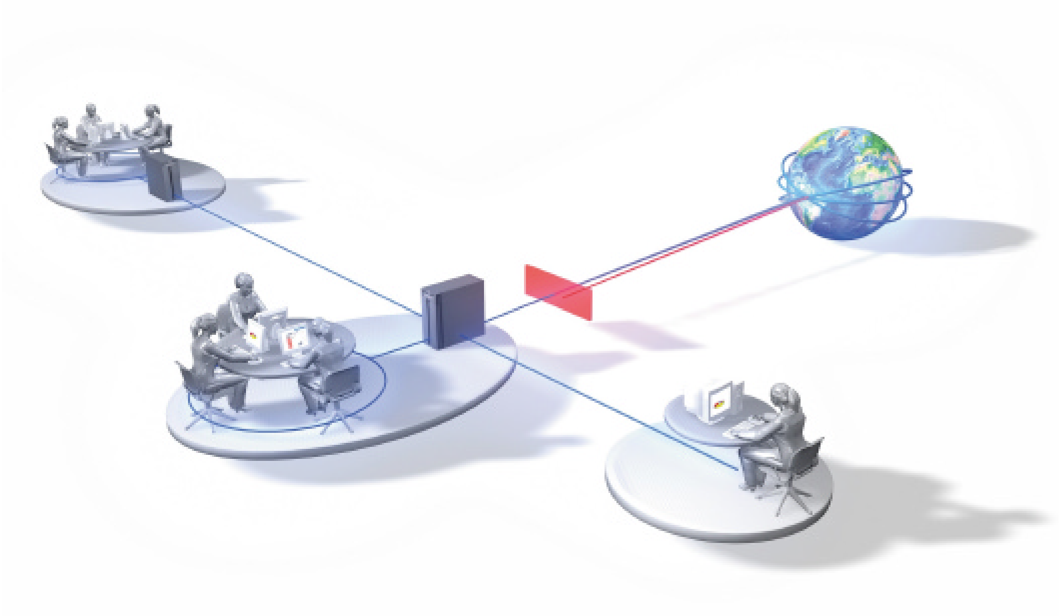
Computer Networks

- Things to Know -



Patrick Gött

Dennis Landscheidt

Stephan Wollny

WIBI 02 A GR

Tutor:

Prof. Dr. Rainer Beedgen

Table of Contents

Table of Abbreviations

IT	Information Technology
cf.	confer
p.	page
pp.	pages
i.e.	*id est*: that is
LAN	Local Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
WLAN	Wireless Local Area Network
PDA	Personal Digital Assistant
cp.	compare
IEEE	Institute of Electrical and Electronics Engineers
max	maximum
Mbit	Megabit
s	second
m	meter
GHz	Gigahertz
OSI	Open System Interconnection
TCP	Transmission Control Protocol
IP	Internet Protocol
e.g.	*exempli gratia*: for example
ISM	Industrial Scientific Medical
MB	Megabyte
IBIT	International Business Information Technology
ISO	International Organisation of Standardization
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
POP	Post Office Protocol
IMAP	Internet Messaging Application Program
SSH	Secure Shell

LDAP	Lightweight Directory Access Protocol
etc	et cetera
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
DNS	Domain Name Service
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
MAC	Medium Access Control
CRC	Cyclic Redundancy Check
DSL	Digital Subscriber Line
TV	Television
ISDN	Integrated Services Digital Network
sqm	square meter
PC	Personal Computer
AP	Access Point
id.	*idem:* the same

Table of Figures

Index of Tables

1. Significance of Computer Networks

Computer networks are an essential part of companies' IT interest, as they offer the possibility to communicate with hundreds of branches in such a way that you can receive business data or gross revenues of these branches in real time. Administration and Management of multinational companies are dependent on these networks.

The first networks were characterized by front end processors, which were function units acting in front of the local networks and communicating with its counterparts from other local networks. Usually these processors were identical concerning their manufacturer. However, the front end processors have been abolished by standardization and decentralization and have been replaced by open communication systems, i.e. hardware components from different manufacturers are capable of communicating. Open communication systems consist of system components that are based on public standards and norms. Components of open communication systems are portable, independent from its manufacturer and thus support interoperability in communication systems (cf. Hansen/Neumann 2001, p. 1113).

