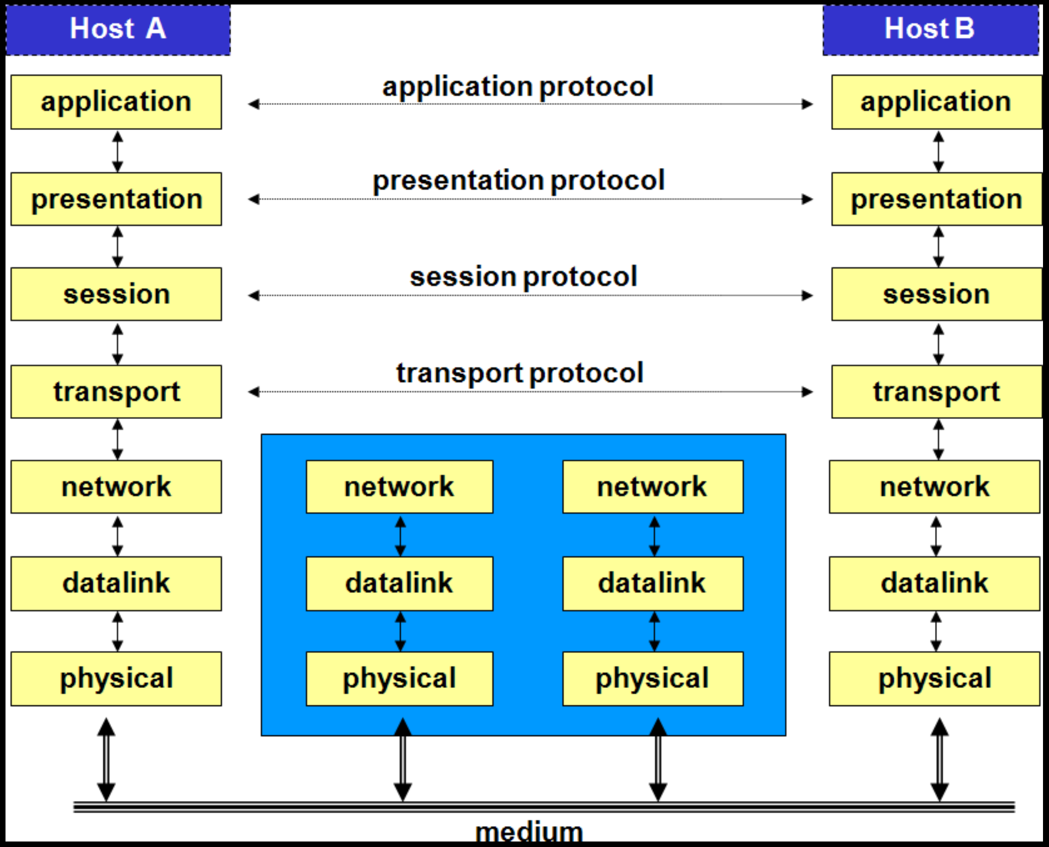
Data Link

The OSI model

In 1979, the International Organization for Standardization (ISO) developed a model to structure and standardise data communication and networks .The ISO's objective was a reference model whereby mutual communication between two systems could take place.

The ISO/OSI model (also called the 7-layer model), shows how system A can communicate with system B (2 systems from 2 different suppliers). Between these systems, different networks can be present; public as well as private networks.

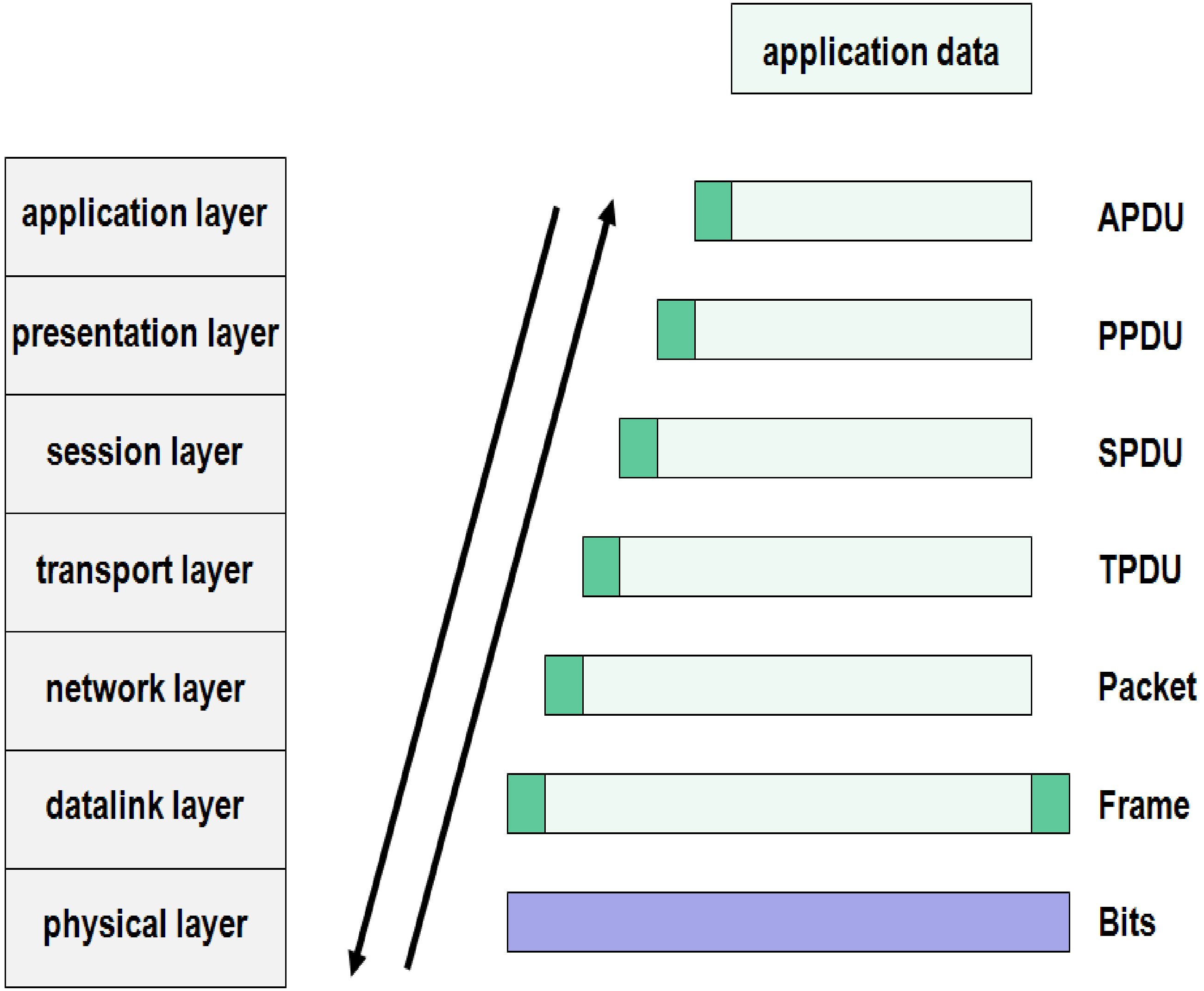
A public network is a network that is accessible by everyone, provided that the conditions that apply to this network are complied with. A private network is mostly company-specific.



The seven layers

- The OSI model consists of seven functional layers. Every layer contains a number of defined functions. A limited enumeration of the different layers is given below:
- PHYSICAL LAYER (layer 1) This layer ensures the connection with the medium via which the information is sent between two points in the network: this means that this layer provides the mechanical, electrical or optical entities that are required to realise, maintain and break off the physical connection
- DATA LINK LAYER (layer 2) The protocols of layer 2 specify how the frames eventually have to be sent over the network. Layer 2 maintains an error detection- and correction mechanism in order to be sure that transmission errors are handled and that data are correctly received on the other side.
- NETWoRK LAYER (layer 3) The addressing is configured on this level. This means that the network finds a route and avoids congestion within the network. The network layer ensures the transport of messages from one node to the other on the sender's route to the final receiver.
- TRANSPORT LAYER(layer 4) The transport layer is responsible for a reliable transmission of data. The transport layer ensures a logical connection between both end systems of the network (a logical point to point connection). This means that a faultless data transport can be realised whereby the data is received in correct order by the receiver.
- SESSION LAYER (layer 5) The control structure of the dialogue (session) between two applications over the network is provided for here, as well as the setting up and termination of such a session.
- PRESENTATION LAYER (layer 6) The protocols in layer 6 determine how data is represented: this is necessary as different computer systems represent numbers and characters in different ways. So, this layer ensures, amongst others, the conversion of character codes, e.g. from ASCII to EBCDIC.
- APPLICATION LAYER (layer 7) This layer provides service to applications that run for the benefit of network system users.

