

HELSINKI UNIVERSITY OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMMUNICATIONS ENGINEERING

Lauri Pietarinen

Wireless Local Area Network in Broadband Access Networks

This Master's Thesis was submitted for examination for the degree of Master of Science in Engineering.

Espoo, 26.3.2001

Supervisor Professor Timo O. Korhonen

Instructor Kimmo Saarela, M.Sc.

Tekijä: Lauri Pietarinen**Työn nimi:** Wireless Local Area Network in Broadband Access Networks**Päivämäärä:** 26.3.2001**Sivumäärä:** 92**Osasto:** Sähkö- ja tietoliikennetekniikka**Professuuri:** Televiestintäjärjestelmät, Koodi: S-72**Työn valvoja:** Professori Timo O. Korhonen**Työn ohjaaja:** DI Kimmo Saarela

Tämä diplomityö käsittelee langattomia lähiverkkotekniikoita (WLAN), joita voidaan käyttää laajakaistaisessa liityntäverkossa. Työssä tutkitaan laajakaistaisia xDSL- tekniikoita, joista ADSL käsitellään yksityiskohtaisemmin. Työssä tarkastellaan myös laajakaistaisen liityntäverkon end-to-end protokolla-arkkitehtuureja sekä ATM-verkossa toimivia IP-kapsulointimenetelmiä.

WLAN sopii hyvin käytettäväksi laajakaistaisessa liityntäverkossa sekä kodeissa että pienissä liikeyrityksissä. Asiakaspäässä olevalla xDSL-verkkopäätteellä voi olla WLAN-liitäntä, joka mahdollistaa helpomman asennuksen verrattuna perinteisiin kiinteisiin lähiverkkotekniikoihin. Työssä esitellään eri WLAN-teknologioita; pääpaino on IEEE 802.11b standardissa. Tämä standardi selostetaan tarkemmin sisältäen MAC- ja fyysisen kerroksen ominaisuudet. Tämä työ antaa yleiskuvan eri WLAN-teknologioista ja niiden hyödyntämisestä.

WLAN-laitteiden yleistyessä on eri laitevalmistajien WLAN-laitteiden yhteensopivuus tullut yhä tärkeämmäksi. Wireless Ethernet Compatibility Alliance (WECA) on määritellyt yhteensopivuustestit IEEE 802.11b standardiin perustuville laitteille. Nämä testit, jotka tehtiin Nokian MW1122 ADSL/WLAN reitittimelle, käsitellään työn kokeellisessa osassa. Suurin osa yhteensopivuustesteistä osoitti, että MW1122 toimii hyvin muiden laitevalmistajien tuotteiden kanssa.

Avainsanat: WLAN, xDSL, ADSL, IP, IEEE 802.11, yhteensopivuus

Author: Lauri Pietarinen**Name of the Thesis:**

Wireless Local Area Network in Broadband Access Networks

Date: 26.3.2001**Number of pages:** 92**Department:** Electrical and Communications Engineering**Professorship:** Telecommunications, Code: S-72**Supervisor:** Professor Timo O. Korhonen**Instructor:** Kimmo Saarela, M.Sc.

This thesis deals with Wireless LAN (WLAN) techniques that can be used in broadband access networks. Broadband xDSL techniques are presented and ADSL is presented in more detail. End-to-end protocol architectures that can be used in broadband access network are discussed and IP encapsulations over ATM are presented in the thesis.

Wireless LAN suits well in a broadband access network architecture at homes and also in case of small business customers. The network terminals that terminate the xDSL connections in customer premises can have WLAN interfaces that enable the easier installation than the traditional wired LANs. Different WLAN technologies are presented and the main focus area is on the IEEE 802.11b standard. This standard is described in more detail including characteristics of MAC and physical layers. This thesis gives an overall picture of different WLAN technologies.

As wireless LAN devices are becoming more common, the interoperability of different manufacturers' WLAN devices has become more important. The Wireless Ethernet Compatibility Alliance (WECA) has defined interoperability tests for IEEE 802.11b based products. These interoperability tests that were done to the Nokia's MW1122 ADSL/WLAN router are presented in the experimental part of the thesis. Most of the interoperability test results showed that the MW1122 operates well with other vendors' products.

Keywords: WLAN, xDSL, ADSL, IP, IEEE 802.11, interoperability

PREFACE

This master's thesis has been done at Nokia Networks in Home and Office Gateways product line that belongs to the Broadband Systems division.

I would like to thank professor Timo Korhonen for guidance and good support during the work.

I would also like to thank my instructor, Kimmo Saarela, for his comments and for the possibility to do the Wi-Fi interoperability measurements in San Jose in Silicon Valley.

I wish to thank all my workmates in the Integration and System Testing group with whom I have had the pleasure to work with. We have always had the great spirit and working climate. Thanks for my workmates, Hannu Kivekäs and Tero Nieminen, for letting me to concentrate on the thesis besides of other work.

In addition I wish to thank Katja for her great support throughout the work.

Espoo, 26.3.2001


Lauri Pietarinen

TABLE OF CONTENTS

DIPLOMATYÖN TIIVISTELMÄ.....	I
ABSTRACT OF MASTER'S THESIS.....	II
PREFACE.....	III
TABLE OF CONTENTS.....	IV
TABLE OF FIGURES.....	VII
GLOSSARY.....	VIII
1. Introduction	1
2. Broadband Access Network Architecture	2
2.1 Network Structure.....	3
2.1.1 Layer 2 Protocol, ATM.....	3
2.1.1.1 ATM Technique.....	4
2.1.1.2 Architecture Layers	5
2.1.2 IP Traffic Encapsulations over ATM	7
2.1.3 IP Tunneling Methods	8
2.2 End-To-End Protocol Alternatives.....	11
2.2.1 Bridge with RFC 2684 Ethernet over ATM.....	11
2.2.2 Bridge with RFC 2516 PPP over Ethernet.....	12
2.2.3 Router with RFC 2364 PPP over ATM	13
2.2.4 Router with RFC 2684 IP over ATM	15
2.2.5 Conclusions	15
2.3 Applications	16
2.3.1 Internet Access for Home Users and Remote Work	16
2.3.2 Internet Access for Small Offices	16
2.3.3 LAN Interconnection for Branch Offices	17
3. XDSL and ADSL	18
3.1 ADSL System	18
3.1.1 Architecture.....	18
3.1.2 Frame Structure	22
3.1.3 DMT Operation.....	23
3.2 Other xDSL Technologies.....	25
3.2.1 ADSL Over ISDN	25
3.2.2 HDSL and HDSL2	26
3.2.3 SDSL and ETSI SDSL.....	27
3.2.4 G.SHDSL	27
3.2.5 VDSL	28
3.2.6 IDSL.....	28
3.3 Frequency Usage of xDSL Technologies.....	28
4. Wireless LAN standards.....	30
4.1 IEEE 802.11	30
4.2 HIPERLAN.....	31
4.2.1 HIPERLAN/1	31
4.2.2 HIPERLAN/2	32
4.2.2.1 Networks topology.....	32
4.2.2.2 Protocol layers	33
4.3 Bluetooth	35
4.3.1 General information.....	35
4.3.2 Network Topology	36
4.3.3 Radio channels	36
4.3.4 Physical Layer.....	37
4.3.5 Error Correction and Checking	38
4.3.6 IrDA Interoperability	38
4.4 HomeRF	39
4.4.1 Medium Access Method	39

4.4.2	Physical Layer.....	39
4.4.3	Network Topology	40
4.5	IrDA	40
4.5.1	Network Topology	40
4.5.2	Protocols	41
4.5.3	Physical Layer.....	41
4.5.4	IrDA Link Access Protocol (IrLAP).....	41
4.5.5	IrDA Link Management Protocol (IrLMP).....	42
4.5.6	Optional Protocols.....	42
4.6	Conclusions	43
5.	IEEE 802.11/ 802.11b	44
5.1	Industrial, Scientific and Medical (ISM) Frequency Band	44
5.2	Network Topology.....	45
5.3	Logical Architecture	46
5.4	Medium Access Control (MAC) Layer	47
5.4.1	Accessing the wireless medium	47
5.4.1.1	Distributed Coordination Function	47
5.4.1.2	Point Coordination Function	49
5.4.2	Fragmentation and Reassembly.....	49
5.4.3	Authentication and Privacy	51
5.4.4	Power Management	52
5.5	Physical Layer	53
5.5.1	Direct Sequence Spread Spectrum	53
5.5.2	Frequency Hopping Spread Spectrum	55
5.5.3	Infrared	57
5.5.4	Modulation Methods.....	57
6.	WLAN in Residential and Small Office Broadband Environment	60
6.1	Applications	60
6.2	WLAN Security	61
6.2.1	Authentication	61
6.2.2	Privacy	62
6.3	WLAN Network Planning	63
6.3.1	Location and Site Survey	63
6.3.2	Frequency Channels	63
7.	Measurements	65
7.1	WLAN Interoperability.....	65
7.2	Description of Measurement Configurations and Methods	65
7.2.1	Measurement Configurations	65
7.2.1.1	Initial tests.....	69
7.2.1.2	Extended Tests	69
7.2.1.3	Special Tests	69
7.2.2	Methods	69
7.2.2.1	Initial Tests.....	70
7.2.2.2	Extended Tests	71
7.2.2.3	Special Tests	71
7.3	Analysis	72
7.3.1	Initial tests.....	72
7.3.2	Extended Tests	73
7.3.3	Special Tests	77
7.4	Results	77
8.	Summary	79
9.	References	81
	APPENDIX A. Configurations in Initial Tests	85
	APPENDIX B. Configurations in Extended Tests	86
	APPENDIX C. Configurations in Special Tests	88
	APPENDIX D. Measured and Target Throughput Values	89

APPENDIX E. Throughput Values in Test Case EA3DT1 90

APPENDIX F. Throughput Values in Test Case EA7DT1 91

APPENDIX G. Throughput Values in Test Case EA7DT2..... 92

TABLE OF FIGURES

Figure 1 Broadband Access Network.....	2
Figure 2 ATM Cell Structure.....	4
Figure 3 ATM VPI/VCI switching [Suitiala 1999].....	5
Figure 4 ATM layers [ITU-T I.363.1 1996].....	6
Figure 5 Basic characteristics of different AALs [Suitiala 1999].....	6
Figure 6 Point-to-Point Tunneling	9
Figure 7 Layer 2 Tunneling	11
Figure 8 Bridge with RFC 2684 Ethernet over ATM	12
Figure 9 Bridge with RFC 2516 PPP over Ethernet.....	13
Figure 10 Router with RFC 2364 PPP over ATM	14
Figure 11 Router with RFC 2684 IP over ATM.....	15
Figure 12 ADSL reference model [ANSI T1.413 1998].....	19
Figure 13 ATU-R transmitter model [ANSI T1.413 1998]	20
Figure 14 ATM transport model [ANSI T1.413 1998]	20
Figure 15 Tone ordering [ANSI T1.413 1998]	22
Figure 16 ADSL superframe structure [ANSI T1.413 1998].....	23
Figure 17 ADSL frequency range [Pendolin 1997]	24
Figure 18 Frequency usage of xDSL technologies.....	29
Figure 19 HIPERLAN/1 frequency channels	32
Figure 20 HIPERLAN/2 Protocol Layers	33
Figure 21 HIPERLAN/2 Transmitter	34
Figure 22 Bluetooth Connections.....	35
Figure 23 Bluetooth's Piconets and Scatternet.....	36
Figure 24 IrDA Protocol Stack.....	41
Figure 25 ISM Bands	44
Figure 26 ISM Bands in Detail	45
Figure 27 IEEE 802.11 Network Topology	45
Figure 28 IEEE 802.11 Logical Architecture.....	46
Figure 29 IEEE 802.11 Protocol Layers	47
Figure 30 Different Spacing Intervals in IEEE 802.11	48
Figure 31 Fragmentation in IEEE 802.11	50
Figure 32 IEEE 802.11 MAC Frame Structure	50
Figure 33 IEEE 802.11 MAC Frame's Frame Control Field	51
Figure 34 Spread Spectrum Technology.....	53
Figure 35 Direct Sequence Spread Spectrum	54
Figure 36 PLCP Frame Format in DSSS.....	55
Figure 37 Frequency Hopping Spread Spectrum	56
Figure 38 PLCP Frame Format in FHSS.....	56
Figure 39 Test Set-Up.....	66
Figure 40 Nokia MW1122 ADSL/WLAN Router and Nokia C111 WLAN Card	68
Figure 41 Nokia MW1122 ADSL/WLAN Router's Back-panel	68
Figure 42 Measured Throughput of MW1122 in Test EA2DT1	74
Figure 43 Measured Throughput of A032 in Test EA2DT1.....	75
Figure 44 Measured Throughput of Lucent AP in Test EA2DT1.....	75
Figure 45 Measured Throughputs Versus Target Values	78

GLOSSARY

A

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACK	Acknowledge
ACL	Asynchronous Connection-Less
ADSL	Asymmetrical Digital Subscriber Line
ANSI	American National Standards Institute
AP	Access Point
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Transmission Unit – Central Office
ATU-R	ADSL Transmission Unit – Remote

B

BER	Bit Error Rate
BRAN	Broadband Radio Access Networks
BSS	Basic Service Set
BSSID	Basic Service Set Identifier

C

CAP	Carrierless Amplitude and Phase
CBR	Constant Bit Rate
CCK	Complementary Code Keying
CHAP	Challenge Handshake Authentication Protocol
CL	Convergence Layer
CLI	Command Line Interface
CO	Central Office
CPCS	Common Part Convergence Sublayer
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CTS	Clear to Send

D

DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DECT	Digital European Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed Interframe Space
DLC	Data Link Control
DMT	Discrete Multi-Tone
DNS	Domain Name Server
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSSS	Direct Sequence Spread Spectrum

E

EIFS	Extended Interframe Space
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute

F

FCC	Federal Communications Commission
FCS	Frame Check Sequence
FEC	Forward Error Correction
FEXT	Far-End Crosstalk
FHSS	Frequency Hop Spread Spectrum
FSK	Frequency Shift Keying

G

GMSK	Gaussian Minimum Shift Keying
3GPP	Third Generation Partnership Project
GSM	Global System for Mobile Communications
GUI	Graphical User Interface

H

HDSL	High-speed Digital Subscriber Line
HDTV	High Definition Television
HEC	Header Error Control
HIPERLAN	High Performance Local Area Network
HRFWG	HomeRF Working Group

I

IAS	Information Access Service
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IDFT	Inverse Discrete Fourier Transform
IDSL	Integrated Digital Subscriber Line
IEEE	The Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Interframe Space
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
ISDN	Integrated Services Digital Network
ISM	Industrial, Scientific and Medical
ISO	International Standardization Organization
ISP	Internet Service Provider
ITU-T	International Telecommunications Union – Telecommunications Standardization Section

L

L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LANE	LAN Emulation
LLC	Logical Link Control
LNS	L2TP Network Server

M

MAC	Medium Access Control
MMAC	Multimedia Mobile Access Communications
MPOA	Multiprotocol Over ATM
MSDU	MAC Service Data Unit

N

NAPT	Network Address Port Translation
NEXT	Near-End Crosstalk
NIC	Network Interface Card
NT	Network Terminal
NTR	Network Timing Reference

O

OAM	Operations, Administrations and Maintenance
OFDM	Orthogonal Frequency Division Multiplex
OS	Operating System
OSI	Open Systems Interconnection

P

PAM	Pulse Amplitude Modulation
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PCF	Point Coordination Function
PDC	Personal Digital Communication
PDU	Protocol Data Unit
PIFS	PCF Interframe Space
PIN	Personal Identification Number
PLCP	Physical Layer Convergence Procedure
PLW	Protocol Service Data Unit Length Word
PN	Pseudo Random
POTS	Plain Old Telephone Service
PPM	Pulse Position Modulation
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSD	Power Spectral Density
PSF	PLCP Signaling Field
PVC	Permanent Virtual Connection

Q

QAM	Quadrature Amplitude Modulation
QoS	Quality of Service

R

RADSL	Rate-Adaptive Digital Subscriber Line
RAN	Remote Access Node
RFC	Request for Comments
RIP	Routing Information Protocol
RLC	Radio Link Control
RTS	Request to Send

S

SAP	Service Access Point
SAR	Segmentation and Reassembly
SCO	Synchronous Connection-Oriented
SDSL	Symmetric Digital Subscriber Line
SFD	Start Frame Delimiter
SHDSL	Single-Pair High-Speed Digital Subscriber Line
SIFS	Short Interframe Space
SIG	Bluetooth Special Interest Group
SIM	Subscriber Identity Module
SNAP	SubNetwork Attachment Point
SNR	Signal to Noise Ratio
SSID	Service Set Identifier
STM	Synchronous Transfer Mode
SVC	Switched Virtual Channel
SVNL	Silicon Valley Networking Laboratory
SWAP	Shared Wireless Access Protocol

T

TCP	Transmission Control Protocol
TDMA/TDD	Time Division Multiple Access/Time Division Duplexing

U

UAWG	Universal ADSL Working Group
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System

V

VBR	Variable Bit Rate
VC	Virtual Channel
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VDSL	Very High-Speed Digital Subscriber Line
VoIP	Voice over IP
VPI	Virtual Path Identifier
VPN	Virtual Private Network

W

WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalence Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

1. INTRODUCTION

This thesis is a study about the Wireless LAN (WLAN) technology in broadband xDSL access networks. Different wireless LAN technologies are presented so that the main focus is on the Institute of Electrical and Electronics Engineers (IEEE) 802.11b technology because it is the most used one at the moment in the market area. XDSL system and especially ADSL are described as well. The presentation of the technologies is a technical review mostly based on the relevant standards that are published. The usability of the wireless LAN technology in residential and small office broadband environment is covered containing, for example, security aspects, different applications and interoperability issues.

Within the thesis, interoperability tests for the Nokia's MW1122 ADSL/WLAN router were done in the Silicon Valley Networking Laboratory (SVNL) in San Jose. The SVNL provides testing services for vendors of wireless LAN devices. Many vendors use the SVNL's testing services to verify the interoperability and conformance of their products. The Wireless Ethernet Compatibility Alliance (WECA) has specified Wireless Fidelity (Wi-Fi) interoperability measurements for the IEEE 802.11b based products. This thesis contains measurement results for the Nokia's MW1122 ADSL/WLAN router. The goal of the tests was to verify the interoperability of the MW1122 with other vendors' products.

The broadband access network architecture is presented in chapter 2 containing information about the ATM and IP traffic encapsulations over ATM. Different IP tunneling methods are presented and also end-to-end protocol alternatives are covered. Typical applications are also discussed.

XDSL system and especially ADSL are presented in chapter 3. In chapter 4 different wireless LAN technologies are presented. IEEE 802.11 standard is presented in chapter 5. Chapter 6 considers WLAN in residential and small office broadband environment. Interoperability measurement results and analysis for the MW1122 ADSL/WLAN router are presented in chapter 7.

2. BROADBAND ACCESS NETWORK ARCHITECTURE

The broadband access network means in practise that the available bandwidth for the customers is more than the traditional dial-up connections that are up to 56 kbps. The ISDN (64 kbps or 128 kbps) can be considered as a broadband access but in this thesis the broadband means xDSL connections. The xDSL connections that telecom operators offer are usually from 256 kbps up to several Mbps. The broadband access network contains network terminals that are located in the customer premises and access multiplexers such as Digital Subscriber Line Access Multiplexers (DSLAM) that are located in the central office side of the network. A typical overall picture of broadband access network is shown in Figure 1.

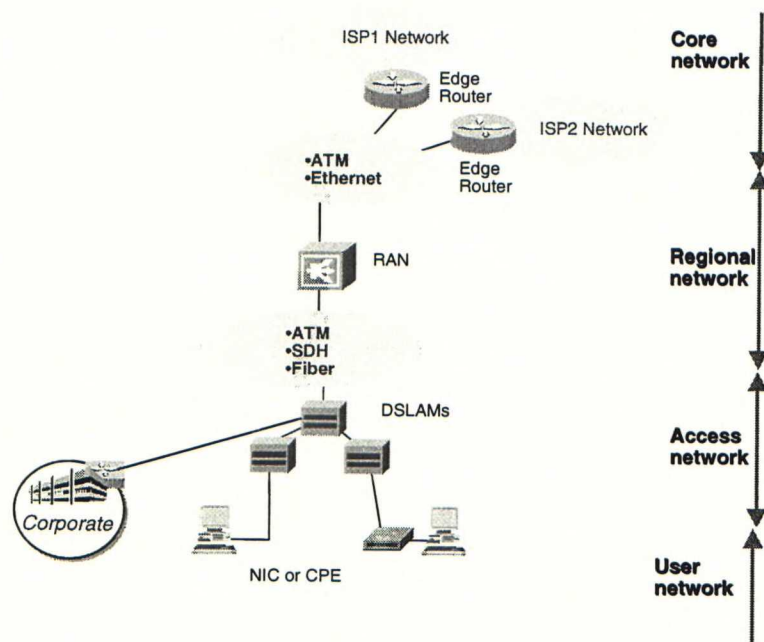


Figure 1 Broadband Access Network

It can be seen that the user network is the LAN of the Network Terminals (NT). The NTs are located in the customer premises and they are also called Customer Premises Equipment (CPE). Network Interface Cards (NIC) can also be used in PCs. Access network contains NTs and DSLAMs. Regional network contains the trunk connections from DSLAMs to Remote Access Node (RAN) that can be a specific router capable of handling different kinds of traffics like Asynchronous Transfer Mode (ATM), ethernet and IP. The ATM is an Open Systems

Interconnection (OSI) reference model's layer 2 technique and it can be used in broadband access networking according to the ADSL Forum's recommendation TR-002 [ADSL Forum TR-002 1997]. ATM will be presented in chapter 2.1.1. Core network is the network between different Internet Service Providers (ISP).

The user network in the broadband access network can be wireless or traditionally wired. The Wireless LAN (WLAN) enables the wireless use of different kinds of applications offered by service providers and corporates.

2.1 Network Structure

2.1.1 Layer 2 Protocol, ATM

The layer 2 refers to the International Organization for Standardization's (ISO) OSI reference model. The OSI model describes the communication process as a seven hierarchy protocol layers, each dependent on the layer beneath it. The seven layers are from bottom to up: physical, data link, network, transport, session, presentation and application. Each layer contains functions between an upper layer and a lower logical boundary. Each layer uses the services of the lower layers in conjunction with its own functions to create new services which are made available to the higher layers [Halsall 1997].

As the Asymmetric Digital Subscriber Line (ADSL) takes care of the physical layer between network terminals and DSLAMs, some link layer technique is needed above ADSL and also below IP. The ATM is used as a layer 2 technique for broadband ADSL end-to-end architecture. The Quality of Service (QoS) is an important issue considering the broadband network architecture generally. Different QoS parameters in ATM are Cell Delay Variation, Maximum Cell Transfer Delay and Cell Loss Ratio. ATM supports also the transmission of wide variety of information like voice, data and video. Considering the broadband access network architecture, ATM is typically used between NT and the RAN.

ATM carries the information streams in cells, consisting of 53-octets. In each cell the 53-octets consist of 5-bytes header and 48-bytes user payload. The asynchronous transfer mode in ATM means that all the different information streams can be mapped asynchronously to the ATM cells but the physical layer transmission is

synchronous [Lynross 1998]. The 53-octets ATM cell structure [ITU-T I.361 1999] is shown in Figure 2.

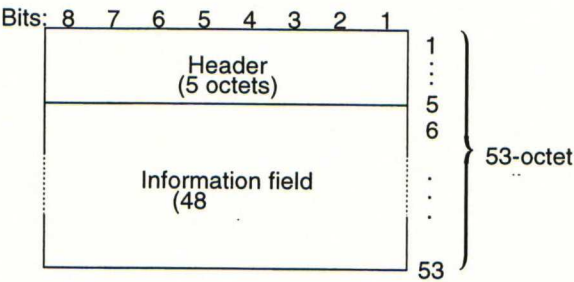


Figure 2 ATM Cell Structure

The ATM technology will not be demonstrated deeply but the basic principles will be described. ATM technology is standardized by International Telecommunications Union–Telecommunications Standardization Section (ITU-T) [Ginsburg 1999]. Another major organization that has been involved is the ATM Forum. Many service providers and equipment manufacturers etc have joined the ATM Forum.

2.1.1.1 ATM Technique

ATM cells are transferred over the physical layer. ATM cell's header has the connection identifiers that are Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). One VPI can carry up to 65536 VCIs and there can be 4096 VPIs [Lynross 1998]. The switching in an ATM network is based on these two connection identifiers. The switching may be done according to a VPI and VCI combination that defines a unique connection or according to the VPI value when all the VCIs inside of the VPI are switched. Figure 3 illustrates the principle of VPI/VCI switching.

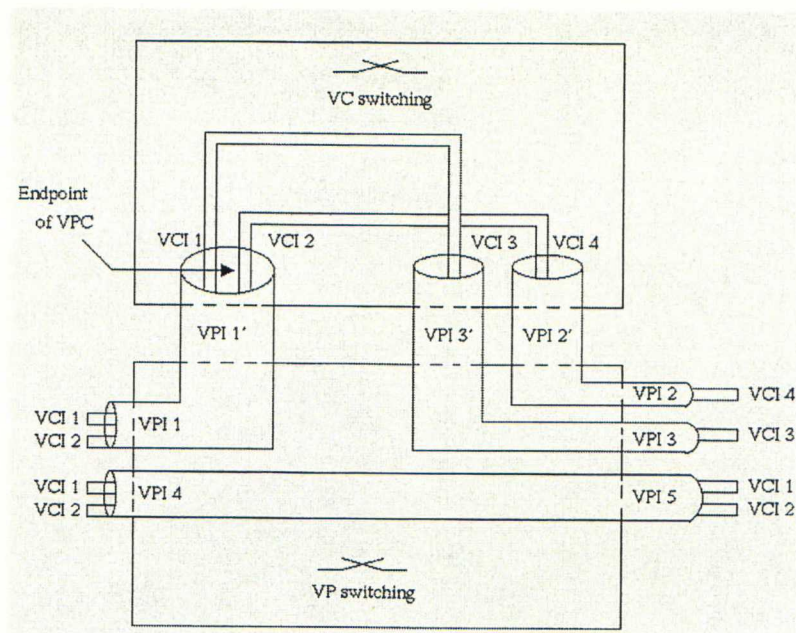


Figure 3 ATM VPI/VCI switching [Suitiala 1999]

In ADSL system the VPI/VCI cross-connection can be done, for example, in the DSLAM. The NT must be configured to use a certain VPI/VCI values and then this connection can be cross-connected in the DSLAM. From the DSLAM the connection can go to ATM network that might have several ATM switches and finally to the RAN where the ATM connection is terminated. The termination includes the decapsulation of the IP traffic from ATM cells and then the user data can be routed in the IP level. The VPI/VCI combination forms a Permanent Virtual Connection (PVC). PVCs are configured to the ATM switches in broadband network. The PVCs are also configured in the NT and in the DSLAM. The virtual connections can also be dynamic Switched Virtual Connections (SVCs). In case of SVCs the configuration of the VC doesn't have to be static. However the permanent VCs are mostly used in ADSL installations [ADSL Forum TR-012 1998].

