Computer Networks

http://int2cn.oncampus.de

state 27.06.2017 11:11

Content

Appendix

Computer Networks

arrangement

In the MOOC “Computer Networks” you will learn about the structure and functions of computer networks with an emphasis on the Internet. After an introductory chapter, the OSI model that is used to organize the remaining chapters is explained. The OSI model divides the tasks that have to be solved in the design of computer networks into different layers so that tasks can be handled separately.

The topics in this MOOC are selected in a way that is useful for computer scientists. Therefore, the lowest layer, which deals with the transmission of data bits via media, is only handled as part of the general presentation of the model. The second layer (Data Link Layer) is treated in chapter 3. This involves focusing on the issue of how to recognize and correct transmission errors as well as rules for shared use of transmission media. Because only data transfer to neighboring devices is possible in layers 1-2, chapter 4 (Network Layer, layer 3 in the model) deals with end-to-end communication that should also work worldwide. In particular, methods for efficient path selection are necessary here. The tasks related to layer 4 (Transport Layer), which are discussed in chapter 5, include dealing with transmission errors in end-to-end communications. The so-called higher layers (layers 5-7) are discussed in chapter 6. Chapter 6 primarily focuses on the World Wide Web and its accompanying protocol HTTP.

There is also a historical presentation available at the end as an optional chapter. This chapter is helpful for understanding the context why technical specifications are the way they are today.

1 Introduction and Network Topologies

arrangement

This introductory chapter discusses the current importance of computer networks, which is to a large extent based on the global adoption of the Internet.

After this motivation, some basic concepts are introduced and basic configuration options for computer networks are discussed along with their respective advantages and disadvantages. Using examples (university networks, wide area networks, networks in data centers), it is shown how these configuration options can be used in practice.

The models and technologies presented in the other chapters are defined by several standardization bodies. Therefore, the end of the chapter presents an overview of the standardization bodies relevant for computer networks.

1.1 Importance of Computer Networks

arrangement

Computer networks are omnipresent today because of the Internet. Whether it is with a DSL connection at home, a notebook at the university or a smartphone while on the go, we access the Internet today from a wide range of places. In the next few years, there will be a rapid increase in devices communicating with other devices via the Internet (the “Internet of Things”) which means the number of networked devices will continue to increase significantly.

While it often remains unclear to the average user how the data from his or her device is transmitted through the Internet, we would like to discuss this in more details in this MOOC.

For a computer scientist, there are a lot of possibilities that emerge from this knowledge, which extends beyond special tasks in network planning (such as campus networks, nationwide networks) or network management. For example, it is important to have an idea of the performance and operation of networks when you are planning and implementing network-based applications. It may not be enough to test such an application only in a local area because the application may then not be scalable later for nationwide or worldwide use (see Transport Layer chapter).

In addition to the career perspective, knowledge about network operations can also be interesting for you as a citizen because it gives you a deeper understanding of issues regarding telecommunications surveillance or net neutrality.

1.1.1 Internet Applications

Today the Internet has become an everyday communications tool because of the applications it offers. A distinction can be made here between the following types of applications:

- World Wide Web (including video portals, examples: Youtube, Vimeo)
- E-mail, messenger services (examples: university mail services, Hotmail, WhatsApp)
- Private or professional networks (examples: Facebook, MySpace, LinkedIn)
- Internet search engines (examples: Google, Bing)
- Encyclopaedias (example: Wikipedia)
- E-commerce (shopping, online banking, auctions) (examples: Amazon, PayPal, eBay)
- Online games (examples: Farmville, World of Warcraft)

Moreover, the Internet serves as the basis for cloud computing, where data, applications or entire networks can be outsourced to service providers in the Internet.

1.1.2 Internet Access

If you want to look at how access to the Internet occurs, you first have to distinguish between the situation in industrialized countries and the situation worldwide.

In industrialized countries such as Germany, telephone networks have been built for more than 100 years, so telephone access is available in almost all buildings. With the help of DSL technologies, these networks can be upgraded to higher bit rates, which makes this option the most widely used way of accessing the Internet. Alternatively, existing cable networks can be used for Internet connections or fibre-optic cables can be built to the end user. In Germany, the latter option is not very common yet because the construction regulations in Germany in comparison with other countries leads to higher costs, which can hardly be compensated by higher revenues (see Presentation of the FTTH Council Europe). In addition to these options for Internet access via fixed networks, mobile wireless Internet access is also playing an increasingly important role because third and fourth-generation mobile networks offer high data rates.

The situation in developing countries differs from industrialized countries because you cannot rely on a good telephone infrastructure there (especially in less densely populated areas). That is why Internet access via mobile networks with higher bit rates is significantly more important there (see Statistics pages of the International Telecommunication Union).

Concerning the growth of the data volume in the Internet, reference is often made to the Visual Networking Index by Cisco. In comparison with the past, only weak growth in data volume can be seen for fixed networks, whereas the data volume for data transmission in mobile networks grows very strongly. An estimate by the Internet Systems Consortium shows that now more than 1 billion devices are connected to the Internet (see ISC pages).

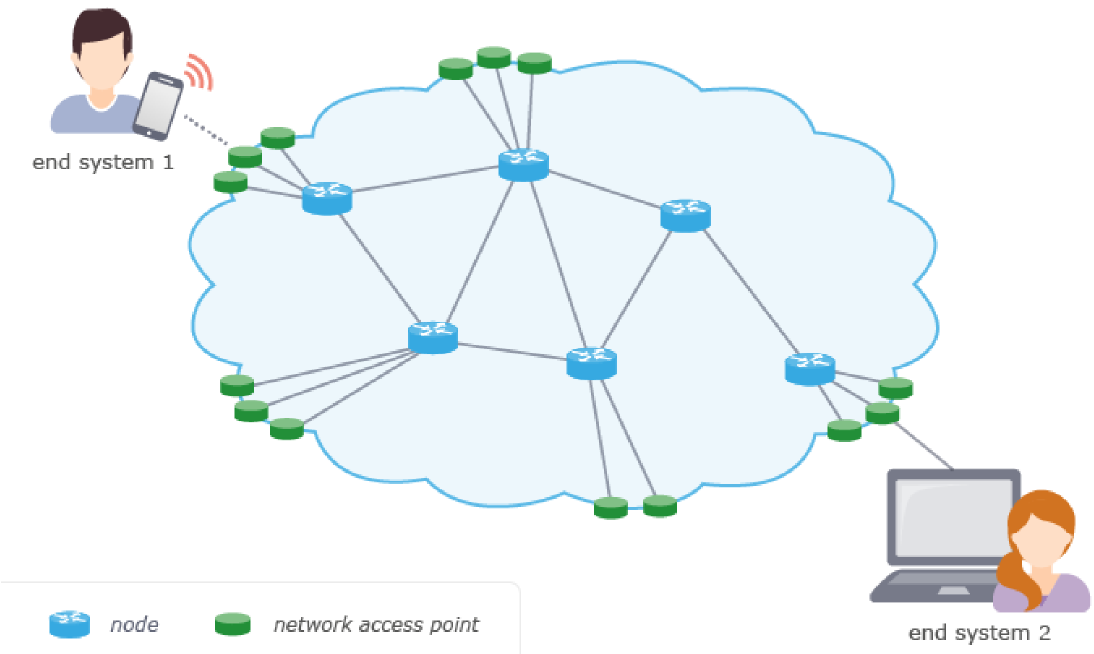
1.2 Fundamentals

arrangement

This section first explains some fundamental concepts and distinguishes between different kinds of computer networks. An important aspect here is the network topology that is used for a specific network. There are several basic topologies that are presented here along with their respective advantages and disadvantages. Following this, several examples of real topologies are explained so you can see how the basic options are used.

