An Integrated Multimedia Based Platform for Teaching Network Security

W Makasiranondh, S P Maj, D Veal,

Edith Cowan University, Perth, Western Australia

Summary
Configuring a secure network is of paramount importance to all organizations. Accordingly staff should be appropriately qualified and trained. The Cisco Network Academy Program (CNAP) recently introduced the Cisco Network Academy Associate (CCNA) Security course for college students, university students and practicing professionals. This course is designed to provide the skills and knowledge to design, configure and manage a secure network. One of the key technologies employed by this course is the Security Device Manager (SDM). However it has been demonstrated that there are significant limitations with SDM. This problem is exacerbated when courses are offered on-line to remotely located students. This paper demonstrates that these problems are addressed when students are provided with an integrated multimedia based platform incorporating SDM and also the State Model Diagram (SMD) method of device configuration and management.
Key words:
Network security, Security Device Manager (SDM), State Model Diagrams (SMDs), Remote Access Networking Laboratories.

1. Introduction

Security is an essential aspect of network configuration and management. Significantly security threats are not only complex but are also constantly and dynamically developing in complexity. In order to address this problem Cisco, the world's largest vendor of network equipment and developer of the world's largest network educational program have introduced the Cisco Network Academy Associate (CCNA) Security Course. The prerequisite for this course is successful completion of the introductory Cisco Network Academy Associate (CCNA) course. The CCNA course teaches the basic skills and knowledge required for configuring and managing a standard but insecure network. The CCNA Security course builds upon this foundation knowledge in order to provide specialist theoretical and practical knowledge in network security. Comprehensive on-line instructional material is available along with the associated workshop exercises. However, it has been demonstrated that there are some major concerns with conducting security based laboratories in an online mode[1]. A key tool in this course is the Security Device Manager (SDM). The SDM is a graphical user interface (GUI) designed to simplify secure device configuration, by means of a menu based interface.

Manuscript received December 5, 2010
Manuscript revised December 20, 2010

There are some important limitations of SDM; for example it cannot be used to configure and manage layer switches [2]. This is a serious limitation as SDM cannot be used to configure protocols such as: Virtual LANs (VLANs); Trunk Aggregation; Spanning Tree Protocol (STP) and other layer 2 related protocols. Even more importantly, SDM cannot be used to ensure a layer 2 switch is properly secured against attacks that include: VLAN hopping; switch spoofing; and port violation. Although more effective network management tools are available commercially, they are not generally cost effective when used solely for learning purposes, and they are not freely available on CNAP based courses.
Despite the limitation of SDM in interacting with layer 2 related devices, using the SDM is relatively easy to configure the network security; for example a site to site Virtual Private Network (VPN) and a firewall can be configured by using the default options. On the other hand, inputting an associated generated configuration code via command line interface (CLI) alone can be considered as a complex task and hence potentially problematic when conducting fault diagnosis. Incorporating another GUI tool, such as Sate Model Diagram (SMD) may compensate this complexity.
Therefore, this study explored the possibility of incorporating more device representation tools to the learning environments.

2. State Model Diagrams

In addition to employing the standard text-based Command Line Interface (CLI) there are considerable advantages to using the State Model Diagram (SMD) method for device configuration and management [3]. It was found that:

Significantly, SMDs allow networking concepts and technical detail to be taught using a single common template. Technical details may be progressively included while maintaining conceptual integrity by means of hierarchical leveling. SMDs may, therefore, support student learning at both introductory and advanced levels [4]

Experimental results have shown that when instruction is based on SMDs students develop a rich conceptual model that is strongly aligned with that of an expert [5]. Significantly the SMD method is universally applicable and it has been demonstrated that this method of device and network protocol modeling can be used for all network devices (switch, router, wireless access points etc) and associated protocols (routing, switching etc) [6]. Furthermore the SMD method has been found to be particularly useful when configuring complex security devices and protocols such as PIX devices and Zone Based Firewalls (ZBFs) [7]. It should be recognized that correct network device configuration is of paramount importance.

