



Training course for the Busch *ComfortTouch* network technology



Busch *ComfortTouch*

Network technology

Duration: 2 days (16 lessons)

Table of Contents

1.	Introduction	4
1.1	Applications in the home network	4
1.2	Structure of a home network	5
1.3	Components in the home network	6
1.4	Transmission media	9
1.5	The DSL router	10
1.6	DSL / ADSL (Appendix)	12
2	Ethernet and wiring	14
2.1	Ethernet / IEEE 802.3	14
	The Ethernet media access method CSMA/CD	16
2.1.1	The Ethernet data package	19
2.1.2	Ethernet developments	20
2.1.3	100 Mbit/s Ethernet (Fast Ethernet)	20
2.1.4	1000 Mbit/s Ethernet (Gigabit Ethernet)	21
2.1.5	10 Gigabit/s Ethernet (10Gbit Ethernet)	21
2.1.6	Overview of Ethernet standards	22
2.1.7	Ethernet in summary	23
2.2	Hub and switch	24
2.3	Wiring	27
2.3.1	Ranges and data transmission rates	29
2.3.2	Bandwidth demand for applications	29
2.3.3	Transmission media	32
2.3.3.1	Copper cables (twisted pair)	32
2.3.3.2	Wireless via radio network (Wi-Fi, wireless LAN)	32
2.3.3.3	Polymer Optical Fiber (POF)	32
2.3.3.4	Via the power grid (Powerline)	33
2.3.3.5	Telephone network (HomePNA) → www.homepna.org	34
2.3.3.6	Cable TV network (TV-Coax-LAN) → www.mocalliance.org	35
3	TCP/IP – Basics	36
3.1.1	The TCP protocol	38
3.1.2	The UDP protocol	38
4	DHCP (Dynamic Host Configuration Protocol)	74
4.1	Basics	74
4.2	Configuration	75
4.2.1	DHCP client	75
4.2.2	DHCP server	77
4.3	DHCP client/server communication	78
5	DNS (Domain Name System)	79
5.1	Introduction	79
5.2	How is the DNS structured?	80
5.3	The domain namespace	81
5.4	Domain name	82
5.5	The DNS server - Nameserver	83
5.6	The DNS client - Resolver	83
5.7	DNS name resolution - Forward Lookup	84
5.8	DNS address resolution - Reverse Lookup	86

5.9	History: the beginnings of name resolution – about the file hosts	87
5.10	Summary	87
6	TCP/IP configuration	88
6.1	General information (short compressed repetition)	88
6.2	Required settings	90
6.3	Configuration	91
6.3.1	Configuration with Windows	91
6.3.2	Configuration with Ubuntu-Linux	92
6.4	Identifying and displaying the current configuration	93
6.4.1	Displaying the current TCP/IP configuration under Windows	93
6.4.2	Displaying the current TCP/IP configuration under Ubuntu-Linux	94
6.5	Testing connectivity with Ping	95
7	Radio LAN (wireless LAN, Wi-Fi)	96
7.1	General information	96
7.1.1	Radio network according to the IEEE 802.11 standard	98
7.1.2	The operating mode: Ad-hoc mode	99
7.1.3	The operating mode: infrastructure mode	99
7.1.4	Network security in the radio network	100
7.1.4.2	Wi-Fi Protected Access (WPA) and TKIP encryption	101
7.1.4.3	Wi-Fi Protected Access 2 (WPA2) and AES encryption	101
7.1.4.4	The 802.1x standard	102
7.1.5	Extensible Authentication Protocol (EAP)	103
7.1.6	Wireless Distribution System (WDS)	104
7.2	Practical application	106
7.3	Wi-Fi setup	108
8	HTTP (Hypertext Transfer Protocol)	110
8.1	The World Wide Web (WWW)	110
8.2	HTTP addressing	111
8.3	HTTP client (web browser)	111
8.4	HTTP server (web server)	112
9	e-mail	113
9.1	e-mail basics	113
9.1.1	e-mail protocols	115
9.1.2	The e-mail account	116
9.1.3	e-mail services via "webmail"	116
10	LAN router	118
10.1	Performance characteristics	118
10.2	Router configuration	119
10.3	What can be configured?	120
11	Strategic error search in the TCP/IP network	122
12	Tools for diagnosis und error search	126
12.1	Displaying the current IP configuration – ipconfig / ifconfig	128
12.2	Testing connectivity – ping	129
12.3	Testing name resolution - nslookup	130
12.4	Route tracing – tracert / traceroute	130
12.5	Analyzing the network - Wireshark	131
12.6	Displaying routing tables netstat / route	132
13	Remote access from the internet to your home network (DynDNS)	133
13.1	Principle of remote access with DynDNS	134
13.2	Configuration for remote access - What must be done?	137

1. Introduction

Learning objectives:

- Recognizing the benefits and uses of a home network
- Knowing the structure and components of a home network
- Assessing the functional scope of a DSL router
- Indicating the transmission media used

1.1 Applications in your home network

Networking your own home is the current trend and is something that cannot be prevented or stopped. Terms like "home entertainment", "home office" and "home automation" are on everybody's lips these days.

Networking is required when, for example, every family member has his/her own computer and requires simultaneous access to the Internet, or everyone wants to use the family color laser printer. People often want to store data from different family members in one central location regardless if this involves conventional text documents, photos, audio or video files. This makes easy storage of your family data, the so-called **backup**, possible.

The following overview lists a few typical applications.

- **Resource sharing**
shared use of the devices and services
 - one internet connection for everyone
 - one color laser printer for the entire family (print service)
 - central data storage and data exchange (file service)
- **Audio / Video streaming**
 - Playing music and video over your network
- **Internet telephony (Voice over IP, VOIP)**
Telephoning via the internet
- **Internet radio (web radio)**
Listening to the radio via the internet
- **Monitoring camera**
Checking and remotely operating the camera via the internet (remote control)
- **Remote access**
Access from outside (on the go) from available resources
 - to private web servers in your home network
 - to a computer via a secure channel (Virtual Private Network, VPN)
 - to the monitoring camera
 - to the home control system (KNX)

Figure 1: Applications in the home network

A glimpse into the future.

Today, separate networks for data (IP network), voice (telephone network) and television (TV network) still exist for the private and the working environment. In the future, and with the appropriate bandwidth, everything will be combined and integrated into a single network, the IP network.

1.2 Structure of a home network

In order to have access to the desired services and functionalities in the home network, the corresponding technical requirements must be fulfilled. A network that is restricted to a single building is called a local network or a **Local Area Network (LAN)**. A home network is thus a typical LAN.

The simplest network consists of two computers that are connected to each other via a direct connection (**crossover cable**) or a coupling element (**switch**). This lets you access one computer from the other. Use this setup to, for example, directly exchange data between two computers.

However, more than two networked devices are usually available. Thus, a DSL router, for example, may be required to permit simultaneous access to the Internet. A network printer that is accessible to all family members and a central database in the network are also regarded as common components of a home network. For reasons of efficiency, several functions are combined in the DSL router. For example, the switch is integrated in the DSL router (more details later) Figure 2 illustrates the typical setup of a home network.

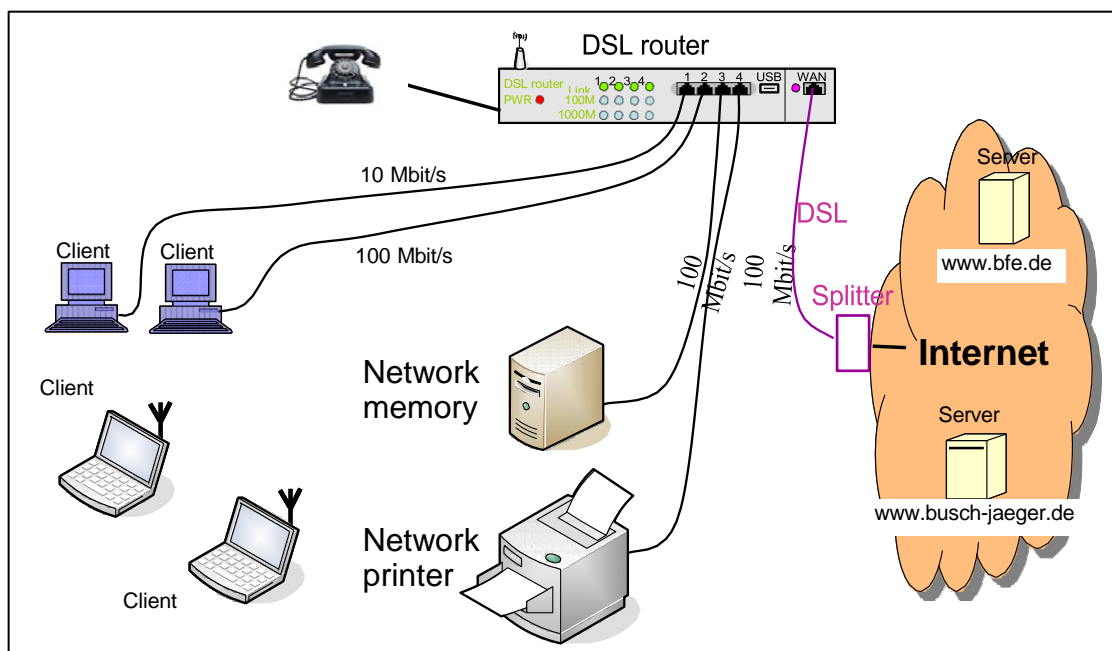


Figure 2: a home network setup

1.3 Components in the home network

The devices to be networked must have a corresponding network interface. This is also referred to as a **LAN** or **Ethernet interface**. The devices are connected to the central coupling element (**switch**) by a LAN cable. Currently, Ethernet interfaces are available for the transmission speeds 10 Mbit/s, 100 Mbit/s and 1000 Mbit/s, where 100 Mbit/s is the most common today. More details are discussed in Chapter 2, "Ethernet and cabling."

The network interface can also be implemented as a wireless solution (**wireless LAN**). Several things must be observed here too that are examined in a separate chapter later.

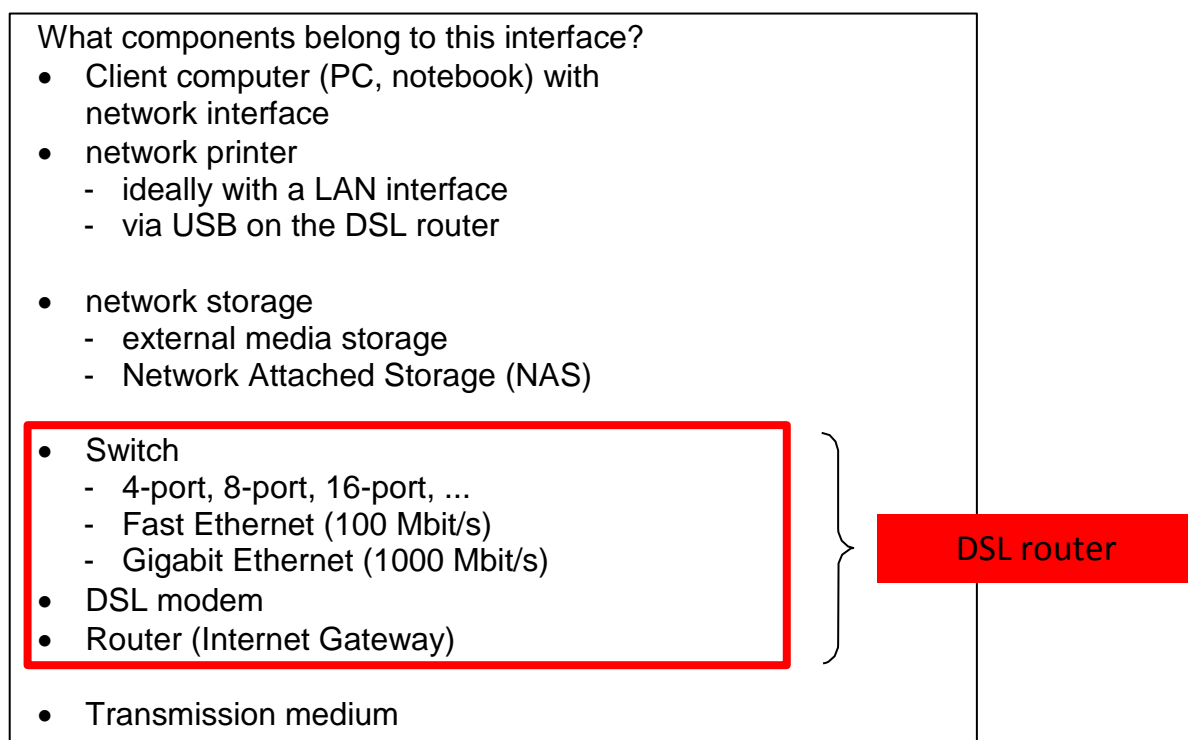


Figure 3: Components in the home network

The home network components are examined more closely in the following:

- **Computer (PC or notebook) with a network interface**
The computers require a LAN card. Cards with **100 Mbit/s (Fast Ethernet)** are standard today and cards with **1000 Mbit/s (Gigabyte Ethernet)** are increasingly available as well. Slower network partners automatically reduce the speed to 100 or 10 Mbit/s. Notebooks often have a network card installed (Wi-Fi adapter, network card with antenna) as well.
The computers are also frequently referred to as a **client** in the network because they also use the services of other devices (e.g. network printer, central data storage).

- **Network printer**

Network printers are central printers in the network that the user can access from his/her computer (client). The network printer is also called a **print server** since it offers its printing services to others, the so-called clients.

A network printer can be used in many different ways in the network. The network printer is most often configured using the browser via a web interface.

The following hard and software implementation methods for network printers are available:

- The printer has its own network interface (IP interface).
- The printer is connected via a USB or parallel interface to a so-called "printer box" that is connected to the network via a LAN interface.
- The printer is connected via USB to a modern DSL router like a Fritz!Box 7170 that has the additional print server function.
- The printer is directly connected to a PC and made available to other users in the network via a Windows share and the running Server service for example.

- **Network storage**

Network storage is used to centrally store data in the network. Each family member can then save his/her media in the form of Office documents, music folders, photos, videos, etc. You can also use network storage to exchange data within your family. The device that makes this kind of external data storage available is also known as a **file server**.

It is also most often configured by your browser via a web interface.

Network storage is possible hardware-wise as follows:

- using an external hard drive with a LAN interface
This is a separate device that you configure using your browser. You can set up areas on the hard drive that only certain users can access. This type of network storage is also called **Network Attached Storage (NAS)**.
- external hard drive with USB interface

The USB hard drive, like the USB printer, can be connected to the DSL router that must have the corresponding file server functionality.

- A special computer in the network provides hard drive memory to other network users. A Windows computer does this using a Windows share and the activated Server service.

- **Switch**

All of the network devices are connected to the switch and are thereby "connected." Specific operating modes and different application areas combined with product variety make switches a complex topic. This variety also justifies the large price differences. However, since no special requirements are imposed on a switch in the home network, it is enough to realize that the switch basically establishes the physical connection between the communicating devices. Switches differ, among other things, in the number of existing network connections, which are also referred to as **ports**. Thus, there are 4-port, 8-port or 16-port switches as well. If more ports are required than a single switch can provide, multiple switches can then be connected (**cascaded**). That's not a problem these days. A 4-port switch is already integrated in standard DSL routers.

- **DSL modem**

The DSL modem connects the home network to the public network (**internet**) via the telephone network. If the DSL modem is available as an external device, it then has two ports. It is connected to the **splitter** (telephone network) on one side and to the router (LAN) on the other side. The DSL modem is often already integrated in a **combination device**, which is usually referred to as a **DSL router**.

Nowadays, it is most often configured via the browser. The provider's identification data is essentially what must be entered here. DSL and its configuration are not part of this seminar. Additional background information on the subject "DSL/ADSL" is provided at the end of this chapter (1.6 DSL/ADSL).

- **Router**

The router is required in the network to forward those data packages that are not intended for a device in the home network to the public network (internet). The router permits simultaneous access to the internet for all the devices. The router may exist as a separate device, but in home networks it is usually integrated in the "DSL router" combination device.

1.4 Transmission media

Different transmission media are used depending on the circumstances and the requirements. An overview shall be provided first. Details will follow in the next chapter.

Overview – Transmission media in the home network

- Wired:
 - Twisted pair cable (Cat 5, Cat 5e, Cat 6)
 - Copper cable
- Wireless
 - Wireless LAN (Wi-Fi)
 - Radio
 - Bluetooth is also possible sometimes
- Synthetic fiberoptic cables
 - POF = Polymer Optical Fiber
 - Light (optical)
- Power line
 - piggybacked over the power grid

Figure 4: overview – transmission media for the home network

1.5 The DSL router

Nowadays, the DSL modem and the router are mostly integrated in a single device. These are then referred to as combination devices. The combination device most often also has a 4-port switch and maybe even a wireless base station (**access point**) The names for the combination device may differ. Names like "**DSL router**", "**Internet Wi-Fi Gateway**" or "**ADSL-Wi-Fi router**" are common. Only a closer look at the product description provides detailed information on the range of functions offered by the combination device.

The advantage of a combination unit is less required space and less power consumption compared to individual components.

However, the entire device must be replaced when one function fails.



Figure 5: T-Com Speedport W 701V



Figure 6: AVM Fritz!Box Fon 7170



DSL router often already contains ...
(combination device)

- DSL modem
- switch with multiple network connections (LAN ports), usually a 4-port switch
 - Fast Ethernet (100 Mbits/s)
 - Giga Ethernet (1000 Mbits/s)
- DHCP server
- radio base station (Wi-Fi access point)
- firewall
- port for internet telephony

Figure 7: DSL router features



DSL router extras are ...

- telephone system for internet and landlines
- port for analog and ISDN telephones
- USB interface for printer → Configuration as a network printer
- USB interface for an external USB hard drive → Configuration as network storage
- "Parental controls" using web filters and timetables
- Configuration options for remote access, including...
 - client for address services such as *dyndns.org*
The router subscribes to a directory service so that it can be accessed from the internet via an easily recognizable name, such as *livestation.dyndns.org*.
 - Configurable port forwarding
makes services like a separate web server or secure access via *ssh* possible from the outside

Figure 8: DSL router – features extras

At this point, reference should be made to DSL routers with a wireless LAN interface:
The Wi-Fi components should at least support the current **802.11g standard** and be capable of secure encryption (**WPA**, Wi-Fi Protected Access)

1.6 DSL / ADSL (Appendix)

DSL is the abbreviation for "Digital Subscriber Line" and refers to a method for digital data transmission over the copper lines of the existing telephone network. A far greater data speed is achieved compared to analog or ISDN modems. A telephone connection does not use the maximum bandwidth of the involved cables. Since the longer route of the connections to the local exchanges of the respective telephone company is mostly routed via coaxial or even fiber optic cables, it is quite possible to use the telephone/ISDN network using the piggyback method for additional digital data.

These methods are given the umbrella term **xDSL**, where the **x** stands for one of the different sub-methods.. With DSL, both data and telephone connections run simultaneously over the same line, separated by **filters** and **signal distributors (splitters)**. This requires a **DSL Modem** which processes the data for the telephone or ISDN network.

The most important DSL methods are **ADSL**, **SDSL**, **HDSL** and **VDSL**. **ADSL** (Asymmetric DSL) provides a higher data rate from the Internet to the connection than vice-versa. **SDSL** (Symmetric DSL), however, provides the same data rate when sending and receiving. ADSL and SDSL have relatively low demands on line quality and enable speeds up to about 1.5 Mbit per second. **HDSL** (High Data Rate DSL) provides 2 Mbit per second and **VDSL** (Very High Data Rate DSL) up to 50 Mbit per second and place the highest demands on line quality.

All DSL methods use the higher ranges of the frequency spectrum of a cable. As a result, the line length must not exceed a certain value so that the maximum transmission speed can be achieved. The DSL signal can be impaired by resonance effects, distortion and outside interference. The longer a line, the smaller the data rate.

DSL methods are used on the lines from the end user to the next exchange or distribution node. This requires a digital exchange and a maximum length of cable section between the end user and the exchange. That's why DSL can primarily be used in urban areas but not in rural areas.

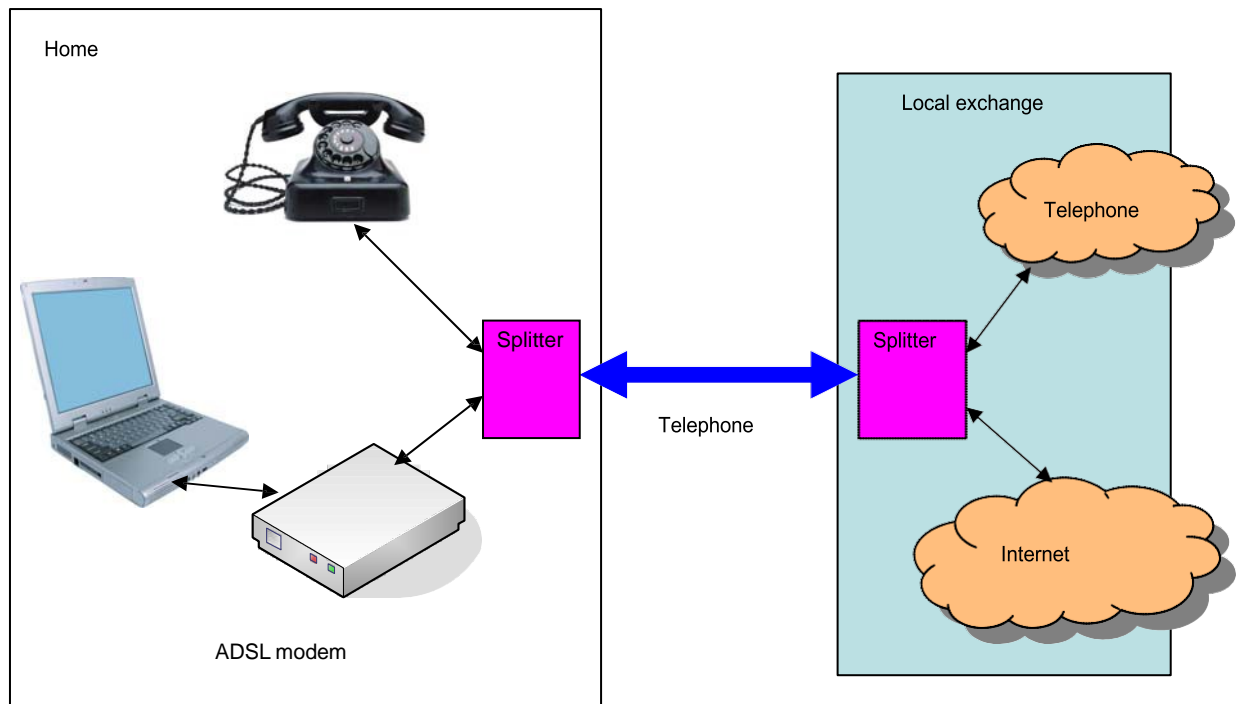


Figure: the principle of ADSL

2 Ethernet and wiring

Learning objectives:

- classify the terms Ethernet and IEEE 802.3
- understand the CSMA/CD Ethernet media access method
- know the common data transmission rates of the Ethernet versions
- understand why only lower transmission rates are often achieved in practice
- apply the term MAC address
- classify the terms Fast Ethernet and Gigabit Ethernet
- explain the tasks of a switch
- specify wiring for the Ethernet

2.1 Ethernet / IEEE 802.3

The beginnings of the local networks hark back to the 70s. The first developments were characterized by company-specific solutions. There were no standards. Different technologies were developed over time. The most common technologies include(d) **Ethernet**, **Token Ring**, **Arcnet** and **FDDI**, whereby the **Ethernet** has become the standard in the local network (**Local Area Network, LAN**). **Ethernet** is the most widely used technology for transmitting data in the network. Whether or not other technologies are more suitable for this purpose has not played a role. The "market" has made this decision simply based on price.

In the late 1970s, the **IEEE (Institute of Electrical and Electronics Engineers)** organization set up a working group to respond to the demand for standards for local networks. **Project 802** was founded to establish network standard on layers 1 and 2 of the OSI reference model (Note: the OSI reference model is an attempt to depict network communication in multiple layers - 7 to be precise). Project 802 included **Working group 802.3**, which developed standards for the Ethernet. Because the IEEE Project 802 mainly defines standards for Ethernet technology, the name **Ethernet** is synonymous with all the specifications suggested and standardized by the **Working Group 802.3**.

Figure 1 roughly shows the developmental stages of the Ethernet.

Ethernet developments

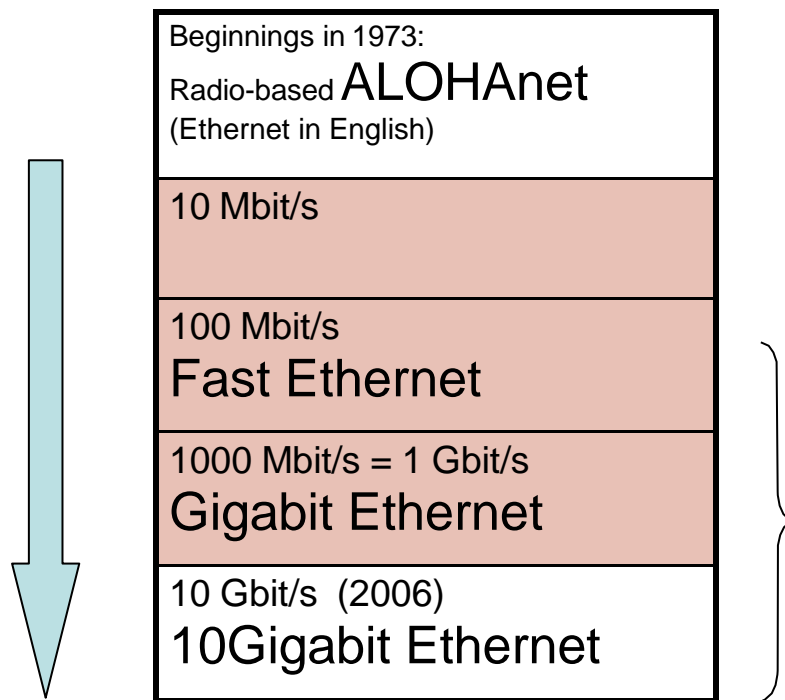


Figure 1: developmental stages of the Ethernet

It began in the 1980s with **10 MBit Ethernet** via coaxial cables, followed by **Fast Ethernet** with 100 Mbit/s, the **Gigabit Ethernet** with 1000 Mbit/s up to **10Gigabit Ethernet** with 10,000 Mbit/s = 10 Gbit/s. The transmission media was also subject to an ongoing adjustment. Initially, only coaxial cables were standardized. Today, twisted pair cables, i.e. twisted copper cables, different fiber optic cables and radio belong to the Ethernet standard as well.

What defines the Ethernet?

Ethernet includes **specifications for cable types and connectors, describes signaling for the bit transmission layer, encoding, transmission speed, and specifies packet formats and protocols**. From the OSI model's point of view, Ethernet specifies both the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). **Ethernet is largely standardized in the IEEE 802.3 standard.**

Practice: today cable types, plugs, etc. are defined by the **DIN standard EN50173-4 for structured cabling**.

The Ethernet media access method CSMA/CD

This section will briefly discuss the basic principle of **CSMA/CD** in order to better understand the difference between the terms **hub** and **switch** later on.

CSMA/CD stands for **Carrier Sense Multiple Access with Collision Detection**. This is the mechanism that Ethernet uses to regulate access to the shared transport medium.

It basically concerns the problem that multiple stations use a shared transmission medium, and that regulations must exist regarding who may use the transport medium when and for how long.

Different approaches are available to solve this problem, which used to be reflected in technologies like **Token Ring**, **Ethernet**, **FDDI**, etc. The following picture depicts these differing approaches.

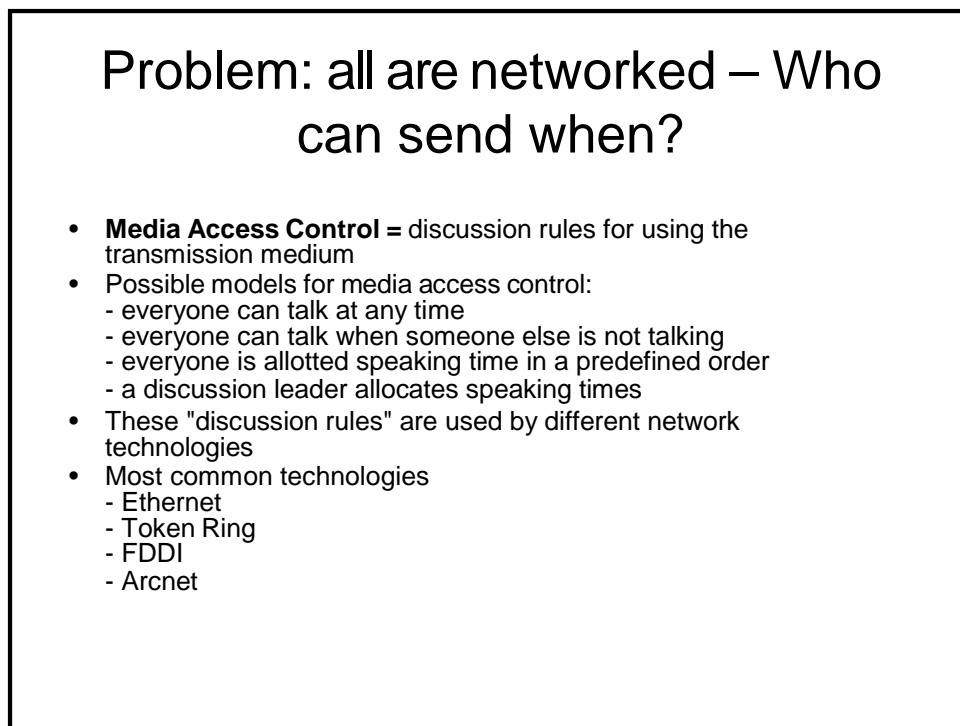


Figure 2: rules for media access.

This is how Ethernet works with CSMA/CD:

The access method to the transmission medium of Ethernet is **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**. As a multiple access network

(**multiple access**), several Ethernet stations can access the transmission medium independently of one another. All the stations permanently monitor the transmission medium (**Carrier Sense**) and can distinguish between a free and occupied line. Transmission is possible when a line is free. While data is being transmitted, the station checks whether another station has transmitted data at the same time and a data collision has occurred (**collision detection**). If no collision has occurred, the transmission was successfully completed. Packets lost by collision are initially repeated multiple times. If multiple collisions occur, packets must be requested again using higher-level protocols, such as **TCP** (term is defined in the next chapter). Network performance is impaired when collisions occur more frequently. Figure 3 explains the "Discussion rules" for CSMA/CD.

"Discussion rules" for Ethernet – CSMA/CD

Carrier Sense, Multiple Access with Collision Detection

- Conversation without a moderator.
- The following rules apply to this kind of a discussion:
 - Each participant can start talking when another person is not talking already (carrier sense)
 - If multiple participants start randomly talking at the same time in a conversation break (multiple access), they must immediately break off their contribution (collision detection).
 - Random delays (or gestures) then determine who may speak next.

Figure 3: "Discussion rules" with Ethernet – CSMA/CD

In an Ethernet network (strictly speaking with a **hub**, explanation later), only one station can thus send information at a single time. If two or more stations send at the same time, the packets collide. These packets are then lost. However, collisions occur frequently in an Ethernet. The more stations there are in the network, the more

collisions there are. This, of course, impairs the data transmission rate. Performance problems can only arise in the home network from an increased number of collisions when a **hub** and not a **switch** is used as the central coupling element. More detailed explanations follow in the "Hub and switches" section.

2.1.1 The Ethernet data packet

Ethernet is a packet-switching network. The data to be transmitted is divided into several small packets. These packets are called **frames**. A frame not only packs the data but also the destination address, the source address and additional control information. The **MAC addresses** are used as addresses. This is the unique address configured by the manufacturer on the hardware side in the network card. This address should not be changed as a rule.

The maximal length/size of an Ethernet package is 1526 bytes. This includes 1500 bytes of data. The minimum length is 72 bytes, with 46 bytes of data. If the amount of data to be transmitted is larger than 1500 bytes, then the data is split up and transmitted in 1500 byte blocks. The following picture shows the structure of an Ethernet packet.

Structure of an Ethernet frame as per IEEE 802.3

Preamble	Destination address	Source address	Type field	Data field	Check field
8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

Preamble	Used to synchronize the recipient and displays the start of the Ethernet packet
Destination address	Address of the recipient (MAC address)
Source address	Sender address (MAC address)
Type field	Displays the protocol type (e.g. TCP/IP, IPX/SPX, NetBEUI). This field is also referred to as a length field.
Data field	The data to be transmitted is located here
Check field	Checksum to detect transmission errors

Figure 4: structure of an Ethernet packet

After a packet has been sent, a "send pause" of 9.6 μ s occurs due to technical reasons. This pause is also referred to as an **interframe gap**. The technical details are not explained further here.

2.1.2 Ethernet developments

The original Ethernet used a coaxial cable as the transmission medium. Each station was thereby connected to several other stations via a cable. The network was then set up as a so-called bus. The cable section was terminated at each cable end with a resistor to avoid signal reflections. The bus structure is called a **bus topology**. However, the bus topology has many disadvantages. For example, the network collapses when only one cable connection is disconnected or when one terminating resistor is missing. Because of the disadvantages of networks with the bus topology and the coaxial cable, Ethernet was extended by Category 3 and 5 twisted pair cables. These are 8-core cables whose cores are twisted in pairs. Cable routing is configured as a **star topology** with **switches** or **hubs** as distribution stations.

However, twisted pair cables only have a range of 100 meters, which makes them unsuitable for networking buildings or connecting network structures (**backbone**). That's why Ethernet was also standardized for fiber optic cables. Coaxial cable no longer plays a role today. Category 5, 5e or better 6 (**CAT 5, CAT 5e or CAT 6 cables**) twisted pair cables are generally used for new installations. CATs are cable standards according to the "structured cabling" system, which are standardized by **DIN EN 50173-4**.

