Design, Simulation, and Performance Evaluation of A Secure, Segmented Multi-Subnet Network Infrastructure with Centralized Services for Educational Computer Engineering Workstation

Art Julian Abrera., David James Delgado., Kiervin Guillena., Kristine Anne R. Laput., Abegail P. Ramirez., Mark Daniel Tomale., Engr. Minerva C. Zoleta

Computer Engineering Department, Eulogio "Amang" Rodriguez Institute of Science and Technology, Nagtahan Street, Sampaloc, Manila, 1008, Philippines

DOI: https://doi.org/10.51244/IJRSI.2026.1306000319

Received: 21 June 2026; Accepted: 26 June 2026; Published: 09 July 2026

ABSTRACT

This study presents the design and simulation of a Computer Engineering Laboratory Network intended to provide reliable communication, centralized resource management, secure access control, and efficient network administration within an educational laboratory environment. The proposed network was developed using Cisco Packet Tracer and incorporates a hierarchical tree topology, logical subnetting, Virtual Local Area Networks (VLANs), static routing, Domain Name System (DNS) services, file-sharing services, and Access Control Lists (ACLs). The network architecture consists of forty (40) workstation computers, one (1) instructor workstation, centralized DNS and file servers, four (4) network printers, a guest wireless network, five (5) Cisco 2960 switches, and two (2) Cisco 2911 routers. Workstations were organized into separate subnet groups to improve traffic management and network scalability, while VLAN segmentation and ACL implementation enhanced security by restricting unauthorized access to critical resources. Simulation-based testing was conducted to evaluate connectivity, routing performance, DNS resolution, file-sharing functionality, and security controls. Results demonstrated successful inter-subnet communication, reliable static routing, effective DNS hostname resolution, operational file-sharing services, and secure isolation of guest wireless users from internal laboratory resources. ICMP and traceroute tests confirmed stable network performance with minimal packet loss and successful end-to-end connectivity across all network segments. The findings indicate that the proposed network design provides a scalable, secure, and manageable laboratory infrastructure capable of supporting instructional, administrative, and student computing requirements. The study demonstrates the effectiveness of integrating hierarchical network design, network segmentation, centralized services, and access control mechanisms in developing a modern Computer Engineering laboratory network.

Keywords: Laboratory Network, Cisco Packet Tracer, Hierarchical Network Design, Network Security, DNS Server, File Sharing, Access Control Lists (ACLs), Static Routing

INTRODUCTION

Technology has become a relevant part of education, especially in programs that require hands-on learning. Computer laboratories provide students with an environment where they can perform programming tasks, network simulations, system development, and other practical activities. To support these activities effectively, a reliable and well-organized computer network is necessary.

A computer network allows multiple devices to communicate, share resources, access the internet, and utilize centralized services such as file storage and printing. In educational laboratories, network reliability is important because interruptions in connectivity can affect learning, laboratory exercises, and overall productivity. As the number of users and devices continues to increase, laboratories require network infrastructures that are secure, scalable, and easy to manage.

Despite the importance of computer networks, many laboratory environments still experience challenges such as unstable connections, network congestion, and difficulties in managing resources and user access. These

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

issues can lead to delays in laboratory activities and reduce the efficiency of both students and instructors. Therefore, proper network planning and design are essential to ensure smooth and reliable operation.

This study focuses on the design of a Computer Engineering Laboratory Network that aims to provide stable communication, efficient resource sharing, and improved network management. Using Cisco Packet Tracer as a simulation tool, the proposed network incorporates structured topology, network segmentation, routing, and security mechanisms to support the needs of students, instructors, and laboratory administrators. The study seeks to develop a network design that can serve as a model for creating a reliable and scalable laboratory environment for educational institutions.

REVIEW OF RELEVANT STUDIES AND THEORIES

Theoretical Framework

This study is grounded in the principles of Systems Theory, Hierarchical Network Design, Network Segmentation, and the Open Systems Interconnection (OSI) Reference Model, which collectively provide a comprehensive theoretical foundation for the design and optimization of a reliable, scalable, and secure Computer Network System (CNS) in a computer laboratory environment. These frameworks are widely adopted in contemporary network engineering research as they explain how architectural structure, logical segmentation, and layered communication collectively influence network performance, fault tolerance, and manageability in multi-user computing environments.

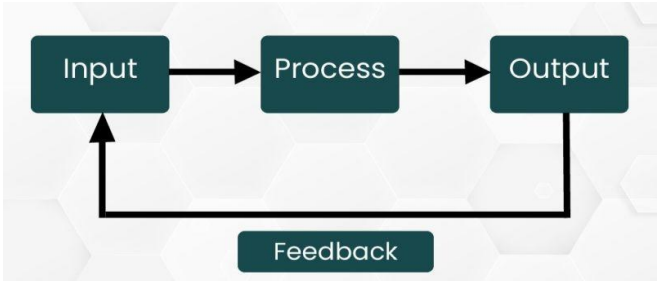

Figure 1. System Theory Model

Systems Theory conceptualizes a computer network as an integrated and interdependent system wherein overall performance is determined by the interaction of all constituent components. Within the context of this study, it justifies the holistic integration of routers, switches, servers, workstations, and peripheral devices into a unified operational system. This perspective emphasizes that network performance degradation or instability cannot be attributed to isolated components alone but rather to the dynamics of the entire system. Accordingly, the proposed design adopts a system-wide optimization approach to mitigate cascading failures and reduce workstation disconnections.

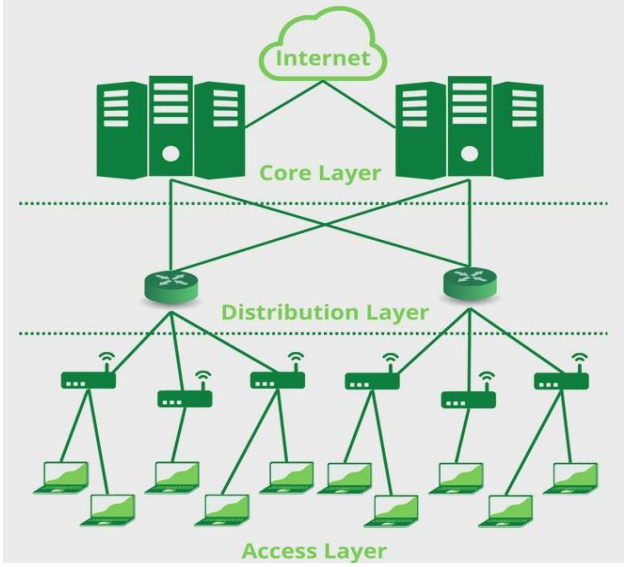

Figure 2. Hierarchical Network Design

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Hierarchical Network Design provides the structural model for organizing network infrastructure into functionally distinct layers to improve scalability, performance, and fault isolation. This study implements a Two-Tier (Collapsed Core) architecture, wherein the Core and Distribution layers are consolidated into a single Core/Distribution switch, while the Access Layer consists of Access Switch 1, Access Switch 2, and a Wireless Access Point. This hierarchical arrangement enhances traffic aggregation efficiency, reduces network complexity, and ensures that localized faults at the access level do not propagate throughout the entire laboratory network.

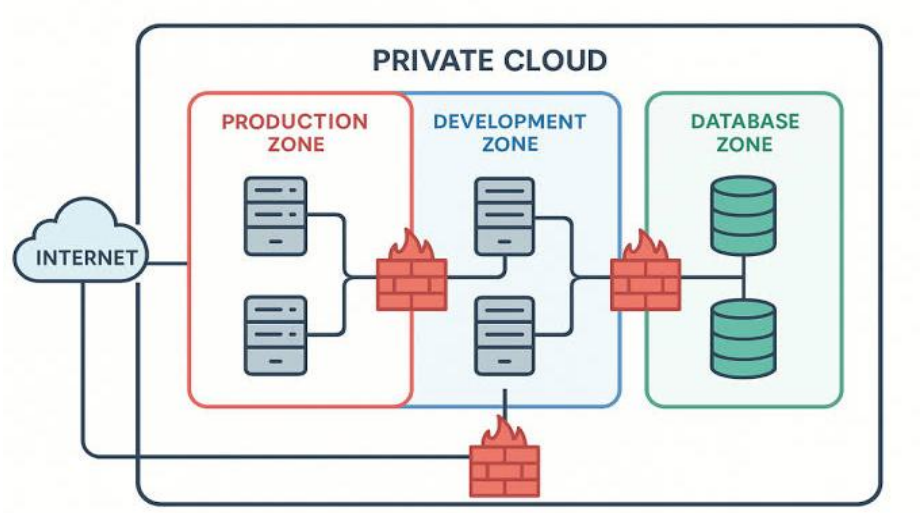

Figure 3. Network Segmentation

Network Segmentation further strengthens the proposed design by dividing the network into smaller, logically isolated subnets using Virtual Local Area Networks (VLANs). This study applies segmentation to separate traffic among workstation clusters, server resources, instructor systems, printer services, and guest wireless access. By confining broadcast domains and isolating network traffic, segmentation significantly reduces congestion, enhances security posture, and improves overall network stability by ensuring that performance issues within one segment do not adversely affect others.

