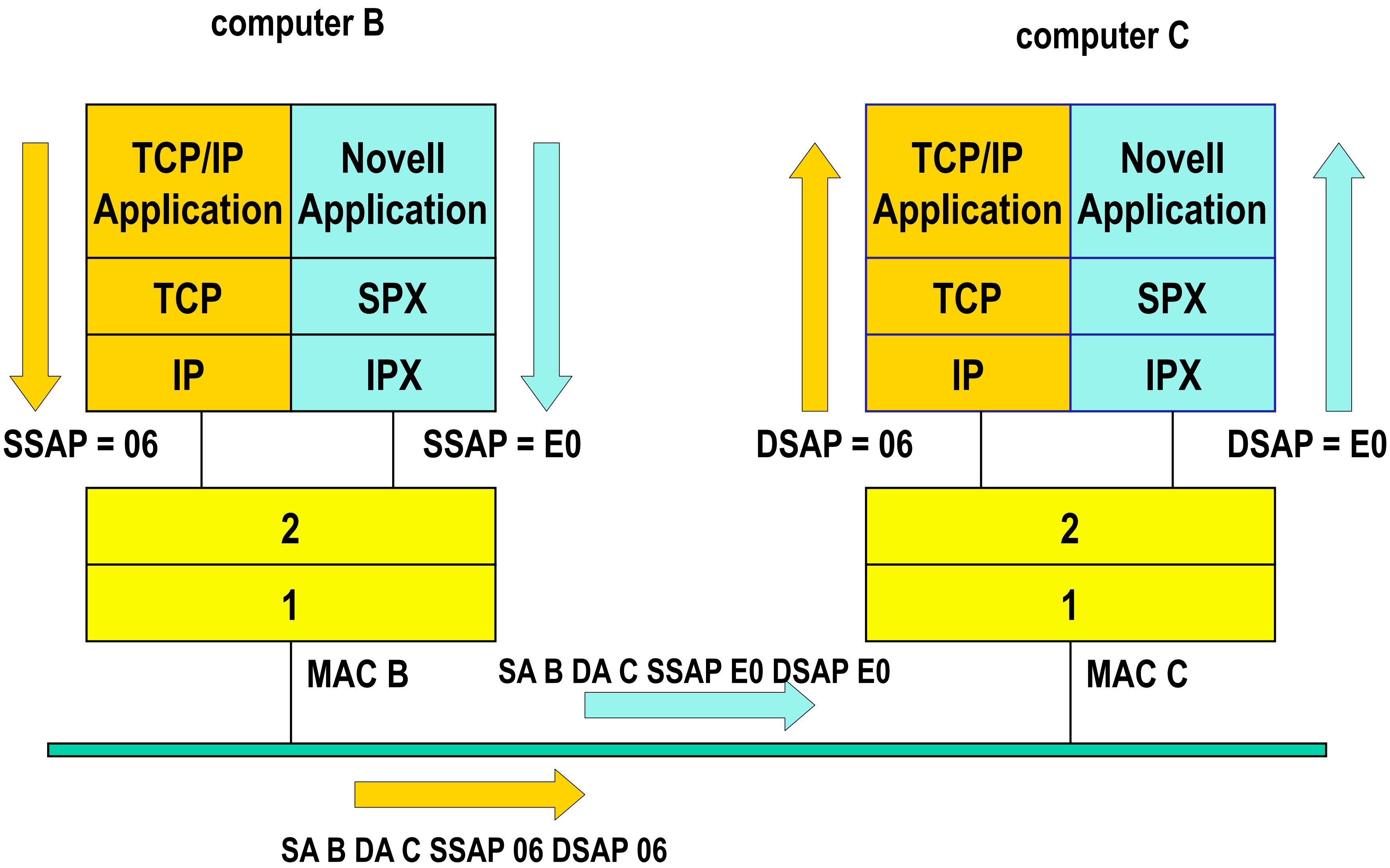
IEEE LAN Framing

- **Every IEEE LAN/MAN protocol carries the Logical Link Control header**
  - DSAP (Destination Service Access Point),
  - SSAP (Source Service Access Point)
  - Control Field = HDLC heritage

Basic L2 frame format of every IEEE protocol

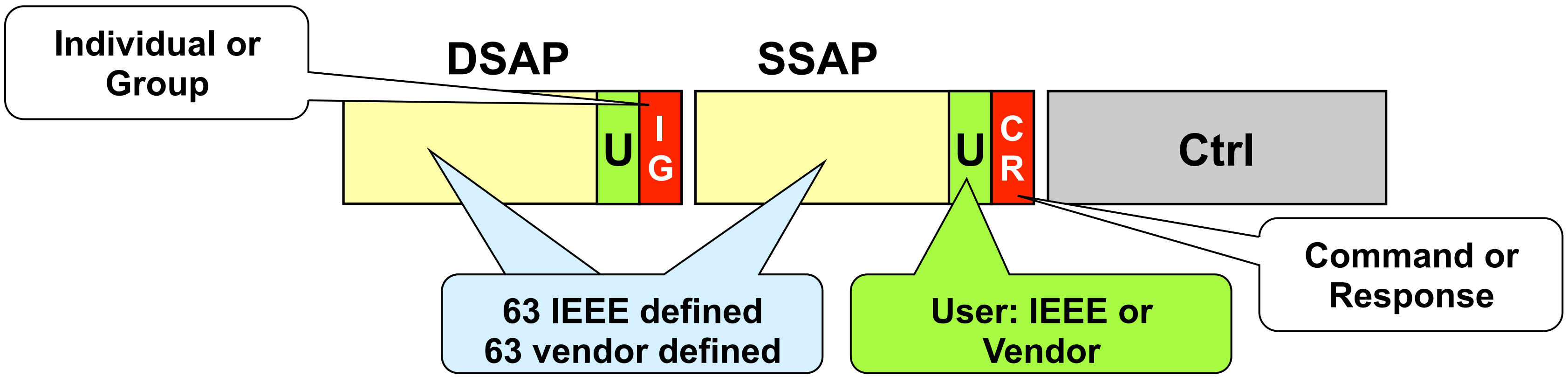


Protocol Stack Distinction



SAP Identifiers

- **128 possible values for protocol identifiers**
- **Examples:**
  - 0x42 … Spanning Tree Protocol 802.1d
  - 0xAA… SNAP
  - 0xF0… NetBIOS
  - 0xE0… Novell
  - 0x06... IP (but not used because IP rides on top of Ethernetv2)



LLC Control Field = HDLC Control Field

0 1 2 .... 6 7 8 9 10 .... 14 15

0	N(S)	P/F	N(R)	I - format (Information)

1	0	S S	x x x	P/F	N(R)	S - format (Supervisory)

0 1 2 3 4 5 6 7

1	1	M M	P/F	M M M	U - format (Unnumbered)

N(S), N(R) ...... send- and receive - sequence numbers
S S, MMM .... selection bits for several functions
P / F .... poll / final bit (P in commands, F in responses; distinction of commands and responses through a dedicated SSAP bit -> C/R bit)

LLC Frame Types and Classes

	Cmd	Control	Resp	Control	Class 1	Class 2	Class 3	Class 4
Type 1	UI	1100p000			x	x	x	x
	XID	1111p111	XID	1111f111	x	x	x	x
	TEST	1100p111	TEST	1100f111	x	x	x	x
Type 2	I	0 n(s) p n(r)	I	0 n(s) f n(r)		x		x
	RR	10000000 p n(r)	RR	10000000 f n(r)		x		x
	RNR	10100000 p n(r)	RNR	10100000 f n(r)		x		x
	REJ	10010000 p n(r)	REJ	10010000 f n(r)		x		x
	SABME	1111p110	UA	1100f110		x		x
	DISC	1100p010	DM	1111f001		x		x
			FRMR	1110f001		x		x
Type 3	AC0	1110p110	AC0	1110f110			x	x
	AC1	1110p111	AC1	1110f111			x	x

LLC Service Methods:

- Class 1:
  - Connectionless unacknowledged service (datagram)
  - Type 1 - frames: UI,XID,TEST
- Class 2:
  - Connection oriented service plus Class 1
  - Type 2 - frames: I,RR,RNR,REJ, SABME,UA,DM
- Class 3:
  - Class 1 plus connectionless acknowledged service
  - Type 1 -frames plus additional type 3 - frames: AC0, AC1
- Class 4:
  - Class 2 plus connectionless acknowledged service
  - Type 2 - frames plus additional type 3 - frames: AC0, AC1

Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

“Ethernet works in practice but not in theory.”

Robert Metcalfe

History (1)

- Late 1960s: **Aloha** **protocol University of Hawaii**
- Late 1972: **Robert Metcalfe developed first Ethernet system based on CSMA/CD**
  - Xerox Palo Alto Research Center (PARC)
  - Exponential Backoff Algorithm was key to success (compared with Aloha)
  - 2.94 Mbit/s

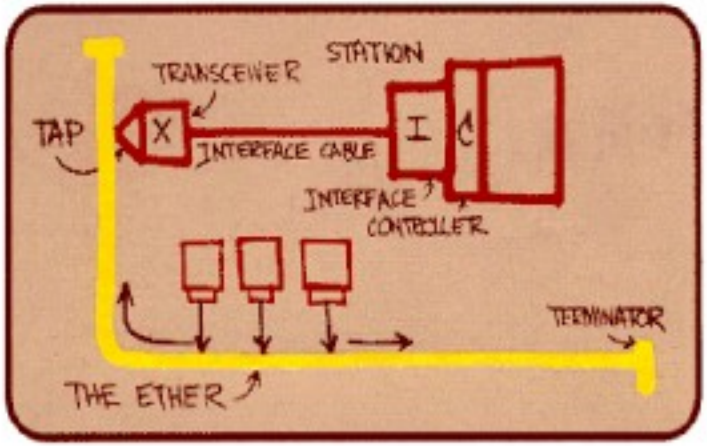
Original Ethernet Frame

Sync	Destination Address	Source Address	Data	CRC
1	8	8	about 4000 bits	16

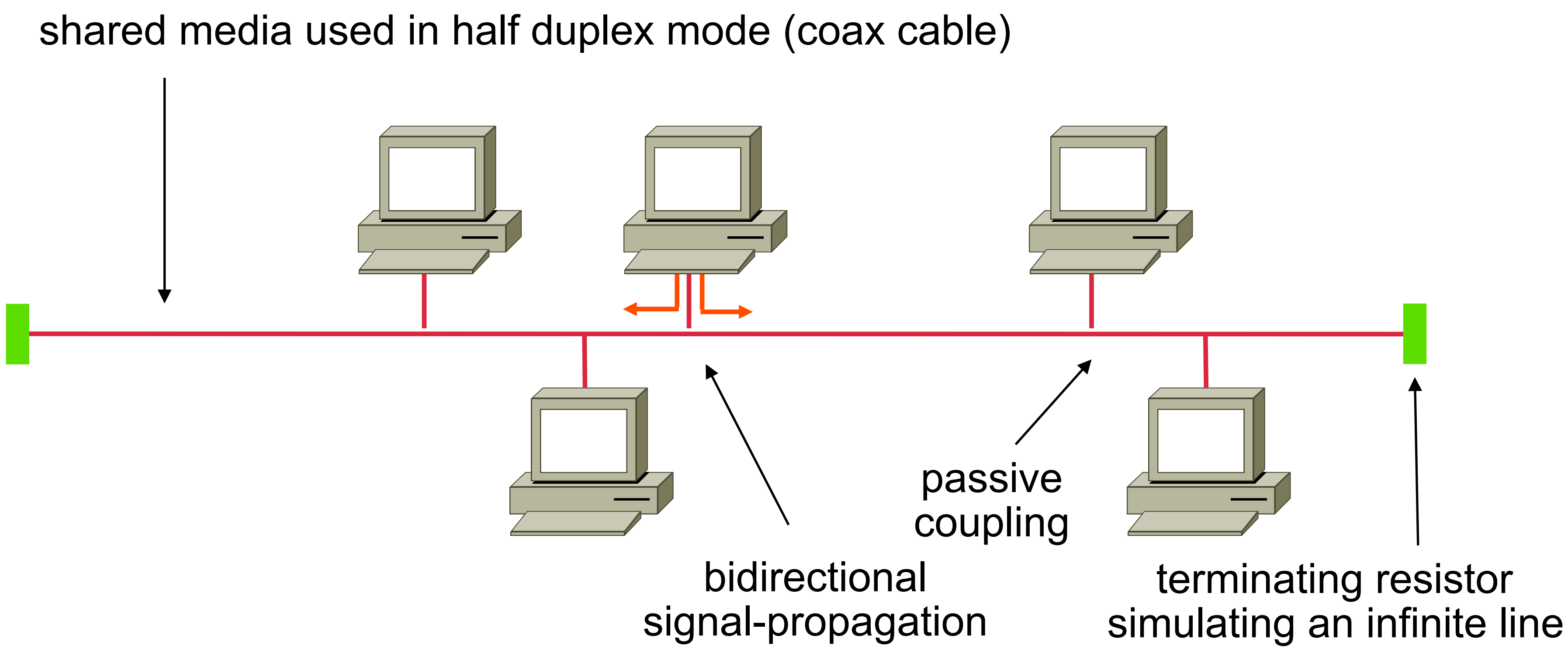
History (2)

- 1976: **Robert Metcalfe released the famous paper:**
  "Ethernet: Distributed Packet Switching for Local Computer Networks"
  - In our context it would be better to call it
    "Asynchronous TDM on a Shared Wire"
    because there is no thing such an
    active packet switch

Original sketch



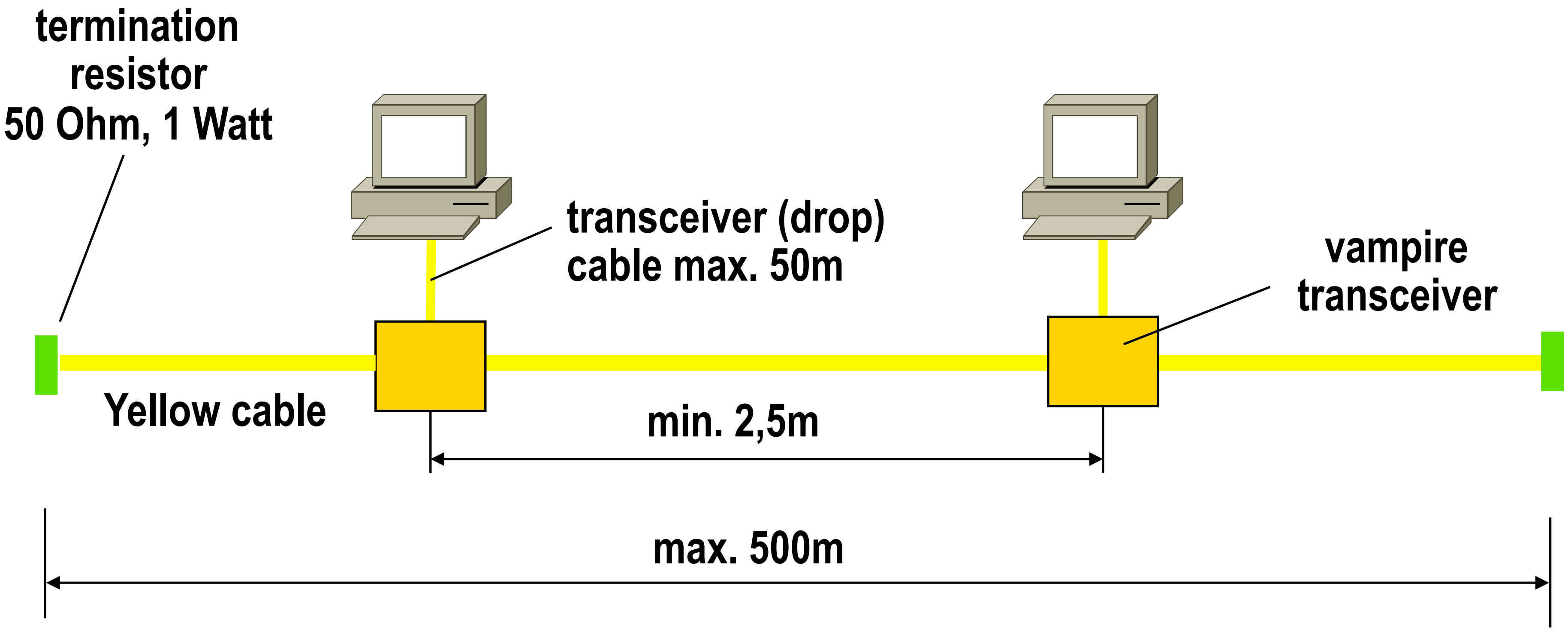
Basic Idea of Ethernet Bus System



History (3)

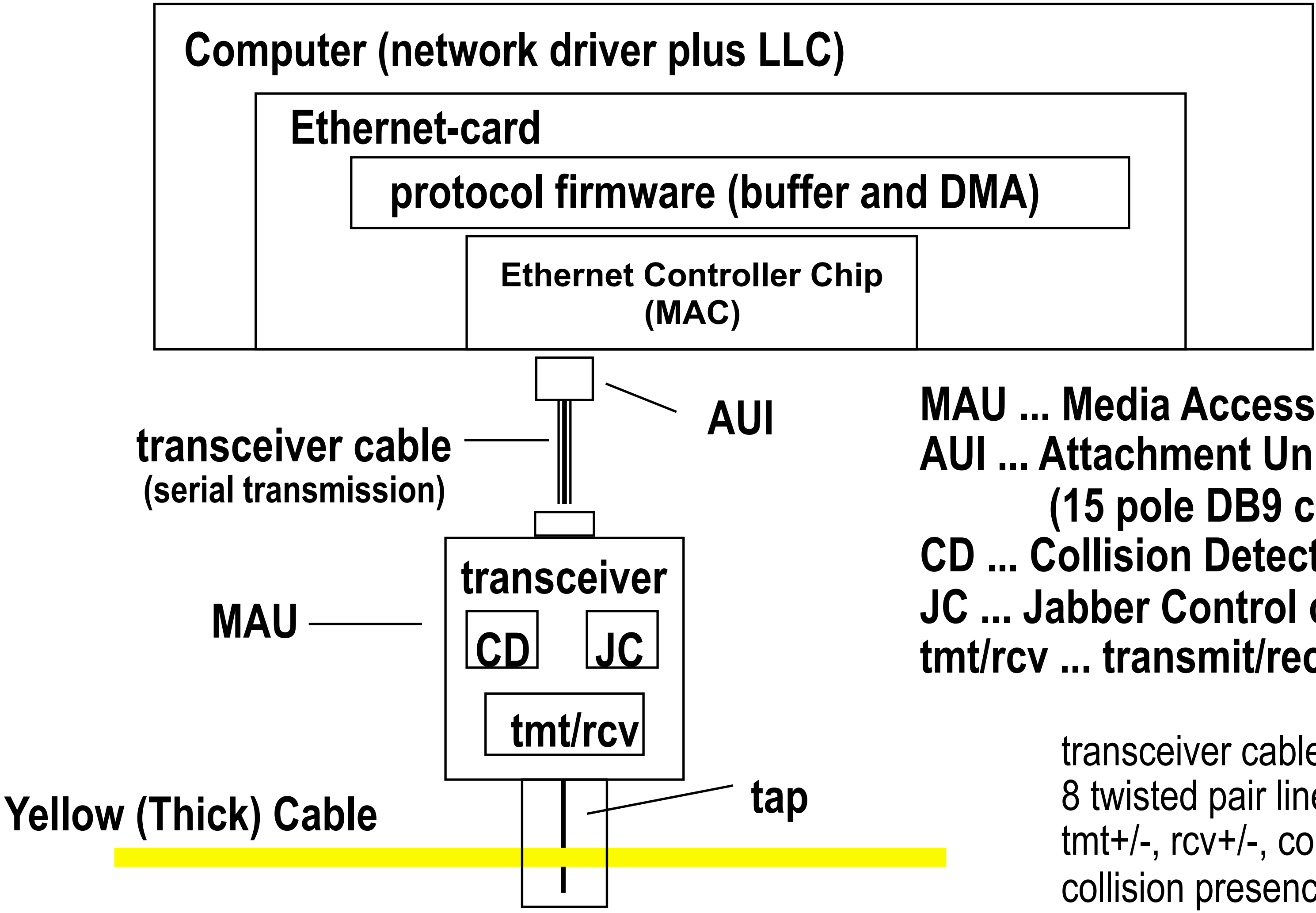
- **1978: Patent for Ethernet-Repeater**
- **1980: DEC, Intel, Xerox (DIX) published the 10 Mbit/s Ethernet standard (Ev1)**
  - "Ethernet II" was latest release (DIX V2.0)
- **Feb 1980: IEEE founded workgroup 802**
- **1985: The LAN standard IEEE 802.3 had been released**
  - Two types with baseband transmission with Manchester encoding, 10 Mbit/s
    - 10Base5 "Yellow Cable"
    - 10Base2 "Cheapernet"
  - One type with broadband transmission
    - 10Broad36 (modulation of carrier) -> like cable TV

10Base5 Parameter



- maximal number of stations: 100
- attachable only at marked points
- cable splitting via coax couplers
- individual cable parts have a length of 23,4m or 70,2m or 117,5m (wave minimum on standing waves due to inhomogeneous media)
- smallest bending radius: 254mm

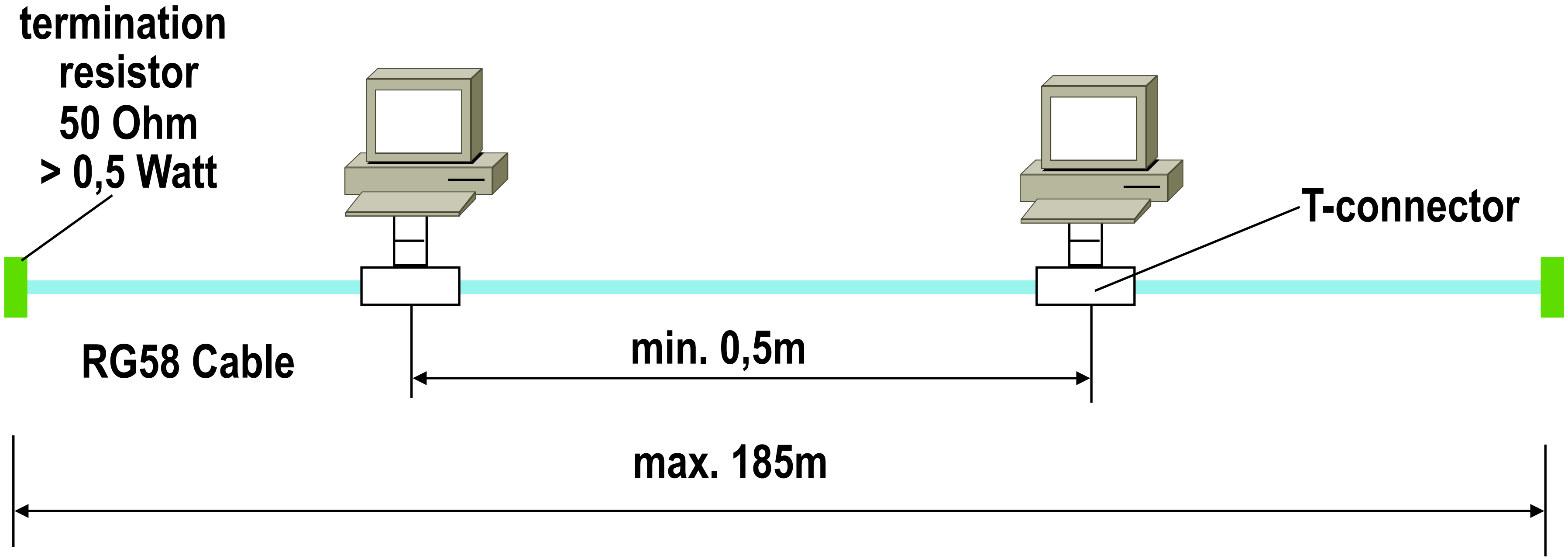
AUI-Connection with 10Base5 Transceiver



MAU ... Media Access Unit
AUI ... Attachment Unit Interface
(15 pole DB9 connector)
CD ... Collision Detecting circuits
JC ... Jabber Control circuits
tmt/rcv ... transmit/receive circuits

