Comprehensive Journal of Science
Volume (10), Issue (38), (Dec, 2025)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) العدد 38 ديسمبر 2025
ردمد: 3014-6266

Designing and Simulation a Secure Network Using Multiple Security Technologies: Port Security, DHCP Snooping, ACL, SSH and Data Protection

Type of the Paper (Applied Scientific Study)

Warda Shafter1, Nuredin Ahmed2

1Departme0nt of Information Technology, Libya Academy for Graduate Studies, Tripoli, Libya 2Department of Computer Engineering, University of Tripoli, Tripoli, Libya

wrdhshftr@gmail.com

تاريخ الاستلام:2025/12/7 –تاريخ المراجعة: 2025/12/11– تاريخ القبول: 2025/12/18– تاريخ للنشر : 2025 /12/24

Abstract

The university network has also become vulnerable to potential threats due to the increase in the numbers of devices and services being connected. The following report describes the creation and simulation of a secure university network using Cisco Packet Tracer. The network incorporates the use of VLAN segregation, Port Security, DHCP Snooping, Access Control Lists, and SSH for secure management. The results demonstrate the network's connectivity, isolation, and stability for use in academic settings, as stated in [1], [2].

Keywords

University Network, Network Security, Cisco Packet Tracer, VLAN, DHCP Snooping, Access Control Lists, SSH.

Introduction

As the growth of corporate and campus networks continues unabated, securing, authenticating, and managing have become the necessity of the day. Next-generation networks have to enable secure communications and safeguard confidential data from threats within and outside network communications, including unauthorized devices, rogue DHCP servers, and unencrypted management communications. [1].

The purpose behind this project is the design and implementation of a secured network over Cisco Packet Tracer, following a multi-layered secured approach that encompasses VLAN segmentation, inter-VLAN routing, traffic management, and Device level secured methods. The outcome verifies that industry-accepted methods for secured design implementations can be applied efficiently in a simulated environment that is very close to real-life implementations.

Related Work

Some research has focused on the secure campus network design involving the use of Cisco Packet Tracer. The secure campus network simulation has been done effectively by utilizing the concept of VLANs and ACLs as depicted in [1]. Some research has also pointed out the efficacy of Packet Tracer as a learning and verification tool as discussed in [2]. Some work has been done that involves protocol level security, protecting the DHCP protocol, and utilization of the concept of VLANs as discussed in [3]– [5].

Methodology

The specific project employs a design-based experimental methodology to design, implement, and validate a secure network, using Cisco Packet Tracer. It includes the network design with VLAN segmentation and structured IP addressing, followed by sequential device configuration with inter-VLAN routing and core services deployment, then Layered security mechanisms will be implemented. Verification was performed to test connectivity, services, and security, and the evaluation at the end targeted at network stability, security effectiveness, and service availability under normal conditions of operation.

Simulation Setup

The section describes the simulation environment and the network components configured in Cisco Packet Tracer to implement and evaluate the secure network design.

Table 1. Simulation Environment Specifications

Parameter	Parameter	Purpose
Router	Cisco 2911 with dual interfaces (192.168.1.1 / 192.168.2.1)	Enables inter-VLAN routing and enforces ACL-based traffic control
Switches	Two Cisco 2960 switches	Provide VLAN-based access switching for different departments
End Devices	PCs assigned via DHCP in LAN 1 and LAN 2	Simulate end-user connectivity in separate network segments
Server	PT-Server with IP 192.168.2.10	Hosts DHCP, DNS, HTTP, and FTP services
Network Segments	LAN 1 (192.168.1.0/24) and LAN 2 (192.168.2.0/24)	Logical separation of departments using VLANs
Network Segments	Cisco Packet Tracer 8.2.2	Used for network design, configuration, and validation

Research phases

Phase 1: Analysis and Planning

This phase involved analyzing project requirements to determine network objectives such as security, segmentation, service availability, and performance requirements. The network topology, VLAN design, IP configuration, and security policies had to be carefully planned based on this analysis in order to achieve scalability, reliability, and conformance to standards in business networking.

Phase 2: Simulation Implementation

In this stage, the design of the planned network was established using Cisco Packet Tracer. Devices within the network, including routers, switches, servers, and user devices, were set up one by one. VLAN isolation, inter VLAN routing, core functions, and multilayer security were established per design criteria.

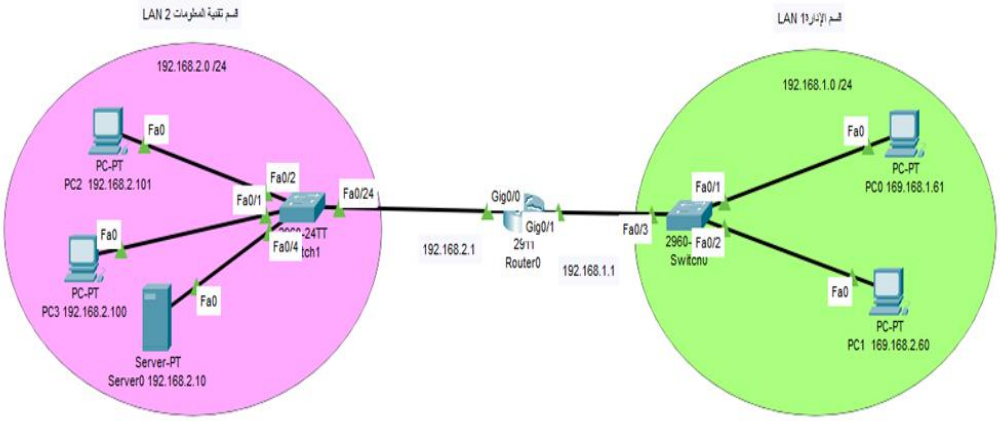

Figure 1. Logical topology of the proposed secure university network

Private IP (192.168.0.0/16) assigns two subnets with a subnet mask of /24. The terminal devices get their IPs from a DHCP server. The IPs are routed in order to help in communications between VLANs.