Protocol overhead in the OSI model



IEEE Standards

- IEEE802.2 Logical Link Control
- IEEE802.3 CSMA-CD (Ethernet)
- IEEE802.5 Token Ring
- IEEE802.11 Wireless LAN & Mesh (Wi-Fi certification)
- IEEE802.15 Wireless PAN
    - IEEE802.15.1 (Bluetooth certification)
    - IEEE802.15.4 (ZigBee certification)
- IEEE802.16 Broadband Wireless Access (WiMAX)
- IEEE802.16e (Mobile) Broadband Wireless Access
- IEEE802.16.1 Local Multipoint Distribution Service
- IEEE802.17 Resilient packet ring
- IEEE802.18 Radio Regulatory TAG
- IEEE802.19 Coexistence TAG
- IEEE802.20 Mobile Broadband Wireless Access
- IEEE802.21 Media Independent Handoff

Ethernet

Ethernet is the basis of LAN networks. Due to its huge market share, Ethernet, despite some disadvantages, scores over all alternative technologies.

Ethernet is only a specification of layers 1 and 2 in the OSI model. It is not a complete network protocol but a subnet on which other protocols such as TCP/IP can work.

A short historical overview:

- 1980: Digital Equipment Corporation, Intel and Xerox released the first Ethernet specification, version 1.0, under the name *Ethernet Blue Book* or DIX standard. It defines *Thick Ethernet* in case of 10Mbps CSMA/CD. The first Ethernet controllers, based on the DIX standard, were available starting from 1982. The second and final version of the DIX standard, version 2.0, was released in November 1982: *Ethernet II*.
- 1983: The IEEE launches the first standard for Ethernet technology. It was developed by the 802.3 group of the IEEE802 committee and this under the name *IEEE802.3 Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Specifications*
- 1985: IEEE802.3a; definition of thin Ethernet 10Base2
- 1987: IEEE802.3d; Fiber Optic Inter Repeater Link (FOIRL). Use of two fibre optic cables to extend the distance between 10 Mbps repeaters up to 1000m.
- 1987: IEEE802.3e; 1Mbps over twisted pair
- 1990: IEEE802.3i; release of the popular 10Base-T; 10Mbps over UTP category 3
- 1993: IEEE802.3j; 10Base-F: distances greater than 2 km over fibre optic
- 1995: IEEE802.3u; 100Base-T and 100Base-F
- 1997: IEEE802.3x: full-duplex Ethernet
- 1997: IEEE802.3y; 100Base-T2

Ethernet

The most important functions of ETHERNET are:

Physical layer

Sending and receiving serial bit streams over a medium.

Detecting collisions.

MAC sublayer:

*access mechanism to the network (CSMA/CD).

*building of the data frames.

LLC sublayer:

*data reliability.

*data channels for higher-level applications

A short historical overview (ctd):

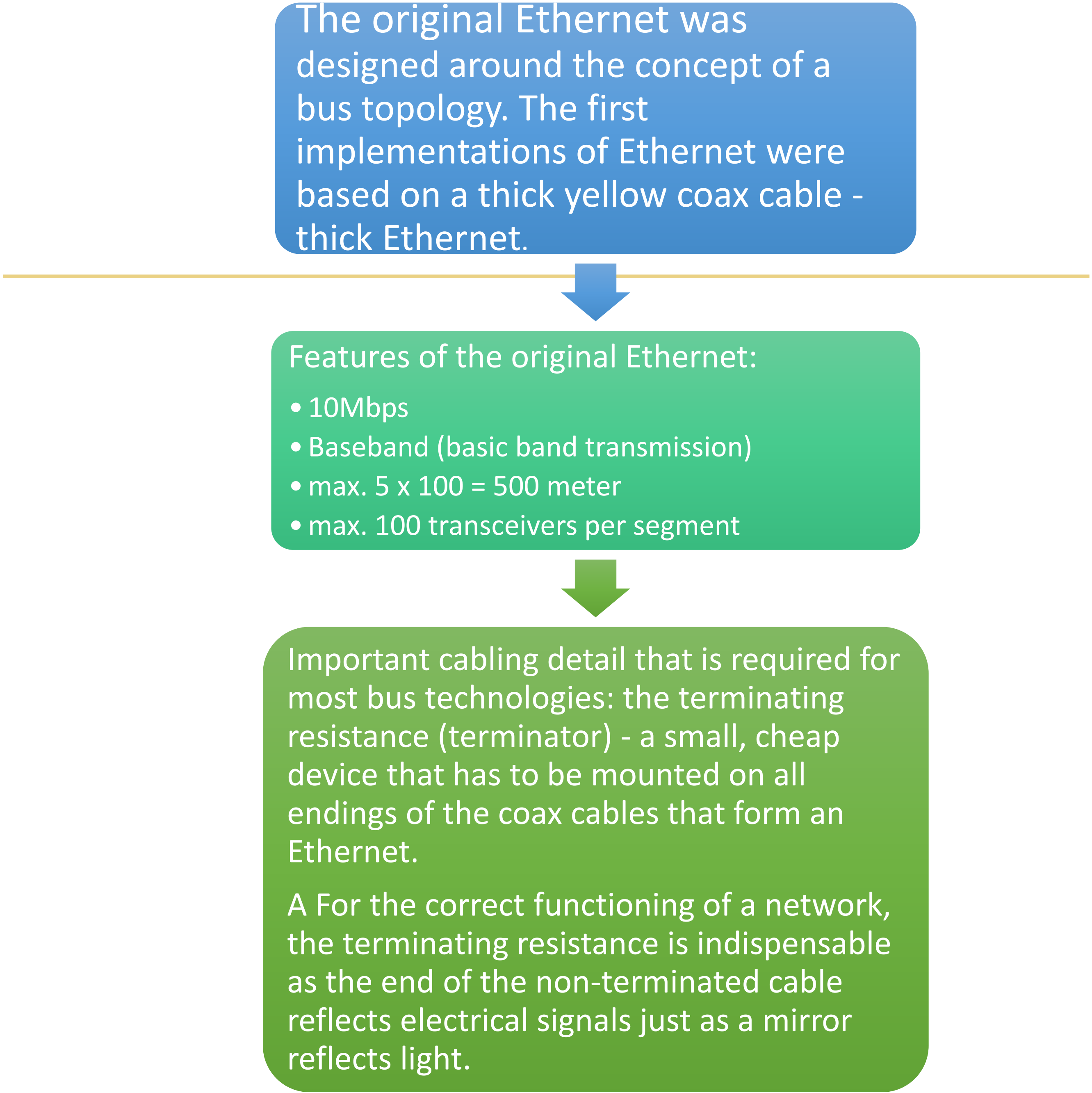
- 1999: IEEE802.3ab; Gigabit Ethernet over twisted pair
  - 1999: IEEE802.3ac; 802.1Q: definition of the Q tag with VLAN and priority information.
- 2003: IEEE802.3af; Power over Ethernet
  - 2006: IEEE802.3an; 10GBase-T
- 2006: IEEE802.3aq; 10GBase-LRM, Ethernet over multimode fiber

Ethernet physical implementations

The most important implementations:

- Thick Ethernet (10Base5)
- Thick Ethernet (10Base2)
- Broadband Ethernet (10Broad36)
- Ethernet over twisted pair (10Base-T)
- Ethernet over Fiber (10Base-F)
- Fast Ethernet (100Base-T / 100Base-F)
- Gigabit Ethernet (1000Base-T)
- Wireless Ethernet

Implementation on coax cable



The original Ethernet was designed around the concept of a bus topology. The first implementations of Ethernet were based on a thick yellow coax cable - thick Ethernet.

Features of the original Ethernet:

- 10Mbps
- Baseband (basic band transmission)
- max. 5 x 100 = 500 meter
- max. 100 transceivers per segment

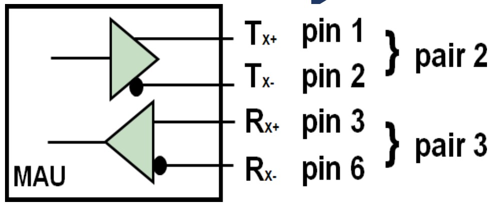
Important cabling detail that is required for most bus technologies: the terminating resistance (terminator) - a small, cheap device that has to be mounted on all endings of the coax cables that form an Ethernet.

A For the correct functioning of a network, the terminating resistance is indispensable as the end of the non-terminated cable reflects electrical signals just as a mirror reflects light.