Fiber optic cables are used to bridge longer distances.

The **Ethernet standards** for the 10 Mbit/s Ethernet for twisted pair cables is **10Base-T**. It is **10Base-5** and **10Base-2** for coaxial cables.

2.1.3 100 Mbit/s Ethernet (Fast Ethernet)

Fast Ethernet is the further development of the Ethernet standard with **100 Mbit/s** using twisted pair cables. Other coding methods were used to increase the transmission rate from 10 Mbit/s to 100 Mbit/s. The range remained confined to 100 meters only. **100Base-T** is the general term for the three 100 Mbit/s Ethernet standards using twisted pair cables: **100Base-TX**, **100Base-T4** and **100Base-T2**, whereby only 100Base-TX is used in Europe.

2.1.4 1000 Mbit/s Ethernet (Gigabit Ethernet)

A high network load caused by many applications (e.g. internet, multimedia, electronic document exchange) makes it necessary to connect central Ethernet stations, such as servers and switches, with more bandwidth than the other stations. **Gigabit Ethernet** was developed based on the original standard. First, for **fiber optic cables**, and later for **Category 5 twisted pair cables** as well. Both versions permit data to be transmitted at **1000 Mbit/s**. Due to the lower fault susceptibility of fiber-optic connections, the fiber optic cable medium knows no upper limits when it comes to fast transmissions. With twisted pair cables, several tricks must be used to achieve this higher speed. **Gigabit Ethernet** always utilizes all 4 wire pairs via twisted pair cables. The data stream is encoded with **PAM5x5** (Pulse Amplitude Modulation with 5 different rules). A new error correction is also used. This technology is beneficial for existing structured copper cabling (twisted pair). This can be used, assuming that the cables are specified for it. The standard for twisted pair cables is **1000Base-T**.

2.1.5 10 Gigabit/s Ethernet (10GBit Ethernet)

10 Gigabit Ethernet has only been standardized since 2006. It is standardized both for fiber-optic and copper cables (twisted pair). To keep the standard flexible, it supports 7 different fiber optic cable types. 10 Gigabit Ethernet can be used regardless of the fiber optic cables used.

For the first time, the CSMA/CD access method was no longer used for Ethernet. It is operated solely in full duplex mode. In full duplex mode, both stations can send and receive simultaneously. The packets of the two stations are then transmitted time-delayed according to a predefined scheme. Half-duplex refers to a method where only one station can always send packets and the other station receives packets. This method is used for CSMA/CD.

The standard for copper cables is **10GBase-T**.

2.1.6 Overview of Ethernet standards

Overview of Ethernet standards

IEEE standard	Designation	Year	Data rate	Cables
802.3	10Base-5	1983	10 Mbit/s	Coaxial cable (yellow cable), 500 m
802.3a	10Base-2	1988	10 Mbit/s	Coaxial cable (BNC), 185 m
802.3i	10Base-T	1990	10 Mbit/s	Twisted pair cable (RJ-45), 100 m
802.3j	10Base-FL	1992	10 Mbit/s	Fiber optic cable
802.3u	100Base-TX	1995	100 Mbit/s	Twisted pair cable (RJ-45), 100 m
802.3u	100Base-FX	1995	100 Mbit/s	Fiber optic cable
802.3z	1000Base-SX 1000Base-LX	1998	1 Gbit/s	Fiber optic cable
802.3ab	1000Base-T	1999	1 Gbit/s	Twisted pair cable (RJ-45), 100 m
802.3ae	10GBase-SR 10GBase-SW 10GBase-LR 10GBase-LW 10GBase-ER 10GBase-EW 10GBase-LX4	2002	10 Gbit/s	Fiber optic cable
802.3an	10GBase-T	2006	10 Gbit/s	Twisted pair cable (RJ-45), 100 m

Figure 5: overview of Ethernet standards

Note:

The specified data transmission rates, also referred to as the **gross data rate**, are not achieved in practice. The protocol overhead and the collisions in the network restrict the data transmission rate, resulting in a lower **net data rate**.

2.1.7 Ethernet summary

Ethernet dominates the LAN sector. Ethernet became the most widely used LAN technology from the 1990s and has made all other LAN standards such as **Token Ring**, **ARCNET** or **FDDI** into niche products for special applications.

Ethernet was originally developed for a bus topology with coaxial cables. This technology, **10Base-5** or **10Base2**, reached a maximal transmission rate of 10 Mbit/s. The most common technologies used today for twisted pair cables **10Base-T** (10 Mbit/s), **100Base-T (Fast Ethernet)**, 100 Mbit/s) and **1000Base-T (Gigabit Ethernet)**, 1000 Mbit/s) work with a star topology.

A **switch** is used as the distributor.

Ethernet in its current form is defined in the **IEEE 802.3 standard**.

Wiring is with twisted pair cables. These Ethernet versions are currently available for the home network:

- **10Base-T**, with a data transmission rate of 10 Mbit/s, cables: at least **CAT 3**
- **100Base-T (Fast Ethernet)**, with a data transmission rate of 100 Mbit/s, cables: at least **CAT 5**
- **1000Base-T (Gigabit Ethernet)**, with a data transmission rate of 1000 Mbit/s = 1 Gbit/s, cables: at least **CAT 5e**
- **PoF**, cheap compared to fiber optic cables, thin (easier to route), 100 Mbit/s

The data transmission rates are, however, not achieved in practice. The data transmission rate is restricted by the protocol overhead and the collisions in the network (caused by CSMA/CD)

The speed is automatically adjusted when several devices with different data transmission speeds are connected to each other.

The device is connected to the network by a network card, also called a **LAN adapter**. The **MAC address (Medium Access Control)**, also called the hardware address or Ethernet address, is used to identify the network card. A station can also have several network cards, where every card has its own MAC address. Example: notebook with integrated LAN and Wi-Fi cards.

The MAC address ...

- is (ideally) unique in the world
- consists of 6 bytes, where the first 3 bytes represent the manufacturer ID and the last 3 bytes the card ID. The MAC address is firmly wired on the card.
- The MAC address is in the data package (frame) so that the correct recipient receives the data. The recipient only accepts the data when it is directed to his/her MAC address.

2.2 Hub and switch

In the beginnings of Ethernet cabling with twisted pair, i.e. in the 10 Mbit/s Ethernet, **hubs** were used as distributors. The hub usually only operates at **one** fixed transmission speed and otherwise only improves the electrical signal on the line. Compared to today's **switches**, it has no "intelligence." That's why a hub is retrospectively called a "**dumb switch**" today. Just like switches, hubs have several port connections. If these are not enough, either a special uplink port or a **crossover cable** can be used to connect additional hubs. Several hubs can be connected, i.e. cascaded, this way.

Since all networked devices share the transmission medium (**shared medium**) in the classical Ethernet, performance is good as long as the traffic volume is small in the network. If several stations want to transmit at the same time, the probability of a collision increases dramatically and sensible work is no longer possible.

The **Switched Ethernet** was developed in order to solve this problem and maximize the available bandwidth. In the **Switched Ethernet**, **hubs** are replaced by **switching hubs (switches)** that break up the collision domain into several, smaller collision domains (mostly one between two communication partners), which reduces the number of collisions or prevents these entirely. Communication in full-duplex mode is also possible when switches are used, i.e. data can be sent and received simultaneously.

The switch records the **MAC addresses** of the connected stations and analyzes the network traffic. Compared to the hub, which forwards the packet to all other network subscribers, it only forwards data to the port that the recipient is connected to. Thus, a sort of point-to-point-connection between the sender and recipient is established via the switch and no collisions can occur in this connection anymore. The switch also has other features that need not be addressed here.

The function of the **switch** and **hub** can be described in technical terms as follows: A **hub** only operates on the OSI layer 1. Pure bit transmission with signal enhancement takes place here. The data is sent to all the stations in the network that are connected to the hub. Although the cabling is star-shaped, it retains its bus structure for signal propagation.

A **switch** operates on the first and second OSI layer. Bit transmission and signal enhancement also takes place, of course. But the switch sends the data only to the MAC address the data is intended for. However, the MAC address is an integral part of the second layer. The switch establishes a point-to-point connection between 2 devices. It should be mentioned at this point that some switches operate on OSI layer 3, but these will not be discussed here.

Only a basic understanding of the function and operation of the switch is relevant to us, also in contrast to the hub.

Conclusion: today, due to its restricted performance characteristics, the **hub** has been displaced by the **switch** and should no longer be used in a network because of performance reasons.

Cascading switches

Common DSL routers have an integrated **switch** with a maximum of 4 LAN connections, also called **ports**. An additional switch with 8 or 12 additional LAN ports can be used whenever more than 4 devices must be connected. The switches are **cascaded**. As with **hubs**, cascading is done either with a **crossover cable** or a special connection. The picture shows how a **switch** is cascaded with a switch that is integrated in the DSL router. This makes a total of 10 ports available.

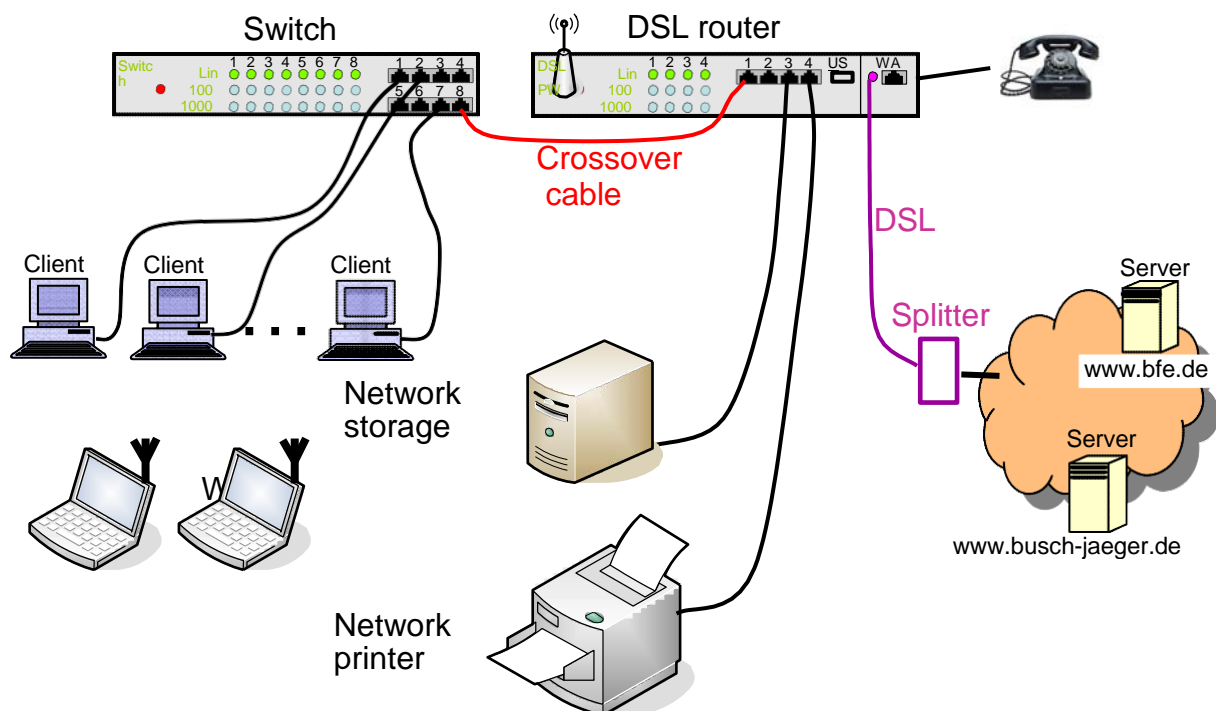


Figure 6: cascading switches

The following error situation may thereby occur with older switches:
Standard cables are made 1 to 1, i.e. Pin 1 at one end corresponds to Pin 1 at the opposite end. In order for the network card sender not to work on the DSL router or switch sender, the latter two internally swap their sender wire pairs with recipient wire pairs.

Data transmission between the switch and PC then works perfectly. Not between the switch and switch since both sides swap the sender wire pairs with the recipient wire pairs. If at least one of the switches does not recognize this and can fix this automatically, then either a **crossover cable** must be used for the connection or a special **uplink connection** must be used on one of the switches or a corresponding pushbutton actuated for the RJ45 connection (**MDIX**) that is used.

Tip:

The illuminated LINK LED on the network cards and the switch/DSL router indicates that the electrical connection is established. This should always be checked first before you search for the error in the IP addresses. On most devices, a flashing Link LED signals data traffic.

2.3 Wiring

The home network uses different media to transmit data. The medium to be selected and the respective wiring technology depend on many factors. The decisive factors are, among other things, the local conditions (existing infrastructure) and the desired applications.

Which transmission media are used in the home network?

- **Wired:** copper cable → twisted pair
For **Fast Ethernet** (100 Mbit/s), at least CAT 5 cables are required and for **Gigabit Ethernet** (1000 Mbit/s) at least CAT5e or CAT6 cables are required. The connection between the terminal and switch is established using a so-called **patch cable**.
- **Wireless** by radio (**Wi-Fi** = wireless LAN, radio network)
The greatest developments are happening here in terms of security and speed.
Currently, the standard is **WLAN 802.11g**. The future is **WLAN 802.11n**.
à refer to the "Wi-Fi" chapter for more information
- **Optically:** plastic optical fiber (**POF** = Polymer Optical Fiber)
This technology is still quite young. For a point-to-point connection and subsequent distribution via a **switch**
- **Over the power grid** (230V grid): -Powerline
Ideally used to couple a remote room, where the network can then be distributed further with a **switch**.

rarer

- telephone network
- cable TV

The most common and desired is certainly a wired networking solution with twisted pair cables. Wireless solutions complement this solution when, for example, you're web surfing with your notebook in the living room. Nowadays, different media are increasingly being used simultaneously in the home network.

Which parameters should you take into account when selecting a transmission medium?

- **Application and bandwidth**
When planning your home network, it is crucial to know which applications should be used in your network, from which the required bandwidth can then

be derived. Applications and their required data rates are listed in tables in Section 2.3.2.

- **Distance**

Another important aspect is the distances to be bridged, combined with the question of whether all the rooms are already networked with cables or can be reached that way. Section 2.3.1 compares the ranges and transmission speeds for the individual media.

- **Spatial conditions**

Three alternatives are available for networking in areas where routing the somewhat bulky twisted pair cables is a complicated matter:

- data communication via radio, wireless LAN (Wi-Fi)
- data communication via the power grid, Powerline
- data communication via light across thinner plastic fiber optic cables, **polymer optical fiber (POF)**

2.3.1 Ranges and data transmission rates

Technology	Range	Gross data rate	Net rate
Fast Ethernet	100 m	100 Mbit/s	94 Mbit/s
Gigabit Ethernet	100 m	1000 Mbit/s	940 Mbit/s
POF	30-50 m	100 Mbit/s	94 Mbit/s
WLAN 802.11g	10-300 m ¹	54 Mbit/s ²	5-25 Mbit/s ¹
WLAN 802.11n ³	10-300 m ¹	300 Mbit/s	5-120 Mbit/s ¹
Powerline ⁴	10-200 m ¹	200 Mbit/s	15-85 Mbit/s ¹

¹ heavily dependent on the surroundings (buildings or power grid)

² more than 54 Mbit/s with proprietary technologies

³ currently being designed, standard expected summer 2008

⁴ three competing, incompatible standards

Figure 7: range and data transmission speed

2.3.2 Bandwidth demand for applications

Application	Data rate	Characteristic
Chatting	< 1 kBit/s	in batches
Telephony	16 to 80 kBit/s	continuous
Internet radio / MP3 playback	32 to 320 kBit/s	continuous
uncompressed audio	1500 kBit/s	continuous
web surfing, e-mail	1000 to 6000 kBit/s	in batches
DivX/XviD video	4000 to 8000 kBit/s	continuous
DVD video	up to 10000 kBit/s	continuous
HD video	up to 20000 kBit/s	continuous
Copying data, backups	100000 to 500000 kBit/s	in batches

Figure 8: bandwidth demand

The sensible use of different transmission media will be demonstrated through an example. The following picture thus shows the floor plan of an apartment with the cabling technology used.

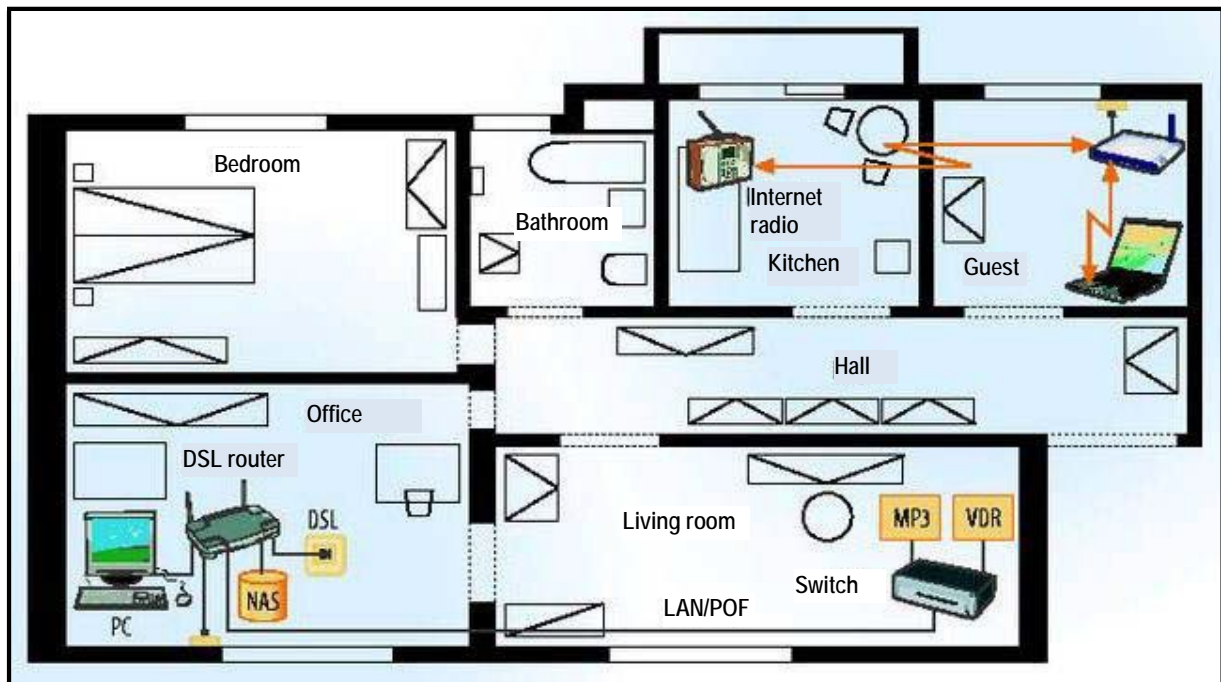


Figure 9: cabling technology in the modern home network (source c't 2007 Issue 12)

Office:

- the only room with "classic" networking via copper cable, i.e. twisted pair
- the location for the DSL router with switch. the switch is ideally Gigabit Ethernet compatible
- Fast connection (at least 100 MBit/s, better 1000 MBit/s) to the **NAS** network storage, which also acts as external media storage.
- Optional: the family color laser printer is also located here (not pictured)
- From here, the living room is connected as a point-to-point connection via POF or twisted pair with at least 100 Mbit/s
- Connecting the guest room and kitchen to the home network via Powerline

Living room:

- directly adjacent to the office
- additional devices can be integrated via a point-to-point connection and its own switch
- media center for video (requires high bandwidth)
- media center for audio

Guest room:

- no direct Wi-Fi access is possible
- convenient connection to the home network is possible via Powerline and access point in the guest room
- The mobile workplace is integrated via radio and suffices as a classical workplace due to its low bandwidth requirements. surfing and texting are not a problem

Kitchen

- web radio can be connected over Wi-Fi, not a bandwidth problem

Conclusion: the ideal home network is created by cleverly combining different technologies, for example, by using Wi-Fi only for mobile devices or stations with a low data rate, such as Internet radios. Point-to-point-connections should be used with a LAN cable or POF whenever a high bandwidth is required (i.e. for video streaming). Because the switch automatically detects the transmission speed, whether 10, 100 or even 1000 Mbit/s, devices with different network interfaces can easily be used in the home network. Thus, a somewhat older computer with a 10 Mbit/s network interface and a modern system with a 100/1000 Mbit/s LAN adapter can be used together, for example.

Wiring the required devices does not represent a major hurdle. It is important to clarify which data transmission rate should be used to transmit the data. This results mainly from the requirements of the PC users themselves. **100 Mbit/s suffice for normal operation. Gigabit Ethernet** should only be considered when large CAD drawings or image files are often transported over the LAN network, for example. The bottleneck lies in the Internet connection. The 100 Mbit/s already common in today's LAN will only be standard here in a few years.

2.3.3 Transmission media

2.3.3.1 Copper cable (twisted pair)

- For **Fast Ethernet** (100 Mbit/s) → at least **Cat 5 cable** (Class D). This cable is standard today.
As with 10Base-T, the maximum length between switch and terminal device is 100 meters. The plug connectors are designed as 8P8C modular plugs and sockets and are often referred to as "RJ-45" or "RJ45."
- for **Gigabyte Ethernet** (1000 Mbit/s) → at least **Cat 6 cable** (Class E)

2.3.3.2 Wireless via radio network (Wi-Fi, wireless LAN)

- There are standards here that are being constantly developed.
- The radio network belongs to the "shared medium." You can connect more than two devices with Wi-Fi. However, the end devices networked with Wi-Fi must share the transmission media of air in order to exchange data.

→ more information is available later in the "Wi-Fi" chapter

2.3.3.3 Polymer Optical Fiber (POF)

An interesting optical medium – the plastic fiber optic cable – has established itself for the home network area since the start of 2007. Other descriptions include **Plastic Optical Fiber** or **Polymer Optical Fiber (POF)**. The material is cheaper than plastic fiber optic cables. At Fast Ethernet speeds, data can be transmitted via a point-to-point-connection. An adapter is thereby used to convert the electrical Fast Ethernet signal into an optical signal. Unfortunately, there are still no common standards available so that the user is bound to a manufacturer.

The T-Com Speedport OptoLAN Starter set is depicted as an example on the next page. This includes a 30 m POF cable and 2 adapters, called **transceivers**. One end of the POF cable is connected to the respective fiber optic transceiver, whose other end is connected to the Ethernet cable and the power supply.

A cutting tool is enclosed to cut the plastic fiber optic cable. The fibers are mounted using a patented clamping mechanism from Ratioplast Optoelectronic.



Figure 10: T-Com Speedport OptoLAN starter set

2.3.3.4 Over the power supply (Powerline)

Stationary devices can be networked over the power line using **Powerline Communications (PLC)**. Adapters, configured as power supply units, transmit the Ethernet data with a shortwave signal over domestic power lines. This allows transmission rates of up to 200 Mbit/s gross (80 Mbit/s net). The adapter is equipped with one RJ45 LAN and one connection to the power supply respectively. One adapter is placed in one free outlet on the router, the other is placed on the device to be networked. The latter can also be a cheap switch that you can then route several LAN devices to. This way you can avoid purchasing additional expensive Powerline adapters. The following figure depicts a Powerline adapter pair.



Figure 11: Powerline Ethernet Bridge

Powerline, too, is also a shared medium, which means that the transfer medium must be shared for any data exchange with PLC-networked end devices.

That's why Powerline should only be used to connect remote rooms via a point-to-point connection.

The following slide looks at some aspects of Powerline technology.

Powerline

- Ethernet via the power supply
- Three different product families (manufacturer)
 - Home Plug AV, UPA, HD-PLC
 - incompatible with each other
 - may not be used together
- adapters should always be used in pairs
- Transmission speeds
 - 200 Mbit/s (gross) → net up to 80 Mbit/s
 - older types 14 to 85 Mbit/s
- Secure encryption
- Price per adapter pair set: €70 to 200
- Disadvantages: no standards, mixing of technologies (different manufacturers, older with new types) is taboo in the same power grid, very manufacturer-dependent

Figure 12: Powerline (PLC) aspects

Note and tip:

those who want to invest in Powerline adapters today must choose a family and then buy any replacement products sorted by model

2.3.3.5 Telephone network (HomePNA) → www.homepna.org

- Has a niche status in this country.
- Requires telephone cabling in each room.
- Example application: to supply guests in hotels
- Output speed max. 320 Mbit/s gross (for 3.1 specification from 12/2006)

2.3.3.6 Cable TV network (TV-Coax-LAN) → www.mocalliance.org

- Has a niche status in this country
- Requires cable TV cabling in every room
- Example application: to supply guests in hotels
- All stations hanging on one line share the throughput (as with Powerline and WLAN)
- Output speed up to 200 Mbit/s

3 TCP/IP – Basics

Learning objectives:

- identify the tasks and function of the TCP/IP protocol
- become familiar with structure of IP addresses
- divide networks into subnetworks
- effect of the subnet mask
- specify the network classes
- understand the routing principle
- understand the concept standard gateway or default gateway
- Meaning/Application of ARP and ICMP
- understand the tasks of TCP and UDP
- able to allocate the port concept as the number that is used to identify a network application

Motivation

Networked devices like PCs, notebooks, server computers, network printers, etc. must speak the same language in order to be able to "speak" to each another. The worldwide "standard language" in the network is **TCP/IP**. The abbreviation stands for **Transmission Control Protocol / Internet Protocol**. This "language" is always been spoken in the **World Wide Web (WWW)** and has completely pushed other "languages" like **IPX/SPX**, **NetBEUI** or **AppleTalk** out of the market.

The advent of the Internet has given **TCP/IP** unprecedented success. It is therefore the network standard around the world in the **LAN (Local Area Network)** and in the **WAN (Wide Area Network)**. The dominance of **TCP/IP** can also be seen by the fact that all network services, be they data, speech, or video/TV, will be transmitted over a TCP/IP network in the future.

In order for a network station to be able to speak the "TCP/IP language," the network card of the corresponding device must be configured for the **TCP/IP protocol**. Basic knowledge about **TCP/IP** is absolutely essential for any successful configuration and, above all, for troubleshooting and will be provided in this chapter.

By the end of the chapter, terms like **IP address**, **subnet mask**, **standard gateway** or **DNS server** should no longer be foreign to you. These parameters need to be successfully configured before the device can participate in network communication.

3.1 Definition and advantages of TCP/IP

History

The origin of TCP/IP, and therefore the Internet, is in the military. During the "Cold War" – in the 1960s – a research group (RAN Corp.) was commissioned by the American government to design a network that could survive a nuclear attack. According to a simple principle, messages should be sent in individually divided and separately addressed packets so that each packet can find its own way in the network. Even if a large part of the network were destroyed, communication would still be ensured. After the introduction of the first test network in 1968, the Advanced Research Project Agency (ARPA) was established as a department of the US Department of Defense to implement the subsequent "real" networking. Under the name ARPANET, more and more computers were networked in the 1970s. The ARPANET protocol, that was called Network Control Protocol (NCP), developed into the TCP/IP and was first introduced to the public in 1978. After the TCP/IP protocol became standardized at the beginning of the 1980s by ISA (International Standards Organization), the actual triumph of the Internet as we know it today began with the integration in our daily work and private life.

TCP/IP - Overview

- TCP/IP are several protocols
- Basis: IP protocol
- Building on this: TCP or UDP
- Most applications use the TCP protocol
- UDP protocol e.g. for audio/video streaming

Figure 1: TCP/IP – Overview

TCP/IP are several protocols

TCP/IP is a **group of protocols or rules (protocol family)** that was introduced in 1984 so that computers can communicate with one another in the network. Although it is common to say "TCP/IP" in one breath, TCP and IP are two different protocols: **TCP** (Transmission Control Protocol) and **IP** (Internet Protocol). More precisely, a third protocol, equal to TCP, should be added: **UDP** (User Datagram Protocol)

Basis: IP protocol

The IP protocol ensures that data packets are sent from one subscriber to another and finds the corresponding ways (**routes**) to transport these data packets with the best possible routes.

Building on this: TCP or UDP

3.1.1 The TCP protocol

The **TCP protocol** builds on the **IP protocol** and is used for many well-known applications like **e-mail** or website browsing. Most network applications use the **TCP protocol**. The **TCP protocol** establishes a fixed and secure connection and expects that all data packets are sent in the correct order and are put together again by the recipient (**network-oriented protocol**).

The **Internet Protocol (IP)** is responsible for **addressing** and for **forwarding or delivering** packages, called **routing**. **IP**, however, does not guarantee that the packets are delivered correctly. **Transmission Control Protocol (TCP)** is responsible for this in the higher layer. **IP** itself takes care of every single packet. If, for example, a data block is to be sent in the network, it is then subdivided into individual data packets by the sender and every packet is "sent on its way." The individual data packets can thus reach their destination over different routes. It can readily occur that the packets from one data block are **routed** differently and arrive in another order at the recipient. On the recipient side, **TCP** monitors whether all the data packets arrive and assembles the subpackets in the correct order to create the overall data block. The data block is then forwarded to the application.

However, **TCP/IP** is anything but an efficient method for transmitting data. With a load capacity of only a few bytes per data packet, this results in a very large administrative component of at least 40 bytes per data packet. Only when you send large data packets of one KByte or more can you reduce the percentage of administrative information.

3.1.2 The UDP protocol

Some applications like streaming audio and video use the UDP protocol and can tolerate the occasional loss of data packets. There is no secure connection for the UDP protocol, so the successful delivery of the data packets is not controlled (**connectionless protocol**). Compared to the TCP protocol, the UDP protocol has the advantage of being much thinner and faster. Moreover, it is counterproductive to repeat a lost packet after 1s, for example, in applications such as voice and video transmissions.

TCP/IP – IP addressing

- Each participant requires a logical address (IP address)
- The IP address must be unique
- Special address areas are defined for "private networks" (non-public, Intranets).
- Applications share a single IP address

Figure 2: TCP/IP – IP addressing

In an IP network, each subscriber needs a unique logical address. This IP address consists of four bytes, each separated a period. Each byte is depicted as a decimal number. One possible IP address is, for example, 192.168.1.80.

The IP address must be unique within the IP network. An IP address for the Internet must therefore be unique worldwide, whereas an IP address for an intranet must only be unique within this network.

Address spaces for intranets were defined (RFC 1597) in order to keep the possibility open of connecting intranets to the Internet. The most common address range is 192.168.0.0 to 192.168.255.255.

Different network applications, such as the e-mail program and browser, are running simultaneously on a single computer. Because the computer has only one IP address, it must be possible to distinguish data packets for each individual network application. An additional number is therefore attached to the IP address – the so-called **port**. Each executed network application receives a unique **port** assignment and can receive or send the data packets responsible for it.

The main advantages of TCP/IP are:

Advantages of TCP/IP

- no manufacturer dependency
- can be implemented on all kinds of devices
- can be used in LAN and WAN
- makes network applications independent of the transmission system
- Suitable for every transmission system

Figure 3: advantages of TCP/IP

- **TCP/IP** is not manufacturer dependent
- **TCP/IP** can be implemented on all kinds of devices (PCs, network printers, panels, etc.)
- **TCP/IP** can be used in **LANs** and **WANs**
- **TCP/IP** makes the network application independent of the transmission system
- **TCP/IP** can transmit data over every transmission system (**Ethernet**, Token Ring, etc.) regardless of where the communication partners are located. **IP** ensures that the data packet reaches its destination and **TCP** controls the data transmission and provides the data stream to the application.

3.2 TCP/IP in the layer model

TCP/IP is a protocol combination that successfully connects the transport and switching layers from the OSI layer model. The **Internet Protocol (IP)** is arranged on the 3rd layer – the switching layer of the OSI layer model. The **Transmission Control Protocol (TCP)** is arranged on the 4th layer – the transport layer of the OSI layer model.

Tasks and function of **TCP/IP** can also be described with a simplified layer model that consists of 4 layers. This model is older than the 7-layer OSI layer model, but completely suffices for our purposes. The following uses the simpler model.

The following figure shows the 4 layers with the associated protocols as well as the allocation of the 4 layers to the OSI layer model. The lowest layer is made up of the **network access/network card layer**, simply also known as the **hardware layer**. The **Internet layer** with the **Internet Protocol (IP)** is above that. Above that is the **transport layer** with the **Transmission Control Protocol (TCP)**. The highest layer is called the **application layer**.

Protocol	Layer	Description
HTTP, FTP, NTP, SSH, ...	4 (OSI 5,6,7)	Application layer
TCP UDP	3 (OSI 4)	Transport layer
ICMP IP ARP	2 (OSI 3)	Internet layer
Ethernet (IEEE 802.3), Token Ring, FDDI, PPP, ...	1 (OSI 1,2)	Network access / Network card layer
		Hardware layer

Figure 4: TCP/IP protocol family in the 4-layer model (incomplete)

Even if this picture, together with the many new concepts, appears confusing at first to a network newcomer, it makes sense to understand network technology in a layered way of thinking in order to better understand the correlations. Only then can **systematic troubleshooting** be conducted in the network later.

The network access/ network card layer

We have already gotten to know an implementation for the lowest layer with **Ethernet (IEEE 802.3)** in the "Ethernet and Cabling" chapter. Alternatives to the Ethernet are FDDI, Token Ring, Arcnet, etc., although these are only niche solutions these days. The lowest layer, also called the **hardware layer**, is responsible for controlling the network hardware and responsible for bit transmission. With regard to the OSI model, two layers are combined into one.

The Internet layer

Among other things, the protocols **IP (Internet Protocol)**, **ICMP (Internet Control Message Protocol)** and **ARP (Address Resolution Protocol)** belong to the Internet layer. We will discuss **IP** in more detail below. The **Address Resolution Protocol (ARP)** is used to find a MAC address for a given **IP address**. The **Internet Control Message Protocol (ICMP)** is of interest to us in connection with the *ping* command, which we also investigate in the "Strategic troubleshooting section."

