AC 2010-1663: MOBILE AND WIRELESS NETWORKS COURSE DEVELOPMENT WITH HANDS-ON LABS

Hetal Jasani, Northern Kentucky University

Hetal Jasani is an assistant professor in the Department of Computer Science at Northern Kentucky University. His research interests include mobile and wireless networks, distributed systems and network security. He teaches graduate and undergraduate courses in the area of computer networking including mobile and wireless networks and network security. He received the Ph.D. from Florida International University in 2006.

Mobile and Wireless Networks Course Development with Hands-on Labs

Abstract

Rapid advances in wireless networks technologies present opportunities for innovative education at undergraduate and graduate level. Wireless networks courses become increasingly popular in colleges (including community colleges) and universities. However, there is a real concern with the lack of hands-on labs based active learning in computer science, engineering and technology curriculums. Hands-on project based learning is found to be the best way of learning and teaching wireless networking technologies. These hands-on projects also provide the problem based learning (PBL).

In this paper, an undergraduate computer information technology special topic course in mobile and wireless networks is presented which is developed based on many hands-on lab activities. In learning the concepts of wireless networks via hands-on labs, students get ample opportunities to understand the underlying principles and concepts of wireless networks. These hands-on labs are chosen to provide sufficient challenges to the students that prepare the engineers and technologists for the next generation solutions. The level of difficulty for this course requires the prerequisites of networking course. For each hands-on lab, each team of students carry out the lab activities in order to successfully implement the particular wireless networks solutions. The course requires the students to collaborate among them and participate in active learning based modules. This paper elaborates innovative projects that are suitable for laboratory work in computer information technology curriculum. It explores both hardware and software components that are now being used for practical exercises in wireless networks courses. This paper discusses the hands-on labs for wireless networks such as site survey, MAC (Medium Access Control) layer settings, upgrading the firmware of wireless devices, etc. In addition, this paper also illustrates the wireless security labs which discuss how to set up WPA/WPA2 (Wi-Fi Protected Access) on Cisco and Linksys wireless access points (AP).

Introduction

The field of wireless networks is dynamically changing due to the advances in the technologies. It becomes more and more vital as people spend more and more time connected to the network from anywhere anytime. Many areas of wireless networks demand highly trained personnel to solve the new challenges such as site survey, wireless security, etc. There is a great demand of technicians and engineers who can maintain and secure the wireless networked environment. While electrical and computer engineering and computer science curriculums offer students few wireless networking courses; this may not enough to train network professionals with the proper background on the newer wireless technologies. Although many courses on computer and wireless networks have been developed in these programs, they are primarily focused on in-depth mathematics, algorithms, and theory. Many of these courses don't use hands-on labs that are the preferred learning style of information technology students[9]. Since computer information technology (CIT) program emphasizes the hands-on based active learning, the previous approaches taken by other programs (computer science/engineering programs) are not suitable

for CIT program. It is also universally accepted that hands-on experiments are the best way to enhance the students' learning which facilitates collaborative based active learning[10].

The goal of mobile and wireless networks course is to familiarize students with several different wireless networking technologies through a series of laboratory experiments using small-scale test beds. The protocols and standards include IEEE 802.11 (a, b, g or simply WiFi)[5,14], Bluetooth (IEEE 802.15)[12], WiMAX (802.16)[13], etc. The CIT program[6] in the Department of Computer Science[7] at Northern Kentucky University[17] offers several courses in networking and system administration. In general, students learn about many networking systems, but had rare opportunity to learn wireless networking technologies. A newly designed special topic course of Mobile and Wireless Network with hands-on laboratory experiments has demonstrated effectiveness in teaching the concepts of different wireless network technologies. This course has been offered to provide a practical view of mobile and wireless networks. The course assumes that students have basic knowledge of networking (i.e., students have taken first course of network administration).

In the rest of the paper, we focus on specific approaches taken at our CIT program. The general course development approach is discussed. Some hands-on labs are illustrated. The assessment from the mobile and wireless course in CIT Program is elaborated. The Conclusions on developing mobile and wireless network course is presented.

Current Networking Courses

Wireless networks course training is often integrated into existing courses or as a separate course using various tools in projects. Many universities have used different networking protocols and devices for hands-on labs in networking courses. Hands-on based training in these wireless networks technologies is not common at the college level for undergrad curriculums due to the cost and complexity of devices/configurations.

