PERFORMANCE STUDY OF AD HOC WIRELESS LAN FOR MULTIMEDIA STREAMING APPLICATIONS

By

KON PEI SIN

FINAL REPORT

Submitted to the Electrical & Electronics Engineering Programme
in Partial Fulfillment of the Requirements
for the Degree
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Universiti Teknologi Petronas
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

PERFORMANCE STUDY OF AD HOC WIRELESS LAN
FOR
MULTIMEDIA STREAMING APPLICATIONS

by

Kon Pei Sin

A project dissertation submitted to the
Electrical & Electronics Engineering Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Approved by:

Ms. Nasreen Badruddin
Project Supervisor

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK

June 2006

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

Kon Pei Sin

ABSTRACT

Wireless Local Area Network (WLAN) provides high-speed and cable-free access for computer-to-computer information transfer within the coverage range. The optional feature of WLAN is ad hoc, which allows the network to be formed and deformed without the need of system administration or access point. Multimedia streaming through WLAN allows users to download and play a small chunk of the multimedia file simultaneously. An ad hoc base wireless network is used in this project rather than infrastructure base due to the simpler architecture, cheaper set up cost of ad hoc network and no system administrator required. Unlike file sharing, streaming will not download the whole file. Streaming can be used for multimedia distribution without users having the illegal copies of the file. In this project, a multimedia file is to be streamed, but not downloaded, through the WLAN without passing through any access point. The host computer broadcast the multimedia file using "media server configurator" while the client computer streamed from the host computer using "streaming media player". Multi-hop streaming allows a node that is totally out of the coverage range to stream from the host computer, using the bridge as a passage. The streaming of the multimedia file is seamless and smooth within the ad hoc network. A node that is out of the coverage range can stream from the host computer by using the multi-hop concept although the distance between the host and the client does affect the performance. In multi-hop wireless network, the streaming process is at its best when the bridge is about 3 meters away from the receiving node.

ACKNOWLEDGEMENTS

First of all, I would like to express my hearty gratitude to my supervisor, Ms. Nasreen Badruddin, for the kind assistance and guidance she has showed me during the pursuit of my Final Year Project. She has provided an excellent and valuable feedback for my project. Without her help, I could not have completed this dissertation successfully.

I would also like to thank Dr. Varun Joeti for the group supervision and guidance provided. I am grateful to the laboratory technicians, Ms. Siti Hawa and Ms. Azira for their kind help and support.

Finally, I would like to express my sincere gratitude to my parents and my friends for their love, encouragement, and prayer. Without their love and support, I could not have finished my project successfully.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background Study

Wireless Local Area Networks (WLAN) has played a key role in revolutionizing the use of technology in society. The term wireless refers to the transmission of information and data without wires. WLAN provide high-speed, cable-free access for computer-to-computer information transfer within the coverage range. Most installed wireless LAN today is infrastructure-based, which requires the use of access point. The access point provides an interface to a distribution system, which enables wireless users to utilize corporate servers and Internet applications. [1]

The optional feature of wireless LAN standard, 802.11b/g specifies the "ad hoc" mode, which allows the network interface card (NIC) to operate in an independent basic service set (IBSS) network configuration. No access points are needed in the IBSS. [2] An ad hoc wireless network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their coverage range. An ad hoc wireless network is self-organizing and adaptive. This means that a formed network can be deformed without the need of system administration. The term "ad hoc" tends to imply "can take different forms" and "can be mobile, standalone, or networked". [3]

Peer-to-Peer (P2P) Networking feature provided by most of the operating system (OS) such as Windows, Linux, and many other OS has a very simple configuration to set up an Ad Hoc network. Two or more PCs can form a peer-to-peer network. In Windows, the P2P grouping is called a workgroup.

Streaming is a process where users download and play a small chunk of the multimedia file smoothly at the same time but without having a copy of the original file. Streaming is different from file sharing where it does not download the whole file. It is normally used for multimedia distribution without the users having illegal copies of the file. It allows the owner of the file to share the contents but the users would not be able to own the file. The live streaming is very useful in broadcasting the football match, videoconference, net meeting, and deliver lecture. Capture devices record and connect to the host computer for broadcast the captured files while the client computer streamed from the host computer as shown in Figure 1 below.

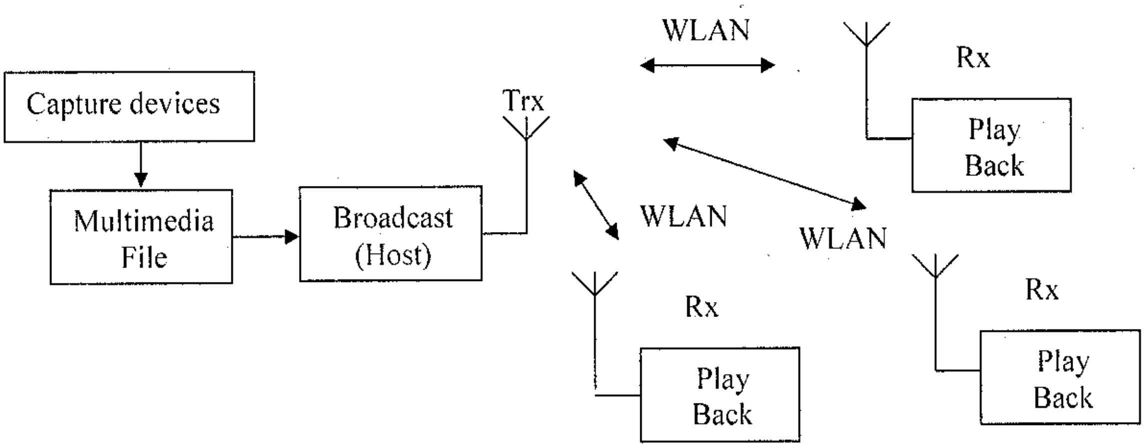


Figure 1: Multimedia Streaming / Live Streaming through WLAN

1.2 Problem Statement

The file sharing and downloading files in Local Area Network (LAN) are very common. In file sharing, the multimedia file shared on the network needs to be completely downloaded in order to play the file. The users will never know the content of the multimedia files until they completely download the file and play it. Thus, the users might not have enough disk space to store such a big multimedia file.

Streaming only allows users to play the multimedia file while downloading small chunks of the file from the source. It will continue download the small chunks while it is playing the multimedia file smoothly. Streaming does not allow the users to download the whole file. It can be used for multimedia distribution without users having illegal copies of the original multimedia file. It allows the owner of the file to share the contents but the user would not be able to own the file.

The basic architecture of networking must be studied in order to proceed with the project. The node discovery in a WLAN, the IP address assign, and the routing of the ad hoc network are the problems that need to be defined. The most challenging part of this project is to allow the node, which totally out of the coverage range to stream the multimedia files by using the multi-hop concept.

1.3 Objectives and Scope of Study

The project goals are as follows:

- Create an ad-hoc wireless network
- Any node within the coverage range should be able to detect the network created
- Users are only allowed to stream the multimedia files but not download the files from the Ad-Hoc network.
- The playing of the multimedia files should be seamless and smooth.
- Create a multi-hop wireless network
- Streaming process in the multi-hop wireless network.

The main purpose of this project is to stream the multimedia file between the host computer and the others node computers with wireless LAN enabled without passing through access point. The streaming process protects the originality of the multimedia files without the users having a copy of the multimedia file. The secondary objective is to learn how to construct an Ad Hoc wireless network in a room to allow multimedia file streaming in the network. The Ad Hoc wireless network created is able to detect any node within the coverage range of the network. The project is being done in Ad-Hoc base rather than the infrastructure base (access point) because the ad hoc network is more suitable for small area data communication and no system administrator is needed. The complexity and cost of setting the network is lower compared to infrastructure base. The multi-hop streaming is one of the objectives, which allow a node that is totally out of the coverage range to stream the multimedia file from the host.

The project concentrates on the creation of wireless network, node discovery in wireless local area network (WLAN), streaming between the two or more wireless enabled computers, and multi-hop streaming. The Ad-Hoc wireless networking, WLAN, multi-hop networking, and the performance of the multi-hop networking are the issues included in the scope of this study.

CHAPTER 2
LITERATURE REVIEW / THEORY

2.1 Wireless Local Area Network (WLAN)

Wireless Local Area Network (WLAN) provides high-speed, cable-free access for computer-to-computer information transfer within the coverage range. They possess all the functionality of local area network (LAN), but without the physical constraints of the wire itself. The wireless nature allows easy implementation, portability, and lower installation costs. Wireless systems can be installed in different environments, such as offices, manufacturing floors, hospitals, or universities.

Wireless networks have their own standards as in wired network. In 1990, the IEEE (Institute of Electrical and Electronic Engineers) formed a group to develop a standard for wireless equipment. The applicable standard for most of the WLAN world is the IEEE 802.11 WLAN standard. The original 802.11b standard limited WLAN speed to 2 Mbps, which is not efficient enough for most networking needs. In September of 1999, The B standard offered two higher speeds, 5.5 Mbps and 11 Mbps. At the same time B was released, A was also added to the 802.11 standard. 802.11a has a maximum speed of 54 Mbps and supports speeds of 48, 36, 24, 18, 12, 9, and 6 Mbps at a frequency of 5 GHz [4]. The reason that 802.11a is faster than 802.11b is because of its higher frequency, more transmission channels, multiplexed transmissions, and an efficient error-checking scheme. In late 2001, a draft was proposed called 802.11g. 802.11g runs on the same RF band as B (2.4 GHz) but uses the transmission techniques of A [4].

