Ambidextrous: Journal of Innovation, Efficiency and Technology in Organizations

https://journal.takaza.id/index.php/ambidextrous

Vol. 5, no. 3, 2026 , pp. 621-633
E-ISSN: 3031-7002

E-mail:ambidex@takaza.id

WLAN Network Design and VLAN-Based Segmentation for Network Management Optimization at PT. Halia Teknologi Nusantara

Muhammad Firgi Maula Alfadil, Hafdiarsya Saiyar
Program Studi Teknologi Informasi Universitas Bina Sarana Informatika Kota Jakarta
Corresponding Author e-mail : muhammadfirgi131@gmail.com

Article History:
Received: 16-10-2026
Revised: 01-11-2026
Accepted: 01-11-2026

Keywords: Access Control List, Cisco Packet Tracer, Network Security, Virtual Local Area Network, Wireless Local Area Network

Abstract *:The development of information technology requires companies to have a secure, structured, and easy-to-manage computer network. This study aims to design a Wireless Local Area Network (WLAN) based on Virtual Local Area Network (VLAN) to optimize network management and security at PT. Halia Teknologi Nusantara. The study uses a quantitative approach with a simulation-based experimental research type. The study population includes the company's network infrastructure on three floors, while the sample consists of a running network scheme and a proposed network design. The research instruments include Cisco Packet Tracer, observation guidelines, and interviews. Data are analyzed descriptively through connectivity testing, inter-VLAN communication, and the application of Access Control List (ACL). The results show that devices in the same VLAN can communicate, access from the Operation VLAN to the internal technical VLAN is successfully blocked, and administrators can access other VLANs according to the configuration. In conclusion, the WLAN design based on VLAN and ACL supports network segmentation, access control, and more structured network management. However, its effectiveness on physical infrastructure still requires direct testing.*

How to Cite : Muhammad Firgi Maula Alfadil, Hafdiarsya Saiyar . (20xx). WLAN Network Design and VLAN-Based Segmentation for Network Management Optimization at PT. Halia Teknologi Nusantara. 5(3). Pp 621-633 https://doi.org/10.61536/ambidextrous.v5i03.963

https://doi.org/10.61536/ambidextrous.v5i03.963

This is an open-access article under theCC-BY-SA License.

Introduction

The development of information technology encourages companies to have a secure, structured, and easy-to-manage computer network infrastructure. Computer networks play a crucial role in supporting data exchange, communication between devices, and access to company resources. However, the use of a flat network architecture, a network that places devices in a single segment without separation based on function or operational needs, can cause problems such as high broadcast traffic, network management difficulties, and increased security risks. Zaidan and Dafitri (2025) explain that

networks that have not implemented segmentation can face challenges in terms of security and network management. This problem is also relevant to the research of Nabawi et al. (2025), which discusses the use of VLAN trunking to separate networks between divisions and limit communication between segments. Therefore, a network design is needed that can separate devices based on operational needs while supporting more effective data communication management.

One technology that can be applied to address these issues is the Virtual Local Area Network (VLAN), a technology that allows a physical network to be divided into several logical segments. Implementing a VLAN can help limit broadcast domains, improve access control, and simplify network management. Sitohang and Pangaribuan (2025) demonstrated that implementing a VLAN can support traffic segmentation and improve network security. In line with this, Agustio and Nainggolan (2023) discussed the implementation of a VLAN combined with an Access Control List (ACL) to filter network access. In Wireless Local Area Networks (WLANs), VLAN segmentation can be used to separate wireless access based on user function and needs. In addition to segmentation, access point placement also needs to be considered to support the coverage and quality of wireless connectivity (Ningsih et al., 2025). Thus, WLAN design needs to consider the network structure, access control, and user connectivity needs.

The network issue was discovered at PT. Halia Teknologi Nusantara, a company engaged in industrial technology, procurement, consulting, and technical training. Based on observations, the company's network had not implemented adequate segmentation, resulting in most devices remaining within the same network segment. Furthermore, the network on each floor used internet connections from different service providers: IndiHome with a bandwidth of 75 Mbps on the first floor, Biznet with 200 Mbps on the second floor, and Oxygen with 25 Mbps on the third floor. This condition presented challenges in structured network management, particularly in monitoring devices and managing access according to the company's operational needs.

Another issue is the lack of network segment-based access restrictions, potentially allowing employee and guest devices to share the same network. Network security still relies on built-in firewalls on Optical Network Terminal (ONT) modems and WPA2-PSK encryption on access points, without advanced segmentation and access control configuration. This situation potentially increases the risk of unauthorized access to corporate resources and the spread of malicious software. Furthermore, the limited capacity of network devices to handle multiple users can impact network performance. Therefore, a more structured WLAN design through VLAN segmentation and access restrictions is needed to support security and ease of network management.

To address these issues, this study employed a simulation-based experimental approach with Cisco Packet Tracer. The network design included the creation of a WLAN topology, VLAN configuration to separate internal employee and guest networks, the implementation of inter-VLAN routing to regulate communication between segments, and the use of ACLs to restrict access to company resources. Amran et al. (2024) also used Cisco Packet Tracer in the network design and testing process to simulate topologies and test device configurations without using physical infrastructure. Setiawan et al. (2024) also used Cisco Packet Tracer simulation in VLAN design, DHCP, and network connectivity testing. This simulation approach aligns with Smera and Sandeep (2022), who discussed the application of simulation in computer network research. Thus, simulation can be used to evaluate designs and identify possible configuration errors before physical implementation.