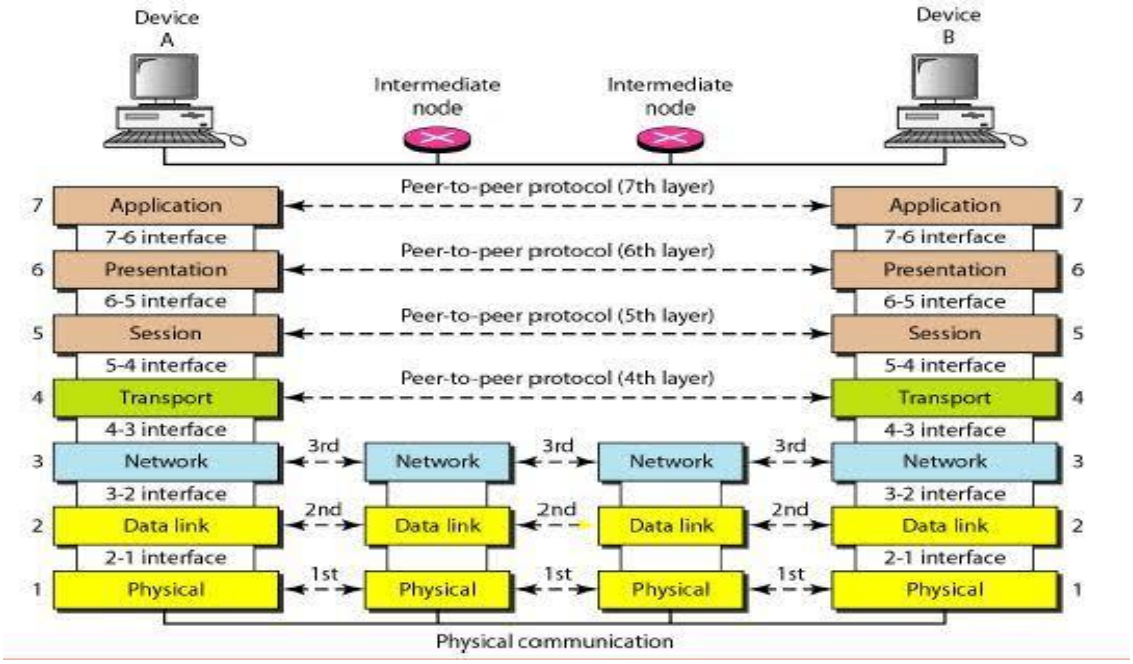

Figure 4. OSI Model

The Open Systems Interconnection (OSI) Reference Model serves as the standardized conceptual framework for understanding and implementing communication processes across network layers. In the proposed

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

architecture, Layer 2 (Data Link Layer) governs switching operations and VLAN implementation at the access layer, enabling efficient local frame forwarding. Layer 3 (Network Layer) facilitates logical IP addressing and inter-VLAN routing at the Core/Distribution switch, while the router/firewall operates as the network boundary, controlling external connectivity and enforcing security policies. This layered abstraction ensures interoperability, modular design, and systematic troubleshooting capability.

Collectively, these theoretical foundations establish a robust engineering basis for the proposed network architecture. Their integrated application enables the development of a structured, fault-tolerant, and scalable laboratory network system that enhances operational efficiency, minimizes downtime, and addresses common connectivity instability issues in educational computer laboratory environments.

RELATED LITERATURE

Computer Laboratory Network has a significant role in educational institutions, where students usually perform practical activities using computers. This network design provides a foundation for communication, file sharing and collaboration among users within the laboratory environment. As the number of connected devices and users continues to increase, educational institutions face challenges related to network management, security, monitoring, and resource sharing. These challenges have encouraged researchers to develop solutions that improve laboratory operations while maintaining secure and efficient communication among network devices.

According to Zapanta, Talirongan, and Talirongan (2021), computer laboratories require effective access control and monitoring mechanisms to ensure the security and proper utilization of laboratory resources. Their study developed an access control and monitoring system that regulated user access and monitored laboratory activities. The researchers found that centralized monitoring improved laboratory management by reducing unauthorized access and providing administrators with better visibility of laboratory operations. Their findings highlight the importance of monitoring systems in maintaining an organized and secure computing environment. This is particularly relevant to educational laboratories where instructors need to supervise student activities while ensuring that network resources are properly utilized.

The need for centralized management is further supported by Ngoie (2021), who proposed a server implementation model for the management of computer laboratories. The study demonstrated that centralized servers improve operational efficiency by providing shared resources, simplifying administration, and strengthening security management. Through centralized services, multiple users can access common resources while administrators maintain control over resource allocation and system configurations. The findings suggest that server-based management remains a critical component of modern laboratory environments, especially when supporting large numbers of users and devices.

In addition to centralized administration, effective communication between instructors and students is an important requirement in laboratory-based learning. Putra et al. (2023) developed a Local Area Network integrated with NetSupport software to support teaching and learning activities in a computer laboratory. Using the Network Development Life Cycle methodology, the researchers designed and evaluated a network capable of supporting classroom monitoring and management. Their results showed that the proposed network achieved high levels of validity, practicality, and effectiveness. Furthermore, the study demonstrated that instructors were able to monitor and assist students more efficiently through centralized supervision tools. These findings indicate that combining network infrastructure with monitoring software can significantly enhance the learning experience within computer laboratories.

As educational networks continue to expand, network segmentation has become an important strategy for improving both performance and security. Suhartanto and Putri (2024) designed a computer laboratory network topology that separated student and teacher users into different network segments. Their study found that segmentation improved network performance by reducing unnecessary traffic while simultaneously enhancing security through the isolation of user groups. The researchers concluded that segmented network architectures provide better control over resource access and simplify network administration. These findings support the implementation of subnet-based laboratory networks where different groups of users require

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

different levels of access and privileges.

The reviewed studies collectively demonstrate that modern computer laboratory networks require the integration of centralized monitoring, server-based resource management, secure network segmentation, and effective access control mechanisms. Previous researchers have shown that monitoring systems improve supervision, centralized servers enhance resource management, VLANs strengthen network organization, and ACLs improve security. However, most existing studies focus on specific aspects of laboratory management individually. Limited research has integrated centralized monitoring, DNS services, file-sharing servers, VLAN segmentation, inter-VLAN communication, static routing, ACL-based security, and hierarchical network topology into a single Computer Engineering laboratory network architecture. Therefore, the present study seeks to address this gap by proposing a comprehensive laboratory network design that combines these technologies to provide secure, efficient, and manageable communication among forty workstation computers, instructor workstations, servers, and other network devices within a simulated Cisco Packet Tracer environment.

METHODOLOGY

A. Research Design

This empirical study utilizes simulation-based engineering research involving structural network modeling, architecture prototyping, and algorithm simulation test methodologies. Given the high investment, operational cost, and structural risk incurred by actual enterprise multi-subnets, the virtual test bed offers the capability to assess connectivity viability, protocol convergence, and constraint boundaries for structure data within a restricted and controlled test environment.

a. Requirements analysis and topology mapping

mapping the structural boundaries of forty (40) distributed desktop workstations, supervisory instructors' screens, networked equipment devices, and centrally located elements like Domain Name System servers and File Sharing servers into segregated broadcast areas. Used Classless Inter-Domain Routing to define IP addressing math that ensures fullIPv4 Address Space reuse, whilst maintaining restricted broadcast presence.

b. Virtual Prototyping and Deployment

Built a multi-tier, branched topology structure via a Cisco Packet Tracer discrete event simulation model, which included manual configuring and implementation of L2 switches(Virtual LAN database isolation, 802.1Q trunk allocation); and L3 devices (inter-VLAN routing utilizing sub-interface/static IP routed convergence standard routing)

c. Empirical Verification and Traffic Tracing

Sent over Internet Control Message Protocol (ICMP)payloads over router boundaries to collect real-time experimental data from the network. The packet analysis will demonstrate network protocol handshakes(Dynamic Host Configuration Protocol (DHCP)lease acquisition, and DNS requests and responses) and report: packet success rate; round trip times; routing convergence under Static IP routes.

B. Laboratory Network Requirements

The laboratory network requirements consist of forty (40) workstation computers, one (1) instructor computer, one (1) DNS server, one (1) file server, two (2) Cisco 2911 routers, and five (5) Cisco 2960 switches. The network is designed to provide communication between all devices, allow file sharing, support domain name resolution, and enable centralized monitoring by the instructor.

C. Proposed Physical Topology

The proposed physical topology follows a hierarchical tree topology. Four access switches are connected to workstation groups, while a central switch serves as the core network device. Two routers connect different

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

network segments and provide routing services between subnets.

D. Proposed Logical Topology

The logical topology divides the network into multiple subnets to improve traffic management and network performance. Router0 manages the 192.168.10.0/24 and 192.168.20.0/24 networks, while Router1 manages the 192.168.30.0/24 and 192.168.40.0/24 networks. The instructor computer and servers operate within the 192.168.60.0/24 network. Static routing is configured between the routers to allow communication among all subnets.

Network Segment	Network Address	Default Gateway	Subnet Mask
PC0 – PC9	192.168.10.0/24	192.168.10.1	255.255.255.0
PC10 – PC19	192.168.20.0/24	192.168.20.1	255.255.255.0
PC20 – PC29	192.168.30.0/24	192.168.30.1	255.255.255.0
PC30 – PC39	192.168.40.0/24	192.168.40.1	255.255.255.0
Instructor and Servers	192.168.60.0/24	192.168.60.2	255.255.255.0
Printer0	192.168.10.20/24	192.168.10.1	255.255.255.0
Printer1	192.168.20.20/24	192.168.20.1	255.255.255.0
Printer2	192.168.30.20/24	192.168.30.1	255.255.255.0
Printer3	192.168.40.20/24	192.168.40.1	255.255.255.0
Wireless Access Point	DHCP	DHCP	DHCP

Table 1. VLAN and IP Addressing Scheme

E. Hardware and Software Requirements

Hardware Requirements

- 2 Cisco 2911 Routers
- 5 Cisco 2960-24TT Switches
- 40 Workstation Computers
- 4 Printers
- 1 WAP (Wireless Access Point) Guest Network
- 1 Instructor Computer
- 1 DNS Server
- 1 File Server
- Copper Straight-Through Cables

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Software Requirements

- Cisco Packet Tracer
- Windows Operating System
- TCP/IP Protocol Suite
- DNS Service
- FTP/File Sharing Service

F. Security and Access Control Design

Network Segmentation via Virtual LANs (VLANs)

The main isolation method that we implement on the network is VLANs. We have broken the workstations into different subnets in either physical rows or in functional groups (Subnets 10.0, 20.0, 30.0, and 40.0). We have created a specific VLAN 30 (Guest_WiFi), which will be segregated at the layer 2 level from the rest of the workstations at the access switches. This ensures that any untrusted wireless traffic coming into the network via a WAP will be trunked into its own broadcast domain, which will not allow the guest user to locally or broadcast to sniff and discover our internal workstations and servers.

Layer 3 Access Control List (ACL)

To govern inter-subnet traffic flow across the logical topology, standard and extended Access Control Lists (ACLs) are deployed at the default gateway boundaries on Router0 and Router1. These packet-filtering rules enforce strict directional containment:

a. Server Infrastructure Protection

Within the core network block (192.168.60.0/24) are our File server, Instructor PC, and the DNS server, and access to these machines for administrative setup purposes has been restricted with filtering rules that only allow the Instructor PC to configure them by its Mac address or IP address.

b. Guest Network Containment

An ACL applied to the outbound interface of the Guest WiFi gateway blocks all inbound traffic directed toward internal subnets (192.168.10.0 through 192.168.40.0), allowing guest devices to communicate exclusively with the DNS server for external web translation and routing to the external WAN.