2.1.1.2 Architecture Layers

ATM is a layered architecture having two main layers, ATM layer and ATM Adaptation Layer (AAL). The AAL translates the information between higher layers and the ATM cells provided by the ATM layer. These two layers correspond to Layer 2 (Link Layer) in the OSI model [Lynross 1998]. The AAL consists of two sublayers, Convergence Sublayer (CS) and Segmentation and Reassembly (SAR) sublayer. Figure 4 illustrates the different layers in the ATM.

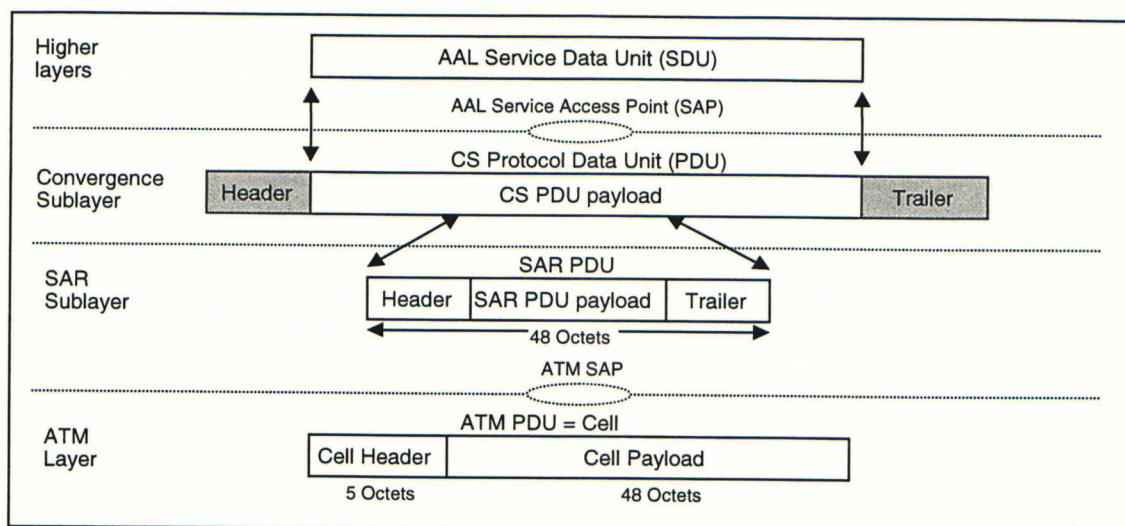


Figure 4 ATM layers [ITU-T I.363.1 1996]

The ATM layer is responsible for adding the 5-bytes header to the 48-octets payload that has been assembled in the AAL. The payload part of the cell is transparent to the ATM layer. So the ATM cell is constructed in the ATM layer and the cell switching takes place in this layer.

The layer above ATM layer is the AAL. This layer is very important because it enables transmission of different services by taking into account the special requirements of each service. The QoS in ATM is defined in the AAL by defining different adaptation layers for different service requirements. In Figure 5 different AALs are defined.

	AAL1	AAL2	AAL3/4	AAL5
Timing Relationship	Required		Not Required	
Bit Rate	Constant	Variable		
Connection Mode	Connection-Oriented			Connection-less
Associated ATM QoS	CBR	rt-VBR	nrt-VBR	UBR
			ABR	

Figure 5 Basic characteristics of different AALs [Suitiala 1999]

Originally five different AALs were developed but because of similarity the AAL3 and AAL4 were combined into a single AAL3/4. Because of the need for low overhead

and simplicity the AAL5 was defined [Lynross 1998]. The AAL5 is most commonly used because it is suitable for transporting the IP traffic. Correspondingly the voice traffic would be better to transfer in the AAL2 that has real-time QoS defined and also timing relationship is required. There are different possibilities to carry the voice in the broadband access network architecture. The voice can be carried by using the Plain Old Telephone Service (POTS) below ADSL, by using ISDN below ADSL or by using Voice over IP (VoIP) with different kinds of xDSL technologies. It is also possible to use the above-mentioned AAL2 to carry the voice over ATM without the need of IP. Generally it can be said that voice could be carried by using some voice over packet technique instead of POTS.

The AAL is divided into two sublayers, CS and SAR. The CS provides the AAL service to the higher layers via a Service Access Point (SAP). CS depends on the service applied and it performs variety of functions, like clock recovery. The SAR accepts CS protocol data units and presents them to the ATM layer as 48-bytes payload. The CS adds a header and trailer that are AAL specific to the higher layer data that it receives. The SAR then adds its own header and trailer if needed. The AAL5 has the lowest overhead and that's why it is so widely used [ITU-T I.363.1 1996].

2.1.2 IP Traffic Encapsulations over ATM

Because the network layer traffic in the internet is based on the IP, the encapsulation of IP into ATM is necessary to define. There are several encapsulation methods available, however some of them have been more used than the others. Different encapsulation protocols are Request For Comments (RFC) 2684 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) that obsoletes RFC 1483, RFC 2364 (PPP over AAL5), RFC 2516 (PPP over Ethernet), RFC 1577 (Classical IP and ARP over ATM), LAN Emulation (LANE) and Multiprotocol over ATM (MPOA). The RFC 2684 and RFC 2364 are explained next in more details.

The RFC 2684 [Grossman and Heinänen 1999] defines two kinds of encapsulation methods, VC multiplexing and Logical Link Control (LLC) encapsulation. RFC 2684 defines how routed and bridged Protocol Data Units (PDU) are carried over the AAL5. The two encapsulation methods differ so that the VC multiplexing reduces fragmentation overhead and the LLC encapsulation requires fewer VCs in a multiprotocol environment. For both multiplexing methods, routed and bridged PDUs are encapsulated within the payload field on an AAL5 Common Part Convergence

Sublayer (CPCS) PDU. LLC encapsulation is used when more than one protocol are carried over the same VC. In LLC encapsulation the protocol types of routed PDUs are identified by prefixing an IEEE 802.2 LLC header to protocol data units. An IEEE 802.1a SubNetwork Attachment Point (SNAP) header may follow the LLC header. In case the LLC encapsulation is used with bridged protocols, both LLC and SNAP headers are used. In VC multiplexing encapsulation there is no need for protocol identification information to be carried in the CPCS-PDU [Grossman and Heinänen 1999].

RFC 2364 [Gross et al. 1998] defines the use of AAL5 for framing Point-to-Point Protocol (PPP) encapsulated packets. RFC 2364 allows the use of two encapsulation methods defined in the RFC 2684, VC multiplexing or LLC encapsulation. When using the LLC, the payload's protocol type is identified by an LLC header [Gross et al. 1998]. There are many advantages when using the PPP-encapsulation. The main advantages are authentication based on Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), IP-address autoconfiguration, multiple sessions, encryption and compression [Ginsburg 1999].

In practice the used IP encapsulation method is done by configuring the CPE and the RAN. The RAN terminates the ATM connection. The whole network architecture affects the configuration method to be used. In some cases bridge-network may be needed and in some cases the route-network may be the most suitable depending on the services to be used. There are many different possibilities for the end-to-end protocols and there is no simple answer what kind of network model should be used.

2.1.3 IP Tunneling Methods

Two different tunneling methods are presented: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP). These two tunneling protocols have been developed for the extension of the PPP protocol. Tunneling means that network's packet is essentially hidden from the transporting network by hiding its original header behind one tacked on by the tunneling protocol. Seeing only that header, routers pass it through the internet to the destination contained in the added IP header, where the VPN server strips away the tunneler's header and the remainder is forwarded on to its ultimate destination. [Fowler 1999]

PPTP in the broadband access network means that the connection taken from the client PC (wired or wireless) is tunneled through the local area network of the NT to the RAN. The NT in this case is configured as a basic router having IP network in its LAN. The client PC initializes the PPTP connection to the NT's LAN-interface's IP-address and then the PPP traffic is forwarded to the ATM PVC by using, for example, RFC 2364 Point-to-Point over ATM (PPPoA) encapsulation. PPTP is specified in the RFC 2637 [Hamzeh et al. 1999]. Figure 6 shows the protocol stack in case the PPTP is used.

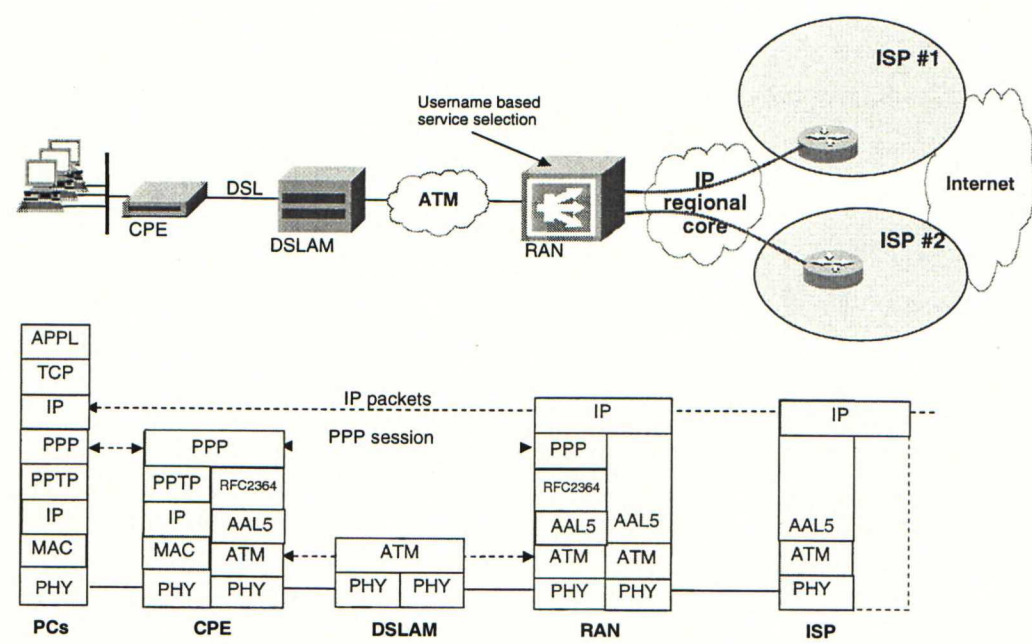


Figure 6 Point-to-Point Tunneling

It must be noted that when the tunneled connection is used, every PPTP connection needs to have own ATM PVC if PPPoA with VC multiplexing is used. If PPPoA with LLC encapsulation is used, several PPTP connections can use the same ATM PVC. In typical xDSL terminals it is possible to have several PVCs configured. Generally it is possible to have, for example, one ATM PVC acting as a router interface by using PPPoA encapsulation and having IP-address in the interface. In addition to this, there may also be Network Address Port Translation (NAPT) and Dynamic Host Configuration Protocol (DHCP) server functionalities configured to the NT. It is also possible to have another PVC configured to support tunneled connection. The PPTP enables the client PC to have Virtual Private Network (VPN) connection to some destination while other clients are able to have internet access at the same time.

The NAT means that the routing software in the NT translates the source IP-address and port number dynamically to the Virtual Channel Connection's (VCC) IP-address and port number. By this way the private IP-network in the NT's LAN or WLAN is hidden and the public IP-address in the VCC is visible to RAN. The VCC's IP-address is shared between several hosts in the private LAN of the terminal and the packets coming from the RAN are mapped back to the original destination addresses [Egevang and Francis 1994, Tsirtsis and Srisuresh 2000].

The another tunneling method, L2TP, is used for the extension of the PPP connection in case there is need to have VPN-connection from the RAN to ISP's or corporate's router. The L2TP can tunnel PPP over layer 2 and layer 3 networks like ATM and IP. As defined in the RFC 2661 [Townesley et al. 1999] the L2TP connection is established between L2TP Access Concentrator (LAC) and L2TP Network Server (LNS). The user can have a PPP connection from the client PC to the LAC that is the RAN of the network operator. This connection can be taken, for example, by using RFC 2516 Point-to-Point over Ethernet (PPPoE) or PPTP connection. The LAC then extends this PPP connection to the LNS that can be located in the ISP's or corporate's premises. The L2TP tunnel consists of the user traffic and the header information necessary to support the tunnel. Therefore, the tunnel provides the encapsulated PPP packets and the requisite control messages needed for the operations between the LAC and LNS [Black 1999]. By this way one point-to-point connection is formed and the L2TP connection is not visible for the end-user. The used protocol stack in case of PPPoE and L2TP used is shown in Figure 7.

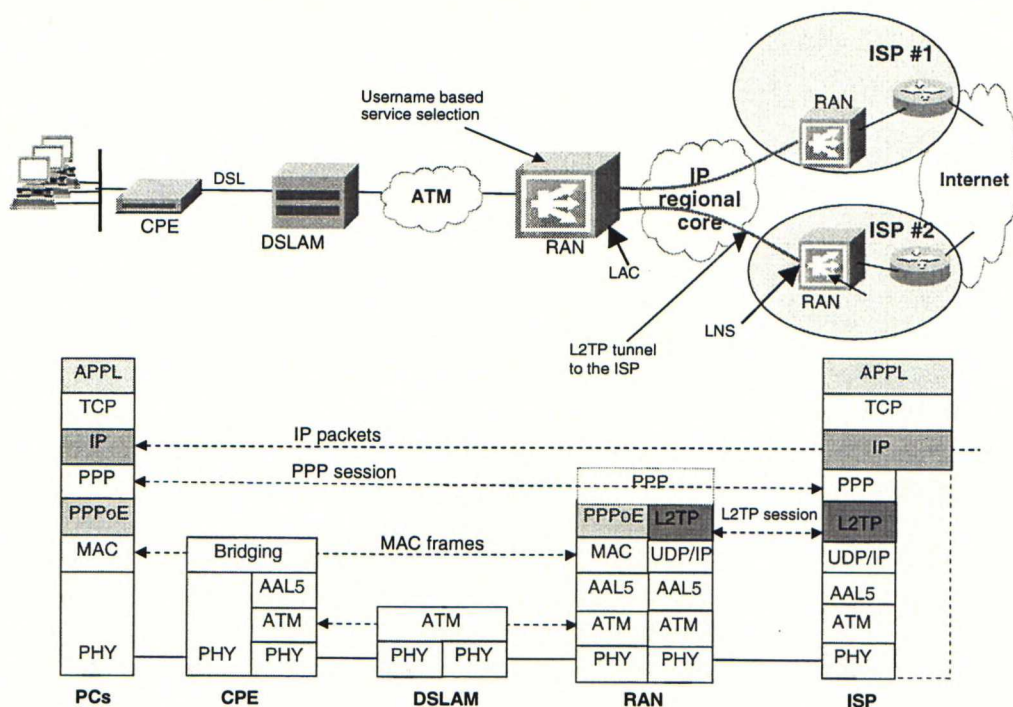


Figure 7 Layer 2 Tunneling

In case PPPoE is used the xDSL NT is a bridge and is transparent for the PPP session. The PPPoE or PPTP sessions with L2TP extensions can be taken both from the WLAN and LAN side of network terminal. In case of home users this set-up enables one family member to have VPN-connection to corporate's router while the others are able to access the internet.

2.2 End-To-End Protocol Alternatives

There are several possibilities for the end-to-end protocol that can be used in the broadband access network. The NT can be a bridge or a router and also local tunneling can be used. In this chapter the most typical end-to-end protocol alternatives are presented.

2.2.1 Bridge with RFC 2684 Ethernet over ATM

The simplest way to use the NT in the access network is to use the RFC 2684 ethernet over ATM encapsulation. In this configuration the NT is configured to work as a basic bridge supporting only bridging. In this case the NT doesn't handle IP traffic at all but works as a transparent bridge in OSI layer 2. The bridging is based on Medium Access Control (MAC) addresses that are in the header of ethernet frame. In case of bridge the NT may also have an IP-address but it would only be for

management purposes to be able to have telnet or Web browser connections to the NT. In bridge mode there is not so much to configure in the NT but in case of WLAN interface the user may need, for example, Web browser management connection to the NT. Web browser management connection could be used to change WLAN specific configurations like authentication and encryption parameters. It is also possible to have a dedicated management ATM PVC, which enables the ISP to use the management connection for different purposes like software upgrades. In Figure 8 the protocol stack for the basic bridge is presented.

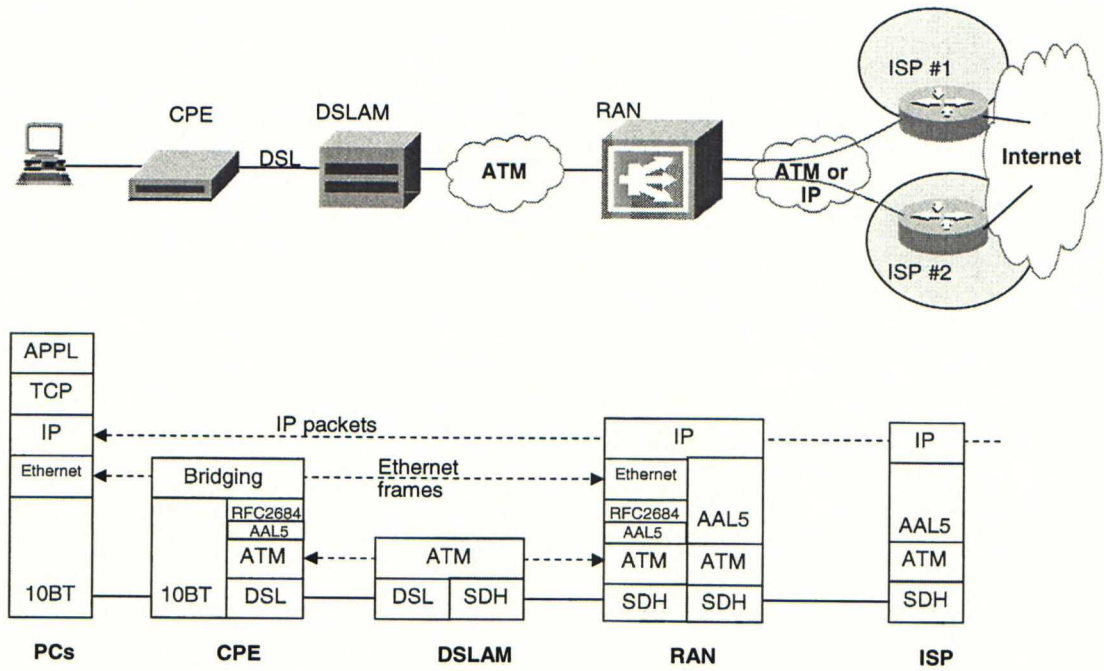


Figure 8 Bridge with RFC 2684 Ethernet over ATM

The CPE forwards ethernet frames from the Wide Area Network (WAN) side of the network to the NT's local area network that can be wired or wireless. The IP-addresses to the client PCs are given with DHCP from the DHCP server that is located behind the RAN. Fixed IP-addresses can be used as well. The IP-address for the client PC must be public, otherwise NAPT must be used somewhere in the network behind the xDSL connection. NAPT hides private IP-addresses and only public IP-addresses can be routed in the internet.

2.2.2 Bridge with RFC 2516 PPP over Ethernet

The second protocol alternative to use in case of bridge is to use the PPPoE that enables point-to-point connections from the client PC (wired or wireless) across the

ATM network. This makes it possible to have authentication-based connections from the client PCs to the destination ISP. The authentication is done and service provider is chosen based on usernames in the RAN. It is possible to have several PPPoE connections simultaneously over one ATM PVC because each PPPoE connection has a unique session identifier as specified in the RFC 2516. The protocol stack that is used in PPPoE is shown in Figure 9.

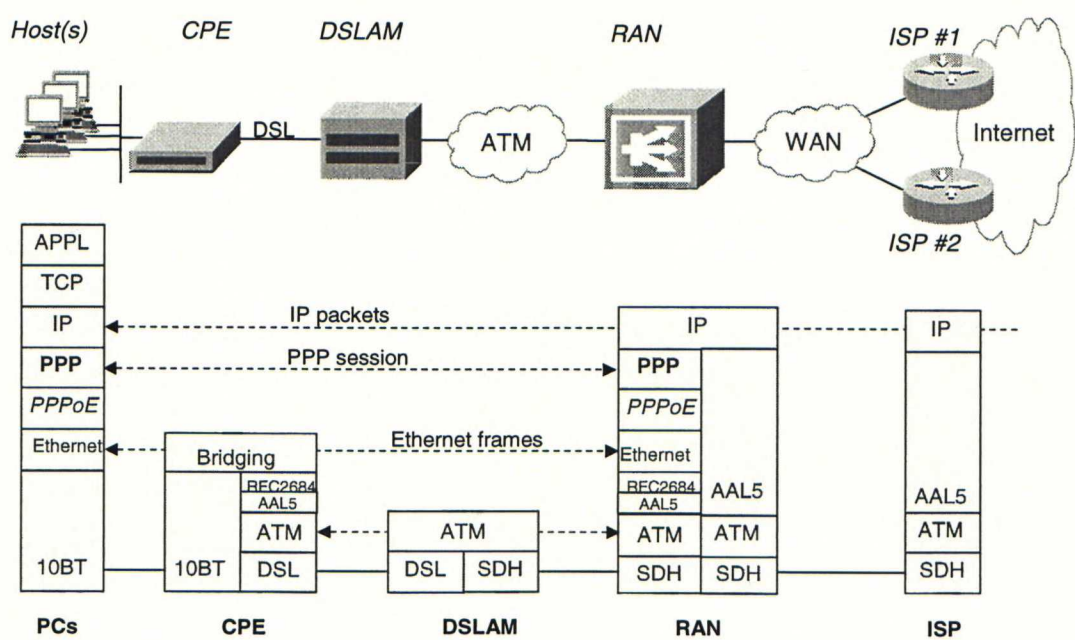


Figure 9 Bridge with RFC 2516 PPP over Ethernet

The traffic is transmitted so that the PPPoE defines how the PPP session is mapped into ethernet frames and the CPE doesn't handle the PPPoE packets at all. It just works as a bridge and the PPP session is from the client PC to the RAN that terminates the session and routes the traffic to ISP's network.

2.2.3 Router with RFC 2364 PPP over ATM

The NT as a router means that the traffic processing is based on the destination IP-addresses in the received IP-packets. The routing decision is based on the routing table. The routing table contains information about all the known networks. The networks can be learned dynamically eg via Routing Information Protocol (RIP) messages. In addition to this static routes may be used. Typically the NT has one default gateway to which all the IP traffic is forwarded if no specific network is found from the routing table. When acting as a router the NT has at least two different IP-networks, WAN and LAN, and the routing is done between them. In case both the wired and wireless LANs are used in the private side of the network, there can be

three different IP-networks: WAN in the xDSL side, LAN and WLAN. The protocol stack for the PPPoA case is shown in Figure 10.

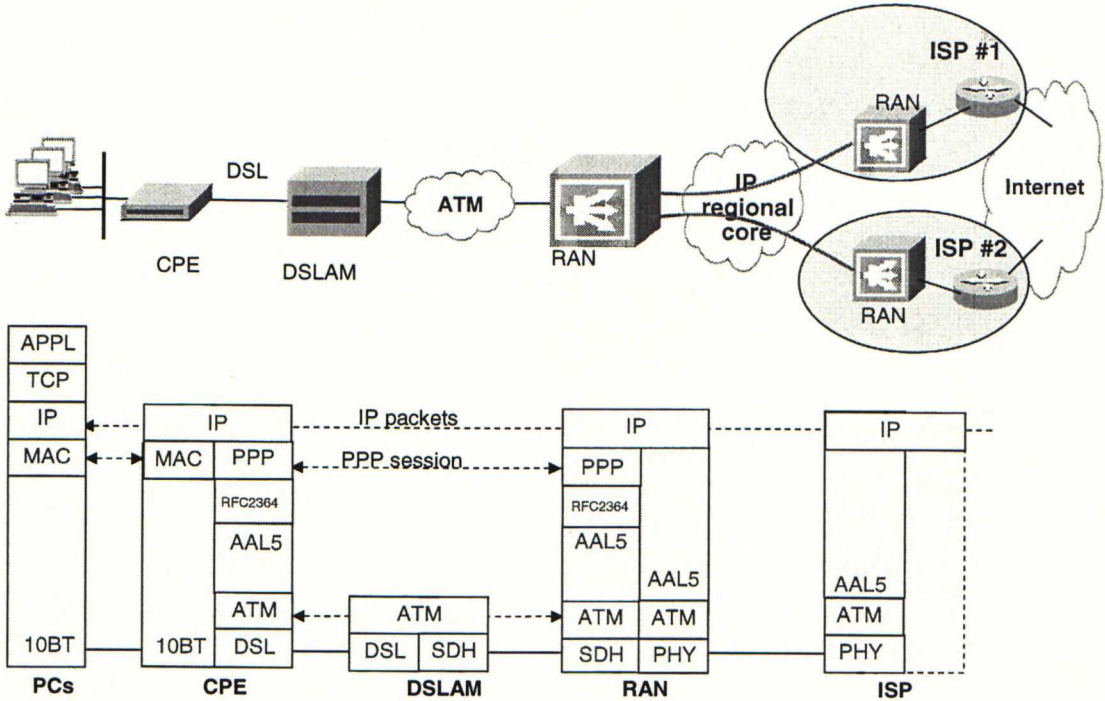


Figure 10 Router with RFC 2364 PPP over ATM

The NT can perform the routing also by using PPPoE encapsulation from the NT to the RAN. The service selection in the NT is possible when the PPPoA or PPPoE encapsulation is used. The PPP connection from the NT to RAN is established based on authentication. The username and password can determine to which ISP the connection is forwarded in the RAN, which enables the use of several ISPs for the end user. In addition to this it would be possible to use one or more PVCs in the NT for PPTP connections. By this way, again, while one or more family members can have tunneled PPP connections to their corporate's router for remote work the others are able to access the service providers.

In case of routing the NT typically performs several different tasks, like DHCP server or relay, Domain Name Server (DNS) or proxy and NAT. The use of the DHCP server enables dynamic host IP-addressing within the local network. When NT is configured as DHCP relay the DHCP server is located somewhere in the network and NT sends all DHCP messages received from the local network to the DHCP server. DNS proxy means that the DNS requests that are received from the local network's hosts are forwarded to the available DNS servers. When acting as a DNS

proxy the NT must know the DNS servers' IP-addresses that can be either statically configured or learned dynamically via PPP.

2.2.4 Router with RFC 2684 IP over ATM

The protocol stack in case of RFC 2684 IP over ATM encapsulation is shown in Figure 11.

