Evaluating and Testing Wireless Local Area Networks

Table of Contents

Project Type:

Research Based Evaluation Project.

Aims:

To research into the technological standards used for wireless internet access encompassing security, social, ethical and legal issues, evaluating the technical and functional differences between wired and wireless standards by IEEE.

Objectives:

1. To investigate into communication procedure used by Wi-Fi
2. To define the protocols and technologies used in Wi-Fi
3. Analyze the vulnerabilities in security faced by IEEE 802.11
4. What effect does it have in the industry?
5. To evaluate which standard will be more successful by considering other technologies.

Keywords:

Wireless Networks, Wi-Fi, WIMAX, wireless protocol standards.

Abstract:

Avoiding high costs and complexity of cabling, wireless connectivity is gaining wide attention both from home and business environment. It is coming to a mutual conclusion that wireless connectivity as a last mile internet connectivity will replace structured cabling, however the current standard Wi-Fi IEEE 802.11 provides a solid platform for development and advancement in this field.

Newer technology standard WIMAX IEEE 802.16 relatively covers issues of providing high bandwidth and long distance connectivity attributes. This research will cover the vulnerabilities and potential of IEEE 802.11 standards compared to wired LAN Standard 802.3 by IEEE. A brief insight of technologies alternative to IEEE standards will be mentioned.

1.0 Introduction:

Wireless Networks use air or space as a medium for transmitting signals. These signals are sent and received to and from one network as electromagnetic waves.
The advent of wireless networks started as early as 1835 when Samuel Morse developed the electromagnetic telegraph enabling messages to be encoded and transmitted serially as dots and dashes. All along the years after that there were inventions, innovations and theories brought to us by names like Alexander Graham Bell, Nobel Prize winner Marconi that led to companies AT&T and Zenith coming up innovative inventions like cordless telephones, remote-control garage openers and portable radios **(1)**.
Nowadays with the accumulative advancements in wireless systems the protocols and standards are made available even for common people to use as they are made affordable and easy to operate without the feeling of having it around in an everyday life.
An endeavour will be made to encompass an evaluative investigation comparing a wireless LAN with wired LAN using 802.3 and 802.11 standards brought in by IEEE. Both these standards use the TCP/IP protocol suite; therefore can be used in conjunction to each other.
The current standard used today, IEEE 802.11 is referred to as Wi-Fi where as the new standard 802.16 referred to as WIMAX will be mentioned in the report.

1.1 Problem Definition:

Although Wireless Networks existed as early as the nineteenth century; however it gained popularity in terms of local area networking when personal computers were made available. The most common wireless LAN used these days is the standard provided by the IEEE that is IEEE 802.11 or WI-FI known to most of us. As Developments are been done in all fields of computing, there is development been done in Wireless LANs as well. Lately a new standard was introduced by the IEEE known WIMAX (IEEE Standard 802.16). With all the advancements in wireless technology taking place, concerns arise whether WLAN or even Wireless WAN technology should replace the wired LANs, reducing costs, structuring and maintaining a cabled infrastructure. Most hardware manufacturers are committed to supply laptops with support for Wireless WANs as early as 2008.

1.2 Test Question:

Most of the world now is moving towards the wireless medium and this is the time when WI-FI has reached the peak of its popularity. Now is the time when a decision is required whether WI-FI will continue and improve by bringing out new and improved (in terms of speed and range) flavours as the current bandwidth provided is up to 54Mbps and the range is no greater than a 100 meter in optimum conditions. Does Wireless Technology have the potential to wipe off wired infrastructure completely and take over as a de-facto medium? Or will both standards continue their role in the market share?
Considering bandwidth allocation, maximum range, security and reliability provided by each technology are not the only factors considered. To come up with an answer regarding the present and the future of wireless media to be commonly used we also have to look into whether manufacturers will be able to promote the chosen technology over the other and will the user community be ready to adopt to that. In order to come up with a conclusion an in-depth analysis is required through preparing and executing test cases to compare and contrast both technology standards using same environment in terms of hardware, software, protocols and tools that will test the efficiency, reliability, availability and security.

1.3 Factors to be considered:

1) **Time:** the project that encompasses the research based on findings from previous researches and testing both type of Local Area Networks in same conditions need to be handed in by the 10th of May that is there are about 10 weeks to complete all tasks.

2) **Cost:** this is an undergraduate project therefore there is not much funding provided for it to carry out. The resources required to carry out this research are similar to that of any course work and therefore no major costs will be incurred to carry out this research. Learning resources like access to inter-library loans, books and online journals are provided free by the university. Hardware and software is already available, some of the software will be download as free licences from the internet.

3) **Quality:** this is to determine how good or rather up to the required standard the project is. The quality of the project should aim for a worthy honours undergraduate degree level.

4) **Scope:** this research covers the details asked in the research question. It also explains the constraints in the research. This means that the focus should be to cover the aspects of the aims and the objectives mentioned in the research. This

research critically analyzes and evaluates the literature searched to draw conclusions on the chosen topic.

5) **Resources:** this is the most important element in the research. It is necessary that the resources required to carry out the research are available. The material required to carry out this research is easily available at the university's library. The resources used for this research are taken from the monthly subscriptions from The IET and BCS. Journals are reviewed using the Athens account and ACM digital library that has resources available in regard to the research topic. The necessary hardware is already available along with the software. Licences for the software used are either already procured, are trial based or free.

1.4 Research Issues:

There are three bold issues that cannot be overlooked. These are as follows:

1) **Legal Issues:** any part of the research cannot claim ownership of an idea or invention that is infringed from another source. There cannot be anything in the research that uses illegal means like surpassing access rights to a piece material to be used in the research.
2) **Ethical Issues:** there should not be anything in the research or while conducting the research that conflicts with the ACM code of Ethics and Professional Conduct. The research should be a contribution to the society in a way that cultural diversity is respected. The research should not harm other research works and due credit should be given to people involved in the research.
3) **Social Issues:** the research should be based on fair actions and there should not be any discrimination based on commercial interests, political reasons or even national origin.

1.5 Research Methodologies:

The research methodologies used during the project will be both Qualitative and Quantitative.

Qualitative Methodology:
In our comparative analysis of the two technologies we will adopt the convention of using Qualitative Research Methodology. During this we will base our work on material made available through other researches already done and then comment on them whether they are true or they have some loop holes. An attempt will be made to interpret the phenomenon described by other research work and constructive perspectives. This research work will state research question rather than prediction based on statistical test results.

Quantitative Methodology:

To draw conclusions of our own, experiments are required to be carried out. The best way to carry out an experiment is to test both technologies using the same test data and conditions. This will prove the actual differences between the two technologies. During these experiments, the theories researched upon will be evaluated first hand with the use of measurement and observations.

1.6 Research Methods:

Data Analysis:

In order to perform data analysis, research literature based on the topic of the research will be referred so that conclusions can be drawn. It is a non-linear process therefore different perspectives on the same topic can be discussed and comments will be included to clarify which is the more reliable and accurate source. While drawing conclusion and reviewing documents the exact meaning will be interpreted that the researcher wants to convey. There will be a critical evaluation and conclusion of the research work conducted in the end.

User Testing:

Both technologies will be tested in the same test environment. To achieve the closest results data used to test both technologies will be same, as well as the software used to test both the WLAN and the LAN will be same. First the software will run on one type of network and then on the other. Observations will be made and results will be recorded to differentiate both technologies.

2.0 Wired and Wireless LANs:

2.1 Introduction:

History of both Wired and Wireless LANs will be looked into within this chapter, what the first implementation was, the inspiration and requirements behind the technologies and why were they developed. This chapter introduces the platform considerations used by both technologies like frequencies, operating current, supporting media and bandwidth developments over the years.

2.2 History and Evolution of Wireless LANS:

The 100 m distance limitation, vulnerability to EMI, the cost and maintenance of the copper wires were the reasons to why wireless LANs came in to being. After the Morse code became popular through the first Atlantic distress signal, experiments were conducted to use wireless technology for transmissions (2). During WWII wireless signals were encrypted and used as an invaluable tool by the U.S military to send signals across from shore to shore in secret from the enemy with an inspiration derived from the Hertzian Waves used by Marconi's radio wave experiments (2). This popularity of wireless technology led to bring the connection of computers as a local area network without using telephone cables.

2.2.1 First Wireless Network:

In 1971the University of Hawaii conducted the ALOHNET research project which was the first successful attempt to use networking technologies along with packet radio communication to achieve a wireless local area network. This project consisted of seven computers spread on four different islands, with the central computer being in Ohau Island and the network using a bidirectional star topology (2). Within the next decade to standardize the development of wireless networks in the industrial (902-928 MHz), scientific (2.24-2.4 GHz) and medical (5.7-5.8 GHz) [ISM] frequency bands, 802.11 was proposed as the IEEE standard for wireless networks by the Federal Communications Commission (FCC). As long as the devices meet the special FCC requirements, the frequencies do not require licenses (2).

2.2.2 Military interest:

The combination of packet data and broadcast radio gained attention of the U.S military and throughout the 70s and 80s Defense Advanced Research Projects Agency (DARPA) invested significantly into this technology to come up with nodes that could configure and reconfigure (self-configure) themselves into a network without the need of an established infrastructure. During the mid 80s DARPA's interests had grown beyond ever however the resulting system lacked both in speed and performance compared to expectations (3).

2.2.3 Commercial Usage:

Packet radio network services were first introduced in the 90's for commercial purposes, however they only supported up to 20Kbps and such services disappeared mainly because of low data rates and high costs (3). Vendors found the ISM band more useful as they did not have to obtain FCC license in order to operate on this band, however the wireless LAN systems were to keep a low power profile and an inefficient signaling scheme so that they do not interfere with the primary ISM band users. This caused the initial wireless LAN systems to suffer poor performance levels in terms of data rates and coverage. Poor performance led to concerns about security, standardization and high costs, which had a deep impact on sales as only few of these systems were used for low level activities like inventory control (3).

2.2.4 Wi-Fi over the Years:

The current generation of wireless LANs 802.11 are based on the LAN standard Ethernet 802.3; that when developed in the 70s had a data rate capacity of 10Mbps (3).

Ever since the 802.11 standard was approved by the IEEE in 1997 there have been great deals of improvements (in terms of Speed, Quality of Service, Security and Global Acceptability) that have been made in this family of wireless local area networks (WLANs) (4).

At the physical layer 2 sub standards 802.11 (a) and (b) were approved in the 1999. The former worked at 5GHz frequency unlicensed band using the Orthogonal Frequency Division Multiplexing (OFDM modulation) and providing raw data rates up to 54Mbps. The latter operated at 2.4 GHz defining a 64 bit complementary code keying (CCK) modulation delivering up to 11Mbps raw data rates (4).

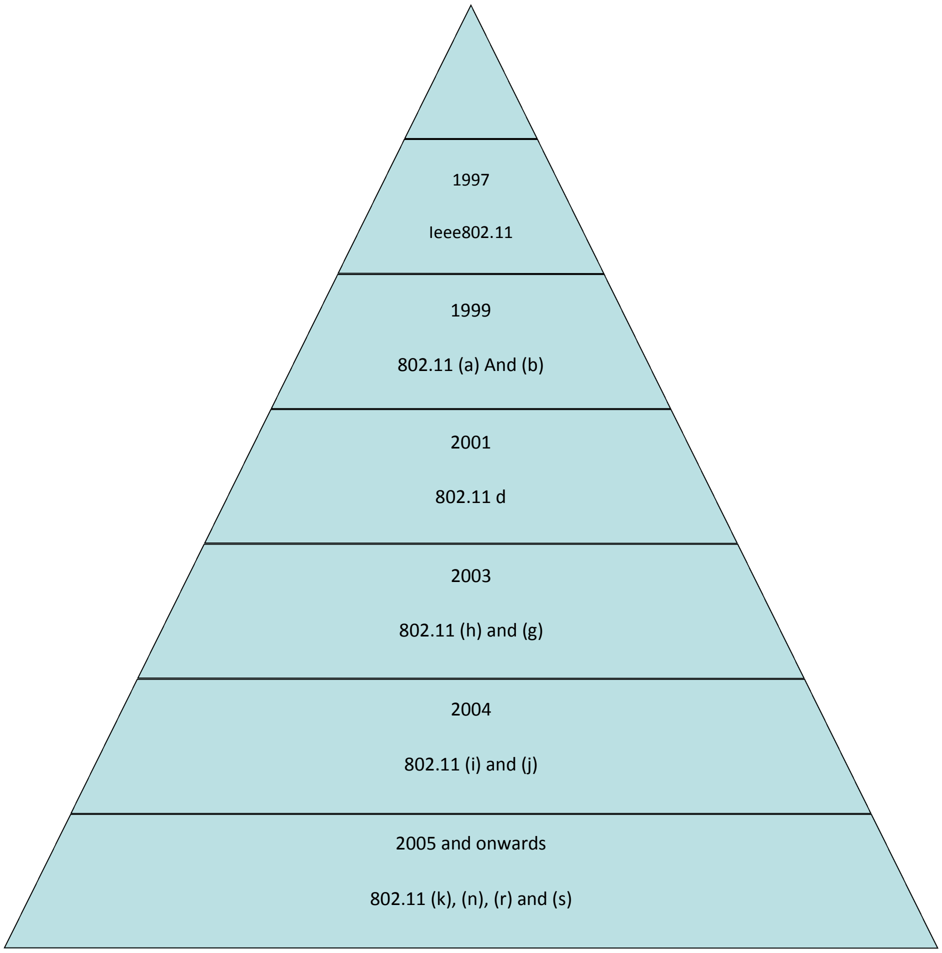
In 2001 and 2003 802.11d and 802.11h were approved so that the physical and MAC layers can be extended to be used in regulatory domains around the globe at 5GHz (4).

A backward compatible extension of 802.11b was approved in 2003 and was set as 802.11g, having the capacity of both OFDM and CCK modulation, operating at 2.4GHz and transferring data rate at 54Mbps (4).

To enhance on security in 2004 another standard 802.11i was approved. Strong authentication and access control mechanisms leveraging RADIUS and the IEEE standard for securing LANs 802.1x (key management) were defined. The standard also includes stronger encryption and data confidentiality using TKIP and AES along with stronger message integrity checking. To operate at 4.9GHz in Japan, 802.11j was approved in 2004 to define regulatory and protocol extensions (4).

With 2005 onwards the 802.11 task group has worked to come up with extensions like (k), (n), (r) and (s). These are focused to bring in uniformity and manufacturer platform independence, achieving speeds greater than 150Mbps, reducing handoff latency when client devices transition between access points or cells, facilitate SIP-based Voice over Wi-Fi and most importantly to work as a mesh standard where access points or cells from multiple manufacturers can self configure into multi-hop wireless topologies (4).

Fig 2.1 below shows Evolution of the IEEE standards for WLANs.



2.3 Ethernet- the wired local area network:

We will be looking at Ethernet, which has been approved as an IEEE 802.3 standard for wired Local Area Networks. The main reason for choosing this is in the research test project is that it has become the de facto standard for wired LANs when even the MACs are switching to TCP/IP. The reasons why 85% of the connected LANS are using Ethernet today are (5):

- Easy management, troubleshooting, implementation and maintenance.
- Implementation being low cost compared to token ring.
- Flexible when determining what topology to implement.
- Allows interoperability between different manufacturers.

2.3.1 Advent of Ethernet:

The Ethernet was developed by the Xerox Corporation in 1974 as a result of an experimental network layout using coaxial cables achieving a data rate of 3Mbps. The protocol technology used to us this network was carrier sense multiple access collision detection or CSMA/CD. The purpose of this was to support a network with busty traffic, having network printing and file sharing. With successful and desirable results Xerox Corp, Intel Corp and DEC formed a three- consortium to jointly develop Ethernet version 1.0 in 1980 that operated with a data rate of 10Mbps (5).

