Approach to Challenges of Learning Computer Network Courses by using Pedagogical Network Tool

Mar Lar Win  
University of Computer Studies, Monywa  
marlarwin.mw@gmail.com

Pan Ei Phyuu  
University of Computer Studies, Monywa  
paneiphyu82@gmail.com

Thazin Nwe  
University of Computer Studies, Monywa  
thazinnwe7@gmail.com

Abstract

Computer network is a region which domain needs expert in networking principle and applicable experience. Teaching computer network concepts is challenging due to theoretical abstract concepts. To understand students in theoretical network field with the aid of virtual laboratories is very important. Network Simulation is a modeling and testing how the network will work without being physically installed. A Virtual Private Network uses tunneling inexpensive use of bandwidth, extendable and adjustable functionality, confidentiality and protected communication among peer sites. In this study, we implement design of VPN tunnel using IPSec framework for configuring secure VPN using Packet Tracer software which enables to work as virtual network environment without using any physical devices. This paper describes as a case study on site-to-site IPSec VPN using packet tracer simulator to the effective teaching and learning of computer network course as an ideal pedagogical tool for learning computer network course effectively.

Keywords: Computer network, Internet Protocol Security, VPN, Cisco Packet Tracer, Network Simulation

1. Introduction

Due to the terms network that are become ubiquitous in common usage, the networking curriculum are raising attractive in academics and high demand for computer networking skills in among the business and industry [6]. Computer network course is described in many textbooks all over the world. Packet Tracer is virtual networking simulation software developed by Cisco Systems and broadly employ among the academic world to facilitate teaching and learning various concepts in computer networks. Packet Tracer enhancement the students creation on network architecture with an almost unrestricted number of tools, simulating operation and using this simulator testing and verifying proposed network architecture and also the learner of networking subject to have an alive study skill [5]. This pedagogical method or educational tool helps students to understand concepts of computer network or theories and improve their network practical skills. Virtual Private Network means logical connection between two communicating end system and it uses encryption along with IP-in-IP tunneling to transfers among the peer sites confidential. Many diverse forms of VPN technologies available for secure data transfer among peer sites such as Point to Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPSec), Secure Socket layer (SSL), Layer 2 Forwarding (L2F) and Generic Routing Encapsulation (GRE). Among them, IPSec was more accessible VPN technology for secure communication at network layer. IPSec tunnelled versions use two key protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP) to provide a framework for configuring secure VPN, which does not require expensive leased-line to communication any peer sites remained concealed from public outsiders [8]. Internet Protocol security (IPSec) framework provides an encrypted tunnel among the peer sites. IPSec is not only a security protocol but also offers a number of security algorithms plus require framework for among peer sites to communicate and whichever algorithms provide security appropriate for the communicating parties [1]. In this paper we are presenting the effective teaching and learning of computer network course using network simulator software as an ideal pedagogical tool for learning computer network courses effectively. For students gaining the hands-on experiences and more realize the theoretical concept of site-to-site VPN using IPSec framework for secure data transfer between private networks over the public network we simulate as case study using lightweight, user friendly network simulator software.

The remaining part of the paper is ordered in sections as: Section 2 presents the Literature Review and Computer Network Course’s Features are covered in Section 3. The implementation and configuration details of site-to-site IPSec VPN with the performance of Cisco Packet Tracer network simulator as the pedagogical tool to support the design in computer network courses as described in Section 4. Finally, in Section 5 we conclude the paper and followed by references.

2. Literature Review

A number of studies have been conducted on area of approach to challenges of learning computer network courses using cisco packet tracer network simulator and implement various case study using this simulator. Vijayalakshmi M., Padmashree Desai, Meenaxi M. Raikar, Department of Computer Science and Engineering submitted the title of ‘Packet Tracer Simulation Tool as Pedagogy to Enhance Learning of Computer Network Concepts’ in 2016[6]. In this paper,
the authors presented the a series of lab assignments are developed for students to give the visualization of network concepts applying a Cisco Packet Trace network simulator in the effective learning of computer network courses and practical exercises helped in active learning of network courses. To measure the learning concepts of network course, before using Packet Tracer tool and after using this tool the authors made assessment of open ended activity and quiz and compare the result of this survey, students learning concepts was significantly improvement.

D. E.Kurniawan, H.Arif, N. Nelmiawati, etc.Department of Informatics Engineering, Politeknik Negeri Batam, Indonesia, presented the IPSec-VPN on Cisco ASA firewall using GNS3 network simulator’ [7]. The authors analyze the network quality of VPN and non-VPN and where in the case, the employment of the IPSec-based VPN and according to the analysis, the VPN protects a Man-in-the-Middle attack and they found the weaknesses of VPN against network attacks such as Denial of Service (DoS) attack that causes the VPN server crashes and VPN client could no longer access the server.