Today, a computer network is a collection of autonomous computers, which are interconnected through data transfer equipments. This means that computers' functions work independently from each other and that they can exchange information. An interconnection between two computers exists, if they can exchange information (cf. Tannenbaum 1992, p. 2).

A common error is the confusion of a distributed system and a computer network. Though their hardware seems to be comparable, the former one provides different software with services that enable operations to be done explicitly by the system. Distributed control and computing are hidden from the user in contrast to the latter one.

2. Classification of Computer Networks

A classification of computer networks can be done according to different aspects. The most significant ones are mentioned below.

2.1. Geographical Criteria

The classification depends on the distance between processors and the networks are categorized according to the following table.

Interprocessor Distance	Classification
0 - 1 km	Local Area Network (LAN)
1 km - 10 km	Metropolitan Area Network (MAN)
10 km - 1000 km	Wide Area Network (WAN)
> 1000 km	Internet

Table 1 – Classification of Networks by Distance

2.2. Physical Criteria

Depending on the physical medium, a network can either be a physical connected network or a wireless one. In the last few years the importance of wireless local area networks and Bluetooth has increased immensely. For this reason they will be dealt with in a more detailed way.

2.2.1. Bluetooth

Bluetooth has been developed by a Swedish company, namely Ericsson in 1995. It is an open standard for data transfer within small distances (up to 10 m). It replaces wired connections and is used for instance for data exchanges between mobiles and headset or printers and PDA's. It uses the licence free wireless net ISM (Industrial Scientific Medical) at a frequency of 2.4 GHz, which corresponds to the IEEE 802.11b standard used by WLAN. Conclusively there are often conflicts between WLAN and Bluetooth. Hence it is not recommendable to employ both techniques at

the same time. Besides this conflict there is the danger of injury of human health (cf. Frisch/ Hölzel/ Lintermann/ Schaefer 2001, p. 98).
Data is transferred in packages up to a size of 1 Mbit/s. The used radio waves for this transfer can pass through fixed bodies and send to various receivers at the same time. Consequently it is a broadcast network.
Bluetooth networks are defined as Pikonets and can have a maximum of eight different adapters. In each Pikonet, one of these adapters adopts a leading role (master device).

2.2.2. Wireless Local Area Networks (WLAN)

In just the past few years, wireless LANs have conquered a significant niche in the local area network market (cf. Stallings 2002, p. 434). The advantages of introducing WLAN are for instance mobility, portability and flexibility. Components can easily be added, wherever you are. Another reason for its success was the inability to provide cabling for networks for example in historical buildings. Nevertheless disadvantages are also known and have been discussed various times in press: costs for components are comparatively high, security of data can be a problem and effects of the radiation are seen as insalubrious.
The most significant applications for a WLAN are LAN extensions, wireless internet access and ad hoc networks.
A wired LAN can be expanded or sometimes even be substituted by a wireless LAN in order to save costs for cabling and offer new services e.g. in hospitals where doctors have access to their patients' data everywhere. Figure 2 illustrates such a LAN extension. Components have access to the WLAN due to their wireless LAN adapter and access points being installed in the building.
Wireless internet access is often used in public buildings, schools and universities, where a lot of users bring their own laptop and can have access to the internet. This is also the idea of the University of Cooperative Education in Mannheim, which intends to offer this possibility to its students. It is often seen as a service.
Last but not least, an ad hoc network is defined as a peer-to-peer network set up temporarily to meet some immediate need (cf. id. 2001, p. 437). In

Latin, *ad hoc* literally means "for this," further meaning "for this purpose only," and thus usually temporary. A fast way of small data exchange between two portal computers or PDA's for example is the use of such a network (cp. Figure 1).