The IEEE then approved a standard 802.3 in 1983 that was very similar to, in fact had its platform set from the Ethernet version 1.0 specification. This standard was officially published in 1985 as the ANSI/IEEE Std. 802.3-1985. There are however enhancements made to these specification to adapt to technology changes (5).

2.3.2 Overview of the Technology:

IEEE 802.3 standard uses Ethernet products that follow the CSMA/CD protocol. It comes in three different flavours (5):

- 10 Mbps – 10 Base-T Ethernet
- 100 Mbps – Fast Ethernet
- 1000 Mbps – Gigabit Ethernet (it has now even branched out to 10 – Gigabit Ethernet reaching 10 times the predecessors data rate)

The CSMA/CD Access Method:

In order for two or more stations to share common media in an environment where there are no switches, the CSMA/CD protocol was developed. This has features that do not require central arbitration, access tokens and not even time slots to indicate when a station is allowed transmission. The media access control is determined for every station on its own as to when to send a frame. This is done in the following way (5):

- Each station listens to the traffic on the media and determines when gaps between frame transmissions occur. This is known as **Carrier Sense**.
- When the network is idol, a listening station can send its frame transmission. This is the **Multiple Access** of the protocol.
- When two stations try to access the network by send packets at the same time, the bit stream from each transmitting stations interferes or collides with each other, resulting in unreadable transmissions for both stations. This is controlled by a back-off algorithm that resets the transmission and allowing one station to have access of the frame transmission share. During this time all other stations are stopped. This is known as **Collision Detection** (5)**.**

2.3.3 Network Elements:

Local Area Networks that use the IEEE standard 802.3 using Ethernet encompass of network nodes and interconnecting media. These can be broadly categorized as two categories (5):

1. **Data terminal equipment (DTE):** Devices such as workstations, servers and printers that are often referred as end stations as they either are the source or destination of data frames.
2. **Data communication equipment (DCE):** Devices such as switches, repeaters, routers or even network interface cards that either receive or forward frames.

2.3.4 The first implementation:

The topology used to implement was a tree topology as that was considered feasible in terms of both cost and simplicity to implement. The characteristic of the layout was a locally distributed computer communication so that the assessments would be margin ably achievable. The size of the network was spread over a distance of 1 km cable length and using minicomputers for which 3Mbps was considered a convenient data transfer (6).

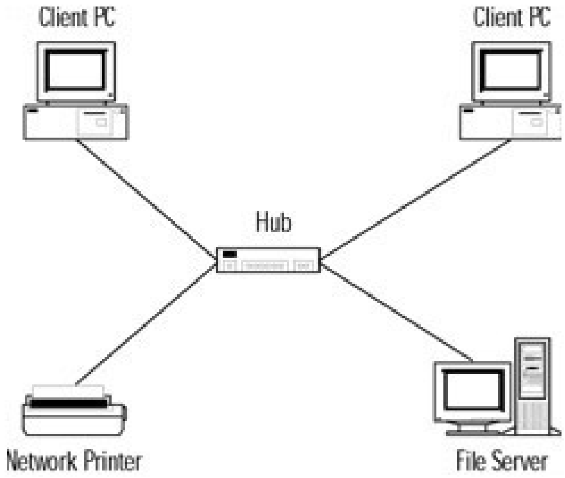
256 stations were involved in the experiment and to allow a rapid low level packet handling among these stations, the first 8-bit byte of the packet was made the destination address, whereas the second byte was made the source address field. 256 stations were chosen as all stations will receive their due share of the bandwidth (6).

2.3.5 Network Topologies:

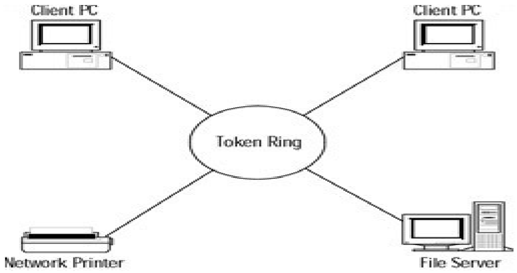
The way computers are connected together is known as a topology. It is very important to focus on topologies while designing a network. Factors like cost and reliability depend on the way we design our network topology (7).

Common types of typologies used are:

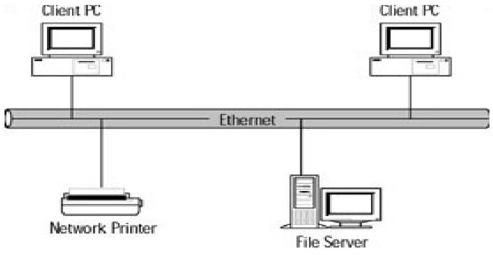
- Star: All stations are connected directly to a single central server or a switch (1, 7).



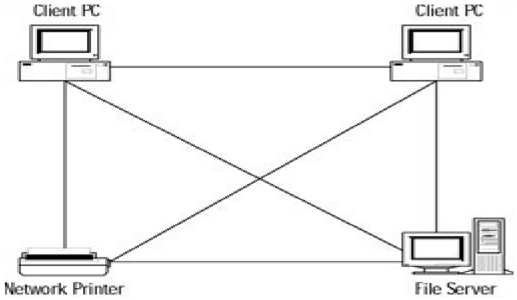
- Ring: All stations are connected in cascading order to make a ring. Each station passes information to the next until it reaches the destination station (1, 7).



- Bus: All Stations are connected to a single cable sharing the same media (1, 7).



- Mesh: Each Station is connected every station in the network (1, 7).



- Tree: Switches are used to connect workstations together. Each switch receives information from one workstation and repeats it to other workstation and switches (7).
- Hybrid: It is a combination of different topologies connected together (7).

2.3.6 Different Cables - Different Ethernet Standards:

The most popular conductive media used today is the Unshielded Twisted Pair (UTP), chiefly for being least expensive (8). With RJ-45 connectors coming with all network cards, UTP has gained popularity. Fiber optics is gaining popularity as well by providing commitment to bandwidth needs (8).

Table 1.1 below shows the different Ethernet cable standards (7).

Standard Ethernet – 10Mbps (7)	10Base5	The first Ethernet cable used – 70s
	10Base2	Coaxial cable, thinner than predecessor, computers connected in a segmented chain – 80s
	10BaseT	Unshielded twisted pair (UTP); lighter, more reliable – 90s
	10BaseFL	Used fiber optics, however

		newer versions of fiber optics exist, therefore rarely used.
Fast Ethernet – 100Mbps (7)	100BaseT4	UTP cable uses all four pair wires for max performance
	100BaseTX	UTP cable achieves results from only 2 pairs of wires, most used today in offices
	100BaseFX	Fiber optic version of Ethernet, most expensive in category.
Gigabit Ethernet – 1Gbps (7)	1000BaseT	Cat 5 UTP cable can run, however preferably 5e or 6.
	1000BaseLX	Uses fiber optic, most popular for Gigabit Ethernet.

2.4 Conclusion:

The infrastructure of the first wireless network was practically sound enough to have a derivation in to a wired LAN architecture that is currently used as the 802.3 standard by IEEE. The 802.3 standard can be used over a different range of wired physical media, where as the 802.11 using the wireless approach uses only space and light as a media. Later sections in the report will cover differences between the two in more detail.

3.0 LAN Performance

3.1 Introduction:

This section will encompass the performance concerns in each of the IEEE standards, 802.3 and 802.11 for wired and wireless LANs. In the performance section technical aspects will be seen of reaching the maximum data rates for both standards.

3.2 Wired Network Performance:

In any wired LAN scheme network performance degrades when the packet transmission time becomes small compared to the medium propagation delay at high speeds. LANs today are required to meet large amounts of data such as image processing with minimum delay. Enhanced data transfer rates and efficient medium access protocols are two key elements to meet increasing demands (9).

It is important for a LAN to operate at least as fast as the devices on it so that the buffering constraints are minimized (9). To provide a LAN frame work scheme that provides service to all devices including peripherals running on it to support speed coping with the incoming requests, the through put should not be degraded with congestion arising on nodes to be served. A solution provided for the best results should be scalable, inexpensive, simple and capable of delivering multimedia services. Best results for this can be achieved with a Passive Optical Network (PON) (10).

In a PON system, an optical Line Terminal (OLT) serves multiple Optical Network Units (ONUs) delivering multimedia services over a shared optical fibre infrastructure. Combining Ethernet to the PON, (EPON) is an efficient and economical architecture for an access network. A standard EPON system operates at data rates of up to 1 Gbit/s shared between 16 ONUs (10).

Fibre solution is predominately the best solution so far as even with a hybrid of a fibre and copper networks are susceptible to a variety of radio frequency impairments that can result in significant loss of packets during data communication. This degrades the Transmission control protocol in performance (11). TCP parameters can however be tuned to increase the network performance up to three folds without requiring any changes in subscribers PCs. These tuning parameters can be by changing and setting a TCP buffer size reducing the frequency and duration of timeouts or by reducing the effect of timeouts. When the socket buffer size increases the probability of timeouts decrease due to acknowledgements (ACK) losses, however a limit is imposed on the TCP socket setting (11).

The EPON network does not face any such problems and can be upgraded using the same equipment ensuring the media is supportive and keeping in consideration the 10GbE Standard by IEEE released in 2002 (10). EPON however has its drawbacks as well, with dispersion penalties become more severe especially in the downlink from the OLT to the ONU, since it operates on the 1490 nm window, with a fibre dispersion of around 17 ps/nm/km and the uplink being operated in the 1310 nm window, close to the zero depression wavelength. This however is the best solution with enhanced EPON even facing degradation problems (10).

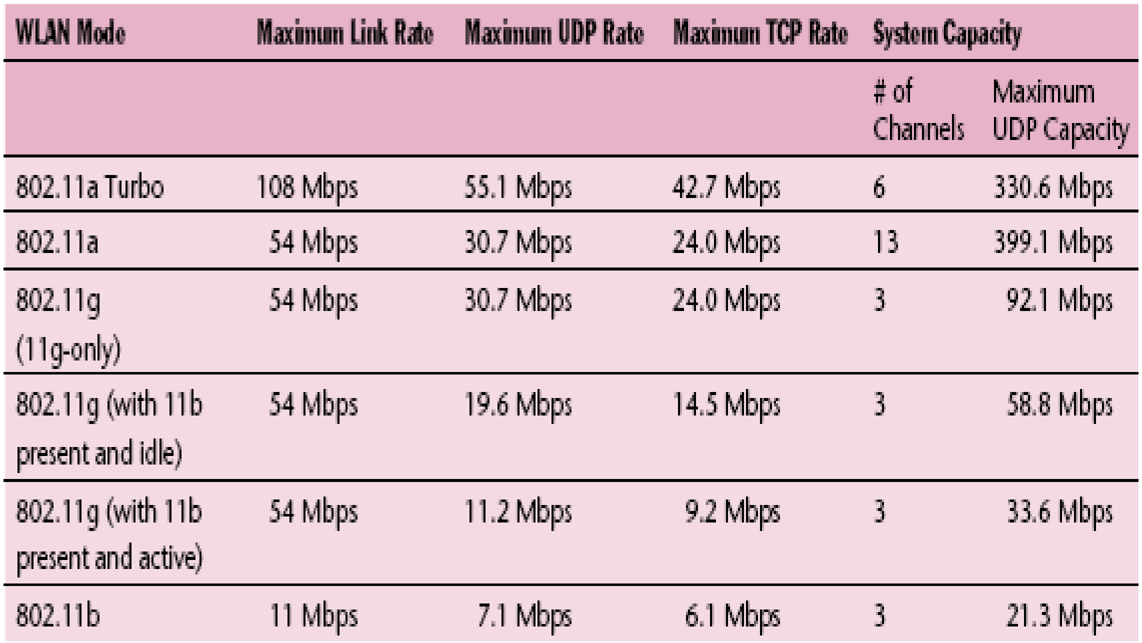
3.3 Wireless Network Performance:

The most common 802.11 standard used is the ‘g’ or ‘b’ with raw data rates of up to 54 Mbps and 11 Mbps, with each block of 8 input bits encoded in to 16 output data bits. These output data bits are transmitted two at a time using eight-quadrature phase shift keying (QPSK) symbols, each symbol being a period of time in which the phase of the carrier is at one of four discrete values. Say for 11 Mbps data stream, 22 Mbps are transmitted that are decoded at the receiver (12).

The four most important performance parameters of any wireless system are user throughput, total system capacity, range and power dissipation (12). Table 3.1 shows different rates by different 802.11 standards.

802.11 WLAN supports two kinds of network operation models: Infrastructure WLAN (IWLAN) and ad hoc WLAN. IWLAN uses the access point to bridge between the wired and wireless networks and optionally provides the polling function for time constrained services. It also uses the ISM band making it popular amongst operators. The bandwidth is spread into 14 partially overlapping channels, however using all channels to transmit data at the same location cause severe EMI that degrade the transmission quality, therefore to increase performance instead of the 83.5 MHz bandwidth designed by the ISM is remodelled by IEEE into 23 or 30 MHz guard bands between two overlapping WLANs (13).

Table 3.1 below shows the theoretical Maximum Throughput and System capacity of various 802.11 Standards (12)**:**



WLAN Mode	Maximum Link Rate	Maximum UDP Rate	Maximum TCP Rate	System Capacity	
				# of Channels	Maximum UDP Capacity
802.11a Turbo	108 Mbps	55.1 Mbps	42.7 Mbps	6	330.6 Mbps
802.11a	54 Mbps	30.7 Mbps	24.0 Mbps	13	399.1 Mbps
802.11g (11g-only)	54 Mbps	30.7 Mbps	24.0 Mbps	3	92.1 Mbps
802.11g (with 11b present and idle)	54 Mbps	19.6 Mbps	14.5 Mbps	3	58.8 Mbps
802.11g (with 11b present and active)	54 Mbps	11.2 Mbps	9.2 Mbps	3	33.6 Mbps
802.11b	11 Mbps	7.1 Mbps	6.1 Mbps	3	21.3 Mbps

If a real-time traffic is running it demands strict performance guarantee from the network. If a station is transmitting real-time multimedia to another station it would require maximum delay for data frames to be bound. For a performance level to be guaranteed to a station, the characteristics of the traffic generated by it should be known so that appropriate resources like transmission time can be allocated to it (14). To ensure this a connection is required by the performance guarantee requesting stations between the PC and the station. In order for this, stations are polled by the PC. The PC can also poll stations that have not ever established connections. For the support of real time services it is essential to determine the time instants when any given station that has established a connection with the PC to be polled. The PC should be provided with the ability to guarantee each connection request it accepts (14).

The TCP throughput depends polynomial on packet loss rate that renders TCP sensitive to spurious packet loss. The TCP congestion control may be desensitizied against random packet loss. The action of dynamic rate shifting, drastically degrades when subject to moderate multiple access contention and significantly diminish TCP throughput as pronounced collision, a form of congestion on the wireless segment in indoor environments dominate channel noise (15). This makes the DCF throughput degrade gracefully under increasing offered load and multiple access contention, but frames and jitter undergo a sudden phase transition at a critical offered load. In contrast to throughput the MAC layer and jitter can benefit from the traffic controls aimed at operating the system outside the saturation region (15).

Wireless internet access can be extend using the Wireless Mesh Networks as well using a number of fixed devices called mesh nodes that form a together a wireless adhoc network. A spatial TDMA (STDMA) approach can be used to maximise the bandwidth to uniformly share the resources among involved mesh nodes and to obtain measures. As global access rights are assigned by STDMA to mesh nodes for wireless channel usage, the scheduling of nodes need to be calculated for given mesh topologies. With results derived from an experiment (16), for every Access Method a worst case occurred for about 17 nodes where Raw Access produced on average an overhead of 37%, Wi-Fi Basic Access 41% and Wi-Fi RTS/CTS Access 44% considering bidirectional communication.

