FRANKFURT UNIVERSITY OF APPLIED SCIENCES

COMPUTER NETWORKS

Data Link Layer - Framing and Switching

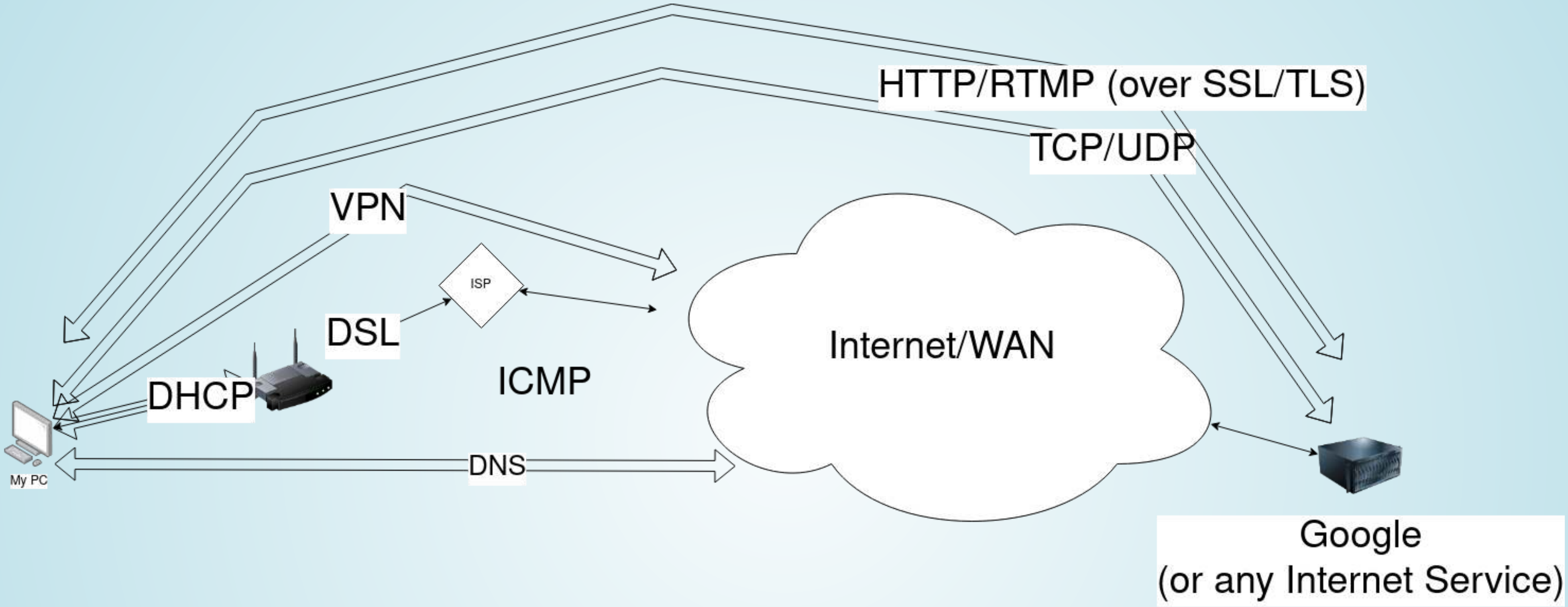
Prof. Dr. Oliver Hahm

2024-11-28

AGENDA

- Framing
  - Frame Detection
  - Ethernet (IEEE 802.3) Frames
  - WLAN (IEEE 802.11) Frames
- Addresses
- Switching
  - Devices
  - Forwarding
  - Loops

REVIEW: THE BIG PICTURE



DATA LINK LAYER

Functions of the Data Link Layer

- Framing Encapsulate network layer datagrams into frames
- Addressing Provide physical addresses (MAC addresses)
- Media Access Coordinate the access of the transmission medium
- Error Control Detect and potentially correct errors
- Flow Control Ensure that the data rate does not exceed the receiver’s capacity

Devices:
Bridge, Switch, Modem

Protocols:
Ethernet, WLAN, Bluetooth, PPP

The Data Link Layer can be split into

- Media Access Control (MAC) sublayer and
- Logical Link Control (LLC) sublayer

OSI Reference Model

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

FRAMING

FRAMING

- The receiver needs to split the bit stream from the Physical Layer into frames
- The sender encapsulates the packets from the Network Layer into frames

FRAME DETECTION

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

EXAMPLE: PROBLEMS IN TELEGRAPH SYSTEMS

A	· —	M	— —	Y	— · — —
B	— · · ·	N	— ·	Z	— — · ·
C	— · — ·	O	— — —	1	· — — — —
D	— · ·	P	· — — ·	2	· · — — —
E	·	Q	— — · —	3	· · · — —
F	· · — ·	R	· — ·	4	· · · · —
G	— — ·	S	· · ·	5	· · · · ·
H	· · · ·	T	—	6	— · · · ·
I	· ·	U	· · —	7	— — · · ·
J	· — — —	V	· · · —	8	— — — · ·
K	— · —	W	· — —	9	— — — — ·
L	· — · ·	X	— · · —	0	— — — — —

Morse Code Used for telegraph systems

Problem

- The sender meant:
  — · ·   — — —
  → *DO*
- The receiver understood:
  ·   · —   —
  → *EAT*

How does the receiver know when a new PDU starts?

FRAME DETECTION

- The start of each frame needs to be marked
- Different ways exist to mark the frames’ borders
  - Character count in the header
  - Byte/Character stuffing
  - Bit stuffing
  - Line code violations of Physical Layer with illegal signals
- All these different procedures have advantages and drawbacks

CHARACTER COUNT IN THE FRAME HEADER

- Include the character count in the header of the frame
- **Example:** the byte-oriented **Digital Data Communications Message Protocol** (DDCMP) of DECnet
- In each frame, the field `Count` contains the number of bytes payload inside the frame

8 Bits	14 Bits	2 Bits	8 Bits	8 Bits	8 Bits	16 Bits		16 Bits
SOH	Count	Flags	RESP	NUM	ADDR	CRC 1	Body	CRC 2
Start of Header	Number of bytes In payload					Checksum of header	Payload	Chacksum of payload

- Potential issue: If the field `Count` is modified during transmission, the receiver is unable to correctly detect the end of the frame

CONTROL SEQUENCES

- Control characters ("Sentinel characters") mark the start and end of the frames

- What is the problem here?
- An upper layer may want to send these bytes!