Oh, et al. (2009) discusses the use of OPNET modeler to model the HAIPE (High-Assurance Internet Protocol Encryption) technology[18]. The problem of using OPNET is that students may not be engaged as much as they do in doing hands-on labs. They have used OPNET because HAIPE is a fairly new encryption technology similar to Internet Protocol Security (IPSec), and it is not easy to teach different components of it with hands-on labs. They also mentioned in their conclusion that some students learn faster and have a better understanding of the concept when using a hands-on approach. However, they did not present any wireless networking. Jasani (2007) has created a wireless course mainly using OPNET modeler software[15]. However, success of this course was mixed and many students wish to have more hands-on lab activities. Hartpence (2009) emphasizes QoS and less wireless in his paper with various hands-on experiments[8]. Abbott-McCune et al. (2008) presented the reconfigurable networking labs for their networking courses[1]. However, they haven't discussed the wireless networks component at all. Cao et al. (2009) discusses the development of networking lab for teaching and research[3]. They have used various tools such as OPNET, Network Simulator (NS-2), Virtual PC, and CPLEX, which enable students to conduct various network modeling, and simulation. However, this is not the best way to enhance the students' learning as they mentioned that building a hands-on experimental lab environment is a challenging for many institutions due to space

constraints, budget limitations, maintenance difficulty. Other people also worked on networking courses which do not have focus on wireless networking[11,16,19,20]. There is a need to create more comprehensive, dedicated course to teach wireless networks technologies that could give students a practical experience. This paper discusses how this course is offered to satisfy this demand and provide college graduates a practical hands-on training.

Course Development

The learning outcomes of mobile and wireless network special topic course in CIT program at NKU are that, by end this course, students should be able to:

- Understand the various wireless LAN standards
- Configure the IEEE 802.11 physical, medium access control and network layer standards
- Conduct the site survey before installing/implementing WLAN
- Understand the wireless LAN security and vulnerabilities
- Configure and troubleshoot the wireless network appliances using the IOS (Internetwork Operating System) commands
- Upgrade the firmware of Linksys wireless router to carry out more advanced wireless networks scenarios.

Course Outline

The hands-on labs are scheduled during semester with various activities in wireless networks. Hands-on labs are selected such a way that students learn all following topics. The topics covered are[2, 4]:

> Wireless LAN Devices and Standards, IEEE 802.11 Physical Layer Standards, IEEE 802.11 Medium Access Control and Network Layer Standards, Planning and Building a Wireless LAN, Conducting a Site Survey, Wireless LAN Security and Vulnerabilities, Implementing Wireless LAN Security, Managing a Wireless LAN, Network Settings and Wireless LAN Troubleshooting, Personal, Metropolitan, and Wide Area Wireless Networks

Sample Hands-on Labs

For the wireless networking hands-on labs, students use several networking devices such as routers, computers, cables, Linksys wireless router, Cisco access points, etc. Some sample labs/exercises are discussed below to demonstrate the major areas of this course. Initially, students perform hands-on experiments using command line interface (CLI) to configure the Cisco Access Point (AP) (e.g., set up IP address, SSID, etc.). Students also carry out more experiments to increase the security of wireless networks by using MAC filter, WEP (Wired Equivalent Privacy)/TKIP (Temporal Key Integrity Protocol), WPA (Wi-Fi Protected Access), WPA2, etc. At last, few more hands-on experiments are performed by upgrading the firmware of Linksys router with open-source DD-WRT. Due to the limitation of space, few hands-on labs are described in this paper. As semester gets ahead, more in-depth and advanced labs are introduced to enhance the advance topic of wireless networking. The sequence has been chosen according to lecture topics. However, many of the labs are independent of each other and anyone can replicate some of the labs in their curriculum.

Equipment Used in Various Hands-on Labs

- Cisco Aironet 1131
- Linksys WRT54GL
- Dell Mini Laptops
- CAT5 Cables
- Console (Rollover) Cables

Lab – Basic Configuration of Wireless Networks using Cisco AP

This experiment aims to introduce the command line interface of Cisco Internetwork Operating System (IOS) to configure the Cisco wireless access point i.e., Aironet 1131. Using various commands, students find the name of Ethernet, radio and BVI interfaces, SSID, MAC address, BIA (burned-in address), bandwidth (BW), default IP address of Ethernet, radio and BVI interfaces. Students setup password to access control the AP for enhanced security. Students also setup IP address, SSID, and authentication method using command line interface. In addition, students setup http secure server using various Cisco commands on Cisco AP to access it via browser securely. Figure 1 and Figure 2 show the general network diagram for this lab setup and some of the later discussed labs.