G. Testing and Evaluation Procedure

The testing procedures are evaluated through simulation in Cisco Packet Tracer. Testing procedures included verifying IP addressing configurations, checking router and switch connectivity, validating static routing tables, and performing end-to-end ping tests between the instructor computer and all workstation computers and other devices. In addition, the tests were conducted to confirm DNS functionality and file transfer operations through the file server. Successful communication among all devices indicated that the network design met the intended laboratory requirements.

RESULTS AND DISCUSSION

A. Simulation-Based Network Design Using Cisco Packet Tracer

The proposed Computer Engineering Laboratory Network was developed and evaluated using Cisco Packet Tracer as a simulation platform. The virtual prototype consisted of forty workstation computers, one instructor

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

computer, one DNS server, one file server, four printers, one wireless access point, five Cisco 2960 switches, and two Cisco 2911 routers.

The simulation environment enabled the configuration and testing of IP addressing, routing, network services, and device connectivity without requiring physical deployment. Figure 1 presents the complete simulated network used for testing and evaluation.

The results confirmed that the proposed LAN design successfully supports workstation communication, file sharing, DNS resolution, printer access, guest wireless connectivity, and instructor supervision. Furthermore, the simulation provided a practical and cost-effective environment for validating the network architecture, identifying configuration issues, and evaluating network functionality prior to actual implementation. Therefore, the Cisco Packet Tracer model served as the experimental platform for assessing the topology, subnetting, routing, services, and security mechanisms of the proposed laboratory network.

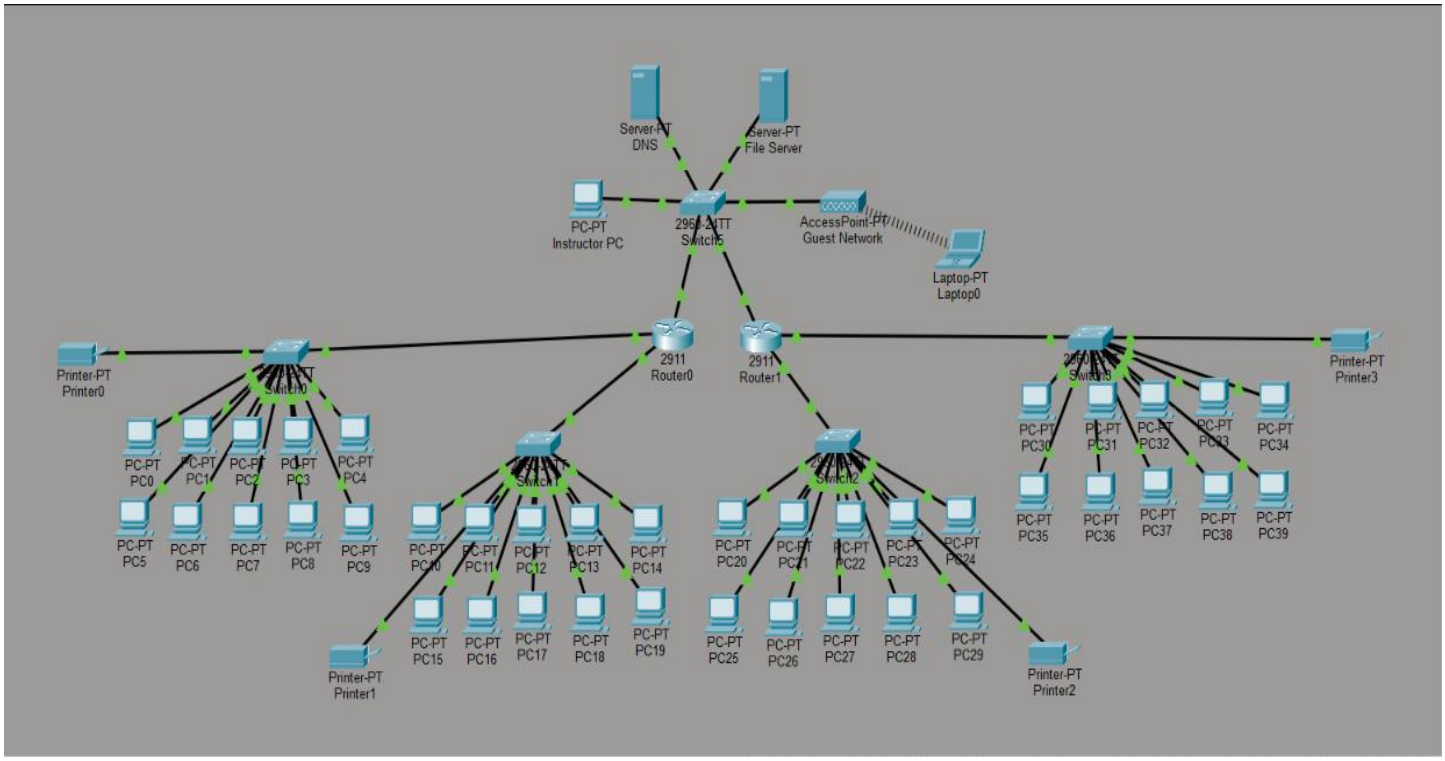

Figure 5. Cisco Packet Tracer simulation model of the proposed laboratory LAN

B. Simulated Hierarchical Tree Topology of the Laboratory Network

The proposed laboratory LAN utilized a hierarchical tree topology, where forty workstation computers were divided into four groups and connected to four access switches. These access switches were linked to a central switch that served as the network aggregation point, while two Cisco 2911 routers provided routing services between network segments. As shown in Figure 1, the topology consisted of access-level and core-level components, enabling communication among workstation groups, servers, printers, and the instructor computer.

The hierarchical design improved network organization, manageability, and scalability by grouping devices according to their functions. Compared to a flat network architecture, this structure simplified configuration, troubleshooting, and future expansion while maintaining efficient inter-subnet communication. Therefore, the topology is well-suited for a Computer Engineering Laboratory as it supports structured administration, traffic management, and network growth.

C. Laboratory Network Design

The simulated laboratory network successfully integrated all required devices and services, including forty

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

workstation computers, one instructor computer, one DNS server, one file server, four printers, one wireless access point, five Cisco 2960 switches, and two Cisco 2911 routers. Each device was configured according to its intended function, with workstations supporting student activities, servers providing centralized services, printers enabling shared printing, and routers facilitating inter-subnet communication.

Network Component	Quantity	Device/Model Used	Purpose in the Simulated LAN
Workstation computers	40	PC-PT	Serve as student computers for laboratory activities, file access, communication testing, and network connectivity verification.
Instructor computer	1	PC-PT	Serves as the supervisory workstation for instructor-centered monitoring and administrative access to selected network resources.
DNS server	1	Server-PT	Provides domain name resolution service for the simulated laboratory network.
File server	1	Server-PT	Provides centralized file storage and file sharing for authorized users in the laboratory network.
Routers	2	Cisco 2911	Provide Layer 3 routing services between different subnets and support static routing across the simulated network.
Switches	5	Cisco 2960-24TT	Provide wired connectivity for workstation groups and serve as access/core switching devices in the hierarchical tree topology.
Printers	4	Printer-PT	Provide shared printing resources for workstation groups within the laboratory network.
Wireless access point	1	AccessPoint-PT	Provides guest wireless connectivity while supporting separation from internal laboratory resources.
Network cabling	As required	Copper straight-through cables	Connects PCs, switches, routers, servers, printers, and other wired network devices in the simulation.
Simulation software	1	Cisco Packet Tracer	Serves as the virtual environment for network modeling, configuration, testing, and packet tracing.

Table 2. Laboratory network device requirements used in the simulation

The design addressed the essential operational requirements of a Computer Engineering Laboratory by supporting file sharing, name resolution, printing services, instructor supervision, and controlled guest access. Furthermore, the structured distribution of devices improved network administration, troubleshooting, and maintenance by organizing workstations into manageable groups, centralizing services, and isolating guest wireless traffic from internal network resources.

D. Logical Subnetting and IP Addressing Scheme

The logical topology divided the laboratory network into multiple IPv4 subnets. The first workstation group, consisting of PC0 to PC9, was assigned to the 192.168.10.0/24 network with the default gateway 192.168.10.1. The second group, consisting of PC10 to PC19, was assigned to the 192.168.20.0/24 network with the default

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

gateway 192.168.20.1. The third group, consisting of PC20 to PC29, was assigned to the 192.168.30.0/24 network with the default gateway 192.168.30.1. The fourth group, consisting of PC30 to PC39, was assigned to the 192.168.40.0/24 network with the default gateway 192.168.40.1. The instructor PC and server resources were assigned to the 192.168.60.0/24 network.

The IP addressing scheme allowed each workstation group to operate within its own network segment. Printers were also assigned IP addresses within their corresponding workstation networks. This structure provided a clear addressing plan for device identification, gateway assignment, and inter-subnet routing. The use of separate subnets also allowed the researchers to test communication across router boundaries and evaluate whether traffic could be forwarded properly between different network segments.

Network Segment / Device Group	**Assigned Devices**	**Network Address**	**Default Gateway**	**Subnet Mask**	**Purpose**
Workstation Group 1	PC0-PC9	192.168.10.0/24	192.168.10.1	255.255.255.0	Provides network connectivity for the first group of student workstations.
Workstation Group 2	PC10-PC19	192.168.20.0/24	192.168.20.1	255.255.255.0	Provides network connectivity for the second group of student workstations.
Workstation Group 3	PC20-PC29	192.168.30.0/24	192.168.30.1	255.255.255.0	Provides network connectivity for the third group of student workstations.
Workstation Group 4	PC30-PC39	192.168.40.0/24	192.168.40.1	255.255.255.0	Provides network connectivity for the fourth group of student workstations.
Instructor and Server Segment	Instructor PC, DNS Server, File Server	192.168.60.0/24	192.168.60.2	255.255.255.0	Provides a separate network segment for instructor supervision and centralized network services.
Printer 0	Printer0	192.168.10.20/24	192.168.10.1	255.255.255.0	Provides printing service for devices in the first workstation network.
Printer 1	Printer1	192.168.20.20/24	192.168.20.1	255.255.255.0	Provides printing service for devices in the second workstation network.
Printer 2	Printer2	192.168.30.20/24	192.168.30.1	255.255.255.0	Provides printing service for devices in the third workstation network.
Printer 3	Printer3	192.168.40.20/24	192.168.40.1	255.255.255.0	Provides printing service for devices in the fourth workstation network.
Guest Wireless Network	Wireless Access Point / Guest Client	DHCP-assigned	DHCP-assigned	DHCP-assigned	Provides guest wireless connectivity through dynamic IP assignment.