ARP assumes an intermediary function for the network access layer (lowest layer) and **ICMP** an intermediary function for the transport layer.

The Transport layer

Besides the aforementioned **Transmission Control Protocol (TCP)**, there is the **User Datagram Protocol (UDP)**. **TCP** implements secured data transmission. No packets can get lost en route. Appropriate measures are taken to ensure this does not happen. This corresponds to sending a letter with acknowledgment of receipt. **UDP** does not guarantee a secure transmission. The letter is simply sent, like we commonly send a letter, in the hope and with the belief that it will also arrive at the recipient.

The Application layer

There are a number of applications available here, some of which are already available when the TCP/IP protocol is installed on your PC. These include **telnet** for remotely operating TCP/IP devices and **ftp** for transferring data between TCP/IP devices. A secure connection can be set up between two computers via the **ssh** protocol. The best-known application layer protocol is certainly **http** to make a **web browser** like Firefox communicate with a web server.

Packing and unpacking data

If data is to be sent over the network, then it is sent down layer-by-layer and then sent over the network hardware. The higher layers use the services of the lower layers. The **application layer** data is thereby divided into smaller packets and receives a respective **header** from each of the underlying layers and sometimes a **trailer** as well. They are repackaged in every layer. On receipt, the data is passed on the reverse way, layer by layer up to the application layer, and then unpacked again accordingly.

Packing and unpacking can be briefly described as follows:

- **Sending**
The higher-level data is packed in a framework during the transition from a higher layer to an underlying layer.
 - A **header** is prefixed
 - Sometimes a **trailer** (e.g. checksum field) as well
- **Receiving**
"Unpacking" at the receiving side
- An additional network load to the actual data is created during transmission (**protocol overhead**)

Client receives the requested website: <http://www.bfe.de/index.html>

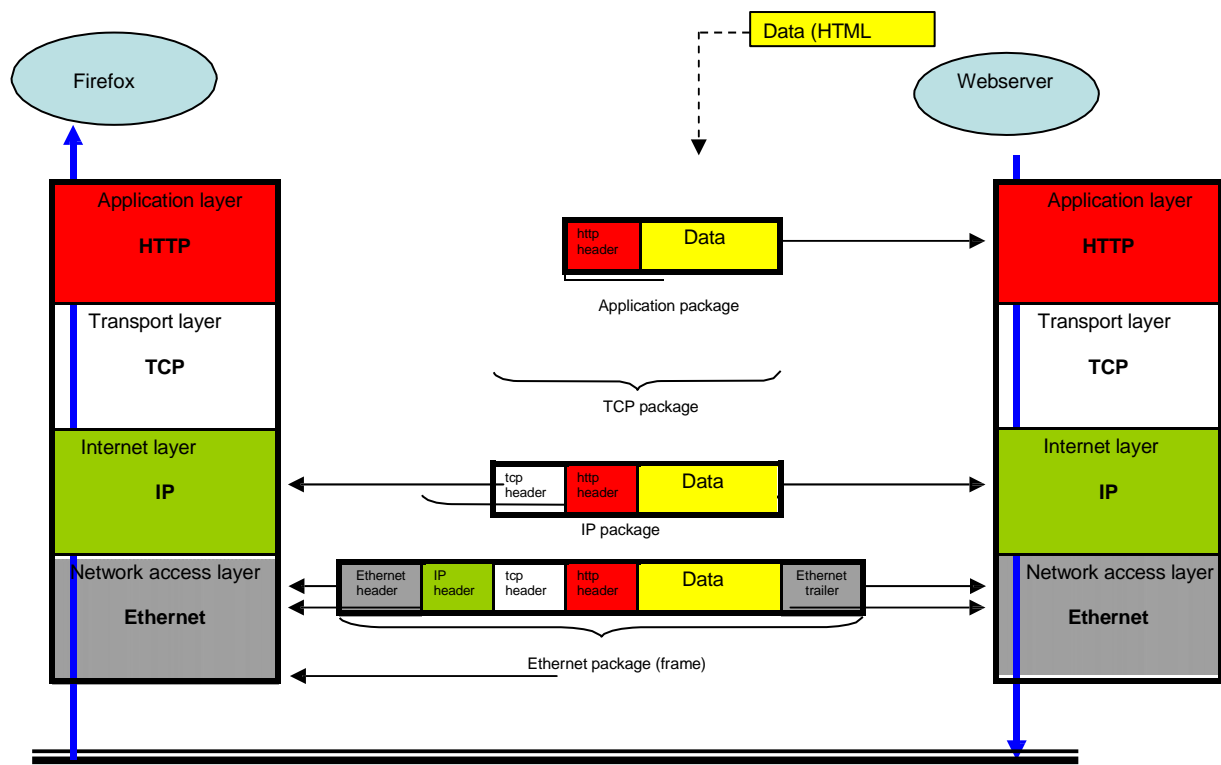


Figure 5: packing and unpacking when sending a data packet

3.3 The Internet Protocol (IP)

The **Internet Protocol**, **IP** for short, is part of the **TCP/IP** protocol family. Its main task is to address data packets and to pass these on in a packet-oriented network, which is called **routing**. All the devices in the network have their own address, called an **IP address**. The address is not used to identify a station, but also to identify a **subnetwork** where a station is located.

The **header** of an IP packet contains among, other things, the following entries:

- IP version
- packet length
- time to live
- checksum
- sender address
- recipient address

The IP addresses are available today for two versions, **IP Version 4 (IPv4)** and **IP Version 6 (IPv6)**. **IPv4** is still the current version. It is also abbreviated to **IP** (without version number).

The IP address according to **IP version 4** is 32 bits. It is split in 4 bytes that are separated by a period ("."). Each byte can receive a decimal value between 0 and 255.

IPv6 addresses consist of 128 bits and are depicted as a string of 16-bit numbers in hexadecimal form with every 2 bytes separated by a colon (":"). An address thus consists of 8 blocks with 16 bits each. Sequences of zeros can be abbreviated once by a double colon ("::"). Because the colon collides with the optional port specification in URLs, **IPv6 addresses** are enclosed in **brackets** here.

IP address according to	
IPv4	127.0.0.1
IPv6	FE80::0211:22FF:FE33:4454
IPv6 in URL	http://[FE80::0211:22FF:FE33:4454]:8080/

This seminar only discusses **IPv4**.

3.3.1. IP addresses according to Version 4

The main component of **IP** are the **IP addresses** that uniquely identify all the stations in the network. At least one IP address is assigned to each network adapter. The IP address is comparable to the street, house number and town of a regular street address. IP addresses let you unambiguously identify the computers in the network. An **IP address** may only exist once in the same network area.

Every computer on the Internet (Internet users) is allocated a unique **32-bit address** on the worldwide Internet for identification purposes.

The IP address is 32 bits (4 bytes) long and can either be depicted as binary, hexadecimal or decimal combination of numbers. The 32-bit address is divided into 8 bits (1 byte) and separated by a period (".") for easy readability.

The following table depicts the same IP address as binary, hexadecimal and decimal.

Depiction	Example IP address			
Binary	11000000.	10101000.	00000001.	01101110
Hexadecimal	C0.	A8.	01.	CE
Decimal	192.	168.	1.	110

Table: IP address in decimal and in binary form

Every byte can receive a decimal value between 0 and 255. The decimal is usually used for IP addresses.

IP addresses according to Version 4

- Address structure

- 32-bit address (4 bytes)
- Presentation as binary, hexadecimal or decimal number combination
→ usually decimal
- Group of four, each 8-bit (1 byte), separated by a decimal point
- Written as a quadruple: ***n . n . n . n***
- Every figure ***n*** 8-bit → n between 0 and 255
- Address is comparable to a house address: street, house number and town
- Address must be unique in the network

Figure 6: IP addresses according to Version 4

3.3.2. Subnet mask

Each **IP address** consists of two parts. The front part represents the **address for the network** where the station is located. Names for this include **network address**, **subnetwork** or simply **network**. The rear part presents the **address for the station**. Where the **IP address** is split is determined by the **subnet mask**. The **subnet mask** is a 32-bit number consisting of a closed chain beginning with 1s and ending with 0s.

- Each interface of a network node has its own unique IP address in the network'.
→ each device with a network interface requires its own IP address
- The IP address is divided into two parts, a **network identifier** and a **host identifier**
- The **network identifier** (= **network address**, **network name**, **network number**, **network ID**) identifies the relevant network
- The **host identifier** (= **station address**, **hostname**, **host ID**) identifies the host in the relevant network
- The network identifier and host identifier are specified using the **subnet mask = network mask**). The subnet mask specifies which bits are used as the network address.
- All the parts of the subnet mask that are assigned "1" in the binary presentation represent the network identifier, thus the 0s represent the host identifier. The "1s" in the subnet mask must be continuous.
- The network address is determined from the bit-by-bit AND link between the IP address and subnet mask.

Figure 7: subnet mask

Example:

Let's look at the **IP address** 192.168.1.110. The **subnet mask** is binary 11111111. 11111111. 11111111. 00000000. In decimal form this is 255.255.255.0. When you place the subnet mask over the **IP address** like a mask, the following division is obtained:

The size of a network is also specified by the subnet mask. You can use it to determine the number of possible hosts in a network. The number of available IP addresses in the relevant network is determined by the number of binary "0s".

Subnet mask	255. 255. 255. 0	11111111.11111111.11111111.00000000
		/
		8 x "0"

For the subnet mask 255.255.255.0, the network comprises $2^8 = 256$ IP addresses. Of those, two addresses may not be used: the lowest, which is the **network address**, and the highest, which is the **broadcast address**.

Network address	192.168.1.0
Broadcast address	192.168.1.255

254 IP addresses are thus left over that can be assigned to the hosts: 192.168.1.1 to 192.168.1.254.

Formula: calculating network size

$$\text{Number of hosts} = (2^{\text{number_of_host_bits}}) - 2$$

Note:

Another common way to depict the subnet mask is via the IP address notation.

Example:

192.168.5.33/**24**

/24 indicates the amount of "1" network bits in the subnet mask.

3.3.4. Network classes

The IP addresses are divided into 5 classes called **Class A**, **Class B**, ..., **Class E**. The **network ID** and the **host ID** have different weightings in each class. Each of these classes contains different network sizes.

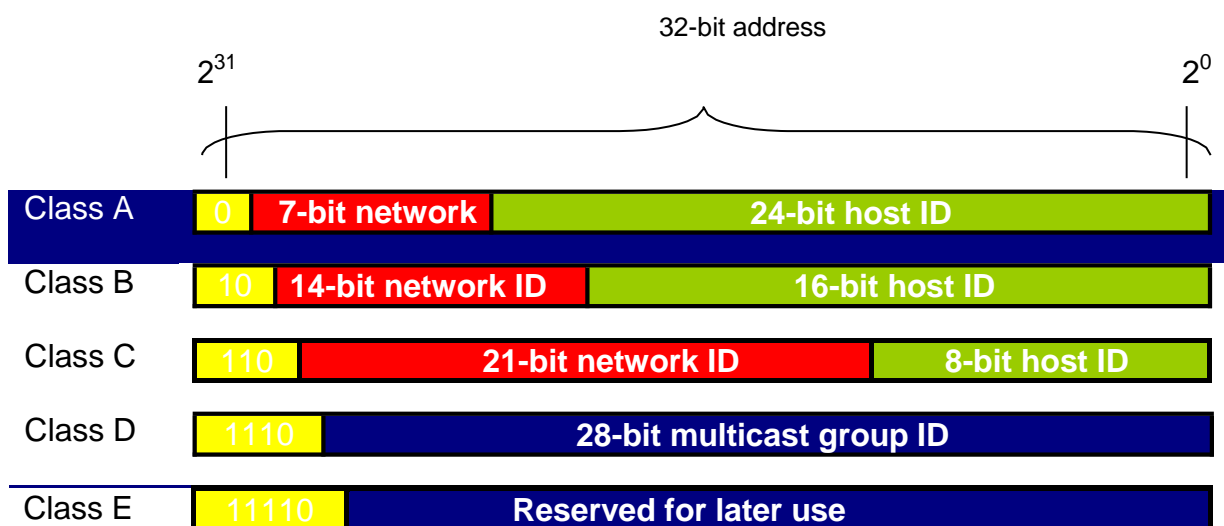
Class A networks are networks with a large number of stations. The top bit is always **0**. The theoretical address range is from 0.0.0.0 to 127.255.255.255. The effective address range is from 1.0.0.1 to 126.255.255.254. Overall, **only 126 Class A networks** are possible. That results in a calculated number of **16.774.214 possible stations per network**.

Class B networks are networks with an average number of stations. The most significant 2 bits are always **10**. The theoretical address range is from 128.0.0.0 to 191.255.255.255. The effective address range is from 128.0.0.1 to 191.255.255.254. Overall, **only 16,384 Class B networks** are possible. This results in a calculated number of **65,534 possible stations per network**.

Class C networks are networks with a large number of stations. The most significant 3 bits are always **110**. The theoretical address range is from 192.0.0.0 to 223.255.255.255. The effective address range is from 192.0.0.1 to 223.255.255.254. Overall, **2,097,152 Class C networks** are possible. This results in a calculated number of 254 possible **stations per network**.

Class D and **Class E** have no meaning for the user.

Note: Class A and B networks are frequently divided into additional subnetworks.



Special address class: (see later in the chapter)



Figure 10: network classes

Only network classes A, B and C provide subnets (network areas).

Class	Network identifier	Host identifier	Addresses from	up to	Subnet mask
A	1 byte	3 bytes	1.x.x.x	126.x.x.x	255.0.0.0
B	2 bytes	2 bytes	128.0.x.x	191.255.x.x	255.255.0.0
C	3 bytes	1 byte	192.0.0.x	223.255.255.x	255.255.255.0

Figure 11: address ranges of the network classes

Class A	<ul style="list-style-type: none"> - most significant bit = 0 - Network component comprises 1 byte, host component 3 bytes - Network addresses from: 0.0.0.0 to 126.0.0.0 (127 is reserved for the loop back address) - 7 bits for different network addresses, 24-bit host address - Number of networks: $2^7 - 1 = 126$ - Number of hosts per network: $2^{24} - 2 = 16,777,214$
Class B	<ul style="list-style-type: none"> - most significant 2 bits = 10 - Network component comprises 2 bytes, host component 2 bytes as well - Network addresses from: 128.0.0.0 to 191.255.0.0 - 14-bit different network addresses, 16-bit host address - Number of networks: $2^{14} = 16,384$ - Number of hosts per network: $2^{16} - 2 = 65,534$
Class C	<ul style="list-style-type: none"> - most significant 3 bits = 110 - Network component comprises 3 bytes, host component 1 byte - Network addresses from : 192.0.0.0 to 223.255.255.0 - 21 bits for different network addresses, 8-bit computer address - Number of networks: $2^{21} = 2,097,152$ - Number of hosts per network = $(2^8) - 2 = 254$
Class D	<ul style="list-style-type: none"> - most significant bit = 1110 - Address range: 224.0.0.0 to 239.255.255.255 - IP multicasts - Multicast addresses can be used to send datagrams to several hosts that belong to a multicast group
Class E	<ul style="list-style-type: none"> - most significant bit = 1111 - Address range: 240.0.0.0 upward - Reserved

Figure 12: network classes in detail

Notes:

The first and last addresses of a network class are each reserved as a **network address** or **broadcast address**.

→ When host addresses are assigned, not all bits of the host ID may be set to "0" or "1."

3.3.4.1 Specially reserved addresses

A number of address areas or even individual addresses are reserved for special purposes within the 32-bit address range:

- **Broadcast addresses**

A broadcast address is used to send a specific data packet to all network PCs. All the bits for the host component are set to "1."

- **Network address**

All the bits for the host component are set to "0". Examples:

Network	Broadcast	Comment
192.168.1.0	192.168.1.255	Not routed (private) Class C network
135.107.0.0	135.107.255.255	Class B network

A loopback is a loop circuit. Sender and receiver are identical in this case. Loopbacks can be used to check the accessibility of a destination. The Internet Protocol (IP) specifies a loopback network. Specially reserved IP addresses are used in the address range from **127.0.0.1 to 127.255.255.254**, whereby **127.0.0.1** is used most often. Most IP implementations support a loopback where all the packets that a computer program sends to that address are addressed to the same computer. The standard for domain names of these addresses is **localhost**. The loopback interface is used by client software, among other things, in order to communicate with a server on the same computer. Because a loopback does not require a physical network connection, a loopback is quite helpful for checking different services.

Example: applications for a loop back interface:

<http://127.0.0.1> → URL for calling up the local web server

- **localhost**

The **127.0.0.1** predefined address identifies the local computer ("localhost"): this address can be used to communicate between application instances on the same IP node without requiring the IP address of the IP node's network interface to be known (or without it even having to be connected to a network at all).

The IP address can be used for testing to see if TCP/IP was correctly installed and configured (correct function of the TCP/IP stack).

Example:

ping localhost → test method for the correct function of the TCP/IP stack
ping 127.0.0.1

- **private – non-public addresses**

Special address spaces are assigned to private networks. These IP addresses may not be used for addressing on the Internet.

3.3.4.2 Private IP address areas

IP addresses are managed by a central organization, the Network Information Center (NIC). If you want to connect to the Internet, you need a fixed IP address, an IP address space or a dynamic IP address assigned by a provider. Address spaces are available particularly for small or large private networks (non-public networks = **Intranets**) that may not be used on the Internet and can be used freely.

Class	Subnet mask	From	to
A	255.0.0.0	10.0.0.0	10255255255255
B	255.255.0.0	172.16.0.0	172.31.255.255
C	255.255.255.0	192.168.0.0	192168255255

Figure 13: private IP address spaces may not be used on the Internet

These IP address spaces are used solely for private IP networks. The private address spaces can be used as often as desired, e.g. internally in company networks. Address assignment is not globally coordinated. IP packets for these addresses are also not forwarded from a **router** in the global Internet so that the individual private networks stay isolated from one another.

Local networks that should not be seen on the Internet require a unique, unambiguous address. That's why special address spaces were reserved for these networks.

Addresses from these spaces may not be used publicly. These addresses are also not routed on the Internet.

3.3.5 The IP packet format

The **IP data packet** consists of a **header** and the space where the data payloads are located. The header precedes the data payloads. The **header** is divided into 32-bit blocks (4 bytes). Information about the service types, packet length, sender and recipient address is stored there. An **IP packet** must contain at least a 20-byte header and 8-byte data payloads or data payloads and fill data. The total length of an IP packet may not exceed 65,535 bytes. Depending on the data volume and transmission method on the bit transmission layer, the data payloads must be divided, or **fragmented**, into several IP packets.

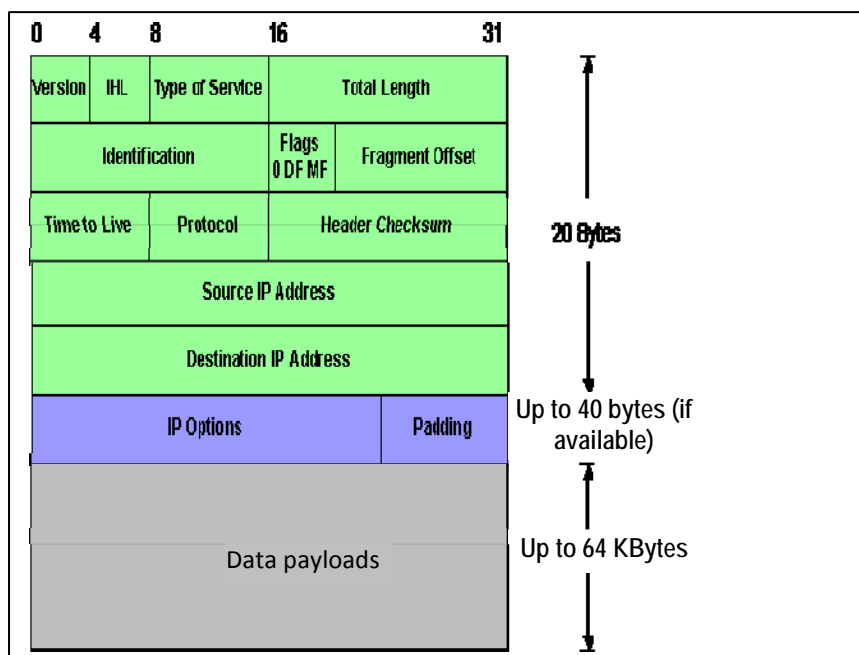


Figure 14: structure of an IP packet

Meaning of the fields in the IP header

Version	The first four bits of the header state the IP protocol version number. A "4" here stands for IPv4
IHL	(IHL = I nternet H eder L ength) specifies the length of the IP header as a multiple of 32-bit words. The maximum value of binary 1111 (decimal 15) corresponds to a header length of 15 x 32 bits = 60 bytes
Type of Service (TOS)	Specifies the quality of the requested service. The field is divided into a 3-bit priority and properties for the transmission of 5 bits.
Total length (packet length)	Packet length, contains the overall length of the IP packet (max 65,535). Subtracting the IHL results in the length of the pure payload data.

Identification (ID)	<p>The value is used to number the data packets. The ID is unique and consecutive. The unique number is necessary for assigning the fragments to a package. → to determine the sequence</p>
Flags	<p>Since the payload data usually does not fit into an IP packet, the data is split up, packed into several IP packets and then sent. This is then called fragmenting.</p> <p>The flags are used to control fragmentation, approve/block fragmentation, last fragment/more fragments follow</p> <p>1.Bit unused 2.Bit don't fragment: = 1 means packet may not be fragmented 3.Bit more fragments = 1 additional fragments follow = 0 not fragmented or last fragment</p>
Fragment Offset	<p>If an IP package contains fragmented payload data, then this field provides the data's position in the original IP packet.</p>
Time to Live	<p>The <i>Time to Live (TTL)</i> field is used to avoid endlessly circulating packets on the Internet (and thus the robustness of the network as well). It is set by an IP packet sender to a value specified by him. On the way through the Internet, every router reduces the value of this field by "1" (and changes the checksum accordingly). When the TTL field reaches the value 0, the packet is rejected. However, the sender is informed about it in this case.</p> <p>TTL values are generally between 30 and 64. Why? Measure against looping</p> <ul style="list-style-type: none"> - is possible with faulty configurations - Every router decrements the TTL field - Packets with TTL=0 are rejected - The rejecting router sends an error message to the sender <p>Application:</p> <ul style="list-style-type: none"> - determining the route on a path through the network - through test packets with TTLs 1,2,3,... - and waiting for error messages - Programs: traceroute (Ubuntu) or tracert.exe (Windows)
Protocol	<p>The protocol to be transmitted. Indication of the next highest protocol</p> <ul style="list-style-type: none"> - TCP (6)

	- UDP (17)
Header Checksum	Contains a 16-bit checksum only about the fields of the IP header, including possible option fields, but without the payload data. It is used to detect any possible bit errors during transmission in the IP header. When this kind of an error is detected, the IP packet is simply discarded to avoid any processing based on erroneous information. The packet sender won't find out about it.
Source IP address destination IP address	Source IP address, sender address, destination IP address, recipient
Options	Other options are possible, but are not used

The fields **Identification**, **Flags** and **Fragmentation Offset** are used to split up an IP datagram into several IP packages for transmission via a network. As a prerequisite for **fragmenting** an IP package, the sender assigns a 16-bit identifier in the **Identification** field: this lets the recipient separate fragments from different datagrams later on (and only assemble those that match).

3.3.6 Routing

If data packets must be sent, it is crucial whether or not the receiver station is located in the same subnetwork. If the receiving station is located in the same network, the data packet can then be sent directly. If the data packet is located in another network, the data packet is then sent to a particular device, called a **router**, which then forwards it to the corresponding network. Two networks with different network addresses can be connected to one another via a **router**. To do so, the **router** must be configured accordingly. However, the router must know where it should send the packet to. Router configuration is not a trivial matter and is not part of this seminar. Several routers can belong to a single network. It is also possible that a router can establish a connection to several networks.

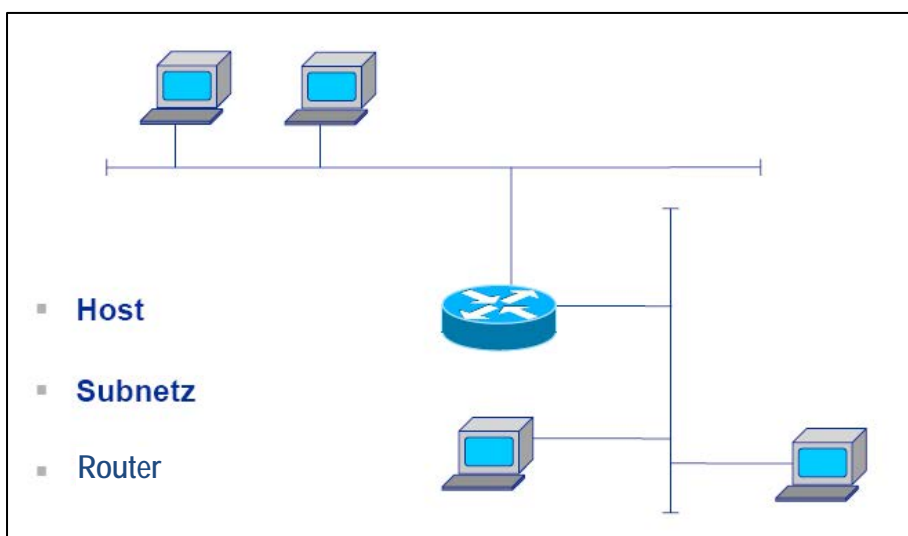


Figure 15: routing principle

Local "mail" can be sent directly. Other "mail" is sent to a distributor, **router**, which takes care of the rest of the delivery.

The IP routing process

The sending station must come to a decision if the "mail" can be delivered directly or if it must be sent to the **router**, which then forwards it. The sending station uses the destination IP address and the subnet mask to determine whether the destination station is located in the local network or not. Local "mail" is addressed directly.

Expressed more technically, this means:

If a data packet must be sent, the sending host must then make a routing decision. A route is a path through a network (possibly across several networks) to a destination host. Routing decisions are made by the **Internet Protocol (IP)**. **IP** determines the network share (network address) of the destination host in order to determine the destination network. **IP** searches for this network address in the computer's local routing table. If no suitable entry is available, the default entry is selected.

In terms of a simple home network, the router is already integrated into the "DSL router." In order to be able to perform this task, it must be entered in the station's IP configuration as a so-called "**default gateway**" (default router).

Situation: simple, small company network with one router. The computers have only one network interface.

Decision-making process on a computer or router...

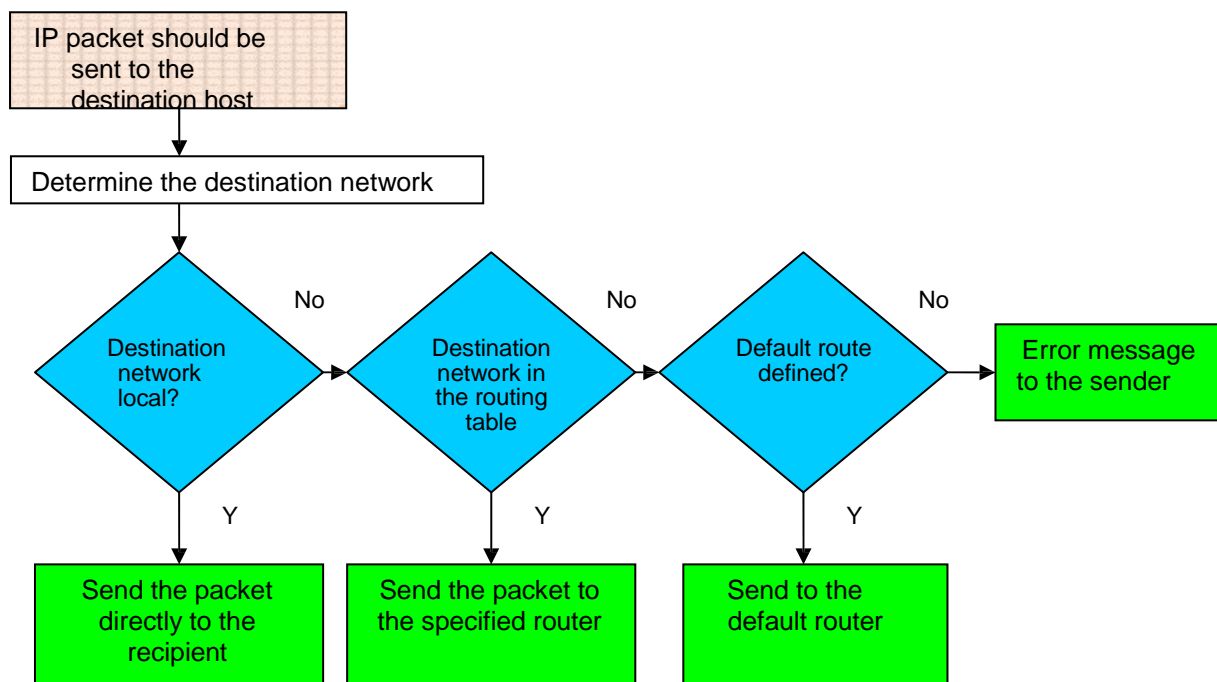


Figure 16: IP routing process – decision tree on one computer or router

Conclusion: a default route should be configured on the computer for unknown destinations.

Internet Protocol (IP) summary

- Every IP address has a network and a host component.
- The network component identifies the network, the host component the host.
- The network component and host component are determined by the subnet mask (network mask).
- All the parts of the subnet mask that are assigned a "1" in the binary notation represent the network component. The 0s represent the host component.
- The "1" in the subnet mask must be continuous.
- The network address is determined bit-by-bit AND link between the IP address and the subnet mask.
- The lowest address in the network is the network address, although this must not be assigned to a host.
- The highest address in the network is the broadcast address. It may not be assigned to a host.
- The number of hosts in a network is $(2^{\text{number_of_host_bit}}) - 2$
- Only computers that are in the same network can mutually "see" each other, i.e. exchange data with one another, without additional aids.

3.4. The Transport Layer

Above the Internet layer (**IP**) is the transport layer with the protocols **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol). **TCP** is connection-oriented and **UDP** connectionless.

The following is a brief overview of **TCP** and **UDP** before the two protocols are regarded in more detail.

- **TCP → connection-oriented**

A fixed connection is established between two networked computers. The connection remains until all the data has been transmitted. This is suitable for large data quantities. The programs involved in the transmission are active the entire time until transmission is completed. **TCP** guarantees a secure transmission.

Example: **HTTP, FTP**

- **UDP → connectionless**

No fixed connection is established. The involved programs do not communicate permanently. This type of data transmission is ideally used for smaller data amounts (for **DNS** requests or time synchronization with **NTP** for example). **UDP** does not guarantee a secure transmission. Applications that use **UDP** must have their own corrective measures for lost or incorrectly received packets because the **UDP** protocol itself does not have these capabilities.

Example: the client sends a request to the server. If the request is not answered, the client repeats the request after a specific interval until he receives an answer. If no answer is received within a set time, a timeout report is produced.

The server sends the answer without worrying about it reaching the requesting host.

Example: **DNS, NTP**

- **Who determines when TCP or UDP is used?**

The protocol on the **application level** determines whether this is a **connection-oriented** or a **connectionless** transmission:

→ see section: application layer

3.4.1 TCP (Transmission Control Protocol)

In the TCP / IP protocol family, **TCP**, as a connection-oriented protocol, takes on the task of data security, data flow control, and takes measures when data loss occurs. TCP works by dividing the data stream from the applications, providing it with a header, and passing it on to the Internet Protocol (**IP**). The data packets are sorted and reassembled at the recipient.

Figure 17 depicts the tasks and functions of **TCP**.

- Secure transmission
- Multiplexes of connections → simultaneous access to the transport layer of several applications
- End-to-end controlled connection
 - Acknowledgement
 - Repeating packets
- Connection management
 - Connection setup
 - Data transmission
 - Connection termination
- Flow control → sequentially numbering the data packets
- Time monitoring the connection
 - Acknowledging data after a specified time, otherwise repetition
- Troubleshooting
 - Checking the data
 - Forwarding error messages
 - Requesting missing packets
- Socket concept
 - Used to uniquely identify a service on a computer
- Process – port
 - identified on a PC by a unique port number
- Formal
 - A TCP-connection is characterized by a 5 value (tuple):
{protocol; local address; local port; remote address; remote port}

```
| {tcp; 131.188.3.150; 1022; 131.188.3.40; 22}  
  
lisa$ netstat -an | grep 131.188.3.40  
131.188.3.150.1022 131.188.3.40.22 17520 0 33580 0 ESTABLISHED  
131.188.3.150.1011 131.188.3.40.22 17520 0 33580 0 ESTABLISHED
```

Figure 17: tasks and functions of TCP

Each data packet that TCP passes on to IP is prefixed by a header that, among other things, contains the following information:

- Source port
- Destination port
- Sequence number
- Checksum
- Control

The following picture depicts the TCP packet structure.

