University of Zurich
Department of Informatics

*Burkhard Stiller*
*Thomas Bocek*
*David Hausheer*
*Cristian Morariu*
*Peter Racz*
*Gregor Schaffrath*
*Martin Waldburger*
*(Eds.)*

# Communication Systems I

TECHNICAL REPORT – No. ifi-2006.09

August 2006

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

B. Stiller, T. Bocek, D. Hausheer, C. Morariu, P. Racz,
G. Schaffrath, M. Waldburger (Eds.):
Technical Report No. ifi-2006.09, August 2006
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.unizh.ch

# Introduction

The Department of Informatics (IFI) of the University of Zürich, Switzerland works on research and teaching in the area of computer networks and communication systems. Communication systems include a wide range of topics and drive many research and development activities. Therefore, during the summer term SS 2006 a first instance of the Communication Systems seminar has been prepared and students as well as supervisors worked on this topic.

The areas of communication systems include among others wired and wireless network technologies, various network protocols, network management, Quality-of-Service (QoS) provisioning, mobility, security aspects, peer-to-peer systems, multimedia communication, and manifold applications, determining important parts of future networks. Therefore, this year's seminar addressed such areas in more depth. The understanding and clear identification of problems in technical and organizational terms have been prepared and challenges as well as weaknesses of existing approaches have been addressed. All talks in this seminar provide a systematic approach to judge dedicated pieces of systems or proposals and their suitability.

## Content

This new and first edition of the seminar entitled "Communication Systems I" discusses a number of selected topics in the area of computer networks and communication systems. The first talk on "QoS in WLAN 802.11 Networks" gives an overview of Quality of Service extension for IEEE 802.11 wireless networks. Talk two on "Comparison and Applications of Short-Range Wireless Technologies" summarizes short-range wireless technologies, like Bluetooth, infrared (IrDA), WLAN, and RFID. "Trusted Computing – Blessing or Danger?" as talk three gives an introduction to and discusses trusted computing. Talk four on "Metro Ethernet" presents the Metro Ethernet network technology for metropolitan area networks. Talk five on "Autonomic Computing" provides an overview of autonomic computing and discusses its potentials and risks. The sixth talk on "NSIS - Signaling in IP Networks" presents and summarizes the work towards a common signaling protocol for IP-based applications.

Talk seven on "Voice over IP (VoIP) Protokolle" discusses various protocols for voice communication in IP networks, including SIP, IAX2, and H.323. "Instant Messaging and Beyond – An Overview and Outlook in Direct Corporate Communications" as talk

eight addresses instant messaging systems in corporate communications. Talk nine on "IP Multimedia Subsystem (IMS)" provides an introduction to the multimedia system for next generation mobile telecommunication systems. Talk ten on "Security in Peer-to-peer Systems" outlines security concerns and aspects in peer-to-peer systems. Finally, talk eleven on "IPv6 – An Architectural Overview" presents the next generation IP protocol.

## Seminar Operation

Based on well-developed experiences of former seminars, held in different academic environments, all interested students worked on an initially offered set of papers and book chapters. Those relate to the topic titles as presented in the Table of Content below. They prepared a written essay as a clearly focused presentation, an evaluation, and a summary of those topics. Each of these essays is included in this technical report as a separate section and allows for an overview on important areas of concern, technology architectures and functionality, sometimes business models in operation, and problems encountered.

In addition, every group of students prepared a slide presentation of approximately 45 minutes to present its findings and summaries to the audience of students attending the seminar and other interested students, research assistants, and professors. Following a general question and answer phase, a student-lead discussion debated open issues and critical statements with the audience.

Local IFI support for preparing talks, reports, and their preparation by students had been granted from Thomas Bocek, David Hausheer, Cristian Morariu, Peter Racz, Gregor Schaffrath, Martin Waldburger, and Burkhard Stiller. In particular, many thanks are addressed to Peter Racz for his strong commitment on getting this technical report ready and quickly published. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of communication systems, both for all groups of students and supervisors. Many thanks to all people contributing to the success of this event, which has happened in a lively group of highly motivated and technically qualified students and people.

*Zürich, August 2006*

# Contents

**1 Quality of Service in WLAN 802.11 Networks** **7**

*Stephan Blatti, Viviane Cantaluppi, Ueli Hofstetter*

**2 Comparison and Applications of Short-range Wireless Technologies** **41**

*Philipp Kräutli, Stéphanie Eugster, Matthias Alder*

**3 Trusted Computing – Blessing or Danger** **75**

*Richard Meuris, Claude Humard, Philippe Hochstrasser*

**4 Metro Ethernet** **113**

*Stefan Weibel, Maik Lustenberger, Roman Wieser*

**5 Autonomic Computing** **143**

*Veronica Garcia, Lukas Knauer, Christophe Suter*

**6 NSIS - Signaling in IP Networks** **177**

*Matthias Altorfer, Daniel Heuberger, Manuel Innerhofer*

**7 VoIP Protokolle** **207**

*Somala Mang, Christian Signer, Baer Jonas*

**8 Instant Messaging and Beyond - An Overview and Outlook in Direct Corporate Communications** **239**

*Marcel Lanz, Philipp Toggweiler, Thomas Rüegg*

**9 IMS – IP Multimedia Subsystem** **275**

*Danar Barzanji, Marcel Steffen, Roger Trösch*

**10 Sicherheit in Peer to Peer Netzwerken** **309**

*Amir Sadat, Christoph Gow, Adrian C. Leemann*

**11 Internet Protokoll Version 6** **343**

*Norbert Bollow, Thomas Rauber, Tobias Wolf*

# Chapter 1

# Quality of Service in WLAN 802.11 Networks

*Stephan Blatti, Viviane Cantaluppi, Ueli Hofstetter*

*In communication systems, the Quality of Service offered by the underlying technology and protocols is one of the most important properties. If it is not possible to setup a separate communication channel between two entities, there is always the same problem: how to coordinate the access of multiple entities to this channel regarding their needs of service quality. While this problem is solved in wired networks through Integrated Services and Differentiated Services, two architectures which guarantee Quality of Service, there is no accurate technique to be used for wireless systems. Together with the increasing importance of mobile computing also the need of Quality of Service for wireless communication is growing. That is why this paper focuses on the proposed IEEE 802.11e standard, which aims to offer the possibility to prioritize and parameterize traffic streams in order to allow QoS deployment in 802.11-based wireless environments. This paper gives first an introduction to the basics of Wireless LAN Communication and the already existing Quality of Service solutions . Then it shows the limitations of the applied techniques and presents the improvements made by the 802.11e standard.*

# Contents

**1.1 Introduction to Quality of Service in WLAN . . . . . 9**
1.1.1 MAC – Media Access Control . . . . . 9
1.1.2 Wireless (802.11) . . . . . 10
1.1.3 Frame format . . . . . 14
1.1.4 Quality of Service – QoS . . . . . 16
**1.2 Limitations of 802.11 for QoS . . . . . 19**
1.2.1 General Limitations . . . . . 19
1.2.2 Distributed Coordination Function . . . . . 20
1.2.3 Point Coordination Function . . . . . 21
1.2.4 Connection through the Access Points . . . . . 23
1.2.5 Data Frames . . . . . 24
1.2.6 Acknowledgments and lost of data . . . . . 25
**1.3 802.11e – Solutions of QoS . . . . . 26**
1.3.1 Introduction . . . . . 26
1.3.2 Traffic Prioritization – Prioritized QoS . . . . . 26
1.3.3 Traffic Parameterization – Parameterized QoS . . . . . 29
1.3.4 HCF – Hybrid Control Function . . . . . 32
1.3.5 Advantages of HCF . . . . . 33
1.3.6 General performance improvements . . . . . 33
**1.4 Summary . . . . . 35**
**1.5 Conclusion . . . . . 36**
**1.6 Annex . . . . . 36**

## 1.1 Introduction to Quality of Service in WLAN

To start with, it might be better to give an intro and explanation to already known terms within the area of wireless networks, in order to familiarize the reader with the topic. All these definitions are based on [5] and [6]. A broader set of definitions used in this document can be found in the Annex, at the end of this paper. After the first rather theoretical section, several limitations of 802.11 for Quality of Service are shown. Section 1.3 describes solutions for the QoS problem as proposed in the 802.11e standard. A summary of the topic and a conclusion is added at the end of the paper.

### 1.1.1 MAC – Media Access Control

The MAC is a lower sub-layer of the OSI data link layer and acts as an interface between Logical Link Control and Physical Layer. The importance of the MAC sub-layer comes from its functions. To be more specific, the MAC is in charge of:

- Recognition of beginning and ending of frames received by the physical layer.
- Rate-limiting of frames for sending.
- Detection of transmission errors by using checksums within frames (recalculation and comparison on receiver side).
- Insertion of source and destination MAC addresses into frames.
- Frame filtering by stations based on source/destination address of frame.
- Control of physical transmission medium.

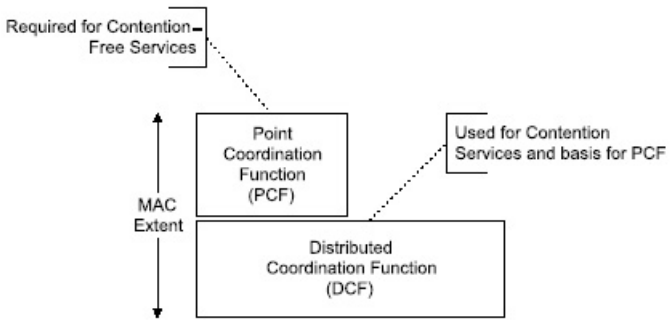



Figure 1.1: MAC architecture [4]

As shown in Figure 1.1, the MAC architecture contains two functions which control the access to the medium. They are described as follows.

**Distributed Coordination Function:** DCF is used by the MAC Layer for sharing the medium between stations in WLANs. It relies on CSMA/CA (find an explanation in the

Annex section), which allows nodes to listen to others before transmitting, for sharing the medium with other stations.

The main problems of this method are listed below:

- Many collisions might occur thus lowering the available bandwidth.
- There is no notion of high or low priority traffic.
- The station which gets access, can keep this access as long desired so other stations might have to wait for a long time before being able to send.
- Generally spoken, there are no QoS guarantees.

**Point Coordination Function:** PCF is a coordination function which is only optionally available. This MAC technique exists in wireless networks which are connected through an **AP** (a central node called Access Point). The AP sends 'beacon' frames at fixed time intervals, and within these intervals the PCF defines two periods: Contention Free Period **CFP** and the Contention Period **CP**. In the latter, only DCF is used. Within CFP, a poll is sent by the AP to allow permission for sending a packet. Thus AP acts as a coordinator, which leads to a better management of QoS. The AP, located 'in the middle' of the wireless network, is seen by all nodes. PCF has some limitations for offering strong QoS support such as the lack of definition of different classes of traffic.

**Fragmentation:** Within the MAC, for increasing reliability and therefore the possibility for successful transmission, fragmentation takes place. It divides MAC service data units into smaller MAC level frames. The process of putting them back together is called defragmentation.

**Positive Acknowledgement:** When sending and receiving frames, positive acknowledgement is used. The receiving STA (station) has to respond with an acknowledgement (ACK frame) when the received frame is correct. More details about this technique can be found in Section 1.2.3.

### 1.1.2 Wireless (802.11)

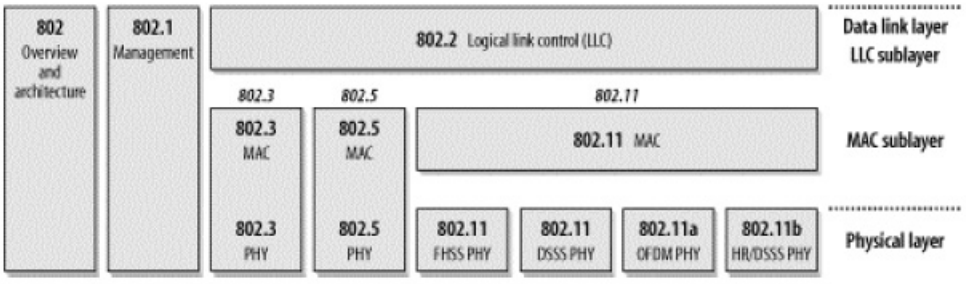



Figure 1.2: 802 Standards Family [4]

In Figure 1.2, an overview of the IEEE 802 standards family is given. Furthermore, IEEE 802.11 sets standards for WLANs, which define methods for sending signals through the air within a limited area (buildings or campuses), with the challenge of mediating access to shared communication medium. There exist several standards in this family, all with service enhancement, extensions or corrections to previous ones. The original standard includes a proposal for CSMA/CA as media access method. One problem was that there existed too much inoperability, therefore it needed to be supplemented. The current version is radio-based with *spread spectrum*. The idea of spreading the signal over a wider frequency than normal is to minimize the narrowband interference from other devices. One type of spread spectrum technique is called *Frequency Hopping* which transmits the signal over a random sequence of frequencies. These random frequencies are actually generated by an algorithm which is used by both sender and receiver. (They hop frequencies synchronously for correctly receiving the frame.) Another type of spread spectrum is called *Direct Sequence*. It represents each bit in the frame by multiple bits in the transmitted signal. It sends a signal which is made by XOR-ing the original bit with n random bits called chipping sequence (again, they are generated). 802.11 defines two physical layers, one with frequency hopping and the other with direct sequence. Another physical standard for 802.11 exists, based on infrared signals, but its range is limited to the interior of buildings [6].

**802.11a:** This standard works within the 5 GHz frequency band. It uses the core protocol and uses an orthogonal frequency-division multiplexing. It has the advantage of having less interference, because not many use this frequency band. The main disadvantage is the restricted to line of sight. This standard is mainly used in the United States [3].

**802.11b:** The 802.11b standard works in the 2.4 GHz band, where the problem of interference through microwaves, mobile phones, Bluetooth exists, because they all use the same frequency band. This standard, as well as standard 802.11a, achieves a higher throughput than the original. It uses same CSMA/CA media access method. This one became rapidly accepted as a wireless LAN technology, because upgrades were easily possible and chip prices were reduced [3] [5].

**802.11e:** This standard was released in late 2005, with new QoS enhancements for LAN applications such as Voice over IP and multimedia streaming. This standard aims to improving the MAC layer. As already said before, the basic MAC layer uses DCF and PCF as coordination functions, but the latter is only available in networks connected through Access Points (AP). Within 802.11e, DCF and PCF are getting better through a coordination function: HCF (Hybrid Coordination Function), with two methods of channel access. First one is the HCF Controlled Channel Access (HCCA) and the second one is Enhanced DCF Channel Access (EDCA). Both define Traffic Classes (TC) with lower and higher priority classes for different tasks.

**EDCA:** Traffic with high priority gets a better chance to be sent than traffic with low priority. Therefore, a station containing high priority traffic waits less time for sending packets than a station containing low priority traffic.

**HCCA:** The HCCA is comparable to the contention free period of PCF, because the Hybrid Coordinator (HC) controls the access to the medium during the CFP, whereas during the CP all stations work in EDCA. More detailed information to the subject on

EDCA and HCCA is given in Section 1.3. HCCA might be the most advanced coordination function, where QoS gets great precision. If QoS is enabled within a station, the request of specific transmission parameter is possible which gives a certain higher work efficiency on networks for applications such as VoIP or video streaming [9].

Complementary to HCCA and EDCA, additional optional protocols are specified for MAC layer QoS such as Automatic Power Save Delivery (APSD), Block Acknowledgements (BA) or Direct Link Setup (DLS). More information about this protocols will be given in Section 1.3.6.

**Difference between Wireless and Ethernet:** A wireless network protocol differs from an Ethernet protocol because it can not just go along with the same algorithm (wait for idle link, transmit and retry if it fails). In wireless networks, there is the problem that nodes do not necessarily have to be within reach of each other, they lack of full connectivity. Additionally to that, the physical layer differs within 802.11 from wired networks. The stations are not protected from outside signals, they communicate over a less reliable medium and they have dynamic topologies [6]. That is why approaches to QoS are not the same ones (see the Limitations Section 1.2 and Solutions Section 1.3).

**Architecture:** As shown in the Figure 1.3 several components are needed to build a WLAN that supports station mobility to upper layers. BSSs (basic service set) are the basic building block of 802.11. STAs (station) 1 to 4 are stations that are members of the BSS and communicate within the BSS (oval cycles). For interconnection of multiple BSSs, a distribution system DS is needed that provides support for handling address mapping and integration of multiple BSSs. Access Points (AP) are stations that provide access to wireless STAs to DS. Therefore, data moves between BSS and DS via an AP. Extended service set (ESS) network type is possible which means that DS and BSS allow 802.11 to create a large wireless network. Stations within such a network may communicate and mobile stations are able to move within the same ESS. For integrating an 802.11 network into a wired LAN, a portal (logical point) is needed. 802.11 specifies services within the stations (SS) and within the distribution system (DSS). These services are used by the 802.11 MAC layer. Station services SS are present in every station, including APs, and contain authentication, deauthentication, privacy, and MSDU delivery. Distribution system services DSS are used to cross media and address space boundaries. They are provided by the DS and accessed via the STA. They contain association, disassociation, distribution, integration, and reassociation.

To mention the difference to Ethernet one more, so called *hidden nodes* may exist within a WLAN. These are nodes which cannot 'see' each other. If two hidden nodes send a signal to a third one, a collision might occur, since the two do not know about each other. Therefore, the MACA mechanism is used: idea of exchanging control frames before sending actual data. Another difference is the *exposed node problem*, which appears when a node sees a transmission that was not meant for him and thus can not transmit during that perion. The surrounding nodes get an information that a transmission is about to start. A *Request To Send* (RTS) frame is sent for asking of transmission possibilities, including the length of the data frame to be transmitted to get a proper time amount for sending. The receiver sends a *Clear To Send* (CTS) frame for giving the permission. If any node sees the CTS frame, it is clear that transmission only possible for the specified

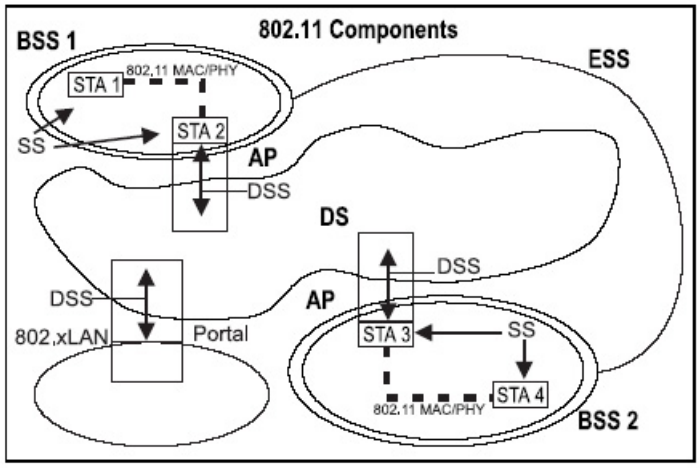



Figure 1.3: IEEE 802.11 architecture [4]

station. On the other hand, if a node only gets the RTS frame, then it is obvious for being close to the sender and not the receiver, and therefore is able to transmit. If the receiver got the frame, it sends an ACK for success which all nodes have to wait for before transmitting. If a collision occurs of two RTS sent at the same time, the collision is not detected immediately (as CA is used instead of Collision Detection CD) but when the CTS does not arrive. Then the sending stations wait a random time and send again. This time is defined by exponential backoff algorithm, same as in Ethernet. (This backoff algorithm is used to schedule retransmission after a collision.)

In ad-hoc configuration, also called independent BSS as shown in Figure 1.4 the wireless network only consists of stations connected with each other (at least two stations are needed). Therefore the ad-hoc architecture differs as it does not contain an AP. Ad-hoc configurations are used for a specific purpose and for a short period of time [3].

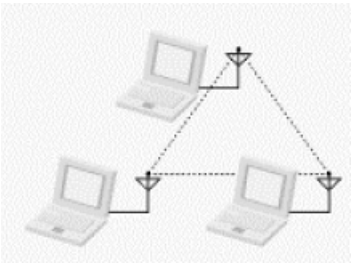


Figure 1.4: Architecture of an independent BSS [3]

Getting back to the BSS architecture, the importance of nodes communicating with an AP before 'talking' to each other was already mentioned. 802.11 specifies the selection of APs and movement of nodes. The AP selection technique is called *scanning*. A node sends probe frames and gets probe response frames as answers from all APs within reach. The node picks one AP and sends an Association Request frame, while the AP replies with an Association Response frame. The whole time, nodes are looking for APs and might change them when getting a better signal of another AP. This is called *active* scanning, where the node is free to change APs any time. *Passive* scanning happens when APs send so

called beacon frames to advertise their capabilities of access point, and then nodes might change to better APs when sending an Association Request frame to the access point.

**Interframe Spacing:** For coordination of access to medium, interframe spacing is important. The different interframe spaces are used to determine medium access priorities. This mechanism is used for the realisation of CSMA/CA. In CA mechanism, transmissions always wait for idle medium. Interframe spacing now creates different priority levels for different traffic. Therefore, high-priority traffic does not have to wait as long as the lower-priority traffic, because it grabs the idle medium first. Four different interframe spaces exist (as seen in Figure 1.5):

**Short interframe space SIFS:** It is used for highest-priority transmissions, such as RTS/CTS/ACK. These transmissions are allowed to start once the SIFS has elapsed.

**PCF interframe space PIFS:** It is used by the PCF during the contention-free operation. Stations that want to transmit in the contention-free period are able to do so when the PIFS time has elapsed.

**DCF interframe space DIFS:** This is the minimum medium idle time.

**Extended interframe space EIFS:** This is not a fixed one, only used if an error occurs within the frame transmission.

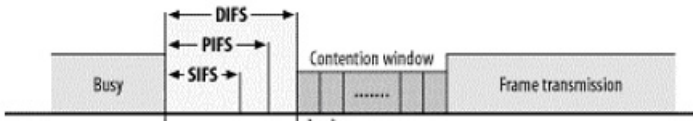



Figure 1.5: Interframe Spacing [3]

### 1.1.3 Frame format

Each frame consists of a MAC header, a variable length frame body, and a frame check sequence (FCS) with a cyclic redundancy code (CRC). An overview of the MAC frame format is given in Figure 1.6.

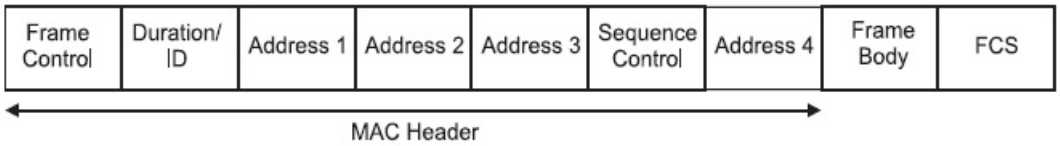



Figure 1.6: MAC frame format [4]

The *frame control field* (16 bit) consists of several subfields, such as protocol version, type, subtype, to DS, from DS, more fragments, retry, more data and so on. A visual overview is given in Figure 1.7.

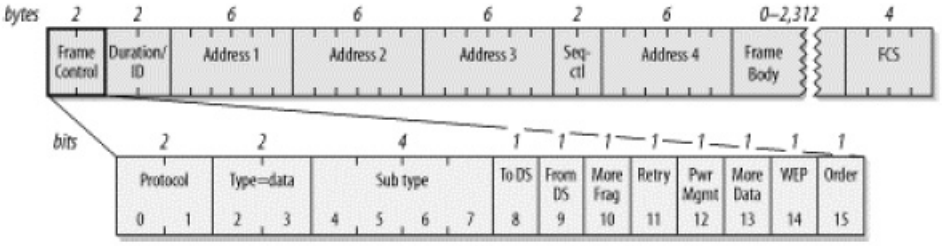



Figure 1.7: Frame control field [3]

In detail, the *Protocol* version field states the version of the 802.11 MAC contained in the frame. The *Type* field stands for the type of frame used. The *Subtype* fields identify the request to send (RTS) and the clear to send (CTS) operations as well as the acknowledgements (ACK). *To DS / From DS* indicated whether the frame is meant for the distribution system or not. Other fields contained here are the *retry* bit (is set when a frame is retransmitted), *power management* bit (for power save mode) and WEP bit for protection and authentication.

The *duration / ID* field (16 bit in length) carries the association identity (AID) of the station that transmitted the frame.

*Address fields*, four in total, are used for the source address SA, destination address DA, transmitting station address TA, and receiving station address RA. These four addresses are needed when a frame is forwarded through a distribution system. In the best case, when sending from one node to another, Addr1 identifies the target node and Addr2 the source node. In the worst case, when a message goes from a wireless node through the distribution system to another wireless node, Addr1 identifies the ultimate destination (DA), Addr2 identifies the immediate sender (the AP that sent frame to ultimate destination) (RA), Addr3 identifies the intermediate destination (AP that sent frame through distributed system) (TA), and Addr4 identifies the original source (SA).

*Sequence Control field* (16 bit) consists of the Sequence Number (12 bit) and the Fragment Number (4 bit), as shown in Figure 1.8.

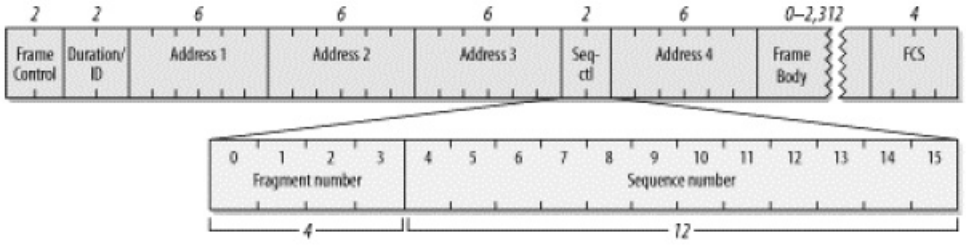



Figure 1.8: Sequence Control field [3]

The *frame body* (variable) contains information about frame type.

The *FCS field* (32 bit) contains the CRC (cyclic redundancy check with underlying mathematical operations). It allows checking the integrity of received frames. In the FCS, all

fields of the MAC header and the frame body are included, and afterwards the access points recalculate the whole FCS [3], [4], [6].

### 1.1.4 Quality of Service – QoS

Although multimedia applications (audio, video and data) can be transmitted through a packet-switched network with a wider bandwidth or faster link speed, today much more is needed. For example, applications have to be sensitive to the timeliness of data in order to get real-time reaction from the user (real-time applications). From the network, they need therefore an assurance that data arrives on time. Because the network and not only the hosts need to provide timely arrival, a new service model is needed where applications can ask for higher service quality assurances. If the network supports that, then it will treat some packets differently than others. A network providing this kind of different level of service is said to support Quality of Service (QoS) [6].

Until recently, QoS was not a big issue, but nowadays it is because certain problems might arise when packets travel from sender to receiver such as [5]:

- Dropped packets: if a router's buffer is full for example, the delivery of packets is not guaranteed, because it might 'drop' packets. The receiver has to make sure that the information is retransmitted and this can cause delays in the total transmission.
- Delay: is a very unpredictable, because packets might wait in queues or take a longer paths while reaching the receiver.
- Jitter: packets arrive with different delays, an effect which is known as jitter. This affects the quality of video or audio streams.
- Out-of-order delivery: packets might arrive in a complete different order than they were originally sent. Therefore, special protocols are needed for rearranging those packets when they reach the destination.
- Error: packets might be wrong directed, combined or corrupted. Then, the receiver has to ask for retransmission again (as if the packet was dropped).

In general, for different types of network traffic, special QoS is needed (*Applications*):

- Multimedia stream needs guaranteed throughput
- IP telephony or VoIP do not need jitter or delay
- Video Teleconferencing needs low jitter
- Safety-critical applications (surgery) need availability.

So to speak, there exist real-time and non-real-time applications. Non-real-time applications, such as FTP or eMail, do not need a guarantee of timely delivery whereas real-time applications do. The following example is a real-time audio application: sound gets converted from an analog-to-digital converter and the packets are transmitted through the network. At the receiving host, the data needs a certain playback time, the point of time when the receiving host needs the data. If a packet arrives late, because of delay or being dropped, it is useless. Real-time applications have the characterisation of late data being complete worthlessness. To make a voice application work, it would be nice of all packets take exactly the same amount of time for traversing the network, but this is very difficult to guarantee. Therefore, a buffer is needed at the receiver side, to buffer up some amount of data in reserve to be allow the audio to be played at the right time. The size of this delay in playing back depends on the use of the audio data. During a conversation, a smaller playback time is wanted. So if data is early, the buffer keeps it until the correct playback time, but if it is late there is no use for it. Real-time applications can be divided in different classes. The tolerance of loss of data is one characteristic. Applications are *loss tolerant*, if they can afford to loose some packets. *Intolerant* ones can not tolerate occasional loss, they need all packets because they are all important for the application. Another characterisation is the adaptability of real-time applications, meaning being able to *adapt* to the amount of delay of packets (i.e. being able to shift the playback time). If an application can adjust their playback time, it is called *delay-adaptive*. If an application is *rate-adaptive*, it is able to trade-off between bit rate and quality [6].

A service model with several classes is needed, to cover all the needs of these applications, i.e. develop a range of service quality. The already developed range of QoS can be divided into two broad categories: *fine-grained* approaches which provide QoS to individual applications and *coarse-grained* approaches which provide QoS to large classes of data or traffic. In the first one we find 'Integrated Services', often associated with Resource Reservation Protocol (**RSVP**) and in the second one is 'Differentiated Services'. ATM is known for providing a set of QoS capabilities and is considered in the fine-grained category (definition see Annex Section). The following sub-sections are based on [6]:

**Integrated Services (RSVP):** In networks this is an architecture that specifies elements to guarantee QoS in data transmissions. One service class is made for applications that require packets never arriving late. For example, this is used for videos and sound reaching the receiver without interruption. The network guarantees the maximal delay and the application sets the play back time for no packet being late. If a packet arrives early, the buffer takes care of it by keeping it within the buffer until its point of time to be sent has arrived. This service is called *guaranteed* service. Another service is known as *controlled load*, which emulates lightly loaded networks for applications that request the service, to keep the load low. To implement a network that provides these services to applications, some key mechanisms are needed:

- Flowspecs: the network is not only told where the packets need to go, but about the type of service is required and about the kind that is put into the network (for need of resources). This provided information is called *flowspec*.
- Admission Control: when asking for a service, the network needs to decide whether it can provide that service or not. This process of deciding is called *admission*

*control.*

- Reservation Protocol: for telling other users and components of the network about service, flowspecs, and admission control, a mechanism is needed, which is the process of *resource reservation* (that is provided by the Resource Reservation Protocol).
- Packet Classifying and Scheduling: when flows, requirements and admission control are set, network switches and routers need to meet these requirements. A key part of this is managing the way packets are queued and scheduled for transmission; this mechanism is called *packet scheduling.*

Many internet providers do not feel about IntServ being the right model because of the scalability. While routers only keep up by moving more bits per second and dealing with larger routing tables, RSVP raises the possibility that every flow might have a reservation, which leads to greater need of storage and periodical refreshing. Therefore the router would need to classify, police, and queue each of these flows. These scalability concerns have prevented the widespread of IntServ, and other approaches were developed:

**Differentiated Services (EF, AF)**

In large networks this method guarantees QoS. One approach of differentiated service divides the traffic into two classes, so called 'premium' and others. Instead of using RSVP to tell the router that a flow is sending premium packets, it is easier for packets to identify themselves when arriving at the router. If a packet enters a DiffServ router, the sender sets the 'type of service' field in the IP header, i.e. better classes get higher numbers. This can be done by using bit 1 for premium and 0 for packet with best effort. The router has to give priority to highest value of 'type of service' field. But, who sets the premium bit and under what circumstances? A common approach is to set the bit by a router that sits between the internet provider's network and another network. This might be useful if the internet provider gets paid for a higher level of service quality. What does a router do if he gets a premium packet? It is needed more than just one bit to tell the router what to do with the packet. Six bits are used out of the old TOS byte which identifies a particular PHB applied to the packet. *Expedited forwarding* EF means that packets should be forwarded by the router with minimal delay and loss. Another PHB is *assured forwarding* that provide customers with high assurance that packets can be delivered.

This more currently accepted approach of differentiated services, works by marking packets due to their type of service they need. Routers and switches use these markings for special queuing strategies to fit performance requirements. Other DiffServ models 'allocate resources to a small number of classes for traffic' [6].

The QoS in ATM (more about this subject can be read in [6] chapter 6.5.4) is similar to the one in an IP using IntServ. While IntServ provides three classes (best effort, controlled load and guaranteed service), ATM comes up with five classes:

- Constant bit rate *CBR*
- Variable bit rate - real-time *VBR-rt* (like guaranteed service)

- Variable bit rate - non-real-time *VBR-nrt* (like controlled load service)
- Available bit rate *ABR*: has a set of congestion-control mechanisms.
- Unspecified bit rate *UBR* (like best effort service)

Let us quickly look at the comparison of RSVP and ATM. With RSVP, the Receiver generates reservation, a Soft state (refresh/timeout) exists, QoS can change dynamically and Receiver heterogeneity is given. With ATM, the Sender generates the connection request, a Hard state (explicit delete) exists, QoS is static for life of connection and Uniform QoS to all receivers is given.

## 1.2 Limitations of 802.11 for QoS

The following section mainly relies on [3] and deals with the restrictions of the 802.11 standard relating to Quality of Service. The 802.11 standard is based on and embedded in a technical and social environment. Some aspects of these general limitations for QoS are introduced in the first part. Now, the problems for QoS of the two main functions, the Distributed Coordination Function DCF and the Point Coordination Function PCF are shown. The following topic is about connections through access points, which limits the capacity of the network as well. Because there exist different types of data, the distinction of priority of data is an offered solution. Read for further details in Section 1.2.5. The transmission, especially in a wireless medium, is not guaranteed, therefore the traffic arises with acknowledgments and lost of data, which is described in Section 1.2.

### 1.2.1 General Limitations

Because the MAC and LLC are parts of the Data Link Layer, they are based on the Physical layer, which limits the possible numbers of signals on the chosen medium. This can be seen in Figure 1.9 that shows the OSI model. The 802.11 standard has regulated some details of the Physical Layer, influenced by worldwide governmental restrictions of use of radio frequency, technical constraints and economical costs.

As already mentioned in Section 1.1, two kinds of signalling for wireless communication exist (infrared and radio waves). Both are used for one bit serial transmission so there is no possibility to transmit parallel signals. The direction of use is half duplex. The first standard in 1997 was able to perform 2 Mbps.

As a result of these constraints is obvious that the more stations will be connected to the network, the more its performance will decrease. It is simple to calculate by the formula 2 Mbps divided by the number of stations. In fact is the result far smaller because of managing the stations, which is also done over the wireless medium, and the collisions and retransmission which also decrease the usable throughput. There are further interferences like such with micro ovens and they may lead to loss of signals.

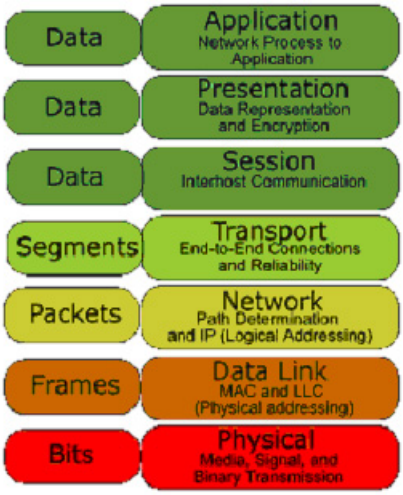



Figure 1.9: The ISO/OSI model

Access to a wired network assumes a connection to the physical medium, i.e. access to the cable. Radio waves transmission is relatively easy to pick up for everybody in the footprint of an AP. So, it is more important to protect the transmissions over the wireless medium to the cost of decreasing performance of the network.

### 1.2.2 Distributed Coordination Function

One problem of the presented situation was to find a process to fairly deliver the data to more than one connected station, called the Coordination Function. In the main function (DCF) every station has in principle the same chance to send or receive a frame. If a STA recognizes that the medium is not idle after DIFS, the backoff algorithm is executed. This function helps to prevent collisions. A backoff window, that opens after the DIFS is divided into slots. The length of slots depends on the physical layer speed and is equal for every slot. It is shorter for faster physical layer. A STA calculates randomly its slot. The STA with the lowest number get the first slot and can transmit before any other STAs. The range of backoff time increases, as shown in Figure 1.10, each time a transmission fails, as in Ethernet.

The 802.11 standard defines backoff time as follows: *Backoff Time = Random() * aSlotTime where Random() = Pseudorandom integer drawn from a uniform distribution over the interval [0,CW], where CW is an integer within the range of values of the PHY characteristics aCWmin and aCWmax, aCWmin <= CW <=aCWmax. It is important that designers recognize the need for statistical independence among the random number streams among STAs. aSlotTime = The value of the correspondingly named PHY characteristic.* In other words, there is no guarantee of delivery on time and so there is actually no QoS.

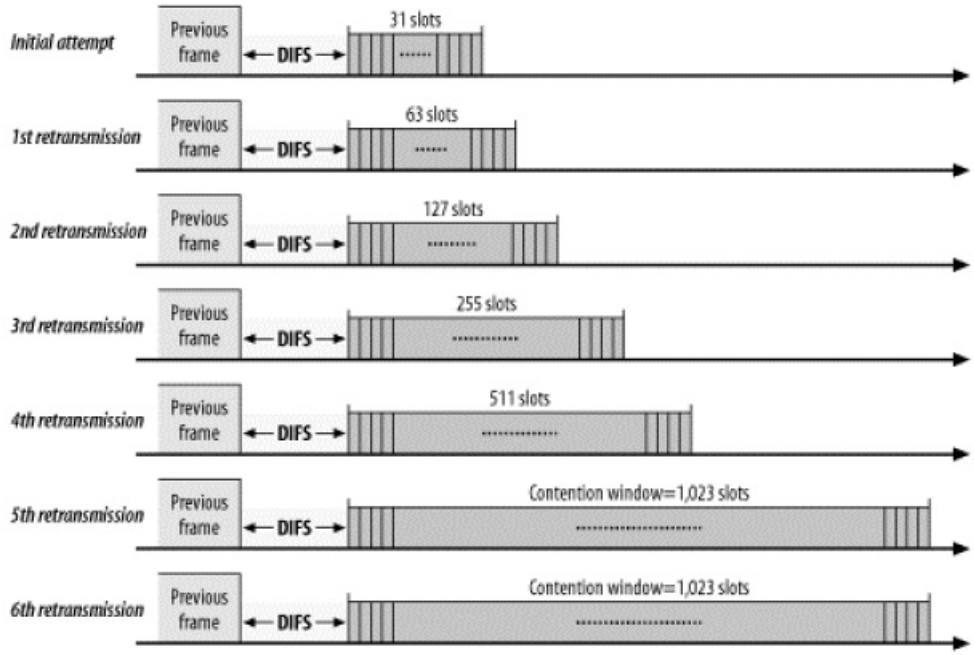



Figure 1.10: Increase of backoff time during retransmission [3]

### 1.2.3 Point Coordination Function

The second optional coordination function provides a mechanism that gives some stations a higher priority. This function is only applicable with infrastructure BSS and its limitation is as strong, that it has never reached a large usage in the practice.

With the success of the 802.11 technologies, additional applications domains required a much better QoS of the wireless network than 802.11 PCF mode could serve. Audio-visual and Voice over IP for example need real-time service of transmission to perform their task. Now, an idea why PCF is unable to solve these tasks appropriately is given (shown in Figure 1.11).

| *Medium* | *Data Rate of Presentation* |
|---|---|
| Speech, telephone quality (PCM) | 64 kbit/s |
| CD quality audio | 172.3 kByte/s |
| Compressed audio 4:1, 37.800 Hz sampling | 43 kByte/s |
| MPEG-1 video | target rate: 1.2 Mbit/s |
| MPEG-2 video (digital video studio) | target rate: 40 Mbit/s |
| Motion JPEG | ~8 Mbit/s (1 audio/video channel) |
| Document imaging | 10 ... 100 MBit/s |
| Scientific imaging | up to 1 GBit/s |

Figure 1.11: Data Rate of Presentation [3]

If PCF is setup within the AP, two periods alternate: the contention period, coordinated by the DCF and on the other side PCF, a span of time without contention. It is possible to configure the relative size of the PCF-period by a network administrator.

The difference to DCF, the contention free period is centrally controlled by a point coordinator (PC), a particular function on the AP. Station in association with the AP can

only transmit frames with the admission of the PC. Main principles of 802.11 DCF transmissions remain in function.

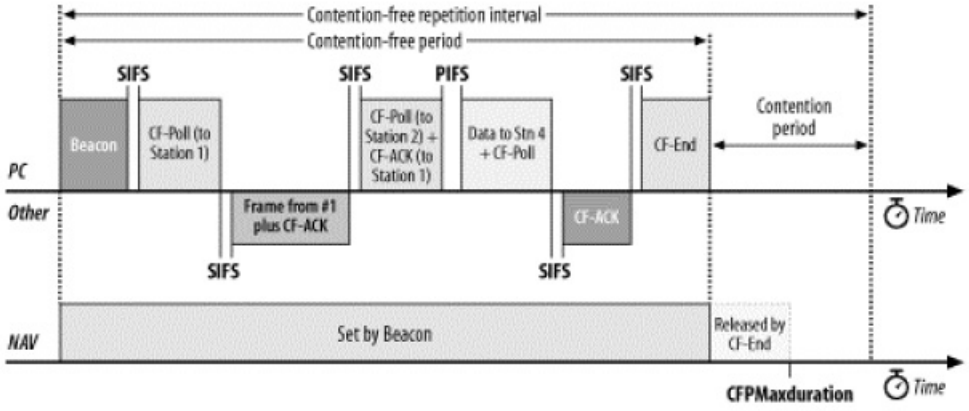



Figure 1.12: DCF transmission [3]

As Figure 1.12 shows, the contention free period starts with a special beacon frame, transmitted by the AP. In there is declared the maximum time of duration for transmission. Every receiving STA sets its Network Allocation Vector (NAV) to this duration. In addition to physical CSMA/CA, 802.11 provides another carrier sensing type: a virtual function called NAV. All stations have to count down the NAV value before they can use CSMA/CA function. The transmission is separated by SIFS and PIFS, so even if a STA hasn't receiving the beacon, it can't access the medium with DIFS.

In the Contention Free Period the PC polls all associated STAs on its Polling List. If a STA receives an adequate polling frame (CF-Poll), it may transmit its data. Normally a STA is permitted to send one frame, except the access point has sent a multiple poll request. STA can register itself as privileged within the Association Request to the network.

**Main Problem in PCF for QoS**

The PCF does not comply for applications with high QoS requirements, because there is no predictable duration of the Contention Free Period. The minimal duration of DCF period is sending one frame. However, the end of DCF can be delayed. The Target Beacon Transmission Time (TBTT) is set for fixed intervals and if the Beacon for starting the PDF period is outstanding on the expected time, the Contention Free Period is shortened about its delay as shown in Figure 1.13.

At TBTT the Beacon Frame is planned to be transmitted. To give control to the AP it has to pass the PIFS. There is a procedure so actually that the delay can arbitrary grow. Fragmentation splits a higher-level packet in fragments. These fragments are sent from the STA in time interval of SIFS, so the AP cannot gain the control over the ESS as shown in Figure 1.14.

Similar problems are found in CFP itself. Every STA on the Polling List will be consulted and all of them may use the fragmentation function. Furthermore, the STA are permitted to switch the physical rate of transmission, so much less data can be sent in the PCF

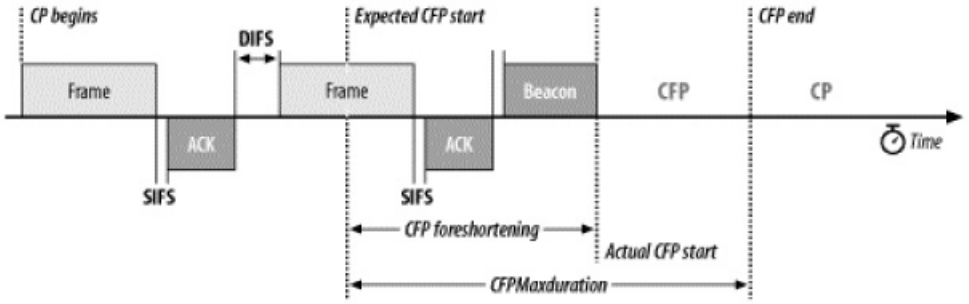



Figure 1.13: Delay shortening [3]

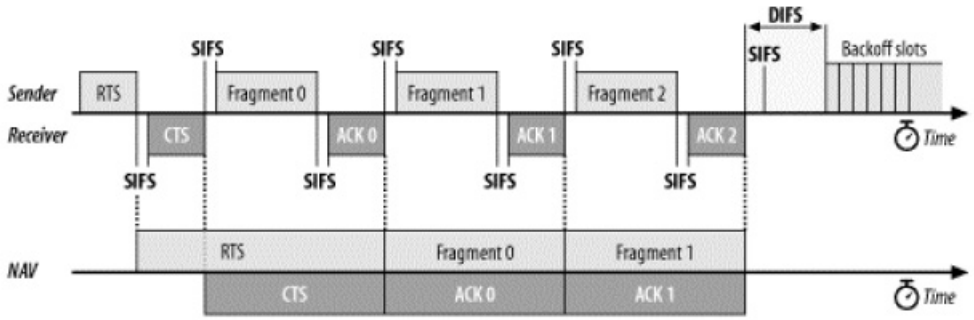



Figure 1.14: Fragmentation [3]

mode. An additional problem is that every STA have to be polled, even if there is no data to send.

### 1.2.4 Connection through the Access Points

As mentioned in the previous Section 1.1, in an infrastructure BSS there is no direct connection between the STAs. Every transmission has to go over the AP and controls every communication in the BSS network. Even if two STAs in the same BSS want to communicate with each other they have to use the AP to relay some data as shown in Figure 1.15.

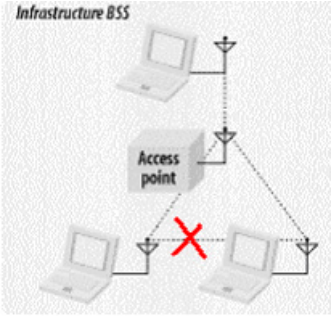



Figure 1.15: Infrastructure BSS [3]

If it would be allowed to make direct connections, the capacity of the network could noticeable grow, but to the cost of much more complexity of the physical layer. In this case STAs would have to manage neighborhood relations in the same BSS.

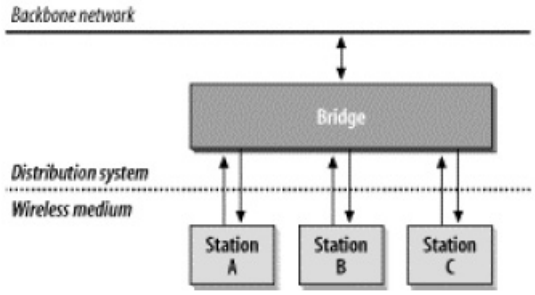



Figure 1.16: Connection through distribution system [3]

It is distinct, that a host on the backbone network has to send its frame over the distribution system. Every STA is also connected trough the distribution system with the network. The only way to send data from station A to station B is using the distribution system (shown in Figure 1.16). There is a bridging engine in the access point, which bypasses the backbone and the BSS network. The bridge is a part of the distribution system.

### 1.2.5 Data Frames

There are three types of major frame types. The most important is the data frame. Data frame carries data from station to station. Data frames are categorized as shown in the following Figure 1.17.

| Frame type | Contention-based service | Contention-free service | Carries data | Does not carry data |
|---|---|---|---|---|
| Data | ✓ | | ✓ | |
| Data+CF-Ack | | ✓ | ✓ | |
| Data+CF-Poll | | AP only | ✓ | |
| Data+CF-Ack+CF-Poll | | AP only | ✓ | |
| Null | ✓ | ✓ | | ✓ |
| CF-Ack | | ✓ | | ✓ |
| CF-Poll | | AP only | | ✓ |
| CF-Ack+CF-Poll | | AP only | | ✓ |

Figure 1.17: Categories of data frames [3]

No other data frames are distinguished. So even if data has not the same priority to send, the 802.11 standard does not differentiate them. For applications with a high QoS

requirement is no particular frame support designated, which can separate the urgent deliveries from the normal ones.

### 1.2.6 Acknowledgments and lost of data

One further special procedure arises from the unreliable principle of transmission. On Ethernet it is appropriate to assume that the data arrives to its destination because of the wired connection between the sender and receiver. In 802.11 there are many reasons why a transmission can fail.

Radio waves frequencies propagate in the ISM band namely in the 2,4 GHz band. Wireless devices have to work within a regulated bandwidth. In the US is this done by the Federal Communications Commission (FCC), in Europe by CEPT European Radio communications Office (ERO) and for Switzerland the Federal Office of Communications (OFCOM/Bakom). These Organisations divide the frequency into bands for different applications such as Broadcasting, Aeronautical Radio navigation, Mobile Phones etc. as shown in Figure 1.18.

**Frequency Allocations Plan**

| Frequency Band | Swiss Allocations | | | | |
|---|---|---|---|---|---|
| | National Allocation | Main Use | Civ/Mil | Notes | Strategy |
| 148.5 - 526.5 kHz | | | | | No changes planned in medium term. |
| 526.5 - 1606.5 kHz | BROADCASTING | Broadcasting primary. | CIV | 531 kHz Beromünster. 558 kHz Monte | |
| | | | | | |
| 2400 - 2450 MHz | FIXED<br>MOBILE<br>Amateur<br>Amateur-satellite<br>5.150<br>5.282 | SRD primary.<br>Amateur secondary.<br>Amateur-Satellite secondary. | CIV | 2400-2500 MHz: ISM-Band.<br><br>2400-2483.5 MHz: Short Range Devices: Non-specific SRDs: RIR1008-11, ERC/DEC/(01)05<br><br>Radio LANs: RIR1010-01, ERC/DEC/(01)07<br><br>Detection of movement: RIR1004-01, | Fixed: No new assignments. |

Figure 1.18: An example of a Frequency Allocation Plan, here is shown that of OFCOM. The Swiss Radio Frequency Spectrum is divided into different bands for various purposes of radio transmission.

Micro ovens work in the same radio frequency spectrum, this indicates why 802.11 radio frequencies are absorbed by water molecules and the receiving in areas with high humidity is worse. A main reason why the 802.11 organization has chosen this band is, it is worldwide free to use (micro ovens electromagnetic propagation has also not to be licensed).

Because of the probability of loss of data, the link layer of 802.11 has to incorporate positive acknowledgments. Every single data frame that is transmitted has to be acknowledged. There is no exception. The process is depicted as shown in Figure 1.19.

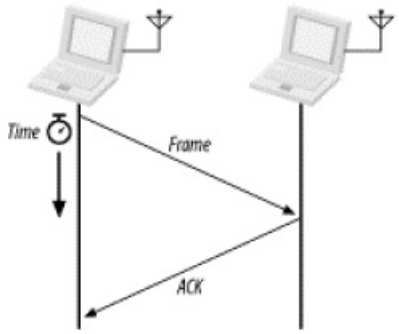



Figure 1.19: Acknowledgment of data frame [3]

This sequence is seen in 802.11 as an atomic operation, so this is treated as a single act without any interruption. Between a frame and its ACK lies a SIFS, so no other STA can get the medium. If an ACK is missing, it is assumed a transmission failure and the send procedure will be repeated.

## 1.3 802.11e – Solutions of QoS

### 1.3.1 Introduction

As mentioned in the previous sections, the MAC functions of the original 802.11 standard are not capable to offer Quality of Service (QoS) in wireless networks. Because QoS becomes more and more important for applications (video, audio), the IEEE 802.11e Task Group [9] defined the new 802.11e standard [10], which should solve this problem. There are two kinds of QoS: first the Parameterized QoS (PaQoS), which satisfies the requirements expressed quantitatively in terms of data rate, delay bound etc. Second, the Prioritized QoS (PrQoS) just guaranties a relative delivery prioritization. In wired networks, both QoS types are already available through algorithms and mechanisms on the network layer. The problem is that they are not applicable in wireless networks, because there is just one transport channel and there are not any routers or other stations which coordinate the traffic. The propoded mechanisms of the 802.11e standard to offer both QoS types and some other innovations to improve the network performance (and help to guarantee higher QoS) will be presented within this paper. This paper will just explain the concepts and not the exact implementation in detail. Fore more information we refer to the IEEE 802.11e standard paper [10].

### 1.3.2 Traffic Prioritization – Prioritized QoS

#### Enhanced distributed channel access – EDCA

The EDCA function of the 802.11e standard is an enhanced version of the 802.11 DCF. The goal of EDCA is to achieve prioritized QoS. In DCF all MAC Data-packets (MACDP)

which should be sent, are stored in one delivery queue using the FIFO principle. It is impossible to handle them according to their priority. As shown in Figure 1.20 in EDCA there are four queues to store MACDPs with different priorities. Each of these queues has an own CW min/max, an own Arbitration IFS (AIFS, equivalent to DCF DIFS), and an own TXOP limit (see 3.4). Each queue tries independently from the others to gain the TXOP. The MACDPs with higher priority are stored in the queue with the smaller average CW and AIFS (which is equivalent to the DIFS in DCF) and a larger TXOP-length. Evidently the chance of this queue to gain a TXOP is much higher, and so their MACDPs are delivered faster. That's the way EDCA provides prioritized QoS.

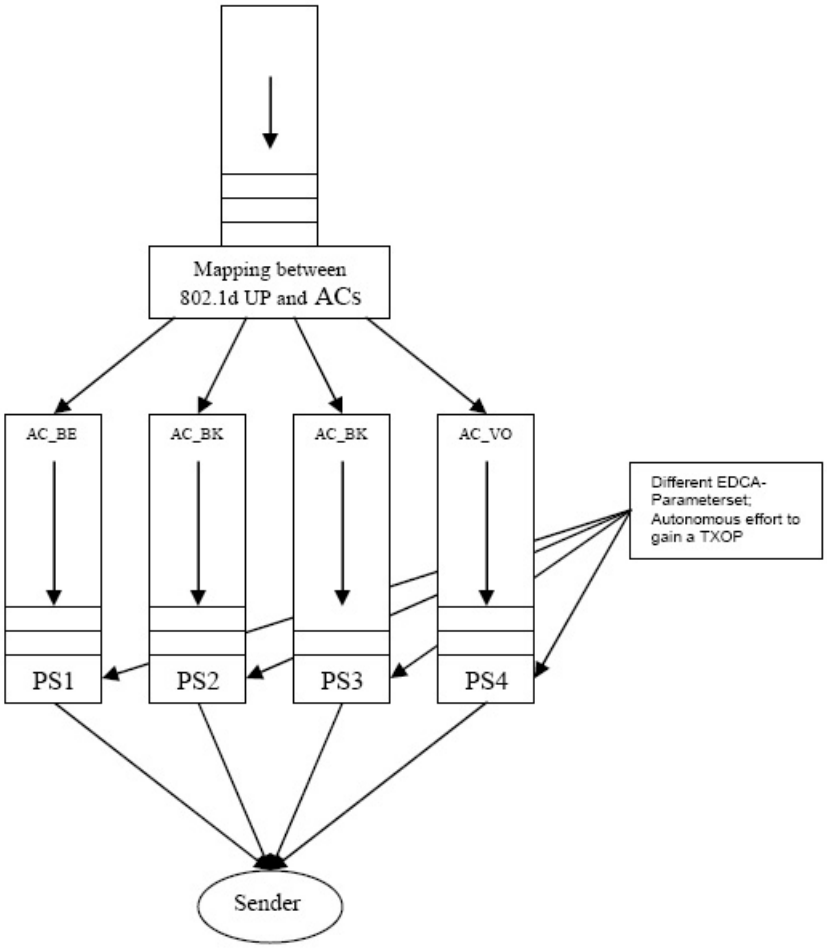



Figure 1.20: Queuing the MACDPs in the Access Classes

The mentioned queues are called Access Classes (AC). Table 1.1 shows their use for different traffic streams. The parameter values of each AC are the same in the whole network. In addition the Hybrid Coordinator (HC, equivalent to the AP in the 802.11 standard) has also the possibility to change those AC values (called EDCA - Parameter Set, shown in Table 1.2). Therefore the HC adds them in a management frame (an enhanced Beacon Frame), which it sends periodically around. Each time the QSTA receives a beacon frame, it updates its parameters. That gives the HC the possibility to react on changed network conditions (modifying the prioritization).

Table 1.1: The Access Classes and their Designation

| Access Category | Designation | Example |
|---|---|---|
| AC-BK | Background | |
| AC-BE | Best Effort | Http |
| AC-VI | Video | Videostreams |
| AC-VO | Voice | VoIP |

Table 1.2: The EDCA - Parameter Set

| AC | CWmin | CWmax | AIFSN | TXOP limit |
|---|---|---|---|---|
| AC-BK | aCWmin | aCWmax | 7 | 0 |
| AC-BE | aCWmin | aCWmax | 3 | 0 |
| AC-VI | (aCWmin + 1)/2 - 1 | aCWmin | 2 | 6.016 or else |
| AC-VO | (aCWmin + 1)/4 - 1 | (aCWmin + 1)/4 - 1 | 2 | 3.264 or else |

**The Mapping between EDCA-Traffic classes and QoS parameters used in other protocols**

The question is now which characteristics of a data packet shall be used to map it into the appropriate AC. The proposition of the IEEE is to use the User Priorities (UP) shown in Table 1.3, which are defined in the 802.1D standard. The 802.1D standard is used for bridging between different 802.x and other standards, where there is no defined direct parameter transformation. For Prioritized QoS (PrQoS) that means that the PrQoS parameters of one standard are mapped in the 802.1D UP and from there, in our case, in an AC. Because an application developer will more probably use UP than the AC we,

Table 1.3: The Mapping between User Properties and Access Classes

| Priority | User Priority | Access Class |
|---|---|---|
| Lowest | Background | AC-BK |
| ⋮ | Best Effort | AC-BE |
| ⋮ | Excellent Effort | AC-BE |
| ⋮ | Controlled Load | AC-VI |
| ⋮ | Video | AC-VI |
| ⋮ | Voice | AC-VO |
| Highest | Network Control | AC-VO |

will give a short survey of the UPs [2]:

- **Network control**: Both time-critical and safety-critical, consisting of traffic needed to maintain and support the network infrastructure, such as routing protocol frames.
- **Voice**: Time-critical, characterized by less than 10 ms delay, such as interactive voice.

- **Video**: Time-critical, characterized by less than 100 ms delay, such as interactive video.
- **Controlled load**: Not time-critical but loss-sensitive, such as streaming multimedia and business-critical traffic. A typical use is for business applications subject to some form of reservation or admission control, such as capacity reservation per flow.
- **Excellent effort**: Also not time-critical but loss-sensitive, but of lower priority than controlled load. This is a best-effort type of service that an information services organization would deliver to its most important customers.
- **Best effort**: Not time-critical or loss-sensitive. This is LAN traffic handled in the traditional fashion.
- **Background**: Not time-critical or loss-sensitive, and of lower priority than best effort. This type includes bulk transfers and other activities that are permitted on the network but that should not impact the use of the network by other users and applications.

As shown in Figure 1.21 information about the UP is stored in the QoS-element of the general MAC Frame [3].

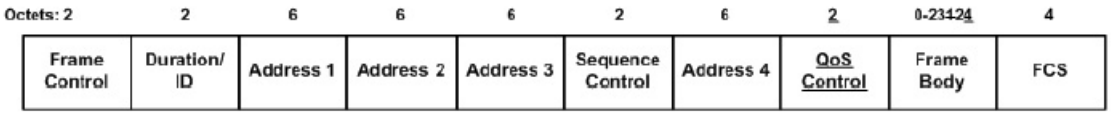



Figure 1.21: The Mac Frame with the QoS element [9]

### 1.3.3 Traffic Parameterization – Parameterized QoS

In this section will be explained how the controlled channel access in PCF can be enhanced to offer parameterized QoS. The Hybrid Coordination will be covered later in Section 1.3.

#### Hybrid coordination function controlled channel access (HCCA)

In HCCA, like in the contention free period of PCF, a Quality of Service Station (QSTA) and its Traffic Stream (TS) have to be registered by the HC, to obtain the right to send (called TXOP in 802.11e) during the CFP. In PCF the AP allocated the right to send without any knowledge of the requirements the stations had. In HCCA every QSTA (and the according Traffic Stream) which intends to be registered by the HC, has to inform the HC about its requirements. The HC allocates the TXOPs according to that information and is thus capable to offer PaQoS. This process is shown in Figure 1.22.

### TSPEC – Specifying the desired QoS

As already mentioned, a QSTA has to specify its requirements in the so called Traffic Specifications (TS). Other than in the PrQoS, where it was only possible to specify the relative QoS, the QSTA has the possibility to ask for an absolute amount of resources.

The most important TSPEC [1]:

- Mean data rate: average bit rate for transfer of the TS (Traffic Stream) packets, in units or bits per second.
- Delay bound: maximum delay allowed to transport a packet across the wireless interface in milliseconds
- Nominal MSDU size: nominal size of the packet, in octets
- User priority: priority to be used for the transport in cases where relative priorization is required
- Maximum MSDU size: maximum size of the TS packets
- Maximum Burst size: maximum size of a data burst that can be transmitted at the peak data rate
- Minimum PHY rate: physical bit rate assumed by the scheduler for transmit time and admission control calculations, in bits per of bits per second.
- Peak data rate: maximum bit rate allowed for transfer of the packets, in units of bits per second.

Using these parameters it is possible to specify exactly the desired QoS.

The QSTA has to send the desired TSPEC to the HC, which checks if it has the capability to guarantee the requested TSPEC or not. If it does, it sends a ACK message to the QSTA, otherwise it enters in negotiations about the TSPEC it is able to provide.

### The mapping between TSPEC Parameters and RSVP parameters

If a QSTA wants to build up a traffic stream to a QSTA in another network, the HC must also check if the route there is able to offer the specified PaQoS. Normally the connection goes through the Internet, and there the already presented RSVP is used for PaQoS, so the TSPEC parameters must be mapped into the RSVP parameters. The 802.11e standard does not propose a specific mapping, but there are external propositions. One example is the proposition of Dimitris Skyrianoglou and Nikos Passas form the Communication Networks Laboratory at the University of Athens [1] shown in Table 1.4.

The RSVP parameters will not be presented in detail here. The reader is referred to the RSVP RFC [8] or other documentation for more information on these.

As one can see the parameters are matching quite well and should be easy to implement.

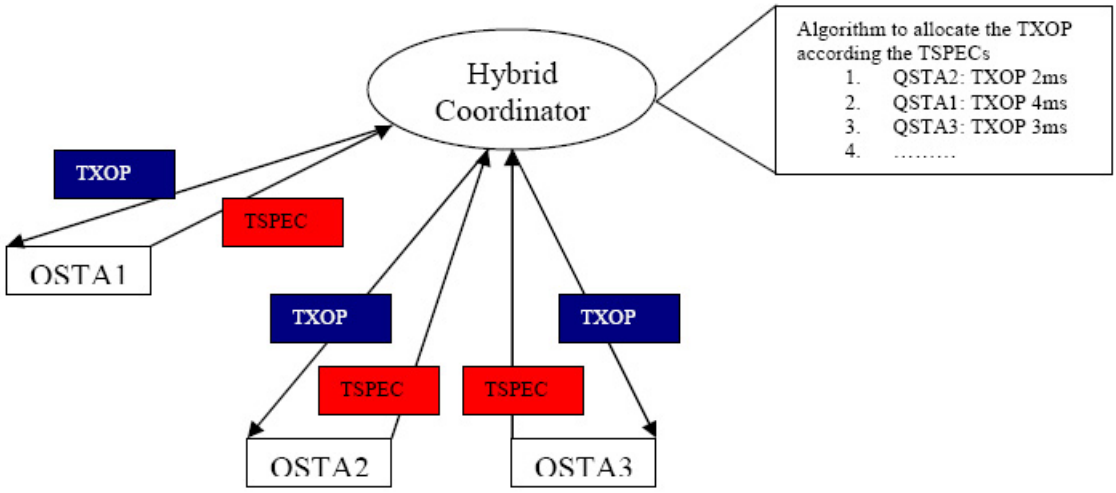



Figure 1.22: The allocation of TXOPs according to the TSPECs

Table 1.4: One proposed mapping between TSPEC and RSVP Parameters

| TSPEC Parameters | RSVP Parameters |
|---|---|
| Mean Data Rate | Bucket rate |
| Peak Data Rate | Peak-Rate |
| Maximum Burst Size | Bucket length |
| Maximum MSDU Size | Bucket length |
| Maximum MSDU Size | Maximum packet size |
| Nominal MSDU Size | Minimum policed unit |
| Peak Data Rate | Desired Rate |
| Delay Bound | Slack Term |

### The TSID

Because the HC must be able to assign an incoming MACDP to a TSPEC it accepted, each TS gets an identifier, the so called Traffic Stream ID (TSID). The QSTA just writes this number in the QoS MACDP field we mentioned, and the HC knows exactly how it has to handle this packet.

### The Transmission Opportunity

One of the most important innovations in the 802.11e standard is the so called Transmission Opportunity (TXOP) that was already mentioned. It guarantees the exclusive access to the transport channel, like in DCF and PCF. But other than in the 802.11 standard, a TXOP allows a QSTA to use the transport channel for a fixed amount of time (and not only to send one MACDP). Because of the variable and unpredictable size of a MACDP (amount of data), this is a precondition for offering QoS.

First of all, this allows giving priority to a TS. The opportunity to send more MACDPs of variable size does not necessary mean the station is allowed to send more data (802.11). But because during the time of a TXOP a QSTA may be allowed to send more than one MACDP, a longer TXOP might also mean as an opportunity to send more data.

For the parameterized QoS, the fixed amount of transmission time a TXOP offers is also very important. Thus the explained effect (multiple frame transmission), the HC knows exactly how much of the guaranteed resources it offers within a TXOP. The other advantage is, that by offering a fixed time to send, the HC is capable to exactly predict when it can allocate the next TXOP (thus minimizing delays).

In EDCA the length of a TXOP is given through the information in the EDCA Parameter Set, in HCCA the HC has the possibility to set the length for every TXOP individually.

### 1.3.4 HCF – Hybrid Control Function

As Figure 1.23 shows, the 802.11e standard allows switching between a Contention Free Period (CFP) and a Contention Period (CP), almost like in PCF. While HCCA is used in the CFP, 'HCCA' and EDCA are used parallel in the CP. So the innovation is that the HC is also able to allocate TXOP during the CP. In the CP, not the originally HCCA mechanism is used (that is why 'HCCA' appears with quotation marks). Because the HC has the right to send immediately after PIFS, it will certainly be the first, and can thus reserve the transport channel. It maybe sends own MACDPs or offers a HCCA TXOP to a QSTA. The HCF combines the presented advantages of EDCA, HCCA and the TXOP. And thus the HC can also gain access the transport channel during the CP and can react whenever network conditions change.

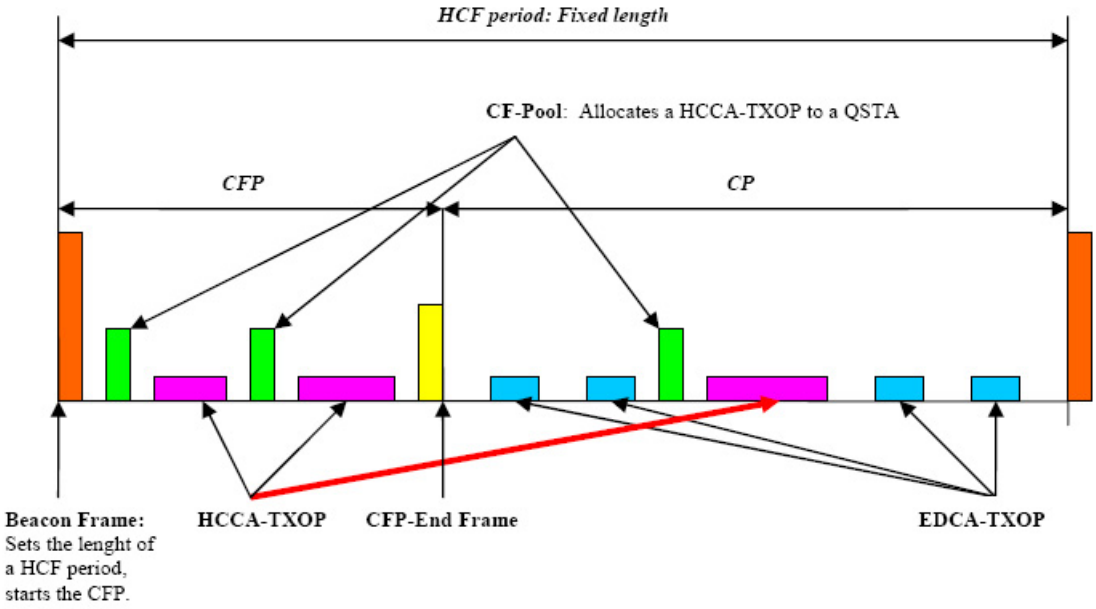



Figure 1.23: The allocation of TXOPs under the control of the HC

### 1.3.5 Advantages of HCF

The assets and drawbacks using HCCA or EDCA exclusively are the same as in 802.11. HCCA offers the better performance than EDCA, because there is no time lost by contending for the TXOP. HCCA is much more difficult to implement than EDCA and thus more expensive.

So why to combine EDCA and HCCA? The reason is probably that not all STAs implement the same 802.11 version a,b,c,d... and therefore use other access mechanisms (and management frames) during the CFP. Fore the HC it is quite difficult to handle so many different kinds of frame types. The mechanism to receive a TXOP during the CP was already the same: try to send. Therefore during EDCA also a non 802.11e STA is able to gain a TXOP in an 802.11e network.

So the HCF combines the network performance of HCCA with the downward compatibility of EDCA.

### 1.3.6 General performance improvements

As already mentioned there are also some new features proposed in the 802.11e standard which can not directly guarantee QoS, but improve efficiency of the network. That is why these are also discussed here.

#### Block acknowledgment

As already explained, if the STA or the AP wanted to send an MACDP in the 802.11 standard, this packet was divided into parts for the reason of reliability and higher efficiency. This was certainly a great idea. But the problem was, that after each fragment, the sender had to wait on a acknowledge message from the receiver, before he could send the next fragment. To reduce this overhead, the 802.11e standard proposes to the so called Block Acknowledgement (BACK). One distinguishes between the immediate BACK mechanism (iBACK) and the delayed BACK mechanism (dBACK).

Using iBACK the sender transmits all packages of a fragmented MACDP without receiving an acknowledgment message for every fragment. At the end it sends a Block ACK Request. If the addressee has received all fragments he sends a Block ACK message. Otherwise it sends an error message in which he tells the sender which packets are lost. If there is already enough time in the TXOP, the sender will send these fragments once again. Else it has to wait until the next TXOP. This mechanism is shown in Figure 1.24.

Maybe the receiver is not able to check the completeness of the received fragment burst before the end of the TXOP. In this case dBACK(shown in Figure 1.25) is may used. The receiver sends a simple ACK-message to the sender. Thus the sender knows that the receiver will send the block acknowledgment latter, probably in the next TXOP.

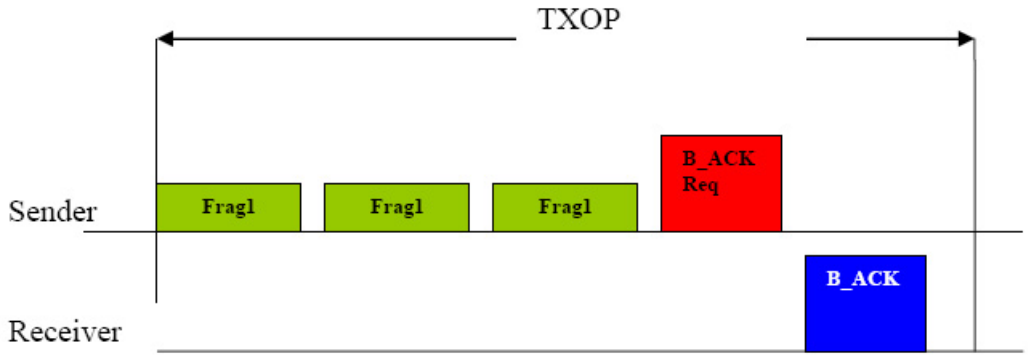



Figure 1.24: The message sequence using iBACK

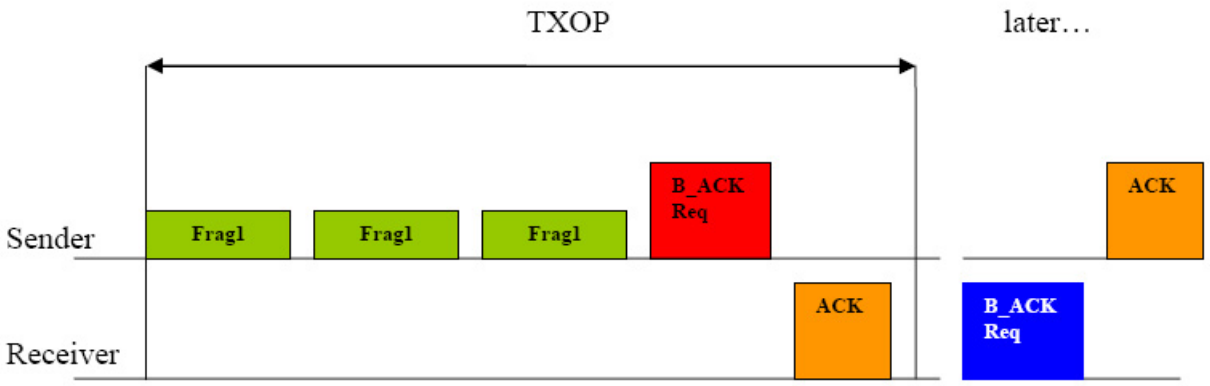



Figure 1.25: The message sequence using dBACK

On one hand, these mechanisms improve the network performance, on the other hand they are difficult to implement and charge the CPU and the Cache. That is why every station has to choose if it wants to use it.

### Direct Link

The 802.11 standard allows the communication of two STAs among each other only over the AP because the sending range of the STAs may be too small to communicate directly. Anyway, in some cases this mechanism was senseless (if the two STA could reach another without a problem). Through this overhead the possible BW for the communication between two stations in the same network was reduced by one half and the AP had also to store a lot of data. That is why the 802.11e standard offers the possibility of a direct communication between two QSTA: The Direct Link (DL), shown in 1.26.

Before MACDPs can be transmitted directly between QSTAs there are a few management operations to be done.

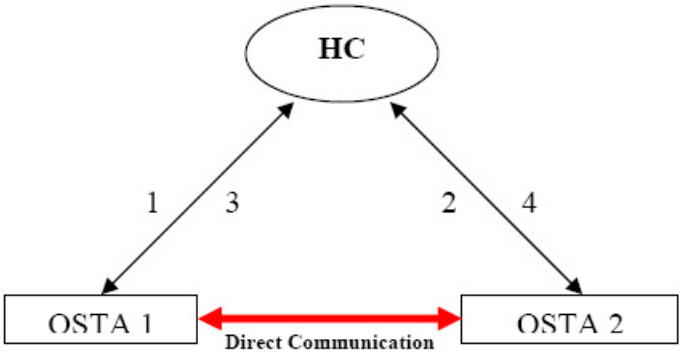



Figure 1.26: Two QSTAs using the direct link

1. QSTA 1, which intends to exchange frames directly with QSTA 2 invokes the DL and sends the DL Request, in which it specifies his capabilities and the MAC address of QSTA 2, to the AP.

2. The QAP forwards the DL Request to QSTA 2.

3. If QSTA 2 accepts the direct stream, it sends a DL response, which extends now the capabilities of QSTA 1 and 2 and their MAC addresses, to the QAP.

4. The QAP forwards the Response Frame to QSTA 1.

The DL becomes active and QSTA1 and QSTA2 are allowed to exchange frames directly. The direct frame exchange is now used whenever QSTA1 or QSTA2 has a TXOP.

Because the direct link frame exchange is much more unsafe then the communication over the AP (because of the higher communication distance) and the main target of 802.11e is to guarantee QoS, the standard defines a timeout mechanism for the DL. The timer counts to zero. After each successful direct transmitted frame, it is reset to the starting time. If the timer reaches zero or a QSTA intents to end the DL, a so called DL Teardown message is send to/from the HC to the QSTA, and informs about the termination of the DL.

## 1.4 Summary

In this paper, an overview to the main topics of wireless network is given. Furthermore, the focus was set on limitations and problems of Quality of Service in 802.11 standards. Several issues within these limitations are shown and explained in section 1.2. The following Section 1.3 gives an insight to the 802.11e standard and its offering of Quality of Service trying to solve some of the problems mentioned in the previous section. The two kinds of Quality of Service are explained, the Traffic Prioritisation and the Traffic Parameterization. At the end of this paper, an annex is given including some main expressions used within this paper as well as a reference list to used books and papers.

## 1.5 Conclusion

As written in this paper, the new standard seems to offer QoS in wireless LAN and thus allows the mobile usage of real-time applications like Voice or Video over IP. But to be successful, a new technique has always to fulfil three conditions: first it has to work in practice and also under real world conditions, second there must be a true advantage for the user and third, it has to be cheap. Will the 802.11e standard work in everyday use? There exist no difficult technical or algorithmically problems to solve, so this point does not present a problem. But where are the advantages for the user? For the use in a privacy environment, the user does not really need this technique, because for most applications the main problem is the bandwidth and not the sharing of it (e.g. TV). Thus the user will use a wired connection anyway. In public usage there is the main problem of fairness. If one user decides to watch TV, another might not have a chance to download a very important paper. The second problem is that the possibility for using QoS depends on the Network Provider, who will not be interested in investing in new technologies before the old ones are amortized. The last problem is the price. Quite obvious, it will not be possible to implement these functions only in software and therefore one has to buy new access points and network cards. For a service, one does not really need, the price will be probably too high. Sadly, at the end the industry will decide if this standard is to be used or not. If they see a possibility to gain money out of it, they will try to force the customer buying and using the new devices, if they are in use for it or not.

## 1.6 Annex

**WLAN** A Wireless Local Area Network, which uses radio waves, is mostly used in rooms, buildings, and campuses. It uses at least one wireless access point for connecting the wireless users.

**CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance** This is a network control protocol with use of carrier sensing. *CSMA* is MAC protocol in which nodes look for other traffic before transmitting, in order to get the media for themselves. *CS*: the transmitter listens before sending (i.e. listen to signals of other stations). If a signal from another station is detected, the transmission has to wait. *MA*: several nodes are able to send and receive on the medium and transmissions can be received by all nodes within the range of the sender. *CA* is used for improving the CSMA performance, by reserving the network for a single transmission. This function is done by a jam signal, which therefore reduces collisions. By sending a jam signal, every node informs others about wanting to transmit data. After this notification, which all other stations in range have received, the transmission of frames starts. Collision prevention is given because other nodes are aware of transmission. The stop of a transmission happens when a jam signal from another station is detected. The station tries to resend the data after a random time.

**Access Point AP** Entity that provides access to distribution services via wireless network.

**Distribution System Service DSS** Services, provided by the DS, that enable the MAC to transport MAC service data units between stations which are not in direct communication with each other over a wireless network. This services transport these data units between the APs, between portals, and between stations. Distribution system services are provided between pairs of 802.11 MACs.

**MAC management protocol data unit MMPDU** Data unit exchanged between MAC entities, to implement MAC management protocol.

**MAC protocol data unit MPDU** Data unit of data exchanged between MAC entities by using services of physical layer (PHY).

**MAC service data unit MSDU** Information that is delivered between MAC service APs.

**Basic Service Set BSS** A set of stations controlled by coordination function.

**Distribution System DS** System used to connect BSS and LANs for creating an ESS.

**Extended Service Set ESS** Set of more connected BSS and LANs which appear as a single BSS to the stations connected with any of those BSSs.

**Station STA** A device which contains an 802.11 MAC and physical layer interface to a wireless network.

**Station Service SS** Services for the transport of MSDUs between stations within a BSS.

**Standard 802.11 Components**

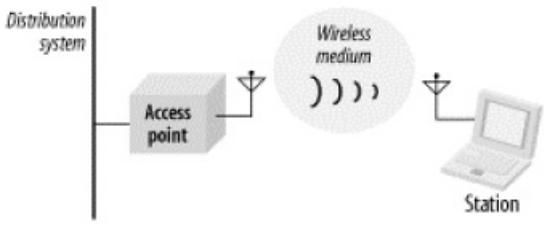



Figure 1.27: 802.11 Components [3]

**ATM – Asynchronous Transfer Mode** This network protocol encodes traffic into cells instead of variable sized packets. It is connection oriented, with connection between points for data exchange (on link layer). Idea was to find a solution between circuit-switched and packet-switched networks by mapping bit-streams and packet-streams onto these cells. For videos and audio low latency and high QoS is needed to handle those streams and therefore using ATM gets into discussion.

**CoS – Class of Service** This is a queuing algorithm which compares packets for classification of packets and assigning queues of different priorities. But is does not ensure priority in delivering packets.

**Traffic Shaping** It controls computer networks in order to guarantee performance, low latency and bandwidth for example. Concepts behind this are classification, queue disciplines, congestion management, fairness and QoS. This mechanism controls the volume and the rate of traffic being sent into the network. The advantages of this method are seen when having a packet bottleneck within a network: less jitter, reduced packet loss and lower latency. It is often used in combination with DiffServ and IntServ.

**WME – Wireless Multimedia Extension (Wi-Fi - Multimedia)** This is a certification based on 802.11e. It provides QoS features and it prioritises traffic according to access categories, although it does not guarantee throughput. Useful for simple applications that need QoS, for example Voice over IP (VoIP) phones.

Streaming media This media is consumed (reading, hearing, viewing) while being delivered, when talking about distribution over computer network. The great development and spreading of streaming media raises the issue about QoS.

# Bibliography


[1] D. Skyrianoglou, N. Passas, A. Salkintzis: Support of IP QoS over Wireless LANs. Vehicular Technology Conference 2004, 17-19 May 2004 Pages 2993-2997 Vol.5.

[2] ANSI/IEEE Standard 802.1d - 1998. Information technology - Telecommunications and information - exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE-SA Standards Board, reaffirmed June 2003.

[3] M. Gast: 802.11 Wireless Networks, the Definitive Guide, 2. nd. Edition, Sebastopol, Ca. O'Reilly, 2005.

[4] ANSI/IEEE Standard 802.11 - 1999. Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Reaffirmed 2003.

[5] Wikipedia Website: `http://en.wikipedia.org`, Last visited: March 2006.

[6] L. Peterson, B. Davie: Computer Networks - A Systems Approach, Morgan Kaufmann Publishers, 3rd edition, 2003.

[7] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss: An Architecture for Differentiated Services, RFC2475, December 1998. `http://rfc.net/rfc2475.html`.

[8] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin: Resource ReSerVation Protocol (RSVP), RFC2205, September 1997. `http://www.ietf.org/rfc/rfc2205.txt`.

[9] ANSI/IEEE Standard 802.11e - 2005. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005.

[10] IEEE Working Groups URL: `http://grouper.ieee.org/groups/802/11/`, Last visited: May 2006.

# Kapitel 2

# Comparison and Applications of Short-range Wireless Technologies

*Philipp Kräutli, Stéphanie Eugster, Matthias Alder*

*Heutzutage sind verschiedene Kurzdistanz-Wireless-Technologien, wie beispielsweise Bluetooth oder IrDA, weit verbreitet, währenddessen andere Technologien noch in der Entwicklung und Standardisierung stehen. Die Zunahme mobiler EDV Geräte wie Laptops und PDAs hat eine erhöhte Nachfrage nach Wireless Personal Area Networks (WPAN) zur Folge. WPANs ermöglichten ursprünglich eine einfache Verbindung von Geräten im Umkreis einer Person oder eines Computers. Davon ausgehend wurde eine Vielzahl neuer drahtloser Anwendungen entwickelt, welche Geräten den Informationsaustausch im Nahbereich ermöglichen. Die meisten dieser Anwendungen werden in der Industrie, Wissenschaft oder Medizin eingesetzt, wobei sie auch im Heimelektronik-Bereich Verwendung finden. Für diese Short-Range Wireless Konnektivität stellen sich verschiedene Anforderungen an die Netztopologie, die eingesetzten Geräte sowie die Sicherheit.*
*Nach einer Einführung in das Gebiet der Kurzdistanz-Wireless-Technologien gibt diese Arbeit einen Überblick über die verschiedenen eingesetzten aufstrebenden Technologien, wie IrDA, Bluetooth, WLAN, NFC, UWB und RFID. Diese Technologien werden aufgrund ihrer verschiedenen Eigenschaften und Schwierigkeiten miteinander verglichen und Lösungsansätze dafür vorgestellt. Auch wird auf die jeweiligen Markdurchdringungen und Trends eingegangen. Die verschiedenen Anwendungsgebiete werden anhand von Heim- oder Geschäftsbeispielen erläutert, die auch gewisse Verbindungen zwischen unterschiedlichen Technologien aufzeigen. Mit Einsicht in die regulatorischen Aspekte von Kurzdistanz-Wireless-Technologien der Schweiz und der Europäischen Union wird diese Arbeit abgerundet. Am Ende der Arbeit wird eine Schlussfolgerung zum präsentierten Thema gezogen.*

## Inhaltsverzeichnis

**2.1 Einleitung . . . . . 43**
**2.2 Übersicht der Wireless Technologien . . . . . 43**
2.2.1 Infrarot . . . . . 43
2.2.2 Bluetooth . . . . . 44
2.2.3 WLAN [12] [13] . . . . . 46
2.2.4 NFC [17] [18] . . . . . 47
2.2.5 RFID [23] [24] . . . . . 48
2.2.6 UWB [16] . . . . . 49
**2.3 Vergleiche und Herausforderungen . . . . . 50**
**2.4 Applikationen . . . . . 50**
2.4.1 Topologie . . . . . 52
2.4.2 Geräte . . . . . 54
2.4.3 Sicherheit . . . . . 56
2.4.4 Einsatzgebiete . . . . . 58
**2.5 Regulatorische Aspekte . . . . . 63**
**2.6 Fazit . . . . . 68**

## 2.1 Einleitung

Wireless Personal Area Networks (WPANs) sind die jüngsten Mitglieder der Netzwerkhierarchie. WPANs wurden entwickelt, um der steigenden Nachfrage noch Verkabelungen und Steckdosen, verursacht von zahlreichen an einem PC angeschlossenen Peripheriegeräten, ein Ende zu setzen. Daher waren WPANs in erster Linie auf Punkt-zu-Punkt Verbindungen ausgelegt. Bluetooh scheint sich, nach einem mühsamen Start, langsam durchzusetzen. Es spricht erfolgreich das Marktsegment unter dem verbreiteten WLAN an, welches heutzutage vollständige Netzwerkfunktionalität anbietet, inklusive Roaming, Sicherheit und Netzwerkmanagement.

Im Rahmen dieses Papers wird auf die wichtigsten dieser Short-range Wireless Technologien und Anwendungen eingegangen. In einem ersten Teil werden die technischen Aspekte und die Entwicklung von WLAN, Bluetooth, IrDA, NFC, RFID und UWB erläutert, sowie deren Bedeutung im Markt untersucht. Danach werden verschiedene Anforderungen an diese Technologien dargelegt und Lösungsansätze für einige daraus resultierenden Probleme präsentiert. Der letzte Teil handelt von den verschiedenen Einsatzgebieten und Anwendungsmöglichkeiten von Short-range Wireless Technologien sowie deren Auswirkungen auf die Gesellschaft im privaten und öffentlichen Rahmen.

## 2.2 Übersicht der Wireless Technologien

Angeregt durch die schnelle Verbreitung der mobilen Telefonie erleben Wireless-Technologien in den letzten 5 Jahren einen beeindruckenden Aufschwung. Kabellose Anwendungen haben sich in Consumer Products wie auch im Business Bereich fest etabliert. Die Technologien haben sich rasant entwickelt und inzwischen einen Stand erreicht, der auch hohen Ansprüchen an Datenübertragungsrate, Sicherheit, Stabilität etc. gerecht werden. Die Tatsache, dass trotzdem noch immer kabelgebundene Produkte entwickelt und vermarktet werden, zeigt aber ganz klar, dass noch längst nicht für alle Anwendungen passende drathlose Übertragungsverfahren verfügbar sind. Oft sind undurchsichtige und schnell ändernde Standards die Ursache für Inkompatibilitätsprobleme, welche die Verbreitung der Technologien bremsen. Nachfolgenden wird auf eine Auswahl von Technologien und Standards eingegangen, welche sich in den letzten Jahren auf dem Markt durchsetzen konnten oder kurz vor einer vielversprechenden Markteinführung stehen.

### 2.2.1 Infrarot

Unter dem Begriff Infrarot versteht man elektromagnetische Wellen mit einer Länge von etwa 780 bis 1000 nm. Die Existenz, dieser für den Menschen unsichtbaren Strahlen, wurde bereits im Jahre 1666 durch Sir Isaac Newton postuliert. Die Technik zur Verwendung dieser Strahlung um Daten drahtlos zu übertragen, ist aber noch relativ jung. Dir Firma `Hewlett Packard` gilt als Pionier dieser Technik. Im Jahr 1979 produzierte `Hewlett Packard` den ersten Taschenrechner, welcher mit einer Infrarot-Schnittstelle ausgestattet war. Somit konnten zum ersten Mal mit einem kommerziellen Produkt Daten zum

Drucker geschickt werden, ohne dass man auf eine Kabelverbindung angewiesen war. Der aus dieser Entwicklung entstandene Standard wurde unter der Abkürzung `SIR` für `Serial Infrared` bekannt. [2]

In den frühen 90er Jahren begannen auch andere Firmen mit der Entwicklung eigener Standards im Bereich der Infrarot-Datenübertragung. Um einen Wildwuchs zu verhindern, und um die Interoperabilität zwischen den Geräten unterschiedlicher Hersteller zu garantieren, wurde im Jahr 1994 die IrDA ins Leben gerufen. Namhafte Firmen wie `Compaq, Digital, IBM, Olivetti, Siemens, AMD, Intel` etc. schlossen sich in Form einer Non-Profit-Organisation zusammen, welche sich auf der CeBIT im Frühjahr 1994 zum ersten Mal der Öffentlichkeit vorgestellt hat. Das gemeinsame Ziel war die Durchsetzung eines Standards zur Datenübertragung auf kurzen Strecken über ein Infrarot-Signal mit 880 nm Wellenlänge. Als Grundlage diente hauptsächlich der von `Hewlett Packard` beschriebene Quasi-Standard `SIR`. [3]

Abbildung 2.1: USB IrDA-Adapter [20]

Die Kosten, um eine Hardware Infrarottauglich zu machen sind extrem tief, was die Verbreitung dieser Technik weiter beschleunigte. Die Tatsache, dass die Übertragungsstrecke auf wenige Meter beschränkt und Sichtkontakt vorausgesetzt ist, sorgt dafür, dass die Datenübertragung auch ohne aufwändige Verschlüsselung ausreichend sicher ist. Der IrDA Standard 1.0 spezifiziert genau gleich wie `SIR` eine Übertragungsrate von 9.6 bis 115.2 kBit pro Sekunde, was für die Übertragung von kleineren Druckaufträgen oder auch die Synchronisation von Kalenderen etc. durchaus genügt. Der aktuelle IrDA Standard 1.1 verspricht Datenraten von bis zu 16 MBit pro Sekunde und vergrössert damit die Andwendungsmöglichkeiten der Datenübertragung mit Infrarot Wellen enorm. Zugleich dringen aber laufend neue Techniken zur drahtlosen Übertragung auf den Markt, welche vor allem in der Übertragungsstrecke markante Vorteile bieten. So muss die Infrarot-Schnittstelle bei neueren Notebooks immer öfter einem Bluetooth-Adapter Platz machen. Mit Hilfe eines universellen Infrarot-Adapters (Abbildung 2.1) kann aber jedes Gerät mit einem passenden USB-Anschluss auch nachträglich kostengünstig infrarottauglich gemacht werden. [1] [3]

### 2.2.2 Bluetooth

Die Technologie namens Bluetooth bahnte sich ihren Weg von der Mobiltelefon-Industrie bis hin zu einer universellen Datenübertragungstechnik, welche heute in verschiedensten

Bereichen eingesetzt wird. Ursprünglich begann die Entwicklung im Jahr 1994 bei den Firmen `Ericsson` und `Nokia`, aus dem Bedürfnis heraus, sich von den Kabeln zwischen Mobiltelefon und Zusatzgeräten zu entledigen. Um mit Bluetooth einen herstellerübergreifenden Standard zu schaffen, wurde im Jahr 1998 die `Bluetooth Special Interest Group`, besser bekannt unter dem Kürzel `SIG`, gegründet. Gemeinsam sollte es schneller und kostengünstiger gelingen, Bluetooth-Sender und -Empfänger zu spezifizieren, welche günstig hergestellt werden können, flexibel sind im Einsatz, wenig Strom verbrauchen, nicht anfällig sind für Störungen und in der Lage sind, Daten für multimediale Anwendungen zu übertragen. [6] [4]

Inzwischen ist der Bluetooth-Standard vom `Institute of Electrical and Electronical Engineers`, kurz `IEEE`, unter der Bezeichnung `IEEE 802.15.1` adaptiert worden. Die ursprüngliche Übertragungsrate von 723.2 kBit pro Sekunde, welche durch die Bluetooth-Versionen 1.0, 1.0B, 1.1 und 1.2 spezifiziert ist, wurde mit der Version 2.0 auf 2.1 Mbit pro Sekunde angehoben. Mit Hilfe der Ultra Breitband Technologie soll die Übertragungsrate in naher Zukunft nochmals markant steigen. Gegenüber der IrDA-Technologie bringt Bluetooth somit nicht unbedingt Vorteile im Bezug auf die Übertragungsrate. Vielmehr ist es die grössere Übertragungsstrecke, und den nicht unbedingt notwendigen Sichtkontakt zwichen Sender und Empfänger, was den entscheidenden Vorteil zu bringen scheint. Bei modernen Notebooks und Mobiltelefonen findet man anstelle einer IrDA-Schnittstelle immer öfter einen Bluetooth-Transceiver. [4] [6]

Bluetooth-Geräte kommunizieren im Frequenzbereich von 2.402 GHz und 2.480 GHz, welcher ohne Lizenz weltweit kostenlos, für Nahbereichs-Funk verwendet werden darf. Andere Geräte wie Schnurlostelefone, Garagentoröffner oder Mikrowellenherde können das Bluetoothsignal stören. Um die Übertragung zu stabilisieren wird daher das sogenannte Frequency Hopping eingesetzt, was bedeutet, dass die Übertragungsfrequenz bis zu 1600 Mal in der Sekunde gewechselt wird. Dieses revolutionäre Verfahren wurde bereits im Jahr 1941 von Hedy Lamarr zum ersten mal beschrieben, und ist noch Heute der Grundstein für eine unterbruchsfreie Datenübertragung per Funk. Die maximale Übertragungsstrecke hängt hauptsächlich von der Sendeleistung ab. Das IEEE spezifiziert drei offizielle Klassen: Die Klasse 3 erreicht mit einer Sendeleistung von 1 mW eine Reichweite von rund 10 Metern, wobei die Klasse 1 mit einer Sendeleistung von 10mW eine beachtliche Distanz von 100 Metern überwinden kann. Mit Hilfe von Richtfunkantennen wird es sogar möglich, Übertragungsstrecken von über 1 Kilometer zu erreichen. [4] [5] [9]

Tabelle 2.1: Bluetooth Versionen

| | Verabschiedung | Übertragungsrate |
|---|---|---|
| 1.0, 10.B | 1999 | 723.2 KBit/s |
| 1.1 | 2000 | 723.2 KBit/s |
| 1.2 | 2003 | 723.2 KBit/s |
| 2.0 | 2004 | 2.1 MBit/s |

### 2.2.3 WLAN [12] [13]

Der Begriff WLAN beschreibt keinen Standard, sondern ist ein Überbegriff für lokale, drahtlose Netzwerke. Das Aloha-Net, welches im Jahr 1969 für den Campus der Universität Hawaii in Betrieb genommen wurde, gilt als erstes WLAN. Das Bedürfnis nach einem Funknetzwerk entstand aufgrund der Tatsache, dass der Universitätscampus über mehrere Inseln verteilt ist. Von einem Standard konnte damals noch nicht die Rede sein. Erst im Jahr 1997 verabschiedete das IEEE den Standard 802.11, welcher theoretisch eine Übertragungsrate von bis zu 2 MBit pro Sekunde erreichte und das lizenzfrei nutzbare Frequenzband von 2'400 bis 2'485 GHz nutzte. De facto konnte aber noch immer nicht von einem Standard gesprochen werden, da der Hersteller noch über sehr viele Parameter selbst bestimmen konnte. Mitunter auch das Modulationsverfahren, was dazu führte, dass Produkte von unterschiedlichen Herstellern fast ausnahmslos inkompatibel waren. [10]

Die Firma `Lucent Technologies` war eine der ersten Firmen, welche WLAN-Komponenten nach dem IEEE 802.11 auf den Markt brachte. Bei dieser Technik, die bei `NCR` eingekauft und unter dem Namen `WaveLan` vermarktet wurde, kam das Frequency-hopping spread spectrum Modulationsverfahren zum Einsatz. `Lucent Technologies` genoss eine monopolartige Stellung im Bereich der Herstellung von WLAN Chipsätzen. Auch das erste iBook von `Apple` mit einem WLAN Modul, welches bereits dem Standard 802.11b entsprach und unter dem Namen `Airport` vermarktet wurde, war mit einem Chipsatz von `Lucent Technologies` bestückt. Innerhalb von kürzester Zeit konnte dank dieser Vermarktung die WLAN Technologie in den Consumer-Bereich vordringen. Mit `Harris Semiconductors` drang ein zweiter Hersteller von WLAN Chipsätzen für den Consumer-Bereich auf den Markt, welcher sehr viel freigiebiger mit Informationen bezüglich der Technik umging. Dadurch fanden sich schnell weitere Hersteller von WLAN Komponenten. Die Zeit der Monopolstellung von `Lucent Technologies` war somit zu Ende, wodurch die Preise auf dem Markt von WLAN Komponenten stark sanken und die Verbreitung der Technologie weiteren Auftrieb erhielt. [11]

Als direkter Nachfolger des 802.11 Standards war eigentlich 802.11a geplant, welcher im Jahr 1999 fertiggestellt wurde. Neu sollten Frequenzen im Bereich von 5 GHz, und ODFM (Orthogonal Frequency Division Multiplexing) als Modulationsverfahren verwendet werden. Dadurch wäre laut Spezifikation theoretisch eine Datentransferrate von bis zu 54 Mbit pro Sekunde möglich. Da dieses Verfahren aber mit der Methode CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) arbeitet, wird in der Praxis kaum ein Datendurchsatz über 18 Mbit pro Sekunde erreicht. Ein weiterer Nachteil ist, dass die Transferrate bei mehreren Clients nochmals erheblich sinkt. Zudem ist der verwendete Frequenzbereich auch Heute noch teilweise nur eingeschränkt lizenzfrei nutzbar. [15]

Aufgrund der Nachteile des 802.11a Standards, hat sich auf dem Markt der ebenfalls im Jahr 1999 spezifizierte IEEE Standard 802.11b durchgesetzt. Die Verwendung des 5 GHz Frequenzbereichs hat sich als zu problematisch erwiesen. Obwohl der Standard IEEE 802.11b, welcher das Modulationsverfahren DSSS (Direct Sequence Spread Spectrum) verwendet, mit einer maximalen Datentransferrate von 11 Mbit pro Sekunde deutlich unter jener des 802.11a Standards liegt, wird diese Technik Heute noch verwendet. Die meisten aktuellen Geräte unterstützen neben IEEE 802.11b auch den im Jahr 2003 ratifizierten Standard 802.11g, welcher die Vorteile einer höheren Datentransferrate von bis zu

54 Mbit pro Sekunde und höherer Reichweite mitsich bringt, und ebenfalls im Frequenzbereich von 2.4 GHz kommuniziert. Gleich wie 802.11a setzt man auch bei 802.11g auf das Orthogonal Frequency Division Multiplexing. Um aber die Abwärtskompatibilität zu 802.11b zu gewährleisten, kann der neue Standard auch mit DSSS umgehen. In der Praxis zeigt sich jedoch, dass der Mischbetrieb von Geräten mit unterschiedlichen Standards starke Einbussen bei der Datentransferrate zur Folge hat.

Der nächste WLAN Standard ist bereits in den Startlöchern, und soll im Verlauf des nächsten Jahres endgültig verabschiedet werden. Zurzeit liegt zwar erst eine Entwurfsspezifikation für IEEE 802.11n vor. Die Hersteller rühren jedoch mit Labels wie „802.11n-Draft-kompatibel“ bereits kräftig die Werbetrommel. Mit einem einfachen Software-Update sollen die Geräte später IEEE 802.11n kompatibel gemacht werden können und garantiert auch mit den älteren Standards zurecht kommen [14]. Dieses Versprechen scheint sehr gewagt, wenn man bedenkt, dass bis Heute noch nicht definitiv entschieden wurde, ob der neue Standard im gleichen Frequenzbereich wie die älteren Standards kommunizieren wird. Um die Datentransferrate und Reichweite entscheidend zu erhöhen setzt der neue Standard auf die bereits von älteren Geräten proprietär verwendete MIMO (Multiple Input Multiple Output) Technologie, welche anstatt nur einer Antenne einen sogenannten Antennen-Array verwendet und dadurch mehrere Signalpfade erzeugt. Die heute erhältlichen 802.11n-Draft-Produkte erreichen unter optimalen Voraussetzungen eine Datentransferrate von bis zu 300 MBit pro Sekunde brutto, was zwar ansehnlich, aber noch weit von den angestrebten 600 MBit pro Sekunde entfernt ist.

Tabelle 2.2: Übersicht der WLAN Standards

| | Übertragungsrate | Frequenzband | Akzeptanz |
|---|---|---|---|
| 802.11 | 1 oder 2 Mbit/s | 2,400 bis 2,485 GHz | veraltet |
| 802.11a | 54 Mbit/s | 5 GHz | geringe Verbreitung |
| 802.11b | 11 Mbit/s | 2,400 bis 2,485 GHz | noch immer stark verbreitet |
| 802.11g | 54 Mbit/s | 2,400 bis 2,485 GHz | stark verbreitet |
| 802.11n | 540 Mbit/s | 5 GHz | noch in der Entwicklungsphase |

Im Jahr 1999 haben sich die führenden Hersteller von WLAN Geräten in Form der Wi-Fi (Wirless Fidelity) Alliance zusammengeschlossen. Ziel dieser Non-Profit-Organisation ist hauptsächlich die Durchsetzung eines weltweit akzeptierten Standards für WLAN. Inzwischen zählt die Organisation über 250 Mitglieder und hat bereits über 2’500 Produkte in Bezug auf die Kompatibilität zertifiziert.

### 2.2.4 NFC [17] [18]

Die Nahfunktechnik `Near Field Communication` (NFC) wurde im Gegensatz zu WLAN oder auch Bluetooth nicht geschaffen, um Distanzen zu überwinden. Vielmehr dient sie zur Kommunikation zwischen zwei Geräten, welche sich unmittelbar nebeneinander befinden. Beträgt der Abstand mehr als ca. 20cm reisst die Verbindung ab. Somit ist diese

Technologie keine Konkurrenz, sonder vielmehr eine Ergänzung zu den üblichen Wireless Technologien. Beispielsweise könnte dank NFC das aufwändige Bluetooth Pairing-Verfahren deutlich vereinfacht werden. Denn anstatt der sonst üblichen Funkraum-Suche, Gerätewahl, Dienstwahl und Passwortübergabe könnte der Datentransfer via Bluetooth initialisiert werden, indem zwei geräte für kurze Zeit direkt nebeneinander gehalten werden. [19]

NFC verwendet das global verfügbare und unregulierte RF (Radio Frequency) Frequenzband im Bereich von 13.56 MHz und erreicht je nach Standard eine Datentransferrate von 106, 212 oder 424 KBit pro Sekunde. Diese äusserst tiefen Datenübertragungsraten schliessen eine Übertragung von Multimediadaten klar aus, was aber in Anbetracht der geringen Reichweite ohnehin kaum Verwendung finden würde. Die Möglichkeit mit NFC Daten im passiven Kommunikationsmodus zu übertragen hingegen, erschliesst gänzlich neue Anwendungsbereiche. Bei diesem Verfahren kann das eine Gerät die für die Kommunikation erforderliche Energie direkt aus dem elektromagnetischen Feld der Gegenstation beziehen. Im Gegensatz zu RFID gibt es bei NFC keine strikte Trennung zwischen aktivem Reader und passivem Tag. Jedes NFC-fähige Gerät unterstützt den aktiven wie auch den passiven Kommunikationsmodus. Für die Datenübertragung kommt ein Peer-to-Peer Protokoll (NFCIP-1) zum Einsatz, welches zwischen dem Initiator und dem Target der Kommunikation unterscheidet. Der Initiator ist das Gerät, das den Austausch der Daten initialisiert und kontrolliert; der Target ist das Gerät, das auf den Request (Anfrage) des Initiators antwortet.

Die Entwicklung von NFC wurde hauptsächlich von den Firmen Sony und Philips vorangetrieben. Heute ist die Technologie als ISO/IEC 18092 und ECMA 340 standardisiert und vermag auch andere Hersteller zu überzeugen. Im Jahr 2004 gründeten Sony und Philips zusammen mit dem Mobiltelefonhersteller Nokia das NFC-Forum, um eine gemeinsame Entwicklung von NFC zu forcieren. Mittlerweile gehören dem Forum zahlreiche weitere Firmen an, darunter MasterCard, Microsoft, Motorola, Samsung, Texas Instrumends und Visa.

### 2.2.5 RFID [23] [24]

Die Wurzeln der RFID Technik reichen bis in den Zweiten Weltkrieg um 1940 zurück, als die Vorläufer der heutigen RFID Transponder und Leseeinheiten zur Freund-Feind-Erkennung eingesetzt wurden. Die ersten RFID-Geräte für den kommerziellen Einsatz wurden jedoch erst um 1970 in Form eines Warensicherungssystems auf den Markt gebracht. Die guten Erfahrungen, welche mit diesem System gemacht wurden, führten dazu, dass auch andere Wirtschaftszweige sich für die Technologie zu interessieren begannen. Anfang der 80er Jahre wurden beispielsweise erstmals Tiere mit RFID Transpondern ausgerüstet. In den USA wie auch in Norwegen wurden RFID-Systeme für das Mautwesen im Strassenverkehr geplant, welche seit den 90er Jahren vermehrt im Einsatz sind. Erst seit wenigen Jahren existieren RFID-Systeme für Zugangskontrollen, bargeldloses Zahlen, Skipässe etc. [21]

Der Grund für den Erfolg von RFID ist wohl die Tatsache, dass RFID Transponder ohne externe Stromquelle wie beispielsweise eine Batterie auskommen. Diese passiven

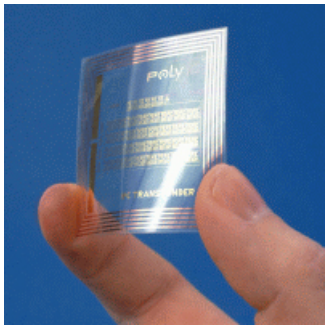


Abbildung 2.2: RFID Transponder [22]

RFID Transponder beziehen die für die Datenübertragung notwendige Energie aus einem Kondensator, welcher durch den induzierten Strom aus dem elektromagnetischen Feld des Senders aufgeladen wird. Dies hat nicht zuletzt auch den Vorteil, dass die Chips äusserst kostengünstig produziert werden können. Die Datenübertragung vom Lesegerät zum Transponder erfolgt in der Regel durch ein Ein- und Ausschalten eines hochfrequenten Magnetfeldes. Der Empfänger kann das Signal dann sehr einfach, durch Gleichrichtung der in der Empfängerspule induzierten Spannung demodulieren. Auch die Datenübertragung in umgekehrter Richtung ist dank der transformatorischen Kopplung zwischen dem Sender und dem Empfänger problemlos möglich.

Mit der Verbreitung der RFID Technologie wurden aber auch kritische Stimmen laut. So wird befürchtet, dass RFID ein grosses Potential zur Gefährdung der Privatsphäre der Konsumenten hat. Dass diese Ängste nicht unbegründet sind, zeigen diverse Vorfälle in den letzten Jahren. Immer wieder wurden RFID Etiketten an Produkten oder Dokumenten angebracht, ohne dass die Person, welche das Objekt erworben hat, davon Kenntnis hatte. Im Bezug auf den Datenschutz wie auch auf die Wahrung der Privatsphäre sind solche Vorgehen höchst bedenklich. [25]

### 2.2.6 UWB [16]

Die relativ neue Datenübertragungstechnik UWB (Ultra wideband), welche seit Februar 2002 lizenzfrei im Frequenzbereich von 3.1 bis 10.6 GHz betrieben werden darf, beschreibt die Nutzung extrem grosser Frequenzbereiche (Abbildung 2.3). Im Gegensatz zu den konventionellen Übertragungstechniken werden die Informationen nicht einer bestimmten sinusförmigen Trägerfrequenz aufmoduliert, sondern durch eine Folge sehr kurzer Impulse übertragen. Das Trägersignal wird dadurch sehr breitbandig und die Sendeleistung verteilt sich auf einen grossen spektralen Bereich. Somit können im selben Frequenzbereich nach wie vor auch schmalbandige Signale übertragen werden. [26]

Diese Technologie eignet sich hauptsächlich für die Datenübertragung auf kurze Distanzen bis ca. 10 Meter. Aufgrund der hohen Datenübertragungsraten von bis zu 1320 MBit/s gibt es eine grosse Anzahl von Anwendungsszenarien. Hauptsächlich die kabellose Anbindung von Peripheriegeräten an PCs liegt im Fokus der Hersteller. Längerfristig sollen so kabelgebundene Anschlüsse wie z.B. USB oder auch Firewire abgelöst werden. Dank

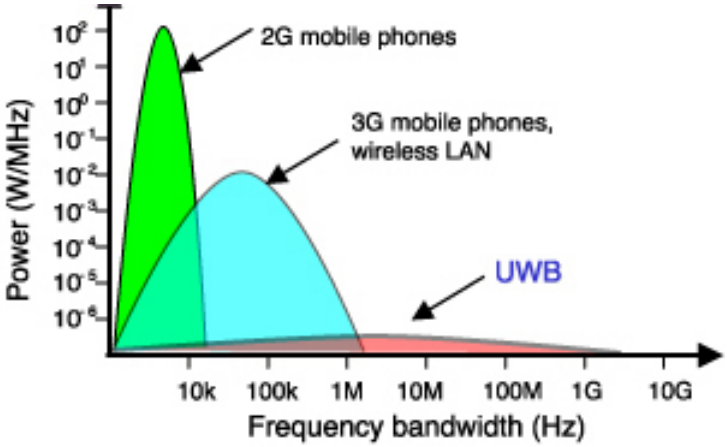



Abbildung 2.3: UWB Frequenzbereich [27]

der hohen Datenübertragungsraten wäre sogar die kabellose Anbindung von Bildschirmen möglich.

## 2.3 Vergleiche und Herausforderungen

Es zeigt sich, dass die heutigen Wirless-Technologien einen sehr hohen Spezialisierungsgrad aufweisen. Die unterschiedlichen Anforderungen an die drahtlose Datenübertragung werden von einer Vielzahl von Technologiestandards abgedeckt. Je nach Anwendungsfall verteilen sich die Prioritäten sehr unterschiedlich auf Kriterien wie Datenübertragungsrate, Reichweite, Stabilität, Sicherheit oder auch die Stärke der Verbreitung eines Standards. Zur Zeit gibt es keine Technologie, welche ihre Stärken in sämtlichen Bereichen ausspielen kann. Die Tabelle 2.3 zeigt einen Ausschnitt der Stärken und Schwächen der vorgestellten Technologien. [28]

Verschiedene aktuelle sowie noch in Forschung stehende Technologien für Short-Range Wireless Anwendungen, wie beispielsweise Infrarot, Bluetooth, WLAN, NFC oder UWB wurden bereits vorgestellt und miteinander verglichen. Ihre technischen Stärken und Schwächen sowie generelle Wireless-Trends wurden im vorangehenden Kapitel erläutert.

Anschliessend wird auf Topologien, Applikationen, Sicherheit, technische Szenarien und auf Anwendungs- und Einsatzgebiete von Short-Range Wireless näher eingegangen. Danach werden regulatorische Aspekte der Schweiz und der Europäischen Union hinsichtlich Short-Range Wireless erläutert.

## 2.4 Applikationen

In letzter Zeit wurde eine Vielzahl neuer Short-Range Wireless Anwendungen entwickelt, welche zwar von klassischen WPANs ausgehen, im Endeffekt aber einen bedeutend anderen Ansatz wählen: Sie erfüllen das Bedürfnis nach echten Netzwerktopologien anstatt reinen Punkt-zu-Punkt Verbindungen. In klassischen WPANs finden Interaktionen meistens

Tabelle 2.3: Vergleich der vorgestellten Wireless Technologien

| | Datenübertragungsrate | Reichweite | Verbreitung |
|---|---|---|---|
| Infrarot | 16 MBit/s | 50cm | Stark, Tendenz sinkend |
| Bluetooth | 2.1 MBit/s | 100m | Stark |
| WLAN | 54 MBit/s | 100m | Sehr stark |
| NFC | 424 KBit/s | 20cm | Schwach, Tendenz steigend |
| RFID (passiv) | 40 KBit/s | 10m | Mittel, Tendenz steigend |
| UWB | 1320 MBit/s | 10m | Sehr schwach, Tendenz steigend |

zwischen Mensch und Maschine statt. Eine grosse Anzahl neuer Short-Range Wireless Anwendungen muss die Interaktion zwischen Machinen, Sensoren oder Bedienungselementen an entfernten Knotenpunkten unterstützen. Solche Netzwerke werden als „sensor actuator“ networks bezeichnet [56]. Wenn HTTP als Applikationsprotokoll verwendet wird, werden die angebotenen Dienste als „Web services“ bezeichnet.

Einige Beispiele für diese Netze:

- Steuerung von Maschinen und Geräten in der industriellen Automation, Smart Home Anwendungen
- Temperatur-, Druck- oder Gas-Sensoren, Ventile und Bedienungselemente, z.B. für die Heizung, Ventilation und Klimaanlage
- Medizinisches Monitoring (in- und ausserhalb des Körpers)

Ein bedeuteder Sachverhalt beherrscht diesen Markt: Je tiefer die Kosten pro Knoten, desto höher die Zahl der Anwendungen. Gegenwärtig wird die Entwicklung neuer wireless Anwendungen durch die Kosten eingeschränkt. Es wird klar, dass Short-Range Wireless Netzwerke eine hierarchische Stufe angehen, welche bis heute von keinem Kabelnetzwerk, welche nur Punkt-zu-Punkt Verbindungen unterstützen, abgedeckt wird. Tabelle 2.4 zeigt die Tatsache, dass zusammen mit den technischen Entwicklungen auch Architekturaspekte diskutiert werden müssen. Dies ist bei Short-Range Wireless Netzwerken besonders wichtig, da Architektur und Topologie nicht vom verdrahteten Pendant übernommen werden kann.

Tabelle 2.4: Hierarchiestufen für verkabelte und kabellose Netzwerke. [61]

| | Drahtnetzwerke | | Drahtlose Netzwerke |
|---|---|---|---|
| PAN | not yet covered | WPAN | Bluetooth, 802.15.4 und ZigBee, proprietär |
| LAN | IEEE802.3 | WLAN | IEEE802.11 (Home RF, HiperLAN/2) |
| MAN | FDDI, IEEE802.3 | WMAN | IEEE802.16, proprietär |
| WAN | X.25, frame relay, ATM | WWAN | GSM, GPRS, UMTS |

Die neuen Protokolle und Standards für Short-Range Wireless Netzwerke stehen einer Vielzahl verschieder An- und Herausforderungen gegenüber. Diese Anforderungen können in drei Gruppen aufgeteilt werden: Topologie, Geräte und Sicherheit. Es bestehen verschiedene Lösungsansätze, besonders im Bereich Sicherheit. Dummerweise stehen die wichtigsten Anforderungen im Konflikt zueinander (s. Abb. 2.4).

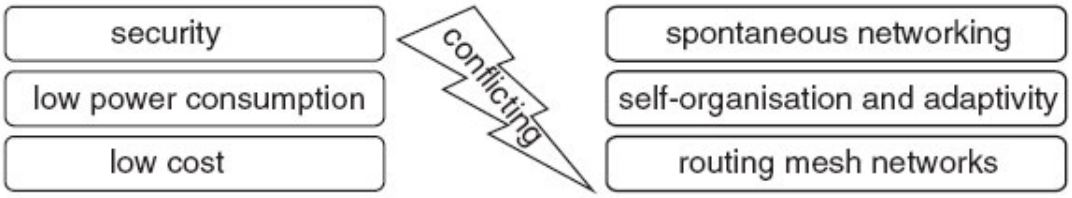



Abbildung 2.4: Zielkonflikte beim Design Short-Range Wireless Netzwerke. [61]

### 2.4.1 Topologie

Folgende Probleme bestehen in Bereich der Netzwerkstrukturen: Sensor-Netzwerke sollten fortgeschrittene Topologien wie z.B. mesh networking unterstützen. Sie sollten selbstorganisierend sein und spontaneous (ad hoc) networking unterstützen. Mobilität ist ein Thema für viele drahtlose Anwendungen, wobei einige auch entweder mit statischen oder nomadischen Topologien arbeiten. Die Anzahl der Geräte im Netzwerk kann stark varieren. Es kann sich um zwei, aber auch um mehrere hundert oder sogar tausend Knoten handeln. Quality of Service ist ebenfalls eine wichtige Anfoderung bei industriell eingesetzten, drahtlosen Einrichtungen.

#### Stern-Netzwerke

Herkömmliche WPAN und WLAN Systeme, da von verdrahteten Punkt-zu-Punkt Netzen abgeleitet, sind meistens in einer Stern-Topologie angeordet (s. Abb. 2.5). Ein fest zugeordneter Access Point sammelt und verteilt Informationen an die mobilen Geräte, welche im Umkreis des APs vorhanden und zu diesem zugehörig sind. Zusätzlich kann ein AP Layer-2 Bridging zu anderen Netzen (z.B. Ethernet) anbieten. Abgesehen vom Netzwerk-Management haben APs nur die Rolle von Zwischenknoten. Die mobilen Geräte sind Endknoten. Direkte Kommunikation zwischen den mobilen Geräten wird nicht unterstützt, kann aber über den zentralen AP ermöglicht werden. Obwohl die Stern-Topologie der einfachste Ansatz ist, wird sie in der Mehrheit der Smart Home Anwendungen eingesetzt.

#### Hierarchische Stern-Netzwerke

Stern-Netzwerke können geclustert werden. In vielen Wireless Systemen sind die APs mitteles Kabel (meistens Ethernet) miteinander verbunden. Allerdings könenn APs auch drahtlos miteinander verbunden werden. Es empfiehlt sich, die Zwischenverbindungen

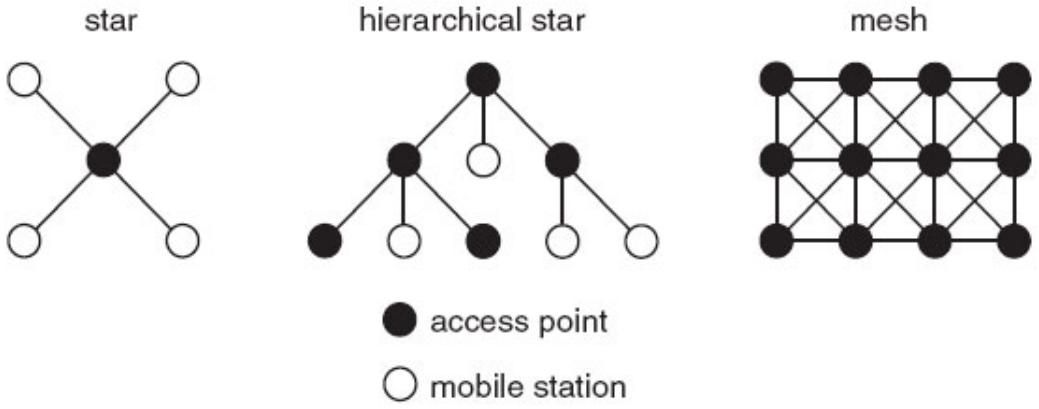



Abbildung 2.5: Topologien für Short-Range Wireless Netzwerke. [61]

mit Protokollen des nächst höheren Netzwerkleves zu bewerkstelligen, um genug Bandbreite für den zusammengefassten Datenverkehr zur Verfügung zu haben. Folglich können WLAN-802.11 APs mit WMAN-IEEE802.16 oder WPAN-Bluetooth APs mittels WLAN-802.11 verbunden werden.

### Mesh Networks

Die Verbindung zwischen den APs kann auch mit dem selben Protokoll, welches die APs für die Kommunikation mit den mobilen Geräten benutzen hergestellt werden. Wenn dies der Fall ist, ist es nur noch ein kleiner Schritt zum Mesh Networking, wo alle Stationen die selbe Doppelfunktionalität haben und gleichzeitig End- und Zwischenknoten sind. Zusätzlich kann angenommen werden, dass alle Stationen die selbe Funktionalität besitzen und auf dem gleichen Level arbeiten, mit Ausnahme von Gateways. Solche Topologien sind als Peer Netzwerke klassifiziert, in denen alle Stationen gleichgestellt sind. Neue Routing-Algorithmen müssen entwickelt und implementiert werden. Es gibt verschiedene Lösungsansätze für dieses Problem:

Benutzung von herkömmlichen Routing-Algorithmen wie sie in Ehernet oder IP-Netzwerken verwendet werden. Dijkstra's „Shortest Path First"-Algorithmus bleibt einer der verbreitetsten Algorithmen in diesem Bereich. In Mesh Networks bedeutet das eine Vielzahl unabhängiger Bäume.

Herkömmliche Ansätze leiden an einem unangemessenen Gebrauch redundanter Pfade. Daher müssen Routing-Algorithmen entwickelt werden, welche intensives Load Sharing erlauben und lokale Kapazitätslimiten und dynamische Auslastungsänderungen einkalkulieren.

Die wachsende Ansprüche an die Routing-Protokolle stellt eine zusätzliche Last an das Netzwerk und die Knoten dar. Die meisten Routing-Protokolle in packet-switched Netzwerken sind in-band Protokolle. Ausserdem sind die meisten Routing-Protokolle auf regelmässigen Austausch von Management-Informationen angewiesen, was in Konflikt zu langen power-down Modi steht. Zusätzlich ist die zuätzliche Last ein Widerspruch zu der Forderung nach tiefen Kosten.

**Quality of Service**

QoS kann in zentralisierten medium-access Entwürfen einfach unterstützt werden. Dies ist der Fall bei Bluetooth und ebenfalls in der Enhanced Distributed Co-ordination Function (EDCF) von IEEE802.11. Diese Konzepte können für das Mesh Networking jedoch nicht übernommen werden, da dies die Gleichgestelltheit aller Stationen stören würde. In traditionellen hierarchischen Stern-Netzwerken folgen die benachbarten Zellen einem Space Division Multiple Access (SDMA) Ansatz und Arbeiten in verschiedenen Kanälen um störungsfreies Arbeiten der benachbarten Zellen zu ermöglichen. In Mesh-Netzwerken, wo alle Stationen den selben Kanal teilen, muss ein Time Division Multiple Access (TDMA) Ansatz gewählt werden. Daher sind EDCF und ähnliche Technologien schwer zu implementieren.

**Netzwerkintegration**

Das Zusammenschalten von Netzwerken ist die Grundlage für inter-networking. Die Integration in ein grosses Meta-Netzwerk kann auf allen Schichten vorgenommen werden:

Layer 1: Verschiedene Medien können verbunden werden, z.B. wireless mit Kabel.

Layer 2: Verschiedene Medium Access Control (MAC) Techniken können nebeneinander bestehen, z.B. CSMA/CD (Ethernet), CSMA/CA (CAN) oder Master-Slave Architekturen.

Layer 3: Verschiedene Switching-Technologien können verbunden werden, z.B. packet- mit circuit-switched.

Layer 7: Verschiedene Formate und Funktionalitäten können zusammenarbeiten, z.B. per XML.

Bei Short-Range Wireless Netzwerke bestehen jedoch wesentliche Hindernisse bei einer solchen Integration: Die Rechenleistung von WPAN Knoten ist beschränkt. Daher können keine ausgewachsenen Protokolle implementiert werden. Dennoch ist es wichtig, dass die Architekturen und Interfaces den entsprechenden Ethernet-IP-TCP-Netzwerken ähnlich sind. In vielen Fällen missachten proprietäre und sogar nicht-proprietäre Ansätze die nützliche Auflage und verhindern ein bequemes Design von Gateways.

### 2.4.2 Geräte

Tiefer Stromverbrauch ist ein wichtiges Anliegen bei allen drahtlosen Anwendungen, da die Drahtlose Kommunikation wenig bringt, wenn man das Gerät trotzdem per Kabel an die Steckdose anschliessen muss. Batteriebetrieb ist daher für fast alle Knotenpunkte unerlässlich. Die Geräte in einem WPAN Netzwerk können wie in Abb. 2.6 klassifiziert werden. Folgende Punkte sind einleuchtend:

- Kommunikation ist eine Erweiterung der Basisfunktionalität von Sensor- und Bedienungsknoten.
- Ein Gerät sollte nur die Funktionalitäten abdecken, welche in einer gegebenen Topologie unbedingt erforderlich sind (Kosteneinschränkung).
- Ein Gerät kann mehr als eine Klasse abdecken. Dies ist besonders in Mesh-Netzwerken der Fall, wo alle Geräte End- und Zwischenknoten zugleich sind.

Die allgemeinen Bestandteile eines Short-Range Wireless Netzwerk-Knotens sind in Abb. 2.7 ersichtlich. Es ist leicht ersichtlich, dass Modularität absolut notwendig ist um die hohen Anforderungen von Hardware-Software Co-design und System-Level Integration zu erfüllen um Entwicklungsvorgang zu erleichtern, erweiterte Topologien zu unterstützen und Kosten zu reduzieren.

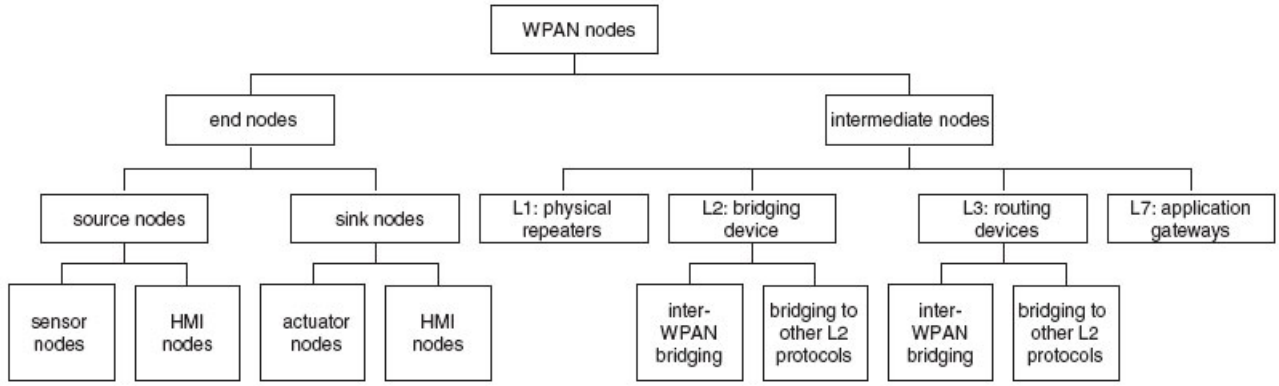



Abbildung 2.6: Klassifizierung von WPAN Knoten. [61]

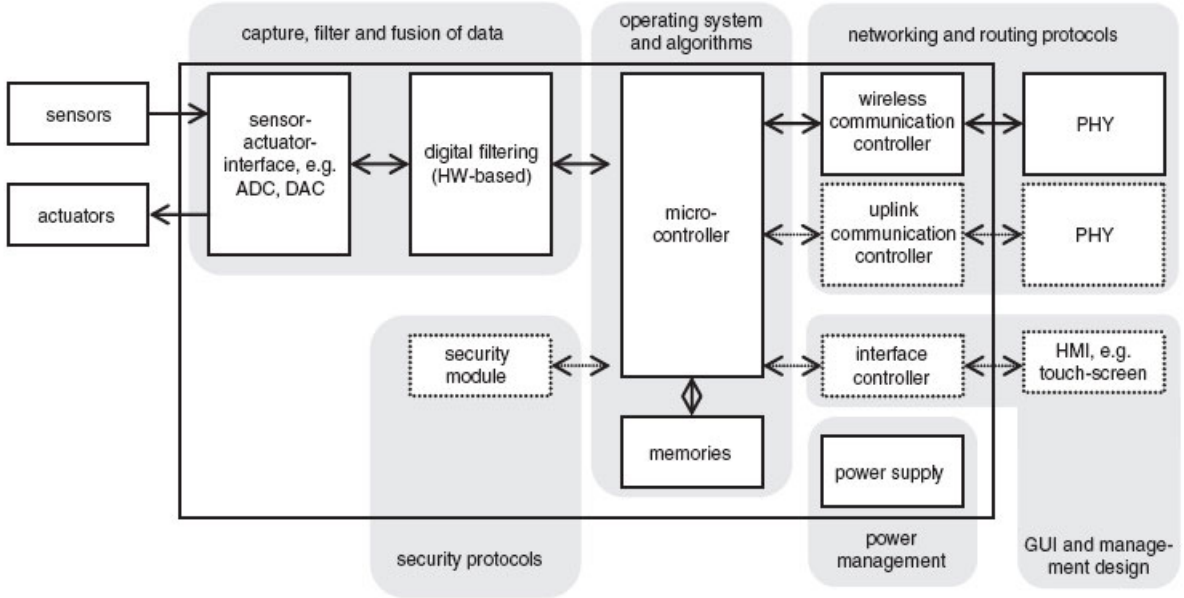



Abbildung 2.7: Trennung von Management- und Datenverkehr im IEEE802.15.4 Standard. [61]

#### Trennung von Management- und Datenverkehr

Klassische Referenzmodelle wie das ISO-OSI Referenzmodell trennen die unterschiedlichen Aufgaben offener System-Interkonnetivität in modulare Layer. Dieser Ansatz ist vorherrschend für reine Datekommunikation, leide aber an Inkonsistenzen in Bezug auf die Integration von Management-Protokollen wie STP, ARP, ICMP oder Routing-Protokollen wie RIP order IGRP. Für Wireless Netzwerke wurde ein anderer Ansatz verwendet, da Netzwerkmanagement-Aufgaben wie Erkennung und Zuordnung von Stationen in Layer-1 und Layer-2 Protokollen eingebunden sind.

#### Stromverbrauch

Sromverbrauch ist ein kritischer Parameter bei batteriebetriebenen WPAN Knoten. Es gibt verschiedene Mittel um den Stromverbrauch niedrig zu halten: Die Skalierung mikroelektronischer Geräte ist elementar, egal welche Netzwerkarchitektur verwendet wird. RF Module arbeiten mit hohen Frequenzen und sind potentielle Stromfresser. Komplexe Modulation und der Gebrauch aufwändiger Filter verbessert die Effizienz der Nutzung des Frequenzbandes, erhöht aber den Stromverbrauch. Dieser Konflikt kann nicht allgemein gelöst werden und gewisse Kompromisse müssen akzeptiert werden. Die Komplexität des Basisbands und des Medium Access sollte so tief wie möglich gehalten werden, damit die zugrundeliegenen Prozessoren mit tiefer Spannung laufen können. Des Weiteren ist es empfehlenswert, lange power-down Zeiten einzubauen, während denen nur Timer am laufen gehalten werden und alle anderen Elemente abgeschaltet werden. Dies ist bei vielen Anwendungen zulässig. Allerdings ist die Möglichkeit zur Implementation von wake-up Systemen erforderlich.