In this lab activity, students get to know the basic commands of Cisco IOS that students are expected to know from their first network administration course (i.e., prereq). If students forget those commands, this lab serves as refresher lab for them.

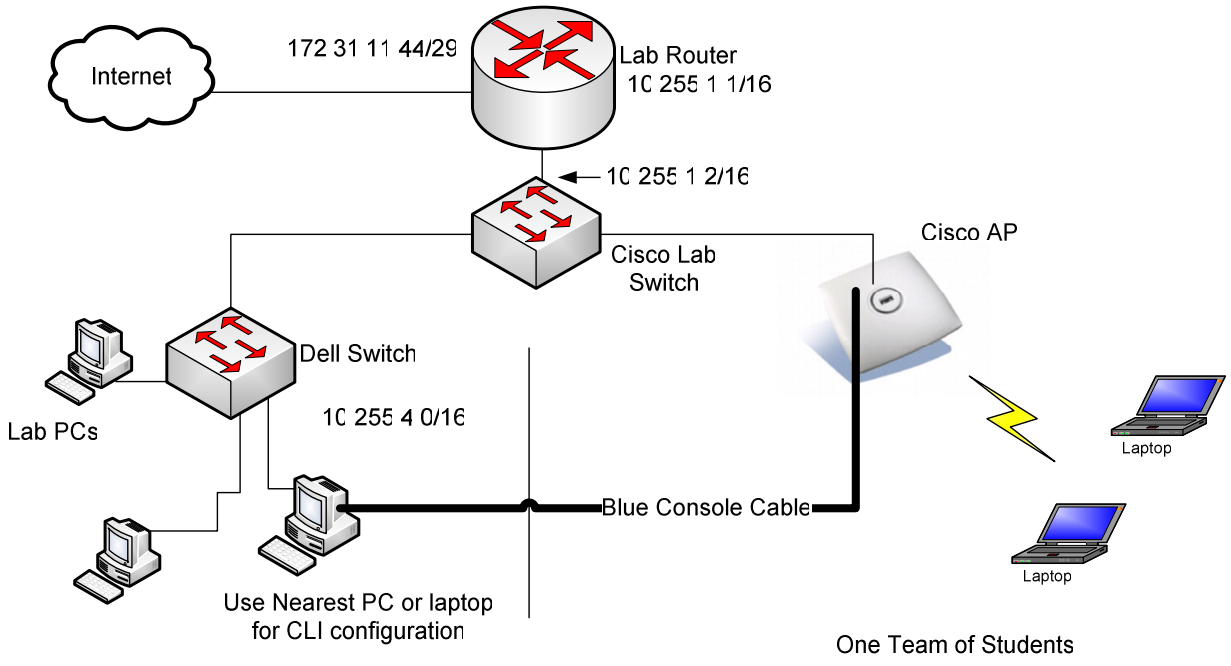

Figure 1. General Network Diagram for Lab Setup (with Cisco AP)

Lab - Configuring Shared Key Authentication on Cisco AP

In this lab, students use the command-line interface to remove open authentication and configure shared key authentication. Shared key authentication is more secure than open system authentications. Students setup encryption cipher and key size for securing AP using Cisco IOS commands. Students test/verify this activity/setup on their laptops to connect using this authentication type and shared key.

Lab – Observe the MAC Settings for the Linksys

Students observe various MAC layer setting of Linksys wireless routers such as authentication type, CTS protection mode, beacon interval, DTIM interval, fragmentation threshold, and RTS threshold. Students get knowledge about each of these parameters and how they affect the performance of wireless networks. Students write a reflection report by including those parameters.