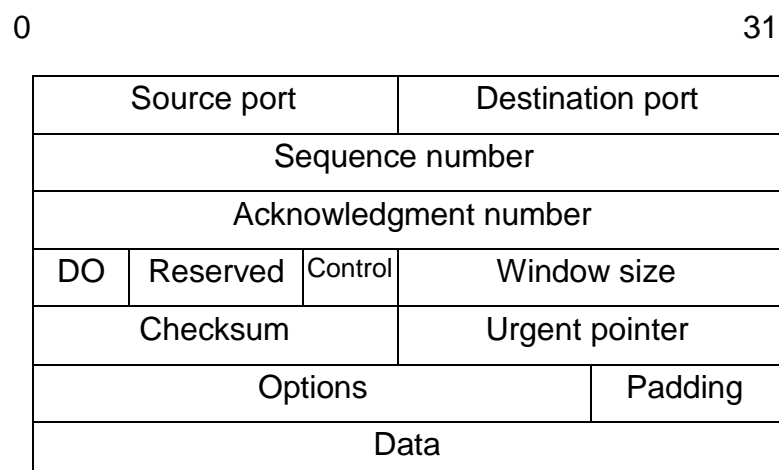


Figure 18: TCP frame structure

Source port	Source port of the sender process
Destination port	Destination port about which process the data is intended for. Continuous numbering of data packets
Sequence number	Information about which data packets (sequence number) were received
Acknowledgment number	Data Offset: begin of the Unused
DO	fields data field
Reserved	Flags for establishing and cancelling connections
control	<ul style="list-style-type: none"> - URG = 1 marks priority data, note Urgent Pointer - ACK = 1 confirms data has been received - Push = 1 data is forwarded immediately (for Telnet always 1)

	<ul style="list-style-type: none"> - RST = 1 sender wants to terminate the connection - SYN = 1 connection should be synchronized - FIN = 1 connection is terminated
Window Size	Framework of the data packets that do not need to be
Checksum	confirmed require a TCP header review
Urgent Pointer	Display for data priority

Ports

As already mentioned at the beginning of this chapter, every running network application on a PC is assigned an additional number – a so-called **port**. This makes it possible for several network applications to run simultaneously on a single system. Several applications can thus simultaneously establish connections to their communication partners over the network. The different data streams are separated from one another by ports.

Data packets that reach their destination via **IP** are assembled by **TCP** and passed to the application via the **port** number. This **port** is constantly monitored by the running application, also known as a process or service

The port number can receive values between 0 and 65535. A part of the ports is assigned and permanently assigned to an application, service or a protocol. They are between 0 and 1023. These ports are managed by the Internet Assigned Numbers Authority (**IANA**).

Port number	Service (protocol)	Description
20	FTP data	File transfer (data transfer from the server to the client)
21	FTP	File transfer (initiation of the session and transmission of the FTP control commands by the client)
22	SSH	Secure shell
25	SMTP	Sending e-mail

80	HTTP	Webserver
110	POP3	Client access for e-mail server
123	NTP	Time synchronization between computers
443	HTTPS	Encrypted web server transmission, mostly with SSL or TLS encryption

Figure 19: examples of known ports

3.4.2. UDP (User Datagram Protocol)

The **User Datagram Protocol (UDP)** is a minimal, connectionless protocol. In contrast to TCP, data transmission is not secured. Instead, it is significantly thinner and allows faster data transmission.

Main features of UDP are:

- unsecured transport protocol
- more efficient than TCP in the LAN area
- no flow control
- application must deal with data losses itself
- use for multimedia applications

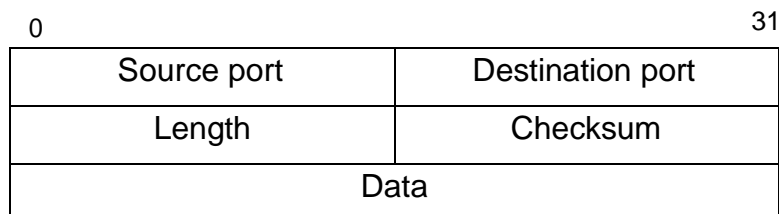


Figure 20 : the UDP frame structure

Source port	Source port, port number of the sending process (optional)
Destination port	Destination port, address of the receiver port, indicates which process the packet should receive
Length	Length field, length of the entire UDP frame
Checksum	Checksum field, checksum of the UDP header if the other systems support this field
Data	UDP data, payload data for the higher protocols max. approx. 64 kByte

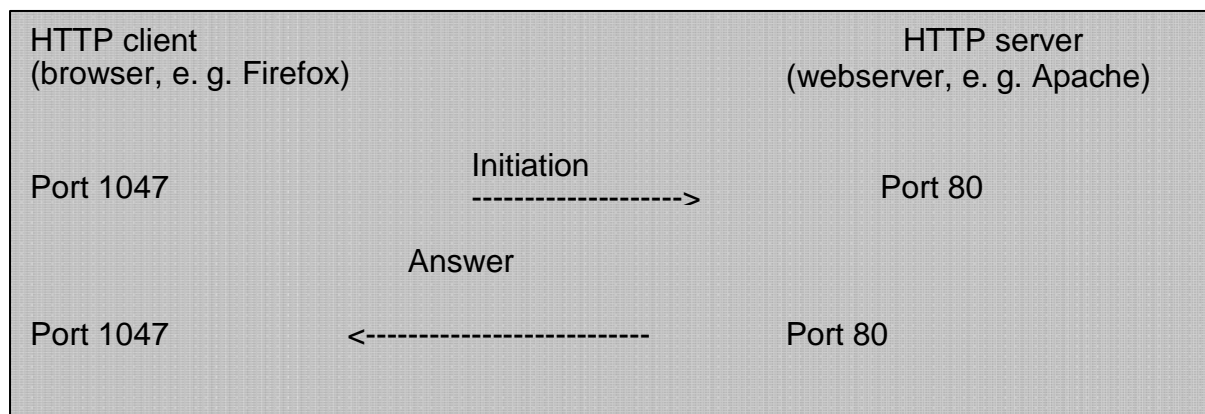
3.5 The Application Layer

The application layer programs use the underlying protocols in order to communicate over the network. These are usually client/server applications. These programs work with **ports**. This is an addendum to the protocol that identifies the application. An **HTTP** connection sends, by default on **Port 80** for example, e-mail with SMTP on port 25 and POP3 on port 110.

Communication is generally opened by the client with this kind of client/server application. The server "listens" to a specific port. The client establishes a connection to the server, thus initiating the connection. It uses a port > 1024 to do this and comes into contact with the relevant server port.

The initiative then goes over to the server. This now connects to the port of the client via its own port.

Example: HTTP communication between client (browser) and server (webserver)



Pairs are created from the IP address and the port number whenever communication takes place. These pairs are called **sockets** and represent the end points of communication.

3.5.1. Application layer protocols based on TCP

ssh Port 22/tcp	Secure Shell <ul style="list-style-type: none">• Secure access on remote computers. Authentication and data transmission are encrypted• Works like a connected terminal
ftp Ports 20/ tcp, 21/tcp	File Transfer Protocol <ul style="list-style-type: none">• Data transmission from/to a remote computer• Works with 2 ports• Active mode: Port 21 commands (control port)

<p>smtp Port 25/tcp</p> <p>http Port 80/tcp</p> <p>https Port 443/tcp</p> <p>pop3 Port 110/tcp</p> <p>imap Port 143/tcp</p>	<p>Port 20 data</p> <ul style="list-style-type: none"> • Passive mode: Data port > 1023 is negotiated <p>Simple Mail Transfer Protocol</p> <ul style="list-style-type: none"> • Electronic post for sending e-mail <p>Hypertext Transfer Protocol</p> <ul style="list-style-type: none"> • The World Wide Web (WWW), for transmitting websites that are formatted with the page-description language (x)html. <p>Hypertext Transfer Protocol Secure</p> <ul style="list-style-type: none"> • Encrypts the data and offers increased security compared to http <p>Post Office Protocol</p> <ul style="list-style-type: none"> • For picking up e-mails from the mail server. Because of its limitations, the e-mail can only be picked up on or deleted from the server. → is increasingly being replaced by IMAP <p>Internet Message Access Protocol</p> <ul style="list-style-type: none"> • For retrieving and managing e-mails in the network. Compared to POP3, the e-mails can stay on the server. This then allows access to the same mailbox from different computers.
<p>nntp Port 119/tcp</p>	<p>Network News Transfer Protocol</p> <ul style="list-style-type: none"> • This protocol is used by news groups

3.5.2. Protocols of the application layer based on UDP

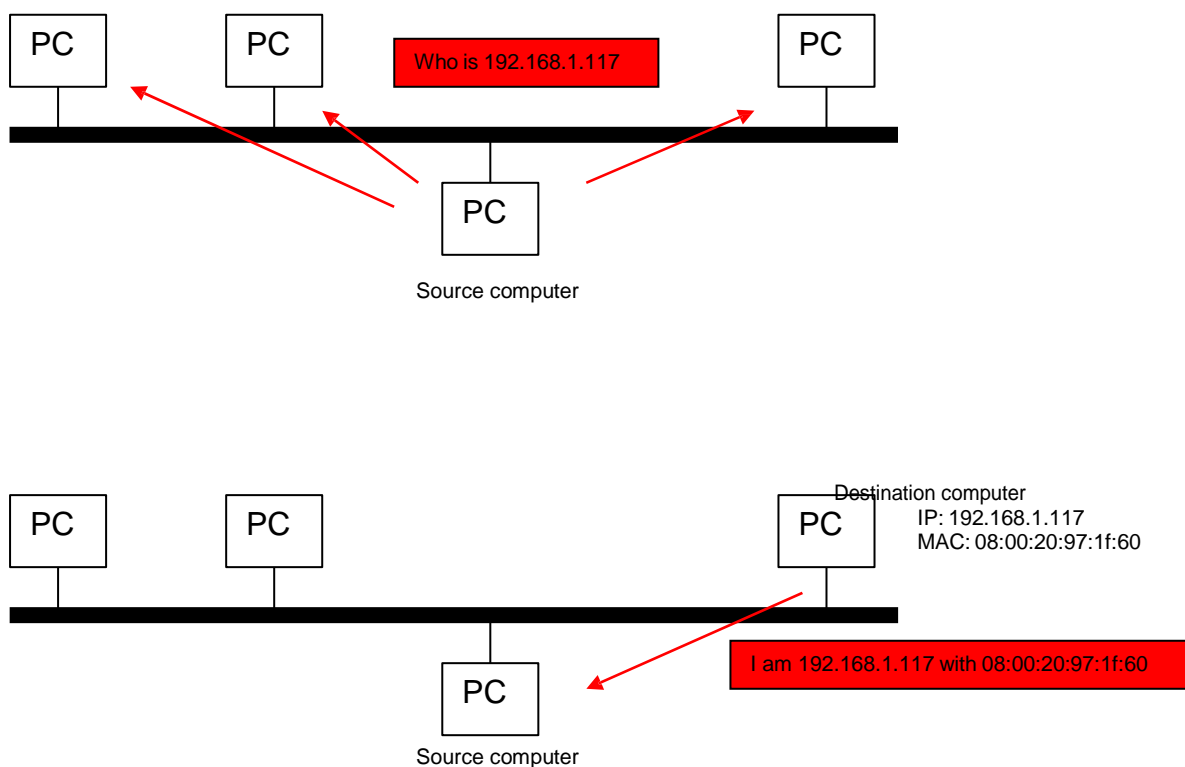
<p>ntp Port 123/udp</p>	<p>Network Time Protocol</p> <ul style="list-style-type: none"> • This protocol is used so that hosts can receive the exact time from high-precision timers like the PTB - the National Metrology Institute of Germany.
<p>dns Port 53/udp/tcp</p>	<p>Domain Name System</p> <ul style="list-style-type: none"> • For name resolution, translating domain names into IP addresses (forward lookup) or vice-versa (reverse lookup). <p>Note: udp or tcp is used based on packet size</p>

3.6 ARP (Address Resolution Protocol)

The **ARP** protocol transmits the network card's 48 bit (6 byte, 12 hexadecimal digits) hardware address (**MAC address**) to the Internet Protocol (**IP**). ARP thereby creates a table in the LAN of all the known hardware addresses. This table is available to the **IP** for data transmission.

- Finding the MAC address for an IP address
- Procedure:
 - Source computer: transmit broadcast with content
 - ... own IP address
 - ... own MAC address
 - ... destination IP address
 - ... dummy MAC address
 - answer from the destination computer (or a Proxy ARP server) with content
 - ... own IP address
 - ... own MAC address
 - ... source IP address
 - ... source MAC address
- Storage of once determined conversions (ARP cache, with aging function)
- ARP does not build on IP

Figure 21: ARP function



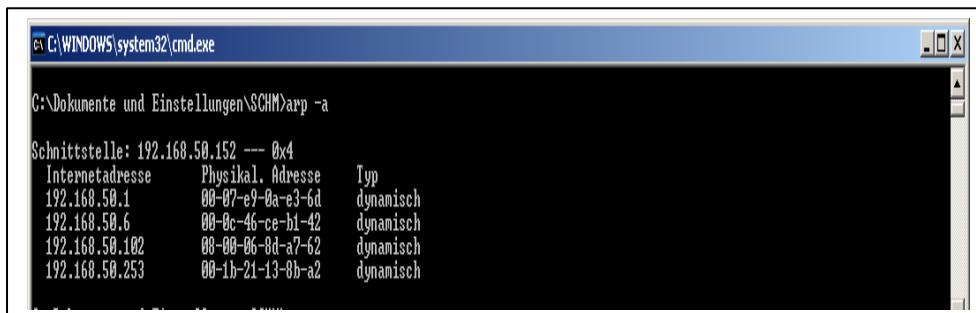
ARP breaks up IP addresses into **MAC addresses (hardware addresses)**.

Ethernet (IEEE 802.3) does not know any IP addresses. Instead it works with the **MAC addresses** of the network cards. Therefore, data can only be sent to another computer when its **MAC address** is known. The TCP/IP data packets, however, only contain the recipient's IP address. This is where **ARP** comes into play. The packet's sender sends an ARP request as a broadcast. This request contains the **source MAC Address**, the **source IP address** and the **destination IP address**.

All computers that are in the same subnet receive this request, but only the host with the destination IP address sends an ARP reply to the source host. The source host can now send the packet.

In order to avoid sending these requests again every time, the answers are buffered for a certain time in the **ARP cache** at the source and destination host.

The **arp** command is available in the Windows command line (in a console window) in order to view the contents of the ARP cache and edit the entries in it. To do so, the **arp** command must be opened with the corresponding options, which can be found in the online help.



```
C:\WINDOWS\system32\cmd.exe
C:\Dokumente und Einstellungen\SCHM>arp -a

Schnittstelle: 192.168.50.152 --- 0x4
Internetadresse      Physikal. Adresse    Typ
192.168.50.1         00-07-e9-0a-e3-6d    dynamisch
192.168.50.6         00-0c-46-ce-b1-42    dynamisch
192.168.50.102       00-00-06-8d-a7-62    dynamisch
192.168.50.253       00-1b-21-13-8b-a2    dynamisch
```

Figure 22: ARP cache notifications on a Windows computer in a console window

You do not need to work with the **arp** command because ARP is fully automatic and the ARP cache purges itself continuously. **ARP** related problems or errors do not normally occur in the network.

3.7 ICMP (Internet Control Message Protocol)

The **Internet Control Message Protocol (ICMP)** is a component of the **Internet Protocol (IP)** and is like an **auxiliary protocol for IP**. The **ICMP** is used to exchange messages (status and error information) via **IP** in the network. The **ICMP** messages are used between computers and active network nodes, such as routers, in order to notify each other about data packet related problems.

Every computer and active network node in the TCP/IP network knows how to use the **ICMP** protocol.

Most **ICMP** packets contain diagnostic information. They are, for example, sent back from the router to the source when the router rejects packets because the destination cannot be reached, **Time to Live (TTL)** has expired, etc.

The structure of an **ICMP** message may be depicted as follows:

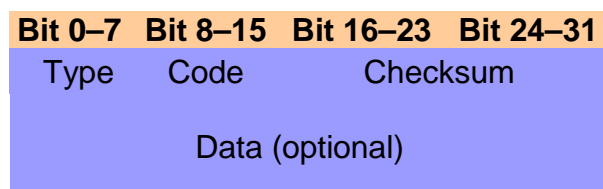


Figure 23: ICMP frame

Important ICMP packet types

ICMP works with different message types (**type field**). Some of these also have a **code field** in order to specify the message more precisely. The "Type" field indicates the class of the ICMP message. The "Code" field specifies the type of message more precisely.

Type	Description	Description
8	Echo Request ("PING")	The echo request is used by the ping command. This command determines whether a host can be reached via the requested IP address.
0	Echo Reply ("PONG")	This is the answer to the ping. The answer is provided when the destination host can be reached at this IP address. Since the echo reply is increasingly being blocked by firewalls these days, this does not say anything about the computer's accessibility however. This can very well still be reached, for example on Port 80 (HTTP).
3	Destination Unreachable	This message is returned when a router detects that the host or the network does not exist or is out of range. A host sends this response when it is not addressable on the

		requested protocol or port.
4	Source Quench	When the buffer capacity is insufficient on a router to pass the packet on to the next router or the host, this message is then sent to the source host. This is a request to reduce the data transmission rate.
5	Redirect	Alternative router information can be sent to a host in this way.
11	Time Exceeded	When the TTL (Time To Live) is exceeded, the router rejects the packet and sends this message to the source host.
12	Parameter Problem	When the packet cannot be processed because of problems with the header parameters, this message is then sent to the source host.
13	Timestamp Request	
14	Timestamp Reply	
17	Address Mask Request	
18	Address Mask Reply	

Figure 24: type field, important ICMP packet types

The following table identifies the content of the Code field, for example, when the "destination is unreachable" This is the type 3 "Destination Unreachable" error message

Code field	Description
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed, DF set
5	Source route failed
6	Destination network unknown
7	Destination host unknown

8	Source host isolated
9	Communication with destination network prohibited
10	Communication with destination host prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service

Figure 25: ICMP code values for message type 3 "Destination Unreachable"

Applying ICMP

Most users rarely come into direct contact with **ICMP**. **ICMP** messages are caused by network stations that want to communicate problems with IP packets to the triggering stations.

Network analysis tools also use **ICMP**. For example, TCP/IP makes tools used for network analysis available on each computer.

The most common tool that uses **ICMP** is the **ping command**. The **ICMP** message can be both incoming and outgoing here. When a host sends a PING (source host), it receives a PONG as an answer from the computer (**host**) that was "pinged" (destination host). The exact opposite is true for the destination host. It receives a PING (incoming) and sends a PONG (outgoing).

A second network analysis tool is **tracert** (under Linux) or **tracert.exe** (under Windows), which can be used to determine which routers transmit data packets to the destination computer. This is a route tracking tool.

Functions

- Network functionality test
 - Echo Request
 - Echo Reply
 - with *ping* command
- Error messages
 - Destination unreachable (from router)
 - Source quench (from router in case of overload)
 - Redirect (from router: use another router)
 - Time Exceeded (TTL was 0)
 - Parameter problem (format error in the header)
- Information services
 - Information request/reply (query IP address for yourself)
 - Address mask request/reply (query subnet mask)
 - Timestamp request/reply (time mark)
- General: error and control messages
- Type field, Code field

Figure 26: ICMP tasks

4 DHCP (Dynamic Host Configuration Protocol)

Learning objectives:

- Understand the DHCP function principle
- Define the tasks and operating mode of the DHCP server
- Indicate what happens when a DHCP client cannot reach a DHCP server
- Specify the DHCP server configuration parameters
- Basic configuration of the DHCP server

4.1 Basics

In order to set up a TCP/IP network, it is necessary to configure every individual station. Each computer thus requires at least one **unique IP address** and one **subnet mask** in order to communicate with the other devices in the same network. The addresses from the **default gateway** and from the **nameserver (DNS server)** are also required as well. Planning, configuration and maintenance is very complex with larger networks.

To reduce this effort, a central Server service (**DHCP server**) for the **fully automatic configuration of TCP/IP** is used.

It is worthwhile to control address allocation via a central **DHCP server** even in a smaller network. Advantages: maintenance is less time-consuming since no work is required on the individual clients. Address conflicts are a thing of the past because the **DHCP server** controls IP address allocation.

Functional principle of DHCP

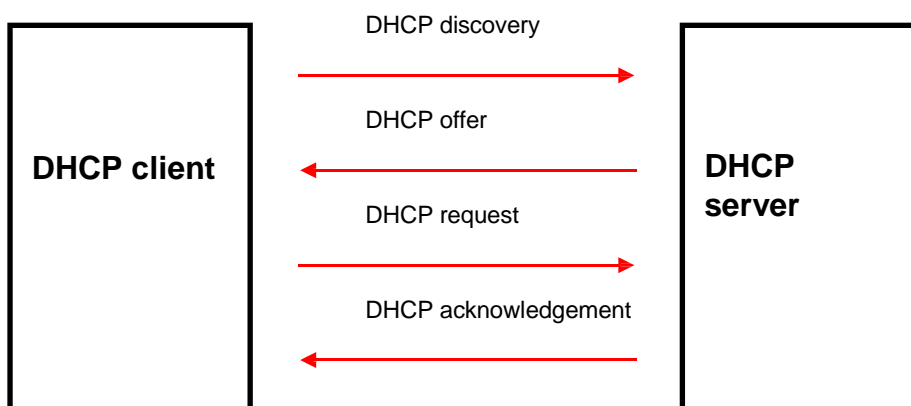


Figure 1: functional principle of DHCP

DHCP is a client-server architecture. The **DHCP server** has a pool of IP addresses that it can freely assign to the **DHCP clients**. Using a multi-step process (DHCP discovery, DHCP offer, etc.), the DHCP client dynamically receives an IP address with subnet mask from the DHCP server for a specific period of time (**lease time**).

If desired, the DHCP server will pass on other parameters such as the default gateway and the nameserver addresses (DNS servers). This minimizes

additional sources of error.

The client's hardware address (**MAC address**), the assigned IP address and the period of validity (**lease time**) are stored on the **DHCP server**.

An additional configuration option of the DHCP server is to assign the same IP addresses to certain clients, which gives them a **quasi static IP address**. This works via a so-called **MAC address reservation**.

4.2 Configuration

4.2.1 DHCP client

Configuring the **DHCP client** under Windows is usually not at all necessary. With the normal basic installation of Windows 2000/XP/Vista, the network environment is already pre-configured in such a way that the client obtains all the information from the **DHCP server**. If a DHCP server is installed and available, the operating system obtains the necessary IP configuration data automatically at system startup. For the Windows computer to work as a DHCP client, the network environment must be configured as follows:

Start → Programs → Control panel → Network control → LAN connection context → Properties → Internet protocol TCP/IP → Properties

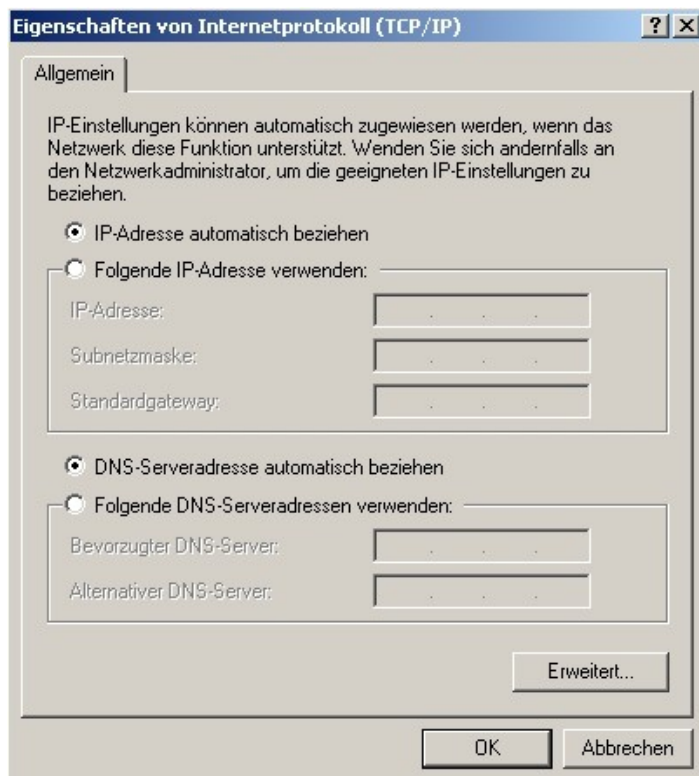


Figure 2: using the DHCP service under Windows

You can also display the current TCP/IP configuration in a terminal window. Use the ***ipconfig /all*** command-line command to display and check the current IP configuration data.

Frequent sources of error

When the PC has received an address from the 169.254.0.1 ... 169.254.255.254 range, this is an indication that the PC would like to obtain the IP addresses automatically, but has not found a DHCP server.

When a PC that is configured to automatically assign an IP address does not find a DHCP server, it assigns itself a randomly selected address from the 169.254.0.0/16 range. Before finally deciding on this address, it transmits a ***ping*** with the selected address as the destination. If no answer follows, the PC assumes that this address is still available. This procedure is called **Automatic Private IP Addressing (APIPA)**.

Note:

The renewed search for a DHCP server can be triggered with the ***ipconfig /release*** and ***ipconfig /renew*** command-line commands. Prerequisite: you must be logged onto your Windows computer with administrator rights.

4.2.2 DHCP server

Automatic IP address allocation requires a so-called **DHCP server** that makes its services available to the DHCP clients. When booting, the devices receive their IP address from the DHCP server from a defined address pool. Nowadays, most hardware DSL routers offer a DHCP service. The following figure shows how this service is set up based on the Fritz!Box 7170 example.

The DSL router must be assigned a static LAN IP address and the IP address pool is defined. No further action is required for the basic configuration of the DHCP server.

4.3 DHCP client/server communication

After the start, an operating system configured as a **DHCP client** (the default setting in Windows XP or 2000 for example) only knows that the TCP/IP protocol must be used, which network card it should use, and that a **DHCP server** will provide any additional information.

The DHCP client must find the **DHCP server** first. It starts a query to all connected network computers and only receives the suitable answer from the **DHCP server**, namely an IP address.

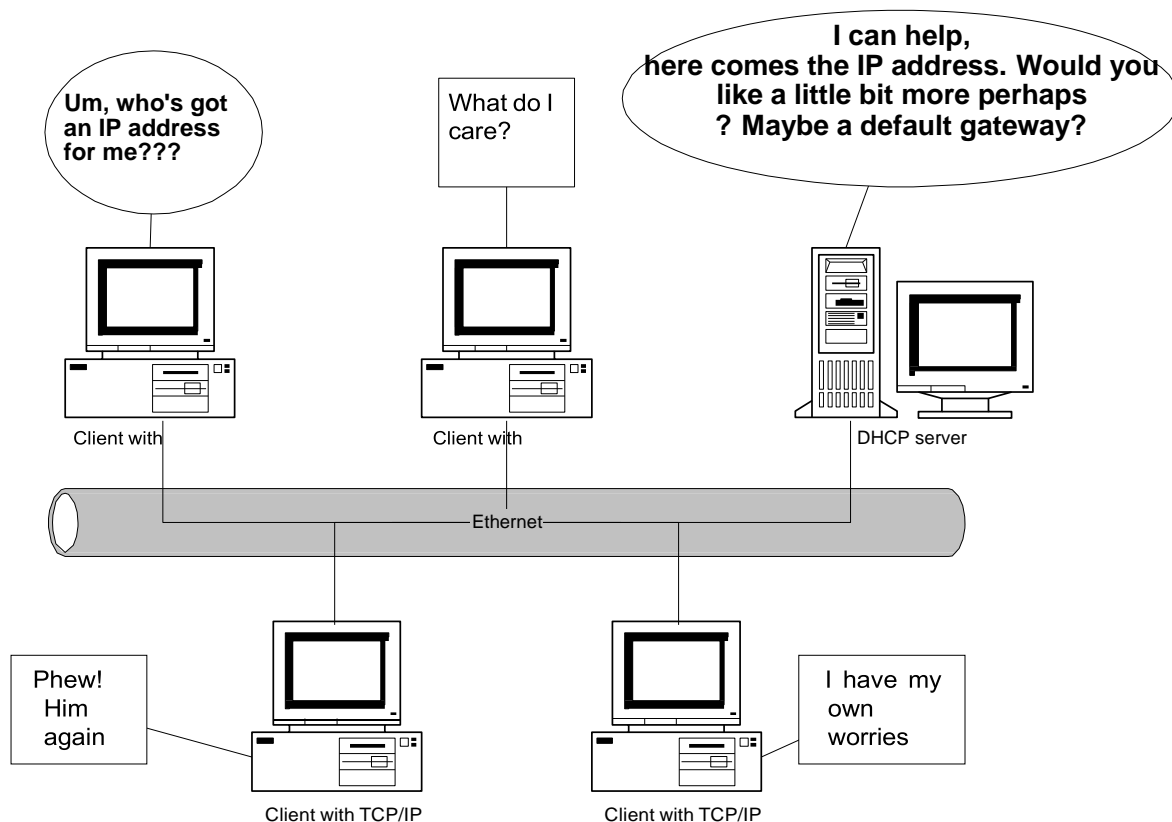


Figure 4: Procedure: DHCP client/server communication

The **DHCP Server** manages a data file that, first of all, contains information that is valid for each client and, second, has a range of IP addresses that are released for clients. When a client asks the server for an IP address, the server determines whether this computer has already received an IP address based on the network card address (also called a **MAC address**). If this is the case, the client is assigned this address again and transmitted with the general information. However, if the client is not known or the previously assigned address has been reassigned in the meantime, a free address is assigned from the pool.

5 DNS (Domain Name System)

Learning objectives:

understand the tasks and function of DNS

recognize the advantages of a domain name as opposed to IP addresses.

know the meaning of and evaluate a fully qualified domain name (FQDN) Indicate the main components of DNS

specify the required configuration parameters for the DNS client

5.1 Introduction

Communication with a computer on the Internet happens via the IP address. However, it doesn't make sense for people to remember this "string of numbers." They would much prefer to work with symbolic names only. Figure 1 shows some differences between the IP address and symbolic names, which are called domain names here.

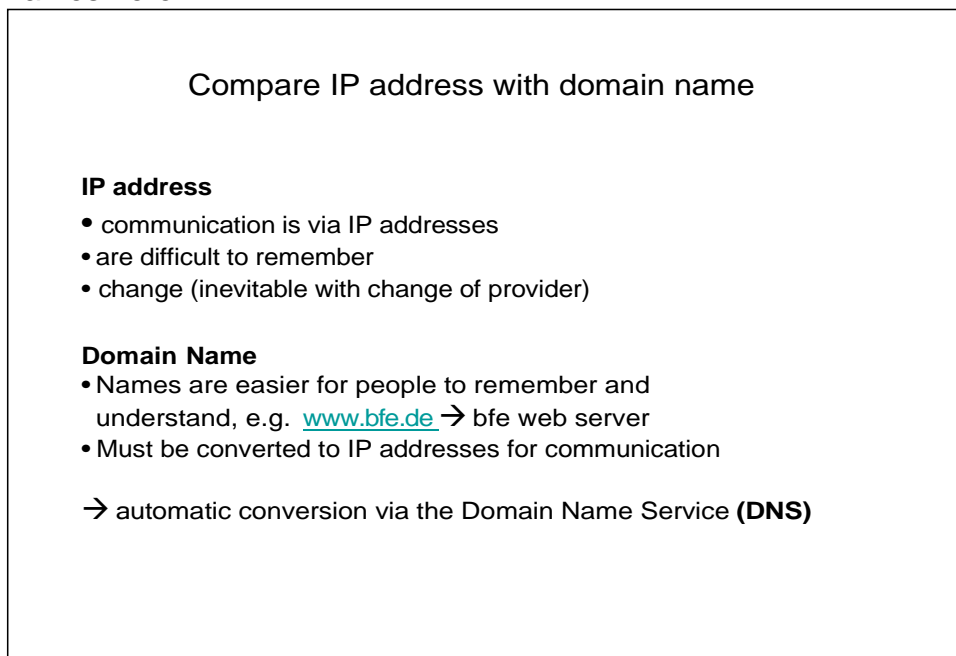


Figure 1: comparing the IP address with the domain name

The Domain Name System (DNS) is one of the most important services on the Internet. Its main task is to answer name resolution requests. Similar to directory assistance, DNS should name a computer name (hostname), the "addressee" on the Internet – for example www.busch-jaeger.de as an answer, the corresponding IP address, the "extension number" – for example 129.35.205.133 - upon request.

Additional properties and performance characteristics of DNS can be depicted based on the following points:

DNS - hierarchically distributed database

The DNS is a hierarchical database that is spread across thousands of servers worldwide to manage the Internet's namespace. This name space is subdivided into so-called zones that independent administrators are responsible for. For local requirements – within a company network, for example – it is also possible to operate a DNS that is independent of the Internet.

Main function of DNS – convert a domain name into an IP address

The DNS is mainly used to convert domain names into IP addresses ("forward lookup"). This is similar to a phone book, which converts the names of the participants to their telephone number. DNS thus offers a simplification because people can remember names much better than strings of numbers. This way, you can generally remember the domain names `www.busch-jaeger.de` more easily than the corresponding `129.35.205.133` IP address.

Also possible using DNS – Conversion of IP address to domain name

Using DNS, a reversed resolution of IP addresses into names is possible ("reverse lookup"). In analogy to the telephone directory, this corresponds to a search for the subscriber name for a known number, which is known within the telecommunications industry under the name "inverse search".

An advantage of DNS – simple change of IP address

A further advantage is, that the IP addresses – for example from Web servers – can be changed relatively risk-free. Because Internet users only address the (unchanged) DNS names, changes to the subordinate IP level stay hidden to them to a great extent. Because several IP addresses can be assigned to a single name, even load balancing can be achieved.

The original task of DNS - replace the "hosts" file The original task was to replace the local hosts files that had been responsible for name resolution until then and that were no longer able to respond to the enormous number of new entries."

5.2 How is DNS structured?

DNS consists of three main components

- domain namespace
- nameserver (DNS server)
- resolver (DNS client)

5.3 The Domain namespace

In order to understand name resolution for **DNS**, you need to know how the **domain namespace** is structured. Starting from a root called ".", the domains are organized in a tree-like structure. The level following the root makes up the so-called **top level domains** (TLDs). One level below that are the **second-level domains**, which either directly follow the computer names (hostnames) or another level of local domains, below which are the computer names.