### 2.4.3 Sicherheit

„Safety is the ability of a system to run along the specification at any time and under all circumstances. Security is the capability of a system to run only in states with no unauthorised information loss or tampering.“ [57] Sicherheit ist aufgrund des offenen Übertragungsmediums einer der Wichtigsten Aspekte in drahtlosen ad-hoc Netzen. Normalerweise werden Kryptographiebasierte Protokolle eingesetzt, um den Sicherheitsbedürfnissen zu entsprechen. Im Falle dynamischer multi-path end-to-end Sicherheit werden hybride Algorithmen verwendet. Symmetrische Algorithmen wie 3DES, RC-4, IDEA oder Blowfish werden bei Punkt-zu-Punkt Kommunikation verwendet, da diese effizient implementiert werden können. Das Problem der grossen Anzahl benötigter Keys wird mit dem Austausch von symmetrischen Keys mittels asymmetrischen Key-Austausch Algorithmen gelöst, z.B. Diffie-Hellman [58].

#### Bestehende Sicherheisarchitekturen

Der IEEE802.11 Standard beschreibt das Wired Equivalent Privacy (WEP) Protokoll als eine Option. WEP Verschlüsselung liegt auf Layer-1 auf, wo alle Kommunikationspartner

einer Zelle den selben symmetrischen Key teilen und einen Algorithmus mit inhärenter Schwachstelle verwenden [59]. Sobald der Key einer Drittpartei bekannt ist, können alle Pakete einer Zelle entschlüsselt werden. In Bezug auf Verschlüsselung ermöglichen neuere Erweiterungen einen per-session per-station Key, wie in WiFi Protected Access (WPA) beschrieben [60]. Ungeachtet dessen vertrauen viele WPAN Technologien weiterhin auf symmetrische Verschlüsselung mit Netzwerk-weiten statischen Keys. Dies ist offensichtlich der Einfachheit des Designs zuzuschreiben. Insbesondere bei Mesh-Netzwerken scheint dies am bequemsten zu sein.

### Mögliche Sicherheitsarchitekturen

In einem Mesh-Netzwek gibt es zwei Arten von Traffic (s. Abb. 2.8): Management Traffic zwischen allen WPAN Knoten erlaubt Erkennung, Verhandlung von Übertragungsparametern und Routing. Ein Grossteil dieses in-band Management Traffics hat broadcast oder multicast Charakteristik. Alle Knoten dienen als Endknoten. Im Falle von Punkt-zu-Punkt Kommunikation dienen alle Knoten zwischen den beiden Parntern als Zwischenknoten.

Aufgrund dieser Beobachtungen können zwei verschiedene Ansätze ins Auge gefasst werden: Gebrauch von geteilten identischen Keys mit allen Knoten im WPAN Netz für Management Traffic. Obwohl dies eine Grundlage für Angriffe darstellt, scheint es die einzig machbare Lösung für Breitbandtraffic zu sein. Dazu kommt, dass die Menge des erforderlichen Management Traffics relative gering ist, so dass kryptoanalytische Angriffe wenig Input zur Verfügung haben. Zusätzlich scheint es ein Fortschritt im Vergleich mit anderen WPAN oder WLAN Netzwerken zu sein, wo der Management Traffic gänzlich unverschlüsselt gesendet wird. Gebrauch von per-session per-connection Keys für den gesamten Datenverkehr mit Punkt-zu-Punkt Charakteristik.

Es gibt u.a. zwei Ansätze: Der klassische end-to-end VPN Ansatz, welcher in jedem Layer-Protokoll implementiert werden kann. Wahrscheinlich werden Protokolle auf Layer-2 oder Layer-3 zum Einsatz kommen. Diese Lösung ermöglicht ausserdem end-to-end Kommunikation mit Geräten ausserhalb des WPAN. Komplette VPN Protokolle könnten jedoch zu aufwändig sein für low-cost WPAN Knoten. Layer-1 Protokolle sind möglich, sind jedoch auf das WPAN beschränkt und enden am Gateway. Dieser Ansatz ist mehr auf low-performance Knoten ausgelegt.

### Ad-hoc Netzwerke und Authentifizierung

Ad-hoc (oder „spontanes“) Networking unterstützt Netzwerke mit plug-in Verbindungen, in welchen einige der Geräte nur für die Dauer eine Session Teil des Netzes sind und die Erkennung und Authentifizierung automatisch abläuft. Ad-hoc Networkiung und Sicherheit sind daher widersprüchliche Dinge, da diese Netze offen sein müssen für zusätzliche Geräte. Authentifizierung von Geräten und/oder Benutzern ist daher entscheidend um ein gewisses Mass an Sicherheit zu gewährleisten. Geräteauthentifizierung kann relative einfach vollzogen werden, jedoch können Eigenschaften wie MAC-Adressen gefälscht oder kopiert werden. In ist WLANs user-based Authentifizierung weit verbreitet. Dieses

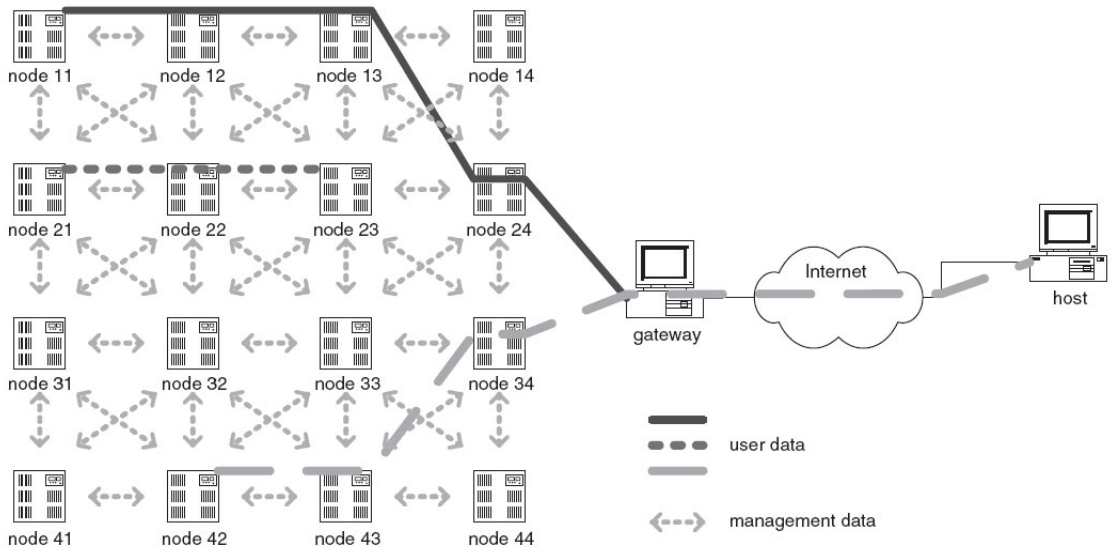



Abbildung 2.8: Traffic Charakteristika in Mesh-Netzwerken. [61]

Konzept kann auf Maschine-Maschine Kommuikation übertragen werden. Es wird vorausgesetzt, dass Maschinen die selbe Rolle wie menschliche Benutzer übernehmen, und gegen eine Datenbank verifiziert werden.

Eine zweistuffige Sicherheitsarchitektur wird vorgeschlagen: In einem ersten Schritt muss eine gegenseitige Authentisierung vollzogen werden. Zu diesem Zweck scheint eine geschlossene Public Key Infrastructure (PKI) angebracht, vorausgesetzt es werden asymmetrische Hash-Keys verwendet. Ein zentraler Knoten wie z.B. ein Gateway kann die Rolle des „trust centers“, der Authentifizierungsdatenbank, übernehmen. Die Glaubwürdigkeit dieses zentralen Knotens kann ausserdem per public-private Key überprüft werden. Der Paketfluss wird in Abb. 2.9 gezeigt. Es ist wichtig, dass nur public-key- und private-key-signierte Informationen via drahtlos Netzwerk übertragen wird. Daher ist einfaches abhören keine Bedrohung. Basierend auf diesem Verifizierungsablauf ist der Austausch von symmetrischen Keys pro Verbindung möglich. Dies führt zu den gängigen Hybrid-Architekturen welche in Protokollen wie SSL oder SSH verwendet werden. Dieser zweite Schritt sollte optional sein. Erstes ermöglicht gegenseitige Authentifizierung ein ausreichendes Sicherheitslevel für die meisten Systeme, zweitens verursacht Verschlüsselung relativ hohe Anforderungen an die Rechenkapazität der Knoten.

### 2.4.4 Einsatzgebiete

Gängigen Zeitungen, Technik-Zeitschriften oder grossen Elektronik-Geschäften nach, geht der heutige Trend geht eindeutig in Richtung Wireless. Während in den Sechziger Jahren revolutionär PS-starke Motoren auf den Markt kamen, in den Siebzigern die Transistoren, in den Achtzigern und Neunzigern die Mikroprozessoren aufkamen, so wird Wireless in der aktuellen Dekade Geschichte schreiben. [29]

Die Wireless Technologie hat den Alltag bereits verändert. Sie beeinflusst das Konsumverhalten. Die zivilisierten Menschen tragen heute andere Geräte mit sich, als noch vor

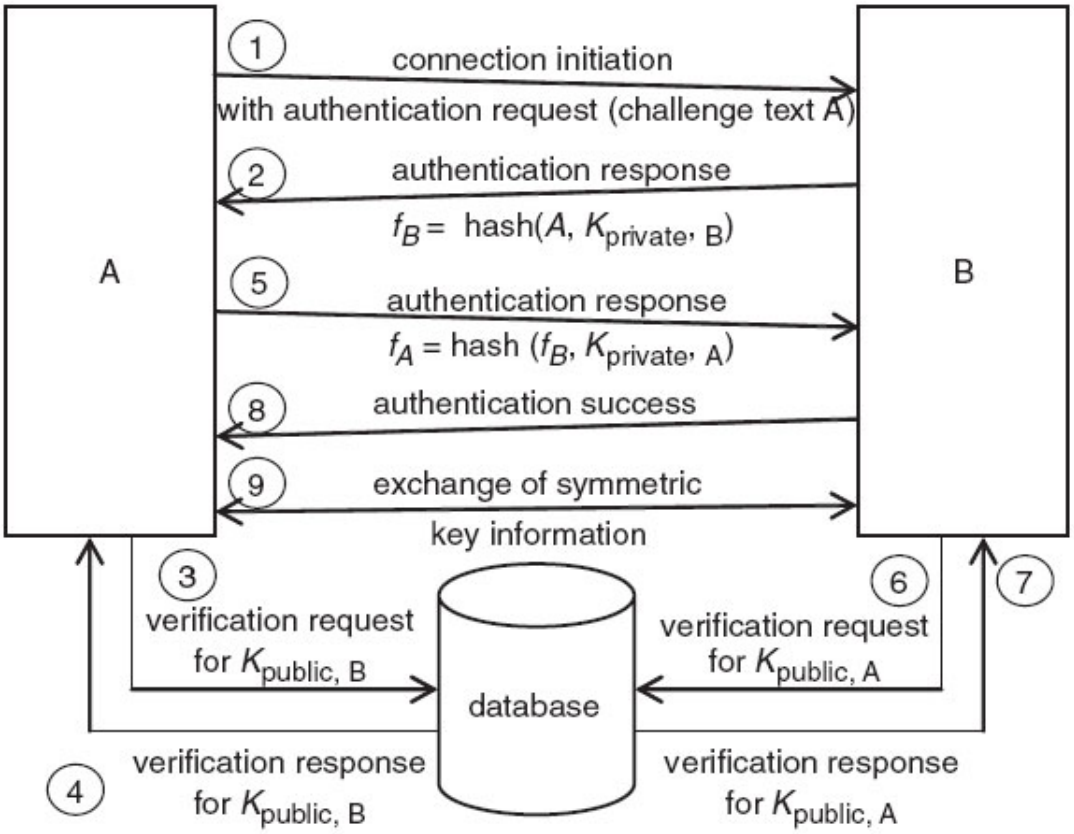



Abbildung 2.9: Authentifizierungsablauf und Key-Austausch. [61]

ein paar wenigen Jahren. Diese beeinflusst den Geschäftsalltag ebenso wie die Freizeit. So ist beispielsweise das Mobiltelefon heute kaum mehr wegdenkbar. Es dient nicht nur der Kommunikation, es widerspiegelt Lebensstile.

Welche Wireless-Technologien sind in der Fülle von Geräten vertreten, die heutzutage gekauft werden? Diese Frage ist nicht einfach zu beantworten. Wie in Abschnitt 2.3 zusammengefasst, ist keine Wireless-Technologie ist die universell anwendbare Technologie, jede deckt eine Nische ab. Die meisten sind für spezifische Gebiete anwendbar, jedoch gibt es viele Überschneidungen.

Im folgenden wird auf den Privat- und Heimgebrauch von zwei spezifischen Kurzdistanz-Wireless-Produkten eingegangen. Erst wird NFC (Near Field Communication), als Technologie mit grossem Zukunftspotential, und danach Bluetooth, als bereits sehr verbreitete Technologie, erläutert.

### Privat- und Heimgebrauch von NFC und Bluetooth

Die `Near Field Communication (NFC)` Technologie ermöglicht, basierend auf herkömmlichen Standards, zwischen elektronischen Geräten eine gänzlich kontaktlose Zwei-Weg-Interaktion. Diese Innovation erlaubt es Konsumenten, ihre elektronischen Geräte mühelos miteinander zu verbringen. So können die Konsumenten ihre PDAs, digitalen Kameras,

Computer und Notebooks, Mobil-Telefone sowie Lautsprecher bequem miteinander verbinden - Kabelgewirr sowie mühseliges Kabel einstecken entfällt.

Die Zukunftsvisionen der NFC Technologie sind gross. Trifft ein Konsument beispielsweise auf eine Konzertwerbung auf einem Plakat, so könnte er sein Mobil-Telefon oder PDA an den auf dem Plakat vorhandenen Tag (Smart Chip) halten. Dies ermöglicht es ihm, Informationen über das Konzert runter zu laden und bei Bedarf sogleich Tickets zu kaufen und diese dann elektronisch auf dem mobilen Gerät zu speichern. Diese elektronischen Tickets ermöglichen dem Konsumenten mühelos den Konzert-Eintritt, ohne je ein Papier in den Händen gehalten zu haben.

NFC soll den Konsum erleichtern, so kann der Konsument beispielsweise eine Reise anhand seines Computers buchen und die Tickets danach auf sein mobiles Gerät laden, in dem er dieses Gerät in die Nähe seines Computers bringt. Ist der Konsument nun am Flughafen, gelangt er ohne Weiteres zu seinen Reise-Informationen, in dem er sein mobiles Gerät an den Gate-Kiosk hält. [30]

Wie sieht es aus mit `Bluetooth`? Die `Bluetooth Special Interest Group (SIG)` gab bereits zum dritten Mal eine unabhängige Studie in Auftrag, die bei Konsumenten das Bluetooth Bewusstsein u.Ä. erforschte. [31] Die Studie befragte über 2100 Personen im Alter von 18 bis 70 Jahren in den USA, Grossbritannien, Deutschland, Taiwan und Japan und brachte interessante Ergebnisse heraus:

- Über zwei-drittel der befragten Taiwanesen besitzen mindestens ein Bluetooth-fähiges Gerät.
- Obwohl in Japan nur eine geringe Menge an Bluetooth Produkten vorhanden ist, sind die japanischen Konsumenten diejenigen, die am meisten bereit sind, viel für die Bluetooth-Funktionalität zu bezahlen.
- Wie in den USA und in Grossbritannien ist in Japan die Anzahl der Bluetooth Geräte in Headsets und Autos signifikant gewachsen.
- Verkäufe von mobilen Telefonen mit Bluetooth-Funktionalität sind massiv angestiegen. Am höchsten war der Anstieg in Taiwan mit 58% und in Deutschland mit 40%.
- Das Bluetooth Logo wird am ehesten in Deutschland erkannt, mit einer Wiedererkennungsrate von 69%.

Wo findet Bluetooth Anwendung? Die Diversität von Bluetooth Anwendungen ist gross. Mit Stand vom 15. April 2006 sind über 442 Produkte im Einsatz: [32]

Im Folgenden wird auf einige Produkte die in Tabelle 2.5 aufgelistet sind, beispielhaft eingegangen.

**Auto** Beispielsweise fährt eine Familie mit dem Auto in den Urlaub. Das Fahrzeug verfügt über ein GPRS Telefon System, über eine Bluetooth unterstützende Unterhaltungselektronik, wie eine Spielkonsole mit DVD-Player mit LCD-Bildschirmen (Liquid

Tabelle 2.5: Bluetooth-Produkte

| Anwendungsbereich | Anzahl Produkte |
|---|---|
| Audio und Visuell | 35 Produkte |
| Automobil | 37 Produkte |
| Games | 8 Produkte |
| Handhelds | 61 Produkte |
| Headset | 98 Produkte |
| Heim-Umgebungen | 102 Produkte |
| Input Geräte | 24 Produkte |
| Medizinischer Bereich | 6 Produkte |
| Telephonie | 93 Produkte |
| Mobil Telephonie Zubehör | 141 Produkte |
| Office Equipment | 127 Produkte |
| Personal Computer | 30 Produkte |
| Einzigartige Produkte | 69 Produkte |

Crystal Display) für die Kinder auf den Hintersitzen. Während der Fahrt benutzt die Fahrerin eines der Bluetooth-Headsets um das Hotel für die kommende Nacht zu reservieren, siehe untenstehendes Bild. Unterdessen laden die Kinder Spiele herunter und senden soeben gemachte Photos via MMS (Multimedia Messaging Service) oder E-Mail an ihre Schulkameraden.

Abbildung 2.10: Beispiel Bluetooth-Anwendung in Automobilindustrie [32]

Fahrzeug-Hersteller versuchen offensichtlich mit der Unterhaltungselektronik Schritt zu halten. Weiter versuchen sie, ihre Fahrzeuge so herzustellen, dass zukünftige Elektronik problemlos in ältere Fahrzeuge eingebaut werden kann. Ziel ist es, dass Fahrzeuge mit Baujahr 2008 mit Geräten mit Baujahr 2015 kompatibel sein sollen. Einige Fahrzeughersteller bekunden aber ihre Mühe mit der sich stetig ändernden Unterhaltungselektronik. Sie entwerfen vorerst ein Heer an neuen Fahrzeugen, die kompatibel mit Bluetooth sein werden.

Auf dem Sekundärmarkt sind bereits Geräte kaufbar, die es erlauben digitale, auf dem Mobiltelefon gespeicherte Musik mit der Auto-Stereo-Anlage abzuspielen.[33]

**Konsolen** Beispielsweise lädt Benjamin, 13jährig, auf einer bekannten Spiel-Webseite im Internet ein Java-basiertes Spiel runter. Via Bluetooth lädt er das Spiel von seinem Computer auf seine multifunktionale Spielkonsole, beispielsweise Zodiac-1. Als am Nachmittag sein Schulkamerad zu Besuch kommt, verbinden sie ihre Konsolen via Bluetooth und spielen das neue Spiel. Einige Tage später lädt Benjamin von Sandro ein Trailer auf sein Gerät, der ihm zeigt, dass es noch mehr Spiel-Levels gibt.

Abbildung 2.11: Zodiac-1. Mobile Unterhaltungskonsole [34]

**Computing** War früher der Schreibtisch mit Papier bedeckt, so ist er heute mit Kabeln umwunden. Jede Installation eines elektronischen Gerätes bringt mindestens ein Kabel mit sich: Maus, Tastatur, Bildschirm, PDA, Telefon-Synchronisationskabel, Digitalkamera, etc.. Diese Kabel sind nicht nur schwer zu ordnen, sie lassen sich auch schlecht verstecken. Bluetooth-fähige Tastatur, Maus, PDAs etc. vereinfachen den Computeralltag. Sie sind kabellos und sind problemlos anbring-, verschieb- oder entfernbar: Beispielsweise einfach die Mini-PilotMouse mit dem Bluetooth-Stick an den Computer anschließen und schon ist sie einsatzbereit. Wenn die Maus nicht mehr gebraucht wird, wird der USB-Mikroempfänger auf die Unterseite der Maus aufgesteckt und ist somit stets zur Hand. Beim Aufstecken des Empfängers schaltet sich die Maus automatisch aus, was auf einen sparsamen Umgang mit der Batterie hinweist.


Abbildung 2.12: PilotMouse Mini Wireless. Mobile kabellose Maus mit aufsteckbarem Empfänger [35]

**Telefonie** Die Kombination von einem Bluetooth unterstützendem Mobiltelefon und Notebook ermöglicht es einem auch ausserhalb des Büros in das Internet zu gelangen. Oder hat man zusätzlich zum Mobiltelefon ein Bluetooth unterstützendes Headset, ermöglicht dies einem das Telefon während der Gespräche in der Tasche zu lassen, und beide Hände sind frei für andere Tätigkeiten.

Die neuen Wireless Standards bringen eine Menge an neuen, serienmässig produzierten Produkten mit sich. Diese grosse Menge senkt die Kosten, was wiederum mehr Produzen-

ten auf den Markt lockt und Wireless noch populärer macht. Das geschätzte Zukunftspotential von Kurz-Distanz Wireless liegt somit sehr hoch. Die Produktpalette beschränkt sich nicht nur auf die Mobil-Telefonie, sie tangiert die Automobil-, Game-, und Büroindustrie ebenfalls. Sogar in der Medizin haben Bluetooth-Produkte Einhalt gefunden. Beispielsweise sind in Spitälern und Ambulanzen telemedizinische Systeme im Einsatz, die die Ärzte mit Informationen über den Patienten versorgen.

## 2.5 Regulatorische Aspekte

In der Schweiz befasst sich das Bundesamt für Kommunikation, kurz BAKOM, mit den Fragen der Telekommunikation, des Radio und des Fernsehens. Das BAKOM nimmt auf diesen Gebieten jegliche hoheitlichen und regulatorischen Aufgaben wahr. Es bereitet die Entscheide von anderen Bundesorganen vor, wie beispielsweise vom Bundesrat, von dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation, kurz UVEK, und von der Eidgenössischen Kommunikationskommission, kurz ComCom, vor.

Das BAKOM stellt die schweizerische Grundversorgung sicher, welche den Zugang zu einem minimalen Angebot an Telekommunikationsdienstleistungen garantiert. Die ComCom hat im Jahre 2002 für die Erteilung der Grundversorungskonzession ein öffentliches Ausschreibungsverfahren durchgeführt. Die einzige Bewerberin war Swisscom Fixnet AG. Somit wird bis 2007 die Grundversorgung schweizweit von Swisscom Fixnet AG garantiert. [36]

Im Folgenden werden erst regulatorische Aspekte der Schweiz beschrieben. [36] Nach diesen Erläuterungen wird ein Einblick in die regulatorischen Aspekte der Europäischen Union gewährt.

**Elektromagnetische Verträglichkeit und Umwelt, WLAN** Für drahtlose Netzwerke ist prinzipiell auch die Verordnung über den Schutz vor nichtionisierender Strahlung, kurz NISV [37], anzuwenden. Nichtionisierend sind UV- und Wärmestrahlung, Licht und Elektrosmog. Diese Energie ist nicht ausreichend, um die Bausteine von Lebewesen (Atome, Moleküle) zu verändern. Die technisch erzeugte nieder- und hochfrequente nichtionisierende Strahlung wird auch als Elektrosmog bezeichnet [38]. Die Einhaltung der Immissionsgrenzwerte der NISV können mit wenigen Millimeter Abstand zur Antenne bereits eingehalten werden. Aufgrund der geringen Sendeleistung von WLAN sind in der NISV keine Anlagengrenzwerte festgelegt. Es kann daher von einer Unbedenklichkeit in Bezug auf nichtionisierende Strahlung ausgegangen werden. Die einzelnen kantonalen Regelungen müssen dennoch beachtet werden.

**Standards, Frequenzen und Sendeleistungen für WLANs** Drahtlose Netzwerke, die folgende Standards gerecht werden, dürfen in der Schweiz betrieben werden:

- DECT
- IEEE 802.11

- IEEE 802.11b
- Hiperlan/1 (nur die untersten 3 Kanäle, jedoch sind keine Geräte auf dem Markt)
- Hiperlan/2 (nur die untersten 3 Kanäle, die restlichen Kanäle sind verboten)
- Bluetooth
- HomeRF

Der Betrieb von drahtlosen Netzwerken, nach folgenden Standards, ist in der Schweiz nicht erlaubt:

- IEEE 802.11a

RLANs (Radio-Local-Area-Network) nach dem Standard IEEE 802.11a arbeiten im 5 GHz-Band. Die Übertragungsraten gehen von 6 MBit/s bis 24 MBit/s, optional sogar bis 54 MBit/s. Dieser IEEE Standard sieht drei Frequenzbänder mit unterschiedlichen Sendeleistungen vor. Da leider dem IEEE 802.11a Standard einige Merkmale fehlen, wie beispielsweise die automatische Kanalwahl und Sendeleistungsregelung, ist er nicht mit HIPERLAN kompatibel. Deshalb ist in Europa der Einsatz von RLAN's nach IEEE 802.11a nicht vorgesehen. Bei einer zukünftigten Revision dieses Standards, die die fehlenden Merkmale definieren würde, würde einem Einsatz dieses Standards nichts mehr im Wege stehen. [41]

Über Geräte nach dem HiSwan-Standard kann noch keine Aussage gemacht werden, da sich dieser noch in Entwicklung befindet.

**Rechtliche Grundlagen** Die Verordnung über den Schutz vor nichtionisierender Strahlung (NISV)[37], soll die schweizer Bevölkerung vor Elektrosmog schützen. Sie setzt Höchstwerte für die kurzfristige Belastung der Menschen fest. Die nichtionisierende Strahlung ist in schweizer Wohn- und Arbeitsumfeldern allgegenwärtig. Sie entsteht bei jeglichen elektrischen Anlagen und Geräten. Der Geltungsbereich der NISV gliedert sich wie folgt:

Von der NISV erfasste Anlagen:

- Hochspannungsleitungen (Frei- und Kabelleitungen)
- Transformatorenstationen
- Unterwerke und Schaltanlagen
- Mobilfunkanlagen
- Richtfunkanlagen
- Drahtlose Teilnehmeranschlüsse (WLL)
- Rundfunkanlagen
- Betriebsfunkanlagen
- Amateurfunkanlagen
- Radaranlagen

Hingegen ist folgendes nicht in der NISV erfasst:

- Mobiltelefone
- Schnurlostelefone
- Bluetooth
- Mikrowellenöfen
- Kochherde
- Elektrische Geräte (wie Fernseher, Computermonitore, Radiowecker, Föhn, Rasierapparate, Bügeleisen, usw.)
- Medizinische Geräte
- Betriebsmittel am Arbeitsplatz

Für die von der NIV nicht geregelten Geräte benötigt es international anerkannte Vorschriften und Standards, um deren Strahlung zu begrenzen. Die Schweiz kann dies nicht im Alleingang erlassen. Ebenso sind die Immissionsgrenzwerte von der NISV international harmonisiert.

Die Frequenzbänder für WLANs sind der Klasse 3 zugeordnet. Es sind sogenannte Sammelfrequenzen die für eine unbegrenzte Anzahl Benutzer zur Verfügung stehen. In dieser Klasse gibt es keinen Schutz vor Störungen durch andere Systeme. Gemäss Art. 22 Abs.1 Fernmeldegesetz [39] ist jede Nutzung des Frequenzspektrums konzessionspflichtig. Das BAKOM hat aber, gestützt auf Art. 8 Bst. a Verordnung über Frequenzmanagement und Funkkonzessionen [40] (Art. 2 Abs.1 Bst e) die Funkanlagen von drahtlosen Netzen von der Konzessionspflicht ausgenommen. Solche WLAN-Anlagen benötigen also für die Nutzung des Frequenzspektrums keine Funkkonzession. Es können aber auch keine Funkkonzessionen für diese Frequenzbereiche erteilt werden, d.h. diese Anlagen dürfen nicht mit einer grösseren als der vorgeschriebenen Sendeleistung betrieben werden.

Werden jedoch WLAN-Anlagen für das Betreiben eines Fernmeldenetzes verwendet, mit welchen eine Anbieterin für Dritte (Teilnehmer oder andere Fernmeldedienstanbieterinnen) Fernmeldedienste (z.B. Sprachübertragung, Datenübertragungsdienste,...) erbringt, so ist eine Dienstekonzession gemäss Art. 4 Abs. 1 FMG9 erforderlich. Dabei spielt es keine Rolle ob das WLAN für den Teilnehmeranschluss oder für die Vernetzung von Fernmeldeanlagen eingesetzt wird. Das Verfahren für die Konzessionserteilung unterscheidet sich dabei nicht vom üblichen Verfahren für die Erteilung einer Dienstekonzession.

**Verordnung über Fernmeldeanlagen** Ab 2000 wurden die Bestimmungen der europäischen Richtlinie 99/05/EG (Radio & Telecommunications Terminal Equipment, R&TTE-Richtlinie) in die Schweizer Gesetzgebung eingebunden. Mit dieser Richtlinie wurden die Wünsche der Industrie umgesetzt, eine europäisch einheitliche Regelung für den Marktzugang von Telekommunikationsanlagen einzuführen. Das vorgängige Konformitätsbewertungsverfahren war die nationale Zulassung, ein langwieriges und zum Teil von Land zu Land verschiedenes Verfahren. Mit dem neuen Verfahren ist der Marktzugang schneller und günstiger möglich.

Die in der schweizerischen Verordnung über Fernmeldeanlagen `FAV` [45] umgesetzten Bestimmung können grob in 2 Kategorien eingeteilt werden: Die Formellen Anforderungen und die technischen Anforderungen. Die formellen Anforderungen decken

die Bereiche Anlagenidentifikation (Kennzeichnung), Anwendungseinschränkungen, Information und Anlagen-Notifikation (Meldung vor Marktzugang des Anlagentyps an die nationale Behörde) ab. Die technischen Anforderungen decken die so genannten grundlegenden Anforderungen, elektrische Sicherheit, elektromagnetische Verträglichkeit und effiziente Nutzung des Spektrums, ab. Als weitere technische Anforderung gilt das Einhalten des nationalen Frequenzzuweisungsplans `NaFZ` und somit das Einhalten der relevanten technischen Schnittstellenanforderung, da die Frequenzhoheit national bleibt.

**Nationaler Frequenzzuweisungsplan NaFZ** Die Frequenzzuweisung an die verschiedenen Funkdienste ist im nationalen Frequenzzuweisungsplan, NaFZ, geregelt [46]. Der NaFZ besteht aus dem eigentlichen Plan, Funkdienste nach Frequenzbereichen geordnet, und den Anhängen mit Regeln für die Benutzung des entsprechenden Frequenzbereichs. Der NaFZ basiert auf dem internationalen Radioreglement der International Telecommunication Unit, ITU [47] und den relevanten Publikationen der European Conference of Postal and Telecommunications Administrations, kurz CEPT [48]. Der nationale Frequenzzuweisungsplan folgt in der Regel deren Vorgaben. Der Plan gibt eine Übersicht über die nationale Verwendung des Frequenzspektrums und unterscheidet zwischen zivilen, militärischen oder geteilten Bändern, sowie zwischen primären und sekundären Zuweisungen. Künftig geplante Zuweisungen sind, soweit als möglich, vermerkt.

Spezifische Frequenzzuteilungen an verschiedene Benutzerkategorien sind direkt im Plan oder als Referenz zu den Anhängen eingetragen. Individuelle Frequenzzuteilungen an einzelne Frequenznutzer sind in der Regel nicht angeführt.

Die für die Benutzung der entsprechenden Frequenzbereiche notwendigen technischen Schnittstellen-Anforderungen sind im NaFZ referenziert. Diese Schnittstellenanforderungen beinhalten die technischen Randbedingungen, die eine Anlage einhalten muss, um in der Schweiz auf dem Markt gebracht und betrieben werden zu können [49]. Ein Bespiel hierzu ist die Schnittstellenanforderung für WLAN/RLAN [50].

Die Detailansicht für 2.4GHz-RLAN zeigt die technischen Rahmenbedingungen für solche Anlagen auf [51]. Die Normen, deren grundlegende Anforderungen eingehalten werden müssen, sind unter Punkt 11 aufgeführt. Diese Normen werden in den europäischen Gremien von Industrievertreter erstellt. Ein Beispiel einer solchen Organisation ist ETSI, das European Telecommunications Standards Institute [52].

**Frequenzbelegung** Die Frequenzbelegung ist historisch gewachsen. Seit einigen Jahren sind europaweit Bestrebungen im Gange, die Frequenzanwendungen zu harmonisieren. Die harmonisierten Anlagenklassen werden als Class-1 Equipment bezeichnet. Diese Class-1 Anlagen müssen den nationalen Behörden nicht mehr gemeldet werden. [53]

Informationen über die in Europa für die Short Range Devices verfügbaren Frequenzen und deren nationale Implementierung sind in der European Radiocommunications Committe, ERC/REC 70-03, zu finden. [54]

**Funkanlagen in Gebäuden** Nicht nur im Freien, sondern auch in unseren Wohnungen gibt es entsprechend immer mehr Funkanwendungen. Dies sind beispielsweise

schnurlose Telefone, Kopfhörer ohne Kabel, Babyfone oder WLAN-Stationen für den drahtlosen Zugang zum Internet. Zwar arbeiten alle diese Geräte mit einer relativ geringen Sendeleistungen, aber sie können die Belastung durch hochfrequente Strahlung in Innenräumen trotzdem dominieren. Um Funk-Immissionen möglichst gering zu halten, sollten diese Funkanlagen deshalb in genügendem Abstand zu geläufigen Aufenthaltsorten wie Bett, Sofa, Schreibtisch oder Kinderzimmer stationiert werden.

Bluetooth-Geräte arbeiten mit einer schwachen Sendeleistungen, entsprechend ist die Strahlenbelastung gering. Für Bluetooth-Geräte existieren drei Leistungsklassen mit maximalen Sendeleistungen von 1 mW, 2,5 mW oder 100 mW (mW = Milliwatt). Alle drei Leistungsklassen liegen tiefer als bei Funktelefon- (DECT, Digital Enhanced Cordless Telecommunications) und LAN-Anwendungen [38]. Somit ist der normale Gebrauch von Bluetooth-Geräten, nach heutigem Stand, unbedenklich.

Die rechtlichen Grundlagen der Schweiz sind im Vergleich mit der EU öffentlich gut ausmachbar. Auf den Internetseiten der BAKOM und admin.ch sind die entsprechenden Gesetzes- und Verordnungsartikel offen gelegt [36] [55] . Eine tiefere Recherche nach EU-Richtlinien über Funk- oder Kurz-Distanz-Wireless-Technologien gestaltet sich hingegen schwierig. Deshalb wird im Folgenden nur kurz auf gewisse Rechtsrahmen der EU eingegangen.

**Rechtsrahmen für die Frequenzpolitik in der EU** [42] Am 7. März 2002 entschied das Europäische Parlament und der Rat über einen Rechtsrahmen für die Funkfrequenzpolitik in der Europäischen Gemeinschaft (Frequenzentscheidung). Da Funkfrequenzen eine knappe Ressource sind, und die Nachfrage nach nutzbaren Funkfrequenzen in den letzten Jahren markant angestiegen ist, wurde die Verwaltung des Funkfrequenzspektrums zunehmend komplexer. Aus diesem Grund soll mit dem Entscheid ein allgemeines Verfahren zur Vereinheitlichung und Rationalisierung der Frequenznutzung innerhalb der Europäischen Union eingeführt werden.

Die Zuweisung der Funkfrequenzen erfolgt im Rahmen internationaler Organisationen, insbesondere auf den Weltfunkkonferenzen der Internationalen Fernmeldeunion, und in Europa durch die Europäische Konferenz der Verwaltungen für Post und Telekommunikation. Dank dieser Entscheidung möchte die EU auch im Rahmen des EG-Vertrags eine größere Rolle in diesem Bereich spielen. Deshalb gehören Funkfrequenzfragen erstmalig auch zum Anwendungsbereich der neuen europäischen Rechtsvorschriften im Bereich der Telekommunikation.

**Funkanlagen und Telekommunikationsendeinrichtungen** [43] Mit dieser Richtlinie wird in der Gemeinschaft ein Regelungsrahmen für das Inverkehrbringen, den freien Verkehr und die Inbetriebnahme von Funkanlagen und Telekommunikationsendeinrichtungen festgelegt. Ziel ist die Schaffung eines offenen, wettbewerbsbestimmten europäischen Marktes für Funkanlagen und Telekommunikationsendeinrichtungen und die Gewährleistung eines hohen Sicherheits- und Gesundheitsschutzniveaus.

**Elektromagnetische Verträglichkeit von elektrischen und elektronischen Geräten** [44] Durch eine vollständige Harmonisierung der Schutzanforderungen an alle elektrische und elektronische Geräte soll der freie Verkehr dieser Waren gewährleistet

werden. Die Richtlinien gelten für alle elektrischen und elektronischen Geräte sowie für Anlagen und Systeme mit elektrischen und/oder elektronischen Bauteilen, die elektromagnetische Störungen verursachen können oder deren Betrieb von diesen beeinträchtigt werden kann.

In den Richtlinien werden die Ziele bzw. wesentlichen Schutzanforderungen festgelegt, denen die zuvor beschriebenen Anlagen bei der Herstellung und vor Inverkehrbringen genügen müssen.

Die Europäischen Normungsgremien erarbeiten Europäische Normen, die auf wesentlichen Anforderungen basieren. Diese nicht-verbindlichen Normen werden im Amtsblatt der Europäischen Union veröffentlicht und in nationale Normen mit identischem Inhalt umgesetzt.

Die regulatorischen Aspekte der EU wie zuvor beschrieben sind nicht in dem Masse tiefgehend wie die Schweizerischen Regelungen. Durch mangelnde Information können die Aspekte nicht klar verglichen werden.

## 2.6 Fazit

Die in dieser Arbeit gezeigte Übersicht der Wireless-Technologien zeigt, dass unter den verschiedenen Standards ein grosse Wettbewerb herrscht. Während die Anforderungen an die drahtlose Datenübertragung stetig zunehmen, drängen immer wieder neue Verfahren und Technologien auf den Markt, welche diese neuen Bedürfnisse zu befriedigen versuchen. Der Trend geht ganz klar hin zur Spezialisierung. Unterschiedliche Standards decken sehr spezifische Bereiche ab, und können kaum zur universellen Datenübertragung verwendet werden. Als konkretes Beispiel sei hier insbesondere NFC erwähnt, welches neben bestehnden Standards wie Bluetooth eine ergänzende Rolle einnimmt.

Wie soeben erläutert, ist keine Wireless-Technologie ist die universell anwendbare Technologie, jede deckt eine Nische ab. Die meisten sind auf spezifische Andwendungen ausgelegt, jedoch gibt es viele Überschneidungen. Die neuen Wireless Standards bringen eine Menge an neuen, serienmässig produzierten Produkten mit sich. Durch die grosse, produzierbare Menge werden die Herstellkosten gesenkt, was wiederum mehr Produzenten auf den Markt lockt und Wireless noch populärer macht.

In der Schweiz ist prinzipiell für drahtlose Netzwerke die Verordnung über den Schutz vor nichtionisierender Strahlung, kurz NISV [37], anzuwenden. Die hoheitlichen und regulatorischen Aufgaben in der Schweiz nimmt jedoch auf dem Gebiet der Telekommunikation das Bundesamt für Kommunikation, kurz BAKOM, wahr. Informationen über die in der Europäischen Union für die Short Range Devices verfügbaren Frequenzen und deren nationale Implementierung sind in der European Radiocommunications Committe, ERC/REC 70-03, aufzufinden. [54] Wie in Abschnitt 2.5 erläutert, sind die regulatorischen Aspekte der EU schwierig zu recherieren und auszuwerten. Dies führte dazu, dass die regulatorischen Aspekte der Schweiz nicht abschliessend mit deren der EU verglichen werden konnten.

Die Kommunikation zwischen unterschiedlichen Geräten ermöglicht einzigartige und innovative Anwendungen. Obwohl Heute sehr leistungsfähige und ausgereifte Technologien

zum Einsatz kommen, bleibt der zugrundeliegende Mechanismus komplex und störungsanfällig. Dementsprechend sind auch die modernsten Übertragungsverfahren noch nicht in der Lage, den kabelgebundenen Technologien in Sachen Sicherheit, Stabilität oder auch Datenübertragungsrate Paroli zu bieten. Somit werden auch heute noch Geschäftsgebäude mit kilometerlangen Kabelsträngen ausgerüstet, was ein nicht vernachlässigbarer Kostenfaktor ist. Dies zeigt, dass in den Wirelesstechnologien noch viel Entwicklungspotential steckt, und dass bisher noch kein Hersteller einen Standard geschaffen hat, welchem die Konsumenten zweifellos vertrauen. Das Potential des zukunftsträchtigen Marktes der Wirelessprodukte ist enorm gross, was die Investitionen in neue Technologien immer weiter ansteigen lässt.

Noch existieren auf dem Markt unzählige Standards für sehr spezifische Anwendungsbereiche. Dies ermöglicht den heutigen Geräten die Kommunikation über diverse Schnittstellen, hat andererseits aber auch zur Folge, dass ein universell einsetzbares Gerät eine Vielzahl von Technologien unterstützen muss um die Kompatibilität sicherstellen zu können. Dass die Benutzerfreundlichkeit unter diesem Umstand leidet ist nicht zu übersehen. Die teils sehr komplexen Konfigurationsmöglichkeiten beispielsweise der Übertragungsverschlüsselung überfordern den typischen Anwender. Da das Rennen zwischen den Technologien aber meist nicht im Bereich der Benutzerfreundlichkeit, sondern eher bezüglich der Datenübertragungsrate oder Reichweite stattfindet, ist der Entwicklungsbedarf in diesem Bereich noch besonders gross.

# Literaturverzeichnis


[1] Wikipedia Deutschland: IrDA http://de.wikipedia.org/wiki/Irda, 14.04.2006.

[2] Wikipedia Deutschland: Infrarot http://de.wikipedia.org/wiki/Infrarot, 14.04.2006.

[3] ad: Standard für Infrarot-Datenübertragung, Heise c't, 05.1994.

[4] Wikipedia Deutschland: Bluetooth http://de.wikipedia.org/wiki/Bluetooth, 14.04.2006.

[5] Wikipedia USA: Bluetooth http://en.wikipedia.org/wiki/Bluetooth, 14.04.2006.

[6] Jürgen Kuri: Wellenbrecher - Von Funk bis Telefon - Alternativen für die Heimvernetzung, Heise c't, 06.1999.

[7] Wikipedia Deutschland: WLAN http://de.wikipedia.org/wiki/Wlan, 14.04.2006.

[8] Wikipedia USA: WLANhttp://en.wikipedia.org/wiki/Wlan, 14.04.2006.

[9] Female Inventors: Hedy Lamarr http://www.inventions.org/culture/female/lamarr.html, 15.04.2006.

[10] Wikipedia Deutschland: IEEE 802.11 http://de.wikipedia.org/wiki/IEEE_802.11, 15.04.2006.

[11] Wikipedia Universität Konstanz: WLAN http://wiki.uni-konstanz.de/, 15.04.2006.

[12] IEEE 802 LAN/MAN Standards Committee http://ieee802.org/, 15.04.2006.

[13] Wi-Fi Alliance http://www.wi-fi.org/, 15.04.2006.

[14] news.ch: Schnelleres WLAN mit 802.11n-Draft-Produkten http://www.news.ch/239289/detail.htm, 16.04.2006.

[15] IEEE 802.11 WIRELESS LOCAL AREA NETWORKS - The Working Group for WLAN Standards http://grouper.ieee.org/groups/802/11/, 07.06.2006.

[16] Zoubir Irahhauten, Homayoun Nikookar, Gerard J.M. Janssen: An Overview of Ultra Wide Band Indoor Channel Measurements and Modeling, IEEE Microwave and Wireless components letters vol. 14 No. 8, 08.2004.

[17] Dominic Bremer: Near Field Communication (NFC)http://www.medien.ifi.lmu.de/fileadmin/mimuc/mmi_ws0506/essays/uebung2-bremer.html, 08.06.2006.

[18] NFC Forum http://www.nfc-forum.org, 08.06.2006.

[19] Wikipedia USA: Near Field Communication http://en.wikipedia.org/wiki/Near_Field_Communication, 09.06.2006.

[20] Maplin Electronics http://www.maplin.co.uk, 09.06.2006.

[21] Wikipedia Deutschland: RFID http://de.wikipedia.org/wiki/RFID, 09.06.2006.

[22] The RFID Weblog: Implementation and Application of RFID technology http://www.rfid-weblog.com, 09.06.2006.

[23] Radio Frequency Identification http://www.rfid-handbook.de, 09.06.2006.

[24] Die StopRFID-Seiten des FoeBuD e.V. http://www.foebud.org/rfid, 09.06.2006.

[25] Hyangjin Lee, Jeeyeon Kim: Privacy threats and issues in mobile RFID, Korea Information Security Agency, 09.06.2006.

[26] Wikipedia USA: Ultra Wideband http://en.wikipedia.org/wiki/Ultra_wideband, 09.06.2006.

[27] IJAK Solutions http://www.ijak.com, 09.06.2006.

[28] Wireless Developer Network http://www.wirelessdevnet.com, 09.06.2006.

[29] Mobile Data Association, http://www.mda-mobiledata.org/mda/, 15.04.2006.

[30] Near Field Communication Forum, NFC, http://www.nfc-forum.org, 14.04.2006.

[31] The Official Bluetooth Membership Site, https://www.bluetooth.org, 14.4.2006.

[32] The Official Bluetooth Web Site, http://www.bluetooth.com, 15.4.2006.

[33] Washington DC 6. April 2006, The Auto Channel, http://www.theautochannel.com/, 15.4.2006.

[34] Tapwave Inc. http://www.tapwave.com/zodiac.html, 3.6.2006.

[35] Kensington Computer Products Group, http://de.kensington.com/html/10728.html, 3.6.2006.

[36] Bundesamt für Kommunikation, BAKOM, http://www.bakom.ch/themen/, 15.4.2006.

[37] Verordnung vom 23. Dezember 1999 über den Schutz vor nichtionisierender Strahlung (NISV), http://www.admin.ch/ch/d/sr/c814_710.html, 15.4.2006.

[38] Departement für Umwelt, Verkehr, Energie und Kommunikation. Bundesamt für Umwelt, BAFU, http://www.umwelt-schweiz.ch/buwal/de/, 15.4.2006.

[39] Fernmeldegesetz vom 30. April 1997 (FMG), http://www.admin.ch/ch/d/sr/c784_10.html, 15.4.2006.

[40] Verordnung vom 6. Oktober 1997 über Frequenzmanagement und Funkkonzessionen (FKV), http://www.admin.ch/ch/d/sr/c784_102_1.html, 16.4.2006.

[41] Faktenblatt über Radio Local Area Networks (RLAN), Bundesamt für Kommunikation, http://expired.id.unibe.ch/network/wireless/RLAN.pdf.

[42] Rechtsrahmen für die Frequenzpolitik, Tätigkeitsbereiche der Europäischen Union, http://europa.eu/scadplus/leg/de/lvb/l24218a.htm, 4.6.2006.

[43] Funkanlagen und Telekommunikationsendeinrichtungen, Tätigkeitsbereiche der Europäischen Union, http://europa.eu/scadplus/leg/de/lvb/l21003a.htm, 4.6.2006.

[44] Elektromagnetische Verträglichkeit von elektrischen und elektronischen Geräten, Tätigkeitsbereiche der Europäischen Union, http://europa.eu/scadplus/leg/de/lvb/l21008.htm, 4.6.2006.

[45] Rechtliche Grundlagen, Verordnungen: Geräte und Anlagen, Bundesamt für Kommunikation BAKOM, http://www.bakom.admin.ch/org/grundlagen/00955/01279/index.html?lang=de, 1.7.2006.

[46] Frequenzen & Antennen, Frequenzpläne: Nationaler Frequenzzuweisungsplan NaFZ, Bundesamt für Kommunikation BAKOM, http://www.bakom.admin.ch/themen/frequenzen/00652/00654/index.html?lang=de, 1.7.2006.

[47] International Telecommunication Union, ITU, http://www.itu.int/home/index.html, 1.7.2006.

[48] European Conference of Postal and Telecommunications Administrations, CEPT, http://www.cept.org/, 1.7.2006.

[49] Rechtliche Grundlagen, Vollzugspraxis: Geräte und Anlagen, Bundesamt für Kommunikation BAKOM, http://www.bakom.admin.ch/org/grundlagen/00563/00575/01285/index.html?lang=de, 1.7.2006.

[50] Technische Schnittstellen-Anforderungen, Drahtlose lokale Netze (SRD), Schweizerische Eidgenossenschaft, Bundesamt für Kommunikation BAKOM, http://www.ofcomnet.ch/cgi-bin/rir.pl?id=1010, 1.7.2006.

[51] Radio Interface Regulation (RLAN 2.4GHz), OFCOM, Federal Office of Communications, http://www.ofcomnet.ch/cgi-bin/rir.pl?id=1010;nb=01, 1.7.2006.

[52] European Telecommunications Standards Institute, ETSI, www.etsi.org, 1.7.2006.

[53] Classification of equipment in accordance with the R&TTE Directive (1999/5/EC), European Radiocommunications Office, http://www.ero.dk/rtte?mid=BB4994F2-8411-4AA9-A6E5-CE893A0E3E5E&frames=no, 30.6.2006.

[54] ERC RECOMMENDATION 70-03, Recommendation adopted by the Frequency Management, Regulatory Affairs and Spectrum Engineering Working Groups, European Radiocommunications Office, `http://www.ero.dk/documentation/docs/docfiles.asp?docid=1622&wd=N`, Version 17.11.2005.

[55] Geräte & Anlagen: Merkblätter, Bundesamt für Kommunikation BAKOM, `http://www.bakom.admin.ch/themen/geraete/00464/index.html?lang=de`, 30.6.2006.

[56] Mackensen, E., Kuntz, W., and M.uller, C.: „Smart wireless autonomous microsystems (SWAMs) for sensor actuator networks“. Presented at SIcon 2004 Conf., New Orleans, USA, January 2004.

[57] Eckert, C.: „IT-Sicherheit“ (Oldenbourg,Munich, Vienna, 2003), ISBN 3-486-27205-5.

[58] Diffie, W., and Hellman, M.E.: „New directions in cryptography“, IEEE Trans. Inf. Theory, 1976, 22, pp. 644 bis 654.

[59] Borisov, N., Goldberg, I., and Wagner, D.: „Security of the WEP algorithm“. Available at: `http://www.isaac.cs.berkeley.edu/isaac/wepfaq.html`.

[60] Wi-Fi Protected Access, available at: `http://www.weca.net`.

[61] A. Sikora: Design challenges of short-range wireless networks, IEE Proc.-Commun., Vol. 151, Oktober 2004s.

# Kapitel 3

# Trusted Computing – Blessing or Danger

*Richard Meuris, Claude Humard, Philippe Hochstrasser*

*Digital gehaltene Daten nehmen im heutigen Informations-Zeitalter einen nicht zu unterschätzenden Stellenwert ein. Dies gilt sowohl für kommerzielle Unternehmen wie auch für Staatsbetriebe. Die weltweit fortschreitende Vernetzung von Informationssystemen setzt diese digitalen Güter dem Risiko externer Attacken aus, deren Zahl in den vergangenen Jahren stetig wuchs. Trotz des vermehrten Einsatzes diverser Sicherheitstools ist es bis heute nicht gelungen, ein mehr oder weniger lückenloses Sicherheitsnetz bereitzustellen. Die Initiative "Trusted Computing" will auf Soft- und Hardwareebene mittels verschiedener Funktionen wie "Integrity Protected Booting", Verschlüsselung, "Sealed Storage" und "Remote Attestation" diese Lücken grösstenteils schliessen und sich als Standard der nächsten Generation von Computersystemen etablieren. Ferner wird als eine Anwendung von "Trusted Computing" das höchst umstrittene "Digital Rights Managements" aufgegriffen und erklärt. In dieser Arbeit werden sowohl die technischen Eigenheiten des diesen Funktionen zugrundeliegenden Computerchips Trusted Platform Module betrachtet als auch zwei Varianten der Trusted Computing Architektur behandelt: NGSCB ("Next Generation Secure Computing Base" von Microsoft) und die offene Sicherheitsarchitektur Perseus. Am Schluss werden unter anderem die möglichen Konsequenzen auf den IT-Markt erörtert und der versprochene Mehrnutzen bzw. mögliche nachteilige Folgen für die Stakeholder (Industrie, Business, Privatnutzer) hintergefragt.*

## Inhaltsverzeichnis

**3.1 Einleitung . . . . . 77**
**3.2 Sicherheitsumfeld . . . . . 78**
3.2.1 Risiken und Attacken . . . . . 79
3.2.2 Sicherheitsparadigmen . . . . . 83
3.2.3 Heutige Sicherheitstools . . . . . 84
3.2.4 Zusammenfassung . . . . . 85
**3.3 Problemstellungen und Ansätze von Trusted Computing . . 85**
3.3.1 Trusted Computing . . . . . 86
3.3.2 Trusted Platform . . . . . 86
3.3.3 Problemstellungen und Ansätze von Trusted Computing . . . . 87
3.3.4 Zusammenfassung . . . . . 89
**3.4 Technische Ansätze von Trusted Computing . . . . . 90**
3.4.1 Trusted Computing Group . . . . . 90
3.4.2 Intel LaGrande Technology . . . . . 95
3.4.3 The Perseus Security Architecture . . . . . 96
3.4.4 Microsft Next-Generation Secure Computing Base . . . . . 98
3.4.5 Zusammenfassung . . . . . 99
**3.5 Das Umfeld von TC . . . . . 99**
3.5.1 TC und Sicherheit . . . . . 100
3.5.2 TC und DRM . . . . . 101
3.5.3 Interessengruppen . . . . . 103
**3.6 Zusammenfassung . . . . . 106**

## 3.1 Einleitung

Aufgrund der in den letzten Jahren stark angestiegenen Vernetzung zwischen der immer grösser werdenden Anzahl von Computersystemen und dem Einsatz immer komplexerer IT-Software ist auch die Zahl der Schwachstellen und den damit verbundenen Bedrohungen stark angestiegen [20]. Lediglich ist nicht zu erwarten, dass die Mittel für die IT-Sicherheit linear mit den Bedrohungen wachsen werden. Zu beachten ist, dass nur ein kleiner Bruchteil der Computerkriminalität gemeldet wird, wodurch das Ausmass der ständig vorkommenden Attacken auf heutige Computersysteme unbekannt bleibt. Einerseits wird dadurch also die Wichtigkeit von IT-Sicherheit (welche sich mit der sicheren Speicherung, Verarbeitung und Übertragung von Daten befasst [28]) vielfach unterschätzt, andererseits wird die Wirksamkeit eingesetzter Sicherheitstechnologien wie Firewall- und Antiviren-Software deutlich überschätzt. [20]. Die IT-Sicherheitsverantwortlichen befinden sich in einer prekären Lage: Werden präventive Massnahmen (Schulungen, entsprechende Software etc.) durchgeführt und dadurch Schäden vermieden, könnte der Sinn dieser Ausgaben undeutlich werden, da Sicherheit nicht direkt messbar ist (es ist nur sehr schwer abschätzbar, wie hoch die Schäden bei geringerer Sicherheit wären). Treten jedoch Schäden auf, werden diese Ausgaben in Frage gestellt, da der Schadensfall nicht verhindert werden konnte.

Eine zentrale Frage im Bereich der IT-Sicherheit ist also, wieviel Geld für welche Massnahmen ausgegeben werden soll. Diese Frage stellen sich natürlich nicht nur Unternehmungen, sondern auch die Privatnutzer, welche gegen Attacken bestmöglichst gefeit sein wollen. Als mehr oder weniger allumfassende Sicherheitsarchitektur will sich Trusted Computing als Sicherheitslösung anbieten. Obwohl der von Trusted Computing benötigte Chip schon in einigen Computersystemen implementiert ist, wird davon heutzutage (2006) noch kaum Gebrauch gemacht.

Im ersten Kapitel wird das aktuelle Sicherheitsumfeld betrachtet: Dazu gehören die vorhandenen Risiken und Attacken, welche Trusted Computing effektiver als die bisherigen aufgesetzten Sicherheitstools bekämpfen will. Die von Trusted Computing als eine auf dem Motherboard implementierte Hardware-Architektur gebotene Funktionalität wird im zweiten und dritten Kapitel dargestellt. Das Konzept des Trusted Computing wird einerseits von einem Konsortium namens Trusted Computing Group, aber auch durch mehrere Einzelorganisationen in entsprechenden Varianten vorangetrieben, auf welche im dritten Kapitel dieser Arbeit eingegangen wird. Ferner wird eine Übersicht der zugrundeliegenden Hardware gegeben. Im vierten Kapitel schliesslich werden mögliche Vor- und Nachteile für die entsprechenden Stakeholder[1] betrachtet, gegeneinander abgewogen und es wird letztendlich versucht zu ermitteln, wie hoch jeweils der Nutzen von Trusted Computing sein könnte. Als mögliche Anwendung soll auch das vor Datendiebstahl schützende Digital Rights Management (kurz DRM) betrachtet werden, welches dank Trusted Computing effektiver zu werden verspricht, obwohl die neue Architektur eigentlich nicht speziell für diese Anwendung konzipiert wurde.

[1] Hersteller, Unternehmen, Privatnutzer

## 3.2 Sicherheitsumfeld

Sicherheit wird als ein Zustand des Nichtvorhanden- oder Geschütztseins vor Bedrohungen und Risiken definiert, wobei Sicherheit stets relativ (situationsbezogen) und nicht direkt messbar ist, was Sicherheit zu einer subjektiv wahrnehmbaren Grösse macht [28]. Vor der heutigen Ära des Internets und der damit geförderten weltweiten Vernetzung war der Aufwand zur Gewährleistung eines akzeptablen Sicherheitslevels noch weit weniger hoch: Einerseits war die eingesetzte Software noch um ein Vielfaches weniger komplex und damit meist weniger anfällig für Sicherheitslöcher, welche bei der heutigen Software meist nicht einmal entdeckt, geschweige denn korrigiert werden. Andererseits war die Übertragung von schädlichem Programmcode (sogenannter Malware, auf welche in diesem Kapitel noch eingegangen wird) meist auf den physischen Austausch von Datenträgern (Disketten und Bänder) angewiesen, was die damalige Verbreitung doch ziemlich limitierte.

Heutzutage ist aufgrund der globalen und lokalen Vernetzung hingegen die Infektion hunderttausender von Computern innerhalb kürzester Zeit möglich, was erheblich höhere Anforderungen an die IT-Sicherheit stellt [27]. Ferner ist der Gesamtwert der heutigen abgespeicherten Informationen wesentlich höher als noch vor Jahrzehnten, wo ein Verlust der Daten in vielen Fällen womöglich noch halbwegs verkraftbar war, da sie nicht nur digital gespeichert waren[2]. In der heutigen Zeit kann Datenspionage und -verlust verheerende Konsequenzen für soziale, wirtschaftliche und staatliche Organisationen haben [36]. In naher Zukunft schon könnte das Brechen von Sicherheitsmechanismen zu volkswirtschaftlichen Desastern führen, falls es beispielsweise keine Alternativen mehr zu E-Commerce (elektronischer Handel) gäbe. So mag es kaum verwundern, dass sich nicht mehr nur Informatiker mit dem unternehmerisch und gesellschaftlich sehr relevanten Aspekt der IT-Sicherheit beschäftigen.

Obwohl Attacken auf Computersysteme ständig stattfinden, vermögen vor allem medienpräsente physisch erfassbare Ereignisse wie die terroristischen Anschläge vom 11.September 2001 auf die U.S.A. das Bedürfnis an grösserer IT-Sicherheit zu forcieren, obwohl dieser Anschlag im Gegensatz zu den gewaltigen menschlichen und wirtschaftlichen Verlusten nur geringfügige IT-bezogene Schäden mit sich brachte. Die Bedrohungslage, der die IT-Sicherheit präventiv und retrospektiv gegenübertritt, ist charakterisiert durch eine zunehmende Angriffsdichte sowie das ständige Auftreten neuer Angriffsformen [20]. Gefragt sind heute nicht mehr nur Flexibilität, Erweiterbarkeit und Bedienungsfreundlichkeit der Computersysteme, sondern auch die immer wichtiger werdenden Qualitäten wie Verfügbarkeit, Vertraulichkeit, Integrität (Schutz des Datentransfers vor Veränderungen), Authentizität und Anonymität [29] [30]. Kosten-Nutzen-Überlegungen für die IT-Sicherheit gestalten sich jedoch schwierig und haben oft den Charakter von Glaubenskriegen, da sich die Erarbeitung einer Bedrohungs-und Risikoanalyse in der Praxis äusserst schwierig gestaltet [20] [28]. Jedoch ist klar, dass sich für Unternehmen Investionen in die IT-Sicherheit ausbezahlen können: Beispielsweise passen Versicherungsagenturen ihre Raten an den gewährleisteten Schutz der Computersysteme an [13].

[2]Diese Redundanz kann man sich heute aber in der Regel nicht mehr leisten

### 3.2.1 Risiken und Attacken

Die zentrale Frage der IT-Sicherheit besteht darin, wie ein Informatiksystem und seine Betriebsmittel (insbesondere die Daten) vor Angriffen (von innen und aussen) geschützt werden kann [28]. Die mögliche Schadenwirkung von Angriffen wird begünstigt durch die Vernetzung von immer mehr Geräten (PC, PDA, Mobiltelefone etc.), welche damit zu potenziellen Zielen werden, aber auch durch Informationen (z.B. Publikation von Angriffs-Software im Internet), die solche Angriffe ermöglichen. Die Motivation der Angreifer variiert inzwischen stark: Neben klassischen Motiven wie dem Erfolgserlebnis (Hacker) oder der Kompensation von Frustrationen (unzufriedene Mitarbeiter) tauchen zunehmend kommerzielle Motive auf, z.B. beim Verkauf gestohlener E-Mail-Adressen an Spammer (Absender unerwünschter Mails) oder beim Verkauf gestohlener Kreditkartendaten an kriminelle Organisationen [20]. Die Angriffe sind heute also diversifizierter angelegt und umfassen neben der technischen Realisierung oft Elemente des Social Engineerings, welche auf soziale Faktoren (z.B. Angst, Handlungsdruck) bauen, um das erwünschte Verhalten des Opfers zu erreichen (z.B. die Preisgabe von Zugangsinformationen). Da Trusted Computing solche nichttechnischen Angriffsformen nicht unmittelbar zu bekämpfen vermag, soll auf sie nicht weiter eingegangen werden. Vielmehr soll kurz auf die allgegenwärtige Problem der schädigenden Malware[3] eingegangen werden, welches Trusted Computing zu vermindern verspricht.

#### Malware

Malware lässt sich gemäss [28] z.B. in vier Hauptklassen von Softwareanomalien und -manipulationen einteilen: Viren, Würmer, Trojanische Pferde und auch Programmierfehler, wobei Programmierfehler je nach Begriffsdefinition nicht immer als Malware betrachtet werden. Moderne Malware tritt immer häufiger als eine Kombination von Viren, Würmern und Trojanischen Pferden auf. Das Kernproblem im Kampf gegen Malware liegt in der Schwierigkeit, gutartigen von bösartigem Programmcode zu unterscheiden. Malware kann in jedem Schritt der Softwareentwicklung eingebracht werden (also auch während der Kompilierung) und deshalb kann potentiell jede Software Träger von Malware sein. Somit löst eine blosse Inspektion des Sourcecodes das Problem in der Regel nicht [28]. Bösartige Malware ist im Gegensatz zu früher (vor den Mitteneunzigern) heutzutage auch von Laien mithilfe entsprechender frei verfügbarer Tools programmierbar. Ein besonderes Problem stellen vor allem in einer High-Level-Scripting-Sprache (wie jene von Microsoft Office) programmierte Malware-Erreger dar, da sie plattformunabhängig agieren können und sich somit mittels Dokumenttransfers schneller verbreiten, ohne auf eine plattformspezifische binäre Datei als Träger angewiesen zu sein [27]. Die Malwarehäufigkeit hat in den letzten Jahren überproportional zugenommen. Selbst schon in Nischenmärkten wie beispielsweise demjenigen der Smartphones hat die Menge der Malware-Erreger in den vergangenen Monaten markant zugenommen (vergleiche Abbildung 3.1 unten). Malware stellt also nicht nur ein Sicherheitsproblem für Computersysteme dar, sondern auch für komplexe Kleinstgeräte [19]. Deshalb wird für Mobiltelefone an einem adaptierten Trusted Computing-Standard gearbeitet [34].

[3] Stammt vom englischen Ausdruck "malicious code" für schädlichen Programmcode

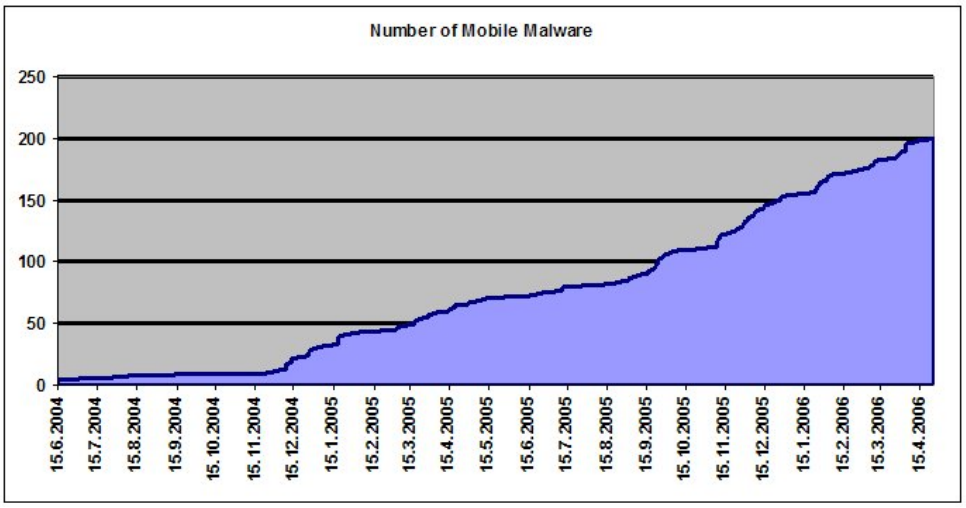



Abbildung 3.1: Zunahme der Malware bei Smart Phones [19].

Trusted Computing verspricht einen Grossteil der Malware in PC-Applikationen zu erkennen und den Bedürfnissen des Nutzers entsprechend Konsequenzen zu ergreifen wie z.B. die Nichtausführung entsprechend sicherheitstechnisch problematischer Software. Es soll aber diesbezüglich betont werden, dass Trusted Computing lediglich eine Hilfe im Kampf gegen Malware, aber niemals ein Garant für ein Malware-freies System darstellt.

**Viren** Viren gehören wahrscheinlich zu den prominentesten Vertretern von Malware, wobei das erste Virus bereits 1981 programmiert wurde [21]. Ein Computervirus setzt sich aus dem Vermehrungs-, Schadens- und Tarnungsteil zusammen, wobei der den Auslöser (Datum, Tastatureingaben etc.) definierenden Schadensteil nicht zwangsläufig vorkommen muss. Heutige Antivirenprogramme identifizieren Viren anhand deren Vermehrungsteil. Somit haben es diese Sicherheitstools aber besonders bei Viren schwer, welche ihren Vermehrungsteil (d.h. ihre Kennung) ständig alterieren (sogenannte polymorphe Viren). Hier soll Trusted Computing greifen und einen besseren Schutz bieten, indem schädliche Programmfragmente erst gar nicht ins System eingeschleust werden [28].

**Würmer** Seit medienwirksamen Ereignissen, wie die durch Würmer (z.B. Melissa 1999, ILOVEYOU 2000, Sasser 2004) entstandenen Schäden in Milliardenhöhe, sind auch Würmer nicht mehr ganz so unbekannt wie noch im Jahre 1988, als experimentell ein erster Wurm programmiert wurde, der mittels Wörterbuchattacken (viel verwendete Wörter werden als Passwort ausprobiert) in viele Systeme eindringen konnte, und somit das Schadenspotential von Würmern aufgezeigt wurde. Unter einem Computerwurm versteht man selbstständigen Programmcode, der in der Lage ist, sich im Netz zu reproduzieren und sich dynamisch über laufende Prozesse weiterzuverbreiten [28]. Im Gegensatz zu Viren richten Würmer häufig keinen direkten Schaden an, jedoch können sie aufgrund ihrer Autoreproduktion und Ausbreitung die Performance von Systemen vermindern.

**Trojanische Pferde** Unter einem trojanischen Pferd oder Trojaner versteht man mit böswilliger Absicht geschriebenen (von evtl. Hackern eingeschleusten) Programmcode, der eine versteckte und nicht spezifizierte bzw. dokumentierte Zusatzfunktion in einem Anwendungs-, Dienst- oder Spielprogramm implementiert. Diese Zusatzfunktion kann die Manipulation des Systems oder die Installation einer Hintertür darstellen [28]. Ein Beispiel von Trojanischen Pferden ist Spyware, die an sensitive Daten des Nutzers wie Kreditkartennummern gelangen will. Der Unterschied zu Viren und Würmern liegt darin, dass sie sich nicht replizieren. Trojanische Pferde werden somit v.a. bei spezifischen Attacken verwendet, wo es darum geht, bestimmte Systeme anzugreifen.

**Programmierfehler** Unter einem Programmierfehler (engl. bug) versteht man einen unbeabsichtigten Fehler in der Programmierung, so dass ein Programm sich nicht gemäss seiner Spezifikation verhält oder gar abstürzt [28]. Die stetig steigende Komplexität von IT-Umgebungen führt zu immer mehr Schwachstellen und damit Risiken. Entsprechende Sicherheitsmassnahmen sind somit schwerer zu erstellen und zu betreiben. Da zudem zwischen der Erkennung einer Schwachstelle und der Information des Herstellers, der Überprüfung des Sachverhalts und der Erstellung und Ausbreitung entsprechender Patches (neukompilierter fehlerbereinigter Programmcode) eine gewisse Zeitspanne vergeht, ist die Angreiferseite hier ebenfalls potenziell im Vorteil, vor allem dann wenn die Patches von den Nutzern erst gar nicht installiert werden [20]. Für Unternehmungen stellt das zu organisierende Patch-Management einen erheblichen Mehraufwand dar [28]. Trusted Computing könnte hier insofern eine positive Auswirkung haben, als dass Softwarehersteller zwecks TC-Konformität motiviert sein könnten, qualitativ bessere Programme zu schreiben, denn sollte Trusted Computing sich eines Tages als Standard etablieren, wird es Software, welche z.B. die von TC unterstützten Common Criteria (Bewertungkriterien bezüglich Sicherheitseigenschaften von IT-Produkten und -Systemen) nicht erfüllt, auf dem Markt schwerer haben [37].

### Risiken

Die privat, öffentlich und unternehmerisch zu beachtenden Risiken können z.B. gemäss [8] grob in drei Hauptkategorien aufgeteilt werden:

**Security Risks: Datenspionage und Datenmanipulation** Die "Security Risks" stellen den grössten potentiellen Gefahrenherd dar, welche einen illegalen Hintergrund hat. Diese Gefahrenquelle geht von (internen oder externen) Personen oder von ihnen programmierte Malware aus, welche sich unberechtigten Zugriff auf gespeicherte oder im Netzwerk transferierte Daten verschaffen wollen [8]. Im schlimmsten Falle können die so ausgehorchten Daten manipuliert und beschädigt werden. Die Ursache für dieses Risiko liegt meistens in Sicherheitslöchern schlecht programmierter Software. Die Trusted Computing Architektur verspricht die mit ihr ausgestatteten Systeme besser vor Angriffen zu schützen, indem die Vertrauenswürdigkeit von potentiellen Kommunikationspartner im Netz vor der Etablierung einer Verbindung überprüft wird. Dieses Verfahren (genannt "Remote Attestation") wird in dieser Arbeit noch erläutert.

**Disruption Risks: Zugriffsstörung** Die "Disruption Risks" sind anders als die eben besprochenen "Security Risks" nicht immer das Resultat illegaler Machenschaften, sondern können auch die Konsequenz auftretender Pannen sein [8]. Das Risiko kann sich in Zugriffsstörungen auf intern oder extern gespeicherte (über das Netzwerk zu beziehende) Daten manifestieren. Das Intensitätsspektrum solcher Zugriffsstörungen reicht von kurzzeitigen Verzögerungen bis hin zu vollständigem Datenverlust. Anders als bei den "Security Risks" werden diese Zugriffsstörungen auch häufig durch Hardwaredefekte und je nach geographischer Lage auch durch Naturkatastrophen (Stürme, Fluten, Erdbeben, Blitzeinschläge...) verursacht. Z.B. werden in den USA mehr als ein Drittel der Zugriffsstörungen durch eben solche Natureinwirkungen hervorgerufen.

**Media Risks: Verletzung von Urheberrechten** Die dritte Hauptkategorie der in einem Sicherheitsdispositiv zu berücksichtigenden Risiken stellen jene des illegalen Austausches von urheberrechtlich geschützten Daten über das Netzwerk dar [8]. Zu "Media Risks" werden desweiteren Domainnamen-, Patent- und Markennamenmissbrauch gezählt. Eine potentiell mögliche Anwendung von Trusted Computing (namens "Digital Rights Management", welche in dieser Arbeit noch dargestellt und erörtert wird) verspricht diesem Missbrauch zumindest teilweise einen Riegel vorzuschieben.

### Diebstahl von urheberrechtlich geschützten Daten

Der Hauptanteil der weiter oben behandelten Risikokategorie "Media Risks" umfasst wie besprochen den Austausch von urheberrechtlich geschützten Daten. Bei diesen Daten kann es sich entweder um Programm- oder Nutzdaten handeln. Bezüglich dieses Kriteriums wird auch folgende Unterteilung vorgenommen:

**Diebstahl von Software** Es wird geschätzt, dass den Herstellern aufgrund des durch Dritte unrechtmässig betriebenen Handels mit illegalen Kopien ihrer Software (engl. software piracy) jährlich Einnahmenseinbussen von etlichen Milliarden Euro resultieren [21]. Aus diesem Grund arbeitet beispielsweise der Softwarehersteller Microsoft mit gesetzlichen Behörden zusammen, um kriminelle Ringe zu zerschlagen, welche die Kopierschutzmechanismen ihrer Betriebssysteme umgehen. Zu diesen Kopierschutzmechanismen (engl. anti-piracy technology) gehört beispielsweise WPA ("Windows Product Activation") des Betriebssystemes Windows XP. WPA überprüft ob das auf einem Computer installierte Windows XP auch tatsächlich durch Microsoft lizensiert wurde. Erst dann wird dem Nutzer ein Bestätigungsidentifikationspasswort zur Aktivierung des Betriebssystemes übermittelt. Softwarepiraterie umfasst nicht nur die öffentliche Verbreitung von illegalen Kopien, sondern auch die private Installation eines Betriebssystemes auf mehreren Rechnern oder die leihweise Weitergabe an Bekannte. Die Softwarehersteller mahnen, dass die Verbreitung illegaler Kopien zu Preissteigerungen ihrer Produkte führen kann. Die Wirksamkeit von Kopierschutzmechanismen wird insofern eingeschränkt, als dass Anleitungen zur Kopierschutzumgehung über das Internet verbreitet und dort von vielen Leuten gelesen werden, die dann so unentgeltlich an die entsprechende Software gelangen. Deshalb sehen Softwarehersteller im potentiellen Trusted Computing Standard ein effektiveres Mittel im

Kampf gegen die Softwarepiraterie, da die Plattformkonfigurationsinformation und somit die Kommunikationsvertrauenswürdigkeit (welche im zweiten Kapitel unter "Remote Attestation" behandelt wird) von der Lizensierung der installierten Software abhängig gemacht werden könnte.

**Diebstahl von Informationen** Die zweite Form des Diebstahls umfasst das unrechtmässigte Vervielfältigen von geschützten, digital gespeicherten Informationen (engl. digital content piracy), wie beispielsweise audiovisuelle Daten [21]. Filesharing-Systeme bieten dem Internetnutzer potentiell indirekt die Möglichkeit, neben privat erstellten Dateien auch urheberrechtlich geschützte Musik- und Videodateien auszutauschen, ohne den gesetzlichen Urhebern der entsprechenden Daten ein Entgelt zu entrichten. Aus diesem Grund hat beispielsweise Microsoft "Digital Rights Management" (DRM) in Windows XP integriert, welches zumindest auf Softwareebene verhindern soll, dass Nutzer Zugriff auf geschützte Inhalte erlangen, für welche sie nicht bezahlt haben. Vom amerikanischen Kongress wurde ein spezielles Gesetz ("Digital Millenium Copyright Act") gutgeheissen, welches ("Reverse Engineering")-Praktiken zur Umgehung von DRM verbieten soll. Andere Staaten wiederum sind bezüglich des Schutzes intellektuellen Eigentums weniger streng, wobei diese gesetzliche Heterogenität das Durchsetzen von urheberrechtlichen Rechten erschwert. Die Vertreiber von geschützten Daten erhoffen sich indes, dass DRM mithilfe Trusted Computing dank hardwaremässiger Unterstützung erheblich effektiver sein wird. Auf DRM wird später noch ausführlicher eingegangen.

### 3.2.2 Sicherheitsparadigmen

Es soll nun eine kleine Auswahl von generell anerkannten "Best Practice"-Ansätzen zur Sicherheitssteigerung genannt werden, auf welche auch die Trusted Computing Architektur baut [9].

**Sicherheit als integraler Bestandteil der Software** Den Idealfall stellen Sicherheitsfunktionen dar, welche als integraler Bestandteil des Betriebssystemes walten und schon beim Entwurf der Betriebssystemarchitektur implementiert werden. Im Falle des beispielsweise hochkomplexen Windows ist es aber nur noch sehr schwer möglich, die gesamte Architektur resistenter gegen Attacken zu gestalten. Einerseits kann die bisherige Architektur nicht ohne Kompatibilitätseinbussen zu früheren Windows-Versionen einfach so verändert werden, andererseits spielt heute der "time-to-market" Faktor eine derartig wichtige Rolle im Softwaremarkt, dass für den sicherheitstechnischen Aspekt der Betriebssystemprogrammierung bisher aus Kostengründen zuwenig Zeit aufgebracht wurde [1]. Ferner wollten die Softwarehersteller Verkäufer von Komplementprodukten nicht mit komplexen Sicherheitsverbesserungen abschrecken. Schlussendlich war die gelieferte Produktqualität im Wettbewerb vielfach viel weniger wichtig als der Verkaufspreis: Aufgrund des "Lemon-Effekts" (asymmetrische Intransparenz bezüglich Produktqualität lässt die Preise sinken) stechen die billigen, schlechteren Produkte sowieso die besseren, teurer herzustellenden Produkte aus. So leiden kommerzielle Betriebssysteme u.a. an kümmerlicher Prozessseparation (d.h. verschiedenen Programmen werden nicht immer verschiedene

Speichersegmente zugewiesen, was sie labiler macht), an Nichtbeachtung des Privilegiumprinzips[4] und an grossen Sicherheitsmängeln bezüglich des Datenstroms von/zu Ein- und Ausgabegeräten [29]. Ein künftig etablierter Trusted Computing Standard könnte nun zu vermehrt qualitativ besser programmierter Software mit weniger Schwachstellen führen, denn eine Trusted Computing konforme Software hat gewisse sicherheitsrelevante Anforderungen zu erfüllen, wobei die Nutzer bei Nichterfüllung gegen die entsprechenden Softwarehersteller dank der von Trusted Computing unterstützten Common Criteria erfolgreich Klage einreichen könnten.

**Sicherheitsarchitektur in Schichten** Es erscheint meist zweckmässig eine hierarchische modulare Sicherheitsarchitektur in Schichten (engl.: defense in depth) anzustreben [9]. Einerseits sind Teile einer solchen Architektur leichter erneuerbar, da zwischen den Schichten klar definierte Schnittstellen fungieren. Andererseits führt eine modulare Herangehensweise an die Programmierung von Sicherheitsmechanismen zu einem einfacheren und übersichtlicheren Design. Idealerweise weisen sämtliche Schichten (z.B. CPU, Speicher, Betriebssystem, Anwendungen) mehr oder weniger dasselbe Sicherheitsniveau auf, denn die "Sicherheitskette" ist nur so stark wie das schwächste Glied dieser Kette [13]. Auch bei Trusted Computing und dessen Varianten kommt diese Schichtenarchitektur zum Einsatz[5]. Ferner genügt es nicht, bloss gewisse Teile einer Computersysteminfrastruktur zu schützen, sondern es muss vielmehr das gesamte System bestehend aus örtlicher Lokalität, Hardware, Software, Netzwerke und Managementprozesse untersucht und geschützt werden (engl.: diversity of defense).

### 3.2.3 Heutige Sicherheitstools

Entsprechend der diversifizierten Bedrohungslage muss die IT-Sicherheit bezüglich Gegenmassnahmen nachrüsten - jedoch meist mit der Konsequenz erhöhter Kosten und Gesamtkomplexität. Während bei den technischen Massnahmen eine fast zu grosse Zahl von Einzellösungen für verschiedenste Bedrohungen bereitsteht, kann die Wirksamkeit der IT-Sicherheit erst durch darauf aufbauende proaktive und reaktive Massnahmen auf das erforderliche Niveau gebracht werden [20]. Mit Trusted Computing wird angestrebt, einen umfassenderen Schutz zu bieten als dies bisher mittels aufgesetzter Sicherheitstools geschah. Die Effektivität der heute verfügbaren Sicherheitstools ist insofern limitiert, als dass die Wirksamkeit von beispielsweise Verschlüsselungs- oder Firewalltools mit der Sicherheit der zugrundeliegenden Plattform, insbesondere also mit dem Betriebssytem, steht und fällt und weit weniger mit dem z.B. verwendeten Verschlüsselungsalgorithmus, da der Angreifer meist die Strategie verfolgt, nicht die Verschlüsselung, sondern andere Schwachstellen anzugreifen [30]. Natürlich determinieren neben dem Betriebssystem auch andere

[4]"Principle of least privilege": Sicherheitsmechanismus, welcher für die adäquate Vergabe von Zugriffsrechten an laufende Softwareprozesse zuständig ist. Mit ihm soll vermieden werden, dass Applikationen mehr Privilegien als unbedingt nötig zugesprochen bekommen. So soll insbesondere das Schadenspotential von Malware eingegrenzt werden.

[5]Bei Microsofts Variante NGSCB, welche im dritten Kapitel besprochen wird, wären die Schichten die folgenden: CPU, Trusted Platfrom Module-Chip, NGSCB, Windows-Betriebssystem, Windows-Applikationen.

Faktoren die Wirksamkeit der Einzellösungen. Beispielsweise ist dies bei einer Antivirensoftware die Qualität und Vollständigkeit der verwendeten Virenmusterdatenbank, welche natürlich periodisch aktualisiert werden sollte [28]. Auch die Möglichkeit, Antivirensoftware durch Integritätsprüfprogramme zu ergänzen, welche zu jeder abgespeicherten Datei mittels einer Hashfunktion eine Prüfsumme verwalten und diese bei jedem Start eines Programmes überprüfen, bieten keinen grossartigen Schutz vor böswillig programmierter Malware. Auch der von Microsoft entwickelte und ab Windows 2000 implementierte "Windows File Protection" (WFP) Sicherheitsmechanismus, welcher das Wiederherstellen von im Administratormodus zerstörten Systemdateien ermöglicht und somit besseren Schutz gegen trivial programmierte Viren mit sich bringt, kann nicht über die Unzulänglichkeiten von Einzellösungen hinwegtäuschen [21]. Trusted Computing bietet sich nun an, derartige Malware erst gar nicht in das System eindringen zu lassen.

### 3.2.4 Zusammenfassung

Angesichts der rasanten Entwicklung der IT ist zu erwarten, dass auch die dargestellten Schwachstellen, die zugehörigen Bedrohungen und die Anstrengungen für die IT-Sicherheit weiter zunehmen werden [20]. Zu den wesentlichen Herausforderungen für die IT-Sicherheit werden die grössere Mobilität und die spontane Vernetzung einer Vielzahl von Geräten ohne zentralen Strukturen ('peer to peer") zählen. Angesichts wachsender Komplexität und Verantwortung sowie kurzer Innovationszyklen wird IT-Sicherheit sowohl zu einer überlebenswichtigen Management-Disziplin in Unternehmen und Institutionen als auch zu einem wünschenswerten Faktor für die Privatnutzer. Der Einsatz einer Trusted Computing Architektur verspricht einen umfassenderen Schutz vor den beschriebenen Gefahren zu bieten als dies momentan mit dem derzeitig verfügbaren Sammelsurium an aufgesetzten Einzellösungen, welche nur einige sicherheitsrelevante Aspekte abdecken, möglich ist.

## 3.3 Problemstellungen und Ansätze von Trusted Computing

Wie im vorherigen Kapitel besprochen wurde, können die heute breit zur Prävention, Kontrolle und Reparatur eingesetzen Sicherheitstools (Antivirensoftware, Firewall etc.) nur gewisse Sicherheitsmängel entschärfen, jedoch auch kombiniert keinen allumfassenden Schutz vor Attacken bieten. Die Sicherheitslücken, in der Kontrolle bisher nicht walten konnte, will Trusted Computing unter anderem mit seiner Philosophie der vielleicht künftig zwischen vernetzten Computersystemen herrschenden bescheinigten Vertrauenswürdigkeit füllen [32]. Das Fundamentum von Trusted Computing wird bereits gelegt – wenn auch noch in stark reduzierter Form: Einerseits sind bereits einige handelsübliche Computer mit der entsprechenden Hardware ausgerüstet, auf welche neben dem Sicherheitskonzept von Trusted Computing und dessen Grenzen in diesem und vor allem im nächsten Kapitel noch eingegangen wird. Mit der Austattung heute verkaufter Computer mit dieser Hardware sollen diese bezüglich Trusted Computing zukunftstauglich gemacht

werden, obwohl heute noch bei weitem unklar ist, ob und wie stark Trusted Computing in naher Zukunft Fuss fassen wird und sich zum Sicherheitsstandard zu etablieren vermag. Andererseits werden beispielsweise im Betriebssystem Windows Server 2003 von Microsoft bereits Datenschutzfunktionen (z.B. Möglichkeit der Kontrolle über selbst erstellte Daten auch auf externen Sytemen) simuliert, welche von Trusted Computing auf Hardwarebasis potentiell geboten werden [1]. Diese und andere Kernfunktionalitäten werden in diesem Kapitel am Schluss kurz betrachtet.

### 3.3.1 Trusted Computing

Das Ziel der Bemühungen stellt die Etablierung eines "trusted PC" dar, der möglichst viel Schutz vor unrechtmässigen externen Eingriffen bieten soll [16]. Trusted Computing ist jedoch nur spärlich gegen interne Attacken durch den Nutzer selbst oder gegen hardwarebasierte Attacken wie Power Analysis (Messung der Leistungsaufnahmeschwankung der Computerhardware) gefeit. Auch ist Trusted Computing in zahlreichen Fällen machtlos angesichts Programmierfehler des Betriebssystemes selber. Damit zumindest ein gewisses Mass an Sicherheit vor externen Attacken gewährleistet werden kann, soll Datensicherheit also statt bisher mittels aufgesetzter Tools (engl. Add-Ons) neu in die Kernoperationen des Systems fest integriert werden [36]. Trusted Computing (TC) stellt eine Kombination von Hardware- und Softwaremassnahmen dar: Um TC-Funktionen zu unterstützen werden Computer also mit kompakter Zusatzhardware (wobei die Spezifikationen bereits veröffentlicht wurden [30]) und mit einem an TC angepassten Betriebssystem ausgestattet, welches zwischen der Hardware und den entsprechenden TC-konformen Applikationen operiert [14]. Die Austattung eines Computersystems mit TC führt zu zusätzlichen Kosten, welche jedoch durch den Einsatz von "kompakten" Komponenten minimiert werden sollen [30]. Optimistische Nutzer hoffen, dass diese Kosten durch grössere Sicherheit (z.B. sollen von Malware betroffene Applikationen bei aktiviertem TC im Idealfall nicht mehr ausgeführt werden) amortisiert werden [14]. Um sich im Markt durchsetzen zu können, soll die Möglichkeit der Deaktiverung von TC bestehen. TC selbst will also wohlgemerkt keine Einschränkungen bezüglich eingesetzter Software machen, jedoch können unter TC ausgeführte Applikationen dies tun. Zur Nutzung der angebotenen Funktionalität sollen nur minimale Anforderungen an Soft- und Hardware gestellt werden. Bei aktiviertem TC können Einschränkungen bezüglich Netzwerkzugriff vollzogen werden. Inwieweit die Trusted Computing Group als das TC entwickelnde Konsortium hier gehen will, ist eine Frage der erwünschten Sicherheitsstufe und der Bereitschaft auf offenen Netzwerkzugang zu verzichten [36]. Ferner können offene Computersysteme, auf denen beliebige Software installiert werden darf, bei Aktivierung von TC in kontrollierte (engl. software-controlled) oder gar geschlossene (engl. software-closed) transformiert werden, auf welchen nur bestimmte (TC-konforme) Software oder keine zusätzliche Software installiert werden darf. [27].

### 3.3.2 Trusted Platform

Unter Trusted Platform (TP) wird eine Computerplattform verstanden, welche speziell mit für TC benötigte Hardwarekomponenten ausgerüstet ist [1]. Bei der von der Trusted

Computing Group entwickelten Hardwarearchitektur ist dies das sogenannte Trusted Platform Module (TPM). Das TPM ist ein auf dem Motherboard integrierter Computerchip, welche ein Sammelsurium an sicherheitstechnisch benötigte Hilfsfunktionen auf Hardwarebasis bereitstellt und somit das Herzstück einer TP darstellt. Alle oder eine Teilmenge dieser Hilfsfunktionen werden für die von TC gebotene Funktionalität benötigt.

### 3.3.3 Problemstellungen und Ansätze von Trusted Computing

Zu den von TC gebotenen Sicherheitsfunktionen gehören die Sicherstellung des Bootprozesses basierend auf einer vertrauenswürdigen Plattformkonfiguration (Integrity Protected Booting), die Konfigurationsintegriät, der Datenschutz (mittels Verschlüsselung), und die Systemidentifikation (Attestation), welche nachfolgend kurz betrachtet werden [4] [14] [19]. Ferner obliegt es dem TPM sicherzustellen, dass nur berechtigte Komponenten Zugriff auf geschützte Ressourcen zugesprochen bekommen [1].

#### Integrity Protected Booting

**Authenticated Booting** Dieser erste Basisservice von Trusted Computing dient einem sicheren Ablauf des Bootprozesses und der Speicherung der Plattformkonfiguration zwecks späterer Systemidentifikation. So vermögen nach dem Laden des Betriebssystemes Applikationen zwecks Interoperabilität ihrerseits genau über das momentan agierende Betriebssystem zu informieren und umgekehrt. Dies wird mithilfe von Zusatzhardware bewerkstelligt, welche eine Art von "Logbuch" über den gesamten iterativen Bootprozess führt: Die Plattformkonfiguration ist nach einem erfolgreichen Bootprozess im TPM als Hashwert gespeichert und zwar in einer "shielded location" (Speicherbereiche für sensitive Daten, auf welche nur privilegierte Prozesse Zugriff haben), in diesem Fall den PCR (Platform Configuration Register). Gestartet wird der Bootprozess in der "Root of Trust", einem Stück Programmcode, der fehlerlos sein muss. Iterativ werden immer grössere Teile von Programmcode im BIOS und schliesslich des Betriebssystemes ausgeführt, nachdem die jeweiligen gebildeten Hashwerte des Programmcodes einem erfolgreichen Vergleich mit den Hashwerten des letzten erfolgreichen Bootens Stand gehalten haben. So wird die Sicherheitsbescheinigung von der Root of Trust auch auf externe Funktionen ausgedehnt [14] [16] [1] [19] [8] [3]. Integrity Protected Booting stellt eine Voraussetzung für "Sealed Storage" und "Remote Attestation" dar, welche nachfolgend noch besprochen werden.

**Secure Booting** Hier werden Sollwerte (Hashwerte der PCR) für die erwünschte Plattformkonfiguration vorgegeben [16]. Das bedeutet, dass das System nur erfolgreich booten kann, wenn die Anforderungen an die Plattformkonfiguration erfüllt werden.

#### Verschlüsselung

Die Verschlüsselungsfunktionen des TPM stellen den zweiten Basisservice von Trusted Computing dar, wobei sich Trusted Computing soft- und hardwaremässiger Verschlüsselungsfunktionen bedient, wobei natürlich die hardwarebasierte Verschlüsselung durch das

TPM mehr Sicherheit versprechen. Die Verschlüsselung geschieht meist asymmetrisch, d.h. mit einem privaten und einem öffentlichen Schlüssel [14] [24].

**Konfigurationsabhängige Verschlüsselung: Sealed Storage** Eine Anwendung der Verschlüsselung ist Sealed Storage (dt. versiegelte Speicherung). Das Prinzip ist folgendes: Bevor selbst erstellte Dateien oder über ein Netzwerk empfangene Dateien auf die Festplatte abgespeichert werden, werden sie verschlüsselt. Vor der Verschlüsselung wird den Daten der bei Speicherung aktuelle Plattformkonfigurationshashwert angehängt. Somit kann der Nutzer auf die gespeicherten Daten künftig nur noch mit derselben Plattformkonfiguration zugreifen, was von der entsprechenden Anwendung zur Öffnung der Dateien überprüft wird. Im Extremfall kann eine Datei sogar nur noch mit einer bestimmten Applikation geöffnet werden. Verschlüsselt werden diese Daten dann mit einem durch den TPM-internen Master Secret Key (welcher das TPM nie verlässt) generierten konfigurationsabhängigen Schlüssel, sodass die abgespeicherten Daten nur noch auf demselben Rechner entschlüsselt werden können [13] [24] [19] [3].

### Remote Attestation: Bescheinigung gegenüber Kommunikationspartnern

"Attestation" selber (was auf deutsch soviel wie Zeugnis, Nachweis oder Bescheinigung bedeutet) stellt den ersten Aspekt der Vertrauenswürdigkeit dar, welcher schon seit Dekaden angestrebt wird und teilweise dank bestimmter Hardware- und Softwareeigenschaften (wie Prozessseparation und differenzierte Privilegienvergabe) auch bewerkstelligt wurde: Der Verlass auf eine Malware-freie Systemkonfiguration. Trusted Computing will nun auch den zweiten Aspekt der Vertrauenswürdigkeit realisieren: Nicht nur der Nutzer selbst soll von der Sicherheit seiner Plattformkonfiguration überzeugt sein, sondern auch ein externes System, mit dem zwecks Datentransfer kommuniziert wird. Die Sicherheitsbescheinigung wird dem externen System hierbei mittels digital signiertem Zertifikat garantiert, welches die plattformkonfigurationsabhängigen Hashwerte enthält (für die Verwendung des Zertifikates werden hierbei TPM-Verschlüsselungsfunktionen benötigt). Das externe System kann daraufhin selber entscheiden, ob es die Kommunikation fortzuführen beabsichtigt [8] [21] [38].

### Schutz vor Datenmissbrauch

Obwohl die Architektur von Trusted Computing nicht speziell für den Schutz von geistigem Eigentum ausgelegt wurde, kann mithilfe TC die Kontrolle von Daten auf externen Systemen im allgemeinen mit der Rights Expression Language (REL) und im speziellen mit Digital Rights Management (DRM) forciert werden, welche nur Anwendungen von TC darstellen und schon heute auf Softwarebasis existieren - wenn auch mit geringerer Effektivität.

**Rights Expression Language (REL)** Die Softwarelösung Microsoft's Information Rights Management (IRM) vermag beispielsweise den Zugriff auf Dokumente einzuschränken, indem die Dokumente zusammen mit Nutzungsregeln chiffriert werden, welche in einer Rights Expression Language (REL) formuliert werden. Diese Regeln könnten z.B. die Nutzung auf einen gewissen Rechnerkreis oder auf ein gewisses Datum einschränken, ein Kopieren verhindern oder gar die Selbstlöschung nach einer gewissen Zeitspanne bewirken. Solche Verfahren könnten durch TPM-basierte TC-Mechanismen hardwaremässig forciert werden [3]. Eine Schwierigkeit besteht einerseits darin, Nutzungsregeln (engl. policies) diskret in maschinenlesbarem REL zu formalisieren, andererseits in der deterministischen Interpretation dieser formal aufgestellten Regeln [12]. Viele komplexe Bestimmungen sind einfach zu verschachtelt und interpretationsabhängig, als dass sie kurzum auf ein Stück Code (z.B in standardisierten XML-Protokollen) reduziert werden könnten.

**Digital Rights Management (DRM)** DRM bestimmt die rechtlichen Eigenheiten des Vertriebs und der (dadurch oft eingeschränkten) Nutzungsmöglichkeiten von digitalen Medien wie Büchern, Musik, Filmen und Software. Die Vertreiber von audiovisueller Multimediadaten zum Beispiel erhoffen sich, dass durch einen künftig etablierten TC-Standard weniger illegal agierende Nutzer imstande sind, sich kostenlos ihre zu schützenden Medien zu beschaffen [13]. Unter anderem hat diese Konsequenz fortlaufende Kontroversen über Folgen von DRM für die freie Marktwirtschaft ausgelöst, auf welche noch im vierten Kapitel näher eingegangen wird [27]. Bisherige DRM-Mechanismen funktionieren auf Softwareebene und sind somit relativ leicht umgehbar. Der Einsatz von TC-Hardware könnte als Nebeneffekt nun die Effektivität des DRM erhöhen [3], obwohl das TPM nicht speziell auf DRM abgestimmt wurde. Sowieso ist das TPM machtlos gegen diesbezüglich interne Attacken seitens des Nutzers, welcher audiovisuelle Informationen trotz DRM mithilfe primitivsten Mitteln wie Mikrofon und Kamera vervielfältigen kann [31]. Es ist also unklar, ob sicherheitstechnisch wirkungsvollere DRM-Mechanismen wirklich den erwünschten gewinnsteigernden Effekt für die Eigentümer der Medieninhalte bringen würden [1]. Kritiker wähnen eine eingeschränkte Nutzung künftiger kommerzieller Applikationen [13], da DRM nicht nur bei Unterhaltungsmedien, sondern auch allgemein für Dokumente aller Art (z.B. wichtige private medizinische Protokolle) und E-Mails eingesetzt werden könnte, was zur Folge haben könnte, dass auf all diese Daten mittels des besprochenen Sealed Storage-Verfahrens nur noch mit gewisser Standard-Software marktmächtiger Firmen zugegriffen werden könnte [3] [1].

### 3.3.4 Zusammenfassung

Trusted Computing (TC) will einen soliden Grundschutz anbieten, welcher angemessen auf neue Anforderungen und Bedrohungen reagieren bzw. deren Auswirkungen auf ein erträgliches Mass reduzieren soll [20]. Eine Trusted Platform stellt sicherheitstechnische Funktionen mittels eines im Motherboard integrierten Computerchips, dem Trusted Platform Module, bereit. In diesem Kapitel besprochene Funktionen wie Integrity Protected Booting, hardwaremässige Verschlüsselung, Sealed Storage, Remote Attestation stellen Eckpfeiler dieser Sicherheitsarchitektur dar.

## 3.4 Technische Ansätze von Trusted Computing

Es bestehen bereits diverse technische Realisierungen von Trusted Computing-Ansätzen, teilweise unter verschiedenen Synonymen, wie zum Beispiel der Next-Generation Secure Computing Base-Initiative von Microsoft [22] oder der Safer Computing Initiative von Intel [17]. Um Trusted Computing zu realisieren, muss sowohl die Hardware, als auch die Software entsprechende Funktionalitäten bereitstellen und implementieren. In diesem Kapitel werden die wichtigsten Initiativen um Trusted Computing kurz vorgestellt und jeweils auf eine Hardware- und eine Software-Architektur genauer eingegangen. Dazu wurde exemplarisch auf der Hardware-Ebene die Trusted Platform Architecture der Trusted Computing Group und softwareseitig das Open-Source-Projekt Perseus ausgewählt, da es sich bei beiden Ansätzen um generische Modelle handelt, die ein breites Anwendungsfeld zulassen und die meisten Funktionalitäten der proprietären Lösungen einschliessen.

### 3.4.1 Trusted Computing Group

Die Hauptaufgabe der Trusted Computing Group besteht darin, Standards im Bereich Trusted Computing auszuarbeiten und zu definieren, und zwar sowohl für Hardwarebauteile wie auch für Software-Schnittstellen. Eines ihrer wichtigsten Erzeugnisse ist die Spezifikation des Trusted Platform-Moduls, ein Sicherheits-Chip, welcher den Grundbaustein der meisten Trusted Computing-Ansätze bildet. Im Rahmen der Darstellung der Trusted Platform Architecture soll die Funktionalität dieses Chips kurz erläutert werden.

#### Entstehung der Trusted Computing Group

Die Trusted Computing Group (kurz TCG) ist eine non-profit Organisation, die aus rund 100 Mitgliedern besteht, die sich aus den verschiedensten Unternehmen zusammensetzen: Hardware- und Softwarehersteller, Systemlieferanten, Netzwerk- und Infrastruktur-Firmen [34]. Die TCG wurde 2003 gegründet und löste die Trusted Computing Platform Alliance (TCPA) ab, da sich deren Entscheidungsfindung als ineffektiv erwiesen hatte. Zudem erhoffte man sich auch einen Imagewechsel, da die TCPA durch eine wenig transparente Öffentlichkeitsarbeit in Verruf geraten war [6]. Die TCG hat die von der TCPA erstellte Spezifikation des Trusted Platform Module (TPM) weiterentwickelt und im Oktober 2003 in der Version 1.2 veröffentlicht. Innerhalb der TCG existieren eine Reihe von Arbeitsgruppen, die an der Entwicklung von Trusted Computing für die unterschiedlichsten Plattformen arbeiten [34]. Darunter auch die Infrastructure Work Group, die mit einer generischen Trusted Platform Architecture die Eigenschaften von Trusted Computing in Internet- und Unternehmens-Systeme integrieren möchte.

#### Trusted Platform Architecture

Die TCG hat unter anderem eine generische Architektur einer Trusted Platform spezifiziert, zu deren Hauptbestandteilen das Trusted Platform Module gehört, das ebenfalls

von der TCG entworfen wurde und auf das weiter unten näher eingegangen wird. In dieser Architekturspezifikation werden primär die Voraussetzungen einer Trusted Platform und der Aufbau einer Chain of Trust, ausgehend von den Roots of Trust, definiert. Die Roots of Trust sind Komponenten, denen grundsätzlich vertraut werden muss, da ein allfälliges Fehlverhalten nicht festgestellt werden kann. Es werden im Allgemeinen drei Roots of Trust unterschieden:

- Root of Trust for Measurement (RTM)
- Root of Trust for Storage (RTS)
- Root of Trust for Reporting (RTR)

Während die letzten beiden Roots of Trust durch das TPM abgedeckt werden, übernimmt normalerweise die CPU die Rolle der RTM. Da die CPU aber nur als ausführende Einheit agieren kann und keinerlei Speicher besitzt, um Instruktionen zu persistieren, müssen die Steuerbefehle an einer anderen Stelle abgespeichert werden, üblicherweise im Boot ROM des Rechners. Dieses Set von Instruktionen wird als „Core Root of Trust for Measurement" bezeichnet, kurz CRTM (vgl. Abbildung 3.2). Die RTM ist ebenfalls die Wurzel der „Chain of Transitive Trust". Nachfolgend werden die jeweiligen Bestandteile der Trusted Platform Architektur kurz erläutert [35, The Trusted Platform].

**Trusted Platform Building Blocks** Die Trusted Building Blocks (TBB) sind diejenigen Bestandteile der Roots of Trust, die über keinen nach aussen abgeschirmten Speicher oder geschützten Funktionen verfügen, wie es zum Beispiel beim TPM der Fall ist. Abbildung 3.2 zeigt ein mögliches Beispiel einer TBB, zusammengesetzt aus dem CRTM im Bios, der Verbindung des CRTM zum Mainboard, der Verbindung des TPM zum Mainboard, sowie dem Controller, dem RAM und einer minimalen Auswahl an Instruktionen innerhalb der CPU.

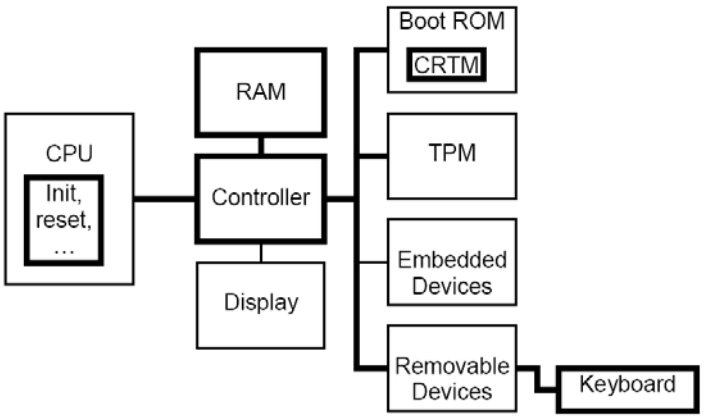



Abbildung 3.2: Die Trusted Building Blocks einer Trusted Platform sind fett markiert

**The Trust Boundary** Die Kombination der Trusted Building Blocks und der Roots of Trusts bildet eine Trust Boundary, eine Vertrauensgrenze. Diese Grenze darf nur auf weitere Komponenten oder Programme ausgeweitet werden, wenn diese zuvor von Geräten innerhalb der Trust Boundary überprüft und für vertrauensvoll befunden wurden.

**Transitive Trust** Diese Ausweitung der Vertrauensgrenze geschieht durch die Anwendung von Transitive Trust, einem Prozess, bei dem eine vertrauenswürdige Komponente eine Gruppe von Funktionen überprüft und danach die Trust Boundary um eben diese Funktionsgruppe ausweitet. Diese kann dann wiederum weitere Komponenten messen und für vertrauenswürdig erklären. Dadurch lässt sich die Vertrauensgrenze nach und nach auf das ganze System ausweiten. Abbildung 3.3 zeigt den Ablauf dieses Vorgangs beim Systemstart, wo sich zu Beginn nur die TBB und die Roots of Trust innerhalb der Trusted Boundary befinden.

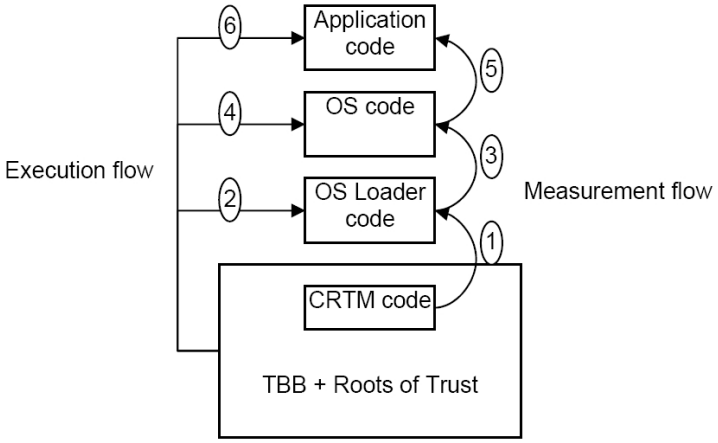



Abbildung 3.3: Transitive Trust beim Systemstart angewendet ausgehend von einer statischen Root of Trust

**Integrity Measurement** Der Measurement-Kernel erzeugt so genannte „Measurement Events“, die aus zwei Klassen von Daten bestehen:

1. Messwerte, die durch Scanning von Programm-Code oder Daten erzeugt werden und eine Repräsentation derselben darstellen, und

2. Hash-Werte, die aus den Messwerten berechnet wurden.

Die Hash-Werte werden temporär im Root of Storage abgelegt, das heisst in so genannten Platform Configuration Registers des TPM. Diese Hash-Werte stellen ein Abbild des gegenwärtigen Systemzustands dar. Wird nur eine Hardware- oder Software-Komponente geringfügig verändert, resultiert auch ein ganz anderer Hashwert.

**Integrity Reporting** Die Root of Trust for Reporting (RTR) hat primär zwei Aufgaben: einerseits die Bereitstellung eines abgeschirmten Speicherbereichs zur Speicherung von Integritätsmessungen, andererseits die Bescheinigung (attestation) der Authentizität der gespeicherten Integritätswerten. Dazu werden die Hashwerte im PCR mit so genannten Attestation Identity Keys (AIK) digital signiert. Diese werden vom TPM selber generiert und gespeichert. Die TCG spezifiziert weiter ein Integrity Reporting Protocol, mit dem die Integrität der eigenen Platform gegenüber einem Dritten bestätigt werden kann.

**TPM als Kommunikations-Endpunkt** Bei der Kommunikation zwischen zwei Systemen in einem verteilten System spielen kryptographische Schlüssel eine wichtige Rolle, wenn es darum geht, die Authentizität, Integrität und Geheimhaltung von Daten zu gewährleisten. Schlüssel bilden damit Kommunikations-Endpunkte und eine falsche Handhabung derselben resultiert in einem Sicherheits-Verlust. Das TPM kann dazu verwendet werden, diese Endpunkte abzusichern, indem es Funktionen für Schlüssel- und Konfigurations-Management bereitstellt.

**Protected Storage** Die Root of Trust for Storage (RTS) ist, wie bereits erwähnt, ebenfalls im TPM implementiert. Ihre Aufgabe ist es, Schlüssel und Daten vor Zugriffen von aussen zu schützen. Der TPM enthält einen begrenzten, flüchtigen Speicher, in dem Schlüssel vorübergehend während Verschlüsselungs- oder Signiervorgängen abgelegt werden können. Nicht benötigte Schlüssel können auch in verschlüsselter Form ausserhalb des RTS bzw. des TPM persistent gespeichert werden.

### Trusted Platform Module

Das Trusted Platform Module, kurz TPM, bildet in der Trusted Platform Architectur der TCG sowie in den meisten anderen Trusted Computing Plattformen einen Teil der „Root of Trust“ (RTR und RTS). Das Vertrauen in diesen Chip wird abgeleitet aus den guten Konstruktionsverfahren, Herstellungsprozessen und industriellen Prüfverfahren, die bei dessen Produktion zum Einsatz kommen. Dies wird durch die Zertifikation gemäss den Common Criteria (CC) belegt [35, Trusted Platform Module Components]. In Abbildung 3.4 sind die einzelnen Komponenten des TPM abgebildet. Deren Funktionen sollen nachfolgend erläutert werden:

**Input/Output (I/O)** Die Ein- und Ausgabe-Komponente bildet die physische Schnittstelle zum TPM. Hereinkommende Nachrichten werden an die jeweiligen Komponenten weitergeleitet. Dabei werden Zugriffsregeln in Verbindung mit der Opt-In-Komponenten, aber auch von anderen TPM-Komponenten, falls benötigt, angewendet.

**Non-volatile storage** Der nicht-flüchtige Speicher des TPM wird zur Speicherung des Endorsement Key (EK), des Storage Root Key (SRK), der Autorisierungsdaten des Besitzers sowie persistenter Flags verwendet. Der Endorsement Key kennzeichnet einen TPM

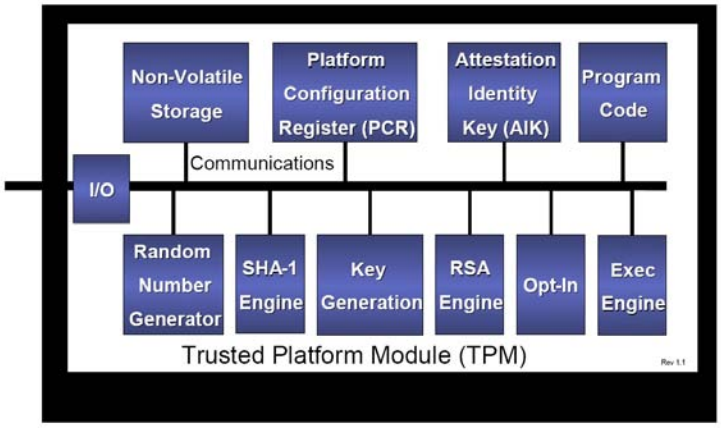



Abbildung 3.4: TPM Komponenten Architektur

eindeutig und bildet gleichzeitig den nicht-öffentlichen Schlüssel des TPM. Er kann nicht migriert werden, d.h. er verlässt den TPM nie und kann somit auch nicht extern gesichert werden. Er dient zur Entschlüsselung von Nachrichten, die mit einem öffentlichen Schlüssel dieses TPMs verschlüsselt wurden. Zusätzlich werden bei der erstmaligen Inbetriebnahme des TPMs die Benutzer-Authorisierungsdaten damit verschlüsselt. Der Storage Root Key dient zur Verschlüsselung von weiteren Schlüsseln (z.B. einem privaten Schlüssel bei der E-Mail-Kommunikation) und bildet somit die Wurzel des TPM-Schlüsselbaumes.

**Platform Configuration Register** Die Platform Configuration Register (PCR) können entweder in flüchtigem oder nicht-flüchtigem Speicher implementiert werden. Es muss auf alle Fälle sichergestellt werden, dass sie bei einem Neustart des Systems oder bei einem Stromverlust der Plattform gelöscht werden.

**Attestation Identity Key** Die Attestation Identity Keys müssen persistent gehalten werden. Es wird empfohlen, die AIK als Blobs (Binary Large Objects) in einem externen Speicher ausserhalb des TPM zu speichern, anstatt im nicht-flüchtigen Speicher innerhalb des TPM. Die TCG hofft, dass die TPM-Hersteller genügend Platz bereitstellen, um zur Laufzeit mehrere AIK Blobs gleichzeitig im flüchtigen Speicher des TPM zu halten, da so die Ausführungsgeschwindigkeit erhöht werden kann.

**Program Code** Der Programm-Code enthält die Firmware zur Messung von Plattform-Geräten. Logisch gesehen bildet dies die „Core Root of Trust for Measurement (CRTM)“. Idealerweise ist die CRTM im TPM enthalten, aber je nach Implementations-Entscheidung kann diese auch in einer anderen Firmware ausserhalb des TPM abgelegt werden.

**Random Number Generator** Der TPM enthält einen „true random-bit“-Generator, der benutzt wird, um einen „Seed“ für die Zufallszahlen-Generierung zu erzeugen. Dies ist unter anderem Voraussetzung für die Schlüsselgenerierung.

**SHA-1 engine** Die SHA-1 Komponente berechnet aus einem gegebenen Input einen entsprechenden Hash-Wert. Dies kann unter anderem zur Berechnung von Signaturen verwendet werden.

**Key generation** Die TCG hat den RSA-Algorithmus zur Verwendung im TPM standardisiert. Diese Komponente wird zur Erzeugung von Signing-Keys und von Storage-Keys verwendet. Dabei muss das TPM Schlüssel bis zu 2048-bit Modulus generieren können, wobei gewisse Schlüssel (SRK, AIK) mindestens einen 2048-bit Modulus aufweisen müssen.

**RSA engine** Die RSA Komponente wird für das Signieren mit Signing Keys, für die Ver- und Entschlüsselung mit Storage Keys sowie für die Entschlüsselung mit dem Endorsement Key verwendet (der Endorsement Key wird niemals für die Verschlüsselung verwendet). Das TCG-Komitee geht davon aus, dass TPMs, die eine solche RSA-Engine enthalten, nicht den US-amerikanischen Import- und Export-Restriktionen unterliegen [7].

**Opt-in** Die Opt-In Komponente implementiert die von der TCG gestellte Anforderung, dass das TPM im vom Kunden gewünschten Zustand ausgeliefert werden kann. Der Zustand kann zwischen deaktiviert bis zu vollständig aktiviert variieren. Der Opt-In-Mechanismus enthält die Steuerungslogik und die Schnittstelle, um sicherzustellen, dass die entsprechenden TPM-Komponenten deaktiviert werden.

**Execution engine** Die Execution-Engine initialisiert den TPM und führt den Programm-Code aus.

### 3.4.2 Intel LaGrande Technology

Intel arbeitet im Rahmen ihrer 'Safer Computing Initiative' an einer eigenen hardwareseitigen Umsetzung von Trusted Computing namens „LaGrande Technology“, kurz LT. Intel möchte vor allem die Kommunikation zwischen den einzelnen Hardwareteilen absichern. Das heisst, der Datenverkehr zwischen Tastatur, CPU und Bildschirm soll verschlüsselt stattfinden, so dass an keiner Stelle im Bus-System eine Manipulation stattfinden kann.

In Abbildung 3.5 sind die Änderungen an der Intel Bus-Architektur mit grauen Kästchen dargestellt. Dabei werden insbesondere die CPU und der Memory Controller Hub (MCH) um neue Funktionalitäten erweitert. Über den Graphics Controller Hub (GCH) wird sichergestellt, dass die Bildausgabe nicht verändert werden kann. Durch die sichere Verbindung zwischen Eingabegeräte und I/O Controller Hub wird die Integrität von Benutzereingaben gewährleistet. Ein zentraler Bestandteil dieser Architektur ist das Trusted Platform Module, das als Wurzel der Vertrauenskette dient und dessen Sicherheitsfunktionen LT verwendet.

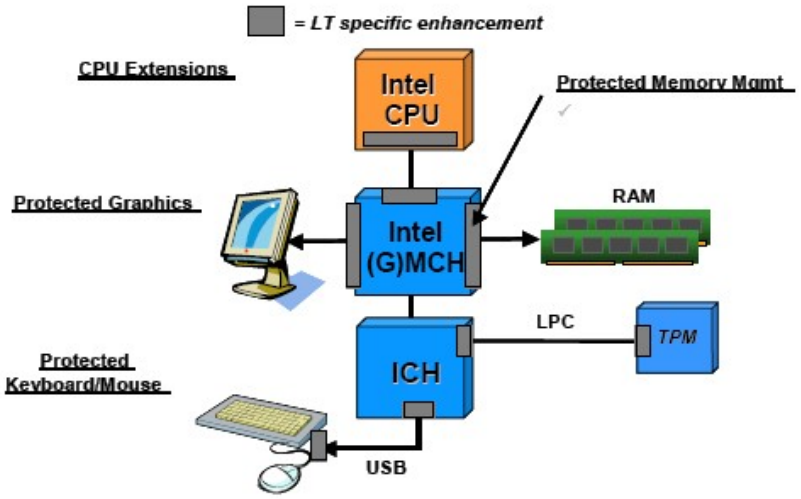



Abbildung 3.5: Intel LaGrande Architektur

### 3.4.3 The Perseus Security Architecture

Eine Trusted Computing Umgebung benötigt neben der Hardware-Unterstützung auch eine entsprechende Betriebssystem-Implementation, welche die Sicherheitsfunktionen verwendet und gegenüber dem Benutzer transparent in Form von Anwendungen und Services anbietet. Wie Eingangs erwähnt, möchten wir auf das Software-Framework, das im Rahmen des Open-Source-Projekts Perseus von der Universität Bochum entworfen wird, genauer eingehen. Es handelt sich hierbei um einen generischen Architekturentwurf, der völlig unabhängig von bestimmen TC-Komponenten oder Betriebssystemen umgesetzt werden kann.

#### Open Security Architectur

Bei dieser offenen Sicherheitsarchitektur sollen die Sicherheitsfunktionen nicht direkt in das Betriebssystem implementiert werden, da dessen Entwicklung viel zu komplex wäre und dadurch die Wahrscheinlichkeit, dass sich Sicherheitslücken und Fehler einschleichen, sehr hoch wird. Stattdessen sollen sämtliche Sicherheitsfunktionen extrahiert und in einem so genannten Security Kernel, der sich zwischen Hard- und Softwareschicht befindet, kompakt implementiert werden. Dadurch soll die Komplexität dieses Kernels gering gehalten und so die Fehleranfälligkeit reduziert werden. Auf diesem Layer sollen dann die Betriebssysteme und Sicherheitsanwendungen aufbauen, die so transparent auf die von der Hardware zur Verfügung gestellten und vom Security Kernel verwalteten Sicherheitsfunktionen zugreifen können [33].

#### 3-Layer-Architektur

Die Perseus Sicherheitsarchitektur besteht aus den drei in Abbildung 3.6 dargestellten Schichten:

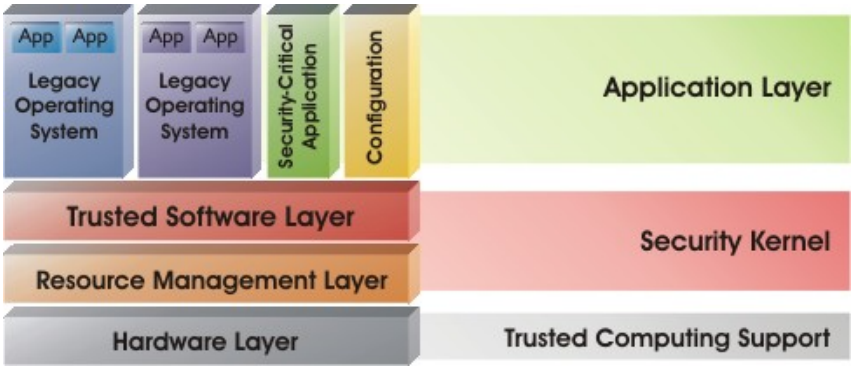



Abbildung 3.6: Perseus 3-Layer-Architektur

Im Hardware-Layer sind die Gerätekomponenten untergebracht, z.B. CPU, Arbeitsspeicher, Ein- und Ausgabegeräte. Dazu gehören aber auch Sicherheitskomponenten, wie z.B. ein TPM, wie er von der Trusted Computing Group spezifiziert wird. Christian Stüble hält fest, dass herkömmliche Hardware-Architekturen nicht in der Lage sind, sämtliche benötigten Sicherheitsfunktionen bereitzustellen [33, Hardware Layer].

Der Resource Management-Layer ist verantwortlich für die Bereitstellung der Hardware-Resourcen und für die Überwachung und Kontrolle von Zugriffen auf die Hardware. Dabei werden insbesondere (aber nicht ausschliesslich) Komponenten wie CPU, Arbeitsspeicher und Trusted Computing-Komponenten verwaltet. Gerätetreiber, die für die Zugriffe auf die Hardware benötigt werden, sind ebenfalls Bestandteil dieser Schicht [33, Hypervisor Layer].

Durch Kombination und Erweiterung der vom Resource Management-Layer bereitgestellten Schnittstelle, generiert der Trusted Software-Layer sicherheitskritische Dienste, die für die Realisierung von sicheren Computer-Plattformen benötigt werden. Eine Hauptaufgabe des Trusted Software-Layers ist es, Sicherheits-Policies in eine konsistente Menge von Zugriffsregeln überzuführen (Policy Translation). Eine weitere Funktion bildet das „Trusted GUI“, das den Schutz der Integrität und Vertraulichkeit von Benutzereingaben (z.B. eines PIN-Codes) und von Ausgaben (z.B. Anzeige eines vertraulichen Dokuments) gewährleistet [33, Trusted Software Layer].

Über dem Trusted Software-Layer folgt der Application-Layer, der die Betriebssysteme umfasst, sowie sicherheitskritische Anwendungen und Sicherheitskonfigurationen. Die Perseus-Architektur bedient sich der Virtualisierungs-Technologie, um eine oder mehrere Instanzen von Betriebssystemen gleichzeitig auszuführen. Der aktuelle Entwicklungsstand bedingt jedoch leichte Modifikationen an den bestehenden Betriebssystemen, was natürlich bei proprietären Lösungen nicht ohne weiteres möglich ist. Das langfristige Ziel von Perseus ist eine so genannten Hardware-Virtualisierung, wodurch herkömmliche Betriebssysteme keine Änderung benötigen. Dabei wird die Hardware von einem Virtual Machine Monitor simuliert, der entweder zwischen Security Kernel und Application-Layer gelegt wird, oder der direkt in den Security Kernel integriert wird, was vor allem für Performancekritische Szenarios von Vorteil ist [33, Virtualization].

**Vorteile**

Das Perseus-Projekt kann einige wesentliche Vorteile einer Open-Source-Entwicklung und von Trusted Computing auf sich vereinen. Nachfolgend seien drei davon erwähnt:

**Vertrauenswürdigkeit** Die reduzierte Komplexität der Trusted Computing Base, das heisst, des Teils eines informationsverarbeitenden Systems, der alle Sicherheitsfunktionen enthält und nach aussen hin abgegrenzt ist [18], verringert die Wahrscheinlichkeit von Fehler während der Entwicklung und der Wartung. Dies erhöht wiederum die Vertrauenswürdigkeit (trustworthiness) der Implementation. Dies ermöglicht auch eine kostengünstige Evaluation gegen Sicherheitsstandards, wie z.B. die Common Criteria, da sich die sicherheitskritischen Komponenten nur selten ändern [33, Advantages].

**Offenheit** Die offene Implementation der sicherheitskritischen Komponenten erhöht gleichermassen die Vertrauenswürdigkeit und die Glaubwürdigkeit des Frameworks. Die offene Architektur ermöglicht es, Änderungen und Verbesserung selber vorzunehmen, ohne von einem bestimmten Hersteller abhängig zu sein. Zudem können Benutzer wie auch Sicherheitsexperten gleichermassen das Design und den Quellcode analysieren und sich vergewissern, dass keine versteckten Funktionalitäten oder Hintertüren eingebaut wurden [33, Advantages].

**Einfache Übertragbarkeit** Die Perseus-Architektur ist so ausgelegt, dass sicherheitskritische Komponenten nur auf der Schnittstelle des darunter liegenden Resource Management Layer aufbauen und nicht direkt auf hardware-spezifische Funktionen zugreifen. So können diese Sicherheitskomponenten ohne grösseren Aufwand auf andere Geräte (PDA, Smart Phones) übertragen werden, indem für jedes Gerät jeweils nur der Resource Management Layer einmalig implementiert werden muss. Die so migrierten Applikationen benötigen kaum Anpassungen, was einerseits kostengünstig ist und andererseits das Risiko, nachträglich Fehler einzubauen, minimiert [33, Advantages].

### 3.4.4 Microsft Next-Generation Secure Computing Base

Neben den Aktivitäten bei der TCG entwickelt Microsoft seine eigene Vision von Trusted Computing. Im Rahmen ihrer Next-Generation Secure Computing Base-Initiative, kurz NGSCB (vormals als „Palladium“ bekannt), sollen Schritt für Schritt Trusted Computing-Funktionalitäten in die Microsoft Betriebssysteme eingebaut werden. Für die kommende Windows-Version, genannt Windows Vista (Codename „Longhorn“), sind zwei Features geplant:

- Secure Startup: Beim Start-Vorgang werden gewisse Kenndaten des Bootprozesses mit zuvor gespeicherten Messungen verglichen. Damit können Veränderungen von Systemdateien oder von Hardware-Komponenten erkannt werden [23].

- Full Volume Encryption: Sämtliche Daten (Programmdateien, Systemdateien, temporäre Cache-Dateien) werden beim Abspeichern auf einen Festspeicher (Harddisk, Wechselmedien) verschlüsselt. Der Schlüssel, der die verschlüsselte Windows-Partition freigibt, wird während des Bootvorgangs erst dann freigegeben, wenn ausgeschlossen werden kann, dass keine Offline[6]-Veränderung stattgefunden hat (z.B. Veränderung von Systemdateien oder der Versuch, ein anderen Betriebssystem zu booten) [23].

NGSCB konzentriert sich dabei auf die software-seitige Implementation von Trusted Computing und setzt eine entsprechende Trusted Computing-fähige Hardware-Platform voraus, wie z.B. die LaGrande-Architektur von Intel. Für die obengenannten Funktionen wird mindestens ein Trusted Platform Module benötigt, das zu den Spezifikationen der TCG konform ist.

### 3.4.5 Zusammenfassung

Bei der Entwicklung von Trusted Computing Systemen nimmt die Trusted Computing Group eine Vorreiterrolle ein. Diese Organisation soll die Standardisierung entsprechender Komponenten sicherstellen und vorantreiben. Sie entwickelt dazu Spezifikationen und Frameworks für verschiedenste Einsatzgebiete, sowohl hardware- wie auch software-seitig. Kern sämtlicher Architekturen bildet das Trusted Platform Module. Diese Spezifikationen finden Eingang in die Planung und Entwicklung zukünftiger proprietärer Hardware- und Betriebssysteme. Daneben existieren auch Open-Source-Ansätze, die eine herstellerunabhängige Umsetzung von Trusted Computing ermöglichen.

## 3.5 Das Umfeld von TC

In diesem Kapitel werden verschiedene Aspekte rund um Trusted Computing besprochen. Hauptsächlich geht es dabei um das Umfeld von TC. Im Abschnitt 3.5.1 wird TC im Umfeld von Sicherheitsüberlegungen behandelt. Die in den vorangegangenen Kapitel beschriebenen Lösungen sorgen selber wieder für weitere Probleme. Einige werden kurz dargestellt und diskutiert. Da man im Zusammenhang mit TC immer wieder die Thematik des Digital Rights Management (DRM) miteinbezieht, werden auch hier das Umfeld von DRM und die Möglichkeiten im Rahmen von TC in einem eigenen Abschnitt erwähnt. Dabei wird besprochen warum DRM notwendig ist und weshalb besondere Probleme im Zusammenhang mit TC entstehen. Im Abschnitt 3.5.3 geht es um die Interessengruppen Rund um TC. Was sich diese durch den TC-Ansatz erhoffen und wie sie die Möglichkeiten und Probleme für ihre eigenen Interessen nutzen, bzw einsetzen können.

[6]Mit „offline“ wird der abgeschaltete bzw. heruntergefahrene Systemzustand bezeichnet.

### 3.5.1 TC und Sicherheit

Im Abschnitt "Attestation" werden Probleme, die dieser Mechanismus hervorruft, behandelt. In diesem Zusammenhang werden auch Probleme mit der Zertifikation von Software und Hardware diskutiert und deren mögliche Auswirkungen auf den Markt dargestellt. Eine weitere wichtige Funktion von TC, die Verschlüsselungsfunktion, bringt ihrerseits auch Probleme mit sich. Diese werden im Abschnitt "Sealed Storage" kurz dargestellt. Bereits heute sind Trusted Plattform Modules (TPM's) im Einsatz. An dieser Stelle wird ein kurzer Einblick gegeben, wie sich die aktuellen Modelle in einem Test verhalten haben.

#### Attestation

Durch das sichere Booten und Erstellen der Hash-Chain wird eine sichere Information erstellt, betreffend der aktuell in Ausführung befindlichen Plattformkonfiguration. Jede Änderung dieser Konfiguration, insbesondere der Softwarekomponenten, durch Patches oder Updates, verändert somit auch die Hash-Chain und somit den konfigurationsabhängigen Wert. Da nicht alle Benutzer ihre Softwarekomponenten immer sofort auf dem aktuellsten Stand halten und unter Verwendung verschiedenster Softwarekomponenten und verschiedener Betriebssystemen, steigt die Anzahl möglicher Konfigurationen stark an. Aufgrund dieser hohen Anzahl ist es somit schwierig, jede Konfiguration betreffend Sicherheit zu verifizieren. Durch diesen Sachverhalt wird die Gefahr abgeleitet, dass z.B. Online-Services nur noch mit einigen wenigen, definierten Konfigurationen zugänglich sein werden. Das heisst: Der Benutzer wird seine Konfiguration so einrichten, dass er Zugang zu den gewünschten Services bekommt. Dies kann dazu führen, dass kleinere Hard- und Softwarehersteller langsam vom Markt verdrängt werden, wenn die betreffenden Produkte nicht in den gängigen, vordefinierten Konfigurationen enthalten sind. Dies wird vor allem kritisch für die kleineren Hersteller, falls Dienstanbieter mit grossen Herstellern zusammenarbeiten. [30] Eine mögliche Lösung dieses Problems der vielen Konfigurationen, ist der Ansatz der Property-based Attestation [30], bei der nicht mehr die genauen Konfigurationen massgebend sind, sondern die gewährleistete Funktionalität (inklusive Sicherheitsanforderungen).