Table 3. IP Addressing Scheme and Subnet Allocation of the Simulated Laboratory Network

The use of multiple subnets improved the logical organization of the laboratory LAN. By separating workstation groups into different IP networks, the design avoided placing all devices in one large undifferentiated broadcast domain. This makes the network easier to manage because each group of workstations can be identified based on its assigned subnet.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

The separate instructor and server subnet also supports better administrative control. Since the instructor computer, DNS server, and file server are placed in a dedicated network, access to these devices can be controlled more effectively using routing rules and access control policies. This design is more appropriate than a flat network because it provides a foundation for traffic filtering, service protection, and structured network monitoring.

E. Static Routing Between Router0 and Router1

Static routing was configured to enable communication among the separated laboratory network segments. Router0 managed the 192.168.10.0/24 and 192.168.20.0/24 workstation networks, while Router1 managed the 192.168.30.0/24 and 192.168.40.0/24 workstation networks. The instructor and server segment operated within the 192.168.60.0/24 network.

The routing tables verified that Router0 contained static routes to the 192.168.30.0/24 and 192.168.40.0/24 networks through Router1, while Router1 contained static routes to the 192.168.10.0/24 and 192.168.20.0/24 networks through Router0. End-to-end ICMP tests further confirmed successful inter-subnet communication among selected workstations, the instructor computer, DNS server, file server, and printers. These results indicate that the static routing configuration was properly implemented and allowed packets to be forwarded across the intended router paths.

```
Router>enable
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1
L       192.168.20.1/32 is directly connected, GigabitEthernet0/1
S    192.168.30.0/24 [1/0] via 192.168.60.3
S    192.168.40.0/24 [1/0] via 192.168.60.3
     192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, GigabitEthernet0/2
L       192.168.60.2/32 is directly connected, GigabitEthernet0/2
```

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.10.0/24 [1/0] via 192.168.60.2
S    192.168.20.0/24 [1/0] via 192.168.60.2
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, GigabitEthernet0/1
L       192.168.40.1/32 is directly connected, GigabitEthernet0/1
     192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, GigabitEthernet0/2
L       192.168.60.3/32 is directly connected, GigabitEthernet0/2
```

Figure 6. Static routing verification between Router0 and Router1 in Cisco Packet Tracer.

The use of static routing was appropriate for the simulated laboratory network because the topology consisted of a limited number of routers and clearly defined subnets. Since the network structure was small, stable, and predictable, static routing provided a simple and controlled method for directing traffic between workstation groups and centralized network resources.

The results show that subnetting alone is not sufficient to support communication across different network segments. Correct gateway assignment and static route configuration were necessary to allow devices from separate subnets to communicate. The successful routing verification demonstrates that the proposed LAN design can maintain logical separation among workstation groups while still allowing authorized access to shared services such as the DNS server, file server, printers, and instructor computer.

F. DNS and File Server Testing

The DNS server and file server were configured as centralized services within the simulated laboratory network to support hostname resolution and file sharing operations. These services were evaluated through DNS resolution testing and FTP-based file access testing using Cisco Packet Tracer workstation simulations.

DNS functionality was verified by issuing a name-resolution request from a workstation using the ping command to www.company.local. As shown in Figure 3, the hostname was successfully resolved to its corresponding IP address (192.168.60.30), and the workstation received four successful ICMP replies with 0%

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

packet loss. This confirms that the DNS server was operational and correctly mapped domain names to IP addresses within the simulated network.

File server functionality was tested through FTP access from a workstation. As shown in Figure 4, the workstation successfully connected to the file server at 192.168.60.30, authenticated using valid credentials, and executed the dir command. The system returned a complete directory listing of shared files stored on the server, indicating that file access and file sharing services were fully operational.

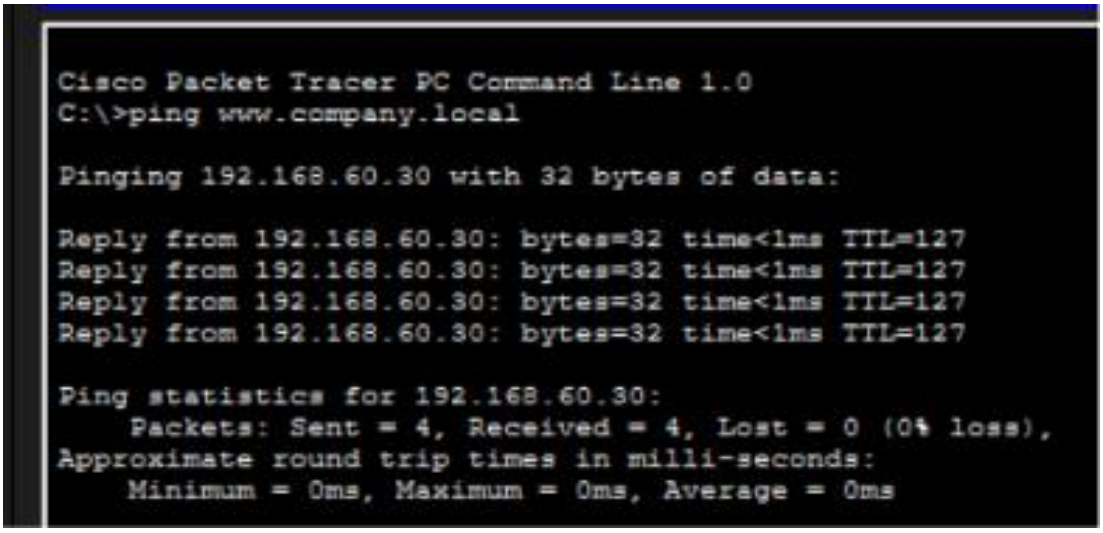

Figure 7. Successful DNS hostname resolution test in the simulated laboratory network

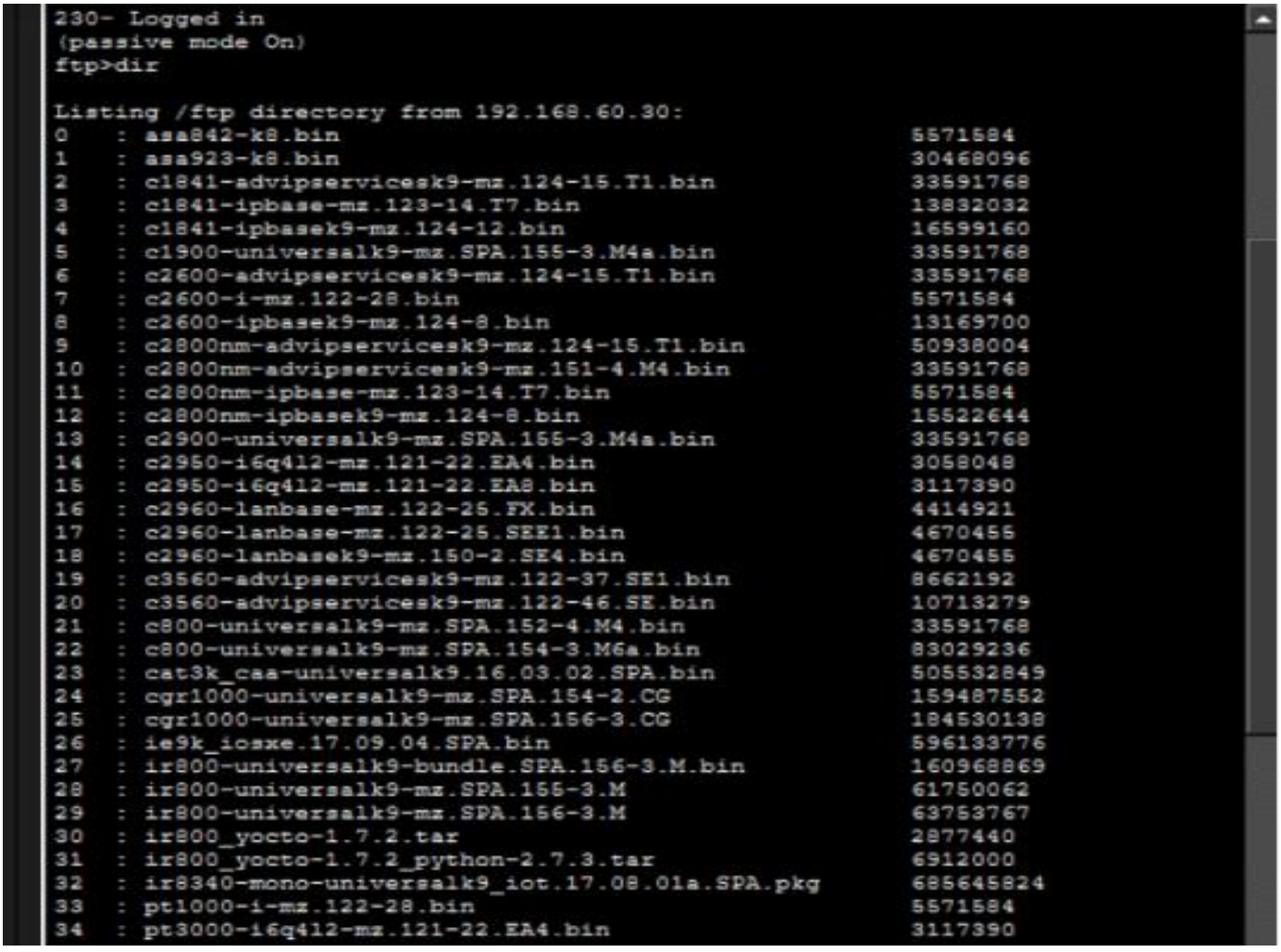

Figure 8. File server access and directory listing using FTP in Cisco Packet Tracer.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

The successful DNS and file server operations demonstrate that the proposed laboratory network is capable of supporting essential centralized network services. DNS improves usability by allowing users to access services through hostnames rather than numeric IP addresses, which aligns with real-world enterprise network practices. The successful resolution of www.company.local confirms that the DNS service was properly integrated into the network architecture.

Similarly, the file server results confirm that centralized file sharing was effectively implemented. The successful FTP login and directory listing indicate that authorized users can access shared resources for academic and laboratory purposes. This reinforces the importance of integrating authentication, routing, and IP configuration to ensure proper service delivery. Overall, the results confirm that both DNS and file sharing services function correctly within the simulated multi-subnet laboratory environment.

G. Ping Testing and ICMP Packet Tracing

End-to-end connectivity was evaluated using ICMP echo requests and traceroute diagnostics. A workstation was used to send a ping request to the destination IP address 192.168.60.19. The results showed four successful replies with zero packet loss and consistent response times, indicating stable connectivity between source and destination devices.

To further validate routing behavior, an ICMP traceroute was performed to determine the path taken by packets. The results showed that the destination was reached within a single hop, and the trace was completed successfully without intermediate failures or delays.

These results confirm that the network provides reliable packet delivery and that inter-device communication within the simulated laboratory environment is functioning correctly.

The successful ping and traceroute results demonstrate that the proposed network design supports efficient and reliable communication between devices. The absence of packet loss and the presence of consistent reply times indicate that the network is stable and properly configured.

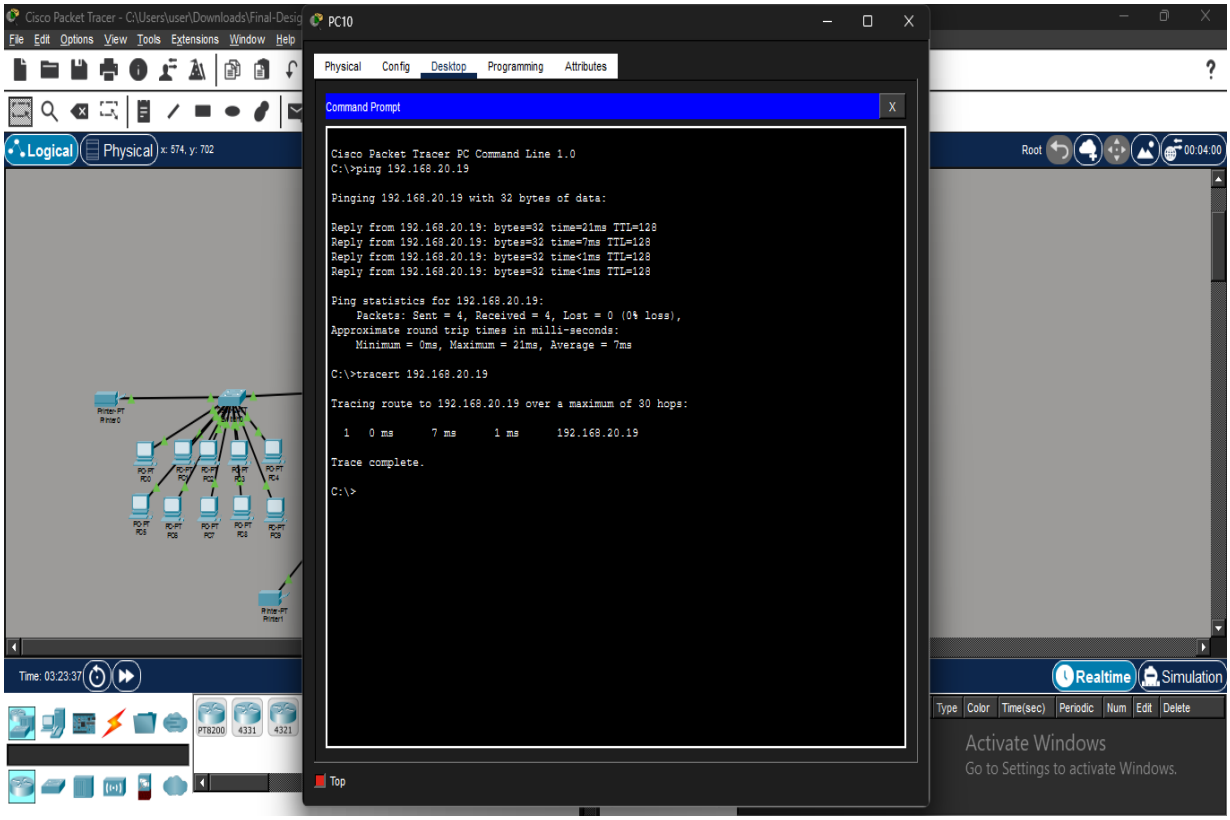

Figure 9. Ping test and ICMP packet tracing result showing end-to-end connectivity in the simulated laboratory network

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Furthermore, the traceroute result suggests that the destination device is reached through a direct or minimally routed path, which is consistent with a well-structured LAN design. This confirms that the routing configuration and subnet integration are functioning as intended within the simulated environment.

Overall, the ICMP testing validates the effectiveness of the proposed laboratory network in supporting real-time communication and inter-device connectivity.

H. VLAN Segmentation and ACL-Based Access Control

The security architecture of the proposed laboratory network integrated VLAN segmentation and Access Control Lists (ACLs) to regulate traffic flow and enforce access control policies within the simulated environment. VLAN segmentation was implemented to logically separate workstation groups, server resources, instructor access, and guest wireless users into distinct broadcast domains. Meanwhile, ACLs were configured at the router level to control inter-subnet communication and restrict unauthorized access between VLANs.

The implemented access control policies successfully enforced network restrictions, where guest network traffic (192.168.70.0/24) was blocked from accessing all internal workstation subnets (192.168.10.0/24 to 192.168.40.0/24), while permitted traffic was allowed toward non-restricted destinations. Testing results confirmed that authorized devices were able to successfully access essential network services such as the DNS server, file server, and shared printers, while unauthorized guest traffic was effectively denied based on the configured ACL rules. These results indicate that the VLAN and ACL configuration was effective in enforcing segmentation and access control within the simulated laboratory network.

