Introduction and Fundamentals
Practical Computer Networks and Applications

Prof. Dr. Christian Baun

Frankfurt University of Applied Sciences
(1971–2014: Fachhochschule Frankfurt am Main)
Faculty of Computer Science and Engineering
christianbaun@fb2.fra-uas.de

Contents

Introduction to PCNA

The course **Practical Computer Networks and Applications** consists of two parts:

1. The theoretical lecture on computer networks
2. The practical lab exercises on the application of computer networks

Theoretical lecture

This slide set is a recap of the theoretical foundations of the course **Computer Networks** from the winter term! It is intended as a reminder of the topics discussed last semester and will give you a brief summary on the protocols and technologies neccessary for this course!

The theoretical foundation for this course

- The Lab Exercise will use technologies from all network layers and therefore the knowledge on the technologies and protocols is necessary for the successful participation in the lab!
- You can use this slide set as a tool for the lab exercises!
- Each lab exercise will be accompanied by a corresponding slide set!

The Foundation

This slide set will give you the foundation on the lab exercises. The practical exercises will demonstrate their use in practice!

Organizational Information

- **E-Mail:** christianbaun@fb2.fra-uas.de

!!! Tell me when problems exist at an early stage !!!

- **Homepage:**
  https://www.christianbaun.de/CompNetLab23/index_en.html

!!! Check the course page regularly !!!

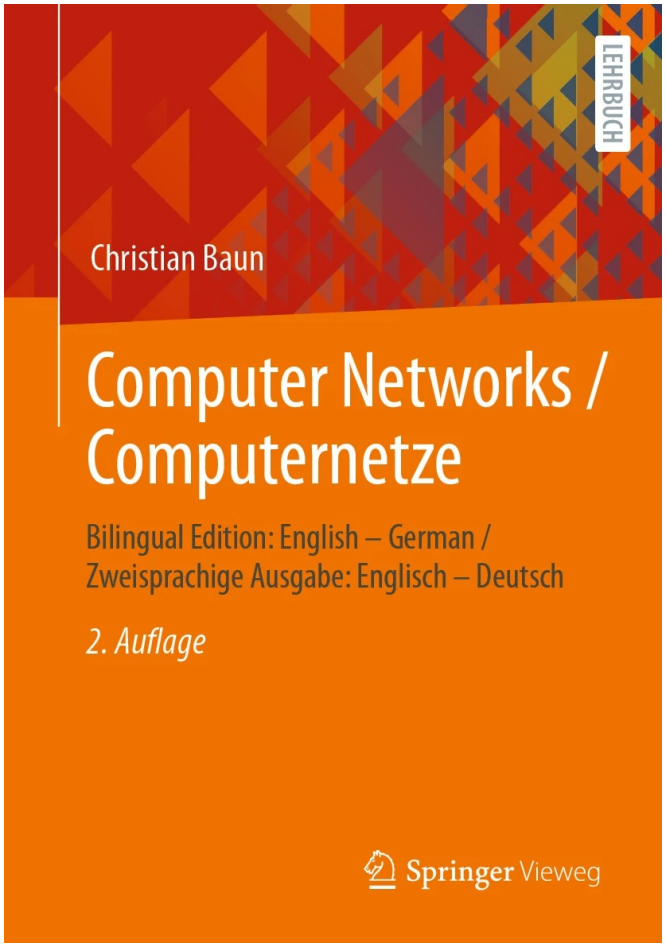
you need to upload your submissions via Moodle

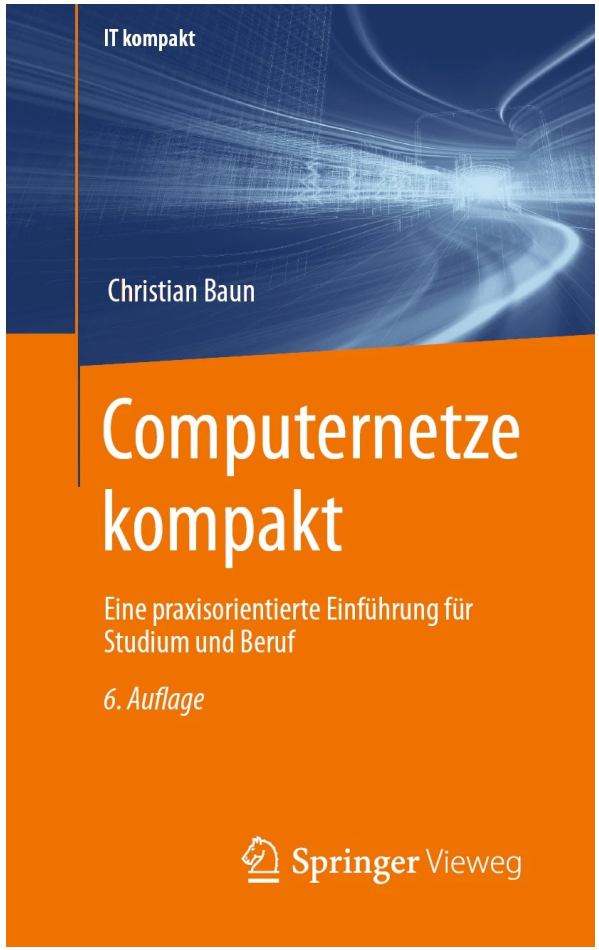
https://campuas.frankfurt-university.de/course/view.php?id=1601

- The homepage contains among others
  - **Schedule of the Course**
  - **Presentation slides**

The content of the English and German slides is identical, but please use the English slides for the exam preparation to become familiar with the technical terms

Literature





- My slide sets were the basis for these books
- The two-column layout (English/German) of the bilingual book is quite useful for this course

You can download both books for free via the FRA-UAS library from the intranet

Learning Objectives of this Slide Set

- Organizational Information
- Fundamentals of computer networks
  - Network services
  - Transmission media
  - Network protocols

This side set includes the topics of the hybrid reference model layers that are most relevant for this course

Contents

Protocols

- A **protocol** is the set of all previously made **agreements** between communication partners
  - These agreements include:
    - Rules for connection establishment and clearing
    - Method of synchronization between sender and receiver
    - Measures for the detection and treatment of transmission errors
    - Definition of valid messages (vocabulary)
    - Format and encoding of messages
- Protocols specify...
  - the **syntax** (= format of valid messages)
  - the **semantics** (= vocabulary and meaning of valid messages)

Reference Models

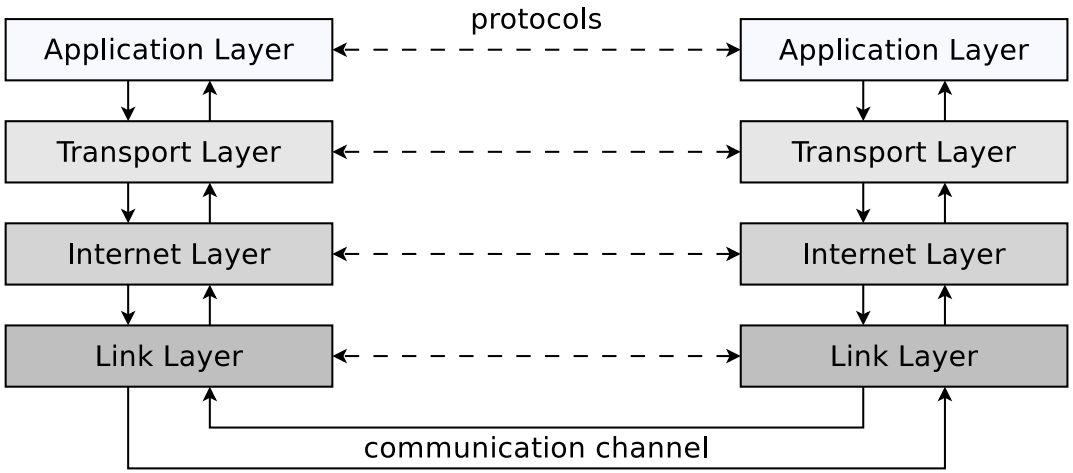
- Communication in computer networks is subdivided into **reference models**
- Each **layer** of a reference model handles a particular aspect of communication and offers **interfaces** to the overlying layer and underlying layer
- Each interface consists of a set of **operations**, which together define a **service**
- In the layers, the data is encapsulated ($\Longrightarrow$ **encapsulation**)
- Because each layer is complete in itself, single protocols can be modified or replaced without affecting all aspects of communication
- The most popular reference models are...
  - the **TCP/IP reference model**,
  - the **OSI reference model**
  - and the **hybrid reference model**

TCP/IP Reference Model or DoD Model

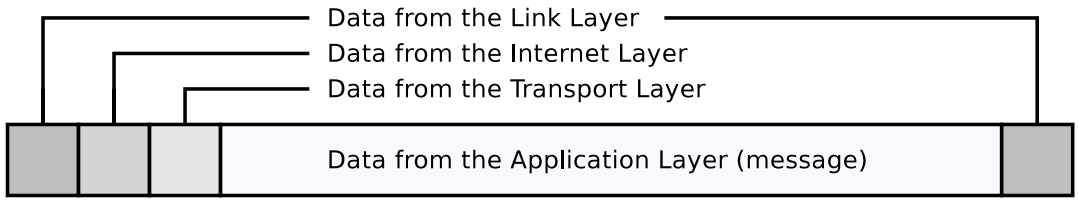
- Developed from 1970 onwards by the Department of Defense (DoD) in the Arpanet project
- Divides the required functionality to realize communication into 4 layers
- For each layer, it is specified, what functionality it provides
  - These requirements are implemented by communication protocols
    - Concrete implementation is not specified and can be implemented in different ways
    - Therefore, for each of the 4 layers, multiple protocols exist

Number	Layer	Protocols (Examples)
4	Application Layer	HTTP, FTP, SMTP, POP3, DNS, SSH, Telnet
3	Transport Layer	TCP, UDP
2	Internet Layer	IP (IPv4, IPv6), ICMP, IPsec, IPX
1	Link Layer	Ethernet, WLAN, ATM, FDDI, PPP, Token Ring

