Session 3532

Virtual Networking Lab (VNL): Its Concepts and Implementation

Steve Liu, Willis Marti, Wei Zhao

Computer Science Department
Texas A&M University
College Station, TX 77843-3112

Abstract

In this paper, we present the architecture and design for a *Virtual Networking Lab (VNL)* that is being developed for hands-on exercises in network engineering curricula at Texas A&M University. The objective of the VNL is to create a remotely accessible environment for students to obtain hands-on networking experiences. Isolation provides for wide scope networking training without compromising operational campus networks and enhances the desirability of remote access. The facility is designed to support fine-grained, detailed instrumentation and experiments on real networking equipment. VNL architecture consists of two major foundations: *Access/Resource Management Servers,* (ARMS), for management of remote users and test bed resources; and the *Micro-Internet Test Bed*, (MITB), for execution of experiments and exercises. ARMS safeguards full and secure access of VNL equipment through the Internet, supports efficient equipment management and provides a structure for pedagogical aid. One of several planned environments, MITB is a small, yet complete inter-networking structure based on the real-world Internet architecture.

1. Introduction

Internet technology continues to transform the social and economic landscape, at a scale and speed larger and faster than invention of telephony. Internet technologies are involved with enormous amounts of intellectual products, including distributed algorithms, databases, information theories, protocol engineering, software engineering, and more. It is not realistic to expect instructors to convey the broad range of Internet knowledge to students using only traditional classroom interactions; nor for students to learn to operate, maintain, design and implement sophisticated networking systems. In addition to textbooks, Internet request for comments (RFC), homework and tests, faculty can thereby show the interactions between theories and systems, and students can put the learned basic knowledge into practice.

Several challenging hurdles need to be overcome to build VNL, but the cost is the first and most critical issue. Although many universities receive heavy discounts for educational use of the equipment, it is critically important to maximize the utilization rate for the best investment returns. The second major issue is related to network security. To provide high fidelity experiences to students, it is necessary for the lab to operate (almost) exactly as the Internet works: IP address space partition and aggregation, routing, access, domain name system (DNS), etc. Most services require the equivalent of *root* (Unix) or *administrator* (Windows) access. And it is necessary to allow students to make mistakes. Unless special care is taken, labs can create major security and service problems for operational networks. The third issue is related to class scheduling. Students acquire their skills stage by stage, and thus they should be granted different levels of privilege in a carefully controlled manner. Otherwise, a poorly implemented exercise can bring chaos to supporting software systems, defeating the purpose of the hands-on lab.

Recognizing the importance of the hands-on lab to the networking engineering education, the Computer Science department has committed to turn those major technical and financial issues into a major opportunity for innovation, and a quantum leap of our teaching approach. The *virtual networking lab* (VNL) represents our answer to these important challenges. VNL consists of two major subsystems: the *access/resource management servers*, (ARMS), for management of remote users and test bed resources; and the *Micro-Internet Test Bed*, (MITB), an environment for execution of experiments and exercises.

Three major access interfaces (from external to internal) are supported in ARMS: web access servers; teaching material server; and direct access servers. These servers are designed to provide remote users the feel and look of the user interfaces of the laboratory devices, yet still prevent misuse of the VNL physical and logical components to affect the operational networks. An additional resource configuration server is responsible for efficient and reliable (re)configuration of laboratory facilities.

The MITB represents the first of what will be several exercise environments in the VNL. Rather than have instructors assemble individual laboratory components for each individual exercise, the VNL will provide pre-configured environments which can be adapted for individual exercises with minimal effort. MITB contains four conceptual tiers: *backbone; aggregation and distribution; local access points;* and *IP applications nodes* that represent different networking functions of the Internet. The backbone layer is responsible for global management of IP addresses (and names) and their routing. The aggregation and distribution layer is responsible for fragmentation and aggregation of major subnet blocks to user clusters, and the local access points are the points from which end users access the network. All IP applications, including the top-tier DNS servers, run on the IP applications nodes.