```
Switch(config-vlan)#
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name STUDENT_A
Switch(config-vlan)#
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name STUDENT_B
Switch(config-vlan)#
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name STUDENT_C
Switch(config-vlan)#
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name STUDENT_D
Switch(config-vlan)#
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name SERVER
Switch(config-vlan)#
Switch(config-vlan)#vlan 60
Switch(config-vlan)#name INSTRUCTOR
Switch(config-vlan)#
Switch(config-vlan)#vlan 70
Switch(config-vlan)#name GUEST
Switch(config-vlan)#
Switch(config-vlan)#end
Switch#show vlan brief
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 10. VLAN configuration and verification using show vlan brief in Cisco Packet Tracer.

```
Router(config-if)#
Router(config-if)#access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)#access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config)#access-list 100 deny ip 192.168.70.0 0.0.0.255 192.168.40.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#interface g0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 11. Access Control List configuration enforcing inter-VLAN security policies in the simulated laboratory network.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=8ms TTL=128
Reply from 192.168.30.10: bytes=32 time=8ms TTL=128
Reply from 192.168.30.10: bytes=32 time=2ms TTL=128
Reply from 192.168.30.10: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 6ms

C:\>
```

Figure 12. Successful ICMP ping test demonstrating end-to-end connectivity between workstation nodes in the simulated laboratory network

The integration of VLAN segmentation and ACL-based filtering significantly enhanced the security model of the proposed LAN design. VLANs reduced broadcast domain size by separating network devices into functional groups, while ACLs provided granular control over inter-VLAN communication. This dual-layer approach ensured that critical resources such as the instructor workstation and server systems remained protected from unrestricted access by student and guest networks.

The findings further emphasize that network security in a laboratory environment should not rely solely on physical topology. Even when devices share the same switching infrastructure, logical segmentation and packet filtering can enforce controlled communication paths. Compared to a flat network architecture, the proposed design improves security, manageability, and scalability by ensuring that only authorized traffic is permitted between defined network segments.

I. Guest Wi-Fi Containment and Internal Network Restriction

The Guest WiFi network was designed to provide wireless connectivity to visitors while ensuring the security of the laboratory network. A dedicated VLAN 70 was implemented to isolate guest devices from the internal laboratory infrastructure. This network segmentation prevents guest users from directly accessing workstation computers, servers, and network management devices.

In configuring the containment and internal network restriction of the Guest Wi-fi, the following…

Create a Dedicated Guest Network

A separate wireless network named Guest WiFi was created to provide internet and network connectivity for visitors and temporary users. This network was separated from the laboratory network to prevent unauthorized access to critical resources.

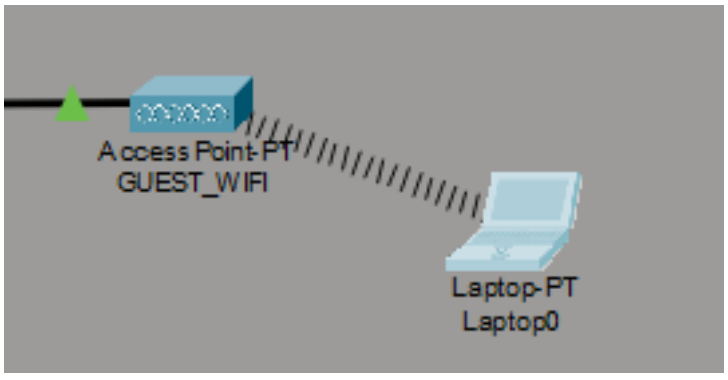

Figure 13. Guest Network

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Configure Wireless Security

The access point was configured with WPA2-PSK authentication, requiring users to enter a password before connecting to the Guest WiFi network with the SSID of "GUEST_WIFI" and WPA2-PSK of "guest12345". This prevents unauthorized users from accessing the wireless network.