TCP/IP Reference Model – Message Structure

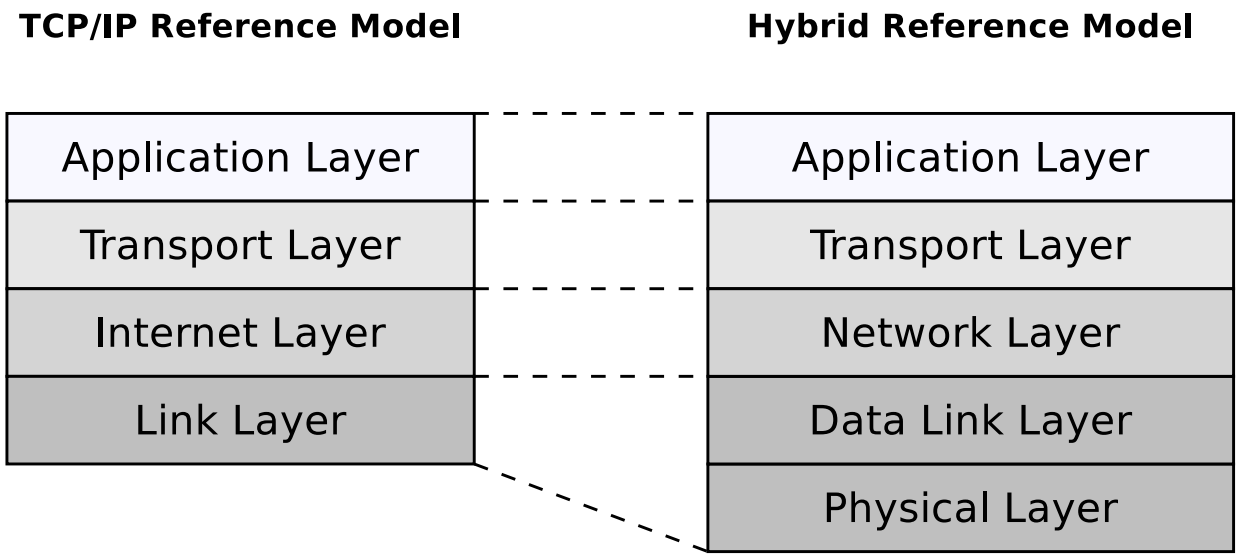


- Each layer adds additional information as **header** to the message
  - Some protocols (e.g. Ethernet) add in the link layer not only a header but also a **trailer** at the end of the message
  - The receiver analyzes the header (and trailer) on the same layer



Hybrid Reference Model

- The TCP/IP reference model is often presented in the literature (e.g. by Andrew S. Tanenbaum) as a 5-layer model
  - Reason: It makes sense to split the **Link Layer** into 2 layers, because they have different tasks
- This model is an extension of the TCP/IP model and is called **hybrid reference model**



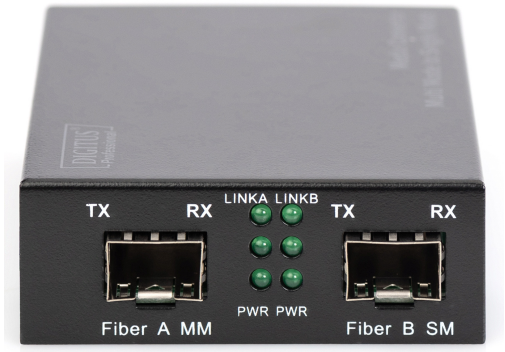
The objects of the individual layers will be discussed on the basis of the hybrid reference model

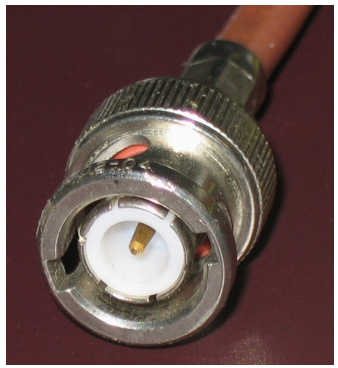
Physical Layer

- **Transmits the ones and zeros**
  - **Physical connection** to the network
  - **Conversion of data in signals**
- Protocol and transmission medium specify among others:
  - How many bits can be transmitted per second?
  - Can transmission take place simultaneously in both directions?
- Devices: **Repeater**, **Hub** (Multiport Repeater)

Hybrid Reference Model

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer





Data Link Layer

- Ensures error-free data exchange of **frames** between devices in physical networks
  - Detects transmission errors with **checksums**
  - Controls the access to the transmission medium (e.g. via CSMA/CD or CSMA/CA)
- Specifies physical network addresses (**MAC addresses**)

Hybrid Reference Model

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

- At sender site: Packs the Network Layer packets into frames and transmits them (in a reliable way) via a physical network from one device to another
- At receiver site: Identifies frames in the bit stream from the Physical Layer
- Devices: **Bridges**, **Layer-2-Switches** (Multiport Bridges) and **Modems** connect physical networks

Network Layer

- Forwards (*routes*) **packets** between logical networks (over physical networks)
  - For this *internetworking*, the Network Layer defines **logical addresses** (**IP addresses**)
  - Each IP packet is *routed* independently to its destination and the path is not recorded
- At sender site: Packs the segments of the Transport Layer in packets
- At receiver site: Unpacks the packets in the frames from the Data Link Layer
- **Routers** and **Layer-3-Switches** connect logical networks
- Usually the connectionless Internet Protocol (IP) is used
  - Other protocols (e.g. IPX) have been replaced by IP

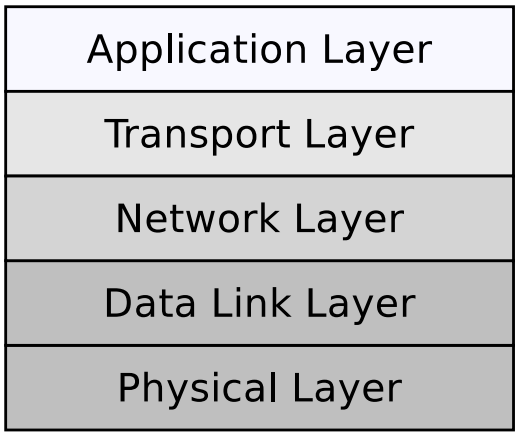
Hybrid Reference Model

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Transport Layer

- Transports **segments** between processes on different devices via so-called end-to-end protocols
- At sender site: Packs the data of the Application Layer into segments
- At receiver site: Unpacks the segments inside the packets from the Network Layer

Hybrid Reference Model



- Addresses processes with **port numbers**
  - Data Link Layer and Network Layer implement physical and logical addressing of the network devices
- Transport protocols implement different forms of communication
  - UDP (User Datagram Protocol): Connectionless communication
  - TCP (Transport Control Protocol): Connection-oriented communication
    - Combination of TCP/IP = de facto standard for computer networks

Different Forms of Communication

- **Connectionless communication**
  - Analogous to a mailbox
  - Sender transmits messages without prior connection establishment
  - Disadvantage: No validation that a segment arrives at the destination
    - If validation is wanted, it must be implemented in the Application Layer
  - Benefit: Better throughput, because of lesser overhead
- **Connection-oriented communication**
  - Analogous to a telephone
  - Prior data exchange, a connection is established between sender and receiver
    - The connection is not terminated, even if no data is transmitted
  - After all data is exchanged, the connection becomes terminated by one of the communication partners
  - Implements flow control and congestion control
    - Ensures lossless segment delivery in the correct order
      $\Longrightarrow$ Successful delivery is guaranteed

Application Layer

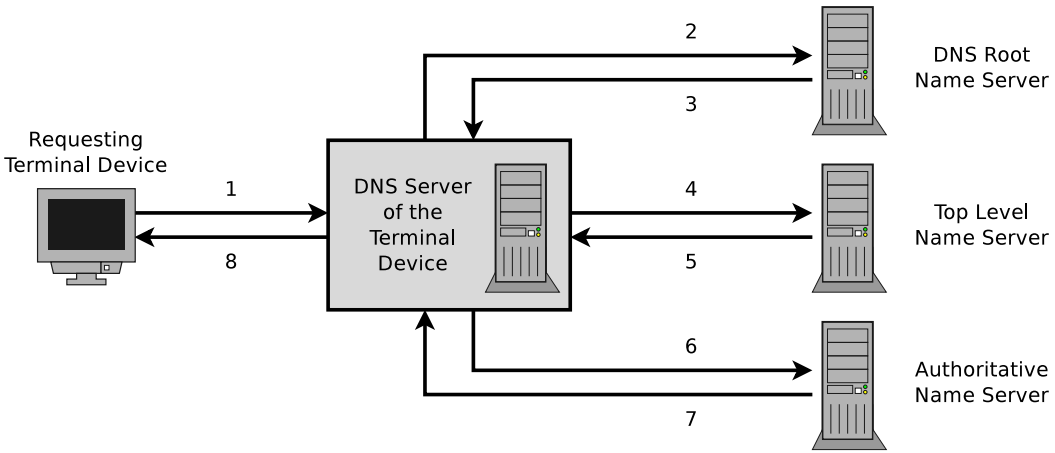
- Contains all protocols, that interact with the application programs (e.g. browser or email program)
- Here are the messages (e.g. HTML pages or emails), formated according to the used application protocol
- Some Application Layer protocols: HTTP, FTP, SMTP, POP3, DNS, SSH, Telnet

Hybrid Reference Model

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

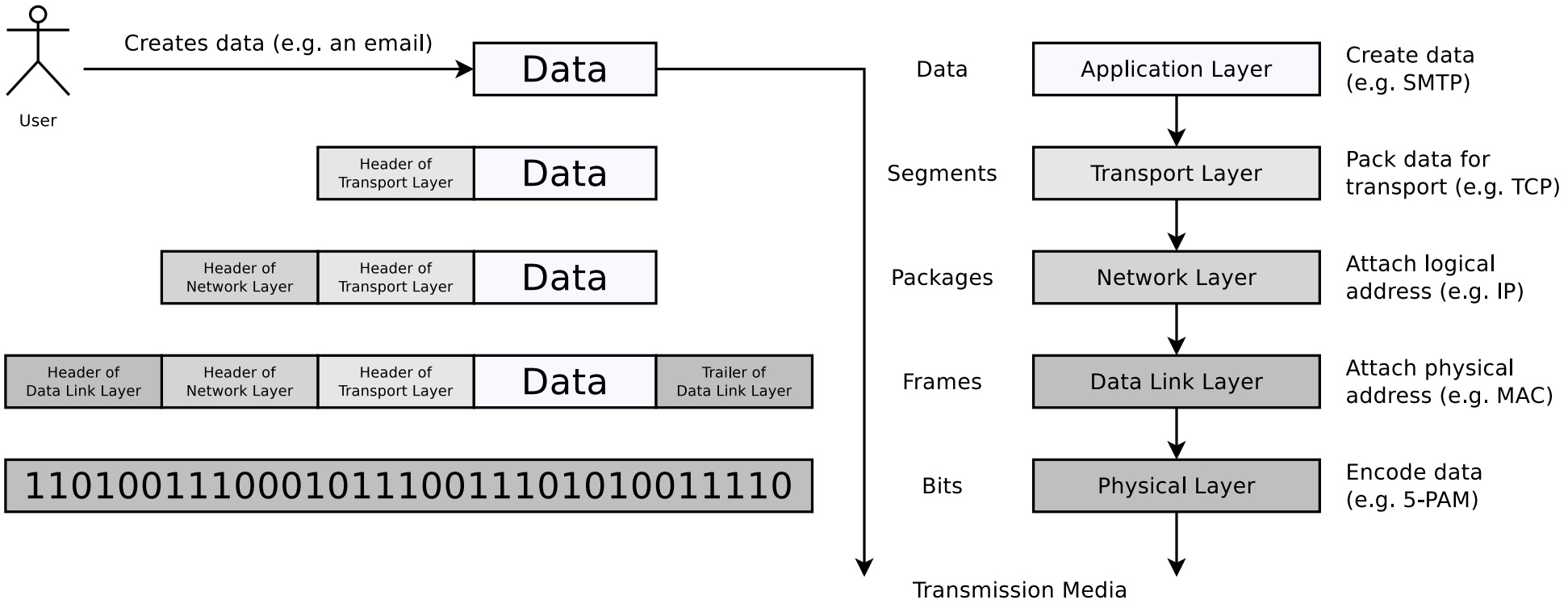
wikipedia.org (CC0)

pixabay.com (CC0)



