*JOURNAL OF INFORMATION SYSTEMS*
Vol. 22, No. 2
Fall 2008
pp. 103–122

# A Discovery-Learning Classroom Case on Accounting Data Transmission Systems

**David R. Fordham**
*James Madison University*

**ABSTRACT:** This paper describes a classroom exercise utilizing a technique known as "discovery learning." The activity involves a hands-on lab composed of basic building blocks of a simple wireless network. Students engage in a physical activity that demonstrates the operation of individual layers of the seven-layer Open Systems Interconnect model. In the process, they uncover conceptual knowledge normally delivered via means that are more traditional such as lecture or reading. During one such lab session, students stumbled upon a real-world control breach. This discovery, completely unplanned by the instructor, vividly illustrated the critical importance of the topical material. The experience greatly increased student interest and motivation. Assessment data confirms that student comprehension and application is significantly enhanced.

## I. INTRODUCTION

In today's accounting information systems, data is rarely—if ever—stored or used in the same location where it is captured. Most modern accounting systems, especially those found in large businesses, make extensive use of complex data transmission technologies. Data moves across local, wide-area, and even global electronic telecommunication networks. These networks often include segments that are part of the public infrastructure, and therefore completely outside the legal, physical, and control domains of the owners, operators, and auditors of a given accounting system.

Because of their complexity, coupled with the lack of access, accountants and auditors often treat these networks as a single "black box" when it comes to assessing risks. In reality, the networks are made up of uncountable components and segments. Each component and segment introduces its own particular set of threats, vulnerabilities, and risks. Further, when connected, the diverse components and segments require interfacing (protocol conversions, media transfers, etc.) and these interfaces introduce additional threats, vulnerabilities, and risks. Finally, the assembly of the various components and links into a holistic network introduces synergistic risks above and beyond those associated with the individual parts.

Accounting students must acquire skill and practice in identifying and assessing the risks associated with accounting systems. However, before they can be expected to assess risks of a data transmission system, students must first have a thorough understanding of the *function and operation* of the components and segments, and how they come together in a design to form the transmission system as a whole.

The author expresses appreciation for the helpful comments and suggestions of the JIS editor, associate editor, and anonymous reviewers, as well as the discussant and participants of the presentation session at the American Accounting Association's 2007 Annual Meeting in Chicago, Illinois.

The complexity of these systems, coupled with the inability to physically observe the inner workings of their operation, makes it difficult for students to fully comprehend their nature. The seven-layer Open Systems Interconnect (OSI) model on which network design and construction is based can serve as a useful framework for comprehension and identification of the loci of various control and security factors. However, this model, being a conceptual rather than physical manifestation, poses its own comprehension difficulties for students, most of whom are novices to electronic communications technology.

This paper describes a classroom exercise that has been used successfully to illustrate the seven layers of the OSI model. The exercise is a demonstration of a simplistic network within the context of the seven layers. The exercise uses a "lab" made up of slow-speed equipment. This equipment, although technologically obsolete, allows students to witness and experience the individual operation of the various layers of the model in a working environment. In this way, students gain valuable hands-on understanding of the operation of electronic data transmission systems.

Appendix B describes one of the most interesting events occurring in the author's teaching career. The exercise forming the basis of this paper was originally designed to allow students to "discover" certain knowledge on their own. This knowledge had been carefully orchestrated by the instructor to be revealed during the conduct of the exercise. However, an unforeseen and unique event occurred during an early execution of the exercise: The electronic wireless equipment being used for the demonstration was inadvertently set to a different radio frequency where it picked up an unencrypted data transmission from a nearby business. While monitoring the signals, students witnessed a real-world breach of internal controls—one that clearly resulted in the loss of a sales transaction record at a local business.

The additional (and completely unanticipated) discovery of a real-world control breach vividly demonstrated the importance of the topical material. The experience provided an indescribably valuable learning experience.

## II. LEARNING OBJECTIVES

The learning objectives for this exercise are derived from two major educational premises, described individually below.

### Premise 1: Accountants and Auditors Must Have a Thorough Understanding of the Details and Complexities of Data Transmission Systems

Modern accounting systems rely on complex electronic transmission systems for the transportation of data. Various segments of these systems use encryption, exotic modulation techniques, complex high-speed packet-switching equipment such as routers and gateways, paths to orbiting satellites, wireless radio waves, paths in which the data is mixed with, combined with, and shared with other, unrelated data, perhaps from unrelated parties. Unlike the route traversed by traditional paper documents, these electronic links are, for practical purposes, completely inaccessible to direct observation, evaluation, and safety assessment by auditors. In many cases, auditors are even unaware of the exact paths traversed by the data.

When closely analyzed, many segments of these modern transmission systems exhibit numerous vulnerabilities and threats to the data's integrity, availability, and confidentiality. The threats and vulnerabilities stem not just from deficiencies in design and implementation; many are *inherent in the very nature* of the transfer process. These threats and vulnerabilities ultimately can have great impact on the accuracy, completeness, authenticity, timeliness, and reliability of the information provided to the end-user (Maiwald 2001).

To evaluate risks associated with transmission processes, auditors routinely take samples of data at the entrance point of the transport process, and compare it to the data coming out at the destination. In this way, they consider the transportation link to be a "black box." This approach fails to address the possibility of threats and vulnerabilities not actively affecting the data at the moment the sample is taken.

In an attempt to address this possibility, auditors may rely on technical specialists to assure them of the integrity, availability, and confidentiality of the route. Unfortunately, these technical specialists are often sorely underqualified in terms of internal control expertise, and therefore sometimes overconfident of the integrity of their systems when it comes to internal control sufficiency (Easttom 2006). Wright and Wright (2002) showed that less than 5 percent of today's IT education programs offer any coursework covering internal controls, or what might be termed classical concepts of checks and balances (segregation of authorization, execution, custody, recording, etc.; independent verification, redundancy or positive verification of accurate data flow; professional skepticism, etc.). In fact, even those few IT programs based in colleges of business often require *no* such training except perhaps as a precursory introduction received in a principles of accounting core business class in which the concepts are normally not solidly linked to technical systems, networks, and transport mechanisms.

One of the major provisions of the Sarbanes-Oxley Act (U.S. House of Representatives 2002) is the emphasis placed on internal controls. Financial reporting is, of course, a major end-use of information from the accounting system, and thus its accuracy, completeness, and integrity is a direct function of the controls on the system—*including* the data transportation activities. Statement of Auditing Standards Number 94 (AICPA 2001) addresses the responsibilities of accountants and auditors in evaluating the controls on the information transportation and transmission systems, especially as applied to online, e-commerce, and other network systems. The standard states that accountants and auditors *themselves* must be thoroughly familiar with all aspects of the system, including design and operation, before they can adequately comprehend and evaluate the sufficiency of the controls.