1.2.1 Nodes and End Systems

A computer network, as exemplified in the figure below, has the task to enable data exchange between **network access points**. Data units are transmitted from one network access point to one or more other network access points.



A communication network

A network consists of **nodes** and **end systems** or **hosts**. Nodes are understood to be all devices that are needed for the forwarding of data and that are invisible “in” the network for users. There are simple types of nodes that just amplify signals (so-called repeaters or hubs), while more complex nodes make path finding decisions using addresses (so-called switches or routers). The exact function of the nodes will be presented in the course of the MOOC.

End systems are connected to the network endpoints. These are generally familiar to us as PCs, printers, smartphones as well as television sets and network-enabled temperature sensors.

1.2.2 Classification of Computer Networks

When considering computer networks, we can classify them according to different criteria.

First, one can make a distinction according to the users for whom the network is designed. There are **public networks**, for which there are standardized options offered by service operators. A user may choose between several options, but in principle the options are the same for everyone. Examples of this include DSL lines, mobile telecommunications networks or Wi-Fi hotspots. In contrast to public networks, there are also **private networks**. These are networks that are created for exclusive use by a closed user group. An example of this is a network for a university campus, which is intended only for the operation of the university and is therefore only used by professors, staff and students. If, for example, a company that has several locations wants to interconnect these locations, a private network would be an option. This would allow the company to configure the network according to their own needs and in particular enable them to implement their own security requirements. However, it would be too costly in such a case to lay cables between different cities solely for this purpose. Therefore, such a network is created in reality by using the infrastructure of other networks and configuring a logical structure on top of it, which acts as a private network. Such a network is called a **virtual private network** (VPN).

When we consider parts of networks, we can distinguish between **core networks** and **access networks**. Core networks (also called backbone networks) are the main connection structures for networks, while access networks make it possible to reach the core network from many locations. Examples of access networks are DSL or cable networks, mobile telecommunications networks (GSM, UMTS, LTE), WLANs, or local area networks in companies or organizations. The so called "Wissenschaftsnetz" (German for scientific network) on the other hand represents the core network for the interconnection of scientific institutions in Germany.

Another important distinction is the size of the network as explained in the following. The technologies mentioned in the explanation should be understood as usual technical implementations. The actual term refers to the network size.

- **Personal area network** (PAN): PAN refers to networks where only the devices of a single user are interconnected with each other such that the extent of this network is less than 10 m. An example is the linking of a smartphone with a wireless headset via Bluetooth or a network consisting of wireless keyboard and mouse together with a computer.

- **Storage area network** (SAN): These are special networks within a data center where servers are connected to storage systems. They have an size of up to 100 m and use specific technologies for this purpose (fiber channel, Infiniband).
- **Local area network** (LAN): A LAN is a network within an organization's location and may have a size of 10 m up to 10 km. For local area networks without special requirements (such as typical office environments), Ethernet technology has become the only choice. The situation is similar in wireless local area networks, where there is now only the Wireless LAN technology. The term wireless LAN is not as general as LAN because the standardization body IEEE calls its technology Wireless LAN. Special networks are used for industrial production areas; they are called field buses. There are also special networks for networking within automobiles.
- **Metropolitan area network** (MAN): A MAN is a network with a size of 10 km to 100 km. In the past, there were specific technologies (such as FDDI) that were designed for MANs. Today LAN or WAN technology is used.
- **Wide area network** (WAN): WAN is a network with a size of more than 100 km, such as a Germany-wide network. In these networks, different technologies are used, such as IP, Ethernet, SDH, OTN, or MPLS.
- **Global area network** (GAN): This term refers to worldwide networks.

In the operation of networks, we can distinguish between **circuit switching** and **packet switching**, but different combinations are also possible. Roughly speaking, circuit switching means that communication routes between communication partners are permanently reserved. This principle comes from telephone networks. In contrast to this, the Internet operates on the basis of packet switching, where data to be transmitted is forwarded in the network in small data units (referred to as packets) independent from each other. This is explained in details in the chapter Network Layer.

Finally, the distinction between a computer network and a **distributed system** should be mentioned. An essential concept here is **transparency**. If the manner of implementation matters, then it is called non-transparent and it belongs to the computer networks area. If the implementation plays no role, then it is called transparent and is part of the distributed systems area. More specifically, for example, there is location transparency (do you know where certain activities take place in the network?), replication transparency (are the network connections and systems redundant and would they still function in case of failure?) and performance transparency (to which extent is the capacity of the network utilized?).

1.2.3 Network Topologies

arrangement

There are various structures that can be used if you want to connect end systems with each other in a fixed network. These structures are called **network topologies**. Often data transmission cannot be performed directly to the receiver so that further forwarding through additional intermediate systems or other end systems is necessary.

In the online version an video is shown here.

Link to video : http://www.youtube.com/embed/a79IqifAnh0

Network topologies

Basic topologies are discussed in the following subsections. The discussion of the advantages and disadvantages is based on the following criteria:

- Costs: Which costs are relevant for the network? How many cables are required and how long do they have to be? How complex are the functions of the systems? Is there a need for additional intermediate systems?
- Installation and expandability: How easy is it to put this network into operation and later expand it to additional devices?
- Transmission capacity: Can only one end system at a time successfully transmit data in the network, or is parallel communication possible? If parallel communication is possible, how many end systems can communicate simultaneously?
- Reliability: What are the effects of errors in the network? If end systems, intermediate systems or cables no longer work, does this affect the whole network?
- Troubleshooting: If typical error situations occur, how difficult is it to find the error and correct it?

- Broadcast: In local networks, you often want to make a broadcast, i.e. all end systems in the network are supposed to receive the data unit. For example, the protocol ARP (see ARP - Address Resolution Protocol) uses broadcasts to locate an end system with a specific IP address. How easy or difficult is it to realize the broadcast?
- Privacy: When two end systems communicate with each other in the network, a third end system might want to listen to this communication. Is it easy for this end system to simply listen to the communication between the other end systems?

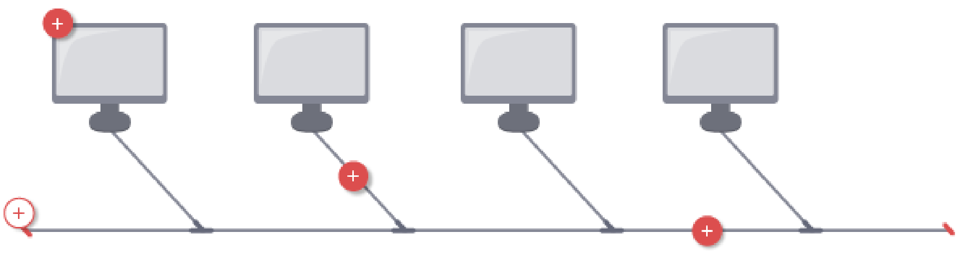
1.2.3.1 Bus Topology

In a **bus topology**, all devices (such as PCs in a computer network) are connected on a bus, i.e. a shared cable. The connection of end systems to the bus is passive. This means that each end system can read data on the bus, but does not have to worry about forwarding them to other terminals. In a bus, all end systems always receive a data unit even if a data unit is usually only intended for a particular end system. A consequence of this is that at any given time only one end system may transmit a data unit via the bus. Otherwise, the data units of different end system would overlap and cannot not be received properly. To avoid signal reflections, the cable ends are terminated by a **terminating resistor**.