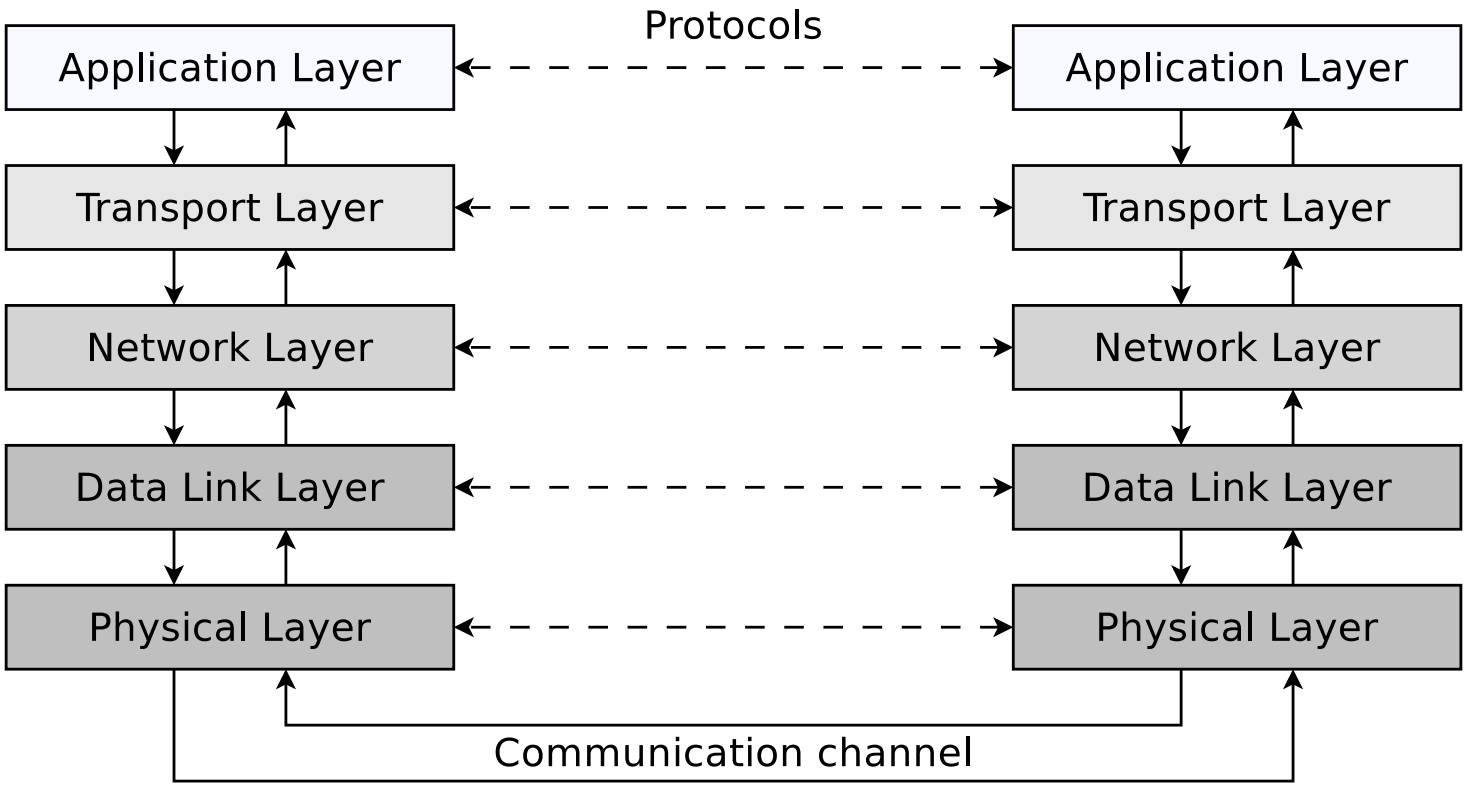
How Communication works (1/2)

- **Vertical communication**
  - Messages are packed from top to bottom layer by layer and extracted at the receiver in the reverse layer sequence
  - **Data encapsulation** and **de-encapsulation**



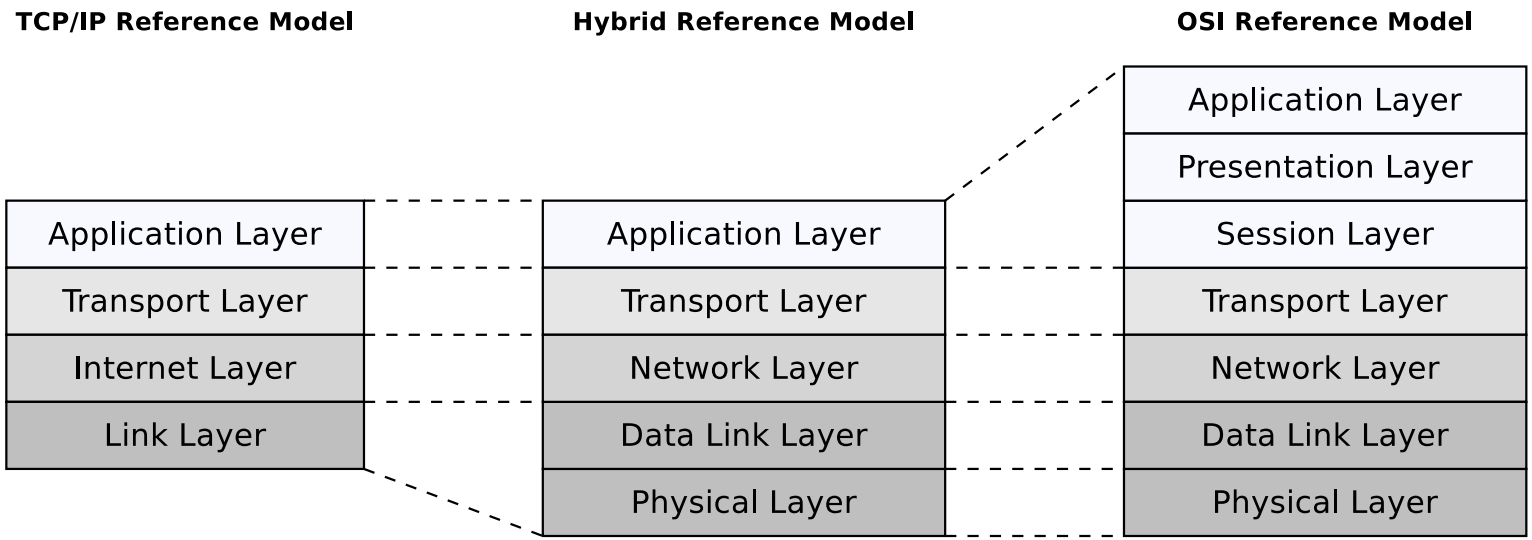
How Communication works (2/2)

- **Horizontal communication**
  - Equal protocol functions are used in the equivalent layers by sender and receiver



OSI Reference Model

- Some years after the TCP/IP reference model (1970s), the OSI reference model was developed from 1979 onwards
  - 1983: Standardized by the Intern. Organization for Standardization (ISO)
  - OSI = Open Systems Interconnection
- The structure is similar to the TCP/IP reference model
  - The OSI model implements 7 layers
- In contrast to the hybrid reference model, the Application Layer functionality is distributed across 3 layers in the OSI reference model



Session Layer

- **Controls the dialogues** (connections) between processes
  - Controls which node is allowed to send next
- Provides checkpointing which is useful for longer data transmissions to enable **synchronization**
  - If the connection fails, returning to a checkpoint avoids starting the transmission from the beginning
- Protocols that meet the required capabilities of the Session Layer are **Telnet** for remote controlling computers and **FTP** for file transmission
  - These protocols can be assigned to the Application Layer too
    - The Application Layer includes the protocols, used by the users' applications
  - FTP and Telnet are used directly by the relevant programs and not by abstract protocols of upper levels
    - Thus, it makes sense to assign these Session Layer protocols to the Application Layer

The Session Layer is seldom used in practice, because all tasks intended to this layer are fulfilled by Application Layer protocols today

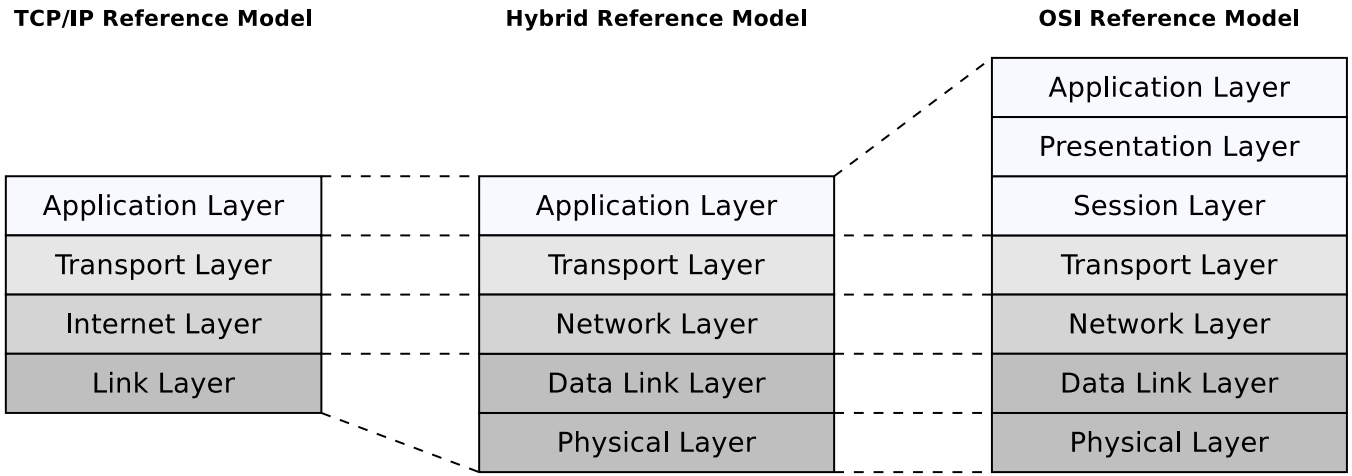
Presentation Layer

- Contains rules for setting the **format (presentation) of messages**
  - The sender can notify the receiver that a message has a specific **format** (e.g. ASCII) to make conversion happen, which is perhaps necessary
  - Data records can be specified here with fields (e.g. name, student ID number...)
  - **Data types and their length** can be defined here
  - **Compression and encryption** could be implemented by this layer

The Presentation Layer is seldom used in practice, because all tasks intended to this layer are fulfilled by Application Layer protocols today

