

**IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER*
UNTUK OPTIMALISASI KEAMANAN MIKROTIK DAN
PEMERATAAN AKSES INTERNET**

SKRIPSI



**ANGGI SAPUTRA
2022230007**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH
2026**

**IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER*
UNTUK OPTIMALISASI KEAMANAN MIKROTIK DAN
PEMERATAAN AKSES INTERNET**

Disusun Untuk Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana
Program Studi Informatika Universitas Prabumulih



**ANGGI SAPUTRA
2022230007**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH
2026**

HALAMAN PENGESAHAN

IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER* UNTUK OPTIMALISASI KEAMANAN MIKROTIK DAN PEMERATAAN AKSES INTERNET

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Program Studi Informatika
Universitas Prabumulih

Oleh :

Anggi Saputra
2022230007

Prabumulih, 10 Juni 2026

Pembimbing I



Iwan Setiawan, S.Kom., M.Kom.
NUPTK. 1541769670130303

Pembimbing II



Hermizahadiwidastra, S.Kom., M.Kom.
NUPTK. 0549767668231073

Ketua Program Studi
Informatika



Iwan Setiawan, S.Kom., M.Kom.
NUPTK. 1541769670130303

HALAMAN PERSETUJUAN

Skripsi ini dengan judul “Implementasi Metode Autentikasi *User manager* untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet” telah dipertahankan dan disetujui dihadapan Tim Penguji Skripsi Program Studi Informatika Fakultas Ilmu Komputer Universitas Prabumulih pada tanggal 22 Juni 2026.

Prabumulih, 22 Juni 2026

Tim Penguji Tugas Akhir

Ketua:

Iwan Setiawan, S.Kom., M.Kom
NUPTK. 1541769670130303

()

Anggota:

1. Hermizahadiwidastra, S.Kom., M.Kom
NUPTK. 0549767668231073

()

2. Jepri Yandi, S.Kom., M.Kom
NUPTK. 3948771672130302

()

**Mengetahui,
Dekan Fakultas Ilmu Komputer**


(Khana Wijaya, S.Kom., M.Kom)
NUPTK. 7146768669130363

**Ketua Program Studi
Informatika**


(Iwan Setiawan, S.Kom., M.Kom)
NUPTK. 154176967013030

PERNYATAAN INTEGRITAS

Saya yang bertanda tangan di bawah ini

Nama : Anggi Saputra

NIM : 2022230007

Program Studi : Informatika

Menyatakan dengan sebenarnya bahwa, skripsi ini benar-benar merupakan hasil karya saya dan tidak terdapat karya orang lain, apabila di kemudian hari terbukti atau dapat dibuktikan bahwa tugas akhir ini hasil *plagiasi*, maka saya bersedia menerima sanksi sesuai dengan ketentuan yang berlaku atas perbuatan tersebut.



Prabumulih, 22 Juni 2026

Yang membuat pernyataan,



Anggi Saputra

NIM. 2022230007

ABSTRAK

Implementasi Metode Autentikasi *User manager* Untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet

Anggi Saputra, 2022230007, 2026

Perkembangan teknologi informasi mendorong institusi pendidikan untuk meningkatkan kualitas layanan digital, termasuk pengelolaan jaringan internet. Di SMK Negeri 3 Prabumulih, jaringan internet belum memiliki mekanisme autentikasi pengguna sehingga seluruh pengguna masih mengakses jaringan menggunakan satu kata sandi *wi-fi*. Kondisi tersebut menyebabkan pembobolan kata sandi, pengelolaan *bandwidth* yang belum optimal, ketidakmerataan akses internet antara ruang kantor dan ruang praktik Teknik Sepeda Motor (TSM) serta Teknik Kendaraan Ringan (TKR), serta masih rentan terhadap gangguan dan akses yang tidak sah dalam jaringan. Penelitian ini bertujuan merancang simulasi topologi jaringan dengan mengintegrasikan autentikasi *user manager* pada *router* mikrotik untuk meningkatkan keamanan jaringan dan pemerataan akses internet. Rancangan meliputi penerapan manajemen *bandwidth*, penambahan *access point* pada ruang praktik, serta konfigurasi keamanan berupa pembatasan hak akses administrator, pemblokiran situs yang tidak sesuai dengan lingkungan pendidikan, dan mekanisme pengamanan untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan. Hasil simulasi menunjukkan bahwa autentikasi pengguna, pembagian *bandwidth*, dan konfigurasi keamanan dapat berjalan sesuai dengan rancangan sehingga meningkatkan keamanan jaringan serta pemerataan akses internet. Hasil penelitian ini diharapkan dapat menjadi usulan pengembangan jaringan internet yang lebih aman, terstruktur, dan merata di SMK Negeri 3 Prabumulih.

Kata Kunci: Autentikasi *User manager*, Mikrotik, Manajemen *Bandwidth*, Keamanan Jaringan.

ABSTRACT

Implementation of the User manager Authentication Method to Optimize Mikrotik Security and Equalize Internet Access

Anggi Saputra, 2022230007, 2026

The advancement of information technology has encouraged educational institutions to improve the quality of digital services, including internet network management. At SMK Negeri 3 Prabumulih, the internet network does not yet implement a user authentication mechanism, allowing all users to access the network using a single shared wi-fi password. This condition leads to password breaches, ineffective bandwidth management, unequal internet access between the administrative office and the Motorcycle Engineering (TSM) and Light Vehicle Engineering (TKR) practice rooms, as well as vulnerability to unauthorized access and interference within the network. This study aims to design a network topology simulation by integrating the user manager authentication method on a mikrotik router to improve network security and ensure more equitable internet access. The proposed design includes bandwidth management, the addition of access points in the practice rooms, and security configurations such as administrator-only access control, and blocking access to websites that are inappropriate for the educational environment. Simulation results indicate that user authentication, bandwidth management, and network security configurations operate as intended, thereby improving network security and supporting more balanced internet access. The proposed network design is expected to serve as a reference for developing a more secure, well-structured, and equitable internet network at SMK Negeri 3 Prabumulih.

Keywords: *User manager Authentication, MikroTik, Bandwidth Management, Network Security.*

KATA PENGANTAR

Puji syukur saya panjatkan atas kehadiran Allah SWT yang telah memberikan segala nikmat dan karunia-Nya kepada kita semua, sehingga skripsi dengan judul “Implementasi Metode Autentikasi *User manager* untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet” dapat diselesaikan sesuai dengan rencana dan waktu yang ditargetkan.

Skripsi ini merupakan salah satu syarat untuk mendapatkan gelar Sarjana di Program Studi S1 Informatika Fakultas Ilmu Komputer Universitas Prabumulih. Penulis banyak menerima bantuan, arahan, dan bimbingan dari berbagai pihak. Penulis mengucapkan terima kasih kepada:

1. Ibu Dr. Yuniar Pratiwi, S.Si., M.Si selaku Rektor Universitas Prabumulih.
2. Bapak Andi Christian, S.Kom., M.Kom selaku Wakil Rektor Universitas Prabumulih.
3. Bapak Khana Wijaya, S.Kom., M.Kom selaku Dekan Fakultas Universitas Prabumulih.
4. Ibu Suhartini, S.Kom., M.Kom selaku Wakil Dekan Bidang Keuangan Fakultas Ilmu Komputer Universitas Prabumulih.
5. Ibu Nur Aini H, S.Kom., M.Si., M.Kom selaku Wakil Dekan Bidang Kemahasiswaan sekaligus selaku Pembimbing Akademik yang telah memberikan bimbingan dan masukan kepada penulis selama perkuliahan.
6. Bapak Iwan Setiawan, S.Kom., M.Kom selaku Ketua Program Studi Informatika Universitas Prabumulih sekaligus Pembimbing I yang telah memberikan bimbingan dan arahan selama penyusunan skripsi ini.
7. Bapak Hermizahadiwidastra, S.Kom., M.Kom selaku Pembimbing II yang telah memberikan bimbingan, saran, serta waktu selama proses penyusunan skripsi ini.
8. Seluruh Bapak dan Ibu Dosen Program Studi Informatika yang telah memberikan ilmu dan wawasan selama perkuliahan.
9. Bapak Achmad Sukri, S.Pd., M.Si selaku Kepala Sekolah yang telah memberikan izin penelitian.

10. Bapak Harry Sunarya, S.T selaku Ketua Program Studi Teknik Kendaraan Ringan Otomotif (TKRO) yang telah memberikan informasi mengenai kendala jaringan internet di ruang praktik TKR.
11. Ibu Rahmi Widia Pratiwi, S.T selaku Ketua Kompetensi Teknik Bisnis Sepeda Motor (TBSM) yang telah memberikan informasi terkait kondisi akses internet di ruang praktik TSM.
12. Kedua orang tua yang senantiasa memberikan doa, dukungan, motivasi, perhatian, serta pengorbanan yang tiada henti kepada penulis sehingga dapat menyelesaikan skripsi ini.
13. Maulidia Rosinta, sebagai pasangan penulis, yang telah memberikan doa, dukungan, semangat, motivasi, serta pendampingan selama proses penyusunan skripsi ini sehingga skripsi ini dapat diselesaikan dengan baik.
14. Diri sendiri, terima kasih telah bertahan, berjuang, dan tidak menyerah hingga sampai di titik ini. Pencapaian ini adalah buah dari kerja keras dan kesabaran diri.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan penelitian dan pengembangan akses internet ini di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi penulis serta semua pihak yang berkepentingan.

Prabumulih, 22 Juni 2026

Penulis



ANGGI SAPUTRA

DAFTAR ISI

	Halaman
HALAMAN JUDUL DALAM	i
HALAMAN PENGESAHAN	ii
HALAMAN PERSETUJUAN	iii
PERNYATAAN INTEGRITAS	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
DAFTAR LAMPIRAN	xxi
DAFTAR SINGKATAN.....	xxii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA.....	8
2.1 Pengertian Implementasi	8
2.2 Pengertian <i>User manager</i>	8
2.3 Pengertian Keamanan Jaringan	9
2.4 Pengertian Mikrotik	10
2.5 Pengertian <i>Access point</i>	10
2.6 Pengertian Manajemen <i>Bandwidth</i>	11
2.7 Pengertian Internet.....	12
2.8 Pengertian <i>Figma</i>	12

2.9	Penelitian Terdahulu	13
2.10	Kerangka Berpikir Penelitian	15
BAB III METODE PENELITIAN		19
3.1	Objek dan Subjek Penelitian.....	19
3.1.1	Subjek Penelitian	19
3.1.2	Objek Penelitian	19
3.1.3	Sejarah	20
3.1.4	Visi Misi SMK Negeri 3 Prabumulih	20
3.1.5	Struktur Organisasi	23
3.1.6	Jadwal Penelitian	26
3.2	Metode Penelitian	27
3.3	Sumber Data	28
3.3.1	Data Primer.....	28
3.3.2	Data Sekunder	29
3.4	Teknik Pengumpulan Data.....	30
3.4.1	Observasi	31
3.4.2	Wawancara.....	31
3.4.3	Dokumentasi.....	32
3.5	Metode Pengembangan Jaringan	32
3.5.1	<i>Analysis</i> (Analisis Kebutuhan)	34
3.5.2	<i>Design</i> (Perancangan Topologi Jaringan).....	34
3.5.3	<i>Simulation</i> (Simulasi Jaringan).....	34
3.5.4	<i>Monitoring</i> (Pemantauan Hasil Simulasi)	35
3.6	Alat Bantu Perancangan	35
3.6.1	Alat Bantu Utama	36
3.6.2	Alat Bantu Proses Konfigurasi Jaringan.....	36
3.6.3	Alat Bantu Simulasi.....	37
3.6.4	Perangkat Implementasi (<i>Prototype</i>)	40
3.7	Pengujian Simulasi	41
BAB IV ANALISA DAN PERANCANGAN.....		52
4.1	Analisa Sistem	52
4.1.1	Analisa dan Evaluasi Sistem Berjalan	52

4.1.2	Analisa Kebutuhan	53
4.2	Perancangan Sistem yang Diusulkan.....	59
4.2.1	Topologi Jaringan	59
4.2.2	Simulasi Perangkat Jaringan.....	60
4.2.3	Perancangan Sistem (Logis)	63
4.2.4	Perancangan Konfigurasi Jaringan	95
BAB V HASIL DAN PEMBAHASAN		109
5.1	Spesifikasi Perangkat.....	109
5.1.1	Perangkat Keras yang digunakan	109
5.1.2	Perangkat Lunak yang digunakan	110
5.2	Konfigurasi <i>Cisco Packet Tracer</i>	112
5.2.1	<i>FastEthernet 0/0</i>	112
5.2.2	<i>FastEthernet 0/1</i>	113
5.2.3	<i>FastEthernet 1/0</i>	114
5.2.4	<i>FastEthernet 1/1</i>	115
5.2.5	Konfigurasi <i>Gateway Internet Server User manager</i>	116
5.2.6	<i>Switch TSM</i>	117
5.2.7	<i>Access point TSM</i>	118
5.2.8	<i>PC TSM</i>	119
5.2.9	<i>Laptop TSM</i>	120
5.2.10	<i>Smartphone TSM</i>	121
5.2.11	<i>Switch TKR</i>	122
5.2.12	<i>Access point TKR</i>	123
5.2.13	<i>PC TKR</i>	124
5.2.14	<i>Laptop TKR</i>	125
5.2.15	<i>Smartphone TKR</i>	126
5.2.16	<i>Switch Ruang Kantor</i>	127
5.2.17	<i>Access point Ruang Kantor</i>	128
5.2.18	<i>PC Ruang Kantor</i>	129
5.2.19	<i>Laptop Ruang Kantor</i>	130
5.2.20	<i>Smartphone Ruang Kantor</i>	131
5.2.21	<i>Printer Ruang Kantor</i>	132

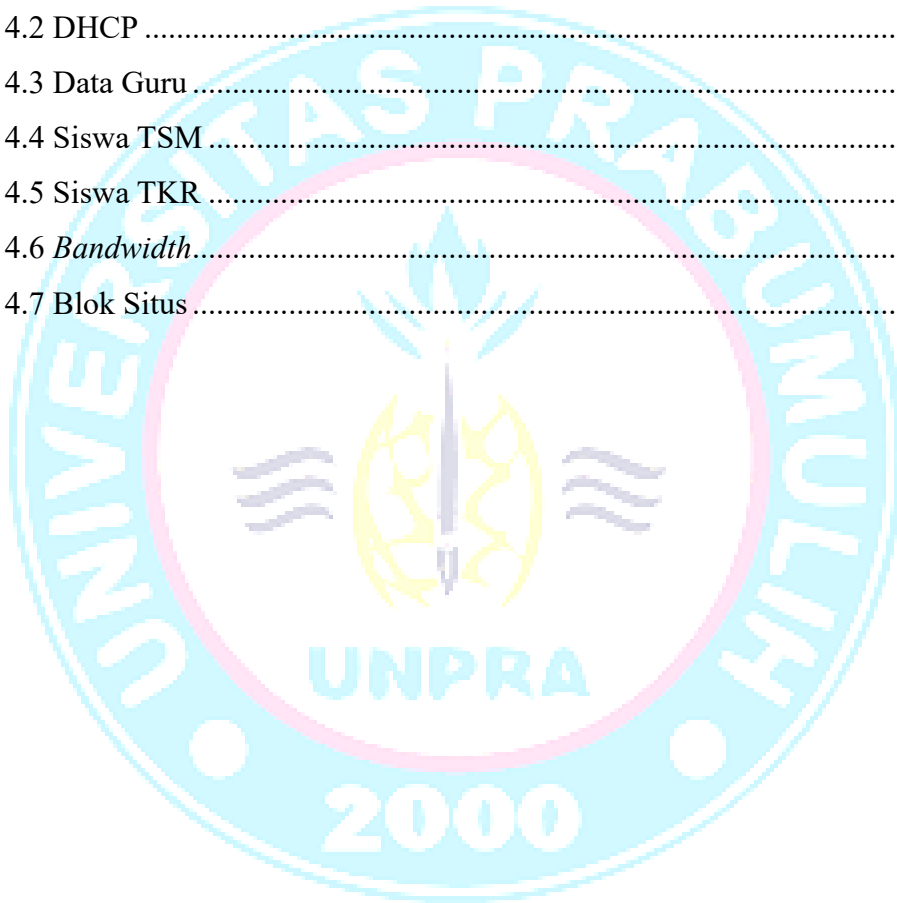
5.3	Konfigurasi Winbox	133
5.3.1	Konfigurasi IP Address	133
5.3.2	DHCP Client	134
5.3.3	NAT Masquerade	135
5.3.4	DNS Setting	136
5.3.5	Hotspot Server	137
5.3.6	Server Profile Hotspot	138
5.3.7	Users Hotspot	140
5.3.8	Users Profile	141
5.3.9	Users Active	142
5.3.10	IP Pool	143
5.3.11	Simple Queue	144
5.3.12	Mangle	145
5.3.13	Blok Akses Konfigurasi	146
5.3.14	Pengamanan Jaringan dengan Pemblokiran Website	147
5.3.15	Schedule	148
5.3.16	Konfigurasi Firewall Client	149
5.4	Konfigurasi Access point	155
5.4.1	Konfigurasi AP Kantor	155
5.4.2	Konfigurasi AP TKR	157
5.4.3	Konfigurasi AP TSM	159
5.5	Pengujian Jaringan	161
5.5.1	Pengujian Menggunakan Web Browser / Chrome	161
5.5.2	Pengujian Menggunakan Command Prompt	179
5.5.3	Pengujian Menggunakan CLI Router Mikrotik	180
5.5.4	Pengujian Menggunakan Simple PDU	182
5.5.5	Pengujian Menggunakan Speedtest	183
5.5.6	Pengujian Menggunakan Angry IP Scanner	185
5.5.7	Pengujian Menggunakan Nmap	188
5.5.8	Pengujian Menggunakan Iperf3	191
5.5.9	Pengujian Menggunakan Aplikasi Pihak Ketiga	196

BAB VI KESIMPULAN DAN SARAN.....	238
6.1 Kesimpulan.....	238
6.2 Saran	239
DAFTAR PUSTAKA.....	240
LAMPIRAN.....	248



DAFTAR TABEL

	Halaman
Tabel 2.1 Penelitian Terdahulu.....	13
Tabel 3.1 Jadwal Penelitian.....	27
Tabel 3.2 Simbol <i>Flowchart</i>	37
Tabel 4.1 <i>IP Address</i>	100
Tabel 4.2 DHCP	101
Tabel 4.3 Data Guru	102
Tabel 4.4 Siswa TSM	103
Tabel 4.5 Siswa TKR	105
Tabel 4.6 <i>Bandwidth</i>	107
Tabel 4.7 Blok Situs	108



DAFTAR GAMBAR

	Halaman
Gambar 2.1 Kerangka Berpikir Penelitian	16
Gambar 3.1 Struktur Organisasi SMK Negeri 3 Prabumulih	23
Gambar 3.2 Tahapan Metode NDLC	33
Gambar 4.1 Topologi Jaringan	59
Gambar 4.2 Modem <i>Iconnet</i>	61
Gambar 4.3 Mikrotik	62
Gambar 4.4 <i>Switch</i>	62
Gambar 4.5 <i>Access point</i>	63
Gambar 4.6 <i>Flowchart</i> Sistem Jaringan	64
Gambar 4.7 <i>Flowchart Form Login</i>	65
Gambar 4.8 Alur Pengujian CMD / <i>Command Prompt</i>	67
Gambar 4.9 Alur Pengujian CLI	69
Gambar 4.10 Alur Pengujian Simple PDU	71
Gambar 4.11 Alur Pengujian <i>Speedtest</i>	73
Gambar 4.12 Alur Pengujian Winbox	75
Gambar 4.13 Alur Pengujian <i>Angry IP Scanner</i>	77
Gambar 4.14 Alur Pengujian Nmap	79
Gambar 4.15 Alur Pengujian Iperf3	81
Gambar 4.16 Alur Pengujian <i>NetCut</i>	83
Gambar 4.17 Alur Pengujian <i>Command Prompt</i> (Cek arp -a)	85
Gambar 4.18 Alur Pengujian <i>Wireless Network Watcher</i>	87
Gambar 4.19 Alur Pengujian P2Pover	89
Gambar 4.20 Alur Pengujian TMAC	91
Gambar 4.21 <i>Network Diagram</i>	93
Gambar 4.22 Wilayah Ruang Kantor	95
Gambar 4.23 Wilayah Ruang Praktik TSM	96
Gambar 4.24 Wilayah Ruang Praktik TKR	97
Gambar 4.25 <i>Form Login Client</i>	98

Gambar 4.26 <i>Form Status Client</i>	99
Gambar 5.1 <i>FastEthernet 0/0</i>	112
Gambar 5.2 <i>FastEthernet 0/1</i>	113
Gambar 5.3 <i>FastEthernet 1/0</i>	114
Gambar 5.4 <i>FastEthernet 1/1</i>	115
Gambar 5.5 <i>Default Gateway 192.168.100.1</i>	116
Gambar 5.6 <i>Switch TSM</i>	117
Gambar 5.7 <i>Mematikan DHCP Access point TSM</i>	118
Gambar 5.8 <i>PC TSM</i>	119
Gambar 5.9 <i>Laptop TSM</i>	120
Gambar 5.10 <i>Smartphone TSM</i>	121
Gambar 5.11 <i>Switch TKR</i>	122
Gambar 5.12 <i>Access point TKR</i>	123
Gambar 5.13 <i>PC TKR</i>	124
Gambar 5.14 <i>Laptop TKR</i>	125
Gambar 5.15 <i>Smartphone TKR</i>	126
Gambar 5.16 <i>Switch Ruang Kantor</i>	127
Gambar 5.17 <i>Access point Ruang Kantor</i>	128
Gambar 5.18 <i>PC Ruang Kantor</i>	129
Gambar 5.19 <i>Laptop Ruang Kantor</i>	130
Gambar 5.20 <i>Smartphone Ruang Kantor</i>	131
Gambar 5.21 <i>Printer Ruang Kantor</i>	132
Gambar 5.22 <i>Address List</i>	133
Gambar 5.23 <i>DHCP Client</i>	134
Gambar 5.24 <i>NAT Masquerade</i>	135
Gambar 5.25 <i>DNS Setiing</i>	136
Gambar 5. 26 <i>Hotspot Server</i>	137
Gambar 5.27 <i>Server Profile Hotspot</i>	138
Gambar 5.28 <i>Login by HTTP CHAP</i>	138
Gambar 5.29 <i>Users Hotspot</i>	140
Gambar 5.30 <i>Users Profile</i>	141
Gambar 5.31 <i>Users Active</i>	142

Gambar 5.32 <i>IP Pool</i>	143
Gambar 5.33 <i>Simple Queue</i>	144
Gambar 5.34 <i>Mangle</i>	145
Gambar 5.35 Blok Akses Konfigurasi	146
Gambar 5.36 Blok <i>Website</i>	147
Gambar 5.37 <i>Schedule</i>	148
Gambar 5.38 Konfigurasi <i>Firewall Client TSM</i>	149
Gambar 5.39 Konfigurasi <i>Firewall Tambahan Client TSM</i>	150
Gambar 5.40 Konfigurasi <i>Firewall Client TKR</i>	151
Gambar 5.41 Konfigurasi <i>Firewall Tambahan Client TKR</i>	152
Gambar 5.42 Konfigurasi <i>Firewall Client Kantor</i>	153
Gambar 5.43 Konfigurasi <i>Firewall Tambahan Client Kantor</i>	154
Gambar 5.44 DHCP AP Kantor	155
Gambar 5.45 <i>Enable Client Isolation Kantor</i>	156
Gambar 5.46 DHCP AP TKR.....	157
Gambar 5.47 <i>Enable Client Isolation TKR</i>	158
Gambar 5.48 DHCP AP TSM	159
Gambar 5.49 <i>Enable Client Isolation TSM</i>	160
Gambar 5.50 <i>Captive Portal Form Login</i>	161
Gambar 5.51 <i>Captive Portal Form Status</i>	162
Gambar 5.52 Sebelum di <i>Block Akses WebFig</i>	163
Gambar 5.53 Sudah di <i>Block Akses WebFig</i>	164
Gambar 5.54 Sebelum di <i>Block Website https://stake.com/</i>	165
Gambar 5.55 Sudah di <i>Block Website https://stake.com/</i>	166
Gambar 5.56 Sebelum di <i>Block Website https://pulaujudiasia.com/</i>	167
Gambar 5.57 Sudah di <i>Block Website https://pulaujudiasia.com/</i>	168
Gambar 5.58 Sebelum di <i>Block Website https://linkselamatjudi.live/</i>	169
Gambar 5.59 Sudah di <i>Block Website https://linkselamatjudi.live/</i>	170
Gambar 5.60 Sebelum di <i>Block Website https://www.onlinedominogames.com/</i>	171
Gambar 5.61 Sudah di <i>Block Website https://www.onlinedominogames.com/</i> ..	172
Gambar 5.62 Sebelum di <i>Block Website https://pwa.playonline.poker/</i>	173
Gambar 5.63 Sudah di <i>Block Website https://pwa.playonline.poker/</i>	174

Gambar 5.64 Sebelum di <i>Block Website</i> https://pokerpatio.com/	175
Gambar 5.65 Sudah di <i>Block Website</i> https://pokerpatio.com/	176
Gambar 5.66 Pengujian <i>MAC Address Admin</i>	177
Gambar 5.67 Akses Konfigurasi Perangkat <i>Client</i>	177
Gambar 5.68 Pengujian <i>Command Prompt</i>	179
Gambar 5.69 NAT (<i>Network Address Translation</i>).....	180
Gambar 5.70 Perangkat <i>Client</i> yang terhubung	180
Gambar 5.71 Pengujian <i>Simple PDU</i>	182
Gambar 5.72 <i>Speedtest</i> Guru.....	183
Gambar 5.73 <i>Speedtest</i> Siswa TSM	183
Gambar 5.74 <i>Speedtest</i> Siswa TKR	184
Gambar 5.75 <i>Scanning</i> 192.168.30.1	185
Gambar 5.76 <i>Scanning</i> 192.168.20.1	186
Gambar 5.77 <i>Scanning</i> 192.168.10.1	186
Gambar 5.78 Nmap 192.168.10.1	188
Gambar 5.79 Nmap 192.168.20.1	189
Gambar 5.80 Nmap 192.168.30.1	190
Gambar 5.81 Sebagai <i>Server</i> dengan IP 192.168.10.25.....	191
Gambar 5.82 Sebagai <i>Client</i> dengan IP 192.168.10.20	192
Gambar 5.83 Sebagai <i>Server</i> dengan IP 192.168.20.36.....	193
Gambar 5.84 Sebagai <i>Client</i> dengan IP 192.168.20.41	193
Gambar 5.85 Sebagai <i>Server</i> dengan IP 192.168.30.23.....	194
Gambar 5.86 Sebagai <i>Client</i> dengan IP 192.168.30.24	195
Gambar 5.87 <i>Netcut</i> sisi TSM.....	196
Gambar 5.88 Sebelum di Aktifkan di Sisi TSM	197
Gambar 5.89 Sudah di Aktifkan di Sisi TSM	198
Gambar 5.90 <i>Netcut</i> sisi TKR	199
Gambar 5.91 Sebelum di Aktifkan di Sisi TKR.....	200
Gambar 5.92 Sudah di Aktifkan di Sisi TKR.....	201
Gambar 5.93 <i>Netcut</i> sisi Kantor	202
Gambar 5.94 Sebelum di Aktifkan di Sisi Kantor.....	203
Gambar 5.95 Sudah di Aktifkan di Sisi Kantor	204

Gambar 5.96 Laptop Korban TSM	205
Gambar 5.97 Hasil Sebelum Diterapkan <i>Client Isolation</i> TSM	206
Gambar 5.98 Hasil Sudah Diterapkan <i>Client Isolation</i> TSM	207
Gambar 5.99 Laptop Korban TKR.....	208
Gambar 5.100 Hasil Sebelum Diterapkan <i>Client Isolation</i> TKR.....	209
Gambar 5.101 Hasil Sudah Diterapkan <i>Client Isolation</i> TKR.....	210
Gambar 5.102 Laptop Korban Kantor	211
Gambar 5.103 Hasil Sebelum Diterapkan <i>Client Isolation</i> Kantor.....	212
Gambar 5.104 Hasil Sudah Diterapkan <i>Client Isolation</i> Kantor.....	213
Gambar 5.105 Pengujian Sebelum Penerapan <i>Client Isolation</i> TSM.....	214
Gambar 5.106 Pengujian Sudah Penerapan <i>Client Isolation</i> TSM.....	215
Gambar 5.107 Pengujian Sebelum Penerapan <i>Client Isolation</i> TKR	216
Gambar 5.108 Pengujian Sudah Penerapan <i>Client Isolation</i> TKR	217
Gambar 5.109 Pengujian Sebelum Penerapan <i>Client Isolation</i> Kantor	218
Gambar 5.110 Pengujian Sebelum Penerapan <i>Client Isolation</i> Kantor	219
Gambar 5.111 <i>Rules Wi-Fi</i> Putus TSM.....	220
Gambar 5.112 <i>Start</i> Putus TSM Sesuai <i>Rules</i>	221
Gambar 5.113 Hasil P2Pover Sebelum Diterapkan <i>Client Isolation</i> TSM.....	222
Gambar 5.114 Hasil P2Pover Sudah Diterapkan <i>Client Isolation</i> TSM.....	223
Gambar 5.115 <i>Rules Wi-Fi</i> Putus TKR	224
Gambar 5.116 <i>Start</i> Putus TKR Sesuai <i>Rules</i>	225
Gambar 5.117 Hasil P2Pover Sebelum Diterapkan <i>Client Isolation</i> TKR	226
Gambar 5.118 Hasil P2Pover Sudah Diterapkan <i>Client Isolation</i> TKR	227
Gambar 5.119 <i>Rules Wi-Fi</i> Putus Kantor	228
Gambar 5.120 <i>Start</i> Putus Kantor Sesuai <i>Rules</i>	229
Gambar 5.121 Hasil P2Pover Sebelum Diterapkan <i>Client Isolation</i> Kantor.....	230
Gambar 5.122 Hasil P2Pover Sudah Diterapkan <i>Client Isolation</i> Kantor.....	231
Gambar 5.123 <i>Cookie</i> Dalam Keadaan <i>Default</i> / Tercentang	232
Gambar 5.124 Menyamar Menjadi MAC Korban	233
Gambar 5.125 Hasil Tidak Dihapus Ceklis <i>Cookie</i>	234
Gambar 5.126 <i>Cookie</i> Dalam Keadaan Tidak Tercentang	235
Gambar 5.127 Menyamar Menjadi MAC Korban	236

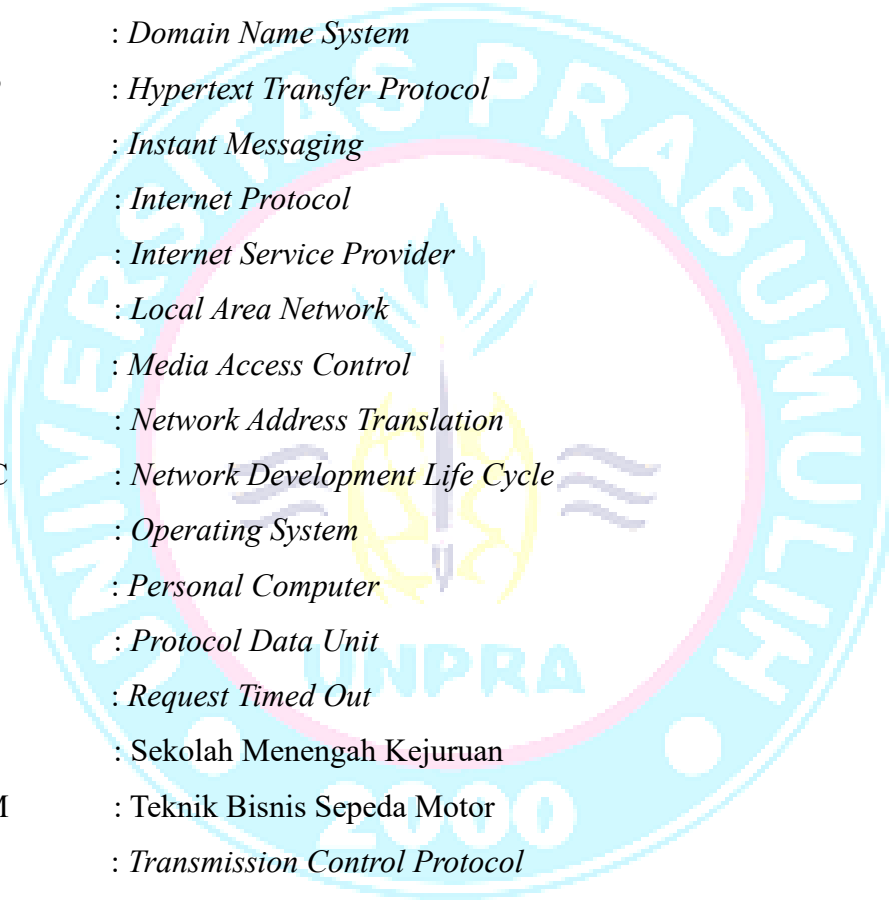


DAFTAR LAMPIRAN

	Halaman
Lampiran 1 Surat Permohonan Penelitian.....	248
Lampiran 2 Surat Balasan Permohonan Penelitian.....	249
Lampiran 3 Dokumentasi Wawancara & Observasi	250
Lampiran 4 Daftar Pertanyaan Wawancara.....	255



DAFTAR SINGKATAN



AP	: <i>Access point</i>
ARP	: <i>Address Resolution Protocol</i>
CHAP	: <i>Challenge Handshake Authentication Protocol</i>
CMD	: <i>Command Prompt</i>
CLI	: <i>Command Line Interface</i>
DHCP	: <i>Dynamic Host Configuration Protocol</i>
DNS	: <i>Domain Name System</i>
HTTP	: <i>Hypertext Transfer Protocol</i>
IM	: <i>Instant Messaging</i>
IP	: <i>Internet Protocol</i>
ISP	: <i>Internet Service Provider</i>
LAN	: <i>Local Area Network</i>
MAC	: <i>Media Access Control</i>
NAT	: <i>Network Address Translation</i>
NDLC	: <i>Network Development Life Cycle</i>
OS	: <i>Operating System</i>
PC	: <i>Personal Computer</i>
PDU	: <i>Protocol Data Unit</i>
RTO	: <i>Request Timed Out</i>
SMK	: <i>Sekolah Menengah Kejuruan</i>
TBSM	: <i>Teknik Bisnis Sepeda Motor</i>
TCP	: <i>Transmission Control Protocol</i>
TMAC	: <i>Technitium MAC Address Changer</i>
TKRO	: <i>Teknik Kendaraan Ringan Otomotif</i>
TKR	: <i>Teknik Kendaraan Ringan</i>
TSM	: <i>Teknik Sepeda Motor</i>
WAN	: <i>Wide Area Network</i>
Wi-Fi	: <i>Wireless Fidelity</i>
WPA2	: <i>Wi-Fi Protected Access 2</i>
WWW	: <i>World Wide Web</i>

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi memberikan pengaruh besar terhadap berbagai bidang kehidupan, termasuk bidang pendidikan. Dengan kemajuan seperti internet, perangkat seluler, dan platform pembelajaran daring, pendidikan kini lebih mudah diakses dan jangkauannya semakin luas. Transformasi ini memungkinkan terjadinya interaksi yang lebih dinamis antara pengajar dan siswa serta memperkaya pengalaman belajar melalui berbagai media (Nurhayati et al., 2024).

SMK Negeri 3 Prabumulih merupakan lembaga pendidikan kejuruan yang memanfaatkan layanan internet untuk mendukung kegiatan akademik dan administrasi. Pusat jaringan berada di ruang kantor yang dilengkapi mikrotik dan *access point* sebagai pengelola konektivitas. Namun pemanfaatan jaringan internet tersebut belum didukung dengan sistem pengelolaan dan pemerataan akses yang optimal, khususnya pada ruang praktik seperti Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR). Kondisi ini menunjukkan adanya kesenjangan antara kebutuhan pembelajaran berbasis digital dengan kesiapan serta pengelolaan infrastruktur jaringan yang tersedia.

Hasil observasi menunjukkan bahwa *router* mikrotik belum menerapkan mekanisme autentikasi pengguna, sehingga akses jaringan masih bergantung pada kata sandi *wi-fi* tanpa adanya sistem autentikasi khusus yang dapat membedakan identitas setiap pengguna dan menyebabkan sering terjadinya pembobolan *password wifi* di sekolah (Nurfanis et al., 2024). Selain itu, administrator belum memiliki kontrol terhadap penggunaan *bandwidth* sehingga distribusi jaringan tidak merata dan kecepatan akses internet menjadi tidak seimbang. Jaringan internet juga masih ada di ruang kantor, sementara ruang praktik TSM dan TKR belum ada akses internet. Akibatnya, kegiatan pembelajaran berbasis digital di ruang praktik sering terganggu karena keterbatasan jangkauan dan kualitas koneksi.

Peningkatan keamanan, efisiensi, dan jangkauan jaringan di SMK Negeri 3 Prabumulih dilakukan melalui perancangan jaringan berbasis simulasi yang didukung implementasi terbatas dengan menghubungkan jaringan dari ruang kantor

ke ruang praktik TSM dan TKR melalui penambahan *access point*. *Router* mikrotik digunakan sebagai pusat manajemen jaringan dengan penerapan autentikasi *user manager* serta pengaturan *bandwidth* antara ruang praktik TSM dan TKR. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun (Syahindra, 2022).

Untuk lebih meningkatkan keamanan jaringan, *router* mikrotik dikonfigurasi dengan pembatasan hak akses administrator sehingga hanya administrator yang berwenang dapat melakukan pengaturan dan perubahan konfigurasi jaringan. Selain itu, sistem juga memblokir akses ke situs-situs yang mengandung konten yang tidak sesuai dengan lingkungan pendidikan guna menjaga keamanan jaringan serta mendukung kedisiplinan dalam penggunaan internet di lingkungan sekolah. Sebagai lapisan keamanan tambahan, diterapkan mekanisme pengamanan untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan. Penerapan keamanan jaringan di sekolah sangat penting untuk melindungi data siswa, guru, dan administrasi dari penggunaan yang tidak sah (Nur Iman & Sholeh, 2024).

Penerapan manajemen *bandwidth* dilakukan untuk mengatur pembagian kapasitas jaringan antara guru di ruang kantor serta siswa di ruang praktik TSM dan TKR melalui konfigurasi pada *router* mikrotik. Pengujian dilakukan menggunakan *command prompt* dengan *test ping* ke alamat internet guna mengamati kualitas koneksi, serta *speedtest* untuk mengukur kecepatan *bandwidth* pada setiap ruangan. Hasil pengujian menunjukkan bahwa pembagian *bandwidth* telah berjalan sesuai dengan konfigurasi yang dirancang. Manajemen *bandwidth* diperlukan agar *bandwidth* yang ada terbagi sesuai kebutuhan pada setiap koneksi yang terhubung (Tsalil Amri & Selamat, 2025).

Sejumlah penelitian mendukung efektivitas konfigurasi jaringan di lingkungan pendidikan. Pengaturan *bandwidth* dan manajemen pengguna menggunakan mikrotik terbukti dapat menstabilkan koneksi dan meningkatkan pemerataan kecepatan akses di sekolah menengah (Anamatalu et al., 2023). Penelitian lain menunjukkan bahwa manajemen jaringan berbasis mikrotik dengan pengaturan DNS dan NAT meningkatkan efisiensi distribusi sinyal di lingkungan sekolah (Sundara et al., 2022). Namun, penelitian tersebut belum secara spesifik

membahas penerapan autentikasi *user manager* yang terintegrasi dengan manajemen *bandwidth* berbasis ruang praktik pada sekolah kejuruan, sehingga diperlukan penelitian yang sesuai dengan kebutuhan ruang praktik TSM dan TKR.

