SETTING UP A MODULAR COMPUTER LAB WITH LIMITED RESOURCES

Stephen O. Agyei-Mensah

Hassan B. Ndahi

With a little bit of imagination and ingenuity, laboratories can be created with domestic-grade, hand-me-down, or refurbished equipment at very little cost.

Introduction

Recent technological developments in information and communication technology are adding new dimensions to the strategies and instructional tools available for teaching and learning. Technological systems that are controlled by a computer provide a rich learning environment that exposes the learner to a variety of representations and configurations, such as realistic models, graphics, and simulation visualization (Doppelt, 2005). Because of the capability of computers today, teaching hands-on technology laboratory courses using tools, equipment, and machines in a traditional laboratory setting is undergoing transformation from strictly lecture and hands-on activities, to a computer-based virtual demonstration (Borchert, 1999). This transformation has reduced a range of problems for students such as inadequate number of apparatus, equipment, and tools, safety issues, inability to use some of the tools and equipment, and time constraints in completing hands-on projects (Haque, 2000).

Numerous computer software applications are available for teaching and demonstrating lab activities through simulation and visualization. This innovation is in line with industry transformation as well. The industry today uses computer software for design, manufacturing, and product testing through simulation or virtual means. This innovation introduces students to the real-world situation after graduation. It is also creating a new and exciting learning environment for both students and teachers. (Roccetti, 2001).

If technology laboratory courses—for example, construction, manufacturing, computer repairs, graphics communication, production technology, transportation, energy and power—are to have separate computer labs, as in most cases, this can be expensive. Certainly, not all programs can afford the cost of setting up a computer lab for each course. One way to solve this problem is to set up a multipurpose computer lab with simulation and visualization software to teach hands-on laboratory activities. The simulation and visualization tools use animation to show how an input/output device functions (Carpinelli, 2004). Computer simulation is an extremely useful tool for conveying engineering concepts to technical as well as non-technical audiences (Cheok, 1993).

Because of budget constraints facing programs with hands-on laboratory courses, it can be cost effective to set up a multi-purpose computer lab that could serve all programs. Students can take part in setting up the computer lab and the installation of software for most of their lab activities. The hands-on exercises to set up a multipurpose computer lab require devices like the Cisco Aironet access point or 3Com AirConnect access point and Cisco Catalyst 1900 switches (Campbell, Calvert & Boswell, 2003). These devices have been used for lab setup exercises in many computer information systems' lab setup instructions. In 2002, these pieces of equipment ranged in cost from $1,000 to $2,500. They now range between $500 and $1,000. However, a little ingenuity can reduce the cost even further.

Sometimes students feel more comfortable with the reconfiguration of older equipment because of familiarity or the lack of oversight by the information-technology staff. There are many inexpensive domestic networking devices on the market whose configuration can offer students the same experience as the expensive Cisco and 3Com devices. For example, Linksys 8-port switches, Linksys 802.11g wireless access point, SMC-managed switch with VLAN capabilities, and D-Link 802.11b wireless network interface cards, all for about $200. The prices for these devices are still declining, just like the prices

of Cisco and 3Com devices. The only disadvantage in using the domestic devices instead of commercial devices is that professors may have to be a little creative in adapting the instructions in the textbooks for the domestic devices. However, the advantages of such an approach are that students welcome hands-on exercises on familiar devices. Additionally, limited departmental and university resources are not stretched, and hands-on activities are easily demonstrated by adapting instruction accordingly.

Computer Lab Network Configuration

The lab is divided into four quadrants, with six computers per quadrant and four different classes assigned to the quadrants (see Figures 1 and 2). There are two instructor workstations for demonstration to students (see Figure 3). The computers can be "hand-me-downs" from the university main general lab when it is upgraded to newer technologies.

Figure 1. Quadrants A and B.

Figure 2. Quadrants C and D.

Figure 3. Instructor Workstations.

Each student is assigned a shuttle with its own hard drive, such as shown in Figure 4. It is the responsibility of each instructor whose class is assigned a quadrant, to schedule his or her students so that only six of them are in there at the same time. With this arrangement, the lab can accommodate students from four different classes doing their projects in the lab at the same time, i.e., communication, production, energy and power, and computer repairs.

Figure 4. Workstation Shuttle Drive.

There is a low-end IBM eServer set up as an Internet gateway to provide Internet access with Network Address Translation to restrict direct access to a campus network. This machine has a second hard drive, so it is also used as a file server (see Figure 5 – black machine).

Figure 5. Internet Gateway and TFTP Server.

