

**PENERAPAN MANAJEMEN DAN KEAMANAN JARINGAN  
WIRELESS BERBASIS MIKROTIK**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



diajukan oleh  
**YOSI ANDRIA**  
**18.11.2163**

Kepada

**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS AMIKOM YOGYAKARTA**  
**YOGYAKARTA**  
**2023**

**PENERAPAN MANAJEMEN DAN KEAMANAN JARINGAN  
WIRELESS BERBASIS MIKROTIK**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



diajukan oleh  
**YOSI ANDRIA**  
**18.11.2163**

Kepada

**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS AMIKOM YOGYAKARTA**  
**YOGYAKARTA**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**PENERAPAN MANAJEMEN DAN KEAMANAN JARINGAN  
WIRELESS BERBASIS MIKROTIK**

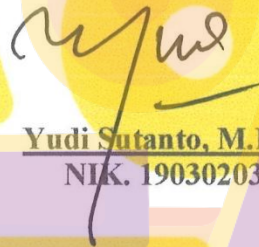
yang disusun dan diajukan oleh

**Yosi Andria**

**18.11.2163**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal Rabu, 23 November 2022

**Dosen Pembimbing,**



**Yudi Sutanto, M.Kom**

**NIK. 190302039**

**HALAMAN PENGESAHAN**  
**SKRIPSI**  
**PENERAPAN MANAJEMEN DAN KEAMANAN JARINGAN**  
**WIRELESS BERBASIS MIKROTIK**

yang disusun dan diajukan oleh

**Yosi Andria**

**18.11.2163**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 23 November 2022

**Nama Penguji**

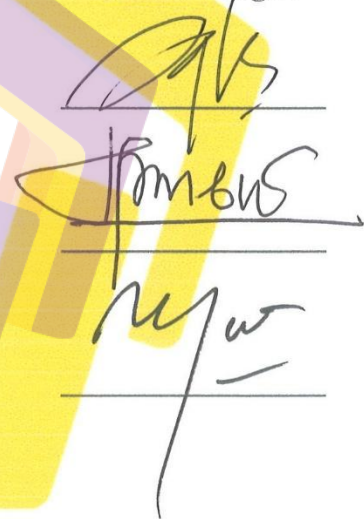
**Susunan Dewan Penguji**

**Tanda Tangan**

**Andika Agus Slameto, M.Kom**  
NIK. 190302109

**Agung Pambudi, ST, M.A**  
NIK. 190302012

**Yudi Sutanto, M.Kom**  
NIK. 190302039



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 23 November 2022

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom.**

NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Yosi Andria  
NIM : 18.11.2163

Menyatakan bahwa Skripsi dengan judul berikut:

**Penerapan Manajemen Dan Keamanan Jaringan Wireless Berbasis Mikrotik**

Dosen Pembimbing : Yudi Sutanto, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 November 2022

Yang Menyatakan,



Yosi Andria

## HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah dan karunia-Nya sehingga tugas akhir ini dapat selesai dengan sebaik-baiknya, dan tidak lupa tugas akhir ini saya persembahkan untuk :

1. Kedua orang tua, Bapak dan Ibu yang selalu memberi dukungan berupa semangat, materi, maupun kerja keras mereka yang diperuntukan kepada saya.
2. Bapak Yudi Susanto, M.Kom. selaku dosen pembimbing yang telah mencurahkan waktu dan tenaganya dalam membantu penyelesaian tugas akhir ini.
3. Kepada segenap dosen Universitas Amikom Yogyakarta yang telah mencurahkan ilmu, waktu, dan tenaga selama saya menimba ilmu.

Kepada saudara maupun teman yang telah memberi dukungan berupa moral dan semangat agar pengerjaan tugas akhir ini dapat selesai dengan baik.

## KATA PENGANTAR

Dengan mengucapkan puji syukur atas kehadiran Tuhan Yang Maha Esa Allah SWT yang telah memberikan rahmat serta hidayah-Nya kepada penulis, sehingga tugas akhir yang berjudul “ **Penerapan Manajemen Dan Keamanan Jaringan Wireless Berbasis Mikrotik**” dapat terselesaikan.

Tugas akhir ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Informatika Fakultas Sains Dan Teknologi Universitas Amikom Yogyakarta.