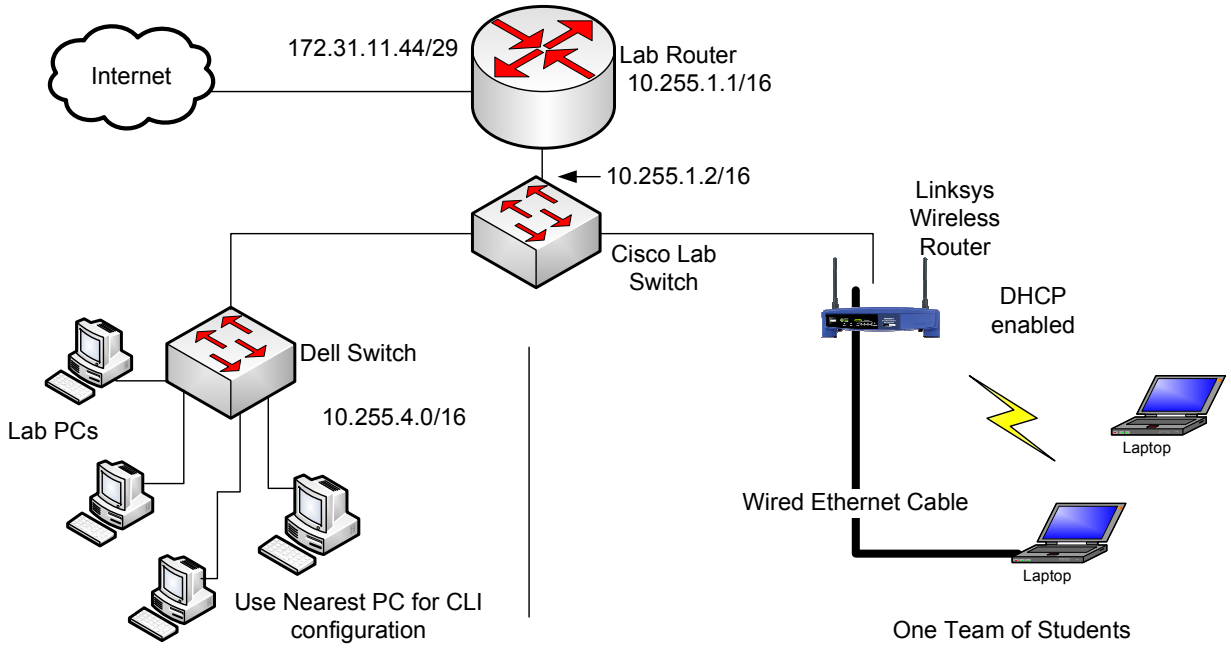

Figure 2. General Network Diagram for Lab Setup (with Linksys Router)

Lab - Evaluating Radio Frequency (RF) Loss

The two factors that have the greatest impact on WLAN RF loss are distance from the access point (AP) and objects between the AP and the client. In this lab activity, students evaluate the RF loss in their wireless environment. Students, on a laptop computer, look for signal strength measurement (status of WLAN). Students move away from AP, and keep measuring the strength with noting the distance. They continue roaming until students no longer can receive the signal. They note the location and distance. They move back towards the AP and stop whenever there is a significant increase in signal strength. They note and record the obstacles that are between laptop and AP. Students go in opposite direction and do the same experiment. In submission,

students create a map that will illustrate the signal strength in building. This lab activity can also serves as site survey. However, many additional tools could be used for site survey.

Lab - Modifying AP Transmit Power and Antenna Diversity

In this lab, students change the transmit power on Cisco AP via web browser using one of the laptops given. Another laptop will be used to measure the effect of power change while moving away from Cisco AP. They continue roaming until students no longer can receive the signal. They note the location and distance. They move back towards the AP and stop whenever there is a significant increase in signal strength. In submission, students create a map that will illustrate the signal strength due to transmit power change. Students repeat this exercise for various power settings. In addition, students change the antenna diversity and repeat same exercise while changing antenna diversity. Students create another map that will illustrate the signal strength due to the change in antenna diversity.

Lab - Investigating Co-Channel Interference using Linksys Router

Students connect their laptops to Linksys as per diagram in Figure 2. They browse the Linksys (192.168.1.1) from one laptop using username and password provided or created by them. They find the current channel which has been used by Linksys. Each team will change the channel as mentioned shown in Table 1 below and save settings (in order to avoid interference):

Table 1. Channel Setting for Each Team

Team	Channel
Team1	1
Team2	6
Team3	11

In each team, one team member browses to www.cnet.com and search for Bandwidth Meter on the site. He or she tests connection speed. Students enter the required information on the Bandwidth Meter speed test web page. They choose wireless as connection type. Each team performs the test speed in Mbps. All 3 students' teams will do this activity on the same time. Now, all 3 student team change channel to 6 at the same time to create interference to each other. The run the test again and note the difference in speed in Mbps due to the interference. Each student write his/her own report and submit the analysis of the results.

