Matti Uljas

Performance Study of Local Area Network Devices in IPTV Use

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi
diplomi-insinöörin tutkintoa varten Espoossa 10.5.2010

Työn valvoja:

Prof. Risto Wichman

Työn ohjaaja:

Jari-Pekka Hela-Aro

Aalto-yliopisto
Teknillinen korkeakoulu

AALTO-YLIOPISTO
TEKNILLINEN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Matti Uljas

Työn nimi: Tutkimus lähiverkon laitteiden suorituskyvystä IPTV käytössä

Päivämäärä: 10.5.2010 Kieli: Englanti Sivumäärä: 11 + 77

Elektroniikan, tietoliikenteen ja automaation tiedekunta
Signaalinkäsittelyn ja akustiikan laitos
Professuuri: Signaalinkäsittely Koodi: S-88

Valvoja: Prof. Risto Wichman
Ohjaaja: Jari-Pekka Hela-Aro

Tässä diplomityössä tutkitaan vaihtoehtoisia tapoja ethernet -kaapeleille suorituskykyisen LAN -verkkon rakentamiseen kotitalouksissa. Tarkastelun pääpaino on WLAN -laitteissa, mutta mukaan on otettu myös yksi sähköjohtoa ja yksi antennikaapelia siirtotienään käyttävää laitetta. Tarkoituksena on selvittää laitteiden suorituskyvyn rajat ja tutkia niiden sopivuutta erityisesti IPTV -signaalin välittämiseen. Laitteiden olisi pystyttävä luomaan suorituskykyinen ja ennen kaikkea luotettava yhteys, mikä kattaa keskivertokokoisen huoneiston.

Nopeat internetyhteydet yleistyvät ja tuovat tullessaan uusia mahdollisuuksia palvelujen tarjoajille. Ne pystyvät tarjoamaan asiakkailleen uusia palveluja, kuten internetvälitteisiä puheluja, televisiokanavia ja videovuokrausta. Uusien palveluiden täysimittaiseen hyödyntämiseen ei enää riitä se, että internetyhteys tuodaan vain tietokoneeseen. Myös televisio ja puhelin pitäisi saada yhdistettyä internetiin. Ongelma voidaan ratkaista ethernet -kaapeleiden avulla, mutta kaapeleiden asentaminen pitkin huoneistoa ei ole aina se esteettisin ratkaisu.

Laitteiden suorituskykyä tutkitaan mittaamalla niiden tiedonsiirtonopeuksia eri protokollien ja siirtoteiden kanssa. Tarkoituksena on kartoittaa mahdollisia ongelma-alueita ja pohtia niiden syitä. Lopullisena päämääränä on nimetä testatuista laitteista ne, jotka soveltuvat IPTV -signaalien siirtämiseen.

Avainsanoja: IPTV, WLAN, Multicast, IGMP, LAN

AALTO UNIVERSITY
SCHOOL OF SCIENCE AND TECHNOLOGY

ABSTRACT OF THE
MASTER'S THESIS

Author: Matti Uljas

Title: Performance Study of Local Area Network Devices in IPTV Use

Date: 10.5.2010 Language: English Number of pages: 11 + 77

Faculty of Electronics, Communications and Automation
Department of Signal Processing and Acoustics
Professorship: Signal Processing

Supervisor: Prof. Risto Wichman
Instructor: Jari-Pekka Hela-Aro

This thesis includes a study of alternative ways to build a fast LAN without Ethernet cables into a common household. The main focus is in the WLAN products but also one product that uses power lines and one product that uses antenna cables to transmit information are included in the study. The purpose is to find out the performance limits of the devices and study their usability especially for the IPTV signal transmission. The devices should be able to create a high performance and reliable connection which should cover a common household.

Fast Internet connections are becoming more and more common. This gives the Internet service providers possibilities to offer new services to the customers. For example, they can relay phone calls, television channels or rented videos to the customers via the Internet connections. This means that the customers have to connect not only their computers to the Internet but also their phone and televisions as well. This problem can be solved with the Ethernet cables but in many case it is not the most aesthetic solution.

The devices performance is studied with the series of tests that measures their capabilities to transmit information while using different transmission protocols and paths. The purpose is to find out the possible trouble spots and to find the explanations to them. The final goal is to name the devices which can be used to transmit IPTV signals.

Keywords: IPTV, WLAN, Multicast, IGMP, LAN

Preface

I would like to thank my supervisor Risto Wichman. I am grateful for his excellent support and fast replies to my questions. I would also like to thank my instructor Jari-Pekka Hela-Aro. I am grateful for his decision to give me an opportunity to do this study and to give me as much freedom to decide the study methods as it was possible. The process to write this thesis was much longer what I had anticipated. I am really relieved that it is finally done.

Otaniemi, 10.5.2010

Matti Uljas

Table of Content

List of Figures

Appendix

List of Tables

Acronyms

ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
BPSK	Binary Phase-Shift Keying
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
dBm	Power ration in decibels compared to one milliwatt
DSLAM	Digital Subscriber Line Access Multiplexer
DUT	Device Under Test
EIRP	Equivalent Isotropically Radiated Power
FFT	Fast Fourier Transform
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IPTV	Internet Protocol Television
ISI	InterSymbol Interference
ISP	Internet Service Provider
LAN	Local Area Network
LOS	Line Of Sight
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MP3	Mpeg-1 Audio Layer 3
OFDM	Orthogonal Frequency-Dimension Multiplexing
OSI model	Open Systems Interconnection Reference Model
PSK	Phase-Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RTS	Ready to Send
SISO	Single-Input Single-Output

TC	Traffic Class
TXOP	Transmission Opportunity
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
VOD	Video On Demand
VoIP	Voice Over Internet Protocol

1. Introduction

This thesis evaluates the performance of different LAN (*Local Area Network*) products, the study's main focus being to test wireless products and their capabilities. The products were tested in different situations while using different transmission protocols. Not only wireless products were tested but also products that use cables (wire lines or coaxial antenna cables) to transmit information. The study, however did not include the products that use Ethernet cables as their main source of information transmission.

Over the past few years the connection speeds to the Internet have been increasing steadily. It is common that customers have an 8 Mbps or even faster download speed. The fast connections make it possible for ISPs (*Internet Service Provider*) to offer additional services, such as: VoIP (*Voice Over Internet Protocol*), IPTV (*Internet Protocol Television*), VOD (*Video On Demand*) and as well as many others. Basically it is possible to use the computer network (Internet) and fast broadband connections to combine many services and then bring them to consumers via a single wire.

Many of the new services like IPTV demand a steady and high speed connection to work as intended. The problem is that especially in old households there is only one or two phone sockets where the ADSL (*Asymmetric Digital Subscriber Line*) modems can be connected and devices like phone, television and computer are usually spread all over the house. This may cause inconveniences because the most commonly used method to create a high performance LAN is to use Ethernet cables. This may lead in to a situation where the customer must lay long cables around his house. Cables are always inconvenient especially when they run through doorways.

The reason why this study was made was to find out if there is an alternative way of creating a high performance LAN, other than by using Ethernet cables. The wireless products are the most obvious solution but do they have capabilities to handle the transmission requirements which the new services like IPTV demand? The other way to do a "wireless" network is to use the wires that every household already has, like power lines and coaxial antenna cables, and use them to transmit the information signal.

Products performance was tested with different transmission protocols. Tests were repeated in different environments so that their range of coverage could be measured. The results were studied and products suitability to build a high performance network was evaluated.

The study was made from the end user's point of view. All the products that were chosen for the tested were designed for customer use. The focus of the tests was in the IPTV and multicast performance. If the tested devices could transmit IPTV signal then their performance is most likely good enough for the other services too. Other important feature was the range of coverage. The products should be able to cover the customer's whole household with high performance network.

It is expected that especially wireless devices might have difficulties with the IPTV and multicast traffic. It is assumed that when transmission path grew longer the quality of IPTV signal will degenerate quickly. In the test is included a very promising WLAN (*Wireless Local Area Network*) device, *Ruckus*. It seems that *Ruckus* might have better performance compared to other WLAN devices especially with IPTV transmission, at least on the paper.

The thesis starts with a brief presentation about wireless transmission. It is discussed what kinds of phenomenon the wireless transmission faces and how these affect to the transmission. This thesis will concentrate more about testing different devices and evaluating them than to the technology and its details. After the short technology presentation it will be presented in more detailed manner what kinds of tests were done and how those were performed. Then the results are presented and the final evaluation about how the tested devices managed is given.

2. Brief Overview of Technology

This chapter will give a brief overview to basics of wireless communication, WLAN technology and multicast transmission. This information helps to better understand what the different tests measure and why some products have better performance than others.

2.1. Basics of Wireless Communication

When information is transmitted through air it faces lots of difficulties including things such as: multipath propagation, interference from other devices, attenuation and changing transmission environments. This chapter will give some basic understanding of wireless communication.

In this chapter is presented the basic ideas about *free space path loss* and the benefits of directional antennas. Also described are the problems that *multipath propagation* can cause and how these can be encountered with multiple antennas.

The basic theory behind the MIMO (*Multiple-Input Multiple-Output*) technology is introduces briefly in this chapter. As well as the implementations that the different WLAN manufacturers use in their devices. The manufactures' implementations differed greatly from each other and strangely enough from the theory presented in the scientific literature.

At the end of this chapter is included a brief overview to WLAN technology. There can be found some basic information about the modulation method and collision avoidance techniques what are used in WLAN devices.

2.1.1. Radio Link and Free Space Path Loss

The *free space path loss* is a common concept in wireless communication which defines the basic attenuation that a signal faces when it travels further away from a transmitter in a free space [1]. In other words, it tells the loss that would occur in a region which is free of all objects that might absorb or reflect the electromagnetic fields. In *free space path loss* it is assumed that the signal is transmitted at equal power in every direction.

A signal transmitted using an ideal isotropic antenna is a similar process as blowing up a balloon. At first when the balloon is still small its colour is dark which means that the surface of the balloon is thick. When the balloon gets bigger its colour starts to fade as the surface gets thinner. In both cases, the balloon has the same amount of rubber but in the latter case it has to cover a larger surface area. This is exactly what happens to a signal in a free space the further away it travels from a transmitter. The signal gets weaker. *Free space path loss* illustrates how much the signal attenuates.

Let us start with a basic radio link: one receiver and one transmitter. They are far away from anything that could cause interference to their wireless communication. Imagine that the transmitter and receiver are hovering in mid air far away from any obstacles. In this kind of situation there is a LOS (*Line Of Sight*) between the communicating pair. Because there are no obstacles near the transmitter or receiver, there will not be any reflecting signals. This means that all the energy that is transmitted from the transmitter travels to the receiver via the LOS path. This is in many ways an ideal situation for wireless communication. A sketch at this kind of radio link is presented in Figure 2.1.

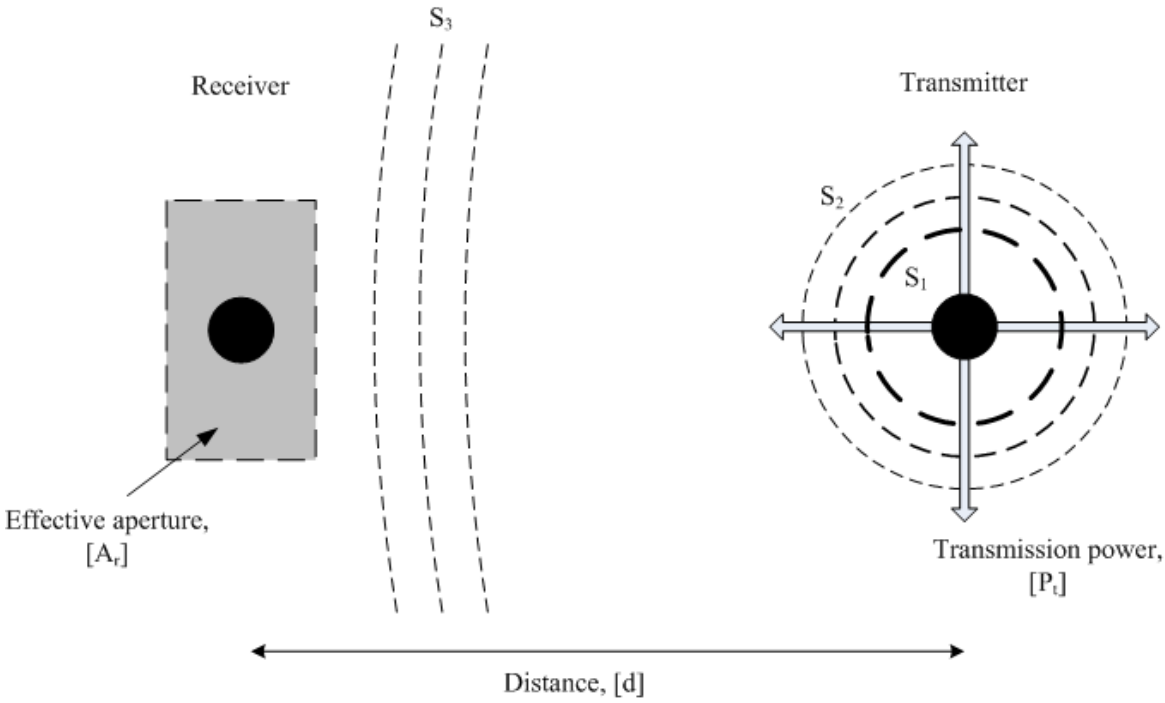


Figure 2.1: Radio link looking from directly above. S_1, S_2 and S_3 represent flux densities at different distances from the transmitter. $S_1 > S_3$ but the overall powers are the same regardless of the distance.

Calculating the *free space path loss* is quite simple. Consider that the transmitter is sending a signal at power P_t through an isotropic antenna which radiates equally in all directions. At distance d from the transmitter, the radiated power P_t is distributed uniformly over a surface area of a sphere of radius d. It is an easy task to determine the *power flux density S* at that distance. This is shown in Eq. (1).

$$S = \frac{P_t}{4\pi * d^2} \tag{1}$$

The transmission loss then depends on how much power is captured by the receiving antenna. This ability is called as antenna's *effective aperture* A_r and it tells the size of the area from where the antenna absorbs the power. The sizes of the antenna's *effective aperture* and its physical size do not necessarily have anything to do with each other. The antenna's physical size can be smaller or bigger than the size of the *effective aperture* [3]. Now the formula to the power P_r that the receiver can absorb can be written. This is shown in Eq. (2).

$$\Pr = S * A_r \tag{2}$$

The size of the *effective aperture* A_r depends on the gain G of the antenna and the used frequency. The dependency is shown in Eq. (3). The antenna's gain means its ability to focus the transmission power in a certain direction [3].

$$A_r = \frac{G * \lambda^2}{4\pi} \tag{3}$$

where λ is the wavelength. Now it is possible to combine all three Eq.s (1), (2) and (3) into one final formula. The result is shown in Eq. (4).

$$P_r = P_t * G * \left(\frac{\lambda}{4\pi * d} \right)^2 \tag{4}$$

From Eq. (4) it is possible to separate the *free space path loss* L_p. This is shown in Eq. 5. The units d and λ must be at the same scale in that formula.

$$L_p = \left(\frac{4\pi * d}{\lambda} \right)^2 \tag{5}$$

As can be seen from Eq. (5), the distance between the devices is in that formula and it is squared. This means that when the distance increases the attenuation also increases but more rapidly. For example, if the distance is doubled the *free space path loss* will grow fourfold. This leads to a situation that the attenuation due to the *free space path loss* will rise very steeply when the distance between the transmitter and receiver gets longer.

There are some ways to counter this attenuation. The most obvious ones are to use more sensitive receivers or to increase the transmission power. Another useful method is to focus the transmission power only in the direction where the receiver is located. This can be done with directional antennas. The next chapter shows how much directional antennas can improve the situation compared to isotropic antennas.

2.1.1.1. Example Calculation of Free Space Path Loss

At first it is calculated how far away the transmitter and receiver can be from each other when both of them use isotropic antennas. No other losses than the *free space path loss* are taken into account. A formula for *free space path loss* is presented in Eq. (5). But before adding the values to that formula, let us modify it slightly. It is more convenient to calculate frequencies in megahertz and distance in kilometers. The modified formula for *free space path loss* is presented in Eq. (6)

$$L_p = \left(\frac{4\pi * d}{\lambda}\right)^2 = \left(\frac{4\pi * f * d}{c}\right)^2 = \left(\frac{4\pi * f_{MHz} * 10^6 * d_{km} * 10^3}{3 * 10^8}\right)^2$$
$$L_p = \left(\frac{40\pi * f_{MHz} * d_{km}}{3}\right)^2 \quad (6)$$

where c is the speed of light and, as it can be seen, only a rough approximation was used. In the last part of Eq. (6), the frequency f_{MHz} is in MHz and the distance d_{km} is in kilometres. Because it is a lot easier to calculate with decibels, Eq. (6) is written a little differently. The decibels form of *free space path loss* is presented in Eq. (7).

$$L_p = \left(\frac{40\pi * f_{MHz} * d_{km}}{3}\right)^2 = 20\log\left(\frac{40\pi * f_{MHz} * d_{km}}{3}\right)$$
$$L_p = 20\log\left(\frac{40\pi}{3}\right) + 20\log(f_{MHz}) + 20\log(d_{km}) \quad (7)$$
$$L_p = 32{,}4 + 20\log(f_{MHz}) + 20\log(d_{km})$$

Let us assume that the transmitter sends a signal at the frequency 2400 MHz and the transmission power is 20 dBm, which is about 100 mW. The receiver sensitivity is -70 dBm. With these starting parameters the signal can attenuate 90 dB before it gets too weak for the receiver. The starting parameters were chosen so that they simulate the WLAN communication. Now these parameters can be entered into Eq. (7).

$$
\begin{aligned}
L_p &= 32{,}4 + 20\log(2400) + 20\log(d) = 90 \\
L_p &= 32{,}4 + 67{,}6 + 20\log(d) = 90 \\
20\log(d) &= -10 \\
d &= 10^{-0{,}5} = 0{,}316km = 316m
\end{aligned}
\tag{8}
$$

With isotropic antennas the result is about 300 meters. Now let us make the same calculation with the assumption that both the transmitter and receiver use slightly directional antennas, which both have 3 dB gains. This means that the transmitter focuses its transmission power towards the receiver. The 3 dB gain means that the signal in the antenna's main slope is about twice as strong as with isotropic antennas. The directional antennas also receive signals better from the direction of their main lobes. So directional antennas do not only focus their transmission power in a certain direction but they also focus their receiving effectiveness too. All the other starting parameters are kept unchanged.

