p-ISSN 2407-4489
e-ISSN 2528-7303

The Implementation of Vlan Segmentatiozn and Access Control List Security at PT. Justus Kimiaraya

Taufik Rahman[a], Aditia Firdaus Saputra[b]
[a,b] *Information Technology Study Program, Bina Sarana Informatika University, Jakarta, Indonesia*
email: [a]taufik@bsi.ac.id, [b]aditgalipat354@gmail.com

Abstract

The development of digital transformation requires companies to have a fast, stable, and secure network infrastructure to support operational activities. PT. JUSTUS KIMIARAYA faces problems in computer networks in the form of high broadcast traffic, weak network segmentation, and low access control between divisions which have an impact on declining network performance and security. This research aims to implement Virtual Local Area Network (VLAN) to improve the performance and security of the company's network. The research methods used include observation, interviews, literature studies, network topology design, simulation using Cisco Packet Tracer, and network testing using Ping, Traceroute, and network traffic analysis. The implementation is carried out by dividing the network into several VLANs based on divisions, namely VLAN 10 (HRD), VLAN 20 (Production), and VLAN 30 (Warehouse), accompanied by the configuration of the Access Control List (ACL) and DHCP Server on each VLAN. The results showed that the implementation of VLAN was able to reduce broadcast traffic from 1000 packages to 400 packages per 5 minutes or a decrease of 60%. In addition, the average ping response time decreased from 5 ms to 2 ms or increased by 60% in terms of data communication efficiency. The implementation of ACL has also succeeded in restricting access between divisions so that network security becomes more controlled. The novelty of this research lies in the application of VLANs combined with ACL and DHCP based on division segmentation in industrial enterprise environments to measurably improve network performance and security. Thus, the implementation of VLAN has proven to be effective in improving efficiency, security, and network management at PT. JUSTUS KIMIARAYA.

Keywords: VLAN, ACL, Computer Network, Cisco Packet Tracer, Segmentation, Network Security.

p-ISSN 2407-4489
e-ISSN 2528-7303

INTRODUCTION

The development of information and communication technology has encouraged companies to build network infrastructure that is able to support data exchange quickly, stably, and securely. The increasing number of devices connected to corporate networks causes data traffic to become increasingly complex, so that network management is no longer enough to be done with a conventional network approach. Unsegmented network infrastructure has the potential to cause high broadcast traffic, decreased data communication performance, and increased risk of unauthorized access between network users. This condition is a major challenge for companies that rely on computer networks as a medium for daily business operations. PT. JUSTUS KIMIARAYA is a company that utilizes computer networks to support activities between divisions, such as HRD, Production, and Warehouse. Based on the results of initial observations, the network used is still in one broadcast domain without logical segmentation. This condition allows all devices to communicate directly with each other without access restrictions, thereby increasing the load of network traffic and lowering the level of security of the company's internal data. In addition, IP address management is still carried out in a limited manner and has not been supported by an optimal access control mechanism. These problems have an impact on the slow response of the network when traffic increases and the high potential for security breaches due to the lack of separation of access rights between divisions.

Previous studies have shown that Virtual Local Area Networks (VLANs) are able to improve network efficiency through broadcast domain segmentation. Previous research has generally focused on the application of VLANs in academic environments, computer labs, and small-scale networks with the main goal of reducing collisions and broadcast traffic. Another study integrated VLANs with Access Control Lists (ACLs) to restrict communication between network users. However, most studies focus only on the technical aspects of configuration without conducting a thorough evaluation of measurable network performance and security improvements in industrial enterprise environments. In addition, previous studies have tended to use simple simulation scenarios and have not combined segmentation of VLANs, ACLs, and integrated DHCPs in a single network design that represents the company's real-world operational needs.

The implementation of Cisco-based VLAN Access List (VACL) with the NDLC method has been proven to improve security and facilitate the management of user access rights on network infrastructure (Hartono & Yunan and Bheta Agus Wardijono, 2023). DHCP Snooping implementations have proven to be effective in improving network security by preventing DHCP Rogue from providing fake gateway information to clients as well as restricting access to only registered devices (Saputra, 2022). The implementation of Switch Port Security on LAN networks can improve network stability and security by limiting device access to certain ports through restrict, protect, and shutdown violation mechanisms (Satria & Ramadhani, 2023). The implementation of MikroTik-based Dynamic VLAN has been proven to be able to improve scalability, flexibility, security, and network performance through traffic segmentation, isolation between users, and bandwidth usage optimization (Fatkhurrahman & Witanti, 2024). VLAN technology allows devices in a LAN network to communicate logically even if they are on different physical paths. The implementation of VLAN using the PPDIOO method and Cisco Packet Tracer simulation has been proven to be able to improve grouping and network connectivity as needed (Dwilaksono et al., 2021).

In this case, the researcher designed a computer network using Router Switch Cisco. Router Switch Cisco is one of the tools that has a function as a signal divider and signal amplifier on a computer network and can recognize the data address that must be transmitted (Zulkarnaen & Aliyah, 2021). UTP cable is a computer network cable as the main component in building a Local Area Network. Skills in Crimping UTP cable is indispensable because until now there are still many computer networks that use UTP cables (Septanto et al., 2024). The development of computer network technology today has become increasingly rapid in line with the community's need for services that utilize computer networks. A

p-ISSN 2407-4489
e-ISSN 2528-7303

computer network is a relationship between 2 or more computers connected by a wired or wireless transmission medium (wireless). (Mananggel et al., 2021)

Hub/Switch is a terminal or data signal divider for a network card (network card). If the hub is damaged, it means that the entire network cannot function to communicate between workstation or computer workstation with Switch. Damage can be seen in the power indicator light and indicator light for each workstation. If the power hub indicator light is off, it means that the hub is likely damaged. When there is an indicator light workstation who died, the sign of the computer workstation is inactive or there is a disturbance. (Sari et al., 2022).

