Journal of Applied Informatics Research Vol. 01 No. 01 (2025) pp. 45~56

Journal of Applied Informatics Research
Faculty of Vocational Studies, Unesa Campus 1, Ketintang, Surabaya, Indonesia
Website: https://journal.unesa.ac.id/index.php/jair/ | Email: jair@unesa.ac.id

Design and Simulation of a VLAN-Based Campus Network Using Cisco Packet Tracer

Fitria[1], M Adamu Islam Mashuri[2], Rosita[3]

[1,2,3]Department of Informatics Management, State University of Surabaya, Indonesia
[1]fitriafitria@unesa.ac.id, [2]mmashuri@unesa.ac.id, [3]rositarosita@unesa.ac.id

ARTICLE INFORMATION

Article history:

Received July 28, 2025
Revised July 29, 2025
Accepted July 30, 2025

Keywords:

Computer network;
VLAN;
Cisco Packet Tracer;
Star Topology;
Subnetting

ABSTRACT

The development of information technology encourages educational institutions to have a reliable and structured computer network infrastructure. This study aims to design a campus computer network using Cisco Packet Tracer simulation with a VLAN segmentation approach and star topology. The methods used include identifying network requirements, designing topology, allocating IP subnets using subnetting techniques, and configuring devices such as routers, switches, and access points. The RIPv2 protocol is used to support communication between VLANs, and DHCP is implemented to facilitate automatic IP address assignment. The simulation results show that all devices in the network can be connected to each other well, as evidenced by connectivity tests using the ping and tracert commands. All tests produced positive responses without any packet loss or failed communication routes. This study proves that Cisco Packet Tracer is an effective tool in designing and testing networks before physical implementation.

1. INTRODUCTION

The development of information and communication technology (ICT) in the current digital era has brought significant changes in various aspects of life, including in the education sector [1], [2]. Universities as higher education institutions are required to be able to provide adequate technological infrastructure to support academic, administrative, research, and community service activities [3]. One important element of ICT infrastructure in the campus environment is a reliable, secure, and efficient computer network [4].

Computer networks enable fast and efficient data exchange between users, devices, and campus information systems, such as Learning Management Systems (LMS), academic portals, digital repositories, and internal email services [5]. In addition, with the increasing use of mobile devices and the Internet of Things (IoT) in academic environments, the need for stable and scalable networks is becoming increasingly important [6], [7].

However, designing and implementing a complex campus computer network spread across multiple buildings and with many users requires significant costs, technical expertise, and careful planning [8]. One approach to reducing risk and costs in the early stages of network development is to conduct simulations prior to actual implementation. These simulations allow for testing of network designs, performance analysis, and evaluation of failure scenarios at minimal cost [9].

One of the most widely used network simulation software is Cisco Packet Tracer, an interactive simulation application developed by Cisco Systems. Cisco Packet Tracer allows users to create virtual network models, configure devices, and monitor the flow of data packets in real time [10]. This application is very useful for both technical training and for the initial design of small to medium-scale networks, including for campus network simulation needs [11].

In large-scale network designs such as campuses, the use of Virtual Local Area Networks (VLANs) is an important solution for network segmentation. VLANs allow logical network separation even though devices are on the same physical switch, thus improving security, bandwidth efficiency, and ease of management [12], [13].

By using VLANs, academic, administrative, laboratory, and student departments can be grouped into separate networks that suit their respective needs and access levels [14].

This research aims to design and simulate a VLAN-based campus computer network using the Cisco Packet Tracer application. The research focuses on creating a network topology spanning multiple buildings/laboratories, configuring VLANs on switches, testing connectivity between network segments, and analyzing simulation results. The results of this research are expected to serve as an initial reference in developing a structured, secure, and flexible campus network infrastructure.

2. RESEARCH METHODS

This research uses an experimental engineering approach by applying Cisco Packet Tracer software-based simulations to the design of a campus-scale computer network. The goal of this method is to produce a network design that is efficient, structured, and easy to implement in a real campus environment. The stages involved include: reviewing computer network concepts, selecting topologies, identifying network requirements, designing the network, and then configuring and testing.

2.1. Computer Network Concept

A computer network is a system consisting of two or more computer devices that are connected to each other to exchange information and share resources, such as files, printers, databases, and internet connections. According to Tanenbaum and Wetherall, a computer network is a collection of autonomous devices that are connected to each other using transmission media and following certain protocol rules in order to communicate effectively [15].

In the context of higher education, computer networks play a vital role in supporting learning processes, research, academic administration, and the integration of campus digital services, such as e-learning, the Academic Information System (SIAKAD), and scientific repositories. The use of computer networks in the campus environment also makes a significant contribution to supporting the digitalization of academic processes and the operational efficiency of institutions [16].

Based on the area covered, computer networks are divided into three main types:

- Local Area Network (LAN): a network with limited coverage, such as within a single building or campus.
- Metropolitan Area Network (MAN): a network that covers an area between buildings or campus locations in one city.
- Wide Area Network (WAN): a large-scale network such as an inter-university network or a connection to the internet.

Computer networks can also be categorized based on their functional architecture:

- Client-Server: there is a server computer that provides services and clients that access them.
- Peer-to-Peer: all computers have an equal role and can share resources with each other without a central server.