With results coming from another analytical model (17), a model-based frame scheduling scheme called MFS achieves a desirable throughput in WLANs. It operates by each node collecting a number of collisions that it encounters during its last inter-transmission interval and infers the number of currently active nodes. With the use of derived analytic model it then determines the current network utilization and computes delay that is artificially introduced to defer transmission of the current pending frame so as to avoid prospective collisions (17).

In a typical home network where one host has good wireless connectivity and the other has bad connectivity, experiments (18) can demonstrate that multiple 802.11g conversations sent through a common wireless access point (AP) cause channel contention that lowers effective throughput. When the wired network layer through put is higher than the effective capacity at the wireless link, the access point queues can severely lower performance for all flows transversing the AP due to increased queuing delay and buffer overflow.

3.4 Conclusion:

Performance in Wireless Technology may not be the same to that of wired networks, however it depends what kind of service is being requested over the network. Two wireless devices on a network may give better results depending on the way they are configured and the type of service requested as compared to wired devices on a network. It is important, whatever the technology medium is, the protocols involved should be compliant enough to handle at least as much data as being run over the network. If the technology is not properly configured for the selected media to run on it may not make any difference if the PC for examples are upgraded to improve productivity.

4.0 LAN Security:

4.1 Introduction:

In the security section it will be seen how secure the networks are in terms of privacy and how prone they each are to attacks. The type of networks mentioned will be the IEEE 802.11 for wireless LANs. Stress will be given on the Security aspects of WLANs as their presence can easily be detected and intruded upon if no prevention is adapted and the WLAN is kept unsecured. Unlike wired LANs that prone to attacks from within using vampire attacks on the cable supplying information.

4.2 WLAN Security:

Security for WLANs can be broken down in two categories; link layer encryption and system-level security mechanisms that manage the key distribution (12). In AP-based networks, it is important to consider the concept of authentication and association. Before a client communicates with an AP it should be authenticated first (either by open system or shared key mode) and then an association request must be sent (19). In an open system mode any one can associate itself leaving a large space for intruders, while in a shared key system it started with the Wired Equivalent Privacy (WEP) which had a lot of holes due to brute force attacks (12, 19) therefore an new shared key system was developed, WPA (also called the Temporal Key Exchange Protocol, TKIP), that scrambles the key between packets and adds a message integrity check to prevent spoofing. This was based on the Advanced Encryption and Data Encryption Standards, both capable of military strength integrity checks (12). This is much more complex and reliable than WEP where only a key was exchanged (19).

A wireless sensor kept open is easily detected and tempts an attack. Having limited energy and computational capabilities, it makes traditional security methodologies difficult or impossible to utilize allowing physical attacks such as jamming or node capture and tampering (20). If an application driven approach is adopted to protect the wireless sensors in a network it will make more reliable for the valid users, providing less opportunity for an intruder. The application should be immune to any illegal activity by adapting to learn injection of false packets, attacks on routing and DoS Attacks (20).

An autonomous wireless sensor network can be set up to perform sophisticated analysis of detecting trends and identifying unexpected, coherent and emergent behaviour (21). When such a system is deployed it primary goal is to provide in-situ users with secure high quality services, enhancing their situational and location awareness. It has local intelligence that decides what information is worth preserving rather taking the bulk of decisions elsewhere. Four types of attacks that can be encountered are; traffic analysis where the attacker knows there is activity on the network, Eavesdropping where the attacker monitors traffic determining the source and destination of the packet, Man-in-the-middle attack where a rogue intermediary is established fooling each side to be part of the transmission or a proxy server and tampering where the data is compromised (21). An autonomous sensor can even detect flooding of packets, exhaustion ad service degradation saving the network from a Denial of Service attack. All this good however for a small network as this solution relies on unique identifiers at the individual sensor level and such a controlled environment for a large scale use will be unrealistic (21).

For a large scale networks an ideal solution can be the use of virtual LANs (VLANs) (12). The use of hotspots and an access mechanism for visitors, users on a given WLAN can be given different privileges. 802.11 networks provide no built-in support for VLANs; however can be configured to work with them (12).

Another solution can be by bridging between an 802.11 base station and an authentication server in the network. Radius Servers are used for authentication servers (12).

To find vulnerabilities with in a network a wireless analyzer can be used to determine where the network may provide an opportunity for an attacker. These are portable devices that are very useful for trouble shooting both security and performance (22).

It is important to have cryptographic algorithms in a WLAN, which by 1998 were not proposed by IEEE (23) but were proposed by other researchers highlight its need mainly because a PC detecting APs may bring up a list of all available in the range, hence raising privacy concerns that may lead to integrity or even availability of data.

It is important to have approximate authentication in WLANs that are involved especially in video streaming (24). This will distinguish forged packets from packets that have natural bit error and even to prevent error resilient video decoding to work on heavily damaged packets. In both cases the maximum number of bit errors that the receiving network interface tolerates should be limited. By using approximate authentication this limit can be set up (24).

Encryption is very essential to be applied within a wireless network even if it the WEP. Considerations should be taken not to broadcast the SSID of the wireless network, as even if the name of the WAP network is broadcasted to the entire neighbourhood any passerby can find and achieve the status (25).

SSID should be kept in the closed mode while using WAP so that it is no visible to all. A closed WAP will not respond unless the probe requests contain its SSID, therefore it must be known in advance (26). For an active intruder using Kismet or AirMagnet as tools may detect closed SSID as well as they detect all wireless activities, however it is still a preventive measure (26).

4.3 Conclusion:

Ever since 1998 developments are made to upgrade security in a wireless LAN. Need for improving in security arose when the use grew wider and the equipment to use a wireless network became very common. For a determined intruder there is never enough security, however the advanced and data encryption standards will keep the confidentiality of the content secure probably even if it is intercepted. Traffic analysis and eavesdropping are still factors that need to be considered that require due consideration to protect against. Probably if a frequency converter is used by the transmitting end and then converted back at the receiving end, traffic would be saved from being monitored as the frequency will be different on which transmission is taking place, while an intruder will be busy listening on 2.4GHz frequency that is assigned for say if using 802.11g.

5.0 Wired Vs Wireless Network Architecture:

5.1 Introduction:

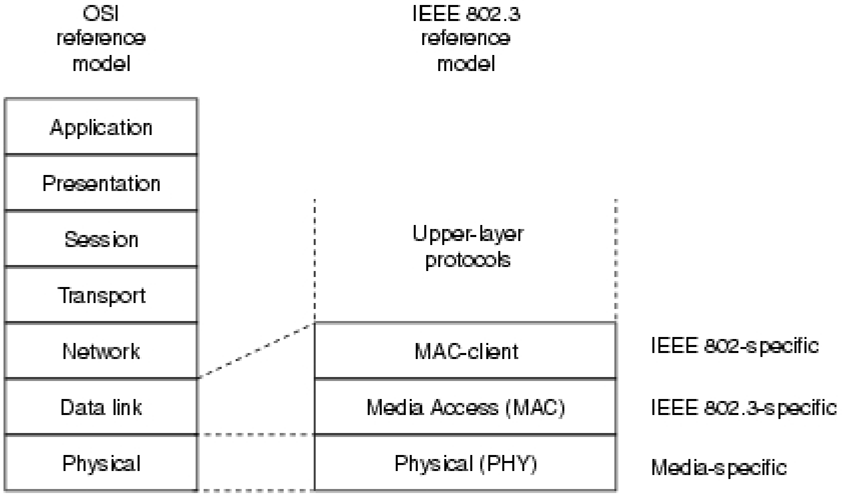
Even though the Ethernet is a derivation of the first wireless network, however the 802.11 architecture is adapted from the 802.3 architecture, both based on the OSI architecture. The main difference in both standards is mainly in the data link layer and the data frame sent over the network. Both standards are interoperable with each other and are configured to supply data from sender to receiver end with minimum delay, error rate and congestion on the available routes. Within this chapter the 802.11 architecture will be looked into compared with the OSI model as well as the 802.3 that was briefly mentioned in the second chapter earlier.

5.2 Ethernet Architecture In relation to ISO Reference Model:

The IEEE physical layer corresponds with the OSI physical layer, however at the data link layer it follows the IEEE 802 data link layer specifications where the data link layer comprises of the Media Access Control (MAC) sub-layer and the MAC-client sub-layer (5). See Fig 5.1 for diagrammatic description.

If there is a DTE unit, the MAC-client sub-layer provides an interface between the Ethernet MAC and the layers above in the protocol stack. If there is a DCE unit, like a bridge perhaps then it provides a LAN-to-LAN interface between LANs that both use the same protocols or even different (like Ethernet-token ring (5).

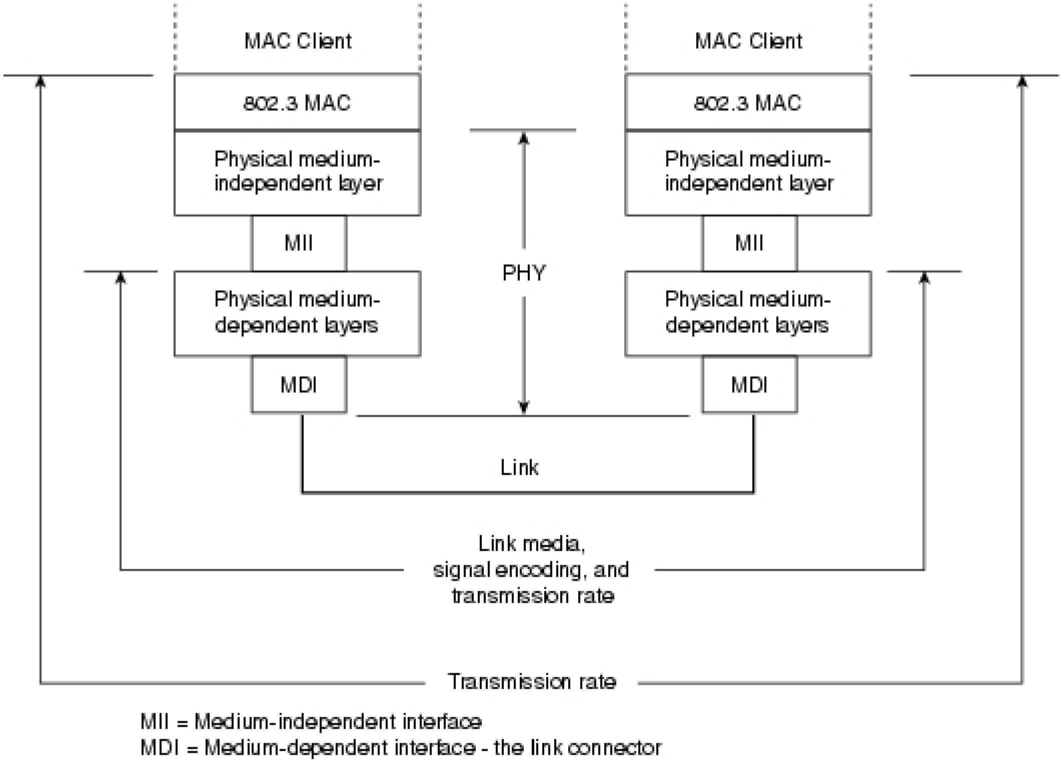
Figure 5.1 below shows the Ethernet logical relationship to ISO Reference Model (5).



The specifications for the logical link layer within the data link layer are common for all IEEE 802 LAN protocols; hence network compatibility becomes the primary responsibility of the particular network protocol (5).

The Mac layer controls the node's access to the network media specific to the individual protocol. The logical requirements should be met by all IEEE 802.3 MACs regardless whether they include one or more of the defined optional protocol extensions. For any two MACs to carry basic communication, the same transmission rate must be supported between both ends (5). See Figure 5.2 for diagrammatic description.

Figure 5.2 below shows the MAC and Physical Compatibility Requirements for basic Data Communication (5).

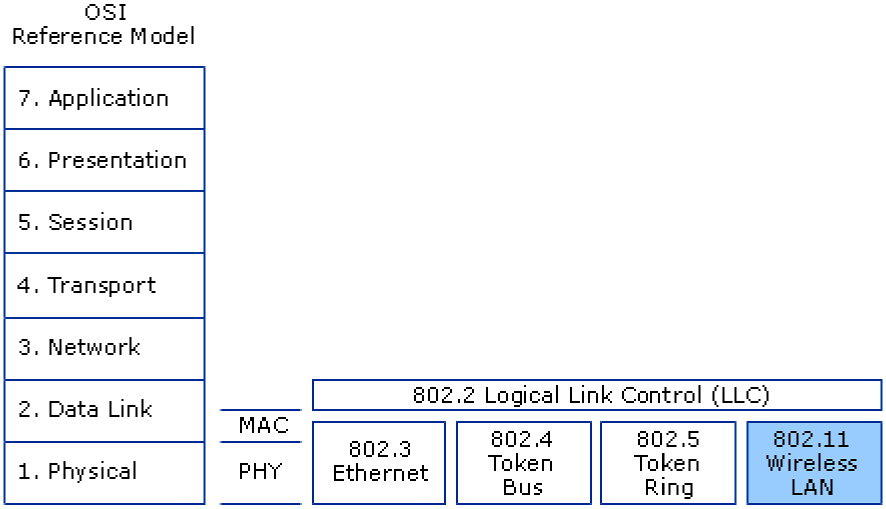

MAC Client
MAC Client
802.3 MAC
802.3 MAC
Physical medium-independent layer
Physical medium-independent layer
MII
MII
PHY
Physical medium-dependent layers
Physical medium-dependent layers
MDI
MDI
Link
Link media, signal encoding, and transmission rate
Transmission rate
MII = Medium-independent interface
MDI = Medium-dependent interface - the link connector

The transmission rate, the data signal encoding and the type of media interconnecting the two nodes should be specific to the 802.3 physical layers. Say, when using the Gigabit Ethernet, that can operate both on twisted pair and optical fiber cable, then each specific type of cable or signal encoding procedure requires a different physical layer implementation (5).

5.3 Wi-Fi Architecture In relation to ISO Reference Model:

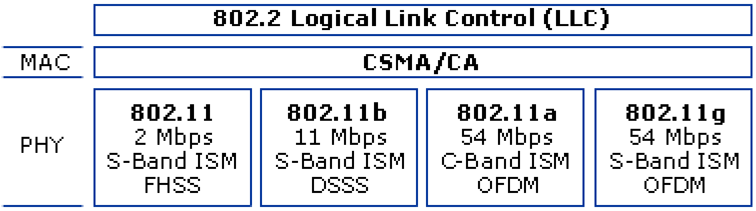
The physical and media access control (MAC) layers are defined by the 802.11 wireless standard by IEEE for communication over the network. At the Physical layer there are number of schemes adopted to define a series of encoding and transmission schemes for wireless communication (27).

The figure 5.3 below shows the physical and MAC layer specifications defined by 802.11 that communicate up to the LLC layer (27).



Among these schemes are the Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM) transmission schemes (27). Both FHSS and DSSS run at 1 and 2 Mbit/s in the 2.4 GHz band (28). OFDM is one the transmission schemes being very successful even in WAN technologies like WIMAX as it uses a large number of close spaced carriers that are modulated with low rate data, and with the signals being orthogonal there is interference contribution (29).

The figure 5.4 below shows the 802.11 standards that exist at the PHY sub layer (27):


802.2 Logical Link Control (LLC)
MAC
CSMA/CA
PHY
802.11 2 Mbps S-Band ISM FHSS
802.11b 11 Mbps S-Band ISM DSSS
802.11a 54 Mbps C-Band ISM OFDM
802.11g 54 Mbps S-Band ISM OFDM

Issues faced by the physical layer are that the performance deteriorates under outdoor channel conditions and powering hotspots in a remote area would be troublesome. Wi-Fi even with its poor spectral efficiency improvement is more attractive than other available options due to providing connectivity at low costs (30).