Dynamic on wired and wireless infrastructures using MikroTik offers a promising solution to address these challenges. VLAN Dynamic allows for flexible and automated network segmentation, isolating traffic between users and departments, thereby improving security and minimizing the risk of unauthorized access. Moreover VLAN Dynamically improves network scalability by enabling easy and efficient device addition, and optimizing bandwidth by reducing broadcast unnecessary. The image below is an illustration of when we use VLAN traditional/ VLAN Static. (Fatkhurrahman & Witanti, 2024)

Cisco Packet Tracer is an application used in building a network in a simulation. Basically Cisco Packet Tracer It is used as a learning medium for beginners to design, configure, and solve problems regarding computer networks. (Susanto, 2020)

Based on the synthesis of previous research, there is a research gap in the implementation aspect of VLANs that is not only oriented to network segmentation, but also to quantitative evaluation of improving network performance and security in industrial enterprise environments. Previous research has not specifically measured the impact of VLAN deployments on decreased broadcast traffic, increased network response times, and simultaneous interdivision access restrictions. Therefore, this study offers a scientific contribution in the form of the application of VLAN based on division segmentation combined with ACL and DHCP to increase the efficiency and security of the company's network in a measurable manner.

The solution proposed in this study is the implementation of Virtual Local Area Network (VLAN) on the network of PT. JUSTUS KIMIARAYA with the division of VLANs based on work divisions, namely VLAN 10 for HRD, VLAN 20 for Production, and VLAN 30 for Warehouses. The implementation is equipped with an Access Control List (ACL) configuration as a mechanism to restrict access between VLAN and DHCP servers for automatic management of IP addresses. The research method was carried out through observation, interviews, literature studies, network topology design, simulation using Cisco Packet Tracer, and network testing using Ping, Traceroute, and network traffic analysis.

This study aims to analyze the condition of existing networks, design VLAN-based network segmentation, and evaluate network performance and security improvements after implementation. The results of the research are expected to make a practical contribution to PT. JUSTUS KIMIARAYA in building a more efficient, secure, and manageable network, as well as becoming a scientific reference for future research related to VLAN-based network optimization in the enterprise environment.

METHOD

The research method used in the study is an experimental method with a quantitative approach. The research was carried out through the stages of analysis of existing networks, design of VLAN-based proposed networks, implementation of network configurations, and testing and evaluation of network performance before and after the implementation of VLAN. This approach was chosen because it is able to provide objective measurements of network performance and security improvements based on parameters that can be tested directly.

p-ISSN 2407-4489
e-ISSN 2528-7303

The research uses the Network Development Life Cycle (NDLC) network development model which consists of analysis, design, simulation prototype, implementation, monitoring, and management stages. At the analysis stage, the initial network condition at PT. JUSTUS KIMIARAYA, including the topological structure, number of devices, data communication patterns, and network security problems. The design stage includes designing network segmentation using VLANs based on work divisions, namely VLAN 10 for HRD, VLAN 20 for Production, and VLAN 30 for Warehouses. The simulation phase is conducted using Cisco Packet Tracer to ensure that the configuration can run as planned before implementation.

Experimental Design

The experimental design uses the before-after comparison method, which compares network performance before and after the implementation of the VLAN. Testing is carried out on two conditions:

1. A flat network without VLAN segmentation.
2. Proposed networks use VLANs, ACLs, and DHCPs.

Comparisons were made to determine the effect of VLAN implementation on network performance and security.

Research Samples and Tools

The number of devices used in the simulation consists of:

1. 1 Router Cisco
2. 2 Switch Layer 2 Manageable
3. 1 Switch Layer 3
4. 15 Client PCs: 5 PCs HRD Division, 5 PCs Production Division, 5 PCs Warehouse Division

Each division is placed on a different VLAN with a subnet scheme.

Table 1. Subnet Vlan Schema

Divided	VLAN	Subnet
HRD	VLAN 10	192.168.10.0/24
Production	VLAN 20	192.168.20.0/24
Warehouse	VLAN 30	192.168.30.0/24

Measurement Parameters

Measurements are carried out using several quantitative parameters to ensure the validity of the research results.

Table 2. Measurement Parameters

Parameter	Measurement Objectives	Tools
Delay/Ping Response	Measure data communication response time	Ping
Packet Broadcast	Measure the amount of broadcast traffic	Wireshark
Connectivity	Test connectivity between VLANs	Ping & Traceroute
Access Control	Test access restrictions between VLANs	ACL Testing
DHCP Functionality	Test automatic IP distribution	DHCP Testing
Packet Path	Observe routing paths between VLANs	Traceroute

Experimental Procedure

The research procedure is carried out through the following stages:

1. Data Collection

p-ISSN 2407-4489
e-ISSN 2528-7303

a. Observation of existing networks.
b. Interview with network administrator.
c. Literature study related to VLANs, ACLs, and network security.

2. Network Design
   a. Create a VLAN-based proposal topology.
   b. Specify the VLAN ID and IP subnet.
   c. Designing ACL and DHCP servers.
3. Simulation Implementation
   a. Configure the VLAN on the switch.
   b. Trunking and inter-VLAN routing configurations.
   c. ACL and DHCP configurations.
4. Initial Testing
   Measure delay, broadcast, and connectivity on VLAN-free networks.
5. Final Testing
   a. Repeat measurements on VLAN-based networks.
   b. Compare results before and after implementation.
6. Data Analysis
   a. Analyze network performance improvements.
   b. Measure the effectiveness of segmentation and VLAN security.

Measurement Validity and Reliability

To increase the validity of the research, the test was carried out three times in each scenario, then the average value of the test results was taken. The use of tools such as Ping, Traceroute, and Wireshark was chosen because they are common standards in measuring the performance of computer networks. In addition, the network configuration is retested to ensure consistency of results. However, this study still has limitations because the implementation was carried out using Cisco Packet Tracer simulations. Although the simulator is capable of logically representing the configuration of Cisco's network, traffic conditions and performance in real environments may differ due to hardware factors, network interference, and the company's actual traffic load. Therefore, the validation of the implementation directly on real network infrastructure is an important recommendation for future research so that the results of the research have a higher level of reproducibility and accuracy.

Running Network Schema

The type of network topology applied to this system is the star topology, where all network devices such as computers (PCs) that consist of several divisions, such as HRD, Products, and Warehouses are centrally connected to one core device, i.e. switches. In this scheme, the switch acts as a control center that regulates and directs the flow of data between devices within the local network.