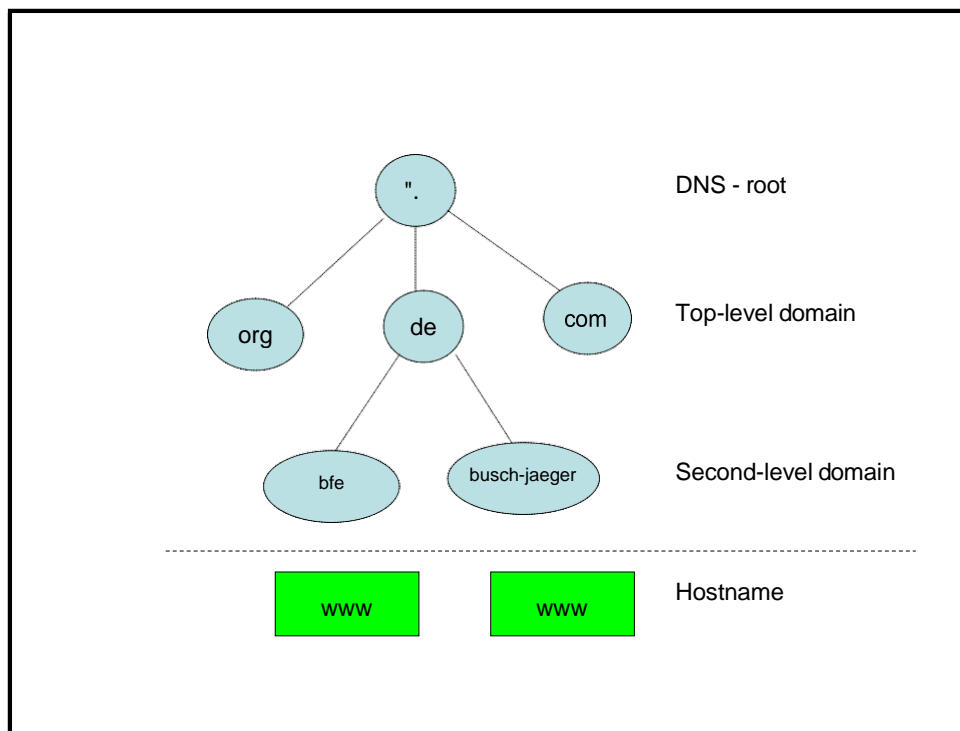


Figure 2: the domain namespace

The top-level domain distinguishes between geographical and organizational types.

Domain	Country	Domain	Organizational form
.at	Austria	.biz	Business, for large and small companies
.ch	Switzerland	.com	Commercial domain
.de	Germany	.coop	Cooperations, cooperatives
.fr	France	.edu	Schools, universities, educational institutions
		.gov	US government agencies
		.mil	The United States military
		.net	Network-specific services and offers
		.org	Non-commercial enterprises and projects

Figure 3: examples of top level domains (TLDs)

A complete list of TLDs is administered by the Internet Assigned Numbers Authority (IANA), the Internet's umbrella organization.

Second-level domains have an arbitrary but unique name within their top level domain. The responsible **Network Information Center (NIC)** for the second-level domain manages the second-level domains. **DENIC eG** (Deutsches **N**etwork **I**nformation **C**enter) is, for example, the central registration point for domains below the top level domain **.de** (for Germany).

Additional **sub-level domains** (subdomains), which the second-level domain operator is responsible for, may exist below the second-level domain.

In last place, on the lowest level, lies the computer name, also called the hostname.

5.4 Domain Name

A complete domain name consists of the concatenation of all levels. The individual levels are separated from another by periods. A domain name is completed with a period. The rearmost period is normally omitted, but, formally speaking, belongs to a complete domain name. The complete domain name is also called a **fully qualified domain name (FQDN)**. A proper and complete domain name is, for example, www.busch-jaeger.de. (Note: the last period belongs to the domain name).

A domain name, such as www.busch-jaeger.de, is always processed in right-to-left order. Beginning with the root ".", the branch "de" (TLD) leads to the branch "busch-jaeger" (registered domain), which, in turn, ends in the period "www" (name of a computer of the "busch-jaeger" domain). The search for a corresponding system thus always takes place down the tree beginning with the root directory.

Hostname	Second-level domain	First-level domain
www.	busch-jaeger.	de.
www.	bfe.	de.

Figure 4: complete domain name - to be precise, a domain must always be written with a period at the end, which represents the root directory.

5.5 The DNS server - nameserver

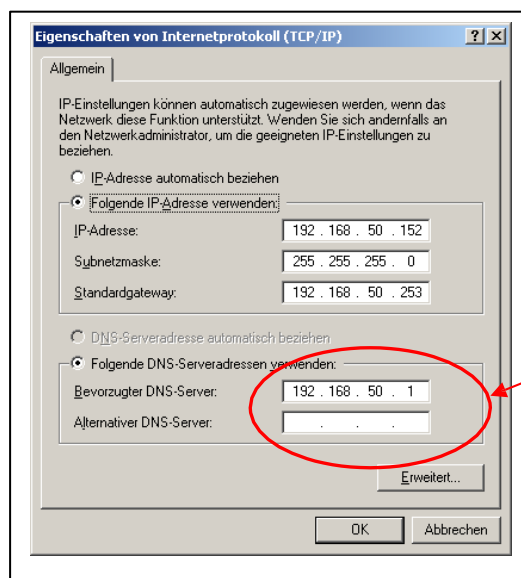
A **DNS server** never occurs alone. A primary and a secondary nameserver is always available. They are independent of one another and fully redundant so that at least one server is always accessible. The secondary nameserver synchronizes its data at regular intervals with the primary nameserver and thus acts as a backup server. In order to avoid having to burden the network with every DNS query, each DNS server has a cache to store successful DNS queries. When called up again, it retrieves already successfully resolved domain names from the cache. The saved data has a lifetime (time-to-live, TTL) of about 2 days. When an IP address is changed by transferring the domain name, the domain is thus available on the entire Internet again after 2 days at the latest.

Besides normal DNS servers, there are also the root servers, of which there are only 13 worldwide. 10 of these are in the USA. The other three are located in London, Stockholm and Tokyo.

5.6 The DNS client - resolver

The DNS client (**resolver**) is directly integrated into TCP/IP and is available there as a software library for DNS name resolution. The DNS client is called a **resolver** and is the intermediary between DNS and the application program. It returns the IP address of a domain name or the domain name of an IP address.

In order for the resolver to work, it requires the IP address from one, ideally from two DNS servers that must be entered in the TCP/IP settings or requested via DHCP.



Both DNS servers must be entered here. Usually, only the DSL router's IP address is entered here.

Figure 5: DNS client configuration

The *nslookup* command-line tool can be used to test DNS.

Who is my DNS server?

C:> nslookup

Which IP does the domain name have?

C:> nslookup www.busch-jaeger.de

5.7 DNS name resolution - forward lookup

If you require the corresponding IP address for a computer name (e.g. from www.busch-jaeger.de), the corresponding entries are first scoured in the cache and then in the local **hosts** file. If you cannot find it there, the system then passes the request on to the responsible nameserver (called the "local nameserver" in Figure 4). Each nameserver has a cache where it temporarily stores the data of the most recently searched queries. It is only when the local nameserver does not have the address in its cache or in a zone that it manages does it start resolving the name from behind, i.e. it prompts one of the root servers (the nameserver has a list of these in its configuration file) to give him the address of the nameserver responsible for the »de« domain. It sends the following request to the delivered address for the address of the nameserver responsible for »busch-jaeger.de«. It finally receives the desired information from latter server which it not only enters into its cache but forwards to the querying client computer as well (see Figure 6 for sequence). This sample query can be performed on the computer with the *nslookup* www.busch-jaeger.de console command (see Figure 7)

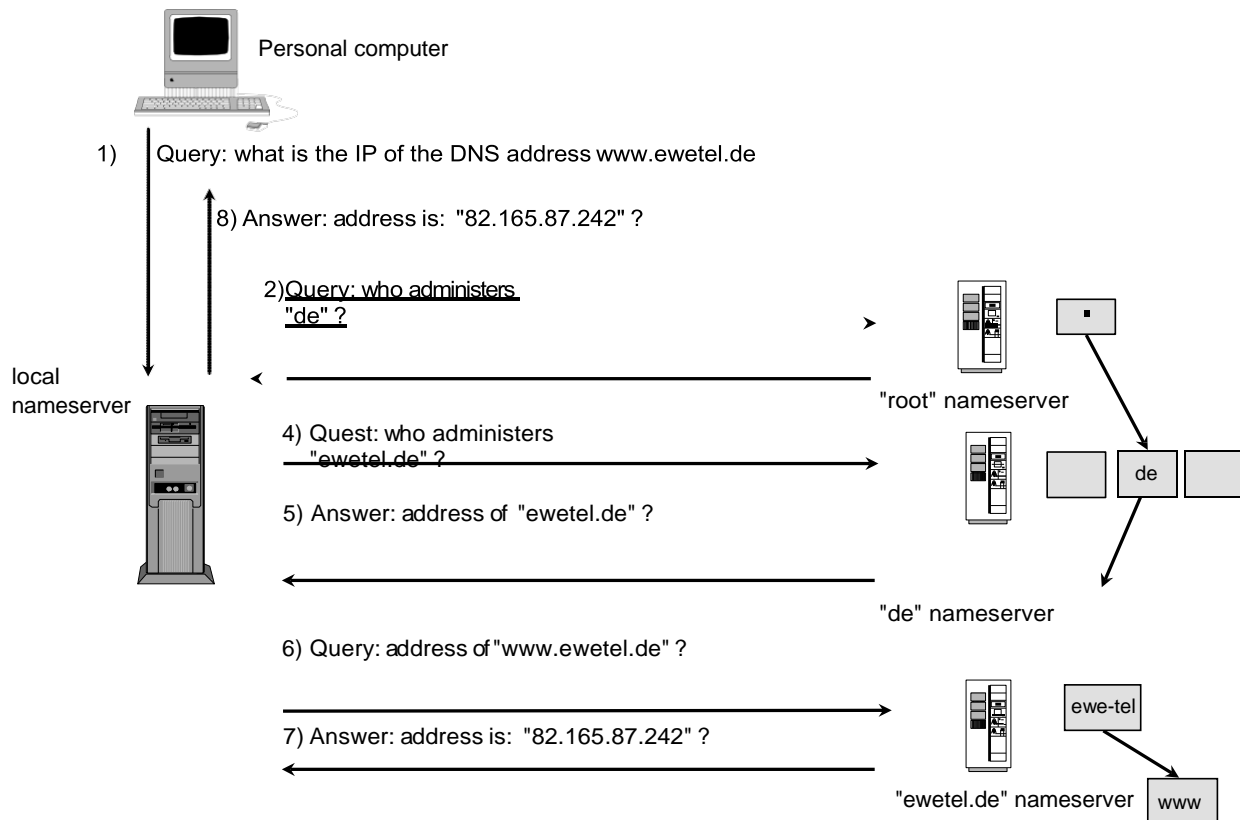


Figure 6 : general sequence of a DNS query

```

C:\WINDOWS\system32\cmd.exe
C:\Dokumente und Einstellungen\SCHM>nslookup www.busch-jaeger.de
Server: vdc1.bfe.net
Address: 192.168.50.1

Nicht autorisierte Antwort:
Name: www.busch-jaeger.de
Address: 129.35.205.133

C:\Dokumente und Einstellungen\SCHM>

```

Figure 7: name resolution with the *nslookup* console command

5.8 DNS address resolution - reverse lookup

A new domain, "in-addr.arpa" (**A**ddress and **R**outing **P**arameter **A**rea domain), was introduced for resolution in the opposite direction (address in name), the so-called *reverse lookup*. 256 subdomains (0..255) are available below this special domain. This subdivision repeats itself a total of 4 times until the 32-bit address is fully depicted. Figures 4 and 5 depict the reverse sequence for the Bfe-Oldenburg mail server.

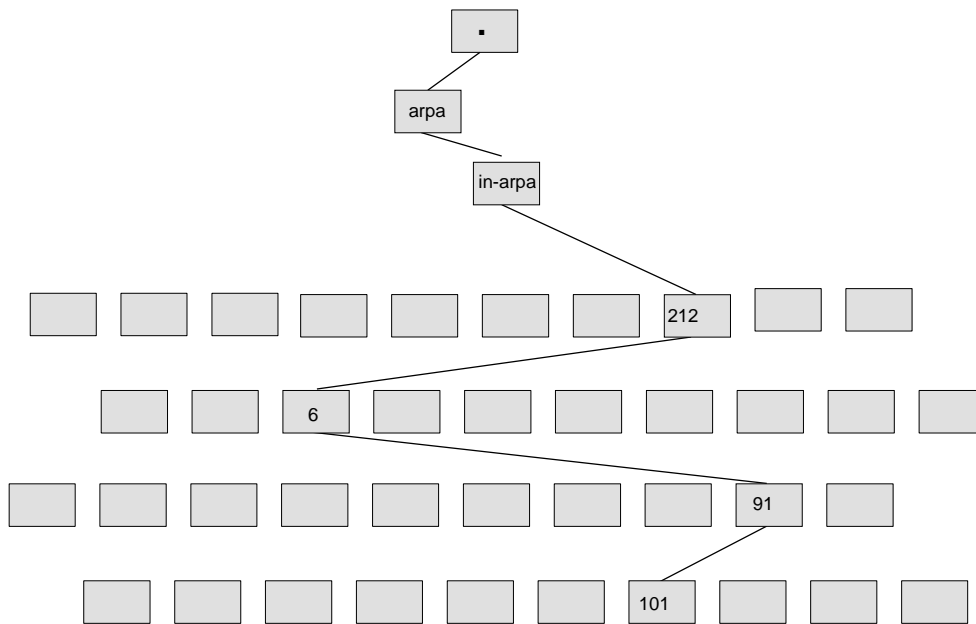


Figure 8: IP address reverse lookup sequence: 212.6.91.101

```
Auswählen Eingabeaufforderung
C:\>nslookup mailgate.bfe.de
*** Der Servername für die Adresse 192.168.1.251 konnte nicht gefunden werden:
Non-existent domain
*** Der Servername für die Adresse 192.168.1.251 konnte nicht gefunden werden:
Non-existent domain
*** Die Standardserver sind nicht verfügbar.
Server: Unknown
Address: 192.168.1.251

Nicht autorisierte Antwort:
Name: mailgate.bfe.de
Address: 212.6.91.101

C:\>nslookup 212.6.91.101
*** Der Servername für die Adresse 192.168.1.251 konnte nicht gefunden werden:
Non-existent domain
*** Der Servername für die Adresse 192.168.1.251 konnte nicht gefunden werden:
Non-existent domain
*** Die Standardserver sind nicht verfügbar.
Server: Unknown
Address: 192.168.1.251

Name: mailgate.bfe.de
Address: 212.6.91.101

C:\>
```

Figure 9: querying an IP address with the nslookup console command

5.9 History: name resolution in the beginning – over the file *hosts*

When the ARPANET (predecessor of the Internet) emerged, it was made up of a few hundred networked computers. The names of all computers, together with the corresponding IP address, were stored as tables in the *hosts* file. The file's content was managed centrally by the Stanford Research Institute's (SRI) **Network Information Center (NIC)**. The administrators sent changes to their subnets by e-mail to the NIC. It input any changes in the central *hosts* file and regularly made a current version of the *hosts* file available on a central computer. The local administrators could download the file and input it in their systems. This kind of data management had several disadvantages:

- The NIC had no influence on how names are allocated. It could happen at any time that a name was allocated twice.
- Management became more and more complex as the ARPANET grew.
- It was not possible to keep the *hosts* file current in the entire network.

To solve the problems, successors were sought where data management could be performed locally but where the data was globally accessible. In addition, the system should dynamically update itself to minimize any interference from the outside. The name space should be hierarchically arranged and guarantee unique names.

Today's **Domain Name Service** or the **Domain Name System (DNS)** emerged from it.

5.10 Summary

The Domain Name System (**DNS**) is a server-based structure for resolving names into IP addresses. The client who wants to resolve a DNS name into an IP address makes a request to the DNS server. The DNS server manages IP addresses and the associated names in a database. If a name is not included, it queries a higher-level DNS server until an IP address can be returned to the requesting client. The **Domain Name System (DNS)** is a distributed, hierarchical system for resolving computer names into IP addresses und vice-versa. DNS returns to the *hosts* file whose contents were used to resolve the name in the ARPANET (predecessor of the Ethernet).

DNS does not have a central database. Instead, the information is spread across many thousands of nameservers (**DNS servers**). The DNS database is a tree-like structure, divided into zones. It begins in the root directory.

6 TCP/IP configuration

Learning objectives:

- indicate which settings are required for a successful TCP/IP configuration
- perform dynamic and static TCP/IP configurations
- perform a TCP/IP configuration on devices with network interfaces
- know the operating system-specific tools for TCP/IP configuration
- know and use the tools for testing the TCP/IP configuration
- use terms like MAC address, IP address and port

After the necessary foundations for TCP/IP communication were laid in the previous chapters, we will now discuss the configuration steps and tools required to do so. TCP / IP configuration is described using the Windows XP/2000 and Ubuntu Linux operating systems as an example.

6.1 General information (short, condensed repetition)

In order for the individual devices to exchange data packages, they must be provided with addresses. Today, only IP addresses (Internet Protocol address) are used. Currently in its 4th version. In the future, the newer version (Version 6) will be more widely used. The 4 bytes of an IP_{v4} address are each separated by a period and stated in dot-decimal notation, e.g. 192.168.40.8. A complete IP address for accessing a web server in the Internet browser would be for example, *http:// 192.168.40.8:80* (the browsers excuse the omission of the last entry ":80"). This address is, similar to a real life company address, made up of 3 components.

- **net**, e.g. 192.168.40.0
comparable to a **street**, e.g. Isabella Street
- **node** or **host**, e.g. 0.0.0.8 = 8
comparable to a **house number** on a street, e.g. 8
- **port** or **service**, e.g. http (80)
comparable to a **company** in an office building, e.g. Helper tax advisors

Notes:

For network information, the node part is set to 0.

For node information, the network portion is set to 0, but the leading zeros of the network portion are omitted.

When entering an IP address on a PC, the **subnet mask** must also be specified. This is used to define the boundary between the network portion and the node portion. The 1s in the mask represent the network portion in the IP address while the 0s in the mask represent the node portion in the IP address.

Example 1 (short street with few houses = node):

192.168.40.8 with subnet mask 255.255.255.0 → network=192.168.40.0 and node=8

Example 2 (long street with many houses = nodes):

10.20.30.8 with subnet mask 255.0.0.0 → network=10.0.0.0 and node=20.30.8

Note:

The decimal 255 corresponds to the binary number 11111111_2 . Thus, 255.255.255.0 expressed in 1s and 0s is $11111111.11111111.11111111.00000000_2$.

A more modern and simpler IP address is becoming more common:

Example

1: 192.168.40.8 with subnet mask 255.255.255.0 = **192.168.40.8/24**

Example

2: 10.20.30.8 with subnet mask 255.0.0.0 = **10.20.30.8/8**

When counted from the left, the number behind the slash indicates the number of bits that belong to the network portion. Thus, in Example 1, the first 3 bytes belong to the network and thus $3 \times 8 = 24$. In Example 2, only the first byte is network, which is why $1 \times 8 = 8$ is indicated behind the slash.

The **port** or **service** identifies the process or the running application on the client or server PC. Thus, a web process (e.g. Firefox browser) and an e-mail process (e.g. Thunderbird client) could run simultaneously on a PC for example. Both services are accessed with the same IP address, but they can be differentiated by the ports - 80 for the web process and 25 for the e-mail process. The port specification is attached to the IP address using a colon. An example of the complete specification of a service, e.g. in the browser, would then be 192.168.40.8:80. The **ports** for the most important services are standardized and can be viewed under <http://www.iana.org/assignments/port-numbers> or the `/etc` directory of the operating systems (File: `/etc/services`). For special purposes, a different port from the standard can be selected for a service. However, the condition is that the client and server must use the same port.

The discussed IP addresses are called **software addresses** or **logical addresses** and must be configured by the network administrator for every device. Alternatively, the administrator can ensure that the IP addresses are automatically assigned by a central service via the DHCP server to the other network devices (DHCP method). Nowadays, the DHCP server is usually integrated in the DSL router and already activated by default.

Moreover, every device with a network interface - be it the network card in your PC, the network printer, the DSL router, Wi-Fi access point, Wi-Fi adapter or even a Bluetooth device - has a **hardware or physical address** which is "burned into it" during manufacture and therefore does not have to be configured by the administrator as well. The manufacturers make sure that these so-called **MAC addresses** are unique worldwide. The **MAC address** is expressed in hexadecimal numbers and is often printed on the device. Example of a **MAC address**: 00-19-B9-52-ED-AA. The current Windows PC addresses are displayed in the input prompt with the command ***ipconfig*** or in more detail with ***ipconfig /all***. The corresponding command under Linux is ***ifconfig***.

6.2 Required settings

The following settings are required for TCP/IP communication:

- IP address
- subnet mask
- router (default gateway)
- DNS server

Settings on the computer

- Pro Interface
 - IP address
 - netmask

- Pro Computer
 - router (default gateway)
 - DNS server
- or DHCP (Dynamic Host Configuration Protocol)
 - then does this itself

TCP/IP must be configured on a workstation using operating system tools. The approach is largely identical for Windows and Ubuntu Linux operating systems.

6.3 Configuration

6.3.1 Configuration for Windows

Start → Programs → Control panel → Network connections → LAN connection context → Properties

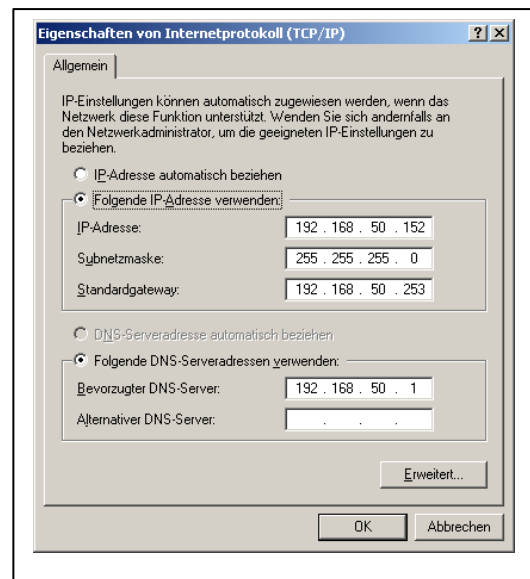
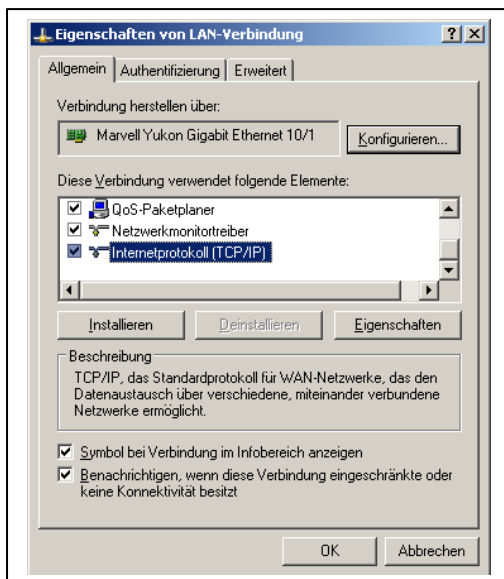


Figure 1: Windows properties of a LAN card Figure 2: Windows TCP/IP configuration

Tip:

The "Show icon in taskbar notification area when connected" checkbox and the checkbox below it always provide an overview of the current status of the LAN connection (default for Vista).

6.3.2 Configuration on Ubuntu-Linux

System → System administration → Network

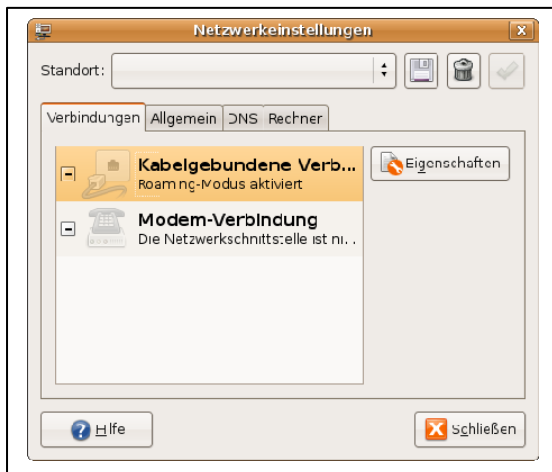


Figure 3: Ubuntu network settings 1

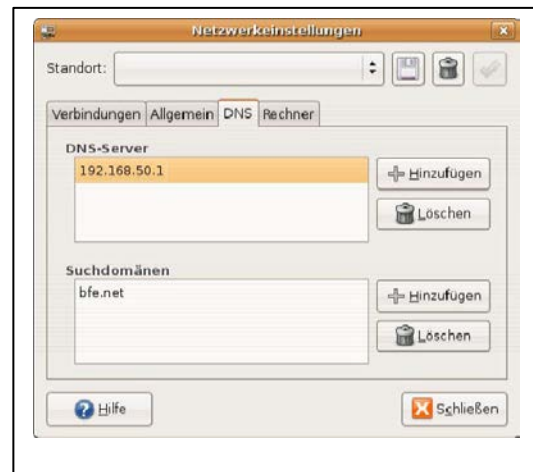


Figure 4: Ubuntu network settings 2



Figure 5: Ubuntu TCP/IP configuration

6.3.3 Requesting a new IP address from the DHCP server

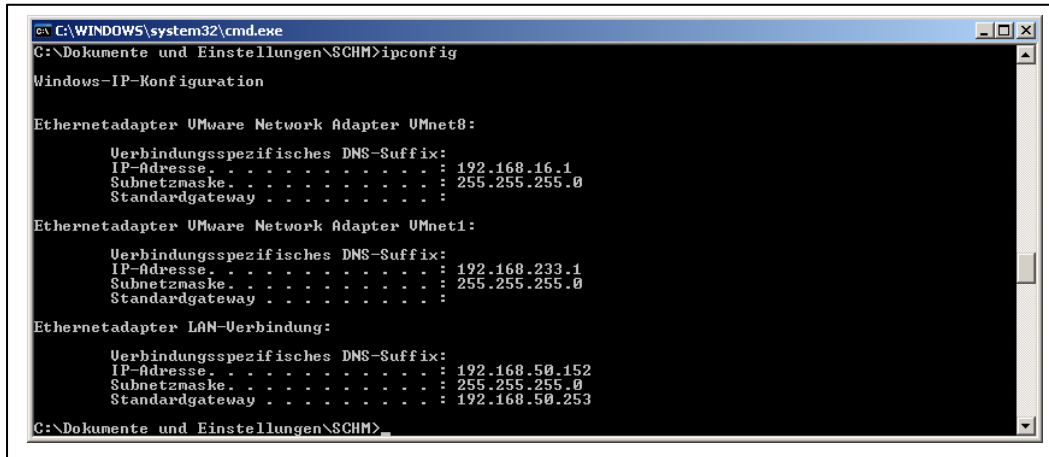
Per console commands

Windows (with administrator rights)	Ubuntu-Linux
<code>ipconfig /release</code>	<code>sudo /etc/init.d/networking restart</code>
<code>ipconfig /renew</code>	

6.4 Identifying and showing the current configuration

6.4.1 Displaying the current TCP/IP configuration under Windows

ipconfig



```
C:\WINDOWS\system32\cmd.exe
C:\Dokumente und Einstellungen\SCHM>ipconfig

Windows-IP-Konfiguration

Ethernetadapter VMware Network Adapter VMnet8:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.16.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter VMware Network Adapter VMnet1:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.233.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

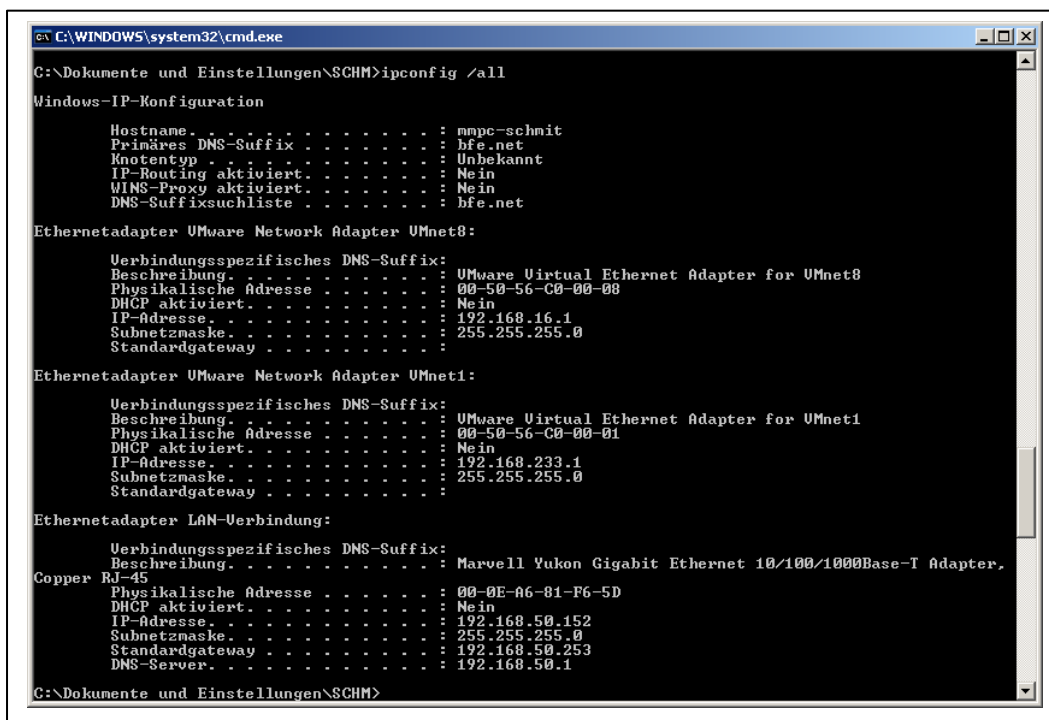
Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.50.152
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.50.253

C:\Dokumente und Einstellungen\SCHM>
```

Figure 6: displaying the IP configuration with ipconfig

ipconfig /all



```
C:\WINDOWS\system32\cmd.exe
C:\Dokumente und Einstellungen\SCHM>ipconfig /all

Windows-IP-Konfiguration

    Hostname. . . . . : mmpe-schmit
    Primäres DNS-Suffix . . . . . : bfe.net
    Knotentyp . . . . . : Unbekannt
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein
    DNS-Suffixsuchliste . . . . . : bfe.net

Ethernetadapter VMware Network Adapter VMnet8:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : VMware Virtual Ethernet Adapter for VMnet8
    Physikalische Adresse . . . . . : 00-50-56-C0-00-00
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.16.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter VMware Network Adapter VMnet1:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : VMware Virtual Ethernet Adapter for VMnet1
    Physikalische Adresse . . . . . : 00-50-56-C0-00-01
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.233.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Marvell Yukon Gigabit Ethernet 10/100/1000Base-T Adapter,
Copper RJ-45
    Physikalische Adresse . . . . . : 00-0E-A6-81-F6-5D
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.50.152
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.50.253
    DNS-Server. . . . . : 192.168.50.1

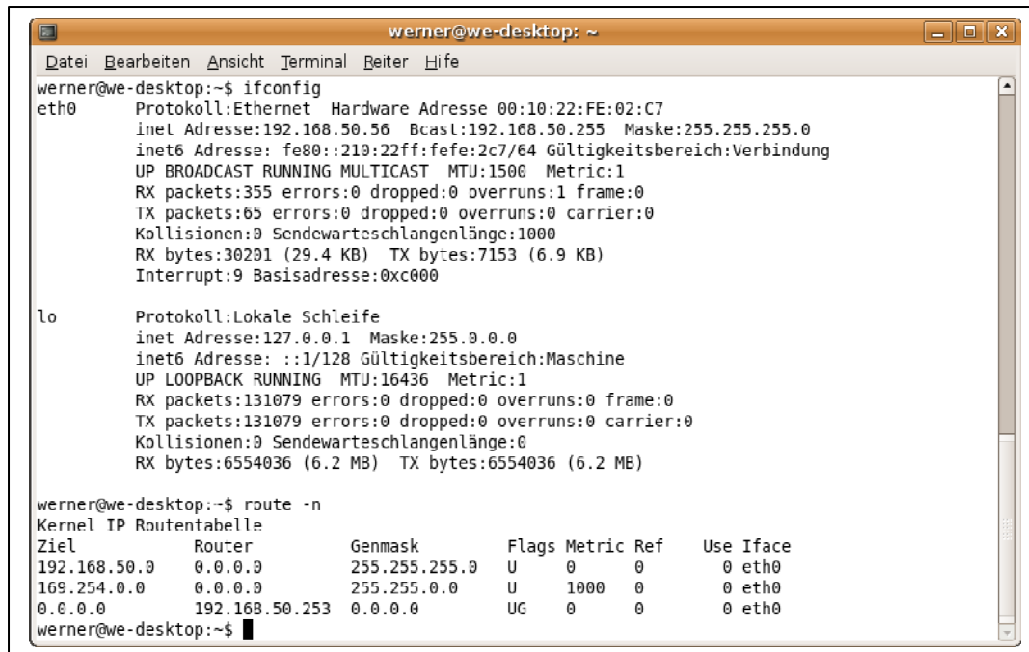
C:\Dokumente und Einstellungen\SCHM>
```

Figure 7: displaying a more detailed TCP/IP configuration with *ipconfig /all*

Displaying current TCP/IP configuration under Ubuntu-Linux

Either using the console commands

ifconfig and *route -n*



```
werner@we-desktop: ~  
Datei Bearbeiten Ansicht Terminal Reiter Hilfe  
werner@we-desktop:~$ ifconfig  
eth0      Protokoll:Ethernet  Hardware Adresse 00:10:22:FE:02:C7  
          inet Adresse:192.168.50.56  Bcast:192.168.50.255  Maske:255.255.255.0  
          inet6 Adresse: fe80::210:22ff:fefe:2c7/64  Gültigkeitsbereich:Verbindung  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:355 errors:0 dropped:0 overruns:1 frame:0  
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0  
          Kollisionen:0 Sendewarteschlangenlänge:1000  
          RX bytes:30291 (29.4 KB)  TX bytes:7153 (6.9 KB)  
          Interrupt:9 Basisadresse:0xc000  
  
lo        Protokoll:Lokale Schleife  
          inet Adresse:127.0.0.1  Maske:255.0.0.0  
          inet6 Adresse: ::1/128  Gültigkeitsbereich:Maschine  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:131079 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:131079 errors:0 dropped:0 overruns:0 carrier:0  
          Kollisionen:0 Sendewarteschlangenlänge:0  
          RX bytes:6554036 (6.2 MB)  TX bytes:6554036 (6.2 MB)  
  
werner@we-desktop:~$ route -n  
Kernel IP Routentabelle  
Ziel          Router          Genmask         Flags Metric Ref    Use Iface  
192.168.50.0  0.0.0.0         255.255.255.0  U        0      0        0 eth0  
169.254.0.0   0.0.0.0         255.255.0.0    U       1000    0        0 eth0  
0.0.0.0       192.168.50.253  0.0.0.0        UC        0      0        0 eth0  
werner@we-desktop:~$
```

Figure 9: displaying the TCP/IP configuration for Ubuntu

Ubuntu offers its own network diagnostic tool. This also lets you display the configuration parameters.

