VLabNet: A Virtual Laboratory Environment for Teaching Networking and Data Communications

Valerie J. H. Powell
powell@rmu.edu
John C. Turchek
turchek@rmu.edu
Peter Y. Wu
wu@rmu.edu
Lawrence C. Franzi
franzi@rmu.edu
Computer and Information Systems, Robert Morris University
Moon Township, PA 15108 USA

Randall S. Johnson
johnsonr@rmu.edu
Ian W. Parker
parker@rmu.edu
Technical Services, Information Systems, Robert Morris University
Moon Township, PA 15108 USA

Christopher T. Davis
davisc@rmu.edu
Educational Technology Center, Robert Morris University
Moon Township, PA 15108 USA

ABSTRACT

This paper describes a way of teaching computer networks with extensive hands-on experience and flexible access, using an array of Xen virtual machines, simulation of routing protocols, and a Cisco router.

Keywords: networks, virtualization, protocol stack

1. INTRODUCTION AND RATIONALE

This paper describes a way of teaching computer networks with extensive hands-on experience, seeking to address the forms of abstraction posed by the use of reference model protocol stacks common to the understanding and implementation of computer networks. A small number of themes guide the student through the material: routing and encapsulation are foremost among them

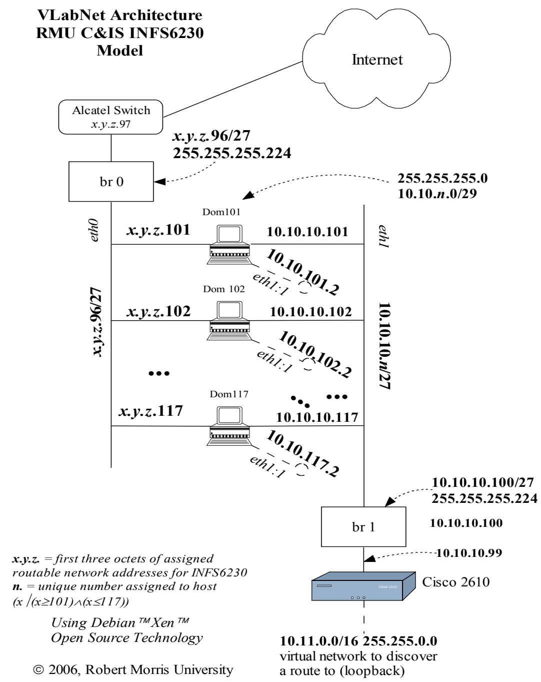
There has been a rapid expansion of using practical laboratory exercises to teach information security and networking as documented in a number of listings and reports covering both academic and commercial settings (Alexander and Lee (2006), Baumgartner et al. (2003), Begnum et al. (2003), Cane and Leitner (2005), Chiroco et al. (2005), Dobrilović and Odadžić (2006), Harvey et al. (2006), Huntley et al. (2004), Kneale et al. (2004), Ma and Nickerson (2006), McEwan (2006), Nakgawa et al. (2003), Ouyang et al. (2005), Scheets et al. (2005), Wu et al. (2004). Powell et al. (2007) describes how a single integrated fundamental setup can serve both information security and network instruction.

The use of virtual machines in teaching information systems (I/S) courses at Robert Morris University (RMU) began in 2006. The initial decision was to exploit virtual machines in an information security course to give the students practice with intrusion detection and other information security activities. We decided that we wanted to use open source technology throughout our learning environment. The success with the information security course led first to the design of a version of the network to support the teaching of networking and subsequently led to integration of the designs of the two courses so that little or no change was required in moving from use of the Xen network facility for teaching information security to use of it for teaching networking.

Historically, specific activities initially chosen for implementation were use of *syslog* and the logger tool, centralized audit using *syslog* configuration, the Snort sensor and setting up local Snort rules, penetration testing (OS fingerprinting; a "mystery" operating system can be used on one member of the virtual machine group to provide practice), and use of *ping* and *telnet*. We did not want to assume that students in the information security course had sufficient capability with Linux to install the tools, so we provided the students with a Xen installation including all needed tools. Of course, instruction in the Linux environment and editing had to be taught for those not having prior experience with Linux.