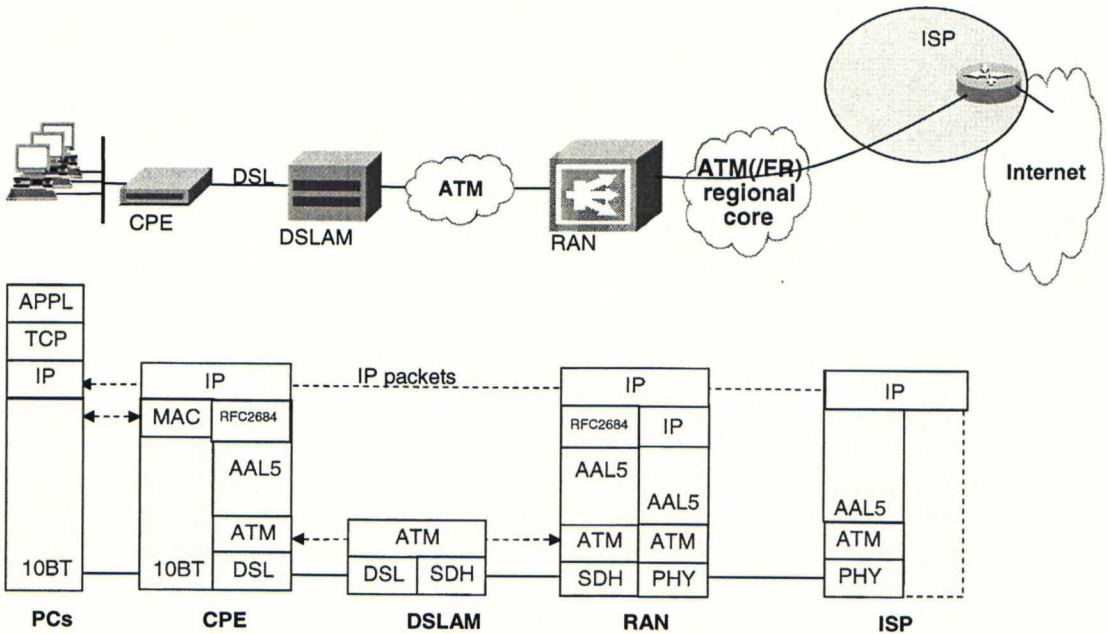


Figure 11 Router with RFC 2684 IP over ATM

When the NT acts as a router and uses the IP over ATM encapsulation the overall protocol stack is quite straightforward. The PPPoA offers dynamic IP-address management because the NT gets the IP-address for its WAN interface during the PPP-handshaking process. In case of IP over ATM the only way to take advantage of the dynamic IP-addresses for the NTs would be to configure the NTs as DHCP clients. However this functionality is just coming to the manufacturers' xDSL devices and also the RAN should support it. That's why it hasn't been used widely yet.

2.2.5 Conclusions

Considering the end-to-end protocol architecture, it can be notified that there are several different possibilities to build the access network. It is also possible to configure the NTs to use several ATM PVCs and to bridge or route traffic between those interfaces. So the possibility for misconfiguration is quite high. However when

the access network for the ISP or network operator is planned the configuration of the NT is made quite simple and easy to understand.

In case of the router it is possible to have own private LAN with private IP-addresses and also PPTP can be used. Typically the router employs also NAT and DHCP server functionalities. The service selection for the end user could happen, for example, by having a simple Web-based management connection from the PC to the NT. Then the end user could change the PPP username and password to choose between the different ISPs.

2.3 Applications

The broadband access network enables the use of different kinds of applications. This chapter describes briefly three typical applications: internet access for home users and remote work, internet access for small offices and LAN interconnection for branch offices. The focus is on the customer premises side of the network and NT's configurations are discussed. The configuration possibilities were already discussed with end-to-end protocol alternatives and this chapter gives only an overall picture of the configuration. The NT enables high-speed internet access for both the wireless and fixed LANs.

2.3.1 Internet Access for Home Users and Remote Work

NT in the broadband access network is suitable for high-speed internet access. In addition to the high-speed access, NT can have features that enable the remote work at the same time. The high-speed internet access can be achieved, for example, by configuring the NT as a router using RFC 2364 PPPoA encapsulation. The PPP link is in this case between NT and RAN. This enables the internet access for both the WLAN and LAN of the NT.

The remote work functionality can be added to the NT by using IP tunneling protocol like PPTP. Additional ATM VCC would be needed for the secured VPN connection for the remote work.

2.3.2 Internet Access for Small Offices

For small offices, NT with WLAN offers a quick way to get high-speed internet access. Wide coverage can be easily gained by using the WLAN. The internet

access can be gained by the same way as already mentioned in case of home users. For example, RFC 2364 PPPoA encapsulation can be used. Security aspects have to be taken into consideration especially in small offices. A basic level of security can be achieved by using the NAT. In the future more advanced firewall features will be added to NTs.

2.3.3 LAN Interconnection for Branch Offices

One possible application for NTs would be LAN interconnection for branch offices. The LAN interconnection can be easily achieved by using the RFC 2684 ethernet over ATM encapsulation. When the NT is a bridge, all network protocols can be used in the corporate network because bridge is transparent to all protocols that are run over ethernet.

3. XDSL AND ADSL

ADSL belongs to the group of xDSL technologies. These technologies have been developed to take advantage of the existing copper network. The American National Standards Institute (ANSI) first approved ADSL in 1995. The international ADSL standard was prepared by the ITU-T. The ITU-T standards for ADSL are most commonly referred to as G.lite (G.992.2) and G.dmt (G.992.1). These standards were approved in June of 1999. The ATM Forum has recognized ADSL as a physical layer transmission protocol for unshielded twisted pair. The DSL Forum was formed in December of 1994 to promote the DSL concept. The DSL Forum has members from many companies including service providers, equipment manufacturers and content providers. The ADSL and other xDSL technologies play a big role in the broadband access network architecture. This chapter describes first the ADSL system in more details and then shortly other xDSL technologies. At the end of the chapter, the frequency usage of different xDSL technologies will be discussed.

3.1 ADSL System

3.1.1 Architecture

There are several organizations that have influenced the development of the ADSL end-to-end architecture. The major organizations are DSL Forum, ATM Forum, the Internet Engineering Task Force (IETF), the ITU, the ANSI, the European Telecommunications Standardization Institute (ETSI) and the Universal ADSL Working Group (UAWG). Figure 12 illustrates the ADSL reference model according to the standard T1.413 [ANSI T1.413 1998].

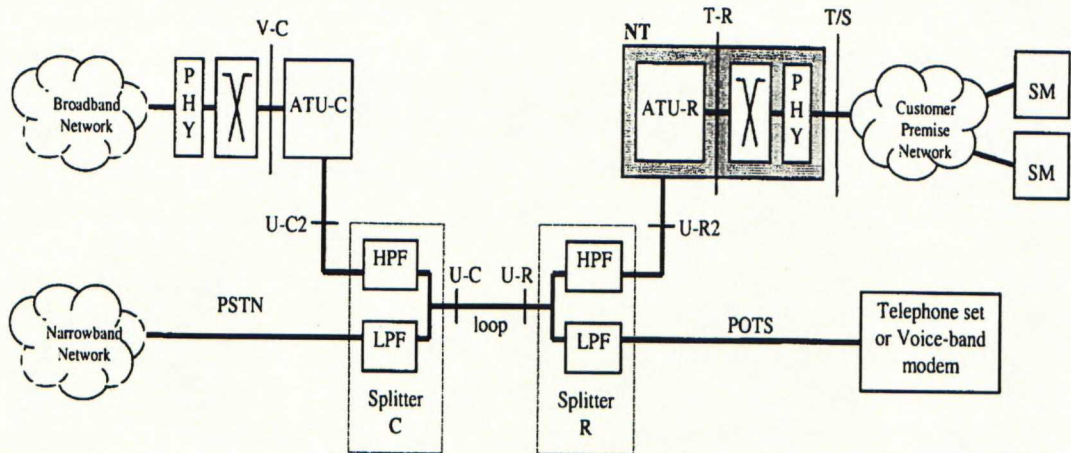


Figure 12 ADSL reference model [ANSI T1.413 1998]

The ADSL end-to-end architecture is formed from the different parts shown in Figure 11. The customer premises side is separated from the central office side. In the customer premises are the network terminals that terminate the ADSL connections. The local network in customer premises is connected to the network terminal. In the central office side, known as Central Office (CO), the ADSL connection is terminated in the DSLAM. The DSLAM multiplexes several ADSL connections. For example Nokia's D50e DSLAM for ETSI markets has 864 ADSL lines terminated when using four-port line cards. The DSLAM has the trunk connection towards the broadband backbone network. Typically this connection is Synchronous Transfer Mode 1 (STM1) that is 155 Mbps.

To be able to have the POTS operating simultaneously at the same twisted pair cable as the ADSL, separated splitters are needed. These splitters are needed both in the ADSL Transmission Unit-Central Office (ATU-C) side and also in the ADSL Transmission Unit-Remote (ATU-R) side of the network. Highpass filters are needed to filter the POTS traffic away for the ADSL part of the modem and lowpass filters to filter away the high frequency part for the traditional telephone. In the DSLAM the POTS traffic is separated from all ADSL lines and is forwarded to the narrowband network. In the future voice traffic may be transferred in the broadband network as well by using some voice over packet technique. In Figure 13, the ATU-R transmitter model is presented.

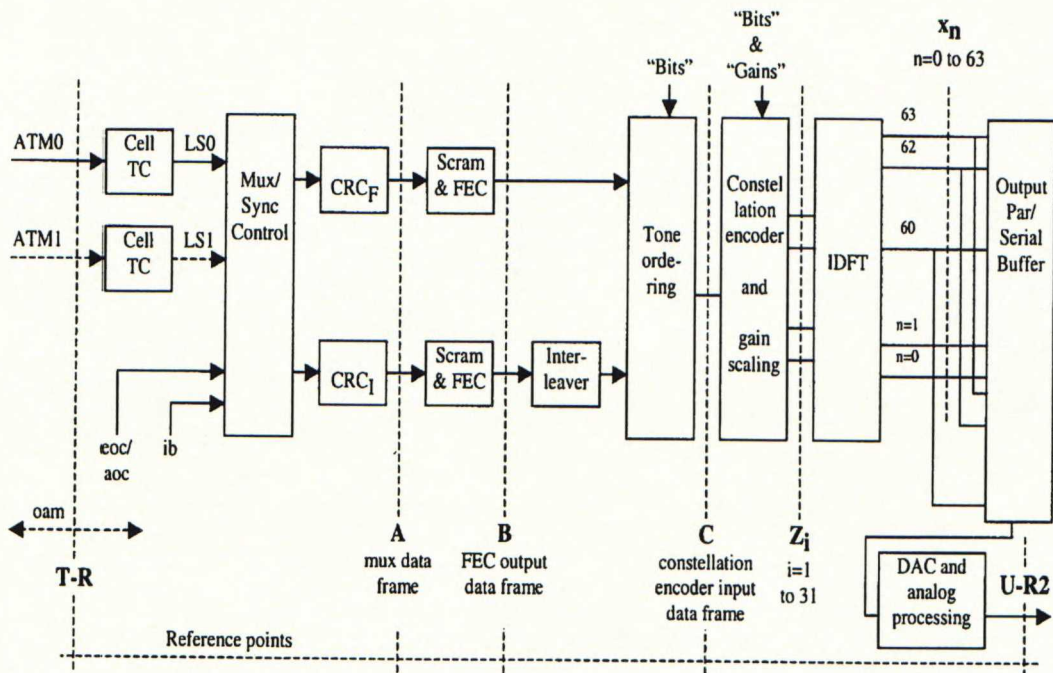


Figure 13 ATU-R transmitter model [ANSI T1.413 1998]

There are the different parts of the network terminal's transmitter in Figure 13. Figure 14 presents the ATU-R transmitter reference model for ATM transport. There are two ATM channels defined in the model, ATM0 and ATM1.

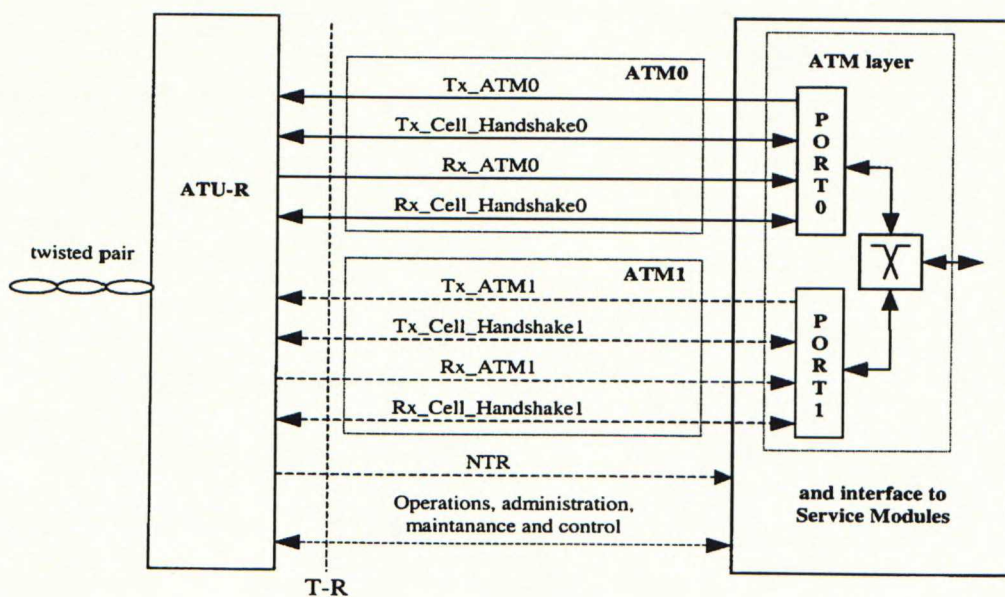


Figure 14 ATM transport model [ANSI T1.413 1998]

The ATM0 channel has to be provided always but the channel ATM1 is optional and may be provided for support of dual latency mode. ADSL systems transporting ATM

have to support bearer channel AS0 downstream and bearer channel LS0 upstream, with each of these bearer channels independently allocable to a particular latency path as selected by the ATU-C at start-up. Therefore, support of dual latency is optional for both downstream and upstream according to the standard. There is also a duplex interface for operations, administration and maintenance (OAM) and control of the ADSL system. Network Timing Reference (NTR) information can be used between both ATUs [ITU-T G.992.1 1999].

The ATM cell stream is forwarded to the Cyclic Redundancy Check (CRC) block that is the first error check method applied in the system. The CRC is generated for each ADSL superframe separately. The CRC codeword concerning ADSL superframe is transmitted in the first frame of the following superframe. Eight bits per buffer type (fast or interleaved) per superframe are allocated to the CRC check bits [ANSI T1.413 1998]. After CRC, scrambling and Forward Error Correction (FEC) are done. The idea of the scrambling is that there wouldn't be too many zeros or ones sequentially, because this might cause DC to the digital-to-analog converters.

After the scrambling of the ADSL superframe is done, the data is forwarded to the FEC coding block. Error correction method is needed because the line condition of the ADSL line can vary quite a lot, so the Signal-to-Noise Ratio (SNR) can change during the transmission. The Bit-Error Rate (BER) of 10^{-7} is typically the definition for errorless transmission and this should be guaranteed. FEC coding uses the Reed-Solomon coding method. It would also be possible to use the Trellis coding. In the FEC coding the purpose is to add redundancy into the bit-stream and then the receiver can check the FEC overhead and correct the corrupted data bits. The Reed-Solomon coding is one form of blockcoding. The Trellis coding is a convolution coding. Both of these methods are applied to achieve coding gain for the data, to reduce the probability of corrupted data that can not be corrected. Both of these coding methods are generally used.

The FEC-coded bitstream is interleaved in the interleaving block of the transmitter. The errors in the ADSL line appear typically in bursts. For this reason the interleaving is applied. In the interleaving the data is rearranged to wider area so that the error bursts are easier to correct in the receiver.

The interleaved coded data is then forwarded to the tone-ordering block. Figure 15 illustrates the tone ordering method [ANSI T1.413 1998].

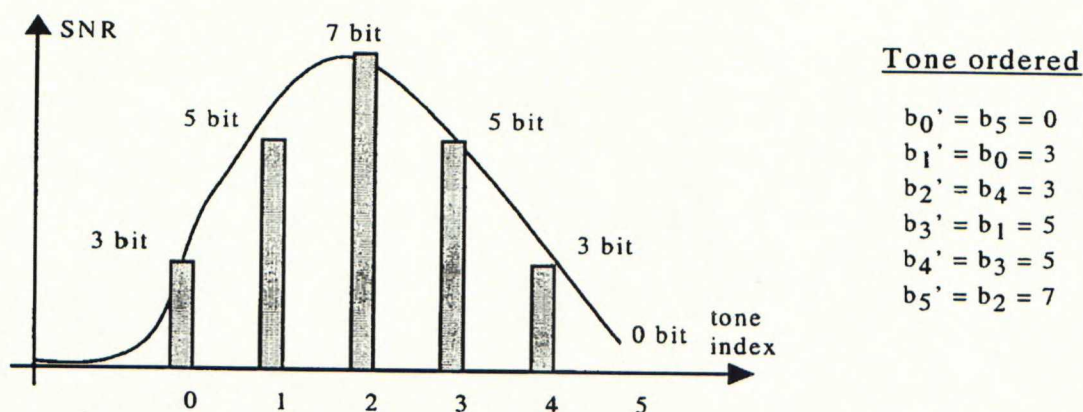


Figure 15 Tone ordering [ANSI T1.413 1998]

In the tone ordering block the transmitted bits are allocated to the appropriate subcarriers according to the signal-to-noise ratios of each subcarrier. The SNRs of tones are calculated in the initialization procedure of the ADSL connection. The subcarriers with high SNRs will get more bits than the subcarriers with lower SNRs. The tone ordering shall first assign all the bits from the fast buffer to the tones with the smallest number of bits assigned to them, and then assign all the bits from the interleaved buffer to the remaining tones. All tones should then be encoded with the number of bits assigned to them. It's then possible that one tone have a mixture of bits from the fast and interleaved buffer [ANSI T1.413 1998].

3.1.2 Frame Structure

ADSL uses the superframe structure shown in Figure 16. Each superframe is composed of 68 data frames numbered from 0 to 67. Data frames are encoded and modulated into Discrete Multi-Tone (DMT) symbols followed by a synchronization symbol. Synchronization symbol carries no user or overhead bit-level data and it is inserted by the modulator to establish superframe boundaries. From the bit-level and user data perspective, the DMT symbol rate is 4000 baud (period = 250 μ s), but in order to allow the insertion of the synchronization symbol the transmitted DMT symbol rate is $69/68 \times 4\,000$ baud [ITU-T G.992.1 1999].

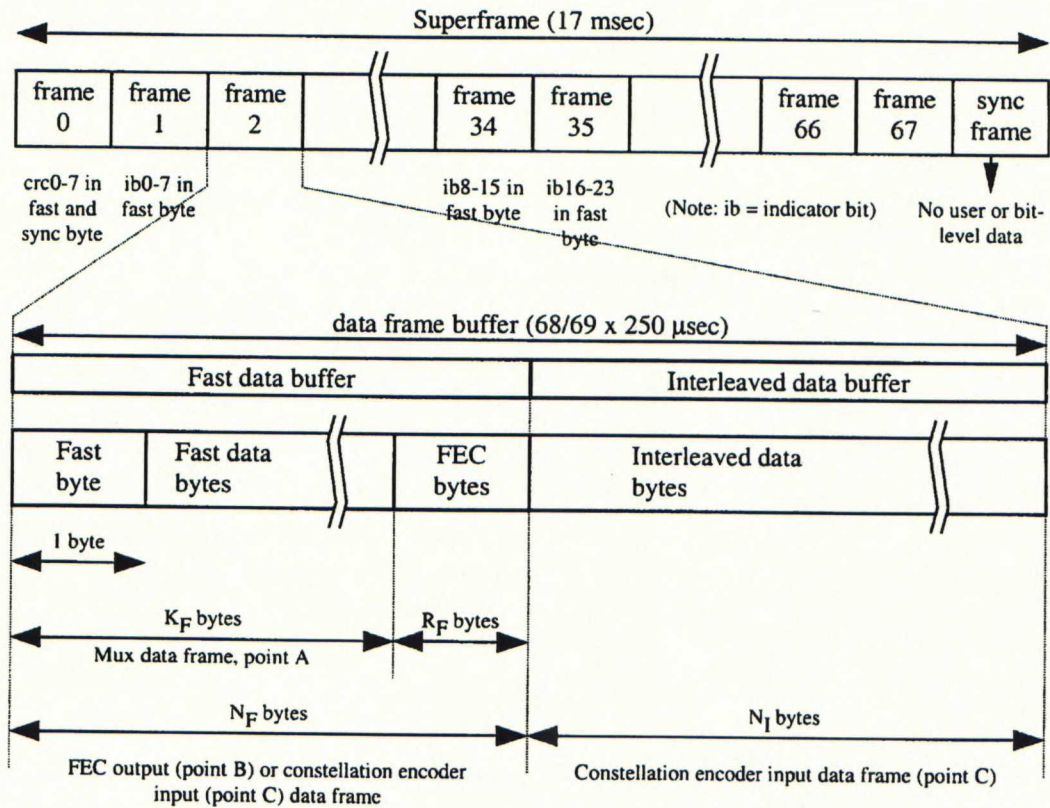


Figure 16 ADSL superframe structure [ANSI T1.413 1998]

Each data frame within the superframe contains data from the fast buffer and the interleaved buffer. The size of each buffer depends on the assignment of bearer channels made during initialization [ITU-T G.992.1 1999].

3.1.3 DMT Operation

The standardized method for modulation in the ADSL system is the DMT modulation. In DMT modulation the data is encoded into many narrow subcarriers. There are overall 256 subcarriers in the ADSL. All the subcarriers are spaced at 4,3125 kHz. The first method for modulation in ADSL was Carrierless Amplitude and Phase (CAP) but nowadays the DMT has gained more popularity [Ginsburg 1999].

There are two types of DMT operation modes, Frequency Division Multiplexing (FDM) and echo cancellation. FDM is the commonly used one. Figure 17 illustrates the frequency range of the ADSL based on FDM. The lower end tones are reserved for upstream transmission. The POTS band is from 0 up to 4 kHz and the bin 0 is used by POTS traffic. The ADSL bandwidth starts from 25 kHz and extends to the 1,1 MHz. The bins 5-31 (from 25 kHz up to 138 kHz) are reserved for upstream

traffic. Correspondingly the bins 32-255 (from 138 kHz up to 1,1 MHz) are reserved for downstream traffic.

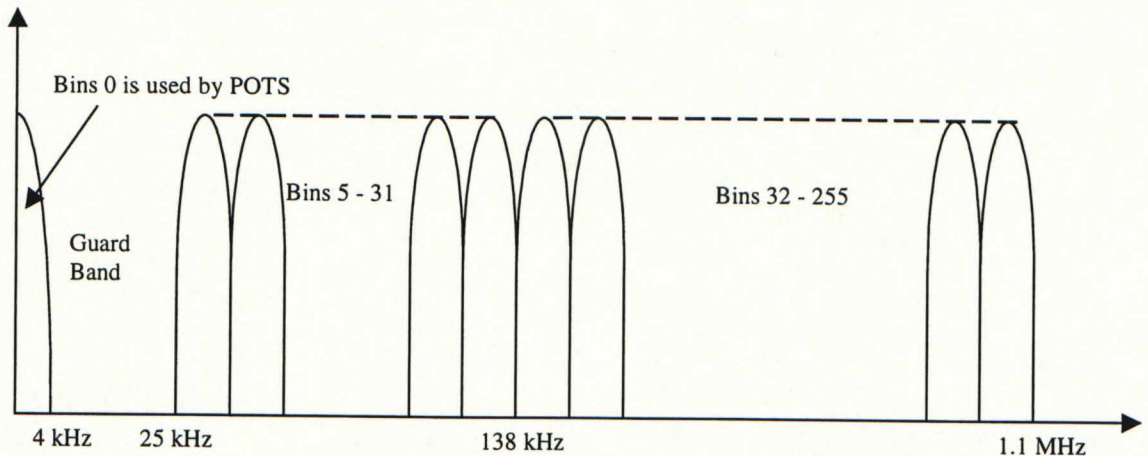


Figure 17 ADSL frequency range

The subcarriers may be modulated by different bit density depending on line noise. The maximum bit density is 15 bits/sec/Hz. In case the interference on some subcarrier is high, the subcarrier may be shut down. The DMT modulation uses the Inverse Discrete Fourier Transform (IDFT) for modulation of the data in each subcarrier. The constellation size may vary up to 256 points. The ITU-T has also defined the splitterless standard G.992.2 (G.lite) that uses only the first 128 subcarriers at corresponding decrease in bandwidth [Ginsburg 1999].

The decision of the amount of bits assigned per subcarrier is made during the ADSL initialization phase. The ATU-C and ATU-R determine the available bit rate depending on the line condition. When both ends start to initialize the link they exchange information regarding the throughput and reliability of the link. After transceiver training and channel analysis, they are ready to exchange detailed information regarding the number of bits and power levels to be used on each DMT subcarrier [ITU-T G.992.1 1999]. The G.dmt standard defines also the Rate-Adaptive mode for ADSL (RADSL). This means that when line conditions change the modem and the corresponding line card in central office side of the network will negotiate the link dynamically without noticeable interrupt for the end user [Ginsburg 1999].

The rate adaptivity of the ADSL means that the available bit rate depends on line conditions and the configured parameters. In the central office side of the network,

there are noise margin parameters in the DSLAM. These noise margin configurations are taken into account when the available bit rate is determined by the ATUs. Three different noise margin parameters can be configured in the DSLAM. These are target noise margin, maximum noise margin and minimum noise margin. All noise margins should be controlled to ensure a BER of 10^{-7} (= 0 dB margin) or better (> 0 dB margin). Target noise margin specifies the noise margin a modem has to achieve to a BER of 10^{-7} . This is seen by the modem with respect to its received signal. For example target noise margin of 6 dB can be used, which means that the BER of 10^{-7} is guaranteed even though the noise in the line increases 6 dBs. Minimum noise margin specifies the margin a modem shall tolerate relative to a BER of 10^{-7} . If the current noise margin falls below this level, the modem shall attempt to increase the far-end output power to get a noise margin above this limit. Maximum noise margin is the noise margin top of the target noise margin the modem shall tolerate relative to a BER of 10^{-7} . If the current noise margin is above this limit, the modem shall attempt to reduce the far-end output power to get a noise margin below this limit. The capacity of RADSL is from 32 kbps up to 10 Mbps in downstream and from 32 kbps up to 1 Mbps in upstream depending on the line conditions. The rate can be adaptively changed in steps of 32 kbps [Alcatel 2000].