BYTE/CHARACTER STUFFING

- The method is called **Byte Stuffing** or **Character Stuffing**, because the...
  - sender **inserts** (stuffs) extra characters into the payload
  - receiver **removes** the stuffed characters from the received payload, before passing it to the Network Layer
- Drawback:
  - Strong relationship with the character encoding (e.g., ASCII)
    - More recent protocols of this layer no longer operate byte-oriented, but bit-oriented because this allows using any character encoding

EXAMPLE: BYTE/CHARACTER STUFFING (BISYNC)

- A protocol, which highlights the frames border with special characters, is the byte-oriented (character-oriented) protocol **Binary Synchronous Communication** (BISYNC), which was invented by IBM in the 1960s

8 bits	8 bits	8 bits		8 bits		8 bits	16 bits
SYN	SYN	SOH	Header	STX	Body	ETX	CRC
Synchronization characters		Start of Header		Start of Text	Payload	End of Text	

- The start of a frame highlights the character SYN
- The start of the header highlights the character SOH (*Start of Header*)
- The payload is between STX (Start of text) and ETX (*End of Text*)

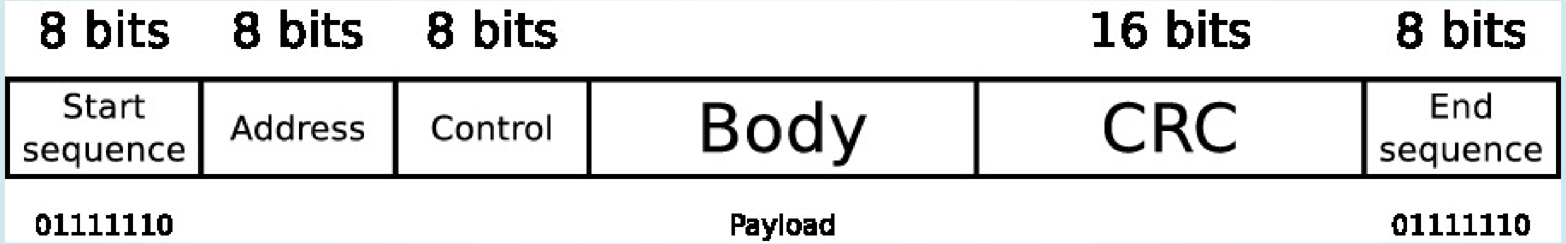
- If the payload (body) contains an ETX character, it it must be escaped by a stuffed DLE (*Data Link Escape*)
- The DLE character is represented in the payload by sequence DLE DLE

BIT STUFFING

- When bit-oriented protocols are used, each frame begins and ends with a special bit pattern
  - With this method the sender **inserts** (stuffs) extra bits into the payload
  - The receiver **removes** the stuffed bits from the received payload, before passing it on
- Advantages:
  - Ensures that the start/end sequence does not occur in the payload
  - Every character encoding can be used with this framing method

EXAMPLE: BIT STUFFING (HDLC)

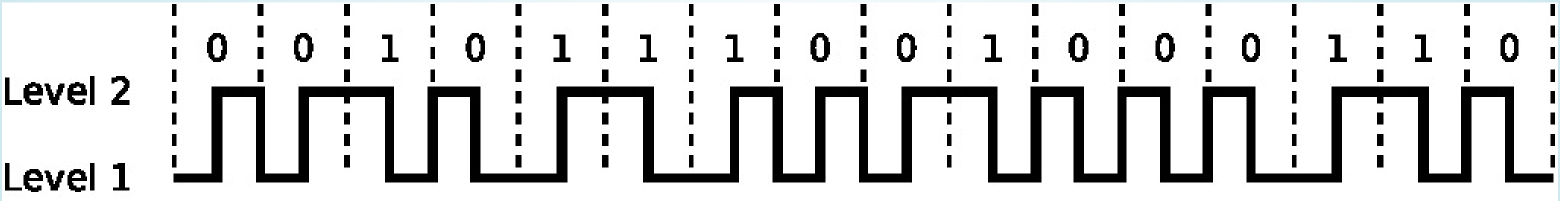
- **Examples:** The protocol **High-Level Data Link Control** (HDLC) and the **Point-to-Point Protocol** (PPP), which implments HDLC
  - Each frame begins and ends with the sequence `01111110`

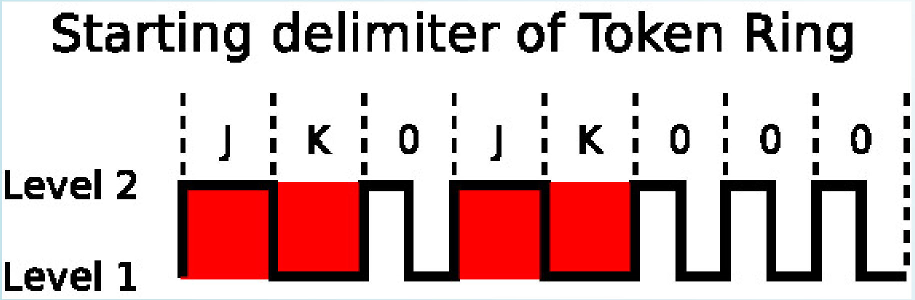


- If the HDLC protocol in the Data Link Layer...
  - of the sender discovers 5 consecutive 1-bits in the bit stream from the Network Layer, it stuffs a 0-bit in the outgoing bit stream
  - of the receiver discovers 5 consecutive 1-bits, followed by a 0-bit in the bit stream from the Physical Layer, it removes (destuffs) the 0-bit

LINE CODE VIOLATIONS

- Depending on the line code used in the Physical Layer, illegal signals can be used to highlight the frame boundaries
  - **Example:** Token Ring uses the Differential Manchester Encoding
    - With this line code, a signal level change occurs inside each bit cell



