



**IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN
LABORATORIUM TELEKOMUNIKASI UPN VETERAN
JAKARTA BERBASIS *VIRTUAL LOCAL AREA NETWORK*
(VLAN)**

SKRIPSI

MUHAMMAD FAHRURIZQI ILHAM

2210314002

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
2026**



**IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN
LABORATORIUM TELEKOMUNIKASI UPN VETERAN
JAKARTA BERBASIS *VIRTUAL LOCAL AREA NETWORK*
(VLAN)**

SKRIPSI

MUHAMMAD FAHRURIZQI ILHAM

2210314002

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK ELEKTRO

2026

HALAMAN PENGESAHAN PENGUJI

Skripsi yang diajukan oleh:

Nama : Muhammad Fahrurizqi Ilham

NIM : 2210314002

Program Studi : S1 – Teknik Elektro

Judul Skripsi : IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN
LABORATORIUM TELEKOMUNIKASI UPN VETERAN JAKARTA
BERBASIS VIRTUAL LOCAL AREA NETWORK (VLAN)

Telah berhasil dipertahankan di hadapan tim penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Pembangunan Nasional Veteran Jakarta.

Silvia Anggraeni, ST., M.Sc., Ph.d
Penguji Utama

Subekti Ari Santoso, S.T., M.Eng.
Penguji Lembaga



Dr. Eng. H. Teguh Firmansyah,
S.T., M.T., IPM.
Dekan Fakultas Teknik

Fajar Rahayu, S.T., M.T.
Penguji I (Pembimbing)

Luh Krisnawati, S.T., M.T.
Koordinator Program Studi
Teknik Elektro

Ditetapkan di : Jakarta
Tanggal Ujian : 16 Juli 2026

HALAMAN PENGESAHAN PEMBIMBING SKRIPSI

**IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN
LABORATORIUM TELEKOMUNIKASI UPN VETERAN
JAKARTA BERBASIS VIRTUAL LOCAL AREA NETWORK
(VLAN)**

Muhammad Fahrurizqi Ilham

NIM. 2210314002

Disetujui oleh,

Pembimbing I



Fajar Rahayu, S.T., M.T.

Pembimbing II



Ayu Mika Sherila, S.T., M.T.

Mengetahui,

Koordinator Program Studi Teknik Elektro

Fakultas Teknik

Universitas Pembangunan Nasional Veteran Jakarta



Luh Krisnawati, S.T., M.T.

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini merupakan hasil karya sendiri dan semua sumber yang dikutip ataupun digunakan sebagai rujukan telah saya nyatakan benar.

Nama : Muhammad Fahrurizqi Ilham

NIM : 2210314002

Program Studi : S1 – Teknik Elektro

Apabila di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 16 Juli 2026

Yang menyatakan,



Muhammad Fahrurizqi Ilham

HALAMAN PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIS

Sebagai *civitas academica* Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Muhammad Fahrurizqi Ilham

NIM : 2210314002

Program Studi : S1 – Teknik Elektro

menyetujui untuk memberikan Hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN LABORATORIUM TELEKOMUNIKASI UPN VETERAN JAKARTA BERBASIS VIRTUAL LOCAL AREA NETWORK (VLAN)

Dengan Hak Bebas Royalti Non-eksklusif ini, Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih-media/formatkan, mengelola (dalam bentuk pangkalan data, merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan pemilik hak cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 16 Juli 2026

Yang menyatakan,



Muhammad Fahrurizqi Ilham

IMPLEMENTASI KEAMANAN SEGMENTASI JARINGAN LABORATORIUM TELEKOMUNIKASI UPN VETERAN JAKARTA BERBASIS VIRTUAL LOCAL AREA NETWORK (VLAN)