System → *System administration* → *Network diagnostics*

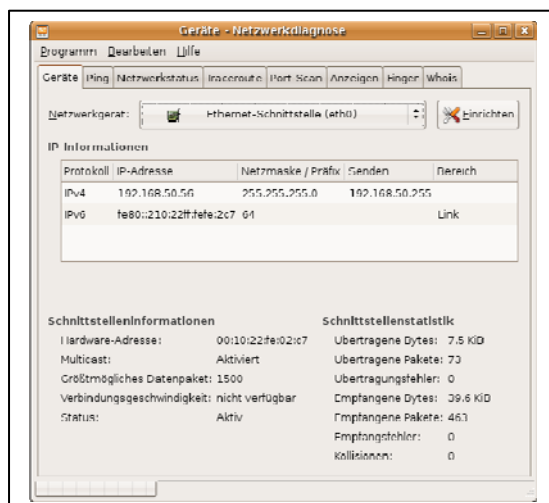


Figure 10: displaying the TCP/IP configuration using the supplied network diagnostics tool

6.5 Testing connectivity with *ping*

Network connectivity can be tested with the *ping* command. *ping* is a simple program that checks whether a specific IP address is available and can receive requests. The acronym "ping" stands for **P**acket **I**nternet or **P**acket **I**nter-**N**etwork **G**roper. The name was invented after the description a submarine crew uses for the sounds of sonar pulse reflected by an underwater object.

The *ping* command sends specific IP packets, so-called ICMP echo requests (**I**nternet **C**ontrol **M**essage **P**rotocol) to a specified destination. Each sent packet is a request for an answer. The response given to a *ping* command includes the success ratio and the round trip time to the destination.

You can use this information to determine whether a connection to the destination is possible. The ping command checks the network card's send and receive function, TCP/IP configuration and network connectivity.

The following types of *ping* commands are possible:

- *ping 127.0.0.1*
 - This is a clear *ping* command that is called an internal **loopback test**. This checks the TCP/IP configuration.
- *ping IP address of the host computer*
 - A *ping* command sent to a host PC checks the TCP/IP address configured for the local host and the connectivity with the host.
- *ping IP address of the default gateway*
 - A *ping* command sent to the default gateway indicates whether the router connecting the local network to other networks can be reached.
- *ping IP address of the remote destination*
 - A *ping* command sent to a remote destination is used to check the connection to a remote host.

7 Wireless LAN (Wi-Fi)

Wireless LAN = wireless network = Radio LAN = radio network

Learning objectives:

- get an overview of Wi-Fis
- classify the many concepts in the Wi-Fi environment
- classify important Wi-Fi standards
- basically configure the Wi-Fi access point
- basically configure Wi-Fi adapters
- identify the security limits of Wi-Fi technologies

7.1 General information

- **Radio LAN standards**
 - Radio networks are standardized
 - IEEE 802.11b, IEEE 802.11g soon also IEEE 802.11n
- **Structures**
 - Radio base stations, **Wi-Fi base station (access points, APs)**
 - Computer with radio Wi-Fi adapters
 - possible additional antennas
 - Shared Media Network as with classical Ethernet



Figure 1: Wi-Fi access point as shown by Figure 2: Wi-Fi router using the example of T-Com Speedport W 100XR AVM Fritz!Box Fon 7170

- **Ranges**
 - In the building: strongly based on the building, approx. 20 – 40 m
 - For antennas >10dbi gain up to 10 km
 - in open terrain: approx. 200 – 400 m
 - The transmission/reception quality is significantly dependent on...
 - ... the local environment (buildings)
 - ... the antenna design
 - ... antenna cable/length, plug, etc.
 - ... interferences with other radio networks
 - ... unobstructed view (you cannot hope for favorable reflections)
- **Transmission performance**
 - is based on the respective standard, for example with IEEE 802.11.g
 - gross 54 MBit/s
 - net approx. 25 MBit/s
- **Security in the wireless LAN**
 - Eavesdropping is easily possible due to the structure
 - The network does not end at the building boundary
 - **Data encryption is required**
- **Actual state**
 - Today, notebooks normally have an Wi-Fi interface ex-works.
 - Many routers contain a **Wi-Fi base station (AP, access point)**
 - Currently, Wi-Fi devices, which transmit according to a draft for the new 802.11n standard.
 - Wi-Fi is always threatened by interference and drops in throughput from other wireless networks. The same applies to power lines from interrupters in the power grid
- **On configuring wireless LANs**
 - Many new terms: SSID, WEP, WPA(2), TKIP, AES, EAP, etc.
 - Some basic knowledge is required to configure Wi-Fi

Wi-Fi advantages

- Mobility
example
:
 - Telephone: wireless Internet telephone
 - Notebook: "surfing" from your sofa without a cable
- No cabling required

Power over Ethernet

Power can also be supplied to the Wi-Fi components over the LAN cable so that no additional cable must be laid for the power supply. This is called **Power over Ethernet (PoE)** and is regulated in the 803.3af standard. Supplying the WLAN access points via Power over Ethernet has become commonplace, particularly in the professional environment. The maximum power consumption is 15.5 watts in the default setting. Special switches, so-called **PoE switches**, are also required.

Theoretical basics:

Source: Partially taken from the "Wireless LAN" manual from Fujitsu-Siemens (440-N00558-Muli1.pdf)

7.1.1 Radio network according to the IEEE 802.11 standard

IEEE 802.11a	5.0 GHz bandwidth	54 MBit/s ☒ are not used with our Wi-Fi devices
IEEE 802.11b IEEE 802.11g (currently)	2.4 GHz bandwidth 2.4 GHz bandwidth	11 MBit/s Gross: 54 MBit/s → real throughput with a good connection: 25 MBit/s Enough for fast DSL transmission (DSL 16000)
IEEE 802.11n (Draft 2.0)	2.4 GHz bandwidth 5 GHz bandwidth	Gross: 144 MBit/s to 300 MBit/s → uses several antennas → real throughput up to 120 MBit/s → approx. 5x faster than the current standard (under optimum conditions)

Figure 3: radio network according to the IEEE 802.11 standard

The standard not only describes modulation and data framing, it also contains an authentication and encryption method called **Wired Equivalent Privacy (WEP)**.

The IEEE standard offers **two operating modes**,

- **ad hoc mode** (peer-to-peer) and
- **infrastructure mode**.

Where does the gross/net difference for Wi-Fi come from?

Transmission on the radio channel happens according to a time-controlled protocol: the data packets on the medium run, actually sometimes at 54 Mbit/s, but because they are interrupted by controlling breaks, the effective throughput is always significantly lower. In case of a poor wireless connection, it can sometimes goes down to 1 or 2 MBit/s. However, the throughput is normally enough to push even a DSL 6000 connection to the limit.

7.1.2 The operating mode: ad hoc mode

A wireless LAN in **ad hoc mode**, also known as peer-to-peer mode, consists of a single-terminated radio cell. Ad hoc radio networks are created when a work group forms, together with its systems, and would like to connect them for data exchange. Systems can be added to an ad hoc radio network as required and leave it again. A unique **network name**, the **SSID** (Service Set Identifier), is available to prevent several ad hoc networks from interfering with each other in radio traffic. The **SSID** is used for addressing so that a data packet can always be assigned to a specific radio cell.

If you want to dial into an existing wireless network, you need the **network name (SSID)** that you enter in the settings for the network card. The network card then searches for a wireless network with this **SSID** at startup. Once the network card has found a wireless network, it will plug into it and you will be able to communicate with the systems in this wireless network. **If two radio cells are very close together, then the radio channels on these networks should be 4 to 5 channels apart.** This applies to the standards IEEE 802.11b, 802.11g and 802.11n.

7.1.3 The operating mode: infrastructure mode

Infrastructure mode not only has mobile stations but a base station as well called the access point. The **access point** assumes the function of a "guardian." **In contrast to ad-hoc mode, each system must log on to the access point before it can exchange data in the radio cell.**

Another **access point** task is to connect the radio cell to a wire-bound Ethernet. Since the **access point** knows exactly which stations are available on the radio side because these are forced to login, it can decide exactly which data must be passed through and which are not. This is known as **bridging**.

Several **access points** with the same **SSID** can be used in order to increase the range of a wireless network.

When a system enters the wireless network, it searches for the access point with the strongest signal among all the accessible **access points** and logs on there. Two systems that are registered at different access points, communicate with each other this way, even if they are not directly within range. When a system also continuously monitors the radio situation even after having logged on, it can detect how the signals grow weaker from one **access point** and grow stronger from another access point, and are handed over in a way that is imperceptible to the user. This is known as **roaming**.

7.1.4 Network security in the radio network

Since the advent of radio networks, security has played a much more critical role than before for the simple reason that it is easier for attackers to tap these connections. In the case of wired networks, most companies can secure the protection of their networks with devices. An attacker would have to gain entry into the company premises in order to log into the LAN and eavesdrop on the network traffic.

All you need to spy on data in the wireless network is a computer with a wireless network card and a suitable location outdoors in the parking lot or in the office next door.

A few prerequisites for secure networking are described below:

- A user must be authenticated by the network before they are granted access to secure the network against intruders.
- The network must be authenticated by the user before allowing his computer to connect to the network. This prevents a radio device from passing itself off as a legitimate network and obtaining access to the user's computer.
- Mutual authentication between user and network must be protected cryptographically. This ensures that you are exactly connected to the desired network and not the wrong one.
- The wireless connection between a computer and the **access point** must be encrypted in such a way that intruders cannot access data that is considered confidential.

Two basic mechanisms are available for this type of secure encryption:

- One method is called the **WEP key**, with preconfigured secret data. WEP keys keep unauthorized users away from the wireless network and encrypt the data of legitimate users.
- The second method is **authentication with the help of an 802.1x protocol**. A variety of underlying authentication protocols are thereby used for access control to the network. The most powerful protocols can secure mutual authentication of users and the network, and can dynamically generate keys to encrypt radio data.

Wired Equivalent Privacy (WEP) with preconfigured keys

Preconfigured **WEP keys (Wired Equivalent Privacy)** are used to assign the same secret key to the client computer and the **access point**. This key is used to encrypt data exchanged between the computer and the **access point**. The WEP key can also be used to authenticate the client computer on the **access point**. If the computer cannot prove that it knows the WEP key, it is denied access to the network.

- If the **access point** demands a WEP key for authentication, you must then assign it to the **access point** in **shared mode**. Set the allocation mode in the Network Properties.
- If the **access point** does not require a WEP key for authentication, this is then known as **open mode**. Set the allocation mode in the Network Properties.

7.1.4.2 Wi-Fi Protected Access (WPA) and TKIP encryption

As an extension to the 802.11 standard, Wi-Fi Protected Access (WPA) includes a set of security extensions beyond **Wired Equivalent Privacy**.

WPA contains the **WEP** architecture, but offers additional protection through dynamic keys based on the **Temporal Key Integrity Protocol (TKIP)**, and offers **Pre-Shared Keys (PSK)** or **Extensible Authentication Protocol (EAP)** via IEEE 802.1x for user authentication.

Like **WEP**, **TKIP** uses the RC4 algorithm for encryption. The key changes temporarily - hence the name of the protocol.

PSK ("previously shared key") generally refers to an encryption method where the keys must be known to both parties prior to communication, i.e. a symmetric method.

7.1.4.3 Wi-Fi Protected Access 2 (WPA2) and AES encryption

Wi-Fi Protected Access 2 (WPA2) and **AES** encryption are the implementation of a security standard for wireless networks according to the Wi-Fi standards IEEE 802.11a, b, g, n and is based on the Advanced Encryption Standard (AES). It is the

successor to WPA.

Encryption takes place according to the **Advanced Encryption Standard (AES)**.

Both a secret text, the "**pre-shared key**" and a RADIUS server can be used (**EAP authentication**) to authenticate the client at the **access point** and vice-versa.

Authentication with a **pre-shared key** is often used for small installations, for example **in homes**. This version is also called "Personal."

In larger networks, RADIUS permits central user administration incl. accounting. In this case, the **access point** forwards the client's authentication request to the RADIUS server and – depending on the success – permits access.

This version of WPA2 is often called "Enterprise."

Note: **WPA**-enabled devices usually cannot be brought up to the WPA2 standard by a firmware update. That's why you must replace your entire Wi-Fi hardware for WPA2 hardware in order to be able to use this standard.

7.1.4.4 The 802.1x standard

The IEEE 802.1x protocol permits authenticated access to a LAN. This standard applies to both wireless and wired networks. 802.1x authentication occurs for a wireless network after 802.11 allocation has occurred. Wired networks use the 802.1x standard without 802.11 allocation.

The **WEP protocol**, which uses preconfigured keys, has several weaknesses in terms of basic administration and security. In order to solve these problems, IEEE has introduced another standard: 802.1x. 802.1x provides better security than the preconfigured WEP keys and is easy to use, particularly in large networks.

When using preconfigured WEP keys, the wireless client computer is authenticated to the network. With 802.1x, the user is authenticated to the network with the credentials (password, certificate or token card). Authentication is not performed by the **access point**, but by a central server. If this server uses the RADIUS protocol, it is called a RADIUS server.

With 802.1x, a user can log into the network from any computer, and many **access points** can share a single RADIUS server for authentication. This makes it much simpler for the network administrator to control access to the network.

7.1.5 Extensible Authentication Protocol (EAP)

802.1x uses the protocol called **EAP** (Extensible Authentication Protocol) to authenticate the client to the server. **EAP** is not an authentication mechanism per se, but a common framework for transporting current authentication protocols. The advantage of the EAP protocol is that the basic EAP mechanism does not need to be changed when developing new authentication protocols.

7.1.6 Wireless Distribution System (WDS)

- It is used to extend the Wi-Fi range
- Application: DSL Internet access is not possible everywhere in the building with one Wi-Fi router
- Makes sense for larger houses and apartments

Wi-Fi problems are often range-related problems. Sometimes, a good router location is just not sufficient to receive the **Wi-Fi** where it is needed. It can best be extended via **WDS** (Wireless Distribution System). By setting up a **WDS repeater** as an additional **Wi-Fi base station**, it is possible to extend the covered range. A router or **access point** (in Figure 3, WDS router 2) picks up the Wi-Fi signal and forwards it. However, this increase in range costs bandwidth: the access point must be connected to the network and the client simultaneously via Wi-Fi. This halves the payload data rate. However, WDS is sufficient to make DSL Internet access available over a long distance for example.

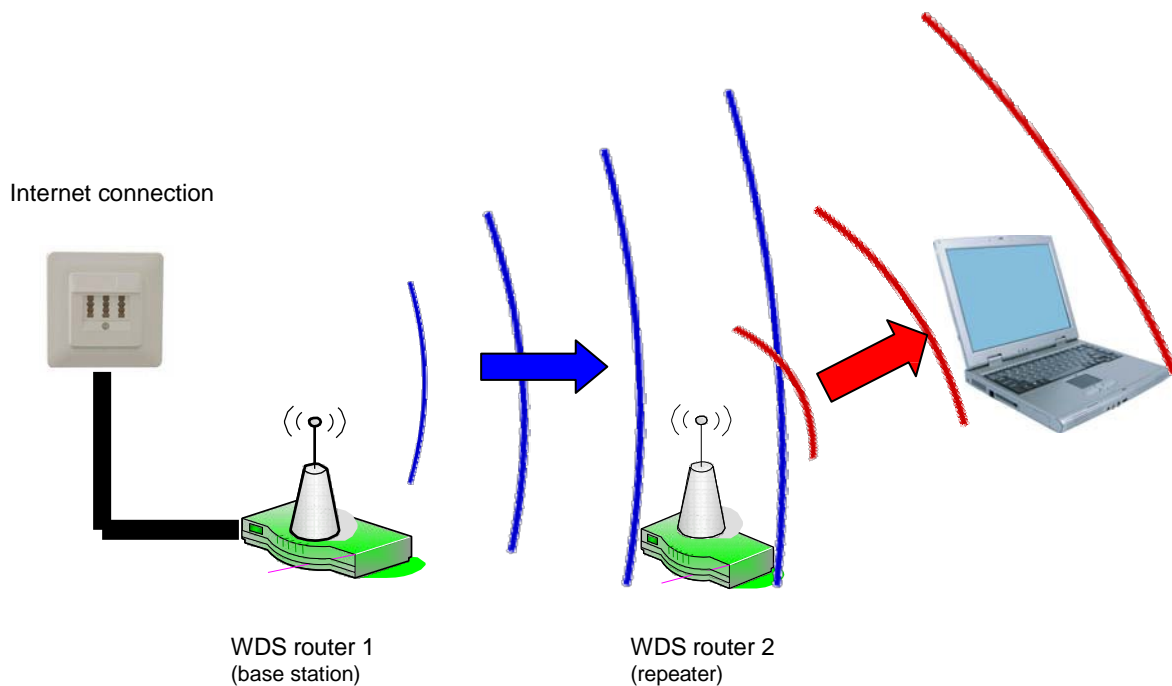


Figure 4: Wi-Fi can easily be extended for WDS-compatible routers – unfortunately at the expense of the data rate

In **WDS** mode, base stations pass data to others on the same radio channel. It is important that **WDS** also works with secure WPA encryption. Unfortunately, most manufacturers are silent about this on the cardboard box or in the manual. **WDS** usually only works with **WPA** when the **base station** and **repeater** are from the same manufacturer because there is no standard for this feature combination. The major drawback of **WDS** is that the usable data rate on the radio channel is at least halved because each data packet is sent twice.

Alternative to extending the range: connect the access point to the router via a cable
→ full bandwidth

Another option, where the usable data rate is not reduced, is to connect the second base station to the home network via another medium – cable, Powerline or fiber optic cable. **The access points thereby use the same radio network names, but clearly different radio channels, for example 1 and 11, so that they don't get mixed up.** The disadvantage here: interruption-free handover of the client – when you're moving about with your laptop for example – is not possible. Although the latest computers may be able to connect to the new radio cell without a problem, ongoing data transmissions are nevertheless interrupted. Since the signal is transmitted via Ethernet, the usable data rate does not decrease with this type of Wi-Fi extension.

If you want everything, that is, full speed as well as a seamless and uninterrupted connection, then you need professional routers that can handle WLAN roaming and are much more expensive than standard routers (starting at € 400 as of early 2008).

7.2 Practical application

Security: encryption methods for Wi-Fi

- The current secure encryption method is **WPA** (Wi-Fi Protected Access, also **WPA2**)
- **WPA** and **WPA2** differ in their preferred encryption algorithm, but not in terms of security, provided you select an unguessable password.
- Insecure encryption method **WEP**
WEP is outdated because its encryption can be cracked within minutes.
- **Wi-Fi base stations** today usually use the secure **WPA** or **WPA2** encryption methods.
- However, not all **Wi-Fi subscribers** can work with these (e.g. MP3 streaming clients). Problem: if you want to use them, you have to switch the Wi-Fi base station back to **WEP** even if all the other Wi-Fi devices can work with **WPA**.
→ Tip: do not use pure **WEP** devices

Dispensable security

- **Hiding the Wi-Fi name (disable SSID broadcasting) SSID = Service Set Identify**
Windows XP conceals hidden **Wi-Fi networks** and their channel so you cannot tell which neighbor you have to settle with regarding overlapping and thus interference-free radio channel coverage.

→ provokes connection problems
- **Address filter (MAC - Access Control List, MAC-ACL)**
The filter for the **MAC addresses** of the **Wi-Fi cards** can be easily circumvented: a "radio snooper" can easily sniff out the used addresses with a tool like *Kismet* and enter it into his Wi-Fi driver.

→ only provides false protection

Terms (important for configuration)

SSID	<p>Service Set Identifier = network name</p> <p>Each radio network has its own name. You can select the wireless network by its name.</p> <p>Network names permit the simultaneous operation of different wireless networks in the same environment without interfering with each other. The network name is a sequence of 32 characters, which is case-sensitive.</p>
WEP	Wired Equivalent Privacy
WPA	<p>Wi-Fi Protected Access</p> <p>As an extension to the 802.11 standard, Wi-Fi Protected Access (WPA) includes a set of security add-ons beyond Wired Equivalent Privacy (WEP)</p>
WPA-TKIP	<p>WPA includes the WEP architecture, but offers additional protection from dynamic keys based on the Temporal Key Integrity Protocol (TKIP), and offers pre-shared keys (PSK) or the Extensible Authentication Protocol (EAP) via IEEE 802.1x for user authentication.</p> <p>Like WEP, TKIP uses the RC4 algorithm for encryption. The key changes temporarily - hence the name of the protocol.</p>
PSK	<p>Pre-shared key</p> <p>PSK ("pre-shared key") is a general description for an encryption method where the keys must be known to both subscribers before communication, i.e. a symmetrical method.</p>
EAP	<p>Extensible Authentication Protocol</p> <p>802.1x uses the protocol called EAP (Extensible Authentication Protocol) to authenticate the client to the server.</p>
WPA2 and AES	<p>Wi-Fi Protected Access 2 (WPA2) and AES encryption are the implementation of a security standard for wireless networks according to the Wi-Fi standards IEEE 802.11a, b, g, n and are based on the Advanced Encryption Standard (AES). It is the successor to WPA.</p> <p>Encryption takes place according to the Advanced Encryption Standard (AES).</p> <p>Both a secret text, the "pre-shared key" and a RADIUS server can be used (EAP authentication) to authenticate the client at the access point and vice-versa.</p>
WDS	<p>Wireless Distribution System</p> <p>In WDS mode, base stations forward data for others on the same radio channel.</p>

7.3 Setting up Wi-Fi

- Simply select **WPA as encryption** (**TKIP** and **AES** are equally good) and enter a good password (pre-shared key, **PSK**). The password may be a bit longer and more complicated since you have to enter it only once anyway at the first contact between the Wi-Fi base and PC.
- Keep **SSID broadcast** active
For Microsoft operating systems to create a seamless connection, "SSID broadcast" should remain active. Contact details such as an e-mail address or telephone number are particularly suitable as the network name (SSID). This is how the neighbors can easily report when their WLAN collides with yours or guests ask for Internet access.
- Specifying the **radio channel**



Figure 5: basic settings for the Wi-Fi base station on the Fritz!Box 7170



Figure 6: configuring security settings for the Wi-Fi base station on the Fritz!Box 7170

8 HTTP (Hypertext Transfer Protocol)

Learning objectives:

- classify the HTTP protocol in the network model as the application protocol
- understand the structure of the Uniform Resource Locator (URL)
- understand client/server communication of the HTTP protocol
- recognize the importance of the HTTP protocol for configuring devices with the network interface
- Understand and use the term "plug-ins"

8.1 The World Wide Web (WWW)

Besides **e-mail**, the **World Wide Web (WWW)** is the most commonly used service of the Internet. The **WWW** uses a software application called a **web browser** to retrieve information as a text, picture, video and audio. The information is shown in the browser in the HTML (Hypertext Markup Language) format. HTML is a description language for creating cross-platform documents. The **Hypertext Transport Protocol (HTTP)** is used for transferring files.

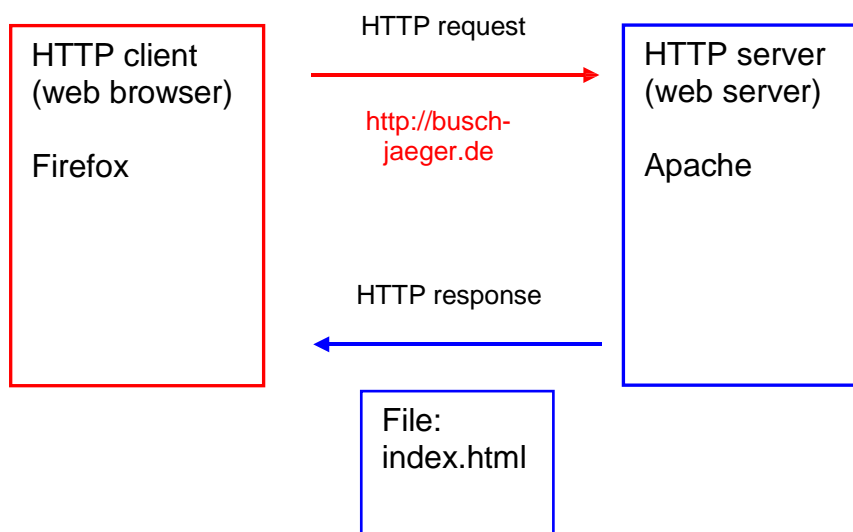


Figure 1: communication between web server and web browser

The transfer takes place based on the client-server principle. The **HTTP client (web browser)** sends its query to the **HTTP server (web server)**. This processes the query and sends its response back. This communication between the client and server takes place on the basis of messages in text format. The messages are usually processed via **TCP** on **Port 80**. The messages are called **request** and **response** and consist of a **header** and the data. The header contains control-related information. The data corresponds to an HTML file that the server sends to the client or the entries in an HTML form that the client sends to the server.

8.2 HTTP addressing

In its request, the **HTTP client** addresses a file that must be located on the **HTTP server**. To do this, the HTTP client sends a **Uniform Resource Locator (URL)** to the **HTTP server**:

<http://Servername.Domainname.TopLevelDomain:Port/Path/File>

Example:

<http://iliass.bfe.de:80/bfeintern/index.html>

The **port** information is optional and only required if the connection is made via a different port than the **default port 80**. Paths and files are separated by the slash "/" and from the server address. If no additional path or file specification follows, the server sends the default file of the domain. Depending on the configuration, this is either the **index.html** or **index.php** file. If the path and/or file have been specified, the **HTTP server** then returns this file. If this file does not exist, it will then try an alternative. If there isn't one, the default error page (Error 404) is sent to the HTTP client.

8.3 HTTP client (web browser)

The **WWW** user can choose between various **web browsers**. Some products are also available across several platforms.

- Firefox (open source → Linux, Windows)
- Internet Explorer (proprietary → Windows only)
- Opera (open source → Windows, Linux)
- Safari (proprietary → MacOS only)
- Lynx (text-based, open source → Linux)

Plug-ins:

To display files in special or manufacturer-specific formats that a normal web browser cannot display, the browser must be configured for **plug-in applications**, so called **plug-ins**. Using these applications, the browser can then call up the programs required for the special files. These include, for example:

- **Flash** – plays back multimedia files created with Macromedia Flash
- **Quicktime** – plays back video files created by Apple
- **Real Player** – plays back audio files

8.4 HTTP server (web server)

Well-known **web servers** are:

- Apache (open source, various platforms)
- Internet Information Server (Microsoft only)

Many devices from the field of automation technology can now be configured with a **web browser** or current status data can be retrieved with the **web browser**. The prerequisite for this is, of course, an implemented, running **web server**. For devices with a network interface, such as an IP camera, these are often server programs programmed in Java.

The **web servers** usually listen on **port 80**. You can find deviations in the product documentation.

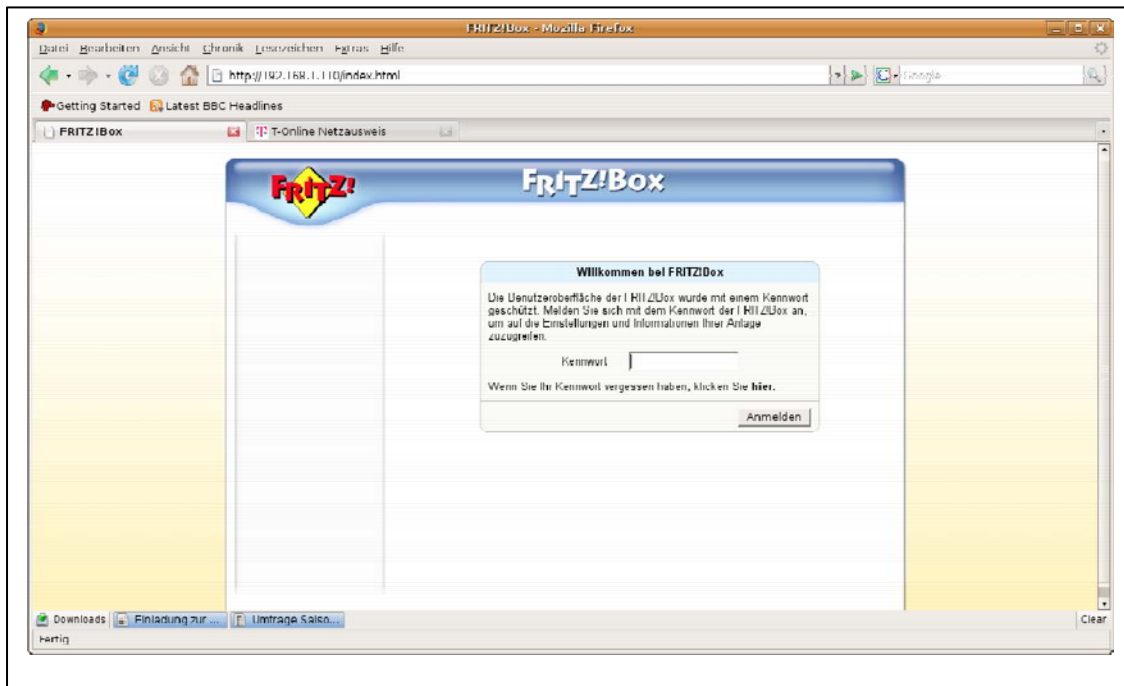


Figure 2: a small web server usually runs on the DSL router as well

9 e-mail

Learning objectives:

- obtain basic knowledge on configuring an e-mail client
- classify the terms SMTP, POP3 and IMAP

Electronic mail, **e-mail** for short, is one of the most frequently used services on the Internet. Corporate communication is no longer conceivable without **e-mail**. Text messages and files are sent from a sender to a recipient via e-mail. Sending and receiving an **e-mail** usually only takes a few minutes, regardless if the recipient is in the office next door or overseas.

Sending a message via **e-mail** is faster and cheaper than the traditional postal mail or fax transmission. Moreover, an e-mail can be made visually appealing with **HTML** so that text markups, color and the use of (background) images, for example, are possible. Documents, images, video or audio files can be sent as an attachment to an e-mail.

In professional and private life, more and more people are taking advantage of this form of information and data exchange for worldwide communication.

9.1 e-mail basics

Sending messages via networks to one or more people is called **e-mail (electronic mail)**. The messages usually consist of pure text. However, you can also attach files of other formats, e.g. text documents, pictures, audio or video, to an **e-mail** as an **attachment**.

In order to be able to use **e-mail**, an **e-mail address** is required. Similar to conventional mail, electronic mail also requires information about the sender and recipient so that a message can be sent.

E-Mail addresses, such as hans@example.com,, are structured according to a uniform format. They consist of a user name (**hans**), an "at sign" (@) and then the complete domain name (**example.de**) according to the **domain name system (DNS)**.

Structure of an e-mail

An e-mail's format is specified in RFC 2822 <http://www.ietf.org/rfc/rfc2822.txt>. Messages are structured in lines according to RFC 2822 (**Internet Message Format**). Each line must be no more than 998 characters and should be no more than 78 characters long. US-ASCII is used as the character set. Lines are completed with CRLF (carriage return - line feed).

The **Internet Message Format** requires that a message be separated into a **header** and a **body**. The **body** contains the actual content of the message, while the **header** contains the meta information, additional information on other data.

Information in an e-mail header

An e-mail is similar to a postcard: it has a sender, a recipient and finally the actual text.

- The **sender's information** ("From") is the e-mail address of the sender. It can be used by the recipient to answer the mail. However, it is also used to return undeliverable mail. The reason is often a typing error since the addresses must always be completely correct.
- The **recipient's information** ("To") is the e-mail address of the recipient. In order to be able to write to a mail partner, you must know his/her exact e-mail address. The same applies here too: be aware of typos or writing errors.
- An **e-mail** also contains another important piece of information: the **subject**, a brief, explanatory line on the content of the **e-mail**.

Generally, besides the sender, recipient and subject, additional **header** information is used, e.g. the creation date of the **e-mail**.

An **e-mail** can always be sent to several recipients. Besides the actual recipient(s), it is also possible to send copies to other recipients as well. There are two ways to do this, abbreviated as "**Cc**" and "**Bcc**":

- "**Cc**" stands for "carbon copy" and is the address of a second recipient to receive a copy of the **mail**. You can also specify any number of recipients here.
- "**Bcc**" stands for "blind carbon copy" and is the address of a second recipient to receive a copy of the mail. You can specify any number of recipients here as well. In contrast to "Cc," the addresses of all "Bcc" recipients are invisible. The recipient of an **e-mail** therefore does not know who this message was also sent to.

9.1.1 e-mail protocols

Three protocols are used on the Internet for the e-mail service:

SMTP	Simple Mail Transfer Protocol	A protocol for transmitting (sending and forwarding) messages, e.g. e-mail
POP3	Post Office Protocol, Version 3	A protocol that allows access to a server that provides e-mails. A protocol for managing mailboxes for computers that are not permanently connected to the Internet.
IMAP	Internet Mail Access Protocol	A protocol for remote access to mail servers. The current version is IMAP4.