Association to Advance Collegiate Schools of Business (AACSB)-accredited schools have for many years required basic courses in information technology. This requirement notwithstanding, studies show that the level of learning at this basic level is insufficient for accounting majors. O'Donnell and Moore (2005) found a critical shortage of IT-qualified accountants and auditors, traceable to deficiencies in accounting curriculum emphasis on information technology. They report that there are "still many students graduating from programs that do not provide sufficient training in IT control, knowledge, or competencies." Both students and practicing accountants recognize the need for more knowledge and skill in technology. O'Donnell and Moore (2005) observe, "Our study is consistent with other research indicating that students are more satisfied with the education they receive in financial accounting, theory, auditing, taxation, and managerial accounting than they are with the education they receive in accounting information systems."

In summary, then, three points appear supported by the literature: (1) it is imperative that accountants and auditors understand the networks and other data transmission techniques sufficiently to evaluate the internal control aspects of the data transmission processes; (2) IT personnel are not sufficiently prepared with the "professional skepticism" required to fully appreciate the internal control requirements of the technology, and thus cannot completely compensate for an accountant/auditor's lack of knowledge about network threats and vulnerabilities, and therefore (3) many of today's accounting students need much more thorough understanding and comprehension of network-related control issues than is presently being provided.

Accounting educators are in a position to address the first and third items, if not also the second.

### Premise 2: Hands-On Learning—More Specifically—Discovery Learning, Is a Useful and Effective Pedagogical Technique

Hands-on *learning* is not the same as hands-on *training*. Hands-on *training* is the natural mechanism for motor-skill development, found in professions such as music, athletics, surgery, aircraft piloting, and similar physical activities. By contrast, hands-on *learning* is generally associated with mental or conceptual material, where the student engages in a physical activity intended to demonstrate, illustrate, or exemplify *conceptual knowledge*, rather than attain/develop/perfect a motor skill.

There is a rich body of evidence illustrating the effectiveness of hands-on learning for enhanced and improved conceptual understanding and comprehension. Education programs in the basic sciences in particular demonstrate the benefits of hands-on activity in conveying conceptual understanding, starting with elementary-school science projects and continuing through the college labs accompanying classes in theoretical physics, chemistry, and biology. An article by deFreitas and Oliver (2006) provides an excellent sampling of studies indicating that hands-on learning in the form of games, simulations, experiments, and the like provide a richer and enhanced educational experience to students than do traditional knowledge-delivery methodologies. Such active participation in the learning process, especially physical participation, supports higher-level cognitive development, and aids both understanding and retention, as well as enabling broader application of the acquired conceptual knowledge to future problems.

There are a number of reports in the accounting literature where application of hands-on learning, the use of technology, games, simulations, and other active experiences have been demonstrated effective in enhancing the quality of learning accounting concepts (Pillsbury 1993; Hermanson 1994; Bryant and Hunton 2000; Drake et al. 2001; Rose et al. 2005; Hayes and Reynolds 2005; Bamber and Bamber 2006). In each case, students were actively engaged in activity that illustrated, demonstrated, reinforced, or otherwise required overt participation to enhance education and conceptual learning.

Of course, it is not enough to simply require students to "do something." The activity must be carefully designed to match with the educational objectives, the students' learning patterns, the course environment, and other factors. The activity must be clearly and unambiguously tied to the concept desired. Articles by deFreitas and Oliver (2006), Bryant and Hunton (2000) and others offer numerous frameworks and recommendations for designing effective hands-on learning experiences.

One of the most effective hands-on learning strategies, especially for conceptual understanding and critical thinking, involves the use of *discovery learning*. In other words, an effective hands-on strategy is to lead the student to the brink of new knowledge, and let the student reveal the knowledge on his/her own. Peters (2005) suggests that the most effective conceptual experiences for lab exercises go beyond simple demonstration and require the student to think critically about the processes, thus "discovering something new."

The presence of a potential for uncovering and discovering provides enhanced motivation for participation. Humans in general derive great pleasure from discovery. Whether unwrapping a birthday gift, opening a Faberge egg, finding a hidden fishing spot, or retrieving a long-lost article of jewelry from under a piece of furniture, the very act of discovering something on our own is generally more emotionally rewarding than simply being provided with exactly the same end result (Liljedahl 2005).

This personal satisfaction from discovery can serve as a powerful stimulant and motivation for both present and future learning. There is a significant literature addressing the "Aha! factor" and the beneficial effect of discovery learning on student motivation and interest (Hecht 1997; Ernest 1987; Ellsworth and Sindt 1994). Dinan (2005) reiterates this idea and recommends that a well-designed learning lab experience should resemble the real world as much as possible, and more importantly, allow students to uncover not only knowledge and concepts, but also problems and solutions. In this way, students will be presented not only with relevance, but also with a challenge followed by a reward.

There is ample evidence that knowledge acquired through discovery is learned more thoroughly, more permanently, and with deeper understanding than knowledge acquired through other channels. In fact, when combined with the contextual understanding available by experiencing the concept and principles operating within its native environment (via hands-on learning), discovery learning is frequently an optimal educational strategy (Orange 2002).

Premise 1 above describes the rationale for including detailed topical coverage of the construction and operation of modern data transmission systems in an accounting course. Today's networks operate at speeds unobservable by humans, involve complicated electronic signals, and various media undetectable by human sensory organs. Students therefore have to *imagine* what is going on inside the boxes, wires, and airwaves. Educational research has shown that comprehension of difficult concepts and hidden operations can be better attained via a physical "model" or tangible "hands-on" learning experience than by mere explanation alone. Further, Premise 2 is supported by evidence that hands-on learning, and in particular, discovery learning, can serve to motivate, inspire, and interest students in the educational task, and thereby increase educational effectiveness and deepen understanding and comprehension. It follows therefore that network operation would be good candidate for a discovery-learning exercise.

The topical coverage of network operation (and associated risks) has for many semesters been embedded in the second AIS course of the accounting curriculum at a mid-sized U.S. masters-level university. The course is taught at the graduate level as a required course in the Accounting Information Systems (AIS) concentration, but can be counted for undergraduate elective credit for students desiring only a baccalaureate degree.[1] One unit (out of six) in the course is devoted to networking. The specific learning objective for the unit involved in this project is as follows:

> Through an understanding of the design and operation of modern networks, students will be able to identify major threats and vulnerabilities to internal control associated with various networking technologies, exemplified by common wired and wireless network architectures, including public and private networks used in e-Commerce and modern accounting systems.

The operative words from the above statement that apply to this case are "through an understanding of the design and operation of modern networks." Modern networks are built upon the basis of the seven-layer Open Systems Interconnect model. This model provides a framework for understanding the operation of *all* networks, whether an electronic network (such as the telephone network, Ethernet, or 802.11), physical network (such as the postal

[1] Both the College of Business and the Accounting Program are AACSB accredited. The university has offered an AIS concentration at both the undergraduate and graduate levels for almost two decades. This particular course addresses accounting information technology, and as such, it includes both conceptual and technical knowledge. The course and the concentration overall have been immensely popular with recruiters. Graduates from the program have indicated very high levels of satisfaction with the overall AIS curriculum, and the knowledge of technology imparted by this course in particular.

system or highway transportation network), or even a simplistic manual network (such as students passing a note across the room during class). Any multi-node point-to-point transfer system can be described within the framework of the OSI. Thus, the OSI serves as a useful basis for explaining the operation of a modern data transmission system.