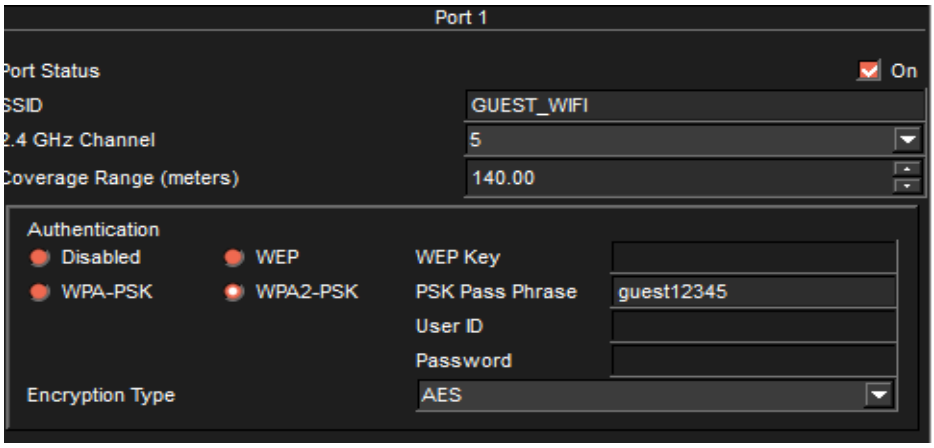

Figure 14. Configuration of Guest WiFi

Implement VLAN Segmentation

The Guest WiFi was assigned to VLAN 70, while laboratory workstations, servers, and administrative devices were assigned to different VLAN and these are the commands in creating VLAN 70. This segmentation logically separates guest traffic from the internal laboratory network.

```
Switch#
Switch#enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 70
Switch(config-vlan)#name GUEST_WIFI
Switch(config-vlan)#
```

Figure 15. Command on VLAN Segmentation

Establish a Dedicated Gateway

Router1 was configured to serve as the default gateway for VLAN 70. This enables guest devices to communicate within the Guest WiFi network while maintaining separation from the internal laboratory infrastructure.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/2
Router(config-if)#no shutdown
Router(config-if)#interface g0/2.70
Router(config-subif)#encapsulation dot1Q 70
Router(config-subif)#ip address 192.168.70.1 255.255.255.0
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 16. Creating Guest WfFi Gateway (192.168.70.1)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Configure DHCP Services

A dedicated DHCP pool was created for VLAN 70 with only 8 specific ip addresses to automatically assign to guest devices. This allows guests to connect easily while maintaining centralized IP address management.

```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.70.1 192.168.70.9
Router(config)#ip dhcp pool GUEST_WIFI
Router(dhcp-config)#network 192.168.70.0 255.255.255.0
Router(dhcp-config)#fdefault-router 192.168.70.1
Router(dhcp-config)#dbddns-server 8.8.8.8
                      ^
```

Figure 17. Configuring DHCP Services

Apply Access Control Lists (ACLs)

Access Control Lists were implemented on Router1 to block communication between VLAN 70 and the laboratory VLANs. These restrictions prevent guest users from accessing laboratory computers, servers, and administrative devices. ACL policies specifically denied access to the Instructor PC, DNS Server, File Server, network devices, and workstation networks. This ensures that sensitive resources remain protected from unauthorized users.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 deny ip 192.168.70.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)#access-list 110 deny ip 192.168.70.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 110 deny ip 192.168.70.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config)#access-list 110 deny ip 192.168.70.0 0.0.0.255 192.168.40.0 0.0.0.255
Router(config)#access-list 110 deny ip 192.168.70.0 0.0.0.255 192.168.60.0 0.0.0.255
Router(config)#access-list 110 permit ip any any
Router(config)#interface g0/2.70
Router(config-subif)#ip access-group110 in
                                      ^
% Invalid input detected at '^' marker.

Router(config-subif)#ip access-group 110 in
Router(config-subif)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 18. Command in the Access Control List for VLAN 70

Verify Network Isolation

Connectivity tests were performed by attempting to access Instructor devices from a guest laptop. Successful implementation was confirmed when guest users could connect to the wireless network but were unable to communicate with protected laboratory resources. As the network was evaluated to ensure that guest users could obtain IP addresses, connect to the wireless network, and remain isolated from internal systems. The results demonstrated that VLAN segmentation and ACL enforcement effectively protected laboratory resources while maintaining wireless accessibility for guests.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

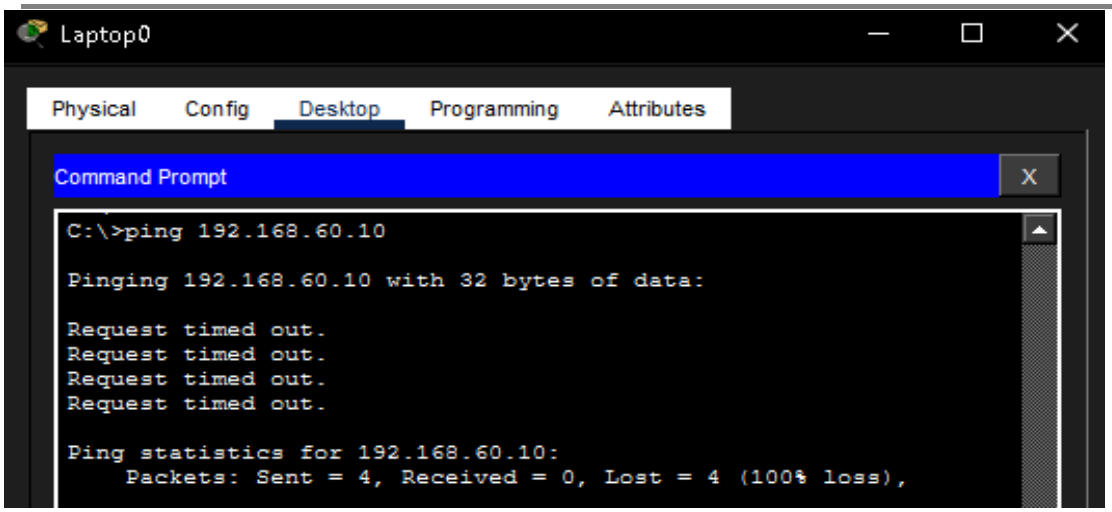

Figure 19. Verification Network Isolation of Laptop0(192.168.70.2) into Instructor PC(192.168.60.10)

J. Overall Evaluation of Connectivity

The overall connectivity of the proposed computer engineering lab network was analyzed to determine the ability of all workstation groups to communicate with the central Instructor PC (192.168.60.10) through different subnet boundaries. This evaluation was carried out using ICMP echo request testing from sample workstation nodes located in each subnet, specifically PC0 (192.168.10.0/24), PC10 (192.168.20.0/24), PC20 (192.168.30.0/24), and PC30 (192.168.40.0/24). Each node conducted a direct ping test to the Instructor PC to verify inter-subnet communication through the configured routing setup.

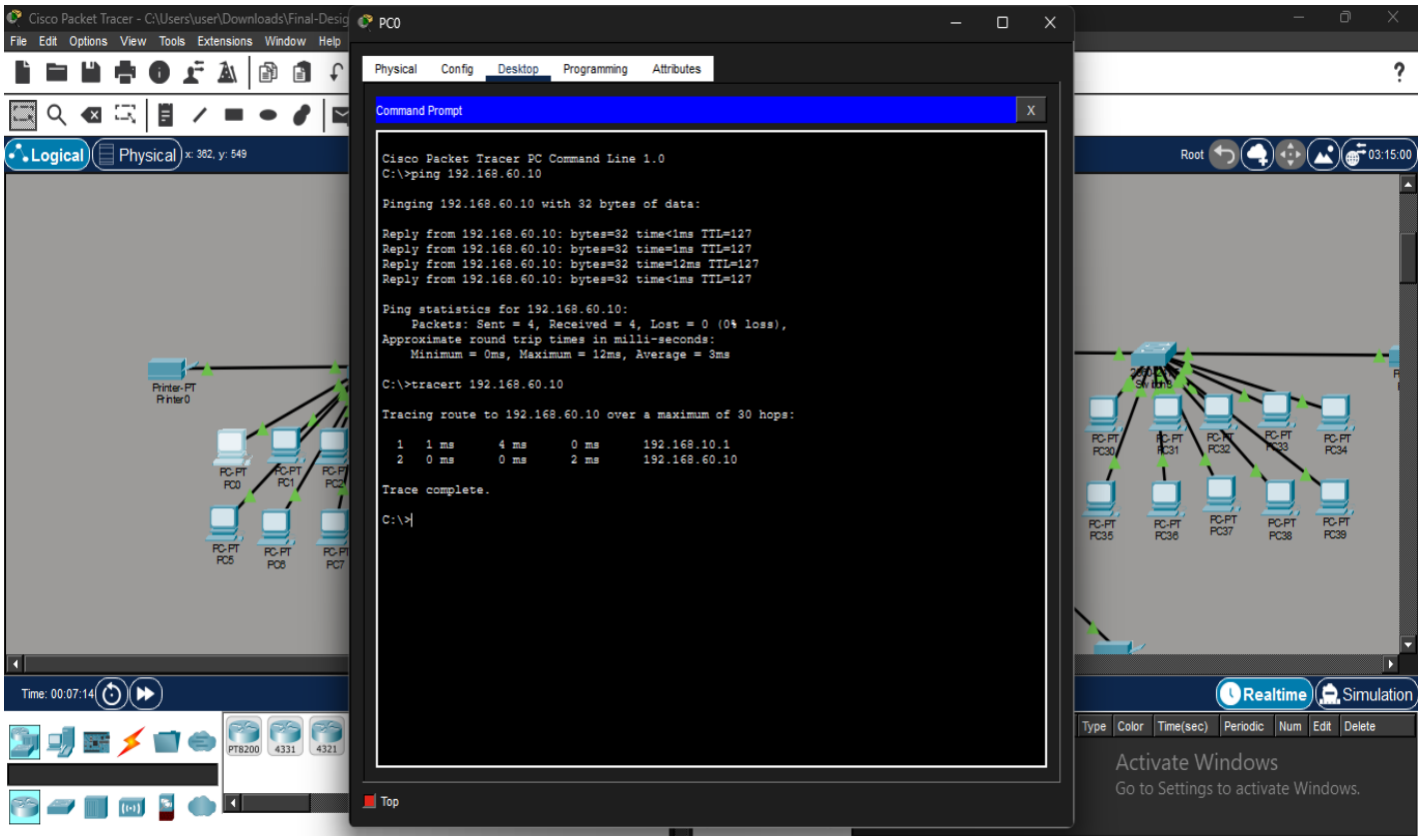

Figure 20: Connectivity Test Result from PC0 (192.168.10.0/24)

The outcomes from PC0 show successful ICMP echo responses from the Instructor PC without any packet loss. This verifies that devices in the initial workstation subnet can effectively communicate with the central server and instructor network via correct gateway setup and routing path navigation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

