Fachhochschule Darmstadt

DIPLOMARBEIT

von

Jörg Abendroth

bearbeitet am

School of Control Systems & Electrical Engineering
School of Electronic & Communication Engineering

Referent:
Prof. Dr. Fuhrmann

Korreferent:
Dr. Davis
Dublin Institute of Technology

SS 2000

Thema

der

DIPLOMARBEIT

Implementation of an IP-based
Wireless in the local loop communication system

The Project Brief

SUPERVISOR: Dr. Mark Davis,Room 325 (Extn. 4797).
DEPARTMENT: Electronic and Communications Engineering.
TITLE: Implementation of an IP-based wireless in the local loop (WLL) communication system.
NO. OF STUDENTS: 2
TECHNICAL AREA: Digital wireless communications networks.
TASK PREDOMINANTLY: Development.
INVOLVING: Hardware and software.
SPECIALIST EQUIPMENT REQUIREMENTS: PC.
PREFERRED TECHNICAL BACKGROUND: Communications Eng.
PROJECT SYNOPSIS: Currently there are two emerging technology trends that are set to become dominant in the telecommunications industry, namely the increasing use of wireless systems and the shift from voice-centric circuit switched networks over to data-centric packet switched networks.
Increasingly, wireline minutes are being replaced by wireless minutes, especially with the phenomenal success of mobile cellular networks. However, recently wireless technologies are being considered as a means of access to the local loop. Wireless in the local loop (WLL) is a system that uses digital radio to connect subscribers to the public switched telephone network (PSTN) instead of the traditional copper twisted pair (known as the "last mile").
The emergence of the packet-switched data networks in recent years has been driven by the explosive growth in the use of the internet. Of particular interest to the telecommunications industry is the development of internet telephony or Voice over IP (VoIP). Although it emerged initially as a technology for making inexpensive telephone calls via the web, VoIP opens the door for the integration of voice, video, and data on a single IP-based network. The growth of IP-based communications networks represents a fundamental shift away from the traditional voice-centric circuit switched networks towards data-centric packet switched networks.
The proposed project is based upon two existing standards: the IEEE 802.11 standard for wireless local area networks (WLAN) and the ITU-T H.323 multimedia standard for IP networks. The basic concept is to configure a WLAN as a WLL system and to use the H.323 standard to support VoIP internet telephony. Having implemented such a packet-switched WLL system, it is then proposed to evaluate its performance with regard to quality of service (QoS) issues such as sound quality and reliability.
BACKGROUND READING: Internet sites on WLL and VoIP.

Abstract

The content of this report describes the technique used in Wireless Local Area Network (WLAN) systems (IEEE 802.11). With a closer look into the used modulation scheme, media access (an example of RTS/CTS is given), antenna system and differences toward wired the LAN. Examples for useful employment and fault localization will be given.
Further voice over IP, the technique used in Internet telephone are described (ITU-T H323 standard). After describing parameters influencing the subjective quality (delay, jitter, BER & throughput), known measurement standards are named and a brief description of the H.323 with a short comparison with SIP is given. At the end of that chapter examples of successful VoIP employments are named.
After one chapter, which introduces network management, used terms and gives example usage of a SNMP management tool. A closer look into quality of service and ways to deliver it is done. This chapter closes with a brief overview about problems related to the task implementing a mobile phone like wireless local loop VoIP network (namely billing, roaming and mobility).
In the second part of the report a description about performance evaluation methods is given, which leads into a detailed test plan. A description about tests, which were performed during the project period are given.
Together with the knowledge of the first part a final conclusion is made with a suggestion for further preceding toward a wireless Internet telephone system, with equal quality and reliability like the todays mobile phone system.

Contents

I Covered Areas **1**

1 WLL **2**
1.1 Introduction . . . 2
1.2 Modulation . . . 2
1.2.1 Narrow Band - Spread Spectrum . . . 2
1.2.2 DSS . . . 3
1.2.3 FHSS . . . 4
1.2.4 FHSS - DSSS . . . 6
1.3 Media Access . . . 6
1.3.1 Introduction . . . 6
1.3.2 IEEE802.3 . . . 7
1.3.3 IEEE802.11 . . . 7
1.4 Antenna System . . . 9
1.4.1 Introduction . . . 9
1.4.2 Transmission Antennas . . . 9
1.4.3 Receiving Antennas . . . 9
1.5 Differences . . . 10
1.5.1 Error Detection . . . 10
1.5.2 Network Participation . . . 10
1.5.3 ROAMING . . . 11
1.6 Note about equipment used in this project . . . 11
1.7 Practical Ideas . . . 12
1.7.1 Maximize the network capacity . . . 12
1.7.2 Access control . . . 12
1.7.3 Fault Detection - with details of the Breezecom equipment 12

2 Voice over IP **14**
2.1 Introduction . . . 14
2.2 About Speech . . . 14
2.3 Parameters influencing the VoIP Quality . . . 16
2.3.1 Delay . . . 17

2.3.2 Jitter . . . 17
2.3.3 BER . . . 18
2.3.4 Throughput . . . 18
2.4 Measurement . . . 18
2.4.1 Introduction . . . 18
2.4.2 MOS . . . 19
2.4.3 Voice Simulator Tool . . . 19
2.5 H323 . . . 22
2.5.1 Introduction . . . 22
2.5.2 Control part of H.323 . . . 22
2.5.3 Data Parts . . . 22
2.5.4 Other information about the H.323 . . . 24
2.6 SIP . . . 25
2.6.1 Overview . . . 25
2.6.2 Comparison with H.323 . . . 25
2.7 VoIP over WLL . . . 26
2.8 Examples of successful VoIP employment . . . 26
2.8.1 As a cheap telephone network . . . 26
2.8.2 Full service Web page . . . 28
2.8.3 Information management . . . 28

3 Network Management 29
3.1 Introduction . . . 29
3.2 Perspectives and Reasons . . . 29
3.3 OSI Model . . . 30
3.3.1 Organizational Model . . . 30
3.3.2 Informational Model . . . 30
3.3.3 Communicational Model . . . 31
3.3.4 Functional Model . . . 31
3.4 SNMP Protocol . . . 34
3.4.1 Introduction . . . 34
3.5 Basic terms . . . 34
3.5.1 MIB . . . 34
3.5.2 MDB . . . 35
3.5.3 Agent and Manager . . . 35
3.5.4 RMON . . . 35
3.5.5 SMI . . . 35
3.5.6 TMN . . . 35
3.6 Scotty a network management software . . . 36
3.6.1 About Scotty/Tkined . . . 36
3.6.2 Short explanation of the handling . . . 37
3.7 Other useful SNMP related softwares . . . 39

3.7.1 ucd-snmptools . . . 39
3.7.2 MRTG . . . 40

4 VoIP over WLAN in the WLL 42
4.1 QoS . . . 42
4.1.1 Introduction . . . 42
4.1.2 QoS in the network . . . 43
4.1.3 Techniques for maintaining a QoS . . . 43
4.2 Voice over **A**synchronus **T**ransfer **M**ode (ATM) . . . 46
4.3 Billing problem . . . 46
4.4 Roaming and Mobility . . . 47

II Tests 48

5 General things about testing 49
5.1 Introduction . . . 49
5.2 How to test . . . 49
5.3 What to test . . . 51
5.4 Standards . . . 52
5.4.1 RFC 2544 Benchmark Methodology for Network Interconnect Devices . . . 52
5.4.2 P 861 . . . 52
5.5 Known common tests . . . 53

6 Approach to develop a test plan 54
6.1 Introduction . . . 54
6.2 Test to perform . . . 54
6.3 Values to be tested . . . 55
6.4 Parameters to be tested . . . 55
6.5 Question to be answered . . . 56

7 The test plan 58
7.1 A special test software . . . 58
7.1.1 Introduction . . . 58
7.1.2 Test Software Features . . . 58
7.2 Chosen tests . . . 61
7.3 Test Instructions . . . 61

III Results and Conclusion **63**

8 Test Series **64**
8.1 Qualitative Tests . . . 64
8.1.1 Objective Description . . . 64
8.1.2 Result . . . 64
8.1.3 Conclusion . . . 64
8.2 First Software Tests . . . 66
8.2.1 Objective Description . . . 66
8.2.2 Result . . . 66
8.2.3 Conclusion . . . 67
8.3 Parameter Tests . . . 67
8.3.1 Objective Description . . . 67
8.3.2 Result . . . 71
8.3.3 Conclusion . . . 71
8.4 Quality Capacity Coverage Tests . . . 71
8.4.1 Objective Description . . . 71
8.4.2 Result . . . 72
8.4.3 Conclusion . . . 72
8.5 Verifying with VoIP Software Tests . . . 72
8.5.1 Objective Description . . . 72
8.5.2 Result . . . 73
8.5.3 Conclusion . . . 73
8.6 Real WLL Setup Test . . . 74
8.6.1 Objective Description . . . 74
8.6.2 Result and Conclusion . . . 75

9 Final Conclusions **79**

IV Appendix **81**

A How to register an own enterprise MIB **A-0**

B Application of Markov Chains in VoIP **B-0**

C Technical Specifications of Breezecom Equipment **C-0**

D Personal Report **D-0**

V Bibliography **E-0**

List of Figures

1.1 Comparison Narrow and Spread Spectrum 3
1.2 DSSS, the signal level can be under the noise level 3
1.3 Spectrum of a FHSS signal 4
1.4 Different FHSS hopping sequences with jamming signal 5
1.5 The described example of two conversations the same time 8

2.1 Markov 6 stages chain 15
2.2 Simplified Markov 4 stages chain 16
2.3 Traffic dump of a Netmeeting call. 20
2.4 Overview about inter working of H.323 protocols (taken out of H323v2 draft) 21
2.5 Example of professionell VoIP Gateway 27

3.1 Everything together and extensive accounting management could bring the network down 33
3.2 Scotty/Tkined main window 36
3.3 Extensions like SNMP trouble allow various ways of querying the nodes. 38
3.4 The MIB tree browser window 39
3.5 Changing a value out of the MIB tree browser. 40
3.6 The during the project programmed private menu in Tkined . . . 41

4.1 Shaping traffic above the maximal bandwidth 44
4.2 Shaping equal important traffic 44

5.1 Traffic marking for monitoring purposes 50

7.1 Flowchart of the used testscript 62

8.1 Map of floor 4 and room 407 of DIT Kevin Street 65
8.2 Plot of parameter MaxNumRetransmission set to 0 68
8.3 Plot of parameter MaxNumRetransmission set to 1 69
8.4 Plot of parameter MaxNumRetransmission set to 5 70
8.5 Setup of simultaneous VoIP and Software test 73

8.6 Picture of Test setup 75
8.7 Histogram of a simplex channel 77
8.8 Histogram of a full duplex 78

Introduction

The Internet becoming more and more popular, while on the other side nearly each second person has a mobile phone. These two facts emerge in the question how far they can both be combined.
Existing solutions for Internet Telephony are known. Mostly they are developed for large scall company gateways, yet a end user wanting to use a common phone for calling is widely overseen. Hence part of the project was it to connect an ordinary phone to the PC. And during the research time only one solution had been found (www.quicknet.com), a modified sound card, with a DSP for hardware voice encoding.
During beginning also Internet telephony was a word used, but only one commercial gateway established Now at the end there are 3 services known, which provide free calls into the public phone networks (*www.hottelephone.com*,*www.dialpad.com* and *www.go2call.com*). And another end user phone to PC adapter is discovered (*www.go2call.com/FNC.asp*).
But why is the packet routed Internet not yet wireless and replaces the switched phone networks ? What would be important for a successful combination of VoIP and WLL ? These are the question standing at the beginning of the project.
To answer these, it had been taken a closer look at the wireless Internet equipment. In the special case of this project Breezecom Wireless Access has been employed.
As new and uncommon questions are answered with new and uncommon equipment through the course of the project a test software has been developed, which is based on the Markov Chain model of a telephone conversation and a survey of real telephone conversations, for helping at this survey the author like to thank Philip Rech and Silke Wolter.
For the technical, organisatorical and overall help and supervision of the project many thanks go to my supervisor Dr. M. Davis, as well as my team partner Eavan Mangan.
As English is not my native language I like to thank Denise O'Brian for helping to correct the grammatical mistakes.

Part I

Covered Areas

Chapter 1

Wireless Local Loop (WLL)

1.1 Introduction

WLL can be either a narrow band packet radio system, a infrared network, or a spread spectrum system. The latter gains more and more in popularity and is also used in this project. Hence the report will be limited to the issues of Spread Spectrum, although parts (e.g. the protocol layer) are identical in the other areas.

1.2 Modulation

1.2.1 Narrow Band - Spread Spectrum

In contrast to earlier analog transmission techniques, today digital techniques are widely used. The advantage is, that the data can be compressed (redundancy can be reduced) in a source independent way. In this respect the Shannon Limit[1] has fundamental importance. This limit tells how much a given data can be compressed, or in other words: the minimum required bandwidth. The narrow band approach tries to use only this bandwidth and extend the amount of data only for error protection and correction purposes.
The spread spectrum approach increases the amount of used bandwidth artificial, but in such a way, that it becomes possible to have two different signals on the same frequency of which both are decodable. Hence the total capacity of all used channels (stations) in one frequency band is larger than having narrow band stations next to each other in that band.

[1] See Communication Engineering Lectures

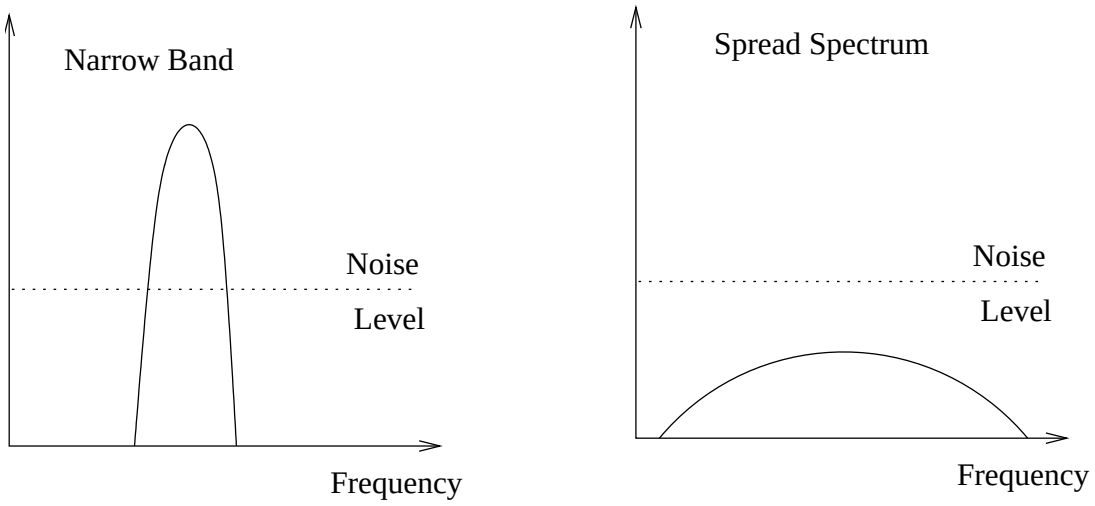

Figure 1.1: Comparison Narrow and Spread Spectrum

1.2.2 Direct Sequence Spread Spectrum (DSSS)

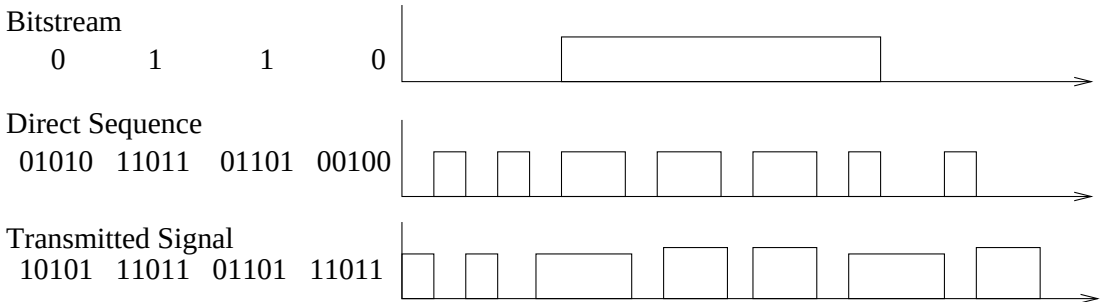

Figure 1.2: DSSS, the signal level can be under the noise level

At this spread spectrum technique, each bit of data will be multiplied by a special sequence. The output are multiple bits, representing the one bit. In the frequency domain the PSD becomes wider, but lower (see figure 1.2 and 1.1). The receiver needs to know the encoding sequence to decode the bit stream, because a different sequence will give a different bit stream. The advantage is that a jamming signal only interferes with one frequency, which means a fraction of the bit stream. However there is still the disadvantage that, besides increasing complexity, in the case of great variations of the noise(fading) level (e.g. another DSSS station nearby or fast relative movements of the two stations) the BER[2] will increase.

[2]Bit Error Rate

1.2.3 Frequency Hopping Spread Spectrum

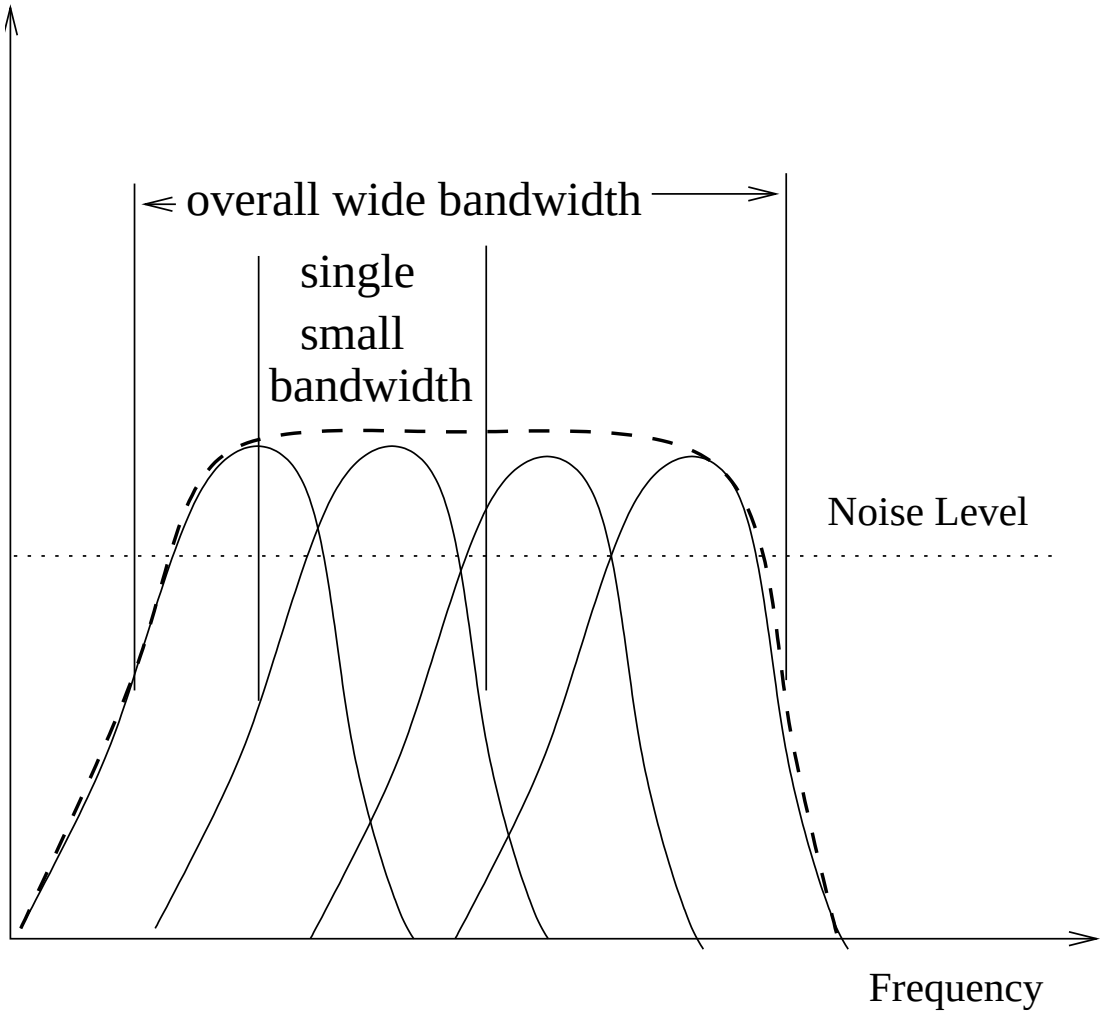

Figure 1.3: Spectrum of a FHSS signal

This technique is similar to FDM[3], but instead of giving each channel its own frequency, all channels use the same frequencies simply at different times. Seen on the long time scale one station needs a wider bandwidth, which also can be called a spread spectrum technique (see figure 1.3).

