Enhancing Teaching and Learning Wi-Fi Networking using Limited Resources to Undergraduates

Nurul I. Sarkar, Auckland University of Technology, Auckland, New Zealand

ABSTRACT

Motivating students to learn Wi-Fi (wireless fidelity) wireless networking to undergraduate students is often difficult because many students find the subject rather technical and abstract when presented in traditional lecture format. This paper focuses on the teaching and learning aspects of Wi-Fi networking using limited hardware resources. It provides a walk-through tutorial on setting up Wi-Fi networks using wireless laptops and access points. Students can easily set up and configure Wi-Fi networks using relatively few computing resources to learn networking concepts more effectively. By measuring the key performance metrics such as network throughput and response times, students are able to gain a deeper understanding of Wi-Fi network performance and related issues. The effectiveness of these Wi-Fi practical learning activities has been evaluated both formally by students and informally in discussion within the teaching team. This paper describes the overall effectiveness of teaching and learning Wi-Fi network fundamentals using limited resources.

Keywords: *Hardware Resources, Network Throughput, Response Times, Undergraduate Students, Wireless Fidelity (Wi-Fi) Networking*

INTRODUCTION

Wireless fidelity (Wi-Fi) networks have been gaining in popularity, both in business and in home networking applications (Hiertz et al., 2010; N. Prasad & Prasad, 2002; R. Prasad & Ruggieri, 2003). With the growing proliferation of mobile equipment, this trend is likely to continue in the future. It is therefore important that undergraduate students of Network Technologies should be exposed to Wi-Fi fundamentals as part of the curriculum.

Many students find that Wi-Fi networking is rather abstract and difficult to understand when presented in traditional lecture format. The apparently overwhelming complexity of the underlying concepts of Wi-Fi often intimidates students. This perception can easily discourage the students from learning in-depth this otherwise exciting and rewarding subject.

DOI: 10.4018/ijwltt.2013100101

This paper addresses issues of student learning introductory wireless networking courses and provides hands-on learning activities on Wi-Fi networking using low-cost wireless cards and access points (APs). It provides a tutorial to guide students in setting up Wi-Fi networks using relatively few computing resources. Although a host of problems are to be expected, given the technical limitations of commercially available hardware, students are encouraged to gain a hands-on practical learning experience in setting up and configuring Wi-Fi networks. The paper also discusses the effectiveness of student learning and comprehension using Wi-Fi based projects.

Wi-Fi technologies are rapidly expanding over the last few years. To meet the users demand for high performance Wi-Fi, 802.11n has been standardized by IEEE in 2009. The 802.11n working group has focused on increasing network throughput and the overall system capacity (*IEEE 802.11n-2009 Amendment 5: Enhancements for Higher Throughput*). Prasad and Prasad (2001) highlight the potential applications of Wi-Fi such as teleconferencing, tele-surveillance, and video-on-demand operating on wireless network backbones. Further developments in capacity (i.e. throughput) and reliability will push these technologies to be used as next generation wireless networks.

The further research and development in high-speed Wi-Fi networking will open an opportunity for students to gain a thorough knowledge and understanding of the technology. An overview of the Wi-Fi technology is presented to help students to develop better understanding and significance of Wi-Fi technology from a technical standpoint. While Wi-Fi brings many benefits to corporate and home network users, the four main benefits of Wi-Fi are highlighted below (*802.11ac: The Fifth Generation of Wi-Fi (Technical White Paper)*; *First New Zealand 1Gbps wireless connect goes to IRL*; *IEEE 802.11s: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Simple Efficient Extensible Mesh (SEE-Mesh) Proposal.*; *What is a Wireless LAN?*):

- **Mobility:** Wi-Fi can provide users with real-time information within the organization without the restrictions inherent with physical connections;
- **Flexibility and Simplicity:** The W-Fi installation does not involved the tedious work of pulling cables through walls and ceilings. It allows access from places unreachable by network cables;
- **Cost:** Overall the installation cost of Wi-Fi is lower than wired LAN. The discrepancy is even higher in dynamic environments requiring frequent moves and changes;
- **Scalability:** W-Fi can be configured relatively easily because there is no physical network cables are required.

Although wireless networks may never completely replace wired networks, they will gain in importance as business assets in the future. Howard (2002) reports that the use of wireless networks for mobile Internet access is also becoming big business, as is indicated by the rising number of wireless internet service providers in the United States. The increasing number of public hotspots also opens the possibility of providing continuous connection to a roaming business traveler (Vaughan-Nichols, 2003).

OVERVIEW OF WI-FI TECHNOLOGY

A wireless network is a data communications system, which uses electromagnetic media such as radio or infrared waves instead of cables. Wireless networks are implemented either to complement or as an alternative to a wired network.

As discussed earlier, the most prominent feature of Wi-Fi is mobility, which provides users with freedom of movement while maintaining connectivity. Flexibility is another advantage of Wi-Fi because it allows connectivity to places physically inaccessible to network cables.