We wanted this course to be effective for information systems students with a variety of backgrounds. Students could begin working with the technology in this networking course even with little prior familiarity with Linux and little prior formal networking instruction. This course was designed so that students received a configuration and did not have to install the original configuration, even though they would learn configuration with respect to certain tools as the course progressed. The Xen environment is set up "fresh" for each course offering by using a template. For contrast see the model presented in Krishnamoorthy (2007), where students design a network, starting with the requirements for a business. and including installing the network interface card, configuring the router, as well as doing wiring and cabling. In the case of the VLabNet examples presented here, students are learning fundamental network concepts by using a network.

With respect to model I/S curricula, the modules may be used with IS2002.6 Networks and Telecommunication and MSIS 2000.3 Data Communications and Networking.



The principal alternative to using VLabNet to teach networking is the traditional approach of lectures, textbook reading assignments, and simulator assignments. A simulation system used in the past at RMU for the same networking course is OPNET. The amount of student time spent using the simulator in such cases is far less than with VLabNet, where topics are introduced using the interactive environment, and students develop documentation of concepts and examples captured, as contrasted with highly structured research activities involving one or more experiments.

2. ARCHITECTURE

This project uses Debian Xen and the Quagga Routing Suite. Xen is a Virtual Machine Monitor (VMM) originally developed by the Systems Research Group of the University of Cambridge Computer Laboratory, as part of the UK-EPSRC funded XenoServers project. The Quagga routing suite simulates the RIP and OSPF protocols. A Cisco 2610 router was attached to the Xen array of virtual machines to provide some direct Cisco router experience. Since a single rack mounted server can deliver the array of virtual machines, no special hardware (wiring or garage drive) is needed. Students can access this system anywhere.

subnet	mask
x.y.z.96/**27**	255.255.255.224
10.10.n.0/**29**	255.255.255.0
10.10.10.100/**27**	255.255.255.224
10.10.10.n/**27**	255.255.255.224
10.11.0.0/**16**	255.255.0.0

Addresses and Masks
Figure 2.2

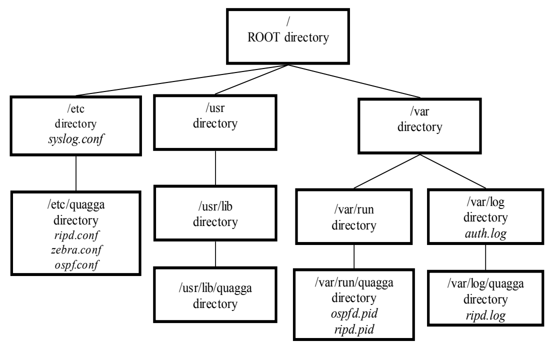
The learning environment was designed to support the exploration of networks and subnets, switches, bridges, routers, and of the individual host in the role of a router. As shown in Figure 2.1, each host has three different addresses, one each for the three interfaces: *eth0*, *eth1*, and *eth1:1*. For example, for host 101, those would be x.y.z.101 (x.y.z. represents the first three octets of VLabNet's externally routable IPv4 addresses) for interface *eth0* (an externally routable address), 10.10.10.101 for interface *eth1* (non-routable externally), and 10.10.101.2 for interface *eth1:1* (also non-routable externally. Students become accustomed to their assigned host having multiple addresses and to using the various addresses each for certain purposes and in certain situations.

A variety of addresses and corresponding masks were designed to assure a variety of address encounters and make it practical and necessary to learn about classless inter-domain routing (CIDR) addressing (see Figure 2-2). The interface identified as *eth1:1* has the property that the nodes reached by that interface are not connected with each other and can only be reached by the respective host to which connected. Thus the host becomes a router to nodes such as 10.10.101.2.