Noor Maizura Mohamad Noor and her colleagues entitle the ‘Effectiveness of Using Cisco Packet Tracer as a Learning Tool: A Case Study of Routing Protocol’ in January 2018[5]. The authors made a questionnaire the students who took the computer network courses and students’ perceptions on using Cisco Packet Tracer network simulator. Before this survey, they created and analyzed on the research area as a case study of two network topologies using one topology use EIGRP routing protocol and another topology used RIPv2 and as comparison of these routing protocol performance metrics (round-trip time, packet loss, packet delivery ratio and throughput). According the results from questionaire, applying the PacketTracer network simulator increased the student’s practical experiences on highest rank and enhanced and improved the students’ understanding of abstract network concepts.

Sheikh Raashid Javid, Assistant-Professor at, School of Computer Engineering, RK University, Gujarat, India, submitted the title of ‘Role of Packet tracer in learning Computer Networks, in May 2014[8]. He describes the features of Packet Tracer and use the simple scenario; in which navigate the various mode of Packet tracer and what type of cables connected to a particular networking device and which port the cable should be connected. Finally, as a conclusion, he presented the challenges in computer network concepts could be effective and efficient of using Cisco Packet Tracer simulator.

3. Computer Network Course’s Features

Networking comprises the core and compulsory curriculum for both Third Year and Fifth Year students in University of Computer Studies Monywa. We have been teaching computer network courses for computer science and computer technology students. Computer network has become the important framework for the study of IT fields with the introduction of emerging technologies such as Big Data, Internet of things (IOT), Cloud computing and other associate applied science [6]. The abstract behavior of networking concepts is challenging in teaching and learning computer network course. Students learning network courses consist of numerous types of protocols applied in data communication in specialty and students will be solid to see their utility in networking curriculum [5]. Computer networking course is vast complex, involving many concepts, protocols, and technologies that are interlinked together in a complicated manner, so many computer networking concepts today that are used TCP/IP reference model, in which this model organized around the “layers” of the network architecture. With a layered architecture students can see through the complexity of computer networking—they learn about the different concepts and protocols in one part of the architecture while seeing the network diagram of how all network components fit together [3]. The OSI and TCP/IP model provides an abstract function decomposition of a network protocol and is commonly used to illustrate network functionality of each layer. Network simulator is software which simulates the network topology composed of various network devices and students using this simulator gaining the hands-on network lab experience relating the various networking design, topology, routing, switching, subnetting and secure data transfer service over public network such as VPN, etc. There are many network simulator and emulator software developed, among them common simulator and emulator software are Cisco Packet Tracer, GNS3(Graphical Network Simulator-3), Boson NetSim, VIRL, EVG-NG, Putty, Secure CRT, Microsoft Visio, PRTG (Paessler Router Traffic Grapher), etc. Among them Packet Tracer was property by Cisco System. Whereas Packet Tracer is a simulator and GNS is an emulator,neatheds to have access Cisco IOS software too. GNS3 is an open source network emulator and Packet Tracer is non-open source cross-platform visual simulation tool, students have new in the field of networking packet tracer, simulator is easier to install and function and use various network devices. For the newbies, GNS3 isbest to shift only after gaining some experience in the interim, so packet tracer simulator is suitable for networking lab to practice the students. Although GNS3 consumes the actual RAM of the device, packet tracer simulation software runs on any modern computer no limitation about processor and storage requirements and it is design for educational aid usage aspedagogical tool for network lab and it is an excellent simulator for entry-lever Cisco certification and it is the extremely lightweight, user friendly tool [9]. The critical contribution of this paper is the using this educational lightweight, user friendly simulator, students to understand the concepts of computer network or theories and improve their network practical skills and alsoemphasis on efficient and effective learning of computer network courses as a sceneryon configuration for site-to-site IPSec VPN with cisco network simulator tool.
4. Implementation and Configuration of Site-to-Site IPSec VPN

We have taught computer networking course for computer science and computer technology students. At fifth year degree level, this course is delivered over 28 periods for 14 weeks, with two hours of class get in touch per week as a one-hour practical and a one-hour lecture. We used Cisco Packet Tracer as an network simulator in our classes. With packet tracer, it is easier to teach and demonstrate complex technical concepts and the design of network systems. In our practical lab design topology (Figure 1) consists of three 1941 routers, three 2960 24 ports switches and three PC. The first task is to implement between router R1 and R3 to support a site-to-site VPN when traffic flows between peer sites securely. We employ the IPSec framework for this configuration topology. In general, tunnels are built using point-to-point connections among peer sites and the data packet passes through the tunnel are encrypted and encapsulated, so the communication between them would be secure. The encapsulation process alters the data packets that are sent to look like ordinary packets so packets sent over the public internet are unnoticed. The IPSec VPN tunnel is from router R1 to router R3 via router R2. Router R2 acts as intermediate bypass network and has no awareness of the VPN. IPSec VPN provides securely transmit the sensitive information over unsecure public networks. As the name implies IPSec protocol work at the network layer and defends and validate IP packets among the peer sites. In our simulation design consist of three routers R1, R2 and R3. As the first task, these routers have configured with the console line password adminconp@55, vty lines with adminvtyp@55and enable password adminnp@55 and then with service password encryption. For the remote access service, Secure Shell SSH account is configure with username SSHadmin and password adminssh@55. For routing between networks the link state routing protocol OSPF is used in our design topology and OSPF router ID 101 is used for this configuration [2]. To assign the IP address of an interface of PC1, PC2 and PC3, click on PC, open DESKTOP window, fill IP address, subnet mask and default gateway.