Die Flexibilität und einfache Erweiterbarkeit von Betriebssystemen, wie auch von Applikationen haben dazu beigetragen, dass sich die Benutzung von PC-Systemen ausgebreitet hat. Genau diese Mechanismen sind es aber auch, die Sicherheitslücken hervorrufen und von Malware ausgenutzt werden können. [27] Hat sich schädliche Software einmal eingenistet, ist es schwierig diese zu entdecken und gegebenenfalls wieder zu entfernen. In einer TC-Umgebung muss sich jedoch ein Programm beim Betriebssystem registrieren um ausgeführt zu werden. Dies verhindert, dass auch Malware unbemerkt ausgeführt wird. Allerdings ist eine TC-Umgebung absolut machtlos wenn Malware Sicherheitslücken, Bugs oder sonstige Schwachstellen von legitimierter Software ausnutzt. TC kann nicht Fehler in Software entdecken und diese als nicht vertrauenswürdig klassifizieren. Dasselbe gilt auch für Hardware, insbesondere für das TPM.[27]

**Sealed Storage**

Sealed storage garantiert, dass die Konfiguration beim Schreiben und Lesen von Daten dieselbe ist. Ist dies nicht der Fall, kann das System die Daten nicht mehr entschlüsseln. [16] Diese Funktion bietet betreffend Datensicherheit neue Möglichkeiten. Mittels sealed storage ist es zum Beispiel möglich Daten, die mit einer bestimmten Applikation erstellt wurden, an diese zu binden. Dies hat zur Folge, dass die betreffenden Daten nur noch mit dieser Applikation gelesen werden können. So können z. B. Microsoft-Dokumente nicht mehr mit Open Office gelesen werden. [5]

Allerdings treten auch diverse Probleme auf. Es kann Vorteile haben, Daten gegen aussen zu schützen indem sie verschlüsselt werden, aber sealed storage bringt auch gegenüber dem Benutzer Nachteile mit sich. Was passiert mit den Daten, wenn z.B. Ein update installiert wird? Wie kann man Daten auf ein neues System migrieren? Im Falle eines Hardwaredefekts des TPM's können die Daten nicht mehr wiederhergestellt werden. Es sei denn, der TPM Hersteller hat den Schlüssel bei sich noch einmal gespeichert. Dies stellt allerdings wieder ein Sicherheitsrisiko dar. Der Benutzer kann seine Daten also nicht mehr frei benutzen, vervielfältigen oder auf andere Geräte verschieben.

**TPM compliance**

Der zentrale Punkt sämtlicher TC-Architekturen bildet das Trusted Plattform Module (TPM). Massgebend für die Korrektheit der TC-Funktionen ist die Implementation des TPM. Um diese zu testen, entwickelt die Applied Data Security Group der Bochumer Ruhr-Universität eine Test-Suite. Obwohl diese noch nicht komplett ist, wurden Im April 2006 erste Ergebnisse veröffentlicht. Diese sind auf `www.prosec.rub.de/tpmcompilance.html` ersichtlich. Es wurden 5 TPM's von 3 verschiedenen Herstellern getestet. Dabei stellt sich heraus, dass ein einziger Testkanditat die Tests bestanden hat und somit als fehlerfrei gilt. Bei einem anderen Produkt bestehen zum Beispiel Mängel in der Umsetzung der TPM-Spezifikation. Die getesteten TPM's sind nicht irgendwelche Prototypen, sondern werden in bereits erhältliche Geräte eingebaut. [11] Die Risiken die eine fehlerhafte oder unvollständige Implementation mit sich bringen, wurden im Abschnitt über Attestation bereits beschrieben. Im Falle von Bugs in Software ist es möglich diese mittels Patches zu beheben. Bei Hardware ist es allerdings in der Regel nicht so leicht, Fehler zu beheben.

### 3.5.2 TC und DRM

Wenn man einen Artikel über Trusted Computing liest, so behandelt dieser praktisch immer auch die Thematik um Digital Rights Management (DRM). Dieser Abschnitt soll den Zusammenhang zwischen TC und DRM erklären. Dazu werden Möglichkeiten gezeigt wie TC eingesetzt werden kann, um DRM durchzusetzen. Gleichzeitig wird aber auch auf Gefahren und Probleme hingewiesen. DRM (Digital Rights Management) wird definiert als ein System, dass die Copyrights von Daten die über das Internet oder andere digitale Medien schützt, indem sichere Verteilung gewährleistet und/oder illegale Verteilung von Daten verhindert wird. Typischerweise schützt ein DRM-System geistiges Eigentum

mittels Verschlüsselung von Daten, so dass diese nur von autorisierten Benutzern benutzt werden können. Oder die Daten werden mit einem digitalen Wasserzeichen markiert, sodass der Inhalt nicht frei verteilt werden kann. [39]

### Umfeld

Die Softwareindustrie, sowie die Musikindustrie erfahren hohe Verluste durch unerlaubtes Kopieren von Daten. Z.B. "auf über 90 % aller Computer in China ist illegal kopierte Software installiert". [25] Durch die Einführung eines Systemes zum Schutze von Inhalten erhoffen sich die genannten Industrien eine Verbesserung der Situation. Die Bemühungen geistiges Eigentum im IT Bereich durch technische Massnahmen erfolgreich zu schützen, benötigt auch einen rechtlichen Rahmen. Dieser ist in den USA durch den Digital Millennium Copyright Act (DMCA) gegeben. DMCA verbietet die Umgehung von Kopierschutztechniken. Im Gegensatz dazu die Schweiz, die mit der momentan laufenden Urheberrechtsrevision verbietet, Schutzmechanismen zu umgehen, aber Kopien für den Privatgebrauch erlauben will. Zu diesem Zweck hat eine Umgehung von Schutzmassnahmen keine rechtlichen Folgen. [10] Aus diesem Beispiel wird die Problematik ersichtlich, dass verschiedene Gesetzesgrundlagen unterschiedliche Handlungsspielräume nach sich ziehen.

### Möglichkeiten und Probleme

Grundsätzlich ist es schwierig, Medieninhalte zu schützen. Denn einerseits soll sichergestellt werden, dass die Inhalte nicht unerlaubt kopiert werden können, andererseits muss die Möglichkeit bestehen, die Inhalte zu konsumieren, sofern sie rechtmässig erworben wurden. In anderen Worten, Musik muss gehört werden können und Videoinhalte müssen gesehen werden können. Nun ist es relativ einfach, eine Kopie von einem Film zu erhalten, nämlich indem man in mit einer Kamera vom Bildschirm erneut aufzeichnet. Gleiches gilt auch für Musik, die mit einem Mikrofon via Lautsprecher aufgenommen wird. Dies ist möglich, auch wenn die Originaldaten gegen unerlaubtes Kopieren geschützt sind.

Nachfolgend ein Beispiel, wie TC hilft, DRM zu unterstützen: Will ein Benutzer Inhalte von einem Anbieter beziehen, so prüft dieser die aktuelle Konfiguration des Benutzers. Wird diese als vertrauenswürdig befunden, so kann der Benutzer den gewünschten Inhalt beziehen. Dieser wird sofort, in Abhängigkeit von der aktuellen Konfiguration, verschlüsselt gespeichert. Der Benutzer kann anschliessend nur mit der betreffenden Konfiguration auf den Inhalt zugreifen. Dies bedeutet für den Benutzer, dass er das Betrachterprogramm, um auf die Inhalte zuzugreifen, nicht wechseln kann, da dies ja eine Veränderung der Konfiguration bedeuten würde. Die betreffenden Inhalte können auch nicht an dritte weitergegeben werden, da diese sicher verschlüsselt sind und somit von dritten nicht lesbar sind. Mit sicher ist in diesem Zusammenhang gemeint, dass jedes Cryptomodul einen einzigartigen Schlüssel verwendet und dieser in die Verschlüsselung von geschützten Inhalten einfliesst. Die Inhalte sind somit vor der Wiedergabe auf fremden Systemen geschützt, selbst wenn sie mit der dafür benötigten Konfiguration gefahren werden.[16]

Das genannte Beispiel einer möglichen Anwendung von TC im Bereich des DRM ist jedoch nur bedingt sicher: Es besteht immer noch die Möglichkeit, die Kommunikation zwischen

TPM und dem Prozessor abzufangen. Mittels Methoden von so genannten Hardwareattacken kann die Kommunikation zwischen TPM und Prozessor abgefangen und verändert werden. Beispiele für Hardwareattacken sind schizophrenic access memory (SPAM) und schizophrenic basic input/output system (SPIOS) mehr dazu im Artikel von Huang, The Trusted PC: Skin-Deep Security. [16] Aus diesen Überlegungen wird ersichtlich, dass die TC-Architektur nicht geeignet ist, ein System vor seinem Benutzer zu schützen. Diesbezüglich gibt es Möglichkeiten, das TPM vor physikalischem Zugriff zu schützen indem das Systemgehäuse versiegelt wird. Diese Vorgehensweise hat jedoch zur Folge, dass somit auch sämtliche anderen Manipulationen an der Hardware unmöglich werden. Eine geeignete Membran am Gehäuse könnte dafür sorgen, dass bemerkt wird wenn das Gehäuse geöffnet wird, dies sogar ohne dass das System in Betrieb ist. Allerdings ist es dann auch unmöglich z.B. eine neue Videokarte einzubauen oder sonstige Hardwareerweiterungen vorzunehmen.

TC ist kein eigentliches DRM-System, kann aber DRM unterstützen, dass unrechtmässige Nutzung von Software oder Wiedergabe von Medieninhalten erschwert wird, sofern diese nicht lizenziert sind. TC kann DRM nicht garantieren wie obige Überlegungen zeigen, kann aber zu einer technischen Lösung für das DRM Problem werden, wenn unsere Gesellschaft zu akzeptieren lernt, dass geistiges Eigentum ein Gut ist, das rechtlichen Schutz verdient. [27]

### 3.5.3 Interessengruppen

Die Interessengruppen rund um TC sind ein weiterer Aspekt in der Diskussion um TC. Dieser wird oft vernachlässigt, ist aber wichtig, als dass er ein gewisses Konfliktpotential beinhaltet. Grundsätzlich können zwei Interessengruppen unterschieden werden. Dies sind, wie in Abbildung 3.7 ersichtlich, die Industrie und die Benutzer (User). Eine weitere dritte Gruppe, jedoch sinnbildlich als Teilmenge der Benutzer dargestellt, sind die Business-User. Sie haben zu grössten Teil die gleichen Interessen wie die Benutzer, zu einem gewissen Teil decken sich die Interessen aber auch mit der Industrie.

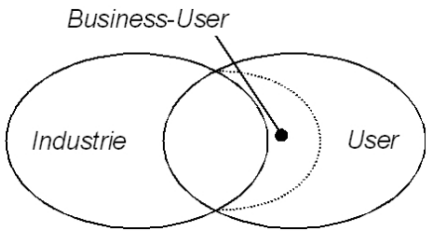



Abbildung 3.7: Interessengruppen

Mit Industrie sind vor allem die Hersteller rund um die TC-Technologie gemeint, sowie Teile der Unterhaltungsindustrie. Benutzer meint die Gruppe, die mit IT-Systemen arbeitet oder diese auch für private Zwecke benutzt. Die separat genannte Gruppe der Business-User besteht aus Unternehmungen und Firmen, die wie die Benutzergruppe IT-Systeme benutzen.

**Die Industrie**

Ein grosser Fehler wurde bei der Entwicklung der Standards gemacht: Diese fanden unter Ausschluss der Öffentlichkeit statt. Dieser Fehler wurde von der TCPA gemacht, wurde aber von der TCG erkannt und verbessert. Dieser Fehler führte zu Unsicherheiten und Spekulationen. Dies verlangsamt die Entstehung von Vertrauen in Trusted Computing.[5] Der Einsatz von TC ermöglicht es, Benutzer stärker an Produkte zu binden, wie es im Abschnitt über Sealed Storage beschrieben wurde. Diese durch TC verstärkte Bindungen erschweren einen Wechsel auf andere Produkte. Dadurch festigen sich bestehende Monopole weiter. [5]

Die Einführung von Trusted Computing würde den Markt verändern. In der TCPA Spezifikation 1.0 ist von einer hierarchischen Struktur von certification authorities die Rede, welche den Zweck haben, Hardware- und Softwarekomponenten zu zertifizieren, die zum Aufbau eines Trusted Computing Systems benötigt werden. [1] Man kann davon ausgehen, dass es sich bei den certification authorities um ein industrielles Konsortium handelt, was nicht sehr abwegig ist, wenn man die Zusammensetzung der TCG betrachtet. Ross Anderson schreibt in diesem Zusammenhang in [1] "Die Kontrolle wird somit zentral von einem industriellen Konsortium ausgeübt". Wobei "Kontrolle" darauf anspielt, dass ein Benutzer eines Trusted Computing Systems einen Teil seiner Kontrolle über sein System abgibt. Diese Problematik wird im Abschnitt über die Benutzer eingehender besprochen.

Durch die gemachten Annahmen stellt sich eine Situation ein, die die Grundlage zur Monopolbildung bildet. Dies wirkt sich nicht marktfördernd aus, wie die folgenden möglichen Auswirkungen aufzeigen: Die certification authorities, welche sich zum Teil aus grossen weltumspannenden Firmen zusammensetzen werden, wie z.B. Medienanbieter oder Betriebssystemhersteller, haben die Möglichkeit, Konkurrenzprodukte (Betriebssysteme, Applikationen) vom Markt auszuschliessen. Ausschliessen dadurch, dass die betreffenden Produkte die TC-Zertifikation nicht erhalten. Kleinere Unternehmen und Hersteller von weniger populären Produkten werden dadurch isoliert und eventuell sogar ganz vom Markt verdrängt.[30] Denn diese Unternehmen müssen ihre Produkte einerseits zertifizieren lassen, was sich als eine grosse Hürde herausstellen kann, und haben ihrerseits auch das Problem, dass sie keine alternativen Produkte mehr absetzen können, wenn Daten an eine bestimmte Applikation gebunden werden.

Des weiteren kann TC ein grosses Problem für Open Source Software werden. Sollte eine Zertifikation erforderlich sein, so wird der Vorteil der Modifikation und Weiterverbreitung zunichte sein. Denn sobald eine Modifikation an der Software stattgefunden hat, wird das Zertifikat ungültig und die Software kann nicht mehr eingesetzt werden.[5]. Die Möglichkeit, zu verhindern dass existierende Produkte modifiziert werden, führt zu verminderter Innovation.[1] Ein für die Industrie angenehmer Nebeneffekt von TC ist, Produkte vor Piraterie schützen zu können. Gemäss der TCPA-FAQ von R. Anderson muss man im Zusammenhang mit DRM "den Nutzer als den Feind betrachten". [2]

**Die Benutzer**

Die Thematik der IT-Sicherheit ist kein Fremdwort für die Benutzergruppe, dennoch herrschen TC gegenüber Unsicherheit und Spekulationen aus oben genannten Gründen vor. Was durchaus begrüsst wird, ist ein gewisser Umfang der Funktionalität.

- Start des Systemes in einem vertrauenswürdigen Zustand (Authenticated Boot)
- Schutz von Schlüsseln
- Schutz von Daten (Sealed Storage)
- Beglaubigung gegenüber von Dritten (Remote Attestation)

Der letzte Punkt der Aufzählung ist jedoch mit Kritik verbunden. Einerseits ist ein Missbrauchspotential vorhanden, andererseits sind damit in der Anwendung Einschränkungsmöglichkeiten gegeben. Will ein Benutzer einen Dienst benutzen, kann der Dienstanbieter den Dienst abhängig von einer bestimmte Konfiguration anbieten, [5] was auf Benutzerseite eine Einschränkung darstellt. Benutzer hatten bisher die alleinige Kontrolle über ihr System, konnten Hardware und Software nach eigenen Präferenzen und Möglichkeiten einsetzen. In Zukunft könnte die Kontrolle, die man über sein eigenes System hat, verringert werden, dafür erhält man im Austausch mehr Sicherheit.[5]

Die anfängliche Unsicherheit hat zu diversen Kritikern geführt. So zum Beispiel den Chaos Computer Club (CCC), der vor einer Umsetzung von TC warnt. R. Anderson ist ein weiterer TC-Kritiker, der zu diesem Thema mehrere Arbeiten verfasst hat und auch der Autor der TC-FAQ [2] ist. Dort wehrt er sich mit Argumenten gegen TC die zu einem grossen Teil DRM betreffen. Einige Aussagen wurden von D. Safford, IBM Research, berichtigt. So z.B., dass man die TCPA nicht mit DRM in den selben Topf werfen kann.[31] Diese kleine Gegenüberstellung von Aussagen soll als Beispiel dienen für die anfänglichen Unsicherheiten in Bezug auf TC. Zu beachten sind die jeweils nicht mehr ganz aktuellen Daten der betreffenden Dokumente (aus dem Jahr 2002). Diese Diskussionen und Spekulationen zusammen mit fehlender Information seitens der damaligen TCPA, schufen die ursprüngliche Unsicherheit, die zu einem gewissen Grad heute noch herrscht.

Für den Endbenutzer ist es schwierig, sich objektiv über Trusted Computing zu informieren. Da die TC-Gegner wie auch Befürworter aggressive Werbung für ihre Positionen propagieren. Seitens der TC-Gegner wurde zum Beispiel das Gerücht in Umlauf gesetzt dass ein Besitzer die Kontrolle über sein System weitgehend verliert und DRM der Musikindustrie ermöglicht die totale Kontrolle über ihre Produkte zu übernehmen, sodass man im schlimmsten Fall nur noch an seinem Geburtstag Zugriff auf eine gekaufte CD hat.[1]

Befürworter werben mit Schutz vor Viren, Würmern, Trojanern, etc. und mit der Sicherheit von persönlichen Daten, dank verschlüsselter Speicherung. Beide Seiten übertreiben und unterschlagen Informationen was den privaten Endbenutzer verunsichert. Denn TC wird nicht unerwünschten Programmen wie Viren, Trojaner, etc. definitiv vom eigenen System verbannen, sondern erhöht die Resistenz vor solchen Programmen. Sind diese jedoch trotzdem einmal auf dem Rechner, können auch sie diese TC-Mechanismen nutzen, was es in diesem Falle nicht einfacher macht, unerwünschte aber bereits eingenistete Programme zu entfernen.[15]

**Zukunft**

Es sind bereits Notebooks im Handel, die Hardware beinhalten die nach ersten Spezifikationen der TCG entwickelt wurde. Das kommende Windows-Betriebssystem namens Vista, benötigt noch nicht zwingend ein TPM. Es ist keine Voraussetzung sondern eine Option. Vista unterstützt bereits einige TC Funktionen, sofern auch das Bios die nötigen Voraussetzungen erfüllt. Die angebotenen Funktionen sind namentlich: Secure Startup und Full-Volume Encryption. [42]

Nach C. Anderka, Pressesprecher bei Intel, wird TC im Business-Umfeld schnell angenommen, da dort die Motivation gross ist, ein sicheres Netzwerk aufzubauen in dem Netzwerkzugriffe der Trusted Plattform unterstehen. Die "normalen Consumer" werden etwas länger brauchen um das System anzunehmen, da es, so Anderka, mehr Zeit braucht bis sich die Vorteile herumgesprochen haben.[44]

Die TCG selber sagt, dass es keinen Nutzungszwang gibt. Zum einen sei das TPM bei der Lieferung per default deaktiviert, zum anderen kann der Benutzer das TPM nach belieben ein- und ausschalten. Allerdings, so Kritiker, besteht die grosse Gefahr, dass Dienste, Dokumente und Informationen nur noch mit eingeschaltetem TPM zugänglich sein werden, sobald eine kritische Masse von Benutzern erreicht ist.[5]

**Fazit**

TC ist eine neue Technologie, ein Werkzeug. Wie und wozu es genau eingesetzt wird, steht noch offen.

**Zusammenfassung**

Die in diesem Kapitel besprochenen Hauptfunktionen der TC-Architektur, Attestation und Sealed Storage bieten eine Möglichkeit an, die Sicherheit zu verbessern. Allerdings kommen mit den neuen Lösungen auch neue Probleme, die zum grössten Teil noch ungelöst sind. Digital Rights Management (DRM) löst grosse Diskussionen im Zusammenhang mit TC aus. Obwohl TC kein DRM-System ist, gibt es Möglichkeiten, DRM zu unterstützen. Allerdings ist TC nicht dazu gemacht, das System vor dem Benutzer zu schützen, sondern gegen Attacken von aussen. Ein weiteres Problem ist der Interessenkonflikt der um TC herum stattfindet: Benutzer sollen einen Teil ihrer Kontrolle über ihr System abgeben, um im Gegenzug mehr Sicherheit zu erhalten. TC ist nicht nur eine leere Theorie, es sind bereits heute Systeme mit einem integrierten Trusted Platform Module (TPM) im Umlauf.

## 3.6 Zusammenfassung

Die Sicherheit in der IT ist ein heikles Thema. Vor allem in Unternehmungen ist es schwierig für die IT-Verantwortlichen, die entsprechende Ausgaben zu rechtfertigen. Privatan-

wender überschätzen dagegen oft die Wirkung von eingesetzten Sicherheitstechnologien. Aufgrund der heutigen globalen Vernetzung ist es umso wichtiger, IT-Systeme vor unerlaubten Zugriffen und Malware zu schützen, da sich die Verbreitung schädlichen Programmcodes wesentlich schneller bewerkstelligen lässt, als vor dem Siegeszug des Internets. Bei der Entwicklung von Betriebssystemen wird bezüglich Sicherheit wenig getan und im nachhinein sind sicherheitsrelevante Verbesserungen in einem hochkomplexen System nur noch sehr schwierig zu bewerkstelligen.

Trusted Computing (TC) wird von der Trusted Computing Group (TCG) ausgearbeitet und spezifiziert. Die TCG bietet eine Architektur an, die Systeme besser schützen kann, als dies heute gewöhnlich durch ein Sammelsurium verschiedener Einzellösungen erreicht wird. Dazu gehört auch eine Hardwarekomponente, das Trusted Platform Module (TPM), das in Kombination mit geeigneten Softwarekomponenten Basisservices und Anwendungen anbietet. Integrity Protected Booting, hardwaremässige Verschlüsselung, Sealed Storage, Remote Attestation sind solche Anwendungen und wurden in Abschnitt 3.3 besprochen.

Die von der TCG spezifizierte Architektur baut auf den drei Roots of Trust und den Trusted Building Blocks (TBB) auf, die auch die Trust Boundary bilden. Diese Vertrauensgrenze darf von Komponenten von ausserhalb nur überschritten werden, wenn diese Komponenten als vertrauenswürdig eingestuft werden. Dieser Vorgang wird durch den Prozess "Transitive Trust" ermöglicht. Das TPM besteht aus einzelnen Komponenten, wie I/O, Non-volatile storage (Speicherung von key's), Platform Configuration Register (PCR), Program Code, Random Number Generator, SHA-1 Engine, Key Generation, RSA Engine, Opt-in und Execution Enginge. Die Funktionsweise der Komponenten wurde kurz erläutert. Weiter wurde auf die hardwareseitige Lösung von Intel LaGrande eingegangen.

Nach der Präsentation einer hardwaregestützten Lösung wurde mit der Perseus Security Architecture auch eine Softwarelösung besprochen. Das Open Source Projekt der Universität Bochum ist ebenfalls eine generische Architektur. Sie besteht aus den drei im folgenden genannten Schichten: Der Hardware Layer, der Resource Management Layer, der zusammen mit der Trusted Software Layer den Security Kernel bildet. Darüber befinden sich die Betriebssysteme in dem Application Layer. Die Vorteile drücken sich, neben den Vorteilen von Open Source Entwicklungen, durch Vertrauenswürdigkeit, Offenheit und einfacher Übertragbarkeit aus.

Auch Microsoft entwickelt eine Version von TC. Die Next-Generation Secure Computing Base-Initiative (NGSCB) soll schrittweise die Microsoft Betriebssysteme in Richtung von Trusted Computing Plattformen führen.

Funktionen, wie Attestation und Sealed Storage, können Verbesserungen der IT-Sicherheit bringen. Gleichzeitig werfen sie weitere Probleme auf. Einige davon werden im Kapitel 3.5 kurz beschrieben. TC ist nicht die Lösung jeglicher Probleme der IT-Sicherheit, da auch TC nicht garantieren kann, dass auszuführender Code frei von Malware ist oder Sicherheitslücken in Form von Seiteneffekten aufwirft.

Eine weitere, heiss diskutierte, mögliche Funktion von TC ist das Digital Rights Management (DRM). Die Software- und Unterhaltungsindustrie erfährt jährlich Milliardenverluste durch Piracy. Mittels TC-Funktionen ist es möglich unzulässigen Zugriff auf Daten,

und somit auch auf Medieninhalte, zu erschweren. Neben der Industrie gibt es noch eine weiter Gruppe die in der Diskussion um TC involviert ist, es sind dies die Benutzer. Befürchtete Einschränkungen und der teilweise Verlust von Kontrolle über das eigene System führt zu Kritik an der TC-Architektur.

# Literaturverzeichnis


[1] Anderson R.: Cryptography and Competition Policy - Issues with 'Trusted Computing', Cambridge University, 2003.

[2] Anderson R.: Trusted Computing Frequently Asked Questions, Version 1.1 (August 2003), www.cl.cam.ac.uk/~rja14/tcpa-faq.html, 18.04.2006.

[3] Anderson R., Bond M., Clulow J., Skorobogatov S.: Cryptographic Processors-a survey, Proceedings of the IEEE (Vol.94, Issue 2, p.357-359, IEEE: 01580505.pdf), http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5, Februar 2006.

[4] Bruschi D., Cavallaro L., Lanzi A., Monga M.: Replay Attack in TCG Specification and Solution, Universität Mailand (Departement für Informatik und Kommunikation), 2005.

[5] Bundesamt für Sicherheit in der Informationstechnik: Trusted Computing im praktischen Einsatz, http://www.bsi.de/sichere_plattformen/trustcomp/infos/tpm_report/praxis_kritik.htm, 20.05.2006.

[6] Bundesamt für Sicherheit in der Informationstechnik: Sichere Plattformen und die Trusted Computing Group, http://www.bsi.bund.de/sichere_plattformen, 04.11.2004.

[7] Bureau of Export Administration: Export Administration Regulations (EAR), http://www.cdt.org/crypto/admin/000110cryptoregs.shtml, 10.01.2000.

[8] Casualty Risk Consulting: Internet and insurance (Information for insurers), Münchener Rückversicherungs-Gesellschaft, www.munichre.com/publications/302-04311$_$en.pdf, 2005.

[9] Cheswick B., Bellovin S., Rubin A.: Firewall and Internet Security (2nd Edition), Addison-Wesley, 2003.

[10] ct - Magazin für Computer und Technik: Schweizer Bekenntnis zur digitalen Privatkopie, Heise Verlag, Ausgabe 10 2006, S. 38,39.

[11] ct - Magazin für Computer und Technik: Sicherheits-Chips auf den Zahn gefühlt, Heise Verlag, Ausgabe 10 2006, S. 28.

[12] Erickson J., Mulligan D.: The Technical and Legal Dangers of Code-based Fair Use Enforcement, Proceeding of the IEEE (VOL. 92, NO. 6), Juni 2004.

[13] Farber, D.: Fame but no riches for cybersecurity, Spectrum (Vol.40, Issue 1, p.51-52, IEEE: 01159731.pdf), http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6, Januar 2003.

[14] Felten, E: Understanding trusted computing; will its benefits outweigh its drawbacks?, Security & Privacy Magazine (Vol.1, Issue 3, p.60-62, IEEE: 01203224.pdf), http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013, Mai 2003.

[15] Hansen M. (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein): Ein zweischneidiges Schwert, Über die Auswirkungen von Trusted Computing auf die Privatsphäre, www.datenschutzzentrum.de/allgemein/trusted_computing.htm, 18.04.2006.

[16] Huang A.: The trusted PC; skin-deep security, Computer (Vol.35, Issue 10, p.103-105, IEEE: 01039525.pdf), http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=2, Oktober 2002.

[17] Intel: LaGrande Technology for Safer Computing, http://www.intel.com/technology/security, 21.05.2006.

[18] Donald C. Latham: Trusted Computer System Evaluation Criteria, Department of Defense, http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html, 26.12.1985.

[19] Leavitt N.: Will proposed standard make mobile phones more secure?, Computer (Vol.38, Issue 12, p.20-22, IEEE: 01556478.pdf), http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=2, Dezember 2005.

[20] Lubich H. P.: Sicherheitsverantwortliche in der Zwickmühle: IT-Sicherheit zwischen Erwartungs- und Kostendruck, Neue Zürcher Zeitung (Orbit-IEX Beilage), 16.05.2006.

[21] Microsoft, http://www.microsoft.com/presspass/legal/allchin.mspx, 23.04.06.

[22] Microsoft: Next-Generation Secure Computing Base, http://www.microsoft.com/resources/ngscb, 21.05.2006.

[23] Microsoft: Secure Startup - Full Volume Encryption: Executive Overview, http://www.microsoft.com/whdc/system/platform/pcdesign/secure-start_exec.mspx, 25.04.2005.

[24] Nugent J., Raisinghani M.: The Information Technology and Telecommunications; Security Imperative; Important Issues and Drivers, Journal of Electronic Commerce Research (Vol.3, No.1), http://www.csulb.edu/web/journals/jecr/issues/20021/paper1.pdf,2002.

[25] NZZ Online, Made in China, http://www.nzz.ch/2006/05/21/wi/articleE50W3.html, 05.06.2006.

[26] Oltsik J.(Enterprise Strategy Group): White Paper, Trusted Enterprise Security, How the Trusted Computing Group (TCG) Will Advance Enterprise Security, www.trustedcomputinggroup.org/news/Industry_Data/ESG_White_Paper.pdf, 18.04.2006.

[27] Oppliger R., Rytz R.: Does trusted computing remedy computer security problems?, Security & Privacy Magazine (Vol.3, Issue 2, p.16-19, IEEE: 01423956.pdf), http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013, März 2005.

[28] Oppliger R., http://www.ifi.unizh.ch/$\~$oppliger/Teaching/Teil1.pdf, 23.04.06.

[29] Reid J., Nieto J., Dawson E., Okamoto E.: Privacy and trusted computing, Queensland University of Technology in Australia and University of Tsukaba in Japan, 2003.

[30] Sadeghi A., Stüble C.: Property-based Attestation for Computing Platforms, Ruhr-University Bochum, 2005.

[31] Safford D.: Clarifying Misinformation on TCPA, IBM Research, Oktober 2002, http://www.research.ibm.com/gsal/tcpa/tcpa_rebuttal.pdf, 19.04.2006.

[32] Stiller B.: Seminar Talks, Titles and Organizational Information (SS 2006), Universität Zürich, 2006.

[33] Christian Stüble: The Perseus Security Architecture, Ruhr-Universität Bochum, http://www.perseus-os.org, 21.05.2006.

[34] Trusted Computing Group: Trusted Computing Group, https://www.trustedcomputinggroup.org, 21.05.2006.

[35] Trusted Computing Group: TCG Specification Architecture Overview, https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf, 28.04.2004.

[36] Vaughan-Nichols, S.: How trustworthy is trusted computing?, Computer (Vol.36, Issue 3, p.18-20, IEEE: 01185209.pdf), März 2003.

[37] Van Essen U.: Common Criteria Version 2.0 fertiggestellt, http://www.bsi.de/cc/artikel1.pdf, 29.05.2006.

[38] Voss A.: Das grosse PC & Internet Lexikon, Data Becker, 2002.

[39] Webopedia http://www.webopedia.com/TERM/D/DRM.html, 21.05.2006.

[40] Wikipedia: http://de.wikipedia.org/wiki/Trusted_Computing_Group, 29.05.06.

[41] Wobst R., Schmidt J.: Konsequenzen der erfolgreichen Angriffe auf SHA-1, http://www.heise.de/security/artikel/56555, 18.02.2005.

[42] www.heise.de, Windows Vista: Microsoft präzisiert Hardware-Voraussetzungen, http://www.heise.de/newsticker/meldung/69336 06.06.2006.

[43] www.heise.de, Kein Vertrauen in Trusted Computing, `http://www.heise.de/newsticker/meldung/39280`, 06.06.2006.

[44] www.macnews.de, Interview: Intel zum Trusted Computing, mit Christian Anderka, Pressesprecher bei Intel `http://www.macnews.de/index.php?_mcnpage=7019`206.06.06.

# Kapitel 4

# Metro Ethernet

*Stefan Weibel, Maik Lustenberger, Roman Wieser*

*In der heutigen Zeit werden eine grosse Menge von Informationen ausgetauscht. Ein häufiges Medium,welches dabei benutzt wird, ist ein Netzwerk. Es existieren bereits heute viele Technologien, wie ATM, Frame Relay, Ethernet oder ADSL. In der Schweiz gibt es zwei Hauptanbieter von Internetzugängen, eine über das Telefonnetz und die andere über das Fernsehnetz. Andere Möglichkeiten von Verbindungen zwischen verschiedenen Standorten sind eigene Leitungen, was mit hohen Kosten verbunden sein kann. Metro Ethernet ist eine der Möglichkeiten, die in den letzten Jahren an Bedeutung gewonnen hat, um ein Netzwerk zu bilden. Dieser Artikel soll ein paar Einblicke geben über verschiedene Technologien, die heute benutzt werden und zeigen wie Metro Ethernet funktioniert.*

## Inhaltsverzeichnis

**4.1 Einleitung . . . . . 115**
**4.2 Grundlagen . . . . . 115**
4.2.1 Ethernet . . . . . 115
4.2.2 Optical Networks . . . . . 116
4.2.3 Frame Relay und ATM Networks . . . . . 116
**4.3 Metro Ethernet Services: Technische Übersicht . . . . . 117**
4.3.1 User Network Interface (UNI) . . . . . 118
4.3.2 Ethernet Virtual Connection (EVC) . . . . . 118
4.3.3 Ethernet Service Definition Framework . . . . . 119
4.3.4 Ethernet Service Types . . . . . 119
4.3.5 Ethernet Service Attribute . . . . . 121
**4.4 Einschränkungen und Möglichkeiten von Metro Ethernet . . 130**
4.4.1 Einschränkungen . . . . . 131
4.4.2 Möglichkeiten . . . . . 132
**4.5 Verwendete Geräte . . . . . 133**
4.5.1 End-User Geräte . . . . . 133
4.5.2 User Provider-Edge . . . . . 133
4.5.3 Provider-Edge Aggregation . . . . . 133
4.5.4 Network Provider-Edge . . . . . 133
**4.6 Beispiele . . . . . 134**
4.6.1 Cisco-Metro-Ethernet-Services . . . . . 134
4.6.2 Fastweb . . . . . 134
4.6.3 Telstra . . . . . 135
4.6.4 Zukunft . . . . . 135
**4.7 Marktsituation Metro Ethernet . . . . . 136**
4.7.1 Ist-Zustand . . . . . 136
4.7.2 Bandbreitenbedürfnisse . . . . . 137
4.7.3 Carrier Technologie Metro Ethernet . . . . . 138
**4.8 Zusammenfassung und Fazit . . . . . 139**

## 4.1 Einleitung

Ein Metro Ethernet ist viel mehr als ein Metro Area Network (MAN)! Metro Ethernet ist in Asien bereits stark im Vormarsch, in Europa und speziell in der Schweiz ist es aber noch nicht so bekannt. Doch um was handelt es sich bei Metro Ethernet? Es geht darum, den Kunden Ethernet basierte Services anzubieten. Damit können zum Beispiel zwei Filialen eines Geschäftes per „Ethernet“ verbunden werden. Die beiden Netzwerke erscheinen wie ein einziges LAN. Doch zwischen den Gebäuden wird auf bewährte Technik wie ATM oder Frame Relay gesetzt. Der Provider sorgt dafür, dass die Rahmen aus dem einen LAN das andere erreichen und kapselt sie in die für den Transport notwendigen Protokolle. Metro Ethernet ist also ein Kunstbegriff, mit Ethernet hat es nicht mehr viel zu tun. Es wird davon ausgegangen, dass der Begriff Ethernet marketingtechnisch verwendet wurde, da Ethernet einen hohen Bekanntheitsgrad hat.

Unsere Arbeit führt den Leser zuerst knapp in Grundlegende Techniken für ein Metro Ethernet ein. Danach wird relativ ausführlich auf technische Aspekte eingegangen. Auch Einschränkungen und Möglichkeiten von Metro Ethernet werden aufgezeigt. Anschliessend folgen einige Angaben zu den Geräten, die für ein Metro Ethernet verwendet werden und einige Beispiele aus der Praxis. Abschliessend beleuchten wir die ökonomischen Aspekte von Metro Ethernet mit dem Schwerpunkt Schweiz und Europa.

## 4.2 Grundlagen

Um zu verstehen, was ein Metro Ethernet alles leisten kann - und was nicht - wird hier ganz kurz auf einige grundlegende Techniken wie Ethernet und ATM eingegangen, auf welchen ein Metro Ethernet zurückgreift, um seine Dienste zu Verfügung zu stellen.

### 4.2.1 Ethernet

#### Geschichte

Das Ethernet wurde 1976 von Bob Metcalfe und David Boggs am Xerox Forschungszenter in Palo Alto entwickelt. Basierend auf dem ALOHANET, welches per Funk verschiedene hawaiianische Inseln miteinander verbunden hatte, wurde das kabelbasierte Ethernet verwendet, um vorher isolierte Personal Computer miteinander zu verbinden. Gegenüber dem ALOHANET konnten die Clients auf dem Koaxialkabel erkennen, ob schon ein anderer Client am Senden ist, und so Kollisionen minimieren (Carrier Sense Multiple Access). Die Entwickler konnten die Datentransferraten auf 10 Mbps ausbauen und sie nannten das Ethernet DIX-Standard. Daraus wurde später der IEEE 802.3 Standard. Mit der Weiterentwicklung des Ethernets wurden die Koaxialkabel mehr und mehr durch die vom Telefon bekannten Twisted Pair Kabel ersetzt. Durch die Twisted Pair Kabel wurde allerdings die maximale Distanz zwischen zwei Geräten erheblich verkleinert. Durch bessere Kabel (100Base-TX, Cat 5 UTP; 100Base-FX, fiber optics) und schnellere Computer entwickelte

sich das Fast Ethernet (IEEE 802.3u). Fast Ethernet bietet Datentransferraten von 100 Mbps. Diese kann (ausser bei 100Base-T4) voll duplex genutzt werden. Mittlerweile erreichen die neuen Ethernet Standards Geschwindigkeiten von 1 Gbps (IEEE 802.3z) und mehr. Diese Standards werden nur noch auf kurzen Distanzen über Twisted Pair Kabel realisiert. Bei längeren Verbindungen wird auf Glasfaserkabel gesetzt. [2]

#### Ethernet heute

Bei der Netzwerkverkabelung innerhalb von Gebäuden ist (Fast) Ethernet mittlerweile Standard geworden. Andere Local Area Networks, wie Token Ring, werden nur noch sehr selten benutzt. Innerhalb der Gebäude werden die Netzwerke vorwiegend mit 100Base-TX realisiert. Für Backbones und Verbindungen zwischen Gebäuden werden häufig Glasfaserkabel verwendet. Ethernet wird heute unter anderem so häufig verwendet, da die benötigten Komponenten relativ billig sind. Ausserdem verdrängte dieser Standard im Office Bereich praktisch alle anderen Konkurrenzstandards, somit bleibt den Anwender praktisch nichts mehr anderes übrig, als auf Ethernet zu setzen. [2]

### 4.2.2 Optical Networks

Wie in Kapitel 4.2.1 schon erwähnt, werden Glasfaserkabel vor allem bei Backbones sowie in lokalen Netzwerken über grössere Distanzen verwendet. Optische Netzwerke haben drei wichtige Komponenten: Die Lichtquelle, das Übertragungsmedium sowie der Detektor. Die einzelnen Bits werden durch Lichtpulse (1) oder der Absenz von Licht (0) übermittelt. Das Übertragungsmedium besteht aus einer sehr dünnen Glasfaser. Die Lichtquelle wandelt elektrische Signale in optische Signale um. Der Detektor kehrt diesen Vorgang wieder um. Der grösste Vorteil von optischen Leitern, gegenüber von Kupferkabeln, ist die grössere Reichweite respektive die kleinere Dämpfung der Signale. Dies lässt sich durch die nahezu totale Reflektion des Lichtes innerhalb des Leiters erklären. Optische Leiter können so bei grossen Datentransferraten bis zu 100 km ohne Verstärkung eingesetzt werden. Ein weiterer Vorteil ist, dass auf derselben Glasfaser Licht in mehreren Frequenzen übertragen werden kann. Dadurch wird die Datentransferrate eines einzelnen Leiters massiv erhöht. Allerdings ist diese Technik für grössere Distanzen nicht geeignet, da es durch Laufzeitunterschiede zu Signalbeeinflussungen kommen kann. Es ist anzunehmen, dass die optischen Netzwerke in Zukunft an Bedeutung gewinnen. Ihre Rolle wird sich dann nicht mehr „nur“ auf Backbone- und Langstreckennetzwerke beschränken, sondern auch in normalen Büronetzwerken anzutreffen sein. [2] [22]

### 4.2.3 Frame Relay und ATM Networks

Frame Relay ist ein Netzwerktyp, der verbindungsorientiert, aber ohne Fehler- und Flusskontrolle arbeitet. Frame Relay ersetzte in den achtziger Jahren die damals verbreiteten X.25 Netzwerke. Da Frame Relay verbindungsorientiert arbeitet, ist die Paketreihenfolge

garantiert. Es wurde verwendet, um verschiedene lokale Netzwerke (LANs) miteinander zu verbinden. Frame Relay wird heute nicht mehr so häufig verwendet. [2]

Der Asynchronous Transfer Mode (ATM) wurde in den frühen neunziger Jahren entwickelt. Es entstand ein Rummel und es wurde gesagt, dass ATM ein Netzwerk sein werde, dass alles könne. ATM funktioniert, wie Frame Relay, verbindungsorientiert. Die Verbindungen werden bei ATM durch virtuelle Kanäle und virtuelle Pfade aufgebaut. Im Header der ATM Zellen werden die Virtual Path Identifier (VPI) und die Virtual Channel Identifier (VCI) abgelegt. Durch diese Angaben können die Switches Zellen mit denselben Sender und Empfänger auch denselben Pfad durch das Netzwerk zuweisen. Dies ist ein grosser Unterschied zwischen ATM und IP. Durch die VPIs, VCIs und die fixe Zellgrösse von 53 Byte (davon 48 Byte Nutzdaten) können die einzelnen Zellen speditiv von den Switches weitergeleitet werden. ATM erlaubt verschiedene Datentransferraten. Meistens wird 155 Mbps verwendet. Als Übertragungsmedien drängen sich vor allem Lichtwellenleiter auf. ATM funktioniert auch mit Kupferkabel. [2] [23] [4]

## 4.3 Metro Ethernet Services: Technische Übersicht

Ethernet Service ist heute weit verbreitet. Das Basismodell eines Ethernet Services wird in Abbildung 4.1 gezeigt. Diese Services haben viele Gemeinsamkeiten, aber auch ihre Unterschiede. Wie auch bei ADSL oder Internet über das Fernsehkabel werden Ethernet Services durch einen Provider angeboten, den Metro Ethernet Network Provider. Kunden Ausrüstungen (Customer Equipment (CE)) schliessen sich dabei an das Metro Ethernet Netzwerk über ein User-Network Interface (UNI) an. Wie auch das Standard LAN benutzt das Metro Ethernet Netzwerk die normalen, heute bekannten Geschwindigkeiten des Ethernets mit 10Mbps, 100Mbps, 1Gbps oder 10Gbps, bekannt von IEEE 802.3 und dort weitgehend standardisiert. Grundsätzlich ist das Metro Ethernet Network (MEN) die Verbindung zwischen zwei LANs. Mehrere MENs können sich über ein Wide Area Network (WAN) verbinden, um so nationale oder sogar internationale Netzwerke zu bilden. [12] [18]

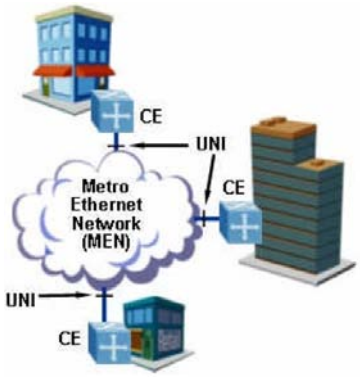



Abbildung 4.1: Basis Model [18]

Das Metro Ethernet besteht eigentlich aus zwei Welten. Die Basis besteht aus Standard LAN. Der zweite Teil sind Verbindungen, die Ethernet Virtual Connection, die das LAN zu privaten Verbindungen macht.

### 4.3.1 User Network Interface (UNI)

Das User-Network-Interface ist die Schnittstelle zwischen dem LAN des Subscribers und dem MEN des Providers. Hier werden die Aufgabenbereiche getrennt. Alles was von vor dem UNI kommt, ist die Angelegenheit des Subscribers, des Kunden, alles was nach dem UNI kommt befindet sich im MEN und ist Sache des Providers. Wie in Abbildung 4.2 gezeigt, gibt es die Klienten Seite und die Provider Seite des UNIs. Die Klienten Seite des UNIs, das UNI-C, gibt dem Subscriber die Möglichkeiten die er benötigt, um sich mit dem MEN zu verbinden, die Provider Seite des UNIs, das UNI-N, bietet alle Dienste, um das MEN mit dem Subscriber zu verbinden. Jedes UNI wird durch einen UNI Identifier eindeutig identifiziert. Diese ID ist ein String, der einzigartig ist. Ein Beispiel ist „ZH-IFI-H24-Port2“ was in Zürich das IFI Gebäude in Zimmer H24 am Port 2 bedeuten könnte. [15] [18] [17]

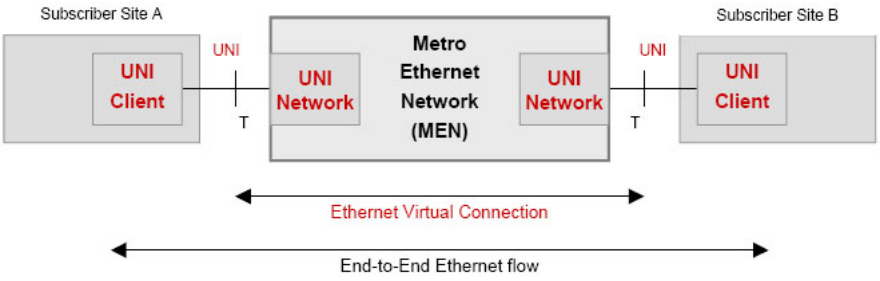



Abbildung 4.2: User-Network-Interface [15]

### 4.3.2 Ethernet Virtual Connection (EVC)

Der Hauptbestandteil des Ethernet Services ist die Ethernet Virtual Connection (EVC). Eine EVC ist durch das Metro Ethernet Forum als „eine Verbindung von zwei oder mehr User-Network-Interfaces“ definiert [14]. Ein Frame, welches in eine EVC geschickt wird, kann von einem oder mehreren UNIs, die am gleichen EVC angeschlossen sind empfangen werden, darf aber nicht wieder zurück zum Sender geschickt werden. Im weiteren darf kein UNI, das nicht mit dem gleichen EVC vebunden ist, dieses Frame empfangen. Ein Frame wird ohne Änderung von Ethernet MAC Adresse und Inhalt ausgeliefert, d.h. das Frame bleibt von Sender bis zum Empfänger intakt. Dies ist ein Unterschied zum normalen geroutetem Netzwerk, wo die Ethernet Frame Headers eventuell weggenommen und verworfen werden. Ein EVC wird durch ein Identifier (EVC ID) identifiziert. Diese ID ist im ganzen MEN eindeutig und wird nicht von Service Frame benutzt. Sie wird für Management und Kontrollzwecke benutzt. Ein Beispiel ist „EVC-0001234-ACME-IFI“ was die 1234. EVC im MEN bedeuten kann und der Subscriber ist das IFI. Grundsätzlich gibt es zwei Typen von EVCs, wie in Abbildung 4.3 dargestellt:

- Punkt-zu-Punkt (Point-to-Point)
- Multipunkt-zu-Multipunkt (Multipoint-to-Multipoint)

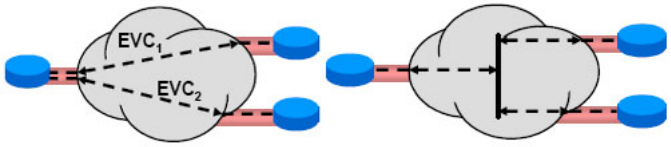



Abbildung 4.3: EVC Point-to-Point und EVC Multipoint-to-Multipoint Verbindung [14]

Bei der Punkt-zu-Punkt Verbindung schliessen sich genau zwei UNIs an ein EVC an, weitere UNIs können daran nicht angeschlossen werden. Sie kann somit als eine private Verbindung zwischen genau zwei LANs angesehen werden. Bei der Multipunkt-zu-Multipunkt-Verbindung schliessen sich zwei oder mehrere UNIs an ein EVC an. Hierbei wird ein Frame als Unicast, Broadcast oder Multicast versendet, je nach dem, wie die Ziel MAC Adresse lautet. [14] [18]

### 4.3.3 Ethernet Service Definition Framework

Um das Verständnis zu verbessern, hat das Metro Ethernet Forum das Ethernet Service Definition Framework erstellt. Mit Hilfe dieses Frameworks wird ein Ethernet Service erstellt. Jeder Ethernet Service besteht aus mindestens einem Ethernet Service Typen, aus einem oder mehreren Ethernet Service Attributen und einem oder mehreren Parameterwerten die mit den Serviceattributen verbunden werden. Abbildung 4.4 zeigt, wie so ein Ethernet Service aufgebaut ist.

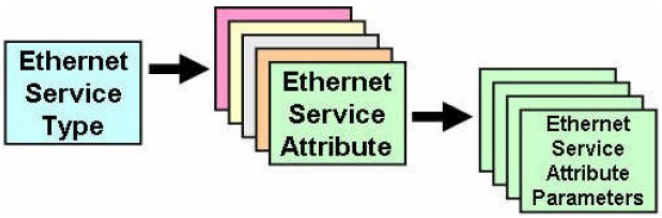



Abbildung 4.4: Ethernet Service Definition Framework [14]

Im Folgenden werden die wichtigsten Charakteristiken dieses Frameworks vorgestellt und anhand von kleinen Beispielen erläutert. [18] [14]

### 4.3.4 Ethernet Service Types

Die Ethernet Service Typen sind grundlegenden Servicekonstrukte, aus denen ein Ethernet Service definiert wird. Bis jetzt wurden zwei Service Typen definiert, Ethernet Line Service und Ethernet LAN Service. [14]

#### Ethernet Line Service Type

Der Ethernet Line Service, kurz E-Line Service, ist eine Punkt-zu-Punkt Ethernet Virtual Connection (EVC) zwischen zwei UNIs. Er wird gebraucht für Punkt-zu-Punkt Verbin-

dungen wie in Abbildung 4.5 gezeigt. In einem E-Line Service kommen immer nur zwei UNIs vor. Möchte man eine neue Verbindung zu einem anderen UNI aufbauen, wird auch ein neuer EVC benötigt.

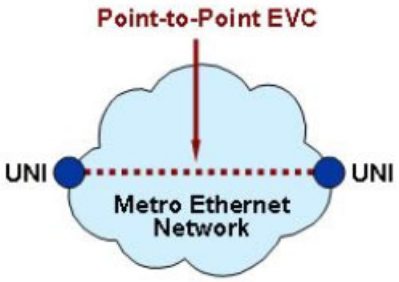



Abbildung 4.5: E-Line Service mit Punkt-zu-Punkt EVC [16]

Bei dieser Art der Verbindung gibt es eine Reihe von verschiedenen Servicen. Die einfachste Art des E-Line Services ist Daten mit symmetrischer Bandbreite in beiden Richtungen zu senden, ohne irgendeine versicherte Bandbreite zu haben, so z.B. Best Effort Service zwischen zwei UNIs mit 10Mbps. Die wichtigsten zwei Arten die hier erwähnt werden, sind die Ethernet Private Line und die Ethernet Virtual Private Line. Es existieren natürlich eine Vielzahl weiterer Services, die erstellt werden können, mit Variationen der Serviceattribute.

Die Ethernet Private Line benutzt ein Punkt-zu-Punkt EVC zwischen zwei UNIs. Sie garantiert eine hohe Transparenz für Service Frames und stellt hohe Ansprüche an Frame Jitter, Verzögerung und Verlust. Service Multiplexing ist nicht erlaubt. So wird z.B. EIR (siehe Kapitel 4.3.5) auf null gesetzt, um eine möglichst gute Verbindung zu erlangen. Die Ethernet Private Line ist vergleichbar mit einer Frame Relay Private Virtual Connection wie in Abbildung 4.6 gezeigt wird. Die Ethernet Virtual Private Line ist grundsätzlich mit der Ethernet Private Line übereinstimmend, bis auf ein paar wichtigen Ausnahmen. So wird z.B. Service Multiplexing erlaubt, was mehrere EVC an einem UNI ermöglicht. Zudem gibt es nicht volle Transparenz der Service Frames, da es mehrere EVCs an einem UNI geben kann. [16] [18]

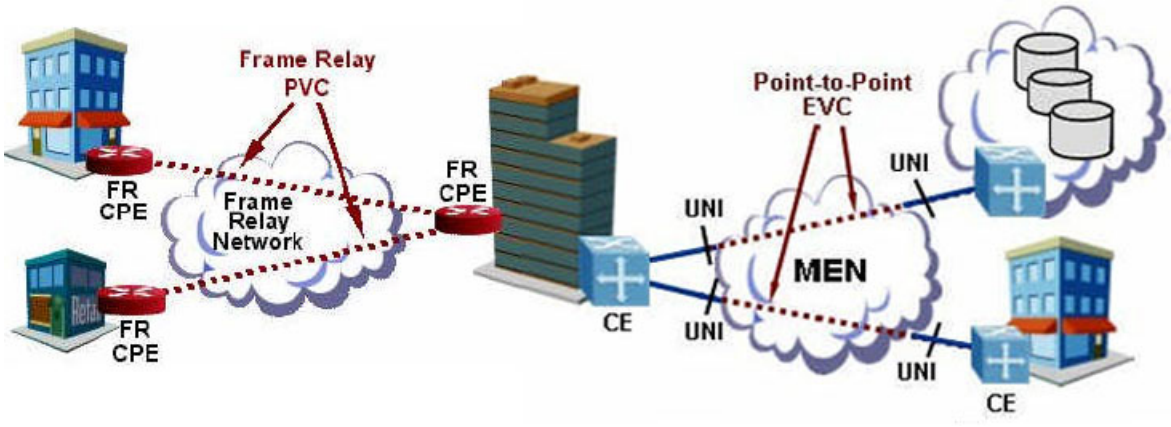



Abbildung 4.6: Frame Relay Analogie zu E-Line Private Line [18]

**Ethernet LAN Service Type**

Der Ethernet LAN Service, kurz E-LAN Service, basiert auf einem Multipunkt-zu-Multipunkt EVC, d.h. er kann zwei oder mehrere UNIs verbinden. Service Frames die von einem Subscriber via UNI an ein Multipunkt EVC gesendet werden, können von einem oder mehreren UNIs, die an diesem EVC angeschlossen sind, empfangen werden. Neue UNIs werden einfach an die bestehende Multipunkt EVC angeschlossen und sind dann fähig mit allen anderen UNIs Service Frames auszutauschen. Hierbei sieht der Subscriber das MEN wie ein LAN. Wie auch beim E-Line Service, gibt es beim E-LAN Service eine breite Palette an Servicen von Best Effort bis zu garantierten Bandbreiten. Service Multiplexing ist beim E-LAN Service möglich. So können E-LAN und E-Line Service über denselben UNI laufen. [16] [18]

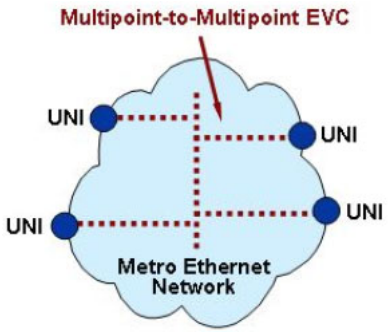



Abbildung 4.7: E-LAN Service mit Multipunkt EVC [16]

**Vergleich von E-Line und E-LAN Service**

Ein E-LAN Service kann auch eine Punkt-zu-Punkt Verbindung darstellen an der nur zwei UNIs beteiligt sind. Obwohl dies gleich erscheint, wie ein E-Line Serice, existieren markante Unterschiede. Beim E-Line Service muss, wenn ein neues UNI hinzugefügt wird, zu jedem anderen UNI auch eine neue EVC hinzugefügt werden, solange er mit allen anderen verbunden sein will. Analog wie beim Frame Relay ein neuer PVC zwischen allen hinzugefügt werden muss. E-LAN vereinfacht dies, indem er nur an die schon existierende Multipunkt EVC angeschlossen werden muss. Das neue UNI kann dann mit allen anderen UNIs kommunizieren, wohingegen es beim E-Line Service für jeden UNI eine neue separate EVC braucht. Somit benötigt es nur E-LAN Service mit einem EVC um eine Mehrfachverbindung zu erreichen. In Abbildung 4.8 wird das dargestellt. Damit ist er alternativen Servicen, wie ATM oder Frame Relay, weit überlegen.

### 4.3.5 Ethernet Service Attribute

Die Ethernet Service Attribute definieren die Fähigkeiten des Ethernet Service Typs. Manche spielen nur beim UNI eine Rolle, andere sind für die EVC wichtig, manche sind wichtig für beide.

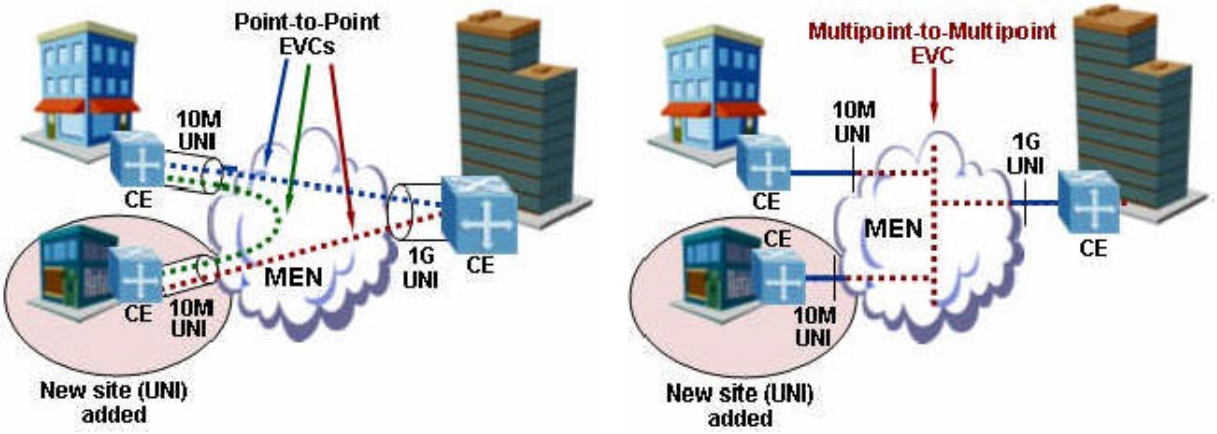



Abbildung 4.8: Hinzufügen eines UNI bei E-Line und bei E-LAN [18]

### UNI Service Attribute

Die physischen Attribute des UNIs sind die Geschwindigkeit, der Modus und das physische Medium. Die Standardgeschwindigkeiten an UNI sind 10Mbps, 100Mbps, 1Gbps und 10Gbps, die Ausarbeitung von 100Gbps ist im Gange. Das Modus UNI Service Attribut gibt Aussagen darüber, ob ein UNI Vollduplex oder Halbduplex unterstützt oder ob er automatisch die Geschwindigkeit erkennt. Das Physische Medium UNI Service Attribut spezifiziert die physische Schnittstelle, welche durch IEEE 801.3-2000 definiert wird. Es beinhaltet unter anderem 10BaseT, 100BaseT und 1000BaseSX. Das MAC Layer Service Attribut beschreibt welche Protokolle am UNI verarbeitet werden. Diese werden durch IEEE 802.3-2002 [8] spezifiziert. Weitere Attribute am UNI sind die Service Multiplexing Attribute, CE-VLAN Attribute und Bündelung Attribute auf die später noch eingegangen wird. [17]

### Bandbreiten Profile

Bandbreiten Profile geben Aussage darüber, wie gut ein Service ist. Anhand der Güte des Services ist es dem Provider möglich die Kosten dem Subscriber zu berechnen. Der Subscriber kann dabei aus einer breiten Palette von Profilen das für ihn passende auswählen und bekommt so genau den Service, den er benötigt. Verschiedene Profile erlauben dem Provider verschiedene Service an einem UNI anzubieten, jeder Service mit dem eigenen Bandbreiten Profil. Dies erlaubt ihm eine sehr hohe Flexibilität im Gegensatz zu anderen angebotenen Verbindungen. Die Bandbreiten Profile Service Attribute sind sowohl für das UNI, als auch für die EVC von Bedeutung. Das Bandbreiten Profil ist ein Limit mit welcher Datenrate Ethernet Frames einen UNI ansteuern können. Diese Profile können sehr verschieden sein für eingehenden und ausgehenden Verkehr. Das Metro Ethernet Forum hat folgende drei Bandbreiten Profile Service Attribute definiert, wie auch in Abbildung 4.9 dargestellt:

- Eingehendes Bandbreiten Profil pro eingehendem UNI

- Eingehendes Bandbreiten Profil pro EVC
- Eingehendes Bandbreiten Profil pro CoS Identifier

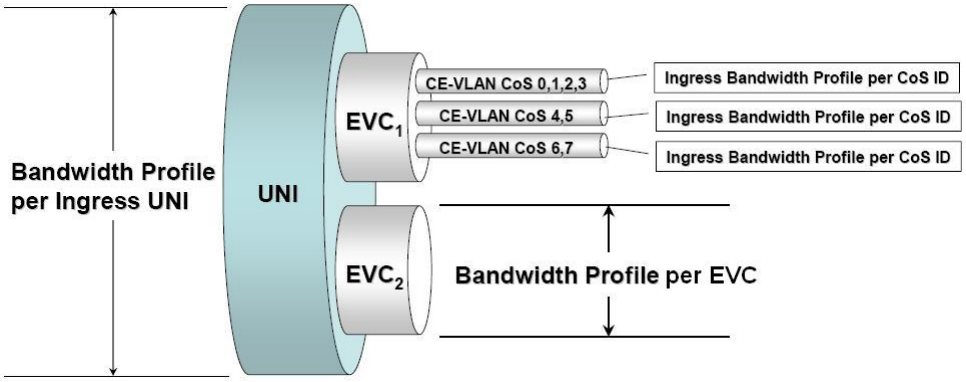



Abbildung 4.9: Bandbreiten Profile [19]

Das Bandbreiten Profil am eingehenden UNI bestimmt, mit welcher Rate Service Frames in ein UNI eingehen. Das Profil am EVC bestimmt, mit welcher Rate Service Frames in ein bestimmten EVC eingehen können. Es ist durchaus möglich, dass verschiedene EVC am UNI verschiedene Datenraten erlauben und somit auch verschiedene Bandbreiten Profile besitzen. Pro EVC können verschiedene CoS ID benutzt werden. Das Banbreiten Profile wird nun am EVC bestimmt durch die CoS ID. [19] [14] [18]

Das Bandbreiten Profil besteht aus sechs Verkehrsparametern <CIR, CBS, EIR, EBS, CF, CM>, welche die Service Farbe bestimmen . Die ersten vier Parameter werden später genauer vorgestellt. CF, das coupling Flag, hat nur 2 Werte, null oder eins. Es entscheidet über die Langzeit Durchschnittsrate der gelben Service Frames. Ist es auf null gesetzt, so ist das Maximum EIR und wenn auf eins EIR + CIR abhängig von den grünen Frames. CR ist der Color Mode. Auch dieses Attribut kann zwei Werte haben, „color-aware“ und „color-blind“. Die Service Farbe bestimmt schliesslich ob das Service Frame weitergeleitet wird oder ob es entfernt wird.

### Service Frame Farbe

Die Service Farbe eines Frames ist ein einfacher Weg, um über das Weiterleiten eines Frames zu entscheiden. Sie wird benutzt um zu entscheiden, ob ein Frame noch mit dem Bandbreiten Profil übereinstimmt oder nicht. Es gibt hier drei Farben, „grün“, „gelb“ und „rot“. Grün bedeutet, dass ein Service Frame noch mit dem Bandbreiten Profil übereinstimmt. Ein Frame wird gelb markiert, wenn es nicht mehr mit dem Bandbreiten Profil übereinstimmt, aber noch mit der Überflussrate des Profils übereinstimmt. Schlussendlich wird ein Frame rot markiert, wenn es nicht mehr in das Profil passt.

Die Farbe bestimmt, wie ein Servie Frame behandelt wird. Grüne Frames werden wie im Bandbreiten Profil spezifiziert versendet und in der Regel nicht entfernt. Gelbe Frames werden normalerweise auch nicht sofort entfernt. Je nach Auslastung und Bedingungen im Netzwerk werden sie aber nicht mehr mit der gleichen Performance versendet. Rote

Frames sind schlussendlich nicht mehr im Profil und werden sofort entfernt. Die Service Farbe wird durch Bandbreiten Profilparameter (CIR, CBS, EIR, EBS) bestimmt. [19]

### CIR und CBS

Die durchschnittliche Datenrate, bis zu welcher Service Frames ausgeliefert werden anhand von Performance Parametern (Jitter, Verzögerund, etc.), heisst garantierten Übertragungsgeschwindigkeit oder Committed Informaiton Rate (CIR). CIR ist eine durchschnittliche Rate, weil alle Servie Frames in der Geschwindigkeit des UNI gesendet werden, also z.B. 100Mbps und nicht wie CIR z.B. 1Mbps. Die Committed Burst Size (CBS) gibt an, bis zu welcher Datenmenge hin die Service Frames gesendet werden und immer noch CIR-übereinstimmend sind.

Service Frames welche eine Datenmenge höher als CBS haben, sind nicht mehr CIR-übereinstimmend und werden entfernt oder mit der entsprechenden „Farbe“ als nicht CIR-übereinstimmend markiert.

Die CIR kann tiefer oder gleich der Datenrate des UNI sein, wobei bei multiplen Bandbreiten die Summe aller CIRs tiefer oder gleich sein muss, wie die Datenrate des UNIs. CIR = 0 würde bedeuten, dass es keine Garantien gibt und dies würde „Best Effort“-Service bedeuten. CIR-übereinstimmende Service Frames werden wie beim Bandbreiten Profil spezifiziert ausgeliefert. [19] [18]

### EIR und EBS

Die kurzzeitige Überschreitung der Übertragungsgeschwindigkeit (Excess Information Rate (EIR) ) beschreibt die durchschnittliche Datenrate die grösser oder gleich CIR ist und bis zu der Service Frames übertragen werden ohne Performance Parameter. Auch diese ist eine durchschnittliche Geschwindigkeit, da das UNI mit seiner Datenrate von z.B. 100Mbps sendet und nicht wie EIR z.B. nur mit 10Mbps.

Die Excess Burst Size (EBS) gibt an, bis zu welcher Datenmenge hin die Service Frames noch EIR-übereinstimmend sind. Hier werden wiederum Service Frames die mit einer höheren Datenmenge als EBS gesendet werden entfernt oder als nicht EIR-übereinstimmend markiert.

EIR ist kleiner oder gleich der Datenrate des UNI und grösser oder gleich CIR. EIR-übereinstimmende Service Frames können ausgeliefert werden, jedoch nicht mit der spezifizierten Performance. [19] [18] In Abbildung 4.10 wird eine Übersicht gegeben, wie Frames markiert werden.

### Farbbestimmung mit Token Bucket Algorithmus

Die Service Farbe wird durch einen Token Bucket Algorithmus bestimmt. Zwei Token Buckets hintereinander bestimmen die Farbe. Der erste Token Bucket behandelt CIR-übereinstimmende Datenraten, der zweite behandelt EIR-übereinstimmende Datenraten.

| Conformance | Color | Service Frame Delivery |
|---|---|---|
| CIR Conformant |  | Service Frames green and delivered per the performance objectives specified in the SLA/SLS. |
| EIR Conformant |  | Service Frames are yellow and may be delivered but with no performance assurances. |
| None |  | Service Frames are red and dropped. |

Abbildung 4.10: Übersicht der Service Farben [19]

Am Anfang ist der Token Bucket voll von „Tokens“. Solange er Tokens beinhaltet, werden Frames durchgelassen und als grün markiert. Dabei werden Tokens verbraucht. Ist der erste Bucket verbraucht kommt der zweite an die Reihe, der über EIR-übereinstimmung entscheidet. Sind immer noch Tokens vorhanden, werden diese als gelb markiert und in das MEN gesendet. Falls keine Tokens mehr vorhanden sind, wird das Frame als rot markiert und entfernt. Tokens werden mit einer gewissen Rate (CIR oder EIR, je nach Bucket) wieder aufgefüllt, so dass sie mit dem Bandbreiten Profil übereinstimmen. In Abbildung 4.11 wird das bildlich veranschaulicht. [19]

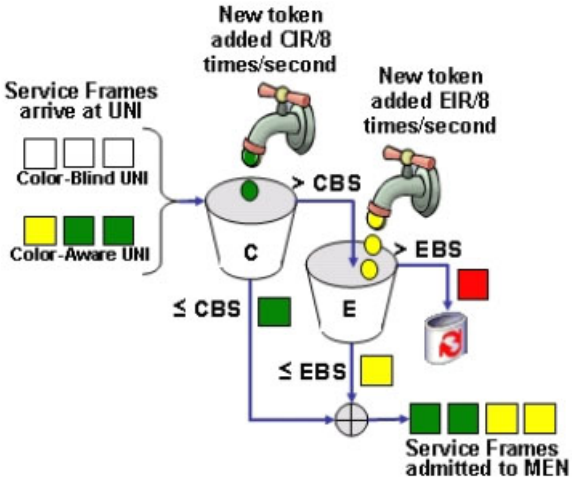



Abbildung 4.11: Token Bucket Algorithmus [19]

### Performance Parameter

Die Performance Parameter beschreiben die Servicequalität die ein Subscriber erfährt. Sie werden einem EVC zugeordnet. Es existieren drei Performance Parameter. Wenn diese definiert werden, müssen sie für alle Service Frames angewendet werden, die mit der Farbe grün markiert sind, nicht aber für jene, die mit gelb oder rot markiert sind. Alle Performance Parameter werden als CoS Attribute gebraucht. All diese Eigenschaften können auf Punkt-zu-Punkt Verbindungen angewendet werden. Die Definition dieser Attribute für Multipunkt Verbindungen werden noch spezifiziert. [17]

### Frame Verzögerung

Die Verzögerung ist ein wichtiger Parameter und hat vor allem Einfluss auf Real-Time Applikationen. Eine kleine Verzögerung muss nicht von Bedeutung sein, doch z.B. beim Telefonieren machen schon kleine Verzögerungen den anderen Teilnehmer unverständlich (National: 25ms, International 100ms bei Telefon, Bei IP-Telephonie 500-700ms) [25]. Die Verzögerung kann in drei Teil aufgeteilt werden. Die Verzögerung von jeweiligen UNI bei Sender oder beim Empfänger und die Verzögerung des MEN. Diese Verzögerung hängt vom jeweiligen Service Provider ab. Die gesamte Verzögerung wird von ersten Bit das eingeht, bis zum letzten Bit das übertragen wird, gemessen. In Abbildung 4.12 wird dies durch A, B und C dargestellt, wobei A+B von UNI abhängig sind und C vom Provider.

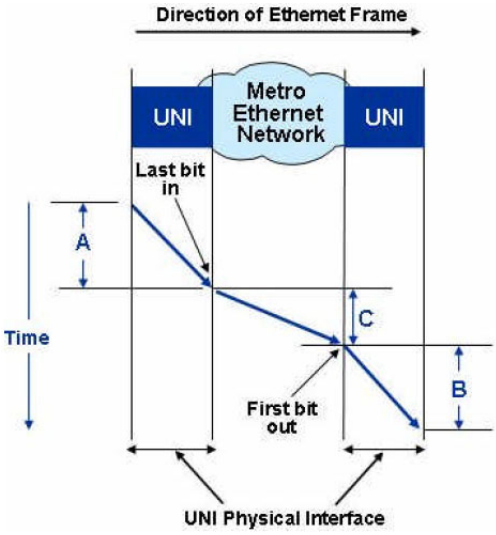



Abbildung 4.12: Teilung der Verzögerung [19]

Frame Verzögerung ist definiert als die maximal gemessene Verzögerung für einen Prozentsatz an erfolgreich übertragenen CIR-übereinstimmenden (grün) Service Frames über ein bestimmtes Zeitinterwall. Zum Beispiel 95% von 1000 Service Frames wurden mit einer Verzögerung von 10ms ausgeliefert. Generell ist der Prozentsatz 95% oder höher basierend auf dem Industriestandard.

### Frame Jitter

Jitter ist die Variation der Verzögerung. Er ist vor allem wichtig für IP-Telephonie und IP-Video, welche einen tiefen und begrenzten Jitter benötigen. Für Non-Real-Time Applikationen spielt Jitter kaum eine bedeutende Rolle. Berechnet wird Jitter mit [17]:

$$Frame\,Jitter = Frame\,Verzögerung - Frame\,mit\,der\,tiefsten\,Verzögerung\,der\,Messung$$

### Frame Verlust

Der Frame Verlust ist der Verlust an CIR-übereinstimmenden (grün) Service Frames gemessen zwischen zwei UNIs über einen bestimmten Zeitraum. Gemessen wird der Verlust

in Prozent.

$Frame\,Verlust = \left(\frac{Gesendete\,Frames - Angekommene\,Frames}{Gesendete\,Frames}\right)$

Der Effekt von Frame Verlusten hat verschiedene Einflüsse auf QoS, abhängig von Applikation, Service oder Protokolle die benützt werden.

### Class of Service Indentifiers

In Metro Ethernet Netzwerken können verschiedene Serviceklassen angeboten werden. Sie werden durch verschieden Serviceklassen ID (CE-VLAN CoS IDs) identifiziert. Jede Serviceklasse hat verschiedene Parameter, welche verschiedene Performance bringt (CIR, EIR, usw. für das UNI und Jitter, Delay, usw. für den Service). Der Subscriber kann selber wählen welche Klasse die für ihn besten ist.

### Physischer Port

Existiert nur eine Serviceklasse pro physischen Port, erhält aller Datenverkehr dieselbe Serviceklasse, was unflexibel ist und dem Subscriber Kosten verursacht. Für verschiedene Serviceklassen würden verschiedene Ports benötigt.

### CE-VLAN CoS (802.1p)

CE-VLAN CoS ist ein Teil des 802.1Q Tags. Es identifiziert die User Priorität. In der CE-VLAN Serviceklasse existieren Serviceklassenbits (802.1p). Dadurch werden bis zu acht Serviceklassen definiert, die durch den Provider definiert werden. Die Serviceklassen können auf verschiedenen Prioritäten basieren, so wird z.B. ein Klasse acht Frame eher weiter geleitet als ein Klasse zwei Frame.

### DiffServ / IP TOS Werte

Differentiated Service oder IP Type of Service Werte können benutzt werden um die Serviceklasse zu bestimmen. IP ToS hat dabei acht verschiedene Serviceklassen. DiffServ benutzt das zweite Byte im IP Kopf, also das IP ToS Feld. Es basiert auf so gennanten Per-Hop-Behaviors (PHB). DiffServ hat 64 verschiedene Werte, die so genannten DiffServ Codepoints (DSCP) um die Serviceklasse zu definieren. Die interessantesten Klassen sind Expedited Forwarding (EF) für tiefe Verzögerung und tiefen Verluste und Assured Forwarding (AF) mit vier Klassen für weniger anspruchsvolle Anwendungen. Mindestens der erste und der letzte Router der Verbindung muss DiffServ, IP ToS oder 801.2p kennen, um die Klasse zu finden. Serviceklassen EVC Attribute definieren die Serviceklasse mit folgenden Parametern:

- Class of Service Identifier

- Frame Verzögerung
- Frame Jitter
- Frame Verlust

### Service Frame Delivery

Eine EVC verbindet zwei UNI um Frames zwischen ihnen auszutauschen. Einige sind Subscriber Datenframes andere Ethernet Kontroll Serviceframes. Der Provider spezifiziert die Frames die ausgetauscht werden können und welche nicht. Es gibt drei Arten Services Frames zu versenden.

- Unicast Service Frame Delivery
- Multicast Service Frame Delivery
- Broadcast Frame Delivery

### Layer 2 Kontroll Protokoll Verarbeitung

Dieses Serviceattribut kann am UNI oder am EVC benutzt werden. Diese Layer 2 Protokolle können von Provider akzeptiert, getunnelt oder verworfen werden.

### VLAN Tag Unterstützung

Service Frames können ein 802.1Q Tag besitzen. Diese Tag wird als Customer Edge VLAN Tag bezeichnet. Der Teil des Tags, welcher User Prioritäten enthält, wird als CE-VLAN CoS bezeichnet, der Teil, der das VLAN identifiziert heisst CE-VLAN ID. Die EVC, in welches ein Service Frame geschickt wird, muss durch eine CE-VLAN ID identifiziert werden. Es ist auch möglich, dass mehrere CE-VLAN IDs auf ein EVC zeigen.

Service Frames können Tags benutzen oder nicht und UNIs können diese verstehen oder nicht. Für UNIs, die VLAN Tags benutzen, muss der Subscriber wissen, wie diese zu benutzen sind. Sowohl Subscriber als auch Provider können VLAN Tags benutzen. Es ist möglich ein zweites VLAN Tag in das Subscriber Service Frame einzufügen (Q-in-Q), wie es auch möglich ist, eine MAC Adresse einzufügen (MAC-in-MAC). Um diese zu unterscheiden, wird eine CE-VLAN ID eingeführt, welche den Subscriber identifiziert.

Es existieren zwei CE-VLAN Preservation Service Attribute:

- CE-VLAN ID Preservation
- CE-VLAN CoS Preservation

Die Preservation beschreibt die Beziehung zwischen eingehendem und ausgehendem Service Frame. Es ist durchaus Möglich, dass ein EVC ein UNI besitzt, der mehr als ein CE-VLAN ID besitzt. In diesem Fall muss das ID Preservation Tag gesetzt sein. Die CE-VLAN CoS Preservation gibt eine Aussage darüber, ob ein CE-VLAN CoS Tag z.B. 802.1p Bits, auf dem EVC modifiziert worden ist oder nicht. Ist das CE-VLAN CoS Preservation Attribute gesetzt, so darf sich CoS Tag nicht verändert werden.

### Mapping VLAN IDs

Wenn ein UNI Tags unterstützt und der andere nicht, müssen die CE-VLAN ID gemapped werden. Die CE-VLAN ID/EVC Map ist eine Sammlung von CE-VLAN ID die auf EVCs verweist. Jedes UNI muss einen Verweis von allen IDs auf ein EVC haben. Hat ein Service Frame eine ID die auf kein EVC zeigt, so wird es umgehend entfernt. Die ID muss nicht global sein und kann auch nur an einem UNI eine Bedeutung haben.

Eine zweite Map existiert, welche die UNIs beinhaltet, die an einem EVC angeschlossen sind. Diese Liste enthält zwei Einträge pro EVC für E-Line Service und zwei oder mehrere für E-LAN Service. Unterstützt ein UNI Tags und der andere nicht, werden diese vom Provider entfernt oder hinzugefügt. Alle möglichen Kombinationen werden in Abbildung 4.13 dargestellt. [17] [18]

| | VLAN Tag Unterstützung | | |
|---|---|---|---|
| **UNI Capability** | **Untagged** | **Tagged** | **Tagged / Untagged** |
| VLAN tags verboten | v | N/A | N/A |
| VLAN tags mapped | v | v | v |
| VLAN tags preserved | N/A | v | v |

Abbildung 4.13: VLAN Tag Unterstützung am UNI [18]

### Service Multiplexing

Service Multiplexing Service Attribute werden gebraucht um multiple EVC an einem UNI zu unterstützen. Die Vorteile sind, dass nur ein UNI (physisches Interface) benötigt wird um mehrere EVC zu unterstützten, was dem Subscriber Kosten erspart, denn er benötigt weniger Router oder Switches und kann die Ausnützung der Ports maximieren. Ein weiterer Vorteil ist, dass der Subscriber weniger Platz für Server, weniger Strom und weniger Verkabelung benötigt. Neue Services können viel einfacher hinzugeschaltet werden. Abbildung 4.14 zeigt wie verschiedene EVCs an einem UNI benutzt werden. [17] [18]

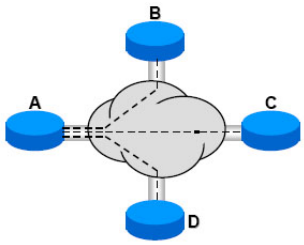



Abbildung 4.14: Service Multiplexing am UNI A [17]

### Bündelung

Benutzt ein UNI das Bündelung Service Attribut, muss er so konfiguriert werden, dass eventuell mehrer CE-VLAN IDs auf ein EVC zeigen. Wenn ein EVC mehrere CE-VLAN IDs hat, muss auch das CE-VLAN ID Presevation Attribut gesetzt sein und die Liste der IDs die auf die EVC zeigen muss bei allen UNIs gleich sein. Zeigen mehr als eine CE-VLAN ID auf ein EVC, so müssen Subscriber und Provider die CE-VLAN IDs, die am UNI gebraucht werden, absprechen, um sie spezifischen EVCs zuzuordnen. Ein Beispiel von Bündelung wird in Abbildung 4.15 gezeigt.

| UNI A | |
|---|---|
| **CE-VLAN ID** | **EVC** |
| 47,48,49 | $EVC_1$ |
| 113 | $EVC_3$ |

| UNI B | |
|---|---|
| **CE-VLAN ID** | **EVC** |
| 47,48,49 | $EVC_1$ |
| 1 | $EVC_2$ |

| UNI C | |
|---|---|
| **CE-VLAN ID** | **EVC** |
| 1 | $EVC_2$ |
| 47 | $EVC_3$ |

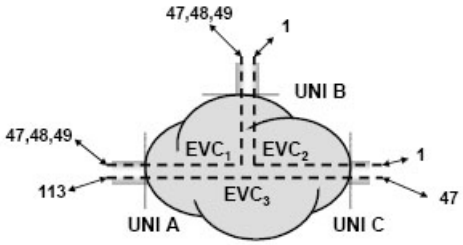



Abbildung 4.15: Bündelung [17]

### Sicherheits Filter

Provider können dem Subscriber erlauben, zusätzliche Sicherheitsfilter hinzuzufügen. Ein Beispiel ist eine Kontrollliste der MAC Adressen, welche an einem UNI erlaubt sind. Alle Frames von anderen Adressen werden vom Provider entfernt.

## 4.4 Einschränkungen und Möglichkeiten von Metro Ethernet

In diesem Kapitel gehen wir auf technische Einschränkungen und Möglichkeiten von Metro Ethernet näher ein. Dabei wird aufgezeigt, dass ein MEN, neben allen Vorteilen auch

gewisse Nachteile hat, aber es bietet den Benutzern auch neue Wege, ihre Kommunikation zu gestalten. Besonders für Firmen sind diese interessant.

### 4.4.1 Einschränkungen

Was für Einschränkungen bringt ein MEN mit sich? Vor allem im Bereich des QoS sind noch nicht alle Probleme gelöst. Es gibt aber auch schwache Schutzmechanismen bei Ausfällen einzelner Leitungen und ein nicht optimales In-Service OAM.

#### Ende-zu-Ende Quality of Service Garantien

Es stellt sich die Frage, wie in Metro Ethernet die Qualität der Ende-zu-Ende Verbindungen sichergestellt werden kann. Dabei sind verschiedene Probleme zu berücksichtigen. Zum einen stellt sich die Frage, was passiert, wenn bei einer stark ausgelasteten Verbindung ein neue Verbindung mit hohen QoS-Anforderungen aufgebaut werden soll. Auch muss in solchen Fällen ein fairer Zugang bei konkurrierenden Verbindungen sichergestellt werden. Weiter ist sicherzustellen, dass die Datenströme über den optimalen Pfad (Spanning Tree Algorithmus) durch das Netzwerk geleitet werden. Auch die Umsetzung von Differentiated Services, insbesondere die Paketfärbung, ist noch problematisch. Es gibt verschiedene Lösungen um die QoS Garantien umsetzen zu können. Die einfachste, aber auch die teuerste, wäre einfach genug Bandbreite zur Verfügung zu stellen. Da diese Lösung ganz klar nicht wirtschaftlich ist, wird sie sich auch nicht durchsetzen können. Ein weiterer Ansatz liegt im Multiprotocol label switching (MPLS). Der MPLS Header besteht aus vier Feldern (Label, QoS, S und TTL), welche insgesamt 32 bit lang sind. Damit können den Routern bestimmte Informationen zur Behandlung der Daten mitgegeben werden. Bei MPLS wird mit dem Label Feld gearbeitet, anhand dessen die Router die Daten weiterleiten können. [11] [2]

#### Schutzmechanismen

Ethernet hat schlechte Schutzmechanismen, die in Kraft treten, wenn das Netz an einer Stelle unterbrochen wird. Das liegt daran, dass der verwendete Spanning Tree Algorithmus sehr langsam bei der Fehlererkennung ist. Im Gegensatz zu den verwendeten Techniken bei der Synchronous Digital Hierarchy (SDH) ist es beim Ethernet möglich, das einzelne Knoten mehrere Sekunden nicht erreichbar sind, obwohl redundante Leitungen existieren würden. Um dem entgegen zu wirken, kann auf mehrere Spanning Trees (Multiple Spanning Trees, IEEE 802.1s) im Netzwerk gesetzt werden. Allerdings sind das dann keine minimale Spanning Trees mehr. Es gibt weitere Lösungsansätze für dieses Problem, wie Rapid Reconfiguration Spanning Tree (IEEE 802.1w), Link Aggregation (IEEE 802.3ad), Resilient Packet Ring (IEEE 802.17) und MPLS. [11]

#### In-Service Operations, Administration and Maintenance (In-Service OAM)

Beim Ethernet existieren, im Gegensatz zu SDH, kaum Möglichkeiten, das Netzwerk bezüglich Bit Error Raten zu überwachen. Diese Möglichkeiten wären teilweise nützlich, um die Erreichbarkeit einzelner Komponenten zu testen. Verschiedene Gremien (IEEE, MEF, ITU-T) haben sich diesem Thema angenommen und eine Arbeitsgruppe der IEEE spezifiziert einen Frame basierten Ansatz, während MEF und ITU-T einen Weg über Ende-zu-Ende In-Service OAM wählen. [11]

#### Skalierbarkeit und Netzwerk Ressourcenbelegung

Da Ethernet nur eine begrenzte Anzahl VLAN Tags anbietet, kann es dadurch zu grossen Einschränkungen für die Provider kommen. Um dieses Problem zu umgehen, setzten einige Gerätehersteller auf proprietäre Tags für die VLANs, die mehr virtuelle Netze zulassen. Hier zeichnen sich aber neue Probleme ab, zum Beispiel, wenn Geräte verschiedener Hersteller zusammen arbeiten sollten. [11] Weitere Probleme zeichnen sich auch hier bei der Verwendung des Spanning Tree Algorithmus ab. Durch den Spanning Tree Algorithmus können Flaschenhalse entstehen, da nicht alle Verbindungen benutzt werden. Hier werden Lösungen diskutiert, die auf MPLS Verfahren basieren. [11]

### 4.4.2 Möglichkeiten

Neben den Einschränkungen, welche im vorherigen Kapitel behandelt wurden, bietet Metro Ethernet auch neue Möglichkeiten. Einige davon werden in diesem Kapitel kurz beschrieben.

#### Dedicated Internet Access

Im Gegensatz zu den heute gängigen Internetanschlüssen über das Fernsehkabel kann mit Metro Ethernet ein dedizierter Anschluss zu einem Internet Service Provider (ISP) gemacht werden. Dies geschieht meistens über ein point-to-point E-Line Service. Durch den Einsatz mehreren EVCs kann ein User auch Anschlüsse zu mehreren ISPs über dasselbe UNI benutzen. Auf der Seite des ISP wird meistens Service Multiplexing eingesetzt, um die Kunden über ein schnelles UNI zu bedienen. [18]

#### LAN Extension

Mit Hilfe der LAN Extension können mehrere Standorte einer Firma zu einem LAN zusammengefasst werden. Bei zwei Standorten wird üblicherweise point-to-point E-Line verwendet, bei mehr als zwei Standorten E-LAN oder multiple E-Line. Eine LAN Extension muss relativ transparent sein, damit der Kunde eigene Dienste über die LAN Extension laufen lassen kann oder wenn er für verschiedene Abteilungen verschiedene VLAN Tags benutzen will. [18]

**Intranet / Extranet L2 VPN**

EVCs haben gegenüber den IP (Level 3) basierten VPNs einige Vorteile. Die IP VPN Geräte sind komplexer und teurer als die Verwendung von EVCs. Ausserdem bieten die EVCs eine bessere Performance und unterstützen grosse Bandbreiten.[1] Diese Vorteile machen sich insbesondere dann bemerkbar, wenn ganze Applikationen outgesourct werden. [18]

## 4.5 Verwendete Geräte

Sind für ein MEN vollkommen neue Geräte notwendig oder funktioniert es auch mit den herkömmlichen Mitteln? Je nachdem, ob die Geräte beim User oder beim Provider stehen, fällt die Antwort unterschiedlich aus.

### 4.5.1 End-User Geräte

Im Heim- oder Büronetzwerk können grundsätzlich die bisherigen Ethernetgeräte (Netzwerkkarten, Switches, etc.) verwendet werden. Dies gilt als grosser Vorteil von Metro Ethernet, da die bisherigen Geräte weit verbreitet, günstig und standardisiert sind.

### 4.5.2 User Provider-Edge

Um den Zugang zum Metro Ethernet zu erhalten, muss ein Gerät installiert werden, dass die „user provider-edge“ Rolle einnimmt. Dieses Gerät, wird typischerweise bei den Benutzern installiert, aber von dem Provider verwaltet. [6]

### 4.5.3 Provider-Edge Aggregation

Diese Geräte sind optional und kommen nur bei grossen Netzwerken zum Einsatz. Sie stellen die Verbindung zwischen dem Benutzer und dem eigentlichen Kernnetz dar. Diese Geräte fassen den Verkehr zusammen und kümmern sich um das Multiplexing und die Staukontrolle. [6]

### 4.5.4 Network Provider-Edge

Die hier verwendeten Geräte stellen sicher, dass die VPLS, MPLS und EoMPLS auf die richtigen Ziele gemappt werden. Diese Geräte stellen also die Verbindung zum Kernnetzwerk (Metro Core) des Providers sicher. [6]

[1] Das Magazin c't hat in [1] ein neues Gerät von der Firma Safenet vorgestellt, welches auf der Schicht 2 die Verbindung verschlüsselt und so gegenüber IPSec weniger Overhead produziert und somit bei den Traffic Kosten spart.

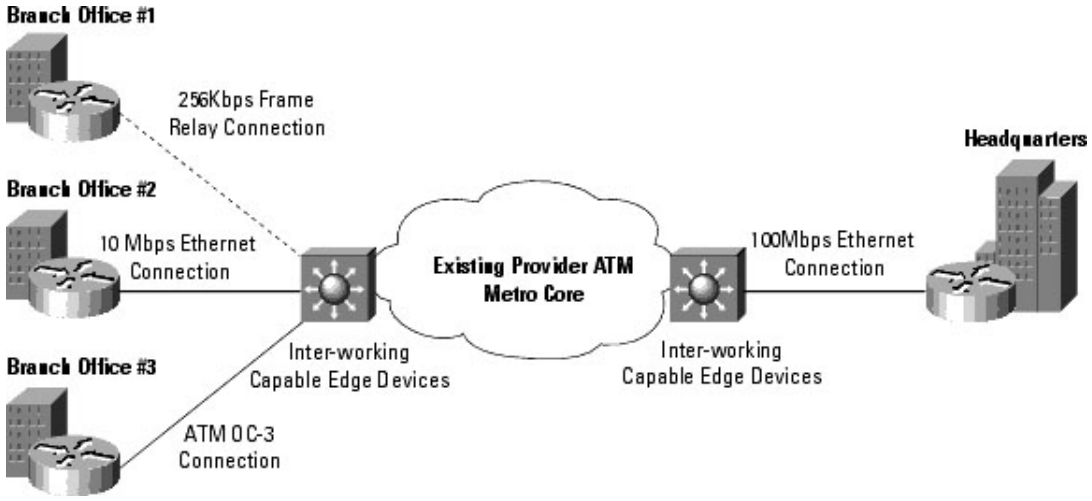



Abbildung 4.16: Metro Ethernet Schema für eine Firma mit mehreren Filialen [13]

## 4.6 Beispiele

In diesem Teil gehen wir der Frage nach, wo MENs bereits im Einsatz stehen und für welche Zwecke sie verwendet werden. Cisco hat im Bereich MEN viel geleistet und kann schon einige erfolgreiche Projekte aufzeigen.

### 4.6.1 Cisco-Metro-Ethernet-Services

Da die herkömmlichen Telefonleitungen bald an ihre Grenzen stossen, hat Cisco im Jahr 2002 das Projekt „Ethernet-to-the-X“ vorgestellt. Damit sollen in Ballungsräumen Haushalte und KMUs mit bis zu 1 Gbps Bandbreite per Glasfaserkabel ans Internet angeschlossen werden. Zuerst plante Cisco die letzte Meile durch einen „fundamental shift“ auf Ethernet umzustellen. Allerdings bringen die vorhandenen Telefonkabel ziemlich schlecht Voraussetzungen dafür mit. Cisco sah sich gezwungen, für seine Metro-Ethernet-Services auf Glasfaserkabel zu setzen. In Hamburg wurde beispielsweise für die kommunalen Behörden ein Netz entwickelt, dass die einzelnen Standorte mit 100 Mbps bis 10 Gbps verbindet. [3]

### 4.6.2 Fastweb

Fastweb (`http://www.fastweb.it`) ist ein Internet Service Provider in Italien, der seit einiger Zeit, vor allem im Grossraum Mailand, schnelles Internet, Voice over IP Telefonie und Fernsehen über dasselbe Glasfaserkabel anbietet. [7] [17]

Fastweb ist in der Lage, das Angebot mit diversen zusätzlichen Diensten, wie Video-on-Demand, auszustatten.[2]

[2] In der Schweiz unternahm die Swisscom-Tochter Bluewin einen ähnlichen Versuch. Da die hier üblichen ADSL Leitungen nicht optimal für TV und Video-on-Demand sind, musste das Projekt StreamIt wieder eingestellt werden. Bluewin plant aber in Zukunft Fernsehen über das Telefonkabel anzubieten

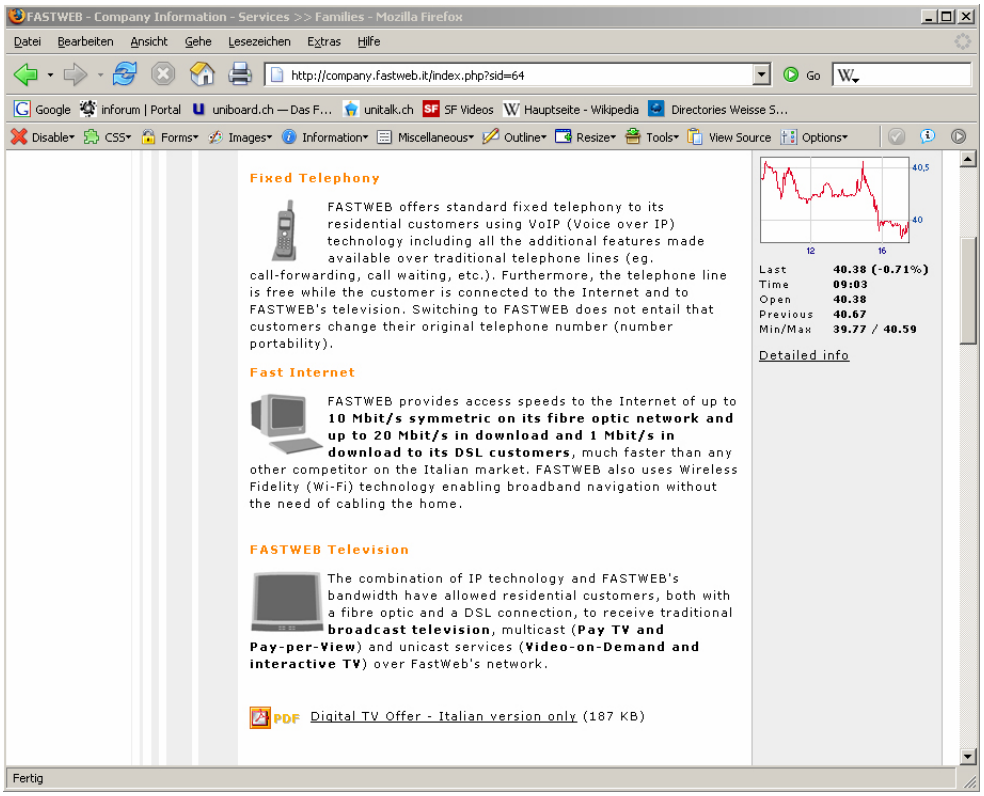



Abbildung 4.17: Das aktuelle Angebot von Fastweb [7]

### 4.6.3 Telstra

Telstra (`http://www.telstra.com`) bietet Bandbreite nach Nachfrage an. Die Kunden können ihre Bandbreite über die Firmenwebsite ihren Bedürfnissen anpassen. Somit können die Kunden flexibel auf Veränderungen reagieren und so nur die (höhere) Bandbreite bezahlen, wenn sie sie wirklich brauchen. Dieses System kann nützlich sein, wenn zum Beispiel externe Backups nach einem Ausfall des Servers, dringend wieder zurückgespielt werden müssen. [3]

### 4.6.4 Zukunft

Es gibt zahlreiche weitere Projekte, die, vor allem mit den Cisco-Metro-Ethernet-Services, in diversen Städten ähnliche Netzwerke, wie die oben vorgestellten, realisieren. Cisco sieht für die Zukunft die Stromversorgern gegenüber den Telekommunikationsfirmen im Vorteil, da diese bereits Kabelschächte besitzen und es damit leicht wird, Glasfaserkabel direkt in die einzelnen Häuser zu legen. [3]

## 4.7 Marktsituation Metro Ethernet

Wenn man Metro Ethernet betrachtet, stellt sich neben den technischen Eigenschaften dieses Metropolitan Area Networks auch die Frage, was diese Annäherung als Alternative der Versorgung der letzen Meile wirklich bringt. Im vorigen Kapitel wurden Aspekte der Bandbreite in der letzen Meile angesprochen. In diesem Kapitel soll näher auf den momentanen Versorgungsgrad durch die Telekomanbieter sowie die Bedürfnisse der Verbraucher eingegangen werden. Auch wird die „Blackbox Metro Ethernet“ näher angeschaut.

### 4.7.1 Ist-Zustand

Eine Übersicht der heute für den Endverbraucher zur Verfügung stehenden Bandbreiten in Europa (Down-/Uploadraten):

- ADSL/2 (25/3 Mbps)
- SDSL (2.3/2.3 Mbps)
- VDSL/2 (54/100+ Mbps)

#### Schweiz

In der Schweiz stehen ADSL und SDSL, sowie weitere Angebote durch regionale Kabelnetzbetreiber mit bis zu ungefähr 10 Mbps Downloadrate zur Verfügung. In der Anbindung über zweidraht Kupferkabel will Swisscom, welche immer noch über die letzte Meile in der Schweiz verfügt, das Netz bis 2007 auf VDSL mit Bandbreiten bis zu 13 Mbps aufrüsten. Die Kabelnetzbetreiber haben ein Glasfasernetz zur Verfügung, mit welchem sie der Konkurrenz punkto Bandbreitengeschwindigkeiten überlegen wären. Da aber seitens der ADSL/VDSL Anbieter noch kein höherer Konkurrenzdruck entstanden ist, warten die Kabelnetzbetreiber anscheinend noch mit dem Anbieten höherer Bandbreiten. [21]

#### Andere Gebiete

In Asien gibt es Angebote, welche die Bandbreiten hierzulande um Längen schlagen. Der Service Provider „Hong Kong Broadband Network“ beispielsweise bietet Bandbreiten von 10 bis 1’000 Mbps über Glasfaserkabel. Er kann somit auch komplementäre Dienste wie Voice-over-IP und Internetfernsehen aus einer Hand bieten. In Europa gibt es meist regionale Anbieter, welche in grösseren Ballungsgebieten schon VDSL mit Bandbreiten zwischen 10 und 60 Mbps (Download) anbieten.

### 4.7.2 Bandbreitenbedürfnisse

Es gibt viele Ansichten bezüglich der Notwendigkeit von höheren Bandbreiten. Tatsache ist, dass die Telekomanbieter Services wie „Triple play“ und mehr aus einer Hand anbieten werden. Dies wird die Bandbreiten auf ein Niveau heben, wie sie aus Asien bekannt sind und den Konkurrenzdruck erhöhen.

#### Grosse Unternehmen

Grosse Unternehmen mit geographisch verteilten Standorten und Abhängigkeit von IT Infrastruktur müssen in leistungsfähige Netzanbindung investieren. Die herkömmlichen Bandbreiten, die für den privaten Endverbraucher ausreichen, kommen hier nicht in Frage und müssen mit einer modernen, leistungsfähigeren Anbindung und Quality of Service Attributen realisiert werden. In Folge mangelnder Alternativen müssen sie auf den Anbietermarkt, den die Telekomunternehmen bilden, zurückgreifen und relativ hohe Investitionen tätigen.

#### Kleine und mittlere Unternehmen

Solche Investitionen sind für kleinere Unternehmen teils undenkbar und stellen ein Hindernis bei den Möglichkeiten einer Erweiterung ihrer IT Infrastruktur dar. Betrachten wir als Beispiel einen Produktionsbetrieb, der Verwaltung und Fabrikation an verteilten Standorten hat und seine IT an beiden Standorten verknüpfen will. Er ist auf ein leistungsfähiges Netwerk angewiesen, da beispielsweise der Produktionsprozess Fernüberwacht- und gesteuert werden, und die betriebswirtschaftliche Software an beiden Standorten in permanenter Verbindung stehen soll. Die Planungsinstanzen werden bei dem heutigen Angebot der Telekomunternehmen den Investitionspreis für die Realisierung eines solchen Projektes als sehr hoch einstufen, da gerade in der letzten Meile die Anbindung per Glasfaser aufwendig und mit baulichen Massnahmen verbunden ist. Aus diesen Gründen lässt sich schliessen, dass die Realisation - auch nur der Anstoss in Form der Idee - den Produktionsprozess fern zu überwachen durch mangelndes Angebot erschwert bis verunmöglicht wird. Weitere kleine und mittlere Unternehmen in folgenden Branchen könnten von einem besseren Preis- Leistungsverhältnis im Telekomanbietermarkt für Bandbreiten grösser als 50 Mbps profitieren:

- Medizinische Dienstleister
- Baubranche/Architektur (Pläne)
- Hotels
- Schulen
- Druckereien

Beispiele für Anwendungsbereiche von Applikationen mit höheren Anforderungen an Bandbreite:

- Audio- Videotelefonie und -konferenzen
- Datenbackup und gemeinsame Netzwerkspeicherung von Daten
- Directory Services, zentralisiert und redundant an verteilten Standorten
- Fernüberwachung und -steuerung von Anlagen
- Datenübertragung grosser Dokumente

Das Bedürfnis an höheren Bandbreiten und alternativen Anbindungen in der letzten Meile wird sich in naher Zukunft also ausprägen und Wirkung, in Form einer Neuausrichtung auf den Markt, bei den Anbietern zeigen.

### 4.7.3 Carrier Technologie Metro Ethernet

In obigem Beispiel kommt zu Tage, dass Bedürfnisbefriedigung an höheren Bandbreiten einhergehen wird mit weiterer Erschliessung der letzten Meile. Die Frage ist, wie die Telekomunternehmen den Vorstoss über diese letzte Meile zum Kunden am ehesten vornehmen werden.

#### Metro Ethernet Forum

Das Vorhaben des Metro Ethernet Forums (`http://www.metroethernetforum.org`) ist es unter anderem die Ethernet Technologie zur Erbringung dieser Dienste einzusetzen. Die Vorteile wurden in den vorigen Kapiteln bereits aufgeführt und lassen sich grundsätzlich mit den Begriffen Kosteneffizienz, Skalierbarkeit und Vertrautheit des Kunden mit Ethernet zusammenfassen. Die Ethernettechnologie bietet günstigere Hardware auf Konsumentenseite und setzt auf dem bereits existierenden Know-how des Unternehmens im LAN-Bereich auf. Mit den technischen Spezifikationen, die das Metro Ethernet Forum in Zusammenarbeit mit Industriegrössen aus der Telekom- und Netzwerkhardwarebranche erarbeitet [20], will man die Interoperabilität der einsetzbaren Netzwerkinfrastruktur gewährleisten und Anreize für den Einsatz der Metro Ethernet Technologie als idealer Approach zum Aufbau von Netzen und Erschliessung der Konsumenten schaffen.

#### Vorteile der Metro Ethernet Technologie

Was aber ist nun genau der Unterschied der MEN-Technologie gegenüber anderen Carrierkonzepten? Von der technischen Seite betrachtet findet eine Schachtelung (encapsulation) der Ethernetpakete in die bestehenden Netze (Mietleitungen, ATM, Frame Relay usw.) der Provider statt. Es ergeben sich dadurch geschachtelte Formen der Pakete wie Ethernet

over SDH, Ethernet over MPLS oder Ethernet over DWDM. Somit können die Anbieter ihre bisherigen Produkte ergänzen - sprich die Kapazitäten ihrer Netzarchitektur ausbauen - und dem Kunden transparente Dienste anbieten, beispielsweise mit den erwähnten User Network Interfaces (UNIs).

#### Blackbox Metro Ethernet

Im Hinblick auf die Transparenz, welche die Blackbox „Metro Ethernet“ somit bietet, wird klar, dass sich das Produkt des Anbieters von einer einfachen Datentransportleitung, bei welcher der Endkunde selber für seine Anbindung sorgte, zu einem zunehmend serviceorientierten Produkt, bei dem einfach der Ethernetstecker in die Dose gesteckt wird, wandeln wird. Auch bei der Verwendung von Ethernet als Common Access Interface kann der Anbieter die Anwendung von SLAs und Mehrwertdiensten (VoIP) auf Layer 3 aufbauend anbieten und realisieren [26].

## 4.8 Zusammenfassung und Fazit

Die Grossen der Telekommunikationsbranche sehen Metro Ethernet als eine skalierbare und leistungsfähige Lösung, mit welcher die Anbieter ihre Produktportfolios ergänzen können. Marktforscher Infonetics Research (`http://www.infonetics.com`) sagte dem Markt für Metro Ethernet Ausrüstung und Services im Jahr 2004 starkes Wachstum und eine kumulierte jährliche Wachstumsrate von 27 Prozent von 2003 bis 2008 voraus (siehe Abbildung 4.18). Das Metro Ethernet Forum hat eine grosse Anzahl vorherrschender Mitglie-

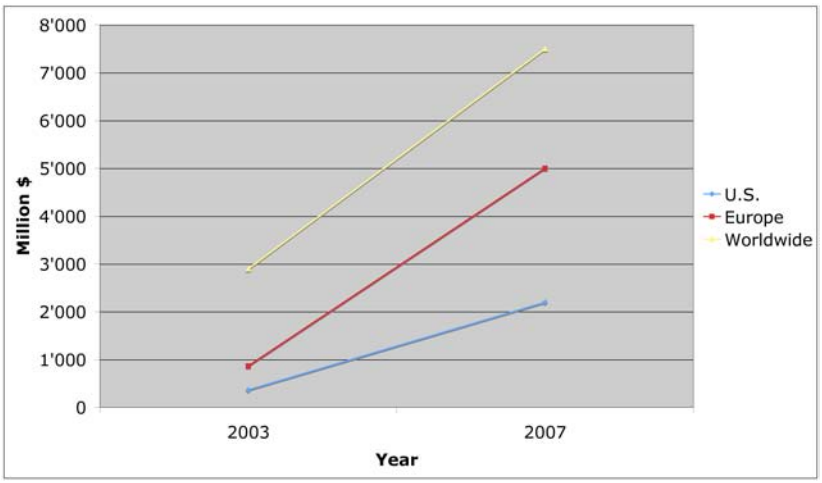



Abbildung 4.18: Entwicklung des Einkommens durch Metro Ethernet Ausrüstung weltweit [9]

der aus der Industrie und wird somit die Einführung und Adoption von standardisiertem Carrier Ethernet in naher Zukunft voranbringen können. Dies soll durch Zertifikation von Netzwerkhardware und Providern, die Carrier Ethernetdienste anbieten, und zahlreiche Verfassungen technischer Spezifikationen geschehen. Die Merkmale die Metro Ethernet als

Carriertechnologie auszeichnen, verbinden Skalierbarkeit und Verfügbarkeit mit Quality of Service Attributen, SLAs und hoher Granularität. Die Netzwerkinfrastruktur ist kundenseitig preisgünstig und ermöglicht dem Provider das Anbieten von attraktiven Produkten (E-LAN, E-Line).

Die Metro Ethernet Technologie bietet technisch sowie auch marketingstrategisch interessante Möglichkeiten für die Realisation von Breitbandanbindungen im Metro-Bereich, in mittelfristiger Sicht vielleicht sogar im WAN-Bereich. Für den Konsumenten werden bessere Preis-Leistungsverhältnisse resultieren, sofern die Anbieter sich entscheiden, weitere Schritte im Angebotsmarkt zu unternehmen. Die Entwicklung der konkurrierenden Angebote wird ihren Teil dazu beitragen.

# Literaturverzeichnis


[1] Ahlers Ernst, Sicheres Metro-Netz, c't - Magazin für Computertechnik, Ausgabe 11/2006, Seite 46.

[2] Andrew Tanenbaum, Computer Networks, 4th Edition, 2003.

[3] Bertuch Manfred, 5 MBit/s für jedermann, c't - Magazin für Computertechnik, Ausgabe 24/2002, S. 58.

[4] Burkhard Kirste, ATM - Asynchronous Transfer Mode, 13.6.1995, `http://www.chemie.fu-berlin.de/glossar/atm.html` , recherchiert April 2006.

[5] Burkhart Stiller und Jochen Schiller, Vorlesungunterlagen „Mobile Communication Systems“, 2006.

[6] Cisco Service Provider Metro Ethernet Architecture Guidelines, White Paper, `http://www.cisco.com/en/US/netsol/ns577/networking_solutions_white_paper0900aecd80351e5c.shtml`, recherchiert Mai 2006.

[7] Firmenwebsite Fastweb, `http://www.fastweb.it`, recherchiert Mai 2006.

[8] IEEE Std 802.3 - 2002, Information technology - Telecommunications and information exchange between systems - Local and metropolian area network - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 8 März 2002.

[9] Infonetics Research, Metro Ethernet Equipment Tops, `http://www.infonetics.com/resources/purple.shtml?nr.met.011904.shtml`, recherchiert Juni 2006.

[10] Jochen Schiller, Mobilkommunikation, 2. überarbeitete Auflage, 2003.

[11] Mark Whalley und Dinesh Mohan, Metro Ethernet Services - A Technical Overview, 2003, `http://www.metroethernetforum.org`, recherchiert April 2006.

[12] Metro Ethernet Forum, Accelerate Worldwide Adoption of Carrier Class Ethernet Network and Services, `http://www.metroethernetforum.org`, recherchiert April 2006.

[13] Metro Ethernet Service Interworking with Frame Relay and ATM, White Paper, `http://www.cisco.com/en/US/netsol/ns577/networking_solutions_white_paper09186a0080126eb7.shtm`, recherchiert Mai 2006.

[14] Metro Ethernet Forum, Tecnical Specification MEF 1, Ethernet Service Model - Phase 1, 10 November 2003, http://www.metroethernetforum.org/TechSpec.htm, recherchiert April 2006.

[15] Metro Ethernet Forum, Tecnical Specification MEF 4, Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, May 2004 http://www.metroethernetforum.org/TechSpec.htm, recherchiert April 2006.

[16] Metro Ethernet Forum, Tecnical Specification MEF 6, Ethernet Service Defenitions - Phase 1, Juni 2004, http://www.metroethernetforum.org/TechSpec.htm, recherchiert April 2006.

[17] Metro Ethernet Formum, Tecnical Specification MEF 10, Ethernet Service Attributes Phase 1, November 2004, http://www.metroethernetforum.org/TechSpec.htm, recherchiert April 2006.

[18] Ralph Santitoro, Metro Ethernet Services - A Technical Overview, http://www.metroethernetforum.org , recherchiert April 2006.

[19] Ralph Santitoro, Bandwidth Profiles for Ethernet Services http://www.metroethernetforum.org, recherchiert April 2006.

[20] Savvas A., 'Metro Ethernet users to be given greater product interoperability', ComputerWeekly.com, Sept. 2005, http://www.computerweekly.com/Articles/Article.aspx?liArticleID=212006, recherchiert Juni 2006.

[21] Schmitt K., 'VATM bezeichnet Deutsche Telekom als Breitband-Bremse', Silicon.de, Okt. 2005, http://www.silicon.de/enid/telecom_und_ip_39.html?c_id=15983, recherchiert Juni 2006.

[22] Wikipedia: Die freie Enzyklopädie, Lichtwellenleiter http://de.wikipedia.org/wiki/Lichtwellenleiter, recherchiert April 2006.

[23] Wikipedia: Die freie Enzyklopädie, Asynchronous Transfer Mode http://de.wikipedia.org/wiki/Asynchronous_Transfer_Mode , recherchiert April 2006.

[24] Wikipedia: Die freie Enzyklopädie, WiMAX http://de.wikipedia.org/wiki/WiMax , recherchiert April 2006.

[25] Wikipedia: Die freie Enzyklopädie, Delay (Telekommunikation) http://de.wikipedia.org/wiki/Delay_\%28Telekommunikation\%29, recherchiert April 2006.

[26] Zier, L.; Fischer, W.; Brockners, F., 'Ethernet-based public communication services: challenge and opportunity', Communications Magazine, IEEE , vol. 42, no. 3, pp. 88-95, March 2004.

# Kapitel 5

# Autonomic Computing

*Veronica Garcia, Lukas Knauer, Christophe Suter*

*Alles wird grösser und besser. So auch die Computerindustrie: die Entwicklung tendiert zu riesigen Computersystemen, so gross, dass sie vom Menschen kaum noch überblickt werden können. Doch wie sollen solche Systeme gewartet werden? Woher nimmt man die entsprechend qualifizierten Arbeitskräfte und ist dies ökonomisch noch sinnvoll? Selbstverwaltende Computersysteme versprechen einen interessanten Lösungsansatz: Systeme, die in der Lage sind, sich selbst zu konfigurieren, zu schützen, zu heilen und zu optimieren. Und das mit minimalem menschlichem Eingriff. Doch was steckt wirklich dahinter? Wie soll solch ein kaum vorstellbares Unterfangen ermöglicht werden? In diesem Bericht wird versucht, die heute bereits existierenden Techniken und Anstätze zu erläutern und herauszufiltern, was bereits vorhanden ist und was noch erforscht werden muss. Dabei werden die theoretischen Grundlagen (so weit vorhanden) und verstärkt das Thema Peer-to-Peer Netzwerke betrachtet. Des weiteren wird untersucht, was Firmen bezüglich selbstverwaltenden Computersystemen oder ähnlichen Ansätzen am Erforschen sind und wie der aktuelle Stand aussieht.*

## Inhaltsverzeichnis

**5.1 Einleitung . . . . . 145**
**5.2 Notwendigkeit von selbstverwaltenden Computersystemen . 146**
5.2.1 Komplexität als Antrieb . . . . . 146
5.2.2 Kosten als Antrieb . . . . . 147
**5.3 Was sind selbstverwaltende Computersysteme . . . . . 148**
5.3.1 Charakteristiken . . . . . 149
5.3.2 Selbstverwaltende Elemente . . . . . 153
**5.4 Risiken und Vorteile . . . . . 155**
5.4.1 Risiken . . . . . 156
5.4.2 Vorteile . . . . . 159
**5.5 Verwirklichung von selbstverwaltende Computersysteme . . 160**
5.5.1 Evolution . . . . . 160
5.5.2 Standards . . . . . 162
**5.6 Existierende Komponenten . . . . . 164**
5.6.1 Routingprotokolle . . . . . 164
5.6.2 Verschlüsselung und Zertifikate . . . . . 165
5.6.3 Persönliche selbstverwaltende Computersysteme . . . . . 165
**5.7 Pläne der IT-Branche zum Thema selbstverwaltende Computersysteme . . . . . 166**
5.7.1 Hewlett-Packard . . . . . 167
5.7.2 Sun Microsystems . . . . . 167
5.7.3 CISCO . . . . . 168
5.7.4 Microsoft . . . . . 168
**5.8 Relevante Forschungsgebiete . . . . . 168**
5.8.1 Peer-to-Peer Netzwerke . . . . . 169
**5.9 Schlusswort . . . . . 172**

## 5.1 Einleitung

Automatisches Managen, Konfigurieren sowie Probleme erkennen und beheben waren schon immer Teil der Forschung und Entwicklung in der Informatik. Mit Autonomic Computing wird diese Tradition weiter geführt, mit dem Unterschied, dass die gesamte IT-Umgebung als eine Einheit betrachtet wird. So wird versucht, die Komplexität nicht nur in den einzelnen Komponenten, sondern auch in der Interaktion derselben zu verstehen und meistern.

Im ersten Teil dieser Arbeit wird erläutert, was die Motivation von Unternehmungen für selbstverwaltende Computersysteme (Autonomic Computing) ist. Ausgehend davon, wird die Definition vom Initiator IBM aufgezeigt, wobei auch auf die Analogien zum menschlichen Körper eingegangen wird. Anschliessend werden die vier grundlegenden Eigenschaften aufgezeigt und näher erläutert. Daneben werden die autonomen Elemente erwähnt, welche die Basiskomponenten bilden und es werden sogenannte Kontrollschlaufen gezeigt, mit denen selbstverwaltende Element ihre Aktionen Überwachen, Planung und Koordinieren.

Aufgrund der Definitionen werden im folgenden Teilstück die Risiken, wobei Sicherheitsaspekte einen wichtigen Stellenwert einnehmen, aber auch die potentiellen Vorteile von selbstverwaltenden Computersystemen aufgezeigt.

Nach diesen Einleitungen, wird das Augenmerk darauf gerichtet, wie selbstverwaltende Computersysteme erreicht werden können. Hierbei seien die 5 Stufen der Evolution erwähnt, welche Kritieren dafür liefern, in welcher Ausprägung auf dem Weg zu selbstverwaltenden Computersystemen sich ein Programm / Applikation momentan befindet. Je höher dabei die Stufe ist, desto selbstverwaltender ist das Programm und desto weniger menschliche Eingriffe werden benötigt.

Aus Sicht der Heimanwender beleuchtet der Abschnitt über persönliche selbstverwaltende Computersysteme den Stand der Dinge. Hierbei werden aktuell verfügbare Sachverhalte aufgezählt, welche auf heutigen Desktop-Computern verfügbar sind. Dazu zählen beispielsweise das Benutzerinterface von WindowsXP, aber auch DHCP und DNS.

Da die Idee von selbstverwaltende Computersysteme etwa 5 Jahre alt ist und stark umworben wurde, ist es kaum verwunderlich, dass sich unzählige andere Firmen dieser Idee anschlossen oder aber auch eigene Zielvorstellungen verfolgten. Anhand einiger prominenter Vertreter, wie zum Bespiel HP oder Sun, zeigt dieses Dokument den aktuellen Stand dieser Firmen auf.

Abschliessend wird das aktuelle Forschungsgebiet Peer-to-Peer Netzwerke unter dem Gesichtspunkt von selbstverwaltenden Computersystemen betrachtet, wobei zuerst eine Analyse erfolgt, welche Basiskritieren für selbstverwaltende Computersysteme in Peer-to-Peer Netzwerken gelten sollte und anhand einer ganzheitlichen Betrachtung wird anschliessend über Sinn und Unsinn von selbstverwaltenden Peer-to-Peer Netzwerke reflektiert.

## 5.2 Notwendigkeit von selbstverwaltenden Computersystemen

Paradoxerweise wird der Erfolg, den IT-Industrie in den letzten Jahren feiern konnte, zu ihrem eigenen Verhängnis. Gemäss Moore's Law [11], nachdem sich durch den technischen Fortschritt die Komplexität eines Systems etwa alle 24 Monate verdoppelt, beginnt hier genau das Problem der IT: eine rasante, exponentielle Entwicklung. Heutzutage finden sich in jedem Haushalt mehrere elektronische Geräte (PDA, mobiles Telefon, Laptop, Internetzugang etc). Diese Geräte wollen gewartet, weiterentwickelt, abgesichert und wenn möglich interoperabel sein.

Ausgehend von dieser stetig wachsenden **Komplexität** von IT-Systemen, die parallel einhergehende zunehmende Heterogenität und die immer grösseren Anforderungen und Herausforderungen an Administratoren zur Wartung dieser Systeme, wird versucht, diese Komplexität zu reduzieren.

Neuerungen in der IT-Branche haben nicht nur positive Auswirkungen auf die Kosten der IT einer Unternehmung. Ein leistungsfähigerer Server sollte eine Leistungssteigerung zur Folge haben. Ist dieser aber mit den Applikationen nicht richtig abgestimmt, setzt kein Nutzenwachstum ein. Unter diesen Umständen bedeutet dieser nur mehr Kosten und keine Vorteile. Es gilt also die verursachenden Kosten durch die erhöhte Komplexität abzufangen und somit keine Einbussen einfahren zu müssen.

### 5.2.1 Komplexität als Antrieb

IBM zeichnet in Beiträgen [1] die Problematik der Komplexität auf, mit der sich die IT Branche in naher Zukunft auseinandersetzen muss und dies bereits macht.

> "More than any other I/T problem, this one — if it remains unsolved — will actually prevent us from moving to the next era of computing." [1]

Die Komplexität setzt sich aus verschiedenen Faktoren zusammen. Einerseits die entstehende Vielschichtigkeit beim Vernetzen von Computern und grösseren Rechnern, anderseits der wachsende Umfang der darunterliegenden Infrastruktur und Verwaltungssoftware solcher Netze. Eine Problemlösung im Bereich der Architektur und Software ist durch neue Designs, Sprachen und Programmiertechniken nicht denkbar. Es wird in Zukunft, und heute nicht möglich sein alle Probleme statisch (vorbeugend) abzufangen, sondern sie müssen zur Laufzeit gelöst werden. Dies impliziert eine schnelle Reaktion, Analyse und Problembehebung unter zeitkritischen Bedingungen. Hierzu ist ein umfangreiches Verständnis des Systems gefordert und diese können nur durch erfahrene, gut ausgebildete Spezialisten durchgeführt werden.

Die Komplexität der Systeme wird mit der Einbindung von Systemen in das Internet eine weitere Dimension annehmen, welche, auch für Spezialisten, nicht mehr bezwingbar ist.

> "As computing evolves, the overlapping connections, dependencies, and interacting applications call for administrative decision-making and responses faster than any human can deliver." [1]

Werden hierzu keine Massnahmen ergriffen, so bedeutet dies der Verlust der Vorteile, die eine Integration von Systemen mit sich bringt. An diesem Punkt entsteht die Idee der Verlagerung der Komplexität in die Systeminfrastruktur und anschliessend deren Verwaltung zu automatisieren. Durch selbstverwaltende Computersysteme wird die zugrunde liegende Komplexität für den Anwender transparent.

### 5.2.2 Kosten als Antrieb

Die Komplexitätsproblematik schlägt sich auch in den Kosten nieder, so ist der Aufwand für das Management umfangreicher Systeme sehr hoch. Gut qualifizierte und erfahrene Systemadministratoren sind notwendig um diese Systeme zu installieren, konfigurieren und optimieren, was meistens dazu führt, dass „Personalkosten die Technologiekosten übersteigen." [4]

Abgesehen davon, dass diese Aufgaben sehr anspruchsvoll sind, müssen sie meistens unter Zeitruck durchgeführt werden. Dadurch entsteht eine Fehlerrate, die nicht zu vernachlässigen ist. Die eingeschlichenen Fehler können unter Umständen sogar zu einem Systemausfall führen. Durch die folgende Grafik (siehe Abbildung 5.1) wird erläutert was für Auswirkungen dies für ein Unternehmen hat. Die Verlustrate wird nach Branchen unterteilt und gibt den durchschnittlichen Verlust pro Stunde an.

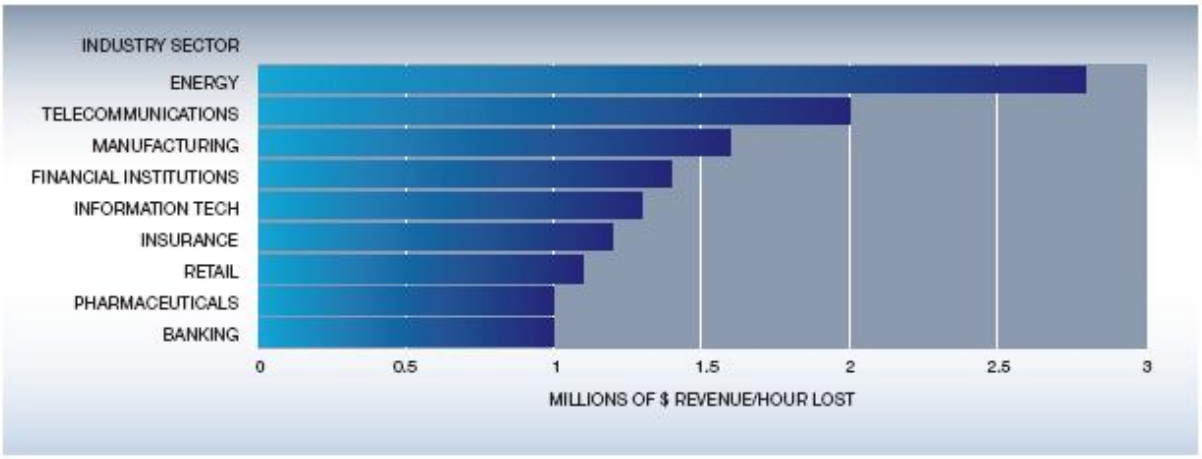



Abbildung 5.1: Durchschnittliche Auswirkung pro Stunde [4]

Ausserdem wird heute eine Systemverfügbarkeit von 24/7 erwartet. Dies ist nicht ohne weiteres möglich, so ist auch eine angemessene Personalplanung gefragt. Eine Verfügbarkeit von qualifizierten Administratoren rund um die Uhr ist kostspielig und muss unbedingt mit einberechnet werden.

Wachsen die Systeme, so sind sie immer schwieriger optimal einzustellen. Nicht optimal konfigurierte Systeme sind logischerweise weniger konkurrenzfähig was sich wieder auf die Kosten bzw. den Erlös eines Unternehmens auswirkt.

Das IT-Budget kann mit der Automatisierung von Verwaltungsaufgaben durch selbstverwaltende Computersysteme geschont werden. Eine höhere Systemzuverlässigkeit durch eine kleinere Fehlerrate kann gewährleistet werden. Sowie optimale Nutzauslastung durch fein abgestimmte Komponenten ist denkbar.

## 5.3 Was sind selbstverwaltende Computersysteme

Aufgrund der erwähnten Komplexität und der daraus resultierenden Kosten rief IBM Ende 2001 den Begriff **Autonomic Computing** [1] , oder auf Deutsch „selbstverwaltende Computersysteme„ , ins Leben. Hinter diesem Schlagwort versteht IBM diejenigen Systeme, die sich ähnlich dem autonomen (vegetativ) menschlichen Nervensystem selbst regulieren. Anhand eines Beispieles sei dies verdeutlicht: man stelle sich eine schwimmende Person vor. Diese Person hat sich nicht bewusst um ihre inneren Vorgänge zu kümmern (Anpassung des Blutdruckes; korrekte Atmung, damit der Sauerstoffgehalt im Blut stimmt; Angleichung der Schweissdrüsen bezüglich Temperaturausgleiches etc). Angenommen, der menschliche Körper würde so funktionieren wie unsere heutigen Computersystem, dann hätte sich diese Person um die meisten dieser Vorgänge selbst aktiv zu kümmern.

Ein selbstverwaltendes Computersystem soll jedoch die Arbeitsweise von Applikationen und Systemen ohne das Eingreifen von Benutzern/Admins kontrollieren, regulieren und steuern können. Dies ist analog dem vegetativen Nervensystem des menschlichen Körpers, welches ohne bewusstes Eingreifen des Menschen dessen Körper steuert.

Abbildung 5.2: Menschliches Nervensystem [22]

Angewandt auf die IT bedeutet dies, dass es ein Netzwerk von organisierten, intelligenten Computer-Komponenten geben muss, welche die benötigten Informationen an den

Endbenutzer korrekt und zum richtigen Zeitpunkt liefern, ohne dass sich dieser darüber Gedanken machen muss. Es wird demnach ein System zur Verfügung gestellt, welches die Administratoren von den Details der Bedienung der Computeranlage und der Wartung (im Idealfall) befreit und gleichzeitig den Endbenutzern mit einer Laufzeit von 24/7 den Zugriff gewährt. Der Grundgedanke dabei ist es, Computersysteme zu entwickeln, welche die Fähigkeit besitzen, sich selbst zu verwalten. Diese Eigenschaft wird von IBM als **Selbstverwaltung** (self-management) bezeichnet und ist eine der wesentlichen Eigenschaften von selbstverwaltenden Computersystemen [2].

Daraus lässt sich eine Verschiebung der Betrachtungsweise ableiten: Datenzugriff und -verarbeitung befinden sich im Mittelpunkt, die Konfiguration und das Aktualisieren der Software übernimmt das autonome System. Die Endbenutzer können sich währenddessen produktiv mit ihren Daten befassen und mit jeder Art von Gerät überall auf der Welt auf ihre Daten zugreifen.

Dies könnte bedeuten, dass sich selbstverwaltende Computersysteme selbständig warten, ihre Operationen den Umwelteinflüssen anpassen und mittels intelligenten Algorithmen einzelne ihrer Komponenten updaten und bei einem allfälligen Problem während einer Aktualisierung selbständig zu einer älteren Version zurückkehren und dabei mittels eines Fehlererkennungsalgorithmus die fehlerbehaftete Komponente isolieren können. Oder auch, dass diese Systeme ihre Auslastung im voraus erahnen und dann ihre Ressourcen den einzutreffenden Begebenheiten anpassen können.