Fast Ethernet

Implementations based on twisted pair

- A major problem with coax is that only half duplex communication can be applied. Ethernet has switched to a topology where twisted pair can also be used: all stations are connected to one or more central hubs. This way, a star topology can be worked out. The maximum segment length between a participant and a hub is 100 meters.
- The variants on twisted pair have evolved from 10Base-T (10Mbps) to 100Base-T (100Mbps) to 1000Base-T (1000Mbps).
- The MAU, developed for twisted pair, is equipped with 4 data pins: 2 for sending, 2 for receiving. This is the basis for full duplex Ethernet. In principle, any point-to-point communication is possible, but every host has to be connected directly with a structure element: a hub or a switch.



Fast Ethernet

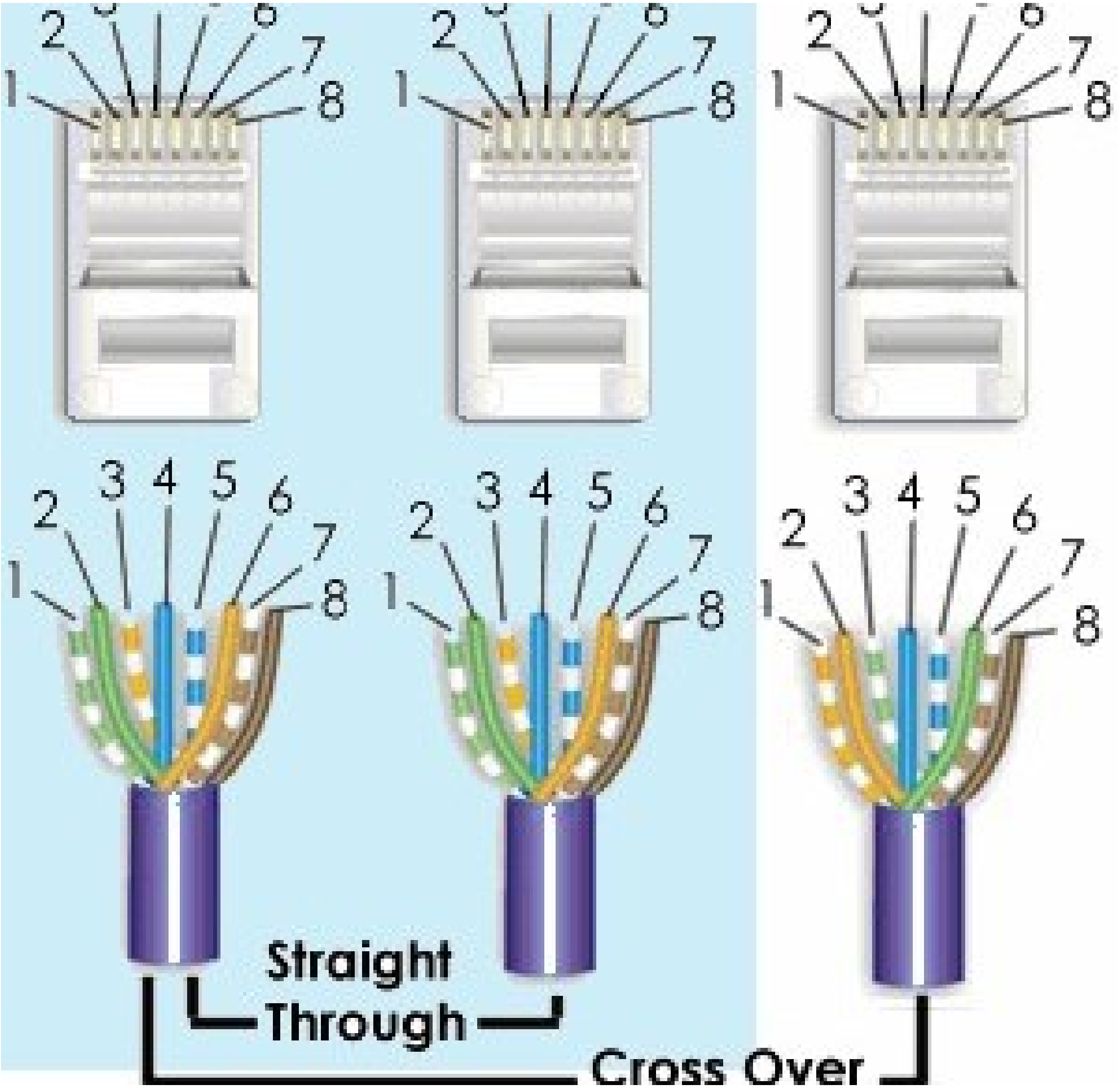
- The UTP cable, e.g. CAT5 (Class 5) UTP (Unshielded Twisted Pair), supports speeds up to 100Mbps. The cable consists of 8 wires, arranged in 4 pairs. The 4 pairs can be identified as 1 is always completely colored and the other one has the same color with white parts in between. Only 2 of the 4 pairs are used in 10/100Base-T (pair 2: orange/white and orange and pair 3: green/white and green).
- The IEEE specification for Ethernet 10/100Base-T requires that the one used pair is connected to pin 1 and pin 2 of the connector while the second pair is connected to pin 3 and pin 6. The other two unused pairs will be connected to pin 4 and 5 and on pin 7 and 8.

4B/5B

Data stream:	0111010000100000
4 bit pattern:	0111 0100 0010 0000
5 bit code:	01111 01010 10100 11110

Cables

- The straight-through cable, also called patch cable, is the cable that we get when we connect both sides of the cable pair 2 with pin 1 and pin 2, while pair 3 is connected with pin 3 and pin 6. This cable can be used for connections between the patch panel and the hub/switch, the PC and the hub/switch or the PC and the wall.
- A cross-over cable is required to set up the PC-PC connections (connection of two end elements) and to secure connections between hub/switch and another hub/switch (connection between two structure elements). In order to make a cross-over cable, we have to switch the used pairs.



Gigabit Ethernet

Pin	Colour	Function
1	green with white	+BI_DA
2	green	-BI_DA
3	orange with white	+BI_DB
4	blue	-BI_DB
5	blue with white	+BI_DC
6	orange	-BI_DC
7	brown with white	+BI_DD
8	brown	-BI_DD

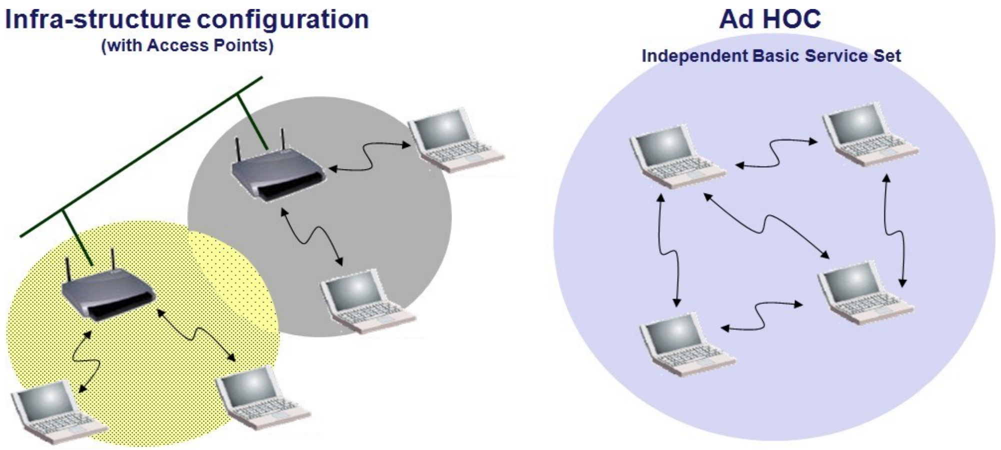
- Gigabit Ethernet targets a data rate of 1000Mbps. In order to realise this, the technology has to be adapted. First, 1000Base-T codes two bits per clock signal (00, 01, 10 and 11) and uses four voltage levels for this.
- Furthermore, 1000Base-T uses all four data pairs of an Ethernet cable. The four data pairs are applied here bi-directionally. Data are sent or received via all four data pairs.
- Gigabit Ethernet therefore still uses the 100Base-T/Cat5 clock rate of 125MHz. The data rate of 1000Mbps is reached as 2 bits are being processed for every clock pulse and this is done via four data pairs.
- This modulation technology is called 4D-PAM5 and currently uses five different voltage levels. The fifth voltage level is used for the error mechanism.
- The table shows the Gigabit Ethernet pin configuration. BI stands for bi-directional while DA, DB, DC and DD stands for data A, data B, data C and data D.

Wireless LAN

- **IEEE802.11**

IEEE defines different standards for wireless LAN in their IEEE802.11 description. The radio connections for a Wireless LAN take place in the 2.4 GHz frequency band, the so-called ISM band (Industrial, Scientific and Medical) or in the 5 GHz band. No licences are required for this. A Wireless LAN uses the so-called spread spectrum technology.