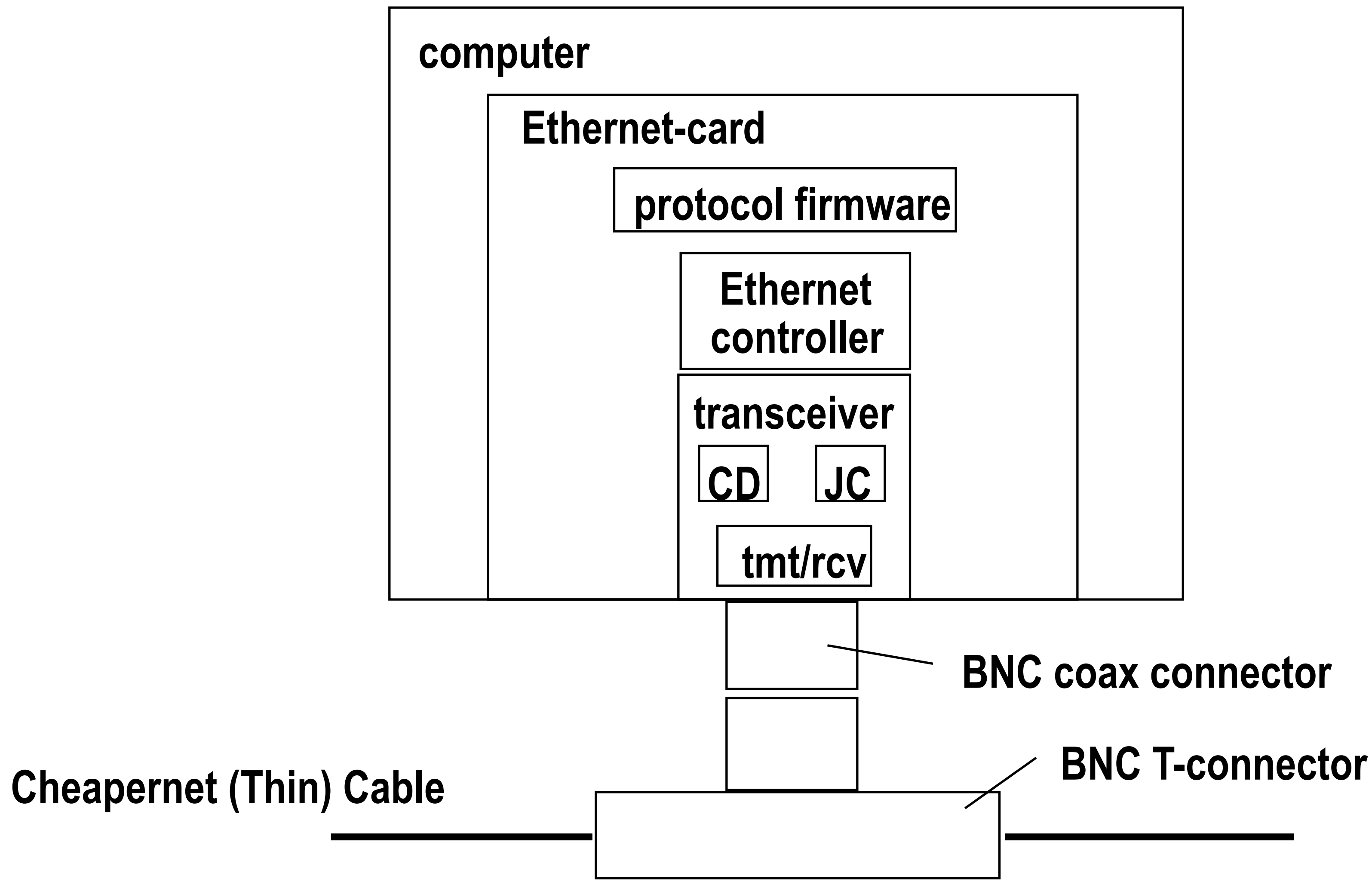
transceiver cable:
8 twisted pair lines for
tmt+/-, rcv+/-, control +/-
collision presence +/-,
3 lines for power, earth, shield

10Base2 Parameter



- maximal number of stations: 30
- attachable at any points
- smallest bending radius: 50 mm

Integrated Transceiver for 10Base2



Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

CSMA/CD (1)

- **Carrier Sense Multiple Access / Collision Detection**
  - Improvement of ALOHA
  - "Listen before talk" plus
  - "Listen while talk"
- **Fast and low-overhead way to resolve any simultaneous transmissions**

1) Listen if a station is currently sending
2) If wire is empty, send frame
3) Listen during sending if collision occurs
4) Upon collision stop sending
5) Wait a random time before retry

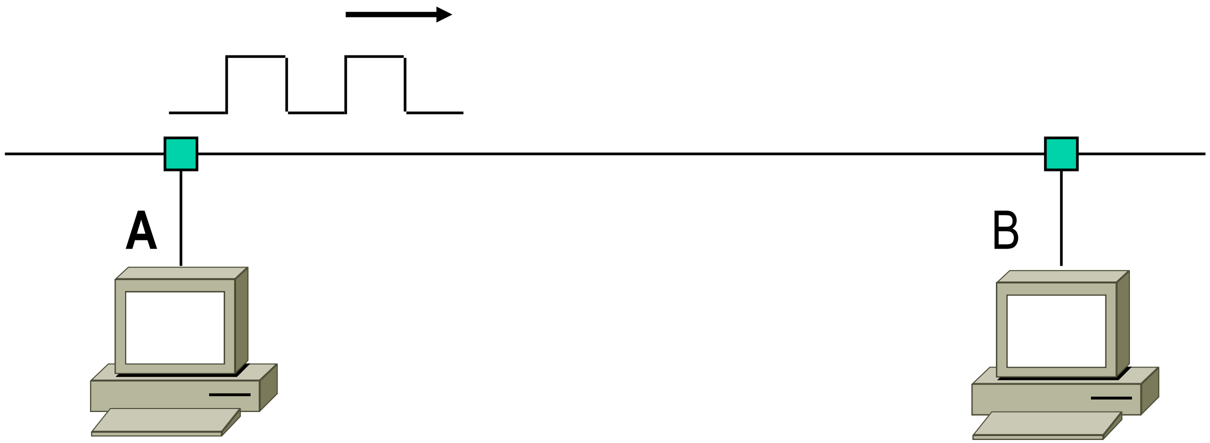
CSMA/CD (2)

- **Details:**
  - Access control based on contention
  - Network stations listen to the bus before they start a transmission
  - Network stations can detect ongoing transmission (CS) and will not start own transmission before ongoing transmission is over
  - But still simultaneous transmissions (MA) cause collisions
    - Collisions are detected (CD) by observing the DC-level on the medium
  - Bus conflict

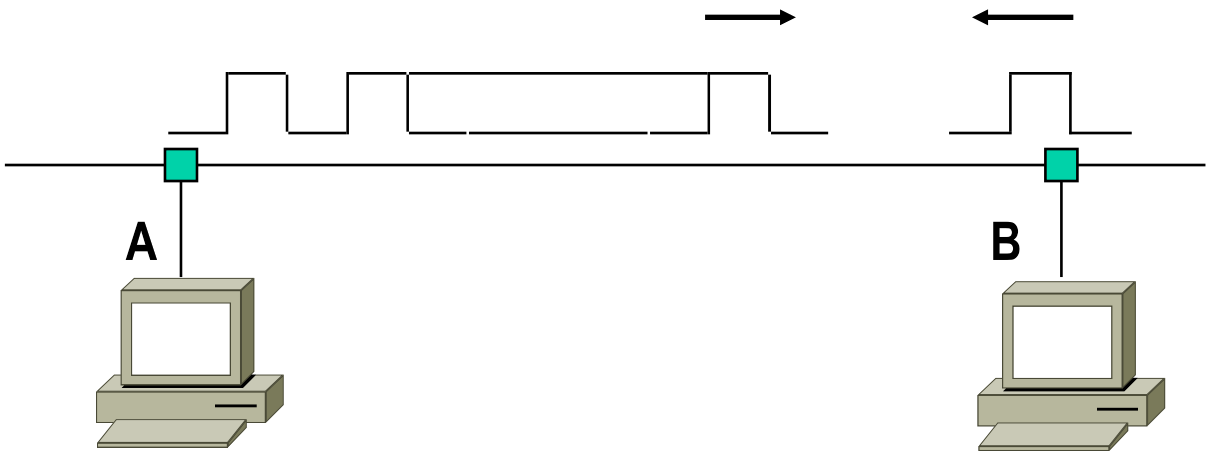
CSMA/CD (3)

- **Conflict resolution:**
  - Aborting of transmission by all involved stations
  - Sending of a JAM-signal (32 bit)
    - To make sure that every station can recognize the collision
    - Collision is spread to a minimum length
  - Starting a random number generator to create a timeout value
    - Truncated binary exponential backoff algorithm (the more often a collision occurs the larger is the range for the random number)
  - After timeout expired, station attempts a retransmission
  - Number of retransmission-trials is limited to 16
    - After 16 collisions in a sequence a error is signaled to the higher layer

Collision Window / Slot Time 1

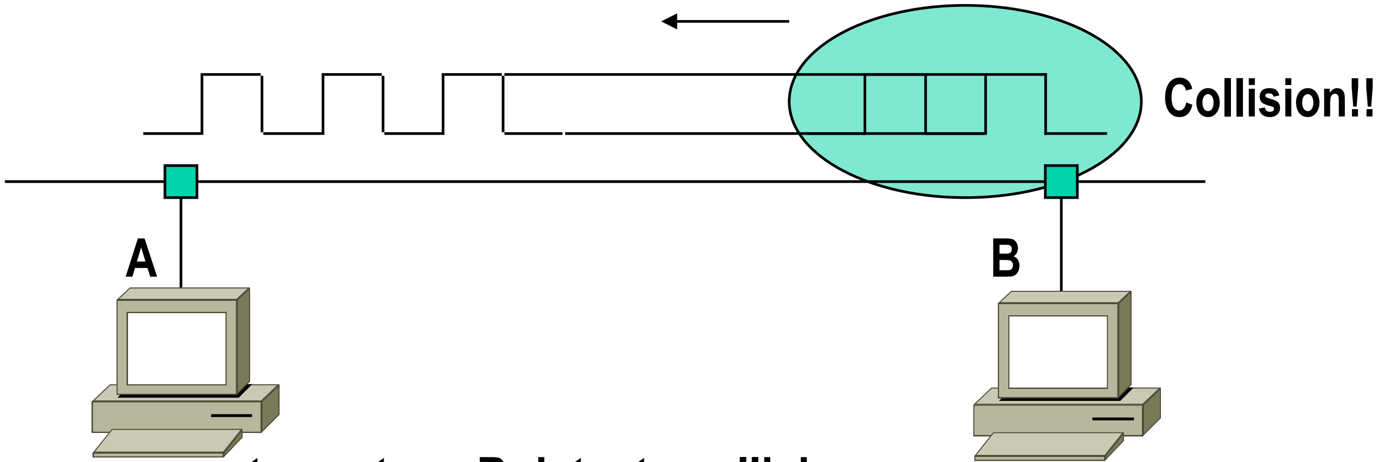


t = x ... A starts transmission

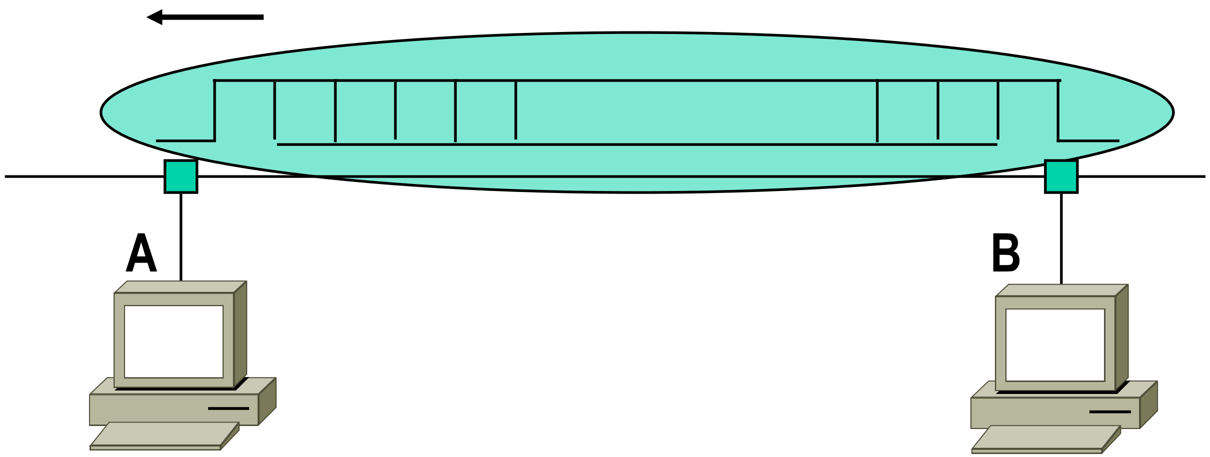


t = x + dt ... B starts transmission

Collision Window / Slot Time 2



t = x+ tp ... B detects collision
tp ... signal propagation time from A to B



t = x + 2tp ... A detects collision

Slot Time

- **Minimum frame length has to be defined in order to safely detect collisions**
- **Each frame sent must stay on wire for a RTT duration – at least**
- **This duration is called "slot time" and has been standardized to be 512 bit-times**
  - 51,2 µs for 10 Mbit/s
  - Hence minimal frame length is 64 byte

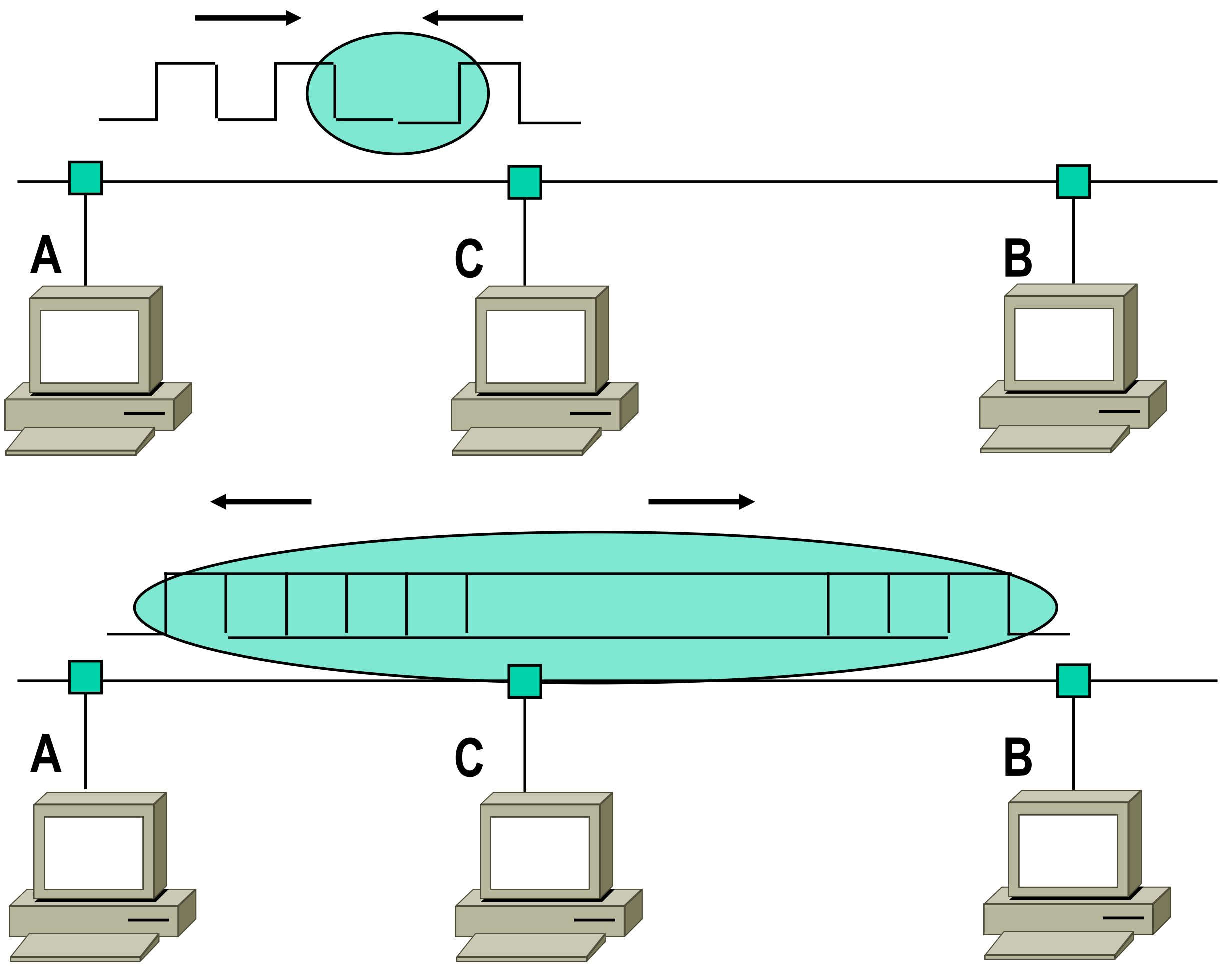
  - Note:
    - The request for fairness limits the maximum frame size, too
    - 1518 byte is the maximum allowed frame size

Slot Time Consequences

- **So minimum frame length is 512 bits (64 bytes)**
- **With signal speed of 0.6c and the delay caused by electronic circuits such as interface cards and repeaters the RTT of 512 bit times allows a network diameter of**
  - 2500 meters with 10 Mbit/s
  - 250 meters with 100 Mbit/s
  - 25 meters with 1000 Mbit/s (!)

NOTE: Only valid on shared media (!)

Collision Extended by JAM Signal !



Exponential Backoff

- **Most important idea of Ethernet !**
- **Provides maximal utilization of bandwidth**
  - After collision, set basic delay = slot time
  - Total delay = basic delay * random
  - 0 <= random < 2^k
    - k = min (number of transmission attempts, 10)
- **Allows channel utilization**
- **After 16 successive collisions**
  - Frame is discarded
  - Error message to higher layer
  - Next frame is processed, if any
- **Truncated Backoff (k<=10)**
  - 1024 potential "slots" for a station
  - Thus maximum 1024 stations allowed on half-duplex Ethernet

Channel Capture

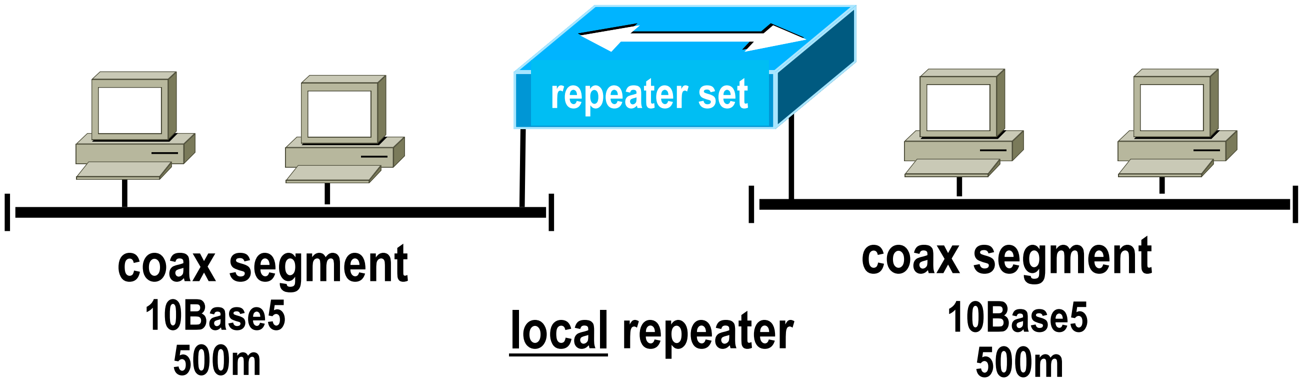
- Short-term unfairness on very high network loads
- Stations with lower collision counter tend to continue winning
- 10 times harder to occur on 100 Mbit/s Ethernet
- Rare phenomena, so no solution against it

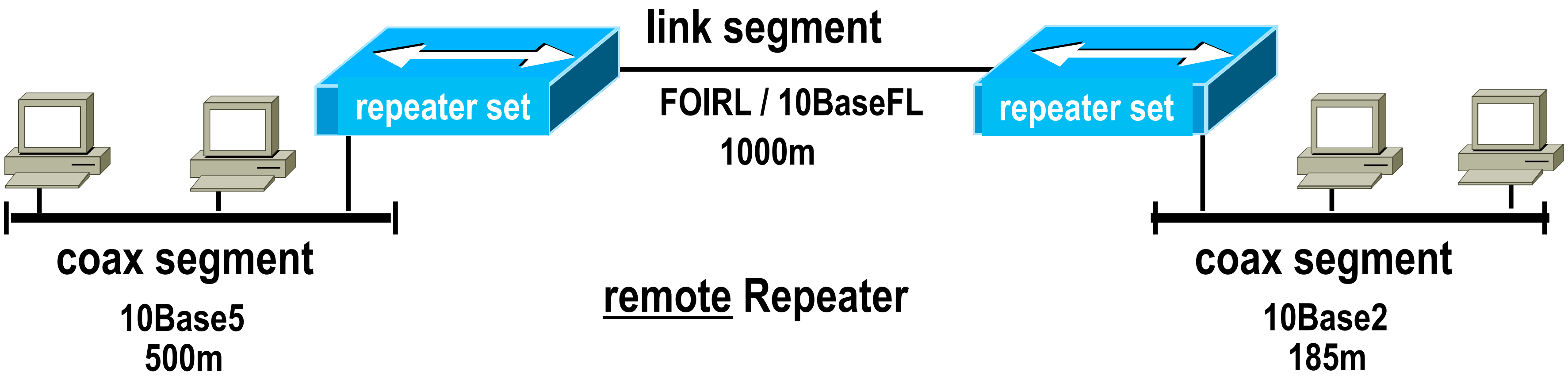
But would I choose
Ethernet for mission-
critical realtime
applications…?

Agenda

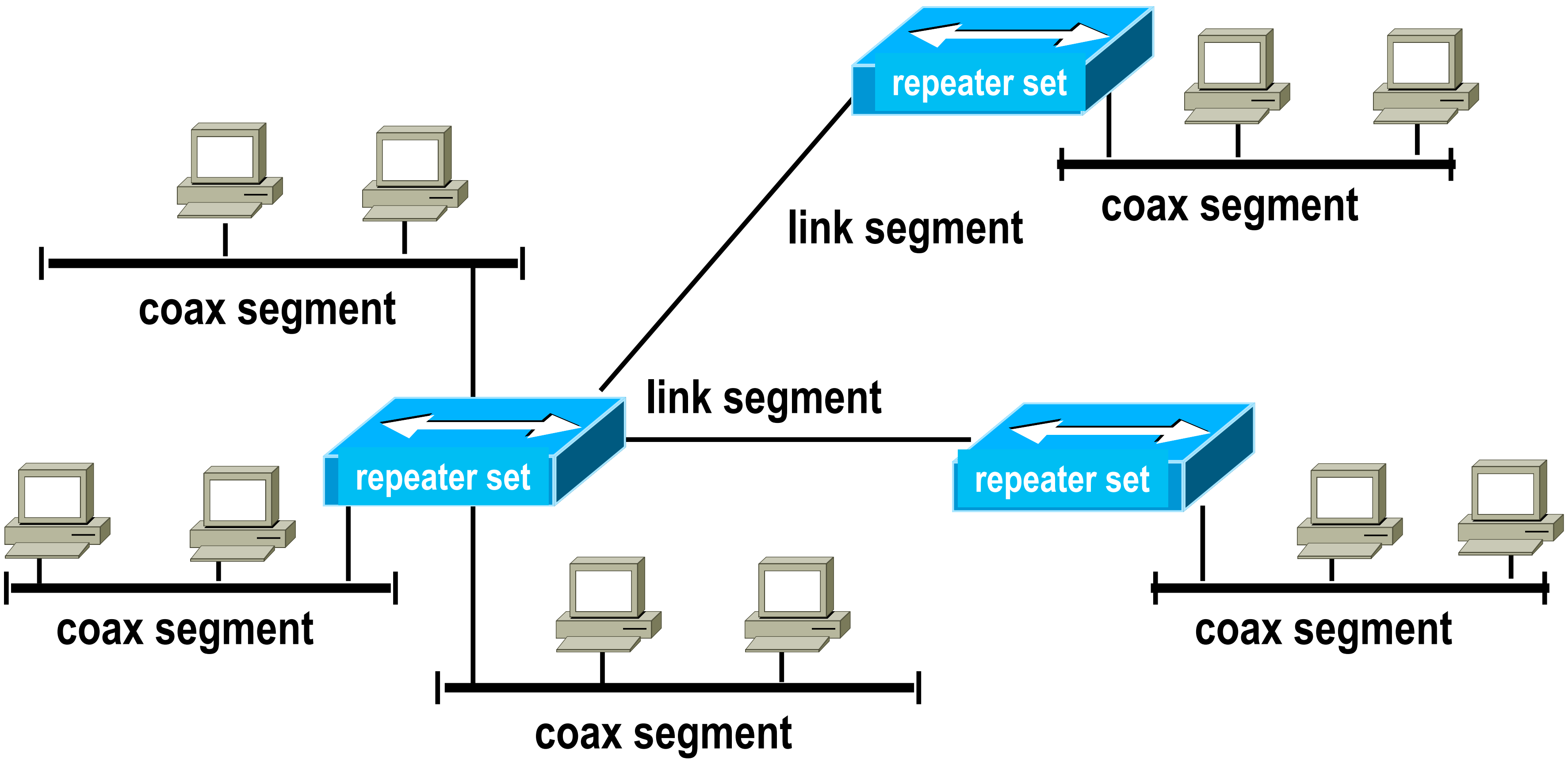
- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