3.2 Other xDSL Technologies

Other xDSL technologies are ADSL over ISDN, High-Speed Digital Subscriber Line (HDSL), Symmetric Digital Subscriber Line (SDSL) and ETSI SDSL, Single-Pair High-Speed Digital Subscriber Line (SHDSL), Very High Speed Digital Subscriber Line (VDSL) and Integrated Digital Subscriber Line (IDSL). Each of these technologies has their own special features. The other xDSL technologies are shortly described in this chapter. Different standard bodies and forums take part in the development of the xDSL standards and specifications.

3.2.1 ADSL Over ISDN

The ITU-T standard for ADSL (G.992.1) defines in its annex B the usage of ADSL over ISDN. The main difference compared to the ADSL over POTS that is defined in the annex A is the used frequency range in low frequencies allowing the operation of the ISDN at the same time. The Power Spectral Densities (PSD) of ATU-C and ATU-R transmitters are described in the standard [ITU-T G.992.1 1999].

ADSL over ISDN is designed for the same kind of broadband services as ADSL over POTS. Asymmetrical high-speed internet access can easily be obtained especially for home users because then higher transmission bandwidth is needed in downstream direction than in upstream direction.

3.2.2 HDSL and HDSL2

HDSL is a bi-directional symmetric transmission system that allows the transport of T1 (1.544 Mbps) and E1 (2.048 Mbps) signals. HDSL is based on ETSI standard TS 101135. HDSL transmission can employ either 2B1Q or CAP modulation methods. In HDSL the signal is transmitted on a single pair or parallel on two or three pairs. The transmission on three pairs is provided by three parallel HDSL transceivers, each operating at 784 kbps, resulting 2352 kbps bit rate. Transmission on two pair is provided by two parallel HDSL transceivers, each operating at 1168 kbps, resulting bit rate of 2336 kbps. Transmission on one pair is provided by one HDSL transceiver operating at 2320 kbps. The HDSL is symmetrical and so it's possible to have the same transmit rate for both downstream and upstream directions. In practice the HDSL technology is mostly utilized by using two parallel pairs for transmitting of T1 and E1 signals [ETSI TS101135 1999].

The newer form of the HDSL technology is the HDSL2 that operates over one copper pair. HDSL2 has been standardized by ANSI and it is designed to transmit the T1 signals. HDSL2 is aimed to be spectrally compatible with other services on adjacent cable pairs. Improved spectral compatibility was one of the key drivers for the new HDSL2 standard. In the HDSL2, improved modulation and coding techniques are used to limit the transmit spectrum and assure spectral compatibility with ADSL [Quilici 2001].

HDSL technology can offer high-speed internet access also for servers, not just for clients because of the symmetric data transmission. High bit-rate can be used in both directions. It's also possible to take advantage of the HDSL technology in LAN extensions, video conferencing and distance learning applications, extending central Private Branch Exchanges (PBX) and transporting E1 and T1 traffic.

3.2.3 SDSL and ETSI SDSL

SDSL provides different data rates up to 2,320 Mbps. SDSL has fixed data rates that are 192, 384, 768, 1152, 1536 and 2320 kbps. SDSL uses the 2B1Q line coding. The SDSL products that are in the market are based on HDSL technology or they are manufacturers' proprietary solutions. The 2B1Q modulation used in many proprietary SDSL systems has a severe interference with ADSL when deployed at data rates above 784 kbps. The SDSL operates without the presence of POTS signal. The voice must then be carried by using some other method. SDSL is not a standardized technology and in the future operators and equipment manufacturers are going to use the ITU-T standard G.SHDSL.

ETSI has also made efforts on standardizing the SDSL technology. ETSI defines in the technical specification TS 101524 the functional requirements of SDSL access transmission based on metallic access cables. According to the TS 101524, the SDSL uses echo cancellation method to provide digital access over existing, unshielded wire pairs. The maximum bit-rate of the ETSI SDSL is same as with HDSL, HDSL2 and SDSL technologies, 2320 kbps [ETSI TS101524 2000].

SDSL is considered to be used mainly by business customers as it provides symmetric data rates. In practice same kind of applications can be offered with SDSL than with HDSL.

3.2.4 G.SHDSL

The G.SHDSL has been specified on the basis of HDSL2 and ETSI SDSL. The standard G.SHDSL uses the same signal modulation and data encoding techniques as HDSL2. SHDSL transceivers are capable of supporting selected symmetric user data rates in the range of 192 kbps to 2312 kbps by using a Trellis Coded Pulse Amplitude Modulation (TC-PAM) line code. They are designed to be spectrally compatible with other transmission technologies deployed in the access network, including other DSL technologies.

The G.SHDSL is standardized by the ITU-T and it will replace the SDSL that has been used as proprietary solutions by different companies. The SHDSL standard is based on the ANSI HDSL2 standard that is aimed for North American markets. SHDSL transceivers do not support the use of analog splitting technology for coexistence with either POTS or ISDN. G.SHDSL standard specifies regional

requirements, including both operational differences and performance requirements, for North America and for Europe [ITU-T G.991.2 2000].

3.2.5 VDSL

The VDSL is supposed to be a functional technology for the market area in the future. VDSL provides bit rates up to 52 Mbps. Very high bit rates can be used for short distances only. There is not just one line coding that can be used in the implementation of the VDSL technology. Two different modulations, Quadrature Amplitude Modulation (QAM) and DMT can be used. Nokia for example uses in its VDSL modem the QAM modulation at the moment. VDSL uses 2-wire copper lines and allows simultaneous use of POTS or ISDN. Standardization of VDSL is going on. According to the ETSI TS 101270, the VDSL is required to co-exist with some existing narrowband services that may be carried on the same wire-pair. This is to ensure that the VDSL system can provide a broadband overlay capability [ETSI TS101270 1999]. VDSL is mainly targeted for broadband application like High-Definition Television (HDTV).

3.2.6 IDSL

IDSL technology reuses the ISDN 2B1Q line encoding for permanent connectivity. ISDN has two B channels for data transmission (64 kbps both) and one D channel (16 kbps) for signaling. The D channel is also used by IDSL so the maximum transmit rate is 144 kbps. The IDSL is a kind of permanent version of ISDN and it's mainly used in the North America.

3.3 Frequency Usage of xDSL Technologies

As the unbundling of the local loop in European countries becomes a reality, and as the xDSL family grows daily, compatibility limitations may arise between transmission systems connected to wire pairs in the same access network cable (i.e. in the same bundle) and possibly between different (competing) network operators. A mixture of transmission technologies is now likely to share the same cable bundle or binder group and compatibility issues related to the used frequency bands, the power transmitted and the duplexing approach between different systems could prevent the most efficient use of the spectral capacity of those cables [ETSI 1999].

The different xDSL systems employ different frequency ranges. Figure 18 gives an overall picture of the frequency usage of xDSL technologies. The figure is very much simplified from the real PSD figures of different xDSL techniques. Exact frequency limitations can be found from the standards.

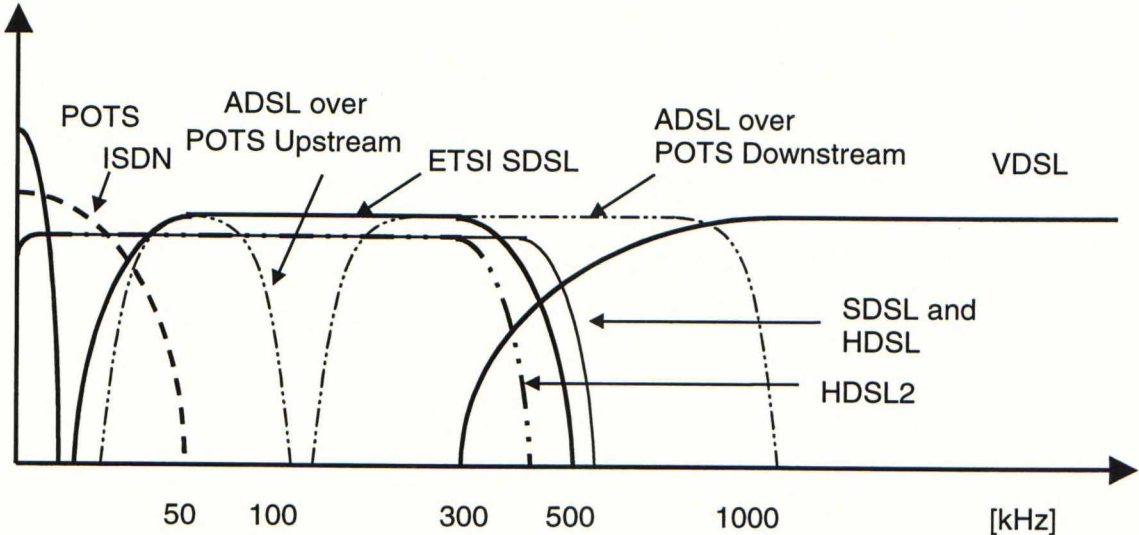


Figure 18 Frequency usage of xDSL technologies

It can be seen from the figure that the different xDSL technologies can have crosstalk effects on each other. HDSL and SDSL technologies cause interference to ADSL, which must be taken into consideration by network operators when making use of different xDSL technologies in same cable bundles. It must be noted that there are several aspects that affect the interference of different technologies like used transmission powers, Near-End Crosstalk (NEXT) effects and Far-End Crosstalk (FEXT) effects.

In general it can be said that the basic HDSL technology by using one copper pair has severe interference affect on the ADSL technology. HDSL and proprietary SDSL have wider bandwidth than the HDSL2 and also the interference effects are more severe. ETSI SDSL and G.SHDSL, that is not in the figure, also uses quite much the same bandwidth as do ADSL, however they are still designed to be spectrally compatible with ADSL. This frequency review of xDSL techniques is very much simplified from the real life situation and a detail examination doesn't belong to the scope of this thesis. There are many aspects that the network operators must take carefully into consideration.

4. WIRELESS LAN STANDARDS

The second generation mobile communications systems have gained popularity worldwide. The most common second generation system has been Global System for Mobile Communications (GSM) in Europe and its competitors around the world: IS-95 in the North America and Personal Digital Communication (PDC) in Japan. The third generation mobile communications systems like Wideband Code Division Multiple Access (WCDMA) have been developed to meet the higher requirements of the wireless data transmission. At the same time different kinds of wireless LAN solutions have been developed for local coverage and to offer high bit-rates. The main purpose of wireless LANs have often been to replace the existing cabling and to offer data transmission regardless of time and place. Considering new installations the wireless LANs offer many advantages compared to the old wired infrastructure. In next chapters different standardized WLAN technologies will be presented.

4.1 IEEE 802.11

IEEE 802.11 is a standard that specifies the physical and MAC layers for wireless local area network. The standard was ratified in June 1997. Newer version of the standard is the edition 1999 that was ratified in August 1999. IEEE 802.11 defines three different radio technologies for physical layer. These are Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Infrared (IR). Infrared is specified in the standard as optional technology. All these physical layers use the same medium access control method, Carrier sense Multiple Access with Collision Avoidance (CSMA/CA). The radio channel uses the unlicensed Industrial, Scientific and Medical (ISM) band that is in the frequency range from 2.4 GHz up to 2.4835 GHz.

There are two extensions for the IEEE 802.11 standard, IEEE 802.11a and IEEE 802.11b. IEEE 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) modulation and it allows data rates up to 54Mbit/s. The system uses 52 subcarriers that are modulated using binary or quadrature phase shift keying, 16-QAM or 64-QAM. The system is aimed for the 5 GHz frequency band [IEEE 802.11a 1999]. IEEE802.11b, also known as IEEE 802.11 High Rate, was ratified in September 1999 to provide higher bit rates for the radio channel compared to the first version of the standard. IEEE 802.11b supports data rates of 1 Mbps, 2 Mbps, 5.5 Mbps and 11

Mbps. There has been demand for high bandwidth for the wireless LAN and IEEE 802.11b provides bandwidth wide enough for most broadband applications. IEEE 802.11 standard is presented in more details in chapter 5.

4.2 HIPERLAN

ETSI Broadband Radio Access Networks (BRAN) Project has defined High Performance Radio Local Area Networks (HIPERLAN) type 1 and HIPERLAN type 2 standards for wireless LANs. HIPERLAN/1 standard's functional specification was defined in July 1998 (EN 300652). As a follower for type 1 standard ETSI BRAN has defined the new standard HIPERLAN/2. The system overview was defined in February 2000 (TR 101683). The first release of HIPERLAN/2 standard was published in April 2000.

HIPERLAN/1 standard specifies a high rate radio LAN communication between devices. It supports bit rates up to 24Mbit/s and operates in the 5GHz frequency. HIPERLAN/2 standard operates on the same frequency and supports bit rates up to 54Mbit/s. HIPERLAN/2 defines specifications for interfaces to 3rd generation mobile communications systems. Supports for radio-access and interfaces for IP- and ATM-networks are specified. In next chapter HIPERLAN/1 is shortly covered and then HIPERLAN/2 is presented.

4.2.1 HIPERLAN/1

HIPERLAN/1 operates in the frequency range 5,15-5,30 GHz. This standard hasn't been very popular in the USA because it doesn't provide interoperability with IEEE 802.11 standard that is widely used in the North America. The standard covers OSI model's layers 1 and 2, the physical layer and the MAC layer.

HIPERLAN/1 uses 5 different frequency channels and it has been specified that all HIPERLAN devices shall use all of these channels for transmission. These channels are shown in Figure 19 as specified in the ETSI standard EN 3000652 [ETSI EN3000652 1998].

Carrier number, c	Centre Frequency, F(c) MHz
0	5 176,468 0
1	5 199,997 4
2	5 223,526 8
3	5 247,056 2
4	5 270,585 6

Figure 19 HIPERLAN/1 frequency channels

Gaussian Minimum Shift Keying (GMSK) is used as a modulation technique in HIPERLAN/1. GMSK is used for high rate transmission and for low rate transmission Frequency Shift Keying (FSK) shall be used. The definition for high rate transmission is 23,5294 Mbps \pm 235 bps. The definition for low rate transmission is 1,4705875 Mbps \pm 15 bps [ETSI EN3000652 1998].

Nowadays quite much attention is being paid to ETSI HIPERLAN/2 standard in the industry and it will be presented next.

4.2.2 HIPERLAN/2

HIPERLAN/2 operates in the 5GHz frequency band. HIPERLAN/2's specification is done in cooperation with other ETSI projects like UMTS and Third Generation Partnership Project (3GPP). This helps HIPERLAN/2 to be successful in the future [Johnsson 1999].

4.2.2.1 Networks topology

HIPERLAN/2 aims at providing high-speed multimedia connections between mobile terminals and different broadband networks. The standard defines also requirements for QoS issues. There are two different operating modes defined in the standard, centralized mode and direct mode. Direct mode means ad-hoc network where the wireless network is formed without a separate Access Point (AP). The centralized mode is respectively a network where every wireless station communicates with each other through an AP. Also connections to wide area network go through the AP.

4.2.2.2 Protocol layers

HIPERLAN/2 specifies three different layers, physical layer, Data Link Control Layer (DLC) and Convergence Layers (CL). The different layers are shown in Figure 20 [Johnsson 1999].

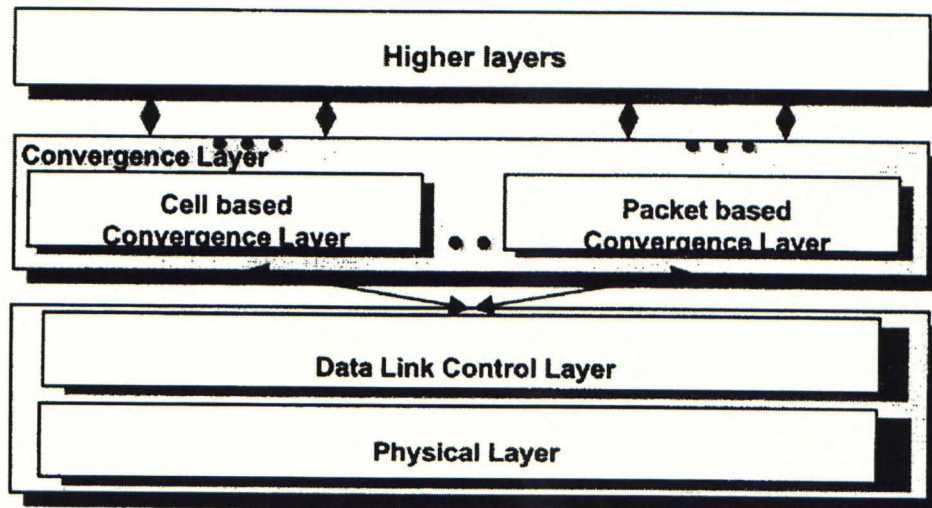


Figure 20 HIPERLAN/2 Protocol Layers

The DLC specifies the medium access method for HIPERLAN/2 air interface that is Time Division Multiple Access/Time Division Duplexing (TDMA/TDD). DLC defines also error control schemes and separate Radio Link Control (RLC) functions including for instance mobile terminal association, authentication and encryption key exchanges. HIPERLAN/2 modulates the radio signal to be transmitted with OFDM modulation, same as is used in the IEEE 802.11a standard. The radio range is usually from 30m up to 150m depending on attenuation and interference.

CL's function is to adapt core broadband network to the HIPERLAN/2 data link control layer. HIPERLAN/2's interoperability with different kinds of broadband core networks is based on several convergence layers for various core networks. Convergence layers are available for higher layer protocols like Ethernet, IP, PPP, Firewire, ATM and UMTS. These protocols form most popular network model techniques at the moment. Access interfaces for 3rd generation mobile communications systems have been developed. HIPERLAN/2 is also compatible with the WLAN technique that is being developed by the Multimedia Mobile Access Communications (MMAC) Association in Japan. The goal of HIPERLAN/2 is to provide air interface for several networks.

Physical layer takes care of the mapping of MAC protocol data units to physical protocol data units. Physical layer also adds necessary signaling information to the transmitted data. The HIPERLAN/2 transmitter's architecture is presented in Figure 21 [ETSI TR101683 2000].

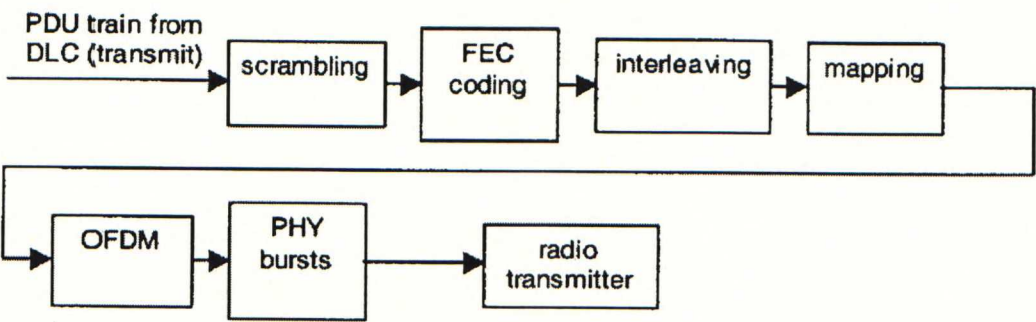


Figure 21 HIPERLAN/2 Transmitter

The necessary functional blocks are scrambling, FEC coding, interleaving, mapping, OFDM modulation and bursting. Table 1 shows the main differences between the ETSI standard HIPERLAN/2 and IEEE standard 802.11 [Dell 1999].

Table 1 Comparison of HIPERLAN/2 and IEEE 802.11

Characteristic	802.11	802.11b	802.11a	HiperLAN/2
Spectrum	2.4 GHz	2.4 GHz	5 GHz	5 GHz
~Max physical rate	2 Mb/s	11 Mb/s	54 Mb/s	54 Mb/s
~Max data rate, layer 3	1.2 Mb/s	5 Mb/s	32 Mb/s	32 Mb/s
Medium access control/Media sharing	Carrier sense-CSMA/CA	Carrier sense-CSMA/CA	Carrier sense-CSMA/CA	Central resource control/TDMA/TDD
Connectivity	Conn.-less	Conn.-less	Conn.-less	Conn.-oriented
Multicast	Yes	Yes	Yes	Yes
QoS support	PCF	PCF	PCF	ATM/802.1p/RSVP/DiffServ (full control)
Frequency selection	Frequency-hopping or DSSS	DSSS	Single carrier	Single carrier with Dynamic Frequency Selection
Authentication	No	No	No	NAI/IEEE address/X.509
Encryption	40-bit RC4	40-bit RC5	40-bit RC6	DES, 3DES
Handover support	No	No	No	No
Fixed network support	Ethernet	Ethernet	Ethernet	Ethernet,IP,ATM,UMTS,FireWire,PPP
Management	802.11 MIB	802.11 MIB	802.11 MIB	HiperLAN/2 MIB
Radio link quality control	No	No	No	Link adaptation

Two new variants are being developed for the HIPERLAN standard. HIPERACCESS is aimed to be a long-range variant intended for residential and

small business customers to access a wide variety of networks. The used frequency range would be 40.5 – 43.5 GHz band. First publications will be available in the first half of 2001. The other variant HIPERLINK will provide high-speed interconnection of HIPERLANs and HIPERACCESS. HIPERLINK will be operating in the 17 GHz frequency and it will provide data rates up to 155 Mbps over distances up to 150-meters [ETSI 2001].

4.3 Bluetooth

4.3.1 General information

Bluetooth Special Interest Group (SIG) is working on a specification for wireless communications. Bluetooth is more a kind of short-range radio link between two devices than a full WLAN technology. It has been developed to replace cables between different kinds of portable and fixed electronic devices. Bluetooth has become de facto standard in the telecommunications industry. The specification 1.0 of Bluetooth was released in July 1999. The purpose is to build Bluetooth on small integrated circuits and embed Bluetooth in different kinds of devices. Figure 22 illustrates the different kinds of connections that can be applied by using Bluetooth.

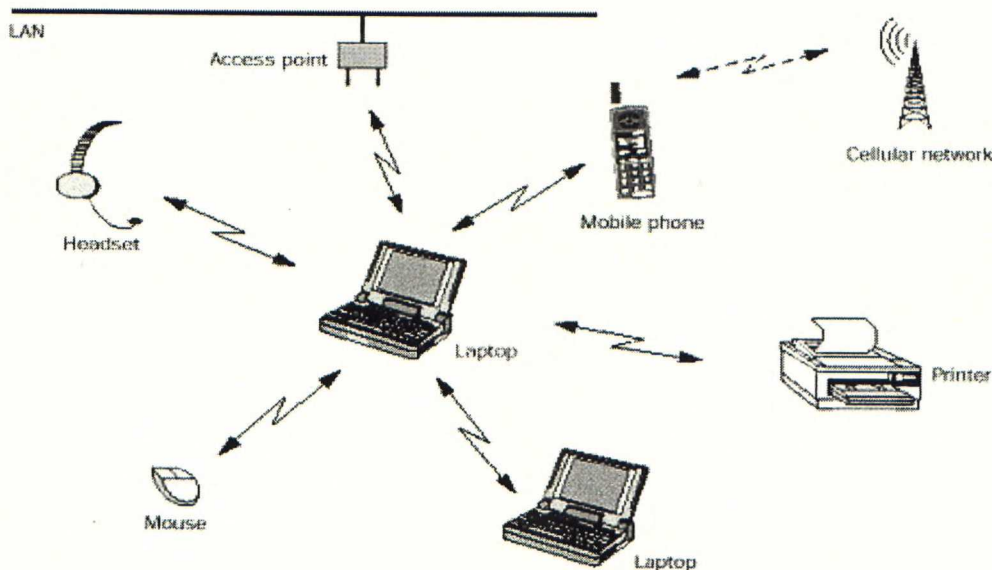


Figure 22 Bluetooth Connections

4.3.2 Network Topology

Bluetooth defines two different connection modes. These are point-to-point and point-to-multipoint connections. In the point-to-multipoint connection, the channel is shared between several terminals and a so-called piconet is formed. If the point-to-point transmission is used then there are two Bluetooth units. In the piconet one Bluetooth unit acts as a master unit while the others are slaves. There can be seven active units in the piconet. More slaves can be in a so-called parked state. These parked slaves are locked to the master and they remain synchronized to the master. The master unit controls the access to the piconet.

If several piconets exist with overlapping coverage, a scatternet is formed. Different hopping channels are used in different piconets and master in one piconet can be slave in another piconet. One slave can participate in several piconets on a time-division multiple basis, however different piconets are not synchronized with each other. In Figure 23 is scatternet that is formed by four separate piconets [Bluetooth SIG 1999].

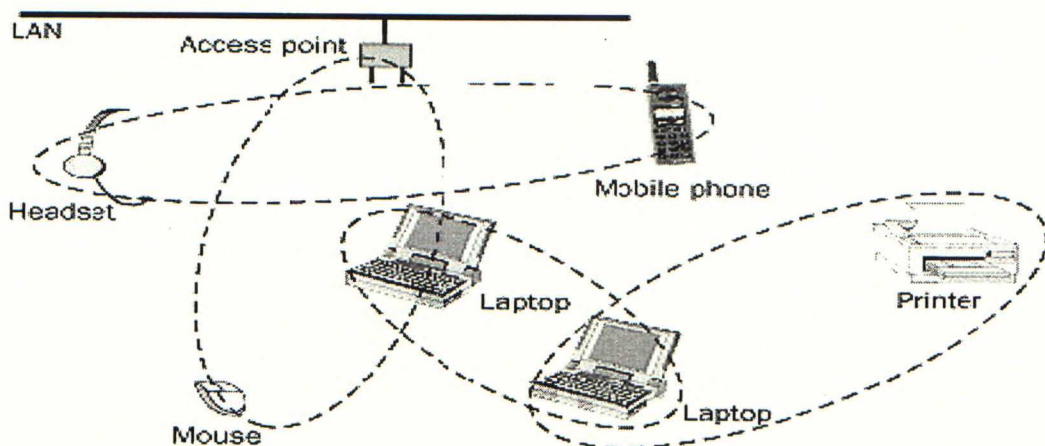


Figure 23 Bluetooth's Piconets and Scatternet

4.3.3 Radio channels

The Bluetooth operates in the 2.4 GHz ISM band. The unlicensed ISM band varies in different countries from 2400 to 2483,5 MHz. Because some countries have their own limitations for ISM band, different kinds of frequency hopping algorithms have been specified to overcome this problem. This means that the Bluetooth could be operational worldwide. Table 2 shows frequency ranges in different areas [Bluetooth SIG 1999].

Table 2 Bluetooth Frequency Ranges

Geography	Regulatory Range	RF Channels
USA, Europe and most other countries	2.400-2.4835 GHz	$f=2402+k$ MHz, $k=0,\dots,78$
Spain	2.445-2.475 GHz	$f=2449+k$ MHz, $k=0,\dots,22$
France	2.4465-2.4835 GHz	$f=2454+k$ MHz, $k=0,\dots,22$

There are proposals in different countries to extend national ISM bands. Harmonization of ISM bands in different countries would help the operation of wireless LAN technologies that operate in this band.