2. Access/resource management servers (ARMS)

The management infrastructure enables controlled, remote access to resources within the test bed and exercises management per session. Our end goal is to automate access and scheduling for efficiency while incorporating pedagogical tools such as assessment and flexibility for instructors in designing exercises. Primary ARMS components (Figure 1) are:

- Web Access Gateway – providing remote users with authenticated, controlled, filtered, “hands-on” access to exercise elements;
- Direct Operations Gateway – providing secure remote access for administrators and/or special requirements;
- Courseware Server – for specialized or restricted content within the lab; and
- Configuration Server – providing real time control over infrastructure connectivity to support multiple exercise configurations.

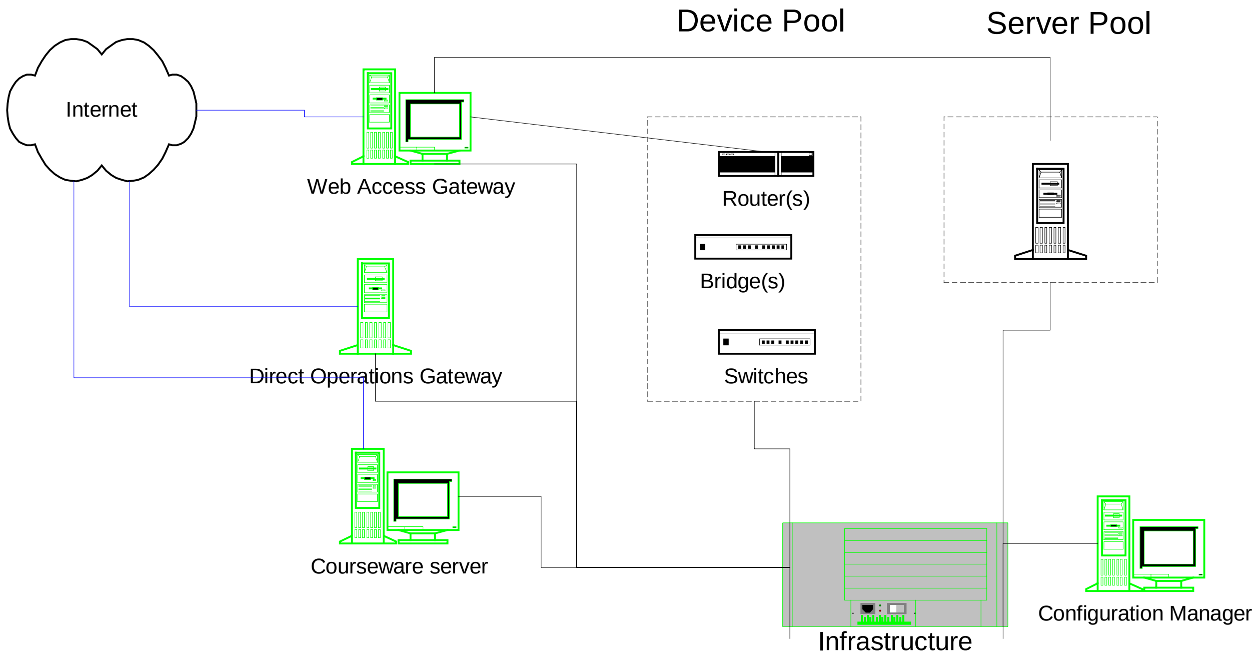

Figure 1 ARMS Overview

The Direct Operations Gateway is being implemented initially with a commercial virtual private network (VPN) gateway. This allows VNL administrators direct access to all components, including those normally invisible to the user such as the infrastructure and configuration manager. Future versions will allow assignment of differing access levels. The courseware server is currently an Apache web server. Future versions may link to the campus WebCT server and streaming video servers. The Configuration Manager shapes the physical connectivity into logical connectivity as desired for specific exercises and environments. For example, the MITB is physically a rack-full of computers connected to an Ethernet switch and an ATM switch. The logical configuration is created by appropriate VLAN assignments of individual switch ports. Additional resources may be linked to the MITB by changing infrastructure VLAN assignments. Because the VLAN capable switches act as transparent bridges, they may be considered infrastructure and not visible to exercise participants.