The OSI model is a conceptual model rather than a physical manifestation. In an effort to promote "an understanding of the design and operation of modern networks," it was decided to demonstrate a physical network within the framework of the conceptual model on which it (and all other networks) are based. An exercise was devised whereby students use an operational working model that they can observe, touch, feel, experiment with, and thus come to understand via experience, and thereby come to understand the associated mental concepts.

This exercise does not enjoy its own formal, stated, learning objective in the traditional sense. Its goal is simply to provide a physical illustration. However, a clear objective can be articulated for the purposes of exercise design:

> Upon completing this exercise, students will be able to describe the design, construction, and operation of a typical electronic network by casting the network elements (and their operation and relationships) within the framework of the different layers of the Open Systems Interconnect model."

## III. LABS

### Lab Design Overview

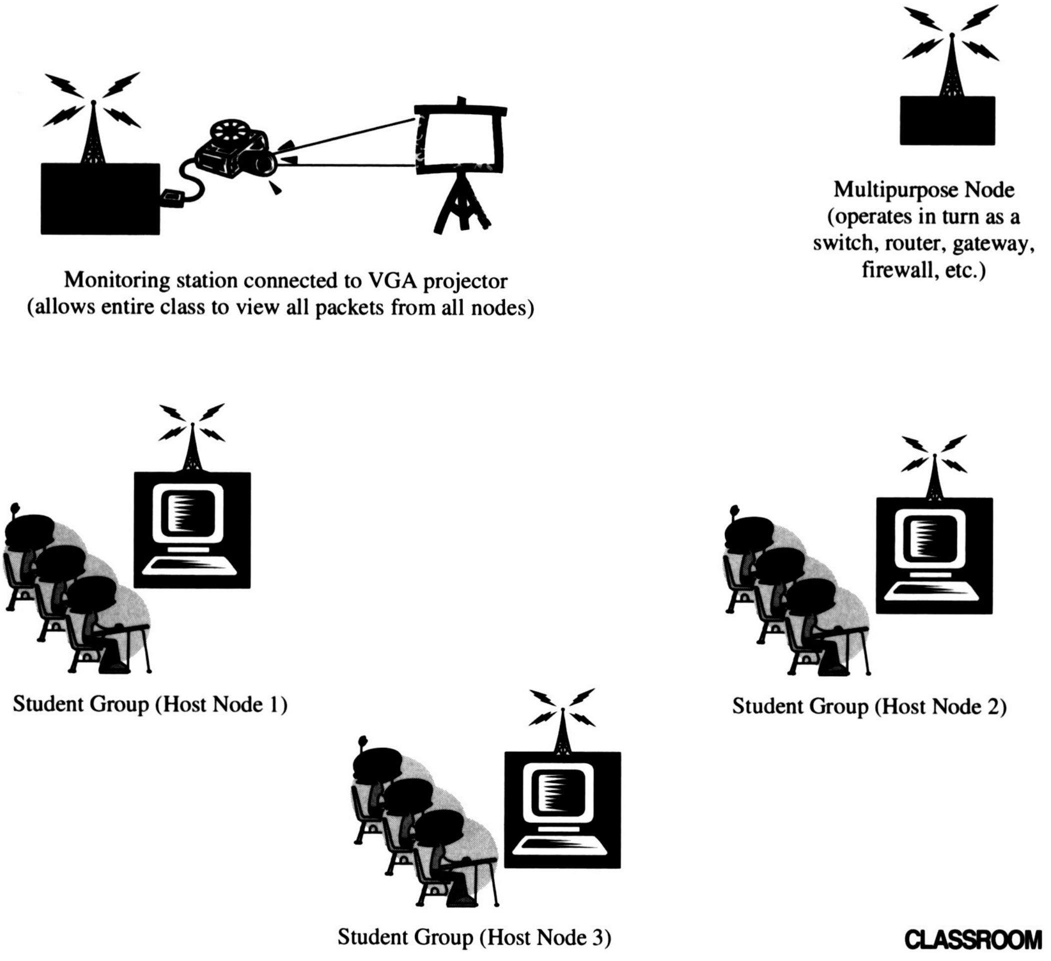
The activity lets students create a simple wireless network using slow-speed equipment, and then use it to observe network operation. The exercise also lets them manipulate the various characteristics of the network and witness the effects of those manipulations. The use of slow-speed equipment enables the students to actually see, via the use of monitoring equipment, the operation of the various network functions that in modern networks operate too fast to be observable by humans. The activity also lets students experience (e.g., play with) the various functions of a network to witness first-hand the manners in which networks can be manipulated (intentionally and unintentionally) to directly affect data security, integrity, and availability.

The exercise can be held in the normal classroom by assembling equipment (described in the next section) into a makeshift electronic laboratory before class begins.

The lab consists of a four-node network: three "host" nodes manned by students, with a fourth node serving various functions in turn as a router, gateway, packet switch. The lab also includes a fifth station that is "receive only," to intercept the network transmissions (in essence, a "packet sniffer") and display the intercepted data to the class using the ceiling-mounted VGA projector. A basic diagram of the overall network is shown in Figure 1.

As with many such lab exercises in the hard sciences, one intent is to offer students an opportunity to view something normally not seen in their everyday experience. Most modern networking gear used today is integrated; that is, modern network equipment performs functions at multiple OSI layers, operates in the background completely transparent to the user, and operates at such high speeds that dozens or hundreds of activities (such as connect requests, responses, retries, etc.) occur in fractions of a second. For this reason, the lab deliberately does not use commercial or standard network equipment such as 802.11 Wi-Fi, Bluetooth, Ethernet, or other common protocols. Rather, this lab uses older (and now obsolete but still available) AX.25 protocol equipment.

**FIGURE 1**
**Diagram of Network Nodes**


Multipurpose Node
(operates in turn as a
switch, router, gateway,
firewall, etc.)
Monitoring station connected to VGA projector
(allows entire class to view all packets from all nodes)
Student Group (Host Node 1)
Student Group (Host Node 2)
Student Group (Host Node 3)
CLASSROOM

The AX.25 protocol (and its parent, the commercial ANSI X.25 network standard) date from the early years of wireless networking when digital wireless technology was evolving from simple point-to-point communication into today's multipoint-to-multipoint networks. A network based on the AX.25 protocol can be constructed of either (1) integrated equipment, or (2) separate components, each one operating at a different "layer" of the OSI model. This lab uses individual components.

The separation of the various individual layers is critical in allowing students to recognize and identify the loci used for interception, data loss, garbling, counterfeiting, spoofing, and other threats and vulnerabilities. It also allows demonstration of countermeasures and controls. However, the actual operation of a network based on separate layers (in terms of the concepts of networking) is still identical in every way to modern commercial network operation.