From the infrastructure side, computer networks consist of:

- Hardware such as switches, routers, access points, UTP/STP cables, and NICs.
- Software such as network operating systems and monitoring applications.
- Transmission media, both wired and radio waves (wireless).

The primary communication protocol used is TCP/IP, which supports logical addressing, packet segmentation, and data routing. Additionally, additional protocols such as DNS, DHCP, HTTP, FTP, and SMTP are also widely used to support specific services.

The development of modern network technology has also encouraged the use of the concept:

- Virtual Local Area Network (VLAN) for logical segmentation of networks.
- Quality of Service (QoS) for priority-based traffic management.
- Firewall and IDS/IPS for network protection against cyber attacks.

Thus, a comprehensive understanding of computer network concepts is an important basis for designing reliable, efficient, and secure ICT infrastructure in a university environment.

2.2. Star Topology

The star topology is one of the most widely used network topologies, especially in local environments such as schools, campuses, and offices. In this topology, each device (host) is connected to a central device, such as a switch or hub, which serves as a control point for data traffic within the network. This connection forms a star-like pattern, with the center of the star controlling all communication between devices.

The main advantage of a star topology is ease of network management and maintenance. If a cable or client device is damaged, it will not affect the connectivity of other devices. Furthermore, troubleshooting can be done more quickly because the communication path is centralized and well-controlled [17].

In its implementation, switches are used more often than hubs because they support efficient data delivery and do not cause data collisions like in hubs. The use of switches also supports logical VLAN segmentation, which is very useful in dividing network traffic based on organizational functions [18].

Some of the advantages of star topology include:

- Easy to install and configure, because each device only requires one cable to the center.
- High fault tolerance, failure of one node does not affect other nodes.
- Easy to expand, simply add cables to the switch to add new devices.

However, this topology also has weaknesses, namely:

- High dependence on the central device (switch); if the switch is damaged, the entire network can be disrupted.
- Installation costs are higher than bus topology because it requires more cables and active devices [19].

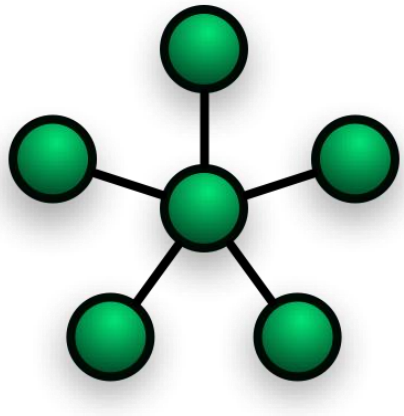

Figure 1. Star topology

2.3. Identify Network Needs

Before designing and implementing a network, a very important initial step is to identify network requirements. This stage aims to determine the number of devices, connection types, topology used, required services, and the functional and non-functional requirements of the network to be built. Accurate identification of requirements will have a direct impact on the efficiency, reliability, and scalability of the network system as a whole [20]. Some important aspects identified in campus network development include:

A. Number and Type of Devices

The devices that will be connected to the network consist of:

- Client devices: lecturer PCs, laboratory computers, TU computers, laptops, and smartphones.
- Active network devices: switches, routers, and access points.
- Server devices: such as file servers, database servers, and academic information system servers.

B. Network Segmentation

To increase efficiency and security, the network is divided into several segments, including:

- Administrative segment (TU)
- Academic segment (lecturer's room and laboratory)
- Infrastructure segment (server)
- Wireless segment (buildings A and B)

This segmentation also allows the implementation of VLANs (Virtual LANs) to logically separate data traffic between departments, even though they use the same physical infrastructure.

C. Required services

Some important network services that must be provided in this system include:

- DHCP (Dynamic Host Configuration Protocol) for IP addressing automation
- DNS (Domain Name System) for name resolution
- Routing between VLANs using the RIPv2 protocol
- Wireless access in building areas A and B

D. IP Address Requirements

Each segment has a different number of devices, requiring efficient IP addressing planning. CIDR is used to allocate IP addresses according to the number of hosts per segment, preventing wasteful IP allocation.

Identification of these needs is the basis for compiling topology designs, subnet allocations, and network device configurations in the simulation implementation stage using Cisco Packet Tracer.

2.4. Network Design

After identifying network requirements, the next step is to design the computer network to be implemented. This network design includes a comprehensive topology overview, network segmentation, and the relationships between devices such as routers, switches, access points, and end devices. The design is performed using Cisco Packet Tracer software, which allows for detailed visualization of network elements and virtual testing of their functionality. This design adopts a star topology combined with the use of VLANs (Virtual Local Area Networks) to logically separate data traffic between departments.

The following figure shows a campus network design scheme consisting of three main routers that manage several network segments such as the server room, lecturer room, administration, computer laboratory, and wireless areas in Buildings A and B. Each router is designed to handle several network IDs with customized configurations using subnetting and routing techniques between VLANs.