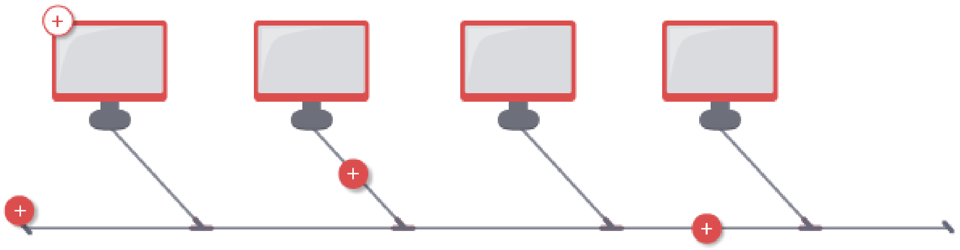
In the online version an rollover element is shown here.

Bus topology

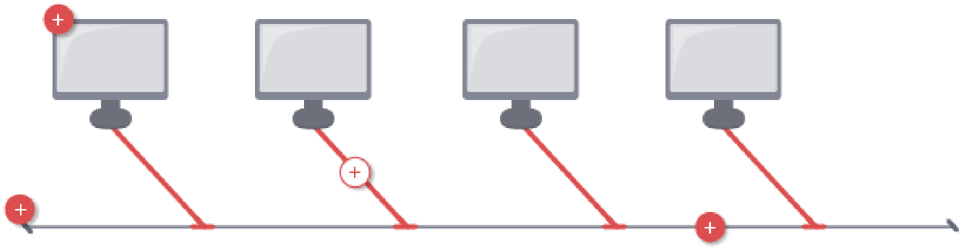
Begin printversion



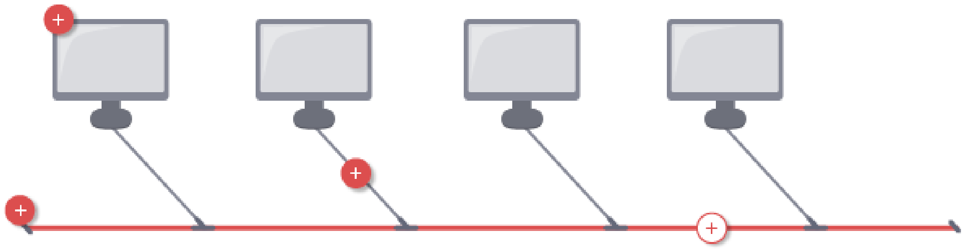
Terminator or terminal resistor with 50 Ohm to prevent reflections of signals.



Typical end system, e.g. a PC, that is connected to the bus via a network card.



A short cable allows to passively attach end systems to the bus.



The bus is a coaxial cable.

End printversion

Advantages and disadvantages of bus topology

Begin printversion

Advantages	Disadvantages
• Cost-effective The cable distances are short and no additional hardware is needed. • Simple installation Each end system can be attached withoou additional hardware and is directly attached to the bus. Additional end systems can be connected to the bus later. An extension of the bus may lead to difficulties (e.g. if the CSMA/CD method is used). • End system failure does not influence complete network Complete failure of a end system does not affect network operation. This is the typical case. If a broken end system sent signal to the bus, it would affect the whole network. • Broadcasting is simple A data unit can easily be sent to all other end systems because each data unit is delivered to all other end systems anyway, at least on the physical level. Usually, the end systems are configured in a way that they check via the destination address whether the data unit is intended for them. They stop to process the data unit if it is not addressed to them.	• Limited capacity No parallel communication is possible. This would lead to collisions of data units and wrong data unit processing. This is an important reason why this topology cannot be used for WANs. • Difficult troubleshooting Disturbances on the bus are difficult to locate especially if end system send erroneous signals. Disturbance can occur due to other cables near the bus or due to loose contacts. • Not secure against eavesdropping Any end system receives all data units on the bus.

End printversion

annotation

The situation in a bus topology is similar to wireless networks. If, for example, there are several participants in a room and they want to use a common WLAN, then only one person can successfully transmit data at a time. Similarly, it is only possible to perform broadcasts and not deliberately send the data only to one other end system (remark: “beamforming” as a possibility of the latest standard is ignored here).

annotation

In the marketing area, the term “bus” is sometimes not used carefully because bus systems were at least temporarily easy to place on the market. USB stands for “universal serial bus” although it is actually a star topology system (see Wikipedia article on USB). That is why there are USB hubs.

1.2.3.2 Star Topology

In a star topology, all end systems are interconnected with each other via an additional network component **(star coupler)** using their own cables. The star coupler is not an end system. It just serves to forward data units. Due to this configuration, every communication runs through the star coupler.

There are two types of star couplers:

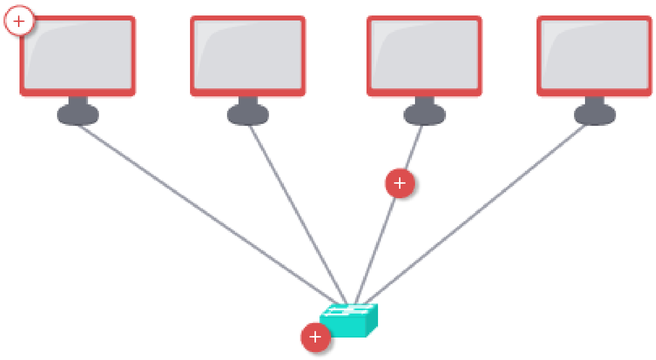
- A **hub** forwards signals that it receives on a port to all other ports. This is relatively simple and therefore inexpensive to implement because, among other things, no addresses have to be evaluated. As a result of this, however, only one device may send data at a time. Otherwise collisions may occur, as with a bus.
- A **switch** forwards signals in a targeted way, i.e. only to the end system that is to receive the data unit. This makes it necessary to evaluate addresses during forwarding and manage which end system is connected to which port. However, this has the advantage that parallel communication between end systems is possible. For example, an end system at port 1 can send a data unit to an end system at port 2 while end systems at ports 3 and 4 simultaneously communicate with each other. The number of parallel communications that is actually possible depends on the internal capabilities of the switch.

In local networks, hubs hardly exist anymore because switches have become increasingly powerful and less expensive over time. Therefore, the discussion of the advantages and disadvantages of the star topology refers to a switch in the center of the star.

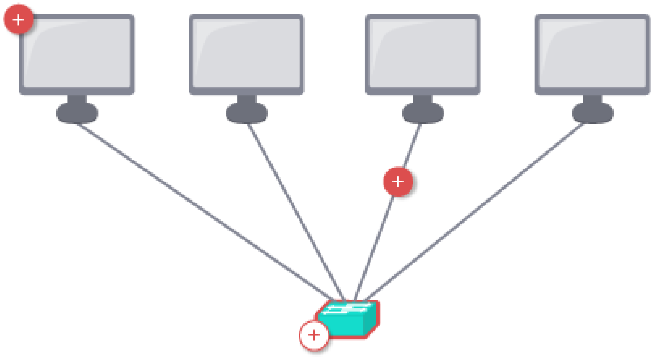
In the online version an rollover element is shown here.