Table 1: Evaluation of configuration interfaces

	Advantages	Disadvantages
CLI	- Can be used for all network devices and protocols - Routinely used by professional in the field	- Verbose, lot of detail that may not be important. - Syntactically exact and demanding. - Difficult to learn and use especially for novices - Device configuration may be time consuming - Cannot display device status - Cannot display protocol status without user intervention
SDM	- Simple to use. - Lacks the granularity of control that is possible with both CLI and SMD - Rapid device configuration - Can display device status - Can automatically display protocol status	- Cannot be used for configuring and managing layer 2 switches. - May generate extensive configuration commands which may be problematic during fault diagnosis
SMD	- Can be used for all network devices and protocols. - Provides a hieratical representation of a network. - Multiple devices and protocols can be simultaneously displayed - Rapid device configuration - Can display device status - Can automatically display protocol status	- Proof of concept software only

According to Van den Akker [8], security breaches may be caused by user errors. Hence network managers must be able to use and clearly understand the system under consideration. Accordingly Nielsen developed criteria for a successful user interface [9]. This was further developed by Johnston who proposed a security Human Computer Interface (HCI-S) [10]. Certainly each method, CLI, SDM and SMD each have their strengths and weaknesses (table 1). However it has been argued that:

The SMD method user interface represents an intermediate to the CLI and SDM. The SMD provides granular configuration control by means of independent but closely coupled functional groups [7].

3. Remote access, on-line instruction

On-line instruction is now a common method of instruction. Not only is it ideally suited to remotely located students but also it is a cost-effective method of course delivery. Many students now routinely use communication technologies such as email, podcast; discussions boards etc and hence have developed skills and aptitudes ideally suited to on-line delivery.
Furthermore, within the field of network technology there are network simulation tools such as Packet Tracer and GNS3. These simulators allow students to create network topologies and then configure the associated virtual devices. Significantly they can be deployed on a standard PC. Packet Tracer is in fact an integral part of the Cisco Network Academy Associate (CCNA) course. However, Cisco recommends Packet Tracer as a software tool to be used in addition to standard, practical, hands-on, laboratory based instruction [11]. It is recognized that such skills are of paramount importance to prospective employers. It is not uncommon for on-site students to enroll as remote students but attend the normal workshops. Simulation tools depict part of the actual hands-on experiences that students may learn from the traditional classrooms. However, practicing with actual devices will give a further realistic experience. A significant problem therefore is providing remote, on-line students with the opportunity to develop their practical skills without access to actual network devices.

4. Enhanced remote access, on-line platform

In order to address this problem a pedagogically rich, interactive on-line learning platform has been developed [12]. Remote on-line students are provided with a PC based interface consisting of two different network device representations (figure 1) and four communication methods:

Device representations are:

- The Command Line Interface (CLI)

- State Model Diagrams (SMDs)

Communication representations are:

- Video stream
- Voice over IP (VOIP)
- Class presentation slide
- Online chat

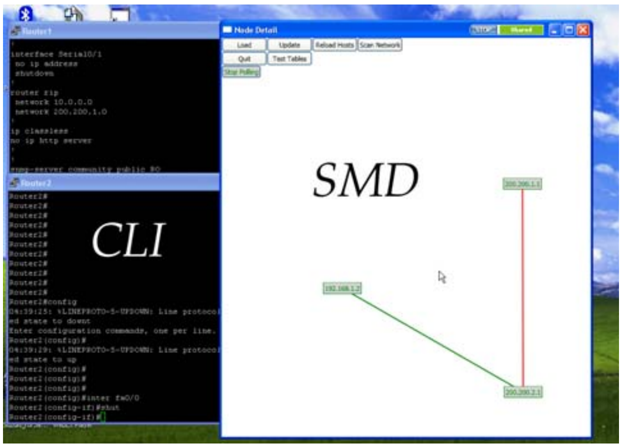

Fig. 1 A standard learning environment consisting of CLI and SMD.