- This technology is specifically meant for fault-prone transmission channels. This is important as these frequency bands (especially the 2.4 Ghz) are also used by many other devices, e.g. Bluetooth.
- A wireless network is in general much less fast than a fixed wired network. A major advantage is flexibility.
- With regard to physical implementation, IEEE802.11 provides the infrastructure configuration or the ad hoc configuration.



Infrastructure configuration

Infrastructure configuration is the configuration whereby a wireless access point is used to connect a wireless LAN with a cabled LAN. The wireless access point functions as central point for the routing of the wireless data traffic. Wireless-enabled computers that are included in an infrastructure mode form a group that is called a Basic Service Set (BSS).

Amaximum of 64 individual computers can be included in a BSS. This is because the capacity of the wireless access point is limited to 64 clients. The complete wireless network has a unique SSID (Service Set Identifier) and is also has a network name.

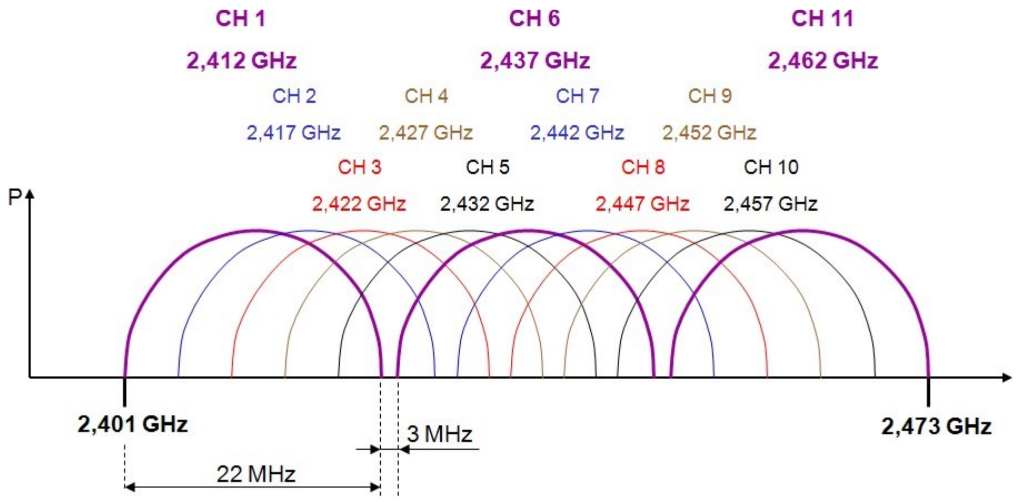
Ad hoc or peer-to-peer relates to a wireless configuration in which every participant communicates directly with the other. An actual organisation of the network is therefore not possible here. An ad hoc wireless LAN consists of a group of apparatuses each equipped with a wireless adaptor that is directly connected to each other and form an independent wireless LAN in this way.

WLAN standards

- Different standards are defined within the IEEE 802.11. These standards use different modulation technologies in order to obtain improved transmission speeds.

STANDARD	FREQUENCY BAND	DATA TRANSMISSION
IEEE802.11b	2.4GHz	11Mbps
IEEE802.11g	2.4GHz	54Mbps
IEEE802.11a	5GHz	54Mbps
IEEE802.11h	5GHz	54Mbps
IEEE802.11n	5GHz and/or 2.4GHz	600Mbps

IEEE802.11b/g



- IEEE802.11b/g uses the 72 MHz band part of the 2.4 GHz band. 11 channels of 22MHz band are defined here, in accordance with the FCC rules. Theoretically this would mean that the bandwidth for these 11 channels is 242 Mbps (11x22 Mbps). In reality, this has to be reviewed as these channels overlap for a large part. Figure 2.5 shows that there are only three non- overlapping channels: channel 1, channel 6 and channel 11.

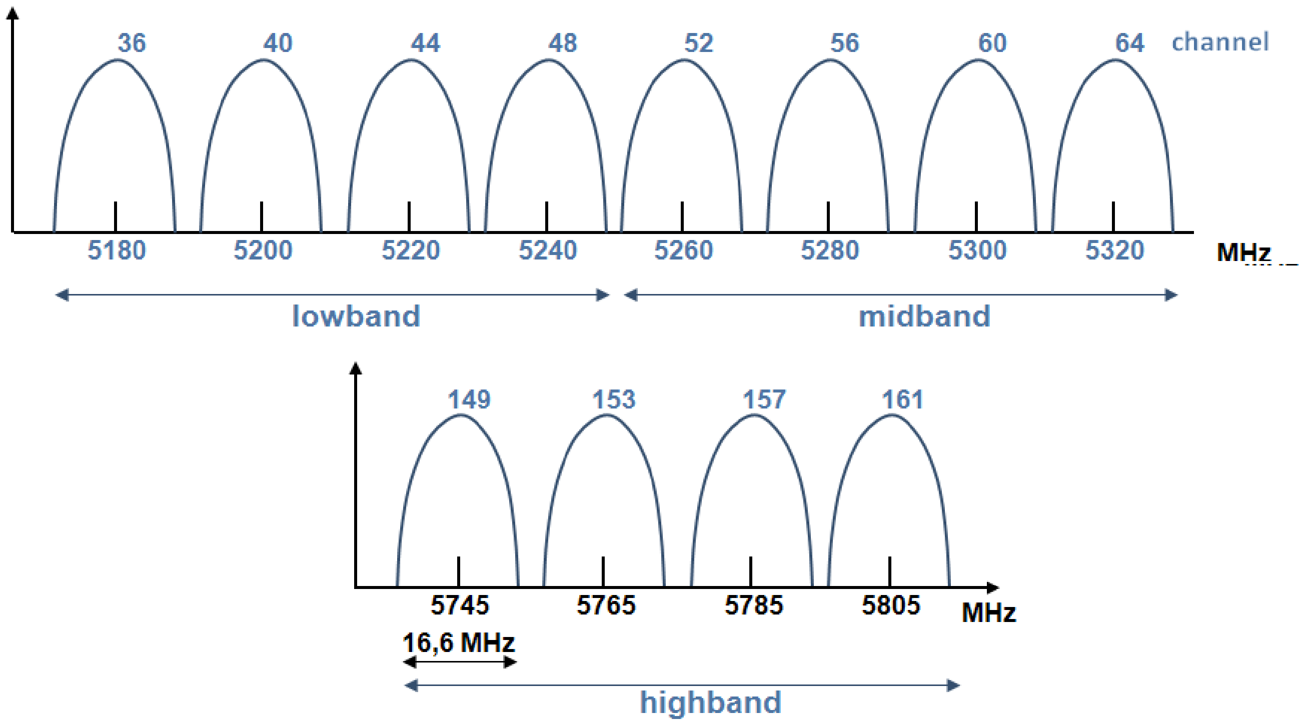
- ETSI defines a slightly wider frequency band for Europe, including 13 channels of 22 MHz band. We can use 4 barely overlapping channels in Europe. These are channel 1,5,9 and 13.