4.3.4 Physical Layer

Bluetooth uses both circuit and packet switching transmission methods. The Bluetooth protocol supports both synchronous voice and asynchronous data at the same channel. Asynchronous data can be transmitted at the separated channel and up to three simultaneous synchronous voice channels can be used. Voice channels support 64kbit/s synchronous transmission each, both in uplink and downlink directions. The asynchronous data channel supports transmission rate of 723,2 kbps in downlink and 57,6 kbps in the uplink direction. If data is transmitted in synchronous mode the available transmit rate is 433,9 kbps [Bluetooth SIG 1999].

In a piconet the master unit can establish two types of links. Synchronous Connection-Oriented (SCO) link is established between master and slave in point-to-point connection. Asynchronous Connection-Less (ACL) link is established between master and slaves in point-to-multipoint connection.

Bluetooth employs FHSS to spread the transmitted data to wide frequency range. Frequency hopping reduces attenuation and interference. TDD is used to transmit the data and the nominal slot length is 625 μ s. The data is transmitted in packets and each packet is transmitted on a different hop frequency. One transmitted packet can cover from 1 up to 5 time slots [Bluetooth SIG 1999].

A pseudo-random (PN) hopping sequence is used to spread the transmitted data over the available frequency channels. Each channel has 1MHz band and there can be from 23 up to 79 channels available depending on the country. In USA and Europe there are 79 channels available and in Japan, Spain and France 23

channels. In each piconet the master unit determines the PN- sequence and the clock phase to be applied. The hopping rate in Bluetooth is 1600 hops/s. In the piconet every unit must be time- and hop-synchronized to the channel to be able to communicate with each other. The transmitted data is modulated using Gaussian Frequency Shift Keying (GFSK) [Bluetooth SIG 1999].

Bluetooth defines three power classes for terminal equipment. Maximum output powers can be 20dBm (100mW), 4dBm (2,5mW) or 0dBm (1mW). The common approach is to use 1mW transmitting power.

4.3.5 Error Correction and Checking

In Bluetooth technology three error correction schemes can be applied, 1/3 rate FEC, 2/3 rate FEC and Automatic Repeat Request (ARQ) for the data. FEC can be used or not. If the FEC isn't needed it doesn't reduce the transmission throughput by giving overhead to the packets. 1/3 rate FEC code is used for the packet header by repeating the header bits three times. Rate 2/3 FEC is used to encode 10 information bits into a 15-bit codeword and it is used in different payload packets. ARQ enables the retransmission of packets if the payload field has errors [Bluetooth SIG 1999].

16-bit CRC code is used in the payload of the transmitted data to check whether there have been errors in the transmission or not. Header Error Correction (HEC) is also used to correct the errors of the packet header. HEC code is in the header field of the Bluetooth packet. Bluetooth defines both authentication and encryption methods to provide secured transmission and usage protection.

4.3.6 IrDA Interoperability

Bluetooth and Infrared Data Association (IrDA) technologies have presented the IrOBEX protocol that enables applications to use either the Bluetooth radio technology or the IrDA technology in the transmission. Both Bluetooth and IrDA are designed to be used in short range wireless communications but they have some fundamental differences in the physical layer protocols. The IrOBEX is mapped over the lower layer protocols of Bluetooth enabling applications to function over both Bluetooth and IrDA.

4.4 HomeRF

The HomeRF Working Group (HRFWG) has developed an open industry specification for wireless local area networks called Shared Wireless Access Protocol (SWAP). The SWAP specification 1.0 was ratified in January 1999.

4.4.1 Medium Access Method

The SWAP specification defines two different medium access methods for both voice and data communication. CSMA/CA has been specified for data traffic and TDMA for voice communications. IEEE 802.11 uses also CSMA/CA that is good for data transmission. The quality of voice transmission is guaranteed better by using TDMA. Those are the main reasons why HomeRF has decided to use both of these medium access methods in its SWAP specification. SWAP specification integrates parts of the IEEE 802.11 CSMA/CA and parts of the Digital Enhanced Cordless Telephone (DECT) standard. TDMA guarantees the latency and bandwidth requirements of real time voice transmission. Both circuit switching and packet switching are supported in the SWAP specification [HRFWG 2000].

4.4.2 Physical Layer

SWAP operates in the 2.4GHz ISM band as do IEEE801.11b and Bluetooth. The transmit power of devices using SWAP is 100mW. SWAP uses FHSS with a hopping rate of 50 hops per second. The modulation method is 2-FSK for data rate of 2 Mbps and 4-FSK for data rate of 4 Mbps. The specification defines the maximum number of devices that can be connected to the network, up to 127 devices are supported. For voice transmission there are 6 full duplex connections. The specification defines encryption methods and power management. In August 2000 it has been decided that the data rate of the SWAP specification will be increased to 10Mbps [HRFWG 1998].

According to the Federal Communications Commission (FCC) the FHSS transmitters operating in the 2.4 GHz band are allowed to use a minimum of 15 hopping channels, spanning a total of 75 MHz. The new rules will allow for hopping channels up to 5 MHz wide. The wider bandwidth will permit the HomeRF to provide higher data speeds. This will increase the HomeRF data speed up to 10Mbps [Federal Communications Commission 2000].

4.4.3 Network Topology

The specification defines two different network topologies, ad-hoc network and a managed network. The managed network has a connection point that coordinates the traffic between stations. The coordination is needed especially for voice transmission that is time critical. The connection point acts also as a gateway to public switched telephone network. Each network has a 24-bit identification code that enables the concurrent operation of multiple co-located networks. The frame structure supports both CSMA/CA and TDMA. The beacons sent by the connection point of the network advertise the used frame structure [HRFWG 1998].

Four different stations are specified to the SWAP network according to the specification. One is the connection point that supports both data and voice transmission. Second is a voice terminal that supports only voice transmission using TDMA that offers the real time transmission for voice. Third station can be a data terminal that supports only CSMA/CA method for data transmission. If both voice and data were needed then the fourth terminal type would be used. Fourth terminal type supports both TDMA for voice and CSMA/CA for data [HRFWG 1998].

4.5 IrDA

The IrDA is an organization that has developed standards for high-speed point-to-point connections. These standards specify a wireless short-range communication between two devices. The infrared data transfer can be used in line of sight case. There are several standards defined by IrDA that uses the same protocol stack with own special features. The different standards are IrDA 1.0, IrDA 1.1 and IrDA 1.2 for lower power. These standards are for different link distances and data rates. IrDA Control has been defined for command and control devices, IrTran-P for transferring of digital still images and IrMC for exchanging of objects in cellular phones.

4.5.1 Network Topology

The IrDA defines a network topology so that there are always a master unit and a slave unit in the network. The infrared communication is however between two devices only and that way it isn't a network in common sense. A network is defined basically as many-to-many communication but Infrared supports only point-to-point communications. The master unit is the control unit of the connection and it initiates the communication. The slave unit correspondingly sends response frames as the

master unit sends command frames to the slave. The IrDA standards specify that each unit can send information only 500 milliseconds at time and then it's the other unit's shift to send. The connection is a half-duplex connection but in some cases full-duplex communication can be simulated too. The definition of master and slave units is just the communication in the second protocol layer. It is invisible for the upper layers and the user don't know which unit acts as a slave. The connection initiation is the same for both master and slave, it is as easy for both parties [Megowan et al. 2000].

4.5.2 Protocols

The protocol stack of IrDA standards is shown in Figure 24 [Megowan et al. 2000] and different layers are next shortly discussed.

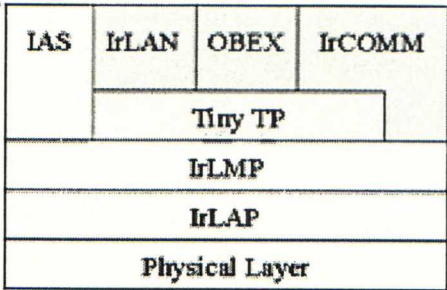


Figure 24 IrDA Protocol Stack

4.5.3 Physical Layer

The distance between two devices using Infrared can be from contact up to circa one meter but longer ranges are being developed. The data rate of Infrared connection can be from 9600 bps to 4 Mbps. IrDA is developing standard for up to 16 Mbps data rates. Physical layer error checking consists of 16-bit CRC for data rates up to 1.152 Mbps and 32-bit CRC for data rates up to 4 Mbps [Megowan et al. 2000].

4.5.4 IrDA Link Access Protocol (IrLAP)

Above of the physical layer is the IrLAP layer that establishes a reliable connection between two devices using infrared. IrLAP layer is according to the OSI model the data link control protocol layer. IrLAP layer provides retransmission, error detection and a low-level flow control. By this way a reliable connection is guaranteed. Two different operation modes are defined for the IrLAP layer, normal disconnect mode

and normal response mode. In the normal disconnect mode the unit must always listen if some station is transmitting before sending own data. The normal response mode defines the connection between devices using the best possible communication parameters [IrDA 1996].

IrLAP layer specifies three framing methods, asynchronous serial-IR framing for data rate of 9.6-115.2 kbps, synchronous serial-IR framing for data rate of 1.152 Mbps and synchronous 4-Pulse Position Modulation (4-PPM) framing. The basic operations for IrLAP layer are connection initiation, device discovery, data sending and disconnection [Megowan et al. 2000].

4.5.5 IrDA Link Management Protocol (IrLMP)

IrLMP provides the multiplexing of IrLAP layer. This means that it is possible to have many channels above of one IrLAP connection. The Information Access Service (IAS) is included in the IrLMP specification providing protocol and service discovery. The address conflict resolution is also included in the IrLMP specification. An addressing scheme is needed to be able to have many channels over IrLAP connection. The addressing differs from the TCP/IP port numbers that are fixed. In the IrLMP specification the addressing is done with logical service AP selectors that have fixed published names and the corresponding names are checked by the information access service [Megowan et al. 2000].

The IrLMP provides same kind of services as IrLAP services but they are now in the layer three. The IrLMP layer adds two additional bytes of control information to the IrLAP layer frames. The two bytes are used for identification of logical SAP selectors. Also the separation between control and data frames is done.

4.5.6 Optional Protocols

There are several so-called optional protocols in the IrDA specifications. The Tiny Transport Protocol (Tiny TP) is so essential that it could be a required protocol. The TinyTP provides a flow control for each IrLMP channel. Also the TinyTP protocol layer does segmentation and reassembly. IrCOMM specifies the serial and parallel port emulation over infrared. The IrCOMM enables different applications to run over infrared without any changes. IrOBEX is an object exchange protocol specifying the exchanging of information like files and graphics. The developing of OBEX standard is being done partly in cooperation with Bluetooth SIG. OBEX enables the

operations of Bluetooth and IrDA at the same environment without remarkable overlapping. IrLAN defines the local area network access for devices like laptops using infrared. IrDA Lite specification doesn't provide an additional protocol layer but it defines a way to implement the smallest possible infrared communication by modifying other protocol layers. The IrDA Lite limits other layers to get the protocol stack lighter [Megowan et al. 2000].

4.6 Conclusions

There are several WLAN technologies present in the market area of the WLAN-devices. There are fundamental differences between different technologies in the physical and MAC layers. The IEEE 802.11b, HomeRF and Bluetooth use the same 2.4GHz frequency band and IEEE802.11a and HIPERLANs use the 5 GHz frequency band. The CSMA/CA protocol is used by the IEEE 802.11b and partly by HomeRF. The TDD is used by HIPERLANs, Bluetooth and partly by HomeRF. The Bluetooth and IrDA differ from the others so that they are originally designed to be short-range links between two devices only. There are supporters and opponents for all these technologies. Because the IEEE 802.11b seems to have gained more popularity than the others have it will be presented in more detail in chapter 5.

5. IEEE 802.11/ 802.11B

This chapter covers the IEEE 802.11 standard for WLAN medium access and physical layer specifications. The standard has been developed by the Institute for Electrical and Electronic Engineers. The IEEE is based in the United States and it has over 320000 members in 150 countries. The IEEE 802 Local and Metropolitan Area Network Standards Committee is a major group that produces the series of standards known as IEEE 802.x. The first version of the standard IEEE 802.11 was ratified in June 1997 [Geier 1999]. The newer version was published in August 1999, it is the so called 1999 edition of the IEEE 802.11 standard.

The primary function of the 802.11 standard is to deliver MAC Service Data Units (MSDU) between peer LLCs. The LLC defines layer 2 synchronization and error control.

5.1 Industrial, Scientific and Medical (ISM) Frequency Band

Wireless products are authorized to operate in the ISM frequency band. The operation in this band does not require any licenses. The unlicensed frequency range encourages companies to develop WLAN techniques. The different unlicensed frequencies are shown in Figure 25.

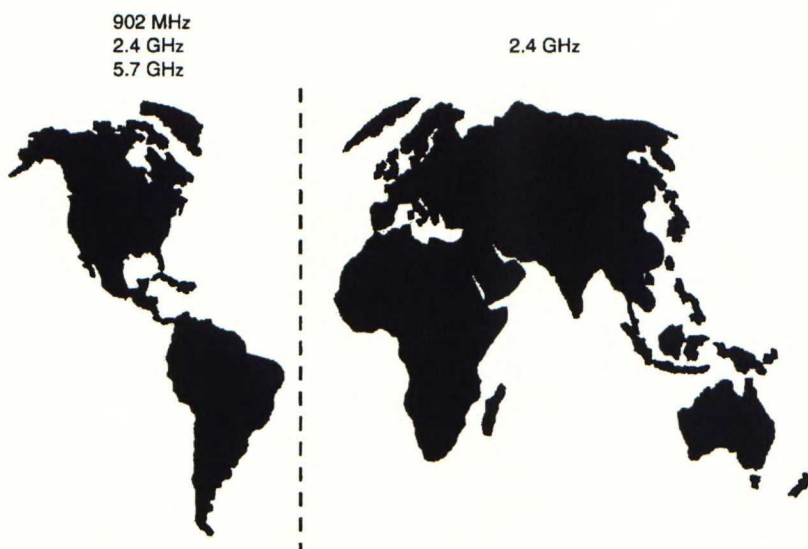


Figure 25 ISM Bands

One can see from the picture that the only unlicensed frequency that is accepted worldwide is the 2.4 GHz. This band was accepted in Europe and Asia in 1995 and in North and South America in the mid-1980s. The three unlicensed frequency bands are shown in detail in Figure 26.

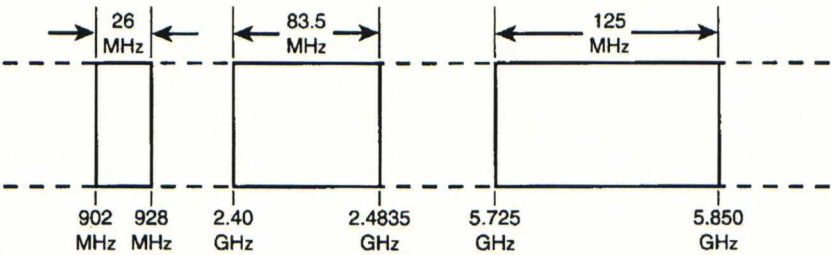


Figure 26 ISM Bands in Detail

The worldwide acceptance of the 2.4GHz frequency band has made many companies to develop products for that frequency. However higher frequency range would offer higher capacity and wider bandwidth. On the other hand it is often more expensive to develop products for higher frequencies and also the range of the radio signals might be shorter at higher frequencies.

5.2 Network Topology

There are two network topologies defined in the IEEE 802.11 standard. These are Independent Basic Service Set (IBSS) networks and Extended Service Set (ESS) networks. The network topologies are shown in Figure 27.

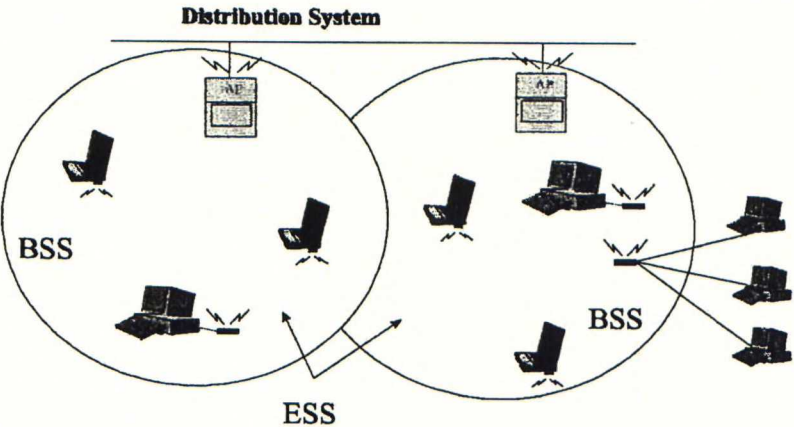


Figure 27 IEEE 802.11 Network Topology

The Basic Service Set network (BSS) is ad-hoc network consisting of at least two wireless stations. This kind of network doesn't have a backbone network at all. The another type of network, the ESS consists of several BSSs that are connected via APs. The ESS networks are also known as infrastructure networks because stations communicate with each other only through the AP. The BSS and ESS networks that are independent are transparent to the LLC layer of the network. The standard doesn't specify a mobile station transition between two ESSs [Geier 1999].

5.3 Logical Architecture

The logical architecture of the IEEE 802.11 standard is shown in Figure 28. The standard specifies three different physical layer techniques that are FHSS, DSSS and IR. Above of the physical layer is the MAC layer and above that the LLC layer. In chapter 5.4 the MAC layer is covered and the physical layer will be discussed in chapter 5.5.

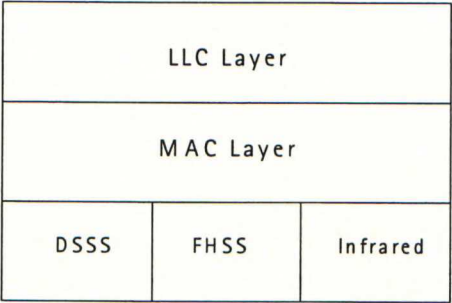


Figure 28 IEEE 802.11 Logical Architecture

The LLC layer provides communication in the layer 2 between two end-user stations as shown in Figure 29.

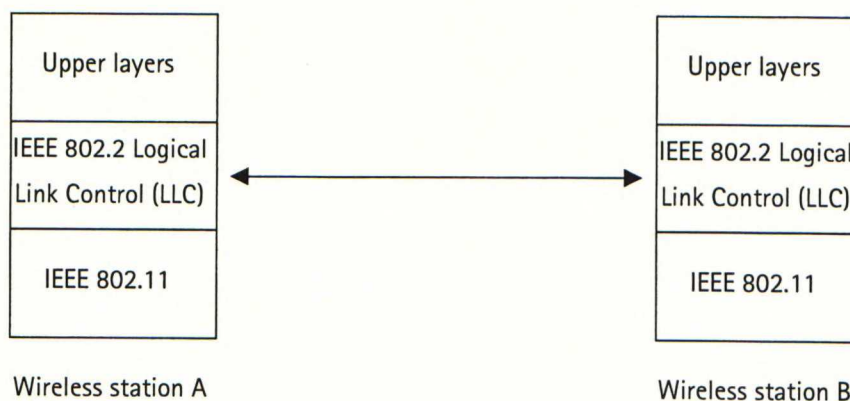


Figure 29 IEEE 802.11 Protocol Layers

Higher layers above of the LLC layers send data down to the LLC layer and expect error-free transmission to the destination. The LLC layer creates an LLC PDU by adding control header to the data packets. The PDU is then handed down through the MAC service access point [Geier 1999].

5.4 Medium Access Control (MAC) Layer

The primary functions provided by the MAC layer are accessing the wireless medium, joining a network and providing authentication and privacy.

5.4.1 Accessing the wireless medium

The standard defines two different coordination functions, Distributed Coordination Function (DCF) and Point Coordination Function (PCF). The primary access protocol is the DCF that uses the CSMA mechanism for sharing the wireless medium.

5.4.1.1 Distributed Coordination Function

The IEEE 802.11 uses the CSMA/CA method. The standard ethernet (IEEE 802.3) uses the CSMA with Collision Detection (CSMA/CD) method but a wireless LAN must avoid collisions, it can't detect them [Geier 1999]. To be able to detect collisions in a wireless environment, one would need a full duplex transmission method that is difficult and expensive to implement. In a wireless environment it can't be assumed that a station wanting to transmit is capable of hearing all other stations in the same coverage area. These are the main reasons why IEEE 802.11 uses CSMA with collision avoidance. The IEEE 802.11 MAC layer also performs

functions like fragmentation, packet retransmissions and acknowledgements, which is usually related to upper layer protocols.

The CSMA/CA works so that if a station wants to transmit, it first senses the medium. The station is allowed to transmit if the medium is free for a specified time. This time period is defined as Distributed Inter Frame Space (DIFS). In case the medium is busy the station defers by using the exponential backoff algorithm. This algorithm defines the method for waiting a time period before trying to transmit again. The station increases the maximum number of the random selection exponentially every time it has sensed the medium that has been busy. This method is also used after each retransmission and after a successful transmission. The receiving station sends to the transmitter an Acknowledge (ACK) frame every time after successful transmission. If the transmitting station doesn't get the ACK-frame it retransmits the frame. When a station wants to transmit data it first transmits a control packet called Request To Send (RTS). For this packet the receiver answers with a Clear To Send (CTS) packet. After receiving a CTS packet the station is allowed to transmit data. However it is also possible to send data without the RTS/CTS transaction, for example, in case of small packets. This is defined with RTS threshold value [IEEE 802.11 1999].

The standard specifies different spacing intervals. These intervals are shown in Figure 30.

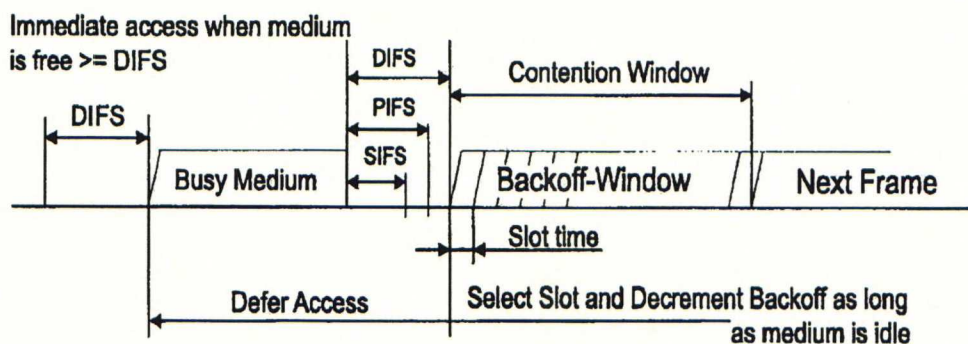


Figure 30 Different Spacing Intervals in IEEE 802.11

The time interval between frames is called the Interframe Space (IFS). The standard specifies four different interframe spaces. These intervals defer a station's access to the medium for different kinds of priority levels. The Short IFS (SIFS) is the shortest

time interval and it is used for ACK and CTS frames. The PCF IFS (PIFS) is used to gain priority access for stations operating under the PCF. DIFS is used for access for stations operating under DCF. The priority for DCF-based transmission is lower than for PCF-based transmission. The fourth interframe space is the Extended IFS (EIFS). It is used by all DCF-based stations as a waiting period whenever the physical layer has indicated to the MAC that a frame transmission, that did not result in the correct reception of a complete MAC frame with a correct FCS value, was begun [IEEE 802.11 1999].

The standard defines two ways for joining the network, passive scanning and active scanning. A station using the passive scanning listens to the radio channels for a specified time and waits for the transmission of beacon frames that have the Service Set Identifier (SSID) that the station wishes to join. In case of active scanning a station sends probe request frames indicating the wanted SSID and waits for the probe response frames from the AP [Geier 1999].

5.4.1.2 Point Coordination Function

In addition to the DCF the standard also defines the optional priority based PCF. The PCF provides contention-free frame transfer. The point coordinator controls the frame transmissions of the stations to eliminate contention for a specific time period. It can be used for services that require real-time transmission like voice and video. The PCF uses the PIFS interframe gap that is shorter than in the DCF function, which provides higher priority for stations under PCF. Both DCF and PCF can be used under the same BSS independently. In case of the PCF the AP of the BSS coordinates the medium access in the network. The AP uses a polling scheme to maintain the coordination of the medium access for the wireless stations in the BSS. The PCF can be used only in the infrastructure network mode [Geier 1999].

5.4.2 Fragmentation and Reassembly

The IEEE 802.11 standard defines the fragmentation and reassembly functions for the MAC layer. In general LAN technologies use quite long packet formats. However in the wireless environment there are many reasons for using shorter packets. The wireless transmission path has quite high bit error rate, which increases the probability of the packet to get corrupted in the radio channel. In case of high degree packet corruption it is reasonable to use smaller packets. Smaller packet size reduces the overhead if many retransmissions are needed. The MAC layer

fragments large packets, for example, from 802.2 LAN to smaller parts. The principle of the fragmentation is shown in Figure 31 [IEEE 802.11 1999].

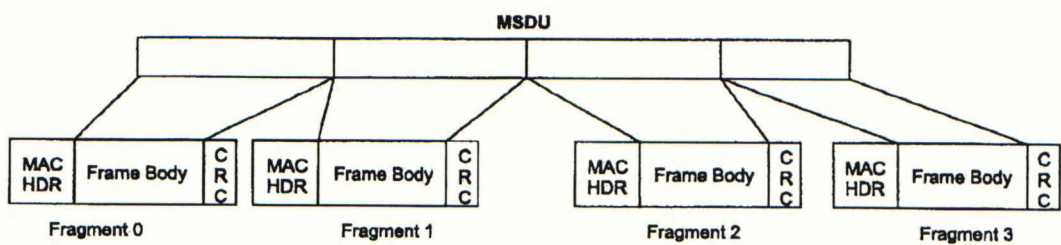


Figure 31 Fragmentation in IEEE 802.11

MAC layer receives the MSDUs from the LLC layer. If the length of the packet is greater than a fragmentation threshold limit, the MSDU will be fragmented into smaller MPDUs. By this way the probability of successful transmission is increased. Each transmitter in the network is capable of doing the fragmentation and each receiver can do the reassembly. Only unicast frames will be fragmented, not the broadcast and multicast frames. The MPDUs will be transmitted independently and each packet will be acknowledged separately.

There are several different MAC frames in the operation of the IEEE 802.11 compliant device. The overall frame structure is presented in Figure 32.

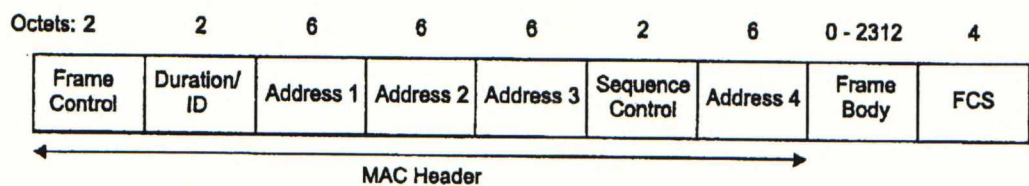


Figure 32 IEEE 802.11 MAC Frame Structure

The MAC frame consists of MAC header and frame body of variable length and FCS field. The frame control field carries information that has been sent from station to station. The duration field contains information about the duration of the next frame transmission, including both data and acknowledgement frames. Typically this field is used by stations to hold off transmissions based on the duration information. The four address fields' information depends on the specific frame types to be sent. Typically these addresses are Basic SSID (BSSID), source and destination addresses. The sequence control is the fragment number and each fragment of a

specific MSDU will have the same sequence number. The frame body field on the MAC frame contains the actual payload. The transmitter calculates the FCS using CRC and places the result in the FCS field. The transmission errors are then being checked by the receiver by calculating the CRC [Geier 1999].