Muhammad Fahrurizqi Ilham

ABSTRAK

Keamanan jaringan penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data pada jaringan laboratorium multi-pengguna. Penelitian ini mengimplementasikan dan menganalisis kombinasi VLAN, *Access Control List* (ACL), *Port Security*, dan *Secure Shell* (SSH) pada jaringan berbasis *router-on-a-stick* menggunakan MikroTik RB750 dan Cisco Catalyst 2960 melalui *trunk* 802.1Q. Jaringan dibagi menjadi empat VLAN berbasis IPv4, VLAN 10 Dosen (192.168.10.0/29, Fa0/5–7), VLAN 20 Mahasiswa (192.168.20.0/29, Fa0/2/3/8/9), VLAN 30 Server (192.168.30.0/29, Fa0/4), dan VLAN 99 Management (Fa0/24). ACL diterapkan untuk membatasi komunikasi antar-VLAN, Port Security menggunakan metode *sticky MAC* dengan mode *shutdown* (VLAN 10, 30) dan *restrict* (VLAN 20), serta SSH mengamankan akses manajemen menggantikan Telnet. Pengujian meliputi *ping* 15 paket untuk konektivitas intra/antar-VLAN sebelum-sesudah ACL, simulasi *MAC spoofing* untuk mengukur status interface, *Violation Count*, dan *Response Time* pada Port Security, serta verifikasi autentikasi SSH dari VLAN 99 dengan RSA 1024-bit dan *strong-crypto*. Hasil menunjukkan VLAN berhasil memisahkan domain jaringan, ACL dan SSH mencapai efektivitas 100%, serta Port Security mendeteksi dan merespons perangkat tidak sah sesuai mode konfigurasi. Kombinasi mekanisme ini meningkatkan keamanan tanpa mengganggu komunikasi yang diizinkan.

Kata Kunci: *VLAN, Access Control List (ACL), Port Security, Secure Shell (SSH), Keamanan Jaringan.*

**IMPLEMENTATION OF VIRTUAL LOCAL AREA NETWORK (VLAN)-
BASED NETWORK SEGMENTATION SECURITY IN THE
TELECOMMUNICATIONS LABORATORY OF UPN VETERAN JAKARTA**

Muhammad Fahrurizqi Ilham

ABSTRACT

Network security is essential for maintaining the confidentiality, integrity, and availability of data on multi-user laboratory networks. This research implements and analyzes a combination of VLAN, Access Control List (ACL), Port Security, and Secure Shell (SSH) mechanisms on a router-on-a-stick based network using a MikroTik RB750 router and Cisco Catalyst 2960 switch connected via 802.1Q trunk. The network is divided into four IPv4-based VLANs: VLAN 10 Lecturer (192.168.10.0/29, Fa0/5–7), VLAN 20 Student (192.168.20.0/29, Fa0/2/3/8/9), VLAN 30 Server (192.168.30.0/29, Fa0/4), and VLAN 99 Management (192.168.100.1/29, Fa0/24). ACL is applied to restrict inter-VLAN communication, Port Security uses the sticky MAC method with shutdown mode (VLAN 10, 30) and restrict mode (VLAN 20), while SSH secures management access in place of Telnet. Testing includes 15-packet ping tests for intra and inter-VLAN connectivity before and after ACL implementation, MAC spoofing simulation to measure interface status, Violation Count, and Response Time for Port Security, and SSH authentication verification from VLAN 99 using 1024-bit RSA keys and strong-crypto. Results show VLAN successfully segmented the network domains, ACL and SSH achieved 100% effectiveness, and Port Security successfully detected and responded to unauthorized devices according to configured modes. This combination of mechanisms enhances laboratory network security without disrupting authorized communication.

Keywords: *VLAN, Access Control List (ACL), Port Security, Secure Shell (SSH), Network Security.*

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT atas segala rahmat, karunia, serta kemudahan yang telah diberikan, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Keamanan Segmentasi Jaringan Laboratorium Telekomunikasi UPN Veteran Jakarta Berbasis Virtual Local Area Network (VLAN)" ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Pembangunan Nasional "Veteran" Jakarta.