Reference Models – Summary

- Conclusion: The hybrid reference model illustrates the functioning of computer networks in a realistic way
  - It distinguishes between the Physical Layer and Data Link Layer
    - This is useful, because the objectives differ a lot
  - It does not subdivide the Application Layer
    - This is not useful and does not take place in practice
    - Functionalities, which are intended for Session Layer and Presentation Layer, are provided by Application Layer protocols and services
  - It combines the advantages of the TCP/IP reference model and the OSI reference model, without taking over their drawbacks



Contents

Ethernet (IEEE 802.3)

- Developed in the 1970s by Robert Metcalfe and others at the Xerox Palo Alto Research Center
  - Data rate of this first Ethernet version: 2,94 Mbps
- 1983: IEEE standard since with 10 Mbps
- The most frequently used (cable-based) LAN technology since the 1990s
  - Ethernet displaced other standards (e.g. Token Ring) or made them niche products for special applications (e.g. FDDI)
- Several Ethernet standards exist
  - They differ among others in the **data rate** and the **transmission medium** used
    - Versions for coaxial cables, twisted pair cables and fiber-optic cables, with data rates up to 40 Gbit/s exist
- The **connection type** to the medium is **passive**
  - This means that devices are only active when they send data

Some Variants of Ethernet

- All these variants are extensions of Thick Ethernet (10BASE5)

Standard	Mbps	Transmission Medium
10BASE2/5	10	Coaxial cables (50 ohm impedance)
10BROAD36	10	Coaxial cables (75 ohm impedance)
10BASE-F	10	Fiber-optic cables
10BASE-T	10	Twisted pair cables
100BASE-FX	100	Fiber-optic cables
100BASE-T4	100	Twisted pair cables (Cat 3)
100BASE-TX	100	Twisted pair cables (Cat 5)
1000BASE-LX	1.000	Fiber-optic cables
1000BASE-SX	1.000	Fiber-optic cables (Multi-mode fiber)
1000BASE-ZX	1.000	Fiber-optic cables (Single-mode fiber)
1000BASE-T	1.000	Twisted pair cables (Cat 5)
1000BASE-TX	1.000	Twisted pair cables (Cat 6)
2.5GBASE-T	2.500	Twisted pair cables (Cat 5e)
5GBASE-T	5.000	Twisted pair cables (Cat 6)
10GBASE-SR	10.000	Fiber-optic cables (Multi-mode fiber)
10GBASE-LR	10.000	Fiber-optic cables (Single-mode fiber)
10GBASE-T	10.000	Twisted pair cables (Cat 6A)
40GBASE-T	40.000	Twisted pair cables (Cat 8.1)

- 2 different transmission modes exist:
  1. **Baseband** (BASE)
  2. **Broadband** (BROAD)

Naming convention

- Part 1: Data rate
- Part 2: Transmission method (baseband or broadband)
- Part 3: 100 times the maximum segment length or the transmission medium

10BASE5 for example means...

- Data rate: 10 Mbps
- Transmission method: Baseband
- Maximum segment length: $5 * 100\text{m} = 500\text{m}$

Variants of Ethernet – Baseband (BASE)

- Almost all Ethernet standards implement the baseband transmission method (BASE)
  - Single exception: 10BROAD36
- Baseband systems have **no carrier frequencies**
  - This means that **data is directly (at baseband) transmitted on the transmission medium**
- Digital signals are injected directly as impulses into the copper cable or fiber-optic and occupy the entire bandwidth of the cable or a part of it
  - Unused bandwidth can not be used for other services

In short...

Baseband systems provide just a **single channel**

Variants of Ethernet – Broadband (BROAD)

Image Source: AVM

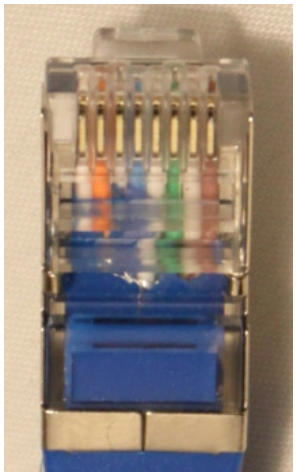
- The data is **modulated to a carrier frequency**
  - This allows to transmit multiple signals at the same time in **different frequency ranges** ('bands')
- Only 10BROAD36 uses the broadband method
  - Because of high hardware costs for the modulation, the system was no economic success
- The broadband concept, used together with Ethernet, was no success, but the concept itself is used today in many areas of communication and telecommunication

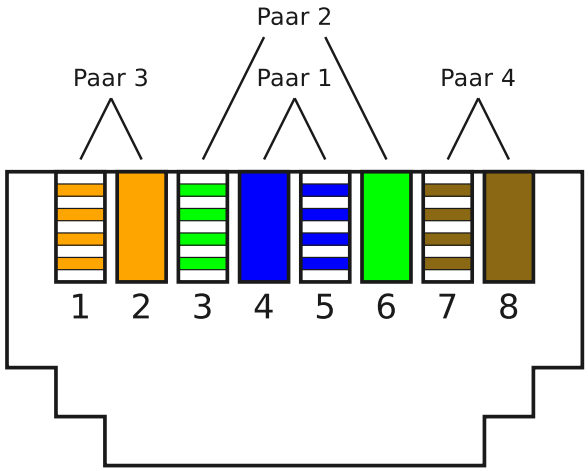
Some fields of application of the broadband concept

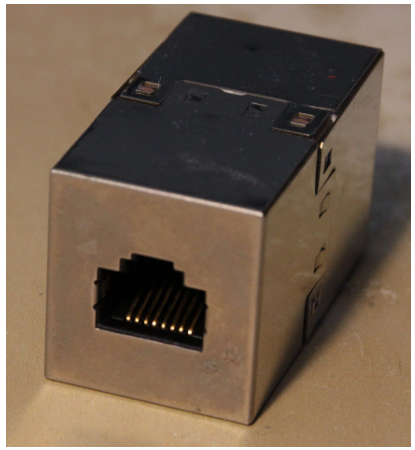
- Via cable television, different TV channels, and with different carrier frequencies, also radio channels, telephone and internet is available
- The electrical power grid can be used to establish network connections ($\Longrightarrow$ Power line communication)

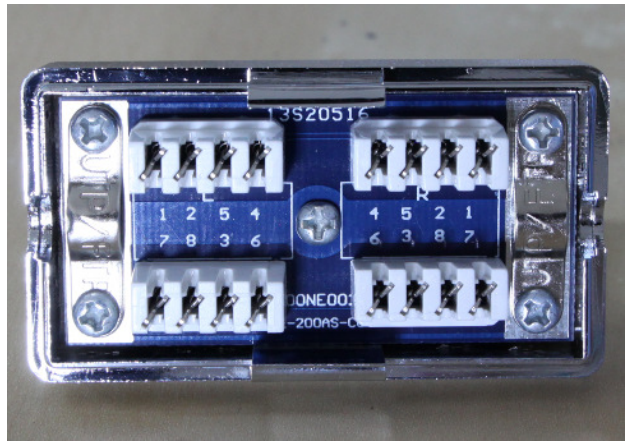
Twisted Pair Cables (1/2)

- The wires of twisted-pair cables are pairwise twisted with each other.
- Twisted pairs are better protected against alternating magnetic fields and electrostatic interferences from the outside than parallel signal wires
- All variants of the Ethernet standard, that use twisted pair cables as transmission medium, use plugs and jacks according to the standard 8P8C, which are usually called RJ45









Twisted Pair Cables (2/2)

- Since the 1990s, twisted-pair cables and RJ45 plugs and jacks are **standard for copper-based IT networking**

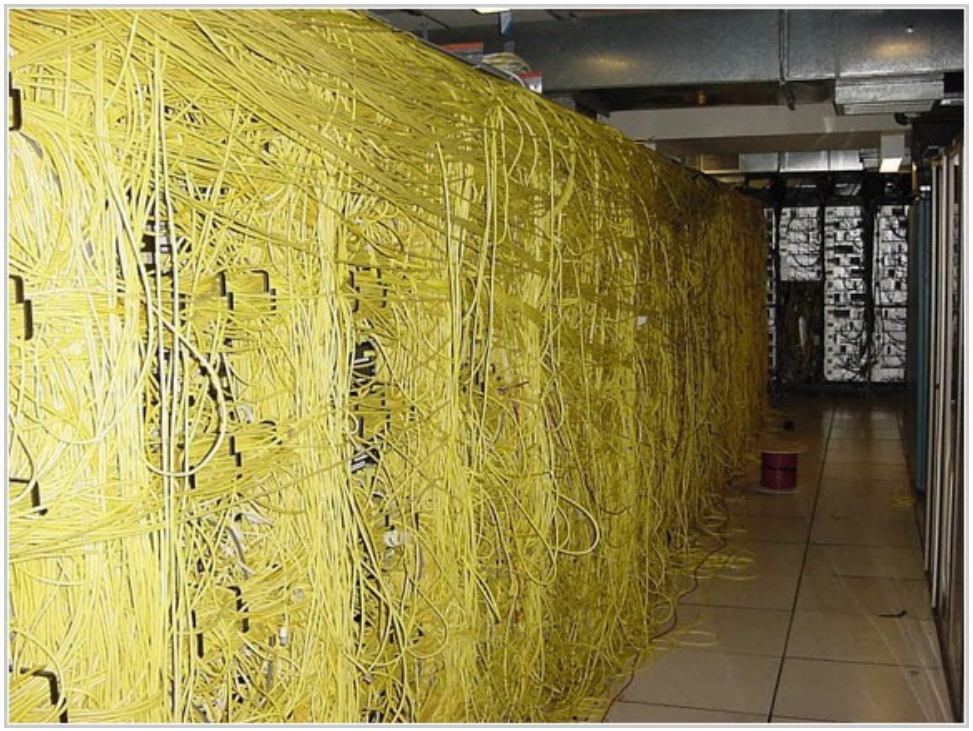
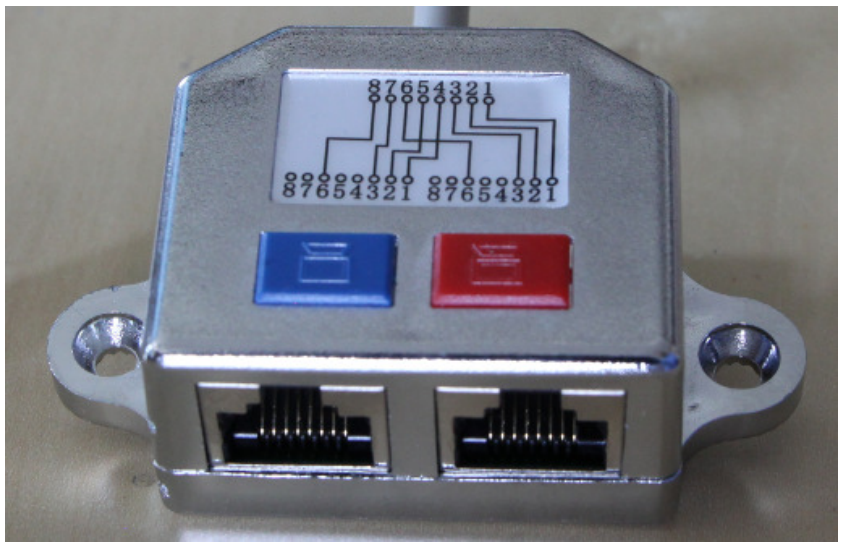