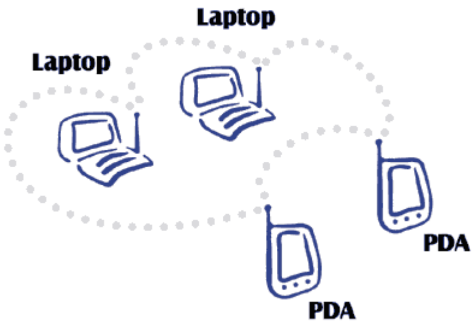


Figure 1 - Ad Hoc Network

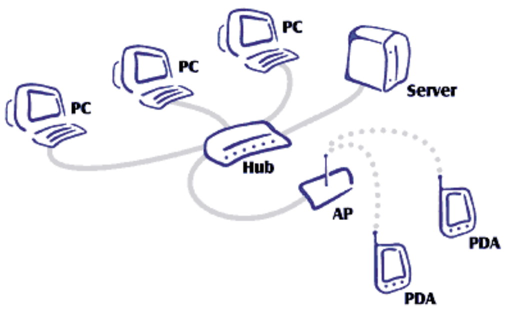


Figure 2 – LAN Extended with WLAN

Since 1990 the IEEE (Institute of Electrical and Electronics Engineers) 802.11 working group has developed a standard for wireless LANs. The most common version of this standard is IEEE 802.11b.

IEEE 802.11 Standards			
	802.11b	**802.11a**	**802.11g**
Max bit rate, raw	11 Mbit/s	54 Mbit/s	54 Mbit/s
net	5.5 Mbit/s	22-26 Mbit/s	17-22 Mbit/s
Frequency Band	2.4 GHz	5 GHz	2.4 GHz
Max range rate	57 m	12 m	19 m

Table 2 – IEEE 802.11 Standards

Like all IEEE-802 standards, 802.11b also focuses on the two lowest layers of the OSI reference model, which will be explained in further detail below (cf. Hansen/Neumann 2001, p. 1241). This results in the fact that you can use any protocol of the transportation layer, e.g. the TCP/IP protocol.

2.3. Structure

Networks can also be categorized depending on the structure of the network and the different ways the nodes (data stations) are related to each other. The network topology defines this structure (cf. id., p. 1134).

In **bus networks**, every workstation (or node) is connected to a main cable called the bus. As a matter of fact, every workstation is directly connected with every other workstation in the network. This fact is equivalent to the **mesh network**, where every node has multiple connections.

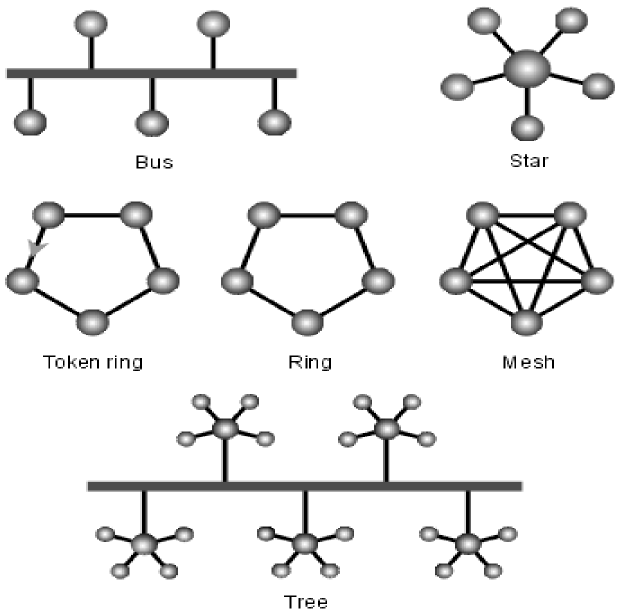


Figure 3 – Network Topologies

A central computer or server, all workstations are connected to, and which they use to communicate with other nodes, is the main feature of a **star network**. In contrast to it, in a **ring network** computers are connected in a closed loop configuration. Adjacent nodes are connected directly. To send data to non-adjacent nodes, inter-workstations are used. A **token ring network** is a specialized kind of a ring. The structure is the same, but information only flows in one direction.

Last but not least, a **tree network** is a mixture of a bus and a star network. The centres of the different stars are connected by a bus.

The main difference between these kinds of nets is the way their communication channels are used. Point-to-point networks (star, tree and mesh networks) for instance provide separate channels and are normally used for extensive networks. Nodes receive messages, investigate them and forward them if necessary (cf. id., p. 1134). On the other hand broadcast networks (ring, token ring and bus networks) use one communication channel so that every node has access to any information that is exchanged.

2.4. Transmission Rate

As a matter of fact a network can also be characterized by its transmission rate, i.e. the volume of data that can be transferred. Accordingly a network is classified as a 10MB/s, a Gigabit or a Terabit one.