Angemerkt sei, dass sich der Begriff autonomic Computing von autonomous Computing insofern abgrenzt, als dass autonomous Computing auf künstliche Intelligenz und menschliche Unabhängigkeit setzt, was bedeutet, dass autonomous Computing weiter geht als autonomic Computing (als Beispiel sei die Roboter-Fussball-Weltmeisterschaft [3] erwähnt, welche als Versuch in diese Richtung geht, um die Abgrenzung zu verdeutlichen). Folglich ist unserer Meinung nach die im deutschen häufig zu findende Übersetzung „autonomes Computing„ als irreführend oder falsch einzustufen. Der in diesem Dokument verwendete Begriff „selbstverwaltende Computersysteme„ bezieht sich immer auf das in englischen Dokumenten benutzte „autonomic Computing„.

### 5.3.1 Charakteristiken

Paul Horn, Senior Direktor und Vizepräsident von IBM Research, definiert die zukünftigen Herausforderungen von selbstverwaltenden Computersystemen mittels folgender vier Eigenschaften (vgl. [4] und Tabelle 5.1):

1. „An autonomic system must configure and reconfigure itself under varying and unpredictable conditions.„

   **Self-Configuring**: Selbst auf einem normalen Web-Server besitzt ein Administrator die Möglichkeit unzählige verschiedene Parameter in den Konfigurationsdateien anzugeben. Wird nun die Anzahl der Computer und deren Programme, welche miteinander agieren, erhöht und sollten die Konfigurationen dynamisch eingestellt werden, erreichen menschliche Administratoren sehr schnell ihre Grenzen. Genau

hier setzen selbstverwaltende Computersysteme an: ein selbstverwaltendes Computersystem sollte die Fähigkeit besitzen, dynamisch seine Ressourcen anzupassen und zugleich sollten Konfigurationen automatisch und dynamisch erstellt werden. Die Herausforderungen hierbei stellt sich in möglichen unerwünschten Nebeneffekten von komplexen Systemen ein: durch die Vielzahl an Konfigurationsmöglichkeiten muss das selbstverwaltende System im Voraus wissen, welchen Einfluss ein Parameter auf verwandte Dienste und Programme hat. Das bedeutet, dass bei jedem sich geänderten Konfigurationsparameter auch sämtlichen davon betroffenen Diensten mitgeteilt werden muss, was geändert wurde. Die Dienste selbst müssen nun wissen, wie sie davon betroffen sind und was für Auswirkungen das haben könnte. Eine nicht korrekte Konfiguration kann unter Umständen nicht nur nahe Dienste betreffen, sondern auf ein gesamtes System übergreifen (siehe dazu auch selbstverwaltende Elemente).

2. "An autonomic system must perform something akin to healing – it must be able to recover from routine and extraordinary events that might cause some of its parts to malfunction."

**Self-Healing**: Damit werden die Möglichkeiten des Systemes beschrieben, das fehlerhafte Verhalten einzelner Komponenten zu lokalisieren - und wenn möglich - diese zu reparieren. Es sollte mögliche Probleme im Voraus erkennen und die Möglichkeiten besitzen, selbständig trotz potentieller Probleme einen ausfallsicheren Betrieb zu gewährleisten. Für die Benutzer sollte dabei nur eine minimale Unterbrechung, im Idealfall gar keine, spürbar sein. Ebenso gilt es potentiellen Datenverlust und Verzögerungen in den Prozessen zu vermeiden.

3. „An autonomic system never settles for the status quo – it always looks for ways to optimize its workings."

**Self-Optimizing**: Aufgrund der oben erwähnten Vielzahl an Konfigurationsparameter und Integrationsmöglichkeiten verschiedener Systeme kann es vorkommen, dass unerwünschte Nebeneffekte auftreten. Ein selbstverwaltendes Computersystem sollte bestrebt sein, kontinuierlich seine Arbeitsabläufe zu optimieren um ein insgesamt effizienteres System zu erreichen. Dies bedeutet, dass es seine momentane Leistungsfähigkeit messen, diese mit Ideal-Werten vergleichen kann und dass es Strategien besitzt, um eine höhere Effizenz anzustreben, wobei sich die Frage stellt, was genau Ideal-Werte sind. Gerade in individuellen, hoch-komplexen Systemen kann dies ein sehr schwieriges Unterfangen darstellen.

4. „A virtual world is no less dangerous than the physical one, so an autonomic computing system must be an expert in self-protection.„

**Self-Protecting**: Selbstverwaltende Computersysteme sollten die Fähigkeit besitzen auf interne und externe Attacken zu reagieren. Dies geschieht auf zwei Arten. Erstens schützen sie das System als ganzes gegen böswillige Attacken und zweitens verfügen sie über die Möglichkeit, aufgrund von Berichten ihrer Sensoren, selbständig Gefahren vorauszuahnen (ähnlich Nagios [12]) und darauf entsprechend zu reagieren, bevor der Ernstfall eingetreten ist. Dies bedeutet, dass es Self-Healing bei Attacken einsetzt und Self-Optimizing benützt, um möglichen Bedrohungen vorzubeugen. Wenn man allerdings die jetztigen Erfolge bezüglich den selbstschützenden

Programmen sieht, scheint sich hier eine sehr grosse Herausforderung für die Forschung zu eröffnen. Alleine aufgrund der Tatsache, dass auf bösartige Software immer reagiert und nicht agiert werden kann, verdeutlicht die Problematik. Verstärkt wird dies dadurch, dass heutige Schädlinge gezielt zuerst die Schwächen der bekanntesten Antiviren-Programme auszunutzen, um diese funktionsunfähig zu machen und anschliessend den befallenen Computer für ihre Zwecke zu missbrauchen. Da sich hier in den letzten Jahren nicht viel geändert hat, darf bezweifelt werden, ob dies selbstverwaltenden Computersystemen besser gelingt. Siehe hierzu auch den Abschnitt über Sicherheit im Kapitel Risiken.

Um diese Charakteristiken zu erreichen, muss ein selbstverwaltendes Computersystem folgendes beherrschen:

1. "To be autonomic, a system needs to „know itself" and consist of components that also possess a system identity.„

   **Self-Defining**: Ein selbstverwaltendes Computersystem sollte die Fähigkeit besitzten, sich selbst in- und auswendig zu kennen. Seine Komponenten sollten eine System-Identität besitzen, woraus folgt, dass das System sich selbst definieren kann. Was auch bedeutet, dass es möglich sein sollte, dass es sich mit anderen System zusammenschliessen und wieder trennen kann. Diese Fähigkeiten sind notwendig, da ein System nicht etwas überwachen kann, von dessen Existenz es keine Kenntniss hat.

2. "An autonomic computing system knows its environment and the context surrounding its activity, and acts accordingly.„

   **Contextually-Aware**: Angenommen ein Benutzer möchte mit seinem mobilen Telephon eine Adresse auf einer Webseite abrufen, dann sollte das selbstverwaltende Computersystem erkennen, mit wem es kommuniziert und was genau die angeforderte Ressource ist. In diesem Fall sollte das Computersystem nicht die gesamte Webseite senden (im ungünstigsten Fall mit sämtlichen Bildern und Animationen), sondern eine auf den Empfänger optimierte Übertragung ermöglichen.

3. "Perhaps most critical for the user, an autonomic computing system will anticipate the optimized resources needed while keeping its complexity hidden."

   **Anticipatory**: Ein Benutzer und die verwendete Applikation führen ihre Aufgaben in einer Computer-Umgebung so aus, dass sie keine Kenntnisse der darunterliegenden Technologie besitzen müssen. Dies bedeutet, dass ein selbstverwaltendes Computersystem in der Lage sein sollte, unerwünschte, nicht zur Erledigung der Arbeit des Benutzers benötigte Informationen herauszufiltern und selbstständig zu verarbeiten. Anhand eines Beispieles sei dies verdeutlicht: Angenommen ein Mensch befindet sich in einem Wald und wird von einem Raubtier überrascht. Sein Körper reagiert instinktiv auf diese Bedrohung, indem er den menschlichen Organismus auf verschiedene Reaktionsmöglichkeiten optimiert. Die Person kann sich auf die relevanten Entscheidungen konzentrieren (zum Beispiel flüchten oder kämpfen), wobei ihr Körper für sämtliche möglichen Aktionen bereit ist.

Für ein selbstverwaltendes Computersystem bedeutet dies, dass es einem Benutzer nur die für seine Entscheidung relevanten Informationen präsentiert und diejenigen Informationen, welche zu den relevanten Informationen führten, möglichst verbirgt. Dies entspricht wiederum dem Wesen von selbstverwaltenden Computersystemen: der Reduktion von Komplexität. Anticipatory wird auch als ultimatives Ziel von selbstverwaltenden Computersystemen betrachtet.

4. „An autonomic system can not exist in a hermetic environment (and must adhere to open standards).“

   **Open**: Ein selbstverwaltendes Computersystem muss auf unterschiedliche Betriebssysteme portierbar und auf einer Vielzahl von Hardwarekomponenten lauffähig sein. Folgendes Beispiel soll dies verdeutlichen: Da ein sich selbstverwaltenden Computersystemen immer Informationen von Teilen seines Systemes benötigt, ist der Informationsaustausch eine weitere Basis von selbstverwaltenden Computersystemen, respektive von den selbstverwaltenden Elementen. Im Regelfall geschieht dies mittels sogenannter Log-Dateien, in welchen einzelne Komponenten Informationen abspeichern. Da normalerweise verschieden Komponenten von unterschiedlichen Herstellern eingesetzt werden, welche wiederum auf verschiedene Arten der Informationsabspeicherung zurückgreifen, wurde ein einheitliches Logging notwendig (wie das WebService Distributed Management, welches seit März 2005 ein OASIS-Standard ist [25]).

   Im Idealfall werden dabei offene Standards verwendet, womit man sich eine grössere Nutzerbasis oder geringere Einstigskosten für interessierte Firmen erhofft. Auch der (Normal-) Fall, dass ein selbstverwaltendes Computersystem in einer sehr heterogenen Umgebung operieren kann, setzt die Benutzung von offenen Standards voraus, um andere Systeme zu verstehen und mit ihnen kommunizieren zu können. Eine Auflistung von aktuellen Standards kann aus dem aktuellen White-Paper von IBM entnommen werden [23] . Geschlossene Standards sind keine Variante, da diese die Interoperabilität einschränken. Es würde dann jeder Hersteller versuchen, seine eigenen Standards zu entwickeln und diese am Markt zu etablieren. Diese Standards wären, in der Mehrheit der Fälle, untereinander inkompatibel und müssten von Konkurrenten oder Mitentwicklern kostenpflichtig lizenziert werden. Dadurch wäre eine gemeinsame Forschungsbasis nicht gegeben und die Zahl der Interessenten an einer Mitarbeit würde stark eingeschränkt. Somit sind offene Standards die beste Möglichkeit für IBM, dass sie ihre Vision verbreiten und neue Interessenten gewinnen können.

Die vorgestellen Charakteristiken werden eine grosse Herausforderung sowohl für die Forschung wie auch für die an selbstverwaltenden Computersystemen entwickelnden Unternehmungen darstellen. Wie erwähnt, funkioniert zum Beispiel Selbstschutz nur in einem geringen Ausmass auf einem heutigen Ein-Benutzer Desktop-System, ganz zu schweigen von einer vernetzten, hochkomplexen Systemumgebung. Aber auch Selbstkonfiguration muss kritisch hinterfragt werden: ist es überhaupt möglich, dass ein grosses, vernetztes System die Möglichkeiten einer Konfigurationsänderung einer seiner Komponenten in ihrem ganzen Ausmass bis ins letze Detail erfassen kann? Und wie können nicht korrekte Änderungen durch solch ein komplexes System überhaupt erkannt, auf eine bestimmte

Tabelle 5.1: Selbstverwaltung heute und wie sie mittels selbstverwandender Computersysteme wäre

| ***Konzept*** | ***Heute*** | ***Selbstverwaltende Computersysteme*** |
|---|---|---|
| *Self-Configuration* | Durch die Heterogenität der IT-Landschaft ist die Installation, Konfiguration und Integration der Systeme zeitaufwendig und fehleranfällig. | Automatische Konfiguration der Komponenten und Systeme unter Zunahme von Richtlinien. |
| *Self-Optimization* | Überhandnehmende Anzahl an Konfigurationsparametern, wobei eine Abnahme nicht in Sicht ist. | Komponenten und Systeme suchen kontinuierlich nach Verbesserungsmöglichkeiten um die Performance und die Effizienz zu erhöhen. |
| *Self-Healing* | Ein Problem in einer grossen und komplexen IT-Landschaft zu lokalisieren ist zeit- und ressourcenintensiv. | Das System entdeckt, diagnostiziert und behebt örtlich begrenzte Software- und Hardware-Probleme. |
| *Self-Protecting* | Entdeckung, Behebung und Verhinderung der Ausbreitung von Angriffen wird von Administratoren erledigt. | Das System verteidigt sich automatisch gegen böswillige Attacken. |

Modifikation zurückgeführt und wieder rückgängig gemacht werden, oder bezogen auf die Charakteristiken: ist das Konzept der Selbstheilung überhaupt anwendbar? Im Abschnitt über Pläne der IT-Branche wird ein Überblick über die Lösung dieser Problematiken gegeben, jedoch befinden sich diese meistens noch im Forschungsstudium.

### 5.3.2 Selbstverwaltende Elemente

Ein selbstverwaltendes Computersystem ist eine interaktive Ansammlung von **selbstverwaltenden Elementen**. Diese bilden die Basiskomponenten, wobei die Elemente untereinander interagieren können. Sie beobachten ununterbrochen ein System oder die Komponenten eines Systemes mit Hilfe von Sensoren und Effektoren (Effectors). Über die Frage, was genau Agentenschaft (agenthood) bedeutet, wird heutzutage viel diskutiert. Eine mögliche Definition wäre folgende, welche bei einer steigenden Anzahl von Wissenschaftlern immer mehr Anklang findet:

> „An agent is an encapsulated computer system that is situated in some environment, and that is capable of flexible, autonomous action in that environment in order to meet its design objectives.„ [13]

Als selbstverwaltendes Element wird ein individueller Systembestandteil bezeichnet, welcher Ressourcen besitzt und Dienste an Menschen und oder andere selbstverwaltende

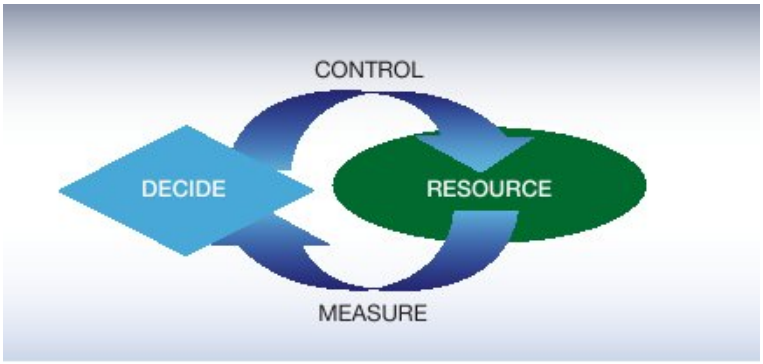



Abbildung 5.3: Kontrollschlaufe [4]

Elemente liefert. Es besteht aus einem oder mehreren verwalteten Elementen, wobei ein solches Element eine Hardware- oder Software-Komponente oder aber auch ein ganzes System sein kann. Ein selbstverwaltendes Element kontrolliert und repräsentiert seine verwalteten Elemente nach aussen. Selbstverwaltende Elemente steuern ihr internes Verhalten und ihre Beziehungen mit anderen selbstverwaltenden Elementen in Übereinkunft mit sogenannten Policies. Diese können auf dreierlei Arten definiert werden:

Erstens können sie durch die Zielsetzung der Entwickler implementiert worden sein. Zweitens können selbstverwaltende Elemente, welche Autorität über ein anderes selbstverwaltendes Element besitzen, dieses beeinflussen und drittens können selbstverwaltende Elemente Unterverträge mit Peer-Elementen eingehen.

Selbstverwaltende Elemente überwachen ihr Verhalten und ihre Beziehungen mit anderen Elementen mittels Sensoren, analysieren diese gesammelten Daten und planen anschliessend, welche Aktion durchgeführt werden soll. Falls vorhanden, wird eine solche Aktion mittels der Effektoren durchgeführt und eine Art von Kontrollschlaufe wird erzeugt. In Abbildung 5.3 wird dieser Zusammenhang graphisch aufgezeigt.

Diese Kontrollschlaufe ist das Wesentliche der Automatisierung innerhalb eines selbstverwaltenden Systems: mittels Messung oder Abtastung einer Aktivität in einem zu kontrollierenden Prozess entscheidet eine kontrollierende Komponente über das weitere Vorgehen und führt die erforderliche Aktion aus. Dabei vergleicht sie den gemessenen Zustand mit einem zu erwartenden Zustand aus einer Knowledge-Datenbank. Ungewünschte Zustände werden an einen Justierer (self-adjuster) übergeben, der die Aktion ausführt. Der Kontroller misst anschliessend erneut den zu überwachenden Prozess um zu bestimmen, ob die ausgeführte Aktion den gewünschten Effekt ausübte. Diese Routine wird in einem kontinuierlichen Kreislauf von Messen, Entscheiden, Ausführen und Nachkontrolle wiederholt.

Dabei müssen selbstverwaltende Elemente fähig sein, sich neuen Zielstellungen anzupassen (proaktiv) und sie müssen die Möglichkeit besitzen, innerhalb eines vernünftigen zeitlichen Rahmens auf Veränderungen, welche in ihrer Umwelt auftreten, zu reagieren (reaktiv). Dies führt aber zu Problemen: wenn ein selbstverwaltendes Element zu stark proaktiv ist, kann es sein, dass es aufgrund von sich bereits wieder geänderten Umweltzuständen irrelevante oder undurchführbare Aufgaben durchführen möchte. Andererseits kann es vorkommen, wenn ein selbstverwaltendes Element zu stark reaktiv ist, dass es seine Aufgaben nicht mehr erfüllen kann, da es beständig auf kurzfristige Bedürfnisse reagiert.

Die Herausforderung besteht darin, den goldenen Mittelweg zu finden. Um diese Ausgewogenheit zu erreichen, müssen kontext-sensitive Entscheidungen gefällt werden. Unter welchen Umständen welche Methode angewandt wird, um ein bestimmtes Ziel zu erreichen, unterliegt dabei einer signifikanten Unberechenbarkeit. Es entsteht ein emergentes Verhalten, was sich negativ auf das ganze System auswirken kann (aber nicht muss).

Selbstverwaltende Elemente bestehen typischerweise aus einem oder mehreren verwalteten Element, wobei diese mit einem einzigen selbstverwaltenden Manager verbunden sind. Dieser Manager kontrolliert und vertritt die verwalteten Elemente nach aussen. In Abbildung 5.4 wird dieser Zusammenhang verdeutlicht.

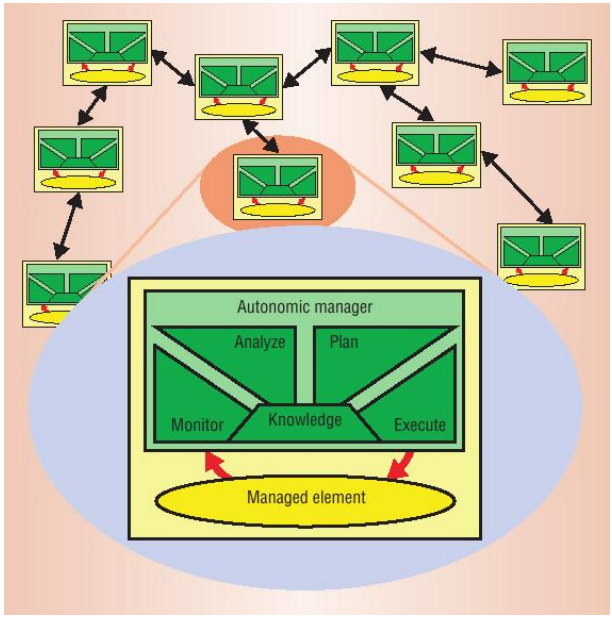



Abbildung 5.4: Struktur eines selbstverwaltenden Elements [2]

Das verwaltete Element kann dabei zum Beispiel eine Hardware- oder eine Software-Komponente sein. Aber es kann auch ein E-Utility (eine Applikation mit einem Abrechnungsdienst) oder ein Applikationsservice sein.

## 5.4 Risiken und Vorteile

Selbstverwaltende Computersysteme bieten Chancen und Risiken. Fehler im System können gravierende Auswirkungen haben. Andererseits sollen selbstverwaltende Computersysteme die Arbeit erleichtern und die Produktivität erhöhen. Dieses Kapitel bietet einen Einblick in die Risiken und die neuen Möglichkeiten.

### 5.4.1 Risiken

#### Sicherheit

Ein wichtiger Punkt in der Sicherheit eines selbstverwaltenden Computersystems ist die Fähigkeit, Eindringlinge zu entdecken. Dies bezieht sich sowohl auf Software-Angriffe, wobei ein Element eines Systems von Angreifern besetzt und für deren Zwecke missbraucht wird, als auch auf Hardware-Angriffe, sprich das Einschleusen eines eigenen Computers in das System. In Abwesenheit menschlicher Kontrollen werden selbständige Systeme, so genannte Intrusion Detection Systems (IDS), wichtiger Bestandteil der Sicherheitsstrategie.

Eindringlinge sind deshalb besonders gefährlich, da sie in der Regel als menschliche Spieler gegen einen Computer antreten. Dies ist zu vergleichen mit einem Schachcomputer, der lediglich auf Datenbanken bekannter Spielzüge zurückgreifen kann, während der Mensch in der Lage ist, neue Züge zu generieren. Da jedoch Schachcomputer unterdessen mit Menschen mithalten können, besteht einerseits Hoffnung auf akzeptabel verlässliche Intrusion Detection. Andererseits gibt es im Schach eine endliche Menge an möglichen Spielvarianten, während die einer ständigen Veränderung unterworfene Computerlandschaft praktisch unabzählbar unendlich viele Angriffsmöglichkeiten bietet. Da ohne künstliche Intelligenz ein sich selbstverwaltendes Computersystem immer nur auf einprogrammierte Muster reagieren kann, unterliegt es gewissen Beschränkungen, wie fehlende Kreativität und Intuition. Auch wenn sich unter Umständen durch emergentes Verhalten eine künstliche Intelligenz herauskristallisieren kann, ist ein solches System einem menschlichen Gegenüber in neuartigen Angriffsszenarien unterlegen, sobald Heuristiken zur Angriffserkennung keine Wirkung zeigen. Einige Angriffsszenarien durch Viren behandelt der Abschnitt über Selbstschutz.

Aufzuspüren sind Angriffe dadurch, dass Komponenten oder Elemente eines Computersystems versagen oder fehlerhaft arbeiten. Jedoch besteht auch die Möglichkeit, dass ein Ausfall oder eine Fehlfunktion auf einen technischen Systemfehler zurückzuführen ist. Normale Systemfehler, beispielsweise durch Hardwaredefekte oder fehlerhafte Software, führen zumeist zu einem einmaligen Fehlverhalten und sind recht zufällig. Ein Angriff hingegen erfolgt gezielt und kann im optimalen Fall das Fehlverhalten mehrfach auslösen. Andererseits folgt ein Systemfehler zumeist bestimmten regelmässigen Mustern, während ein Angreifer seine Spuren zu verwischen und verharmlosen versucht. Deshalb sind Systeme zur Erkennung und Entdeckung von Angriffen niemals zu hundert Prozent verlässlich und werden immer false negatives oder auch false positives produzieren. Ihre Hauptaufgabe besteht darin, die Zeit zwischen dem Eindringen und der Entdeckung möglichst zu verkürzen und zu versuchen, geeignete Gegenmassnahmen zu ergreifen. Als erste Gegenmassnahme müssen betroffene Systemteile und Elemente an Kommunikation nach aussen gehindert werden. Ist dies nicht möglich, so müssen sie ganz deaktiviert werden. Anschliessend ist Wiederherstellung notwendig. Für Daten, und insbesondere für sensitive Daten, ist es wichtig, Korruption zu entdecken und zu beheben. Optimal für Datenhaltung sind also verteilte, redundante Datenspeicher. Die Datenintegrität wird am Besten durch Verschlüsselung geschützt. [10]

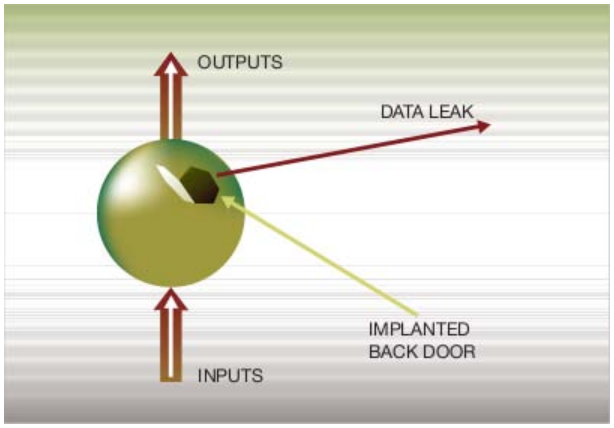



Abbildung 5.5: Backdoor in funktionaler Einheit [10]

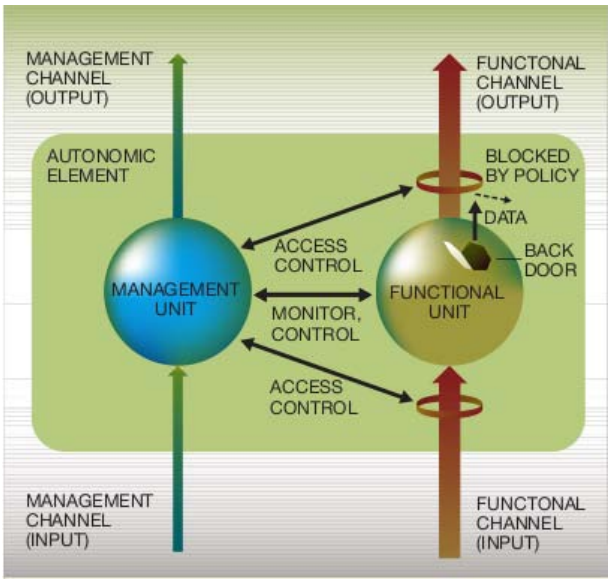



Abbildung 5.6: Backdoor in selbstverwaltendem Computersystem [10]

Ein geeignetes Mittel zur Entdeckung von Eindringlingen sind Mobile Agenten. Dabei handelt es sich um Programme, welche selbständig von einem Element eines selbstverwaltenden Computersystems zum nächsten wechseln und dort weiter ausgeführt werden können [5]. Sie laden Schemadefinitionen aus verteilten Datenbanken und verteilen sich zufällig über das gesamte System. Ihre Vorteile sind die zentrale Konfigurierbarkeit, da nur die Datenbankeinträge aktualisiert werden müssen und der ressourcenschonende Umgang im Gegensatz zu einem statischen System. Mobile Agenten sind nicht permanent auf jedem autonomen Element aktiv, sondern nur auf einigen wenigen. Im Gegensatz dazu ist ein statisches System permanent auf sämtlichen Elementen aktiv und beansprucht dort Speicher sowie Rechenzeit.

Durch die neuartige, erweitere Architektur der Elemente von selbstverwaltenden Computersystemen sind jedoch auch weitergehende Sicherheitsmassnahmen möglich. Jedes selbstverwaltende Element besteht aus einer funktionalen und einer verwaltenden Einheit. Die verwaltende Einheit kontrolliert die Datenflüsse der funktionalen Einheit und

gestattet oder verbietet anhand von Sicherheitspolicen die Kommunikation. Konnte eine Backdoor, sprich eine versteckte Zugriffsmöglichkeit aufgrund von Softwarefehlern oder als Folge von erfolgreichen Angriffen, in einer funktionalen Einheit eines herkömmlichen Computersystems bisher zu einem Datenleck führen ‘(siehe Grafik 5.5), so wird dies im selbstverwaltenden Computersystem verhindert ‘(siehe Grafik 5.6). Es ist jedoch besonders wichtig, dass die Verwaltungseinheit und die Policendatenbank gut gegen Manipulation geschützt werden. Gelingt es einem Angreifer die Police zu verändern, so dass seine Kommunikation erlaubt wird, dann wird das System die ganzen verfügbaren Ressourcen aufbieten um sicherzustellen, dass die Informationen an den Eindringling geliefert werden können.

Das System der Sicherheitspolicen ist jedoch sehr komplex und aufgrund der hohen Datenmenge vom Menschen kaum überschaubar. Insbesondere kann hier schnell eine grosse Datenmenge anfallen, da jede in Betracht kommende Möglichkeit der Kommunikation und des Datenflusses per Policen abgedeckt werden muss. Die Generierung und Verwaltung der Policen muss deshalb rasch dem System selbst überlassen werden. [10]

### Patch Management

Auch für selbstverwaltende Computersysteme sind Programmierfehler ein Problem. Treten durch Programmierfehler Sicherheitslücken auf, so ist das System weitgehend machtlos. Deshalb ist auch in den Rechenzentren der Zukunft das Einspielen von Patches und aktualisierten Versionen einer Software enorm wichtig. Der Vorteil eines automatisch ablaufenden Patch-Vorgangs liegt klar auf der Hand: Die Aktualisierung der Software geschieht viel schneller, als wenn sie erst vom Administrator angestossen werden muss. Dies kann sehr wertvoll sein, werden die Intervalle zwischen Bekanntwerden einer Sicherheitslücke und dem Auftauchen erster Schadsoftware doch immer kürzer [30]. Die Systeme müssen folglich auch die Fähigkeit haben, selbständig Informationen über Sicherheitslücken und Aktualisierungen für die auf ihnen laufenden Programme zu beziehen. Dies kann beispielsweise durch zentrale, maschinenlesbare Newsticker erfolgen. Der Updateserver stellt hier einen Newsticker bereit, welcher vom Clienten in regelmässigen Zeitintervallen abgefragt wird. Updatebenachrichtigungen können aber auch per Abonnement-System, in welchem der Server die registrierten Clienten direkt benachrichtigt, herausgegeben werden. Voraussetzung ist hier, dass die zu benachritigenden Clienten dem Server bekannt sind, während bei einem Newsticker die Clienten anonym bleiben.

### Ausfälle

Geht ein selbstverwaltendes Computersystem von falschen Annahmen über sich selbst oder seine Umgebung aus, kann es zu Störungen, Performanceeinbrüchen bis hin zu Ausfällen kommen. Falsche Annahmen treffen kann es aufgrund von fehlerhaften Datenbeständen, falschen Angaben des technischen Personals oder auch durch fehlerhafte Algorithmen zur Bestimmung des aktuellen Zustandes. Erkennt das System nicht selbst, dass seine Optimierungsversuche die Lage verschlechtern statt zu verbessern, kann dies zum

Zusammenbruch führen. Werden nicht rechtzeitig Gegenmassnahmen ergriffen, muss eine Unternehmung, die auf selbstverwaltende Computersysteme setzt mit Einbussen in der Produktivität rechnen. Vermutlich die grösste Ausfallgefahr geht von kaskadierenden Ausfällen aus, wenn ein oder mehrere Elemente abstürzen und weitere Teile des Systems mit sich reissen.

#### Administrative Flexibilität

Zwar sollen selbstverwaltende Computersysteme den Administratoren das Leben vereinfachen. Doch wenn das System Fehler macht oder sich anders verhält als sich der Techniker dies vorstellt, so wird der Techniker versuchen, das Systemverhalten wieder zu korrigieren. Bieten die selbstverwaltende Computersysteme nicht genügend komfortable Möglichkeiten zu manuellen Eingriffen, kann sich daraus ein Wartungsalbtraum ergeben, der den Techniker unter Umständen mehr Zeit kostet, als er für eine manuelle Konfiguration von Beginn weg gebraucht hätte.

#### Verlust der Kontrolle

Doch nicht nur ein Mehraufwand für Administratoren kann sich daraus ergeben. Gemäss dem Plan von IBM soll in den Unternehmungen kein Techniker mehr notwendig sein, da sich das System selbständig um solche Aufgaben kümmern soll. Doch was soll der IT-Verantwortliche nun unternehmen, wenn das System sich nicht gewünscht verhält oder ausfällt? Diese Frage können oder wollen die Verfechter von selbstverwaltenden Computersystemen, allen voran die Forscher von IBM, bislang nicht beantworten. Das Problem hierbei ist natürlich auch, dass sich die Frage noch nicht richtig stellen lässt, solange jegliche Erfahrungen mit solchen Systemen fehlen.

### 5.4.2 Vorteile

Aus selbstverwaltenden Computersystemen verspricht man sich grosse Vorteile. Vor allem aber auch den Nutzen der IT-Technologie und deren Vernetzung beizubehalten.

Wie in vielen Bereichen der „traditionellen“ Industrie wurde dieser Schritt der Automatisierung schon erfolgreich durchgeführt und so war es möglich der Komplexität einzelner Abläufe entgehen zu können. Auch selbstverwaltende Computersysteme haben zum Ziel, sich von der Komplexität der Systeme zu entlasten. So ist es möglich sich auf neue Herausforderungen zu konzentrieren. Die Entlastung bedeutet für Administratoren auch mehr Zeit sich der Zielvorgabe eines Systems zu widmen. So wird die Zeit nicht mehr nur für die Funktionsfähigkeit eines Systems aufgewendet, sondern für die optimale, businessorientierte Anpassung des Systems.

Durch das Automatisieren werden viele Fehler vermieden, die durch gestresste Systemspezialisten unbemerkt ausgelöst werden. Auch Auswirkungen auf Veränderungen können besser und schneller abgefangen werden und führen so zu stabileren Umgebungen. Die

Ausfallsrate nimmt somit drastisch ab und eine negative Auswirkung auf den Erlös ist abwendbar.

Beim Testing verspricht man sich weitere Vorteile, denn hier werden sich Veränderungen zeigen. So muss eine neue Komponente nicht mehr in einer isolierten Umgebung getestet werden, sondern wird direkt in das aktive System eingebunden. Dies ist ein Vorteil, weil Testumgebungen teilweise nicht identisch mit der aktiven Umgebung sind und dadurch nicht vollständig getestet werden können. Demzufolge können noch unbekannte Wechselwirkungen in der aktiven Umgebung auftreten, die zu Problemen führen. Nach dem Paradigma von selbstverwaltenden Computersystemen werden selbstverwaltende Elemente eingespiesen, die durch die selbstkonfigurierende Charakteristik des Systems sich selbständig nahtlos in das System einfügen können. So kann eine Kostenreduktion erreicht werden, da grosse Teile des Testings entfallen.

Durch Wegfall eines grossen Teils des technischen IT-Personals sollen Unternehmen Kosten sparen können. Da selbstverwaltende Computersysteme aber auch in Richtung Outsourcing tendieren, muss möglicherweise nicht mehr eine grosse Infrastruktur gekauft werden. Stattdessen mietet man die benötigten Ressourcen gemäss dem anfallenden Bedarf.

## 5.5 Verwirklichung von selbstverwaltende Computersysteme

Selbstverwaltende Systeme können nicht abrupt eingeführt werden, dafür empfiehlt IBM eine Evolution des Systems anzustreben. So kann die Durchführung dieses Ansatzes fliessend ermöglicht werden. Für die Realisierung muss auch der Aspekt der Standards berücksichtigt werden, hierfür werden Problematik und Standardisierungsbestreben nachfolgend aufgeführt.

### 5.5.1 Evolution

Der Übergang zu selbstverwaltenden Computersystemen soll nicht eine Revolution sondern eine Evolution sein [4]. Statt einem schlagartigen Austausch aller Komponenten sollen existierende Systeme durch Softwareaktualisierungen und neue Programme schrittweise vom konventionellen zum selbstverwaltenden Zusammenarbeiten überführt werden. Deshalb hat IBM den Weg zu selbstverwaltenden Computersystemen in fünf Stufen eingeteilt und dafür Charakteristiken festgelegt. Diese Stufen beinhalten keinen Zeitplan, sondern sehen nur fliessende Übergänge durch Fortschreiten der Technik vor. Einen raschen Überblick, wie dieses Voranschreiten erfolgen soll, zeigt die Grafik „Stufen der selbstverwaltenden Computersysteme„ , welche im weiteren etwas erläutert werden soll.

Im ersten Evolutionslevel wird jedes Systemelement einzeln verwaltet. Die bedeutet einen hohen Aufwand für das IT-Personal für die Überwachung und Instandhaltung der Infrastruktur. Üblicherweise müssen die zuständigen Personen die Systeme lokal überwachen

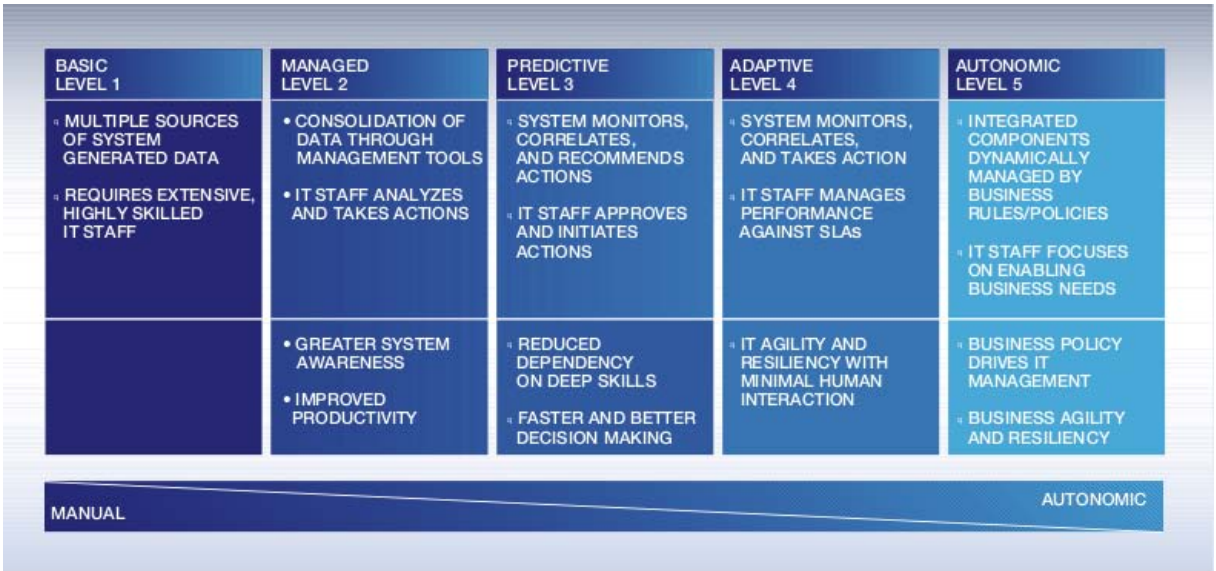



Abbildung 5.7: Stufen der selbstverwaltenden Computersysteme [4]

und können auf Probleme nur reagieren. Das Personal muss tiefere Kenntnisse der verwendeten Plattformen und Produkte haben und lokal verfügbar sein. Wichtigstes Instrument zur Leistungsbewertung ist die Zeit, bis Probleme behoben und Aufträge erfüllt sind.

Im zweiten Evolutionslevel, dem „Managed Level„ , werden über Verwaltungswerkzeuge Informationen konsolidiert gesammelt und ausgewertet. Logdaten werden also zentral gespeichert und von spezieller Software derart aufbereitet, dass sie essenziellen Fakten vom Techniker innert kürzester Zeit erfasst werden können. Statt auf für jeden Server und für jeden Dienst einzelne Logfiles zu betrachten, genügt nun für die häufigsten Fälle ein Blick in die zentrale Auswertung. Die Systemelemente bieten grundlegende Möglichkeiten der Selbstüberwachung. Last wird verteilt, Angreifer erkannt und Software automatisiert installiert. Als Bewertungsinstrumente dienen die Systemverfügbarkeit und die Zeit zur Behebung von Trouble-Tickets. Entsprechend konzentrieren sich die Administratoren auf die Automatisierung von Installationen und Leistungsmanagement um Ausfallzeiten möglichst kurz zu halten. Die meisten Systeme befinden sich heute zwischen dem ersten und zweiten Level.

Der dritte Evolutionslevel, der „Predictive Level„ , zeichnet sich dadurch aus, dass die Systeme beginnen selbständig Muster zu erkennen und dem administrierenden Personal Vorschläge zur Konfiguration unterbreitet. Die Kenntnisse des IT-Personals werden breiter aber weniger tief. Die Zufriedenheit der Anwender wird ein immer wichtigeres Instrument der Bewertung. In Echtzeit kann das gegenwärtige Leistungsverhalten angezeigt und für die Zukunft errechnet werden. Ständig wiederkehrende Routinearbeiten werden vollautomatisiert ausgeführt. Die plattformunabhänige und -übergreifende Kommunikation gewinnt entscheidend an Bedeutung. Durch Globalisierung und weltweite Verknüpfung müssen IT-Systeme nun permanent verfügbar sein. Erste Schritte für diesen Level sind bereits gemacht.

Durch Reifung der Software und hohe Zuverlässigkeit der vom System errechneten Konfigurationsvorschläge, kann in den vierten, den „Adaptive Level„ , übergegangen werden.

Die Systeme setzen ihre Konfigurationsvorschläge nun selbständig um und treffen Entscheidungen anhand ihres Wissens über aktuelle Systemvorgänge. Das IT-Personal wird kleinere Eingriffe in die Ressourcen-Policen vornehmen und so das Systemwissen ergänzen. Die Ressourcenverwaltung wird so durch System und Techniker gemeinsam optimiert. Für das IT-Personal gewinnt Kenntnis über die Betriebsabläufe ständig an Bedeutung. Da die IT immer entscheidender in Betriebsabläufe eingreifen wird, kann ein gut optimiertes EDV-System den Geschäftserfolg stark beeinflussen.

Um nun als selbstverwaltendes Computersystem zu gelten, muss sich im fünften Evolutionslevel das System vollständig selbst an die Ziele anpassen. Das IT-Personal wird dem System lediglich neue Ziele vorgeben müssen.

Zusammenfassend kann also gesagt werden, dass mit laufendem Fortschritt dieser Evolution die Systeme immer selbständiger werden, während das zuständige Personal immer weniger technische dafür mehr betriebswirtschaftliche Kenntnisse besitzen muss. [4] Das hier referenzierte Dokument stammt aus dem Jahre 2003. In den drei Jahren bis heute sind erstaunlich grosse Fortschritte in Richtung des selbstverwaltende Computersysteme gemacht worden. Kann diese Geschwindigkeit beibehalten werden, ist es durchaus denkbar, dass Computersysteme schon in absehbarer Zeit weitgehend selbständig agieren können.

### 5.5.2 Standards

Für die Realisierung der Vision der selbstverwaltenden Computersysteme ist eine strikte Einhaltung von Standards notwendig. In einem selbstverwaltendem Computersystem interagieren verschiedensten Elemente miteinander. Eine so hoch heterogene Umgebung muss sich auf gemeinsame Standards einigen um eine Zusammenarbeit garantieren zu können.

Hier muss unbedingt erwähnt werden, dass sich die Standards zu selbstverwaltenden Computersystemen über viele Gebiete der Informatik hindurch erstrecken, bspw. im Gebiet der Sicherheit, Datenformat, Richtlinien, usw. Die Frage zu, wer für diese Standardisierung zuständig ist bzw. sein wird drängt sich auf. Soll dies anhand einer Unterteilung pro Gebiet geschehen? Werden diese Organisationen auch die Ziele der selbstverwaltende Computersysteme verfolgen? Oder ist es besser eine ganzheitliche Standardisierung unter der Vision der selbstverwaltenden Computersysteme anzustreben? Sollen offene oder proprietäre Standards angewendet werden? Eine Regelung in dieser Hinsicht ist heute noch nicht abzuschätzen.

Es folgt eine Auswahl der existierenden und entstehenden Standards, die für selbstverwaltende Computersysteme relevant sind.

#### Distributed Management Task Force (DMTF)

**Common Information Model (CIM)** : beschreibt Standards für das Management von IT-Systemen, Netzwerke, Anwendungen und Dienste. CIM stellt vor allem für verteilte Anwendungen einheitliche Managementschnittstellen zur Verfügung. [14]

Die Applications Working Group, Utility Computing Working Group und Server Management Working Group entwickeln jeweils Standards für CIM, die für die Autonomic Computing Initiative von grosser Bedeutung sind.

**Internet Engineering Task Force (IETF)**

**Policy - Core Information Model (RFC3060)** : ist das Objekt-orientierte Informationsmodell für das Abbilden von Richtlinieninformation. Zusätzlich dient Policy - Core Information Model als Erweiterung zu CIM. [15]

**Simple Network Management Protocol (SNMP)** : SNMP dient der Überwachung und Steuerung von Netzwerkelementen. Die Kommunikation zwischen der zentralen Überwachungsstation und der überwachten Geräte wird mittels SNMP geregelt.

**Dynamic Host Configuration Protocol (DHCP)**

**Domain Name System (DNS)**

**Lightweight Directory Access Protocol (LDAP)**

**Kerberos**

**Organization for the Advancement of Structured Information Standards (OASIS)**

**Web Services Security (WS-Security)** : liefert die technischen Grundlagen für die Umsetzung von Sicherheitsfunktionen, wie z. B. Integrität und Vertraulichkeit in Nachrichten. [16]

**Web Services Distributed Management (WS-DM)** : definiert eine Webdienste Architektur fürdie Verwaltung von verteilten Ressourcen. [16]

**Web Services Resource Framework (WS-RF)** : definiert ein offenes Framework für die Modellierung und Zugriff der Ressourcen über Webdienste. [16]

**Web Services Notification (WS-N)** : ermöglicht Webdienste Informationenuntereinender auszutauschen. [16]

**Java Community Process**

**Java Management Extensions (JSR3, JMX)** : stellt eine Management Architektur, APIs und Dienste bereit, die für das Erstellen von webbasierte, verteilte, dynamische und modulare Lösungen für das Verwalten von Java Ressourcen dienen. [17]

**Logging API Specification (JSR47)** : definiert APIs für Fehler-und Ablaufverfolgungsprotokollierung. [17]

**Java Agent Services (JSR87)** : definiert eine Menge von Objekte und Dienstschnittstellen,die Einsatz und Betrieb von selbst verwaltende Agenten unterstützen. [17]

**Portlet Specification (JSR168)** : definiert APIs für Portalcomputing in Bezug auf die Gebiete Aggregation, Personalisierung, Darstellung und Sicherheit. [17]

**Storage Networking Industry Association (SNIA)**

**Storage Management Initiative Specification (SMI-S)** : entwickelt und standardisiertinteroperable Speicherverwaltungstechnologien. [18]

**Global Grid Forum (GGF)**

**Open Grid Services Architecture (OGSA)** : beschreibt eine Architekturfür eine dienstorientierte grid computing Umgebung, die im Unternehmen wie auchin der Wissenschaft eingesetzt wird. [19]

**Grid Resource Allocation Agreement Protocol (GRAAP-Working Group)** : beschreibt ein geeignetesRessourcenverwaltungsprotokoll für Grid Umgebungen, die die Vorreservierung derRessourcen erlaubt. [19]

**The Open Group**

**Application Response Measurement (ARM)** : beschreibt eine allgemeine Methode für die Integrierung von Unternehmensanwendungen als verwaltbare Einheiten. Der ARM-Standard erlaubt Benutzern, ihre Unternehmensführungsinstrumente zu erweitern, sodass eine Ende-zu-Ende Verwaltungsfähigkeit entsteht, welche sich aus Messungen der Anwendungsverfügbarkeit, Anwendungsleistung, Anwendungsnutzung und Ende-zu-Ende Abwicklungszeit, zusammensetzt. [20]

## 5.6 Existierende Komponenten

Neben den zuvor aufgeführten Standards weisen wir nun kurz auf zwei Gruppen bereits existierender Komponenten hin. Jedoch müssen für die tauglichkeit in selbstverwaltenden Computersystemen noch Verbesserungen vorgenommen werden, welche Gegenstand aktueller Forschungen und Industriebemühungen sind.

### 5.6.1 Routingprotokolle

Selbstverwaltende Computersysteme müssen intelligente Routing-Protokolle beherrschen, da eine funktionierende Vernetzung der Elemente existenziell ist. Einzelne Verbindungen dürfen nicht überlastet werden, eine ausgefallene Verbindung muss durch ein redundantes System ersetzt werden können. Schliesst sich ein Computer einem Netzwerk an und muss eine bandbreitenintensive Operation durchführen, so kann dies zur Überlastung des Netzwerks führen. Sinnvoller ist es, erst zu prüfen und eine Statistik zu erstellen oder vom

System zu erfragen, wann der Link wenig belastet ist und erst zu einem solchen Zeitpunkt das Netzwerk für sich selbst zu beanspruchen.

### 5.6.2 Verschlüsselung und Zertifikate

Datensicherheit und -Integrität wird in selbstverwaltenden Computersystemen eine stärkere Betonung erhalten müssen, als dies in heutigen Systemen der Fall ist. Kommunikation sollte möglichst nur verschlüsselt erfolgen, wobei sich die Kommunikationpartner über Zertifikate gegenseitig ihre Identität beweisen. Mittels Trusted Computing und dem TPM können fälschungssichere Zertifikate generiert und sicher gespeichert werden [27], [26]. Zusätzlich sind auch die heute schon genutzten Möglichkeiten der hierarchischen Zertifikatsherausgeber [28] oder alternativ der dezentralen Trust-Webs möglich. In letzterem bürgt ein Element des Systems für andere Elemente [29].

### 5.6.3 Persönliche selbstverwaltende Computersysteme

Aktuelle Betriebssysteme für den Desktop bieten grundlegende selbstverwaltende Eigenschaften, jedoch sind diese noch stark lokal beschränkt. Einige unterstützen den Administrator, wiederum andere erhöhen die Produktivität des Anwenders. In der Folge werden einige selbstverwaltende Verhaltensweisen aufgezählt, welche von heute genutzten Betriebssystemen, insbesondere Windows XP oder erweiternder Software geboten werden. Viele dieser Fähigkeiten zur Selbstverwaltung erhalten die Systeme durch Implementierung von oben erwähnten Standards.

Mittels Imaging-Software kann ein Administrator eine Betriebssystem-Installation vorkonfigurieren und verteilen. Da das System-Image auch nachträglich noch angepasst werden kann, besteht die Möglichkeit dies für einzelne Nutzer oder ganze Gruppen zu personalisieren. Mittels Update-Software kann das Betriebssystem sowie darauf installierte Software auf dem aktuellen Stand gehalten werden. Dies funktioniert schon mit dem in Windows integrierten Tool zumeist zuverlässig. Über eigene Updateserver kann eine Unternehmung jedoch bestimmte Updates zurückhalten oder zusätzliche Updates einspielen lassen. Schlägt ein Update fehl und versetzt das System in einen nicht funktionsfähigen Zustand, so kann wieder auf eine zuvor festgelegte Konfiguration zurückgeschritten werden. Dazu wird mittels spezieller Software auf einer versteckten Partition der Festplatte ein komplettes Abbild der Installation angelegt. Über weitere Software können auch Gerätetreiber sowie Firmware aktualisiert werden.

Über das Dynamic Host Configuration Protocol (DHCP) und Domain Name System (DNS) können einige Kommunikationsfunktionen automatisiert werden. Ein Computer kann sich dadurch zum Teil selbständig konfigurieren und in ein Netzwerk eingliedern. Leider bietet DHCP nur eine ungenügende Anzahl Konfigurationsparameter. Einstellungen für Mailserver, Proxyserver, sowie Sicherheitseinstellungen zum Beispiel für VPNs oder für drahtlosen Zugang müssen meistens noch immer manuell vom Benutzer vorgenommen werden. Alternativ kann innerhalb eines Netzwerksegmentes über Broadcasts oder Multicast DNS nach Ressourcen wie Druckern, Scannern oder Dateifreigaben gesucht

werden. Für grössere Netze ist dies jedoch aufgrund des hohen Netzwerk-Overheads eine ungeeignete Lösung und sollte über ein erweitertes Protokoll zur Netzwerkkonfiguration zentralisiert erfolgen.

Windows kann das Benutzerinterface selbst optimieren, so werden zuletzt genutzte Programme in einer gesonderten Ablage angezeigt. Dadurch kann der Benutzer sehr schnell wieder darauf zugreifen. Windows verfolgt auch die Benutzung von Desktop-Objekten und bietet ein regelmässiges Aufräumen an, jedoch wird dies von vielen Anwendern als störend erachtet. Fenster in der Taskbar werden bei Bedarf zusammengefasst. Dies spart Platz und erhöht die Lesbarkeit und Aussagekraft der Fenstertitel. Nachteil ist eine allenfalls reduzierte Übersichtlichkeit, da nicht mehr ständig sämtliche Fenster über einen Klick zu erreichen sind. Zusatzsoftware kann die Festplatte defragmentieren und die Daten umstrukturieren, so dass häufig genutzte Dateien physisch so angeordnet werden, dass ein beschleunigter Zugriff erfolgt. Es ist jedoch zu bedenken, dass dieser Vorgang selbst relativ viele Ressourcen beansprucht und während der Defragmentierung oft nur ein langsameres oder gar eingeschränktes Arbeiten möglich ist.

Selbstschutz ist ein wichtiger Aspekt selbstverwaltender Computersysteme. Primäres Schutzziel sind die Benutzerdaten. Diese sind anfällig gegen Benutzerfehler, Systemversagen und Angriffe von aussen. Es gilt sowohl die Integrität als auch den Zugriff zu schützen. Backups sind deshalb unumgänglich wobei viele Backup-Methoden und -Programme existieren. Backups können periodisch zu bestimmten Zeitpunkten ausgeführt, vom Benutzer manuell angestossen oder proaktiv als Reaktion auf Systemereignisse, wie beispielsweise einem angehenden Festplattendefekt, ausgelöst werden. Backups können lokal, beispielsweise auf ein wiederbeschreibbares optisches Medium oder auf über das Netzwerk auf einem räumlich entfernten Server angelegt werden. Für Kommunikation und Speicherung von Daten ist Verschlüsselung ein weiteres Beispiel einer proaktiven Datenschutzmassnahme. Moderne Desktop-Betriebbsysteme bieten transparente Verschlüsselung von Dateien und Verzeichnissen. Hauptproblem der Verschlüsselung ist die Schlüsselverwaltung. Eine Möglichkeit zur sicheren Schlüsselverwahrung bietet beispielsweise das TPM aus der „Trusted Computing Alliance„ , welches immer öfter in Computern verbaut wird. Jedoch ist bei einer Beschädigung des TPM der Schlüssel und somit die verschlüsselten Daten verloren. [9]

## 5.7 Pläne der IT-Branche zum Thema selbstverwaltende Computersysteme

IBM startete im Oktober 2001 mit der Veröffentlichung eines Manifestes die “Autonomic Computing Initiative“, die Initiative zu selbstverwaltenden Computersystemen. Viele Unternehmen schlossen sich der Idee an oder hatten schon eigene Entwicklungspläne in diese Richtung gestartet. In diesem Kapitel werden einige dieser Ansätze vorgestellt, welche das Bestreben der Branche nach Automatisierung von Aufgaben zeigt.

### 5.7.1 Hewlett-Packard

Hewlett-Packard (HP) kündigte im Dezember 2001 deren neue Vision „Adaptive Infrastructure“ an [21]. Diese soll die sich immer schneller verändernden Geschäftsbedürfnissen unterstützen indem sich Unternehmen jeder Grössen, den Marktkonditionen schneller anpassen können.

Adaptive Infrastructure basiert auf der „Evolution einer virtuellen Daten-Center Architektur, die flexibel, überall vorhanden, kosteneffizient, universell verwaltbar und für Unternehmen jeder Grösse zugänglich ist.“ [21]

Hierfür sind laut HP Innovation in Software und Hardware Technologien erforderlich. HP teilt die bevorstehenden Aufgaben wie folgt auf:

**Virtual Presence and Control** (virtuelle Präsenz und Kontrolle): dies ermöglicht einen sicheren Zugang und Kontrolle zu Computern, Servern und Netzwerkressourcen unabhängig vom Standort.

**Automated System Provisioning** (automatisierte Systemversorgung): Die Entwicklung und Change Management werden automatisiert.

**Intelligent Fault Resilience** (intelligente Fehlerwiderstandsfähigkeit): Systemausfälle vermeiden, durch intelligente Diagnose-, Prognosefähigkeiten, die eine schnelle Reaktion ermöglichen.

**Dynamic Resource Scaling** (dynamische Ressourcenanpassung): Je nach Bedarf von Ressourcen, kann diese in Echtzeit angepasst werden.

### 5.7.2 Sun Microsystems

Sun stellte im Herbst 2002 deren Autonomic Computing Ansatz unter dem Namen N1 vor. N1 ist die Betrachtung der Server, Verbindungen, Speichermöglichkeiten als eine Einheit. Dieser Einheit wird automatisierten Verwaltungsaufgaben übergeben.

Erreichen möchte dies Sun in drei Phasen:

**Phase 1** Virtualisierung der Datencenter, d.h. Computer, Netzwerkelemente, Speicherung bilden einen zusammenfassenden Ressourcenpool. Die Ressourcen werden zentral reserviert, verteilt, überwacht und gemessen.

**Phase 2** Anwendungen werden automatisch bereitgestellt.

**Phase 3** Dynamisches Policy Management, d.h. für bereitgestellte Services können je nach Notwendigkeit Richtlinien gesetzt und angepasst werden, z.B. Unterteilung der Benutzer in Prioritätsgruppen.

Sun befindet sich momentan in Phase 2. Im Mai 2005 wurde die Software N1 Service Provisioning zum Verkauf angeboten, diese ermöglicht laut Sun Microsystems einfache Bereitstellung von Anwendungen und Konfigurationsfehler werden weitestgehend vermieden. Eine Entlastung des Systemadministrators ist in dem Sinne gewährt, dass die Analyse einer Auswirkung nicht mehr aufs kleinste Detail durchgearbeitet werden muss. Die Bereitstellung von Anwendungen verläuft schnell und in wenigen Minuten anstelle von Tagen.

### 5.7.3 CISCO

CISCO entwickelte bereits an einer Adaptive Network Care (ANC) Lösung, als die Autonomic Computing Initiative (ACI) von IBM bekannt wurde. Es konnten Synergien zwischen ANC und ACI festgestellt werden. Dies bewog IBM und CISCO sich zusammen zu schliessen und das Adaptive Services Framework (ASF) zu entwickeln. CISCO und IBM haben in einen Whitepaper das ASF beschrieben. Daraus sind die folgenden Hauptfunktionalitäten entstanden:

- Mechanismen zur Modellierung von Adaptiven Domänen
- Gemeinsames Event Format
- Gemeinsames Format zur Definition von Filtern
- Gemeinsames Format zur Definition von Problemen
- Protokolle durch die Beziehungen der einzelnen Einheiten bestimmt
- Definition von Nachrichtenformaten
- Mechanismen für die Nutzung von Brachenstandards

### 5.7.4 Microsoft

Microsoft vereinte im Jahr 2003 die bis anhin verteilte Management Software Linie unter dem Namen Dynamic Systems Initiative (DSI). Microsoft behält den Focus auf der Software und entwickelt im Bereich der Entwicklungstools, Betriebssysteme, Managementtools und Anwendungen weiter.Wie auch andere Unternehmen setzt Microsoft die Methode Virtualisierung der Datencenter ein.

## 5.8 Relevante Forschungsgebiete

Anhand von Peer-to-Peer Netzwerken wird ein aktuelles Forschungsthema aufgezeigt. Zu Beginn wird Peer-to-Peer kurz präsentiert, anschliessend wird aufgrund von Basis- und Autonomiekriterien die Selbstorganisation von Peer-to-Peer Netzwerken erläutert. Zum Schluss werden anhand eines fiktiven, sich selbstorganisierendes Peer-to-Peer Netzwerkes die potentiellen Möglichkeiten dargelegt.

### 5.8.1 Peer-to-Peer Netzwerke

Als ein Peer-to-Peer (P2P) Netzwerk bezeichnet man die Kommunikation unter Gleichartigen (engl. peer: Ebenbürtiger, Gleichgestellter). Im Gegensatz zum klassischen Client-Server Ansatz, bei dem die Clients auf die Ressourcen des Servers zugreifen, sind in einem P2P-Netzwerk alle Computer gleichberechtigt. Dies bedeutet, dass die Peers gleichzeitig Dienste in Anspruch nehmen, aber auch dass sie Dienste für die anderen Peers zur Verfügung stellen können. Jeder Peer kann so in einem Netzwerk gleichzeitig Server und Client sein.

Es existieren zwei Haupttypen von P2P-Netzwerken:

1. Beim sogenannten **reinen** P2P-Netzwerk sind die Peers sowohl Server wie auch Clients. Daneben existiert kein zentraler Server um das Netzwerk zu überwachen und es existiert kein zentraler Router.

2. In einem **hybriden** P2P-Netzwerk hingegen werden Informationen über die Peers auf einem zentralen Server gespeichert, wobei dieser auf Anfragen der Peers antwortet. Auf den Peers werden die Ressourcen verwaltet und jeder Peer ist selbst dafür verantwortlich dem Server mitzuteilen, welche Ressourcen (z.B. Dateien) den anderen Peers zur Verfügung stehen.

Die Selbstorganisation der Peers ist in einem reinen P2P-Netzwerk absolut essentiell, da es keine zentrale Kontrollinstanz gibt. De Meer und Koppen [8] stellten folgende Kriterien für Selbstorganisation in einem P2P-Netzwerk auf, wobei sie Basiskriterien und Kriterien für Autonomie unterschieden.

Folgend zuerst die Auflistung der Basiskriterien:

- Die **Grenzen** innerhalb eines P2P-Systemes sollten von den Peers selbst festgelegt werden, wobei als Grenze die Möglichkeit des Neueintrittes von Peers in das Netzwerk definiert ist. Peers, welche anderen Peers die Möglichkeit geben, in das Netzwerk einzutreten (oder den Zugang verweigern), werden oft als Bootstrap-Nodes bezeichnet.

- Ein selbstverwaltendes P2P-System kann und muss fähig sein, seine **Struktur nachzubauen**. Dies kann das Hinzufügen, Entfernen oder das Ändern eines Peers, seiner Daten oder seiner Verbindungen oder Beziehungen zu anderen Peers beinhalten. Nachbau muss nicht notwendigerweise bedeuten, dass eine identische Kopie erstellt wird, es kann auch Mutationen beinhalten.

- Ein selbstverwaltendes P2P-System kann und muss fähig sein, seine **Struktur zu ändern**. Als Beispiel sei die Änderung der Verbindungen oder der Zusammenschluss zu einem Cluster erwähnt.

- Ein selbstverwaltendes P2P-System ist in **Form** einer Hierarchie, einer Heterachie oder beidem aufgebaut. Heterachie bezeichnet eine Netzwerkstruktur, die ein grosses

Ausmass an Konnektivität erlaubt und bei der jeder Knoten mit jedem Nachbarsknoten verbunden ist. Die hat Auswirkungen auf die Struktur des Systemes, zum Beispiel ob ein einziger Ausfallpunkt (single-point-of-failure) oder fixe Kommunikationspfade existieren.

- Ein selbstverwaltendes P2P-System sollte in der Lage sein, **Störungen** aus seinem Umfeld wahrzunehmen. Eine solche Störung kann zum Beispiel der Ausfall eines Peers oder eine DoS-Attacke sein.
- Ein selbstverwaltendes P2P-System besitzt die Möglichkeit, auf eine **Störung zu reagieren**. Dies will heissen, dass das System zum Beispiel eine Autorisation der Peers, um gefälschte Inhalte auszusondieren, oder einen redundanten Aufbau des P2P-Systemes vornehmen kann.

Die Kriterien der Selbstverwaltung sind:

- Falls in einem solchen System Störungen auftreten, dann müssen die nicht richtig funktionierenden Komponenten die Möglichkeit besitzen, mit dem restlichen System in einer bidirektionalen Art zu **kommunizieren**.
- Ein selbstorganisiertes P2P-System versteckt die Einzelheiten seines Aufbaues vor seinem Umfeld um die **Komplexität zu reduzieren** (black-box als Beispiel).
- Als Vorausetzung für Kreativität innerhalb eines selbstorganisierenden Systemes ist es notwendig, dass das System **Zufälligkeit** nutzt. Dies erlaubt mit geringem Aufwand die Bildung von neuen Strukturen.
- Ein selbstverwaltendes System befindet sich in einem **kritischen Zustand**. In einem System, in dem eine Ordnung vorhanden ist, sind alle Beziehungen homogen geordnet und stabil, es kann kein unvorhergesehenes Ereignis eintreten. Während in einem System, in dem Unordnung herrscht, es beinahe unmöglich ist, eine Gesetzmässigkeit festzustellen, da bei den sich im System befindlichen Komponenten keine Beständigkeit festgestellt werden kann. Ein kritischer Zustand befindet sich genau zwischen diesen beiden Extremen, wobei ein System, dass sich in einem solchen Zustand befindet, grundsätzlich stabil ist. Es besitzt jedoch die Möglichkeit, sich zu ändern, wobei dabei anfallende Störungen lokal gehalten werden. Ein kritischer Zustand erhöht auch den Flexibilitätsgrad, da das System in der Lage ist, verschiedene Variationen von Störungen zu meistern.

  Ein Beispiel für ein System, welches sich in einem kritischen Zustand befindet, ist das Abelian Sandpile-Modell [24]: In diesem Modell werden wiederholt Sandkörner auf ein **zufälliges** Feld von der Grösse eines *nxn*-Grids geträufelt. Wenn die maximale Aufnahmefähigkeit eines Feldes (z.B. 4) überschritten wird, werden die Sandkörner dieses Feldes gleichmässig auf seine vier Nachbarfelder aufgeteilt, je ein Sandkorn wird den Nachbarfeldern zugewiesen. Auf dem Feld, welches den Vorgang ausgelöst hatte, ist die Anzahl der Sandkörner anschliessend 1 (x-4). Sandkörner, welche den Rand des Grids überschreiten, werden aus dem System entnommen. Simulationen von diesem Modell zeigten, dass in viele Felder eines solchen Systemes sich die Anzahl der Sandkörner zwischen 1 und 3 bewegt. Diese Felder befinden sich in

einem stabilen Zustand, da ein zusätzliches Sandkorn nicht die Struktur des gesamten Systemes verändern würde. Aber es existieren einige Felder mit der kritischen Grösse von 4. In diesen Feldern würde ein zusätzliches Sandkorn eine Strukturveränderung hervorrufen. Unter der Annahme, dass neue Sandkörner zufällig verteilt werden, ist die Wahrscheinlichkeit, dass ein Feld mit einer nicht-kritischen Grösse von einem Sandkorn getroffen wird, grösser als die Wahrscheinlichkeit, dass ein Feld mit einer kritischen Grösse getroffen wird. Dies führt dazu, dass die Kombination von kritischen und nicht-kritischen Feldzuständen mit der zufälligen Verteilung der Sandkörner zu einem mehrheitlich stabilen System führt.

- Ein selbstverwaltendes P2P-System zeichnet sich des weiteren durch **emergentes Verhalten** aus. Das bedeutet, dass es Eigenschaften aufweisen kann, welche zu Beginn nicht geplant/vorhanden waren, sondern sich im Laufe der Zeit herauskristallisiert haben. Emergenz ist per Definition nicht in einem individuellen Teilsystemen enthalten, sondern bildet sich aus der Interaktion der verschiedenen Komponenten heraus.

Zusammengefasst kann man sagen, dass die heutigen P2P-Systeme wie eDonkey oder Gnutella einige dieser Kriterien teilweise erfüllen, jedoch stellt sich die Frage, ob überhaupt mehr Selbstorganisation erforderlich ist. So wie es jedoch aussieht, ist dies der Fall: ein P2P-Netzwerk, welches sowohl die Basis-, wie auch die Autonomie-Kriterien erfüllt, würde sämtliche Nachteile heutiger P2P-Netzwerke aufwiegen. Der Eintritt in ein solches Netzwerk könnte von den einzelnen Peers dynamisch ermittelt werden, was sich vor allem bei einer hohen Fluktuation der Peers als Vorteilhaft erweisen würde. Aber auch die dadurch gegebene Möglichkeit, dass jeder Peer entscheiden kann, ob ein neuer Peer eintreten darf, würde den Aufbau eines robusten Netzwerkes erlauben, was wiederum die Gefahr des Ausfalls von strategischen Knoten verringert. Da hier die Kommunikation der einzelnen Peers von elementarer Wichtigkeit ist, müsste eine intelligente Möglichkeit des Informationsaustausches vorhanden sein. Dies wiederum würde zwangsläufig auf die Möglichkeit der Selbstkonfiguration hindeuten, da durch diesen Austausch von Informationen die Peers in der Lage wären, sich selbst und andere, abhängig von den äusseren, dynamischen Umständen, zu konfigurieren. Der Bedrohung durch das Einschleusen von korrupten Daten in das Netzwerk könnte durch Selbstheilung entgegengewirkt werden, wobei zum Beispiel in dem erwähnten Informationsaustausch auch Auskünfte über vorhanden Daten inklusive einer Möglichkeit der Integritätsprüfung vorhanden wären. Damit könnte ein solcher Peer erkennen, dass einzelne seiner angebotenen Daten korrumpiert wären (vorausgesetzt der Peer selbst ist vertrauenswürdig). Diese Informationen würden redundant im Netzwerk verteilt werden und mindestens jeder Peer, welche entsprechende korrupte Daten anbietet, müsste über diese Information verfügen. Gesetzt den Fall, dass trotzdem korrupte Daten im Netzwerk vorhanden wären, könnte, sobald diese als nicht erwünschte Daten identifizert werden, mittels des Informationsaustausches den anderen Peers mitgeteilt werden, dass es diese Daten nicht mehr weiter verbreitet werden. Dieser Selbstschutz-Mechanismus könnte noch weitergehen und zum Beispiel auch Peers abfangen, welche selbst keine Daten weiterverbreiten, sondern nur von anderen Peers Daten herunterladen (sogenannte Freeriders).

Einem weiteren Problem von klassischen P2P-Netzwerken könnte auch Einhalt geboten werden: da Daten über mehrere Computer verteilt sind, kann es schwierig sein, von diesen

eine Sicherung anzulegen. Sich selbstverwaltende Peers könnten die Möglichkeit besitzen, selbständig zu erkennen, wann gewisse Daten nicht mehr hinreichend zur Verfügung gestellt werden und beginnen, diese im Netzwerk weiterzuverbreiten.

Wie an diesen Beispielen zu erkennen ist, bauen die einzelnen Elemente vor allem auf dem Informationsaustausch zwischen den Peers auf. Dies kann man in Analogie zu den selbstverwaltenden Elementen sehen: jeder Peer ist ein solches Element und mittels Kontrollschlaufen interagiert er mit anderen Peers seines Netzwerkes. Dadurch wäre der Informationsfluss, die Ausführung und Kontrolle sowie die Analyse der ausgeführten Aktion gegeben. Dabei sollte die für diesen Informationsaustausch benötigte Ressourcenverwendung (zum Bespiel Netzwerk- und CPU-Auslastung, oder Festplattenkapazität) nicht ausser acht gelassen werden. So wie die aktuelle Forschung zu diesem Thema im Moment aussieht, wird es aber noch ein langer Weg sein, bis ein P2P-Netzwerk über die erforderlichen Eigenschaften für Selbstverwaltung verfügt.

## 5.9 Schlusswort

Die Verfechter der Initiative zu selbstverwaltenden Computersystemen versprechen viel und betreiben einen dementsprechenden hohen Promotionsaufwand. Aber nicht unbedingt mehr als frühere Vordenker der Informatik. Die Hauptidee ist einfach: Der technische Fortschritt soll die Produktivität durch erhöhten Einsatz von Informatikmitteln steigern und das Personal der IT-Abteilungen dennoch entlasten, wobei der wichtigste Punkt die finanzielle Entlastung sein dürfte.

Im Prinzip ist dies nichts Neues, nichtsdestoweniger kann die Idee als Neuerung gelten, denn es wird die gesamte IT-Umgebung als Einheit betrachtet, wobei die gegenseitigen Wechselwirkungen von beispielsweise Applikationen, Server, usw. berücksichtigt werden. Hier zeigt sich auch die Wichtigkeit gemeinsamer Standards, damit ein solcher Ansatz realisiert werden kann. Eines davon ist das Common Information Model (CIM) (siehe Kapitel 1.5.2), welches Managementschnittstellen für verteilte Anwendungen beschreibt, aber auch der Standard für ein gemeinsames Log-Dateiformat sei hier erwähnt. Es bleiben jedoch noch viele ungeklärte Sachverhalte bei den Standards, da viele Fragen nicht beantwortet sind und sich die einzelnen Unternehmungen unter wirtschaftlichen Aspekten nicht zu offenen, gemeinsam verwendeten Standards durchringen werden, bis sich solche zuerst am Markt etabliert haben und die Eintrittsbarrieren für Unternehmungen mit anderen Ansätzen zu hoch sind. Da sich dieser Markt allerdings noch in den Kinderschuhen befindet, wird das nicht allzuschnell von statten gehen.

Bislang liegen teilweise noch Konzepte in unklarer Form vor. Dies zeigt sich täglich sehr drastisch an der Malware/Virenproblematik, welche bis jetzt, trotz den gemeinsamen Anstrengungen von Politik und Wirtschaft, nicht in den Griff zu bekommen waren. Von Selbstschutz kann hierbei noch überhaupt keine Rede sein. So ist auch klar, dass heute betroffenen Personen in dieser Hinsicht dem Konzept von selbstverwaltenden Systemen kritisch und skeptisch gegenüberstehen. Dies wohl nicht zu unrecht.

Aus diesem Grund wird auch von IBM eine Evolution der Systeme vorgeschlagen, damit die fehlenden oder unvollständigen Konzepte mit der Zeit und der Entwicklung der IT-Welt mitgehen und angepasst werden müssen. Ob sich die Evolution so gestalten wird, wie es IBM darstellt, ist nicht klar, denn während in einem Bereich grosse Fortschritte gemacht werden, sind andere noch nicht über das erste Level hinaus gekommen.

Natürlich steht die ganze Idee erst am Anfang und es wurde wenig konkretes realisiert. Was wirklich jemals verwirklicht wird und in welcher Form dies geschieht oder ob sich das ganze in eine komplett neue Richtung entwickelt, wird die Zukunft zeigen.

# Literaturverzeichnis


[1] P. Horn: Autonomic Computing: IBM's Perspective on the State of Information Technology; IBM Corporation, October, 2001, http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf.

[2] J. Kephart, D. Chess: The Vision of Autonomic Computing; IEEE Computer, Vol. 36, No. 1, pp. 41-50, January, 2003, http://www.research.ibm.com/autonomic/research/papers/AC_Vision_Computer_Jan_2003.pdf.

[3] RoboCup 2006 - Bremen / Germany; http://www.robocup2006.org, June, 2006.

[4] A. Ganek, T. Corbi: The Dawning of the Autonomic Computing Era; IBM Systems Journal, Vol. 42, No. 1, 2003, http://www.research.ibm.com/journal/sj/421/ganek.pdf.

[5] Noria Foukia, Jarle G. Hulaas and Jürgen Harms: Intrusion Detection with Mobile Agents; http://www.isoc.org/inet2001/CD_proceedings/Foukia/inet.pdf.

[6] G. Carle, R. H. Katz, B. Plattner, M. Smirnov: Dagstuhl Seminar on Autonomic Networking; Dagstuhl, Germany, January, 2006, http://www.dagstuhl.de/06011/.

[7] E. Gelenbe: User Cooperation and Autonomy in Autonomic Networks; Keynote Speech, Networking Conference, May, 2005, http://www.cs.uwaterloo.ca/conferences/networking2005/coming/keynotes/Gelenbe.pdf.

[8] Ralf Steinmetz, Klaus Wehrle: Peer-to-Peer Systems and Applications, Springer, September, 2005.

[9] D. F. Bantz, S. Mastrianni, C. Bisdikian, A. Mohindra, D. Challener, D. G. Shea, J. P. Karidis, M. Vanover: Autonomic personal computing; IBM Systems Journal, Vol. 42, No. 1, 2003, http://www.research.ibm.com/journal/sj/421/bantz.pdf.

[10] D. M. Chess, C. C. Palmer, S. R. White: Security in an autonomic computing environment; IBM Systems Journal, Vol. 42, No. 1, 2003, http://www.research.ibm.com/journal/sj/421/chess.pdf.

[11] Gordon E. Moore: Cramming more components onto integrated circuits; Electronics, Vol. 38, No. 8, April, 1965, ftp://download.intel.com/research/silicon/moorespaper.pdf.

[12] Nagios; http://www.nagios.org/, June, 2006.

[13] N. Jennings, K. Sycara, M. Wooldridge: A Roadmap of Agent Research and Development; Int. Journal of Autonomous Agents and Multi-Agent Systems, 1998.

[14] Distributed ManagementTask Force (DMTF); http://www.dmtf.org/home; June, 2006.

[15] Internet Engineering Task Force (IETF); http://www.ietf.org/; June, 2006.

[16] Organization for the Advancement of Structured Information Standards (OASIS); http://www.oasis-open.org/home/index.php; Juni 2006.

[17] Java Community Process; http://jcp.org/en/home/index; June, 2006.

[18] Storage Networking Industry Association (SNIA); http://www.snia.org/home; June, 2006.

[19] Global Grid Forum (GGF); http://www.gridforum.org/; June, 2006.

[20] The Open Group; http://www.opengroup.org/; June, 2006.

[21] Compaq Redefines IT Landscape with Adaptive Infrastructure; Houston, December, 2001, http://www.hp.com/hpinfo/newsroom/press/2001pmc/pr2001120501.html?jumpid=reg_R1002_USEN; May, 2006.

[22] Nervensystem; http://www.bbc.co.uk/health/images/300/body_systems.jpg.

[23] IBM: An architectural blueprint for autonomic Computing; White Paper, Third Edition, June, 2005.

[24] P. Bak, C. Tang, K. Weisenfeld: Self-organized Criticality: an explanation of 1/f noise; A Physical Review, Vol. 38, 1987.

[25] Organization for the Advancement of Structured Information Standards (OASIS), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm; Juni, 2006.

[26] Sundeep Bajikar: Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper; http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf; June 2002.

[27] Trusted Computing Group Frequently Asked Questions; https://www.trustedcomputinggroup.org/about/faq; July 2006.

[28] Entrust: Ressources: What is a PKI; http://www.entrust.com/pki.htm; July 2006.

[29] Carl Ellison: Certificate Comparisons; http://world.std.com/~cme/html/web.html; Juli 2006.

[30] Symantec: Internet Security Threat Report - 1. Jahreshälfte 2004; http://www.symantec.com/region/de/PressCenter/Threat_Reports.html.

# Kapitel 6

# NSIS - Signaling in IP Networks

*Matthias Altorfer, Daniel Heuberger, Manuel Innerhofer*

*Die Bandbreite, welche vor allem den Endbenutzern zur Verfügung steht, nimmt stetig zu. Dazu kommen immer mehr Applikationen, die eine hohe Bandbreite benötigen, um überhaupt mit zufrieden stellender Qualität zu funktionieren. Dies stellt Netzwerkadministratoren vor die immer schwieriger werdende Aufgabe, die ständig wachsenden Ansprüche zu berücksichtigen. Gleichzeitig werden die Netzwerke immer komplexer und Datenströme passieren mehrere Domänen. Um diesen Ansprüchen Herr zu werden, wurden über die letzen Jahre die verschiedensten Protokolle entwickelt. Das wohl bekannteste ist RSVP, um Netzwerkressourcen zu reservieren. Im Hintergrund dieser Erfahrungen hat sich die Next Steps in Signaling (NSIS) Working Group gebildet, mit dem Ziel ein IP basiertes Signalisierungsprotokoll zu definieren. Dieses neue Protokoll sollte in der Lage sein, die vielfältigen Ansprüche moderner Applikationen, Netzwerke und Geräte zu erfüllen.*

## Inhaltsverzeichnis

**6.1 Einleitung . . . . . 179**
**6.2 Signalisierungsprotokolle . . . . . 179**
6.2.1 Signalisierungsprotokolle in der Telefonie . . . . . 179
6.2.2 Signalisierungsprotokolle in IP Netzwerken . . . . . 179
**6.3 Das NSIS Protocol Suite Framework . . . . . 180**
6.3.1 Aufgabe des Frameworks . . . . . 180
6.3.2 Die grundlegenden Konzepte des Frameworks . . . . . 180
6.3.3 Das NSIS Schichtenmodell . . . . . 184
**6.4 General Internet Signaling Transport (GIST) . . . . . 188**
6.4.1 GIST Protokoll Stack . . . . . 188
6.4.2 GIST Nachrichten . . . . . 189
6.4.3 GIST Transport Mechanismus . . . . . 191
6.4.4 GIST Zustandsautomaten . . . . . 191
6.4.5 GIST Signaling Application API . . . . . 192
**6.5 QoS NSLP . . . . . 192**
6.5.1 Wozu braucht QoS Signaling? . . . . . 192
6.5.2 QoS NSLP Aufbau und Konzepte . . . . . 193
6.5.3 Beispiele für QoS NSLP Operationen . . . . . 200
6.5.4 QoS NSLP versus RSVP . . . . . 203
**6.6 Fazit . . . . . 204**

## 6.1 Einleitung

Wir starten mit einer Einführung in Signalisierungsprotokolle in der Telefonie sowie auch in IP Netzwerken. Danach wird das NSIS Protocol Suite Framework der Internet Engineering Taskforce mit seinen zwei Schichten, der Signalisierungsschicht NSL und der Transportschicht NTL erklärt. GIST, ein konkreter Implementierungsvorschlag für das NTL Protokoll, wird in einem weiteren Teil beschrieben. Auch auf eine Applikation des NSL Protokolls, auf das QoS NSLP wird detailliert eingegangen. Ein Fazit schliesslich liefert dann die wichtigsten Erkenntnisse dieser Arbeit.

## 6.2 Signalisierungsprotokolle

### 6.2.1 Signalisierungsprotokolle in der Telefonie

In der Telekommunikation wird Signalisierung als Übertragung von Information zu Steuerungszwecken verstanden. Das klassische und wahrscheinlich noch am weitesten verbreitete Beispiel ist die Signalisierung im Telefonnetz. Die konkreten Aufgaben des Signalisierungsprotokolls am Beispiel eines Telefonanrufs können wie folgt beschrieben werden:

- Finden des angerufenen Teilnehmers
- Verbindungsaufbau möglich
- Klingeln
- Schalten der Sprachkanäle
- Freigabe der Sprachkanäle

Diese Aufgaben werden mithilfe von Signalisierungs-Nachrichten wahrgenommen.

### 6.2.2 Signalisierungsprotokolle in IP Netzwerken

Während sich in der Telephonie die Out-of-Band Signalisierungsvariante mit einem eigenen Signalisierungsnetzwerk durchgesetzt hat, wird in IP-Netzwerken ausschliesslich in-band Signalisierung verwendet. Klassische Telefonnetzwerke beschränken sich eigentlich nur auf den Service der Sprachübermittlung. In IP-Netzwerken treffen wir aber eine Vielzahl von möglichen Services mit den unterschiedlichsten Anforderungen in Bezug auf den Datenaustausch und den ihnen benöntigten Ressoucen. Dies führte zum Verlangen nach einem vielseitig einsetzbaren aber doch einheitlichen Signalisierungsprotokoll für IP-Netzwerke. Bekannte Signalisierungsprotokolle wie RSVP [16], SIP [17] oder SIGTRAN [18] wurden jeweils für eine bestimmte Applikation oder einen bestimmten Zweck

entwickelt. Dadurch schränken sie ihre Weiterverwendung ein oder zwingen benutzende Applikationen zu unverhältnismässigen Kompromisse und Anpassungen.

Der Haupttreiber hinter diesem neuen Protokoll sind die sicherlich ständig zunehmenden Quality of Service Ansprüchen vieler Applikationen. Dazu sollen aber auch Konfigurationsaufgaben (z.B. von Firewalls) und Netzwerkverwaltung über das neue Protokoll möglich sein. Zu diesem Zweck wurde von der IETF die Next Steps in Signaling (NSIS) Working Group gegründet [2]. Sie befasst sich mit den Anforderungen und dem Design dieses neuen Signalisierungsprotokolls.

## 6.3 Das NSIS Protocol Suite Framework

Im Jahr 2001 bildete die Internet Engineering Taskforce (IETF) eine neue Arbeitsgruppe namens Next Steps in Signalling (NSIS) Working Group. Die Verantwortlichkeit der Arbeitsgruppe umfasst die Standardisierung eines Protokolls für die IP-Signalisierung.

### 6.3.1 Aufgabe des Frameworks

Als Funktion des Frameworks definiert die NSIS Working Group folgendes: 'The role of this framework is to explain how NSIS signaling should work within the broader networking context, and to describe the overall structure of the protocol suite itself.' [3] Gemäss RFC 4080 [3] sollten dabei vor allem Themen wie Routing, Mobility, Sicherheit sowie Interaktionen mit dem Netwerkressourcenmanagement betrachtet werden.

### 6.3.2 Die grundlegenden Konzepte des Frameworks

#### Signalisierungskonzepte

Ein flexibles Signalisierungsprotokoll sollte eine Signalisierung durch mehrere Domänen hindurch unterstützen. Signalisierungen sollten also sowohl in den Hosts, in den Domänengrenzknoten (Edge Nodes) als auch in den Knoten innerhalb einer Domäne möglich sein. Die NSIS Protokoll Suite erlaubt eine Ende-zu-Ende, eine Edge-zu-Edge, sowie auch eine Host-zu-Edge-Signalisierung.

Abbildung 6.1 zeigt ein Beispiel für eine Host-zu-Edge-Signalisierungskonfiguration. Die roten Quadrate auf der Abbildung zeigen die so genannten NSIS Entitäten. Als NSIS Entität definiert RFC 4080 'The function within a node that implements an NSIS protocol' [3]. Ein weiterer wichtiger Begriff in diesem Zusammenhang, ist der Begriff der so genannten Peer-Verbindung. RFC 4080 definiert diesen Begriff folgendermassen: 'A signaling relationship between two adjacent NSIS entities (i.e., NEs with no other NEs between them)' [3]. Den 'Sprung', welchen die Signalisierungsnachrichten machen müssen, um von einer Entität zur nächsten zu gelangen, bezeichnet man als NSIS-Hop. Die einzelnen Entitäten besitzen die Fähigkeit Statusinformationen über ihre Peers, also die angrenzenden

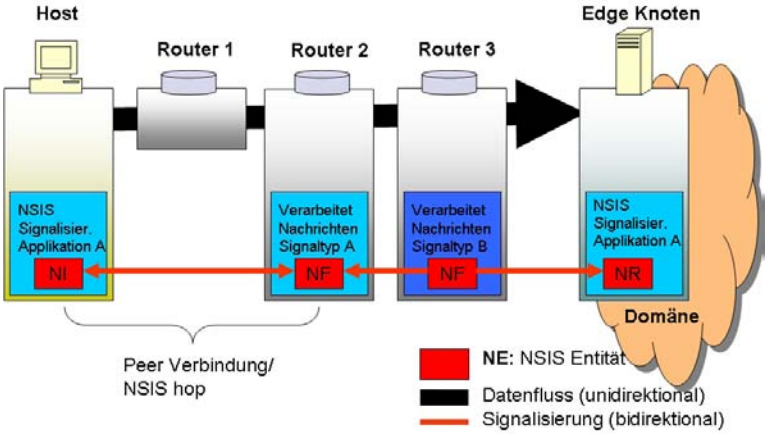



Abbildung 6.1: Beispiel für eine Ende-zu-Edge Signalisierungskonfiguration [1]

NSIS Entitäten, zu speichern. In vielen Fällen, vor allem bei mobilen Knoten, werden diese Informationen aber nur für kurze Zeit gültig sein. Aufgabe der NSIS Enitäten ist es bidirektional Informationen bezüglich des Status des Datenflusses austauschen. Wie in [1] beschrieben, initiiert ein Knoten, NSIS Initiator (NI) genannt, die Signalisierung. Die Knoten, welche sich auf dem Signalisierungspfad befinden, so genannte NSIS Forwarders (NF), fangen dann die Signalisierungsnachrichten ab und leiten sie weiter. Der NSIS Responder (NR) schliesslich terminiert die Signalisierung. Entlang des Datenpfades ist es weder notwendig, dass jeder Router NSIS tauglich ist, noch, dass jeder Router denselben Signalisierungsapplikationstyp unterstützen muss. Beispielsweise sind Nachrichten des Signalisierungsapplikationstyps A für den Router 3 transparent und werden dort nicht verarbeitet.

Denkbar sind auch Fälle, bei denen es notwendig ist, dass die Signalisierung von Entitäten, welche zwischen den Endknoten liegen, so genannten Signalisierungsproxies, initiiert bzw. terminiert werden muss. Ein Beispiel wäre ein Szenario in welchem die Endknoten NSIS nicht unterstützen. Oft verlangen auch Sicherheitsaspekte eine Konfiguration, in der der Einsatz von Signalisierungsproxies erforderlich wird. Abbildung 6.2 zeigt ein Beispiel für eine solche Konfiguration. Hier findet die Signalisierung nur zwischen Proxy1 und Proxy2 statt. Die Endknoten erhalten bzw. senden keine Signalisierungsnachrichten.

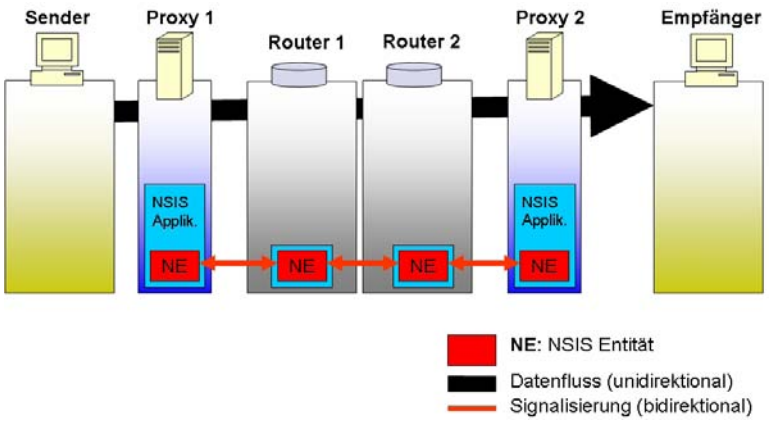



Abbildung 6.2: Signalisierung mittels Proxy [1]

### Abtrennung des Nachrichtentransportes von den Signalisierungsapplikationen

Um den Anforderungen eines generischen und erweiterbaren Signalisierungsprotokolls gerecht zu werden, werden die Protokollaufgaben in zwei Protokollschichten unterteilt. Es wird zwischen einer Signalisierungsschicht, der so genannten NSIS Signaling Layer (NSL) und einer Transportschicht, der NSIS Transport Layer (NTL), unterschieden. Aufgabe der Transportschicht ist es Signalisierungsnachrichten zuverlässig zu übermitteln. In der darüber liegenden Signalisierungsschicht werden diverse applikationsspezifische Dienste zur Verfügung gestellt. Beispiele dafür wären Dienste für die Ressourcenreservierung, Dienste für die Firewall- und Network Adress Translator-Konfiguration oder Dienste für die Messung des Netzwerkstatus. Auf die genaue NSIS Architektur wird später detailliert eingegangen.

### Pfadgekoppelte und pfadentkoppelte Signalisierung

Pfadgekoppelte Signalisierung bedeutet, dass die Signalisierung nur entlang des Datenpfades stattfindet. Dies heisst aber nicht, dass der Signalisierungs- und der Datenpfad zwangsläufig gleich verlaufen müssen, denn nicht alle Knoten des Datenpfades müssen auch für die Signalisierung verwendet werden. Denkbar wäre beispielsweise, dass sich auf dem Datenpfad Knoten befinden, welche keine NSIS Signalisierung unterstützen. Gemäss RFC 4080 [3] können die Nachrichten für die Adressierung entweder direkt mit der Adresse der Nachbarentität versehen werden, gleich wie die Datenpakete adressiert oder mit Hilfe der Router Alert Option an die nächste Entität geschickt werden.

Bei der pfadentkoppelten Signalisierung findet die Signalisierung entlang von Entitäten statt, bei welchen man vermutet, dass sie nicht auch für den Datenpfad verwendet werden und die Signalisierungsendknoten müssen nicht mit den Datenendknoten übereinstimmen. Für die Adressierung gibt es hier nur eine Möglichkeit und zwar explizit die Adresse der Nachbarentität anzugeben.

### Sender- und empfängerinitiierte Signalisierung

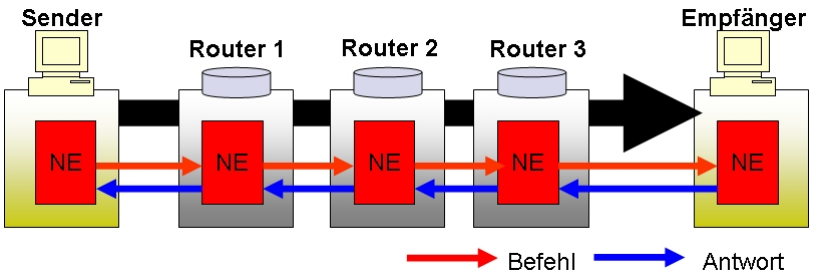



Abbildung 6.3: Senderinitiierte Signalisierung

Das NSIS Framework unterstützt einen sender- und einen empfängerinitiierten Ansatz. Abbildung 6.3 zeigt eine senderinitiierte Signalisierung am Bespiel einer Ressourcenreservierung (in dieser Anwendung ist die Signalisierung unidirektional). Hierbei ist der

Sender verantwortlich für den Datenfluss, er initiiert die Signalisierung und verwaltet die Datenflussverarbeitung. Der Sender schickt dem Empfänger einen Ressourcenreservierungsbefehl. Der Empfänger schickt dem Sender dann je nach Status eine positive oder negative Antwort.

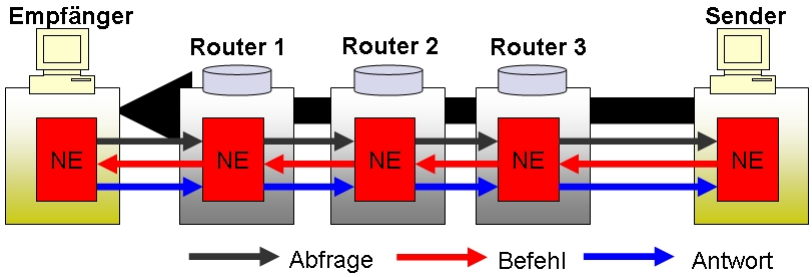



Abbildung 6.4: Empfängerinitiierte Signalisierung

Abbildung 6.4 zeigt ein Beispiel für eine empfängerinitiierte Signalisierung. Hier ist der Empfänger verantwortlich für die korrekte Datenflussverarbeitung. Der Empfänger schickt dem Sender eine Anfrage für eine Reservierung, der Sender führt dann diesen Befehl in Richtung zum Empfänger aus. Abschliessend schickt der Empfänger dann dem Sender eine Antwort, ob die Reservierung erfolgreich war oder nicht.

### Trennung von Peer-Ermittlung und Transportmechanismus

Die NSIS Protokoll Suite trennt strikt zwischen dem Auffinden der Peer-Entitäten und der Zustellung der Signalisierungsnachrichten. Diese Trennung ermöglicht den Einsatz von Sicherheitsprotokollen, wie TLS und IPSec/IKEv2, und Transportprotokollen TCP und SCTP.

### Einführung eines Session Identifier

Unter einem Session Identifier versteht man nach [1] folgendes: 'A session identifier is a cryptographically random number which is used to probabilistically uniquely identify a signaling session and signaling state'. Unter einem Data flow versteht man nach [1] 'a unidirectional sequence of packets between the same end points which all follow a unique path through the network'. Flows werden mittels einem Flow Identifier zum Beispiel mittels des Differentiated Services Code Point (DSCP) gekennzeichnet. Der Session Identifier wird unabhängig vom Flow Identifier eingesetzt. Dieser Ansatz erlaubt mehr Flexibilität: Während einem Handover beispielsweise können die Quell- oder Zieladressen verändert werden. So ein Handover kann den Flow jedoch nicht den Session Identifier verändern und damit kann dann der neue Flow auf dieselbe Session abgebildet werden. Ein anderes Beispiel bei dem sich der Einsatz eines Session Identifiers als nützlich erweist, ergibt sich dann, wenn verschiedene Flows, wie sie zum Beispiel aufgrund von Load Sharing auftreten, auf eine Session abgebildet werden müssen.

**Flowaggregation**

Eine reine per Flow Signalisierung bereitet Skalierungsprobleme und ist für grossangelegte Netzwerke sicherlich keine effiziente Lösung. Die NSIS Protocol Suite bietet daher eine Möglichkeit eine Signalisierung für eine Aggregation von Flows durchzuführen.

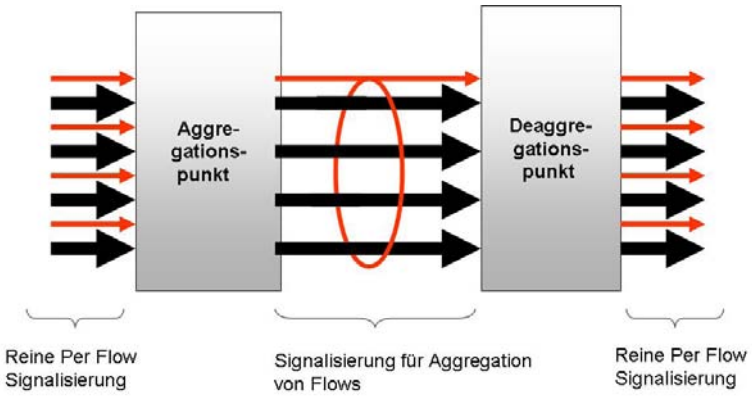



Abbildung 6.5: Flowaggregation

Abbildung 6.5 zeigt ein Beispiel einer Flowaggregation. In den so genannten Singalisierungsaggregationspunkten fasst eine Signalisierungsapplikation einzelne Flows zu einem Aggregat zusammen. Dabei muss in der Signalisierungsschicht auch spezifiziert werden, was eine Aggregation von Flows in ihrem Kontext überhaupt bedeutet. Die Zusammenfassung der Flows zu einem Aggregat kann beispielsweise dadurch geschehen, dass die einzelnen Flows mit einem gemeinsamen Differentiated Services Code Point (DSCP) markiert werden oder auch durch Einsatz von Tunneling-Systemen. Vor dem Aggregations- bzw. nach dem Deaggregationspunkt wird per Flow-Signalisierung verwendet, innerhalb der beiden Punkte sollte aber eine Signalsierung für ein Flowaggregat stattfinden. Mittels der Aggregationssignalisierung erzielt man erhebliche Performancevorteile. Sie kann jedoch nur für die pfadgekoppelte Signalisierung verwendet werden.

### 6.3.3 Das NSIS Schichtenmodell

**Architektur**

Wie bereits oben erwähnt, wird die NSIS Protocol Suite in zwei Schichten, eine Transportschicht namens NTL und eine Signalisierungsschicht mit dem Namen NSL unterteilt. Damit wird ein modulares Design erreicht. Abbildung 6.6 zeigt welche logischen Komponenten in welche Schicht gehören. Innerhalb der Signalisierungsschicht können sich mehrere NSIS Signaling Layer Protocols (NSLPs) befinden, welche nach [1] applikationsspezifische Funktionalität inklusive Formate und Nachrichtenverarbeitungsregeln für die NSLP-Peer-Beziehung bereitstellen. Innerhalb der Transportschicht befindet sich das NSIS Transport Layer Protocol (NTLP). Auf die einzelnen logischen Komponenten der Transportschicht und auf ihre mögliche Verwendung wird in der Beschreibung des Frameworks nicht gross eingegangen. Möglich sind aber Szenarien, wie sie Abbildung 6.6

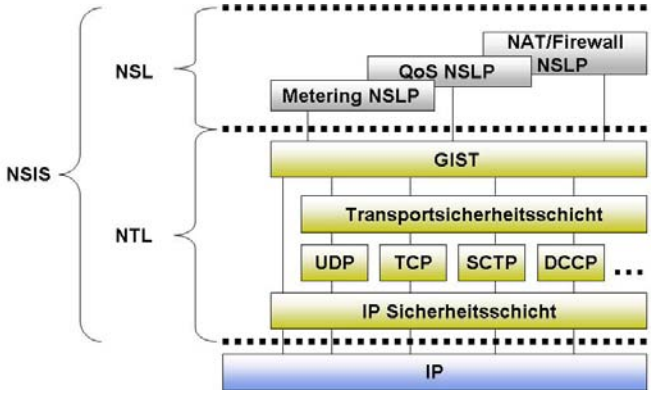



Abbildung 6.6: Logische Komponenten [1]

zeigt. Besondere Beachtung verdient das Nachrichtenprotokoll General Internet Signaling Transport Protocol GIST. GIST wird in einem späteren Kapitel genauer beschrieben.

### NSIS Transport Layer Protocol (NTLP)

Das NTLP funktioniert nur zwischen zwei benachbarten NSIS Entitäten und ist somit ein Hop-by-Hop Protokoll. Alles was weiter als bis zur nächsten Peer Entität geht, ist Aufgabe der oberen Schichten. Die Idee hinter dieser Restriktion ist eine Reduktion der Komplexität und eine Einschränkung von potentiellen Fehlern auf die beiden benachbarten Entitäten anstatt auf möglicherweise das ganze Internet. Die Signalisierungsnachrichten, welche zum Senden bereit sind, werden an die NTL Schicht zusammen mit der Information, welchen Flow sie betreffen übermittelt.

Nachrichtenübermittlung beinhaltet auch die Suche und Auswahl von passenden Peers. Diese Peer-Ermittlung kann gemäss RFC 4080 [3] entweder ein aktiver Prozess sein, indem spezifische Signalisierungspakete benutzt werden oder ein passiver, welcher als Nebeneffekt eines spezifischen Adressierungsmodus auftritt. Es gibt 2 Verfahren, um Signalisierungsnachrichten zu adressieren.

Die erste, eine passive Peer-Ermittlung, ist die Ende-zu-Ende Adressierung. Hier wird die Signalisierungsnachricht direkt an die Zieladresse des Data Flows adressiert. Einige Entitäten entlang des Datenpfades fangen die Nachrichten ab und leiten sie weiter. Die Signalisierungsnachrichten sollten exakt entlang des Datenpfades verlaufen. Dieses Verfahren wird beispielsweise beim Suchen des ersten Downstream-Peer verwendet.

Bei der Peer-Peer Adressierung werden die Signalisierungsnachrichten an eine Entität gerichtet, welche näher an der Zielentität liegt als die Entität, welche gerade die Signalisierungsnachrichten verarbeitet. Die Peer-Peer Adressierung erfordert eine aktive Peer-Ermittlung. Die dafür benötigte Peer-Discovery-Komponente kann als eine Subschicht von NTL betrachtet werden und benötigt für die Ermittlung den Data Payload und die Adresse der Entität, von welcher die Nachrichten geschickt wurden. Das Peer-Peer Adressierungsverfahren wird beispielsweise beim Reverse Routing eingesetzt.

Nachdem die nächste Peer-Entität ermittelt wurde, werden von der NTL dann rohe IP Pakete an diese Entität gesendet. Im Peer-Peer Adressierungsfall tragen die Nachrichten die Adresse der nächsten Peer-Entität, im Ende-zu-Ende Adressierungsfall, sind diese in irgendeiner Weise markiert (z.B. mittels des Protokollnummer-Feldes), damit passende Entitäten die Nachrichten abfangen können. Falls sich beim empfangenden Knoten keine passende Signalisierungsapplikation befindet, leitet die NTL dieser empfangenden Peer-Entität die Signalisierungsnachrichten gerade direkt weiter, andernfalls werden sie an die betreffende Signalisierungsapplikation geschickt. Die Applikation kann dann weitere Signalisierungsnachrichten generieren, welche wiederum mittels NTLP verschickt werden können.

Nach RFC 4080 [3] sollte folgende Funktionalität in der NTL bereitgestellt werden:

1. Bundling von kleinen Nachrichten kann optional von der NTLP bereitgestellt werden. Unbundling sollte von der NTL jedoch immer unterstützt werden.

2. Nachrichten-Fragmentierung und fragmentiertes Weiterleiten bis zur Ziel-NSL sollte auch in der NTL zur Verfügung gestellt werden, da das Fragmentieren von grossen IP Nachrichten zu reduzierter Zuverlässigkeit führen kann.

3. Eine zuverlässige Übermittlung von Signalisierungsnachrichten kann die Performance erheblich verbessern. Das Entdecken und Beheben von Applikationsschichtfehlerursachen bleibt aber weiterhin Aufgabe der NSLP.

4. Das NTLP sollte Stausituationen erkennen können und mit der Fähigkeit ausgestattet sein die Transmissionsrate der Signalisierungsnachrichten anpassen zu können.

### NSIS Signaling Layer Protocol (NSLP)

Das Signalisierungsschichtprotokoll (NSLP) benutzt die generische Funktionalität von NTLP. Für die Kommunikation werden nach RFC 4080 [3] zwei Basiskontrollprimitive benutzt: 'Send Message', um die Signalisierungsnachrichten an die NTLP zu übergeben und 'Receive Message', um die Nachrichten von der NTLP an die NSLP zu übergeben. Eine Signalisierungsapplikation kann sich beim NTLP registrieren oder auch wieder deregistrieren. Dies ermöglicht ein effizientes Handling der Signalisierungsnachrichten. Weiter gibt es einen Fehlerservice. Dieser Service erlaubt Fehlermeldungen seitens der Applikation an die NTL zu schicken oder auch umgekehrt. Schliesslich gibt es noch einen Feedbackdienst. Damit kann die NTL die Applikation beispielsweise über eine Routenveränderung unterrichten.

Die traditionelle Anwendung für die Signalisierung ist sicherlich die QoS Signalisierung. Auf das NSLP für QoS wird detailliert in einem späteren Kapitel eingegangen. NSLPs können aber nicht nur für die Ressourcenreservierung verwendet werden.

Ein Beispiel für eine andere Anwendung von NSLP zeigt Abbildung 6.7, das sogenannte Metering NSLP. Monitoring Probes überwachen und messen den Data Flow und transportieren die Daten dann von dort zu einer Messentität, der so genannten Metering Entity

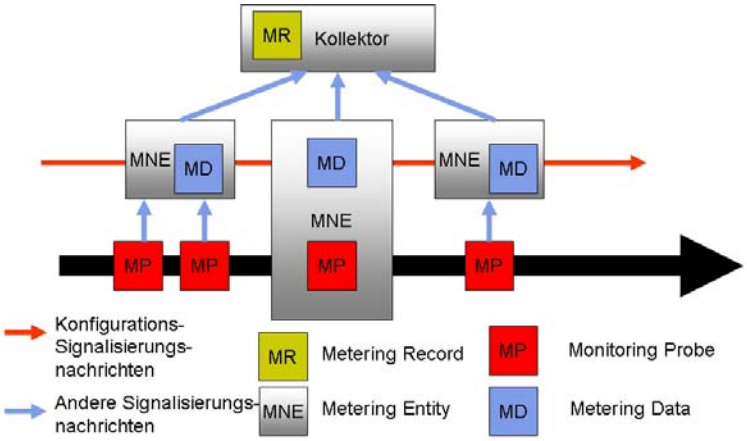



Abbildung 6.7: Metering NSLP Architektur[9]

(MNE). Die Messentitäten können durch Signalisierungsnachrichten konfiguriert werden, was genau sie sammeln sollen. Zusätzlich zu den Daten ihrer Monitoring Probes kommen meist noch weitere Daten hinzu, wie beispielsweise Informationen über die Session. Die Messentitäten übermitteln dann die Daten an einen Kollektor. Der Kollektor korreliert die Daten zu einzelnen Events und produziert einen Messdatensatz. Für Metering NSLP sind unterschiedliche Einsatzszenarien denkbar:

1. Ein Beispiel wäre eine Abbrechung eines Bezuges irgendeines mobilen Services. Bespielsweise das Streamen eines Videos von einem Applikationsserver. Die einzelnen Messentitäten können genau erfassen, was, wann, wo und mit welcher Dienstgüte in Anspruch genommen wurde, die Daten können dann an einen Kollektor gesendet und für die Rechnungserstellung aggregiert werden.

2. Ein weiterer Einsatzbereich ist das prüfen, ob die vertraglich zugesicherte Dienstgüte mit der tatsächlichen Dienstgüte übereinstimmt.

3. Intrusion Detection Systeme können Metering NSLP als Messinstrument einsetzen. Die einzelnen Messentitäten können so konfiguriert werden, dass sie einen bestimmten Flow überwachen.

Ein weiteres Beispiel für ein NSLP ist das NAT/Firwall NSLP. NAT wird eingesetzt um den IP Adressraum zu erweitern. Eine Middlebox wandelt Adressen eines internen privaten Netwerkes in eine öffentliche Adresse um. Die Hosts können somit von aussen nicht direkt angesprochen werden. Bei einer Firewall wird basierend auf Regeln bestimmter Traffic nicht durchgelassen. NAT und Firwalls können ein Hindernis für bestimmte Applikationen (z.B. Peer2Peer oder VoIP) darstellen. Mit Hilfe von Signalisierungsnachrichten kann eine Firewall, bevor ein Host Daten sendet, konfiguriert werden, so dass die Daten einer Applikation ungehindert die Firewall passieren können oder es können NAT Bindings erstellt werden, damit eine Applikation von aussen mit einem Rechner des privaten Netzwerkes direkt kommunizieren kann.

## 6.4 General Internet Signaling Transport (GIST)

GIST [4] ist ein konkreter Implementierungsvorschlag der NSIS Working Group des NTLP-Layers [4] von NSIS. GIST stellt pfadgekoppelte Signalisierung zur Verfügung. In der vom NSIS Framework vorgegebenen Trennung von Signalisierungs-Applikationen und Protokoll bietet GIST den Applikationen auf der Basis existierender Transport und Sicherheitsprotokolle eine eigene Nachrichten-Schicht [4]. Signaling Applikationen und GIST haben je ihre eigene Zustandsverwaltung. Hier unterscheidet sich NSIS wesentlich von anderen Signalisierungsprotokollen, die auch den Applikationszustand verwalten. GIST ist also völlig losgelöst von den GIST benutzenden Applikation. Der Dienst von GIST besteht in der Informationsweitergabe für die GIST benutzenden Applikation in der von den Applikationen über speziell gesetzte Parameter verlangten Art und Weise. Mögliche Einstellungen sind zum Beispiel Reliablity und Securtiy.

### 6.4.1 GIST Protokoll Stack

GIST ist ein pfadgekoppeltes Signalisierungsprotokoll. Den Anforderungen des NSIS Framework folgend trennt GIST die pfadgekoppelte Signalisierung in einen Routing- und einen Transportteil. Im Routingteil wird entschieden wer die sogenannten GIST-Peers sind, wie sie erreicht werden und welche Informationen über die Peers gesammelt und gehalten werden. Der Transportteil von GIST ist für die Übertragung der Signalisierungsinformation verantwortlich [3] und benutzt gängige Protokolle der Transportschicht für die Übermittlung. Dies hat in der GIST-Implementation zu dem in Abbildung 6.8 illustrierten Aufbau des Protokoll-Stacks geführt. Abbildung 6.8 illustriert eine weitere Aufteilung des GIST Messaging Layers in einen Message Encapsulation Teil und in einen GIST Zustandsverwaltungsteil.

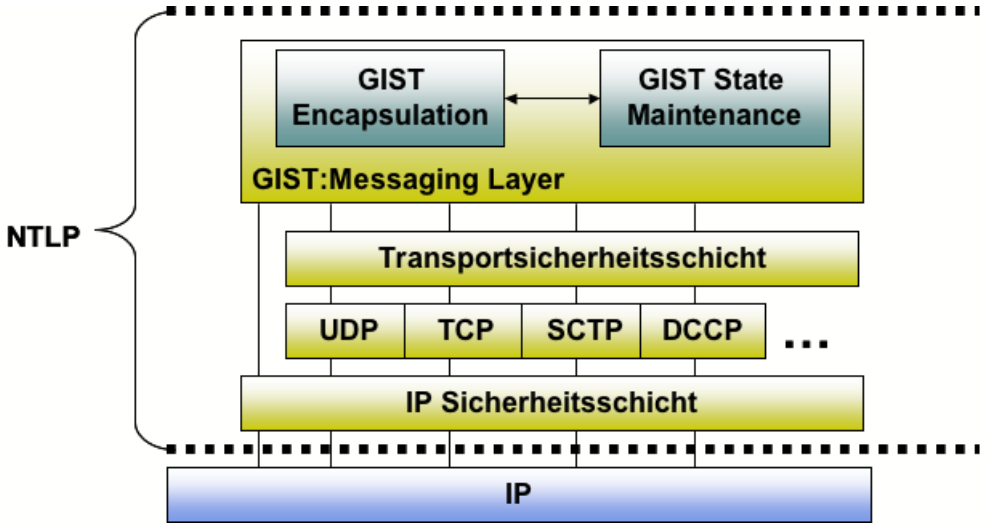



Abbildung 6.8: GIST Protokoll Stack [4]

### 6.4.2 GIST Nachrichten

Innerhalb von GIST gibt es insgesamt sechs unterschiedliche GIST-Nachrichten. Diese Nachrichten haben ihre Gültigkeit nur zwischen GIST-Peers. Sie sind für GIST benutzende Applikationen nicht ersichtlich. Mit Hilfe dieser Nachrichten organisiert die GIST Schicht den Transport von Signalisierungsnachrichten für Signalisierungsapplikationen wie zum Beispiel Ressourcenreservation in einem QoS-Umfeld. Zusätzlich dazu können GIST-interne Zustände so unterhalten und verändert werden. Alle dem GIST-Layer von den NSLP-Applikationen übergebenen Nachrichten werden also in die Entsprechenden GIST-Nachrichten gepackt. Versendet werden GIST-Nachrichten entweder im Datagram-Mode oder im Connection-Mode, welche in 1.4.3 genauer erklärt werden.

Alle GIST Nachrichten enthalten den Common-Header. Dieser setzt sich aus der GIST-Version, Nachrichtenlänge, NSLPID, GIST Hop Counter, Message Type, Source Adressing Mode, Response Request und Explicit Routing Flag zusammen.

#### GIST-Query

Die GIST-Query wird immer im Datagram-Mode verschickt. Sie kann schon NSLP-Daten beinhalten und muss immer beantwortet werden. GIST-Querys werden verschickt, um Informationen über benachbarte GIST-Knoten zu erhalten. Neben dem Nachrichten-Header enthält sie die `Message-Routing-Infomation` (MRI), worin beschrieben wird, wie die Nachricht geroutet werden soll. Durch die `Session-Identification` SID, können die Nachrichten den entsprechenden GIST-Sessions zugeordnet werden. Im `Stack-Proposal` werden Vorschläge zu Transport- und Sicherheitsprotokoll gemacht.

```
GIST-Query = Common-Header
             Message-Routing-Information
             Session-Identification
             Network-Layer-Information
             Query-Cookie
             [ Stack-Proposal Stack-Configuration-Data ]
             [ NSLP-Data ]
```

#### GIST-Response

Die GIST-Response kann entweder im Datagram-Mode oder im Connection-Mode verschickt werden. Sie beinhaltet die invertierten `Message-Routing-Information` , die `Session-Identification` der Query und das `Query-Cookie`. Zum Aufbau des Messaging Associate Status muss die Nachricht auch das `Responder-Cookie` beinhalten. Enthält die Nachricht ein Responder-Cookie muss sie beantwortet werden.

```
GIST-Response = Common-Header
                Message-Routing-Information
```

```
                Session-Identification
                [ Network-Layer-Information ]
                Query-Cookie
                [ Responder-Cookie
                    [ Stack-Proposal Stack-Configuration-Data ] ]
                [ NSLP-Data ]
```

### GIST-Confirm

Die GIST-Confirm Nachricht kann in Datagramm- oder Connection-Mode verschickt werden. Sie muss auch die invertierte MRI, die SID und das Responder-Cookie beinhalten.

```
GIST-Confirm = Common-Header
               Message-Routing-Information
               Session-Identification
               Network-Layer-Information
               [ Responder-Cookie
                   [ Stack-Proposal
                       [ Stack-Configuration-Data ] ] ]
               [ NSLP-Data ]
```

### GIST-Data

Die GIST-Data Nachricht enthält keine Kontrollobjekte sondern nur NSLP Daten.

```
GIST-Data = Common-Header
            Message-Routing-Information
            Session-Identification
            [ Network-Layer-Information ]
            NSLP-Data
```

### GIST-Error

Die GIST-Error Nachricht wird gebraucht, um Probleme im GIST-Layer zu übermitteln. Diese Nachricht wird im Datagram-Mode verschickt (NSLP-Errors werden als Payload einer GIST-Data Nachricht verschickt).

```
GIST-Error = Common-Header
             [ Network-Layer-Information ]
             GIST-Error-Data
```

**GIST-Hello**

GIST-Hello Nachricht wird nur im Connection-Mode verschickt. Mit dieser Nachricht wird einem GIST-Peer mitgeteilt, dass der Sender die Messaging Association offen behalten will. Wenn nicht verlangt, ist ihre Beantwortung optional.

```
GIST-MA-Hello = Common-Header
```

### 6.4.3 GIST Transport Mechanismus

GIST kennt zwei verschiedene Übertragungsarten für GIST-Nachrichten Datagram-Mode und Connection-Mode. Der Datagram-Mode wird vor allem für die GIST-Query verwendet. Datagram-Mode Nachrichten benutzen keine Transportschicht-Sicherheitsmechanismen und werden in UDP-Nachrichten übermittelt. Die Empfänger-IP wird entweder aus den Datenflussinformationen abgeleitet oder auf Basis vorgängig erstellten Nachbarschaftszuständen genommen. Im Connection-Mode können nur Nachrichten verschickt werden, für die eine sogenannte Messaging Associate Beziehung aufgebaut wurde. Die Protokolleinstellungen dieser Messaging Association können dementsprechend wiederverwendet werden. Als Übertragungsprotokolle können hier zum Beispiel Transmission Control Protocol (TCP), Stream Control Transmission Protocol (SCTP) oder Datagram Congestion Control Protocol (DCCP) verwendet werden.

### 6.4.4 GIST Zustandsautomaten

Der GIST-Layer hält seine eigenen Zustandsautomaten, die unabhängig von NSLP-Applikationen sind. In der GIST-Implementierung werden vier kooperierende Zustandsautomaten beschrieben [4].

- Die *Node-SM* ist die für jeden GIST-Knoten existierende State-Machine. Sie verarbeitet alle Nachrichten, die keiner anderen speziefischen State-Machine zugeordnet werden können. Sie ist immer vorhanden und instanziert neue Zustandsautomaten für jeden neuen Flow.

- Die *Query-SM* hat ihre Gültigkeit während des Aufbaus einer Messaging Association und verarbeitet Query- und Confirm-Nachrichten.

- Die *Response-SM* wird pro Datenstrom und Signalisierungsrichtung instanziert. Sie unterhält den Routing-Zustand für jeden Datenstrom.

- Die *MA-SM* wird mit jeder Messaging Association aufgebaut. Sie verwaltet den Auf- und Abbau von den Peer-to-Peer Verbindungen und Timer für jede Verbindung.

### 6.4.5 GIST Signaling Application API

GIST bietet NSLP benutzenden Applikationen ein einheitliches API zur Benutzung der Signalisierungsmechanismen von GIST. Zur Interaktion mit einer Applikation kennt GIST sechs verschiedene Nachrichten:

- `SendMessage` wird verwendet, wenn eine Applikation eine Nachricht verschicken möchte.
- `ReceiveMessage` wird von GIST verwendet, um eine Nachricht an die Applikation zu übergeben.
- `MessageStatus` ist eine Nachricht von GIST an die Applikation. Darin werden entweder Fehler bei der Übertragung mitgeteilt werden oder zum Beispiel die von GIST gewählten Sicherheitseinstellung bei der Nachrichtenübermittlung. Die Applikation kann darauf mit einem Abort antworten, wenn sie die gewählten Einstellungen als ungenügend klassifiziert.
- `NetworkNotification` ist eine Nachricht von GIST an die Applikation die gesendet wird, wenn GIST über Informationen verfügt, die für die Applikation interessant sein könnten.
- `SetStateLifetime` wird von der Applikation benutzt um GIST mitzuteilen, wie lange ein Routing-State behalten werden soll oder ob ein Routing-State nicht mehr benötigt wird.
- `InvalidateRoutingState` wird von der Applikation an GIST übergeben, um GIST mitzuteilen, dass der entsprechende Signaling-Peer wahrscheinlich nicht mehr erreichbar ist.

## 6.5 QoS NSLP

In diesem Kapitel wird nun ein konkretes Beispiel einer Signaling Applikation vorgestellt, die auf dem NSIS Framework basiert. Das Beispiel behandelt Quality of Service (QoS) NSIS Signaling Layer Protocol (NSLP) wie es von der IETF im Draft [5] beschrieben wurde. QoS NSLP ist unabhängig von der QoS Spezifikation und zugrundeliegenden Architektur. QoS NSLP wurde so gestaltet, dass es unabhängig von einem bestimmten QoS Model ist, wie z.B. IntServ oder DiffServ. Es unterstützt mehrere QoS Modelle.

### 6.5.1 Wozu braucht QoS Signaling?

Für eine reibungslose Übertragung, müssen alle Router zwischen dem Sender und Empfänger die benötigten Ressourcen zur Verfügung stellen. Wenn nicht alle Router die benötigten Ressourcen bereitstellen, entsteht ein Flaschenhals, die Servicequalität ist nicht mehr gewährleistet. Signalisierung wird zwischen den Akteuren für Auf- und Abbau der Reservationen verwendet.

### 6.5.2 QoS NSLP Aufbau und Konzepte

#### Terminologie

- `QNE`: Eine NSIS Entität (NE), welche QoS NSLP unterstützt.
- `QNI`: Der erste Knoten in der Reihe von QNEs, der eine Reservationsanfrage für eine Session behandelt.
- `QNR;` Der letzte Knoten in der Reihe von QNEs, der eine Reservationsanfrage für eine Session behandelt.
- `Session`: Eine Session ist eine Verbindung zwischen QNI und QNR, die sich auf einen Datenfluss bezieht.

#### Möglicher Aufbau einer QNE

In Abbildung 6.9 ist ein möglicher Aufbau einer QNE aufgezeichnet. Reinkommende Messages werden vom 'Input packet processing' Modul herausgefiltert und an GIST zur weiteren Verarbeitung übergeben. Nur Messages die zu QoS NSLP gehören, werden dann weiter gereicht.

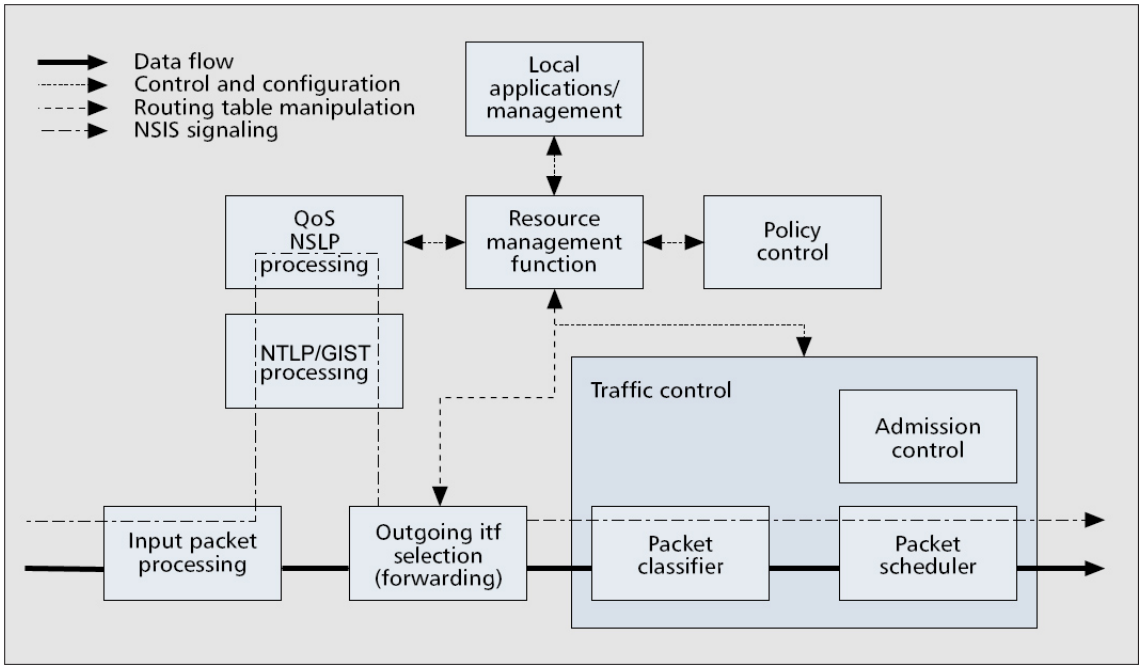



Abbildung 6.9: Aufbau einer QNE [5]

Die 'Resource Management Function'(RMF) behandelt QoS Anfragen. Die notwendigen Parameter werden ihr von QoS NSLP in Form des QSPEC Objekts übergeben. Die RMF verwaltet die Ressourcen auf der QNE und speichert auch den Reservationszustand. Wenn eine Reservation beantragt wurde, koordiniert die RMF die Prüfung der Anfrage.

Zwei Module entscheiden über die Anfrage. Die 'Policy Control' prüft ob die QNE, welche die Reservation startete, die Berechtigung dazu hatte. Die 'Policy Control' wird üblicherweise einen externen AAA Service anfragen. Das zweite Modul ist die 'Admission Control'. Sie überprüft ob überhaupt die nötigen Ressourcen für die Reservation vorhanden sind. Wenn die Reservation akzeptiert wird, übergibt die RMF dem 'Packet Classifier' die korrekten Parameter, damit das QoS angewendet wird.

Fehlermeldungen werden an den Absender der Reservation Message geschickt. Anfragen können auch von einer lokalen Applikation kommen, sei es eine User Applikation (z.B. Multimediaanwendung) oder Netzwerkmanagement Applikation (z.B. die Initialisierung eines Tunnels für eine aggregierte Reservation).

### Signaling Messages

Das QoS NSLP hat vier Signaling Messages. Eine Message besteht aus einen Common Header, gefolgt von einer variablen Menge von Objekten. Alles zusammen ist verpackt in einem GIST-NSLP Datenobjekt.

### Common Header

Der Common Header ist nicht das selbe wie der GIST Common Header. Er beschreibt den Nachrichtentyp. Es gibt vier Typen: Reserve, Query, Response und Notify. Des weiteren beinhaltet der Common Header Message Flags und Generic Flags. Message Flags sind je nach Messagetyp definiert. Generic Flags gibt es nur eines, das Scoping Flag. Das Scoping Flag wird im Kapitel Message Scoping erklärt.

### RESERVE

Die RESERVE Message ist die einzige Message die den Reservationszustand einer QNE verändern kann. Man benutzt sie zum erstellen, verändern und entfernen von Reservationen entlang des Datenpfades. Ob eine gleiche Reserve einmal oder mehrmals zu einer QNE gesendet wird, macht keinen Unterschied, weil die zuletzt empfangene Message die Zustandsänderung der Vorangegangenen ersetzt.

Das Format der Reserve Message sieht wie folgt aus:

```
RESERVE = COMMON_HEADER
          RSN [ RII ] [ REFRESH_PERIOD ] [ *BOUND_SESSION_ID ]
          [ [ PACKET_CLASSIFIER ] QSPEC [ QSPEC ] ]
```

An erster Stelle an dem Common Header kommt die Reservation Sequence Number (RSN), deren Zweck im Kapitel Message Sequencing genauer beschrieben ist. Die RSN ist das einzige Objekt, dass in jeder Reserve Message vorhanden sein muss. Die Verwendung vom REFRESH_PERIOD Objekt wir im Kapitel Softstate behandelt. Das BOUND_SESSION_ID

Objekt wird für Session Binding verwendet. Das QSPEC Objekt enthält alle nötigen Parameter für die Reservation. Mehr zum QSPEC Objekt im gleichnamigen Kapitel.

### QUERY

Mit der Query Message können Informationen über den Datenpfad gesammelt werden, ohne dass eine Reservation vorgenommen wird. Im Falle einer empfängerinitiierten Reservation oder bei gewissen QoS Modellen, kann das Netzwerk 'getestet' werden.

Das Format der Query Message sieht wie folgt aus:

```
QUERY = COMMON_HEADER
        [ RII ][ *BOUND_SESSION_ID ]
        [ PACKET_CLASSIFIER ] QSPEC [ QSPEC ]
```

Eine Query Message muss mindestens ein QSPEC Objekt enthalten. Das QSPEC Objekt wird hier zur Speicherung der Informationen verwendet. Wenn eine QNE die Query Message zum Sammeln von Informationen verwenden will, muss ein RII Objekt vorhanden sein, um eine passende Response Message generieren zu können. Das BOUND_SESSION_ID Objekt wird für Session Binding verwendet.

### RESPONSE

Die Response Message wird als Antwortnachricht auf Reserve oder Query verwendet. Dies kann unter anderem die Bestätigung einer erfolgreichen Zustandsmanipulation sein oder eine Fehlermeldung, wenn z.B. die Reservation missglückt ist.

Das Format der Response Message sieht wie folgt aus:

```
RESPONSE = COMMON_HEADER
           [ RII / RSN ] INFO_SPEC
           [ QSPEC ] [ QSPEC ]
```

Die Response Message muss ein INFO_SPEC Objekt enthalten. Das INFO_SPEC Objekt enthält Informationen darüber, ob ein Erfolg, kein Erfolg oder ein Fehler eingetreten ist.

### NOTIFY

Dient zur Informationsübermittlung an eine QNE. Im Gegensatz zu einer Response Message muss die Notify Message nicht als Antwort auf einen vorangegangene Nachricht erfolgen.

Das Format der Notify Message sieht wie folgt aus:

```
NOTIFY = COMMON_HEADER
         INFO_SPEC [ QSPEC ] [ QSPEC ]
```

Auch die Notify Message muss ein INFO_SPEC Objekt enthalten. Im Objekt angegeben ist der Grund für die Informationübermittlung. Je nach INFO_SPEC können ein oder zwei QSPEC Objekte mit zusätzlichen Informationen angehängt werden.

### QSPEC Objekt

Das QSPEC Objekt ist ein zentraler Bestandteil für QoS NSLP und wird ausführlich im Draft 'QoS-NSLP QSPEC Template' [11] beschrieben. Es ist Teil der QoS NSLP Messages, ist aber undurchsichtig für QoS NSLP. Die Informationen relevant für ein QoS Model werden im QSPEC Objekt gespeichert. Das QoS Model ist die Methode um QoS für den Datenverkehr zu erlangen. Das Model entscheidet wie sich die Ressource Management Funktion (RMF) verhalten soll und wie es die QSPEC interpretieren muss. QoS NSLP reicht das QSPEC Objekt der RMF zur Verarbeitung weiter. Die QSPEC Parameter bieten eine einfache Sprache, die von möglichst vielen QoS Modellen wieder verwendet werden kann.

Das QSPEC hat folgende Parameter:

```
QSPEC = <QSPEC Version> <QOSM ID> <QSPEC Control Information> <QoS Description>
```

An erster und zweiter Stelle sind Informationen zur Identifizierung. <QSPEC Version> gibt an, welche Version verwendet wird. <QOSM ID> ist die ID des eingesetzten QoS Models. <QSPEC Control Information> sendet RMF Funktionen, welche nicht von QoS NSLP definiert wurden. Dies ermöglicht das Erstellen neuer Funktionen, die für das QoS Model gebraucht werden.

```
<QoS Description> = <QoS Desired> <QoS Available> <QoS Reserved> <Minimum QoS>
```

<QoS Description> beschreibt QoS. QoS Desired, QoS Available, QoS Reserved, und Minimum QoS sind QSPEC Objekte, die Input und Output für die RMF sind.