Penulis menyadari bahwa penyusunan skripsi ini tidak lepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua tercinta, Bapak Nasrudi dan Ibu Evarita, atas segala doa, kasih sayang, dukungan moral maupun material, serta kesabaran yang tiada henti diberikan kepada penulis selama menempuh pendidikan hingga menyelesaikan skripsi ini. Tanpa pengorbanan dan dukungan Ayah dan Ibu, penulis tidak akan sampai pada tahap ini.
2. Ibu Fajar Rahayu selaku Dosen Pembimbing I, yang telah meluangkan waktu, memberikan bimbingan, arahan, serta masukan yang sangat berharga selama proses penyusunan skripsi ini.
3. Ibu Ayu Mika Sherila selaku Dosen Pembimbing II, yang telah memberikan masukan dan saran dalam penyempurnaan skripsi ini.
4. Rekan-rekan mahasiswa Teknik Elektro, khususnya rekan asisten praktikum Jaringan Komputer dan Komunikasi Data, atas dukungan dan kerja sama selama ini.
5. Serta semua pihak yang tidak dapat disebutkan satu per satu, yang telah membantu baik secara langsung maupun tidak langsung dalam penyelesaian skripsi ini.
6. Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi

perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi penulis khususnya, serta bagi pembaca dan pengembangan ilmu pengetahuan pada umumnya.

Jakarta, Juli 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN PENGUJI	ii
HALAMAN PERNYATAAN ORISINALITAS.....	iii
HALAMAN PENGESAHAN PEMBIMBING SKRIPSI.....	iv
HALAMAN PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIS.....	v
ABSTRAK	vii
<i>ABSTRACT</i>	viii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	xx
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xv
DAFTAR LAMPIRAN	xvi
DAFTAR SINGKATAN.....	xvii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	3
1.5 Sistematika Penulisan.....	4
BAB 2 TINJAUAN PUSTAKA.....	6
2.1 Penelitian Terdahulu.....	6
2.2 Landasan Teori	12
2.2.1 Model Referensi OSI (<i>Open Systems Interconnection</i>)	12
2.2.2 <i>Virtual Local Area Network (VLAN)</i>	14
2.2.3 <i>Router-on-a-Stick</i>	15
2.2.4 <i>Port Security</i>	17
2.2.5 <i>Secure Shell (SSH)</i>	19
2.2.6 <i>Spanning tree protocol</i>	20
2.2.7 <i>Access Control List (ACL)</i>	20

2.2.8 Metode Perancangan Jaringan	22
2.2.9 Cisco Packet Tracer.....	23
2.2.10 PuTTY	24
2.2.11 Packet Delivery Ratio (PDR).....	25
2.2.12 Packet Loss Ratio (PLR).....	25
2.2.13 Round-Trip Time (RTT).....	25
BAB 3 METODE PENELITIAN	26
3.1 Tahapan Penelitian	26
3.2 Perancangan Topologi.....	27
3.2.1 Diagram Alir Simulasi	30
3.2.2 Diagram Alir Implementasi	32
3.3 Pengujian Sistem Keamanan	34
3.4 Tahapan Implementasi	36
3.4.1 Implementasi Algoritma <i>Access Control List</i>	36
3.4.2 Implementasi Algoritma <i>Port Security</i>	37
3.4.3 Implementasi Algoritma <i>SSH Key Exchange</i>	38
3.5 Pengolahan dan Analisis Data.....	39
3.6 Jadwal Penelitian.....	39
BAB 4 HASIL DAN PEMBAHASAN	41
4.1 Fase Persiapan / <i>Prepare</i>	41
4.1.1 Kebutuhan Perangkat Keras dan Perangkat Lunak	41
4.2 Fase Desain & Perencanaan / <i>Design & Planning</i>	44
4.2.1 Topologi Jaringan Perancangan VLAN	44
4.2.2 Perancangan <i>IP Address</i>	46
4.2.3 Perancangan Sistem Keamanan Antarsegmen	47
4.3 Fase <i>Implement & Operate</i>	49
4.2.1 Konfigurasi VLAN pada <i>Switch</i>	49
4.2.2 Konfigurasi <i>Routing</i>	51
4.2.3 Konfigurasi <i>SSH</i>	53
4.2.4 Konfigurasi <i>Port Security</i>	55
4.2.5 Konfigurasi <i>Access Control List (ACL)</i>	60
4.4 Fase Optimasi / <i>Optimize</i>	63