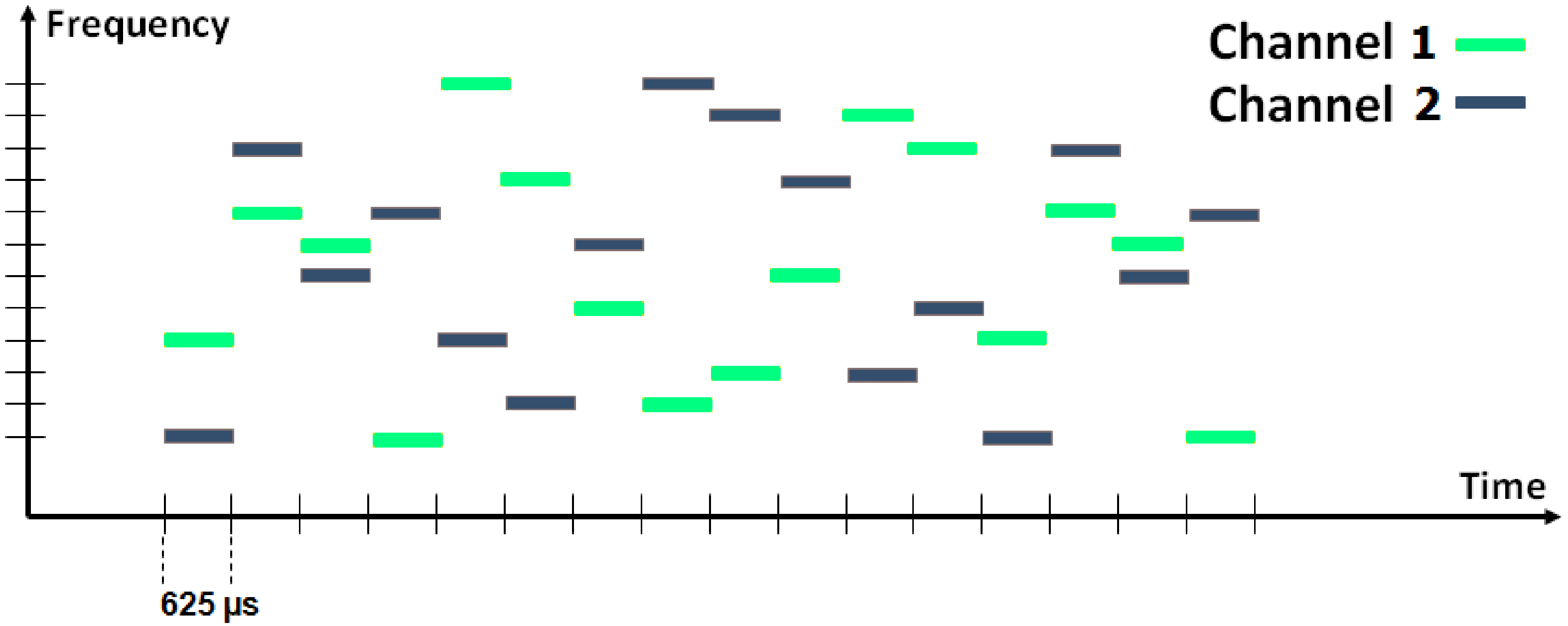
- IEEE802.11b supports a maximum speed up to 11 Mbps. IEEE802.11g supports a maximum speed up to 54 Mbps. The speed is decreased dynamically in case of a bad connection or great distance to the access point.

IEEE802.11a/h

- IEEE802.11a uses the complete 5GHz band. With the application of OFDM (Orthogonal Frequency Division Multiplexing), the maximum (theoretical) speeds of up to 54Mbps are reached. Within Europe, 8 non-overlapping channels of 20MHz wide can be used over the two lowest bands of the 5GHZ UNII band.

- As opposed to the USA, the use of the 5GHz band in Europe has quite a few restrictions. Therefore, the IEEE802.11a was converted into the IEEE802.11h. Two important protocols were added in order to eventually comply with the European regulations:
  - DCS (Dynamic Channel Selection):the AP will automatically look for another channel if it appears that the channel is used by another application.
  - TPC (Transmit Power Control): just the required capacity is transmitted





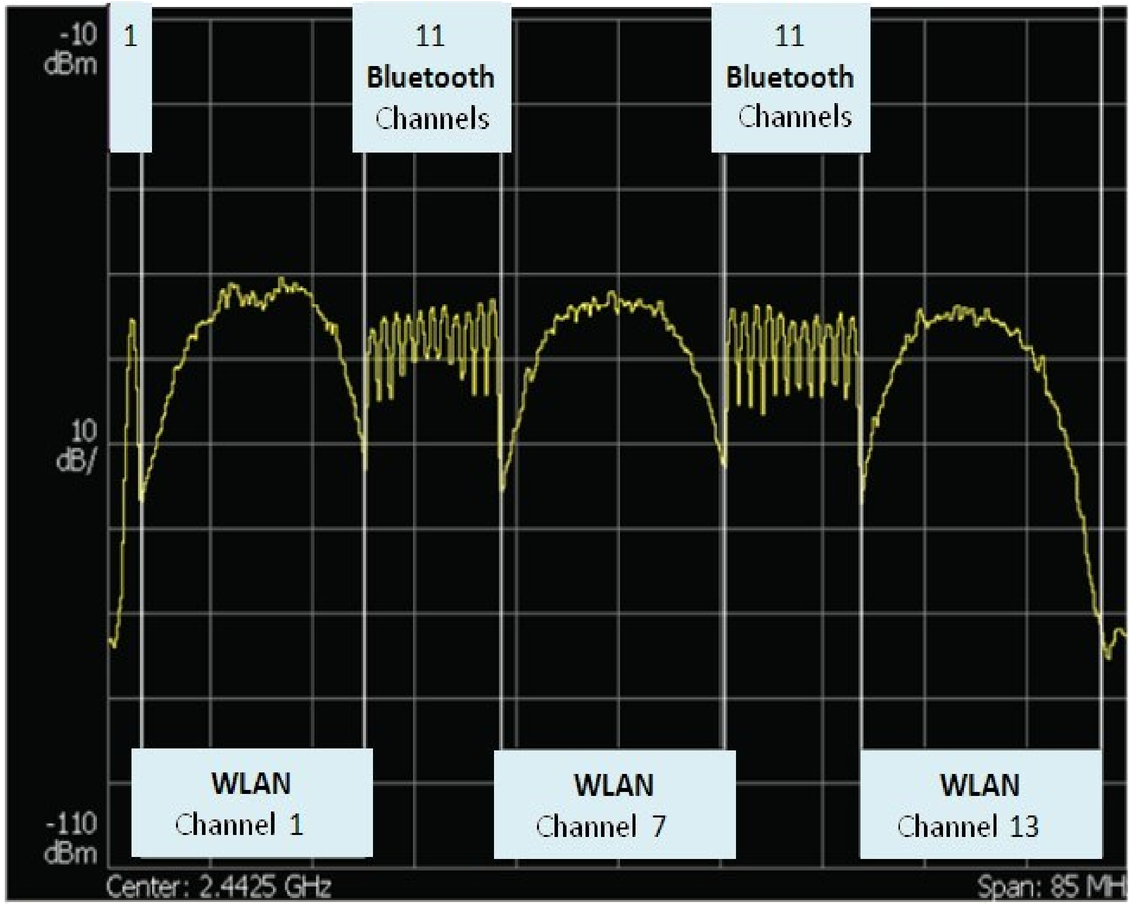
Bluetooth

- The basic technology (two bottom layers of the OSI model) is standardised in the IEEE802.15.1. Moreover, the Bluetooth SIG (Special Interest Group) defines different application profiles, like serial communication and transmission of Ethernet data frames.

- Bluetooth uses the 2.4 GHz licence-free ISM band. As opposed to WLAN, the data to be sent are not spread out over a wider frequency band but FHSS (Frequency Hopping Spread Spectrum) is applied. The 2.4 GHz band is divided over 79 channels of 1 MHz. Figure 2.7 shows the functioning of FHSS. 1600 hops per second can be carried out. Each time, every data frame is sent on another frequency. This means that different logic channels can be active in parallel.

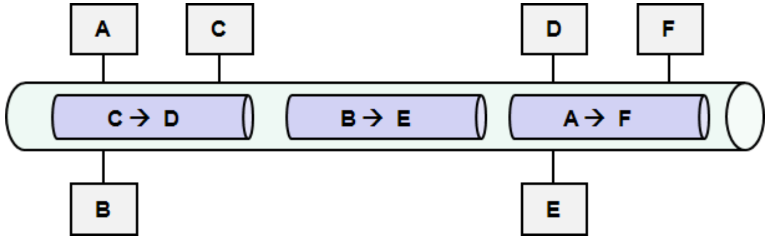
Coesistence IEEE802.11 and Bluetooth

- A great advantage of the use of Bluetooth in the industry is the perfect co-existence with WLAN. If there is interference on a Bluetooth frequency as a WLAN channel is active on the same frequency, then Bluetooth can avoid this/these frequency (ies). As this is a frequently occurring issue, Bluetooth has integrated an automated co-existence mechanism: Adaptive Frequency Hopping (AFH).
- This mechanism enables Bluetooth to suspend certain 'bad' frequencies temporarily from the hopping list. Figure 2.8 shows how there is enough space in case of a full 2.4GHz band where three separate WLAN channels are active. The WLAN channel uses a statistic frequency band. Bluetooth can adapt and choose from adequate number of frequencies to avoid interference.