2.5. Functionality

The objective and functionality of a network can be the supply of users, the connection between servers and the connection between different networks. The first one is indicated as a frond-end net whereas the second one is considered as back-end one. Finally, a network mainly intending to connect various networks is a backbone net.

3. The Layer Model

3.1. Application of the Layer Model

As pointed out above the topology of computer networks is often very complex. Consequently computer networks require high coordination standards. In these networks a lot of problems have to be solved, like e.g. addressing. In general experts come to the conclusion, that the definition of communication partner's cooperation in networks is a complex problem (cf. id., p. 1143).
There are two approaches to solve this problem. One possibility is manufacturer dependent systems, so called **closed** or **proprietary systems**. As long as all computers in a network use hard- and software from the same manufacturer, information exchange is not as difficult, since they use certain standards e.g. with protocols. However, these systems often have the disadvantage, that it is nearly impossible to integrate elements from other manufacturers into the network.
The more common networks are so called **open systems**. In these networks there are certain rules manufacturers have to pay attention to in order to assure communication between the different work stations. It is open to others for the purpose of information exchange in the sense that all open systems use the appropriate standards.
The solution for the problem of different network architectures is the implementation of certain standards. One way to do this is the so called **layer model**. It describes the differentiation of distinct tasks in order to reduce the complexity of communication within networks.
Consider the following example (cp. Figure 4) from everyday life, which is used to describe the functionality as well as the basic principles of the layer model.
In his practical term an IBIT student worked in Tokyo. After a while, he decides to write a letter to his former boss, because this appears to be more personal than just an email. His former boss only speaks Japanese; our example's IBIT student only speaks German. Since he neither knows

the language nor does he know the address of the company, the student hands the letter out to his firm.

The company's shipping department knows that there is somebody in Tokyo, who speaks English and so the letter is translated into English. The IBIT student neither knows the language the letter is tanslated to nor which further steps are taken by the firm and in which order they are done. The business seeks out the exact address und hands the letter out to the post office.