The MAC frame's first field, the frame control field, is shown in Figure 33. The frame control field defines the various different MAC frame types that can be sent in the IEEE 802.11 wireless network.

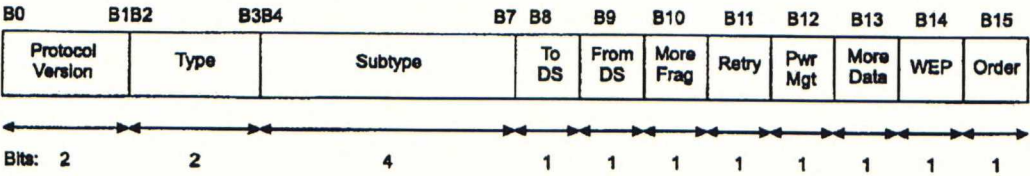


Figure 33 IEEE 802.11 MAC Frame's Frame Control Field

The protocol version field is currently always defined to be zero. The type and subtype fields define whether the frame is a management or data frame and they also define the function of the frame like association request, probe response, RTS, ACK etc. There are many different type and subtype combinations. To Distribution System (DS) and from DS bits are set if the frames are arriving or leaving the DS. The more fragment bit tells if another fragment will follow the frame. The retry bit is set if the frame is a retransmission frame and the power management bit is used in case of the station is in a sleep mode. The more data field bit is set if the station is going to send another frame to the station that is in power save mode. The Wired Equivalent Privacy (WEP) field indicates that the data bits have been encrypted using a secret key. The order field can be used if the receiving frames should be processed in order [Geier 1999].

5.4.3 Authentication and Privacy

The authentication process is always done between two parties, either between station and AP or between two stations in case ad-hoc network is used. The standard IEEE 802.11 defines two basic types of authentication methods, open system authentication and shared key authentication. The default authentication is the open system authentication that is essentially a null authentication algorithm. The AP and station that are using the open system authentication may become

authenticated if the station requests it. The other method, shared key authentication, relies on a WEP algorithm. In the shared key authentication only the stations that are using the specific secret key can be authenticated [IEEE 802.11 1999].

The standard defines the security services by the WEP as follows: confidentiality, authentication and access control in conjunction with layer management [IEEE 802.11 1999]. The secret key should be delivered for the users beforehand, which doesn't depend on the IEEE 802.11. The network manager takes care of the key management functions. The authentication and encryption together using the WEP provide sufficient security protection against eavesdropping. WEP uses the RC4 algorithm from the RSA Data Security. WEP is a symmetric algorithm in which the same secret key is used for encipherment and decipherment [IEEE 802.11 1999].

5.4.4 Power Management

The wireless stations are usually portable devices and the power consumption of the devices should be optimized. This is the reason why power management functionality has been defined. The power management in case of the IEEE 802.11 means that the wireless stations can be in so called sleep modes when they are not transmitting or receiving data and these power saving modes decrease the power consumption.

The power management is available for the infrastructure network so there must be an AP in which the stations are connected to. The stations don't lose information because the AP will buffer the packets that are addressed to the stations in power save mode. The power management functions are carried so that the AP monitors the power-management-bit in the frame control field of the MAC header. By this way the AP can maintain a record of those stations that are currently in power save mode. Stations can learn that it has frames buffered at the AP by listening to the beacons sent periodically by the AP. The station may request the AP to send the buffered packets or when the station returns to active state the AP forwards those packets automatically [Geier 1999].

5.5 Physical Layer

The standard IEEE 802.11 defines three different physical layer techniques to be applied below the MAC layer. These are Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum and Infrared.

The spread spectrum means that the signal's power is spread over a wide frequency band. This bandwidth sacrificing is done to get processing gain that is to achieve better signal-to-noise performance. The wide signal is robust against narrow band interference. Figure 34 illustrates the meaning of the spread spectrum technology [Geier 1999].

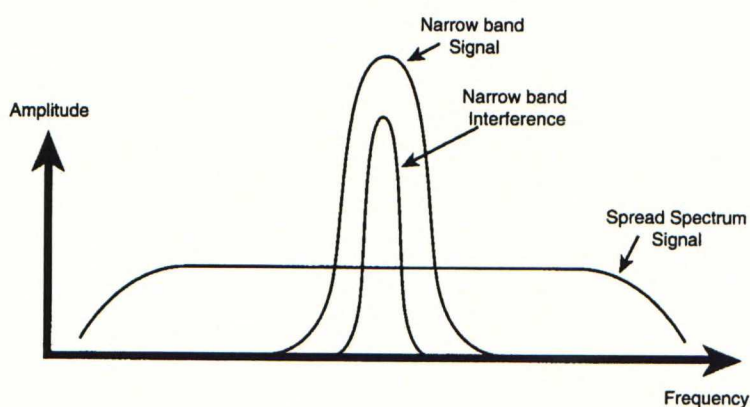


Figure 34 Spread Spectrum Technology

The narrow-band jamming-signal interferes only with a small portion of the spread spectrum signal. This makes it possible for the receiver to better demodulate the received signal because there is less interference and fewer errors compared to the situation when no spread spectrum is used [Geier 1999].

5.5.1 Direct Sequence Spread Spectrum

In the DSSS communication the data signal is spread by using a chipping code. This chipping code is higher rate bit sequence and when the data signal is combined with the chipping code, processing gain will be achieved [Geier 1999]. The chipping code can also be referred to as PN code or spreading code. According to the FCC's regulations, the DSSS system shall provide a processing gain of at least 10 dB. This shall be accomplished by chipping the baseband signal at 11 MHz with an 11-chip PN code [IEEE 802.11 1999]. The 11-chip Barker sequence is applied. An example of the operation of DSSS is shown in Figure 35.

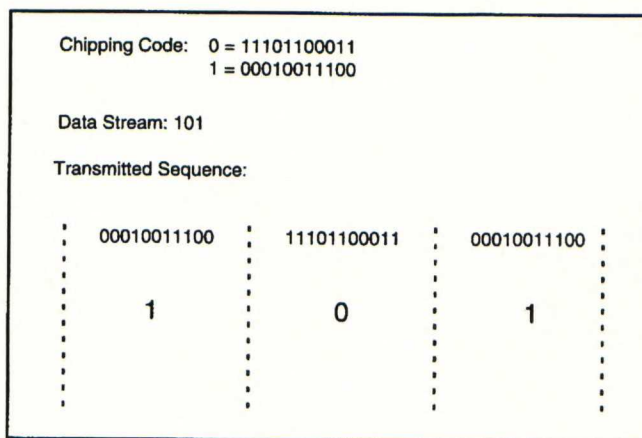


Figure 35 Direct Sequence Spread Spectrum

The data stream 1,0,1 is transmitted by spreading it with the related chipping codes. The transmitted bit sequence is thus much longer than the original data sequence, which gives processing gain.

According to the standard the maximum allowable output power depends on the geographic location. In the USA the maximum output power is allowed to be 1000mW (according to FCC 15.247), in the Europe 100mW (according to ETS 300-328) and in the Japan 10 mW (according to the MPT ordinance for Regulating Radio Equipment, Article 49-20). The minimum transmit power is 1 mW.

The physical layer performs the so called convergence function that defines a method of mapping the IEEE 802.11 MAC MPDUs into a framing suitable for sending and receiving data. This functionality is performed by the Physical Layer Convergence Procedure (PLCP). The PLCP frame format structure suitable for DSSS radio transceivers is shown in Figure 36. The PPDU is formed by adding the PLCP preamble and headers to the PSDUs.

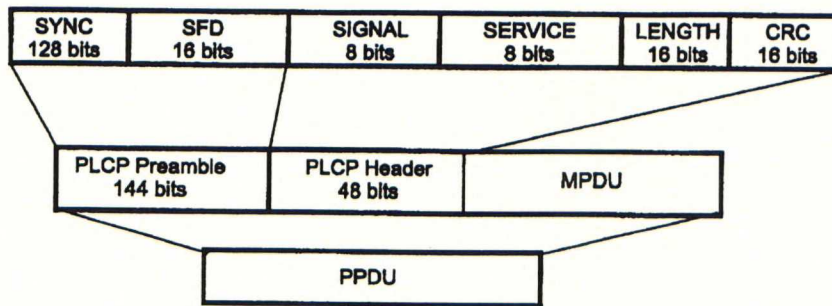


Figure 36 PLCP Frame Format in DSSS

The first SYNC field consists of scrambled bits so that the receiver could perform the synchronization. The Start Frame Delimiter (SFD) field provides the indication of the start of the frame. The signal field indicates the used modulation method. The service field is used in the high rate operation that is based on the IEEE 802.11b. The length field indicates the number of microseconds required to transmit the MPDU. The above mentioned fields are protected by using the 16-bits CRC. The above mentioned frame structure is based on the standard IEEE 802.11. The high rate extension IEEE 802.11b uses the same frame structure because these two standards must be interoperable. The only differences are in the use of the bits in the service field of the PLCP header and in the encoding of the rate in the signal field. The IEEE 802.11b defines also an optional short PLCP PPDU format that can be used to minimize overhead and to maximize the network data throughput.

5.5.2 Frequency Hopping Spread Spectrum

The FHSS technology uses a spreading code that hops from frequency to frequency as a function of time. The frequency range is wide and in case of IEEE 802.11 FHSS the carrier will hop over the 2.4 GHz frequency band between 2.4 GHz and 2.483 GHz [Geier 1999].

The manufacturers are required to use at least 75 different frequencies per transmission channel when using the FHSS technology. Also the maximum time spent at a particular frequency during any single hop is required to be 400 ms. Figure 37 shows the hopping frequency as a function of time [Geier 1999].

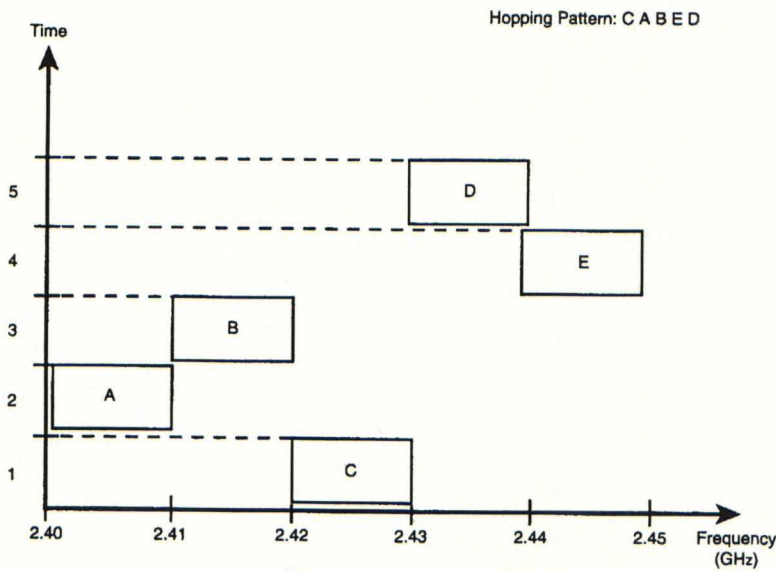


Figure 37 Frequency Hopping Spread Spectrum

The receiver stations must automatically synchronize to the correct hopping sequence to be able to receive the data correctly. The frequency hopping method reduces interference effectively because the interfering signal will affect the spread spectrum signal only if both are transmitting at the same frequency at the same time. For this reason the aggregate interference will be low. Different hopping patterns can be used if several operating radios would use the same frequency band [Geier 1999].

The PLCP frame format that is suitable for FHSS radio transceivers is shown in Figure 38.

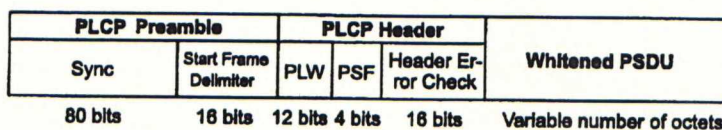


Figure 38 PLCP Frame Format in FHSS

The functionality of sync and SFD fields is the same as in case of the DSSS PLCP structure. The PSDU Length Word (PLW) field specifies the number of octets contained in the PSDUs. The PLCP Signaling Field (PSF) indicates the data rate of the PSDU. The HEC field is an error detection field. The whitening means that the data is randomized with a scrambler to minimize the DC.

5.5.3 Infrared

One of the three physical layer alternatives for the implementation of the IEEE 802.11 standard is the IR. However the DSSS and the FHSS are the most used ones. There are many special features in the IR. There are no frequency regulations in the use of the IR. The two devices using IR communication are supposed to be quite near because the range is relatively short. Better noise immunity can be reached by using the IR than the two spread spectrum methods

The IR physical layer uses light in the wavelengths from 850-nm up to 950-nm for signaling. The same band is used by the common consumer devices such as remote controls as well as other data communications equipment like IrDA devices. Unlike usually the IR in case of the IEEE 802.11 doesn't have to be directed, which means that the line of sight situation is not needed. This makes it possible to construct a true local area network containing several devices [IEEE 802.11 1999].

The transmission range would typically be about 10-meters and when more sensitive receivers would be used up to about 20-meters. The IR physical layer relies on both reflected IR energy as well as line of sight IR energy for communication. The used environment affects the range of the IR communication. In case there are no line of sight situation and the environment lacks of reflecting surfaces, the IR could suffer reduced range [IEEE 802.11 1999].

It must be noted that unlike the DSSS and FHSS methods the IR will operate only in indoor environments because the IR radiation doesn't pass through walls and most windows attenuate the IR radiation effectively. A single physical room contains the IR signal, which can have security aspects. The IR transmission doesn't suffer much on interference from other station because if some other station is transmitting continuously with very strong signal, it can be placed in a different room.

5.5.4 Modulation Methods

The modulation method that is being used depends on the data rate that is used by the transmitter and receiver. The standard IEEE 802.11 defines two data rates, 1Mbps and 2 Mbps. The 1 Mbps uses Differential Binary Phase Shift Keying (DBPSK) modulation and the data rate 2 Mbps is based on Differential Quadrature Phase Shift Keying (DQPSK) modulation. The extension IEEE 802.11b that is using the DSSS transmission provides higher data rates, 5.5 Mbps and 11 Mbps. The high

rate access is based on the Complementary Code Keying (CCK) modulation. An optional PBCC mode is also defined for the high rate access but that is not going to be described here. Above mentioned modulation methods are used by the direct sequence method. In addition the frequency hopping method uses GFSK modulation for the data rates 1 Mbps and 2 Mbps as defined in the standard IEEE 802.11. The basic functionality of the four modulation methods will be covered.

The DBPSK modulation is based on the phase variation of the carrier frequency. The noise typically doesn't affect phase of a signal. The different binary symbols are represented by the variation of the phase. The phase variation thus maintains the information content of the transmitting signal. The carrier's signal phase is shifted according to the binary data that has to be transmitted. If the bit input is 0 then the phase change is 0 radians. If the bit input is 1 then the phase change is π radians [IEEE 802.11b 1999].

The DQPSK modulation uses four different phase changes in the modulation of the signal. The input to the modulator is combinations of two bits. The phase changes for the bit combinations 00, 01, 11, and 10 are respectively 0, $\pi/2$, π , and $3\pi/2$ radians. Because each two bit symbols are transmitted at 1 Mbps the data rate becomes 2 Mbps [IEEE 802.11b 1999].

CCK is used for the high rate extension for the standard using the DSSS. The CCK modulation employs 8-chip spreading code while the 1 Mbps and 2 Mbps transmissions use 11-chip Barker codes. The 8-chip code word is based on complementary codes. The spreading code word is based on a certain formula and the phases of chips are changed. The modulation for the transmission of 5.5 Mbps uses four bits per symbol and for the transmission of 11 Mbps eight bits per symbol are transmitted. In the code word there are 4 phase terms. One of them modulates all of the chips, which is used for the QPSK rotation of the whole code word. The other three phase terms modulate every odd chip, every odd pair of chips and every odd quad of chips respectively [IEEE 802.11b 1999].

In the GFSK modulation the carrier frequency varies and by this way the different binary symbols are represented. The information is thus carried by the frequency changes of the signal. Typically noise affects the amplitude of the signal, not the frequency. The 1 Mbps data rate for the frequency hopping system is modulated by using two level GFSK modulations. This means that there are two different

frequencies that are varied from the center frequency. For logic 1 the modulator transmits on a frequency that is a center frequency plus frequency deviation and for logic 0 on a center frequency minus the frequency deviation. Typically the frequency deviation is 160 kHz. The 2 Mbps data rate is modulated by four level GFSK modulation and the principle is the same as in two level modulation. The difference is that now there are four different frequencies used representing different combinations of two bits. So the data rate is doubled by using the four level modulation instead of the two level modulation [Geier 1999].

6. WLAN IN RESIDENTIAL AND SMALL OFFICE BROADBAND ENVIRONMENT

The WLAN is suitable for residential and small office broadband environments. The standard IEEE 802.11b provides bandwidth wide enough for most broadband services. The WLAN matches well in the xDSL broadband access network architecture that was presented in the chapter 2. The end-user is not dependent on the network terminal's location if WLAN is used. The network terminal is an AP for wireless stations that are connected to it. The WLAN brings a new aspect to the broadband access model because the users can take advantage of the modern state-of-the-art xDSL/WLAN devices without wires.

6.1 Applications

Nowadays the mobile phone has become very popular, which could mean that people want to use mobile applications in the future as well. The internet should be accessible by using portable devices. At the moment the third generation mobile applications and GSM-evolution devices are not widely available yet. The need for the use of computers does not disappear very fast even if the third generation mobile devices would become commonly available. The strong need for the high-speed internet access is common in many countries.

There are many different places where the wireless LAN could be used. It would be possible to take advantage of the WLANs in corporates' networks, branch offices, public access zones, small offices, and homes. In corporates and branch offices the WLAN extends the already existing wired network and it is very easy and fast to install. The wireless access to the corporate's Intranet would be possible anywhere from the buildings. The wireless connectivity would also be useful, for example, in meeting rooms and offices. Also the Intranet access would be possible in common areas like lobbies. The public access zones bring new customers for WLAN device manufacturers. Different areas like hotels, airports, exhibitions and campus areas could take advantage of the wireless internet access solutions.

This chapter focuses on WLANs in small office and home environments because the xDSL WAN connection is most usable in these environments. Corporates and other large places would not perhaps need the xDSL connection but they could have already installed ATM connection to the internet. This chapter considers WLAN

security aspects and network planning issues. In small office environments, like in sales offices, WLANs are flexible solutions to exploit. WLAN is also very good alternative to new companies that don't want to invest in wired network infrastructure. At homes the WLAN brings many benefits. There is no need to think that much where to locate desktops and laptops because they all can be wirelessly connected to the AP and no cables are needed. It is also easy to have internet access from several laptops at the same time. In many cases it would also be possible to use the internet access outside the building like in the garden because the coverage of the WLAN is quite high.

6.2 WLAN Security

The WLAN security concerns small offices but also home users. There is quite a big difference comparing the WLAN to the traditional cabled home and office network because there are no physical boundaries for the network access. Basically there are two types of security problems, unauthorized network access and eavesdropping. The solution for unauthorized network access is authentication and for eavesdropping encryption. This chapter covers the security methods considering the WLAN part of the network.

When considering corporate's networks different kinds of security gateway solutions come into question too. In addition to these, for example, VPN solutions could be used. IP Security (IPSec) is rapidly becoming the VPN protocol of choice. IPSec encompasses most, if not all, of the elements required for a VPN. It can be used in its entirety as a VPN protocol all by itself, or elements of it can be used to establish standards for other VPN protocols. IPSec is an extension of the standard IP protocol, securing the network at the IP level with authentication and encryption. IPSec can be used to enhance layer 2 protocols such as L2TP or PPTP [Hamzeh et al. 1999].

6.2.1 Authentication

Especially the IEEE 802.11b devices may have long range varying from 20 up to 100-meters depending on the surroundings. This makes it possible to access the network even outside buildings. That's why some authentication method is required. The Nokia's MW1122 ADSL/WLAN router has authentication methods for its WLAN interface based on clients' MAC-addresses and WEP keys.

The basic identifier of the WLAN is the network's name. With correct network name it is possible to know that the right network is being accessed. It is possible to configure to the MW1122 access list based on MAC-addresses, which allows only those MAC-addresses to be authenticated to the AP. It is also possible to restrict the number of WLAN clients that can be connected to the AP at the same time. Every WLAN PC card has a unique MAC-address that can be used in the authentication of the end-user.

The WEP keys can also be used as an authentication method in addition to the encryption. The APs can be configured so that authentication is possible only with a certain WEP key. It is possible to use either one key for several stations or specific keys. If one shared key is used, then all the stations that are using the same key can be authenticated to the AP. This could be the case, for example, in small offices. If better security is needed then the specific WEP keys should be used. In this case every WLAN station needs to have a specific WEP key that is bounded to the WLAN PC card's MAC-address. The specific keys together with shared keys provide quite a good level of security. WEP keys can be stored in smart cards and then it is possible to use smart cards for delivering the secret WEP keys for the end-users. The smart cards are usually protected by a Personal Identification Number (PIN) code like Subscriber Identity Module (SIM) cards in GSM. It is also easy to monitor from the AP how many WLAN stations are connected to the network.

6.2.2 Privacy

The privacy in WLAN means that some effective encryption method should be used to prevent the eavesdropping. Nowadays it is quite easy to monitor the traffic between WLAN stations and APs. To prevent this the standard IEEE 802.11b provides encryption based on the Wireless Equivalent Privacy. The standard provides two level of encryption, using the 40-bit or 128-bit WEP keys. The longer the key, the longer it takes to decrypt the information sent and the higher is the level of security. The WEP algorithm is symmetric in which the same secret key is used for encipherment and decipherment. The WEP keys based on the IEEE 802.11b provide sufficient level of security, however better encryption methods are being developed.

When the one shared WEP key is used then all the traffic is encrypted by using this shared key. The end-users must know the shared key that is used in the AP. If the

specific keys are used then all the unicast traffic is encrypted by using the specific key. The shared key is also needed because multicast and broadcast traffic is encrypted by using the shared key.

6.3 WLAN Network Planning

6.3.1 Location and Site Survey

When setting up a wireless network, there are several issues that should be taken into consideration. One of the issues is the AP's location. In case the AP is the NT in the broadband access network architecture, the WAN connection must be taken into account too. The WAN connection needs the xDSL line cable to be connected to the NT. In general the location should be the best possible to get optimal coverage and performance for the wireless network. At home environment and small offices there are not so many places where the AP could be located. The biggest advantage of the site survey and location planning can be achieved in large building environments like hotels etc. If there are several stations using the same wireless network the throughput is shared between the stations. So the capacity of the network strongly depends on the amount of the users.

Site surveying can be done to determine the best possible AP locations. In practice readings from various places are got to find out an optimal locations. The first step in the site survey is to check out facility blueprints to make preliminary coverage area planning. Then the permanent user locations affect the AP's location. The obstacles that may reduce or weaken radio propagation should be taken into account as well the potential sources of interference like other RF devices. The location is finally verified by site survey tool. With site survey tools, the power of the received radio signal is checked in different locations and also bit-rates and packet error rates are checked.

6.3.2 Frequency Channels

The IEEE 802.11 standard defines the radio channels that can be used in different countries. Table 3 shows the channels that can be used in the DSSS system.

Table 3 Frequency Channels in IEEE 802.11 DSSS

Channel No:	Frequency (GHz)	USA and Canada	Europe	Spain	France	Japan
1	2.412	x	x			
2	2.417	x	x			
3	2.422	x	x			
4	2.427	x	x			
5	2.432	x	x			
6	2.437	x	x			
7	2.442	x	x			
8	2.447	x	x			
9	2.452	x	x			
10	2.457	x	x	x	x	
11	2.462	x	x	x	x	
12	2.467		x		x	
13	2.474		x		x	
14	2.484					x

If there are several APs in the same coverage area using the same radio channel, the capacity is shared between the APs. So the radio channel planning could help to avoid this problem. There should be a separation of five channels in the same coverage area between APs to get the optimal channel separation. In the Europe, for example, channels 1, 6 and 11 could be used if there would be three APs in the same coverage area. The separation of channels prevents interference effect from other APs and the throughput won't decrease for this reason.

In practise the biggest advantage of the radio channel planning will be got in apartment building environment. There can be several APs in same coverage area and those APs can be installed by different network operators or ISPs. It can be possible to use different radio channels in different APs by configuring the radio channels randomly. This way the probability, that there would be two or more APs next to each other using the same radio channels, will decrease.

7. MEASUREMENTS

This chapter describes the Wi-Fi interoperability measurements that were done in the SVNL in San Jose in February 2001. Measurement configurations and methods are presented. At the end of the chapter the analysis and results are discussed.

7.1 WLAN Interoperability

Because the WLAN devices are becoming more popular, there has been need for defining interoperability for different manufacturers' devices. This chapter focuses on the interoperability of Nokia MW1122 ADSL/WLAN router with other vendors IEEE 802.11b based WLAN products. It is possible to buy, for example, Lucent and 3COM WLAN PC cards and use these cards at home or at the office with MW1122. It would be usefull to know beforehand if the MW1122 is interoperable with other vendors WLAN PC cards.

The goal of the WECA is to ensure interoperability among IEEE 802.11b High Rate products from many manufacturers, and to promote this technology within both business and consumer markets. The interoperability tests were executed to get measurement results of the interoperability of the Nokia MW1122 ADSL/WLAN router. The Wi-Fi interoperability can be seen as a mark of multi-vendor interoperability.

7.2 Description of Measurement Configurations and Methods

7.2.1 Measurement Configurations

The Wi-Fi tests were divided into three parts: initial tests, extended tests and special tests. For the tests, certain WLAN-specific parameters like ESSID, WEP-keys and used radio channels were configured in the AP.

In the interoperability tests there were four WLAN-clients from different manufacturers: Lucent, 3COM, Aironet and Symbol. It is specified by the WECA that these WLAN-clients should be used in the interoperability tests. On the 15th of March 2000 Cisco Systems completed its acquisition of Aironet and the Aironet's products are now Cisco's products. These WLAN-clients were used in every test

case with different kinds of configurations. The used laboratory test set-up is shown in Figure 39.