Table.2 Design Section Components

Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN
Router0	**Gig0/0**	**192.168.2.1**	**255.255.255.0**	**N/A**	**2**
Router0	**Gig0/1**	**192.168.1.1**	**255.255.255.0**	**N/A**	**1**

PC0	**Fa0**	**192.168.1.61**	**255.255.255.0**	**192.168.1.1**	**1**
PC1	**Fa0**	**192.168.1.60**	**255.255.255.0**	**192.168.1.1**	**1**
PC2	**Fa0**	**192.168.2.101**	**255.255.255.0**	**192.168.2.1**	**2**
PC3	**Fa0**	**192.168.2.100**	**255.255.255.0**	**192.168.2.1**	**2**

Table 3. IP addressing plan for university departments

VLAN	Subnet	Mask	Default Gateway	Usable Range	Broadcast
VLA1	192.168.1.0	24/	192.168.1.1	192.168.1.2 – 192.168.1.254	192.168.1.255
VLA2	192.168.2.0	24/	192.168.2.1	192.168.2.2 – 192.168.2.254	192.168.2.255

Phase 3: Testing and Evaluation

This phase entailed testing the network after its implementation. This was performed in a systematic approach employing network test commands. The network was tested in regard to its connectivity, functionality, security, as

Connectivity

Network connectivity is responsible for ensuring network performance and network stability. Network connectivity enables communications among various devices spread across different VLANs. Network connectivity is achieved using a well-organized IP allocation system, which includes dynamic IP allocation performed by the router and the DHCP server. A Cisco 2911 router connects LAN 1 and LAN 2 via inter-VLAN routing, and Access Control Lists are used for security purposes. Access Control Lists enable secure data transfer and hence achieve a secure university network.

The table reflects successful connectivity between the device and the server over the two subnets with no packet loss, thereby indicating appropriate communication and further showing the efficacy of the network configuration.

Table4. Successful ping replies between LAN1 and LAN2

Parameter	Result
Source Device	PC2 (192.168.2.101)
Destination Device	Server0 (192.168.2.10)
Packet Size	32 bytes
Packets Sent	4
Packets Received	4
Packet Loss	0%
Maximum Delay	10 ms
Average Delay	5 ms

6. VLAN Configuration

VLANs logically separate departments to reduce broadcast traffic and enhance security. IEEE 802.1Q trunking enables VLAN tagging between switches and the router [5].

The table shows that all configured VLANs are active, meaning VLANs have been successfully configured and will be ready to forward network traffic.

Table.5. VLAN Configuration and Status Display on Router

VLAN	VLAN Name	Status
1	default	Active
1002	fddi-default	Active
1003	token-ring-default	Active
1004	fddinet-default	Active
1005	trnet-default	Active

7. Network Security

The set of security features includes Port Security, DHCP Snooping, IP Source Guard, ACLs, and device management by SSH. This is a defense in depth approach to network security.

From the above table, it is confirmed that all the implemented security measures have been configured successfully.

Table6 .Validation Results of Implemented Network Security Mechanisms

Security Mechanism	Configuration Description	Validation Method	Result
HTTP Service	HTTP service enabled on Server0 to provide web access	Browser access test	Successful
HTTPS Service	HTTPS enabled to ensure secure web communication	Secure browser connection	Successful
FTP Service	FTP service enabled with authenticated user access	FTP login and file access test	Successful
Access Control Lists (ACLs)	Extended ACL applied to restrict unauthorized access between VLANs	show ip access-lists command	Successful
DHCP Snooping	DHCP Snooping enabled on switches to prevent rogue DHCP servers	show ip dhcp snooping database	Successful
Secure Device Management	Router and switch configurations verified via CLI	show running-config	Successful

8.Results

The proposed project designed and implemented an efficient and secure network using Cisco Packet Tracer that included all the major security features such as Port Security, DHCP Snooping, IP Source Guard, ACLs, and SSH. The proposed network handled the flow of traffic effectively through VLANs with effective security for external as well as internal communications.

9. Discussion

The outcome of this task reveals that the network security solution implemented was able to provide a secure connection, segmented the network using VLANs, controlled access, as well as ensured regulated communication between various departments through inter-VLAN routing using ACLs. Security measures such as DHCP Snooping, IP Source Guard, and SSH ensured security of the network from various network attacks without slowing down network performance. This exercise tends to prove that Cisco Packet Tracer is an efficient network simulation software.

10. Conclusion

The proposed network design proves that secure, scalable university networks can be effectively designed and validated using Cisco Packet Tracer. Dynamic routing and redundancy mechanisms are one of the enhancements to be made in the near future.

11.References

[1] A. H. Ahmed and M. N. A. Al-Hamadani, "Designing a Secure Campus Network and Simulating it Using Cisco Packet Tracer."

[2] N. M. M. Noor, N. Yayao, and S. Sulaiman, "Effectiveness of Using Cisco Packet Tracer as a Learning Tool: A Case Study of Routing Protocols."

[3] T. Murkomen, "Performance, Privacy, and Security Issues of TCP/IP at the Application Layer: A Comprehensive Survey."

[4] D. A. Pradana and A. S. Budiman, "The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from Rogue Attack."

[5] T. Rahman and Q. Aprianto, "Implementation of VLAN and ACL for Network Security at SDIT Ibnu Hajar Bekasi."