In simplified terms, the use of AX.25 equipment allows the instructor to break the network down into basic components and functions that can be individually identified, observed in operation, studied, and manipulated in the classroom. Students actually watch the individual various network activities happening (such as data being formed into packets, connect requests being sent, connection confirmations being returned, data packets being transmitted and received, packets colliding, retries being attempted, etc.). Students experience and actually witness many concepts that previously had merely been mental explanations: time-division multiplexing and frequency-division multiplexing; simplex, half-duplex, and full-duplex communication; synchronous and asynchronous transmission; socket layers; and other similar concepts fundamental to understanding network operation. In this way, the conceptual understanding of those terms is enhanced, deeper learning occurs, enabling thinking to take place at a higher level.

Additionally, by using separate pieces, students have the opportunity to manipulate parts of the network to simulate and introduce (and then ameliorate) many of the threats and vulnerabilities inherent in (and introduced to) networks, both wired and wireless. Students see and understand the reasons and causes of authentication problems, handshaking problems, compatibility problems, radio interference, radio wave propagation anomalies, identity spoofing, packet counterfeiting, pinging, jamming, flooding, and other threats and vulnerabilities. By manipulating timing parameters, power levels, network configurations, traffic volume, etc., students witness and experience the simulated effects of distance, volume, adjacent channel intermod, and other characteristics of wireless communication. Finally, students experiment with encryption and other security measures to see the beneficial or detrimental effects on other network operation, effectiveness, and efficiency of the various encryption approaches.

The exercise is deliberately designed to facilitate numerous "discoveries" by students. These are not so much true discoveries in the scientific sense, but are "revelations" where students uncover knowledge new to them, or alternatively uncover information in a new context, where they had not expected it to appear. Some of these discoveries are based on previously learned conceptual material—by conducting the steps of the exercise, students reveal them in actual use and context. Other discoveries are made via analysis of observed but apparently unexplainable events, where the instructor encourages students to think about what they are seeing, to compare it with what they have learned technically, and attempt to develop answers to their own questions.

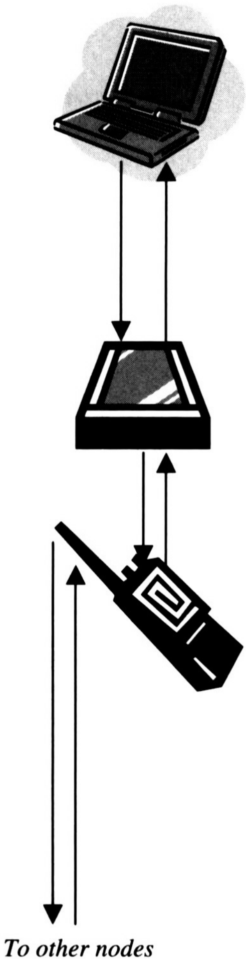
## Lab Construction Details

The heart of the network laboratory is a set of three host nodes. Each host consists of a laptop computer, a terminal node controller, and a VHF two-way radio. Figure 2 illustrates the components of each host node of the network.

The host nodes are using the laptop computers merely as "dumb terminals." (The laptops are not functioning as computers, except for running terminal-emulation software. They are functioning only as keyboards and screens.) In this way, students experience the Application Layer (Layer 7 of the OSI): by typing on the keyboard and seeing the screen, the students are actually interfacing directly with the network at its most fundamental level, rather than operating through network interface cards, drivers, APIs, GUIs, or network operating systems. In other words, students themselves are acting as the application program interface (API) and accessing the network "at the bare metal," so they can watch what is happening *inside* the network.

The serial port on the laptop is connected via RS-232 serial cable to an outboard piece of equipment called a Terminal Node Controller (TNC). This is a piece of AX.25 equipment

**FIGURE 2**
**Components of each Node**



Laptop computer in terminal mode: corresponds to Application Layer 7

Terminal Emulation Software, ASCII via RS-232 serial port corresponds to portion of Presentation Layer 6

Terminal Node Controller: corresponds to Data Link Layer 2, also illustrates Networking Layer 3

VHF Radio transceiver: corresponds to Physical Layer 1

By using the keyboard, students connect to other nodes (corresponding to Session Layer 5), and transfer files (corresponding to Transport Layer 4). Their screen displays traffic addressed to their node only, although the class monitoring station displays all packets regardless of originating or destination node.

which accepts data (and commands) from the keyboard, formats it into packets, and passes the packets along its output port to the communications channel. (Normally, in today's modern integrated networks, this would be handled by the application program interface, network card, network card driver, and network operating system socket, all working together transparent to the user. However, in this lab, students get to see the interactions, addressing, packet header construction, etc. actually happening in real time.)

Of course, since networks, by definition, operate bi-directionally, the TNC also takes incoming packets from the communication channel, checks the packet for integrity and accuracy, strips the header and trailer, and passes the information to the screen. In so doing, the TNC performs elementary format translation and offers a peek at the operation of the Presentation Layer (Layer 6 of the OSI), as well as a simplistic illustration of the operation of a gateway.

Additionally, the TNC also handles connect requests, packet acknowledgements to the originating station, packet retries, and other functions of the Data Link Layer (Layer 2 of the OSI).

The TNC is a versatile piece of equipment and can be programmed for various speeds and protocols. However, in this lab, we use only AX.25 protocol and perform all transmissions at 1200 baud. The use of 1200 baud (painfully slow by today's standards, but still usable for trivial text transfer) allows students to actually watch, count, and read individual data packets including the headers, trailers, checksums, message digests, address identifications, packet-type designations, and other "overhead" activities. Again, these are activities normally invisible to users but which can have significant effect on internal control and security.

Transmissions at 1200 baud are slow enough for students to actually hear the sound of the signal being modulated onto the analog communications channel carrier. Students thereby witness a physical demonstration of modulation and the operation of modems: signal conversion from digital to analog, and analog to digital.[2]

For the actual communications channel, each TNC is connected to a simple two-way VHF radio. The modulated output of the TNC is wired to the microphone input of the radio. The speaker jack of the radio is wired to the demodulation input port of the TNC.

The radios are capable of operating in multiple modes and on many different frequency bands, but in this lab, they are used on the 146 MHz band using only narrow-band frequency modulation (FM). This places their operation within the FCC Part 97 radio service, which allows educational and hobbyist experimentation.[3]

The radios are essentially simple voice walkie-talkies. The push-to-talk nature of the transceivers offers a demonstration of half-duplex operation, contrasting with simplex operation of a broadcast radio station or the full-duplex operation of a cell phone. The radios illustrate the Physical Layer (Layer 1 of the OSI), and offer a rich opportunity for experimenting with real-world wireless problems: interference, interception, jamming, spoofing, eavesdropping, shared-channel volume, etc.