At the MAC layer 802.11 defines two different access methods, the Distributed Coordinated Function with the basic access method being Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism and the Point Coordination Function (28). In order to reduce the probability of two stations colliding because they are cannot hear each other the standard defines a Virtual Carrier Sense mechanism in which a station wanting to send sends a request to send RTS packet over the network. The packet with most seniority is honoured (28).

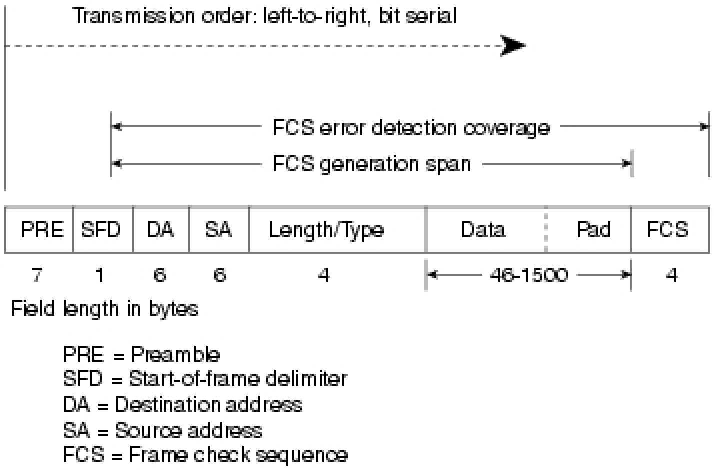
The MAC layer of the 802.11 is responsible for fragmenting and reassembling packets sent over the network. The size of packets handled is small. In a typical LAN the Ethernet packet is very long (up to 1518 bytes) which has its disadvantages of higher Bit Error Rate. When the packet is small the probability of a packet being corrupted is reduced, the less overhead is caused due to retransmission, in a Frequency Hopping System the smaller the packet, the less the chance there is that the transmission will be postponed after the dwell time (28).

There are however issues with the MAC layer of the 802.11 mainly for long distance links, routing and re-configurability. The value used for the acknowledgement ACK timeout is too small (default slot time value 20µs) to work over long-distance links therefore keeping it designed for a small number of people sharing a channel in an indoor setting (30).

5.4 Ethernet MAC Frame Format:

The Ethernet frame is basic and defined for all MAC implementations. The basic frame consists of 7 fields (figure 5.5); however several additional optional formats can be defined to extend the protocols basic compatibility (5).

The figure 5.5 below shows the basic IEEE 802.3 MAC Data Frame Format (5):



- **Preamble (PRE)** -7 bytes. The PRE is an alternating pattern in binary telling the receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream (5).
- **Start-of-frame delimiter (SOF) -** 1 byte. The SOF is an alternating pattern in binary, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address (5).
- **Destination address (DA)** - 6 bytes. The DA field identifies which station(s) should receive the frame. The left-most bit in the DA field indicates whether the address is an individual address (indicated by a 0) or a group address (indicated by a 1). The second bit from the left indicates whether the DA is globally administered (indicated by a 0) or locally administered (indicated by a 1). The remaining 46 bits are a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network (5).
- **Source addresses (SA)** - 6 bytes. Identifies the sending station. The SA is always an individual address and the left-most bit in the SA field is always 0 (5).
- **Length/Type** - 2 bytes. This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format. If the Length/Type field value is less than or equal to 1500, the number of LLC bytes in the Data field is equal to the Length/Type field value. If the Length/Type field value is greater than 1536, the

frame is an optional type frame, and the Length/Type field value identifies the particular type of frame being sent or received (5).

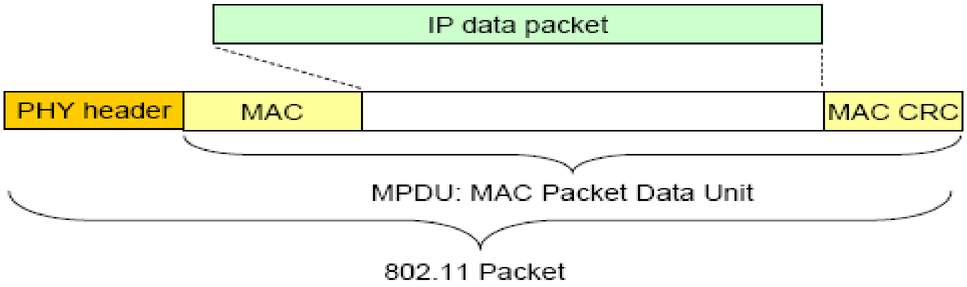
- **Data** - Is a sequence of *n* bytes of any value, where *n* is less than or equal to 1500. If the length of the Data field is less than 46, the Data field must be extended by adding a filler (a pad) sufficient to bring the Data field length to 46 bytes (5).
- **Frame check sequence (FCS)** - 4 bytes. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames. The FCS is generated over the DA, SA, Length/Type, and Data fields (5).

5.5 MAC Frame format for 802.11:

The 802.11 MAC frame (figure 5.6), consists of a MAC header, the frame body, and a frame check sequence (FCS). The Frame Control field contains control information used to define the type of 802.11 MAC frame and provide information necessary for the following fields to understand how the MAC frame processed (27).

When the packet is assembling, the payload data from the IP layer or the data that is being communicated is encapsulated with MAC data and the four byte segment of data that functions as a check sum referred to as CRC or FCS. This data is assembled in to the MAC Packet Data Unit (MPDU). The synchronisation header is appended by the PHY layer as the packet is transmitted (31).

The figure 5.6 below shows the 802.11 packet encapsulation (31).



Components of the Frame (figure 5.7)**:**

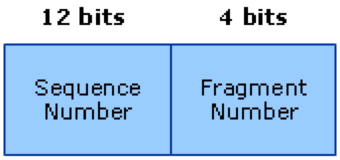
The Frame Control field: contains data of the protocol version of the 802.11 standards, the function of the frame, whether the frame is going to the existing distributed system, more fragments are following, the frame is retransmitted, the encryption supported by it and information for all frames to be processed in order (27).

Duration/ID Field: This field is used for all control type frames, except with the subtype of Power Save (PS) Poll, to indicate the remaining duration needed to receive the next frame transmission. When the sub-type is PS Poll, the field contains the association identity (AID) of the transmitting STA (27).

Address Fields: Depending upon the frame type, the four address fields will contain a combination of the following address types (27):

Sequence Control: The Sequence Control field contains two subfields, the Fragment Number field and the Sequence Number field, indicating the sequence number and the number of each frame sent over the fragmented frame (27).

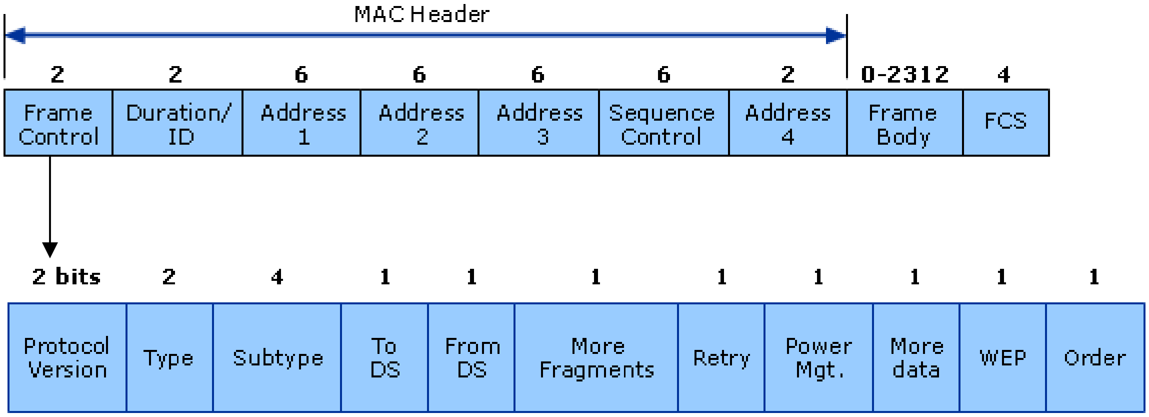
Sequence Control Field



Frame Body: The frame body contains the data or information included in either management type or data type frames (27).

Frame Check Sequence: The transmitting STA uses a cyclic redundancy check (CRC) over all the fields of the MAC header and the frame body field to generate the FCS value. The receiving STA then uses the same CRC calculation to determine its own value of the FCS field to verify whether or not any errors occurred in the frame during the transmission (27).

The figure 5.7 below shows the MAC frame format for 802.11 expanding the Frame Control Field. Numbers represent bytes (27).



5.6 Conclusion:

The mechanisms used by both Ethernet and Wi-Fi are almost the same to access the network through the MAC layers, there are however some adjustments made in the MAC frame for 802.11 that makes it different bringing disadvantages of both speed and retransmissions handling. The implementation for the physical layer is also different as Ethernet uses a physical medium of either twisted pair (copper wires) or fibre optics, where as space or light is used by 802.11 as a medium for communication. There are limitations found due to lack of power efficiency in 802.11 compared to 802.3, however the packet size in 802.11 is smaller therefore efficiency is brought in with fewer retransmissions due to less error rate and corrupted traffic. Considerations can be brought in, probably improving signal strength with less power consumptions capabilities to upgrade 802.11 to a level better than the one which requires guided media.

6.0 Implementation:

6.1 Introduction:

This section will focus on to find differences through testing both LAN and WLAN in same conditions. There will be a simple each LAN and WLAN established comprising of two laptops communicating between each other through a router (See A1.0 in the Appendix section for further details on hardware and software used during testing both IEEE standards). The findings gathered by previous researches will act as post-positivists claims for developing knowledge to carry out the research. Observations will be made every time the technologies are tested with a different test case. These test observations will be recorded and be commented upon through evaluations. Test cases will be based on performance both on the network and connection to the internet. There will be a test case to find the vulnerabilities found in each network standard.

6.2 Test Plan:

There will be a software based testing, when the test LAN and WLAN using IEEE 802.3 and 802.11b/g will be used. The IEEE standard 802.3 will be tested first by testing the software first with the LAN card enabled whereas the Wireless LAN adapter disabled and vice versa when testing the IEEE 802.11 standard. Screen shots will be captured and documented to show the differences between the two standards. The WLAN will be enabled with WPA encrypted authentication, which is the highest level of encryption available. The purpose of having this encryption in the test network is that there is no point testing the unsecured network. The main reason for it is that it is no longer used even by people with little knowledge of securing the network. WEP encryption is also avoided as it is a low level encryption and a test should be provided in the most secure environment.

6.3 Test Findings:

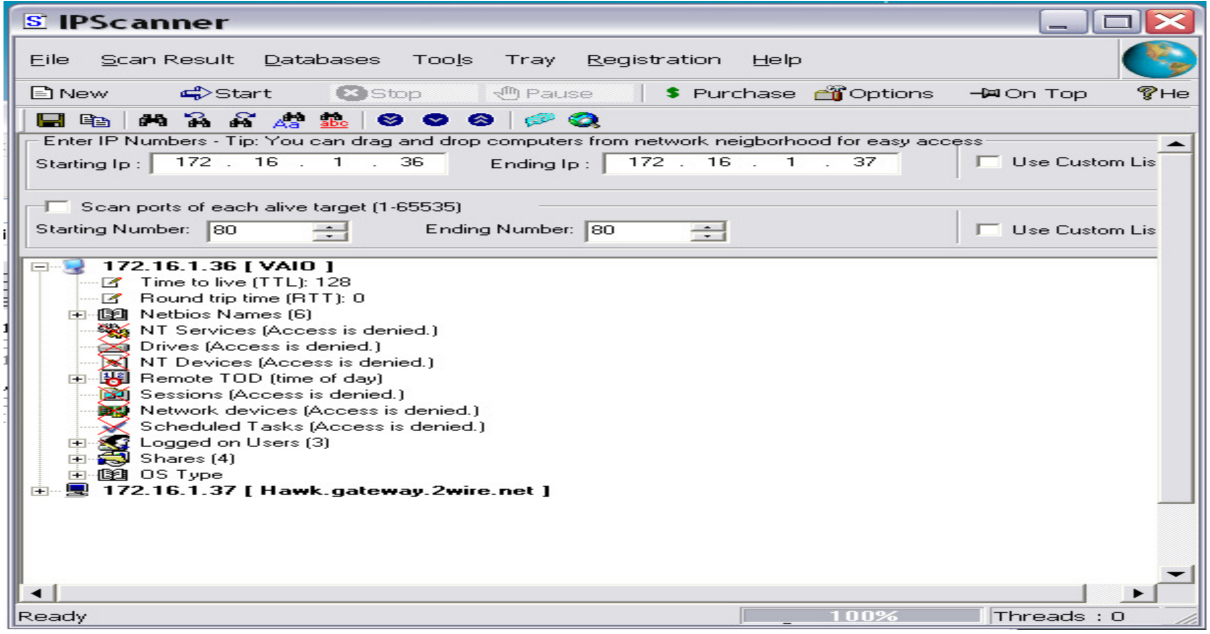
6.3.1 Round-Trip Time Findings:

The first test was conducted on both LAN and WLAN to check the performance of the technologies with the test network setup, under same conditions. The purpose of this test was to check how long it takes for a packet to reach from computer to another in a network or the Round Trip Time (RTT). To observe this software called IPScanner was used. After the software was run the RTT for LAN was recorded as 0 seconds, hence the time it took for the packet to reach the destination was less than 1 second; however when the IPscanner run over a wireless network the RTT was recorded as 5 seconds. This proves the wired LAN is at least 5 times more performing than a wireless LAN.

See Picture Set 6.1 for Screen Shots of the test.

Picture Set 6.1 below shows the IPscanner returning the RTT for both test runs.