Di dalam jaringan komputer, *Domain Name System* (DNS) berperan penting di dalam menterjemahkan dan memetakan alamat *domain* ke dalam alamat *Internet Protocol* (IP) atau sebaliknya. Dengan demikian, DNS berfungsi sebagai sebuah *database* terdistribusi, untuk menyimpan data-data *hostname* dan *IP address* dari setiap komputer atau *server* pada jaringan (Pratama et al., 2024). *Network Address Translation* (NAT) adalah metode pemetaan ruang alamat IP ke yang lain dengan memodifikasi informasi alamat jaringan di *header* IP paket saat mereka *transit* melintasi perangkat perutean lalu lintas atau *router* (Rizqillah et al., 2023).

Penelitian ini dilakukan dalam bentuk simulasi penerapan metode autentikasi *user manager* pada jaringan lokal di SMK Negeri 3 Prabumulih yang meliputi ruang kantor, ruang praktik TSM, dan TKR. Selain itu, penelitian ini juga didukung dengan implementasi terbatas menggunakan perangkat nyata sebagai bentuk validasi terhadap hasil perancangan yang telah dibuat. Simulasi mencakup perancangan topologi jaringan, konfigurasi autentikasi, serta penambahan *access point* untuk memperluas jangkauan sinyal. Pemerataan akses internet diterapkan melalui pembagian *bandwidth* antara ruang praktik TSM dan TKR. Kebaruan penelitian ini terletak pada integrasi autentikasi *user manager* dan manajemen *bandwidth* berbasis ruang praktik dalam simulasi jaringan.

Tujuan Penelitian ini adalah memberikan solusi terhadap permasalahan distribusi dan keamanan jaringan di SMK Negeri 3 Prabumulih melalui rancangan simulasi topologi jaringan berbasis autentikasi *user manager* dan manajemen *bandwidth*, serta mengoptimalkan pemanfaatan jaringan internet di ruang praktik TSM dan TKR secara efektif dan optimal. Hasil rancangan diharapkan dapat menjadi acuan penerapan bagi pihak sekolah untuk meningkatkan efisiensi, pemerataan, dan keamanan akses internet di lingkungan SMK Negeri 3 Prabumulih. Berdasarkan uraian tersebut, penelitian ini berjudul “Implementasi Metode Autentikasi *User manager* untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet.”

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah ini adalah sebagai berikut:

1. Bagaimana cara menerapkan metode autentikasi *user manager* untuk meningkatkan keamanan jaringan internet di lingkungan sekolah?
2. Bagaimana pengaturan manajemen *bandwidth* dapat diterapkan untuk membedakan kebutuhan akses jaringan antara guru di ruang kantor serta siswa di ruang praktik Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR)?
3. Bagaimana rancangan jaringan dengan penambahan *access point* dapat memperluas jangkauan sinyal ke ruang praktik TSM dan TKR tanpa mengurangi kestabilan koneksi?
4. Bagaimana penerapan pengaturan pembatasan akses pada router dapat membatasi hak konfigurasi hanya bagi administrator, memblokir alamat-alamat situs yang mengarah pada konten yang tidak sesuai dengan lingkungan pendidikan, serta menerapkan mekanisme pengamanan untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan?
5. Bagaimana proses pengujian konektivitas internet dilakukan menggunakan perintah *ping* untuk memastikan jaringan yang telah dirancang dapat terhubung ke internet dengan baik?

1.3 Batasan Masalah

Penelitian ini dibatasi pada hal-hal berikut:

1. Pengujian pada *cisco packet tracer* dalam penelitian ini dibatasi hanya pada penggunaan fitur *simple PDU* untuk menguji konektivitas jaringan. Pengujian difokuskan pada verifikasi bahwa hanya perangkat administrator yang dapat melakukan ping ke *router* mikrotik sesuai dengan konfigurasi keamanan yang telah diterapkan.
2. Penelitian ini tidak membahas pemblokiran situs yang menggunakan domain dinamis atau domain yang terus berubah dan diperbarui secara

otomatis, sehingga efektivitas pemblokiran bergantung pada daftar domain yang telah dikonfigurasi oleh administrator jaringan.

3. Implementasi jaringan dibatasi pada penggunaan jaringan lokal (LAN) dan *hotspot* tanpa membahas pengelolaan jaringan internet skala besar.
4. Penelitian ini tidak membahas aspek keamanan jaringan tingkat lanjut seperti enkripsi data, *penetration testing*, serangan siber, maupun sistem keamanan jaringan enterprise secara mendalam.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menerapkan metode autentikasi *user manager* untuk meningkatkan keamanan jaringan internet melalui pengaturan *login*.
2. Menerapkan manajemen *bandwidth* untuk mengatur pembagian kapasitas jaringan antara guru di ruang kantor serta siswa di ruang praktik Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR).
3. Menerapkan pembatasan akses pada *router* agar hanya administrator yang dapat melakukan konfigurasi, memblokir situs yang tidak sesuai dengan lingkungan pendidikan, serta melindungi perangkat dari gangguan antar pengguna dalam jaringan.
4. Merancang sistem jaringan dengan penambahan *access point* agar jangkauan sinyal internet dapat menjangkau ruang praktik TSM dan TKR.
5. Melakukan pengujian terhadap jaringan yang telah dirancang baik melalui simulasi maupun implementasi terbatas untuk memastikan sistem berjalan sesuai dengan rancangan.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Manfaat Teoritis
 - a. Menambah wawasan dan referensi ilmiah dalam bidang manajemen jaringan komputer, khususnya terkait penerapan autentikasi *user*

manager, manajemen *bandwidth*, serta pengelolaan keamanan jaringan di lingkungan pendidikan.

- b. Menjadi bahan kajian dan rujukan bagi peneliti selanjutnya yang ingin mengembangkan sistem manajemen jaringan berbasis autentikasi pengguna.
- c. Memperkaya literatur akademik mengenai implementasi sistem kontrol akses dan distribusi *bandwidth* pada institusi pendidikan kejuruan.

2. Manfaat Praktis

- a. Bagi SMK Negeri 3 Prabumulih: Menjadi acuan dalam pengembangan dan pemerataan jaringan internet agar dapat menjangkau ruang praktik TSM dan TKR secara optimal.
- b. Bagi Guru dan Siswa: Meningkatkan kenyamanan serta pemerataan akses internet dalam mendukung proses pembelajaran berbasis digital, khususnya di ruang praktik TSM dan TKR.
- c. Bagi Administrator Sekolah: Memberikan panduan teknis dalam penerapan autentikasi pengguna, pembagian *bandwidth*, serta peningkatan keamanan jaringan seperti pembatasan akses *router* agar hanya administrator yang dapat melakukan konfigurasi, dan pemblokiran alamat situs yang tidak sesuai dengan kebijakan sekolah serta melindungi perangkat dari gangguan antar pengguna dalam jaringan.
- d. Bagi Pihak Lain: Dapat dijadikan contoh penerapan sistem autentikasi dan manajemen jaringan yang efektif bagi sekolah atau lembaga lain dengan permasalahan serupa.

1.6 Sistematika Penulisan

Penulisan Skripsi ini disusun agar memberikan gambaran yang jelas mengenai tahapan penelitian, sebagai berikut:

BAB I PENDAHULUAN

Menjelaskan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Berisi teori implementasi, *user manager*, keamanan jaringan, mikrotik, *access point*, manajemen *bandwidth*, internet. Bab ini juga mencakup hasil penelitian terdahulu dan kerangka berpikir penelitian.

BAB III METODE PENELITIAN

Menjelaskan metode penelitian yang digunakan, lokasi dan waktu penelitian, teknik pengumpulan data, metode pengembangan sistem, alat bantu perancangan, pengujian sistem.

BAB IV ANALISIS DAN PERANCANGAN

Bab ini membahas proses analisis serta perancangan simulasi jaringan yang dilakukan berdasarkan permasalahan yang diteliti. Tahapan analisis digunakan untuk mengidentifikasi kebutuhan simulasi sebagai landasan dalam merancang simulasi jaringan yang akan dikembangkan.

BAB V HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil pengujian simulasi jaringan yang telah dirancang dalam penelitian ini. Hasil pengujian tersebut dianalisis untuk memberikan gambaran mengenai kinerja sistem jaringan yang diteliti berdasarkan rencana yang telah dibuat.

BAB VI KESIMPULAN DAN SARAN

Bab ini memuat kesimpulan dan saran dari hasil pengujian simulasi jaringan. Kesimpulannya menjawab masalah penelitian yang telah dirumuskan, sedangkan saran ditujukan untuk pengembangan simulasi selanjutnya.

BAB II

TINJAUAN PUSTAKA

2.1 Pengertian Implementasi

Implementasi adalah suatu tindakan atau pelaksanaan dari sebuah rencana yang disusun secara matang dan terperinci. Dengan melakukan implementasi setelah perencanaan dianggap baik (Kriswantoro & Ayatullah, 2023). Dalam kamus besar bahasa indonesia, implementasi biasanya berarti penerapan atau implementasi. Istilah “implementasi” umumnya dikaitkan dengan tindakan yang diambil untuk mencapai suatu tujuan tertentu. (Carlos et al., 2024).

Implementasi merupakan kelanjutan dari kegiatan perancangan. Tahap ini merupakan tahapapan supaya siap untuk di operasikan dan dapat dipandang sebagai usaha untuk mewujudkan rancangan yang telah di rancang. Langkah-langkah dalam tahap implementasi ini adalah urutan kegiatan awal sampai akhir yang harus dilakukan dalam mewujudkan rancangan yang telah di rancang. Setelah perancangan selesai, maka menampilkan hasil dari rancangan yang telah dirancang berikut akan dibahas tentang implementasi uji coba rancangan yang dibangun (Khair et al., 2021).

Berdasarkan pendapat tersebut, dapat disimpulkan bahwa implementasi merupakan proses penerapan dari rencana yang telah disusun secara matang untuk mencapai tujuan tertentu. Dalam penelitian ini, implementasi dilakukan pada kondisi jaringan di SMK Negeri 3 Prabumulih, di mana jaringan internet masih terpusat pada ISP utama yang hanya tersedia di ruang kantor. Melalui proses implementasi dalam bentuk simulasi, rancangan pengembangan jaringan dirancang agar dapat diperluas ke ruang praktik sehingga akses internet di sekolah menjadi lebih merata dan terkelola.

2.2 Pengertian User Manager

User Manager merupakan sebuah sistem atau alat yang digunakan dalam mengelola akun pengguna, termasuk otentikasi, otorasi, dan pelacakan penggunaan. Dalam konteks mikrotik, *user manager* adalah fitur dari *RouterOS* yang memungkinkan administrator untuk dapat mengelola akses pengguna ke jaringan

dan sumber daya yang tersedia (Aditama Purba & Nurhayati, 2024). *User manager* akan lebih mempermudah seseorang didalam pembuatan suatu layanan internet secara luas, seperti layanan *hotspot-hotspot* di dunia pendidikan misalnya di lingkungan sekolah, kampus, *cafe*, *mall* dan sebagainya (Fauzan Fitriani & Sujadi, 2023).

Berdasarkan dua peneliti tersebut, dapat disimpulkan bahwa *User manager* merupakan sistem yang berfungsi mengelola autentikasi, otorisasi, dan penggunaan jaringan secara terpusat sehingga memudahkan administrator dalam mengatur akses dan memantau aktivitas pengguna. *User manager* fitur *server* yang dimiliki oleh mikrotik digunakan untuk melakukan autentifikasi *user* yang *login* ke dalam sebuah jaringan, memberikan kebijakan terhadap *user* tersebut (Ningsy Guncya, 2024).

2.3 Pengertian Keamanan Jaringan

Keamanan jaringan merupakan praktik yang dilakukan untuk melindungi sistem komputer, perangkat, dan data dari ancaman baik yang berasal dari dalam maupun luar jaringan (Ananda Khairunnisa et al., 2024). Keamanan jaringan adalah serangkaian tindakan dan praktik yang dirancang untuk melindungi sistem komputer dan data dari serangan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan mereka (Wijoyo et al., 2023).

Keamanan jaringan merupakan serangkaian kebijakan dan praktik yang diterapkan untuk mencegah dan memantau akses tidak sah, modifikasi, atau penolakan jaringan komputer dan sumber daya yang dapat diakses oleh jaringan. Keamanan jaringan merupakan berkaitan tentang mengaktifkan akses ke data di jaringan, yang dikendalikan oleh administrator jaringan. Pengguna memilih atau diberikan nama pengguna dan kata sandi atau informasi otentifikasi lainnya yang memungkinkan (Asrin et al., 2024).

Berdasarkan kedua definisi tersebut, dapat disimpulkan bahwa keamanan jaringan merupakan suatu upaya terstruktur yang bertujuan untuk menjaga sistem komputer, perangkat, dan data agar tetap terlindungi dari berbagai ancaman, baik dari dalam maupun luar jaringan. Dalam penelitian ini, keamanan jaringan yang ditambah meliputi pemblokiran situs yang dianggap tidak pantas untuk diakses di

lingkungan sekolah guna menjaga keamanan dan kenyamanan penggunaan internet, serta pembatasan akses ke *router* sehingga hanya admin yang dapat melakukan pengaturan (Arbi Murad et al., 2025).

2.4 Pengertian Mikrotik

Mikrotik merupakan perangkat keras dan sistem operasi yang berfungsi untuk meningkatkan keandalan jaringan komputer. Mikrotik dilengkapi dengan fitur-fitur khusus untuk jaringan IP dan jaringan *wireless*, sehingga sangat ideal untuk digunakan dalam jaringan *wi-fi* (Sianhar & Marhalim, 2025). Mikrotik adalah perusahaan perangkat keras dan perangkat lunak yang berbasis di Latvia, yang didirikan pada tahun 1996 oleh John Trully dan Arnis Riekstins. Mikrotik awalnya berfokus pada pengembangan sistem operasi untuk *router* berbasis Linux yang kemudian dikenal sebagai Mikrotik *RouterOS* (Martani et al., 2024).

MikroTik menawarkan berbagai fitur *routing* dan *switching* yang canggih dan populer di kalangan pengguna jaringan yang membutuhkan solusi yang andal dan terjangkau. Produk mikrotik banyak digunakan di berbagai ukuran jaringan, mulai dari rumah tinggal hingga perusahaan besar (Cahya et al., 2023).

Berdasarkan pendapat para ahli tersebut, Mikrotik merupakan perangkat keras dan sistem operasi yang dirancang untuk meningkatkan keandalan jaringan komputer melalui berbagai fitur pendukung jaringan IP dan *wireless*, sehingga sangat sesuai digunakan dalam jaringan *wi-fi*. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun (Novi Syahputri et al., 2023).

2.5 Pengertian Access point

Access point adalah perangkat keras jaringan komputer yang menghubungkan piranti nirkabel dengan jaringan lokal menggunakan teknologi, seperti *wi-fi*, *bluetooth*, *wireless*, dan lain sebagainya (Safila Dewi & Syaripudin, 2024). Pada *wireless* LAN, terdapat alat untuk mentransmisikan data disebut dengan *Access point* (AP) dan terhubung dengan jaringan LAN melalui kabel (Ningsih et al., 2025).

AP adalah perangkat yang menghubungkan perangkat nirkabel ke jaringan kabel, seperti LAN atau internet. AP berfungsi sebagai penghubung antara perangkat pengguna dan jaringan. Contohnya *router wi-fi* di rumah atau kantor (Hasibuan, 2025).

Berdasarkan pendapat para ahli tersebut, *access point* dapat dipahami sebagai perangkat keras jaringan yang berfungsi untuk menghubungkan perangkat nirkabel dengan jaringan lokal menggunakan teknologi seperti *Wi-Fi*, *bluetooth*, dan koneksi *wireless* lainnya. Dalam penelitian ini, *access point* digunakan untuk menyebarkan jaringan internet yang sebelumnya hanya tersedia di ruang kantor agar dapat menjangkau ruang praktik TSM dan TKR, sehingga akses internet dapat digunakan secara lebih merata di ruang praktik tersebut.

2.6 Pengertian Manajemen *Bandwidth*

Maksud dari manajemen *bandwidth* ini adalah bagaimana kita menerapkan pengalokasian atau pengaturan *bandwidth* dengan menggunakan sebuah PC *router* Mikrotik. Manajemen *bandwidth* memberikan kemampuan untuk mengatur *bandwidth* jaringan dan memberikan level layanan sesuai dengan kebutuhan dan prioritas sesuai dengan permintaan *user/client* (Al Khoiri & Kuswandi, 2024). Manajemen *bandwidth* adalah suatu mekanisme untuk dapat mengatur rate dan prioritas *traffic data* yang dikirimkan melalui suatu *Network Interfaces* ke jaringan (Ichsansyah et al., 2024).

Manajemen adalah proses perencanaan, pengorganisasian, pengarahan, dan pengendalian sumber daya yang ada untuk mencapai tujuan tertentu secara efektif dan efisien. Dalam konteks jaringan komputer, manajemen melibatkan pengelolaan sumber daya jaringan seperti perangkat keras, perangkat lunak, dan *bandwidth* untuk memastikan ketersediaan layanan yang optimal bagi seluruh pengguna (Frederic P. Sitanggang et al., 2025).

Dari ketiga pendapat tersebut, dapat disimpulkan bahwa manajemen *bandwidth* merupakan proses pengaturan dan pembagian kapasitas jaringan agar setiap pengguna memperoleh layanan sesuai kebutuhan dan prioritasnya. Dalam penelitian ini, manajemen *bandwidth* diterapkan untuk mengatur pembagian akses

jaringan antara guru di ruang kantor serta siswa di ruang praktik TSM dan TKR agar penggunaan jaringan lebih stabil dan terkontrol.

2.7 Pengertian Internet

Internet singkatan dari *Interconnected Network* adalah infrastuktur global yang luar biasa kompleks yang menghubungkan miliaran perangkat komputer di seluruh dunia. Ini adalah jaringan global yang memfasilitasi pertukaran informasi, komunikasi, dan kolaborasi di tingkat global (Rizky et al., 2024). Internet secara sederhana adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia (Fitrian & Sujadi, 2023).

Melalui internet, pengguna dapat mengakses berbagai jenis informasi dalam berbagai format seperti teks, gambar, audio, *video*, dan lainnya melalui jaringan *World Wide Web*. Internet juga memberikan fleksibilitas kepada individu atau kelompok untuk bekerja tanpa terikat oleh batasan lokasi dan waktu, sehingga mereka dapat menjalankan tugas dengan komputer dan internet kapan saja dan di mana saja sesuai kebutuhan (Rahmayanty et al., 2023).

Berdasarkan pendapat para ahli tersebut, dapat disimpulkan bahwa internet merupakan jaringan global yang menghubungkan berbagai perangkat dan jaringan komputer di seluruh dunia untuk mendukung pertukaran informasi, komunikasi, dan kolaborasi. Internet menjadi sumber utama konektivitas yang kemudian dikembangkan dari ruang kantor ke ruang praktik TSM dan TKR agar akses jaringan dapat dimanfaatkan secara lebih merata di ruang praktik tersebut.

2.8 Pengertian Figma

Figma adalah alat membuat *prototyping* atau alat desain antarmuka pengguna dan kolaborasi waktu nyata (*real-time*), *Figma* memungkinkan penggunanya bekerja sama dalam proyek dan tim. *Figma* juga memudahkan penggunanya dalam membuat *desain* antarmuka pengguna dan *prototipe*, sehingga memfasilitasi proses *desain* secara lebih efisien (Ramadhani & Hidayati, 2025). *Figma* adalah sebuah perangkat lunak desain yang digunakan untuk membuat tampilan dan pengalaman

antarmuka pengguna untuk perangkat *desktop*, seluler, dan aplikasi lainnya (Wisnu Prio Pamungkas et al., 2024).

Figma adalah alat desain berbasis *cloud* yang telah merevolusi cara perancang bekerja dan berkolaborasi. Dirilis pertama kali pada tahun 2016, *Figma* dengan cepat menjadi favorit di kalangan perancang UI/UX dan pengembang produk karena kemampuannya yang kuat dan fleksibilitasnya yang tinggi. Alat ini memungkinkan perancang untuk membuat *prototype*, mendesain antarmuka, dan berkolaborasi secara *real-time* dengan tim (Kurniasari et al., 2025).

Berdasarkan pendapat para ahli tersebut, dapat disimpulkan bahwa *Figma* merupakan perangkat lunak desain antarmuka pengguna (UI) dan pembuatan *prototype* berbasis *cloud* yang mendukung kolaborasi secara *real-time*. *Figma* memudahkan perancang dan pengembang dalam membuat, mengelola, serta mengembangkan *desain* untuk berbagai platform, seperti *desktop* dan perangkat seluler, dengan lebih efisien. Kemampuan kolaboratif yang dimiliki *Figma* memungkinkan anggota tim bekerja secara bersamaan dalam satu proyek sehingga proses perancangan, evaluasi, dan pengembangan produk digital dapat dilakukan dengan lebih efektif dan terstruktur.

2.9 Penelitian Terdahulu

Penelitian terdahulu merupakan kajian terhadap hasil penelitian sebelumnya yang memiliki keterkaitan dengan topik yang sedang dibahas. Kajian ini bertujuan untuk mengetahui sejauh mana penelitian serupa telah dilakukan, metode yang digunakan, serta hasil yang telah dicapai oleh peneliti lain sebagai bahan perbandingan dan pengembangan dalam penelitian ini. Beberapa penelitian yang relevan dapat dilihat pada Tabel 2.1 di bawah ini.

Tabel 2.1 Penelitian Terdahulu

NO	Judul	Penulis (Tahun)	Hasil
1	Analisis Kinerja Internet	(Mafakhiri, 2021)	Manajemen <i>bandwidth</i>
	<i>Hotspot</i> dengan Menerapkan		menggunakan <i>user manager</i>
	<i>Bandwidth Management</i>		meningkatkan kestabilan

	Menggunakan Mikrotik <i>User manager</i>		jaringan <i>hotspot</i> dan mengurangi beban trafik pada jam sibuk.
2	Jaringan Komputer Berbasis <i>Radius Server</i> untuk Meningkatkan Pemanfaatan Internet di Madrasah Aliyah Al-Azhaar Ummu Suwanah	(Abdillah Hasibuan & Subhiyanto, 2021)	Mengimplementasikan <i>hotspot</i> dengan <i>login</i> pengguna + manajemen <i>user</i> + pembatasan <i>bandwidth</i> .
3	<i>Captive Portal</i> Dan Implementasi <i>Bandwidth Management</i> di Stikes St. Elisabeth Semarang	(Siswanto et al., 2021)	Pembatasan <i>bandwidth</i> tiap user melalui <i>queue</i> sederhana di Mikrotik, membantu mengelola kuota <i>hotspot</i> di institusi.
4	Desain dan Implementasi <i>Management Bandwidth</i> Pada <i>Hotspot</i> Mikrotik Di Smk Mutiara 17 Agustus Bekasi	(Fauzi et al., 2022)	Sistem manajemen <i>bandwidth</i> menggunakan <i>simple queue</i> dapat bekerja dengan baik dan di implementasikan di sekolah.
5	Implementasi <i>User manager</i> Mikrotik Dalam <i>Authentication Login</i> Pada <i>Hotspot</i>	(Ngatono et al., 2024)	Sistem autentikasi <i>User manager</i> mempermudah validasi pengguna dan pengelolaan <i>login</i> .
6	Implementasi Sistem <i>Hotspot</i> Mikrotik Sebagai Upaya Pemerataan Jaringan Internet Di Pedesaan	(Dian Candra Wirlaksana et al., 2024)	Penelitian ini menunjukkan bahwa <i>hotspot</i> mikrotik dapat memperluas jangkauan internet dan meningkatkan kestabilan akses di wilayah pedesaan melalui konfigurasi dasar dan pengaturan <i>hotspot</i> sederhana.
7	Manajemen <i>Bandwidth</i> Dan Kontrol Akses Jaringan Menggunakan Mikrotik Pada Lembaga Paud	(Hasanah et al., 2025)	Manajemen <i>bandwidth</i> dan <i>voucher hotspot</i> meningkatkan reliabilitas internet di PAUD dan pengelolaan akses pengguna.
8	Optimasi Infrastruktur Wi-Fi dan Manajemen <i>Bandwidth</i> di Sekolah Menengah Menggunakan Teknologi Mikrotik	(Ramayanti & Saputra, 2025)	Optimasi AP + alokasi <i>bandwidth</i> melalui <i>Queue Tree</i> membuat kualitas sinyal dan kecepatan lebih baik di sekolah.

Sumber : data diolah oleh penulis (2026)

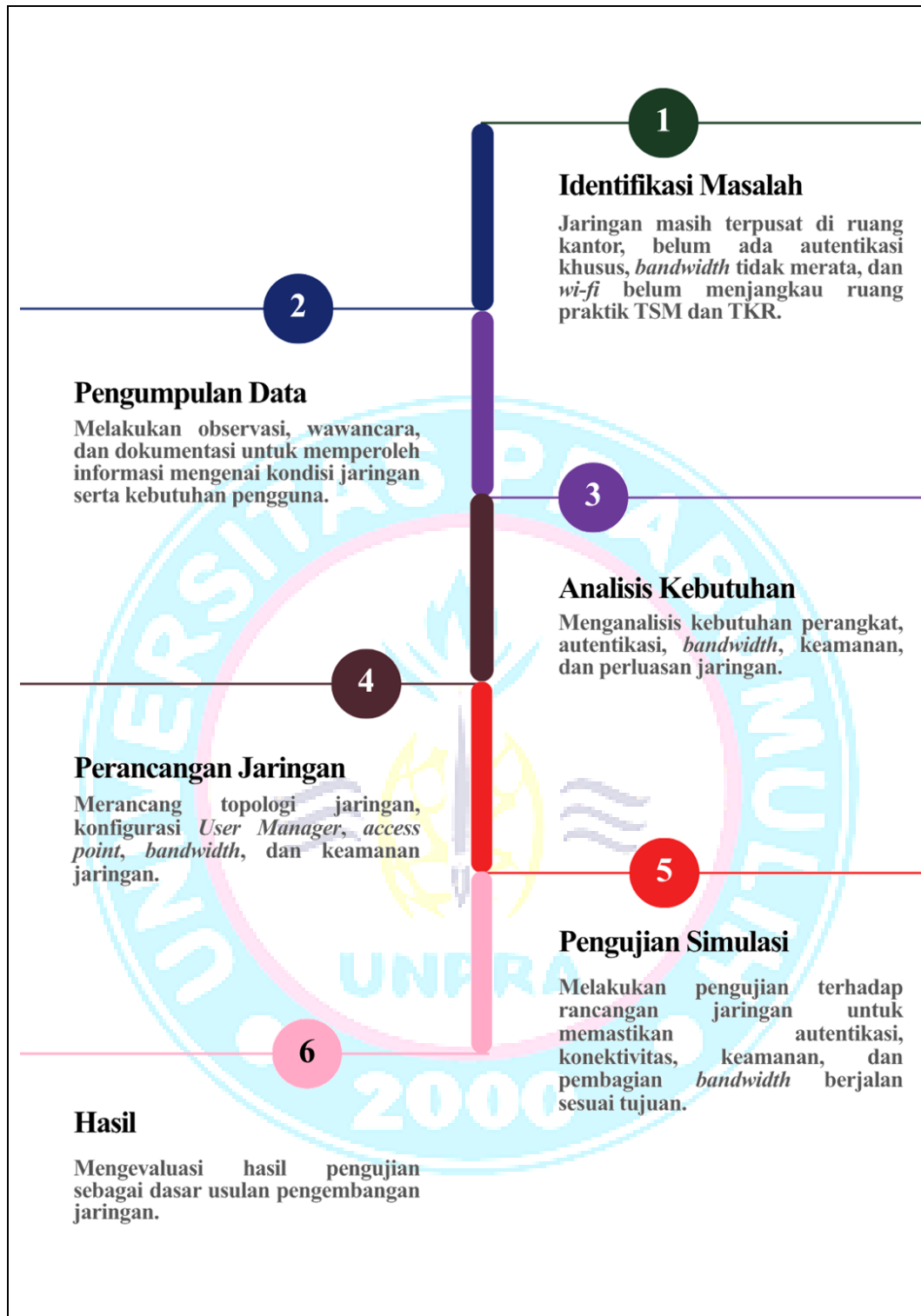
Berdasarkan Tabel 2.1, penelitian terdahulu menunjukkan bahwa penerapan manajemen *bandwidth* dan sistem autentikasi berbasis mikrotik, seperti *user*

manager, manajemen *bandwidth*, *captive portal*, mampu meningkatkan kestabilan jaringan serta mengoptimalkan penggunaan *bandwidth* di berbagai institusi pendidikan. Hasil penelitian tersebut menyatakan bahwa pembatasan *bandwidth* per pengguna, pengelolaan *login* pengguna, serta kontrol akses jaringan dapat mengurangi beban trafik pada jam sibuk, meningkatkan reliabilitas internet, serta memperbaiki kualitas sinyal dan kecepatan akses.

Perbedaan karakteristik dan kebutuhan pada setiap institusi menyebabkan penerapan sistem jaringan tidak dapat disamakan antara satu tempat dengan tempat lainnya. Oleh karena itu, penelitian ini difokuskan pada penerapan autentikasi *user manager*, manajemen *bandwidth*, serta penguatan keamanan jaringan untuk mendukung pemerataan akses internet di SMK Negeri 3 Prabumulih, khususnya pada ruang praktik TSM dan TKR, sehingga dapat menunjang kegiatan pembelajaran berbasis digital secara lebih optimal, aman, dan terkontrol.

2.10 Kerangka Berpikir Penelitian

Untuk memberikan gambaran yang lebih jelas mengenai alur penelitian, diperlukan kerangka berpikir yang menggambarkan tahapan sistematis dalam penyusunan dan pelaksanaan penelitian ini. Kerangka berpikir berfungsi sebagai panduan untuk memahami keterkaitan antara tahapan yang dilakukan mulai dari identifikasi masalah hingga penarikan kesimpulan. Secara umum, kerangka berpikir penelitian ini dapat dilihat pada Gambar 2.1 berikut:



Sumber : data diolah oleh penulis (2026)

Gambar 2.1 Kerangka Berpikir Penelitian

Kerangka berpikir penelitian ini menjelaskan tahapan yang dilakukan dalam menyelesaikan permasalahan jaringan internet di SMK Negeri 3 Prabumulih. Setiap tahapan disusun secara sistematis mulai dari identifikasi masalah hingga diperoleh hasil penelitian, sehingga proses penelitian dapat berjalan sesuai dengan tujuan yang telah ditetapkan.

Tahap pertama adalah identifikasi masalah, yaitu mengamati kondisi jaringan internet yang ada di SMK Negeri 3 Prabumulih. Berdasarkan hasil observasi, jaringan internet masih terpusat di ruang kantor, sedangkan ruang praktik TSM dan TKR belum memiliki akses internet. Selain itu, jaringan masih menggunakan keamanan WPA2 dengan satu kata sandi yang digunakan bersama sehingga belum memiliki mekanisme autentikasi pengguna. Kondisi tersebut menyebabkan pembagian *bandwidth* belum terkelola dengan baik dan keamanan jaringan masih perlu ditingkatkan (Ramadanti et al., 2025).

Tahap kedua adalah pengumpulan data, yang dilakukan melalui observasi, wawancara, dan dokumentasi. Observasi dilakukan untuk mengetahui kondisi jaringan yang sedang berjalan, wawancara dilakukan dengan pihak sekolah untuk memperoleh informasi mengenai kendala dan kebutuhan jaringan, sedangkan dokumentasi digunakan untuk mengumpulkan data pendukung, seperti perangkat jaringan, denah ruangan, dan kondisi lokasi penelitian. Data yang diperoleh menjadi dasar dalam penyusunan rancangan jaringan.

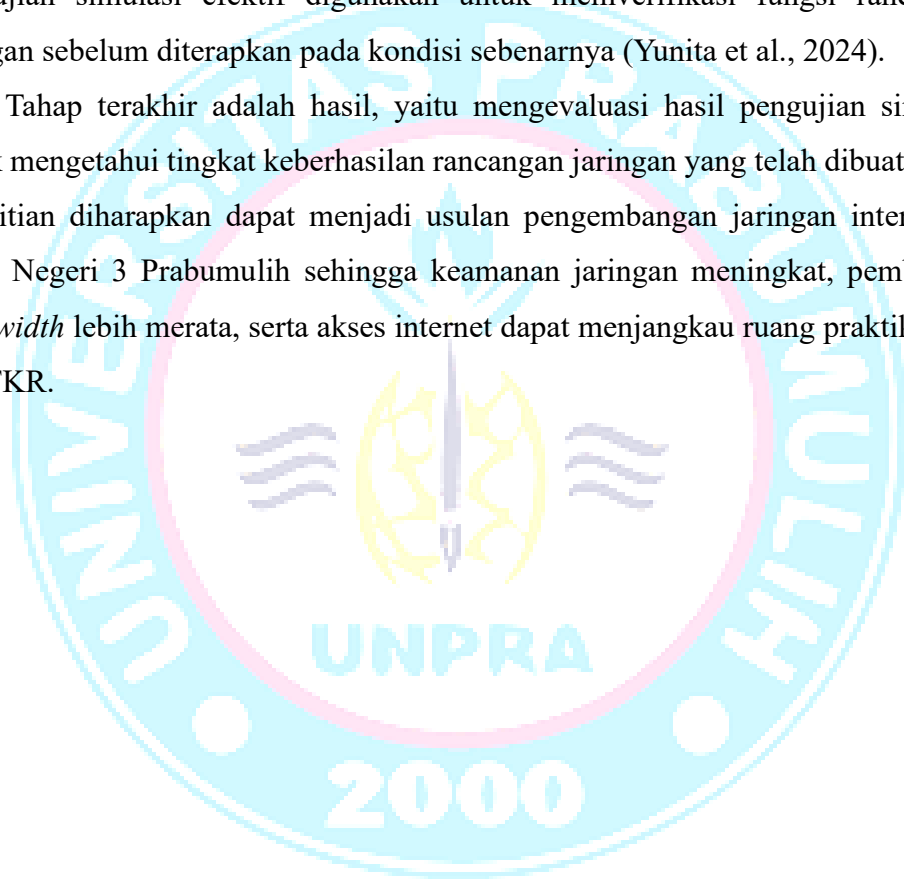
Tahap ketiga adalah analisis kebutuhan, yaitu menganalisis hasil pengumpulan data untuk menentukan kebutuhan jaringan yang akan dikembangkan. Analisis meliputi kebutuhan perangkat jaringan, mekanisme autentikasi menggunakan *user manager*, pembagian *bandwidth*, peningkatan keamanan jaringan, serta perluasan jangkauan jaringan menuju ruang praktik TSM dan TKR.

Tahap keempat adalah perancangan jaringan, yaitu menyusun rancangan topologi jaringan beserta konfigurasi yang diperlukan berdasarkan hasil analisis kebutuhan. Perancangan meliputi penambahan *access point* pada ruang praktik, konfigurasi *user manager* sebagai autentikasi pengguna, pengaturan *bandwidth*, serta penerapan konfigurasi keamanan pada *router*, seperti pembatasan akses

administrator dan pemblokiran akses menuju situs yang tidak sesuai dengan lingkungan pendidikan (Zulkarnaen, 2021).

Tahap kelima adalah pengujian simulasi, yaitu melakukan pengujian terhadap rancangan jaringan untuk memastikan seluruh konfigurasi berjalan sesuai dengan tujuan penelitian. Pengujian dilakukan terhadap autentikasi *user manager*, konektivitas jaringan, pembagian *bandwidth*, serta mekanisme keamanan yang telah diterapkan, sehingga dapat diketahui bahwa rancangan jaringan telah berfungsi sesuai dengan kebutuhan. Salah satu penelitian menyatakan bahwa pengujian simulasi efektif digunakan untuk memverifikasi fungsi rancangan jaringan sebelum diterapkan pada kondisi sebenarnya (Yunita et al., 2024).

Tahap terakhir adalah hasil, yaitu mengevaluasi hasil pengujian simulasi untuk mengetahui tingkat keberhasilan rancangan jaringan yang telah dibuat. Hasil penelitian diharapkan dapat menjadi usulan pengembangan jaringan internet di SMK Negeri 3 Prabumulih sehingga keamanan jaringan meningkat, pembagian *bandwidth* lebih merata, serta akses internet dapat menjangkau ruang praktik TSM dan TKR.



BAB III

METODE PENELITIAN

3.1 Objek dan Subjek Penelitian

3.1.1 Subjek Penelitian

Subjek dalam penelitian ini adalah pihak yang terlibat dalam penggunaan dan pengelolaan jaringan internet di SMK Negeri 3 Prabumulih, yaitu administrator jaringan sekolah, guru, serta siswa khususnya pada ruang praktik TSM dan TKR. Subjek penelitian ini dipilih karena mereka merupakan pengguna langsung sekaligus pengelola sistem jaringan yang akan menerapkan autentikasi *user manager*, manajemen *bandwidth*, serta penguatan keamanan jaringan. Administrator berperan dalam proses konfigurasi dan pengelolaan jaringan, sedangkan guru dan siswa menjadi pengguna utama layanan internet dalam kegiatan pembelajaran berbasis digital.

3.1.2 Objek Penelitian

Objek penelitian ini adalah SMK Negeri 3 Prabumulih yang berlokasi di Jl. Raya Sungai Medang Nigata, Sungai Medang, Kecamatan Cambai, Kota Prabumulih, Provinsi Sumatera Selatan 31146. Penelitian berfokus pada sistem jaringan internet sekolah melalui penerapan autentikasi *user manager*, manajemen *bandwidth*, serta perluasan jangkauan jaringan ke ruang praktik TSM dan TKR menggunakan rancangan simulasi mikrotik. Pemilihan objek ini didasarkan pada kondisi jaringan yang masih terpusat di ruang kantor, belum menjangkau ruang praktik secara optimal, dan seluruh perangkat masih menggunakan satu kata sandi *wi-fi* tanpa autentikasi khusus.

Kondisi ini juga menimbulkan kerentanan keamanan karena belum adanya pembatasan akses *router* dan pemblokiran IP yang tidak sesuai untuk lingkungan pendidikan. Melalui perancangan autentikasi pengguna, pembagian *bandwidth*, dan penambahan *access point*, penelitian ini diharapkan menjadi masukan bagi pihak sekolah untuk penerapan lebih lanjut dalam pengembangan jaringan di SMK Negeri 3 Prabumulih.

3.1.3 Sejarah

SMK Negeri 3 Prabumulih merupakan salah satu lembaga pendidikan kejuruan negeri yang berdiri sebagai upaya pemerintah dalam memperluas akses pendidikan vokasi di Kota Prabumulih, khususnya di wilayah Kecamatan Cambai. Sekolah ini resmi didirikan berdasarkan SK Pendirian Nomor 10295/SK.SMK.3/Disdik.SS/2020 pada tanggal 2 Juni 2020, dan memperoleh Izin Operasional melalui SK Nomor 067/3083/SK.SMK.3/Disdik.SS/2021 pada tanggal 1 Maret 2021. Berlokasi di Jl. Raya Sungai Medang Nigata, Sungai Medang, Kecamatan Cambai, Kota Prabumulih.

SMK Negeri 3 Prabumulih dibangun di atas lahan seluas kurang lebih 7.800 m² yang kemudian dikembangkan menjadi sarana pendidikan kejuruan dengan ruang kelas, laboratorium, serta fasilitas penunjang lainnya. Dalam tahap awal operasional, sekolah ini dipimpin oleh kepala sekolah Achmad Sukri yang bertanggung jawab membangun struktur organisasi dan sistem pembelajaran sesuai standar pendidikan kejuruan.