Lab - Measuring Ad Hoc Mode Throughput

It is important to know for students that a wireless access point, although primarily a data link layer device, operates like a hub. The bandwidth is shared and the actual throughput is much less than students might expect. 802.11 systems use CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) for media access rather than CSMA/CD (Carrier Sense Multiple Access/Collision Detect), which is used for Ethernet. Collision avoidance is used because wireless devices have no way to detect a collision. One of the reasons for the lower than expected throughput is the way CSMA/CA operates. It is important for students to know that

there is much more overhead associated with CSMA/CA than with CSMA/ CD. In addition, this overhead increases as the number of users accessing the network simultaneously increases - just like it does when using a hub. In general, the more devices a wireless frame must pass through, the lower the throughput. So, it is expected that transferring a file using ad hoc mode would be more efficient than transferring the same file using one or more access points in infrastructure or repeater mode. The purpose of this lab is to measure the throughput realized when transferring a file from one peer to another using ad hoc mode. In this lab students team use ad hoc mode to transfer a file using FTP. Dell Mini laptops are provided to configure the FTP server and FTP client on separate laptop. Students create ad hoc network between them, transfer large file (i.e., 75 MB) and measure the throughput for ad hoc mode.

Lab - Measuring Infrastructure Mode Throughput with a Cisco AP

In previous lab, students transfer a very large file from one laptop to another directly as laptops are connected in ad hoc mode. In this lab, students transfer the same file using infrastructure mode. So, there is a Cisco 1131 access point in between two laptops. It may increase the overhead and delay in communication. Consequently, it may reduce aggregate throughput. Students measure the throughput in this lab and use to compare with next lab activity in which they use Linksys router instead of Cisco AP.

Lab - Measuring Infrastructure Mode Throughput with a Linksys Router

Many people are using Linksys wireless routers or similar residential wireless gateway devices in their homes or small businesses. These relatively low-cost devices do more networking functions than a basic access point like the Cisco Aironet 1131. In addition to accepting wireless clients, many residential wireless gateways also accept wired clients. They also perform network address translation (NAT) and act as routers. While residential wireless gateways are able to handle the wireless traffic of very few users, these devices do not have the configuration options or the power of a device such as the Cisco 1130 series access point.

In previous lab, students transfer a very large file from one laptop to another through the Cisco 1131 access point. The purpose of this lab is to compare that file transfer throughput to the throughput realized using a residential wireless gateway. In this lab, students transfer the same file through a Linksys wireless router instead of Cisco 1131 access point. The throughput measured is compared to the infrastructure mode throughput measured previously. Students write reflection report summarizing their experience.

Lab – Upgrade the Linksys firmware using DD-WRT

Linksys WRT54GL routers have the ability to be flashed with open source firmware from the likes of DD-WRT and have lots of non-standard features. This lab introduces students to flash a Linksys WRT54GL with open source DD-WRT firmware. After completing this lab, students get to know how to upgrade firmware on a router.

DD-WRT is a third party developed firmware released under the terms of the GPL for many IEEE802.11a/b/g/n wireless routers based on a Broadcom or Atheros chip reference design. DD-

WRT offers many advanced features not found in the original factory firmware on these devices. Among other features not found in the original Linksys firmware, DD-WRT adds the Kai Daemon for the Kai Console Gaming network, WDS (Wireless Distribution System) wireless bridging/repeating protocol, Radius Authentication for more secure wireless communication, advanced Quality of Service controls for bandwidth allocation, and software support for the SD-Card hardware modification.

Students connect laptop using CAT5 cable to one of the switch Ethernet ports on the back of the Linksys router. Students download the DD-WRT firmware and upgrade the Linksys router using Cat5 cable connection. Students also learn that they should not use wireless connection to upgrade firmware as connection will be broken during the process of firmware upgrade.

Lab - VPN (Virtual Private Network)

This lab activity gives students the knowledge how to setup a Remote Access VPN to students' own personal network using DD-WRT based Linksys router. After completing this lab, students get to know how to setup and connect to a VPN. In this lab, each team of students configures a PPTP (point to point tunneling protocol) server on their wireless DD-WRT router. Then, they configure the users that students want to allow remote access to and then students setup a connection to that VPN from a foreign host as shown in Figure 3.