There are some challenges faced on WLAN such as radio signal interference. It is possible to have third party interference that using wireless bridging or other wireless devices operating in the same frequency band. Many other devices, such as cordless phone (portable phone), microwave ovens, wireless speakers, blue-tooth devices, and security devices, also use these frequencies. Power consumption is always an issue with laptops and PDAs, because the power and battery have limited lives. In a closed network, a single vendor solution has advantage on interoperability and management to avoid the possibility of one vendor blaming the other for equipment failures. Security in the IEE 802.11 specification, which applies to 802.11b/a/g, has come under such analysis. IEEE enhanced Wired Equivalent Privacy (WEP) to provide robust authentication options with 802.1x to make 802.11 based WLAN secure. At the same time, IEEE is looking to stronger encryption mechanisms [5]. WLAN using the TCP/IP protocols helps protect the network against any loss or corruption of data over the air. Because of differences in component configuration, placement, and physical environment, every infrastructure application is a unique installation. There are many unknowns concerning the safe limits of human exposure to RF radiation [5].

2.2 Ad-Hoc Wireless Network

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. A mobile ad hoc network (MANET) is a system of wireless mobile nodes, which can dynamically self-organize into temporary network topologies. MANET allows people and devices to inter-network in areas without any existing of infrastructure (access point). The formed network can be deformed on the fly without the need for any system administration.

Ad hoc nodes should be able to detect the presence of other such devices and to perform the necessary handshaking to allow communications and sharing of the information and services [6]. Ad hoc devices not only can detect the presence of connectivity with neighbouring devices/nodes, but also identify what type the devices are and their corresponding attributes. Since an ad hoc wireless network does not rely on any fixed network entities, the network itself is essentially infrastructure-less. There is no need for any fixed radio base stations, any wires or fixed routers.

However, due to the presence of mobility, routing information will have to change to reflect changes in link connectivity [6].

There are some challenges faced in mobile ad hoc networks. To prevent interference, ad hoc networks must operate over some form of allowed or specified spectrum range. Most microwave ovens operate in the 2.4GHz band, which can therefore interfere with wireless LAN systems. Since multiple mobile ad hoc nodes share the same media, access to the common channel must be made in a distributed fashion, through the presence of a MAC protocol. The MAC protocol must compete for access to the channel while at the same time avoiding possible collisions with neighbouring nodes [6]. Ad hoc mobile networks are different from packet radio networks since nodes can move freely resulting in a dynamically changing topology. In ad hoc mobile networks, mobile devices must perform both the role of an end system and an intermediate system. Hence, forwarding packets on the behalf of others will consume power, and this can be quite significant for nodes in ad hoc wireless network. Ad hoc networks are intranets and they remain as intranets unless there is connectivity to the Internet. Such confined communications have already isolated attackers who are not local in the area.

To join an IP network and communicate with others, a node needs to be configured either manually by an administrator or automatically through a server. However, the manually configured is impractical for large networks as well as in the case of a mobile ad hoc network due to mobility of nodes. There are two ways to distribute IP address auto-configuration mechanisms for mobile ad hoc networks, which is RADA (Random Address Allocation) and LiA (Linear Address Allocation). RADA is base on random IP address selection, while LiA linearly assigns new addresses by utilizing the current maximum IP address value. There is an improved version of LiA, known as LiACR (Linear Allocation with Collision Resolution), which reduces control overhead.

2.3 Multi-hop Wireless Network

Multi-hop wireless networks combine the characteristics of both wireless and mobile ad hoc networks. In multi-hop wireless networks, the existence of a communication link between the node and the host is not required. Indeed, a (usually small) number of other nodes relay the communication between the node and the host.

Several benefits can be expected from the use of multi-hop wireless network. First, the energy consumption of the mobile devices (nodes) can be reduced. The energy consumption required for radio transmission grows linearly with the distance. Therefore, the battery life of wireless devices can be extended if packets are routed in small hops from the host to the node. Second, as an immediate positive side effect of the reduced transmission energy, the interference is reduced. Third, if the nodes are not too remote from each other, they can communicate independently from the infrastructure. Fourth, the number of fixed antennas can be reduced. Finally, the coverage of the network can be increased using multi-hop wireless network [7].

Although Multi-hop wireless networks are attractive at first sight, multi-hop wireless networks raise a number of problems. For example, in conventional wireless networks with access point, base stations usually are in charge of channel allocation, the synchronization, and power control of mobile devices. To accomplish these tasks, the base stations take advantage of their direct communication link with every mobile device currently visiting their cell. It is quite difficult to extend these operating principles to multi-hop wireless networks.

2.4 Peer-to-Peer (P2P) in Windows

Fortunately, Windows, Linux, and many other OS provide for a very simple ad hoc network called peer-to-peer networking. In a conventional computer network, a server can support many PCs. The server and PC are very different, in both software and function. The server functions are to authenticate PS users, interconnect PCs to the server and each other. This architecture is called client/server. The individually networked PCs act as clients, rather than peers of the server. However, there is another method to connect PCs into network [8]. Two or more PCs can form a peer-to-peer network. In Windows, this P2P grouping is called a workgroup.

CHAPTER 3

METHODOLOGY / PROJECT WORK

3.1 Procedure Identification

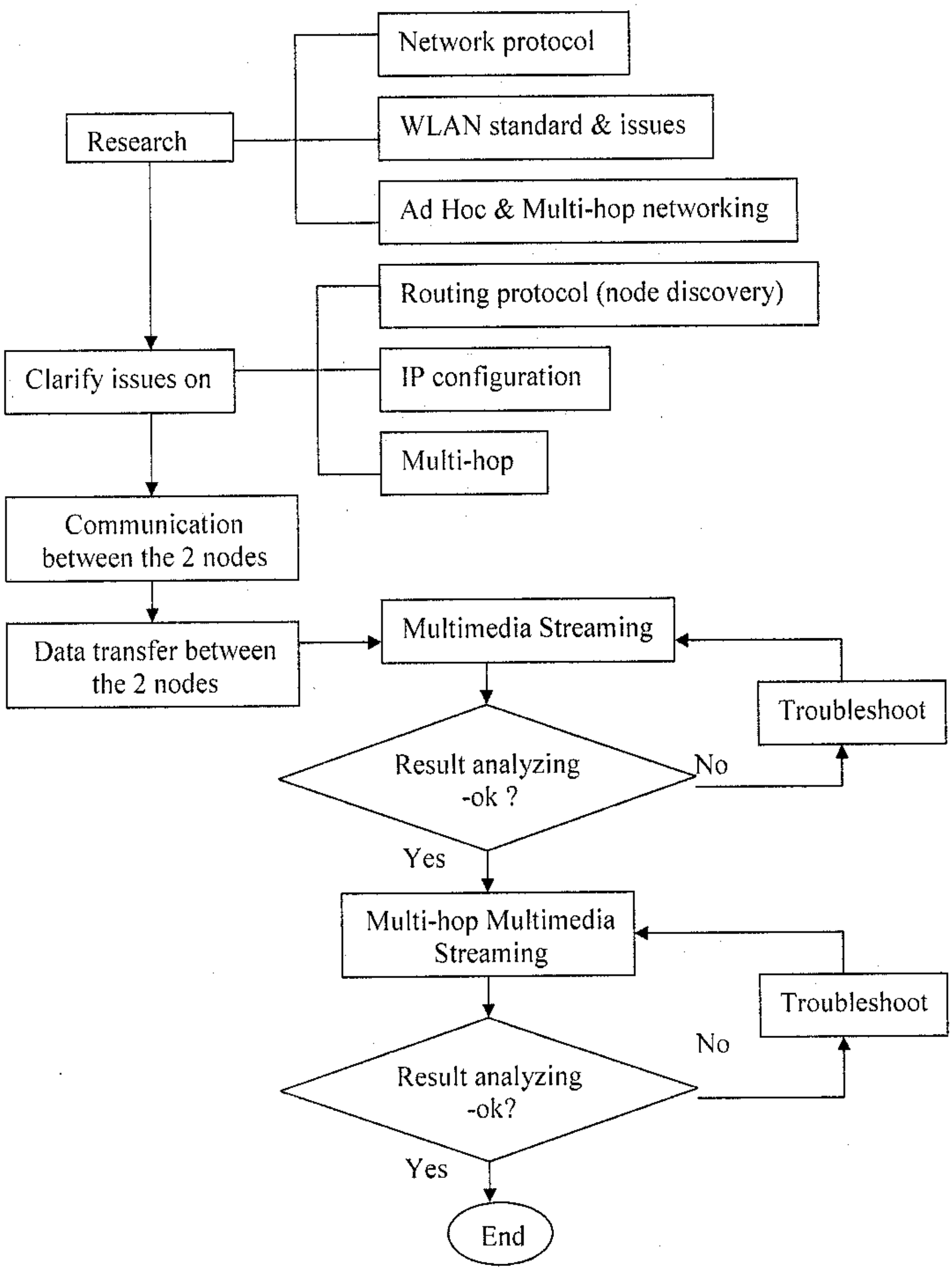


Figure 2: Final Year Project planning procedures

The planning procedure for the final year project is clearly illustrated in Figure 2. In the earlier stage of the project, research on the network protocol, wireless local area network (WLAN), the ad-hoc wireless network, and the multi-hop wireless network has been done. Then, the issues on routing protocol, IP configuration, and multi-hop networking are clarified. The project is continued by conducting the wireless network within two nodes in a laboratory at block 22. After the network set up, the data are transferred from one node to the other to prove the wireless network is functioning. Multimedia file streaming is experimented by using the network created with different distance between the nodes. The project proceeds with the multi-hop multimedia file streaming. Another node, which is totally out of the coverage range, can stream from the host by using the multi-hop concept. Experimental on the distance between nodes and the data transfer rate of the multi-hop streaming is carried out to evaluate the performance of the streaming in multi-hop wireless network.

3.2 Tools / Equipments Required

1. Two wireless LAN enabled computers

   Nowadays, all laptops come with the integrated Wi-Fi enable card with the latest technology of Intel Centrino®

2. 802.11b/g USB wireless adapter

   A USB 2.0 wireless adapter, which is used to attach to the desktop computer so that it becomes WLAN enabled. This USB wireless adapter uses the IEEE 802.11g standard

3. Multimedia file

   A video clip, MTV, and anime, which normally for entertainment purposes are considered as a multimedia files.