Seiring berjalannya waktu, SMK Negeri 3 Prabumulih mulai membuka beberapa kompetensi keahlian yang relevan dengan kebutuhan industri lokal, seperti Teknik Kendaraan Ringan, Teknik dan Bisnis Sepeda Motor, serta kompetensi yang terkait dengan sektor migas. Kehadiran sekolah ini menjadi bagian penting dari pengembangan sumber daya manusia di Kota Prabumulih, mengingat daerah ini memiliki potensi industri yang menuntut tenaga kerja terampil khususnya di bidang teknik.

Dengan akreditasi kategori A serta fasilitas praktik yang terus ditingkatkan, SMK Negeri 3 Prabumulih berkomitmen menjadi pusat pendidikan vokasi yang mampu menghasilkan lulusan terampil, berdaya saing, dan siap masuk ke dunia kerja maupun melanjutkan pendidikan ke jenjang yang lebih tinggi.

3.1.4 Visi Misi SMK Negeri 3 Prabumulih

Visi, misi, dan tujuan SMK Negeri 3 Prabumulih menjadi landasan utama penyelenggaraan pendidikan kejuruan yang berkualitas. Ketiganya berfungsi sebagai arah dan pedoman bagi seluruh warga sekolah dalam mengembangkan kompetensi, karakter, dan mutu layanan pendidikan secara berkelanjutan. Dengan

memahami visi, misi, dan tujuan tersebut, kegiatan pembelajaran dan penelitian dapat berjalan lebih terarah serta selaras dengan upaya sekolah dalam membentuk lulusan yang bertaqwa, mandiri, kreatif, dan mampu berkolaborasi di berbagai lingkungan kerja maupun sosial.

a. Visi

Terbentuknya peserta didik yang bertaqwa, mandiri, kreatif dan mampu berkolaborasi.

b. Misi

1. Membentuk peserta didik yang beriman dan menjalankan nilai-nilai agama dalam kehidupan sehari-hari.
2. Membentuk peserta didik yang mampu berwirausaha.
3. Mampu berpikir kreatif dan inovatif.
4. Mampu untuk membangun keterampilan sosial dan kerja tim.

c. Tujuan

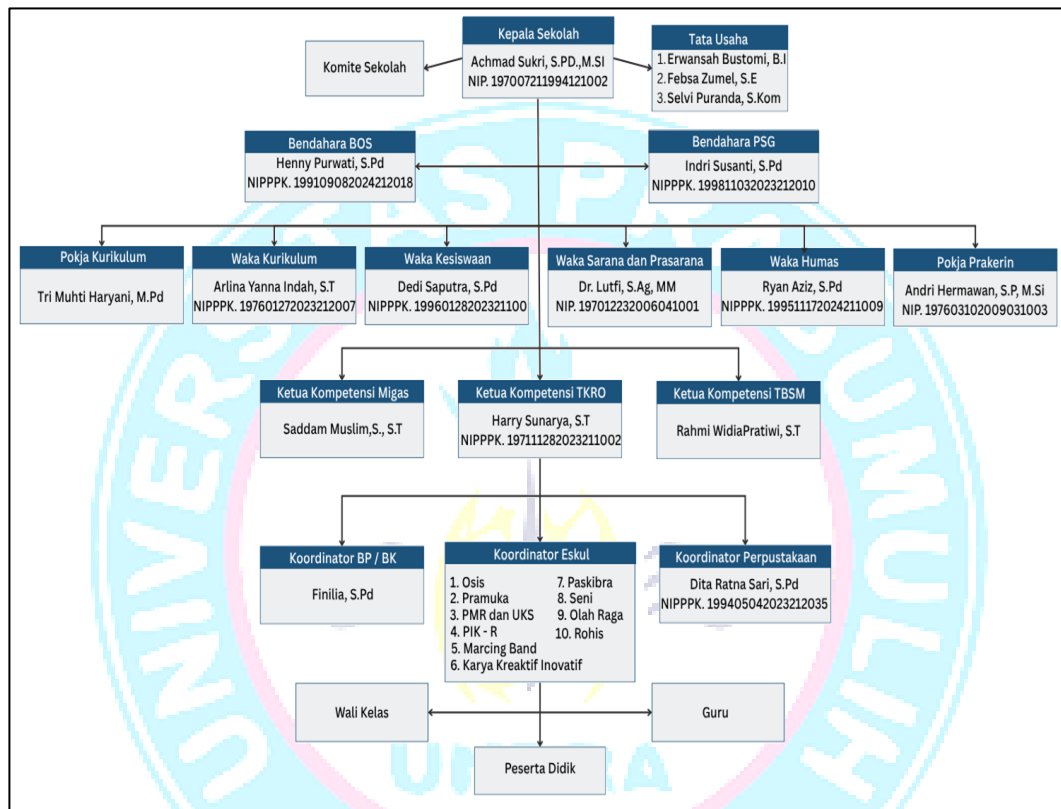
1. Tujuan Terkait Misi 1: Peserta Didik yang Beriman dan Bertaqwa
 - a. Meningkatkan Kualitas Sikap Spiritual: Terwujudnya peningkatan rerata skor penilaian sikap spiritual peserta didik minimal sebesar 5% setiap tahun ajaran (diukur melalui penilaian P5 dan laporan guru agama).
 - b. Pembiasaan Ibadah: Tercapainya tingkat partisipasi peserta didik dalam kegiatan ibadah rutin sekolah (Shalat Dhuha/Jumat/Keagamaan lainnya) minimal 90%.
 - c. Karakter Mulia: Seluruh peserta didik menunjukkan peningkatan disiplin, kejujuran, dan tanggung jawab yang tercermin dari penurunan pelanggaran tata tertib dan peningkatan apresiasi perilaku baik.
2. Tujuan Terkait Misi 2: Peserta Didik yang Mampu Berwirausaha (Mandiri)

- a. Keterampilan Berwirausaha: Minimal 80% peserta didik mampu menyelesaikan tugas proyek/mandiri.
 - b. Peningkatan Kemandirian: Terlaksananya program inkubasi bisnis/Unit Produksi Sekolah secara berkelanjutan yang melibatkan minimal 20% peserta didik di jurusan terkait.
 - c. Keterserapan DUDI/Wirausaha: Mencapai angka 10% lulusan yang memilih jalur berwirausaha mandiri dalam satu tahun setelah kelulusan, selain keterserapan ke Dunia Kerja/Studi Lanjut.
3. Tujuan Terkait Misi 3: Mampu Berpikir Kreatif dan Inovatif (Kreatif)
- a. Inovasi Pembelajaran: Minimal 80% guru menerapkan model pembelajaran berbasis proyek (*Project-Based Learning*) yang mendorong siswa menghasilkan karya atau solusi inovatif di bidang kejuruan mereka.
 - b. Hasil Karya: Setiap jurusan menghasilkan minimal 3 karya inovatif atau produk teknologi terapan yang dipublikasikan atau diikutsertakan dalam kompetisi di tingkat regional/nasional setiap tahunnya.
 - c. Literasi Teknologi: Meningkatnya kemampuan peserta didik dalam menguasai teknologi terkini yang relevan dengan jurusan, diukur melalui sertifikasi atau hasil uji kompetensi.
4. Tujuan Terkait Misi 4: Membangun Keterampilan Sosial dan Kerja Tim (Kolaborasi)
- a. Penguatan Kerja Tim: Seluruh kegiatan praktik dan pembelajaran produktif dilaksanakan dengan sistem kerja tim (kolaborasi) yang terstruktur, menghasilkan peningkatan nilai keterampilan sosial pada rapor peserta didik.
 - b. Hubungan Industri: Tercapainya kemitraan dengan Dunia Usaha/Dunia Industri (DUDI) yang berkualitas, ditandai dengan minimal 10 DUDI yang aktif terlibat dalam penyesuaian kurikulum, pengajaran (Guru Tamu), dan pelaksanaan Praktik Kerja Lapangan (PKL) setiap tahun.
 - c. Kepemimpinan Sosial: Minimal 15% peserta didik aktif terlibat dalam organisasi sekolah (OSIS, Rohis, UKS, Ekskul).

3.1.5 Struktur Organisasi

Struktur organisasi di SMK Negeri 3 Prabumulih disusun untuk mendukung pelaksanaan kegiatan belajar mengajar dan administrasi sekolah secara efektif. Struktur ini menunjukkan pembagian tanggung jawab antara kepala sekolah, wakil kepala sekolah, ketua kompetensi keahlian, serta unit kerja pendukung lainnya.

Gambaran struktur organisasi dapat dilihat pada Gambar 3.1 berikut:



Sumber : SMK Negeri 3 Prabumulih, 2025

Gambar 3.1 Struktur Organisasi SMK Negeri 3 Prabumulih

Berdasarkan gambar 3.1 struktur organisasi SMK Negeri 3 Prabumulih, dapat dijelaskan bahwa struktur ini menggambarkan susunan dan hubungan antar unsur yang berperan dalam penyelenggaraan kegiatan pendidikan di SMK Negeri 3 Prabumulih.

1. Kepala Sekolah

Kepala sekolah memegang tanggung jawab penuh atas seluruh kegiatan penyelenggaraan pendidikan di SMK Negeri 3 Prabumulih. Kepala sekolah mengoordinasikan seluruh wakil bidang, ketua kompetensi

keahlian, staf tata usaha, serta komite sekolah untuk memastikan kegiatan pembelajaran, administrasi, dan manajemen sekolah berjalan sesuai standar dan kebijakan dinas pendidikan.

2. Komite Sekolah

Komite sekolah berperan sebagai mitra kepala sekolah dalam memberikan pertimbangan, dukungan moral, finansial, serta pengawasan demi peningkatan mutu pendidikan. Komite juga membantu menjembatani kepentingan masyarakat dan satuan pendidikan.

3. Tata Usaha (TU)

Bagian Tata Usaha bertanggung jawab pada administrasi sekolah, seperti pengelolaan data lembaga, pengarsipan, layanan administrasi siswa dan guru, serta kelancaran operasional harian sekolah. Anggotanya terdiri dari:

- a. Erwansah Bustomi, B.I
- b. Febsa Zumel, S.E
- c. Selvi Puranda, S.Kom

4. Bendahara BOS

Bendahara BOS mengelola dana Bantuan Operasional Sekolah, mulai dari perencanaan, penyaluran, realisasi, hingga pelaporan sesuai juknis. Tugas ini memastikan seluruh kegiatan sekolah yang didanai BOS berjalan transparan dan akuntabel.

5. Bendahara PSG (Praktik Sistem Ganda)

Bertanggung jawab dalam pengelolaan administrasi dan pendanaan kegiatan PSG/prakerin siswa, termasuk kerja sama industri, pendataan siswa praktik, serta laporan kegiatan.

6. Waka Kurikulum

Wakil kepala sekolah bidang kurikulum mengatur seluruh kegiatan akademik, penyusunan jadwal pelajaran, distribusi tugas guru, supervisi pembelajaran, serta pelaksanaan evaluasi akademik. Dibantu oleh Pokja Kurikulum dalam penyusunan perangkat pembelajaran dan administrasi akademik.

7. Waka Kesiswaan
Mengelola seluruh kegiatan yang berkaitan dengan pembinaan siswa, kedisiplinan, organisasi siswa, layanan konseling, dan pengembangan karakter.
8. Waka Sarana dan Prasarana
Bertanggung jawab pada seluruh fasilitas sekolah, meliputi perawatan bangunan, ruang belajar, laboratorium, peralatan praktik, inventarisasi, dan pengadaan sarana pendukung pembelajaran.
9. Waka Humas
Mengelola hubungan eksternal sekolah seperti kerja sama dengan DUDI (Dunia Usaha dan Dunia Industri), komunikasi dengan orang tua, pemerintah, serta instansi eksternal lainnya. Humas juga mengelola informasi publik dan citra sekolah.
10. Pokja Prakerin
Mengatur pelaksanaan Praktek Kerja Industri (Prakerin/PKL), mulai dari penempatan siswa, penjadwalan, monitoring, hingga evaluasi hasil praktik. Pokja ini juga bekerja sama dengan Bendahara PSG dan Waka Humas.
11. Ketua Kompetensi Keahlian (Migas, TKRO, TBSM)
Setiap kompetensi keahlian memiliki ketua program yang bertanggung jawab terhadap kegiatan pembelajaran khusus jurusan, pengelolaan laboratorium, penyusunan kurikulum vokasi, serta menjalin kerja sama industri sesuai bidang keahlian masing-masing:
 - a. Kompetensi Migas
 - b. Teknik Kendaraan Ringan Otomotif (TKRO)
 - c. Teknik dan Bisnis Sepeda Motor (TBSM)
12. Koordinator BP/BK
Bertugas memberikan layanan bimbingan dan konseling, mulai dari pembinaan kedisiplinan, konsultasi pribadi dan akademik siswa, hingga penanganan masalah perilaku dan sosial.

13. Koordinator Ekstrakurikuler

Mengatur berbagai kegiatan ekstrakurikuler sekolah seperti OSIS, Pramuka, PMR, UKS, Paskibra, Seni, Olahraga, Rohis, dan Marching Band. Koordinator ini memastikan pengembangan minat dan bakat siswa berjalan terarah dan konsisten.

14. Koordinator Perpustakaan

Mengelola layanan perpustakaan, administrasi buku, peminjaman, pengembangan bahan ajar, serta penyediaan sumber belajar bagi siswa dan guru.

15. Guru dan Wali Kelas

Guru bertanggung jawab terhadap proses belajar mengajar, penyusunan perangkat pembelajaran, serta penilaian hasil belajar siswa. Wali kelas mengelola pembinaan siswa dalam satu kelas, administrasi kelas, absensi, dan komunikasi dengan orang tua.

16. Peserta Didik

Peserta didik menjadi pusat seluruh kegiatan sekolah. Seluruh struktur organisasi bekerja untuk mendukung proses pembelajaran, pembentukan karakter, serta pengembangan kompetensi siswa agar siap melanjutkan pendidikan atau bekerja di dunia industri.

3.1.6 Jadwal Penelitian

Penelitian ini direncanakan berlangsung selama 6 bulan dengan rincian kegiatan yang disusun secara bertahap dan sistematis. Perencanaan waktu penelitian dibuat agar setiap tahapan dapat terlaksana dengan baik, terarah, serta sesuai dengan target yang telah ditentukan. Pembagian waktu ini juga bertujuan untuk mengoptimalkan proses pengumpulan data, analisis kebutuhan sistem, perancangan jaringan, hingga tahap pengujian, yang rincian pelaksanaannya adalah sebagai berikut:

Tabel 3.1 Jadwal Penelitian

No	Kegiatan	Bulan Ke 1	Bulan Ke 2	Bulan Ke 3	Bulan Ke 4	Bulan Ke 5	Bulan Ke 6
1	Identifikasi masalah dan observasi awal	✓	✓				
2	Wawancara dan dokumentasi	✓	✓				
3	Analisis kebutuhan sistem jaringan		✓	✓			
4	Perancangan Topologi Jaringan			✓	✓		
5	Simulasi dan pengujian pada <i>Cisco Packet Tracer</i> (Simple PDU, konektivitas)			✓	✓		
6	Implementasi terbatas menggunakan alat peraga (MikroTik, <i>Access point</i> , Internet)				✓	✓	
7	Konfigurasi sistem (<i>User manager</i> , manajemen <i>bandwidth</i> , keamanan jaringan)				✓	✓	
8	Pengujian jaringan (<i>Web Browser</i> , CMD, CLI, <i>Speedtest</i> , Winbox, <i>Tools</i>)					✓	✓
9	Analisis hasil pengujian					✓	✓
10	Penyusunan laporan penelitian						✓

Sumber: Penulis, 2026

3.2 Metode Penelitian

Penelitian dalam kamus Webster mempunyai arti memeriksa atau mencari kembali. penelitian diartikan lebih luas sebagai suatu pemeriksaan atau pengujian yang teliti dan kritis dalam mencari fakta dan prinsip-prinsip penyelidikan guna

memastikan suatu hal. maka disimpulkan bahwa penelitian adalah kegiatan ilmiah dalam mencapai tujuan tertentu dengan metode yang logis. Dengan demikian penelitian memiliki 3 (tiga) unsur penting, yaitu sasaran, adanya usaha untuk mencapai sasaran dan metode ilmiah. Metode Penelitian merupakan cara ilmiah yang digunakan untuk mendapatkan data sebagai informasi pendukung penelitian dengan tujuan tertentu (Risa, 2021).

Sejalan dengan tujuan penelitian yang berfokus pada pengembangan akses internet ke ruang praktik, penelitian ini menggunakan pendekatan deskriptif kualitatif. Pendekatan ini dipilih untuk menggambarkan secara jelas proses perancangan topologi jaringan, integrasi autentikasi *user manager*, serta peningkatan keamanan dan perluasan jangkauan internet di SMK Negeri 3 Prabumulih. Penelitian kualitatif adalah penelitian yang digunakan untuk meneliti pada kondisi objek alamiah, dimana peneliti merupakan instrumen kunci (Fattah Nasution, 2023).

3.3 Sumber Data

Sumber data dalam penelitian adalah subjek tempat data diperoleh atau diambil. Apabila peneliti menggunakan kuesioner atau wawancara untuk mengumpulkan data, maka sumber data disebut responden, yaitu orang yang merespon atau menjawab pertanyaan-pertanyaan peneliti, baik pertanyaan lisan maupun tulisan dan apabila peneliti menggunakan teknik observasi, maka sumber datanya bisa berupa benda, gerak dan peristiwa (Ramadona Wijaya et al., 2025).

Sumber data dalam penelitian kualitatif dapat dikategorikan menjadi data primer dan sekunder. Data primer diperoleh langsung dari wawancara, observasi, atau interaksi langsung dengan subjek penelitian, sedangkan data sekunder berasal dari dokumen, buku, atau sumber tertulis lainnya (Mardatillah & Murhayati, 2025). Sumber data diperoleh dari dua jenis, yaitu data primer dan data sekunder, yang keduanya saling melengkapi dalam mendukung hasil penelitian.

3.3.1 Data Primer

Data primer adalah sumber informasi utama yang dikumpulkan secara langsung oleh peneliti dalam proses penelitian. Data ini diperoleh dari sumber asli,

yaitu responden atau informan yang terkait dengan variabel penelitian. Data primer dapat berupa hasil observasi, wawancara, atau pengumpulan data (Sulung & Muspawi, 2024). Dalam penelitian ini, data primer diperoleh melalui wawancara dan observasi langsung terhadap kondisi jaringan di SMK Negeri 3 Prabumulih.

Sumber data primer meliputi:

1. Harry Sunarya S.T sebagai Ketua Program Studi Teknik Kendaraan Ringan Otomotif (TKRO), Narasumber ini memberikan informasi mengenai permasalahan internet di ruang praktik TKR, seperti lemahnya sinyal, keterbatasan jangkauan, dan hambatan koneksi lainnya yang memengaruhi kegiatan pembelajaran berbasis digital.
2. Rahmi WidiaPratiwi S.T sebagai Ketua Kompetensi Teknik Bisnis Sepeda Motor (TBSM), Narasumber ini diwawancarai untuk mengetahui bagaimana kondisi akses internet di sekolah, khususnya di ruang praktik TSM. Pertanyaan dalam wawancara difokuskan pada kekuatan sinyal, jangkauan jaringan, dan kendala koneksi yang terjadi saat proses pembelajaran berlangsung.

Wawancara juga menanyakan lokasi akses internet utama sekolah serta bagaimana sistem keamanan jaringan yang digunakan, termasuk apakah sudah menerapkan autentikasi pengguna atau masih menggunakan satu *password wi-fi*. Pertanyaan lainnya menggali bagaimana dampak kondisi jaringan tersebut terhadap pembelajaran digital, serta harapan dan kebutuhan narasumber terkait penambahan *access point* dan peningkatan sistem jaringan agar kegiatan praktik TSM dapat berjalan lebih optimal.

Data primer tersebut digunakan untuk memahami kondisi nyata akses internet di lingkungan sekolah serta menggambarkan kebutuhan jaringan yang mendukung kelancaran proses pembelajaran.

3.3.2 Data Sekunder

Data sekunder adalah data yang sudah ada dan telah dikumpulkan oleh orang lain atau lembaga untuk tujuan lain (Sar'an et al., 2025). Dalam penelitian ini, sumber data sekunder meliputi:

1. Arsip dan dokumen internal sekolah

Arsip ini mencakup data absensi salah satu kelas TSM dan TKR yang menggunakan ruang praktik tersebut. Data tersebut digunakan untuk mengetahui berapa jumlah peserta didik yang memanfaatkan akses internet selama pembelajaran berlangsung, serta dokumentasi terkait sarana seperti dokumentasi dalam bangunan yang terkait ruang praktik. Dokumen tersebut memberikan informasi mengenai penggunaan internet sehingga membantu peneliti memahami dasar kondisi sistem sebelum dirancangnya pengembangan akses internet di lingkungan sekolah.

2. Literatur ilmiah dan referensi terkait.

Literatur yang digunakan meliputi buku, jurnal, artikel ilmiah, serta penelitian terdahulu yang membahas autentikasi *user manager*, konfigurasi mikrotik, penggunaan *access point*, manajemen *bandwidth*, keamanan jaringan, serta pemanfaatan internet dalam lingkungan pendidikan. Literatur tersebut menjadi landasan teoritis yang memperkuat konsep perancangan simulasi, mendukung analisis terhadap kondisi jaringan, serta memberikan dasar ilmiah dalam penerapan solusi yang diusulkan dalam penelitian ini.

Berdasarkan pemanfaatan berbagai sumber data sekunder, dapat disimpulkan bahwa data sekunder berperan penting dalam mendukung penelitian ini. Arsip dan dokumen internal sekolah memberikan gambaran awal mengenai penggunaan layanan internet dan infrastruktur jaringan yang tersedia, sementara literatur ilmiah memberikan dasar teori mengenai autentikasi *user manager*, mikrotik, *access point*, manajemen *bandwidth*, dan keamanan jaringan. Dengan demikian, data sekunder melengkapi data primer dan memperkuat analisis dalam perancangan pengembangan jaringan di SMK Negeri 3 Prabumulih.

3.4 Teknik Pengumpulan Data

Pengumpulan data adalah proses sistematis untuk mengumpulkan dan merekam informasi yang relevan dengan tujuan penelitian tertentu. Dalam konteks

penelitian, pengumpulan data berfungsi untuk memperoleh informasi yang valid dan dapat diandalkan, yang nantinya akan dianalisis guna menjawab pertanyaan atau hipotesis yang diajukan (Romdona et al., 2025). Pengumpulan data merupakan langkah penting dalam penelitian ini, karena kualitas data yang diperoleh akan sangat memengaruhi ketepatan perancangan simulasi yang dikembangkan. Untuk itu, digunakan beberapa teknik pengumpulan data, yaitu observasi, wawancara, dan dokumentasi.

3.4.1 Observasi

Observasi adalah pengumpulan data melalui proses pencatatan gerak dan aktivitas manusia atau benda, atau peristiwa yang tidak terorganisir, berupa pertanyaan atau percakapan dengan individu yang diteliti (Wahyuni & Tamrin, 2024). Observasi menunjukkan bahwa jaringan internet di SMK Negeri 3 Prabumulih hanya tersedia di ruang kantor dan belum menjangkau ruang praktik TSM serta TKR.

Jaringan juga tidak memiliki sistem autentikasi, sehingga siapa pun dapat terhubung hanya dengan mengetahui kata sandi *wi-fi*, yang menyebabkan pembobolan *password* dan sulitnya pengendalian jaringan. Karena itu diperlukan autentikasi *user manager*, perluasan jangkauan jaringan, serta peningkatan keamanan melalui konfigurasi menyembunyikan IP lokal di balik IP publik, pembatasan akses sehingga hanya admin yang dapat melakukan ping dan *login* ke *router*, serta pemblokiran IP yang tidak sesuai untuk lingkungan pendidikan.

3.4.2 Wawancara

Wawancara merupakan salah satu metode yang paling umum digunakan dalam pengumpulan data pada penelitian kualitatif. Di kalangan perawat, aktivitas ini sering kali dianggap mudah karena mereka terbiasa berinteraksi dan menggali informasi dari pasien dalam praktik sehari-hari (Fadila et al., 2025). Wawancara dilakukan pada tanggal 1 Desember 2025 dengan Ketua Kompetensi TBSM dan Ketua Kompetensi TKRO. Wawancara ini bertujuan untuk menggali informasi terkait kondisi jaringan di sekolah, kendala yang terjadi di ruang praktik TSM dan

TKR, penyebab lemahnya akses internet, serta kebutuhan pengembangan jaringan agar kegiatan pembelajaran berbasis digital dapat berjalan optimal.

Dari wawancara ini, penulis memperoleh data yang memperkuat perlunya penerapan autentikasi *user manager*, penambahan *access point*, serta penambahan peningkatan keamanan pada *router* mikrotik yang sudah ada di ruang kantor untuk mengatasi permasalahan jaringan yang dialami di lingkungan SMK Negeri 3 Prabumulih khususnya di ruang praktik.

3.4.3 Dokumentasi

Dokumen ialah catatan peristiwa yang sudah berlalu. Dokumen bisa berbentuk tulisan, gambar atau karya-karya monumental dari seseorang. Dokumen yang berbentuk gambar, misalnya foto, gambar hidup, sketsa dan lain-lain (Putri & Murhayati, 2025). Dokumentasi dilakukan dengan mencatat kondisi jaringan di SMK Negeri 3 Prabumulih, khususnya di ruang kantor, ruang praktik TSM, dan ruang praktik TKR. Berdasarkan hasil dokumentasi, diketahui bahwa akses internet hanya tersedia di ruang kantor menggunakan layanan *iconnet*, namun ruang kantor belum memiliki autentikasi untuk internet nya.

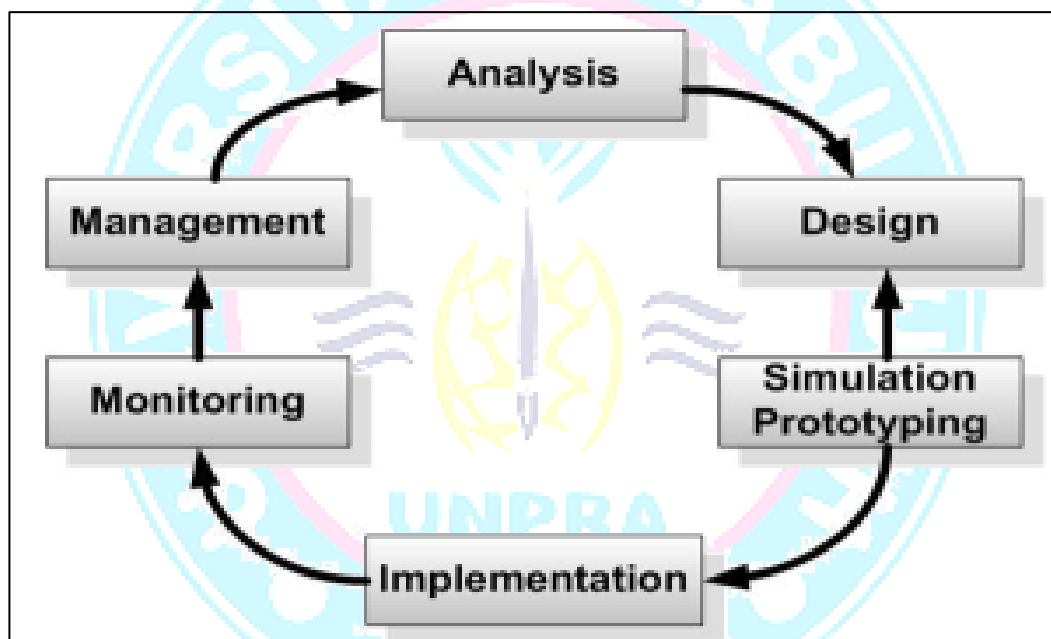
Ruang praktik TSM dan TKR belum memiliki *access point*, sehingga jaringan tidak menjangkau area tersebut. Data dokumentasi ini menjadi dasar untuk menggambarkan kondisi awal jaringan dan digunakan sebagai acuan dalam merancang simulasi penambahan *access point*, perluasan jangkauan internet, serta penerapan autentikasi *user manager* dan penambahan konfigurasi keamanan.

3.5 Metode Pengembangan Jaringan

NDLC atau *Network Development Life Cycle* merupakan suatu metode yang digunakan dalam mengembangkan atau merancang infrastruktur jaringan yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui kinerja jaringan. Model tersebut memiliki tahapan yang dimulai dari tahapan analisis, desain, simulasi prototype, implementasi, monitoring, dan manajemen (Rahman et al., 2023). *Network Development Life Cycle* adalah metode mengembangkan atau rancang infrastruktur dengan memantau kinerja jaringan. Hasil dari analisis kinerja

jaringan digunakan sebagai bahan pertimbangan dalam membuat desain jaringan (baik desain jaringan fisik atau jaringan logis) (Ariyadi et al., 2023).

Metode pengembangan jaringan yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC). Metode ini dipilih karena memberikan alur kerja yang terstruktur dalam merancang, membangun, dan melakukan simulasi jaringan. Pendekatan ini sesuai dengan penelitian yang berfokus pada simulasi perluasan akses internet ke ruang praktik TSM dan TKR, penambahan autentikasi *user manager* pada mikrotik, serta peningkatan keamanan jaringan. Dengan NDLC, proses pengembangan dapat dilakukan lebih terarah dan selaras dengan kondisi nyata di lapangan.



Sumber : Wikusoul (2025)

Gambar 3.2 Tahapan Metode NDLC

Berdasarkan gambar 3.2 di atas, dapat dilihat bahwa terdapat enam tahapan NDLC. Penelitian ini hanya menggunakan empat tahapan pengembangan jaringan, yaitu *Analysis*, *Design*, *Simulation*, dan *Monitoring*. Adapun penjelasan dari setiap tahap adalah sebagai berikut:

3.5.1 *Analysis* (Analisis Kebutuhan)

Tahap analisis dilakukan untuk memahami kondisi jaringan yang ada di SMK Negeri 3 Prabumulih. Pada tahap ini, peneliti melakukan observasi langsung di ruang kantor, ruang praktik TSM, dan ruang praktik TKR. Hasil analisis menunjukkan bahwa internet hanya tersedia di ruang kantor, terdapat mikrotik dan *access point* di ruang kantor, namun mikrotik tersebut belum memiliki sistem autentikasi pengguna. Selain itu, belum terdapat perangkat pendukung seperti *access point* di ruang praktik TSM dan TKR. Tahap ini bertujuan untuk memetakan kebutuhan jaringan serta mengidentifikasi permasalahan utama sebelum masuk ke tahap perancangan.

3.5.2 *Design* (Perancangan Topologi Jaringan)

Pada tahap perancangan, peneliti mulai merumuskan solusi berdasarkan permasalahan yang ditemukan pada tahap analisis. Perancangan meliputi pembuatan topologi star yang menghubungkan ruang kantor dengan ruang praktik TSM dan TKR melalui penambahan *access point*, serta pemanfaatan mikrotik sebagai pusat autentikasi *user manager*.

Topologi *star*, yang juga disebut topologi bintang, adalah jaringan yang memiliki bentuk konvergensi dari hub tengah ke setiap hub atau pengguna. Pada topologi star, biaya penggunaan dapat dikatakan rata-rata (Rifka Khairiansyah et al., 2024). Pada mikrotik tersebut direncanakan penambahan konfigurasi agar hanya administrator yang dapat melakukan *ping* dan melakukan pengaturan *router*, serta penambahan pemblokiran terhadap situs yang tidak sah agar perangkat di ruang praktik TSM, TKR, maupun ruang kantor tidak dapat mengakses situs yang diblokir. Selain itu, diterapkan mekanisme pengamanan untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan. Hasil tahap ini berupa rancangan topologi yang siap diuji melalui simulasi.

3.5.3 *Simulation* (Simulasi Jaringan)

Tahap ini dilakukan untuk menguji rancangan jaringan. Simulasi mencakup proses autentikasi pengguna melalui *user manager*, pengaturan pembagian *bandwidth* antara ruang praktik TSM dan TKR, serta pemeriksaan alur koneksi dari

ruang kantor hingga ruang praktik. Simulasi ini bertujuan memastikan bahwa topologi dan konfigurasi yang telah dirancang berjalan sesuai fungsi dan mampu menyelesaikan masalah jaringan yang sebelumnya ditemukan di sekolah.

Tahap pengujian juga didukung dengan implementasi terbatas menggunakan perangkat nyata seperti *router*, sumber internet, dan *access point*. Implementasi ini bertujuan untuk memvalidasi hasil perancangan agar lebih mendekati kondisi jaringan sebenarnya, khususnya dalam pengujian autentikasi, manajemen *bandwidth*, konektivitas jaringan, dan keamanan jaringan.

3.5.4 Monitoring (Pemantauan Hasil Simulasi)

Monitoring dilakukan untuk mengevaluasi kinerja jaringan berdasarkan hasil simulasi. Pada tahap ini peneliti memantau stabilitas koneksi, melihat *form login* autentikasi ruang kantor dan ruang praktik TSM dan TKR, pemerataan *bandwidth*, serta respons keamanan jaringan. Pemantauan ini digunakan untuk menilai apakah rancangan sudah memenuhi kebutuhan sekolah atau masih memerlukan perbaikan. Hasil *monitoring* menjadi dasar untuk menarik kesimpulan akhir mengenai efektivitas rancangan simulasi jaringan yang dikembangkan.

3.6 Alat Bantu Perancangan

Dalam membuat simulasi jaringan komputer kita dapat menggunakan salah satu *software* yaitu *cisco packet tracer*, dengan menggunakan aplikasi ini seorang administrator jaringan dapat mengetahui secara pasti sistem jaringan yang ada (Colanus Rally Drajana & Bode, 2021). Alat bantu perancangan simulasi pada penelitian ini memiliki peranan penting dalam membantu peneliti merancang, menguji, serta mengimplementasikan skenario jaringan secara virtual sebelum diterapkan pada lingkungan nyata di SMK Negeri Prabumulih. Penggunaan alat bantu ini dilakukan pada setiap tahapan penelitian mulai dari perancangan topologi, pemodelan proses, pengukuran kualitas jaringan, hingga pengujian autentikasi pengguna.

3.6.1 Alat Bantu Utama

Cisco Packet Tracer adalah sebuah aplikasi yang digunakan untuk membangun jaringan secara simulasi. Aplikasi *cisco packet tracer* biasanya digunakan oleh pemula untuk mengajarkan mereka cara merancang, mengkonfigurasi, dan memecahkan masalah jaringan (Rahmat et al., 2024). *Cisco Packet Tracer* menjadi salah satu software simulasi yang paling populer digunakan dalam pembelajaran jaringan komputer, baik di perguruan tinggi maupun di SMK. Aplikasi ini menawarkan berbagai fitur yang mampu merepresentasikan jaringan komputer secara virtual dengan cukup akurat (Henrayanto Denny Yulizar & Haris, 2025).

Dalam penelitian ini, *cisco packet tracer* digunakan sebagai alat utama dalam merancang dan mensimulasikan jaringan yang diusulkan. Penggunaan aplikasi ini membantu dalam melakukan pengujian konfigurasi serta analisis kinerja jaringan secara virtual sebelum diterapkan pada lingkungan nyata. Dengan demikian, *cisco packet tracer* sangat mendukung keberhasilan penelitian dalam menghasilkan model jaringan yang optimal dan sesuai dengan kebutuhan pengguna, serta dapat menjadi masukan bagi pihak SMK Negeri 3 Prabumulih dalam pengembangan jaringan internet di sekolah.

3.6.2 Alat Bantu Proses Konfigurasi Jaringan

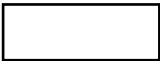
Flowchart adalah alat visual yang digunakan untuk menggambarkan proses atau alur kerja secara sistematis dan jelas. Simbol-simbol yang digunakan dalam *flowchart*, seperti kotak untuk langkah- langkah, panah untuk arah aliran, dan berlian untuk keputusan membantu mengilustrasikan langkah-langkah dalam proses dengan cara yang mudah dipahami. Manfaat *flowchart* meliputi pemodelan proses bisnis, analisis sistem, perancangan solusi yang lebih efisien, serta dokumentasi yang membantu dalam pemahaman dan komunikasi proses kerja (Rahmadan & Eri Gunawan, 2024).

Langkah pertama dalam penelitian ini adalah membuat diagram alur (*flowchart*), yang digunakan untuk menggambarkan langkah-langkah yang harus dilakukan dalam proses konfigurasi jaringan. Proses ini dimulai dengan menentukan konfigurasi untuk beberapa topologi jaringan, yang mencakup

pemilihan jenis koneksi dan perangkat yang akan digunakan, seperti *router*, *switch*, dan *server* (Ariyadi & Jordi, 2024).

Berikut adalah simbol-simbol *flowchart* dapat dilihat pada tabel 3.1 berikut :

Tabel 3.2 Simbol *Flowchart*

No	Gambar	Nama	Keterangan
1		<i>Terminator</i>	Menunjukkan mulai atau selesainya sebuah proses
2		<i>Process</i>	Menyatakan apa yang akan dilakukan dalam diagram alir.
3		<i>Decision</i>	Proses atau langkah yang menghasilkan keputusan atau kondisi tertentu. Di titik ini, selalu ada dua pilihan yang tersedia untuk melanjutkan aliran dalam kondisi yang berbeda.
4		<i>Input/Output</i>	Bisa digunakan untuk menunjukkan data masuk atau keluar.
5		<i>Arrow</i>	Menunjukkan bagaimana proses dan algoritma berjalan.

Sumber : (Aprilian & Afriansyah, 2024)

3.6.3 Alat Bantu Simulasi

Dalam proses pengembangan jaringan pada penelitian ini, pemanfaatan alat bantu simulasi memiliki peranan penting untuk memastikan bahwa konfigurasi jaringan berjalan sesuai dengan rancangan serta mampu menggambarkan kondisi operasional yang sebenarnya. Penggunaan beberapa *tools* ini memungkinkan peneliti untuk melakukan pengujian, pemantauan, dan validasi terhadap konektivitas, pemblokiran akses, serta kinerja jaringan.

Web Browser merupakan aplikasi atau *software* yang digunakan untuk melakukan pencarian atau menjelajahi internet guna memperoleh informasi dari suatu *web*. Pada awalnya, *browser* hanya dapat menampilkan teks, namun pada

perkembangannya *web browser* kini tidak hanya menampilkan teks saja, tetapi juga dapat mendukung pemutaran multimedia seperti video dan suara (Hariani, 2021). *Web browser* digunakan sebagai media untuk menguji akses *form login* oleh guru di ruang kantor serta siswa di ruang praktik TSM dan TKR. Melalui *browser*, peneliti dapat memverifikasi apakah IP yang diizinkan maupun yang diblokir telah berfungsi sesuai dengan kebijakan akses yang ditetapkan pihak sekolah.

CMD merupakan aplikasi berbasis *Command line interpreter* pada *system operasi Microsoft Windows* (Allo & Widiasari, 2024). *Command Prompt (CMD)* digunakan untuk melakukan pengujian konektivitas dasar seperti *ping* terhadap *IP* jaringan maupun internet. Melalui CMD, peneliti dapat mengevaluasi parameter penting seperti *jitter*, *packet loss*, dan *delay* yang menggambarkan kualitas jaringan. Fitur ini membantu dalam menentukan apakah jaringan berada dalam kondisi stabil atau memerlukan perbaikan konfigurasi.

Command Line Interface (CLI) adalah antarmuka pengguna yang paling populer dan paling dasar untuk berinteraksi dengan komputer (Rosnelly & Wira Yudha, 2023). *Command Line Interface (CLI)* dimanfaatkan untuk mengamati keseluruhan konfigurasi perangkat jaringan. Melalui CLI, peneliti dapat memeriksa paket yang dikirim maupun diterima, total *byte* yang digunakan, serta memastikan bahwa setiap ruang praktik telah menerima konfigurasi sesuai kebutuhan. Penggunaan CLI memberikan visibilitas mendalam terhadap performa serta integritas jaringan yang sedang disimulasikan.