Sending e-mails

SMTP is a transport protocol for sending, forwarding and delivering messages. **An e-mail program uses this protocol only to send the mails.** SMTP is specified in RFC 2821.

Receiving e-mails

The **Post Office Protocol (POP3)** is used to receive e-mails. When accessing e-mail via POP3, a mail server stores a user's messages locally in a user's mailbox. This user can then display the existing messages, transfer ("pick up") these to his/her own computer and delete messages. Typically, e-mail users are only connected to the Internet for a short time and "retrieve e-mails" before disconnecting.

Besides **POP3**, the **Internet Mail Access Protocol (IMAP)** is also frequently used for remote access to mail servers. The current version of **IMAP** is defined as **IMAP4** in RFC 2060. Compared to **POP3**, **IMAP4** allows different usage models: like **POP3**, it is possible to work offline, i.e. move the messages periodically from the mail server to the user's computer in order to read them there. However, **IMAP4** also lets you leave messages on the server - in a kind of online operating mode - and transmit these only when required. Finally, hybrid usage types are also supported where some of the messages are read and manipulated online, while another part can be viewed in offline mode, although any changes made in offline mode can also be traced on the server at a later time. In the latter case, the server would remain the main storage location for the messages. Another feature of **IMAP4** is, for example, simultaneous access to mailboxes used by several users.

Note:

Because of the different protocols used to send and receive **e-mail**, various entries must be made in an e-mail program before **e-mail** can be fully utilized. Your Internet service provider will provide you with the necessary addresses and authentication data when it provides you your e-mail account.

9.1.2 The e-mail account

In order to send and receive e-mails, you need

- an Internet connection
- an e-mail program
- an e-mail account with its own e-mail address

Your e-mail account is usually made available by your Internet provider. You will be informed of the following access data:

- Username
- Password
- Computer name or address of the SMTP and POP3 or IMAP server.

In order to use the e-mail account, you must enter this data into your e-mail program.

9.1.3 e-mail services via "webmail"

Apart from the e-mail service offered by your Internet provider, free or at least low-cost web-based e-mail services (**webmail**) are available. You can access these services over the **WWW** via a **web browser** and can thus send and receive your personal mails from any computer with Internet access - even abroad.

Some well-known webmail services in Germany are:

- **GMX:** (<http://www.gmx.de>)
- **Web.de:** (<https://freemail.web.de>)
- **T-Online:** (<https://email.t-online.de>)

e-mail programs

In order to manage and create e-mails, you need an e-mail program, also known as an e-mail client. A large selection of these is available.

Besides the Microsoft products **Outlook** and **Outlook Express**, some very high-performance open source solutions are available, such as **Thunderbird** and **Evolution**.

The e-mail clients must initially be configured with the data offered by the provider in order to permit access to "your mailbox" or you are also able to send e-mails yourself. The corresponding instructions and assistance are offered by the providers or can be found everywhere in the Internet.

The product features of e-mail applications include, among other things:

- **Filters** (rules). Filters are used to set down rules to perform specific tasks with incoming or outgoing mail. For example, you can have incoming e-mails stored in specific directories according to criteria, such as the sender or subject line, in order to keep a better overview.
- **Autoreply**. These "automatic responses" are prepared response letters to incoming mail. These can be used to, for example, automatically send acknowledgement of receipt e-mails for incoming customer orders. The autoreply function usually requires a filter option.
- **Multi-POP**. This functionality lets you manage several e-mail accounts. Several accounts can be queried one after the other without having to enter the basic settings for the SMTP and POP servers again.
- **PGP (Pretty Good Privacy)**. This program encrypts messages transmitted via the Internet. This authentication and encryption method is considered very secure. The application is free for private users but it is not supported by every e-mail program.
- **Templates**. These "templates" are comparable to sample letters. They help to streamline the paperwork. Usually, a program offers some standard templates, which can be extended as desired.
- **Spellcheck**. This function has also proven its worth in word processing. It is intended to support both the new German spelling rules and several other languages.

10 LAN router

Learning objectives:

- know the performance characteristics of current LAN routers
- know access options for configuration and diagnostics on LAN routers
- perform a factory reset
- estimate the product features of a combination LAN router device

Alternative names for LAN routers are

- **DSL-LAN router**
- **ADSL-WLAN router**
- **Wireless-G**
- **ADSL-Home gateway**

Routers for small networks not only provide the Internet connection, but, with all kinds of additional functions, also act as the communications center of the LAN. These combination devices can integrate the **DSL modem** and/or a **radio base station (wireless access point)** for example. The combination device requires less space and power than individual components. However, if a function fails, the entire device must also be replaced immediately.

The following pictures show two types of **WLAN routers** with an integrated DSL modem.



Figure 1: T-Com Speedport W 701V



Figure 2: AVM Fritz!Box Fon 7170

10.1 Performance characteristics

The LAN router often already includes ...

- ADSL modem
- several network ports (LAN ports), normally a 4-port switch (previously a hub)
 - Fast Ethernet (100 MBits/s)
 - Giga Ethernet (1000 MBits/s)

- DHCP server
- Wireless base station (Wi-Fi base station of Wi-Fi access point)
- Firewall
- Connection for Internet telephony (Voice over IP)

Additional router extras include ...

- Telephone hub, connection for analog telephones
- USB interface for printers → configuration as network printer (print server)
- USB interface for external USB hard drive with Samba server for "Windows file sharing"
- "Parental controls" using web filters and timetables
- Client for address services such as *dyndns.org*
The router subscribes to a directory service so that it can be accessed from the Internet via an easily recognizable name such as *lvestation.dyndns.org*.
- Configurable port forwarding
Makes services like your own webserver or secure access via *ssh* possible from outside
- For routers with Wi-Fi: it should meet at least comply with the current **802.11g standard** and ensure secure encryption

10.2 Router configuration

Software wizards make the installation process simple. However, some manual work is still required for the security settings. Current routers are set up via the **web browser**. **Microsoft Internet Explorer** is the first choice for this task because many programmers do not seem to test their router pages with other **web browsers**. Many current routers use **JavaScript**, which must be activated. Popups should also be allowed.

The **URL** of the configuration pages and the default password to be entered on the login page are in the documentation. With the T-Com Speedport 701-V for example, this occurs via:

<http://speedport.ip>

and the default password: 0000

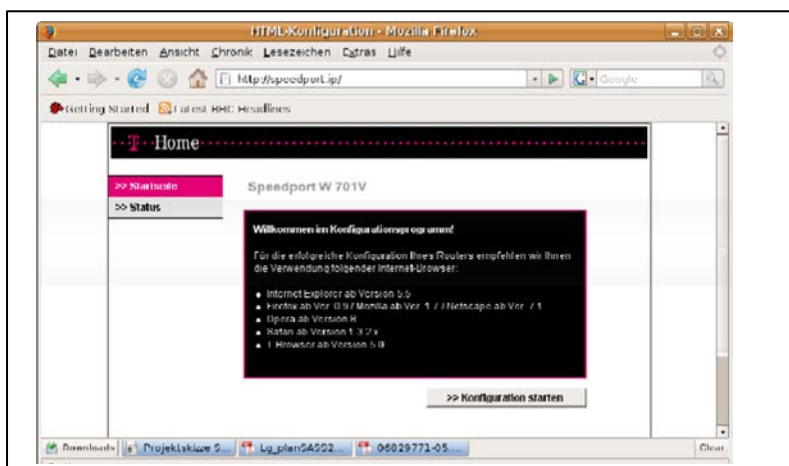


Figure: calling up the configuration page on the Speedport 701V

If the login page appears, but the default password from the documentation does not open the input, then press the Reset button to **restore it to the factory settings (factory reset)**. To do this, you usually have to hold down the reset button for about half a minute. More detailed information should be provided in the manual.

10.3 What can be configured?

- **Internet access**

→ Settings for an integrated ADSL modem

VPI=1 VCI=32 Encapsulation=LLC

Dial-up method = PPOE (external modem required) user name and password (provider data)

Note: these parameters are not discussed in this seminar

- **DHCP server**

Automatically supplies the corresponding client systems with IP configuration parameters.

- **poss. firmware upgrade**

In the configuration program, go to the firmware page, click on the downloaded file and click again to start the update. After the update, the router automatically reboots so that the entire procedure may take 5 minutes.

Note: surprisingly, an update is often required for new devices as well

- Take **preliminary security measures**. These include ...

... replacing the configuration's default password with a customized password

... deactivating remote maintenance (remote control or remote configuration)

... disabling Universal Plug&Play (**UPnP**), no port forwarding function of UPnP

... no additional firewall rules (NAT entries, port forwarding only)

Network Address Translation (NAT) protects against direct attacks from outside

- **Radio network (Wi-Fi)**

Encryption should be set here. In many routers, the wizard configures the basic setting without encryption. **Note:** according to the law, those who use **Wi-Fi** without encryption shall be held liable should anyone else use it for criminal activities.

- **Time server (NTP, Network Time Protocol)**

The devices synchronize their internal clocks with time servers via the Internet. American or Taiwanese servers are often preset here. To reduce the load on these servers and to increase their accuracy, you should enter a server closer to your network such as the *ptbtime1.ptb.de* and *ptbtime2.ptb.de* operated by the National Metrology Institute of Germany (PTB).

- **Providing services from the LAN for the Internet → DynamicDNS**

Special steps are required if you want to, for example, access a web server in the LAN (home network) from outside the network (from the Internet). Special safety precautions must also be taken.

This topic is examined in a separate chapter.

- **Activating Voice-over-IP gateway (VOIP)**

The router also has ports for analog telephones or ISDN telephony. The following parameters must still be configured: the phone number assigned by the VOIP provider, user name and password, as well as the two servers - the SIP Registrar and the SIP Proxy (normally identical addresses). Some models require that you then separately specify which telephone rings under which VOIP phone number. Dialing rules, call blocking and call forwarding are also configurable.

VOIP is not part of this seminar.

Universal Plug & Play (UPnP)

A protocol developed by Microsoft that any programs on a station in the LAN can use to create port extensions without any access control. Developed for online games (to simplify installation), it also permits Trojans to install themselves as servers on the Internet. The router's online status can also be queried via UPnP. This is not critical in terms of safety. Better routers permit it, both functions

Network Translation Address (NAT)

Protects against direct attacks from outside. Since the router receives only one address from the provider when dialing in, it must translate the requests from all the PCs on the home network (LAN) to this address and use a table to assign the answers from the Internet to the correct PC. An entry is only made in the NAT table when the connection has been established from the LAN. That's why the router discards packets that an attacker sends without being requested to do so from the Internet because he cannot deliver these to a LAN PC because a NAT entry is missing.

11 Strategic troubleshooting in the TCP/IP network

Learning objectives:

- get to know and apply troubleshooting strategies in the TCP/IP network
- use the network layer model for strategic troubleshooting

Connection and communication problems in the network can be very complex and multi-faceted. A systematic approach is essential when troubleshooting. Understanding the network layer model as described in the "TCP/IP - Basics" chapter plays an important role here.

Strategic troubleshooting in the TCP/IP network

- Check the physical connection
- Check the current IP configuration
- Test the network software interface
- Check the network card and driver
 - is the TCP/IP stack successfully installed?
- Check the connection to computers in the local network
- Check the connection to the router (default gateway)
- Test routing - Check the connection to computers in the remote network
- Test name resolution (DNS)

Figure 1: overview of the necessary steps for troubleshooting in the TCP/IP network

Troubleshooting in the TCP/IP network should be performed in the specified order. The following examines the individual steps in more detail:

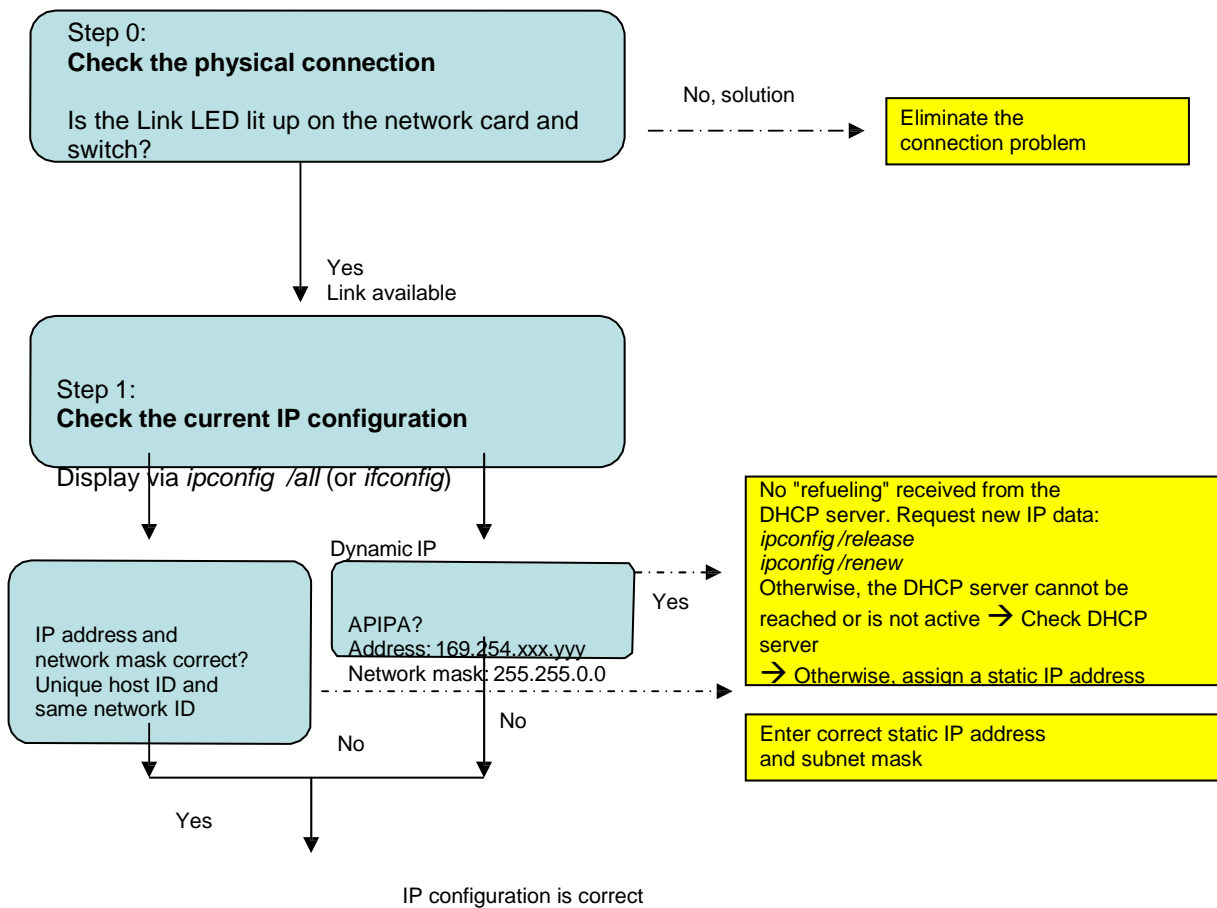


Figure 2: step 0 and step 1

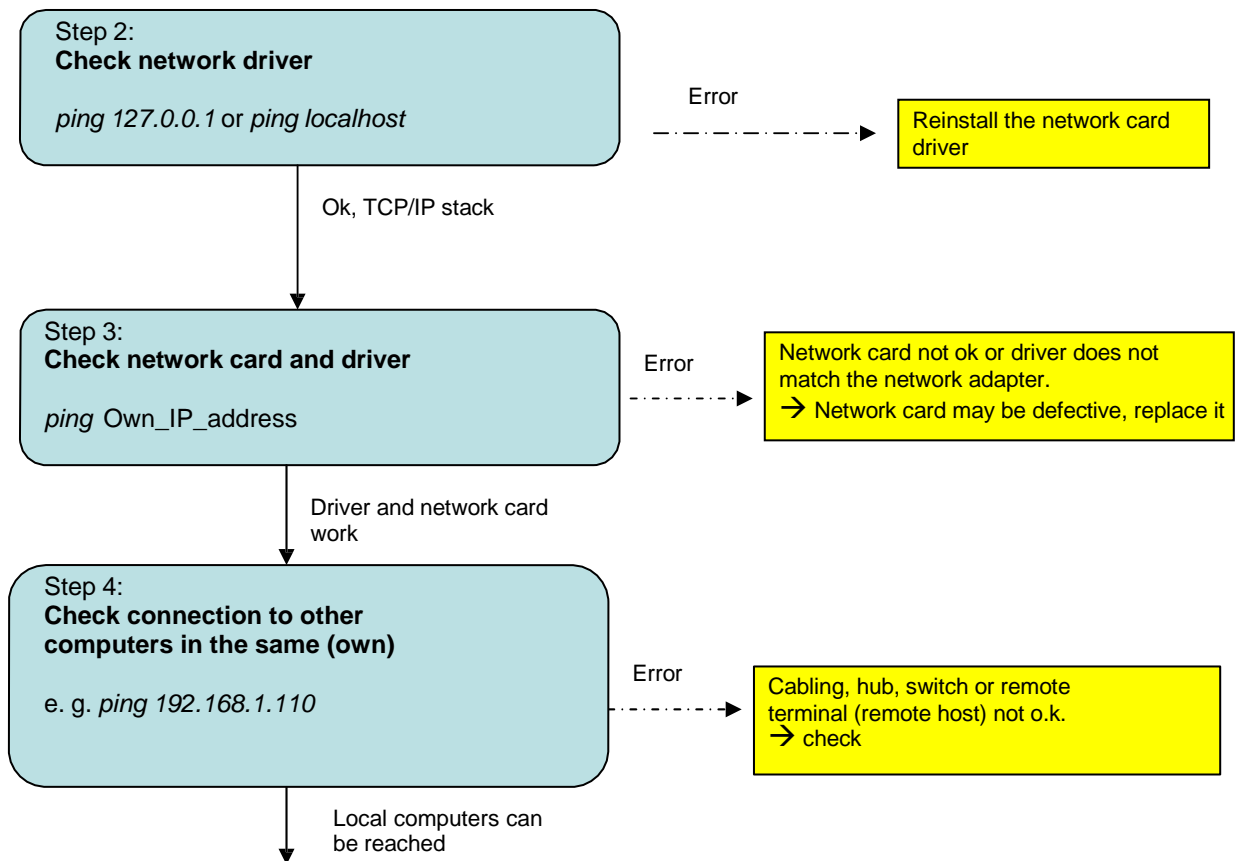


Figure 3: Step 2 to Step 4

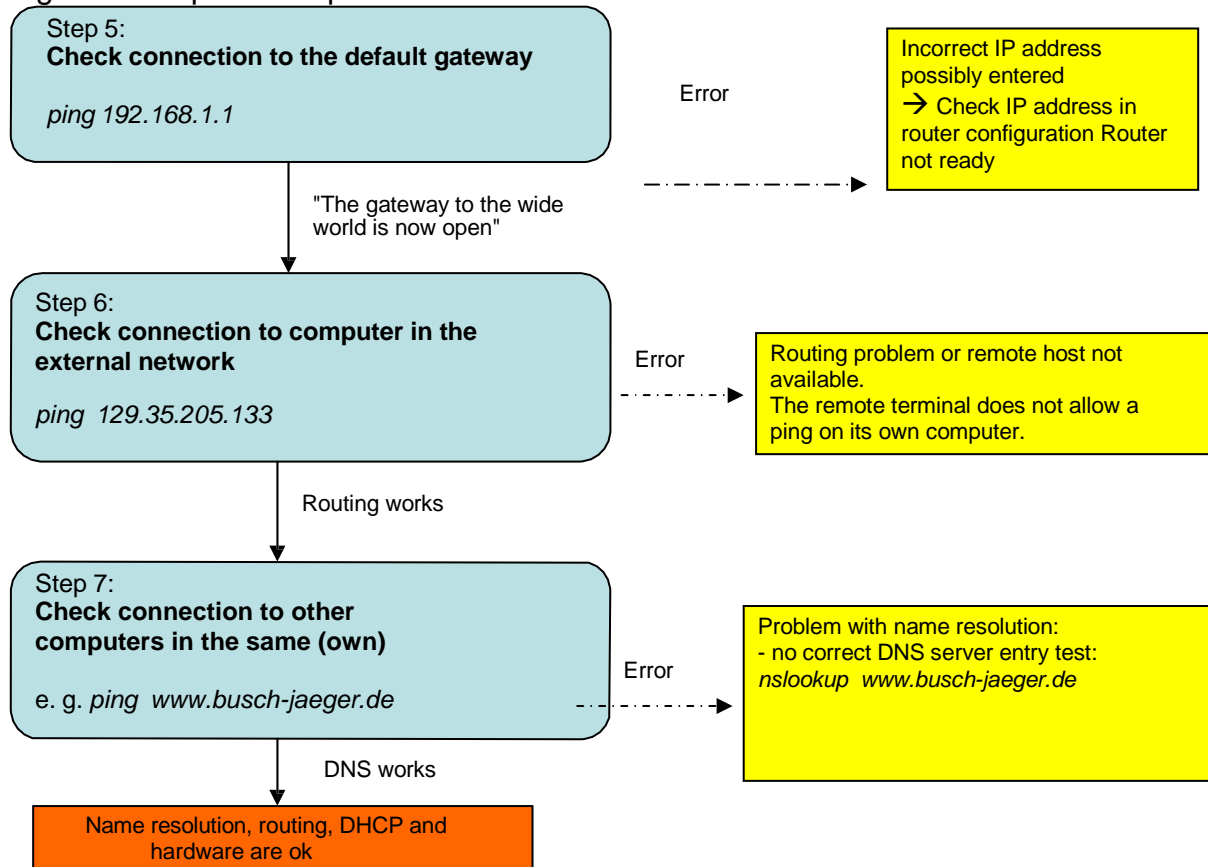


Figure 4: Step 5 to Step 7

Additional information:

On Step 0:

The illuminated LINK LED on the network cards and the switch/DSL router indicates that the electrical connection is established. This should always be checked first before you search for the error in the IP addresses for example. A blinking LINK LED indicates data traffic on most devices.

On Step 1: APIPA (Automatic Private IP Addressing):

If the address is 169.254.yyy.xxx with the subnet mask: 255.255.0.0: then *Autoconf* was activated on the client. It comes into play when the DHCP server cannot be reached repeatedly. This simply means that the client could not hear the DHCP server.

This event is also logged in the system log of the event display in Windows XP/2000 and can be viewed as a "DHCP error" there.

12 Tools for diagnosis and troubleshooting

Learning objectives:

- get to know and apply important troubleshooting tools in the TCP/IP network
- get to know and apply diagnostic tools for the TCP/IP network
- identify possible uses and limits of the tools

Programs that belong to the "TCP/IP package" ("on-board resources"),

- software from the operating system manufacturer and
- tools from third-party providers are available for
- troubleshooting and network analysis in the TCP/IP network. Some of these are very complex and require in-depth knowledge of the network.

The following table provides an overview of the most important tools.

Tool	Ubuntu	Windows
Display the current IP configuration	<code>ifconfig</code> and <code>route -n</code>	<code>ipconfig</code> or <code>ipconfig /all</code>
Connectivity	<code>ping 127.0.0.1</code> <code>ping 192.168.2.55</code> <code>ping 129.35.205.133</code> <code>ping www.busch-jaeger.de</code>	<code>ping 127.0.0.1</code> <code>ping 192.168.2.55</code> <code>ping 129.35.205.133</code> <code>ping www.busch-jaeger.de</code>
Name resolution (DNS)	<code>nslookup www.busch-jaeger.de</code>	<code>nslookup www.busch-jaeger.de</code>
Route tracing	<code>tracert 129.35.205.133</code>	<code>tracert 129.35.205.133</code>
Display ARP table (translate IP address to MAC address)	<code>arp -a</code>	<code>arp -a</code>
Professional network analyzer	Wireshark (previously	Wireshark (previously
Display open ports	<code>nmap localhost</code>	<code>netstat</code>
Display the routing table	<code>route -n</code>	<code>netstat -rn</code>

Figure 1: overview of tools for diagnosis and troubleshooting in the TCP/IP network

Operating systems too already include a few software tools. Ubuntu Linux, for example, comes with a very convenient network diagnostics tool.

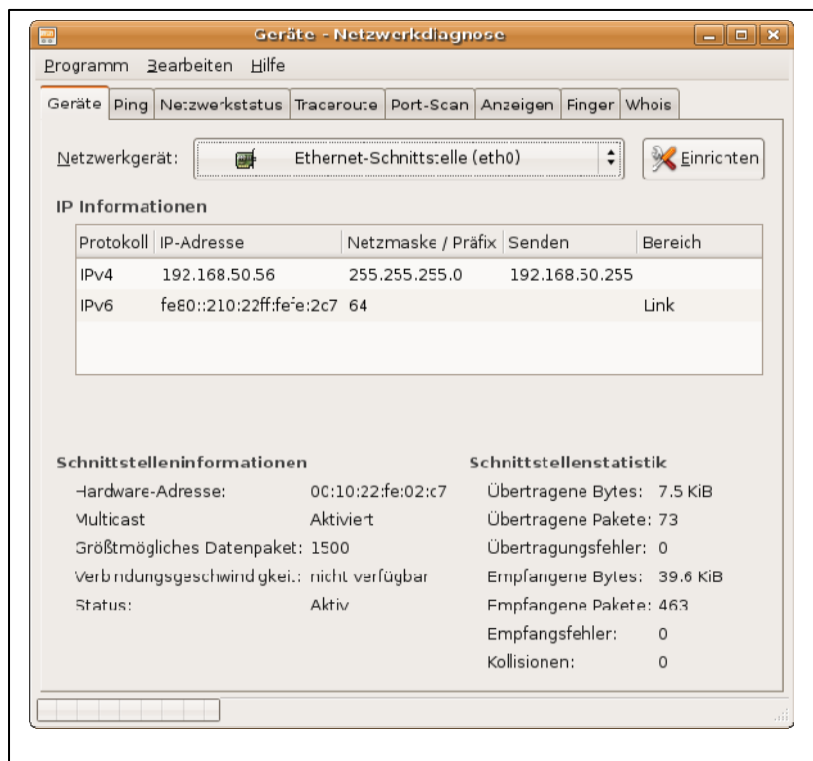
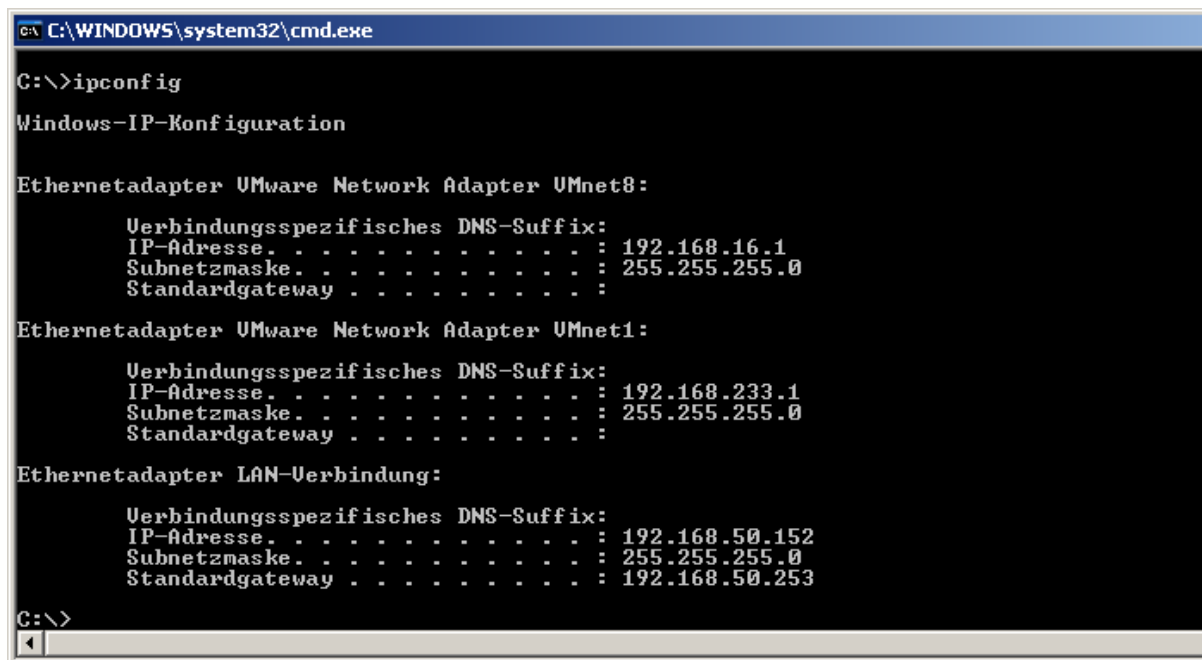


Figure 2: Ubuntu Linux comes with a convenient network diagnostics tool.

12.1 Display current IP configuration – *ipconfig* / *ifconfig*



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig

Windows-IP-Konfiguration

Ethernetadapter VMware Network Adapter VMnet8:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.16.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter VMware Network Adapter VMnet1:

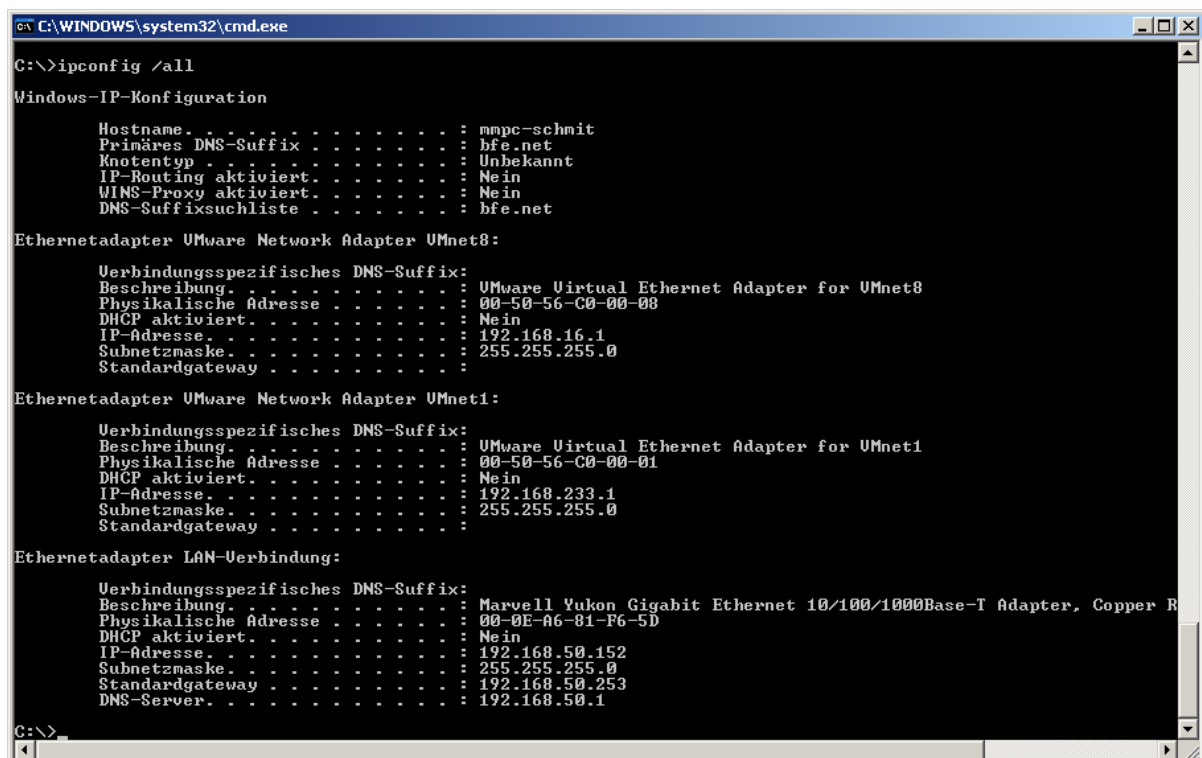
    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.233.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse. . . . . : 192.168.50.152
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.50.253

C:\>
```

Figure 3: display current IP configuration with *ipconfig*



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Windows-IP-Konfiguration

    Hostname. . . . . : mmpc-schmit
    Primäres DNS-Suffix. . . . . : bfe.net
    Knotentyp . . . . . : Unbekannt
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein
    DNS-Suffixsuchliste . . . . . : bfe.net

Ethernetadapter VMware Network Adapter VMnet8:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : VMware Virtual Ethernet Adapter for VMnet8
    Physikalische Adresse . . . . . : 00-50-56-C0-00-08
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.16.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter VMware Network Adapter VMnet1:

    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : VMware Virtual Ethernet Adapter for VMnet1
    Physikalische Adresse . . . . . : 00-50-56-C0-00-01
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.233.1
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

Ethernetadapter LAN-Verbindung:

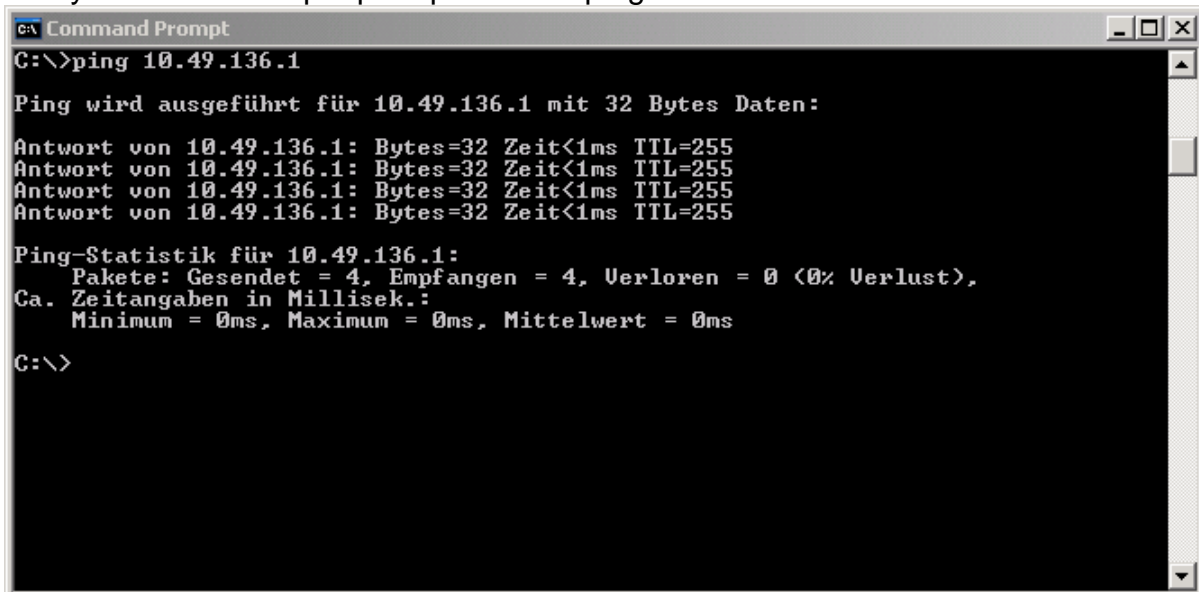
    Verbindungsspezifisches DNS-Suffix:
    Beschreibung. . . . . : Marvell Yukon Gigabit Ethernet 10/100/1000Base-T Adapter, Copper R
    Physikalische Adresse . . . . . : 00-0E-A6-81-F6-5D
    DHCP aktiviert. . . . . : Nein
    IP-Adresse. . . . . : 192.168.50.152
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.50.253
    DNS-Server. . . . . : 192.168.50.1

C:\>
```

Figure 4: display current IP configuration in detail with *ipconfig /all*

12.2 Check connectivity – *ping*

Whether the devices can in principle exchange data with each other can be easily tested in the input prompt with the ping command



```
C:\>ping 10.49.136.1

Ping wird ausgeführt für 10.49.136.1 mit 32 Bytes Daten:

Antwort von 10.49.136.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 10.49.136.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 10.49.136.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 10.49.136.1: Bytes=32 Zeit<1ms TTL=255

Ping-Statistik für 10.49.136.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

C:\>
```

Figure 5: checking connectivity with the ping command.
Is the node 10.49.136.1 reachable.