This platform does not provide actual hands-on experience but does provide students with visual communication with the devices they are actually configuring. This is important because novice learners need to make the conceptual transition from the 'concrete' to the 'abstract' [13]. Interaction with a physical device is therefore of paramount importance to novice students.

Furthermore in some institutions, especially in developing countries, there may simply be no alternative due to the lack of information and communication technology (ICT) devices for instructional purposes [14]. A standard Cisco based new unit (3 routers, 3 switches and wireless equipment) costs approximately AUS$19,000. Such a unit is suitable for only two students at a time. A class set of 10 units, suitable for a class of twenty students, is likely to be prohibitively expensive for many institutions. They may need to consider also the rapid falling rate of equipment price on the period after purchased, which can fall as quick as 17% annually [15]. Although second hand equipment can be purchased from the internet as an economical alternative, they may not be reliable and some institutions policies may prevent acquiring these used equipment.

Preliminary trials indicate there are advantages to employing this pedagogically enhanced learning platform. According to this preliminary study, it elaborated the need of incorporating multimedia learning environment by demonstrating the benefit of accessing to more than CLI control of the laboratory [12].

5. Incorporating SDM into the enhanced remote access on-line training platform

The Security Device Manager (SDM) was incorporated into the Enhanced Remote Access on-line platform as a third method of device representation (figure. 2). One of the challenges of providing GUI based configuration tools was the tools normally require direct IP connectivity to the devices. The security devices in the laboratory are normally separated from live production networks. Hence, direct IP connectivity to these devices seems to be prohibited and considered as potential risk to the ongoing network. However, this study provided these tools in the learning environment as an alternative of device representation.

Device representations are:

- The Command Line Interface (CLI)
- State Model Diagrams (SMDs)
- The Cisco - Security Device Manager (SDM)

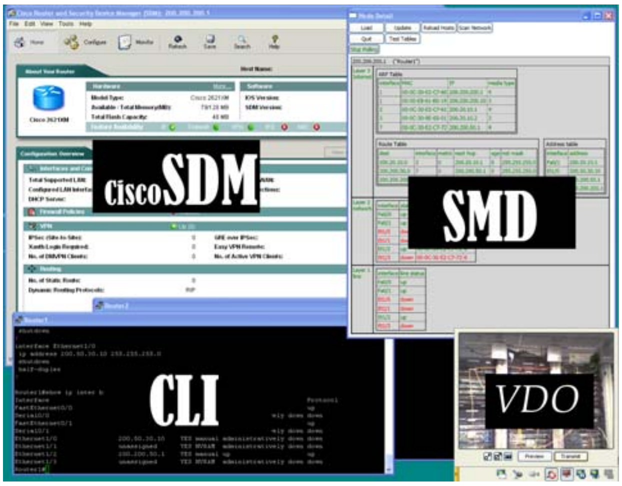

Fig. 2 User view of Remote access screen, incorporating Cisco SDM.

Enhanced Remote Access on-line platform learning environment allows students, within the limitations of each software tool, to interact with network devices and protocols using all three device representations. Work to date has demonstrated that all three software tools can operate concurrently. Changing a device configuration using, for example, the CLI automatically results in the associated change in the SDM and SMD device representations. Similarly changing a device configuration using the SDM automatically effects changes when viewed by the other representations. Preliminary trials were conducted over a remote link (100km). Despite the computational overheads associated with Graphical User Interfaces there was no perceptible deterioration in performance. However further trials are needed in order to evaluate the effects, if any, of remote access to users in other countries with communication links that may be problematic.

Our trials accessing the system found that an average hour data consumption rate was around 218MB, which can be calculated at approximately 0.48 Mbps or 496 Kbps bandwidth consumption. This was tested via a 7497/975 Kbps ADSL connection. Some acceptable delay, of about 2 seconds, may occur with this high bit rate. However, when testing at the lower bandwidth 64kbps, the response rate of the system fell drastically. Delay was increased to 10 seconds for any GUI action undertaking. As expected, CLI commands could be used normally as they are purely text based and were not affected by this slower connection.