Simple PDU adalah *tools* yang digunakan untuk menambahkan sederhana pada topologi jaringan (Khairi Faldi & Hadi, 2023). *Simple PDU* digunakan sebagai alat untuk mensimulasikan proses *ping* secara visual dalam lingkungan simulator. Dengan fitur ini, peneliti dapat melihat apakah pengiriman pesan berhasil (*success*) atau gagal, sekaligus memvalidasi jalur komunikasi antar perangkat dalam skenario simulasi jaringan.

Winbox adalah sebuah *software* atau *utility* yang digunakan untuk meremot sebuah server mikrotik kedalam mode GUI (*Graphical User Interface*) melalui *operating system windows* (Siswanto, 2023). Dengan Winbox, pengguna dapat mengakses dan mengatur berbagai fitur *RouterOS* secara visual tanpa perlu menggunakan antarmuka baris perintah. Winbox digunakan sebagai alat untuk

melakukan konfigurasi dan monitoring jaringan secara langsung pada perangkat *router*.

Angry IP Scanner *Angry IP Scanner* adalah aplikasi serbaguna yang digunakan untuk memindai dan mencari alamat IP aktif di jaringan dan memberikan informasi detail tentang *port* terbuka pada setiap perangkat yang terdeteksi Ayman et al. (2024). Dengan *Angry IP Scanner*, pengguna dapat dengan cepat mengidentifikasi perangkat yang terhubung dalam suatu jaringan serta mengetahui status *port* yang terbuka. Aplikasi ini digunakan sebagai alat untuk melakukan pemindaian jaringan dan analisis awal terhadap perangkat yang aktif.

Nmap adalah alat yang digunakan untuk memindai *port* yang terbuka dari IP publik atau domain. Alat ini juga dapat digunakan untuk melihat versi dari *port* yang terbuka (Made Adi Surya Permana et al., 2025). Dengan Nmap, pengguna dapat mengetahui layanan yang berjalan pada jaringan serta mengidentifikasi *port* yang terbuka. Dalam penelitian ini, Nmap digunakan sebagai alat untuk mendukung keamanan jaringan dengan melakukan analisis terhadap *port* yang terbuka guna meminimalisir potensi akses tidak sah.

Iperf3 merupakan alat yang umum digunakan dalam pengukuran *throughput* jaringan, karena mampu mengevaluasi kapasitas *transfer* data secara relevan dan akurat antara dua perangkat dalam suatu jaringan (Muhajir & Utami, 2026). Dengan iperf3, pengguna dapat melakukan pengujian performa jaringan untuk mengetahui kualitas koneksi yang dihasilkan. Dalam penelitian ini, iperf3 digunakan sebagai alat untuk menguji penerapan manajemen *bandwidth* sehingga dapat diketahui apakah pembagian *bandwidth* telah berjalan sesuai dengan konfigurasi yang ditetapkan.

Melalui pemanfaatan berbagai alat bantu tersebut, proses pengujian dan simulasi jaringan dapat dilakukan secara lebih terarah, komprehensif, dan akurat. Setiap alat memberikan kontribusi dalam memverifikasi konektivitas, keamanan, serta kinerja jaringan sehingga konfigurasi yang dirancang dapat berjalan sesuai dengan tujuan penelitian. Dengan demikian, sistem yang dikembangkan diharapkan mampu memenuhi kebutuhan pengelolaan akses jaringan dan monitoring konektivitas pada lingkungan praktik di sekolah.

3.6.4 Perangkat Implementasi (*Prototype*)

Dalam proses pengembangan jaringan pada penelitian ini, penggunaan perangkat nyata sebagai implementasi terbatas (*prototype*) memiliki peranan penting untuk mendukung hasil perancangan yang telah dilakukan. Pemanfaatan perangkat ini bertujuan untuk memastikan bahwa konfigurasi jaringan tidak hanya berjalan pada tahap simulasi, tetapi juga dapat diterapkan pada kondisi yang lebih mendekati lingkungan sebenarnya. Dengan adanya implementasi terbatas, peneliti dapat melakukan pengujian langsung terhadap autentikasi pengguna, manajemen *bandwidth*, serta konektivitas jaringan secara nyata.

Router merupakan perangkat utama dalam jaringan yang berfungsi untuk mengatur lalu lintas data serta menghubungkan beberapa jaringan menjadi satu kesatuan. Pada penelitian ini, *router* digunakan sebagai pusat pengelolaan jaringan yang bertugas dalam mengatur autentikasi pengguna melalui *user manager*, melakukan pembagian *bandwidth*, serta menerapkan kebijakan keamanan jaringan. Melalui penggunaan *router*, peneliti dapat memastikan bahwa setiap pengguna memperoleh hak akses sesuai dengan perannya, baik sebagai guru maupun siswa.

Sumber internet digunakan sebagai media penghubung jaringan lokal dengan jaringan global sehingga memungkinkan dilakukannya pengujian akses secara langsung. Dengan adanya koneksi internet, peneliti dapat menguji apakah jaringan yang telah dikonfigurasi mampu memberikan akses yang stabil serta sesuai dengan kebijakan yang telah ditetapkan. Penggunaan sumber internet juga memungkinkan evaluasi terhadap kualitas jaringan berdasarkan parameter konektivitas yang dihasilkan.

Access point merupakan perangkat yang berfungsi untuk mendistribusikan jaringan secara nirkabel kepada pengguna. Dalam penelitian ini, *access point* digunakan sebagai media penghubung antara perangkat *client* dengan jaringan utama. Melalui *access point*, pengguna dapat terhubung ke jaringan untuk melakukan proses autentikasi serta mengakses layanan yang tersedia. Selain itu, *access point* juga berperan dalam memperluas jangkauan jaringan ke ruang praktik sehingga konektivitas dapat terdistribusi secara merata.

Melalui pemanfaatan perangkat implementasi terbatas ini, proses pengujian jaringan dapat dilakukan secara lebih realistis dan terarah. Hasil dari pengujian

tersebut digunakan sebagai bentuk validasi terhadap perancangan jaringan yang telah dibuat, sehingga sistem yang dikembangkan mampu memenuhi kebutuhan pengelolaan jaringan serta mendukung aktivitas pembelajaran di lingkungan sekolah.

3.7 Pengujian Simulasi

Pada penelitian ini, proses pengujian dilakukan melalui serangkaian pengujian jaringan yang dirancang untuk memastikan bahwa seluruh konfigurasi, aturan akses, serta mekanisme pengelolaan jaringan berjalan sesuai dengan perancangan. Pengujian dilakukan secara sistematis menggunakan alat bantu simulasi serta didukung dengan implementasi terbatas untuk memverifikasi fungsionalitas dan keandalan jaringan.

Pengujian difokuskan pada beberapa fitur dan konfigurasi utama, antara lain:

1. Tahapan Menggunakan *Web Browser*

Tahapan *web browser* dilakukan untuk melihat *form login captive portal*, mengonfirmasi *login* antara guru dan siswa, serta menguji IP/situs yang telah diblokir.

- a. Tahapan pertama yaitu membuka *Web Browser* pada PC/Laptop guru atau siswa.
- b. Tahapan kedua yaitu memasukkan alamat IP *gateway* atau alamat *server user manager (captive portal)* pada kolom URL.
- c. Tahapan ketiga yaitu memastikan *form login captive portal* tampil dengan benar.
- d. Tahapan keempat yaitu melakukan *login* menggunakan *username* dan *password* guru yang telah dibuat, lalu mengamati apakah akses internet berhasil diberikan.
- e. Tahapan kelima yaitu melakukan *login* menggunakan akun siswa dan memastikan sistem merespons sesuai hak akses yang ditentukan.
- f. Tahapan keenam yaitu mencoba mengakses IP atau situs yang telah dimasukkan ke daftar blokir.

- g. Tahapan ketujuh yaitu memastikan sistem menolak atau memblokir akses tersebut sesuai konfigurasi *filtering* yang telah diterapkan.

2. Tahapan Menggunakan CMD (*Command Prompt*)

Tahapan CMD dilakukan untuk mengecek konektivitas internet, serta mengukur *packet loss*, *jitter*, dan *delay*.

- a. Tahapan pertama yaitu membuka aplikasi CMD (*Command Prompt*) pada sistem operasi *windows*.
- b. Tahapan kedua yaitu mengetikkan perintah *ping google.com -t* untuk melakukan pengujian konektivitas internet secara terus-menerus.
- c. Tahapan ketiga yaitu mengamati hasil *reply* yang diterima dari server tujuan untuk memastikan perangkat berhasil terhubung ke jaringan internet.
- d. Tahapan keempat yaitu menghitung nilai *packet loss* berdasarkan jumlah paket data yang gagal terkirim selama proses pengujian berlangsung.
- e. Tahapan kelima yaitu mengamati nilai *time* (ms) pada hasil *ping* untuk menganalisis besar kecilnya *delay* pada jaringan.
- f. Tahapan keenam yaitu melakukan pengujian secara berulang untuk melihat kestabilan koneksi jaringan berdasarkan perubahan nilai *delay* yang digunakan sebagai indikator *jitter*.

3. Tahapan Menggunakan CLI (*Command Line Interface*) Router

Tahapan CLI dilakukan untuk mengecek koneksi aktif pada *router* mikrotik dan memastikan proses translasi IP (*Network Address Translation/NAT*) berjalan dengan baik.

- a. Tahapan pertama yaitu membuka aplikasi winbox dan masuk ke *router* mikrotik menggunakan akun administrator.
- b. Tahapan kedua yaitu membuka menu new terminal pada *router* mikrotik.
- c. Tahapan ketiga yaitu mengetik perintah */ip firewall connection print* pada terminal *router* mikrotik.

- d. Tahapan keempat yaitu menjalankan perintah untuk menampilkan daftar koneksi aktif pada jaringan *hotspot*.
 - e. Tahapan kelima yaitu mengamati alamat IP sumber (*SRC-ADDRESS*) dari perangkat client dan alamat IP tujuan (*DST-ADDRESS*) yang terhubung ke internet.
 - f. Tahapan keenam yaitu memastikan koneksi jaringan berjalan dengan baik berdasarkan munculnya status koneksi aktif dengan protokol TCP dan port HTTPS (443).
 - g. Tahapan ketujuh yaitu memastikan proses translasi IP (*NAT*) berjalan dengan baik sehingga perangkat *client* pada jaringan lokal dapat mengakses internet melalui *router* mikrotik.
4. Tahapan Menggunakan *Simple PDU*
- Tahapan *Simple PDU* dilakukan untuk memastikan hanya admin yang dapat melakukan *ping* ke *router*.
- a. Tahapan pertama yaitu memilih fitur *Simple PDU* pada menu *Cisco Packet Tracer*.
 - b. Tahapan kedua yaitu mengirimkan PDU (*ping*) dari perangkat admin ke *router*.
 - c. Tahapan ketiga yaitu memastikan status pengiriman berhasil (*successful*).
 - d. Tahapan keempat yaitu mengirimkan PDU dari PC/Laptop ruang praktik (*non-admin*) ke *router*.
 - e. Tahapan kelima yaitu memastikan hasilnya gagal (*failed/request timed out*).
 - f. Tahapan keenam yaitu menyimpulkan bahwa konfigurasi pembatasan akses berjalan dengan baik karena hanya admin yang dapat melakukan *ping* ke *router*.
5. Tahapan Menggunakan *Speedtest*
- Tahapan *speedtest* dilakukan untuk mengukur kecepatan internet yang diterima oleh pengguna serta memastikan pembagian *bandwidth* berjalan sesuai dengan konfigurasi yang telah diterapkan.

- a. Tahapan pertama yaitu menghubungkan perangkat *client* (laptop/HP) ke jaringan melalui *access point*.
- b. Tahapan kedua yaitu membuka *web browser* pada perangkat *client*.
- c. Tahapan ketiga yaitu mengakses situs layanan *speedtest*.
- d. Tahapan keempat yaitu menjalankan pengujian kecepatan internet (*download* dan *upload*).
- e. Tahapan kelima yaitu mencatat hasil kecepatan yang diperoleh oleh pengguna.
- f. Tahapan keenam yaitu membandingkan hasil kecepatan antara pengguna guru dan siswa.
- g. Tahapan ketujuh yaitu memastikan bahwa pembagian *bandwidth* telah berjalan sesuai dengan kebijakan yang telah ditentukan.

6. Tahapan Menggunakan *Angry IP Scanner*

Tahapan *Angry IP Scanner* dilakukan untuk memindai alamat IP aktif dan mengidentifikasi perangkat yang terhubung dalam jaringan.

- a. Tahapan pertama yaitu membuka aplikasi *Angry IP Scanner*.
- b. Tahapan kedua yaitu memasukkan range alamat IP yang akan dipindai sesuai dengan jaringan yang digunakan.
- c. Tahapan ketiga yaitu menjalankan proses *scanning* dengan menekan tombol *Start*.
- d. Tahapan keempat yaitu menunggu hingga proses pemindaian selesai dilakukan.
- e. Tahapan kelima yaitu mengamati daftar IP yang aktif beserta informasi *port* yang terbuka.
- f. Tahapan keenam yaitu mengidentifikasi perangkat yang terhubung dan memastikan hanya perangkat yang diizinkan yang aktif dalam jaringan.

7. Tahapan Menggunakan Nmap

Tahapan Nmap dilakukan untuk menganalisis port yang terbuka serta layanan yang berjalan pada jaringan.

- a. Tahapan pertama yaitu membuka aplikasi Nmap atau terminal/*command prompt*.
 - b. Tahapan kedua yaitu memasukkan perintah scanning sesuai dengan target IP yang akan dianalisis.
 - c. Tahapan ketiga yaitu menjalankan proses *scanning port* pada jaringan.
 - d. Tahapan keempat yaitu menunggu hingga proses *scanning* selesai.
 - e. Tahapan kelima yaitu mengamati hasil *scanning* berupa daftar *port* yang terbuka dan layanan yang berjalan.
 - f. Tahapan keenam yaitu mengevaluasi hasil untuk mendeteksi potensi celah keamanan pada jaringan.
8. Tahapan Menggunakan Iperf3
- Tahapan iPerf3 dilakukan untuk menguji performa jaringan dan mengukur *throughput* sebagai bagian dari pengujian manajemen *bandwidth*.
- a. Tahapan pertama yaitu membuka aplikasi iperf3 pada perangkat *server*.
 - b. Tahapan kedua yaitu menjalankan iperf3 dalam mode *server*.
 - c. Tahapan ketiga yaitu membuka iperf3 pada perangkat *client*.
 - d. Tahapan keempat yaitu memasukkan alamat IP *server* pada perangkat *client*.
 - e. Tahapan kelima yaitu menjalankan pengujian *throughput* antara *server* dan *client*.
 - f. Tahapan keenam yaitu mengamati hasil pengujian berupa nilai *thg* yang diperoleh.
9. Tahapan Pengujian Ketahanan Jaringan Menggunakan NetCut
- Tahapan pengujian menggunakan *netcut* dilakukan untuk menguji ketahanan sistem jaringan terhadap upaya pemutusan koneksi internet pada perangkat yang terhubung ke jaringan.
- a. Tahapan pertama yaitu membuka aplikasi *netcut* pada perangkat yang bertindak sebagai penyerang.

- b. Tahapan kedua yaitu melakukan identifikasi perangkat target yang terhubung pada jaringan yang sama.
- c. Tahapan ketiga yaitu memilih perangkat target berdasarkan alamat *IP address* dan *MAC address* yang terdeteksi oleh aplikasi *netcut*.
- d. Tahapan keempat yaitu mengaktifkan fitur *speed control* atau *lag control* pada perangkat target yang dipilih.
- e. Tahapan kelima yaitu mengatur nilai *bandwidth* perangkat target hingga batas minimum (0) untuk mensimulasikan pemutusan akses internet.
- f. Tahapan keenam yaitu melakukan pengujian akses internet pada perangkat target setelah pengaturan *bandwidth* diterapkan.
- g. Tahapan ketujuh yaitu mengamati hasil pengujian untuk mengetahui apakah koneksi internet pada perangkat target terputus atau tidak.
- h. Jika koneksi internet target terputus, maka sistem pertahanan dinyatakan gagal karena perangkat kehilangan akses internet. Setelah itu pengaturan *netcut* dikembalikan ke kondisi normal atau fitur *speed control* dihentikan.
- i. Jika koneksi internet target tidak terputus dan perangkat masih dapat mengakses internet dengan lancar, maka sistem pertahanan dinyatakan berhasil.
- j. Tahapan terakhir yaitu mendokumentasikan hasil pengujian yang diperoleh, kemudian proses pengujian selesai.

10. Tahapan Pengujian *Command Prompt* arp -a

Tahapan pengujian *Command Prompt* dilakukan untuk memastikan bahwa perangkat yang terhubung pada jaringan *hotspot* tidak dapat berkomunikasi secara langsung dengan perangkat lain yang berada pada jaringan yang sama.

- a. Tahapan pertama yaitu menghubungkan perangkat korban ke jaringan *hotspot* yang telah dikonfigurasi dengan fitur *client isolation*.

- b. Tahapan kedua yaitu menjalankan perintah *ipconfig* pada *command prompt* (CMD) perangkat korban untuk melihat informasi konfigurasi jaringan.
 - c. Tahapan ketiga yaitu melakukan verifikasi terhadap IPv4 *address* dan *default gateway* yang diperoleh perangkat korban.
 - d. Tahapan keempat yaitu memastikan bahwa perangkat korban telah terhubung ke jaringan *hotspot* dengan status aktif dan dapat mengakses jaringan.
 - e. Tahapan kelima yaitu pada perangkat penyerang menjalankan perintah *arp -a* untuk menampilkan tabel ARP yang berisi daftar alamat IP dan MAC *address* perangkat yang terdeteksi pada jaringan.
 - f. Tahapan keenam yaitu mendeteksi dan mengidentifikasi alamat IP perangkat korban yang terdapat pada tabel ARP.
 - g. Tahapan ketujuh yaitu menjalankan perintah *ping* menuju alamat IP perangkat korban dari perangkat penyerang untuk menguji komunikasi antar perangkat dalam jaringan yang sama.
 - h. Tahapan kedelapan yaitu mengamati hasil pengujian. Jika fitur *client isolation* bekerja dengan baik, maka akan muncul pesan *request timed out* (RTO) dan nilai *packet loss* mencapai 100%.
 - i. Tahapan kesembilan yaitu menyimpulkan bahwa fitur *client isolation* berhasil diterapkan karena komunikasi antar *client* pada jaringan *hotspot* telah terblokir.
 - j. Tahapan terakhir yaitu mendokumentasikan hasil pengujian yang diperoleh, kemudian proses pengujian selesai.
11. Tahapan Pengujian Keamanan Jaringan Menggunakan *Wireless Network Watcher*.

Tahapan pengujian menggunakan *wireless network watcher* dilakukan untuk memastikan bahwa fitur *layer 2 isolation* (*client isolation*) bekerja dengan baik sehingga perangkat yang terhubung pada jaringan *hotspot* tidak dapat saling mendeteksi maupun berkomunikasi secara langsung.

- a. Tahapan pertama yaitu menghubungkan perangkat penyerang ke jaringan *hotspot* yang telah dikonfigurasi dengan fitur *client isolation*.
- b. Tahapan kedua yaitu menjalankan aplikasi *wireless network watcher* pada perangkat penyerang.
- c. Tahapan ketiga yaitu melakukan pemindaian jaringan lokal menggunakan aplikasi untuk mendeteksi perangkat-perangkat yang terhubung pada jaringan yang sama.
- d. Tahapan keempat yaitu mengamati daftar perangkat yang berhasil terdeteksi dari hasil pemindaian jaringan.
- e. Tahapan kelima yaitu memverifikasi hasil pemindaian. Jika fitur keamanan berjalan dengan baik, hanya *routerboard* (*gateway*) dan perangkat penyerang yang akan terdeteksi pada daftar perangkat.
- f. Tahapan keenam yaitu memastikan bahwa perangkat korban tidak muncul atau tidak terdeteksi pada hasil pemindaian jaringan.
- g. Tahapan ketujuh yaitu menyimpulkan bahwa fitur *layer 2 isolation* (*client isolation*) telah berhasil diterapkan karena perangkat client tidak dapat saling mendeteksi.
- h. Tahapan kedelapan yaitu mengamati bahwa komunikasi horizontal antar *client* pada jaringan telah terblokir sehingga akses langsung antar perangkat tidak dapat dilakukan.
- i. Tahapan kesembilan yaitu memastikan bahwa upaya serangan seperti *ARP spoofing* maupun pemindaian perangkat pada jaringan gagal dilakukan karena perangkat target tidak dapat ditemukan.
- j. Tahapan terakhir yaitu mendokumentasikan hasil pengujian yang diperoleh, kemudian proses pengujian selesai.

12. Tahapan Pengujian Ketahanan Jaringan Terhadap Serangan ARP Spoofing Menggunakan P2Pover

Tahapan pengujian menggunakan P2Pover dilakukan untuk menguji efektivitas fitur *client isolation* dalam mencegah serangan ARP spoofing yang bertujuan membatasi atau memutus akses internet perangkat target pada jaringan *hotspot*.

- a. Tahapan pertama yaitu menghubungkan perangkat penyerang dan perangkat korban ke jaringan *hotspot* yang sama.
- b. Tahapan kedua yaitu membuka aplikasi P2Pover pada perangkat penyerang.
- c. Tahapan ketiga yaitu membuat rule baru dengan nama "*wifi putus*" yang akan digunakan untuk melakukan pengujian terhadap perangkat target.
- d. Tahapan keempat yaitu melakukan konfigurasi *bandwidth* sebesar 10 KB/s serta mengaktifkan pemblokiran layanan WWW, P2P, dan IM pada *rule* yang telah dibuat.
- e. Tahapan kelima yaitu melakukan *bind rule* ke perangkat target yang akan dijadikan korban pengujian.
- f. Tahapan keenam yaitu menekan tombol *start* untuk menjalankan *rule* yang telah dikonfigurasi.
- g. Tahapan ketujuh yaitu memastikan status aplikasi berubah menjadi *running*, yang menandakan proses pengujian telah aktif.
- h. Tahapan kedelapan yaitu mengamati proses ARP *reply spoofing* yang dijalankan oleh aplikasi menuju perangkat target.
- i. Tahapan kesembilan yaitu melakukan validasi pada perangkat korban untuk mengetahui dampak serangan yang dilakukan.
- j. Tahapan kesepuluh yaitu menguji koneksi internet pada perangkat korban menggunakan layanan *speedtest* dan youtube.
- k. Tahapan kesebelas yaitu mengamati hasil pengujian. Jika perangkat korban masih dapat mengakses internet dengan

normal, maka serangan tidak berhasil memengaruhi koneksi jaringan.

- l. Tahapan kedua belas yaitu menyimpulkan bahwa fitur *client isolation* berhasil memblokir paket *ARP spoofing* sehingga komunikasi langsung antar client tidak dapat dimanfaatkan oleh penyerang.
- m. Tahapan terakhir yaitu mendokumentasikan hasil pengujian yang diperoleh, kemudian proses pengujian selesai.

13. Tahapan Menggunakan *Technitium MAC Address Changer* (TMAC)

Tahapan TMAC dilakukan untuk menguji apakah perangkat yang melakukan *MAC address spoofing* masih dapat memperoleh akses internet setelah fitur *cookie* pada *hotspot* mikrotik dinonaktifkan.

- a. Tahapan pertama yaitu memastikan konfigurasi *hotspot* mikrotik menggunakan metode autentikasi HTTP CHAP dengan fitur *cookie* dalam keadaan tidak diaktifkan.
- b. Tahapan kedua yaitu menghubungkan perangkat korban ke jaringan *hotspot* dan melakukan login menggunakan *username* dan *password* yang valid hingga berhasil terhubung ke internet.
- c. Tahapan ketiga yaitu membuka aplikasi *Technitium MAC Address Changer* (TMAC) pada perangkat penguji, kemudian menyalin *MAC address* milik perangkat korban.
- d. Tahapan keempat yaitu mengubah *MAC address* pada perangkat penguji menjadi sama dengan *MAC address* perangkat korban menggunakan aplikasi TMAC.
- e. Tahapan kelima yaitu menghubungkan kembali perangkat penguji ke jaringan *hotspot* menggunakan *MAC address* hasil penyamaran.
- f. Tahapan keenam yaitu mengamati respons sistem *hotspot* untuk mengetahui apakah perangkat diarahkan ke halaman *login hotspot* atau langsung memperoleh akses internet tanpa proses autentikasi ulang.

- g. Tahapan ketujuh yaitu mendokumentasikan hasil pengujian sebagai dasar evaluasi efektivitas penonaktifan fitur *cookie* dalam mencegah penyalahgunaan sesi *login* melalui teknik *MAC address spoofing*.

Selama proses pengujian, setiap hasil yang diperoleh dibandingkan dengan output yang diharapkan untuk memastikan bahwa konfigurasi jaringan berjalan sesuai dengan perancangan. Hasil pengujian baik melalui simulasi maupun implementasi terbatas menunjukkan bahwa sistem jaringan yang dirancang mampu berjalan dengan baik sesuai dengan tujuan penelitian.



BAB IV

ANALISA DAN PERANCANGAN

4.1 Analisa Sistem

4.1.1 Analisa dan Evaluasi Sistem Berjalan

a. Analisa Sistem Berjalan

Proses pengelolaan jaringan internet di SMK Negeri 3 Prabumulih saat ini masih menggunakan metode sederhana dan belum menerapkan sistem pengelolaan jaringan yang terstruktur. Akses internet berpusat di ruang kantor dengan menggunakan *router* mikrotik, kemudian didistribusikan melalui *access point* dengan satu kata sandi *wi-fi* yang digunakan secara bersama oleh seluruh pengguna. Pengguna, baik guru maupun siswa, dapat langsung terhubung ke jaringan tanpa melalui proses autentikasi, sehingga tidak terdapat identifikasi pengguna secara jelas di dalam sistem jaringan. Selain itu, penggunaan jaringan belum diatur berdasarkan hak akses atau kebutuhan masing-masing pengguna.

Dalam kondisi tersebut, seluruh perangkat yang terhubung ke jaringan memiliki akses yang sama tanpa adanya pembatasan. Penggunaan *bandwidth* tidak dikelola sehingga setiap pengguna dapat menggunakan kapasitas jaringan secara bebas sesuai kebutuhan masing-masing. Selain itu, jangkauan jaringan internet masih terbatas dan belum menjangkau seluruh area sekolah, khususnya pada ruang praktik Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR). Hal ini menyebabkan akses internet di beberapa area belum tersedia secara optimal dan belum dapat mendukung kegiatan pembelajaran berbasis digital secara maksimal.

Sistem jaringan yang berjalan saat ini memiliki beberapa kelemahan. Tidak adanya mekanisme autentikasi pengguna menyebabkan keamanan jaringan menjadi rendah dan rentan terhadap penyalahgunaan akses. Selain itu, tanpa adanya manajemen *bandwidth*, penggunaan internet menjadi tidak merata karena pengguna tertentu dapat menghabiskan kapasitas jaringan lebih besar dibandingkan pengguna lainnya. Administrator juga mengalami kesulitan dalam melakukan pemantauan dan pengendalian terhadap pengguna jaringan karena tidak adanya sistem yang dapat mengidentifikasi aktivitas masing-masing pengguna. Kondisi ini mengakibatkan pengelolaan jaringan menjadi kurang efektif, distribusi akses

internet tidak merata, serta berpotensi menghambat proses pembelajaran yang membutuhkan koneksi internet yang stabil dan terkontrol.

b. Evaluasi Sistem Berjalan

Berdasarkan analisa terhadap sistem jaringan yang berjalan saat ini, diperlukan solusi yang mampu mengatasi kelemahan dalam keamanan, pengelolaan pengguna, serta pemerataan akses internet. Sistem yang diusulkan adalah sistem jaringan berbasis mikrotik dengan penerapan autentikasi *user manager* dan manajemen *bandwidth* yang memungkinkan setiap pengguna melakukan *login* sebelum mengakses jaringan. Melalui proses autentikasi tersebut, administrator dapat mengidentifikasi pengguna yang terhubung serta mengatur hak akses sesuai dengan kebutuhan masing-masing.

Sistem jaringan yang diusulkan diharapkan mampu meningkatkan keamanan jaringan dengan membatasi akses hanya kepada pengguna yang terdaftar, serta mengurangi penyalahgunaan jaringan. Selain itu, penerapan manajemen *bandwidth* memungkinkan pembagian kapasitas internet secara lebih merata antara guru dan siswa, sehingga kualitas koneksi menjadi lebih stabil. Penambahan *access point* juga dilakukan untuk memperluas jangkauan jaringan hingga ke ruang praktik Teknik Sepeda Motor (TSM) dan Teknik Kendaraan Ringan (TKR), sehingga akses internet dapat digunakan secara optimal di seluruh area sekolah. Dengan demikian, sistem yang diusulkan ini dapat meningkatkan efisiensi, pemerataan, serta keandalan jaringan dibandingkan dengan sistem sebelumnya yang masih sederhana.

4.1.2 Analisa Kebutuhan

a. Kebutuhan Pengguna (User)

Sistem jaringan berbasis mikrotik ini digunakan oleh beberapa jenis pengguna dengan peran yang berbeda, yaitu:

1. Administrator (Admin Jaringan)

Administrator berperan sebagai pengelola sistem jaringan. Administrator dapat melakukan konfigurasi, mengelola, dan memperbarui pengaturan jaringan. Selain itu, administrator juga dapat melakukan monitoring terhadap aktivitas pengguna serta memastikan

keamanan jaringan berjalan dengan baik sesuai dengan kebijakan yang telah ditetapkan.

2. Guru

Guru berperan sebagai pengguna jaringan yang memiliki hak akses tertentu. Guru dapat mengakses internet untuk keperluan pembelajaran, administrasi, serta pencarian informasi yang mendukung kegiatan belajar mengajar. Selain itu, guru mendapatkan alokasi *bandwidth* yang lebih besar dibandingkan siswa agar aktivitas yang dilakukan dapat berjalan dengan lebih optimal dan stabil.

3. Siswa (TSM & TKR)

Siswa berperan sebagai pengguna utama dalam pemanfaatan jaringan di ruang praktik. Siswa dapat mengakses internet untuk kegiatan pembelajaran setelah melakukan proses *login* melalui sistem autentikasi yang telah disediakan. Akses yang diberikan kepada siswa dibatasi sesuai dengan kebijakan jaringan yang diterapkan, baik dari segi *bandwidth* maupun akses terhadap situs tertentu.

b. Kebutuhan Data

Data yang dibutuhkan dalam sistem jaringan meliputi:

1. Data Pengguna (*User manager*)

Data pengguna berisi informasi akun yang digunakan untuk mengakses jaringan, meliputi *username*, *password*, dan kategori pengguna (administrator, guru, atau siswa). Data ini digunakan untuk proses autentikasi serta pengaturan hak akses dalam jaringan.

2. Data IP Address

Data IP *address* berisi informasi alamat jaringan yang digunakan oleh setiap perangkat yang terhubung. Data ini digunakan untuk mengatur komunikasi antar perangkat agar dapat saling terhubung dalam jaringan lokal maupun internet.

3. Data *Bandwidth*

Data *bandwidth* mencakup pengaturan kecepatan akses internet yang diberikan kepada setiap pengguna atau kelompok pengguna. Data ini

digunakan untuk mengatur pembagian *bandwidth* agar penggunaan jaringan lebih merata dan tidak terjadi penumpukan trafik.

4. Data Aktivitas Jaringan (*Log Monitoring*)

Data aktivitas jaringan digunakan untuk mencatat aktivitas pengguna, seperti *login*, penggunaan *bandwidth*, serta akses jaringan. Data ini dimanfaatkan untuk monitoring dan evaluasi kinerja jaringan.

c. Kebutuhan Fungsional

Kebutuhan fungsional merupakan fungsi utama yang harus dimiliki oleh sistem jaringan berbasis mikrotik. Adapun kebutuhan fungsional sistem yang akan dibangun adalah sebagai berikut:

1. Sistem dapat menyediakan koneksi jaringan internet yang dapat diakses oleh pengguna melalui perangkat yang terhubung ke *access point*.
2. Sistem dapat mengarahkan pengguna ke halaman *login* (*captive portal*) sebelum dapat mengakses internet.
3. Sistem dapat melakukan autentikasi pengguna menggunakan *username* dan *password* yang terdaftar pada *user manager*.
4. Sistem dapat memberikan akses internet kepada pengguna yang berhasil *login* sesuai dengan hak akses yang dimiliki.
5. Sistem dapat membatasi penggunaan *bandwidth* pada setiap pengguna pengguna sesuai dengan kebijakan yang telah ditentukan.
6. Sistem dapat mengelola pembagian *IP address* secara otomatis menggunakan DHCP.
7. Sistem dapat melakukan konfigurasi NAT agar jaringan lokal dapat terhubung ke jaringan internet.
8. Sistem dapat melakukan monitoring aktivitas jaringan pengguna melalui *tools* yang digunakan.

d. Kebutuhan Non-Fungsional

Kebutuhan non-fungsional merupakan kebutuhan yang berkaitan dengan kualitas sistem jaringan, bukan pada fungsi utama sistem. Kebutuhan ini mencakup

aspek keamanan, kinerja, kemudahan penggunaan, keandalan, dan kompatibilitas sistem. Adapun kebutuhan non-fungsional sistem adalah sebagai berikut:

1. Keamanan (*Security*)

Sistem harus memiliki mekanisme autentikasi berupa *username* dan *password* untuk membatasi akses pengguna. Setiap pengguna hanya dapat mengakses jaringan sesuai dengan hak akses yang dimiliki. Selain itu, sistem harus mampu membatasi akses ke *router* hanya untuk administrator serta melakukan pemblokiran terhadap alamat IP atau situs tertentu yang tidak diizinkan.

2. Kinerja (*Performance*)

Sistem harus mampu memberikan koneksi internet dengan waktu respon yang cepat dan stabil. Jaringan diharapkan tetap berjalan dengan baik meskipun digunakan oleh banyak pengguna secara bersamaan serta mampu mengelola penggunaan *bandwidth* secara efisien.

3. Kemudahan Penggunaan (*Usability*)

Sistem harus dirancang agar mudah digunakan oleh pengguna, baik guru maupun siswa. Proses *login* dan akses jaringan dibuat sederhana sehingga pengguna tidak mengalami kesulitan dalam menggunakan layanan jaringan.

4. Keandalan (*Reliability*)

Sistem harus dapat berjalan secara stabil dan meminimalkan terjadinya gangguan jaringan. Koneksi internet harus tetap tersedia dan dapat digunakan sesuai dengan kebutuhan pengguna.

5. Ketersediaan (*Availability*)

Jaringan harus dapat digunakan selama kegiatan pembelajaran berlangsung sehingga dapat mendukung aktivitas belajar mengajar secara optimal.

6. Kompatibilitas (*Compatibility*)

Sistem jaringan harus dapat digunakan pada berbagai perangkat seperti laptop dan smartphone dengan sistem operasi yang berbeda tanpa mengalami kendala berarti.

e. Analisa Perangkat Keras & Lunak (*Hardware & Software*)

Analisa perangkat keras dan perangkat lunak dilakukan untuk mengetahui spesifikasi minimum yang dibutuhkan agar sistem jaringan berbasis mikrotik dapat berjalan dengan baik dan optimal. Analisa ini mencakup kebutuhan perangkat yang digunakan dalam proses perancangan, simulasi, konfigurasi, serta pengujian jaringan.

Perangkat keras (*hardware*) merupakan komponen fisik yang digunakan dalam sistem jaringan, seperti *router*, komputer, dan perangkat pendukung lainnya yang berfungsi untuk menjalankan proses komunikasi data. *Hardware* berperan sebagai sarana utama dalam membangun dan menjalankan jaringan komputer. Pada penelitian ini, penggunaan perangkat keras difokuskan pada perangkat inti yang mendukung proses implementasi jaringan. Pemilihan perangkat dilakukan secara terbatas dengan mempertimbangkan kebutuhan utama sistem, sehingga tetap mampu merepresentasikan kondisi jaringan yang dirancang tanpa harus menggunakan seluruh perangkat yang terdapat pada simulasi.

Perangkat lunak (*software*) adalah sekumpulan program atau aplikasi yang digunakan untuk mengatur dan mengendalikan perangkat keras agar dapat menjalankan fungsi tertentu sesuai dengan kebutuhan jaringan. *Software* berperan sebagai penghubung antara pengguna dan perangkat keras dalam pengelolaan sistem jaringan. Agar sistem dapat dikembangkan dan disimulasikan secara stabil meskipun dalam ruang lingkup terbatas, diperlukan standar minimum perangkat keras dan perangkat lunak sebagai berikut:

1. Perangkat Keras (*Hardware*)

Kebutuhan Perangkat Jaringan minimal:

- a. *Router* Mikrotik: Minimal seri RB750 (atau seri yang mendukung fitur *bandwidth management*).
- b. Sumber Internet: Modem Orbit Star A1 atau versi setara sebagai penyedia konektivitas.
- c. *Switch*: Minimal *switch* 5 port dengan dukungan kecepatan 10/100 Mbps.

- d. *Access point*: Minimal *access point* dengan standar *wireless IEEE 802.11n (N300)* dan mendukung konektivitas *wi-fi 2.4 GHz*.
- e. Kabel LAN (UTP): Kategori 5e (Cat5e) sebagai media penghubung fisik.

Kebutuhan Perangkat Pengembang minimal:

- a. Laptop/PC: Dengan prosesor minimal *Intel Core i3*.
- b. RAM: Kapasitas minimal 4 GB.
- c. Penyimpanan: Kapasitas minimal 256 GB.