Star topology

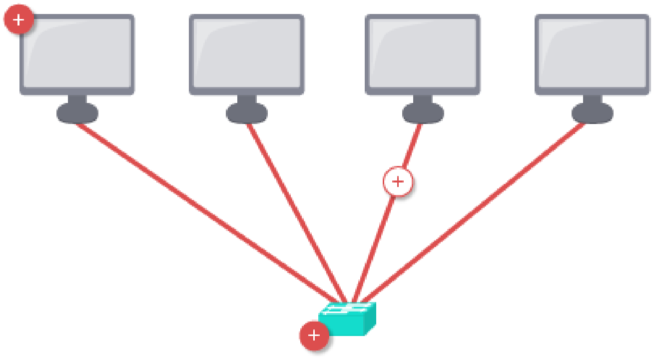
Begin printversion



Typical end system, e.g. a PC, which is connected to the central network component.



In a star topology, there is a central network component to which each end system has an exclusive link.



A typical twisted pair network cable with RJ45 plug.

End printversion

Advantages and disadvantages of the star topology (with switch)

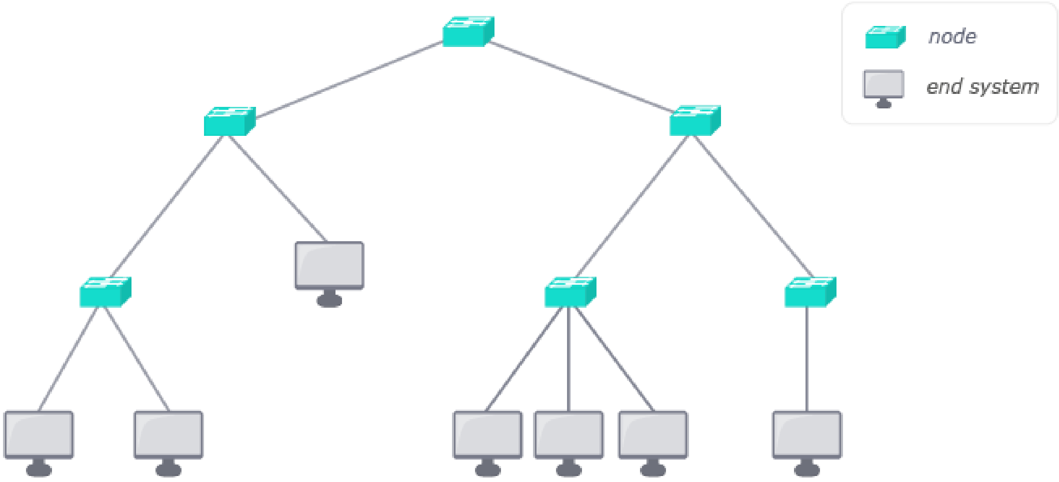
Begin printversion

Advantages	Disadvantages
• High capacity The switch enables parallel communication between end systems. Therefore, possibilities for communication are much better than witout this option. • Easy troubleshooting Since each end system has its own network segment, the errors can easily be mapped to a link or end system. • Easy expansion Switches have a certain number of ports (e.g 24 or 48 ports). As long as there are free ports additional end systems can be connected easily. • Broadcasting is simple In case of a broadcast the switch can work like the simpler it. It sends the broadcast on all ports (except of the input port). Therefore, a broadcast is easy to realize.	• Single point-of-failure The main disadvantage of the topology is related to the switch. If the switch fails, the whole network does not work anymore. In contrast, the failure of an end system or of the link to an end system only affects the end system. • Costs for cables and switch Each end system has to be directly connected to the switch, which requires a lot of cables. Often the switch cannot be placed in the center of the star due to the constraints of the building. The star point has to be acquired. However, as already mentioned before, switches became a lot cheaper over the years.

End printversion

1.2.3.3 Tree Topology

If several stars are combined to form a larger unit by connecting star couplers together, it results in a tree topology.



Tree topology

This structure often provides the basis for a **hierarchical network** that is typically used in office buildings. For example, if a company has several adjacent office buildings on their premises, the network could be reasonably organized in the following way: In the lowest hierarchy level, all work spaces on one floor are grouped together; in the next level, the different floors are grouped together, and in the last level the various buildings of the company are grouped together.

The advantages and disadvantages of the tree topology result from the features of the star topology. In particular, the failure of one node leads to the separation of subnets from the rest of the network. In addition, one must keep in mind that a lot of traffic can aggregate at the upper levels of the hierarchy. This can be counteracted with higher transmission bit rates at the higher levels (such as 10 Gbit/s there and 1 Gbit/s at the lower levels), but such a topology is nevertheless only appropriate for use in a local area.

1.2.3.4 Ring Topology

In a **ring topology**, all end systems are connected in a ring with each other. Each end system is connected to two other end systems, which are clearly defined as predecessor and successor, so data units are always only sent in one direction. If a device fails or the line is disconnected, the network is no longer functional.

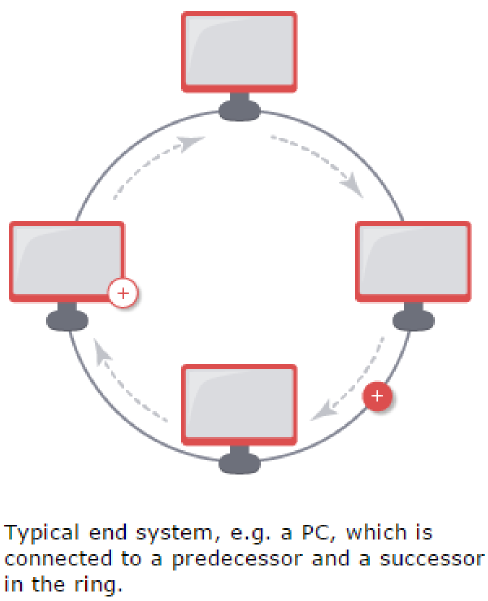
Acknowledgements to confirm the successful reception of data units are often implemented. In case of a successful reception an end system sets an acknowledgement bit and then forwards the data unit further on the ring. Through the ring structure, the data unit returns later to the sender, who can then do a bit-by-bit comparison to determine whether a transmission error has occurred.

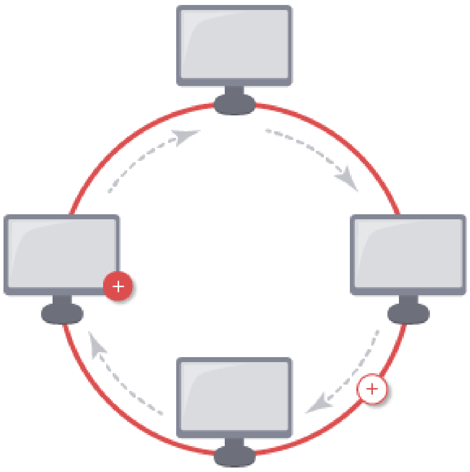
In the ring, end systems each receive the data units and forward them further after they have regenerated them. During regeneration, the original signal strength is restored. This operation enables large expansions of ring topologies. Moreover, each link does not have to be implemented using the same medium, which means that copper cables as well as fibre-optic cables can be used for the links of the topology. However, such cases are very rare.

In the online version an rollover element is shown here.

Ring topology

Begin printversion





The ring can be built based on various transmission media, such as twisted pair, coaxial, or fibre optic cable.