This research aims to produce a more structured, secure, and easy-to-manage VLAN-based WLAN infrastructure design at PT. Halia Teknologi Nusantara. The urgency of this research lies in the company's need to improve network management efficiency, reduce the risk of unauthorized access, and separate network access according to user needs. The novelty of this research lies in the adjustment of the WLAN segmentation design to the company's network conditions, especially the separation of internal employee and guest networks accompanied by the implementation of ACL and testing via Cisco Packet Tracer. The results of this research are expected to be a reference for network design that can be considered for physical implementation in the company.

Method

This study uses a simulation-based experimental approach to design a Virtual Local Area Network (VLAN)-based Wireless Local Area Network (WLAN) at PT. Halia Teknologi Nusantara.

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Simulations were conducted using Cisco Packet Tracer to design the topology, configure VLANs, inter-VLAN routing, and Access Control Lists (ACLs), and test network connectivity and access restrictions. The use of simulation allows network designs to be tested in a virtual environment before being physically implemented. This approach aligns with Smera and Sandeep (2022), who discussed the use of simulation in network design testing.

The research instruments included Cisco Packet Tracer and observation and interview guidelines to obtain information about the company's network conditions. Data collection was conducted through observations of network topology and devices, interviews with operational personnel and employees, and literature studies. According to Creswell and Creswell (2018), the selection of data collection techniques needs to be tailored to the research objectives and approach. Data were analyzed descriptively by comparing the current network and the proposed design based on the results of connectivity testing within VLANs, inter-VLAN communication, and ACL implementation.

The research object is the computer network infrastructure of PT. Halia Teknologi Nusantara, which includes the network on the first, second, and third floors. The research sample consists of a running network schematic and a proposed network design simulated using Cisco Packet Tracer. The object selection is based on network problems identified through observation, particularly the lack of network segmentation and access restrictions based on user needs.

The research procedure consists of four stages. First, network requirements analysis based on observations and interviews. Second, WLAN topology design and SSID and VLAN mapping according to company needs. Third, network simulations are running and the configuration of the proposed design, which includes VLANs, inter-VLAN routing, and ACLs. Fourth, device connectivity within the same VLAN, inter-VLAN communication, and access restrictions on company resources are tested. The test results are used to evaluate the suitability of the design to the company's network needs.

Results and Discussion

Proposed Network

In an effort to optimize network management and improve network security on the PT. Halia Teknologi Nusantara network, the author proposes a new network design by replacing...*router*, the addition of managed switches, Access Points that support VLAN features as well as the implementation of Virtual Local Area Networks (VLANs) to break down the network into several different network segments and the implementation of Access Control Lists (ACLs) to improve security by limiting each network segment's access to company resources.

Network splitting is done by dividing the company network into several segments.*VLAN*For employee divisions and guest network segments, each VLAN segment on the network is distributed via SSIDs that have been configured with each VLAN on the Access Point.

Access Control List(ACL) is implemented on Ruijie routers which functions to limit communication between network segments and prevent unauthorized access to internal company resources by unknown devices.

1. Network Topology

In the proposed network topology design proposed by the author, in order to optimize the management and security of the PT. Halia Teknologi Nusantara network, the author uses a star topology with additional network segmentation based on Virtual Local Area Network (VLAN) and Access Control List (ACL).

As for the topology design, the author proposes to merge the entire network into one network infrastructure with the Ruijie router as the network management center and Virtual Local Area Network (VLAN) distribution center. Each port on the managed switch is also configured to suit its use, such as ports connected to end devices such as access points configured in access mode, while ports connected to routers are configured in trunk mode.

Each Access Point is directly connected to a managed switch on each floor, where each port on each switch has been configured for each VLAN, where each access point has been configured with a different SSID for each VLAN. The different SSIDs serve to separate the guest network and the employee network of each division, thereby increasing network security and simplifying the management and administration of the company's network.

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

The topology proposed by the author is as follows:

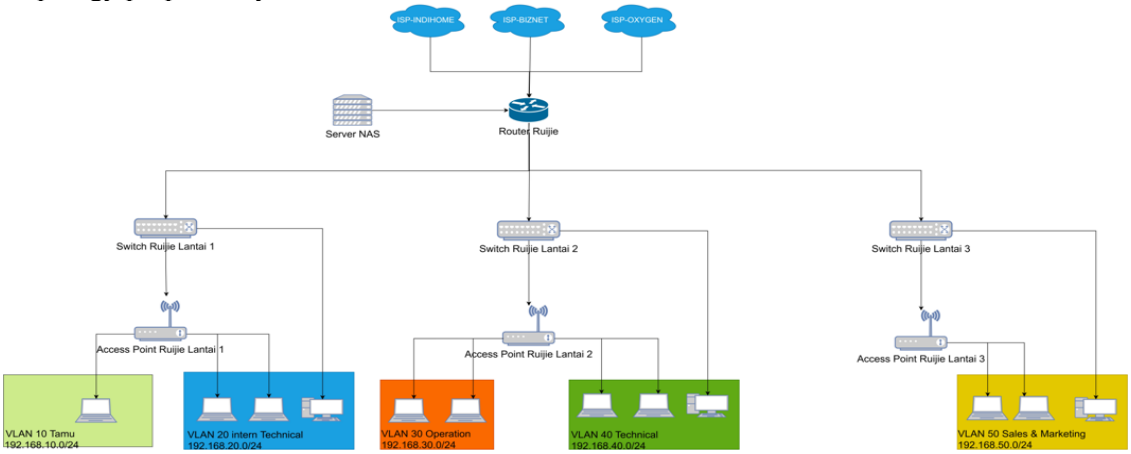


Figure 1. Proposed Network Topology
Source: Author's Documentation Results

2. Network Scheme

The proposed network schematic designed by the author illustrates communication between network devices and client devices simulated using Cisco Packet Tracer. The simulated proposed network schematic consists of a router, managed switch, access point, and end-user devices such as laptops and PCs.