- `QoS Desired:` Beschreibt die gewünschte QoS, wofür der Sender die Reservation will.
- `QoS Available:` Parameter, welche die vorhandenen Ressourcen beschreiben. Sie werden für das sammeln vor Informationen gebraucht.
- `QoS Reserve:` Parameter, welche die reservierten Ressourcen beschreiben.
- `Minimum QoS:` Zusammen mit QoS Desired und QoS Available beschreibt Minimum QoS einen QoS Bereich. Wenn die QNE die gewünschte Reservation, wie in QoS Desired beschrieben, nicht erfüllen kann, wird die Reservation solange verringert, bis das Minimum erreicht wird.

### Softstate

Reservationen auf den QNEs sind Softstate. Das bedeutet, dass sie nach Ablauf einer gewissen Zeit erneuert werden müssen, ansonsten wird die Reservation entfernt. Dies geschieht durch ein wiederholtes Senden der Reserve Message. Die Zeit bis zur Erneuerung wird in Millisekunden im REFRESH_PERIOD Objekt angegeben. Das REFRESH_PERIOD Objekt ist nicht zwingend Teil der Reserve Message. Wenn es nicht vorhanden ist, wird als vorgegebener Wert 30 Sekunden genommen.

Der Gegensatz zu Softstate ist Hardstate bei dem der Zustand erst dann abgebaut wird, wenn eine explizite Teardown-Message gesendet wird.

### Reduced Refresh

Um nicht jedes mal eine vollständige Reserve Message zu schicken, wenn die Reservation erneuert werden muss, gibt es eine verkürzte Reserve Message. Die verkürzte Message muss kein QSPEC Objekt beinhalten und auch kein PACKET_CLASSIFIER Objekt.

### Lokale QoS Modelle

Eine Domain kann ein lokales QoS Model bestimmen und somit selber bestimmen, was für seine Ressourcen die beste Methode ist. Um dies zu bewerkstelligen, muss die QNE am Rand der Domain der Reserve Message ein passendes QSPEC Objekt hinzufügen. Siehe Abbildung 6.10. Die QSPEC Objekte lassen sich stapeln, das ursprüngliche QSPEC bleibt somit in der Message erhalten. Alle QNEs verwenden das oberste QSPEC für ihre Reservation. Die QNE beim Ausgang der Domain entfernt das QSPEC Objekt wieder, wodurch das alte wieder an die erste Stelle des Stapels tritt.

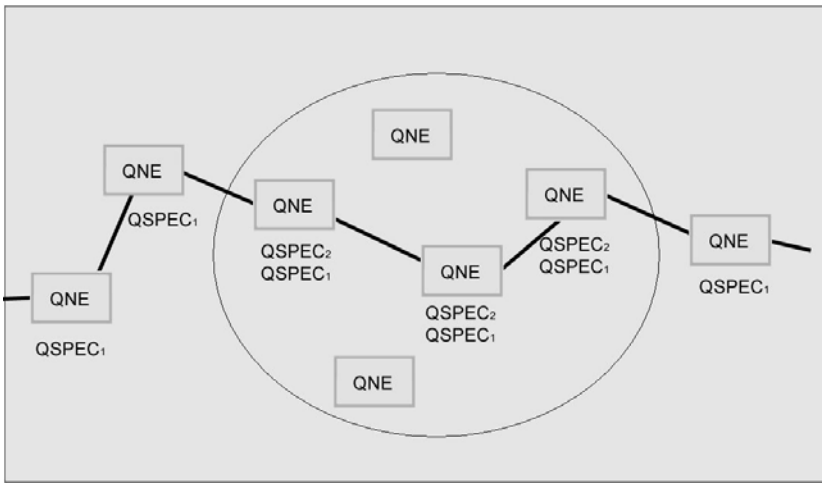



Abbildung 6.10: Reservation mit lokalem QoS Model [5]

### Message Sequencing

Die Reihenfolge der Reserve Messages, in der sie eine QNE erreichen, ist für seinen Zustand relevant, da die zuletzt erreichte Reserve Message die vorherrschende Reservation ersetzt.

Um Messages die in der falschen Reihenfolge ankommen oder dupliziert wurden, zu erkennen und somit falsche Reservationsänderung zu verhindern, haben die Reserve Messages eine Sequenz Nummer, die sog. Reservation Sequence Number (RSN). Die RSN ist nur zwischen zwei benachbarten QNEs (Peers) signifikant. Darum muss die RSN nur zwischen zwei Peers eindeutig sein und nicht entlang des gesamten Pfades.

Die RSN ist eine Seriennummer, welche neben der Eigenschaft die Reihenfolge der Messages zu markieren, auch Information darüber gibt, ob der Sender der Nachricht neu gestartet hat. Dies ist z.B. der Fall wenn ein Reboot der Hardware stattgefunden hat oder die Software neu gestartet wurde. Die Information wird Epoch Identifier genannt. Der Epoch Identifier ist eine Zahl, welche beim Start der Software neu bestimmt wird. Sie bleibt solange gleich bis ein Neustart erfolgt.

Nach jeder gesendeten Reserve Message muss die RSN erhöht werden. Wenn eine QNE eine Reserve Message empfängt, wird wie folgend mit der Message verfahren:

- Wenn die RSN grösser ist als der momentan gespeicherte Wert, muss die Reservation entsprechend modifiziert werden. Dies unter der Voraussetzung, dass die Policy Control und Admission Control dies erlaubt.
- Ist die RSN gleich dem gespeicherten Wert, wird ein Refresh der Reservation durchgeführt (Siehe Softstate).
- Falls die RSN kleiner ist, dann ist die Message nicht in der korrekten Reihenfolge und muss ignoriert werden. Ist jedoch der Epoch Identifier verschieden vom gespeicherten Wert, dann muss die Reserve Message als gültig behandelt werden und die Reservation der QNE entsprechend modifiziert werden.

### Session Binding

Sessions können zueinander in Beziehung gesetzt werden. Das wird Session Binding genannt. Eine Session mit Session ID SID A ist an eine Session mit SID B gebunden, wenn in ihren Messages ein BOUND_SESSION_ID Objekt vorhanden ist. Im Objekt steht die ID von Session B. Wenn Session B kein BOUND_SESSION_ID Objekt mit der ID von A hat, stehen die Sessions in einer asymmetrischen Beziehung. Eine Session kann mehrere Sessions an sich binden. Die Beziehung die durch Session Binding angezeigt wird, löst an sich keine Aktionen in der QNE aus. Die QNEs können jedoch anhand dieser Informationen Massnahmen ergreifen.

Session Binding wird z.B. für aggregierte und bidirektionale Reservationen verwendet. Wenn eine QNE eine Message erhält mit einem BOUND_SESSION_ID Objekt, muss sie das Objekt in alle Messages kopieren, die sie für diese Session verschickt.

### Aggregierte Reservation

Eine aggregierte Reservation dient zur Reduktion von Einzelreservationen auf dem selben Pfad und somit zur Reduktion der Verarbeitungslast, die durch Signaling Messages auf den QNEs verursacht werden.

Eine aggregierte Reservation kommt wie folgt zustande. Eine normale Reservation wird initiiert (siehe Abbildung 6.11). Beim Aggregator angekommen wird eine neue Reservation (in der Abb. Reserve') für den aggregierten Fluss initiiert. Der Aggregator markiert die Messages der individuellen Reservation, damit sie von den folgenden QNEs nicht inspiziert werden. Markiert werden sie durch einen vordefinierten NSLP-ID Wert. Der NSLP-ID Wert ist ein Parameter der `SendMessage`-Funktion des GIST API. Der Deaggregator entfernt die Markierung wieder, indem er den NSLP-ID Wert wieder auf den QoS-NSLP-Vorgabewert setzt. Für die aggregierte Reservation ist der Deaggregator der QNR.

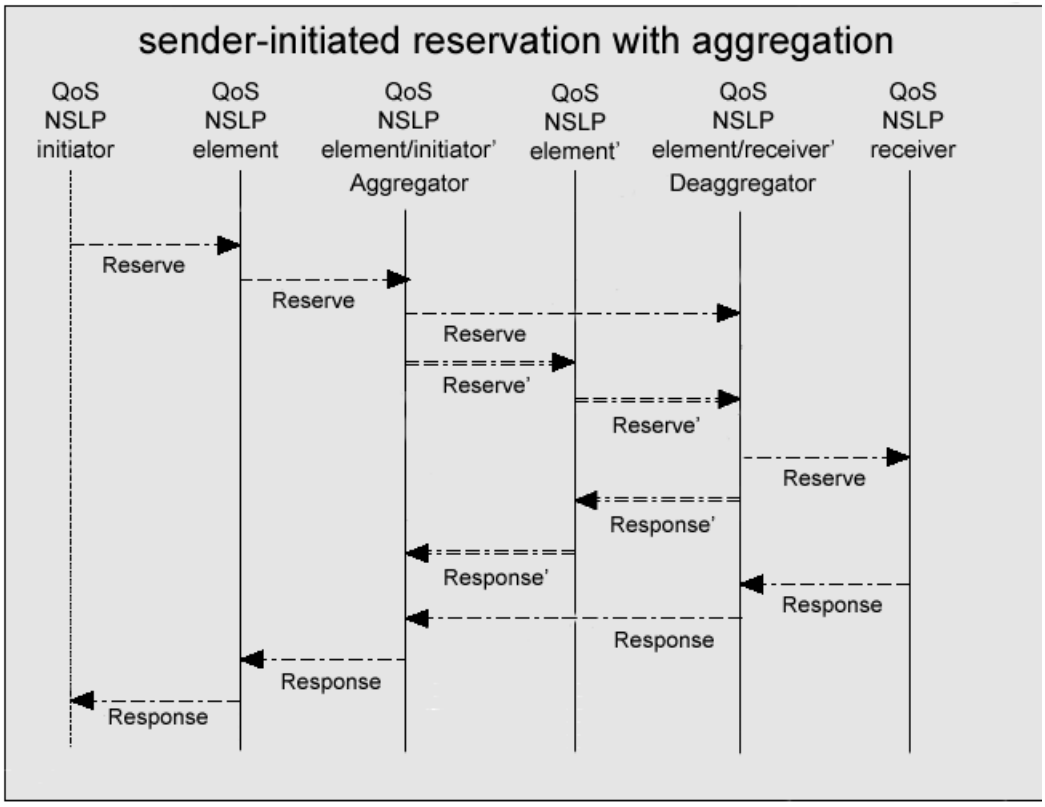



Abbildung 6.11: Senderinitiierte Reservation mit Aggregation [5]

### Message Scoping

Der Bereich in dem sich Messages bewegen, kann auf mehrere Arten eingeschränkt sein. Eine QNE kann lokale Regeln haben, welche entscheiden ob eine Message weiterverarbeitet wird oder nicht. Man kann die Reichweite der Reserve oder Query Message mit dem

SCOPING Flag einschränken. Ist das Scoping Flag 0, dann darf sich die Message auf dem ganzen Pfad bewegen. Ist das Flag 1, darf sie nur bis zur nächsten QNE.

Die Response Message wird nur bis zu der QNE weitergegeben, welche die Response Message mittels RII Objekt angefordert hat.

#### Priorität

Da manche Messages oder Reservationen wichtiger sind als andere, können Messages und Reservationen eine Priorität zugewiesen werden.

GIST gibt Möglichkeiten Messages eine Priorität zuzuweisen. Die Priorität einer Reservation kann mittels QSPEC Parameter festgelegt werden.

#### Rerouting

Wenn sich der Pfad der Datenübertragung ändert, muss sich QoS NSLP anpassen. Dafür müssen Routenänderungen erkannt, neue Reservationen entlang des neuen Pfades gemacht und eventuell die alte Reservation entfernt werden. Routenänderungen sind auf drei Stufen erkennbar. Die erste Stufe ist, dass bestimmte QNE oder GIST Implementationen von einem Routing Modul die Informationen beziehen. Dies liegt ausserhalb des NSIS Frameworks. Bei der Zweiten stellt GIST die Informationen über sein API bereit. Bei der dritten erkennt QoS NLSP selbst die Änderung.

Eine QNE erkennt eine Änderung, wenn sie eine Message bekommt, welche eine veränderte Source Identification Information (SII) hat. Die SII-handle ist Teil des GIST API und markiert eine QNE eindeutig. Eine veränderte SII zeigt also an, dass sich der Absender der Message geändert hat und somit auch der Pfad.

Eine neue Reservation kommt wie folgt zustande. Wenn die QNE beim Scheidepunkt eine verkürzte Reserve Message an den nächsten Knoten des neuen Pfades schickt, löst dies bei jenem Knoten einen Fehler aus. Dieser schickt eine Response Message mit dem Error zurück. Dies bewirkt dass eine komplette Reserve Message mit QSPEC Objekt verschickt wird. Diese Reserve Message macht auf dem neuen Pfad die Reservation. Wenn die Response Message als Bestätigung für die gelungene Reservation zurück kommt, muss die QNE am Scheidepunkt eine Reserve Message mit gesetztem T-Flag den alten Pfad entlang schicken, um die alte Reservation abzubauen.

### 6.5.3 Beispiele für QoS NSLP Operationen

#### Senderinitiierte Reservationen

Im Falle einer senderinitiierten Reservation erstellt der Sender eine Reserve Message. Siehe Abbildung 6.12. Er ist somit der QNI (QoS NSLP initiator). In der Reserve Message

enthalten, ist ein QSPEC Objekt, welches die benötigten Parameter für das gewählte QoS Modell beschreibt. Diese Reserve Message wird anschliessend über GIST an die nächste QNE gesendet. Die Nachricht wird in dieser QNE verarbeitet. In der Policy Control der QNE wird entschieden, ob der Initiator die Berechtigung hat eine Reservation zu erstellen und in der Admission Control wird geprüft, ob überhaupt die nötige Ressourcen für die Reservation vorhanden sind. Fallen diese Entscheidungen positiv aus, installiert die QNE entsprechend dem QSPEC Objekt eine Reservation. Anschliessend generiert die QNE eine neue Reserve Message, üblicherweise basierend auf der empfangenen Nachricht. Diese Nachricht wird dann an GIST übergeben und an die nächste QNE übermittelt. Das ganze wiederholt sich bis der QNR (QoS NSLP receiver) erreicht wird. Der QNR kann der Empfänger der Daten sein, kann aber auch einfach der letzte Knoten sein der QoS NSLP unterstützt.

Ein Knoten kann von seinem direkten Nachbar (Peer) eine Bestätigung anfordern. Dies wird durch das setzten des A-Flags erreicht. Die Bestätigung erfolgt in Form einer Response Message. Die Response Message kann einerseits bestätigen dass die Installation erfolgreich war oder andererseits eine Fehlermeldung liefern.

Ein Konten kann eine Response Message anfordern, indem er der Reserve Message ein Request Identification Information (RII) Objekt hinzufügt. Das RII ist eine Zahl die so gewählt ist, dass sie sehr wahrscheinlich nur ein einziges mal in der Session vorkommt. Wenn ein weiterer Knoten auch eine Response Message möchte, dann muss kein weiteres RII Objekt hinzufügen werden. Er muss einfach die bereits vorhandene Nummer speichern und hereinkommende Response Messages, welche auch ein RII Objekt haben, mit dem Wert vergleichen. Die Response Message muss danach weiter in Richtung des Knotens geschickt werden, welcher ursprünglich das RII hinzugefügt hat.

Wenn ein Knoten eine Reserve Message mit einem RII Objekt empfängt, schickt er nur in folgenden Situation einen Response Message:

1. Das Scoping Flag ist gesetzt oder
2. Die QNE ist die letzte auf dem Pfad der aktuellen Session.

Normalerweise fügt der QNI das RII hinzu um eine Bestätigung der Reservation zu bekommen. Wenn ein Timeout der Response Message stattfindet, darf nur der Knoten, welcher das RII Objekt ursprünglich hinzugefügt hat, die Reserve Message erneut senden.

### Senden eines Query

Die Query Message kann dazu verwendet werden, Information entlang des Datenpfades zu sammeln. Dies kann z.B. vor einer tatsächlichen Reservation stattfinden. Die Query Message enthält auch ein QSPEC Objekt. Dazu noch ein Idendifikationsobjekt, welches dazu verwendet wird die Response Message so zu markieren, dass sie der Query Message zugeordnet werden kann. Die Query Message wird über GIST an die nächste QNE übermittelt.

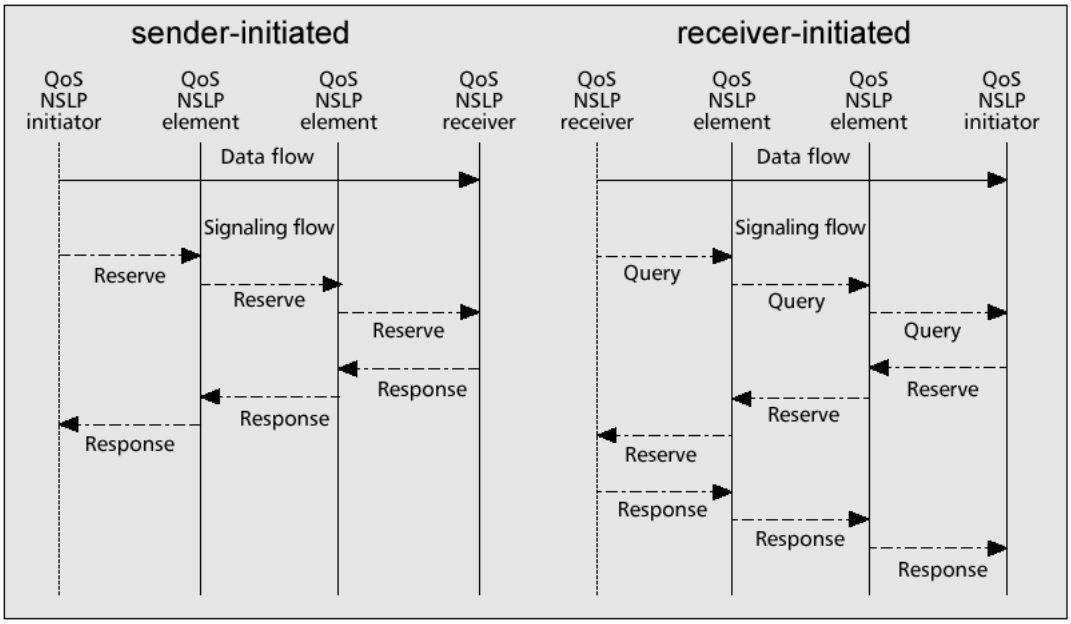



Abbildung 6.12: Senderinitiierte Reservation und empängerinitiierte Reservation [5]

Der Empfängerknoten inspiziert die Query Message und generiert eine neue Query, welche zusätzlich noch die angeforderten Information enthält. Ein Beispiel für solche Informationen ist die vorhandene Bandbreite der QNE für eine eventuelle Reservation. Solange der Knoten nicht der QNR ist oder der Geltungsbereich (Scope) der Query noch nicht erreicht wurde, wird die neue Message an die nächste QNE gesendet.

### Empängerinitiierte Reservationen

Bei der empfängerinitiierten Reservation sendet der Sender (QNR) zuerst eine Query Message mit gesetztem R-Flag. Siehe Abbildung 6.12. Die Query Message enthält ein QSPEC Objekt. Die Query muss keine Response Message auslösen, enthält also kein RII Objekt.

Die Query Message wird vom QNR über GIST zur nächsten QNE gesendet, welche die Nachricht liest. Wenn es das verwendete QoS Modell verlangt, werden dem QSPEC Objekt benötigte Information über die Pfadcharakteristik hinzugefügt. Danach wird aufgrund der Alten eine neue Query Message generiert, welche dann zur nächsten QNE gesendet wird. Dies geschieht solange bis der Empfänger erreicht ist.

Das R-Flag zeigt an, dass der Empfänger (QNI) die Reservation machen soll. Er generiert eine Reserve Message. Dafür nimmt er das QSPEC Objekt, welches mit der Query Message gekommen ist. Die Reserve Messages werden analog der senderinitiierten Reservation von peer zu peer weitergeleitet. Sie nehmen den entgegengesetzte Weg der Query Messages bis zum Sender (Dabei wird der GIST reverse path state verwendet). Jeder Knoten kann auch hier seiner Reserve Message ein RII Objekt hinzufügen, um eine Response Message anzufordern. Abschliessend wird vom QNR eine Response Message gesendet, um die Reservation zu bestätigen.

Tabelle 6.1: Zusammenfassung der Grundlegenden Eigenschaften von RSVP und QoS NSLP [1]

| | RSVP | NSLP QoS |
|---|---|---|
| Protokol Struktur | Eine Schicht | Zwei Schichten |
| Transport | IP oder UDP | TCP, STCP, UDP, DCCP |
| Reservations-initiatoren | Empfänger | Empfänger und Sender |
| States | Soft | Soft |
| QoS Modelle | IntServ, DiffServ | IntServ, DiffServ und andere |
| Scope of Signaling | End-to-end | End-to-end, host-to-edge, edge-to-edge |
| Multicast | Ja | Nein |
| Mobilität | Nein | Ja |
| Bi-direktional | Nein | Ja |
| Aggregation | Ja | Ja |
| Summary Refresh | Ja | Ja |
| Priority/preemption | Ja | Ja |

**Bidirectionale Reservationen**

Wenn sowohl ein Datenfluss von einer QNE A zu einer QNE B geht und von B nach A, können die Signaling Sessions mittels Session binding aneinander gebunden werden. Dies wird Bidirektionale Reservation genannt. Es werden zwei Szenarien unterschieden:

- Zwei senderinitiierte Sessions werden aneinander gebunden, z.B eine senderinitiierte von A nach B und eine von B nach A.
- Eine senderinitiierte und eine empfängerinitiierte Session werden aneinander gebunden, z.B. eine senderinitiierte von A nach B und eine empfängerinitiierte von A nach B.

Beide Seiten müssen sich vorher absprechen welche Variante sie wählen wollen. Diese Absprache muss ausserhalb des NSIS Frameworks passieren.

### 6.5.4 QoS NSLP versus RSVP

In Tabelle 6.1 sind die Eigenschaften von QoS NSLP und RSVP aufgelistet. Die Vorteile von QoS NSLP gegenüber RSVP sind Folgende:

- QoS NSLP kann mehrere verschiedene QoS Modelle auf dem gleichen Datenpfad anwenden, mit einer einzigen Signaling Message.
- Der Transport der Messages von QoS NSLP (und GIST allgemein) unterstützt sowohl unzuverlässige (z.B. UDP) wie auch zuverlässige (z.B. TCP) Protokolle. Im Gegensatzt zu RSVP welches nur unzuverlässige verwendet

- Sowohl Sender als auch Empfänger kann bei QoS NSLP einen Reservation aufbauen. Bei RSVP kann nur der Sender.
- Durch die Verwendung von GIST in mehreren Signaling Protokollen, könnten Drittanwendungen wie z.B. Firewalls und NATs besser Rücksicht auf Signaling Applikationen nehmen, weil sie nur zu GIST kompatibel sein müssen und nicht noch zum Signaling Protokol der Applikation. Das könnte auf längere Sicht die Zuverlässigkeit von QoS NSLP gegenüber der von RSVP steigern.
- RSVP kann nur Ende-zu-Ende Verbindung erstellen. QoS NSLP kann Ende-zu-Ende, Host-zu-Edge und Edge-zu-Edge.

Der Vorteil von RSVP gegenüber QoS NSLP ist, dass RSVP IP Multicast unterstützt. Eine Implementation wäre theoretisch auch in QoS NSLP realisierbar, wurde jedoch nicht umgesetzt, da IP Multicast nicht weit verbreitet ist. Daher wiegt dieser Nachteil auch nicht schwer.

## 6.6 Fazit

Die Bestrebungen der IETF, die Signalisierung in der IP-Umgebung zu standardisieren, sind sicherlich Begrüssenswert. Es stellt sich aber die Frage, ob es das angestrebte universelle Signalisierungsprotokoll überhaubt gibt. Es ist auch ganz klar zu sagen, dass das eigentlich universelle die NTLP-Schicht ist. Die NSLP Applikationen werden immer sehr vielfältig sein und es auch bleiben. Es erstaunt auch, dass in [4] keine Verweise auf andere Signalisierungsprotokolle gemacht werden. Alle Verweise sind auf RSVP oder direkt auf NSLP-Applikationsvorschläge. Dies würde die Vermutung unterstützen, dass NSIS keine universelles sondern ein weiteres Signalisierungsprotokoll ist, mit einer Anzahl bestimmter Applikationen.

# Literaturverzeichnis


[1] Xiaoming Fu, H. Schulzrinne, A. Bader, D. Hogrefe, C. Kappler, G. Karagiannis, H. Tschofenig, S. Van den Bosch: NSIS: a new extensible IP signaling protocol suite, IEEE Communications Magazine, Vol. 43, Issue 10, October 2005.

[2] Next Steps in Signaling (NSIS) IETF Working Group, `http://ietf.org/html.charters/nsis-charter.html`.

[3] R. Hancock, G. Karagiannis, J. Loughney, S. Van den Bosch: Next Steps in Signaling (NSIS): Framework, IETF RFC 4080, June 2005.

[4] H. Schulzrinne, R. Hancock: GIST: General Internet Signaling Transport, Internet-Draft, draft-ietf-nsisntlp-09.txt, Februar 2006.

[5] J. Manner, G. Karagiannis, and A. McDonald: NSLP for Quality-of-Service signaling, Internet draft, draft-ietf-nsis-qos-nslp-10.txt, March 2006.

[6] J. Manner and X. Fu: Analysis of Existing Quality-of-Service Signaling Protocols, RFC 4094, `http://www.rfceditor.org/rfc/rfc4094.txt`.

[7] R. Hancock et al.: A Problem Statement for Path-Decoupled Signaling in NSIS, Internet draft, work in progress `http://www.ietf.org/internetdrafts/draft-nsis-pds-problem.txt`, July 2005.

[8] M. Stiemerling, H. Tschofenig, and C. Aoun: NAT/Firewall NSIS Signaling Layer Protocol (NSLP), Internet draft, work in progress, `http://www.ietf.org/internet-drafts/draftietf-nsis-nslp-natfw-11.txt`, April 2006.

[9] F. Dressler et al.: NSLP for Metering Configuration Signaling, Internet draft, work in progress, `http://www.ietf.org/internetdrafts/draft-dressler-nsis-metering-nslp-02.txt`, July 2005.

[10] C. Kappler and X. Fu: A QoS Model for Signaling IntServ Controlled- Load Service with NSIS, Internet draft, work in progress, `http://www.ietf.org/internet-drafts/draft-kappler-nsisqosmodel-controlled-load-02.txt`, July 2005.

[11] J. Ash, A. Bader, and C. Kappler: QoS-NSLP QSPEC Template, Internet draft, work in progress, `http://www.ietf.org/internet-drafts/draft-ietf-nsis-qspec-09.txt`, March 2006.

[12] S. Lee et al.: Applicability Statement of NSIS Protocols in Mobile Environments, Internet draft, work in progress, `http://www.ietf.org/internet-drafts/draft-ietf-nsis-applicabilitymobility-signaling-04.txt`, March 2006.

[13] C. Shen, H. Schulzrinne, S. Lee, and J. Bang: Internet Routing Dynamics and NSIS Related Considerations, Technical Report CUCS-007-05, Department of Computer Science, Columbia University, New York, NY 10027, 2005.

[14] H. Schulzrinne and R. Hancock. GIMPS: General Internet Messaging Protocol for Signaling, Internet Draft, Internet Engineering Task Force, Work in progress, 2004.

[15] B. Stiller: Quality of Service - Dienstgüte in Hochleistungsnetzen, 1996.

[16] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, RFC 2205, September 1997.

[17] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, SIP: Session Initiation Protocol, RFC 3261, `http://www.ietf.org/rfc/rfc3261.txt`, June 2002.

[18] Signaling Transport (sigtran) Working Group, `http://www.ietf.org/html.charters/sigtran-charter.html`.

# Kapitel 7

# VoIP Protokolle

*Somala Mang, Christian Signer, Baer Jonas*

*Diese Arbeit vergleicht die VoIP-Protokolle SIP, IAX2, H.323 und betrachtet zudem Skype. Diese Protokolle werden anhand der Punkte Übersicht, Hauptbestandteile, Funktionalität und Sicherheit detailliert beschrieben. Der Fokus dabei liegt auf SIP. Nach diesen Ausführungen betrachten wir die Unterschiede der Protokolle in den folgenden Punkten: Genereller Überblick, Protokollstruktur, Zentralisierungsgrad, Effizienz, Anwendungen sowie NAT und Firewalleinschränkungen. Am Ende werden die drei Protokolle bezüglich zukünftiger Entwicklungen im Bereich VoIP bewertet.*

## Inhaltsverzeichnis

**7.1 Einleitung . . . . . 209**
**7.2 VoIP Protokolle . . . . . 209**
7.2.1 SIP . . . . . 209
7.2.2 H.323 . . . . . 218
7.2.3 IAX2 . . . . . 223
7.2.4 Skype . . . . . 227
**7.3 Vergleich . . . . . 230**
7.3.1 Übersicht . . . . . 230
7.3.2 Protokollstruktur . . . . . 231
7.3.3 Zentralisierungsgrad . . . . . 231
7.3.4 Effizienz . . . . . 232
7.3.5 Anwendungen . . . . . 232
7.3.6 NAT und Firewall . . . . . 233
**7.4 Schlussfolgerungen . . . . . 234**

## 7.1 Einleitung

Der Begriff Voice over IP (VoIP) war lange negativ besetzt, da er während dem Internet Hype sehr häufig zur Sprache gekommen ist. Durch das Scheitern der New Economy sahen nun viele den Entscheidungsträger VoIP als gescheiterte Technologie. Seit 2001 jedoch stösst diese Technologie auf immer breiteres Interesse und erfreut sich sehr starker Zuwachszahlen.

Interessant ist nun jedoch vor allem die Betrachtung der dem VoIP zugrunde liegenden Protokolle. Die wichtigsten drei Protokolle sind SIP [8], IAX [37] und H.323 [25]. Diese Arbeit wird Skype, welches bereits über mehrere Millionen User verfügt, ebenfalls streifen.

Die Interessen der Telekommunikationsanbieter wiederspiegeln die Spezifikation von H.323, welches von der ITU (International Telecommunication Union) stammt.

Das dritte Protokoll im Zusammenhang mit VoIP ist IAX. Dieses entstand erst nach der Spezifikation von SIP und H.323. Ziel dieses Protokolls, welches von M. Spencer und F. Miller spezifiziert wurde, war die Geschwindigkeit und Effizienz von VoIP zu steigern.

Diese Arbeit ist folgendermassen strukturiert:

- Kapitel 2 bietet einen Überblick über die vier wichtigsten Protokolle. Betrachtet werden der Initiator des Protokolls und dessen Ziele. Die technischen Aspekte, wie die Funktion, die Architektur und die wichtigsten Bestandteile des Protokolls werden erläutert. Der Schwerpunkt liegt dabei auf SIP, wobei H.323 als sehr umfassende Spezifikation ebenfalls sehr umfangreich beschrieben wird.
- Kapitel 3 vergleicht nun die verschiedenen Protokolle. Dabei werden technische Aspekte, momentane Anwendungen, Effizienzkriterien aber auch aktuelle Sicherheitsfragestellungen das Grundgerüst des Vergleichs bilden.
- Kapitel 4 fasst noch einmal die grundlegenden Thesen zusammen und bewertet die vier Protokolle in Bezug auf die zukünftige Entwicklung von VoIP.

## 7.2 VoIP Protokolle

### 7.2.1 SIP

#### Übersicht

Session Initiation Protocol ist ein standardisiertes Protokoll der IETF, für das 1996 erste Vorschläge auftraten. Seither wurde dieses Protokoll ständig weiterentwickelt. Der Hauptbegründer von SIP ist Henning Schulzrinne, der auch das Realtime-Protokoll entwickelt hat [2]. Mit der steigenden Anzahl verschiedener Internetanwendungen wuchsen

auch die Anforderungen. Bei der Entwicklung von SIP wurde auf die Implementierbarkeit, Erweiterbarkeit, Skalierbarkeit und Flexibilität geachtet [7]. 1999 wurde SIP unter RFC2543 standardisiert und im Jahr 2001 auf den neuen Stand in RFC3261 gebracht [4].

Durch das rasche Wachstum des Internets erhöht sich die Zahl der Internetanwendungen laufend. Einige davon sind Voice-, Video-, Chat-Applikationen oder Games, die in unserer Zeit [1] nicht mehr wegzudenken sind. In VoIP wird SIP oft zur Verwaltung und Koordination von Sitzungen in IP-Telefonie oder Videokonferenzen eingesetzt. Der Aufbau der Verbindung mit SIP und die hierbei agierenden Komponenten wie der User Agent Client (UAC) bzw. User Agent Server (UAS), Location Server, Proxy Server, Redirect Server und Registrar Server werden in den Abschnitten Hauptelemente und Funktionalität näher beschrieben. Der grundsätzliche Zweck von SIP ist der Aufbau der Session zwischen den Teilnehmern. Es soll hier erwähnt sein, dass dieses Protokoll nicht als Datenaustausch, sondern zur Herstellung der Verbindung unter den Teilnehmern eingesetzt wird. Für den Datenaustausch [3] sind andere Protokolle zuständig wie SDP (Session Description Protokoll) und Realtime Transport Protokoll (RTP), die in diesem Dokument aber nicht näher beschrieben werden.

Zu einer Verbindung zwischen den Teilnehmern gehören SIP-Nachrichten, die sich in SIP-Request und SIP-Response unterscheiden. Ersteres wird für die Initialisierung benötigt und letzteres als Bestätigung der erhaltenen Anfrage, die den Status ebenfalls mitteilt. Generell gilt für SIP Nachrichten, dass sie textbasiert und zeilenweise strukturiert werden/sind. Die Nachricht besteht aus der Startzeile, dem Message Header und einem Message-Body [6]. Die SIP Uniform Resource Identifier (SIP URI) [8], die zur Identifikation des Users notwendig ist, hat die Form sip:username@domain. Wie bei vielen Internetanwendungen spielt auch bei SIP die Sicherheit eine wichtige Rolle.

Das Kapitel Session Inititation Protocol wird folgendermassen strukturiert: Zuerst werden die Hauptelemente und die Beziehungen zueinander erläutert. Danach folgt ein Abschnitt über die Funktionalität von SIP, über die Registrierung des Teilnehmers und die Beschreibung der SIP-Nachricht. Zum Schluss werden die Sicherheitsaspekte von SIP behandelt.

### Hauptelemente

SIP beschreibt folgende fünf Hauptelemente:

**User Agent** Wie beim herkömmlichen Telefonieren wird eine Verbindung zwischen dem Anrufer und dem Angerufenen hergestellt. Der Begriff User Agent ist die Instanz beziehungsweise der Endpunkt, bei dem der Call initiiert wird. Er kann im SIP Telefon oder auch in einem Computer implementiert sein. Je nach Situation ist er ein User Agent Client oder ein User Agent Server. Wenn er eine Anfrage abschickt, fungiert er als User Agent Client, sein Zustand wechselt jedoch, sobald er eine Antwort vom Empfänger erhalten hat, in einen User Agent Server [8]. Jeder User Agent hat sich beim Registrar anzumelden, welches mit der Register-Methode geschieht. Auf diese Weise macht er sich im Netzwerk bekannt und ist dann für andere User Agent erreichbar.

**Location Server** Über jeden angemeldeten Teilnehmer werden Informationen im Location Server gespeichert. Es sind Informationen über die IP Adressen der User und welche Dienste sie beanspruchen [9]. Der Location Server ist verantwortlich für die Speicherung der SIP Adressen und kann sie dynamisch lokalisieren. Dadurch fördert er die Mobilität und die bessere Erreichbarkeit des Users. Wenn ein Call initiiert wird, kommt der Location Server ins Spiel und liefert die gewüschte aktuelle Adresse zurück.

**Proxy Server** Die User können Registrierungen oder Anfragen (Requests) an den Proxy Server senden. Seine Aufgabe besteht darin, diese Requests an die User Agent Clients und die Responses an die User Agent Server weiterzuleiten. Er sorgt hierbei für ein optimales Routing [8]. Man kann ihn also als einen Zwischenhändler zwischen dem User Agent A und dem User Agent B betrachten, der die Requests so nah wie möglich an den Zielempfänger bringt [8]. Ausserdem kann er Anforderungen vom Benutzer bezüglich der Authentifikation erzwingen, die aber erst im Abschnitt Sicherheitsaspekte beschrieben werden. Für die Weiterleitung muss der Proxy Server die SIP Adresse ausfindig machen, nach welcher der User Agent Client eine Anfrage gestellt hat. Somit wendet sich der Proxy Server an den Location Server, der für ihn die Zieladresse lokalisiert [9]. Der Proxy Server ist ausserdem in einen Stateless und Stateful Server zu unterteilen. Im Stateless Modus leitet der Proxy Server jeden Request weiter und löscht nach der Weiterleitung die Informationen über diese Nachrichten [8].

**Redirect Server** Anders als beim Proxy Server dient Redirect Server nicht als Weiterleitungsfunktion. Er nimmt lediglich Requests auf, sammmelt alternative Zieladressen von Teilnehmern und gibt die gültige Zieladresse direkt an den Anfragenden zurück. Mit der Wahl der richtigen Zieladresse fördert er ausserdem die Robustheit der Signalisierung [8] und entlastet damit den Proxy Server, da der User Agent selbst die gefundene Adresse kontaktieren kann. Wie der Proxy Server interagiert auch er mit dem Location Server, da er aufgrund seiner Aufgabe ebenfalls die SIP Adressen ausfindig machen muss.

**Registrar Server** Der Registrar Server nimmt die Registrierungsanfragen der User entgegen und verwaltet sie. Die SIP-Adresse, die mit dieser Nachricht verbunden ist, wird in den Location Server gebracht. Dieser wird durch den Registrar Server in den aktuellen Zustand gebracht und vor Inkonsistenz geschützt [9].

### Funktionalität

In diesem Kapitel geht es um die Funktionalität des SIP und die grundsätzlichen Methoden von SIP, die im Ablauf eines Calls und in ihrer Handhabung benötigt werden. Alle Methoden sind hier aufgelistet und kurz erklärt:

- INVITE : Initialisierung der Session durch Einladung zur Kommunikation [9].
- ACK : Bestätigungsnachricht, dass der Empfänger den Request erhalten hat [9].

- BYE : Hiermit wird der Call beendet [9].
- CANCEL : Benötigt, wenn keine Rückantwort kommt und User Agent Client den Call abbrechen will [9].
- REGISTER : Registrierungsnachricht mit aktueller SIP Adresse [9].
- OPTIONS : Möglichkeit, Informationen über die Fähigkeiten der User Agents herauszufinden [8].

Bei der Funktionalität betrachtet SIP folgende Aspekte: Es sind die Lokalisierung des Users über den Location Server, die Erreichbarkeit des User Agents mittels der SIP Adresse, die Bestimmung der Parameter über die Dienste des Users (Capabilities), der Aufbau der Session mit dem INVITE Request und zu guter Letzt das Management der Session [8].

Das folgende Beispiel erläutert die Prozedur eines Aufrufs. Um das Beispiel übersichtlich zu gestalten, wurden nur die wichtigsten Nachrichten notiert.

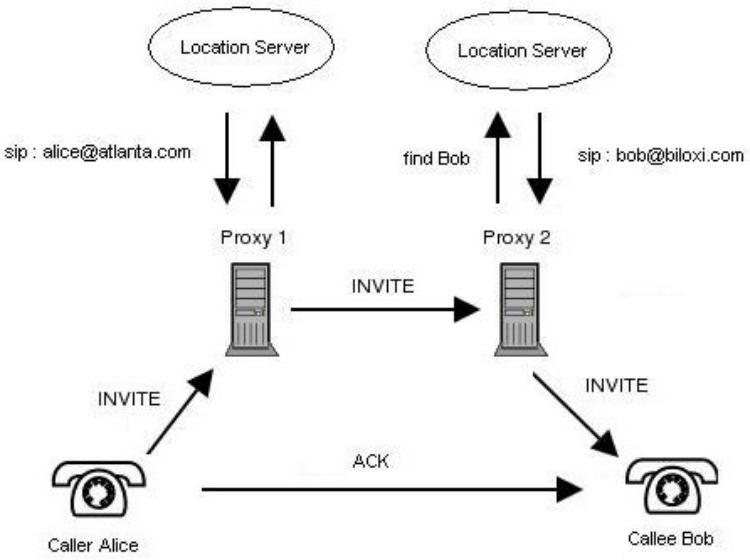



Abbildung 7.1: SIP Kommunikation [5]

Ein User Agent namens Alice, im obigen Bild der Caller, lädt mit einem INVITE-Request einen User Agent Bob, den Callee, zu einer Session ein. Dieser Request geht zunächst an den Proxy Server von Alice, bei dem sich die Domain ihrer SIP-Adresse befindet. Der Proxy Server gibt danach als Bestätigung eine 100 Trying Response an den Caller zurück.Mit Hilfe von einem Domain Name Service findet er Proxy Server 2. Da nun dessen IP-Adresse bekannt ist [8] kann die INVITE-Request an Proxy Server 2 geschickt werden. Nach Empfang der Nachricht schickt dieser eine 100 Trying Response an den Proxy Server 1 zurück. Proxy Server 2 fragt bei seinem Location Server die aktuelle Zieladresse von Bob nach [3]und leitet den Request an Bob weiter. Bei Bob trifft nun die Einladung ein, die er annehmen oder ablehnen kann. Eine 180 Ringing Response geht auf gleichem Weg über die beiden Proxies zu Alice zurück und zeigt an, dass es bei Bob nun klingelt [8].

Bob nimmt den Call an und sendet eine 200 OK Response an Alice, welche eine ACK-Nachricht an Bob zurücksendet. Alice und Bob kennen nun die gegenseitigen Adressen und sind bereit für die Media Session. Wenn einer der beiden die Session beenden will, muss er den anderen mit der BYE-Nachricht benachrichtigen. Dieser bestätigt mit 200 OK Response [3], worauf die Session abgebrochen wird.

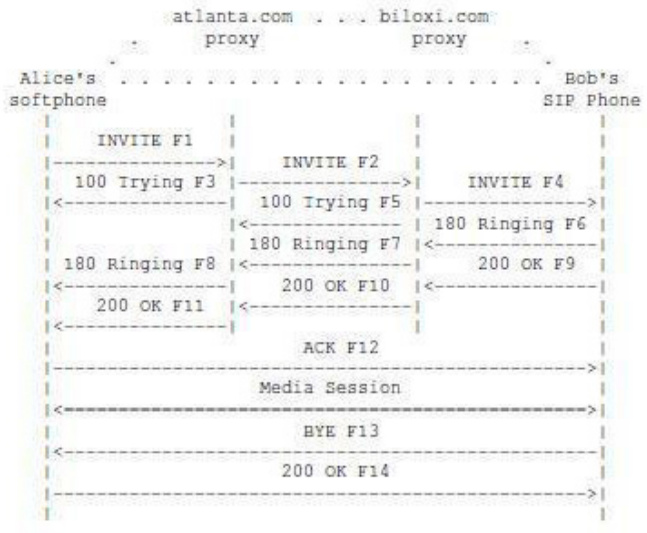



Abbildung 7.2: SIP Verbindungsaufbau [8]

Wenn ein Teilnehmer, während der Session eine Änderung an ihr vornehmen will, wird dies mittels einer Re-INVITE-Methode innerhalb der schon etablierten Verbindung bewerkstelligt. Änderungen können zum Beispiel die SIP Adressen, Codecs oder Ports [8] betreffen, je nach dem, um welche Verbindungsparameter es sich handelt. Derjenige User sendet dann die modifizierten Parameter mit der Re-INVITE-Methode ab. Bei Akzeptanz erhält er eine 200 OK Response und die veränderten Parameter werden umgesetzt. Andernfalls kommt eine Fehlermeldung [8], die besagt, dass die Veränderung nicht toleriert wird.

Der Vorteil mit dieser Methode ist die einfache Möglichkeit einer Sessionänderung, ohne dass dabei die Verbindung gestört und abgebrochen wird [3]. Aber diese Methode zur Sessionänderung kann sich auch als nachteilig erweisen. Dies dann, wenn der Netzwerkverkehr zusätzlich belastet wird, wodurch dann Netzwerkstau resultieren kann [8].

In Bezug auf den INVITE-Request spielt die CANCEL-Methode auch eine wichtige Rolle. Der mit INVITE initialisierte Verbindungsaufbau kann dadurch vorzeitig [3] unterbrochen werden. Die CANCEL-Methode wird in Zusammenhang mit INVITE bei versuchtem Verbindungsaufbau benutzt. Bei bestehender Verbindung wird die BYE-Methode angewendet [8] für die Terminierung der Session.

Als nächstes wird nun die Registrierung behandelt. Die Registrierung jedes User Agents ist sehr wichtig, da mit der Anmeldung die Informationen über ihn aufgenommen werden und für den Aufbau der Session notwendig sind. Denn wie bereits aufgezeigt, muss erst die SIP Adresse des anzurufenden Endpunkts bekannt sein. Diese Daten gehen an den Registrar

Server, der mit den neuen Informationen aktualisiert wird [8]. Für den Proxy Server und Redirect Server spielt daher die Aktualisierung des Registrar Servers eine zentrale Rolle.

Die OPTION-Methode dient dazu, Informationen bezüglich der unterstützten Methoden [8], Erweiterungen, Codecs und weitere Fähigkeiten abzufragen. Diese Informationen können für die Session nützlich sein und liefern Hinweise [8], ob der betroffene User Agent Server dessen INVITE-Request akzeptieren wird oder nicht.

Zur Unterscheidung der Nachrichtenart werden hier die verschiedenen Elemente nochmals aufgezählt. SIP-Requests sind bekanntlich INVITE, ACK, BYE, CANCEL, OPTIONS und REGISTER. SIP-Responses sind die aus dem vorherigen Beispiel genannten 100 Trying, 180 Ringing, 200 OK Responses. Es gibt zusätzlich noch weitere Arten der Responses [3] beispielsweise 301 Moved Permanently, 406 Not Acceptable, 505 SIP Version not supported und 600 Busy Everywhere [6].

SIP Responses sind abhängig von der Request-Methode. Bestehend aus einem numerischen Statuscode aus drei Bit langen Integer Codes, die den Zustand der Session beschreiben [6]. Hier nochmals allgemein aufgelistet [8]:

- 1xx : Request erhalten und weitere Bearbeitung
- 2xx : Request erfolgreich und akzeptiert
- 3xx : Weitere Bearbeitung und Weiterleitung nötig
- 4xx : Fehlermeldung auf Clientseite aufgrund falscher Syntax
- 5xx : Fehlermeldung auf Serverseite, wo Request nicht erfüllt werden kann
- 6xx : Globale Failure, Ausführung des Requests auf keinem Server erfolgreich

Jede SIP-Nachricht hat die gleiche Struktur. Die Nachricht des INVITE-Requests von Alice [8] kann wie folgt aussehen:


Abbildung 7.3: INVITE-Request [8]

**Sicherheitsaspekte**

In diesem Abschnitt wird gezeigt, welche Sicherheitsaspekte SIP berücksichtigt und inwiefern diese im Standard [8] spezifiziert sind. Die betrachteten Sicherheitskriterien sind: Authentizität, Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit, Verbindlichkeit und Anonymität / Pseudonymität.

SIP-Nachrichten enthalten sensible Informationen über die Teilnehmer der Session. Aus ihnen kann ermittelt werden, wer wann wie lange mit wem kommuniziert hat. Um die Privatsphäre zu schützen, müssen alle Informationen die Auskunft über die User geben, verschlüsselt oder anonymisiert werden.

Die Abbildung 7.2.1 zeigt die Sicherheitsmechanismen, welche in SIP vorgesehen sind.

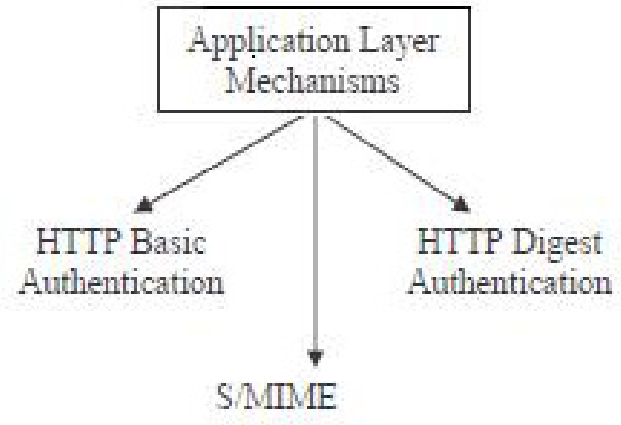



Abbildung 7.4: SIP Sicherheitsmechanismen [16]

**Authentizität** In SIP wird die Authentizität mit einem challenge-basierten Mechanismus geregelt, dessen Basis die Authentizität in http ist. Der Mechanismus, den SIP anwendet ist HTTP Digest Authentification, der die Erweiterung von HTTP Basic Authentification darstellt [20]. Nachdem der Client den Server anspricht, versendet der Server eine 401 Unauthorizised Response, welches eine Challenge Aufgabe für den Client darstellt, bei der er nun die gültige Antwort liefern muss [18]. Bei einem Proxy Server würde für die Authentizität eine 407 Proxy Authentication an den Client zurückgehen. Bei falschen Antworten erscheint im Browser die Forbidden-Nachricht, und er erhält somit keinen Zugriff.

Für die Authentifikation werden Header benutzt, die den Typ des Mechanismus, den Realm (die eindeutige SIP-Adresse eines Benutzers), die zu schützende Domain, der Username und das Passwort [21] beinhalten. Hier ein Beispiel [20]:

Allerdings ist zu erwähnen, dass dieser Authentifikationsmechanismus ungenügend ist, weil die Nachrichten mit dem From Header Field und To Header Field sichtbar sind. Der


Abbildung 7.5: SIP Authentifikation Header [15]

Grund dafür ist, dass eine Verschlüsselung dieser Daten fehlt, und sie im Klartext übermittelt werden. Dies stellt ein Sicherheitsrisiko dar. Ein Dilemma ist, dass die Zwischenhändler, beispielsweise der Proxy Server, diese Informationen für die korrekte Weiterleitung benötigen [8]. Eine weitere Schwäche ist zudem, dass der Server sich nicht selbst an der betreffenden Stelle authentifiziert, bevor er die Challenge absendet [19]. Er kann sich zwar Authentisieren, aber es ist nicht geregelt, dass er dies tun muss [8]. Angriffsbeispiel dieses Thema stellt Registration Hijacking dar, in der sich jemand im Namen eines Benutzers unberechtigterweise anmeldet[8].

**Vertraulichkeit und Integrität** Ein weiterer Angriffspunkt bei SIP ist, dass Proxy Server, die Routingentscheidungen treffen müssen und bei Versenden von Request, diese Nachrichten verändern können. Eine Drittperson kann sich bei der Kommunikation zwischen die Teilnehmer stellen und bekommt durch ein Täuschungsmanöver die Nachrichten, die eigentlich nur für den richtigen Zielempfänger bestimmt waren. Ohne eine Verschlüsselung der Nachricht kann die Drittperson sie modifizieren.

In SIP werden die beiden Sicherheitskriterien Vertraulichkeit und Integrität durch S/MIME (Secure Multipurpose Internet Mail) spezifiziert. Die User Agents benutzen Zertifikate, mit denen sie sich autorisieren und die SIP-Nachricht mit einem Key verschlüsseln können [8].

Der User Agent Client sendet einen Request, der mit S/MIME gesichert ist und eine Signatur enthält. Die Authentizität und Integrität werden durch die digitale Signatur gewahrt und die Nachricht verschlüsselt, um die Vertraulichkeit zu schützen [18]. Wenn nun der User Agent Server diese Nachricht bekommt, sollte er zuerst das Zertifikat validieren. Die Validierung geschieht am besten mit einer Zertifizierungsauthorität. Die Zertifizierungsauthorität prüft das Zertifikat und übermittelt es bei Gültigkeit dem User Agent Server. Dieses Zertifikat enthält den Namen des Besitzers, der die Nachricht geschickt hat. Der User Agent Server vergleicht nun den Namen mit demjenigen im From Header Field der Nachricht. Bei Übereinstimmung kann er sich über die Herkunft der Nachricht sicher sein. Dieselbe Prozedur läuft bei User Agent Client, der den Vergleich mit dem To Header Field macht.

Die Vertraulichkeit der Nachrichten wird durch die ganzheitliche Verschlüsselung zwar gewahrt. Wegen der End-to-End-Beziehung bezüglich der korrekten Weiterleitung von

Requests und Responses müssen jedoch die hierfür relevanten Header Fields wie Request-URI, Route und Via für die Proxies erkennbar sein. Aus diesem Grund ist es notwendig, dass man der Vertrauenswürdigkeit des Proxy Servers vertrauen kann, und er sie nicht zu anderen Zwecken nutzt [8].

**Verfügbarkeit** Um die Verfügbarkeit von SIP-Netzen zu prüfen, muss die Architektur in Bezug auf Denial-of-Services Attacken (DoS) betrachtet werden. Prinzipiell ist jeder Knoten im Netzwerk einem DoS Angriff ausgesetzt, denn jeder Knoten kann mit Nachrichten überlastet werden, sodass er seine eigentliche Aufgabe nicht mehr ausführen kann. Besonders anfällig für solche DoS Angriffe sind die verschiedenen SIP Proxy-Server, da sie vom Internet her direkt angesprochen werden können. Hierzu könnte z.B. die Re-Invite Nachricht verwendet werden, um die Datenlast auf dem Server einfach zu erhöhen [22]. Selbst eine Firewall kann diese Gefahr nicht komplett bannen, sondern nur verringern. Da SIP für den Datentransfer UDP-Ports verwendet, können auf diese Angriffe ausgeführt werden, so dass nicht der SIP-Server sondern die Firewall überlastet wird.

Ein ähnlicher Effekt kann mittels eingeschleuster BYE-Nachrichten erreicht werden. Dazu muss ein Angreifer die Etablierte Session beobachten und die entsprechenden Parameter auslesen. Wurden alle erforderlichen Daten besorgt, kann der Angreifer mittels einer konstruierten BYE-Nachricht die Session beenden.

**Verbindlichkeit** Für die Verbindlichkeit oder Nicht-Abstreitbarkeit der Nachrichten muss die Herkunft der Daten beziehungsweise die des Senders nachweisbar sein. Die entsprechenden Teilnehmer müssen sich identifizieren, wie bereits in Authentizität und Vertraulichkeit und Integrität beschrieben. Die Verbindlichkeit der Nachrichten hängt davon ab, welche Sicherheitsmechanismen der SIP-Provider implementiert hat. SIP baut auf anderen Sicherheitsmodellen auf, anstatt eigene zu definieren [8]. So kann Beispielsweise S/MIME eingesetzt werden, um eine Verschlüsselung und signierung der Nachrichten gewährleisten zu können.

**Anonymität / Pseudonymität** Die Sicherheitskriterien Anonymität und Pseudonymität können anhand der Bedeutung des From- und To- Header Fields erläutert werden. Diese Header Fields weisen auf die logische Identität des User Agent Clients beziehungsweise auf die des User Agent Servers hin [8]. Die URI (Uniform Ressource Identifier) und optional der Name sind darin enthalten. Deswegen spielt mit der Authentifikation auch die Geheimhaltung aller Informationen über den User assoziiert [1] eine bedeutende Rolle.

Hierzu gibt es die Möglichkeit der selektiven Anonymität, um Header Fields zu verschlüsseln. Wenn ein User Informationen über sich verbergen will, kann er dies tun indem er einen Request mit einem Header Field verschickt, das keine persönlichen Daten enthält [8]. Dazu kann er den Namen Anonymous als Pseudonym angeben und eine beliebige URI wählen wie dieses Beispiel zeigt: sip:anonymous@anonymizer.invalid. Im Request ist ein zweites From Header Field vorhanden, welches die richtige Adresse des Senders beinhaltet. Dieses ist jedoch verschlüsselt ist und nur für den Empfänger ersichtlich [8]. Es können

aber nicht alle Header verschlüsselt werden. Der To-Header muss für die Routingentscheidung angegeben werden [1]. Dies ist bei Vertraulichkeit und Integrität bereits erwähnt worden.

**Schlussfolgerungen** Die oben genannten Punkte zeigen, dass SIP Sicherheitsrichtlinien definiert. Diese sind jedoch nicht immer verbindlich, was den Anbietern von SIP-Servicen die Freiheit lässt, diese zu implementieren oder auch nicht. Durch eine mangelhafte Implementation erwachsen oft Bedrohungen, die VoIP zu einem Risikofaktor werden lassen.

Um eine ausreichende Sicherheit gewährleisten zu können, müssen die im Standard genannten Sicherheitsmechanismen (S/MIME, Digest Authentifikation, usw) zwingend implementiert sein. Zudem muss bei der Architektur des Netzwerks auf die Eigenschaften von SIP Rücksicht genommen werden. Dies kann beispielsweise mit einem Application-Layer Firewall gemacht werden, welcher SIP Nutzdaten analysieren kann. Nur so kann Angriffen vorgebeugt werden.

### 7.2.2 H.323

#### Übersicht

H.323 ist eine Empfehlung der ITU(International Telecommunication Union). Die Ausarbeitung des Standards geschah durch die ITU-T, des Gremiums der ITU welches den grössten Teil aller Empfehlungen der ITU erarbeitet [30]. Das Ziel gemäss [25] ist, dass verschiedene Instanzen untereinander real-time Audio übertragen können. Es soll also ein Gespräch zweier Gesprächspartner möglich sein, aber ebenfalls eine Telefon-Konferenzschaltung mehrerer Teilnehmer. Video und Datenkommunikation sind ebenfalls vorgesehen, aber als optional deklariert. Die durch H.323 ermöglichten Kommunikationsmittel bieten keinen QoS(Quality of Service).

Die erste Version der Spezifikation entstand 1996. Seit damals gab es regelmässige Updates der ITU-T Empfehlung. Seit Beginn 2006 ist die Version 6.0 aktuell, welche die seit 2003 bestehende Version 5.0 ablöste.

Die H.323 Empfehlung [25] legt folgendes fest:

- Beschreibung der Architektur mit dessen Komponenten.
- Das Management der Verbindungen und des Austausches.
- Das Interworking zwischen verschiedenen Netzen, d.h. die netzübergreifende Kommunikation zwischen IP und den Netzen der Telefonieanbieter wie ISDN oder der Vorgänger QSIG.

H.323 ist als Umbrella-Spezifikation[29] definiert, d.h. dass H.323 bereits alle nötigen protokolltechnischen Bestandteile zur Audio Kommunikation mitbringt. Die Umbrella-Spezifikation baut auf verschiedenen H.x Protokollen auf, welche bereits ebenfalls durch

die ITU-T spezifiziert wurden. Die in H.323 vorgesehene Kommunikation verschiedener Endpunkte kann über eine Punkt-zu-Punkt Verbindung, über ein Netz(innerhalb IP) oder per Interworking über verschiedene Netze verwendet werden. Nach [30] basiert H.323 auf dem ISDN-Protokoll Q.931. Darum kann H.323 gut für Interworking verwendet werden. Interworkingszenarien sind denkbar zwischen IP(Internet mit TCP/IP) und ISDN(z.B. Telefonieanbieter Vermittlungsstellen), bzw. zwischen IP und QSIG(auf ISDN basierendes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen[33]).

### Hauptelemente

Der H.323 Standard definiert die, für den real-time Austausch benötigten Hauptelemente. Die nachfolgende Abbildung veranschaulicht diese Elemente und vor allem den Fokus von H.323, welcher sich auf paketbasierte Netze beschränkt, aber durch den Gateway mit anderen leistungsvermittelnden Netzen verbunden und kompatibel ist:

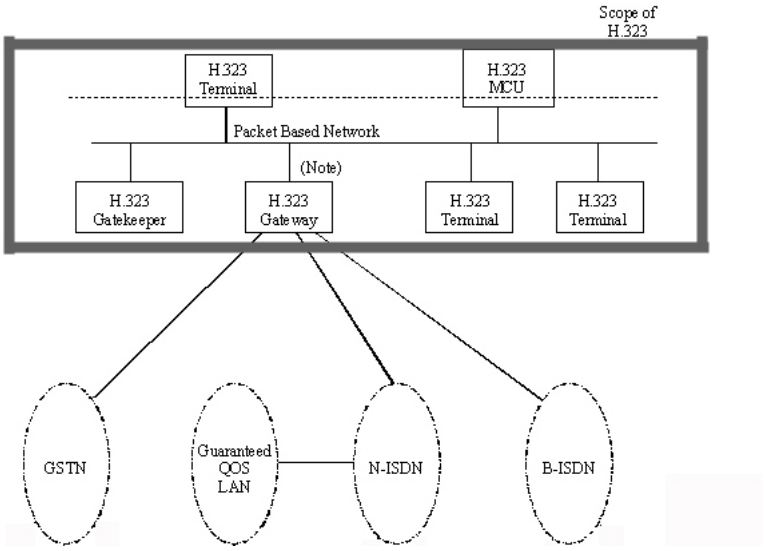



Abbildung 7.6: H.323 Hauptelemente [25]

Die wichtigsten Komponenten der H.323 Spezifikation sind [25]:

- Terminal: Ein H.323 Terminal ist ein Endpunkt des Netzwerkes welcher Echtzeit-, 2-Weg-Kommunikation mit anderen H.323 Terminals, Gateways oder MCUs (Multipoint Control Units) betreibt. Ein solcher Endpunkt kann Nur-Sprache, Sprache und Daten, Sprache und Video oder alle drei Kommunikationsmittel kombiniert zur Verfügung stellen. Ein Terminal ist somit Beispielweise das Gerät mittels welchem Alice per IP mit Bob, welcher einen herkömmlichen Telefonfestnetzanschluss(mit ISDN Vermittlungsstelle dazwischen) besitzt, sprechen will.
- Gateway: Ein H.323 Gateway ist ein Endpunkt des Netzwerks welcher Echtzeit-, 2-Weg-Kommunikation zwischen H.323 Terminals in einem paketorientierten Netzwerk und anderen ITU Terminals auf einem leitungsvermittelten Netzwerk (switched circuit network) oder zu anderen H.323 Gateways ermöglicht. Er ist somit

die Schnittstelle zwischen verschiedenen Netzen. Der Gateway fungiert als Übersetzer, d.h. er übersetzt sowohl die Nutzdaten mit beispielsweise den netzspezifischen Codecs, als auch die Signalisierungsdaten in beide Richtungen.

- Gatekeeper: Der Gatekeeper ist eine wichtige H.323 Instanz im Netzwerk welche Adressierung, Zugangskontrolle und Registrierung im Netzwerk für H.323 Terminals, Gateways und MCUs übernimmt. Optional kann der Gatekeeper auch für Terminals, Gateways und MCUs das Management der Bandbreiten oder die Lokalisierung der Gateways übernehmen. Durch das Übernehmen von Signalisierungsfunktionen entlastet der Gatekeeper die Terminals. Der Gatekeeper ist jedoch in der Spezifikation nicht zwingend vorgeschrieben. Seine Funktionalität kann auch von den Terminals übernommen werden.

- MCU (Multipoint Controll Unit): Die MCU ist eine H.323 Instanz im Netzwerk welche die Kontrolle von drei oder mehr teilnehmenden Terminals in einer Mehrpunkt-Konferenz bereitstellt. Die MCU besteht aus einem MC(Multipoint Controller) und einem MP(Multipoint Processor), welcher nicht zwingend vorgeschrieben ist. Aufgabe des MC ist es einerseits die Terminal-Eigenschaften auszuhandeln, welche von allen Terminals eingehalten werden können und andererseits die Konferenzsteuerung zu übernehmen. Der MP kommt ebenfalls dann zum Tragen, wenn Sprache, Video oder Daten gemixt oder bearbeitet werden müssen. Die MCU kann auch zwei Terminals miteinander in einer Punkt-zu-Punkt Konferenz verbinden, welche dann später ebenfalls durch den MC in eine Mehrpunkt-Konferenz mit zusätzlichen Terminals umgewandelt wird.

**Funktionalität**

Die im vorherigen Kapitel definierten Komponenten kommunizieren in IP Netzen mittels IP Paketen [25]. Diese IP Pakete werden mittels folgender Kriterien klassifiziert: Video, Audio, Daten, Kommunikationsprotokoll, Signalisierung. H.323 legt nun die Art und Weise der Informationsströme in diversen Sub-Spezifikationen fest:

- H.225 (Signalisierung) [32]: H.225 ist ein Subprotokoll des H.323 Standards. Es übernimmt die Rufsignalisierung, d.h. den Aufbau, die Kontrolle und die Beendigung einer H.323 Kommunikation. Diese Kommunikation kann nun zwischen Gatekeeper und Terminal oder direkt zwischen den beteiligten Terminals stattfinden. Die Kontrolle einer H.323 Kommunikation beinhaltet beispielsweise die Registrierung der Terminals beim Gatekeeper oder allfällige Bandbreitenanpassungen oder der Austausch von Statusmeldungen. Die Kodierung der H.225 Nachrichten wird in Q.931 definiert. Dieses Rahmenformat findet ebenfalls bei der Signalisierung von ISDN(Integrated Services Digital Network) Anwendung. Wichtige Q.931 Mitteilungen sind Setup, Call Proceeding, Alerting, Connect, Release Complete und Facility.

- H.245 (Kontrolle Multimedia Kommunikation) [31]: H.245 ist das Kontrollprotokoll für die Multimedia Kommunikation. Jedes Terminal hat mittels H.245 die Möglichkeit seine Kommunikationsfähigkeiten den anderen Terminals mitzuteilen. Hat eine Partei beispielsweise keine Webcam, so kommuniziert sie dies mittels H.245. Dafür

kontrolliert das Protokoll die Verhandlung und legt dann fest wie die verschiedenen Terminals miteinander kommunizieren, d.h. welches Kommunikationsmittel und welcher Codec verwendet wird oder an welche Ports der UDP-Datenstrom weitergereicht wird.

- H.324 (Übertragung mit niedrigen Bandbreiten) [28]: Dieser Standard wurde ins Leben gerufen, damit bei niedrigen Bandbreiten eine Echtzeit-Kommunikation möglich ist.

- G.7xx (Audio Codecs) und H.26x (Video Codecs) [28]: H.323 definiert verschiedene Audio- und Videocodec Standards. Diese dienen dazu, dass die real-time Daten in komprimierter Form schnell und effizient übermittelt werden können und dann vom Empfänger problemlos dekomprimiert werden können. Für die Komprimierung der Sprache hat die ITU-T deshalb verschiedene Codec Spezifikationen für Video und Sprache in H.323 eingebaut. Dies ist die G.7xx Serie für die Übertragung von Sprache und die H.26x Serie zur Videokomprimierung.

- T.4 (Telefax) [28]: In H.323 ebenfalls vorgesehen ist die Übermittlung von Fax. Dies wird in den Standards T.4, T.30, T.37 und T.38 definiert. Hier sind beispielsweise der Faxversand in Echtzeit, per Store-and-Forward gesicherte Übertragung oder der traditionelle Faxversand über öffentliche Netze geregelt.

**H.323-Verbindungsaufbau** Die Spezifikation von H.323 [25] definiert verschiedene mögliche Szenarien für den Aufbau einer Verbindung. Entscheidend ist vor allem die Frage, wie viele Terminals und Gatekeepers bei einem Verbindungsaufbau involviert werden müssen. Ebenfalls denkbar ist der Fall, dass ein Terminal nur einen anderen Terminal anrufen möchte, wobei aber auch hier entscheidend ist, ob beide bei demselben Gatekeeper registriert sind.

Das in der nachfolgenden Abbildung gezeigte Szenario mit ensprechenden Erläuterungen zeigt die nötigen Schritte für den Aufbau einer Verbindung. Beteiligt sind nur zwei Terminals, welche beide bei demselben Gatekeeper registriert sind. Eine weitere Annahme ist die Entscheidung des Gatekeepers, das Routing der Call Signalling Nachrichten den Terminals zu überlassen.

Das Subprotokoll H.225 kommt nun hier in (1), (2), (3), (4), (5), (6), (7) und (8) zur Anwendung. Ab (8), wo der Datenstrom beginnen kann, ist das Kontrollprotokoll H.245 zuständig, welches den Multimedia Datenstrom kontrolliert.

Als erstes initiiert Endpunkt 1 den Austausch der ARQ(Admission Request message)/ ACF(Admission Confirm message) mit dem Gatekeeper bei welchem er registriert ist. Im ARQ werden Informationen zum gewünschten Kommunikationspartner verpackt, aber auch Informationen der zur Verfügung stehenden Bandbreite. Der Gatekeeper antwortet nun mit dem ACF. Der ACF beinhaltet die Information welche Call Signalling Channel Transport Adresse Endpunkt 2 besitzt.

Nun sendet Endpunkt 1, der nun weiss, wo sich Endpunkt 2 befindet, die Setup Nachricht. Diese wird mittels einer H323-URL(Unified Ressource Locator) durch das Netzwerk

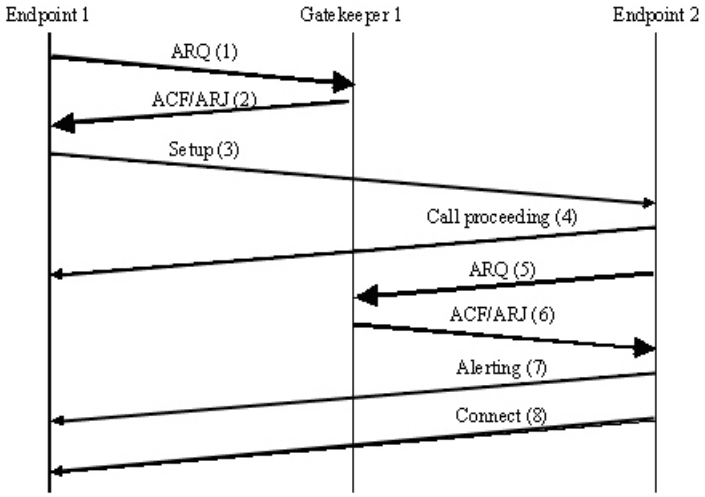



Abbildung 7.7: H.323-Verbindungsaufbau [25]

gerouted. Konkret sieht diese URL folgendermassen aus: „h323: user @ hostport [ url-parameters ]“. Wenn Endpunkt 2 die Anfrage empfängt, initiiert dieser nun ebenfalls ein Austausch des ARQ/ACF mit dem Gatekeeper bei welchem er registriert ist.

Nun wird zu dem Zeitpunkt, wo der Benutzer des Endpunktes 2 über die Anfrage informiert wird, eine Alert Nachricht an Endpunkt 1 geschickt. Diese wäre bei einer einfachen Telefonanwendung das Läuten des Telefons beim Angerufenen, welches beim Anrufenden ein Rufzeichen generiert. Dieser weiss dann, dass der Anruf aufgebaut werden kann. Nimmt Endpunkt 2 den Anruf an, wird eine Connect Nachricht mit der H.245 Control Channel Transport Adresse an den Endpunkt 1 verschickt.

Wenn die Verbindung zwischen den zwei Endpunkten steht, werden die Sprach- und Videodaten direkt übertragen. Diese werden bei H.323 immer über UDP übertragen. Die Rufkontrollinformationen, Signalisierungsnachrichten oder Daten werden gemäss H.323 Standard [25] über TCP übertragen. Zwischen der Applikationsschicht und der Transportschicht befindet sich aber gemäss [25] noch eine zusätzliche Schicht für die Übertragung von Video und Sprache: RTP(Real-Time Transport Protocol). Dieses Protokoll wurde von der IETF ursprünglich definiert und von der ITU-T in H.323 übernommen. Das RTP kennzeichnet bei dem Sender die real-time Daten und fügt einen Zeitstempel sowie eine Sequenznummer an [34]. Dies ermöglicht es dem empfangenden Terminal zu spät ankommende Pakete als solche zu erkennen und zu verwerfen. Ohne RTP wäre eine Übertragung via UDP von Sprache in Echtzeit undenkbar, da die UDP Pakete nicht wie bei TCP geordnet beim Empfänger ankommen. RTP ergänzt die Pakete um Sequenznummern. Mit dieser Zusatzinformation kann der Empfänger die Pakete wieder in die richtige Reihenfolge bringen und nicht aktuelle zu spät angekommene Pakete, als solche erkennen und verwerfen.

**Sicherheitsaspekte**

Das Thema Sicherheit ist in der Unterspezifikation H.235 spezifiziert [26]. Der Fokus der ITU-T liegt auf Authentifizierung und Datenschutz durch Verschlüsselung. Die anderen Sicherheitskriterien werden nur am Rande erwähnt und dadurch eine konkrete Implementation den Entwicklern überlassen.

Laut Spezifikation [25] können H.323 Instanzen auf paketbasierten Netzwerken kein QoS garantieren. Aus diesem Grund kann der real-time Datenstrom weder dem Kriterium der Verbindlichkeit, noch der Verfügbarkeit genügen. Bei der Authentifizierung wird der Advanced Encryption Algorithm (AES) in H.235 vorgeschlagen. Vertraulichkeit und Integrität des Informationsstroms wird durch eine End-Zu-End-Verschlüsselung garantiert. Anwendung finden hier verschiedene Verschlüsselungsalgorithmen mit den unterschiedlichsten Schlüssellängen. Authentifizierung geschieht durch einen Diffie-Hellman- Schlüsselaustausch. Nicht geregelt in H.323 und offen gelassen ist die Anonymität.

Der beste Angriffspunkt für Hacker-Angriffe ist der Gatekeeper. Dieser stellt bei H.323 ein enormes Sicherheitsproblem dar. Ein potentieller Hacker kann, wenn er den Gatekeeper kontrolliert, den ganzen real-time Datenstrom mitschneiden. Falls der Datenstrom jedoch verschlüsselt ist, wird die Analyse des Inhalts durch den Angreifer enorm erschwert, da die Pakete erst am Ziel und nicht beim Gatekeeper wieder entschlüsselt werden. In gewissen Fällen genügt es dem Angreifer jedoch schon, wenn er weiss, wer mit wem kommuniziert. Ein zusätzliches Angriffszenario ist die Vortäuschung einer falschen Identität beim Gatekeeper. Dies Form des Angriffs wird in [27] genau beschrieben.

Grundsätzlich lässt sich jedoch sagen, dass die ITU-T sehr intensiv an der Verbesserung ihrer Sicherheitsspezifikation H.235 gearbeitet hat. Die Spezifikation ist heute in der Version 3.0 sehr umfangreich.

### 7.2.3 IAX2

**Übersicht**

Das IAX Protokoll (Inter-Asterisk EXchange) ist kein offiziell verabschiedeter IETF Standard und wurde von Marc Spencer und Frank Miller spezifiziert. Das Protokoll nicht als RFC, sondern erst als Internet-Draft vor [37]. IAX wurde erst nach der Veröffentlichung der Standards SIP und H323 entwickelt. Das Ziel dabei war, die OpenSource-Telefonanlage Asterisk effizient miteinander zu verbinden, was somit auch das Haupteinsatzgebiet von IAX ist. Für die Verbindung wollten die Entwickler nicht auf bestehende Protokolle zurückgreifen, da diese mit gewissen Problemen behaftet waren. Im März 2004 wurde IAX in der Version 1 vorgestellt [39], im Januar 2005 wurde dann die Version 2 von IAX (IAX2) publiziert, auf die sich diese Arbeit bezieht [37]. Der neueste Draft des Standards der IAX Spezifikations ist zu finden unter [38].

Das IAX Protokoll ermöglicht das Management und die Übertragung von beliebigen Streamingdaten über ein IP-Netzwerk, der Fokus liegt aber bei der Übertragung von Sprachdaten (VoIP). Das Ziel der Entwicklung war einerseits die benötigte Bandbreite für VoIP so

klein als möglich zu halten und andererseits das NAT-Problem (Network Address Translation) zu lösen. Das NAT-Problem bei SIP besteht darin, dass im SIP-Protokollheader IP-Adressen eingetragen werden. Ein einfache NAT-Übersetzung verunmöglicht jedoch das direkte Adressieren. Es müsste eine Übersetzung im SIP-Protokollheader stattfinden, was jedoch bei einem normalen NAT-Router nicht implementiert. Beim Versucht, diese Probleme zu lösen ist ein Protokoll entstanden, dass eine Point-to-Point Architektur aufweist und sowohl für das Management, als auch für die Datenübertragung zuständig ist. Somit besteht IAX eigentlich aus zwei Protokollen. Für beide Aufgaben wird UDP (User Datagram Protocol) über den bei der IANA angemeldeten Port 4569 verwendet [40]. Dadurch kann IAX auch eingesetzt werden, wenn sich die Benutzer hinter NAT-Routern befinden. Damit mehrere Gespräche über denselben UDP Port möglich sind, benutzt IAX eine 15-Bit Call Number. Diese Nummer ist nicht mit einer Telefonnummer zu verwechseln, sie kennzeichnet nur die verschiedenen Gespräche, die über denselben Port geführt werden. Um das Protokoll so effizient wie möglich zu gestalten, wurde es als binäres Format definiert.

Im folgenden Kapitel werden zuerst die Hauptbestandteile von IAX erklärt. Danach wird auf die Protokollfunktionalität eingegangen und es werden IAX Version 1 und IAX Version 2 miteinander verglichen. Zum Schluss werden die Sicherheitsaspekte von IAX betrachtet.

### Hauptelemente

Eine spezielle Hardwareinfrastruktur ist nicht notwendig, es gibt jedoch auch Hardwareimplementationen von IAX wie z.B. Snom 100 [41]. Als Vertreter der IAX-Unterstützenden Software ist sicherlich die Telefonanlage Asterisk zu nennen, die der Ursprung für die Entwicklung von IAX war. Wird eine solche Telefonanlage verwendet, melden sich die IAX-Clients (Hosts) bei der Telefonanlage an, um Verbindungen aufbauen zu können [42].

### Funktionalität

Die Kommunikation mittels IAX wird mit Hilfe von Frames (Nachrichten) abgewickelt. Es können zwei grundsätzliche Typen unterschieden werden: Full Frames und Mini Frames. Des Weiteren gibt es in den einzelnen Frames noch Felder, wo Informationen über den Inhalt der Frames gespeichert werden können, so dass eigentliche Untergruppen von Frames entstehen. Die drei erwähnten Oberarten werden in den folgenden Kapiteln genauer betrachtet, die einzelnen Untergruppen werden nur am Rande erwähnt.

**Full Frame** Die Übertragung dieser Frames muss vom Empfänger bestätigt werden. Welche Art der Bestätigung erwartet wird, ist vom Inhalt des Full Frames abhängig. Da alle Full Frames auf irgendeine Weise bestätigt werden müssen, werden vor allem Kontroll- und Synchronisationsinformationen mittels Full Frames ausgetauscht. Es können jedoch auch andere Datentypen wie Audio oder Videodaten versendet werden, dies jedoch auf Kosten der Effizienz.

Der Aufbau der Full Frames ist in Abbildung 7.8 ersichtlich. Dabei haben die einzelnen


Abbildung 7.8: Full Frame [41]

Felder folgende Bedeutung:

- F: 0 oder 1, in Abhängigkeit, ob das Frame ein Full Frame ist (1) oder nicht (0).
- callnr: 15-Bit Call Number welche die Gespräche auf der Seite eines Hosts eindeutig kennzeichnet.
- R: 0 oder 1 in Abhängigkeit, ob das Frame nach einer gewissen Zeit neu übertragen werden soll (Retransmission).
- dcallnr: 15-Bit Call Number welche die Gespräche auf der Seite eines Hosts eindeutig kennzeichnet.
- ts: Zeitstempel für das Frame.
- seqnr: Sequenznummern für die Pakete.
- type: Typ des Frames. Hiermit können spezielle Unterklassen der Frames gebildet werden. Anhand von diesen Angaben werden die Daten in Data interpretiert. Spezielle FrameTypes sind Control oder IAX Control Frames. Diese werden zur Steuerung benutzt und können nur als Full Frame eingesetzt werden.
  - Control: Notwendig für das Session Management. Diese Informationen sind abhängig vom entsprechenden Host.
  - IAX Control: Austausch von IAX spezifischen Informationen, die nicht Hostabhängig sind, wie Beispielsweise die ACK-Nachrichten.
- c: Interpretationsart der Unterklassen
- sub: Zusatzinformationen zu den Daten im Feld Nutzlast. Hier können beispielsweise die Kompressionsformate der Daten definiert werden.
- Nutzlast: Daten des Frames

**Mini Frame** Diese Frames werden im Gegensatz zu den Full Frames nicht bestätigt. Sie eignen sich für den Transport von Daten, da sie nur sehr wenige Informationen in ihrem Header haben. Alle nötigen Informationen über den Inhalt der Mini Frames werden mittels der Full Frames und deren Subklassen übermittelt. Aufgebaut sind die Mini Frames wie folgt:

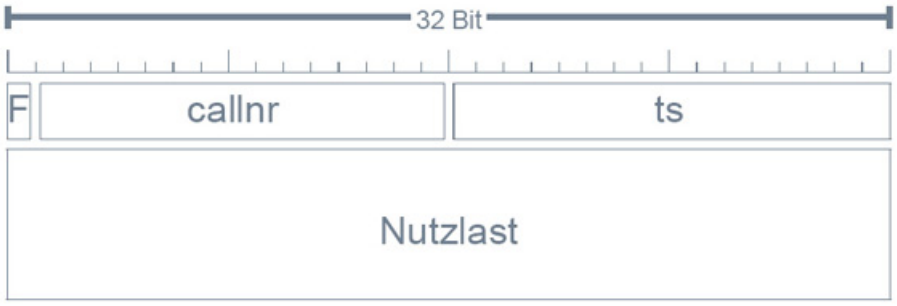



Abbildung 7.9: Mini Frame [41]

- F: Full Frame Information. Ist bei Mini Frame auf 0 gesetzt.
- Source Call Number: 15-Bit Call Number, welche die Gespräche auf der Seite eines Hosts eindeutig kennzeichnet.
- Timestamp: Zeitstempel für das Frame.
- Nutzlast: Daten des Frames

**Round-Trip Delay und Heartbeat** IAX berechnet für die Full Frames eine geschätzte Round-Trip Zeit, die ERTD (Estimated Round-Trip Delay). Als Grundlage dafür dienen die Timestamps in den Full Frames. Diese Berechnung erfolg jedesmal, wenn ein Full Frame gesendet und die entsprechende Bestätigung erhalten wurde. Anhand von der so ermittelten Zeit kann überprüft werden, ob ein Full Frame verloren gegangen ist. Sollte ein Full Frame nicht in der ERTD bestätigt werden, wird das Frame neu gesendet und die ERTD wird erhöht, bis entweder eine Bestätigung eintrifft oder das Maximum der Versuche erreicht ist. Dieses Maximum ist abhängig von der Anzahl der Sendeversuche (10 Mal) oder von einer maximalen Zeit (60 Sekunden).

Um zu überprüfen, ob ein Host noch erreichbar ist oder nicht, kann die sogenannte Heartbeat Funktion verwendet werden. Dazu werden zwei Fälle unterschieden:

- Besteht eine Verbindung zwischen zwei Hosts, so wird nach 15 Sekunden ohne ein Full Frame eine PING Nachricht ausgelöst. Da diese selbst ein Full Frame ist, muss sie bestätigt werden. Wird sie nicht innerhalb der ERTD bestätigt, wird sie so lange neu versendet, bis die oben genannten Maximalwerte erreicht worden sind. Kommt keine Bestätigung an, wird die Verbindung getrennt.

- Besteht keine Verbindung, kann ein Host einen anderen Host prüfen, ob der andere Host antwortet. Dazu wird eine POKE Nachricht gesendet, die ebenfalls ein Full Frame ist. Auch diese Nachricht wird so lange gesendet, bis das definierte Maximum erreicht ist. Danach wird angenommen, dass der gewünschte Host zur Zeit nicht verfügbar ist.

#### Unterschied zu IAX1

In den vergangenen Jahren hat sich der IAX-Standard stark verändert und wurde immer umfangreicher. Da das ursprüngliche Ziel von IAX die Verbindung von Telefonanlagen war, wurden Teile wie die Registrierung, Authentifizierung oder das Rufnummernmanagement nicht in den ersten Standard von IAX gepackt. Im neuesten Standard [38] werden nun auch solche Aufgaben als ein Bestandteil des IAX-Protokolls definiert. Zudem wurde im Wechsel von IAX Version 1 zu Version 2 auch der Port geändert, von 5036 auf Port 4569 [39].

#### Sicherheitsaspekte

Ein Nachteil von IAX ist, dass die Nutzdaten der IAX-Frames ursprünglich nicht verschlüsselt werden konnten [41]. Erst seid dem Draft Anfang März 2006 [38] ist auch eine Verschlüsselung möglich. Ohne diese Verschlüsselung wäre es möglich, dass unbefugte Personen Gespräche mithören oder deren Inhalt verändern. Bei der Authentifizierung können neben dem offensichtlich unsicheren plaintext Verfahren auch ein Verfahren mit md5 und RSA zur Anwendung kommen. Die Authentifizierung ist nicht im IAX Standard definiert, sondern speziell in Zusammenarbeit mit Asterisk-Servern definiert. Da im betrachteten Standard [37] das gesammte User- und Rufnummernmanagement nicht spezifiziert war, kann zu den Punkten Authentizität und Verbindlichkeit keine Aussage getroffen werden. Ein Angriff auf die Verfügbarkeit (Denial of Service, DoS) ist nicht ausgeschlossen und wird im neuesten Standard [38] sogar ausdrücklich erwähnt. Ein solcher Angriff könnte durch Full Frames erreicht werden, mit denen der IAX Client bombardiert wird.

### 7.2.4 Skype

#### Übersicht

Skype ist eine Peer-to-Peer Software, die es Benutzern ermöglicht, VoIP mit dem proprietären Skype-Protokoll zu benutzen. Die Software kann kostenlos bezogen werden, Gebühren werden nur für spezielle Dienstleistungen verlangt, wie das Skype-Out (Anrufe von Skype ins normale Telefonnetz). Über das Protokoll sind fast keine Informationen zu finden, da es sich um ein kommerziell genutztes Produkt handelt, dass Closed-Source ist. Nur die Programmierer von Skype wissen, wie das Protokoll im Detail aussieht, für alle anderen ist Skype eine BlackBox. Es wurden schon Versuche unternommen, die Skype-Software zu knacken oder zumindest den Netzverkehr transparent darzustellen, jedoch

besitzt Skype eine ausgefeilte Verschleierungstechnik, welche es fast unmöglich macht, den internen Mechanismus zu verstehen [46] [47].

### Hauptelemente

Das Skype-Netzwerk besteht aus den Komponenten Skype Login Server, Super Nodes und Hosts. Beim Aufstarten der Software versucht diese, sich beim Skype Login Server anzumelden. Dazu werden Benutzername und Passwort mit den gespeicherten Daten verglichen. Der Login Server ist kein eigentlicher Skype-Konten im Netzwerk, er ist lediglich für die Authentifizierung notwendig. Er garantiert, dass es jeden User genau einmal im gesamten Netz gibt. Die Skype Login Server sind zentral organisiert. Wurde der User akzeptiert, meldet sich der Host bei einem Supernode an. Supernodes sind eigentlich normale Hosts, die jedoch über einen schnellen CPU, viel Speicher, eine öffentliche IP und eine grosse Bandbreite verfügen. Das Skype Netzwerk ist in Abbildung 7.10 abgebildet.

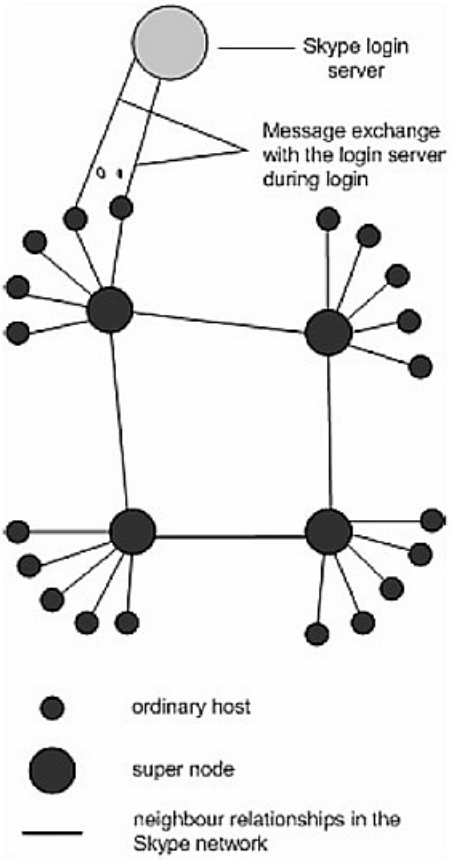



Abbildung 7.10: Skype Network

### Funktionalität

Da die Skype Software sehr gut geschützt ist, können nur Vermutungen über die Funktionalität des Skype-Protokolls angestellt werden. Die hier präsentierten Informationen stammen aus den Testreihen von [46] und [47].

- Bandbreite: Skype verwendet Codecs um die zu übertragende Datenmenge so klein als möglich zu halten. Damit kann Skype bereits ab einer Bandbreite von 32 kb/s eingesetzt werden. Verlässliche Informationen welche Codecs dazu verwendet werden, gibt es jedoch nicht.

- Ports: Skype benutzt einen bei der Installation definierten Port, kann aber auch über die Ports 80 (HTTP) und 443 (HTTPS) betrieben werden. Die Kommunikation kann über TCP oder UDP erfolgen, jedoch funktioniert Skype ohne TCP nicht. Auf UDP kann Skype verzichten. Normalerweise werden das Sessions-Management und der Datenaustausch über unterschiedliche Ports gemacht.

- Verschlüsselung: Der Datentransfer von Skype ist laut Aussage von [48] durch einen 256-Bit Schlüssel geschützt. Für den Schlüsseltausch werden 1536- bis 2048-Bit-RSA-Schlüssel verwendet.

- Authentifizierung: Die Authentifizierung der Teilnehmer erfolgt über ein challenge-response Verfahren mit dem von Skype zertifizierten Schlüsselpaar. Ist das Verfahren erfolgreich, wird ein symmetrischer Schlüssel ausgehandelt, mit dem dann der Datentransfer verschlüsselt wird.

- NAT und Firewall: Stellen für Skype keine Probleme dar. Es wird spekuliert, dass eine Variante des STUN [51] und TURN [52] Protokolls verwendet wird.

- Profildaten: Da die Profildaten auf den Super Nodes verteilt sind, müssen sie vor willkürlichen Veränderungen geschützt werden. Daher sind die gespeicherten Profildaten digital signiert. Dadurch soll eine unautorisierte Veränderung verhindert werden [48].

### Sicherheit

Ein Punkt bezüglich Sicherheit ist die Glaubwürdigkeit der Software an sich. Skype schreibt auf seiner FAQ Seite, dass keine Malware, Spyware oder Backdoors im Code eingebaut sind [48]. Zudem wird dort vermerkt, dass für den Datentransfer und für den Schlüsseltausch das AES- respektive das RSA-Verfahren eingesetzt würden. Ob diese Aussagen auch der Wahrheit entsprechen, konnte bis zum heutigen Zeitpunkt nicht validiert werden. Die Sicherheitsexperten in [46] kommen jedoch zum Schluss, dass beinahe der gesammte Datenverkehr verschlüsselt ist. Die Datenintegrität sollte somit gewährleistet sein. Es ist jedoch nicht ausgeschlossen, dass von einer solchen Software Gefahr ausgeht, wie das Beispiel [53] zeigt. Dabei wird beschrieben, wie ein ungwollter Dateitransfer provoziert werden kann. Den Programmierern ist es gelungen, einen Fehler im Programmcode aufzuspüren und auszunützen.

Zudem wurde in [47] ein Weg aufgezeigt, wie man ein eigenes Skype-Netzwerk erstellen könnte und so die Kontrolle über die einzelnen Knoten hätte. Dadurch könnten Schlüssel abgefangen werden und somit wären die Gespräche (theoretisch) abhörbar. Ein weiteres Problem stellt die Mehrfachbenutzung dar. Skype kann auf mehreren Maschinen gleichzeitig mit demselben User betrieben werden. Alle Chatnachrichten werden zu allen Instanzen

übertragen. Wenn es einem Hacker gelingt, Username und Passwort zu erraten, kann er alle Chatnachrichten mitlesen. Dazu muss der Hacker sich nur als „unsichtbar“ anmelden.

Ein Denial-of-Service Angriff kann auf Grund der Architektur und des Programms nicht ausgeschlossen werden. Das Herzstück von Skype sind die Skype Login Server. Fallen diese Server aus, kann sich kein User mehr am Netzwerk anmelden.

Skype besitzt keinen Mechanismus, um die Identität eines Users zu überprüfen. Ob der eingegebene Name, die Adresse usw. der Wirklichkeit entsprechen, ist somit nicht evaluierbar. Es kann also sein, dass es sich beim Gesprächspartner nicht um die gewünschte Person handelt. Dies kann v.a. für Firmen Konsequenzen haben, wenn sie Skype einsetzen. Zudem kann der Datenverkehr von Skype nicht überwacht werden, was ein Problem bezüglich Sicherheitspolicen darstellen kann.

## 7.3 Vergleich

In diesem Kapitel werden die vorgestellten Protokolle miteinander verglichen. Nach einem generellen Überblick über die Protokolle werden die Protokollstruktur, der Zentralisierungsgrad, die Effizienz, die Anwendungen sowie die NAT- und Firewallproblematik thematisiert.

### 7.3.1 Übersicht

Bei den Vergleichen muss immer bedacht werden, dass der Funktionsumfang der vier VoIP Protokolle stark divergiert. SIP ist nur für Sessions zuständig. H.323 bringt als Umbrellaspezifikation bereits alle nötigen Bestandteile für eine real-time Multimedia Kommunikation mit. IAX2 stellt eine Spezifikation für Transport und Session dar. Skype ist proprietär und hat bereits alle nötigen Funktionalitäten implementiert.

Die Protokolle SIP und IAX werden in Zusammenarbeit mit der IETF spezifiziert und sind somit öffentlich zugänglich. Ebenso kann der Standard H.323 direkt bei der standardisierenden Instanz, der ITU-T, bezogen werden. Entwickler können so die spezifizierten Protokolle in ihre Programme umsetzen und sind unabhängig von anderen Parteien. Zudem ermöglichen diese Standards eine Interoperabilität mit Systemen, die von anderen Entwicklern hergestellt wurden. Dadurch, dass die Standards öffentlich zugänglich sind, können auch Gateways erstellt werden, die z.T. ein SIP-Netzwerk mit einem H.323 Netzwerk verbinden. Skype ist im Gegensatz dazu proprietär und kann nicht eingesehen werden. Daher lassen sich nur Vermutungen über die wirkliche Funktionalität von Skype anstellen. Des Weiteren ist es nicht möglich, SIP mit Skype zu verbinden [49]. Für Skype existiert lediglich eine API mit der sich Skype in andere Programme einfügen lässt [50].

### 7.3.2 Protokollstruktur

Das SIP Protokoll ist textbasiert und ähnelt dem HTTP Protokoll. Der Aufgabenbereich von SIP beschränkt sich lediglich auf das Sessionsmanagement. Der Transport der VoIP-Daten muss von anderen Protokollen, wie z.B. RTP (Real-Time Transport Protocol) übernommen werden. Dadurch erreicht SIP eine hohe Flexibilität, da kein spezielles Protokoll vorgeschrieben ist. Ändernde Anforderungen können durch das Hinzfügen von weiteren Schichten, wie z.B. einer Verschlüsselungsschicht, schnell abgedeckt werden.

H.323 ist ein nicht textbasiertes, sondern binäres Protokoll. H.323 hat durch das Wesen einer Umbrella-Spezifikation einen modularen Aufbau und bietet alle Subspezifikationen für VoIP über IP Netze. Es existieren diverse Substandards der H.x Reihe wie beispielsweise H.225 oder H.245. Diese wurden allerdings allesamt von der ITU-T spezifiziert (Ausnahme: RTP-Protokoll der IETF). Sollen neue Funktionen in das Protokoll eingearbeitet werden, muss die Spezifikation diese liefern.

IAX ist nicht textbasiert, sondern ein binäres Protokoll. Daraus ergibt sich das Problem, dass die Daten nur mit einem entsprechenden Client gelesen werden können. Bei einem textbasierten Format, wie SIP ist dies nicht notwendig. Ausgerichtet ist IAX vor allem auf den effizienten Transfer von Daten für VoIP Anwendungen. Im neuesten Standard ist auch das Usermanagement zu finden [38]. Dadurch, dass das Protokoll mehrere Funktionen in einem einzigen Protokoll vereint, ist der Aufbau nicht modular wie bei SIP oder H.323. Änderungen können nicht einfach durch den Austausch einer Schicht erreicht werden, was die Flexibilität dieses Protokolls einschränkt.

Über Skype können keine Aussagen bezüglich der Protokollstruktur gemacht werden, da diese nicht zugänglich ist. Die Flexibilität dieses Protokolls hängt von der entwickelnden Firma Skype ab.

### 7.3.3 Zentralisierungsgrad

SIP hat eine relativ dezentrale Organisation. Beim Aufbau der Session werden die Requests über die Proxy Server weitergeleitet. Bei der Weiterleitung der Requests werden Routingentscheidungen getroffen, bei der sie möglicherweise über mehrere Proxy Server gehen müssen bis der Zielempfänger gefunden wird. Die Suche nach der Zieladresse geschieht somit auf dezentrale Weise.

VoIP mittels H.323 kann völlig dezentral betrieben werden. Im einfachsten Fall gibt es nur zwei Terminals die alle Aufgaben, welche zur real-time Sprachübermittlung nötig sind, alleine übernehmen können. Falls aber ein Endpunkt aus dem paketbasierten Netz auf das herkömmliche ISDN-Netz telefonieren möchte, ist ein Gateway notwendig, der die Pakete und Signalisierungsinformationen zwischen den verschiedenen Netzen übersetzt. Zusätzlich sind in H.323 auch Gatekeepers, die die Endpunkte entlasten sollen und MCUs, welche Konferenzen ermöglichen, vorgesehen. Gemäss [27] ist jedoch der Gatekeeper die wichtigste Instanz, weshalb H.323 als eher zentrale Organisation bezeichnet werden kann. Möglich ist aber auch, dass diverse Gatekeeper im paketbasierten Netzwerk verwendet werden. Dies würde eher wieder eine dezentrale Organisation darstellen.

Der betrachtete Standard IAX2 macht keine Aussagen zum Zentralisierungsgrad. Allerdings verbindet IAX Asterisk-Server untereinander. Es kann daher angenommen werden, dass IAX komplett dezentral aufgebaut werden kann. Dies z.B. als komplette Peer-to-Peer Architektur.

Bei Skype werden die Kommunikation zwischen den Usern und das Usermanagement dezentral gelöst (Super Nodes und Client-Network). Der Datentransfer läuft entweder direkt von Host zu Host oder wird über Super Nodes umgeleitet. Das Anmelden ist nur über den zentral organisierten Skype-Server möglich. Fällt dieser Server aus, ist es nicht mehr möglich, sich in das Skype-Netzwerk einzuwählen. Das Netzwerk besteht somit aus drei logischen Ebenen: Die zentrale Anmeldeebene, die Super Node Ebene für das Usermanagegment und die Host Ebene mit allen angemeldeten Usern.

### 7.3.4 Effizienz

Effizienz zu messen kann verschiedenes heissen. Wir fokussieren uns darauf wie effizient die Protokolle vom Entwickler in die Anwendungen eingebaut werden können und wie effizient tendenziell die VoIP-Anwendungen mit den entsprechenden Protokollen betrieben werden können.

Die Spezifikation von SIP hatte die Zielsetzung ein einfach implementierbares Protokoll zu sein. Dies hat die IETF durch die Basis der HTTP-Protokollstruktur erreicht. Die Entwickler kennen HTTP und somit ist SIP für sie sehr einfach nachvollziehbar. Da SIP jedoch kein binäres Protokoll darstellt, erhöht sich die benötigte Bandbreite. Zudem geht Effizienz verloren, da für den Datentransfer und dessen Signalisierung ein anderes Protokoll verwendet werden muss.

H.323 ist generell interessant für sehr professionelle und grosse Anwendungen. Die umfassende Beschreibung von H.323 komplett zu implementieren ist aber mit sehr grossem Aufwand verbunden, da nur schon eine Übersicht über alle H.x Standards einen immensen Aufwand mit sich bringt. Dies kann das Entwicklungsbudget neuer Anwendungen sprengen und ist auch der Grund, weshalb häufig das verständlichere SIP implementiert wird.

Die Effizienzvorteile von IAX gegenüber SIP werden in [43] hervorgehoben. Dies scheint durch die Reduktion auf das Minimum und den binären Charakter des Protokolls möglich zu sein.

Skype ist scheinbar effizient gelöst. Vor allem die benötigte Bandbreite von 32 kbit/s für Skype ist sehr gering. Ein Grund dafür sind sicherlich die verwendeten Codecs. Wie die Implementation aber im Detail aussieht, kann nicht beurteilt werden.

### 7.3.5 Anwendungen

SIP ist sehr flexibel und ist deshalb ein gutes Protokoll zur Implemetation von Multimedia-Anwendungen. Instant Messaging, das für Windows Server 2003 herausgegeben worden

ist und Windows Messenger verwenden SIP als Basis [23]. Internet-Telefonie mittels SIP ist möglich durch die Verwendung der Fritzbox [24]. Diese macht VoIP mit normalen Telefonen bei ausgeschaltetem Computer möglich.

H.323 wurde beispielsweise in NetMeeting [36] verwendet. NetMeeting bot VoIP Funktionalitäten und wurde in Windows 2000 und XP eingebaut. Seit Windows XP wurde dieses jedoch durch den MSN Messenger abgelöst, ist jedoch immer noch integriert. Das Pendant in Linux ist Ekiga [30]. Dies wurde jedoch nur mittels H.323 implementiert, damit eine Kommunikation mit NetMeeting von Microsoft gewährleistet war. Da seit Windows XP NetMeeting an Bedeutung verloren hat, ist nun auch Ekiga in der neuen Version 2.0 auf die Implementierung von SIP umgestiegen [35]. Für IAX gibt es einige implementierte Softwareclients wie [44] zeigt. Zudem werden auch des öfteren Produkte veröffentlicht, die mehr als nur ein Protokoll unterstützen, wie der Softwareclient von Tele2, der sowohl IAX als auch SIP unterstützt [45].

Skype hat sich fest auf dem PC etabliert, zumal die Software neu zu eBay gehört. Dadurch wird die Popularität dieser Software weiter steigen. Neben der normalen PC / Mac Version ist Skype auch für den PDA und für Linux verfügbar. Zudem sind auch normale Telefone auf dem Markt, die an den PC bzw. ans normale Telefonnetz angeschlossen werden können. Seit kurzem sind auch Skype-fähige Telefonanlagen im Handel erhältlich [54].

### 7.3.6 NAT und Firewall

SIP hat ein Problem, wenn ein Client hinter einer Firewall oder einem NAT-Router sitzt. Das kommt daher, dass für den Transport und das Sessionsmanagement unterschiedliche Ports verwendet werden und dass im SIP-Header die IP-Adresse der Clients notiert ist.

H.323 leidet ebenfalls am NAT-Problem und der Problematik von Firewalls. Gemäss [27] gibt es hierbei jedoch verschiedene Lösungsansätze. Gewisse Firewall Produkte erkennen UDP Pakete als H.323 Pakete können diese nach einer Analyse des Kontrollkanals in das interne Netz weiterleiten. Falls die eigene Firewall dies nicht unterstützt gibt es die Möglichkeit einen H.323 Proxy einzusetzen, der die Durchreichung und Analyse der Pakete übernimmt.

Da IAX komplett auf IP-Adressen im Protokoll verzichtet und die gesamte Kommunikation über einen Port funktioniert, hat IAX keine Probleme mit NAT-Routern oder Firewalls. Zudem lässt sich eine Firewall einfacher konfigurieren, wenn genau ein Port verwendet wird. Ein weiterer Vorteil von IAX ist, dass der zu verwendende Port bei der IANA registriert ist. Somit muss nur ein Port bei der Firewall freigeschaltet werden.

Wie es Skype schafft, Firewalls und NAT-Router zu umgehen, ist nicht eindeutig nachvollziehbar. Allerdings haben es die Entwickler geschafft, eine effiziente Lösung zu implementieren, denn Skype funktioniert in fast jeder Umgebung. Einer der Faktoren ist sicherlich, dass Skype einen Port dynamisch bei der Installation auswählt, zur Alternative aber auch zwei „well known“ Ports verwenden kann, die Ports 80 und 443. Zudem kann der Datentransfer sowohl mit UDP als auch mit TCP erfolgen. Als weiteres Hilfsmittel zur Bewältigung von Firewalls stehen die Super Nodes zur Verfügung. Über diese können

die Daten umgelenkt werden, sodass die Firewall den Datentransfer zulässt (z.B. mittels TCP über den Port 80).

## 7.4 Schlussfolgerungen

Zurzeit wird ein Trend in Richtung des SIP-Protokolls beobachtet. SIP bietet eine einfache Implementierbarkeit und ein grosses Mass an Flexibilität. Entwickler können auf dem bestehenden Know-How SIP Implementationen vornehmen. Durch die angebotene Modularisierung von SIP bietet sich dem Entwickler ein optimales Rüstzeug für Multimediakommunikationsanwendungen.

H.323 wird zukünftig im Endbenutzer Bereich eine untergeordnete Rolle spielen. Für die Telekomanbieter, die H.323 mittels ITU-T spezifizieren, ist H.323 eine Möglichkeit in Zukunft stärker auf paket-orientierte Netzwerke zu setzen. H.323 bietet durch seine Kompatibilität mit ISDN-Netzen eine Verbindung herkömmlicher Festnetztelefonie mit derjenigen von VoIP.

Das Überleben der IAX-Spezifikation ist eng mit dem Fortbestehen der Asterisk-Telefonanlagen verbunden. Für kleinere Firmen interessant ist die Möglichkeit, die internen Gespräche über IAX abzuwickeln, denn sowohl die Telefonanlage Asterisk als auch viele Produkte sind im Internet frei verfügbar. Dies ist eine kostengünstige Alternative zu herkömmlichen, proprietären Telefonanlagen. Die dafür notwendige Bandbreite wird durch IAX auf ein Minimum reduziert. Zudem hat IAX im Vergleich zu SIP keine Probleme mit Firewalls oder NAT-Routern, was die Konfiguration ebenfalls vereinfacht.

Skype kann eine führende Rolle im Bereich Instant-Messaging und Computer-zu-Computer Telefonie einnehmen. Dies wird gefördert durch die bereits bestehende installierte Basis und den damit verbundenen Netzwerkexternalitäten. Diese Netzeffekte entstanden durch die Effizienz und Einfachheit der Skype-Software. Im Bereich Internet-Telefonie wird Skype eine untergeordnete Rolle spielen, da es durch die proprietäre Implementierung mit anderen Standards nicht kompatibel ist.

Zudem geht der Trend in die Richtung von Komplett-Lösungen, wobei Telefonie, Internet-Anbindung, Fernsehen und Video-Streaming über eine Schnittstelle zum Endbenutzer gelangen.

# Literaturverzeichnis


[1] IETF: Overview of the IETF, http://www.ietf.org/html.charter/sip-charter.html, zuletzt aufgerufen: 05.06.2006.

[2] Henning Schulzrinne of Columbia University, http://www.cs.columbia.edu/~hgs, zuletzt aufgerufen : 04.06.2006.

[3] Institut für Informatik Freiburg: Grundlagen von VoIP am Beispiel SIP, http://www.ks.uni-freiburg.de/download/papers/telsemWS05/VoIP-SIP/SIP%20AusarbeitungBraun.pdf, zuletzt aufgerufen: 6.06.2006.

[4] Datus AG: Voice over IP IETF Standard SIP, http://www.datus.de/fileadmin/download/pdf/Kap3-IETF_SIP_Auzug.pdf, 2004, zuletzt aufgerufen: 06.06.2006.

[5] Dhiman D. Chowdhury, Unified IP Internet-working, Verlag Springer 2001.

[6] Hochschule Mittelweida: Voice over IP, http://www.htwm.de/ngeilich/voip/sip.htm, zuletzt aufgerufen: 05.06.2006.

[7] Diverse Autoren: Wikipedia Begriff: Session Initiation Protocol, http://de.wikipedia.org/wiki/Session_Initiation_Protocol, zuletzt aufgerufen: 26.05.2006, 02.09.

[8] Network Working Group: Session Initiation Protocol,http://www.ietf.org/rfc/rfc3261.txt, zuletzt aufgerufen: 06.06.2006.

[9] Douglas E. Comer, Computer Networks and Internets with Internet Applications, Pearson Prentice Hall, Fourth Edition 2004.

[10] Diverse Autoren: Wiki Begriff: SIP, http://www.voip-info.org/wiki-SIP, zuletzt aufgerufen: 06.06.2006.

[11] Selbst erstellt aus RFC3261 und aus Institut für Informatik Freiburg: Grundlagen von VoIP am Beispiel SIP, http://www.ks.uni-freiburg.de/download/papers/telsemWS05/VoIP-SIP/SIP%20AusarbeitungBraun.pdf, zuletzt aufgerufen: 06.06.2006.

[12] Jan Janak: SIP Introduction, http://www.iptel.org/ser/doc/sip_intro/sip_introduction.html, Figur 1-7. und Autor: Dhiman D. Chowdhury, Unified IP Internet-working, Verlag Springer 2001, 30.05.2006.

[13] Network Working Group: Session Initiation Protocol, http://www.ietf.org/rfc/rfc3261.txt, zuletzt aufgerufen: 06.06.2006.

[14] IETF: RFC3261, http://www.ietf.org/rfc/rfc3261.txt, zuletzt aufgerufen: 06.06.2006.

[15] Andreas Steffen, Daniel Kaufmann, Andreas Stricker: Sip Security, http://security.zhwin.ch/DFN_SIP.pdf, zuletzt aufgerufen: 04.06.2006.

[16] Qi Qiu: Study of Digest Authentication for Session Initiation Protocol (SIP), http://www.site.uottawa.ca/~bob/gradstudents/DigestAuthenticationReport.pdf, Figur 3, 12.2003.

[17] Mike Hartmann: Sicherheitsaspekte bei SIP, http://www.tecchannel.de/telko/daten/432698/index6.html, zuletzt aufgerufen: 04.06.2006.

[18] Rolf Oppliger, Internet and Intranet Security, Artech House, Second Edition 2001.

[19] Rolf Oppliger, Security Technologies for the World Wide Web, Artech House, Second Edition 2002.

[20] Andreas Steffen, Daniel Kaufmann, Andreas Stricker: Sip Security, http://security.zhwin.ch/DFN_SIP.pdf, zuletzt aufgerufen: 04.06.2006.

[21] Qi Qiu: Study of Digest Authentication for Session Initiation Protocol (SIP), http://www.site.uottawa.ca/~bob/gradstudents/DigestAuthenticationReport.pdf, 12.2003.

[22] http://download.securelogix.com/library/SIP_Security030105.pdf, zuletzt aufgerufen: 05.6.2006.

[23] Siemens Communications Enterprise Systems: SIP Session Initiation Protocol für SIP-Lösungen im Unternehmen, http://www.sofind.de/global/files/siemens/sip/siemens_Whitepaper_SIP.pdf,Version 1.0, 2004.

[24] diverse Autoren: Fritz Box, http://www.wer-weiss-was.de/faq1225/entry1812.html, zuletzt aufgerufen: 07.06.2006.

[25] ITU: ITU-T Recommendation H.323 Version 6.0, http://www.packetizer.com/voip/h323/standards.html, 04.2006.

[26] ITU: Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals - Version 3.0, http://www.packetizer.com/voip/h323/standards.html, 05.2003.

[27] Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V., Technische Universität Dresden: Sicherheit bei Videokommunikation, http://www.tu-dresden.de/t2002/4_sicherheit.pdf, 10.2002.

[28] Mathias Hein, Michael Reisner: VOIPANGO - H.323 / SIP, http://www.pyramid.de/voipango/oxid.php/sid/x/shp/oxbaseshop//cl/content/tpl/df14419788ec45166.11076348, zuletzt aufgerufen: 05.06.2006.

[29] Dipl.-Ing. Gerd Henning, Hans-Peter Mutzel: Power für VoIP-Netze, http://dbindustrie.work.svhfi.de/AI/resources/59d1949e325.pdf, 01.2001.

[30] diverse Autoren: Wikipedia Begriff: H.323, http://de.wikipedia.org/wiki/H.323, zuletzt aufgerufen: 05.06.2006.

[31] diverse Autoren: Wikipedia Begriff: H.245, http://de.wikipedia.org/wiki/H.245, zuletzt aufgerufen: 05.06.2006.

[32] diverse Autoren: Wikipedia Begriff: H.225, http://de.wikipedia.org/wiki/H.225.0, zuletzt aufgerufen: 05.06.2006.

[33] diverse Autoren: Wikipedia Begriff: QSIG, http://de.wikipedia.org/wiki/QSIG, zuletzt aufgerufen: 05.06.2006.

[34] diverse Autoren: Wikipedia Begriff: RTP, http://de.wikipedia.org/wiki/Real-Time_Transport_Protocol, zuletzt aufgerufen: 05.06.2006.

[35] diverse Autoren: Wikipedia Begriff: Ekiga, http://de.wikipedia.org/wiki/Ekiga, zuletzt aufgerufen: 05.06.2006.

[36] diverse Autoren: Wikipedia Begriff: NetMeeting, http://de.wikipedia.org/wiki/NetMeeting, zuletzt aufgerufen: 05.06.2006.

[37] M. Spencer, F. Miller: Inter-Asterisk EXchange (IAX) Version 2, http://www.cornfed.com/iax.pdf, zuletzt aufgerufen: 28.05.2006.

[38] M. Spencer, B. Capouch, E. Guy, F. Miller, K. Shumard: IAX: Inter-Asterisk EXchange Version 2, http://www.ietf.org/internet-drafts/draft-guy-iax-01.txt, zuletzt aufgerufen: 28.05.2006.

[39] http://www.voip-info.org/wiki/index.php?page=IAX, zuletzt aufgerufen: 28.05.2006.

[40] IANA: PORT NUMBERS http://www.iana.org/assignments/port-numbers, zuletzt aufgerufen: 28.05.2006.

[41] Holger Schildt: VoIP mit IAX, http://archiv.tu-chemnitz.de/pub/2004/0051/data/iax.pdf, zuletzt aufgerufen: 28.05.2006.

[42] Holger Schildt: AsteriskVoIPErprobung, http://archiv.tu-chemnitz.de/pub/2004/0008/data/asterisk.pdf, 01.10.2003, zuletzt aufgerufen: 28.05.2006.

[43] M. Spencer: IAX versus SIP, http://www.voip-info.org/wiki-IAX+versus+SIP, zuletzt aufgerufen: 05.06.2006.

[44] Inter Asterisk eXchange, http://de.wikipedia.org/wiki/IAX, zuletzt aufgerufen: 05.06.2006.

[45] D. Sokolov: Parlino: VoIP-Client von Tele2 http://www.heise.de/newsticker/meldung/72647, heise.de, zuletzt aufgerufen: 05.06.2006.

[46] S. A. Baset, H. Schulzrinne: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf, 15.09.2006, zuletzt aufgerufen: 29.05.2006.

[47] http://www.secdev.org/conf/skype_BHEU06.handout.pdf.

[48] Skype: Skype-Datenschutz FAQ, http://www.skype.com/intl/de/help/faq/privacy.html, zuletzt aufgerufen: 29.05.2005.

[49] Skype: Skype-Datenschutz FAQ, http://www.skype.com/intl/de/help/faq/technical.html, zuletzt aufgerufen: 31.05.2005.

[50] Skype: Welcome to Skype Developer Zone, https://developer.skype.com/DevZone, Skype, zuletzt aufgerufen: 31.05.2005.

[51] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy: STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). RFC 3489, IETF, 03.2003.

[52] J. Rosenberg, R. Mahy, C. Huitema: TURN: traversal using relay NAT. Internet draft, Internet Engineering Task Force, 07.2004.

[53] bo: Skype-Bug ermöglicht Dateiklau, http://www.heise.de/newsticker/meldung/73353, 20.05.2006, heise online, zuletzt aufgerufen: 29.05.2006.

[54] http://accessories.skype.com/, Skype.com, zuletzt aufgerufen: 05.06.2006.

# Kapitel 8

# Instant Messaging and Beyond - An Overview and Outlook in Direct Corporate Communications

*Marcel Lanz, Philipp Toggweiler, Thomas Rüegg*

*Diese Studie beleuchtet einleitend den Begriff Unternehmenskommunikation und zeigt einige gebräuchliche Kommunikationstechnologien mit deren Vor- und Nachteilen auf. Dabei zeigt sich, das Instant Messaging (IM) viele positive Eigenschaften hat und deshalb sehr beliebt und weit verbreitet ist. Das Ausmass, wie stark IM bereits eingesetzt wird, und die Gründe dafür, verdeutlicht eine Erhebung, welche die META Group 2004 durchgeführt hat. In der Folge wird der Schwerpunkt auf IM und verwandte Technologien gelegt. Nach einer Vorstellung der technologischen Basis werden mögliche Anwendungen und zukünftige Szenarien für die Unternehmenskommunikation, deren Voraussetzungen, bzw. Anforderungen aufgezeigt. Praktische Beispiele runden die Erkenntnisse ab. Eine Zusammenfassung ein Fazit und ein Ausblick schliessen diese Seminararbeit ab.*

## Inhaltsverzeichnis

**8.1 Einleitung . . . . . 241**
8.1.1 Ausgewählte Kommunikationstechnologien im Überblick . . . . 241
8.1.2 Die heutige und künftige Rolle von Instant Messaging . . . . . 244
8.1.3 Abgrenzung und Aufbau dieser Studie . . . . . 247
**8.2 Technische Hintergründe, verwandte Technologien . . . . . 247**
8.2.1 Systeme, Architekturen und Protokolle . . . . . 248
8.2.2 Herausforderungen und Lösungen . . . . . 254
8.2.3 Trends . . . . . 256
8.2.4 Akzeptanz . . . . . 259
8.2.5 Zukünftige Entwicklung . . . . . 260
**8.3 Instant Messaging im Geschäftsumfeld . . . . . 261**
8.3.1 Umgang unter Anwender . . . . . 261
8.3.2 Einsatzmöglichkeiten und zukünftige Szenarien für unternehmensweite Kommunikation . . . . . 262
8.3.3 Anforderungen . . . . . 264
**8.4 Geschäftsfälle . . . . . 268**
**8.5 Zusammenfassung, Fazit und Ausblick . . . . . 269**

## 8.1 Einleitung

Eine gute Unternehmenskommunikation ist entscheidend für den Unternehmenserfolg. Unter Unternehmenskommunikation [2] versteht man die Gesamtheit aller Kommunikationsmittel und -massnahmen um das Unternehmen und seine Leistungen bei allen relevanten Zielgruppen darzustellen. Sie beinhaltet sowohl die interne Kommunikation, d.h. den Austausch von Informationen und die Förderung der Kooperation zwischen den Mitarbeiter und Mitarbeiterinnen innerhalb des Unternehmens, wie auch die externe Kommunikation mit Kunden, Lieferanten, anderen Unternehmen sowie Ämtern und Behörden. Der Begriff Kommunikation wird gerade im heutigen, elektronischen Zeitalter oft falsch verstanden. Gemäss Christopher Harris-Jones von Ovum [3], einer internationalen Unternehmensberatung, welche Einflüsse der technologischen Veränderungen im Informations- und Kommunikationstechnologiemarkt auf die Unternehmen untersucht, ist Kommunikation nur dann Kommunikation, wenn der Empfänger einer Nachricht diese 100% versteht und dies dem Sender bestätigt. Also eine klassische Zweiwegkommunikation. Hingegen ist das einfache Versenden, z.B. einer E-Mail, ohne Bestätigung des Empfängers, dass er sie erhalten und vollständig verstanden hat, keine Kommunikation, sondern lediglich ein Versenden einer Nachricht.

Ausgehend von einer kurzen Vorstellung von einigen gebräuchlichen Kommunikationstechnologien mit deren Vor- und Nachteilen wird vertieft auf Instant Messaging (IM) eingegangen. Anhand einer Erhebung, welche den Einsatz von IM im täglichen Leben untersuchte wird aufgezeigt, dass IM mit seinen vielfältigen Funktionen und positiven Eigenschaften sehr beliebt und dementsprechend weit verbreitet ist. Neben all den Vorteilen die IM auch hat, bringt diese Technologie aber auch einige Sicherheitsrisiken mit sich. In der Schlussfolgerung wird kurz darauf eingegangen.

### 8.1.1 Ausgewählte Kommunikationstechnologien im Überblick

Es gibt eine Vielzahl von Kommunikationstechnologien und Methoden um Informationen auszutauschen oder um Kollaboration zu ermöglichen. Es ist nicht möglich, eine abschliessende Präsentation aller Möglichkeiten zu geben. Wir beschränken uns hier auf eine Auswahl von gängigen Technologien:

- Telefon
- Fax
- Short Message Service (SMS)
- E-Mail
- Intranet
- Docweb
- Blogs

- Wikis
- Instant Messaging
- Diskussionsgruppen

Sowohl das Telefon, der Fax sowie das E-Mail System mit seinen kollaborativen Eigenschaften wie Kalender sind heute in keiner Firma wegzudenken. Ebenso wenig wie das Intra-/Internet und Docweb, welches Zugang zu allen wichtigen Informationen und Dokumenten bietet.

Das Telefon ermöglicht eine Zwei- bzw. Mehrwegkommunikation, d.h. es ermöglicht den schnellen Informationsaustausch zwischen zwei TeilnehmerInnen, oder bei einer Konferenzschaltung zwischen beliebig vielen TeilnehmerInnen. Der Vorteil des Telefonats ist, dass man sich einfach ausdrücken und unklare Aussagen durch Nachfragen korrigieren kann. Dank Mobiltelefonie ist die Erreichbarkeit der Teilnehmer sehr hoch. Aber dennoch sind da einige Nachteile nicht zu unterschätzen. Damit der Informationsaustausch mittels Telefon möglich wird, müssen alle Teilnehmer zur gleichen Zeit erreichbar sein und können in dieser Zeit keiner anderen Tätigkeit nachgehen. Im weiteren dürfen Telefonate nicht ohne Einverständnis aller Teilnehmenden aufgezeichnet werden [4] und somit ist das einmal gesagte zu einem späteren Zeitpunkt nicht mehr abrufbar. Zudem kann man zwar Missverständnisse hinsichtlich unklarer Aussagen eliminieren, doch ist nach wie vor nicht auszuschliessen, dass alle TeilnehmerInnen auch das Gleiche verstanden haben.

Der Fax bietet die Möglichkeit Dokumente jederzeit zu übertragen. Dabei erhält der Sender eine Bestätigung, dass das Fax an das gewählte Gerät übermittelt wurde. Aber das bedeutet nicht, dass die Nachricht auch angekommen ist. Um dies zu klären ist nachfolgend z.B. ein Telefonat nötig. Im weiteren hat das Fax den Nachteil, dass die übermittelten Daten nicht elektronisch verfügbar sind und somit nicht gespeichert und allenfalls weiter verarbeitet werden können. Da verschiedene Technologien die elektronische Übermittlung von Dokumenten und Daten ermöglichen, ist den Faxgeräten im heutigen elektronischen Zeitalter keine grosse Bedeutung mehr beizumessen.

Anders sieht es bei E-Mail Systemen aus. E-Mail Systeme erlauben den elektronischen Austausch von Nachrichten und Dokumenten, bzw. Daten als Anhang. Sie sind die verbreitetste Methode der schriftlichen Kommunikation und sie sind sehr effektiv. Sie können jederzeit geschrieben und versendet werden. Der Empfänger erhält die Nachricht genau dann, wenn er entweder bei herkömmlichen E-Mail Systemen aktiv die Nachrichten abruft oder bei moderneren Systemen, den sog. Push-Mail die Arbeit der Zustellung des Mails dem Server überlässt. Moderne E-Mail Systeme beinhalten auch kollaborative Eigenschaften wie z.B. Kalender, die von allen MitarbeiterInnen einer Firma eingesehen werden können (selbstverständlich abhängig von den gewährten Rechten) und einfache Terminvereinbarungen mit verschiedenen Teilnehmern ermöglichen. Neben all den Vorteilen haben E-Mail Systeme auch Nachteile in der Kommunikation. Gerade weil es so einfach ist, ein E-Mail zu schreiben und/oder an mehrere Adressaten weiter zu leiten, werden zu viele Informationen versendet. Dies hat zu Folge, dass einige Empfänger regelrecht mit Mail's überflutet werden. Als Konsequenz werden einige E-Mails nur noch

überflogen oder gar nicht mehr gelesen. Der Sender darf folge dessen nicht davon ausgehen, dass seine Mails effektiv vom Empfänger empfangen, gelesen und verstanden wurden und somit potentielle Aktionen vom Empfänger ausgeführt werden.

Mittels Short Message Service (SMS) können schriftliche Kurznachrichten entweder von Mobiltelefonen oder von anderen technischen Geräten wie Computer, Palmtops, etc. auf Mobiltelefone oder auch Faxgeräte versendet werden. Ist das Empfangsgerät nicht eingeschaltet, dann wird die Mitteilung beim Mobilfunk-Anbieter solange zwischengespeichert, bis das Empfangsgerät eingeschaltet wird. Mittels SMS ist Kommunikation im Sinne einer Zweiwegkommunikation nur schwer möglich, da die Mitteilungen eine limitierte Länge haben. Dennoch ist der SMS Service sehr nützlich, da z.B. Statusmeldungen, als typische Vertreter von Einweginformationen an eine grosse Anzahl Empfänger gesendet werden können.

Der Begriff Blog steht für Weblog. Es handelt sich hierbei um eine Webseite im Inter- bzw. Intranet, die von einem oder mehreren Autoren regelmässig mit Einträgen ergänzt wird. Diese Einträge können Texte, Links auf andere Webseiten, Bilder und Videos enthalten. Das Ziel von Blogs ist lediglich Informationen für andere zur Verfügung zu stellen. Also eine klassische Einwegkommunikation.

Die Wiki Software ermöglicht mehreren Autoren schnell und einfach eine Inter-/Intranetseite mit Wissen zu füllen. Das Wort Wiki wurde vom hawaiianischen Wort „wikiwiki“, was abgeleitet „schnell“ bedeutet [5]. Wiki's sind als Wissensmanagement-Tool im Umfeld der „Entwurfsmuster“ - Theoretiker entstanden. Der Vorteil der schnellen Wissensaufbereitung wird jedoch getrübt mangels Kontrolle. Die Tatsache, dass jeder Leser der Seite auch die Rolle des Autors übernehmen kann, hat zur Folge, dass einerseits geschriebener Text überschrieben werden kann und dass anderseits falsches oder unkorrektes Wissen publiziert werden kann. Aus diesem Grund sind Wikis in Unternehmen nur bedingt einsetzbar und werden nach unserer Meinung keine Rolle im Rahmen der Unternehmenskommunikation spielen.

Instant Messaging (IM) ermöglicht Kommunikation über ein Netzwerk in Echtzeit [6]. Entstanden ist IM bereits in den 80er Jahren. Verbreitet wurde IM aber erst Mitte 90er, mit der Erfindung der sog. Buddylist (Liste mit Freunden) und dem Internet Boom. Da sowohl Sender und Empfänger online sind, findet eine klassische Zweiweg- oder bei mehreren Teilnehmern eine Mehrwegkommunikation in schriftlicher Form und in Echtzeit statt. Die meisten gängigen IM Applikationen bieten zudem die Möglichkeit Daten und Dokumente auszutauschen und statt schriftlicher Kommunikation auch Video oder Telefonkonferenzen durchzuführen. Obwohl viele Firmen die Möglichkeiten von IM heute noch nicht offiziell nutzen, wird sich das in Zukunft stark ändern. Der Grund dafür werden wir Ihnen im nächsten Unterkapitel vorstellen.

Obwohl E-Mail und IM sehr effektiv sein können, empfiehlt es sich bei einer Kommunikation zu einem bestimmten Thema zwischen vielen Teilnehmern mittels so genannten Diskussionsgruppen bzw. Inter-/Intranet Foren zu arbeiten. Obwohl Diskussionsgruppen nicht in Echtzeit kommunizieren können, wie es beispielsweise mittels IM der Fall ist, können Informationen doch in der Geschwindigkeit von E-Mails ausgetauscht werden. Der grosse Vorteil ist jedoch, dass es viel einfacher ist der Konversation zu folgen und zu einem späteren Zeitpunkt nochmals darauf zurück zu kommen.

### 8.1.2 Die heutige und künftige Rolle von Instant Messaging

Wie im vorhergehenden Unterkapitel bereits kurz erwähnt, wird IM in vielen Unternehmen noch nicht offiziell genutzt. Mit offiziell genutzt meinen wir, dass die Unternehmen die Kommunikation mittels IM ermöglicht, indem sie die benötigte Software installieren und Warten. Tatsache ist, dass in den Unternehmen die Kommunikation mittels IM schon seit 2004 sehr stark verbreitet ist, auch wenn die Software nicht offiziell installiert und somit zur Verfügung gestellt wird. Dies verdeutlicht die folgende Statistik welche die META Group, ein weltweit führendes Marktforschungs- und Beratungsunternehmen im Bereich der Informationstechnologie und der Business Transformation 2004 über den Einsatz von IM im täglichen Leben erstellt hat [7].

Fokus der Erhebung war zu erkennen, wie IM im täglichen Leben, z.B. für den Heimgebrauch, im Geschäft, via mobile Geräte eingesetzt wird. Dazu wurden Endbenutzer verschiedenen Alters (zwischen 20-65 Jahren), von 300 globalen Firmen unterschiedlicher Grössen und von verschiedenen Segmenten befragt.

Tabelle 8.1: Fakten zur Erhebung

| Kriterium | Kenngrösse |
|---|---|
| Altersdurchschnitt | 45.9 Jahre |
| Segmentierung der Unternehmensgrösse | 1-99 Angestellte (33%)<br>100-999 Angestellte (16.3%)<br>1000 oder mehr Angestellte (50.7%) |
| Unternehmensspannweite:<br>(mehr als 22 Unternehmensbereiche wurden in die Erhebung einbezogen) | IT Services, High Tech und Consulting (29.3%)<br>Bildungswesen (7.3%)<br>Software Entwicklung (6.7%)<br>Finanzdienstleistung (6%)<br>Gesundheitswesen/Pharmazie (5%)<br>Dienstleistungsbetriebe (5%)<br>etc. |

#### Schlüsselbefunde

#### Einsatz von IM Services im Heimgebrauch vs. Geschäftsgebrauch

Der Einsatz von IM für den Heimgebrauch ist stark verbreitet. Interessanterweise wird jedoch IM noch stärker in Unternehmen eingesetzt. Dabei ist das Verhältnis Heimgebrauch/Geschäftsgebrauch abhängig von der Unternehmensgrösse, wie Tabelle 8.2 zeigt:

Dieser Trend erklärt sich dadurch, dass grössere Unternehmen eher die Bereitschaft haben, neuere Technologien einzusetzen um die Produktivität zu vergrössern. Tatsache ist, dass sich dies grössere Unternehmen im Vergleich zu den kleineren und mittleren finanziell auch besser leisten können. Kleinere und mittlere Unternehmen tendieren dazu, abzuwarten bis neue Technologien stark verbreitet sind und somit die Marktpreise sinken. Die dennoch

Tabelle 8.2: Einsatz von IM im Heimgebrauch vs. Geschäftsgebrauch

| Unternehmensgrösse | Heimgebrauch | Geschäftsgebrauch |
|---|---|---|
| kleinere Unternehmen | 37% | 57% |
| mittlere Unternehmen | 30% | 61% |
| grössere Unternehmen | 28% | 71% |

sehr hohe Zahl des IM Einsatzes für Geschäftszwecke überrascht jedoch nicht. Dies lässt sich dadurch erklären, dass „public IM Services“ kostenlos vom Internet heruntergeladen werden und einfach und schnell installiert werden können.