Access to VNL facilities for the normal user is through the Web Access Gateway (WAG). The goal of the WAG is provide a lab experience to remote users identical to what would be provided to local users. It also provides additional features helpful to the teaching mission of the VNL. Fortunately, the salient component of the lab experience is not physical manipulation but rather access to device control interfaces (console or browser-based). Rather than allow uncontrolled access via TELNET or even secure access through a VPN, the WAG is inserted as a tweak-able filter between the user and the devices. The internal arrangement of the WAG is shown in Figure 2.

Structure of Web Access Gateway

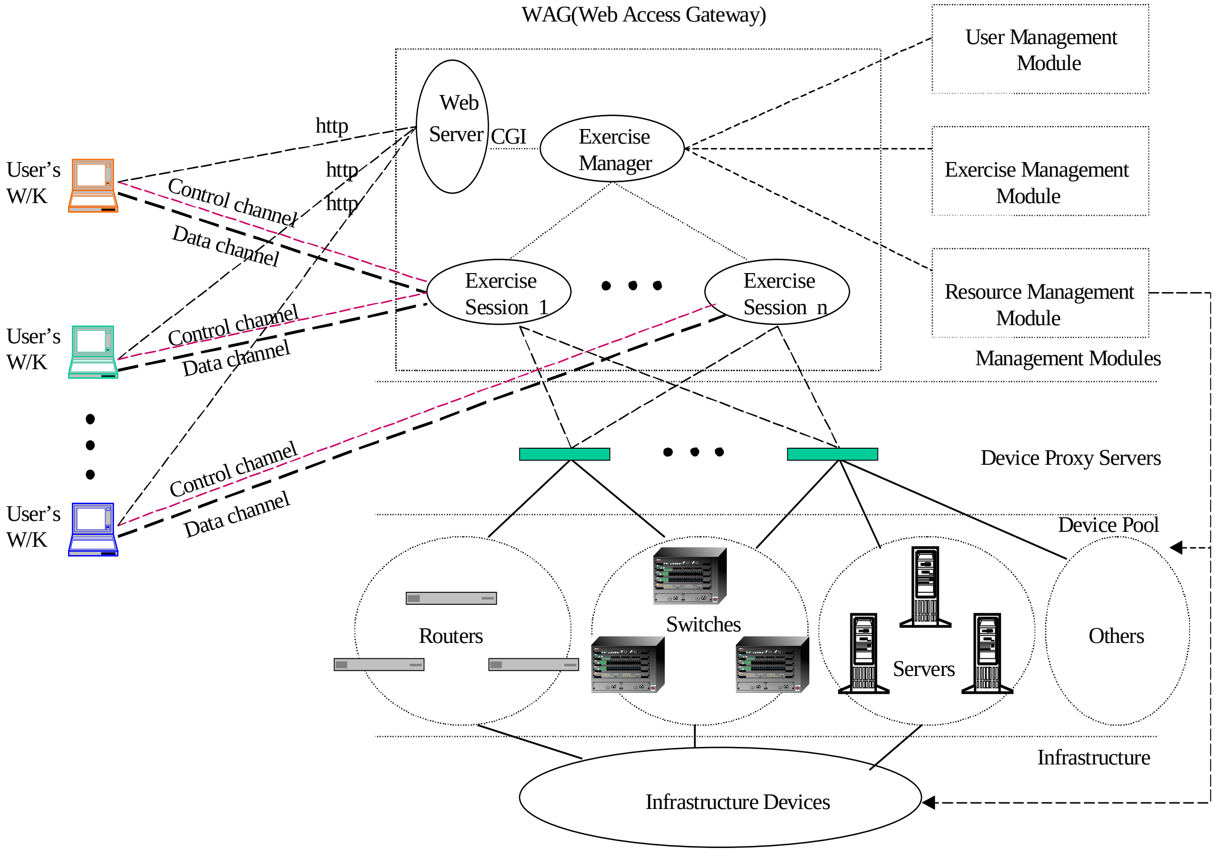

Figure 2 Structure of Web Access Gateway

In operation, the user (a) accesses the WAG with a browser, (b) is authenticated then (c) allowed to select an exercise from a list constructed depending upon an individual's progress and instructor's plan. Other administrative services such as viewing assessment or progress reports are potential options. The Exercise Manager component retrieves information from the various data modules and invokes a Session manager. Resource assignments have been coordinated by the Exercise Manager and devices initialized to a known state. The Session Manager has been passed exercise parameters such as actual devices assigned, any command filters and time limits on this user for this exercise. The user's browser is downloaded a Java TELNET-work-a-like applet with authentication tokens which establishes communication directly with the Session Manager. Future versions will allow students to cooperate in a single exercise session instead of just one user, one exercise. The Session Manager contacts device proxies to establish communication paths and perform any initialization required prior to start of the exercise. Device proxies are used to simplify interface programming in the session managers. For most devices, the proxy needs to provide a RS-232 connection to the console port on the device. This is implemented in the VNL with a terminal server, with its serial ports directly connected to device console ports. The Session Manager on the WAG connects via the network to the proper port on the terminal server and serves as relay for user commands and device responses.

In addition to controlling the connections between assigned devices and users, the session manager acts as a filtering relay between users and devices. As shown in Figure 3, the session manager can log communications for later evaluation. Or it can provide some real time feedback and assessment, by ensuring certain commands are issued before others. The Session manager filter can also restrict the commands/information sent to the devices, based upon exercise restrictions defined by the instructor. For example, the first lesson in a series of router exercises might restrict the user to commands for viewing, but not changing information. In the last lesson, the student could issue any command (except, perhaps, initializing the device flash memory).

The Exercise Manager, Session Manager(s) and device proxy functions are implemented as separate objects for ease of programming and also for future growth. While one server currently runs all the software needed for exercise access, it is a straightforward extension to implement separate servers if load gets too high or additional special services are needed.