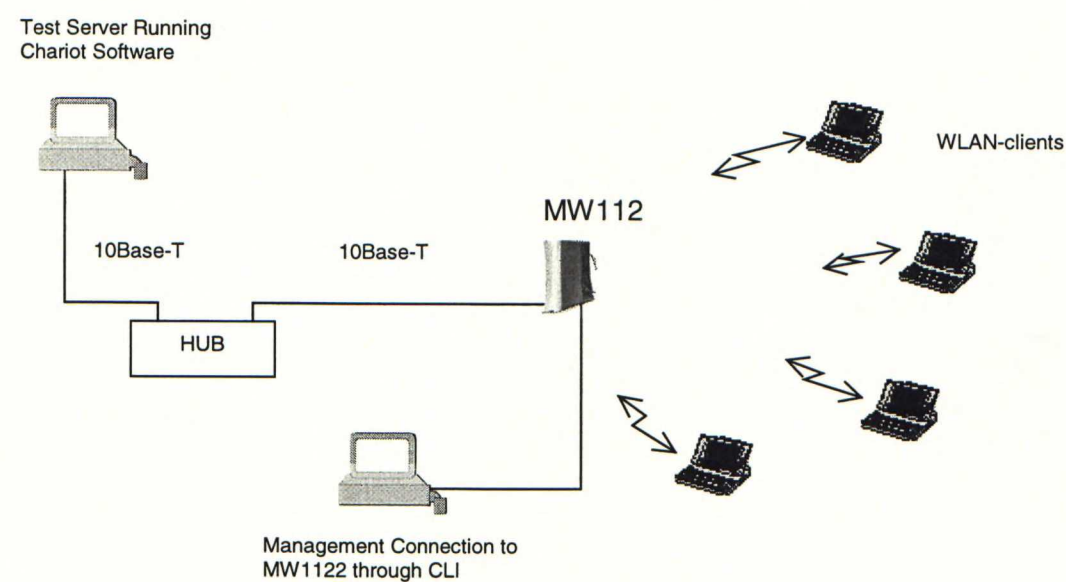


Figure 39 Test Set-Up

The MW1122's ethernet port was connected to the ethernet HUB by using straight ethernet cable. The test server, installed in Windows NT Operating System (OS), was also connected to the HUB. The MW1122 was controlled by using the Command Line Interface (CLI) by connecting the MW1122's CLI port to the desktop by using a specific CLI cable. The different manufacturers' WLAN-cards were installed on laptops that were using Windows 98 OSs. The WLAN-card which was used in the MW1122 was Nokia C111 with Nokia C950 external omnidirectional antenna.

The measurement software that was running in the test server was Chariot version 3.1 from Ganymede Software Inc (today NetIQ Corporation). Chariot testing software includes a large set of standard, editable scripts that can be used to define a particular traffic flow between two endpoints. The script definition, test configuration, test execution, and reporting of results are managed through the Chariot console, which in this case was the test server connected to the ethernet HUB. The application scripts that were used in the tests make the same Application Programming Interface (API) calls to the network protocol stacks that real applications make, which causes the protocol stack to perform the same work involved in sending and receiving data.

The models of the used WLAN-clients were:

Lucent ORINOCO PC Card-Silver

3COM AirConnect 11 Mbps Wireless LAN PC Card

Cisco Aironet 340 Series Wireless PC Card

Symbol Spectrum24 High Rate 11 Mbps Wireless LAN PC Card

The basic configuration of MW1122 that was used in the tests was:

```
system
hostname MW1122
eth
bridging
wlan
network-name svn1
radio-channel usa 5
wep default-key 1
wep mode wi-fi required
wep key-entry 1 40-bit 0x0123456789
slave-to-eth
vcc1
pvc 9 100 eth-llc
bridging
vcc2
vcc3
vcc4
vcc5
vcc6
vcc7
vcc8
vbridge
ip address 153.69.254.179 255.255.255.0
mngtvcc
common
```

In the MW1122's configuration bridging was enabled in the ethernet interface and WLAN was slaved to the ethernet. The parameters that were changed during the tests were, for example, network-name, radio channels, WEP-mode and WEP-keys. The VCC1's configuration wasn't used in the tests because ADSL interface wasn't connected. The IP-address in the vbridge-interface was used for the management of the MW1122.

Picture of the MW1122 and the C111 WLAN card is shown in Figure 40.



Figure 40 Nokia MW1122 ADSL/WLAN Router and Nokia C111 WLAN Card

The software versions of the MW1122 that were used in the tests are shown below.

Application software: Gx1x2211.R09

Boot software: Bxxx2100.R09

WLAN firmware: 3.02.79

ADSL Firmware: Alcatel 3.6.70 for ADSL over POTS

Different interfaces of the MW1122 are shown in Figure 41.

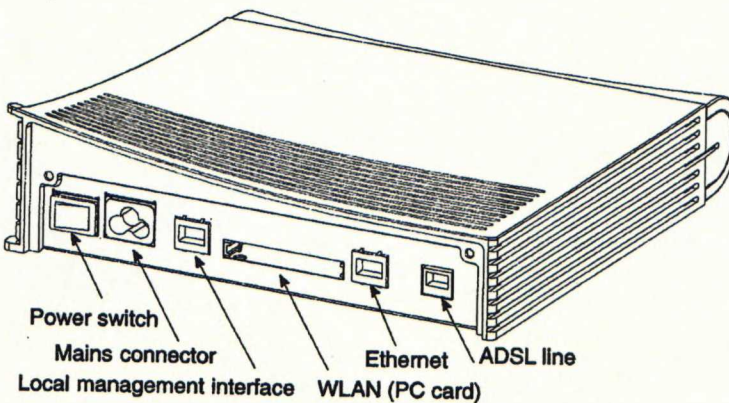


Figure 41 Nokia MW1122 ADSL/WLAN Router's Back-panel

The connected interfaces, in addition to the mains connector, were local management interface for CLI connection, WLAN and ethernet. The ADSL line wasn't connected because the Wi-Fi interoperability tests were executed with the WLAN and ethernet interfaces of the MW1122 only. The tests could have been done by using the ADSL and WLAN interfaces but the SVNL didn't have DSLAM and other equipment for this. WECA doesn't either specify the use of xDSL connection as a WAN interface for the Wi-Fi tests [WECA 2000].

7.2.1.1 Initial tests

In initial tests WLAN-clients from different manufacturers were configured as shown in the table in Appendix A. The parameters that were configured both in WLAN-clients and in MW1122 were: RTS threshold, fragmentation, WEP keys, power-save mode, AP's channel and AP's basic rates. The MW1122 supports automatically all different basic rates that the standard defines and the used rate is determined during the WLAN-client's association to the MW1122. The RTS, fragmentation, WEP and power-save and basic rates were discussed in chapter 5. The available radio channels for the DSSS system were discussed in chapter 6.

In addition to the configurations shown in Appendix A, additional configuration was made to the MW1122. This configuration used radio channel 4 and 40-bits WEP-key 0xABCDEABCDE.

7.2.1.2 Extended Tests

The used configurations in the WLAN-clients and in the MW1122 are shown in Appendix B. The configured parameters were the same as in the initial tests. Two tables in Appendix B show the two different configuration test set-ups that were used.

7.2.1.3 Special Tests

The special tests included multicast tests and the used configurations are shown in Appendix C. The parameters that were configured were again the same as in initial tests.

7.2.2 Methods

The interoperability measurements for the MW1122 were made by using the WLAN and LAN interfaces of the device as mentioned before. So the traffic was generated through these two interfaces. The goal of the MW1122 interoperability tests was to make sure that the MW1122 can operate with a variety of ESSIDs, can handle RTS, fragmentation, WEP, power save, different channels and different basic rates.

7.2.2.1 Initial Tests

The goal of the MW1122's initial tests was to test the AP's ability to work with stations from a variety of manufacturers. The tests included configurations with and without RTS, with and without fragmentation, with and without WEP, and with and without power save mode. Also various channels were tested.

In the initial tests different tasks were executed with different kinds of configurations. The MW1122 was first tested against Lucent WLAN-client. The MW1122 was powered on with its defined configuration (as shown in the Appendix A). The laptop with Lucent WLAN-card was also powered on with the specific configuration. After this the MW1122 and the station were both examined to determine whether or not the client properly associates with the MW1122.

After this three different throughput tests were done by using the Chariot testing software. First script, called Data Transfer (DT) 1, emulates a large file transfer from the WLAN-client to the test server. The second script DT2 emulates a large file transfer from the test server to the WLAN-client. The third script called DT3 emulates a series of transactions between client and server.

The measured and target throughputs are the amount of received bits as a functions of time. Traditionally the throughput can be considered as amount of received data compared to the transmitted data. However in this thesis the throughput values are reported as a function of time. This is also the way in which the Chariot testing software reports the results when measuring the throughput.

The tests were done first by using the Lucent WLAN-client and then 3COM, Cisco and Symbol WLAN-clients. So the MW1122 was tested to work with all these four vendors' devices separately. After these tests all four stations were brought up with the same configuration parameters for RTS, fragmentation and power save as before. The MW1122 was configured to use the channel 4 and WEP key 0xABCDEABCDE. These two settings were done in the WLAN-stations as well. By using this set-up, in which all four stations were connected to the MW1122, it was checked that the four WLAN-clients can be associated properly to the MW1122 at the same time.

7.2.2.2 Extended Tests

The extended tests were done to examine whether or not the MW1122 can interoperate within various parameter settings in WLAN-clients. The tests that were done in the extended tests were the same as in the initial tests but the used configurations were different.

7.2.2.3 Special Tests

The special tests contain more specialized tests involving certain unique aspects of MW1122 behavior. The special tests were divided into five different parts: reassociation/roaming, data payload, multicast, intra-BSS transfer and negative tests. These tests are described next.

7.2.2.3.1 Reassociation/Roaming

In this test it was examined if the MW1122 is capable of handling reassociation properly. The test was done by using another AP in addition to the MW1122. The MW1122 was first off and the other AP was on. A WLAN-client was associated with the other AP. The WLAN-client was forced to roaming when the another AP was turned off and the MW1122 was turned on. Internet Control Message Protocol (ICMP) echo requests were generated from the test server by using the ping-command. Then it was examined if correct ICMP echo replies were got from the station, before and after the MW1122 was turned on. Both APs were using the same ESSID.

7.2.2.3.2 Data Payload

This test was done to verify the MW1122's ability to encapsulate packets correctly. It was checked that various packets were correctly received and transferred in both directions. The different payload types that were tested were: DIX Ethertypes, LLC (802.2) packets, RFC1042 and basic ethertype transfer for 8137 and 80F3. The different payload types were tested by using the Ethernet 802.2, Ethernet 802.3 and Ethernet V2 frame types. The IPX was used both in the test server and in the WLAN-station. The data transfer was again tested by using the ICMP echo requests.

7.2.2.3.3 Multicast

Two WLAN-clients were connected to the MW1122 and multicast stream was transferred through the MW1122. The used IP-address for multicast was 225.0.0.1. The multicast traffic was transmitted by using User Datagram Protocol (UDP). This test was done by using a specific multicast script in the Chariot testing software.

7.2.2.3.4 Intra-BSS Transfer

In this test it was checked if two WLAN-clients that were connected to the MW1122 were able to communicate with each other through the AP.

7.2.2.3.5 Negative Tests

The negative tests were done to verify that the WLAN-clients were not able to associate and transfer data through the MW1122 if they had mismatched configurations. The different mismatched configurations were: wrong ESSID, wrong case in ESSID, ESSID substring, wrong WEP key and wrong WEP mode.

7.3 Analysis

7.3.1 Initial tests

In the initial tests the Lucent, 3COM, Cisco and Symbol WLAN-clients and the MW1122 were first configured as shown in Appendix A. The Lucent WLAN-client and the MW1122 was then powered on and it was seen that the Lucent was associated to the MW1122 properly. The Lucent was examined by using the Graphical User Interface (GUI) of the WLAN-card's software that was installed in the laptop. The MW1122 was examined by using the commands 'show wlan table' and 'debug wlan ctrl'. With these commands it was seen that the client was associated properly with correct WEP-key and it was also possible to see the MAC-address of the client. The association was also verified by using the ICMP echo requests. The ICMP echo requests were generated from the test server to the WLAN-client's IP-address. Correct ICMP echo replies were got from the WLAN-client.

After this the three throughput tests were done. First the Chariot software's DT1 test was done and then the DT2 and DT3 tests. These tests were named as A1DT1, A1DT2 and A1DT3. The throughput values and the corresponding target throughputs for the tests are shown in Appendix D. The target values of the

throughputs are defined by WECA from the average results of the tests that have been done by using Lucent, 3COM, Cisco and Symbol APs and WLAN-clients with all different combinations. The measured throughput value is the average value got from the Chariot testing software. The results were good because the measured throughput values exceeded the target values as can be seen from Appendix D.

The same tests were then done by using the 3COM WLAN-client. The association was done properly between MW1122 and 3COM with the corresponding configurations. The MW1122 and 3COM were examined to verify the association and make sure the correct ICMP echo requests were got. The three throughput tests were done and they were named as EA2DT1, EA2DT2 and EA2DT3. The measured throughput values were good and exceeded the target values.

The same tests were then done by using the Cisco WLAN-client. First it was verified that the client was properly associated with the MW1122 and then it was checked that ICMP echo replies were received correctly. The values of the throughput tests, named A3DT1, A3DT2 and A3DT3, were again above the target values except the A3DT3 in which the measured value was exactly the target value.

The tests were also done by using the Symbol WLAN-client and the association succeeded well. The throughput values of the tests A4DT1, A4DT2 and A4DT3 were again higher than the target values.

After these tests the additional configuration by using the radio channel 4 and WEP-key 0xABCDEABCDE was made and all the four WLAN-clients were powered on. Associations of all four clients succeeded and the correct ICMP echo replies were received.

7.3.2 Extended Tests

The extended tests were the same as the initial tests but the used configurations were different as shown in Appendix B. There were two different configurations in one WLAN-client and the throughputs were measured with both of these configurations. In all different test cases the associations succeeded well between the WLAN-clients and the MW1122. The throughput values of the tests are shown in Appendix D. Test cases are named from EA1DT1 up to EA8DT3. It can be seen from the results that the measured throughput values are well above the target values except in tests EA2DT1, EA3DT1, EA7DT1 and EA7DT2. The values of

these four tests didn't reach the target values and that's why these test cases were examined in more detail.

To get better throughput values different possible sources of errors were taken into consideration. First of all it was assumed that there might be interference in the used radio channel. Maybe some other AP might have used the same radio channel. For this reason the tests were also done by using some other radio channels but it didn't affect the results. The used WLAN-cards in the laptops were then changed and also the laptops were changed but these too didn't affect the results. It was also examined that there was no other AP at the same coverage area.

It was assumed that the measurement environment could have caused interference in the radio path and that's why the throughputs were not so good. There were some metallic racks and shelves quite near to the MW1122 and the WLAN-clients and this was assumed to cause errors to the test results. To overcome this hypothesis it was decided to measure the same throughput values with the same test set-up by using other APs to be able to have comparison. The Nokia A032 AP and Lucent AP were used to measure throughput values for the four test cases. The measured throughput values of the MW1122, A032 and the Lucent AP are shown in Figures 42,43 and 44.

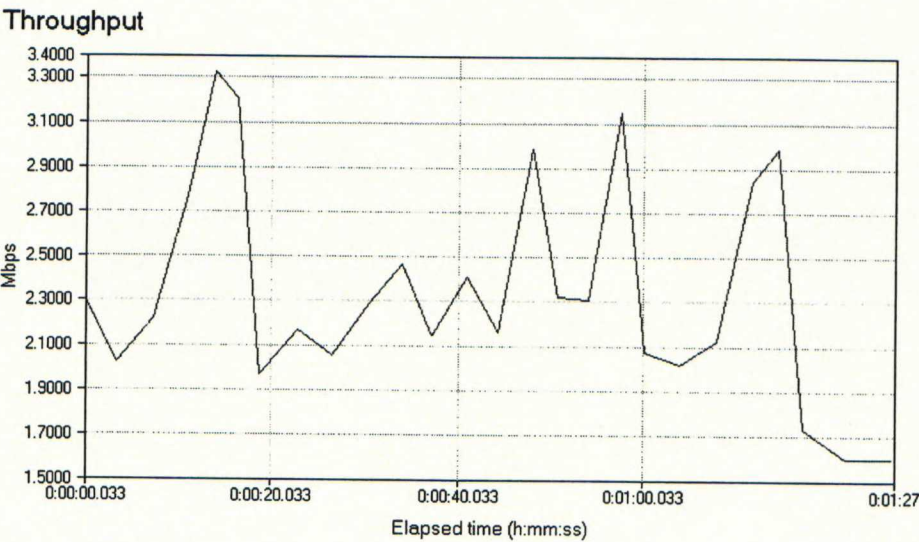


Figure 42 Measured Throughput of MW1122 in Test EA2DT1

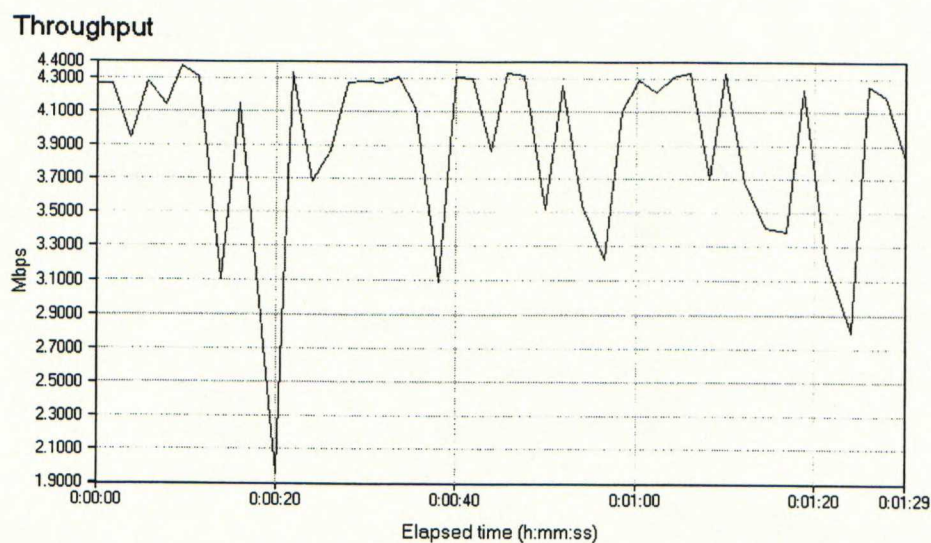


Figure 43 Measured Throughput of A032 in Test EA2DT1

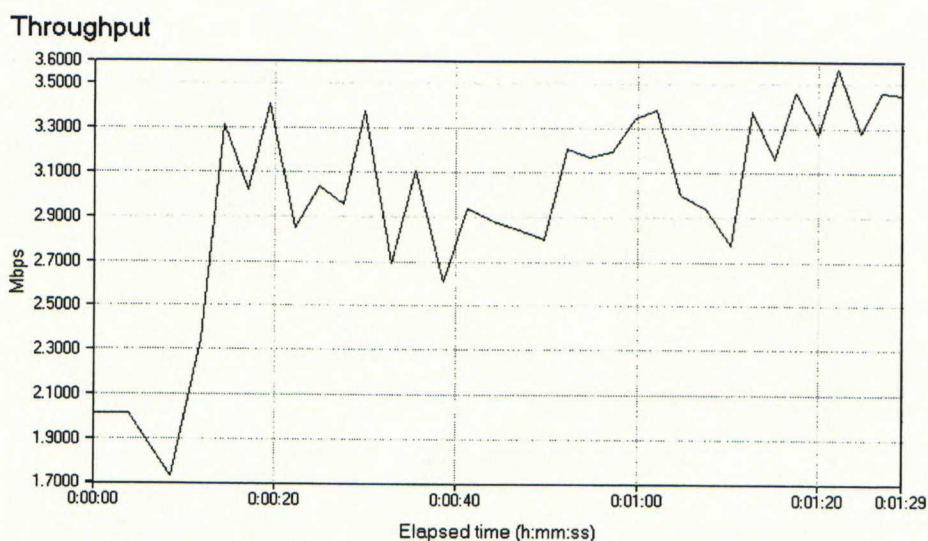


Figure 44 Measured Throughput of Lucent AP in Test EA2DT1

The average level of the MW1122's throughput was 2.305 Mbps and for A032 it was 4.06 Mbps. The result for Lucent AP was 3.3 Mbps. The target throughput value for this test was 3.1 Mbps. These results indicate that the reason for the MW1122's low throughput values is not the measurement environment because A032's and the Lucent AP's throughput values are much higher. However it should be noticed that there is big variation in the result of the MW1122 indicating that there might have been interference in the radio path. The variations of the A032 and Lucent AP throughput values were quite high as well but the levels of throughputs were much higher. After this throughputs were measured also in the three other cases to see if the throughput levels differ.

The measurement results in test case EA3DT1 are shown in Appendix E. In this case the measured average throughput value of the MW1122 was 0.147 Mbps. The target value was 0.2 Mbps. As can be seen from the figures in Appendix E the throughputs of A032 and Lucent were better than with MW1122. The throughputs were stable and there was not much variation in the results of any AP.

The results in test EA7DT1 are shown in Appendix F. In this case the average throughput value of the MW1122 was 0.102 Mbps and the target was 0.15 Mbps. The values of the A032 and the Lucent AP were again better.

The results in test case EA7DT2 are shown in Appendix G. In the test EA7DT2 the throughput value of the MW1122 is first high, decreases and then stays stable. The throughput of the A032 is quite stable but with Lucent there is some variation. The throughput values were, again, higher with the A032 and the Lucent APs than with the MW1122.

All these four tests showed that with the same test set-up and laboratory environment the throughput values of the MW1122 were lower than with the A032 and the Lucent APs. For this reason some additional modifications for the MW1122 were made. The tests were then also made by changing the external antenna that was used in the MW1122 but this didn't affect the results. Also different Nokia C111 WLAN-card was used and then also the MW1122 unit was changed to another one. Two different configurations were also used in addition to the one presented before. In the new configuration bridging was also enabled in the WLAN interface and the WLAN interface was not slaved to the ethernet interface but this either didn't better the results. After this a newer application software version and also newer WLAN firmware were loaded into the MW1122. All these didn't however affect the throughput results. It was also checked that the WLAN and ethernet ports of the MW1122 didn't have any errors. Errors or abnormal behavior wasn't found from the statistics of the MW1122.

The default values of the MW1122's WLAN parameters were changed so that the beacon interval was changed from 200 to 100 and fragmentation threshold from 2301 to 2346. These values are the most common among different manufacturers' WLAN devices according to the SVN's engineer Calvin Hui. These parameter changes didn't however better the results. It was noticed that the ethernet collision

led in the MW1122 was blinking meaning that there were collisions in the ethernet. This might have decreased the throughput but on the other hand it is normal that collisions occur in the ethernet. Although efforts were done to better the throughput values, the cause of the low throughput wasn't found.

7.3.3 Special Tests

In the special tests different cases that were mentioned before were tested. The roaming test succeeded well. First Lucent AP was powered on and the 3COM WLAN-client was associated to that. Then the Lucent AP was powered off and MW1122 was powered on. Because both APs used the same ESSID the client was able to associate to the MW1122 automatically. This test was also done by using MW1122 with 3COM and Cisco APs. The reassociations were done properly in all these cases.

The support of different payload types was tested by using Ethernet 802.2, Ethernet 802.3 and Ethernet V2 frame types both in the test server and in the WLAN-client. Also IPX was tested. In all of the cases ICMP echo replies were correctly received when sending the requests from the server to the client.

The throughput values of the multicast test were above the target values as shown in Appendix D. The multicast test was done by using all four WLAN-clients. In the intra-BSS transfer test it was checked that two stations connected to the MW1122 were able to communicate with each other. This was verified with ICMP echo requests and correctly received replies. When performing the negative tests it was seen that the MW1122 works the way it should work. The WLAN-clients from different manufacturers were not able to associate with the MW1122 if they had a mismatched configuration.

7.4 Results

Generally it can be said that the Nokia MW1122 ADSL/WLAN router is well functional in a multivendor environment. The tests showed that the MW1122 can operate with various different parameter settings in the different manufacturers' WLAN-clients. The results from initial, extended and special tests were good and all the different configurations worked well. The associations succeeded and correct ICMP echo replies were received.

The values of the measured throughput tests are compared to the target throughput values in Figure 45.

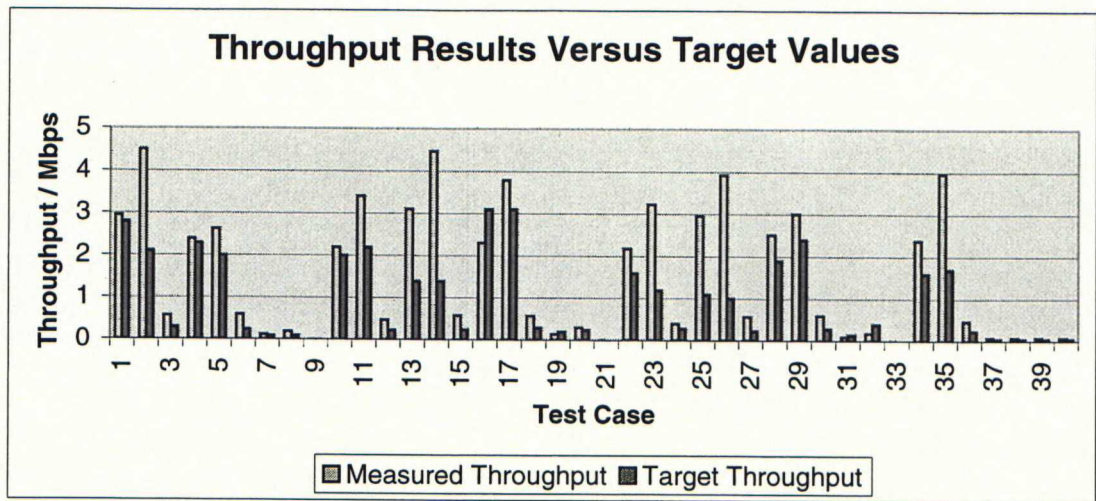


Figure 45 Measured Throughputs of MW1122 Versus Target Values

The measured Wi-Fi interoperability throughputs of the Nokia MW1122 ADSL/WLAN router were good and in most of the cases the measured values were much higher than the target values as can be seen from Figure 45. However in four of the 40 different throughput test cases the measured values were below the target values. To get better results many different things were done trying to find out the reason for the low throughput. However better results were not achieved. Because of that the throughput measurements in those four test cases were also done for the Nokia A032 AP and for the Lucent AP. The throughputs of these two APs were then compared to the MW1122's throughput values and it was found out that the A032 and the Lucent AP had better throughputs with same measurement set-ups and laboratory environment.

As a conclusion of the tests it can be said that it would be usefull to purchase the same Chariot testing software to Nokia's own research and development laboratory. Then it could be possible to repeat the tests and try to reproduce the problem that occurred with four test cases in which the target throughput values couldn't be reached. Then the throughputs could be examined in more detail. The purchase of the software and building of the testing environment as well performing the tests again in Nokia's own laboratory will take some time and that doesn't belong to the scope of this thesis.