4. Media server configurator

   The software used at the host computer to broadcast the multimedia files

5. Streaming media player

   The software used at the client computer to stream the multimedia file from the host computer.

6. Ethereal

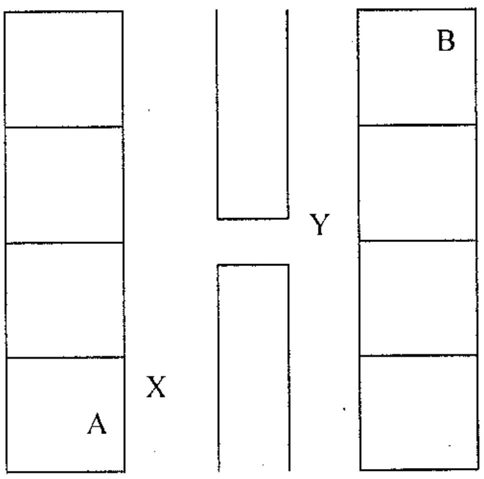
   The software used to evaluate the packet / data transfer rate in a wireless network.

7. Measuring tape

   A measuring tool to measure the distance between nodes

3.3 The Experiment Environment

All the experiments and troubleshooting of this project is done in the laboratories in block 22. The set up of the wireless network between nodes A, B, X, and Y are shown in Figure 3 where node A and node B are desktop with the USB wireless adapter while node X and node Y are laptop with wireless enabled (Intel Centrino®).



*The drawing is not according to scale

Figure 3: The top view of EE block 22 and the locations of all nodes

3.4 Setting Up The Wireless Local Area Network (WLAN)

An experiment was conducted to detect the Wireless network created by the 54 Mbps 802.11g wireless USB 2.0 adapters. A wireless local area network (WLAN) is created using the laptop (Intel Centrino®) with ad-hoc peer-to-peer connection. The wireless local area network is set up by simply give a network name (SSID) and configuring the network authentication to "open" and data encryption to "disable" so that no network key is required. The settings of the wireless local area network are as shown in Figure 4.

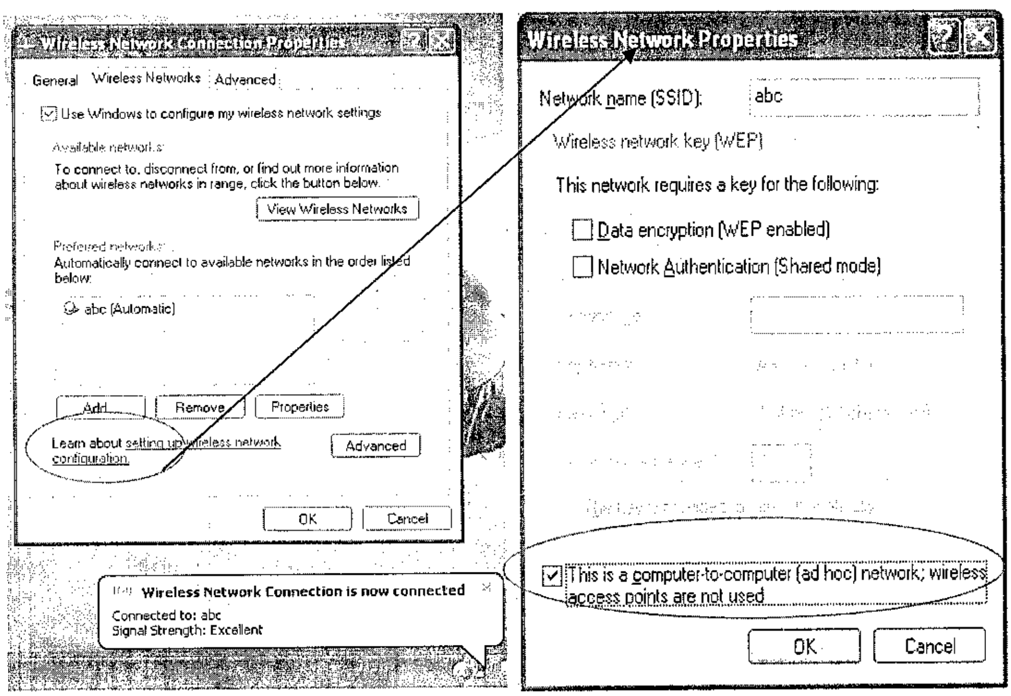


Figure 4: The setting of a wireless local area network.

To ensure that the computer does not connect to any access point within the coverage range, the option "This is a computer-to-computer (ad-hoc) network; wireless access points are not used" at the bottom must be checked as shown in Figure 4. The setting is completed by clicking the "OK" and an icon pop-up at the right bottom corner indicated the wireless network connection is now connected.

After the ad-hoc peer-to-peer wireless network is set up, other nodes, which are within the coverage range, can easily connect to the wireless network created. The desktop with the wireless USB adapter or any Intel Centrino® laptop shows the wireless network icon on the right bottom corner as shown in Figure 5.

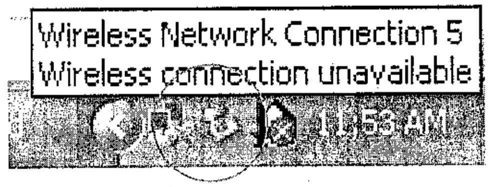


Figure 5: The icon of wireless network connection

The wireless network connection icon is double clicked. The window as in Figure 6 and Figure 7 shows the available network connection within the coverage range for the desktop with USB wireless adapter and laptop with Intel Centrino® separately. The specific network name is selected, thus, connection is made to the particular network by clicking on the connect button.

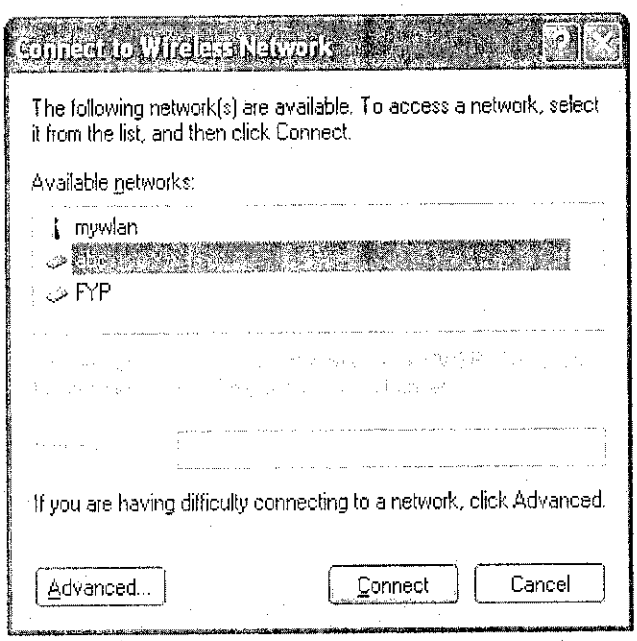


Figure 6: The Wireless network connection available (desktop - USB wireless adapter)

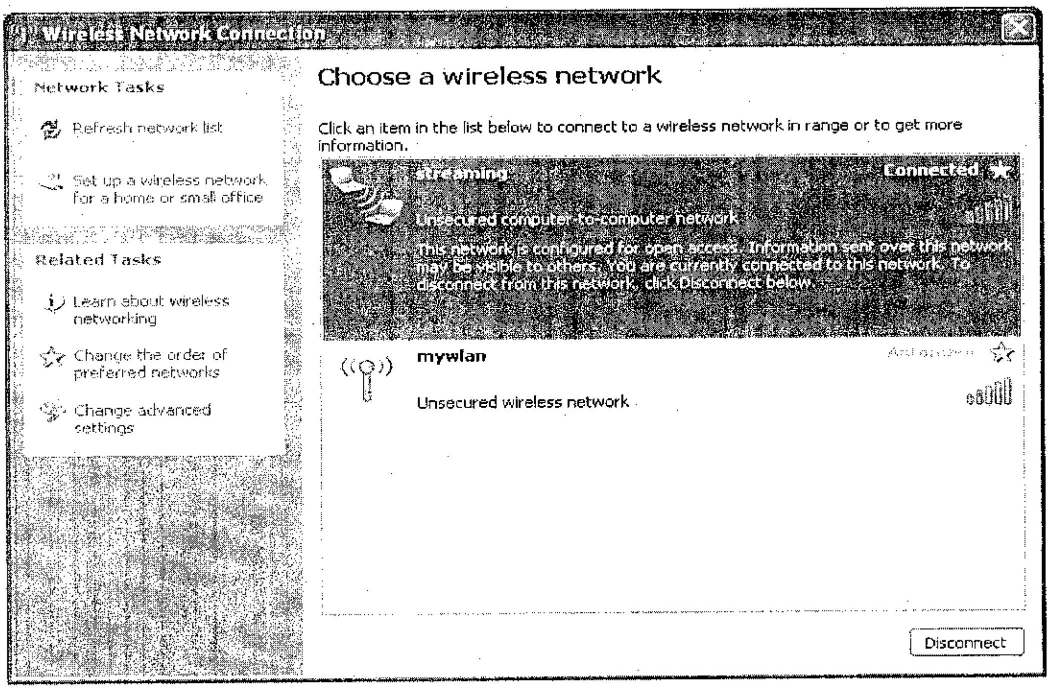


Figure 7: The Wireless network connection available (Intel Centrino® laptop)

After the devices are connected to the wireless network, it a pop up message appears on the right bottom corner to indicate the wireless network is connected. It is found that both nodes connected to the wireless network are automatically assigned with individual IP address as shown in Figure 8.