Ping – Packet Internet Groper – is the most commonly used tool to test a network connection to another station or just test the local TCP/IP stack. An **ICMP Echo Request** ("PING") type **ICMP** packet is sent to the network station when the **ping** command is executed. When the station has received the ICMP packet, it sends an **ICMP Echo Reply** ("PONG") type ICMP packet back.

Note: In Windows, the *ping* command only executes the "PING" a total of 4 times in a row. Linux executes a continuous "PING." Press the <Ctrl> + <C> key combination to abort.

12.3 Check name resolution - *nslookup*

The nslookup tool, which comes with TCP/IP, can be used to check the name resolution with DNS.



```
C:\>nslookup www.busch-jaeger.de
Server: vdc1.bfe.net
Address: 192.168.50.1

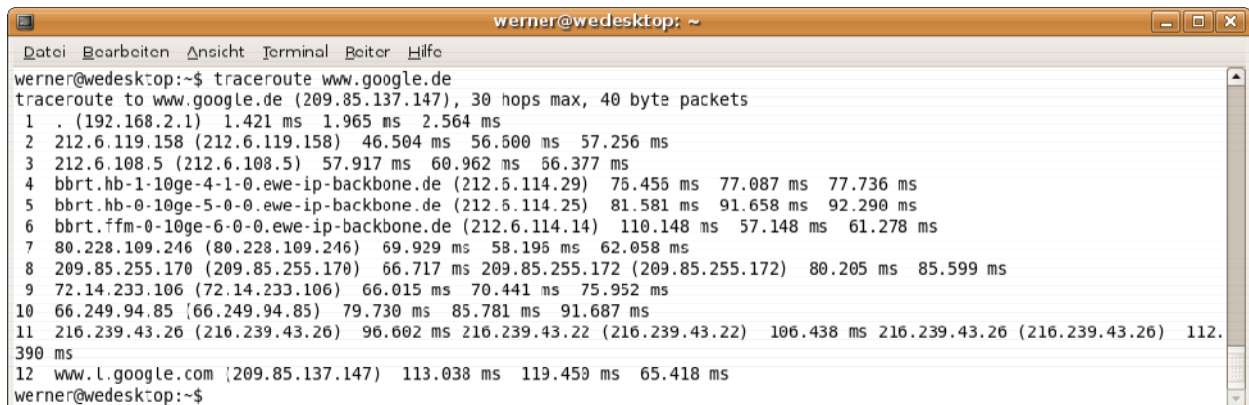
Nicht autorisierte Antwort:
Name: www.busch-jaeger.de
Address: 129.35.205.133

C:\>
```

Figure 6: checking the Domain Name Service (DNS name resolution)

12.4 Route tracing – *tracert* / *traceroute*

The tracert (Windows) or traceroute (Linux/Unix) program provides even more information about the network connection between the local and a remote station. Trace Route traces back the route and makes it visible.



```
werner@wedesktop: ~
Datei Bearbeiten Ansicht Terminal Beiter Hilfe
werner@wedesktop:~$ traceroute www.google.de
traceroute to www.google.de (209.85.137.147), 30 hops max, 40 byte packets
 1 . (192.168.2.1) 1.421 ms 1.965 ms 2.564 ms
 2 212.6.119.158 (212.6.119.158) 46.504 ms 56.500 ms 57.256 ms
 3 212.6.108.5 (212.6.108.5) 57.917 ms 60.962 ms 66.377 ms
 4 bbrt.hb-1-10ge-4-1-0.ewe-ip-backbone.de (212.5.114.29) 76.455 ms 77.087 ms 77.736 ms
 5 bbrt.hb-0-10ge-5-0-0.ewe-ip-backbone.de (212.5.114.25) 81.581 ms 91.658 ms 92.290 ms
 6 bbrt.ffm-0-10ge-6-0-0.ewe-ip-backbone.de (212.6.114.14) 110.148 ms 57.148 ms 61.278 ms
 7 80.228.109.246 (80.228.109.246) 69.929 ms 58.195 ms 62.058 ms
 8 209.85.255.170 (209.85.255.170) 66.717 ms 209.85.255.172 (209.85.255.172) 80.205 ms 85.599 ms
 9 72.14.233.106 (72.14.233.106) 66.015 ms 70.441 ms 75.952 ms
10 66.249.94.85 (66.249.94.85) 79.730 ms 85.781 ms 91.687 ms
11 216.239.43.26 (216.239.43.26) 96.602 ms 216.239.43.22 (216.239.43.22) 106.438 ms 216.239.43.26 (216.239.43.26) 112.390 ms
12 www.l.google.com (209.85.137.147) 113.038 ms 119.459 ms 65.418 ms
werner@wedesktop:~$
```

Figure 7: determining the route to the destination using tracert/traceroute

When the tracert or traceroute command is executed, an ICMP command (ping) is sent to the destination address with a TTL value set to "1." The router that detects the expired lifetime of the data packet discards the packet and returns a "Time Exceeded" (type 11) ICMP message. The incrementing TTL value is used to identify all the routers on the route to the destination.

12.5 Analyzing the network - Wireshark

Wireshark (previously known as Ethereal) is a powerful open source network analysis software that is available for Linux, Mac OS and for Windows. This popular tool analyzes network traffic on the protocol level. The sniffer goes deep into detail and permits a look into the protocol headers for example. Professionals can easily use this tool to troubleshoot problems.

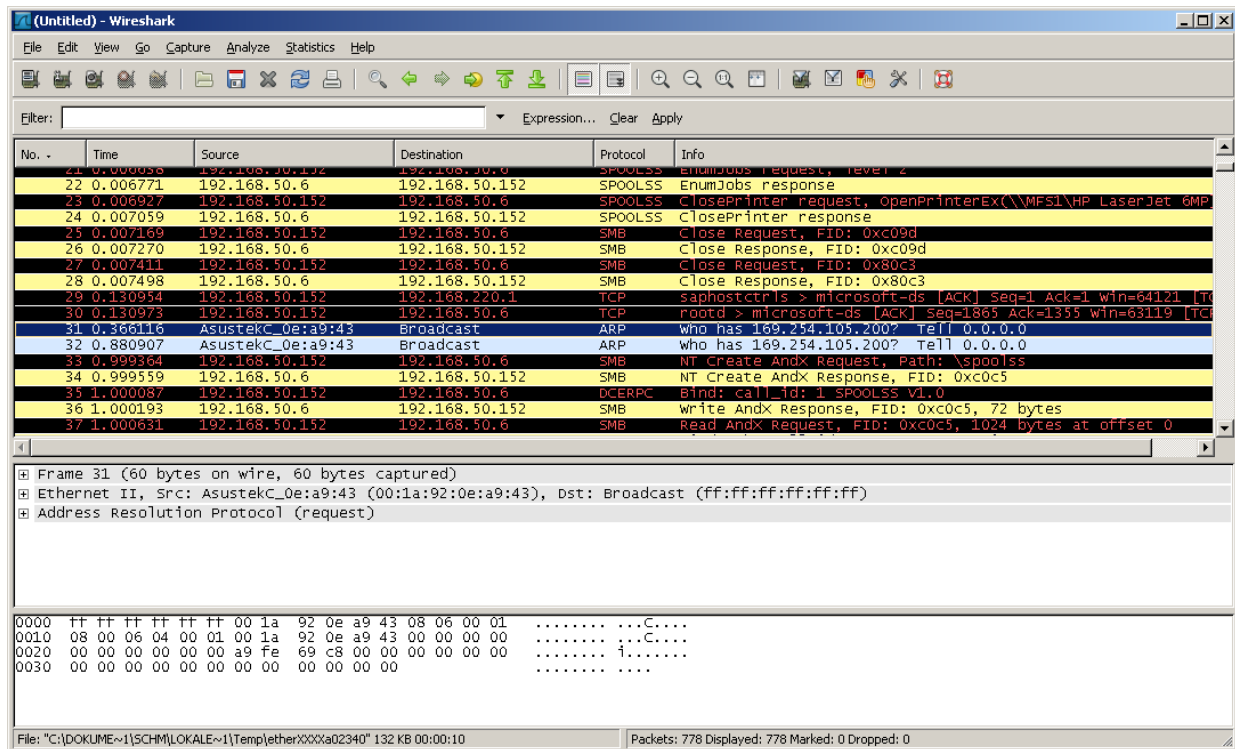


Figure 8: the Wireshark network analyzer

12.6 Display routing tables *netstat / route*

```
C:\WINDOWS\system32\cmd.exe

C:\>netstat -rn

Routingtabelle
=====
Schnittstellenliste
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ..... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x4 ...00 0e a6 81 f6 5d ..... Marvell Yukon Gigabit Ethernet 10/100/1000Base-T Adapter.
=====
Aktive Routen:
=====
Netzwerkziel   Netzwerkmaske   Gateway   Schnittstelle   Anzahl
0.0.0.0        0.0.0.0         192.168.50.253 192.168.50.152   20
127.0.0.0      255.0.0.0       127.0.0.1     127.0.0.1        1
192.168.16.0   255.255.255.0   192.168.16.1   192.168.16.1     20
192.168.16.1   255.255.255.255 127.0.0.1     127.0.0.1        20
192.168.16.255 255.255.255.255 192.168.16.1   192.168.16.1     20
192.168.50.0   255.255.255.0   192.168.50.152 192.168.50.152   20
192.168.50.152 255.255.255.255 127.0.0.1     127.0.0.1        20
192.168.50.255 255.255.255.255 192.168.50.152 192.168.50.152   20
192.168.233.0   255.255.255.0   192.168.233.1 192.168.233.1    20
192.168.233.1   255.255.255.255 127.0.0.1     127.0.0.1        20
192.168.233.255 255.255.255.255 192.168.233.1 192.168.233.1    20
224.0.0.0      240.0.0.0       192.168.16.1   192.168.16.1     20
224.0.0.0      240.0.0.0       192.168.50.152 192.168.50.152   20
224.0.0.0      240.0.0.0       192.168.233.1 192.168.233.1    20
255.255.255.255 255.255.255.255 192.168.16.1   192.168.16.1     1
255.255.255.255 255.255.255.255 192.168.50.152 192.168.50.152   1
255.255.255.255 255.255.255.255 192.168.233.1 192.168.233.1    1
Standardgateway: 192.168.50.253
=====
Ständige Routen:
Keine

C:\>
```

Figure 9: display routing tables under Windows

The routing table of the local computer can be displayed under Windows with ***netstat -r(n)*** and under Linux with ***route -n***.

Netstat offers many more possibilities. The ***netstat*** command line tool can be used to retrieve all active TCP, UDP and IP connections, the routing table and detailed statistics on the TCP/IP data.

List all active connections	<i>netstat -a</i>
List the routing table	<i>netstat -r[n]</i>
Display detailed statistics of the TCP/IP data	<i>netstat -s</i>

13 Remote access from the Internet to the home network (DynDNS)

Learning objectives:

- understand the principle of dynamic DNS (DynDNS)
- identify the steps required to configure DynDNS
- configure a dynamic DNS for a home network

Motivation

You want your PC or another IP device in your home network to be always accessible from the Internet at the same web address (domain name) even though the public IP address assigned by your DSL Internet provider is constantly changing.

From the Internet, you want to, for example, ...

- ... access a web server in your home network via HTTP protocol
- ... access a monitoring camera in your home/company network
- ... allow remote desktop access to a desktop PC in your home network
- ... access a home server via *ssh* for maintenance
- ... allow access to home data via FTP protocol when you're away from home
- ... establish a VPN connection to a computer in your home network

or, in general,:

- ... provide a service for the Internet from your home network.

In this case, you must use a **dynamic name service** on the Internet, the so-called **dynamic DNS (DynDNS)**, and set it up for your home network.

Using **Dynamic DNS**, you can ensure that a web server on your PC (or another service), for example, can always be reached via a fixed **URL** on the Internet. To do this, you must register once with a **Dynamic DNS** provider on the Internet and reserve a **domain name** (e.g. *mycam.dyndns.org*) there. An additional function in the DSL router then compares the IP address currently assigned by the Internet provider with this **domain name** every time the Internet connection is established.

This chapter examines the theoretical basics and the practical implementation for **Dynamic DNS**.

DynDNS – in brief

Dynamic DNS (DynDNS) lets you access a computer with a permanently changing IP address via a defined name. This is required, for example, when you want to access a server that is behind a DSL router. The WAN interface of the DSL router is assigned a new public IP address by the Internet provider every 24 hours. With the help of DynDNS, you do not always have to find the public address every time first in order to access the server. It can be accessed directly via the name. It should be noted that such a name is considerably easier to remember than an IP address.

13.1 Principle of remote access with DynDNS

Almost all internet providers assign dynamic IP addresses to their customers. The customer is assigned a new IP address for each dial-up or connection setup. It does not matter whether the Internet connection is established with a modem, ISDN or DSL. Even for customers with a DSL flat rate, the connection is automatically disconnected after 24 hours. If you now want to operate a server, like a small web server, over your own DSL connection, you then require **dynamic DNS (DynDNS)**.

The server should always be accessible via the same domain name. DNS is responsible for translating a domain name into an IP address. Only the WAN interface of the DSL router is always visible to the outside, to the Internet. In order for the server to always be available under the same hostname, the entry must be updated on the nameserver (DNS) after an address change.

This method is called **dynamic DNS**. Many providers of dynamic DNS are available, **such as** dyndns.org, regfish.com **and** noip.com.

One of the most popular providers of this service is **dyndns.org**. There, it is possible to register a **hostname** (computer name, **domain name**) free of charge and have its IP address updated dynamically. Software called **DynDNS client** is required in the home network. It reports the IP address assigned by the provider to **dyndns.org**.

Today, many DSL routers already come with a **DynDNS client**. If the router does not have this feature, the update must be initiated from a PC in the home network.

Special tools for this are available depending on the operating system. Linux has the **RunDNS** tool. Windows, the **DynDNS Updater** for example.

Other IP devices, such as IP cameras, usually also have a DynDNS client.

After successful configuration, the DynDNS client reports the current public IP address to its DynDNS service provider every time you connect to the Internet.

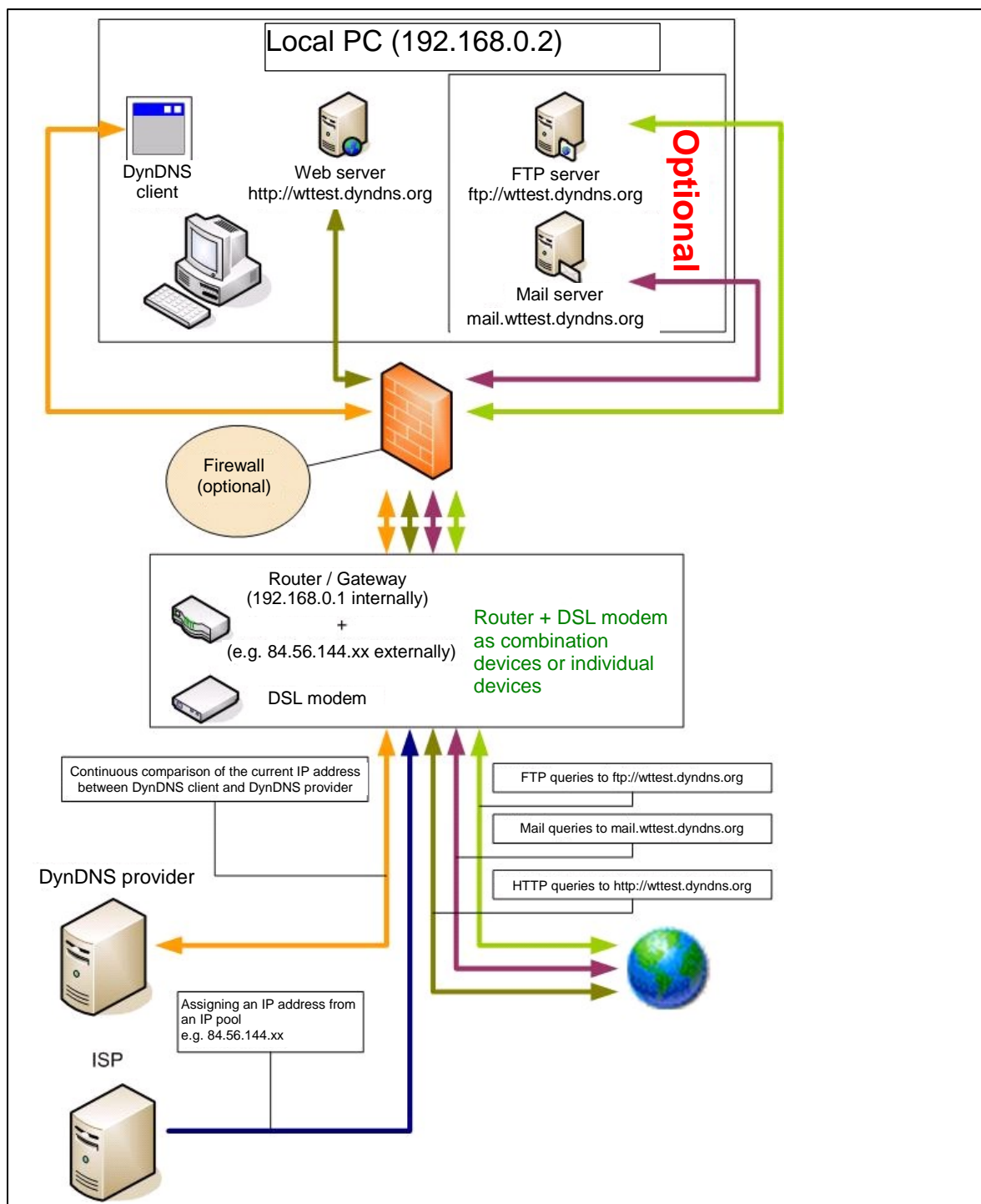


Figure 1: principle of remote access with DynDNS

Source: <http://www.wintotal.de/Artikel/dyndns/dyndns.php>

Important!

For security reasons, the service computer should be located in a protected zone, a demilitarized zone (DMZ), on the home network.

What is my IP address?

If you want to find out which IP address you are currently using online, you can call up the <http://www.wieistmeineip.de/> URL for example.

Background information:

Since you are calling up this page via a router with **Network Address Translation (NAT)**, you will not see the IP address of your client computer here. Clients behind routers often use IP addresses from the privately reserved address space according to RFC 1918 (see chapter TCP/IP basics, Private IP address spaces). Thus, addresses from the networks 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16. These networks are not routed on the Internet. If your PC has the IP address 192.168.1.31, for example, your router will translate this address into an official address. This official address is assigned to the DSL router by your internet service provider when the connection is being established. The www.wieistmeineip.de website shows you

13.2 Configuration for remote access - What must be done?

Additional information on the Internet under:

<http://www.wintotal.de/Artikel/dyndns/dyndns.php> _
<http://www.easy-network.de/dyndns-einrichten.html>

To put your own server, e.g. web server, behind a DSL router into the Internet requires quite a bit of work. The following describes how to do this using the **dyndns.org** DynDNS service provider as an example. The DSL router is the **Fritz!Box 7170**. The procedure and configuration is done accordingly for other providers for DynDNS services or DSL router products.

Several providers of **DynDNS** services are available. These include, amongst others, *dyndns.org*, *regfish.com* and *noip.com*. Some of these services are offered free of charge. The following examines the free version of *dyndns.org*, which allows up to 5 DynDNS entries.

All of the DynDNS service providers let you manually update the DNS entries via a web interface or via a special **DynDNS client**. A client is already integrated in modern DSL routers these days. If this is missing, corresponding client software must be installed as a service on a PC or other IP device in the home network. The most convenient way is, of course, an automatic update by the DSL router.

The following steps are required:

1. Configuring the router to be permanently online

The DSL router requires a continuous connection to the Internet in order for the home server to be continually accessible from the Internet. A configuration tool in the DSL router offers an option called "Always on," "Stay connected," "Auto reconnect" or similar. Normally, it is located near the *Idle timeout*, which is its opposite.

Specifically for the Fritz!Box:

<http://fritz.box> → Internet → Access data → Connection settings → Maintain continuous Internet connection

2. Applying for a Dynamic DNS service

The router's IP address, which changes at each dial-in, must be assigned a static name. This is ensured by such services as *dyndns.org*. The Admin creates an account on the website and registers a "DynamicHost" like *mycam.dyndns.org*.

In order to use the DynDNS service, we first have to register ourselves at this kind of service provider and create an account.

At DynDNS.org, this is done at <http://www.dyndns.org/account/create.html>

Note: The **username** has nothing to do with the hostname, which needs to be entered later

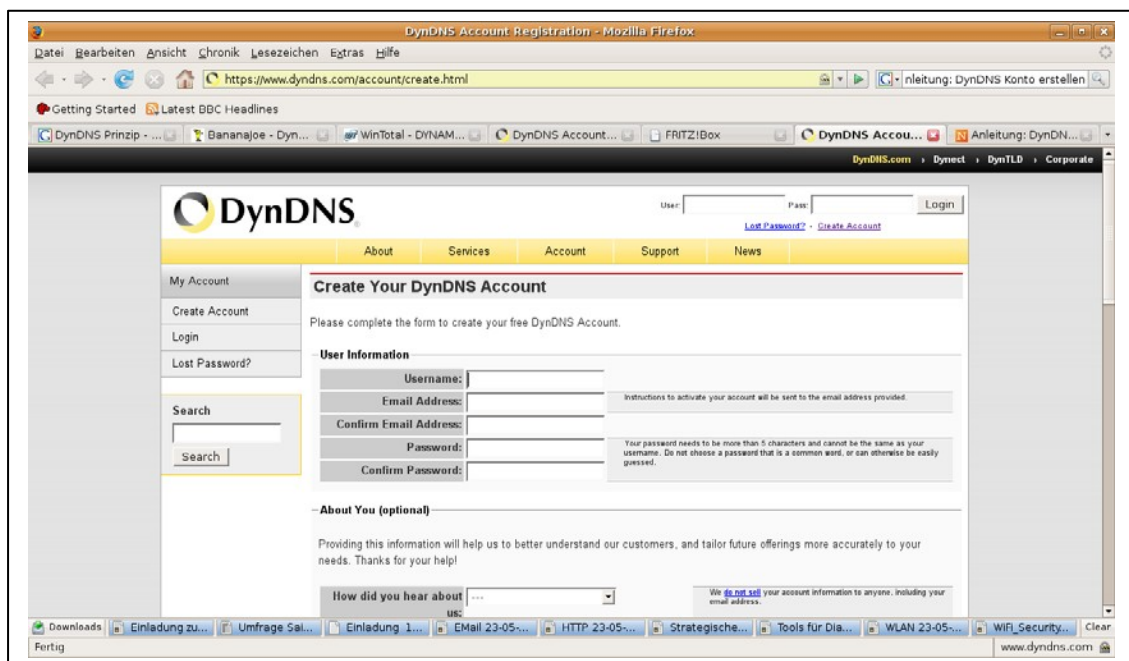
The image shows a screenshot of a web browser window titled "DynDNS Account Registration - Mozilla Firefox". The address bar shows the URL "https://www.dyndns.com/account/create.html". The page content includes the DynDNS logo, a navigation menu with links like "About", "Services", "Account", "Support", and "News", and a "Create Your DynDNS Account" form. The form has sections for "User Information" (Username, Email Address, Confirm Email Address, Password, Confirm Password) and "About You (optional)". There are also links for "My Account", "Create Account", "Login", and "Lost Password?". The browser's taskbar at the bottom shows several open windows, including "Downloads", "Einladung zu...", "Umfrage Sal...", "Einladung 1...", "Email 23-05...", "HTTP 23-05...", "Strategische...", "Tools für Dia...", "WLAN 23-05...", and "WIFI Security...".

Figure 2: registering with your DynDNS provider

All you need to do now is enter the required host(s) at dyndns.org. To do so, log in to dyndns.org with your created account

Log in with account → My Service → Add New Hostname

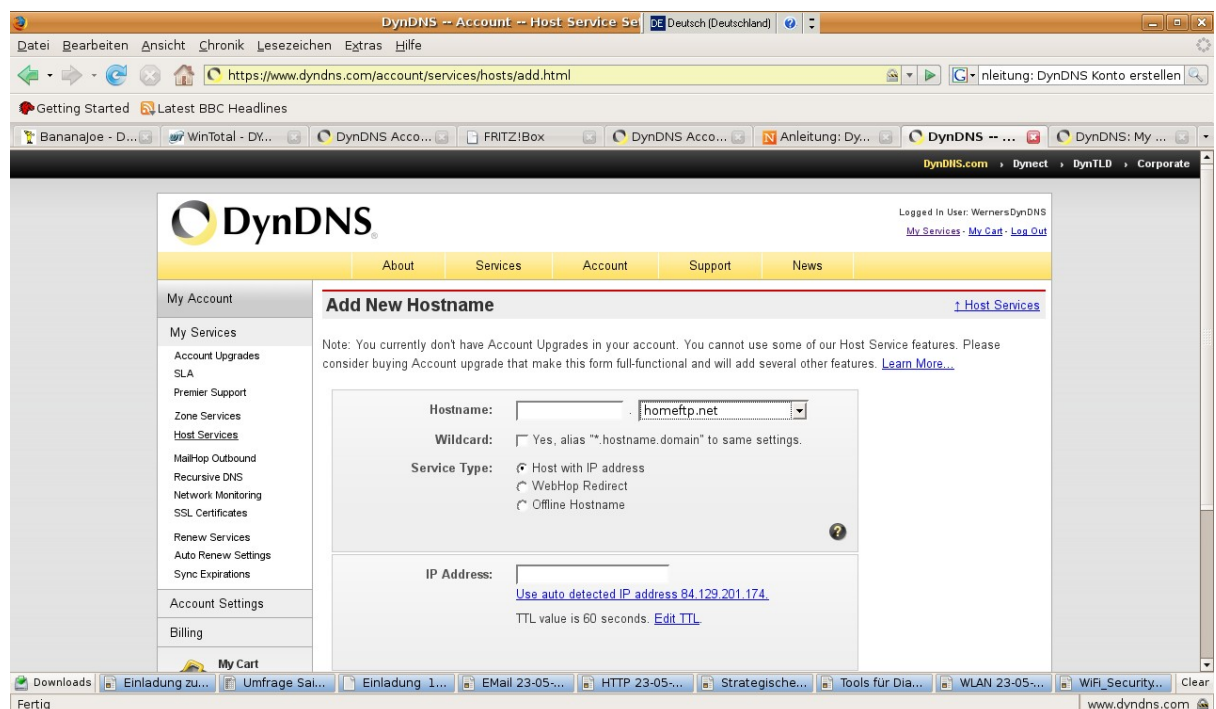


Figure 3: creating a DynDNS address

After the hostname has been created, you can already check the name resolution
nslookup mycam.dyndns.org

3. Configuring the router for DynDNS - Activating the DynDNS client

The account data (username/password) and the domain name (computer name, e.g. *mycam.dyndns.org*) is entered in the DSL router under "DynamicDNS" at the DynDNS service provider. This will register the new IP address at *dyndn.org* with each dial-up. Shortly thereafter, the DSL router can be accessed from the network under its name.

Note: If the DSL router does not contain a **DynDNS client**, then DynDNS client software must be installed on a computer in the home network (e.g. for Windows, DynDNS Updater).

Checking the DynDNS functionality:

To check this, it is very practical when the router responds to ping requests **from the Internet**:

ping mycam.dyndns.org

Alternatively:
`nslookup mycam.dyndns.org`

The "Ping block" or "Deny WAN request" function must be switched off on the current routers. This setting is intended to hide the router from hackers who use ping scans to search for victims on the Internet. However, professionals won't be deterred by ping scans so that security is not impaired when the ping block is deactivated.

Specifically for Fritz!Box: prerequisite

- In order to use DynDNS, the Fritz! Box must be set up for router operation:
<http://fritz.box> → Internet → Access data → Use access data (Fritz!Box works as a DSL router)

Setting up a DynDNS client on the Fritz!Box

- Switch the user interface to Expert mode

<http://fritz.box> → System /View → Display expert settings → Apply

- DynDNS provider, domain name and the access data of the DynDNS provider
<http://fritz.box> → Internet → Dynamic DNS

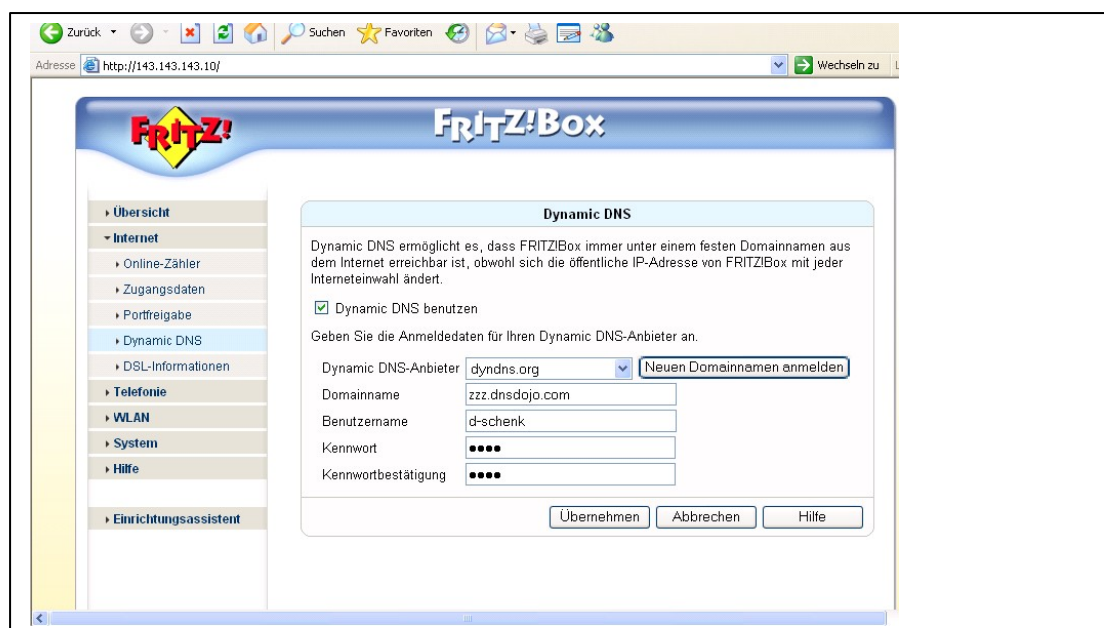


Figure 4: setting up a DSL router as a DynDNS client requires the DynDNS provider, domain name and account data from the DynDNS provider.

4. Activating port forwarding for a computer on a router

If you now contact a service in the home network via the DynDNS name, e.g. <http://mycam.dyndns.org>, the router does not know (because of Network Address Translation) where to send the packages. The trick is to create static entries in the NAT table which forward these kinds of packets to a computer in the LAN. The standard term for this is **port forwarding**. Which computer receives the data is decided based on the protocol, TCP or UDP, and the port. Some DSL router manufacturers also use the term "Virtual Server," which is actually used for a different purpose.

If, for example, a web server is running on computer 192.168.1.110 in the home network, the TCP port 80 is then forwarded to this address. This means that the web server can be reached via the browser at .

Small improvement:

Attackers usually first search for a vulnerable web server using many addresses on the default port 80. It is therefore recommended to use a different external port on the router and, for example, forward the TCP port 52510 of the DSL router to port 80 on the server computer. In this way you can escape the first wave of attacks with some luck and gain the necessary time for the web server update. However, the URL changes to a grandparent-unfriendly <http://mycam.dyndns.org:52510/>.

Specifically for the Fritz!Box:

<http://fritz.box> → Internet → Port enable → New port enable



Figure 5: port forwarding configuration on the Fritz!Box 7170