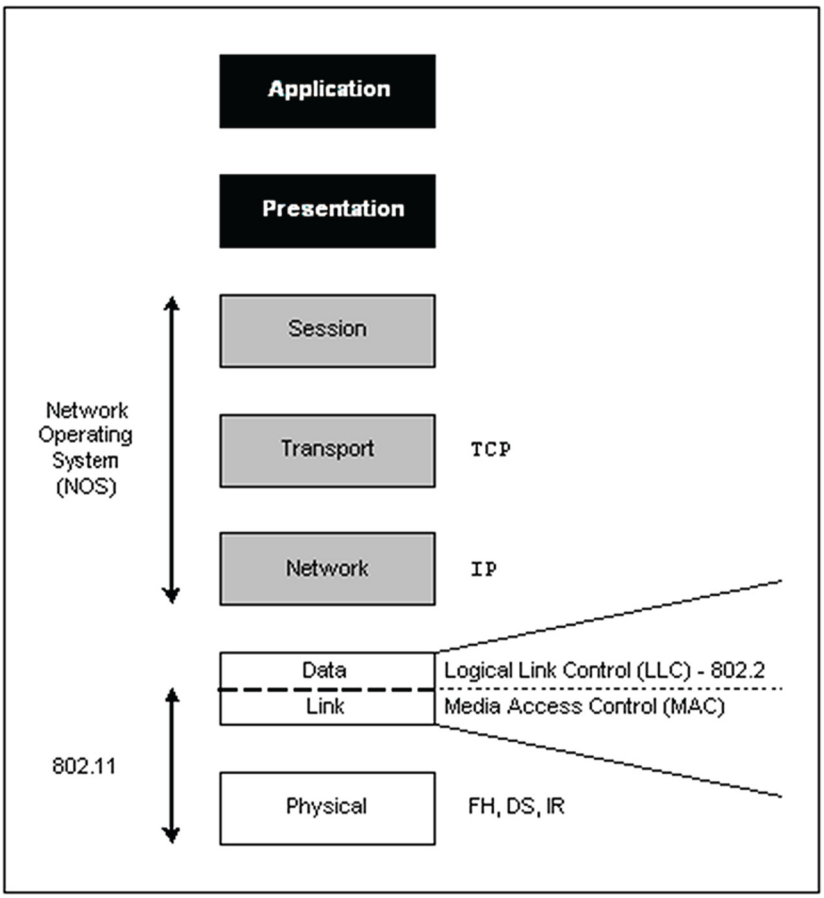
The application of wireless network is not confined only to substituting for wired networks. It enables communication schemes not available in wired networks. With the proliferation of mobile computers and handheld devices, such as PDAs and cellular phones, the role of Wi-Fi networks is becoming more important as means of data exchange.

Several standards have emerged to implement the Wi-Fi network in the following three areas: The Bluetooth standard (IEEE 802.15) is now dominating the wireless personal area network (WPAN) implementation, whereas the IEEE 802.11 family of specifications is now standard for WLAN implementations. In the wireless wide area network (WWAN) domain, several mobile communication technologies such as GSM, GPRS, and CDMA 2000 are still competing with each other to become the ultimate standard.

The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards define the protocols at the physical (PHY) and medium access control (MAC) layers. The MAC sublayer is the bottom part of data link layer as shown in Figure 1.

At the PHY layer, three different transmission techniques are used by 802.11: frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and infrared (IR). For the 802.11b/g specification, only the direct sequence spread spectrum is used.

Figure 1. IEEE 802.11 in the ISO/OSI protocol stack



However, Bluetooth technology uses frequency hopping spread spectrum although it uses the 2.4 GHz band as 802.11b.

The original 802.11 standard uses 11 bit chipping code called the Barker Sequence, to send data via radio waves. Each 11-bit sequence represents one single bit of data. A transmission technique called binary phase shift keying (BPSK) is used to transmit the sequences at the rate of 1 million bits per second, which corresponds to the basic 1 Mbps data transfer rate of the 802.11. A more sophisticated technique referred to as quadrature phase shift keying (QPSK) is used to achieve a 2 Mbps data transfer rate. Instead of Barker sequences, the 802.11b uses complimentary code keying (CCK). When CCK is used, a 16-bit sequence transmitted over the radio channel contains either 4 or 8 information bits and can achieve data transfer rate of 5.5 Mbps and 11 Mbps, respectively.

At the MAC layer, the fundamental protocol component specified by the 802.11 is the distributed coordination function (DCF). The DCF utilizes a carrier sense multiple access with collision avoidance (CSMA/CA) channel access method. When a station finds that no other station transmits within a predetermined time called the inter-frame space (IFS); it transmits its own frame. In unicast transmission, the receiving station is expected to reply with an acknowledgement (ACK), in a similar fashion to the standard automatic repeat request (ARQ) control mechanism. A mechanism called backoff procedure is used by DCF to prevent frame collision which results from stations transmitting simultaneously (Golmie, Van Dyck, Soltanian, Tonnerre, & Rebala, 2003).

To complement the DCF, another protocol called point coordination function (PCF) provides a centralized, polling based access mechanism. To utilize PCF, an access point (AP) is required to perform the point coordination function. The PCF is an optional feature of the IEEE 802.11 MAC layer, and is not supported by all Wi-Fi devices.

In PCF, the AP acts as the central access coordinator. It applies the round robin algorithm to poll the stations within the service set. Unlike DCF, stations wishing to transmit data must first obtain permission from the PC using the request to send and clear to send (RTS/CTS) scheme. When a polled station does not have data to transmit, it sends a null frame. Otherwise the station is allowed to transmit its data frame (Youssef, Vasan, & Miller, 2002).

Wi-Fi Transmission Issues

The use of the unlicensed 2.4 GHz radio band for Wi-Fi transmission medium leads to interference problems. In most countries the 2.4 GHz spectrum is crowded with other radio devices such as cordless phones, microwave ovens, and Bluetooth devices. Due to the effect of radio interference, Wi-Fi network performance drops. With the ever increasing popularity of Bluetooth WPAN, the potential problem of interference becomes sufficient to compel researchers to find mechanisms that allow Wi-Fi and Bluetooth to coexist (Ophir, Bitran, & Sherman, 2004).

Wi-Fi networks have limited range, typically covering up to 46m indoors and 100m outdoors from the nearest AP (Ferro & Potorti, 2005). While significantly greater distance coverage than Bluetooth (i.e. 10m), Wi-Fi performance can be an issue when a station is located near the limit of Wi-Fi range from the other station or the AP.

The nature of radio frequency broadcasting raises security concerns for Wi-Fi networks. Unlike wired networks where access is limited by physical connections, any devices within the range of Wi-Fi network can intercept the packets and potentially intrude into the network. This potential threat necessitates the use of data encryption to minimize the risk of intrusion.

Wi-Fi Network Design Issues

The basic building block of a wireless network is the basic service set (BSS) architecture. A BSS consists of a set of fixed or mobile Wi-Fi stations. The simplest network configuration is the independent BSS (IBSS) which is an ad-hoc

network consisting two or more stations without any infrastructure other than peer-to-peer cooperation.