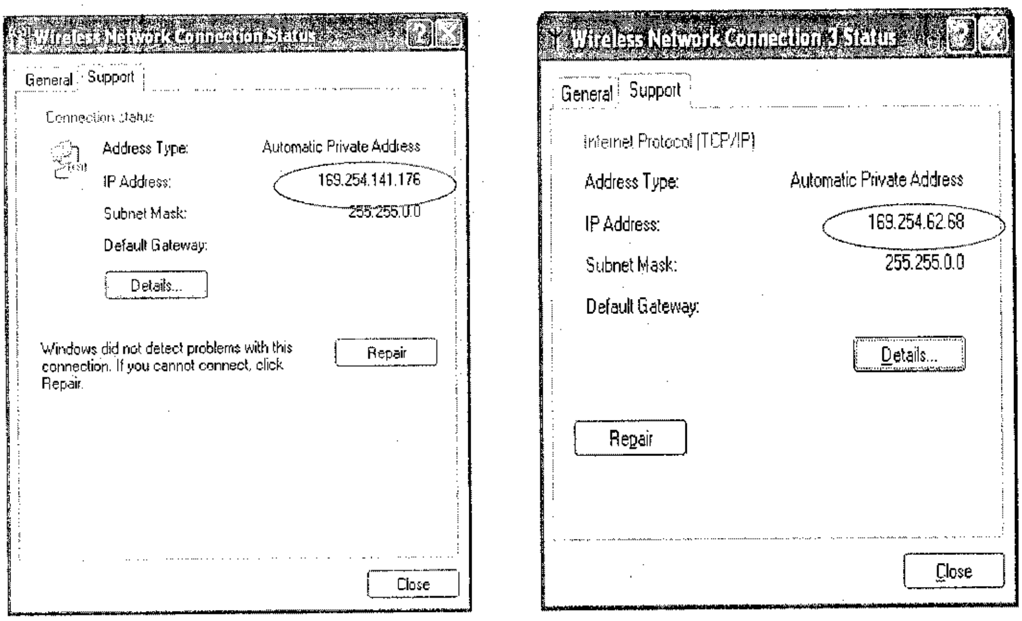


Figure 8: The Wireless network connection status of both nodes

3.5 Streaming Process

The general streaming process is shown in Figure 9. The wireless network is set up accordingly as mention in section 3.4. The file sharing and downloading is to ensure the stability of the wireless network created. The host computer as well as the client computer is installed with the software "media server configurator" and "streaming media player" separately, are configured accordingly. The host computer IP address is entered and the streaming process is initiated.

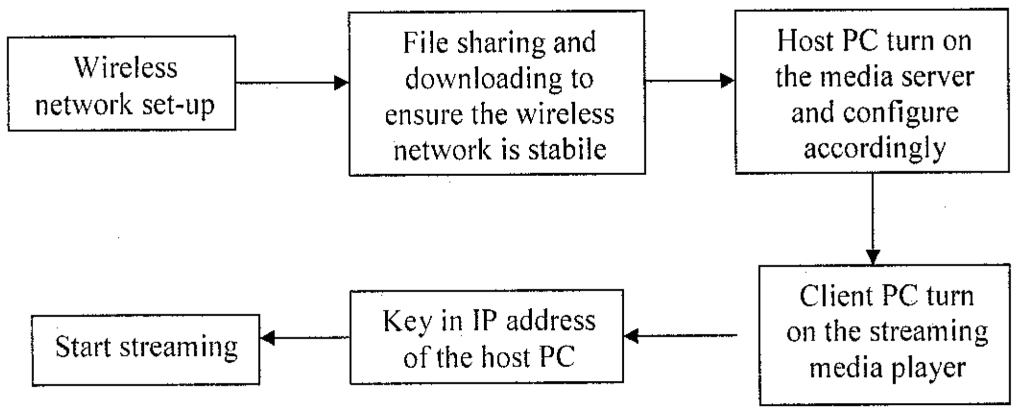


Figure 9: Steaming process procedures

3.5.1 Setting Up The Host Computer (Server)

The software "media server configurator" is installed in the host computer. To begin the streaming process, the software - media server configurator is started and a new virtual folder is added as shown in Figure 10. The virtual folder is added by browsing through the folder in the hard disk drive of the host computer where the multimedia file is stored. A description and folder name is required for the multimedia files folder. The other settings are left as the default options, as shown in Figure 11.

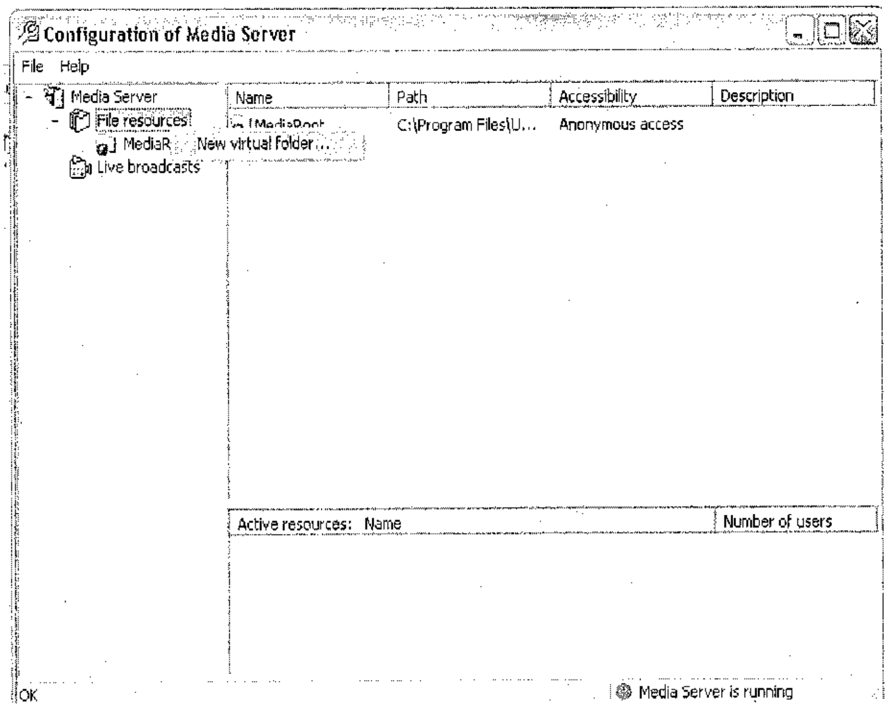


Figure 10: The media server configurator

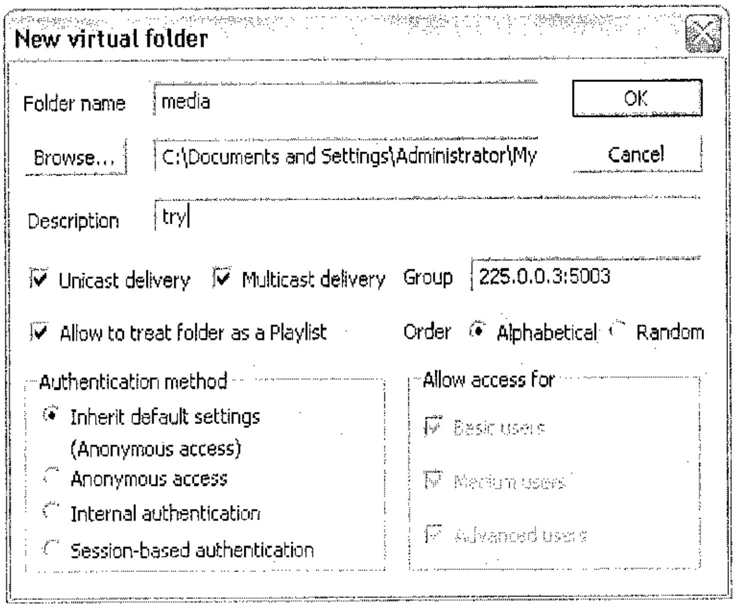


Figure 11: The virtual folder set-up

When the setting of the virtual folder is done, it shows the list of multimedia files in the particular location of the hard disk drive as in Figure 12. By right clicking on the folder name and choosing "start multicasting", the server starts to broadcast the multimedia files to the entire wireless network.

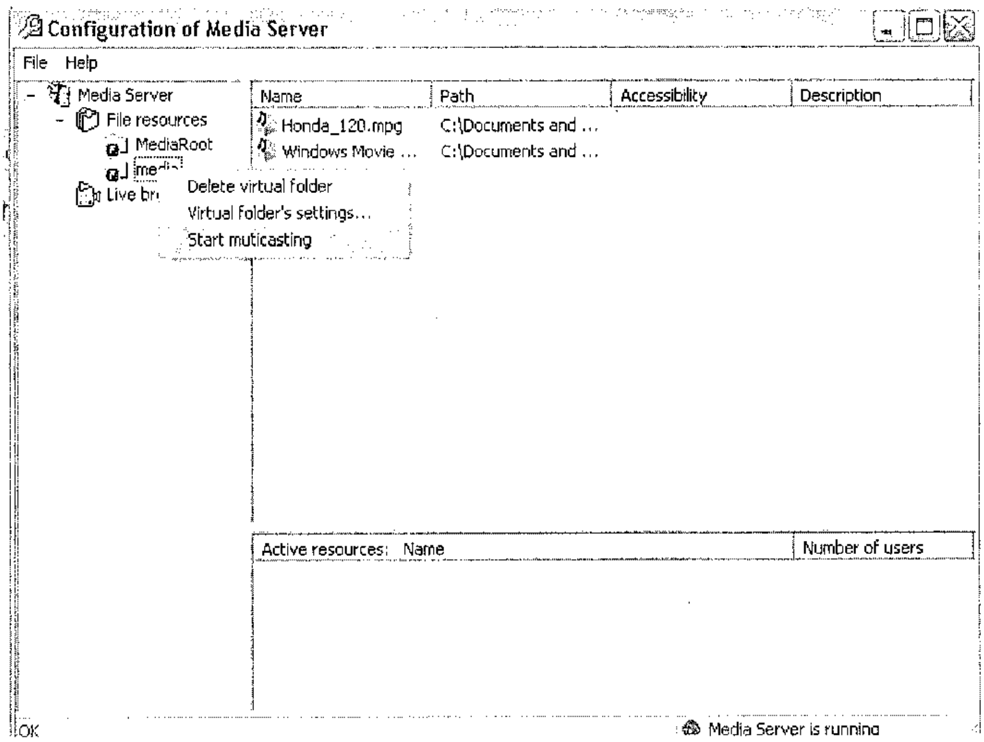


Figure 12: Broadcast the multimedia files from the host computer

3.5.2 Setting Up The Client Computers (nodes)

The client computer is installed with the software "streaming media player" in order to stream the multimedia files from the host computer. The streaming media player is started. In the "play" tab on the left top corner, the *Play remote playlist* is clicked and a window as in Figure 13 appears. The IP address of the media server is entered in the column provided. The other important information, which needs to be keyed in, is the folder name. The folder name is the virtual folder name in the media server. After all the information is entered in, the streaming process can be initiated by clicking on the play button of the streaming media player. The streaming media player streamed the multimedia file from the host computer as shown in Figure 14.