IP Scanner through Ethernet:



Enter IP Numbers - Tip: You can drag and drop computers from network neigborhood for easy access

Starting Ip : 172 . 16 . 1 . 36 Ending Ip : 172 . 16 . 1 . 37 □ Use Custom Lis

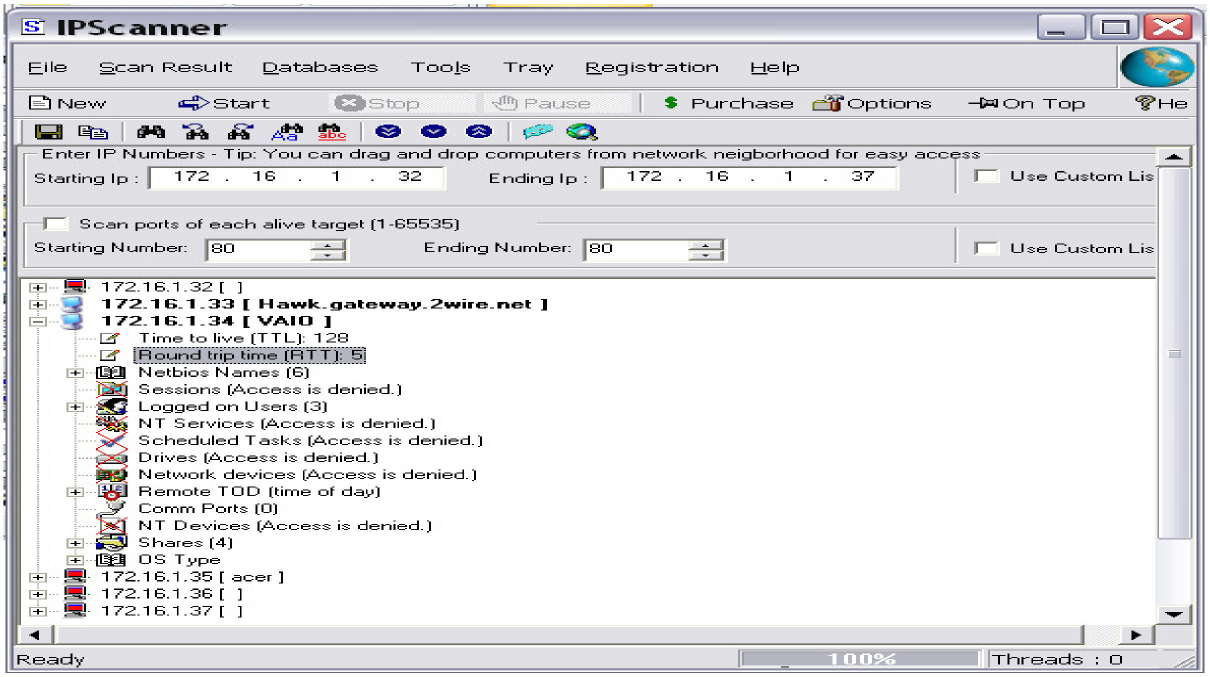
□ Scan ports of each alive target (1-65535)

Starting Number: 80 Ending Number: 80 □ Use Custom Lis

```
172.16.1.36 [ VAIO ]
    Time to live (TTL): 128
    Round trip time (RTT): 0
    Netbios Names (6)
    NT Services (Access is denied.)
    Drives (Access is denied.)
    NT Devices (Access is denied.)
    Remote TOD (time of day)
    Sessions (Access is denied.)
    Network devices (Access is denied.)
    Scheduled Tasks (Access is denied.)
    Logged on Users (3)
    Shares (4)
    OS Type
172.16.1.37 [ Hawk.gateway.2wire.net ]
```

Ready 100% Threads : 0

IP scanner through Wi-Fi



Enter IP Numbers - Tip: You can drag and drop computers from network neigborhood for easy access

Starting Ip : 172 . 16 . 1 . 32 Ending Ip : 172 . 16 . 1 . 37 □ Use Custom Lis

□ Scan ports of each alive target (1-65535)

Starting Number: 80 Ending Number: 80 □ Use Custom Lis

```
172.16.1.32 [ ]
172.16.1.33 [ Hawk.gateway.2wire.net ]
172.16.1.34 [ VAIO ]
    Time to live (TTL): 128
    Round trip time (RTT): 5
    Netbios Names (6)
    Sessions (Access is denied.)
    Logged on Users (3)
    NT Services (Access is denied.)
    Scheduled Tasks (Access is denied.)
    Drives (Access is denied.)
    Network devices (Access is denied.)
    Remote TOD (time of day)
    Comm Ports (0)
    NT Devices (Access is denied.)
    Shares (4)
    OS Type
172.16.1.35 [ acer ]
172.16.1.36 [ ]
172.16.1.37 [ ]
```

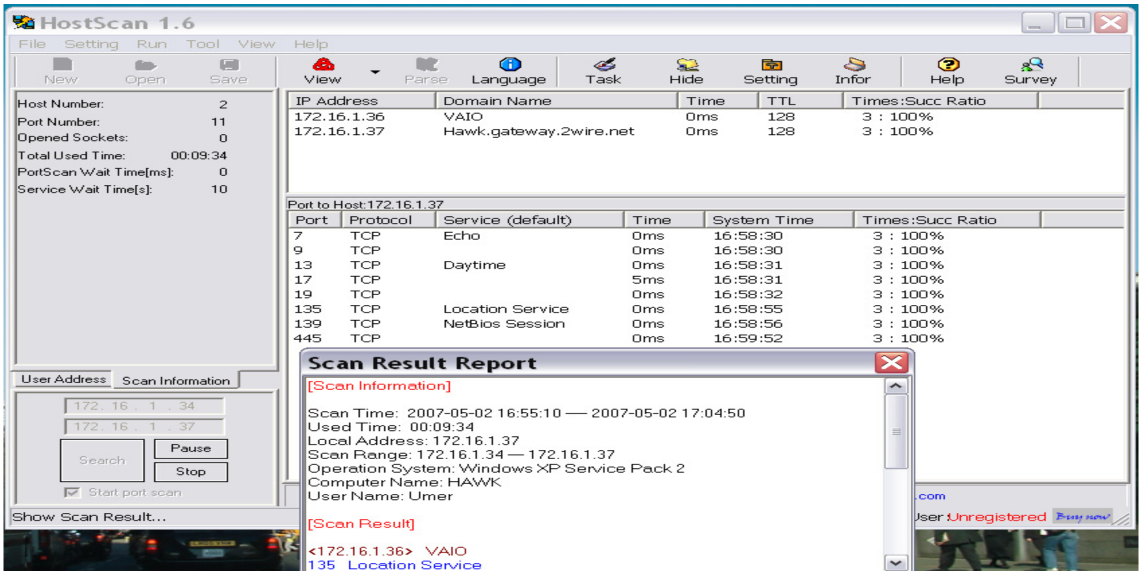
Ready 100% Threads : 0

6.3.2 Port Scan Findings:

The purpose of this test is to find how long it takes to scan for a range of ports on hosts connected on a network in a specific IP range. The software used in the test run was HostScan. As there were two laptops and there were limited ports selected, it scanned the two hosts on the network finding 11 ports open on the network. The time taken by Ethernet was 9 minutes and 34 seconds, while it took 9 minutes and 38 seconds for the Wireless network to scan the 11 open ports. See Picture Set 6.2 for Screen Shots of the test.

Picture Set 6.2 below show HostScan Findings for Port Scan.

Hot scan through Ethernet:


HostScan 1.6
File Setting Run Tool View Help
New Open Save View Parse Language Task Hide Setting Infor Help Survey
User Address Scan Information
Pause
Stop
Search
Start port scan
Show Scan Result...
.com
Jser :Unregistered Buy now

```
Host Number:                2
Port Number:               11
Opened Sockets:             0
Total Used Time:     00:09:34
PortScan Wait Time[ms]:     0
Service Wait Time[s]:      10

172. 16 . 1 . 34
172. 16 . 1 . 37
```

IP Address	Domain Name	Time	TTL	Times:Succ Ratio
172.16.1.36	VAIO	0ms	128	3 : 100%
172.16.1.37	Hawk.gateway.2wire.net	0ms	128	3 : 100%

Port to Host:172.16.1.37

Port	Protocol	Service (default)	Time	System Time	Times:Succ Ratio
7	TCP	Echo	0ms	16:58:30	3 : 100%
9	TCP		0ms	16:58:30	3 : 100%
13	TCP	Daytime	0ms	16:58:31	3 : 100%
17	TCP		5ms	16:58:31	3 : 100%
19	TCP		0ms	16:58:32	3 : 100%
135	TCP	Location Service	0ms	16:58:55	3 : 100%
139	TCP	NetBios Session	0ms	16:58:56	3 : 100%
445	TCP		0ms	16:59:52	3 : 100%

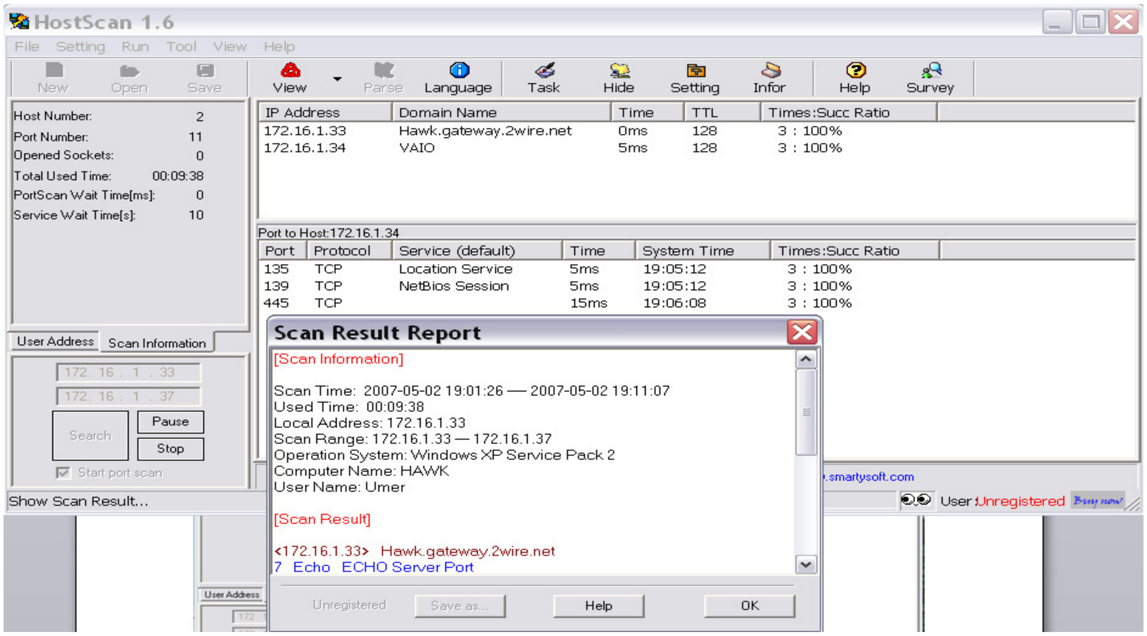
```
Scan Result Report
[Scan Information]

Scan Time:  2007-05-02 16:55:10 —— 2007-05-02 17:04:50
Used Time:  00:09:34
Local Address: 172.16.1.37
Scan Range: 172.16.1.34 — 172.16.1.37
Operation System: Windows XP Service Pack 2
Computer Name: HAWK
User Name: Umer

[Scan Result]

<172.16.1.36>  VAIO
135  Location Service
```

Hot Scan through Wi-Fi:


HostScan 1.6
File Setting Run Tool View Help
New Open Save View Parse Language Task Hide Setting Infor Help Survey
User Address Scan Information
172 . 16 . 1 . 33
172 . 16 . 1 . 37
Search Pause Stop
Start port scan
Show Scan Result...
.smartysoft.com
User :Unregistered Buy now
Unregistered Save as... Help OK

Host Number: 2
Port Number: 11
Opened Sockets: 0
Total Used Time: 00:09:38
PortScan Wait Time[ms]: 0
Service Wait Time[s]: 10

IP Address	Domain Name	Time	TTL	Times:Succ Ratio
172.16.1.33	Hawk.gateway.2wire.net	0ms	128	3 : 100%
172.16.1.34	VAIO	5ms	128	3 : 100%

Port to Host:172.16.1.34

Port	Protocol	Service (default)	Time	System Time	Times:Succ Ratio
135	TCP	Location Service	5ms	19:05:12	3 : 100%
139	TCP	NetBios Session	5ms	19:05:12	3 : 100%
445	TCP		15ms	19:06:08	3 : 100%

Scan Result Report

[Scan Information]

Scan Time: 2007-05-02 19:01:26 — 2007-05-02 19:11:07
Used Time: 00:09:38
Local Address: 172.16.1.33
Scan Range: 172.16.1.33 — 172.16.1.37
Operation System: Windows XP Service Pack 2
Computer Name: HAWK
User Name: Umer

[Scan Result]

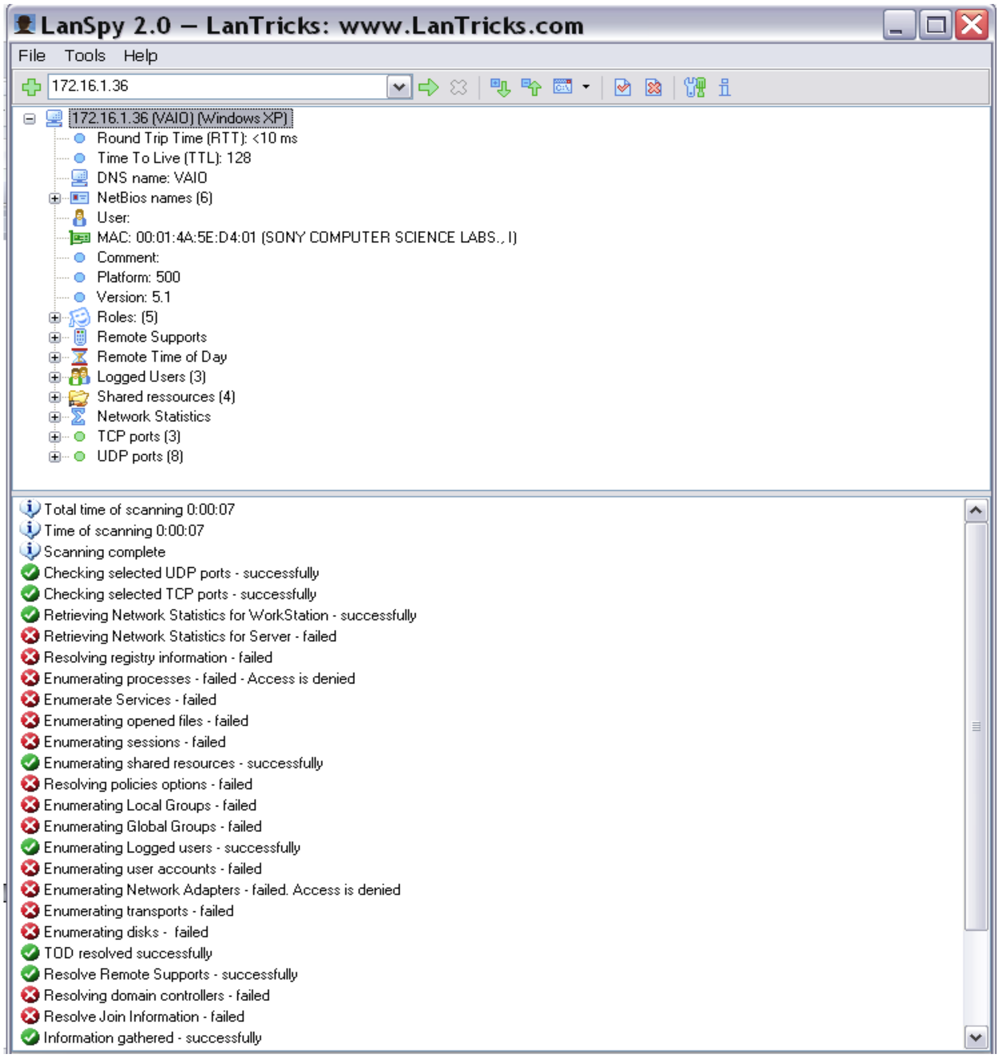
<172.16.1.33> Hawk.gateway.2wire.net
7 Echo ECHO Server Port

6.3.3 Remote Host Scan Findings:

The purpose of this test is to scan for services running on remote hosts on a local network. The software used to test this was LanSpy version 2.0. Services running on the remote host were shown in a given time T seconds for both the wired LANs and WLANs. The RTT on both runs was less than 10 seconds, however when it took 7 seconds for Ethernet to complete the scan, it took 1 minute and 56 seconds. The advantage scanning through the wireless network was only one that it scanned for 9 UDP services running on the remote host whereas Ethernet only exposed 8 UDP services running on the remote host. See Picture Set 6.3 for Screen Shots of the test.

Picture Set 6.3 below shows the time taken by LanSpy to scan for services on the remote host.

