

NETWORK SECURITY OPTIMIZATION USING VLAN, FIREWALL, AND ACL AT PT. ANDALAN NIAGA EXPRESSINDO

Marsel*; Astriana Mulyani

Informatics Study Program
Universitas Nusa Mandiri, Jakarta, Indonesia
<https://nusamandiri.ac.id>
mrslsujadi@gmail.com*, astriana.atm@nusamandiri.ac.id
(*) Corresponding Author



The creation is distributed under the Creative Commons Attribution-NonCommercial 4.0 International License.

Abstract—PT. Andalan Niaga Expressindo (ANX), an international freight-forwarding company, currently runs a computer network without VLAN segmentation or an Access Control List (ACL), so all divisions share one broadcast domain with unrestricted inter-division access, raising the risk of unauthorized access to company data. This study designs a division-based VLAN scheme for four divisions (HRGA & Accounting, Document, Sales, and Customer Service), combined with Router-on-a-Stick inter-VLAN routing, a DHCP server, an ACL restricting inter-VLAN access, and a firewall filtering internal-external traffic. All configuration, implementation, and testing were carried out entirely within the Cisco Packet Tracer simulation environment, not on the company's production network. Twenty-four test scenarios were executed, covering VLAN activation status, inter-VLAN connectivity, DHCP address allocation, ACL permit/deny behavior in both directions, and firewall rule matching for internal-to-external, external-to-internal, and service-specific traffic. Results show the four VLANs were successfully activated, inter-VLAN routing worked as configured, the DHCP server correctly allocated addresses per division, the ACL correctly permitted and denied traffic according to the configured direction and rule, and the firewall correctly matched traffic against its configured rules. Within this simulation, the design demonstrated improved access control between divisions and is expected to improve network security and administrative efficiency if applied to the actual network, pending validation on physical devices. This research contributes an integrated, simulation-tested design combining VLAN, inter-VLAN routing, a DHCP server, an ACL, and a firewall for a freight-forwarding company network, an integration not jointly examined in the reviewed prior studies.

Keywords: Access Control List, Cisco Packet Tracer, Firewall, Network Security, VLAN.

Abstrak—PT. Andalan Niaga Expressindo (ANX), perusahaan freight forwarding internasional, saat ini menjalankan jaringan komputer tanpa segmentasi VLAN maupun Access Control List (ACL), sehingga seluruh divisi berada dalam satu broadcast domain dengan akses antar-divisi yang tidak dibatasi, yang meningkatkan risiko akses tidak sah terhadap data perusahaan. Penelitian ini merancang skema VLAN berbasis divisi untuk empat divisi (HRGA & Accounting, Dokumen, Sales, dan Customer Service), dikombinasikan dengan inter-VLAN routing metode Router-on-a-Stick, DHCP server, ACL yang membatasi akses antar-VLAN, dan firewall yang menyaring lalu lintas internal-eksternal. Seluruh konfigurasi, implementasi, dan pengujian dilakukan sepenuhnya di dalam lingkungan simulasi Cisco Packet Tracer, tidak pada jaringan produksi perusahaan. Sebanyak 24 skenario pengujian dilakukan, meliputi status aktivasi VLAN, konektivitas antar-VLAN, alokasi alamat DHCP, perilaku permit/deny ACL pada kedua arah, serta pencocokan aturan firewall untuk lalu lintas internal-ke-eksternal, eksternal-ke-internal, dan lalu lintas berbasis layanan. Hasil pengujian menunjukkan keempat VLAN berhasil diaktifkan, inter-VLAN routing berfungsi sesuai konfigurasi, DHCP server berhasil mengalokasikan alamat sesuai divisi, ACL berhasil mengizinkan dan menolak lalu lintas sesuai arah dan aturan yang dikonfigurasi, serta firewall berhasil mencocokkan lalu lintas dengan aturan yang ditetapkan. Dalam lingkup simulasi ini, rancangan menunjukkan peningkatan kontrol akses antar-divisi dan diharapkan dapat meningkatkan keamanan serta efisiensi administrasi jaringan apabila diterapkan pada jaringan sebenarnya, dengan syarat dilakukan validasi pada perangkat fisik. Kontribusi penelitian ini adalah rancangan terintegrasi dan teruji secara simulasi

yang menggabungkan VLAN, inter-VLAN routing, DHCP server, ACL, dan firewall untuk jaringan perusahaan freight forwarding, integrasi yang belum dibahas secara bersamaan pada penelitian-penelitian sebelumnya yang ditinjau.

Kata Kunci: Access Control List, Cisco Packet Tracer, Firewall, Keamanan Jaringan, VLAN.

INTRODUCTION

Computer networks have become an essential part of operational activities across many fields, including education, government, and industry, because they enable fast, accurate, and efficient exchange of data and information (Sulianta, 2025; Army et al., 2022). A network is commonly divided into smaller logical segments to organize traffic according to organizational needs, a practice generally referred to as network segmentation (Putra & Mansyur, 2023; Nirsal et al., 2024). As the scope and complexity of network usage grow, network security becomes an increasingly critical issue; a network without adequate security measures is vulnerable to threats such as unauthorized access, misuse of access rights, and potential data leakage, which can disrupt network stability (Akhiruddin & Sutabri, 2023; Rahman & Hakim, 2026).

PT. Andalan Niaga Expressindo (ANX) is an international logistics and freight-forwarding company that relies on a computer network to support administrative tasks, data communication, internet access, and the management of its information systems. Observation shows that the company currently uses a firewall on its Mikrotik router and a single IP subnet for network management, but it has not implemented Virtual Local Area Network (VLAN) segmentation or an Access Control List (ACL) mechanism to restrict communication between divisions. As a result, users from different divisions can still freely access one another's network resources without any clear access restriction, which increases the risk of unauthorized access to company data.