When a set of BSSs are connected by a fixed network infrastructure, the resulting topology is called an extended service set (ESS). An ESS is a set of one or more BSSs connected by a distribution system (DS), which is not specified by the IEEE 802.11 standard. The DS can take the form of wired networks or some other form of wireless network. A Wi-Fi network with all the typical components is illustrated in Figure 2.

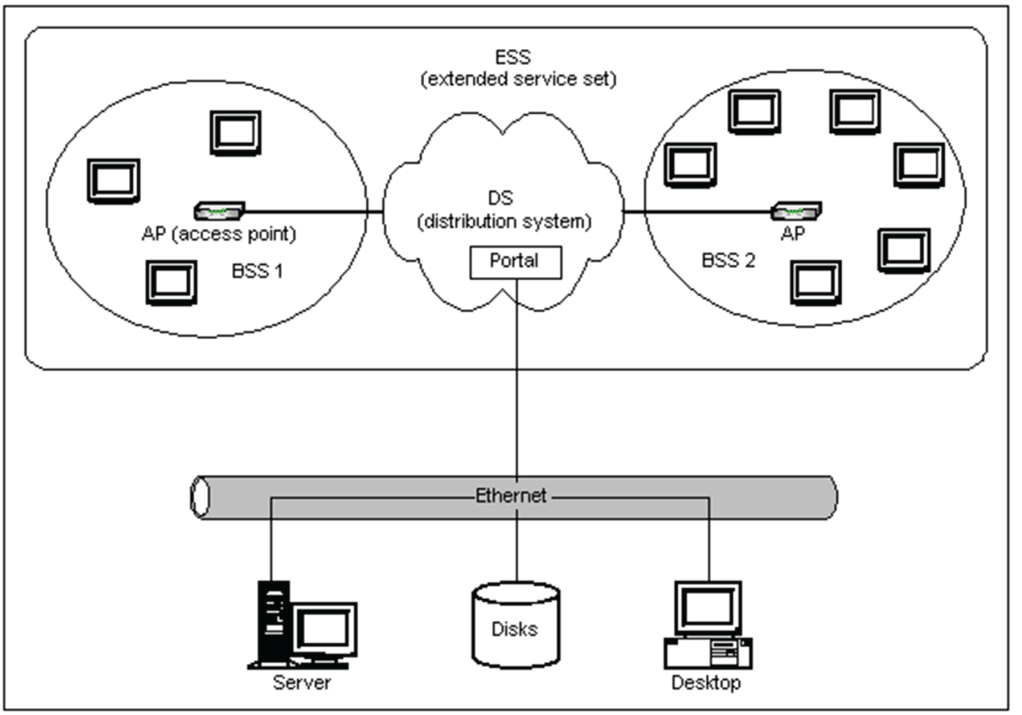
The stations connected to the DS are called access points (APs). An AP offers distribution system services, which allow data exchange between stations of different BSSs. An AP normally performs a function called point coordination (PC), which employs a round robin policy to poll each station for data transmission.

Wi-Fi Standards

The IEEE released the 802.11 standard for WLAN in 1997. The specification requires a data transfer rate of 1 Mbps and 2 Mbps while retaining compatibility with existing LAN hardware and software infrastructure. The standard defines protocols for MAC layer and physical transmission in the unlicensed 2.4 GHz radio band. After successful implementation by commercial companies such as Lucent Technologies, amendment was made for a better performance in the same year. The resulting standard was 802.11b, which specifies higher data transfer rates of 5.5 and 11 Mbps.

The 802.11b differs from the 802.11 in the MAC layer even though it retains compatibility with its predecessor. The physical layer (PHY) is left unchanged. The 802.11b standard was

Figure 2. A typical Wi-Fi network architecture



approved in 1999 and during that year the term wireless fidelity or Wi-Fi was introduced. The 802.11b has proven to be very successful in the commercial domain and majority Wi-Fi devices still support 802.11b standard.

In parallel with the 802.11b, another variant of the original 802.11 was developed called 802.11a, which differs from both 802.11 and 802.11b by using the 5 GHz band rather than 2.4 GHz band. The 5 GHz radio band is unlicensed in the United States but not in many other countries especially in Europe. The 802.11a provides up to 54 Mbps, which is much faster than both 802.11 and 802.11b. However the use of different radio frequencies denies compatibility between 802.11a and 802.11/802.11b. Nevertheless the 802.11a was found satisfactory and approved in 1999. More on Wi-Fi standards can be found in (*IEEE Std. 802.11-2007, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part:11: Wireless Medium Access Control (MAC) and Physical Layer (Phy) Specifications, (Revision of IEEE 802.11-1999)*, 2007).

To resolve the incompatibility problem between the standards, an amendment to 802.11a was approved in 2003. The new standard is referred to as 802.11g, which operates in the 2.4 GHz radio band while retaining the 54 Mbps data transfer rate of the 802.11a. There are other standards in the 802.11 family, such as 802.11n, 802.11u, and 802.11ad as summarized in Table 1.

EXPERIMENT DETAILS

In this section we describe the implementation aspect of 802.11 WLAN using available wireless equipment. We first describe Wi-Fi networks set up both in ad-hoc (IBSS) and infrastructure (ESS) modes. We then focus on the experiments and Wi-Fi performance measurement.

Hardware and Software Requirements

A number of hardware and software applications are used in the experiment. The requirement for IBSS, BSS and ESS differs mainly in the presence of the AP. The following is the more

Table 1. IEEE 802.11 standards family

Standard	Description	Status
802.11	WLAN; up to 2 Mbps; 2.4 GHz	Approved June 1997
802.11a	WLAN; up to 54 Mbps; 5 GHz	Approved September 1999
802.11b	WLAN; up to 11 Mbps; 2.4GHz	Approved September 1999
802.11g	WLAN; up to 54 Mbps; 2.4GHz	Approved June 2003
802.11f	IAPP (Inter-AP Protocol)	Approved 2003
802.11h	Use of the 5 GHz band in Europe	Approved 2003
802.11i	New encryption standards	Approved November 2004
802.11e	New coordination functions for QoS	Approved November 2005
802.11n	MIMO physical layer	Approved October 2009
802.11u	Emergency QoS	Approved February 2011
802.11ad	Very high throughput Wi-Fi	Approved December 2012
802.11ac	Next generation WLAN Draft	Draft in 2012; final in 2014

detailed description of the resources used in the experiment.