Students can explore the difference between the traffic on interfaces eth0 and eth1. In contrast to the information security course, where the emphasis is on eth0 traffic, in the networking course emphasis is on *eth1* and *eth1:1* traffic. They also work with the difference between the externally routable *eth0* addresses and the internally routable addresses on the other two interfaces.

3. ORIENTATION TO ENVIRONMENT

Orientation of students to the environment introduces the tools used in the course, the Linux environment, the 5-layer "hybrid" reference model, the ISO reference model 7-layer protocol stack, the directory structure of the learning environment (see Figure 3.1), and methods of documenting discoveries and progress.



Directory model (selected subdirectories) for RMU Virtual Laboratory Network (VLabNet) Hosts

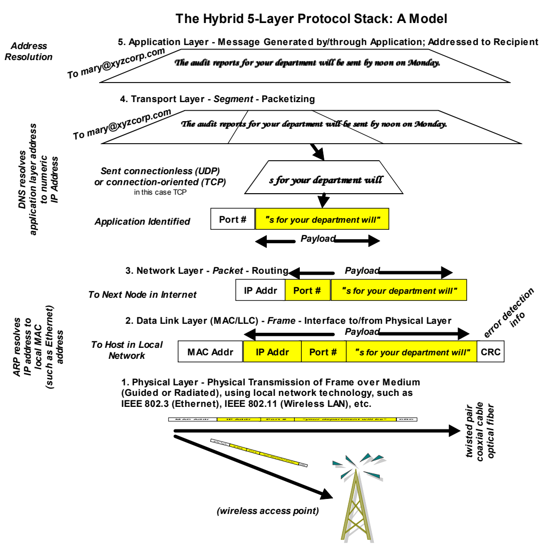
Students are given examples of what to look for in the traffic that they can capture using *tcpdump* and *tethereal* and practice capturing and documenting examples. Initially the course focuses on the structure of the components of the protocol data units (PDUs) and how to recognize the types of PDUs that they are assigned to document. Students are encouraged to work in pairs, which they can do in class, in the laboratory, or at home as they coordinate their efforts over the phone. Examples are posted in online documentation. The externally routable addresses for their virtual machines allow them to work wherever they wish.

These activities can be conducted during class time on wirelessly linked laptops. Frustrations with technology or concepts can be met and resolved collectively with the instructor as a "guide by the side" instead of a "sage on the stage." Such educational activities promote collaborative skills as required in the new management models (Tapscott and Williams, (2006)). As sharing skills develop, the classroom atmosphere becomes "electric."

Experience shows students rapidly learn, for example, to distinguish unicast, multicast, and broadcast addresses, and to understand layering in Internet messages. Online documentation shows examples to guide students in their efforts to capture and document assigned types of messages, and their features.

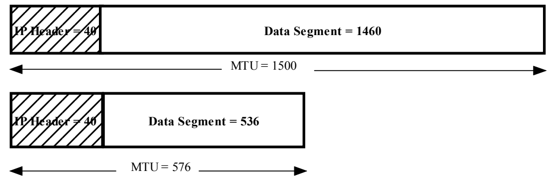
4. CONCEPTUAL THEMES

Several themes follow the learning process throughout the course: layered protocol stack reference models, routing discovery, encapsulation, addressing, data units, protocol identification, bit budget (Maximum Transmission Unit (MTU; see Figure 4.1), Maximum Segment Size (MSS). In performing the Generic Routing Encapsulation (GRE) tunneling exercise, students should notice the reduced MTU (1476) for the tunnel, due to more bits being consumed by headers in the encapsulation process. Here is an example of the "Protocols in frame" report for a captured tunnel message: `eth:ip:gre:ip:icmp:data`, documenting the encapsulation.