8. SUMMARY

This thesis discussed WLAN technologies and especially IEEE 802.11 technology that can be used in the broadband access network that is based on xDSL technologies. NTs that are located in the customer premises side of the network can have WLAN interfaces in addition to the traditional wired LANs. The presentation of the broadband access network included layer 2 protocol ATM and IP encapsulations over ATM. Also IP tunneling methods were discussed. The broadband access network can utilize different kinds of end-to-end protocols and these were also presented. After having got an adequate understanding of the access network architecture different applications were shortly described.

The different xDSL technologies were presented and especially ADSL were discussed in more detail. Different xDSL technologies have their own special features and it was seen that there are several different standardization bodies that take part in the standardization work of these technologies. Frequency usage of xDSL technologies was also shortly covered.

There are several WLAN technologies present at the market area, like IEEE 802.11, HIPERLAN, Bluetooth, HomeRF and IrDA. These technologies were presented and the IEEE 802.11 standard was examined in more details. The presentation of WLAN in residential and small office broadband environments included applications, WLAN security aspects and network planning issues.

The interoperability tests were made to the Nokia's MW1122 ADSL/WLAN router. The WLAN of the MW1122 is based on the IEEE 802.11b standard and these IEEE 802.11b based Wi-Fi interoperability tests are specified by the WECA. The tests were made in the SVNL in San Jose. The measurements showed that the MW1122 works well in a multivendor environment with different kinds of configurations. The throughput tests against other vendors' products showed that in most of the cases MW1122 had high throughput values. However in some of the throughput tests the measured values were not very high and the reason for this was analysed. In general the MW1122 can be said to be interoperable with other vendors' IEEE 802.11b based products.

It can be said that WLAN suits well in home and small office environments. The wireless LAN is quite quick to install and coverage can be easily achieved. XDSL

gateways together with wireless LAN enable remote work and offer easy and flexible way to have high-speed internet connection both at homes and at small offices. However there are several issues that have to be taken into account when employing the WLAN, especially security aspects.

There are different xDSL technologies present in the market area and the standardization of the xDSL technologies has proceeded. There are also many WLAN technologies in the market area and also their standardization has developed during the past few years. The interoperability between different manufacturers' devices both in xDSL and WLAN technologies has become more important for network operators, ISPs and equipment manufacturers. The improvement of the interoperability encourages the network operators and ISPs to use devices from different manufacturers. In general the interoperability promotes the technology and markets of xDSL and WLAN technologies. There is a good possibility that markets of the xDSL/WLAN gateways will increase significantly in the near future.

9. REFERENCES

ADSL Forum Technical Report, TR-002, ATM over ADSL Recommendations, March 1997

ADSL Forum Technical Report, TR-012, Broadband Service Architecture for Access to Legacy Data Networks over ADSL Issue 1, June 1998

Alcatel Microelectronics, CTRL-E Interface Specification, May 2000

ANSI, T1.413 Issue2, Network and Customer Installation Interfaces- asymmetric Digital Subscriber Line (ADSL) Metallic Interface, June 1998

Black, U., PPP and L2TP: Remote Access Communications, Prentice Hall PTR, Upper Saddle River, New Jersey 07458, 1999

Bluetooth Special Interest Group, Specification of the Bluetooth System; Core, Version 1.0 B, December 1999

Dell, White Paper, Wireless Technologies, August 1999

Egevang, K., Francis, P., RFC 1631, The IP Network Address Translator (NAT), May 1994

ETSI Standard, EN 300 652, High Performance Radio Local Area Network (HIPERLAN) Type 1; Functional specification, Version 1.2.1, July 1998

ETSI Technical Report, TR 101 683, HIPERLAN Type 2; System Overview, Version 1.1.1, February 2000

ETSI Technical Specification, TS 101 135, HDSL core specification and applications for combined ISDN-BA and 2048 kbit/s transmission, Version 1.5.2, September 1999

ETSI Technical Specification, TS 101 270-1, Very High speed Digital Subscriber Line (VDSL); Part 1: Functional requirements, Version 1.2.1, October 1999

ETSI Technical Specification, TS 101 524-2, Symmetric single pair high bit rate Digital Subscriber Line (SDSL); Part2: Transceiver requirements, Version 1.1.1, June 2000

ETSI's WebPages, 2001, <http://www.etsi.org/technicalactiv/HIPERLAN2.htm>

ETSI's WebPages, Spectral Compatibility – Classification of signals, 1999, <http://www.etsi.org>

Federal Communications Commission, Amendment of Part 15 of the Commission's Rules Regarding Spread Spectrum Technology, August 2000

Fowler, D., Virtual Private Networks: Making the Right Connection, Morgan Kaufmann Publishers, San Francisco, California, 1999

Geier, J., Wireless LANs: Implementing Interoperable Networks, Macmillan Technical Publishing, 1999

Ginsburg, D., Implementing ADSL, Reading Massachusetts USA, July 1999, Addison-Wesley

Gross G., Kaycee M., Lin A., Malis A., Stephens J., RFC-2364, PPP over AAL5, July 1998

Grossman D., Heinänen J., RFC-2684, Multiprotocol Encapsulation over ATM Adaptation layer 5, September 1999

Halsall, F., Data Communications, Computer Networks and Open Systems, United Kingdom 1997, Addison-Wesley

Hamzeh K., Pall G., Verthein W., Taarud J., Little W., Zorn G., RFC 2637, Point-to-Point Tunneling Protocol, July 1999

HomeRF Working Group, Technical Presentation, 2000

HomeRF Working Group, Technical Summary of the SWAP Specification, March 1998

IEEE Standard, IEEE Std 802.11-1999, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, August 1999

IEEE Standard, IEEE Std 802.11a-1999, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, September 1999

IEEE Standard, IEEE Std 802.11b-1999, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, September 1999

Infrared Data Association, Serial Infrared Link Access Protocol (IrLAP), Version 1.1, June 1996

ITU-T, Draft G.991.2, Single-Pair High-Speed Digital Subscriber (SHDSL) transceivers, February 2000

ITU-T, G.992.1, Asymmetrical Digital Subscriber Line (ADSL) Transceivers, June 1999

ITU-T, Recommendation I.361, B-ISDN ATM Layer Specification, 1999

ITU-T, Recommendation I.363.1, B-ISDN ATM Adaptation Layer specification: Type 1 AAL, 1996.

Johnsson, M., HIPERLAN/2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band, Version 1.0, HIPERLAN/2 Global Forum, 1999

Lynross Training & Consultancy, Advanced ATM (module 1), course material for course number T223, London, 1998.

Megowan, P., Suvak, D., Knutson, C., IrDA Infrared Communications: An Overview, Counterpoint Systems Foundry, Inc., 2000

Pendolin, H., Rate Adaptive Digital Subscriber Line Modem based on CAP technology, Helsinki University Of Technology, Sähkötekniikan osasto, Diplomityö, 1997.

Quilici, J., Broadband Access: G.SHDSL: Reaching the Access Network, Communication Systems Design web page 2001, <http://www.commsdesing.com>

Suitala, T., ATM switching chipset in an access node, Helsinki University of Technology, Sähkötekniikan osasto, Diplomityö, 1999.

Townsley W., Valencia A., Rubens A., Pall G., Zorn G., Palter B., RFC 2661, Layer Two Tunneling Protocol "L2TP", August 1999

Tsirtsis, G., Srisuresh, P., RFC 2766, Network Address Translation - Protocol Translation (NAT-PT), February 2000

Wireless Ethernet Compatibility Alliance (WECA), Wi-Fi System Interoperability Test Plan, Version 1.0a, March 28, 2000

APPENDIX A. CONFIGURATIONS IN INITIAL TESTS

Parameter	WLAN-Station values	MW1122 values
RTS Threshold (bytes)	Lucent: Off 3COM: 300 Cisco: Off Symbol: 400	Default (2301) Default Default Default
Fragmentation (bytes)	Lucent:Off 3COM: 500 Cisco:500 Symbol: Off	Default (2301) Default Default Default
WEP	Lucent: Key=0x9876543210 3COM: Off Cisco: Off Symbol: Key=0x0123456789	Key=0x9876543210 Off Off Key=0x0123456789
Power Save	Lucent: No 3COM: No Cisco: On, PSP Symbol: On	- - - -
Channel	Lucent: - 3COM: 3 Cisco: - Symbol: -	1 3 6 11
Basic Rates	Lucent: - 3COM: All Cisco: - Symbol: -	1,2 All 1,2 All

APPENDIX B. CONFIGURATIONS IN EXTENDED TESTS

Parameter	WLAN-Station values	MW1122 values
RTS Threshold (bytes)	Lucent: Off 3COM: 300 Cisco: 300 Symbol: 400	Default (2301) Default Default Default
Fragmentation (bytes)	Lucent:Off 3COM: Off Cisco:500 Symbol: Off	Default (2301) Default Default Default
WEP	Lucent: Key=0x9876543210 3COM: Off Cisco: Off Symbol: Key=0x0123456789	Key=0x9876543210 Off Off Key=0x0123456789
Power Save	Lucent: No 3COM: On Cisco: On Symbol: On	- - - -
Channel	Lucent: - 3COM: 3 Cisco: - Symbol: -	2 4 5 7
Basic Rates	Lucent: - 3COM: - Cisco: - Symbol: -	All All All 1,2

Parameter	WLAN-Station values	MW1122 values
RTS Threshold (bytes)	Lucent: 256 3COM: Off Cisco: Off Symbol: Off	Default (2301) Default Default Default
Fragmentation (bytes)	Lucent: Off 3COM: 500 Cisco: 500 Symbol: Off	Default (2301) Default Default Default
WEP	Lucent: Key=0x9876543210 3COM: Off Cisco: Off Symbol: Key=0x0123456789	Key=0x9876543210 Off Off Key=0x0123456789
Power Save	Lucent: No 3COM: No Cisco: On Symbol: No	- - - -
Channel	Lucent: - 3COM: 3 Cisco: - Symbol: -	8 9 10 11
Basic Rates	Lucent: - 3COM: All Cisco: - Symbol: -	All 1,2 All 1,2

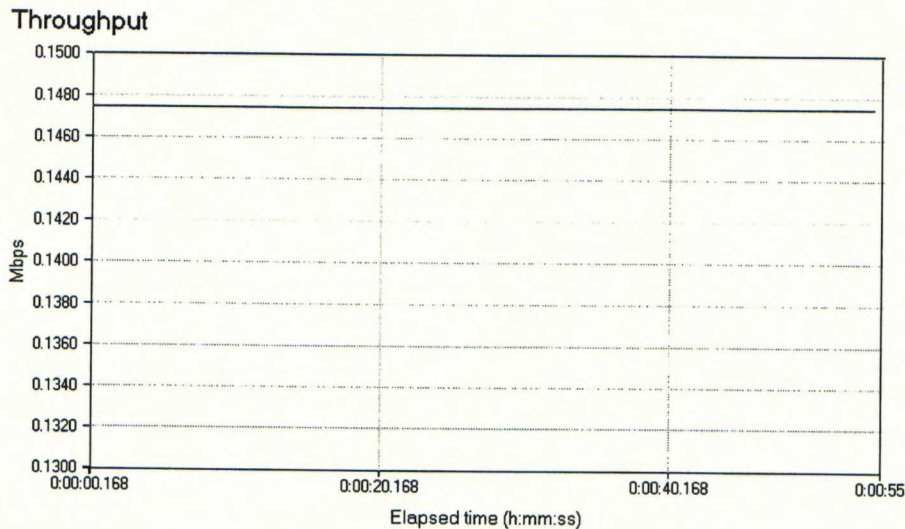
APPENDIX C. CONFIGURATIONS IN SPECIAL TESTS

Parameter	WLAN-Station values	MW1122 values
ESSID	3COM: "Multicast" Cisco: "Multicast" Lucent: "Multicast"	"Multicast" "Multicast" "Multicast"
Beacon Interval (ms)	3COM: Default Cisco: Default Lucent: 150	Default (200) Default Default
Channel	3COM: 8 Cisco: 8 Lucent: 8	8 8 8
RTS Threshold (bytes)	3COM: Default Cisco: Default Lucent: Default	Default (2301) Default Default
Fragmentation (bytes)	3COM: Default Cisco: Default Lucent: Default	Default (2301) Default Default
WEP	3COM: Key=0x0123456789 Cisco: Key=0x0123456789 Lucent: Key=0x0123456789	Key=0x0123456789 Key=0x0123456789 Key=0x0123456789
Basic Rates	3COM: All Cisco: All Lucent: All	All All All

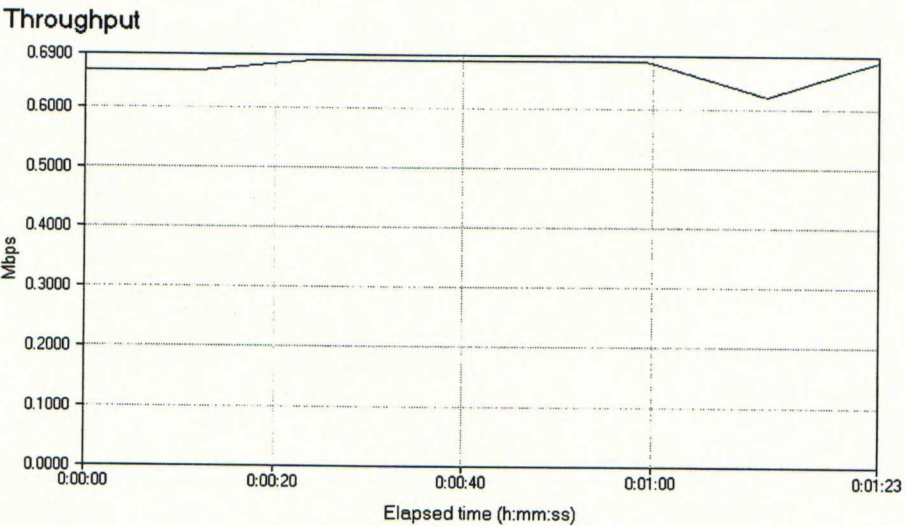
APPENDIX D. MEASURED AND TARGET THROUGHPUT VALUES

Test	Measured Average Value / Mbps	Target Value / Mbps
A1DT1	2.941	2.8
A1DT2	4.506	2.1
A1DT3	0.582	0.3
A2DT1	2.395	2.3
A2DT2	2.621	2.0
A2DT3	0.598	0.25
A3DT1	0.12	0.1
A3DT2	0.193	0.1
A3DT3	0.004	0.004
A4DT1	2.194	2.0
A4DT2	3.413	2.2
A4DT3	0.483	0.23
EA1DT1	3.102	1.4
EA1DT2	4.463	1.4
EA1DT3	0.583	0.25
EA2DT1	2.305	3.1
EA2DT2	3.787	3.1
EA2DT3	0.57	0.3
EA3DT1	0.147	0.2
EA3DT2	0.306	0.25
EA3DT3	0.004	0.003
EA4DT1	2.183	1.6
EA4DT2	3.227	1.2
EA4DT3	0.405	0.29
EA5DT1	2.953	1.1
EA5DT2	3.925	1.0
EA5DT3	0.582	0.24
EA6DT1	2.515	1.9
EA6DT2	3.012	2.4
EA6DT2	0.605	0.29
EA7DT1	0.102	0.15
EA7DT2	0.18	0.4
EA7DT3	0.004	0.002
EA8DT1	2.383	1.6
EA8DT2	3.958	1.7
EA8DT3	0.485	0.25
MCA1DT	0.08	0.05
MCA2DT	0.077	0.05
MCA3DT	0.077	0.05
MCA4DT	0.076	0.05

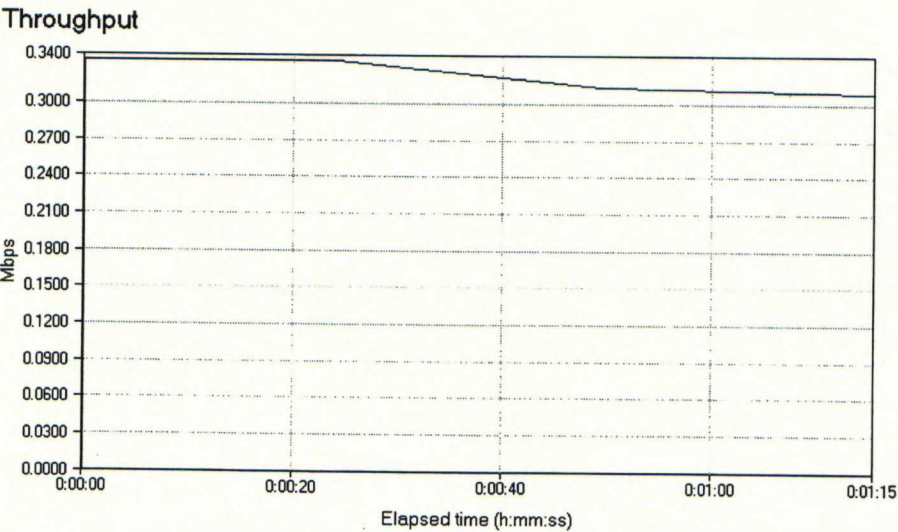
APPENDIX E. THROUGHPUT VALUES IN TEST CASE EA3DT1



Measured Throughput of MW1122

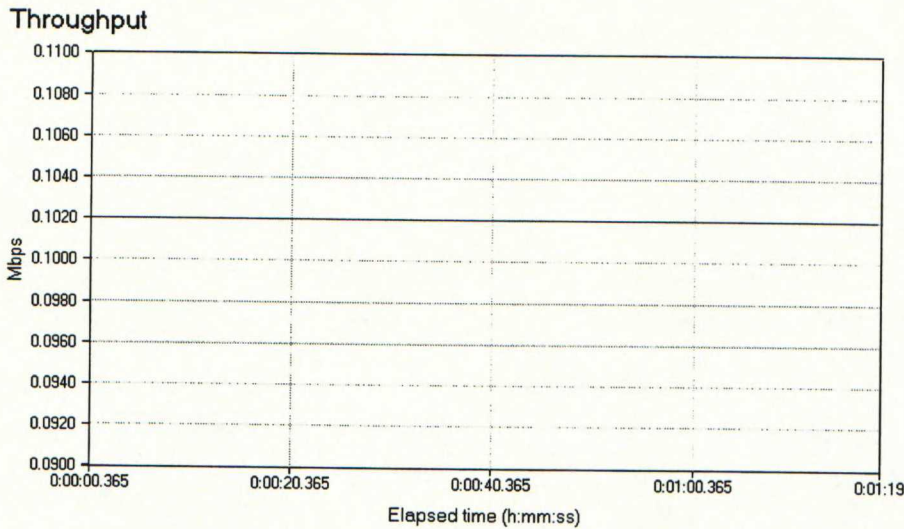


Measured Throughput of Nokia A032

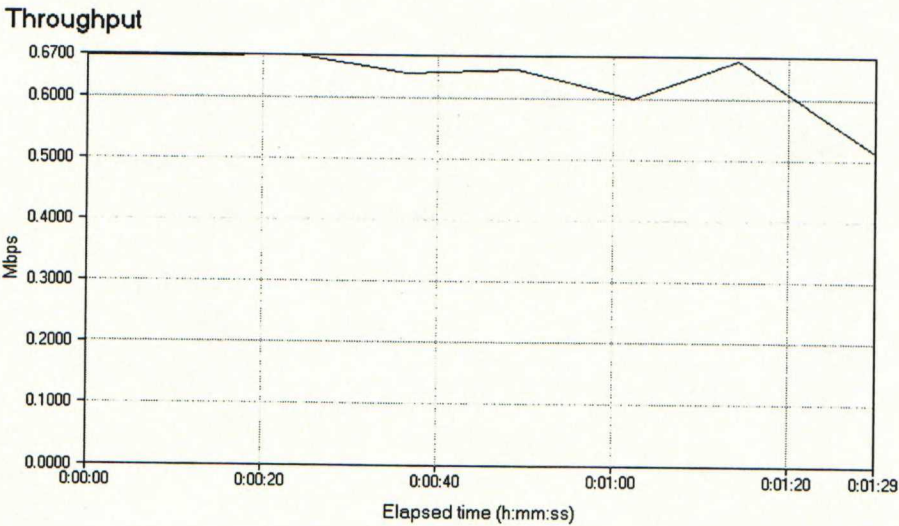


Measured Throughput of Lucent AP

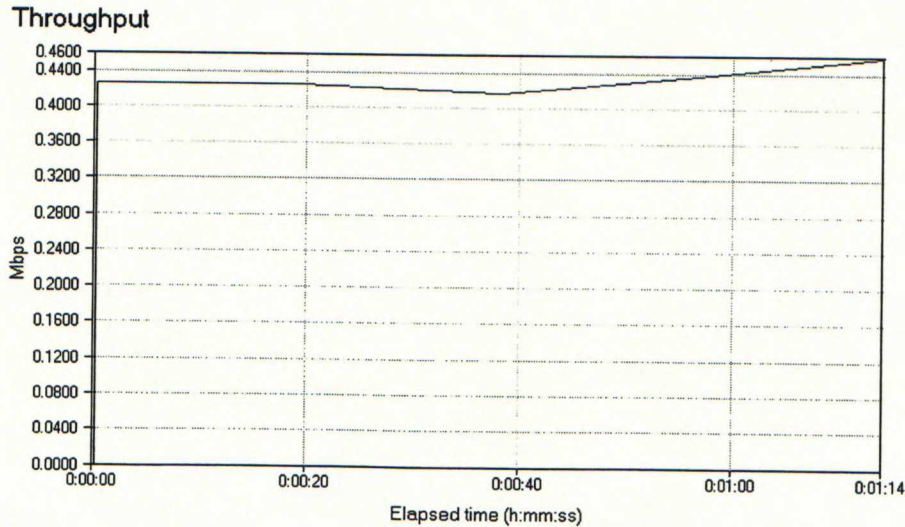
APPENDIX F. THROUGHPUT VALUES IN TEST CASE EA7DT1



Measured Throughput of MW1122

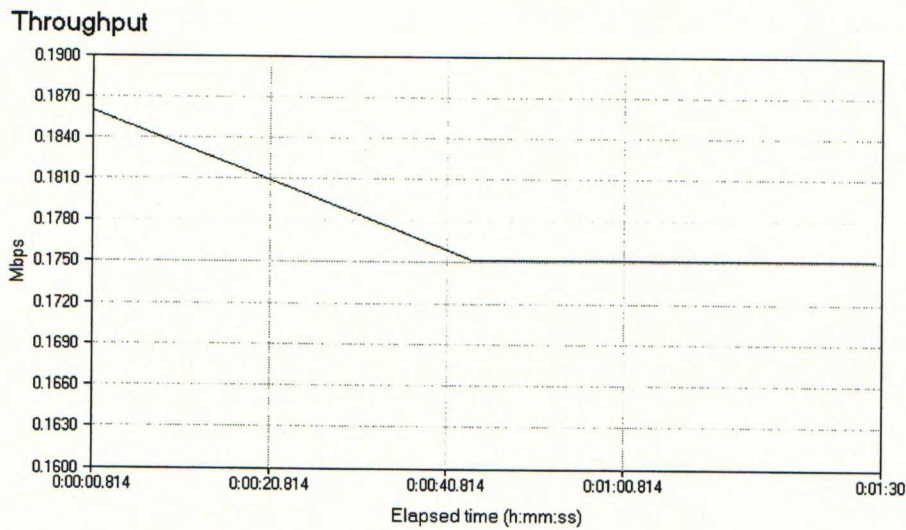


Measured Throughput of Nokia A032

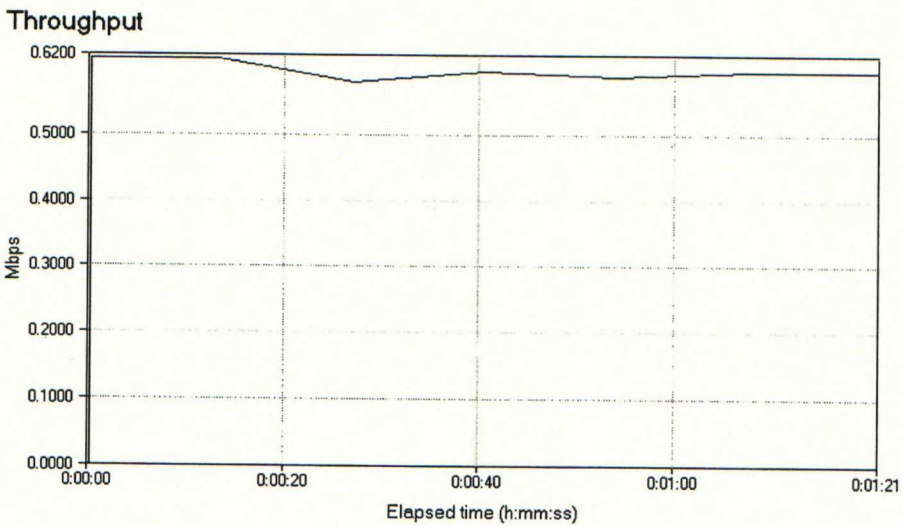


Measured Throughput of Lucent AP

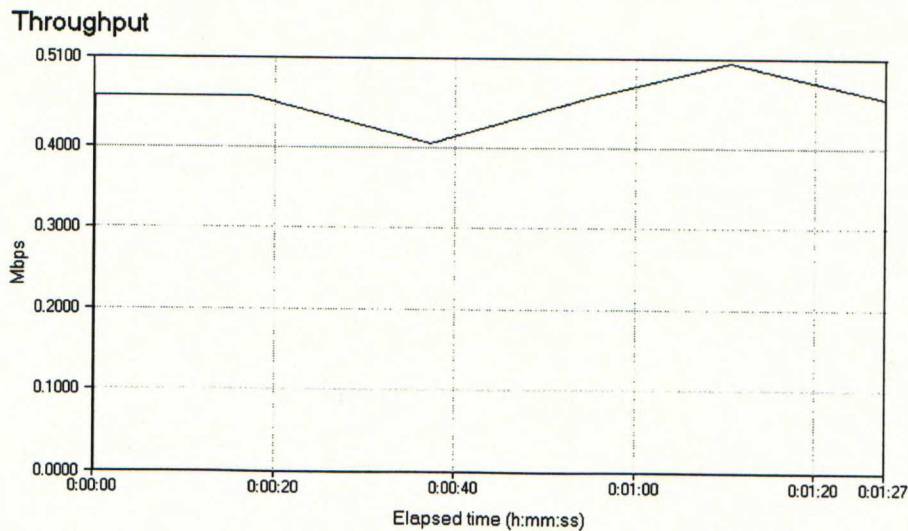
APPENDIX G. THROUGHPUT VALUES IN TEST CASE EA7DT2



Measured Throughput of MW1122



Measured Throughput of Nokia A032



Measured Throughput of Lucent AP