Penulis menyadari bahwa jika tanpa dukungan dan bimbingan dari berbagai pihak, skripsi ini mungkin tidak dapat terselesaikan. Oleh karena itu saya selaku penulis menyampaikan terimakasih kepada :

1. Allah SWT karena atas karunia dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga kelak dapat memberikan manfaat pada kemudian hari.
2. Bapak Prof. Dr, M.Suyanto, M.M selaku Rektor Universitas Amikom Yogyakarta
3. Bapak Yudi Susanto, M.Kom. selaku Dosen Pembimbing yang telah memberikan arahan dalam penyusunan tugas akhir ini
4. Segenap Dosen, Staff, dan Karyawan Universitas Amikom Yogyakarta yang telah membantu penulis dalam menyelesaikan tugas akhir ini.
5. Orang tua, beserta saudara maupun teman yang selalu mendoakan dan memberi dukungan kepada penulis.

Penulis berharap tugas akhir ini dapat bermanfaat pada semua pihak yang telah membantu dalam penyelesaian karya tulis ini, dan penulis menyadari masih ada kekurangan yang mungkin tidak disadari karena masih ada keterbatasan wawasan dan pengalaman.

Yogyakarta, 23 November 2022

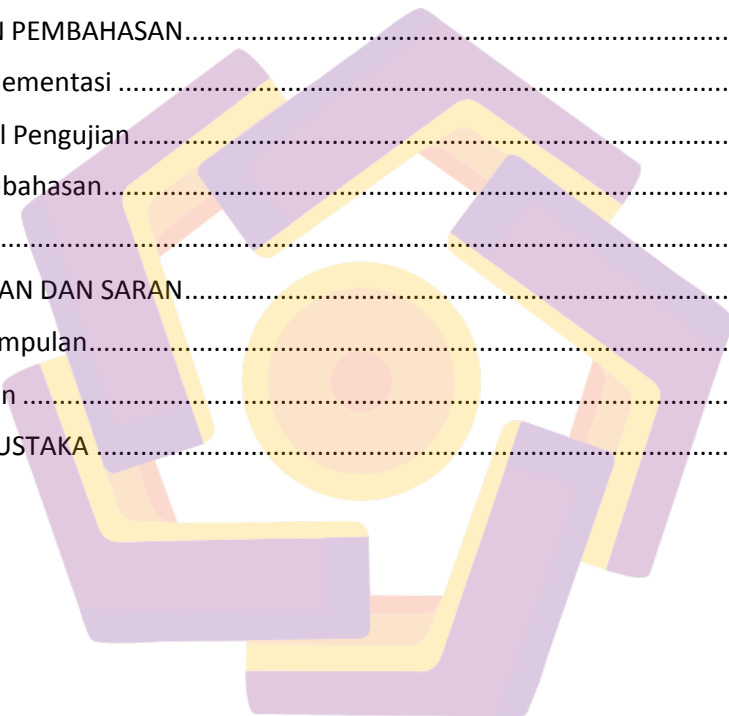
Penulis

## DAFTAR ISI

HALAMAN COVER .....	<b>Error! Bookmark not defined.</b>
HALAMAN JUDUL .....	<b>Error! Bookmark not defined.</b>
HALAMAN PERSETUJUAN .....	iii
HALAMAN PENGESAHAN .....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	v
HALAMAN PERSEMBAHAN .....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL .....	x
DAFTAR GAMBAR.....	xi
DAFTAR ISTILAH .....	xiii
INTISARI.....	xiv
Abstract.....	xv
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Tujuan Penelitian .....	2
1.4 Batasan Masalah.....	3
1.5 Manfaat Penelitian.....	3
BAB II.....	4
LANDASAN TEORI.....	4
2.1 Kajian Pustaka .....	4
2.2 Dasar Teori .....	39
2.2.1 Mikrotik.....	39
2.2.2 Bandwidth .....	39
2.2.4 VPN.....	40
2.2.5 Hotspot .....	41
2.2.6 Filter Rules Dan Layer 7.....	42
2.2.7 PPDIIO.....	42



BAB III.....	45
METODOLOGI PENELITIAN.....	45
3.1 Analisis Masalah.....	45
3.2 Penanganan Masalah.....	45
3.3 Alat dan Bahan Penelitian.....	46
3.4 Metode Penelitian .....	47
3.5 Alur Penelitian.....	48
3.6 Perancangan .....	50
BAB IV.....	52
HASIL DAN PEMBAHASAN.....	52
4.1 Implementasi .....	52
4.2 Hasil Pengujian.....	66
4.2 Pembahasan.....	89
BAB V.....	91
KESIMPULAN DAN SARAN.....	91
5.1 Kesimpulan.....	91
5.2 Saran .....	92
DAFTAR PUSTAKA .....	93