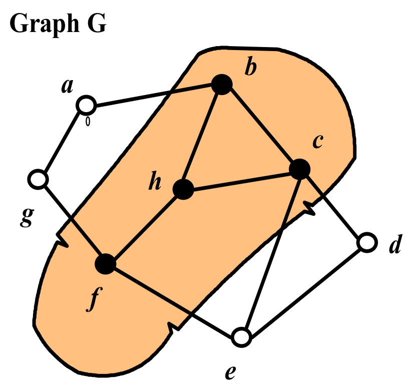
Protocol Stack Model
Figure 4.2

Future planning envisions adding Autonomous Systems (AS) and Border Gateway Protocol (BGP). Two protocol stack reference models are used in the course: the Hybrid Internet 5-layer protocol stack (Figure 4.2), and the ISO reference model 7-layer protocol stack.



Headers and Data Segments: MTUs
Figure 4.1

Students begin the course with a naïve impression of Internet messages that transmit Web and e-mail data. Gradually their perspective develops to include all the kinds of messages necessary to support the Internet as they observe traffic using the various interfaces available in VLabNet and document the different types of messages.



Vertices ***h*** and ***b*** are adjacent (path ***hb*** has a path length of ***1***) and are **therefore neighbors**.
So are ***h*** and ***f***, ***h*** and ***c.***
N(h), the **neighborhood** of ***h,*** is shown by vertices that have black fill; the vertices not in the neighborhood of ***h*** have no fill.

Note the use of the concept of neighbors in building *link state packets* for *link state routing* or in *distance vector routing* algorithms.

Neighborhood Graph Model
Figure 4.3

The most important theme in the course is routing discovery. Students are shown how to consult routing tables at different stages in the course and are encouraged to determine how the data in routing tables develops and is maintained. To ascertain where routing comes from, students explore routing information and routing information protocols. They begin with the concepts of neighbor and neighborhood, so that they realize that the "heart" of routing information and routing discovery is always direct communication among neighbors.

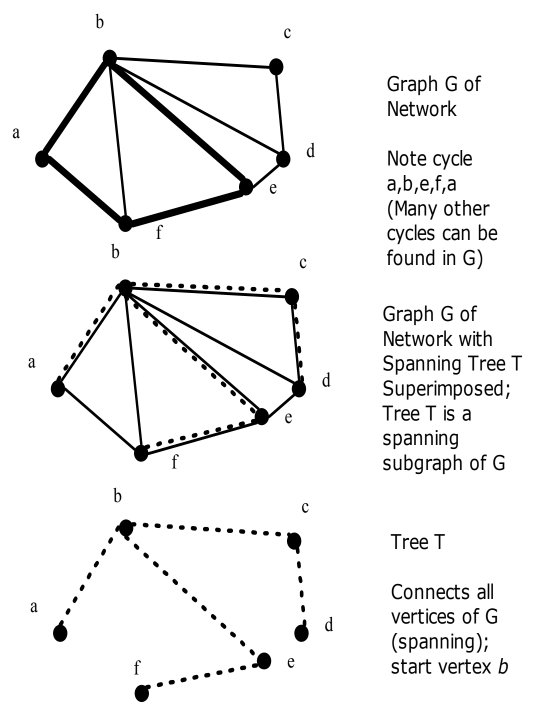
The sequence of exploration in the course is (1) static routing, (2) dynamic routing 1: Routing Information Protocol (RIP, distance vector; unicast peers), (3) dynamic routing 2: Open Shortest Path First (OSPF, link state; multicast peers), and (4) dynamic routing 3: a Cisco 2610 Router and Cisco's EIGRP rationale. The culmination of routing experience in the course is (5) using generic routing encapsulation (GRE) to establish tunnels. A tunnel needs to be established in both directions between a pair of hosts before proceeding to verification. Close teamwork collaboration is required in this process.

Students experiment with broadcast floods and verify the maintenance of spanning trees using the STP protocols.

To understand protocol data units and their components and encapsulation, they begin with the concepts of payload and "tare." They analyze data unit components to distinguish the payload from the other parts of a PDU component. In the process they learn about the concepts of message delineation, addressing at different protocol stack levels, differentiating types of messages, and error control information (CRC). They learn by inspection about length and specifying length, MTUs (see Figure 4.1), MSSs, fixed-length elements, and variable-length elements. They explore lengths of PDUs and PDU components by causing fragmentation (using *ping* to generate oversize packets) and documenting and analyzing the impacts of fragmentation. Concepts that seem very abstract in textbooks become practical exercises.