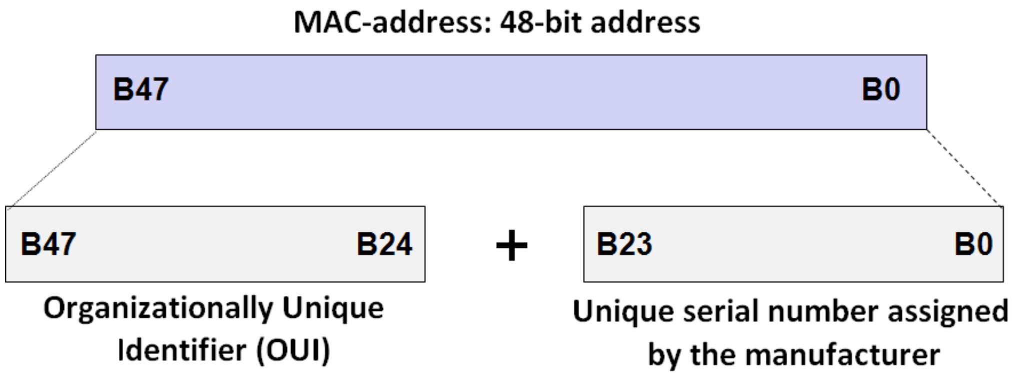


Packet Switching

- Packet switching is mostly applied for computer-to-computer communication. In computer networks, a random quantity of data is not trans- ported uninterruptedly. Instead, the network system divides the data into small blocks and packets that are sent separately. Computer networks are therefore also called packet switching networks. There are two reasons to choose usage of packets:
- Sender and receiver have to coordinate the transmission. In case of transmission errors, lot of data may be lost. If the data is divided into smaller blocks, then it is easier for the sender and receiver to determine which blocks are still intact on arrival..
- Several computers make common use of underlying links and hardware. A network has to ensure that all computers have equal direct access to a shared communication facility. A computer cannot occupy a shared resource for longer than it takes to send one packet.



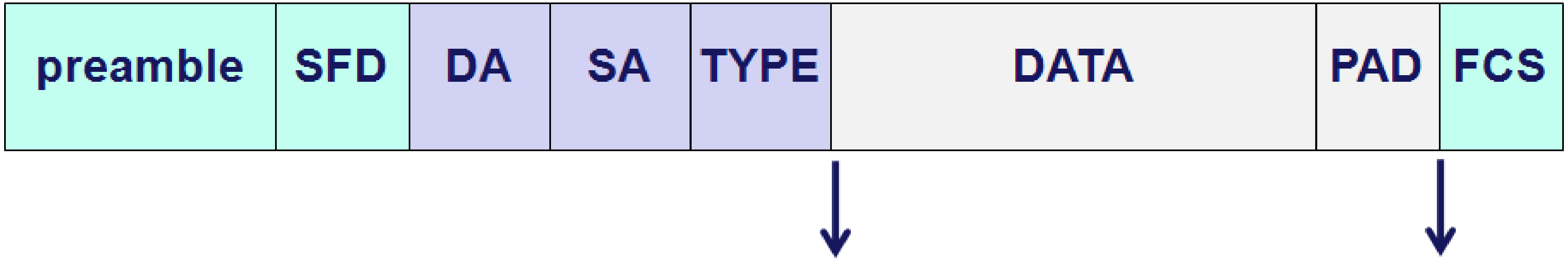
MAC address


MAC-address: 48-bit address
B47
B0
B47
B24
+
B23
B0
Organizationally Unique Identifier (OUI)
Unique serial number assigned by the manufacturer

- On a common transmission medium of a LAN, every station has to have a unique address.
- Every participant has an Ethernet address, a physical address that is unique for the network card: the MAC address (Medium Access Control Address).
- Every manufacturer of network cards gives each card a unique address number that is stored in the ROM of the card.
- The MAC address consists of 48 bits (6 bytes) and is divided into two groups of three bytes. The highest 24 bits form a manufacturer number issued by XEROC. There are 4194302 possible manufacturer numbers. Phoenix Contact, for example, is assigned manufacturer number 00A045h.
- The lowest 24 bits form a serial number. Every MAC address has to be unique.

The Ethernet dataframe

- An Ethernet frame consists of at least 46 actual data bytes and a constant number of 26 protocol bytes (overhead). This minimum number of data bytes is necessary for the definition of the slot time. following fields are defined in an Ethernet data frame:
- Preamble: is a series of 56 bits alternating with 1 and 0. These bits are used for synchronisation and give each participant the time to observe the activity on the bus before the actual data arrives.
- SFD: the start of frame delimiter (10101011), the last byte of the preamble, indicates to the receiver that the actual data is on its way.
- DA: the destination address. The destination MAC address field identifies the station or the stations that have to receive the message. This field takes 6 bytes of space. The destination address can be an individual, a multicast or a broadcast address. The MAC broadcast address is FF FF FF FF FF FF.
- SA: the source address. The source MAC address field identifies the station from where the message originates. This field is 6 bytes long.



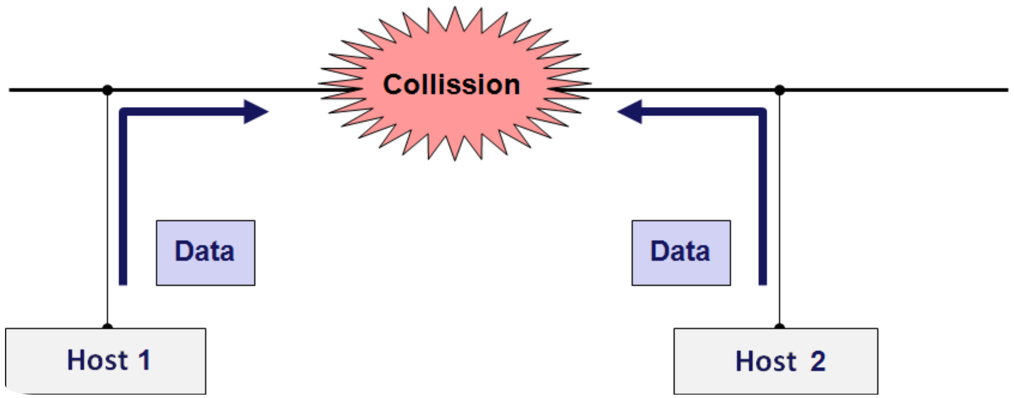
data field: min. 46 bytes, max 1500 bytes

Dataframe (ctd)

- The IEEE802.3 defines the field TYPE as LENGTH field in order to be able to send the number of actual data bytes.
- Xerox does not use type numbers below 1500 and as the maximum length of a data frame is 1500, no overlapping is possible and both definitions can be used.
- DATA: the data field contains the data to be sent. This data field is transparent- this means that the content of this field is completely free for Ethernet. Only the length has to be a minimum of 46 bytes and not more than 1500 bytes.
- PAD: the padding bits are random data bits that, if necessary, can be added to the data in order to reach the minimum required 46 bytes.
- FCS: the check sum is a 4-byte CRC value that the sender creates and sends. The receiver can check the integrity of the data with this code.

0600h	XNS
0800h	IP (Internet Protocol)
0806h	ARP protocol
0835h	Reverse ARP protocol
8100h	IEEE802 1.q tag frame (VLAN)

CSMA/CD



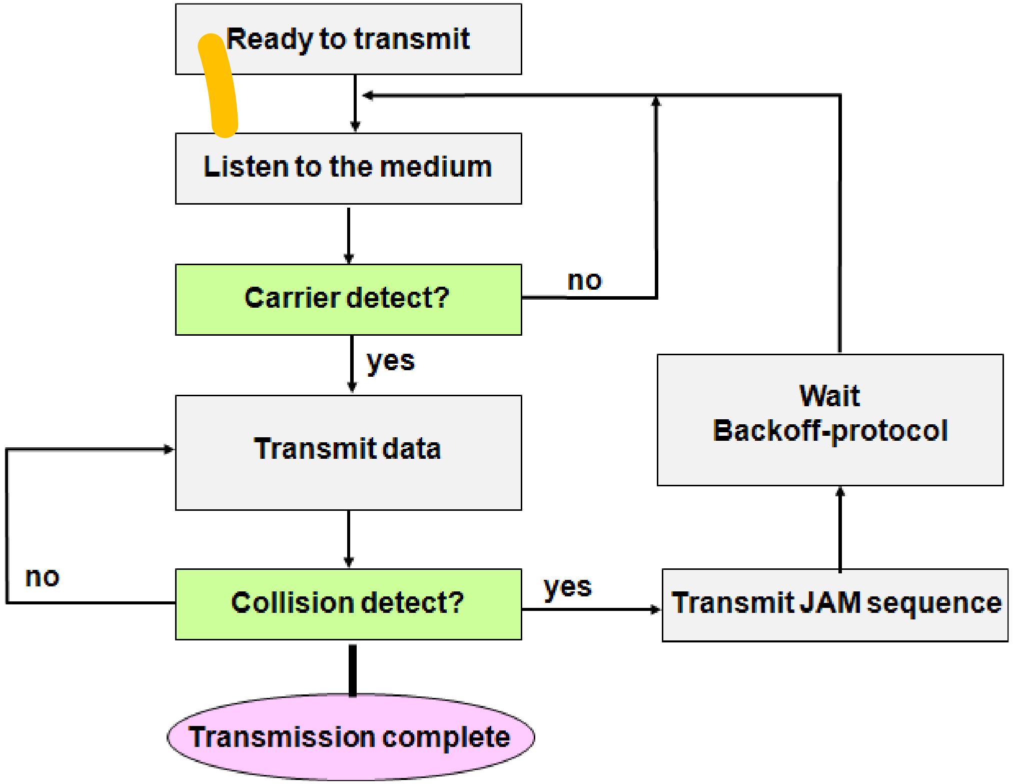
- Ethernet uses the CSMA/CD (Carrier Sense Multiple Access / Collision Detect) protocol. With CSMA/CD, two or more stations can use a common transmission medium. In order to send a data frame, a station has to wait for an ’idle period’- when the bus is inactive and not a single participant is sending data. It will then send a message that is heard by all other participants.
- If a second participant is sending a message at the same time, then a collision will be detected. The participant that detects a collision first, sends an error frame.