The sequence that the different channels use is called the hopping sequence. Different regions and countries have fixed different hopping sequences. This also limits the number of stations, which could be in the same band at the same time. The advantage is, that a jamming signal is mostly is only on one of the frequencies, and only for the time when the data is sent on this frequency the

[3]Frequency Devision Multiplexing

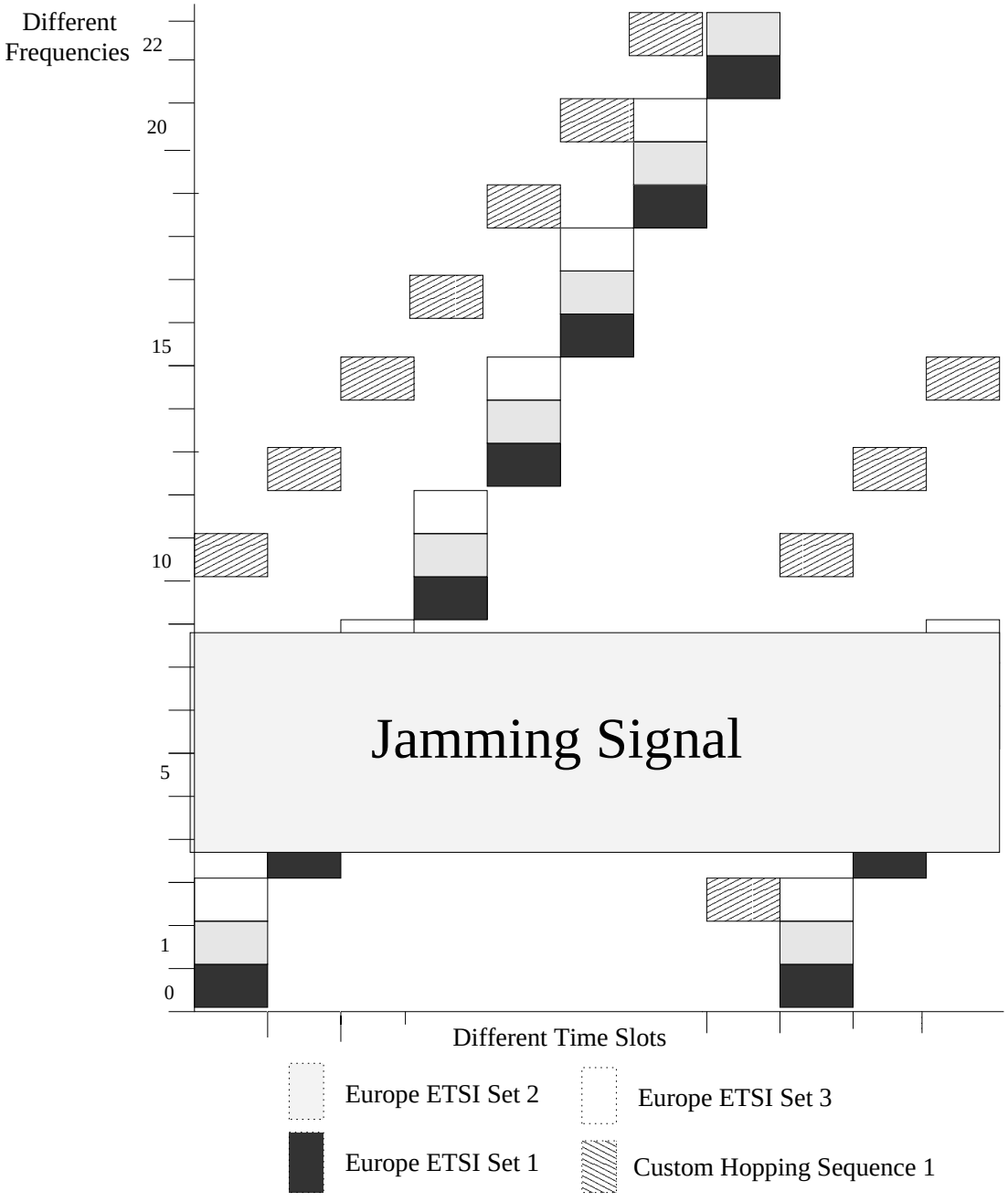

Figure 1.4: Different FHSS hopping sequences with jamming signal

signal will be disturbed and the bit stream will have errors. As an example, in a fixed station environment it is even possible to measure the number of packets with errors on the different frequencies and decide on a hopping sequence, which avoids the jammed frequencies (like the custom sequence in figure 1.4). However, the disadvantage is that the hops need to be coordinated very accurately, hence synchronization is important. This increases the complexity. Also as the station only stays on one frequency for a certain time (default 64ms) there is a maximum length of the packets (about 192 kByte at 3MBit/s Bit rate). In some rare cases this is too small. For these cases packet fragmentation has been introduced into the the IEEE[4] 802.11.

1.2.4 FHSS - DSSS

Parameter	DSSS	FHSS
Coallocation	is done by deviding band into 4 sub bands	is done by different hopping sequences (theoretical 26 different sequences)
Interference Immunity	good until certain level, then impossible to operate	as different frequencies are used the quality will deteriorate slowly
interference station of same kind nearby, while friend far away	need to adapt via power control mechanisms	no problem as there are always unblocked hops
throughput	transmit continously, hence higher throughput	need to spend time for hopping and resynchronizing
Circuit complexity	higher processing amount	processing consists of switching frequencies, which is much easier to implement

1.3 Media Access

1.3.1 Introduction

There are several ways to use a given frequency range with different logical channels. In the following section only a brief brief outline of the most common ways is given and only details about the one used in the project equipment are discussed. This is also the quasi standard, which has becomes more and more popular.

[4]Institute of Electrical and Electronical Engineers

Frequency Division Multiple Access: Each channel gets its own frequency. The advantage of this is that a guaranteed bandwidth is given. A disadvantage is that some frequencies are have more interference than other. Also the channel limit needs to be kept within certain limits, otherwise neighbor channel interference takes place.

Time Devision Multiple Access: The time will be divided into times lots, which are owned by the different channels. It is Important, that all station clocks are synchronized.

Code Devision Multiple Access: An unique spreading code is associated with each user. This means the changing of a conversation partner needs a change of code patterns, which is a disadvantage in a network, as all like to communicate with all.

Carrier Sense Multiple Access: Like TDMA the same frequencies are used by all, at different times. The difference is that there are no predefined times lots, but a distributed mechanism to handle access. The rest of this section gives a closer look of this standard.

1.3.2 Wired World (IEEE802.3)

One of the big issues in every network is determining who will be using the resources to transmit a message and at which time. In a wired network (in case of Ethernet 802.3) this is decided by CSMA/CD[5], which means each station monitors the media (wire) and if the media is free it starts to send. It continues to monitor if the transmission is not disturbed by other sending stations (collision detect). This works, especially as the wire guarantees, that all stations hear each other.

1.3.3 Wireless World (IEEE802.11)

As on the wireless medium it is not guaranteed that all station hear each other, and so the collision detection does not work all the time. For example this could mean station A (e.g. an access point) is on a hill hearing all stations, while station B and C are on the opposite side of the hill but can not hear each other. However both have an excellent connection to the base station. One easy way to avoid collisions would be to introduce a send permission issued by station A, like in the Amateur Radio Packet Radio network (DAMA[6] protocol). However there are disadvantages, which are outlined in the following example. In a mountain area on each hill is an access point, while in the valleys

[5]CSMA/Collision Detect
[6]Demand Assigned Multiple Access

several stationary and mobile stations exist. A data collecting mobile station needs to be connected to the network the whole time. To enable this, together with interlinks of the access points, all stations need to be on the same frequency.

Of course a concept using special interlink frequencies, different entry frequencies for each access point and a multi band mobile station receiver, which monitors the quality of all possible access points, would be far more advanced, but needs much more planing, coordinating and complex technology. Therefore this example is not too far from reality

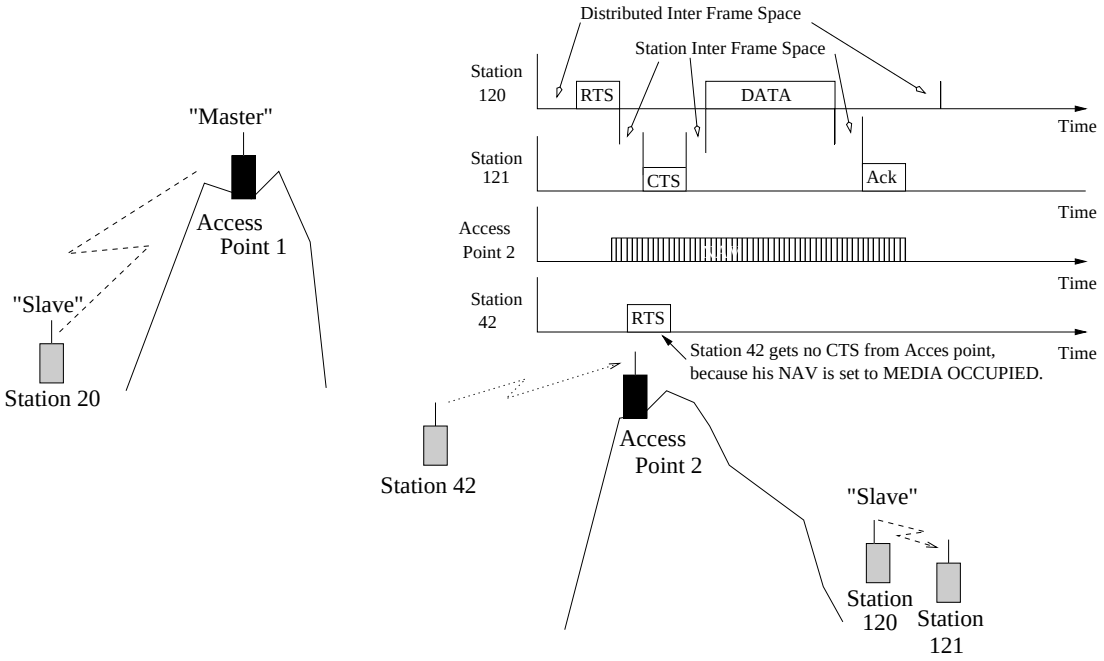

Figure 1.5: The described example of two conversations the same time

Remembering the solution of the master slave relationship brings the question, which of the stations is the master (probably the access point), and how does the master on hill 1 give slave 120 permission to send if both can not hear each other (out of range). Also the question if slave 120 may be allowed to talk to his neighbor (slave 121), while the master talks to slave 20. As long as both conversations do not disturb each other (still out of range). Therefore it is necessary to implement again distributed media access mechanisms, but this time keeping in mind that not all stations can hear each other, but some station hear more stations than other (see figure 1.5). In the 802.11 this is be done by CSMA/CA[7] namely with an RTS[8] and CTS[9]. This works like shown in figure 1.5. Station

[7]CSMA/collision avoid
[8]Ready To Send
[9]Clear To Send

120 sends a RTS, showing that it would like to send. The destination station 121 knows if it also doesn t hear any other station (or doesn t know about a scheduled transmission) and sends back a CTS . Hence if the media is free on both sides the transmission starts. All station in the range of the 120 and 121 set their NAV[10] accordingly (wait - media occupied). While master 1 and slave 20 didn t hear about the on going transmission they can start their transmission independently. Of course this does mean that during the access point - access point transmissions potentially more stations need to be silent, while conversation between neighbor nodes take less network capacity.

1.4 Antenna System

1.4.1 Introduction

Once it has been determined that a station pair has the frequency for its own, the next concern is how to maximize the data rate and therefore the receiving conditions. Especially in the WLAN, which will be mostly employed indoors, the conditions can vary quite a lot. There can be temporal shadowing e.g. if a one stands in the direct line sight to the access point. Other electronic office equipment (namely the copying machine, with its flash; or microwave ovens) may give jamming signals. But the biggest problem is the multi path propagation. A solution, other than increasing the output power of the sender, is to use antenna diversity at the receiving side. The following section deals with various ways of diversity , but first a thought about the transmission antennas is given.

1.4.2 Transmission Antennas

Beside special cases, in which the working range is very special (e.g. along a long corridor), the transmission antennas need not conform to any special form, like directional. Sometimes at omnidirectional transmitting antenna is especially liked, for example if the stations can be also on lower and upper floors than the access point.

1.4.3 Receiving Antennas

The already named diversity, can be achieved in different ways.

Physical dislocation of two antennas: While the bandwidth requirement is the same, and the antenna size increases no other disadvantage takes place.

[10] Network Allocation Vector

This exploits that multi path propagation is very location dependent. A distance between $\frac{1}{4}\lambda$ at frequencies above 1 GHz is reasonable good for the Signal to Noise improvements gained.

Using several Frequencies: As the bandwidth are increased this method will not be used in WLL. Bandwidth here is a to valuable item, to be used for other than capacity improvements.

Polarized Transmission: Using a vertical and horizontal polarized transmitting antenna would enable it to do polarized diverty. However this would need twice as much output power, as two antennas need to be feed independently.

Field Component Diversity: This is a very theoretical and not much tested way to improve the received signal. The idea is to exploit the fact that the same information is in the E and H field of an electromagnetic wave.

Time diversion: Sending the same data twice is a way to eliminate short term influences like multi path propagation. However this also decreases the maximum bit rate (or needed bandwidth).

1.5 Differences toward plain 802.3

1.5.1 Error Detection

In case of a collision or transmission error another mechanism is implemented differently in 802.11, than in 802.3. At the wire a collision is detected early and transmission errors caused by anything other than collisions are very rare. In the wireless LAN an ongoing collision is not detected by the sending stations (this would need to have complex full duplex capable transceivers) and further errors because of noise, distortions and multi path transmissions are likely. While on the wire no error detection (beside the collision detection) is done, the wireless standard has error detection implemented. In case of a detected error there will be a retransmission, this mechanism brings the BER[11] into the range of wired media. However this has the disadvantage is explained in section 2.7 (page 26).

1.5.2 Network Participation

In the wired world one can participate in a network if he is connected via cable to others. No real access control is done. In the special case of VPNs[12] there is

[11] Bit Error Rate
[12] Virtual Private Networks

access control and encryption on the transport layer.
However access control is implemented in 802.11 in form of the ESSID[13]. The ESSID can be seen like the Workgroup in the Windows environment. Only a client with the same ESSID can associate with the access point. Thus it is possible to form working groups at the same frequence and hopping sequence, although it would be more efficient to divide by hopping sequences as station of the same hopping sequence need to share the bandwidth.

1.5.3 ROAMING

In the case of a mobile station it is possible, that it can go out of range of the original access point and move into the range of another. As the IEEE802.11 provides ”roaming” the network connections of the mobile station will not be lost. The station will keep it‘s IP address and as the IP network is flexible in routing the packets will find its new path to the new access point. However there could be a time for restructuring until the network routes settled. Roaming is a very basic service compared to the necessaries of Mobile IP, which provides world wide roaming, including change of IP addresses to adapt to the local network structure.

1.6 Note about equipment used in this project

During this project a Breezecom wireless LAN was used, which uses FHSS spread spectrum at 2.4 GHz, employing IEEE 802.11 CSMA/CA media access control and location diversity to maximize the receiving capabilities. As the equipment uses 802.3 compatible twisted pair network on the wired side installation into an existing LAN is very easy. In most cases the already installed network card, with the according software does not need to be changed at all. Problems can occur if the needed bandwidth exceeds the nominal 3 MBit/s wireless bit rate (1.6 MBit/s nominal end to end bit rate). It is a very good solution in case that a company wants to extend for example its changing conference rooms with network capability, without installing multiple times a new network or a visiting external should get access to the network. For more information see appendix **??** especially 1.3.1,1.3.2 and 1.3.5, as well as the technical specifications.

[13]Extended Service Set ID

1.7 Practical Ideas

1.7.1 Maximize the network capacity

In case of a nearly fixed network environment e.g. a company will use the given office for half a year and use the wireless LAN instead of a fixed LAN to save installation costs. In this case it would be possible for the network administrator to use site survey software to find out about that special environment. This would mean the tester takes a laptop with the software and measure the signal strength and throughput on different locations in the office building. According to the measurements he could change the location of the access points and the stations to maximize the network capacity (minimize the BER[14]).
Also a survey about the number of packets transmitted about one frequencies may give information about jamming signals at certain frequency. Then it is possible to change the hopping sequence to avoid these frequencies and again minimize the BER.

1.7.2 Access control

The ESSID as part of the 802.11 protocol allows a kind of access control, the problem could be that once the ESSID is guessed correctly the network is open. This could be prevented by using VPNs, which are not only limited to the wireless network. In this case it would be possible to have a VPN on the wireless and wired LAN, then without association to a VPN no further services (e.g. access to mail server, Internet access) are available. The VPN access server also allows a remote unit to join e.g. over the Internet. Hence a mobile worker could join and work from abroad, as if they were in the office. As VPNs provide more extensive security features eaves dropping in the WLL is also prevented. As some of the newer implementations can allow encryption on the transport layer, it is important to note, that encryption from the VPN and encryption on the transport layer only increases the overhead and decreases the network capacity. Hence it is important to keep an overview to, show which features are provided by the different components.

1.7.3 Fault Detection - with details of the Breezecom equipment

Here are some ideas about searching for faults in WLL systems. First of all it is important to have access to the error messages of the WLL units, which can be done via SNMP or the local terminal adapter. In the case of a single connection

[14]Bit Error Rate

problem it can always be monitored if the associated station counter (see section 3.7.1 for how to do it) goes up, which means the WLL connection is alright. Try to access e.g. a web page (better send a ping to the DNS/SSfootnoteDomain Name Service server), this initial traffic is needed to publicize the IP address of the PC at the SA[15]. As the AP[16] keeps a list of addresses connected to the SA (only one per SA10 or 4 per SA40) it only routes packets to the wireless LAN if the address has an entry. This means a first net access from the PC on the SA is needed to update the APs list (for example a ping www.breezecom.il) .

It is necessary to have the ESSID and hoping sequence parameters the same. Beside the LED indicators on the front of the SA or AP it may also be useful to look at the RXPacketsFromLan, TXPacketsToLan, RXPacketsFromWLAN and TXPacketsToWLAN counters. This is a very fast indicator if the PC really sends traffic and if the AP also knows that this traffic needs to go to the SA. In case of NovelNetware File Server, one likes to enable IPX.
In case the connection works basicly, the following steps can be implemented to improve quality. A first idea would be to look at the packets per frequency counters and RSSI[17] value. If the units location of the unit can not be improved, a different set of antennas with more directivity may help. The last but very complex method would be to adjust the MaxRetransmissionCounter and/or discardTimeout, which are fundamental 802.11 timers and may influence the overall performance for a certain network traffic type. During the project it was tested how far these values alter the performance.

[15]Station Adapter
[16]Access Point
[17]Radio Signal Strength Indicator

Chapter 2

Voice over IP

2.1 Introduction

Today, Voice over IP is very widely used, with network specialists it seems to be as equally important as the Internet boom to the general population. But what is the reason for this ? Why do the people just not start to simply use it ?
There are numerous problems, some of which are: no clear accepted standard for inter operability, no guarantees about overall quality accepted by the end user (including reliability, understandability, reachability from other telecommunication networks), existing networks can not provide needed QoS[1], address translation to connect to POTS[2] networks, billing problem and not lastly the security issue. Some of them are not real VoIP problems, as for example the billing does not affect the speech quality in any way. For this reason these problems are discussed in a later chapter 4 (page 42), where it is tried to name all the problems important for a service provider, but not directly related to VoIP (or WLL).
It is assumed, that only telephone conversation situations occur, excluding e.g. radio broadcasting or streaming audio of music clips. Distant learning classes, are named as a special case, without further suggestions toward the type of traffic, they produce.

2.2 About Speech

Before someone can start to think about how to transport voice in any form about any kind of network it is useful to become clear about the different speech patterns:

[1] Quality of Service
[2] Plain Old Telephone System

- Talkspurt;
- Pause;
- Doubletalk;
- Mutual Silence;
- Alternative Silence;
- Pause in isolation;
- Solitary talkspurt;
- Interruption;
- Speech after Interruption;
- Speech before Interruption.

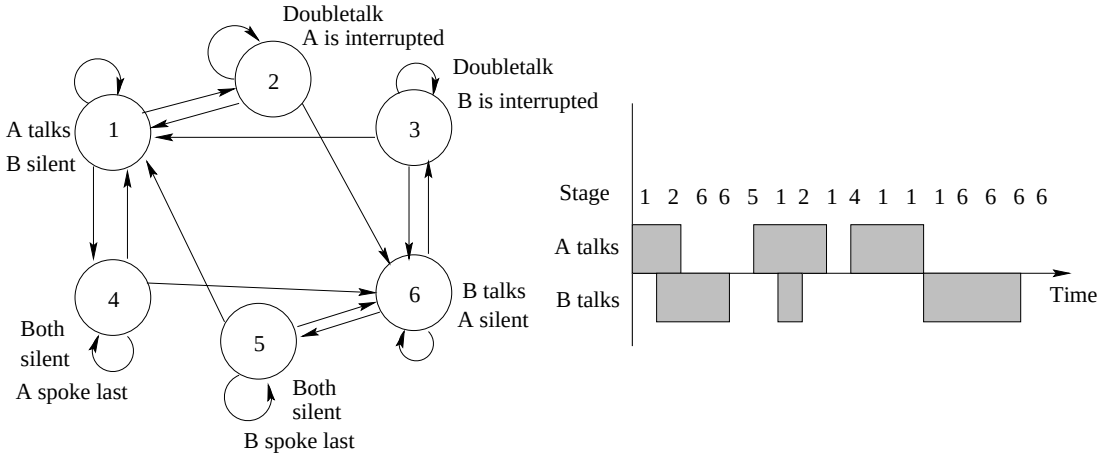

Figure 2.1: Markov 6 stages chain

Corresponding to the patterns generated data traffic can be defined. With a two person telephone conversation it is assumed person A and person B can either speak or stay silent, this corresponds to data traffic or no data traffic. It needs to be further clarified, that a certain mean value (e.g. volume value) of speech during a certain time period results in network packet with voice data. All voice events below this threshold will result in no network data packet send. Back to the speech patterns, stages can now be introduced, which can be seen as the different patterns. This results in the Brady Model, which is a 6 stage Markov Chain[3] describing a telephone conversation (see figure 2.1 and 2.2). Although this model is very accurate, the complexity is large. By concluding stage

[3]see also appendix B

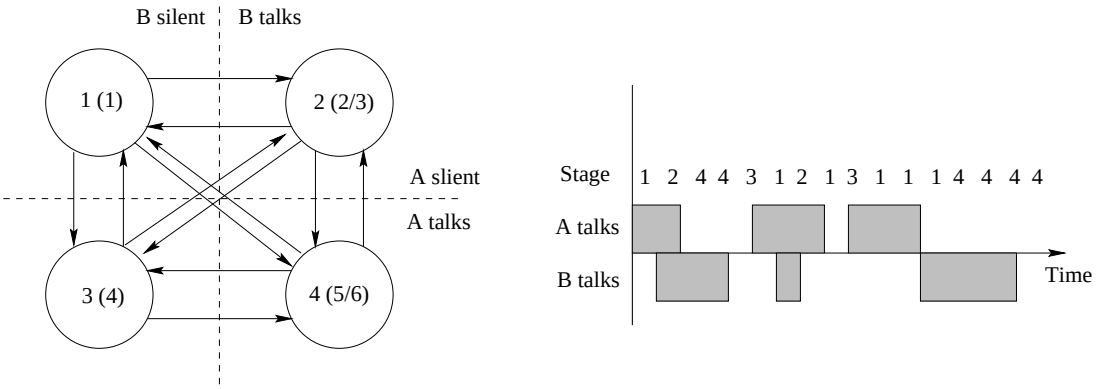

Figure 2.2: Simplified Markov 4 stages chain

2 and 3 (4 and 5) into a single stage, the model becomes easier, but not less accurate in terms of the actual transmission on the network. Using this model it is possible to understand the network usage caused by the voice conversation. Further on it becomes possible to develop a VoIP emulation tool, which will be described in the 7.1 section (page 58).