Components of Exercise Session

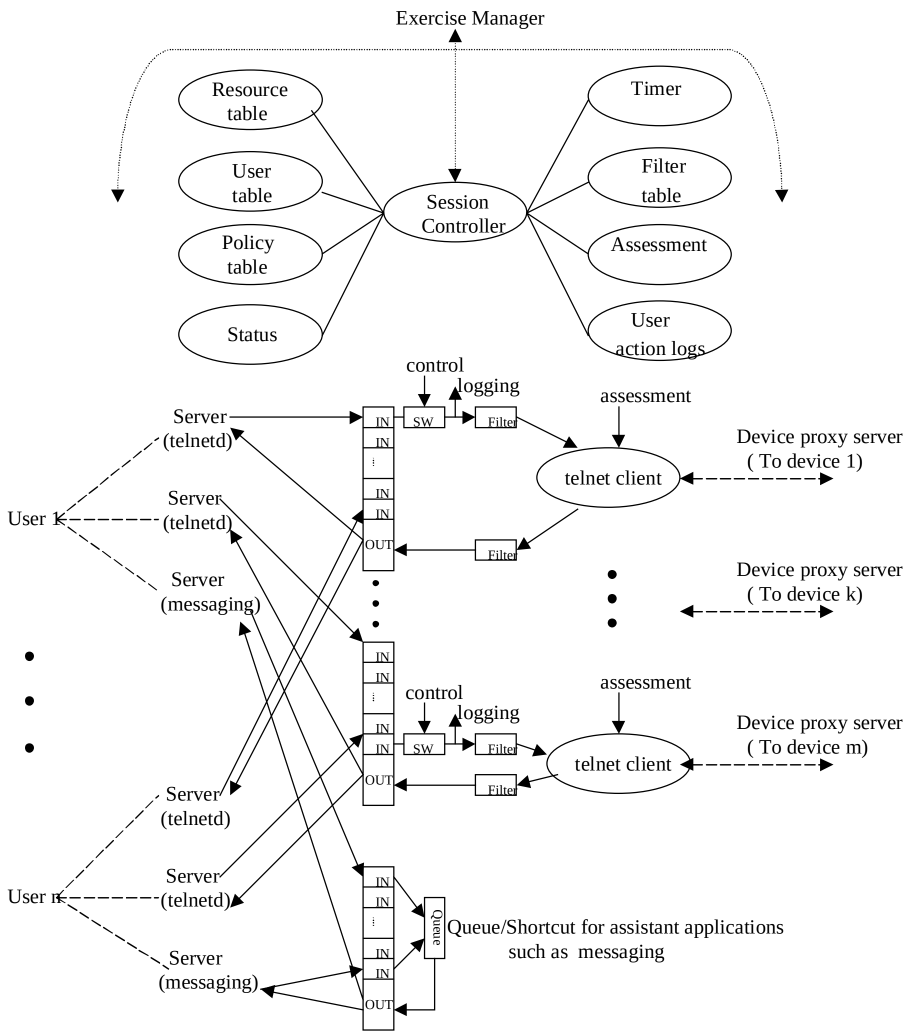

Figure 3 Session Manager Internals

3. Micro-Internet Test Bed (MITB)

The goal of the MITB is to provide a preconfigured, realistic environment where instructors can create a full spectrum of networking experiments and exercises for students. The MITB supports the ability to *exercise, implement,* and *test* different networking protocols, management strategies and Internet applications. By making the basic environment persistent, students may interact across classes as well as within a class. For example, an undergraduate course might implement a new web server, while a graduate class deploys instruments and analyzes performance.

Following the hierarchical architecture of the Internet, MITB is top-down divided into four functional tiers (Figure 4): routing backbone; routing distribution and aggregation; local access points; and hosts. Different network connectivity devices (routers, switches, firewalls) interconnect these tiers, and the VNL infrastructure management enables addition/deletion of other routing devices, hosts, and applications for various exercises. A set of restricted devices form a stable, vertical interconnections between layers form the core of the MITB and are made robust in the face of student activities.