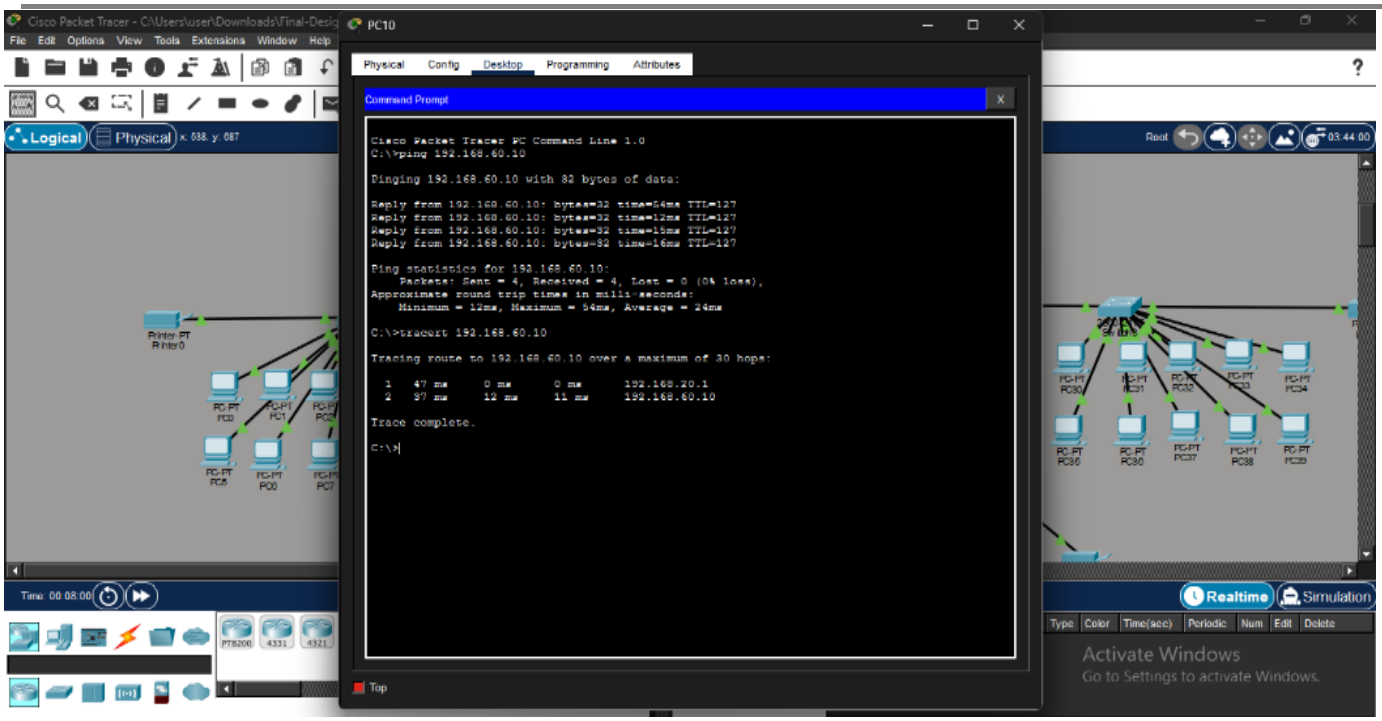

Figure 21 : Connectivity Test Result from PC10 (192.168.20.0/24)

The connectivity test conducted from PC10 indicates reliable response success from the destination network. The lack of packet loss verifies that inter-subnet communication between the second workstation group and the instructor network is completely functional and reliable.

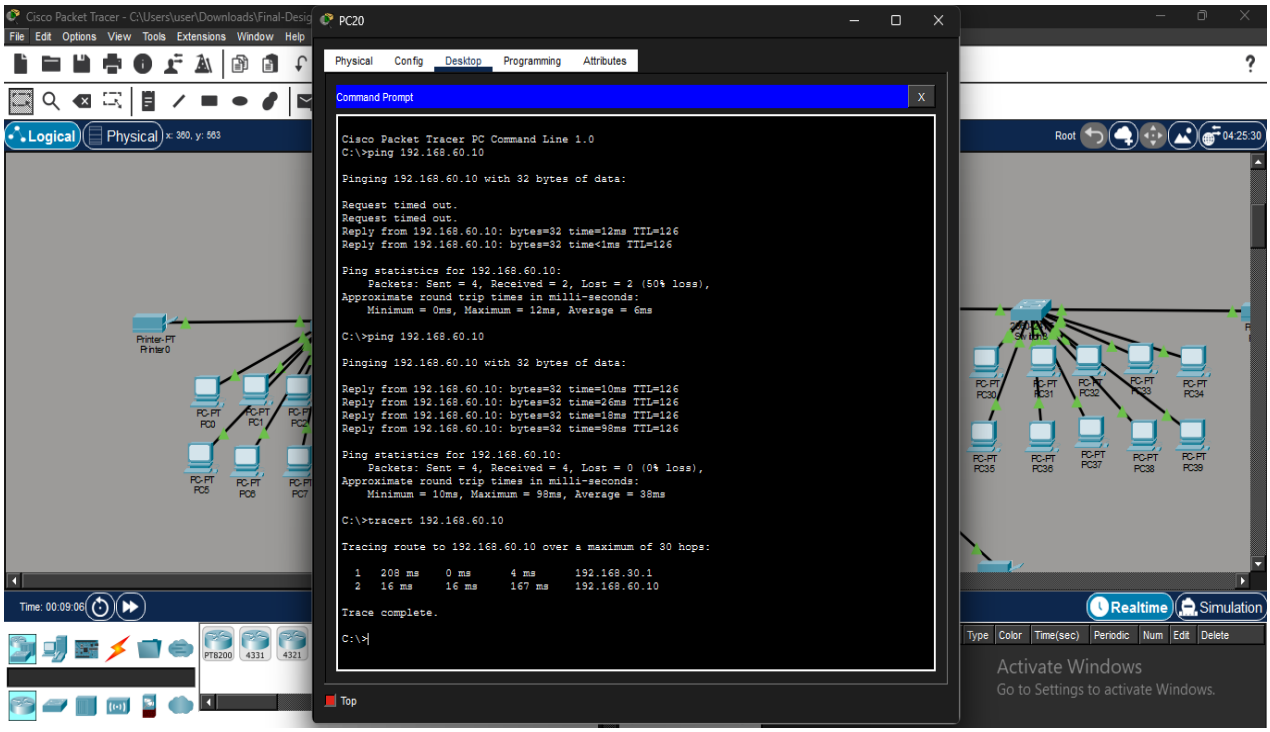

Figure 22: Connectivity Test Result from PC20 (192.168.30.0/24)

The connectivity test from PC20 initially exhibited intermittent packet loss during the first ICMP run, with only two of four packets being successfully received, leading to temporary packet loss. Nonetheless, a later test showed consistent connectivity with full ICMP responses and 0% packet loss. This behavior suggests a temporary initial delay probably linked to network convergence or address resolution activities. Additional verification with the tracert command validated successful packet movement through the set routing path, arriving at the Instructor PC through the correct gateway and intermediate network segments.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

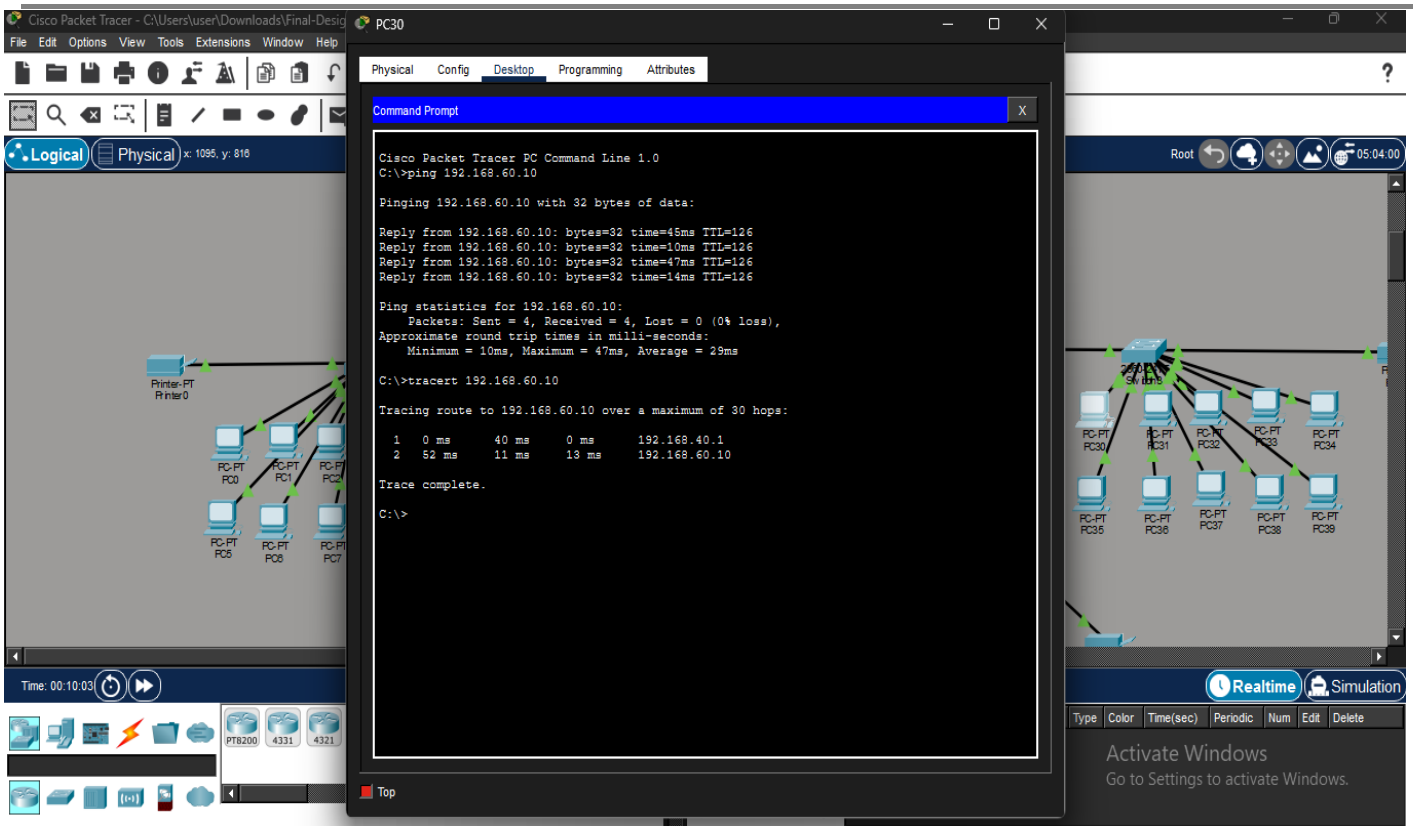

Figure 23: Connectivity Test Result from PC30 (192.168.40.0/24)

The fourth workstation group successfully established complete connectivity to the Instructor PC, verifying that all access-layer subnetworks are correctly set up and able to interact with the centralized server infrastructure.