**Einfluss einer Richtlinie, die den IM-Einsatz in der Firma regelt**

Wahrscheinlich haben die meisten Unternehmen Richtlinien hinsichtlich Einsatz von E-Mail und Telefon erlassen und kommuniziert. Doch Richtlinien hinsichtlich Instant Messaging fehlen noch mancherorts. Dieses Manko sollten sich die Unternehmer bewusst werden, denn Richtlinien haben doch einen gewissen Einfluss auf das Verhalten der Mitarbeiter. Zum Beispiel hat die Erhebung ergeben, dass wenn der Einsatz von IM durch eine Richtlinie verboten ist, sich erfreulicherweise immerhin 49% der Befragten daran halten. In kleineren Unternehmen würden nur 10% der Befragten IM dennoch einsetzen und in grösseren Firmen sogar nur deren 3%. Tabelle 8.3 zeigt auf, wie viele % der Befragten IM im Zusammenhang mit dem Vorhandensein einer Richtlinie einsetzen würden.

Tabelle 8.3: Benutzung von IM in Abhängigkeit einer Richlinie

| Richtlinie | Benutzung von IM |
|---|---|
| vorhanden, IM verboten | 2.5% |
| vorhanden, limitierter Gebrauch erlaubt | 45% |
| nich vorhanden | 47% |
| nicht bekannt, ob vorhanden oder nicht | 5% |

**Persönlicher- vs. Geschäftsgebrauch, abhängig vom Einsatzort**

Sowohl beim Heimgebrauch, wie auch im Geschäftsgebrauch wird IM für persönliche wie auch geschäftliche Zwecke eingesetzt, wie Tabelle 8.4 zeigt:

Tabelle 8.4: Zweck des IM Einsatzes abhängig vom Einsatzort, bwz. Einsatzmittel

| Einsatzort/-Mittel | persönlicher Einsatz | Einsatz für's Geschäft | beides |
|---|---|---|---|
| zu Hause | 44% | 7% | 49% |
| im Geschäft | 5% | 43% | 52% |
| mobiles Gerät | 17% | 20% | 63% |

**Wahrgenommene Werte für den Einsatz von IM in Unternehmen**

IM wird als sehr effizient und angenehm im Einsatz empfunden. Speziell die Echtzeitkommunikation wird stark geschätzt, wie folgende, nicht abschliessende Auflistung der Gründe für den IM Einsatz zeigt.

- Schnellere Reaktion, bzw. Antwort als mit E-Mail 78%
- schnelle Problemlösung 74%
- Multitasking 71%
- Presence - Die Möglichkeit zu sehen, ob Mitarbeiter, Kollegen/-innen oder Freunde online und verfügbar sind 63%
- Die Möglichkeit, schnell die Aufmerksamkeit einer oder mehrere Personen zu erhalten 62%
- Jemand zu erreichen, der ein E-Mail nicht beantwortet hat oder nicht zurück gerufen hat 37%

**Fast alle Funktionen, welche IM Applikationen bieten werden eingesetzt**

Die meisten IM Applikationen bieten wesentlich mehr Funktionen als nur Chat. Fast alle Funktionen, welche IM Applikationen bieten, wie z.B. File Transfer, Voice, Video, Conferencing, etc. werden sowohl zu Hause, wie auch im Geschäft benutzt. Siehe Tabelle 8.5.

Tabelle 8.5: Einsatz der verschiedenen verbreiteten Funktionen von IM Applikationen

| Funktion | zu Hause | im Geschäft |
|---|---|---|
| Messaging (Chat) | 98% | 95% |
| File Transfer | 42% | 41% |
| Conferencing | 17% | 46% |
| Voice | 27% | 15% |
| Video | 22% | 12% |

**Schlussfolgerung**

Die oben dargestellten Fakten verdeutlichen, dass IM ein sehr beliebtes, effizientes Werkzeug auch für Geschäftszwecke darstellt und somit in Zukunft immer mehr zum Einsatz kommen wird. Dies bedeutet für Unternehmen, dass sie dieses Thema sehr ernst nehmen müssen und in ihre IT-Strategie mit einbeziehen, denn IM Applikationen bringen einige Sicherheitsrisiken mit sich. Um hier einige zu nennen [8]:

- offene, unsichere Verbindungen
- Denial of Service (DoS)
- betrügerisches Auftreten durch Annahme einer fremden Identität
- Viren und Würmer via File Transfer Funktion
- Klartext Speicherung von IM Einstellungen in der Registry oder von archivierten Messages

- Unsichere Standardeinstellungen hinsichtlich Privatsphäre und Sicherheit
- bösartige Hyperlinks, welche über Messages versendet werden

Selbstverständlich hat der IM- und IT Sicherheits-Markt diese Probleme schon längst erkannt und arbeitet mit Hochdruck daran, sichere (und selbstverständlich kostenpflichtige) Lösungen für Unternehmen zu entwickeln. Um dies zu verdeutlichen hier ein Auszug aus einem IT-News Artikel von Gartner Group Deutschland [9]:

*„MessageLabs, ein Dienstleister aus dem Bereich der E-Mail-Sicherheit hat einen kleinen Anbieter für Instant Messaging im Geschäftskundenumfeld übernommen. Dies deutet darauf hin, dass Services und Sicherheitsangebote in den Bereichen E-Mail und IM zusammenwachsen...“*

### 8.1.3 Abgrenzung und Aufbau dieser Studie

Da einerseits Instant Messaging Einsatz bereits stark verbreitet ist und noch stärker verbreitet werden wird und anderseits IM Applikationen viele nützliche Funktionen bereitstellen, welche Echtzeitarbeit und Kooperation fördern, konzentrieren wir uns im Folgendem auf diese Gebiet. In Kapitel 8.2 stellen wir die technische Basis von IM und verwandten Technologien vor. In Kapitel 8.3 werden dann mögliche Anwendungen und zukünftige Szenarios für die Unternehmenskommunikation, deren Voraussetzungen, bzw. Anforderungen vorgestellt und mit Geschäftsmodellen abgerundet. Zur Illustration der vorgestellten Informationen werden im Kapitel 8.4 dann Geschäftsfälle, also praktische Beispiele vorgestellt. Eine Zusammenfassung, unser Fazit und ein Ausblick schliessen dann diese Arbeit ab.

## 8.2 Technische Hintergründe, verwandte Technologien

Dieses Kapitel befasst sich mit den technischen Aspekten von Instant Messaging. Als erstes wird ein Überblick über die häufigsten Protokolle und Architekturen gegeben und anschliessend werden die Protokolle OSCAR [14] des AOL Instant Messangers AIM [15] und XMPP/Jabber [16] detaillierter betrachtet und verglichen. Als zweites werden die technischen Herausforderungen und mögliche Lösungen im Hinblick auf einen Einsatz in Unternehmungen diskutiert. Im dritten Teil werden einige Trends diskutiert, wobei die Erweiterung zu mobilen Endgeräten spezielle Beachtung finden wird. Im Hinblick auf eine Integration von Instant Messaging in Unternehmensapplikationen wird der Live Communication Server 2005 von Microsoft [17] und IBM Lotus Sametime 7.5 [18] betrachtet. Im vierten Teil wird kurz die Akzeptanz von Instant Messaging aus technischer Sicht für Firmen im Allgemeinen und etwas ausführlicher die Akzeptanz von neuen Entwicklungen bei Serviceprovidern diskutiert. Zum Schluss gibt der fünfte Teil einen Ausblick und fasst die wichtigsten Teile des Kapitels zusammen.

### 8.2.1 Systeme, Architekturen und Protokolle

Wie in 8.1.1 bereits erwähnt, gibt es IM-Systeme schon länger. Als Vorläufer kann man den UNIX Befehl `talk` sehen, der eine einfache textuelle Zweiwegkommunikation am Terminal ermöglicht. 1988 wurde das erste weit verbreitete Protokoll für einen IM ähnlichen Service, Internet Relay Chat (IRC) vom Finnen Jarkko Oikarinen entwickelt und im Mai 1993 von der Internet Engingeering Task Force (IETF) mit dem Request For Comment (RFC) 1459 zum Standard erhoben. Dieser ist heute immer noch in Betrieb und wird auch weiterentwickelt. RFC 2811 beschreibt den Kern der aktuellen Version. Im November 1996 wurde ICQ (ein Wortspiel aus „I Seek You“) vom israelischen Startup Mirabilis ins Leben gerufen. ICQ war der erste IM Client im eigentlichen Sinne mit Buddy List und Präsenzinformation. Er verbreitete sich sehr schnell und konnte im Mai 1997 bereits 850'000 registrierte Nutzer zählen [20]. Bereits Im Januar 1997 startete Yahoo mit seinem Yahoo Instant Messanger [21] und 4 Monate später brachte AOL den AIM auf den Markt. Im Juni 1997 wurde Mirabilis mit ICQ von AOL aufgekauft und die Protokolle wurden kurz darauf integriert auch wenn bis heute separate Clients erhältlich sind.

#### Architekturen für IM

Es gibt grundsätzlich zwei Architekturvarianten, wie zwei IM Clients miteinander kommunizieren können: entweder direkt oder über einen Server. Für Login, Authentifizierung und den Austausch von Präsenzinformation kommunizieren alle hier betrachteten Systeme über einen Server. Für den Austausch der eigentlichen Textnachrichten verwenden wiederum alle Protokolle ausser das bereits erwähnte IRC und das weiter unten diskutierte, auf dem Session Initiation Protocol (SIP) basierende SIP/SIMPLE die Kommunikation über den Server. Für die weiteren Services wie Dateitransfer oder Videokonferenz kommen andere Protokolle zum Einsatz, die immer direkt zwischen den Clients kommunizieren, nur schon deshalb, weil die Datenmenge sonst zu gross wäre. Bei der Architektur mit dem Server gibt es wiederum zwei verschiedene Architekturen, die Ein- und die Mehrserverarchitektur (vgl. Abb. 8.1).

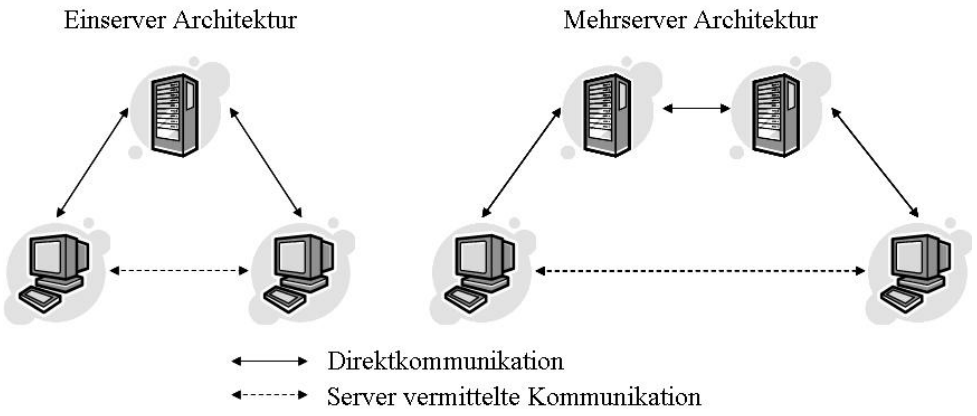



Abbildung 8.1: Generische Architekturen für IM nach [8]

Bei der Einserverarchitektur muss es sich nicht zwingend um einen einzelnen physischen Server handeln, sondern es kann auch ein Cluster aus Servern und Proxies sein, die geo-

graphisch verteilt sein können, aber alle zur gleichen Domain gehören und von derselben Organisation betrieben werden. Dieser Ansatz bringt einige gewichtige Nachteile mit sich. So ist die Leistungsfähigkeit bei einer grossen Zahl von Benutzern eher schlecht, da die zentrale Infrastruktur stark belastet wird. Auch die Skalierbarkeit ist durch die zentrale Struktur nicht optimal. Im Bereich der Sicherheit fällt ein Angriff auf die Einserverarchitektur einfacher, sei es, um unerlaubterweise an Daten zu kommen oder beispielsweise mittels Denial-of-Service Attacken das System lahmzulegen.

Demgegenüber bietet die Mehrserver Architektur im Bereich der Leistungsfähigkeit und Skalierbarkeit vorteile durch die dezentrale Struktur. Bei der Sicherheit sind prinzipiell Vorteile möglich, allerdings nur, wenn die konkrete Architektur sorgfältig entworfen wird. Die Komplexität der Mehrserver Architektur ist zu Beginn generell höher, sowohl bei der Spezifikation und Implementation als auch in der Wartung. Tabelle 8.6 fasst die Vor und Nachteile der beiden Architekturen zusammen.

Tabelle 8.6: Vor- und Nachteile der Ein- und Mehrserver Architektur nach [22]

| Eigenschaft | Einserver Architektur | Mehrserver Architektur |
|---|---|---|
| Skalierbarkeit | beschränkt | gut |
| Verwundbarkeit | gross | mittel |
| Leistungsfähigkeit | beschränkt | gut |

Von den in diesem Papier betrachteten Protokollen verwenden alle quelloffenen eine Mehrserver Architektur, die proprietären eine Einserver Architektur. Dies macht unter Berücksichtigung der Vor- und Nachteile durchaus Sinn. Die proprietären Systeme sind älter und wurden vermutlich in kürzerer Zeit unter Beteiligung verhältnismässig weniger Personen entwickelt als die breit abgestützten quelloffenen Systeme. Somit war zu Beginn auch die Benutzerzahl der proprietären Systeme kleiner und die Netze liessen und lassen sich einfacher überwachen und beispielsweise einfacher gegen unerwünschte Teilnehmer mit anderen als den systemeigenen Clients absichern.

### Überblick über Systeme und Protokolle

Heute existiert eine grosse Anzahl von IM Systemen und Protokollen. Wikipedia [23] listet über 25 Protokolle und über 55 Clients auf. Viele dieser Protokolle sind proprietär. Schon rein aufgrund der Anzahlen wird klar, dass es für diverse Protokolle mehrere Clients gibt. Ebenso klar ist, dass die Freunde einer bestimmten Person mit grosser Wahrscheinlichkeit nicht alle dasselbe System benutzen. Um nicht den ganzen Bildschirm mit diversen Clients der verschiedenen Systeme zu füllen gibt es heute eine stattliche Anzahl von Multiprotokoll Clients die sich gleichzeitig in verschiedenen Systemen anmelden können, wenn auch für jedes System ein eigenes Konto benötigt wird.

Eine solche Vielfalt legt natürlich eine Standardisierung nahe. Die IETF hatte mit IRC schon ziemlich früh einen Standard in der Hand, der allerdings mit den neuen Funktionen wie Präsenzinformation über das ganze Netz und Buddylists nicht mithalten konnte. 1999 gründete die IETF die Instant Messaging and Presence Protocol (IMPP) Working

Group um Anforderungen und ein Framework für Instant Messaging zu erarbeiten und gegebenenfalls ein Protokoll zu definieren, dass diese Anforderungen auch erfüllt [24]. Wie schon in der vorsichtigen Formulierung der Ziele vorweggenommen, hatte diese Arbeitsgruppe grosse Probleme, sich auf ein Protokoll zu einigen und es auch nie soweit gebracht. Also sollte der Markt entscheiden, welches Protokoll sich durchsetzen soll und es wurden drei Arbeitsgruppen gegründet: Application Exchange (APEX), die einen Standard verabschiedet hat, der aber keine grosse Verbreitung fand, Presence and Instant Messaging Protocol (PRIM), die sich nicht einmal auf einen Entwurf einigen konnte und SIP for Instant Messaging and Presence Leveraging Extension (SIMPLE), die einen Standard verabschiedet hat. Die IMPP Arbeitsgruppe sollte dabei mit ihrem Modell dafür sorgen, dass Interoperabilität gewährleistet werden kann.

Heute verfügt die IETF über zwei Standards, nämlich das erwähnte SIMPLE, welches auf das weit verbreitete SIP aufsetzt und in den RFCs 3856, 3857, 3858 und 3994 spezifiziert ist sowie Extensible Messaging and Presence Protocol (XMPP) der entsprechenden Arbeitsgruppe mit den RFCs 3920, 3921, 3922 und 3924 [16]. Die SIMPLE Arbeitsgruppe ist nach wie vor sehr aktiv und hat 15 aktive Drafts fertig gestellt [25]. Auf dieses Protokoll wir in 8.2.3 weiter eingegangen. XMPP wurde im zweiten Anlauf aus dem von der Jabber Open Source Gemeinschaft eingereichten Entwurf im Oktober 2004 zum Standard erhoben. Es wird weiter unten in diesem Abschnitt behandelt.

Neben der IETF gibt es auch noch die Instant Messaging and Presence Service (IMPS) Spezifikation. IMPS wurde ursprünglich von grossen Mobilfunkherstellern darunter Ericsson, Motorola und Nokia unter dem Namen Wireless Village ins Leben gerufen. Unterdessen ist die Spezifikation von der Open Mobile Alliance (OMA) [40] übernommen worden und liegt seit Oktober 2005 in der Version 1.2.1 vor. Version 1.3 existiert als Entwurf. IMPS ist ein textbasiertes Protokoll zum Austausch von Textnachrichten und Präsenzinformationen mit dem Ziel, Interoperabilität zwischen den verschiedenen mobilen Clients und über Gateways mit den bestehenden und zukünftigen Services herzustellen. Mehr Details werden unter 8.2.3 behandelt.

Bei den proprietären Protokollen betrachten wir hier die bekanntesten. Allen gemeinsam ist, dass keine offiziellen Informationen zugänglich sind und die auf dem Internet verfügbaren Informationen durch Reverse Engineering v. a. von Entwicklern von Multiprotokoll Clients gewonnen wurden und immer noch werden. Ebenfalls den meisten gemeinsam ist die Tatsache, das es regelmässig zu Versionsänderungen kommt und dies nicht nur, um neue Funktionalitäten zu ermöglichen oder Fehler zu beseitigen sondern oft auch nur um die Authentifizierung anzupassen und somit die Multiprotokoll Clients solange aus dem entsprechenden Netz auszuschliessen, bis die neue Protokollversion wiederum analysiert und die Ergebnisse veröffentlicht werden.

Open System for Communications in Real-time (OSCAR) ist das binäre Protokoll von AOLs AIM [15] und von ICQ [20]. OSCAR wird weiter unten detaillierter betrachtet. Mobile Status Notification Protocol (MSNP) ist das Protokoll von Microsfts MSN Messenger [26]. MSNP ist ein textbasiertes Protokoll und unterstützt diverse Services wie Textnachrichten, Audi/Video Chat, Bilder und andere. Die Authentifikation geschieht über ein Passport Konto, wobei MSNP neben der Emailadresse des Passport Kontos auch noch einen Anzeigenamen und einen Spitznamen unterstützt. Microsoft wollte MSNP ur-

sprünglich zu einem offenen Standard machen und reichte bei der IETF einen Entwurf ein, den die Firma dann aber verfallen liess [14]. Der Entwurf ist unter [27] zugänglich. Yahoo verwendet zwei verschiedene Protokolle, zum einen YMSG für seinen Messenger [21] und YCHT für den Java basierten Chat Client. Die Protokolle sind schlecht dokumentiert und Yahoo scheint sich grosse Mühe zu geben, fremde Clients aus seinem Netzwerk zu halten [14], weshalb hier nicht auf weitere Details eingegangen wird.

Tabelle 8.7 zeigt eine einfache Zusammenfassung der hier besprochenen Protokolle.

Tabelle 8.7: Übersicht über IM Protokolle

| Protokoll | Urheber | Lizenz | Adressierung | Transportschicht Sicherheit |
|---|---|---|---|---|
| IMPS | OMA | offen | wv:name@domain.tld e. g. wv:bob@unizh.ch | teilw. |
| MSNP | Microsoft | proprietär | Mailadresse (.NET Passport) e. g. alice@unizh.ch | nein |
| OSCAR | AOL | proprietär | Benutzername oder UIN e. g. 12345678 | nein |
| SIP/ SIMPLE | IETF | offen | sip:name@domain.tld e. g. sip:bob@unizh.ch | ja |
| XMPP/ Jabber | Jeremie Miller IETF | offen | name@domain.tld/resource e. g. alice@unizh.ch/office | ja |
| YMSG/ YCH | Yahoo | proprietär | Benutzername e. g. alice_mueller | nein |

Im Folgenden wird auf OSCAR und XMPP etwas detailliert eingegangen. Der unterste Level des binären OSCAR Protokolls besteht aus so genannten FLAP Frames, die als Paket Frame auf dem kontinuierlichen TCP Stream dienen und ein Kanal Konzept ähnlich dem Port Konzept von TCP bieten. Auf den FLAP Frames bauen die SNAC Pakete auf. Sie werden als Basiseinheit zwischen Client und Server transportiert. Ein FLAP Frame kann genau ein SNAC Paket enthalten, wobei bis auf die Header die Länge beider Pakete variabel ist. AIM Befehle werden in SNAC Pakete verpackt, wobei über 200 Befehle existieren und die Weiterentwicklung des Protokolls läuft einfach über den Ersatz von Befehlen. Dies ist nur ein grober Überblick, mehr Details finden sich in [14]. Um sich mit dem OSCAR Netzwerk zu verbinden meldet sich der Client per TCP auf Port 5190 beim Autorisationsserver login.oscar.aol.com resp. login.icq.com. Allerdings scheint auch jeder andere TCP Port zu funktionieren. Die User ID besteht dabei aus einem alphanumerischen String und kann frei gewählt werden. Nach erfolgreicher Autorisation erhält der Client ein Session Cookie und die Adresse eines Basic Oscar Servers (BOS). Bei diesem meldet sich dann der Client mit dem Cookie und handelt Verbindungsparameter sowie vorhandene resp. gewünschte Services aus. Für weitere Details siehe [28, 29]. Im Netzwerk existieren etliche BOS, wobei der Authentisierungsserver diese zur Lastverteilung braucht. Neben OSCAR existiert auch noch ein Protokoll Namens Talk to OSCAR (TOC). TOC ist ein textbasiertes Wrapper Protokoll zu OSCAR das über Gateways funktioniert, die TOC in

OSCAR übersetzen und umgekehrt. Ursprünglich gab AOL TOC einmal unter der GPL frei, zog das Dokument später aber wieder zurück [14].

Bei XMPP handelt es sich um einen offiziellen Standard der IETF. Es ist in vier RFCs definiert und zwar in "XMPP: Core" (RFC 3920) [30], "XMPP: Instant Messaging and Presence" (RFC 3921) [31], "Mapping the XMPP to Common Presence and Instant Messaging (CPIM)" (RFC 3922) [32] und "End-to-End Object Encryption in the XMPP" (RFC 3923) [33]. Die Architektur von XMPP besteht dabei aus Clients, Servers und Gateways wobei eine Multiserver Architektur zur Anwendung kommt, wie in Abb. 8.2 zu sehen ist.

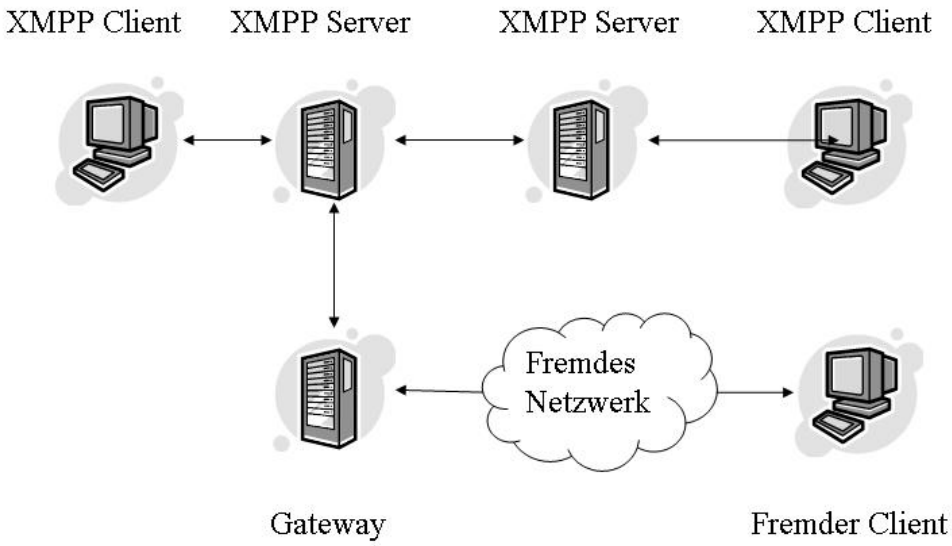



Abbildung 8.2: XMPP Architektur

Jeder Client gehört zu einem Server. So funktioniert auch das Adressierungsschema genannt Jabber ID (JID) name@domain.tld/ressource, wobei jeder Benutzer mehrere Ressourcen haben kann: Damit werden mehrfache Logins ermöglicht, beispielsweise kann sich ein Teilnehmer von zuhause und unterwegs mit seinem Mobiltelefon anmelden. Die Clients kommunizieren ausschliesslich über die Server über eine TCP Verbindung. Das Gateway übersetzt XMPP Nachrichten in andere Protokolle und bindet somit andere Systeme an. Dabei hält sich XMPP an die Standards der IMPP Arbeitsgruppe, die in den RFCs 2778 und 2779 beschrieben sind. RFC 3922 beschreibt das Mapping von XMPP zu CPIM. XMPP besteht aus XML Strömen und XML Stanzen (Stanze: italienische Versform). Ein Verbindungsaufbau ist schematisch in Abb. 8.3 dargestellt.

Der Client öffnet zuerst eine TCP Verbindung und etabliert dann mittels `<stream>` einen XML-Stream. Somit ist eine unidirektionale Verbindung geöffnet. Wird eine bidirektionale Verbindung benötigt, so öffnet der Server ebenfalls mit dem `<stream>` Tag einen XML Stream. Tritt ein Fehler auf, so sendet der Partner ein `<error>`. Nachdem der Stream geöffnet ist, können Stanzen geschickt werden, wobei es die drei Typen gibt, `message`, `presence` und `iq` (Info/Query). Alle Stanzen haben bestimmte gemeinsame Attribute, so z. B. `to` für den Empfänger. Der Server muss also die Stanze zum im `to` Attribut genannten Empfänger routen. Nachdem alle Stanzen gesendet sind, schliessen der Client und der Server den Stream wieder und er Client baut die TCP Verbindung ab. Dadurch, dass nur der Client TCP Verbindungen öffnen muss, gibt es keine Probleme mit NAT. All

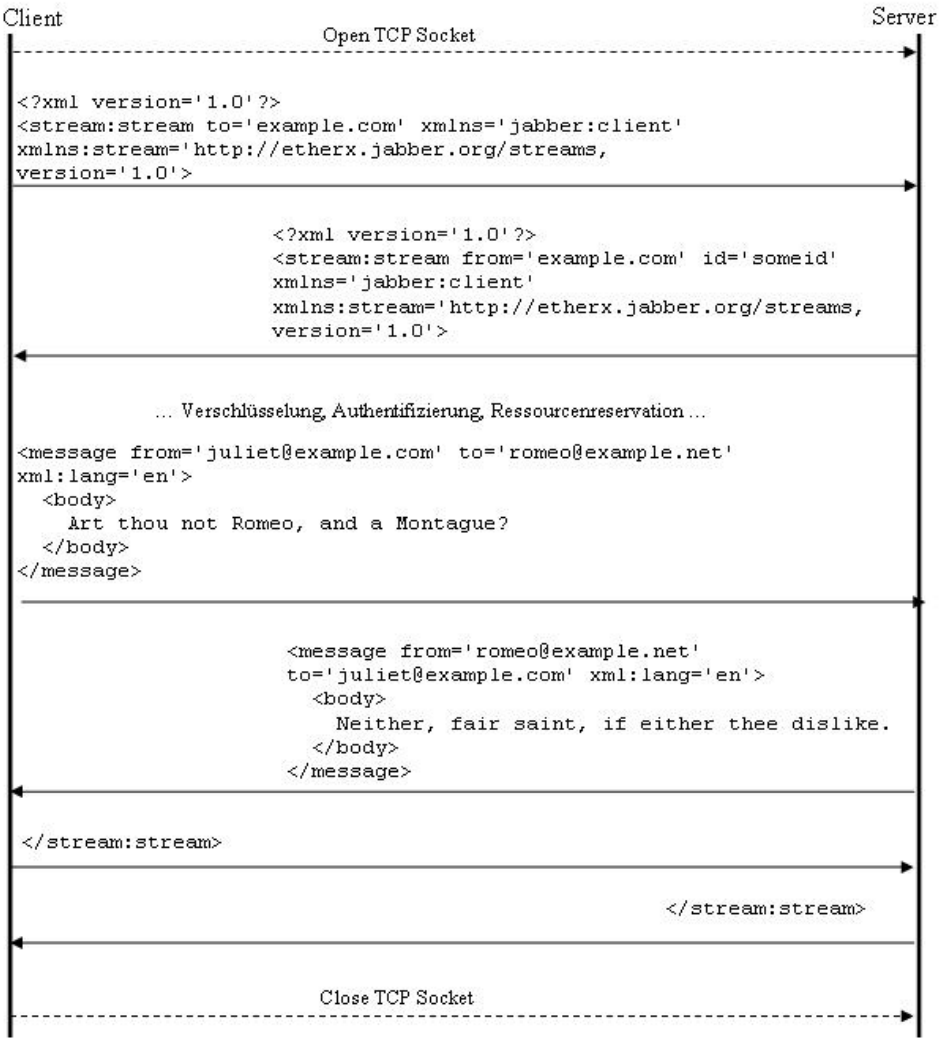



Abbildung 8.3: XMPP Verbindungsaufbau

dies zeigt nur einen kleinen Ausschnitt aus dem XMPP Protokoll. Weitere Details sind in den RFCs zu finden [30, 31, 32, 33].

Der Vergleich dieser beiden Protokolle zeigt auf den ersten Blick grosse Unterschiede in der Komplexität der Protokolle. XMPP ist durch seine XML Struktur leicht verständlich und mit heutigen Softwaremitteln leicht zu implementieren. OSCAR hingegen ist wesentlich komplexer, was ja auch durch die Tatsache unterstrichen wird, dass AOL mit TOC ebenfalls ein textbasiertes Wrapperprotokoll entwickelt hat. Weiter lässt sich für XMPP mit dem im RFC 3923 beschriebenen Verfahren relativ leicht eine End zu End Verschlüsselung implementieren und durch die verteilte Mehrserver Architektur können Informationen z. B. in Firmen komplett unter Kontrolle gehalten werden. Durch die offene Spezifikation gibt es keine ev. versteckten Sicherheitslücken (was natürlich bei der Implementation immer noch vorkommen kann). Allerdings muss man OSCAR zu gute halten, dass es weniger Datenaufkommen generiert und weniger ressourcenhungrig ist, als dies bei XML und dessen Parsing der Fall ist. Trotzdem überwiegen unserer Ansicht nach die Vorteile von XMPP.

### 8.2.2 Herausforderungen und Lösungen

In diesem Teil werden zuerst Herausforderungen im technischen Bereich betrachtet und zwar sowohl aus Sicht von Privatpersonen wie auch aus Sicht von Unternehmungen, wobei der Schwerpunk auf letzteren liegt. In einem zweiten Teil werden dann auf Basis des vorangehenden Abschnitts Lösungen gesucht.

#### Herausforderungen

Wie bereits in 8.1.2 dargestellt, stellt die Sicherheit eine der grössten Herausforderungen dar. Grundsätzlich bestehen bei IM die gleichen Gefahren, wie bei Email mit dem grossen Unterschied, dass sich bei IM einerseits die Benutzer der Gefahr viel weniger bewusst sind und andererseits durch die nahezu Echtzeitkommunikation alles viel schneller abläuft. Ein Beispiel: Es meldet sich per IM jemand vom Helpdesk und verlangt das IM Passwort, weil ein Server defekt ist. Passiert das mit Email, so sind sich heute viele Nutzer bewusst, dass hinter solchen Anfragen selten Wohlwollen steckt. Im interaktiven Gespräch ist es aber viel schwieriger, sich solcher Aktionen zu widersetzen, zumal der Angreifer ja auf etwaige Zweifel direkt Bezug nehmen kann. Ein anderes Beispiel betrifft Viren. Bei Email vergeht viel mehr Zeit, bis eine gross Anzahl von Nutzern erreicht ist als das bei IM der Fall ist, wo zu jedem Zeitpunkt Hunderttausende von Nutzern online sind. Dies ist bei Sicherheitslücken in den Clients im vergleich zu Email besonders gravierend, ist doch denkbar, dass sich so Viren oder Würmer innerhalb von Sekunden verbreiten.

Für den privaten Benutzer sind, vorausgesetzt er gibt nicht gerade sein Bankinformationen preis, solche Attacken zwar äusserst ärgerlich, aber selten existentiell. Für Firmen sieht die Situation anders aus. Diese sind sich von der technischen Seite her der Gefahren sehr wohl bewusst und haben für Email und Web ausgefeilte Sicherheitsmassnahmen mit Firewalls, Proxies mit Inhaltsfiltern, Mailservern mit Virenscannern und Intrusion Detection Systemen vorgesorgt. All dies nützt bei IM allerdings wenig, weil sich heute am meisten verbreiteten Clients der grossen Anbieter um „benutzerfreundlich“ zu sein diverse Tricks einfallen lassen um an Firewalls und Proxies vorbei zu ihren zentralen Servern und somit zu ihrem IM Netz zu kommen.

So können die meisten Clients ihr Protokoll über http tunneln und somit die Firewall umgehen. Ist dann ein http Proxy im Einsatz, so verfügen fast alle Clients über die nötigen Einstellungen um auch über den Proxy Verbindung aufnehmen zu können. Einige suchen sogar nach automatischen Proxykonfigurationsfiles oder schauen sich die Konfiguration am Browser ab. Dies macht es für Virenscanner und Proxies schwierig, den Datenverkehr zu überwachen. [34].

Eine weitere Gefahr besteht im Inhalt der Nachrichten. Der private Benutzer kann selber entscheiden, welche seiner Informationen er preisgibt und ob er will, dass die halbe Welt sieht, ob er online ist. Auch dies kann wiederum ärgerliche, aber selten existenzielle Folgen haben. Für Firmen präsentiert sich die Situation auch hier anders. So sind Geschäftsgeheimnisse durch IM akut gefährdet, weil auch in diesem Falle klassische technische Massnahmen nicht greifen und weil weiter bei zentralen Einserver Architekturen aus Nachrichten an das nächste Stockwerk meist unverschlüsselt über den Server des IM

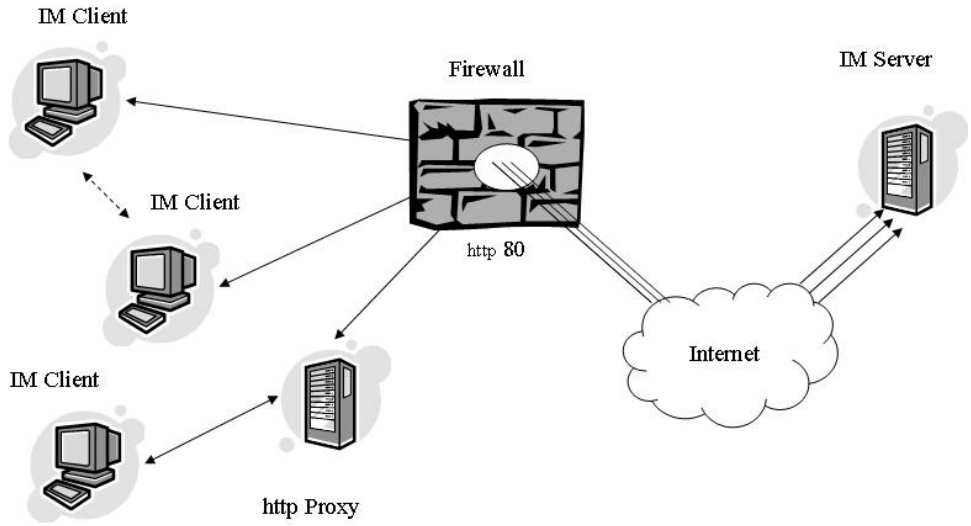



Abbildung 8.4: IM Clients im Unternehmen nach [34]

Netzbetreibers laufen. Und selbst wenn sie verschlüsselt sind, bleibt bei proprietären Protokollen nichts anderes übrig als dem Anbieter zu vertrauen. Neben der Vertraulichkeit ist die Firma auch bei der Authentizität vollständig auf den externen Anbieter angewiesen, da sie im Gegensatz zu den eigenen Mailservern keinen Einfluss auf die Authentisierung der Nutzer und somit auf deren zuverlässige Identität nehmen kann. Bei den Präsenzinformation beseht für alle Mitarbeiter ein Risiko, in ihrer Privatsphäre beeinträchtigt zu werden, zum Beispiel durch Überwachung durch die Vorgesetzten. Aber auch für die Firma besteht aufgrund der potentiell global sichtbaren Präsenz ihrer Mitarbeiter eine Gefahr, liefert doch diese Information einen guten Angriffspunkt für Social Engineering mit dem Ziel, der Firma zu schaden.

Eine Herausforderung, die sich bei privaten Nutzern nicht stellt, ist die aufgrund verschiedener regulatorischer Vorschriften wie den Sarbanes Oxley Act oder Basel II sich ständig verschärfende Aufbewahrungspflicht für diverse Informationen, insbesondere Kommunikationsdaten. Im Falle von IM nützt die ganze teure Emailarchivierung nichts, wenn sich der IM Client daran vorbeitunnelt. Ebenso sieht es mit der Verfügbarkeit aus. Wenn eine Unternehmung ein System produktiv einsetzen will, sind die Anforderungen an die Verfügbarkeit meist höher als bei privaten Nutzern. Die grossen IM Netzwerke mit Einserver Architektur sind aber primär für private Nutzer ausgelegt und die Firmen sind den Betreibern komplett ausgeliefert und können bei den bestehenden Angeboten sich nicht einmal über Service Level Agreements absichern.

Die meisten dieser technischen Probleme werden durch den Einsatz von Multiprotokoll Clients noch verschärft, da diese die proprietären Protokolle kaum 100% korrekt implementieren dürften.

### Mögliche Lösungen

Eigentlich alle angesprochenen Herausforderungen lassen sich mit den erwähnten offenen Protokollen oder doch zumindest mit ihrer Weiterentwicklung meistern. Der zentralste

Punkt liegt in der Mehrserver Architektur von XMPP und SIMPLE. Dadurch, dass der Server, der die Authentifizierung vornimmt, die Präsenzinformation verwaltet und die Nachrichten weiterleitet, im Einflussbereich der Firma stehen kann, lassen sich die Probleme mit der internen Vertraulichkeit, der Authentizität wenigstens Firmen intern und alle Probleme, die durch das Tunneln der Daten entstehen, lösen. Sowohl die Firma wie auch ihre Mitarbeiter müssen jetzt primär ihren Administratoren vertrauen, bzw. können diese auch kontrollieren. Durch die Offenheit der Protokolle lassen sich die Verfahren prinzipiell überprüfen und es ist möglich, Gateways einzurichten, die die Daten die die Unternehmung verlassen oder erreichen, auf ihren Inhalt zu prüfen.

Für die Interoperabilität zu den proprietären Produkten können die offenen Standards alleine zwar nichts beitragen aber die potentiell fehlerhafte Umsetzung auf die proprietären Protokolle kann zentral und in kontrolliertem Rahmen auf dem firmeneigenen Gateway passieren. Auf diese Art können mittels geordneter Archivierung auch die Anforderungen der Regulierungsbehörden erfüllt werden. End-zu-End-Verschlüsselung ist problemlos realisierbar auch wenn sich für die Authentisierung und den Schlüsseltausch bzw. eine Private Public Key Infrastruktur die gleichen Probleme wie bei Email stellen.

Für alle Gefahren, die sich aufgrund des mangelnden Bewussteins der Benutzer sowie durch die Unterschiede in der Wahrnehmung von Email und IM ergeben, sehen wir keine technische Lösung. Auch die Gefahr durch Social Engineering lässt sich nicht mit einem Protokoll lösen. Dazu braucht es interne Sicherheitsrichtlinien und eine fundierte Schulung und Sensibilisierung der Mitarbeitenden wie dies in anderen Bereichen auch üblich ist.

### 8.2.3 Trends

In diesem Teil werden mögliche Trends diskutiert und ihre technische Umsetzung kurz beleuchtet. Zum einen werden die verschiedenen Möglichkeiten im Zusammenhang mit der Mobilkommunikation behandelt, zum anderen die im vorherigen Teil angesprochenen Lösungen zur Integration von IM an zwei konkreten Produkten kurz besprochen.

Wenn sich, wie wir erwarten, IM in Unternehmen durchsetzt, so wird es sicher ein grosses Bedürfnis geben, IM auch unterwegs zu nutzen, also auf dem Mobiltelefon. Dies ist zwar heute bereits Möglich, gibt es doch Clients von Yahoo [21] und Microsoft [26] für Handys. Auch Multiprotokoll Clients zum Beispiel für das Mobile Betriebssysemm Symbian [35] sind erhältlich. Weiter besteht die Möglichkeit, beispielsweise bei Yahoo via SMS am IM teilzuhaben oder mit dem in immer mehr Mobiltelefonen enthaltenen Browser. Diese Möglichkeiten werden jedoch v. a. im privaten aber auch im geschäftlichen Bereich stark von dem Verhalten der Service Provider beeinflusst. Siehe dazu 8.2.4.

Eine weitere Möglichkeit, Nachrichten ohne Zeitverzögerung auf das Mobiltelefon zugestellt zu erhalten, ist das sogenannte Push-Email. Für den Sender einer Nachricht läuft alles genau gleich wie bei einer normalen Email. Wenn der Empfänger keine spezielle Adresse benutzt, merkt er nicht einmal, dass es sich um eine Push-Email Nachricht handelt. Auf der Empfängerseite besteht der Unterschied darin, dass der Client des Empfängers nicht beim Server nachfragen muss, ob neue Emails vorhanden sind, sondern der Server dem registrierten Client meldet, wenn eine Nachricht ankommt und sie auch gleich zustellt.

So kann Email eigentlich wie Instant Messaging genutzt werden. Bei uns ist Push-Email noch nicht stark verbreitet, die Chancen stehen aber gut, dass es auch bei uns grössere Verbreitung findet.

Ein weiterer Trend im mobilen Bereich ist das sogenannte Push-to-Talk over Cellular (PoC). Bei PoC werden, wie der Name sagt, Sprachdaten auf Knopfdruck über einen Paketservice wie GPRS an einen oder mehrere Teilnehmer übertragen. Dabei handelt es sich um eine Halbduplexverbindung, weshalb während dem Sprechen auch der Knopf gedrückt werden muss. Damit lässt sich ein Mobiltelefon also wie ein Walkie Talkie benutzen. PoC ist ein Standard der OMA [42]. Es ist denkbar, dass PoC die Alternative zum mobilen IM wird, da v. a. im Geschäftsumfeld die heutigen Handytastaturen als umständlich empfunden werden. Allerdings müsste man dann das Problem lösen, wenn mobile mit nicht mobilen Teilnehmern kommunizieren wollen. Denkbar wäre eine Übersetzung von Text in Sprache und umgekehrt. Dabei müsste die Umwandlung von Sprache in Text aus Performancegründen wahrscheinlich auf der Serverseite geschehen. Heute ist PoC zwar mit fast allen Handys der neuesten Generation möglich, wird aber von den wenigsten Serviceanbietern unterstützt. Auch eine Integration in Lösungen für Firmen oder eine Umsetzung der angesprochenen Umwandlung von Sprache zu Text ist uns nicht bekannt.

Ein weiterer Trend ist die zunehmende Integration von verschiedenen Kommunikationsservices in die bestehenden IM Applikationen wie Videokonferenz, die Möglichkeit, gemeinsam Dokumente zu bearbeiten [38], Ink Notes [26], eine Möglichkeit Notizen von einem Touch Screen zu versenden, die Kombination von IM und Voice over IP (VOIP) [39] usw. Die meisten dieser Möglichkeiten bieten sich zurzeit in Bereich der privaten Nutzung, werden aber sicher auch das geschäftliche Umfeld erreichen. In Unternehmungen wird zudem die Integration von längst bestehenden Groupwarelösungen mit IM ähnlich weit gehen wie vor einiger Zeit die Integration von Adressammlung, Email und Kalender.

### Technologien und Produkte zu den Trends

Das in 8.2.1 bereits erwähnte IMPS ermöglicht IM Dienste bereits heute auf den Mobiltelefonen und wird rege weiterentwickelt. Abbildung 8.5 zeigt seine Architektur.

Auch die Architektur von IMPS ist eine dezentrale Mehrserver Architektur und auch sie beinhaltet ein Gateway zu anderen potentiell auch proprietären Protokollen. Mit IMPS ist volle IM Funktionalität möglich. CSP bezeichnet das Client Server Protokoll, SSP das Server Server Protokoll. Auch hier ist weitgehende Sicherheit möglich. Die für die langsamen Mobilfunkverbindungen wichtige Datenmenge ist im Vergleich zu SIMPLE je nach Szenario grösser oder kleiner. Für Details siehe [22].

Für das erwähnte Push-Email gibt es auf dem Markt verschiedene Lösungen. Für die meisten uns bekannten Systeme gilt, das sie für kleine Unternehmen teuer sind. Der bekanntest Anbieter ist Research in Motion (RIM), die ein System namens BlackBerry anbietet[36]. Dabei handelt es sich einerseits um den BlackBerry Entreprise Server, der mit Microsoft Exchange und Lotus Domino zusammenarbeitet und den Dienst bereit stellt. Andererseits bietet RIM mobile Geräte für den Empfang und Versand von Emails an. In der Zwischenzeit hat RIM ihr System auch an andere Hersteller lizenziert, so dass bspw. Nokia auch

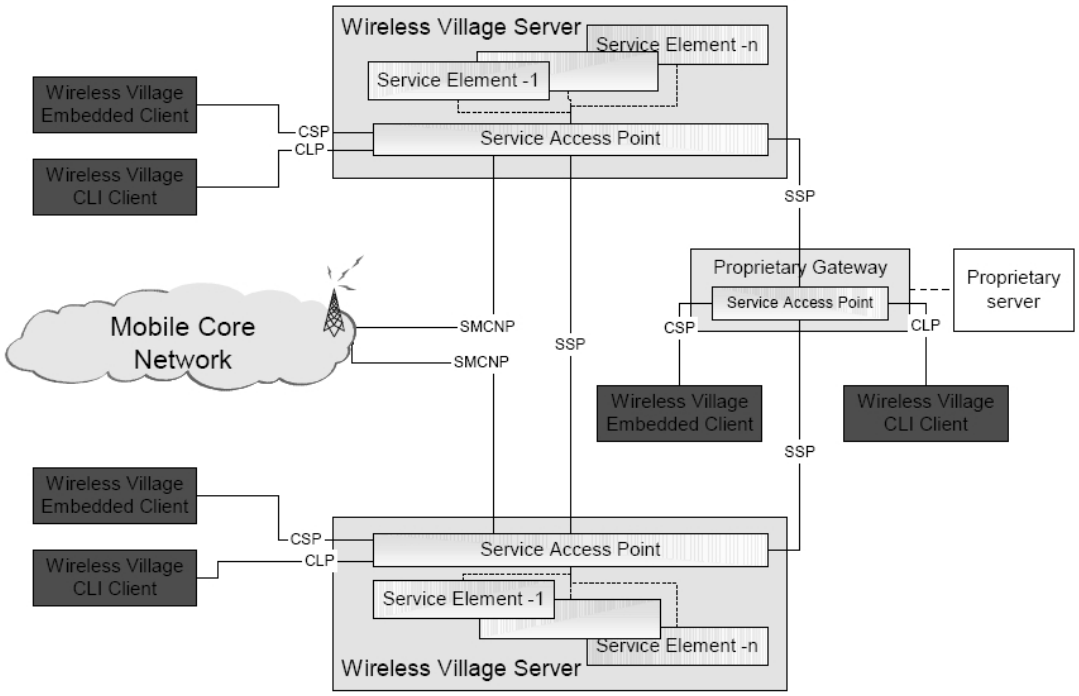



Abbildung 8.5: Architektur von Wireless Village/IMPS [40]

Handys mit BlackBerry Clients anbietet. In den Vereinigten Staaten ist der BlackBerry Dienst äusserst populär und wird auch intensiv von Regierungsstellen benutzt. Eine kürzliche Diskussion um eine Einstellung des Services aufgrund von Patentsteitigkeiten machte dies deutlich [37]. Die Firma Sonyericsson bietet in einigen Handys auch die Möglichkeit, Push-Email mit dem im IMAP Protokoll vorhandenen IDLE Befehl zu nutzen [43].

Zu den im vorhergehenden Abschnitt und unter 8.2.2 diskutierten Lösungen sind wir auf folgende Produkte gestossen. Einerseits der Live Communication Server 2005 (LCS) von Microsoft [17] und andererseits auf IMB Lotus Samtime 7.5. Der LCS basiert auf SIP/SIMPLE und integriert sich natürlich nur mit Microsoft Produkten sehr stark in bestehende Umgebungen mit Email, Push-Email, Groupware, in Form von MS Exchange, File- und Collaborationserver in Form von MS Sharepoint, Directoryserver zur sicheren Authentifikation mit MS ActiveDirectory usw. Letztendlich sind fast alle von Microsoft verfügbaren Kommunikations- und Kollaborationsprodukte integriert und ermöglichen ein hoch integriertes Arbeiten mit einem offenen Protokoll und einer Mehrserverarchitektur mit ausgereiften Sicherheitsfeatures. Natürlich wird auch diese Lösung ihre Tücken haben, insbesondere ist die Gefahr von Implementationsfehlern bei so hoch integrierten Produkten nicht zu vernachlässigen. Aber vom Lösungsansatz her entspricht der LCS weitgehend den vorhin vorgestellten Lösungen.

IBMs Sametime 7.5 bietet ebenfalls weitgehende Integration der verschiedenen Serverprodukte um Lotus Domino. Besonders erwähnenswert ist das für Ende 2006 angekündigte Real Time Collaboration (RTC) Gateway, dessen Architektur in Abb. 8.6 dargestellt ist.

Die Architektur des Gateways folgt einer einfachen Plugin Architektur mit Konnektoren für die verschiedenen Protokolle wie VP (proprietäres Protokoll von Lotus Sametime),

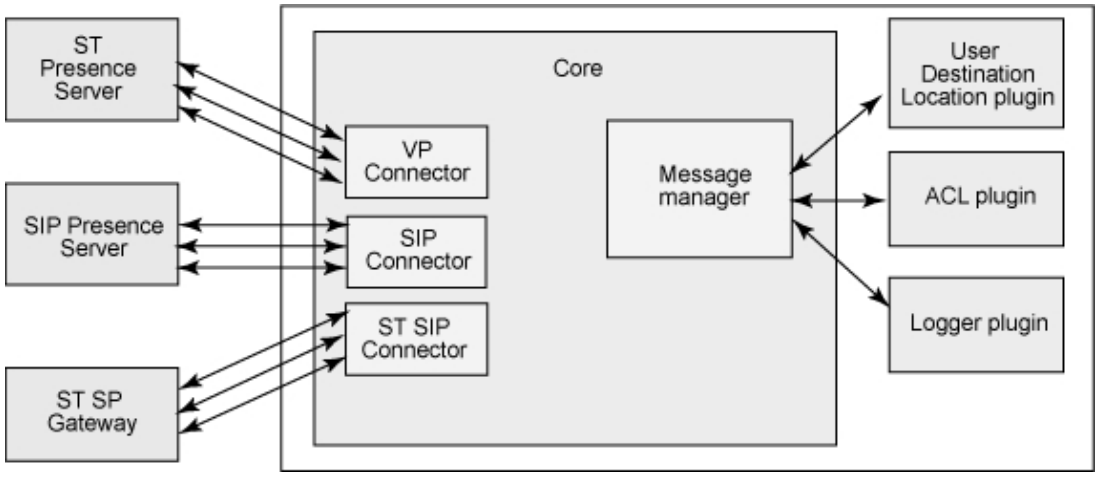



Abbildung 8.6: Architektur des Lotus RTC Gateways [18]

SIP, und potentiell vielen weiteren Protokollen wie SIMPLE, XMPP, MSNP, OSCAR etc. Daneben existiert im Kern ein Nachrichten Manager, der Plugins für Zugriffkontrolle (ACL), Archivierung/Logging und Routing enthält und einfach erweiterbar ist. Das alles setzt auf einem Applikationsserver auf. Die Idee dabei ist, dass es nicht nur innerhalb der Firma zuverlässige IM Services braucht, die die zuvor diskutierten Kriterien erfüllen sondern auch Konnektivität nach ausserhalb der Firma braucht, ohne diese Eigenschaften zu verlieren. Natürlich sind das bisher nur Marketinginformationen, da das Gateway noch gar nicht erhältlich ist und die Realität präsentiert sich dann oftmals nicht ganz so umfangreich. Allerdings gilt auch hier, dass der Architekturansatz und die Verwendung von Konnektoren zu den offenen Standardprotokollen in die richtige Richtung weisen.

### 8.2.4 Akzeptanz

In diesem Teil wird ganz kurz auf die Problematik der Akzeptanz neuer Technologien und Services bei den Benutzern eingegangen. Der Schwerpunkt aber stellt die Diskussion um die Akzeptanz der neuen Standards und Services bei den Softwareproduzenten und Serviceprovidern.

#### Akzeptanz bei den Benutzern

Benutzer v. a. im meistens auf Sicherheit und Kontinuität bedachten Firmenalltag üben meistens Zurückhaltung, wenn es um neue Informations- und Kommunikationstechnologien (IKT) geht (hierbei wird nicht an innovationsfeindliche Mitarbeitende gedacht, aber es gibt nur verhältnismässig wenige Leute, die zur Aufgabe haben, in einer nicht zur IKT gehörenden Firma, sich den ganzen Tag mit Innovationen im Bereich der IKT zu beschäftigen). Es überwiegt Unsicherheit und Skepsis. Um dem vorzubeugen ist es extrem wichtig, dass nur ausgereifte Produkte zum Einsatz kommen und die Business Prozesse vorher auf einen geeigneten Einsatz analysiert worden sind. Dabei muss auch immer die Möglichkeit bestehen, dass die Analyse zum Schluss führt, IKT in einem Bereich nicht

einzusetzen. Wenn es dann gelingt, mit richtigem Einsatz am richtigen Ort die Benutzer zu begeistern und die Prozesse sinnvoll zu unterstützen, wird sich bald niemand mehr vorstellen können, wie die Arbeit vorher ohne möglich war.

#### Akzeptanz bei Herstellern und Serviceprovidern

Bei Firmen aus dem IKT würde man auf den ersten Blick eigentlich keine Skepsis gegenüber den innovativen IKT vermuten. Allerdings zeigt ein Blick auf den Markt dass nach wie vor viele Standards nicht unterstützt werden. So gibt es nur wenige Mobilfunkanbieter, die IMPS unterstützen, obschon ein Grossteil der heutigen Mobiltelefone mit entsprechenden Applikationen ausgerüstet sind. Erst kürzlich haben einige grosse Mobilfunkanbieter beschlossen, IMPS nun endlich stärker voranzutreiben um der immer stärkeren Ausbreitung von kostenlosen IM Applikationen wie AIM, Yahoo und MSN entgegenzutreten [41]. In diesem Fall scheint es zumindest nicht ganz abwegig zu vermuten, dass IMPS lange nicht unterstützt wurde um das blühende Geschäft mit SMS nicht zu kannibalisieren. In eine ähnliche Richtung weist die Tatsache, dass es bis vor kurzem kaum Handys gab, deren Mail Clients Fotos als Attachment versenden konnten. Die Mobilfunkanbieter wollten sich wahrscheinlich das Geschäft mit MMS nicht vermiesen.

Eine ähnliche Tendenz zeigt sich darin, dass es keine ernsthaften Anstrengungen gibt, die proprietären Protokolle der grossen IM Anbieter zu integrieren. AOL hat zwar Anfangs 2006 eine Bibliothek für die Entwicklung eigener IM Clients freigegeben, allerdings verbieten die Lizenzbedingungen explizit Multiprotokollclients und mit einer harten Registrierpflicht und Signatur der Bibliothek will AOL dies offensichtlich auch durchsetzen. Alle drei grossen, AOL, Yahoo und MSN treten immer noch als Portalbetreiber auf und wollen ihren IM Nutzern möglichst viele Services aber auch Werbung bieten und die Nutzer unbedingt an ihr Portal binden. Auf diesem Hintergrund ist es fraglich, wie schnell die durchaus durchdachten offenen Standards grosse Verbreitung finden.

### 8.2.5 Zukünftige Entwicklung

Aufgrund der angesprochenen Trends scheint klar, dass sich IM weiterentwickelt und zwar in zwei Richtungen: Zum einen werden mobile Anwendungen zunehmen, zum anderen wird die Integration von neuen Services in IM Clients fortschreiten und durch die Integration von IM in Unternehmenslösungen werden neue Anwendungsszenarien für IM entstehen.

Für die mobilen Anwendungen ist mit IMPS ein Standard vorhanden und es gibt, wenn auch vornehmlich auf proprietären Protokollen beruhend, bereits etablierte Lösungen. Eine gute Chance sehen wir für Push-Email, da Email bestens etabliert ist und Unternehmen nicht auf Serviceprovider angewiesen sind, um diesen Service zu nutzen. Für die weiter gehenden Ansätze von mobilem IM wie der Sprachumsetzung, die wir vorschlagen, wird sich erst noch zeigen müssen, ob sie sich durchsetzen. Auch sind die Technologien hierzu zwar grundsätzlich vorhanden, es gibt aber noch keine Standards. Wie dargelegt, werden die Serviceprovider bei solchen Entwicklungen eine wichtige Rolle spielen, weil sie den mobilen Teil des Netzwerks kontrollieren.

Für die Integration zusätzlicher Services wie Videochat und Voicechat sind die Technologien und Protokolle vorhanden, sowohl im proprietären wie auch im offenen Bereich. Hier besteht die Herausforderung hauptsächlich in der Kombination der verschiedenen Standards und, auch wenn die nicht im Interesse aller Anbieter liegt, in der Interoperabilität, sowohl für die bestehenden wie auch für die neuen Services. Gerade der letztgenannte Punkt dürfte schwierig zu lösen sein, da sich durch die Vielfalt der Protokolle eine grössere Zahl von Kombinationsmöglichkeiten ergibt, welche dem Ziel der Interoperabilität nicht zuträglich ist. Bei der Integration in Unternehmenslösungen sind v. a. die bereits etablierten Anbieter gefragt, da kaum ein Unternehmen bereit sein wird, seine ganze Infrastruktur umzustellen, nur um eine neue, integrierte IM Lösung zu erhalten. Da die meisten der etablierten Unternehmenslösungen nicht auf Open Source Software beruhen dürfte es für Drittanbieter schwierig sein, eine weit gehend Integrierte IM Lösung für bestehende Systeme anzubieten. Trotzdem erleichtern natürlich die offenen IM Standards, allen voran SIMPLE die Interoperabilität zwischen verschiedenen Anbietern, da sich mit SIP grundsätzlich Sitzungen für diverse Services verwalten lassen. Auch wenn bei Unternehmen ein grosser Teil des Nutzens aus der internen Integration gezogen werden kann, wird auch hier die Interoperabilität eine der grössten Herausforderungen werden. Zusammenfassend kann gesagt werden, dass die technologische Basis auch für zukünftige Services brauchbar ist, und die grossen Herausforderungen in der Interoperabilität und der Etablierung der Services liegen werden.

## 8.3 Instant Messaging im Geschäftsumfeld

Das folgende Kapitel behandelt den Einsatz von IM in Unternehmungen. Zu Beginn wird der Umgang unter IM Anwendern betrachtet. Danach werden die Einsatzmöglichkeiten von IM aufgezeigt und die Anforderungen, gegliedert in technische Anforderungen, Benutzeranforderungen und organisatorische Anforderungen, formuliert.

### 8.3.1 Umgang unter Anwender

Der Tenor von IM Nachrichten ist meistens umgänglich, informal und freundlich. Häufig wird die Gross-Kleinschreibung zu Gunsten schnellerem Schreibens vernachlässigt und wichtige Aussagen mit mehreren Ausrufezeichen, z.B „You got it!!!“, unterstrichen, dazu später mehr. IM wird mehr als nützliche Spielerei angeschaut und Email als der grosse, ernsthaftere Bruder des IM. Das kommt daher, dass IM eine interaktive Kommunikation erlaubt, weil Antworten wie bei einem Gespräch nur wenig Zeit verzögert eintreffen. Email erinnert mehr an Briefe schreiben, darum wird bei Email auch mehr auf Förmlichkeiten geachtet.Ein weiterer Grund für den informalen Charakter von IM Sitzungen, ist dass die Gesprächspartner meist bekannt sind. Die Freundesliste eines Angestellten (Buddylist) besteht für gewöhnlich aus ungefähr 22 Kontakten. Darunter 16 Mitarbeiter und 6 Familienangehörige. Regelmässigen Kontakt pflegt der Angestellte aber nur mit 5 bis 6 Kontakten[11].

Das folgende Zitat zeigt einen Auszug aus einem Dialog über IM zwischen der Sekretärin Melissa und dem Manager Alan. Man kann erkennen, dass Aussagen zum Teil durch mehrere aufeinander folgende Ausrufezeichen untermalen wird (siehe Zeile 11). Dies dient dazu, Emotionen in den Text einfliessen zu lassen und somit die Unterhaltung persönlicher zu gestalten. Analog zu den Aussagen, können Fragen mit mehreren Fragezeichen hervorgehoben werden (siehe Zeile 1). Eine weitere effiziente Möglichkeit zum übertragen von Emotionen ist die Verwendung von emoticons (siehe Zeile 27).

1 melissa (8:33:32 AM): The fire is out???????? [there has been
2 an embarrassing public relations problem]
3 Auto response from alan: (8:33:32 AM): I'm idle...may be
4 asleep. [Alan was there but working on another computer. The
5 message was a personalized automatic response.]
6 alan (8:33:45 AM): not quite...still putting it out
7 melissa (8:37:13 AM): I can send some water. Just talked with
8 Georgina....Marsha is running around with her head cut off!!!!!
9 alan (8:37:29 AM): jut put Carl on my calendar at 10 am, for
10 half-hour. [Carl was able to help solve the problem.]
11 melissa (8:37:45 AM): You got it!!!!!
12 melissa (8:38:43 AM): By the way....I can go to lunch if I can
13 catch a ride with you...Beth has the car for lnch.
14 alan (8:38:56 AM): fine with me!
15 alan (8:39:12 AM): also, do you know when will sam jones be
16 back?
17 [Melissa turned to Jackie who kept Sam's calendar and asked her
18 about Sam's schedule.]
19 melissa (8:40:39 AM): Sam will be coming in on June 1 as of this
20 moment
21 alan (8:40:56 AM): oh...not here this fri, eh?
22 melissa (8:41:11 AM): NO....He is in Hawaii at the moment.
23 alan (8:41:24 AM): right...for the shareholders meeting.
24 melissa (8:42:09 AM): You got it...Making Gail crazy needing
25 paperwork from Stan's group yesterday at 4pm and they are out
26 on an Offsite....
27 alan (8:42:34 AM): :-)

Abbildung 8.7: Auszug IM Sitzung [11]

### 8.3.2 Einsatzmöglichkeiten und zukünftige Szenarien für unternehmensweite Kommunikation

IM eignet sich unter anderem besonders für kurze Fragen und Verdeutlichungen. Das soll anhand von folgendem Beispiel aufgezeigt werden.

Helen ist eine Websitedesignerin und muss häufig im Auftrag ihrer Kunden an bereits erstellten Websites Änderungen vornehmen. Bei diesem Vorgang stellen sich Helen viele

Detailfragen, weil sie die Website genau nach den Vorstellungen des Auftraggebers erstellen muss. IM eignet sich in diesem Fall in besonders hohem Mass, weil sie bei Fragen bezüglich Layout der Website, vorausgesetzt der gewünschte Kommunikationspartner ist online, sofort eine Antwort bekommt. Sie nimmt dann die Änderungen vor und fordert den Kunden wieder über IM auf diese zu begutachten. Bei Nichtgefallen kommen die weiteren Änderungswünsche wiederum kaum zeit verzögert bei Helen an. IM ermöglicht in diesem Szenario eine wesentlich effizientere Arbeitsweise als es zum Beispiel Email kann. Hätte Helen dem Kunden per Email mitgeteilt, dass die ersten Änderungen vorgenommen wurden und der Kunde erst am nächsten Morgen wieder seine Emails beantwortet hätte, hätte sich der ganze Vorgang um mehrere Tage verzögert [11].

Die kurze Zeitverzögerung, mit der die Nachricht beim Kommunikationspartner eintrifft, ist auch für die nächste Einsatzmöglichkeit von zentraler Bedeutung. Koordination und Terminvereinbarung profitieren enorm von einer schnellen Einigung bezüglich eines Datums, das allen betroffenen passt. Per IM kommt eine Absage oder Zusage innerhalb kürzester Zeit (Sekunden bis Minuten) zurück. Eine Email wird wahrscheinlich nur ein paar Stunden bis einen Tag später gelesen und beantwortet, was den Prozess massiv verlangsamt. IM ist im günstigen Fall sogar schneller als eine Terminvereinbarung per Telefon. Angenommen der gewünschte Kontakt ist im IM verfügbar, die Frage für einen Termin lautet:“Hallo Peter, hast du am Fr, 1.6. um 14.00 Zeit für ein Meeting im Büro 315?“ Die Antwort nach ca. 5 Sekunden lautet:“Ja“.

Der Inhalt einer IM Nachricht kann sehr vielfältig sein. Von Fragen über Antworten bis zu Bestätigungen ist alles Möglich. Auch die Delegation von Aufgaben an Mitarbeiter ist eine Einsatzmöglichkeit von IM.

Der heutige Arbeitsdruck erschwert das socialising innerhalb des Unternehmens, ist aber nach wie vor von grosser Bedeutung um ein produktives Arbeitsklima zu erhalten. Mitarbeiter benutzen IM um sich zum Mittagessen oder für die Kaffeepause zu verabreden. Vorher geschah dies in einem kurzen Gespräch. Die Unmittelbarkeit von IM reduziert wiederum den Organisationsaufwand auf ein absolutes Minimum.

Wie bereits erwähnt, sind in einer Freundesliste nicht nur Arbeitskollegen und Kunden vorzufinden, sondern auch Familienangehörige. Die Auswertung einer Umfrage von Nardi B., Whittaker S. and Bradner E. (2000)[11] hat gezeigt, dass sich die Kommunikation der Mitarbeiter mit deren Familienangehörigen in den meisten Fällen auf ein kurzes „Hallo, Liebling“ oder ähnlich beschränkt. Solche kurzen Mitteilungen sind wie eine kurze Verschnaufpause zu verstehen und geben dem Mitarbeiter Kraft für neue Aufgaben.

Die aufgezeigten Möglichkeiten verdeutlichen den flexiblen Einsatz von IM. IM wird für kurze Fragen und Verdeutlichungen, Koordination und Terminvereinbarung, Delegation von Aufgaben an Mitarbeiter, socialising und Kommunikation mit Familienangehörigen benutzt. Also hauptsächlich kollaborative Arbeit. IM wird aber auch benutzt um das Arbeitsklima zu verbessern. Zu den ernsthaften Einsatzmöglichkeiten gesellen sich auch Witze und lockere Sprüche, die einem guten Arbeitsklima dienlich sind.

IM Systeme für den privaten Einsatz unterstützen je länger je mehr Audio und Videoübertragung. Der Vorteil ist nicht von der Hand zu weisen, gibt es doch viele Situationen, in

denen ein kurzes Gespräch deutlicher und verständlicher ist als eine Textnachricht. Mit Videoübertragung ist es zusätzlich möglich das Gespräch mit Gesten und Gesichtsausdrücken zu untermalen. Das ist ein nicht zu vernachlässigender Punkt bezüglich Verständlichkeit der Mitteilung. Computer an modernen Arbeitsplätzen sind bereits mit Mikrophon und Videokamera ausgerüstet. Es wird also nur eine Frage der Zeit sein, bis sich Audio und Videoübertragung auch in Business IM Systemen durchsetzen wird.

### 8.3.3 Anforderungen

Die technischen Anforderungen und die Benutzeranforderungen / organisatorischen Anforderungen beeinflussen sich gegenseitig. Was der Benutzer von einem IM System erwartet und erwarten kann, hängt von der technischen Umsetzbarkeit der Benutzeranforderungen / organisatorischen Anforderungen ab. Die technische Umsetzbarkeit hängt wiederum von den Anforderungen ab. Das folgende Kapitel ist unterteilt in die Unterkapitel technische Anforderungen und Benutzeranforderungen / organisatorischen Anforderungen. Weil sich diese Arbeit aber insbesondere mit IM Systemen für Organisationen befasst, ist ein weiteres Unterkapitel den spezifischen Anforderungen von Organisationen an IM Systeme gewidmet.

#### Technische Anforderungen

Adminstratoren stellen besondere Anforderungen an ein IM System. Das System muss, damit es gewartet und überwacht werden kann, die Möglichkeit bieten Kommunikationspfade von Innen nach Aussen und umgekehrt aufzuzeichnen. Meistens laufen die gesamten IM Vorgänge über einen Proxyserver ab, welcher dann den erfolgten Verkehr in ein Logfile schreibt, das auf Unregelmässigkeiten überprüft werden kann. Über den Proxyserver wollen die Administratoren auch ihre durchsetzten können. Ein Administrator will zum Beispiel keinen Dateitransfer zwischen den IM Clients erlauben. Durch Einstellungen auf dem Proxyserver kann er das verhindern. In den Richtlinien kann auch festgelegt werden, wer IM benutzen darf und welche Clients die Anwender benutzen dürfen [10].

In Unternehmen ist es wichtig, dass Kommunikationsvorgänge aufgezeichnet werden können. Finanzinstitute sind sogar von Gesetztes wegen dazu verpflichtet. Ein Enterprise IM System sollte also in der Lage sein, alle Nachrichten, die das System empfangen und verschickt hat, auszugeben.

Die ersten IM Systeme für Privatanwender übermittelten Nachrichten im Klartext. Der Sicherheit wurde also keine Beachtung geschenkt. Die Anforderungen an ein Enterprise IM System bezüglich Sicherheit sind hoch. Die Schnittstelle zur Aussenwelt soll keine Schlupflöcher für Angreifer enthalten und doch die Benutzbarkeit nicht einschränken. Des weiteren sollen die Nachrichten verschlüsselt übermittelt werden, damit sie nicht durch Dritte gelesen werden können. Die Authentifizierung der Benutzer muss ebenfalls durch aktuelle Sicherheitsverfahren vorgenommen werden. Denkbar sind digitale Zertifikate und das public/private Key Verfahren.

Wie bereits erwähnt, gibt es mehrere Anbieter von Enterprise IM Systemen. Innerhalb eines Unternehmens ist die Kompatibilität mit hoher Wahrscheinlichkeit sichergestellt, da ein Unternehmen intern kaum 2 verschiedene Systeme einsetzen wird. Will das Unternehmen aber über IM mit anderen Unternehmen kommunizieren, ist die Interoperabilität zwischen den in den Unternehmen eingesetzten Enterprise IM Systemen von zentraler Bedeutung. Die Interoperabilität der IM Systeme für die private Verwendung war bisher schlecht. Zu Beginn waren die Systeme der grossen Anbieter (AOL, Microsoft,Yahoo) nicht kompatibel zueinander, weil jeder ein proprietäres Verfahren einsetzte um die Benutzer an das eigene System zu binden. Der parallele Betrieb von zwei oder sogar drei Clients um die Freunde und Bekannten in unterschiedlichen Netzwerken zu erreichen, war nicht aussergewöhnlich. In einer Unternehmung ist das nicht denkbar, weil der parallele Betrieb von Enterprise Systemen auf den Servern und Clients auf den Computer der Mitarbeiter den Administrationsaufwand in die Höhe treiben. Es sind Bemühungen der Internet Engineering Task Force im Gange, einen Standard für die Übermittlung von IM Nachrichten einzuführen [10]. Ein von allen eingehaltener Standard würde die sowohl die Interoperabilität zwischen IM Systemen verschiedener Anbieter vereinfachen als auch die Integration von IM in Geschäftsprozesse erleichtern. Die Integration in Geschäftsprozesse, also eine Applikations-/und Prozessintegration wird unter „Organisatorische Anforderungen“ besprochen.

In grossen Unternehmen mit vielen Mitarbeitern ist eine leistungsstarke Kommunikationsinfrastruktur nötig um das aufkommende Datenvolumen zu verarbeiten. Vor allem Audio und Videounterstützung in IM verursacht - sofern eingesetzt - einen hohen Datentransfer.

### Benutzeranforderungen

Das Grundkonzept von IM ist das Versenden von Nachrichten an Personen, welche dann auf die Nachricht eine Antwort schreiben können. Grundlegende Benutzeranforderungen sind also das Suchen und Finden von Personen im System und das Speichern der Kontaktinformationen in einer, häufig als Freundesliste bezeichneten, Liste. Somit wird das schnelle Versenden von Nachrichten an häufig gebrauchte Kontakte ermöglicht.

Ein Vorteil von IM ist die Unmittelbarkeit, mit der eine Meldung bei einem Kommunikationspartner eintrifft und gegebenenfalls auch beantwortet wird. Gängige IM Systeme melden eine eingehende Nachricht, je nach Einstellungen, grafisch und akustisch dem Empfänger. Das hat sowohl Vor- als auch Nachteile. Die Vorteile liegen auf der Hand: der Empfänger weiss, dass eine neue Nachricht eingegangen ist und kann diese, ganz im Sinne des Verwendungszweckes eines IM Systems, prompt beantworten. Der Nachteil ist, dass dieser eigentlich nützliche Umstand den Empfänger gegebenenfalls auch stören kann. Häufige Unterbrüche können die Produktivität von besonders konzentrationsintensiven Arbeiten massiv verschlechtern. Der Nutzer muss also in der Lage sein seinen Kommunikationspartnern zu signalisieren, in was für einem Zustand er sich befindet: darf gestört werden / darf nicht gestört werden. Es ist in aktuellen IM Systemen üblich, dass Nachrichten an einen „darf nicht gestört werden“ Teilnehmer zwar ausgeliefert, der Nachrichteneingang aber weder grafisch noch akustisch gemeldet wird, so dass der Empfänger die Nachrichten später lesen kann.

Das System soll aber nicht nur Unterscheiden zwischen „darf gestört werden / darf nicht gestört werden“ sondern soll sowohl context awareness, reachability und location awareness unterstützen. Diese Funktionen sind in aktuellen IM Systemen noch nicht gänzlich vorhanden, werden aber in Prototypen untersucht und weiterentwickelt. [12]

**context awareness** Was tut der Benutzer gerade. Ist er am Telefonieren oder in einem Gespräch?

**reachability** Kann der Benutzer erreicht werden oder nicht?

**location awareness** Befindet sich der Benutzer in seinem Büro oder ist er unterwegs. Das kann für einen Arbeitskollegen eine wichtige Information sein, wenn er zum Beispiel etwas abholen möchte.

Es geht darum, dass die Kontakte möglichst viel und für sie nützliche Informationen über den gewünschten Kommunikationspartner in Erfahrung bringen können. Durch Applikationsintegration kann das System ein laufendes Telefongespräch oder ein im Gange befindlicher Termin erkennen und dem IM System als Aktiviätsinformation bereitstellen. Die nächste Version von Lotus Notes Sametime Client Lotusphere, siehe Abbildung 8.8 zeigt an, wenn ein Kontakt ein Telefongespräch führt.


Abbildung 8.8: Aktivitätsanzeige Lotus Notes Sametime

Die Abbildung 8.9 zeigt die Verfügbarkeitsoptionen, die ein Benutzer im Client setzen kann. Im „offline“ Modus kann der Benutzer nicht erreicht werden. Im „online“ Modus ist der Benutzer ohne Einschränkung erreichbar. Je nach Einstellung schaltet die Aktivitätsanzeige nach fünf Minuten ohne Benutzerinteraktion auf „Abwesend“ und nach zwanzig Minuten auf „Nicht verfügbar“. In diesen beiden Modi werden die Nachrichten jedoch genau gleich, mit Ton und grafischer Anzeige beim Empfänger angezeigt. Im „Beschäftigt“ Modus, werden die Nachrichten ausgeliefert, aber weder klanglich noch grafisch Untermalt.

Beim Einsatz von IM kann es vorkommen, dass sich der Empfänger einer Nachricht kurz vor dessen Versand beim System abmeldet, eine Störung mit der Internetverbindung auftretet oder sich ein Betriebssystemausfall ereignet. In einem solchen Fall sollen die Nachrichten nicht verloren gehen, sondern bei der nächsten Anmeldung des Empfängers an das IM System ausgeliefert werden. Diese Anforderung ist der Anforderung Nachrichten

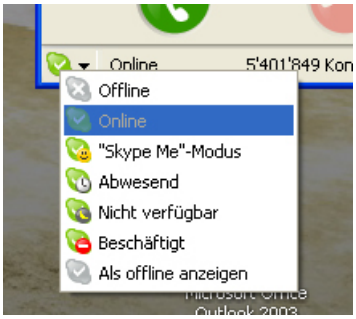



Abbildung 8.9: Verfügbarkeitsoptionen Skype

auch an Kontakte zu versenden, die gerade offline sind, ähnlich. Das Prinzip ist dasselbe: Die Nachrichten sollen bei der nächsten Anmeldung des Empfängers an das IM System ausgeliefert werden.

### Organisatorische Anforderungen

Die Anforderungen an ein IM System im Geschäftsumfeld sind umfassender als die Anforderungen, die Anwender für den privaten Einsatz an ein IM System stellen. Im weiteren wird ein IM System für Organisationen als Enterprise IM System bezeichnet.

Die grossen drei Anbieter von privaten IM Systemen AOL, Microsoft mit dem Live Communication Server 2005 und Yahoo mit dem Yahoo! Messenger haben das Potential des Einsatzes von IM in Unternehmen erkannt und bieten jeweils auch Enterprise Editionen an: AOL mit AOL Enterprise AIM Service, Microsoft mit MSN Messenger Connect for Enterprises und Yahoo mit dem Yahoo Messenger Enterprise Edition. Daneben gibt es auch weiter Enterprise IM Systeme auf dem Markt, was in diesem Zusammenhang aber nicht von Relevanz ist.

Um im heutigen Geschäftsumfeld erfolgreich sein zu können, werden in Unternehmen Prozesse integriert, automatisiert und synchronisiert um einen End-zu-end Prozess zu erhalten. IM soll in der Unternehmung also nicht ein „Inselsystem“ sein, sondern in die Applikationslandschaft integriert werden und Teil des Geschäftsprozesses werden. Denkbar ist zum Beispiel die Übernahme eines Termins mit wenigen Mausklicks in einen Terminplaner wie Microsoft Outlook mit allen nötigen Details wie teilnehmende Personen, Ort und Zeit.

Untersuchungen [12] haben gezeigt, dass Gespräche, die mit IM beginnen meist später über ein anderes Medium weitergeführt werden. Ein IM Gespräch kann in einer Sitzung, einem Telefongespräch, einer Audio- / Videokonferenz oder einem Anruf enden. Das bedeutet, dass IM nicht als ein isolierter Kommunikationskanal betrachtet werden soll, sondern als Teil eines ganzen Spektrums von Kommunikationsmedien. Um die eben besprochene Integration zu ermöglichen, müssen Email, VoiceOverIP, videoconferencing, applicationsharing und Kalenderanwendungen ein Interface anbieten, auf das über das IM zugegriffen werden kann.

Bisher wurde der Fokus auf die Anforderungen an die IM Applikation gelegt. Für eine Unternehmung ist aber nicht nur die Einsatzmöglichkeit der Applikation entscheidend, sondern auch die Fähigkeit der Mitarbeiter die Möglichkeiten zu nutzen. Die Applikation muss darum Verständlich und möglichst leicht und schnell erlernbar sein, damit sich zu den Anschaffungs- und Betriebskosten nicht budgetsprengende Schulungskosten gesellen. Weisungen über den Umgang mit IM als Kommunikationsmedium soll nach der Schulung der Mitarbeiter von allen Betroffenen verstanden und angewendet werden können.

Archivierung der Mitteilungen ist nicht nur ein technische Anforderung, sondern auch eine organisatorische Anforderung. Ausgetauschte IM Nachrichten sollen sich bei erneutem Kontakt wieder anzeigen lassen, damit sich der Mitarbeiter schnell wieder an das beim letzten Kontakt behandelte Thema erinnern kann. Wichtiges soll man markieren können, damit dieser Vorgang beschleunigt werden kann.

## 8.4 Geschäftsfälle

Die im Kapitel „Einsatzmöglichkeiten und zukünftige Szenarien für unternehmensweite Kommunikation“ aufgezeigten Einsatzmöglichkeiten ermöglichen es dem Unternehmen, IM nicht nur intern als Kommunikationsmittel einzusetzen, sondern auch mit unternehmensexternen Personen zu kommunizieren. IM bietet sich an auch mit Kunden, Lieferanten und Partnern eingesetzt zu werden.

Ein möglicher Geschäftsfall mit einem Kunden besteht in einem live Kundensupport durch IM. Dieser Supportkanal bietet im Vergleich zum Support per Email wesentliche Vorteile. Der Kunde kann die vom Supporter gegebenen Anweisungen gerade ausführen und sich bei Problemen zu Worte melden, auf die der Supporter dann in real-time eingehen kann. Als Beispiel dazu: Ein Grafiker hat sich ein Produkt von Adobe gekauft und kann sich nicht online registrieren. Er meldet sich über seinen IM Client beim Adobe Support. Der Supporter liest die IM Nachricht des Kunden und entscheidet sich, mit dem Kunden ein Audiogespräch zu führen, weil ihm die Supportanfrage zu wage formuliert ist. Nach einem klärenden Gespräch erkennt der Supporter das Problem: Der Kunde ist auf der falschen Website um sich für das Produkt zu registrieren. Damit der Supporter nun die richtige URL nicht diktieren muss, schickt er ihm den Link als Textnachricht über das IM System. Mittels eines Video-streams könnte der Supporter dem Kunden auch an seinem Bildschirm vorzeigen, wie ein spezifisches Problem zu lösen ist. Im Falle der Registrierung des Adobe Produktes hätte der Supporter also dem Kunden Mausklick für Mausklick vorzeigen können, was er zu tun hat um die Registrierung erfolgreich abzuschliessen. Kann der Supporter die Anfrage des Kunden nicht selber beantworten weil das sein Wissen übersteigt, kann er in seiner Freundesliste einen Mitarbeiter suchen, der die Frage am ehesten beantworten kann und ihn mit dem Kunden verbinden. Die Frage über die Abrechnung des Supports soll hier nur am Rande behandelt werden. Weil die Telefongebühren wegfallen, muss das Unternehmen eine andere Form der Bezahlung finden. Möglich wäre die Bezahlung per Kreditkarte nach Minuten oder pro Supportanfrage. Für vertrauenswürdige Kunden bietet sich eine monatliche Rechnungsstellung an.

Ein Geschäftsfallszenario mit einem Lieferanten könnte folgendermassen aussehen: Ein Unternehmen bestellt bei einem Anbieter für Elektronikzubehör 20 Flachbildschirme. Bei der Inbetriebnahme der Geräte wird eine Unschärfe des Bildes festgestellt. Der Verantwortliche kontaktiert den Support des Lieferanten und wird darauf aufmerksam gemacht, dass die Bildschirmauflösung angepasst werden muss.

Der Kontakt zu Partnern ist ebenfalls ein geeignetes Einsatzgebiet von IM: Drei Rechtsanwaltbüros vermitteln sich gegenseitig Kunden, die einen Anwalt für ein spezifisches Problem suchen. Weil sie sich gegenseitig ergänzen entsteht keine Konkurrenzsituation. Nach dem Eingang eines Auftrages klären die Anwälte untereinander ab, wer den Auftrag übernehmen wird und ob Zusammenarbeit durch Wissensaustausch nötig ist.

Diese beispielhaften Geschäftsfälle sollen die breite Einsatzmöglichkeit von IM aufzeigen. Wie im vorangehenden Kapitel bereits erwähnt, ist die Interoperabilität zwischen den IM Systemen der Unternehmung und ihren Partnern, Lieferanten und Kunden von entscheidender Bedeutung.

## 8.5 Zusammenfassung, Fazit und Ausblick

Unter Unternehmenskommunikation versteht man die Gesamtheit aller Kommunikationsmittel und -massnahmen um das Unternehmen und seine Leistungen bei allen relevanten Zielgruppen darzustellen. Sie beinhaltet somit sowohl die interne, als auch die externe Kommunikation. Eine gute Unternehmenskommunikation ist entscheidend für den Unternehmenserfolg.

Eine Vielzahl von Kommunikationstechnologien sind auf dem Markt erhältlich und eignen sich unterschiedlich für die konkreten Kommunikationsbedürfnisse. Eine der Kommunikationstechnologien sticht jedoch aus den verbreiteten Technologien hervor, nämlich Instant Messaging (IM). Die Einsatzmöglichkeiten von IM sind breit und flexibel. Die in Kapitel 8.3 vorgestellten Einsatzmöglichkeiten von IM verdeutlichen, dass IM in manchen Fällen eine effizientere Arbeitsweise ermöglichen, als z.B. mit E-Mail oder anderen Kommunikationsmittel. Gerade die Unmittelbarkeit, mit welcher Informationen ausgetauscht, verifiziert und darauf reagiert werden kann, ist sehr angenehm und bringt manchen Zeitgewinn im Erledigen der anfallenden Aufgaben.

Die hohe Arbeitslast die MitarbeiterInnen heutzutage in den Unternehmen bewältigen müssen, erschwert das „Socialising“, d.h. die Möglichkeit teilweise informelle, persönliche Gespräche zu führen. Der daraus resultierende potentiell negative Einfluss auf das produktive Arbeitsklima kann mittels Einsatz von IM stark reduziert werden. Die Möglichkeit sich z.B. zum Mittagessen oder zur gemeinsamen Kaffeepause zu verabreden kommt einerseits einer kurzen Verschnaufpause gleich, anderseits sind gerade diese Treffen wichtig für diversen Informationsaustausch, der sich wiederum positiv in der Produktivität der MitarbeiterInnen äussert.

So beliebt und effizient IM Applikationen auch sind, so bringen sie auch einige Sicherheitsrisiken mit sich. Gerade deshalb müssen Unternehmen das Thema IM sehr ernst nehmen und in ihre IT-Strategie miteinbeziehen.

**Fazit**

- Instant Messaging (IM) ist sehr beliebt und verbreitet sich immer mehr.
- Unternehmen müssen IM zwingend in ihre IT-Strategie miteinbeziehen, da IM viele Sicherheitsrisiken mit sich bringt.
- Unternehmen tun sich gut daran, IM offiziell als Teil ihrer Infrastruktur zur Verfügung zu stellen. Einerseits hält dies MitarbeiterInnen davon ab, kostenlose und potentiell unsichere „public Instant Messaging“ Applikatonen vom Internet herunterzuladen und zu installieren und anderseits kann damit das produktive Arbeitsklima erhöht werden.
- Unabhängig davon, ob Unternehmen den Einsatz von IM verbieten, einschränken oder voll zulassen wollen, sollten sie eine Richtlinie für den Einsatz von IM erlassen und kommunizieren. Es hat sich nämlich gezeigt, dass ein Grossteil der MitarbeiterInnen sich an solche Richtlinien halten, wenn sie sie kennen.
- Die technologische Basis für den Einsatz von IM im Unternehmen und die Entwicklung von neuen Services ist vorhanden.
- Es gibt für die meisten Bereiche offene Protokolle.
- Die Herausforderung aus technischer Sicht besteht hauptsächlich in der Interoperabilität der bestehenden und zukünftigen Services.
- Die Einsatzmöglichkeiten von IM sind sehr breit. Die Kommunikation kann sich auf das Unternehmen intern beschränken und so die Arbeitsproduktivität unter den Mitarbeitern erhöhen. Denkbar sind aber auch Supportaufgaben für Kunden, die, wie bereits aufgezeigt, eine hohe Flexibilität aufweisen.
- Durch Presence Informationen, die der IM Client den andern IM Teilnehmern mitteilt, wird die Produktivität eines Mitarbeiters durch ständige Unterbrüche nicht gemindert, da er nur dann Mitteilungen empfängt, wenn er dazu auch bereit ist.

**Ausblick**

Der Trend von zukünftigen Enterprise IM Systemen zeigt deutlich hin zu einer höheren Integration von bereits bestehenden Applikationen. Integriert werden können zum Beispiel andere Kommunikationsplatformen, Terminplaner, Archivierungs- und Sortiertools. Da das IM System meistens nur der Beginn eines Austausches zwischen zwei oder mehreren Personen ist, soll es innerhalb des IM Systems möglich sein auf andere Medienkanäle zu wechseln. Während einer IM Sitzung soll es per Mausklick möglich sein auf ein Telefongespräch zu wechseln oder eine Videokonferenz zu initialisieren. Ähnlich soll es sich mit Terminen verhalten, die per Mausklick in einen Terminplaner eingefügt werden können. Termine sollen als Presence Informationen den anderen IM Teilnehmern angezeigt werden, automatisch, versteht sich. Die Archivierung von IM Nachrichten soll sich in die der Emails, Termine und Telefonate integrieren und per Suchmaschine gefunden werden. IM soll sich also in den Workflow und die Applikationslandschaft der Unternehmung integrieren und damit eine höhere Effizienz der Unternehmenskommunikation ermöglichen.

# Literaturverzeichnis


[1] Dr. Wolfgang Martin, Richard Nußdorfer, Portale in einer service-orientierten Architektur (SOA), 5.6.2006 http://www.intersystems.de/pdf/wp_pm-portale_deutsch.pdf

[2] Wikipedia, Unternehmenskommunikation, http://de.wikipedia.org/wiki/Unternehmenskommunikation, 5.6.2006

[3] Christopher Harris-Jones: Communication:the heart of collaboration an KM, July 2005

[4] Eidgenössischer Datenschutzbeauftragter: Erläuterung zur Telefonüberwachung am Arbeitsplatz, März 2004 http://www.edsb.ch/d/themen/weitere/telefonueberwachung_d.pdf

[5] Wikipedia, Wiki, http://de.wikipedia.org/wiki/Wiki, 29.5.2006

[6] Wikipedia, Instant Messaging, http://en.wikipedia.org/wiki/Instant_messaging, 26.04.2006.

[7] META Group Inc., Best Practices: Collaboration and Messaging, Edition 1, 2004

[8] Mohammad Mannan, P.C. van Oorschot: Secure Public Instant Messaging: A Survey, September 2004

[9] Gartner Research, MessageLabs-Zukauf deutet auf eine Konvergenz von E-Mail und Instant Messaging hin, Dokumentnummer G00134044 vom 28.10.2005

[10] G. Lawton: Instant Messaging Puts on a Business Suit, Computer, Vol. 36(3), March 2003, pp. 14-16, http:// dx.doi.org/10.1109/MC.2003.1185208 (available from within UniZH network)

[11] Nardi, B., Whittaker, S. and Bradner, E. (2000). Interaction and Outeraction: Instant Messaging in Action. In Proceedings CSCW'2000, ACM Press.

[12] John C. Tang, James Begole: Beyond Instant Messaging, http://doi.acm.org/10.1145/966712.966718, 9.6.2006

[13] J. von Knop, H. Frank. Netzwerk- und Computersicherheit. W. Bertelsmann Verlag, 2004.

[14] Jari Karppanen: Proprietary Instant Messaging and Presence Protocols, Department of Computer Sciences, Univeritiy of Helsinky, http://www.cs.helsinki.fi/u/leggio/courses/papers/proprietary.pdf, 2005.

[15] American Online (AOL): AOL Instant Messanger, http://www.aim.com/, abgerufen Juni 2006.

[16] IETF: Extensible Messaging and Presence Protocol Working Group, http://www.ietf.org/html.charters/OLD/xmpp-charter.html, abgerufen Juni 2006.

[17] Microsoft Corporation: Live Communication Server 2005, http://www.microsoft.com/office/livecomm/prodinfo/default.mspx, abgerufen Juni 2006.

[18] IBM: IBM Lotus Sametime 7.5, http://www.ibm.com/software/sw-lotus/products/product3.nsf/wdocs/homepage, abgerufen Juni 2006.

[19] IRC.org: http://www.irc.org/, abgerufen Juni 2006.

[20] ICQ.com: http://www.icq.com, abgerufen Juni 2006.

[21] Yahoo Inc. http://www.yahoo.com, abgerufen Juni 2006.

[22] Peter Salin: Mobile Instant Messaging Systems - A Comparative Study and Implementation, Department of Computer Science and Engineering, Helsinki University of Technology, http://www.tml.tkk.fi/Publications/Thesis/Salin-IMPS.pdf, 2004.

[23] Wikipedia.org: Comparison of Instant Messengers, http://en.wikipedia.org/wiki/Comparison_of_instant_messengers, abgerufen Juni 2006.

[24] IETF: Instant Messaging and Presence Protocol Working Group, http://www.ietf.org/html.charters/OLD/impp-charter.html, abgerufen Juni 2006.

[25] IETF: SIP for Instant Messaging and Presence Leveraging Extensions Working Group, http://www.ietf.org/html.charters/simple-charter.html, abgerufen Juni 2006.

[26] Microsoft Corp: MSN Messenger, http://messenger.msn.com, abgerufen Juni 2006.

[27] R. Movva, W. Lai: Messaging and Presence Protocol, IETF Draft, http://www.hypothetic.org/docs/msn/ietf_draft.txt, abgerufen Juni 2006.

[28] Jeremy Hamman: AIM/OSCAR Protocol, http://www.geocities.com/smokeyjoe12345/OscarProtocol.htm, abgerufen Juni 2006.

[29] A. V. Shutko: OSCAR (ICQ v7/v8/v9) protocol documentation , http://iserverd.khstu.ru/oscar/, abgerufen Juni 2006.

[30] P. Saint-Andre: Extensible Messaging and Presence Protocol (XMPP): Core, IETF RFC 3920, http://www.ietf.org/rfc/rfc3920.txt, 2004.

[31] P. Saint-Andre: Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence, IETF RFC 3921, http://www.ietf.org/rfc/rfc3921.txt, 2004.

[32] P. Saint-Andre: Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM), IETF RFC 3921, http://www.ietf.org/rfc/rfc3922.txt, 2004.

[33] P. Saint-Andre: End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP) (CPIM), IETF RFC 3921, http://www.ietf.org/rfc/rfc3923.txt, 2004.

[34] St. Middendorf: Potentielle Gefahr fürs Netz: Instant-Messaging- und Peer-to-Peer-Dienste, iX-Magazin für professionelle Informationstechnik, 7/2004, S. 96.

[35] IM+: Multi-system Mobile Instant Messenger 2.1.12, IM+: Multi-systemMobileInstantMessenger2.1.12 abgerufen Juni 2006.

[36] Research in Motion: BlackBerry, http://www.blackberry.com/, abgerufen Juni 2006.

[37] Heise Newsticker: USA fürchten um Agenten und Soldaten bei drohendem Blackberry-Aus, http://www.heise.de/newsticker/meldung/69440, abgerufen Juni 2006.

[38] Smarttech: smartideas, www.smarttech.com/smartideas, abgerufen Juni 2006.

[39] Skype, http://www.skype.com/.

[40] Open Mobile Alliance, Push to Talk over Cellular Working Group, http://www.openmobilealliance.org/, abgerufen Juni 2006.

[41] Heise Newsticker, http://www.heise.de/newsticker/meldung/69547, abgerufen Juni 2006.

[42] Open Mobile Alliance, http://www.openmobilealliance.com/tech/wg_committees/poc.html, abgerufen Juni 2006.

[43] Heise Newsticker: UMTS-Flachmann mit Push-Email via IMAP IDLE, http://www.heise.de/newsticker/meldung/69515, abgerufen Juni 2006.

# Chapter 9

# IMS – IP Multimedia Subsystem

*Danar Barzanji, Marcel Steffen, Roger Trösch*

*The IP Multimedia Subsystem (IMS) is a new technology, a so-called Next Generation Network (NGN), which is standardised by the 3rd Generation Partnership Project (3GGP). It enables a technology independent access to a multitude of services which have not been possible, or only usable through the Internet. These are for instance Push-To-Talk, realtime video sharing, instant and voice messaging, video conferencing and the usage of interactive applications on the basis of IP.*
*An IMS system offers other advantages. For example Quality of Service (QoS) that guarantees an appropriate quality of a certain service especially regarding bandwidth and short delays. Another benefit of IMS is the flexibility of charging; the system offers several different charging models. Additionally, in the aspect of interworking the IMS breaks new ground.*
*Thanks to its special architecture, the system is very flexible in terms of implementation and customisations can be easily realised. This is owed to the independence of each individual IMS element which was already pre-arranged up from the draft. Additionally, this characteristic makes it possible to use past and future technologies cross-linked without any problems. Only functions and interfaces are standardised by 3GPP in each individual IMS element and therefore everybody who wants to introduce IMS has a minimum limitation in the system implementation. Communication within IMS is mainly based on the Session Initial Protocol (SIP) that enables multimedia features like video-, voice-, instant messaging, online gaming and many more.*
*This paper deals with all relevant aspects of IMS. The fundamental architecture is described with the most important elements of this standard. Moreover, protocols used in IMS are illustrated and explained. Finally, services which can be realised in IMS are exemplified.*

## Contents

**9.1 Introduction . . . . . 278**
9.1.1 Benefits of IMS . . . . . 278
9.1.2 3GPP . . . . . 279
**9.2 Architecture . . . . . 279**
9.2.1 IP multimedia session . . . . . 280
9.2.2 Quality of service (QoS) . . . . . 280
9.2.3 Charging . . . . . 281
9.2.4 Access independence . . . . . 284
9.2.5 Interworking . . . . . 284
9.2.6 Roaming . . . . . 284
**9.3 IMS Components . . . . . 285**
9.3.1 Call Session Control Function (CSCF) . . . . . 286
9.3.2 Databases HSS and SLF . . . . . 287
9.3.3 Interworking elements . . . . . 287
9.3.4 Application server (AS) . . . . . 288
9.3.5 Media Resource Function (MRF) . . . . . 288
9.3.6 Support entities . . . . . 289
9.3.7 Access entities . . . . . 289
**9.4 IMS Concepts . . . . . 290**
9.4.1 Registration . . . . . 290
9.4.2 Session establishment . . . . . 291
9.4.3 Security . . . . . 291
9.4.4 IMS entry point . . . . . 292
9.4.5 S-CSCF assignment . . . . . 292
9.4.6 User profile . . . . . 293
9.4.7 Connectivity to non-IMS user . . . . . 293
**9.5 Protocols . . . . . 293**
9.5.1 SIP (Session Initiation Protocol) . . . . . 294
9.5.2 Use of SDP in SIP . . . . . 300
9.5.3 Media Plane Protocols . . . . . 301
9.5.4 Authentication and security protocols . . . . . 303
**9.6 Service Examples . . . . . 304**
9.6.1 Push-To-Talk . . . . . 304
9.6.2 Real-time Video Sharing . . . . . 304
9.6.3 Interactive Applications . . . . . 304
9.6.4 Instant-/ voice messaging . . . . . 305

9.6.5 Video conferencing . . . . . 305
**9.7 Summary . . . . . 305**

## 9.1 Introduction

These days, Internet users frequently use all the colourful and interactive services they get. Several applications that use the data highway for communication became a daily habit and we can not live without it anymore. These are for example email, browsing the web, VoIP, instant messaging, video conferences and many more. These services often consume high bandwidth and therefore we use it in our office or at home where we fortunately have a broadband access. But what can we do, if we want to access the Internet everywhere we go? The easiest way to handle this demand would be using the 2G or 3G network. Unfortunately, the 2G technology is circuit-switched based and the low bandwidth makes it impossible to use these features. This technology was designed to transport voice and only a small amount of data. Later on the 2.5G standard brought the General Packed Radio Service (GPRS). It is faster and it uses a packed-switched domain. Even the speed is little faster, comfort and reliability is below a standard analogue dial-up line. Fortunately, we got the 3G technology that offers a cell based packed-switched high-speed access to the Internet. However, 3G offers several enhancements compared to GSM it still has a few weak points. These are Quality of Service (QoS), charging, problems with peer-to-peer and multi-sessions connections. For this reason, a standards-based architecture was constructed that addresses all the problems below. It is called the IP Multimedia Subsystem (IMS) [1], [2].

### 9.1.1 Benefits of IMS

In the very basic architecture the 3G Technology does not offer QoS. For a standard data transmission on a 3G network, such as checking email or download a ring tone, is no need to have a particular grade of service quality. But let us think about a video conference or other multimedia services. These special applications need a particular QoS for the time of use. This need can be managed by an IMS that establishes a particular degree of service quality.

A second reason for IMS is the charging function. This new functionality is needed because the old charging mechanisms cannot be used any more. The manifold new and often traffic intensive mobile services will generate a huge amount of data and so the user will be charged inadequately high. This is because the mobile providers traditionally charge the utilisation of the packet-switched system byte per byte. The IMS will offer a different approach to handle charging in a more flexible and more appropriate way. This will result in a more beneficial situation for both the provider and the mobile user.

A third cause for an integration of an IMS is the necessity of a peer-to-peer connection of several multimedia services which an ordinary 3G system can not offer. The IMS will offer a worldwide standardised IP-based accessibility to reach all you colleagues for a chat or all the other communication things the future will bring up [1], [2].

### 9.1.2 3GPP

During the late 1980s and 1990s, the European Telecommunications Standard Institute (ETSI) was the organisation that standardised the Global System for Mobile Communication (GSM). Later on, the ETSI also defined the GPRS network architecture. In the year 1998 the 3GPP was founded by representatives from Europe, Japan, South Korea, the USA and China. This organisation specified the third-generation mobile system (3G), the Wide Code Division Multiple Access (WCDMA) and also the Time Division/Code Division Multiple Access (TD-CDMA) radio access.

In 1999, the 3GPP decided to release each year a technical specification for the mobile evolution. The Release 4 from the year 2000, contained the first time a specification called All-IP that was later renamed to IMS. The following Release 5 introduced the IMS as a part of 3GPP and introduced it as a standardised access-independent IP-based architecture that interworks with voice and data networks for fix and mobile users. This architecture may facilitate interoperability between PSTN, ISDN, Internet, GSM and CDMA. At the moment, the 3GPP works on Release 7 and 8 [1].

## 9.2 Architecture

As we already mentioned, the IMS architecture was designed to go a step further into the mobile communication future. Telecommunication providers realised, that it is in the long term no longer possible to make profit out of the ”old-fashioned” mobile communication systems. At this point, the IMS came across and opened a new and bright way to offer several new and not yet seen services that were not possible before. So the main purposes of the IMS were:

- Combining the latest in technology
- Making the mobile internet paradigm come true
- Creating a common platform to develop diverse multimedia services
- Creating a mechanism to boost margin due to extra usage of mobile packet-switched networks

To ensure that this framework works properly and guarantees the IP multimedia services to end-users, the 3GPP defined some IMS requirements that must be supported by the systems. All these requirements are elaborated in the 3GPP TS 22.228 [9]. These are [2]:

- Support of IP Multimedia Sessions
- Support of Quality of Service (QoS)
- New charging arrangements
- Access independence
- Support of interoperability and roaming

### 9.2.1 IP multimedia session

The basic requirement a client needs to access in the IMS system is IP connectivity and it has to use the IPv6 protocol [10]. Although some of the early IMS implementations use IPv4, the end goal is still IPv6. To manage this ambiguity the IMS should support both protocols to guarantee IPv6-IPv4 interoperability [3].

There are two possibilities to get the IP connectivity in an IMS Release 5 Figure 9.1. In the first one, the user equipment (UE) accesses the network as a visitor (roaming). It will get an IP address from the visited infrastructure. Let us assume that we are in a Universal Mobile Telecommunication System (UMTS) network. Then all the elements such as the Radio Access Network (RAN), Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) are located in the visited network.

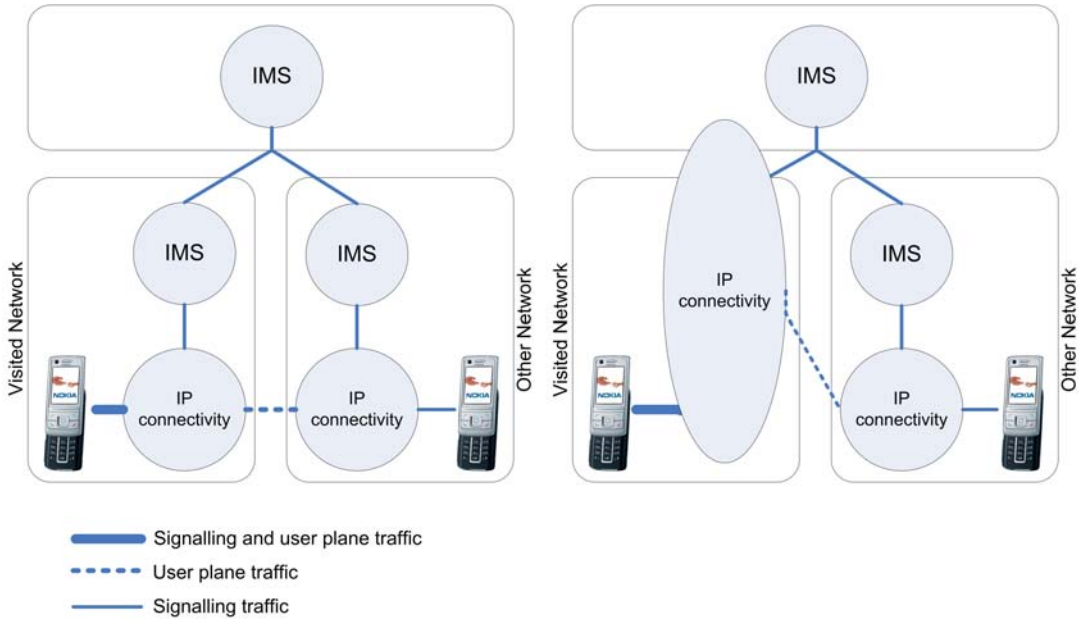



Figure 9.1: IMS connectivity options when a user is roaming [1]

In the second possibility, the UE still gets his IP address from the home network by roaming in a foreign network. In this situation only the RAN and the SGSN are used in the visited network and all other elements are located in the home network. This fact allows having all the fancy new IMS services without having an IMS system in the visited network. Theoretically it should be possible to access the home IMS system by only using a GPRS access in a visited network. In practice, this will not happen because the routing efficiency will not be fast enough to deal with a real time service [1].

### 9.2.2 Quality of service (QoS)

Quality of service (QoS) means that a certain performance is guaranteed to all the applications that require it. On the public Internet we often have to deal with long delays and sometimes packets do not arrive in the same order than sent. Occasionally, it happens

that packets even never arrive at the planned destination. This characteristic is not appropriate for a voice or a video call. These services need a real time packets delivery and should not have a delay or even lost message parts. This would cause a mess in voice or video stream and so, it will not be possible to follow the call any more. For this reason, the IMS needs reliable functionalities to get rid of these drawbacks. Sometimes it is not that easy as it seams, to fulfil expectations the users have about the performance of the mobile access. Each person has different preferences and the network providers have to find a reasonable solution for all of them. In a shared medium such as the Internet, it is quite difficult to offer a certain level of performance. An IMS deals with this by having certain allocated resources for each service that is reserved for only one particular duty. For this approach we need an end-to-end implementation that has a certain demand on the equipment on both sides, on the mobile device and the access network. Having a certain quality of service, does not only address the home IMS. In case of an inter-domain connection, it is equally important to have the required performance. To ensure this, the IMS providers need service level agreements with all involved parties. Any QoS assurances are only as good as the weakest link in the "chain" between sender and receiver [5].

During the Session Initiation Protocol (SIP) session set-up, the UE negotiate the QoS requirements with the IMS. They have to find an agreement about following parameters [1]:

- Media type, direction of traffic
- Media type bit rate, packet size, packet transport frequency
- Usage of real time transport Protocol (RTP) payload for media types
- Bandwidth adaptation

When all parameters were negotiated at the application level, the UE allocates the required resources from the access network. The UE will now encode all the data packets with an appropriate protocol (e.g. RTP) and will send it from the access to the transport network by using a transport layer protocol (e.g. TCP or UDP) over IP. To guarantee the QoS by roaming in a foreign network it is important for the operators to negotiate service level agreements (SLA) with competitors to have the same performance trough the entire network. In UMTS, the GPRS roaming exchange backbone would be used by providers to deal with [2].

### 9.2.3 Charging

All mobile operators rely on the users to pay their bills for the usage of their network. To handle this task, operators use several technical elements to guarantee a correct and appropriate price. Normally, we find two different methods for charging the user; the offline and the online charging. An online charging system interacts in real-time with a user's account. It offers several different methods for all possible services. Examples are that the AS makes a request for initialising a session or it asks how long a user is allowed to participate in a phone conference. In an offline charging system, the charging progress

will be started after the end of a session. For this reason it does not need a real-time service. This offline charging system is used when mobile companies send the bills to their users on a regularly base. For these two different approaches of charging, the IMS needs a specialised implementation in the architecture [1], [2].

### Offline charging

The Charging Collection Function (CCF) is the central component of an offline charging. It receives all the accounting messages from the IMS components. They all use the Rf reference point. This interface uses the DIAMETER protocol for the accounting request (ACR) between the IMS components and the CCF. Based on that, the CCF generates the Charging Data Records (CDR) and transmits the CDR to the billing system that generates the final CDR out of all the records it has got from all the IMS components. Figure 9.2 shows such an IMS offline charging architecture. In this particular case, both users are roaming. In a non-roaming situation it would have only one CCF on each side. By using the CCF it is possible to deal with charging data from several different IMS elements. These are: Application Server (AS), Multimedia Resource Function Controller (MRFC), Proxy-Call Session Control Function (P-CSCF), Serving-CSCF (S-CSCF), Interrogating-CSCF (I-CSCF), Breakout Gateway Control Function (BGCF) and Media Gateway Control Function (MGCF) [1], [2].

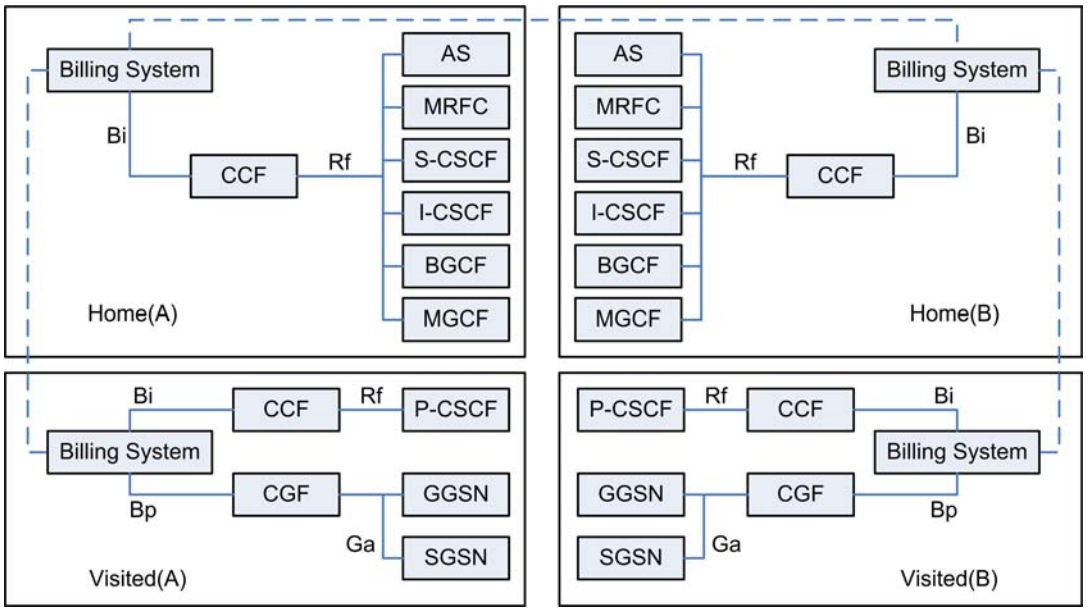



Figure 9.2: IMS offline charging architecture [1]

A CCF can be implemented in two different ways. One possibility is to integrate the CCF directly into the IMS components. A more appropriate way is a stand alone solution that deals much better with high loads and therefore it does not need a buffer functionality.

In a Packed Switched Domain (PS), the Charging Gateway Function (CGF) transmits the charging data from SGSN and GGSN. In general, the functionality of CGF is the same

than the CCF in an IMS domain. The difference is that the CGF gets valid CDRs from SGSN or GGSN [11].

For the transmission of the CDR from the CCF into the billing system, the BI reference point is used. Because of the huge variety of different billing systems, the 3GPP does not define a standard protocol. The recommendation is FTP over TCP/IP for the file interface.

### Online Charging

In an online charging environment the Serving-CSCF (S-CSCF), Application server (AS) und Multimedia Resource Function Controller (MRFC) of the IMS are in account for charging Figure 9.3. The AS and MRFC use the Ro reference point for the communication to the Event Charging Function (ECF), by using the DIAMETER protocol. The S-CSCF uses the IMS Service Control (ISC) reference point for the transmission to the Online Charging System (OCS).

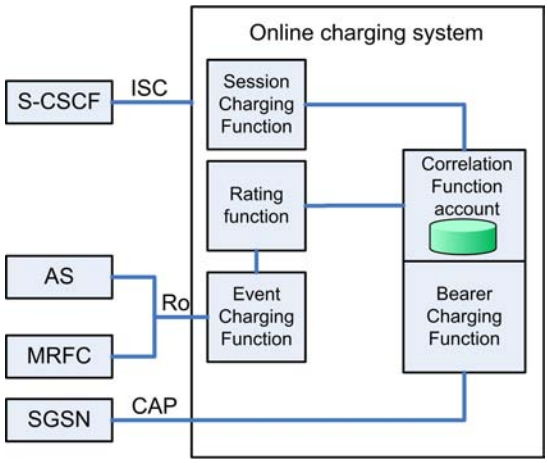



Figure 9.3: IMS online charging architecture [1]

Online charging has two different functionalities. One is event charging and the other is session charging. An example of an event charging issue is when a user wants to subscribe a news service. His request will reach an AS or MRFC. The AS or MRFC will ask the ECF by using the Ro, if this service will be allowed to be used by the customer. The ECF has now two different models for the authorisation; the immediate event charging or the event charging with unit reservation. In the immediate event charging model, the ECF will calculate an appropriate tariff for the service and will subtract the money on the user's account. Further on, it inform the AS or MRFC that the requested service can be delivered. In the event charging with unit reservation model, the ECF reserve a specific sum for this service on the account of the user. Then it informs the requesting component about the available resources on the user's account. These resources are allowed data volumes or time. After the service delivery, the AS or MRFC report how much resources were consumed and the ECF charges the users' accounts. This model is normally used when the length or data volume of a service is not known in advance.

The Session Charging Function (SCF) receives requests from the S-CSCF via the ISC reference point and performs the accounting based on the resources a session needs. The SCF checks the user's account and decides whether to allow or deny a session. The SCF is also able to interrupt a ongoing session when the user's account is empty. It also supports the event charging with unit reservation model.

The Bearer Charging Function (BCF) controls bearer usage for example in terms of traffic volumes or using time. The SGSN requests permission for bearer usage, using the CAMAL Application Part (CAP) reference point. Then the BCF interacts with the user's account and the rating functions for the charging.

The rating function is dealing with the determinations of units, prices and tariffs. It calculates the amount a user has to pay for a consumed service based on non-monetary units such as service units, data volumes and time. After the calculation, the account balance of the user will be updated [1].

### 9.2.4 Access independence

The idea of IMS is that it is access independent. This means that it is possible to connect the IMS by any network. The access can be fixed, mobile or wireless with packet-switching technologies, such as GPRS, UMTS, CDMA2000, WLAN, WiMAX, DSL or cable. For older technologies that are circuit-switched based, such as POTS and GSM, it is necessary to use a gateway to access the IP-based network [6]. This access independence opens a variety of new mobility features. The access independence allows making hand-over between the different access technologies. It is possible to work on a mobile device in an office building being connected to a WLAN access point. By leaving the building, the device will perform a handover to UMTS or another infrastructure. The user will be permanently connected without an interruption and he can work or attend a conference call [4].

### 9.2.5 Interworking

Although the world is getting more and more connected by communication technologies, we can not expect that all communication providers change their infrastructure from one day to another to an IMS. For this reason, as already mentioned, it is really important for IMS to support the access independence. Furthermore, it is also essential for IMS to support the interworking of all the technologies that are able to access the IMS. It should be irrelevant if someone access with POTS, ISDN, GSM or the internet to communicate with someone using an IMS. In addition, it should also be possible to access with systems that were not being developed by the 3GPP community [9], [1].

### 9.2.6 Roaming

Today, it is important for many people to be independent of a particular geographical place without abandon their communication facilities. This means that the communication

systems have to support roaming. An IMS supports several types of roaming. The most striking one is roaming between different technologies. As an example, it allows to roam between the WLAN in an office and UMTS outside the building without an interruption. Given that not all providers offer an IMS, it is important having an accessibility from everywhere to his own home IMS. For example by using GPRS roaming. In order to provide this service, the foreign network has to offer RAN, SGSN and GGSN to access the home IMS. Another necessarily feature is the inter-domain roaming between IMS and CS. If a user is not reachable in a IMS domain, it has to be possible to route to a CS domain. It should be clear that these two technologies have several different functionalities and not all of them are supported on both sides [1].

## 9.3 IMS Components

In IMS, the 3GPP decided not to standardise the nodes of the system but the functionalities that the system should support. The architecture is a construction of functions that interwork with standardised interfaces. The IMS providers can make their implementation however they want. This "free concept" allows having a particular IMS element not necessarily in only one "box". It is possible to combine several elements in one node. In the same way, it is also possible to split functionality into two or more separate nodes. In general, a lot of providers follow the recommendation of the 3GPP. A reason for this is the fact that many IMS hardware manufactures follows the standards. Figure 9.4 shows the IMS architecture standardised by 3GPP. It also shows the different interfaces between the nodes. In this paper, we only focus on the important ones [2].

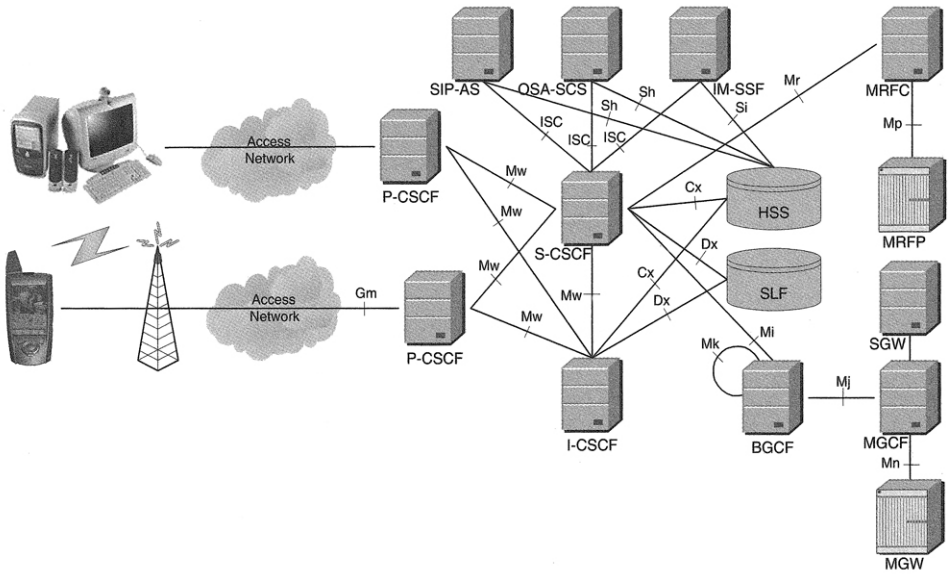



Figure 9.4: 3GPP IMS architecture overview [2]

The IMS architecture design is split into three layers. The layers are the services/application, IMS and the transport layer Figure 9.5). This approach represents the enclosed three planes structure that allows having the multi accessibility of IMS, because each layer has

a particular duty. Thus, it is quite easy to introduce a new functionality or implement further access technologies.

The service and application layer includes all the servers and elements to offer the wide range of different services. All elements those are responsible for the operation in an IMS, are situated in the IMS Layer. As the name implies, the transport layer is handling the accessibility to the IMS and the transport of data from in- and outside.

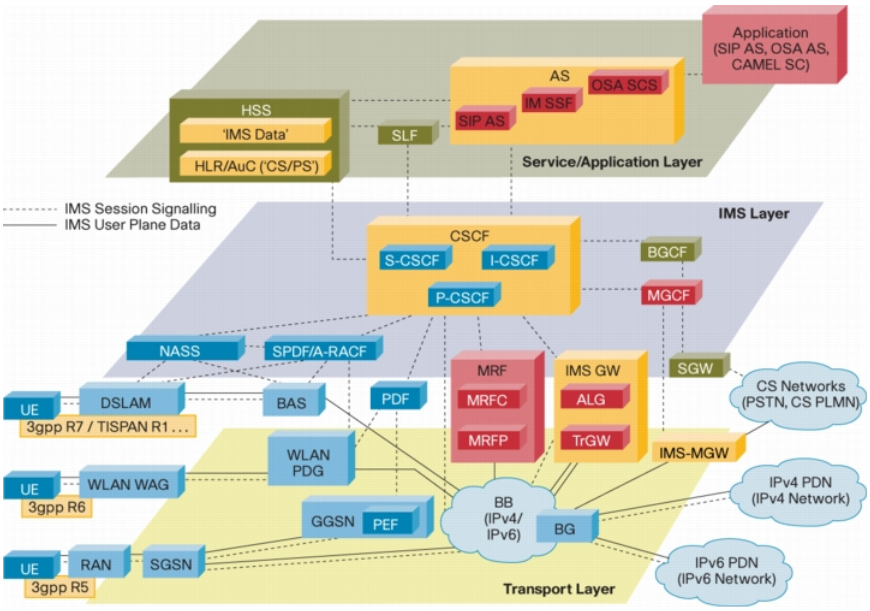



Figure 9.5: The three layer architecture [14]

It is possible to group the IMS architecture in six main categories. These are session management and routing family (CSCFs), databases (HSS, SLF) interworking elements (BGCF, MGCF, MGW, SGW), services (AS, MRFC, MRFP), support entities (THIG, SEG, PDF) and charging. For the access by using a GPRS, WLAN or DSL interface, the IMS needs some additional elements. More at the end of this section.

### 9.3.1 Call Session Control Function (CSCF)

CSCF is an important node of IMS and is responsible for all call session control signalling in the IMS using SIP. We can differentiate three types with diverse functionalities:

#### Proxy-CSCF

P-CSCF acts as the first point of contact for the user equipment within the IMS and can be located either in the same network or in a visited network [7]. Responsible functions are: proxy function for requests, security functions, verification of SIP requests, compression and decompression of SIP messages, policy decision function and generating charging information [2].

**Interrogating-CSCF**

"I-CSCF is a contact point within an operator's network for all connections destined to a subscriber of that network operator. There may be multiple I-CSCFs within an operator's network" [1]. Performed functions are: forwarding SIP request and responses to S-CSCF, providing topology hiding of the home network, obtaining names of S-CSCF from HSS and retrieving user location information.

**Serving-CSCF**

S-CSCF is always located in the home network and is a central point of signalling. It handles the registration with the help of the HSS and it decides whether a application server is needed in order to ensure a service request is handled in an appropriate manner. There can be several S-CSCF in a network and they can serve many terminals according to the capacity [2].

### 9.3.2 Databases HSS and SLF

All data of subscribers are stored in the central repository called Home Subscriber Server (HSS). This information is required for establishing sessions and providing services. It contains identification information, security information, location information and user profile information [7]. Moreover, the HSS provides information about the S-CSCF of a user. "DNS/ENUM entity translates the different public identifiers of the user. It provides name to address translation required by the call session control entities" [8].

Subscription Locator Function (SLF) is a database that obtains queries about users' addresses and provides the requestor with all related information from the HSS [2].

### 9.3.3 Interworking elements

Breakout Gateway Control Function (BGCF) is only used from IMS originated calls into a circuit-switched domain. This can either be within the same network or to another network. In the first case, the BGCF selects a MGCF for further handling of the session, and in the other case the request will be forwarded to another GGCF in the selected network. Furthermore, the BGCF can report account information and collect statistical information [1].

The Media Gateway Control Function (MGCF) mainly does the protocol conversion and mapping of SIP between IMS and a circuit-switched domain. The Signalling Gateway (SGW) performs protocol conversions on a lower layer and the Media Gateway (MGW) converts between the Real-Time Function (in IMS) and the Pulse Code Modulation (in CS). Interworking between IMS and CS domains is described more explicit in Section 9.4.7.

### 9.3.4 Application server (AS)

The ASs are the elements in IMS that offer the multimedia services. It might happen that a service is the result of a collaboration of several AS that work together. It is also possible having an AS that is in a third-party location, connected to the IMS. The main functions of an AS are [1]:

- The possibility to process and impact an incoming SIP session received from the IMS.
- The capability to originate SIP requests.
- The capability to send accounting information to the CCF and the OCS.

We have three different categories for ASs:

A **SIP AS** hosts a variety of different IP multimedia applications that are offered on a SIP-base. All the IMS services in future will run on such SIP application servers.

The **OSA-SCS** (Open Service Access - Service Capability Server) offers a interface to the OSA framework Application Server. This allows functionalities like: call control, user interaction, user status, data session control, terminal capabilities, account management, charging and policy management for developing services [1]. In addition, it is possible to access the IMS securely from external networks. The OSA-SCS uses the OSA Application Program Interface (API) to communicate with the OSA AS.

The **IM-SSF** (IP Multimedia Service Switching Function) is integrated in the IMS architecture to offer further usage of the former services, based on CAMEL (Customized Application for Mobile network Enhanced Logic) that were designed for GSM. The IM-SSF makes it possible for the gsmSCF (GSM Service Control Function) to control an IMS Session. It communicates with IM-SSF by the CAP (CAMEL Application Part) protocol.

### 9.3.5 Media Resource Function (MRF)

The MRF provides the home network with a source of media. It supports multi-party multimedia conversations, message playing, mix media streams, media conversion and any sort of media analyses [2].

MRF is divided into a controller (MRFC) and a processor (MRFP). The MRFC interprets SIP signalling from S-CSCF in order to create and schedule ad-hoc conference sessions and alter conferences members. MRFP enables manipulation in the connectivity layer and performs the mixing of incoming streams, media stream source and media stream processing [1].

### 9.3.6 Support entities

**Policy Decision Function (PDF)** is responsible to make policy decisions coming from P-CSCF. The decisions are based on session and media related information and are for example providing, updating, revoking authorisation decisions and informing P-CSCF when bearer is lost or modified [1].

**Topology Hiding Inter-network Gateway (THIG)** is a function that can be used in the I-CSCF for a signalling-based hiding of configuration, capacity and topology of the network from the outside [9].

**Security Gateway (SEG)** is a gateway which tunnels data encapsulated in a security payload between to security domains. It is part of the network domain security described in Section 9.4.3.

### 9.3.7 Access entities

#### GPRS access (R5)

The **Serving GPRS Support Node (SGSN)** is the connecting part between the packed core network and the RAN. It supervises the control and traffic-handling function of the IMS PS domain. The control function has two different tasks, the mobility and session management. The mobility management processes the location and the status of the UE. It also handles the subscriber and UE authorisation. The Session management deals with connection admission control and changes in the existing data connections. Furthermore, it verifies the service and resources of the 3G network. The SGSN works as a relay between UE and GGSN. This also includes the QoS handling and generating charging information.

The **Gateway GPRS Support Node (GGSN)** offers interworking with external packed based networks. The main task of a GGSN is to set-up a connection between external networks with IP-based applications and services and the UE. These networks are either a IMS or the internet. It routes IP packets with corresponding SIP signalisation from the UE to the P-CSCF and vice versa. The GGSN offers the access to different networks, the user want to connect. If a UE wants to connect a IMS service by using GPRS, the GGSN assigns a dynamic IP to the UE and so it is able to receive a IMS service. In addition, the GGSN generates charging information as well [1], [2].

#### WLAN access (R6)

The **Wireless LAN Wireless Access Gateway (WLAN WAG)** is the component that allows accessing the IMS by Wireless LAN. It forwards the incoming data to the **Wireless LAN Packet Data Gateway (WLAN PDG)** or vice versa [14].

**DSL access (R7)**

To access the system by DSL a **Digital Subscriber Line Access Multiplexer (DSLAM)** is necessary. The **Base Station (BAS)** forward the data to the IMS or vice versa [13].

## 9.4 IMS Concepts

The purpose of this chapter is to give an overview of the different concepts of IMS. For the registration (section 9.4.1) a request needs to be sent to the appropriate IMS entity. This entity can be found with a so-called Proxy-Call Session Function (P-CSCF) discovery (9.4.4). The mobile device has to obtain an identity from the identity module (9.4.2) before a registration can be performed. Subsequently, an authentication is carried out (9.4.3) and the user profile will be downloaded (9.4.6) to the assigned S-CSCF (9.4.5). Section 9.4.7 briefly handles the interoperability between traditionally circuit-switched users and IMS users.

### 9.4.1 Registration

Figure 9.6 shows the two phases of a registration. In a first phase, the IMS terminal sends a SIP request with its identity and its home domain name to the P-CSCF which forwards the request to an Interrogating-CSCF (I-CSCF). The Home Subscriber Sever (HSS) provides the I-CSCF with information about the selection of the appropriate S-CSCF. Afterwards, the request will be sent to this S-CSCF which realises that the terminal is not authorised and sends back a challenge.

In a second phase, the terminal calculates the challenge and delivers its response back on the same way. If the S-CSCF accepts the response, it downloads the terminal's user profile from HSS and sends back a response to the terminal. After a certain time the registration needs to be renewed otherwise the authorisation will expire.

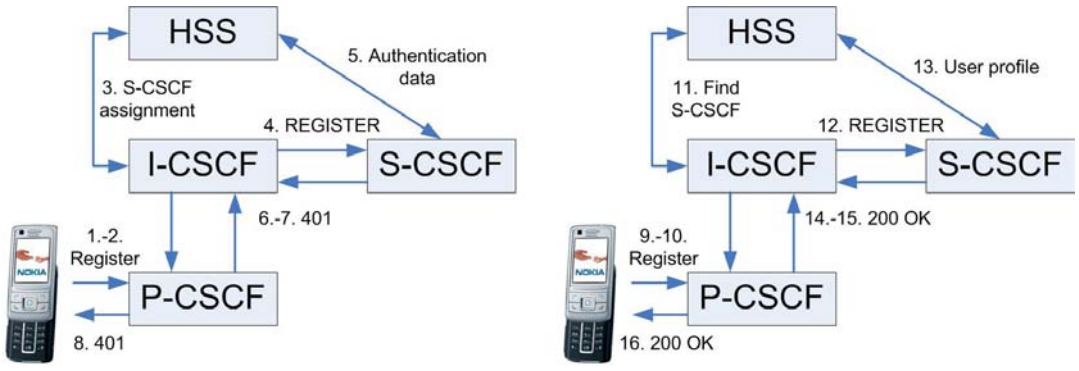



Figure 9.6: A high-level IMS registration flow [1]

### 9.4.2 Session establishment

For setting up a session from one terminal to another, terminal A has to send a SIP INVITE to its P-CSCF which checks the user identity before forwarding the request to the S-CSCF. Die S-CSCF searches the entry point of terminal B's home network and sends the request to the corresponding I-CSCF that finds the responsible S-CSCF with help of the HSS. Eventually the request ends up at the C-CSCF that sends the request to terminal B after a privacy check. B delivery a response to A on the same way back and after a few more back and forth the session is established and the actual application can start.