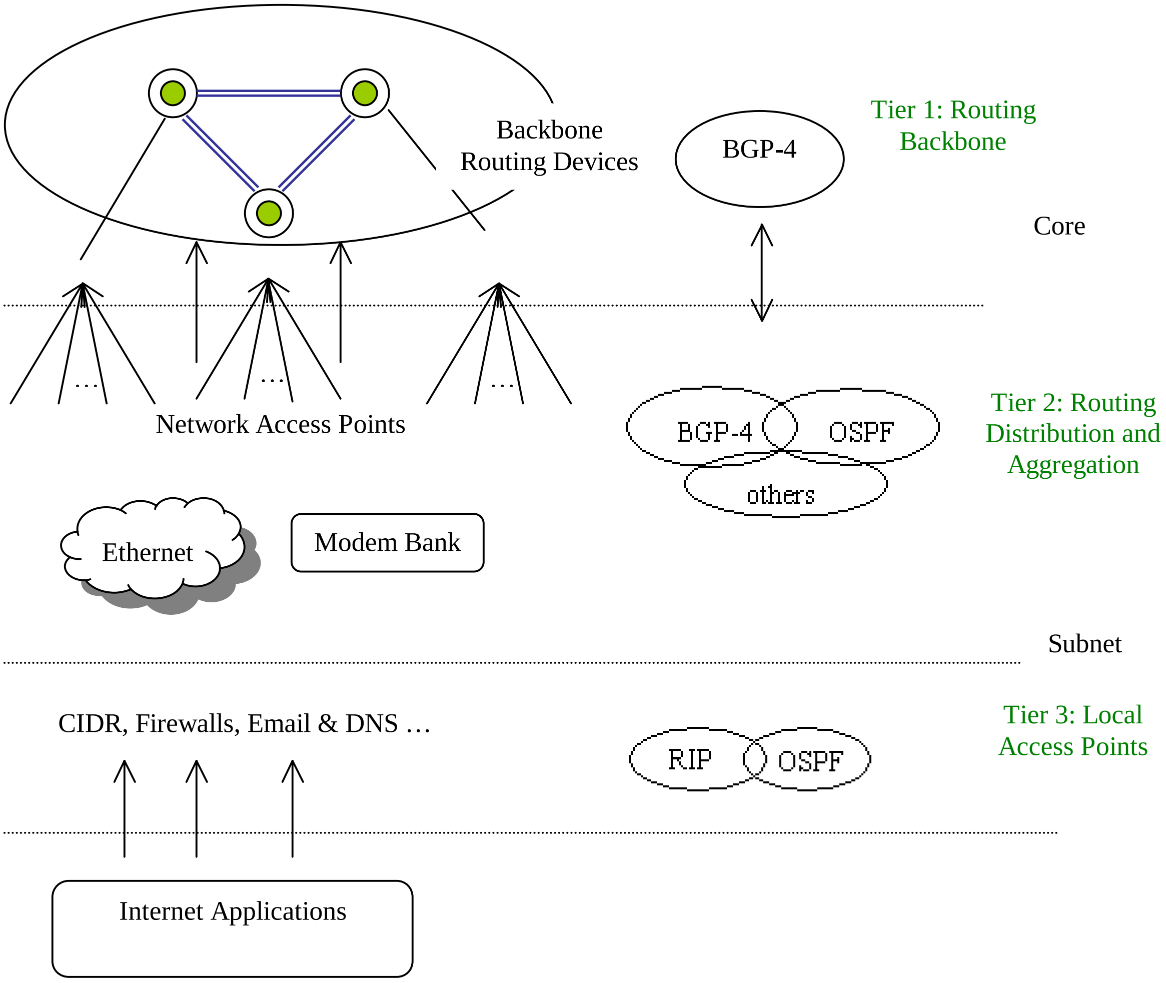

Figure 4 Logical Structure of Access Hierarchy in MITB environment

Logically, the MITB consists of four campuses interconnected via two backbones. An ATM switch, configured with two separate ELANs, provides connectivity for the nodes designated as backbone nodes. The routing backbone represents the highest level of the Internet hierarchy. Interconnected at this level are multiple *campuses,* each of which constitutes one or more routing *autonomous systems* (AS), to provide the global interconnectivity. The campuses each consist of three or four additional routers, configured in different topologies. Campuses can be analogous to universities or large enterprises, or an ISP with several customers. Planned exercises include BGP configuration, BGP operation with backbone failures, IPv6 deployment and opportunities for traffic monitoring.

The second routing tier is typically managed as a regional network by an Internet service provider (ISP). Each ISP typically has its own routing backbone running OSPF, RIP or a similar protocol. Issues include upstream IP subnet address aggregation, and downstream resolution of supernet IP addresses. Exercises include address space management (CIDR fragmentation and aggregation), firewalls, network monitor usage and DNS.

Local access points are the Internet "outlets" from which Internet hosts access the global Internet using a global IP address. The main networking issues include assignment of static and dynamic IP (e.g., DHCP; BOOTP), local DNS management for assignment of host names, traffic management and interconnection of the client and server machines. Exercises will cover caching systems, DHCP configuration, NAT and proxy servers. Most exercises in this area will be conducted in two modes: stand-alone; and connected as a node in the MITB.

Regular hosts comprise the final tier in the MITB model of the Internet. Initial exercises will focus on network configuration issues. The VNL has both Linux and Microsoft Windows 2000 hosts available. There is still a technical problem in remote "console" configuration for the Microsoft Windows 2000 systems.