4.3.1 Pengujian Konektivitas dalam VLAN yang Sama	63
4.3.2 Pengujian Konektivitas Antar-VLAN Sebelum ACL	65
4.3.3 Pengujian Konektivitas Antar-VLAN Setelah ACL.....	70
4.3.4 Pengujian <i>Port Security</i>	71
4.3.5 Pengujian SSH.....	77
4.5 Analisis Hasil Pengujian	78
4.4.1 Analisis Segmentasi VLAN	78
4.4.2 Analisis Keamanan Akses	80
4.4.3 Analisis Efektivitas ACL terhadap <i>Unauthorized Access</i>	82
4.4.4 Analisis Perbandingan Sebelum dan Sesudah Konfigurasi.....	84
BAB 5 PENUTUP.....	87
5.1 Kesimpulan.....	87
5.2 Saran.....	88
DAFTAR PUSTAKA	
DAFTAR RIWAYAT HIDUP	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1 Model Referensi OSI	14
Gambar 2.2 Jaringan VLAN.....	15
Gambar 2.4 <i>Port Security dynamic learning</i>	18
Gambar 2.5 <i>Sticky Port Security</i>	19
Gambar 2.6 <i>Secure Shell</i>	20
Gambar 2.7 Konfigurasi ACL	22
Gambar 2.8 PPDIOO	22
Gambar 2.9 <i>Cisco Packet Tracer</i>	24
Gambar 3.1 Tahapan Penelitian.....	27
Gambar 3.2 Perancangan Topologi Jaringan.....	28
Gambar 3.3 Diagram Alir Simulasi.....	30
Gambar 3.4 Flowchart Implementasi	32
Gambar 4.1 Topologi Perancangan VLAN	44
Gambar 4.3 Hasil perintah <i>show vlan brief</i>	50
Gambar 4.6 Verifikasi Konfigurasi <i>Trunking</i>	51
Gambar 4.7 Konfigurasi <i>Interface VLAN</i> pada Router MikroTik.....	51
Gambar 4.8 Verifikasi Interface VLAN	52
Gambar 4.9 Verifikasi <i>Gateway</i> Setiap VLAN	52
Gambar 4.10 Konfigurasi SSH pada Router Mikrotik	53
Gambar 4.11 Verifikasi Alamat Akses SSH	53
Gambar 4.12 Verifikasi Enkripsi SSH	54
Gambar 4.13 Verifikasi user SSH Terdaftar	54
Gambar 4.14 Hasil Akses SSH.....	55
Gambar 4.16 Hasil Verifikasi <i>Port Security</i> pada <i>Interface Fa0/5</i>	57
Gambar 4.17 Konfigurasi Port Security Mode Restrict	58
Gambar 4.18 Konfigurasi Port Security Metode Static Mode Shutdown	59
Gambar 4.19 Hasil perintah <i>show port-security</i>	59
Gambar 4.20 Hasil Perintah <i>show port-security address</i>	60
Gambar 4.21 Konfigurasi ACL pada <i>Router MikroTik</i>	61
Gambar 4.22 <i>Rules ACL</i>	61

Gambar 4.23 Hasil <i>ping</i> menuju <i>Gateway</i> VLAN 20	63
Gambar 4.24 Hasil <i>ping</i> dari PC Mahasiswa-1 ke <i>gateway</i>	64
Gambar 4.25 Pengujian Konektivitas VLAN 10 ke VLAN 20	66
Gambar 4.26 Pengujian Konektivitas VLAN 10 ke VLAN 30	66
Gambar 4.27 Pengujian Konektivitas VLAN 20 ke VLAN 10	67
Gambar 4.28 Pengujian Konektivitas VLAN 20 ke VLAN 30	67
Gambar 4.29 Pengujian Konektivitas VLAN 30 ke VLAN 10	68
Gambar 4.30 Pengujian Konektivitas VLAN 30 ke VLAN 20	68
Gambar 4.31 <i>firewall rules</i> MikroTik	70
Gambar 4.32 Hasil verifikasi <i>Port Security</i> pada <i>interface FastEthernet0/5</i>	73
Gambar 4.33 Hasil perintah ' <i>ip service print</i> '	77
Gambar 4.34 Hasil Login <i>SSH</i>	78