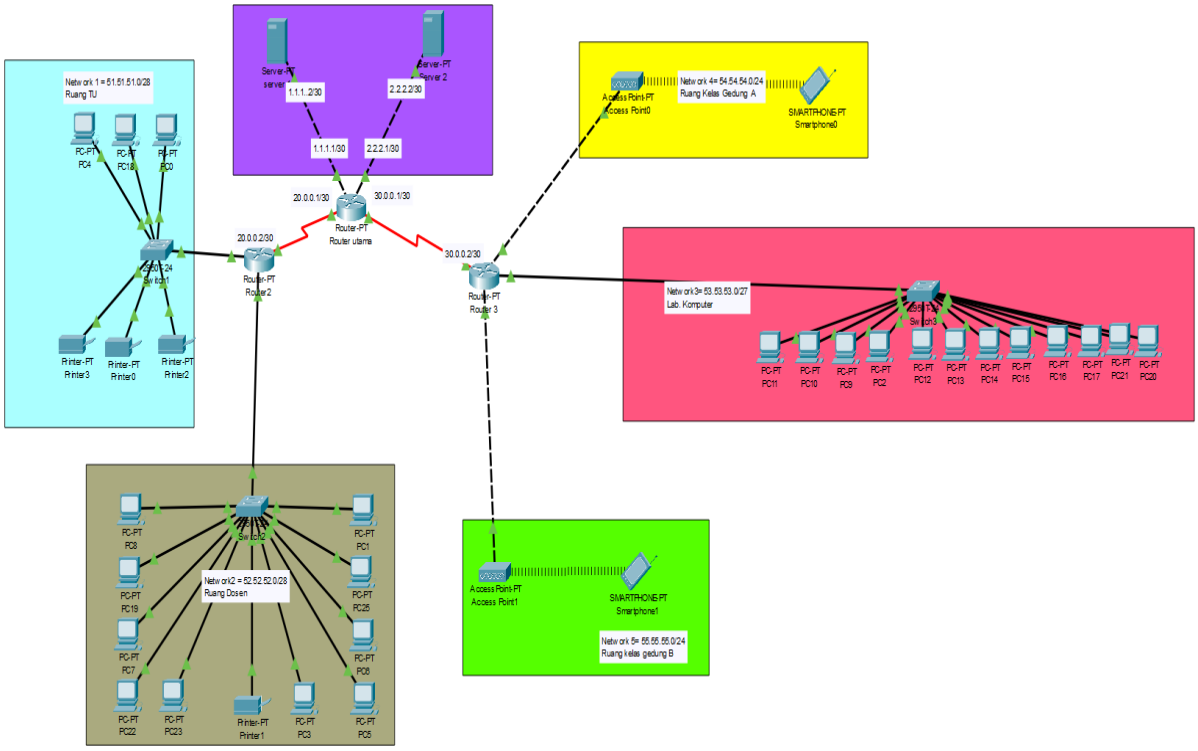

Figure 2. Network design

In the topology that we created, each router has several network IDs, which are explained as follows:

1. Main Router: This router acts as the central device connecting other routers, and communication between them must pass through it. In a real-world implementation, this router will also act as a bridge or gateway to the Internet Service Provider. This router manages the Network ID for the server room.
2. Router 2 manages two network IDs: the Lecturer's Room and the Administration Room. The entire network uses wired media, with no wireless connections.
3. Router 3 is the router that has the most Network IDs, there are 3 Network IDs, namely the Network for the Computer Laboratory, Building A, and Building B. The network on router 3 has 2 networks that are distributed using wireless media, namely the network in Building A and Building B.

2.5. Network Configuration

After the network design is completed, the next step is configuring the network devices to ensure they operate according to the design. This configuration is performed in stages on each major network component, such as routers, switches, and end-user devices. The configuration focuses on assigning IP addresses, establishing VLANs, setting up trunking between switches, routing between VLANs using RIPv2, and configuring DHCP to automatically distribute IP addresses to client devices.

All configurations were performed within the Cisco Packet Tracer simulation environment, allowing for hands-on testing of network connectivity. Configuration was performed manually via the command-line interface (CLI) for flexibility and industry-standard practices. The following details the configuration steps performed on each device.

2.5.1. Server Room

The server room needs 2 usable IPs for 2 servers, because there are 2 servers, we create 2 Network IDs for the server room using CIDR /30 which has 2 usable IPs (for the Server Interface and Router / Gateway Interface) with the following IP Table:

Table 1. Server 1

Network ID	1.1.1.0/30
Netmask	255.255.255.252
Number of Segments	64
Number of Usable IPs	2
Block ID used	0-3
Broadcast	1.1.1.3/30
Gateway	1.1.1.1/30
Usable IP Range	1.1.1.1-1.1.1.2

Table 2. Server 2

Network ID	2.2.2.0/30
Netmask	255.255.255.252
Number of Segments	64
Number of Usable IPs	2
Block ID used	0-4
Broadcast	2.2.2.3/30
Gateway	2.2.2.1/30
Usable IP Range	2.2.2.2-2.2.2.2

2.5.2. Administration room

The Administration Room has a need for 3 PCs and 3 printers, so 6 usable IPs are needed, the CIDR we use is /28 with the following details:

Table 3. Administration

Network ID	51.51.51.0/28
Netmask	255.255.255.240
Number of Segments	16
Number of Usable IPs	14
Block ID used	0-15
Broadcast	51.51.51.15/28
Gateway	51.51.51.1/28
Usable IP Range	51.51.51.1-51.51.51.14