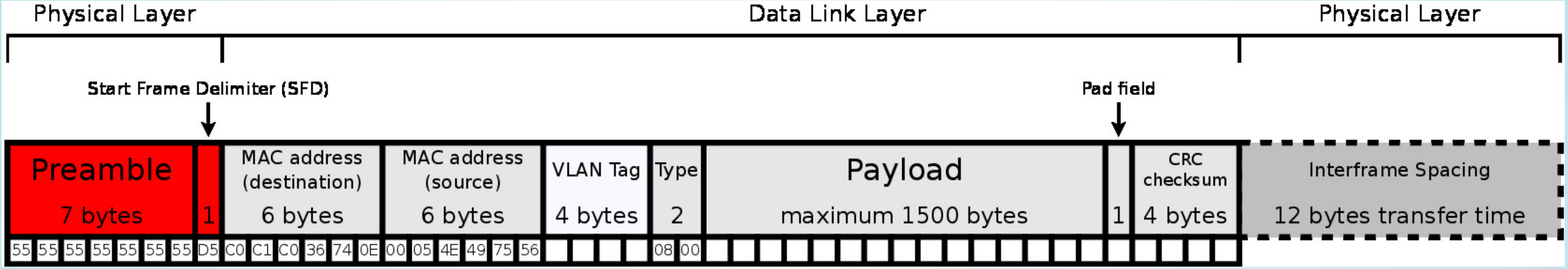


- If Token Ring is used, frames start with a byte (**starting delimiter**) which **contains 4 line code violations**

The second last byte (**ending delimiter**) of a Token Ring frame contains the same 4 line code violations as the starting delimiter

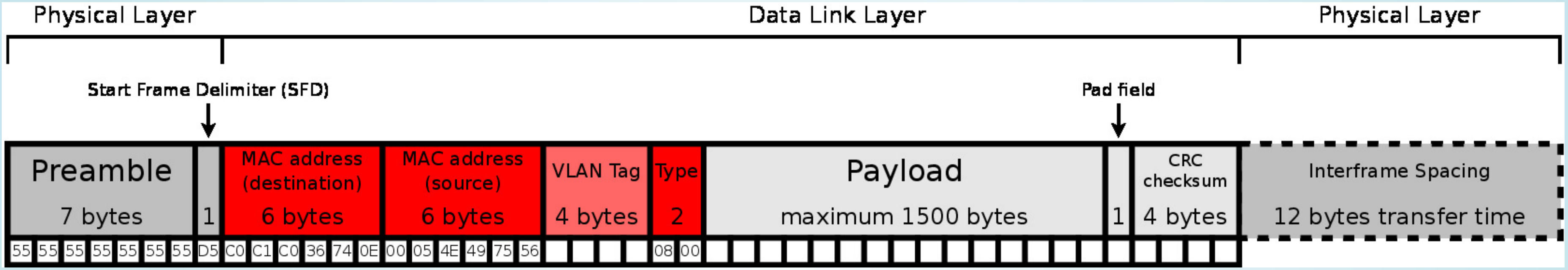
ETHERNET (IEEE 802.3) FRAMES

PREAMBLE AND SFD



- Preamble is a 7 bytes long bit sequence `101010 ... 1010`
  - Allows the receiver to synchronize with the clock and to identify the beginning of the frame
  - Is followed by the SFD (1 byte) with the bit sequence `10101011`

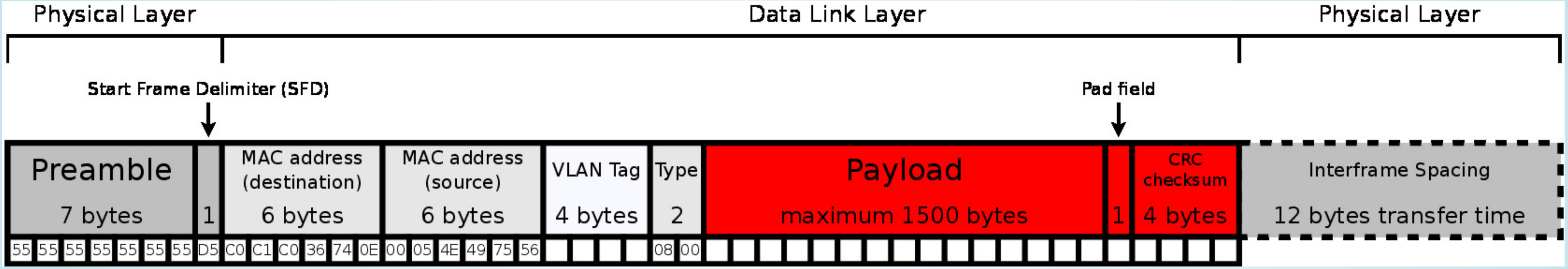
ADDRESSES AND VLAN TAG



- The field Type contains the information what protocol is used in the network layer
  - If IPv4 is used, the field Type has value `0x0800`
  - If IPv6 is used, the field Type has value `0x86DD`
  - If the payload contains an ARP message, the field Type has value `0x0806`

1. The address format has been adopted by other IEEE 802 standards like WLAN or FDDI.
2. Introduced by IEEE 802.1Q or IEEE 802.1ad.

FRAME SIZE AND CHECKSUM

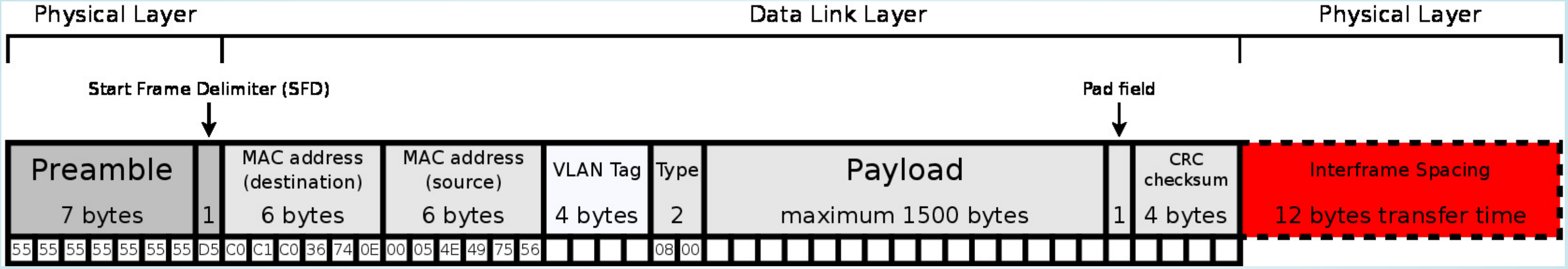


- Minimum size of an Ethernet frame: 72 bytes
- Maximum size (incl. preamble and SFD): 1526 bytes (1530 bytes incl. VLAN tag)