Hardware

For the basic service set, at least two Wi-Fi capable computers are required. This is a fairly loose requirement, which can be satisfied by most commercial computer hardware. However, the configuration for wireless laptops and APs that we used in the experiment is shown in Tables 2 and 3.

A different configuration is used for the extended service set (ESS). In an ESS network, an AP is used in addition to two Wi-Fi stations. A third computer is also required to simulate the wired network the AP is attached to (see Table 3).

Software

The IEEE 802.11b protocol automatically establishes data-link-level connection whenever the Wi-Fi enabled hosts are active and within range to each other. To measure the actual throughput however, connection at the application layer is also required. Special software applications are used to enable such connection to take place.

Table 2. Basic service set hardware specification

System	Specification	
Host 1 (H1)	Make: CPU: RAM: OS: Wi-Fi:	Toshiba Mobile Intel® Celeron® 2.4GHz 496MB Windows XP Professional 2002 SP 1 WLAN adapter D-Link 650+ 802.11b
Host 2 (H2)	Make: CPU: RAM: OS: Wi-Fi:	Toshiba Mobile Intel® Celeron® 2.4GHz 496MB Windows XP Professional 2002 SP 1 WLAN adapter Cisco 350 802.11b

Table 3. Extended service set hardware specification

System	Specification	
Host 1 (H1)	Make: CPU: RAM: OS: Wi-Fi:	Toshiba Mobile Intel® Celeron® 2.4GHz 496MB Windows XP Professional 2002 SP 1 WLAN adapter D-Link 650+ 802.11b
Host 2 (H2)	Make: CPU: RAM: OS: Wi-Fi:	Dell Intel® Pentium® M 1.4GHz 512MB Windows XP Professional 2002 SP 1 Intel® PRO/Wireless LAN 2100 3A Mini Adapter
AP Controller	Make: CPU: RAM: OS: Wi-Fi:	Toshiba Mobile Intel® Celeron® 2.4GHz 496MB Windows XP Professional 2002 SP 1 D-Link DWL-900AP+ connected through crossover Ethernet cable

Colligo WE software from Colligo Networks (*Colligo Workgroup Edition 3.2*) enables users of Wi-Fi capable devices to exchange information. The communication can take place either in ad-hoc mode or infrastructure mode. It is necessary that every participant of a Colligo network session has a copy of the software installed on the computer. More complete information regarding the software can be obtained from the company's website at http://www.colligo.com/products/workgroupedition/. Evaluation copy of the software is also available to download from the website.

The Colligo has many useful features such as interactive chat, unidirectional message delivery, virtual whiteboard, and file transfer. The file transfer feature is crucial for this experiment as it provides the means of measuring the link throughput. Colligo has been designed for non-technical users. The implication is that Colligo is relatively easy to setup in a typical setting such as in a wireless ad hoc network. On the other hand, very little control is provided for technical users to customize the settings. This restriction makes it especially difficult for setting up a wireless network in an infrastructure mode.

To set up an infrastructure network, appropriate application is required to configure and control the AP. In this example, the AP hardware comes with AirPlus Access Point Manager configuration software. The AirPlus Access Point manager is a Window based program, which allows setting up the access point parameters from a computer through a wired connection. The AP manager therefore is needed only in setting up the network in infrastructure mode. As an alternative, the AP can also be managed using an internet browser such as Microsoft Internet Explorer.

IBSS Practical Setup

The following setup procedure creates a Colligo basic service set consisting of two Wi-Fi stations as shown in Figure 3. Setting up such a Colligo ad-hoc network session is relatively simple and straightforward.

To initiate a session, all participating stations must activate their Wi-Fi adapter and run the Colligo software. When Colligo is used for the first time, it is also necessary to enter a user name and other personal details for identification purposes.

Figure 4 shows the Colligo main screen for user '*benny*'. Clicking on '*create instant network*' button on the upper right corner will either create a new BSS or join an existing ad-hoc network. The same procedure is repeated by other users wishing to join the network.

Following a successful ad-hoc network connection, the user names of other stations will be listed in the main window. The time it takes for hosts to detect each other varies from a few seconds to several minutes. Figure 5 shows that a remote user named '*wilson*' has been detected. The name of the remote user is written in Italics to indicate that the user has not yet been authenticated and therefore is unable to communicate or gain access to the network resources.

Right-clicking on the remote user name will activate the authentication menu ensuring that the remote user is a legitimate member of

Figure 3. Simple two stations BSS

Figure 4. Colligo ad-hoc network

the BSS. When the authentication is successful, the remote user name is no longer written in italics, indicating that access to network has been granted to the user (Figure 5). Once the remote user is authenticated, all communication features of Colligo can be used. The next step is to set up a file transfer session in which the link throughput can be measured. Figure 6 shows the Colligo main menu to initiate the file transfer.

