A VENDOR NEUTRAL LOCAL AREA NETWORKING LABORATORY COURSE

Samuel Liles

Purdue University Calumet, Indiana; Email: sliles@purdue.edu

ABSTRACT

The successful execution of a local area networking course that meets the first objective of a vendor neutral environment and does not require substantial infrastructure is an important goal. The second objective to be met with a vendor neutral laboratory course is teaching the fundamentals of local area networking in an open and exciting atmosphere of discovery. There is a particular set of laboratory exercises that can support a course environment that meets such diverse objectives. Having those laboratory exercises vendor and teaching text neutral becomes a challenging endeavor.

The details of the laboratory exercises examine the overall objective of the laboratory requirement, the high level view of the course information, and basic set up information for the laboratory exercises. Each laboratory exercise should have a specific set of outcome based objectives that map to the course level within the curriculum, the laboratory objectives should map to the course correctly, and the topics should assist in building the steps of the course. All of this meshing of objectives to curriculum is done in a vendor neutral environment while exposing students to the concepts of local area networking that can be applied to all vendor devices. The basics of the laboratory local area networking course include such diverse topics as cabling, TCP/IP, switching on the local area network, broadcast devices, and planning. The laboratory course introducing local area networking builds upon previous theory courses, and then continues to build upon each laboratory experience within the course.

1. INTRODUCTION

Simple, fast, and cheap are used to describe many technologies in today's world. A vendor neutral environment allows for a highly flexible learning environment that supports the outcome based objectives of a course. Though vendors will find themselves within specific niches it is possible to circumvent vendor specific technologies utilizing a variety of open source technologies (Zimmerli). Specifically it appears that almost the entire networking laboratory can be duplicated utilizing a variety of tools. It is important to note that just replacing equipment to make a laboratory environment would be expensive, not necessarily serve the student, and in

itself become a vendor specific environment. Who could really say a networking student has the best learning environment if they never saw a Cisco router?

Driving a specific objective that a course will easily map to the Bloom taxonomy it became imperative that the student experience encompass a group of goals (McKeachie). Starting with discovery and working with the student to evaluative thinking within one course led to some choices on what topics to include. Starting with the basic hardware devices (including cabling), and working through the advanced hardware devices to include switches, the course was created with out a hardware specific component. Firewalls can exist as a Cisco device, or they can exist as a Microsoft device. As a firewall is the border of a local area network working backwards, devices are added to the network such as switches, hubs, servers, and work stations.

A standardized laboratory essay is expected from each student or student team. The laboratory essay has an abstract, steps of the process as the student worked a problem, issues or concerns section, and conclusion. The conclusion is written separately by each student in a team thereby giving a personal response by each student to the laboratory essay (McKeachie). This standardized write up is used across several courses and the students are accustomed to the concept of some laboratory exercises are individual effort and some exercises are collaborative.

2. THE LAB ENVIRONMENT

The lab is a converted technology classroom. Two equipment racks contain a variety of devices that are shared among different classes. The racks specifically contain hardware devices such as hubs, switches, and routers. The first experience for the student is working from the Ethernet port on the back of their computer to the port in the wall of the classroom, mapping that port to the punch down found on the rack. That will show the student what is the current configuration of the network. Students are required to "repair" the network at the completion of the laboratory process.

An interesting device that exists in the network configuration is a Digi Port Concentrator (Digi). This device as used by industry allows multiple students to have serial access to different devices. As a concentrator network access to the "Digi" creates a shared environment and greatly facilitates hardware devices configurations. Students are given a log in to the device and allowed to configure a limited number of devices. In more advanced classes the students will actually configure and control the device for the introductory students. The "Digi" though vendor specific allows for the manipulation and control of any vendors equipment that is configurable from the serial port. This is especially important with devices that have boot commands on the serial port such as the Cisco router

.

2.1 Laboratory exercises 1 and 2

The first two laboratory exercises fill a niche in the curriculum. As in lecture, the students are still exposed to the first concepts of the local area network and it is imperative that previous skills developed are built upon. Within the current environment the expectation exists that students will have the ability to install any standard operating system. Within the curriculum

laboratory exercise one is the first time the student is asked to dual boot a work station. The latest version of Windows Server 2003 is installed on to a workstation removable disk leaving enough room to also install Linux Fedora Core 3. This allows the laboratory exercises to have a significant amount of flexibility in the adoption of specific operating system technologies.

The second laboratory exercise would seem trivial at first within a sophomore course, but it is a remarkable skill and requirement for industry. The student is asked to create a set of two cables to the required standards. The first cable, a simple CAT5 Ethernet cable, is usually created with no issues. The second cable is a standardized cross-over cable and the exercise of creating the cable begins the process of students discovering there is something different between the ways network hardware devices talk to each other. The students are told during laboratory exercise two that they will need these cables in the future to hook up network devices. The students are asked to research the rules on which cable works with what devices and in which scenarios.