2.5.3. Lecturer's Room

The lecturer's room requires 10 PCs and 1 printer, so 11 usable IPs are needed, the CIDR we use is /28 with the following details:

Table 4. Lecturer Room

Network ID	52.52.52.0/28
Netmask	255.255.255.240
Number of Segments	16
Number of Usable IPs	14
Block ID used	0-15
Broadcast	52.52.52.15/28
Gateway	52.52.52.1/28
Usable IP Range	52.52.52.1-52.52.52.14

2.5.4. Computer lab

The computer laboratory has 20 PCs which require 20 usable IPs, therefore we use CIDR /27 with the following details:

Table 5. Computer Laboratory

Network ID	53.53.53.0/27
Netmask	255.255.255.224
Number of Segments	8
Number of Usable IPs	30
Block ID used	0-31
Broadcast	53.53.53.31/27
Gateway	53.53.53.1/27
Usable IP Range	53.53.53.1-53.53.53.30

2.5.5. Building A

Building A has many classrooms, because of the many needs, we use CIDR 24 with 254 usable IPs. With the following details:

Table 6. Building A

Network ID	54.54.54.0/24
Netmask	255.255.255.0
Number of Segments	1
Number of Usable IPs	254
Block ID used	0-255
Broadcast	54.54.54.255/28
Gateway	54.54.54.1/28
Usable IP Range	54.54.54.1-54.54.54.254

2.5.6. Building B

Building B has many classrooms, because of the many needs, we use CIDR 24 with 254 usable IPs. With the following details:

Table 7. Building B

Network ID	55.55.55.0/24
Netmask	255.255.255.0
Number of Segments	1
Number of Usable IPs	254
Block ID used	0-255
Broadcast	55.55.55.255/24
Gateway	55.55.55.1/24
Usable IP Range	55.55.55.1-55.55.55.254

2.5.7. Network Router

Network IDs are also required for communication between routers. This time, we'll divide the network IDs into two: 1. Main Router - Router 2, and 2. Main Router - Router 3. In these two networks, the main router acts as the gateway. The configuration details are as follows:

Table 8. Main Router-Router 2

Network ID	20.0.0.0/30
Netmask	255.255.255.252
Number of Segments	64
Number of Usable IPs	2
Block ID used	0-3
Broadcast	20.0.0.3/30
Gateway	20.0.0.1/30
Usable IP Range	20.0.0.1-20.0.0.2

Table 9. Main Router-Router 3

Network ID	30.0.0.0/30
Netmask	255.255.255.252
Number of Segments	64
Number of Usable IPs	2
Block ID used	0-3
Broadcast	30.0.0.3/30
Gateway	30.0.0.1/30
Usable IP Range	30.0.0.1-30.0.0.2

3. RESULTS AND DISCUSSION

Testing is performed after all network configurations are completed in Cisco Packet Tracer software. The purpose of this testing is to ensure that all network devices can communicate with each other and that connectivity between network segments is functioning as expected. Testing is performed using an ICMP communication approach using the ping command and route analysis using tracert.

3.1. ICMP testing via PING command

Testing connectivity in a computer network is a crucial step to ensure that all connected devices are properly configured and able to communicate with each other. One of the most common methods for testing connectivity is through the Internet Control Message Protocol (ICMP), specifically the ping command. This command works by sending an echo request packet to the destination IP address and waiting for a reply. If the destination device responds, the connection is considered successful; conversely, if there is no response or the request times out, there may be a configuration or topology issue.

In this campus network simulation, ping tests were conducted from various devices spread across several network segments, including the administration room, lecturer rooms, computer labs, and mobile devices in buildings A and B. The goal was to test communication between VLANs and ensure that the routing configuration between subnets was working properly. Furthermore, this test was used to verify the effectiveness of the DHCP service in automatically distributing IP addresses.

For example, Figure 3 to Figure 7 shows the results of connection tests from each source device to the destination, such as from the TU room PC to Server 1, from the lecturer room PC to Server 2, and so on. All tests showed positive results with four replies and no packet loss (0% packet loss), which indicates that the VLAN configuration, subnetting, and routing protocol (RIPv2) have been successfully implemented.

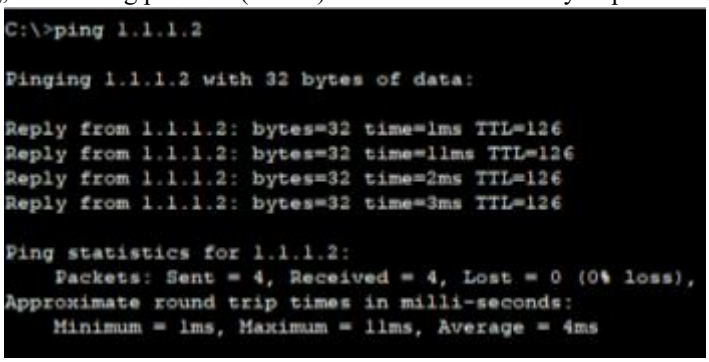

Figure 3. Testing from the TU room PC to server 1

This image shows the results of a connection test from a PC in the Administration room (VLAN 10) to Server 1 (VLAN 40). The ping results show four replies with a stable TTL (Time to Live) value, indicating that the inter-VLAN communication channel is functioning properly. There are no request timeouts, indicating that the inter-VLAN routing and IP addressing configuration on both devices is running smoothly.