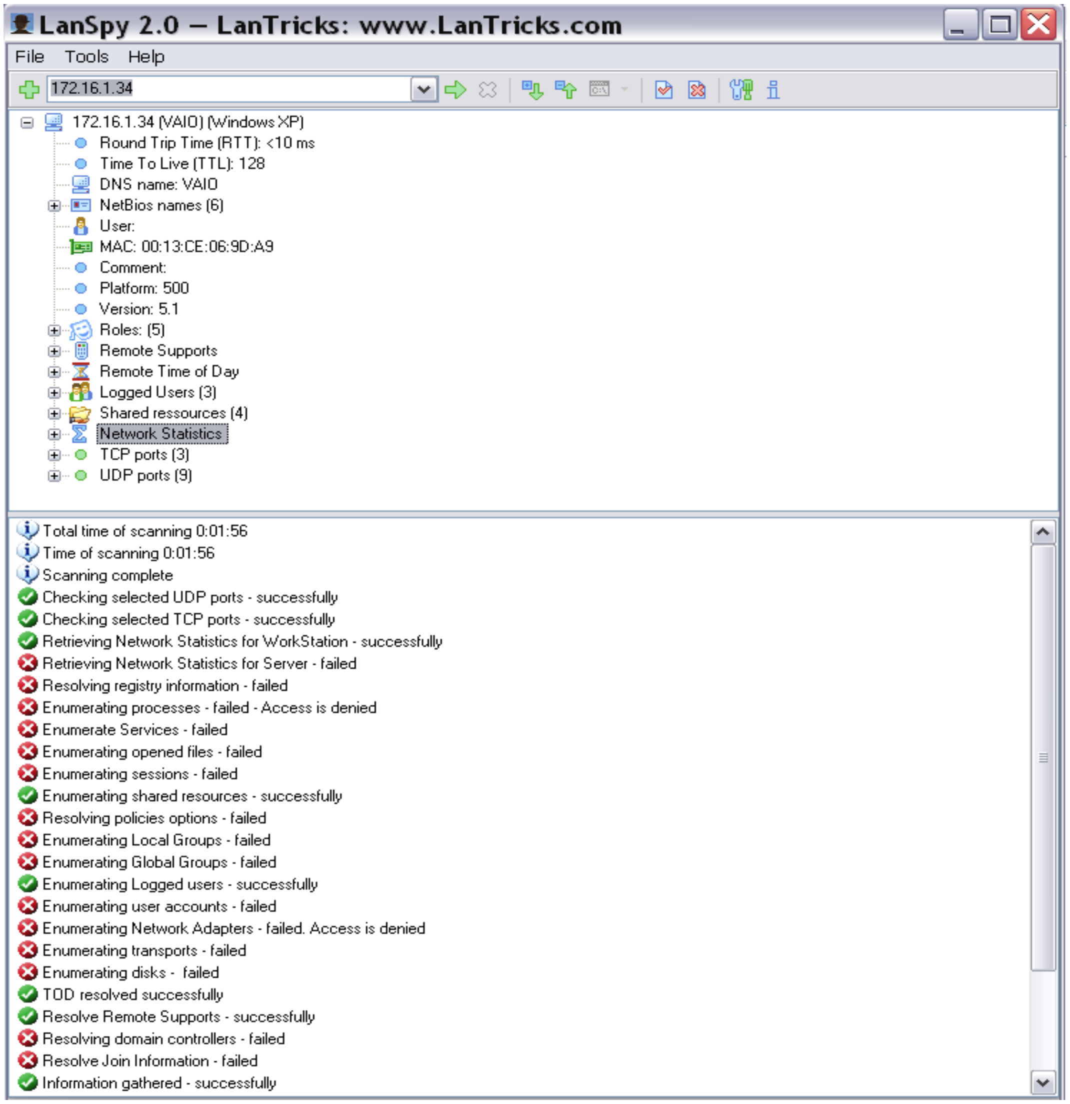
LanSpy on Ethernet:



```
172.16.1.36 (VAIO) (Windows XP)
    Round Trip Time (RTT): <10 ms
    Time To Live (TTL): 128
    DNS name: VAIO
    NetBios names (6)
    User:
    MAC: 00:01:4A:5E:D4:01 (SONY COMPUTER SCIENCE LABS., I)
    Comment:
    Platform: 500
    Version: 5.1
    Roles: (5)
    Remote Supports
    Remote Time of Day
    Logged Users (3)
    Shared ressources (4)
    Network Statistics
    TCP ports (3)
    UDP ports (8)
```

```
Total time of scanning 0:00:07
Time of scanning 0:00:07
Scanning complete
Checking selected UDP ports - successfully
Checking selected TCP ports - successfully
Retrieving Network Statistics for WorkStation - successfully
Retrieving Network Statistics for Server - failed
Resolving registry information - failed
Enumerating processes - failed - Access is denied
Enumerate Services - failed
Enumerating opened files - failed
Enumerating sessions - failed
Enumerating shared resources - successfully
Resolving policies options - failed
Enumerating Local Groups - failed
Enumerating Global Groups - failed
Enumerating Logged users - successfully
Enumerating user accounts - failed
Enumerating Network Adapters - failed. Access is denied
Enumerating transports - failed
Enumerating disks -  failed
TOD resolved successfully
Resolve Remote Supports - successfully
Resolving domain controllers - failed
Resolve Join Information - failed
Information gathered - successfully
```

LanSpy on Wi-Fi:



```
172.16.1.34 (VAIO) (Windows XP)
    Round Trip Time (RTT): <10 ms
    Time To Live (TTL): 128
    DNS name: VAIO
    NetBios names (6)
    User:
    MAC: 00:13:CE:06:9D:A9
    Comment:
    Platform: 500
    Version: 5.1
    Roles: (5)
    Remote Supports
    Remote Time of Day
    Logged Users (3)
    Shared ressources (4)
    Network Statistics
    TCP ports (3)
    UDP ports (9)
```

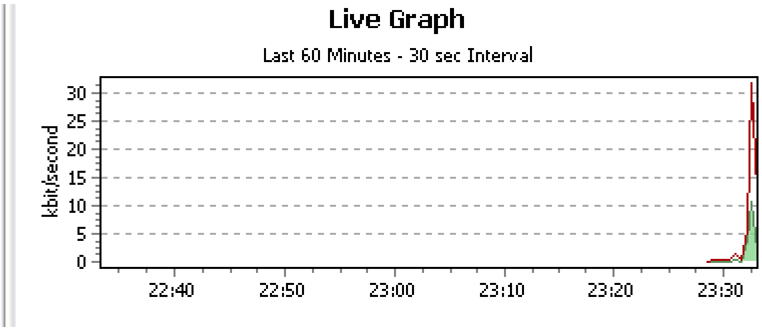
```
Total time of scanning 0:01:56
Time of scanning 0:01:56
Scanning complete
✓ Checking selected UDP ports - successfully
✓ Checking selected TCP ports - successfully
✓ Retrieving Network Statistics for WorkStation - successfully
✗ Retrieving Network Statistics for Server - failed
✗ Resolving registry information - failed
✗ Enumerating processes - failed - Access is denied
✗ Enumerate Services - failed
✗ Enumerating opened files - failed
✗ Enumerating sessions - failed
✓ Enumerating shared resources - successfully
✗ Resolving policies options - failed
✗ Enumerating Local Groups - failed
✗ Enumerating Global Groups - failed
✓ Enumerating Logged users - successfully
✗ Enumerating user accounts - failed
✗ Enumerating Network Adapters - failed. Access is denied
✗ Enumerating transports - failed
✗ Enumerating disks -  failed
✓ TOD resolved successfully
✓ Resolve Remote Supports - successfully
✗ Resolving domain controllers - failed
✗ Resolve Join Information - failed
✓ Information gathered - successfully
```

6.3.4 Internet Traffic Flow Findings:

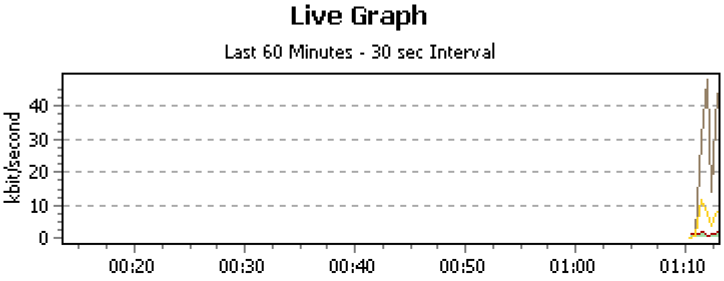
This test was run to show the difference between the internet traffic flows with both network standards. The software used to test run was PRTG Traffic Grapher version 5.0. With the help of this software we can determine the number of bytes received and the number sent in a given time T while using an internet browser of casual surfing like checking a web based email account. While using Ethernet in 3 minutes the number there were over 30 Kbit/s received while the number of bytes sent were a little over 10 Kbits/s. When the wireless adapter was used for same browsing in the same time, maximum number of bits received was 40 Kbits/s against a little over 10 Kbits/s that were sent. See Picture Set 6.4 for Screen Shots of the test.

Picture Set 6.4 below shows the graphs plotted show the bit rate against time.

PRTG Traffic Grapher on Ethernet:



PRTG Traffic Grapher on Wi-Fi:

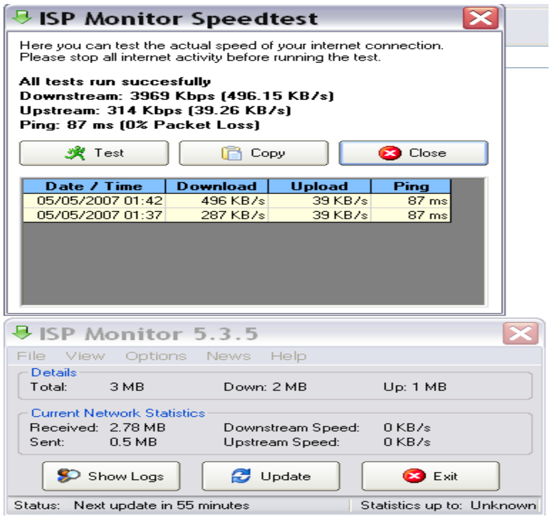


6.3.5 ISP Performance Findings:

The purpose of this test is to carry find out the difference between the two network standards while using internet from a service provider. The software uses mechanisms like pinging websites to note the uptime and downtime for the ISP connection. In both instances the ping was for 87ms with 0% packet loss. When the connection was tested running on Ethernet card, the upstream came as 314 Kbps while the downstream came as 3969 Kbps. When the computer wirelessly connected to the same ISP, the upstream connection was recorded as 309 Kbps while the downstream was 2296 Kbps. Therefore again proving that Ethernet transmits more than Wi-Fi even when the data sent and received is in the controlled bandwidth that can easily be supported by each network standard. See Picture Set 6.5 for Screen Shots of the test.

Picture Set 6.5 below show ISP testing ISP Performance for both Networks:

ISP Monitor on Ethernet:



Here you can test the actual speed of your internet connection.
Please stop all internet activity before running the test.

All tests run succesfully
Downstream: 3969 Kbps (496.15 KB/s)
Upstream: 314 Kbps (39.26 KB/s)
Ping: 87 ms (0% Packet Loss)

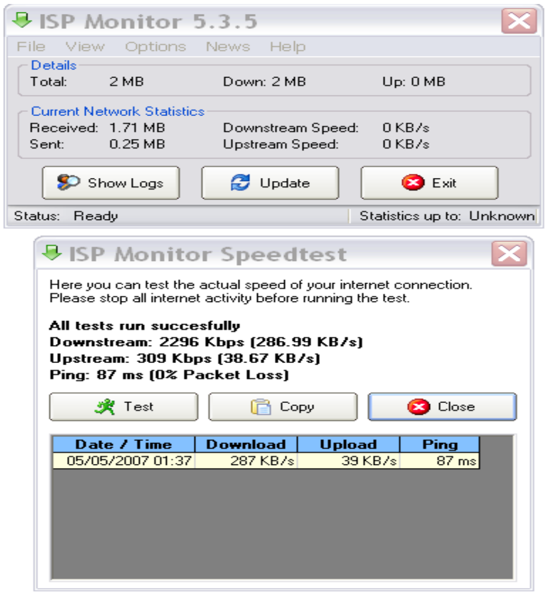
Date / Time	Download	Upload	Ping
05/05/2007 01:42	496 KB/s	39 KB/s	87 ms
05/05/2007 01:37	287 KB/s	39 KB/s	87 ms

Total: 3 MB Down: 2 MB Up: 1 MB

Received: 2.78 MB Downstream Speed: 0 KB/s
Sent: 0.5 MB Upstream Speed: 0 KB/s

Status: Next update in 55 minutes Statistics up to: Unknown

ISP Monitor on Wi-Fi:



Details
Total: 2 MB Down: 2 MB Up: 0 MB

Current Network Statistics
Received: 1.71 MB Downstream Speed: 0 KB/s
Sent: 0.25 MB Upstream Speed: 0 KB/s

Status: Ready Statistics up to: Unknown

Here you can test the actual speed of your internet connection.
Please stop all internet activity before running the test.

All tests run succesfully
Downstream: 2296 Kbps (286.99 KB/s)
Upstream: 309 Kbps (38.67 KB/s)
Ping: 87 ms (0% Packet Loss)

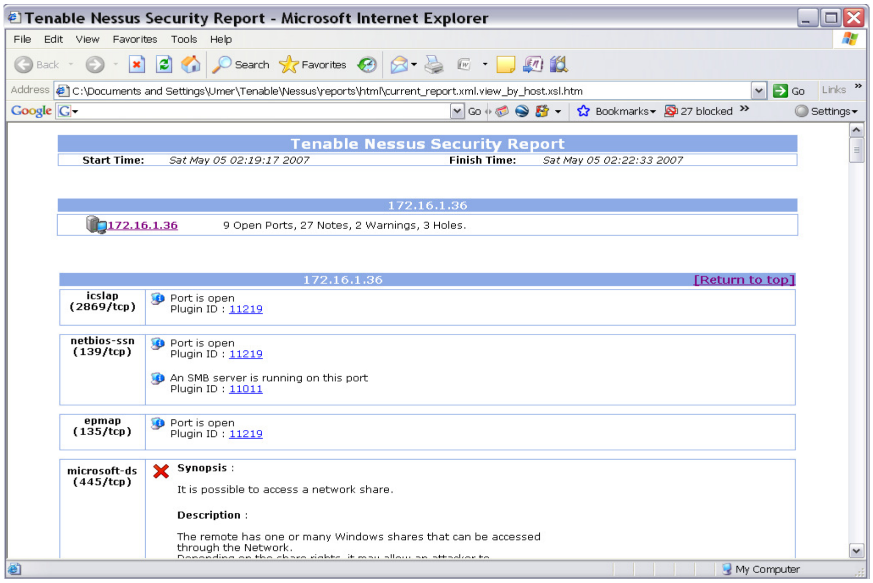
Date / Time	Download	Upload	Ping
05/05/2007 01:37	287 KB/s	39 KB/s	87 ms

6.3.6 Network Vulnerability Scan Findings:

The purpose of this test is to find the vulnerabilities in a network that uses each standard. The software used will be Nessus, which is the most popular network vulnerability scanner. Both networks will be tested by running this software under same casual conditions with security features set to default both on the operating system and the security tool. The firewalls are disabled and there is no anti-virus software in operation to maximize the objective of this test run. The security tool exposed 3 holes in the Ethernet network that included easy remote access, shares and execution of arbitrary codes. There is a warning from the tool that the server allows to perform recursive queries to be performed. For the tool to run on Wi-Fi it took about 3 minutes to complete the task with 3 security holes that included easy remote access, shares and execution of arbitrary codes were found. The risk factor for remote access is low for both networks, however for network shares and execution of arbitrary codes is high. This shows that neither the basis of media nor the difference in its access technology has an effect on the vulnerability of the network. See Picture Set 6.6 for Screen Shots of the test.