2.3 Parameters influencing the VoIP Quality

Introduction

In considering VoIP as a telephone replacement, one of the first questions will be, is the quality the same ? - Short answer can be either Yes or No, just depending on the case, in which the topic was discussed. The existing codecs together with the existing high bandwidth and redundant network equipment would make it possible to deliver the same service like the PSTN[4]. The caveat is, that this assumes, that the whole network uses this high bandwidth, the network is limited to a certain number of Hops[5]. Ideally speaking the mobile phone networks, like the GSM is nothing but a digital computer network, with an even smaller average bandwidth like the Internet backbones. The only, but big difference is, that the parameter of this network do not change (i.e. GSM is circuit switched), meaning:

1. Delay
2. Jitter
3. Bit Error Rate (BER)

[4]Public Switched Telephone Network
[5]stops with a routing decision of a device - which will increase the delay

4. Throughput

Once an IP network can provide this, VoIP will equal the PSTNs. (the way to achieve this is discussed in the chapter 4.1 (page 42).
In the following different parameters and their meaning for the VoIP quality are examined.

2.3.1 Delay

This is the most vital parameter, as a normal telephone network seldom has one way delays longer than 150ms. A survey[6] states that 400ms is the maximum possible for conversation. What happens then is the following. Person A says something, not sure if person B agrees. To get a positive feedback person A makes a break of normally approximately 1 second. During this time B would have thought about it and either give some kind of positive feedback or start to talk to explain his own opinion. In case of a long delay person B would hear already 400ms after about the break (Question for feedback) and will start to think about it, maybe 700ms later he decided to give his own opinion and starts to talk. At this time (400ms + 700ms = 1.1s) A is already talking again, because he believes B has no real opinion about it (maybe did not understand some points). 400ms later (1.5s after the beginning of As pause) the speech of B arrives at A, while A is talking himself. Irritated , maybe he will back off and a kind of random media access decision will start, depending on the nature of B and A either one of them will be talking afterwards.
This examples shows, why early VoIP applications (e.g. Netmeeting 2.1, Speak Freely) implemented a half duplex conversation only. By making the speaker aware that only one can talk at one time the behavior changes a bit allowing longer breaks, staying confident without positive feedback and structuring the speech to more clear questions. This kind of behavior can be observed on the CB[7] and in slightly less power at the Amateur Radio Bands, as well.

2.3.2 Jitter

This factor is in the PSTN, but can lead to sequencing in the VoIP. Jitter is the variation in time delay (e.g. the last packet had 30ms delay, while this has 40ms delay, hence the jitter is 10ms). The big problem, caused by jitter is either packet loss (highly increased BER) or permanent increased delay. The only cure for jitter is to implement a jitter buffer. Thus it is necessary to collect the network packet and normally keep them for a certain time. In case of variations of the

[6] Ericsson Technical Review
[7] Citizen Band, public radio band

delay, the time the buffer keeps them varies, too. This gives at the point after the jitter buffer an increased but fixed delay. The nice side effect is that if the packets arrive out of order, but still in the buffer delay it is possible to reorder them. In case of bad performance of current VoIP software in a local, high speed LAN the problem is mostly a big jitter buffer (normally necessary for WAN[8] connections).

2.3.3 BER

The BER is caused by transmission errors or packet loss. During a VoIP session in case of BER the decoder can only try to minimize the effect of the lose of data. Mostly comfort noise will be inserted, which sounds familiar to the human ear, but does not provide real information. The subjective opinion will be much better, than if silence was to be inserted. As the voice data is transmitted in 20ms frames (or less), the time without data is usually short, depending on the underlying transmission layer (see 2.5.3).

2.3.4 "Throughput"

This factor is included, because in the computer network world this is an important factor. The opinion is stated, that VoIP it has minor value. The reason for this opinion lies in the structure of VoIP communication. Mostly at the beginning the available bandwidth is discovered and a apropiate voice codec is chosen. This codec needs a certain bandwidth, which means even if the throughput is twice as big, the codec does not use more. As as the quality is depending on the codec the available throughput influences the quality only indirectly. Assuming a network will provide a minimum throughput to be able to use the certain codec chosen by the user, hence bigger throughput increases the network capacity (number of simultaneous VoIP conversations), but not the quality for the one conversation.

2.4 Measurement

2.4.1 Introduction

Referring to the quality influencing parameters described above, it seems easy to develop a objective measurement technique. But the reality shows, that the importance of the different parts contributing to the overall VoIP quality is not yet understood. For example a long delay with 0 jitter and small BER would be suitable. While the same delay with bigger BER would be unusable, small delay

[8] Wide Area Network

with the same bigger BER may be sufficient for a conversation. The thresholds and coefficients are not yet well understood .
Several subjective approaches have been made, which can be seen as enough in terms of comparison. However if policies and larger scale surveys want to be developed, an objective scaling needs to be developed. The next paragraphs introduce some of todays approaches.

2.4.2 Mean Opinion Score - a subjective approach

The opinion of many testers will equalize extreme opinions and be comparable with another test of different testers. In this approach a scale of 1=bad 2=poor 3=fair 4=good 5=excellent is given and each of the testers decides the quality of the given sample. Different techniques can be compared. It is also possible to compare e.g. different bit rate encoding schemes, but it is important to note that suitability for a special purpose depends not only on the quality, but also on the bandwidth and complexity.

2.4.3 Voice Simulator Tool

While trying to compare different queuing techniques and the influence of the delay on a telephone conversation a thesis had been carried out at the GTE Laboratories Incorporated developing a Voice Simulation tool (see [11]).
First an understanding of the telephone conversation had to be developed. With discovering that some words triggers reply (talkspurt) on the other side. Ideally a delayed trigger signal will output the reply with a delay too. Next step was to record a telephone conversation. Marking each channel with trigger and triggered marks. The two separated files were taken into 2way, the main simulation tool, which could be exchanged to simulate e.g. WLL behavior, other queuing techniques or certain behavior of the network. As output the delay of each trigger signal is given another tool incoperated the delayed triggered events into two output files. One how the conversation sounded from person A and one from side of person B. Using this method it was possible to simulate and generate samples for comparison from the same input conversation, using different network behaviors, by replacing the 2way program. The advantage is that the result, the output files can be publicized easily.

```
17:20:23.301683 147.252.133.185.1108 > 147.252.133.130.1720: S
5935863:5935863(0) win 8192 <mss 1456> (DF)
      > > Call initiation via H225 TCP port 1720 < <
17:20:23.301752 147.252.133.130.1720 > 147.252.133.185.1108: S
523628848:523628848(0) ack 5935864 win 32032 <mss 1456> (DF)
17:20:23.302740 147.252.133.185.1108 > 147.252.133.130.1720: . ack 1 win 8736
(DF)
17:20:23.308542 147.252.133.185.1108 > 147.252.133.130.1720: P 1:179(178) ack
1 win 8736 (DF)
17:20:23.308603 147.252.133.130.1720 > 147.252.133.185.1108: . ack 179 win
31854 (DF)
17:20:23.366681 147.252.133.130.1720 > 147.252.133.185.1108: P 1:5(4) ack 179
win 32032 (DF)
17:20:23.481414 147.252.133.130.3213 > 147.252.133.185.1090: FP
4175703441:4175703453(12) ack 5324543 win 32032 (DF)
      > > Signalling done via H.245 < <
17:20:23.503771 147.252.133.185.1108 > 147.252.133.130.1720: . ack 5 win 8732
(DF)
17:20:23.503838 147.252.133.130.1720 > 147.252.133.185.1108: P 5:249(244) ack
179 win 32032 (DF)
17:20:23.510392 147.252.133.185.1110 > 147.252.133.130.3217: S
5936072:5936072(0) win 8192 <mss 1456> (DF)
      > > Answere to H.245 openening of channel into other direction < <
17:20:23.510449 147.252.133.130.3217 > 147.252.133.185.1110: S
517494216:517494216(0) ack 5936073 win 32032 <mss 1456> (DF)
      > > (...) lines erased from exchange of capabilities < <
17:20:24.104607 147.252.133.130.3217 > 147.252.133.185.1110: P 113:139(26) ack
179 win 32032 (DF)
      > > start of RTP stream < <
17:20:24.174725 147.252.133.185.2326 > 147.252.133.130.5000: udp 252
17:20:24.204045 147.252.133.185.2326 > 147.252.133.130.5000: udp 252
17:20:24.234610 147.252.133.185.2326 > 147.252.133.130.5000: udp 252
17:20:24.263485 147.252.133.185.2326 > 147.252.133.130.5000: udp 252
17:20:24.294296 147.252.133.185.2326 > 147.252.133.130.5000: udp 252
   > > Each 20-30ms goes one 252 byte RTP packet with voice data out. < <
```

Figure 2.3: Traffic dump of a Netmeeting call.

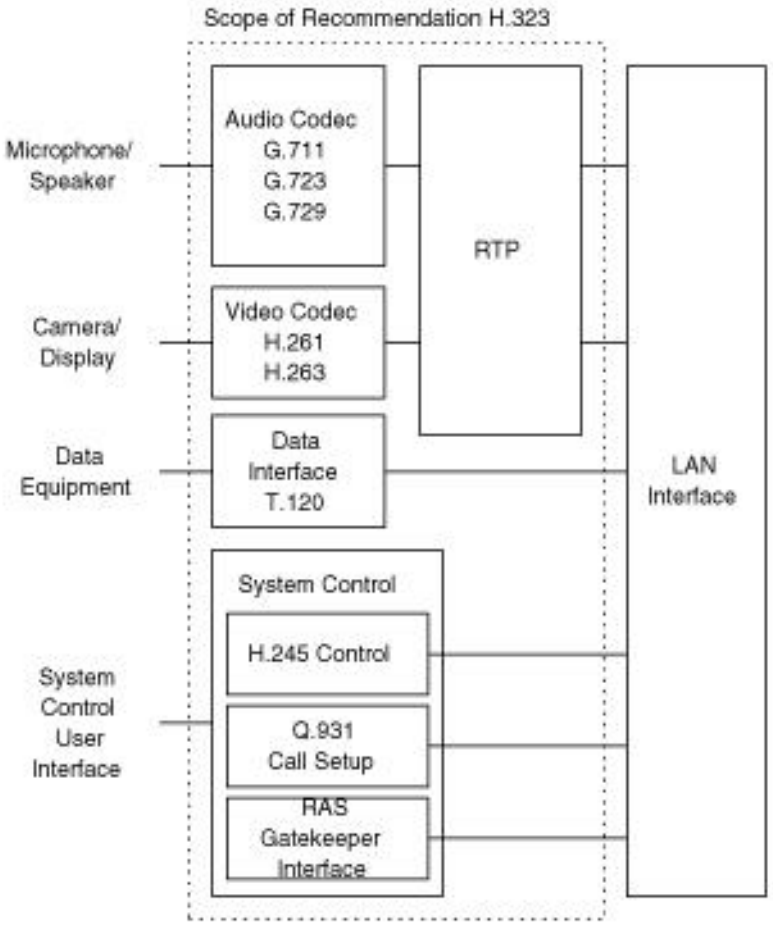

Figure 2.4: Overview about inter working of H.323 protocols (taken out of H323v2 draft)

2.5 H323

2.5.1 Introduction

Having common codecs, sufficient bandwidth and a minimal delay is still not enough for employing a successful VoIP system. Call control, resource management and transport of the voice data are parts of the H323 protocol suite. In the following section the main parts of the H323 suite, the control and the transport part are explained.

2.5.2 Control part of H.323

H.225

Call control and signaling is done by this standard. This includes synchronization of media format and capabilities, as well as a address service for reachability. A fast test if a client may be H.323 compliant is to do a telnet session to port 1720, which is the H.225 control port. Clients using the H.323 codecs (i.e. G.723), not using the same port scheme are not compliant.

H245

Handles especially the opening and closing of the media streams. Also indications during the stream (e.g. a bit rate change) is done in this standard.

2.5.3 Data part of H.323

H.261,H.263,G.711,G.722,G.728,G.723, G.729

Are the standards for the different media formats. G.723 is chosen as the default standard for a H323 terminal, meaning all H323 systems need to know at least G.723 for compliance (An interesting note is that the G.723 needs to be licensed). For a comparison of the different voice codecs (G - standards) see table 2.1.

Realtime Transport Protocol

Not directly described in the H.323, but used by the Media protocols. This in the IEEE RFC[10] 1889 described protocol and is suitable for transporting any kind of multimedia data. To explain why a special protocol is needed, and not just one of the TCP/IP suite can be used, I would like to suggest thinking about the nature

[9] Parts of the information were taken out of [2] and [3]

[10] Request for comments

Table 2.1: Comparison of G standards [9]

Standard	Bit rate (bit/sec)	Packet size (byte)	Description
G.711	64	310	3.1 kHz bandwidth
G.722	64		7 kHz
G.728	16		3.1kHz bandwidth
G.723	5.3	78	3.1kHz bandwidth
G.723.1	6.3	84	3.1kHz bandwidth
G.729	8		3.1kHz bandwidth used in Frame relay

of real time data, for example an audio stream. Basically the stream consists of 20ms pieces of data; how the speech needs to be formed. A conversation is based on playing these pieces continously and in both directions. Lets assume a piece (frame, slot) gets lost. The decoder gets after the last packet in sequence no new data. As the time definitely goes on there will be 20ms, the one from the lost packet, where the decoder does not know what kind of sound it shall play. For this something called comfort noise has been introduced, the human ear will be more accustomed to it, than to complete silence. Using this comfort noise the decoder can go on until 20ms later the next slot needs to be decoded. Again the decoder tries to get data from the network. The question is, which data would the decoder prefer: *The data from the previous slot (which is now filled with comfort noise) or the data of the next (now actual) slot ?*
- Less people answer the data from the previous slot. If you did, you have overseen the fact, that time can not be reversed. Also waiting until the next correct slot in sequence arrived (and then play on to the new slots) would mean increasing the delay and at worst having the remote station talking for 5 minutes more, after both parties had hung up.
The correct answer is the next (actual slot). Putting the answer into different words. For you it is more important to get the current data, than getting all data correctly. Mostly you would like to tell a router having troubles with the voice data packets to throw the old away and forward the new faster, instead of trying to deliver all data. At this point it is referred to section 1.5.1 (page 10) and section 2.7 (page 26).
The kind of protocol needed in the above paragraph is not available in the IP family. The protocol nearest to the desired properties is the UDP[11]. Which still does not provide timestamps, to determine if there maybe was silence between the

[11]Universal Datagram Protocol

two consecutive packets or sequence numbers to know about packet loss. Hence RTP has been developed. RTP also provides the possibility to give each media stream an ID. In this way it is possible, that one recipient gets a high quality media stream, which needs more bandwidth, while another gets a low quality media stream, which requires a limited bandwidth. The sender would encode media in high quality, sending it parted on two RTP streams. Stream A would have a unique media stream id and be enough to decode a low quality media stream. Stream B would also have an unique media stream id, but would have a reference to stream A as well. This stream consists of extra data making stream A a higher quality stream. As there is a timestamp and sequence number it is possible to join stream A and B into one media stream at the receiver side.

Realtime Transport Control Protocol

Given the example of above with the possibility of two different quality media stream, it will be easy to understand the usage of RTCP[12]. During the whole communication session the receiver is giving a feedback to the sender. This can be useful if a connection, which was a high quality one, becomes worse and on the way to the recipient of i.e. a high quality bit stream loses half of its packets. The network in between is obviously overloaded. If the sender keeps on sending a high bit rate bit stream the network will only become more overloaded - maybe having no chance to recover from the short burst of traffic. As the data is not arriving anyway, there is no point in continuing to send the high quality media stream. It would be better if the sender would send a low quality media stream, where extra data is missing, instead of sending a high quality bit stream where half of any data will be lost. Using the RTCP the receiver can inform the sender about its conditions and the number of packets received and missed. This allows the sender to adjust the quality, reducing the network load and maybe helping to solve a temporary overload. In the RTCP reports are also included which conversation partners are included in the broadcast enabling statistics about the audience to be kept.

2.5.4 Other information about the H.323

Gatekeeper/Gateway

These two terms seem to be equal, in fact the meaning is nearly the same. The gateway may be seen as a special kind of gatekeeper. While the gatekeeper is completely a H.323 unit, the gateway also connects the H.323 world to for example the PSTN. A scenario with a gatekeeper can be a high speed backbone

[12]Defined in the IEEE RFC 2205-2209

and a low speed branch of a local network. At the border between these two a H.323 gatekeeper can receive a high quality bit stream and generate a low quality (low bandwidth) bit stream for the local network. A gatekeeper can also be used to redistribute the data, while the main broadcast sender has only gatekeepers as recipients, the gatekeepers will have end users as recipients, hence the call connect and disconnect will be handled by the gatekeeper and the main station will have less work. A gatekeeper can be part of a firewall building a VPN[13] with other gatekeepers securing the traffic over the public network in between.

2.6 Session Initiation Protocol

2.6.1 Overview

The SIP protocol is developed by the IETF[14] with experiences of the SMTP[15] and HTTP[16] in mind. Main goal was to develop a light weight, scalable and easy to modify protocol, which still has all features of common protocol. As the name tells it this protocol is only meant for the initiation of a call, while the data transfer is also done using the RTP and RTCP protocols. Further a SDP protocol is developed for capability exchange and agreement of common features. However there is no minimal capabilities required nor a standardized way of setting up further additional streams (for example white board sharing or video). More over these features are understood as extra calls, which are set up and forgot about afterwards by the SIP server.

2.6.2 Comparison with H.323

These difference can be caused by the people developing the different standards. The H.323 is developed by the ITU, which background is the telecommunication circuit switched networks. In circuit switched networks a high synchronization and detailed switch of functions is necessary. The SIP is developed by the IETF, which has developed large parts of the Internet Protocols. The de central, maybe chaotic approach of the Internet is seen in these protocols. For example a HTTP message can be read and understood without by a human without knowing about the protocol itself (a ”GET 127.0.0.1/index.html” is clearly a request for a special document).
In H.323 it is tried to standardize all possible events using different headers and elements. SIP tries only to establish a common base, where additional events

[13]Virtual Private Network
[14]Internet Engineering Task Force
[15]Simple Mail Transfer Protocol
[16]Hyper Text Transfer Protocol

may been added.
Like described with with the additional features above a SIP server sets up a call and forget about it, allowing it to handle a larger amount of calls in the same time, while a H.323 Gatekeeper needs to pass along all H.245 messages during the established calls.
In SIP if a call needs to be forwarded the SIP server acts as a proxy calling the next known location of the user. H.323 needs for this procedure two protocols interacting in the right way. Further it is possible to do the same think in another way (opening a conference for three, where one will not answer, hence it will end up in a communication between two).
Beside the complexity in implementation the H.323 endpoints this introduces also complexity in firewalling the protocol. A firewall needs to understand all the involved protocols. In SIP only one request is sent, which firewall needs to understand. In case the request is extended by extra fields the firewall can either know the extension, pass it through as the basic connection is allowed or strip the extension with a notification to the sending part. As the whole protocol is like the http a plain text protocol content matching can be done by for example regular expressions using known http methods[17].

2.7 VoIP over WLL

After explaining above, that VoIP tries to transmit the data fast rather than complete, and explaining in the WLL chapter, that for decreasing the BER, the IEEE802.11 protocol uses retransmission on the data layer. One of the main questions in VoIP over WLL is, how far these two work contrary to each other. At the moment no surveys are known, which investigate this issue. It is understood as part of the project to find if the retransmission has a negative influence on the VoIP performance over WLL. A special test is described and performed in 8.3.

2.8 Examples of successful VoIP employment

2.8.1 As a cheap telephone network

After talking about the telephone conversation properties, examining the delay importance it is obvious that VoIP can be used as a telephone replacement. Advantages are named below and further one commercial solution is described, namely the Definity system of Lucent Technologies.

[17] see also [9]

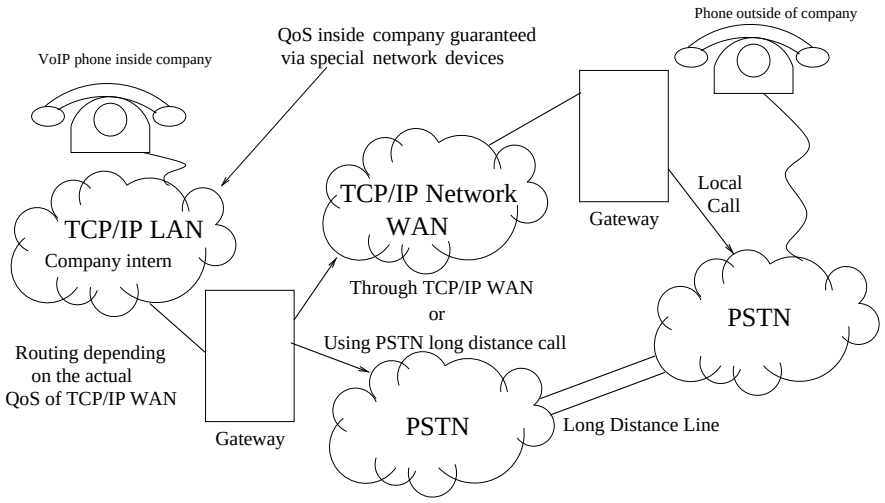

Figure 2.5: Example of professionell VoIP Gateway

- No double cabling as the computer network can be used for phone calls as well;
- One stop solution, no different contracts for phone and data traffic;
- as data traffic is cheaper, international VoIP calls are cheaper as well;
- much easier re rout-able in case of traveling business man, he can keep the same phone number;
- mostly easier to use, already existing communication solutions try to exploit the user interface comfort of the computer for the telephone, at VoIP this is guaranteed;
- short term solution for overcome availability problem exists.

The last point is probably the biggest fear for a business person. An important phone call and the quality is bad - the professional image is lost, or even worse a call has to be made and the phone is not available. To benefit from VoIP, but keep the reliability of the PSTN Lucents Definity system has a built in backup system. The system monitors the quality of the network before and during the calls. Depending on the measured values and the given importance of the call it decides to route the call over the data (IP) or the voice (PSTN) line (see figure 2.5). As most of the calls will be company internal, with less importance in quality a multi national operating company would be able to decrease costs and keep the professional outside image. Another advantage of the system is that PC work places without telephone lines would be able to get a extension number from the Definity server, without additional costs.