Because now we have 3 dB gains at the both ends of the link, this gives us altogether 6 dB more to the attenuation margin. This in turn means that the signal can attenuate 6 dB more than with isotropic antennas. In this case, the attenuation due to the *free space path loss* can be 96 dB. Again the parameters are entered to Eq. (7).

$$
\begin{aligned}
L_p &= 32{,}4 + 67{,}6 + 20\log(d) = 96 \\
20\log(d) &= -4 \\
d &= 10^{-0{,}2} = 0{,}631km = 631m
\end{aligned}
\tag{9}
$$

With directional antennas the connection is possible over 600 meters away. The result is quite clear. With directional antennas one can increase the transmission range at both ends of the link. The transmitter will send stronger signal towards the receiver which in turn can receiver signals more efficiently from its main slope. However this is not the case in reality. Regulations set boundaries for the maximum field strength.

In Finland the regulations require EIRP (*Equivalent Isotropically Radiated Power*) for WLAN devices to be 100 mW or less [2]. EIRP is the amount of power that a theoretical isotropic antenna would emit to produce the peak power density observed in the direction of maximum antenna gain. The transmitter's EIRP value is the transmission power plus antenna gain minus losses in transmission lines. This means that with WLAN devices only

the receiver's directional antenna can amplify the signal. So one more calculation is needed to clarify how much directive antennas can enhance the WLAN communication if they obey the existing rules.

All the other parameters are kept unchanged. Because only the receiver can benefit from the directive antenna, the signal can attenuate only 3 dB more than with isotropic antennas. This means that the signal can attenuate 93 dB. Once again the parameters are entered to Eq. (7).

$$\begin{aligned} L_p &= 32{,}4 + 67{,}6 + 20\log(d) = 93 \\ 20\log(d) &= -6{,}6 \\ d &= 10^{-0{,}33} = 0{,}468km = 468m \end{aligned} \qquad (10)$$

The connection is possible about 150 meters further away than with isotopic antennas. The benefit of using directive antennas is still noticeable.

2.1.1.2. Summary of Free Space Path loss

As the results showed, it is a good idea to use directional antennas. The maximum distance between transmitter and receiver crew to almost double when directional antennas were used. In theory, it is impossible to get as good results with isotropic antennas as with directional antennas. Of course, if the transmission path is trivial isotropic antennas suit just fine. But when the transmission path gets more complex, the directional antennas give far better results if they are aimed correctly.

Control is also needed. If directional antennas are aimed badly they are even worse than isotropic antennas. In theory, it would be quite simple task to aim two stationary directional antennas so that they would give the best performance. In real world, however, that is a more demanding process. The radio environment is constantly changing: Someone or something can block the currently used path or new interference sources can arise, like microwave ovens. Basically if you want the best performance when using directional antennas you should be constantly redirecting them.

2.1.2. Multipath Propagation

Another harmful phenomenon that normally causes problems in wireless communications is *multipath propagation*. This phenomenon occurs when signal from transmitter can travel to the receiver via more than one path. The signal can, for example, reflect from a wall or the ground. *Multipath propagation* is inevitable especially indoors and in urban environments where WLAN devices are usually used. A simplified situation is presented in Figure 2.2. *Multicast propagation* may cause some extra attenuation and disturbance which is called as *multipath fading*.

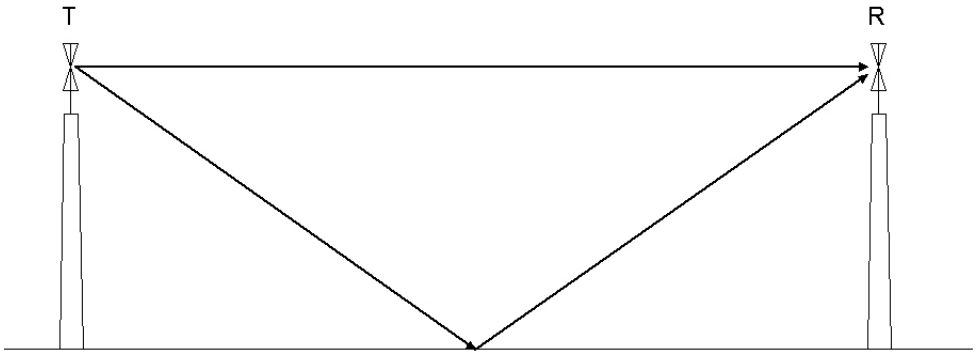


Figure 2.2: Signal can travel to the receiver R via two different paths: LOS and reflecting on the ground. This phenomenon is called the multipath propagation and it may cause multipath fading.

Every path that the signal travels has unique parameters: delay, attenuation, phase change, arriving and departing directions. This means that when the transmitter sends a single symbol, the receiver picks up multiple symbols which are all slightly different. This causes interference, especially when some paths' delays are longer than the used symbol time. In this case, the sent symbol will disturb the following symbol which is transmitted right after it.

In the worst situation, the length difference from two different paths is half of the wavelength or its uneven manifold. In this case, two received signals would cancel each other out due to their phase difference [4]. With the frequency 2400 MHz, which WLAN devices use, the half wavelength is about 6 cm. One reflection from a wall or ceiling can easily create this phenomenon.

Multipath fading is a very unpredictable phenomenon. The radio environment is constantly changing and *multipath fading* can turn a good connection into a bad one almost in an instant. Even small (compared to the wavelength) movements of devices can cause this. The extra attenuation due to this phenomenon can be several tens of decibels. So it can really cripple the wireless communication.

2.1.3. Diversity

Diversity is a one way to counter the effects of *multipath propagation*. There are many different types of diversity. The most common ones are: time diversity, frequency diversity and spatial diversity. They all share a common principle; the same signal is sent or at least received more than once. In time diversity the information is sent multiple times over the same channel but at different times. In frequency diversity the information is sent multiple times at the same time but at different frequencies. Because some of the devices that are going to be tested use spatial diversity, next is provided a description of how it works and why it enhances the device's performance.

In spatial diversity the information is sent only once but it is received with multiple antennas. Basically, this means that the signal is being sent via different paths to the receiver. In Figure 2.3 is presented the spatial diversity with two receiving antennas.

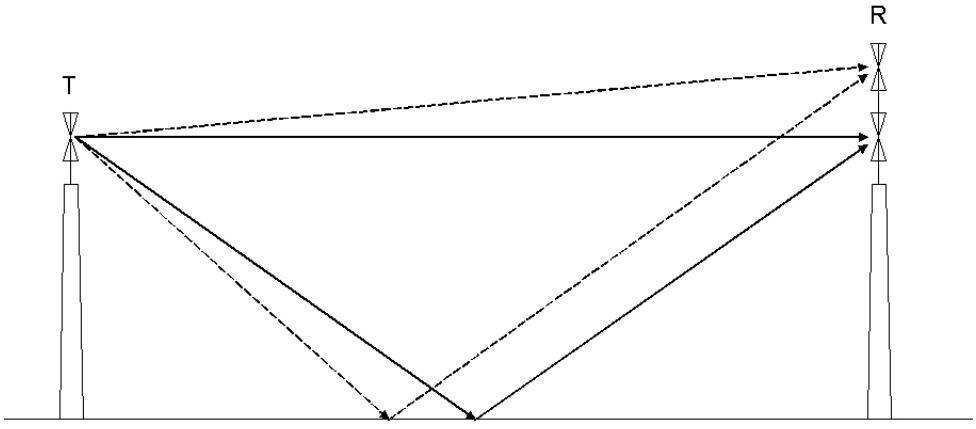


Figure 2.3: The receiver R now pick ups two signals. The receiver can then decide which signal to use for symbol detection.

Now the receiver picks up two signals, one from each antenna. The receiver can then choose the signal which has better quality and ignore the other. The idea behind this is that it is very unlikely that both signals face a high attenuation due to *multipath fading* at the same time. If the receiver is more sophisticated it can even combine the two received signals into a single even stronger signal. This will help noticeably against the attenuation caused by *multipath propagation*.

2.1.4. Multiple-Input Multiple-Output

The multiple signals from the *multipath propagation* can cause a lot of troubles for radio communication as has already presented in the previous chapters. MIMO technology can turn these extra paths to unique radio channels. With MIMO technology, the radio link capacity can be increased dramatically.

The MIMO technology is quite a new thing in the WLAN world and there are only loose guidelines about what can be called MIMO. Both *Planet* and *Ruckus* claim that they use MIMO antenna technology in their WLAN products. It is true that they both have multiple antennas, *Planet* has three and *Ruckus* six, but their ways if implementing MIMO differs much from each other. Next is discussed how the MIMO concept is defined in the scientific literature and then is presented how *Ruckus* and *Planet* have implemented it.

2.1.4.1. MIMO in Scientific Literature

The basic idea behind MIMO is that the transmitter sends two or more signals carrying unique information at once. The signals are sent using the same frequency band. The only difference between the signals is that they are send via different antennas. This is where the MIMO gets its MI (Multiple-Input) part. The MO (Multiple-Output) part is draw up from the fact that the signal is received with multiple antennas [5].

In traditional radio communication, the idea of sending more than one signal at the same time on the same frequency band would be impossible. The sent signals would disturb each other severely and this would make the reception impossible. Even in QAM (*Quadrature Amplitude Modulation*) where two signals are merged together and transmitted at

the same time, there are mechanics to keep the signals separated. Phase difference will ensure that the QAM signals can be detected correctly.

In the MIMO system there is no such mechanic. The signals are damaged for good and there is no simple way to repair them. The receiver has to count on brute force and solve the sent signals mathematically. This is possible if there are enough independent measurements from the sent signals. It is necessary to have more than one antenna at the reception to get those measurements. A MIMO link needs multipath propagation to work properly. A simplified radio link where MIMO transmission can take place is presented in Figure 2.4.

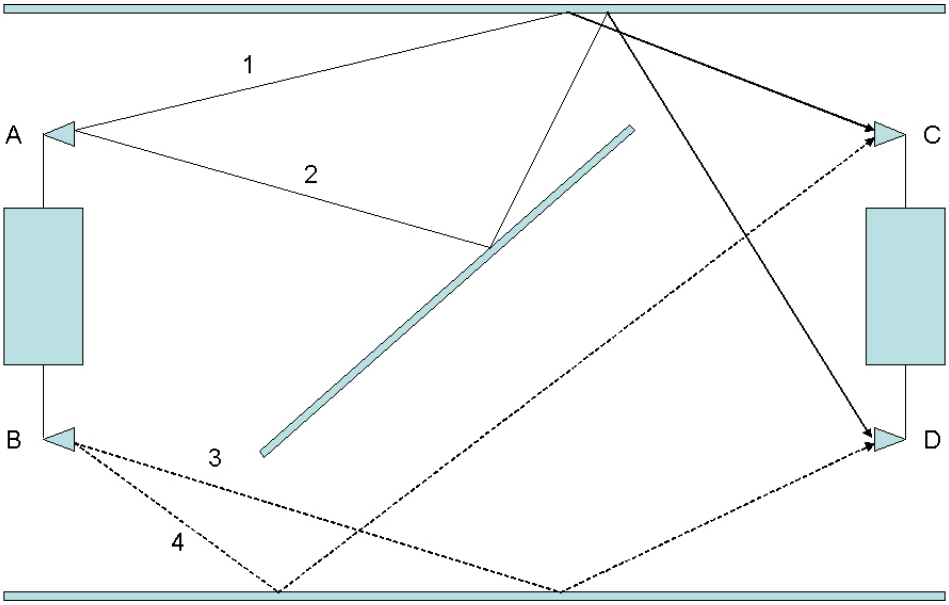


Figure 2.4: Multiple paths are formed between the communicating devices. In normal circumstances this would cause interference. But for MIMO technology this creates opportunities to transmit more information using the same amount of bandwidth.

Figure 2.4 shows four paths on which the signal can travel from the transmitter to receiver. Every path is unique, they are different lengths and they have a different amount of reflections. The received signals from these paths have different characteristics such as angle of reception, delay and phase.

The mathematical theory behind MIMO is presented in Figure 2.5. In theory, everything looks surprisingly simple. All that needs to de done to solve the transmitted signals is a

common matrix operation and that is it. In real life this is as simple as it is in theory but the tricky part is to estimate the channel matrix correctly.

After the receiver has estimated the channel matrix it can start to gather information pieces from different paths. When the receiver has enough samples from the sent signals it can calculate the sent symbols. A MIMO system can use every signal from every path to improve the symbol detection. This gives significant benefits compared to the traditional SISO (*Single-Input Single-Output*) method where the receiver picks only one signal and tries to detect the sent symbol from that.

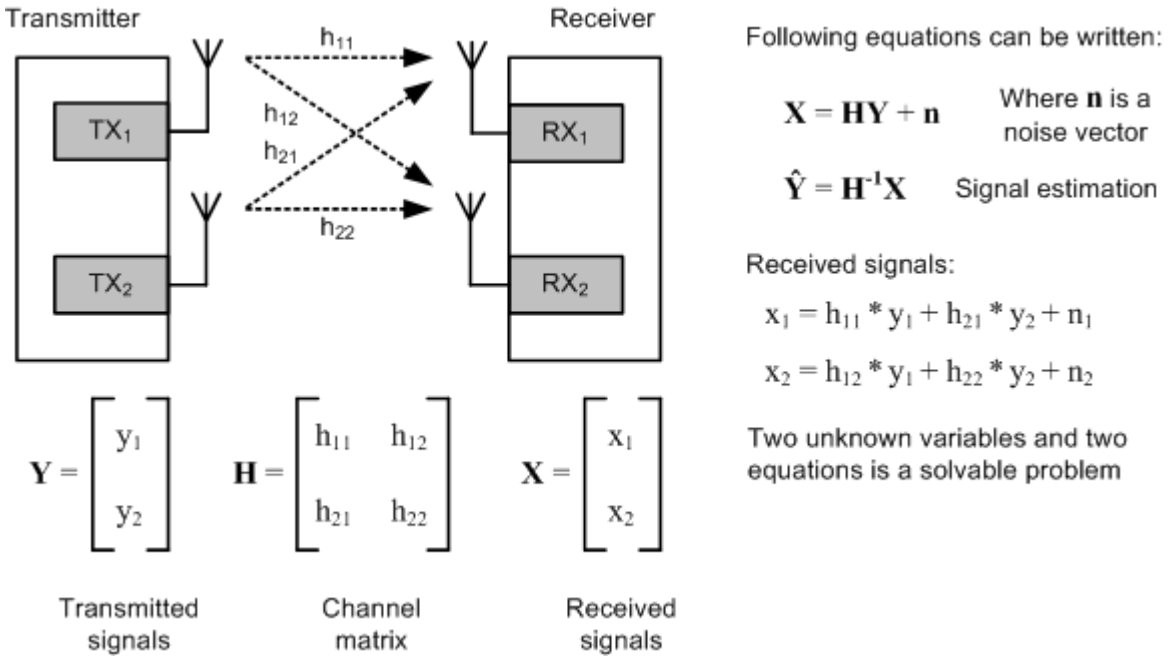


Figure 2.5: At least in theory the signal detection in MIMO is quite simple. In real life the hardest part is to estimate the channel matrix correctly.

Basically using MIMO technology in the situation which is presented in Figure 2.4, the system can transmit twice as much data in the same bandwidth and time as it is possible with traditional SISO technology. In theory, with more antenna pairs the link's channel capacity would rise linearly.

Just because a receiver and transmitter have multiple antennas does not make a radio system a MIMO system. It might as well mean that the system has some sort of spatial or frequency diversity to fight against multipath effects.

2.1.4.2. MIMO in Ruckus

Traditionally, isotropic antennas are used in WLAN products. This makes sense because WLAN devices want to cover as large an area surrounding them as is possible. The easiest way to do this is to transmit the signal in every direction at equal power. The advantage is that the device does not have to know where the receivers are. The disadvantage is that the signal is also sent in directions where there are no receivers. This causes unnecessary interference with other devices that are using the same frequency bandwidth.

In *Ruckus* devices this is done differently. There are six directional antennas in both the *Ruckus* AP (*Access Point*) and adapter. Devices do not use all the antennas at the same time. Only about two or three antennas per device are activated at any given moment. *Ruckus* devices have an algorithm that determines from the received signal what antennas will be used [6]. This means that *Ruckus* devices "know" where others WLAN devices are and then focuses its transmission and reception powers in those directions. This makes the coverage area larger than with isotropic antennas. Also the interference with other devices is fainter. The idea is presented in Figure 2.6.

This is the feature what *Ruckus* calls MIMO. This is not exactly how MIMO is presented in the scientific literature. In the end, this is nothing more than a mechanism for an active alignment of the transmission and reception power. Nevertheless, this feature is very effective and it gives *Ruckus* devices an edge compared to the other tested WLAN products. This is clearly shown in Chapter 5 where the results are presented.