Picture Set 6.6 below shows reports generated by the Vulnerability Scanner:

Nessus on Ethernet:


Tenable Nessus Security Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\Umer\Tenable\Nessus\reports\html\current_report.xml.view_by_host.xsl.htm
Go Links
Google Go Bookmarks 27 blocked Settings
My Computer

Tenable Nessus Security Report

Start Time: *Sat May 05 02:19:17 2007* **Finish Time:** *Sat May 05 02:22:33 2007*

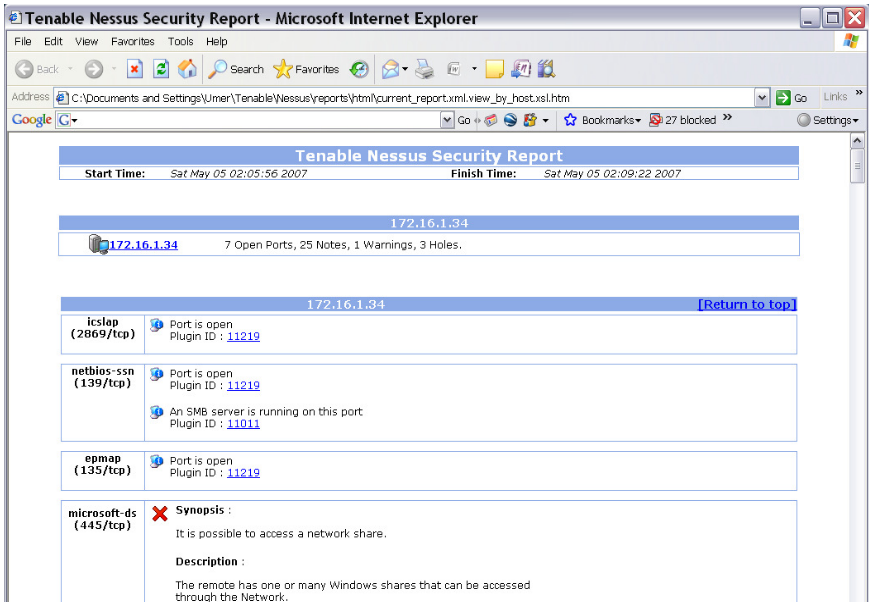
172.16.1.36

172.16.1.36 9 Open Ports, 27 Notes, 2 Warnings, 3 Holes.

172.16.1.36 [Return to top]

icslap (2869/tcp)	Port is open Plugin ID : 11219
netbios-ssn (139/tcp)	Port is open Plugin ID : 11219 An SMB server is running on this port Plugin ID : 11011
epmap (135/tcp)	Port is open Plugin ID : 11219
microsoft-ds (445/tcp)	**Synopsis** : It is possible to access a network share. **Description** : The remote has one or many Windows shares that can be accessed through the Network. Depending on the share rights, it may allow an attacker to

Nessus on Wi-Fi:


Tenable Nessus Security Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\Umer\Tenable\Nessus\reports\html\current_report.xml.view_by_host.xsl.htm
Go Links
Google Go Bookmarks 27 blocked Settings

Tenable Nessus Security Report

Start Time: *Sat May 05 02:05:56 2007* **Finish Time:** *Sat May 05 02:09:22 2007*

172.16.1.34

172.16.1.34 7 Open Ports, 25 Notes, 1 Warnings, 3 Holes.

172.16.1.34 [Return to top]

icslap (2869/tcp)	Port is open Plugin ID : 11219
netbios-ssn (139/tcp)	Port is open Plugin ID : 11219 An SMB server is running on this port Plugin ID : 11011
epmap (135/tcp)	Port is open Plugin ID : 11219
microsoft-ds (445/tcp)	**Synopsis** : It is possible to access a network share. **Description** : The remote has one or many Windows shares that can be accessed through the Network.

6.4 Considerations during Testing:

The WLAN was tested in optimum performance with full signal strength. This was done so that maximum results are achieved when compared to the wired LAN. It was thought that it will not be just to test a WLAN against a LAN if it has weak signal strength. It was also made sure there are cordless or mobile phones in close proximity or a microwave oven running as they all cause interference for a WLAN. For the wired LAN considerations were made that there is no or minimum EMI during the communication by seeing there was no florescent lighting or power cable running lose to the Ethernet cables.

6.5 Possibilities Avoided:

There could have been a good possibility of running this test on a UNIX system. 3 UNIX operating systems were considered (Knoppix 5.0, Backtrack and Linux SUSE) for this test however none of the operating systems come with built-in support for WPA encryption, therefore UNIX operating systems were dropped for the test cases.

6.5 Conclusion:

When tests were run on both LAN standards the network performance shown by the wired LAN was very efficient compare to the Wireless LAN. The RTT for when estimated was 0 for a LAN, however for WLAN it came up to 5 seconds when using IPScanner. This is a key factor in performance as this is the time it takes for packet to reach from source to destination over a network. In some cases however it is not all that important as when LanSpy was run it recorded RTT for both networks as less than 10 seconds. Port scanning again for the LAN was quicker as it scanned the same number of ports in 4 seconds less while using HostScan. It actually depends what the target being achieved is, when LanSpy was run on both networks it took over a minute more to scan the WLAN with a remote host however it exposed 1 UDP service more than compared to when the LAN was scanned.

On casual surfing the web and monitored under the PRTG Traffic Grapher software, it was noted for the same pages surfed the downstream for the WLAN was 10 Kbps more than the LAN. The upstream for both networks was 10 Kbps. This can either prove that extra packets were downloaded when pages were loaded or probably it a WLAN requires more data to be downloaded for the same pages accessed. This theory however contradicted when the ISP monitor software was run. It pinged some websites and the results showed that with 0% packet loss the upstream for LAN was 5 Kbps more compared to the WLAN. Not only this, the downstream for the LAN was over 1 Mbps more than the WLAN in a ping of 87ms.

When the networks were tested using the vulnerability scanner Nessus, it took 1 minute longer for the results to come from a LAN compared to WLAN. WLANs are generally considered to be more vulnerable than the wired LANs; however there were same number of holes found in both networks with an additional warning of allowing performing recursive queries for a LAN compared to the WLAN. Vulnerabilities could increase for a WLAN, however it used the most secured authentication encryption compared to being unsecured or WEP encryption.

It should be noted that results can vary if different wireless cards were used or the configuration of the devices were different.

7.0 Future: Wi-Fi and other wireless technologies:

7.1 Introduction:

Wireless Networks are used to communicate devices using space air as a medium. Although there are no wires attached between devices, still the base stations (access points) which the devices use to send and receive data are somehow wired to the ground network or carrier backbone. Wireless local area networks function as a peer to peer network. Multiple access points within range allow devices to roam. When a device leaves the range of a base station the configuration is handed off to the next base station within the range. This section will focus on some alternate technologies other than Wi-Fi that can work as WAN technologies like WIMAX, increasing the range of use.

7.2 Wi-Fi again, Wi-NOT let it be WIMAX:

Wi-Fi 802.11 the standard provided by the IEEE provides a connection based shared access to the wireless channel. This is done with the presence of the MAC layer that provides a time-bounded delivery in an asynchronous transmission. The MAC layer uses a basic access method to sense the channel before transmitting data. The alternative way is to request permission to send the data frame before a transmission takes place. In both these transmission there is a variable change in packet loss, the fraction of retransmission and the packet service time, considering the state to be either saturated or in transition. If the model of the MAC layer is simplified in a way that a queue is maintained of messages awaiting transmission from the MAC layer, the messages that arrive at a full queue are dropped, thus saving retransmission due to errors. With modifications to serial simulation there is reduction to events needed while parallel simulation benefits from better look ahead (32).

WIMAX- Worldwide Interoperability Microwave Access protocol 802.16 Standard provided by the IEEE is similar to Wi-Fi as they are both wireless technologies detailed with a MAC layer that supports a physical layer, however it covers a larger area and provides a higher data rate. The standard is finalized however different versions have been come up by different people, say Korea has come up with their own version known as the WiBro. WIMAX uses access technologies like CDMA that has high speed and low latency. It uses Orthogonal Frequency Division Multiplexing that is a pure IP-based infrastructure with a signal processing method that supports high data rates. Security provided by WIMAX supports both the Advanced Encryption Standard and the Triple Data Encryption Standard. This safeguards against eavesdropping, theft of service and secures the wireless broadband interface. A weakness found in WIMAX today can be its non availability today. This is probably because it will reveal features of 4G even before 3G has truly exploited itself (33).

Wi-Fi has gained its popularity in a very small time and this is due to WLANs in business and homes. Applications are being made to use Wi-Fi to transfer voice over WLAN. Compared to cabling this is very economical and easy way of configuring and maintaining, however Wi-Fi suite is made of complex protocols, not only that the layers in a suite are not fully separable, therefore if such applications are to run the design of the WLAN should be test. There are software developed that test the design of a WLAN through emulation. Each layer is test separately for example the physical and protocol layer have independent testing (34).

WIMAX being a modern wireless connectivity technology should guarantee to the QoS standards of providing real time traffic support. This was tested using VoIP software and a WIMAX equipment. It shows that the performance increases after 10 calls. There was no effect on the uplink when a bottleneck on downlink was created. A number of experiments were conducted and a conclusion is arisen that the uplink provided with WIMAX is better than its downlink (35).

In order to increase the range of wireless access Transient Access Points can be used. These are wireless internet connection mesh nodes. This can be done by forming a wireless ad-hoc network. Mesh networks require each node to communicate with the other freely; however the mesh hardware is shipped with the Wi-Fi cards. The architecture of Wi-Fi is designed to work over radio channel and therefore it is not possible to assign global access strategies. For a sender to send packets to a receiver, it is only that sender that should be allowed to carry on. This can be taken care by Collision Control techniques. TDMA is a technique that can be applied while devising a wireless mesh network to increase bandwidth (36).

If wireless mesh networks are implemented between cities there would not be a need of investing in technologies like 3G cellular and WIMAX as the same great coverage, speed and reliability can be achieved using the same wireless networks, being easier on deployment. The architecture of a mesh networks is more like the internet with all the nodes being peers to others that are in range. Mesh networks work out to be more efficient in a way that if one node is overloaded with traffic or is crashed the data is simply routed around it. The problem with mesh networks is ‘hopping’ that is every time a signal passes from one node to another the bandwidth drops (37).

Although WIMAX is adapted free from the errors found in previous technologies it still has to overcome considerations to perfect a metropolitan area network. WIMAX started off as a line of sight wireless technology however a newer version known as the 802.16-2004 non line of sight (NLOS) is a fixed wireless service. For mobile computing further enhancement was done, orthogonal FDM was introduced to achieve a maximum data rate of 15 Mbits/s for a range of 3 miles. 802.16-2005 (the mobile version) is an alternative to 3G mobile Internet access service. This has created a direct competition for cellular technologies using CDMA due to EVDO and WCDMA due to HSPDA. Even though WIMAX will be in the lime light until next year hardware manufacturers are dedicated in investing in this technology (38).

By mid 2007 a wireless technology known as the zigbee will be introduced as companies like Motorola, Samsung and Philip have pledged in the development of the technology. Based on the use of IEEE 802.15.4's physical and MAC layers, transmission is carried on as the application and security layer are defined in such a way to enable interoperability between products manufactured by different companies. It is aimed for control and monitoring applications with a range of up to 70m and low power consumption being a key asset. The operating bands are licence free and all three bands have various data rate. CSMA techniques are implemented so that Zigbee can operate in congested radio environments supporting star, mesh and cluster tree or hybrid topologies (39).

Huge investments have been staked in bringing out WIMAX, if it works out it will outcast 3G cellular networks. There has been a competitive aggression between large vendors to gain the technology to deal with multiple input multiple output transmissions improve antenna coverage range so that the range pf personal broadband can increase (40).

WIMAX having the potential of providing higher bandwidth, still it is unclear as to what the actual costs of implementation and charge for services will be. Providing bandwidth up to 40Mbits for mobile networks it is way up compared to existing 3G networks based on EV-DO technology (41).

An introduction of Wi-Fi in trains will complement the existing services like gprs and 3G provided by the cellular companies. Mobile phone companies have invested not only in Wi-Fi hotspots but also WIMAX that has services faster than HSPDA. Some cellular companies are reluctant to bring out WIMAX due to the reason of ownership of services. The other hurdle faced is how to equip the carriages with hardware to support it as a hotspot (42).

Although WIMAX is a newer and improved technology with higher coverage and high date rate even though it lacks in the quality of service that is provided by 3G networks primarily because the handover mechanism between base stations is that of used by Wi-Fi having support for different physical layers. This type of architecture provides no guarantees even though it is a connection oriented service. Wi-Fi on the other hand does guarantees of QoS due to the presence of an alternative mechanism of admission control. The choice of the network depends on whether the application used requires QoS and at what level (43).

Mobile WIMAX is set to be available and there are reasons why fixed WIMAX is not gaining popularity. Other reason can be that DSL is cheap technology with relatively good performance, making fixed WIMAX strive in the market share. Mobile WIMAX will appear as 4G network. Wi-Fi may require WIMAX on its backbone to provide services to the end user (44).

As compared to Wi-Fi, WIMAX provides over 4 times the number of subcarriers over a variable bandwidth of 1 to 28 MHz. With more subcarriers and a variable length guard interval, the spectral efficiency has increased from 15% to 40% compared to Wi-Fi. The error vector magnitude of Wi-Fi is higher than WIMAX makes WIMAX have a longer range. Wi-Fi transmits and receives functions on the same channel where as WIMAX transmits and receives functions at a different channel and at a different time. In Wi-Fi the output power is virtually fixed however in WIMAX the devices closer to the base stations emit less output power whereas the ones further away emit maximum output power. WIMAX chips however are not that integrated as the Wi-Fi chips (45).

There are some complexities that can arise in the physical layer of WIMAX as scrambling is more difficult to detect as it can be caused due to natural sources of noise. If AES is not applied in the MAC layer there can be major threats of interception, intrusion and even modification (46).

7.3 Conclusion:

Wi-Fi is a solution most widely used today due to the very reason the ISM licence to operate is free to operate and the equipment required is readily available, rather comes with standards PCs off the shelf. It is a technology heavily invested upon by technology giants and it is very hard for investors to ‘hand-off’ to a new technology so quickly without the desired returns on it. WIMAX, however if invested upon is a promising future, binging the expansion of range when it can be used as a LAN technology as well. It is for the tech giants to decide whether WIMAX or others like WiBro and Zigbee will come in to replace Wi-Fi at all, will they provide a platform for Wi-Fi and replace only the wired WAN telephone cable system or will all technologies will enjoy their competitive share in the market.

8.0 Evaluation:

The main difference between the 802.3 and the 802.11 standard is that in the way the network architecture of the data link layer of the two is different because of the differences in the packet format. With better mechanisms to access the media between multiple hosts WLAN has a bright future in the industry. There are other factors that support the promotion of WLANs compared to the wired LANs like cost of cabling and structuring cabling for network communications. Scalability is another factor that is promoting WLANs over the conventional LANs as there is no problem of moving devices around without worrying about changing office layout plans.

Businesses have however invested heavily in wired Giga Ethernet due to performance factors. Ethernet is defiantly more performing than Wi-Fi. A factor that is behind this performance measuring is that Gigs of data is allowed to pass through the guided media. The rate at which data is moved at a lower rate in WLAN is constrained to technology it supports; rather the data is contained not allowing maximum performance due to requirements in WLANs. An example of this can be seen that when requirements for a fast WLAN are increasing 802.11n is coming out in the market with a rate of 108 Mbps/s. It can be clearly explained that if data is allowed to move across the WLAN at the same rate it is moved on a wired LAN, the performance will be much greater. This is because the packet size for Wi-Fi is smaller resulting in less Error rate. An improvement can be done in the WLAN communication by increasing the ACK timeout and increasing the number of channels that are shared between the hosts.

Security is also a concern that cannot be neglected in a local area network. The existence of SSID is a major security concern even if the authentication is encrypted using WPA. A determined attacker will try best to intrude in to the system. For an intruder to attack a wired LAN, conventional methods are adopted with vampire attacks on the Ethernet cable running through. For both wired and wireless LAN, a system administrator can monitor trends on the network. With a few software tools installed any new device connected to the network can be monitored. Both LANs and WLANs can be configured in the same way to prevent intrusions. For WLANs MAC addresses of devices can be registered with the network system to allow only specified devices to connect. Routers can be configured to hide the SSID, preventing temptations for every device that has wireless access.

9.0 Recommendations:

There is a trend arising in investing in to wireless networks. WLANs should be configured to be accessed over a longer range with better security features.

With the initiation in wireless WAN technologies like WIMAX 802.16 by IEEE, wireless communications are gaining popularity. If the WLANs can be extended to the extent of roaming with the help of WAN technologies, it will be very convenient when mobile computing can become a conventional device in offices and later be roamed around from city to city with a WAN platform to support its backbone.