Image source: `memegenerator.net`

- Ethernet 10BASE-T and Fast Ethernet 100BASE-TX both only use 2 pairs of wires for sending and receiving
- This allows using **Ethernet Splitters**



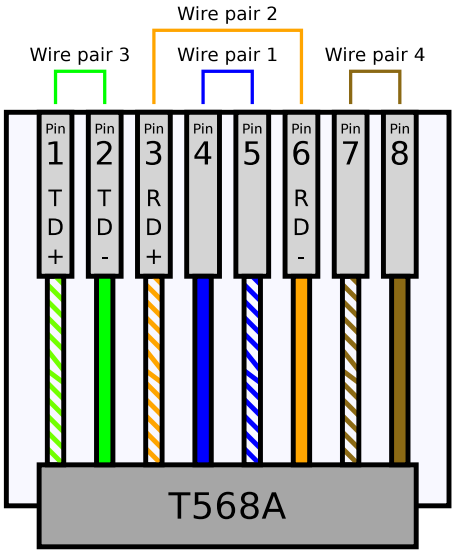
- Fast Ethernet 100BASE-T4 and Gigabit Ethernet 1000BASE-T both use all 4 pairs of wires for sending and receiving

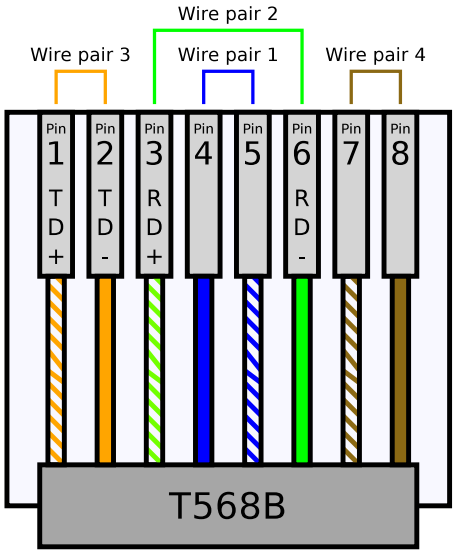
Why are 2 pairs of wires used for sending and receiving?

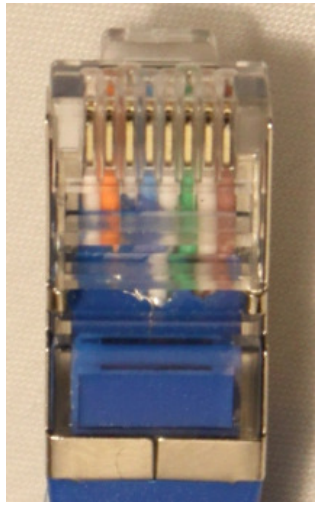
See 'Complementary Signal' on slide 35

Wiring

- T568A and T568B are standards for the pin assignment of the RJ45 plugs and jacks and are used for Fast Ethernet 100BASE-TX and Gigabit Ethernet 1000BASE-T
  - Difference: The wire pairs 2 and 3 (green and orange) are interchanged
  - Mixing T568A and T568B in a computer network is a bad idea







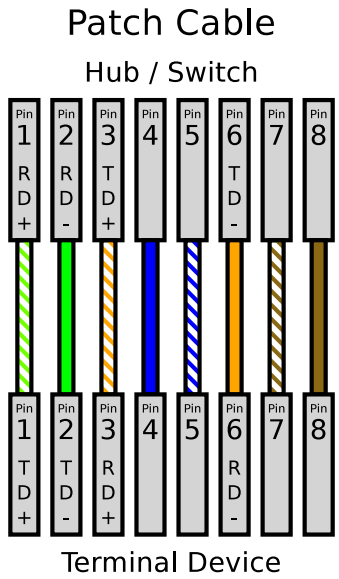
This is T568B

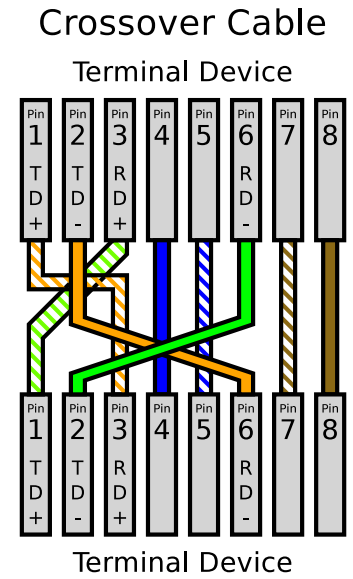
When using 10BASE-T, 4 PINs are used – The remaining wire pairs are not used

- `TD+` and `TD-` (Trancieve Data) is the wire pair for data output signal
- `RD+` and `RD-` (Recieve data) is the wire pair for data input

Crossover Cables and Patch Cables

- A **Crossover cable** can connect 2 terminal devices directly
  - It connects the send and receive lines of both devices
- To connect more than just 2 network devices, **patch cables** are used
  - In this case, a Hub or a Switch is required





- Some Hubs and Switches provide an **uplink port** for connecting another Hub or Switch
  - The uplink port is internally crossed

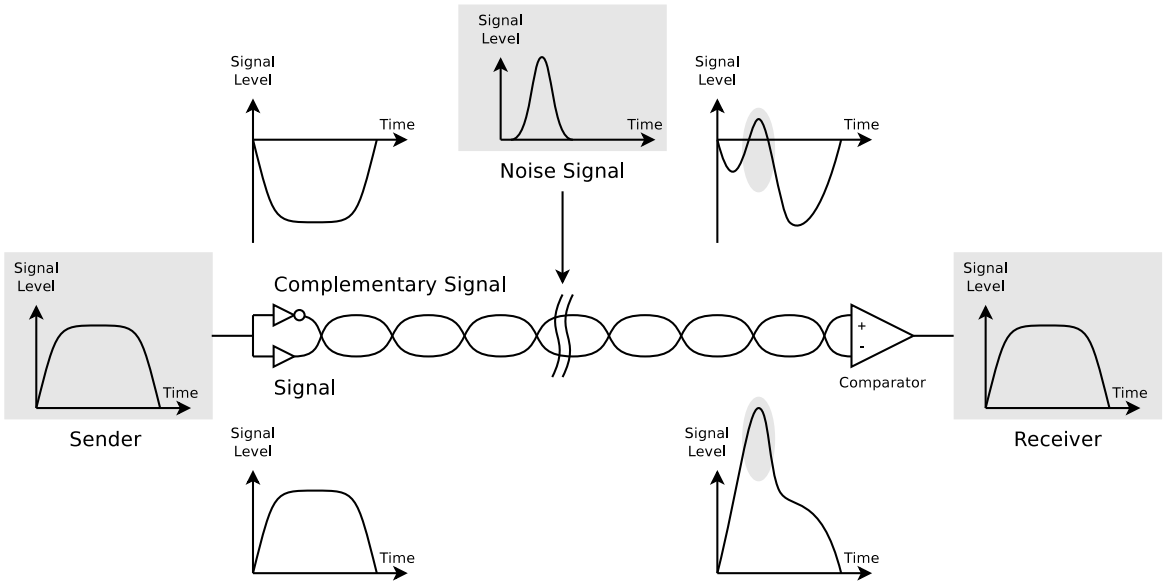
Auto-MDIX allows using crossover lines and patch cables any time

- Modern network devices automatically detect the send and receive lines of connected network devices
- All network devices, which support Gigabit Ethernet 1000BASE-T or faster, implement Auto-MDIX

Complementary Signal

Source: Jörg Rech. Ethernet. Heise. 2008 and Wikipedia

- Via the wire pair a complementary signal is sent (on one wire 0 V to +2.8 V and on the other wire 0 V to -2.8 V)
  - This allows the receiver to **filter out interfering signals**
  - Furthermore, it **reduces electromagnetic emission**



- The signal level of line A=Payload Signal+Noise
- The signal level of line B= −Payload Signal+Noise

- The difference of the signal levels of line A and line B at receiver side is: [+Payload Signal+Noise] − [−Payload Signal+Noise] = 2∗Payload Signal
- Result: Regardless of the level of the noise signal, the difference between the payload signal and the complementary signal remains the same

Shielding of different Twisted Pair Cables

- Twisted pair cables are often equipped with a metal shield to prevent electromagnetic interferences

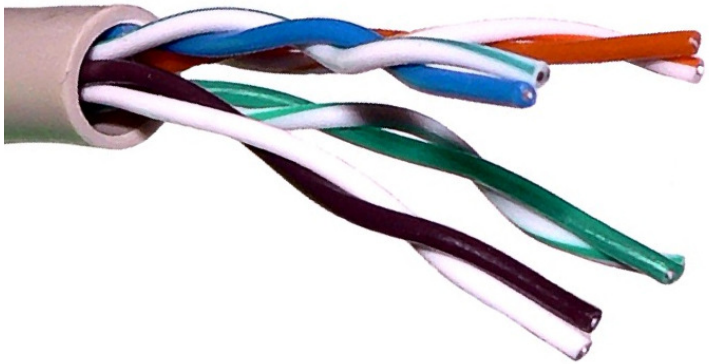
Label	Meaning	Cable shielding	Pair shielding
UUTP	*Unshielded Twisted Pair*	none	none
UFTP	*Foiled Twisted Pair*	none	foil
USTP	*Shielded Twisted Pair*	none	braiding
SUTP	*Screened Unshielded Twisted Pair*	braiding	none
SFTP	*Screened Foiled Twisted Pair*	braiding	foil
SSTP	*Screened Shielded Twisted Pair*	braiding	braiding
FUTP	*Foiled Unshielded Twisted Pair*	foil	none
FFTP	*Foiled Foiled Twisted Pair*	foil	foil
FSTP	*Foiled Shielded Twisted Pair*	foil	braiding
SFUTP	*Screened Foiled Unshielded Twisted Pair*	braiding and foil	none
SFFTP	*Screened Foiled Foiled Twisted Pair*	braiding and foil	foil

- The label scheme follows the schema `XXYZZ`
  - `XX` is the cable shield
    - `U` = unshielded, `F` = foil shielding , `S` = braided shielding, `SF` = braided shielding and foil
  - `Y` is the pair shielding
    - `U` = unshielded, `F` = foil shielding , `S` = braided shielding
  - `ZZ` stands for twisted pair (TP)