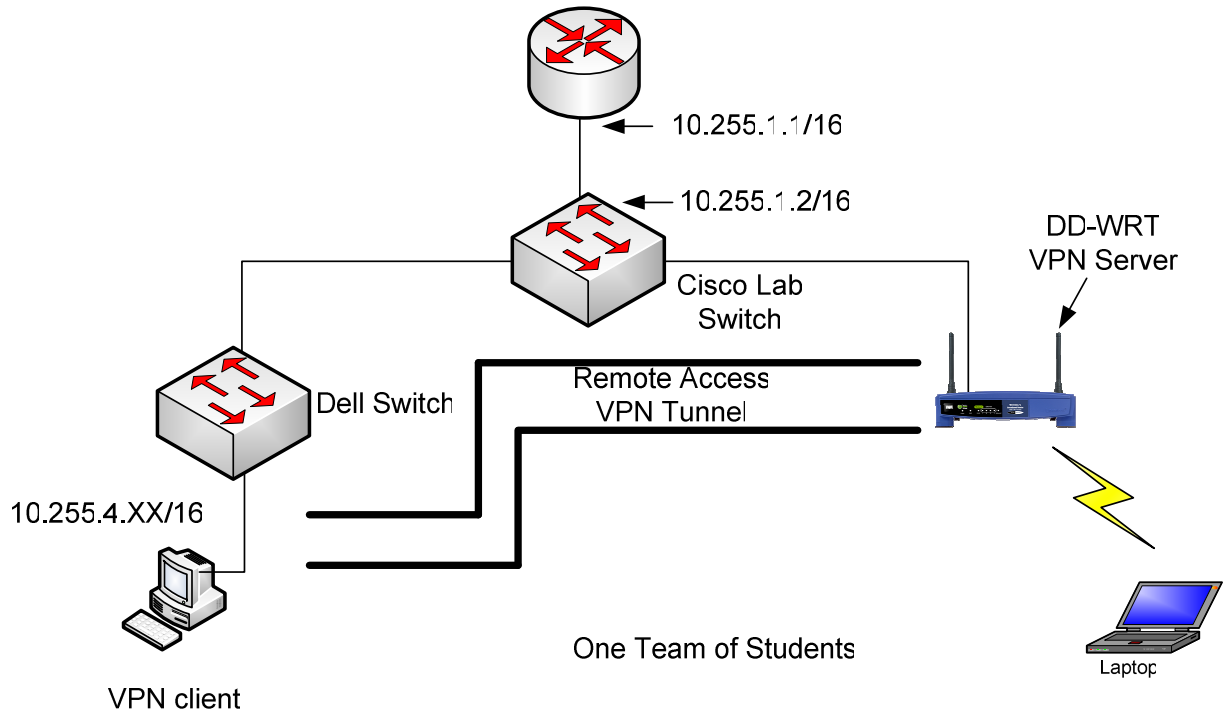

Figure 3. Network Diagram for VPN Setup

A remote access VPN connection over the Internet enables a remote access client to initiate a dial-up connection to a local ISP instead of connecting to a corporate or outsourced network

access server (NAS). By using the established physical connection to the local ISP, the remote access client initiates a VPN connection across the Internet to the organization's VPN server. When the VPN connection is created, the remote access client can access the resources of the private intranet. The following figure shows remote access over the Internet. The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks in this case.

Lab – Setup DD-WRT Router in Repeater Mode

One of the major drawbacks to wireless LANs is the limitation of range due to many factors such as interferences and radio wave limitations. DD-WRT routers have added capabilities to WRT54GL router. Students configure it to be a universal wireless repeater, meaning it receives any wireless signal SSID and rebroadcast it back out. In this lab, each team of student configures two wireless APs. One of them is setup as repeater to repeat the signal for increasing the range of wireless networks. Students test/verify that they are able to connect Internet via both access points although laptop is only connected to repeater as shown in Figure 4.