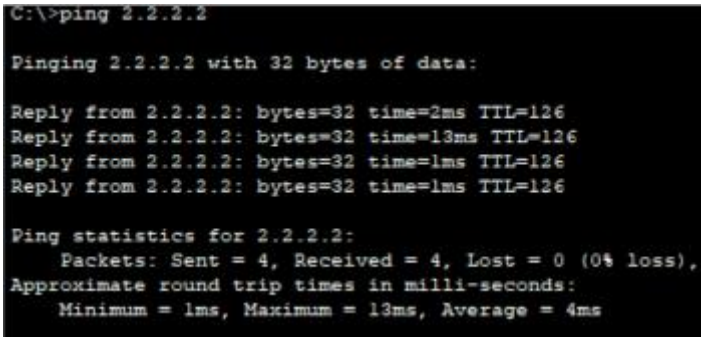

Figure 4. Testing from the Lecturer's Room PC to Server 2

This image shows the results of a connection test from a PC in the lecturer's room (VLAN 20) to Server 2 (also on VLAN 40). As before, the ping was successful without packet loss. This success indicates that routing from VLAN 20 to VLAN 40 has been correctly configured using the RIPv2 protocol, and there are no issues with IP distribution from the DHCP server.

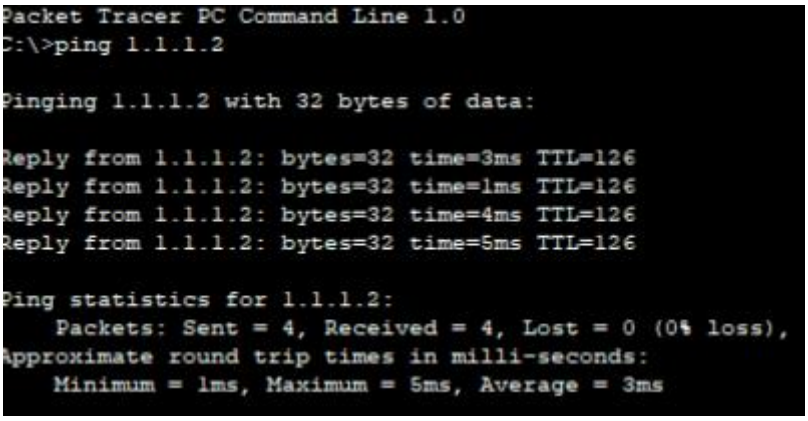

Figure 5. Testing from the Computer Lab PC to server 1

In this figure, a test was conducted from a PC in the computer lab (VLAN 30) to Server 1. All replies were received without significant delay, with the default TTL indicating the route had no more than three hops. This indicates that access from the client in the lab to the central server is smooth and stable.

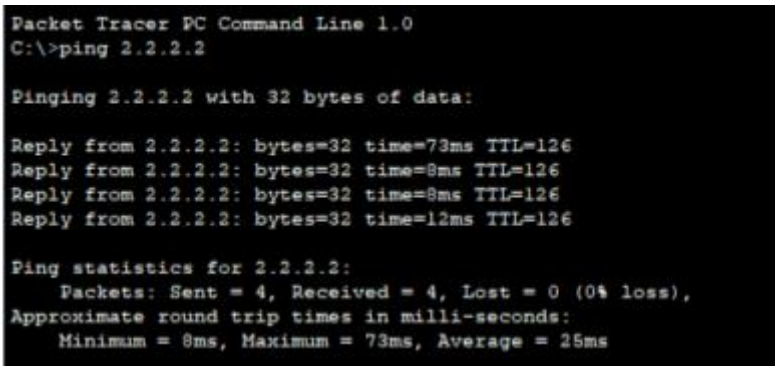

Figure 6. Testing from smartphone Building A to server 1

This image demonstrates the ping results from a smartphone device on Building A's wireless network (VLAN 50) to Server 1. Communication was successful without error. This proves that connectivity from the wireless network to the wired backbone has been effectively established and the wireless VLAN has been configured correctly.

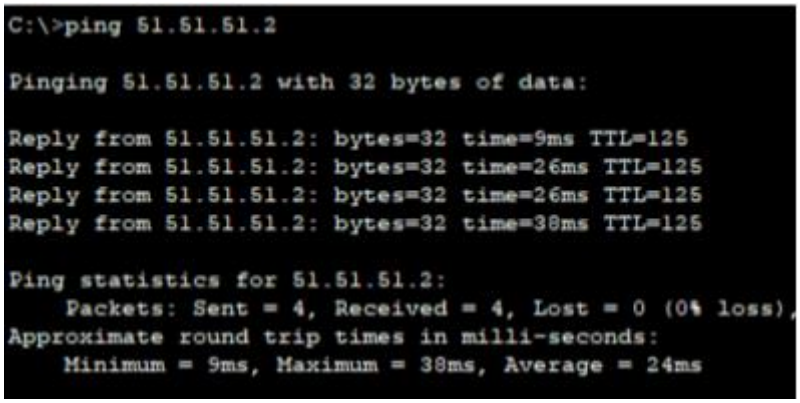

Figure 7. Testing from Building B Smartphone to TU room PC

The final image shows the test results from a mobile device in Building B (VLAN 60) to a PC in the Administration Room (VLAN 10). Ping responses were received perfectly without any timeouts, indicating that all inter-VLAN communication paths through the router were functioning as expected.