Kebutuhan Perangkat Uji *Client* minimal:

Laptop:

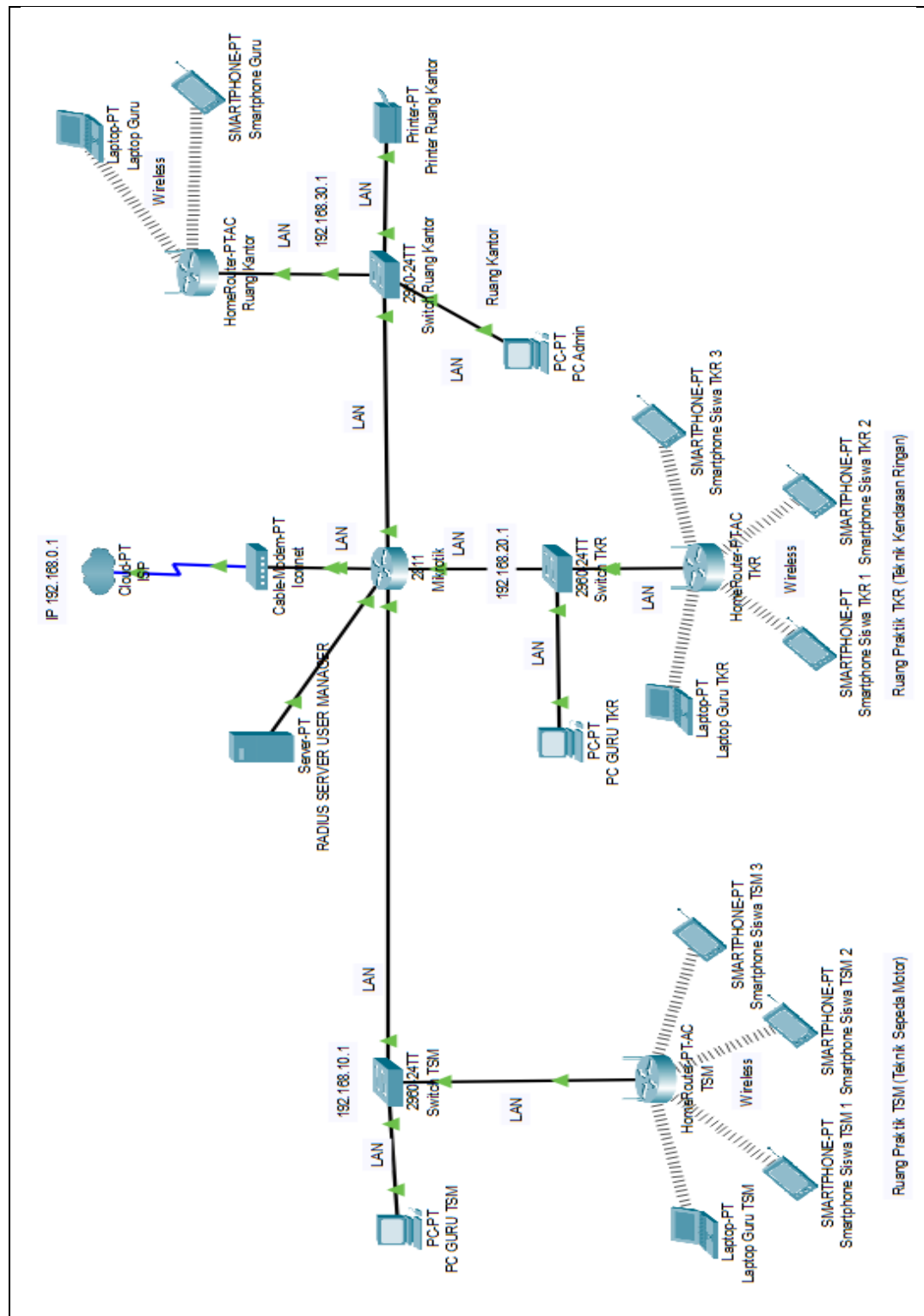
- a. Laptop/PC: Dengan prosesor minimal *Intel Core i3*.
- b. RAM: Kapasitas minimal 4 GB.
- c. Penyimpanan: Kapasitas minimal 256 GB.

2. Perangkat Lunak (*Software*)

- a. Sistem Operasi: *Windows 10 (64-bit)* atau lebih tinggi.
- b. *Visual Studio Code*: Minimal versi 1.80 dengan bahasa pemrograman HTML dan *extension Live Server*
- c. Aplikasi Simulasi & Konfigurasi: *Cisco Packet Tracer* dan Winbox.
- d. *Tools* Analisis Jaringan: *Angry IP Scanner*, Nmap, dan iPerf3.
- e. Alat Pengujian Koneksi: *Command Prompt (CMD)*, *Speedtest*, dan *Ping Test*.
- f. *Tools* Pengujian Keamanan Jaringan: *NetCut*, TMAP, P2Pover, perintah ARP (*arp -a*) pada *Command Prompt*, dan *Wireless Network Watcher*.
- g. *Website*: *Google Chrome* atau *Mozilla Firefox*.

4.2 Perancangan Sistem yang Diusulkan

4.2.1 Topologi Jaringan



Sumber: Penulis, 2026

Gambar 4.1 Topologi Jaringan

Topologi Jaringan pada Gambar 4.1 menunjukkan rancangan yang digunakan dalam penelitian ini dengan menerapkan topologi *star* (bintang) sebagai struktur utama jaringan. Dalam arsitektur ini, *router* mikrotik berperan sebagai titik pusat (*central node*) yang mengelola seluruh lalu lintas data dan terhubung langsung dengan sumber internet. Penggunaan topologi *star* dipilih karena memberikan kemudahan dalam manajemen jaringan, di mana setiap jalur koneksi bersifat independen sehingga jika terjadi gangguan pada satu jalur ruangan, hal tersebut tidak akan memengaruhi konektivitas di ruangan lainnya.

Dari *router* pusat tersebut, jaringan didistribusikan melalui kabel ke beberapa *switch* yang menghubungkan masing-masing ruangan, seperti ruang praktik TSM, ruang praktik TKR, dan ruang kantor. Setiap ruangan dilengkapi dengan *access point* yang berfungsi untuk mendistribusikan jaringan secara nirkabel kepada perangkat *client* seperti laptop dan *smartphone*. Pembagian jaringan ini disertai dengan segmentasi *IP address* yang berbeda pada setiap ruangan untuk mempermudah pengelolaan dan pengaturan akses. Melalui penerapan topologi *star* ini, sistem jaringan dirancang agar mampu mendukung proses autentikasi pengguna, manajemen *bandwidth*, serta penerapan keamanan jaringan secara terpusat, sehingga setiap pengguna mendapatkan hak akses sesuai dengan kebijakan yang telah ditentukan.

Sebagai pelengkap dari rancangan digital tersebut, pengujian nyata pada saat sidang dilakukan melalui simulasi terbatas menggunakan alat peraga fisik. Dalam simulasi ini, peran penyedia internet (ISP) *iconnet* digantikan oleh modem telkomsel orbit, yang kemudian dihubungkan ke satu buah *router* mikrotik sebagai pengelola jaringan, satu buah *switch* sebagai penghubung distribusi jaringan, dan satu buah *access point* sebagai pemancar sinyal *wi-fi*. Meskipun menggunakan perangkat yang lebih ringkas, simulasi terbatas ini tetap merepresentasikan alur kerja utama dari topologi kompleks yang telah dirancang, mulai dari penerimaan sumber internet hingga distribusi akses ke pengguna akhir.

4.2.2 Simulasi Perangkat Jaringan

Sebagai pelengkap dari rancangan digital yang telah dibuat, penelitian ini juga melakukan simulasi terbatas menggunakan perangkat jaringan nyata sebagai

bentuk validasi hasil simulasi. Pada rancangan topologi jaringan, sumber internet menggunakan layanan *iconnet* sebagai representasi koneksi internet utama di lingkungan sekolah. Namun, pada tahap demonstrasi sidang, sumber internet disimulasikan menggunakan modem telkomsel orbit sebagai pengganti sementara ISP. Modem tersebut kemudian dihubungkan ke *router* mikrotik, *switch*, dan *access point* untuk mendukung proses distribusi jaringan. Adapun gambar perangkat dapat dilihat pada gambar berikut.



Sumber: Penulis, 2026

Gambar 4.2 Modem *Iconnet*

Layanan internet *iconnet* digunakan sebagai representasi sumber koneksi internet utama pada rancangan topologi jaringan di lingkungan sekolah.



Sumber: Penulis, 2026

Gambar 4.3 Mikrotik

Router mikrotik digunakan sebagai pusat pengelolaan jaringan yang mengatur autentikasi pengguna, manajemen *bandwidth*, dan distribusi koneksi internet.



Sumber: Penulis, 2026

Gambar 4.4 Switch

Switch digunakan untuk menghubungkan perangkat jaringan agar proses distribusi koneksi dapat berjalan dengan baik.



Sumber: Penulis, 2026

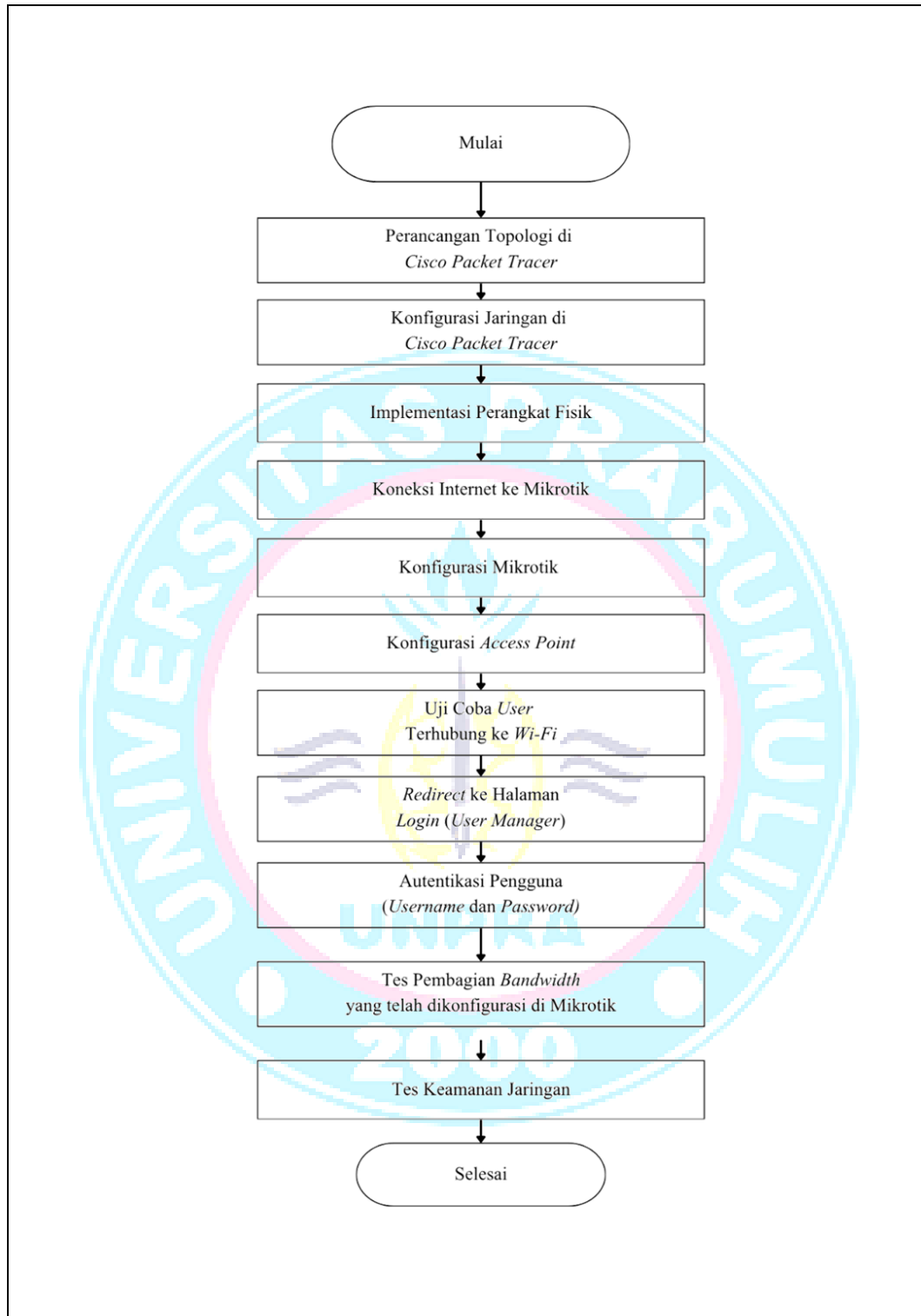
Gambar 4.5 *Access point*

Access point digunakan untuk memancarkan jaringan *wi-fi* sehingga perangkat pengguna dapat terhubung ke jaringan secara nirkabel.

4.2.3 Perancangan Sistem (Logis)

Perancangan sistem logis merupakan tahapan yang bertujuan untuk menggambarkan cara kerja sistem jaringan berdasarkan fungsi dan kebutuhan pengguna. Perancangan ini dituangkan dalam bentuk *flowchart* untuk menjelaskan alur proses jaringan serta *network diagram* untuk menggambarkan hubungan antar perangkat jaringan, jalur koneksi kabel, penggunaan *port*, dan pembagian jaringan pada setiap ruangan sehingga memudahkan proses konfigurasi, dan dokumentasi.

1. *Flowchart* Alur Perancangan

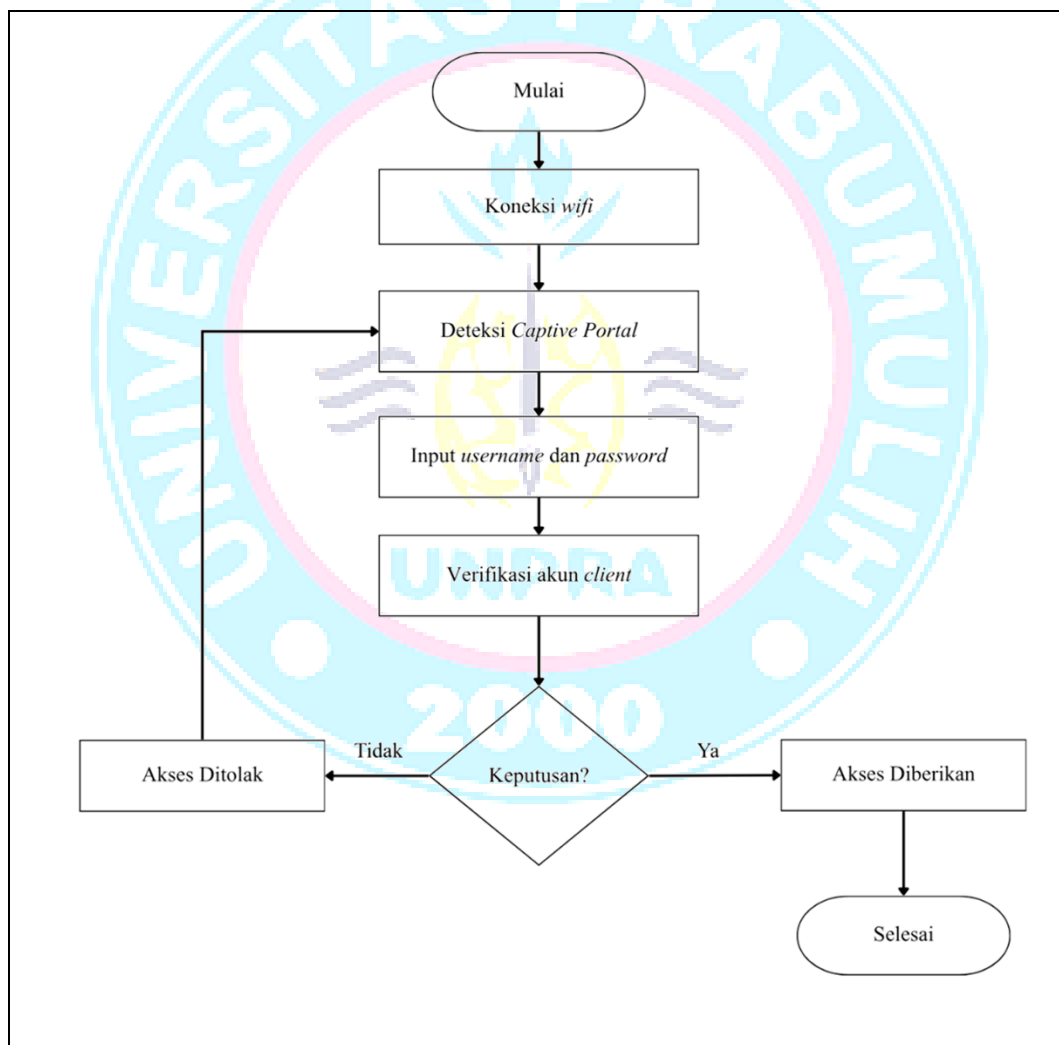


Sumber: Penulis, 2026

Gambar 4.6 *Flowchart* Sistem Jaringan

Flowchart pada Gambar 4.6 menggambarkan alur proses perancangan dan implementasi sistem jaringan yang dimulai dari tahap desain topologi menggunakan simulasi, kemudian dilanjutkan dengan konfigurasi jaringan. Selanjutnya dilakukan implementasi pada perangkat fisik, penghubungan jaringan, serta konfigurasi perangkat seperti mikrotik dan *access point*. Pada tahap akhir, sistem menerapkan autentikasi pengguna, manajemen *bandwidth*, serta keamanan jaringan sehingga sistem dapat berjalan sesuai dengan kebutuhan yang telah dirancang.

2. Flowchart Form Login

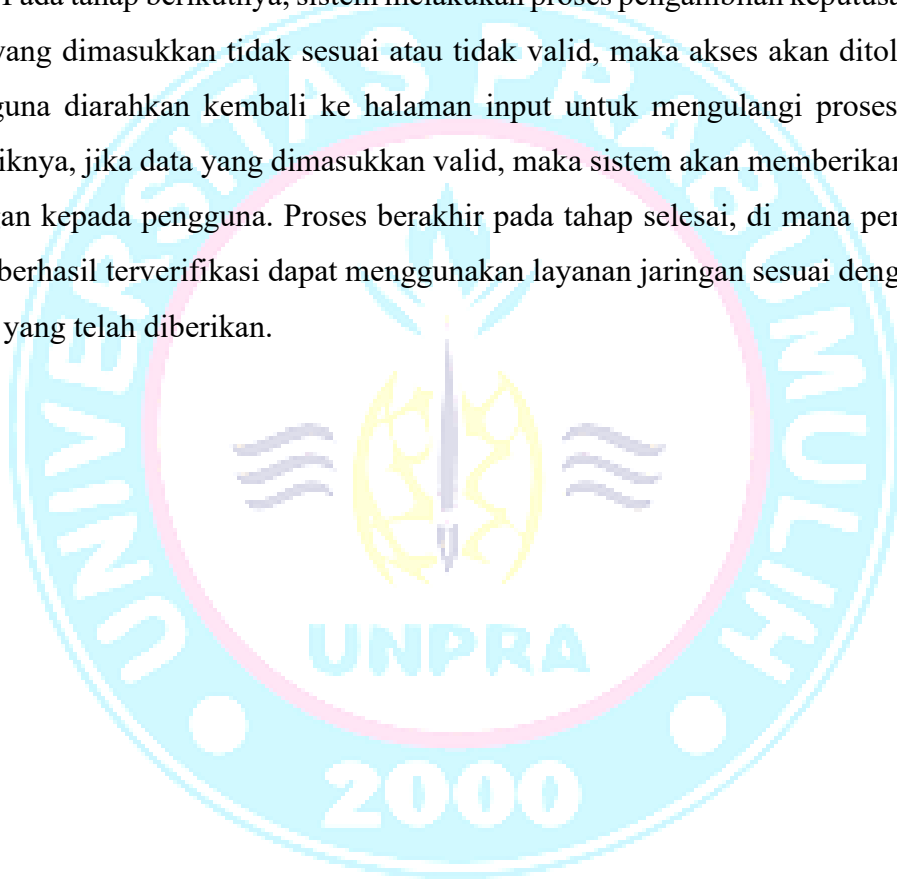


Sumber: Penulis, 2026

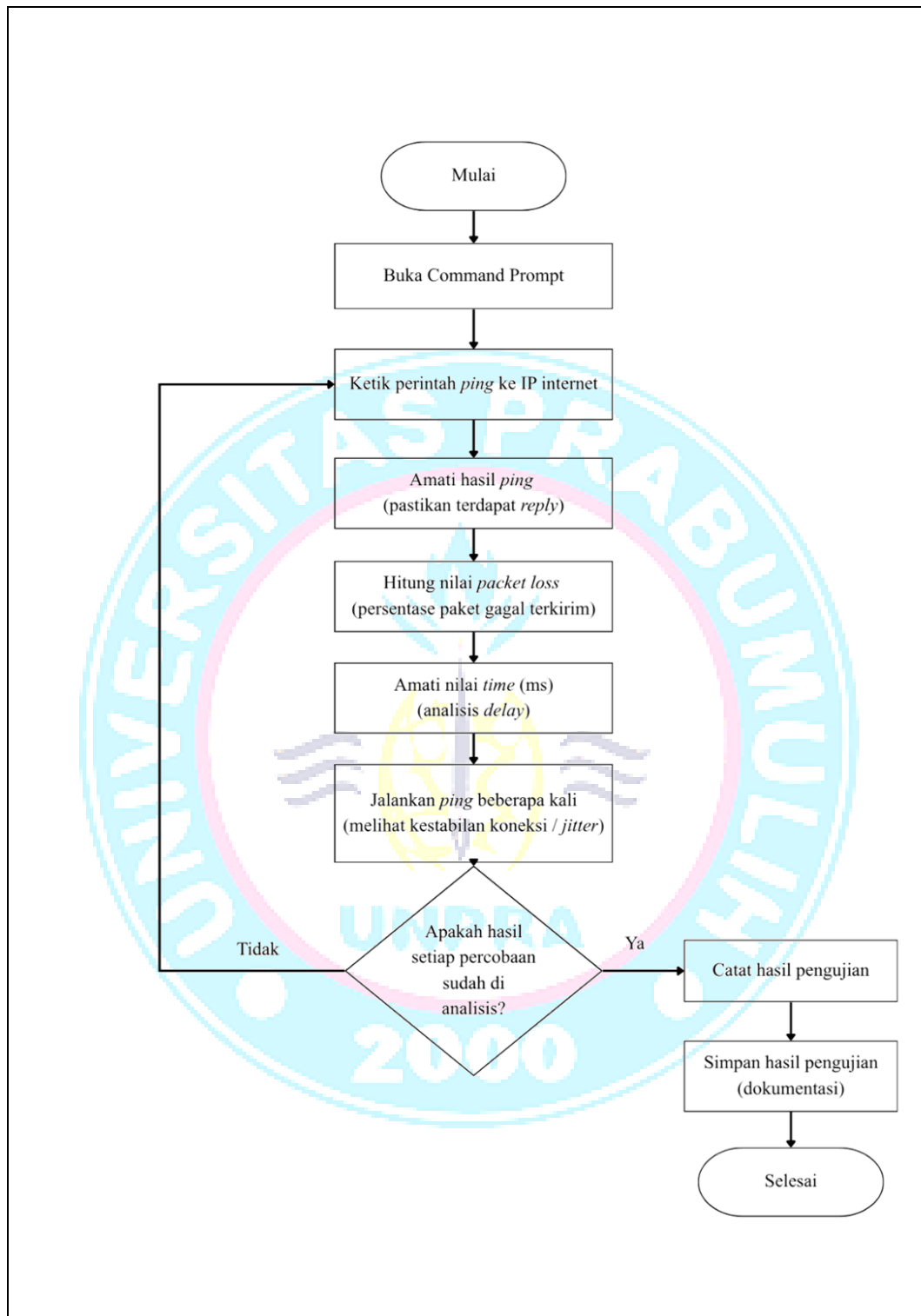
Gambar 4.7 Flowchart Form Login

Flowchart pada gambar tersebut menggambarkan alur proses autentikasi pengguna pada jaringan wifi berbasis *captive portal*. Proses dimulai dari tahap Mulai, kemudian pengguna melakukan koneksi ke jaringan *wi-fi* yang tersedia. Setelah perangkat terhubung, sistem akan melakukan deteksi *captive portal* untuk mengarahkan pengguna ke halaman *login*. Selanjutnya, pengguna diminta melakukan *input username & password* sebagai bentuk autentikasi. Data yang dimasukkan kemudian diproses pada tahap verifikasi akun *client* untuk memastikan bahwa akun yang digunakan *valid* dan terdaftar dalam sistem.

Pada tahap berikutnya, sistem melakukan proses pengambilan keputusan. Jika data yang dimasukkan tidak sesuai atau tidak valid, maka akses akan ditolak dan pengguna diarahkan kembali ke halaman input untuk mengulangi proses *login*. Sebaliknya, jika data yang dimasukkan valid, maka sistem akan memberikan akses jaringan kepada pengguna. Proses berakhir pada tahap selesai, di mana pengguna yang berhasil terverifikasi dapat menggunakan layanan jaringan sesuai dengan hak akses yang telah diberikan.



3. Flowchart Pengujian CMD

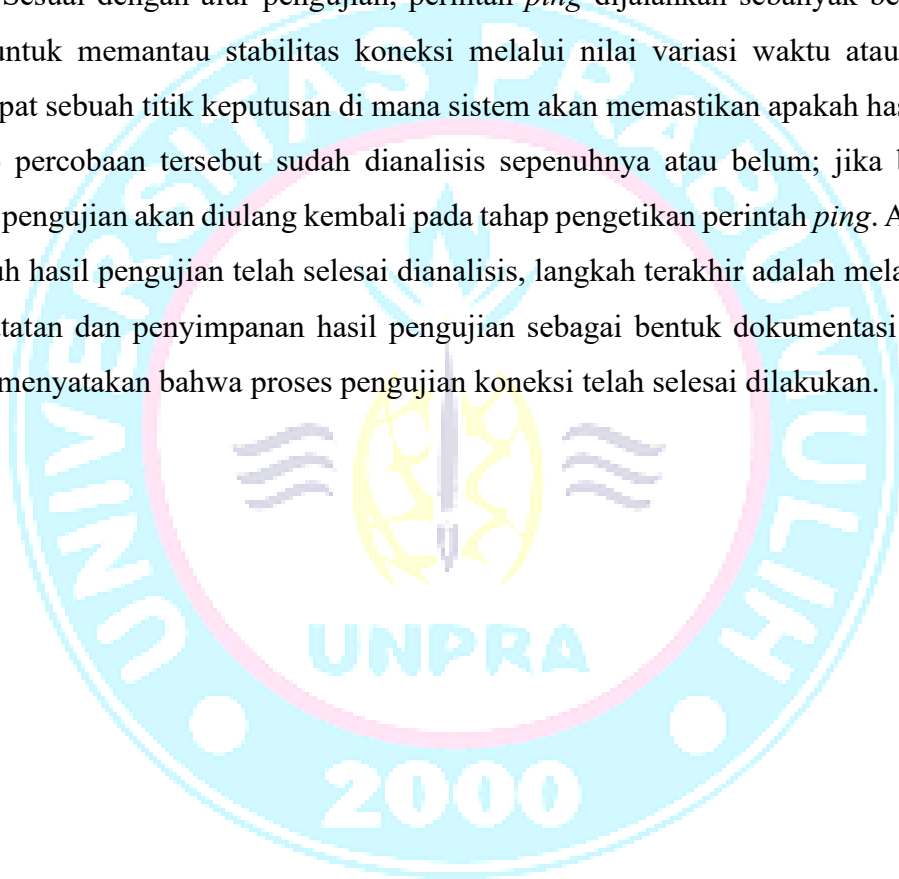


Sumber: Penulis, 2026

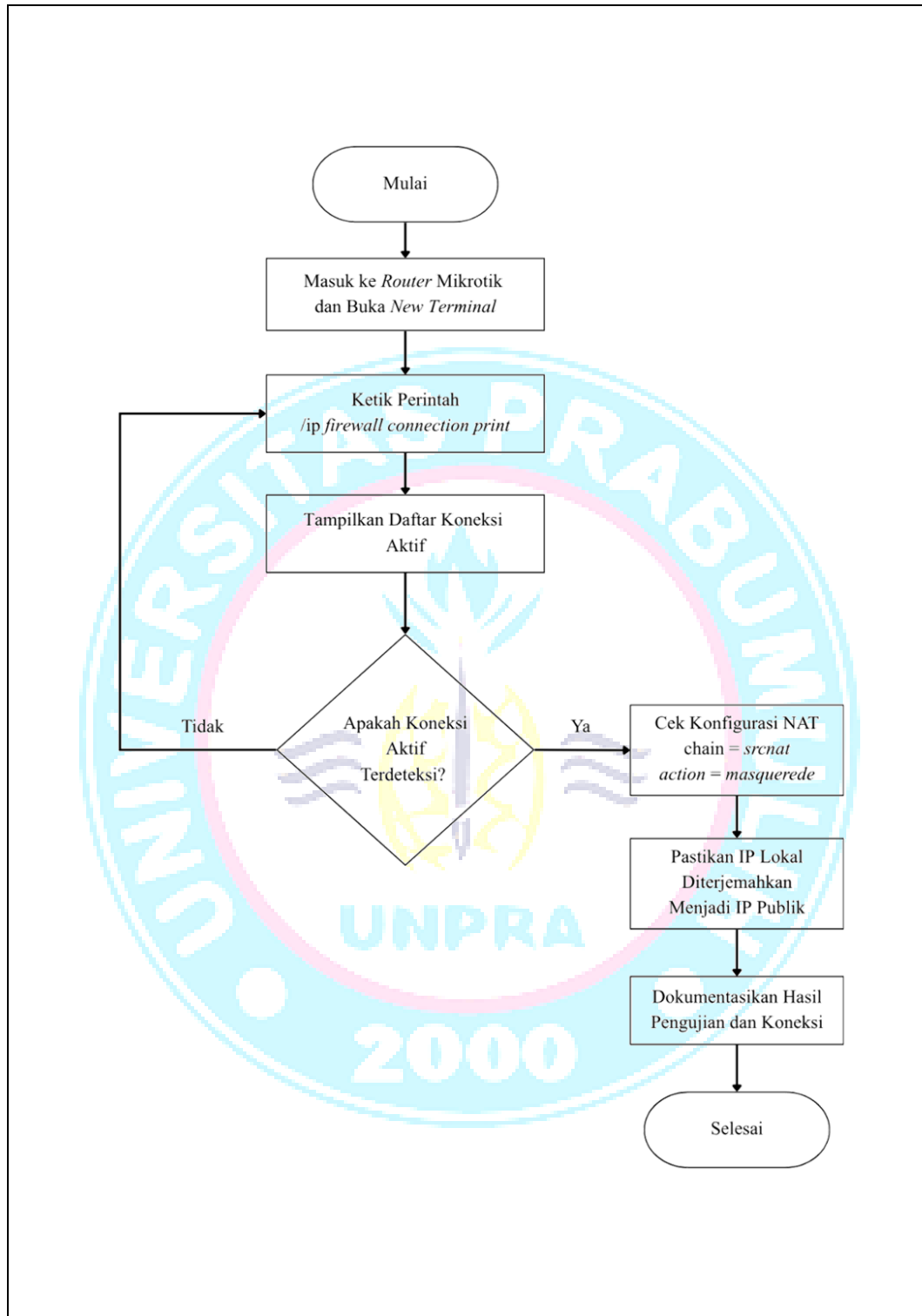
Gambar 4.8 Alur Pengujian CMD / Command Prompt

Flowchart pada gambar tersebut menggambarkan alur proses pengujian konektivitas jaringan yang dilakukan melalui terminal komputer secara sistematis. Proses dimulai dengan membuka jendela *command prompt*, kemudian dilanjutkan dengan mengetikkan perintah *ping* ke alamat IP internet untuk memverifikasi jalur komunikasi. Tahap pengamatan dilakukan dengan memastikan adanya respon (*reply*), menghitung nilai *packet loss* untuk mengetahui persentase kegagalan pengiriman data, serta menganalisis nilai waktu dalam satuan milidetik (ms) guna mengukur tingkat penundaan atau *delay* pada jaringan tersebut.

Sesuai dengan alur pengujian, perintah *ping* dijalankan sebanyak beberapa kali untuk memantau stabilitas koneksi melalui nilai variasi waktu atau *jitter*. Terdapat sebuah titik keputusan di mana sistem akan memastikan apakah hasil dari setiap percobaan tersebut sudah dianalisis sepenuhnya atau belum; jika belum, maka pengujian akan diulang kembali pada tahap pengetikan perintah *ping*. Apabila seluruh hasil pengujian telah selesai dianalisis, langkah terakhir adalah melakukan pencatatan dan penyimpanan hasil pengujian sebagai bentuk dokumentasi teknis yang menyatakan bahwa proses pengujian koneksi telah selesai dilakukan.



4. Flowchart Pengujian CLI



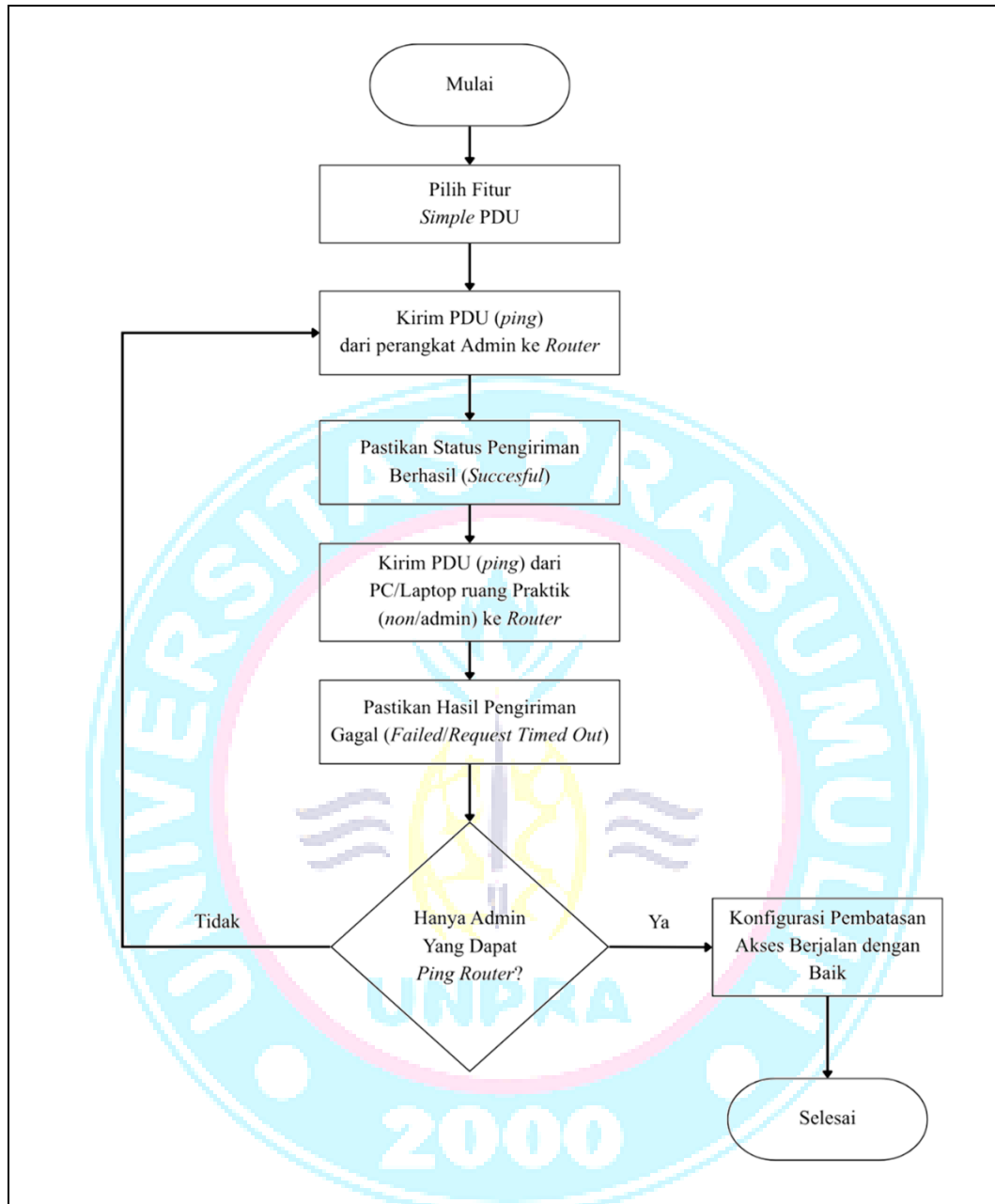
Sumber: Penulis, 2026

Gambar 4.9 Alur Pengujian CLI

Flowchart pada gambar tersebut menggambarkan alur proses pengujian menggunakan *command line interface* (CLI) pada *router* mikrotik untuk memeriksa koneksi aktif dan konfigurasi *network address translation* (NAT). Proses dimulai dengan masuk ke *router* mikrotik dan membuka *new terminal* sebagai media untuk menjalankan perintah pengujian. Administrator kemudian mengetikkan perintah */ip firewall connection print* untuk menampilkan daftar koneksi aktif yang sedang berlangsung pada *router*. Informasi yang ditampilkan digunakan untuk mengetahui apakah koneksi aktif telah terdeteksi atau belum.

Jika koneksi aktif belum terdeteksi, maka proses kembali ke tahap menjalankan */ip firewall connection print* hingga koneksi aktif dapat ditampilkan. Jika koneksi aktif berhasil terdeteksi, pengujian dilanjutkan dengan melakukan pemeriksaan konfigurasi NAT pada *router* mikrotik. Pemeriksaan berikutnya dilakukan untuk memastikan bahwa alamat IP lokal dapat diterjemahkan menjadi alamat IP publik melalui mekanisme NAT. Proses ini bertujuan untuk mengamati translasi alamat IP yang terjadi pada *router* saat perangkat melakukan komunikasi jaringan. Hasil pengujian dan informasi koneksi kemudian didokumentasikan sebagai data pengujian. Setelah dokumentasi selesai dilakukan, proses pengujian CLI pada *router* mikrotik dinyatakan selesai.