2.8.2 Full service Web page

Of course there are also situations, where VoIP is not used to replace the telephone network. As today the web side of a company is of great value and some decision will be made by looking into the knowledge base [18] of the companies web side. It could be useful and valuable if the customer could use the same place or address to get live support. No longer would a customer need to search for the companies local representatives phone number, a click at the call local support will redirect the VoIP call to the next (and working) support center. It would be also possible to reroute the call into the PSTN without need of VoIP equipment at each local branch.

2.8.3 Information management

Information and management of the same is vital today. It can be important for a business person to be reached at all costs in case of an important call. For e.g. this call would come from a certain person and not from the coworker it would be possible to distinguish if it is necessary to reroute a call to the home phone during the vacations. Todays phone systems are able to reroute calls, probably are also able to reroute deciding on the phone number, but less people know how to set this up using the 10+x buttons on the phone. One solution would be to extend the phone with a more comfortable user interface, another would be to interface the phone to the PC to use software such as a GUI[19]. If then the user wants e.g. important calls sent via voice mail to his current location. Or be able to listen to the message of a new incoming call, while being in conversation. The question is if interfacing the computer with the telephone line for call processing and re-formating the data again for sending it via the telephone network, could be easier done by staying in the computer network area. In this case not every computer would need a special ”forward-backward” conversion card, but only a software, sound card and network connection. The later two are available in all current PCs.

[18] modern term for the support section
[19] Graphical User Interface

Chapter 3

Network Management

3.1 Introduction

Every network needs to be managed once it has reached a certain size. Network management and its tools can make the life of a network administrator easier. It is very useful to look at the overview of the network software and study the details of the systems concurrently. The possibilities to remotely configure the units and obtain an abstract overview of the information (i.e. in a MIB-tree), like in graphs is also very useful. The network administrator soon becomes a network manager involved and concerned with all aspects of the system and not only with the pure functionality.
During the project it became clear, that network management can be useful to remotely influence the parameters of the test network network, run the tests and collect the values, without writing everything down by hand. From this collected data it is easy to prepare graphs and make comparisons. As there is no big difference in collecting 1 value or 10, values seeming to be unimportant can be collected and may be useful for validating purposes later on. There for this chapter gives an insight into the use of and reasons for network management on a larger scale.

3.2 Perspectives and Reasons

Like the use of a LAN, the management of it can also be seen from different perspectives, which are:

1. Physical e.g. location and structure;

2. Organizational e.g. dependency toward a certain department;

3. Functional e.g. importance of service;

4. Informational e.g. values, which can describe a status;

5. Security e.g. description of status.

These perspectives show the different reasons for using network management. Someone wants to have an overview of the available nodes, while someone else needs to constantly monitor the performance indicators of the network. Others may want to adjust the network behavior according to certain events and necessities. In order to deal with all these different perspectives and needs, it is necessary to create a network model. At present the OSI model is the only standard for network management models.

3.3 OSI Model

The OSI model best describes the network in its different subareas. Namely there are 4 different models in the OSI network model.

1. Organization Model;

2. Information Model;

3. Communication Model;

4. Functional Model.

3.3.1 Organizational Model

The Organizational Model describes the structure of the management system, wherever there are information collection units, which report to and are controlled by a higher network management system. It will also describe the structure of the management system if there are several equally ranked controllers, which do or do not exchange information about their status and actions. According to the organizational model a network can have a central notification or message collection point, which only has a monitoring character, while the units are controlled individually.

3.3.2 Informational Model

The Information Model is concerned about the way the information is structured and stored. It is possible to have a central database unit. Or, like at all SNMP

systems, one database for the description of the available informations (MIB[1]) and another one for the storing of the actual information from each node (MDB[2]). The information model ensures that the information is stored in a logical and self explanatory manner. This has led to the introduction of the ASN.1 [3] has been introduced.

3.3.3 Communicational Model

The Communication Model provides different ways to access the information. Mainly it is divided between a get (request) and set (response) relationship, or the advanced trap/notification relationship. At the first (get/set) it is needed that the management unit sends a query to the unit and retrieves the information in the response. At the second (trap/notification) the unit sends traps or notification to the configured trap servers. These servers store the information which then is available directly. It is also possible, that different kind of traps will be sent to different trap servers. This limits the network traffic to times when there are changes. In a system without trap servers someone needs to query all information each time via a get request.

3.3.4 Functional Model

The Functional Model can again be divided into subsections.

1. Configuration Management;
2. Fault Management;
3. Performance Management;
4. Security Management;
5. Accounting Management.

Configuration Management

Configuration management involves the remote configuration of these units. Parameters such as used ports, protocols or the information about the location of the unit can be established. However, more importantly, thresholds for trap signals (e.g. maximal packet loss) can be set up. A scenario, where the configuration system sets a threshold, which will produce a trap, which is received by the fault management is likely.

[1]Message Information Base
[2]Message Data Base
[3]Abstract Syntax Notation 1

Fault Management

The fault management mostly receives information about faults or critical values, then decides how to react to (mostly) automatically repair the problem (e.g. re routing the traffic or shutting down a secondary server to give more bandwidth to the important one). The fault management software can also put out a fault tracker note, which can be handled to the maintenance unit. The maintenance unit reports the result on the tracker note, suggests better solutions and closes the fault log. In this way the network manager has an overview of the health of the network and the frequent problems that arise. Together with the reports of the maintenance units he can decide to change the structure of the network to become more fault resistant.

Performance Management

Performance management like fault management gives information about the overall network, with forecasts on difficulties. Part of performance management nowadays is testing. The times when a network grew are over. Today it is vital to influence the structure from the beginning, and before introducing new elements to i.e. improve the performance, it is important to carry out regression (see 5.3 page 51) and reliability (see 5.3 page 51) tests. Results from these tests even can be used in performance management.

Security Management

Security management is not only the monitoring and preventing of manipulation by third party forces, but also the monitoring of the reliability or security that can be offered to a service. In many of todays businesses, the computer network is the most vital part of the company, not least in the financial services sector. Not only is a good network performance important, it is vital to have the service permanently available. Security management can implement last levels of ordered chaos for example re configurating the whole network to provide these vital services, even in times where everything is going wrong. The quality of security management today is highly dependent on the people planing and monitoring the network. As common ways of securing a network are established, it is important to note that not all concepts can be implemented everywhere. This is due to the network structure which is already in place. Hence specialists need to adapt the ideas toward the local network structure.

Accounting Management

Accounting management is probably the most by non computer specialist misused management, also probably the only seen by them. Here the costs of the network

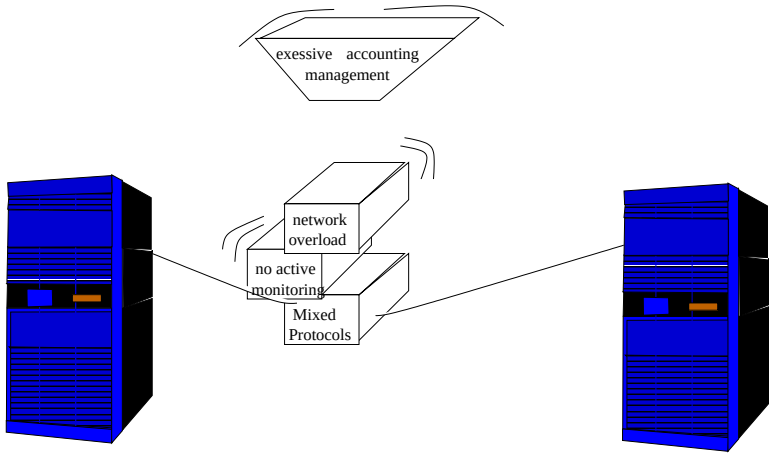

Figure 3.1: Everything together and extensive accounting management could bring the network down

are important. Mostly accounting management decides the question whenever take the leased fast, reliable line or the slow, faulty own installation. Outsiders mostly try to prioritize the accounting management, as this is the only one where money can actually be saved. Seeing only the costs the improved service is not seen, thus the accounting management is contradictional to the other managements. Of course it is possible to push the use of cheap lines, while keeping the other standards, but this is only possible to a certain degree. Especially if later on the need for higher quality arises it is not seen by everyone, that the accounting management is more for trying to keep the costs small, than for guaranteeing certain standards.

3.4 Simple Network Management Protocol

3.4.1 Introduction

This protocol inhabits most of the OSI network management model ideas, but was developed by the IETF[4]. As it is the first to give practical guides how to implement and use the network management it is widely adopted. There is another similar approach, the Bluetooth standard. Which emphasizes the management of all kinds of units. It is hoped that it will be implemented in every electronic device in the future.

3.5 Basic terms

Firstly of the terms are explained and later their usage is shown in a practical example.

3.5.1 Management Information Base

A MIB is needed to know which information is available and how to query it. The notation of the MIB database is given in the 1988 version of ASN.1 (X.200), which is part of the OSI standard. It is important to understand that a MIB is not the place where the data is stored, but the information about what data is available. Hence it is important to have a MIB file together with new developed products. By introducing the new MIB file into the MIB database of a management software, the software becomes capable of querying and viewing all of the available values.
The MIB can be seen as a tree, which has different branches. For example each company has their own sub branch under *.iso.org.dod.internet.private.enterprises* where it can organise the data available from its products[5]. Also most products understand the MIB objects of RFC[6] 1213, which allows querying of the main important features. In the case of a Breezecom wireless LAN unit, the RFC 1213 allows the statistics and status of the unit to be queried, but does not give access to the special wireless information. By introducing the Breezecom MIB into the MIB it is also possible to also get statistics about the packets per frequency and change the used hopping sequence.

[4]Internet Engineering Task Force
[5]A description how to register a own MIB can be found in the appendix A
[6]Request for comments

3.5.2 Management Data Base

This is the place where the actual information is stored. Each Software has its own format, but allows export into a well documented file format. Graphs and representation of the data are formed from the MDB. Most queries can be answered by a lookup in the MDB, but also by querying the actual device directly.

3.5.3 Agent and Manager

Agent is the software, which is built into the device to be monitored. The agent collects the information and delivers it via the network to the manager, which can be either another software in special hardware, or a software suite. If a hardware e.g. a Network Testing tool has a manager build in, it still needs an agent if it wants to distribute the results via SNMP.

3.5.4 Remote MONitoring MIB

This is a special MIB created for monitoring the network, while other MIBs are created for accessing special values. The RMON MIB it is tries to collect all the basic functions needed to manage a network. This enables the use of management software with nodes of different vendors, if all products understand the RMON MIBs. This standard is described in the RFC 1310.

3.5.5 Structure of Management Information

The in section 3.5.1 introduced tree view comes out of the SMI, which organizes all the different parts (RMON, SNMP, MIB-2, private MIBs) into a big object tree. The MIB of the SNMP can be found at *.iso.ord.dod.interntet.mgmt.mib-2*. The enterprise MIBs is in a different branch, while the RMON MIB is a sub branch of the SNMP MIB-2.

3.5.6 Telecommunication Management Network

TMN comes from the telecommunication area and is therefore well established. Originally the ITU[7] has incoperated the TMN into the OSI standard, but as the whole OSI standard is complex, difficult and expensive to implement today, TMN is also part of the widespread SNMP. TMN addresses the needs of the business, by introducing Quality, Service, Availability, Costs and other into the management unit. Hence it is important to note, that although the business depends on quality guarantees and billing systems, it is not naturally part of the IP[8]. The difficulties

[7]International Telecommunication Union
[8]Internet Protocol

in trying to introduce various services (other than the capacity dependent) into the IP and using TMN to manage them has yet to be overcome. Details are discussed in the next chapter (4).

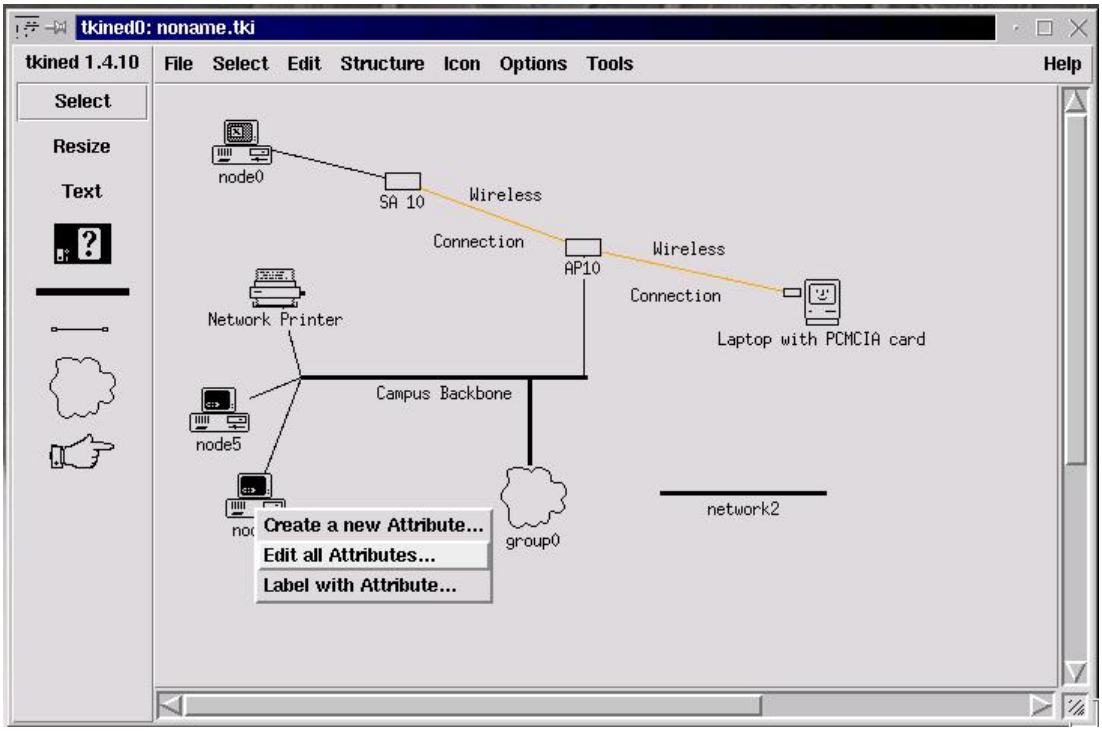

Figure 3.2: Scotty/Tkined main window

3.6 Scotty a network management software

3.6.1 About Scotty/Tkined

Scotty and Tkined, as well as TCL/TK is distributed under the GPL[9], which means it is free to use and modify by everybody, as long as no direct profit will be taken from it. It is possible to use the software to distribute together with your network equipment. One is not allowed to sell the software to others. However service in installing and maintaining the software installation can be billed. The idea behind this is to make software publicly available at no cost and to allow others to contribute in fixing bugs or enhancing it for special cases. As the maintainers use their free time to write this software it is usually better documented and more carefully written than commercial software, which needs to conform to

[9]Gnu Public License

certain time constraints and costs of production.
TCL[10] is a scripting language, which is enhanced by TK[11] to enable a GUI[12].
Scotty delivers an interface to the TNM[13] library, which gives access to the network services. Tkined[14] provides the user GUI to the underlying functions and makes the final tool look like a commercial programmed software.
Scotty can be obtained from:
`http://wwwsnmp.cs.utwente.nl/~schoenw/scotty/`
and is available in a Linux and Windows version.

3.6.2 Short explanation of the handling

The main window (see figure 3.2) gives an overview of the network. It is possible to place several nodes into a group and let them display as a cloud, like at the bottom of the diagram. Clicking at the cloud shows details of that group. Each node has attributes, like the name and address. There are two ways to start using scotty. Firstly by the TCP discover function, which draws a map with all discovered IP addresses, later these can be renamed to more meaningful mnemonics.
Secondly by drawing the map by hand and editing each node‘s address to its real address. In this way it is possible by i.e. the SNMP trouble tool to select a node and query the needed information.

[10] Tool Command Language
[11] Tool Kit
[12] Graphical User Interface
[13] Tcl extension for Network Management
[14] TK Interactive Network Editor

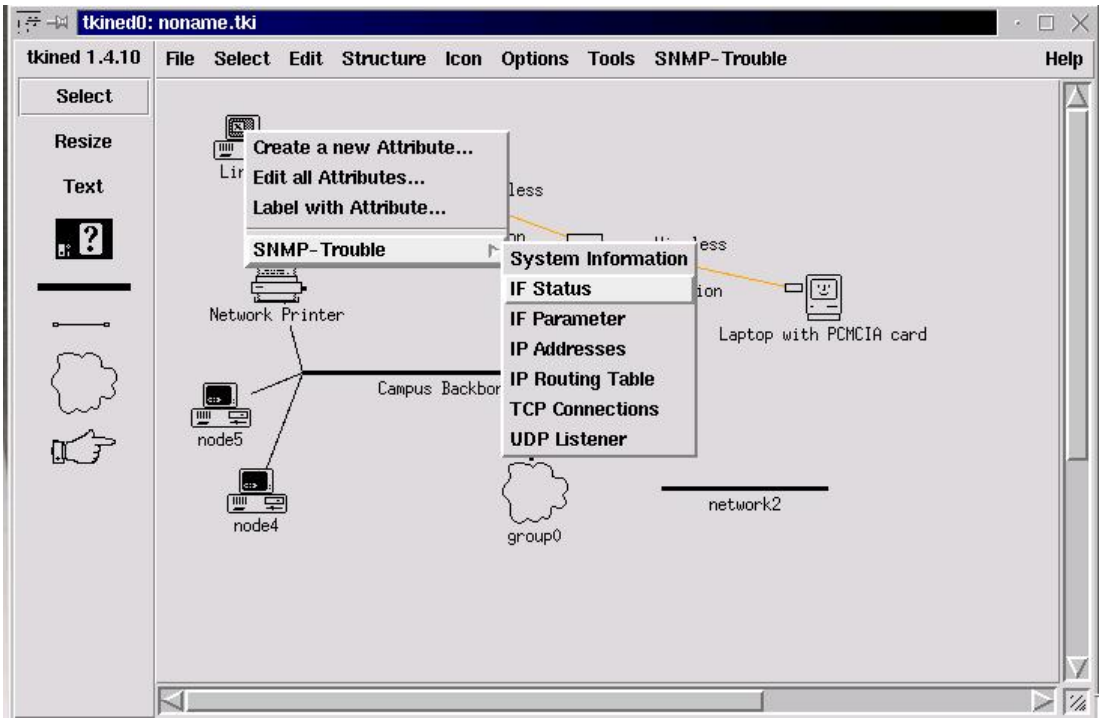

Figure 3.3: Extensions like SNMP trouble allow various ways of querying the nodes.

The result of the query in figure 3.3 is the following:

```
Interface status of Linux [147.252.133.130]:
ifIndex ifDescr            ifAdminStatus ifOperStatus (ifType)
    1   lo0                       up           up    (softwareLoopback)
    2   eth0                      up           up    (ethernet-csmacd)
    3   tunl0                   down         down    (other)
    4   vmnet1                  down         down    (other)
    5   vmnet0                  down         down    (other)
```

Another Tool is the MIB tree browser (see figure 3.4), which gives an overview of the different query-able functions. One can browse down the subtrees until the desired information is found, without knowing the exact name of it. For example it is desired to change the capacity of the wireless LAN, as the device is a special Breezecom equipment, the search is starting at the Breezecom node under the enterprises. Following the BreezecomPrvRev, Breezecomprivatemib a

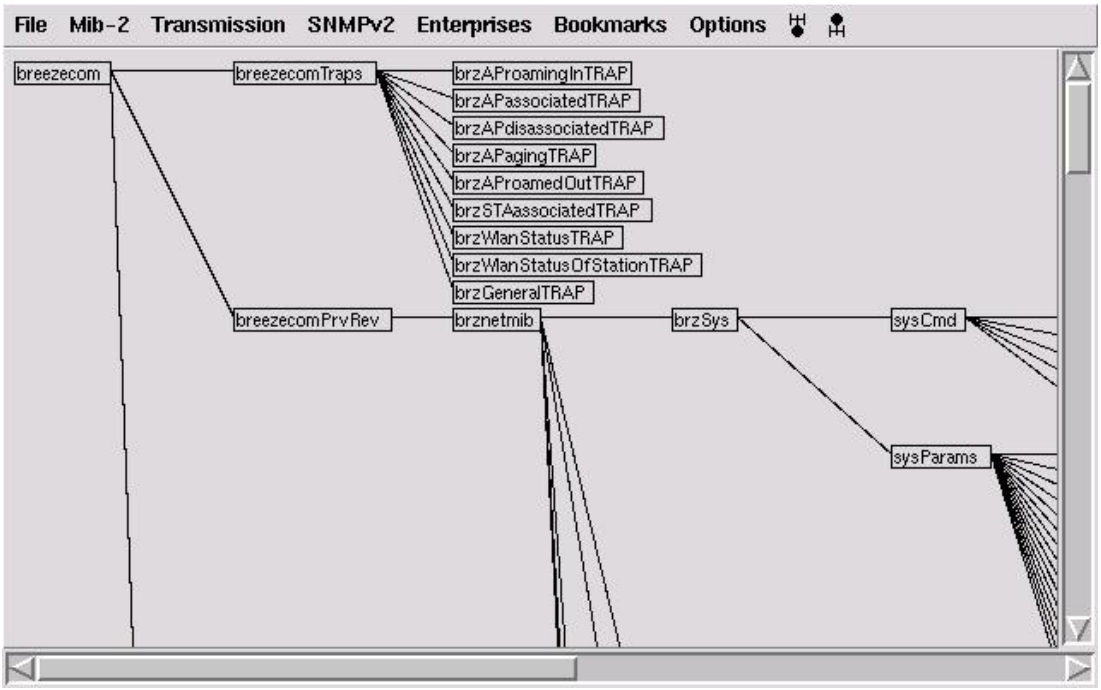

Figure 3.4: The MIB tree browser window

sub branch called brzWlan is found, which looks interesting. Finding that the brzWlanParams has an object called BrzWlanRate, which could be changed from 2MBit/s to 3MBit/s (see figure 3.5) gives the solution. If the targeted unit was selected before, the value can be changed within the MIB tree browser.

Also, as the source code is available, it is possible to put the most frequently needed parameters into a Tkined private menu, which has been done as a small part of the project for the Breezecom MIB (see figure 3.6).