Local / Remote Repeater

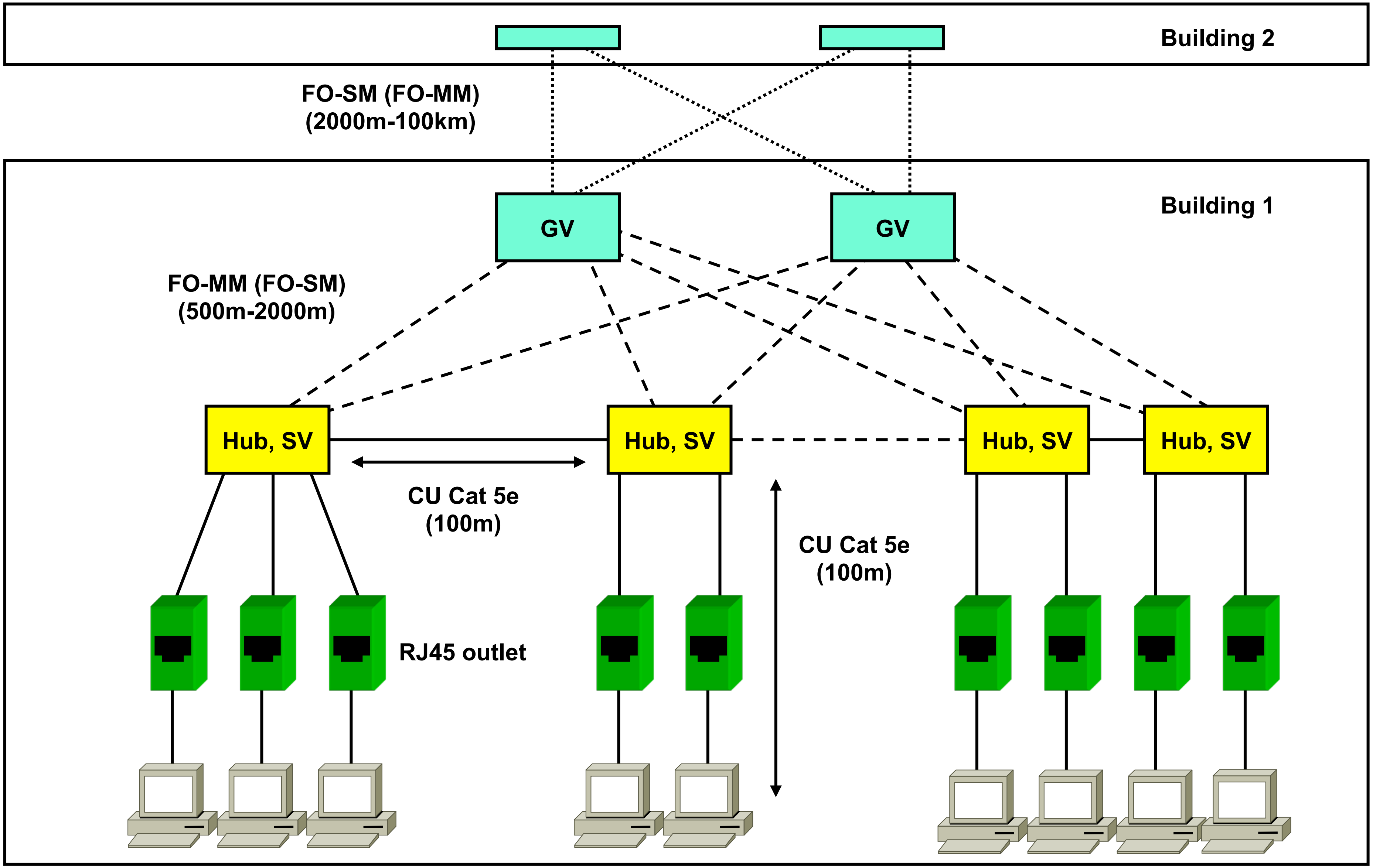




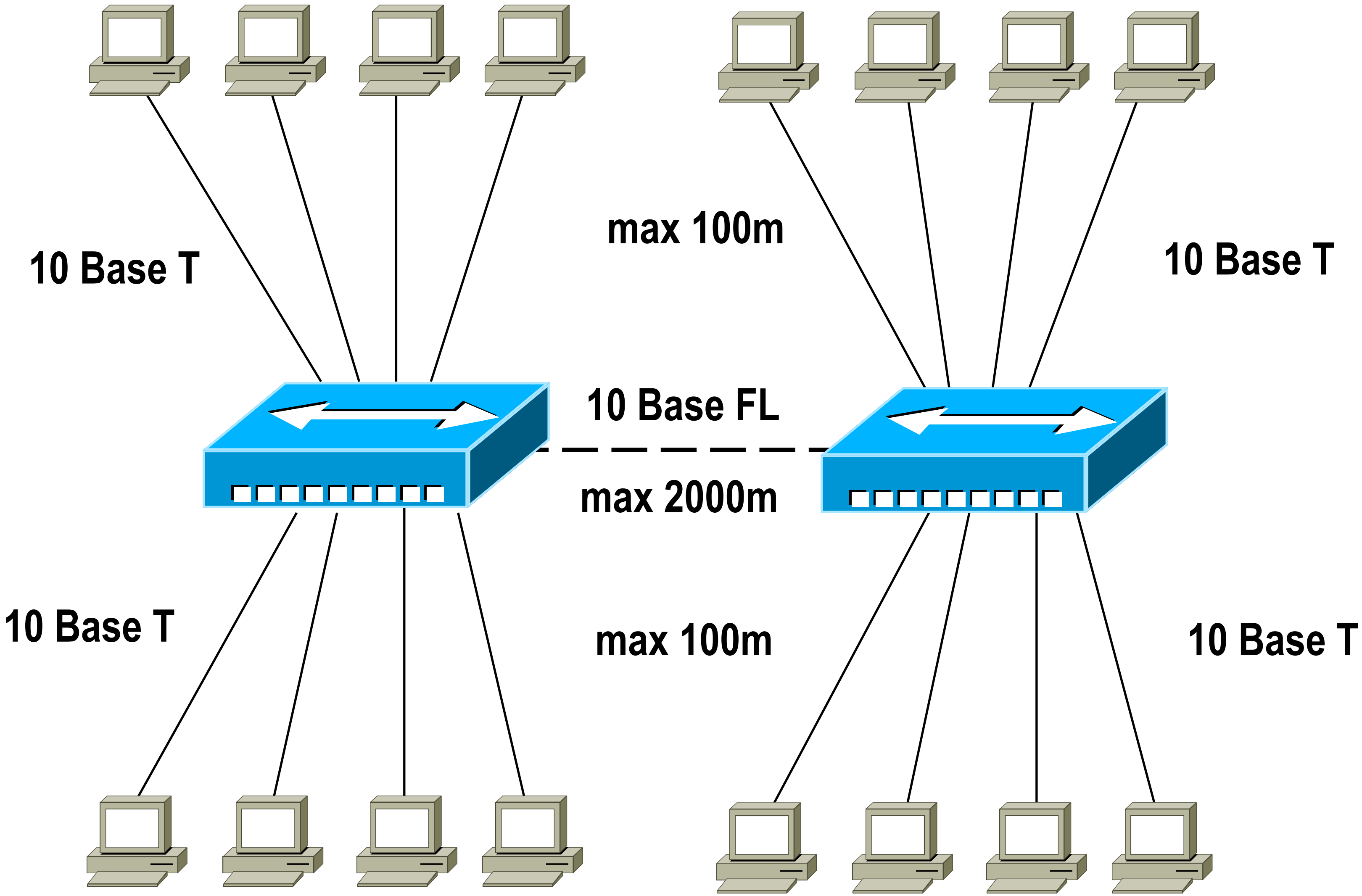
Multiport Repeater - One Collision Domain



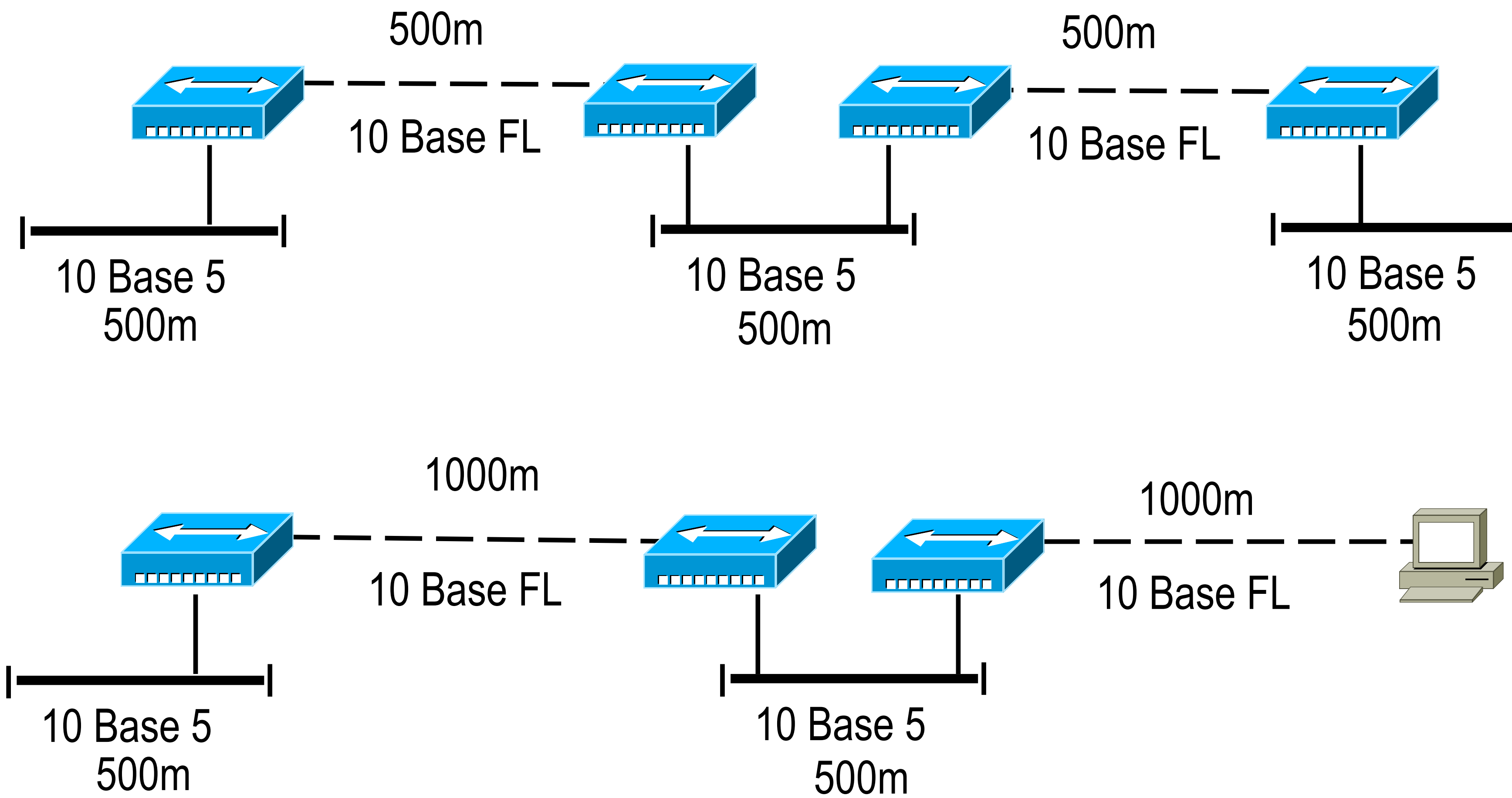
Structured Cabling (Building / Campus)



Multiport Repeater as „Hub“



Repeater-Rules

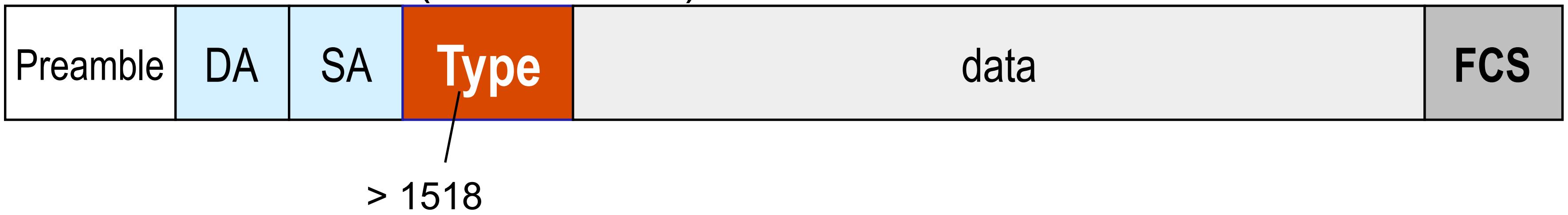


Agenda

- **Introduction**
- **IEEE 802**
- **Logical Link Control**
- **Ethernet**
  - Introduction
  - CSMA/CD
  - Elements and Basic Media-Types
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

Ethernet Version 2 Frame
(aka DIX Frame -> DEC, Intel, Xerox)

Ethernet Version 2 ("Ethernet II")

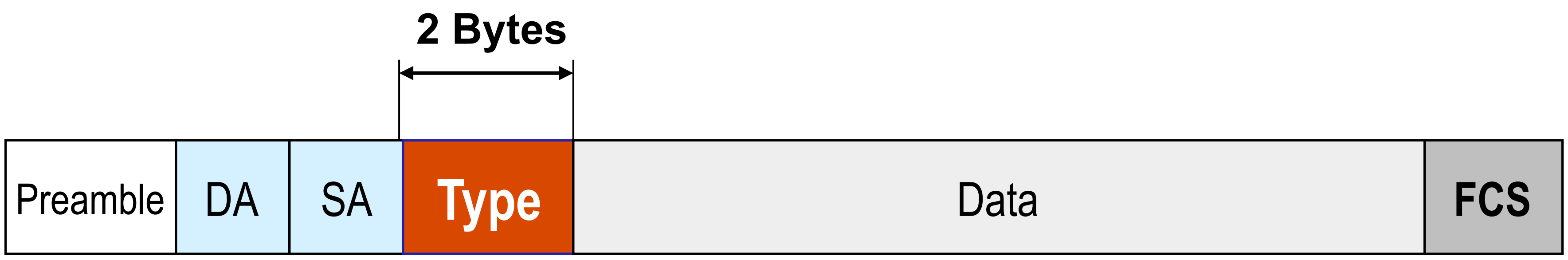


Preamble .... For clock synchronization (64 Bit)
(62 bits 10101.....01010 + 2 bits 11 as SD)

DA .... Destination MAC-Address (48 Bit)
SA .... Source MAC-Address (48 Bit)
Type .... Protocol-type field (16 Bit)
Data .... Payload
FCS .... Frame Check Sequence (32 Bit)
based on CRC (Cyclic Redundancy Check)

DIX Type Field

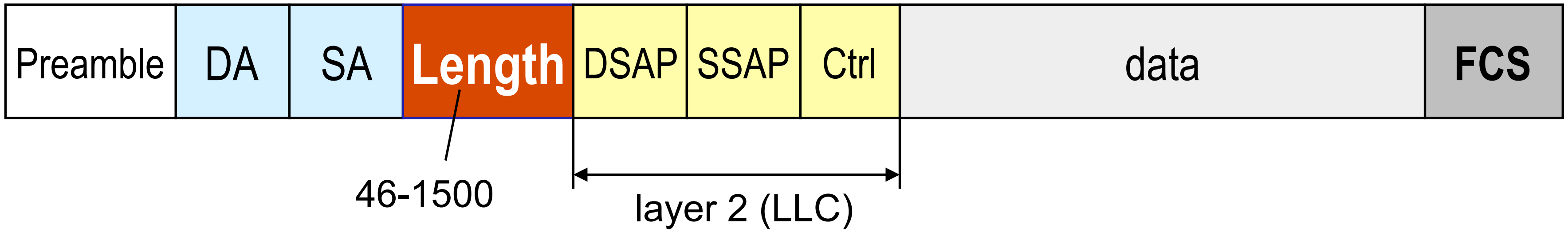
- **2-bytes Type field to identify payload (protocols carried)**
  - Most important: IP type 0x800
- **No length field**



"THE" Ethernet Frame

IEEE 802.3/802.2 Frame

802.3 with 802.2 (LLC)



Length field instead of Ev2 type field

Additional 802.2 LLC header for implementation of HDLC-like protocol procedures on LAN wire

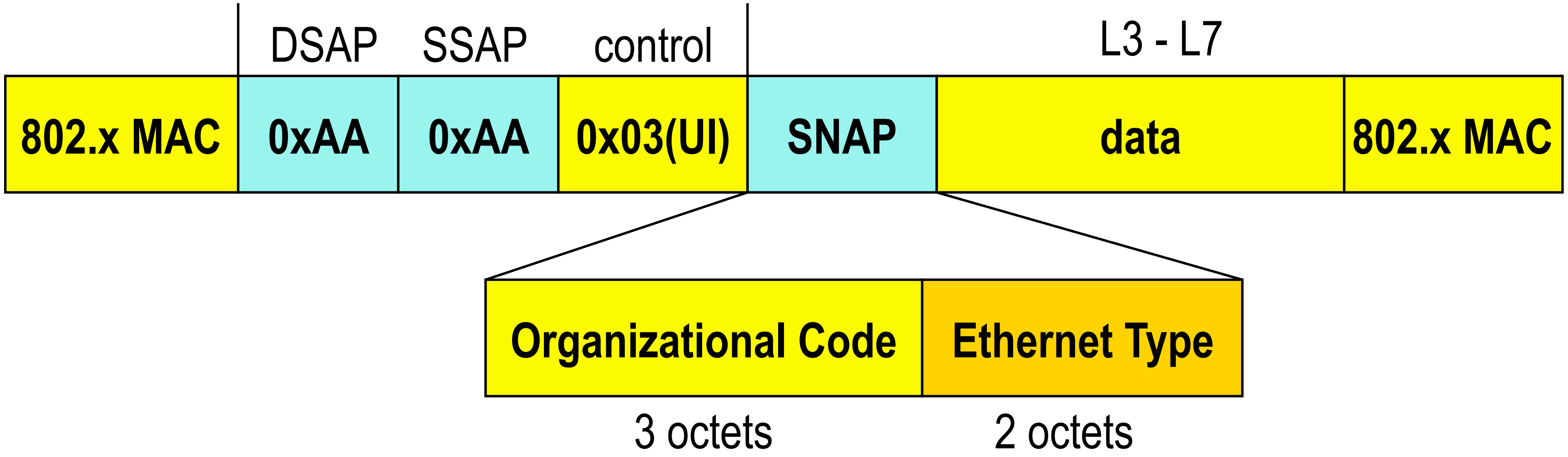
Length .... Of IEEE 802.3 frame (16 Bit)
= bytes following without FCS (46-1500)

LLC …………….Logical Link Control (HDLC for LAN)
DSAP (Destination Service Access Point) 8 Bit
SSAP (Source Service Access Point) 8 Bit
Ctrl (Control) (8 or 16 Bit)

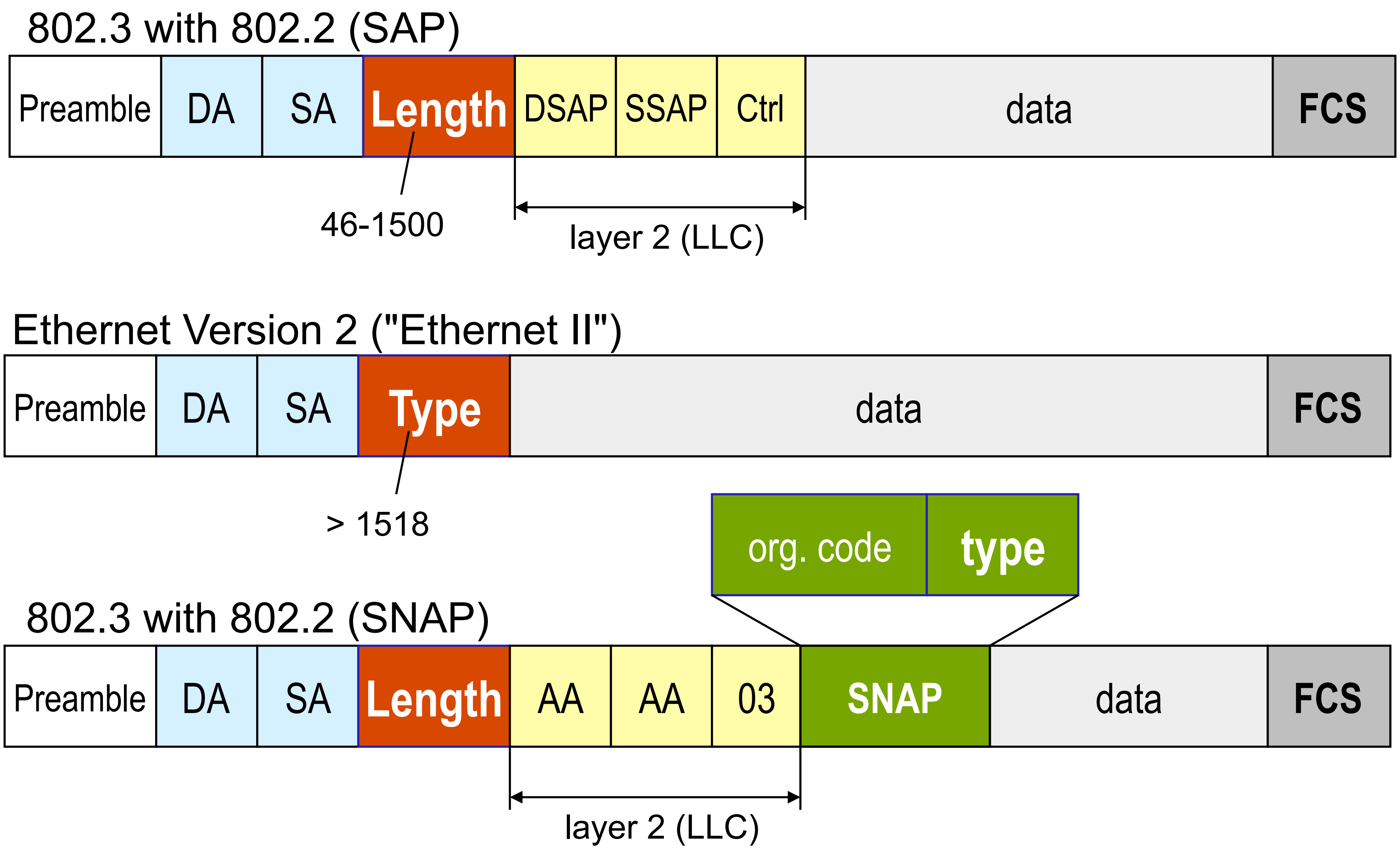
- **Ethernet II and 802.3 can coexist on the same cable, but each associated sending and receiving station must use the same format.**
- **Fortunately all type-field values are larger than 1518 (max** frame **length), so any incoming frame can be recognized and handled properly.**

SNAP Frame

- **Demand for carrying type-field in 802.4, 802.5, 802.6, ... also !**
  - Convergence protocol was needed to transport Ethernet V2 type information over IEEE LANs -> SNAP
- **Subnetwork Access Protocol (SNAP) header introduced**
  - If DSAP=SSAP=0xAA and Ctrl=0x03
  - then a 5 byte SNAP header follows containing 3 bytes organizational code plus 2 byte DIX type field



Frame Types Summary



Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **Bridging versus Routing**

What is Bridging?

- **Packet switching principle in connectionless mode applied to layer 2**
  - The already well known store and forward principle of WAN world (OSI layer 3 intermediate system) was taken by the LAN community

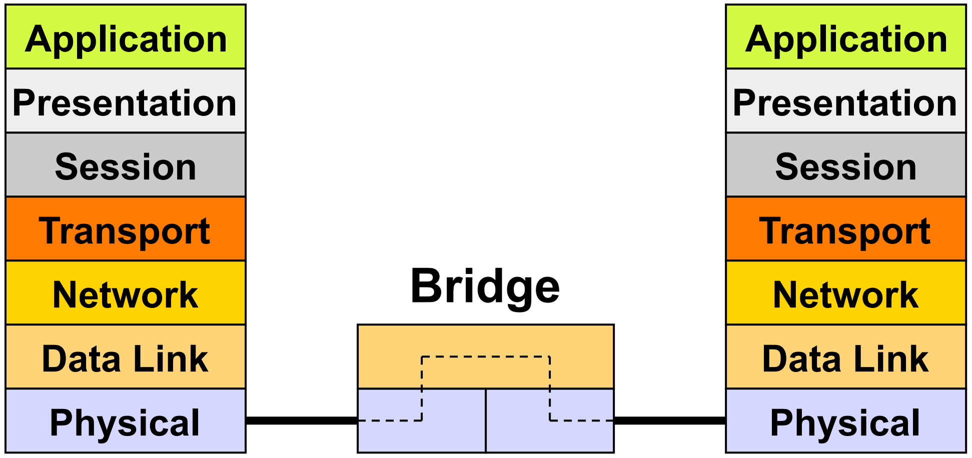
- **Adapted to work with MAC addresses**
  - Instead of unique and structured OSI layer 3 (routable) addresses we have only unique and unstructured OSI Layer 2 (MAC) addresses

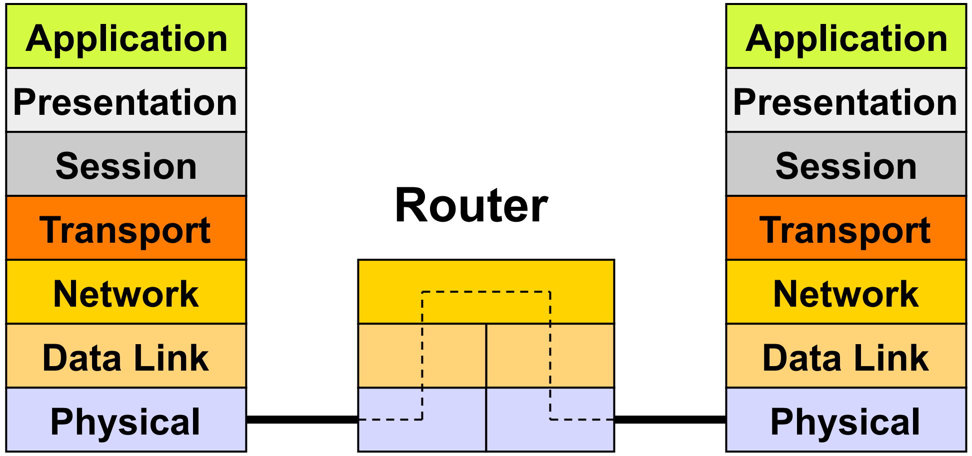
- **The bridging table or MAC address table**
  - Is used for forwarding decisions in the same way as a routing table already outline in chapter “Network Principles”
  - Signposts to reach a given MAC address by pointing to the corresponding physical port
    - MAC address -> Port mapping

Why Packet Switching on LAN?