The lab is set up with one host node located on one side of the room, with approximately one-third of the students gathered around its respective laptop computer. An identical host node is set up on the other side of the room with another third of the students, and a third node is set up in the back of the room with the final group of students. Each node consists of one laptop in terminal mode, one TNC, and one two-way radio (Figure 1). Each node is manned by approximately four or five students, and students take turns at the keyboard.

[2] In addition to forming the heart of modem technology, analog/digital (A/D) converters are ubiquitous components of data capture equipment in today's accounting systems: bar code scanners, magnetic strip readers, fingerprint and voice-recognition systems, DTMF input devices, RFID readers, etc. All are based on A/D converters, a fundamental principle which is unfamiliar to many accountants.

[3] It must be emphasized that the radios used in this lab require an FCC license to operate. The Part 97 license can be obtained by almost any U.S. citizen for under $20 by taking and passing a 50-question examination; the exam is easily passable after a few hours of preparation by almost anyone who has completed high-school physics. Alternately, an educator can use other frequency bands under other radio services licensed by the FCC.

The receive-only monitoring station is set up in the front of the room, and the output of its signal decoder is connected to the overhead VGA projector. In this way, all students can see the content of all data packets being transmitted over the frequency, regardless of which station originated the packets or to where the packet is addressed.

The final node is set to the side of the classroom and manipulated as required by the instructor during the first day of the lab. On the second day, this node is set up outside the classroom, unknown to the students, where it can serve as a hidden node, operated by a confederate of the instructor who simulates a hacker or war-driver.

In summary, the laboratory is a simple four-station AX.25 packet switching network involving three hosts and a digipeater, along with one monitoring station.

### Operation of the Lab

Although this case is typically used as a two-day lab, it lends itself to an abridgement consisting solely of demonstration. However, it must be emphasized that the most benefit can be gained from the "discovery" process: students are more motivated, excited, and demonstrably learn better when they are discovering, rather than merely watching.

Prior to engaging in the lab, students will need to have significant exposure to concepts of internal control, including the management assertions associated with financial audits, (e.g., occurrence, completeness, accuracy, existence, etc.). This might have occurred in a previous course, but it is always good to have a quick review just before the lab exercise.

It is also assumed that before beginning the lab, students have learned (memorized) the seven layers of the OSI and know the names and associated activities of each layer, even if they don't yet have a complete appreciation for how the layers work or how they interrelate. In this way, the "discovery" they make will be their sudden "aha moment" when they comprehend the actual operation of what they previously memorized by rote.

The author does not use a student handout or outline, preferring instead to allow students to uncover a sequence of "discoveries" on their own as they engage in the physical activities. The students are coached and instructed in technique based not on a structured "recipe" or checklist, but rather by the route of their questions and curiosity. By not providing a handout or agenda, the lab seems less like a "class" and more like a "fun activity"—a real departure from the classical learning environment.

The radical departure from the traditional classroom protocol is one of the deliberate features of the exercise which seems to significantly elevate the enjoyment, motivation, and stimulation for the pursuit/engagement of the activity. It is only at the end of each process or task, when the instructor "re-phrases" what the students have witnessed, that the association between the activity and the conceptual material (terminology, etc.) becomes clear, and the students realize that they are witnessing a physical manifestation of the conceptual knowledge they "blindly memorized" in previous class sessions.

This is the essence of "discovery learning." In essence, the "learning" process is no longer a "knowledge transfer." The students synthesize the knowledge by combining the terms they blindly memorized by rote (from earlier classes) with what they just witnessed at each stage or task. By associating what they saw with what they knew, they combine the two to yield the desired knowledge and understanding. As the studies cited above show, knowledge acquired in this manner is generally learned more thoroughly and retained longer than knowledge delivered in the traditional delivery processes such as handouts, textbooks, PowerPoint® slides, and other structured transfer techniques.

## IV. STUDENT RESPONSE AND EVIDENCE OF EFFECTIVENESS

This hands-on discovery exercise quickly became one of the most popular activities in any accounting course at the institution. Informal word-of-mouth praising the "fun activity" circulated among students and was even occasionally cited as one of the reasons some students considered an AIS concentration. Student interest and motivation has unquestionably been stimulated.

However, the interest, motivation, and impetus for learning significantly increased in the second semester the lab exercise was in use, through an unanticipated "accident." Appendix B describes a unique incident whereby the monitoring station actually witnessed a real-world control breach involving the apparent loss of a sales transaction record at a local business located within radio range of the receiving station. The first-hand witnessing of an actual internal control breach greatly increased student interest as word quickly spread about the real accounting problems that could have been avoided had accountants better understood the operation of the data transmission technology.

Relating back to the course unit's learning objective, students needed enhanced understanding of network operation so they would "be able to identify major threats and vulnerabilities to internal control associated with various networking technologies." The exercise itself did not present a new learning objective. Rather, it was hoped the exercise would serve as a more effective learning vehicle for existing topical coverage. Accordingly, no assessment instruments or rubrics were changed or added as a result of introducing this exercise. In other words, students were expected to perform the same assessment tasks after receiving the lab as students in previous semesters had with the less active, more traditional, classroom learning experience covering the same material.

A comparison of before-and-after performance on the assessment rubrics show unequivocal learning enhancement. In addition to the increased attention, interest, and motivation cited by students in their informal conversations, the assessment data confirmed that students had a deeper understanding of network operation, as evidenced by their improved performance on the assessment instruments and rubrics. In fact, student learning was enhanced far beyond the instructor's expectations.

Student scores on the networking unit overall went from being the lowest of the six units, to being the highest. Almost all students are now scoring perfectly on networking concepts on the examination, even though the exam tasks have not materially changed (beyond the normal semester-to-semester alteration necessary to avoid cheating).

Additionally, students now consistently score near perfect on the networking aspects of the comprehensive group project students undertake at the end of the course. Further, student understanding and comprehension as evidenced by class discussion is noticeably higher, and increased student enthusiasm and enjoyment is unmistakable. Formal institutional assessment levels on the embedded measures results for this learning objective have moved from being marginally "Satisfactory" to being "Exceptional."

Table 1 shows a summary of the performance of students on assessment rubrics associated with the networking unit. The table compares the average student performance on the rubrics as measured in the six semesters prior to the introduction of the lab exercise (column 4) to the average student performance on those same rubrics in the three semesters in which the lab was used (column 5). The rubric standard and level of difficulty remained constant across the nine semesters. (Based on the near-perfect scores of students, the instructor is planning to increase the difficulty to continue to provide challenge to the students.)

**TABLE 1**
**Comparative Results of Student Performance**

| (1)<br>Assessment Rubric | (2)<br>Possible Perfect Score | (3)<br>Assessment Criteria for Satisfactory/ Exceptional Rating | (4)<br>Average across Six Semesters before Lab | (5)<br>Average across Three Semesters with Lab |
|---|---|---|---|---|
| Composite of thirteen examination questions | 100% | 70%/90% | 70% | 98% |
| Professor's Subjective Evaluation of Discussion Understanding | 30 points | 20/25 points | 21 points | 29 points |
| Group Project Grade—Segment on Networking | 20 points | 15/18 points | 12 points | 19 points |

## V. SUMMARY

This case can be thought of as being similar to the chemistry labs, physics labs, and other hands-on discovery exercises more common among the hard sciences than in accounting. Such hands-on learning is an ideal way to illustrate complex concepts within a context, while simultaneously stimulating interest and attention and rewarding students with the emotional pleasure of discovery. The wholly unexpected discovery (described in Appendix B) provided additional interest, motivation, and stimulation in students, and vividly illustrated the importance of the topical material, providing an exceptionally effective learning environment.