- The maximum frame size [1] of Ethernet limits the payload to 1500 bytes
  - The Pad field can be used to increase the frame length to the minimum frame size (72 bytes)
    - This is required for the collision detection ⟶ medium access control
- The last field contains a checksum [2] (32 bits)

1. Generically called the Maximum Transfer Unit (MTU).
2. The checksum covers all fields except for preamble and SFD.

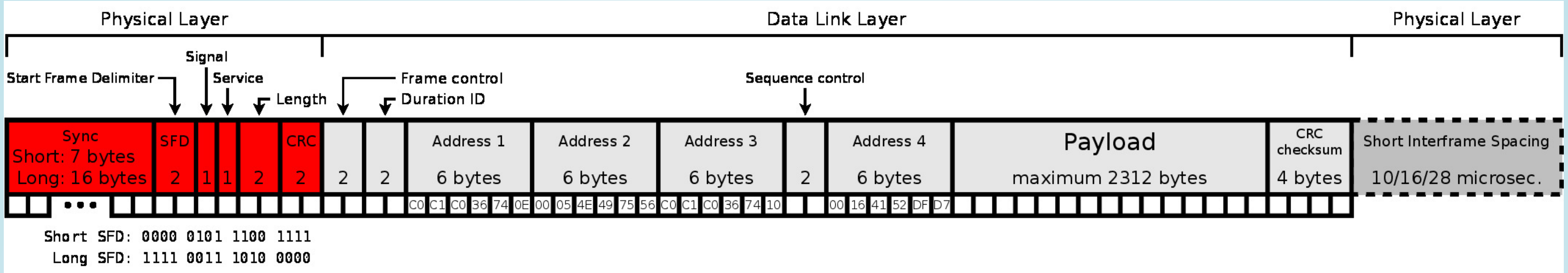
INTERFRAME SPACING



- The Interframe Spacing or Interframe Gap is the minimum idle period between the transmission of Ethernet frames
- The minimum idle period is 96 bit times (12 bytes)
  - It is 9.6 microseconds when using 10 Mbps Ethernet
  - It is 0.96 microseconds when using 100 Mbps Ethernet
  - It is 96 nanoseconds when using 1 Gbps Ethernet
- Some network devices allow to reduce the Interframe Spacing period
  - **Benefit**: Better data rate is possible
  - **Drawback**: For the receiver it may become impossible to detect the frames' borders ($\Longrightarrow$ the number of errors may rise)

WLAN (IEEE 802.11) FRAMES

PREAMBLE AND LAYER 1 HEADER

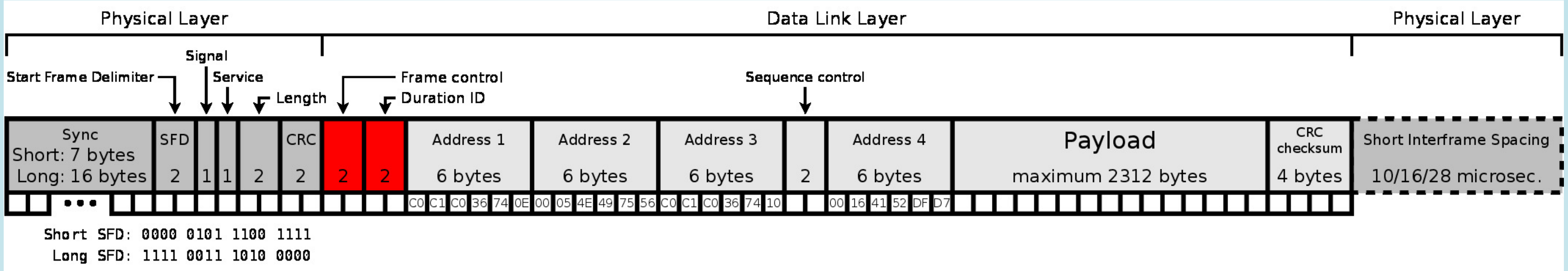


Frame format for **IEEE 802.11b**

- For the Physical layer, the standard comprises…
  - a preamble to synchronize the receiver including a SFD [1]
  - a Signal field, specifying the payload data rate (1 to 11 Mbit/s)
  - a Service field, may contain additional information
  - a Length field, specifying the transmission time for the payload in microseconds
  - a CRC field, which contains a checksum over the fields Signal, Service and Length

1. The Short Preamble Format is an optional standard which is not supported by all devices.

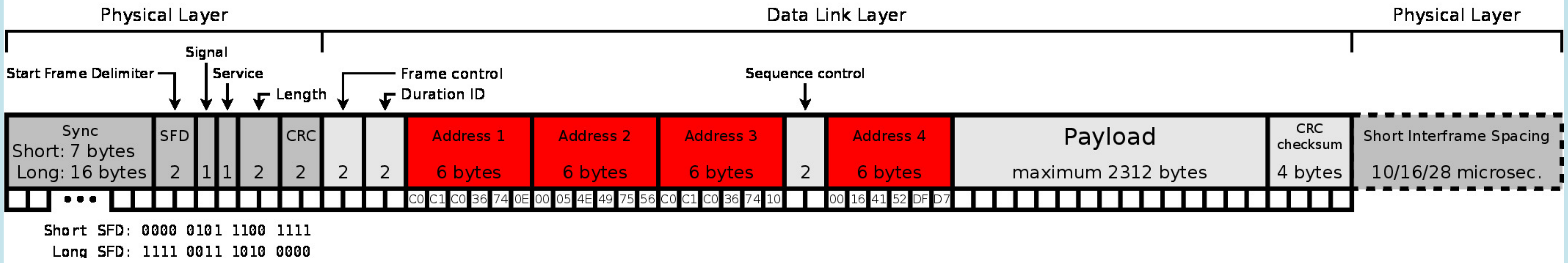
FRAME SIZE, FRAME CONTROL, AND NAV



- The field Frame Control (2 bytes) contains several smaller fields
  - Among other things, the protocol version, the type of frame (e.g., data frame or beacon), encryption with the WEP method
- The field Duration ID (2 bytes) contains a duration value for the update of the counter variable Network Allocation Vector (NAV) → Medium Access Control