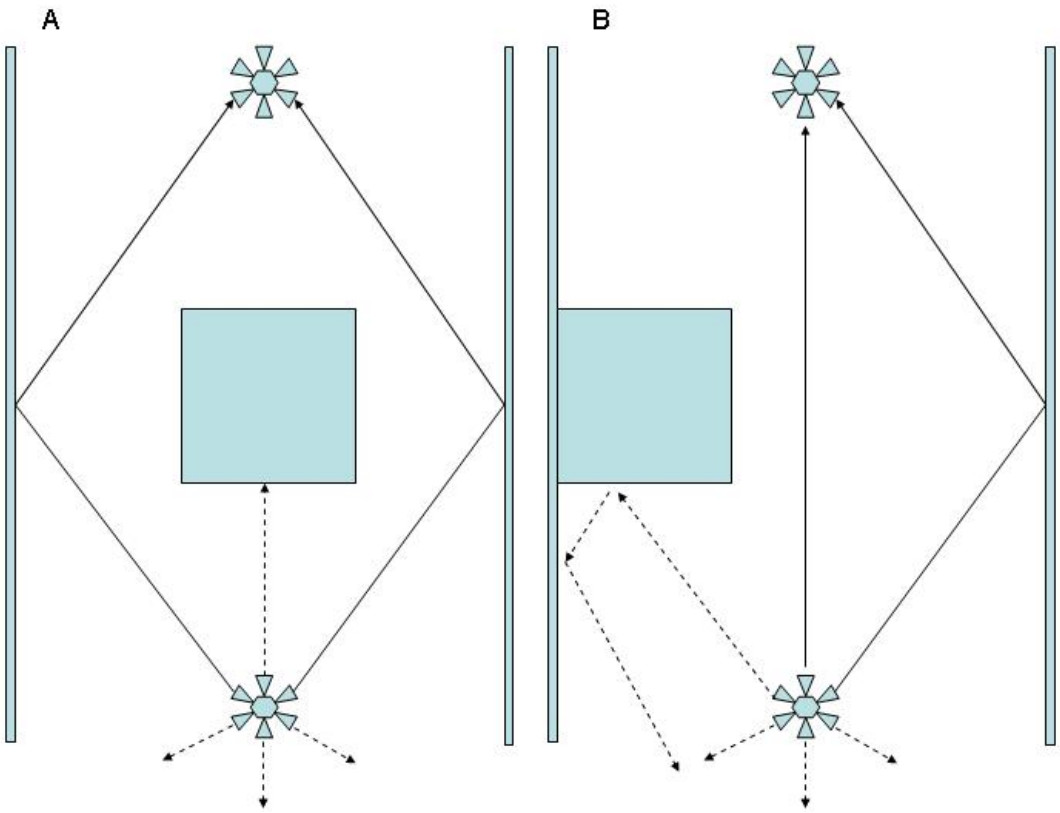


Figure 2.6: A and B show how the Ruckus changes the active antennas when situation alters.

The *Ruckus* device has six independent antennas which are slightly directional. Therefore it is not strictly an antenna array. The antennas are used separately and it is suspected that only one antenna at a time is used for transmission. This means that only one signal is sent. The signal can be received with several antennas. Because the exact way how the *Ruckus* devices send and receive signals is a trade secret, only assumptions can be presented. These assumptions are based on presentations and conversations with the *Ruckus* sales personnel. It would probably be wise to view this information with slight scepticism.

2.1.4.3. MIMO in Planet

The *Planet* WLAN device has three antennas, one for transmission and two for reception [7]. In other words, the *Planet* device sends only one signal which is received with two antennas. The *Planet* interpretation of MIMO is even further away from the scientific literature than *Ruckus*. The feature that *Planet* calls MIMO should rather be called SIMO (*Single-Input Multiple-Output*).

The advantage over a common SISO WLAN is that the two receiving antennas provide the device a spatial diversity mechanism. This means that the *Planet* device has a way to fight against signal fading caused by *multipath propagation*. This also gives an opportunity to combine the two received signals which gives a little edge compared to traditional WLAN devices, although not as large as what *Ruckus* gets. This can be also seen in Chapter 5 with the results.

2.2. Basics of WLAN Technology

This chapter includes a short technology presentation of WLAN showing how the channels are distributed in the IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 standard. Also discussed is the kind of modulation method used in WLAN devices and why this method was chosen. Lastly information is given about the kind of collision avoidance techniques, in other words access methods, which are used in WLAN devices.

It is good to know some of the basic of WLAN technology so that the forthcoming presentation of tests and their results would be more meaningful. This knowledge helps to make conclusions about what qualities different tests measure and, perhaps, helps to identify the reasons why the tested devices perform differently in the tests.

2.2.1. Channel Distribution in IEEE 802.11

The IEEE 802.11 standard defines the rules how WLAN devices should work. Next is presented briefly how the channels are distributed in the IEEE 802.11G standard. This knowledge is somewhat useful in the following chapters when the testing setups and results are presented.

The IEEE standard 802.11G operates around the 2,4 GHz frequency with a maximum raw data rate of 54 Mbps. The used bandwidth is divided up into 14 overlapping channels whose centre frequencies are 5 MHz apart. The allowed channels differ from country to

country. For example, in the United States only the channels 1-11 can be used, respectively in Europe the channels 1-13 are allowed.

The standard 802.11G specifies the spectral masks for every channel. In fact, the given spectral mask is very loose and the signals on different channels create much interference to channels near them. This leads to a situation that adjacent channels cannot be used close to each other.

In the IEEE standard 802.11G it is required that the signal power must be attenuated by at least 30 dB from its peak energy at ±11 MHz from the channel's centre frequency. The attenuation must be at least 50 dB at ±22 MHz from the centre frequency. The channel's spectral mask is illustrated in Figure 2.7.

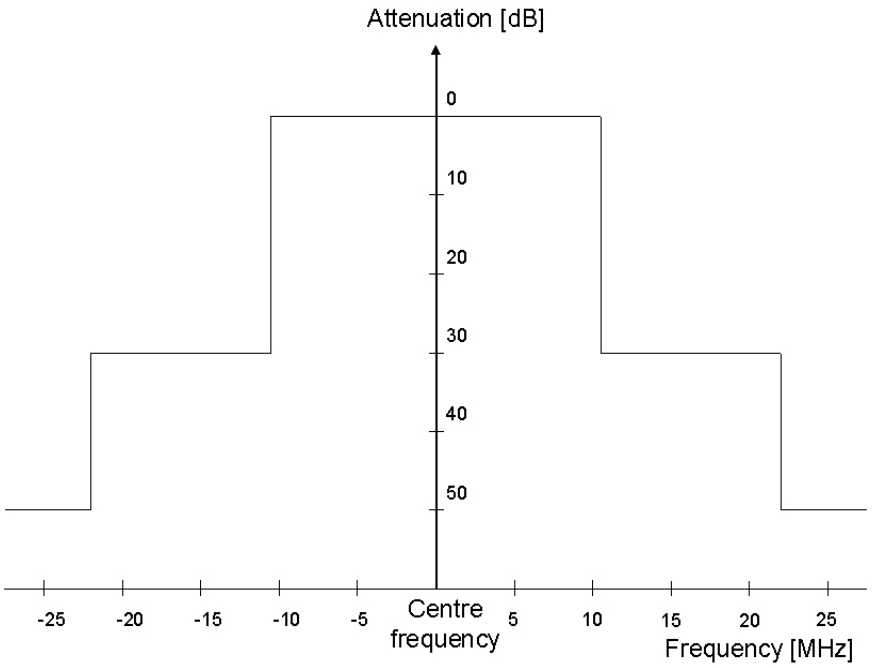


Figure 2.7. WLAN channel's spectral mask.

The gap between the adjacent channels' centre frequencies are only 5 MHz and the attenuation starts not until after 11 MHz apart from the centre frequency. This leads to the situation where the channels that are close to each other cause a massive amount of interference to each other. In fact only channels 1, 6 and 11 are far enough to each other for the 50 dB attenuation. This is presented in Figure 2.8.

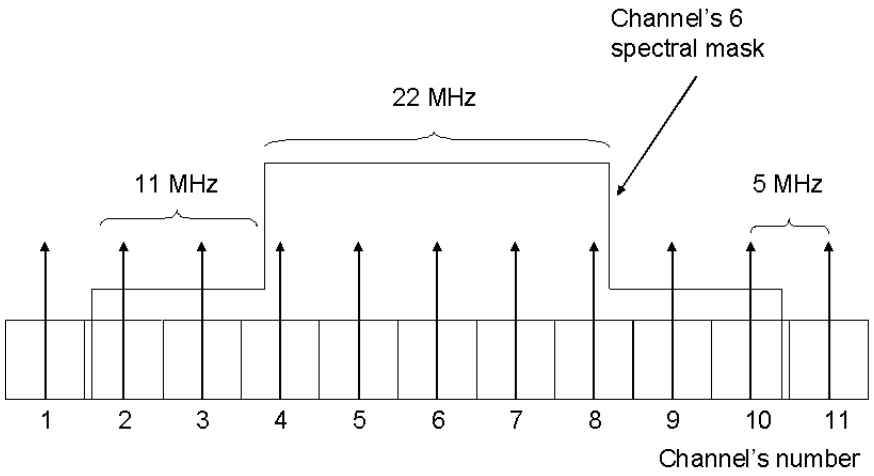


Figure 2.8: Only channels 1 and 11 (or greater) are far enough from channel 6 for the 50 dB attenuation.

So although there are lots of channels defined in the standard 802.11G, only three channels can be used without causing interference with each other.

2.2.2. Orthogonal Frequency-Dimension Multiplexing

WLAN devices use the OFDM (*Orthogonal Frequency-Dimension Multiplexing*) modulation method. OFDM is a frequency dimension multiplexing which means that different stations can transmit at the same time but they have to use different frequencies, also known as channels.

The distinct feature of OFDM is that every channel is divided into a large number of closely spaced orthogonal subcarriers, also known as sub-channels [8]. This is presented in Figure 2.9. Every sub-channel is modulated with a conventional modulation scheme. Depending on the used transmission rates, either PSK (BPSK, QPSK) or QAM (16QAM or 64QAM) modulation methods are used. PSK stands for *Phase-Shift Keying* and QAM *Quadrature Amplitude Modulation*.

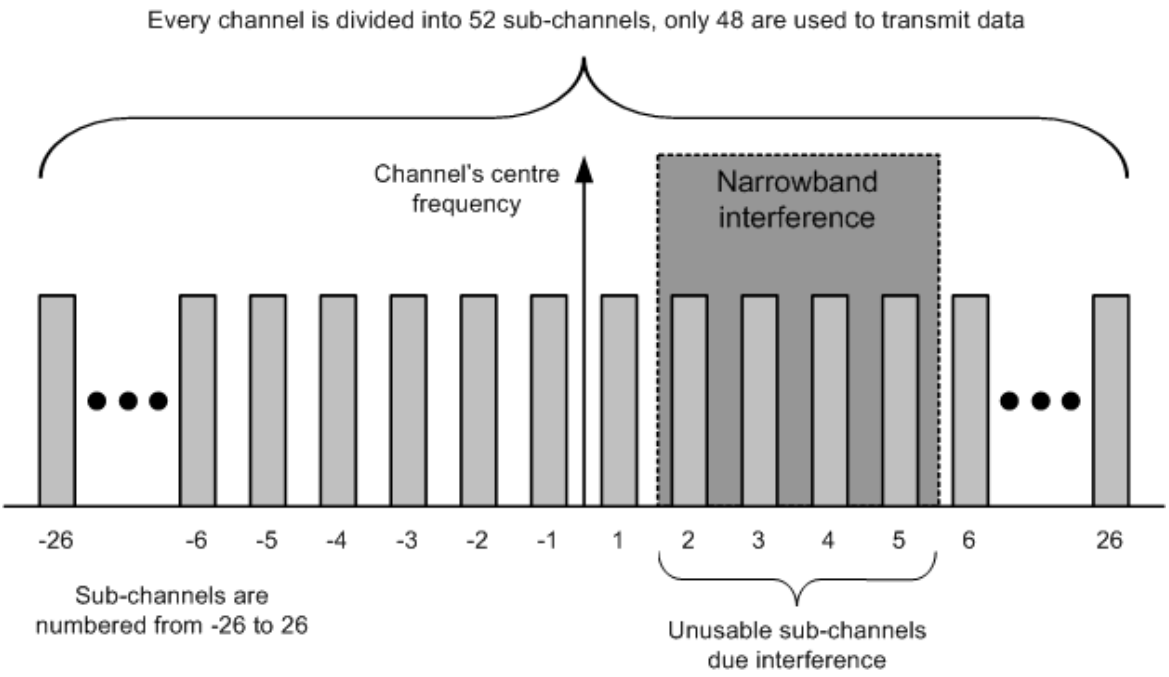


Figure 2.9: WLAN channels are divided into sub-channels which improve narrowband interference resistance and make the data transmission more robust.

It is not shown in Figure 2.9 but the sub-channels are partially on top of each other. This is illustrated more accurately in Figure 2.10. The waveform that is used to transmit information in the sub-channels is called the sinc-function. This waveform makes it possible to use the available frequency range very efficiently [9]. It should be underlined that in OFDM the sinc-waveform is used in the frequency domain. This creates a small problem because before transmission it must be solved what the signal looks like in time domain. This means that the inverse Fourier transformation must be performed on the signal. The FFT (*Fast Fourier Transform*) algorithm is an efficient way to make this transformation. The same kind of transformation must be done at the receiving end too.

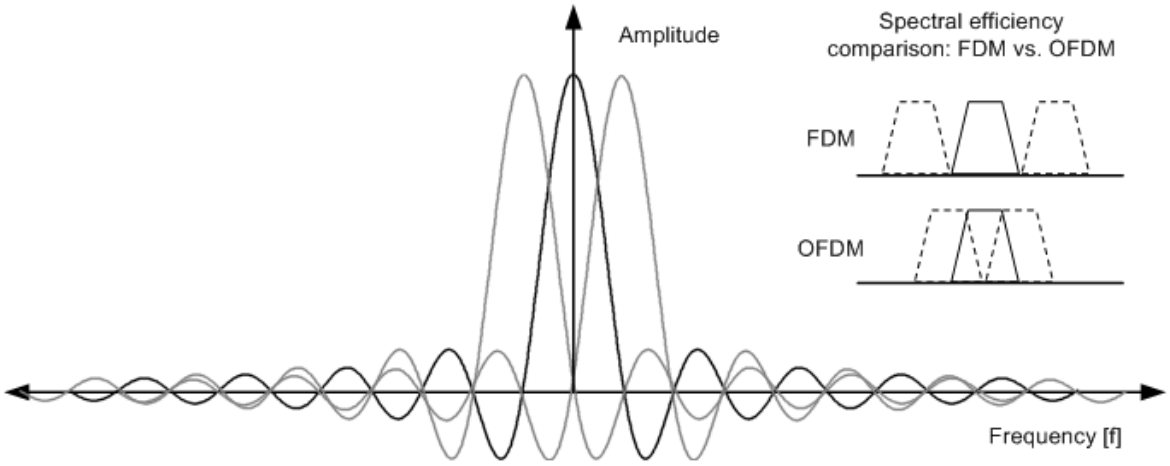


Figure 2.10: In OFDM sub-channels overlaps with each other but that does not interfere the symbol detection. Overlapping sub-channels increases spectral efficiency greatly.

Every WLAN channel has 48 sub-channels reserved for the data transmission and every sub-channel can transmit up to 6 bits at once. Therefore, every symbol can transmit altogether 288 bits. To be able to achieve a 54 Mbps data rate, WLAN devices must send 250 000 symbols per second when $^{3}/_{4}$ coding rate is used. The symbol duration is 4 µs which is quite long [10].

OFDM have many qualities that are extremely helpful in the environments where WLAN devices are usually used. For example, the slow symbol rate makes it possible to use longer guard intervals. This in turn helps to eliminate ISI (*Intersymbol Interference*). OFDM also has a good resistance against narrowband interference, illustrated in Figure 2.9, and better frequency selective fading than single carrier schemes. Multipath propagation can cause frequently selective fading and ISI.

Almost all the good qualities result from the fact that OFDM uses multiple sub-channels. It does not cripple the whole connection if there are some sub-channels that cannot be used. This makes OFDM a very robust technology which is very well suited to the harsh environment, from the signal's point of view, which WLAN devices usually face.

2.2.3. Access Method

Because of the used multiplexing method, only one station can send data at a time on any channel. Otherwise the data gets corrupted and the receivers cannot understand it. To prevent stations interrupting each other a CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) multiple access method is used.

The basic principle behind the CSMA/CA is quite simple. Every station that wants to send data first listens a little while to make sure that no other station is currently sending on the used channel. If the station detects that the channel is clear it starts to send its data. But if the stations detects that the channel is already been used, it waits until the transmission stops and after that it starts its own transmission [11]. Of course, in reality the mechanism is a little more complicated. The timeline of CSMA/CA is presented in Figure 2.11

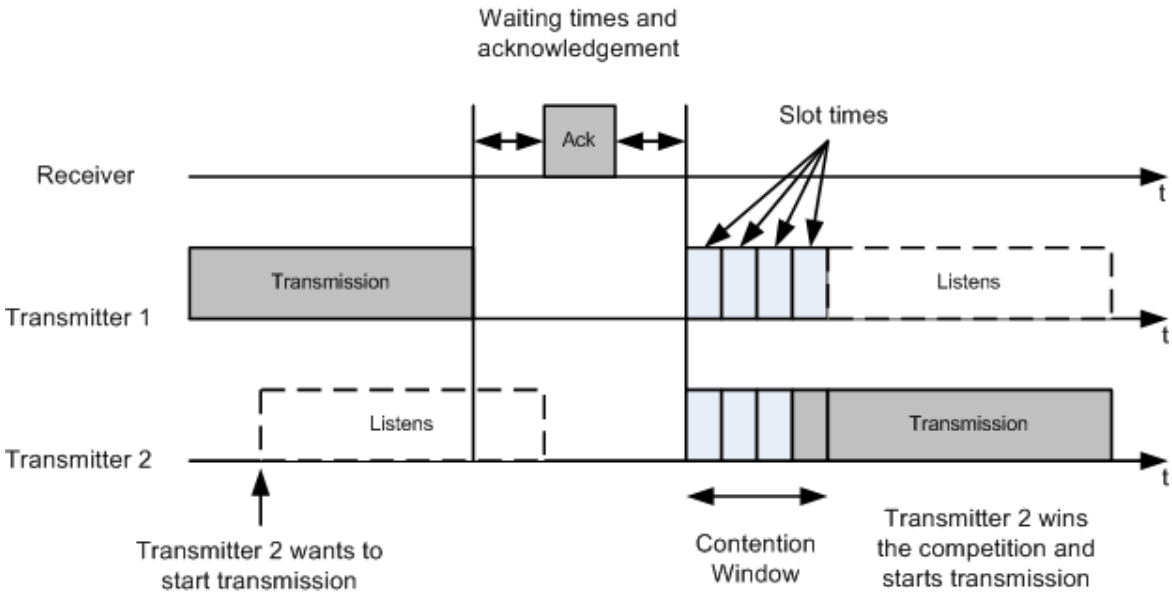


Figure 2.11: Stations start their transmissions only if the channel is free. Otherwise they wait the acknowledge signal and contention window where the next transmitter is decided randomly.

After a transmission the receiver sends an acknowledgement signal. This informs that the transmission has ended and the contention window is going to be activated briefly. The contention window is divided into seven slot times. Every station that wants to start a transmission chooses randomly one slot on which it will start a transmission. If more than one station chooses the same slot, a collision occurs. After a collision the amount of the slots in the contention windows is doubled up to 255. The station which was luckiest and

chose an earlier slot than the other stations is allowed to start its transmission. When the other stations notice that someone has started a transmission they start to listen and wait for the next contention window.