- **LAN was originally designed for shared media**
  - But too many clients cause performance problems
    - Higher probability for collisions in case of Ethernet
- **Bridge separates two (or more) shared-media LAN segments**
  - Only frames destined to the other LAN segment are forwarded, frames destined to own LAN segment are not forwarded
  - Number of collisions reduced (!)
- **Different bridging principles**
  - Ethernet: Transparent Bridging
  - Token Ring: Source Route Bridging

OSI Comparison





- **Bridging is**
  - Connectionless packet switching on OSI layer 2 using unique but unstructured MAC addresses without any topology information
  - L2 Signposts in the MAC address table
- **Routing is**
  - Connectionless packet switching on OSI layer 3 using unique and structured addresses which contain topology information
  - L3 Signposts in the routing table

Bridging versus Routing

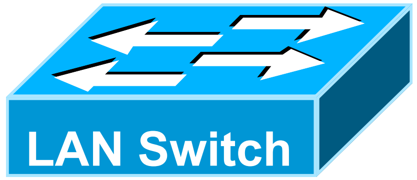
- **Bridging works on OSI layer 2**
  - Forwarding of frames
  - Use MAC addresses only
  - Termination of physical layer (!)
  - Invisible for end-systems on a bridged LAN
- **Routing works on OSI layer 3**
  - Forwarding of packets
  - Use routable addresses only (e.g. IP)
  - Termination of both layer 1 and 2
  - Visible for end-systems (e.g. default router in IP)

Bridge History

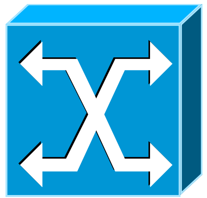
- **Bridges came after routers!**
- **First bridge designed by Radia Perlman**
  - Ethernet has size limitations
  - Routers were single protocol and expensive
- **STP (Spanning Tree Protocol)**
  - Is an important part of any bridged network
  - Ethernet has no hop count (or IP time-to-live field) to implement a kill mechanism in case of loops
- **IEEE 802.1D contains**
  - Transparent bridging and STP

What is an Ethernet Switch?

- **A switch *is* basically a bridge, differences are only:**
  - Faster because implemented in HW
  - Multiple ports
  - Improved functionality (e.g. VLAN)

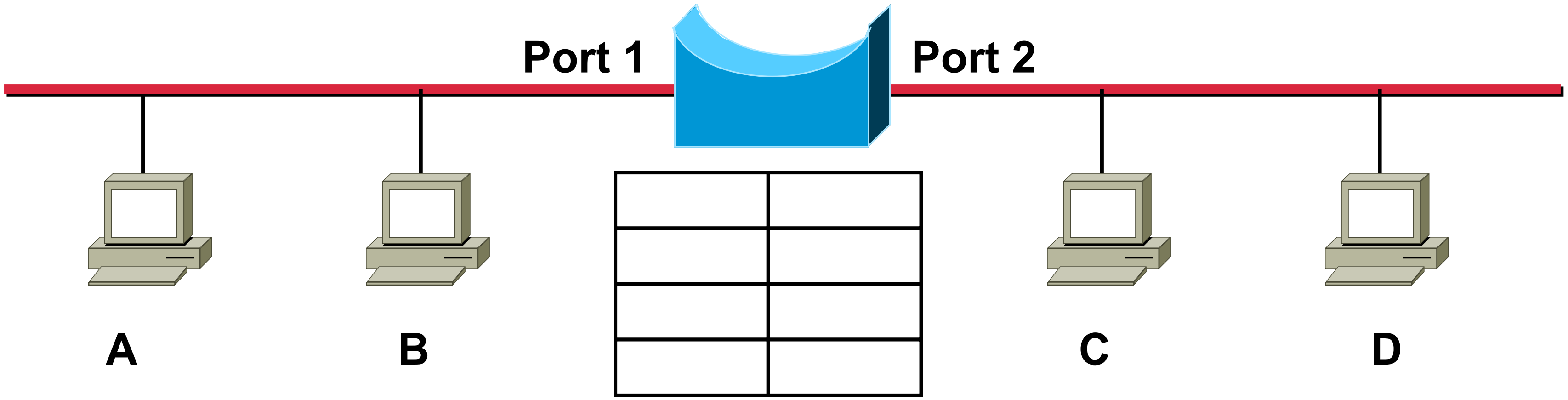


- **Don't confuse it with WAN Switching!**
  - Completely different !
  - Connection oriented (stateful) VCs



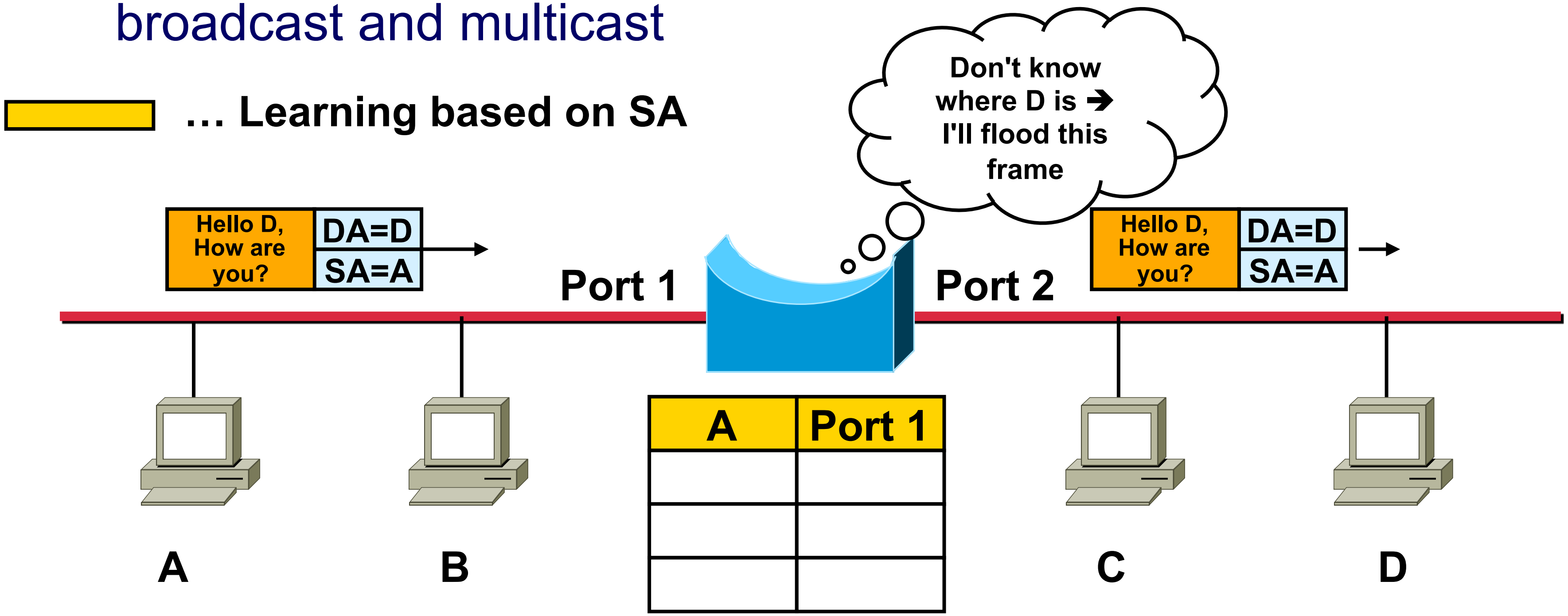
Transparent Bridging

- **Designed for "plug & play"**
- **Upon startup a bridge knows nothing**
  - MAC address table is empty
    - Exceptional case: static entries are configured by the network administrator, but that is hard work
- **Bridge is in learning mode**
  - Dynamic entries are built on the fly



Learning

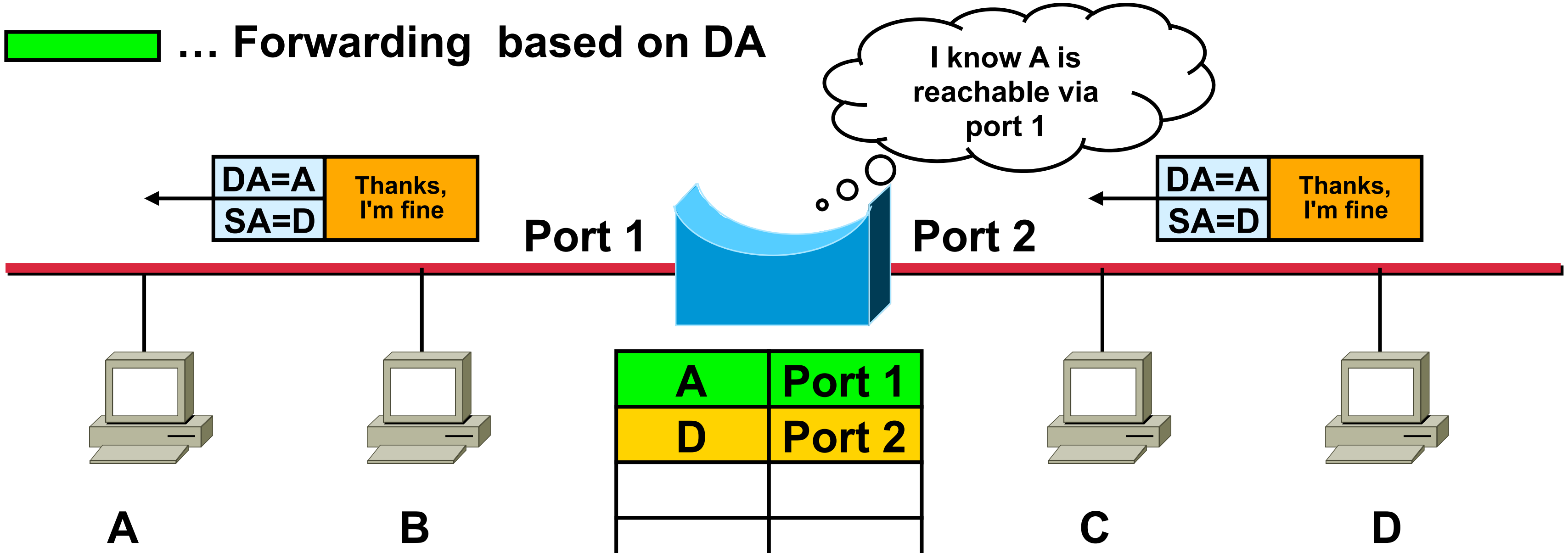
- **Once stations send frames the bridge notices the source MAC address**
  - Entered in bridging table
- **Frames for unknown destinations are flooded**
  - Forwarded on all ports. Same rule applies to Ethernet broadcast and multicast



A	Port 1

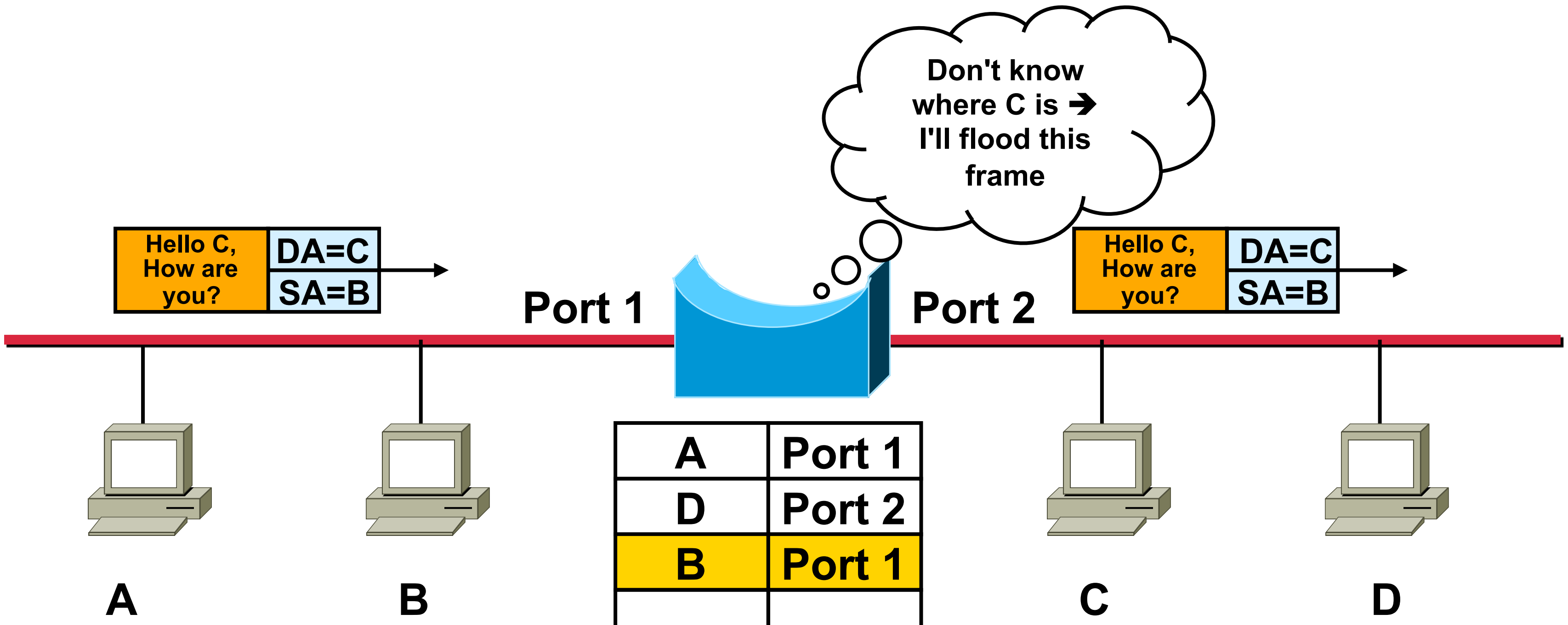
Learning ➔ Table Filling (1)

- **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

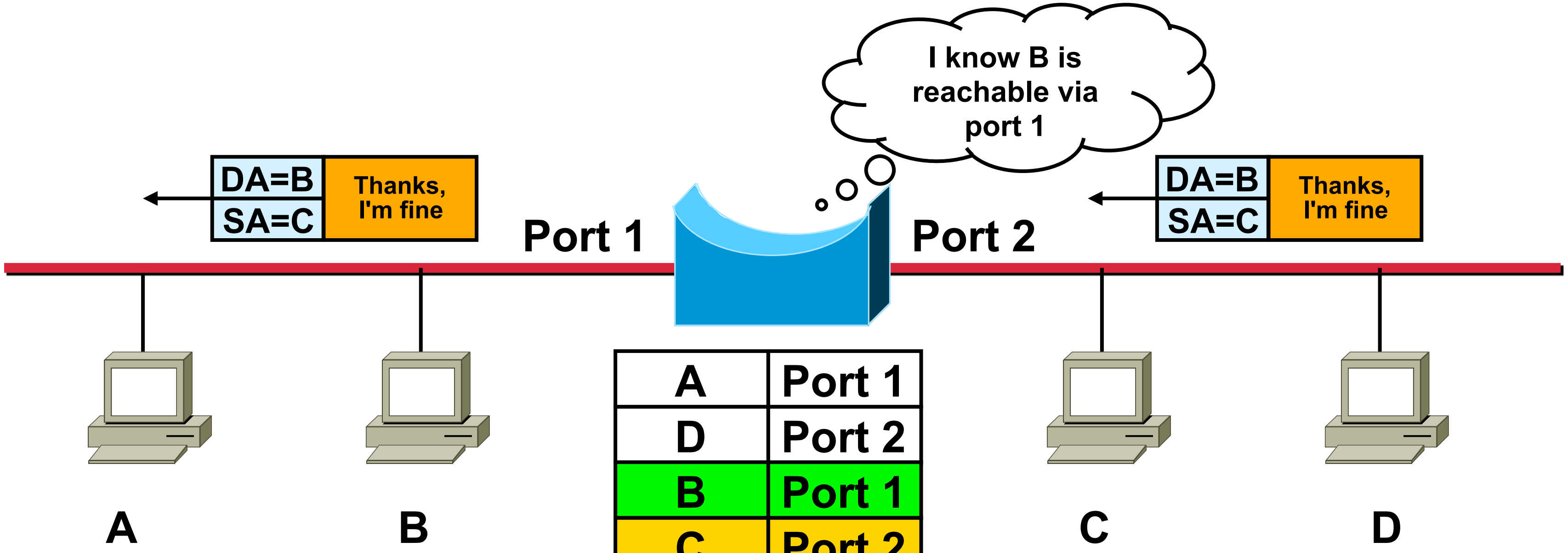
Table Filling (2)



A	Port 1
D	Port 2
B	Port 1

Table Filling (3)

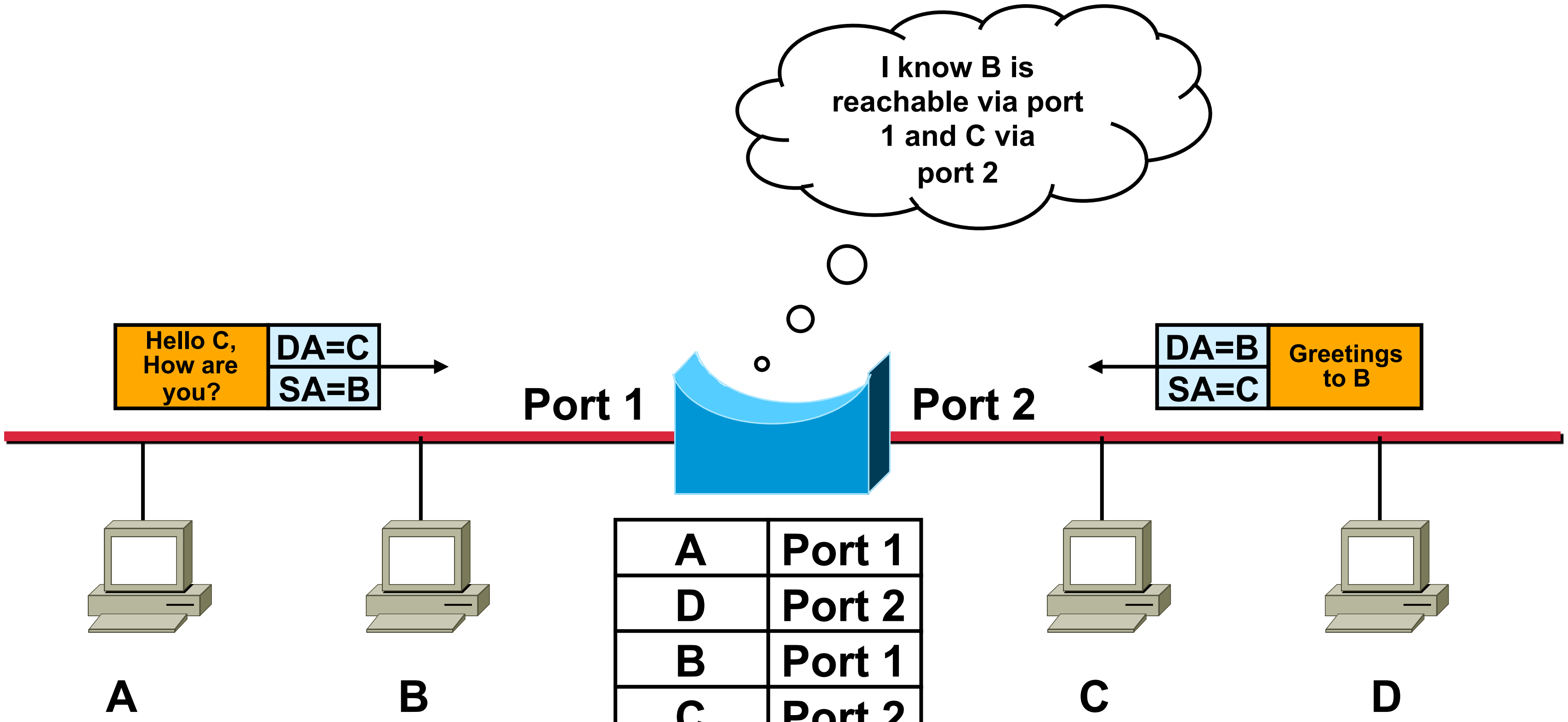
- **After some time the location of every station is known – simply by listening!**
- **Now only forwarding and filtering of frames**
  - Based on destination address



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

Table Filling – Forwarding

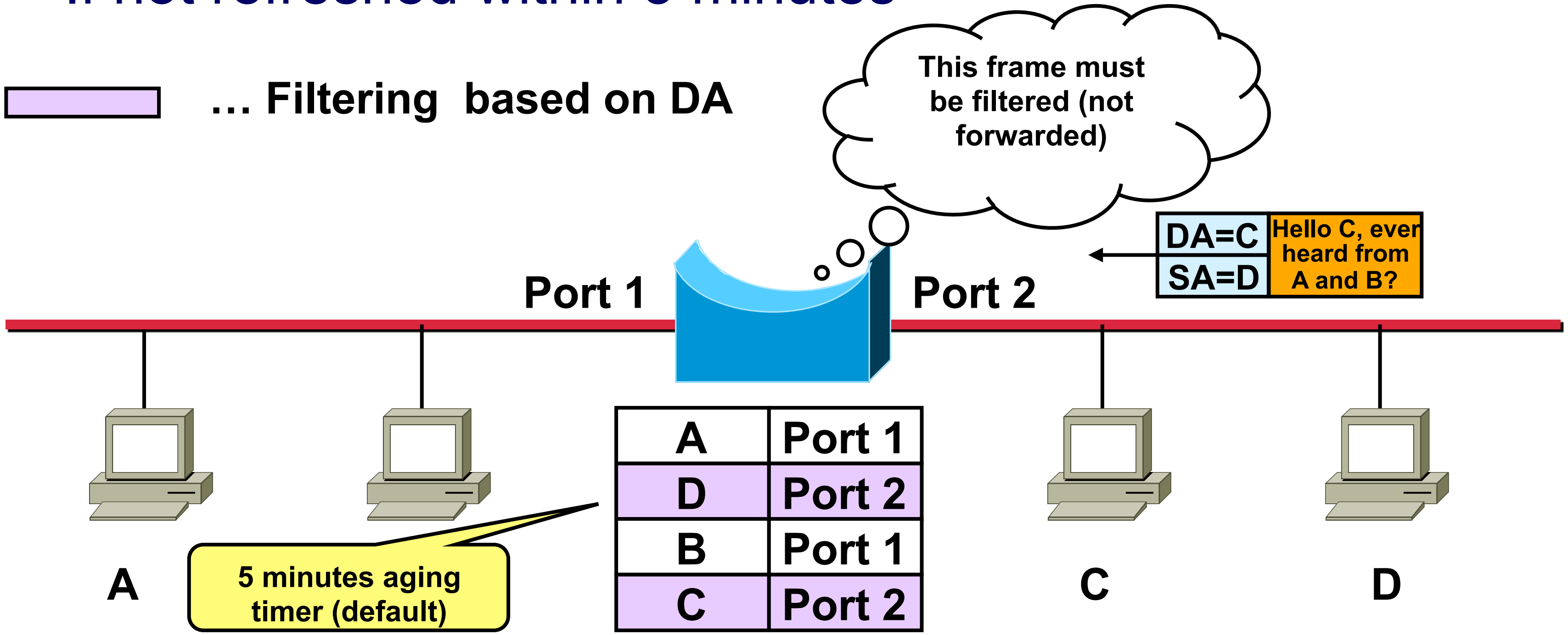
- **Collision domains are separated**
  - Frames can travel in their LAN segments at the same time



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

Table Filled – Filtering

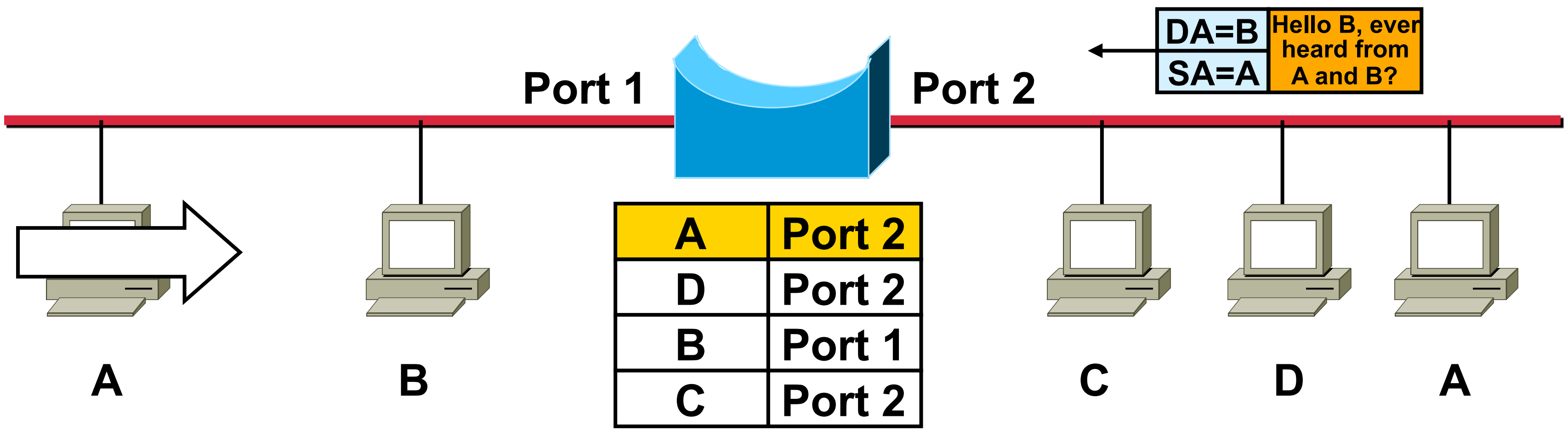
- **Frames whose source and destination address are reachable over the same bridge port are filtered**
- **Entries times out**
  - If not refreshed within 5 minutes



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

Last Seen – Last Win

- **Now assume notebook with MAC A is moved**
- **Address is immediately relearned**
  – With the first frame containing source MAC A on the other port
- **Imagine the problem**
  – If there are duplicated MAC address in the LAN !!!