The results from the ICMP echo request testing generally indicate efficient communication between all workstation groups and the Instructor PC. Three workstation groups (PC0, PC10, and PC30) showed a steady 0% packet loss; however, PC20 faced brief packet loss during the first run but achieved stable connectivity in subsequent tests. Overall, all workstation teams effectively established complete communication with the central network.

These findings confirm that the IP addressing technique, default gateway configuration, and implementation of static routing are properly set up within the network. Since every workstation group operates within a unique IPv4 subnet, effective communication requires proper inter-network routing via the hierarchical framework. The results also indicate that the routers effectively manage traffic between the workstation subnets (192.168.10.0/24 to 192.168.40.0/24) and the instructor/server subnet (192.168.60.0/24), ensuring seamless end-to-end connectivity across the simulated lab network.

In general, the results confirm that the proposed network design offers a reliable and functional communication environment. The connectivity behavior observed validates the success of the hierarchical topology and routing setup in enabling controlled and dependable inter-subnet communication within the simulated computer engineering lab network.

CONCLUSION

This study successfully designed, evaluated, and validated a robust Local Area Network (LAN) architecture specifically optimized to meet the rigorous and volatile operational demands of a modern Computer Engineering Laboratory. By departing from conventional flat network topologies, this research demonstrated that the integration of the Cisco Three-Tier Hierarchical Model with logical segmentation via IEEE 802.1Q Virtual Local Area Networks (VLANs) yields a resilient infrastructure capable of isolating heavy experimental payloads from primary academic systems.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Empirical evaluations conducted within the simulation and deployment phases confirmed that the implementation of Rapid Spanning Tree Protocol (RSTP) effectively eliminates architectural loop vulnerabilities, providing sub-second convergence times critical during hardware-in-the-loop (HIL) testing. Furthermore, the strategic application of Access Control Lists (ACLs) at the distribution layer successfully enforced absolute traffic isolation, preserving the integrity of administrative and instructional nodes without imposing throughput degradation or latency penalties upon student workstations. Ultimately, this structural framework offers a highly scalable, secure, and reproducible network blueprint that successfully aligns institutional data security requirements with the dynamic, hands-on pedagogical demands of engineering education.

RECOMMENDATIONS

To optimize the long-term scalability and security of the proposed laboratory network, the following targeted advancements are recommended:

1. **Deploy Software-Defined Networking (SDN):** Transition the architecture to an SDN framework to allow dynamic, automated bandwidth allocation and real-time traffic shaping based on active laboratory modules (e.g., prioritizing VLSI simulations over standard web traffic).

2. **Implement Network Access Control (NAC):** Integrate IEEE 802.1X authentication to automatically detect and isolate diverse hardware endpoints—such as microcontrollers and FPGA kits—into the experimental VLAN, mitigating rogue device vulnerabilities.

3. **Integrate Link Aggregation (LACP):** Configure IEEE 802.3ad Link Aggregation Control Protocol across high-traffic trunk connections to establish structural redundancy, doubling backbone throughput and preventing single-point-of-failure downtimes.

ACKNOWLEDGEMENT

The researchers would like to express their sincere gratitude to **Minerva C. Zoleta** for her invaluable guidance, expertise, and unwavering support throughout the development of this study. Her insightful recommendations, constructive feedback, and encouragement greatly contributed to the successful completion of this research. Her dedication to academic excellence and commitment to mentoring students inspired the researchers to strive for quality and professionalism in every stage of the project.

The researchers also extend their appreciation to the **Eulogio 'Amang' Rodriguez Institute of Science and Technology**, particularly the Computer Engineering Department, for providing the knowledge, resources, and learning environment necessary for conducting this study.

Finally, the researchers would like to thank their families, friends, and classmates for their continuous encouragement, understanding, and support throughout the research process. Their motivation and assistance played a significant role in the completion of this work.

To God be the glory for His guidance, strength, and blessings throughout this endeavor.

REFERENCES

1. Athab, O. A., & Saheb, A. M. (2022). Design and implementation of electronic infrastructure for academic establishment. arXiv preprint. https://doi.org/10.48550/arXiv.2202.03801
2. Bahry, M. S., & Sugiantoro, B. (2018). Analysis and implementation IEEE 802.1Q to improve network security. IJID (International Journal on Informatics for Development), 6(2), 7–13. https://doi.org/10.14421/ijid.2017.06202
3. Biabani, M., Yazdani, N., & Fotouhi, H. (2023). Developing a novel hierarchical VPLS architecture using Q-in-Q tunneling in router and switch design. Computers, 12(9), 180. https://doi.org/10.3390/computers12090180

4. Chou, T. S., & Hempenius, N. (2020). An assessment of practical hands-on lab activities in network security management. Journal of Cybersecurity Education, Research and Practice, 2019(2), Article 4. https://doi.org/10.62915/2472-2707.1055
5. Cisco Networking Academy. (2023). CCNA: Enterprise networking, security, and automation course materials. https://www.netacad.com
6. Cisco Systems. (2021). Cisco Data Center Infrastructure 2.5 Design Guide. Cisco Press.
7. Cisco Systems. (2023). Cisco Packet Tracer user guide. https://www.netacad.com/courses/packet-tracer
8. Cisco Systems. (2024a). Introduction to networks (CCNA 1) companion guide. Cisco Press.
9. Cisco Systems. (2024b). Routing and switching essentials (CCNA 2) companion guide. Cisco Press.
10. Forouzan, B. A. (2013). Data communications and networking (5th ed.). McGraw-Hill Education.
11. IEEE Standards Association. (2018). IEEE 802.1Q standard for VLAN tagging. https://standards.ieee.org
12. Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.
13. Mashuri, M. A. I. (2024). Design and simulation of a VLAN-based campus network using Cisco Packet Tracer. Journal of Applied Informatics Research, 3(1), 12–25.
14. Ngoie, I. (2021). Server implementation model for the management of computer laboratories: A case study of Richfield Institute of Technology. SSRN. https://ssrn.com/abstract=3876055
15. Olifer, N., & Olifer, V. (2005). Computer networks: Principles, technologies and protocols for network design. Wiley.
16. Pokorný, M., & Zach, P. (2013). Design, implementation and security of a typical educational laboratory computer network. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 61(4), 1077-1087. https://doi.org/10.11118/actaun201361041077
17. Putra, L. O. A. S., Effendi, H., Hendriyani, Y., & Ambiyar. (2023). Development of a local area network with NetSupport in learning in a computer laboratory. Indonesian Journal of Computer Science, 12(4). https://doi.org/10.33022/ijcs.v12i4.3327
18. Stallings, W. (2013). Data and computer communications (10th ed.). Pearson.
19. Suhartanto, A., & Putri, S. B. (2024). Perancangan topologi jaringan lab komputer sekolah dengan segmentasi siswa dan guru. Eduscotech, 5(1). https://journal.udn.ac.id/index.php/eduscotech/article/view/541
20. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5th ed.). Pearson.
21. Zapanta, D. B., Jr., Talirongan, H., & Talirongan, F. J. B. (2021). Access control and monitoring: A system for computer laboratory. Mediterranean Journal of Basic and Applied Sciences, 5(1), 18–27. https://doi.org/10.46382/MJBAS.2021.5102

ABOUT THE AUTHORS

Abegail P. Ramirez is a Bachelor of Science in Computer Engineering student at Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST) in Manila, Philippines. She holds a **National Certificate in Computer Systems Servicing NC II (CSS NC II)**, anchoring her academic foundation in practical hardware configuration, networking, and systems maintenance. Her research and academic interests center on embedded systems, microcontroller-based automation, and computer systems design, with practical experience developing Arduino-based automation systems and applied computing solutions to solve real-world problems.

Kristine Anne R. Laput is a Third-year college student taking up a Bachelor of Science in Computer Engineering at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST) and a **Computer Systems Servicing (CSS) NC II certificate holder**. She has a strong foundation in software and hardware development, programming, GUI design, SolidWorks, and system design. Passionate about technology and innovation, she continuously develops her skills to create practical and user-centered engineering solutions.

Art Julian D. Abrera is a 3rd-year Bachelor of Science in Computer Engineering student at Eulogio "Amang" Rodriguez Institute of Science and Technology. He is developing skills in both coding and hardware systems, with foundational knowledge in computer programming, circuit fundamentals, and system

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

troubleshooting. He also has hands-on experience in computer laboratory setups and basic hardware maintenance gained through academic activities and laboratory work. He continues to strengthen his technical abilities in software development and hardware integration as part of his Computer Engineering training, while improving his problem-solving skills and practical understanding of computer systems.

Mark Daniel Tomale is a third-year college student taking up a Bachelor of Science in Computer Engineering at Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He has completed **Arduino Programming** under the **Special Opportunity Program (SOP)** and obtained **TESDA National Certificate II (NC II) in Computer Systems Servicing (CSS)**. He has a strong foundation in computer programming and mechatronics systems, with hands-on experience in microcontroller-based projects, circuit design, and logical algorithmic programming. His technical skills include Arduino programming, basic electronics troubleshooting, and hardware/software integration. He is eager to further develop his skills in embedded systems and automation technologies and apply them in real-world engineering applications.

David James A. Delgado is a third-year Computer Engineering student at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He has a strong interest in programming and software development, particularly in subjects related to coding, system analysis, and computational problem-solving. He is currently building his technical foundation with the goal of becoming a software engineer, aiming to apply his skills in designing and developing efficient, reliable, and practical software solutions that address real-world needs.

Kiervin N. Guillena is an aspiring Computer Engineer currently pursuing his degree at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He is a **TESDA National Certificate II (NC II) holder in Computer Systems Servicing (CSS)**, a credential that highlights his proficiency in hardware assembly, network configuration, and system maintenance. He is dedicated to bridging the gap between hardware architecture and software development. With a focus on precision and innovation, he continues to expand his expertise in system automation and hardware-software integration, aiming to contribute impactful solutions to the field of computer engineering.

Engr. Minerva C. Zoleta, a Professional Computer Engineer, is a dedicated Computer Engineering Professor at the Eulogio "Amang" Rodriguez Institute of Science and Technology in the Philippines, specializing in Embedded Systems, Operating Systems, and Computer Network and Security. With a strong background in academia and industry. She has been instrumental in shaping the next generation of Engineers through innovative teaching methods and hands-on research. Engr. Zoleta holds a Master's degree in Electrical Engineering with a major in Computer Engineering at the Technological University of the Philippines, Manila, and is pursuing her doctoral degree in Engineering with a specialization in Computer Engineering at the Technological Institute of the Philippines. She has presented and published research on topics such as embedded systems, IoT applications, and wireless communication in international conferences and journals.