Previous studies suggest that network segmentation may improve the security and management efficiency of a network by separating traffic according to user needs, while access-control mechanisms can restrict inter-network access so that data communication takes place more safely in line with organizational policy (Rahman & Hakim, 2026). Conversely, a network that has not implemented segmentation and access control is prone to security risks such as unauthorized access, data leakage, misuse of access rights, and excessive broadcast traffic (Rahman & Hakim, 2026).

Several prior studies provide the theoretical and empirical basis for this research. Agustio and Nainggolan (2023) examined the application of VLAN on a MAN network combined with ACL-based filtering and found that VLAN improves network management by separating traffic according to user groups. Rahman and Dasuki (2025) studied ACL implementation as an access-control method on a LAN and found that ACL can restrict user access rights based on specific IP addresses so that unauthorized traffic can be limited according to the applied security policy. Dwipoyono and Sudarsono (2023) examined firewall implementation for network security and found that a firewall is able to filter inbound and outbound traffic, preventing unauthorized access. Similarly, Sitohang and Pangaribuan (2025) evaluated VLAN-based traffic segmentation using Cisco Packet Tracer and reported improved security-related indicators within their simulation, reinforcing the relevance of VLAN as a segmentation mechanism. However, among the studies reviewed in this research, VLAN, ACL, and firewall mechanisms were generally examined separately, while their integration with Router-on-a-Stick inter-VLAN routing and DHCP within a single end-to-end network design was not explicitly evaluated.

This study makes three main contributions. First, it proposes an integrated network design combining VLAN segmentation, Router-on-a-Stick inter-VLAN routing, DHCP, ACL-based access control, and packet-filtering firewall rules within a single simulated network environment. Second, it introduces an explicit access-requirements matrix to define permitted and restricted communication between divisions before configuration. Third, it provides a structured simulation-based testing procedure covering VLAN activation, inter-VLAN connectivity, DHCP allocation, ACL behavior, and firewall rule matching.

This study's design and testing were limited to four of PT. Andalan Niaga Expressindo's seven divisions HRGA & Accounting, Document, Sales, and Customer Service because these divisions have dedicated client workstations (25 PCs in total) that routinely exchange internal data and were identified, through observation and interview, as the segments most in need of differentiated access control. The Sales and Marketing, Project and Nomination, and Information Technology divisions were not modeled as separate VLANs in this study; extending the segmentation to cover these remaining divisions is left as a direction for further research once the design proposed here has been validated. In addition, HRGA and Finance and Accounting were combined into a single VLAN (VLAN 10) rather than given separate VLANs because both divisions manage the company's most

sensitive internal data employee and payroll data for HRGA, and financial and cash-flow records for Accounting and together have only five workstations; grouping them keeps the addressing scheme simple while the ACL still isolates this combined, sensitive segment from the Document, Sales, and Customer Service divisions.

The design and simulation are carried out using the Network Development Life Cycle (NDLC) method (Prasetyo, Infitharina, & Febriyansyah, 2025). Consistent with the scope described above, this research is limited to the requirement-analysis, design, simulation/prototyping, and simulated-implementation stages within Cisco Packet Tracer, and does not extend to configuration or deployment on the company's physical production network.

Based on the problems described above, this study aims to: (1) analyze the weaknesses of the network currently running at PT. Andalan Niaga Expressindo; (2) design a division-based VLAN segmentation scheme together with Router-on-a-Stick inter-VLAN routing, a DHCP server, an ACL, and a firewall based on a documented access-requirements matrix; and (3) implement and test the resulting configuration within the Cisco Packet Tracer simulation environment to verify that it behaves as designed, providing a basis for future validation and deployment on the company's physical network.

MATERIALS AND METHODS

This research uses a design-and-simulation approach that follows the Network Development Life Cycle (NDLC) method (Prasetyo, Infitharina, & Febriyansyah, 2025), which generally consists of six stages: analysis, design, simulation/prototyping, implementation, monitoring, and management. Because this research ends at verifying the configuration inside Cisco Packet Tracer and does not extend to deployment on the company's production equipment, the fourth stage used here is a simulated implementation rather than a full implementation. Table 1 summarizes the activity and output produced at each stage used in this study.

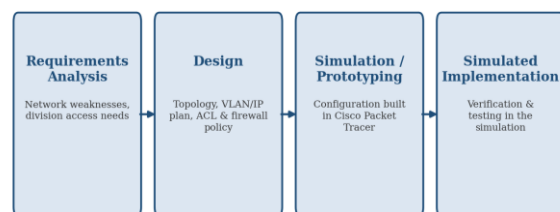
Table 1. NDLC Stages, Activities, and Outputs Used in This Study

Stage	Main Activity	Output
Requirement Analysis	Reviewing the current topology, IP addressing, and security condition through observation and interview	List of network weaknesses and division access requirements
Design	Planning the new topology, VLAN/IP addressing scheme, and ACL/firewall policy	Proposed topology diagram, VLAN/IP addressing table,

Stage	Main Activity	Output
Simulation/Prototyping	Building and configuring the proposed design in Cisco Packet Tracer	access-requirements matrix A working Packet Tracer project file with all devices configured
Simulated Implementation	Verifying and testing the configuration using CLI show commands and connectivity/service tests	Test results and CLI verification logs used as the basis for the Results and Discussion section

Source: (Research Results, 2026)

The relationship between these four stages is illustrated in the research flowchart in Figure 1.