The situation gets even more complicated if the two transmitting stations in Figure 2.11 are so far away from each other that they do not notice if the other station is already transmitting. This problem is called the *Hidden Station* problem and it is solved with the RTS (*Ready to Send*) and CTS (*Clear to Send*) signals. In this case, the station which wants to start a transmission first sends the RTS signal. When the receiving station gets the RTS signal, it sends the CTS signal to every station inside its range of coverage. Now all stations know that the channel is reserved for a while. When the station that sent the RTS signal gets the CTS signal it starts its transmission. When the transmission ends the receiver sends the ACK signal.

CSMA/CA is very well suited to the WLAN hierarchy where every station is treated equally. Usually there are no centre stations which could control the traffic, like in a GSM network where the base station supervises the traffic. In GSM networks every device asks permission for transmission from the base station which then can give them unique time slots and frequencies so that there will be no collisions.

2.2.4. Quality of Service

As the previous Section 2.3.2 shows that in a WLAN network under normal circumstances the transmission rates to certain stations cannot be guaranteed. The transmission rights are granted randomly between the stations. The abstraction “normal circumstances” means the situation where there are multiple independent WLAN networks working in the same area and channel, without mutual control. The best thing what can be done is to give priorities to the certain data types so that when the station gets the transmission window it can send the high priority data first.

This kind of QoS (*Quality of Service*) was introduced to the WLAN world with the 802.11e amendment to the 802.11 standard. In this amendment eight different TCs (*Traffic Classes*) were introduced along with TXOP (*Transmission Opportunity*). Different data

packets can be divided into different TCs. Classes are divided in the same way as they are in the 802.1q/p. High priority packets are sent more frequently than low priority ones [12].

TXOP defines the maximal transmission durations for the different TCs. When a station wins the contention and it gets the right to transmit, it can send as many packets as it can in the time duration that is define in TXOP. High priority TCs naturally have longer TXOP durations than low priority TCs. In conclusion, high priority traffic is sent more often and larger quantities at once than low priority traffic.

The 802.11e standard is not implemented fully in every WLAN device on the market. The devices might have been manufactured before the amendment was finalised or the manufacturers does not implement them properly. Every WLAN device that was chosen for the tests had at least partially implemented the QoS. For example, the *Ruckus* device had only four QoS levels: *voice*, *video*, *best effort* and *background* [13].

2.3. Basics of multicast transmission

Multicast is a transmission protocol which is used when it is necessary to deliver the same information to several clients simultaneously. Multicast is a so called *one-to-many* connection. This chapter will provide a basic understanding of the multicast transmission protocol, presenting how the multicast and unicast transmissions differ from one to the other.

2.3.1. Multicast is One-to-many Connection

A multicast transmission is used in streaming applications like Internet radio or IPTV. It is a very efficient way to deliver identical information simultaneously to a large number of users. All streaming media will benefit from multicast. Figure 2.12 presents how unicast and multicast differ from each other.

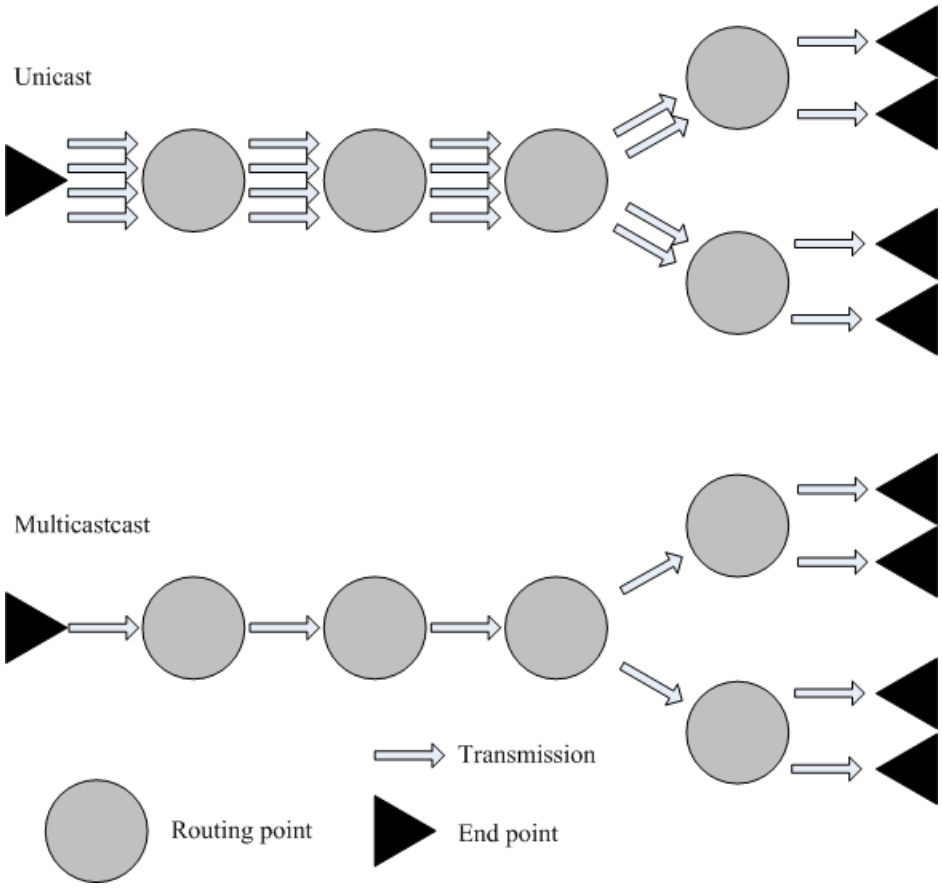


Figure 2.12: Difference between unicast and multicast type of transmission.

If four end points request the same data, it can be sent to them separately. This generates a lot of traffic in a network. Every routing point receives and transmits the same packet multiple times. In multicast, however, packets are sent only once between the routing points.

Using unicast in the case depicted in Figure 2.12, a packet is sent and received altogether 20 times, until it arrives at all the end points which requested it. If multicast is used instead, it takes only 9 transmissions until all the endpoints have got their packets. In certain situations multicast can save a lot of transmission bandwidth.

2.3.2. Internet Group Management Protocol

Every router and gateway which is capable of transmitting multicast traffic keeps track of what multicast groups the neighbouring network devices listens. They use the IGMP (*Internet Group Management Protocol*) messages to communicate with each other [14].

Based on the received information the multicast devices either deliver the received multicast packets forward or destroy them.

Devices in the IGMP hierarchy have two roles. They can be clients or routers. It is also possible that the same device is a client to one device and the router to some other. Clients are the ones which makes all the requests. The routers just keep track of the clients' requests and deliver the multicast packets to the right clients.

There are only two kinds of messages in the IGMPv3 protocol: *membership reports* and *membership queries*. When an IGMP client wants to join or leave a multicast channel it sends a membership report to the nearest multicast router. Membership queries are sent by the IGMP routers and they are used to check on what channels the clients are listening. When a client receives a membership query it will send a membership report back to the router. The IGMP hierarchy and used messages are shown in Figure 2.13.

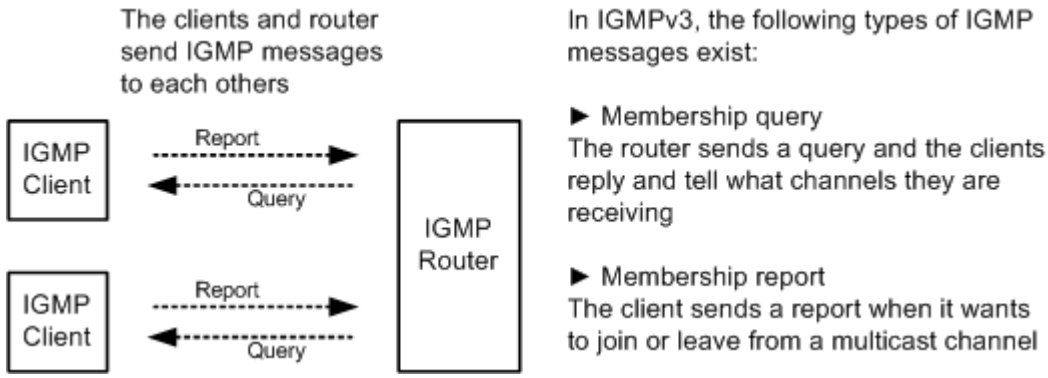


Figure 2.13: The IGMP has basically two types of messages: queries and reports.

In theory everything is surprisingly simple. The router has a table where it marks all the clients that are receiving one or more multicast channels. The router updates the table every time it receives the multicast report from a client. The router also sends membership queries to all the clients to check that there are no dead clients in its multicast table. Some times the clients go offline before they can send the leave message. The query is sent every couple of minutes. The exact interval depends on the router's settings.

In its table, which is called also the *multicast table* in this thesis, the router has all the information that it needs and the router can send the multicast packets to the right clients.

2.3.3. Structure of Multicast Network

In the real world the structure of a multicast network is more complex than what was presented in Figure 2.13. There are many different network devices between the IGMP router and the IGMP client. This makes the IGMP messaging more complex. A typical layout is presented in Figure 2.14.

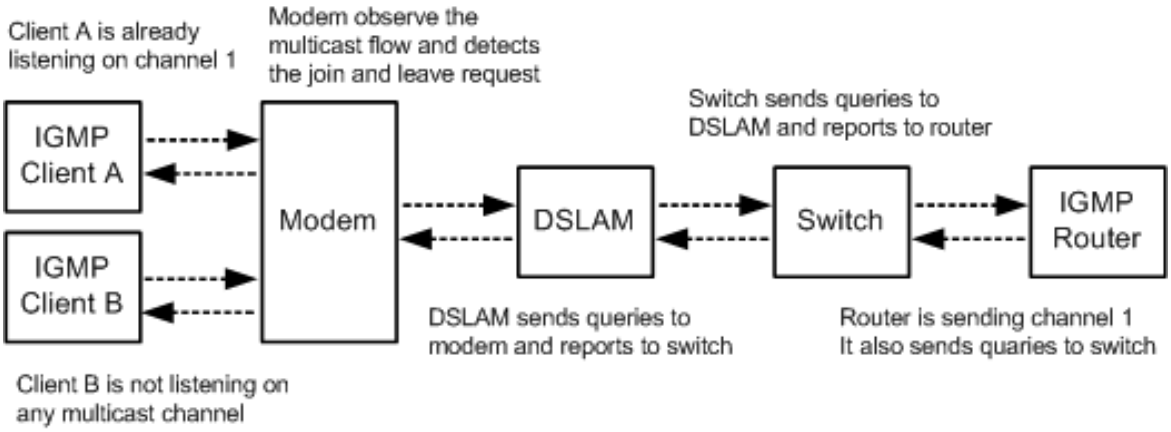


Figure 2.14: The IGMP client and router do not send IGMP messages directly to each other. Network elements communicate only with theirs closest neighbours.

It is not practicable to send IGMP messages directly between the client and router. This would generate unnecessary traffic in the network. Keeping in mind that there can be thousands of clients who are receiving some multicast channels from the same router. Also, the delay would rise unnecessarily if the join and leave messages would have to travel all the way from the clients to the router.

This problem has been solved so that every multicast device has its own multicast table. Basically the network devices send IGMP messages only with their neighbouring devices. An exception to this is the modem which might not have this kind of feature.

For example, if *Client B* in Figure 2.14 would want to join channel one, it would send the join request to the modem. Because the modem is already receiving the requested channel it does not have to relay the join request any further. The modem could just start to send the channel one also to the *Client B*. The generated network traffic would be minimal. Furthermore the other network devices do not really care if *Client B* is receiving the channel

one or not. They are already sending the channel one to the modem because the *Client A* is receiving that channel.

2.3.4. IGMP Snooping

IGMP control messages are sent as multicast packets. In other words, the messages and the actual data stream are warped in similar packets. There is no way to detect one from the other just by looking at the packets. This causes problems to the modem in Figure 2.15 which should be able to notice the join and leave requests.

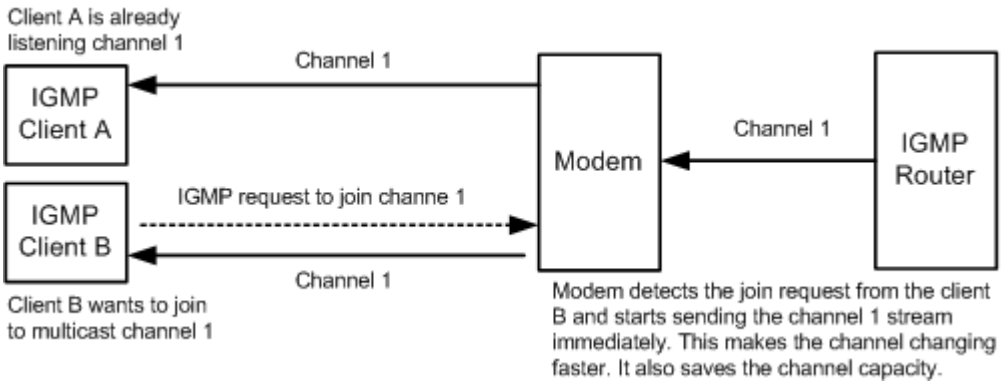


Figure 2.15: The join request travels upstream until it reaches a device which already receives the requested channel. The request is then terminated and the channel is redirected towards the client.

One way to overcome this problem is to open all received multicast packets and look inside what they contain. This method is called as IGMP snooping and it is used in some of the modem and WLAN devices [15].

The only problem with IGMP snooping is that the modems are OSI (*Open Systems Interconnection Reference Model*) layer 2 (*Data Link Layer*) devices and IGMP snooping requires them to examine some layer 3 (*Network Layer*) information from multicast packets.

When IPTV or other high bandwidth demanding type of multicast streams is used, the modem will receive quite a few multicast packets. To inspect every one of them the modem would need either a special hardware solution or fast CPU (*Central processing unit*). IGMP Snooping implemented on a low-end switch with a slow CPU could have a severe performance impact when data is sent at high rates.

IGMP snooping is a useful method to reduce unnecessary traffic. The IGMP messages travel upstream only as far as it is necessary and the actual data streams are duplicated only when the network actually branches. IGMP snooping combined with a slow CPU, however, might also be the reason for some devices' poor multicast performance. The test and results are presented in Chapters 4 and 5.

3. Presentation of the Devices

This chapter will present the devices which were chosen for the tests. A short comment of why the specific devices were chosen is given. The distinctions between the different devices, if there are any, are described briefly as well.

The main focus is on WLAN devices, but also two solutions that rely on wires were chosen for the tests. At the end of this chapter is a brief operation description of the wire / cable devices.

3.1. Devices under Testing

The range of devices that were chosen for testing was kept as diverse as possible. Four different manufacturer's WLAN devices were chosen. Two of them were traditional models and the other two were MIMO models. Additionally two devices that use wires to transfer information were chosen: one of that uses common power cables and the other uses common antenna cables. All the devices that were tested are presented in Table 3.1.

Table 3.1: A list of the tested devices.

Device	Category	Short Description
A-Link WL54AP2	WLAN	Common WLAN access point / adapter.
ZyXEL G-570S	WLAN	Common WLAN access point / adapter.
Planet WMRT-414	WLAN	WLAN router that uses MIMO antenna technology.
Ruckus MF2900 / MF2501	WLAN	WLAN access point and adapter pair. Uses MIMO antenna technology.
Coaxsys TVnet/C	Wired	Uses antenna cables to transfer data.
Planet PL-201	Wired	Uses power lines to transfer data.

Although *Coaxsys TVnet/C* and *Planet PL-201* use cables to transmit information, they were chosen for the test. Because they use cables that can be found in every household, these devices are considered "wireless". Users do not have to lay any separately cables to use these devices. On top of that, a wired connection is almost always more reliable than wireless one. Some of the new services, like IPTV, require a fast and reliable connection. These were the main reasons for the decision to add these wired devices to the test.

All the WLAN products that were chosen for the tests were 802.11G compatible. *A-Link WL54AP2* and *ZyXEL G-570S* are traditional WLAN products. Both of them have only one antenna. *A-Link* is a product that is already at the end of its life. In other words the manufacturer does not produce these devices any more. *ZyXEL,* at the other hand, was a brand new product when the tests were done. These devices were added to the tests so that it was possible to compare products of different generations.

Planet WMRT-414 and *Ruckus* are WLAN devices which both have multiple antennas and their manufacturers tell that these products use the MIMO technology. Manufacturers promise up to three times as large coverage area and much faster transmission speeds for MIMO devices than with traditional WLAN devices. It is quite interesting to find out how well MIMO products fulfil these promises. These devices were selected so that it could be

tested what kind of performance effect MIMO has when compared to traditional SISO products.

3.2. Coaxial Cable and Power Wire Devices

The principle of the *Coaxsys TVnet/C* and *Planet PL-201* products are quite similar. Both of them use cables that every household has. The best part is that these cables are usually installed inside the house's walls and they cover every part of the house. The disadvantage is that these cables are normally used to transmit other signals. This forces the *Coaxsys* and *Planet* devices to use higher frequencies that what the cables are designed for. This may cause some problems with attenuation.

Because these devices use networks that do not have any or have only a little control mechanism, the signal will spread everywhere. This may have harmful effects to other similar devices which are located in the same network. Of course, this is also a security risk.

3.2.1. Planet - Power Lines

In power lines the normal traffic is electricity and it travels at a frequency of 50 or 60 Hz. *Planet* power line adapters use a frequency band of 4,3-20,9 MHz [16]. There is a big gap between these two "signals". The main reason for this is that the electricity is transmitted with enormous power compared to ordinary information signals. And because there are no filters in power line networks, there is a lot of interference.

Power lines are not designed to transmit information signals which can cause problems. For example, the fuses might cause problems to the connection if the devices are not located under the same fuse. The good side is that there is lot of power sockets scattered throughout the whole house. This gives more freedom for device placement.

3.2.2. Coaxsys - Antenna Cables

In antenna cables the normal traffic is the TV signal and it travels at a frequency of 44-890 MHz. *Coaxsys* operates at frequencies above 1 GHz [17]. The good side is that the coaxial cables are designed to transmit information signals so the only problem is that with the higher frequency the attenuation is also higher. The disadvantage is that a normal household might have only one or two antenna sockets.