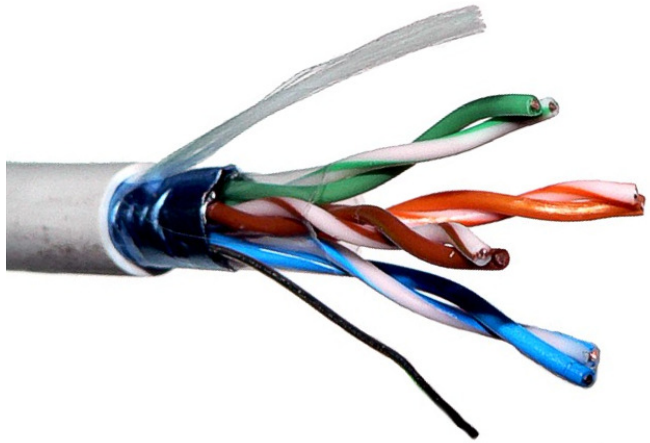
Twisted Pair Cables – Examples

Image Source: (Kabel): Wikipedia (CC0)

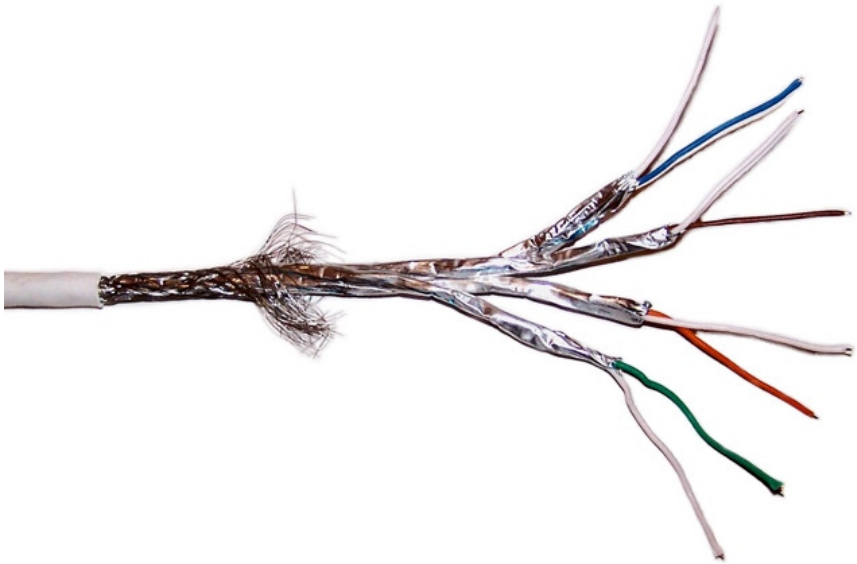
Example 1: UTP



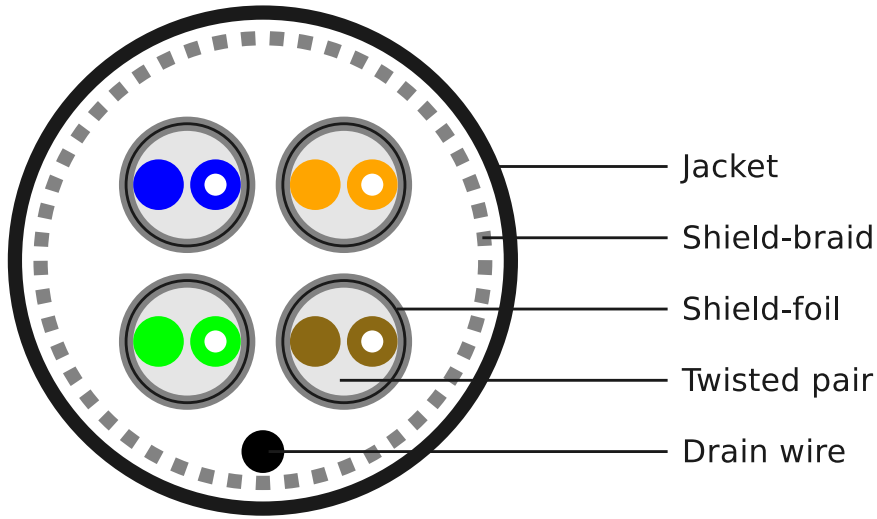
Example 2: FUTP = FTP



Example 3: SFTP

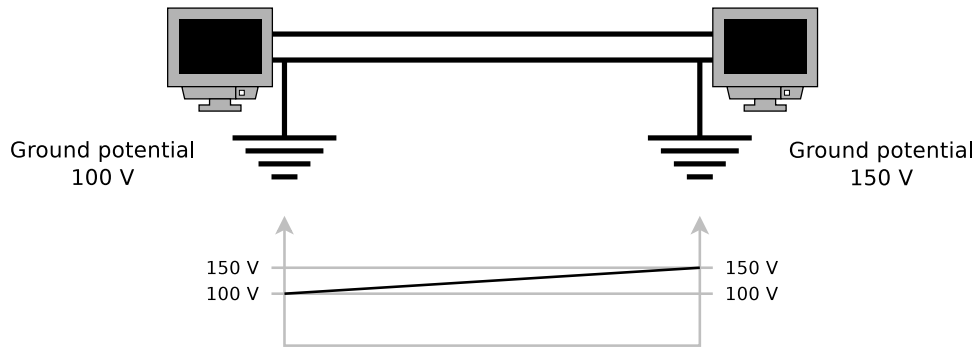


Structure (SFTP)



Shielded or Unshielded Cables?

- Shields must be electrically grounded on both sides of the cable
  - If only one end of a shielded cable is grounded, an antenna effect occurs



- This results in a compensation current ($I = \frac{V}{R}$)
  - Compensating currents cause problems during operation or even the destruction of network devices
- For this reason, shielding can only be used if both sides of the cable have the same ground potential and therefore **shielded cables cannot be used to connect different buildings**
  - Possible solutions are the installation of fiber-optic cables between buildings, laser bridges or wireless networks

Categories of Twisted Pair Cables (1/3)

- Different categories of twisted pair cables exist
- The performance of a network connection is determined by the component of the lowest category
  - Example: Devices, which support Cat6, are connected via a Cat5 cable
    - This reduces the performance of the connection to the values of Cat5
- **Category 1/2/3/4**
  - Not common today (except for telephone cables)
- **Category 5/5e**
  - Cat5e is guaranteed Gigabit Ethernet-compatible
    - It meets stricter test standards than Cat5 cables
  - Common in most current LANs

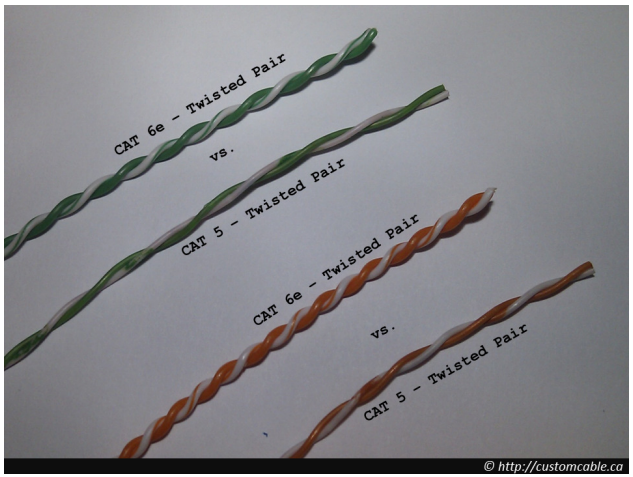
Category	Max. frequency	Compatible with...
Cat-5	100 MHz	100BASE-TX (100 Mbps, 2 wire pairs, 100 m) 1000BASE-T (1 Gbps, 4 wire pairs, 100 m)
Cat-5e	100 MHz	2.5GBASE-T (2.5 Gbps, 4 wire pairs, 100 m)

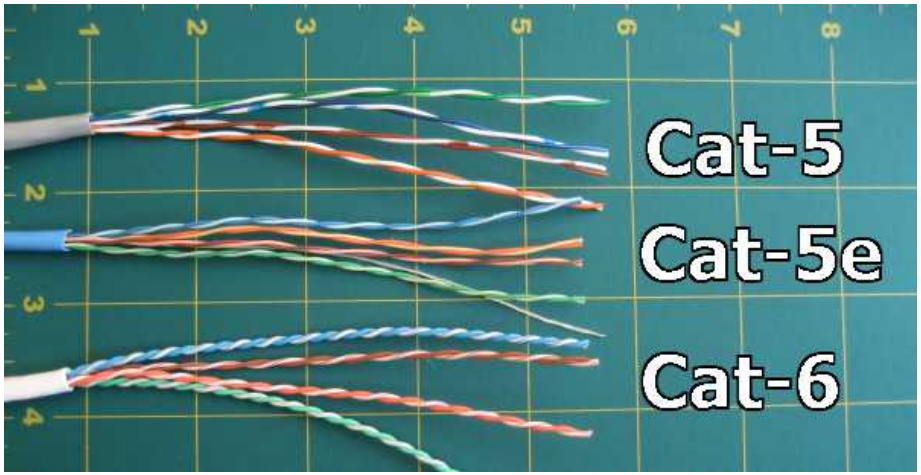
Categories of Twisted Pair Cables (2/3)

Image Source: Reddit

- **Category 6/6A**

Category	Max. frequency	Compatible with. . .
Cat-6	250 MHz	5GBASE-T (5 Gbps, 4 wire pairs, 100 m)
		10GBASE-T (10 Gbps, 4 wire pairs, 55 m)
Cat-6A	500 MHz	10GBASE-T (10 Gbps, 4 wire pairs, 100 m)





Main differences (of the structure) between the categories: number of twists per wire length (cm) and thickness of the jacket

- More twists per cm $\Longrightarrow$ less interference (noise)
- Cat 5/5e has 1-2 twists per cm. Cat 6 has 2 or more twists per cm
- Thickness of the cladding $\Longrightarrow$ less crosstalk
- Crosstalk is the mutual interference of parallel lines

Categories of Twisted Pair Cables (3/3)

- **Category 7/7A**
  - For Cat 7 and Cat 7A cables, other connectors (e.g., TERA or GG45) and sockets than RJ45 were initially intended
    - However, these connectors were not successful in the market
    - **Cat 7 and 7A cabling with RJ45 connectors offers no benefits over category 6A cables**

Category	Max. frequency	Compatible with...
Cat-7	600 MHz	10GBASE-T (10 Gbps, 4 wire pairs, 100 m)
Cat-7A	1000 MHz	10GBASE-T (10 Gbps, 4 wire pairs, 100 m)

- **Category 8.1**
  - This standard supports cables of up to 30 m in length
  - Cables of this length are mostly sufficient for data centers

Category	Max. frequency	Compatible with...
Cat-8.1	2000 MHz	40GBASE-T (40 Gbps, 4 wire pairs, 30 m)

Information printed on Twisted Pair Cables (1/2)

Do you understand the most important cable characteristics that are printed on twisted pair cables?