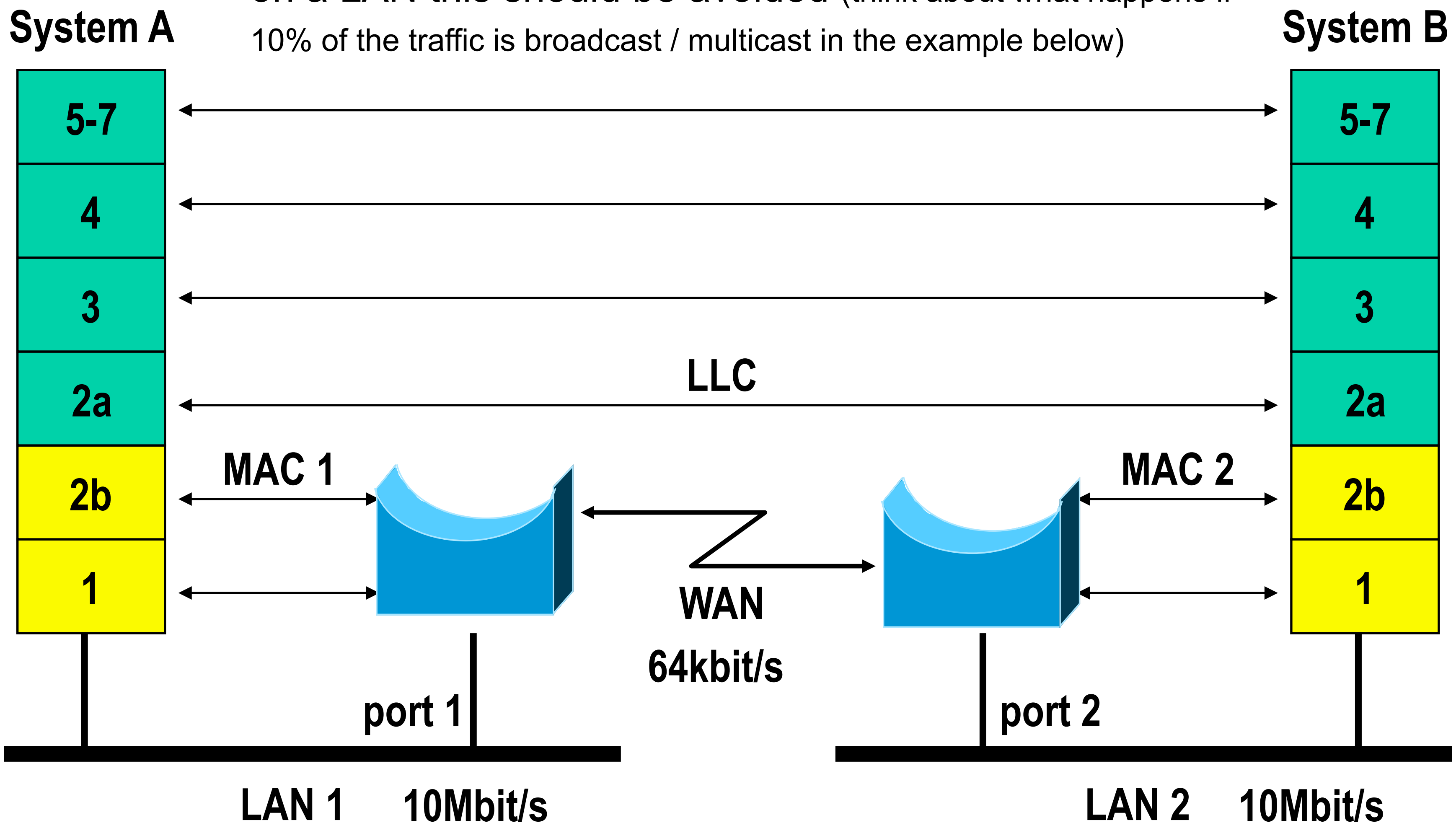


Most Important !

- **Bridge separates LAN into multiple collision domains**
- **A bridged network is still one broadcast domain**
  - L2 broadcast and L2 multicast frames are always flooded
- **A switched network works the same way as a bridged network**
  - Ethernet switch instead good old bridge
- **A router separates the whole LAN into multiple broadcast domains**
  - L2 broadcast are therefore limited to a location and does not spread over the whole network

Remote Bridging ? (!!! TB means Broadcast Domain!!)

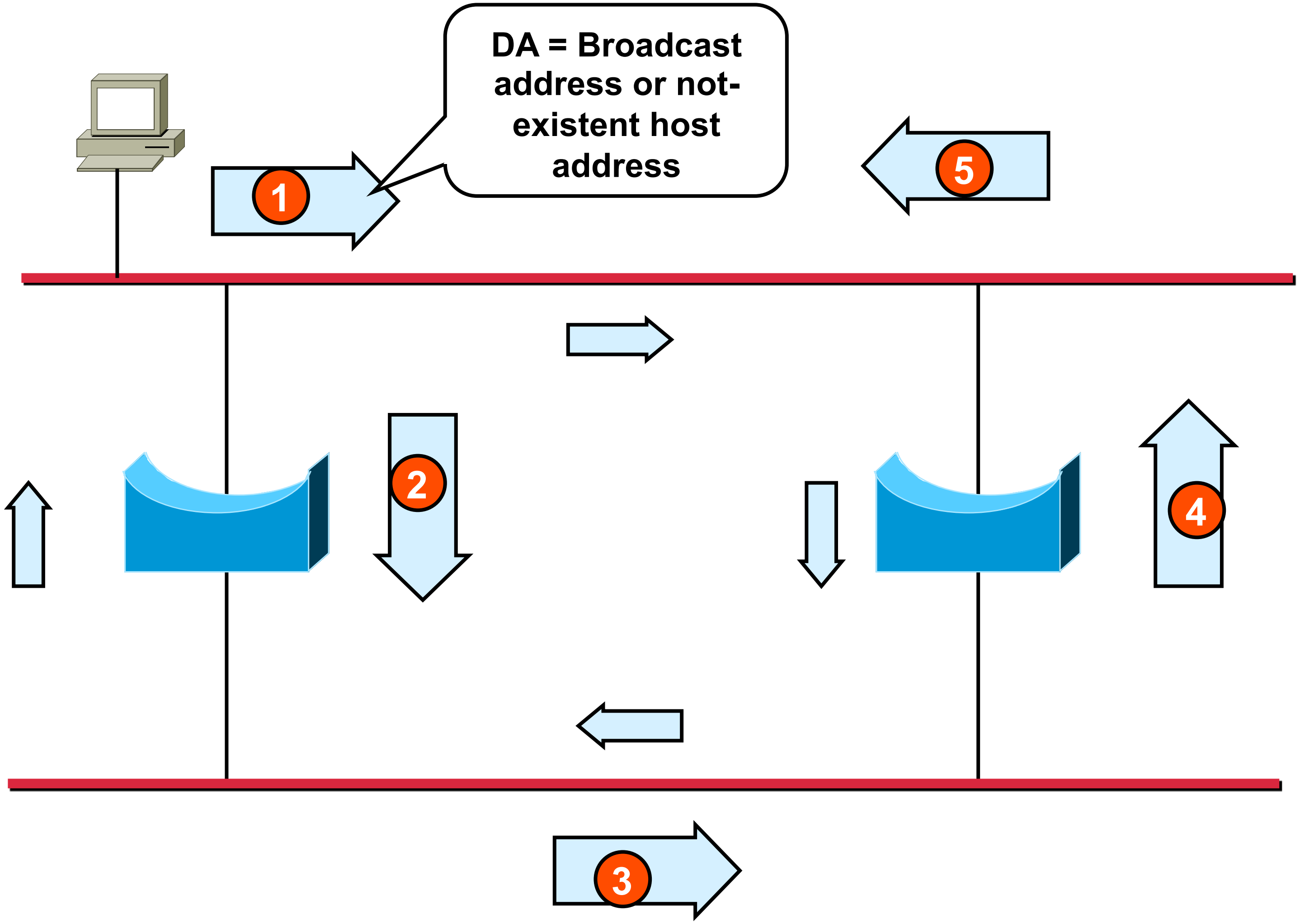
Because of inherent L2 broadcast / multicast percentage on a LAN this should be avoided (think about what happens if 10% of the traffic is broadcast / multicast in the example below)



Bridging Problems

- **Redundant paths lead to**
  - Endless cycling of frames
  - Continuous table rewriting
  - Blocking of buffer-resources
  - Stagnation of the LAN
  - Broadcast storms
- **To eliminate these unwanted effects**
  - Spanning Tree Protocol (STP) is necessary
- **No load sharing possible and no ability to select best path**
  - It is just bridging and not routing

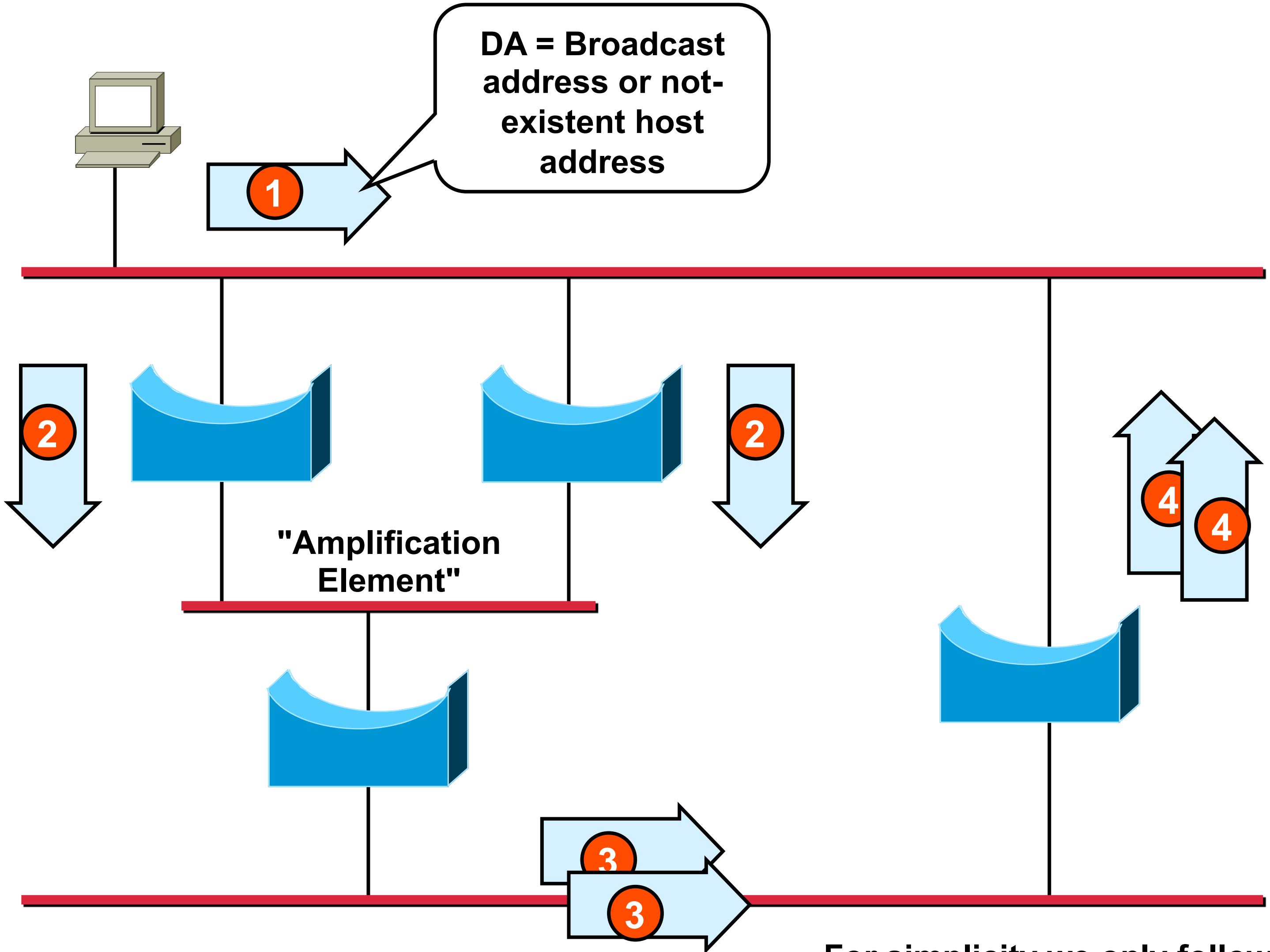
Endless Circling



Endless circling following the other path

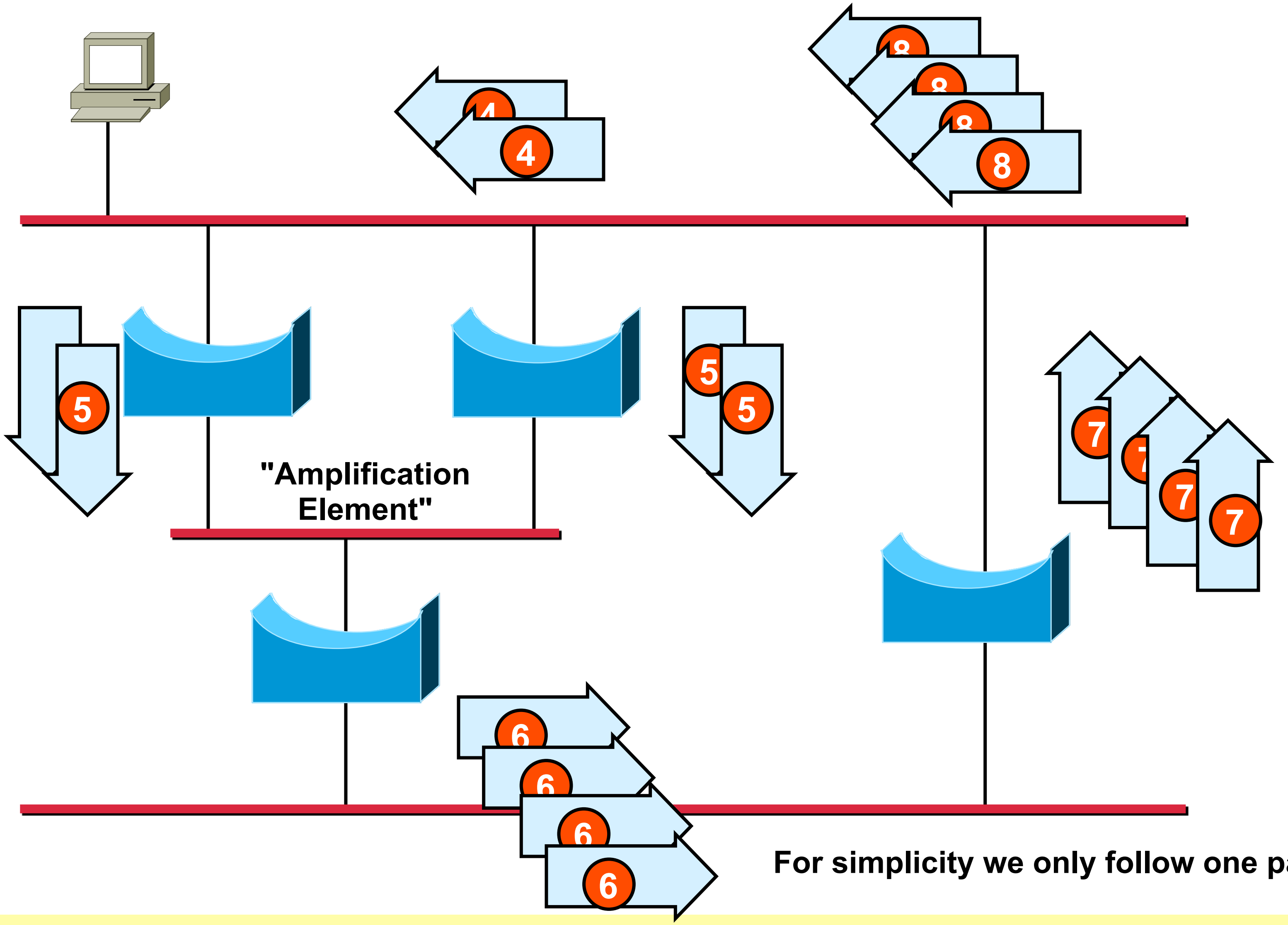
For simplicity we only follow one path

Broadcast Storm (1)



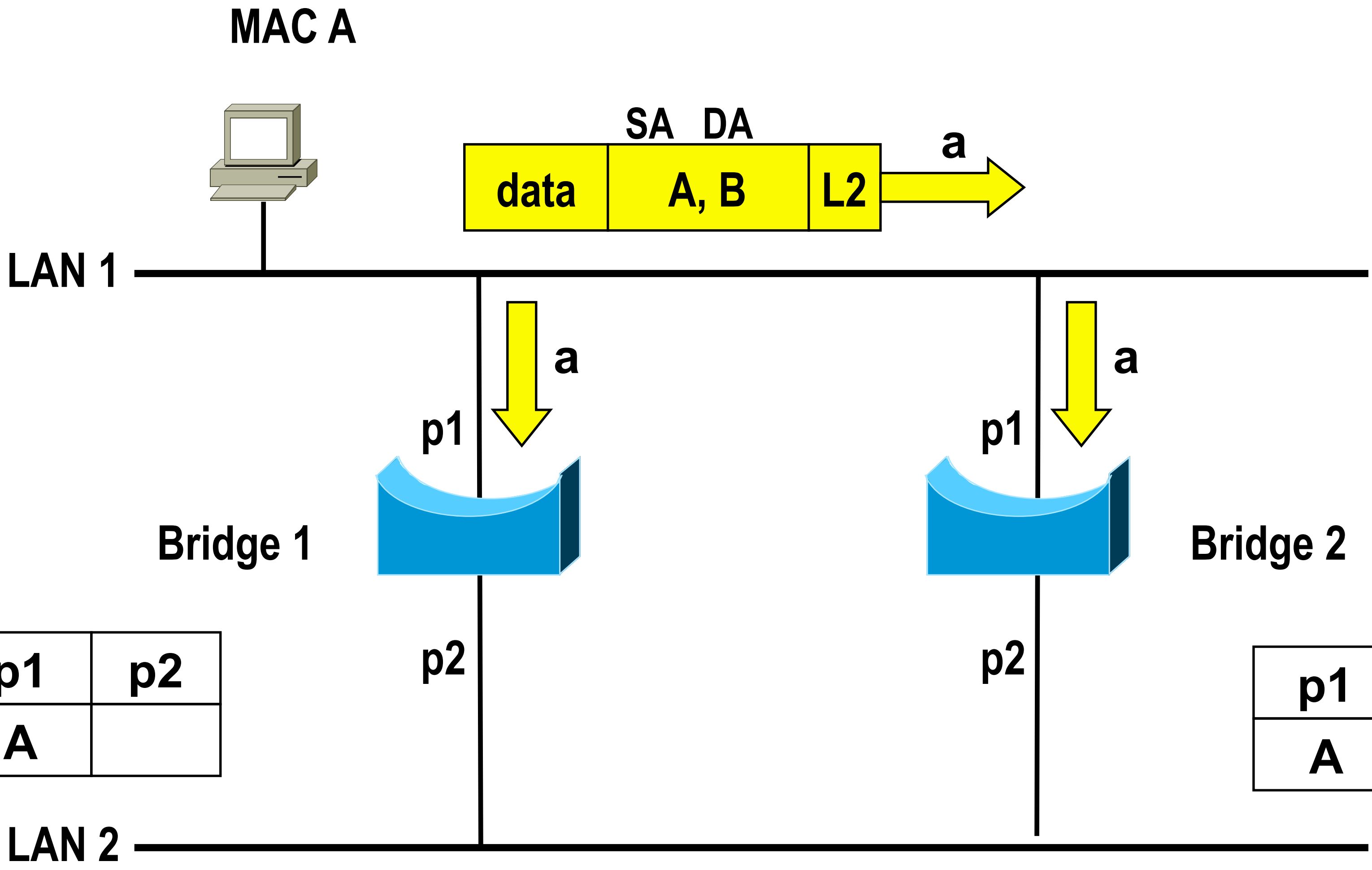
For simplicity we only follow one path

Broadcast Storm (2)