The other disadvantage is that the household's antenna cable network can include filters or circulators that hinders or even blocks the *Coaxsys'* signal. This was the case in the test environment. *Coaxsys* devices could not form connections between each others even when they were plugged into adjacent antenna sockets.

4. Testing

This chapter includes information about testing, including the knowledge about what sort of tests were done, under what kind of environment. This chapter also contains information about the equipment and programs that were used in the tests. Basically, this chapter seeks to clarify the reasons why different tests were done and gives some information about the surroundings where the tests were performed. More detailed information can be found in Chapter 5 along with the results of the tests.

Discovering how well the DUTs (*Devices Under Test*) could handle the multicast and IPTV transmission was considered to be the most important knowledge to be obtained from these tests. This is the reason why the tests emphasize this area.

4.1. Testing in General

Information travels in many different forms and packets within the Internet. For example, a file transmission normally uses TCP, or a VoIP conversation uses UDP or even a IPTV stream which uses a multicast type of data transmission. This means that LAN devices must also be able to handle all these different kinds of transmission protocols.

It is quite important that some protocols have higher priorities than the others when it is decided how much bandwidth is allocated for each. VoIP calls and live video streams need a steady transmission speed and low latency to guarantee high quality reception. On the

other hand, a common file transmission does not need a steady transmission speed or low latency. It only takes slightly longer when the speed is slower. So LAN devices should have some mechanisms to allocate more bandwidth and priorities to those protocols that need it.

With WLAN devices, the range of the coverage is also very important, as well as the ability to endure interference from different sources, like other WLAN devices or microwave ovens.

In summary, there are lots of pitfalls a LAN product can fall into. One reason for these tests was to find out how well different manufacturers have been able to avoid these pitfalls.

The tests were focused on WLAN devices. Other devices, those that uses antenna cables and power lines, were tested briefly. Because they use cables to transmit data, their test environments differ greatly from that which wireless products face. Therefor, their test results may not be compared too closely. But some estimation can be made about how well different devices can be used in different kinds of situations. Next are presented what kinds of tests were performed and what parameters were measured.

4.2. Testing Equipment and Programs

Most of the tests were done by using two computers which were connected to each other with different DUTs, see Figure 4.1. With this kind of test setup both ends of the link could be monitored. The other reason for the kind of test setup chosen was to keep the testing environment as simple as possible.

With wireless DUTs the connection between two computers was protected with WEP (*Wired Equivalent Privacy*) encryption. WEP was used to guarantee that only test traffic could use the connection between the test computers. Neither computer was connected to the Internet or other networks when the tests were performed. Only test programs were

running on the computers while tests were performed. All measures were taken that were considered necessary to guarantee that the results were as accurate as possible.

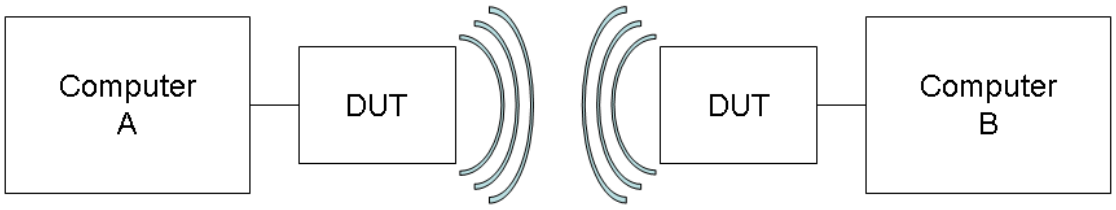


Figure 4.1: Devices were tested using this kind of test setup. The test setup was simple and both ends could be easily monitored.

Two programs were used to measure different parameters: *Iperf* and *VLC Media Player*. *Iperf* is a program which measures qualities and speeds of different transmission protocols. With the *Iperf* program, it is possible to generate different kind of traffic, like TCP or UDP. After the generated traffic is sent, the program gives a summary of how well the transmission was performed. This program was used to find out the DUT's transmission capabilities. In Appendix can be found the a detailed description how this program was used in testing.

The *VLC Media Player* is a program that plays different kinds of multimedia files. With this program it is also possible to stream and receive streamed multimedia files. With the *VLC Media Player* different kinds of multimedia files were streamed between the test computers. In Appendix can be found more detailed description of how this program was used in testing.

4.3. Testing Environment

All the tests were performed in a two-storey office building which was located at the street level of an apartment building. This means that the walls and ceilings are made of thick concrete and there are lots of people moving around affecting the signal. Both of these features hinder wireless connections. On top of that there were a lot of other WLAN devices

in the vicinity. Luckily most of them used channel 6 so that tests could be done over channels 1 or 11 without too much interference. Nevertheless, the testing environment for the WLAN products was quite harsh.

One must remember that there are several factors which have an effect on wireless transmission. The test environments were kept as close to identical as possible for all DUTs. Even still, every test was slightly different from the other tests. It was not possible to exactly replicate the test environment for every test. The channel which had the lowest interference was used in the tests. This sometimes led to a situation where different a channel had to be used when different DUTs were tested. This may affect the results slightly. In order to achieve more accurate results almost all the tests were repeated two or three times.

Figure 4.2 and Figure 4.3 present the rough layout of the office. Measurements are not exact but they should give some understanding about the environment where the tests were performed. All the test setups are marked in that figure with symbols but these are explained later in Chapter 5.

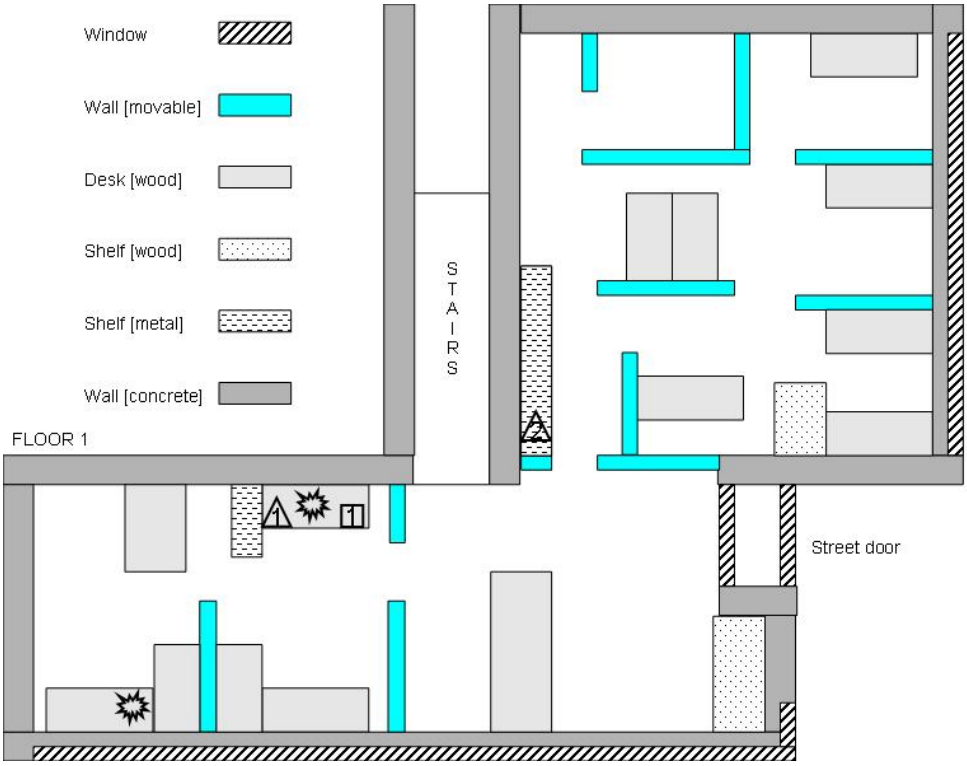


Figure 4.2: Downstairs of the office building used for tests

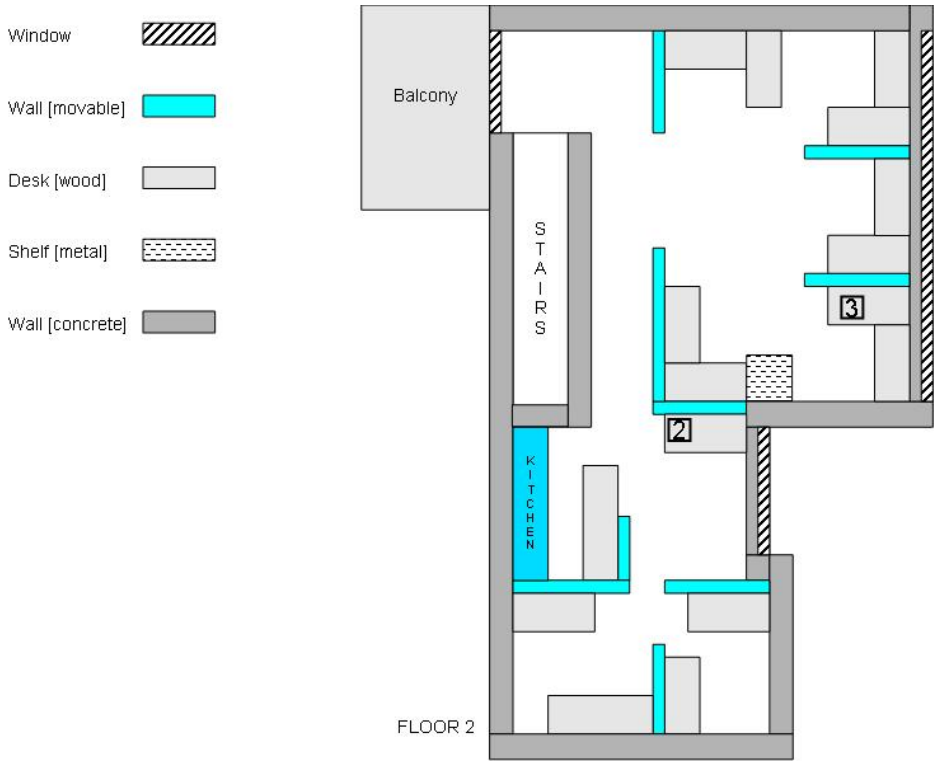


Figure 4.3: Upstairs of the office building used for tests

4.4. Testing Aspects

In this chapter is a short description of the tests that were performed. They can be divided into two groups: *protocol* and *streaming* tests. The protocol tests are presented first. After that the streaming tests are presented. The following tests were mainly done only with WLAN devices. In Section 4.5 is told how those devices which use wires were tested.

4.4.1. Protocol Tests

The aim of the protocol tests was to find out how well different DUTs handle the most common transmission protocols: TCP and UDP. The speed of data transmission was the main parameter what was monitored in these tests. But it was also interesting to find out whether devices have some kind of performance gap between these two protocols. One other interesting aspect was to find out how distance affects these protocols. Does one pro-

tocol diminish faster than the other or do they behave similarly? These tests were mainly done with the *Iperf* program. A multicast protocol test was also included in protocol tests.

4.4.1.1. TCP

The TCP protocol is the most common protocol used in the Internet. For example, it is used when WWW-pages are loaded or emails are read, it is also used when files are transferred from place to place. The TCP protocol ensures that the transmitted packets are received in the right order and without errors. Packets with errors or those which are lost during a transmission are resent.

As the TCP protocol ensures that the transmission is free from errors, the only measurable parameter is speed. This was measured in two different ways: with the *Iperf* program and by transmitting a large file from one computer to the other and measuring how long the transfer takes.

4.4.1.2. UDP

The UDP protocol is normally used when the transmitted signal does not tolerate delays or latency well. Typical situations are live video or audio streams, such as Internet radio or a VoIP call. There is no error detection in this protocol whatsoever. Lost or incorrect packets are not resent. If connection is good and a packet stream is steady then the quality is good, but it degenerates quite quickly if the connection is poor and packets are lost.

With UDP the most interesting parameter is the packet loss percentage. It was tested how fast the DUTs could transmit UDP streams with a decent packet loss percentage. The test was done with the Iperf program. The transmission speed was altered and the packet loss percentage was monitored.

4.4.1.3. Multicast

Because of multicast's nature explained in Section 4.6, it is impossible to resend lost or damaged packets. Multicast can only be used with the UDP protocol. Again, the packet loss percentage is the most interesting parameter to be monitored. The DUTs ability to handle multicast traffic was tested in the same way as UDP performance was tested. In

other words, multicast traffic streams were generated at different speeds and the packet loss percentage was measured. The multicast performance test was done with *Iperf* program.

4.4.2. Streaming Tests

Streaming media means a media that is consumed while it is being delivered. A common television is a good example of a streaming media. When a television is turned on it starts to display a program that a broadcasting company is currently sending. The television does not record programs anywhere before its displays them.

The streaming tests, measure how well the DUT handles unicast and multicast streams. Next is explained briefly how the different streaming tests were performed.

4.4.2.1. Streaming Media Files between Computers

In these tests one computer sends an audio or video file in a streaming format and the other computer receives and plays it. The playback quality was evaluated by visual and audio inspection.

Most of the streaming tests were done using both uni- and multicast type file transmission. The unicast type of transmission was tested because during the multicast tests it appeared that some DUTs had poor multicast performance. The unicast tests were, therefore, made for reasons of comparison. The performance difference between uni- and multicast was the variable to be measured.

The DUTs ability to give priorities to a multicast type of traffic was tested as well. While the multicast streaming was in progress a file transmission from one computer to the other was started. The time that was taken in transmission was measured and the quality of video and audio was monitored. This test was only done with multicast streaming.

4.4.2.2. IPTV and Interference

The DUTs' capabilities to transmit the IPTV signal were also tested. The IPTV signal is multicast so some of the previous test can give good estimations about this test's results. The IPTV signal was provided by IPTV distributor Maxinetti.

One device was connected to an ADSL modem and the other was connected to an IP set-top-box, which in turn was connected to a TV set. The qualities of different channels were monitored.

To test how well the DUT endures interference during the IPTV transmission, an interference signal was created. This was done by creating a wireless connection between two computers and sending different kinds of files between them over different channels. The effects of interference on the IPTV quality were monitored. Two *A-Link WL54AP2* devices were used to produce the interference signals.

4.5. Wire/Cable Dependent Devices

There is no multipath propagation in wires, however there can still be reflections and echo signals. Also, interference from other devices is fainter than in wireless communication. In other words, the transmission environment is more stable. This usually makes wired connections more reliable. The attenuation is the main problem what the wired devices face. Due to these reasons the wired devices were tested more briefly than WLAN devices.

All that needs to be tested with wire/cable dependent devices is how much they tolerate attenuation before their performance starts to deteriorate. For *Coaxsys TVnet/C* a separate test environment was build which is presented in Figure 5.1. With *Planet PL-201* this was not done because there was no method to measure the exact amount of attenuation that the signal was facing in power cables. Therefore *Planet PL-201* was tested, like the WLAN products were, in different locations.

Basically, all the same tests that were done with WLAN devices were performed with the wired devices. Although some of those tests, like the IPTV test, were carried out more briefly with the wire / cable dependent devices.

5. Results

In this chapter is presented a description of how the tests were done and what the results were. The chapter is divided into four sections: *protocol*, *streaming*, *IPTV* and *Coaxsys* tests. The different sections hold the results from the different tests. Every section has a short description about the testing environment and how the tests were made. After that the results are presented. Every section includes also some brief speculations about the results, evaluating how well the tests went and why some devices showed better performance than others.

5.1. Protocol Tests

The test results and setups of the protocol tests are presented next. The protocol tests included TCP, UDP and multicast tests. The chapter starts with the presentation of the test setups in order to give a good overview of how the tests were done. The results are presented after that with the evaluations.

5.1.1. Protocol Tests Setups

All protocol tests were repeated in three different locations. One had a very easy transmission path so that the upper limit of the DUT performance could be measured. Others had more difficult transmission paths so that the DUT range of coverage could be measured.

The idea was to study how fast the DUT performance diminishes when the transmission path gets longer and more demanding.

Next are presented the protocol test setups. The placements of the DUTs are described with the information about what is special in each test setup. Some DUTs were tested several times in some test setups with different configurations. Wire/cable dependent devices had different testing methods which are presented here as well.

5.1.1.1. Test Setup 1: Upper Limit

The transmission path was kept as simple as possible. The WLAN products were placed near each other and there was an undisturbed LOS between the transmitter and receiver. In Figure 4.2 the place of the transmitter is marked with the symbol "1" and the place of the receiver is marked with the symbol "1".

The *Coaxsys TVnet/C* was tested using an external coaxial cable about three meters long. To connect the *Planet PL-201s*, an extension cord of also about three meters long was used.

The *Ruckus* devices were tested twice, once using normal settings and once using "super" settings. In normal settings *Ruckus* devices use only one channel and the limit of the transmission speed is the common 54 Mbps. In the "super" mode the devices use multiple channels and the theoretical maximum speed of the transmission is raised to 108 Mbps. *Ruckus* was tested with both settings in all the other test setups too.

5.1.1.2. Test Setup 2: Medium Transmission

In this test the transmitter was located downstairs and the receiver upstairs. In Figure 4.2 and Figure 4.3 these are marked with the symbols "1" and "2". There was no dominating LOS path anymore. The signal had to penetrate the thick concrete ceiling or reflect its way along the stairs. Either way is quite demanding and the signal will attenuate greatly before it reaches the receiver. The signal path is about ten meters if it chooses to take the stairs. If it goes trough the ceiling the path is much shorter.

The *A-Link WL54AP2* was tested two times: once with normal antennas and once with highly directional antennas. This is a good way to study how much directional antennas increase the *A-Link* performance with demanding transmission paths. The antennas which were used had 14 dBi gains. In theory this means that the received signal's power can be 28 dB (about 600 times) greater than when normal antennas are used. This test was repeated in the last test setup as well.

Planet PL-201 devices were also tested using the same placement of the computers what were used when the WLAN devices were tested. The *PL-201* devices were plugged into power sockets which were located near to the computers. In the office there were two kinds of power sockets, ones which were labeled as ATK-socket and others which were unlabelled. All those power sockets that were labeled as ATK-sockets were under the same fuse. The *PL-201* devices were tested two times: once when both ends were connected to ATK-sockets and once when the other end was connected to ATK-socket and the other end to the normal power socket.

Coaxsys TVnet/C products were not tested in this or the next test setups. It was tested separately and its performance results can be found at Section 5.4.