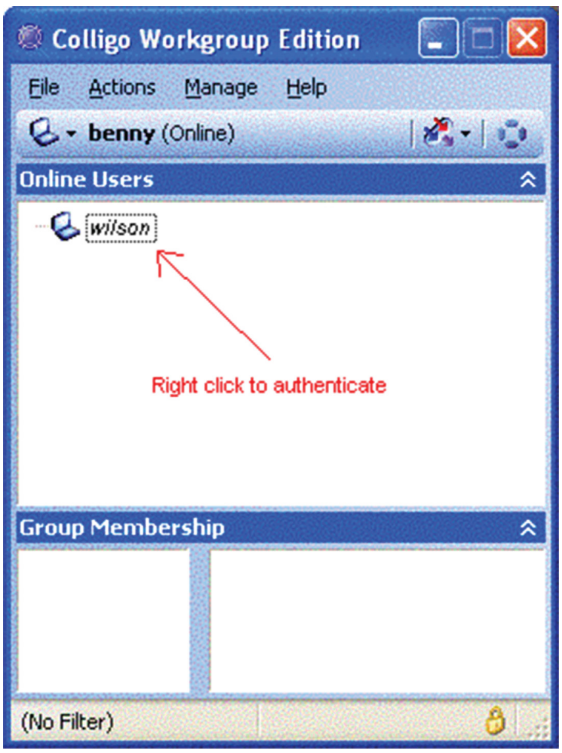
Colligo allows us to transfer a batch of files to a number of users. The empty lists in Figure 6 must be correctly populated before the file transfer can begin. Clicking on the '*Add User*' button brings another window where all remote users are listed (Figure 7). In this example, only one remote user called '*wilson*' is selected. Now select the file(s) from the local drive for transmission (Figure 7). Clicking on the '*Send*' button will initiate a confirmation sequence, which is immediately followed by the actual file transfer.

BSS and ESS Setup

In the infrastructure mode, the wireless network operates under the coordination of an AP. The AP itself is connected to a wired network such as a LAN. In a simple home network, the AP can be directly connected to a router, which provides access to the Internet (Figure 8). Two stations such as *Host 1* and *Host 2* communicate through an AP to access the Internet.

The AP is connected to a wired network even when access to the Internet is not required. In our case, no access to the Internet is required. The wired network is simulated by a third host called '*AP Controller*'. The AP Controller is

Figure 5. Authenticating a remote user and gain access to the network



connected to the AP with a crossover Ethernet cable as shown in Figure 9.

The AP must be configured in such a way that allows a Colligo network to be established. Configuring the AP can only be completed from the AP controller host using either the AP manager or the web browser as discussed. When the AP is active and connected to the controller host, launching the AP manager will show the summary tab (Figure 10). The screen capture shows the parameters set to run a Colligo wireless network in infrastructure mode.

Some of the parameters shown in the summary tab are static; whereas, others are variables that need to be set with correct values:

- **AP Name:** The name assigned to the particular AP. In larger networks several APs may be used, which makes it necessary to assign unique names to each to avoid naming conflict;
- **SSID:** Stands for Service Set ID, which is a unique name for the service set. The Colligo software works correctly if the SSID is set to 'COLLIGO' as shown Figure 11. Setting the AP's SSID to anything other than COLLIGO will prevent the Colligo wireless network from establishing;
- **IP Address:** In this context is the address of the AP for the wired connection to the controller host. The default factory value is 192.168.0.50, which indicates that the AP is designed for the use in small networks only. The controller host must use a compatible IP address to communicate with the AP through the Ethernet cable;
- **MAC Address:** Displayed in the summary tab is the one used in the wireless connection. This value is permanently assigned to the AP and cannot be changed;
- **Channel:** Needs to be set to a number that does not conflict with another nearby AP.

Figure 6. Initiating file transfer

Since there is no other AP within range, an arbitrary channel number can be used;

- **WEP Security:** Refers to the Wired Equivalent Privacy security scheme. When turned on, all devices in the network must use the same encryption key. For simplicity, this feature is turned off.

The most important settings are configured in the '*AP Setting*' tab. Figure 11 shows the configuration already set for a Colligo network in infrastructure mode.

The '*Mode Setting*' selector defines what role the AP device will assume in its operation. The device cannot perform more than one mode at a time:

1. **Access Point:** The default operation mode of the device, which creates a wireless LAN on infrastructure mode;
2. **Wireless Client:** The AP acts as an adapter, which transforms an 802.3 Ethernet device into an 802.11b wireless client;
3. **Wireless Bridge:** Used to utilize two APs to connect two wired LANs with wireless medium;
4. **Multi-Point Bridge:** An extension of the wireless bridge, where multiple APs are used to connect more LANs;
5. **Repeater:** The device is used to extend the range of the network when the wireless hosts are out of range of the actual LAN-connected AP.

In the experiment we set up the mode as *Access Point*. In practice, setting the mode to other than '*Access Point*' always results in the network failure. Once the AP is configured, the wireless infrastructure network is ready to operate and the wireless hosts can join the

Figure 7. File transfer setup completed

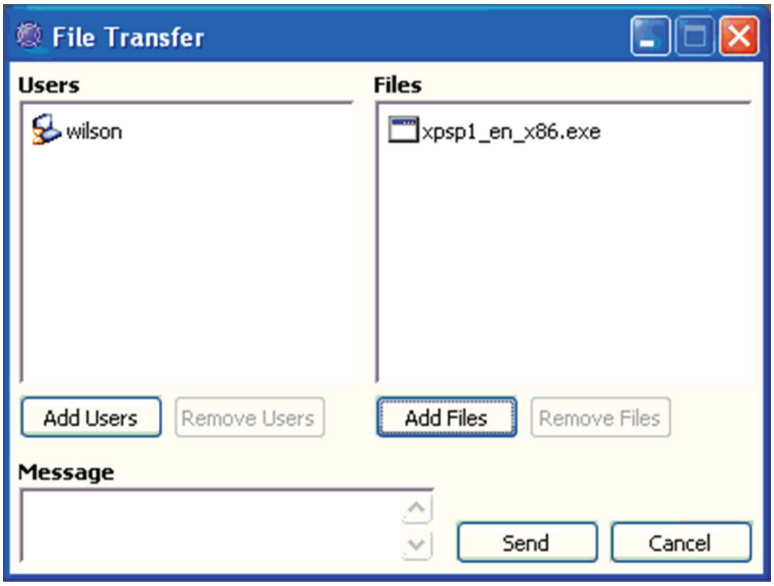
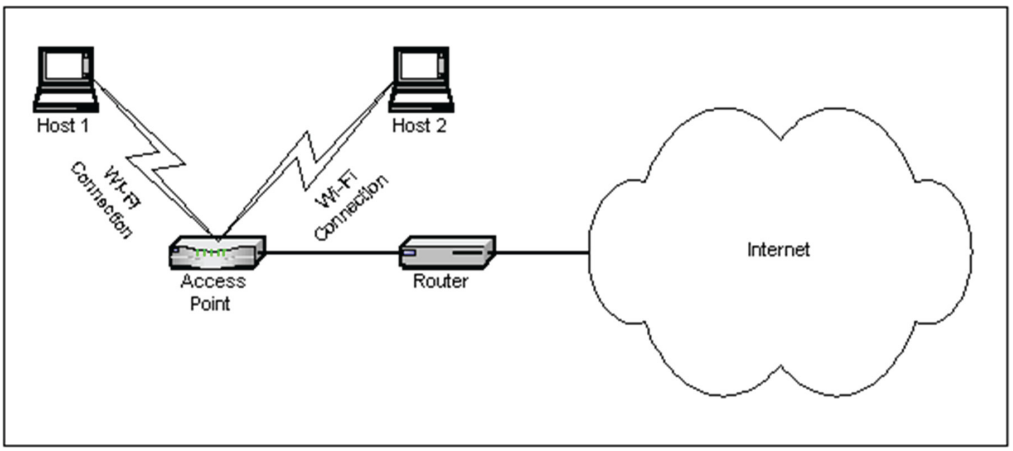