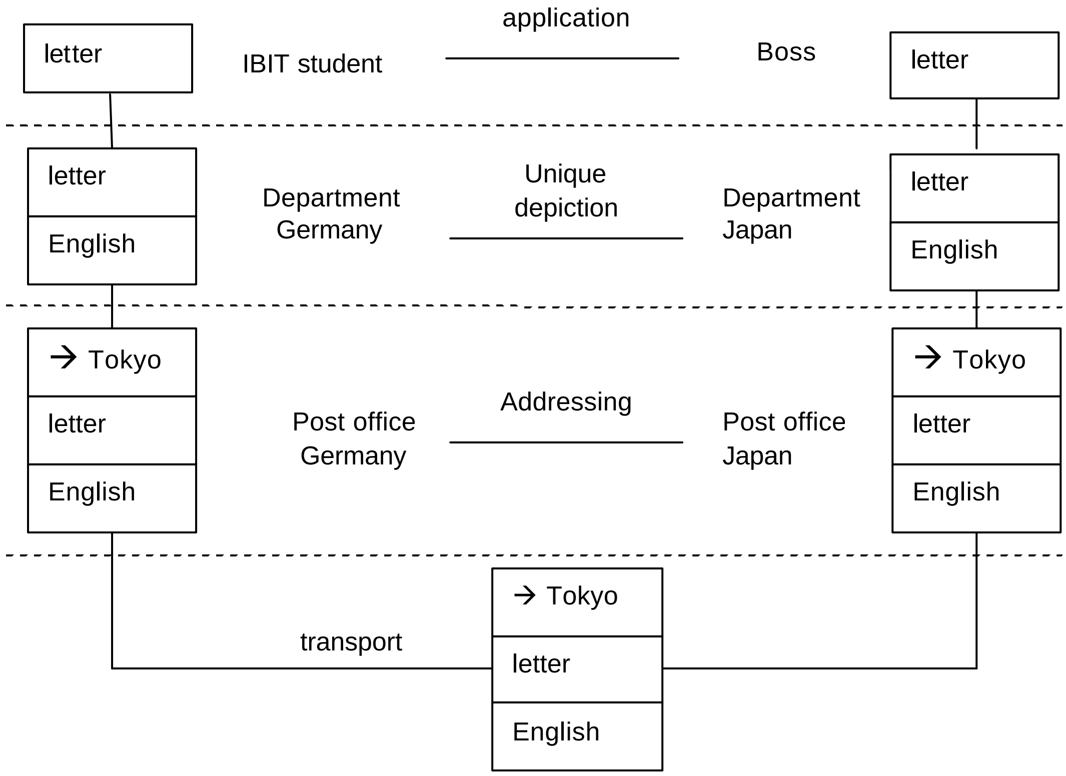


Figure 4 - Example of a Layer Model in Everyday Life (Wiedemann Script S. 43-45)

The next steps are not known to any of the previously involved departments. Whether the letter is sent by truck, boat or plane, is out of the firm's and the post office's control. It can be assumed, that the letter arrives in Japan, where it passes through the same departments/layers, but in the opposite direction.

This example is supposed to point out, how communication is handled in computer networks. The lowest layer corresponds to the transport protocol. It is used to exchange the media –the letter- via post road. The next higher layer is responsible for the addressing, the following for a unique depiction.

In our case this is the translation into English. The highest layer corresponds to the application.

An important criterion: Every single layer uses the lower layer's services and is only active in its own area of responsibility.

It is of great importance to understand, that not only the highest layers communicate (IBIT student and boss), but that communication also takes place between the lower levels. Every single layer adds relevant information for partners on the same level of hierarchy.

3.2. The ISO/OSI Layer Model

ISO in association with several other international and national committees have produced the most common layer model for Open Systems Interconnection, known as OSI. This is a very loose standard, which promotes the development of protocols designed to permit open systems interconnection. It also functions as a framework into which existing standards may be slotted. It should act as an aid in designing future protocol standards.

Keep in mind that it is only an abstract model that does not describe any sort of soft- or hardware. The internals of the layers is of no importance, but the interfaces are and each successive layer uses the facilities of the previous one. By standardizing the function of layers and their interfaces OSI attempts to allow a user to alter techniques used in a given layer without affecting the appearance of the overall system to the user. This will allow the user to switch manufacturers without having to sacrifice his system.

The OSI model consists of seven layers:

- Physical Layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application Layer

Each layer (called (n)-layer) provides a service to the layer immediately above it in the hierarchy ((n+1)-layer) and is defined by the services it provides. For each layer there is the definition of a protocol which governs how peer entities (processes on the same level) communicate with each other. The functions of each layer will be described in the next section.

3.3. The Functions of the Seven Layers

1. The **physical layer** provides electrical, functional, and procedural characteristics to activate, maintain, and deactivate physical links that transparently send the bit stream. This involves specifics about the cables, the plug and the corresponding pin assignment. It only recognises individual bits ("1" or "0"), but not characters or multicharacter frames. Furthermore the direction of the data stream has to be specified. In addition one hast to differentiate between serial and parallel data transfer (cf. Zenk 2003, pp. 283-284).
2. The **data link layer** provides functional and procedural means to transfer data between network entities and (possibly) correct transmission errors. Furthermore, it provides for activation, maintenance, and deactivation of data link connections, grouping of bits into characters and message frames, character and frame synchronisation, error control, media access control, and flow control.
3. The **network layer** provides independence from data transfer technology, relaying and routing considerations. Moreover, it masks peculiarities of data transfer medium from higher layers and provides switching and routing functions to establish, maintain, and terminate network layer connections and transfer data between users. Furthermore it splits packages into the corresponding length.
4. The **transport layer** provides transparent transfer of data between systems, relieving upper layers from concern with providing reliable and cost effective data transfer; provides end-to-end control and information interchange with quality of service needed by the

application program. It is the first true end-to-end layer. The transport layer is the uppermost layer of the transport system.