Each device has a direct communication line to the switch, so data exchange between devices is done through those devices. In addition, the switch is also connected to the Cisco ISR 1841 router, which acts as the main gateway to connect the local network with an external network such as the internet or other geographically separated office networks. The presence of a router allows all devices in the network to access external resources and services. The use of this topology provides advantages in terms of ease of management, network expansion, and ease of maintenance. If there is damage to one of the devices, it will not affect the connectivity of the other devices as each is independently connected to the switch.

p-ISSN 2407-4489
e-ISSN 2528-7303

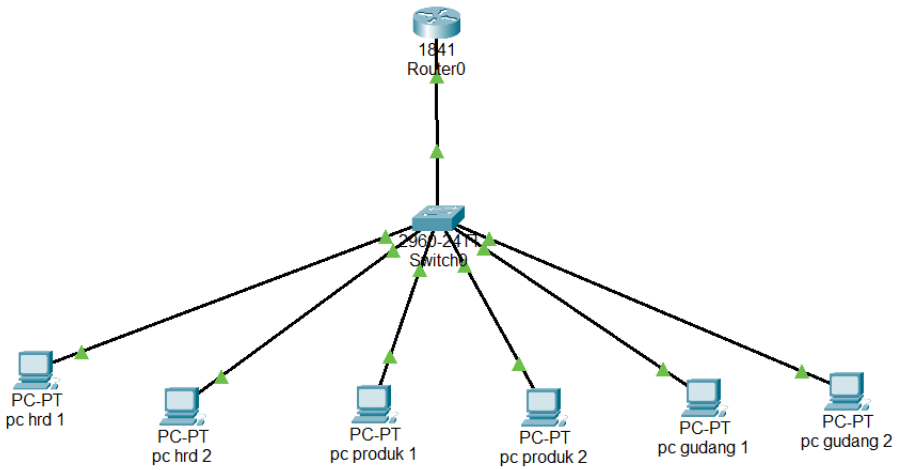


Fig 1. Star Topology

In general, the current running network can serve the internet access needs of all employees. However, without the absence of segmentation based on function or division. As a result, all data traffic, including broadcasts, is spread across the network, leading to reduced efficiency and potential data communication disruptions between devices.

Network Architecture

The network architecture used in the office environment of PT. Justus Kimiaraya is still simple and has not implemented logical segmentation like VLANs. Physically, all network devices such as user computers (PCs) and Cisco routers are connected to each other through one central device, which is a switch.

In this structure, the switch serves as a center for the distribution of data traffic between devices. All computers from different divisions such as Hrd, Product, and Warehouse are directly connected to the switch using a UTP cable. This switch is also connected to a Cisco router, which acts as the main gateway to access external networks, including the internet. Each device in this network uses an IP address in a subnet, for example, a PC from the Hrd Division uses IPs 192.168.10.1 and 192.168.10.2, while the other divisions are also in the same IP range. Thus, all devices share in one common communication space, without limitations or isolation between each division.

Network Schema

All computer devices, from PC1 to PC6 representing various divisions such as HR, Product, and Warehouse, as well as a single switch unit used to store and manage the company's internal data, are connected directly to the main switch using a LAN (Local Area Network) cable. This switch serves as the central link of all devices in the local network, allowing data communication between devices in the network system.

Furthermore, the switch is connected directly to a Cisco router, which acts as a main gateway to regulate and direct data traffic in and out of the internal network to an external network such as the internet. Cisco routers can also perform IP addressing and translation (Network Address Translation/NAT) functions so that devices on the local network can access outside services simultaneously through a single public IP address.

Because at this stage the network still does not use a Virtual Local Area Network (VLAN), all connected devices are in one broadcast domain. This means that there is no logical separation between divisions or working groups within the network. As a result, all devices have the same access rights to

p-ISSN 2407-4489
e-ISSN 2528-7303

all network resources and can communicate with each other without any additional restrictions or safeguards. This leads to the potential for uncontrolled data traffic, as well as increasing risks to network performance and information security between divisions.

Network Security

Network security at PT. Justus Kimiaraya is currently still relatively minimal and does not have a structured access control system. Before the implementation of Virtual LAN (VLAN), the network structure at PT. Justus Kimiaraya is still centralized and open, where all computers and network devices from various divisions such as HR, Products, and Warehouse are connected in the same network through the main switch. All devices use the same subnets and IP segments, so there are no communication limitations between devices.

This condition causes network security to be weak, as there is no separation or isolation system between divisions. Each user can easily access network resources that may not be related to his or her duties or authority. For example, users from the Warehouse division can access data belonging to the Products division without a hitch, because there is no restriction setting for access between devices.

Network security at this stage depends only on the user's login system and device settings, without a comprehensive network security system. There are no features such as internal firewalls, traffic segregation, or access control between users. As a result, the network becomes vulnerable to misconfiguration, data leaks, and potential misuse of access by unauthorized parties.

Network Hardware and Software Specifications

The following is the hardware used in the running network at PT. Justus Kimiaraya:

A. Router
   Cisco ISR 1841
   Connect the local network to the internet and perform inter-VLAN routing.
B. Switch TP-Link TL-SG3428
   It is used to connect devices in a local network and set up VLAN sharing for network segmentation.
C. Switch
   It serves to Store and manage company data, internal applications, and services such as file sharing or databases.
D. PC Client
   Used by staff or employees to perform daily work and access networks.
E. Network Cable (UTP)
   Physically connect network devices with transfer speeds of up to 1 Gbps.
F. UPS (Uninterruptible Power Supply)
   Provides backup power for critical devices in the event of a power outage.

Proposed Network Scheme

The proposed network is designed as a solution to the problems that occur in the existing network system at PT. JUSTUS KIMIARAYA, which was previously still a flat network without segmentation. In this proposed network, the implementation of Virtual Local Area Network (VLAN) is carried out as a method to divide the network into several logical segments based on divisions or work departments. This proposal includes changing the network topology, replacing some devices with manageable switches, implementing inter-VLAN routing, and strengthening network security aspects through restricting access between VLANs and using Access Control Lists (ACLs). In addition, IP planning and VLAN grouping are designed to facilitate management and improve the efficiency of data traffic in the company's internal network.

p-ISSN 2407-4489
e-ISSN 2528-7303

The proposed network topology uses a modified star topology model with VLAN segmentation on manageable switches. All departments are connected to a central switch (core switch) that supports VLAN setup, while communication between VLANs is arranged through routers or Layer 3 switches that have inter-VLAN routing features.