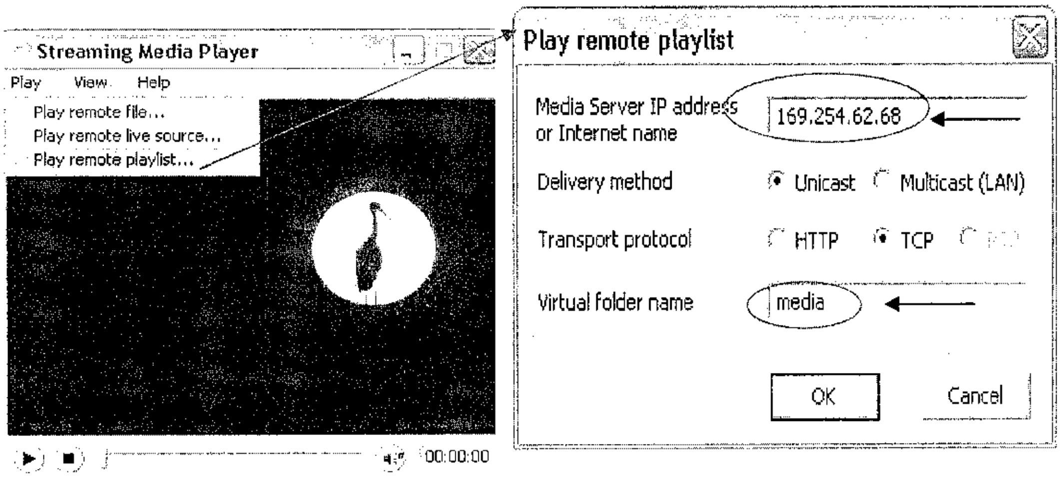


Figure 13: The streaming media player and the configuration.

Figure 14: The streaming media player streamed from the host computer.

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Experiment 1: Ad Hoc (Peer-to-peer) Wireless Network Streaming

1. An ad hoc wireless network is set up between Laptop X (Intel Centrino®) and Desktop A (USB wireless adapter) in the laboratory at EE block 22 as shown in Figure 15. (*Please refer to section 3.4 for setting up wireless network*).

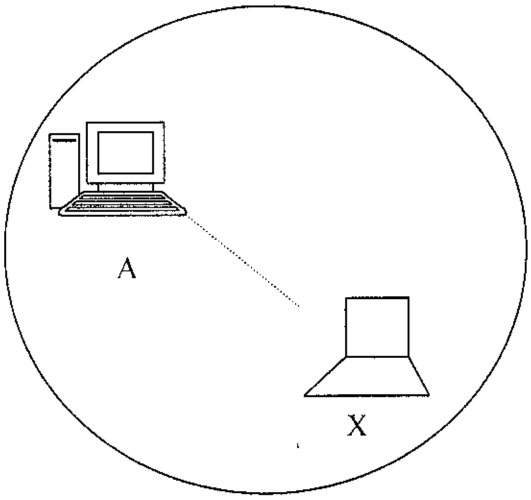


Figure 15: Ad-hoc Wireless Local Area Network

2. The streaming process as mentioned in section 3.5 is done within the wireless network created where Desktop A act as the media server while Laptop X streamed from the server.

The multimedia file streaming in ad hoc wireless network is successful as Laptop X (client) can stream the multimedia file smoothly from the Desktop A (host) provided Laptop X is within the coverage range of Desktop A. When the Laptop X is moved around within the coverage range, the two nodes stay connected and they are able to stream the multimedia files. The performance of the streaming process depends on the distance of node from the host. The distance between Desktop A and Laptop X is 1.80m and the data transfer rate is 5714 Kbit/s.

4.2 Experiment 2: Three Nodes Multi-hop Wireless Network Streaming

1. An ad hoc wireless network is set up between Laptop X (Intel Centrino®) and Desktop A (USB wireless adapter) in the laboratory at EE block 22 as shown in Figure 15.
2. The Laptop X is moved far away from the Desktop A until the wireless connection no longer exists. (*See Figure 16*)

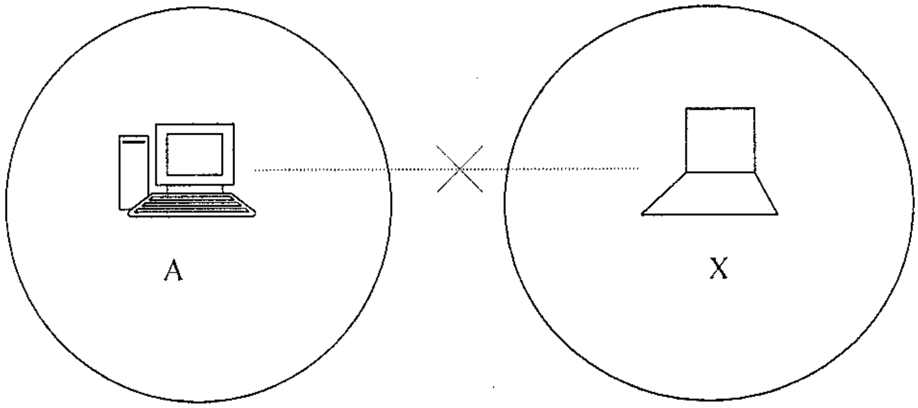


Figure 16: Two different networks with independent coverage range

3. An additional node Laptop Y (Intel Centrino®) is added in the middle of Desktop A and Laptop X as shown in Figure 17.

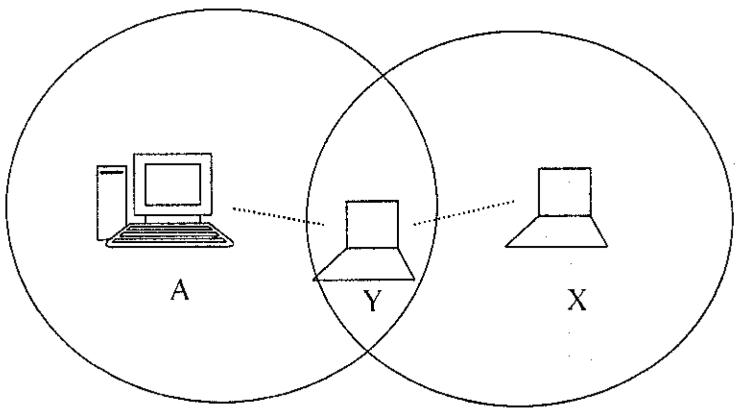


Figure 17: A multi-hop wireless local area network

4. The streaming process as mentioned in section 3.5 is done within the multi-hop wireless network created where Desktop A act as the media server while Laptop X and Laptop Y streamed from the server.

When Laptop X is moved out of the coverage range of Desktop A, the wireless connection no longer exists. Therefore, the streaming process fails to perform and both nodes have independent network with two different coverage ranges as shown in Figure 16. By adding in an additional node – Laptop Y, in the middle of Desktop A and Laptop X as shown in Figure 17, the Laptop Y acts as a "bridge" for Desktop A and Laptop X. All nodes (A, X and Y) stay connected together under the same network and the streaming process is successful within this network where Desktop A acts as the server while Laptop X and Y as receiving nodes. The distance between Desktop A and Laptop Y is 1.80m and the data transfer rate is 5714 Kbit/s while the distance between the receiving end node Laptop X and Desktop A is 15.78m and the data transfer rate is 3517 Kbit/s. This shows that the distance does affect the performance of multimedia streaming in WLAN.

4.3 Experiment 3: Four Nodes Multi-hop Wireless Network Streaming

1. A multi-hop wireless network is set up between Desktop A (USB wireless adapter), Laptop X and Laptop Y (Intel Centrino®) as shown in Figure 17.
2. An additional node Desktop B (USB wireless adapter) is added at the far end of the network as shown in Figure 18.

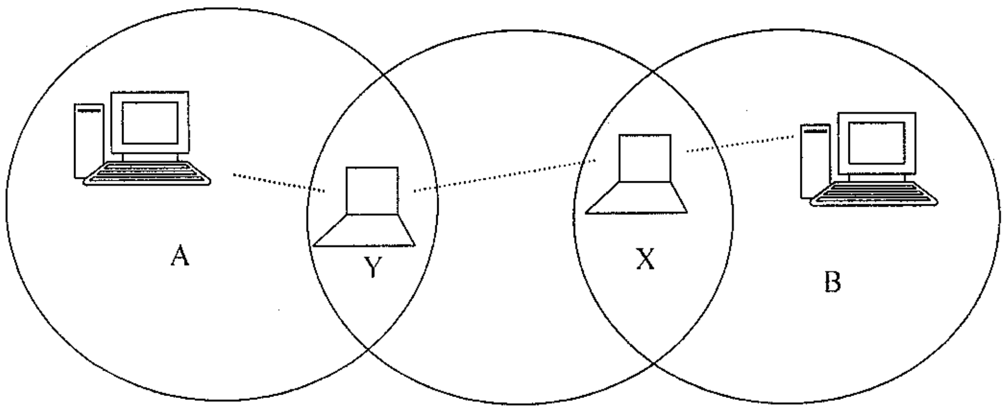


Figure 18: Multi-hop wireless local area network with four nodes

3. The streaming process as mentioned in section 3.5 is done within the multi-hop wireless network created where Desktop A act as the media server while Laptop X, Laptop Y, and Desktop B streamed from the server.
4. The distance between the host and the clients is measured.
5. The data transfer rate of every node is recorded and analyzed.