For simplicity we only follow one path

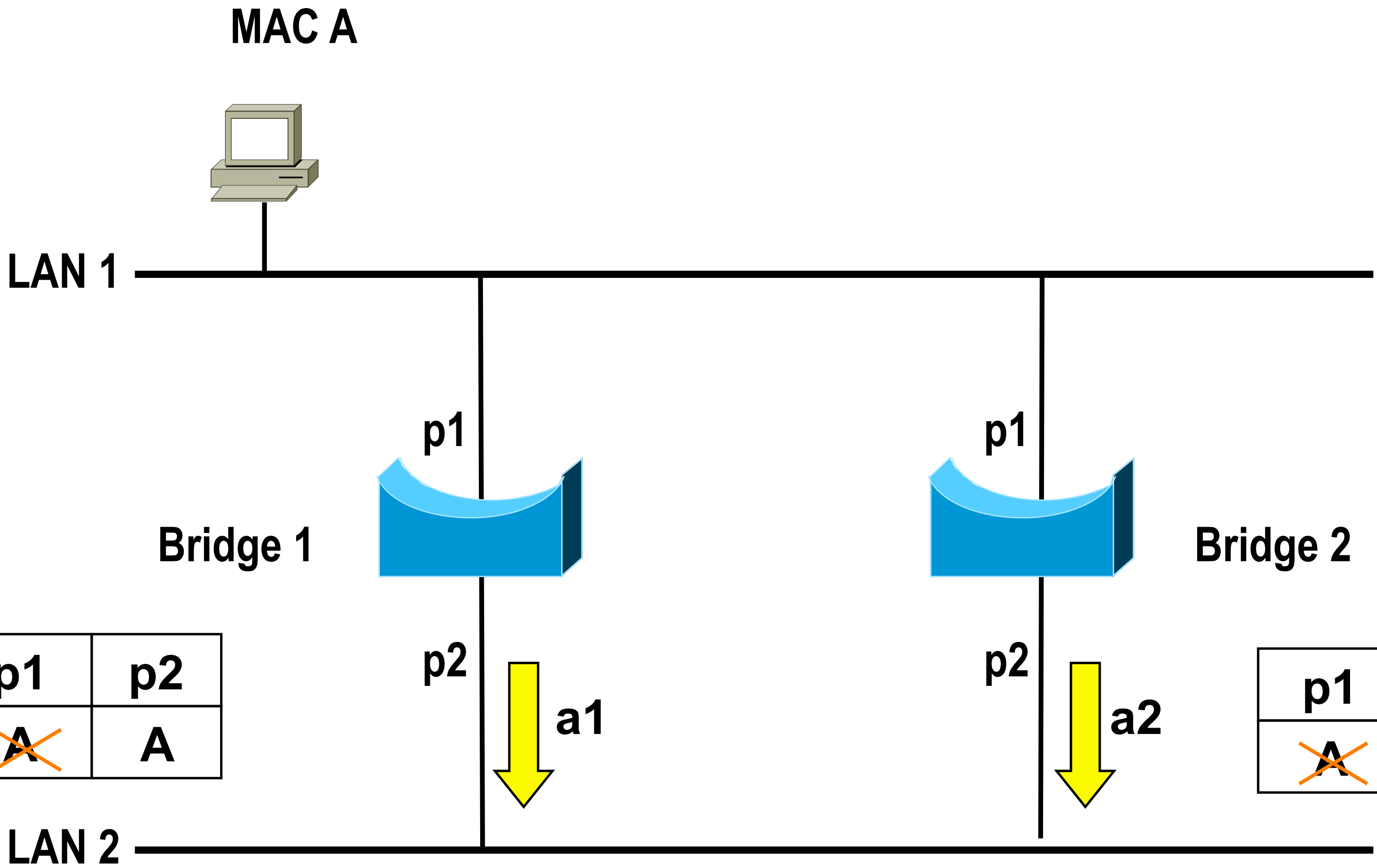
Table Rewriting (Unknown Destination) 1



p1	p2
A	

p1	p2
A	

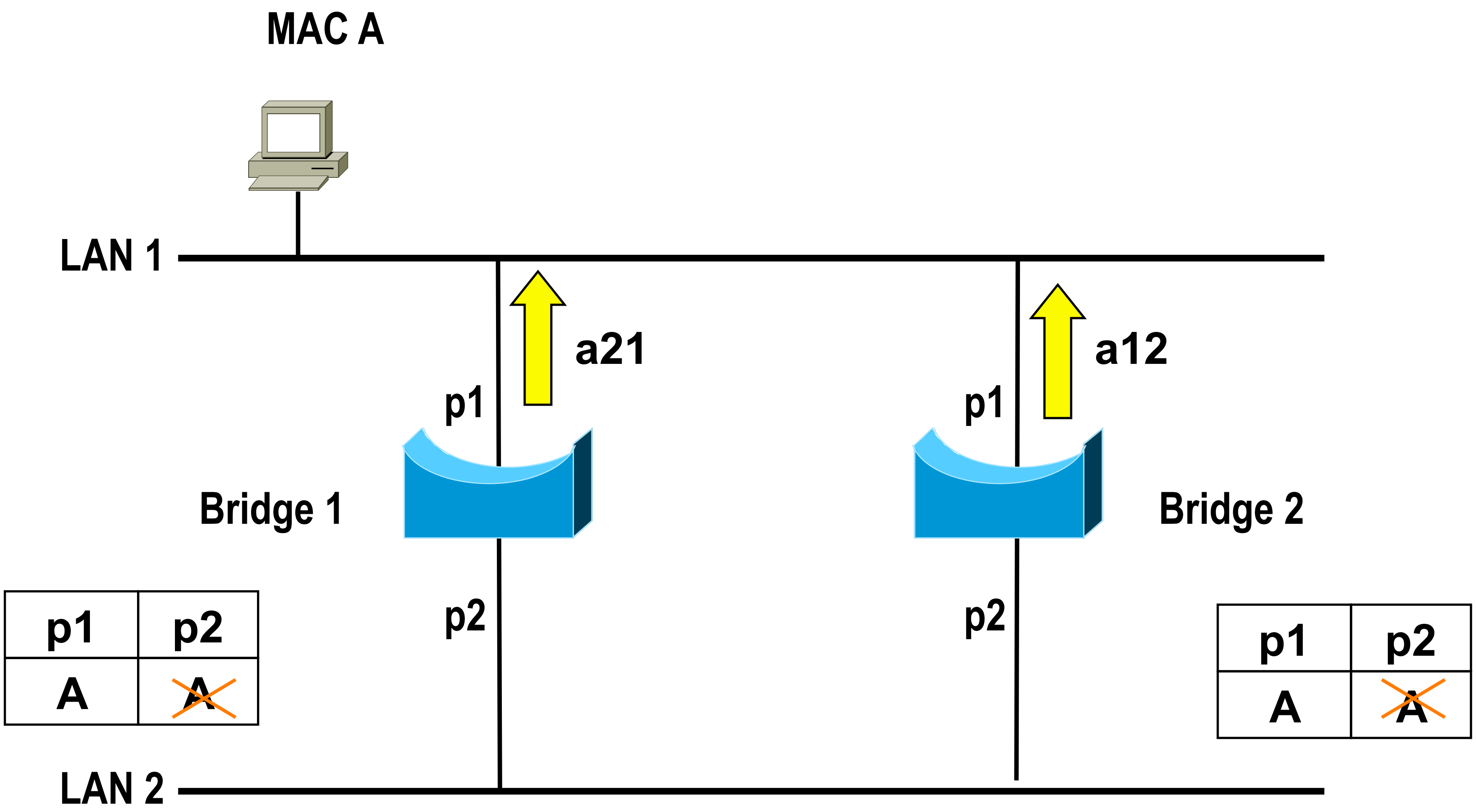
Table Rewriting (Unknown Destination) 2



p1	p2
~~A~~	A

p1	p2
~~A~~	A

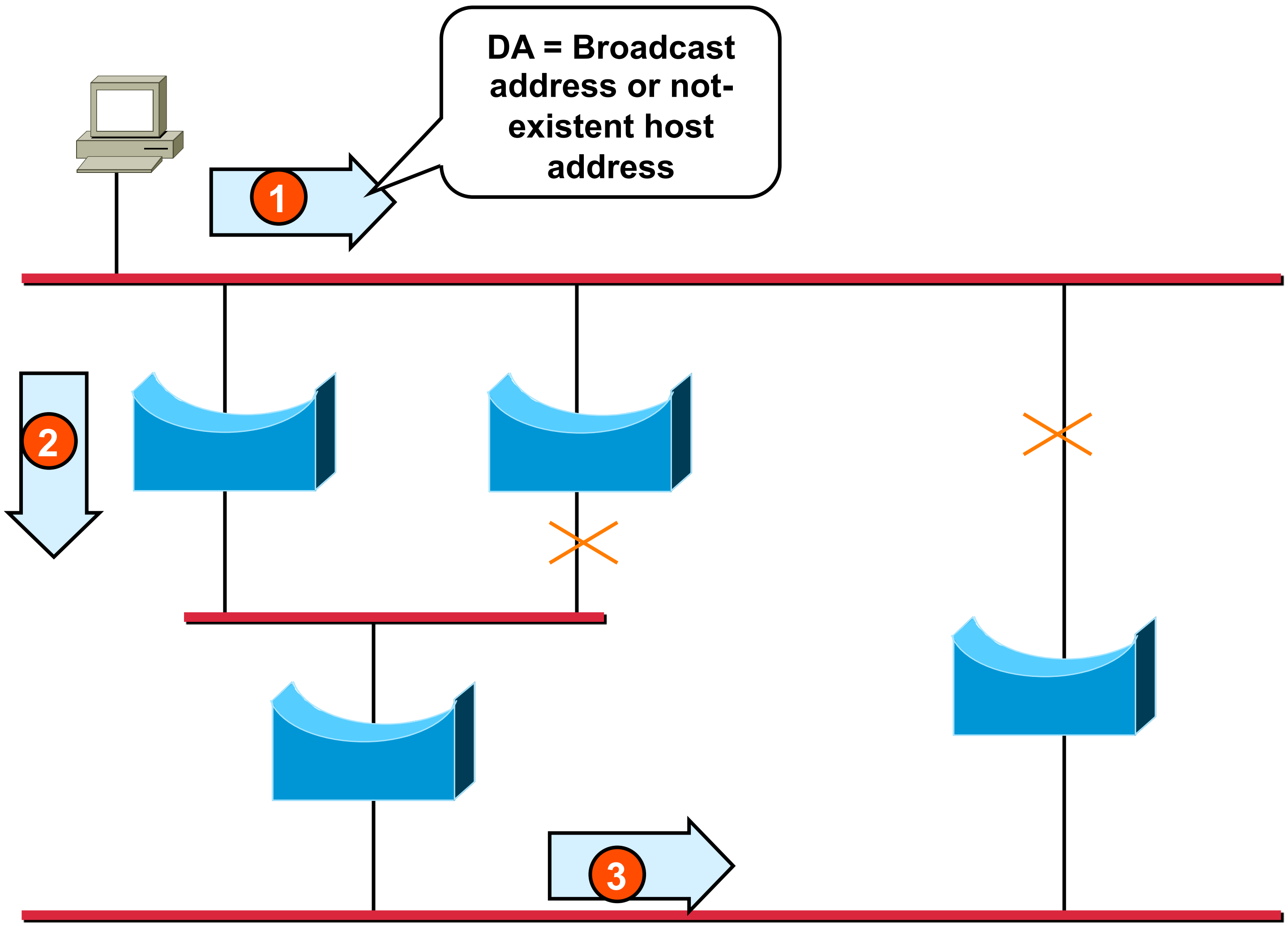
Table Rewriting (Unknown Destination) 3



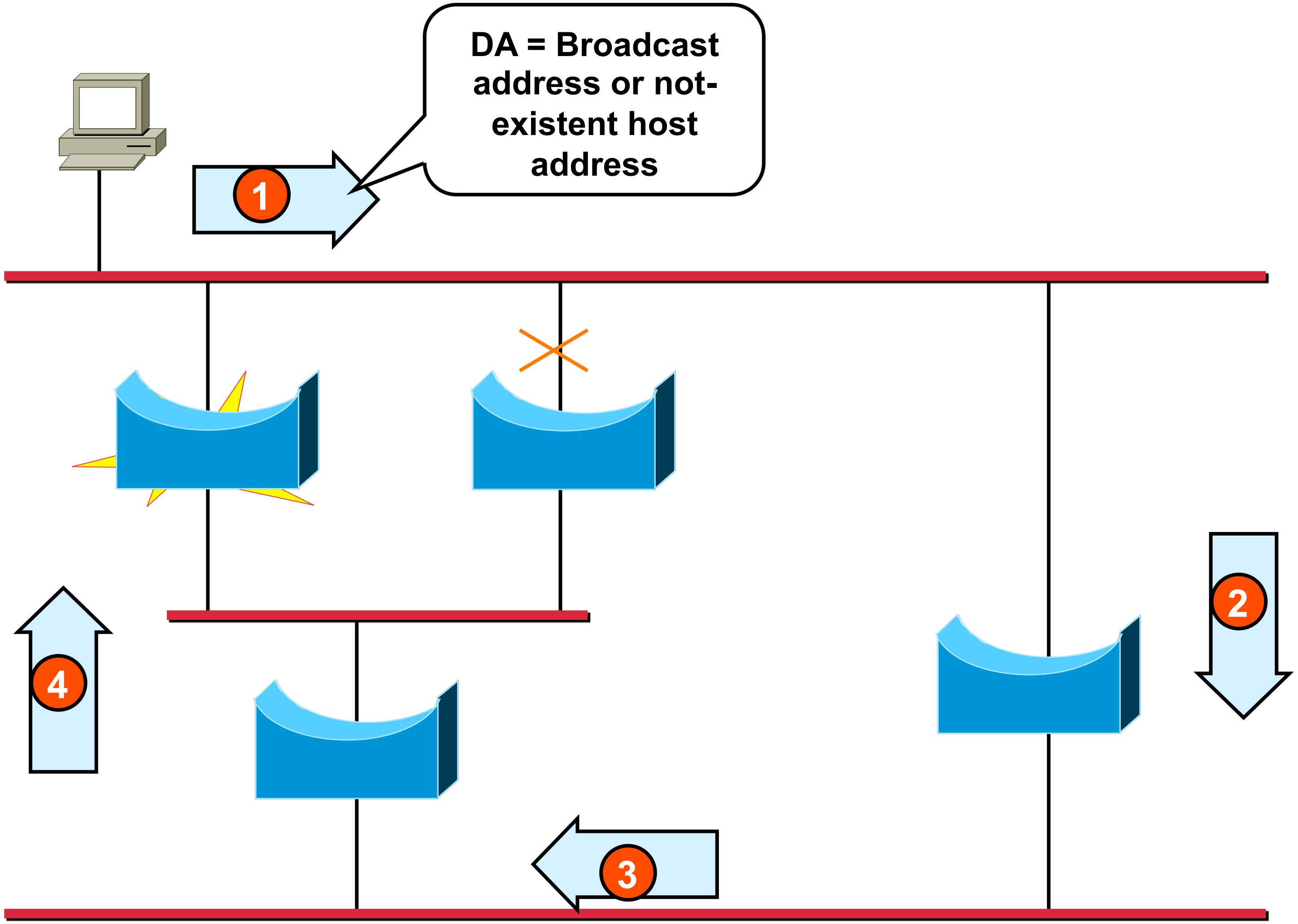
Spanning Tree

- **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

STP in Action (1)
No Broadcast Storm



STP in Action (2)
Bridge Failure – New STP Topology



Agenda

- **Introduction to LAN**
- **IEEE 802**
- **Logical Link Control**
- **Legacy Ethernet**
  - Introduction
  - CSMA/CD
  - Repeater, Link Segments
  - Framing
- **Transparent Bridging**
- **<u>Bridging versus Routing</u>**

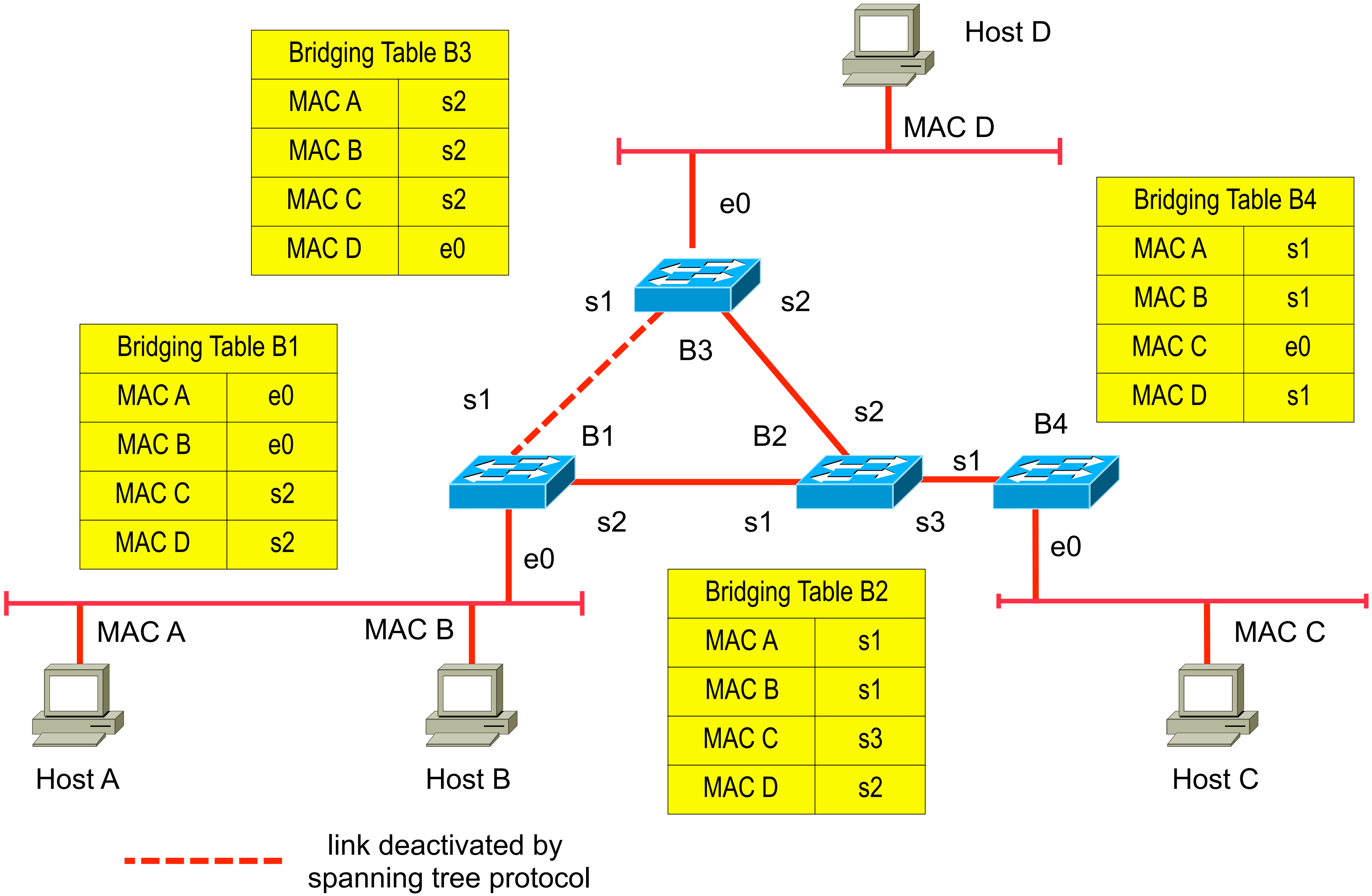
Bridging versus Routing

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
−	Bridge must process every frame	+	Router processes only packets addressed to it
−	Number of table-entries = number of all devices in the whole network	+	Number of table-entries = number of IP networks (Net-IDs) only
−	Spanning Tree eliminates redundant lines; no load balance is possible	+	Redundant lines and load balance are possible
−	No flow control (may be changed by usage of MAC Pause command)	−	Flow control is possible in theory (router is seen by end systems) but ICMP source quench is not the right way

Bridging versus Routing

Bridging		Routing	
−	No LAN/WAN coupling because of high traffic (broadcast domain!)	+	Does not stress WAN with subnet's L2 broad- or multicasts; commonly used as "gateway"
−	Paths selected by STP may not match communication behavior/needs of end systems	+	Router knows best way for every destination a packet is sent for
+	Faster, because implemented in HW; no address resolution	−	Slower, because usually implemented in SW; address resolution (ARP) necessary; hardware-optimization overcomes this nowadays
+	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, STP lacks from a global view of the network topology	+	Routing-protocols necessary to determine network topology, modern link-state routing has network topology database in router and hence a global view

Example Topology for Review Bridging



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

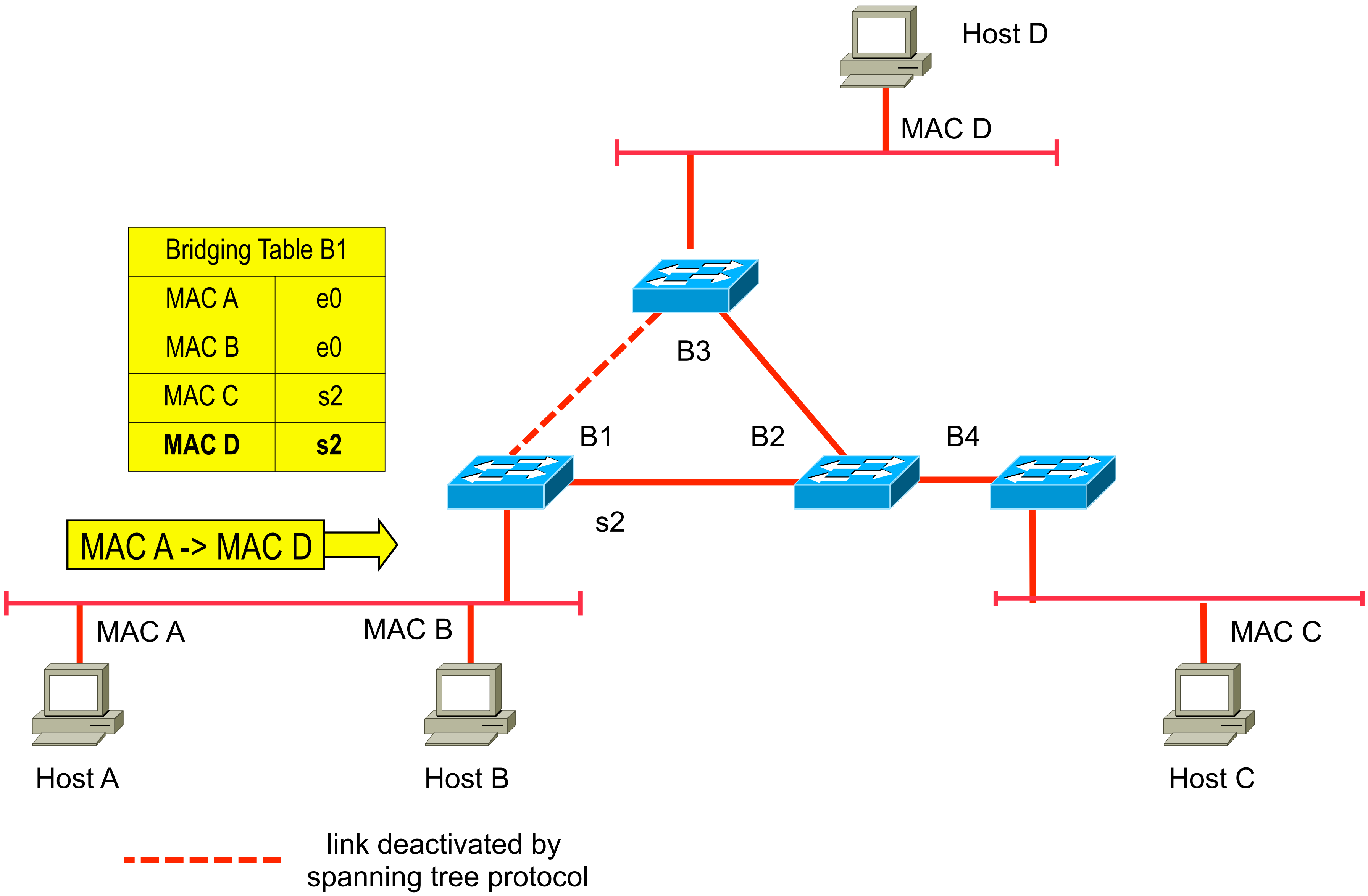
Bridging Table B4	
MAC A	s1
MAC B	s1
MAC C	e0
MAC D	s1

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

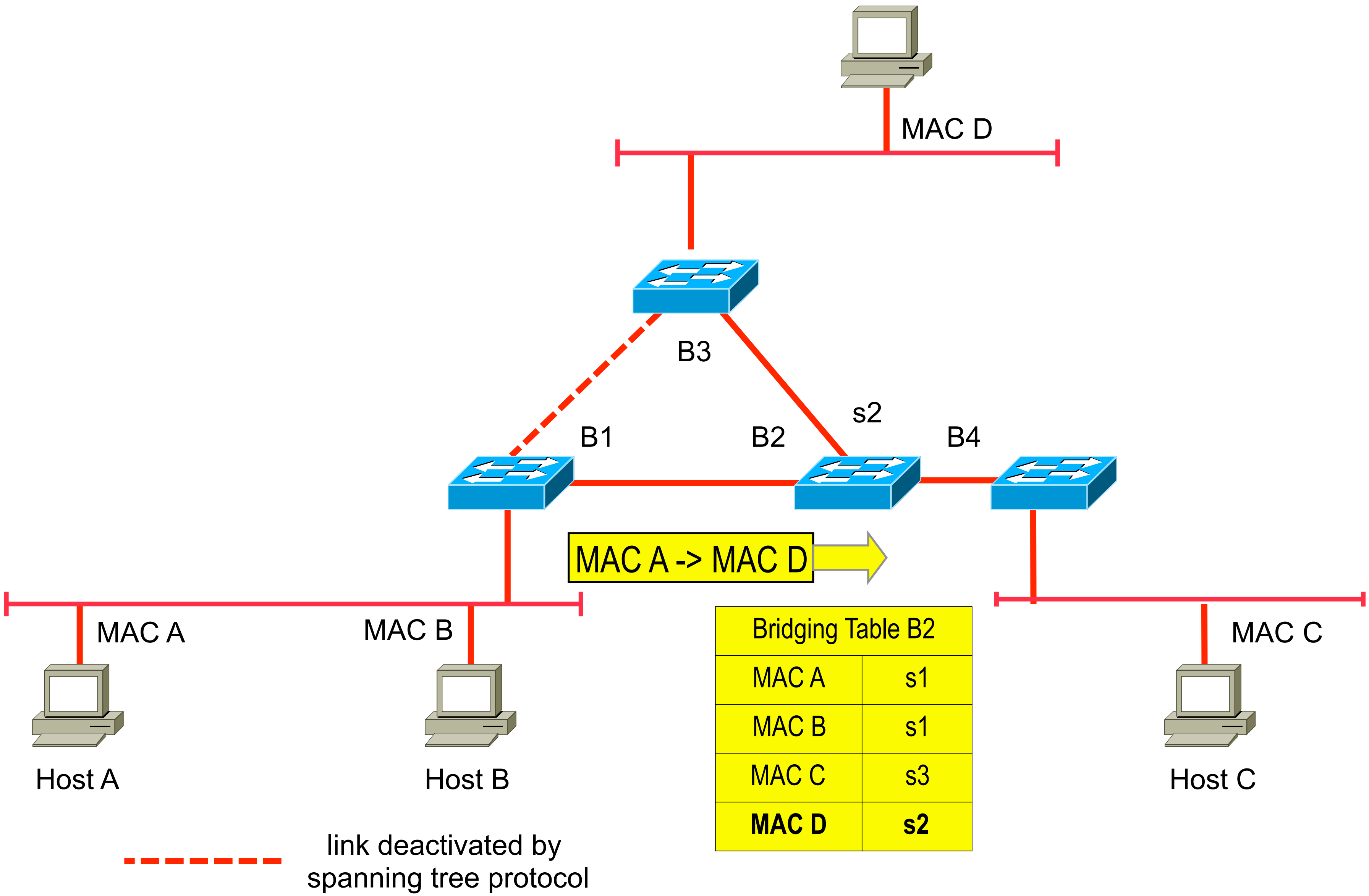
Bridging Table B2	
MAC A	s1
MAC B	s1
MAC C	s3
MAC D	s2

Frame MAC A to MAC D (1)