Source : (Research Results, 2026)

Figure 1. Research Flowchart Based on the NDLC Method

The data sources used in this study consist of primary data obtained directly from PT. Andalan Niaga Expressindo through field observation and an interview with the company's IT staff, and secondary data obtained from books and scientific journals relevant to computer networks and network security. Observation and the interview were conducted in April 2026, prior to the design stage described below.

Data were collected using three techniques. Observation involved a direct review of PT. Andalan Niaga Expressindo's network to understand the network system currently in use. An interview was then conducted directly with the company's IT staff to obtain information about the current network condition, the devices in use, the IP numbering protocol, the network security methods applied, and the problems faced by the company; this information was used as the basis for identifying each division's access requirements, described next. A literature study was also carried out by searching for references from books, scientific journals, and other sources relevant to computer networks and network security, particularly network device inventories and infrastructure analysis (Adriansyah, Huzaifah, & Pulungan, 2023).

Each division's access requirements were determined from the interview results together with the sensitivity of the data handled by each division. HRGA and Finance and Accounting were classified as the highest-sensitivity segment because they process employee and financial data, and were therefore assigned the most restrictive inbound policy: no other VLAN may initiate access into this segment. The Document, Sales, and Customer Service divisions were classified as operational/customer-facing segments that do not routinely need to reach one another's resources directly, but that legitimately receive information disseminated by HRGA & Accounting (e.g., administrative memos, financial approvals). Based on the interview findings and the sensitivity of the information handled by each division, an access-requirements matrix was developed to define permitted and restricted communication between VLANs. The matrix presented in Table 2 subsequently served as the policy basis for designing the ACL rules evaluated in the simulation.

Table 2. Access Requirements Matrix Between Divisions

Source \ Destination	HRGA & Accounting	Document	Sales	Cust. Service	Internet
HRGA & Accounting	—	Allowed	Allowed	Allowed	Allowed
Document	Denied	—	Allowed	Allowed	Allowed
Sales	Denied	Allowed	—	Allowed	Allowed
Customer Service	Denied	Allowed	Allowed	—	Allowed

Source: (Research Results, 2026)

The simulation was developed using Cisco Packet Tracer version 8.2.2. The software was used to configure and test VLAN segmentation, IEEE 802.1Q trunking, Router-on-a-Stick inter-VLAN routing, DHCP, ACL-based access control, and packet-filtering firewall rules. Cisco Packet Tracer was selected because it supports the Cisco IOS command set needed to configure VLAN, trunking, Router-on-a-Stick inter-VLAN routing, DHCP, ACL, and ACL-based firewall rules, and because it has been used in comparable network-security simulation studies (Sitohang & Pangaribuan, 2025). The simulated topology used one router, two switches, one access point, one server, and 25 client PCs, representing the devices identified during the requirement-analysis stage and reflecting a client-server communication model (Rizal, Supiyandi, Zen, & Eka, 2022).

Based on the access-requirements matrix, IP addressing was re-planned using a Class C scheme, with each VLAN assigned its own network address and the router subinterface acting as the default gateway (Azizah, 2026), as summarized in Table 3.

Table 3. Planned VLAN and IP Addressing Scheme

VLAN ID	VLAN Name	Division	Network Address	Gateway
10	HRGA	HRGA & Accounting	192.168.10.0/24	192.16.8.10.1
20	DOKUMEN	Document	192.168.20.0/24	192.16.8.20.1
30	SALES	Sales	192.168.30.0/24	192.16.8.30.1
40	CS	Customer Service	192.168.40.0/24	192.16.8.40.1

Source: (Research Results, 2026)

Table 4 summarizes the core configuration commands used to implement VLAN creation, trunking, Router-on-a-Stick inter-VLAN routing at the network's Layer-2/Layer-3 boundary (Ariadi & Saputra, 2024), the DHCP server, the ACL, and the firewall; the complete configuration process and its verification are presented in the Results and Discussion section together with the corresponding test results.

Table 4. Core Network Configuration Commands

Component	Core Command(s)
VLAN creation	vlan 10 ; name HRGA (repeated for VLAN 20/DOKUMEN, 30/SALES, 40/CS)
Trunk	switchport mode trunk ; switchport trunk allowed vlan 10,20,30,40
Inter-VLAN routing	interface gi0/1.10 ; encapsulation dot1Q 10 ; ip address 192.168.10.1 255.255.255.0 (repeated per VLAN subinterface)
DHCP server	ip dhcp pool HRGA ; network 192.168.10.0 255.255.255.0 ; default-router 192.168.10.1 ; dns-server 8.8.8.8
ACL	access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 ; access-list 100 permit ip any any ; interface gi0/1.10 ; ip access-group 100 out
Firewall	access-list 101 permit tcp any any established ; access-list 101 deny ip any any ; interface gi0/0 ; ip access-group 101 in

Source: (Research Results, 2026)

The network infrastructure information analyzed in this study consists of the company's device inventory (one Mikrotik RB450GX router, one Asus router, one HP Office 16-port switch, one Cisco 24-port switch, one Cisco access point, one internal server, one photocopier scan server, and 25 client PCs distributed across four divisions), the current IP addressing scheme (a single

192.168.1.0/24 segment obtained automatically through DHCP), and the existing security configuration, which consists only of the firewall feature on the Mikrotik router.

Data analysis was carried out descriptively through the four NDLC stages used in this study, as summarized in Table 1. In the requirement-analysis stage, the current topology, IP addressing scheme, and security condition of each division were reviewed to identify network weaknesses. In the design stage, a new topology was created and IP addressing was re-planned as shown in Table 3, together with the access-requirements matrix in Table 2 used to derive the ACL and firewall policies. In the simulation/prototyping stage, the proposed design was built and configured in Cisco Packet Tracer using the core commands summarized in Table 4. In the simulated-implementation stage, the configuration was verified using CLI commands (show vlan brief, show interfaces trunk, show ip interface brief, show ip dhcp binding, show access-lists) together with connectivity and service-level tests between divisions, so that the effectiveness of the design could be evaluated within the simulation before any consideration of applying it to the company's real network.