End printversion

To protect the system from total failure in the event of an error, two parallel rings are usually created. In the second ring, the communication flows in the opposite direction of the first ring. The following discussion is based on such a scenario.

Advantages and disadvantages of the ring topology (double ring)

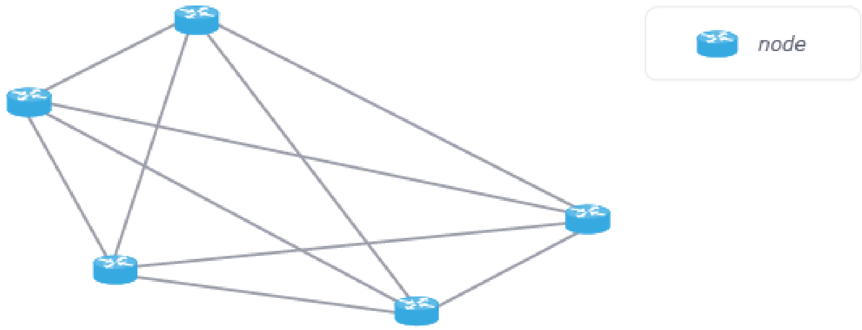
Begin printversion

Advantages	Disadvantages
• Parallel communication In a double ring parallel communication on both rings is always possible. Whether it is also possible to transmit data units on different links of the same ring in parallel, depends on the specific system. A former system for LANs called Token Ring did not allow for this due to the timing constraints. However, such a parallel communication is possible in today's WANs. • Easy extension Additional end systems can simply be added to the ring. Due to the regeneration of signals, large network sizes are possible for this topology. • Broadcasting is easy In a ring topology it is easy to realize a broadcast. An end systems sends the broadcast to the ring which then travels through the ring. Later, it arrives again at the sender who can remove it from the ring.	• Low robustness In a double the failure of one link can be compensated by using the other ring. However, a broken end system which cannot forward an data leads to a complete failure. At this point it should be mentioned that it is possible to implement a topology which is a ring only when regarding it from a logical point of view. On the physical level it can be star topology with a so called wire center in the middle of the star. The wire center allows to exclude broken end systems from the ring so that ring can still be used. This implementation as physical star has the disadvantage that is does not allow for large network sizes. • Complex systems Since end systems need to have capabilities to actively regenerate signals and due to more complex network management, the end systems are relatively expensive. For LANs these cost factors are often more relevant than relative low costs for cables. • No protection against eavesdropping Because each data unit traverses the whole ring to be removed from the ring by the sender, all other end systems receive the data unit and can take a look into the communication contents. • Error search difficult If the ring does not work anymore, several investigation steps may be necessary to identify the broken link or end system.

End printversion

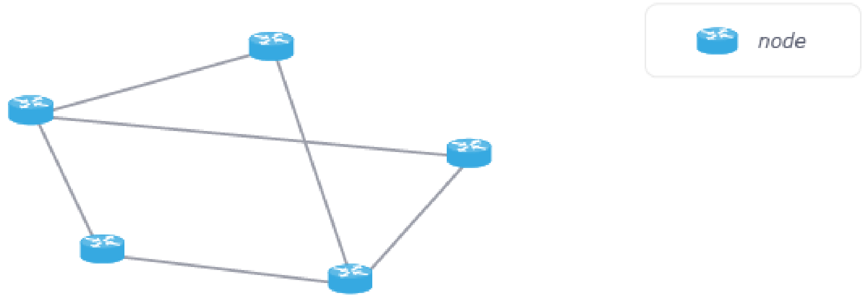
1.2.3.5 Mesh Topology

In a **mesh topology**, there are redundant connections, intended to protect the network against failures. In a **fully meshed network**, all nodes of a network are connected with each other. This situation is, however, only theoretical even starting with a few nodes because the cost and effort for implementing all the connections for the mesh increases significantly.



Fully meshed network

If the possible redundant connections are only partially realized, it is a **partially meshed network**. In this case, you can e.g. design the network so that every node is connected with at least three other nodes. Then you can continue to communicate despite the failure of two links.



Partially meshed network

The discussion of advantages and disadvantages is based on a partially meshed network.

Advantages and disadvantages of a partially meshed network

Begin printversion

Advantages	Disadvantages
• High robustness against failures The redundant links can compensate the failures of some links. In addition, the failure of a node does not affect the whole network. • Parallel communication Several parallel communications are possible in such a network. • Simple error search If errors in the network occur, still large parts of the network still work. Therefore, it is relatively easy to find out which link or node does not work anymore.	• High costs Many connections have to be implemented. This means, a lot of cables are needed , but also a lot of interfaces on the nodes. In addition, a path finding problem needs to be addressed because there are often several paths which can be used to send data units from one node to another node. This capability has to be implemented on the nodes as well. • Extension difficult If a new node is added to the topology, this node should be linked to the others in a redundant way as well. This requires more effort than in other topologies. • Broadcasting difficult As discussed before, broadcasting is easy in other topologies. However, there is a difficulty in this topology. If a node works in a way that it send the broadcast on all other ports (except of the input port), a flood of data units will occur due to duplicates. Therefore, additional measures are needed to control the flood. One can imagine that it would be possible to recognize data units as duplicate by indicators in the data unit. However, the typical situation is that broadcasts are not allowed in this topology. • Eavesdropping may be possible In this network eavesdropping may be possible. It depends whether a path between two nodes uses another node which wants to get access to their communication.

End printversion

Partially meshed networks are used in important networks only, especially in wide area networks. In these cases, the nodes are not end systems but network nodes to which LANs are connected. These LANs can then be implemented using one of the other topologies.