In this network scheme, the Ruijie router acts as a data traffic control center as well as VLAN configuration, ACL and company network management where the managed switches on each floor and servers are connected directly to the router, while each managed switch is connected directly to the access point and employee PC on each floor.

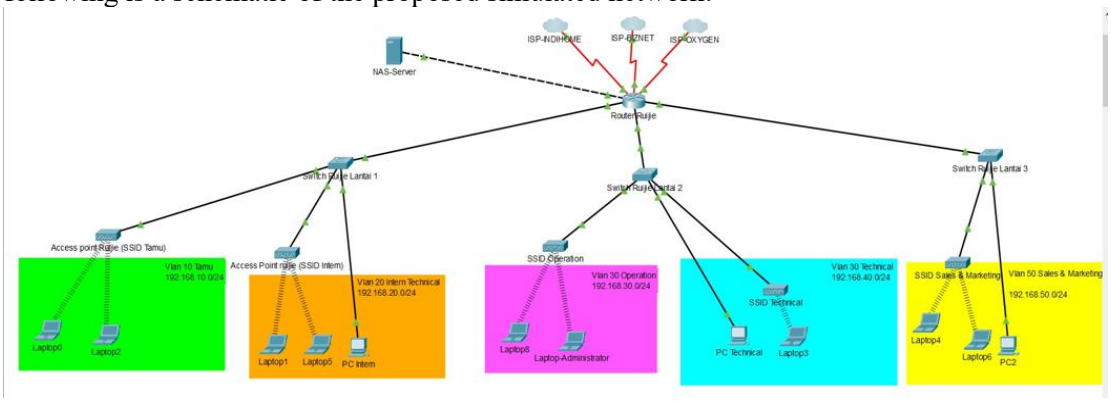
Each access point on each floor is given a different SSID according to the VLAN segment to separate the guest network and the internal employee network such as VLAN 10 for guests and VLAN 20, 30, 40 and 50 for each employee division so that it can optimize network traffic by dividing one network into several small networks which limit the distribution of broadcasts to only certain VLANs, thereby reducing the traffic load received by network devices.

Each VLAN on each floor is given a different IP address with Dynamic Host Configuration Protocol (DHCP) on each VLAN which functions to provide automatic IP addresses to end-user devices on each VLAN, except for the IT Administrator's laptop and NAS server which are given static IP addresses.

To improve network security, this network scheme also implements Access Control List (ACL) to limit access to Guest VLANs and VLANs between Employee divisions so that each VLAN cannot connect to each other unless given access, as well as disabling unused ports to minimize the risk of illegal access from unauthenticated devices.

The proposed network scheme is simulated using Cisco Packet Tracer, which aims to provide an initial overview of the network and test the proposed network scheme before it is actually implemented in the field to minimize the risk of configuration errors in the network.

The following is a schematic of the proposed simulated network:



https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Figure 2. Proposed Network Schematic
Source: Author's Documentation Results

3. Network Security

In the proposed network schematic, the author proposes several additional security systems to enhance network security against threats such as unauthorized access and data leaks, which could compromise company performance and data confidentiality. The proposed network security measures are as follows:

A. Implementation of network segmentation with Virtual Local Area Network (VLAN)

Virtual Local Area Network(VLAN) functions to divide the network into several logical network segments so that each network cannot be directly connected. In this network design, VLANs are used to create network segmentation, namely VLANs 20, 30, 40 and 50 which are intended for internal employees and VLAN 10 which is intended for guests. Each VLAN is configured with a different subnet and access to each VLAN is restricted which serves to improve and maintain data security on each network segment.

B. Implementing Access Control List (ACL) to limit Network Access

Access Control List (ACL) functions as a control on access to each VLAN on the network where ACL will limit access to VLAN 10 (Guest) so that it cannot connect to the employee VLAN and limit access to employee VLANs (VLAN 20,30,40,50) so that only VLANs that are given access can access resources on the company network.

C. Disabling the Wi-Fi Feature of the ONT Modem

In an effort to improve network security, any Wi-Fi features on the ONT modem are disabled as a step to reduce the risk of unauthorized access from unauthenticated devices via wireless.*Wireless*).

D. Turn off ports on the Router or Switch that are not in use

Deactivation*by*t which is used on network devices such as managed switches, routers and modems functions as physical protection for the network from the threat of unauthenticated network access from internal or external parties and makes it easier for administrators to monitor network connections because they only need to monitor the ports that are on.

Application Design

In this study, to demonstrate the proposed network design, the author uses Cisco Packet Tracer to simulate the network design and its configuration for testing the network design without having to change the current network configuration, thus minimizing the risk of errors in the network configuration. The configuration is carried out via the Command Line Interface (CLI) on the network device.