RESULTS AND DISCUSSION

Current Network Condition

Observation and interview results show that PT. Andalan Niaga Expressindo, an international freight-forwarding company located in South Jakarta, employs 31 staff across seven divisions connected through a star-topology network. Internet access with bandwidth up to 150 Mbps is supplied by ISP Biznet through a Biznet modem to a Mikrotik RB450GX router, which is connected to an HP Office 16-port switch and, via a trunk link, to a Cisco 24-port switch. All 25 client computers, the internal server, the photocopier scan server, and a Cisco access point (offering four SSIDs, including one dedicated guest SSID) are connected through these two switches. Table 5 summarizes the network devices currently used.

Table 5. Network Devices at PT. Andalan Niaga Expressindo

No	Device	Quantity
1	Biznet Modem	1 unit
2	Mikrotik RB450GX Router	1 unit
3	Asus Router	1 unit
4	HP Office 16-Port Switch	1 unit
5	Cisco 24-Port Switch	1 unit
6	Cisco Access Point	1 unit
7	Internal Server	1 unit
8	Photocopier Scan Server	1 unit
9	Client PC	25 units

Source: (Research Results, 2026)

The entire network still uses a single IP segment, 192.168.1.0/24, with addresses assigned automatically through DHCP on the Mikrotik router; no VLAN segmentation or ACL has been implemented, so every device shares one broadcast domain. Although the Mikrotik router provides basic firewall protection for internet-facing traffic, no mechanism restricts communication between divisions, so a user in one division can freely access the resources of another. Table 6 shows the distribution of client computers across the four divisions selected for VLAN segmentation in this study, whose selection rationale was explained in the Introduction.

Table 6. Number of Computers per Division

Division	Number of PCs
HRGA & Accounting	5
Document	9
Sales	7
Customer Service	4
Total	25

Source: (Research Results, 2026)

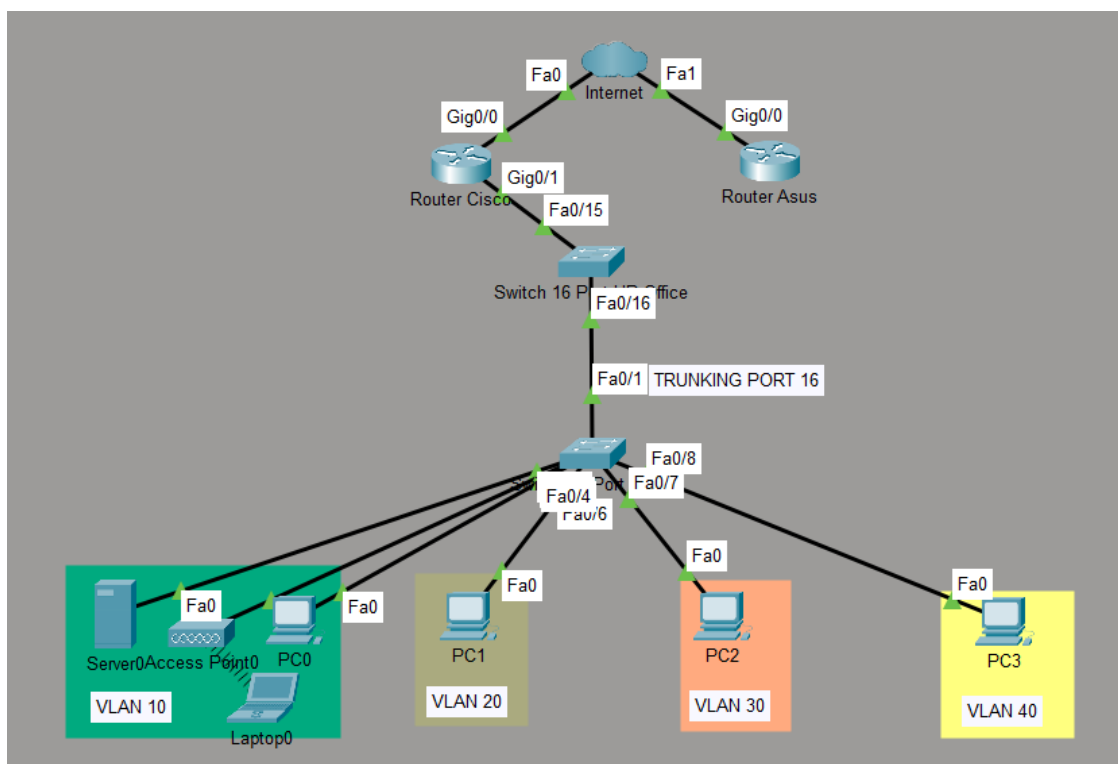
Based on this analysis, the identified weaknesses are: (1) the absence of VLAN segmentation, so all devices remain on one physical network; (2) the absence of an ACL, so inter-division communication is unrestricted; (3) a firewall that is only focused on general internet-access security and is not yet used to control inter-division access; (4) an unstructured IP addressing scheme, which complicates network management and monitoring; and (5) a wireless network that is not yet integrated with VLAN segmentation.

Proposed Network Design

To address these weaknesses, this research proposes replacing the existing Mikrotik router with a Cisco router that natively supports VLAN, inter-VLAN routing, ACL, and firewall configuration, while retaining the existing HP Office 16-port switch and adding a Cisco Switch 2960 24-port to support VLAN implementation. The proposed topology, following the addressing plan in Table 3, is shown in Figure 2.