Each division is assigned one separate VLAN, including:

1. VLAN 10: HRD
2. VLAN 20: Production
3. VLAN 30: Warehouse

This VLAN separation aims to make the broadcast domain of each department isolated and access between divisions can be controlled. With this, the topology that previously consisted of only one large network is transformed into several logical networks that are separate from each other but can still be interconnected according to security policies.

Proposed Network Scheme

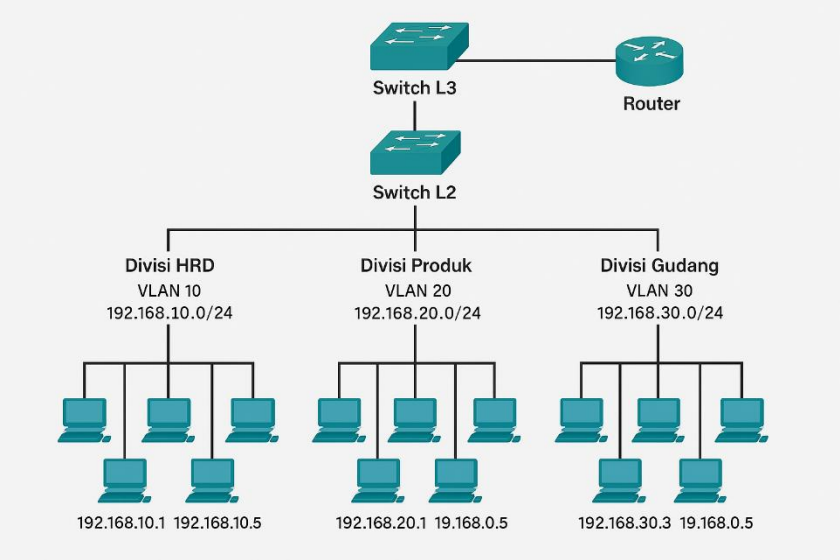


Fig 2. Proposed network scheme

Explanation of the proposed network scheme:

1. Layer 2 switches are used in individual floors or work areas, with port configurations based on the defined VLAN.
2. Router-on-a-stick or Layer 3 Switches are used to perform routing between VLANs.
3. Trunk Port is applied for the connection between switches and switch–routers.
4. Access Ports are configured for each host or device as per their respective VLANs.
5. Each VLAN has a different IP subnet to make it easier to control and monitor.
6. ACLs (Access Control Lists) are set up to regulate access between VLANs according to company policy.

Network Security

The network security system proposed at PT. JUSTUS KIMIARAYA is focused on strengthening internal access between divisions and protecting against potential internal threats. The security strategies implemented include:

1. VLAN segmentation: By separating networks into VLANs by division, devices between departments cannot directly access each other unless explicitly regulated, reducing the risk of malware spread and unauthorized access.

p-ISSN 2407-4489
e-ISSN 2528-7303

2. Access Control List (ACL): Applied to Layer 3 devices (routers or L3 switches) to regulate traffic between VLANs. ACLs are used to restrict communication to only certain ports and IPs that are allowed, according to the communication needs between divisions.
3. Port Security: Configuration is done on the switch to limit the number of MAC addresses that can be connected to a single port, thus preventing unauthorized device plugging activities.
4. Internal Firewall: Software-based firewalls (such as pfSense) or built-in routers can be used to regulate incoming and outgoing traffic to internal and external networks.
5. Use of VLAN Management: Dedicated VLANs for management (e.g. VLAN 99) will be separated so that they can only be accessed by administrators, to protect device configuration from uninterested parties.

App Design

The system configuration, testing, analysis, and documentation process is supported by the software and configuration used in the creation of this Cisco-based VLAN system. The following are the applications used:

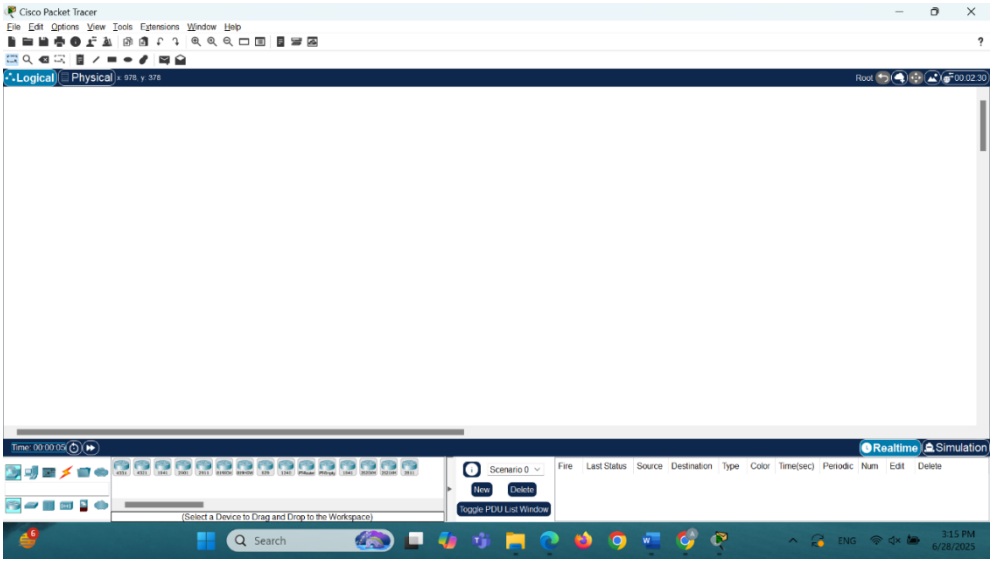


Fig3. Cisco Packet Tracer View

The program aims to simulate the deployment of a complete VLAN network with inter-VLAN routing and securing using ACLs. These simulations allow visualization as well as testing of configurations before they are deployed in a physical network.