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



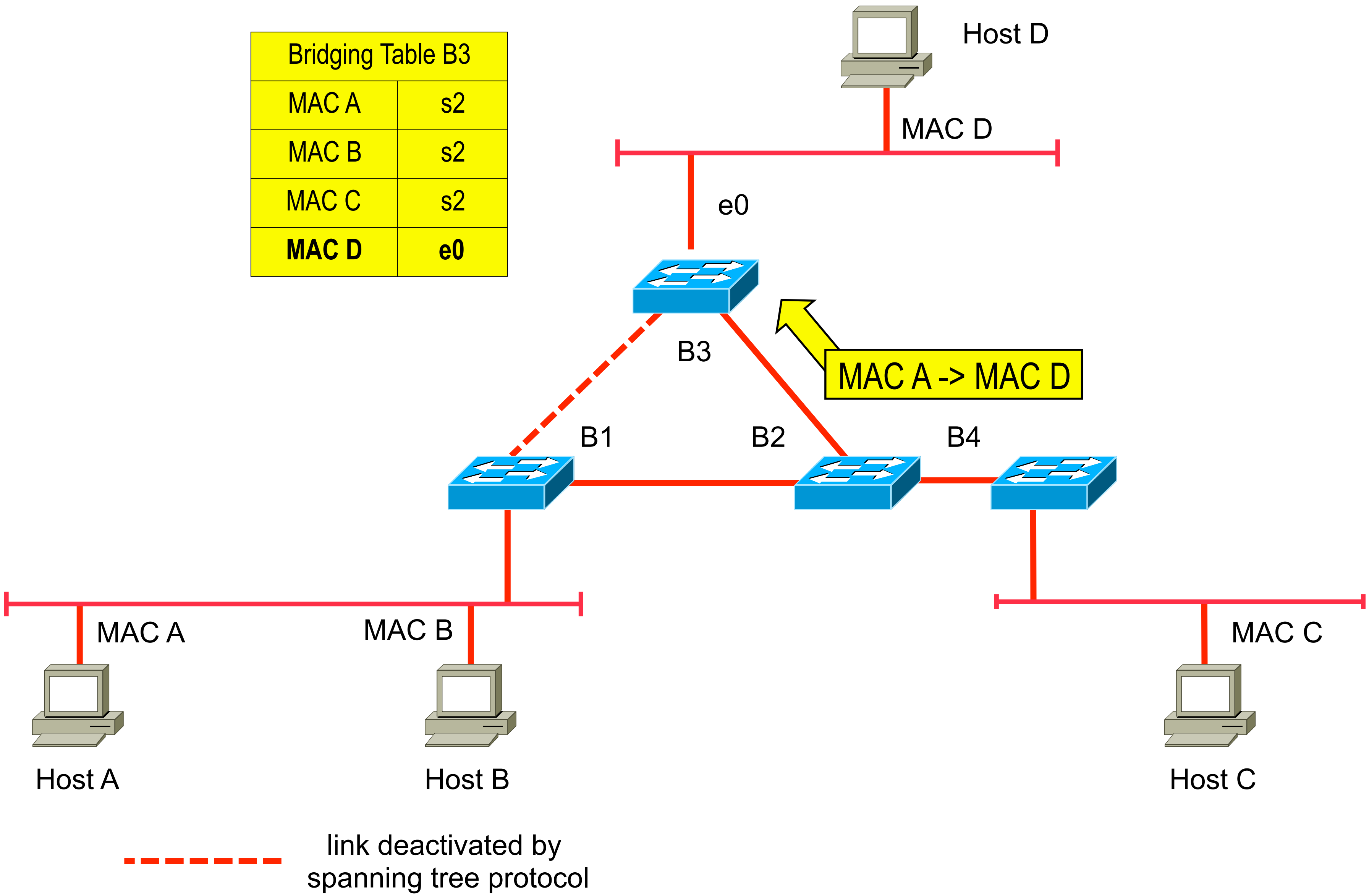
Frame MAC A to MAC D (2)



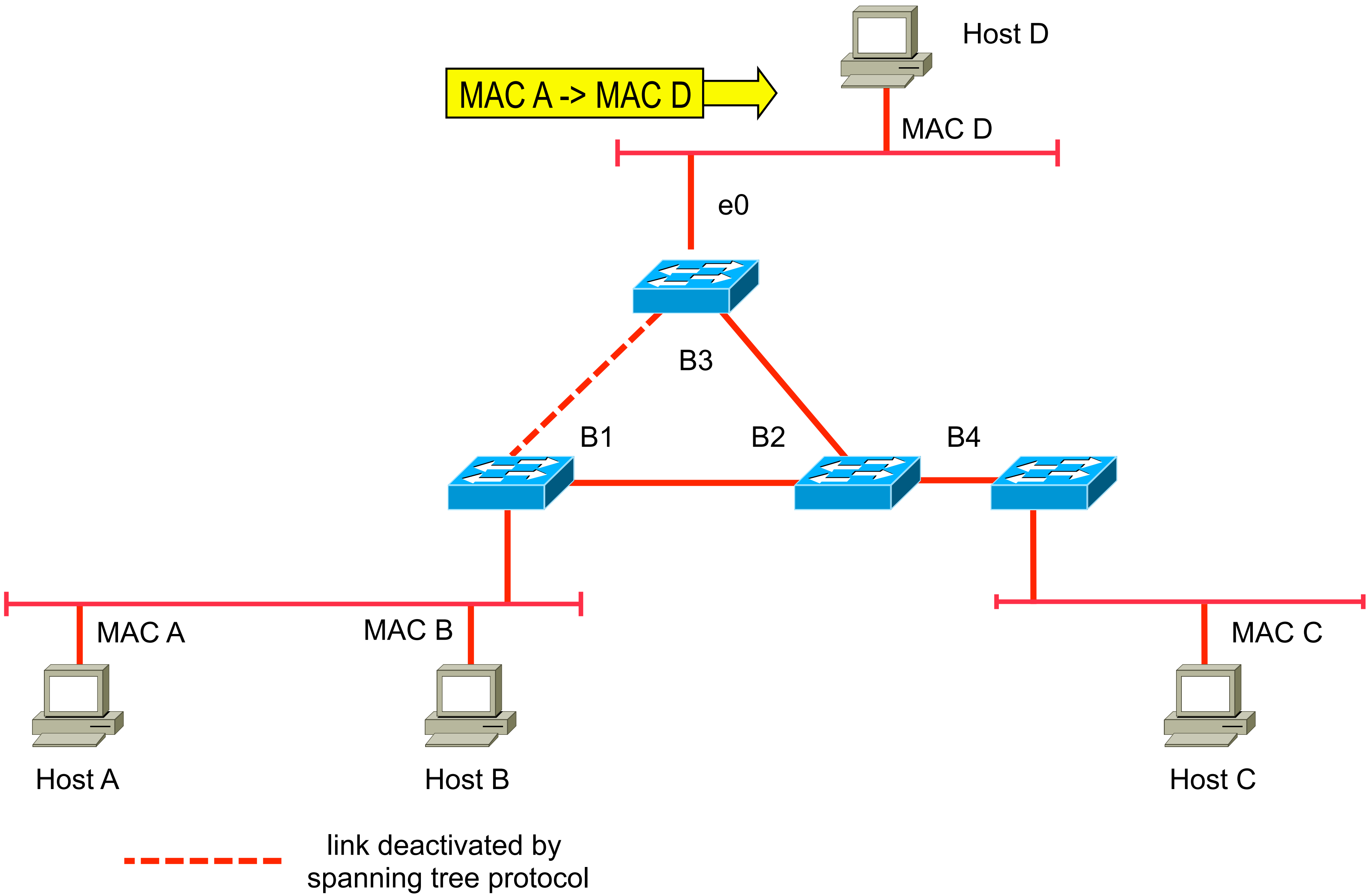
Bridging Table B2	
MAC A	s1
MAC B	s1
MAC C	s3
MAC D	**s2**

Frame MAC A to MAC D (3)

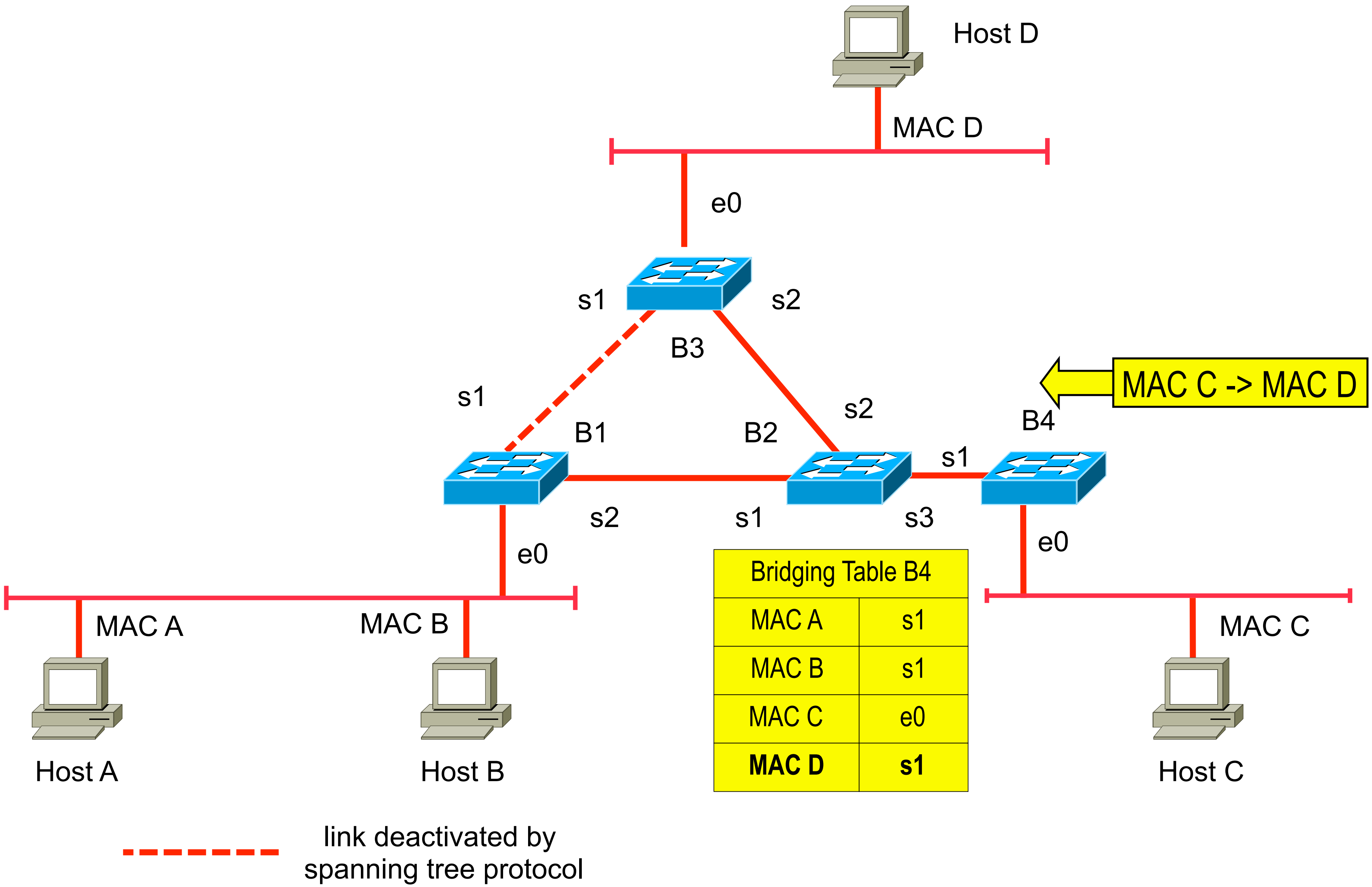
Bridging Table B3	
MAC A	s2
MAC B	s2
MAC C	s2
MAC D	**e0**



Frame MAC A to MAC D (4)

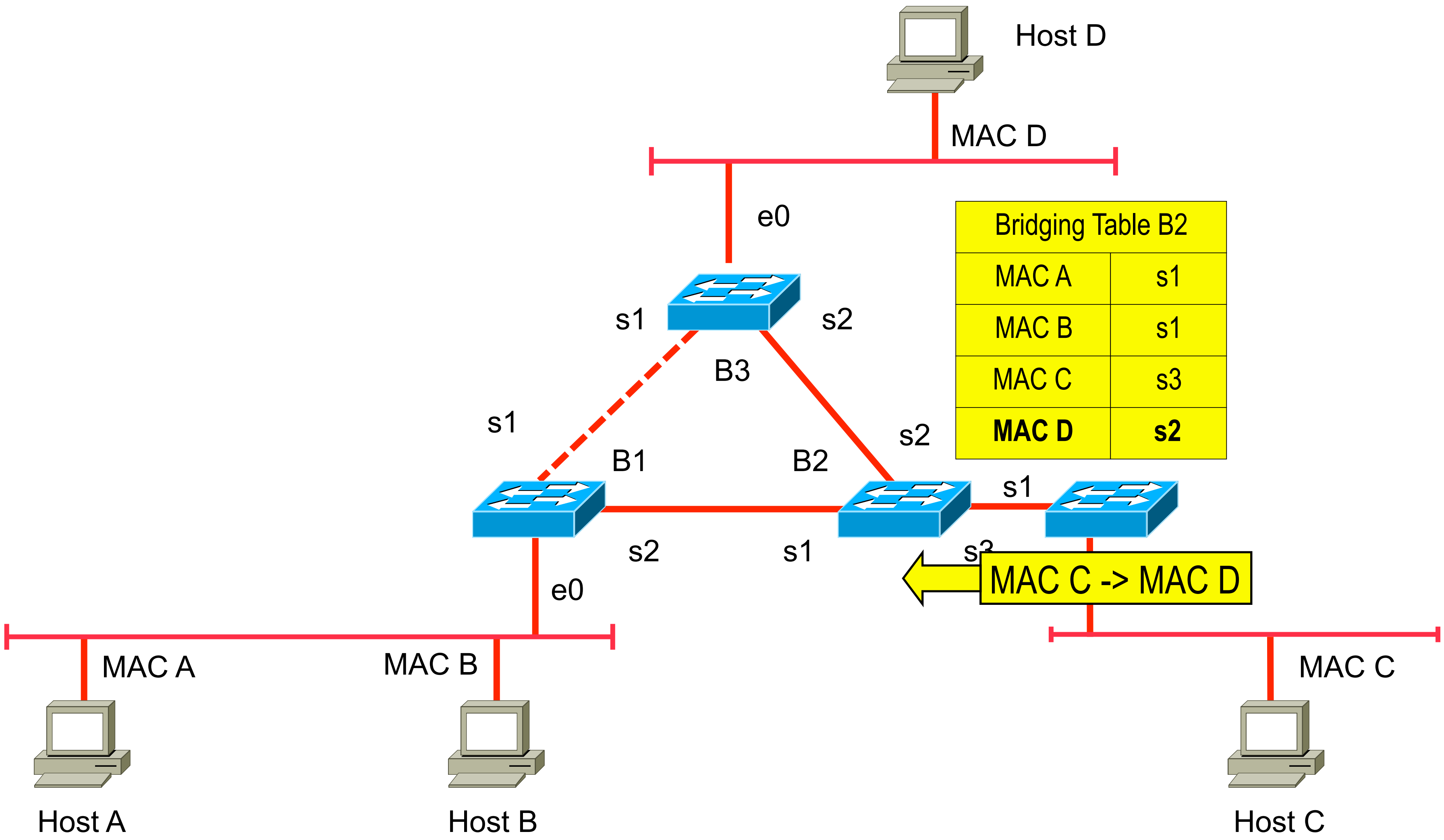


Frame MAC C to MAC D (1)



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

Frame MAC C to MAC D (2)



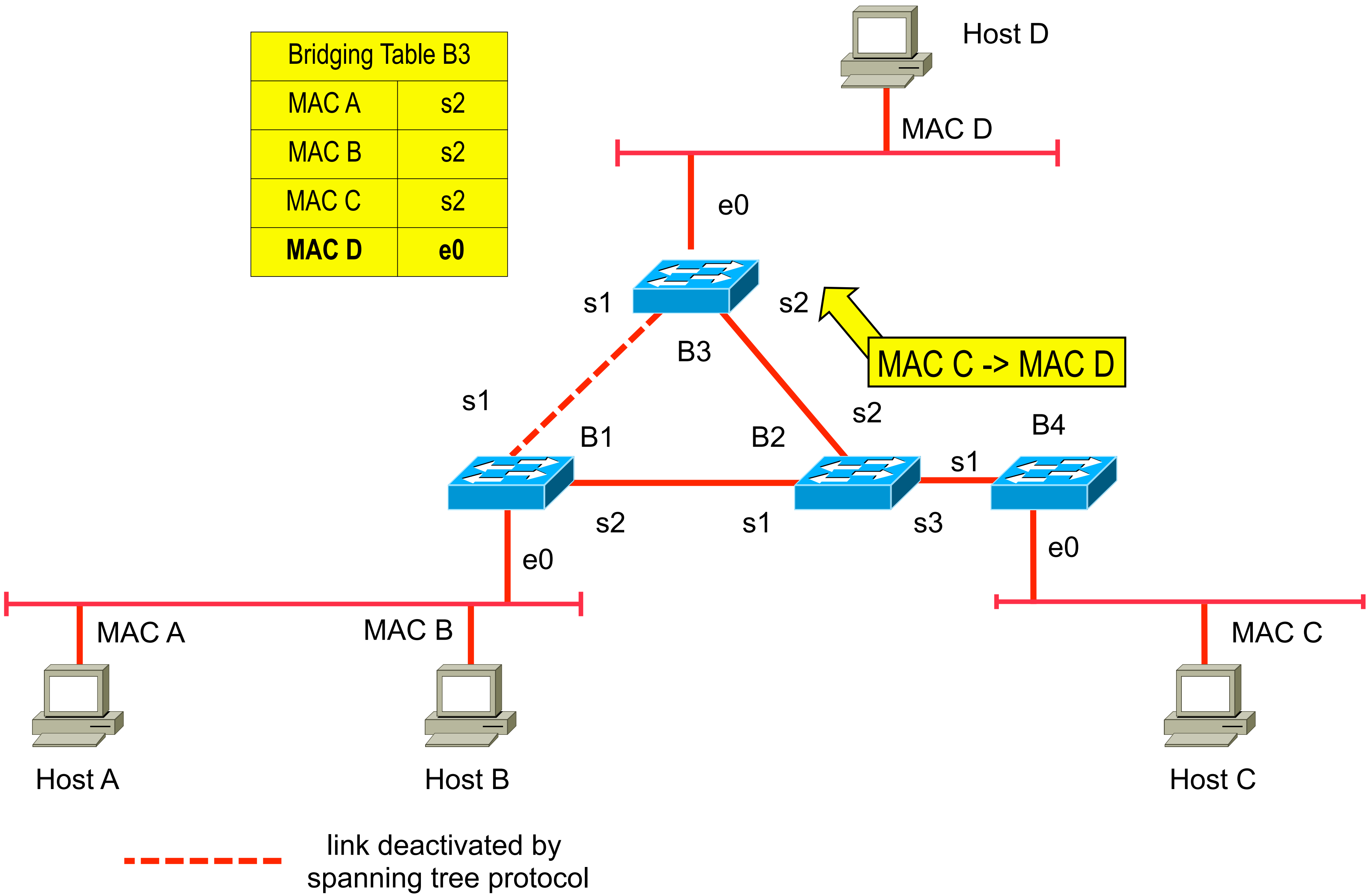
Bridging Table B2	
MAC A	s1
MAC B	s1
MAC C	s3
MAC D	**s2**

link deactivated by
spanning tree protocol

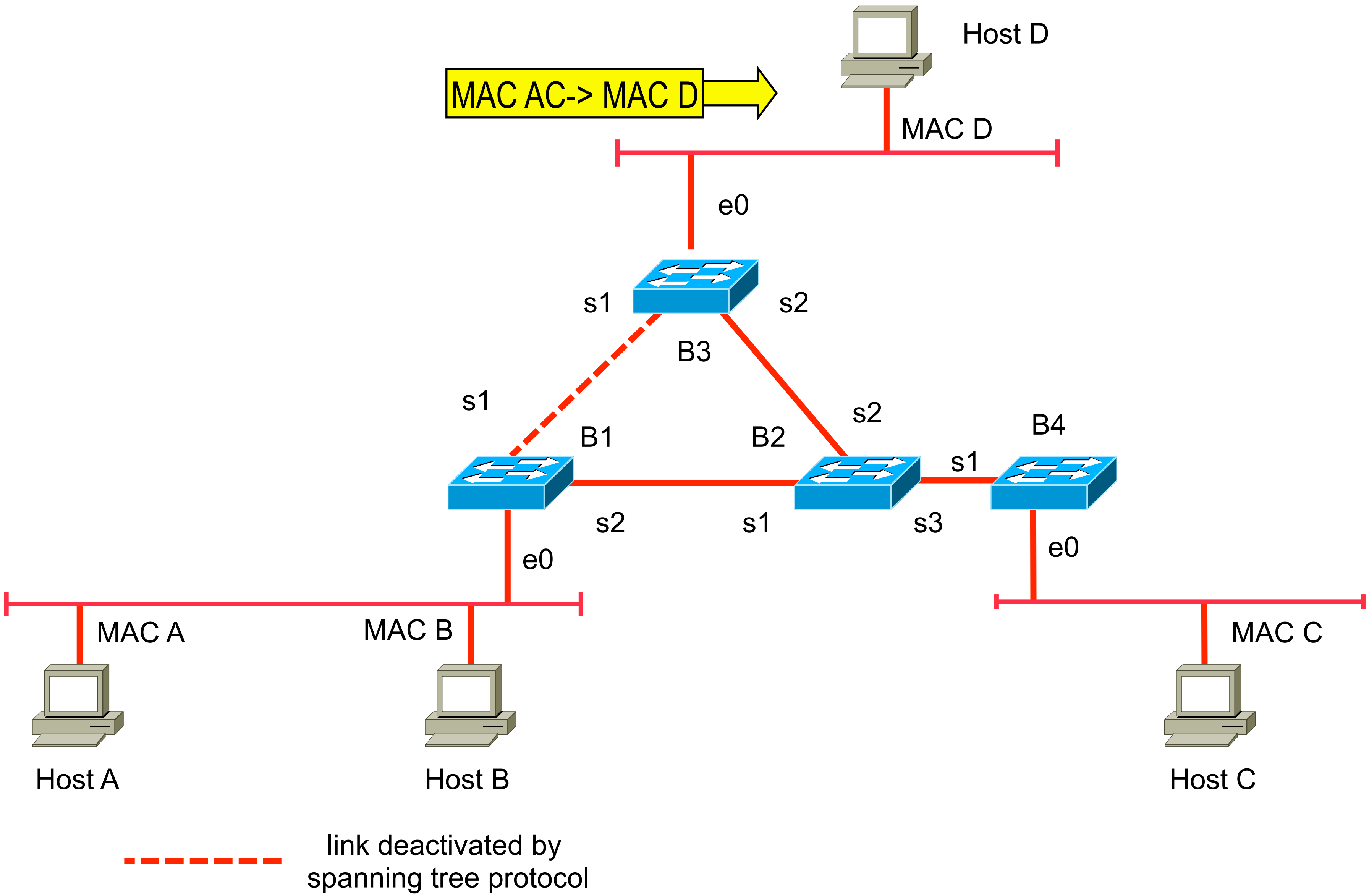
Frame MAC C to MAC D (3)

Takes Same Path as Frame from MAC A to MAC D -> No Load Distribution

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



Frame MAC C to MAC D (4)



Requirements for Routing

- **Consistent layer-3 functionality**
  - For entire transport system
  - From one end-system over all routers in between to the other end-system
  - Hence routing is not protocol-transparent
    - all elements must speak the same „language“
- **End-system**
  - Must know about default router
  - On location change, end-system must adjust its layer 3 address
- **To keep the routing tables consistent**
  - Routers must exchange information about the network topology by using routing-protocols or network administrator has to configure static routes in all routers

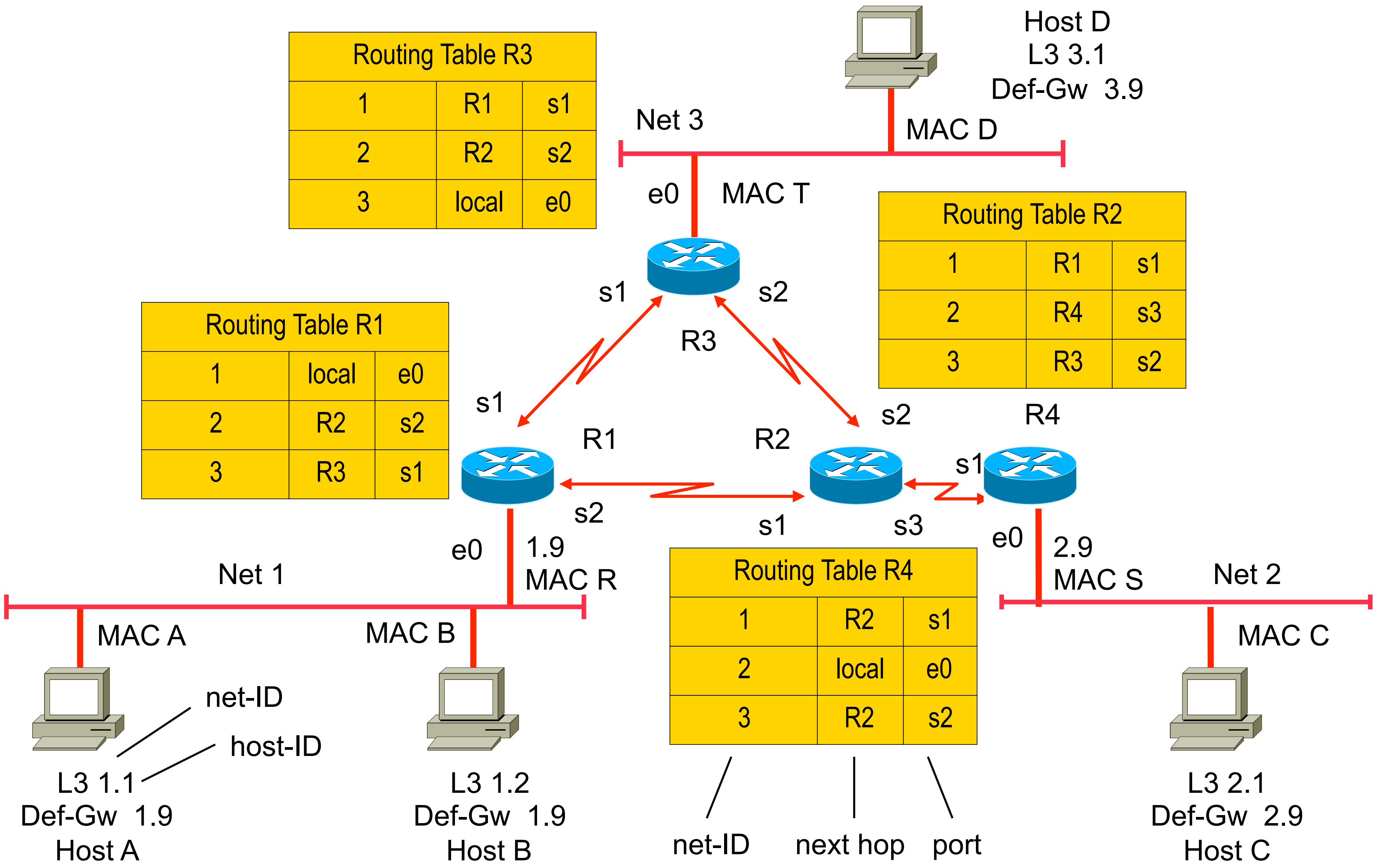
Routing Facts 1

- **In contrast to bridges**
  - Router maintains only the network of the layer 3 addresses in its routing table
  - The routing table size is direct proportional to the number of networks and not to the number of end-systems
- **Transport on a given subnet**
  - Still relies on layer 2 addresses
- **End systems forward data packets for remote destinations**
  - To a selected router (default gateway, default router) using the router's MAC-address as destination
  - Only these (unicast MAC addressed) packets must be processed by the router