IMS has a private and public identity for the user identification. The private one is defined by the home network, is unique and has the form of a network access identifier (NAI) which is stored securely in the IMS Identity Module (ISIM). The private identity is only used for registration and not for normal SIP messages. The public identities are, as it might be guessed from the name, public and can be published. They must have the form of either a SIP URI (i.e. user@example.com) or a tel URI (+41431234567).

"IP Multimedia Services Identity Module (ISIM) is an application residing on the Universal Integrated Circuit Card (UICC), which is a physically secure device that can be inserted and removed from a user equipment." [1]. An ISIM contains six different submodules:

- Security keys (Identifiers, Integrity, Ciphering)
- Private user identity
- Public user identity
- Home network domain name (entry point of home network)
- Administrative data (manufacturer/provider specific)
- Access Rule Reference

In order to access the packet switched domain, the UICC contains a Universal Subscriber Identity Module (USIM) that includes security parameters, allowed access points and maybe applications.

### 9.4.3 Security

The IMS security module can be divided into three blocks: authentication and key agreement (AKA), network domain security and IMS security for SIP-based or HTTP-based services.

The most central part of the security in IMS is the secret key which is shared by the ISIM and the authentication centre (AUC). A random challenge (RAND) and a network authentication token (AUTN) is generated for the authentication. The ISIM verifies the AUTN and solves the RAND using its secret key and sends back the authentication (RES). On success, a pair of cipher and integrity key will be established using AKA.

Most of the transmissions in 2G networks were sent in plain text and this matter has been changed in 3G networks. With Network Domain Security (NDS), the entire IP-based traffic in the core network is protected using the mechanism of IP security (IPSec). Homogeneous security policies are used in security domains which are operated by a particular authority. Data authentication and integrity are mandatory for an exchange between components within a security domain but are only protected on the IP layer. In the event of a data transfer beyond a security domain to another, there is a need of a security gateway (SEG) that tunnels data securely into another security domain. The SEG may contain additionally packet filtering or firewall functionalities but mainly it has to encapsulate data in a security payload (ESP) which includes the entire IP datagram.

SIP is an essential part of IMS and therefore SIP signalling has to be protected. This is done with a transitive trust domain. The trust module is based on identity that is given by an established connection to another entity. Additionally, there is a privacy extension for ensuring that none of the identities is exposed to an entity outside the trusted domain. As AKA does not run directly on IP and need a transport possibility, it is obvious to use SIP.

Aside from SIP-based traffic, there is a HTTP-based traffic. It uses AKA for authentication and key agreement too and is applied between the user equipment and the Bootstrapping Server Function (BSF). Further applications can be activated using the Network Application Function (NAF) after establishing a session. Authentication is tamper-proofed by the bootstrapped session key, confidentiality and integrity by the Transport Layer Security (TLS).

### 9.4.4 IMS entry point

There are two mechanisms to discover the IMS entry point: one uses the DHCP's domain name system (DNS) and the other uses the GPRS method. "In the DHCP DNS procedure, the UE sends a DHCP query to the IP connectivity access network, which relays the request to a DHCP server. The UE can request either a list of SIP server domains names of the P-CSCF(s) or a list of SIP server IPv6 addresses of the P-CSCF(s)" [1]. In case the UE gets returned a domain name, it has to perform a DNS query to the DNS server in order to get the IP address of the entry point.

In the GPRS method, the UE activates a PDP context request to the SGSN that itself creates a PDP context request to the Gateway GPRS Support Node (GGSN). The GGSN then responds with the IP-addresses of the entry point.

### 9.4.5 S-CSCF assignment

The I-SCSF is responsible for the selection and assignment of the S-CSCF considering the required capability that is transmitted between HSS and I-CSCF within a capability attribute value pair (AVP). It contains a mandatory and optional capability attribute and a server name with a SIP URI. Based on this information the I-CSCF is able to allocate

different S-CSCF to users depending on the required capabilities. If it is not possible to meet the required capabilities, the I-CSCF applies a ”best fit algorithm” [1].

### 9.4.6 User profile

Operators need to assign a user profile for each IMS subscription. This profile can have more than one private user identity. Furthermore, a subscription may have more than one service profile that is stored in the HSS and consists of three parts: Public Identification (already described in Section 9.4.2), Core Network Service Authorisation and Initial Filter Criteria. The Core Network Service Authorisation carries media policy information that allows defining different subscriber profiles with diverse customer classes. The structure of Initial Filter Criteria involves Trigger Points and Application Servers. It is stored in the Trigger Point which indicated Application Server should be contacted.

### 9.4.7 Connectivity to non-IMS user

Most users still have a circuit-switched (CS) terminal and it is therefore preferable that IMS interwork with CS networks. There is need of converting mechanisms at the user plane and at the control plane. In the control plane, MGCF performs the mapping of SIP signalling to the call control in CS networks and in the user plane the MGW translates the two different protocols. Figure 9.7 shows an example of an IMS user calling a CS user.

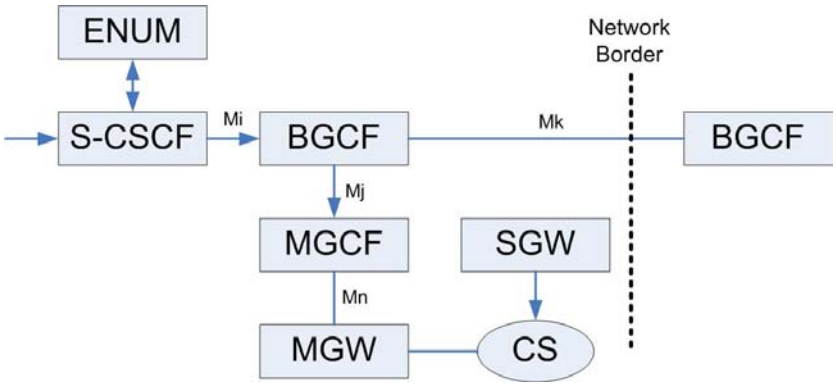



Figure 9.7: IMS-CS interworking configuration when an IMS user calls a CS user [1]

## 9.5 Protocols

This section covers the protocols that have been defined in the architecture of the IMS. At first the core protocol of IMS SIP (Session Initiation Protocol) will be described in details, which is used in the signalling or session control. In second part of this section we would describe the protocols that are used in the media plane finally the protocols that are responsible of authentication and security would be shown.

### 9.5.1 SIP (Session Initiation Protocol)

The protocol chosen by the 3GPP for the session control in the IMS is the Session Initiation Protocol (SIP). SIP is signalling protocol developed to set up, modify and tear down multimedia sessions over the Internet. It was developed by the Internet Engineering Task Force (IETF) as part of the Internet Multimedia Conferencing Architecture, and was designed to dovetail with other Internet protocols such as TCP, UDP, IP, DNS and others [15]. The SIP specification has been adopted by the IETF as "RFC 3261." As such, it is freely available to anyone to download from the IETF Web site (www.ietf.org)

SIP is a request-response protocol created to establish 'sessions' in IP network. In the present context, a session might be a simple one-to-one voice call or it could be a more complex one-to-many multimedia conference. It is similar to – and has been designed to work alongside – other internet protocols like http and SMTP. SIP effectively enables telephony functionality to be treated as just another Web application that can be integrated with other internet services.

SIP is text-based and extensible protocol that is meaning new methods and headers can be defined and easily integrated in the core protocol. Many extensions to SIP exist, and many of these extensions can be found in list of SIP-related RFCs and drafts defined by IETF.

SIP is what is known as a peer-to-peer protocol. This means that two device – or, more precisely, endpoints – can communicate without any intervening infrastructure. However, peer-to-peer SIP does not work well if multiple, complex services are supported solely in end devices. This is partly because of bandwidth restrictions associated with the devices, but also because with service like voicemail, the network needs to provide service even when the device is unavailable – i.e., when it is switched off or out of coverage. As a result, SIP needs what are known as proxy and registrar elements to control how complex communication is handled. In the following sections we will analyze SIP main components in general and then show how they are used in IMS network.

#### SIP Components

According to SIP definition it is a signalling protocol. As the name implies, the protocol allows two ends-points to establish media sessions with each other. The main functions [15] of signalling protocols are

- Location of an end-point;
- Contacting end-point to determine willingness to establish a session;
- Exchange of media information to allow session to be established;
- Modification of existing media sessions;
- Tear-down of existing media sessions.

In order to implement these functionalities, there are different SIP components. There are three main elements, user agents (UA), SIP Gateways and SIP servers. In following subsections we will analyze each element in details.

**SIP User Agents**
A SIP-enabled end-device is called a SIP user agent (UA) [15]. The main purpose of SIP is to enable sessions to be established between user agents. As the name implies, a user takes direction or input from a user and acts as an agent on their behalf to set up and tear down media sessions with other user agents. UAs traditionally use TCP (Transmission Control Protocol)[3] and UDP (User Datagram Protocol)[4] port to connect to SIP servers and other SIP endpoints. Since SIP may be used with any transport protocol, there is no requirement that a UA must support either TCP or UDP for message transport.

There are tow different parts of User Agent, User Agent Client (UAC) and User Agent Server (UAS). An UAC is logical entity, which sends SIP requests and receives answers to those requests. An UAS is a logical entity that sends answers to SIP requests. Both entities are in every user agent, to allow the communication between different user agent.

A SIP user agent implementation must at least include support of the methods INVITE and ACK (They will be described in next sections) and be able to interrupt any unknown response. It must also support SDP (Session Description Protocol) for media description. Details of SDP are in following section.

**SIP Gateways**
A SIP gateway is an application that interfaces a SIP network to a network utilizing another signalling protocol. In terms of the SIP protocol, a gateway is just a special type of user agent, where the user agent acts on behalf of another protocol rather than human [15]. A gateway terminates the SIP signalling path and can also terminate the media path, although this is not always the case.

Another difference between a user agent and gateway is the number of the users supported. While a user agent typically supports a single user. A gateway can support hundreds or thousands of users.

**SIP Servers**
SIP servers are applications that accept SIP requests and respond to them. The types of SIP servers are logical entities. Actual SIP server implementations may contain a number of server types, or may operate as a different type of server under different conditions. Because servers provide services and features to user agents, they must support both TCP and UDP for transport. Note that the protocol used between a server the location service or database is not general SIP. The figure 9.8 shows the interaction of user agents, servers, and a location service.

**Proxy Servers**
A SIP proxy server is an intermediate entity that receives a SIP request from a user agent acts on behalf of the user agent in forwarding or responding to the request. This server has a similar functionality to an HTTP Proxy. It has the task of routing the requests that receive from other entities. In order to process this task SIP proxy server typically has access to a database or a location service to aid it in processing the request (determining

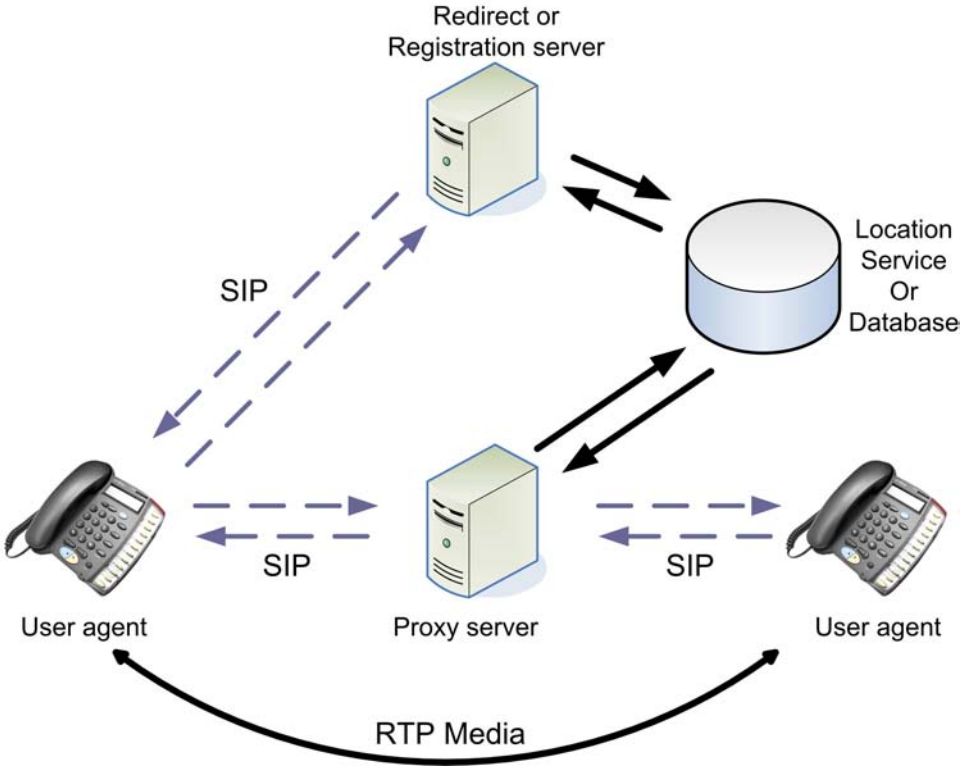



Figure 9.8: SIP user agent, server, and location service interaction [15]

next hop). The interface between the proxy and the location service is not defined by the SIP protocol. There are two types of Proxy Server: Stateful Proxy and Stateless Proxy.

**Stateless Proxy** : A stateless proxy server does not keep the state of the transaction during the requests processing, Once the message has been parsed, processed, and forwarded or responded to, no information about the message is stored no call leg information is stored. It never retransmits a message, and does not use any SIP times. A stateless proxy has no memory of any request or response it has sent or received.

**Stateful Proxy** : A stateful proxy server keeps track of requests and responses received in the past and uses that information in processing future requests and responses. There is a type of stateful proxy server with ability of forwarding a request to a number of locations at the same time. This forking proxy server keeps track of each of the outstanding requests and response to each, as shown in Figure 9.9.

To handle a TCP request from a user agent the proxy must be stateful, since a user agent will assume reliable transport and rely on the proxy for retransmissions on any UDP hops in signalling path.

**Redirect Servers**
A redirect server redirects the request back to the user agent indicating that the user agent needs to try a different route to get to the recipient. It generally happens when a

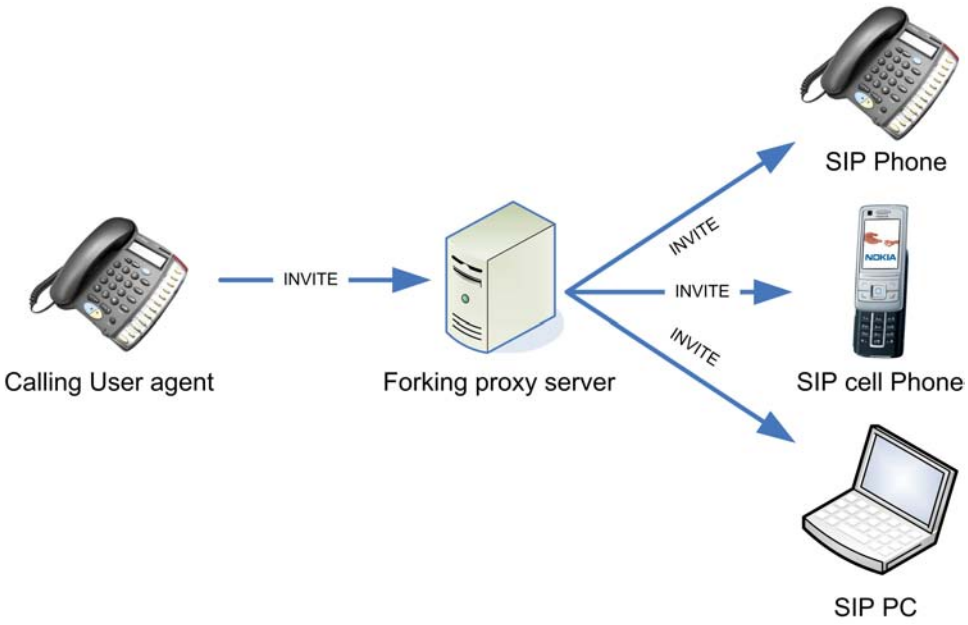



Figure 9.9: Forking proxy operation [15]

recipient has moved from its original position either temporarily or permanently. Like a proxy server, a redirect server uses a database or location service to look up user.

**Registration Servers**
As discussed in the previous section the proxy server finds the address of recipient by accessing a specified database. This address is stored in the database by a server that is called Registration Server. A user agent sends a SIP REGISTER request to the SIP registrar server. The SIP registrar server receives the message and knows as a result the IP address of the user agent. It stores the SIP URL and the IP address of the sender in the database. Registration is not required to enable a user agent to use a proxy server of outgoing calls. It is necessary for a user agent to receive incoming calls from proxies that serve it.

### Transmission of SIP messages using UDP and TCP

In the Internet Multimedia Protocol stack [15] Figure 9.10 SIP is a layer four, or application layer, protocol. It can use either TCP or UDP for transport layer, both of which use IP for Internet layer.

**UDP Transport** : By using UDP, each SIP request or response message is usually carried by a single UDP datagram or packet. Most SIP messages easily fit in a single datagram. The lack of handshaking or acknowledgment in UDP transport means that a datagram could be lost and a SIP message along with it. The checksum , however, enables UDP to discard errored datagrams, allowing SIP to assume that a received message is complete and error-free.

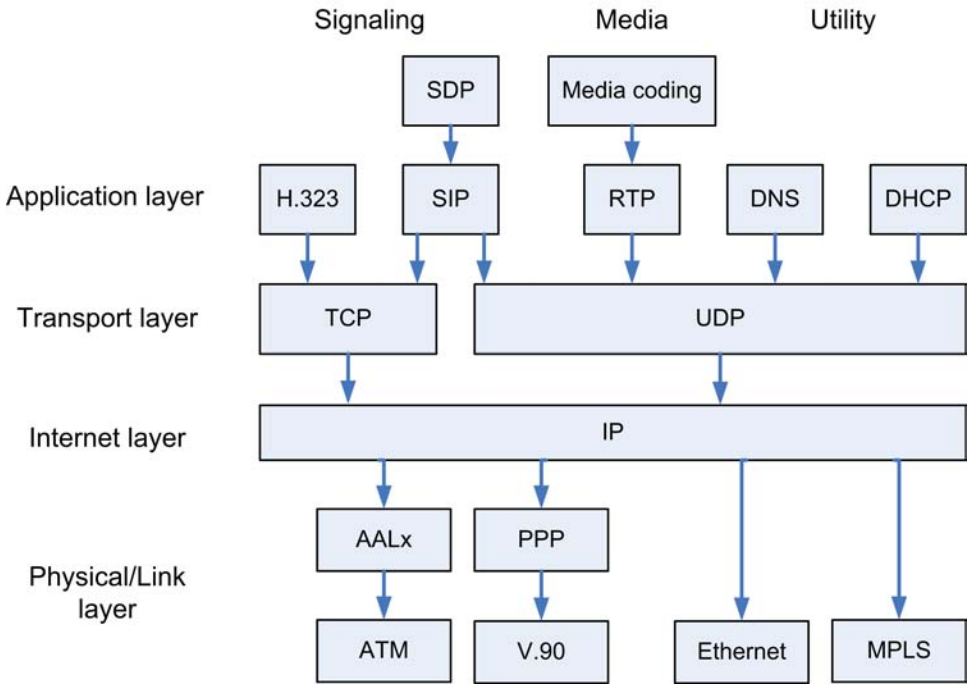



Figure 9.10: The Internet Multimedia Protocol stack [15]

**TCP Transport** : By using TCP, the transmission is reliable, but at a cost of complexity and transmission delay over the network.

### SIP Messages

There are tow types of messages that are used in SIP to establish a connection between end-devices. The types are request (methods) and response messages. The base SIP specification defines several mechanisms through which the protocol can be extended. This allows designers to add new feature, such as call transfer or message waiting indicator, as they become necessary. Each SIP-based implementation needs to support base methods, and then implement whichever feature extensions they intend to use. SIP can be extended in three major ways [16]:

- By defining new message body types
- By defining new headers.
- By defining new message types

### SIP request messages

SIP request messages are called methods too and considered ”verbs” in the protocol, because they request a specific action to be taken by another user agent or proxy server. There are six original methods described in the SIP specification document in version 2.0 of SIP. The basic or original methods are INVITE, REGISTER, BYE, ACK, CANCEL,

and OPTIONS. The INFO and PRACK methods are described in separate Internet-Drafts that are likely to became RFCs in the near future.

The base methods of SIP are summarized below. For complete description of these methods the reader is referred to [15].

**INVITE :** The INVITE method is used to establish media sessions between user agents. Responses to INVITEs are always acknowledged with ACK method. Its body contains the media information of the caller and quality of service (QoS) or security of information.

**REGISTER:** The REGISTER method is used by a user agent to notify a SIP network of its current IP address and the URLs for which it would like to receive calls.

**BYE:** The BYE method is used to terminate an established media session.

**ACK:** The ACK method is used to acknowledge final response to INVITE requests.

**CANCEL:** It is used to terminate pending searches or call attempts. It can be generated by either user agents or proxy servers.

**OPTIONS:** It is used to query a user agent or server about its capabilities and discover its current availability.

However there are additional methods that can be used. For example INFO, SUBSCRIBER, etc. (published in other RFCs)

**SIP response messages**
A SIP response is a message generated by a user agent server or SIP server to reply to a request generated by a user agent client. Responses are numerical and are classified by the first digit of the number. For example the 180 Ringing is an informational class response, identified by the first digit a 1.

There are six classes of SIP responses. The first five classes were extended from HTTP; the sixth was created for SIP. The classes are shown in Table 9.1 for complete description of these classes the reader is referred to [15].

**SIP Headers**

Headers are used to transport the information to the SIP components. They can be used in compact form. SIP headers in most cases follow the same rules as HTTP headers. Headers are defined as header : field where header is case-insensitive token used to represent the header, and field is case-insensitive set of tokens that contain the information. The main headers are shown in the table 9.2.

Table 9.1: SIP Response Classes

| Class | Description | Action |
|---|---|---|
| 1xx | Informational: Indicates status of call prior to completion, also called provisional | If first informational response, the client should switch from timer T1 to timer T2 for retransmission. |
| 2xx | Success: request has succeeded | If for an INVITE, ACK should be sent; otherwise, stop retransmission of the request |
| 3xx | Redirection: server has returned possible locations | The client should retry request at another server |
| 4xx | Client error: the request has failed due to an error by the client | The client may retry the request if reformulated according to response |
| 5xx | Server failure: The request has failed due to an error by the server | The request may be retried at another server |
| 6xx | Global failure: the request has failed | The request should not be tried again at this or other servers |

#### SIP Addressing

In general, the caller does not directly know the IP address of the target to send the INVITE to him. An IP address cannot be used like a telephone number. One reason is that IP addresses are often dynamically assigned due to the shortage of IP version 4 addresses. Ideally, there would be one address that would identify client wherever it is. In fact, there is an Internet Protocol that does exactly that, with e-mail. SMTP uses a host or system independent name (an e-mail address) that does not correspond to a particular IP address.

SIP use e-mail like names for addresses. SIP uses URLs like most Internet protocols. SIP URLs can also handle telephone numbers, transport parameters, and a number of other items. They are used in a number of places including the To, From and Contact headers, as well as the Request-URI, which indicates the destination. An example SIP URL contains the schema sip a ":", then a user-name@host or IPv4 address followed by an optional ":", then the port number, or a list of ";" separated URI parameters [15]:

*sip:joesph.fourier@transform.org:5060;transport=udp;user=ip;method=INVITE;*

*ttl=1;mddr=240.101.102.103;Subject=FFT*

### 9.5.2 Use of SDP in SIP

SIP uses Session Description Protocol to describe the media content of the session. SDP contains the following information about the media session [15]:

- IP Address (IPv4 address or host name);
- Port number (used by UDP or TCP for transport);

Table 9.2: SIP Main Headers

| **Header** | **Description** |
|---|---|
| Call-ID | Unique identifier for each calls and contains the host address. It must be the same for all the messages. |
| Via | Shows the transport protocol used and the request route, each proxy adds a line to this field |
| From | Shows the address of the caller |
| To | Show the address called user of the request. |
| Cseq | begins with a random number and it identifies in a sequential each message. |
| Contact | shows one (or more) address than can be used to contact the user |
| User Agent | The client agent who deal the communication. |

- Media type (audio, video, interactive whiteboard; etc.);
- Media encoding schema (PCM A-Law, MPEG II video, etc).

SDP is intended for describing multimedia sessions for the purpose of session announcement, session invitation, and other forms of multimedia session initiation. The default message body type in SIP is *application/sdp*. The caller lists the media capabilities that it is willing to receive in SDP in either an INVITE or in ACK. The target lists its media capabilities in 200 OK response to the INVITE.

#### Use of SIP By IMS

To use SIP in IMS network, its specification has to be extended, therefore; new extensions have been defined to headers and parameters to address the specific needs of telecommunications operators. Table 9.3 shows the new parameters that have been added to SIP.

IMS architecture has introduced several Private Headers (P-Headers) into IETF to meet telephony needs. P-Headers are optional extensions to SIP. Table 9.4 shows an overview to this header. For more details the reader is referred to [19].

### 9.5.3 Media Plane Protocols

This section covers some overview of protocols used in IMS architecture to enable the transport of real-time packets containing voice, video, or other information over IP.

Table 9.3: SIP extension regarding parameters [18].

| Parameter | Description |
|---|---|
| auth-param | It is WWW-authenticate header, which is used to pass the Integrity Key and Cipher Key during the registration process that sets up the integrity protected relationship between the UE and P-CSCF. |
| tokenized-by | It is used to carry encrypt/decrypt strings within the SIP headers to implement the I-CSCF THIG function |
| icn-charging-info | It is defined for P-Charging-Vectorheader, which is used to include IP Connectivity Network charging information. |
| – | New parameter defined for P-Access-Network-Info, which provides information on the access network serving the UE. |

Table 9.4: Private Header (P-Header) Extensions SIP for 3GPP

| Header Field | Use |
|---|---|
| P-Associated-URI | Lists other URIs associated with the user |
| P-Called-Party-ID | Lists the URI of the called party |
| P-Visited-Network-ID | Identifies the visited network |
| P-Access-Network-Info | Identifies the access network |
| P-Charging-Function-Addresses | Contains charging information |
| P-Charging-Vector | More charging information |

### RTP (Real-time Transport Protocol)

The Real-time Transport Protocol (or RTP) defines a standardized packet format for delivering audio and video over the Internet. It was developed by the Audio-Video Transport Working Group of the IETF and first published in 1996 as RFC 1889 [Schulzrinne]. As shown in the protocol stack of the Figure 9.10, RTP is a layer four, or application layer, protocol that uses UDP for transport over IP. RTP is not text encoded, but uses a bit-oriented header similar to UDP and IP. RTP is always used in combination with RTCP (RTP Control Protocol), which provides statistics and information about the media stream.

RTP allows for the detection some of problems introduced by an IP network. In Table 9.5 the problems with their detecting methods used by RTP are listed. RTP allows detection of these problems but leaves it up to the codec to deal with the problem.

Once the session between tow end-devices is established using SIP, the information needed to select codecs and send the RTP packets to the right location is carried in the SDP message body.

Table 9.5: RTP detection methods

| **Problems** | **Detecting method** |
|---|---|
| Packet loss | It can be detected by a gap in the *Sequence Number* field |
| Variable transport delay | It can be detected by the *Time Stamp* field |
| Out of sequence packet arrival | It can be detected by out-of-sequence *Sequence Number* |

#### RTP Control Protocol (RTCP)

The RTP Control Protocol (RTCP) is related protocol also defined in RFC 1889 that allows participants in a RTP session to send each other quality reports and statistics [15]. The Quality of Service (QoS) statistics can be generated by using RTCP to report the peer entities.

The most important use of RTCP is to perform the mapping between the RTP timestamps and a reference a clock. Using this reference clock enables the receivers to perform media synchronization such as co-relating audio and video packets so that both are played back at the same instance. This important in video conferencing application [17].

#### Common Open Policy Service Protocol

IMS uses the IETF's Common Open Policy Service protocol to ensure quality of service, which is important for telephony and other traffic that doesn't tolerate latency. COPS enables the communication of QoS and other traffic policy information between a policy server and clients. This protocol is used in *Go* reference point, that interests to ensure that the QoS and source and Destination addresses of the intended IMS media traffic matches the negotiated value in IMS level.

### 9.5.4 Authentication and security protocols

#### DIAMETER

Diameter is an authentication, authorization and accounting (AAA) protocol developed by the Internet Engineering Task Force. Diameter is used to provide AAA services for the range of access technologies [1]. IMS's home subscriber server (HSS) is the system's master database of information about subscribers, including their names and locations, services they have permission to access, and data to be used with the authentication and authorization processes. IMS uses the IETF's Diameter protocol to let devices access the HSS and then provide the necessary authentication, authorization, and, for billable communications, accounting services.

## 9.6 Service Examples

### 9.6.1 Push-To-Talk

Push-To-Talk (PTT) is a service that allows sending a time-limited voice message to other users like a walkie-talkie. Users can press and hold a button and speak to one person or even an entire group, but only one person can talk at a time because PTT is a half-duplex service.

PTT does not require any new radio technologies and will therefore be one of the first IMS-based services provided by operator. At the beginning, there were several different incompatible types of specifications and it was not possible to interoperate with devices from different vendors. Ericsson, Motorola, Nokia and Siemens eventually teamed up and created a standard called Push-To-Talk over Cellular (PoC) [2].

In charge of a standardisation of PTT for IMS is the Open Mobile Alliance (OMA) which was provided the PoC specification. OMA published the first version of their specification in April 2005. At the same time IETF is amending the SIP architecture in order that a complete Push-To-Talk service is possible with IMS.

In a technical point of view PTT works similar like Voice-over-IP. A PoC session has to be established using SIP and then the PoC performs floor control and media distribution. Voice packets, so-called ”talk bursts”, are transmitted by RTP. Even when only two people are connected, the media path traverses the PoC server which allows buffering the media packets. This is called the early media service which is on one hand good at reducing delays; on the other hand it causes problems if the terminating user is not reachable. In this case PoC has to interrupt the user while they are speaking to inform about the failure of delivery.

Another Problem that OMA faces is the assumption of PoC that all users are connected to the same PoC server. In terms of charging it is easier for operators to have an own PoC and therefore a multi-operator architecture is needed which causes challenges regarding floor control in distributed environments.

### 9.6.2 Real-time Video Sharing

Real-time video sharing is a SIP-based multimedia streaming and peer-to-peer service that works with both circuit- and packet-switched connections. It offers the possibility to exchange video clips or live videos simultaneously with an IMS packet-switched connection during a normal circuit-switched call. This service enables spontaneous sharing of experiences, surroundings and information [12].

### 9.6.3 Interactive Applications

Interactive gaming in the internet is already very popular these days and so are downloads of Java-based games for mobile devices. It is self-evident that the demand of interactive gaming against other mobile users will increase rapidly as soon as operators provide this feature. IMS makes this service available. Users can establish an interactive gaming session over an IP multimedia core to other mobile users and play against them [12].

Another possibility of interactive applications is the sharing of personal data, as that of calendar information, contact details and other files.

### 9.6.4 Instant-/ voice messaging

Instant messaging is a communication service that makes written conversations happen in near-realtime. This service is actively used in private life as well as in business. Not only can the message contain text but also pictures, video files or any other generic file. There are two different modes of instant messaging: pager-mode and session-based [1].

The pager-mode has been included in the Release 5 from 3GPP and uses the method MESSAGE. This kind of instant messaging is mainly used for sending messages from the Application Server (AS) or other components in the IMS to an IMS terminal. Session-based instant messaging was defined in Release 6 and can be used for messages from a IMS terminal to another or several other terminals. An IMS terminal can set up a session to another terminal with an INVITE request via the regular IMS nodes. As soon as a session is established, messages can be sent between end points using the Message Session Relay Protocols (MSRP) [2].

Voice messaging is similar to instant messaging with the difference that the content is an audio file. User can record a message with their mobile devices or use an existing one and send it to one or several recipient. This form of a message is much faster then type in the message on a mobile phone and it is even a more personal message [12].

### 9.6.5 Video conferencing

For a video conference within IMS we need a conference bridge service that extends the point-to-point into a multi-point service. Every participating mobile device is connected via the conference bridge service which neglects the underlying infrastructure and takes for granted that the connections are provided by the appropriate standard [12].

There are two different ways to create a conference, the one that uses SIP is set up ad-hoc without a schedule and does not last for long. On contrary, the scheduled ones use the conference policy control protocol (CPCP) that gives more control for the creator of the conference. Each conference has a unique URI which represent the conference policy. The client-server protocol CPCP can be used to manipulate the rules defined on the conference policy server, such as lifespan, available roles and membership policies [1].

## 9.7 Summary

The architecture and all standards, on which IMS is based, were defined and have been extended step by step by 3GPP. There are many improvements within IMS. Not only are these improvements interesting for network operators, but also for end users. Innovations were made in the area of quality of service, in new charging methods, in IP-based networks, in access independence and in the collaboration between different systems. The entire IMS architecture is divided into three different layers. The transport layer controls all kind of accesses and communication in IMS. The actual IMS layer combines all functionalities needed for operating a service. The

third layer contains all service and application elements that are required for a provision of novel services.

The protocols that have been defined in the architecture of the IMS are SIP, RTP/RTCP, COPS and Diameter. SIP is a signaling and control protocol, which is used in IMS networks to establish, modify and terminate multimedia sessions. In order to use SIP in IMS networks, new headers named P-Headers and parameters have been defined. SDP is used for describing media sessions. IMS uses RTP to delivery real time media such as audio and video using UDP as the transport protocol. RTCP and COPS are used to ensure quality of service. Diameter protocol provides the IMS with necessary authentication, authorization, billing communications and accounting services.

IMS enables services that have not been possible with mobile devices before. These are for example Push-to-Talk for a kind of walkie-talkie communication with mobiles, real-time video sharing, interactive applications, instant messanging or video conferencing.

As already mentioned, IMS is very flexible in access independence thanks to its modular design. It is possible to continue using an older infrastructur of a mobile network operator without building a completely new network. The question comes up whether such a heterogenous is reasonable or if it would have been better to create a completely new modern system. In an economic point of view is the given IMS type the best solution for both user and network operator. Users can still use their current mobile devices and do not need specific devices. IMS providers can integrate their existing infrastructure into IMS and can reach the break-even point sooner. Time will tell how long it will take until the majority of providers have changed to IMS. Ideas for new services will not run out quickly.

# Bibliography


[1] Poikselkä, M.; Mayer, G.; Khartabil, H.; Nierni, A.: The IMS – IP Multimedia Concepts and Services in the Mobile Domain, John Wiley & Sons, 2004.

[2] Camarillo, G.; Garcia-Marin, M.A.: The 3G IP multimedia subsystem (IMS), Wiley, 2004.

[3] El-Malki, K.: Mobile Multimedia Opportunities (IMS) and IPv6-IPv4 Interworking, Ericsson, http://www.sicta.ch/files/pdf134.pdf, 07.06.2006.

[4] Motorola: Motorola IP Multimedia Subsystem, Motorola, http://www.motorola.com/networkoperators/pdfs/new/IMS-WhitePaper.pdf, 05.06.2006.

[5] Nokia: White Paper – IP Convergence Based On SIP, Nokia, http://sw.nokia.com/id/d9589d7d-ee9d-4d16-8419-b339c01ad37a/White_Paper_IP_Convergence_Based_On_SIP_v1_0_en.pdf, 05.06.2006.

[6] Wikipedia: IP Multimedia Subsystem, Wikipedia, http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem, 05.06.2006.

[7] Bannister, J.; Mather, P.; Coope, S.: Convergence Technologies for 3G Networks, John Wiley & Sons, 2004.

[8] Drempetic, T.; Rihtarec, T.; Bakic, D.: Next Generation Networks Architecture For Multimedia Applications, 4th EURASIP Conference, http://ieeexplore.ieee.org/iel5/8652/27422/01220523.pdf?arnumber=1220523, 06.06.2006.

[9] 3GPP: TS 23.228 V6.6.0, 3GPP, http://www.3gpp.org, 21.06.2004.

[10] 3GPP: TS 23.221 V5.11.0, 3GPP, http://www.3gpp.org, 27.09.2004.

[11] 3GPP: TS 32.200 V4.5.0, 3GPP, http://www.3gpp.org, 02.10.2003.

[12] 3G Americas: IP Multimedia Subsystem IMS – Overview and Applications, 3G Americas, http://www.3gamericas.org/pdfs/ims_july2004.pdf, 06.06.2006.

[13] Lainé, Ph.; Drevon, N.; Cannet, J-M.: White Paper – CONVERGED MULTIMEDIA COMMUNICATIONS, Alcatel, http://www.alcatel.com/doctypes/articlepaperlibrary/pdf/ATR2005Q1/A0503-Telephony_models-EN.pdf, 06.06.2006.

[14] Cisco: Cisco Service Exchange Framework: Supporting the IP Multimedia Subsystem, Cisco, http://www.cisco.com/en/US/netsol/ns549/networking_solutions_white_paper0900aecd80395cb0.shtml, 06.06.2006.

[15] Johnston, A.B.: SIP: Understanding the Session Initiation Protocol, Artech House, 2004 (2nd Edition).

[16] Galindo, L.A.: Interworking of IP Multimedia Core Networks between 3GPP and WLAN, IEEE Wireless Communication, June 2005.

[17] Koukoulidis, V.; Shah, M.: The IP Multimedia Domain in Wireless Networks – Concepts, Architecture, Protocols and Applications, IEEE Sixth International Symposium on Multimedia Software Engineering, 13-15 Dec. 2004 Pages 484 - 490.

[18] Knightson, K.; Morita, N.; Towle, T.: NGN Architecture: Generic Principles, Functional Architecture, and Implementation. IEEE Communications Magazine, Volume 43, Issue 10, Oct 2005 Pages 49-56.

[19] Garcia-Martin, M., E. Henrikson, and D. Mills, Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP), RFC 3255, 2003.

[20] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson: RTP A Transport Protocol for Real-Time Applications, Lawrence Berkeley National Laboratory January 1996: RFC 1889.

# Kapitel 10

# Sicherheit in Peer to Peer Netzwerken

*Amir Sadat, Christoph Gow, Adrian C. Leemann*

*Peer to Peer Systme gewinnen im professionellen Umfeld immer mehr an Bedeutung. Breite Anwendungsfelder werden von der Technologie erschlossen. Unter anderem auch Einsätze in sensitiven Bereichen, die neue sicherheitstechnische Anforderungen stellen. Im Folgenden wird nach einer kurzen Einführung in verschiedenen Peer to Peer Systeme auf mögliche sicherheitskritische Schwächen und auf Verwundbarkeiten der verschiedenen Peer to Peer Architekturen eingegangen. Denkbare Attacken werden beleuchtet und mögliche Lösungsansätze oder Gegenmassnahmen diskutiert.*

## Inhaltsverzeichnis

**10.1 Peer to Peer Netzwerke – Möglichkeiten und Ausprägungen 311**
10.1.1 Einleitung . . . . . 311
10.1.2 P2P Systeme, eine Plattform für Piraterie? . . . . . 312
10.1.3 Vor- und Nachteile von Peer to Peer Systemen . . . . . 313
10.1.4 Business Tauglichkeit von Peer to Peer Netzwerke . . . . . 314
**10.2 Aufbau von Peer to Peer Systemen . . . . . 315**
10.2.1 Die klassische Client/Server Architektur . . . . . 316
10.2.2 Peer to Peer Architekturen . . . . . 317
10.2.3 Unstrukturierte Peer to Peer Netzwerke . . . . . 317
10.2.4 Strukturierte Peer to Peer Netzwerke . . . . . 320
**10.3 Sicherheitsbedrohungen in Peer to Peer Netzwerken . . . . . 323**
10.3.1 Angriffe auf Peer to Peer Systeme . . . . . 324
**10.4 Beispiele . . . . . 336**
10.4.1 Data Backup Service . . . . . 336
10.4.2 File Storage Service . . . . . 338
**10.5 Fazit Sicherheit in Peer to Peer Netzwerke . . . . . 338**

# 10.1 Peer to Peer Netzwerke – Möglichkeiten und Ausprägungen

## 10.1.1 Einleitung

Peer-to-Peer (P2P) Systeme, von der Film- und Musikindustrie als grosse Bedrohung dargestellt, nehmen heutzutage im legalen Sektor einen immer höheren Stellenwert ein. Mit dem Wegkommen vom teils illegalen Filesharing hin zur Netztechnik der Zukunft müssen Sicherheitsaspekte solcher Systeme neu gewichtet werden. Einerseits arbeiten die Programmierer der Tauschbörsen daran, ihre Netzte sicher gegen Infiltration aus dem Anti-Piraterie-Lager zu schützen, andererseits erkennen renommierte Softwarehersteller auch das Potential von P2P für die Geschäftswelt. Dadurch steigen die Anforderungen bezüglich Sicherheit solcher Systeme gegen böswilligen Einfluss Dritter. Hier tauchen neue Probleme auf, mit denen man sich bis anhin nicht bewusst auseinandergesetzt hatte.

Als brisantes Beispiel kann man sich die Verwendung von P2P Systeme im medizinischen Bereichen vorstellen. Es kursieren Ansätze um Spitäler und Ärzte global zu verbinden. Ziel wäre es, jederzeit und von überall, auf relevante Daten des Patienten wie beispielsweise Krankengeschichte, Röntgenbilder etc. zugreifen zu können. Dies wäre sicherlich auch im Client Server Betrieb mit einer zentralen Verwaltungsstelle denkbar, aber in Anbetracht der enormen Datenmenge wohl eher unrealistisch. Schweizer Spitäler würden bloss durch Röntgenbilder eine Datenmenge von ca. 0.7TB anhäufen.[1] Hier würde ein hoher Datenverkehr produziert und somit Backups erschwert, was über eine P2P-Lösung elegant umgangen werden könnte. Im Falle, dass der Patient den Spital wechseln müsste, könnte das Pflegepersonal im P2P-Patiententennetzwerk die benötigte Historie suchen und von den Peers (anderen Spitälern, dem Hausarzt, Spezialisten etc.) laden. Hier müssen Sicherheitsbedenken geäussert werden, denn beispielsweis könnten die Krankenkassen sehr an diesen Daten interessiert sein um gewisse risiko Patienten aus ihrem Kundenstamm zu eliminieren.

Die folgende Arbeit versucht Bedrohungen und Massnahmen auzuzeigen, welche heutzutage in P2P Systemen vorkommen oder in Zukunft zu erwarten sind.

In einem ersten Schritt wird die Entstehung von Peer-to-Peer und der sich vollziehende Wandel von Tauschbörsensoftware hin zu einer zukunftsweisenden Möglichkeit, Dateien zu verwalten beleuchtet. Ein grösserer Abschnitt führt in die verwendeten Techniken ein und bildet die Grundlage um P2P spezifische Sicherheitsbedenken und Gefahren verstehen zu können. Konkret werden im Anschluss Schwachstellen aufgezeigt und Lösungsansätze diskutiert. An praxisorientierten Beispielen werden abschliessend deutlich gemacht wie verwundbar ein P2P System in den verschiedenen Stadien der Entwicklung (Startphase, Wachstumsphase, Sättigung) ist und wie dem entgegen gewirkt wird.

[1] Bsp. Annahme von 168'937 Patienten am Inselspital Bern müssen bei jedem 5. ein bis drei Röntgenbilder von ca. 2Mb angefertigt werden.

### 10.1.2 P2P Systeme, eine Plattform für Piraterie?

Peer to Peer, ein äusserst negativ behaftetes Wort für die meisten, die sich nicht mit dem Thema auseinandergesetzt haben. Schlagzeilen wie 'Die Musikindustrie verzeichnet jedes Jahr einen Verkaufsausfall von Milliarden aufgrund Filesharing über das Internet.' oder 'Neuster Kinofilm zwei Wochen vor Premiere bereits im Internet verfügbar.' sind massgebend für diesen schlechten Ruf verantwortlich. Gemäss einer Studie [1] im Auftrag der MPAA (Motion Picture Association of America [2]) verzeichnete Hollywood im Jahre 2005 einen geschätzten Ausfall von 6.1 Milliarden US-Dollar durch Piraterie. Ein enormer Anteil dieses Verlustes entsteht aber durch private Kopien von gekauften DVDs. So tritt z.B. in der Studie nach den USA, Mexiko an zweiter Stelle als Verursacher von 488 Mio. US-Dollar Verlust auf. In Anbetracht der technischen Gegebenheiten, ist es schwer denkbar, dass die Mexikaner sich alle diese Filme aus dem Internet herunterladen. Die nötige Infrastruktur, wie schnelle DSL-Zugänge und die benötigte Hardware ist nicht verfügbar oder von der Bevölkerung nicht zu erstehen. Nur für ca. 5 Prozent der Bevökerung ist das Inernet zugänglich [5]. Noch erstaunlicher ist, dass Schweden, welches als Filesharing Hochburg der Welt gilt, nicht in den Top 8 vertreten ist. Nichtsdestotrotz wird mit aller Kraft an Gesetzten und Massnahmen gegen P2P Benutzer gearbeitet. Abzustreiten sind diese unglücklichen Auswüchse natürlich nicht, jedoch wäre es einen Fehler, die P2P Technik an und für sich als diabolisches Werk zu brandmarken. Wie viele andere Techniken ermöglicht P2P Handlungen, welche sich im juristischen Grenzbereich befinden. Niemand käme beispielsweise auf die Idee, die GSM Technik zu verunglimpfen, da sie die Koordination im organisierten Verbrechen erheblich erleichtern kann.

Bekannt wurde die P2P Technologie, und somit auch das Filesharing, durch das Programm Napster [3] im Jahre 1998. Die Software durchkämmte den Computer auf dem Sie installiert wure nach MP3 Songs und sandte die Kataloginformationen an die Datenbank des Napster Servers. An letzteren konnten die Nutzer Suchanfragen stellen und bei einem Treffer die IP Adressen des MP3 - File 'Besitzers' in Erfahrung bringen. Nun konnte direkt (Peer - to - Peer) das gewollte File getauscht werden. Die Napster 'Gemeinde' wuchs rasant und erreichte kurz vor der Abschaltung fast 38 Millionen Nutzer. Zweifellos haben P2P Systeme, ja vielleicht sogar P2P als modernes Konzept des 21. Jahrhunderts, ihren Aufschwung diesem massenfähigen Pionier zu verdanken. Die RIAA (Recording Industry Association of America [4] ), gestärkt von der Band Metallica war mit den Tätigkeiten von Napster jedoch alles andere als einverstanden und wurden Anfang 2000 mit ihren Anwälten vorstellig. Schliesslich meldeten immer mehr Musiker ihre Einwände und die Server von Napster mussten vom Netz genommen werden. Der zentrale Server erwies sich als 'Schwachstelle', denn er war direkt angreifbar, bzw. einklagbar.

Es dauerte nicht lange bis findige Köpfe ein Nachfolgeprodukt präsentierten. Die Richtung zu einer dezentralen Lösung der Suchserver lag nahe und so wurde das Gnutella, das eMule [6] und das KaZaA - Netzwerk [7] ins Leben gerufen.

Im Monat Mai des Jahes 2006 betrug die durchschnittliche Partizipation am eMule Netzwerk ca. 4 Mio. Peers. Eine kontinuirliche Zuhname zeichnet sich trotz aller Bestreben der Gesetzgeber und Industrien deutlich ab. [8]

Auch im 'legalen' Bereich wurde kräftig an der P2P Technologie geforscht. Der MSN Mes-

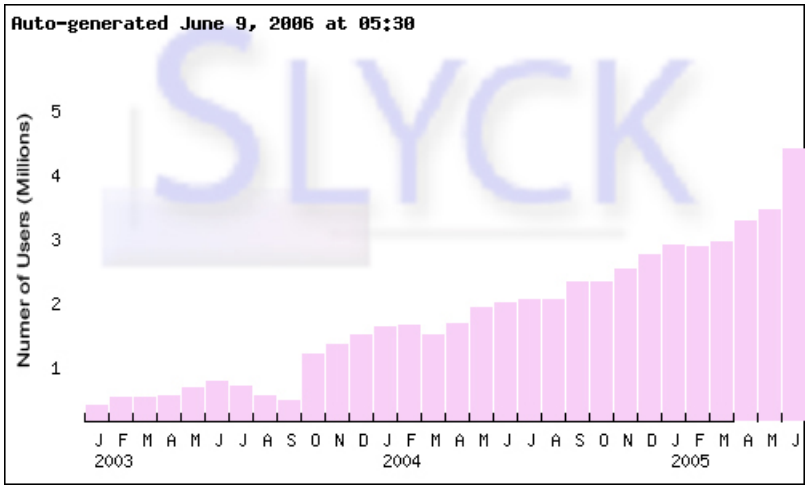



Abbildung 10.1: aktuelle eMule Peer Statistik, [8]

senger oder die allseits bekannte Internet - Telefongesellschaft Skype [9] verwenden P2P Grundlagen der sogenannten 'Dritten Generation' für ihre Dienste. Die Technik ist aber nicht unumstritten und viele Firmen verbieten z.B. ihren Mitarbeitern die Verwendung von Skype. Verfügt die Firma über hohe Internetbandbreiten und eine ungenügende Firewall, dann werden die einzelnen Skype Peers schnell zu sog. Supernodes erkoren, die für Suchanfragen und Weiterleitungen 'missbraucht' werden.

### 10.1.3 Vor- und Nachteile von Peer to Peer Systemen

In gewissen Anwendungsgebieten zeigt sich bereits heute, dass der Client - Server Betrieb nicht für alle Zeit bestehen wird, da die Architektur anfällig auf Flaschenhälse ist und immer öfter an ihre Grenzen stösst. Speicherplatz und Bandbreite wachsen zwar kontinuierlich, jedoch zu langsam um mit den interessanten Neuerungen und revolutionären Anwendungen Schritt halten zu können.

Für die P2P Architektur spricht unter anderem, dass äusserst geringe Eintrittsbarrieren bestehen um an einem Netzwerk teilnehmen zu können. Die Partizipation und auch das Verlassen des Netzwerks verlaufen relativ unkompliziert und beeinträchtigen die Funktionalität des Systems im Normalfall nicht. Mit P2P ist die Möglichkeit gegeben auf einen ungeheuren Informationsreichtum zuzugreifen. Es ist denkbar, dass Bibliotheken ihre Inhalte in einem einzigen, grossen P2P Netz zusammenführen und zur Verfügung stellen, gegebenenfalls als kommerziellen Dienst. Somit könnte man äusserst schnell und effizient enorme Datenbestände durchforsten und sich die Ergebnisse auch noch lokal herunterladen.

Mit dem verteilten Ansatz kann oftmals auf hochperformante Server verzichtet werden, da die Such- und Indexierungsaufgaben auf die angeschlossenen Desktoprechner verteilt werden. Serveradministratoren, spezielle Serversoftware und Wartung der Systeme entfällt komplett, was riesige Kosteneinsparungen ermöglicht. Der grösste Vorteil erwächst dementsprechend durch das Teilen von Ressourcen und der Ressourcenlast. Ein Rechner, der momentan keine Arbeit verrichtet, oder über genügend freie Prozessorkapazität

verfügt kann in einem P2P Netzwerk effizient zur Erledigung von gemeinsamen Aufgaben verwendet werden. Diese Technik wird auch 'Grid Computing' genannt. So kann man zum Beispiel heute brachliegende Rechenpower und Festplattenspeicher mit SETI@home2 [10] der Universität von Berkeley zur Verfügung stellen. Diese verwenden die Privaten Ressourcen zur Forschung nach Ausserirdischer Intelligenz. (Search for Extra-Terrestrial Intelligence.) [11]

Durch die Verteilung der Daten auf den verschiedenen Peers und der damit einhergehenden Replikation, ist eine reaktiv gute Datensicherheit gewährleistet. Relativ, da unter Umständen Peers sich nicht mehr beteiligen und somit Daten 'verschwinden' könnten. Bei Bearbeitung und Aktualisierung von Files müsste man natürlich Änderungsanomalien in Betracht ziehen und Strategien zur Vermeidung festlegen.

Weiter ist es denkbar, Wartungsaufgaben an Rechnern vorzunehmen, die irgendwo am anderen Ende der Welt zu finden sind.

Vorteile in P2P Netzwerke gibt es wie gesehen noch so einige, doch sollen sich einige davon auch als Sicherheitslücken herausstellen.

### 10.1.4 Business Tauglichkeit von Peer to Peer Netzwerke

Wie in der Einführung angedeutet gibt es Bestrebungen die P2P Technik im Business Bereich weiter zu entwickeln. DMS (Document Management Systems) sind ein interessantes Feld für neue Entwicklungen. Das Projekt Opencola[12] [13] verwendet zum Beispiel den Ansatz von 'shared active folders' (gemeinsame, aktive Ordner). Das bedeutet, dass die Mitglieder in ihrem Ordner interessante Links ablegen und den anderen so zugänglich machen. Eine Suchanfrage an Opencola durchforstet dann neben bekannten Suchmaschinen auch noch die Ordner, die zum Interessengebiet passen. Das bedeutet, dass Suchmaschinenergebnisse noch durch Handanlegen von Menschen optimiert werden. Der Kostenpflichtige Service scheint aber nicht mehr verfügbar zu sein.

Microsoft arbeitet seit geraumer Zeit an einem Produkt namens 'Groove Virtual Office'. Groove[14] ermöglicht Gruppenarbeit, egal wo sich die Mitglieder gerade befinden. Man teilt Dateien und arbeitet gemeinsam an diesen, während Groove sich selber um die Synchronisation und aktuellste Version kümmert. Alle relevanten Geschäftsanwendungen wie Instant Messaging, White Boards, voice conference, usw. sollen von Groove abgedeckt werden. Im Gegensatz zu bekannten Anwendungen von beispielsweise Lotus muss dabei kein zentraler Server vorhanden sein. Alles wird via P2P Netzwerk auf jedem Peer synchronisiert. Die Daten sind nicht wie in anderen DMS an einem Ort primär vorhanden.

BBC hat gerade eine Testphase einer sehr interessanten P2P Anwendung abgeschlossen. Der so genannte BBC iMP[15] (Integrated Media Player) macht es möglich, verpasste TV und Radio Programme noch einmal anzusehen bzw. anzuhören. Eine Woche lang kann der Inhalt der Sendung aus einem P2P Netzwerk gratis heruntergeladen werden. Die Sendungen würden aber ein enormes Trafficvolumen generieren, dem nur mit gewaltigen Investitionen in Serverhardware entgegengewirkt werden könnte. Darum werden die Sendungen nicht von einem zentralen Streaming Server zur Verfügung gestellt, wie es etwa bei

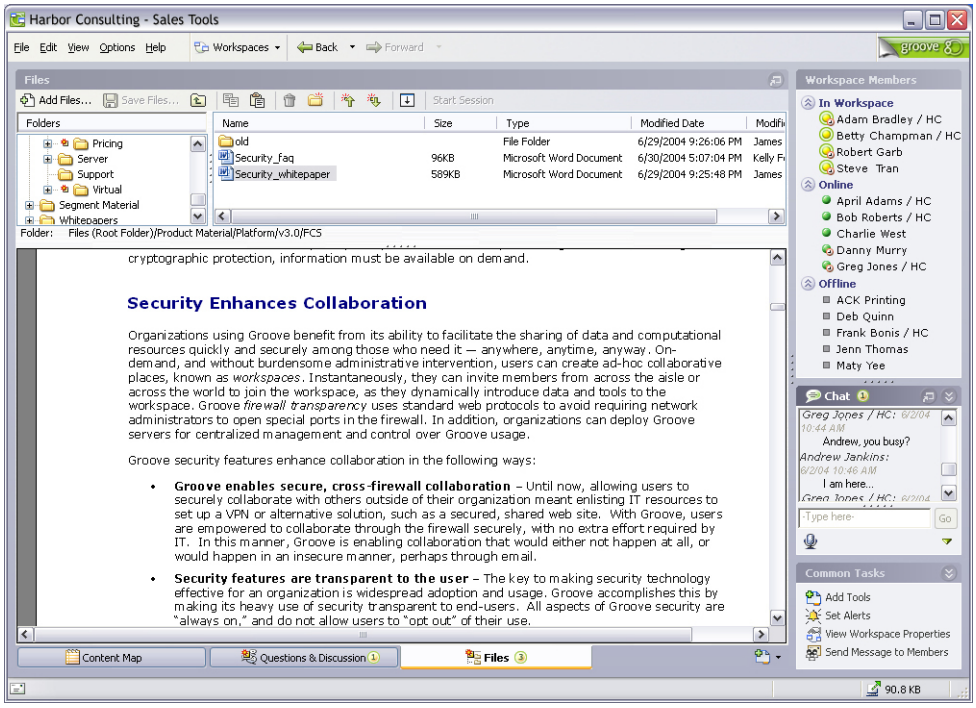



Abbildung 10.2: Screenshot Microsoft Groove Project

SFDRS der Fall ist, sondern von einem oder mehreren Peers im Netzwerk bezogen. BBC setzt dabei in ihrer Software auf das Bittorrent - Protokoll, und jeder Peer, der den Service bezieht, wird auch automatisch den Service den anderen anbieten. Einseitiges Herunterladen ohne selber zu teilen ist somit nicht möglich (zumindest nicht auf konventionellem Wege), die Last wird gleichmässig verteilt. Um die Weiterverbreitung von Sendungen zu verhindern, hat jedes File durch DRM (Digital Rights Management) nur eine 'Gültigkeit' von einer Woche. Auch Softwarehersteller verwenden bereits Bittorrent-Varianten um Updates und Patches ökonomisch zu verteilen.

Leider wird aber oft das Potential von derartigen Ansätzen verkannt und es sind Bestrebungen im Gange, die P2P Technologie als ganzes zu verbieten. 'Verleitung zu Urheberrechtsverletzungen', so soll der neue Strafbestand heissen, den US Senator Hatch[16] gerne in den Gesetzestexten niedergeschrieben sähe. So könnte es faktisch möglich werden in den USA jedes P2P Programm zu verbieten, welches rein hypothetisch zu einer Verletzung von Urheberrechten führen könnte. Aufgrund der Tatsache, dass sogar Warner einen 'Pakt mit dem Teufel'[17] schliessen will und künftig selber Filme per P2P vertreiben möchte, ist es unwahrscheinlich, dass solche Gesetze abgesegnet werden und die aufstrebende Netzwerktechnik ausbremsen können

## 10.2 Aufbau von Peer to Peer Systemen

Trotz rapide steigender Leistungs- und Übertragungsraten der Kommunikationstechnologie und der permanenten Weiterentwicklung von ohnehin schon leistungsfähigen Computern, ist die heutige Technik den Anforderungen oft nicht gewachsen. Auch werden zur


Abbildung 10.3: Screenshot BBC iMP Player

Verfügung stehende Ressourcen nicht genügend genutzt oder liegen brach. Fast immer liegen derartige Probleme an einer suboptimalen Architektur, die Flaschenhälse hervorbringt. Diese können verschiedenster Natur sein: mangelnde Bandbreite durch überlastete Server, zu wenig Speicherkapazität, ungenügende Rechenleistung. P2P Systeme versuchen, eben dieser Problematik Einhalt zu gebieten. Wie sie das zu gedenken tun und die resultierende Funktionsweise soll in diesem Kapitel kurz beleuchtet werden, damit ein Grundverständnis für potentielle Sicherheitsprobleme und deren Lösungsansätze vorhanden ist.

### 10.2.1 Die klassische Client/Server Architektur

Bei der klassischen Client/Server Architektur (die kein P2P System darstellt) gibt es genau zwei Rollen:

- Der Server, der einen Dienst zur Verfügung stellt (im allgemeinen wenige, jedoch hochperformant)
- Der Client, der Dienste in Anspruch nimmt (im allgemeinen viele)

Stellt man sich einen einzelnen Server vor, der als File- oder Webserver fungiert, und tausende Clients, die gleichzeitig Requests an eben diesen Server senden, ist es nicht verwunderlich, dass trotz der hohen Performanz des Servers ein Flaschenhals entsteht (der Server und/oder die vom Server ausgehende Linien sind überfordert) und die Performanz für jeden Beteiligten einbricht: Diese Architektur skaliert nicht. Gewisse P2P Netzwerke verwenden die Client/Server Architektur im weitesten Sinne als eine zentrale Koordinationsstelle, aber da es sich dabei nicht um ein P2P System ansich handelt, wird sie nicht weiter im Detail behandelt. Es sei jedoch erwähnt, dass eben diese Implementation als

Abbildung 10.4: Client/Server Architektur

'Single Point of Failure' ein verwundbares Ziel für potentielle Angreifer darstellt, die den Server beispielsweise mit DDoS (Distributed Denial of Service) Attacken unerreichbar machen können.

### 10.2.2 Peer to Peer Architekturen

Obwohl es verschiedene P2P Architekturen und Ansätze gibt, liegt allen dasselbe Prinzip zugrunde: Es gibt im Optimalfall nur eine einzige Rolle für alle Beteiligten, nämlich die des Peers (Peer = 'Gleichgestellter'). Jeder Peer kann sowohl als Server fungieren und Dienste anbieten, als auch gleichzeitig als Client fungieren und Dienste von anderen Peers anfordern. Der Peer als 'Servent' (Server + Client). Wächst oder schrumpft ein P2P Netzwerk, dann steigt bzw. sinkt sowohl das Angebot als auch die Nachfrage in diesem. Jede dieser Architekturen hat verschiedene Vorteile, birgt aber auch diverse, unterschiedliche Sicherheitsrisiken.

Oft spannen Peer-to-Peer Systeme eine sogenannte Overlay-Architektur auf. Dadurch können beteiligte Peers auf eine bestimmte, wohldefinierte Art (je nach P2P System verschieden) adressiert werden. Das Overlay ist lediglich eine virtuelle Architektur, unabhängig von der physikalischen Architektur. Knoten, die im Overlay nah beieinander positioniert sind können auf physikalischer Ebene extrem weit auseinanderliegen. Es ist deshalb möglich, dass - von der physikalischen Sicht gesehen - sehr ungünstige Konstellationen zustande kommen.

### 10.2.3 Unstrukturierte Peer to Peer Netzwerke

#### Zentralisiertes Peer to Peer (1. Generation)

Das zentralisierte P2P System revolviert um einen zentralen Server, der für die Indexierung von Inhalten verantwortlich ist und eine Art Datenbank mit Wissen über die Peers im Netzwerk implementiert. Er ist also gewissermassen der Koordinator, der Informationen hält und bei Bedarf weiterreicht. Der eigentliche Datenaustausch findet direkt von Peer zu Peer statt, weshalb es trotz zentraler Instanz als P2P Architektur zählt.

Abbildung 10.5: Zentrales Peer to Peer

Vorteil der zentralen Instanz ist, dass sie wohlbekannt ist. So besteht beispielsweise beim Bootstrapping (das Initiale 'finden' des Netzes) in der Regel nicht die Gefahr, dass ein bösartiger Knoten einen Peer in ein falsches Netzwerk lotsen kann. Gravierende Nachteile hingegen sind, dass der Server als alleiniger Koordinator und Herzstück eine Schwachstelle für Angriffe bietet, die sowohl technischer als auch gesetzlicher Natur sein können. Als Beispiel sei hier Napster genannt, welches durch die Musikindustrie und der RIAA deshalb erfolgreich stillgelegt werden konnte, weil sie gezielt den Betreiber des zentralen Servers ermitteln und zur Strecke bringen konnten. Stellen wir uns Peer-to-Peer Applikationen im kommerziellen Business Bereich vor, können die Folgen gegen dieses schwache Glied in der Kette viel fataler sein als eine Meute aufgebrachter Filesharer.

### Reines P2P (1. Generation)

Wie der Name schon verrät, liegt diesem Ansatz ein dezentralisiertes Konzept zugrunde. Sie kommt ohne zentrale Entität(en) zurecht. Ein 'echtes' P2P System. Requests werden durch Flooding an die jeweiligen Nachbarknoten weitergeleitet (Schneeballprinzip). Limitiert wird das Fluten durch die TTL (time to live), einer maximalen Anzahl von Hops, die ein Request zurücklegen kann, bevor er gestoppt wird. Positive Antworten - sofern vorhanden - werden auf dem gleichen Wege per Rückwärtsrouting an den Initiator des Requests gebracht.

Abbildung 10.6: Reines Peer to Peer

Reine P2P Systeme sind äusserst robust gegen 'gewaltsame' Angriffe. Selbst wenn einzelne Knoten stillgelegt werden, beeinflusst das die Funktionalität des Systems nicht. Da ausserdem die Inhalte im reinen P2P Netzwerk stets repliziert sind, ist es für einen Angreifer nicht möglich, alle Replikationen eines Datums zu ermitteln. Durch den Wegfall eines 'Central Point of Knowledge' hat es also auch eine hohe Resistenz gegen gezielte Denial of Service Attacken. Ein Angreifer würde es schwierig haben, in einem Backup System sensitive Daten gezielt anzugreifen und unverfügbar zu machen.

Auf der anderen Seite ist das System dadurch unsicher, dass es für einen bösartigen Knoten ein Kinderspiel ist, sich einzuklinken und falsche oder fehlerhafte Daten zu verbreiten. Auch ist es möglich, das Routing innerhalb des Netztes erheblich zu stören, indem man falsche Routinginformationen verbreitet. Ein Ansatz, um diesen Angriffen entgegenzuwirken, wäre eine Art 'Web of Trust' aufzubauen, also ein Netz nur mit Knoten, denen man ausdrücklich vertraut. Doch dazu mehr in Kapitel DHT-spezifische Attacken.

### Hybrides Peer to Peer (2. Generation)

Hybride P2P Systeme kann man als Variante der zentralen Systeme bezeichnen. Der Aufbau ist hierarchisch: mehrere Leafnodes hängen jeweils an sogenannten Superpeers (zeichnen sich durch besondere Merkmale aus, e.g. hohe Performanz, hohe Zuverlässigkeit/Uptime), welche wiederum untereinander verbunden sind.

Abbildung 10.7: Hybrides Peer to Peer

Die Superpeers sollen die Performanz und Effizienz des Netztes steigern und übernehmen bestimmte Aufgaben wie Lookups oder Suche von Inhalten. Requests werden dabei von den Leafnodes an die Superpeers gegeben, die untereinander kommunizieren und Resultate zurückliefern. Wie beim zentralisierten Peer-to-Peer findet auch hier der Datenaustausch schlussendlich zwischen einzelnen Peers statt.

Es kann immer noch eine gewisse Immunität gewahrt werden, da kein Single Point of Failure existiert, während zur gleichen Zeit die Effizienz des Systems auf einem hohen Niveau bleibt[18].

### 10.2.4 Strukturierte Peer to Peer Netzwerke

Strukturierte P2P Netzwerke wurden entwickelt, um vorhandene Schwachstellen und Mängel von unstrukturierten P2P Netzwerke (Bandbreite, Speicher, Prozessorstärke) zu beheben. Im Wesentlichen sollen die Skalierbarkeitsprobleme gelöst werden. Zusätzlich leiden die unstrukturierten P2P NW an Ungewissheit und Uneffizienz der Suche nach spezifischen Inhalten, wie sie beispielsweise durch das Flooding erfolgen [20]. Die Inhalte sind nicht, wie bei unstrukturierten Netzwerke auf zufälligen Knoten gelagert, sondern sind über eine verteilte Indexstruktur (distributed indexing structure) an spezifische Knoten im Netzwerk gespeichert. Diese verbesserte Skalierbarkeit konnte dank 'Distributed Hash Tables' (DHT) erreicht werden, welche diese verteilte Indexstruktur beinhaltet. [19]

#### Distributed Hash Tables (3. Generation)

Als DHT wird die verteilte Indexstruktur basierend auf Hash-Tabellen bezeichnet. Die ersten Ausprägungen wurden um das Jahre 2001 entwickelt. Die Entwicklung wurde massgebend durch File-Sharing-System-Entwickler gefördert, welche zum Ziel hatten, eine hohe Skalierbarkeit zu erreichen und die Organisation von eintretenden bzw. verlassenden Knoten zu verbessern, sowie eine bessere und verlässliche Suche ohne Angriffspunkt (bspw. Napster) zu erreichen. Dieser Ansatz entspricht demzufolge dem goldenen Mittelweg von zentralem Server und dem Flooding-Prinzip, wobei deren Schwachstellen umgangen werden konnte. Elementar für DHTs ist die Benützung des Overlay Netzwerks. Die gehashten Schlüssel von Datenobjekten werden gleichmässig auf die Knoten verteilt, wobei jeder Knoten für einen Teilschlüssel die Verantwortung trägt. Diese Teilschlüssel der Knoten variieren und passen sich dynamisch an die Knotenmenge im System an. Zudem verfügt jeder Knoten über eine Systemsicht, welche den Routingprozess verbessert und Suchanfragen so über wenige Knoten ans Ziel ermöglichen. Die Aufnahme von neuen Knoten in das Netzwerk verläuft über ein Protokoll, welches den Neuen mit einem bereits existierenden verbindet und die Anbindung an die Nachbarschaftsknoten durch die Erstellung von neuen Routingtabellen erreicht. Diese Routingtabellen ermöglichen die Zuordnung von Daten und Informationen im System und erlauben die Anbindung von tausenden oder Millionen von Knoten ins Netzwerk. Zudem ist das System fehlertolerant, wobei der Ausfall mehrerer Knoten keine Auswirkungen auf die Funktionalität des Systems zur Folge hat.

Auf Grundlage von DHT und unterschiedlicher Such- und Managementstrategien wurden einige Implementierungen entwickelt. Die wichtigsten sollen hier kurz erläutert und beschrieben werden, um den Mechanismus von DHT zu vertiefen.

#### Content Addressable Network

CAN verwendet DHT in Form eines Koordinatensystems, welches in mehrere Rechtecke, Zonen genannt, aufgeteilt ist. Der Schlüssel bezieht sich auf die Koordinate. Jeder Knoten ist für seine eigene Zone verantwortlich und ist über diese Zonengrenzen identifiziert. Die Schlüssel werden in demjenigen Knoten gespeichert, in welcher Zone sich die entsprechende Koordinate befindet. Der Knoten enthält jeweils die Routingtabelle aller ihrer

benachbarten Knoten. Die Suche verläuft über die Weitergabe der Suchanfrage an die Nachbarknoten, welche sich auf dem Weg der entsprechenden Koordinate befinden, um so schlussendlich an den Knoten zu gelangen, welcher den entsprechenden Schlüssel speichert. Neue Knoten werden einem beliebigen Koordinatenraum zugeordnet. Der Neue Knoten findet über einen bereits im System befindlichen Knoten den entsprechenden Knoten, welcher sich bereits in der entsprechenden Zone befindet. Über diesen Knoten erhält er die Routingtabelle mit allen Nachbarknoten und gibt sich diesen 'Nachbarn' zu bekennen. Die Zonen werden nun so aufgeteilt, dass jeder Knoten wieder eine Zone für sich beansprucht. Beim Verlassen eines Knotens wird ein Nachbar die Zone übernehmen und mit seiner eigenen verschmelzen, oder beide kurzfristig verwalten. Falls ein Knoten fehlschlägt, wird der Knoten mit der kleinsten Zone diese übernehmen. Um die daraus resultierenden Koordinatenprobleme zu beheben, läuft im Hintergrund von CAN ein Reorganisations-Algorithmus, welcher eine Neuzuordnung festlegt. CAN implementiert ausserdem dyna-

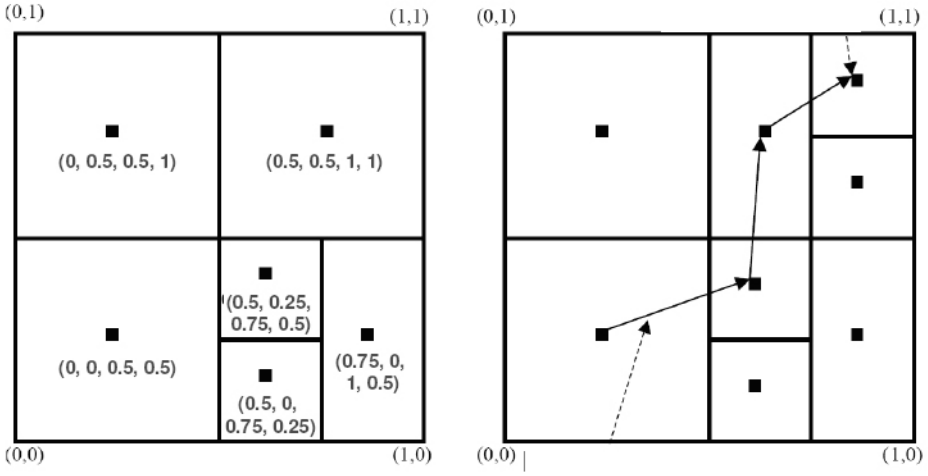



Abbildung 10.8: CAN Routing Algorithmus [21]

misches Routing, indem ein Knoten die Route zum Endpunkt bestimmen kann. Das Ziel ist es zum einen, den bestmöglichen Weg durch das Koordinatensystem zu finden, um die Effizienz zu steigern und zum anderen, eine Ausfallsicherheit zu bieten, sollten gewisse Knoten unerreichbar sein. Was auf den ersten Blick als willkommenes Feature erscheint, soll sich jedoch als schwerwiegendes Sicherheitsdefizit herausstellen [21] [22].

### Chord

In Chord sind die Knoten und Schlüssel in einem Ring angeordnet, wobei die Knoten über eine ID und die Daten über einen Schlüssel eindeutig identifiziert werden können. Dabei ist der Knoten für denjenigen Schlüssel verantwortlich, dessen numerischer Schlüssel-ID am nächstes unterhalb der Knoten-ID liegt. Der Knoten wird deshalb 'Successor' (Nachfolger) des Schlüssels genannt. Suchabfragen für einen entsprechenden Schlüssel werden von dem Knoten an den nächsten Knoten weitergereicht. Wird der Knoten mit der ID grösser als der gesuchte Schlüssel erreicht, so hält er den gesuchten Schlüssel. Die Routingtabelle in Chord, 'Fingertabelle' genannt, hält die anderen Knoten im Kreis fest, um die Suchanfrage zu optimieren. Die Suchfrage schlägt nur dann fehl, wenn gerade mehrere nachfolgende

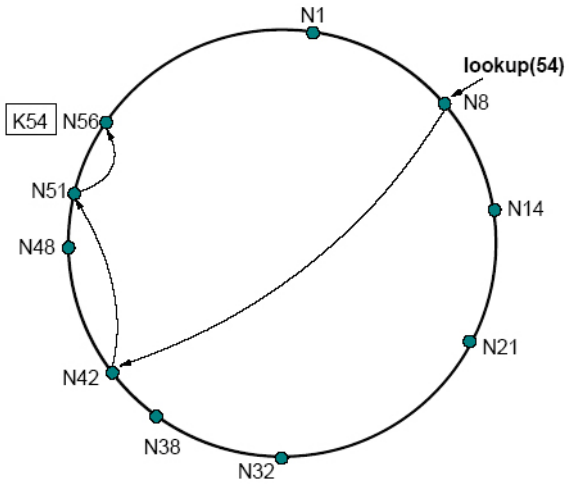



Abbildung 10.9: Zirkulärer Adressraum von Chord [21]

Knoten hintereinander auf dem Ring nicht funktionieren. Ein neuer Knoten wird zufällig im Ring platziert. Er bekommt seine ID, indem er einen anderen Knoten anfragt. Die Vorgängerknoten ergänzen den neuen Knoten in ihrer Nachfolgerliste. Chord legt seinen Schwerpunkt auf Robustheit und Korrektheit, diese Eigenschaften werden durch einfache Algorithmen sichergestellt [21].

### Pastry

PASTRY ist wie CHORD auf einem Ring aufgebaut. Jeder Knoten wird durch seine ID auf dem Ring identifiziert und beinhaltet dessen Positionsangaben. Die Weitergabe von Suchanfragen wird durch ein Abstimmen der ID-Nummern gesteuert. Die ID identifiziert sowohl den Knoten wie auch den Schlüssel, da der Schlüssel auf demjenigen Knoten liegt, bei dem die IDs am nächsten sind. Die Routingtabelle ist zu vergleichen mit der Fingertabelle von CHORD. Das so genannte 'leaf set' enthält die Knoten, welche sich in der Nähe im Identtifizierraum befinden, was in CHORD über die so genannte 'successor List' erfolgt. Das Nachbarschaftliche Verhältnis von Knoten wird in einem 'Nachbarschaftsset' festgehalten. Bei der Suche (Routing) wird in zwei Zwischenschritte aufgeteilt. Beim ersten schaut der Knoten, ob der gesuchte Schlüssel innerhalb des Bereichs des 'Leaf set' liegt. Dies heisst, dass sich die der Schlüssel auf den umliegenden Knoten befindet. Suchanfragen, welche eine längere Distanz betreffen, werden durch eine höher Ebene des Präfixes weitergeleitet, was bedeutet, dass die Annäherung über einen weiteren Bereich (im Falle der ID Nummer) weitergeleitet wird, bis das Matching zutrifft. Dieser Vergleich erfolgt über die Routingtabelle. Bei Eintritt in das System, wählt der betreffende Knoten eine ID. Dieser Knoten sucht aufgrund von Näherung einen Nachbarknoten. Nun baut er seine Routingtabelle, 'leaf set' und sein 'Nachbarschaftsset' auf. Um Fehlerknoten zu handhaben, werden in PASTRY Knoten über das Nachbarschaftsset bezüglich ihrer Existenz geprüft. Falls die Suchanfrage an einen fehlerhaften Knoten gerät, kann der sendende Knoten einen anderen Knoten aus derselben Reihe der Routingtabelle wählen um so schlussendlich die Suchanfrage erfolgreich abschliessen. [18]

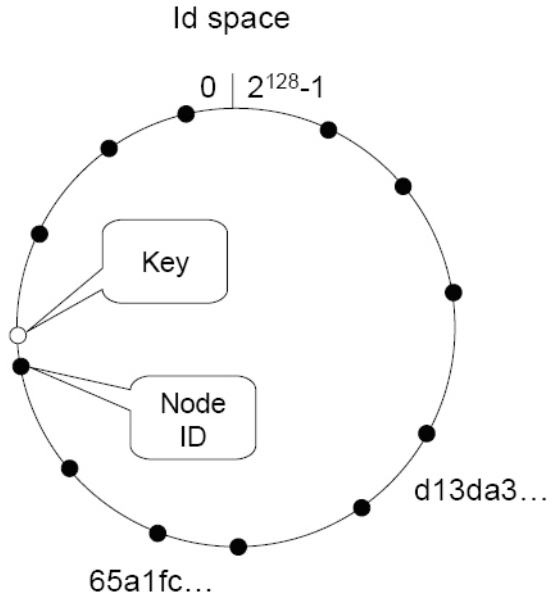



Abbildung 10.10: Pastry, Prof. Dr. Burkhard Stiller; [37]

## 10.3 Sicherheitsbedrohungen in Peer to Peer Netzwerken

Peer-to-Peer Systeme bieten elegante Lösungsansätze für aktuelle Problemstellungen und zukünftige Dienstleistungen. Neben all den Vorteilen, die sie bieten, darf man nicht vergessen, dass sie auch eine ganze Reihe von Nachteilen in Form von Sicherheitsproblematiken mit sich ziehen. Besonders die Offenheit und Anonymität der Systeme - beides Kernelemente und eigentliche Stärken von P2P -, sollen sich als gravierende Nachteile herausstellen. Denn die Eintrittsbarrieren für Angreifer die sich in ein Netz einklinken wollen (um dann Schaden anzurichten), sind praktisch null. Weiterhin ist P2P der dritten Generation (erste/zweite Generation: unstrukturiert, dritte: strukturiert) zwar effizient und effektiv wie selten zuvor, doch bedeutet Struktur auch, dass es für einen Angreifer um ein Vielfaches einfacher ist, ein System gezielt zu attackieren. Die Sicherheitsbedrohungen müssen nicht unbedingt ausgefuchste Exploits oder aufwändige Overtakes von Partitionen des Netzwerkes sein, sondern können sich auch schlicht dadurch manifestieren, dass Peers ihre Dienste den anderen Peers verweigern. So können sie etwa über ihren Content oder ihre Leistungsfähigkeit lügen, um beispielsweise beim Filesharing weniger anbieten zu müssen oder generell die Last zu senken. Manchen Angriffen liegen inhaltliche, semantische Konzepte zu Grunde, während anderen Attacken die Infrastruktur der Systeme angreifen. Das Ergebnis ist jedoch dasselbe, die P2P Netzwerke werden verlassen. Entweder 'freiwillig' vom Benutzer weil es unbrauchbar geworden ist oder weil es in der Funktionalität irreparablen Schaden erlitten hat.

### 10.3.1 Angriffe auf Peer to Peer Systeme

#### Network Poisoning/Rogue Files

Wie der Name schon verlauten lässt, versuchen Angreifer hierbei das Netzwerk zu 'vergiften'. Besonders beim Filesharing ist dies ein beliebtes Vorgehen und einfach zu bewerkstelligen, indem man Dateien zur Verfügung stellt, die etwas anderes sind als sie zu sein vorgeben oder aber fehlerbehaftet sind.

Akteure beim Network Poisoning sind sogenannte Spoofer. Benutzer, welche unbrauchbare Daten zur Verfügung stellen. In einem weiteren Schritt ist es natürlich auch möglich, dass man bösartigen Code - sprich Viren - in einer Datei versteckt, die etwas anderes zu sein vorgibt. Der Wolf im Schafspelz sozusagen. Beim ehemals beliebten Filesharing Netzwerk KaZaa [7] etwa werden bei jeder Suche, gleichgültig was der Suchbegriff enthalten mag, fast schon standardmässig einige Treffer zurückgeliefert, in denen sich Viren verbergen. Für fortgeschrittene Benutzer ist es nicht allzu schwierig, solche Spielchen zu durchblicken und grösseren Schaden zu vermeiden. Für den unerfahrenen Benutzer stellt dies jedoch eine grosse Bedrohung dar. Es ist einleuchtend, dass die Kredibilität der P2P Netzwerke darunter zu leiden hat, je häufiger solche Vorkommnisse sind. Das Netzwerk verliert an Attraktivität, schlussendlich 'stirbt' es, wenn die Verseuchung zu grosse Ausmasse annimmt.

Aus den vergangenen Jahren entstammen diverse Berichte, dass Junk-Inhalte auch bewusst von P2P Gegnern wie Medien-Firmen lanciert wurden, um die Online-Piraterie in P2P Netzwerke zu bekämpfen. So soll laut [23] etwa die IFPI [24] Spoofer angestellt haben, welche Files in den Umlauf gebracht haben, die Störungen verschiedener Art enthalten. Auf der einen Seite war es so möglich, gezielt Informationen (sprich: IP Adresse) über die Nutzer zu erhalten, die illegales Filesharing betrieben und zum anderen sassen sie schlussendlich mit einer beschädigten oder unbrauchbaren Datei da. Konkret kann das ein MP3 File mit Anomalien wie plötzliche Stille oder Rauschen sein. Der User hat also gleich doppelt Ressourcen verschwendet, erstens um die Datei herunterzuladen und zweitens um zu ermitteln, dass die Datei überhaupt ein 'Fake' war. Das Problem hierbei: man kann nicht im Voraus erahnen, welche die fehlerfreien Dateien und welche die präparierten sind.

Als Gegenmassnahme kann man sich ein Rating-System wie das 'Integrity Rating' von KaZaa [25] vorstellen. Benutzer können damit zur Verfügung gestellten Dateien mit vier verschiedenen Flags markieren:

- Excellent : Has complete file data (metadata) describing the file and is of an excellent technical quality.
- Average : Has some file data (metadata) describing the file, is of a moderate technical quality.
- Poor : Poor technical quality, no file data (metadata).
- Delete File : Where the file should not be shared e.g. it is virus infected, of unusable technical quality, or illegal.

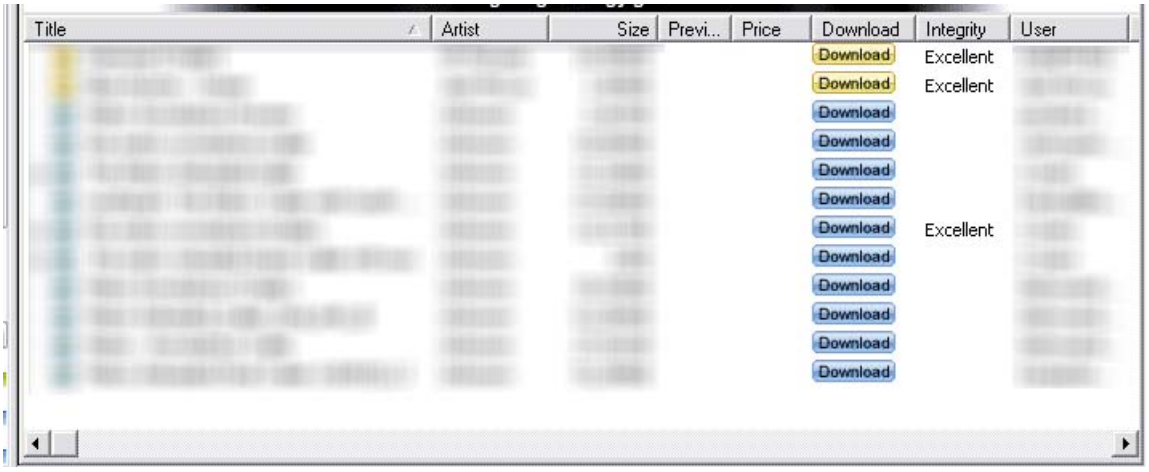



Abbildung 10.11: Integrity Rating von KaZaA

Auf den ersten Blick mag das eine zufriedenstellende Lösung darstellen, aber es ist auch für bösartige User möglich, vom System Gebrauch zu machen und Junk-Files als tadellos zu markieren. Das Potential des Rating Systems ist also höher (im guten wie auch im schlechten Fall), je mehr Benutzer kooperieren.

Weitaus bessere Ansätze bieten hier Hash Funktionen. In der Praxis hat jede Datei einen eindeutigen Hashwert (Überschneidungen sind zwar möglich, aber höchst unwahrscheinlich), mit der sie identifiziert werden kann. Hat ein Benutzer also den Hash einer gewünschten Datei, kann er sie mit dem angezeigten Wert in der Applikation vergleichen um sicherzugehen, dass sie authentisch ist. Die japanischen Filesharing Applikationen Share und Winny unterstützen jeweils Downloads mit Hilfe von Hashwerten und besitzen (inoffizielle) Datenbanken mit zahlreichen Einträgen [26] [27]. Diese Datenbanken können allerdings auch als eine Schwachstelle angesehen werden, denn jeder beliebige Benutzer kann neue Einträge erstellen und so Fakes verbreiten.

Als zusätzliche Sicherheit dienen daher bei beiden Applikationen noch der Benutzername und der sogenannte Tripcode (ein Passwort, auf den eine Hashfunktion angewendet wird), die eine Person eindeutig zu identifizieren vermögen. So ist es möglich, offizielle Updates von Share gezielt vom offiziellen Autor selbst zu beziehen (Updates von Share sind ausschliesslich über Share selbst beziehbar). Natürlich muss man auch hier abwägen, ob man anderen User vertrauen kann/will oder nicht, doch die Erfahrung zeigt, dass die Rate für fehlerhafte Files bei Share extrem tief ist.

Wie man sieht, stellt Network Poisoning besonders dadurch eine Gefahr dar, dass es eine sehr einfach durchzuführende Attacke darstellt und es keine Verteidigung gibt, will man das P2P System offen und anonym halten. Es wird nicht wie bei anderen Angriffen das Netzwerk in der Grundfunktionalität gestört. Hier leidet die Kredibilität und Attraktivität je mehr vergiftete Dateien im Umlauf sind. Mit den Integrity-Ratings und den Hashes/IDs/Datenbanken sind zwar Lösungsansätze gegeben, jedoch dienen sie auch nur der Schadensbegrenzung und bieten überdies nicht einen kompletten Schutz gegen Rogue Files. Als einzig denkbare Lösung käme eine zentrale Instanz (als Verteiler von Ratings oder Halter der Datenbank) in Frage, welcher man mit absoluter Sicherheit vertrauen

kann. Doch das würde erstens gegen die P2P Prinzipien der heutigen Generation verstossen und zweitens wiederum als Single Point of Failure eine Angriffsfläche für andere, gravierendere Angriffe bieten.

### Rational Attack

Damit Peer-to-Peer Systeme effizient operieren können, muss jeder Peer die Funktion des 'Servents' annehmen und auch ausüben. Peers sollten optimalerweise im selben Masse Dienste und Ressourcen zur Verfügung stellen, wie sie diese in Anspruch nehmen. Dabei kann Ressource verschiedene Bedeutungen haben, etwa 'shared Content' oder aber zur Verfügung gestellte Bandbreite, deshalb betraf der 'Rational Attack' in der Vergangenheit besonders Filesharing Applikationen, stellt aber in Zukunft auch ein Problem für Applikationen aus anderen Bereichen wie Backup Systeme dar. Wie die Erfahrung zeigt, ist es ein Wunschdenken, dass alle Peers diese Art der Fairness ausüben. Sogenannte 'Freeloader' sind Benutzer, welche Ressourcen beziehen ohne dabei selber Inhalte zur Verfügung zu stellen. Mögliche Gründe für ein solches Verhalten:

- Limitierte Ressourcen der Anwender: Selbst, wenn ein Anwender gerne mehr Bandbreite zur Verfügung stellen möchte, ist das von der technischen Seite unmöglich, denn die meisten Heimanschlüssen bieten im Vergleich zu den verfügbaren Downloadraten sehr minime Uploadraten. Oft kassiert ein ISP (Internet Service Provider) vom Benutzer auch abhängig vom transferierten Datenvolumen, auch ökonomische Aspekte fliessen also mit ein.
- Intentionale Beschränkung der Ressourcen: Anwender können egoistisch handeln und ihre Ressourcen nicht teilen, einfach durch Böswilligkeit oder anderen unerfindlichen Gründen. Beim Filesharing ist der angebotene Content darüber hinaus oftmals illegal, was dazu führt, dass viele Anwender entweder Dateien erst gar nicht teilen oder aber das Uploaden an andere Peers komplett unterbinden, um Problemen aus dem Weg zu gehen. Diese Problematik dürfte allerdings bei offiziellen Businessapplikationen aus dem Weg geräumt sein.

Im Gegensatz zum Network Poisoning kann gegen Rational Attacks einfacher und mit relativ wenig Aufwand (auf Benutzerseite) vorgegangen werden. Am effektivsten ist eine Art 'Reward-System', das einem Peer mehr Leistungen zuspricht, je mehr er derer anbietet. So hat man etwa beim Filesharing Tool Bittorrent schnellere Downloadraten, je mehr man uploadet. Das P2P Backup System Samara [28] sorgt dafür, dass ein Peer nur so viel Backupspeicher zur Verfügung gestellt bekommt, wie er selbst zur Verfügung stellt. Hubs (Server) beim Filesharing Programm DC++ [29] können an Benutzer Minimalanforderungen stellen (Anzahl der Uploadslots und minimale Menge an shared Content), denen die Verbindung verwehrt wird, sofern sie jene nicht erfüllen.

Das Problem ist, dass längst nicht alle Applikationen solch einen Mechanismus integriert haben, dieser schlecht implementiert ist oder er sich nicht selten umgehen lässt. So kann man etwa im Fall von DC++ die Uploadrate nicht in der Applikation limitieren, es jedoch mit einem externen Programm wie Netlimiter [30] nachholen, ohne dass es bemerkt wird.

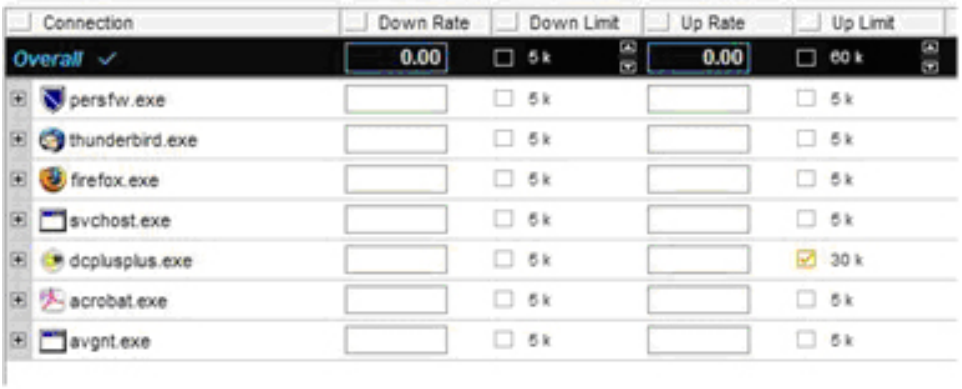



Abbildung 10.12: Screenshot von Netlimiter

Obwohl P2P Netzwerke in den letzten Jahren einer immensen Entwicklung und Verbesserung nachgekommen sind, bleibt immer noch Verbesserungspotential in den Bereichen 'freeriding', 'Junk Inhalte', und Sicherheitsbedrohungen aufgrund böser Absichten.

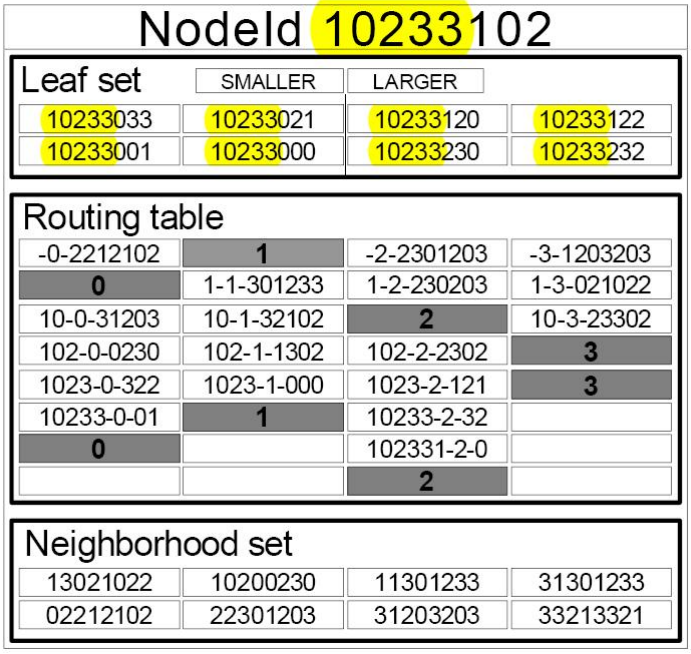
### DHT-spezifische Attacken

Bei strukturierten Peer-to-Peer Systemen mit DHT ist ein fehlerfreies Routing elementar, denn anders als bei unstrukturierten Systemen kennt man Dateninhalte bereits und muss sich nur noch um das 'Lookup' (Nachschlagen) derer kümmern. Korrekte und fehlerfreie Routing-Tabellen sind daher eine Notwendigkeit, um das System möglichst effizient und am Leben zu erhalten. Angreifer können ihre Attacken eben darauf konzentrieren und einen wunden Punkt treffen.

**Incorrect Lookup Routing** Es gibt zwei Möglichkeiten, wie bösartige Knoten das Routing durcheinander bringen können [33]:

- Lookups an nicht existierende und/oder falsche Knoten weiterleiten
- Zufällige Knoten für Schlüssel-verantwortlich erklären (obwohl sie es nicht sind)

Die falsche Weiterleitung von Lookups kann je nach DHT Algorithmus entdeckt werden oder nicht. Normalerweise sollte mit jeder Weiterleitung die Nachfrage ein Stück näher an das finale Ziel gelangen. Der jeweilige 'Nachfrager', der die Anfrage weiterleitet, muss also lediglich überprüfen, ob dies tatsächlich der Fall ist. Knoten sollten deshalb in der Lage sein, diesen Prozess zu beobachten. CAN - welches das 'Koordinatensystem' verwendet (Siehe Kapitel Strukturierte P2P Netzwerke) - ist deshalb sicherheitstechnisch anfällig für diese Attacke, während Pastry - mit dem 'Präfix-Routing' (Siehe Kapitel Strukturierte P2P Netzwerke) - dagegen gewappnet ist. Der Anfragende Peer kann die Suchresultate überprüfen und vergleichen ob, er näher an sein Ziel navigiert wird oder ein Fehlleitungsversuch vorliegt. Wird so ein Versuch detektiert, kann der Initiator der Anfrage ein Backtracking zum letzten korrekten Knoten vornehmen und ihn anhalten, für die Weiterleitung einen anderen Knoten zu wählen.



Nodeld 10233102

Leaf set

| SMALLER | | LARGER | |
|---|---|---|---|
| 10233033 | 10233021 | 10233120 | 10233122 |
| 10233001 | 10233000 | 10233230 | 10233232 |

Routing table

| | | | |
|---|---|---|---|
| -0-2212102 | 1 | -2-2301203 | -3-1203203 |
| 0 | 1-1-301233 | 1-2-230203 | 1-3-021022 |
| 10-0-31203 | 10-1-32102 | 2 | 10-3-23302 |
| 102-0-0230 | 102-1-1302 | 102-2-2302 | 3 |
| 1023-0-322 | 1023-1-000 | 1023-2-121 | 3 |
| 10233-0-01 | 1 | 10233-2-32 | |
| 0 | | 102331-2-0 | |
| | | 2 | |

Neighborhood set

| | | | |
|---|---|---|---|
| 13021022 | 10200230 | 11301233 | 31301233 |
| 02212102 | 22301203 | 31203203 | 33213321 |

Abbildung 10.13: Abstrahierte Pastry Routing Tabelle [38]

Wird ein zufälliger Knoten für Schlüssel fälschlicherweise für verantwortlich erklärt, kann es dazu führen, dass der Schlüssel (aus der Sicht des Systems) an einem falschen Ort gespeichert wird oder nicht gefunden werden kann. Zwei Massnahmen sollen helfen, dagegen zu schützen. [33] Zum einen sollte der Anfragende Knoten jeweils verifizieren, dass der Zielknoten zustimmt, das Endziel der Anfrage zu sein (korrekte IP Adresse als schwacher Identifikationsschlüssel). Zum anderen sollte es vermieden werden, dass Knoten sich selbst arbiträr IDs spezifizieren können. Schlüssel sollten den Knoten nämlich auf nachweisbare Art und Weise zugewiesen werden, damit die Richtigkeit der Assoziation überprüft werden kann. Auch hier hat CAN Sicherheitsmängel.

**Incorrect Routing Updates** DHT basierte Protokolle bauen ihre Routing-Tabellen mit Hilfe ihrer Nachbarn auf. Durch die Veränderungen des Netzwerks (Joins und Leaves) ist die Struktur ständigen Veränderungen unterworfen. Es sind Updates der Tabellen vonnöten, um das System funktionsfähig zu erhalten. Angreifer können ihren Nachbarn schlechte oder falsche Routinginformationen liefern, aus denen eine korrumpierte Routing-Tabelle resultiert. Als Folge werden Anfragen im Netzwerk falsch weitergeleitet. Durch das Präfix-System von Pastry können falsche Routinginformationen durch Vergleiche mit dem problemlos identifiziert werde. Jeder Tabelleneintrag muss über ein Korrektes Präfix verfügen. Es ist jedoch ratsam, die Erreichbarkeit der Knoten zu überprüfen, bevor ein Knoten seine Tabellen erneuert [38].

Erlauben Algorithmen dynamisches und flexibles Routing, wie es bei CAN der Fall ist, können Angreifer Knoten mit Updateinformationen beliefern, die zwar korrekt, jedoch suboptimal sind [33]. So können sie Knoten propagieren, die eine hohe Latenz vorweisen oder sogar andere bösartige Knoten. Als Resultat sinkt die Effektivität des Routings und des Systems stark. Denkbar wäre sogar eine Kettenreaktion, wenn der Angreifer über

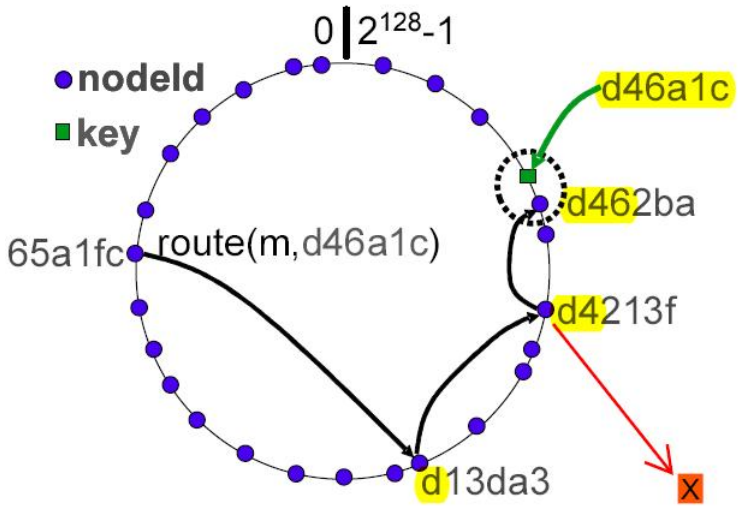



Abbildung 10.14: Vorgehen beim Pastry Routing [39]

viele Knoten verfügt. Die Auswirkungen sind im gleichen Masse destruktiv wie im ersten Fall, jedoch verdeckter und deshalb nur schwierig aufzuspüren. Um das Problem zumindest einzudämmen, könnte man Routinginformationen nur unter bestimmten Umständen akzeptieren. Beispielsweise nur, wenn Knoten erreichbar sind und dabei bestimmte Leistungsaspekte wie eine kleine Latenz zwischen zwei Knoten erfüllt sind.

### Partitioning

Damit ein Peer einem bestehenden Peer-to-Peer Netzwerk beitreten kann, muss es in einem ersten Schritt einen wohlbekannten Peer kontaktieren, der ihn mit dem Netzwerk bekanntmachen kann (beispielsweise durch Serverlisten oder Knoten die im Programm 'hardcoded' sind, etc.). Diesen Prozess nennt man 'Bootstrapping'. Die Partitioning Attacke macht sich die Schwäche zu Nutze, dass dieser Peer auf externe Hilfe angewiesen ist und hat es darauf abgesehen, während des Bootstrappings jenen in ein falsches, paralleles Netzwerk zu lotsen, das von mehreren, bösartigen Knoten aufgespannt wurde. Dieses parallele Netzwerk kann dazu verwendet werden, anderen Peers Dienste zu verweigern oder aber dieselbe Funktionalität wie das authentische vortäuschen, um das Verhalten von Peers zu analysieren und Informationen zu erschliessen, die andernfalls uneinsichtlich gewesen wären.

Einen Schutz gegen das Partitionieren eines P2P Netzwerks bietet das Bootstrapping über eine sichere Instanz, durch einen Knoten, der mit vollständiger Sicherheit nicht bösartig ist. Nicht immer ist dies jedoch ein einfaches Unterfangen, denn die Adressierung der Maschinen im Internet ist nicht zwingend statisch, wenn nicht sogar die Ausnahme. Werden die IP Adressen etwa über einen DHCP Server dynamisch verteilt, ist es möglich, dass sich der gestern noch 'saubere Knoten' heute plötzlich als bösartig herausstellt. [33]

Aus Anwendersicht ist es in reinen P2P Netzen schwierig, eine solche Attacke zu bemerken, besonders wenn das Parallelnetzwerk als das Original getarnt ist. Wenn man die

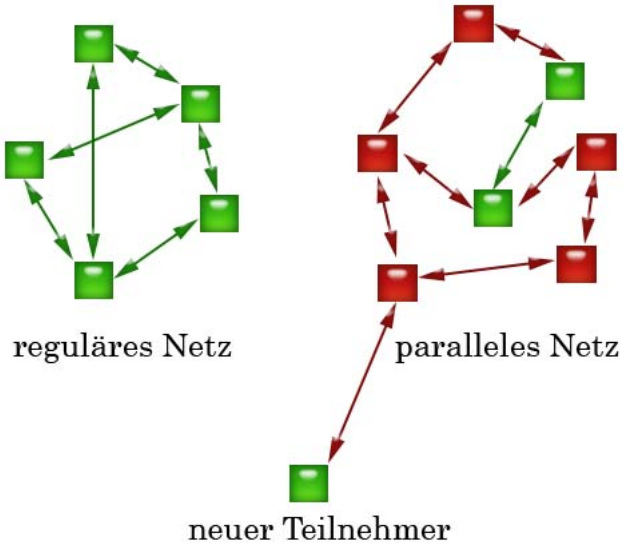



Abbildung 10.15: Partitioning in Peer to Peer

schwerwiegenden Folgen in Betracht zieht, ist es wünschenswert, dass P2P Applikationen Verteidigungsmechanismen gegen Partitioning bereits integrieren.

### Man-in-the-middle Attack

Beim Man-in-the-middle Attack schaltet sich ein Knoten zwischen zwei kommunizierende Peers. Der Angreifer hat dabei zwei Möglichkeiten:

- passiver Angriff: Abhorchen des Verkehrs, Analysieren des Verkehrs, etc.
- aktiver Angriff: Spoofing Angriffe

Solange er sich passiv verhält, gibt es für die zwei Kommunikationspartner keine Möglichkeit, ihn zu detektieren. Durch die gesammelten Informationen und Analyse derer kann er dann eine aktivere Rolle einnehmen und Nachrichten verändern oder sogar fälschen. Werden sensitive Daten über das P2P Netzwerk gesendet, ist schon die Tatsache, dass überhaupt abgehorcht werden kann, sehr bedenklich.

Abbildung 10.16: passiver Angriff [40]

Da man sich für einen erfolgreichen Angriff im Overlay Netzwerk (also auf Applikationsebene) zwischen zwei Knoten platzieren muss, sind P2P Systeme besonders anfällig dafür. Sehr oft kann man nämlich seine Knoten ID arbiträr wählen oder sie wird pseudo-zufällig

Abbildung 10.17: aktiver Angriff [40]

generiert, was jedoch umgangen werden kann. So ist es leicht, sich gezielt zwischen zwei bestimmte Teilnehmer zu schalten.

Um Man-in-the-Middle Angriffe zu verunmöglichen respektive um davor zu schützen gibt es wiederum zwei Möglichkeiten:

- eine physikalisch abhörsichere Leitung
- kryptographische Verfahren

Ersteres ist gegenwärtig ein Ding der Unmöglichkeit, besonders wenn man P2P Systeme mit ihren unzähligen Verbindungen in Betracht zieht, die sich (phsyikalisch) über weite Gebiete erstrecken. Die kryptographischen Verfahren jedoch genügen, um sowohl die Authentizität als auch den Inhalt zu schützen. So könnte ein Knoten an jede gesendete Nachricht seine digitale Signatur anhängen, damit der Empfänger die Authentizität überprüfen kann. Auch kann der Sender seine Nachricht mit dem öffentlichen Schlüssel des Empfängers (öffentlich verfügbar) verschlüsseln, so dass potentielle Angreifer den Inhalt nicht im Klartext lesen können. Der Empfänger kann dann mit seinem privaten Schlüssel, den natürlich nur er besitzt, die Nachricht entschlüsseln und lesen. Ähnliche verfahren werden in anderen Bereichen wie eMail eingesetzt, beispielsweise durch PGP (Pretty Good Privacy) [34], und haben sich in der Praxis als äusserst sicher erwiesen und bewährt. Damit solche Verschlüsselungsverfahren sicher bleiben, müssen 'initial Man in the Middle Attacks' unterbunden werden. Dabei schaltet sich der Angreifer schon in der Phase der Schlüsselvergabe dazwischen und verfügt somit über die nötigen Mittel, um den Chiffriertext zu entziffern. Auch muss gewährleistet sein, dass die öffentlichen Schlüssel authentisch und integer sind.

### Denial of Service (DoS)

Denial of Service Attacken sind dadurch charakterisiert, dass sie dem normalen Benutzer eines Systems dessen Dienste unzugänglich machen wollen [35]. Die für P2P Systeme gefährlichste Methode einer DoS Attacke stellt das Flooding dar, bei dem das Netzwerk mit 'Garbage-Paketen' (Pakete mit unsinnigem Inhalt) geflutet wird, so dass der reguläre Verkehr stark gestört oder sogar verunmöglicht wird. Noch viel mächtiger ist Flooding, wenn mehrere Hosts beteiligt sind, eine sogenannte Distrubuted Denial of Service (DDoS) Attacke. Oft verwendet der Angreifer dazu Zombie Computer, die er von seiner Maschine aus durch Würmer fernsteuern kann [36]. Einerseits sind gewisse Peer-to-Peer Systeme aufgrund ihrer Verteilung resistent gegen Denial of Service Attacken (Wegfall eines Single

Point of Failure), andererseits aber bei Verwendung von Flooding-Mechanismen anfällig auf die Garbage-Pakete.

So ist einfach, ein Client/Server System oder ein zentralisiertes Peer-to-Peer System lahmzulegen, indem man die Server flutet und abschiesst. Gefährlich für verteilte Peer-to-Peer Systeme wird es dann, wenn es einem Angreifer gelingt, Systeme mit Würmern zu infizieren (über das Peer-to-Peer System selbst oder aber auch auf konventionellem Weg), um so in ihre Kontrolle zu gelangen und eine DDoS Attacke zu lancieren. Da diese Angriffe von einer grossen Anzahl Hosts ausgeführt werden, die unter Umständen auch legitim sein können, ist es schwierig, wenn nicht unmöglich, den Angriff komplett zu blocken.

Auf Server als Single Point of Failure zu verzichten, die potentielles Ziel eines solchen Angriffs sind und auch möglichst wenige Supernodes einzusetzen, die ein rasantes Ausbreiten von Würmern begünstigen, ist eine vorbeugende Massnahme. Als weitere Massnahme gegen DDoS hat sich das 'Pricing' durchgesetzt, bei dem die erlaubte Anzahl von Requests über Zeit für jeden Peer restriktiert ist. Schickt ein Peer einem anderen einen Request, antwortet der Empfänger mit einem rechenintensiven Puzzle, beispielsweise einem MD5 Hash, den der Sender dann in einen String zurückführen muss (durch Bruteforcing). Erst, wenn er dem Empfänger mit der richtigen Lösung antwortet, wird dieser den Request anerkennen und antworten.

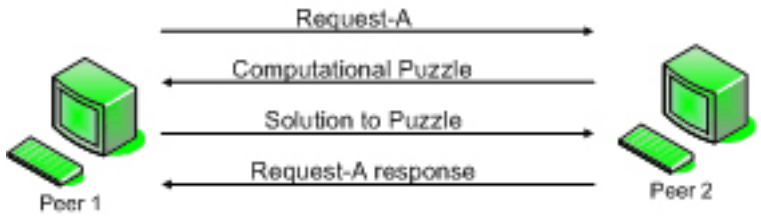



Abbildung 10.18: Vorgehen beim Pricing [41]

### The Sybil Attack

Ein Psychologe würde es Multiple Persönlichkeitsstörung nennen, im P2P Bereich bezeichnet man das Vorspielen von multiplen Identitäten eines Systems als Sybil Attacke. Attacke und nicht Krankheit, da gezielt versucht wird ein P2P Netzwert zu sabotieren.

**Grundlage für Sybil Attacke** Viele bekannte P2P Anwendungen verfügen über keine Authentifizierung bezüglich Zugangskontrolle. Durch das Fehlen einer zentralen Koordinationsstelle, welche die einzelnen Rechner eindeutig identifizieren kann, ermöglicht es nun, dass ein Rechner mehr als eine Identität vorspielen kann. Die Verteilung von Dateien oder das Teilen von Ressourcen bedarf jedoch einer genauen Unterscheidung von einzelnen Systemen. Sollten zwei angeblich unterschiedliche Systeme doch ein und das Selbe sein, können Redundanz - Probleme auftreten und Suchanfragen fehlgeleitet werden. Es ist somit auch möglich Redundanz und etwaige Sicherheit vorzugeben, obwohl mehrfach auf die gleiche Ressource zugegriffen wird. Bösartige Netzteilnehmer können grössere Anteile des

Netzwerkes kontrollieren, indem sie mehrfach Systeme replizieren. Es wird so versucht, dass möglichst viele Operationen über die vorgespielte Identität laufen.

Leider wird in vielen der verwendeten Algorithmen die eindeutige Kennung der Knoten über den Hashwert der IP-Adresse eines Peers geregelt. Diese schwachen Identifikationsschlüssel stellen ein grosses Risiko dar, denn wie bekannt, ist es leicht mit sog. IP - Spoofing die IP Adresse eines Systems beliebig zu manipulieren. IPv6 wird das Problem nicht Lösen, da hier ein noch grösserer Raum von Adressen zur Verfügung steht und dieser somit auch für Missbrauch genutzt werden kann.

**Ausmass der Sybil Attacke** Um das Ausmass und Potential einer Sybil Attacke zu verstehen, sollte man folgende Fakten in Betracht ziehen: Es wurde beispielsweise gezeigt, dass in einem 100'000 Knoten umfassenden Netzwerk eine Einschleusung von 1000 fehlerhaften Knoten eine Verminderung von erfolgreichem Weiterleiten der Suchanfragen (Routing) um 35 Prozent bewirkt [19]. Auch bei ausgefeilteren Routing-Techniken, wie 'Secure P2P Routing' (alternative Suchpfade werden benutzt) ist dieses Schadensausmass mit der Kontrolle eines Viertels aller Knoten möglich. In speziellen Fällen wie zum Beispiel beim Pastry Algorithmus, der die ID's im eindimensionalen Raum verteilt, ist eine erfolgreiche Manipulation noch einfacher. Durch einige Fehlerhafte Knoten, zB. im oberen Bereich der ID's ist es möglich grössere Teile des Netzwerkes lahm zu legen.

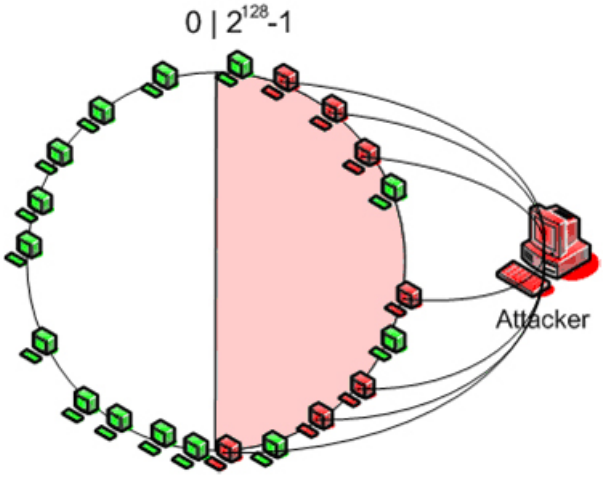



Abbildung 10.19: Sybil Attacke in einem Peer to Peer Netzwerk

In diesem Rahmen ist es auch möglich weiteren Schaden anzurichten und eine sog. Eclipse Attacke zu starten. Es wird versucht das Netzt in 2 Teile zu spalten, so dass die Kommunikation zwischen den Teilen in jedem Fall über einen schadhaften Knoten erfolgen muss. Jetzt werden von den manipulierten Knoten aus die Routingtabellen der gutartigen sabotiert, gefälschte Nachrichten von einem Netz in andere geschickt und weitere Knoten manipuliert [19].

**Vorgehen gegen Sybil Attacke** In momentan verfügbaren P2P Systemen sind relativ wenige Abwehrmechanismen gegen die Sybil Attacken bekannt. Eine Möglichkeit zur eindeutigen Identifikation der Peers wäre ein kontrollierter Zugang via Private Key. Es

soll sich aber zeigen, dass auch ohne die hierbei wieder nötige zentrale Stelle sich die Sybil Attacken limitieren bzw. sehr stark erschweren lassen.

Eine Lösung des Problems ist durch die verteilte Struktur des Netzwerkes keine leichte Aufgabe und wie in allen Bereichen der Informatik lässt sich ein Angriff erschweren, verunmöglichen jedoch nicht.

Man greift hierbei wie bei der Abwehr von DoS - Attacken auf ein 'Puzzle - Solving' zurück. Das bedeutet, dass ein 'interessierender' Knoten zuerst ein Puzzle lösen muss um den Zugang zum System zu bekommen. Das lösen des Puzzles soll so aufwändig gestaltet sein, dass es nicht möglich ist innert vernünftiger Zeit genügend fehlerhafte Knoten einzuschleusen. Dieses Konzept verfolgt das Admission Control System (ACS) für strukturierte P2P Systeme. Hier wird eine hierarchische Anordnung aufgebaut mit einem sog. 'bootstrap' Knoten als Wurzel. Dieser erlaubt vertrauenswürdigen Knoten den Zugang. (z.B. bedeutende ISP's ) Ein Knoten der sich neu im Netzwerk registrieren möchte, muss nun von allen Instanzen bis zur Wurzel Zugang erhalten. Dazu wird auf jeder Stufe ein Puzzle zur Lösung präsentiert. Auf jeder Ebene erhält der Knoten nach erfolgreichem Lösen des Puzzles einen 'Token', was symbolisiert, dass er die Aufgabe dieser Ebene erfolgreich abgeschlossen hat. Die Technik findet beispielsweise im Gnutella Netzwerk Verwendung. Diese Technik bedingt jedoch einiger Kompromisse. Zum einen müssen die Knoten auf höherer Ebene ständig verfügbar und vertrauenswürdig sind. Des Weiteren bedarf die Baumstruktur beim Hinzufügen oder Verschwinden von Knoten einer Reorganisation um die ausgewogene Struktur sicherzustellen.

Wie erwähnt ist damit aber nicht die Attacke unterbunden sondern einfach so erschwert, dass es wenig Sinn macht ein solches Netwerk zu attackieren. Attacken sind dennoch denkbar und lassen sich in zwei denkbare Szenarien unterscheiden:

Zum einen Attacken, bei denen der Angreifer einen Teil der oberen Knoten im ACS ausmacht. Hier kann der betreffende Knoten Token herausgeben um direkt Zugang zu höheren Stellen zu erhalten, ohne alle Puzzles gelöst zu haben. Dies lässt sich jedoch relativ einfach kontrollieren, denn der Elternknoten des bösartigen Knoten kann leicht überprüfen wie viele Token verteilt werden. Überschreitet der Knoten eine gewisse Anzahl verteilter Token, wird er vom Netzwerk mitsamt des ganzen Baumstückes darunter vom Netzwerk getrennt. Nun müssen sich alle Knoten, auch die gutartigen noch einmal anmelden und die Puzzle wieder neu lösen.

Andererseits kann auch von nicht zum ACS gehörenden Knoten Attacken gefahren werden. Da alle Puzzles gelöst werden müssen, dauert es sehr lange, bis ein Angreifer viele Knoten im Netzwerk positioniert hat. Man versucht das weiter zu verhindern, in dem man nur eine kleine Anzahl Token pro Zeiteinheit zulässt.

Letzter Schwachpunkt in dieser Architektur ist die Wurzel, der bootstrap. Hier muss sichergestellt werden, dass sie möglichst immer verfügbar ist. Techniken wie Hot Swap und andere aus Serverbetrieben bekannte Vorkehrungen werden hier angewendet. Bei einem Totalausfall der Wurzel könnte das Netzwerk trotzdem noch über die Level Eins Knoten, die ISP's betrieben werden [19].

**Cutoff Window** Um zu verhindern, dass ein Angreifer über einen langen Zeitraum Identitäten anhäuft um dann eine grosse Attacke zu fahren, verlangt man neben dem lösen der Puzzle zum Einstieg ins Netzwerk von Zeit zu Zeit von jedem partizipierenden Knoten erneut das lösen einer Aufgabe. Die Zeit bis zum Ablauf der Tokens steurt man über das sogenannte Cutoff Window. Dazu hat das jeweils abgegebene Token nur eine bestimmte Gültigkeitsdauer. Vor dem Ablauf kann der Knoten ein neues Token anfordern und so nach erfolgreichem absolvieren der Arbeit ohne Unterbruch weiter operieren. So kann verhindert werden, dass ein Angreifer Token sammeln kann. Natürlich werden auch gutartige Knoten mit zusätzlichem Aufwand belastet, jedoch lässt sich dieser Mehraufwand durch die Grösse des Cutoff Window gut steuern.

**Spezielle Probleme (Startup Network)** Grossen Problemen sieht man sich gegenübergestellt, wenn man analysiert was passieren kann, wenn das Netzwerk gleich beim Start, wenn noch relativ wenige Knoten vorhanden sind, attackiert wird. Es wurde beispielsweise gezeigt, dass in einem Netwerk mit 36 Knoten bereits 4 Knoten ausreichen, um mehr als 10 Prozent zu kontrollieren. Bei 5 Minuten Aufwand um eine ID zu erhalten, würde man dafür nur 20 Minuten benötigen. Ein Schritt wäre in der Anfangsphase die Puzzle massiv aufwändiger zu gestalten und je mehr Knoten vorhanden sind die Schwierigkeit schrittweise zu reduzieren, mit dem Nachteil, dass der Zugang zum Netz in der Anfangsphase drastisch erschwert ist. Besser ist die Lösung bei welcher dem Ersten Knoten ein z.B. zweistündiges Puzzle zu lösen hat, ein weiterer Knoten, welcher 10 Minuten später kommt eines von 1h 50 min usw. Somit werden nach den zwei Stunden auf einen Schlag sehr vielen Knoten Zugang gewährleistet [19].

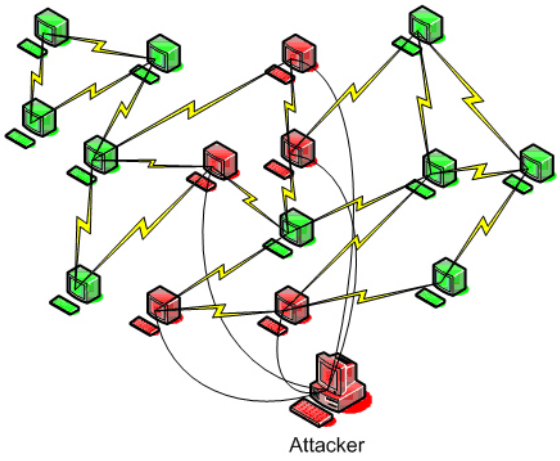



Abbildung 10.20: Sybil Attacke in Initialphase des Netzwerkes

**ACS Simulationen** Als Admission Control System (ACS) bezeichnet man einen kontrollierten Zugang zum Peer to Peer Netzwerk. In der Anfangsphase des Netzwerks ist die Verwundbarkeit hoch und man sucht nach Möglichkeiten die Attacken zu erschweren und minimieren. In einer Simulation [19] des ACS Zugangsmodell bei der verschiedene Cut-off Fenster und verschiedene Angreifer verglichen wurden, wurde festgestellt, dass:

- der Moment, in dem der Angreifer das Netzwerk attackiert sehr wichtig ist. Ein Angriff zu einem Zeitpunkt zu dem das Netz schon über viele gutartige Knoten verfügt ist nicht sehr effizient, vor allem wenn ein einzelner Angreifer tätig ist.
- Der Angriff eines Einzelnen lässt sich einigermassen kontrollieren, so erreicht er auch nach knapp 90 Stunden nicht mehr als 10 Prozent der Knoten zu sabotieren
- Die Attacke von mehreren, in diesem Falle 8 Angreifern, führt aber in der gleichen Zeit zu einer Manipulation von 35 Prozent der Knoten
- Durch ein gezieltes Cut-off Window lassen sich diese Zahlen auf unter ein Prozent für einen Angreifer, respektive 5 Prozent für die 8 Angreifer reduzieren.
- Setzt der Angriff gleich zur Initialzeit des Netzwerk ein, so vermag der/die Angreifer grössere Bereiche in kurzer Zeit zu kontrollieren. Innerhalb von 5 Stunden verfügten die 8 Angreifer in der Simulation bereits über 6 prozent der Knoten.

## 10.4 Beispiele

### 10.4.1 Data Backup Service

Üblicherweise werden bei Backups Daten auf ein anderes Medium geschrieben, welches als 'sicher' und sich nicht am 'bedrohlichen' Netz befindet. Dies erfordert oft zusätzliche Hardware und eine Menge Speicherkapazitätsmedien, welche diese Daten tragen sowie ein bewachtes Warehouse. Auf der anderen Seite können Backups auch von gewissen Anbietern auf Basis derer Software direkt im Internet erfolgen. Dies ermöglicht ein tägliches Backup ohne grossen Aufwand. Jedoch sind die Preise für einen solchen Backupservice gerade für Privatanwender beträchtlich [31].

pStore ist ein Backup System basierend auf einem adaptiven P2P Netzwerk und verspricht manche Mängel gegenwärtiger Backup-Lösungen zu beheben. Es schöpft unbenützten Festplattenspeicher aus und nutzt verteilte Redundanz für ein günstiges und verlässliches Daten-Backup, und der User benötigt dafür nur eine Internetverbindung. Die Experimente [32] haben ergeben, dass trotz Ausfall von ca. 25 Prozent der Knoten beträchtliche 95 Prozent des Datenbestands vorhanden bleibt. Zudem soll das System weniger als 10 Prozent der Bandweite und 85 Prozet weniger Speicherkapazität als herkömmliche Lösung benötigen. Solche Lösungen könnten vielerlei Kosten und beträchtlichen Aufwand sparen. Ein Benutzer würde seine Backup Files über einen fremden Knoten im Netzwerk hervorrufen. Über ein User-Interface könnte der Benutzer alle seine Funktionen betätigen und das Intervall der Backups individuell konfigurieren.

Im Folgenden werden verschiedene Sicherheitsaspekte bezüglich P2P Backuplösungen behandelt und mögliche Gegenmassnahmen evaluiert.

Die Vertraulichkeit gegenüber den Partnern bestimmt einen wesentlichen Aspekt eines Backup-Konzepts. Es muss ein Ansatz gewählt werden welcher verhindert, dass vertrauliche Daten missbraucht werden können. Demzufolge müsste jeder Rechner dem Partner

seine Daten über einen kryptologischen privaten Schlüssel versenden, welcher nur ihm bekannt ist, um zu verhindern, dass diese Daten in falsche Hände geraten. Die Integrität der Backup-Daten müsste über paarweise Authentifikation über einen geteilten privaten Schlüssel verlaufen. Zusätzlich soll es nicht möglich sein bei der Übertragung der Backups an den Daten beziehungsweise Dokumenten weiterzuarbeiten, um Kollisionen zu vermeiden. Über ein integriertes Dokumentenmanagementsystem wird gewährleistet, dass immer das letzte Backup über die Versionsnummer lokalisiert wird.

Ein Aspekt, dem viele P2P Systeme nicht gewappnet sind, ist die Trittbrettfahrerei-Problematik. Im Zusammenhang mit Backups würde dies bedeuten, dass der Trittbrettfahrer seine Dokumente über Partner speichern würde, selber aber keinen Platz zur Verfügung stellen würde, eine Ähnliche Verhaltensweise wie die Freeloader. Um dieser Problematik zu begegnen könnten Vereinbarungen getroffen werden, welche gelegentliche Checkups ermöglichen. Dieser Vorschlag aus [31] entspricht einer gewissen Vertrauensbildung. Bei Missbrauch würde der Täter vom Netzwerk verdrängt werden. Zusätzliche schlagen sie vor, eine maximale Abwesenheit von 2 Wochen zu erlauben, da sonst der Backup zu unregelmässig erfolgen würde. Dies setzt jedoch eine starke Bindung an den Rechner voraus und würde aus unserer Sicht Privatanwender zu wenig berücksichtigen bzw. wäre für den Geschäftsbereich die geeignetere Lösung.

Eine weitere Form der Trittbrettfahrerei ist der Diebstahl von Bandbreite. Zum Beispiel könnte ein Cracker über seinen Backup-Partner (Piraterie-)Software an weitere verbreiten, indem er seine Bandbreite verwendet. Dies würde er erreichen können, indem er die IP-Adresse via Email an seine Verbündeten versenden würde. Die Empfänger könnten dann die Software über das Opfer downloaden und ihm so hohe Übertragungslasten zufügen. Dieser Problematik könnte leicht begegnet werden, indem nur eine beschränkte Anzahl Lese-, und Schreibrechte pro Tag zur Verfügung gestellt würden. Diese Beschränkungen müssten aber je nach Fall bzw. Anforderung unterschiedlich definiert sein.

Eine weitere Bedrohung ist die böswillige Zerstörung des Netzes, welche entweder aus Prestige-Gründen oder gezielt auf eine Person oder Firma erfolgen könnte. Diese Bedrohung beinhaltet zwei unterschiedliche Ausprägungen. Einerseits dass Daten vernichtet werden und andererseits, dass bestimmte Personen vom Netzwerk ausgeschlossen werden. Der Angreifer des Disrupter Attack versucht über die Kontrolle von mehreren Partner, den gesamten Backup zu verhindern. Die Kontrolle über viele Partner setzt aber die erwähnten Bedingungen in diesem Kapitel voraus, dass er mit einer Grosszahl von Partnern den Speicherplatz teilt, das heisst auch ihnen gewissen Speicherplatz anbietet, nur so könnte ein grosser Schaden angerichtet werden. Dies erfordert aber eine enorme Speicherkapazität auf Seiten des Angreifers, was dieses Unterfangen nur beschränkt attraktiv macht. Diesen hohen Speicherplatz kann er nur umgehen, wenn er einen aktiven Man-in-the Middle Angriff lanciert und den Partnern den Anschein gibt, die Daten lokal auf seinem Rechner zu halten, wobei er diese Daten nur zwischen seinen Partnern weiterreicht. Eine Massnahme gegen solche Angriffe wäre, von Zeit zu Zeit die Block-Zugangs-Protokolle leicht zu ändern. Dass heisst, der Man-in-the-middle könnte den zufällig zu lesenden Block nicht dem Partner zur Verfügung stellen und die Attacke würde demzufolge auffliegen.

Dieser Ansatz verhindert trotzdem nicht die Möglichkeit, dass ein Angreifer spezifisch einen oder wenige Rechner attackiert.

Die genannten Attacken sind im Gegensatz zu anderen Sicherheitbedrohenden Angriffen wie Virus, denial-of-service eher uneffizient, da sie 'nur' den Backup verhindert und in dem Sinne nicht zu Datenverlusten führt, bzw. erst nach längerer Zeit zu schwerwiegenden Verlusten führen können. [31]

### 10.4.2 File Storage Service

Die File-Verwaltung in P2P Netzwerke ist mit wesentlich höherem Aufwand und anderen Anforderungen zu gewährleisten als in gewöhnlichen Client-Server-Architekturen, wo die Aufgaben zur Verwaltung der Files und Daten zentral über den Server geregelt werden. Die Files sind auf mehreren Knoten im System gespeichert und werden über eine Sequenz von Ziffern gekennzeichnet. Im Gegensatz zu File-Sharing Applikationen, wo nach bestimmten Inhalten gesucht wird gelingt die Suche im Datenspeichersystem nur über diese Sequenz pro File, welches den gesuchten Ort angibt [18]. Ein mögliches Angriffszenario wäre, wenn ein im Netzwerk partizipierender Knoten vorgibt Informationen und Daten zu speichern, den Zugriff zu diesen jedoch verweigert oder diese gar nicht besitzt. Diese Problematik kann mit dem falschen Weiterleiten bei Suchanfragen verglichen werden. [38] schlagen in ihrem Paper folgende Gegenmassnahmen vor, um dieser Attacke entgegenzuwirken. Sie empfehlen Replikate über das ganze Netzwerk über verschiedene Knoten zu halten, um die Abhängigkeit von einem möglicherweise unkorrekten Knoten zu vermindern bzw. die Verantwortung über die Existenz von Daten auf verschiedene Knoten zu verteilen. Dies setzt voraus, dass die Knoten unabhängig von einem einzigen Knoten auf Replikas zurückgreifen können und dieser Zugang ermöglicht wird. Ihre Faustregel besagt, dass auf jeden Fall ein einziger verantwortlicher Knoten verhindert werden muss, damit das Vorhandensein von Daten jederzeit gewährleistet ist. Die Sicherheitsbedenken in diesem Aspekt sind demzufolge die Zugangsberechtigungsregeln der Knoten in Anbetracht der Schreib-, Leserechte über die Files. Eine mögliche Zugangskontrollliste könnte auch das Verhalten der einzelnen Peers überwachen und es organisieren, damit diese ordnungsgemäss agieren und fehlerhafte Knoten ausschliessen [33] [18].