By introducing physical, tangible demonstrations of difficult mental concepts, coupled with discoverable "Aha!" moments, this experience provides empirical evidence that the use of in-class "lab" sessions can increase interest, participation, and resulted in active learning. It is expected that relatively few, if any, other instructors have the expertise, access to equipment, or desire to duplicate this particular exercise, and certainly stumbling across a real-world incident in front of students should be considered (hopefully) a rare occurrence. However, this experience should serve as an inspiration to instructors who might be struggling with similar difficulty getting concepts across to students, or who are seeking ways to motivate and stimulate student thinking. Accounting educators should always remain alert for opportunities to introduce hands-on learning, especially ones that can be designed to facilitate discovery learning, whether contrived or accidental.

## APPENDIX A
## A SUGGESTED STUDENT PROTOCOL

The material actually covered in the lab can vary from instructor to instructor, depending on the instructor's individual strengths, knowledge, background, and experience, as well as how deep into OSI operation the instructor wishes students to delve. For this reason, a one-size-fits-all recipe cannot realistically capture the potential benefits from using this lab.

While each instructor must have a carefully prepared agenda and list of items to be covered, the allure of discovery learning from the students' perspective is the thrill of "stumbling upon the unexpected" via the pursuit of curiosity. For that reason, the best applications of discovery learning will appear to the student to be a completely unscripted series of discoveries that are made in the pursuit of interest, the order being dependent upon student reaction to successive "discoveries" and expression of desire.

Below is a sample series of activities, accompanied by a set of questions which can be posed to students during the course of the series, to get them thinking, and thereby establishing a relationship between what they are seeing and what the instructor desires they learn. Notice that the learning is not in the form of "knowledge transfer" as much as it is "knowledge synthesis" via the student relating what they just saw to what they previously "memorized." In other words, the students themselves are synthesizing the conceptual understanding from an internal mental *combination* of previously meaningless memorization with a just-witnessed physical manifestation.

Activity 1: Assemble your "station" by (1) starting the terminal emulation software on your computer, (2) connecting your computer's serial port to the Terminal Node Controller, and (3) connecting the TNC to the radio. Question: which layer(s) of the OSI are being prepared for use by starting the terminal emulation software? ... by the connection to the TNC? ... by the connection to the radio?

Activity 2: As directed by the instructor, type connection requests on your keyboard that instruct the TNC to establish a connection with a second group's station. Watch the packets on the monitoring screen at the front of the classroom. Notice the form of your connect request packets, and the acknowledgement and reply packets (as displayed on the monitoring screen at the front of the classroom). Question: which layer(s) of the OSI are being illustrated by your "connection"?

Activity 3: After establishing the connection, exchange some messages with the other station. (For example, ask the other group a question, invite them to join you for lunch after class, or ask what they think the score will be for the football game this weekend.) On the monitoring screen, notice the serial numbering of the information packets, and notice the form of the acknowledgement packets. Question: which layer(s) of the OSI are illustrated by your message contents? Which layer is illustrated by the acknowledgement packets? How do you think the serial numbers are used by the TNCs?

Activity 4: Following the directions of the instructor, transfer a small file to the other station. By watching the monitoring screen, notice how the file has been broken up into packets. Pay particular attention to the serial numbers, the acknowledgements, and the other overhead packets. Question: which layer(s) of the OSI are at work here? How do these layers interact?

Activity 5: Notice the interruption in transmission. Question: What do you think caused this? What did the TNC do to attempt to recover? What layer of the OSI might be at work here?

Activity 6: Issue a disconnect command to de-activate the connection you have been using. Following the directions of the instructor, use the commands provided to connect your station to a third station, using the second station as a digipeater. Notice the new form of the information packets on the monitoring screen, and the new form of the acknowledgement packets. Question: which layer is being illustrated here, and what leads you to that conclusion?

Activity 7: Notice the new packet types being exchanged by the TNCs as a result of your use of the digipeater. Question: What layer is being illustrated by these packets? Using what you know about this layer, make a guess about the meaning of the data elements contained in these packets.

Activity 8: Notice the packets which appear on the monitoring screen when two stations attempt to transmit simultaneously. Questions: what is this called? Why were the additional packets generated? How did the stations resolve the contention? What layer(s) of the OSI are being illustrated by this activity? How might this affect network performance or throughput? What do you think happens as more and more stations are added to the network? Which management assertions might be affected by this? At what point do you think the retries and overhead packets will overwhelm the network traffic? Can you think of a way to ease this congestion? What layer(s) are involved in that solution?

Activity 9: Notice the "intruder" packet pointed out by the instructor. Questions: If the instructor had not pointed out the intruder packet, could you have identified it? How? What solutions can you come up with to deal with this problem? What ramifications does this have for accountants and auditors? Which of the management assertions are affected by this incident?

Activity 10: Send a confidential message (one that cannot be seen on the monitoring screen by the rest of the class) from your group to one of the other groups. Question: What ramifications does this have for accountants and auditors? Does this mean there is no way to exchange information confidentially? Does your experience prove that wireless networks are open to the public and can be intercepted by anyone with the proper listening equipment? What solution can you come up with to deal with this problem?

Activity 11: Use your "solution" for private communication to pass a confidential message to another group. Questions: What drawbacks did you discover to this method? How does this drawback apply to the world of e-commerce and internet nodes?

## APPENDIX B
## AN UNEXPECTED DISCOVERY: A REAL WORLD CONTROL BREACH

During the execution of this lab exercise in the second semester, an actual incident occurred without warning or planning. This incident vividly demonstrated—far beyond the instructor's wildest expectations—the real-world consequences of failure to appreciate the internal control ramifications of accountants not fully understanding the operational details of networking technology.

The second semester the lab was used, during the set-up of the equipment, the monitoring station in the front of the classroom (projecting the received data) was inadvertently tuned to a different radio frequency. Suddenly the monitoring station received a data packet over the radio, even though the other nodes were not yet operational. This stray data transmission obviously came from a source outside the room. A few seconds later, a second packet appeared, followed shortly by a third. By looking at the data in the packets (shown on the overhead screen), the students and instructor surmised that the packets contained data on some kind of business transactions. The data contained what appeared to be small dollar amounts (numbers between 010.00 and 040.00), quantities (numbers between 03.500 and 20.000), the current time and date, letters that might represent a product code, a node identifier, and a lengthy string of numbers that could possibly be account numbers or perhaps credit card numbers. Each data packet was responded to by an acknowledgement packet, apparently from the destination node.