5. Contrarily the **session layer** is the lowest layer of the application system. It provides mechanisms for organising and structuring dialogues between application processes; mechanisms allow for two-way simultaneous or two-way alternate operation, establishment of major and minor synchronization points, and techniques for structuring data exchanges.
6. The **presentation layer** provides independence to application processes from differences in data representation, which is in syntax; syntax selection and conversion provided by allowing the user to select a "presentation context" with conversion between alternative contexts.
7. The **application layer** is concerned with the requirements of application. All application processes use the service elements provided by the application layer. The elements include library routines which perform interprocess communication, provide common procedures for constructing application protocols and for accessing the services provided by servers which reside on the network. (cf. Hansen 2001, pp. 1146-1149)

4. The Internet Architecture

The most common and most important protocols on layer four to seven are the Internet-Protocols, which are referred to as the TCP/IP-protocol-family. It consists of four layers that are producer independent and makes up the logical foundation of the internet. Actually the naming for the protocol family is a bit misleading. Even though TCP (Transmission Control Protocol) and IP (Internet Protocol) are the two most important protocols of the TCP/IP family a lot more protocols are included. The OSI model can also be transferred to the internet architecture, although it only uses four instead of seven layers. Some experts say that the fact that the seven layers of the ISO/OSI model have been reduced to just four layers is the reason for the great success of TCP/IP. Moreover its advantages are caused by its simple construction and great flexibility.

<table>
<tr><td>Application layer</td><td rowspan="3">Application layer</td><td rowspan="3">HTTP, FTP, SMTP, POP, IMAP, LDAP, Telnet, SSH, etc.</td></tr>
<tr><td>Presentation layer</td></tr>
<tr><td>Session layer</td></tr>
<tr><td>Transport layer</td><td>Transport layer</td><td>TCP, UDP</td></tr>
<tr><td>Network layer</td><td>Internet layer</td><td>IP, ICMP</td></tr>
<tr><td>Data link layer</td><td rowspan="2">Link layer</td><td>ARP, IEEE 802</td></tr>
<tr><td>Physical layer</td><td>Hardware</td></tr>
<tr><td>ISP/OSI model</td><td>internet model</td><td>realization</td></tr>
</table>

Table 3 – Classification of the 4-Layer Model

Other advantages include the simplicity to connect different networks with each other. This can be achieved via Gateways or Routers. Consequently workstations from different networks can communicate with each other (cf. Zenk 2003, p. 293). The four internet layers can be described as follows:

1. The internet protocols do not define any independent protocols of the physical and data link layer. However, the **link layer** defines interface and help protocols, so that they can cooperate with protocols of lower layers.

On this layer there are network protocols. Practically this indicates the combination of hardware, e.g. a network adapter and software, in most cases the corresponding driver. Protocols on this layer can itself have lower protocols, but this is not defined. The most common protocol for LANs is the Ethernet-family, which will be described in further detail in one of the following sections.

2. The **internet layer** is the same as OSI's network layer. In this layer IP plays a mayor role. Amongst other things IP defines worldwide distinct internet addresses, the IP addresses – a 32 bit number, consisting of four parts separated by periods. In order to assure that users can recall certain IP-addresses at a later point of time the numeric IP-addresses can be transferred to symbolic addresses via the internet service DNS (Domain Name Service). These addresses are the base of choosing the way in the internet. Furthermore, these protocols support the combination of different network technologies to one single logical net.
3. The **transport layer** consists of the second core protocol: TCP. It provides a reliable full duplex data stream between two communication partners. This data stream allows two workstations to communicate at the same time, i.e. it provides a two-way connection. Upon using this protocol the user can send data in any size or split it into any given number of packages, without having to take into consideration, which package has to be sent first. TCP adds its own header to the package, which identifies the port it wants to address at the defined workstation in the internet layer. Ports define, which server program is about to be addressed on the workstation. Common ports are 80 for HTTP or 25 for SMTP for example. An alternative protocol to TCP is UDP. TCP und UDP are never used together. TCP serves as a byte-stream-channel and UDP as a news channel.
4. UDP and TCP are the base for the **application layer**. SMTP (Simple Mail Transfer Protocol,) FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol) and Telnet are possible applications. The ports defined for the application layer never address a clearly

distinct program, but a program that uses a clearly defined protocol. The allocation of the ports (0 – 1023) have been agreed upon worldwide, i.e. port 80 will always indicate a HTTP server on any workstation. In other word upon opening a website this service will always get port 80. Still it is possible to open more instances. Every website after the first will dynamically receive a new port thus ensuring that more than one server of the same protocol can be accessed at the same time.