As for the configuration steps, they are as follows:

1. Accessing the Command Line Interface (CLI) on the router

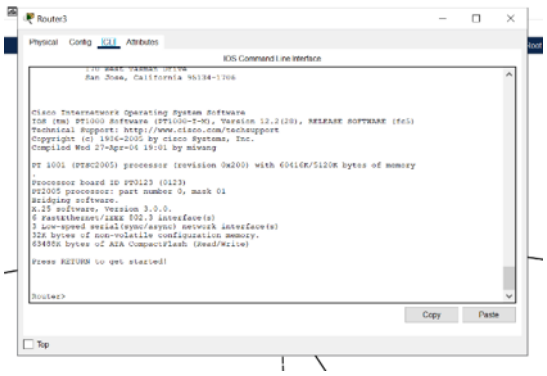


Figure 3. Router CLI Menu Display
Source: Author's Documentation Results

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

When you first access the router on Cisco Packet Tracer, the router is still in "User EXEC Mode" where to start the configuration, you need the "Enable" command on the Command Line Interface (CLI) on the router to switch from User EXEC Mode to Privileged EXEC mode.

2. Accessing Router Configuration Mode

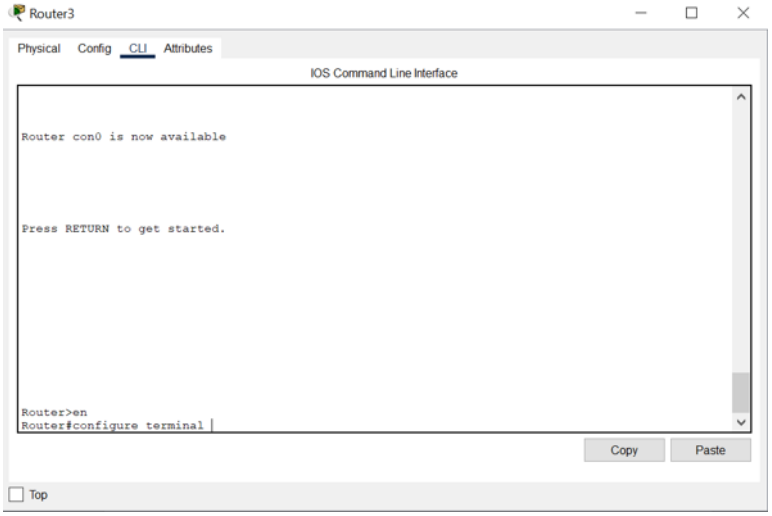


Figure 4. Accessing Global Configuration Mode on the Router

Source: Author's Documentation Results

After entering User Exec Mode, to be able to start configuring the router, you need to use the "configure terminal" to switch from Privileged EXEC mode to "mode".*Global Configuration*" on the router.

3. DHCP Configuration on Router

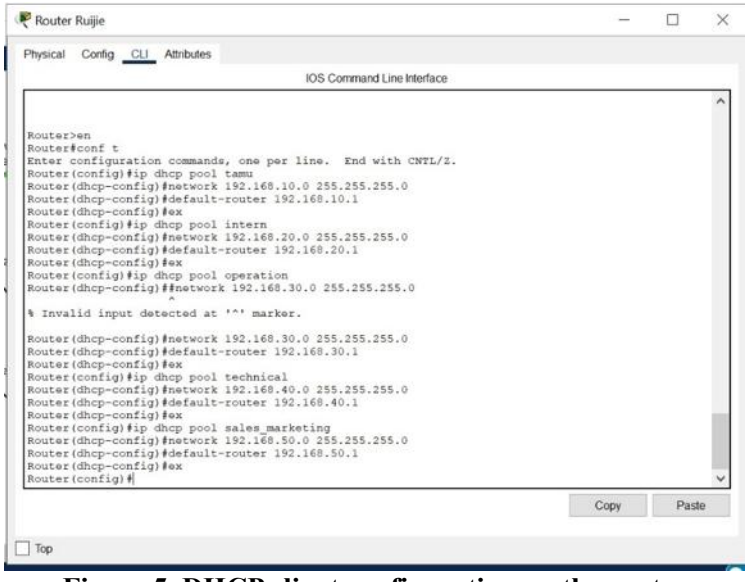


Figure 5. DHCP client configuration on the router

Source: Author's Documentation Results

So that each VLAN can get an IP address dynamically, each VLAN is configured with a different DHCP pool according to the VLAN. The configuration can be done after entering global configuration mode, then use the command "#IP DHCP pool [VLAN name]" to create a DHCP pool, then use the network [192.168.xx] command according to the IP you want to use, then use the default-router [192.168.xx] command to provide a gateway IP for each DHCP pool VLAN.