3.7 Other useful SNMP related softwares

3.7.1 ucd-snmptools

This tool set can be used to query SNMP agents (e.g. *snmpwalk 147.252.133.149 public .iso.org.dod.internet.private.enterprises.breezecom.breezecomrvRev.brzWlan.brzAp.bssInfo.bssNumOfStations*) , but it also brings a agent with it. It runs on Windows and Linux and hence it it possible that e.g. the status of a Windows PC will be monitored using a network management software. As it is well documented it would be easy to extend the ucd MIB to be able to monitor special devices connected to the PC running the UCD-SNMP-Agent. The package can be obtained from:

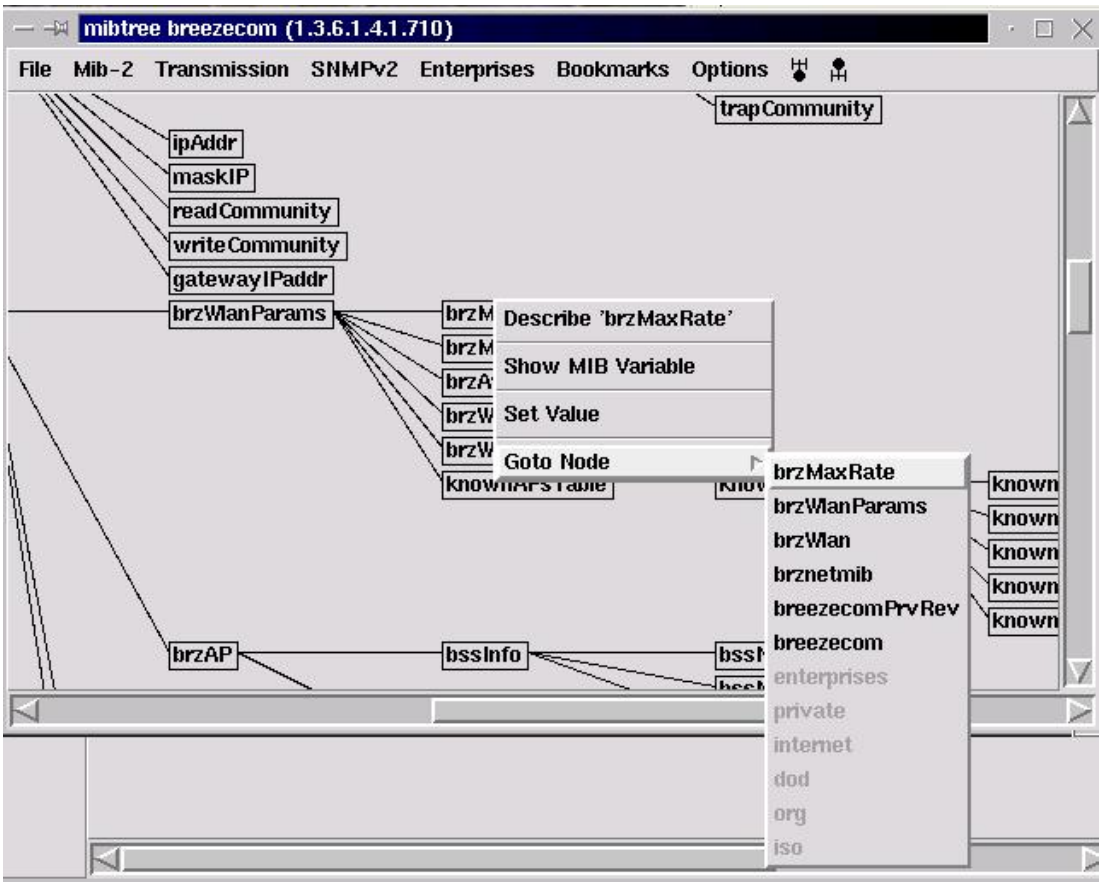

Figure 3.5: Changing a value out of the MIB tree browser.

`http://ucd-snmp.ucdavis.edu`

3.7.2 MRTG- Multi Router Traffic Grapher

MRTG is a Perl[15] script running preferably on a web server to produce graphs about the traffic usage of certain interfaces from certain SNMP devices. It is possible to query any device and any integer value of the network. The output graphs can be, daily, weekly, monthly and yearly views, with different HTML[16] pages for different MIB entities. As it is a Perl script it runs both under Unix and Windows. It can be obtained from:
`http://ee-staff.ethz.ch/~oetiker/webtools/mrtg`

[15]Practical Extraction and Report Language
[16]Hype Text Markup Language

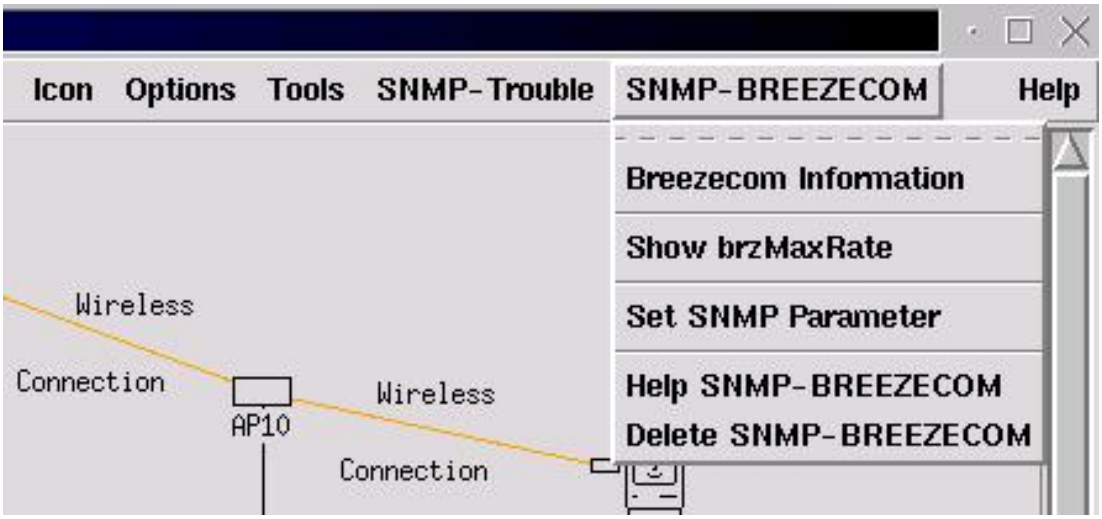

Figure 3.6: The during the project programmed private menu in Tkined

Chapter 4

VoIP over WLAN in the WLL

4.1 QoS

4.1.1 Introduction

Key to all real time applications are factors subsystems can count on. In first place it is not important, that something takes long, but it is important that the maximal time can be predicted. Given a controlling system monitoring a nuclear plant. In case of an abnormality it is important to react in a certain time, if the programmer knows about the time it takes to fulfill his command and how long it takes maximal to recall his subroutine in case of no success, he can decide how hard he can work against a situation without forcing the system into a problematic situation on the opposite side. Also it would be possible to assume maximal variance as there is a maximal time it takes to notice a variance. Although these examples are from the general real time applications. The QoS or in other words, the minimal bandwidth, maximal delay and maximal BER, is the same for real time voice data. If the VoIP software knows about these factors it can choose a apropiate codec and error control mechanisms. According to the way these limits will be kept there are three types of QoS.

Best effort

Although it is a QoS type, it is no real one. The limits can be seen as experience values, without any guarantee to hold them. The system tries to provide best service, but has nothing to prevent failing to do so.

Soft QoS

Here the limits are hold 90the limits will not been hold. Which again make it unusable for critical real time applications. However there are mechanism in this kind of QoS to nearly guarantee the staying in the limits.

Hard QoS

The limits are guaranteed to be hold. The makes special mechanism necessary and other convenient programming features impossible. In terms of operating system architecture this means for example, that a sampling routine needs to be done independently from the master CPU, because in case of a real time dependent interrupt everything else needs to be able to ignored. Hence waiting the sampling time to collect the stored value may be impossible. Today real time operating systems are mainly found on embed systems, were the possible waiting stages can be overseen easily. However approaches for BSD and Linux have been done, while a Windows NT based approach is not known yet.

4.1.2 QoS in the network

For QoS in the network environment this means, that either soft limits or embed devices like hubs and switches are necessary. However as VoIP telephone call is certainly not as important as the control of a nuclear plant, the existing soft QoS ideas are worth mentioning.

4.1.3 Techniques for maintaining a QoS

Passive Adapting

As todays network do not have a build in QoS function, the todays VoIP protocols does not rely on this. Instead they are adapting the quality and used bandwidth to the actual network situation using the RTCP protocol. See section 28 for more details.

Differented Services

A first step to be able to establish a QoS is to part the traffic into different traffic types. This is known as ”Differentiated Services” and allows for example uncritical traffic like emails to be delivered when the network load permits it, while a real time stream may get privileges or in case of a hard QoS capable network, may get a ”No resources available” message, in case the network can not provide the

requested QoS.
A first step to QoS is the payload type in the RTP protocol, further easy to implement steps would be to distinguish by the destination port. Later on it would be desired that all network traffic producing application sort their traffic themselves into the adequate group.

Traffic Shaping

Once all traffic is sorted into the different types, it becomes possible to monitor the traffic of each group and artifical delay one type of traffic, because it would otherwise take to much bandwidth. For example one high bandwidth traffic would be shaped by delaying its packet to fit into the maximal possible bandwidth threshold, as seen in figure 4.1. Important to note is, that in case both traffics have

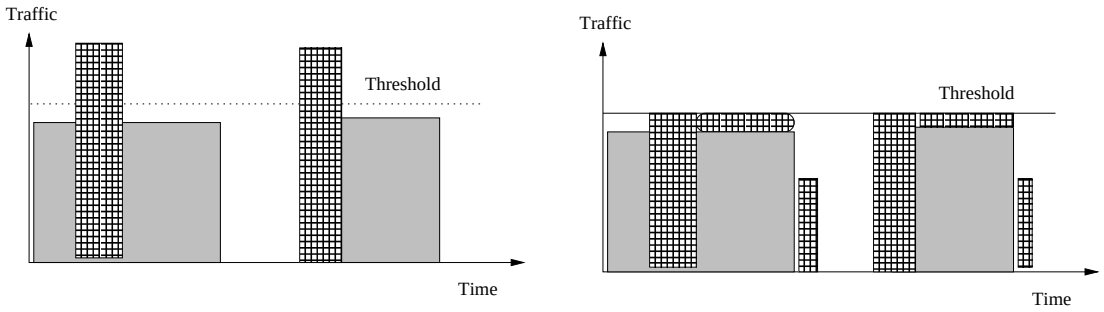

Figure 4.1: Shaping traffic above the maximal bandwidth

the same importance a different shaping is more effective, as otherwise the traffic with the lower maximal, but higher average bandwidth would have advantages against the traffic, which is bursty, with high amounts of data, but uses in the average a much lower bandwidth. The important detail herby is the amount of time the shaped traffic gets delayed. Incase of 4.1 the delay for the bursty traffic is high, while in 4.2 the delay of both is small.
More details can be found in [5].

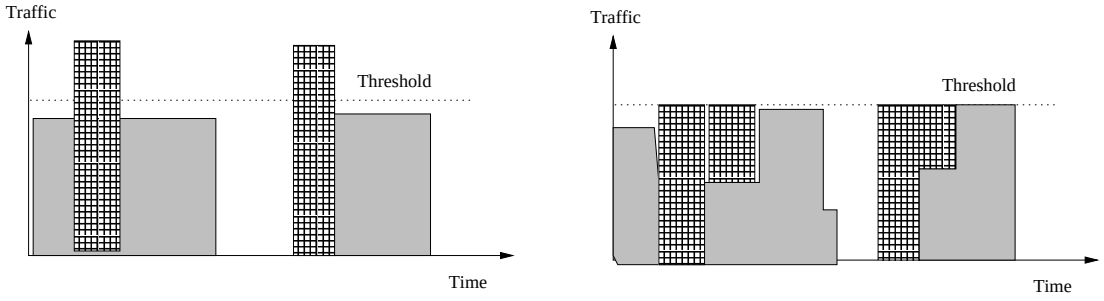

Figure 4.2: Shaping equal important traffic

Queueing in Wireless Networks

Similar to the traffic shaping is the queuing approach. While traffic shaping looks at the overall traffic from one type, queuing looks at the traffic of different stations. In wireline networks A model called Fluid Fair Queueing (FFQ) is tried approximated by different queuing algorithms. However, in wireless networks this model impracticable. As in a wireless channel bursty channel errors and location dependent channel errors exist, which bring disadvantages to only one bit stream, which either is transmitting during the error bursts or, whose location has more channel errors. For the queuing algorithm this means, that a previously neglected changing of scheduling priorities depending if there was a error burst becomes possible. Further it need to taken into account, that for some times not all stations be ready for scheduling, because of location dependent errors. If finally also the special situation, that in a wireless network cell not all stations hear each other, is recalled. It becomes clear that the MAC[1] can not be done by a distributed coordination function DCF), but needs a point coordinated function(PCF) from the access point. This also makes it necessary, that a cell structure is applied and neighboring cells use different logical channels. The basic idea of IEEE 802.11 (having a equal distributed media access method like in IEEE 802.3) needs to be reviewed. Current Voice networks, like the DECT and GSM network already have this point coordinated function with circuit like media access techniques. In the future the big question will be, are the advantages of a de central, independent of one station, working network are more, than the need for guaranteed QoS, which does need a centralized coordination (and calculation of actual QoS of the different streams and stations). For more information about the fair scheduling approach in wireless networks the reader is referred to [7].

QoS in IPv6

While the idea of marking different traffic types and priorities are not included in IPv4, the new generation IPv6 has these included. A priority field divides between 15 traffic types, with the devision of congestion controlled traffic and non congestion controlled traffic. Table **??** shows the types of congestion controlled traffic. This traffic may be delayed or thrown away in case of overload conditions. While non congestion controlled traffic are real time streams, like VoIP. By including this field into the header of the IP protocol it becomes for network devices much easier to do traffic shaping and prioritized delivery, as the payload does not need to be analyzed to guess how important the traffic may be.

[1] Media Access Coordination

802.1p

Like in IPv6 all packets are sorted into priority classes by applying a header extension at the IPv4 header. 802.1p compliant devices then are able to route traffic at prioritized routes. However as this is a pseudo standard implemented by several, but not all network device manufacturers it is not advisable to rely any new implementation on this extension.

4.2 Voice over Asynchronus Transfer Mode (ATM)

Another approach for maintaining a QoS in a wireless LAN would be to use Wireless ATM (WATM). As ATM is a circuit switched network protocol, the QoS is part of the protocol. However WATM meets the same difficulties described in queuing in wireless networks. The typical ATM features for rely on high bit rates with nearly no errors. Further the considered frequency bands will allow only cells of a few hundred meters, which would introduce an increased number of handoff processes, which again decreases the channel capacity.

4.3 Billing problem

Only connected to VoIP indirectly, but equal important when it comes to business application of VoIP over WLL is the billing problem. So far either time or volume (data amount) is the unit, which needs to be paid. The Internet backbone today, still like in the early time, is shared and mostly provided for free. For example at the border from the commercial Internet to the WIN[2], which all major German universities belong to, the commercial Internet Service Providers (ISPs) do not need to pay. Of course they are only able to route traffic to and from universities into this network. Once introduced different traffic types and hence types of expensive real time traffic it could happen that the commercial ISPs route the expensive traffic to the next WIN gateway instead of routing it the way with the least hops, but mainly through their own network. Further time critical traffic, which needs special networks will increase the price of network capacity, while people never producing these traffic may claim to be not willing to pay more for the same or even lower quality then before (delay, throughput). One idea would be to introduce PSTN like channels, which need to be paid for. This would also introduce a higher amount of administrative work as an IP packet may not travel each time the same route. Yet a billing concept, which adapts the nature of the de central organized Internet is needed. Or like in some countries a monthly submission fee instead of payment per volume needs to be introduced.

[2]Wissenschafts Informations Netz, Scientific Information Network

4.4 Roaming and Mobility

From the mobile phone network it is seen as natural, that all phones are reachable under the same phone number every where in the world. Further a conversation while sitting in the train and crossing the country does not need to be interrupted, because the mobile changes the association from one cell to another. Translated into Internet terms this means, that an IP address needs to be valid (and reachable) any where in the world. Further the routing table needs to be able to changed for a particular connection, even if the interface generally is still full functional.
Today Routing is done by subnets and central main routing servers. Once the computer discovered the IP address of the destination computer it sends the packet out on the default interface. If the packet reaches a node with several interfaces the packet will be routed on the one refering to this subnetwork or the default one. By that way the packet travels up to the default gateways (mostly in direction of WAN networks) until one node definitely knows where the destination address is located and routes the packet not to the default interface, but to the interface of that special subnet. This works well, because computer within the same subnet are located in the same network area (for example 147.252.132, 147.252.133 and 147.252.134 are the subnets of the DIT). But once a node is mobile and associated in an area of a different subnet (for example a laptop of the DIT is visiting a German university, which IP subnet is 194.25.12). A packet trying to reach this node (for example from the German university) will be routed up into the WAN, into the subnet of the DIT, where the information, that this node is out of house (or specific associated in Germany subnet 194.25.12) found. Hence the packet is send to the node via its home network. Desired would be now, for all further packets, that the IP address of the node is known to be in a different subnet and the packets routed directly to that subnet instead of routing it via the nodes home subnet. In other word this means, that routing by subnets is no longer possible, because all nodes may be out of house and a different routing needs to become possible, which would increase the routing table size significantly. However these feature is not implemented into the IPv4. The Mobile IPv4 and IPv6 do have these features, hence a wireless telephone network like IP network better uses IPv6 instead of IPv4. The mobility of keeping the connection even if the routing changes, is reached by the same feature, which allows the roaming. For information about Mobile IP see [1].

Part II

Tests

Chapter 5

General things about testing

5.1 Introduction

Reading about Network Testing brings fault location instantly to mind. Less often heard is the testing of a not yet bought system - the kind of testing used for making better decisions. Testing is hardly ever used on an already running system.
Inspite of this, network products are bought and afterwards it is found that there are problems. Sometimes a decision is even made based on the simple price and features of the marketing prospect. Employing testing techniques and a bit of structural planning would change the outcome quite immensely. Firstly, a list of employed services, used network protocols and also type of produced network traffic mix. Using these input parameters and asking the network device supplier for one test sample would allow to testing to see if the device can handle the traffic and also brings the desired improvement in bandwidth. This means not only the pure performance parameters, but also compatibility is tested. Keeping the test records allows later to predict the necessary improvements, while the network load increases. How to do this testing, what special test techniques can be found for VoIP will be the content of this chapter.

5.2 How to test

There are 3 main ways to perform tests:

1. Using a generator and measurement unit;
2. Monitoring the real network;
3. Analyzing the network traffic.

The second and third way implies an existing network, with the users producing traffic. These techniques can be used to permanently test and monitor the network status. Analyzing the traffic can help to produce the input for generating traffic and measuring new equipment, as well as finding network faults.
Monitoring can also be used as a final real live test of new equipment. The monitored values should either stay the same or improve after bringing in the new equipment.
Using a generator and measurement unit is the best way to test a new device before introducing it into the network. A testbed can be built, which can be reused for all new devices. These initial tests will produce an entry report helping later to determine faults. In this testbed it is important that the generator produces not only enough test traffic, but also the same kind of traffic load occurring in the real live network. Further it should be able to increase the load, emulating an increased number of users and application. As the packets generated by the generator are known, mostly the measurement unit is even in the same cover, measuring different values is much easier than at the monitor or analyzer. Also a generator does not need to be a special device, it can be as simple as a test script starting file transfers, controlling GUIs of programs and recording the response times.
Hence some monitoring tools mark (see figure 5.1) the traffic and by these marks one can to calculate e.g. delay of a certain type of traffic. However these increases, if not done properly, can cause network overhead overhead. Hence influencing the values.

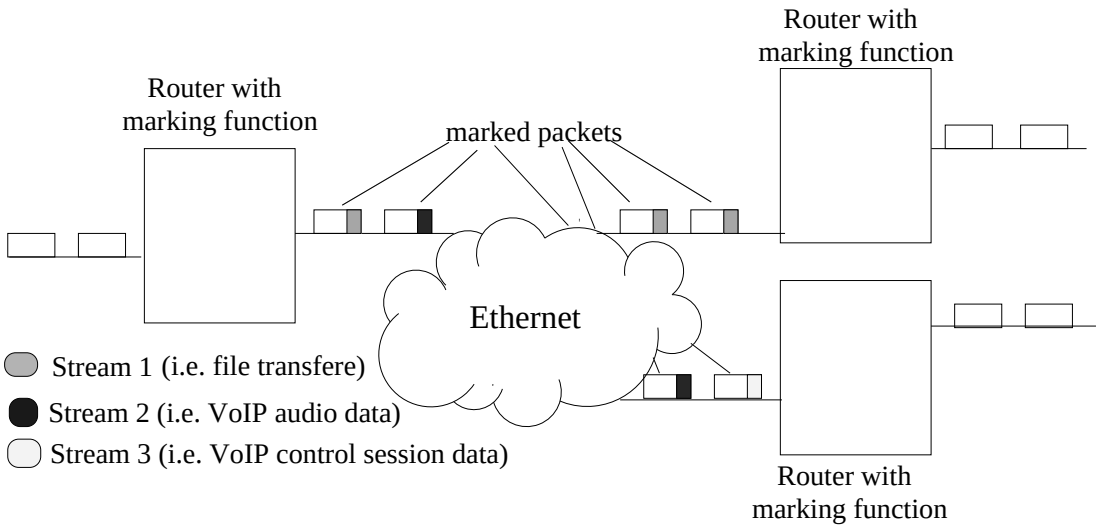

Figure 5.1: Traffic marking for monitoring purposes

5.3 What to test

First ten test objectives like named in [17] are described.

Application Response Time: This is probably the test most useful for the user. The test is performed using the end user application (e.g. Word to print a document, Netscape to download an internet page). And measuring the time it takes until the result is seen. All lower layers are put together into the application response time.
The number of users may be increased to emulate a higher load.

Application Feature/Functional: Test given product features, its output and behavior. During the functional test the load is increased. Sometimes it may occur, that for example the output of a heavy load indicator indicates a heavy load although the local threshold for a heavy load is higher. Hence common reactions to an indicated heavy load by this indicator will be different (i.e. less aggressive) than if another indicator notifies about a near breakdown of the network.