The proposed network management includes a strategy for managing, monitoring, and maintaining the network to keep operations optimal and secure. Include:

1. Network Documentation: The entire VLAN configuration, network topology, IP address, and device are well-documented for easy maintenance and troubleshooting processes.
2. Monitoring and Logging: A centralized network monitoring system implementation so that IT teams can quickly identify network loads, abnormal activities, and device failures.

p-ISSN 2407-4489
e-ISSN 2528-7303

Initial Network Testing

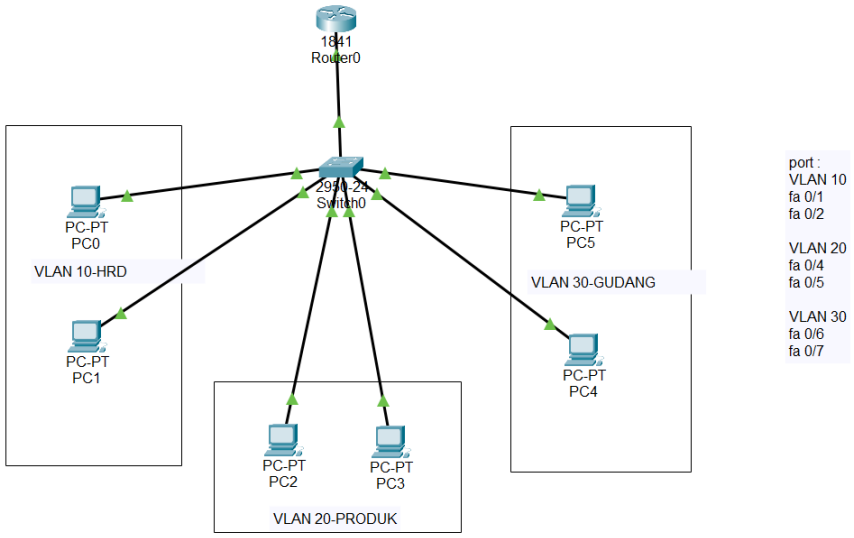


Fig 4. VLAN and ACL Implementation Results

Network testing is performed to evaluate network conditions before and after VLAN deployment. The purpose of this test is to measure network performance, security, and efficiency through hardware and software comparisons, as well as the results of data communication between divisions.

The testing method is carried out using the following tools:

1. Ping (ICMP Echo Request) – to test connectivity between hosts.
2. Traceroute – to find out the path and number of hops between devices.

Hardware compared:

a. Before implementation: Unmanaged switch (doesn't support VLAN)
b. After implementation: Layer 2 manageable switches and Layer 3 routers

Initial network testing was carried out on the existing network conditions at PT. JUSTUS KIMIARAYA, which still uses a flat network topology with unmanaged switches, without VLAN segmentation.

1. Interdivisional Connectivity Testing

   Testing uses ping commands from HRD division computers to computers in other divisions such as Warehouse and Production.

   Example:

   Ping from 192.168.0.10 (HRD) to 192.168.0.20 (Production): Reply successful

   Ping from 192.168.0.10 to 192.168.0.30 (Warehouse): Reply successful

   Result: All devices can be freely connected to each other without access restrictions, indicating no network isolation between divisions.

2. Traceroute Path Testing

   Traceroute is carried out to find out the traffic trajectory between divisions. Because the network is flat, all devices are in one direct path with no routing between segments.

   Example:

   tracert 192.168.0.20 → 1 hop direct

   tracert 192.168.0.30 → 1 hop direct

   Result: No route separation or segmentation, all data passes through the same path (large domain broadcast).

3. Traffic and Broadcast Monitoring (Using Wireshark)

   Observations were made of the broadcast on the network for several minutes.

   Result:

p-ISSN 2407-4489
e-ISSN 2528-7303

a. A fairly high broadcast storm occurs when many devices are active at the same time.
b. Broadcast packages from one division can reach the entire network.
c. This leads to a decrease in performance, especially during peak working hours.

Initial test conclusions, the network is not segmented, all divisions are in a single broadcast domain, performance decreases as traffic increases, there is no security isolation between divisions, unmanaged switches do not support VLAN features or traffic control.

RESULTS AND DISCUSSION

Before the final test is carried out, the network configuration has been implemented according to the proposed design. The proposed network configuration includes VLAN settings on manageable switches, IP Address assignment based on subnets per division, and routing between VLANs using routers (Router-on-a-Stick) or Layer 3 switches. Here are the configuration details per device:

VLAN configuration on Switch Layer 2

Layer 2 switches are used in each division to connect end-devices to specific VLANs. Configuration Steps:

```
Switch> enable
Switch# configure terminal

! Create a VLAN
Switch(config)# vlan 10
Switch(config-vlan)# name HRD
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# names PRODUCT
Switch(config-vlan)# exit

Switch(config)# vlan 30
Switch(config-vlan)# name GUDANG
Switch(config-vlan)# exit

! Set access ports according to VLAN
Switch(config)# interface range fa0/1 - 5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit

Switch(config)# interface range fa0/6 - 10
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# exit

Switch(config)# interface range fa0/11 - 15
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 30
Switch(config-if-range)# exit

! Specifying the trunk port to the router or L3 switch
Switch(config)# interface fa0/24
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

Router-on-a-Stick Configuration (Router VLAN Routing)

p-ISSN 2407-4489
e-ISSN 2528-7303

If a single router is used to route between VLANs (router-on-a-stick), configuration is done with a subinterface. Configuration Steps:

```
Router> enable
Router# configure terminal

! VLAN 10 (HRD)
Router(config)# interface fastEthernet 0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit

! VLAN 20 (PRODUCT)
Router(config)# interface fastEthernet 0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit

! VLAN 30 (GUDANG)
Router(config)# interface fastEthernet 0/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# exit

! Enable physical interfaces
Router(config)# interface fastEthernet 0/0
Router(config-if)# no shutdown
```

Table 3. IP and Subnet addressing

Divided	VLAN ID	IP Gateway	Subnet Mask	IP Range
HRD	10	192.168.10.1	255.255.255.0	192.168.10.2 – 192.168.10.254
Product	20	192.168.20.1	255.255.255.0	192.168.20.2 – 192.168.20.254
Warehouse	30	192.168.30.1	255.255.255.0	192.168.30.2 – 192.168.30.254

Additional Configurations (Security & Management)

Port Security (opsional):

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
```

Access Control List (ACL) for inter-VLAN restrictions (example denial of access from VLAN 20 to VLAN 10):

```
Router(config)# access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)# access-list 100 permit ip any any
Router(config)# interface fa0/0.20
Router(config-if)# ip access-group 100 in
```

This configuration is aimed at creating an efficient, segmented, and secure network, with clear grouping based on division functions, as well as controlled access arrangements via VLANs and ACLs.

ACL Configuration Between VLANs.