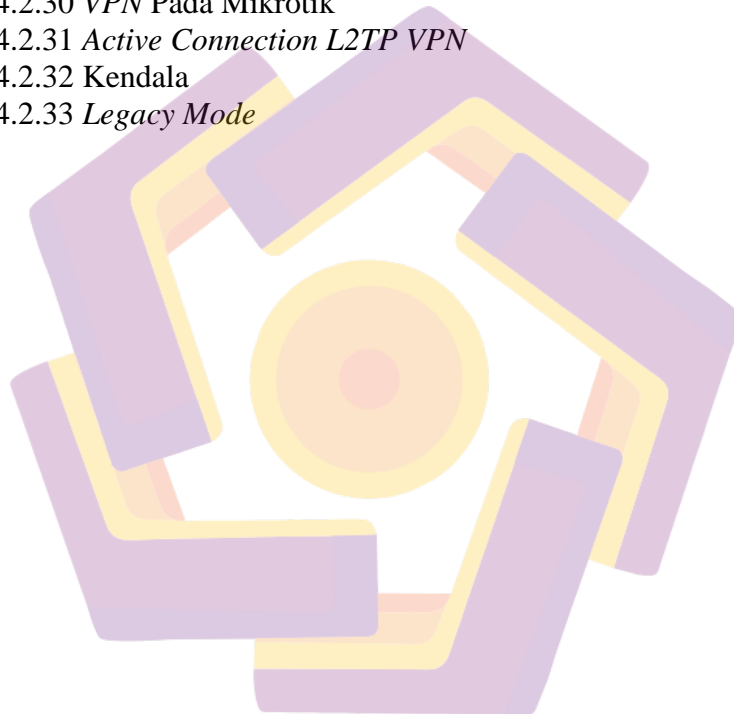
## DAFTAR TABEL

Tabel 2.1.1 Tabel Perbandingan Penelitian	12
Tabel 2.1.1 Tabel Lanjutan	13
Tabel 2.1.1 Tabel Lanjutan	14
Tabel 2.1.1 Tabel Lanjutan	15
Tabel 2.1.1 Tabel Lanjutan	16
Tabel 2.1.1 Tabel Lanjutan	17
Tabel 2.1.1 Tabel Lanjutan	18
Tabel 2.1.1 Tabel Lanjutan	19
Tabel 2.1.1 Tabel Lanjutan	20
Tabel 2.1.1 Tabel Lanjutan	21
Tabel 2.1.1 Tabel Lanjutan	22
Tabel 2.1.1 Tabel Lanjutan	23
Tabel 2.1.1 Tabel Lanjutan	24
Tabel 2.1.1 Tabel Lanjutan	25
Tabel 2.1.1 Tabel Lanjutan	26
Tabel 2.1.1 Tabel Lanjutan	27
Tabel 2.1.1 Tabel Lanjutan	28
Tabel 2.1.1 Tabel Lanjutan	29
Tabel 2.1.1 Tabel Lanjutan	30
Tabel 2.1.1 Tabel Lanjutan	31
Tabel 2.1.1 Tabel Lanjutan	32
Tabel 2.1.1 Tabel Lanjutan	33
Tabel 2.1.1 Tabel Lanjutan	34
Tabel 2.1.1 Tabel Lanjutan	35
Tabel 2.1.1 Tabel Lanjutan	36
Tabel 2.1.1 Tabel Lanjutan	37
Tabel 2.1.1 Tabel Lanjutan	38
Tabel.3.3.1 Alat Dan Bahan Penelitian	48
Tabel 3.6.1 Pembatasan <i>Bandwidth Upload Dan Download</i>	50
Tabel 4.1.1 <i>Ip Address</i>	52
Tabel 4.2.1 <i>Download Dan Upload Saya</i>	72
Tabel 4.2.1 Lanjutan	73
Tabel 4.2.2 <i>Download Dan Upload Orang Tua</i>	73
Tabel 4.2.2 Lanjutan	74
Tabel 4.2.3 <i>Download Dan Upload Adik</i>	74
Tabel 4.2.3 Lanjutan	75