Example: `E188601 (UL) TYPE CM 75°C LL84201 CSA TYPE CMG FT4 CAT.5E PATCH CABLE TO TIA/EIA 568A STP 26AWG STRANDED`

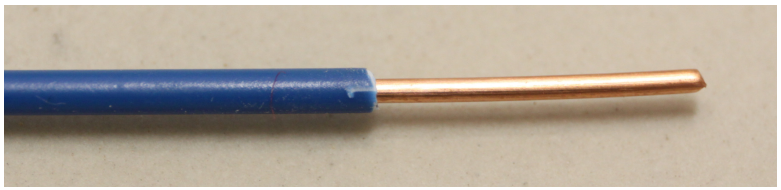
- **PATCH/CROSS/CROSSOVER**: see slide 34
- **UTP/STP/FTP/SFTP**: see slides 36-37
- **CAT5/5E/6/7/8**: see slides 39-41
- **24AWG/26AWG/28AWG**: American wire gauge (AWG) informs about the diameters of the wires
  - 24AWG = 0.51054 mm, 26AWG = 0.405 mm, 28AWG = 0.321 mm
  - Larger wire diameter $\Longrightarrow$ less electrical resistance for the electronic signals $\Longrightarrow$ lower attenuation
    - 24AWG cables have lower attenuation than 26AWG or 28AWG cables
  - 28AWG cables are thinner than 24AWG or 26AWG
    - Thinner cables block airflow in server racks less and simplify the installation

Information printed on Twisted Pair Cables (2/2)

Do you understand the most important cable characteristics that are printed on twisted pair cables?

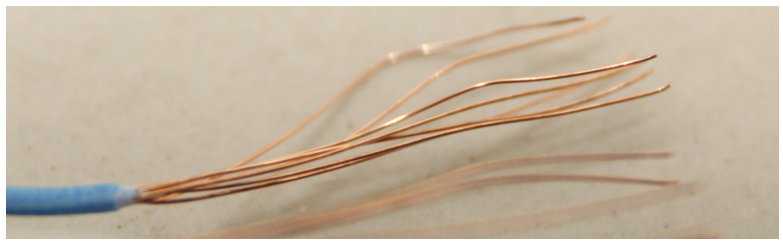
Example: `E188601 (UL) TYPE CM 75°C LL84201 CSA TYPE CMG FT4 CAT.5E PATCH CABLE TO TIA/EIA 568A STP 26AWG STRANDED`

- **60°C/75°C**: Temperature information stands for flame tests
- **SOLID/STRANDED**
  - **Solid** cables use solid copper wires. Such cables are well suited for permanent infrastructure installation. They have a lower attenuation and cost less compared to stranded cables
  - **Stranded** cables consist of multiple strands of wires wrapped around each other. They are typically used to create patch cables because they are very flexible. Attenuation of stranded cables is higher compared to solid cables. Thus, they are used for shorter distances



Left image: Solid cable

Right image: Stranded cable



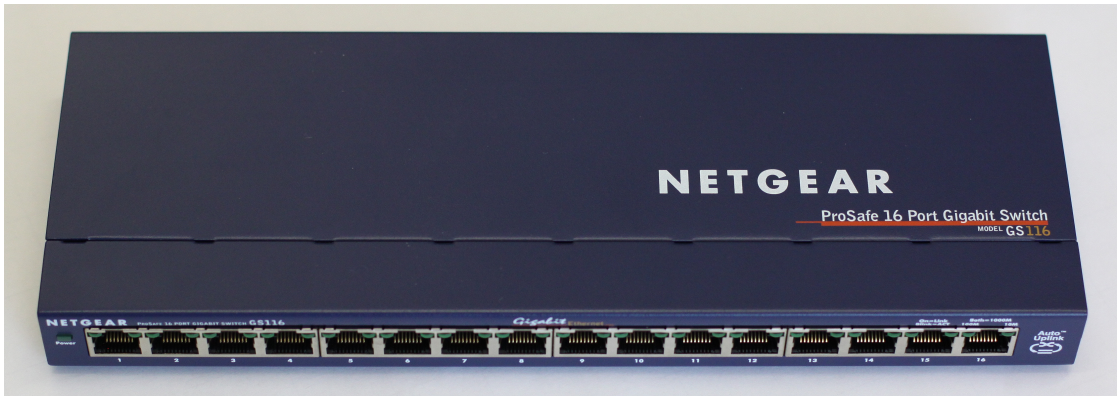
Contents

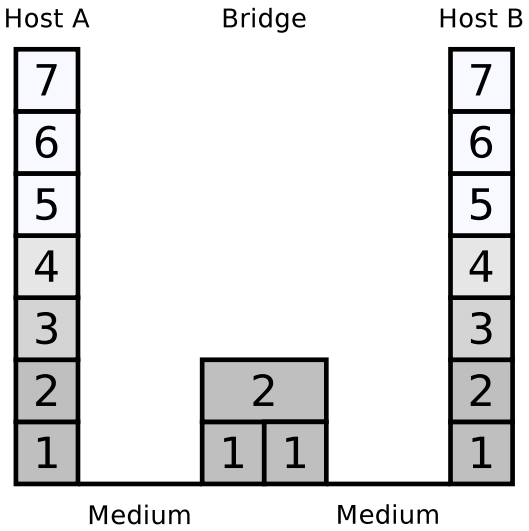
Learning Objectives of this Slide Set

- Data Link Layer (part 1)
  - Devices of the Data Link Layer
    - Learning Bridges
    - Loops on the Data Link Layer
    - Spanning Tree Protocol
    - Impact on the collision domain
  - Addressing in the Data Link Layer
    - Format of MAC addresses
    - Uniqueness of MAC addresses
    - Security aspects of MAC addresses

Devices of the Data Link Layer: Bridges

- Devices of the Physical Layer increase the length of physical networks
  - For connecting different physical networks, **Bridges** are required because they forward frames from one physical network to another one
- A Bridge has only 2 ports
  - Such bridges usually connect networks based on different technologies (transmission media) $\Longrightarrow$ see slides **??** and **??**
- Simple Bridges forward all incoming frames





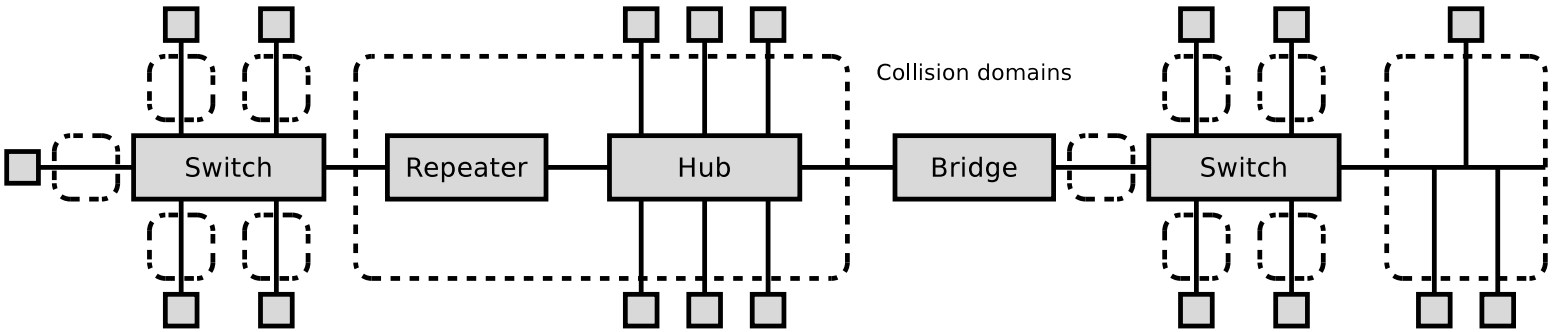
- Bridges with > 2 ports are called **Multiport Bridge** or **Layer-2-Switch**
  - They typically provide 4-48 interfaces

Functioning of Bridges and Layer-2-Switches

- Bridges and Switches check the correctness of the frames via **checksums**
- Bridges do **not need addresses** for filtering and forwarding the frames, because they do not actively participate in the communication
  - They operate transparent, just like the devices of the Physical Layer
    - Reason: They do not communicate on a higher protocol layer as the Data Link Layer

Collision Domain – Bridges and Layer-2-Switches

- Bridges and Switches operate on Data Link Layer and forward frames from one physical network to other ones
- **Each physical network is a separate collision domain**
  - If a physical network is split by a Bridge or a Switch, also the collision domain is split
    - As effect, the number of collisions drops
- For Bridges and Switches, each port forms its own collision domain



- In a *fully switched network*, each port of the Switches is connected with just a single network device
  - Such a network is collision-free and state of the art

Addressing in the Data Link Layer

- The Data Link Layer protocols specify the format of the physical network addresses
- **Terminal devices (Hosts)**, **Routers** and **Layer-3-Switches** require physical network addresses
  - Such devices must be addressable on Data Link Layer because they provide services at upper protocol layers
- **Bridges** and **Layer-2-Switches** do not actively participate in the communication
  - Therefore, they don't require physical network addresses for their basic functionality, which is the filtering and forwarding of frames
  - Bridges and Switches require physical network addresses, when they implement the STP to avoid loops, or when they offer services from an upper protocol layer
    - Examples are monitoring services or graphical web interfaces for administration tasks
- **Repeaters** and **Hubs** that operate only at the Physical Layer, have no addresses

MAC Addresses (1/2)

- The **physical network addresses** are called **MAC addresses** (Media Access Control)
  - They are independent from the logical addresses of the Network Layer
- Ethernet uses the **Address Resolution Protocol** (ARP) to resolute the logical addresses of the Network Layer (IPv4 addresses) to MAC addresses
  - For IPv6, the **Neighbor Discovery Protocol** (NDP) provides the identical functionality and operates in a similar way
- MAC addresses have a length of 48 bits (6 bytes)
  - Thus, the address space contains 2^{48} possible addresses
- In order to make the representation compact and human-friendly to read, MAC addresses are usually written in hexadecimal notation
  - The bytes are separated from each other with dashes (-) or colons (:)
- Example of the notation: `00-16-41-52-DF-D7`

MAC Addresses (2/2)

- 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
    - However, this modification applies only until the next reboot of the computer
- **MAC broadcast address**
  - If a network device wants to send a frame to all other devices in the same physical network, it inserts MAC broadcast address in the destination address field of the frame
  - All 48 bits of this MAC address have the value 1
  - Hexadecimal notation: `FF-FF-FF-FF-FF-FF`
  - Bridges and Switches do not forward frames to other physical networks, that contain the MAC broadcast address in the destination address field

Uniqueness of MAC Addresses

- The first 24 bits of the MAC address space are managed by the Institute of Electrical and Electronics Engineers (IEEE)
  - These 24 bits long addresses are called **MA-L** (MAC Address Block Large) or **OUI** (Organizationally Unique Identifier)
  - The OUIs can be checked in this IEEE database:

    `http://standards.ieee.org/develop/regauth/oui/public.html`
- The remaining 24 bits are specified by the hardware vendors independently for their network devices
  - That address space allows $2^{24} = 16,777,216$ individual device addresses per OUI

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

- Smaller address spaces are available too: **MA-S** (MAC Address Block Small) and **MA-M** (MAC Address Block Medium)