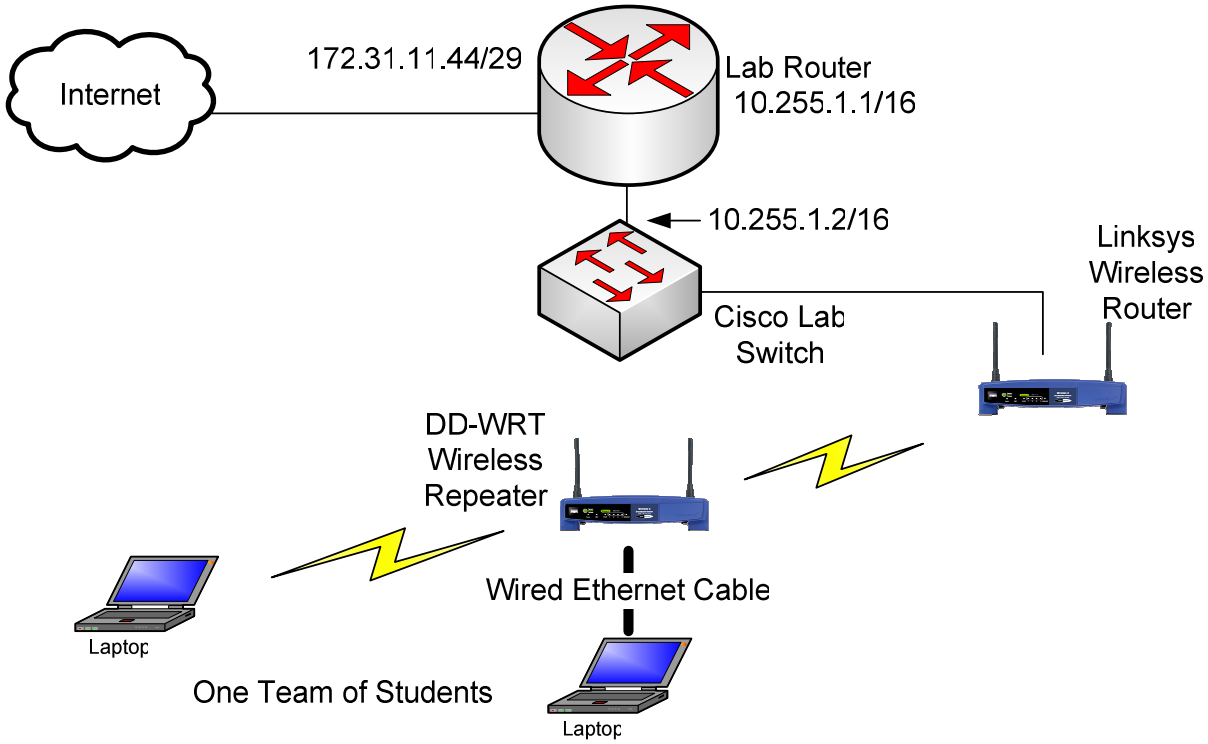

Figure 4. Network Diagram for Repeater Mode

Lab - Wireless LAN Security

Without including the wireless network security, course objectives could not be fully fulfilled as wireless network security is very important topic. Students are asked to perform lab to setup the various security on Cisco and Linksys wireless access points. Students perform the following lab activities:

- Set a MAC address filter on wireless AP
- Configure WEP (Wired Equivalent Privacy) on wireless AP

- Set dynamic WEP keys on wireless AP
- Setting Cisco Migration Mode on wireless AP
- Setting Up WPA (Wi-Fi Protected Access) on wireless AP
- Setting up WPA2 on wireless AP

MAC address is the basic security method of controlling the access to wireless networks. However, it is not secure method as MAC address could be spoofed easily with many free available tools. WPA Migration Mode is an access point setting defined by Cisco that enables both WPA and non-WPA clients to associate to an access point using the same SSID. It will enable a "diverse" group of devices to all use the same access point whereas normally they could not.

By performing the above activities, students could understand the weakness of WEP, and dynamic WEP. Students also understand the WEP could be cracked easily with tools available for free. WPA, with its dynamically changing key, is a far better security method. Students set up AP to use WPA. Students also configure the WPA2 which is the most secure ways of providing the wireless access to the users. Students learn that the corporation should use WPA2 in order to provide confidentiality and privacy of data communication over the wireless link.

Assessment, Students Feedback and Teaching Reflection

Various methods were used to formally assess the effectiveness of this course, including tests, the evaluation of student work, and the instructor's assessment. At the end of the semester, an anonymous survey was conducted to evaluate the content and effectiveness of the course. The overall response from students regarding whether the course met their expectations was very positive. Here is a summary of results of the survey:

- This course helps students to learn various wireless technologies.
- Students have a better understanding of wireless networks issues.
- The hands-on labs were very useful to get students engaged in learning.
- Although some of the labs are complex, it is rewarding to see the outcomes of them.

The future improvement for this course is to add more advanced hands-on labs involving wireless networks technologies and tools.

Conclusions

Wireless networks courses become increasingly popular in colleges (including community colleges) and universities. In learning the concepts of wireless networks via hands-on labs, students get ample opportunities to understand the underlying security technologies that prepare the engineers and technologists of the next generation. The objective of this paper was to describe the mobile and wireless network course using laboratory and project assignments. Students carry out experiments using Cisco and Linksys networking devices such as switches, routers and APs, submit lab reports and completed evaluation forms to give a feedback in order to improve and update the assignments for upcoming semesters. Students found this course along with lab assignments useful in understanding the theory of mobile and wireless networks, and

gaining practical experience. Consequently, students have shown great enthusiasm in this course, and student interest is expected to grow as we offer this course again.