4. VLAN Configuration on Switch

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

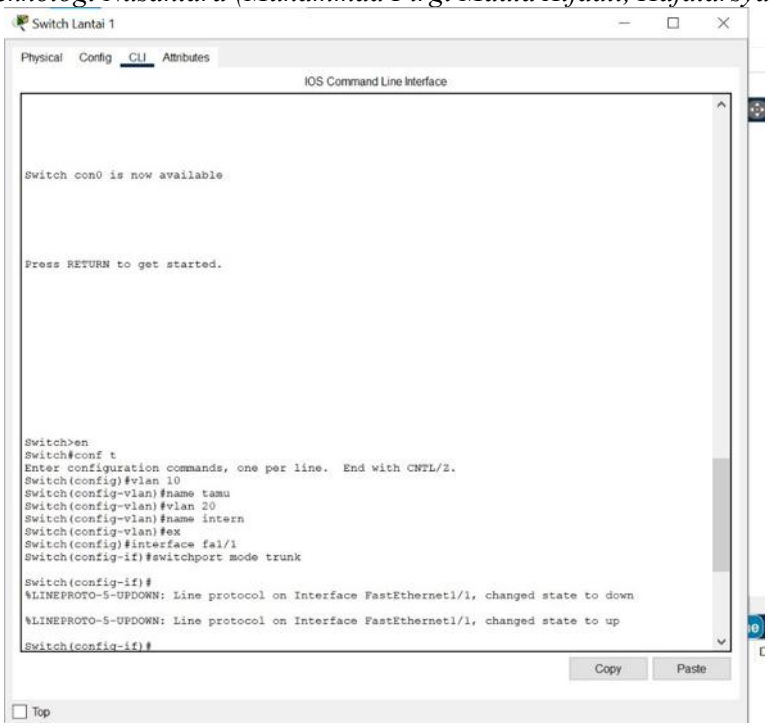


Figure 6. Configuration*VLAN on Switch*
Source: Author's Documentation Results

VLAN configuration is done by configuring it directly on the switch using the #VLAN[vlan name] command after entering global configuration mode, where each switch is configured with a different VLAN, after that select the port that will be used as a trunk/access port, the trunk port is configured as a delivery traffic path for many VLANs from the router/switch or vice versa while the access port is configured for one VLAN used for end-user devices to be able to connect to the VLAN.

An example of the access port configuration is on the 2nd floor switch where the fa2/1 port is configured as an access port used to channel VLAN 40 (technical) via cable to the PC belonging to the technical division.

```
Switch(config)#interface FastEthernet2/1
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 40
Switch(config-if)#
```

Figure 7. Access Port Configuration on the 2nd Floor Switch
Source: Author's Documentation Results

5. Inter-vlan Routing Configuration

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

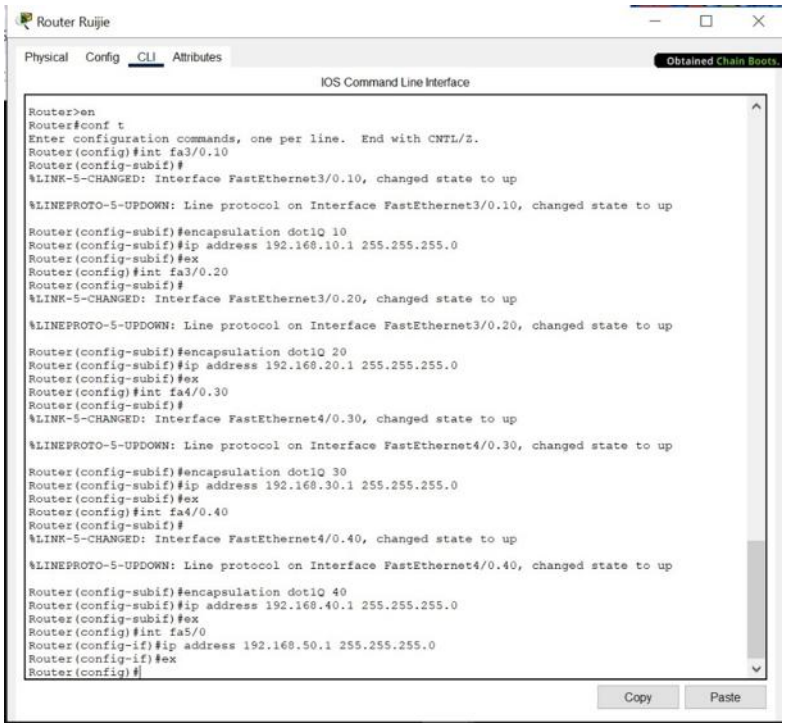


Figure 8. Inter- Configuration*VLAN Routing*
Source: Author's Documentation Results

Inter-VLAN routing configuration is done by creating a sub-interface with the command #interface [interface/.[sub-interface] on the physical interface that you want to use as the VLAN sub-interface, then use the command #encapsulation dot1Q [ID_Vlan] to allocate tags to each VLAN frame, each sub-interface is also given an IP address as the default gateway so that each VLAN on the network can be connected to each other.

6. Access Control List Configuration

```
ip access-list extended Block_vlan_tamu
 permit udp any eq bootpc any eq bootps
 deny ip 192.168.10.0 0.0.0.255 host 192.168.1.2
 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip 192.168.10.0 0.0.0.255 any
ip access-list extended Block_vlan_intern
 permit udp any eq bootpc any eq bootps
 permit ip any host 192.168.30.10
 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip 192.168.20.0 0.0.0.255 any
ip access-list extended Block_vlan_operation
 permit udp any eq bootpc any eq bootps
 permit ip host 192.168.30.10 any
 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip 192.168.30.0 0.0.0.255 any
ip access-list extended Block_vlan_technical
 permit udp any eq bootpc any eq bootps
 permit ip any host 192.168.30.10
 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
 permit ip 192.168.40.0 0.0.0.255 any
ip access-list extended Block_vlan_salesmarketing
 permit udp any eq bootpc any eq bootps
 permit ip any host 192.168.30.10
 deny ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
 permit ip 192.168.50.0 0.0.0.255 any
```

Figure 9. Access Control List Configuration
Source: Author's Documentation Results

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Access control list configuration is done on the router which is done by creating a named ACL with the command "#ip access-list extended [ACL_Name]", then if you want to limit access between VLANs or services use the command "#deny ip [192.168.xx] [wildcard mask] host [192.168.xx]" for example, if you want to limit access from the guest VLAN to the internal VLAN and the server use the command "#deny ip 192.168.10.0 0.0.0.255 host 192.168.1.2" to block access from the guest VLAN to the server and "deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255" to block access from the guest VLAN to the internal technical VLAN and add the command "#permit ip 192.168.20.0 0.0.0.255 host 192.168.1.2" so that the internal technical VLAN can access the server.