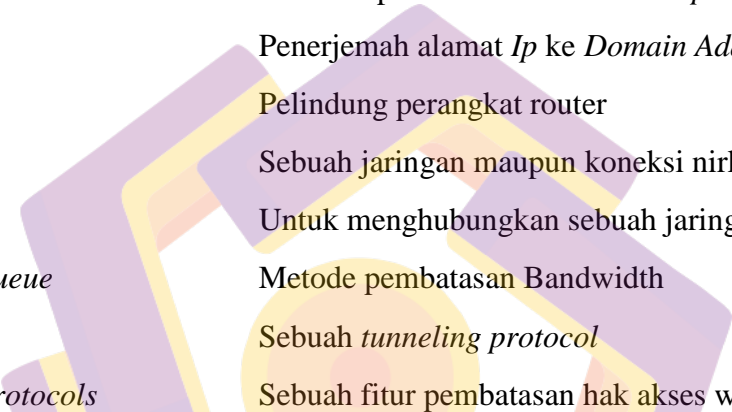
## DAFTAR GAMBAR

Gambar 3.4.1 Metode PPDIOO	47
Gambar 3.5.1 <i>Flow Chart</i> PPDIOO	49
Gambar 3.6.1 Topologi Jaringan	50
Gambar 4.1.1 <i>Address List</i>	52
Gambar 4.1.2 <i>DHCP Server</i>	53
Gambar 4.1.3 <i>DNS Setting</i>	53
Gambar 4.1.4 <i>Firewall</i>	54
Gambar 4.1.5 <i>Test Ping</i> Mikrotik	54
Gambar 4.1.6 <i>Setting Ip Address PC</i>	55
Gambar 4.1.7 <i>Security Profile</i>	56
Gambar 4.1.8 <i>Wireless Interface</i>	57
Gambar 4.1.9 <i>Bridge</i>	58
Gambar 4.1.10 <i>Bridge Ports</i>	58
Gambar 4.1.11 <i>Wireless Tables</i>	58
Gambar 4.1.12 <i>Hotspot Servers</i>	59
Gambar 4.1.13 <i>Hotspot Server Profile General</i>	60
Gambar 4.1.14 <i>Hotspot Server Profile Login</i>	60
Gambar 4.1.15 <i>Hotspot Users</i>	61
Gambar 4.1.16 <i>Simple Queue</i>	61
Gambar 4.1.17 <i>Queue Types</i>	62
Gambar 4.1.18 <i>Queue Tree</i>	62
Gambar 4.1.19 <i>Firewall Mangle</i>	63
Gambar 4.1.20 <i>L2TP Server</i>	63
Gambar 4.1.21 <i>PPP Secrets</i>	64
Gambar 4.1.22 <i>PPP Profiles</i>	64
Gambar 4.1.23 <i>Firewall L7 Protocol</i>	65
Gambar 4.1.24 <i>Firewall Filter Rules</i>	65
Gambar 4.2.1 <i>Hotspot Saya Login</i>	66
Gambar 4.2.2 <i>Hotspot Orangtua Login</i>	67
Gambar 4.2.3 <i>Hotspot Adik Login</i>	67
Gambar 4.2.4 <i>Hotspot Saya Berhasil Login</i>	68
Gambar 4.2.5 <i>Hotspot Orangtua Berhasil Login</i>	68
Gambar 4.2.6 <i>Hotspot Adik Berhasil Login</i>	69
Gambar 4.2.7 <i>Hotspot Active User</i>	69
Gambar 4.2.8 <i>Ip Address DHCP Hotspot Saya</i>	70
Gambar 4.2.9 <i>Ip Address DHCP Hotspot Orangtua</i>	71
Gambar 4.2.10 <i>Ip Address DHCP Hotspot Adik</i>	71
Gambar 4.2.11 Hasil Blokir Akses Twitter Saya	76
Gambar 4.2.12 Hasil Blokir Akses Instagram Saya	77
Gambar 4.2.13 Hasil Blokir Akses Facebook Saya	77
Gambar 4.2.14 Hasil Blokir Akses Twitter Orangtua	78
Gambar 4.2.15 Hasil Blokir Akses Instagram Orangtua	78
Gambar 4.2.16 Hasil Blokir Akses Facebook Orangtua	79
Gambar 4.2.17 Hasil Blokir Akses Twitter Adik	79