- Maximum frame size of a WLAN frame (link layer part): **2346 bytes**

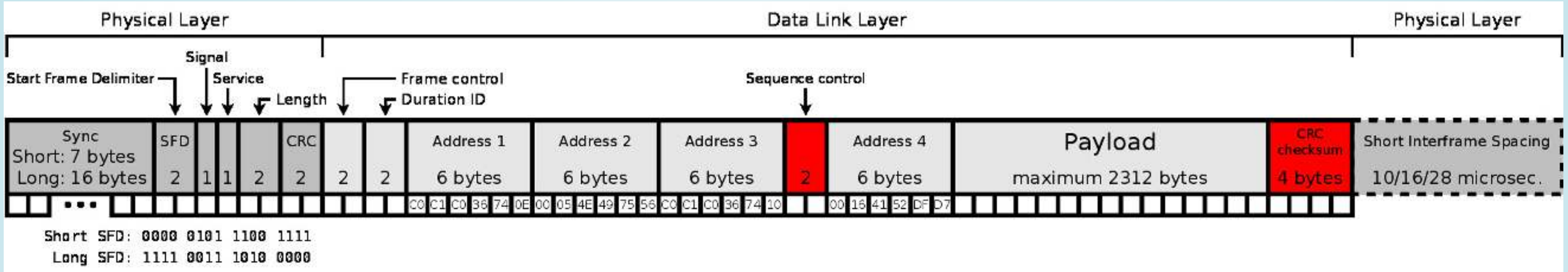
ADDRESS FIELDS AND SSIDS



Possible use of the address fields:

- Address 1: MAC of receiver (Destination Address)
- Address 2: MAC of sender (Source Address)
- Address 3: Used for filtering
- Address 4: is used for communication between APs in ESSID configuration or in a mesh network

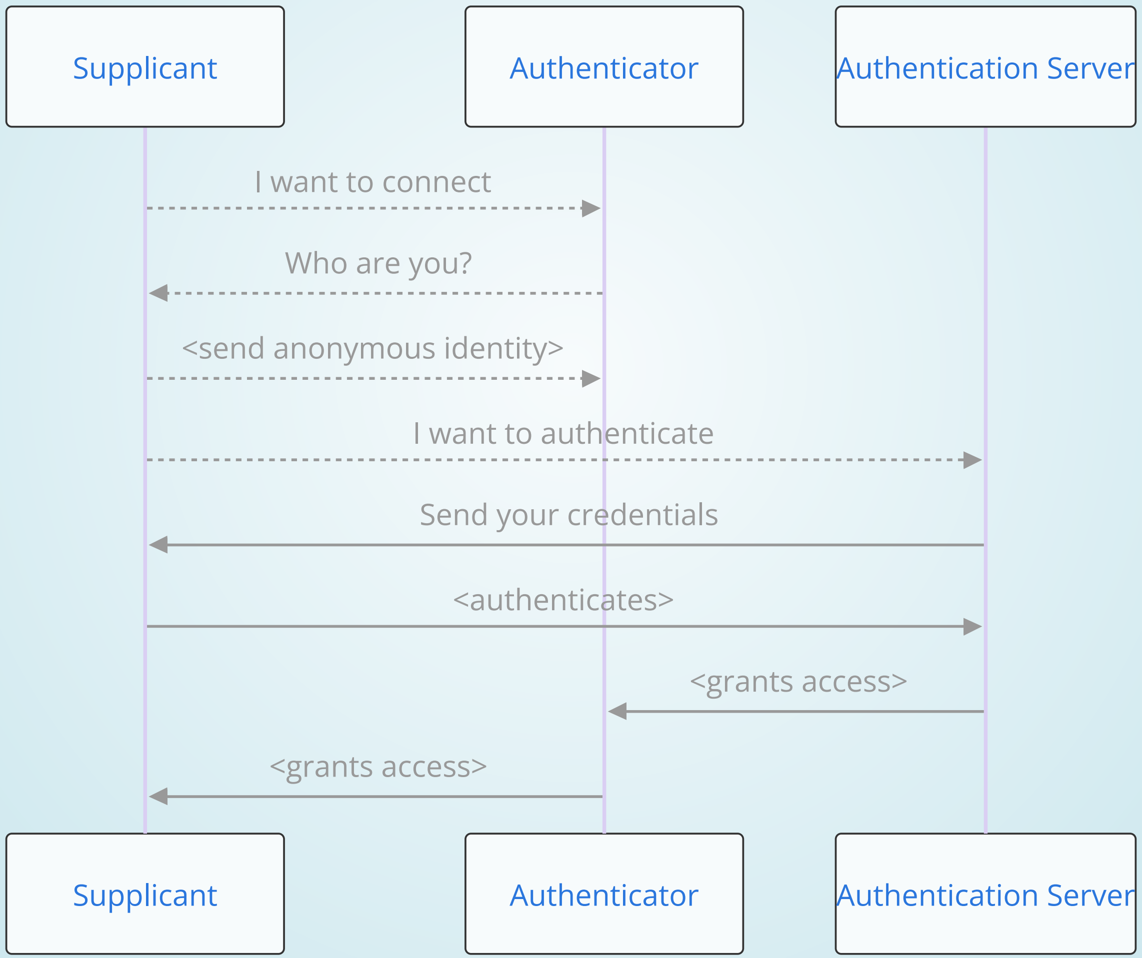
SEQUENCE CONTROL AND CRC



- The field Sequence Control (2 bytes) consists of a fragment number (4 bits) and a sequence number (12 bits)
  - If a frame has been split into several fragments, the sequence number is equal for all fragments
- The final field contains a CRC checksum (32 bits) that covers all fields, except the payload

IEEE 802.1X AND EAP

IEEE 802.1X is a standard for port-based link access control. In WLAN networks like for instances eduroam the Extensible Authentication Protocol (EAP) is used.