To provide a comprehensive overview of the test results, Table 1 summarizes the ping results from five primary devices to different target destinations. All tests were successful, indicating that communication between devices and between VLANs was functioning normally and no network issues were detected during the testing process.

Table 10. Connectivity Test Results

No	Testing	Objective	Results
1	Administration Room PC → Server 1	1.1.1.2	Reply x4, 0% Packet Loss
2	Lecturer Room PC → Server 2	2.2.2.2	Reply x4, 0% Packet Loss
3	PC Computer Lab → Server 1	1.1.1.2	Reply x4, 0% Packet Loss
4	Smartphone Building A → Server 1	1.1.1.2	Reply x4, 0% Packet Loss
5	Smartphone Building B → PC Administration Room	51.51.51.X	Reply x4, 0% Packet Loss

From these results, it can be concluded that all configured devices communicated successfully without packet loss. This indicates that the IP configuration, VLAN allocation, inter-subnet routing settings, and DHCP services were implemented correctly and functioning as intended.

3.2. Route Analysis with tracert

After performing a basic connectivity test using the ping command, the next step in network evaluation is to analyze the data path between devices using the tracert (Trace Route) command. This command is used to trace the path a data packet takes from a source device to its destination, providing information about each hop it passes through.

The purpose of using tracert in this simulation is to ensure that inter-VLAN routing is configured correctly and to identify any suboptimal communication paths or problems with the connecting routers. Each hop in the tracert output indicates the router or gateway the packet passes through, along with the response time.

The analysis was performed from five different devices in each VLAN segment to a specific destination device, and the results are visualized in Figures 8 through 12. The results show that data travels through one or two routers depending on the device location and destination, and there is no significant delay in response time. This indicates that the RIPv2 routing protocol has performed well to deliver routes between VLAN subnets.

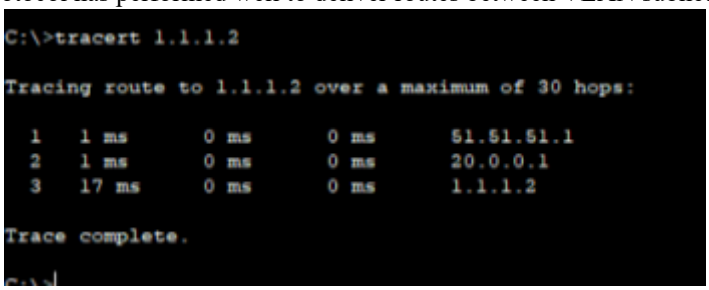

Figure 8. Testing from the TU room PC to server 1

This figure shows that data from a PC in VLAN 10 to Server 1 in VLAN 40 passes through a single router (the default gateway) and is forwarded directly to its destination. This indicates that the static routing configuration, or RIPv2, has detected the fastest and most efficient route between segments.

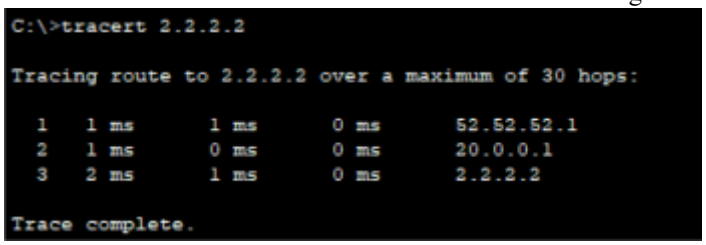

Figure 9. Testing from the Lecturer's Room PC to Server 2

The results in this image show two hops before arriving at Server 2. The first hop is the VLAN 20 router, and the second hop is the VLAN 40 router. This shows that the path between the routers has been configured sequentially and the route can be traversed properly without errors.

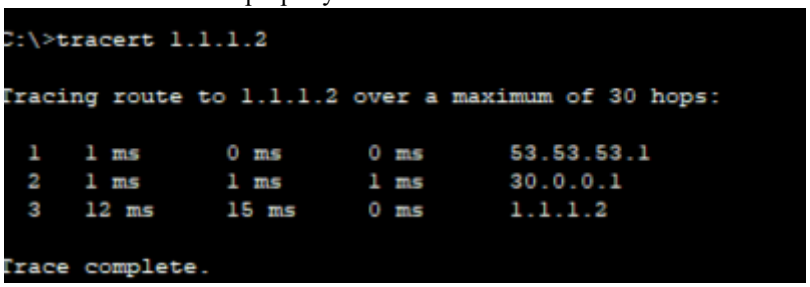

Figure 10. Testing from the Computer Lab PC to server 1

This figure shows three hops: first to the local gateway (VLAN 30), then to the distribution router, and finally to Server 1. This shows a segmented network topology with stable connection paths in each VLAN.