Exercise Design

We plan to develop new networking exercises in steps. First, we will focus on implementation and/or usage of a few, key networking functions. Emphasis is placed on important concepts rather than completeness (depth over breadth). As exercises are expanded and validated in the VNL, the difficulty should increase from system configuration and operation through implementation to system design. We anticipate that users at easier (earlier) levels will provide a rich "problem" environment for users needing management problems.

Recognizing that network engineering is a broad topic, initial exercises will reside in one of five areas:

- Global and local name and IP address management

  IP address partition and assignment of Internet names to domains, local networks, hosts, web sites, and various types of service accounts. A focal point of this category is to understand the basic principle of the DNS server database, the trust relationship among different classes of DNS servers, authorization of IP.

- Routing protocols

  Internet is based on a mutual trust mode for interoperation between Internet devices. Misbehaved nodes that give up inconsistent information, or calculate the inbound data incorrectly may lead to numerous anomalies, such as routing loops, routing black holes, splitting of routing domains, and even impersonation of IP identities.

- Transport technologies (e.g., Ethernet, ATM, wireless),

  Understanding end-to-end data delivery must include and understanding of transport characteristics. Exercises focus on integration of different transport technologies and their global management issues.

- Bandwidth management (scheduling and prioritization)

  The objective of this area is to investigate issues related to management of the network bandwidth, so that applications can share it in a controlled manner. Control of bandwidth allocation, prioritization and scheduling of connections, protection from performance attacks, e.g., distributed denial of service (DDoS).

- Internet applications

  DNS/Web/File/Mail Server configuration, intrusion detection and protection.

4. Summary

VNL represents an aggressive approach to quality instruction of network engineering students in higher education. Integrating numerous complex functions into a lively training environment makes it a major challenge. The research team is vigorously pursuing the project, with helpful input from industry partners. The laboratory is an ongoing activity, benefiting from continuous improvement and frequent technology updates. The remote-access technology provides a useful tool for both lecture courses and distance learning. The ease of configuration for different exercises makes it valuable for semester-based courses as well as short courses or continuing education for professionals. Successful integration of the VNL into coursework will significantly improve the teaching quality of the networking engineering classes. Students and faculty together may learn and teach ever-changing networking technologies in a flexible and secure environment.

Acknowledgement

The research reported in this paper is partially supported by the NSF, contract number NSF ITR grant EIA-0081761. We thank Marconi Communications Inc. for their generous donation for the major switching infrastructure of VNL.

5. REFERENCES

[1] L. Benetazzo, M. Bertocco, F. Ferraris, A. Ferrero, C. Offelli, M. Parvis, and V. Piuri, “A Web-Based Distributed Virtual Educational Laboratory,” in *Proc. Instrumentation and Measurement Technology Conference*, Venice, Italy, May 24 –26, 1999, pp. 1851-1856.

[2] L. Biely, “The Virtual Laboratory: An Application Environment for Computational Science and Engineering”, Internet2, Available at http://www.internet2.edu/html/virtual_laboratory.html, October 25, 2000.

[3] N. Kapadia, M. Lundstrom, J. Fortes, and K. Roy, “Network-Based Simulation Laboratories for Microelectronics Systems Design and Education,” in *Proc. IEEE International Conference on Microelectronic Systems Education*, Arlington, Virginia, July 21-23, 1997, pp. 23-24.

[4] M. Kassouf, S. Pierre, C. Levert, and J. Conan, “Modeling a Telecommunication Platform for Remote Access to Virtual Laboratories,” in *Proc. IEEE Canadian Conference on Electrical and Computer Engineering*, Alberta, Canada, May 9-12, 1999, pp.127-132.

[5] Y. Lee, W. Ma, D. Du, and J. Schnepf, “Creating a Virtual Laboratory,” in *Proc. IEEE Multimedia Computing and Systems*, Ottawa, Ontario, Canada, June 3-6, 1997, pp.642-643.

Acknowledgements: The work reported in this paper is supported in part by NSF ITR grant EIA-0081761, and grants from Marconi Communications plc and Micromuse, Inc.