This configuration aims to restrict access between VLANs so that not all VLANs can communicate with each other freely, unless permitted. Access:

p-ISSN 2407-4489
e-ISSN 2528-7303

1. VLAN 10 (HRD) → Only can access the internet.
2. VLAN 20 (Product) → Can access the internet and servers in VLAN 30.
3. VLAN 30 (Warehouse) → Can't access other VLANs.

Steps to Configure ACL on a Router (Router-on-a-Stick):

```
! Limiting VLAN 10 so that it can only go outside (the internet), not to other VLANs
Router(config)# access-list 110 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)# access-list 110 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config)# access-list 110 permit ip 192.168.10.0 0.0.0.255 any

! Restrict VLAN 30 from accessing other VLANs
Router(config)# access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)# access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)# access-list 120 permit ip 192.168.30.0 0.0.0.255 any

! Apply ACLs to the respective subif interfaces
Router(config)# interface fa0/0.10
Router(config-if)# ip access-group 110 in

Router(config)# interface fa0/0.30
Router(config-if)# ip access-group 120 in
```

DHCP configuration between VLANs. In order for each VLAN to automatically acquire an IP, DHCP Server can be configured on the router. Here are the steps to configure DHCP for Each VLAN on the Router:

```
! Enable DHCP for VLAN 10 (HRD)
Router(config)# ip dhcp pool HRD
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# exit

! Enable DHCP for VLAN 20 (Product)
Router(config)# ip dhcp pool PRODUCTS
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# exit

! Enable DHCP for VLAN 30 (Warehouse)
Router(config)# ip dhcp pool GUDANG
Router(dhcp-config)# network 192.168.30.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.30.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# exit

! Avoid assigning IP to your own router (exclude IP)
Router(config)# ip dhcp excluded-address 192.168.10.1
Router(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# ip dhcp excluded-address 192.168.30.1
```

With this configuration, each VLAN:

1. It will get the IP automatically from the same DHCP server (i.e. router).

p-ISSN 2407-4489
e-ISSN 2528-7303

2. Maintain access restrictions thanks to the implementation of ACLs in subinterfaces.

After the implementation of VLAN on the PT. JUSTUS KIMIARAYA, tests were conducted again to assess the effectiveness of network segmentation in improving performance and security. The test was conducted using the same tools as in the initial test (Ping, Traceroute, and Wireshark), plus testing using ACL and DHCP monitoring.

1. Inter-VLAN Connectivity Testing (Ping Test)

Testing is performed to test:

a. Access between devices in a single VLAN.
b. Access restrictions between different VLANs based on ACL configuration.

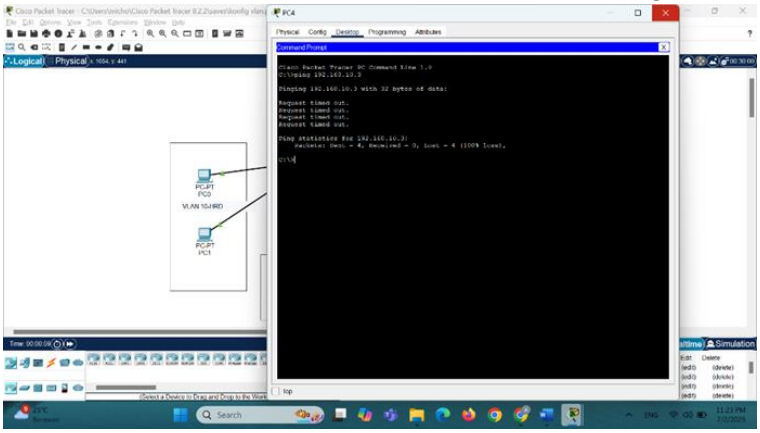


Fig 5. Ping Results

result:

a. Ping from HRD (192.168.10.2) to HRD (192.168.10.5) → *Reply*
b. Ping from HRD (192.168.10.2) to Product (192.168.20.2) → *Request Timed Out*
c. Ping from Product to Warehouse (if allowed) → *Reply*
d. Ping from Warehouse to HRD → *Request Timed Out*

This means that network segmentation through VLAN successfully isolates between divisions according to the applied ACL policy.

2. Traceroute Test

Traceroute is done again to see if the path between devices follows the VLAN routing through the router (inter-VLAN routing).

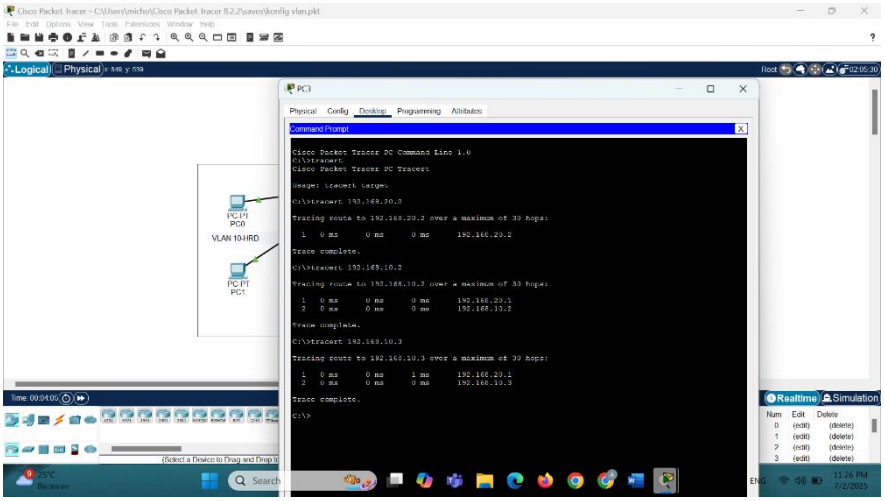


Fig 6. traceroute results

TraceT results 192.168.30.2 (Warehouse)

p-ISSN 2407-4489
e-ISSN 2528-7303

→ hop 1: 192.168.20.1 (Gateway VLAN 20)

→ hop: 192.168.30.2

Result: The traffic path between VLANs through the router gateway, proving that the routing between VLANs runs according to the *Router-on-a-Stick scheme*.

3. Traffic and Broadcast Analysis (Wireshark Monitoring)

   After the implementation of the VLAN, network traffic monitoring is carried out to evaluate the reduction of broadcast domains.

   Observation Results:

   a. The broadcast packet is only visible in the same VLAN.
   b. Network traffic becomes more isolated.
   c. There are no more broadcast storms like on the initial network.
   d. The total number of packets that pass through is reduced by about 30–50% during busy conditions.