Students explore connection-oriented networking by identifying and documenting the elements of the TCP three-way handshake and other elements of TCP communication. *Ssh* connections can be captured from *eth0* traffic representing their own connections with their virtual machines.

Certain graph-theoretic concepts are emphasized in the course, particularly the tree (as an acyclic connected graph represented by the spanning tree protocol (STP) and other uses; see Figure 4.4), and neighbor (adjacent node) and neighborhood (the set of adjacent nodes; see Figure 4.3) as the "building block" of routing discovery. Coverage of the spanning tree leads to a discussion of when redundancy is beneficial in networking and when not. Practical examples of exploiting the spanning tree concept are Internet multicast routing, non-redundant bridging (IEEE 802.1D), and various Cisco switching protocols. Online documentation provides references to textbook discussions of these protocols and links to appropriate Cisco documentation. Coverage of the neighborhood concept (See Figure 4.3) supports discussion of link state and distance vector routing strategies as implemented in the RIP and OSPF dynamic routing protocols. In the exploration process students can observe and document routing discovery using these protocols. This exploration leads to discussion of the process of convergence in dynamic routing protocols as well as of how and why such protocols maintain a current representation of the state of the network.



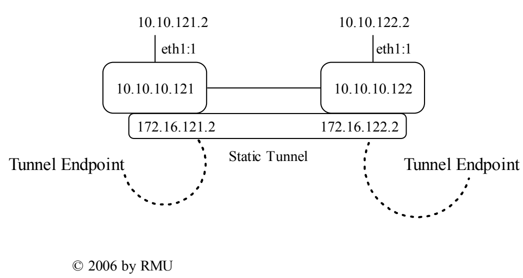
Spanning Tree Model
Figure 4.4

5. INSTRUCTIONAL STRATEGIES AND METHODS

The use of real-time simulations in the classroom is strongly supported by educational theory as a productive and effective pedagogical practice. Major theories that support the use of this technology include, Bloom's Taxonomy, Tomei's Taxonomy, and Gardener's theory of Multiple Intelligences.

It is a commonly held belief that students learn more efficiently when instructors engage them in higher order thinking. Virtual lab technology provides the instructor with the means to challenge students with these higher order tasks. The use of virtual lab technology is focused in the analysis, synthesis, and evaluation areas of the taxonomy. This is evidenced by the use of the technology in the classroom. As the students are using the virtual lab, they are constantly forced to make very quick connections between what they know and what they are experiencing. In addition, the real-time environment provides an excellent opportunity for the students to make predictions regarding network behavior and to test assumptions without damaging an exiting network infrastructure. This type of learning and experimenting is an essential and often overlooked element of an effective information systems curriculum.

RMU VLabNet Generic Routing Encapsulation Exercise



Model of Generic Routing Encapsulation
Figure 5.1

In addition to traditional educational theory, such as Bloom's Taxonomy (Bloom et al. (1956), virtual lab experiences allow instructors to provide students with higher order technology experiences as well. Tomei's Taxonomy is a widely accepted educational technology model that provides the framework for the proper use of technology in the classroom. The virtual lab technology touches on many of the levels of Tomei's Taxonomy and provides students with valuable higher order technology experiences. For example, this technology aligns itself very well with the Decision-Making and Integration levels of the taxonomy. In the Decision-Making level, students must "apply electronic tools for research and problem solving". (Tomei, 2001) Additionally, the virtual lab technology allows students and instructors to "[c]onsider the consequences of inappropriate uses of technology" and also allows them to "[a]ssimilate technology into a personal learning style". (Tomei, 2001) These instructional activities align with the Integration level of Tomei's Taxonomy and further reinforce the higher order technology skills that provide students with the most enriching classroom experiences.