Figure 8. ESS for home use



network. The Colligo software automatically sets the SSID for each host to "COLLIGO" every time it is started. To join the ESS, a host only needs to launch Colligo and wait for the connection to establish automatically. In contrast to the procedure with the BSS, the "*create instant network*" button should not be clicked. The user name of other hosts will appear on the main Colligo window list a few minutes after a host enters the ESS coverage. The routine for authenticating other users, sending files and other actions is identical to that in ad hoc mode.

Figure 9. Simplified ESS

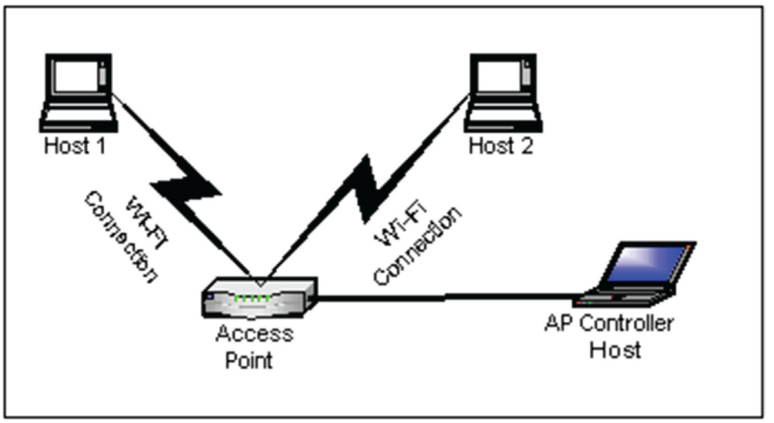


Figure 10. AP manager summary tab

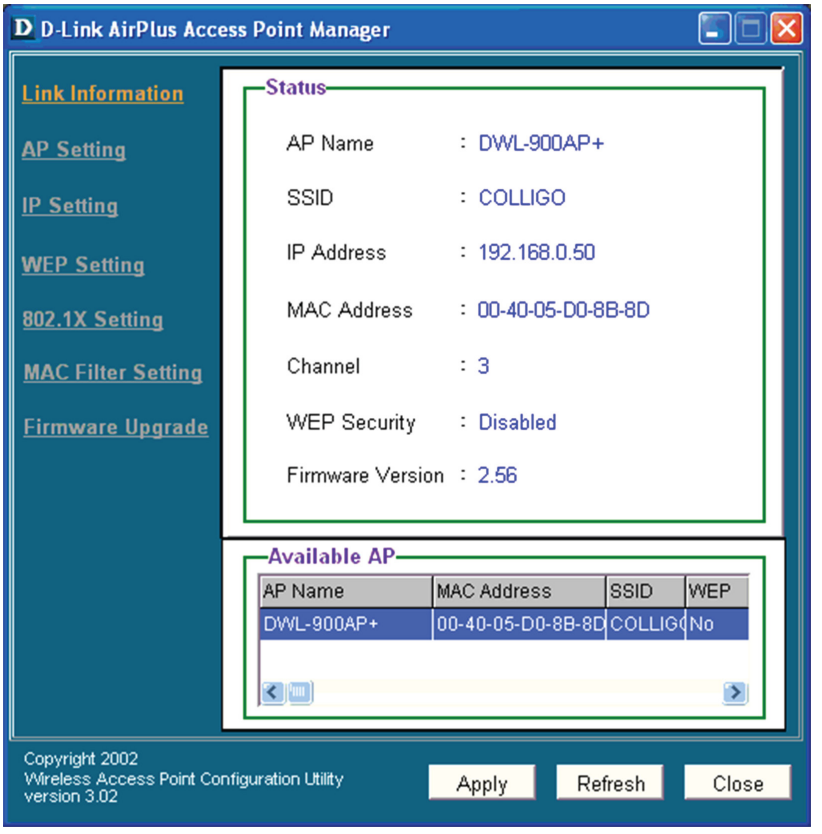
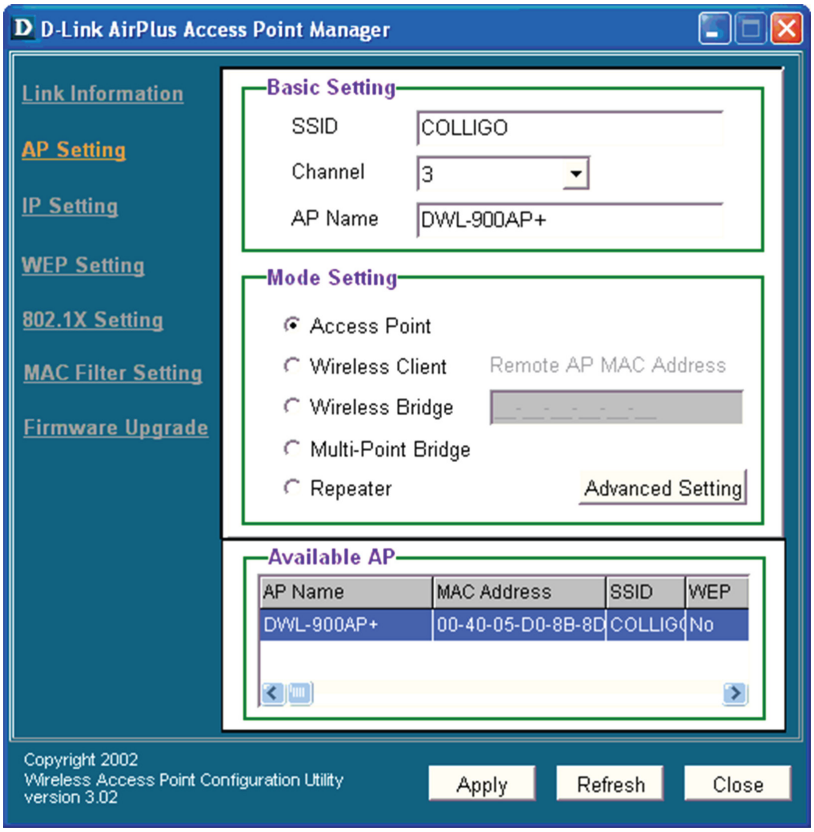