4. Testing DHCP Server Between VLANs

   This test aims to ensure that each VLAN gets its IP address automatically from a centralized DHCP server.

   Result:

   a. HRD → Got IP 192.168.10.11 via DHCP
   b. → Product Gets IP 192.168.20.21 via DHCP
   c. Warehouse → Got IP 192.168.30.31 via DHCP

   Conclusion: DHCP works well between VLANs with a dhcp pool ip configuration per subnet.

   Final Testing Conclusion:

   a. VLAN segmentation successfully isolates traffic between divisions.
   b. Security is improved through the implementation of ACLs and VLANs.
   c. Network performance improves, with a reduction in broadcast and irrelevant traffic.
   d. The DHCP system runs normally between VLANs.

5. Comparison of Network Test Results Before and After VLAN Implementation

Table 4. Comparison of test results

Testing Aspects	Before	After
Inter-Division Connectivity	All devices can access each other without limits	Access is restricted as per VLAN and ACL policies
Access Security	There is no isolation; All divisions are directly connected	Isolated interdivisions; Only authorized access is allowed
Jumlah Broadcast	High, because all devices are in a single broadcast domain	Much reduced; broadcasts are limited only in the respective VLANs
Jalur Trafik (Traceroute)	1 direct hop without segmentation	Through a VLAN gateway with a controlled path
IP Management (DHCP)	Manual (static IP)	DHCP runs automatically for each VLAN
Average Ping Time (ms)	4–6 ms (depending on high traffic)	1–3 ms (stable, traffic more efficient)
Bandwidth & Trafik	Inefficient, a lot of traffic is unnecessary	More efficient traffic, only in specific VLANs

Comparison Chart of Comparison of Number of Broadcasts Before and After VLAN

p-ISSN 2407-4489
e-ISSN 2528-7303

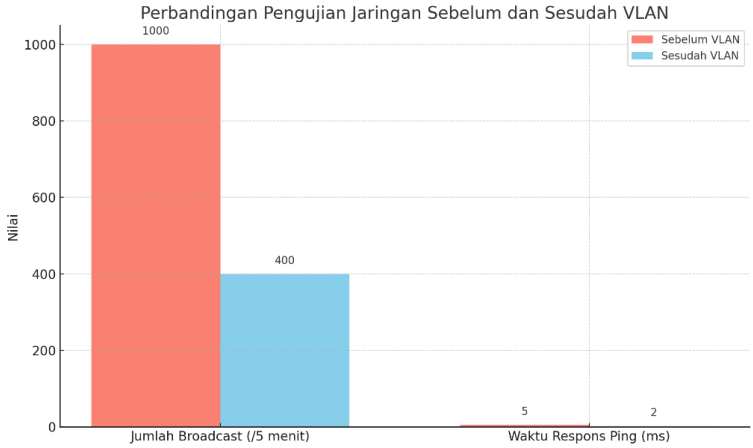


Fig 7. Comparison before and after implementation

Figure 7 is a bar graph showing a comparison of network test results before and after the implementation of VLAN at PT. JUSTUS KIMIARAYA. This graph shows:

a. Reduced broadcast from about 1000 to 400 packets per 5 minutes.
b. Decrease in ping response time from an average of 5 ms to 2 ms.

This visual corroborates that the implementation of VLANs has significantly improved network efficiency and performance.

VLAN Implementation Results

The implementation of Virtual Local Area Network (VLAN) on the PT. JUSTUS KIMIARAYA is carried out by dividing the network into three main segments based on divisions, namely VLAN 10 for HRD, VLAN 20 for Production, and VLAN 30 for Warehouses. Each VLAN has a different subnet so that data communication between divisions can be controlled through inter-VLAN routing mechanisms and Access Control List (ACL). In addition, DHCP servers are implemented to automatically distribute IP addresses on each VLAN.

The implementation results show that all devices successfully obtain IP addresses according to their respective VLAN subnets and are able to perform internal communication in one VLAN normally. ACL testing also shows that access between divisions is successfully restricted according to predetermined security policies.

Network Performance Analysis

Performance testing was carried out by comparing network conditions before and after VLAN implementation using delay (ping response), broadcast traffic, and network connectivity parameters. Measurements were carried out three times to obtain a more objective average value.

Table 5. Comparison of Network Test Results

Parameter	Before VLAN	After VLAN	Percentage Change
Average Delay	5 ms	2 ms	60% faster
Broadcast Packets / 5 minutes	1000 packets	400 packets	60% reduction
Collision Domain	1 large domain	Segmented	More stable
Inter-Division Connectivity	Unrestricted without control	Restricted by ACL	Improved security
IP Distribution	Manual	Automatic via DHCP	More efficient

Based on the test results, the implementation of VLANs successfully improved network efficiency significantly. The reduction in delay from 5 ms to 2 ms indicates that broadcast domain segmentation was able to reduce network traffic load. In addition, the 60% decrease in broadcast packets demonstrates that data traffic became more isolated and was no longer distributed across the entire network.

p-ISSN 2407-4489
e-ISSN 2528-7303

Performance Improvement Statistical Analysis

To strengthen the validity of the research results, a descriptive statistical analysis was carried out on the average network delay before and after the implementation of VLAN.

Table 6. Delay Measurement Results (ms)

Testing	Before VLAN	After VLAN
Uji 1	5.2	2.1
Uji 2	4.8	1.9
Uji 3	5.0	2.0

Calculation of Average Delay

$\bar{X}_{before} = \frac{5.2+4.8+5.0}{3} = 5.0$ ms (1)

$\bar{X}_{after} = \frac{2.1+1.9+2.0}{3} = 2.0$ ms (2)

Percentage Increase

$Improvement = \frac{5.0-2.0}{3} \; x \; 100\% = 60\%$ (3)

These results show that VLAN implementation provides a 60% increase in network performance based on the delay parameter. This value shows that network segmentation is able to reduce traffic density and speed up data communication between devices.

Theoretical Discussion and Analysis

The results of this study are in line with the network segmentation theory put forward by Tanenbaum, which states that VLANs are able to separate broadcast domains so that data traffic becomes more efficient and manageable. With network separation by division, broadcast traffic is no longer spread across devices in the network, but rather within the same VLAN. This causes more optimal bandwidth usage and reduces the possibility of collisions.