Then, to allow IT administrators to access each VLAN, use the command "#permit ip host 192.168.30.10 any" in VLAN operation to allow IT administrators to access it. Then, at the end of each ACL, use the command "permit ip [subnet VLAN] [wildcard mask] any" to allow access beyond that previously restricted.

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface FastEthernet3/0.10
Router(config-subif)# ip access-group Block_vlan_tamu in
Router(config-subif)#exit
Router(config)#
Router(config)#interface FastEthernet3/0.20
Router(config-subif)# ip access-group Block_vlan_intern in
Router(config-subif)#exit
Router(config)#
Router(config)#interface FastEthernet4/0.30
Router(config-subif)# ip access-group Block_vlan_operation in
Router(config-subif)#exit
Router(config)#
Router(config)#interface FastEthernet4/0.40
Router(config-subif)# ip access-group Block_vlan_technical in
Router(config-subif)#exit
Router(config)#
Router(config)#interface FastEthernet5/0.50
Router(config-subif)# ip access-group Block_vlan_salesmarketing in
Router(config-subif)#exit
```

Figure 10. Access Group Configuration

Source: Author's Documentation Results

After all ACLs have been configured, the next step is to enter the ip access-group on each VLAN subinterface, with the command "interface [subinterface_name] ip access-group [ACL_name] in".

Network Management

In order for the network design to run well, the author provides several suggestions regarding network management so that network stability can be maintained, the suggestions are as follows:

1. Centralized DHCP server control

IP address management on the network is done centrally on the router device via a DHCP server, so that the distribution of IP addresses for each device on each VLAN can be done dynamically, which can make it easier for IT administrators to distribute IP addresses on the company network compared to configuring IP addresses manually.

2. Device documentation and network configuration

Network device and configuration documentation is necessary to assist administrators in troubleshooting any network outages. Network documentation also serves as a guide for new IT administrators in understanding the devices and configurations on the company network.

3. *Monitoring*Network Periodically

Network monitoring is carried out periodically to ensure that every device and network performance in the company continues to run well, as well as to ensure that network security is maintained from unknown access that tries to connect to the company network.

4. Centralized Access Point Management

Each access point on the company network is configured centrally using a cloud-based network management platform, where IT administrators can configure several access points at once without having to configure each access point one by one, so that this approach can make it easier for IT administrators to carry out management and configuration such as setting SSID, VLAN or bandwidth management on network access points.

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Network Testing

Network testing in this study was carried out by testing a network simulation simulated on Cisco Packet Tracer. The purpose of network testing is to test the configuration implemented in the network simulation and to compare the test results before and after the implementation of VLAN segmentation and Access Control List (ACL) in the network design simulation.

Initial Network Testing

In this initial testing phase, the network design has not yet been integrated into a single network, and VLAN segmentation and access restrictions using Access Control Lists (ACLs) are being implemented. In this testing, the author focused on connectivity testing on network devices to ensure that each device is properly connected.

1. Ping test connection between devices

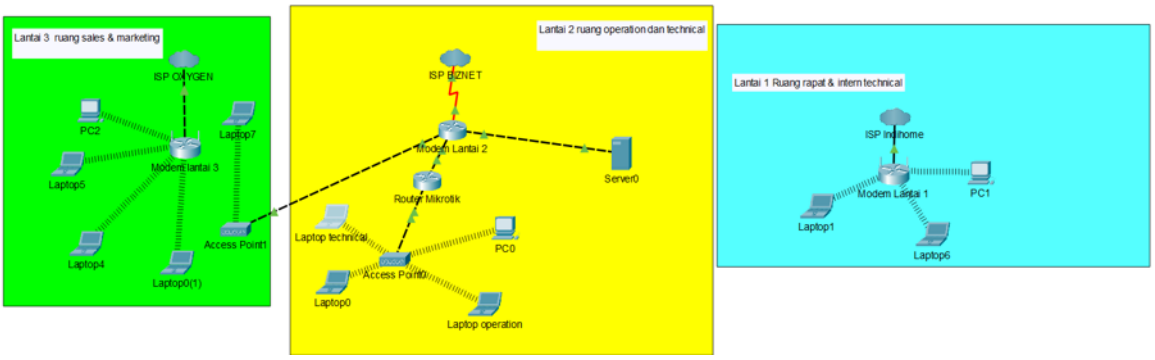


Figure 11. Simulation Before Implementation*VLAN*
Source: Author's Documentation Results

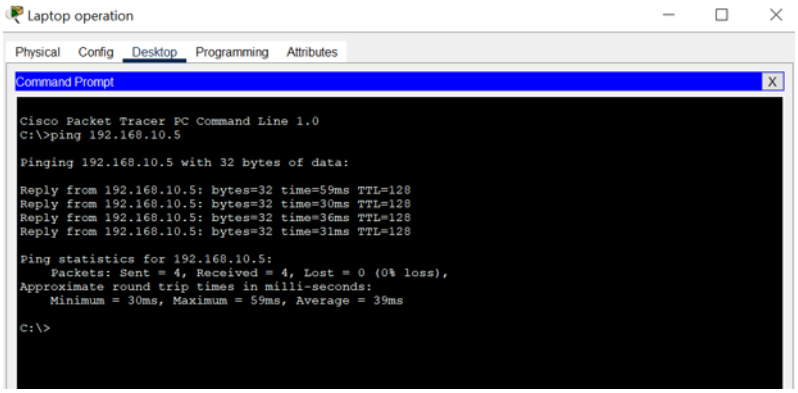


Figure 12. Testing Connections between Devices Before Implementation*VLAN*
Source: Author's Documentation Results