ACL Direction and Firewall Type

Before presenting the configuration steps, two methodological points are clarified. First, the ACL used to protect the HRGA & Accounting VLAN is a numbered, extended access list applied outbound on the router subinterface serving VLAN 10 (Gi0/1.10 in the simulation). Applying the ACL on this single subinterface, rather than separately on the Document, Sales, and Customer Service subinterfaces, filters all traffic attempting to enter the 192.168.10.0/24 network regardless of which



Source: (Research Results, 2026)

Figure 2. Proposed Network Topology

VLAN it originates from, which keeps the policy consistent with the access-requirements matrix in Table 2 using a single rule set. Second, the firewall implemented in this study is a stateless, rule-based packet-filtering firewall built from an extended access list applied on the router's interface facing the internet, not a dedicated stateful firewall appliance or a Cisco Zone-Based Policy Firewall; the established keyword was used to approximate basic stateful behavior for return TCP traffic, but the design does not perform full stateful session tracking as a dedicated firewall device would.

VLAN Configuration and Activation

The four VLANs were created on the Cisco Switch 2960 through the CLI and named according to their division (HRGA, DOKUMEN, SALES, CS), as summarized in Table 4 and shown in Figure 3. The show vlan brief output (Figure 3) confirms that all four VLANs were created and remained active, and that assigning each division to its own VLAN removes the divisions from a single flat broadcast domain into four independent broadcast domains, consistent with the segmentation strategy examined by Agustio and Nainggolan (2023) and by Sitohang and Pangaribuan (2025) using the same simulation tool. Because this study did not capture broadcast-traffic volume, CPU utilization, or any other quantitative indicator before and after segmentation, this discussion is limited to

confirming that the intended logical separation was achieved within the simulation; it does not claim a measured reduction in broadcast traffic or an improvement in network performance.

```
Switch(config)# vlan 10
Switch(config-vlan)# name HRGA
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name DOKUMEN
! (repeated for VLAN 30/SALES and VLAN 40/CS)
```

CISCO-SWITCH#show vlan brief		
VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10 HRGA	active	
20 DOKUMEN	active	
30 SALES	active	
40 CS	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddi-trunk-default	active	
1005 trunks-default	active	

Source: (Research Results, 2026)

Figure 3. VLAN Configuration on the Cisco Switch

The VLAN activation and port-assignment results are summarized in Table 7.

Table 7. VLAN Activation Status

VLAN ID	VLAN Name	Status	Assigned Ports
10	HRGA	Active	Fa0/2–Fa0/5
20	DOKUMEN	Active	Fa0/6
30	SALES	Active	Fa0/7
40	CS	Active	Fa0/8

Source: (Research Results, 2026)

Trunk and Inter-VLAN Routing (Router-on-a-Stick)

Access ports were configured so that interfaces FastEthernet0/2–0/5 became members of VLAN 10, FastEthernet0/6 of VLAN 20, FastEthernet0/7 of VLAN 30, and FastEthernet0/8 of VLAN 40 (Figure 4). A trunk link using the IEEE 802.1Q standard was then configured between port 16 of the HP Office switch and port FastEthernet0/1 of the Cisco switch, allowing all four VLANs to be carried over a single physical connection toward the router (Figure 5).

```
CISCO-SWITCH#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/15, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 HRGA	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5
20 DOKUMEN	active	Fa0/6
30 SALES	active	Fa0/7
40 CS	active	Fa0/8
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Source: (Research Results, 2026)

Figure 4. Access Port Configuration

```
CISCO-SWITCH#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CISCO-SWITCH(config)#int fa0/1
CISCO-SWITCH(config-if)#sw mode trunk
CISCO-SWITCH(config-if)#sw trunk allowed vlan 10,20,30,40
CISCO-SWITCH(config-if)#ex
CISCO-SWITCH(config)#ex
CISCO-SWITCH#
%SYS-5-CONFIG_I: Configured from console by console
CISCO-SWITCH#show int trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking      1
Port      Vlans allowed on trunk
Fa0/1     10,20,30,40
Port      Vlans allowed and active in management domain
Fa0/1     10,20,30,40
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     40
CISCO-SWITCH#
```

Source: (Research Results, 2026)

Figure 5. Trunk Configuration

Inter-VLAN routing was implemented on the Cisco 1941 router using the Router-on-a-Stick method, in which a single physical interface (GigabitEthernet0/1) was divided into four subinterfaces, each encapsulated with dot1Q and assigned as the default gateway of its respective VLAN (Figure 6).

```
Router(config)# interface gi0/1.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
! (repeated for subinterfaces .20, .30, and .40 using Table 3)
Router#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	down
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/1.10	192.168.10.1	YES	manual	up	up
GigabitEthernet0/1.20	192.168.20.1	YES	manual	up	up
GigabitEthernet0/1.30	192.168.30.1	YES	manual	up	up
GigabitEthernet0/1.40	192.168.40.1	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

Source: (Research Results, 2026)

Figure 6. Inter-VLAN Routing Configuration

Table 8. Inter-VLAN Connectivity Test Results (ICMP Ping)

No	Source	Destination	Result
1	HRGA	Document	Success
2	HRGA	Sales	Success
3	HRGA	Customer Service	Success
4	Document	Sales	Success
5	Sales	Customer Service	Success

Source: (Research Results, 2026)

The Router-on-a-Stick method was chosen, rather than a multilayer (Layer-3) switch with switched virtual interfaces, because the devices considered in this design consist of a single router and Layer-2 switches only; Router-on-a-Stick allows inter-VLAN routing to be implemented with this hardware combination at a lower cost, which is appropriate for a small-to-medium enterprise such as PT. Andalan Niaga Expressindo. The five ping scenarios in Table 8 confirm that packets can traverse the router between VLANs when not explicitly restricted; because ping only verifies ICMP reachability, it does not by itself confirm that application-level services would behave correctly, which is why the ACL and firewall tests below also include service- and port-level checks rather than ICMP alone.