Table 1: The measurements of the data transfer rate in multi-hop wireless network

	A to B (far)	A to X (medium)	A to Y (near)
Distance (m)	29.38	15.78	1.80
Total packets sent	7988	7865	7924
Total time (s)	148	136	128
Data sent rate (packet/s)	53.97	57.83	61.91
Data received rate (Kbit/s)	865	3517	5714

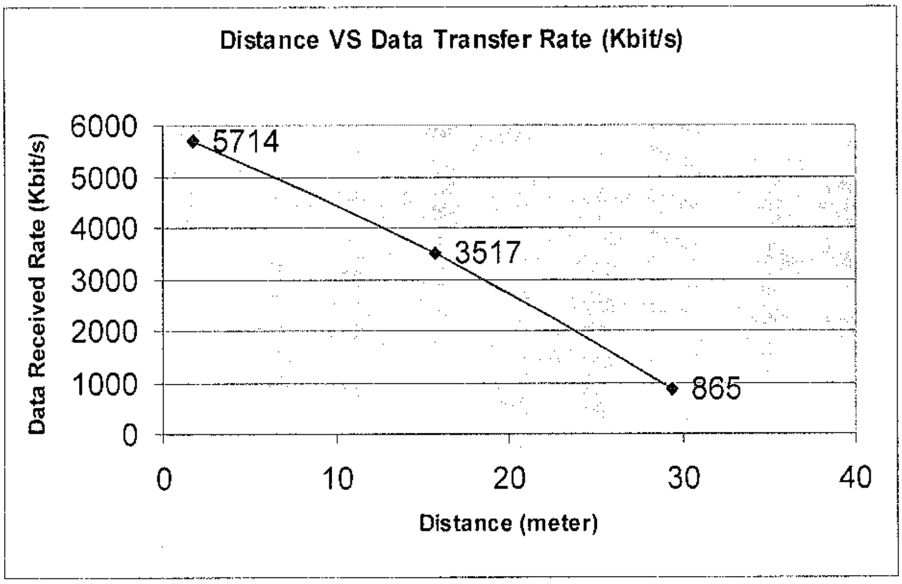


Figure 19: The distance VS data transfer rate (Kbit/s)

Desktop A and Desktop B are in two different networks, if Laptop X and Laptop Y are not placed in between. With Laptop X and Laptop Y acting as bridges, all nodes A, B, X, and Y are connected under the same network. It is found that the multimedia file can be successfully streamed between Desktop A and Desktop B.

The data transfer rate for different distances are investigated to evaluate the performance of the multi-hop wireless network. A two minutes video clip is streamed and the data transfer rate are observed. This is summarized in table 1. Figure 19 shows the graph is plotted from the result in table 1 and it shows that the distance of the node from the host does affect the data received rate at the clients. The nearer the node toward the host, the higher the data transfer rate and vise versa.

4.4 Experiment 4: Multi-hop Wireless Network Streaming without Access Point

1. A wireless network is created by Laptop Y (Intel Centrino®).
2. Laptop Y is moved near to Desktop A (USB wireless adapter) and Desktop A establishes the connection to the wireless network.
3. After Desktop A is connected, Laptop Y is moved to the location of Desktop B (USB wireless adapter), which is far away from Desktop A.
4. This will cause Desktop A to lose connection to the network because it is outside the coverage range of the wireless network. However, now, Desktop B is connected to the network. The scenario is clearly illustrated in Figure 20.

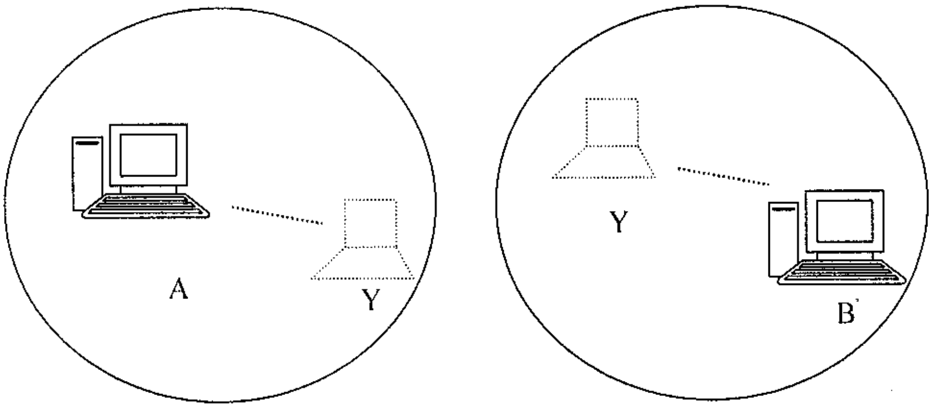


Figure 20: The connection of laptop Y to desktop A and desktop B

5. The Laptop Y is disconnected from the wireless network.
6. An additional node Laptop X (Intel Centrino®) is added in between Desktop A and Desktop B and a distance 1m away from the Desktop B as shown in Figure 21.

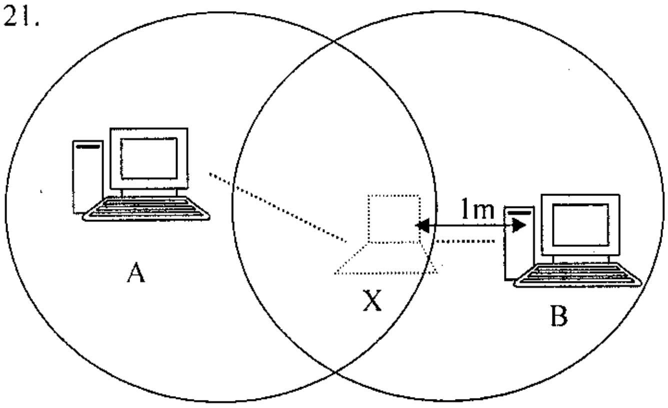


Figure 21: Multi-hop wireless local area network without access point.

7. The streaming process as mentioned in section 3.5 is done within the multi-hop wireless network created where Desktop A act as the media server while Laptop X and Desktop B streamed from the server.
8. The data transfer rate of the receiving node (Desktop B) is recorded in table 2.
9. The distance between the bridge (Laptop X) and the receiving node (Desktop B) is changed to 2m, 3m, 4, and 5m.
10. The data transfer rates of the receiving node for every distance are recorded in table 2.

Table 2: The data transfer rate in multi-hop wireless network (moving bridge)

Distance between X and B	**1m**	**2m**	**3m**	**4m**	**5m**
Total packet received	-	14568	13856	14540	15238
Total time elapsed (s)	-	367	198	426	498
Received rate (packets/s)	-	39.69	69.98	34.13	30.60
Received rate (Kbits)	-	531	1157	438	379

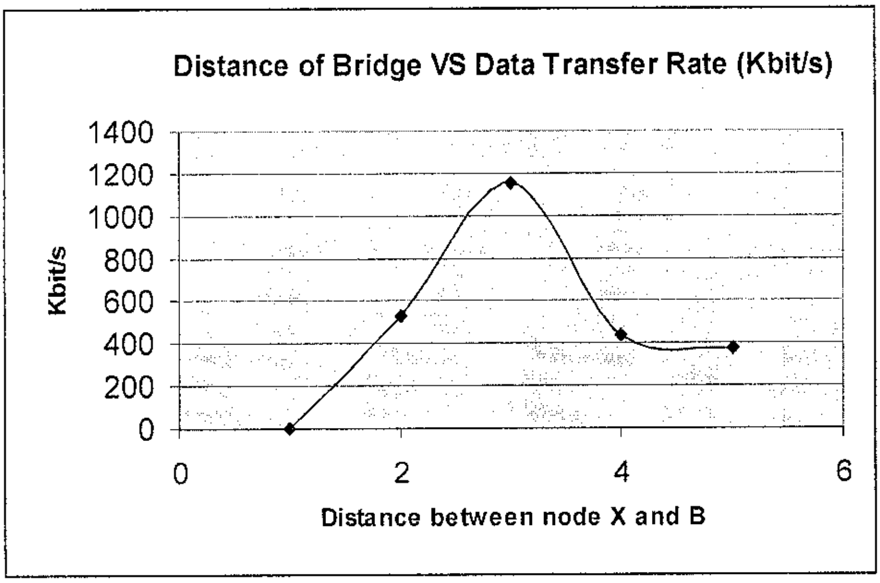


Figure 22: The distance of bridge from the receiving end node VS data transfer rate (Kbit/s)

The set up of the wireless network by using another node - Laptop Y, and disconnect it later on, is to provide Desktop A and Desktop B two independent wireless network. An additional node – Laptop X is then placed in between Desktop A and Desktop B as a bridge. The usage of the extra node Laptop Y to create the network is to avoid the existence of the access point where the Laptop Y is the originator of the wireless network, and thus acts as an access point. If this is the case then the wireless network created is not a purely ad hoc network, as it still needs a central main node for the network to exist.

The Laptop X is placed in between Desktop A and Desktop B as a bridge to connect all three nodes under the same wireless network. The streaming process is successfully done from Desktop A to Desktop B. This shows that the wireless network created is purely ad hoc and no access point is needed.

The performance of the streaming is observed when the bridge is placed at different distance from the receiving node and the result is summarized in table 2. It is found that streaming process is failed to perform when the bridge is placed about 1 meter from the receiving node. This is probably caused by the bridge is too far away from the host as it totally lost connection from the wireless network. The performance of the streaming process is optimum when the distance between the bridge and the receiving node is at 3 meters. The performance of streaming process degrades when the bridge is moved further than 3 meter away from the receiving node. The scenario is clearly illustrated in Figure 22.