It was guessed that the monitoring station was picking up a two-way exchange of data between a piece of mobile or remote data collection equipment and its respective base accounting information system. The 2.4 GHz band being monitored at the time is used by thousands of different types of unlicensed low-power wireless equipment, from baby monitors, garage door openers, keyless auto lock systems, and even commercial wireless equipment including 802.11b and 802.11g network gear. The band is widely used for wireless accounting data collection equipment, such as handheld inventory counters, RFID readers, and other wireless equipment. Microwave ovens also operate in this band. Because of the shared nature of this band, anyone can legally monitor transmissions, regardless of source or content (FCC 2005).

On a hunch, on the next class day, the instructor sent a graduate assistant to a local gasoline station a quarter-mile from campus. This station had recently replaced its gas pumps with pay-at-the-pump models. The graduate assistant was instructed to purchase a gallon of gas on the instructor's credit card. Sure enough, while the class watched, a packet came across the screen displaying the instructor's credit card number—in unencrypted plain-text! The packet was duly acknowledged by what apparently was the gas station's local computer located in the building.

A minute later, a second packet came across, repeating the credit card number and this time containing the dollar amount and gallon quantity of the sale. This packet too was dutifully acknowledged by the receiving network node attached to the station's accounting computer.

The class was apparently listening to the wireless link between the pump and the gas station building. The first transmission exchange represented the pump's request for credit approval, and the second transmission was the pump's completion of the sale. In each case, the pump's packets were acknowledged by "ack" packet responses from the station's computer, confirming to the pump its data had been properly received and recorded, in accordance with standard data-link layer protocol.

(Once each packet was received by the station building's computer, it of course was probably passed on to the credit card processing company, the gas station headquarters, and/or other locations, using different network links, possibly a satellite link, telephone land line link, etc. Those links were not detected.)

If this discovery was not enough to awe both student and instructor, what happened next was even more astounding. As the class watched, a second pump began transmitting packets to complete a $37.00 sale. However, the second pump's packets were for some reason not acknowledged by the station's computer. As it was designed to do, the second pump began to "retry," repeating its packet transmission twice every second. Obviously, something was keeping the station computer from properly receiving the packet, or at least preventing the station's computer from acknowledging the data.

The pump continued its unsuccessful attempts to "complete the sale" for two or three minutes, when suddenly there came from the station house a packet containing all zeros. The pump immediately ceased transmitting its completion-of-sale packets, and a few seconds later, the same pump transmitted a new packet containing a new credit card number.

What had happened? This situation presented an impromptu critical thinking exercise. Upon returning to campus (and returning the instructor's credit card!), the graduate assistant reported that after completing his sale, he had gone inside the station building to purchase a drink. He noticed another customer heating a pastry in the station's microwave oven. On his way in, however, he noticed a customer at another pump outside who had completed pumping his gas, and seemed to be waiting for a receipt. After a minute or so, this customer apparently gave up on getting his receipt and drove away. A new customer came to the same pump, and had trouble activating it. The new customer used the intercom button and informed the station attendant that the pump would not activate. Therefore, as the graduate assistant at the counter watched, the station attendant pressed the "hard reset" button on the station's pump control console. The hard-reset cleared the pump, activating it for the new customer. However, it also apparently cleared the previous $37.00 sale the pump had been attempting to transmit!

When this information was presented to the students, a valuable integrative thinking exercise was played out. Students used their knowledge to properly deduce that the microwave oven (operating near the frequency of the low-power network link) was interfering with the transmission, preventing its reception by the station computer. The pump properly began retrying. However, the station node never received the pump's transmission. The completion-of-sale packet could not get through because of the interference caused by radio leakage from the microwave oven.

Apparently, the pump had been designed to defer printing the customer receipt until after receiving confirmation that the sale had been duly completed. Hence, the customer at the pump did not immediately receive a printed receipt. After a minute or two, the first customer gave up and drove away.

A new customer arrived at the pump, which was still busy trying to get its completion-of-sale packet through. When the pump would not activate for the new customer, she signaled to the attendant. The attendant, not fully understanding the technology, not knowing how the network operated, unaware of the potential interference from the oven, and unaware of the potential for an unrecorded sale, pressed the hard-reset button on the console in an attempt to activate the pump for the new customer. The reset process apparently transmitted the all-zeros packet seen by the class addressed to the pump.

The reset packet reset the pump's microprocessor, effectively killing the $37.00 sale. The station computer never learned how much gas the first customer pumped, and odds are that the first customer's credit card account was never charged for the $37.00 purchase!

This real world experience graphically illustrated the risks and vulnerabilities inherent in modern data transfer systems in a manner far more effective than anything the instructor could have conceived. A scenario taking place across the next three weeks served as even more emphasis of the importance of accountants needing a thorough understanding of network design and operation.

As a service to the company, the instructor wrote a nice letter to the controller at the gas station's corporate headquarters, explaining the incident. A polite and professional response was received wherein the controller denied that such an event could happen. The controller made four assertions in his response: (1) he had been assured by the company's technical support staff that the low-power transmitter in the pump could not be received more than 100 feet away from the station property and thus we could not have been listening to their transmissions; (2) the technical support staff had assured him that the pump's transmissions were digital and therefore could not be received by radio receivers, further convincing him that we could not have eavesdropped on his station's transmission; (3) the technical support staff did not believe heating a pastry in a properly-shielded microwave oven could possibly interfere with the commercial wireless equipment they had used in their network; and (4) the network staff had reassured him that their system was well designed and could not possibly miss a sale because the network equipment is programmed to re-send its data if for any reason the data is not received by the receiving computer. The controller expressed steadfast confidence and faith in his network technical staff. He repeated his disbelief that his systems could have possibly missed a sale.

All four assertions of the controller were erroneous, and all four resulted from his lack of knowledge of how the network operated, and the threats/vulnerabilities of modern network systems. In contrast, the network designer and technical staff may have possibly known something about how the network operated, but were unaware of, or did not have a full appreciation for, internal control concepts and the threats and vulnerabilities to the accounting data resulting from the environment coupled with designed operation of their data transportation system. (Another explanation is that the technical staff were skilled in network construction at a high level (being able to connect and configure components), but lacked the basic fundamental knowledge of exactly how the various components worked.)

As for the controller's first assertion, the range of a wireless signal is more dependent on the receiver than the transmitter power. NASA's Pioneer and Voyager spacecraft are almost ten billion miles from earth (several times farther than the planet Pluto) and yet their paltry 35-watt signal remains readable (Peat 2007). More relevant, empirical experiments have proven that milliwatt signals used in commercial networking gear (for example, 802.11 networks, designed for useful operating ranges of up to 300 feet) can be easily and reliably copied and effectively used for workable data connections over distances of *at least 56 miles*, even using standard off-the-shelf 802.11 equipment (Fordham 2005). The fact that the class had witnessed a data packet containing the instructor's personal credit card number, in clear plaintext, showed conclusively that the class was indeed receiving the pump's transmissions.