6. Conclusions

This paper has demonstrated that remote, on-line access may be considerably enhanced by incorporating three network configuration tools – the Command Line Interface, State Model Diagrams and the Security Device Manager. Despite the higher bandwidth overheads during preliminary trials there was no measurable deterioration in performance except when using in the lower speed connection. Further work is needed in this important area of remote laboratory access.

References

[1] S.P. Maj, D. Veal, and L. Yassa, "A Preliminary Evaluation of the new Cisco Network Security Course," International journal of computer science and network security, vol.10, pp.183-187, 2010.

[2] S.P. Maj and D. Veal, "Using State Model Diagrams to Manage Secure Layer 2 Switches," International journal of computer science and network security, vol.10, pp.141-144, 2010.

[3] S.P. Maj, G. Murphy, and G. Kohli. "State models for internetworking technologies," Frontiers in Education, 2004. FIE 2004. 34th Annual, F2G-10-15 2004.

[4] S.P. Maj and D. Veal, "State Model Diagrams as a Pedagogical Tool: An International Evaluation," Education, IEEE Transactions on, vol.50, pp.204-207, 2007.

[5] S.P. Maj, G. Kohli, and T. Fetherston, "A pedagogical evaluation of new state model diagrams for teaching internetwork technologies," Proceedings of the Twenty-eighth Australasian conference on Computer Science - Volume 38, 2005.

[6] S.P. Maj and D. Veal, "An Evaluation of State Model Diagrams for Secure Network Configuration and Management," International journal of computer science and network security, vol.10, pp.66-72, 2010.

[7] S.P. Maj, W. Makasiranondh, and D. Veal, "An evaluation of Firewall configuration methods," International journal of computer science and network security, vol.10, pp.1-7, 2010.

[8] T. Van den Akker, Q.O. Snell, and M.J. Clement, "The YGuard access control model: set-based access control," Proceedings of the sixth ACM symposium on Access control models and technologies, 2001.

[9] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," Proceedings of the SIGCHI conference on Human factors in computing systems: Empowering people, 1990.

[10] J. Johnston, J.H.P. Eloff, and L. Labuschagne, "Security and human computer interfaces," Computers & Security, vol.22, pp.675-684, 2003.

[11] Frequency asked questions: new CCNA curricula (2009), December 2nd 2009, http://www.cisco.com/web/learning/netacad/downloads/pdf/newCCNAfaq.pdf

[12] W. Makasiranondh, S.P. Maj, and D. Veal, "A pedagogical rich interactive on-line learning platform for Network Technology students in Thailand," Thirteen Australasian Computing Education Conference, In print.

[13] J. Piaget, The origins of intelligence in children, New York: International Universities Press 1952.

[14] P.T.J. James, "Academic staff perceptions of ICT and eLearning a Thai he case study," Turkish Online Journal of Educational Technology, vol.7, pp.36-45, 2008.

[15] M. Doms and C. Forman, Prices for local area network equipment. Working papers in applied economic theory, 2003.

A/Prof S. P. Maj has been highly successful in linking applied research with curriculum development. He was awarded an ECU Research Leader of the Year in 2000, and Vice-Chancellor’s Excellence in Teaching Award in 2002, and 2009. He received a National Carrick Citation in 2006. He is the only Australian judge for the annual IEEE International Student Competition and was the first Australian reviewer for the American National Science Foundation (NSF) Courses, Curriculum and Laboratory Improvement (CCLI) program.

Dr. David Veal is a Senior Lecturer at Edith Cowan University. He is the manager of Cisco Network Academy Program at Edith Cowan University and be a unit coordinator of all Cisco network technology units. His research interests are in Graphical User Interface for the visually handicapped and also computer network modeling.

Woratat Makasiranondh received the B.Eng in Telecommunication Engineering from Suranaree University of Technology, and M.S. degrees in Computer Science from Rangsit University in 2001 and 2005, respectively. After working in the IT industry he became an academic member of Rangsit University. He is currently on study leave and undertaking his doctorate research at Edith Cowan University in the field of network technology education.