Regression: Compares the performance, reliability, and functionality of a new release to the current employed release. Also comparisons between different manufacturers could be possible. This measure ensures that no complications occur after change of a network device.

Throughput: Measures the value of bytes or packets per second. The difference in the application response time is that this tests only the network layer and not the processing time of a slow computer with a complex application.

Acceptance: During acceptance testing all different possible inputs will be performed, the network load will be increased until near breakdown and the in this test found thresholds will be used later for alarm indicators. This test can be seen as the final proof of functionality before going into real life.

Configuration Sizing: Different configurations are tried and e.g. the application response time or throughput is used to determine the best configuration. Doing this before employing the device in the real network helps to avoid down times and complaints.

Reliability: The device under test is run with a normal network load for a longer period of time. This increased uptime may lead to a failure, which won t be noticed even with increased load. Typical test duration may be 24 to 72 hours.

Product Evaluation: Not really a test, but an important concern. The input parameters of the other tests are influenced by the used subsystems and

technology. E.g. introducing HUBs using IPX, may be perfect for connecting a printer or file server to the network, but if user PCs with Internet facilities wanted to be connected to the network problems may occur. In this case the product features (and maybe price) were perfect, while the technology caused problems later on.

Capacity Planing: Like the acceptance objective, this tries to determine excessive capacity and plan in advance. If not, during acceptance testing discovered a special test may be performed, increasing the load until a breakdown to determine the maximal capacity.

Bottleneck Identification and Problem Isolation: A test objective with not only one (maybe new) device in mind, but the whole network. Hence the test report can be compared to the other device reports and problem areas could be marked. In case of faults these areas may be examined closely.

More about concrete tests to perform in section 5.5. First standards, which test may be based on, are described.

5.4 Standards

5.4.1 RFC 2544 Benchmark Methodology for Network Interconnect Devices

This RFC defines tests that may be used to describe the performance characteristic of a network interconnecting device. It includes detailed descriptions of the test set up to be used, frame formats and types, calculation of packet loss rate and delay. Further features included, like broadcast, routing updates, multiple ports and system recovery. In the appendix reference values are given.
For the scope of this project the delay and packet loss definitions are used, which partly also explained in RFC1242 (Benchmarking Terminology for Network Interconnect Devices). Furthermore the idea of building a test setup without influences from outside, was approved by this document.
The whole document can be found on the accompanying CD-ROM.

5.4.2 P 861

This is an ITU standard, which is developed to measure the subjective quality of voice band codecs. An algorithm called PSQM[1] is developed, which transfers the speech signal out of the normal physical domain into an internal psychoacoustic

[1]Perceptual Speech Quality Measurement

domain. This transfer is done by applying the psychoacoustic model (like also used in the MP3 compression), time-frequency mapping, frequency warping, intensity warping, asymmetric masking, cognitive model. Finally the speech signal distortion is measured in frames and a result is given in a PSQM value, which is also set into relation of the common MOS value. As the system can be connected to ATM, IP and any kind of voice transmitting system it is suitable for measuring VoIP over WLL as well.

5.5 Known common tests

PING: For a network generally one test is using the PING command to find out if the destination is reachable and the round trip delay. The default method of Ping is to wait until one packet returns and then send the new test packet. However there is a option to continously send packets, which allow to do a round trip measurement under heavy load.

TCPDUMP: This command is both used for analytical and monitoring purpose. A test via for example a application software is done and the network traffic is monitored via tcpdump. Later during emulation of network traffic via a test tool a tcpdump of the emulated traffic can be compared to the real monitored traffic.

NetPerf or a simple FTP file transfer: Target of this test is to measure the throughput, by transmitting large amount of data.

Qualitative Test Conversation: In case of VoIP testing, of course, a conversation using common VoIP software is another test.

Chapter 6

Approach to develop a test plan

6.1 Introduction

After outlining the various tests and test objectives. Now it is described how a test plan can be developed.

6.2 Test to perform

First some tests are chosen, which are performed nearly everywhere. These are common tests, which values may be useful later on. They are also seizing the environment or may discover some interesting values. Depending on these tests it may be possible to develop further more specific tests.

Qualitative Quality test As the overall objective is to learn about VoIP over WLL, one of the basic tests is to actually run a VoIP conversation over the WLL system. Doing this gives a feeling of the subjective quality and maybe let me later order values to subjective qualities. This test can be seen as a kind of application response time test, because the whole underlying architecture including the voice encoding is tested.

Field strength test While doing the quality test the field strength and location will be noted. This can bring some information about the range, multi path and general operation.

Throughput Although it is not important for VoIP, it may be good to have these results later and use them as an argument to prove the conclusion.

Breezecom Build In Site Survey As this is a provided test, it is interesting to see if it can give enough information. And hence further tests would

not be needed. However the problem is that this test is only built into the Breezecom equipment.

6.3 Values to be tested

Another approach to determine, which value shall be monitored, while changing the environment parameters. The idea could be to discover indicators for certain situations, to be able to establish thresholds, or connect the subjective good quality to a machine measurable scale.

Number of simultaneous VoIP sessions: To have indicator for the capacity.

Distance: To get an idea about the coverage.

Delay: A vital value for a VoIP conversation.

Packet Loss/BER: Together with the delay maybe an objective indicator if it is possible to have a VoIP conversation.

Jitter: Connected with the delay as it influences the quality.

6.4 Parameters to be tested

This approach tries to figure out to what extent a certain parameter influences the situation. Basicly the parameter will be changed and the results monitored. Depending on the result a further test maybe be carried out with another change in the parameter.

packet size: To bring the Quality into the tests. Different voice codecs produce packets of different sizes.

Mobility: Just to see whether this parameter influences the quality in almost stationary mode, drastically.

Dwell Time: The idea is to calculate the duration/length of a data frame packet and ensure that the dwell time is bigger. If it is smaller it is believed the performance will decrease.

Power level: To simulate more distance and worse conditions.

RTS Threshold: As this counter decides if a RTS/CTS handshake is needed or if the packet will be sent directly. This may allow to adapt better to the VoIP requirement to either send through fast or forget about it. However this may also increase the packet loss drastically.

Max. Number of retransmissions: Again try to limit the "TCP" effect, because RTP (UDP) packets are not retransmitted like TCP. Maybe this could be a key to improve the VoIP performance significantly.

(Antennas:) One can notice that changing the antenna system would influence the quality as well. However it is assumed that the influence of the distance, power level and antenna system are very similar. Hence testing different antennas would not bring more information into the VoIP over WLL test. Antenna diversity, range and receiving test are widely done in other areas and the results can be taken without further study [1].

6.5 Question to be answered

Another totally different approach is to develop questions out of the theoretical knowledge and try to answer these by theory or by developing special tests.

Retransmission influence toward VoIP: From theory it is known that VoIP needs to have as little delay as possible. Also the jitter needs to be minimal. Again the packets need to be either transmitted quickly and in order rather than completely. A late packet stopping more packets from being transmitted will cause more problems than a packet lost during the transmission. Hence one question is if manipulating the maximal number of retransmission and RTS threshold would optimize the VoIP performance. Another question is, how far the throughput, general delay and maybe TCP (e.g. telnet session) performance will be decreased.

Capacity: There are two kinds of capacity

1. The number of people able to carry out VoIP conversations over one WLL link;
2. The number of stations able to carry out VoIP conversations in the WLL system.

This leads to the question whether the RTS/CTS mechanisms decreases the bandwidth in the case of several VoIP conversations.

Small packets high administrative overhead: As each packet will be routed separately, one idea is that a high number of small packets will cause more problems than the same amount of data packed into less, but larger packets. Especially at WLL equipment, where a RTS/CTS cycle needs to be done. It is interesting to see whether increased quality (packet size) in a VoIP conversation will cause no other disadvantages.

[1] see [10]

Influence of mixing traffic: In case of e.g. a wireless bridge, it is likely that a VoIP conversation and data traffic will occur at the same time. As the VoIP conversation uses UDP packets and so far no priority system has been introduced the question is: Is the quality the same if two VoIP conversations take place or if one VoIP conversation and one data transmission takes place.

Chapter 7

The test plan

7.1 A special test software

7.1.1 Introduction

After defining the test outline it was searched for programs to measure the desired values. Beside throughput and round-trip delay measurement programs no usable software. The commercial tools were hardware based, which limits their flexibility to certain packet sizes and frame rates, or did not provide downloadable evaluation versions. Hence it was decided to write a special VoIP performance measurement tool (shortly called VoIPperf).
Doing this allowed also to integrate the tests and output the results in the way, desired. More over it became possible to run more than one VoIP session from one PC, emulating increased capacity.

7.1.2 Test Software Features

Send-Silent Timer Matrix: During a telephone conversation mostly only one person is talking, while the other listens, this fact is exploited by switched circuit systems which allow other telephone conversations to be transmitted during the silent times. By this method it is possible to have nearly 180% capacity on one line. As the VoIP programs also have silent period detection, hence only transmit, if real speech data is given it would be possible for the system under test to recover during the silent periods. Further it could be possible to reuse the free bandwidth in the silent times and hence have more than theoretical capacity of VoIP conversations over the system. None of the given tools implemented this function.

My program takes transition probabilities (e.g. if speaker A stops talking or if speaker B interrupts speaker A - both talking temporally at the same time), which had been found by a field survey of about 2 hours of phone conversations. It is also possible to determine the duration of the test conversation, allowing long term and short term tests.

Time-Synchronization: The well known PING command measures the round trip delay, which differs from the one way delay, which is important for the VoIP conversations. Measuring a one way delay requires both clocks to be synchronized, which is more complex than average testing. My software synchronizes the clocks at the beginning while measuring 20 times the round trip delay (like requested in the RFC2544) assuming that the half of the average round trip delay is the momentary average one way delay. The required routing update frame is already done by the set up of the control session. After the synchronization a actual time together with the assumed average one way delay is sent to the server. When measuring the delay both programs calculate the absolute delay by taking the clock difference into account. As the program is intended for use in the LAN environment an accuracy of 5ms can be assumed. However tests have shown that the accuracy is under 1ms.

Delay: For measuring the delay the software adds to each packet a timestamp consisting of two long int variables (second and nanoseconds after 1 June 1970). Directly after the return of the receive function another timestamp from the local clock is taken. Together with the adjustment value from, calculated during the time synchronization, the one way delay can be calculated.

Jitter: Each time the old delay is saved and after arrival of the next packet the jitter is calculated.

$$Jitter = abs(Delay_{oldpacket} - Delay_{newpacket})$$

Bit Error Rate: At the beginning of the test a random sequence, according to the desired packet size, is created. This sequence is transmitted together with the sent silent timer matrix. Hence both sides know the correct bit sequence and the Bit Error Rate can be calculated by comparing each bit of the packets.

Packet Loss: A sequence number from 1-100 is used, which is counts one up each time a packet is send. The receiver saves the old value and compares if the new value is the old value plus 1 (or old value minus 99 in case of a 100 to 1 transition).

CPU load: During the development phase the output of the program was a summary of the test. The maximal, minimal and average delay and jitter and the Bit Error Rate, as well as the total lost packets were output. However at the point where several instances of the program are run at the same time thoughts about to minimize the CPU load are made. The output were changed to writing each delay and timestamp into a file and calculating the average and other values later by an external program. For a comparison of the work need to be done by the software with the work need to be done by a VoIP software, see table 7.1. This comparison and a CPU load monitoring made it clear that the CPU load will not influence the tests. However a precariously limitation of 8 simultaneous connections were made.

20ms pause between each packet: Unlike other test tools, which send a continuous stream or wait until the system has processed the previous test packet. My software emulated the behavior of a VoIP system. If the software is in the sending phase it sends each 20ms a packet out. This value is derived from the 20ms frames used by many audio recorders and codecs. A sample of captured Netmeeting 3.00 traffic shows (see figure 2.3, that Netmeeting outputs each 30ms a packet, sometimes even faster as it also outputs RTCP and control session packets.

Table 7.1: Comparison of work to be done by VoIP software and the test program

VoIP software (e.g. Netmeeting)	My Software (VoIPperf)
gather information from sound card	
encode data (silent detection, coding)	
copy encoded data to buffer	copy random data to buffer
calculate timestamp	take time from clock
copy timestamp to buffer	copy timestamp to buffer
hand buffer over to network layer	hand buffer to network layer
receive packet	receive packet
read packets timestamp	get time from clock
sort into jitter buffer	calculate BER
take out of jitter buffer	write to file
decode data	
send information to sound card	
Further:	
Calculate RTCP reports	
Handle e.g. video stream or shared white board	

7.2 Chosen tests

Three major test sequences have been selected.

Qualitative Quality Test For seizing the general impression. During this test the field strength, location, subjective quality level (1-5) and remarks were recorded.

Quantitative First Test As shown in figure 7.1 shown, a test script (bash shell script) is run. This automation makes it possible to gather a large number of information and keep them for later use. All data is kept in a different subdirectories after a certain naming scheme.
During each test run either the parameters are changed (e.g. packet size or output power level) or the number of clients is increased.

Finding Answers This sequence was finalized after the first test series had been run. The reason for this sequence is to test certain matters. The test includes:

- Change of RTS Threshold;
- Change of Maximal Number of Retransmissions;
- Do a longterm test;
- Do a test with half packet size.

7.3 Test Instructions

1. (a) Set new location
   (b) Record signal strength
   (c) Do a VoIP conversation
   (d) Record results (subjection quality impression, remarks)
2. (a) Set distance
   (b) Start script, fill out test description form
   (c) Control result for very obvious problems
   (d) Change distance rerun test script
3. (a) Set distance and produce additional not VoIP network traffic
   (b) Start script, fill out test description form
   (c) Control result for very obvious problems
   (d) Change distance rerun test script

4. (a) Change max retransmission number
   (b) Run test script
5. (a) Change RTS threshold
   (b) Run test script

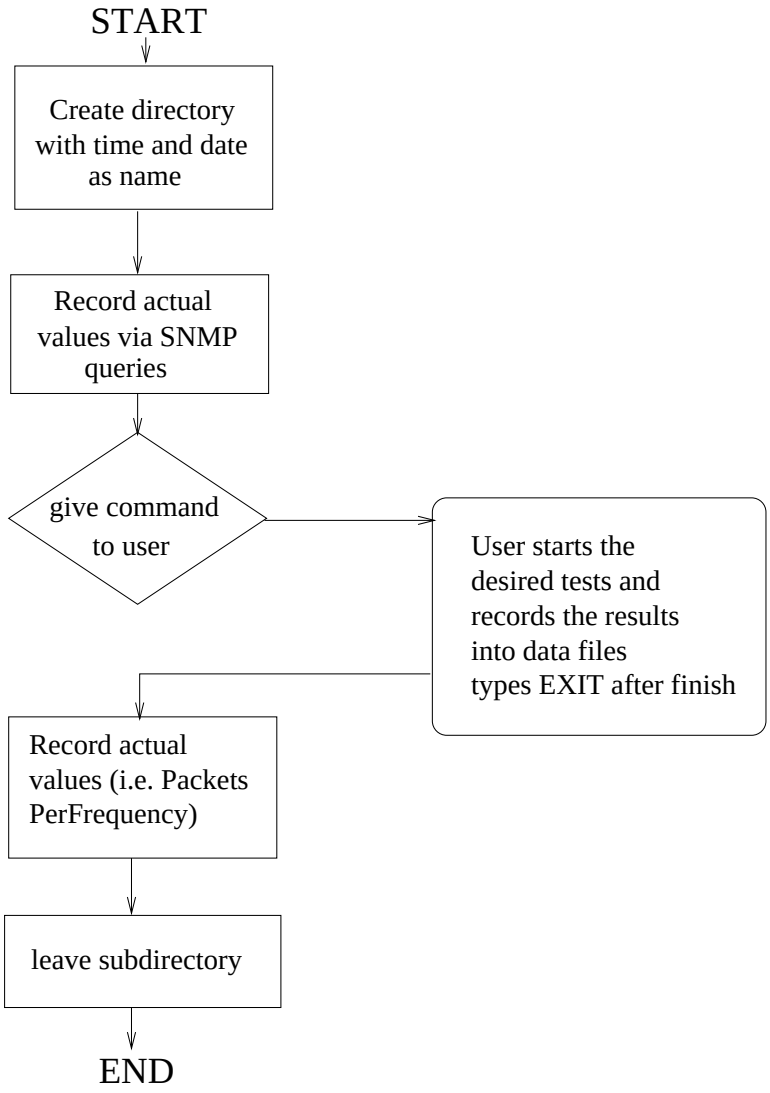

Figure 7.1: Flowchart of the used testscript

Part III

Results and Conclusion

Chapter 8

Test Series

8.1 Qualitative Tests

8.1.1 Objective Description

One Laptop with the PCMCIA Card, Netmeeting 2.11 and a PC with OpenAm[1] or Voxilla VoIP software. The Laptop moved on a trolley through floor 4 and parts of floor 3 of the DIT Kevin Street building (see figure 8.1 for a map). The field strength was measured by the Breezecom software and the answering machine was called. The 30 second speech quality was observed. As the Answering machine needs to have the speech in 8kHz 8 Bit ADPCM samples, the basic quality was less then the original recording. (Later a test with the Phonejack and the same OpenAM recording showed, that the quality heard in a telephone was good quality).

8.1.2 Result

The range is very limited, which means only half way down floor 4 (toward staff canteen), all way down the floor in direction of the new building,

8.1.3 Conclusion

As long as there was a connection the quality was good, however there were times without a connection. This is caused by the association process, which seems to have a limit of around -72 dBm threshold and will deassociate at about -80 dBm. As the main result it can be seen that this system is only for one room use only and each room should have its own Access Point.

[1] Open Answering Machine

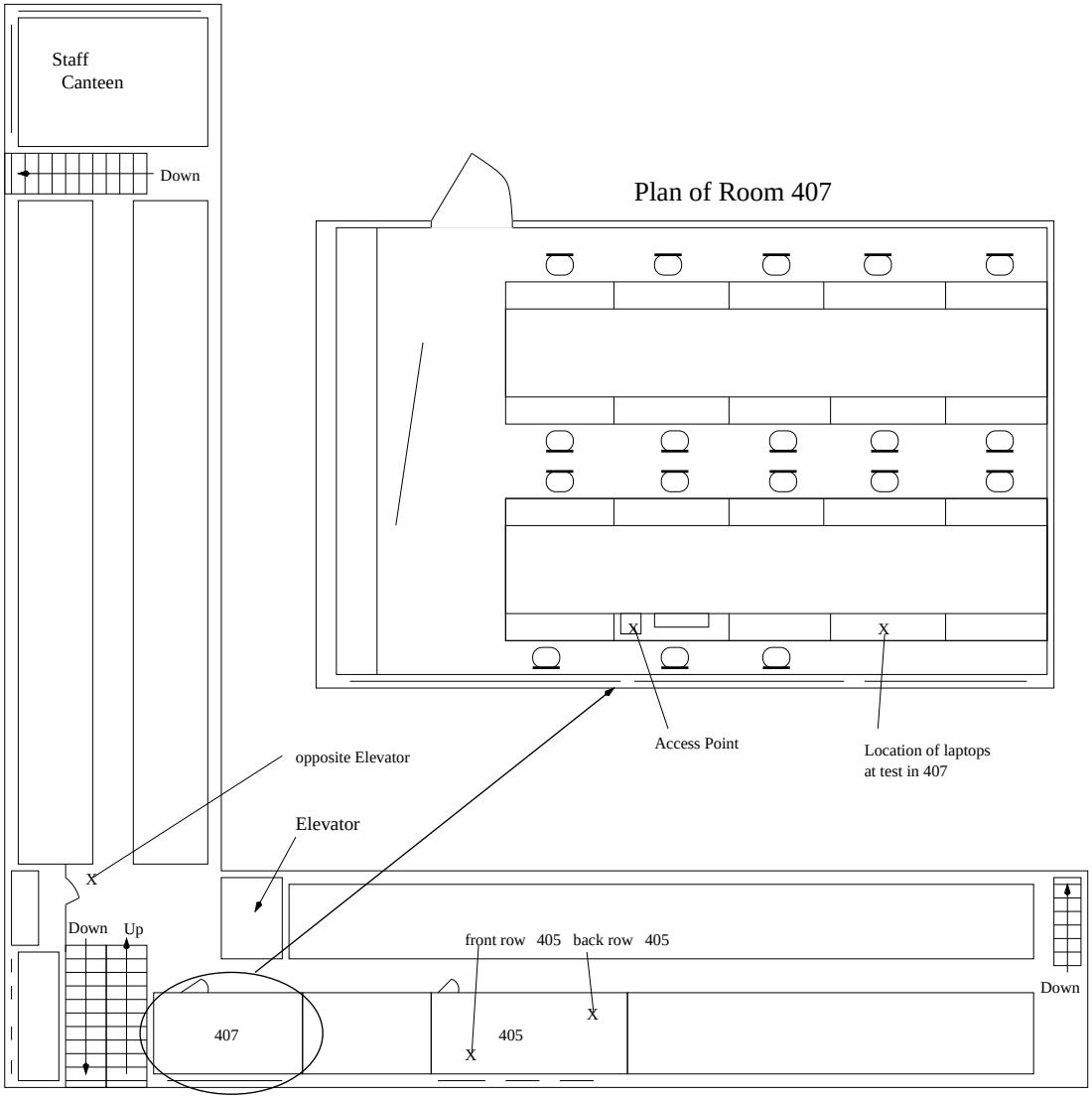

Figure 8.1: Map of floor 4 and room 407 of DIT Kevin Street

8.2 First Software Tests

8.2.1 Objective Description

The test software (VoIPperf) were run on a Linux PC and Laptop. The location of the Access Point was on top of the PC (marked in the room plan 407), not on the shelf or a special location, but directly connected to the PC via a special crossed cable (no other network traffic then the test traffic).
The testscript recorded via SNMP first the actual access point values (RSSI value to station, RTSThreshold..) and counters. Then the test software were run. The recorded values were stored into a file, during the first tests this were only the delays without the timestamps, after the second test series also the timestamp.
The laptop was moved out of the room 407, along the floor in direction of the new building. As the connection still was -70 dBm at room 405 it was gone into room 405, where the connection went down to -75 dBm. In the last row the connection was about -80dBm.
Tests in the third floor showed that there was a connection at one corner of the stairs and still half way down to second floor, but if there needs to be a reassociation process, because of lost connection), the station would not reassoziate unless it was gone back to the third floor corner of the stairs.
Two further tests outside of the building with the Access Point not moved showed that there is a quite good (-70dBm) connection again on the parking place.
After change of location of the Access Point to directly to the window, this time the whole IPX network traffic was transmitted. Going to the park next to the building the real distance with a direct line of sight was tested. The Connection was -76 dBm at about 200m distance, but still with a clear line of sight.