5. Flowchart Pengujian Simple PDU



Sumber: Penulis, 2026

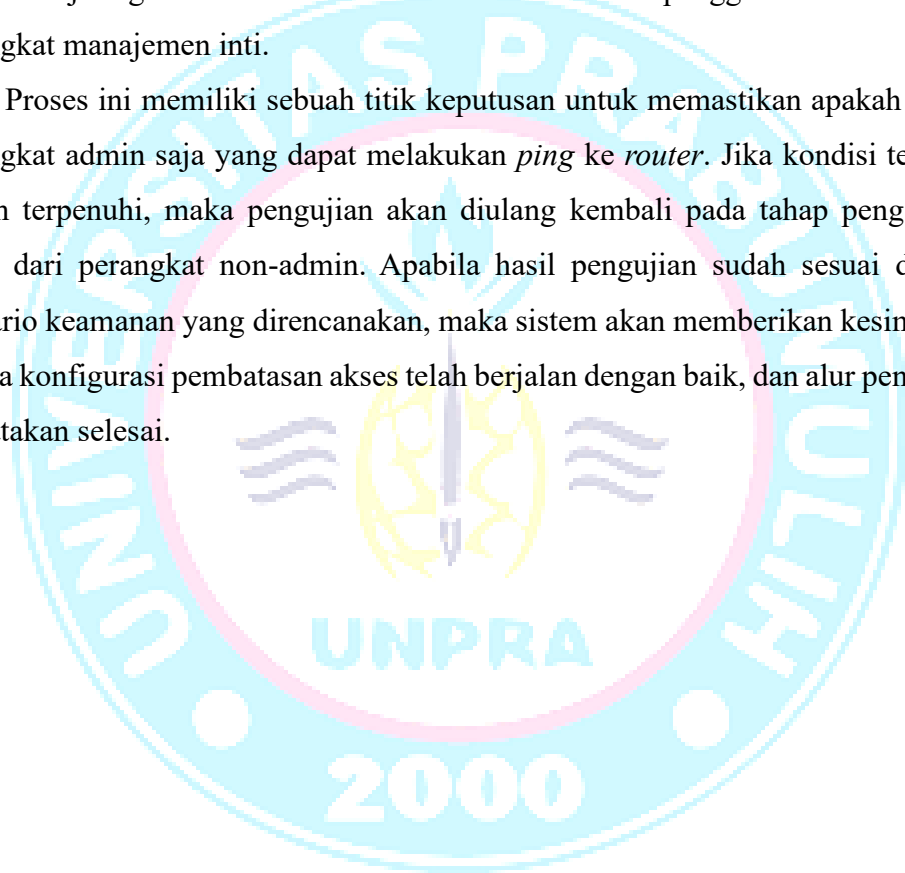
Gambar 4.10 Alur Pengujian Simple PDU

Flowchart pada gambar tersebut menggambarkan alur proses pengujian pembatasan akses perangkat melalui simulasi pengiriman paket data menggunakan fitur *simple PDU*. Proses diawali dengan memilih fitur tersebut untuk melakukan uji coba koneksi berupa perintah *ping* dari perangkat admin menuju *router* utama. Pada tahap ini, penguji harus memastikan bahwa status pengiriman paket data

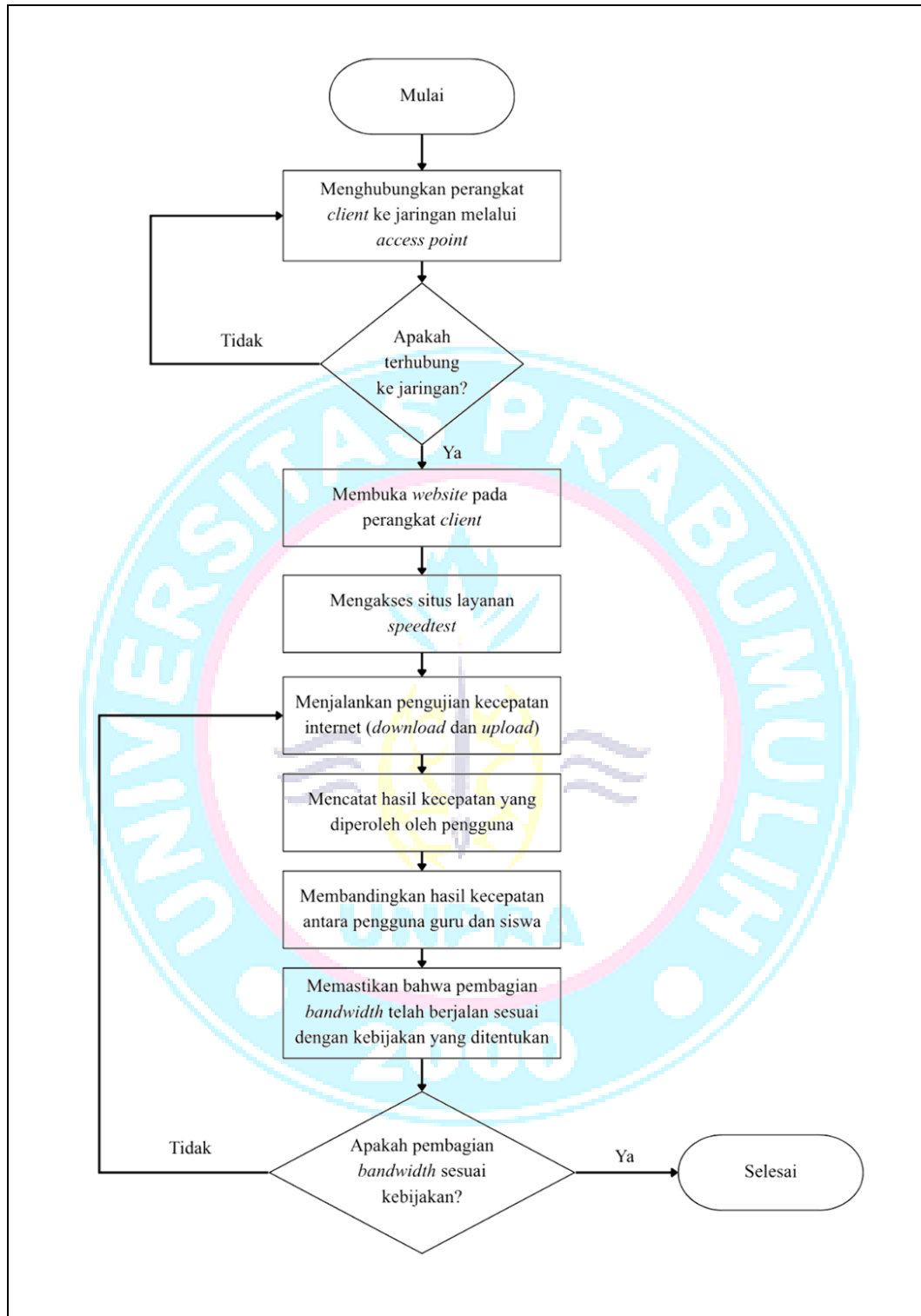
menunjukkan hasil yang berhasil atau *successful*, yang menandakan bahwa perangkat administrator memiliki hak akses penuh untuk berkomunikasi dengan *router*.

Langkah selanjutnya adalah melakukan pengujian perbandingan dengan mengirimkan PDU dari perangkat non-admin, seperti PC atau laptop yang berada di ruang praktik, ke arah *router*. Berbeda dengan pengujian sebelumnya, pada tahap ini hasil yang diharapkan adalah pengiriman harus gagal dengan keterangan *failed* atau *request timed out*. Hal ini dilakukan untuk memverifikasi bahwa kebijakan keamanan jaringan telah berhasil memblokir akses dari pengguna umum menuju perangkat manajemen inti.

Proses ini memiliki sebuah titik keputusan untuk memastikan apakah hanya perangkat admin saja yang dapat melakukan *ping* ke *router*. Jika kondisi tersebut belum terpenuhi, maka pengujian akan diulang kembali pada tahap pengiriman paket dari perangkat non-admin. Apabila hasil pengujian sudah sesuai dengan skenario keamanan yang direncanakan, maka sistem akan memberikan kesimpulan bahwa konfigurasi pembatasan akses telah berjalan dengan baik, dan alur pengujian dinyatakan selesai.



6. Flowchart Pengujian *Speedtest*



Sumber: Penulis, 2026

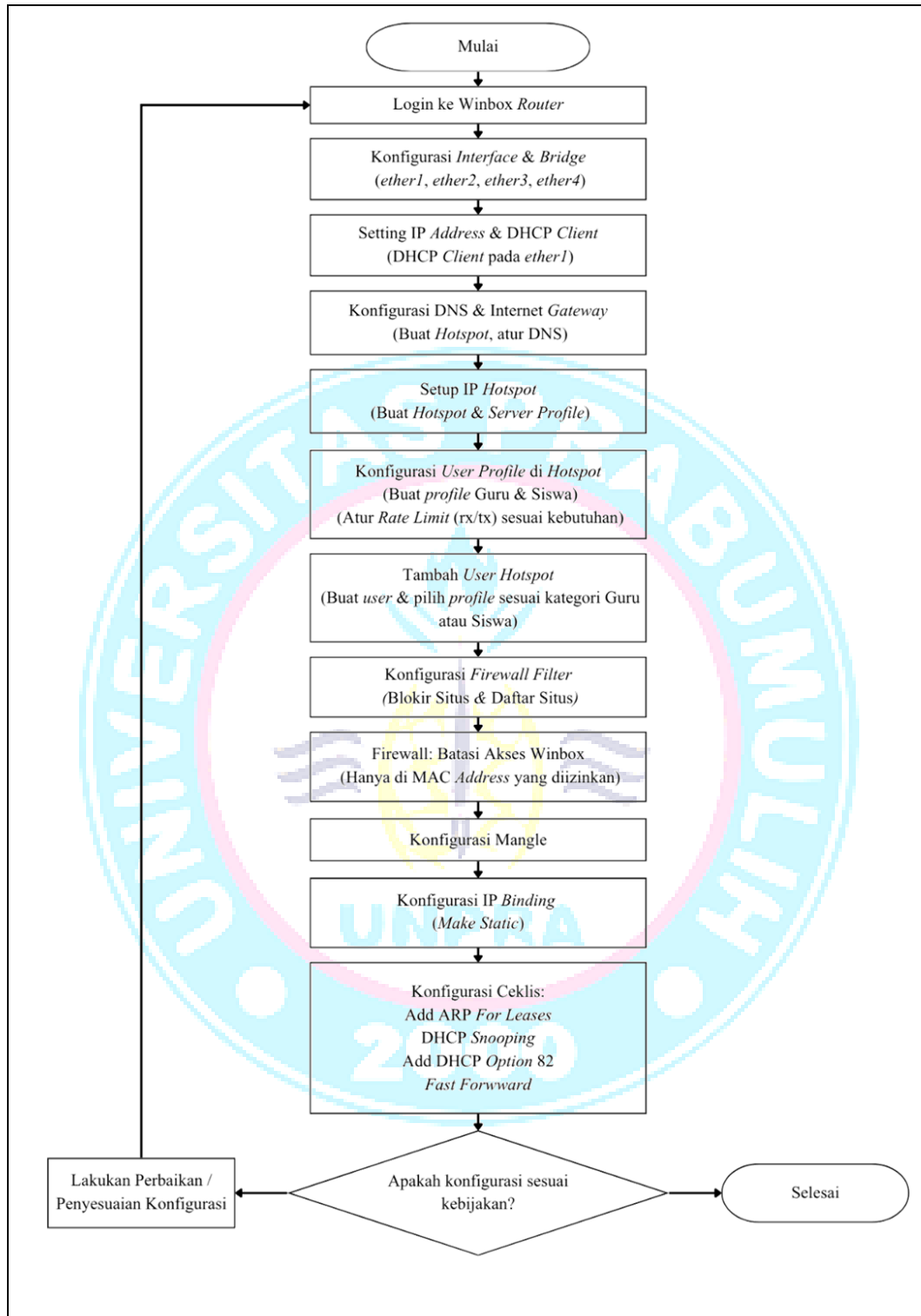
Gambar 4.11 Alur Pengujian *Speedtest*

Flowchart pada gambar tersebut menggambarkan alur proses pengujian dan verifikasi manajemen *bandwidth* pada jaringan nirkabel secara sistematis. Tahap awal dimulai dengan menghubungkan perangkat *client* ke jaringan melalui *access point*, diikuti dengan pemeriksaan status koneksi jika perangkat belum terhubung, maka proses akan kembali ke tahap penyambungan ulang hingga status dinyatakan berhasil. Setelah terhubung, pengguna diarahkan untuk membuka *web browser* pada perangkat tersebut guna mengakses situs layanan *speedtest*.

Langkah teknis selanjutnya adalah menjalankan pengujian kecepatan internet untuk mengukur performa *download* dan *upload* secara langsung. Hasil kecepatan yang diperoleh kemudian dicatat dan dibandingkan antara kelompok pengguna, dalam hal ini antara guru dan siswa, untuk memastikan bahwa pembagian *bandwidth* telah berjalan sesuai dengan kebijakan yang telah ditentukan sebelumnya.

Proses ini diakhiri dengan sebuah titik keputusan untuk memvalidasi apakah pembagian *bandwidth* tersebut sudah memenuhi standar kebijakan jika ditemukan ketidaksesuaian atau ketidaksesuaian, maka pengujian kecepatan akan diulang kembali untuk memastikan akurasi data. Apabila hasil perbandingan dinyatakan sudah sesuai dengan target konfigurasi, maka seluruh rangkaian alur pengujian dinyatakan selesai.

7. Flowchart Pengujian Winbox



Sumber: Penulis, 2026

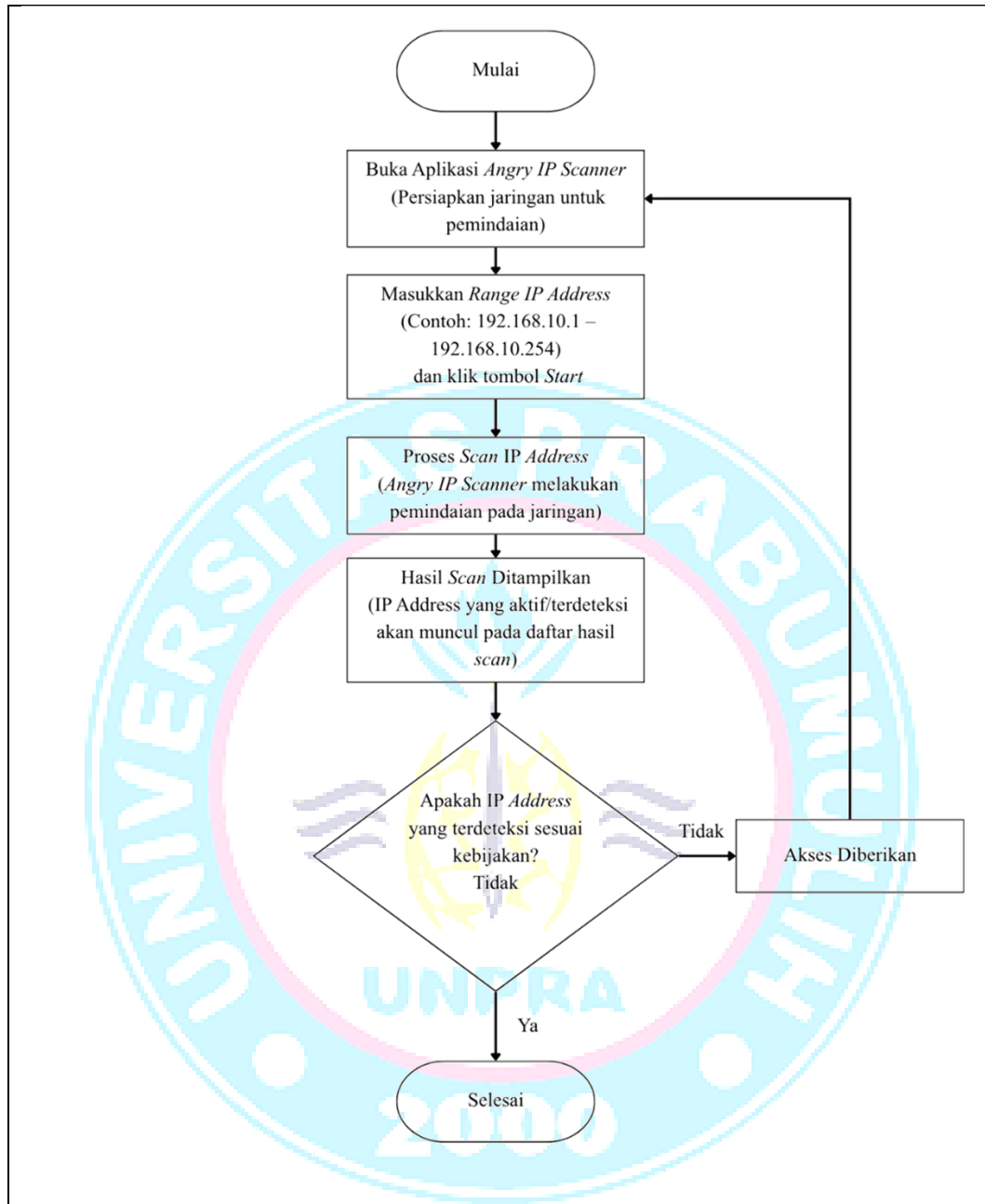
Gambar 4.12 Alur Pengujian Winbox

Flowchart pada gambar tersebut menggambarkan alur proses konfigurasi manajemen jaringan pada *router* mikrotik menggunakan aplikasi winbox. Proses dimulai dengan melakukan login ke *router* melalui winbox untuk mengakses menu konfigurasi yang tersedia. Konfigurasi dilanjutkan dengan pengaturan *interface* dan *bridge* yang meliputi *ether1*, *ether2*, *ether3*, dan *ether4*. Tahap berikutnya adalah melakukan pengaturan *IP address* serta mengaktifkan *DHCP client* pada *ether1* agar *router* dapat memperoleh alamat IP secara otomatis dari jaringan sumber internet. Konfigurasi DNS dan internet *gateway* kemudian dilakukan untuk mendukung layanan akses internet. Pada tahap ini juga dilakukan pembuatan layanan *hotspot* yang akan digunakan sebagai media autentikasi pengguna jaringan.

Pengaturan *hotspot* dilanjutkan dengan pembuatan *user profile* untuk kategori guru dan siswa. Masing-masing profil dapat diberikan pengaturan *rate limit* sesuai kebutuhan jaringan. Setelah profil dibuat, administrator menambahkan akun pengguna *hotspot* dan menentukan profil yang sesuai dengan kategori pengguna. Tahap berikutnya adalah melakukan konfigurasi *firewall filter* untuk mengatur pemblokiran akses ke situs tertentu. Pengamanan *router* juga dilakukan dengan membatasi akses winbox sehingga hanya perangkat dengan *MAC address* yang diizinkan yang dapat melakukan pengelolaan *router*.

Konfigurasi kemudian dilanjutkan dengan pengaturan *mangle* dan *IP Binding*. Pada bagian *IP binding* dilakukan pengaturan *make static* untuk menetapkan data pengguna tertentu secara permanen. Beberapa opsi tambahan kemudian diaktifkan, yaitu *Add ARP for leases*, *DHCP snooping*, *Add DHCP option 82*, dan *fast forward* untuk mendukung pengelolaan serta keamanan jaringan. Seluruh konfigurasi yang telah dibuat kemudian diperiksa untuk memastikan kesesuaiannya dengan kebijakan jaringan yang diterapkan. Jika konfigurasi belum sesuai, maka dilakukan perbaikan atau penyesuaian konfigurasi dan proses pemeriksaan diulangi kembali. Jika konfigurasi telah sesuai dengan kebijakan yang ditetapkan, maka proses konfigurasi dinyatakan selesai.

8. Flowchart Pengujian Angry IP Scanner



Sumber: Penulis, 2026

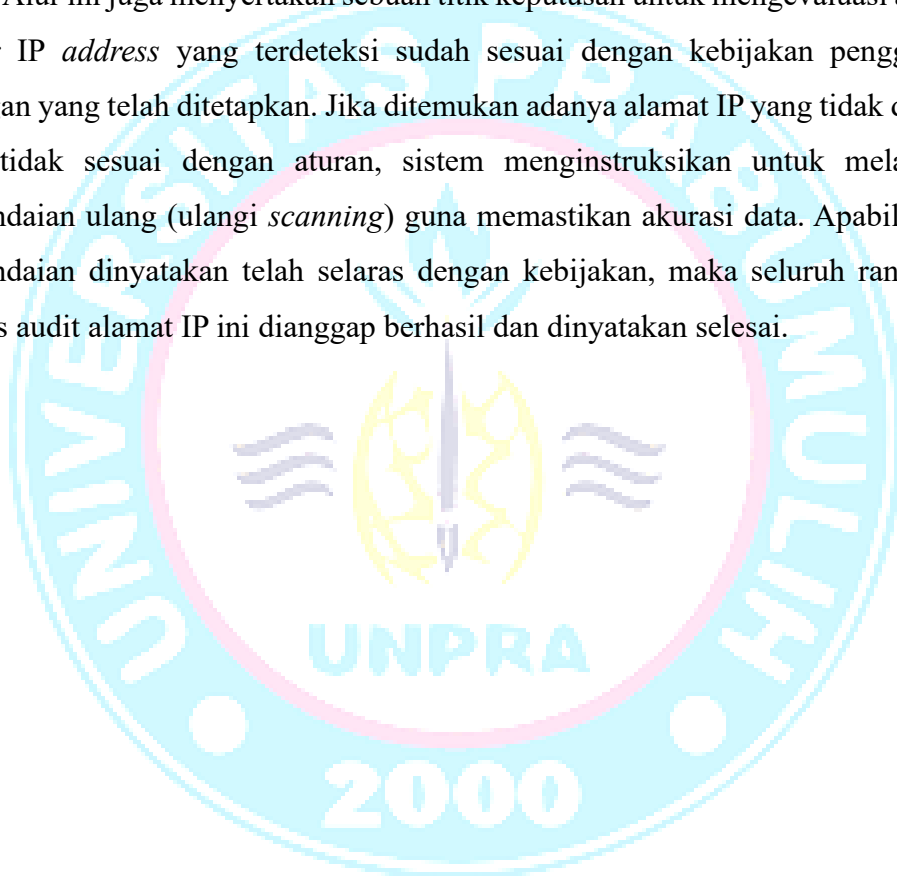
Gambar 4.13 Alur Pengujian Angry IP Scanner

Flowchart pada gambar tersebut menggambarkan alur proses pemindaian jaringan menggunakan perangkat lunak *angry IP icanner* untuk melakukan audit terhadap alamat IP yang aktif dalam suatu jaringan. Proses dimulai dengan membuka aplikasi *angry IP scanner* dan mempersiapkan infrastruktur jaringan yang akan dipindai. Langkah teknis selanjutnya adalah memasukkan *range* IP

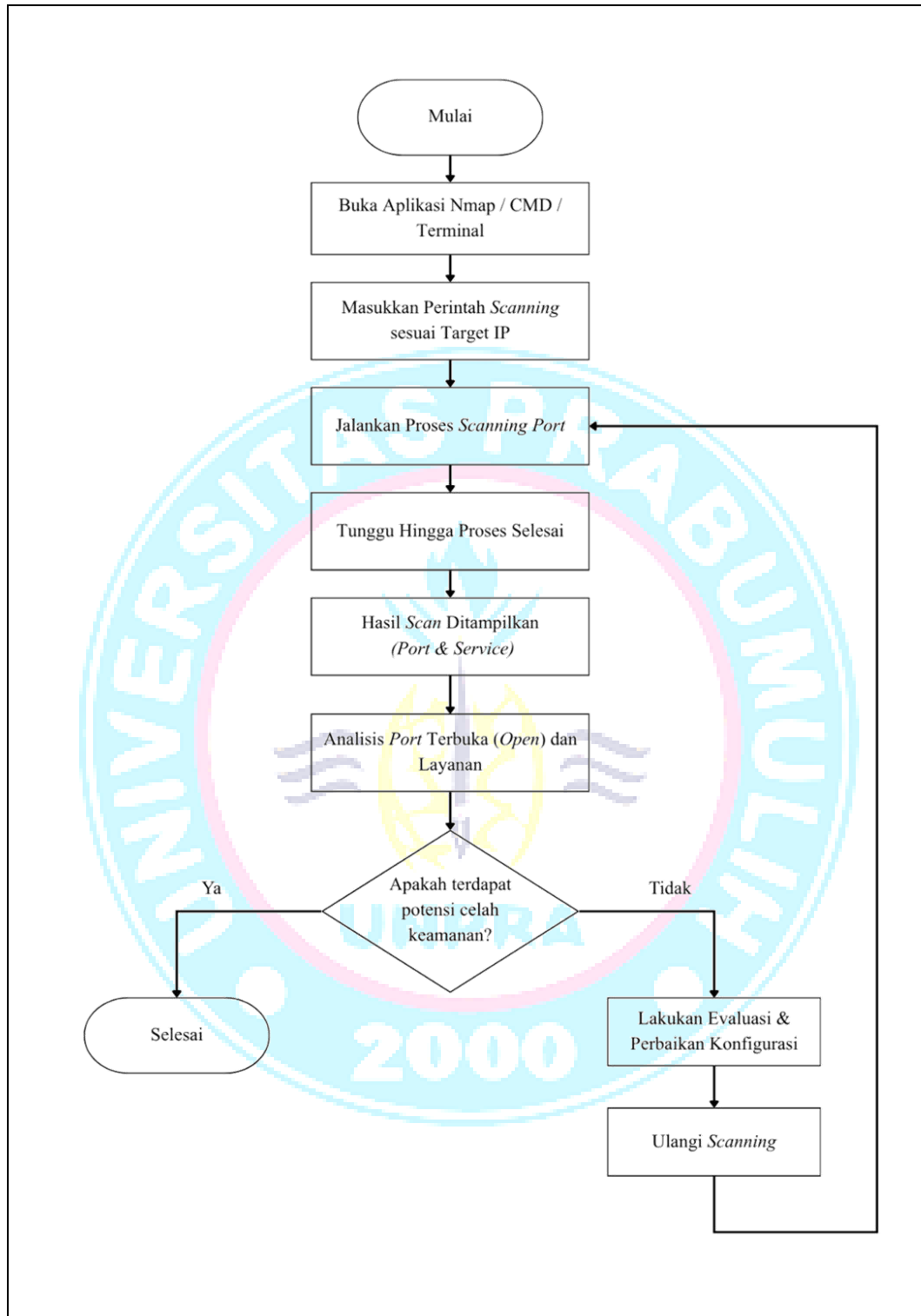
address yang spesifik (sebagai contoh: 192.168.10.1 hingga 192.168.10.254) dan menekan tombol *start* untuk memulai pencarian otomatis.

Selama proses berlangsung, aplikasi akan melakukan pemindaian secara menyeluruh pada rentang jaringan tersebut. Hasil dari pemindaian kemudian akan ditampilkan dalam bentuk daftar, di mana IP *address* yang berstatus aktif atau terdeteksi akan muncul secara otomatis. Tahap ini memungkinkan administrator untuk mengidentifikasi perangkat apa saja yang sedang terhubung ke dalam ekosistem jaringan sekolah pada saat itu.

Alur ini juga menyertakan sebuah titik keputusan untuk mengevaluasi apakah daftar IP *address* yang terdeteksi sudah sesuai dengan kebijakan penggunaan jaringan yang telah ditetapkan. Jika ditemukan adanya alamat IP yang tidak dikenal atau tidak sesuai dengan aturan, sistem menginstruksikan untuk melakukan pemindaian ulang (ulangi *scanning*) guna memastikan akurasi data. Apabila hasil pemindaian dinyatakan telah selaras dengan kebijakan, maka seluruh rangkaian proses audit alamat IP ini dianggap berhasil dan dinyatakan selesai.



9. Flowchart Pengujian Nmap



Sumber: Penulis, 2026

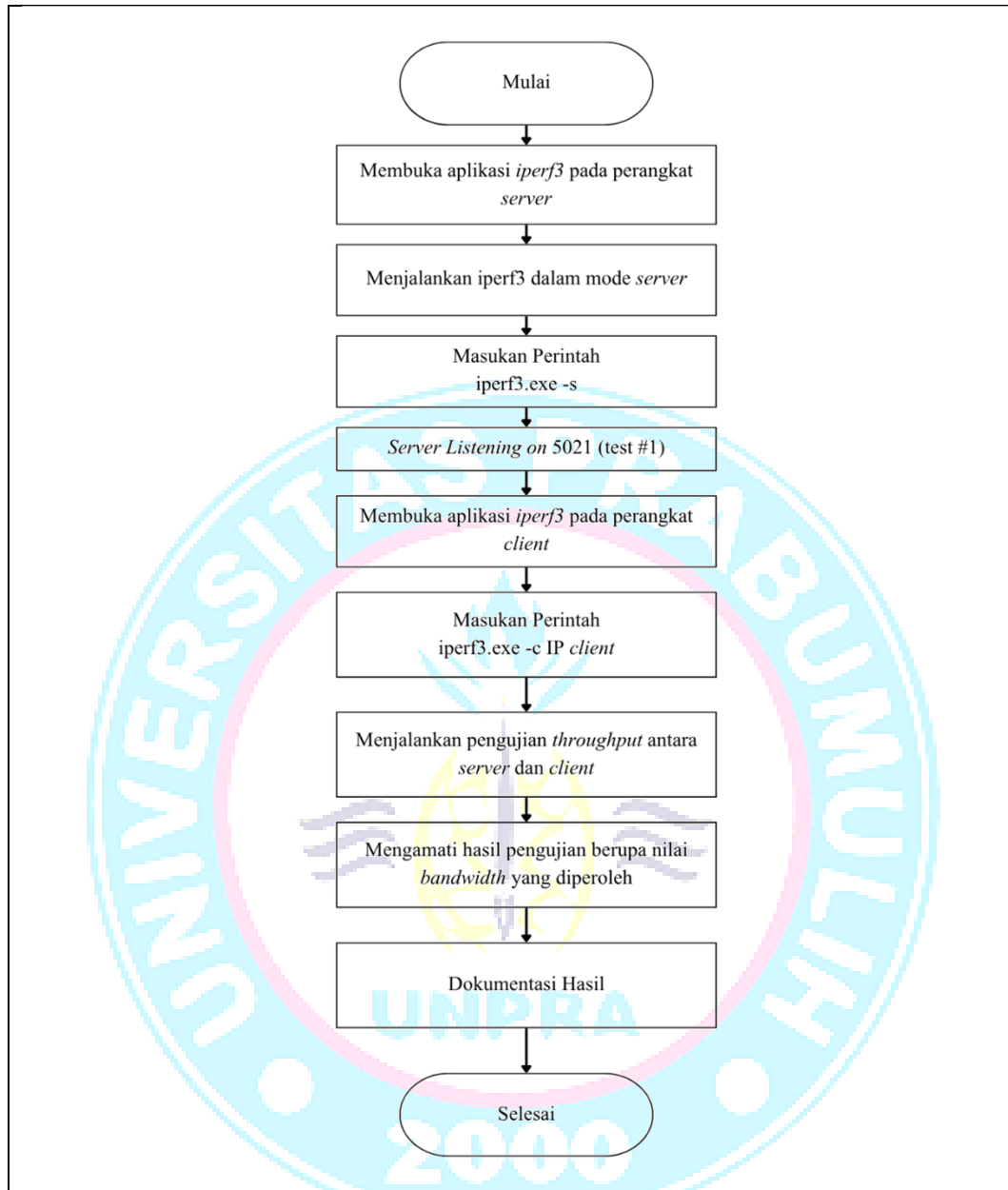
Gambar 4.14 Alur Pengujian Nmap

Flowchart pada gambar tersebut menggambarkan alur proses pengujian keamanan jaringan melalui teknik *port scanning* menggunakan aplikasi nmap, *command prompt*, atau Terminal secara sistematis. Proses diawali dengan membuka salah satu aplikasi tersebut, yang kemudian dilanjutkan dengan memasukkan perintah *scanning* spesifik sesuai dengan alamat IP target yang ingin diaudit. Setelah perintah dimasukkan, administrator menjalankan proses *scanning port* dan menunggu hingga sistem menyelesaikan pemindaian seluruh layanan yang aktif.

Langkah teknis selanjutnya adalah pengamatan terhadap hasil *scan* yang ditampilkan, yang mencakup informasi mengenai nomor *port* serta jenis *service* (layanan) yang sedang berjalan. Hasil tersebut kemudian dianalisis secara mendalam untuk mengidentifikasi mana saja *port* yang terbuka dan layanan apa yang menyertainya. Tahap analisis ini sangat krusial guna memetakan potensi titik masuk dalam infrastruktur jaringan.

Alur ini juga menyertakan sebuah titik keputusan untuk mengevaluasi apakah dari hasil analisis tersebut ditemukan potensi celah keamanan. Jika sistem mendeteksi adanya kerentanan (pilihan "tidak" pada logika keamanan yang diharapkan), maka instruksi selanjutnya adalah melakukan evaluasi dan perbaikan konfigurasi pada perangkat jaringan, yang kemudian diikuti dengan pengulangan proses *scanning* untuk memastikan perbaikan telah efektif. Apabila kondisi keamanan telah dinilai memadai dan potensi celah telah teratasi (pilihan "ya"), maka seluruh rangkaian proses audit keamanan *port* ini dinyatakan selesai.

10. Flowchart Pengujian Iperf3



Sumber: Penulis, 2026

Gambar 4.15 Alur Pengujian Iperf3

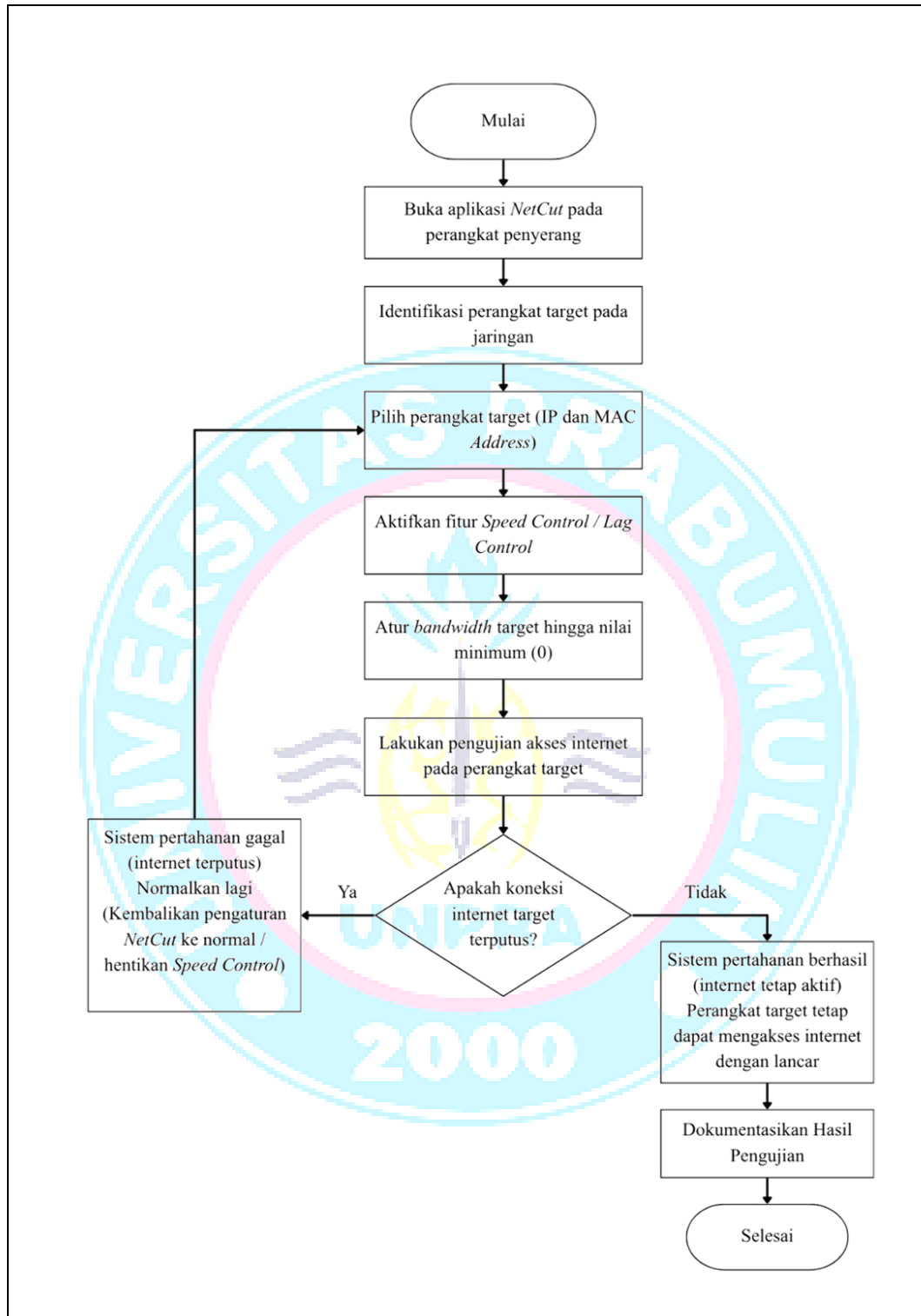
Flowchart pada gambar tersebut menggambarkan alur proses pengujian performa jaringan menggunakan aplikasi iperf3 untuk mengukur nilai *throughput* antara perangkat *server* dan *client*. Proses dimulai dengan membuka aplikasi iperf3 pada perangkat *server*. Aplikasi kemudian dijalankan dalam mode *server* dengan memasukkan perintah iperf3.exe -s. Setelah perintah dijalankan, *server* berada pada kondisi *listening* dan siap menerima koneksi pengujian dari perangkat *client*.

Pengujian dilanjutkan dengan membuka aplikasi iperf3 pada perangkat *client*. Pada perangkat *client*, pengguna memasukkan perintah iperf3.exe -c IP *client* untuk menghubungkan *client* ke *server* yang telah aktif.

Perintah tersebut digunakan untuk menjalankan pengujian *throughput* antara *server* dan *client*. Selama proses pengujian berlangsung, aplikasi iperf3 mengirim dan menerima data guna mengukur performa jaringan yang sedang diuji. Hasil pengujian kemudian diamati dengan melihat nilai *bandwidth* yang ditampilkan oleh aplikasi iperf3. Nilai tersebut digunakan sebagai data untuk mengetahui kemampuan *transfer* data pada jaringan yang diuji. Informasi dan hasil pengujian yang diperoleh selanjutnya didokumentasikan sebagai data pengujian. Setelah proses dokumentasi selesai dilakukan, pengujian performa jaringan menggunakan iperf3 dinyatakan selesai.



11. Flowchart Pengujian *NetCut*



Sumber: Penulis, 2026

Gambar 4.16 Alur Pengujian *NetCut*

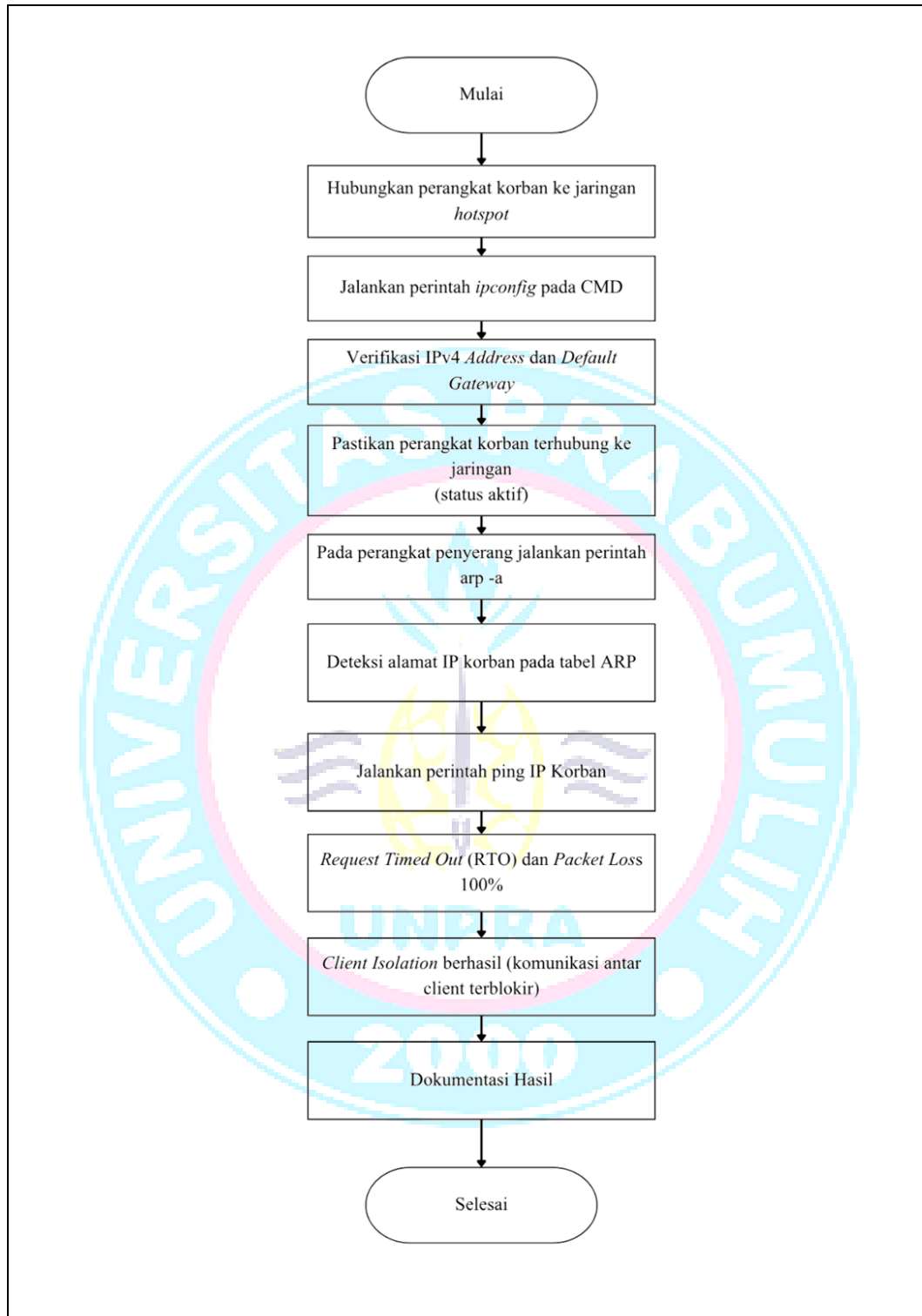
Flowchart pada gambar tersebut menggambarkan alur proses pengujian ketahanan jaringan terhadap serangan pemutusan koneksi menggunakan aplikasi *netcut* pada jaringan *hotspot*. Proses pengujian diawali dengan membuka aplikasi *netcut* pada perangkat penyerang, kemudian melakukan identifikasi perangkat target yang terhubung pada jaringan yang sama. Setelah perangkat target berhasil ditemukan berdasarkan alamat IP dan MAC *address*, penguji memilih perangkat tersebut sebagai sasaran pengujian.