ADDRESSES

ADDRESSING IN THE DATA LINK LAYER

- The Data Link Layer protocols specify the format of the physical network addresses
- Terminal devices (Hosts) or Routers
  - Such devices must be addressable on Data Link Layer because they provide services at upper protocol layers
- Bridges and Switches do not actively participate in the communication
  - Typically they do not require an address, because their main purpose is filtering and forwarding of frames
  - Their address becomes relevant to establish a hierarchy ($\longrightarrow$ see slide) or providing a configuration interface
- Note: **Repeaters** and **Hubs** that operate only at the Physical Layer, have no addresses

MAC ADDRESSES

EUI-48 and EUI-64 MAC addresses can be formed according to the numbering spaces based on Extended Unique Identifiers (EUI) managed by the IEEE:

EUI-48 (e.g., Ethernet, WLAN, Bluetooth) and EUI-64 (Firewire, 6LoWPAN, Zigbee)

BROADCAST AND MULTICAST MAC ADDRESSES

- The least significant bit (LSB) of an addresses' first byte is called the Individual/Group (I/G) bit
- It indicates whether the frame is intended for a single receiver (unicast) or multiple ones (multicast/broadcast)
- MAC broadcast address
  - In IEEE 802 networks all 48 bits of this MAC address have the value 1
  - Hexadecimal notation: FF-FF-FF-FF-FF-FF
- Frames with the I/G bit set are sent only once but forwarded to multiple (potentially all) ports of the switch

UNIQUENESS OF MAC ADDRESSES

- Each MAC address is intended to be permanently assigned to a network device and unique
  - But it is often possible to modify MAC addresses by software
- T
  r
  t

MAC addresses	Manufacturer	MAC addresses	Manufacturer
00-20-AF-xx-xx-xx	3COM	00-0C-6E-xx-xx-xx	Asus
00-00-0C-xx-xx-xx	Cisco	08-00-2B-xx-xx-xx	DEC
00-01-E6-xx-xx-xx	Hewlett-Packard	00-02-B3-xx-xx-xx	Intel
00-04-5A-xx-xx-xx	Linksys	00-04-E2-xx-xx-xx	SMC
00-03-93-xx-xx-xx	Apple	00-50-8B-xx-xx-xx	Compaq
00-02-55-xx-xx-xx	IBM	00-09-5B-xx-xx-xx	Netgear

- T
  independently for their network devices
  - That address space allows $2^{24} = 16,777,216$ individual device addresses per OUI for IEEE 802 devices

SECURITY ASPECTS OF MAC ADDRESSES

- For WLAN, MAC filters are often used to protect the Access Point
  - In principle, this makes sense, because the MAC address is the unique identifier of a network device
- However, the security level of MAC filters is low because MAC addresses can be modified via software
  - The method is called MAC spoofing

Working with MAC addresses under Linux

- Read out the own MAC address(es): `ip link` or `ifconfig`
- Read out the MAC address(es) of the neighbors (mostly the Routers): `ip neigh`
- Set MAC address: `ip link set dev <Interface> address <MAC Address>`

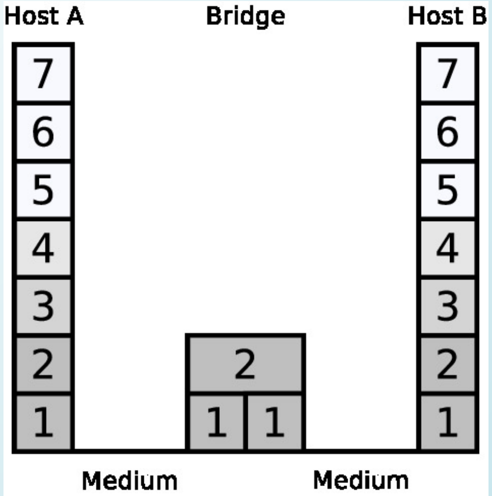
SWITCHING

DEVICES

- What is the purpose of the devices on Layer 1?
- Which additional functionalities can be introduced on Layer 2?

DEVICES OF THE DATA LINK LAYER: BRIDGES

- Remember: Devices of the Physical Layer increase the length of physical networks
- For connecting different physical networks, bridges are required
- A bridge has only 2 ports
  - They typically connect networks based on different technologies $\Longrightarrow$ see slides and
- Bridges with $>$ 2 ports are called Switch



DEVICES OF THE DATA LINK LAYER: BRIDGES

Virtual Bridges Bridges can be virtualized in software (e.g., to connect virtual machines)

- Simple bridges forward all incoming frames
- Bridges and switches check the correctness of the frames via checksums
- They operate transparently

EXAMPLE: WLAN BRIDGE

- Integrates network devices with RJ45 jacks (e.g., network printers, desktops, gaming consoles,...) into a wireless local area network (WLAN)
- Connects a cable-based network with a wireless network

EXAMPLE: LASER BRIDGE

- Connect two sites via laser
  - Each site is equipped with a transmitter (TX) and a receiver (RX) ($\longrightarrow$ Transceiver)
  - Allows for a high data rate
  - Requires line of sight

Source: http://www.made-in-zelenograd.com and http://www.laseritc.ru

Interesting build instructions for your own laser bridge

- https://hackaday.com/2017/04/19/go-wireless-with-this-diy-laser-ethernet-link/
- http://blog.svenbrauch.de/2017/02/19/homemade-10-mbits-laser-optical-ethernet-transceiver/

FORWARDING

LEARNING BRIDGES

- The forwarding table is not complete all the time
  - This is not a problem, because the table is only used for optimization
    - If no entry for a given address exists, the frame is typically sent on all ports