The internet architecture is not such a strict layer model as the OSI model. Programmers can develop and add any applications and channel abstractions, which are based on an existing protocol (cf. Peterson/Davie 2000, p. 39).

5. CSMA/CD and Ethernet (IEEE 802.3)

Ethernet is the most common LAN standard. It was developed in Palo Alto by Robert Metcalf and David Boggs in 1973 (cf. Hansen/ Neumann 2001, p. 1201). It is a diffusion network that uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and offers a maximum bit rate of 10 Mbit/s.

Nowadays IEEE 802.3 is one of the most successful protocols in the market. It is based upon the physical- and data link layer of the OSI layer model. Its frame (cp. Figure 7) and consequently its functionality are quite easy to understand. It starts with the preamble, which is responsible for data synchronisation and is followed by the destination and source address. These addresses are MAC (Medium Access Control) addresses and each one comprises of 6 bytes. The first 3 bytes are reserved for the manufacturer for instance Intel, 3 Com or DLink and the other half is used for a unique identification of every network device. Hence, you can address any network card as it has a unique address. The type indicates the higher layer protocol, usually IP (cf. http://www.cs.umd.edu/~shankar/417-F01/Slides/chapter5b-aus/sld013.htm, March 6th 2004). The transferred data can comprise up to 1,500 bytes, while CRC (cyclical redundancy check) just needs four. CRC is a method to detect errors in data transfer. If an error is detected the frame will be deleted.

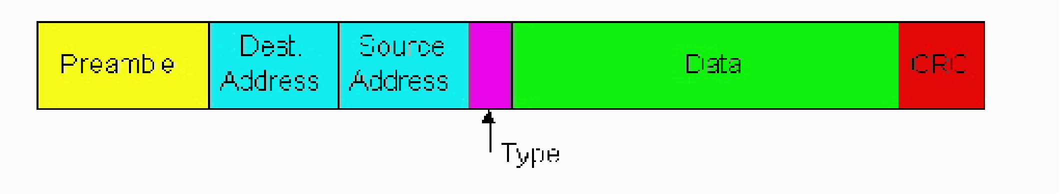


Figure 5 – Structure of an Ethernet Frame

The access to data in an Ethernet is realized due to the use of CSMA/CD. All components in this kind of network use an equally shared medium for communication. The sending of data can however only be realized by one workstation at any point of time. To send data, every device has to determine whether the medium is occupied or not. If it is not vacant the interface has to wait an intern frame gap of 96 bytes before starting to send. Nevertheless there is the possibility of two interfaces starting to send at the same time after having determined that there is no traffic in the medium, which would result in a collision of data and lead to data errors. To avoid these incidents every component in the network is capable of realizing such a collision by sending an interference signal, the so called jam. As a matter of fact the above described collision would be detected by both interfaces and both would stop sending immediately. In order to assure that the transfer of data is not stopped, an integrated random mechanism determines whether a component directly continues to send or waits an interval, which is indicated as slot time. If the usage rate of the network is comparatively high, the intervals generated are longer in order to avoid additional collisions. If the frame was not sent after 16 attempts it would be rejected and send an error message to the above protocol layers (cf. Frisch/ Hölzel/ Lintermann/ Schaefer 2001, p. 88).

Depending on the speed of an Ethernet-LAN one distinguishes between Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s), Gigabit-Ethernet (1000 Mbit/s), and 10-Gigabit-Ethernet (10000 Mbit/s). Estimates show that about 90 percent of all installed network cards is equipped with one of the Ethernet-ports, which clearly identifies Ethernet as the leading and most important standard worldwide (cf. Zenk 2003, p. 84).

6. A Glance at the Future

Actually this paper only covered a small part of what can be said concerning networks but the developments in the past 10 years make it nearly impossible to cover every single aspect of networks including the different cables, the different DSL-techniques, cable modems, Wireless MAN's, Internet via digital TV, ISDN, cellular phone network, private radio networks, or satellites. All of these technologies open new doors concerning the build-up of any kind of network in the future.

The speed of the industrial branch of networks makes it almost impossible to keep up with all the alternatives. Just to give an example: While back in 1999 only about 200,000 households had a DSL-connection to the internet this number is going to augment to 13.4 million in 2004 (cf. Hansen/Neumann 2001, p.1278).