Tahap berikutnya adalah mengaktifkan fitur *speed control* atau *lag control* yang tersedia pada aplikasi *netcut*. Selanjutnya, parameter *bandwidth* target diatur hingga mencapai nilai minimum dengan tujuan mensimulasikan upaya pemutusan koneksi internet pada perangkat korban. Setelah konfigurasi serangan diterapkan, dilakukan pengujian akses internet pada perangkat target untuk mengetahui kondisi koneksi jaringan selama proses pengujian berlangsung.

Proses pengujian ini dilengkapi dengan titik keputusan untuk mengevaluasi apakah koneksi internet pada perangkat target berhasil diputus atau tidak. Apabila koneksi internet target terputus, maka dilakukan proses normalisasi dengan mengembalikan konfigurasi *netcut* ke kondisi semula atau menonaktifkan fitur *speed control*. Setelah proses normalisasi dilakukan, pengujian dapat diulangi kembali dari tahap pemilihan perangkat target.

Apabila perangkat target masih dapat mengakses internet selama proses pengujian berlangsung, maka tahapan pengujian dilanjutkan ke proses dokumentasi hasil pengujian. Seluruh hasil pengamatan kemudian dicatat sebagai bagian dari proses evaluasi keamanan jaringan. Dengan demikian, rangkaian pengujian menggunakan aplikasi *netcut* dinyatakan selesai.

12. Flowchart Pengujian *Command Prompt* (Cek arp -a)



Sumber: Penulis, 2026

Gambar 4.17 Alur Pengujian *Command Prompt* (Cek arp -a)

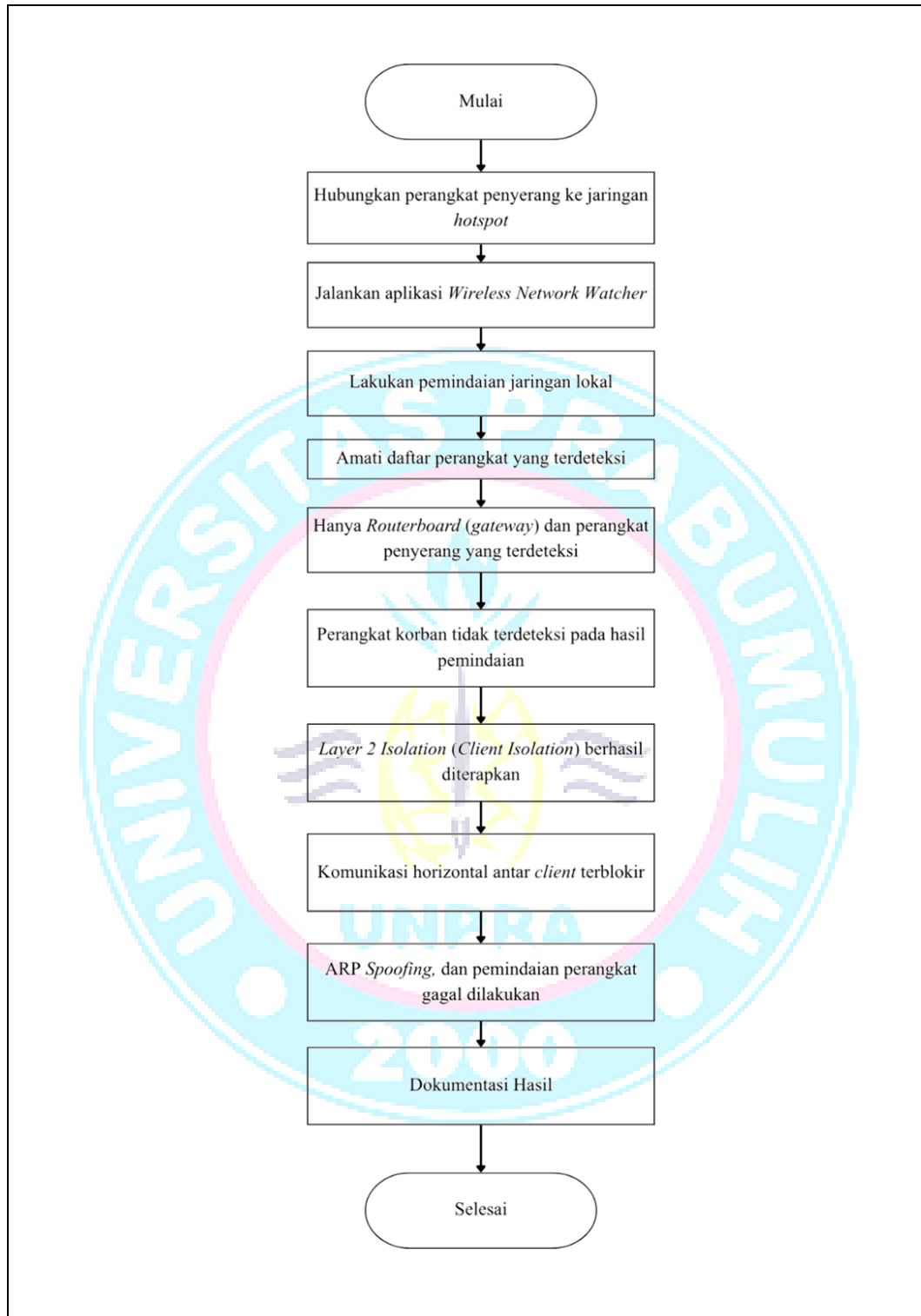
Flowchart pada gambar tersebut menggambarkan alur proses pengujian keamanan jaringan untuk memverifikasi efektivitas fitur *client isolation* dalam mencegah komunikasi langsung antar perangkat yang terhubung pada jaringan *hotspot* yang sama. Proses pengujian dimulai dengan menghubungkan perangkat korban ke jaringan *hotspot*, kemudian dilakukan pemeriksaan konfigurasi jaringan menggunakan *command prompt* melalui perintah *ipconfig*. Perintah ini digunakan untuk memperoleh informasi alamat IPv4 dan *default gateway* yang diberikan oleh *server* DHCP.

Setelah memastikan perangkat korban terhubung ke jaringan, pengujian dilanjutkan dari sisi perangkat penyerang. Pada tahap ini, penyerang menjalankan perintah *arp -a* untuk menampilkan tabel *address resolution protocol* (ARP) yang berisi daftar alamat IP dan MAC *address* yang terdeteksi pada jaringan lokal. Melalui informasi tersebut, penyerang berupaya mengidentifikasi keberadaan perangkat korban pada jaringan yang sama.

Tahap berikutnya dilakukan dengan mengirimkan paket ICMP *echo request* menggunakan perintah *ping* menuju alamat IP perangkat korban. Pengujian ini bertujuan untuk mengetahui apakah komunikasi horizontal antar pengguna *hotspot* masih dapat dilakukan serta untuk mengevaluasi efektivitas mekanisme *client isolation* yang diterapkan pada jaringan.

Hasil pengujian diamati melalui respons yang diterima dari perangkat target. Tahapan ini digunakan untuk menilai apakah perangkat penyerang dapat berkomunikasi secara langsung dengan perangkat korban yang berada pada segmen jaringan yang sama. Proses pengujian dilakukan sebagai bagian dari validasi keamanan jaringan terhadap potensi komunikasi antar klien yang tidak diinginkan. Setelah seluruh tahapan pengujian selesai dilakukan, hasil pengujian didokumentasikan sebagai bagian dari proses evaluasi keamanan jaringan. Dengan demikian, proses pengujian keamanan jaringan menggunakan perintah *ipconfig*, *arp -a*, dan *ping* dinyatakan selesai.

13. Flowchart Pengujian *Wireless Network Watcher*



Sumber: Penulis, 2026

Gambar 4.18 Alur Pengujian *Wireless Network Watcher*

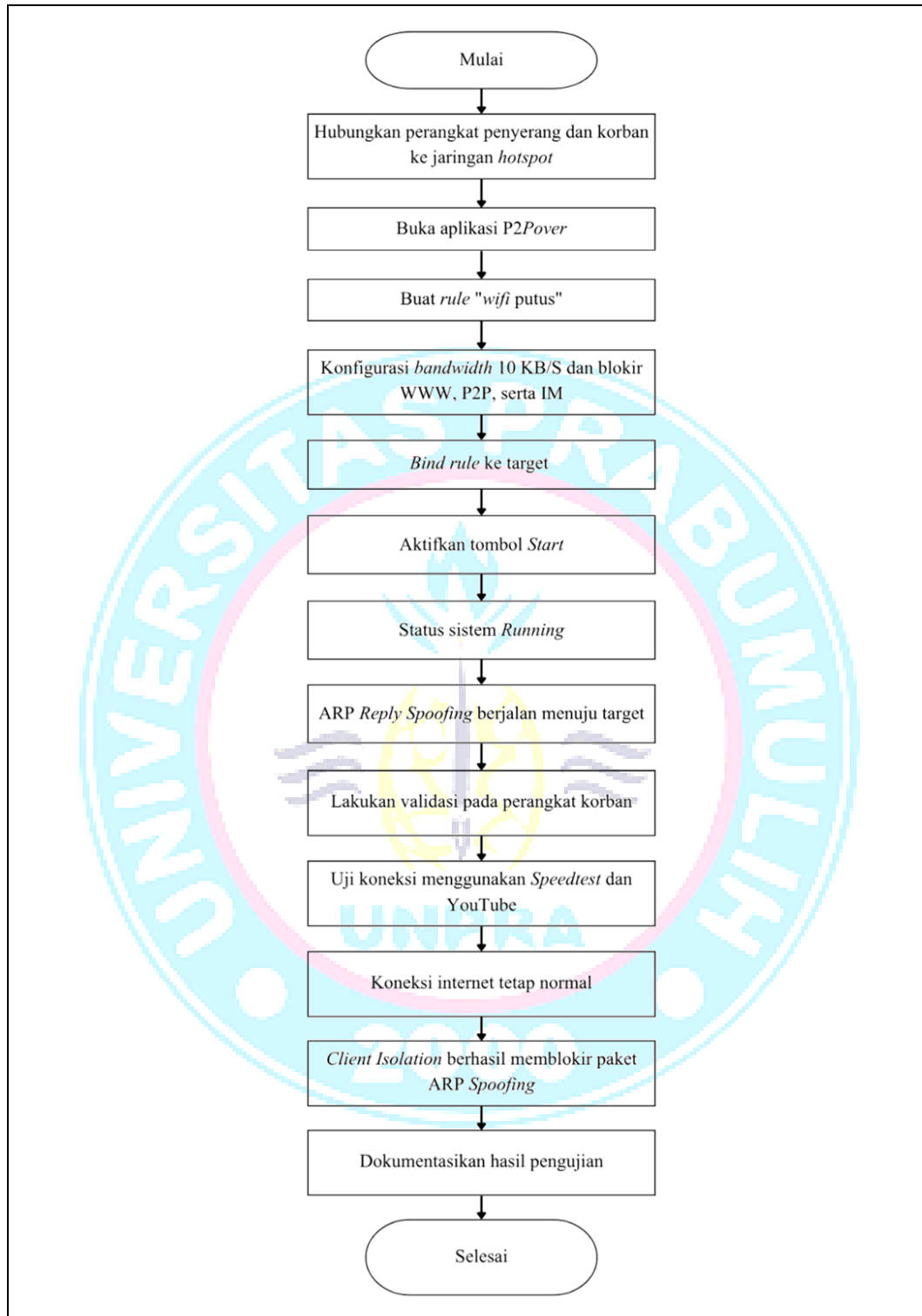
Flowchart pada gambar tersebut menggambarkan alur proses pengujian keamanan jaringan menggunakan aplikasi *wireless network watcher* untuk memverifikasi efektivitas penerapan fitur *client isolation* pada jaringan *hotspot*. Proses pengujian diawali dengan menghubungkan perangkat penyerang ke jaringan *hotspot* yang menjadi objek pengujian. Setelah perangkat berhasil terhubung ke jaringan, penguji menjalankan aplikasi *wireless network watcher* sebagai alat pemindai jaringan untuk mengidentifikasi perangkat-perangkat yang aktif pada segmen jaringan lokal.

Tahap selanjutnya dilakukan dengan menjalankan proses pemindaian jaringan lokal menggunakan aplikasi tersebut. Hasil pemindaian kemudian diamati untuk mengetahui daftar perangkat yang berhasil terdeteksi oleh sistem. Penguji selanjutnya melakukan pemeriksaan terhadap perangkat-perangkat yang muncul pada hasil pemindaian untuk melihat apakah perangkat lain yang berada pada jaringan yang sama dapat terdeteksi oleh aplikasi.

Proses pengujian ini bertujuan untuk mengevaluasi tingkat visibilitas antar perangkat dalam jaringan *hotspot* serta mengamati efektivitas mekanisme *layer 2 isolation* atau *client isolation* yang diterapkan pada *access point*. Melalui tahapan ini, penguji dapat mengetahui apakah perangkat yang terhubung ke jaringan masih dapat saling mendeteksi dan melakukan pemetaan informasi dasar jaringan.

Pengujian juga digunakan untuk menilai potensi terjadinya komunikasi horizontal antar klien yang dapat dimanfaatkan sebagai langkah awal berbagai aktivitas pemindaian dan pengumpulan informasi jaringan. Seluruh tahapan pengujian dilakukan menggunakan aplikasi *wireless network watcher* sebagai alat bantu untuk melakukan identifikasi perangkat yang berada pada jaringan lokal. Setelah seluruh tahapan pengujian selesai dilakukan, hasil pengujian didokumentasikan sebagai bagian dari proses evaluasi keamanan jaringan. Dengan demikian, proses pengujian menggunakan aplikasi *wireless network watcher* dinyatakan selesai.

14. Flowchart Pengujian P2Pover



Sumber: Penulis, 2026

Gambar 4.19 Alur Pengujian P2Pover

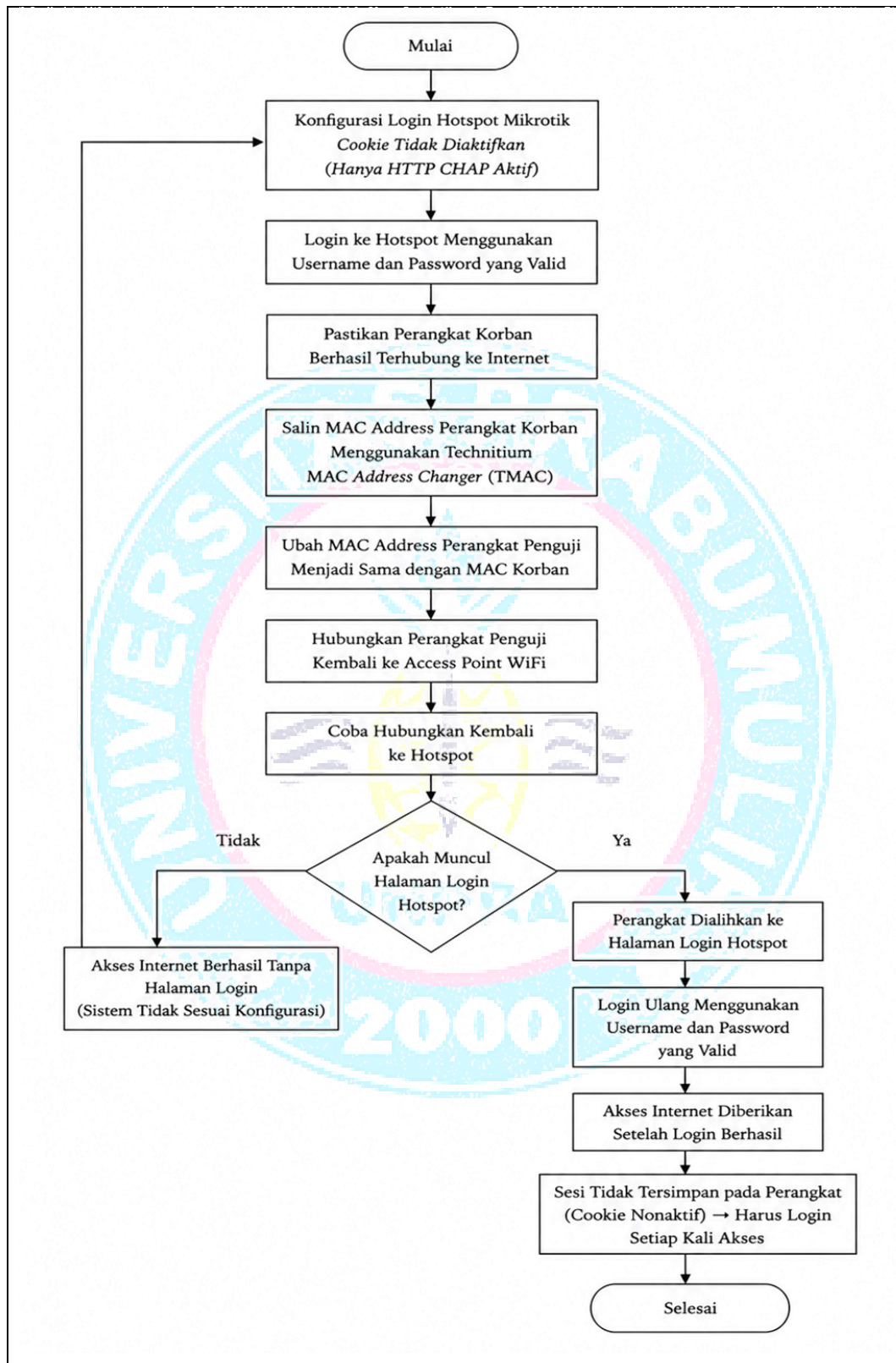
Flowchart pada gambar tersebut menggambarkan alur proses pengujian keamanan jaringan menggunakan aplikasi *P2Pover*. Proses pengujian diawali dengan menghubungkan perangkat penyerang dan perangkat korban ke jaringan *hotspot* yang sama. Setelah kedua perangkat terhubung, aplikasi *P2Pover* dijalankan pada perangkat penyerang untuk melakukan simulasi serangan terhadap perangkat target.

Tahap berikutnya adalah membuat sebuah aturan (*rule*) bernama *wifi* putus yang digunakan sebagai parameter pengujian. *Rule* tersebut kemudian dikonfigurasi dengan pembatasan *bandwidth* serta pemblokiran beberapa layanan jaringan. Setelah konfigurasi selesai, *rule* diikatkan (*bind*) ke perangkat target berdasarkan alamat IP yang telah ditentukan.

Selanjutnya, penguji mengaktifkan tombol *start* sehingga sistem masuk ke kondisi *Running*. Pada tahap ini, aplikasi mulai menjalankan proses *ARP reply spoofing* yang diarahkan ke perangkat target. Setelah serangan dijalankan, dilakukan validasi pada perangkat korban untuk mengetahui pengaruh serangan terhadap koneksi jaringan yang digunakan.

Proses validasi dilakukan dengan melakukan pengujian koneksi internet menggunakan aplikasi *speedtest* serta mengakses layanan youtube. Tahapan ini bertujuan untuk mengevaluasi kondisi koneksi jaringan pada perangkat korban selama proses pengujian berlangsung. Setelah seluruh tahapan pengujian selesai dilakukan, hasil pengujian didokumentasikan sebagai bagian dari proses evaluasi keamanan jaringan sebelum pengujian dinyatakan selesai.

15. Flowchart Pengujian TMAC



Sumber: Penulis, 2026

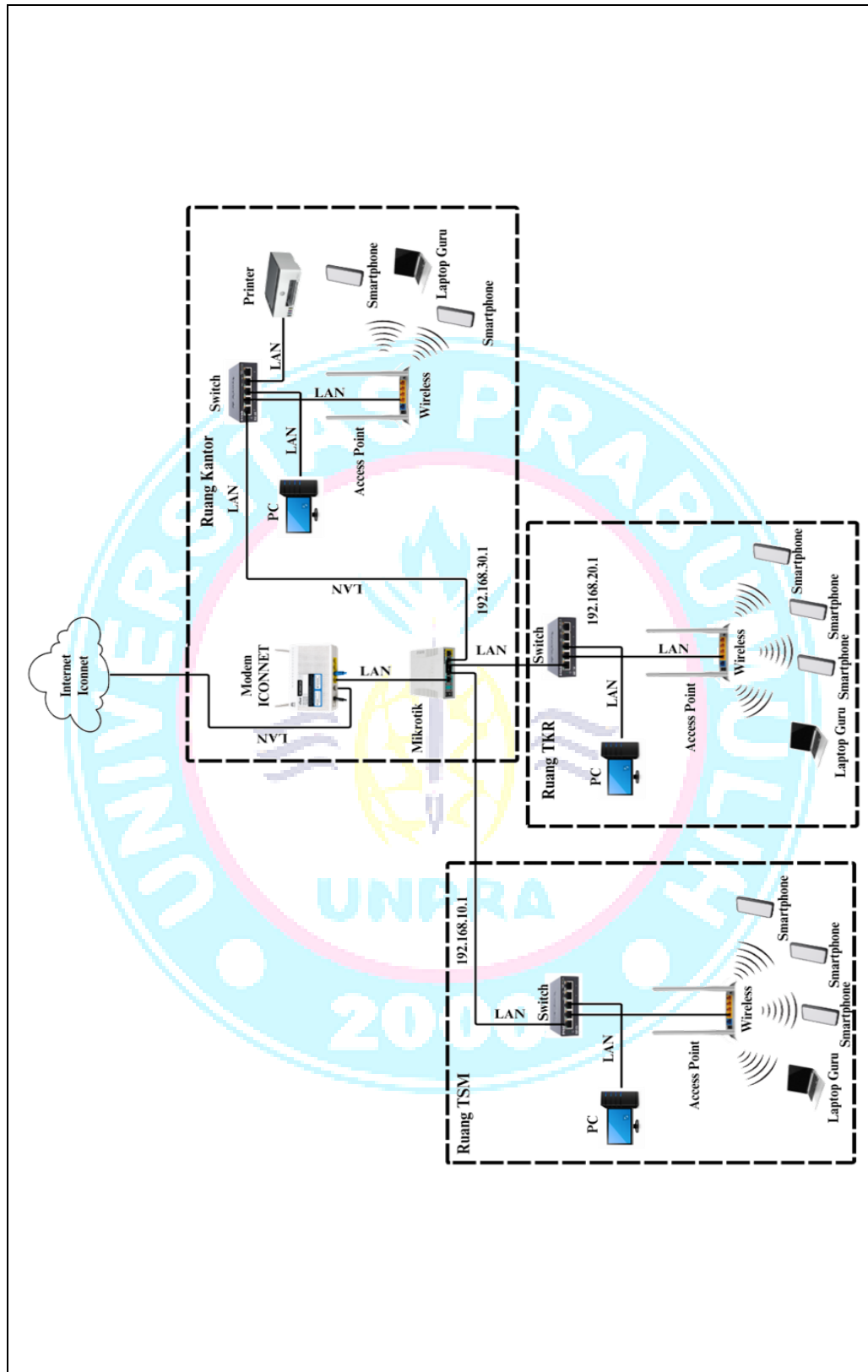
Gambar 4.20 Alur Pengujian TMAC

Flowchart pada gambar tersebut menggambarkan alur pengujian keamanan jaringan menggunakan aplikasi *Technitium MAC Address Changer* (TMAC) setelah fitur *cookie* pada *hotspot* mikrotik dinonaktifkan. Pengujian diawali dengan mengonfigurasi *hotspot* agar hanya menggunakan metode autentikasi HTTP CHAP. Perangkat korban melakukan *login* menggunakan *username* dan *password* yang valid hingga berhasil terhubung ke internet.

Penguji menyalin *MAC address* perangkat korban menggunakan aplikasi TMAC, kemudian mengubah *MAC address* perangkat penguji menjadi sama dengan *MAC address* perangkat korban. Perangkat penguji mencoba menghubungkan kembali ke jaringan *hotspot* menggunakan identitas *MAC address* tersebut.

Proses pengujian dilanjutkan dengan mengamati apakah perangkat diarahkan ke halaman *login hotspot*. Apabila halaman *login* muncul, pengguna harus melakukan autentikasi ulang menggunakan *username* dan *password* yang valid sebelum memperoleh akses internet. Sebaliknya, apabila perangkat langsung memperoleh akses internet tanpa *login*, konfigurasi *hotspot* belum berjalan sesuai dengan yang diharapkan sehingga perlu dilakukan konfigurasi ulang. Hasil pengujian digunakan untuk mengevaluasi bahwa menonaktifkan fitur *cookie* mampu mencegah penyalahgunaan sesi *login* melalui teknik *MAC address spoofing*, sehingga proses pengujian dinyatakan selesai.

16. Network Diagram



Sumber: Penulis, 2026

Gambar 4.21 Network Diagram

Network diagram pada gambar tersebut menggambarkan rancangan topologi jaringan yang digunakan untuk menghubungkan seluruh perangkat pada beberapa ruangan di lingkungan sekolah secara terstruktur dan sistematis. Diagram dimulai dari koneksi internet yang berasal dari layanan *ICONNET*, kemudian diteruskan menuju modem sebagai perangkat penerima jaringan dari penyedia layanan internet. Setelah itu, koneksi jaringan diteruskan ke perangkat mikrotik yang berfungsi sebagai pusat pengaturan lalu lintas jaringan, manajemen IP address, serta penghubung antar jaringan pada setiap ruangan.

Dari mikrotik, jaringan kemudian didistribusikan menuju beberapa *switch* yang berada pada ruang kantor, ruang TSM, dan ruang TKR melalui koneksi LAN. Masing-masing *switch* berfungsi untuk membagi koneksi jaringan ke berbagai perangkat yang ada di setiap ruangan, seperti komputer (PC), *printer*, dan *access point*. *Access point* yang terhubung ke *switch* digunakan untuk menyediakan koneksi *wireless* sehingga perangkat seperti *smartphone* dan laptop guru dapat terhubung ke jaringan tanpa menggunakan kabel.

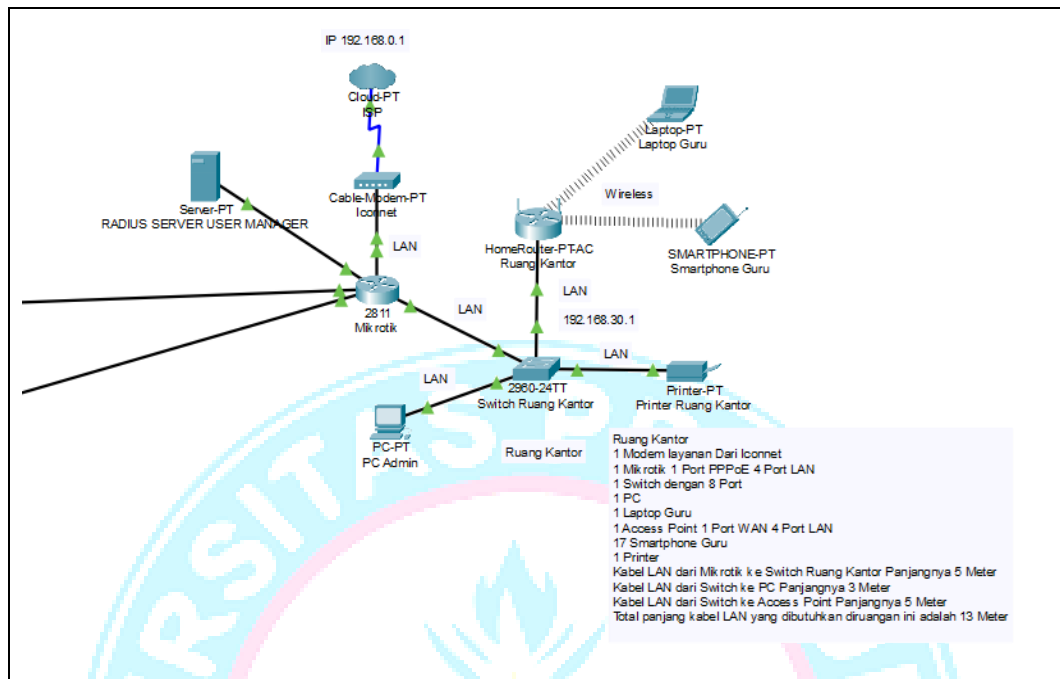
Pada *network diagram* tersebut juga terlihat adanya pembagian segmentasi IP *address* pada setiap ruangan, seperti jaringan 192.168.10.1 pada ruang TSM, 192.168.20.1 pada ruang TKR, dan 192.168.30.1 pada ruang kantor. Pembagian IP ini bertujuan untuk mempermudah pengelolaan jaringan, meningkatkan keamanan, serta meminimalkan terjadinya gangguan komunikasi data antar perangkat.

Selain menunjukkan jalur koneksi jaringan, diagram ini juga menggambarkan hubungan antara perangkat jaringan kabel (LAN) dan jaringan nirkabel (*wireless*) yang saling terintegrasi dalam satu sistem jaringan sekolah. Dengan adanya topologi jaringan ini, proses distribusi internet, komunikasi data, serta pengelolaan perangkat jaringan pada masing-masing ruangan dapat berjalan dengan lebih efektif, stabil, dan terorganisir sesuai kebutuhan infrastruktur jaringan sekolah.

Network diagram ini juga digunakan sebagai dokumentasi dan panduan dalam proses instalasi maupun pemeliharaan jaringan komputer. Melalui *diagram* tersebut, teknisi jaringan dapat mengetahui alur jalur kabel jaringan dari perangkat satu ke perangkat lainnya, mengetahui koneksi kabel terhubung ke port mana saja pada mikrotik, *switch*, maupun *access point*.

4.2.4 Perancangan Konfigurasi Jaringan

1. Wilayah Ruang Kantor



Sumber: Penulis, 2026

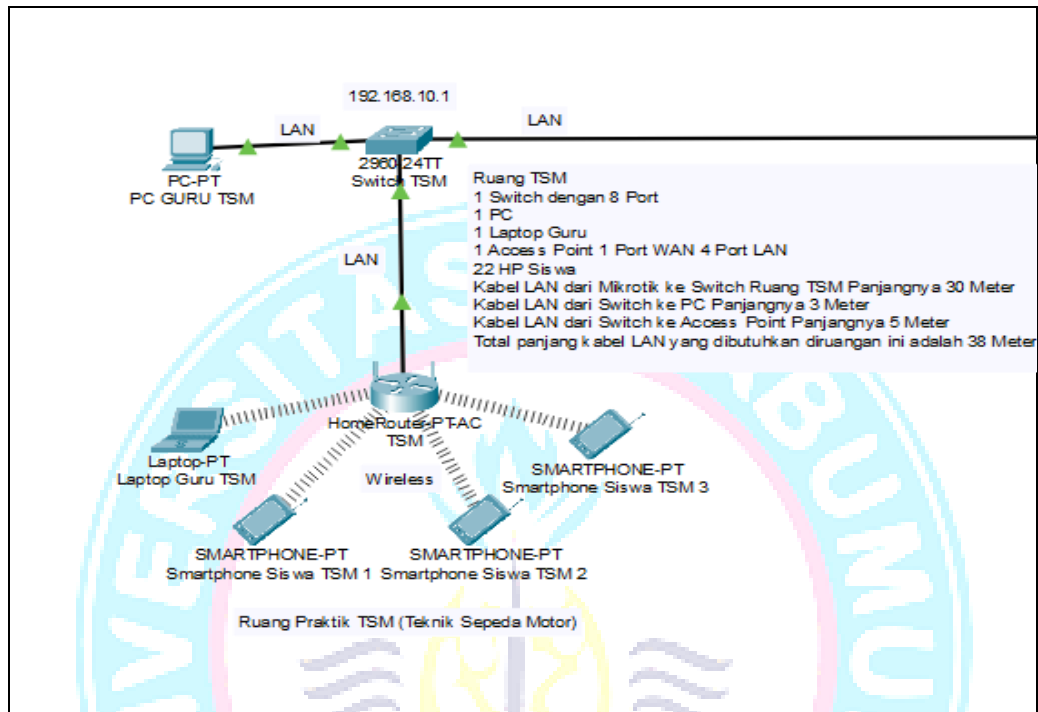
Gambar 4.22 Wilayah Ruang Kantor

Berdasarkan rancangan topologi di atas, infrastruktur jaringan pada wilayah ruang kantor diawali dengan penggunaan *cable modem iconnet* yang berfungsi sebagai gerbang utama (*gateway*) untuk menerima pasokan layanan internet dari penyedia jasa (ISP). Dari titik ini, koneksi dialirkan menuju *router* mikrotik 2811 yang bertindak sebagai pusat kendali untuk mengatur manajemen lalu lintas data serta kebijakan keamanan. Perangkat *router* ini juga terhubung secara terintegrasi dengan (*user manager*) yang bertugas khusus untuk memproses autentikasi pengguna.

Setelah diproses oleh *router*, akses jaringan diteruskan menuju *switch* ruang kantor (2960-24TT) yang berperan sebagai pusat distribusi kabel ke berbagai perangkat operasional di area tersebut. Melalui *switch* ini, sinyal internet diarahkan langsung ke perangkat terminal seperti PC admin untuk kebutuhan administratif dan *printer* agar dapat digunakan secara bersama-sama dalam satu jaringan lokal. Selain koneksi fisik, jalur distribusi juga mengarah ke *access point* (*homerouter-PT-AC*) yang memancarkan sinyal nirkabel di wilayah kantor. Hal ini

memungkinkan perangkat seperti *smartphone* dan laptop guru untuk terhubung ke dalam ekosistem jaringan sekolah secara efisien tanpa memerlukan kabel tambahan.

2. Wilayah Ruang Praktik TSM



Sumber: Penulis, 2026

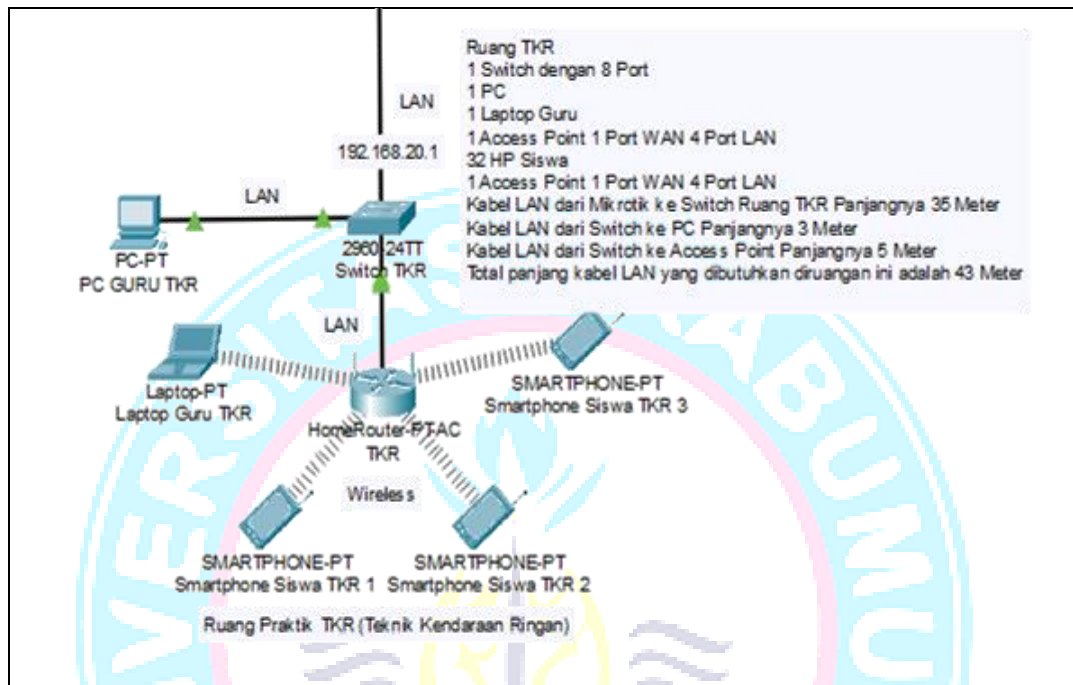
Gambar 4.23 Wilayah Ruang Praktik TSM

Berdasarkan rancangan topologi di atas, infrastruktur jaringan pada wilayah Ruang Praktik TSM (Teknik Sepeda Motor) dikonfigurasi sebagai area pelayanan akses nirkabel bagi siswa dan guru praktikan. Jalur distribusi data pada area ini dimulai dari switch TSM (2960-24TT) yang berfungsi sebagai titik penghubung kabel utama dari jaringan pusat sekolah menuju ruang praktik. Melalui *switch* ini, koneksi dialirkan secara fisik menggunakan kabel LAN menuju perangkat PC Guru TSM untuk mendukung kegiatan instruksional dan administrasi nilai di dalam ruangan.

Switch tersebut juga terhubung ke *access point* (*homerouter-PT-AC TSM*) yang berperan penting sebagai pemancar sinyal *wi-fi* khusus di wilayah praktik TSM. Perangkat ini berfungsi sebagai jembatan nirkabel agar perangkat seperti laptop dan *smartphone* Siswa dapat terhubung ke ekosistem jaringan sekolah secara

simultan. Dengan adanya infrastruktur ini, seluruh aktivitas digital di Ruang Praktik TSM dapat berjalan secara terintegrasi, baik untuk keperluan akses modul pembelajaran digital maupun koordinasi teknis selama praktik berlangsung.

3. Wilayah Ruang Praktik TKR



Sumber: Penulis, 2026

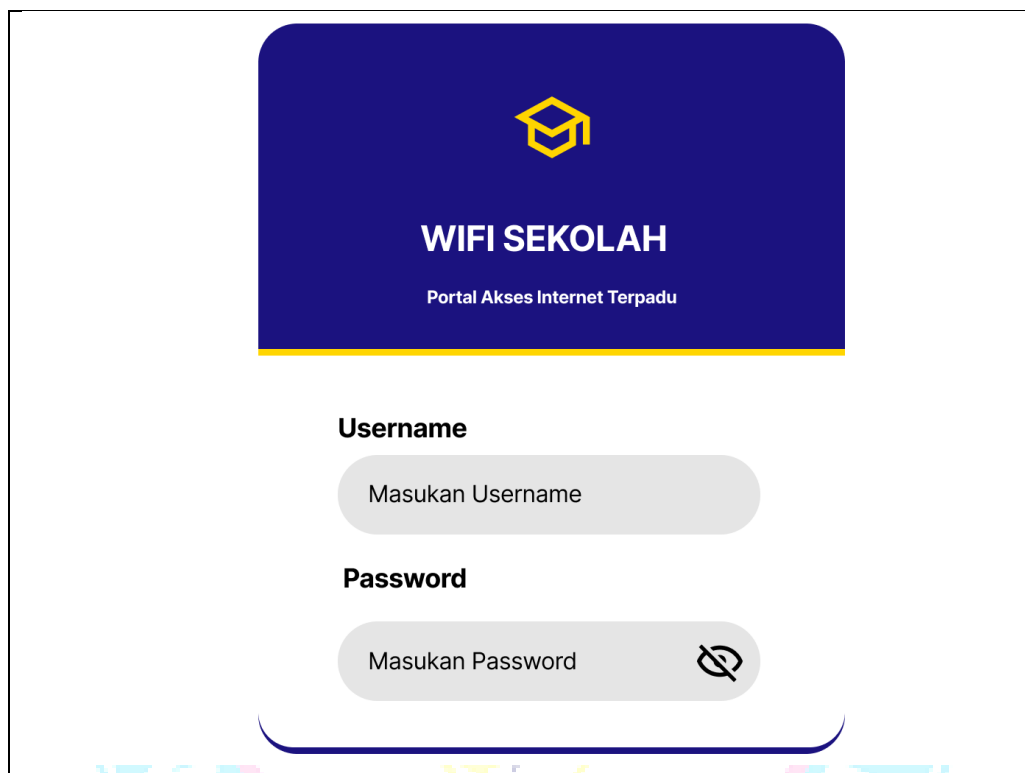
Gambar 4.24 Wilayah Ruang Praktik TKR

Berdasarkan rancangan topologi di atas, infrastruktur jaringan pada wilayah ruang praktik TKR (Teknik Kendaraan Ringan) dikonfigurasi untuk menyediakan akses internet terpadu bagi siswa dan tenaga pendidik di area bengkel. Jalur komunikasi data di wilayah ini bermuara pada *switch* TKR (2960-24TT) yang berfungsi sebagai titik distribusi utama kabel dari jaringan pusat sekolah. Melalui *switch* tersebut, koneksi dialirkan secara fisik menggunakan kabel LAN menuju PC guru TKR untuk mendukung keperluan administrasi praktik dan media pembelajaran di dalam ruangan.