Because of the vast differential of learning styles of students in college and university classrooms, it is essential to provide the most appropriate and adaptive learning experiences to accommodate the needs of each student. The use of the virtual lab technology conforms to the many of the dimensions of the Gardener's theory. Logical-mathematical and spatial dimensions are easily addressed during the use of the virtual lab. "The ability to handle long chains of reasoning and to recognize patterns and order in the world" (Kauchak and Eggen, 2005) is a hallmark of the logical-mathematical dimension. Allowing the students to experiment and create real world situations in the virtual lab fosters the reasoning and pattern recognition skills associated with logical-mathematical thinking. "The ability to perceive the world accurately, and to recreate, transform, or modify aspects of the world in the basis of one's perceptions" (Kauchak and Eggen, 2005), the defining characteristic of spatial intelligence, is a skill essential for network administrators and is a skill that is easily practiced in the environment of the virtual lab. By utilizing technology that addresses several different intelligences (Gardner, 1997), the instructor provides avenues to learning for a large array of students in the class.

The most-used exploration tools are *ping* (ICMP). *telnet* (TCP) and *ssh*, *netstat*, *arp*, *ip route* and *route, tcpdump*, *tethereal*, *traceroute*. The specification, configuration, and reporting tools are *netstat, ip route, ifconfig, ip addr*. Support tools are *ps, VMStat, date, ls, cd, jobs, kill*.

In the networking course the textbook (Tanenbaum (2003)) becomes a practical guide. In this instructional setting, students appeared to appreciate the technical level of the Tanenbaum text much more than in a course taught in the traditional manner. They learned to use Tanenbaum as a reference. In developing this paper we also reviewed a technical level textbook that might be used in such a course in Mexico: Molina (2006).

The principal resources valuable for the instructor are Schmied (2005), which was a major source of information in designing VLabNet, Sanders (2007), which provides many practical examples of what students can look for while exploring traffic patterns, Orebaugh et al. (2007), and Mancil (2002), especially Chapter 1 on "Routing Building Blocks," Odom and McDonald (2006), with excellent coverage of the routing table in Chapter 9 on "Basic Router Troubleshooting."

The networking course using VLabNet was designed to serve students with a variety of backgrounds. Sanders (2007) provides many examples of tasks that can be assigned to students with advanced interests, as in Chapter 8 "Fighting a Slow Network," while other students focus on basic concepts. Our experience has been that students with advanced interests receive an excellent experience working side by side with students having basic or introductory interests by paying attention to "internal differentiation" needs within the group of students. It is productive to involve students with advanced interests in peer tutoring, noting Madrid et al. (2007). Such students report learning more than they expected in the processes of peer tutoring and assisting students with less networking background.

Observer impressions of how this course design is different from traditional teaching of networks with lecture and laboratory cite the group experience with discussion and teamwork and immediate use of the virtual machine computing environment, augmented by some peer tutoring, as contrasted with students going from the lecture situation to a different environment, the laboratory, where they mostly work on their own. Any technical or learning problems encountered are dealt with through the presence of the instructor (and peer tutors).

The revision of the course to include the practical activities described here led to a corresponding revision of assessment. Practice and assessment items were designed that reflect the types of exploration pursued by students in the course. Topics covered in such assessment include CIDR notation, protocols and protocol stack layers as revealed by the notation in tethereal decoding, recognizing first octets of special significance (10, 172, 192, 127, 255, 0), and predicting masks for given network addresses. Assessment items that would have been difficult with book learning are easy with exploration of traffic and such items help students recognize the progress they have made.

The challenges of designing and implementing such a course include assuring that not just skills, but concepts are the focus of the course and that telecommunications and network topics not directly related to the VLabNet experience are adequately covered.

The final VLabNet assignment in the networking course, implementing tunneling using Generic Routing Encapsulation (GRE; see Figure 5.1), builds on everything learned so far in the course, especially on encapsulation, but also the selection and use of tools to test and verify the correctness of their configuration, and to make modifications where the configuration is not yet correct.