In this test, the author tried to test the connection between devices by using the ping command on the laptop in the operations division to the laptop in the technical section, where the ping results showed that the two devices could connect directly to each other, without any segmentation that limits network access on each segment.

Final Network Testing

In this testing phase, the author tested the proposed network design to ensure that the VLAN segmentation worked properly. The author also created several scenarios, such as testing connectivity on devices within the same VLAN, testing interVLAN routing, and testing ACLs on the network.

1. Testing Connections between Devices in One VLAN

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

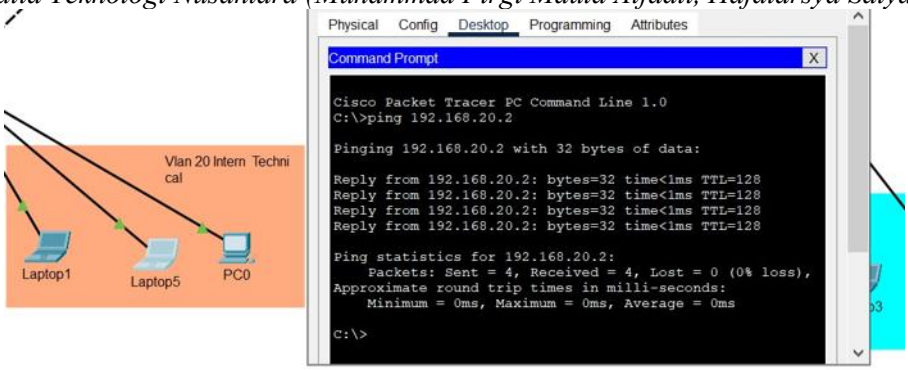


Figure 13. Testing Device Connections on the Same VLAN
Source: Author's Documentation Results

In the test above, the author conducted a test using the ping command on the device on the internal technical VLAN, where the test results showed that the devices on the internal technical VLAN could connect to each other well.

2. Testing Device Connections between Different VLANs

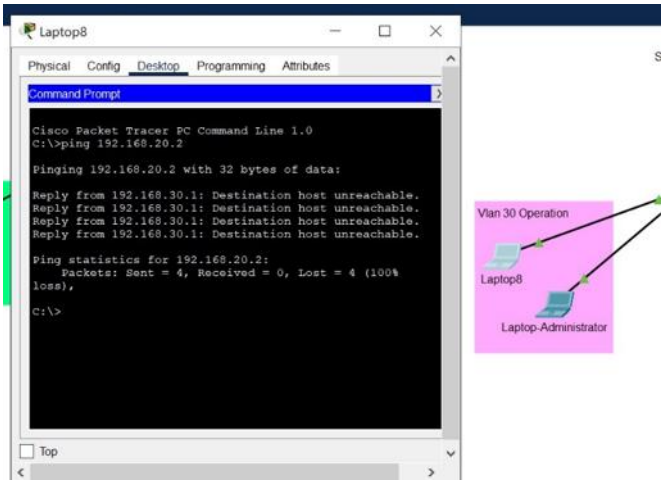


Figure 14. Testing the device connection on*Different VLANs*
Source: Author's Documentation Results

In the second test, the author conducted a test on the connection between the Operation VLAN to the internal technical VLAN using the ping command, where the test results showed that the ACL successfully blocked traffic from the Operation VLAN to the internal technical VLAN.

3. Testing Administrator Access to another VLAN

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

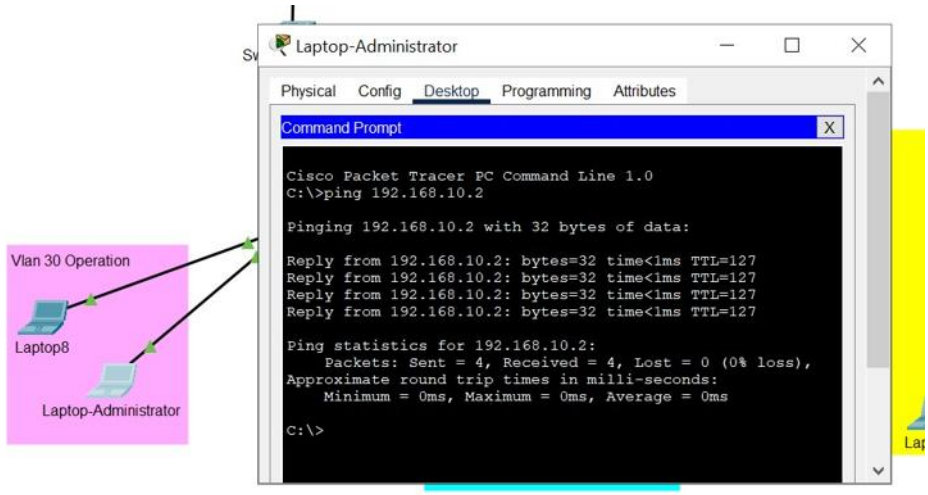


Figure 15. Testing Administrator Access to*Other VLANs*

Source: Author's Documentation Results

Based on the test results on administrator access to other VLANs, it shows that the administrator on VLAN 30 successfully accessed VLAN 10, which shows that ACL and Inter-vlan routing worked well according to the configuration.

Network Comparison

To clarify the test results, the author compared the network before and after implementing VLANs. This comparison covered: network structure, network segmentation, security, network management, and broadcast traffic.

Table 1. Network Comparison

Source: Author's Documentation Results

Aspect	Before VLAN Implementation	After VLAN Implementation
Network Structure	The network is still in the form of a flat network and has not implemented network segmentation, so that many network devices are in the same domain.	The network is divided into several network segments using VLANs based on user groups. This allows each device to be grouped based on function and needs.
Network Security	The network still does not implement access restrictions on the network, thus increasing the risk of cyber attacks, such as unauthorized access between devices and company resources.	Access to the network is regulated through the implementation of ACLs, so that only devices/network segments that are granted access can access company resources.
Network management	Network management is quite difficult because the network is still in the form of a flat network, so that many devices are still in the same domain, thus complicating the network management process.	Network management can be done more easily and in a structured way, because each device is grouped based on VLAN, making it easier to manage and troubleshoot the company network.
Broadcast Traffic	Broadcast traffic is still very high because there are still many devices in the same broadcast domain, which causes broadcast packets sent by devices to be received by many devices in the same broadcast domain so that broadcast traffic becomes high.	Broadcast traffic is limited to each VLAN, so that broadcast traffic does not spread directly throughout the network.

Conclusion

This research produces a Wireless Local Area Network (WLAN) network design based on

https://doi.org/10.61536/ambidextrous.v5i03.963
This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license