## 10.5 Fazit Sicherheit in Peer to Peer Netzwerke

Zurzeit stellt P2P momentan noch keine genügende Lösung für Businessanwendungen dar. Diesbezüglich fehlen noch geeignete Massnahmen um die bestehenden Sicherheitsprobleme zu lösen. Der Sicherheitsaspekt gewinnt erst seit kurzem grössere Bedeutung in der Forschung und Entwicklung der Systeme. Der böse Ruf von P2P-Netzwerken verdrängt das möglich Potenzial, geeignete Anwendungsgebiete zu entdecken. Zweifelsohne stellten P2P-Anwendungen eine Lösung für bestehende und in Zukuft zu erwartende Kommunikationsengpässe dar. Bestehende Lösungen stellen immer einen Tradeoff bezüglich Sicherheit und Performanz dar, der in vielen Fällen in Richtung Performance deutet. Zum einen können Firmen problemlos bereits heute P2P-Applikationen wie beispielsweise Skype verwenden, es ist jedoch nicht zu empfehlen vertrauliche Daten über diesen Kanal auszutauschen. Auf der anderen Seite können P2P-Applikationen auf Sicherheitsaspekte fokussiert sein, diese 'sicheren' Lösungen beeinträchtigen jedoch die Performanz stark

und hemmen entsprechend die Benutzbarkeit der Lösung. Ziel bzw. Fokus zukünftiger Forschung in diesem Bereich sollten Sichere Lösungen ohne allzu grosser Beeinträchtigung der Performanz darstellen.

# Literaturverzeichnis


[1] Sarah Mcbridge and Geoffrey A. Fowler,Studios See Big Rise In Estimates of Losses To Movie Piracy, Wall Street Journal Online, 03.05.2006, http://online.wsj.com/article_print/SB114662361192442291.html.

[2] Motion Picture Association Of America Website, http://www.mpaa.org/ zuletzt besucht: 12.05.2006.

[3] Napster Website, http://www.napster.com/ zuletzt besucht: 02.06.2006.

[4] Recording Industry Association of America Website, http://www.riaa.com/ zuletzt besucht: 12.06.2006.

[5] Yucatan guide, Fakten und Zahlen von Mexiko http://www.yucatan-guide.de/land_leute.htm zuletzt besucht: 25.06.2006.

[6] Emule Project Website, http://www.emule-project.net/ zuletzt besucht: 02.06.2006.

[7] Kazaa Website, http://www.kazaa.com/ zuletzt besucht: 06.06.2006.

[8] Slyck Website, P2P Statistiken, http://www.slyck.com/stats.php/ zuletzt besucht: 24.05.2006.

[9] Skype Internettelefonie Website, http://www.skype.com/ zuletzt besucht: 12.05.2006.

[10] SETI Project Website, http://setiathome.berkeley.edu/ zuletzt besucht: 24.05.2006.

[11] Informationen zu SETI, http://en.wikipedia.org/wiki/SETI/ zuletzt besucht: 02.06.2006.

[12] Opencola Project Info, http://www.infotoday.com/newsbreaks/nb021118-2.htm/ zuletzt besucht: 12.06.2006.

[13] Opencola Website -> nicht mehr im Betrieb), http://www.opencola.com/ kein Besuch möglich.

[14] Groove Office von Microsoft, http://www.groove.net/home/index.cfm/ zuletzt besucht: 02.06.2006.

[15] BBC iMP Player, `http://www.bbc.co.uk/dna/mbimp/` zuletzt besucht: 24.05.2006.

[16] Senator Hatch, `http://hatch.senate.gov//` zuletzt besucht: 24.05.2006.

[17] Warner vertreibt Filme per BitTorrent, `http://www.spiegel.de/netzwelt/netzkultur/0,1518,415303,00.html/` zuletzt besucht: 24.05.2006.

[18] Ralf Steinmetz, Klaus Wehrle, Peer-to-Peer Systems and Applications, Lecture Notes on Computer Science Volume 3485, Springer Publishing, ISBN: 3-540-29192-X.

[19] Hosam Rowaihy, William Enck, Patrick McDaniel, and Thomas La Porta, Department of Computer Science and Engineering, Pennsylvania State University, Limiting Sybil Attacks in Structured P2P Networks.

[20] Dragos Ilie Karlskrona, Blekinge Institute of Technology, Gnutella Network Traffic Measurements and Characteristics.

[21] Hari Balakrishnan, M. Frans Kaashoek, David Karger, Robert Morris, Ion Stoica, MIT Laboratory for Computer Science, Looking up data in P2P Systems.

[22] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, Scott Shenker, Dept. of Electrical Eng. + Comp. Sci., University of California, Berkeley, A Scalable Content-Addressable Network.

[23] I poisoned P2P networks for the RIAA, `http://www.theregister.co.uk/2003/01/17/i_poisoned_p2p_networks/` zuletzt besucht: 24.06.2006.

[24] IFPI, `http://www.ifpi.org/` zuletzt besucht: 24.06.2006.

[25] Kazaa File Rating, `http://www.kazaa.com/us/help/glossary/ratings.htm/` zuletzt besucht: 02.06.2006.

[26] ShareDB, `http://www.sharedb.com/` zuletzt besucht: 24.05.2006.

[27] HashDB, `http://www.hashdb.com/` zuletzt besucht: 12.06.2006.

[28] Landon P. Cox, Brian D. Noble, University of Michigan, Samsara: Honor Among Thieves in Peer-to-Peer Storage.

[29] DC Plusplus, `http://dcplusplus.sourceforge.net/` zuletzt besucht: 02.06.2006.

[30] Netlimiter, `http://www.netlimiter.com/` zuletzt besucht: 12.06.2006.

[31] Mark Lillibridge, Sameh Elnikety, Andrew Birrell, Mike Burrows, Michael Isard, HP Systems Research Center, A Cooperative Internet Backup Scheme.

[32] Christopher Batten, Kenneth Barr, Arvind Saraf, Stanley Trepetin, Laboratory for Computer Science, MIT, pStore: A Secure P2P Backup System.

[33] Emil Sit, Robert Morris, Laboratory for Computer Science, MIT, Security Considerations for Peer-to-Peer Distributed Hash Tables.

[34] PGP Website, `http://www.pgp.com` zuletzt besucht: 24.05.2006.

[35] DoS, http://www.cert.org/tech_tips/denial_of_service.html zuletzt besucht: 12.06.2006.

[36] DoS auf Wikipedia, http://en.wikipedia.org/wiki/Denial_of_service#Distributed_DoS_.28DDoS.29_attacks zuletzt besucht: 02.06.2006.

[37] Vorlesungsunterlagen SS2006 Peer to Peer Systems and Applications, Prof. Dr. Burkhard Stiller, http://www.csg.unizh.ch/ zuletzt besucht: 24.05.2006.

[38] Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems, http://research.microsoft.com/~antr/PAST/pastry.pdf/ zuletzt besucht: 24.05.2006.

[39] SplitStream: High-Bandwidth Multicast in Cooperative Environments, http://project-iris.net/irisbib/papers/splitstream1:sosp19/paper.pdf zuletzt besucht: 24.05.2006.

[40] Vorlesungsunterlagen Sicherheit in der Informationstechnik, PD Dr. Rolf Oppliger, Universität Zürich.

[41] Vulnerabilities of P2P Systems, http//www.medianet.kent.edu/surveys/IAD06S-P2PVulnerabilities-marling/index.html zuletzt besucht: 12.06.2006.

# Kapitel 11

# Internet Protokoll Version 6

*Norbert Bollow, Thomas Rauber, Tobias Wolf*

IPv6 *ist eine Weiterentwicklung des Internet Protokolls, die die aktuelle Version* 4 *ersetzen soll. Diese Seminararbeit gibt einen Überblick über die* IPv6*-Protokollarchitektur und die zugrundeliegenden technischen und sozioökonomischen Anreize und offenen Fragen. Wir sagen voraus, dass sich* IPv6 *durchsetzen wird, wenn auch eher langsam.*

*Schwerpunkte unserer Beschreibung der Protokollarchitektur sind das Format des neuen, vereinfachten Headers, die Möglichkeiten der* IPv6 *Kommunikation mit mobilen Geräten und die neuen Möglichkeiten zur automatischen Konfiguration von IP-Adressen. Wir vergleichen* IPv4 *und* IPv6 *im Hinblick auf Paketformat, Fragmentierung, Adressierung, Neighbor Discovery und Netzwerkkonfiguration. Ausserdem diskutieren wir die Möglichkeiten von* IPsec *in den Bereichen von Authentifizierung und Verschlüsselung sowie das* IKE *Protokoll zum Schlüsseltausch, sowie noch offene Sicherheitsfragen im Bereich von Neighbor Discovery und Multihoming.*

*Schliesslich diskutieren wir die Machbarkeit der Umstellung auf* IPv6 *und die ökonomischen Anreize, die gegeben sein müssen, damit* IPv6 *sich insbesondere gegen die Alternative der Ausweitung des Einsatzes von* NAT (*Network Address Translation*) *durchsetzen kann. Wir stellen fest, dass in der jetzigen Situation die ökonomischen Anreize dafür nicht ausreichen. Es ist also damit zu rechnen, dass* IPv6 *sich erst dann wirklich durchsetzen kann, wenn durch technische Fortschritte in anderen Bereichen (beispielsweise durch ein neues Schicht* 4 *Protokoll) die ökonomische Situation für die Umstellung auf* IPv6 *günstiger geworden ist.*

## Inhaltsverzeichnis

**11.1 Einleitung . . . . . 345**
**11.2 Einzelheiten zu IPv6 . . . . . 346**
11.2.1 Der IPv6 Header . . . . . 346
11.2.2 IPv6-Adressen . . . . . 348
11.2.3 Autokonfiguration . . . . . 350
11.2.4 IPv6 Routing . . . . . 351
11.2.5 Experimentelle Nutzung von IPv6 über 6to4 Relays . . . . . 354
11.2.6 Mobile IP . . . . . 355
11.2.7 Zusammenfassung . . . . . 357
**11.3 Vergleich zu IPv4 . . . . . 357**
11.3.1 Paketformat . . . . . 358
11.3.2 Fragmentierung . . . . . 358
11.3.3 Adressierung . . . . . 359
11.3.4 Neighbor Discovery Protokoll . . . . . 360
11.3.5 Netzwerkkonfiguration . . . . . 361
11.3.6 Zusammenfassung . . . . . 362
**11.4 Sicherheit (IPsec) . . . . . 362**
11.4.1 Authentifizierung (AH) . . . . . 363
11.4.2 Verschlüsselung (ESP) . . . . . 363
11.4.3 Schlüsselaustausch (IKE) . . . . . 364
11.4.4 Zusammenfassung . . . . . 365
**11.5 Offene technische und Sicherheitsfragen . . . . . 366**
11.5.1 Neighbor Discovery Sicherheit . . . . . 366
11.5.2 Multihoming . . . . . 368
11.5.3 Zusammenfassung . . . . . 368
**11.6 Machbarkeit der Umstellung auf IPv6 . . . . . 369**
11.6.1 Software . . . . . 369
11.6.2 IPv6 Anbieter in der Schweiz . . . . . 369
11.6.3 Internationaler Rückgang des Enthusiasmus für IPv6 . . . . . 370
**11.7 Ökonomische Aspekte der Umstellung auf IPv6 . . . . . 371**
11.7.1 Die fehlende Kompatibilitätsforderung . . . . . 372
11.7.2 Vergleich zu NAT . . . . . 373
11.7.3 Verschiedene mögliche Entwicklungen . . . . . 374
11.7.4 Ausser IPv4 (mit NAT) keine Alternativen zu IPv6 . . . . . 375
11.7.5 Beurteilung der verschiedenen Szenarien . . . . . 376
**11.8 Ausblick . . . . . 377**

## 11.1 Einleitung

Unser Ziel mit der vorliegenden Arbeit besteht darin, uns einen Überblick über die IPv6-Protokollarchitektur und die zugrundeliegenden technischen und sozioökonomischen Anreize zu verschaffen.

Unsere Methode besteht zunächst einmal in der Lektüre der von der IETF bereitgestellten „RFC“ („Request for Comments“) Dokumente. Die IETF (Internet Engineering Task Force) ist sehr informell organisiert; es handelt sich weniger um eine Organisation als um einen weitgehend Internet-basierten Prozess, in dem alle an der Weiterentwicklung des Internets interessierten Personen mitarbeiten können. Die in diesem Prozess verabschiedeten Dokumente werden als „RFC“ („Request for Comments“) bezeichnet. Diese Bezeichnung betont, dass technisch fundierte Einwände und Verbesserungsvorschläge jederzeit willkommen sein sollen; dies ist eine Grundlage der Diskussionskultur, auf der die IETF aufgebaut ist. Die Bezeichnung „RFC“ sollte nicht als Aussage darüber verstanden werden, inwieweit die Aussagen des Dokuments als für das Internet verbindlich anzusehen sind. Viele RFCs werden als Standards für das Internet angesehen; die Anreize für ihre Einhaltung sind sozialer und ökonomischer Natur. Eine Durchsetzung solcher Standards durch irgendeine Form von Polizeigewalt gibt es nicht. Andere RFCs haben eher den Charakter eines Diskussionsbeitrags, der als langfristig interessant angesehen wird. Auf jeden Fall wird der IETF-Prozess in der weltweiten Internet-Community als entscheidend für die Entwicklung der grundlegenden Internet-Protokoll-Infrastruktur angesehen. Wir sehen deshalb die in diesem Prozess produzierten RFC-Dokumente als einen wesentlichen Ausgangspunkt für die vorliegende Seminararbeit an.

Darüber hinaus haben wir die von den Seminar-Organisatoren vorgeschlagene weitere Literatur beachtet und auch selber Literatur gesucht, mit dem Ziel, uns ein realistisches Bild zu verschaffen, inwieweit die im IETF-Prozess erarbeiteten Ideen in der Praxis umgesetzt werden. Neben den technischen Spezifikationen sind dabei auch die wirtschaftlichen Rahmenbedingungen und Anreize zu beachten. Von besonderem Interesse in diesem Zusammenhang ist die von Bernstein [3] an der Vorgehensweise der IETF geäusserte, begründete Kritik. Bernsteins Einwand betrifft einen ökonomischen Aspekt, der in der IETF zu wenig beachtet wird. Dennoch sagen wir voraus, dass sich `IPv6` durchsetzen wird, wenn auch eher langsam, und möglicherweise erst nachdem sich durch technische Weiterentwicklungen auf anderen Protokollschichten neue Anreize für `IPv6` ergeben.

Die Seminararbeit ist wie folgt strukturiert: **Abschnitt 11.2** gibt einen Überblick über die Ausgestaltung des neuen Internet Protokolls IPv6, wobei insbesondere auf das Format des neuen, vereinfachten Headers, auf die Möglichkeiten der `IPv6` Kommunikation mit mobilen Geräten und auf die neuen Möglichkeiten zur automatischen Konfiguration von IP-Adressen eingegangen wird. Im **Abschnitt 11.3** vergleichen wir `IPv4` und `IPv6` im Hinblick auf Paketformat, Fragmentierung, Adressierung, Neighbor Discovery und Netzwerkkonfiguration. Anschliessend diskutieren wir in **Abschnitt 11.4** die Möglichkeiten von `IPsec` in den Bereichen von Authentifizierung und Verschlüsselung sowie das `IKE` Protokoll zum Schlüsseltausch, und in **Abschnitt 11.5** die noch offenen Sicherheitsfragen im Bereich von Neighbor Discovery und Multihoming. Schliesslich besprechen wir in den **Abschnitten 11.6 und 11.7** die Voraussetzungen und die ökonomischen Anreize für die Umstellung auf `IPv6`.

## 11.2 Einzelheiten zu IPv6

Dieses Kapitel soll einen Überblick über die Ausgestaltung des neuen Internet Protokolls IPv6 geben. Es wird auf das Format des neuen, vereinfachten Headers eingegangen, wie auch auf die optionalen Erweiterungs-Header. Es wird aufgezeigt, wie eine IPv6-Adresse dargestellt wird und welche Möglichkeiten für Kurzschreibweisen der doch erheblich längeren Adressen es gibt. Eine Neuerung in IPv6 ist die Möglichkeit zur Stateless Address (Auto) Configuration. Ihre Funktionsweise wird betrachtet und die damit verbundene Duplicate Address Detection erläutert. Weiterhin diskutieren wir, wir mit der 6to4-Technik IPv6-Pakete über das IPv4-Internet getunnelt werden können, ohne dass dieser Tunnel explizit konfiguriert werden muss. Abschliessend widmen wir uns der Mobilitätsunterstützung von IPv6 und betrachten die beiden Ansätze für Mobile IP.

### 11.2.1 Der IPv6 Header

Genau wie in IPv4 und in vielen anderen Protokollen besteht auch in IPv6 jedes Paket aus 2 Komponenten, dem Header und der Payload. Es besteht jedoch die Möglichkeit der Verkettung mehrerer Header. Der IPv6 Header ist durch den vergrösserten Adressraum um einiges grösser als der IPv4 Header. Vom Aufbau her ist er aber wesentlich einfacher gestaltet als sein Vorgänger. Seine Länge ist fix und er besteht aus weniger Feldern, wodurch er einfacher zu verarbeiten ist.

#### Der IPv6 Basis-Header

Der IPv6 Basis-Header ist immer 40 Bytes gross und besteht aus insgesamt 8 Feldern. In der Abbildung 11.1 ist der Aufbau des IPv6 Basis-Header grafisch veranschaulicht.[9]

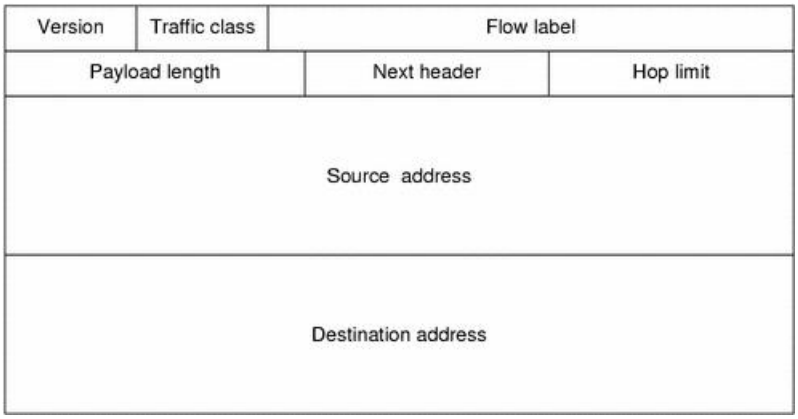



Abbildung 11.1: Der IPv6 Header

Im Folgenden werden die einzelnen Felder des IPv6 Basis-Headers kurz erläutert:

**Version (4bit):** Dieses Feld dient zur Angabe der verwendeten IP-Version. In unserem Falle hätte das Feld den Wert $0110_2$, also 6 für IPv6. Dadurch ist es möglich, dass ein Knoten sowohl IPv6- als auch IPv4-Pakete verarbeitet.

**Traffic class (8bit):** Dieses Feld dient der Priorisierung von Paketen. Anhand dieses Feldes können Pakete von Anwendungen mit unterschiedlichen Anforderungen an das Netzwerk unterschieden werden und somit QoS (Quality of Service) besser eingehalten werden. Im Falle von Stausituationen in einem Knoten können bestimmte Pakete bevorzugt bzw. zurückgestellt werden. Natürlich darf dieses Feld nicht beliebig durch den Benutzer gesetzt werden, sondern muss durch die Anwendung bzw. eine Netzwerküberwachungsinstanz sinnvoll gesetzt werden.

**Flow label (20bit):** Dieses Feld dient zur Kennzeichnung von zusammengehörenden Datenflüssen. Das heisst zur Kennzeichnung einer Sequenz von IP-Paketen einer Applikation, die alle an dieselbe Zieladresse gerichtet sind, beispielsweise von einer Videoübertragung. Gekennzeichnete Pakete können gesondert behandelt werden und somit effizienter durch das Netz geschleust werden. Gehört ein Paket nicht zu einem Datenstrom und bedarf deshalb auch keiner gesonderten Behandlung, so enthält das Feld den Wert 0. Damit das Flow Label effizient ausgewertet werden kann, steht es vorne im Header und ist stets unverschlüsselt.

**Payload Length (16bit):** Dieses Feld gibt die Grösse der transportierten Nutzdaten in Bytes an. Es werden sämtliche hinter diesem IP-Header folgenden Bytes bis zum Ende des Paketes gezählt, inklusive der optionalen Erweiterungs-Header.

**Next Header (8bit):** Wie bereits erwähnt, gibt es in `IPv6` optionale Erweiterungs-Header. Dieses Feld enthält den Code des nächst folgenden Headers. Es werden dieselben Werte verwendet wie im `IPv4`-Protokoll-Feld.

**Hop Limit (8bit):** Dieses Feld gibt die maximale Anzahl von Routern an, die das Paket auf seinem Weg vom Startpunkt zu seiner Destination durchlaufen darf. Jeder passierte Router dekrementiert diesen Wert um 1. Erreicht dieses Feld den Wert 0, so wird das Paket verworfen und eine Fehlernachricht (über eine ICMP-Nachricht) an den Absender zurückgesendet. Dadurch wird verhindert, dass ein fehlgeleitetes Paket beliebig lange im Kreis herum geschickt wird.

**Source Address (128bit):** Dieses Feld enthält die `IPv6`-Adresse des Absenders. Diese Adresse ist immer eine Unicast-Adresse.

**Destination Address (128bit):** Dieses Feld enthält die `IPv6`-Adresse des Empfängers. Dies kann eine Unicast-, Multicast- wie auch eine Anycast-Adresse sein (Siehe Kapitel „Unicast, Multicast und Anycast“).

### Erweiterungs-Header

Im Feld „Next Header“ wird der Protokolltyp des zu transportierenden Paketes mitgeführt, wobei eine mehrfache Verschachtelung von Headern möglich ist. Die verschachtelten Header werden als Erweiterungs-Header bezeichnet. Durch die Verwendung dieser Erweiterungs-Header können die verschiedensten Funktionen erfüllt werden, wie beispielsweise das Tunneling von Protokollen, Source Routing, Authentication,...

Wenn mehrere Erweiterungs-Header ineinander verschachtelt sind, ist es notwendig, dass eine bestimmte Reihenfolge eingehalten wird. Der Header für das Source Routing wird

direkt im Router verarbeitet und darf daher nicht verschlüsselt sein. Er muss also vor dem verschlüsselten Teil stehen. Der für die Nutzlast verantwortliche Header muss ganz am Ende stehen.

Die Reihenfolge der einzelnen Header wurde in [RFC2460] wie folgt festgelegt.

**Reihenfolge der Erweiterungs-Header:**

- `IPv6` Basis-Header
- Hop-by-Hop Option Header
- Destination Options Header
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulation Security Payload Header
- Destination Options Header
- Upper Layer Header

### 11.2.2 `IPv6`-Adressen

Die markanteste Änderung von `IPv4` zu `IPv6` ist die Erweiterung des Adressraumes. Es stehen neu 128 bit anstelle von den bisher verfügbaren 32 bit zur Verfügung. `IPv6` stellt also ca. $10^{38}$ verschiedene IP-Adressen bereit. Zu den in `IPv4` bereits bekannten Adresstypen Unicast und Multicast ist noch der Anycast Typ dazu gekommen. [17] Auf die Charakteristiken dieser drei Typen gehen wir im Abschnitt „Unicast, Multicast und Anycast“ ein.

#### Schreibweise und Struktur einer `IPv6` Adresse

Würde man eine `IPv6` Adresse genau wie eine `IPv4` Adresse schreiben, so würde man eine sehr lange Zahlenkette erhalten. Zur Vereinfachung hat man sich entschieden, eine `IPv6` Adresse in 8 durch Doppelpunkt voneinander getrennte Zahlenblöcke einzuteilen, die jeweils als 4stellige Hexadezimalzahl geschrieben werden.

**Beispiel:** 1234:3EF4:573A:8356:005B:0000:4305:6543

Führende Nullen in einem Block können weggelassen werden. Jeder Block muss aber immer mindestens eine Hexadezimalziffer enthalten (mit Ausnahme der im nächsten Abschnitt beschriebenen Situation).

**Beispiel:**

1234:3EF4:573A:8356:5B:0:4305:6543

Die oben bereits erwähnte Ausnahme bildet eine Folge von Blöcken, die nur aus Nullen besteht (0000). Solche Folgen können ganz weggelassen werden und werden durch 2 aufeinanderfolgende Doppelpunkte (::) repräsentiert. Der durch die zwei Doppelpunkte abgekürzte Bereich wird dann um die nötige Anzahl von Null-Blöcken erweitert, bis die Adresse wieder aus 8 Blöcken besteht.

**Beispiel:**

1234:0000:0000:0000:0000:7356:A456:97F3

ist gleichbedeutend wie

1234::7356:A456:97F3

Aus Gründen der Eindeutigkeit der Adressen darf jeweils nur eine Folge von Nullen abgekürzt werden. Bei den weiteren dürfen nur die führenden Nullen weggelassen werden, eine Null muss aber geschrieben werden.

**Beispiel:**

1234:0000:0000:7356:A456:0000:0000:97F3

zulässig Abkürzungen sind:

1234::7356:A456:0:0:97F3 1234:0:0:7356:A456::97F3

nicht zulässig ist:

1234::7356:A456::97F3

Die IP-Adressen verfügen über eine flexible Struktur, wobei die vorderen Bits zur Kennzeichnung des Netzes verwendet werden. Dies ist aus `IPv4` unter dem Begriff der Subnetzmaske bekannt. Dazu schreibt man hinter der IP-Adresse durch ´/´ getrennt die Anzahl Bits, die notwendig sind, um das Netz zu kennzeichnen.

**Beispiel:**

3625:7465:53:342A::/56

### Unicast, Multicast und Anycast

In `IPv6` gibt es drei verschiedene Adresstypen: die Unicast-, Multicast- und Anycast-Adressen. Unicast-und Multicast-Adressen gab es auch schon in `IPv4`. Zudem gab es in `IPv4` noch die Broadcast-Adressen, diese wurden aber in `IPv6` nicht übernommen und durch den gezielten Einsatz der Multicast-Adressen ersetzt.

**Unicast:** Eine Unicast-Adresse bezieht sich immer nur auf einen Knoten im Netz. Die Source Address im Header ist immer eine Unicast- Adresse. Die Menge der Unicast-Adressen kann weiter in Global-Unicast, Site-Local-Unicast und Link-Local-Unicast unterteilt werden. Link-Local-Unicast haben das Präfix FE80::/10. Sie können nur zur Kommunikation innerhalb des entsprechenden physikalischen Links verwendet werden. Site-Local-Unicast lassen sich durch das Präfix FEC0::/10 erkennen. Sie werden von Border-Routern nicht weitergeleitet und können somit das jeweilige Netz nicht verlassen. Für Global-Unicast-Adressen gibt es keine Beschränkungen, sie können überall eingesetzt werden.

**Multicast:** Mittels Multicast kann ein Paket an eine Gruppe gesendet werden. Dabei wird das Paket an jedes Mitglied der Gruppe übermittelt. Sämtliche Multicast-Adressen beginnen mit dem Präfix FF00::/8.

**Anycast:** Dieser Typ von Adressen ist neu in `IPv6`. Ein Anycast richtet sich wie ein Multicast an eine Gruppe von Empfängern. Das zu sendende Paket wird aber nur an ein Mitglied der Gruppe ausgeliefert. Die Wahl, an welches Mitglied es ausgeliefert werden soll, unterliegt dem Router. Anycast-Adressen haben kein spezielles Präfix, sie sind Teil der Unicast-Adressen und können somit auch nicht von ihnen unterschieden werden. Bei der Konfiguration muss explizit angegeben werden, dass es sich bei dieser Adresse um eine Anycast-Adresse handelt.

### 11.2.3 Autokonfiguration

Anhand seiner Mac-Adresse (Layer 2) kann sich ein Knoten eine Interface-ID berechnen. Die Interface-ID bildet die letzten 64 Bit der späteren IP Adresse. Die Interface-ID ist innerhalb des Links eindeutig und erlaubt es dem Knoten Nachrichten innerhalb des Links zu verschicken, bevor er eine vollständige IP-Adresse hat. Nun kann der Knoten über die Multicast-Adresse FF02::2 alle Router, die sich im selben Segment befinden, erreichen. Auf eine solche Anfrage hin antwortet ein Router mit zahlreichen Informationen. Unter anderem auch mit einem Adressbereich für Unicast-Adressen. Das Gerät kann sich dann selbst eine IP-Adresse aus diesem Bereich zuweisen. Dies läuft vollautomatisch, ohne jegliches Zutun des Benutzers, ab. Bei dieser Art der Adressvergabe handelt es sich um eine „Stateless Address (Auto)Configuration“. Das bedeutet, dass die Zuweisung durch das Gerät selbst stattfindet und nicht Buch geführt wird über die bereits vergebenen Adressen. Zur Vermeidung der Mehrfachvergabe von Adressen existiert DAD (Duplicate Address Detection). Jedes Gerät muss, nachdem es sich eine Adresse zugewiesen hat, DAD durchführen und somit sicherstellen, dass seine Adresse einmalig ist.[42]

#### DAD (Duplicate Address Detection)

DAD muss für jede Unicast-Adresse durchgeführt werden, egal ob diese „stateless“, „stateful“ oder manuell zugewiesen wurde. Wird DAD auf eine Adresse angewandt, so wird diese auf provisorisch gesetzt. Um zu überprüfen, ob die IP-Adresse bereits vergeben ist, sendet der Knoten eine spezielle Anfrage (Neighbor Solicitation) aus. Als Zieladresse enthält die Nachricht die eigene, zu überprüfende Adresse. Dabei muss natürlich sichergestellt werden,

dass kein „Loopback“ stattfindet, ein Knoten also nicht auf seine eigene Anfrage antwortet. Als Absenderadresse wird die unspezifizierte IP-Adresse (0::0) verwendet. Dadurch kann die Nachricht als Nachricht zur Erkennung der doppelten Adressvergabe erkannt werden. Existiert nun bereits ein Knoten, der die zu überprüfende Adresse verwendet, so erkennt er seine eigene Adresse als Zieladresse einer Nachricht zur Erkennung doppelt vergebener Adressen. Er antwortet darauf mit einer Nachbarschaftsbekanntmachung und meldet seiner Managementinstanz, dass seine Adresse doppelt vergeben ist. Beide, also auch der Knoten, der die Adresse bereits besessen hat, werden daraufhin diese Adresse nicht mehr verwenden. Erhält das Gerät aber innerhalb der spezifizierten Zeit keine Antwort auf seine Anfrage, so kann davon ausgegangen werden, dass die Adresse noch nicht vergeben ist. DAD bietet aber keine vollkommene Garantie, dass eine Adresse einmalig ist. Ist beispielsweise ein Knoten kurzfristig vom Netzwerk getrennt, wenn die Anfrage zur Erkennung doppelt vergebener Adressen verschickt wird, so antwortet er nicht, auch wenn er dieselbe Adresse besitzt.[42]

### 11.2.4 `IPv6` Routing

IP befindet sich auf der Schicht 3 (Network Layer) des ISO/OSI-Referenzmodells. Die Aufgabe dieser Schicht besteht im wesentlichen darin, die Übertragung von Nachrichten von einem Sender zum einem Empfänger durch ein beliebig komplexes Netz zu ermöglichen. Diese Kommunikation kann innerhalb eines autonomen Systems stattfinden (Intra Domain) oder aber aus einem autonomen System durch das Internet in ein anderes autonomes System (Inter Domain) führen. Zur Vermittlung innerhalb eines autonomen Systems wie auch zur Vermittlung zwischen autonomen Systemen kommen Router zum Einsatz. Die Aufgabe eines Routers besteht darin, zu entscheiden, welchen Weg ein Paket nehmen soll und es dementsprechend weiterzuleiten. Die Entscheidung wird anhand der IP-Adresse getroffen. Zu diesem Zweck wurde in `IPv6` die Adressarchitektur so gestaltet, dass die Wegwahl einfach ist, aber auch den sich ändernden Umständen im Internet Rechnung getragen werden kann. Die Weiterleitungsentscheidung erfolgt jeweils nach dem Longest Prefix Match-Prinzip. Das bedeutet, dass die Einträge in den Routingtabellen auf ihre Übereinstimmung mit der Zieladresse hin überprüft werden. Ausgewählt wird der längste Eintrag, der vollständig mit den ersten Stellen der Zieladresse übereinstimmt. [43]

Globale Unicast-Adressen besteht aus mehreren Teilen und lassen sich dadurch hierarchisch ordnen. Da eine Adressen ein Zusammenschluss mehrerer Segmente ist, spricht man auch von einer aggregierbaren Adresse. Die einzelnen Bestandteile einer aggregierbaren Adresse werden in der Abbildung 11.2 veranschaulicht.

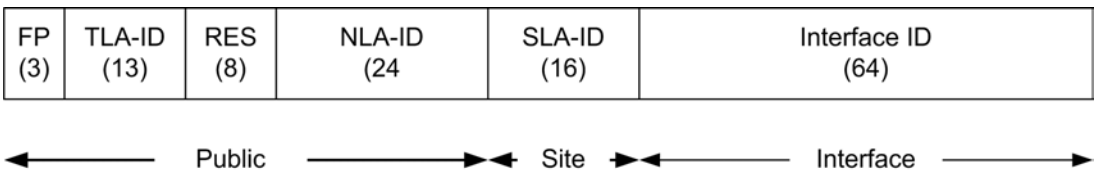



Abbildung 11.2: Aufteilung einer aggregierbaren Adresse

**FP (Format Prefix):** Kennzeichnet eine aggregierbare globale Unicast-Adresse.

**TLA-ID (Top-Level Aggregation Identifier):** Gibt die oberste Hierarchiestufe der Netzbetreiber an.

**RES** Reserviert für Erweiterungen der TLA-ID oder der NLA-ID.

**NLA-ID (Next-Level Aggregation Identifier):** Nächst niedrigere Hierarchiestufe eines Netzbetreibers. Dieser Bereich kann durch den Provider weiter unterteilt werden.

**SLA-ID (Site-Level Aggregation Identifier):** Stufe der privaten Netzbetreiber.

**Interface ID (Interface Identifier):** Kennzeichnung der Schnittstelle eines Netzknotens.

Durch die Möglichkeit der Unterteilung der NLA-ID können verschiedene Hierarchiestufen erreicht werden. Dies liegt in der Kompetenz des Providers. Eine flache Hierarchie erlaubt die optimale Ausnutzung des Adressraumes, lässt aber die Routingtabellen sehr gross werden.

Zur Vergabe von Adressräumen an Endkunden sind drei verschiedene Szenarien vorgesehen. Im Normalfall erhält der Endkunde einen /48-Adressraum. Das entspricht immer noch einer Anzahl von $2^{80}$ oder ca. $1.2 \cdot 10^{24}$ möglichen Adressen. Wenn von Anfang klar ist, dass nur genau 1 Subnetz benötigt wird, wird ein /64-Adressraum vergeben. Ein /128-Adressraum oder genauer gesagt, eine einzige Adresse wird nur dann vergeben, wenn nur ein einzelner Knoten angeschlossen werden soll.[22]

### Intra Domain Routing

Ein privates Netz ist normalerweise durch eine geringe Anzahl von Vermittlern und Verbindungen charakterisiert. Die Komplexität ist gering und das Netz als Ganzes überschaubar. Durch dieses Faktum können ganz andere Mechanismen zur Wegwahl eingesetzt werden als im Inter Domain Routing. Beispielsweise Open Shortest Path First (OSPF) oder Routing Information Protocol (RIP). Sowohl OSPF wie auch RIP sind auch schon in `IPv4` verfügbar, sie wurden aber noch speziell für die Verwendung in `IPv6` angepasst und deshalb werden sie im Weiteren kurz erläutert. [43]

**Open Shortest Path First (OSPF):** Für diese Methode ist es notwendig, dass die Netzwerktopologie und die Verbindungskosten bekannt sind. Dadurch wird dann der Weg mit den geringsten Kosten ausgewählt. Was man unter Wegkosten versteht, muss allerdings zuerst definiert werden. Eine Möglichkeit wäre die Verzögerung (hohe Verzögerung = hohe Kosten). Mittels des Hello-Protokolls, kann durch Hello-Nachrichten an die direkt benachbarten Router die Topologie, ermittelt werden. Wenn die Topologie bekannt ist, werden mittels Shortest Path-Algorithmus von Dijkstra die kürzesten Wege berechnet (Unter folgendem Link finden Sie eine kleine Animation, die den Shortest Path-Algorithmus von Dijkstra gut veranschaulicht und erklärt: http://www.gik.uni-karlsruhe.de/766.html). Das Resultat wird in einer Baumstruktur gespeichert und dient als Basis zur Wegwahl.[43]

**Routing Information Protocol (RIP):** In RIP erfolgt die Weiterleitung nach dem Prinzip der minimalen Anzahl passierter Zwischenkanten. Die Wegkosten werden hierbei

gänzlich ausser Acht gelassen. RIP baut darauf auf, dass die gesamte Struktur eines Netzwerkes bekannt ist und ist deshalb nur für kleine Netzwerke geeignet. Um die anfangs noch leeren Routingtabellen zu füllen, teilt jeder Router den anderen Routern im selben Netz per Multicast mit, an welches Subnetz er angeschlossen ist. Aus den so erhaltenen Informationen werden die kürzesten Wege ermittelt und in der Routingtabelle gespeichert. Ein Router teilt den anderen seine Routingtabelle wie auch allfällige Änderungen im Netzwerk, ebenfalls per Multicast mit. So wird sichergestellt, dass jeder Router über eine aktuelle Routingtabelle verfügt. Da jeder Router allen anderen seine Routingtabelle in gewissen zeitlichen Abständen per Multicast mitteilt, kommt es in grossen Netzwerken zu übermässigem Netzwerkverkehr. Durch jeden zusätzlichen Router wird das Problem noch verschärft, was zur Folge hat, dass RIP für grosse Netze nicht skaliert. [43]

### Inter Domain Routing

Die im Intra Domain Routing eingesetzten Protokolle gehören alle zu der Familie der Exterior Gateway Protocols. Ursprünglich wurde in `IPv6` das Inter Domain Routing Protocol Version 2 (IDRPv2) verwendet. Dieses Protokoll ist für mehrere Protokollfamilien geeignet und unterstützt auch Multiprotokoll-Routing. Später wurde dann aber auch das in `IPv4` verwendete Border Gateway Protocol Version 4 (BGP-4) für `IPv6` angepasst. Das hat dazu geführt, dass momentan 2 Internet-Routing Protokolle für `IPv6` zur Verfügung stehen. IDRPv2 und auch BGP-4 sind sogenannte Pfad-Vektor-Protokolle. Die Wahl des Weges kann dabei wie bei RIP nach der minimalen Anzahl passierter Zwischenknoten bestimmt werden oder aber auch nach einer anderen vorgegebenen Routingstrategie. In die Routingtabelle wird nicht nur der nächste Knoten für das Erreichen eines bestimmten Zieles eingetragen, sondern gleich mehrere, vollständige Wege, die zum Ziel führen. Dadurch kann beim Ausfall von Teilstrecken direkt auf Alternativen zurückgegriffen werden.[43]

**Inter Domain Routing Protocol Version 2 (IDRPv2):** In der Sichtweise von IDRPv2 besteht das gesamte Netz aus Endnetzen oder Transitnetzen. Innerhalb eines Endnetzes werden Intra Domain Routing Verfahren angewendet. Endnetze werden durch sogenannte „Boundary Intermediate Systems“ (BIS) an das Internet angeschlossen. Transitnetze verfügen über eine Transit-Router(TR). Bei IDRPv2 werden nur die BIS und die TR in die Wegwahl miteinbezogen. Jeder Router baut sich durch die Routing- Informationen eine Datenbasis der erreichbaren Ziele auf. Die Routing-Informationen enthalten Pfadangaben der zu erreichenden Ziele und werden nur an direkte Nachbarn gesendet. Um die Routing-Tabellen nicht übermässig gross werden zu lassen wird im Kernbereich des Internets stark zusammengefasst. Die Routing-Informationen werden nicht wie in RIP periodisch verschickt sondern nur nach Änderungen an der eigenen Tabelle. Dadurch wird der Verkehr auf ein Minimum beschränkt.[43]

**Border Gateway Protocol-4 (BGP-4):** BGP-4 ist in seiner Funktionsweise der von IDRPv2 sehr ähnlich. Als Pfad-Vektor-Protokolle speichert es die Informationen für den gesamten Weg, inklusive aller zu passierenden Netze, bis zum Zielnetz fest. Die benötigten Routing-Informationen werden mittels Pakete mit sogenannten „Network Layer Reachability Information“ verschickt. Neben den Weginformationen für erreichbare Netze enthalten die Routing Informationen auch IP-und Link-Layer-Adressen der zu passierenden Router. Anhand dieser Informationen errechnet BGP-4 dann den optimalen Weg.

**Sonderbehandlung von Paketen mit gesetztem Flow Label**

Wir wissen bereits, dass das Flow Label zur Kennzeichnung von sogenannten Datenflüssen dient. Das Flow Label enthält entweder den Wert 0 (ist nicht gesetzt) oder einen zufälligen Wert zwischen 1 und FFFFFF (ist gesetzt). Durch ein gesetztes Flow-Label kann eine gesonderte Behandlung von Paketen im Router erreicht werden. Dies ist aber nicht garantiert, denn die IPv6-Spezifikation erlaubt es, dass ein Router ein gesetztes Flow Label ignoriert. Ist ein Router aber so konfiguriert, dass er Flow Label berücksichtigt, so kann der Routingprozess deutlich beschleunigt werden. Trifft ein Paket mit einem noch nicht bekannten Flow-Label ein, so wertet der Router das Flow-Label sowie die Absende- und Zieladresse aus und trifft seine Routingentscheidung. Den gewählten Weg und das dazugehörige Flow-Label speichert der Router nun für eine gewisse Zeit in seinem internen Cache. Trifft nun ein weiteres Paket mit demselben Flow Label ein, so holt sich der Router die Information über den Weg direkt aus dem Cache. Dadurch werden die markierten Pakete, zum einen, alle auf demselben Weg verschickt und zum anderen auch noch schneller. Gerade für Echtzeitanwendungen ist dies natürlich sehr wünschenswert.[33]

### 11.2.5 Experimentelle Nutzung von IPv6 über 6to4 Relays

Zur Definition der Architektur einer neuen Version eines etablierten Protokolls gehört auch eine Strategie, um die Umstellung auf die neue Version genügend einfach zu machen, während gleichzeitig die Interoperabilität mit Nutzern der alten Version gewahrt bleiben muss.

Die RFCs 3056 und 3068 ([6], [18]) definieren ein Verfahren, durch das jedermann, der über einen IPv4 Internet-Zugang verfügt, Zugang zum IPv6-Internet hat. Die IPv6-Pakete werden dabei über das IPv4-Internet getunnelt, ohne dass eine explizite Konfiguration des Tunnels notwendig wäre. Dies geschieht mittels je einer speziell definierten IPv4- und IPv6-Anycast-Adresse, wie folgt:

Wer einen solchen 6to4 Zugang zum 6to4-Internet möchte, kann ein lokales IPv6-Netzwerk einrichten, das über einen 6to4 Relay-Router mit dem IPv4-Internet verbunden wird. In diesem IPv6-Netzwerk werden sogenannte 6to4-Adressen verwendet, das sind IPv6-Adressen, deren Netzwerk-Teil aus dem Code 2002 (hexadezimal) gefolgt von der IPv4-Adresse des Relay-Routers besteht. In allen Routern des lokalen IPv6-Netzwerk wird die spezielle Anycast-Adresse 2002:c058:6301:: als Defaultroute gesetzt. Der Relay-Router nimmt unter dieser Adresse IPv6-Pakete an, die er in IPv4-Pakete einpackt und über das IPv4-Internet an die als spezielle Anycast-Adresse definierte IPv4-Adresse 192.88.99.1 schickt. Über diese Anycast-Adresse erreichen die Pakete einen Relay-Router, der sowohl mit dem IPv4-Internet als auch mit dem IPv6-Internet verbunden ist. Dort wird das IPv6-Paket wieder ausgepackt und über das IPv6-Internet auf den Weg zur Zieladresse geschickt.

Auch in die andere Richtung, also vom IPv6-Internet zu einem lokalen, über einen 6to4 Relay-Router mit dem IPv4-Internet verbundenen IPv6-Netzwerk, können Pakete übertragen werden: Diese Pakete sind an eine mit 2002 beginnende 6to4-Adresse adressiert, sie

werden deshalb zu einem 6to4 Relay-Router geroutet, der mit dem IPv4-Internet verbunden ist. Dieser Relay-Router packt das IPv6-Paket in ein IPv4-Paket ein, dessen IPv4-Zieladresse aus der 6to4-Adresse entnommen wird, an die das IPv6-Paket adressiert ist. So gelangt das Paket zu dem 6to4 Relay-Router, dessen IPv4-Adresse in der 6to4 IPv6-Adressen enthalten ist.

Im Vergleich zur direkten IPv6-Anbindung über einen IPv6-unterstützenden ISP ergibt sich die zusätzliche Komplikation, dass man ankommende 6to4 Pakete darauf prüfen muss, ob sie gewissen Sicherheits-Bedingungen genügen, siehe [37].

Mit der in diesem Abschnitt diskutierten 6to4-Technik ist es im Prinzip für jedermann einfach möglich, Zugang zum IPv6-Internet zu bekommen. Solange wie alle wichtigen Dienste im Internet bestimmt über IPv4 und nur zum Teil auch über IPv6 erreichbar sind, bedeutet die Verwendung der 6to4-Technik allerdings in der Regel einen Performance-Verlust gegenüber der Verwendung von IPv4: Sei etwa $A$ ein Client, der an das IPv4-Internet angeschlossen ist, der aber (indem er als sein eigener 6to4 Relay-Router agiert) auch mit dem IPv6-Internet kommunizieren kann. Weiterhin sei $B$ ein Server, der über verschiedene Interfaces sowohl mit dem IPv4- als auch mit dem IPv6-Internet verbunden ist. Dann wird es für $A$ in der Regel von Vorteil sein, für die Kommunikation mit $B$ IPv4 zu verwenden, weil bei der Verwendung von 6to4 die Pakete über einen 6to4 Relay-Router geroutet werden müssen, was in der Regel zu einer grösseren Übertragungsverzögerung und im Fall einer starken Auslastung des Relay-Routers zu Paketverlusten führen wird.

Eine mit der Performance von IPv4 vergleichbare Performance lässt sich in der Regel mit IPv6 nur dann erreichen, wenn beide Kommunikationspartner direkt (d.h. nicht über 6to4-Relays) mit dem IPv6-Internet verbunden sind. Die Frage nach ökonomischen Anreizen, die zu einer allgemeinen Umstellung auf IPv6 führen könnten, diskutieren wir unten in Abschnitt 11.7, wo wir darlegen, dass es mit IPv6 in dieser Hinsicht ernsthafte Probleme gibt.

### 11.2.6 Mobile IP

Heutzutage nimmt die Mobilität ständig zu. Ein Gerät hat keinen festen Standort mehr, sondern kann seine Position beliebig wechseln. Trotz der ständigen Wechsel der Position sollte das Gerät so weit als möglich immer erreichbar sein. Befinden wir uns in einem fremden Netzwerk, so können Pakete, die an unsere Heimadresse gesendet werden, uns nicht direkt erreichen. Aufgrund ihres Präfixes der IP-Adresse werden die Pakete an unser Heimnetzwerk gesendet.

Zur Behebung dieses Problems verfügt IPv6 über die Erweiterung „Mobile IP“. Es gibt mehrere Varianten für die Realisierung von Mobile IP. Der erste Ansatz ist in der Abbildung 11.3 veranschaulicht und wird im weiteren noch erklärt.

Mobile IP ermöglicht die Kommunikation unabhängig vom aktuellen Standort. Dies geschieht mit der Hilfe eines sogenannten Home Agent. Dieser Home Agent befindet sich immer im unserem Heimnetz und nimmt Pakete für uns entgegen und übernimmt die Weitervermittlung.

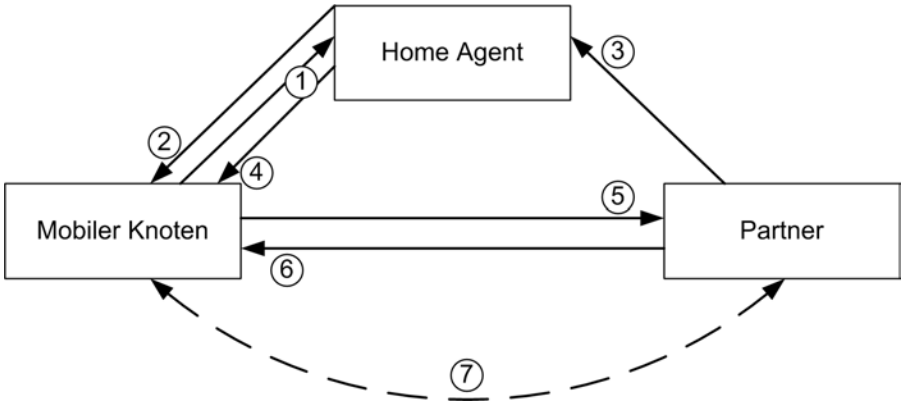



Abbildung 11.3: Arbeitsweise von Mobile-IPv6

Wählt sich ein mobiler Knoten in ein fremdes Netzwerk ein, so erhält er eine IP-Adresse des fremden Netzes zugewiesen.

Nun sendet der mobile Knoten ein Paket mit seiner neuen Adresse (Care-of-Address) und der Binding-Update-Option zu seinem Home Agent (1). Der Home Agent bestätigt das Binding mit der Binding-Acknowledge-Option (2). Will nun ein Partner ein Paket an den mobilen Knoten senden, sendet er es zunächst ins Heimnetz des mobilen Knotens, wo es vom Home Agent entgegengenommen wird (3). Der Home Agent packt das Paket in ein weiteres Paket, das er an den mobilen Knoten sendet (4), dies bezeichnet man als Tunneling. Nach dem Entpacken des ursprünglichen Paketes kennt der mobile Knoten die Adresse des eigentlichen Absenders. Nun kann der mobile Knoten ein Paket mit seiner Care-of-Address und der Binding-Update-Option an den Partner senden (5). Dieser übernimmt die Care-of-Address des mobilen Knotens und antwortet mit der Binding-Acknowledge-Option (6). Von nun an kann die Kommunikation zwischen dem mobilen Knoten und dem Partner direkt stattfinden (7), ohne zuerst über den Home Agenten gehen zu müssen.[43]

Dieser Ansatz wird auch als als Fast Mobile IPv6 bezeichnet, da er ein optimales Routing zwischen dem mobilen Knoten und seinem Partner erlaubt.

Neben dem bereits erklärten Ansatz gibt es noch weitere Ansätze für die Realisierung von Mobile IPv6. Einer ist bis und mit Schritt 4 es vorher erklärten Ansatz identisch. Dabei schickt der mobile Knoten aber keine Binding-Update-Option mit seiner Care-of-Address an den Partner. Der mobile Knoten tunnelt seine Nachrichten zurück an seinen Home Agent, der sie dann zum Partner weiter leitet. Das Tunneling zwischen dem mobilen Knoten und dem Home Agent findet also bidirektional statt. Der Vorteil dieses Ansatzes ist, dass der Partner keine Informationen über das fremde Netzwerk, in dem sich der mobile Knoten aufhält, erhält. Dafür wird aber in Kauf genommen, dass die Pakete unter Umständen massiv längere Wege zurücklegen können.

Ein weiterer Ansatz wird als „Hierarchical Mobile IPv6“ bezeichnet. Dabei kommt neben dem Home Agenten zusätzlich ein mobiler Ankerpunkt („mobile anchor point“) zum Einsatz. Dieser mobile Ankerpunkt fungiert nun gewissermassen wie ein lokaler Home Agent. Der mobile Ankerpunkt bildet die regionale Care-of-Address auf die lokale Care-of-Address ab. Die Kommunikation mit einem Partner, der sich im gleichen Netz befindet

kann unabhängig vom Home Agenten, nur über den Ankerpunkt, geschehen. Wechselt der mobile Knoten nun den Link innerhalb des Netzes, so informiert er nur den Ankerpunkt über seine neue lokale Care-of-Address. Eine Information des Home Agenten ist nur beim Verlassen des Netzwerkes nötig, da nur dabei die regionale Care-of-Adresse ändert.[39]

Mobile IPv6 profitierte von den Erfahrungen, die durch Mobile IPv4 gesammelt werden konnten. Zudem konnten auf der Basis von IPv6 interessante Neuerungen eingebaut werden. Der aus Mobile IPv4 bekannte Foreign Agent wird nicht mehr benötigt. Mobile IPv6 arbeitet in allen Umgebungen ohne eine spezielle Unterstützung durch lokale Router. Optimiertes Routing ist nun ein fester Bestandteil und nicht mehr bloss eine nicht standardisierte Erweiterung. Durch die Verwendung von IPv6 Neighbor Discovery statt ARP ist Mobile IPv6 unabhängig von jedem bestimmten Link-Layer.[24]

### 11.2.7 Zusammenfassung

Die wesentlichste Neuerung in IPv6 ist er massiv vergrösserte Adressbereich. Eine Folge davon ist, dass eine IPv6-Adresse aus 8 Blöcken von jeweils 4 Hexadezimalzahlen besteht. Der IPv6-Header wurde ebenfalls angepasst. Die Anzahl von Feldern wurde reduziert und er verfügt neu über eine feste Grösse. Dadurch ist der IPv6-Header einfacher handhabbar als sein Vorgänger aus IPv4. Zur automatisierten Vergabe von IP-Adressen wurde in IPv6 die Stateless Address (Auto) Configuration eingeführt. Für das Intra-Domain-Routing wurden die bereits in IPv4 verwendeten Algorithmen Open Shortest Path First und Routing Information Protocol übernommen und angepasst. Für das Inter Domain Routing wurde das Inter Domain Routing Protocol Version 2 entwickelt und das Border Gateway Protocol 4 angepasst. Zur Unterstützung der Mobilität ist Mobile IP ein fester Bestandteil von IPv6. Bei der Entwicklung von IPv6 wurden also bewährte Bestandteile aus IPv4 übernommen sowie Schwächen von IPv4, wie die beschränkte Anzahl von Adressen, behoben.

## 11.3 Vergleich zu IPv4

In diesem Abschnitt möchten wir einen groben Vergleich zwischen IPv6 und seinem Vorgänger IPv4 aufzeigen. Wichtige Unterschiede haben sich beim Paketformat, bei der Adressierung und der Behandlung von Fragmentierung ergeben. Diese werden wir im Folgenden detaillierter betrachten, ebenso wie die Unterschiede die sich durch das Neighbor Discovery Protokoll und die neuen Mechanismen zur Netzwerkkonfiguration ergeben haben. Die Neuerungen im Bereich Routing wurden schon in Abschnitt 11.2.4 betrachtet, ebenso wie die erweiterte Unterstützung von mobilen Knoten in Abschnitt 11.2.6. Zuletzt ist auch noch die Unterstützung von Sicherheitsfunktionen (IPsec) zu nennen, die im Gegensatz zu IPv4 nun zwingender Bestandteil von IP in der Version 6 geworden ist. Ein Überblick über IPsec wird noch separat im Abschnitt 11.4 erfolgen.

### 11.3.1 Paketformat

Der neue IPv6 Header wurde bereits im Abschnitt 11.2.1 vorgestellt. Er unterscheidet sich in mehrfacher Hinsicht von dem in IPv4 verwendeten. Während der IPv4 Header eine minimale Länge von 20 Bytes hatte, war er dennoch variabler Grösse, da verschiedene optionale Felder Bestandteil des Headers sein konnten. IPv6 hingegen setzt hier auf ein vereinfachtes System. Der Header ist neu aufgeteilt in einen Main Header mit fester Grösse 40 Bytes, der nur die in jedem Fall notwendigen Felder enthält. Alle Felder, die nicht regelmässig benötigt werden, sowie die Behandlung der Optionen wurden in das Konzept der Erweiterungsheader ausgelagert.

Unverändert blieben die Felder „Version“, „Source Address“ sowie „Destination Address“. Nur ihr Inhalt oder die Feldgrösse wurden angepasst. Zwei Felder wurden der Verwendung nach beibehalten aber umbenannt um die heutige Nutzung besser zu reflektieren, „Traffic Class“ (ehemals „Type of Service“) sowie „Hop Limit“ (früher „Time to Live“). Da der IPv6 Main Header eine feste Grösse besitzt, wurde das „Internet Header Length“ Feld entfernt. Auch die „Header Checksum“ gibt es nicht mehr, da entschieden wurde dass Prüfsummen auf Transport- und Datensicherungsschicht mehr als ausreichend sind. Die für die Fragmentierung relevanten Felder „Identification“, „Flags“ sowie „Fragment Offset“ wurden in einen Erweiterungsheader verlagert, dazu später noch mehr. Hinzugekommen ist nur ein einziges Feld, das „Flow Label“. Schlussendlich verbleiben zwei Felder, die umbenannt wurden und in IPv6 eine etwas andere Semantik als in IPv4 besitzen, „Payload Length“ (vormals „Total Length“) und „Next Header“ (früher „Protocol“).

Wie schon erwähnt werden die vordefinierten IPv4 Optionen in IPv6 mit den Erweiterungsheadern umgesetzt. Dies hat zur Folge, dass neue Optionen unter Umständen eine Neuspezifizierung zur Folge hätten. Um in dieser Hinsicht grösstmögliche Flexibilität zu bewahren, enthält IPv6 noch ein zusätzliches Optionen-System, welches praktisch beliebige Erweiterungen ohne Neuspezifizierung des Protokolls selbst erlaubt. Eingebettet werden diese in einen Erweiterungsheader, entweder den „Hop-by-Hop Options“ oder den „Destination Options“ Header, je nachdem ob die Optionen bei jedem Knoten auf dem Weg oder nur am Ziel Verwendung finden sollen. Ein erwähnenswertes Merkmal dieser Optionenheader ist, dass sie ein Feld enthalten, welches angibt, was mit dem IP Paket geschehen soll, wenn ein Knoten die Option nicht erkennt. Mögliche Aktionen sind dabei die Option einfach zu ignorieren oder das Paket zu verwerfen, beides ohne oder mit Fehlermeldung (ICMP „Parameter Problem“ Nachricht) an den Absender.

### 11.3.2 Fragmentierung

IPv6 hat etliche fundamentale Änderungen im Bereich der Fragmentierung gegenüber seinem Vorgänger erfahren. Dies fängt schon bei der Grösse der minimalen „Maximum Transmission Unit“ („MTU“) des darunter liegenden physischen Netzwerks an. Die Spezifikation von IPv4 schreibt eine minimale MTU von 576 Bytes vor, die alle Knoten verarbeiten können müssen. IPv6 hat diese Untergrenze erhöht, neu muss eine MTU von mindestens 1280 Bytes unterstützt werden. Da es in beiden Fällen natürlich möglich (und auch wahrscheinlich) ist, dass das darunter liegende physische Netzwerk höhere MTUs

verträgt, gibt es sowohl für IPv4 als auch IPv6 das sogenannte „Path MTU Discovery“ Verfahren. Die einfache Idee hinter diesem Verfahren ist, dass durch Austesten verschiedener MTU Grössen die maximal mögliche MTU einer Verbindung ermittelt werden kann. Knoten auf dem Weg, die ein Paket bestimmter Grösse nicht weiterleiten können, melden dies mit einer ICMP Nachricht zurück an den Absender.

Path MTU Discovery spielt in IPv6 eine wichtigere Rolle als in IPv4. Während es in IPv4 jedem Knoten erlaubt ist ein Paket zu fragmentieren, darf dies in IPv6 nur noch der ursprüngliche Absender. Dies hat sowohl Vor- als auch Nachteile. Mit dem Verfahren in IPv4 ist es möglich, dass Pakete mehrstufig fragmentiert werden. Bereits vom Absender fragmentierte Pakete werden unter Umständen von Routern auf dem Weg zum Ziel noch diverse weitere Male fragmentiert. Dies ist ein Problem, da die Router zwar fragmentieren, nicht aber zusammensetzen, wenn das nächste Netzsegment wieder eine höhere MTU erlauben würde. IPv6 verhindert diese mehrstufige Fragmentierung und steigert auch die Effizienz, da Router sich nicht mehr um Fragmentierung kümmern müssen. Ein Nachteil der neuen Lösung entsteht im Fall von wechselnden Übertragungswegen verschiedener Pakete einer gegebenen Kommunikationsverbindung, weil die unterschiedlichen Wege unterschiedliche MTUs besitzen können. Da nicht mehr „ad hoc“ auf dem Weg fragmentiert werden kann, muss der Absender bei ICMP „Package too big“ Fehlermeldungen erneut Path MTU Discovery ausführen.

Auch der Fragmentierungsprozess selbst sieht unterschiedlich aus. Bei IPv4 wird der Header des ursprünglichen IP Pakets transformiert und mit dem ersten Fragment verwendet, die übrigen Fragmente erhalten neue Header. Die für die Fragmentierung relevanten Daten werden dabei direkt im IPv4 Header gespeichert, der somit auch Platz verschwendet, wenn gar keine Fragmentierung auftritt. IPv6 löst das Thema Fragmentierung über die Erweiterungsheader, ein nicht fragmentiertes Paket verschwendet somit keinen unnötigen Platz. Der Main Header des ursprünglichen Pakets wird dabei für jedes Fragment weiter verwendet und ein Fragmentheader mit den relevanten Feldern eingefügt. Die Behandlung der ursprünglichen Erweiterungsheader teilt sich in zwei Elemente. Erweiterungsheader die nur das Ziel betreffen (Authentication, Encapsulating Security Payload sowie final Destination Options Header) werden dem ersten Fragment mitgegeben bzw. auf die verschiedenen Fragmente aufgeteilt. Erweiterungsheader die für den Weg relevant sind (Routing, Hop-by-Hop Options sowie „en route“ Destination Options Header) werden in jedes Fragment eingefügt.

### 11.3.3 Adressierung

Der Abschnitt 11.2.2 hat die wesentlich Merkmale von Adressierung in IPv6 bereits erläutert. Die IPv4 Situation dürfte hinlänglich bekannt sein, wir beschränken uns in diesem Abschnitt daher auf folgende Anmerkungen:

Neben dem enorm vergrösserten Adressraum von 32 Bit auf 128 Bit, ist ein erwähnenswerter Unterschied die Semantik einer IP Adresse. Unter IPv4 ist eine Adresse semantisch grösstenteils wertlos, unter IPv6 hingegen lassen sich dank des hierarchischen Aufbaus (vgl. Abbildung 11.2) relativ zuverlässige Rückschlüsse auf die Lage eines Knotens anhand seiner Adresse ziehen. Insbesondere sind nun Adressen nicht mehr willkürlich den

Interfaces zugeordnet, sondern lassen sich aus gegebenen Informationen erstellen. Der 64 bit Interface Identifier Teil der Adresse wird beispielsweise sofern möglich aus einer existierenden Interface ID abgeleitet (im Fall von Ethernet der 48 bit MAC Adresse). Dies erleichtert die Konfiguration und Übersicht über ein Netz natürlich enorm. Einziger Nachteil dieser Lösung ist, dass mit wechselndem Interface auch ein Adresswechsel einhergeht.

Auch ein paar Worte zu „speziellen“ Adressen sind angebracht. `IPv4` reserviert für Loopback Funktionalität ein gesamtes Klasse-A Netz (127.0.0.0/8). Da mittlerweile erkannt wurde, dass dies wenig Sinn macht, gibt es in `IPv6` nur noch eine einzige Loopback Adresse (::1). Eine weitere Form von „speziellen“ aber dennoch sehr häufig genutzten `IPv4` Adressen sind die privaten Adressbereiche (10.0.0.0/8, 172.16.0.0/12 sowie 192.168.0.0/16), welche nicht ins Internet geroutet werden und somit per NAT umgesetzt werden müssen. Die NAT Situation fällt in `IPv6` weg, aber es gibt dennoch Adressbereiche, die nicht unbeschränkt geroutet werden. Dies sind zum einen die Site-Local Adressen (FEC::/10), welche nicht aus einer Site hinaus geroutet werden, und zum anderen die Link-Local Adressen (FE8::/10), welche das lokale physische Netzwerk nicht verlassen.

Abschliessend noch zu den Multicast Adressen: Dieser Adresstyp war zwar auch schon in `IPv4` bekannt, wurde aber nicht gross genutzt und lange Zeit auch von Hardware nur schlecht unterstützt. Während Multicast für `IPv4` optional war, ist es für `IPv6` nun zwingender Bestandteil. So wurde auch auf die gesonderten Broadcast Adressen (welche eine Adressierung aller Knoten eines Netzes über eine einzige Adresse ermöglichen) von `IPv4` verzichtet und dieses Konzept statt dessen mit Multicast realisiert. `IPv4` Broadcasts waren auf ein Link-Local Netz beschränkt, und wurden über eine spezielle Adresse innerhalb des Adressbereichs des Netzes angesprochen (alle Bits des Host Teils auf „1“ gesetzt). `IPv6` verwendet nun unabhängige Adressen dafür, und alle Knoten eines Teilnetzes lassen sich auch über Link-Local Abgrenzungen hinweg ansprechen. Dies geschieht über die Multicast Adressen FF0x::1, wobei das „x“ das Ausmass der gewünschten Empfänger angibt (1 für Node-Local, 2 für Link-Local, 5 für Site-Local und 8 für Organization-Local). Durch diese möglichen Abstufungen ist das neue System bedeutend flexibler als das alte Broadcast System von `IPv4`, und auch einfacher da statt einer vom spezifischen Netz abhängigen Broadcast Adresse eine wohl definierte, feste Multicast Adresse für den selben Zweck verwendet werden kann.

### 11.3.4 Neighbor Discovery Protokoll

Mit der Spezifikation von `IPv6` gab es natürlich auch grundlegende Änderungen in Protokollen die IP unterstützend zur Seite stehen. Es wurden sowohl bestehende Protokolle angepasst (z.B. ICMP) und erweitert als auch ein vollkommen neues definiert. Auf dieses neue „Neighbor Discovery“, kurz „ND“ Protokoll, welches gleich mehrere Funktionen erfüllt für die in `IPv4` andere, einzelne Protokolle zuständig waren, möchten wir noch näher eingehen. Der Begriff Nachbar bezieht sich hierbei auf Knoten die direkt miteinander kommunizieren können, sich also im gleichen physischen Netzwerk befinden. Zur Durchführung seiner Funktionen verwendet ND ICMPv6 Nachrichten. Seine Aufgaben lassen sich grob in drei Kategorien gliedern, Host-Router Funktionen, Host-Host Funktionen sowie Umleitungsfunktionen.

In die erste Kategorie fallen grundlegende Funktionen. Bevor ein Host mit dem Internet kommunizieren kann, muss er wissen, welcher Router seine Pakete annimmt und weiter leitet, er muss grundlegende Information über den Router und das eigene Netzwerk in Erfahrung bringen. ND bietet in diesem Gebiet Möglichkeiten, einen Router überhaupt zu finden und von diesem die notwendigen Parameter zu erhalten. Es ersetzt damit im wesentlich die ICMPv4 Router Discovery. Ebenfalls in dieses Gebiet fällt die schon früher besprochene Autokonfiguration, welche auch mit ND abgewickelt wird.

Die zweite Kategorie umfasst Funktionen zur direkten Host zu Host Kommunikation. Ein Host muss entscheiden können, ob ein Paket direkt oder indirekt zugestellt werden soll, und muss im direkten Fall die physische Adresse des Ziels ermitteln können. ND ermöglicht beide diese Funktionen und ersetzt damit sowohl die Prüfung mit der Subnetzmaske aus `IPv4` als auch das ARP Protokoll. Auch zu dieser Gruppe zählen Funktionen zur Bestimmung, ob ein Nachbar noch erreicht werden kann oder nicht, und die bereits früher erwähnte Duplicate Address Detection (DAD).

Als letzte Kategorie verbleibt die Umleitungsfunktion. Hierbei geht es darum, dass Router Hosts über bessere Routen unterrichten können und die Hosts danach zukünftig die Pakete direkt an den besser geeigneten Router leiten. Diese Entsprechung zum ICMPv4 Redirect ist neu ebenfalls in das ND Protokoll eingebettet.

### 11.3.5 Netzwerkkonfiguration

`IPv4` kennt im wesentlich zwei Arten der Adresskonfiguration, Adressen können entweder manuell statisch gesetzt werden oder dynamisch durch eine externe Quelle zugewiesen werden. Die manuelle Konfiguration eines grösseren Netzwerks ist höchst unpraktikabel, weshalb Methoden entwickelt wurden, die Vergabe von einer zentralen Stelle aus dynamisch zu erledigen. Dies ist die primäre Aufgabe des DHCP Protokolls. Beide diese `IPv4` Varianten gehören jedoch der „stateful“ Kategorie an, die Konfiguration muss irgendwo als Status gespeichert werden, sei es direkt auf dem Host im manuellen Fall oder indirekt auf einem Server im Fall von DHCP.

Für `IPv6` wurden Möglichkeiten gesucht, die Konfiguration noch besser zu automatisieren. Das Ergebnis ist eine vollkommen automatische Variante („stateless“ Autokonfiguration), die ohne jegliche externe Statusinformationen auskommt und bereits in früheren Abschnitten vorgestellt wurde. Neben dieser neuen Möglichkeit zur Adresskonfiguration wurde die alte „stateful“ Autokonfiguration mit Hilfe von DHCP (genauer gesagt dem aktualisierten DCHPv6) ebenfalls beibehalten. Ein Knoten erhält von seinem zuständigen Router die Information, auf welche Weise er sich konfigurieren soll. Im Fall der „stateless“ Variante erhält er vom Router ein Netzwerk Präfix und kombiniert diesen mit seinem selbst generierten Interface Identifier Teil, im „stateful“ Fall erhält er die Adresse eines externen DHCP Servers, an den er sich für die Konfiguration wenden soll.

Der neue Autokonfigurationsmechanismus scheint auf den ersten, flüchtigen Blick DHCP überflüssig zu machen, das ist aber ein Trugschluss. Während zwar die grundlegende Konfiguration (IP Adressen, Default Router, etc.) durchaus vollständig von der neuen Autokonfiguration erledigt werden kann, erlaubt DHCP noch zusätzlich weitere interessante

Optionen an die Knoten zu übermitteln. So war beispielsweise die Zuweisung von DNS Servern die ein Knoten nutzen kann nicht von Anfang an Bestandteil der IPv6 Autokonfiguration, ein entsprechendes „DNS Discovery“ wurde erst nachträglich spezifiziert. Für die Übermittlung einer Vielzahl anderer Optionen führt der Weg allerdings nach wie vor zu DHCP, und natürlich auch wenn Adressen nur mit einer bestimmten, beschränkten Nutzungsdauer vergeben werden sollen (Leasing).

### 11.3.6 Zusammenfassung

In diesem Abschnitt haben wir die interessanten Unterschiede zu IPv4 dargestellt, und insbesondere die Themen Paketformat, Fragmentierung und Adressierung genauer beleuchtet. Ebenfalls sind wir kurz auf das Neighbor Discovery Protokoll und die neuen Konfigurationsmechanismen von IPv6 eingegangen und haben diese in den Vergleich zu entsprechenden IPv4 Mechanismen gestellt. Ausführlichere Vergleiche können bei Bedarf aus den verschiedenen Spezifikationen ermittelt werden, welche wir im folgenden noch kurz anführen.

Die detaillierten Spezifikationen von IPv4 sowie IPv6 finden sich in [34] und [9], die Adressarchitektur von IPv6 separat in [17]. ICMPv4 sowie ICMPv6 werden in [35] und [7] definiert. Das APR Protokoll sowie die ICMP Router Discovery sind in [36] und [8] beschrieben. Die Spezifikation des ND Protokolls steht in [30], und mehr Informationen zur „stateless“ Autokonfiguration gibt es unter [42].

## 11.4 Sicherheit (IPsec)

Als die ursprünglichen Internet Protokolle vor mehr als 25 Jahren definiert wurden, wurde dem Thema Sicherheit nicht sehr viel Bedeutung geschenkt. Die Anzahl Knoten im Netz war gering, die Gruppe der Teilnehmer überschaubar. In der heutigen Zeit sieht die Situation dagegen radikal anders aus. Vertrauliche Informationen werden regelmässig über das Internet übertragen, und potentielle Angreifer können überall auf dem Weg zwischen zwei oder mehreren Kommunikationspartnern sitzen.

Da das Internet Protokoll für solche Einsatzgebiete ungeeignet war, wurden verschiedene Einzellösungen entwickelt, die das Problem in höheren Protokollschichten in Angriff nahmen (z.B. SSL, das primär zur Absicherung von HTTP Transfers verwendet wird). Was aber nach wie vor fehlte, war wichtige Funktionen wie Authentifizierung und Verschlüsselung generell zur Verfügung zu stellen, unabhängig von den höheren Protokollen.

Mit der Entwicklung von IPv6 wurde die Gelegenheit genutzt, eine Sicherheitslösung auf IP-Ebene zu etablieren. Das Ergebnis war die „Sicherheitsarchitektur für das Internet Protokoll“, auch „IP Security“ oder kurz „IPsec“ genannt, welche sowohl für IPv6 als auch IPv4 zur Verfügung steht. In den folgenden Abschnitten werden wir die wichtigsten Elemente von IPsec kurz beleuchten.

### 11.4.1 Authentifizierung (AH)

Die erste Anforderung an gesicherte Kommunikation ist Authentifizierung und Integrität der übermittelten Nachrichten. Das „Authentication Header“, kurz „AH“ Protokoll nimmt sich dieser Problematik an. Es erlaubt dem Empfänger die Authentifizierung des Absenders, die Gewissheit, dass der Inhalt der Nachricht auf dem Übertragungsweg nicht verändert wurde und schützt weiterhin auch gegen sogenannte Replay Attacken, bei denen ein Angreifer abgefangene Pakete erneut einschleust.

#### Funktionsweise

Die Idee hinter dem AH Protokoll ist ziemlich einfach. Es wird das zu authentifizierende Paket genommen, mit einem Hashalgorithmus sowie dem gemeinsamem Schlüssel der beiden Kommunikationspartner ein Hashwert („Integrity Check Value“, „ICV“) berechnet, und dieser dann zusammen mit weiteren Feldern als neuer Header dem ursprünglichen Paket vorangestellt. Der Empfänger berechnet aus dem empfangenen Paket ebenfalls diesen Hashwert, und, sofern das Ergebnis mit dem im Header enthaltenen ICV übereinstimmt, wurde die Nachricht nicht verändert.

IPsec kann entweder im Transport- oder im Tunnelmodus arbeiten. Bei ersterem wird nur das Paket der darüber liegenden Transportschicht mit einbezogen, bei letzterem wird das gesamte IP Paket verwendet und zusammen mit dem Authentication Header in ein neues IP Paket eingepackt. Wo genau der AH platziert wird hängt vom verwendeten Modus sowie der IP Version ab:

Bei `IPv6` ist der AH einer der Erweiterungsheader, der im Transportmodus vor allen Zieloptionenheadern und einem allfälligen ESP Header steht, jedoch hinter allen sonstigen Erweiterungsheadern. Verkettet wird der AH über die in `IPv6` üblichen „Next Header“ Felder. Im Tunnelmodus wird der AH hinter den kapselnden, neuen IP Header und vor das gesamte ursprüngliche IP Paket gestellt.

Unter `IPv4` und Transportmodus wird der AH zwischen dem Paket der Transportschicht und dem IP Header platziert. Der AH verweist dabei wieder via „Next Header“ Feld auf das Transportschicht Feld, der ursprüngliche `IPv4` Header besitzt solch ein Feld allerdings nicht. Statt dessen wird dessen „Protocol“ Feld dazu verwendet anzuzeigen, dass als nächstes ein AH folgt. Im Tunnelmodus wird der AH wieder zwischen den neuen IP Header und das ursprüngliche IP Paket gestellt.

Detaillierte Informationen, der Headeraufbau und vieles mehr finden sich in [27].

### 11.4.2 Verschlüsselung (ESP)

Das bereits erwähnte AH Protokoll stellt die Integrität einer Nachricht sicher. Für gewisse Anwendungen reicht dies bereits aus, für andere ist jedoch auch eine geheime Übertragung der Nachricht erwünscht. Zu diesem Zweck kann das „Encapsulating Security Payload“, kurz „ESP“ Protokoll eingesetzt werden.

**Funktionsweise**

Im wesentlich nimmt ESP das geheim zu übertragende Paket und verschlüsselt dieses mit einem Verschlüsselungsalgorithmus unter Verwendung des geheimen Schlüssels der beiden Kommunikationspartner. Der Empfänger entschlüsselt dieses auf seiner Seite wieder entsprechend. Zusätzlich können die verschlüsselten Daten entweder mit einem eigenen, zu AH ähnlichen Verfahren authentifiziert werden, oder ESP kann in Kombination mit AH eingesetzt werden.

Während AH mit einem einzelnen Header auskommt, verteilt ESP seine Felder auf drei Teile: Einem ESP Header, einem ESP Trailer sowie einem optionalen „ESP Authentication Data“ Feld. Der Header mit Verwaltungsinformationen wird vor den verschlüsselten Daten platziert, der Trailer bestehend aus Füllbytes (um die zu verschlüsselnden Daten an allfälligen Blockgrössen auszurichten) sowie dem „Next Header“ Feld hinter den Daten. Anzumerken ist hierbei, dass der Trailer vor der Verschlüsselung an das ursprüngliche Paket angehängt wird und entsprechend auch mit verschlüsselt wird. Hinter den verschlüsselten Daten steht schliesslich optional das „Authentication Data“ Feld, welches ähnlich wie beim AH Protokoll einen Hashwert über den ESP Header und die verschlüsselte Nachricht inklusive Trailer enthalten kann.

Die Platzierung des ESP Headers geschieht analog zum Fall des AH Headers, welcher oben bereits besprochen wurde. Der ESP Trailer und das „Authentication Data“ Feld folgen im Transportmodus dem Paket der Transportschicht und im Tunnelmodus dem gekapselten IP Paket. Erwähnenswert ist noch, dass das „Next Header“ Feld aus dem ESP Trailer natürlich auf den ersten Header innerhalb des verschlüsselten Pakets und somit „rückwärts“ zeigt. Wird ESP zusammen mit AH eingesetzt, wird zuerst verschlüsselt und dann authentifiziert, entsprechend steht der AH Header vor dem ESP Header.

Für genaue Details, den Headeraufbau und viele weitere Informationen siehe [28].

### 11.4.3 Schlüsselaustausch (IKE)

Sowohl das AH als auch das ESP Protokoll benötigen zur Erfüllung ihrer Aufgaben zusätzliche Helfer. In erster Linie sind dies natürlich verschiedene Hash- und Verschlüsselungsalgorithmen, daneben aber auch Verfahren um die Zuordnung verschiedener Sicherheitsfunktionen zu wohldefinierten Kommunikationsverbindungen zu ermöglichen. Damit Authentifizierung und Verschlüsselung überhaupt funktionieren können, müssen die verwendeten Schlüssel natürlich auch beiden Seiten bekannt sein.

Eine Möglichkeit dies zu erreichen, wäre bei beiden Kommunikationspartnern manuell einen festen, vordefinierten Schlüssel einzurichten. Diese Lösung ist aber einerseits unflexibel und skaliert schlecht, da für jede Verbindung zwischen zwei verschiedenen Knoten ein unterschiedlicher Schlüssel gewählt werden sollte. Eine bessere Lösung ist eine automatische Generierung und Verteilung von Schlüsseln an die beteiligten Parteien. An diesem Punkt setzt das „Internet Key Exchange“, kurz „IKE“ Protokoll an.

**Funktionsweise**

IPsec gruppiert die für jede einzelne gesicherte Verbindung massgebenden Regeln, Optionen und weitere relevante Daten in sogenannten „Security Associations“, kurz „SAs“ und hält diese in einer Datenbank. Sowohl der AH als auch der ESP Header enthalten jeweils ein ID Feld, welches genau eine solche SA referenziert, womit jedes IPsec Paket eindeutig einer bestimmten gesicherten Verbindung zugeordnet werden kann. Das IKE Protokoll ist nicht nur für den Austausch von Schlüsseln zuständig, sondern allgemein für die gemeinsame Erstellung einer neuen SA zwischen zwei Kommunikationspartnern. Das Protokoll teilt sich in zwei Phasen:

In der ersten Phase handeln die beiden Kommunikationspartner aus, auf welche Weise sie weitere Informationen gesichert übertragen möchten. Es wird dabei eine neue SA erstellt, welche nur für die weiteren Verhandlungen verwendet wird. Typische Attribute, die hierbei bestimmt werden, sind die Wahl des zu verwendenden Verschlüsselungs- sowie Hashalgorithmus, die Methode zur Authentifizierung der Kommunikationspartner (z.B. über pre-shared keys) und selbstverständlich die zu verwendenden Schlüssel.

In einer zweiten Phase werden anschliessend die SAs für die zur weiteren sicheren Kommunikation zu benutzenden Protokolle ausgehandelt. Falls sowohl AH als auch ESP verwendet werden sollen, wird für jedes der beiden Protokolle eine eigene SA erstellt. Vorteil der Aufteilung in zwei Phasen ist hier, dass gleich mehrere SAs in der zweiten Stufe ausgehandelt werden können ohne dass der grössere Aufwand der ersten Phase mehrfach ausgeführt werden muss.

Weiterführende Informationen zum Protokoll unter [25].

### 11.4.4 Zusammenfassung

In den vorhergegangenen Abschnitten haben wir die wichtigsten Elemente von IPsec kurz vorgestellt. Dies waren das „Authentication Header“ Protokoll welches Authentifizierung und Integrität sicherstellt, das „Encapsulating Security Payload“ Protokoll welches Verschlüsselung erlaubt, sowie das „Internet Key Exchange“ Protokoll zur automatischen Aushandlung von Security Associations. Dabei konnte hier nur ein recht oberflächlicher Überblick gegeben werden. Für detailliertere Informationen zu den einzelnen Bestandteilen wurde bereits auf die relevanten RFCs verwiesen, ein Gesamtüberblick über die IPsec Architektur findet sich in [26].

IPsec lässt sich auf verschiedene Arten implementieren. Die eleganteste Lösung ist es IPsec direkt in den IP Stack zu integrieren. Dies wird für `IPv6` die Regel sein, für `IPv4` allerdings nur die Ausnahme. Denn die Anpassung der Vielzahl bestehender `IPv4` Stacks ist nicht wirklich praktikabel. Zum nachträglichen Aufrüsten mit IPsec Funktionalität bietet sich dafür der sogenannte „Bump in the Stack“ Ansatz an, IPsec wird hierbei direkt unterhalb des bestehenden IP Stacks zwischen Internet- und Datensicherungsschicht positioniert.

## 11.5 Offene technische und Sicherheitsfragen

Während bei der Entwicklung von IPv6 die Sicherheit in Bezug auf die Kommunikation zwischen Endknoten einbezogen und IPsec entwickelt wurde, blieben andere Aspekte unberücksichtigt oder sind erst in den Jahren danach relevant geworden. Es gibt nach wie vor eine Reihe offener Fragen sowohl zum Thema Sicherheit als auch allgemeiner technischer Natur. In diesem Abschnitt wollen wir zwei Bespiele genauer anschauen.

Als erstes werden wir Sicherheitsprobleme im Zusammenhang mit dem Neighbor Discovery Protokoll diskutieren, da diese im Hinblick auf die immer grössere Verbreitung von Wireless Netzen in den letzten Jahren an Relevanz gewonnen haben. Als zweites zeigen wir technische Schwierigkeiten und Sicherheitsprobleme im Bereich Multihoming auf.

### 11.5.1 Neighbor Discovery Sicherheit

Während die Gefahr in Bezug auf Sicherheit bei der Kommunikation zwischen Knoten verschiedener Netze schon länger als mögliche Gefahr erkannt wurde, ging man bei der Entwicklung der IPv6 Protokollfamilie, insbesondere des ND Protokolls davon aus, dass das lokale physische Netz sicher wäre und nur aus vertrauenswürdigen Knoten bestünde. Mit der zunehmenden Mobilität der letzten Jahre sowie der Verbreitung von Wireless Technologien kann dies aber mittlerweile nicht mehr als gegeben betrachtet werden.

Ein böswilliger Knoten hat die Möglichkeit praktisch mit allen von ND zur Verfügung gestellten Funktionen Missbrauch zu treiben. Ein Modell zur Klassifizierung sowie tatsächliche Bedrohungen wurden bereits in [31] veröffentlicht. Arkko et al. haben dies in [1] erneut aufgegriffen, und stellen mögliche Lösungsvorschläge vor. Das Problem rührt in erster Linie daher, dass Nachrichten und Header Felder von einem böswilligen Knoten beliebig gefälscht werden können und insbesondere keine Überprüfung der aufgeführten Absenderadresse stattfindet.

Mögliche Angriffe teilen sich in reine „Denial of Service“ („DoS“) sowie Umleitungsattacken auf. Alleine für reine DoS Angriffe stehen einem böswilligen Knoten bereits diverse Optionen offen. So kann er unter anderem beispielsweise einfach auf sämtliche DAD Anfragen antworten und somit verhindern, dass ein legitimer Knoten eine gültige Adresse erhält, oder sich als Router ausgeben und anderen Knoten ungültige Parameter für die Autokonfiguration geben. Umleitungsattacken bei denen sich der böswillige Knoten auch wieder als Router ausgibt und gefälschte „Redirect“ Nachrichten verschickt, können sowohl für weitere DoS Varianten als auch für „Man-in-the-Middle“ Attacken verwendet werden, bei welchen der böswillige Knoten Kommunikation abhören und manipulieren kann.

Es besteht zwar die Möglichkeit ND Nachrichten mit IPsec AH zu authentifizieren und auch deren Integrität sicherzustellen, aber das reicht leider nicht aus. Um bereits die grundlegenden Funktionen wie Autokonfiguration etc. zu schützen müssten die notwendigen Schlüssel manuell in den Knoten konfiguriert werden. Dies wird aufgrund schlechter Skalierbarkeit in Netzen mit mehr als einer handvoll Knoten sehr schnell unmöglich, und die einzige definierte Automatisierungsvariante (IKE) benötigt bestehende gültige IP Adressen auf beiden Seiten, die noch nicht vorhanden sind.

Arkko et al. schlagen mit ihren Konzepten von „Cryptographically Generated Addresses“ („CGA“) sowie „Address Based Keys“ („ABK) zwei Verfahren vor um der geschilderten Problematik zu begegnen.

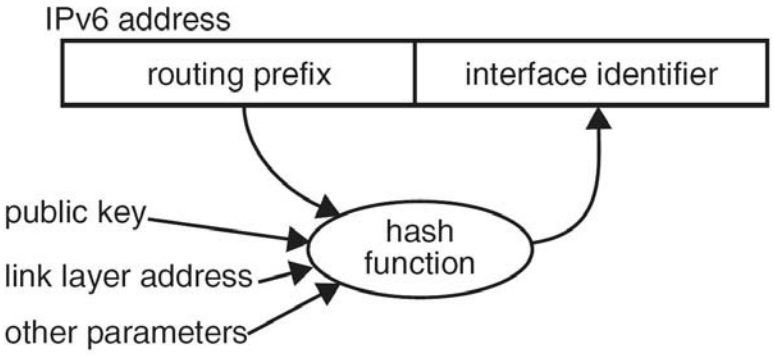



Abbildung 11.4: Generierung einer CGA Adresse

Die Idee hinter CGA ist, den Interface Identifier Teil einer `IPv6` Adresse durch einen kryptographischen Hashwert zu ersetzen (vgl. Abbildung 11.4). Als Eingabe für die Hashfunktion dienen dabei ein öffentlicher Schlüssel des Knotens, seine Adresse der Datensicherungsschicht sowie weitere Parameter. Die Authentizität und Integrität einer Nachricht kann nun vom Empfänger überprüft werden, wenn die Nachricht mit dem privaten Schlüssel des Absenders signiert wurde. Der öffentliche Schlüssel sowie andere Parameter die als Eingabe für die Hashfunktion gedient haben müssen natürlich ebenfalls mitgeschickt werden, sonst kann der Empfänger den Hash nicht nachvollziehen und mit der verwendeten Absenderadresse vergleichen.

CGA reicht raus, um die Host-Host Funktionen von ND abzusichern, ebenso wie die Umleitungsfunktionen (dazu vergleicht ein Empfänger zusätzlich noch ob die Absenderadresse mit seinem zuständigen Router übereinstimmt). Ein böswilliger Knoten kann aber unter seiner eigenen, überprüfbaren Adresse Nachrichten mit böswilligem Inhalt versenden und damit immer noch Angriffe auf die Host-Router Funktionen ausführen indem er sich einfach als ein weiterer Router ausgibt.

Hier kommt das zweite Verfahren ABK ins Spiel. Bei ABK übernehmen die Adressen selbst die Funktion des öffentlichen Schlüssels. Es wird eine externe, vertrauenswürdige Instanz benötigt, die aus der Adresse eines Knotens einen privaten Schlüssel erzeugen kann und diesen auf einem sicheren Weg zurück an den Knoten übermittelt. Das Verfahren lässt sich analog zum Einsatz auf dem Interface Identifier Teil auch auf Netzwerkpräfixe anwenden. Jeder legitime Router erhält dabei einen privaten Schlüssel für jedes zu ihm gehörende Netzwerkpräfix, und signiert Nachrichten die ein bestimmtes Netzwerkpräfix betreffen mit dem zugehörigen Schlüssel. Da ein Empfänger davon ausgehen kann, dass nur ein legitimer Router von der externen, vertrauenswürdigen Instanz entsprechende private Schlüssel erhalten hat, kann er den Nachrichten vertrauen.

### 11.5.2 Multihoming

Unter „Multihoming“ versteht man die Situation, dass ein Knoten auf mehreren Interfaces Adressen aus verschiedenen Netzen besitzt und somit in all diesen Netzen beheimatet ist. Grund für Multihoming ist häufig, dass man einen Knoten redundant an das Internet anbinden möchte und er auch bei Ausfall einer Leitung noch erreichbar bleiben soll.

Während Multihoming für neu eingehende Verbindungen relativ einfach zu realisieren ist, gibt es ein grosses Problem mit bereits bestehenden Verbindungen, wenn die aktuelle Übertragungsstrecke zusammenbricht. Die Protokolle der Transportschicht verwenden die IP Adresse zur Identifikation des Endpunktes einer Verbindung, die somit dann auch nicht inmitten einer Übertragung gewechselt werden darf. In [20] werden mögliche Verfahren verglichen, die sich der Multihoming Problematik annehmen.

Grundsätzlich muss der Transportschicht eine konstante Adresse präsentiert werden, während für das tatsächliche Routing auf IP Ebene dann jeweils eine der gültigen Adressen zur Verwendung kommt. Es wird also ein Verfahren benötigt, das logische Adressen auf physische abbildet und natürlich auf beiden Seiten der Kommunikationsverbindung vorhanden sein muss. Dieser Ansatz ist zwar elegant, öffnet aber auch potentielle Sicherheitslücken, die in [32] analysiert wurden. Die grösste Gefahr besteht darin, dass Pakete an nicht beabsichtigte Zieldestinationen umgeleitet werden.

Eine mögliche Lösung stellen Bagnulo et al. in [2] vor. Sie verwendet die bekannten Präfixe der an den multihomed Knoten angeschlossenen Netze, die ja die erste Hälfte seiner `IPv6` Adressen ausmachen. Die Idee ist nun, aus sämtlichen Netzwerkpräfixen des betroffenen Knotens plus einer zufällig generierten Bitfolge einen kryptographischen Hashwert zu berechnen und diesen dann in den Interface Identifier Teil der Adresse des Knotens einfliessen zu lassen.

Wird einem potentiellen Kommunikationspartner eine neue Adresse für den Knoten genannt, erhält er sowohl die Netzwerkpräfixe als auch die zufällig generierte Bitfolge mitgeteilt. Auf Basis dieser Information kann der Empfänger mit einer einfachen Hashwert Berechnung testen, ob die Mitteilung tatsächlich von einem legitimen Absender stammt, da der Interface Identifier Teil der Absenderadresse ja mit dem Hashwert übereinstimmen muss (und das Netzwerkpräfix natürlich mit einem der übermittelten). Damit ein Angreifer die Kommunikation auf sein eigenes Netz umleiten kann, müsste er eine passende Zufallsfolge finden welche in Kombination mit den Präfixen einen korrekten Hashwert ergibt. Dafür sind jedoch im Mittel 2 hoch 61 Versuche notwendig, was für aktuelle Rechenkapazitäten eine ausreichende Hürde darstellt.

### 11.5.3 Zusammenfassung

Dieser Abschnitt hat in Form von den zwei Bespielen Neighbor Discovery und Multihoming dargelegt, dass es für `IPv6` noch ungelöste technische und Sicherheitsfragen gibt. Die tatsächliche Anzahl geht natürlich weit über das Beschriebene hinaus, es gibt somit für die kommenden Jahre mehr als genug Arbeit für Forschung und Wissenschaft auf diesem Gebiet.

Beide vorgestellten Lösungen arbeiten damit, den Interface Identifier Teil der IPv6 Adresse durch einen kryptographischen Hashwert zu ersetzen. Sollten sich solche Verfahren etablieren, wird der potentielle Semantikgewinn der IPv6 Adressen gegenüber ihren Vorgängern leider wieder reduziert. Denn der Vorteil von Hashfunktionen ist ja genau, dass aus dem Hashwert nicht auf die ursprüngliche Eingabe (und somit auf die zugrunde liegende Datensicherungsschicht Adresse) zurück geschlossen werden kann.

## 11.6 Machbarkeit der Umstellung auf IPv6

In diesem Abschnitt untersuchen wir, inwiefern im Hinblick auf die Bereiche Software und Netzwerkdienstleistungen die technischen Voraussetzungen für die Umstellung auf IPv6 erfüllt sind, und wir untersuchen weiterhin, ob der nötige Enthusiasmus eher zunimmt oder abnimmt. Die Betrachtung jedes dieser Aspekte spricht dafür, dass ein rasches Fortschreiten der Umstellung auf IPv6 unwahrscheinlich ist; die Gründe dafür werden jedoch erst im folgenden Abschnitt 11.7 über die ökonomischen Aspekte klar.

### 11.6.1 Software

Während noch anfangs 2000 Guardini, Fasano und Girardi [15] erhebliche Mängel im Bereich der Unterstützung von IPv6 durch grundlegende Applikations-Software beklagten, sind diese Probleme mindestens für GNU/Linux und *BSD inzwischen gelöst, siehe [4]. Auch Microsoft bietet IPv6-Unterstützung an, siehe [29].

Anders sieht es mit der IPv6-Unterstützung durch Anwendungsprogramme aus, die mit dem Betriebssystem gebündelt, sondern separat davon kommerziell vertrieben werden. Gallaher [13] schätzt aufgrund einer Umfrage unter Software-Herstellern, dass erst im Jahr 2010 50% dieser Software-Firmen in ihren Produkten IPv6 Unterstützung anbieten werden.

### 11.6.2 IPv6 Anbieter in der Schweiz

Nach Angaben der „Swiss IPv6 Task Force“[40] kann man in der Schweiz von zwei kommerziellen ISPs IPv6 Internet-Anbindungen bekommen, nämlich von Cyberlink und von der Dolphins Network Systems AG. Cyberlink AG hat auf Anfrage bestätigt, dass tatsächlich native IPv6 ADSL-Anschlüsse angeboten werden, und zwar zu demselben Preis wie die entsprechenden IPv4-Angebote. Die Angabe über die “Dolphins Network Systems AG” ist aber veraltet, dieser Provider tritt nicht mehr am Markt auf.

Ausserdem bietet SWITCH (ein nichtkommerzieller, auf akademische Institutionen und Forschungseinrichtungen spezialisierter ISP) neben IPv4 auch IPv6 Internet-Anbindungen an.

### 11.6.3 Internationaler Rückgang des Enthusiasmus für IPv6

Die im Jahr 2002 mit viel Enthusiasmus gegründete „Swiss IPv6 Task Force“ ist momentan mindestens nach aussen hin total inaktiv: Es sind keine Veranstaltungen geplant, Anfragen betreffend Mitgliedschaft werden nicht beantwortet, und die Kontaktinformationen auf der Website sind nicht mehr aktuell.

Auch international gab es um das Jahr 2002 grossen Enthusiasmus für IPv6, der seitdem stark abgenommen hat. Beispielsweise heisst es in einer Pressemitteilung der EU Kommission vom 21. Februar 2002 [11]: „‚IPv6 ist die technische Voraussetzung für das Zusammenwachsen von Internet und Mobilkommunikation, also einen Bereich, in dem Europa weltweit führend ist,‘ erläutert Erkki Liikanen, das für Unternehmen und die Informationsgesellschaft verantwortliche Kommissionsmitglied. ‚Die Bedeutung von IPv6 für die Wettbewerbsfähigkeit Europas kann gar nicht überschätzt werden. Um IPv6 zu verwirklichen, muss Europa seiner erstklassigen Forschung nun ein entsprechendes politisches Engagement zur Seite stellen.‘“

Eine solche politische Bereitschaft zu ernsthaftem Engagement ist heute nicht mehr in vergleichbarem Mass vorhanden. Bei vergleichbaren Gelegenheiten hat die EU Kommission in ihren offiziellen Mitteilungen die Umstellung auf IPv6 in den letzten Jahren nicht mehr erwähnt.

Auch auf der von der „Working Group on Internet Governance“ (WGIG) erstellten Liste von „Internet Governance“ Themen kommt IPv6 nicht vor (siehe z.B. [10]), obwohl das Thema eindeutig auf diese Liste gehört. Aufgrund der Zusammensetzung und der Geschichte der WGIG ist dies ein starker Beleg dafür, dass die Problematik der Umstellung auf IPv6 zur Zeit von keiner der drei grossen Stakeholder-Gruppen „Regierungen“, „Industrie“ und „Zivilgesellschft“ als ein wichtiges, aktuelles Thema wahrgenommen wird: Die UNO hat unter dem Namen „World Summit on Information Society“ (WSIS, Weltgipfel zur Informationsgesellschaft) zwei grosse internationale Konferenzen organisiert, die erste 2003 in Genf und die zweite 2005 in Tunis. Beim ersten Gipfel in Genf gab es einen grossen Streit, im wesentlichen zwischen Vertretern der US-Regierung, die die politische Aufsicht über die Tätigkeit der für das Internet wichtigen US-Organisation „Internet Corporation for Assigned Names und Numbers“ (ICANN) wahrnimmt, und der EU, die den verständlichen Wunsch nach einer Internationalisierung dieser Aufsichtsfunktion mit der Forderung verband, die Aufgaben der ICANN an die International Telefone Union (ITU) zu übertragen. Diese Forderung ist nicht sehr sinnvoll, weil die ITU weder Interesse daran hat, die Aufgaben der ICANN zu übernehmen, noch über entsprechende Kompetenzen verfügt. Aus der Sicht eines Machtpokers zwischen USA und EU ist die Forderung jedoch verständlich, denn in der ITU gilt das Prinzip „ein Land, eine Stimme“, wodurch die EU-Länder dort zusammen (insbesondere im Vergleich zu den USA, die über nur eine Stimme verfügen) erheblichen Einfluss haben. Weil am Gipfel in Genf keine Einigung möglich war, wurde eine Arbeitsgruppe eingesetzt, die „Working Group on Internet Governance“ (WGIG), die aus vierzig Vertretern von Regierungen, Industrie und Zivilbevölkerung bestand, wobei jede dieser drei Stakeholder-Gruppen ungefähr gleich stark vertreten war. Diese Arbeitsgruppe hat schnell erkannt, dass eine Fixierung auf die ursprüngliche Streitfrage nichts bringt. Insbesondere hat sich die Arbeitsgruppe nicht nur für Fragen im Zuständigkeitsbereich von ICANN (wie etwa Domain-Namen und Internet

Protokoll Nummern) interessiert, sondern allgemeiner die verschiedenen Prozesse analysiert, durch die Fragen entschieden werden, die im Zusammenhang des Internets von öffentlichen Interesse sind („Internet Governance“). In ihrem einstimmig verabschiedeten Bericht hat diese Arbeitsgruppe unter anderem die Einrichtung des „Internet Governance Forum“ (IGF) vorgeschlagen, bei dem es sich nicht um ein Entscheidungsgremium, sondern um ein Forum zum offenen Gedankenaustausch zwischen Vertretern der verschiedenen Stakeholder-Gruppen handeln soll. Dieser Vorschlag, der dann in Tunis angenommen wurde, ist sicher auch Ausdruck der von den Arbeitsgruppen-Mitgliedern als positiv erlebten Erfahrung des Dialogs mit Vertretern von anderen Stakeholder-Gruppen. (Für eine ausführlichere Darstellung der Hintergründe und Arbeit der WGIG siehe [14] und [10].)

Im Februar 2006 hat die UNO in Genf eine Konsultation organisiert, bei der es unter anderem um die Frage der nach den möglichen Themen für das IGF ging. Auch bei dieser Gelegenheit hat niemand `IPv6` als Thema vorgeschlagen (siehe [23]), obwohl jede Interessengruppe mit einem entsprechenden Anliegen die Möglichkeit gehabt hätte, sich so zu äussern. Das Fehlen von `IPv6` auf der Themenliste der WGIG ist folglich nicht ein spezifisches Phänomen, das nur die WGIG-Arbeitsgruppe betrifft, sondern Ausdruck dessen, dass die Umstellung auf `IPv6` im allgemeinen nicht mehr als ein wichtiges Diskussionsthema wahrgenommen wird. (Dabei waren durchaus Personen an diesen Konsultationen anwesend, die sich mit der Umstellung auf `IPv6` befassen. Dass dennoch `IPv6` nicht als Thema vorgeschlagen wurde, muss nicht notwendigerweise an geringem Enthusiasmus für diese Thema liegen. Eine andere denkbare Erklärung besteht darin, dass diejenigen, die sich unabhängig von ökonomischen Anreizen mit diesem Thema befassen, das unten in Abschnitt 11.7 besprochene weitgehende Fehlen solcher Anreize nicht als erhebliches Problem wahrnehmen.

## 11.7 Ökonomische Aspekte der Umstellung auf `IPv6`

Die technische Infrastruktur des Internets von `IPv4` auf `IPv6` umzustellen verursacht in verschiedenen Bereichen erhebliche Kosten:

- Software-Anpassungen
- Anpassung der grundlegenden Netzwerkinfrastruktur der ISPs (dazu gehört das Einrichten von Gateways zwischen `IPv4`- und `IPv6`-Netzwerken, oder weitergehende Dual-Stack-Fähigkeit).
- Umstellung von Firmen-Netzwerken
- Umstellung der persönlichen LANs von Privatnutzern
- Umstellung von Webservern und Betrieb von Proxy-Servern
- Umstellung von Mailservern und Sicherstellung der Email-Erreichbarkeit sowohl via `IPv4` als auch via `IPv6` während der Übergangsphase

Ob die Umstellung von IPv4 auf IPv6 tatsächlich geschieht, das hängt davon ab, dass auf allen Ebenen die entsprechenden Investitionen tatsächlich getätigt werden. Es gibt verschiedene mögliche Motivationen für eine solche Investitionsentscheidung:

1. Die Entscheidung ist am einfachsten, falls absehbar ist, dass die Investition zu einem konkreten Nutzen führen wird, der die Kosten weit übersteigt, und falls klar ist, dass der Nutzen bei einer schnellen Umsetzung der Entscheidung am grössten sein wird. Wenn die Situation so klar ist, wird die Investition in jeder gutgeführten Firma rasch entschieden und umgesetzt werden.

2. Viel schwieriger ist die Entscheidung, wenn man zwar hofft, dass sich mit einer schnellen Investitionsentscheidung ein grosser Nutzen erzielen lässt, aber die Zusammenhänge nicht so klar absehbar sind. In diesem Fall hängt die Entscheidung stark von der Risikobereitschaft des Unternehmers ab.

3. Schliesslich kann die Entscheidung durch ökonomischen Zwang erfolgen, weil die Alternativen vom Markt verschwinden.

Andererseits gibt es einen starken ökonomischen Anreiz, bei IPv4 zu bleiben, solange wie die grosse Mehrheit der Internet-Benützer IPv4 verwendet. Beispielsweise ist es für eine Firma mit keinem absehbaren ökonomischen Nutzen, wohl aber mit Risiken verbunden, schneller als andere das Firmennetzwerk auf IPv6 umzustellen: Einerseits werden solche Firmen, die frühzeitig auf IPv6 setzen, sich Kinderkrankheiten in der Unterstützung von verschiedenen Anwendungsprogrammen für IPv6 herumärgern müssen. Andererseit müssen diese Firmen das Risiko tragen, dass sich IPv6 vielleicht doch nicht wie erwartet durchsetzt. Diese Probleme lassen sich umgehen, in dem man so lange wie möglich weiterhin IPv4 benützt. Wer damit rechnet, dass sich die grosse Mehrheit der Internet-Nutzer so verhalten könnte, kann nicht mit dem Erfolg der Umstellung auf IPv6 rechnen, was zu umso vorsichtigerem Verhalten im Hinblick auf eine eventuelle eigene Umstellung auf IPv6 führen wird.

Bernstein [3] hat darauf hingewiesen, dass dieses Problem dadurch massiv verstärkt wird, dass die IETF dieser Problematik zu wenig Beachtung geschenkt hat:

### 11.7.1 Die fehlende Kompatibilitätsforderung

Nach Bernstein [3] gibt es bei der von der IETF vorgeschlagenen Vorgehensweise zur Umstellung auf IPv6 nicht nur kaum ökonomische Anreize für eine rasche Umstellung auf IPv6, sondern es gibt starke negative Anreize gegen eine Umstellung auf IPv6, die daraus resultieren, dass die IETF bisher keine klaren Regeln aufgestellt hat, die IPv4-basierte Internet-Server (etwa ab einem bestimmten Datum) zur Kompatibilität mit IPv6-basierten Clients verpflichten würde.

Eine solche Kompatibilitäts-Verpflichtung könnte, basierend auf der in RFC 3056 [6] 6to4-Methode zum Einpacken von IPv6-Datenpaketen in IPv4-Paketen, etwa wie folgt formuliert werden:

> Ab Datum-XXXX muss jeder Webserver, der auf IPv4 TCP-Port 80 Verbindungen entgegennimmt auch 6to4-Pakete akzeptieren und beantworten, die eine IPv6 TCP-Verbindung zu Port 80 betreffen. Die 6to4 IPv6 TCP-Verbindung ist als völlig äquivalent zu Verbindungen zu IPv4 TCP-Port 80 zu behandeln. Analog muss ab Datum-XXXX jeder Mailserver Port 25-Verbindungen nicht nur in Form von IPv4 TCP akzeptieren, sondern auch als 6to4 IPv6 TCP-Verbindung.

Solange die IETF keine solche Kompatibilitäts-Verpflichtung proklamiert, ist davon auszugehen, dass es im Internet akzeptiert wird, wenn man sich nicht um die Umstellung auf IPv6 kümmert.

Die Konsequenz davon ist, dass alle, die IPv6 einführen wollen, zusätzlich dafür sorgen müssen, dass sie auch die Fähigkeit haben, mit IPv4 Internet-Hosts zu kommunizieren. Dafür braucht es mehr als nur einen 6to4-Gateway oder „Dual Stack“ (d.h. sowohl IPv6 als auch IPv4 unterstützende) Router-Infrastruktur. Vielmehr braucht es bei der aktuellen Strategie zur Einführung von IPv6 für jedes Protokoll auf der Applikationsschicht, mit dem Kommunikation zwischen IPv6- und IPv4-Hosts möglich sein soll, einen Proxy-Server oder Gateway, der auf der Applikationsschicht die Kommunikation zwischen IPv6- und IPv4-Hosts ermöglicht. Nur ein kleiner Teil der Internet-Nutzer wird bereit sein, die diesem Aufwand entsprechenden zusätzlichen Kosten zu tragen, wenn sich nicht ein klarer ökonomischer Nutzen daraus ergibt. Dieses Argument spricht dafür, dass es möglicherweise nie zu der kritischen Masse von IPv6 Benützern kommt, ab der es nicht mehr als nötig angesehen wird, jeden Internet-Dienst mindestens auch über IPv4 anzubieten.

### 11.7.2 Vergleich zu NAT

Es besteht kein Zweifel daran, das in nicht allzuferner Zukunft eine erhebliche Knappheit an IPv4 IP-Nummern auftreten wird, siehe etwa [16]. Es stellt sich jedoch die Frage, ob dies (wie von vielen Autoren angenommen) zu einer allgemeinen Umstellung auf IPv6, oder eher zu einer zunehmenden Verwendung von NAT führen wird.

Nehmen wir an, dass für ein Firmennetzwerk nicht genug IPv4 IP-Nummern zur Verfügung stehen, um jedem Gerät eine globale IPv4-Nummer zuordnen zu können.

Ist es für die Firma nun besser, IPv6 oder ein privates IPv4-Netzwerk und NAT zu verwenden?

NAT ist sehr einfach einzurichten und zu konfigurieren. An der Grenze des Firmennetzwerks zum öffentlichen Internet wird in der Regel sowieso eine Firewall platziert, und es ist praktisch kein zusätzlicher Aufwand, diese so zu konfigurieren, dass sie auch für NAT zuständig ist. Web-Browser funktionieren hinter NAT-Gateways genauso so gut, wie wenn man direkt mit dem Internet verbunden wäre, ohne dass der Systemadministrator eigens einen Gateway oder Proxyserver einrichten muss, wie das nötig ist, um von einem IPv6-Netzwerk aus auf IPv4-Webserver zugreifen zu können. Auch was Mailserver betrifft, ist die Systemkonfiguration bei Verwendung von NAT und einem privaten IPv4-Netzwerk einfacher als bei Verwendung von IPv6 für das firmeninterne Netzwerk.

Ein echtes Problem stellt die NAT-Technik für Peer-to-Peer Anwendungen dar. Im Hinblick auf diesen Anwendungskreis ist IPv6 eindeutig besser als die Verwendung eines IPv4-Netzwerks mit NAT. Weil jedoch Peer-to-Peer Anwendungen in einer breiten Öffentlichkeit in erster Linie als eine technische Möglichkeit zur Copyright-Verletzung wahrgenommen wird, während NAT als "Security-Technologie" wahrgenommen wird ([12]), wird dieses Argument kaum den Ausschlag zur Umstellung von Firmennetzen auf IPv6 geben.

### 11.7.3 Verschiedene mögliche Entwicklungen

A priori sind verschiedene Szenarien denkbar, wie die Umstellung von IPv4 auf IPv6 ablaufen könnte:

#### Szenario A: Von Benutzerinteressen getriebene rasche Protokoll-Umstellung

Wenn es zu irgendeinem Zeitpunkt im Bereich der Applikations-Software eine Entwicklung gibt, durch die dem Endbenutzer ein erheblicher Vorteil durch die Benützung von IPv6 entsteht, kann daraus für ISPs ein ökonomischer Zwang entstehen, die Angebote für Endbenutzer (Privatpersonen sowie Firmen) relativ rasch auf IPv6 umzustellen.

#### Szenario B: Von Spekulation getriebene rasche Protokoll-Umstellung

Theoretisch denkbar wäre auch, dass ISPs in der Erwartung, dass eine solche „Killer-Applikation" für IPv6 bald aufkommen könnte, rein spekulativ in eine rasche Umstellung auf IPv6 investieren, noch bevor eine nennenswerte Nachfrage unter Endbenutzern nach IPv6 aufkommt.

#### Szenario C: Langsame Protokoll-Umstellung im Rahmen von sowieso nötigen Infrastruktur-Erneuerungen

In diesem Szenario geschieht die Umstellung auf IPv6 in der Regel im Rahmen der nächsten sowieso nötigen Erneuerung der Netzwerk-Infrastruktur. So kann auf IPv6 umgestellt werden, auch wenn kaum jemand genug Interesse an IPv6 hat, um extra dafür Geld auszugeben.

#### Szenario D: Der Prozess der Protokoll-Umstellung könnte völlig ins Stocken geraten

Es könnte sich auch zeigen, dass sich die Schwächen von IPv4 durch NAT und eine Reihe weiterer Massnahmen weitgehend in den Griff bekommen lassen, und die ökonomischen Effekte im Zusammenhang der fehlenden Kompatibilitätsforderung (siehe Abschnitt 11.7.1) sich als so stark erweisen, dass IPv4 noch für lange Zeit der De-facto-Standard für das Internet-Protokoll bleibt.

**Szenario E: Der Prozess der Umstellung von IPv4 auf IPv6 könnte durch ein neues Protokoll auf Schicht 4 des OSI Referenz-Modells wieder in Bewegung gebracht werden**

Die Spezifikation eines solchen Protokolls kann die wichtigen Kompatibilitätsforderungen enthalten, und dadurch in dem Mass, wie sich das neue Protokoll durchsetzt, die ökonomischen Effekte, die heute die Umstellung auf IPv6 bremsen und ganz zum Stocken zu bringen drohen, ausser Kraft setzen. Die Umstellung auf IPv6 erfolgt in diesem Szenario im Rahmen von sowieso nötigen Infrastruktur-Erneuerungen, also viel langsamer als in den Szenarios A und B oben postuliert, aber wenigstens würde nichts mehr dagegen sprechen, bei der nächsten Infrastruktur-Erneuerung auf IPv6 umzustellen.

### 11.7.4 Ausser IPv4 (mit NAT) keine Alternativen zu IPv6

In einem „ISP Column“ Artikel [21] im Januar 2006 schrieb Huston: „In the near term, und possibly in a longer term of some decades to come, “extinction” is not a very likely outcome for IPv6 — there is simply no other option on our horizon, so if we are to move away from IPv4 sometime soon then IPv6 is what we will be using instead.“[1] Die Richtigkeit dieser Einschätzung ist unumstritten. Die Frage ist nur, ob die Entwicklung des Internets wirklich dahingeht, dass das Internet als ganzes IPv4 durch ein anderes Protokoll ersetzt, oder ob vielleicht das Gros der öffentlichen Webserver und Mailserver weiterhin IPv4 verwenden wird, während IPv6 nur am Rande als Alternative zu NAT zum Einsatz kommt. Immer wieder wurde die Knappheit der IPv4 IP-Nummern als wesentlicher Grund dafür angegeben, dass IPv4 nicht auf Dauer im Internet verwendet werden könne. Beispielsweise heisst es in der Pressemitteilung der EU Kommission vom 21. Februar 2002 [11]: „Es wird davon ausgegangen, dass der IPv4-Adressraum bis etwa 2005 ausgeschöpft sein wird.“ Tatsächlich besteht kein Zweifel daran, dass in wenigen Jahren eine erhebliche Knappheit an IPv4 IP-Nummern auftreten wird, siehe etwa [16]. Dies ist jedoch kein zwingender Grund zur Abkehr von IPv4. Auch wenn es nicht genug IPv4-Nummern gibt, um jedem Gerät, dass über das Internet kommunizieren können soll, eine eigene IPv4-Nummer zuweisen zu können, ist der Raum der IPv4 IP-Nummern doch gross genug, um das aktuelle Modell des Internets, in dem Webserver und Mailserver in der Regel nicht von jedem Benützer selber sondern von ISPs und spezialisierten Hosting-Anbietern betrieben werden, auf Dauer weiterhin mit festen IPv4 IP-Nummern versorgen zu können. PCs von Endbenutzern funktionieren mit diesem Modell des Internets auch ohne feste eigene IP-Nummern, wobei sich wie in Abschnitt 11.7.2 oben diskutiert mit Hilfe von NAT viele PCs eine IP-Nummer teilen können. So führt die Knappheit der IP-Nummern dazu, dass auch PCs, die ununterbrochen eingeschaltet und mit dem Internet verbunden sind, nicht nebenbei als Internet-Server genutzt werden können. Möglicherweise haben viele ISPs und Hosting-Anbieter ein klares ökonomisches Interesse daran, dass sich dieser *Status quo* nicht ändert.

[1] deutsche Übersetzung: „In der nahen Zukunft, und möglicherweise auch längerfristig mit einem Horizont von mehreren Jahrzehnten, ist ein „Aussterben“ kein sehr wahrscheinliches Schicksal für IPv6 — es gibt einfach keine absehbare Alternative. Daher wird, falls wir uns in der nahen Zukunft von IPv4 wegbewegen werden, IPv6 das sein, was wir stattdessen verwenden werden.“

### 11.7.5 Beurteilung der verschiedenen Szenarien

Eine rasche Umstellung wie in den Szenarios A und B ist unrealistisch. Grundsätzlich erfüllen aus der Sicht von Anwendungsprogrammen IPv4 und IPv6 denselben Zweck, nämlich den Transport von Daten über das Internet. Alles was mit IPv6 möglich ist, ist grundsätzlich auch mit IPv4 möglich. Mit IPv6 lässt sich die Komplexität der nötigen Netzwerkinfrastruktur und der an den Endpunkten nötigen Software reduzieren. Dies ist selbstverständlich wünschenswert, aber von Seiten der Endbenutzer ist aus diesem Grund keine starke Nachfrage speziell nach IPv6 zu erwarten, wie dies in **Szenario A** postuliert wurde. Das Interesse der Endbenutzer ist an Kommunikationsdiensleistungen, und wenn sich diese mit IPv6 kostengünstiger erbringen lassen als mit IPv4, dann ist dieser Kostenvorteil die ökonomische Motivation zur Umstellung auf IPv6.

**Szenario B** ist erst recht völlig ausgeschlossen. Nach den Schocks durch das Platzen der Dot-Com Blase und den extrem teuren Fehlinvestitionen in überteuerte UTMS-Lizenzen ist die Risikobereitschaft vieler grosser Marktteilnehmer gering. Dazu kommt, dass sich alle Kommunikationsdienste auch über IPv4 abwickeln lassen; das Risiko eines grossen Marktanteil-Verlusts durch verspätete Umstellung auf IPv6 ist also vernachlässigbar klein.

Gegen **Szenario C** sprechen Bernsteins bereits oben in Abschnitt 11.7.1 erwähnte Argumente. Die Probleme lassen sich für HTTP und SMTP umgehen, wenn jeder ISP einen Proxy-Server für HTTP zur Verfügung stellt, sowie einen Mailserver, der sowohl über IPv4 als auch über IPv6 erreichbar ist. Die Annahme, dass man mit IPv6 Kommunikationsdienstleistungen billiger als mit IPv4 erbringen könne, erscheint jedoch unplausibel, solange sich die Anbieter von IPv6 basierten Kommunikationsdienstleistungen zusätzlich zu ihrem IPv6 Netzwerk auch noch um Kompatibilität mit IPv4-Nutzern kümmern müssen. Wenn jedoch mit der Umstellung auf IPv6 keine Kostenersparnis möglich ist, worin besteht dann der ökonomische Anreiz für diese Umstellung?

Die Experten sind sich einig, dass **Szenario D** auf Dauer kaum vorstellbar ist. Zu viel spricht aus technischen Gründen gegen die langfristige Verwendung von IPv4, und ausserdem würde dieses Szenario den nationalen Interessen vieler Länder erheblich zuwiderlaufen. Zur Zeit ist die Umstellung auf IPv6 kein politisches Thema, aber wenn weiterhin nicht viel in Richtung auf die Umstellung auf IPv6 geschieht, werden irgendwann IPv4-Nummern so knapp werden, dass der Unmut aller Länder geweckt werden wird, die sich durch ihre im Vergleich zur USA kleinen Zuteilungen von IPv4-Nummern benachteiligt sehen.

Demgegenüber erscheint **Szenario E** durchaus plausibel. Ein Vorschlag für ein solches Schicht 4 Protokoll ist das "Quick Queues Protocol" QQP [5]. Bevor ein solches neues Protokoll einen nennenswerten Beitrag zur Förderung der Umstellung auf IPv6 leisten kann, muss es sich jedoch zunächst einmal soweit durchsetzen, dass es zu einem Standard-Bestandteil der Software praktisch aller neuen Internet-Server (insbesondere Webserver und Mailserver wird) und in der Defaultkonfiguration auch in dem Sinn aktiv ist, dass sich die über IPv4-basiertes TCP und UDP erreichbaren Dienste der Anwendungsschicht auch über QQP erreichen lassen. Für einen solchen Deployment-Erfolg sind neben den Überlegungen im Hinblick auf die Umstellung auf IPv6 auch andere technische Vorzüge

gegenüber TCP und UDP wichtig, wie QQP sie in verschiedenen Bereichen wie unmittelbarer Unterstützung für Webservices, QoS-Garantien, Multihoming und mobilitätsbedingter Änderbarkeit von IP-Adressen anbietet. Selbstverständlich muss QQP auch in IPv4-Netzwerken einsetzbar sein. Im aktuellen Spezifikations-Entwurf wird dies unter anderem durch die Forderung erreicht, dass IPv4-basierte QQP-Server 6to4-Pakete interpretieren und generieren können müssen.

Falls QQP sich in dieser Form durchsetzt (womit zunächst einmal nicht eine Verdrängung von IPv4-basiertem TCP und UDP gemeint ist, sondern nur, dass in der Defaultkonfiguration QQP als Alternative zur Verfügung steht), dann werden mit der Zeit (indem die grosse Mehrzahl der Internet-Server entweder komplett durch neue Server ersetzt wurden, oder sie durch Software-Updates QQP-fähig wurden) die meisten Internet-Dienste über QQP auch für IPv6-Nutzer zugänglich, ohne dass dafür auf der Anwendungsschicht Gateways eingerichtet werden müssen. Dadurch würden in diesem Fall die wesentlichen ökonomischen Hindernisse, die in der jetzigen Situation eine allgemeine Migration zu IPv6 verhindern, hinfällig.

## 11.8 Ausblick

Zusammenfassend halten wir fest, dass die Version 6 des Internet Protokolls insbesondere im Hinblick auf die viel grössere Anzahl der zur Verfügung stehenden Adressen entscheidende Vorteile gegenüber Version 4 aufweist. Die Methode der „Network Address Translation“ (NAT), mit der sich bei Verwendung von IPv4 das Problem der Adressknappheit weitgehend umgehen lässt, ist mindestens langfristig keine gute Lösung, weil dieser Ansatz im Widerspruch zu den grundsätzlichen Prinzipien der Protokollarchitektur des Internets steht. Dennoch sind zum jetzigen Zeitpunkt die ökonomischen Anreize nicht ausreichend, um eine weitgehende Umstellung von IPv4 auf IPv6 zu bewirken. Langfristig ist jedoch damit zu rechnen, dass IPv4 irgendwann nicht mehr den Anforderungen genügen wird. Dies wird dazu führen, dass dann genügend starke ökonomische Anreize zur IPv6 Verwendung entstehen.

# Literaturverzeichnis


[1] ARKKO, Jari; AURA, Tuomas; KEMPF, James; MÄNTYLÄ, Vesa-Matti; NIKANDER, Pekka: *Securing* IPv6 *neighbor and router discovery.* Proceedings of the 3rd ACM workshop on Wireless security WiSE '02 (September 2002).

[2] BAGNULO, Marcelo; GARCIA-MARTINEZ, Alberto; AZCORRA, Arturo: *Efficient security for* IPv6 *multihoming* ACM SIGCOMM Computer Communication Review, Volume 35 Issue 2 (April 2005).

[3] BERNSTEIN, Dan J.: *The* IPv6 *mess.* (Februar 2003). http://cr.yp.to/djbdns/ipv6mess.html

[4] BIERINGER, Peter et al.: *Current Status of* IPv6 *Support for Networking Applications* (2006) http://www.deepspace6.net/docs/ipv6_status_page_apps.html

[5] BOLLOW, Norbert: QQP - *Quick Queues Protocol.* Work in Progress (May 2006). http://www.ietf.org/internet-drafts/draft-bollow-qqp-02.txt

[6] CARPENTER, Brian E. and MOORE, Keith: RFC 3056 – *Connection of* IPv6 *Domains via* IPv4 *Clouds.* (Februar 2001). http://www.ietf.org/rfc/rfc3056.txt

[7] CONTA, A., and DEERING, S.: RFC 2463 – *Internet Control Message Protocol (ICMPv6) Specification* (December 1998). http://www.ietf.org/rfc/rfc2463.txt

[8] DEERING, Stephen E. (Ed.): RFC 1256 – *ICMP Router Discovery Messages.* (September 1991). http://www.ietf.org/rfc/rfc1256.txt

[9] DEERING, Stephen E., and HINDEN, Robert M.: RFC 2401 – *Internet Protocol, Version 6* (IPv6) *Specification* (Dezember 1998). http://www.ietf.org/rfc/rfc2460.txt

[10] DRAKE, William J. (Ed.): *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (WGIG). Published by: The United Nations Information and Communication Technologies Task Force, New York, 2005.

[11] EU Pressemitteilung: *Kommission für das Internet der nächsten Generation.* (Februar 2002). http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/02/284

[12] FORD, Mat: *Barriers to* IPv6 *adoption.* (2003). http://www.ipv6.org.eg/Barriers_to_IPv6_Adoption.pdf

[13] GALLAHER, Michael P.: IPv6 *Economic Impact Assessment* Planning Report 05-2. Prepared by: RTI International for: (U.S.) National Institute of Standards & Technology (October 2005). http://www.nist.gov/director/prog-ofc/report05-2.pdf

[14] GELBSTEIN, Eduardo und Jovan KURNALIJA: *Internet Governance: Issues, Actors And Divides.* Diplo Foundation (October 2005). http://www.diplomacy.edu/isl/ig/

[15] GUARDINI, Ivano and FASANO, Paolo and GIRARDI, Guglielmo: IPv6 *operational experience within the 6bone.* (März 2000). http://carmen.cselt.it/papers/inet2000/index.htm

[16] HAIN, Tony: A Pragmatic Report on IPv4 Address Space Consumption. The Internet Protocol Journal - Volume 8, Number 3 http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html

[17] HINDEN, R., and S. DEERING: RFC 3513 – *Internet Protocol Version 6* (IPv6) *Addressing Architecture* (April 2003). http://www.ietf.org/rfc/rfc3513.txt

[18] HUITEMA, C.: RFC 3068 – *An Anycast Prefix for* 6to4 *Relay Routers.* (Juni 2001). http://www.ietf.org/rfc/rfc3068.txt

[19] HUITEMA, C.: RFC 4380 – *Teredo: Tunneling* IPv6 *over* UDP *through Network Address Translations* (NATs). (Februar 2006). http://www.ietf.org/rfc/rfc4380.txt

[20] HUSTON, G.: RFC 4177 – *Architectural Approaches to Multi-homing for IPv6* (September 2005). http://www.ietf.org/rfc/rfc4177.txt

[21] HUSTON, G.: IPv6 – *Evolution or Revolution.* Internet Society: ISP Column. (Januar 2006). http://www.potaroo.net/papers/isoc/2006-01/ipv6revolution.html

[22] IAB (Internet Architecture Board) and IESG (Internet Engineering Steering Group): *IAB/IESG Recommendations on* IPv6 *Address Allocations to Sites* (September 2001). http://www.ietf.org/rfc/rfc3177.txt

[23] IGF Secretariat: *Consultations on the convening of the IGF.* February 2006. http://intgovforum.org/meeting.htm

[24] JOHNSON, David B. and Charles E. PERKINS and Jari ARKKO: RFC 3775 – *Mobility Support in IPv6* (June 2004). http://www.ietf.org/rfc/rfc3775.txt

[25] KAUFMANN, C. (Ed.): RFC 4306 – *Internet Key Exchange (IKEv2) Protocol* (Dezember 2005). http://www.ietf.org/rfc/rfc4306.txt

[26] KENT, S.: RFC 4301 – *Security Architecture for the Internet Protocol.* (Dezember 2005). http://www.ietf.org/rfc/rfc4301.txt

[27] KENT, S.: RFC 4302 – *IP Authentication Header.* (Dezember 2005). http://www.ietf.org/rfc/rfc4302.txt

[28] KENT, S.: RFC 4303 – *IP Encapsulating Security Payload (ESP)* (Dezember 2005). http://www.ietf.org/rfc/rfc4303.txt

[29] Microsoft Corporation: IPv6 *for Microsoft Windows: Frequently Asked Questions* (Published: September 23, 2002; Updated: May 4, 2006). http://www.microsoft.com/technet/itsolutions/network/ipv6/ipv6faq.mspx

[30] NARTEN, T., and NORDMARK, E.: RFC 2461 – *Neighbor Discovery for IP Version 6 (IPv6)* (December 1998). http://www.ietf.org/rfc/rfc2461.txt

[31] NIKANDER, P. (Ed.), KEMPF, J., and NORDMARK, E.: RFC 3756 – IPv6 *Neighbor Discovery (ND) Trust Models and Threats* (May 2004). http://www.ietf.org/rfc/rfc3756.txt

[32] NORDMARK, E., and LI, T.: RFC 4218 – *Threats Relating to* IPv6 *Multihoming Solutions* (October 2005). http://www.ietf.org/rfc/rfc4218.txt

[33] PARTRIDGE, Craig: RFC 1809 – *Using the Flow Label Field in* IPv6 (June 1995). http://www.ietf.org/rfc/rfc1809.txt

[34] POSTEL, J.: RFC 791 – *Internet Protocol.* (September 1981). http://www.ietf.org/rfc/rfc791.txt

[35] POSTEL, J.: RFC 792 – *Internet Control Message Protocol.* (September 1981). http://www.ietf.org/rfc/rfc792.txt

[36] PLUMMER, David C.: RFC 826 – *An Ethernet Address Resolution Protocol.* (November 1982). http://www.ietf.org/rfc/rfc826.txt

[37] SAVOLA, Pekka und PATEL, C.: *Security Considerations for* 6to4. RFC 3964. (Dezember 2004). http://www.ietf.org/rfc/rfc3964.txt

[38] SAVOLA, Pekka: *Measuring the internet's vital statistics: Observations of* IPv4 *traffic on a* 6to4 *relay.* ACM SIGCOMM Computer Communication Review, Volume 35, Issue 1, S. 23–28 (Januar 2005).

[39] STILLER, Burkhard: Vorlesungsunterlagen zur Veranstaltung „Mobile Communication Systems“ Sommersemester 2006 an der Universität Zürich: Modul 8. http://www.csg.unizh.ch/teaching/ss06/mobsys/intern/M08-2up.pdf

[40] Swiss IPv6 Taskforce: *Links* http://www.ch.ipv6tf.org/?cid=116

[41] KOZIEROK, Charles M.: *The* TCP/IP *Guide.* (December 2005). http://www.tcpipguide.com/

[42] TOMSON, S., and T. NARTEN: RFC 2462 – IPv6 *Stateless Address Autoconfiguration* (December 1998). http://www.ietf.org/rfc/rfc2462.txt

[43] WIESE, Herbert: Das neue Internetprotokoll IPv6, Carl Hanser Verlag, 2002.

Alle oben zitierten URLs wurden im Juli 2006 referenziert.