CHAPTER 5
CONCLUSION

The advantage of the streaming process allows the users to download and playback the multimedia file simultaneously. Thus, no big capacity of disk space required for storing an unknown content multimedia file. Streaming can be used for multimedia distribution without users having the illegal copies of the file. It allows the owner of the file to share the contents but then user would not be able to own the file.

The multimedia file must be streamed via two or more Wi-Fi enabled computer without passing through any access point. A node that is totally outside the coverage range of the network can also stream the multimedia files by using multi-hop wireless network passing through a bridge. The distance of the nodes from the host does affect the data transfer rate and thus affecting the performance of the streaming. The nearer the client node to the host, the higher the data transfer rate and vice versa. Every device has different signal strength and coverage range. The experiment results can be more accurate if all the wireless devices used are of the same model. The distance between the bridge and the receiving end node is about 3 meters to have the best performance of streaming process in multi-hop wireless network.

The streaming process is improved with no limitation of nodes. Therefore, a node outside the range can also stream by multi-hop networking. The signal strength of the wireless network can be improved to do larger distance multimedia files streaming. To improve this project, it is proposed that software will allow the users to choose any of the multimedia files in the playlist to be streamed rather than just playing all the multimedia files in order.

REFERENCES

[1] J.Trulove, *Build Your Own Wireless LAN with projects,* 2002, McGraw-Hill, New York.

[2] A. Santamaria, F.J.Lopez Hernandez, *Wireless LAN Standards and Applications,* 2002, Artech House Publisher, Boston, London

[3] M. Iiyas, *The handbook of Ad-Hoc Networks*, 2002, CRC Press, Florida

[4] Wikipedia, the free encyclopedia, "Wireless LAN", Jan 2006, http://en.wikipedia.org/wiki/WLAN

[5] A. Santamaria, F.J.Lopez Hernandez, *Wireless LAN Systems*, 1994, Artech House Publisher, Boston, London

[6] C.K. Toh, *Ad Hoc Mobile Wireless Networks, Protocols and systems,* 2002, Prentice Hall, New Jersey

[7] M.Jakobsson, J.P.Hubaux and L.Buttyan, *A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, Proceedings of Seventh International Financial Cryptography Conference (FC),* 2003, Gosier, Guadeloupe

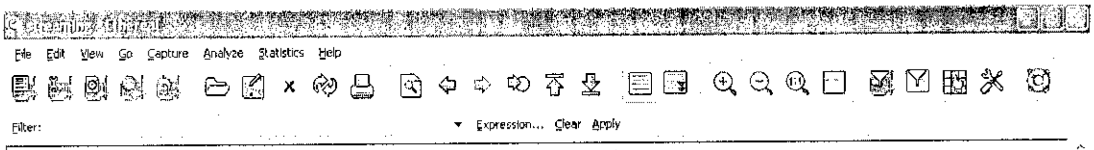
[8] D.Moore and J.Hebeler, *Peer-to-Peer: Building Secure, Scalable, and Manageable Networks,* 2002, Mc Graw Hill / Osborne

[9] E.M.Belding-Royer, K.A.Agba, G.Pujolle, *Mobile and Wireless Communications Networks,* 2004, Springer, New York

[10] Video LAN-free software and open source video streaming solution for every OS, 6th May 2006 (latest update), http://www.videolan.org

APPENDICES

The results of packets transfer in USB wireless adapter



No.	Time	Source	Destination	Protocol	Info
1053	38.032918	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1054	38.220411	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1055	38.220579	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1056	38.231132	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1057	38.231184	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1058	38.267871	169.254.141.176	Broadcast	ARP	Who has 169.254.45.10? Tell 169.254.141.176
1059	38.267891	169.254.45.10	169.254.141.176	ARP	169.254.45.10 is at 00:12:bf:19:48:a4
1060	38.269834	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
1061	38.269878	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS…
1062	38.271828	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=1 Ack=1 Win=17520 Len=0
1063	38.271997	169.254.141.176	169.254.45.10	TCP	[TCP segment of a reassembled PDU]
1064	38.330783	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1065	38.330935	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1066	38.341524	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1067	38.341690	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1068	38.463496	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=1 Ack=17 Win=17504 Len=0
1069	38.553030	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1070	38.553258	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1071	38.588963	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1072	38.589150	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1073	38.599321	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1074	38.599415	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1075	38.747541	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1076	38.747781	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1077	38.780967	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1078	38.781120	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1079	38.818116	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1080	38.818256	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1081	38.904762	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [PSH, ACK] Seq=1 Ack=17 Win=17504 Len=311
1082	38.985920	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1083	38.986102	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1084	38.986499	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=312 Ack=17 Win=17504 Len=1460
1085	38.986532	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
1086	39.008735	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=1772 Win=17520 Len=0
1087	39.030264	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=2346 Ack=17 Win=17504 Len=1460
1088	39.030353	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [PSH, ACK] Seq=3806 Ack=17 Win=17504 Len=5…
1089	39.031204	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1090	39.031323	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1142	40.261550	169.254.141.176	169.254.45.10	TCP	[TCP Window Update] 1045 > 5119 [ACK] Seq=17 Ack=19004
1143	40.261597	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=19004 Ack=17 Win=17504 Len=1460
1144	40.261670	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=20464 Ack=17 Win=17504 Len=1460
1145	40.262542	169.254.141.176	169.254.45.10	TCP	[TCP Window Update] 1045 > 5119 [ACK] Seq=17 Ack=19004
1146	40.262555	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [PSH, ACK] Seq=21924 Ack=17 Win=17504 Len=1…
1147	40.262575	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=23384 Ack=17 Win=17504 Len=1460
1148	40.262591	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [PSH, ACK] Seq=24844 Ack=17 Win=17504 Len=1…
1149	40.262607	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=26304 Ack=17 Win=17504 Len=1460
1150	40.262622	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=27764 Ack=17 Win=17504 Len=1460
1151	40.262642	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=29224 Ack=17 Win=17504 Len=1460
1152	40.262667	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=30684 Ack=17 Win=17504 Len=1460
1153	40.262685	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=32144 Ack=17 Win=17504 Len=1460
1154	40.264647	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1155	40.268522	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=21924 Win=17520 Len=0
1156	40.268548	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=33604 Ack=17 Win=17504 Len=1460
1157	40.268568	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=35064 Ack=17 Win=17504 Len=1460
1158	40.268584	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=36524 Ack=17 Win=17504 Len=1460
1159	40.269513	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=23384 Win=17520 Len=0
1160	40.269557	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=37984 Ack=17 Win=17504 Len=1460
1161	40.269575	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1045 [ACK] Seq=39444 Ack=17 Wi…
1162	40.275629	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
1163	40.281518	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=26304 Win=17520 Len=0
1164	40.281548	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=40904 Ack=17 Win=17504 Len=1460
1165	40.281568	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1045 [PSH, ACK] Seq=42364 Ack…
1166	40.291517	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=29224 Win=17520 Len=0
1167	40.291546	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [ACK] Seq=43824 Ack=17 Win=17504 Len=1460
1168	40.291567	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1045 [ACK] Seq=45284 Ack=17 Wi…
1169	40.294849	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=32144 Win=17520 Len=0
1170	40.294895	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [PSH, ACK] Seq=46744 Ack=17 Win=17504 Len=1…
1171	40.294925	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1045 [ACK] Seq=48204 Ack=17 Wi…
1172	40.297593	169.254.141.176	169.254.45.10	TCP	1045 > 5119 [ACK] Seq=17 Ack=35064 Win=17520 Len=0
1173	40.297638	169.254.45.10	169.254.141.176	TCP	5119 > 1045 [PSH, ACK] Seq=49664 Ack=17 Win=17504 Len=4…
25637	[illegible]	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=[illegible] Win=17520 Len=0
25638	179.339409	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=892716 Ack=17 Win=17504 Len=1460
25639	179.339426	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=894176 Ack=17 W…
25640	179.341376	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=879576 Win=17520 Len=0
25641	179.341399	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=895636 Ack=17 W…
25642	179.343425	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=882496 Win=17520 Len=0
25643	179.343453	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [PSH, ACK] Seq=897096 Ack=17 Win=17504 Len…
25644	179.343478	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=898556 Ack=17 W…
25645	179.348406	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
25646	179.348563	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=885416 Win=17520 Len=0
25647	179.348584	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=900016 Ack=17 Win=17504 Len=1460
25648	179.348604	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=901476 Ack=17 W…
25649	179.360528	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=888336 Win=17520 Len=0
25650	179.360559	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=902936 Ack=17 Win=17504 Len=1460
25651	179.360584	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=904396 Ack=17 W…
25652	179.361284	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=891256 Win=17520 Len=0
25653	179.361296	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=905856 Ack=17 Win=17504 Len=1460
25654	179.361311	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=907316 Ack=17 W…
25655	179.369284	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=894176 Win=17520 Len=0
25656	179.369299	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=908776 Ack=17 Win=17504 Len=1460
25657	179.369314	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=910236 Ack=17 W…
25658	179.370380	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=897096 Win=17520 Len=0