6. CONCLUSION

It was practical to redesign the course in networking to utilize a practical learning environment based on the use of Xen virtual machines. Students encounter the virtual machines configured and installed with tools in place and ready to use. Concept themes developed and repeated throughout the course helped students move from practical experiences involving group interaction to a technical level of understanding together with perspective on important concepts in computer networks. The technology used supports a wide range of learning environments from group work in the classroom to individual and small team work at home. Assessment had to be redesigned to accommodate the different type of learning in the course. Even students with little background in networking adapted readily to the assignments, which focused on identifying assigned protocol data units and their components.

ACKNOWLEDGEMENTS

The close collaboration of Technical Services, RMU Information Technology, is gratefully acknowledged.

REFERENCES

Alexander and Lee (2006). Alexander, M., and Lee, J. A., "A Scalable Xen and Web-based Networking Course Delivery Platform," Education and Technology (2006) at http://wwww.actapress.com/PaperInfo.aspx?PaperID=2750

Baumgartner et al. (2003). Baumgartner, F., Braun, T., Kurt, E., and Weyland, A., "Virtual routers: a tool for networking research and education," *Computer Communication Review* 33, 3 (2003), pp. 127-135.

Begnum et al. (2003). Begnum, Kyrre, Koymans, Karts, Krap, Arjen, and Sechrest, John, "Using Virtual Machines in System Administration Education," 4th International System Administration and Network Engineering Conference (2004), see: http://www.nluug.nl/events/sane2004/ ; http://www.nluug.nl/events/sane2004/abstracts/ab.html?id=115 ; and http://www.nluug.nl/events/sane2004/overview.html#115

Bloom et al. (1956). Bloom, B. S., ed., Englehart, M. D., Furst, E. J., Hill, W. H., Krathwohl, D. R., *Taxonomy of Educational Objectives: The Classification of Educational Goals*, Handbook 1: Cognitive Domain (McKay, 1956).

Cane and Leitner (2005). Cane, J. and Leitner, L., "A virtual network laboratory for instruction and research," Conference Proceedings – IEEE SOUTHEASTCON (2005), pp. 651-655.

Chiroco et al. (2005). Chirico, M., Scapolla, A.M., and Bagnasco, A., "A new and open model to share laboratories on the Internet," *IEEE Transactions on Instrumentation and Measurement* 54, 3 (2005), pp. 1111-1117.

Dobrilović and Odadžić (2006). Dobrilović, Dalibor, and Odadžić, "Virtualization Technology as a Tool for Teaching Computer Networks," *Enformatika* v. 13 (2006), 126-130.

Gardner (1997). Gardner, Howard, *Frames of Mind, The Theory of Multiple Intelligences* (Basic Books, 1997).

Harvey et al. (2006). Harvey, V. J., Johnson, R. S., and Turchek, J. C.. "A Model for Virtual Laboratory Intrusion Detection Experience," Kennesaw State University Information Security Curriculum Development (INFOSECCD) Conference, 2006.

Harvey et al. (2007). Harvey, V. J., Johnson, R. S., and Turchek, J. C. "Virtual Laboratory Intrusion Detection Experience for Information Systems Professionals," *Information Systems Education Journal, 5* (5). http://isedj.org/5/5/. ISSN: 1545-679X. (2007) (Online at http://isedj.org/5/5/; also appears in *The Proceedings of ISECON 2006:* §3722. ISSN: 1542-7382.)

Huntley et al. (2004). Huntley, Christopher L, Mathieu, Richard G., and Schell, George P., "An Initial Assessment of Remote Access Computer Laboratories for IS Education: A Multiple Case Study," *Journal of IS Education* 15 (Winter 2004), 397-407.

Kauchak and Eggen (2005). Kauchak, D. and Eggen, P. *Introduction to teaching, 2nd ed*. Pearson, 2005.

Kneale et al. (2004). Kneale, Bruce, De Horta, Ain Y., Box, Ilona, "VELNET: Virtual Environment for Learning Networking," 6th Australian Computing Education Conference (ACE, 2004), Dunedin, New Zealand, in Research and Practice in Information Technology (Lister, Raymond, and Young, Alison, eds.), v. 30.