1.2.4 Example Networks

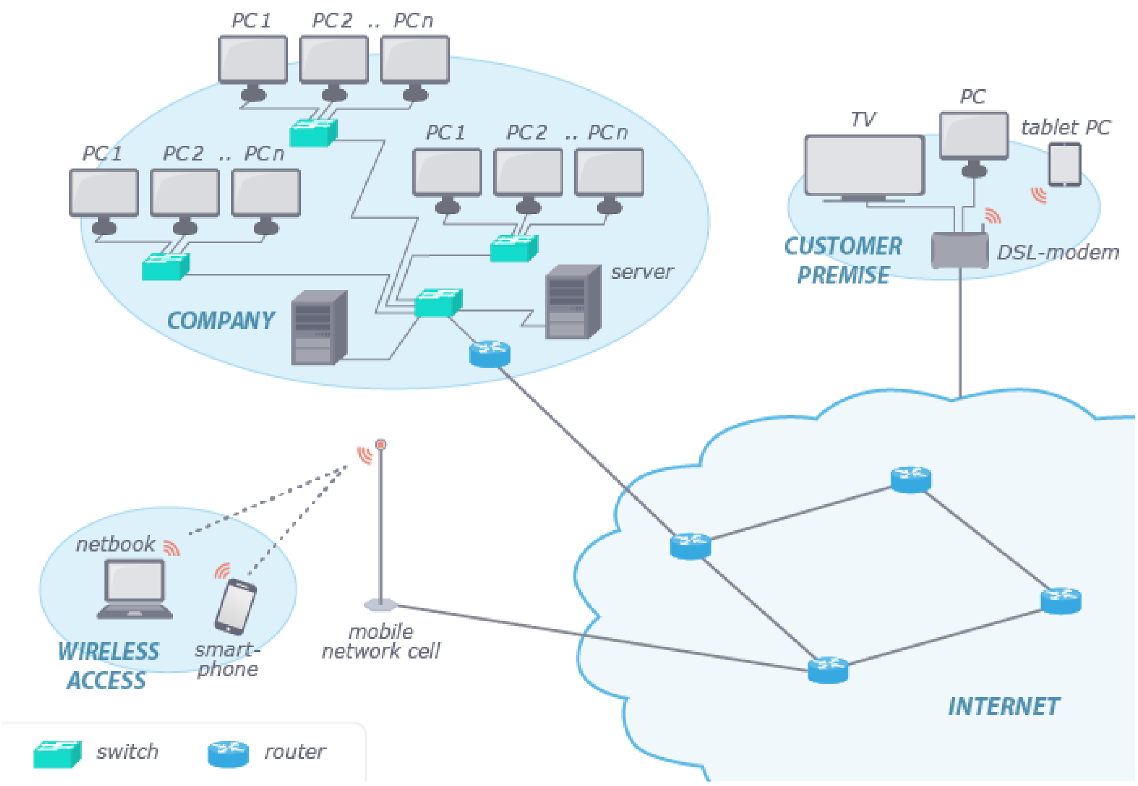
arrangement

In the online version an video is shown here.

Link to video : http://www.youtube.com/embed/9d9OlNoykp4

Example topologies

The topologies described in the previous section can be combined to take advantage of multiple network types. In particular, we see a combination of many topologies in the Internet, which consists of the connection of many individual networks. The following example of a network configuration can be used for illustration; the operations of the individual networks will be explained in more detail later.



Internet configuration example

Company: A network of a company. The PCs in each department are connected with each other via a switch. Multiple departments are in turn connected with each other via a switch. Servers are also connected to this switch. A router connects the company's network to the Internet.

Router: A router determines the paths by which data unit will be transmitted to the receiver.

Internet: A large global, high-performance network, which has been built by many organizations. All these organizations are also called ISPs (Internet Service Provider). Each of these ISPs has its own network, called a backbone. The backbone is mainly based on a set of partially meshed routers.

Private premise: A usual private premise has several computers, tablet PCs and telephones. The devices are connected to the Internet via the telephone network using DSL or a cable modem.

Smartphone: Mobile phone, which can be used for Internet access.

Netbook: Lightweight notebook version for mobile Internet access.

Mobile radio cell: The radio area of a base station for a mobile telecommunications network of the various mobile telecommunications providers. All mobile cells together provide in a nationwide network for wireless telecommunication.

Examples of real networks will be explained in the following subsections.

1.2.4.1 University Networks

An abstract scenario is presented here as an example of a university network. Configurations like this can be found at many universities today. However, often in practice you have to determine how to deal with the remnants of previous network generations. This example should therefore be regarded as a model for a completely new campus.

First, a basic idea of the design here is that important network components are doubled so the failure of a single device can be compensated. The connection to the wide area network therefore happens via two routers, where the current routers are also internally redundant (for example: two power supplies). These routers implement two different connections to the wide area network. Wide area networks for scientific purpose are operated by National Research and Education Networks (NRENs). Examples of NRENs are Internet2 and ESnet in the USA and the Wissenschaftsnetz (meaning scientific network) in Germany.

Within the university network, the routers are connected to two central switches. Firewalls, central servers and WLAN controllers are connected to both switches. In addition, the central switches are connected with additional switches for the respective buildings; redundant connections to both central switches are usual here as well. Within buildings, the building switches are connected to floor switches, and the user end systems are connected to these floor switches. Such switches have, for example, 48 ports with a bit rate of 1 Gigabit/s for the end systems and are then connected to the higher level at 10 Gigabit/s.

One should not calculate the data rate for the connection according to the higher level by assuming that all users will simultaneously use their network access at the full bit rate. Experience has shown that this is almost never the case and would otherwise lead to an oversized and far too expensive network. The degree to which redundant structures are also implemented within buildings varies.

An important question is also the extent to which VoIP is used. For new installations, you want to avoid a separate data network, so end-users receive VoIP phones, which are also connected to switches. You have to consider how to ensure good quality for VoIP calls so that they are not disturbed by data transfers. VoIP data units can be treated with preference in the network, or the VoIP phones can be connected to separate switches.

In addition to this network structure, there is also the university's data center, which houses important servers and storage systems. Within such a data center, there are special storage area networks, which differ in their mode of operation from the other areas of the university campus.

1.2.4.2 Wissenschaftsnetz

The universities in Germany are connected with each other and with other networks via the Wissenschaftsnetz. The Wissenschaftsnetz, abbreviated in its present generation as X-WiN, is operated by DFN-Verein (an association to which many universities and research institutions belong).

With regard to the network, one has to distinguish between two levels. On the one hand, there is the so-called optical platform (for an illustration, see topology map). It consists of fiber-optic links between cities in Germany where the sites of the X-WiN are found. Typically, these sites are housed on the campuses of important universities or research institutions. In technical terms, the fiber-optic connections consist of fiber-optic pairs because each fiber-optic unit can only be used in one direction. The pairs of fiber are leased on a long-term basis by DFN-Verein from various providers. These providers often lay large cable bundles consisting of hundreds of fibers and offer individual fibers for lease. The DFN-Verein installed DWDM technology on these unlit fibers (technical term: “dark fiber”) in order to transmit data using them. Explained in a simplified manner, this means that the bit streams are transmitted via fibers using different colours of the light. For example, 10 Gbit/s can be transmitted with yellow light, 10 Gbit/s with green light, and 100 Gbit/s with blue light. In reality, different wavelength ranges are used that are not part of visible light. While the laser for generating the light signals and the receiving photodiodes only need to be installed at the respective end points for the connections, it may be necessary to refresh the signals along the path. This is necessary after about 80 km. Currently the DWDM technology from ECI Telecom is used.

A logical topology is implemented on the basis of the optical platform. It consists of routers, which are placed at all locations of the X-WiN. The models ASR 9000 and 7609 from the manufacturer Cisco are used for this purpose. The routers are interconnected, and the logical topology is different from the real topology. If, for example, you look at the path between Hanover and Frankfurt, you see that Göttingen, Kassel, Marburg and Giessen lie between them. Using the optical technology, however, it is possible to let the light beams pass through a site without evaluating the signals on the light beam locally. Using this technology, you can logically create a direct connection between Hanover and Frankfurt. You can imagine this as an express train that does not stop at smaller stations. Even though every site is connected to the logical topology, this direction connection is sometimes implemented in addition if there is a higher demand for transmission capacity between some sites. This is particularly the case to and from Frankfurt because the very important Internet exchange node DE-CIX is located there. This Internet exchange connects the networks of many providers.

The current topology of X-WiN is presented twice a year at the DFN Betriebstagung event in a presentation entitled "Neues aus dem X-WiN" (first day, before lunch). The slides including the current topology can be accessed afterwards on the event webpage.

1.2.4.3 GEANT

In the various European countries, there are research networks similar to Germany’s Wissenschaftsnetz (e.g. SWITCH in Switzerland or GARR in Italy). These in turn are connected to one another via the European research network GEANT. When data is transmitted, for example, from a German university to a French university, the data units are first found in the network of the German university. Then they are transferred to the Wissenschaftsnetz and subsequently enter via GEANT into the French research network RENATER. In France, there are also specific regional networks through which the French university network is reached.