A course in wireless networks has been developed for computer information technology students. Due to the shortage of similar courses, this is the first of its kind providing the students solid practical skills at the undergraduate level. The primary objective of this paper was to present hands-on laboratory assignments in wireless networking. Few newly developed significant hands-on examples are presented. WPA2 based wireless security labs are carried out by the students. These labs help graduating students to improve their skills that enhance the job hunting skills and marketability of them. In the future, more advanced labs would be developed to cover advanced topics in wireless network such as network management, etc. Tomato open source firmware upgrade could be used to perform various lab activities instead of DD-WRT open source firmware such as RADIUS server, QoS, etc. Moreover, this course will also benefit industry by offering skills which are practical and valuable.

We believe that this paper will help others to reuse, redesign and redevelop hands-on modules for mobile and wireless networking courses in both electrical engineering and computer science programs. Some these hands-on labs could be used as either introducing laboratory modules in existing computer network courses or to aid in the creation of new stand-alone mobile and wireless networking course.

Bibliography

[1] Abbott-McCune. S., Newtson, A. J., Girard , J., Goda, B. S., (2008). Developing a Reconfigurable Network Lab, Proceedings of the 9th ACM SIGITE conference on Information technology education, pp255-258

[2] Cannon, K., Lab Manual for CWNA Guide to Wireless LANs, Second Edition, Thomson Course Technology, 2006.

[3] Cao, X., Wang , Y., Caciula, A., Wang, Y. (2009). Developing a Multifunctional Network Laboratory for Teaching and Research, Proceedings of the 10th ACM SIGITE conference on Information technology education, pp155-160.

[4] Ciampa, M., CWNA Guide to Wireless LANs, Second Edition, Course Technology Incorporated, 2006.

[5] Cisco Systems Inc., (2002). A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite, Retrieved March 19, 2010, from Cisco website: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

[6] CIT Program at NKU, http://informatics.nku.edu/csc/undergraduate/cit/index.php, last accessed March 19, 2010.

[7] Department of Computer Science at NKU, http://informatics.nku.edu/csc/index.php, last accessed March 19, 2010.

[8] Hartpence, B. H. (2009). QoS Content and Experiences for IT, Networking and Security Programs, Proceedings of the 10th ACM SIGITE conference on Information technology education, pp60-64.

[9] Helps, C. R. G., Ekstrom, J. J. (2008). Evaluation of a Computer Networking Class in Information Technology, Proceedings of the 9th ACM SIGITE conference on Information technology education, pp259-268.

[10] Hernandez-Leo, D., Asensio-Perez, J. I.., and Dimitriadis, Y. (2006). Collaborative learning strategies and scenario-based activities for understanding network protocols. In Proc. Frontiers in Education Annual Conference., 2006.

[11] Hill, J. M. D., Carver, C. A. Jr., Humphries, J. W., Pooch, U. W. (2001). Using an isolated network laboratory to teach advanced networks and security, ACM SIGCSE Bulletin archive, 33(1), pp36-40.

[12] IEEE 802.15 WPAN High Rate Alternative PHY Task Group 3a (TG3a), Dec. 2002 [Online]. Available: http://www.ieee802.org/15/pub/TG3a.html, last accessed March 19, 2010.
[13] IEEE 802.16-2004, IEEE Standard for Local and Metropolitan Area networks-Part 16: Air Interface for Fixed Broadband Wireless Access. (2004).
[14] IEEE, Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specification, IEEE 802.11 Draft Version 4.0, May 1996.
[15] Jasani, H., (2007). Developing an Innovative Mobile and Wireless Networks Course, NMW Section of ASEE, Houghton, MI.
[16] Meiselwitz, G., (2008). Information Security across Disciplines, Proceedings of the 9th ACM SIGITE conference on Information technology education, pp99-104.
[17] Northern Kentucky University (NKU), http://www.nku.edu/, last accessed March 19, 2010.
[18] Oh, T., Mishra, S., Pan, Y., (2009). Teaching High-Assurance Internet Protocol Encryption (HAIPE) Using OPNET Modeler Simulation Tool, Proceedings of the 10th ACM SIGITE conference on Information technology education, pp161-165.
[19] Rosenberg C., Koo, S. G. M. (2002). Innovative and easy-to-deploy communication networking laboratory experiments for electrical and computer engineering students, Proceedings of 32nd Annual conference on Frontiers in Education, Como, Italy.
[20] Yuan, D., Zhong, J., (2009). An Instructional Design of Open Source Networking Lab and Curriculum, Proceedings of the 10th ACM SIGITE conference on Information technology education, pp37-42.