5.1.1.3. Test Setup 3: Difficult Transmission

In this test the transmission path was even more difficult than it was in the previous test setup. The signal has to travel longer distance, penetrate thicker ceiling and endure more reflections. The idea of this test was to measure DUT's range of coverage and their performance in really tough situations. Only the WLAN devices were tested in this test setup. The transmitter is again marked with the symbol "1" in Figure 4.2 and the receiver is marked with the symbol "3" in Figure 4.3.

With the *A-Link WL54AP2*, it was tested to see how much a repeater would enhance the performance. The repeater's place is marked with the symbol "2" in Figure 4.3. In this test the signal was first transmitted from the transmitter to the repeater. Then the repeater transmitted the signal to the receiver. The repeater decoded the signal when it received it and encoded the signal again before it was transmitted to the receiver. The same WLAN channel was used on both links: transmitter to repeater and repeater to receiver.

The transmitter's and receiver's MAC (*Media Access Control*) addresses were removed from each others *allowed access* lists to make sure that all the traffic travels through the repeater. Therefore the transmitter could not communicate with the receiver directly but the repeater could communicate with both of them. A third *A-Link WL54AP2* device was used as a repeater.

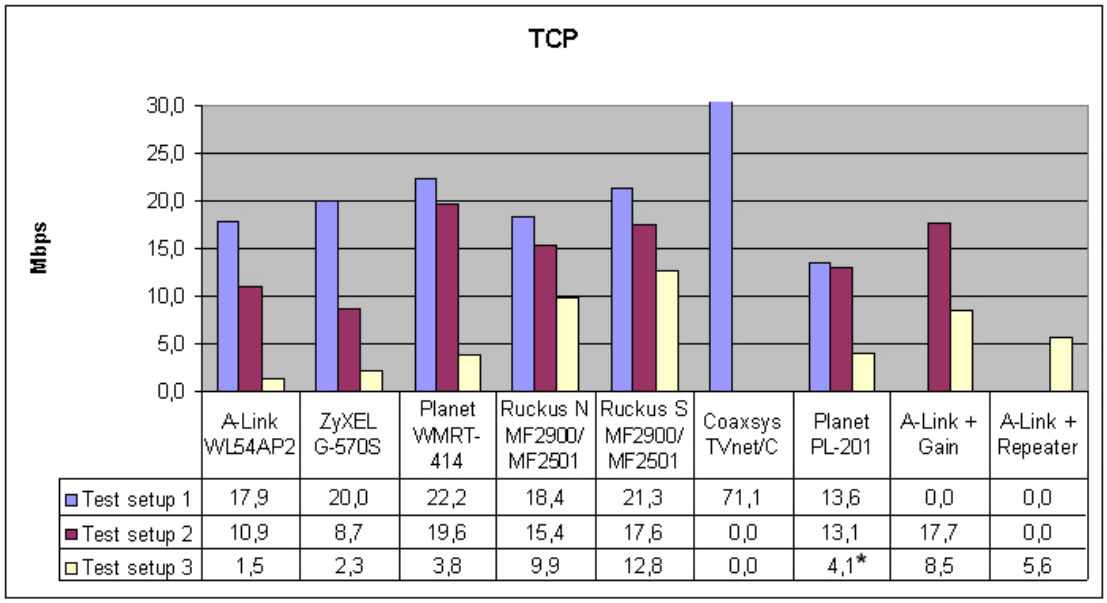
5.1.2. Protocol Tests Results

Here are presented the results of the protocol tests. The results are divided into three categories: *TCP*, *UDP* and *multicast*. For every category the results are presented from each test setup.

5.1.2.1. TCP Results

The TCP test's main interest was to find out how fast transmission speeds could be maintained by the DUT. The *Iperf* program was used to measure this. The results are presented in Table 5.1. It was also measured how long it took to transfer a large file, the size of 100 MB, from one computer to other. These times are presented in Table 5.2.

*Table 5.1: Results from the TCP protocol tests. * Denotes that the Planet PL-201 devices were tested in the test setup 2 but that the other device was connected to an ATK-power socket and the other was connected to a normal power socket.*



	A-Link WL54AP2	ZyXEL G-570S	Planet WMRT-414	Ruckus N MF2900/ MF2501	Ruckus S MF2900/ MF2501	Coaxsys TVnet/C	Planet PL-201	A-Link + Gain	A-Link + Repeater
Test setup 1	17,9	20,0	22,2	18,4	21,3	71,1	13,6	0,0	0,0
Test setup 2	10,9	8,7	19,6	15,4	17,6	0,0	13,1	17,7	0,0
Test setup 3	1,5	2,3	3,8	9,9	12,8	0,0	4,1*	8,5	5,6

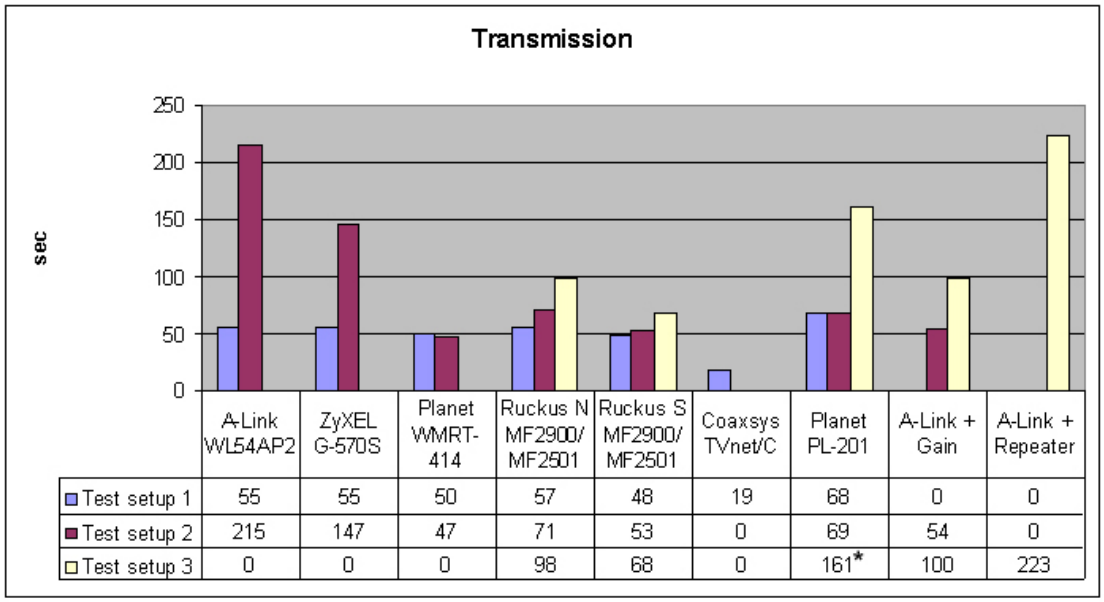
As it can be seen from Table 5.1, every device managed very well in the first test setup. There were no big differences in performance between all of the WLAN devices. The *Coaxsys TVnet/C* had superior TCP transmission capacity. This was not a big surprise because coaxial cables are designed to transmit information signals. The worse TCP performance was the *Planet PL-201*, its datasheet reveal a reason for that. It is told that the maximum TCP traffic speed is only 14 Mbps. So the real reason for its poor performance is that it probably uses a robust modulation method.

In the second test setup the differences between WLAN devices start to show. The newer MIMO devices handle this test somewhat better than the traditional devices. The reason for this is that both *Ruckus MF2900/MF2501* and *Planet WMRT-414* have some means to counter the signal attenuation. *Ruckus* has directive antennas and a smart algorithm that controls which antennas are active. *Planet* has two receiving antennas, so it can combine two the received signals to create a single stronger signal.

Only the *Ruckus* could handle the hardest transmission path. Connections with the other devices were very unreliable. This is shown better in Table 5.2 where are presented the

times that it took to transmit the 100 MB file from one computer to the other. With the other devices the transmission was interrupted, at all three times that this was tried, before the whole file was transmitted.

*Table 5.2: Results from the file transmission tests. * Denotes that the Planet PL-201 devices were tested in the test setup 2 but that the other device was connected to an ATK-power socket and the other was connected to a normal power socket.*



	A-Link WL54AP2	ZyXEL G-570S	Planet WMRT-414	Ruckus N MF2900/ MF2501	Ruckus S MF2900/ MF2501	Coaxsys TVnet/C	Planet PL-201	A-Link + Gain	A-Link + Repeater
Test setup 1	55	55	50	57	48	19	68	0	0
Test setup 2	215	147	47	71	53	0	69	54	0
Test setup 3	0	0	0	98	68	0	161*	100	223

The extra tests that were made with the *A-Link WL54AP2* devices show that directivity plays a big role in reliable connections. When highly directional antennas were attached to the *A-Link* its performance was increased greatly. What the results do not show is that the antennas had to be directed quite carefully before the good results could be obtained.

As it can be seen from Table 5.1 and Table 5.2, a repeater has some positive results to the performance. The increase in performance is not that significant but it is enough for slow file transmission like surfing in the Internet. Because all the three devices used the same channel they generate interference with each other. This is probably the major reason for the quite poor performance.

The *Ruckus* in "super" mode gave only a slightly better results compared with the normal mode. The manufacturer's promises that the "super" mode would double the transmission

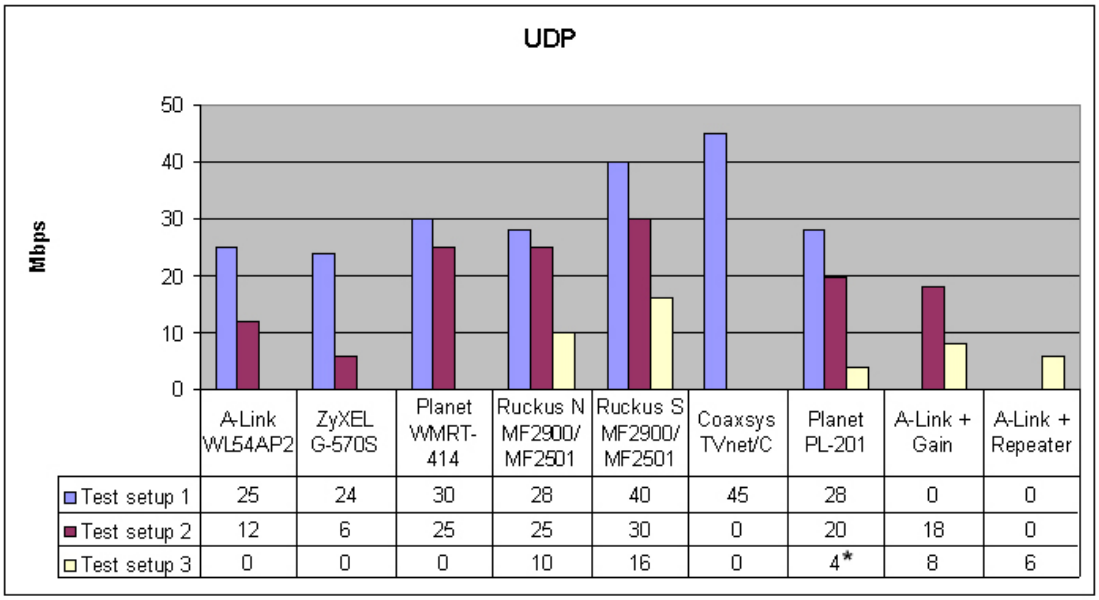
speed are greatly exaggerated. But the increase in the performance was still noticeable and the difference between normal and "super" performance did not shrink even in the most demanding test setup.

Planet PL-201 performance depended a greatly on what power sockets were used. When both ends were attached to ATK-power sockets the TCP transmission speed in test setup 2 was about 13 Mbps. But when the transmitting device was connected to a normal power socket the TCP transmission speed diminished to 4 Mbps. It appears that when the signal has to travel through a fuse it will attenuate or distort greatly. Comparing the results from the first and second test setups show that the devices maintain transmission speed at a high rate, if both ends are under the same fuse.

5.1.2.2. UDP Results

The UDP protocol does not detect errors or resend lost packets, therefore, the most interesting aspect to monitor is the packet loss percentage. In Table 5.3 are presented the transmission speeds that different DUTs could sent with a decent packet loss percentage. The boundary for what was a decent packet loss percentage and what was not, was chosen to be one percentage. The UDP tests were done with the *Iperf* program.

*Table 5.3: Results from the UDP protocol tests. * Denotes that the Planet PL-201 devices were tested in the test setup 2 but that the other device was connected to an ATK-power socket and the other was connected to a normal power socket.*



	A-Link WL54AP2	ZyXEL G-570S	Planet WMRT-414	Ruckus N MF2900/ MF2501	Ruckus S MF2900/ MF2501	Coaxsys TVnet/C	Planet PL-201	A-Link + Gain	A-Link + Repeater
Test setup 1	25	24	30	28	40	45	28	0	0
Test setup 2	12	6	25	25	30	0	20	18	0
Test setup 3	0	0	0	10	16	0	4*	8	6

The results follow along the same lines with the TCP tests results. It is interesting to find out that WLAN products could transmit the UDP traffic significantly faster than the TCP traffic especially when the transmission path was trivial. In contrast to the to TCP test where no clear winner could be found on the easy transmission path, in the UDP test the *Ruckus* with the "super" settings had by far the best performance compared to the other WLAN devices.

The biggest difference was the *Coaxsys TVnet/C* poor performance compared with its TCP results. When it was tried to generate faster than 45 Mbps UDP streams with TVnet/C devices, the recorded transmission speed dropped always to 28 Mbps. Maybe there is some sort of UDP traffic controller in *TVnet/C* that limits the speed to 45 Mbps.

In summary those devices that performed well in the TCP tests performed well in the UDP tests as well. *Ruckus* was again the only device that could maintain it performance in the most demanding test. When the *A-Link* got some help, directive antennas or repeater, it also could transmit UDP traffic in the last test setup.

This test and the previous TCP test have shown that directivity alone is not enough to guarantee a good connection. In *Ruckus* devices, the antennas have much weaker directivity than those used with *A-Link*. Still the *Ruckus* outperformed the *A-Link* quite clearly. The *A-Link* antennas were directed manually before the test. The antennas were aimed in those directions where the signal was thought to travel the easiest.

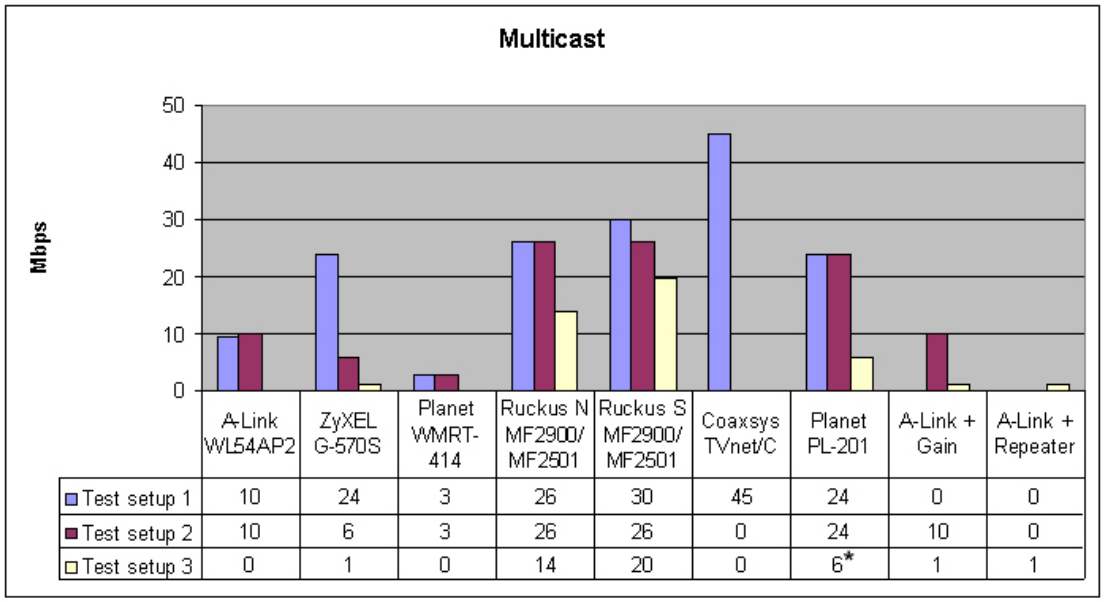
The *Ruckus* in turn constantly measures the incoming signal and detects the direction from where the received signal is the strongest. The *Ruckus* can change the direction where it focuses its transmission power very rapidly. This gave to the *Ruckus* a clear edge compared to the *A-Link* and that is the reason why the *Ruckus* triumphed in the most demanding test. This test clearly shows that the control is as important as the directivity in environments where WLAN devices operate.

5.1.2.3. Multicast Results

Multicast traffic was measured in the same way as the UDP traffic. Multicast streams were generated at different speeds and the packet loss percentages were measured. The results

can be found in Table 5.4. The decent packet loss boundary was chosen to be one percentage as it was in the UDP tests. The multicast tests were done with the *Iperf* program.

*Table 5.4: Results from the multicast tests. * Denotes that the Planet PL-201 devices were tested in the test setup 2 but that the other device was connected to an ATK-power socket and the other was connected to a normal power socket.*



	A-Link WL54AP2	ZyXEL G-570S	Planet WMRT-414	Ruckus N MF2900/ MF2501	Ruckus S MF2900/ MF2501	Coaxsys TVnet/C	Planet PL-201	A-Link + Gain	A-Link + Repeater
Test setup 1	10	24	3	26	30	45	24	0	0
Test setup 2	10	6	3	26	26	0	24	10	0
Test setup 3	0	1	0	14	20	0	6*	1	1

As it can be seen from Table 5.4, multicast transmission really cripples some WLAN devices. The best example is *Planet WMRT-414*. It could transmit UDP traffic at a speed of 30 Mbps but its multicast transmission speed was only 3 Mbps. The reason for this might be that the devices are using the IGMP snooping and the high quality IPTV transmission stress the device's CPU too much. So it might be so that the device just cannot process all the multicast packets so it has to limit the transmission. More information about the IGMP snooping can be found in Section 2.3.4.

The *ZyXEL G-570S* and *Ruckus MF2900* and *MF2501* were the only WLAN devices that could transmit the multicast type of traffic as well as the UDP type of traffic. As in the previous tests, *Ruckus* worked surprisingly well compared to the other products in the most demanding test.