FORWARDING STRATEGIES

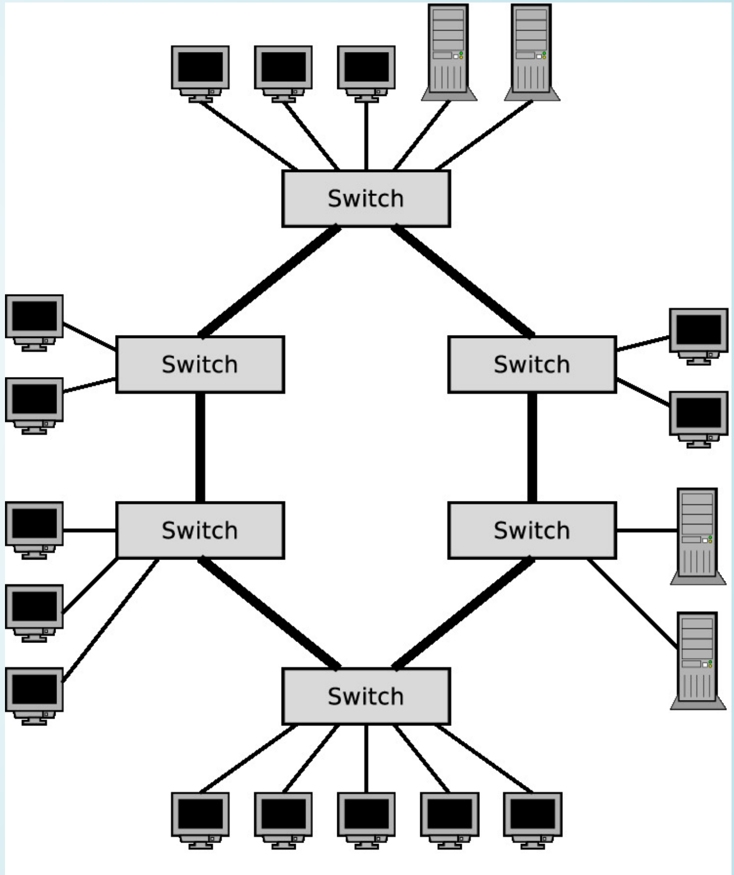
- A switch can implement different forwarding strategies:
  - Store-and-Forward
    The whole frame is received and buffered. After checking its integrity it is forwarded
  - Cut-Through
    As soon as the destination address field has been received, the frame is forwarded towards the receiver
  - Adaptive Cut-Through
    Cut-Through strategy is used unless a certain error threshold is reached ($\longrightarrow$ store-and-forward)
  - Fragment-Free-Cut-Through
    If the first 64 bytes are received without an error, the frame is forwarded

LOOPS

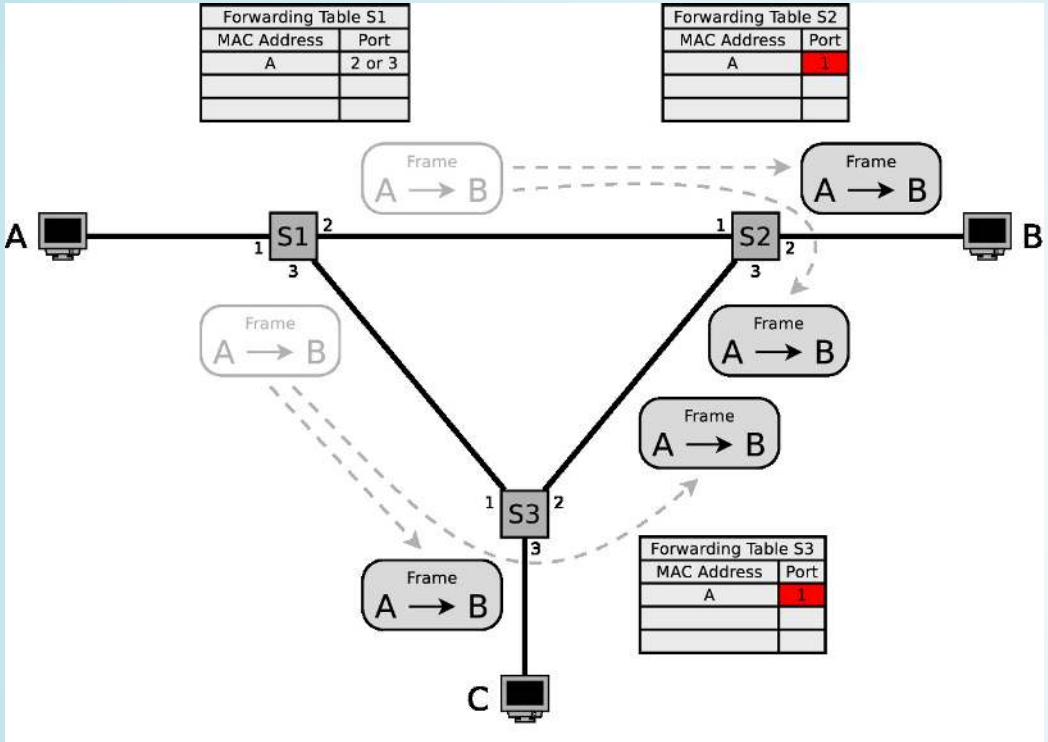
LOOPS ON THE DATA LINK LAYER

Loops are a potential issue on the Data Link Layer:

- On the Data Link Layer only one path per destination should exist at one point in time
  - Otherwise frames get duplicated and arrive multiple times at the destination
- Loops can reduce the performance of the network or even lead to a network failure
  - On the other hand, redundant connections serve as a backup in case of a cable failure



EXAMPLE OF LOOPS IN A LAN



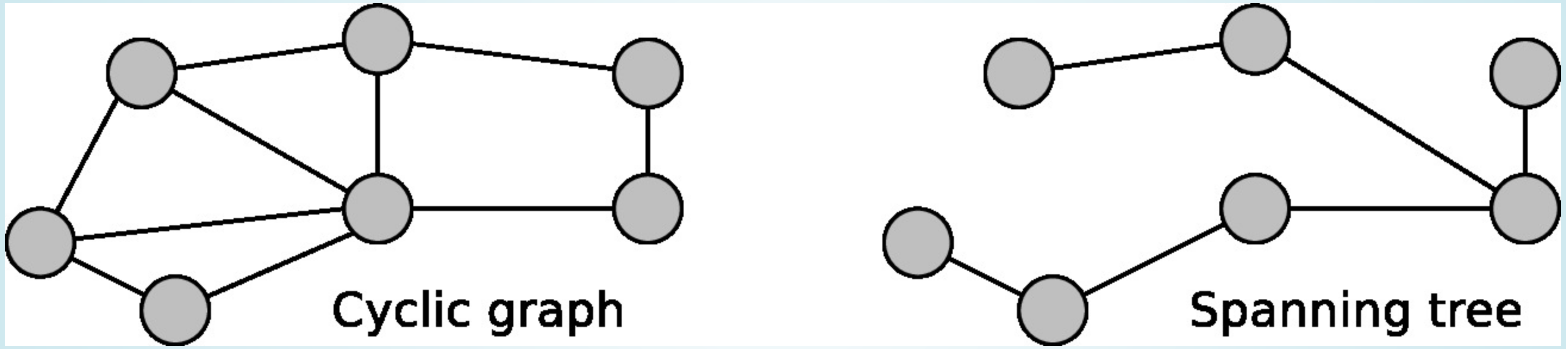
- Ethernet does not contain any TTL or HopLimit
  - Therefore, this loop will not stop until the tables in the switches contain an entry for node B