DHCP Server Configuration

A DHCP server was configured on the Cisco router with a separate address pool for each VLAN, complete with the gateway address, subnet mask, and DNS server (8.8.8.8), so that client computers receive an IP address automatically according to their division (Figure 7).

```
Router(config)# ip dhcp pool HRGA
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
! (repeated for pools DOKUMEN, SALES, and CS using Table 3)
```

```
Router#show ip dhcp pool
```

Pool HRGA :	
Utilization mark (high/low)	: 100 / 0
Subnet size (first/next)	: 0 / 0
Total addresses	: 254
Leased addresses	: 0
Excluded addresses	: 4
Pending event	: none
1 subnet is currently in the pool	
Current index	IP address range
192.168.10.1	192.168.10.1 - 192.168.10.254
	Leased/Excluded/Total
	0 / 4 / 254
Pool DOKUMEN :	
Utilization mark (high/low)	: 100 / 0
Subnet size (first/next)	: 0 / 0
Total addresses	: 254
Leased addresses	: 0
Excluded addresses	: 4
Pending event	: none
1 subnet is currently in the pool	
Current index	IP address range
192.168.20.1	192.168.20.1 - 192.168.20.254
	Leased/Excluded/Total
	0 / 4 / 254
Pool SALES :	
Utilization mark (high/low)	: 100 / 0
Subnet size (first/next)	: 0 / 0
Total addresses	: 254
Leased addresses	: 0
Excluded addresses	: 4
Pending event	: none
1 subnet is currently in the pool	
Current index	IP address range
192.168.30.1	192.168.30.1 - 192.168.30.254
	Leased/Excluded/Total
	0 / 4 / 254
Pool CS :	
Utilization mark (high/low)	: 100 / 0
Subnet size (first/next)	: 0 / 0
Total addresses	: 254
Leased addresses	: 0
Excluded addresses	: 4
Pending event	: none

Source: (Research Results, 2026)

Figure 7. DHCP Server Configuration

The DHCP address allocation results for each VLAN are presented in Table 9.

Table 9. DHCP Address Allocation Test Results

Division	DHCP Pool	Example Assigned Address	Gateway	Result
HRGA & Accounting	192.168.1.0/24	192.168.10.2	192.16.8.10.1	Successful
Document	192.168.2.0/24	192.168.20.2	192.16.8.20.1	Successful
Sales	192.168.3.0/24	192.168.30.2	192.16.8.30.1	Successful
Customer Service	192.168.4.0/24	192.168.40.2	192.16.8.40.1	Successful

Source: (Research Results, 2026)

The show ip dhcp binding output verified that each client PC received an address from the correct pool for its division and could reach its assigned gateway. Within this simulation, automatic allocation removes the need for administrators to configure IP addresses manually on each of the 25 client PCs, which is expected to simplify day-to-day network administration if applied operationally (Fitriana, Sepriano, & Judijanto, 2025).

ACL Implementation and Testing

Following the access-requirements matrix in Table 2 and the direction described above, an extended ACL was applied outbound on the VLAN 10 subinterface to permit traffic from HRGA & Accounting while denying inbound traffic originating from the Document, Sales, and Customer Service VLANs (Figure 8).

```
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 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)# access-list 100 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)# access-list 100 permit ip any any
Router(config)# interface gi0/1.10
Router(config-subif)# ip access-group 100 out

Router#sh access-lists
Extended IP access list 100:
10 permit icmp any 192.168.10.0 0.0.0.255 echo-reply
20 permit tcp any 192.168.10.0 0.0.0.255 established
30 deny ip any 192.168.10.0 0.0.0.255
40 permit ip any any
```

Source: (Research Results, 2026)

Figure 8. Access Control List (ACL) Configuration

The results of the ACL testing scenarios are summarized in Table 10.

Table 10. ACL Test Results

N	Test Scenario	Expected	Actual
1	Document → HRGA & Accounting (ICMP echo request)	Denied	Denied

N	Test Scenario	Expected	Actual
2	Sales → HRGA & Accounting (ICMP echo request)	Denied	Denied
3	Customer Service → HRGA & Accounting (ICMP echo request)	Denied	Denied
4	HRGA & Accounting → Document (ICMP echo request)	Permitted	Permitted
5	HRGA & Accounting → Sales (ICMP echo request)	Permitted	Permitted
6	HRGA & Accounting → Customer Service (ICMP echo request)	Permitted	Permitted
7	Return traffic to Document after an HRGA-initiated session	Permitted	Permitted
8	HTTP request (TCP port 80) from Document to the HRGA internal server	Denied	Denied

Source: (Research Results, 2026)

The show access-lists match counters increased only on the deny entries corresponding to Document, Sales, and Customer Service traffic directed at 192.168.10.0/24, and remained unchanged for permitted directions, indicating that the rules matched traffic as intended. Scenario 8 shows that the same ACL also denies application-level (HTTP) traffic in the restricted direction, not only ICMP, which addresses the concern that ping alone is not sufficient evidence of correct access control. These results are consistent with the access-restriction behavior reported by Rahman and Dasuki (2025) for ACL implementation on a LAN, and support the outbound, single-subinterface placement described above as a way of enforcing the access-requirements matrix with one rule set instead of three separate rule sets.