The test could have been better if the wireless adapters were 802.11n as that is the latest technology provided by IEEE. If there were more resources provided for the test to conduct it would have been a good test case to hide the SSID and then scan it though an Air wave analyzer software like kismet that can detect hidden SSIDs. For this an external antenna is required with the help of a wireless adapter that can scan other frequencies.

To improve the security of the wireless network a recommendation can be made to change the way communication is carried on in a network. A wireless adapter can be designed in such a way that when it sends out the data it should modulate the frequency of the traffic. The configured router and receiving device on that network should be able to demodulate and modulate the traffic. As the listening intruder will be focused on the 2.4 GHz frequency band, the network will be protected. There is however a consideration in this case, the frequency band needs to be licensed to a have a legitimate network because the ISM band is a free licence running on 2.4 GHz.

10. Conclusion:

The project was prepared over a period of 10 weeks and completes the requirement of testing and evaluating local area networks. 46 documents were referenced using white papers, journals and scientific articles from reliable sources like the ACM digital library, Athens account, The IET journals, BCS Online Members only area and other industry giants in the field of computing.

The original paper that mentions the advent of Ethernet protocol written by the Robert M. Metcalfe and David R. Boggs of the Xerox Palo Alto Research Centre was also referenced in the research of this paper.

The methodology and method chosen to gather material for the research and test were selected as they cover the scope to gather constructive information about the subject. The test findings cover the aims and objectives mentioned of the project.

The articles searched were critically evaluated to see the relevance with the topic. The literature was taken from trusted sources to be sure of authenticity and reliable.

I believe Wi-Fi will not eradicate the Wired LAN for a couple of years due to performance in terms of bandwidth available, however with Giga Wi-Fi coming in the market, it will not be late when there is a complete turn over to WLANs especially when technologies like WIMAX will be shortly available to support as a backbone for mobile computing using WAN Local Loop capabilities, handover and roaming technologies.

Appendix:

A 1.0 Hardware/Software used in testing the Network:

Hardware:

- 2 * Laptops with Intel mobile processors and LAN cards.
- Intel wireless adapter 802.11b on remote host and 802.11b/g on the server.
- BT wireless 802.11b/g ADSL router with wireless support up to 54 Mbps and LAN support up to 100 MBps.

Operating System:

- Microsoft Windows Xp Home Edition on both Computers

Testing Software:

- Nessus Vulnerability Scanner
- LanSpy
- Wireshark
- Airsnare
- PRTG Traffic Grapher
- ISP Monitor
- IPScanner
- HostScan 1.6
- CAT IP monitor
- Emsa Bandwidth Monitor

References:

1. Networking Explained 2nd Edition, Authors: Michael A. Gallo and William M. Hancock, ISBN: 1555582524, Digital Press 2002. Book was taken from British Computer Society's Online Members Only Library.
2. History of wireless: http://www.jhsph.edu/wireless/history.html
3. Overview of wireless communication—cambridge press pdf, by Andrea Goldsmith. www.cambridge.org/0521837162. Source: ACM digital Library.
4. 802.11 technologies: Past, Present and Future, Published by Troops Networks in August 2004. Copyright 2005.
5. Ethernet technologies: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm#wp1020560
6. Ethernet: Distributed Packet Switching for Local Computer Networks
   Robert M. Metcalfe and David R. Boggs
   Xerox Palo Alto Research Center. http://www.acm.org/classics/apr96/
7. Networking for Dummies 2nd Edition, by Douge Lowe. Published by Wiley Publishing Inc. Copyright 2005. ISBN 13:978-0-7645-9939-2.
8. Network Communications Technology, by Dr. Ata Elahi, Southern Connecticuit University. Published by Delmar Thomson Learning. Copyright 2001. ISBN: 07668-1388-6.
9. High-Speed Local Area Networks and their performance: A survey. By Bandula W. Abeysundara and Ahmed E. Kamal. University of Alberta. Source: ACM Computing Surveys, Vol 23, No 2, June 1991.
10. Performance Evaluation of the Physical layer for the 10Gbit/s Ethernet Passive Optical Networks. By Silvia Pato, Paulo Monteiro and Henrique Silva. Source ACM Digital Library; ACM: 1-59593-513-4/06/09. Dated: September 2006.
11. TCP for high performance in Hybrid fiber Coaxial Broad-band Access Networks, by Reuven Cohen and Srinivas Ramanthan. Source: IEEE/ACM Transactions on Networking, Vol 6, No.1, February 1998.
12. The family dynamics of 802.11, by Bill Mcfarland and Michael Wong, Atheros Communication. Source: ACM digital Library. Publication Date: May 2003.
13. High performance Wireless Switch Protocol for IEEE 802.11 Wireless Networks, by Jenhui Chen, AI-Chun Pang, Shianm-Tsong Sheu and Hsueh-Wen Tseng. Source: ACM digital library. Copyright 2005.
14. Scheduling of real time traffic in IEEE 802.11 wireless LANs, by Constantine Courtas, Sanjay Gupta and Ness B. Shiroff. Source: ACM digital library. Publication Year: 2000. Publisher: JC Baltzer, Science Publishers.

15. On the Performance Characteristics of WLANs: Revisited. By Sunwoong Choi, Kihong Park and Chong-Kwon Kim. Copyright 2005 ACM 1-59593-022-1/0/0006.
16. Bandwidth overhead in Wi-Fi mesh networks for providing fair internet access. By Thomas Scherer and Thomas Engel. Source: ACM digital library. Copyright: 2006 ACM 1-59593-502-9/06/0010.
17. Improving Protocol capacity with model-based frame scheduling in IEEE 802.11-operated WLANs. By Hwangnam Kim and Jennifer C. Hou, University of Illinois. Copyright: 2003 ACM 1-581113-753-2/03/0009
18. Performance analysis of the interwined effects between network layers for 802.11g transmissions, by Jon Gretassson, Fen Li, Mingzhe Li, Ashish Samant, Huahui Wu, Mark Claypool and Robert Kinicki, Worcester Polytechnic Institute, USA. Copyright 2005 ACM 1-59593-183-X/05/0010.
19. Wi-Fi Exposed, by Andrea Bittau. Copyright 2004, the ACM Student Magazine. Source: ACM digital Library.
20. An application-driven perspective on wireless sensor network security, by Eric Sabbah, Adnan Majeed, Kyoung-Don Kang, Ke Liu and Nael Abu-Ghazaleh, State University of New York. Source: ACM digital Library. Copyright: 2006 ACM 1-59593-486-3/06/0010.
21. Answer: Autonomous Wireless Sensor Network, by Stephen Olariu, Mohamed Eltoweissy and Mohamed Younis. Source: ACM digital library. Copyright: 2005 ACM 1-59593-241-0/05/0010.
22. Troubleshooting Wireless LANs to improve Wi-Fi uptime and Security, Fluke Networks. White paper. Copyright 2005 fluke Corporation. Source; ACM digital library.
23. Security protocol for IEEE 802.11 wireless local area network, by Se Hyun Park, Aura Ganz and Zvi Ganz. Moble Networks and Applications 3 (1998) 237-246. Published by: Baltzer Science Publishers BV. Source ACM digital library.
24. Enhancing Wireless Video streaming using lightweight approximate authentication, by Gabor Feher, Duapest University of technology and Economy. Copyright 2006 ACM 1-59593-486-3/06/0010. Source: ACM digital library.
25. Wireless Infidelity I: War Driving, by Hal Berghel. Communications of the ACM, September 2004/ vol.47. No.9. Source: ACM digital library.
26. Wireless Infidelity II: Airjacking, by Hal Berghel and Jacob Uecker. Communications of the ACM, December 2004/ vol.47. No.12. Source: ACM digital library.
27. How 802.11 Wireless Works: http://technet2.microsoft.com/windowsserver/en/library/370b019f-711f-4d5a-8b1e-4289db0bcafd1033.mspx?mfr=true. Updated March 28, 2003.

28. IEEE 802.11 Technical Tutorial, by Breeze Wireless Communications Ltd. http://www.qsl.net/n9zia/wireless/pdf/802.11.pdf.
29. What exactly is OFDMA, by Ian Poole. Page 46-47, IET Communications Engineer, April/May 2007 Issue.
30. Turning 802.11 Inside-Out, by Pravin Bhagwat, Bhaskaran Raman, Dheeraj Sanghi. ACM Sigcomm Computer Communications review, Vol. 34, Number 1: January 2004. Source: ACM digital Library.
31. Low Power Advantage of 802.11a/g vs. 80211b, white paper by Texas Instruments. Copyright 2006, Texas Instruments Incorporated. SPLY006-December 2003.
32. Towards High Performance Modelling of the 802.11 Wireless Protocol, Authors: Jason Liu, David M. Nicol, L. Felipe Perrone, Michael Liljenstam. Proceedings of the 2001 Winter Simulation Conference by B.A. Peters, J.S. Smith, D.J. Medeiros and M.W.Rohrer, eds
33. WIMAX to The World?, Author: Teri Robinson, Publication Year December 2005.
34. Double Barrelled Wi-Fi Test, Author: Richard A Quinnell, Publication Date 2005, Made Available by Reed Elsevier Inc.
35. Performance Evaluation of a WIMAX Testbed under VoIP Traffic, Authors: Nicola Scalabrino, Francessco De Pellegrini, Imrich Chlamtac, Andrea Ghittino and Sandra Pera. Copyright September 2006, Reference: ACM 1-59593-X/06/0009.
36. Bandwidth Overhead in Wi-Fi Mesh Networks for Providing Fair Interent Access. Authors: Thomas Scherer and Thomas Engel. Copyright October 2006. Reference: ACM 1-59593-502-9/06/0010.
37. Municipalities Starting to Mesh. Author: Eric Nee. Publication Date: March 2005. Copyright of CIO Insight is the property of Ziff Davis Media Inc.
38. Ready for WIMAX? Author: Louis E. Frenzel, Communications Test Editor. Publication Date: 09.14.06. Copyright of Electronic Design (www.electronicdesign.com) is the property of Penton Publishing.
39. What Exactly is …ZigBee?, Author: Ian Poole. Published by IEE Communication Engineer Magazine. Publication: Aug/Sept 2004.
40. Forward Motion – WIMAX: A vision for personal broadband. Author: Kevin Fitchard. Publication Date: 10.9.06. Published by Prism Business Media.
41. WIMAX Still at start-up Mode for Corporate Applications. Author: Matt Hamblen. Publication Date: October 16, 2006. Published by Computer World. Article even available at www.computerworld.com.
42. Can Wi-Fi catch the train?, Author: Iain Morris, features editior Telecommunications International Magazine. Publication date: September 2006. Copyright of Telecommunications- International Edition.

43. No Guarantees, Author: Chris guy. Published by IET Communication Engineer magazine. Issue Date: Aug/Sept 2006.
44. A Revolution in the Making. Author: David Sandham. Published by IET Communication Engineer magazine. Issue Date: Oct/Nov 2006.
45. Challenges of WIMAX Design. Author: Darcy Poulin. Published by IET Communication Engineer magazine. Issue Date: Oct/Nov 2006.
46. WIMAX/802.16 Threat Analysis, Author: Michel Barbeau. Publication Date: October 2005. Reference: ACM 1-59593-241-0/05/0010.

Bibliography:

1. Local Networks by William Stallings, Honeywell Information Systems, Inc, McLean, Virginia 22102. Source: Computing Surveys, Vol 16, No.1, March 1984. ACM 0360-0300/84/0300-0003.

2. Computer Networks, Fourth Edition by Andrew S. Tanenbaum. Published by Prentice Hall (Pvt.). 2003. ISBN -81-203-2175-8

3. Computer Networking with Internet Protocols and Technology, by William Stallings. Published by Pearson Education in 2004. ISBN 81-297-292-4.

4. Distributed Systems, Principles and Paradigms, by Andrew S. Tanenbaum and Maarten van Steen. Published by Pearson Education in 2005. ISBN 81-7808-789-8.

5. Multimedia Communications, Applications, Networks, Protocols and Standards by Fred Halsall. Published by Pearson Education in 2005. ISBN 81-7808-532-1

6. Cryptography and Network Security, principles and Practices, 3rd Edition, by William Stallings. Published by Prentice Hall in 2005. ISBN 81-203-2385-8.

7. Hacking for Dummies by Kevin Beaver. Published by Wiley Publishing, Inc. Copyright 2004. ISBN 0-7645-5784-X.

8. Network Protocols, by Andrew S. Tanenbaum. Source ACM digital library ACM 0010-4892/81/1200-0453. Copyright 1981.

9. Public vs. Private Wi-Fi by Gilbert Held. International Jounal of Network Management. Published online in Wiley Interscience. DOI:10.1002/nem.560. Copyright 2005.

10. Comprehensive Analysis of the 802.11 by Peter P. Pham. Mobile Networks and applications 10, pg 691-703, 2005. Source ACM digital library. Copyright 2005.

11. Saving Energy during Channel Contention in 802.11 WLANs, by V.Baiamonte and F. Chiasserini. Mobile Networks and Applications 11, 287-296, 2006. Published online 31st March 2005.

12. Architecture and Techniques for Diagnosing Faults in IEEE 802.11 infrastructure Networks, by Atul Adya, Paramvir Bahi, Ranveer Chandra and Lili Qiu. Source ACM digital Library. ACM 1-58113-868-7/04/0009. Publication Date: Sept. 2004.

13. Improving Protocol Capacity with Model-based Frame Scheduling in IEEE 802.11- operated WLANs by Hwangnam Kim. Source ACm digital Library ACM 1-58113-753-2/03/0009. Copyright 2003.

14. Performance Investigation of IEEE 802.11 MAC in Multihop Wireless Networks, by Jianhua He, Dritan Kaleshi and Zhong Fan. Source: ACM digital library. ACM 1-59593-1880-/05/0010. Copyright 2005

15. Security protocol for IEE 802.11 wireless local area network, by Se Hyun Park. Mobile Networks and Applications 3 (1998) 237-246. Copyright Baltzer Science Publishers BV.

16. Robust Rate Adaption for 802.11 Wireless Networks by Starsky H.Y Wong. Source ACM digital library. ACM 1-59593-286-0/06/0009. Copyright 2006.

17. Top 10 Security Checklist for SOHO Wireless LANs, by David Colman, AirSpy networks. Copyright 2004 CWNP.

18. Wi-Fi Certified for WMM – Support for Multimedia Applications with QoS in Wi-Fi networks, by Wi-Fi Alliance. Dated; September 1, 2004. Source: ACM digital library.

19. How Wi-Fi works. “How WiFi Works?” CNN. 5 Dec. 2004. http://www.cnn.com/interactive/tech/0303/wifi.explainer/content1.html

20. Mark, Jon W. Wireless Communications and Networking. Upper Saddle River, NJ: Prentice Hall, 2003.

21. Wireless Standards wars. Author: John Walko. Published in the IET Communication Engineer magazine April/May 2006 issue.

22. HSDPA Inside. Author: Juan Pablo Conti. Published in the IET Communication Engineer magazine Aug/Sept 2006 issue.

23. Emerging Mobile Wimax antenna technologies. Author: Paul Piggin. Published in the IET Communication Engineer magazine Oct/Nov 2006 issue.

24. Wimax Roaming off and Running. Author: Dan O’Shea. Published for Telephony magazine. Year: Oct 2006. Copyright by Prism Business Media.

25. Wifi Mania. Author: Claudia Kienzle. Published by IEE Communication Engineer magazine, Issue Dated: Aug/Sept 2004.

26. 802.11_Architecture.pdf. Power point presentation by Avaya Communications. http://wireless.ictp.trieste.it/school_2002/lectures/ermanno/HTML/802.11_Architecture.pdf.

27. Performance Evaluation of the physical layer for 10 Gbps Ehtnernet Passive Optical Networks, Silvia Pato. Source ACM digital library. ACM 1-59593-513-4/06/09. Copyright 2006.