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	6
Tabel 3.1 Total Pengujian.....	35
Tabel 3.2 Jadwal Penelitian	40
Tabel 4.1 Kebutuhan Perangkat Keras	41
Tabel 4.2 Kebutuhan Perangkat Lunak	43
Tabel 4.3 Perancangan IP Address dan Port	46
Tabel 4.4 Regulasi <i>ACL</i> antar- <i>VLAN</i>	48
Tabel 4.5 <i>Rules Access Control List</i>	62
Tabel 4.6 Hasil Pengujian Konektivitas Dalam <i>VLAN</i> yang sama	64
Tabel 4.7 Rekapitulasi Hasil Pengujian Sebelum <i>ACL</i>	69
Tabel 4.8 Rekapitulasi Hasil Pengujian Setelah <i>ACL</i>	71
Tabel 4.9 Hasil Verifikasi <i>Secure MAC Address</i>	72
Tabel 4.10 Hasil Pengujian <i>Port Security Mode Restrict</i>	75
Tabel 4.11 Hasil Pengujian <i>Port Security Mode Shutdown</i>	76
Tabel 4.12 Rekapitulasi Hasil Pengujian Segmentasi <i>VLAN</i>	79
Tabel 4.13 Rekapitulasi Hasil Pengujian <i>Port Security</i>	81
Tabel 4.14 Hasil Pemberlakuan <i>ACL</i> untuk Perangkat Tidak Sah	83
Tabel 4.15 Perbandingan Sebelum dan Sesudah Konfigurasi Keamanan.....	85

DAFTAR LAMPIRAN

- Lampiran 1.** Konfigurasi VLAN di *Switch Mode Access*
- Lampiran 2.** Verifikasi *MAC Address*
- Lampiran 3.** Hasil Konfigurasi *Port Security* di Port Fa0/4
- Lampiran 4.** Hasil *Security Violation Count* Setelah Pelanggaran
- Lampiran 5.** Hasil *Port Security* di setiap *Port*
- Lampiran 6.** Hasil *Ping* antar VLAN
- Lampiran 7.** *System Log Port*
- Lampiran 8.** Lembar Konsultasi Pembimbing 1

DAFTAR SINGKATAN

ACL	: <i>Access Control List</i>
CLI	: <i>Command Line Interface</i>
DHCP	: <i>Dynamic Host Configuration Protocol</i>
IANA	: <i>Internet Assigned Numbers Authority</i>
ICMP	: <i>Internet Control Message Protocol</i>
IEEE	: <i>Institute of Electrical and Electronics Engineers</i>
IETF	: <i>Internet Engineering Task Force</i>
IOS	: <i>Internetwork Operating System</i>
IP	: <i>Internet Protocol</i>
ISP	: <i>Internet Service Provider</i>
LAN	: <i>Local Area Network</i>
MAC	: <i>Media Access Control</i>
OSI	: <i>Open Systems Interconnection</i>
PC	: <i>Personal Computer</i>
PDR	: <i>Packet Delivery Ratio</i>
PLR	: <i>Packet Loss Rate</i>
RFC	: <i>Request for Comments</i>
RSA	: <i>Rivest–Shamir–Adleman</i>
RTT	: <i>Round-Trip Time</i>
SSH	: <i>Secure Shell</i>
STP	: <i>Spanning Tree Protocol</i>
TCP/IP	: <i>Transmission Control Protocol/Internet Protocol</i>
VLAN	: <i>Virtual Local Area Network</i>
VTY	: <i>Virtual Teletype</i>