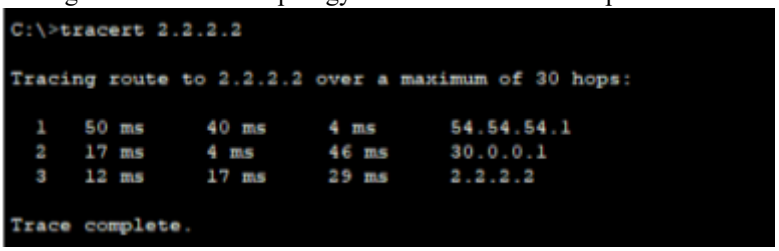

Figure 11. Testing from smartphone Building A to server 1

Devices on Building A's wireless network traverse two hops: access point → wireless VLAN router → server VLAN router. Despite using a wireless network, no delays or errors are visible in the tracert output, indicating that the wireless network has been configured correctly.

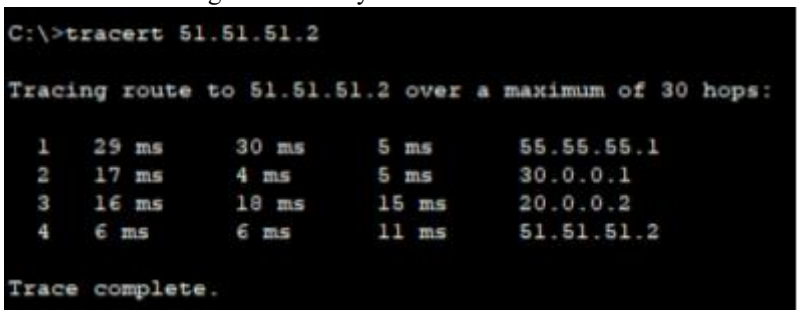

Figure 12. Testing from Building B Smartphone to TU room PC

Three hops are visible: first from the access point VLAN 60, then to the central router, and finally to VLAN 10. This illustrates optimal interconnection between segments despite passing through multiple VLAN logical paths.

4. CONCLUSION

This research has successfully designed and simulated a campus computer network using Cisco Packet Tracer with a VLAN segmentation approach and a star topology. The design process involved identifying network requirements based on the work units within the campus environment, as well as assigning IP addresses using subnetting techniques for efficiency and ease of management.

Simulation results showed that the network configuration, including VLAN settings, DHCP, and inter-VLAN routing using the RIPv2 protocol, worked well. Connectivity testing using ping and tracert commands from various devices on each network segment demonstrated that all devices could connect seamlessly, both wired and wirelessly.

With this design and simulation, educational institutions have a baseline that can be used to implement a real-world physical network. Furthermore, using Cisco Packet Tracer as a simulation tool has proven effective in minimizing the risk of configuration errors before implementation in a real-world environment. This study is limited to the design and simulation stages without real-world deployment. Future work can integrate IoT device connectivity and implement advanced network security measures, such as firewalls and VLAN-based access control, to further support the scalability and resilience of campus networks.

ACKNOWLEDGEMENTS

The authors express their deepest gratitude to the institutions and faculties that have provided support in the form of facilities, infrastructure, and laboratory facilities used in this research. Thanks are also extended to fellow lecturers and students in the Informatics Management Study Program, Faculty of Vocational Studies, Surabaya State University, who participated in the network simulation and testing process using Cisco Packet Tracer.

The author also appreciates the contributions of the reviewers and journal editors who provided corrections and constructive suggestions to improve this article. The moral support and motivation of his family also contributed to the successful completion of this research.

REFERENCES

[1] PN Varne, PJ, S. Shetty, TAK, & NC Gowda, “Campus Network Design and Implementation using Cisco Packet Tracer”, Int. J. Comput. Learn. Intelligence, vol. 2, no. 4, pp. 163–168, Dec. 2023.https://doi.org/10.5281/zenodo.10254264

[2] K. Swapna, B. Nandeeshwar, B. Gagan, A. Aravind and B. Ravi, "Campus Network Design Using Cisco Packet Tracer", 2025 10th International Conference on Signal Processing and Communication (ICSC), Noida, India, 2025, pp. 45-50,https://doi.org/10.1109/ICSC64553.2025.10968176

[3] T. Al-Khraishi and M. Quwaider, “Performance evaluation and enhancement of VLAN via wireless networks using OPNET modeler”, arXiv, Jul. 2020.

[4] AH Ahmed and MNA Al-Hamadani, “Designing a secure campus network and simulating it using Cisco Packet Tracer”, Indonesia. J. Electr. Eng. Comput. Sci., vol. 23, no. 1, pp. 479–489, July 2021,http://doi.org/10.11591/ijeecs.v23.i1.pp479-489

[5] BK Prahani et al., “Learning Management System (LMS) Research During 1991-2021: How Technology Affects Education”, Int. J. Emerg. Technol. Learn. (iJET), vol. 17, no. 17, pp. 28–49, Sept. 2022,https://doi.org/10.3991/ijet.v17i17.30763

[6] E. Soegoto, H. Soegoto, and DS Soegoto, "A Systematic Literature Review of Internet of Things for Higher Education Architecture and Implementation", Indonesian Journal of Science & Technology, vol. 7, no. 3, pp. 511–528, Dec. 2022,https://doi.org/10.17509/ijost.v7i3.51464