To the *Coaxsys TVnet/C* and the *Planet PL-201*, the multicast did not cause any problems. Their transmission speeds with multicast traffic were as good as with UDP traffic.

5.2. Streaming Tests

In the streaming tests two different kinds of multimedia file were streamed between the computers. To test how well the DUTs handle an easy - in other words not so bandwidth demanding - streaming, a MP3 (*Mpeg-1 Audio Layer 3*) music file was used. This file had a constant bit rate of 192 Kbps. More demanding streaming tests were done with a video file which was in Mpeg-2 format and its bitrate was about 4,2 Mbps. The streaming tests were done with unicast and multicast traffic types. The media files were streamed and received with the *VLC Media Player* program.

In this thesis, the computer which was used to transmit the stream is called as a *streaming server* or just *server*. The computer that was used to receive and play the streamed file is called as *client*. In the following chapters these names are sometimes used while addressing these computers.

The devices ability to give priorities to media streams and multicast traffics was tested in the streaming tests. At the same time when the server was streaming the media file to the client a file transmission was started. The quality of the received signal was monitored during the file transmission. Also the time taken to transmit the whole file from one computer to the other was measured.

The streaming tests were performed in the same locations as the protocol tests. The test setups are presented in Section 5.1.1. The results are presented for one test area at a time. All the devices were not tested in all test setups.

5.2.1. Test Setup 1: Upper Limit

This section gives some background to the basics of estimation. A good level of quality means that the voice and image of the multimedia file can only contain some minor errors which appear now and then. The errors should not disturb the enjoyment of the video or music. Average quality means that there were some larger errors, like whole picture freezes for a second or two, or so many little errors that they disturb the watching or listening experience. Finally bad quality means that there was almost constantly some sort of errors that makes enjoyable watching and listening impossible. The results from the first test setup are presented in Table 5.5.

Table 5.5: Results from the streaming tests in test setup 1. ***S*** *->* ***C*** *means that the file was transmitted from the streaming server to the client and* ***C*** *->* ***S*** *means that the file was transmitted from the client to the server.*

	Video about 4,3 Mbps		Audio about 192 Kbps		Video streaming (multicast) + 100MB file transmission	
					Video quality	transmission time [s]
	unicast	multicast	unicast	multicast	S -> C / C -> S	S -> C / C -> S
A-Link	G	G	G	G	G / G	75 / 79
ZyXEL	G	G	G	G	A / B	81 / 98
Planet (WLAN)	G	B	G	G	G* / G*	77 / 80
Ruckus N	G	G	G	G	G / G	78 / 84
Ruckus S	G	G	G	G	G / G	84 / 86
Coaxsys	G	G	G	G	G / G	27 / 39
Planet (PL)	G	G	G	G	G / G	95 / 103

G = Good B = Bad A = Average

*Unicast type of transmission was used instead of multicast

From Table 5.5 it can be learnt that every, except the *Planet WMRT-414*, can transmit and receive streamed files in both unicast and multicast format. The *WMRT-414* multicast performance is not good enough to transmit multicast video even without other traffic. This is why in the *WMRT-414* file transmission test a unicast transmission method was used instead of multicast.

All of the devices succeed well in a QoS test where a file was transmitted at the same time as a video stream was in progress. Only the *ZyXEL G-570S* had some problems in giving

priorities to the video stream. When the transmission times in Table 5.2 are compared with the transmission times in Table 5.5, it can be seen that it took about 30 seconds longer to transmit the 100 MB file with a concurrent video stream than without any other traffic.

5.2.2. Test Setup 2: Medium Transmission

For the second test setup the, the transmission path was made more challenging. All the same tests were repeated and the results are presented in Table 5.6. The *Coaxsys* was not tested in this or the next test setup. More *Coaxsys* tests can be found in Section 5.4.

Table 5.6: Results from the streaming tests in test setup 2. ***S -> C*** *means that the file was transmitted from the server to the client and* ***C -> S*** *means that the file was transmitted from the client to the server.*

	Video about 4,3 Mbps		Audio about 192 Kbps		Video streaming (multicast) + 100MB file transmission	
					Video quality	transmission time [s]
	unicast	multicast	unicast	multicast	S -> C / C -> S	S -> C / C -> S
A-Link	G	G	G	G	G / G	136 / 156
ZyXEL	G	G	G	G	B / B	91 / 300**
Planet (WLAN)	G	NT	G	G	G* / A*	116 / 166
Ruckus N	G	G	G	G	G / G	120 / 85
Ruckus S	G	G	G	G	G / G	77 / 110
Planet (PL)	G	G	G	G	G / G	112 / 134

G = Good B = Bad A = Average NT = Not Tested

*Unicast type of transmission was used instead of multicast

**Transmission time was over 300 sec

Results show that all devices, except those that had problems in test setup 1, performed very well. Comparing to the previous test there is a greater variation in the transmission times. Nevertheless, the quality of the video stream was good. From the transmission times it can be seen that it is easier to transmit a file in the same direction as the stream. Only with *Ruckus*, with normal settings, was the file transmitted faster from the client to the streaming server than from the server to the client.

5.2.3. Test Setup 3: Difficult Transmission

There were no real hopes of successful performance for the most of the WLAN products tested in this last and most demanding streaming test. It was, however, interesting to see how well the *Ruckus* could handle this hardest of transmission paths. The results are presented in Table 5.7. The *Planet* power line device was not tested in this test setup.

Table 5.7: Results from the streaming tests in test setup 3. ***S*** *->* ***C*** *means that the file was transmitted from the server to the client and* ***C*** *->* ***S*** *means that the file was transmitted from the client to the server.* ***G*** *after A-Link means that the highly directional antennas were used and* ***R*** *after A-Link means that the repeater was used.*

	Video about 4,3 Mbps		Audio about 192 Kbps		Video streaming (multicast) + 100MB file transmission	
					Video quality	transmission time [s]
	unicast	multicast	unicast	multicast	S -> C / C -> S	S -> C / C -> S
A-Link	NT	NT	B	B	NT / NT	NT / NT
A-Link (G)	B	B	G	G	NT / NT	NT / NT
A-Link (R)	A	B	G	B	NT / NT	NT / NT
ZyXEL	NT	NT	B	B	NT / NT	NT / NT
Planet (WLAN)	NT	NT	G	B	NT / NT	NT / NT
Ruckus N	G	G	G	G	G / A	175 / 140
Ruckus S	G	G	G	G	G / B	165 / 136
	G = Good		B = Bad		A = Average	NT = Not Tested

Again, the *Ruckus* was the only one that could perform in the most demanding test environment. The others could not even transmit the audio file properly. With these devices it was no use to even try to transfer a video file or make the QoS test. Almost the only errors in streamed multimedia quality with the *Ruckus* appeared when the file was transmitted from the client to the streaming server.

It is interesting to find out that in this last test setup the file was transmitted much faster from the client to the server than the other way round. In other test setups the file was usually transmitted faster when it was sent from the server. One can make an assumption that, at least with the *Ruckus*, the QoS decisions are made inside the device and it affects only departing traffics. In other words, *Ruckus* devices do not communicate with each

other and tell if they are sending high priority traffic which needs a bandwidth reservation, so that the other *Ruckus* devices could take this into account when they are allocating the transmission resource to their own traffics.

5.3. IPTV Test Setup

The IPTV test setups differ a slightly from the protocol and streaming tests. The transmitter was moved into another location. This was done because the IPTV tests need an IPTV signal and the only place in the office where the IPTV signal could be received was located elsewhere.

5.3.1. IPTV Tests in General

The IPTV test was done only with the WLAN products. With the other devices it was only tested whether they could transmit IPTV signal without problems. The *Coaxsys TVnet/C* and the *Planet PL-201* passed that test with good grades. The qualities of the transmitted signals were good and no flaws were seen in the TV picture quality during the tests. Only short cables, of about 3 meters long, were used in this test. With the WLAN devices, the IPTV testing was more comprehensive.

The IPTV signal was first received with an ADSL modem and then it was transferred wirelessly to a set-top-box and TV. The IPTV signal was transmitted via channel 1. Other surrounding WLAN's used mostly the channels 6 and 11 so channel 1 had the lowest interference level.

The DUTs' ability to endure interference was measured also in the IPTV tests. This was done by creating an interfering WLAN connection between the two computers. Using this connection it was possible to generate different kinds of interference on different channels. Two *A-Link WL54AP2* devices were used to produce the interference signal

Two different kinds of interfering signal were used: file transmission and video streaming. The file transmission uses all the bandwidth that it can get and so it generates much interference. The video streaming in contrast, uses only a certain amount of bandwidth which is much less than that which the file transmission uses. In other words, the video streaming generates less interference than the file transmission. The interfering traffics were generated to the channels 11, 6 and 1 while the IPTV signal was transmitted on channel 1. The quality of the IPTV stream was monitored

Because the IPTV uses a multicast type of transmission method, the *Planet WMRT-414* was not tested. This device had so poor multicast performance that it was unable to even transmit the IPTV signal which needs about 6 Mbps constant transmission speed.

5.3.2. Test Setup 1: Easy IPTV

The location of the ADSL modem and the transmitting part of the WLAN link are marked with symbol "" in Figure 4.2. In the same figure the places of the receiver, set-top-box and TV are marked with the symbol "". As can be seen, the transmission path is very short and quite easy.

The interfering devices are marked with symbols "  " in Figure 4.2. The other interfering device was placed almost next to the receiver that tried to receive the IPTV signal. Because the interfering signal is extremely strong, this is also a good test to measure the robustness of the DUTs against interference.

The results are shown in Table 5.8. The basis of the estimation is the same as for the streaming tests. The *A-Link* was tested only without any improvements such as high gain antennas or repeaters and the *Ruckus* was tested only in normal mode.

Table 5.8: Results from the IPTV tests in the easy test setup.

		A-Link	ZyXEL	Ruckus N
	No interference	G	G	G
Streaming (4,3 Mbps)	on same channel	A	G	G
	on channel 6	A	G	G
	on channel 11	B	G	G
File transmission	on same channel	B	G	G
	on channel 6	B	G	B
	on channel 11	B	G	G
	G = Good	B = Bad	A = Average	

As Table 5.8 shows, the *ZyXEL* and *Ruckus* devices were able to tolerate the interference surprisingly well. Keeping in the mind that the interfering device was right next to them and still the quality of the received IPTV signal was good.

The *A-Link* had some trouble coping with the interference but without it the quality was good. The *A-Link* devices poor performance in this test can partly be caused by that fact that the interference signal was created with other *A-Link* devices. The devices that created the interference signal and the devices that transmitted the IPTV signal were identical. The *A-link* receiver is probably optimised to receive signals from another *A-link* device, therefore it probably receives the interference a slightly better than the other devices.

The only "B" (bad quality) in the *Ruckus* column is in an unexpected place. The interference is at its peak when the file is transmitted over the same channel as the IPTV signal. This situation the *Ruckus* cleared very well. But why, then is the IPTV's quality bad when the file is been transmitted over the channel 6? There are two possible reasons for this: concurrence or the *Ruckus* devices uses channel 6 for something.

It is possible that, at the same moment when the test was performed, there was an interference peak from some unknown source, and this affected the connection so much that the quality degenerated. This test was repeated afterwards when other tests were done and the situation was the same, so this explanation is not very likely.

The other explanation is that the *Ruckus* uses channel 6 for some sort of communication or signalling. In that case the, file transmission could interrupt that communication so much that the IPTV signal could not get through properly. This is almost as unlikely an explanation as the previous one. This phenomenon was not studied in greater details so the cause remained a mystery.

5.3.3. Test Setup 2: Medium IPTV

The transmitter was located in the same place as it was located in the previous test, being marked with the symbol "  " in Figure 4.2. The receiver was placed upstairs, in Figure 4.3 being marked with the symbol "  ". The source of interference is marked in Figure 4.2 again with the symbols "  "and the way of generating it is also identical to the previous test. This test measures the DUTs' abilities to transfer the IPTV signal in a little more demanding environment. The results are presented in Table 5.9.

Table 5.9: Results from the streaming tests in the mediocre test setup.

		A-Link	ZyXEL	Ruckus N
	No interference	G	M	G
Streaming (4,3 Mbps)	on same channel	G	B	G
	on channel 6	G	A	G
	on channel 11	G	A	G
File transmission	on same channel	B	B	G
	on channel 6	A	B	G
	on channel 11	G	A	G
	G = Good	B = Bad	A = Average	

The transmission path was a little harder than in the previous test but the interference was much fainter. This caused a great deterioration in the *ZyXEL G-570S* performance. On the other hand, *A-Link WL54AP2* performance improved noticeable. From this it can be assumed that the *G-570S* handles the interference better than the *WL54AP2* but it has problems with the operation range. In contrast, the *WL54AP2* has a better operation range but it has problems with interference tolerance.

5.3.4. Summary of IPTV Tests

The *Ruckus* seems to outperform both of its rivals. It has a good tolerance against interference and its range of operation was excellent. It does not show in the tables but the quality of the voice and picture was better with the *Ruckus* devices than with the other devices. When the tests were done with the *Ruckus*, the playback of the IPTV streams were most of the time flawless. When the other devices were tested the playback quality was good but some small errors occurred now and then.

5.4. Coaxsys TVnet/C test

The *Coaxsys TVnet/C* was tested separately. From the signal point of view, the environment in the cable is far more stable than in the air. This makes testing a lot easier: It's not necessary to do the tests in different locations. All that needs to be done is to add attenuation between the devices and then measure the transmission speeds. With coaxial cables it is quite easy to add attenuation because there are several external attenuators to choose from. With power cables, however, this is trickier. This is the reason why only the *Coaxsys TVnet/C* was tested in this way.

The test setup is presented in Figure 5.1. The attenuators, which were used in this test, were adjustable and their maximum attenuation was 20 dB. Short cables were used to connect the different parts together. Their overall length was about 5 meters. Cable attenuation was not taken into consideration. The results are presented in Table 5.10. Unfortunately there was no method to measure the exact attenuation that the signal was facing. This is the reason why all the attenuations which are marked in Table 5.10 are only rough estimations.

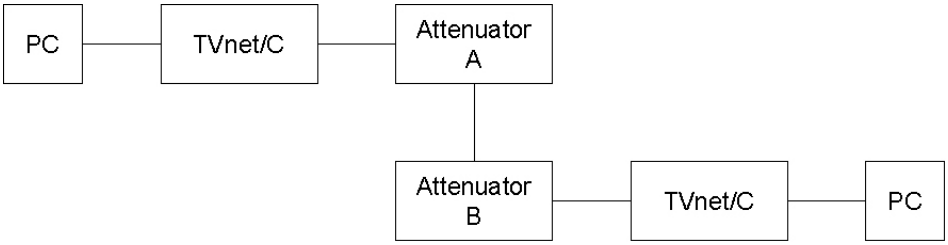
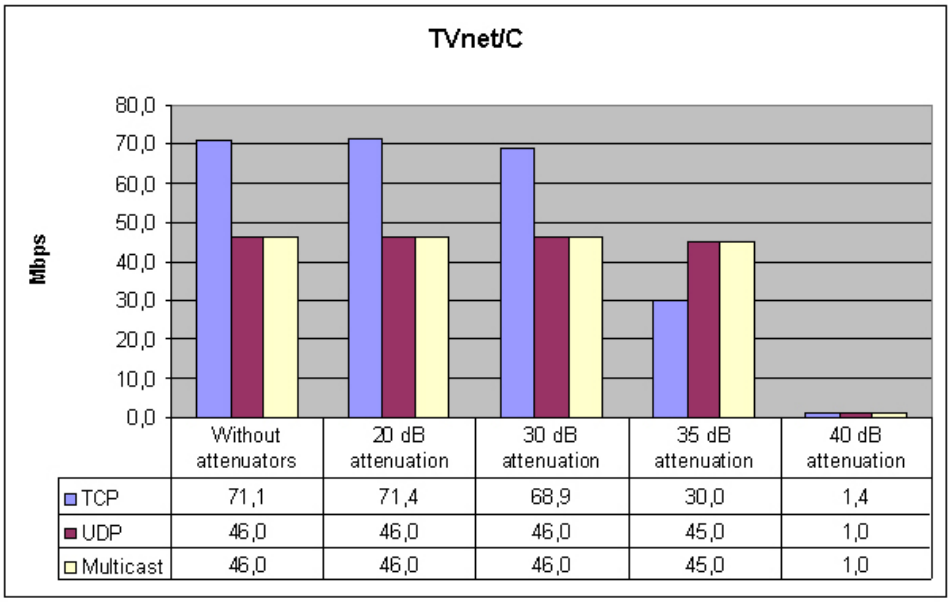


Figure 5.1: Test setup for Coaxsys TVnet/C. Both the attenuators were adjustable and their maximum attenuation was 20 dB.

This test gives only imprecise results for the maximum attenuation that the devices can handle. It gives more precise answer to the question: What effects does the attenuation have on the performance?

Table 5.10: Results from the Coaxsys tests.



	Without attenuators	20 dB attenuation	30 dB attenuation	35 dB attenuation	40 dB attenuation
TCP	71,1	71,4	68,9	30,0	1,4
UDP	46,0	46,0	46,0	45,0	1,0
Multicast	46,0	46,0	46,0	45,0	1,0

As Table 5.10 shows, the *TVnet/C* can withstand almost 40 dB attenuation. Table 5.10 also tells that the attenuation starts to affect the performance only when its magnitude is over 30 dB. After that the performance degenerates relatively fast.

When the test was done with 35 dB attenuation an interesting thing was observed. In this test the TCP transmission speed was very unstable. Sometimes it was very fast, all the way up to 50 Mbps, and sometimes it halted completely. The average speed was 30 Mbps. Be-

cause UDP and multicast traffics need stable transmission speeds, one might think that there would be lots of errors when these transmission protocols were tested. But as Table 5.10 shows this was not the case. The packet loss percentage with the UDP and multicast protocols were as low as it was in the previous tests. It would have been interesting to study this phenomenon more closely but there was no time for that.

The thing that the results in Table 5.10 do not show is that after 10 Mbps speeds the UDP and multicast transmissions started to lose packets. This happened regardless of the amount of attenuation. The packet loss percentage never became got greater than one percent until the upper limit was reached. The lost packets were divided evenly for the duration of the transmission. Only once a larger error cluster occurred.