GEANT was originally an acronym, where the G stood for Gigabit. In 2000, it was still outstanding that a bit rate of 1 Gbit/s could be reached, whereas the network today already contains numerous 100 Gbit/s connections (see topology map). Similar to the X-WiN, GEANT consists of an optical level and an IP platform (see short description on the GEANT webpage). The manufacturer Infinera provides the DWDM technology, and Juniper is the supplier for the routers. GEANT is financed by the EU; there was also a rule that applied until the 2010s that there could only be one network site (point of presence) per country. This no longer applies, so that e.g. Germany now also has a site in Hamburg in addition to Frankfurt.

In the US, there are the research networks Internet2 and ESnet, which share a common optical platform. ESnet supports research institutions with very high bit rate requirements, while Internet2 connects many scientific organizations. ESnet provides a portal where current status data of the network is freely accessible.

1.2.4.4 Further Example Networks

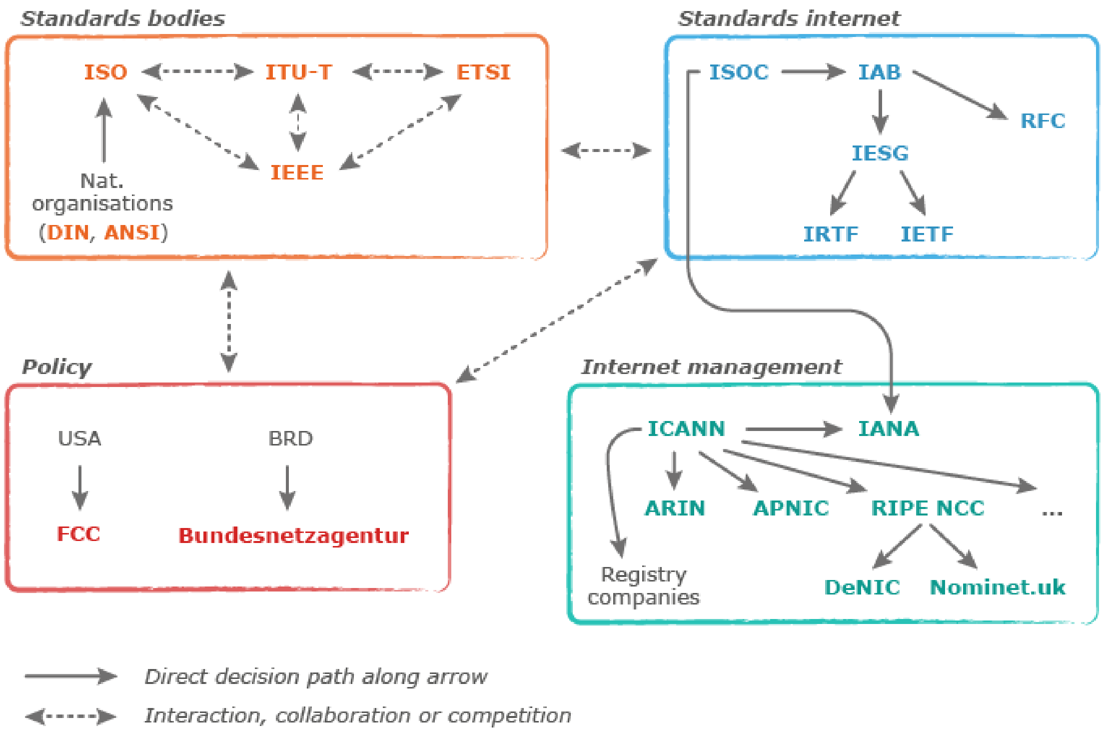
In a blog post, Facebook presented its data center in Altoona (US state of Indiana) in detail. This network is characterized by a very strong meshing of different areas. This strong internal meshing seems to be necessary given that there are many cross-relationships between the data stored on the various systems because a lot of information needs to be linked together to reply to user requests.

Although this is not a single network, at this point a map of the undersea cables laid throughout the world should be mentioned. These undersea cables, whose installation is very complex (see interview with an expert from the Japanese company NEC), are the backbone of global communications. It can be seen that in some areas relatively few cables are available. For example, the communication between Europe and South America often takes place via Miami (see news about BELLA project). A project by Facebook and Microsoft on a transatlantic cable is presented in a Wired.com article.

1.3 Standardization and Regulation

arrangement

For computer networks that are connected worldwide through the Internet to function reliably, common standards are needed. Therefore, this section describes organizations that provide such standards. As you will see, standardization directly related to the Internet is distinct from the usual approaches of other standardization organizations. In addition, the management of domain names and Internet address ranges is introduced as well as the role of government regulations.



Important organizations for Internet standardization and administration and their relations to other standards bodies and politics

1.3.1 Standardization in general

The **ISO** (International Organization for Standardization), which has its headquarters in Geneva, was founded in 1947 for the international standardization of various areas. Each country is represented in this organization through national standards organizations. Germany is represented by DIN (Deutsches Institut für Normung e.V.) and the US is represented by ANSI (American National Standards Institute). In the field of computer networks, the OSI model is of great importance. This model is discussed in chapter 2.

While the ISO covers almost all possible standardization areas, there are two exceptions. Standardization in the area of electricity and electronics is done by IEC (International Electrotechnical Commission). **ITU** (International Telecommunications Union), which is also located in Geneva and was founded in 1865, is responsible for the area of telecommunications. As a specialized agency of the United Nations (UN), ITU coordinates the construction and operation of telecommunications networks and services. It is responsible for the regulation, standardization, coordination and development of international telecommunications. The standards for telecommunications are issued by the sub-organization **ITU-T**, where each standard begins with a letter followed by a dot and a number. For example, the standard G.652 specifies the features for a fibre-optic cable type. The name of ITU-T was CCITT (Comité Consultatif International Télégraphique et Téléphonique) until 1993; this older name is rarely used.

In the telecommunications sector, there is also **ETSI** (European Telecommunications Standards Institute), which was founded in 1988 and is headquartered in Sophia-Antipolis. This organization was founded for the establishment of telecommunications standards for Europe such as the Euro-ISDN. The standardization activities of ETSI in the area of mobile communications are very important; they established the GSM standard for the second generation of mobile telecommunications. After this standard was adopted by other continents, its further development and the development of the UMTS and LTE standards has been continued by ETSI together with comparable organizations from other continents as part of the 3rd Generation Partnership Project.

IEEE is originally an American association for standardization in the field of electrical engineering. This means that many companies work together here to agree on common standards. However, the representatives of the respective companies always have the interests of their own company in view. In practice, the specifications of IEEE for local area networks in the 802 working group are very important. This working group developed the Ethernet standard for local fixed networks (802.3) and the Wireless LAN standard (802.11). The standards of the 802 working group can be downloaded free of charge.

1.3.2 Standardization in the Internet

Standardization related to the Internet works significantly different from the standardization bodies described in the Standardization in general section. This way is expressed in the motto “We reject kings, presidents and voting. We believe in rough consensus and running code” (see TAO document). The approach has resulted fom the way how the Internet evolved. One of the first Internet nodes (the network was then called ARPAnet) was installed at the University of California at Los Angeles in 1969. A group of graduate students discussed there about how protocols should look like for operating the network. They assumed, however, that BBN, which was the company providing the hardware for the Internet node, would also provide appropriate software so that their own considerations would not be relevant. BBN, however, only delivered the hardware, which led to the protocols established by the students being used. In this respect, the rather informal manner of cooperating amongst students was adopted such that the technical specifications are still called RFCs (Request for Comments) today.