2.2 Laboratory exercises 3

Client configuration and discovery is accomplished utilizing a set of known client tools. Specifically for a windows client the commands bootcfg, getmac, pgresult, ipconfig, netstat, msconfig, tracert to a known address, pathping to a known address, route print, arp –a, and finally system info are commands that student utilize to gather specific information about their system. This discovery laboratory exercise allows the student a chance to implement the first level of critical thinking skills. A second often over looked benefit of this laboratory is that students now have a tool set of discovering issues with a local area network.

As part of our vendor neutral environment students are asked to research and provide a set of commands that work within the Linux environment that they are able to boot into. Each of the commands in the windows environment maps to a Linux command and the period of discovery in finding the correct commands gives the student their first chance at detailing and researching answers to a technical issue.

2.3 Laboratory exercise 4

Ping utilities and internet protocol address tracing utilities open a new awareness within the student to the power of TCP/IP. A series of tools have been added to the curriculum to allow for a multiple vendor and vendor neutral environment. It may be easier to discover and teach the use of one tool, but experience with students suggests that they will go further and experiment on their own with the tools once they are exposed to the tools.

IP-Tools (IP-Tools) has multiple features and capabilities to diagnose and analyze IP networks. Students do a variety of self directed exercises with this tool and advance to other tools. Sam Spade (Sam Spade) is an interesting tool that students enjoy experimenting with and details similar but different information from the predecessor IP Tools. Sam Spade is a freeware download. Neo Trace (Neo Trace) has visual and audio feedback. Once students are exposed to this tool they spend significant time playing and learning how the tool works. With this tool in place and the background of the other tools students discover how “whois” and “finger” commands work. They understand that the tools are using Internet Protocol to analyze and

provide the feedback. These tools though demo ware provide an open and vendor neutral answer to teaching high level network discovery.

2.4 Laboratory exercise 5 and 6

The manipulation and understanding of Internet Protocol addressing schemes has been covered in the literature extensively, and the seminal book by Douglas Comer (Comer, 2000) is a handy reference. Within this laboratory exercise students who have had the lecture portion and theory are asked to convert Decimal, DWORD, Octal, Hexadecimal, and find the DNS registry for IP addresses by hand. This is important for system administrators to understand as different operating systems will handle the IP address scheme in either of these formats (e.g. Solaris subnets using hexadecimal).

Melding in with the prior laboratory 5 we find the laboratory exercise 6 the act of subnetting will build upon previous successes. Several methods in lecture are taught that are independent of vendor methods. Within the lab they begin by using the "by hand" methods to provide subnetting to different classes and address spaces. Students figure the number of hosts and other typical subnetting tasks.

Once students have successfully completed the task of manipulating the IP addresses by hand they are exposed to a tool provided by Solarwinds (Solarwinds). The Subnet calculator provides extensive information including the conversion factors to other formats. More importantly it provides the number of hosts. The subnet calculator is freeware and available for download. Students are also exposed to the Boson subnet calculator (Boson) also available for free as well as with many text books. This provides the students a few tools to evaluate in preparing answers to questions posed within the lab.

2.5 Laboratory exercise 7

Once a network has been set up or a client is on the network there are a variety of things that can occur and cause problems. Congestion, IP conflicts, DNS, and DHCP issues. To create a successful laboratory experience students are asked to install a free open source product called Ethereal (Ethereal). Ethereal is installable on either Linux or Windows. The Windows version requires WinPcap to be installed first, but with that in place students should be able to view network traffic easily. There are ethical and legal issues outside the scope of this document that should be considered when sniffing traffic, but the process within the laboratory should be sanctioned.

Students begin by executing commands (e.g. on Windows operating systems flushdns, registerdns, ipconf /renew, etc…) . The students gather the packets from this exercise and watch the commands as they register on the network, and how they are replied to. The tool Ethereal makes this extremely interesting for the students as they can see the binary, hexadecimal, and textual representation of the TCP stream. Further experimentation by opening a telnet, ftp, and HTTP session show some of the flaws in the TCP/IP protocol and security issues with the local area network. Students are amazed to see clear text passwords sent to machines, and invariably some student on a shared medium will check their personal email and expose their password. As

a policy all students are told that there is no expectation of privacy or security of data within the laboratory environment. This is an excellent time to introduce further topics in security of local area networks.