Krishnamoorthy (2007). Krishnamoorthy, S. "An Experience Designing and Teaching a Hands-on Project-based Networking Technologies Course for IS and IT." *Information Systems Education Journal, 5* (22). http://isedj.org/5/22/. ISSN: 1545-679X

Ma and Nickerson (2006). Ma, Jing, and Nickerson, Jeffrey V., "Hands-On, Simulated, and Remote Laboratories: A Comparative Literature Review," *ACM Computing Surveys*, v. 38, No. 3, Article 7 (Sept. 2006), 1-24.

Madrid et al. (2007). Madrid, L.D., Canas, M., Ortega-Medna, M., "Effects of Team Competition versus Team Cooperation in Classwide Peer Tutoring." *Journal of Educational Research*, 100 (3) pp. 155-160.

Mancill (2002). Mancill, Tony, *Linux Routers: A Primer for Network Administrators,* 2nd ed*.* Prentice Hall PTR (2002).

McEwan (2006). McEwan, William, "Virtual Laboratory Network – Christchurch Polytechnic Institute of Technology (CPIT), New Zealand: A detailed Case Study HowTo," Sept. 2001 at http://user-mode-linux.sourceforge.net/case-studies.html , 2006.

Molina (2006). Molina, Francisco J., *Redes de Área Local*, 2nd ed. (Alfaomega Grupo, 2006).

Nakgawa et al. (2003). Nakagawa, Y., Suda, H., Ukigai, M., and Miida, Y., "An innovative hands-on laboratory for teaching a networking course," *Proceedings – Frontiers in Education Conference*, 1 (2003), pp. T2C14-T2C20.

Odom and McDonald (2006). Odom, Wendell, and McDonald, Rick, *Router and Routing Basics: CCNA 2 Companion Guide,* Cisco Press, 2006).

Orebaugh et al. (2007). Orebaugh, Angela, Ramirez, Gilbert, Burke, Josh, Morris, Greg, Pesce, Larry, and Wright, Joshua, *Wireshark & Ethereal: Network Protocol Analyzer Kit* (Syngress, 2007).

Ouyang et al. (2005). Ouyang, Y., Dong, Y., Zhu, M., Huang, Y., Mao, S., and Mao, Y., "ECVLab: A web-based virtual laboratory system for electronic circuit simulation," *Lecture Notes in Computer Science*, 3514, I (2005), pp. 1027-1034.

Powell et al. (2007). Powell, V. J. H.; Johnson, R. S.; Turchek, J. C.; Davis, C. T.; Wu, P.Y.; Parker, I.W., VLabNet: The Integrated Design of Hands-on Learning in Information Security and Networking, *Proceedings, Information Security Curriculum Development Conference*. (Kennesaw State University, 2007).

Sanders (2007). Sanders, Chris, *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*, (No Starch Press, 2007).

Scheets et al. (2005). Scheets, G., Weiser, M., and Sharda, R., "Changing a standard telecommunications laboratory to a same-time-different-place virtual laboratory format: Techniques utilized and lessons learned," IEEE Transactions on Education, 48, 4 (2005), pp. 713-718.

Schmied (2005). Schmied, G. *Integrated Cisco and UNIX Network Architectures* (Cisco Press, 2005).

Tanenbaum (2003). Tanenbaum, Andrew S., *Computer Networks*, 4th ed. (Prentice Hall PTR, 2003.)

Tapscott and Williams, (2006) Tapscott, D, and Williams, A.D., *Wikinomics* (Portfolio, 2006).

Tomei (2001). Tomei, L.A.,. *Teaching digitally: A guide for integrating technology into the classroom*. Christopher-Gordon Publishers, Inc., 2001

Wu et al. (2004). Wu, Y., Chan, T., Jong, B., Lin, T., and Liang, Y., "A web-based dual mode virtual laboratory supporting cooperative learning," International Conference on Advanced Information Networking and Application (AINA; 2004), 1, pp. 642-647.