There is also an old, "hand-me-down" tower computer with three shuttles set up as the Trivial File Transfer Protocol (TFTP) server for six Cisco 2500 series routers. It doubles as console for the same routers and has no connection to the campus network and, therefore, the Internet, for security reasons.

The lab has a cabinet with rack-mounted devices including two 24-port patch panels, six Cisco 2500 series routers, two D-Link 26-port switches, and one multi-speed 8-port SMC switch with VLAN functions. This is a security feature that allows up to eight workgroups to operate separately without file-sharing, placing a virtual firewall between them to protect from unwanted access. Packets are physically unable to be sent between different work groups through the switch. This feature can be disabled or enabled (Kay, 2003).

Internet connectivity is provided to the workstations through a patch panel and a D-Link switch through NAT with the IBM gateway and a Linksys WAP. The other switch provides connectivity from workstations to the Cisco routers through hyper-terminal and telnet sessions over TCP/IP.

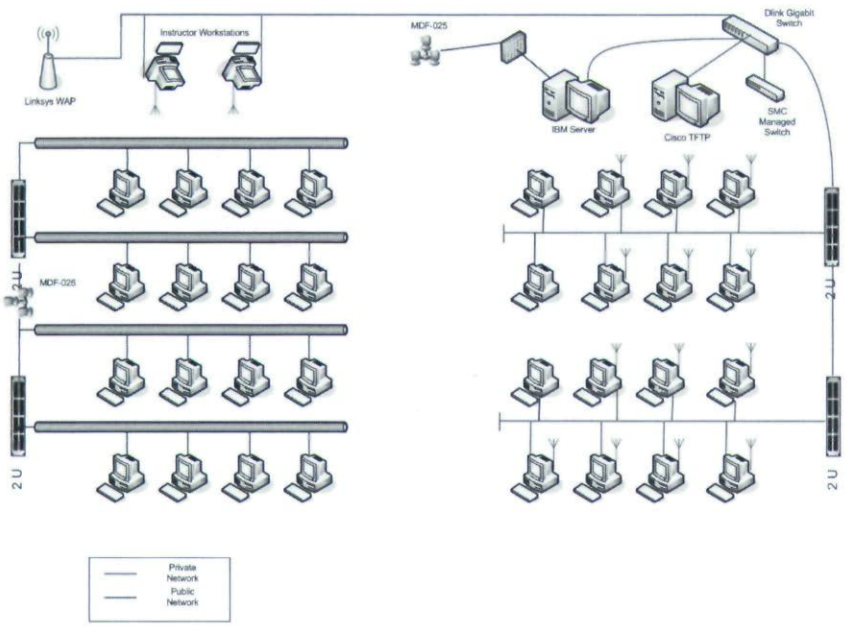

Figure 6. Lab Network Topology.

Figure 6 shows the network topology of the lab, incorporating the equipment described in the paragraphs above. All the equipment assembled above costs under $1,000—they are very low-cost network devices. These have allowed the delivery of instruction incorporating hands-on projects in technology-related classes. These devices enabled students to perform several lab activities, including setting up wireless local area networks (WLANs), honey pots, virtual local area networks (VLANs), tunneling, bastion hosts, monitoring, encryption, wireless security, simulation, and visualization etc.

Students are required to bring their own wireless network interface cards (WNICs) to lab sessions since they are so small, could be easily misplaced, and are so inexpensive now. Also, the students will take better care of them, it will avoid sharing, and everyone will have an opportunity to perform the tasks (as opposed to group situations where there are fewer devices and some students become spectators). The activity that follows is used to secure a WLAN.

Wireless LAN Lab Setup

Devices Used:

1. Wireless access points (WAP) of any brand.
2. Computers to be wired into the WAP used as a configuration console.
3. Wireless network interface cards (WNICs) of any type (USBs are less expensive).
4. Computers on which to install the WNICs.

Setup tasks:

After you have set up the WAP and WNICs with the default settings, tested them and found them working, you need to secure your wireless connections to prevent unauthorized access to and utilization of your network. You can secure your WLAN by changing the default settings on the WAP. Don't forget to test your wireless connections after each step so as to eliminate as many variables as possible if things don't work at a particular point (Morgan, 2004).

It is best if students work in groups of at least two.