Over time, it has been recognized that a certain organizational structure is necessary. The umbrella organization created for this purpose is the **Internet Society**, which is a nonprofit organisation. This holds also for its affiliated organizations. Anyone can register for free to join. For Germany, there is the ISOC-DE (Internet Society German Chapter).

Technical development is driven by the **IAB** (Internet Architecture Board). Its 13 members have the task to look at the development of the Internet as a whole. The **IESG** (Internet Engineering Steering Group) coordinates activities between the various IETF working groups and is subordinated to the IAB. The **IETF** (Internet Engineering Task Force) is an open international association of network designers, operators and companies that contribute to the development of the Internet and its operation and draw up proposals for new protocols and technologies. The association is officially represented by the ISOC. While the IETF focuses on current technical issues, the **IRTF** (Internet Research Task Force) takes care of fundamental issues and problems regarding the Internet. Research groups are working on the topics of Internet protocols, applications, architecture and technologies.

As mentioned previously, the documents regarding standardization in the Internet are called RFCs. The RFCs are given a status, i.e. they may, for example, no longer be valid because they have been superseded by newer RFCs. Only a small proportion of the

RFCs are therefore currently valid standards (see list of standard RFCs). An important principle is that an RFC with the status of "draft standard" has been implemented independently by two different groups. This allows for the detection of ambiguities in the RFCs. Once an RFC is published, it will not be changed anymore. To achieve uniform presentation, the RFCs are checked by an **RFC Editor**. Until 1998, it was only one person (Jon Postel); today it is a small group. The RFCs can be accessed on the Internet free of charge. A review on 40 years of RFCs was published as RFC 5540. The page arkko.com contains some statistics about RFCs. You can see here that the RFCs originated in the early years from authors working in science and research. With the increasing importance of the Internet and its commercialization, more and more authors are working for companies.

In addition to e-mail, the World Wide Web, invented in 1990, is the application that led to the current importance of the Internet. The further development of related languages such as HTML, CSS, XML, etc. is headed by the **W3C** (World Wide Web Consortium). Its technical specifications are called recommendations.

1.3.3 Internet Administration

In order for the Internet to be used, domain names and IP address ranges have to be administrated. This management is organized in a hierarchical manner, with the umbrella organization **ICANN** at the top. ICANN (Internet Corporation for Assigned Names and Numbers) was founded in 1998 as a nonprofit organization to carry out the assignment and management of IP addresses and domain names. The **IANA** (Internet Assigned Numbers Authority), which has existed since 1988, is now a subunit of ICANN. It manages the assignment of IP addresses, domain names and port numbers. Until 2016, ICANN was under the supervision of the US government and was then transferred to a multi-stakeholder model.

The IP address blocks and administration of domain names are distributed to five Regional Internet Registries (RIRs) that are responsible for different parts of the world.

- AfriNIC (African Network Information Centre) for Africa
- APNIC (Asia-Pacific Network Information Centre) for Asia and the Pacific
- ARIN (American Registry for Internet Numbers) for North America
- RIPE NCC (RIPE Network Coordination Centre) for Europe and the Middle East
- LACNIC (Latin America and Caribbean Network Information Centre) for Latin America and the Caribbean

RIPE provides address spaces to the ISPs. These work as Local Internet Registries (LIR) so that they provide address spaces to their customers. For example, DFN-Verein has got address spaces from RIPE that it can further distribute to the connected universities.

The domain name administration is further delegated to national registries. For Germany, this is **DENIC** (Deutsches Network Information Center), which is a registered cooperative of German ISPs. Their responsibilities include:

- Operation of the primary name server for the top-level domain DE
- Nationwide central registration of domains under the top-level domain DE
- Administration of the Internet in cooperation with international bodies

The IANA commissions companies to carry out the management of generic top-level domains. So, for example, Verisign manages the TLDs .com and .net. The registration of each domain name can be carried out at registries (see list of registrars at ICANN).

1.3.4 Government Regulation

Governments authorize national authorities to oversee the communications sector. This involves in particular regulating competition between different providers. The situation in many countries is that incumbent providers such as Deutsche Telekom AG in Germany would continue to occupy a dominant position if certain restrictions were not imposed.

In Germany, the **Bundesnetzagentur** (translation is federal network agency) is responsible for this. In addition to telecommunications, the authority also takes care of regulation in the areas of “electricity and gas”, “mail” and “railways”. The telecommunications market is thereby regulated for example by awarding licenses for mobile telecommunication networks. For example, for the issuing of a licence for the LTE mobile communications standard, network provisioning in rural areas was made a prerequisite for installation in urban areas. End customers who have problems with their network provider may appeal to the Bundesnetzagentur.

In the USA, the FCC (Federal Communications Commission) has the role of the Bundesnetzagentur with respect to telecommunications.

1.3.5 Other Organizations

To complete the overview, examples of other important organizations are mentioned here.

The **BSI** (Bundesamt für Sicherheit in der Informationstechnik, translation is federal office for information security) promotes the development of technologies for secure IT networks. Its "IT-Grundschutz" (IT baseline protection guidelines) documents provide recommendations on how organizations can build their IT infrastructure in a secure manner. These recommendations are available in German and English. Bürger-CERT is intended for individual citizens. You can subscribe to a newsletter which provides warnings about current weaknesses in popular software.

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V., translation is German association for information technology, telecommunications and new media) is Germany's leading association for companies in information, telecommunications and new media.

1.4 Exercises - Introduction and Network Topologies

task

Tasks for beginners

Task 1:
Use the web page speedtest.net to check the performance of your Internet connection. Give answers to two questions afterwards.

Task 2:
Cisco's Visual Networking Index is a frequent reference related to data volume growth in the Internet. Take a look at the current document and retrieve two pieces of information from it.

Task 3:
The European research backbone network GEANT allows for an insight into its current network state via a network weathermap. In this view it is possible to click on each link to get more detailed information (see also graphs). Try out the possibilities of the tool and give answers to two questions afterwards.

Tasks for advanced learners

Task 1:
In the questions related to the last task for beginners the term peering has already been mentioned. Take a look at the web pages of DE-CIX, which is one of the largest Internet exchange points in the world and is located in Frankfurt, Germany, to find out what this term exactly means.

Task 2:
Submarine cables are a crucial part of the infrastructure for global communication. Answer one question about a selected submarine cable by using a worldwide submarine cable map.

Task 3:
RFCs are important documents related to standardization in the Internet. RFCs can be accessed on IETF's web pages. How the IETF works is explained in the TAO document. In addition, there is the external page arkko.com which provides statistics about RFCs. Answer three questions about RFCs later on.

Task 4:
Persons who are responsible for network domains from an administrative and a technical point of view have to be mentioned in the whois service. Such a service for the .de domain is available at DENIC. Reply to a question in this context.

1.5 Summary - Introduction and Network Topologies

In this chapter, you have been given an overview of the complexity of today's computer networks. They are the result of many years of development, which led to their worldwide expansion. This expansion was, however, possible only on the basis of international standards.

Today computer networks are a part of information technology, which is currently subject to extremely rapid changes. Developments such as cloud computing, high-performance mobile devices and the Internet of Things are contributing dramatically to such changes.