As for the controller's second assertion, he misunderstood the technical support staff's assurance that digital wireless signal could not be "received by a radio receiver." Any wireless signal can be received by an appropriately tuned radio receiver—by definition, that is what a radio receiver is. The technical support staff may have meant that digital signals could not be read and understood by human ears the way an analog transmission (such as a radio broadcast) can. It is true that digital signals are not normally interpretable by the human ear, but they are perfectly readable by digital decoders such as the TNC being used by the class. The network staff was apparently overlooking the possibility of the interception of the wireless signals by someone who possessed such a decoder, even though the decoders are legally and readily available to the general public and can be obtained from dozens of outlets around the country.

As for the third assertion, microwave ovens are simply radio transmitters where the transmitted signal, instead of radiating to a remote receiver, is sealed inside a metal box where it can be reflected and re-used—the multiple bombardment of the food by high-power radio signals causes heating. While almost all of the radio wave is kept inside the sealed box, there is still a minute amount of leakage around door cracks and through the viewing glass filter. The allowable leakage from standard microwave ovens, while miniscule and negligible from a health standpoint, is still many dozens of times stronger than that necessary to interfere with and prevent reception of nearby low-power (milliwatt) digital signals like those used in commercial wireless networks (FCC 2005).

Finally, analyzing the patterns of interactions between the pump and station computer node showed that the pump was indeed re-trying to get its sale through, just as the technical support staff had expected. However, the support staff had not counted on the station attendant manually overriding this control. The data witnessed by the class showed unquestionably that the pump had ceased all attempts at retries once the reset signal was received. The sale was most likely never recorded by the station's computer, and thus never passed along for credit-card billing, or recording in the company's financial records. The clerk had not been informed of the unintended consequence of resetting the pump, possibly because the technical support staff's background and training did not include appreciation for the need to fully assess such risks to the accounting data.

By witnessing this actual incident in person, the class learned an invaluable lesson about internal control. The experience drove home the importance of accountants and auditors needing a good understanding the operation of networks. It vividly illustrated, even emphasized, the lack of internal control understanding (or at least appreciation) possessed by some technical support network personnel.

In epilogue, the following semester, the instructor experimented with the eavesdropping receiver to try to tune in the packets from the station to duplicate the scenario. This time, it was discovered that the station had changed modulation to spread-spectrum (greatly alleviating interference from point sources, like the microwave oven), and more importantly, the packets were now fully encrypted, making the content unreadable. It is assumed that in spite of his initial protestations in his letter to the instructor, the controller had followed up, discovered additional knowledge about networking, and implemented the changes in network design. It is also assumed that additional controls were also put in place outside the network to at least detect, if not correct, any sales that may still be missed by the network. (Students in the course were able to think of several possible control activities that would have detected unrecorded sales, ranging from memory modules in the pumps to taking periodic inventory of the station's tanks.)

## TEACHING NOTES

Teaching Notes are available only to full-member subscribers to the Journal of Information Systems through the American Accounting Association's electronic publications system at http://www.atypon-link.com/action/showPublisherJournals?code=AAA. Full member subscribers should use their personalized usernames and passwords for entry into the system where the Teaching Notes can be reviewed and printed.

If you are a full member of AAA with a subscription to the Journal of Information Systems and have any trouble accessing this material, please contact the AAA headquarters office at office@aaahq.org or (941) 921-7747.

## REFERENCES

American Institute of Certified Public Accountants (AICPA). 2001. *The effect of Information Technology on the auditor and consideration of internal control in a financial statement audit.* Statement of Auditing Standards Number 94: Profession Standards, Vol. 1. AV Sec 319. New York, NY: AICPA.

Bamber, E. M., and L. S. Bamber. 2006. Using 10-K reports brings management accounting to life. *Issues in Accounting Education* (August): 267–290.

Bryant, S. M., and J. E. Hunton. 2000. The use of technology in the delivery of instruction: Implications for accounting education researchers. *Issues in Accounting Education* (February): 129–162.

deFreitas, S., and M. Oliver. 2006. *Computers and Education* (April): 249–264.

Dinan, F. J. 2005. Laboratory-based case studies: Closer to the real world. *Journal of College Science Teaching* (October): 27.

Drake, A., S. F. Haka, and S. F. Ravenscroft. 2001. An ABC simulation focusing on incentives and innovation. *Issues in Accounting Education* (August): 443–472.

Easttom, C. 2006. *Computer Security Fundamentals.* Upper Saddle River, NJ: Pearson/Prentice Hall.

Ellsworth, P. C., and V. G. Sindt. 1994. Helping Aha! to happen. *Educational Leadership* (February): 40–44.

Ernest, P. 1987. The Aha! experience. *Mathematics in School* (January): 10–11.

Federal Communications Commission. 2005. *Title 47, Telecommunications, Part 15 as Amended.* Code of Federal Regulations (CFR). Washington, D.C.: FCC: Office of the Federal Register.

Fordham, D. R. 2005. IEEE 802.11 experiments in Virginia's Shenandoah Valley. *QST Journal of the American Radio Relay League* (July): 35–41.

Hayes, D., and J. K. Reynolds. 2005. Caroline's Candy Shop: An in-class role-play of the revenue cycle. *Journal of Information Systems* (Spring): 131–154.

Hecht, F. 1997. The Aha! factor. *Director* (July): 59.

Hermanson, D. R. 1994. The effect of self-generated elaboration on students' recall of tax and accounting material: Further evidence. *Issues in Accounting Education* (Fall): 301–318.

Liljedahl, P. G. 2005. Mathematical discovery and affect: The effect of Aha! experiences on undergraduate mathematics students. *International Journal of Mathematical Education in Science and Technology* (Mar–Apr): 219–234.

Maiwald, E. 2001. *Network Security: A Beginner's Guide*. Berkeley, CA: Osborne/McGraw-Hill.

O'Donnell, J., and J. Moore. 2005. Are accounting programs providing fundamental IT control knowledge? *The CPA Journal* (May): 64–67.

Orange, C. 2002. *The Quick Reference Guide to Educational Innovations: Practices, Programs, Policies, and Philosophies*. Thousand Oaks, CA: Corwin Press.

Peat, C. 2007. Spacecraft escaping the solar system: Where are they now? Available at: http://www.heavens-above.com/solar-escape.asp?

Peters, E. 2005. Reforming cookbook labs. *Science Scope* (Nov–Dec): 16–21.

Pillsbury, C. M. 1993. Systems softball: An interactive group game for teaching internal control evaluation. *Issues in Accounting Education* (Spring): 128–139.

Rose, J. M., A. M. Rose, and C. S. Norman. 2005. A service learning course in accounting information systems. *Journal of Information Systems* (Fall): 145–172.

U.S. House of Representatives. 2002. The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H. R. 3763]. Washington, D.C.: Government Printing Office.

Wright, S., and A. M. Wright. 2002. Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* (Supplement): 99–130.