1. Disable the wired NICs on all computers that are going to access the WAP with a WNIC.
2. Install WNICs and their drivers on one or more computers, following the instructions of the manufacturers and making sure that each WNIC is set to obtain its IP address automatically.
3. Set up the Linksys WAP and connect it to one computer with a CAT5 cable, according to the manufacturer's instructions. This will be the wired configuration console, which is not very critical since you can access the WAP through the wireless clients as well.
4. Test your wireless connections on the client workstations with the default settings, and if everything is working properly then you are ready to set up the basic security features on WLAN.
5. At the configuration console or wireless client workstation, start your Web browser.
6. In the address bar, type 192.168.1.1
7. A window should open asking for a user name and password.
   a. no user name
   b. password is **admin**
8. Change default password from **admin** to your **last name**.
   a. Test the default password.
   b. Test the new password.
   c. Test access to the WAP configuration setup with the clients.
9. Change the **default SSID** to your group number (e.g. **group01**).
   a. Test client access—there should still be connection.
10. Disable **SSID broadcast.**
    a. Test client access—there should be no connection.
11. Manually set up SSID on the clients—there should be connection now.
12. Change default IP address from **192.168.1.1** to **192.168.0.176**.

a. Test access with default IP address—there should no access.
b. Test access with new IP address—there should access now.

13. Enable **WEP** encryption and set a pass phrase and/or generate encryption keys.
    a. Test access—there should be no access.
    b. Set up encryption on clients and test access—there should access now.
14. Enable **MAC address filter** and specify the MAC addresses of the WNICs that are allowed to connect to your WAP.
    a. Put in the MAC address of the console first.
    b. Put in the MAC addresses of some of the clients, and not others.
    c. Test access by all clients—some should connect, others shouldn't.
15. Specify the **number of connections allowed.**
    a. Make the number smaller than the number of clients and test access by all clients and let clients report results.
16. Change the **default starting IP address** to something else and verify the DHCP address range the system generates based on the number of connections allowed and the starting IP address.
    a. Assign static IP addresses out of the new range to some of the clients and test access by all clients and let clients report results.
17. Explore the other security features, like filtering IP address range, filtering port range, filtering MAC addresses, filtering multicast, and filtering Internet NAT redirection.
18. Reset the WAP after you are done either from the Web interface or the reset button on the WAP.

By this time, the students should have a good understanding of how to secure a wireless local area network.

As basic and inexpensive as a Linksys WAP is, you can see that there are several options for securing a wireless network, and the experience should be similar even if you were using a more expensive Cisco Aironet or 3Com Airconnect hardware.

Summary

The pressure on educational institutions offering programs related to technology is mounting because of rapidly changing technologies. Students coming out of these programs should have some competencies in the setup, configuration, and use of the equipment in the field. Shrinking budgets in schools and colleges have been a limiting factor affecting institutions' ability to keep up with equipping their labs to reflect industry standards. This situation certainly affects the ability of the institutions to offer meaningful hands-on practice to students. However, with a little bit of imagination and ingenuity, laboratories can be created with domestic-grade, hand-me-down, or refurbished equipment at very little cost. In review, we have illustrated the setup of a computer lab with discarded computers and domestic-grade equipment and presented the use of the lab to provide a hands-on class activity to secure a wireless local area network similar to the way it would be done in industry.

References

Borchert, R.(1999). Development and assessment of hands-on and visualization modules for enhancement of learning in mechanics. *ASSE Annual Conference Proceedings and Exposition: Engineering Education to Serve the World.* Charlotte, NC.

Campbell, P., Calvert, B, & Boswell, S. (2003). *Security+ guide to network security Fundamentals.* Boston, MA: Thomson Course Technology.

Carpinelli, J.D. (2004). The relatively simple computer system simulator—a tool for Computer system organization and architecture. *Computers in Education Journal, 14*(4), 36-41.

Cheok, K.C. (1993). Computer visualization teachware for evaluating the performance of control system. *Proceeding of the American Control Conference Part II,* San Francisco, CA

Doppelt, Y. (2005). Assessment of project-based learning in a mechatronics context. *Journal of Technology Education, 16*(2), 7-24.

Haque, M.E. (2000). Java simulation-based soil mechanics laboratory course studio. *Proceedings of the ASEE Annual Conference and Exposition: Engineering Education Beyond the Millenium*, 3895-3901.

Kay, T. (2003). *Mike Meyer's certification passport Security+*. Mcgraw Hill Osborne, New York, NY.

Roccetti, M. (2001). A design for a simulation-based multimedia learning environment. *Simulation. 76*(4), 214-221.

Stephen O. Agyei-Mensah *is an associate professor in the Department of Computer Information Science at Clarion University of Pennsylvania, Clarion, Pennsylvania. He can be reached via e-mail at smensah@clarion.edu*

Hassan B. Ndahi *is an associate professor in the Department of Occupational and Technical Studies, at Old Dominion University in Norfolk, Virginia. He can be reached via e-mail at hndahi@odu.edu*