CSMA/CD flow

- A participant that wants to send data will first check the network on a *carrier*, or the presence of a station that is sending data. If an active carrier is detected, then the sending is delayed.

- If no active carrier is detected for a period that is equal to or greater than the interframe gap, then this station can start sending the message. During the sending of the message, the participant will continue to check the medium on collisions. A network interface therefore has to send data and check the medium at the same time. If a collision occurs, then the participant stops the sending immediately and a 32-bit jam sequence is sent. If the collision is detected early, then the frame preamble will be sent before the jam sequence is sent. This jam sequence is necessary in order to make sure that the length of the collision is sufficiently long so that all participants can observe the collision. After sending the jam sequence, the participant will have to wait for a random period of time before making a new attempt: this process is called Backoff.

- A few important additional definitions:
- Interframe gap: Ethernet participants have to plan a minimum period without activity ('idle period') between the sending of two frames. The minimum interframe gap is 96 bit times (9.6μs for the 10Mbps version, 960ns for 100Mbps Ethernet and 96ns for Gigabit Ethernet.
- Slot time: this parameter is defined as 512 bit times for the 10Mbps and the 100Mbps versions, and 4096 bit times for Gigabit Ethernet. The minimum transmission time for a complete data frame should be at least one slot time. The time required so that all participants can observe a collision, cannot be more than one slot time.

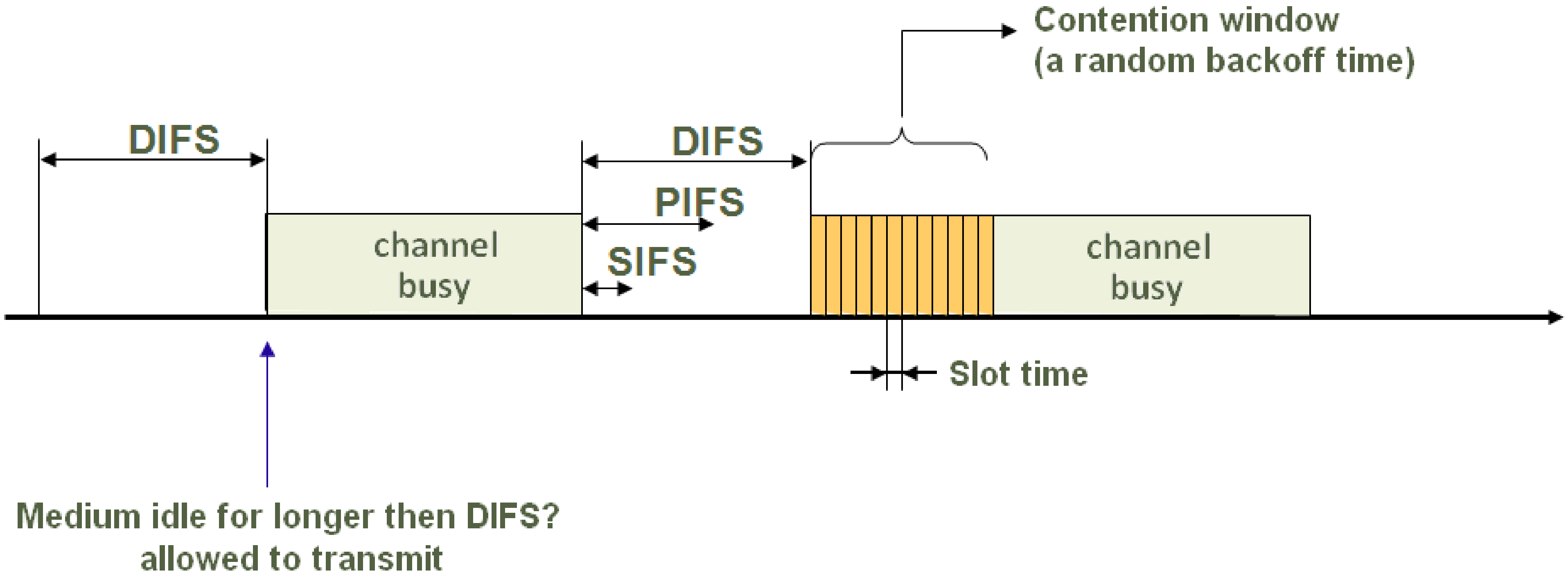


CSMA/CA

- The CSMA/CD technology of wired Ethernet cannot be applied to wireless Ethernet. The standard describes half-duplex radios, while sending the data it cannot be checked whether any collisions take place. In order to solve this, another technology is applied, namely CSMA/CA. Instead of detecting collisions, collisions will be avoided, CA: collision avoidance.

The chance of collisions is the greatest right after an occupied medium. That is why waiting times and a recovery phase are defined.

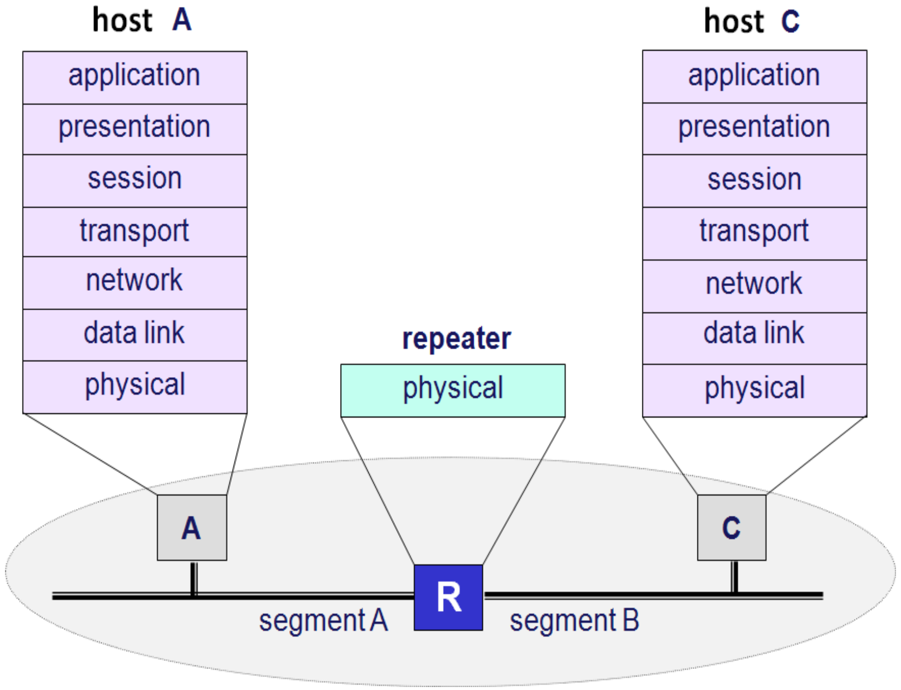
- SIFS (Short Interframe Spacing): shortest waiting time for medium access (thus highest priority). The access point uses this waiting time for the sending of ACK messages.
- PIFS (PCF Interframe Spacing): medium priority, this time is used for the polling actions of an access point.
- DIFS (DCF Interframe Spacing): lowest priority for medium access, applicable to normal participants on the wireless segment.



Structure elements for Ethernet: The repeater

- The maximum segment length of a LAN is determined by the used medium and the applied access mechanism. In order to cancel the length restriction, methods are rapidly searched to link several segments one after another. The first and most simple method is to use a repeater. A repeater is a signal amplifier that transmits packets transparently, independent of the package content. A repeater is used to connect two or more Ethernet segments together.

- Both segments can have a different medium. A 10Base-T based segment, for example, can be connected to a fibre segment by means of a repeater. Another important feature of a link on the basis of a repeater is that not only the data bits are transmitted but also any collisions and signal errors. Network segments that are connected mutually via a re- peater are therefore prone to fault situations; a problem on one segment multiplies over all other segments. In modern local networks, based on Ethernet, repeaters are mainly used to connect segments of different media with each other.