In summary, *TVnet/c* worked very well and it has capabilities to transmit several IPTV signals simultaneously. Its only problem is the attenuation. The antenna cables are designed for lower frequencies than what *TVnet/C* uses. Because of this the attenuation that the *TVnet/C* signal faces is far greater that that faced by an ordinary TV signal. For example, in a common antenna cable type RG-6, the attenuation for a signal with a frequency of 500 MHz is about 21 dB/100m and for 1000 MHz, which *TVnet/C* uses, the attenuation is about 31 dB/100m. In other words, the operating range is a quite small but it should cover the normal household.

6. Interpretation of Results

This chapter contains a brief conclusion about the results presented in Chapter 5. The performances of the WLAN and wire/cable devices are evaluated separately. The strengths and weaknesses of the devices are figured out. Also there are speculations about in what kinds of situation these devices could be used. In particular their suitability for IPTV transmission was evaluated.

The *Ruckus* devices performed almost overwhelmingly well compared to the other WLAN devices, especially in the most demanding tests. At the end of this chapter there is a brief description of the technical features of the *Ruckus* devices. It is assumed that these features are the reason why the *Ruckus* devices performed so well.

6.1. WLAN devices

The performances of the WLAN devices are evaluated in Table 6.1. Every device handled the TCP/UDP traffics well. This was not a big surprise because the TCP and UDP protocols are the most used protocols in normal Internet traffic. On the other hand the difficulties which the *Planet WMRT-414* faced in the multicast and IPTV tests came as a surprise. It appears that not every manufacturer designs their products for multicast traffic.

The *Ruckus* had by far the best range of coverage of the WLAN devices. This does not, however, mean that the other devices had bad coverage. Every tested device could easily

cover an average sized apartment. The *Ruckus* ability to maintain a good transmission speed even when the transmitter and receiver were far away was unique. The other devices could not do this.

The *Ruckus* was the only one that got a *good* rating in IPTV column in Table 6.1. The reason for this is that the *Ruckus* was the only tested WLAN device that could transmit an IPTV signal flawlessly. With the other devices the quality was quite good but small errors occurred occasional. The difference was not as notable as one might thing when looking the table.

Interference resistance was only tested briefly and it was not one of the key aspects of the tests. The results in Table 6.1 *Interference resistance* column should be taken more as guidelines and not as well tested results.

Table 6.1: Conclusion from the tested WLAN devices.

Device	TCP / UDP	Multicast	IPTV	Range	Interference resistance
A-Link	good	average	average	average	average
ZyXEL	good	good	average	average	good
Planet	good	bad	bad	average	average
Ruckus	good	good	good	good	good

6.1.1. A-Link WL54AP2

The *A-Link WL54AP2* device was the oldest of the WLAN devices in the test. This device had a good TCP and UDP performance when the transmission path was relatively easy. Nevertheless it had some problems with multicast. The highest speed at which a multicast type of traffic could be transmitted was 10 Mbps. It is enough for one standard definition IPTV channel which needs about a 6 Mbps stream. Even though the *A-Link* was also quite vulnerable to interference, it had a relatively good operating range.

Because of its flaws the *A-Link* is not well suited for IPTV transmission. It can transmit one IPTV channel but the quality will not be stable enough for enjoyable viewing. Otherwise, it is still a very good WLAN device for normal usage.

6.1.2. ZyXEL G-570S

The *ZyXEL G-570S* device had slightly better TCP and UDP performance than the *A-Link WL54AP2* but it also degenerated faster when a transmission path grew longer. The *ZyXEL* could cope with multicast traffic very well, being able to transfer several IPTV channels at once. The tolerance for interference from other WLAN devices was excellent. The only disadvantage in this device was its operating range. This really bring this device down, otherwise it would be a really good product for IPTV transmission.

The quality of the IPTV signal was quite good but the short operating range really hinders its usefulness. The *G-570S* is not an ideal device for IPTV transmission but it could probably be used in that sort of transmission as long as the transmission path is trivial.

6.1.3. Planet WMRT-414

The *Planet WMRT-414* device was a brand new MIMO device and it failed miserably in the multicast test. It could transfer multicast traffic only at a speed of 3 Mbps. This clearly ruins any hope for IPTV usage. This is really a shame because the *WMRT-414* had a somewhat better operating range than the *A-Link* or *ZyXEL* had. The TCP and UDP performance was very good.

This device shows that not every WLAN product, even if they claim to use new MIMO technology, can transmit multicast. Those two receiving antennas slightly increase the operating range, giving the *WMRT-414* a little edge over traditional WLAN devices. This is a good WLAN device but it cannot be used with multicast or IPTV.

6.1.4. Ruckus MF2900 and MF2501

The *Ruckus* was very successful in the every test. Multicast traffic did not cause any problems to these devices, providing that the traffic flow was from the *MF2900* (access point) to the *MF2501* (adapter). In the other direction, the multicast signals did not travel at all. The operating range was far greater than any other tested WLAN device had. Even the quality of the IPTV signal with the *Ruckus* was slightly better than with the other WLAN devices.

MF2900 and *MF2501* are designed for IPTV transmission and it shows. These devices can be used to transmit IPTV signals even if the transmission path is difficult. Of course, the *Ruckus* device is also an excellent product for normal WLAN use.

6.2. Wire/Cable devices

In Table 6.2 are the evaluations from the wire/cable devices. There is no interference column because these kinds of tests were not made. Both the *Coaxsys* and *Planet* are capable of transmitting multicast and IPTV signals almost as well as normal TCP/UDP signals.

The only disadvantage with these devices is that their operating range is hard to evaluate. Even if the sockets are located closely together it is hard to tell if they really are connected. The cables can travel a long way inside the house's walls or there might even be filters or circulators that prevent the signal from passing through.

Table 6.2: Conclusion from the tested power line and antenna cable device.

	TCP / UDP	Multicast	IPTV	Range
Coaxsys	good	good	good	depend
Planet	good	good	good	depend

6.2.1. Coaxsys TVnet/C

The *Coaxsys TVnet/C* had by far the best performance in every aspect that was tested. Only the operating range may cause some problems. It is usually unknown how the antenna cables are laid in households. How long they are and what kinds of filters there may be installed. Beforehand it is very difficult to know whether this device will work in that particular installation environment. Unlike with the WLAN devices, with the *Coaxsys TVnetC* there is not much to be done if the connection does not work.

When the connection is possible, the *TVnet/C* can easily transfer multiple IPTV channels. Because the signal travels in the cable, the connection is very stable which means a good quality. If the household has multiple antenna sockets and the antenna network does not have filters that block the signal, the *Coaxsys* is a good LAN device.

6.2.2. Planet PL-201

The *Planet PL-201* had a good overall performance. Transmission speeds were lower than with the *Coaxsys* but that was not a problem. Unfortunately, the *Planet PL-201* operation range could not be measured. But maybe that would have been fruitless because it depends so much on the power cables and their condition.

The *Planet PL-201* can be used to transmit multicast and IPTV signals. The *PL-201*, however, suffers from the same problem as the *Coaxsys TVnet/C*: one can never know beforehand will the connection work or not. And there is very little that anyone can do if the connection does not work.

6.3. Technical Presentation of Ruckus

The *Ruckus* had clearly the best results almost in every test that was made among the WLAN devices. One reason is that the *Ruckus MF2900* (access point) and *MF2501* (adapter) are specially designed for IPTV transmission [18]. In that kind of transmission a

steady bitrate of about 5-6 Mbps is essential. Designers have, therefore, included some smart features in these devices.

First at all, the access point and adapter are not identical. They are designed to work as a pair. Both of them can still work with other WLAN devices but then some of the special features cannot be used.

6.3.1. Antennas

Antennas are the main reason why the *Ruckus* had the largest range of coverage. Both the *MF2900* and *MF2501* have six directional antennas and the devices automatically choose the best antennas to use. As the example calculation in Section 2.1 showed, that even with weak directional antennas the gain in the coverage range was significant. A receiver using directional antennas can receive a stronger signal than with isotropic antennas.

The ability to monitor and change the transmission path also improves the connection's stability and interference tolerance. When something disturbs the signal at the current transmission path, the device can just choose another transmission path which has lower interference. This really helps to keep transmission speeds at a decent rate for the IPTV signal.

6.3.2. Quality of Service

Other very beneficial features the *Ruckus* device has is its ability to give priorities to different kinds of traffics. It differentiates and manages IPTV streams separately from all other traffic types. This algorithm guarantees that the IPTV signal has all the bandwidth that it needs.

6.3.3. Resendable UDP and Multicast Packets

When UDP or multicast type of traffic is transferred via *Ruckus* devices, they reveal one quite unique feature: resendable UDP / multicast packets. When the UDP and multicast

packets travel through a *Ruckus* access point (*MF2900*), those packets are modified so that they can be resent if needed. In the adapter (*MF2501*), these packets are modified back to their normal form. This procedure needs buffers and that means delay. The exact amount of delay what this will produce wasn't measured. This might cause some problems with services that demand delay sensitive two way signalling.

This feature improves the quality of the IPTV signal a staggering amount. The wireless communication is unstable and some transmitted packets are lost for sure. Resending lost and damaged packets is an easy way to make sure that the receiver gets all the sent packets correctly. This was probably the main reason why the *Ruckus* was able to transmit a good quality IPTV signal even under harsh conditions.

7. Conclusion

The reasons why this study was made was to find out could a high performance LAN be built without relying on Ethernet technology. In other words, we wanted to find out if it would be possible to build a network without laying any additional cables. The network should be wireless or in another way unnoticeable. That is why four WLAN devices were tested along with two devices that used antenna cables and power wires to transmit information. The network should have enough transmission capabilities to transfer a single IPTV stream (standard definition TV channel) and the network should cover a common household.

The study showed that WLAN devices have considerable differences in performances. Especially well, this was confirmed in their varying multicast capabilities. Some devices which performed well when other protocols were used had great difficulties to transfer a multicast type of traffic. Devices that used wires had more stable performance between different transmission protocols. The person who is going to built a wireless network must ponder carefully about what kind of traffic there will be travelling there and choose the devices accordingly.

The study revealed that there are alternatives for the Ethernet cables. A high performance network can be built wirelessly or by using power lines or antenna cables. Only one WLAN device (*Ruckus*) had the required performance and coverage capabilities to do this. The other WLAN devices had quite good performance in most of the tests but they also had some flaws and problems. The Achilles' heel for the majority of the wireless devices was the range of coverage and the ability to handle multicast traffic.

Wire line and antenna cable devices had the required performance so these devices can be used to a build high performance LAN. Their only problem was that their transmission path is usually unknown. To know the transmission path one should have the knowledge about how the wires and cables are installed when the house was build. This makes the panning harder because it is very hard to evaluate if the connection between devices is possible.

Although the test environment was problematic the testing went well. The measured performance results and the observed capabilities were similar. This leads to the conclusion that the performed tests were accurate and the results are reliable.

The devices were tested in three different test setup but all of them were located in the same office building. The tests that were made during this study should be repeated in different locations. It would be interesting to find out how this would affect the performance of the devices especially the range of coverage. In this study it was only tested how well the devices could transmit a standard definition IPTV stream. The devices should be tested also with a high definition IPTV stream which is more demanding than the standard definition.

This study clearly showed that the WLAN devices have noticeable differences in their performance. But it also showed that WLAN devices can be very reliable and have large coverage if they are designed for that. Due to this study a conclusion can be made that the wire line and antenna cable devices are a viable alternative for an Ethernet based network for household use.

The future of WLAN is very interesting. The new IEEE 802.11n standard is going to be released. It promises to greatly increase the transmission speed and also the range of coverage. These new improvements will surely give much more opportunities to WLAN. The only question is how well the manufacturers can implement them. The only way to find out that is to do a similar study to this one with the new products once they have been released to the market.

Appendix

Iperf v.1.7.0

Iperf is a network testing tool that can create TCP, UDP and multicast data streams and measure the throughput of a network that is carrying them. *Iperf* has to be installed on at least two computers before measurements can be performed. One computer acts as a server and the other is a client. The used test setup is presented in Figure A.1.

Figure A.1: The Iperf server and client communicated with each other through the link that the DUTs have created.

TCP measurements

TCP traffic was measured using the following commands.

Server: **`Iperf -s`**

Client: **`Iperf -c 192.168.1.33 -t x`**

Where **`-s`** denotes the server and **`-c 192.168.1.33`** denotes that the computer is a client and it communicates with the server whose IP address is 192.168.1.33. The **`-t x`** determines the duration of the test in seconds. The values **`x`** = 10, 20 and 30 were used in the tests.

UDP measurements

UDP traffic was measured using the following commands.

Server: `Iperf -s -u`

Client: `Iperf -c 192.168.1.33 -u -t 30 -b y`

Where `-u` denotes that the test is performed using a UDP data stream. All the UDP tests were executed using a 30 second test duration. The `-b y` determines the used data transmission rate of the test. Different `y` values were used and the packet loss percentage was monitored. Data transmission rate was increased steadily until the packet loss percentage exceeded one percent. Every test was repeated three times and if the packet loss percentage was lower than one percent in at least two tests the data rate was increased.

Multicast measurements

Multicast traffic was measured using the following commands.

Server: `Iperf -s -u -B 224.0.67.67`

Client: `Iperf -c 224.0.67.67 -u -t 30 -b y`

Where `-B 224.0.67.67` denotes the used multicast channel. The used multicast channel was picked randomly. Because the test network contained only two computers, there was no fear that the traffic would interfere with any other transmissions. The multicast tests were performed in a similar fashion as the UDP tests.

VLC Media Player

The same kind of test setup was used with *VLC Media Player* than what was used with *Iperf*. The one computer acted as a server and the other acted as a client. The server streamed the multimedia file to the client. The quality of the streamed media file was monitored.

Unicast streaming

The following commands were used.

Server: `VLC Test.mpg --sout udp:192.168.1.34`

Client: `VLC udp:`

Where **`Test.mpg`** is the name of the streamed file. The **`--shout udp:192.168.1.34`** determines which address the stream is transmitted to. In the client the **`udp:`** means that the *VLC* starts to play the stream that is sent to it.

Multicast streaming

The following commands were used.

Server: **`VLC Test.mpg --sout udp:224.0.67.67`**

Client: **`VLC udp:@224.0.67.67`**

Where **`udp:@224.0.67.67`** determines the channel which the client listens. The server sends the stream to that multicast channel and the client plays it.

References

1. A. Bruce Carlson, Paul B. Crilly, Janet C. Rutledge (2002) Communication Systems (4th edition). Published in New York [850 pages]

2. Viestintävirasto (2007) Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä [network documentation]. Published in Helsinki [referenced 18.09.2008]. Available: http://www.ficora.fi/index/saadokset/maaraykset.html [document: 15 X/2007 M.pdf]

3. Ismo Lindell, Keijo Nikoskinen (1997) Antenniteoria (4th edition). Published in Helsinki [347 pages]

4. Neil Gerein (2003) A Spatial Diversity Scheme - For Fixed Point Indoor Wireless Communication [network documentation]. Published in Saskatoon [referred 28.10.2008]. Available: http://library2.usask.ca/theses/available/etd-12232003-182252/unrestricted/Neil_Gerein_thesis.pdf

5. Jacob Sharon (2006) Introduction to Wireless MIMO - Theory and Applications [network documentation]. Published in Stony Brook University [referenced 18.09.2008]. Available: http://www.ieee.li/pdf/viewgraphs_wireless_mimo.pdf

6. Ruckus Wireless (2008) Presentation PDF about Ruckus' BeamFlex technology [network documentation]. Published in Internet [referenced 31.10.2008]. Available: http://www.ruckuswireless.com/pdf/fs-beamflex.pdf

7. Planet Network and Communication (2006) Presentation PDF about Wireless WMRT-414 MIMO Broadband Router [network documentation]. Published in Internet [referenced 31.10.2008]. Available: http://www.planet.com.tw/en/product/images/4923/C-WMRT414-1_s.pdf

8. Muhammad I R, Surva S D & Frank H.P. Fitzek (2005) OFDM Based WLAN Systems [network documentation]. Published in Aalborg University, [referenced 18.09.2008]. Available: http://kom.aau.dk/~imr/RadioCommIII/TR_OFDM_review.pdf

9. A. Bruce Carlson, Paul B. Crilly, Janet C. Rutledge (2002) Communication Systems. Published in New York [850 pages]

10. Michael Hall (2006) Course' "Wireless Personal, Local, Metropolitan, and Wide Area Networks" lecture notes [network documentation]. Published in Helsinki University of Technology [referenced 31.10.2008]. Available: http://www.comlab.hut.fi/studies/3240/luentokalvot/5_wlan3.pdf

11. Kihong Park (2004) Data Communication and Computer Networks [network documentation]. Published in Purdue University [referenced 18.09.2008]. Available: http://www.cs.purdue.edu/homes/park/cs536-wireless-3.pdf

12. Andrzej Duda (2004) 802.11 and QoS [network documentation]. Published in Joseph Fourier University [referenced 18.09.2008]. Available: ftp://ftp-sop.inria.fr/mascotte/David.Coudert/ecotel/2004/Cours/ca5-Qos_802-11-duda-ecotel04-final.pdf

13. Ruckus Wireless (2005) MediaFlex 2900 Multimedia Access Point User's Guide [network documentation]. Published in Internet [referenced 31.10.2008]. Available:

14. Jupiter Networks (2007) Introduction to IGMP for IPTV Networks [network documentation]. Published in Internet [referenced 25.05.2009]. Available: http://www.juniper.net/solutions/literature/white_papers/200188.pdf

15. Cisco (2002) IP Multicast Technology Overview [network documentation]. Published in Internet [referenced 25.05.2009]. Available: http://www.cisco.com/en/US/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.pdf

16. Planet Technology Corporation (2007) Powerline Ethernet Bridge Data Sheet [network documentation]. Published in Internet [referenced 02.04.2010]. Available: http://www.planet.com.tw/en/support/download.php?mt=0

17. Coaxsys (2005) Installation Manual & Troubleshooting Guide [network documentation]. Published in Internet [referenced 02.04.2010]. Available: http://www.smarthome.com/manuals/30000.pdf

18. Ruckus Wireless (2005) MediaFlex 2900 Multimedia Access Point User's Guide [network documentation]. Published in Internet [referenced 02.04.2010]. Available: http://support.ruckuswireless.com/documents/14-mf2900-user-guide/download