[7] A. Trivedi, J. Gummeson, and P. Shenoy, "Empirical Characterization of Mobility of Multi-Device Internet Users," arXiv preprint, Mar. 2020.https://doi.org/10.48550/arXiv.2003.08512

[8] MK Ezad Bin Sulaiman, “Teaching Creativity Using a Realistic Multi-User Operation: Packet Tracer”, arXiv, Dec. 2020.https://doi.org/10.48550/arXiv.2101.02009

[9] SW Nourildean, YA Mohammed & HA Attallah, "Virtual Local Area Network Performance Improvement Using Ad Hoc Routing Protocols in a Wireless Network", Computers, vol. 12, no. 2, 2023, Art. 28.https://doi.org/10.3390/computers12020028

[10] SH Moz, MA Hosen and NFI Tanny, "Campus Network Configuration, Monitoring and Data Flow Simulation using Cisco Packet Tracer", 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 793-798,https://doi.org/10.1109/ICICT57646.2023.10134506

[11] OA Athab & AM Saheb, “Design and Implementation of Electronic Infrastructure For Academic Establishment”, arXiv, Feb. 2022.https://doi.org/10.48550/arXiv.2202.03801

[12] A. Shaik, “A Survey of Emerging Techniques for Large Networks of Virtual Local Area Networks (VLANs) with Benefits and Limitations”, International Journal of Current Engineering and Technology, vol. 14, no. 6, pp. 478–487, Dec. 2024.https://doi.org/10.14741/ijcet/v.14.6.11

[13] YM Ajiji, GT Cirella, FJ Galas, HM Jadah, and AO Adeniran, "Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise", International Journal of Advanced Networking and Applications, vol. 12, no. 6, pp. 4750–4762, 2021,https://doi.org/0.35444/IJANA.2021.12604

[14] T. Al-Khraishi and M. Quwaider, “Performance evaluation and enhancement of VLAN via wireless networks using OPNET modeler”, arXiv, Jul. 2020.https://doi.org/10.48550/arXiv.2007.06997

[15] M. Ashmel M. Hashim, I. Tlemsani, and R. Matthews, “Higher education strategies in digital transformation,” Education and Information Technologies, vol. 27, pp. 3171–3195, 2022,https://doi.org/10.1007/s10639-021-10739-1
[16] E. Abad-Segura, LMC Benavides, JTJ Arias, AMD Arango-Serna and DJW Burgos, “Digital transformation in higher education institutions: A systematic literature review”, Sensors, vol. 20, no. 11, Art. 3291, Jun. 2020,https://doi.org/10.3390/s20113291
[17] L. Yang, X. Hua, Y. Yang, "On structure and substructure fault tolerance of star networks", J. Supercomput., vol. 79, pp. 9157–9179, May 2023,https://doi.org/10.1007/s11227-022-05036-8
[18] Wikipedia contributors, "Star network", Wikipedia, The Free Encyclopedia, accessed Jul. 2025.
[19] L. Yang, X. Hua, and Y. Yang, “On structure and substructure fault tolerance of star networks,” Journal of Supercomputing, vol. 79, pp. 9157–9179, May 2023,https://doi.org/10.1007/s11227-022-05036-8
[20] G. Li et al., “Typical Networking Architectures for Campus Networks and Case Practice”, in Smart Campus – Digitalization and Data Analytics, A. Unal, P. Mitra, and Y. Demchenko, Eds., Springer, 2023, ch. 15, pp. 245–260.https://doi.org/10.1007/978-981-19-3029-4_15

AUTHOR BIOGRAPHY

<table>
<tr><td>  </td><td>**Fitria** is a lecturer in the Department of Informatics Management, Surabaya State University, Indonesia. She earned a Bachelor of Education (S.Pd.) from Makassar State University in Informatics and Computer Engineering. She earned a Master of Education (M.Pd.) from Makassar State University in Technology and Vocational Education. She also earned a Doctorate (Dr.) from Makassar State University in Vocational Engineering Education. Her primary research interests are the Development and Implementation of Online Learning Models. She can be contacted via email at fitriafitria@unesa.ac.id.</td></tr>
<tr><td>  </td><td>**M Adamu Islam Mashuri** is a lecturer at the Department of Informatics Management, Surabaya State University, Indonesia. He earned his Bachelor of Applied Engineering (S.Tr.T) from the Surabaya State Electronics Polytechnic (PENS) in Telecommunication Engineering, Surabaya in 2021. He also earned his Master of Applied Computer (M.Tr.Kom) from the Surabaya State Electronics Polytechnic (PENS) in Informatics and Computer Engineering, Surabaya in 2023. He mainly researches the Internet of Things and Artificial Intelligence. He can be contacted via email: mmashuri@unesa.ac.id.</td></tr>
<tr><td>  </td><td>**Rosita** is a lecturer in the Department of Informatics Management, Surabaya State University, Indonesia. She earned a Bachelor of Education (S.Pd.) from Surabaya State University in Information Technology Education. She also earned a Master of Education (M.Pd.) from Surabaya State University in Vocational Technology Education. Her primary research interests are the Development of Computer-Based Learning Media and Innovative Technology-Based Learning Models. She can be contacted via email at rositarosita@unesa.ac.id.</td></tr>
</table>