Similar examples can be found here:

- *Olivier Bonaventure*. http://cnp3book.info.ucl.ac.be/2nd/html/protocols/lan.html
- *Rüdiger Schreiner*. Computernetzwerke. Hanser (2009)

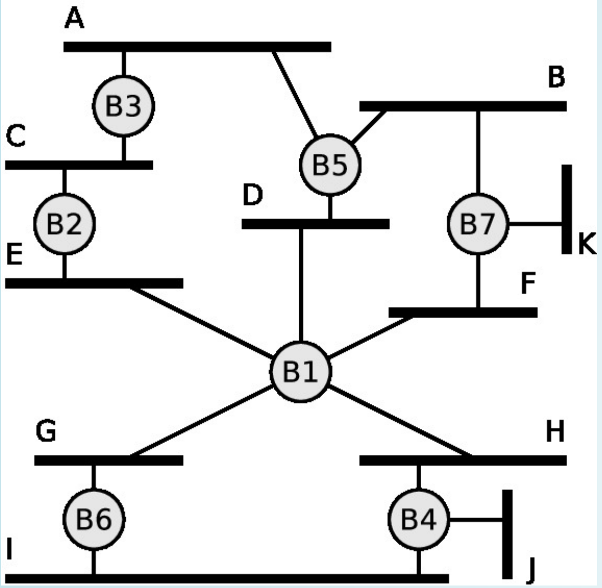
HANDLE LOOPS IN THE LAN

- Bridges need to be able to handle loops
- Solution: create logical hierarchy



- A computer network, which consists of multiple physical networks, is a graph that may contain loops
  - The spanning tree is a subgraph of the graph that covers all nodes, but is cycle-free, because edges have been removed
  - The implementation of the algorithm is the Spanning Tree Protocol (STP)

SPANNING TREE PROTOCOL



Source: Peterson, Davie. *Computernetze*

The STP was developed in the 1980s by Radia Perlman at Digital Equipment Corporation (DEC)

- The figure contains multiple loops
  - Via the STP, a group of bridges can reach an agreement for creating a spanning tree
    - By removing single ports of the bridges, the computer network is reduced to a cycle-free tree
- The algorithm works in a dynamic way
  - If a bridge fails, a new spanning tree is created

The protocol and format of the configuration messages are described in detail in the standard IEEE 802.1D

SPANNING TREE PROTOCOL – BRIDGE ID

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

- For the functioning of STP, each bridge needs an unique identifier
  - Length of the identifier (bridge ID): 8 bytes
  - 2 different implementations of the bridge ID exist

1. Bridge ID according to IEEE

- The bridge ID consists of the bridge priority (2 bytes) and MAC address (6 bytes) of the bridge port with the lowest port ID
  - The bridge priority can be set by the administrator himself and can have any value between 0 and 65,535
  - Default value: 32,768

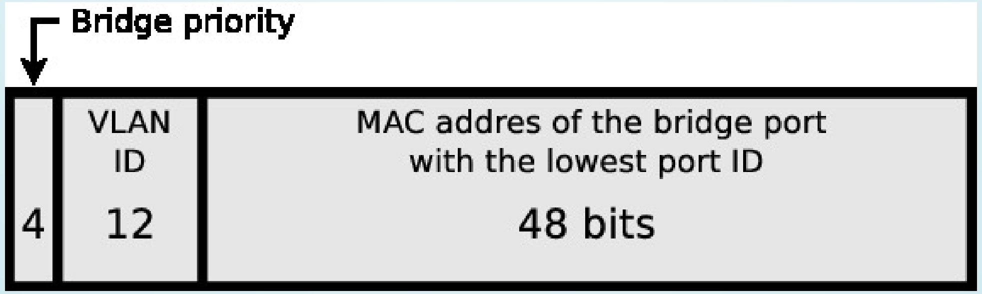
Bridge priority	MAC addres of the bridge port with the lowest port ID
16 bits	48 bits

SPANNING TREE PROTOCOL – CISCO BRIDGE IDS

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

2. Cisco extension of the bridge ID, introducing the Extended System ID

- Cisco supports bridges where each virtual LAN (VLAN) creates its own spanning tree
- The original 2 bytes long part for the bridge priority is subdivided
  - 4 bits now represent the bridge priority
    ⟹ only 16 values can be represented
    ⟹ the value of the bridge priority need to be zero or a multiple of 4,096
    ⟹ `0000` = 0, `0001` = 4,096 ... `1110` = 57,344, `1111` = 61,440
  - 12 bits are called Extended System ID and encode the VLAN ID
    ⟹ The content matches the VLAN tag of the Ethernet frames
    ⟹ With 12 bits, 4,096 different VLANs can be addressed



SPANNING TREE PROTOCOL – FUNCTIONING

The path costs have been standardized by the IEEE, but can be adjusted manually

Data rate	Path costs
10.000 Mbps	2
1.000 Mbps	4
100 Mbps	19
16 Mbps	62
10 Mbps	100
4 Mbps	250

SUMMARY

You should now be able to answer the following questions:

- What are the tasks of the Data Link Layer and what are the sublayers?
- Which mechanisms exist to detect the mark a frame?
- Which information does a frame contain?
- What are the properties of a MAC address and how do it look for IEEE 802 networks?
- How does switching/forwarding work?
- What is the problem of loops on the Data Link Layer and how can it be tackled?