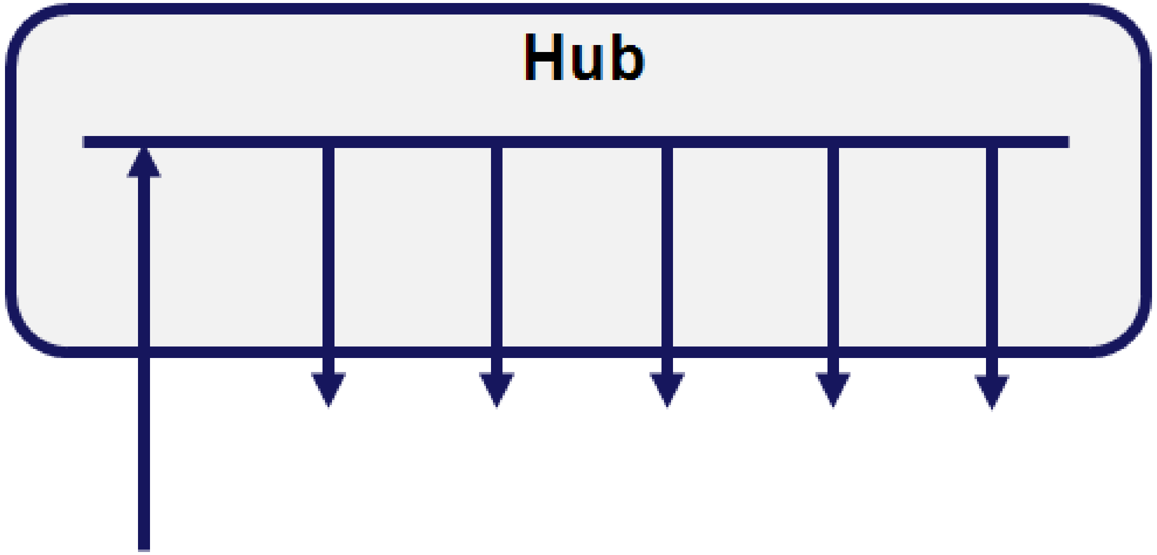


Structure elements for Ethernet: The hub

- A hub is actually a multiport repeater: it regenerates incoming signals to all other ports. All segments that are connected with each other via a hub are a collision domain.

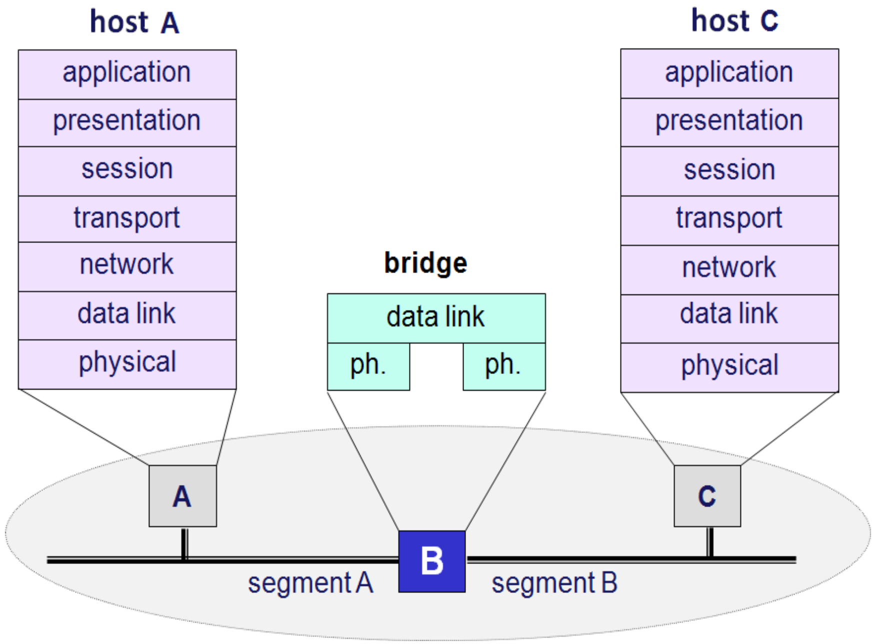
- A hub is available in several different versions. These versions differ in the number of ports, the media types that are supported and the extensibility.

- An important functionality of the modern hub is the option for network management. It is at least possible to switch off the ports and to detect whether failures have taken place.



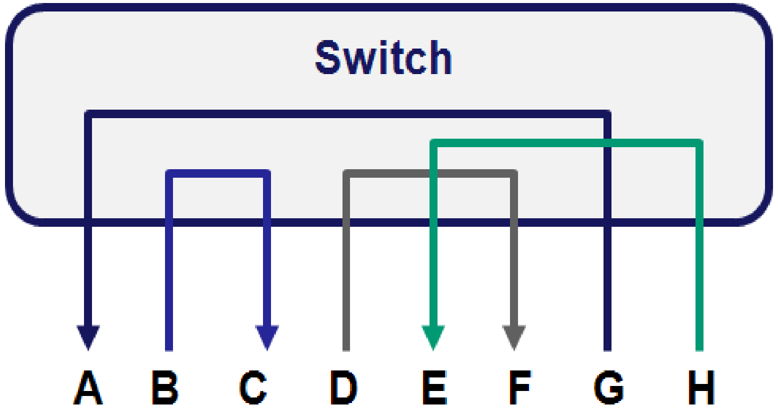
Structure elements for Ethernet: The bridge

- A bridge can be equipped with more than two network ports. In that case, the term switch is used. A MAC address table is updated from a software point of view for every port.
- This table is filled by listening on the relevant segment of the network and by copying all MAC addresses that occur on that segment to the table.
- Every address is retained for a limited time and is deleted again as soon as a certain time (the hold time) has lapsed. This technique avoids that inactive stations are addressed or that stations are not recognised anymore.

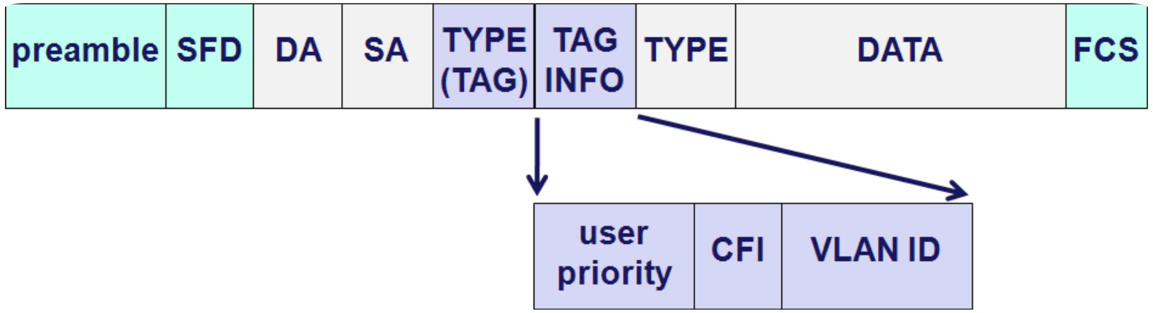


Structure elements for Ethernet: The switch

- Linking the segments of a local network via a switch has a number of advantages over the link with a repeater or a hub. When using a switch, a segment is not loaded with the frames of the other segment that do not belong there from an addressing point of view.
- The load per segment is reduced by this bridge function. At the same time, fault situations are not transmitted as the switch also checks the correct building of the frame. Finally, the bridge also avoids that collisions between frames are transmitted from one segment to the other.
- Every port of a switch closes a collision domain. If every participant connects directly to the port of a switch, then many collision domains occur but each domain only contains one participant and no collisions can occur. The switch is elaborated upon in another part of the document.



IEEE802.1Q tagged frame



- The IEEE802.1Q describes 4 extra bytes, divided into two extra fields in the Ethernet frame in order to use for new applications. One of these applications is VLAN (see also in this chapter).
- Description of the extra fields:
- TYPE(TAG), 2 bytes: has the value 8100h to specify that this frame is a tagged frame and therefore contains an extra information field
- VLAN TPID, 2 bytes: VLAN Tag Protocol Identifier
  - User priority, 3 bits: the priority of the frame is included, the priority code (a num- ber between 0 and 7) is described in IEEE802.1p.
  - CFI: Canonical Format Indicator. The IEEE802.1Q is only developed for Ethernet or Token Ring. This bit is 0 for Ethernet and 1 for Token Ring.
  - VLAN ID: Identification of the VLAN, 4094 possibilities.
    - FFFFh reserved
    - 0000h no VLAN, frames with priority (Profinet IO)