Routing Facts 2

- **Flow control between router and end system is principally possible**
  - End systems knows about the local router
- **L2 Broadcast/multicast-packets in the particular subnet**
  - Are blocked by the router so L2 broad/multicast traffic on the subnets doesn't stress WAN connections
- **Independent of layer 1, 2**
  - so coupling of heterogeneous networks is possible
- **Routers can use redundant paths**
  - meshed topologies are usual
- **Routers can use parallel paths for load balancing**

Example Topology for Intro Routing



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

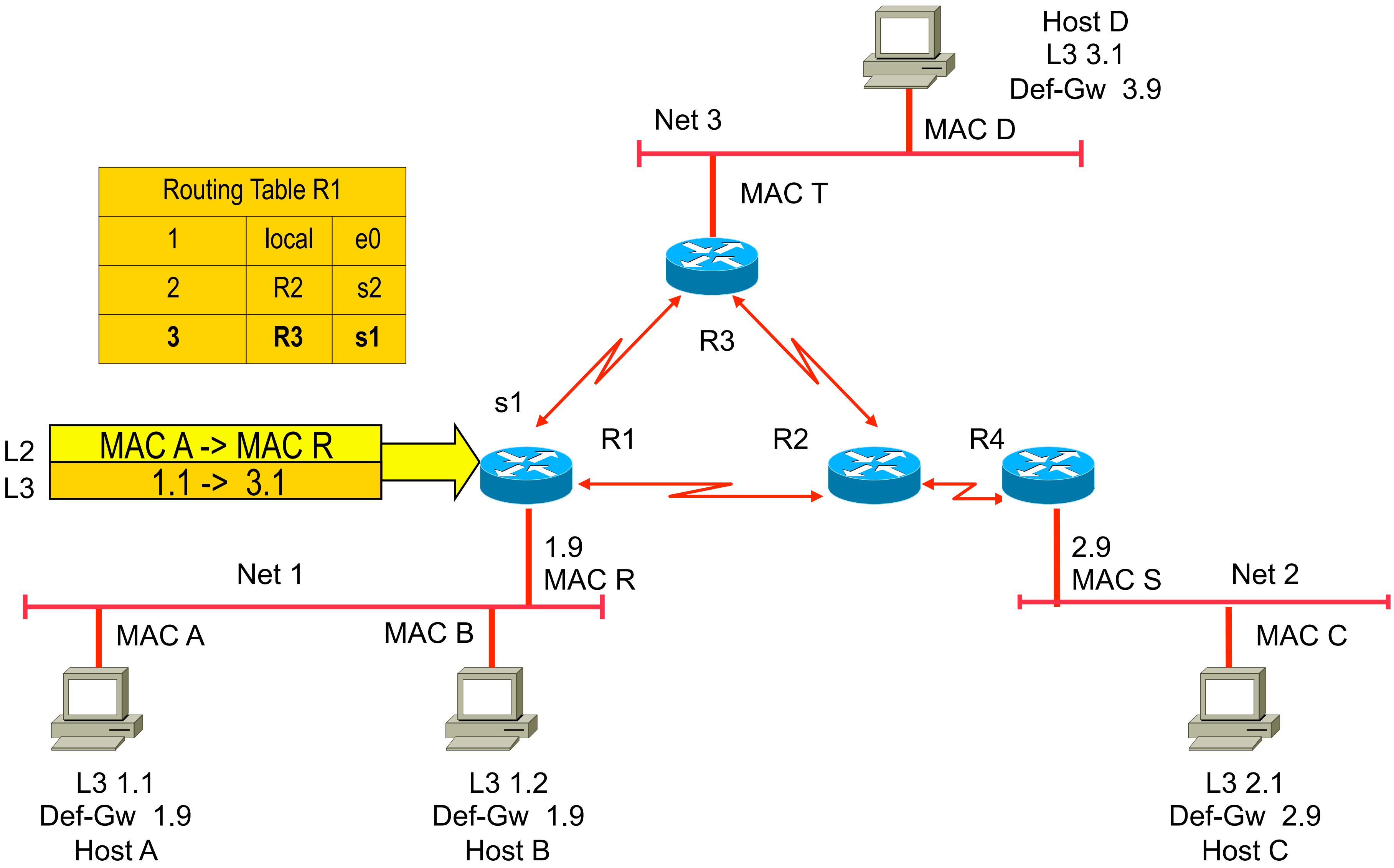
Routing Table R2		
1	R1	s1
2	R4	s3
3	R3	s2

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

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

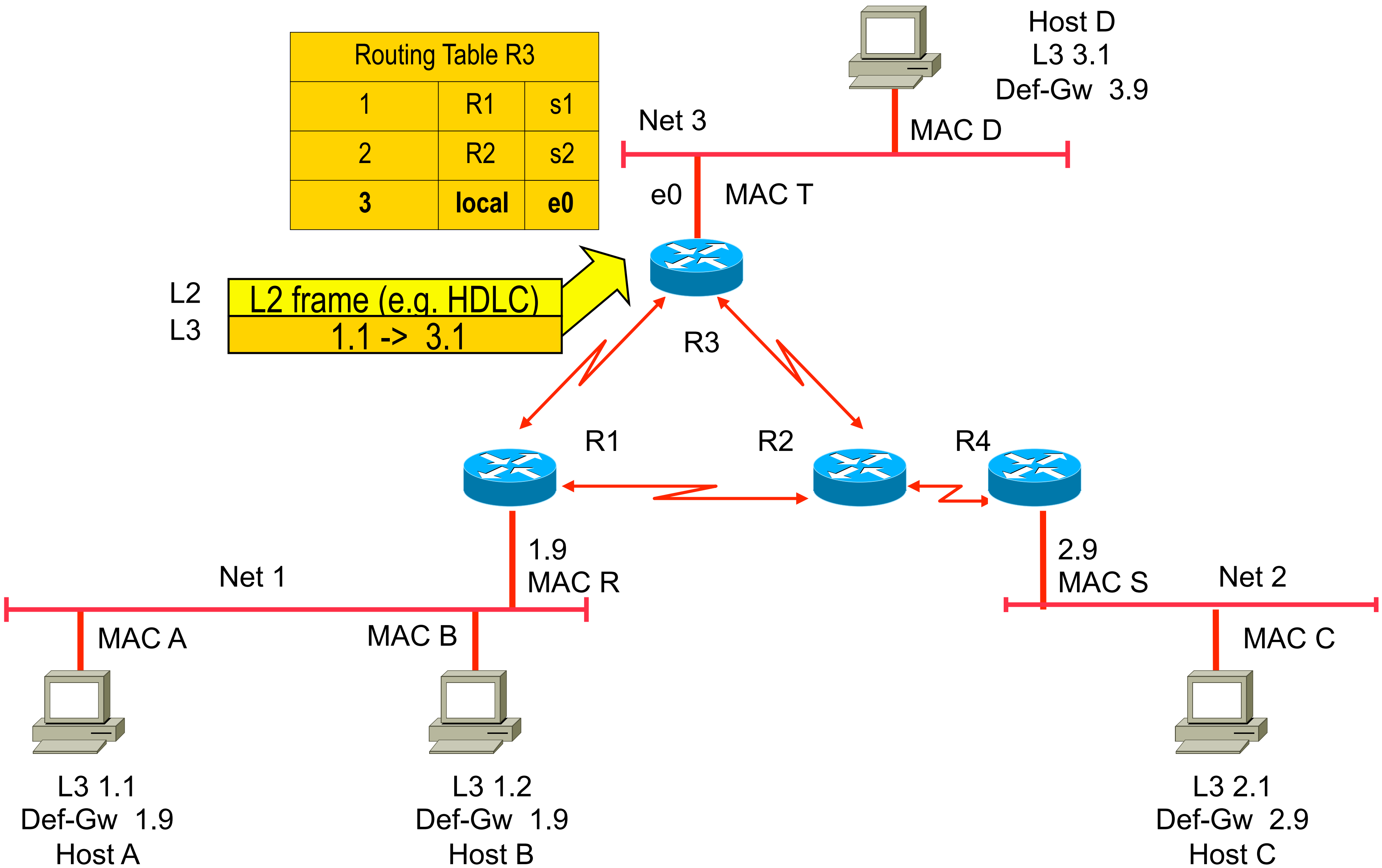
Packet 1.1 to 3.1 (1)

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

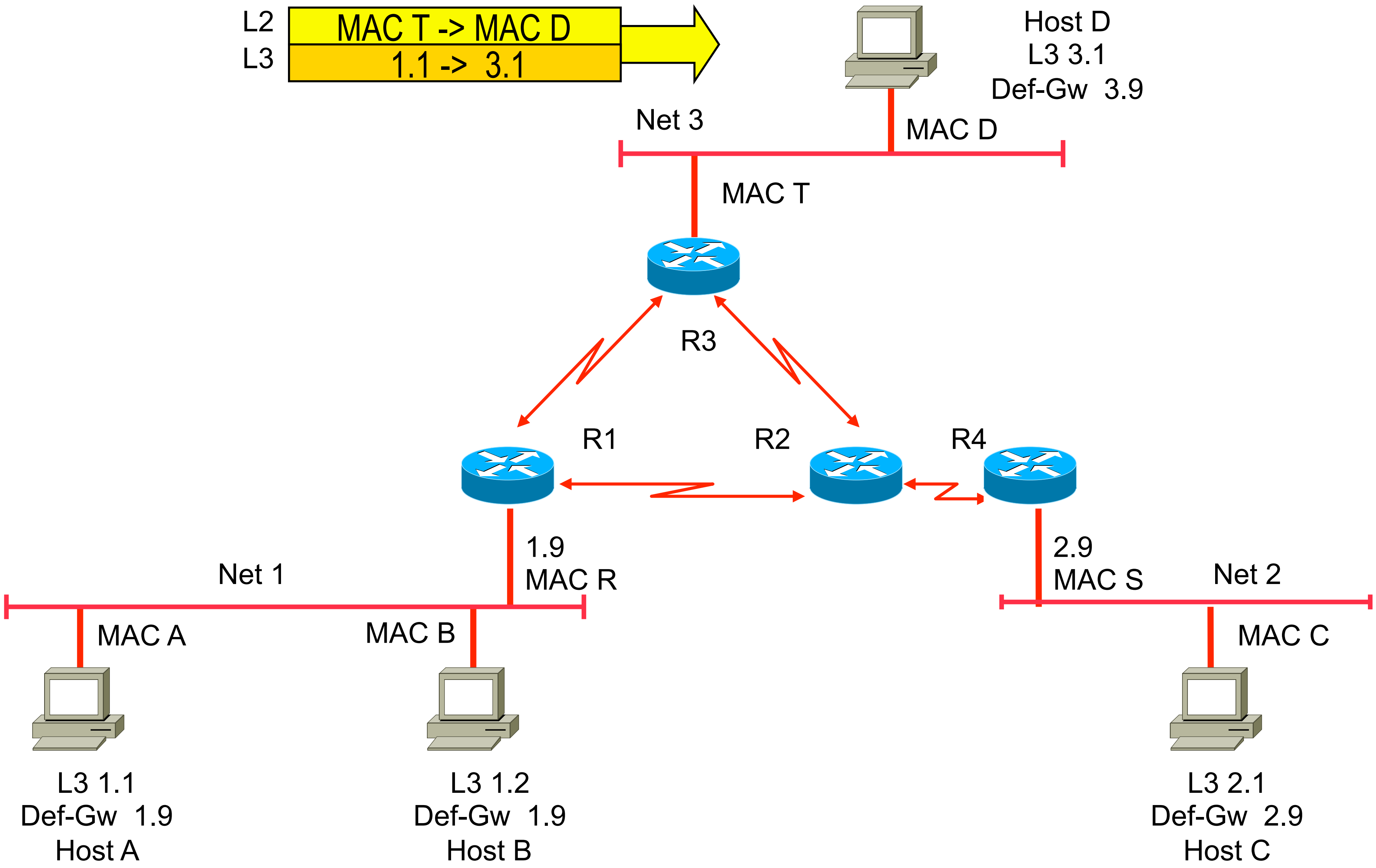


Packet 1.1 to 3.1 (2)

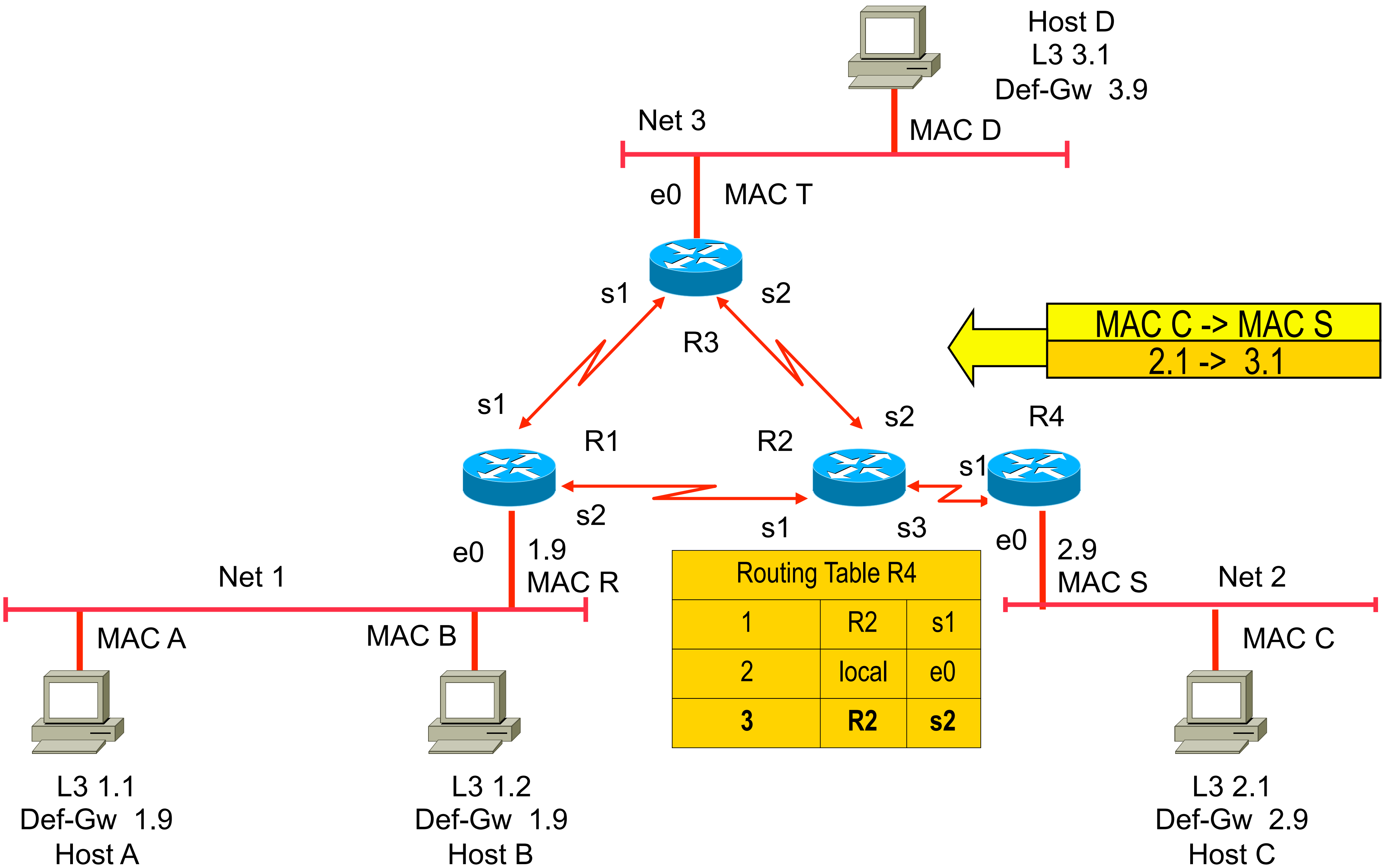
Routing Table R3		
1	R1	s1
2	R2	s2
3	**local**	**e0**



Packet 1.1 to 3.1 (3)

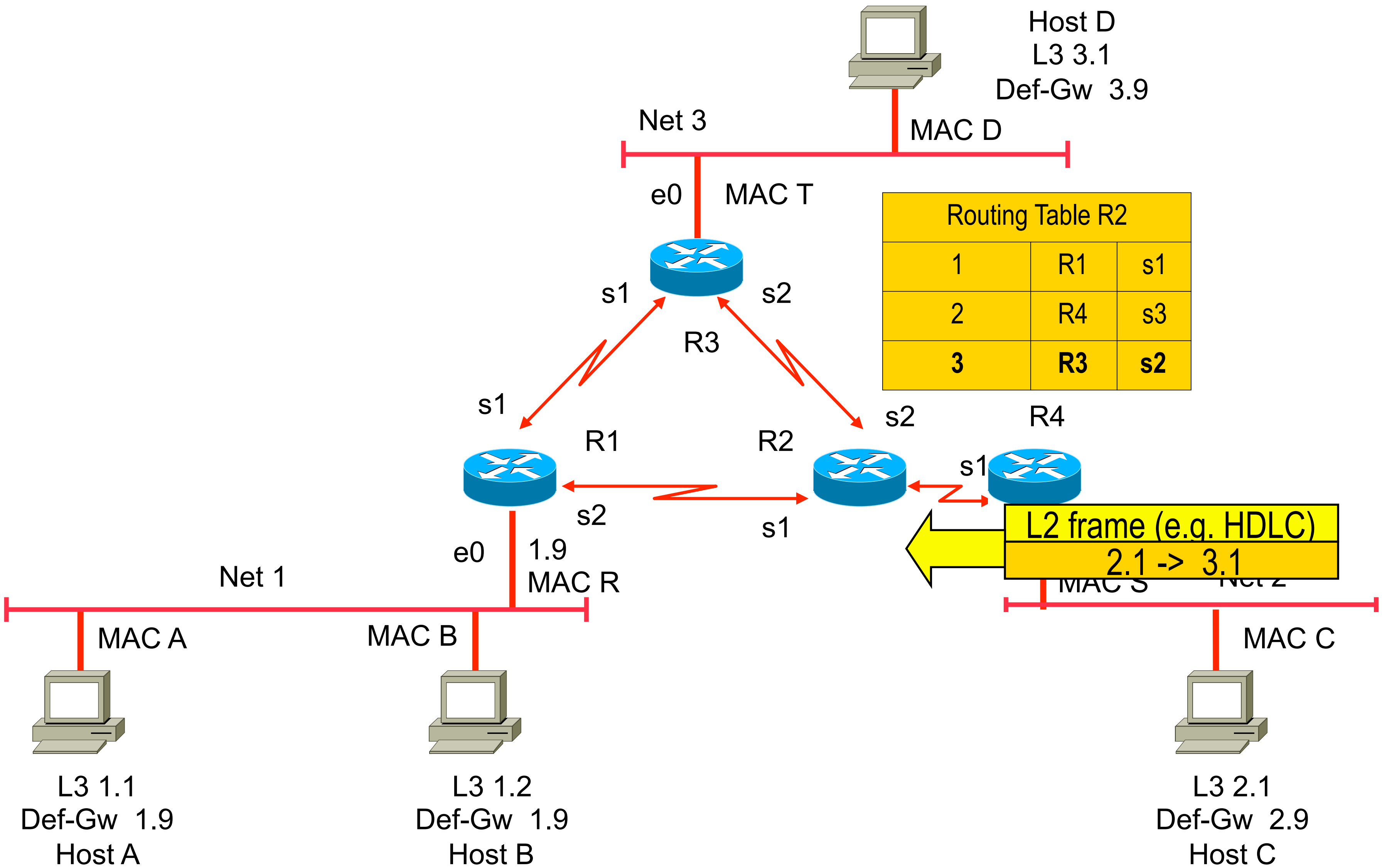


Packet 2.1 to 3.1 (1)



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

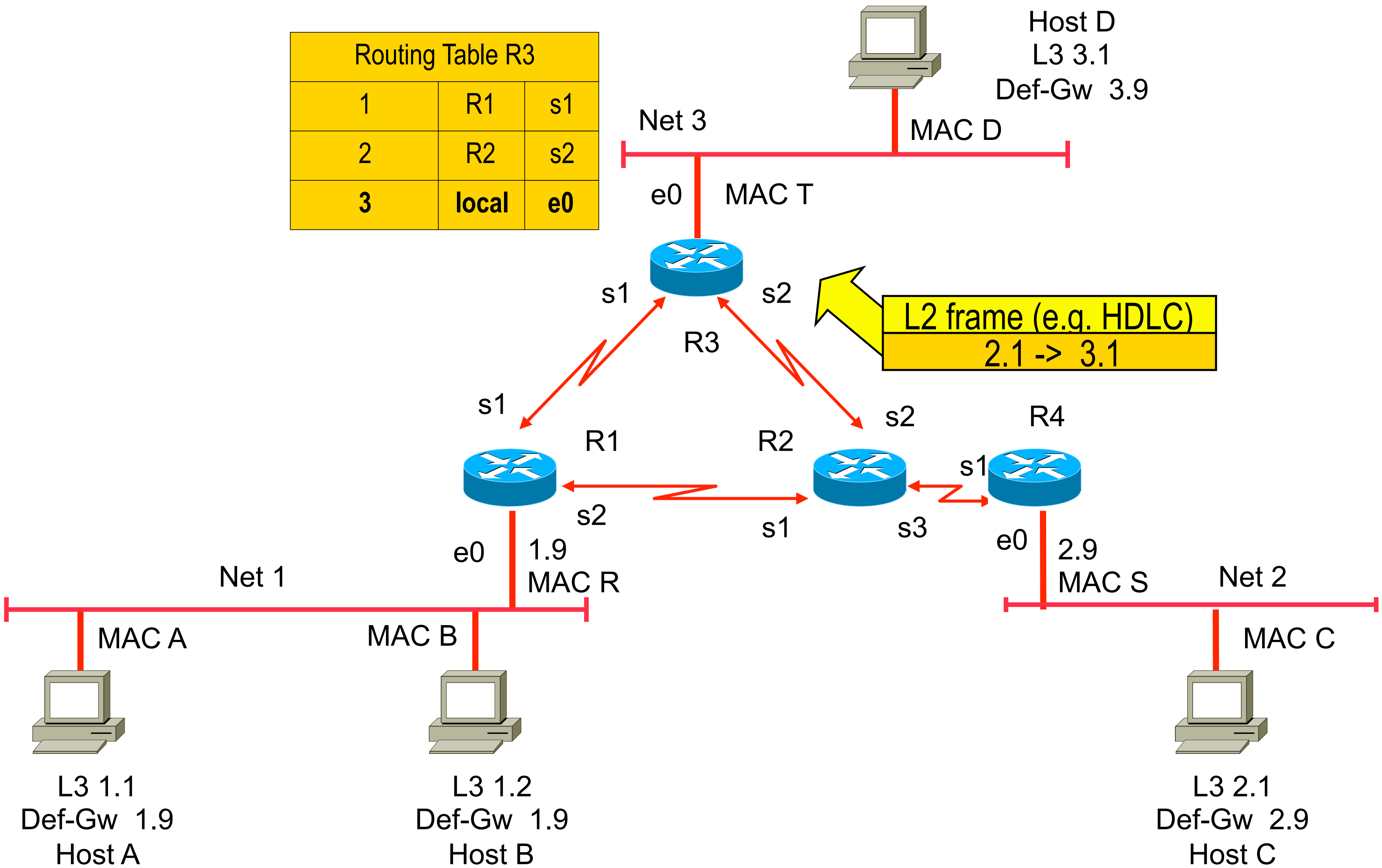
Packet 2.1 to 3.1 (2)



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

Packet 2.1 to 3.1 (3)
Takes Different Path as Packet from 1.1 to 1.3 -> Load Distribution

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



Packet 2.1 to 3.1 (3)