Firewall Implementation and Testing

A firewall policy was implemented on the router's internet-facing interface using an additional extended access list that permits established connections and traffic originating from the internal VLANs toward external networks, while denying all other unmatched inbound traffic (Figure 9).

```
Router(config)# access-list 101 permit tcp any any established
Router(config)# access-list 101 permit ip 192.168.10.0 0.0.0.255 any
Router(config)# access-list 101 permit ip 192.168.20.0 0.0.0.255 any
Router(config)# access-list 101 permit ip 192.168.30.0 0.0.0.255 any
Router(config)# access-list 101 permit ip 192.168.40.0 0.0.0.255 any
Router(config)# access-list 101 deny ip any any
Router(config)# interface gi0/0
Router(config-if)# ip access-group 101 in
```

```
Router#show access-lists
Extended IP access list 100
10 permit icmp any 192.168.10.0 0.0.0.255 echo-reply (4 match(es))
20 permit tcp any 192.168.10.0 0.0.0.255 established
30 deny ip any 192.168.10.0 0.0.0.255 (4 match(es))
40 permit ip any any
Extended IP access list 101
10 permit tcp any any established
20 permit ip 192.168.10.0 0.0.0.255 any
30 permit ip 192.168.20.0 0.0.0.255 any
40 permit ip 192.168.30.0 0.0.0.255 any
50 permit ip 192.168.40.0 0.0.0.255 any
60 deny ip any any
```

Source: (Research Results, 2026)

Figure 9. Firewall Configuration

Table 11. Firewall Test Results

N	Test Scenario	Rule Tested	Result
1	Internal host → internet, HTTP (TCP/80)	Permit internal → outside	Permitted
2	Internal host → internet, HTTPS (TCP/443)	Permit internal → outside	Permitted
3	Return traffic from internet after an internal-initiated session	Permit tcp established	Permitted
4	Unsolicited inbound connection from outside to an internal host	Deny ip any any (implicit/explicit)	Denied
5	ICMP ping from outside network to the router's external interface	Deny ip any any (implicit/explicit)	Denied

Source: (Research Results, 2026)

The results of the packet-filtering firewall tests are presented in Table 11. Scenarios 1–3 confirm that the established keyword correctly permitted return traffic for connections initiated from inside the network, while scenarios 4–5 confirm that unsolicited inbound traffic was denied. These results are consistent with the filtering behavior reported by Dwipoyono and Sudarsono (2023). However, because the established keyword only inspects the TCP flags of individual packets rather than maintaining a full connection-state table, this mechanism approximates, rather than fully replicates, the behavior of a dedicated stateful firewall; a production deployment intended to withstand more sophisticated traffic patterns would benefit from a purpose-built stateful firewall or a Cisco Zone-Based Policy Firewall instead of ACL-based filtering alone.

Comparison and Discussion

Table 12 summarizes the condition of the network before the study and the behavior of the proposed configuration observed within the Cisco Packet Tracer simulation.

Table 12. Comparison of Network Conditions Before the Study and Within the Simulated Configuration

Aspect	Before (Observed)	Within Simulation (After Configuration)
Network segmentation	All devices on one network	Divided into 4 VLANs by division
Broadcast domain	Single broadcast domain	4 logically separate broadcast domains (not measured)

Aspect	Before (Observed)	Within Simulation (After Configuration)
IP addressing	Mostly manual, unstructured	Automatic via DHCP server per VLAN
Inter-division communication	No access restriction	Controlled via inter-VLAN routing and ACL
Data security	No dedicated access restriction	Access to the HRGA & Accounting VLAN restricted by ACL
Firewall	General internet-access filtering only	Rule-based filtering of internal/external traffic
Network management	Single, undifferentiated segment	Segmented; expected to ease administration

Source: (Research Results, 2026)

Overall, within the scope of the Cisco Packet Tracer simulation, the 24 test scenarios indicate that the proposed configuration behaved as designed: VLANs were activated and logically isolated, inter-VLAN routing and the DHCP server functioned as configured, and the ACL and firewall rules permitted and denied traffic consistently with the access-requirements matrix in Table 2. These results are consistent with the qualitative findings of Agustio and Nainggolan (2023) on VLAN segmentation, Rahman and Dasuki (2025) on ACL-based access restriction, Dwipoyono and Sudarsono (2023) on firewall-based filtering, and Sitohang and Pangaribuan (2025) on VLAN evaluation using Cisco Packet Tracer. Unlike those studies, the present design integrates all four mechanisms and documents them against a single access-requirements matrix; however, because this study relied solely on functional simulation testing and did not collect quantitative network-quality indicators such as throughput, latency, packet loss, or broadcast-traffic volume (Makmur, Shaddiq, & Saragih, 2025), it cannot claim, and does not claim, that the design measurably improves network performance or security in an absolute sense. What can be concluded is that, within the simulation, the design demonstrated the intended access-control behavior and is expected to improve network security and ease network administration (Fitriana, Sepriano, & Judijanto, 2025; Sinaga et al., 2026) if the same logic is validated and deployed on the company's physical network. Because Cisco Packet Tracer models a simplified subset of Cisco IOS and the company's current router runs Mikrotik RouterOS rather than Cisco IOS, deploying this design operationally would require either adopting Cisco-compatible hardware, as assumed in this design, or translating the VLAN, ACL, and firewall logic into the equivalent Mikrotik RouterOS configuration, and in either case validating the configuration on physical devices before production use.

CONCLUSION

This study designed and tested, entirely within the Cisco Packet Tracer simulation environment, a network configuration for PT. Andalan Niaga Expressindo that integrates VLAN segmentation, Router-on-a-Stick inter-VLAN routing, a DHCP server, an Access Control List, and a firewall for four of the company's divisions—HRGA & Accounting, Document, Sales, and Customer Service. Across 24 simulated test scenarios, the four VLANs were successfully activated, inter-VLAN routing and the DHCP server functioned as configured, the ACL correctly permitted and denied traffic between divisions according to the access-requirements matrix defined in this study, and the firewall correctly matched traffic against its configured rules for internal-to-external, external-to-internal, and return traffic.