Virtual Local Area Network (VLAN) to optimize network management and security at PT. Halia Teknologi Nusantara. Based on the simulation results using Cisco Packet Tracer, the implementation of VLAN allows the separation of employee networks based on divisions and guest networks into different segments, thereby limiting the spread of broadcast traffic on each VLAN. The implementation of inter-VLAN routing supports communication arrangements between segments, while Access Control List (ACL) is used to limit access according to the established network policy. The test results show that devices in the same VLAN can communicate well, access from the Operation VLAN to the internal technical VLAN is successfully blocked, and administrators can access other VLANs according to the configuration. These results indicate that the proposed design can support more structured network management and improve access control to the company's internal resources. Practically, this design can be a reference for companies in integrating inter-floor networks, managing IP addresses through DHCP, documenting configurations, and carrying out regular network monitoring.

This study has limitations because the testing was conducted using Cisco Packet Tracer simulations, so the results do not fully reflect the physical implementation conditions, including the actual performance of the wireless network, device capacity, connection stability, and quality of service when used by multiple users simultaneously. Furthermore, the study does not provide quantitative measurements of changes in broadcast traffic, latency, throughput, and network security levels before and after the design is implemented. Therefore, further research is recommended to conduct direct implementation and testing on corporate infrastructure, accompanied by Quality of Service (QoS) measurements, user load testing, and evaluation of the effectiveness of ACL rules for various access scenarios. Further developments could also include centralized access point management, real-time network monitoring, and bandwidth management based on the needs of each division. With this advanced testing, it is hoped that the network design can be evaluated more thoroughly before being implemented as a corporate operational infrastructure.

Bibliography

Agustio, D. P., & Nainggolan, E. R. (2023). Penerapan Virtual Local Area Network pada jaringan MAN dengan metode filtering berbasis Access Control List di Dinas Komunikasi dan Informatika Kota Serang. Jurnal Komputer Antartika, 1(1), 32–38. https://doi.org/10.70052/jka.v1i1.5

Amran, A., Zuhria, S. A., Ramadhani, M. D., Susmawati, P. R., Diana, S. N., Ulum, L. B., Aulita, R. N., Firdaus, F. A., Latifah, D., & Astutik, A. (2024). Simulation of local area network (LAN) computer network using Cisco Packet Tracer at SMP Negeri 1 Grabagan. Jurnal Mandiri IT, 12(3), 175–182. https://doi.org/10.35335/mandiri.v12i3.260

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Nabawi, F., Juliyanto, & Fahlevi, M. R. (2025). Perancangan jaringan Virtual Local Area Network (VLAN) trunking untuk isolasi beda divisi dengan switch Cisco pada KPID DKI Jakarta. Device, 15(2), 250–260. https://doi.org/10.32699/device.v15i2.10447

Ningsih, S., Satra, R., & Gaffar, A. W. M. (2025). Analisis penempatan access point pada jaringan Wireless LAN Fakultas Agama UMI. Jurnal Minfo Polgan, 13(2), 2463–2472. https://doi.org/10.33395/jmp.v13i2.14510

Sitohang, S., & Pangaribuan, H. (2025). Analisis keamanan dan kinerja jaringan pada implementasi VLAN sebagai upaya segmentasi trafik menggunakan Cisco Packet Tracer. Jurnal Sains Informatika Terapan, 4(2). https://doi.org/10.62357/jsit.v4i2.673

Smera, C., & Sandeep, J. (2022). Networks simulation: Research based implementation using tools and approaches. In 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT). IEEE. https://doi.org/10.1109/GCAT55367.2022.9972119

Zaidan, Y., & Dafitri, H. (2025). Efektivitas segmentasi menggunakan VLAN dan inter-VLAN routing pada jaringan komputer di perusahaan. Journal Computer and Technology, 3(2), 102–110. https://doi.org/10.69916/comtechno.v3i2.417

This open-access article is distributed under a Creative Commons Attribution (CC-BY-SA) 4.0 license