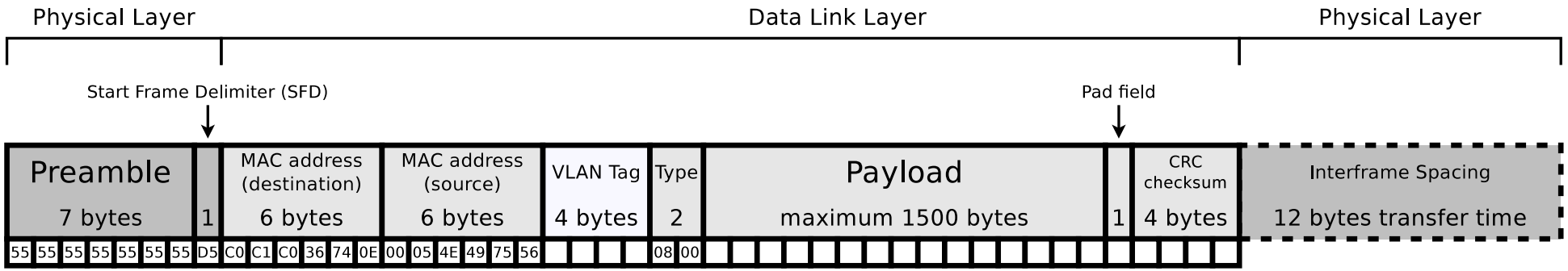
Security Aspects of MAC Addresses

- 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

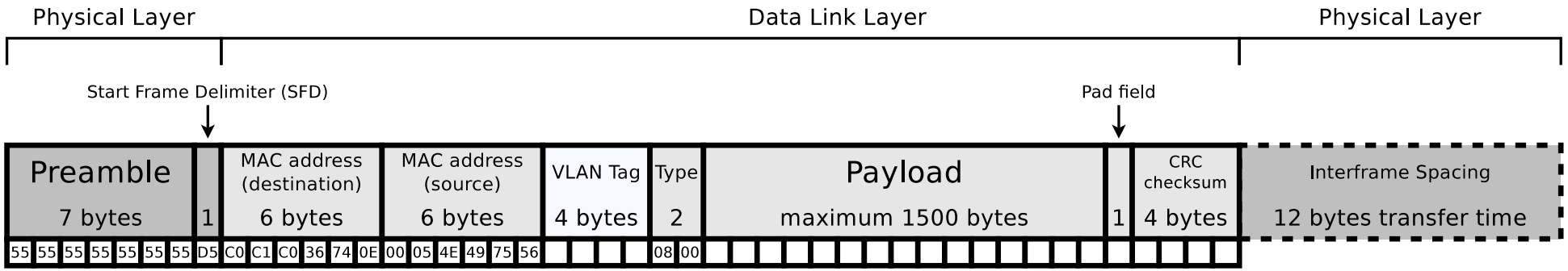
- Read out the own MAC address(es): `ip link` or `ifconfig`
- Read out the MAC address(es) of the neighbors (mostly the Routers): `ip neigh`
- Set MAC address: `ip link set dev <Interface> address <MAC Address>`
- Alternative: `ifconfig <Interface> promisc`
  and next: `ifconfig <Interface> hw ether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

Framing in current Computer Networks (1/4) – Ethernet



- Up-to-date Data Link Layer protocols (e.g. Ethernet and WLAN) work bit-oriented and not byte-oriented
  - Reason: This way, every character encoding can be used
- Preamble is a 7 bytes long bit sequence `101010 ... 1010`
  - Is used in bus networks (topologies) to synchronize the receiver with the clock and to identify clearly the beginning of the frame
  - Is followed by the SFD (1 byte) with the bit sequence `10101011`

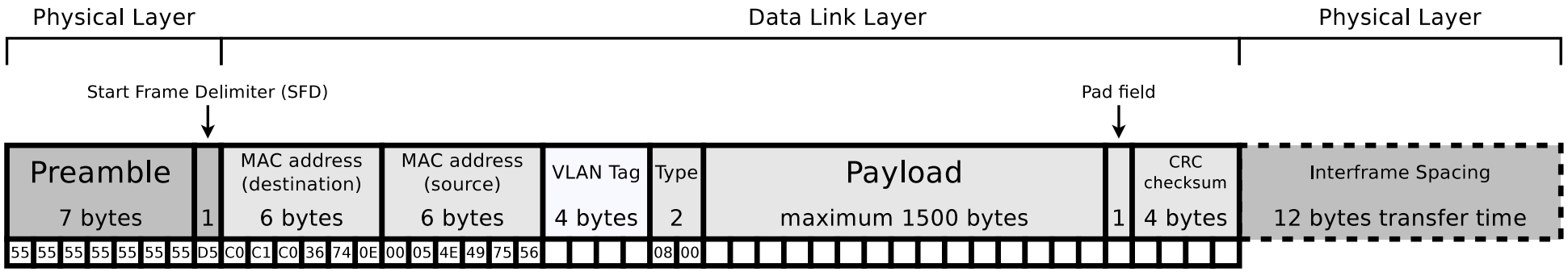
Framing in current Computer Networks (2/4) – Ethernet



- The fields for the physical addresses (MAC addresses) of sender and destination are 6 bytes long each
- The 4 bytes long optional VLAN tag contains, among others...
  - a 12 bits long VLAN ID ($\Longrightarrow$ see slide set 4)
  - and a 3 bits long field for the priority information
- The field `Type` contains the information what protocol is used in the next upper protocol 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`

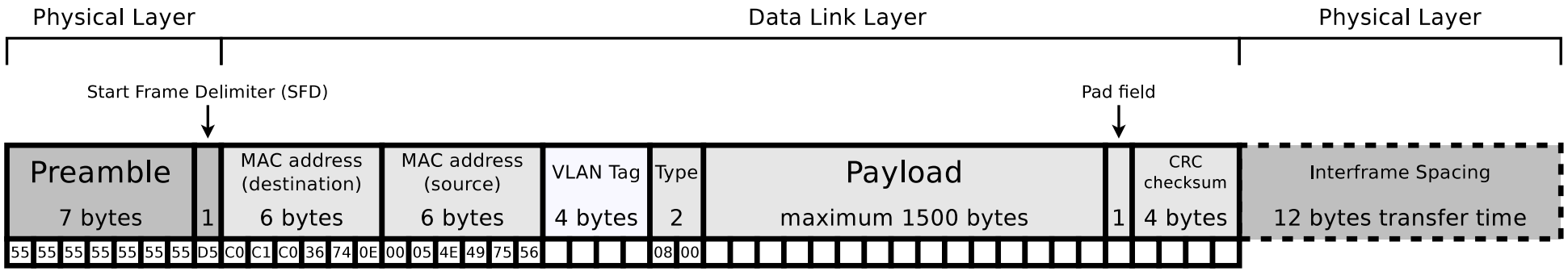
Framing in current Computer Networks (3/4) – Ethernet



- Minimum size of an Ethernet frame: 72 bytes
- Maximum size (including preamble and SFD): 1526 bytes
- The VLAN tag increases the maximum size by 4 bytes

- Each frame can contain a maximum of 1500 bytes payload
  - With the Pad field, the frame length can be increased to the minimum frame size (72 bytes) when needed
    - This is required to get the collision detection via CSMA/CD working ($\Longrightarrow$ slide set 6)
- The last field contains a checksum (32 bits) for all fields, except the preamble and SFD

Framing in current Computer Networks (4/4) – Ethernet



- The **Interframe Spacing** or **Interframe Gap** is the minimum idle period between the transmission of Ethernet frames via the transmission medium
- 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 collisions may rise)

Functioning of ARP (1/2)

- The **Address Resolution Protocol** (ARP) is used to resolve IP addresses of the Network Layer to MAC addresses of the Data Link Layer
- If a network device wants to transmit data to a receiver, it uses the receiver's IP address on the Network Layer
- But on the Data Link Layer, the MAC address is required
  - Therefore, **address resolution** must be carried out in the Data Link Layer
  - To find out the MAC address of a network device in the LAN, ARP sends a frame with the MAC broadcast address `FF-FF-FF-FF-FF-FF` as destination address
    - Each network device in the LAN receives and analyzes this frame
    - The frame contains the IP address of the searched network device
  - If a network device has this IP address, it sends an ARP response to the sender
    - The reported MAC address stores the sender in its local ARP cache

Functioning of ARP (2/2)

- The **ARP cache** is used to speed up the address resolution
  - It contains a table with these information for each entry:
    - Protocol type (IP)
    - Protocol address of the sender (IP address)
    - Hardware address of the sender (MAC address)
    - Time To Live (TTL)
  - The TTL is set by the operating system
  - If an entry in the table is used, the TTL is extended
- Modern Linux distributions discard entries after $\approx$ 5 minutes

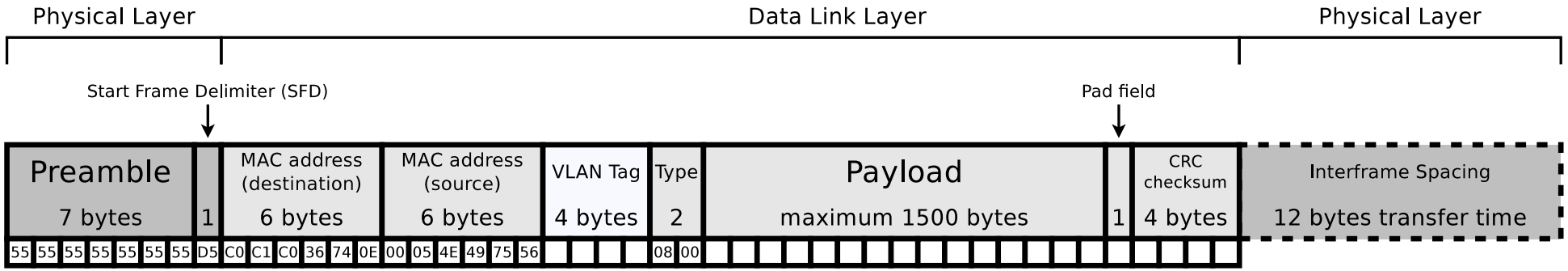
The ARP cache can be displayed via `arp -n` or `ip neighbour`

```
# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.178.1            ether   9c:c7:a6:b9:32:aa   C                     wlan0
192.168.178.24           ether   d4:85:64:3b:9f:65   C                     wlan0
192.168.178.41           ether   ec:1f:72:70:08:25   C                     wlan0
192.168.178.25           ether   cc:3a:61:d3:b3:bc   C                     wlan0
```

Address resolution requests can be send manually via `arping`

Structure of ARP Messages

- ARP messages are transmitted as payload via Ethernet frames
  - `type` = `0x0806` (for the ARP protocol)



- `HLEN` = hardware address (MAC address) length in bytes
  - For Ethernet: 6 bytes
- `PLEN` = IP address length in bytes
  - For IPv4: 4 bytes

32 bits (4 bytes)

Hardware type		Protocol type
HLEN	PLEN	Operation
MAC address (sender)		
MAC address (sender)		IP address (sender)
IP address (sender)		IP address (target)
IP address (target)		MAC address (target)
MAC address (target)		

In an ARP request is the content of the field `MAC address (target)` irrelevant