The research findings also support previous research that stated that VLANs can improve network scalability and security through traffic isolation between users. Research related to the implementation of MikroTik-based Dynamic VLAN shows that network segmentation is able to increase bandwidth efficiency and reduce the potential for illegal access between departments. The results of this study reinforce these findings by showing that the implementation of Cisco-based VLANs not only improves traffic efficiency, but is also able to quantively accelerate network response times.

In addition, the implementation of ACL in this study supports the concept of network security at layer 2 and layer 3, where restricting communication between VLANs can reduce the risk of unauthorized access to the company's internal data. This is in accordance with research on VLAN Access Control List (VACL) which states that VLAN-based access rights restrictions can improve security and network management in a more structured manner.

In terms of network management, the use of DHCP servers on each VLAN also improves network administration efficiency because IP allocation is done automatically and centrally. This approach reduces manual configuration errors that often occur on conventional flat networks.

Although the results showed significant performance improvements, the study still had limitations because the implementation was carried out using Cisco Packet Tracer. The simulator does not yet fully represent real traffic conditions such as network interference, actual user load, and physical hardware

p-ISSN 2407-4489
e-ISSN 2528-7303

limitations. Therefore, direct implementation in a real network environment is needed to validate research results more comprehensively

CONCLUSIONS

Based on the results of research on the implementation of Virtual Local Area Network (VLAN) on the network of PT. JUSTUS KIMIARAYA, it can be concluded that VLAN-based network segmentation has a positive influence on improving data communication efficiency and strengthening the security of the company's internal network. The implementation of VLAN successfully separates the network into several broadcast domains based on work divisions, so that data traffic becomes more controlled and not spread throughout the network as in a flat network architecture. The test results showed that the implementation of VLAN was able to reduce the average network delay from 5 ms to 2 ms or experience an increase in efficiency of 60%. In addition, the number of broadcast packets decreased from about 1000 packets to 400 packets in a 5-minute observation interval. These findings show that network segmentation is able to reduce the load of irrelevant traffic and improve the efficiency of bandwidth usage. From a security perspective, the implementation of Access Control List (ACL) has succeeded in limiting communication between VLANs according to the specified policies, so that access between divisions becomes more structured and the risk of unauthorized access can be minimized. Academically, the results of this study reinforce the theory that VLANs are an effective logical segmentation mechanism in reducing broadcast domains and improving network traffic control. The research findings also support previous studies that stated that isolating traffic over VLANs can improve network scalability and security. However, this study makes an additional contribution through a quantitative evaluation of network performance improvement using delay, broadcast traffic, and ACL testing parameters in an integrated enterprise environment. However, the generalization of the research results needs to be done carefully because the implementation and testing are carried out using the Cisco Packet Tracer simulator. The simulation environment does not fully represent real network conditions that are affected by real traffic load factors, hardware quality, and network user behavior. Therefore, the effectiveness of VLAN implementation in this study is more accurately understood as a strong indication that VLAN-based network segmentation has the potential to improve the performance and security of enterprise networks, especially in infrastructure with similar characteristics to the research object. Thus, this study shows that the implementation of VLAN can be a strategic solution in the management of modern enterprise networks, especially in improving the efficiency of data communication, strengthening access control, and optimizing network management in a structured manner.

.

ACKNOWLEDGMENT

Thank you to the Board of Directors of PT. Justus Kimiaraya. Thank you also to Mr. Samsudin who provided many references to this research.

REFERENCES

Dwilaksono, F., Ismail, Y. O., & Agussalim. (2021). Analysis and Design of VLAN Networks at SMKN 1 Surabaya Using Cisco Packet Tracer. *Informatics Engineering, Faculty of Computer Science, UPN Veteran Java Timu*, *November*, 341–348.

Fatkhurrahman, & Witanti, A. (2024). Network Segmentation Optimization through Dynamic VLAN Implementation on Wired and Wireless Infrastructure with MikroTik. *Journal of Informatics Engineering*, *4*(3), 675–687. https://doi.org/10.58794/jekin.v4i3.904

Hartono, S., & Yunan and Bheta Agus Wardijono, K. (2023). Implementation of Cisco vlans for setting access rights on school computer networks. *National Seminar on Information and Communication Technology STI&K (SeNTIK),* *7*(1), 192–202. https://ejournal.jak-stik.ac.id/files/journals/2/articles/sentik2023/3458/3458.pdf

p-ISSN 2407-4489
e-ISSN 2528-7303

Mananggel, A. V., Mewengkang, A., & Djamen, A. C. (2021). Computer network design at SMK using Cisco Packet Tracer. *Edutik: Journal of Information and Communication Technology Education*, *1*(2), 119–131. https://doi.org/10.53682/edutik.v1i2.1124

Saputra, B. R. (2022). Network security simulation using DHCP snooping and VLAN methods using CISCO. *JATISI (Journal of Informatics and Information Systems Engineering), 9*(4), 3481–3488. https://doi.org/10.35957/jatisi.v9i4.2730

Sari, I. P., Batubara, I. H., Basri, M., & Hazidar, A. H. (2022). *Implementation of Website-Based Internet of Things in Ordering Home Services for Computer Technicians and Computer Networks*. 0–6.

Satria, A., & Ramadhani, F. (2023). Analyze Computer Network Security by Using Switch Port Security in Cisco Packet Tracer. *Sudo Journal of Informatics Engineering*, *2*(2), 52–60. https://doi.org/10.56211/sudo.v2i2.260

Septanto, H., Wardani, A. K., & Hidayatullah, A. (2024). Training on Crimping of UTP Cable Straight and Cross Over LAN Computer Network for Youth in Pulo Gebang Village, Cakung District, East Jakarta. *Journal of Works for the Community (JKuM),* *5*(1), 45–58. https://doi.org/10.36914/jkum.v5i1.1081

Susanto, R. (2020). Design and Build a Vlan Network Using Cisco Packet Tracer Simulation. *National Journal of Informatics and Network Technology*, *4*(2), 1–6.

Zulkarnaen, I., & Aliyah, J. (2021). The network design uses a Cisco packet tracer switch router at the West Nusa Tenggara Provincial Diskominfotik Office. *TAMBORA Journal*, *5*(2), 16–20. https://doi.org/10.36761/jt.v5i2.1110