One of the most important developments in the future of networks is going to be in the WLAN sector. As of today the boundaries of wireless networks lie within the premises of one company or household. Plans for projects in Berlin or San Francisco exist, depicting Internet access via WLAN for the whole city with a transfer rate of 11 Mbit/s.

The UMTS technology might be able to set new standards in the cellular phone market. Transfer rates of up to 2 Mbit/s in the just the smallest UMTS cell could prove to be the innovation in order to connect a whole people with each other (cf. id., pp. 1280-1283).

Just Ethernet in the development of LAN technologies is showing an immense growth rate. What started out as a standard for 10 Mbit/s LANs now evolved to a standard that makes transfer rates possible that exceed the initial invention by 1000 times, which is even faster than the development in the workstation market. Nevertheless even though the 10 Mbit/s is still standard for most LANs today, market tendencies show that the faster standards are implemented as well and their numbers are growing. Analysts predict that the Gigabit Ethernet will become the standard sooner or later even for home users (cf. id., p. 1288).

Tendencies show that the current standard of the Internet protocol (IPv4) will not suffice in the future regarding the increasing demands of new

Internet techniques. One of the major problems is the lack of available IP-addresses. Another weak point of the current standard is the inability to calculate the check sum of the incoming packages fast enough. Faster transfer on layer one and two of the OSI layer model make it almost impossible to calculate them fast enough, even though processor capacity augments at an incredibly fast rate as well.

Consequently the new Internet protocols (IPv6) have several enhancements:

- IP addresses will be extended from 32 to 128 Bits. This will ensure a total of 2^{128} IP-addresses, which corresponds to 10^{24} IP-addresses per sqm on earth.
- IPv6 can address not just one workstation, but a group of them
- It guarantees a certain quality of service
- Enhanced cryptographic protocols
- Simplified header, which ensures a faster transfer rate concerning broad band connections.

The version of the protocol can be extracted out of the header file once it reaches its destination (cf. id. 2001, pp. 1291-1292). Actually the migration to the new IPv6 standard has already begun and all products that have remotely to do with Internet protocols have already altered their production in the past years in order to be compatible once IPv6 is the unchallenged standard.

Considering that in the future not just every notebook or PC has an IP-address but every cellular phone, all PDA's, and probably even the future refrigerator that automatically orders new food once the stock gets too low, this was one of the absolutely necessary inventions in the network industry (cf. http://www.heise.de/tr/aktuell/meldung/43548, April 4th 2004).

Conclusively networks have become an integral part of our everyday life. Possibly even without us even noticing it. Studies without the vast possibilities of the internet seem sheer impossible. Synchronization of PDA's or cellular phones with Outlook has become just another daily procedure like the coffee in the morning once you start work. Networks are all around us and their significance and possibilities will most likely increase in the future.

This paper most likely did not cover every aspect of networks but it gave a brief overview of the idea behind it and what problems had to be solved and still have to be solved today in order to ensure successful communication between different devices.

Bibliography

Badach, A., Hoffman, E. (2001): Technik der IP-Netze, Wien 2001

Comer, D.E. (2002): Computernetzwerke und Internets, 3rd Edition München 2002

Frisch, W., Hölzel, H.-J., Lintermann, F.-J., Schaefer, U. (2001): Vernetzte IT – Systeme, Troisdorf 2001

Hansen, H.R., Neumann, G. (2001): Wirtschaftinformatik 1, 8th Edition., Wien 2001

Peterson, L., Davie, B. (2000): Computernetze – Ein modernes Lehrbuch, 2nd Edition, Heidelberg 2000

Stallings, W. (2001): Wireless Communication and Networks, New Jersey 2001

Tannenbaum, A.S. (1992): Computer-Netzwerke, 2nd Edition., Attenkirchen 1992

Zenk, A. (2003): Lokale Netze, 7th Edition, München 2003

Other sources

Towsley, D. (2001): Summary of MAC protocols, in: http://www.cs.umd.edu/~shankar/417-F01/Slides/chapter5b-aus/index.htm, March 6th 2004

Garfinkel, S. (2004): Garfinkel Kolumne: Internet, Version 6, in: http://www.heise.de/tr/aktuell/meldung/43548/0, April 4th 2004