![Figure 1. Topology for site-to-site IPSec VPN tunnel](image)

4.1. Implementation of IPsec Parameters on Peer Routers R1 and R3

Initially, we need to define the interesting traffic, which is a traffic that we want to encrypt for securely transfer of our sensitive information among two sites. Packet filtering controls access to a network by analyzing the incoming and outgoing packets and accept or deny the traffic based on selected criteria such as source and destination IP address and the protocol carried within the packet. A router acts as a packet filter when it forward or deny packets according to our select filter rules. An Access Control List (ACL) is a sequential list of permit or denies statements. In this simulation, Access Control Lists ACL 110 is used to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. We want all traffic flow between private networks 172.16.1.0/24 and 172.16.3.0/24 to be encrypted. However, not all other traffic from the LAN on R2 to the Internet will pass through the VPN tunnel [7]. On router R1 to check the Security Technology package license information has enable or disable enter the show version command and if the Security Technology package has not been enabled use the license boot module c1900 technology-package securityk9 command to enable security packages. Accept the end-user license agreement, save the running-configuration file and reload the router to enable the security license. In order to check security technology package has been enabled, type the show version command again. When there is traffic between the router R1 to router R3 networks, the interesting traffic will trigger the implemented IPSec VPN and the traffic between two peers would be encapsulated and encrypted. All other traffic sourced from non-peer site will not be encrypted [2].

R1(config)# access-list 110 permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255

The security strategy implemented in router R1, encrypts the Internet Key Exchange (IKE) version 1 protocol with AES-256 for encryption and pre-shared key with vnp@55 and group 5 for authentication. Create group-policy tunnel security with ISAKMP policy 10 for router R1 to combine the authentication and
encryption, a crypto map entry is created to set up the security associations. Enter the following commands on router R1 to configure these parameters.

R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2.
R1(config)# crypto ipsec transform-set VPN-SET esp-aesesp-sha-hmac

Identify an ipsec-isakmp using sequence number 10 and configure the crypto map on the outgoing interface and bind the VPN-MAP crypto map to the outgoing Serial 0/0/0 interface.

R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
R1(config)# interface s0/0/0

Before the interesting traffic passing through tunnel, issues the show crypto ipsecsa command on peer router R1 to verify whether the IPSec VPN tunnel is properly implement or not.

R1# show crypto ipsecsa

As can be see the number of packets encapsulated, encrypted, decapsulated, and decrypted has more than zero (Figure 3), which indicates that the IPsec VPN tunnel is working properly and the traffic between peer sites were secure.

Create uninteresting traffic which is R2 network from R1 network, ping PC2 from PC1 (Figure 4).

On the destination router R1, type the show crypto ipsecsa command and check output. The number of encapsulated, encrypted, decapsulated, and decrypted packets has not changed which indicates that uninteresting traffic is not encrypted (Figure 5).
As a result, by simulating VPN tunnel with IPsec framework we can see that IPsec protocol protects and authenticates the transfer traffic among peer sites over insecure channel such as Internet.

5. Conclusion

Cisco Packet Tracer is all-inclusive, lightweight user friendly education tool with innovative features that assist students, who have new in the field of network learning in computer courses with efficiently and effectively. Nowadays, we need a cost effective technique that provides for a secure data transfer between the communication parties over public network such as internet that can be achieved by using Virtual Private Network using IPsec framework. Site-to-Site IPsec VPN tunnel provides the all enterprise network privacy issues and valuable services without disturbing the communication service. The critical contribution of this paper is the using pedagogical network simulator, students to understand the concepts of computer network or theories and improve their hands-on network configuration skills. Because of network devices are expensive, before implementing on the real world network, using lightweight user friendly network simulator, students can get the hands-on experience, so as a scenario for configuration of site-to-site IPsec VPN. It also illustrates the step-by-step instruction for the implementation and simulation of VPN gateway routers at VPN tunnel and information through the tunnel are encrypted and encapsulated and on non-VPN tunnel, the communication of two parties cannot get this effect. Because of the cost and the chances of causing damage to the real equipment, packet tracer is cost effective tool, which gives a feeling, as if a student is working to reality. This network simulator is a lightweight, easy and user friendly tool, use various network devices on this simulator and understand abstract concepts of network courses and students can achieve their own innovative network design and project using this simulator and this good practice skill support for their working environment.

Acknowledgement

I would like to acknowledge to Prof; Dr Soe Soe Khaing, Rector, University of Computer Studies, Monywa for her encouragement, valuable comments, guidance, suggestions and her permission to do this research paper.

References