These findings are simulation results only; they demonstrate that the configuration behaves as designed within Cisco Packet Tracer and do not constitute evidence of improved security or performance on a live production network, since no production deployment, load testing, or quantitative measurement of throughput, latency, packet loss, or broadcast-traffic volume was carried out. Accordingly, this study does not claim that the broadcast domain was measurably reduced, only that the design logically separates each division into its own VLAN. A further limitation is that the router, switches, and end-user devices modeled in Cisco Packet Tracer represent a simplified subset of Cisco IOS behavior and do not fully reflect the performance, feature set, or configuration syntax of the company's actual hardware, which currently includes a Mikrotik-based router; consequently, testing and validation on physical devices, or adaptation of the configuration to the actual hardware platform, is a necessary step before any operational deployment.

For future research, it is recommended that the design be validated on physical devices, that quantitative measurements of throughput, latency, packet loss, and broadcast traffic be collected before and after implementation, that the remaining three divisions be included in the segmentation scheme, and that additional security mechanisms such as VPN, IDS/IPS, or IEEE 802.1X authentication be evaluated; periodic monitoring using dedicated network-management software is also recommended once the design is deployed operationally.

REFERENCE

- Adriansyah, R. A. F., Huzaifah, A. S., & Pulungan, A. F. (2023). Analisa Perangkat Jaringan Komputer Kampus. *Jurnal Minfo Polgan*, 12(2), 2344–2352. <https://jurnal.polgan.ac.id/index.php/jmp/article/view/13267/2161>
- 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, 32–38. <https://ejournal.mediaantartika.id/index.php/jka/article/view/5/6>
- Akhiruddin, D. R., & Sutabri, T. (2023). Analisis Peningkatan Keamanan pada Simple Network Time Protocol (SNTP) untuk Mendeteksi Cybercrime dalam Aktifitas Jaringan. *Blantika Multidisciplinary Journal*, 2(1), 141–152. <https://blantika.publikasiku.id/index.php/bl/article/view/9/21>
- Ariadi, F., & Saputra, S. (2024). Pengenalan Model 7 OSI Layer pada Siswa-Siswi SMA Islam Terpadu Insan Madani 8. *Praxis: Jurnal Pengabdian Kepada Masyarakat*, 4(2), 30–36. <https://www.pijarpemikiran.com/index.php/praxis/article/view/689/654>
- Army, W. L., et al. (2022). *Teknologi Jaringan Komputer*. Widina Bhakti Persada Bandung.
- Azizah, E. S. N. (2026). IP Address pada Jaringan Komputer. *Jurnal Informatika Indonesia*, 1(2), 88–93. <https://ejournal.samudrailmu.com/index.php/jfi/article/view/102/98>
- Dwipoyono, N., & Sudarsono, A. (2023). Penerapan Firewall pada Sistem Keamanan Jaringan Komputer di Sekolah SMK Negeri 5 Seluma. *Jurnal Media Infotama*, 19(2), 454–464. <https://jurnal.unived.ac.id/index.php/jmi/article/view/4355/3681>
- Fitriana, Y. B., Sepriano, & Judijanto, L. (2025). *Administrasi Jaringan*. PT. Sonpedia Publishing Indonesia.
- Makmur, Z., Shaddiq, A., & Saragih, Y. (2025). *Buku Ajar Kualitas Jaringan*. HADLA Media Informasi.
- Nirsal, N., et al. (2024). *Buku Ajar Jaringan dan Internet*. PT. Sonpedia Publishing Indonesia.
- Prasetyo, F. H., Infitharina, E., & Febriyansyah, M. (2025). Penerapan Metode Network Development Life Cycle (NDLC) dalam Pengembangan Jaringan Komputer. *Journal of Informatics and Communication Technology*, 1–8.

- https://ejournal.akademitelkom.ac.id/j_ict/index.php/j_ict/article/view/410/244
- Putra, F. P. E., & Mansyur, M. U. (2023). *Jaringan Komputer Untuk Pemula*. PT. Literasi Nusantara Abadi Grup.
- Rahman, M., & Dasuki, M. (2025). Implementation of Access Control List (ACL) as a Protection and Traffic Control Method in Local Area Network (LAN) Infrastructure. *Jurnal Computer Science and Information Technology (CoSciTech)*, 6(1), 68–76. <https://ejurnal.umri.ac.id/index.php/coscitech/article/view/9102/3534>
- Rahman, T., & Hakim, L. (2026). Analisis dan Implementasi Segmentasi Jaringan WiFi Karyawan dan Guest Berbasis Userman pada PT. Internetwork Komunikasi Indonesia. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 10(1), 1650–1657. <https://ejournal.itn.ac.id/jati/article/view/16738/9034>
- Rizal, C., Supiyandi, Zen, M., & Eka, M. (2022). *Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server*. Jurnal BIT, 3(1), 27–33. <https://doi.org/10.47065/bit.v3i1.255>
- Sinaga, A. S. R. M., Jabat, D. E. B., Siahaan, R. F., Sinaga, D. C. P., Budiman, T., & Purba, M. (2026). *Manajemen Jaringan*. Madani Kreatif Publisher (Madani Berkah Abadi).
- 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), 264–270. <https://rcf-indonesia.org/home/index.php/jsit/article/view/673/385>
- Sulianta, F. (2025). *Dasar dan Konsep Jaringan Komputer*. Feri Sulianta Press.