8.2.2 Result

The high decrease of field strength as soon as the room is left (-40dBm down to -65 dBm) and the complicated reassociation process, where the station needs to not only go back to the point of last association, but far more until a good reception. Shows that the system is clearly developed for one room only, which is not a negative thing, if known. The test and a round trip delay measurement, showed that the delay with long distance (far side of wall) is 2 to 3 times higher, than in the same room. First idea could be that the wave needs to travel farer, but of course the speed of the radio wave and the distance difference should give no notable time difference at all. As it was nearly exact 2 and 4 times faster the increased delay is probably caused by the retransmission of packets. During the tests on floor 4 the delay was either around 10ms or 20ms, which could be seen as no or one retransmission, while the delays in the park were 20ms or 60ms, which can be seen as one or two retransmissions. That there is 60ms instead of 40ms

is explained with the fact, that all the IPX[2] traffic was also transmitted, which is quite a lot as in the whole DIT servers from all its institutes can be seen and used. For the TCP/IP traffic the Breezecom units can determine if the traffic is for the remote station (needs to be transmitted) or if it can be omitted, hence the wireless bandwidth is used effectively. However this is not possible for the IPX traffic.

8.2.3 Conclusion

As a definite, not VoIP related, result it can be seen, that on a WLL system only traffic understandable by the units should be used. As then the mechanism of deciding if the traffic is for the station or not is possible. Imagine that two station would be associated and both station would need to get the whole IPX traffic (about 1Mbit/s bandwidth), would mean the system is overloaded only by IPX traffic without any useful application running.
The test in the park and along the corridors showed also, that the attenuation through walls, probably the then needed longer way through reflection and influence of multi path transmission, is much higher than on the direct way. This clearly makes the system only usable for mobile users in the same room. If two office rooms should be connected it is possible to find a good location inside the second room and use it, but with the PCMCIA card in a laptop two rooms are no good idea.
The software tests have so far given no significant results, like the near region test there were peaks and streams without any high delay.

8.3 Parameter Tests

8.3.1 Objective Description

As the objective was to determine the influence of the MaxRetransmissions parameter and the change of RTSThreshold. This value was changed and tests with one client over 5 minutes and 4 clients over 1 minute was done. The location was:

- 407 near by the base station (-40dBm)
- opposite the elevator in floor 4 (-65dBm)
- back row of room 405 (-79dBm)

[2]Internet Packet eXchange a protocol developed by Novell and mostly used for File and Print server, no real routing capabilities

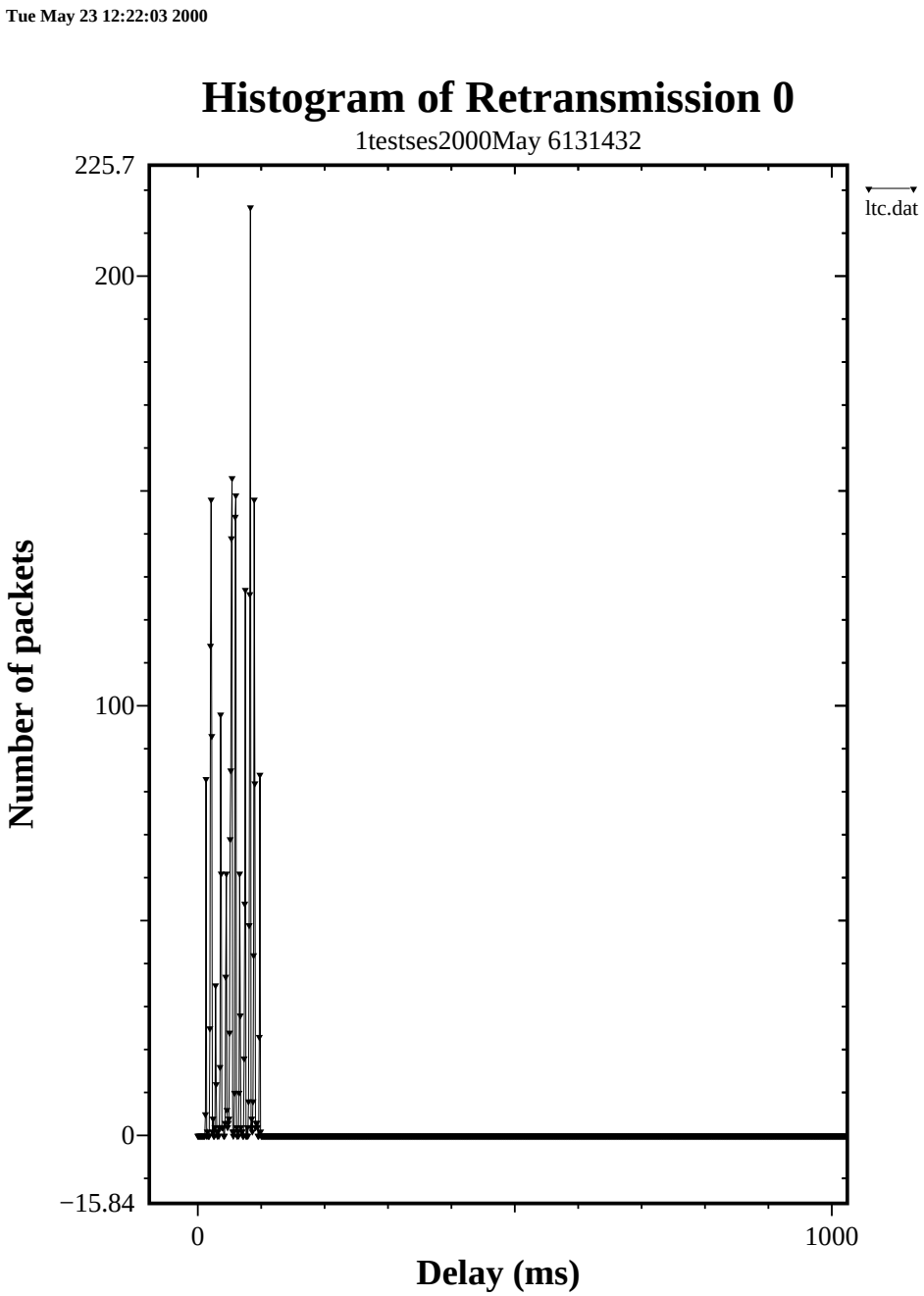

Figure 8.2: Plot of parameter MaxNumRetransmission set to 0

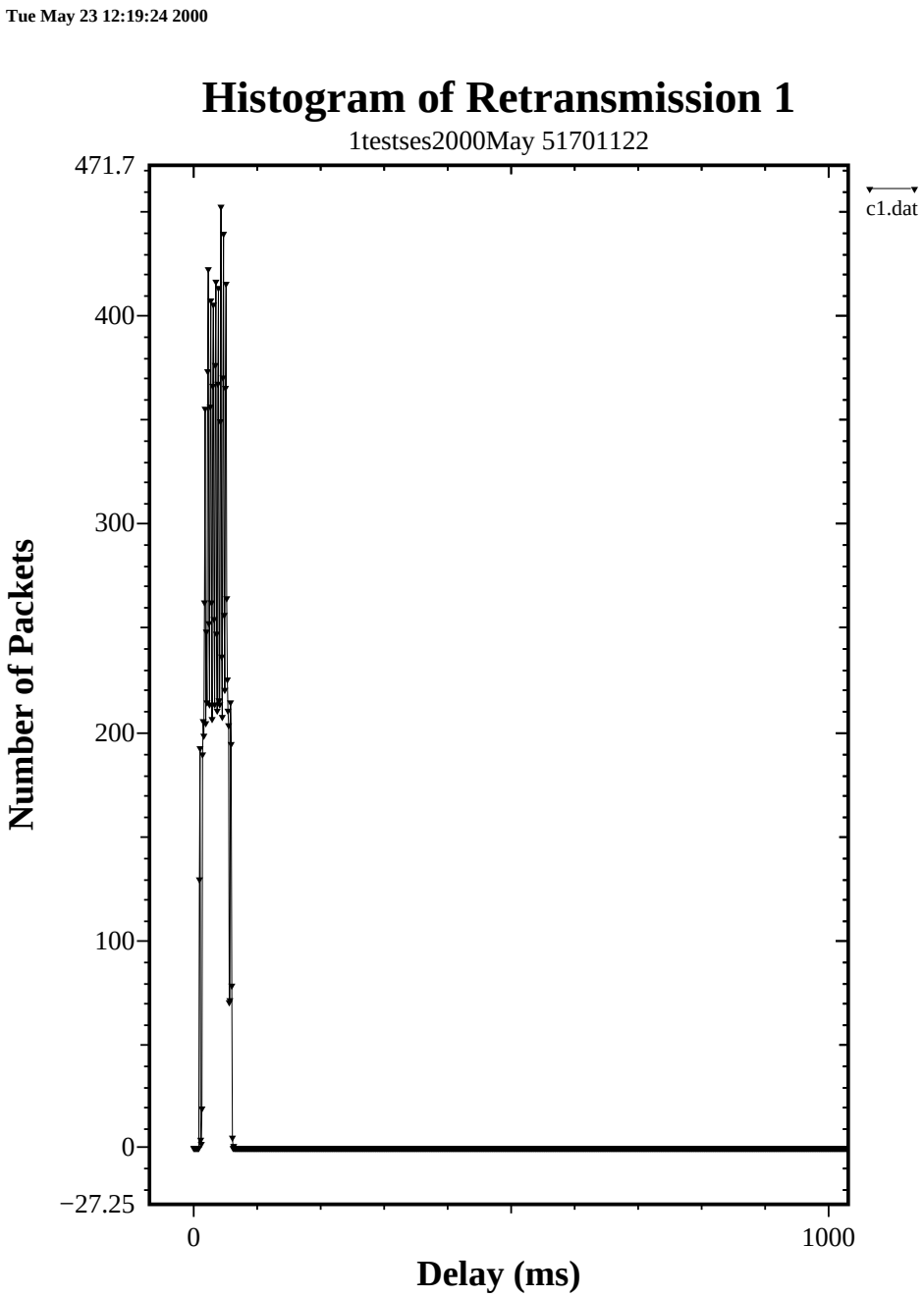

Figure 8.3: Plot of parameter MaxNumRetransmission set to 1

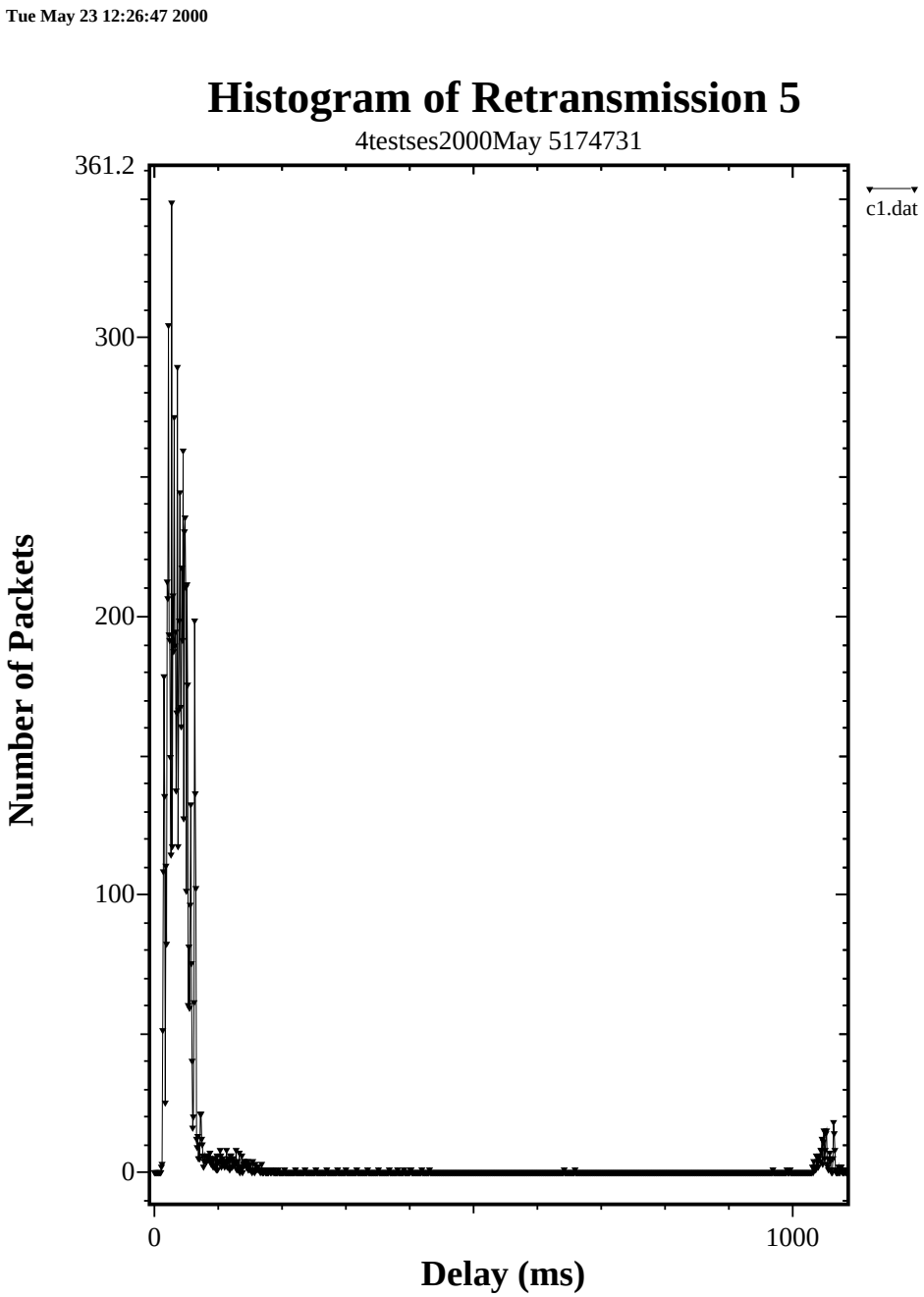

Figure 8.4: Plot of parameter MaxNumRetransmission set to 5

8.3.2 Result

As seen in figures 8.2,8.3 and 8.4 , a histogram of the delay against the number of received packets with that delay, the influence of the retransmission counter is high. While the default value of maximal 1 retransmission gave the best results - the highest number of low delay packet with no high delay packets at all. The retransmission value of 0 showed that there is a packet loss and retransmission is necessary. A TCP connection (telnet/ssh) with retransmission set to 0 in the back row of 405 (-79dBm) was not possible, because TCP assumes no high packet loss rate, hence it has a long timeout timer, which then retransmittes the packet and starts again for a long time. The retransmission of the IEEE 802.11 has a much smaller timer and uses the RTS/CTS with error correction. However after moving back into a good reception area (room 407) the TCP connection recovered and was usable again.
For the changed RTS threshold the same observations were made like at retransmission set to 0. Maybe a slightly worse condition, as already at opposite the elevator it was hard to use the TCP connection. However it is believed, that the conditions were a bit better at the retransmission test, because at least both station new that there will be a transmission at the given time (via the RTS/CTS handshake). Without a RTS/CTS handshake the receiving station needs to receive and decode the packets correctly at the first try.

8.3.3 Conclusion

These two mechanisms, although they are implemented as adjustable parameters are best set to the default value of maximal 1 retransmission and 120byte RTS threshold. In a fixed direct link it may be useful to change the values to a higher number of retransmissions in the case the link is really bad. Or to a higher RTS value in case the link is very good.

8.4 Comprehensive Quality Capacity Coverage Tests

8.4.1 Objective Description

This test was done with the Access Point under the table and the receiving laptop on the table or a bit farer away (see figure **??**. Using the Breezecom field strength meter the field strength was set to different values (10 dBm steps) and 2, 4 and 8 clients were started to do a capacity test. Each run was repeated with different packet sizes to emulate different quality bit streams. The decreasing field strength

was reached by shading the access point with a metallic plate and moving the receiving antennas.

8.4.2 Result

Although this was the most comprehensive test the objective to become a clear result about Capacity, Coverage and Quality was not reached. As the main reason it can be seen, that there is an increasing delay by the test time, which cause is not known yet. This delay make the results not trustable. However the direction, can be seen. There are always bit streams with only a low delay, while other bit streams have some or a large number of peaks.
The result graphs showed a interesting minimum at -55dBm, which was verified partly by repeating this test several days later. It is not clear what this minimum is caused by, but as the other uncertainty, the steady increasing delay is still in the test. Further conclusion can be made after understanding the steady increasing delay and repeating the tests.

8.4.3 Conclusion

For the capacity of the WLL system it can be predicted, that for more then one VoIP conversation that some conversations work well, while others in the same time have problems. This is derived out of the observation that the number of peaks after -47dBm increase significantly. Verifying tests have been done and are described in the next section.
For the quality this is not a big influence, especially as a high quality VoIP channel can be reached with 56kBit/s, which is low compared to the measured net bandwidth of 1.5MBit/s. The limitation hereby is more the administrative work and maybe the buffer sizes of the wireless units, which no information are given about in the technical specifications.

8.5 Verifying with VoIP Software Tests

8.5.1 Objective Description

Objective was to verify some results of the comprehensive test and to also learn about the behavior if two stations were associated to one access point. For the test setup see figure 8.5.
One Netmeeting running laptop connected to a Voxilla running PC. the laptop had the PCMCIA card, while the PC was directly connected to the access point. A second laptop with the station adapter was doing the tests using the test software like in the comprehensive test. The number of clients and packet size were

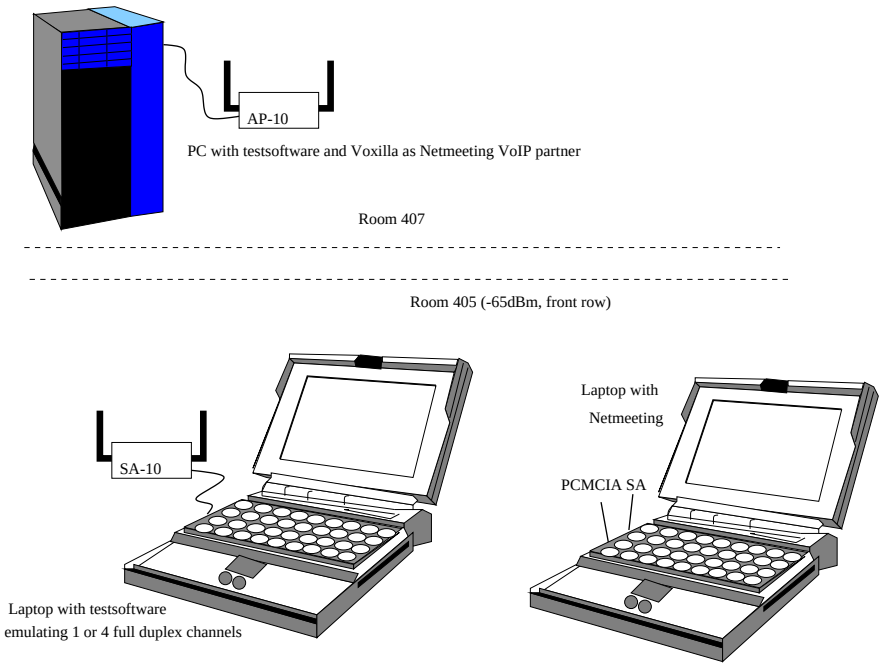

Figure 8.5: Setup of simultaneous VoIP and Software test

changed and all the time it was tried to do simultaneously a VoIP conversation.During all tests both laptops were nearby each other and the clients were emulating full duplex VoIP channels.

8.5.2 Result

Further a test back in room 407 showed that the last missing voice channel from the access point to the laptop was due to a software problem, it can be assumed that two full duplex 84 byte packet size channels work well.

8.5.3 Conclusion

During the tests the phone rang, but no voice connection was made, because of the different protocols. The initial control session is done via TCP to port 1720, after this the data (voice) is send via RTP (UDP) to port 5000, which is a insecure connection. As the packet size of Netmeeting was 84 byte and the emulation software used 258 byte packet size (RTS threshold 120 byte at that time) the RTP packets of Netmeeting were send without a RTC/CTS handshake, hence easier got lost. The second test with 84 byte both connections (test software and Netmeeting), showed at equal conditions two VoIP connections are possible.

Table 8.1: Mixed Test Results

Field strength, Location	VoIPperf setup	Netmeeting reaction
-40dBm 407	4 clients 180,120 and 84 byte packet size	everything worked well, good quality VoIP conversation
-78dBm 405 back row	different	no connection
-65dBm 405 front row	no other traffic	good quality VoIP channel
	4 clients 84 byte packet size	Phone rang, but no voice
	1 client 258 byte packet size	The phone rang at the access point side and half words and sometimes sounds arrived, no sound from the access point to the laptop
	1 client 84 byte packet size	The connection Laptop to access point worked well, but no voice in the other direction

However the question is if in a mixed traffic environment the WWW traffic, which is also TCP, does push through harder, then then the VoIP traffic. For this case differentiated traffic streams need to be implemented.
Seen from the point of view of how far this tests verify the comprehensive test results, it is believed that it can safely be assumed that the highly increased number of peaks at lower field strength indicate that VoIP conversations are nearly impossible. The minimum at -55 dBm can not be explained and may be caused by special multi path conditions.

8.6 Real WLL Setup Test

8.6.1 Objective Description

To verify the measuring method of the test software the following test setup had been done (see figure 8.6). The software running on the laptop was connected via the AP to the PC, which used the SA. First a simplex test stream was sent.

Figure 8.6: Picture of Test setup

Then a full duplex test stream was sent. Both times the signal was relayed by the access point, hence two times media access need to be gained.
The first test was with a packet size of 258 bytes and 10 minutes test time, which corresponds to about 30000 packets. Later a verifying test with half the time had been made. Both results were compared and histograms of the simplex and full duplex connections produced.