Figure 11. The AP setting tab



EXPERIMENTAL RESULTS

A text file of size 137 MB was transferred from the Host 1 to the Host 2 using 'Send Files' feature of the Colligo™ Workgroup Edition 3.2, which allowed us to obtain the file transmission time (*Colligo Workgroup Edition 3.2*). Different host formations were used to examine the effects of distance on the throughput performance. Tables 4 and 5 summarize the experiment results.

ANALYSIS AND INTERPRETATION

As shown in Table 4, a 4.5 Mbps throughput rate was achieved in ad-hoc mode although the bandwidth was 11 Mbps. The poor performance was due to the retransmission of a large number of data packets that had been lost. Conducting the experiment within a room may also have contributed to the low throughput. At 2.4 GHz,

Table 4. File transfer time in ad-hoc mode

Distance (m)	Obstacle	Transmission Time	Throughput (Mbps)
1	0	3m50s	4.66
1	1	4m00s	4.46
16	0	3m57s	4.52

Table 5. File transfer time in infrastructure mode

Distance (m) H1-H2	Distance (m) H1-AP	Distance (m) H2-AP	Transmission Time	Throughput (Mbps)
1	1	2	10m45s	1.66
1	2	2	9m50s	1.82
1	1	1	10m20s	1.73
2	1	1	15m10s	1.18
32	12	20	9m33s	1.87
17	12	12	10m30s	1.70

the radio wavelength is only 12.5cm. At such a short length, signals echoed by various surfaces within the room will reach the receiver in various phases. The result is that at any given time, signals with varying phases and amplitudes will either reinforce or cancel each other as they reach the receiver's antenna. The original signal is therefore received in a distorted form. This problem is called multipath interference, and is common in mobile communication (Stallings, 2002).

Increased distance and the presence of obstacles also degrade network performance noticeably. This effect is indeed unavoidable since the radio signals used have very low power. Overcoming obstacle and distance problem by increasing the power is not really an option since it will also increase the chance of interfering with other wireless networks nearby.

A drastic performance drop is observed when the network operates in infrastructure mode. On average the throughput in infrastructure mode is only around 40% that of ad-hoc mode. Since the network uses PCF to synchronize the communications, the network is more efficient in using the available bandwidth by the use of fewer control packets. The poor throughput can therefore be explained by the mechanism by which data packets are transmitted from sender to the AP and then from the AP to the receiver. It is very likely that the AP uses a store-and-forward scheme, which results in the channel being occupied for twice as long.

On the other hand, the infrastructure mode makes it possible for wireless hosts to communicate when they are out of range from each other as long as both are within the AP's range. This implies that more flexibility and mobility is achieved at the expense of lower throughput.

EVALUATION BY STUDENT FEEDBACK

The Wi-Fi projects were offered to two graduate students as part of their summative assessment towards 'Net-centric Computing' a postgraduate course. The project learning outcomes include: (1) setting up and testing Wi-Fi projects; (2) demonstration of working prototype to project supervisors; (3) development of teaching resources for classroom use; (4) written report – containing summary of findings and reflective statements; and (5) oral presentation to the staff and students.

The Wi-Fi projects were successfully completed and students indicated that they had learned Wi-Fi networking by practical activities included in the Wi-Fi projects. This is evident from the student's reflective statements, as follows:

Student 1:

The Wi-Fi project has helped me immensely to develop a sound knowledge of Wi-Fi technol-

ogy. During the practical project, I discovered that there are various issues with regard to the deployment of Wi-Fi technology. The level of exposure and knowledge that I gained from the hands-on experiment, I would have never achieved from just a theoretical mode of learning.

There are many positives that can be drawn from a hands-on project like the Wi-Fi propagation measurement. A project such as this helps you to understand and appreciate technology better, which may not possible from a mere theoretical form of learning. I would strongly recommend hands-on projects to others who are interested to gain in-depth knowledge and experience of the technology.

Student 2:

By taking up the hands-on project, I realised that with a correct approach, the subject of networking in general and Wi-Fi in particular is no more difficult than other subjects in computing science. By understanding the basic issues of the technology, one can make sense on why the designers built the devices the way they did. Further, it challenges us to think about how various aspects of the technology can be improved.

With an engineering background, I never believe in any new technology unless I see it actually working. The project convinced me that the Wi-Fi technology does work, and any person willing to invest time studying and experimenting can learn to set up his or her own Wi-Fi network. Also the experience enriches us with another skill that may be important in our career later.