2.6 Laboratory exercise 8

The ping or ICMP laboratory exercise has the student setting a variety of flags on ICMP packets and observing the packet structure in Ethereal. Though Windows is used as an example this will work in Linux and a variety of other operating systems including Macintosh OS X. A few students found it interesting that constraints and packet structure could change between operating systems. Utilizing Ethereal as the monitoring devices students are asked to open a command window type "ping -?", and "tracert --?" this provides the switch options for each command. Utilizing the switch options of each command the students experiment with the commands and the switches finding the differing packet forms and types that the switches produce. Students are exposed to further depth of the ICMP structure and can observe the specific difference. This also builds upon the knowledge students will be required to utilize in future courses for troubleshooting. Specifically several of the skills required in security courses can utilize these skills for operating system fingerprinting and analysis. Students who complete this laboratory exercise should have a deeper understanding of exactly what ICMP is doing as it operates on the network.

2.7 Laboratory exercise 9

Students have dealt with all of the elements of diagnosis, design, client side utilities, but they have not built a local area network until this laboratory exercise. Buildings upon the successes of previous laboratory exercises students add a few new skills to their toolbox of success. Students working in groups develop IP naming schemas based on earlier laboratory exercises. Students are asked to use differing classes and plug the computers into the different hubs that are not connected directly.

Though the hubs may be connected to a switch the broadcast domains are separated. Students can see how this would work. Students in each group are then asked to put both groups' connections into the same hub. As broadcast devices this creates chaos and the computers cannot connect reliably and they have significant issues. To insure the creation of network traffic able to saturate the network a vendor neutral Network Traffic Generator (Traffic) is utilized. Students evaluate each design via Ethereal, and simply watching the collision lights on the Hub.

2.8 Laboratory exercise 10

The final exercise requires students to build a Virtual Local Area Network (VLAN). Though at this time 3COM switches are utilized any switch with the ability to implement a VLAN could be used. VLAN's can also be built in Linux and with specialized operating system software distributions. Students create the VLAN based on a scenario, are provided the manuals, and the details of how VLAN's work as part of the lecture. Students are also exposed to a port concentrator that allows several students access to the same switch and login capabilities to numerous networking devices.

Students experiment using the tools they have already been given, and push the boundaries of traffic and congestion control. As part of the scenario students are asked about how to pass traffic out of their VLAN to the network. Some switches have an analyzer port, and more specifically some switches have backbone routing capability on a designated port. Students exposed to these specific skills will be able to analyze and build most local area networks.

3 SUMMARY AND CONCLUSION

The creation of a laboratory course that includes significant content that is vendor neutral achieves several objectives. The objective of being inexpensive and easily replicable is an asset to academia. The fact that each of these laboratory exercises can be replicated by the student with minimal equipment encourages life long learning. Often the objective of comparing the similarities between vendors is not considered, while showing the vendor specific method of accomplishing a task is validated. Though all course work is constantly moving with the changes in technology it is interesting to note that the concepts of networking remain stable while the equipment that they are using forges ahead to the tune of change. Student feedback from the course shows an increasing interest in networking, and students from this course in other courses are found to have a good grasp and understanding of the principles.

REFERENCES

Boson TCPIP Subnet Calculator, "http://www.softforall.com/HomeEducation/TeachingTools/Boson_TCPIP_Subnet_Calculator05160023.htm" (Last accessed January 26, 2005)

Comer, Douglas (2000) "Internetworking with TCP/IP Principles, Protocols, and Architectures" 4th Edition, Prentice Hall.

Digi CM, "http://www.digi.com/products/consolemanagement/digicm.jsp", (Last accessed January 26, 2005)

Ethereal: A Network Protocol Analyzer, "www.ethereal.com", (Last accessed January 26, 2005)

IP-Tools, "http://www.ks-soft.net/ip-tools.eng", (Last accessed January 26, 2005)

Mckeachie, Wilbert J. et al. (2002) "Teaching Tips Strategies, Research, and Theory for College and University Teachers" Eleventh Edition, Houghton Mifflin.

Network Traffic Generator "http://sourceforge.net/projects/traffic/, and http://robert.rsa3.com/traffic.html", (Last accessed January 26, 2005)

Neo Trace Express 3.25, "http://www.networkingfiles.com/PingFinger/Neotraceexpress.htm", (Last accessed January 26, 2005)

Sam Spade, "http://www.samspade.org", (Last accessed January 26, 2005)

Solarwinds Advanced Subnet Calculator, "http://www.solarwinds.net/Tools/Free_tools/Subnet_Calc"

WinPcap – Windows Packet Capture Library, "http://winpcap.polito.it", (Last accessed January 26, 2005)

Zimmerli, S., M. A. Steinemann, et al. (2003). "Resource management portal for laboratories using real devices on the Internet." Computer Communication Review **33**(3): 145-151.