Gambar 4.2.18 Hasil Blokir Akses Instagram Adik	80
Gambar 4.2.19 Hasil Blokir Akses Facebook Adik	80
Gambar 4.2.20 <i>Setup Connection</i>	81
Gambar 4.2.21 <i>Connect to Workplace</i>	82
Gambar 4.2.22 <i>Internet Address VPN</i>	82
Gambar 4.2.23 <i>VPN Username dan Password</i>	83
Gambar 4.2.24 <i>VPN Connecting</i>	83
Gambar 4.2.25 <i>Connection Error</i>	84
Gambar 4.2.26 <i>VPN Connection Properties</i>	85
Gambar 4.2.27 <i>VPN Connection Properties Advance Settings</i>	85
Gambar 4.2.28 <i>Connect VPN Connection</i>	86
Gambar 4.2.29 <i>VPN Pada Personal Computer</i>	87
Gambar 4.2.30 <i>VPN Pada Mikrotik</i>	87
Gambar 4.2.31 <i>Active Connection L2TP VPN</i>	97
Gambar 4.2.32 <i>Kendala</i>	88
Gambar 4.2.33 <i>Legacy Mode</i>	89



## DAFTAR ISTILAH



<i>Bandwidth</i>	Sebuah besaran data yang dapat melewati network
<i>VPN</i>	Sebuah sambungan komunikasi yang bersifat pribadi
<i>Hotspot</i>	Sebuah jaringan yang dapat diakses tanpa kabel
<i>Ip Address</i>	Sekumpulan bilangan biner
<i>PPDIOO</i>	Metode pengembangan jaringan komputer
<i>DHCP SERVER</i>	Protokol pendistribusian alamat <i>Ip Address</i>
<i>DNS</i>	Penerjemah alamat <i>Ip</i> ke <i>Domain Address</i>
<i>Firewall</i>	Pelindung perangkat router
<i>Wireless</i>	Sebuah jaringan maupun koneksi nirkabel
<i>Bridge</i>	Untuk menghubungkan sebuah jaringan berbeda
<i>Simple Queue</i>	Metode pembatasan Bandwidth
<i>L2TP</i>	Sebuah <i>tunneling protocol</i>
<i>Layer7 Protocols</i>	Sebuah fitur pembatasan hak akses web

## INTISARI

Melihat pesatnya perkembangan jaringan internet dan teknologi saat ini yang mempengaruhi sektor sosial maupun pendidikan yang sekarang umumnya menggunakan jaringan internet sebagai sarana komunikasi, rekreasi, penyelesaian tugas maupun pekerjaan yang senantiasa di selesaikan di rumah dikarenakan kondisi new normal yang sekarang tengah dihadapi, dan dikhawatirkan akan berdampak pada psikologis yang disebabkan oleh suatu hal negative yang terkandung dalam dunia maya atau internet dan kerentanan keamanan.

apabila tidak digunakan secara bijak pada suatu hal yang terkoneksi dengan jaringan internet tersebut yang disebabkan oleh kelalaian maupun ketidaktahuan akan pentingnya keamanan dan kesehatan jaringan yang akan menimbulkan kerugian pada pengguna jaringan tersebut, dinatara kerugian tersebut, antara lain adalah terjadinya serangan maupun akses hal illegal yang disebabkan oleh ketidaktahuan atau kelalaian pengguna sah terhadap jaringan dan akses illegal tanpa seizin pemilik maupun pengguna yang sah.

dalam hal ini dikhawatirkan jaringan yang tentunya di gunakan oleh anggota rumah atau keluarga dan beberapa pengguna lain yang di izinkan menggunakan jaringan tersebut mengakses hal yang tidak aman maupun illegal yang dapat menyebabkan kerentanan keamanan jaringan, oleh karena itu sangat penting untuk mengamankan dan memanajemen suatu jaringan yang terkoneksi dengan internet supaya terbentuknya jaringan aman dan terorganisir, dan sehat untuk digunakan dalam lingkungan rumah sosial keluarga sesuai kebutuhan masing masing individu.

**Kata-kunci :** Jaringan, Internet, Keamanan, Rumah, Illegal

## Abstract

*Seeing the rapid development of the internet network and current technology that affects the social and educational sectors, which now generally use the internet network as a means of communication, recreation, completion of tasks and work that are always completed at home due to the new normal conditions that are currently being faced, and it is feared that it will have an impact psychologically caused by a negative thing contained in cyberspace or the internet and security vulnerabilities.*

*if it is not used wisely on something connected to the internet network caused by negligence or ignorance of the importance of network security and health which will cause losses to network users, among these losses, among others are attacks or access to illegal things caused by ignorance or negligence of legitimate users of the network and illegal access without the permission of the owner or authorized user.*

*in this case it is feared that the network is certainly used by members of the house or family and several other users who are allowed to use the network to access things that are not safe or illegal which can cause network security vulnerabilities, therefore it is very important to secure and manage a network that is safe and secure. connected to the internet so that a safe and organized network is formed, and is healthy for use in a family social home environment according to the needs of each individual.*