25904	179.696229	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1111504 Win=17520 Len=0
25905	179.696266	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [PSH, ACK] Seq=1127564 Ac
25906	179.701221	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1114424 Win=17520 Len=0
25907	179.701242	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=1129024 Ack=17 Win=17504 Len=146
25908	179.701297	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [PSH, ACK] Seq=1130484 Ac
25909	179.704212	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1117344 Win=17520 Len=0
25910	179.704226	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [PSH, ACK] Seq=1131944 Ack=17 Win=17504 Ler
25911	179.704274	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=1133404 Ack=17
25912	179.711221	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1120264 Win=17520 Len=0
25913	179.711252	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [PSH, ACK] Seq=1134864 Ack=17 Win=17504 Ler
25914	179.711312	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [PSH, ACK] Seq=1136324 Ack=17 Win=17504 Ler
25915	179.711404	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1123184 Win=17520 Len=0
25916	179.712225	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1126104 Win=17520 Len=0
25917	179.714210	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=1129024 Win=17520 Len=0
27438	182.052027	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2461855 Ack=17
27439	182.052946	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
27440	182.055847	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2448715 Win=17520 Len=0
27441	182.055872	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2463315 Ack=17 Win=17504 Len=146
27442	182.055891	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2464775 Ack=17
27443	182.058914	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
27444	182.062840	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2451635 Win=17520 Len=0
27445	182.062858	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2466235 Ack=17 Win=17504 Len=146
27446	182.062874	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2467695 Ack=17
27447	182.063934	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2453095 Win=17520 Len=0
27448	182.063973	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2469155 Ack=17
27449	182.065982	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2456015 Win=17520 Len=0
27450	182.066013	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2470615 Ack=17 Win=17504 Len=146
27451	182.066036	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2472075 Ack=17
27452	182.069576	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
27453	182.072901	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
27454	182.073029	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2457475 Win=17520 Len=0
27455	182.073063	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2473535 Ack=17
27456	182.073848	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2460395 Win=17520 Len=0
27457	182.073877	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [PSH, ACK] Seq=2474995 Ack=17 Win=17504 Ler
27458	182.073900	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2476455 Ack=17
27459	182.076341	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2463315 Win=17520 Len=0
27460	182.076379	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2477915 Ack=17 Win=17504 Len=146
27461	182.076404	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2479375 Ack=17
27462	182.079946	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2466235 Win=17520 Len=0
27463	182.079971	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2480835 Ack=17 Win=17504 Len=146
27464	182.079994	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2482295 Ack=17
27465	182.085835	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2469155 Win=17520 Len=0
27466	182.085854	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2483755 Ack=17 Win=17504 Len=146
27467	182.085872	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2485215 Ack=17
27468	182.093822	169.254.141.176	169.254.45.10	TCP	1048 > 5119 [ACK] Seq=17 Ack=2472075 Win=17520 Len=0
27469	182.093839	169.254.45.10	169.254.141.176	TCP	5119 > 1048 [ACK] Seq=2486675 Ack=17 Win=17504 Len=146
27470	182.093888	169.254.45.10	169.254.141.176	TCP	[TCP Window Full] 5119 > 1048 [ACK] Seq=2488135 Ack=17

Figure 23: The SMC results

The results of packets transfer in Intel Centrino ® laptop

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
5812	99.175973	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5813	99.176817	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5814	99.256537	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5815	99.256733	169.254.141.176	169.254.45.10	TCP	1050 > 5119 [FIN, ACK] Seq=0 Ack=2803124 Win=16528 Len=0
5816	99.257395	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5817	99.259089	169.254.45.10	169.254.141.176	TCP	5119 > 1050 [ACK] Seq=2803124 Ack=1 Win=17504 Len=0
5818	99.303889	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5819	99.304272	169.254.45.10	169.254.141.176	TCP	5119 > 1050 [FIN, ACK] Seq=2803124 Ack=1 Win=17504 Len=0
5820	99.304291	169.254.141.176	169.254.45.10	TCP	1050 > 5119 [ACK] Seq=1 Ack=2803125 Win=16528 Len=0
5821	99.345783	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5822	99.368270	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
5823	99.370354	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460
5824	99.370388	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=1 Ack=1 Win=17520 Len=0
5825	99.370454	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=16
5826	99.492415	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=1 Ack=17 Win=17504 Len=0
5827	99.589918	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=1 Ack=17 Win=17504 Len=323
5828	99.591671	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5829	99.592599	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5830	99.686422	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=324 Ack=17 Win=17504 Len=1460
5831	99.686488	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=1784 Win=17520 Len=0
5832	99.687968	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5833	99.688920	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5834	99.690250	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5835	99.713697	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5836	99.741489	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=1784 Ack=17 Win=17504 Len=1460
5837	99.742935	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=3244 Ack=17 Win=17504 Len=1460
5838	99.742968	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=4704 Win=17520 Len=0
5839	99.744364	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=4704 Ack=17 Win=17504 Len=1460
5840	99.747368	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=6164 Ack=17 Win=17504 Len=1460
5841	99.747383	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=7624 Win=17520 Len=0
5842	99.749088	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=7624 Ack=17 Win=17504 Len=1460
5843	99.751043	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=9084 Ack=17 Win=17504 Len=1460
5844	99.751056	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=10544 Win=17520 Len=0
5845	99.752498	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=10544 Ack=17 Win=17504 Len=1460
5846	99.753958	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [ACK] Seq=12004 Ack=17 Win=17504 Len=1460
5847	99.753973	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=13464 Win=17520 Len=0
5848	99.755666	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=13464 Ack=17 Win=17504 Len=1460
5849	99.755693	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=14924 Win=17520 Len=0
5857	99.858793	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=19816 Ack=17 Win=17504 Len=1460
5858	99.874810	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=21276 Win=17520 Len=0
5859	99.875204	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=21276 Ack=17 Win=17504 Len=40
5860	99.920772	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5861	99.921733	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5862	99.923130	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5863	99.923981	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5864	99.925514	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=21316 Ack=17 Win=17504 Len=1460
5865	99.925541	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=22776 Win=17520 Len=0
5866	99.926125	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=22776 Ack=17 Win=17504 Len=199
5867	99.927906	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=22975 Ack=17 Win=17504 Len=1460
5868	99.927920	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=24435 Win=17520 Len=0
5869	99.928263	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=24435 Ack=17 Win=17504 Len=17
5870	99.965365	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5871	99.966127	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5872	100.005662	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=24452 Ack=17 Win=17504 Len=1460
5873	100.005684	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=25912 Win=17520 Len=0
5874	100.006661	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=25912 Ack=17 Win=17504 Len=555
5875	100.008257	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5876	100.009506	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5877	100.010682	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=26467 Ack=17 Win=17504 Len=808
5878	100.010696	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=27275 Win=16157 Len=0
5879	100.049260	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5880	100.050097	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5881	100.051135	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=27275 Ack=17 Win=17504 Len=840
5882	100.094347	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5972	101.405757	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5973	101.406500	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
5974	101.431365	169.254.45.10	169.254.141.176	TCP	5119 > 1055 [PSH, ACK] Seq=61461 Ack=17 Win=17504 Len=1460
5975	101.431387	169.254.141.176	169.254.45.10	TCP	1055 > 5119 [ACK] Seq=17 Ack=62921 Win=17520 Len=0
13518	124.443524	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5787382 Ack=17 Win=17504 Len=1460
13519	124.445137	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5788842 Ack=17 Win=17504 Len=1460
13520	124.445152	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5790302 Win=17520 Len=0
13521	124.448941	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5790302 Ack=17 Win=17504 Len=1460
13522	124.450675	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [PSH, ACK] Seq=5791762 Ack=17 Win=17504 Len=1460
13523	124.450705	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5793222 Win=17520 Len=0
13524	124.452419	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5793222 Ack=17 Win=17504 Len=1460
13525	124.454416	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5794682 Ack=17 Win=17504 Len=1460
13526	124.454429	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5796142 Win=17520 Len=0
13527	124.455925	169.254.45.10	169.254.141.176	DCERPC	Alter_context: call_id: 67111168, 4 context items, 1st UUID:
13528	124.457659	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5797602 Ack=17 Win=17504 Len=1460
13529	124.457673	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5799062 Win=17520 Len=0
13530	124.459320	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5799062 Ack=17 Win=17504 Len=1460
13531	124.460869	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5800522 Ack=17 Win=17504 Len=1460
13532	124.460884	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5801982 Win=17520 Len=0
13533	124.462882	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5801982 Ack=17 Win=17504 Len=1460
13534	124.464424	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5803442 Ack=17 Win=17504 Len=1460
13535	124.464463	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5804902 Win=17520 Len=0
13536	124.466035	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
13537	124.467240	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
13538	124.468659	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
13539	124.470055	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5804902 Ack=17 Win=17504 Len=1460
13540	124.471752	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5806362 Ack=17 Win=17504 Len=1460
13541	124.471784	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5807822 Win=17520 Len=0
13542	124.473225	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5807822 Ack=17 Win=17504 Len=1460
13543	124.475247	169.254.45.10	169.254.141.176	TCP	5119 > 1056 [ACK] Seq=5809282 Ack=17 Win=17504 Len=1460
13544	124.475261	169.254.141.176	169.254.45.10	TCP	1056 > 5119 [ACK] Seq=17 Ack=5810742 Win=17520 Len=0

[illegible]	[illegible]	[illegible]	[illegible]	TCP	[illegible]
74393	446.168946	169.254.45.10	169.254.141.176	TDS	Unknown Packet Type: 0 (Not last buffer) (Not last buffer) (ı
74394	446.168958	169.254.141.176	169.254.45.10	TCP	1064 > 5119 [ACK] Seq=18 Ack=17385431 Win=17520 Len=0
74395	446.170467	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
74396	446.172134	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
74397	446.172148	169.254.141.176	169.254.45.10	TCP	1064 > 5119 [ACK] Seq=18 Ack=17388351 Win=17520 Len=0
74398	446.175612	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
74399	446.177277	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
74400	446.177296	169.254.141.176	169.254.45.10	TCP	1064 > 5119 [ACK] Seq=18 Ack=17391271 Win=17520 Len=0
74401	446.178690	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74402	446.179865	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
74403	446.180772	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74404	446.185147	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74405	446.187934	169.254.45.10	169.254.141.176	TCP	[TCP segment of a reassembled PDU]
74406	446.187955	169.254.141.176	169.254.45.10	TCP	1064 > 5119 [ACK] Seq=18 Ack=17392263 Win=16528 Len=0
74407	446.227637	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74408	446.228531	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74409	446.419264	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74410	446.420004	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74411	446.437135	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74412	446.438037	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74413	446.506178	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x1a471868
74414	446.539108	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74415	446.539844	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74416	446.550491	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74417	446.551374	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74418	446.746956	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001
74419	446.752297	169.254.45.10	225.0.0.1	UDP	Source port: 1254 Destination port: 5001

Figure 24: The ACER laptop results