8.6.2 Result / Conclusion

The first result was a histogram with a nearly rectangular distribution at the low delays. A Gaussian distribution was expected.
Seeing the packet delay - time graph the steady increased delay could again be observed. After applying the following correction:

$$\begin{aligned} Delay_{increased} &= Delay_{end} - Delay_{start} \\ Delay_{increased} &= 190ms - 8ms \\ &= 182ms \end{aligned}$$

together with the duration of the test

$$\begin{aligned}\Delta_{increasedDelay} &= \frac{Delay_{increased}}{durationoftest} \\ &= \frac{182ms}{10minutes} \\ &= \frac{18.2ms}{1minute} \\ &= \frac{1ms}{3297ms}\end{aligned}$$

This means each 3297ms the measurement will have a deviation of 1ms. After correcting the measured values with this. The following graph 8.7 could be drawn, with an average delay of 8ms . The expected Gaussian curve and shift of the average delay (i.e. to 11ms) in case of a higher network load (i.e. full duplex channel see figure 8.8) can be seen.
The number of high delayed packets seems to be to high. Imagining a threshold at 100 ms delay after which the packets were seen as lost. Let calculate a imaginative packet loss of 18% . To compare this with an independent measurement a flood ping of 10000 packets were done, which showed peak delays of 1000ms and a packet loss rate of 38% . As the flood ping sends out packet as fast at it can, while the program sends out each 20 ms it is believed this result can be seen as a verification.

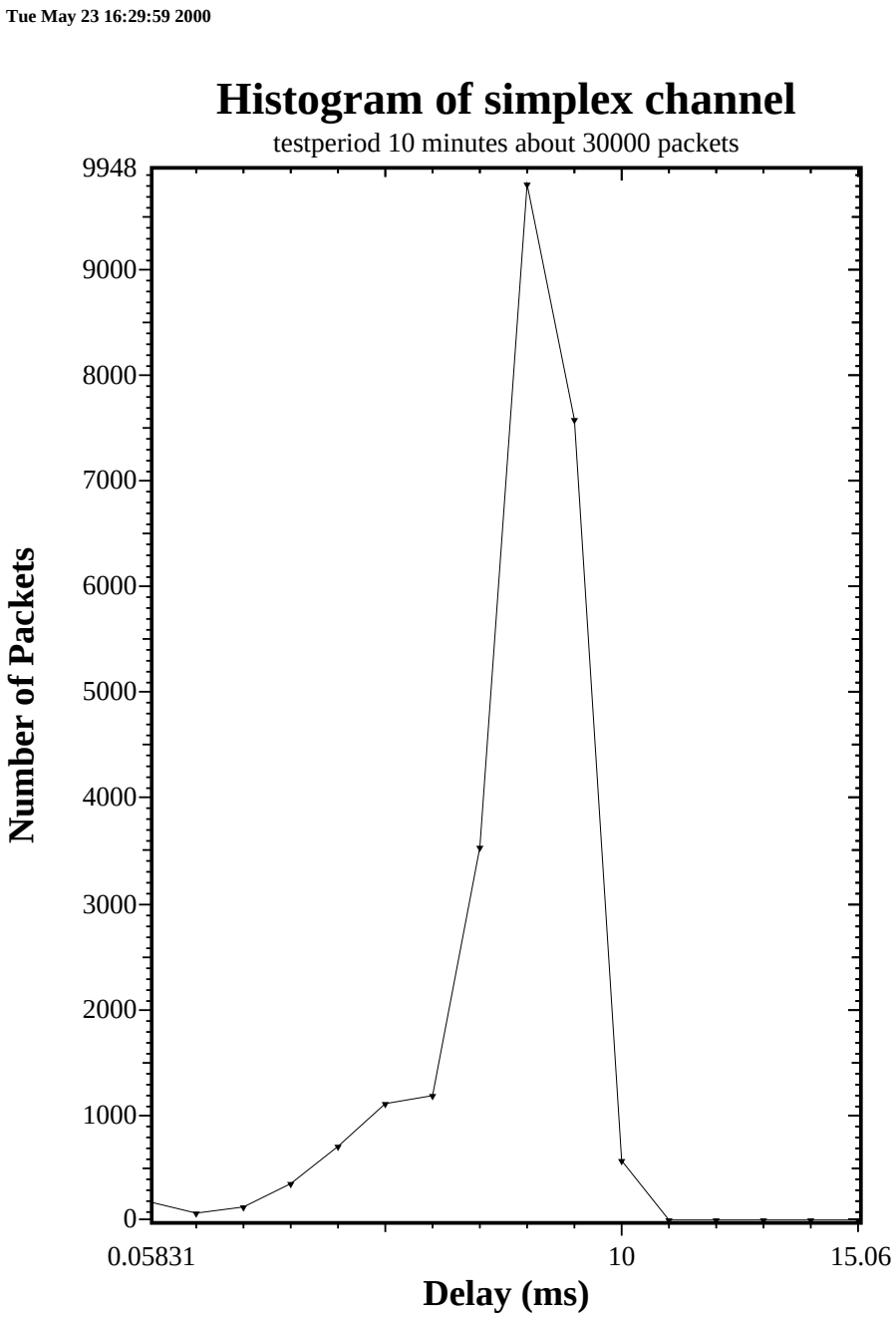

Figure 8.7: Histogram of a simplex channel

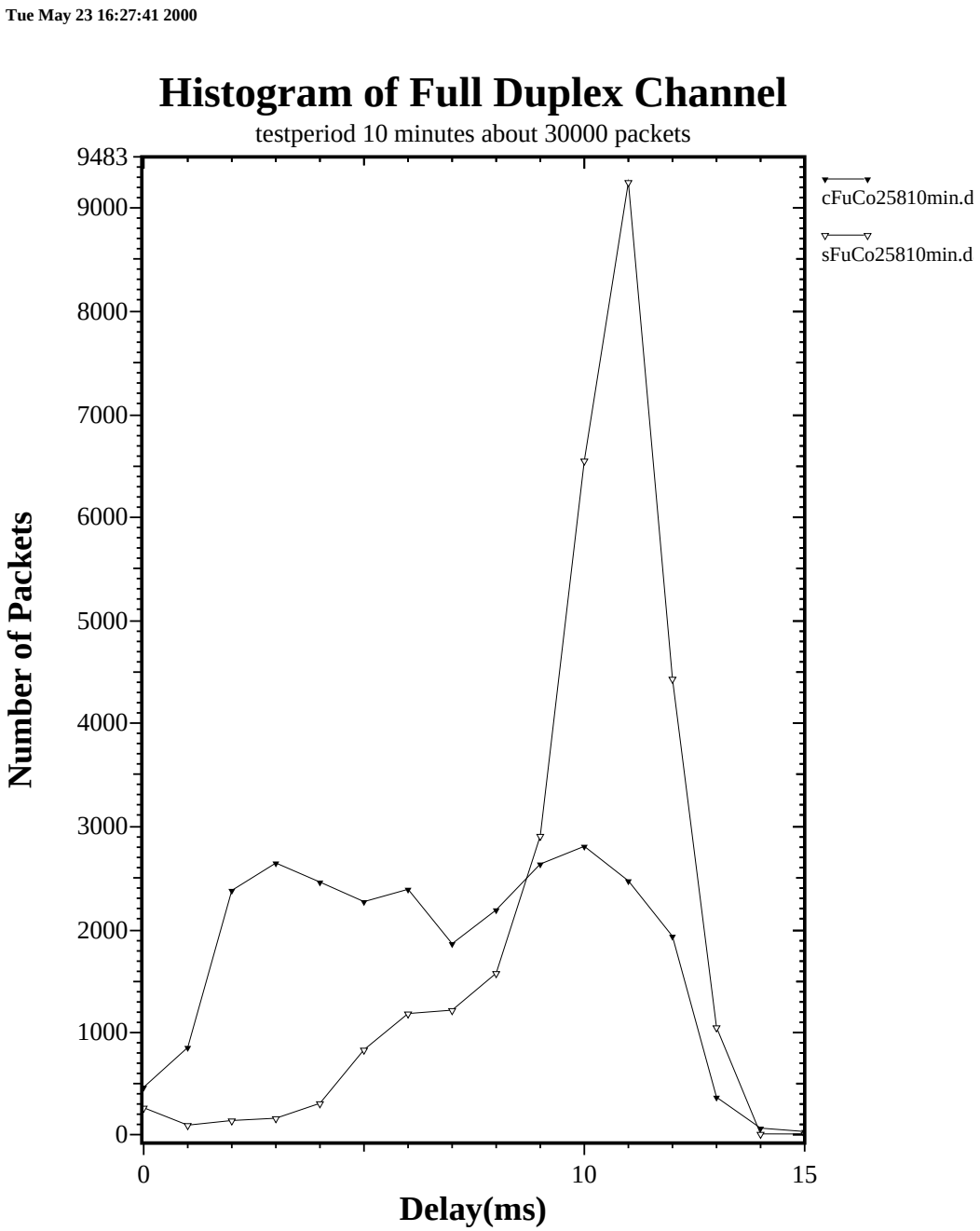

Figure 8.8: Histogram of a full duplex

Chapter 9

Final Conclusions

Although the software can measure the jitter this feature was not used. Also exact numbers are not given, with the reason for the increasing delay not clearly identified. However it is trusted in the direction of the results, which were verified by the 8.5 tests. In a real live setup the capacity of the WLL system should not been calculated by taking the net network capacity (1.65Mbit/s) and divide it by the bit rate the codec needs (e.g. 6.3 kBit/s), which would give a possible of 238 simultaneous simplex channels. Even taken 150 simultaneous simplex channels, as soon as mixed network traffic is involved the delay times become unpredictable. This can be seen at the test with 1 client 258 byte packet size full duplex and one Netmeeting connection with packet size of 84 byte. As todays application does not produce traffic marked as different types, the needed QoS could not be provided. This would be a first main starting point to improvements. As surely the wireless equipment develops further as well, the implementation of e.g. a traffic marking network layer could be started and tested on the wired LAN first. Later up to date wireless equipment could be used.

The last test, which tried to verify the measurements of the software could show, that after understanding the increased delays the software can be used to compare for example developed queuing algorithms. The question hence is if the software together with the whole operating system, which also needs to do memory management, graphical user interface and scheduling tasks, can be seen as a trusted measurement tool or more as a testbed to determine improvements?

Further the tested systems mobility was very limited, which develops the question if a hand over process would take a large amount of network capacity ? So far the reassociation process to quite a long while, which, of course, also was caused by the fact that the distance was large. With several access points a reassociation could be faster as the as soon the other access point is in range already data (e.g. the hopping sequence) could be collected. And a reassociation would be done at

could conditions. However it is not clear how much this influences the network capacity.

For a fixed environment, which maybe connects houses via directional antennas surely the different parameters (maximal number of retransmissions, RTS threshold) are useful, while a in house setup can gain most improvements by varying the location of the stations. Here a clear line of sight is desired. And information can be also gathered by using the site survey software provided by the manufacturer. Again for a customer telephone network like network, which connects houses and not computers in the same room. Tests with a large distance and fixed setup need to be done. From the point of importance for VoIP over WLL, it can be said, that these test better are performed after QoS had been introduced.

Part IV

Appendix

Appendix A

How to register an own enterprise MIB

The Internet Assigned Numbers Authority is responsible for assigning and keeping track of the used numbers.
You can email them at IANA-MIB@isi.edu or phone them at 310-822-1511 x239.
Have the following informations ready:

- Company Name
- Address
- Voice Phone
- Name of Contact
- Contact's Address
- Voice Phone
- Fax Number
- Email

For postal mail:

Internet Assigned Numbers Authority
USC/Information Science Institute
4676 Admiralty Way
Marina del Rey, CA 90292-6695

(This information is taken from the comp.protocols.snmp-SNMP-FAQ)

Appendix B

Application of Markov Chains in VoIP

Markov Chains describe stochastical processes by noting all possible states and the transition probabilities. These derived model than can be used for a steady state analysis. For example if in one city the number of people buying a car is known. Further it is known how many will buy brand A after buying last time brand B (transition probability), and how many revert from brand A to brand C. A Markov chain steady state analysis can predict how many cars of brand A, B and C are in that city after a longer period of time .
In the network environment this analysis can be used to predict the buffer usage in a routing devices. It is possible to find out the ideal buffer sizes and likelihood of a buffer overflow. As a VoIP conversation also is a stochastic process and can be seen as a Markov chain the average bandwidth usage can be predicted by using the steady state analysis.
Beside this a transition reward analysis would allow to analyze the influence of codec change (change of used bandwidth) in a heavy loaded network.

Appendix C

Technical Specifications of Breezecom Equipment


Access Point (AP), Station Adapter (SA) and PCMCIA card (SA_PC)

BreezeNET PRO.11 Series Technical Specifications

PRODUCT FEATURES	AP-10, SA-10, SA-40, WB-10, all Model D bridges	SA-PCR / SA-PCD
Data Rate	Up to 3 Mbps	Up to 3 Mbps
Net throughput	Up to 1.9 Mbps	Up to 1.6 Mbps
Aggregate	Over 15 Mbps (overlapped cells)	
Range		
Integrated atennaes	2,000 ft. (600 meters)	2,000 ft. (600 meters)
External antennas	6 miles US/FCC	6 miles US/FCC
Office environment	500 ft. (150 m)	500 ft. (150 m)
High speed roaming	Up to 60 mph (90 km/h)	Up to 60 mph (90 km/h)
No. of APs per wired LAN	Unlimited	
Max. no. of Co-located cells (access points)	15	
Load sharing support	Yes	Yes
WIRED LAN INTERFACE		
Compliant with	Ethernet/IEEE 802.3 CSMA/CD	
Physical interface	10BaseT	PCMCIA 2.1 Type II slot
Connector type	RJ-45	PCMCIA 2.1 Type II
Network Operating Systems	ALL	Windows 95/98 & NT, NetWare 3.x, 4.x, DOS
Network Drivers	N/A	NDIS 2, NDIS 3, ODI
Wireless LAN Interface	Compliant with IEEE 802.11	Compliant with IEEE 802.11
RADIO SPECIFICATIONS		
Type	Frequency Hopping Spread Spectrum	Frequency Hopping Spread Spectrum
Frequency Range	2.4 GHz - 2.4835 GHz Industrial, Science, Medical band	2.4 GHz - 2.4835 GHz Industrial, Science, Medical band
Antenna System	Dual diversity	Dual diversity
Transmitted Power		
Integrated antennas	10 mW or 100 mW (20 dBm) EIRP	100 mW (20 dBm) EIRP
External antennas	50 mW or (17 dBm) atthe connector Upt to 36 dBm EIRP for 24 dBi antenna	
Sensitivity @ 1 Mbps	-83	-83
@ 2 Mbps	-75	-75
@ 3 Mbps	-67	-67
Modulation	2, 4, 8 Multilevel GFSK	2, 4, 8 Multilevel GFSK
Demodulation	DSP based w/ adaptive equalization	DSP based w/ adaptive equalization
Approvals of Compliance	FCC part 15, ETS 300-328, UL, UL/C, TUV/GS, CE	FCC part 15, ETS 300-328, UL, UL/C, TUV/GS, CE
CONFIGURATION & MANAGEMENT		
Configuration and Setup	Via local monitor port (serial RS-232) and SNMP	Via PC-based software
Site survey	Via local monitor port (serial RS-232)	Via PC-based software
LED indicators	Power on, Wired LAN activity, WirelessLAN syncronization, Wireless LAN signal Quality/load	Link status, data traffic
SNMP management	Yes	
S/W upgrade	Yes, using TFTP download	Yes, using PC
ELECTRICAL		
External power supply	100 V - 250 V, 50 - 60 Hz 0.5 A	From PCMCIA slot
Input Voltage	5 VDC	5 VDC
Power Consumption	1.5 A (peak)	TX: 360 mA/RX: 285 mA (peak)
Power Save Mode		Avg: TX & RX less than 30 mA
SIZE & WEIGHT		
Dimensions (w/o antennas)	5.1" x 3.4" x 1.35" (13cm x 8.6cm x 3.4cm)	Standard PCMCIA Type II
Weight	0.9 lb (0.4 kg)	1.1 Oz (32g)
ENVIRONMENTAL		
Operating temperature	32 F - 105 F (0 C - 40 C)	32 F - 105 F (0 C - 40 C)
Operating humidity	5 % - 95 % non condensing	5 % - 95 % non condensing

Appendix D

Personal Report

Time plan

Period	planed tasks	done tasks
1#28Feb-	collecting background information on WLL, VoIP, H323	Collected background information, playing around with the Breezecom equipment, wrote this serial port, WWW gateway to access the local terminal via web browser
2#5Mar-	collecting background information like previous, also in Breezecom, H323 solutions	collected background information about WLL, VoIP solution as well as what kind of card could be used to interface the phone to the PC
3#12Mar-	familiarizing with Breezecom equipment, network setup, local terminal + background reading on SNMP	Mainly reading about SNMP, also already reading about measurement techniques, quite intensive search for tools, found MRTG, installed it, tried to access local HUB for QoS tests on local network
4#19Mar-	familiarizing with SNMP + background reading on measurement techniques	testing some softwares with SNMP, writing this private menu in Scotty/Tkined, while installing the UCD tools a bit longer journey until I could remote control via SNMP the Breezecom equipment
5#26Mar-	test measurement techniques, develop more detailed ideas and background reading on H323	Read more about measurement techniques, very first development of software
6#2Apr-	develop specification for test setup, first test environment setups and test of tests	More software development, sometimes in the Trinity library to learn about better ways to program and measure the things. Mainly writing software

Period	planed tasks	done tasks
7#9Apr-	carry out specified test or finish specification	Writing software and first 2 chapter of the part 1 (introduction to working field)
8#16Apr-	carry out tests, order review collected information	Finishing the software and writing of the chapter
9#23Apr-	finish tests, order and review collected information + first thinking about result conclusions	write the rest of the first part of the report, do first real test setup tries
10#7May-	develop conclusions, verify with current research situation of other research groups, prepare information	do the various test series (first sizing, parameter, comprehensive area), do the tests with Eavan (VoIP and software the same time, she going to the park and I switching antennas to see difference)
11#14May-	prepare information for report and presentation	drawing figures for report, write last chapters, research for presentation, mainly how to do a call into the phone network without paying - own gateway failed, because DIT phone system is half digital
12#21May-	prepare presentation and report	Search for reason for increasing delay, finishing report (very helpful corrections from Mr. Davis), drawing figures for report, last corrections and preparing report CD-ROM

Work done, possible subjects for examinations

The main areas of my part of the project I would say had been how to do the quantitative test measurement, by writing a own software. Reason for this was also to prepare a survey including capacity, coverage and quality - due to the increasing delay problem, this failed partly. I believe it would be something to solve in about 2-3 weeks more time.
Of course the Breezecom wireless LAN equipment is also my part of the project and beside the actual circuit diagram, I believe I can install and optimize the LAN, as well as finding errors in a existing setup.
SNMP and network management could be also seen as part of the project, out of private interest I maybe learned more then necessary and know now about setup and usage examples. Actually analyzing the DIT LAN wasn t finished, because the HUB, although manageable, did not have IP addresses assigned. I did not want to bother using the SLIP port to reconfigure them, also because

this is clearly not my responsibility.
As writing the software and setting up the answering machine (using the Openh323 software) was done by me, I would also be able to answer questions about H323. Some traffic analyzes for finding the packet size, times between packets and getting the VoIP setup to work gave me also a feeling about this protocol.
One of my ideas for the presentation was to set up the Quicknet card as a gateway (IP network PSTN) using the Linux software or delivered Windows software. Hence I know have basic knowledge about the cards, knowing how to install and test them under Linux.

Part V

Bibliography

Bibliography

[1] Shi (1998) *Mobility Management im Internet und by Wireless ATM* Diplomarbeit an der FH-Dieburg WS 1997/98

[2] Hsiung, J.Fischer, M.Masi, Cuffie, Scheurich *An Approach to IP Telephony Performance Measurement and Modeling in Government Environments* http://198.6.250.9/inet99/proceedings/4p/4p_2.htm

[3] techguide.com, Telogy Networks *Voice over IP* http://www.techguide.com/comm/sec_html/voiceip.shtml

[4] Minoli (1998) *Delivering Voice over IP Networks* Wiley, ISBN 0-471-25482-7 (Trinity Library Code HL-206-507)

[5] Kilkki, Kalevi (1999) *Differentiated services for the Internet* Prentice Hall ISBN 1-578-70132-5 (Trinity Library Code HL-220-62)

[6] Greenstein, Larry (1998) *Transporting Voice Traffic over Packet Networks* International Journal of Network Management 8 1998 page 227-234

[7] Lu, Bharghavan, Srikant (1999) *Fair Scheduling in Wireless Packet Networks* IEEE/ACM Transactions on Networking Vol 7., No 4, August 1999

[8] Breezecom *Manual to WLL equipment*

[9] Schulzrinne, Rosenberg *A Comparison of SIP and H.323 for Internet Telephony* http://www.cs.columbia.edu/~hgs/papers/Schu9807_Comparison.pdf

[10] Talvitie, Hovinen, Haemaelaeinen *Channel Measurement, Characterization and Modeling for Wireless Local Loops* International Journal of Wireless Information Networks Vol.5 No. 1, 1998

[11] Conway, Moon, Skelly (1996)*Synchronized Two-Way Voice Simulation Tool for Internet Phone Performance Analysis and Evaluation* Computer Performance Evaluation Modelling Techniques and Tools, A conference summary (Trinity Code 500.164 L3.1245)

[12] Sinner, Sigle (1998) *Toward Wireless Multimedia Communications. Current Standards and Future Directions* International Journal of Wireless Information Networks Vol5. No 1 1998

[13] Santamaria, Lopez-Hernandez(1994) *Wireless LAN Systems* ISBN 0-89006-609-4 Artech House

[14] Molinari, Zekar (1994)*Drathlose Lokale Netze* ISBN 3-89238-091-0 DATACOM Verlag

[15] Meyer, Plemmons (1993) *Linear Algebra, Markov Chains, and Queueing Models* ISBN 0-387-94085-5 / 3-540-94085-5 Springer Verlag

[16] Various *The OpenH323 Project Homepage* http://www.openh323.org

[17] Buchanan (1996) *The art of testing network systems* Wiley ISBN 0-471-13223-3 (Trinity Library Code HL-196-879)

[18] *Newsgroup: com.protocols.snmp* E.g. http://www.dejanews.com discussion group comp.protocl.snmp

[19] *Linux Howtos Documentation* E.g. http://www.linux.org

ERKLÄRUNG

Ich versichere, daßich die Arbeit ohne fremde Hilfe angefertigt und mich anderer als der von mir angegebenen Hilfsmittel nicht bedient habe.

Dublin, 26 Mai 2000

.....