I would recommend similar projects to anyone interested in practical experiments and is not shy of technical challenges. They are also suitable for veterans of theoretical investigations who want to enrich their skill and experience with practical ones.

CONCLUDING REMARKS

In this paper we reported a series of Wi-Fi experiments and measurements made at various locations of the AUT University's WY office building to gain an insight into the performance of Wi-Fi links in an office environment. This research involves both literature review and practical activities based on IEEE 802.11 Wi-Fi.

The use of electromagnetic waves as the medium instead of cables presents many technical challenges. To begin with, the available radio band is limited and most ranges are licensed by governments across the world. This restriction forces various wireless devices to crowd into the same unlicensed bands. The radio communication environment introduces noise, interference, and security issues. Despite the high growth of WLANs in recent years, the wireless network may not replace the wired networks completely. It is most likely that both wired and wireless networks will coexist in the future.

The results obtained show that data transfer rate through the wireless medium is much lower than the wired network. The wireless connection is also fragile, which necessitates that the whole transmission process be repeated whenever the connection drops during file transfer session. Because of these limitations, wireless networks at present serve mainly as a connectivity solution rather than as a performance solution. This may change in the future however, as new wireless technologies supporting quality of service (QoS) are also being developed.

We found that the ad-hoc network mode provides better throughput in a low populated network. The same network operating in infrastructure mode provides only about half the throughput of the ad-hoc network. It is very likely that the AP uses store-and-forward algorithm in delivering the data packets, which results in the drastic performance drop. The AP however is indispensable when the stations are out of range of each other. The technical difficulties encountered during the experiment suggest that Wi-Fi technology is not yet mature. This is indicated by the complexity of the set-

ting up procedure and the incompatibility that is common between Wi-Fi devices.

As it grows, wireless technology will provide research opportunities in several areas. Future research relevant to the scope of this project will mainly involve bandwidth increase and optimization, which are aimed at throughput improvement. At present the 802.11-based network has many limitations because it provides services on 'best effort' basis. Perhaps new wireless standards such as 802.11e will provide better QoS.

In anticipation of the increased available bandwidth, various network-based business and multimedia applications are also being developed. The required bandwidth for delivering the data in various presentation formats are also provided in their discussion.

ACKNOWLEDGMENT

I would like to thank my former student Wilson Siringoringo for setting up and conducting Wi-Fi experiments.

REFERENCES

802. *11ac: The Fifth Generation of Wi-Fi (Technical White Paper)*. (2013). Retrieved August 29, 2013, from http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/white_paper_c11-713103.html

Colligo Workgroup Edition 3.2. (2013). Retrieved January 20, 2013, from www.colligo.com/

Ferro, E., & Potorti, F. (2005). Bluetooth and Wi-Fi wireless protocols: A survey and a comparison. [see also IEEE Personal Communications]. *Wireless Communications, IEEE*, *12*(1), 12–26. doi:10.1109/MWC.2005.1404569

First New Zealand 1Gbps wireless connect goes to IRL. (2011). Retrieved September 12, 2011, from http://www.irl.cri.nz/newsroom/media-releases/first-new-zealand-1gbps-wireless-connect-goes-irl

Golmie, N., Van Dyck, R., Soltanian, A., Tonnerre, A., & Rebala, O. (2003). Interference evaluation of bluetooth and IEEE 802.11 systems. *Wireless Networks*, *9*(3), 201–211. doi:10.1023/A:1022821110023

Hiertz, G., Denteneer, D., Stibor, L., Zang, Y., Costa, X. P., & Walke, B. (2010). The IEEE 802.11 universe. *IEEE Communications Magazine*, *48*(1), 62–70. doi:10.1109/MCOM.2010.5394032

Howard, D. (2002). It's a Wi-Fi world. *netWorker*, *6*(3), 26–30. doi:10.1145/569207.569209

IEEE 802.11n-2009 amendment 5: Enhancements for higher throughput. (2013). Retrieved June 6, 2013, from http://en.wikipedia.org/wiki/IEEE_802.11n

IEEE 802.11s: Wireless LAN medium access control (MAC) and physical layer (PHY) Specifications: simple efficient extensible mesh (SEE-Mesh) proposal. (2013). Retrieved August 29, 2013, from https://mentor.ieee.org/802.11/dcn/05/11-05-0562-00-000...

IEEE Std. 802.11-2007, IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part:11: Wireless medium access control (MAC) and physical layer (Phy) specifications, (Revision of IEEE 802.11-1999). (2007). New York.

Ophir, L., Bitran, Y., & Sherman, I. (2004). Wi-Fi (IEEE 802.11) and bluetooth coexistence: issues and solutions. In *Proceedings of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004)* (Vol. 842, pp. 847-852).

Prasad, A. R., Prasad, N. R., Kamerman, A., Moelard, H., & Eikelenboom, A. (2001). Performance evaluation, system design and network deployment of IEEE 802.11. *Wireless Personal Communications*, *19*, 57–79. doi:10.1023/A:1011994424763

Prasad, N., & Prasad, A. (2002). *WLAN systems and wireless IP for next generation communications*. Boston, MA: Artech House.

Prasad, R., & Ruggieri, M. (2003). *Technology trends in wireless communications*. Artech House.

Stallings, W. (2002). *Wireless communications and networks*. Prentice Hall.

Vaughan-Nichols, S. (2003). The challenge of Wi-Fi roaming. *Computer*, *36*(7), 17–19. doi:10.1109/MC.2003.1212682

What is a wireless LAN? (2013). Retrieved September 1, 2013, from http://sss-mag.com/pdf/proximwhat-wlan.pdf

Youssef, M. A., Vasan, A., & Miller, R. E. (2002). Specification and analysis of the DCF and PCF protocols in the 802.11 standard using systems of communicating machines. In *Proceedings of the 10th IEEE International Conference on Network Protocols* (pp. 132-141).