Selain jalur kabel, *switch* ini juga terhubung ke perangkat *access point* (*homerouter-PT-AC* TKR) yang bertugas memancarkan sinyal *wi-fi* khusus di wilayah praktik TKR. Perangkat ini berperan sebagai jembatan nirkabel sehingga berbagai perangkat *mobile* seperti laptop dan *smartphone* siswa dapat terhubung ke

ekosistem digital sekolah tanpa hambatan kabel. Dengan struktur ini, seluruh kegiatan praktik yang membutuhkan akses informasi digital dapat berjalan secara efisien dan terorganisir di seluruh area ruang praktik TKR.

4. Form Login / Captive Portal



Sumber: Penulis, 2026

Gambar 4.25 Form Login Client

Halaman portal *login* ini merupakan antarmuka awal yang wajib dilalui oleh setiap pengguna saat ingin terhubung ke jaringan melalui *access point*. Sistem ini berfungsi sebagai gerbang keamanan digital yang mencegah akses ilegal dari pengguna yang tidak terdaftar. Setiap perangkat yang mencoba menangkap sinyal *wi-fi* akan secara otomatis diarahkan ke halaman ini untuk melakukan proses autentikasi sebelum diberikan izin akses internet penuh.

Proses masuk ke jaringan dilakukan dengan cara mengisi identitas resmi berupa *username* beserta kata sandi pada kolom yang telah tersedia. Data tersebut nantinya akan divalidasi langsung oleh *router* mikrotik menggunakan protokol keamanan tertentu guna memastikan kredensial pengguna tetap terlindungi.

Apabila data yang dimasukkan terbukti valid, sistem akan segera membuka blokir akses dan mengizinkan perangkat pengguna untuk mulai melakukan aktivitas penjelajahan di internet.

5. *Form Status Login Berhasil*

JARINGAN AKTIF
Selamat Belajar & Gunakan Internet dengan Bijak

achmad.sukri

Selamat Anda terhubung di jaringan Kantor

ID Sesi: 192.168.30.23

UPLOAD 130.4 Kib	DOWNLOAD 134.4 Kib
----------------------------	------------------------------

WAKTU AKTIF
41s

Alamat IP	192.168.30.23
Alamat MAC	20:16:D8:08:64:99
Penyegaran Status	1m

PUTUSKAN KONEKSI

Sumber: Penulis, 2026

Gambar 4.26 *Form Status Client*

Halaman status ini merupakan antarmuka informatif yang secara otomatis muncul pada layar perangkat pengguna setelah proses *login* dinyatakan berhasil oleh sistem mikrotik. Halaman ini berfungsi sebagai pusat informasi bagi pengguna dengan memberikan konfirmasi visual bahwa koneksi telah berada dalam kondisi "jaringan aktif". Selain itu, terdapat teks keterangan yang menunjukkan bahwa pengguna telah berhasil terhubung ke jaringan pada ruangan atau lokasi tertentu, sehingga pengguna dapat mengetahui dengan jelas jaringan yang sedang digunakan.

Melalui tampilan ini, pengguna dapat memantau informasi penggunaan internet secara *real-time*, yang mencakup jumlah data yang telah diunggah (*upload*), data yang telah diunduh (*download*), serta total durasi waktu aktif

(*uptime*) selama sesi berlangsung. Sistem juga menyajikan informasi teknis yang spesifik untuk setiap sesi, seperti identitas akun pengguna, ID sesi, alamat IP yang dialokasikan, dan alamat MAC perangkat yang terhubung.

Selain sebagai media informasi, halaman ini menyediakan fitur navigasi utama berupa tombol "putuskan koneksi" yang memungkinkan pengguna untuk mengakhiri sesi internet secara aman. Dengan adanya fitur tersebut, pengguna dapat memutuskan koneksi secara mandiri apabila telah selesai menggunakan jaringan sehingga sesi akses dapat ditutup dengan baik.

6. Konfigurasi IP Address

Tabel 4.1 IP Address

No	Interface	IP Address	Subnet Mask
1	FastEthernet 0/0	Public IP ISP	Menyesuaikan ISP
2	FastEthernet 0/1	192.168.10.1	255.255.255.0
3	FastEthernet 1/0	192.168.20.1	255.255.255.0
4	FastEthernet 1/1	192.168.30.1	255.255.255.0

Sumber: Penulis, 2026

Pengaturan alamat IP pada sistem ini berfungsi untuk membagi jalur komunikasi data berdasarkan area kerja yang telah ditentukan di lingkungan sekolah. Jalur utama yang menghubungkan seluruh jaringan ke internet melalui ISP atau modem dikonfigurasi pada interface *FastEthernet* 0/0 dengan *Public* IP ISP yang menyesuaikan konfigurasi dari penyedia layanan internet. Konfigurasi ini menjadi pintu masuk data dari luar jaringan menuju sistem kontrol pusat pada mikrotik.

Sistem ini menggunakan tiga segmen jaringan lokal yang berbeda untuk memisahkan lalu lintas data di setiap wilayah. Pada wilayah ruang praktik TSM, alamat 192.168.10.1 ditetapkan melalui interface *FastEthernet* 0/1 sebagai gerbang lokal (*gateway*) bagi para siswa. Sementara itu, untuk wilayah ruang praktik TKR, jalur komunikasi data diatur melalui interface *FastEthernet* 1/0 dengan alamat

192.168.20.1. Terakhir, wilayah Ruang Kantor memiliki jalur tersendiri pada interface *FastEthernet* 1/1 dengan alamat 192.168.30.1 guna mendukung kebutuhan administratif sekolah.

7. Konfigurasi DHCP

Tabel 4.2 DHCP

No	Ruangan	Pool Name	Range IP Address	DNS Server
1	TSM (Fa0/1)	pool-TSM	192.168.10.254	8.8.8.8
2	TKR (Fa1/0)	pool-TKR	192.168.20.254	8.8.8.8
3	Kantor (Fa1/1)	pool-Kantor	192.168.30.254	8.8.8.8

Sumber: Penulis, 2026

Berdasarkan rancangan tabel konfigurasi DHCP di atas, infrastruktur jaringan ini dilengkapi dengan sistem alokasi alamat IP otomatis untuk memudahkan setiap perangkat klien terhubung ke jaringan di masing-masing wilayah. Layanan DHCP ini berfungsi untuk memberikan alamat IP secara dinamis kepada perangkat pengguna tanpa perlu melakukan konfigurasi manual pada setiap laptop atau smartphone. Pada wilayah Ruang Praktik TSM, sistem menyediakan *pool-TSM* dengan rentang alamat mulai dari 192.168.10.2 hingga 192.168.10.254, sementara untuk Ruang Praktik TKR dialokasikan melalui *pool-TKR* dengan rentang 192.168.20.2 hingga 192.168.20.254.

Wilayah Ruang Kantor juga memiliki alokasi khusus melalui *pool-Kantor* dengan rentang alamat 192.168.30.2 hingga 192.168.30.254 guna mendukung operasional administrasi. Sesuai dengan pengaturan tersebut, setiap perangkat yang terhubung juga akan mendapatkan konfigurasi DNS *server* otomatis menggunakan alamat 8.8.8.8 agar proses penerjemahan nama domain internet berjalan dengan lancar.

8. Konfigurasi *User manager*

a. Tabel Guru

Tabel 4.3 Data Guru

No	Nama Lengkap	<i>Username</i>	<i>Password</i>
1	Achmad Sukri, S.Pd., M.Si	achmad.sukri	Achmad@12
2	Erwansah Bustomi, B.I	erwansah.bustomi	Erwansah@23
3	Febsa Zumel, S.E	febsa.zumel	Febsa@34
4	Selvi Puranda, S.Kom	selvi.puranda	Selvi@45
5	Henny Purwati, S.Pd	henny.purwati	Henny@56
6	Indri Susanti, S.Pd	indri.susanti	Indri@67
7	Tri Muhti Haryani, M.Pd	tri.muhti	Tri@78
8	Arlina Yanna Indah, S.T	arlina.yanna	Arlina@89
9	Dedi Saputra, S.Pd	dedi.saputra	Dedi@21
10	Dr. Lutfi, S.Ag., MM	dr.lutfi	Lutfi@32
11	Ryan Aziz, S.Pd	ryan.aziz	Ryan@43
12	Andri Hermawan, S.P, M.Si	andri.hermawan	Andri@54
13	Saddam Muslim, S.ST	saddam.muslim	Saddam@65
14	Harry Sunarya, S.T	harry.sunarya	Harry@76
15	Rahmi Widia Pratiwi, S.T	rahmi.widia	Rahmi@87
16	Finilia, S.Pd	finilia	Finilia@98
17	Dita Ratna Sari, S.Pd	dita.ratna	Dita@11

Sumber: Penulis, 2026

Berdasarkan tabel data di atas, sistem manajemen pengguna pada jaringan ini dikelola menggunakan fitur *user manager* di mikrotik untuk mengorganisir akun-akun yang memiliki hak akses internet. Dalam tabel tersebut, terdapat daftar identitas tenaga pendidik yang berjumlah sebanyak 17 akun guru, di mana setiap akun telah dipersonalisasi dengan nama lengkap, *username*, serta kata sandi yang spesifik. Penentuan kredensial ini bertujuan untuk menjaga keamanan akses dan memudahkan administrator dalam melakukan pemantauan aktivitas penggunaan internet bagi setiap guru secara individu.

Sistem ini memastikan bahwa setiap akun guru memiliki kredensial yang unik untuk proses autentikasi pada halaman *captive portal*. Dengan adanya basis data yang terstruktur ini, *router* mikrotik dapat mengenali setiap pengguna yang masuk dan menerapkan kebijakan akses yang telah ditetapkan sebelumnya, baik dari segi durasi waktu aktif maupun batasan kecepatan *bandwidth*. Pengelolaan akun secara terpusat melalui tabel data guru ini memberikan efisiensi dalam administrasi jaringan sekolah, sehingga seluruh tenaga pendidik dapat terhubung ke ekosistem digital dengan prosedur yang aman dan terdata.

b. Tabel Siswa TSM

Tabel 4.4 Siswa TSM

No	Nama Lengkap	Username	Password
1	Agus Syahputra	agus.syahputra	Agus#771
2	Akbar Vinata	akbar.vinata	Akbar#552
3	Arya Prima	arya.prima	Arya#663
4	Bayu Arta Sena	bayu.sena	Sena#991
5	Firzaan Milzaki	firzaan	Firzaan#341
6	Gilang Saka Riyuda	gilang.saka	Gilang#778
7	Lita Agustina	lita.agustina	Lita#889
8	M. Falen Putra Pratama	falen.putra	Falen#550

9	M. Okta Nur Saputra	okta.saputra	Okta#662
10	Melandi Fratama Putra	melandi.putra	Melandi#101
11	Muhammad Bagas Damarian	bagas.damarian	Bagas#778
12	Muhammad Farel	farel	Farel#992
13	Nabila	nabila	Nabila#331
14	Obit Taudi Nando	obit.nando	Obit#775
15	Prima Desta	prima.desta	Prima#224
16	Rivano	rivano	Rivano#667
17	Yusni	yusni	Yusni#889

Sumber: Penulis, 2026

Berdasarkan tabel data di atas, sistem manajemen pengguna untuk wilayah ruang praktik juga dikelola melalui fitur *user manager* pada mikrotik. Dalam tabel tersebut, terdapat daftar akun khusus untuk Siswa TSM (Teknik Sepeda Motor) yang berjumlah sebanyak 17 akun, di mana setiap siswa memiliki identitas unik berupa nama lengkap, *username*, dan kata sandi masing-masing. Pengaturan akun secara individu ini bertujuan untuk memastikan keamanan akses serta memudahkan pihak sekolah dalam mengontrol durasi pemakaian internet selama kegiatan praktik berlangsung di bengkel TSM.

Sesuai dengan rancangan tersebut, setiap akun siswa akan melalui proses autentikasi pada halaman *captive portal* sebelum diizinkan terhubung ke jaringan *wi-fi*. Dengan adanya *database* 17 akun siswa TSM ini, *router* mikrotik dapat menerapkan kebijakan pembatasan *bandwidth* yang berbeda dari akun guru, sehingga distribusi kecepatan internet di lingkungan sekolah tetap terjaga dan adil. Manajemen akun ini juga berfungsi sebagai sistem absensi digital sederhana untuk melihat siapa saja siswa yang aktif menggunakan fasilitas internet saat jam pelajaran praktik.

c. Tabel Siswa TKR

Tabel 4.5 Siswa TKR

No	Nama Lengkap	Username	Password
1	Adi Ariski	adi.ariski	Adi#725
2	Adil Pratama	adil.pratama	Adil#832
3	Al Juansyah	al.juansyah	Juansyah#91
4	Aldi Alfian	aldi.alfian	Aldi#771
5	Almutede Ansyah	almutede	Ansyah#552
6	Alzar Daven Rizki	alzar.rizki	Daven#660
7	Andes Ramadhan	andes.ramadhan	Andes#883
8	Angga Saputra	angga.saputra	Angga#992
9	April Ramza	april.ramza	April#445
10	Arjuna Raga Pratama	arjuna.raga	Arjuna#318
11	Awansyah	awansyah	Awan#721
12	Bayu Anggara	bayu.anggara	Bayu#547
13	Denis	denis	Denis#234
14	Dika Pernandes	dika.pernandes	Dika#845
15	Diki Candra	diki.candra	Diki#392
16	El Abib Anandi	el.abib	Abib#657
17	Hози	hozi	Hози#908
18	Marsel Saputra	marsel.saputra	Marsel#110
19	Muhammad Iqbal Fahriansyah	iqbal.fahri	Iqbal#776
20	Muhammad Rafli	rafli	Rafli#664

21	Nando Perdana	nando.perdana	Nando#225
22	Nauval Irwansyah	nauval.irwan	Nauval#889
23	Paril Adiya	paril.adiya	Paril#340
24	Pedro Jeri Handaka	pedro.jeri	Pedro#671
25	Radev Priyanka	radev	Radev#553
26	Raya Andaka	raya.andaka	Raya#118
27	Restu Singgi	restu.singgi	Restu#777
28	Rudi Ansah	rudi.ansah	Rudi#292
29	Taufik Hidayat	taufik.hidayat	Taufik#901
30	Yayan Sanjaya	yayan.sanjaya	Yayan#643
31	Yolan Saputra	yolan.saputra	Yolan#778
32	Zaki Tri Prasetyo	zaki.prasetyo	Zaki#516

Sumber: Penulis, 2026

Berdasarkan tabel data di atas, sistem manajemen pengguna pada wilayah ruang praktik juga dikelola melalui fitur *user manager* pada mikrotik. Dalam tabel tersebut, terdapat daftar akun khusus untuk siswa TKR (Teknik Kendaraan Ringan) yang berjumlah sebanyak 32 akun, di mana setiap siswa memiliki identitas unik berupa nama lengkap, *username*, dan kata sandi masing-masing. Pengaturan akun secara individu ini bertujuan untuk memastikan keamanan akses serta memudahkan pihak sekolah dalam mengontrol durasi pemakaian internet selama kegiatan praktik berlangsung di TKR.

Sesuai dengan rancangan tersebut, setiap akun siswa akan melalui proses autentikasi pada halaman *captive portal* sebelum diizinkan terhubung ke jaringan *wi-fi*. Dengan adanya database 32 akun siswa TKR ini, *router* mikrotik dapat menerapkan kebijakan pembatasan *bandwidth* yang berbeda dari akun guru, sehingga distribusi kecepatan internet di lingkungan sekolah tetap terjaga dan adil. Manajemen akun ini juga berfungsi sebagai sistem absensi digital sederhana untuk

melihat siapa saja siswa yang aktif menggunakan fasilitas internet saat jam pelajaran praktik berlangsung.

d. Konfigurasi *Bandwidth*

Tabel 4.6 *Bandwidth*

No	Nama <i>Queue</i>	<i>Target Network</i>	<i>Upload</i>	<i>Download</i>
1	Limit_Guru	192.168.30.0/24	5M	5M
2	Limit_Siswa_TSM	192.168.10.0/24	3M	3M
3	Limit_Siswa_TKR	192.168.20.0/24	3M	3M

Sumber: Penulis, 2026

Berdasarkan tabel konfigurasi di atas, sistem manajemen lalu lintas data pada jaringan ini dilengkapi dengan fitur *simple queue* pada mikrotik untuk mengatur pembatasan kecepatan internet bagi setiap kelompok pengguna. Pengaturan ini berfungsi untuk memastikan distribusi *bandwidth* berjalan secara adil dan mencegah terjadinya dominasi penggunaan data oleh satu pihak tertentu. Pada wilayah ruang kantor, kelompok limit guru diberikan alokasi kecepatan maksimal sebesar 5 Mbps baik untuk aktivitas *upload* maupun *download*.

Sesuai dengan rancangan tersebut, pembatasan juga diterapkan pada area praktik untuk menjaga kestabilan koneksi selama proses pembelajaran berlangsung. Kelompok limit siswa TSM dan limit siswa TKR masing-masing diberikan batasan kecepatan maksimal sebesar 3 mbps untuk jalur *upload* dan *download*. Dengan adanya pembatasan ini, *router* mikrotik dapat secara otomatis mengontrol ketersediaan sumber daya internet sehingga seluruh perangkat yang terhubung tetap mendapatkan kualitas koneksi yang stabil sesuai dengan peruntukan wilayahnya masing-masing.

e. Blok Situs

Tabel 4.7 Blok Situs

No	URL	Sebelum <i>Filtering</i>	Sesudah <i>Filtering</i>
1	stake.com	<i>Allow</i>	<i>Drop / Deny</i>
2	pulaujudiasia.com	<i>Allow</i>	<i>Drop / Deny</i>
3	linkselamatjudi.live	<i>Allow</i>	<i>Drop / Deny</i>
4	onlinedominogames.com	<i>Allow</i>	<i>Drop / Deny</i>
5	pwa.playonline.poker	<i>Allow</i>	<i>Drop / Deny</i>
6	pokerpatio.com	<i>Allow</i>	<i>Drop / Deny</i>

Sumber: Penulis, 2026

Berdasarkan tabel konfigurasi di atas, sistem keamanan jaringan ini dilengkapi pemblokiran terhadap situs-situs tertentu yang dianggap tidak relevan dengan kegiatan belajar mengajar. Kebijakan ini diterapkan guna menciptakan lingkungan digital yang sehat serta menjaga produktivitas pengguna selama berada di ekosistem jaringan sekolah. Sebagaimana tertera dalam rancangan, beberapa alamat URL seperti situs permainan judi daring yang sebelumnya berstatus *allow* (diizinkan), kini telah diubah menjadi status *drop / deny*.

Sesuai dengan pengaturan tersebut, *router* mikrotik akan secara aktif melakukan pemindaian terhadap setiap paket data yang mengarah ke domain-domain yang telah terdaftar dalam tabel filtrasi. Apabila terdapat perangkat klien yang mencoba mengakses alamat tersebut, sistem akan secara otomatis memutuskan koneksi atau memberikan respons penolakan akses sehingga halaman tidak dapat ditampilkan. Langkah ini menjadi bagian penting dalam manajemen kebijakan keamanan jaringan untuk meminimalisir penyalahgunaan fasilitas internet sekolah oleh siswa maupun pihak lainnya.

BAB V

HASIL DAN PEMBAHASAN

5.1 Spesifikasi Perangkat

Dalam penelitian ini, proses perancangan dan pengembangan jaringan didukung oleh penggunaan berbagai perangkat yang berperan penting dalam setiap tahapan penelitian. Perangkat tersebut digunakan mulai dari tahap analisis kebutuhan jaringan, perancangan topologi, konfigurasi *router* mikrotik, penerapan autentikasi *user manager*, hingga proses simulasi dan pengujian jaringan agar sistem dapat berjalan sesuai dengan kebutuhan di SMK Negeri 3 Prabumulih.

Penggunaan perangkat yang tepat membantu mempermudah proses konfigurasi jaringan, meningkatkan efektivitas pengelolaan *bandwidth*, serta mendukung keamanan dan pemerataan akses internet pada ruang kantor, ruang praktik TSM, dan ruang praktik TKR. Selain itu, pemanfaatan perangkat yang sesuai juga berpengaruh terhadap kestabilan koneksi jaringan serta keberhasilan implementasi simulasi yang dilakukan. Adapun perangkat yang digunakan dalam penelitian ini terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*software*) yang saling mendukung dalam proses implementasi metode autentikasi *user manager* untuk optimalisasi keamanan mikrotik dan pemerataan akses internet.

5.1.1 Perangkat Keras yang digunakan

Perangkat keras yang digunakan dalam penelitian ini merupakan perangkat yang mendukung proses perancangan, simulasi, dan implementasi jaringan terbatas berbasis mikrotik untuk optimalisasi keamanan jaringan serta pemerataan akses internet di SMK Negeri 3 Prabumulih. Perangkat tersebut digunakan dalam proses konfigurasi autentikasi *user manager*, pengaturan manajemen *bandwidth*, penerapan keamanan jaringan, hingga pengujian konektivitas jaringan.

Penggunaan perangkat keras yang sesuai sangat berpengaruh terhadap kelancaran proses simulasi jaringan, kestabilan koneksi internet, serta keberhasilan penerapan autentikasi dan pembagian *bandwidth* pada jaringan sekolah. Selain itu,

perangkat keras juga digunakan untuk mendukung pengujian keamanan jaringan seperti pembatasan akses *router*, pemblokiran situs yang tidak pantas di akses, mekanisme melindungi perangkat dari gangguan antar pengguna dalam jaringan, serta perluasan jangkauan jaringan melalui *access point* agar akses internet dapat digunakan secara lebih merata. Oleh karena itu, pemilihan perangkat keras yang tepat menjadi salah satu faktor penting agar proses pengembangan dan pengujian jaringan dapat berjalan secara optimal dan efisien. Adapun spesifikasi perangkat keras yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Spesifikasi Laptop yang digunakan:
 - a. *Processor: Intel(R) Core (TM) i5-3317U CPU @ 1.70GHz*
 - b. *RAM: 8 GB*
 - c. *Storage: 128 GB*
2. *Modem: Telkomsel Orbit Star Z1 MF293N 4G LTE*
3. *Mikrotik RB951G-2HnD*
4. *Access point TL-WR840N 300 Mbps Wireless Speed 5dBi Antennas*
5. *Switch: NETGEAR ProSAFE GS108Ev3 Plus 8 Port Gigabit Ethernet (10/100/1000 Mbps)*
6. *Kabel LAN: UTP Cat 5e Ethernet Cable*
7. *Perangkat Uji Client:*
 Spesifikasi Laptop yang digunakan:
 - a. *Processor: Intel(R) Core (TM) i3-6006U CPU 2.00Ghz*
 - b. *RAM: 4 GB*
 - c. *Storage: 128 GB*

5.1.2 Perangkat Lunak yang digunakan

Perangkat lunak yang digunakan dalam penelitian ini berperan sebagai pendukung utama dalam proses perancangan topologi, konfigurasi, dan pengujian jaringan berbasis mikrotik untuk optimalisasi keamanan jaringan dan pemerataan akses internet. Perangkat lunak tersebut digunakan untuk melakukan konfigurasi autentikasi *user manager*, pengaturan manajemen *bandwidth*, penerapan keamanan

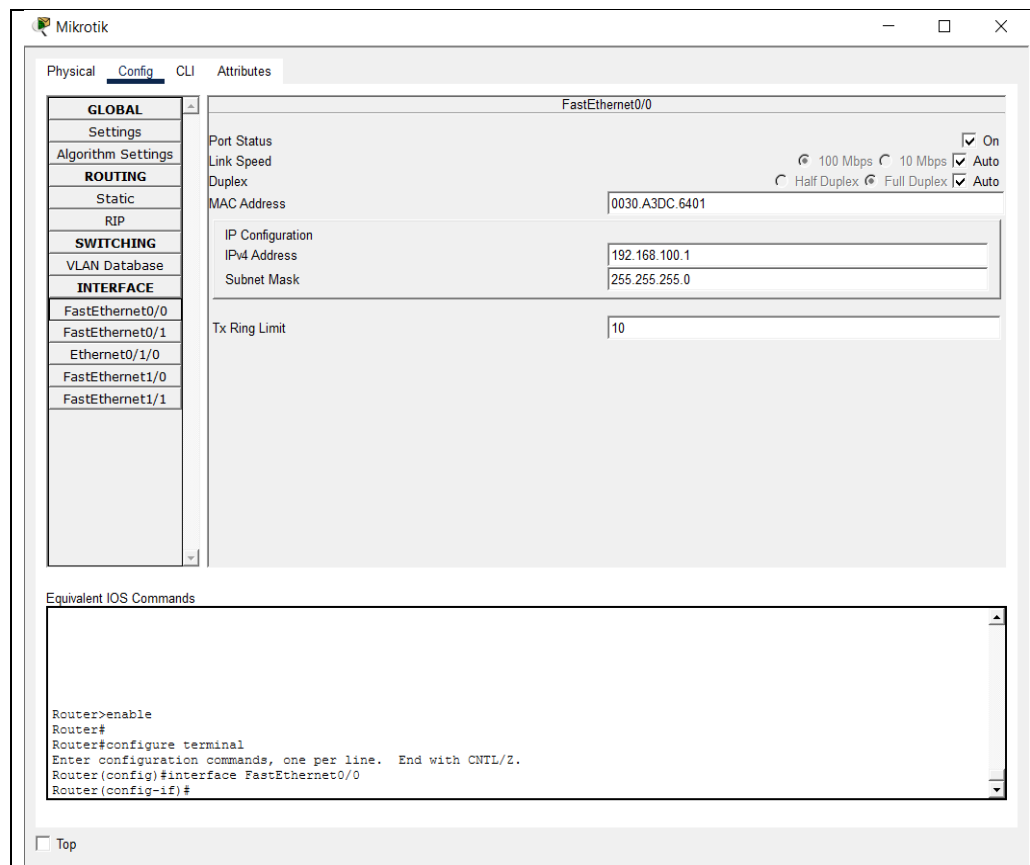
jaringan, pembuatan topologi simulasi, hingga proses pengujian konektivitas jaringan agar sistem dapat berjalan sesuai dengan kebutuhan pengguna.

Penggunaan perangkat lunak yang tepat membantu proses konfigurasi dan pengembangan jaringan menjadi lebih efektif, mempermudah pengelolaan jaringan, serta menjaga kestabilan koneksi internet saat digunakan pada ruang kantor, ruang praktik TSM, dan ruang praktik TKR. Selain itu, perangkat lunak juga digunakan untuk mendukung proses monitoring dan pengujian jaringan seperti pengujian *ping*, verifikasi *login user manager*, serta pengecekan keamanan jaringan pada *router mikrotik*. Oleh karena itu, perangkat lunak memiliki peranan penting dalam memastikan seluruh konfigurasi jaringan dapat berfungsi dengan baik dan optimal. Adapun perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Sistem Operasi: *Microsoft Windows 10 Home Single Language*
2. *System Type: 64-bit Operating System, x64-based Processor*
3. *Cisco Packet Tracer Version 9.0.0.0810*
4. WinBox (64bit) v3.41
5. *RouterOS v6.49.19*
6. *Visual Studio Code versi 1.119.0*
7. Bahasa Pemrograman: *HTML Live Server 5.7.10*
8. *Angry IP Scanner Version: 3.9.3*
9. *Nmap Version: 7.99*
10. *iPerf3 Version: 3.21*
11. *SpeedTest Version: 1.15.200*
12. *Chrome Version: 148.0.7778.179 (Official Build) (64-bit)*
13. *NetCut Version: 3.0.276*
14. *Command Prompt Version: 10.0.18362.1256*
15. *Wireless Network Watcher Version: 2.44*
16. *P2Pover Version: 4.25*
17. *TMAC Version: 6*

5.2 Konfigurasi Cisco Packet Tracer

5.2.1 FastEthernet 0/0



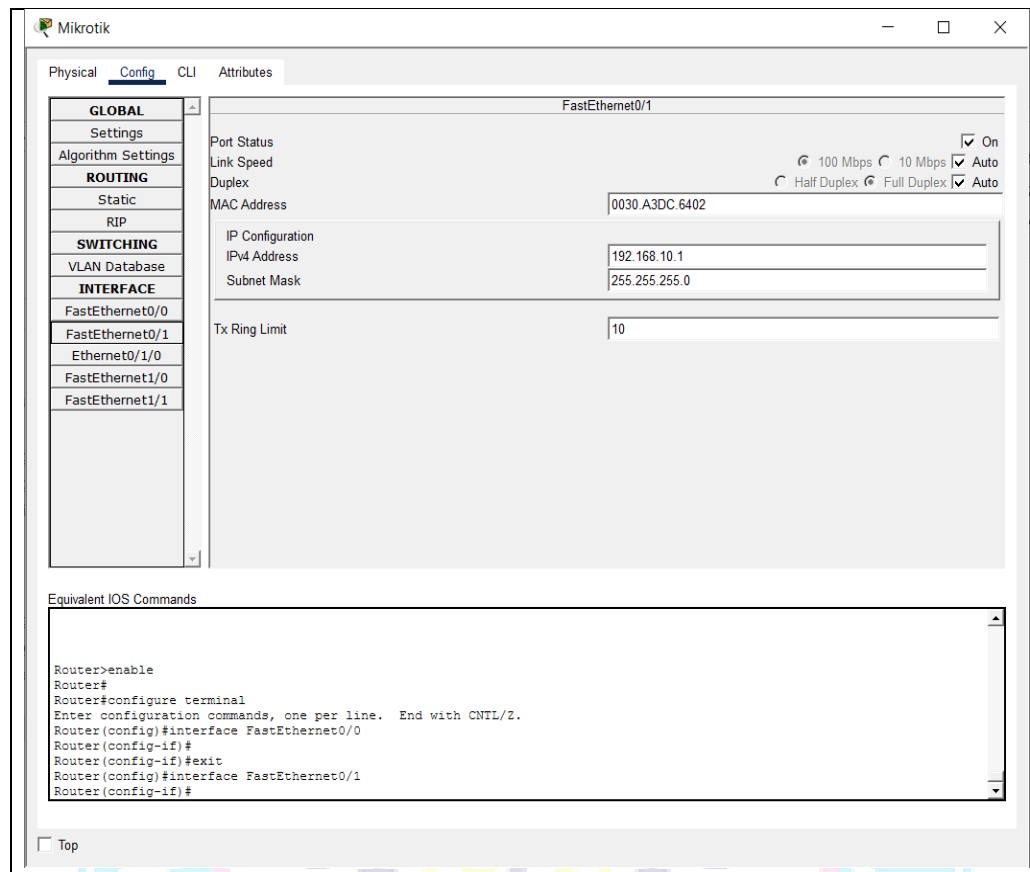
Sumber: Penulis, 2026

Gambar 5.1 FastEthernet 0/0

Gambar di atas menunjukkan konfigurasi *interface FastEthernet0/0* pada *router* di *cisco packet tracer* yang digunakan sebagai simbol koneksi internet pada simulasi jaringan. *Interface* tersebut diberikan alamat IP 192.168.100.1 dengan *subnet mask* 255.255.255.0 sebagai representasi jaringan internet pada topologi yang dibuat.

Pengujian dilakukan dengan cara mengirimkan *ping* dari perangkat *client* menuju alamat IP 192.168.100.1. Jika proses *ping* berhasil dilakukan, maka dapat disimpulkan bahwa perangkat *client* telah berhasil terhubung ke *router interface FastEthernet0/0* dengan alamat IP 192.168.100.1 pada simulasi *cisco packet tracer*.

5.2.2 FastEthernet 0/1



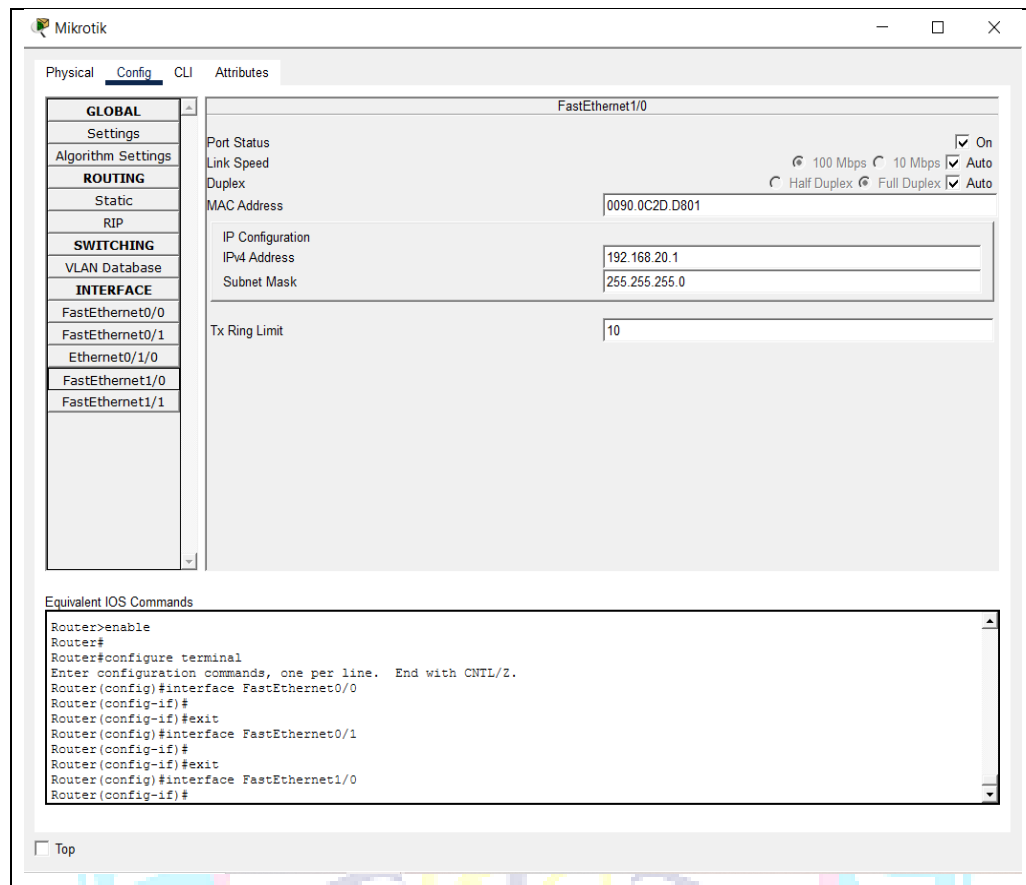
Sumber: Penulis, 2026

Gambar 5.2 FastEthernet 0/1

Gambar di atas menunjukkan konfigurasi *interface FastEthernet0/1* pada *router* di *cisco packet tracer* yang digunakan sebagai *gateway* jaringan ruang praktik TSM. Pada konfigurasi tersebut, *interface FastEthernet0/1* diberikan alamat IP 192.168.10.1 dengan *subnet mask* 255.255.255.0. Alamat IP tersebut berfungsi sebagai *gateway* utama bagi seluruh perangkat *client* yang berada pada jaringan ruang praktik TSM.

Dalam topologi jaringan ini, perangkat *client* akan memperoleh alamat IP secara otomatis menggunakan layanan DHCP yang telah dikonfigurasi pada *router*. Dengan adanya DHCP, *client* tidak perlu melakukan pengaturan alamat IP secara manual karena sistem akan memberikan alamat IP, *subnet mask*, dan *gateway* secara otomatis saat perangkat terhubung ke jaringan.

5.2.3 FastEthernet 1/0



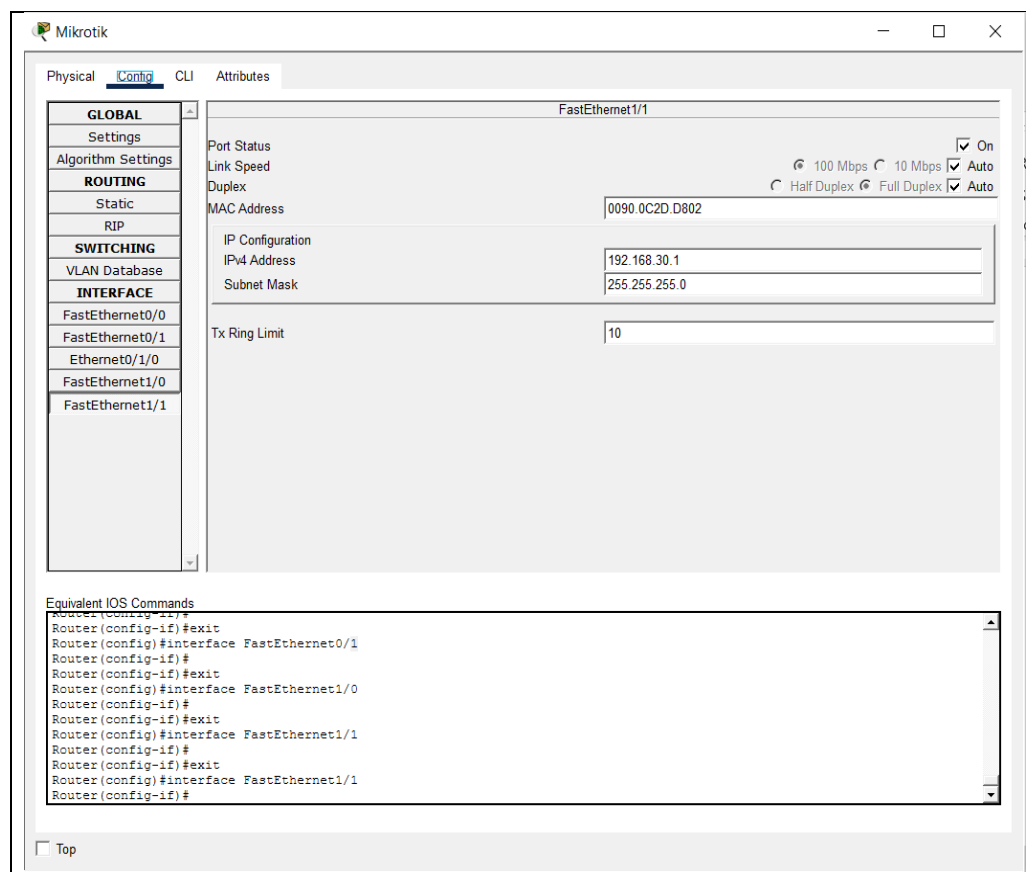
Sumber: Penulis, 2026

Gambar 5.3 FastEthernet 1/0

Gambar di atas menunjukkan konfigurasi *interface FastEthernet1/0* pada router di *cisco packet tracer* yang digunakan sebagai *gateway* jaringan ruang praktik TKR. Pada konfigurasi tersebut, *interface FastEthernet1/0* diberikan alamat IP 192.168.20.1 dengan *subnet mask* 255.255.255.0. Alamat IP tersebut berfungsi sebagai *gateway* utama bagi seluruh perangkat *client* yang berada pada jaringan ruang praktik TKR.

Dalam topologi jaringan ini, perangkat *client* akan memperoleh alamat IP secara otomatis menggunakan layanan DHCP yang telah dikonfigurasi pada *router*. Dengan adanya DHCP, *client* tidak perlu melakukan pengaturan alamat IP secara manual karena sistem akan memberikan alamat IP, *subnet mask*, dan *gateway* secara otomatis saat perangkat terhubung ke jaringan.

5.2.4 FastEthernet 1/1



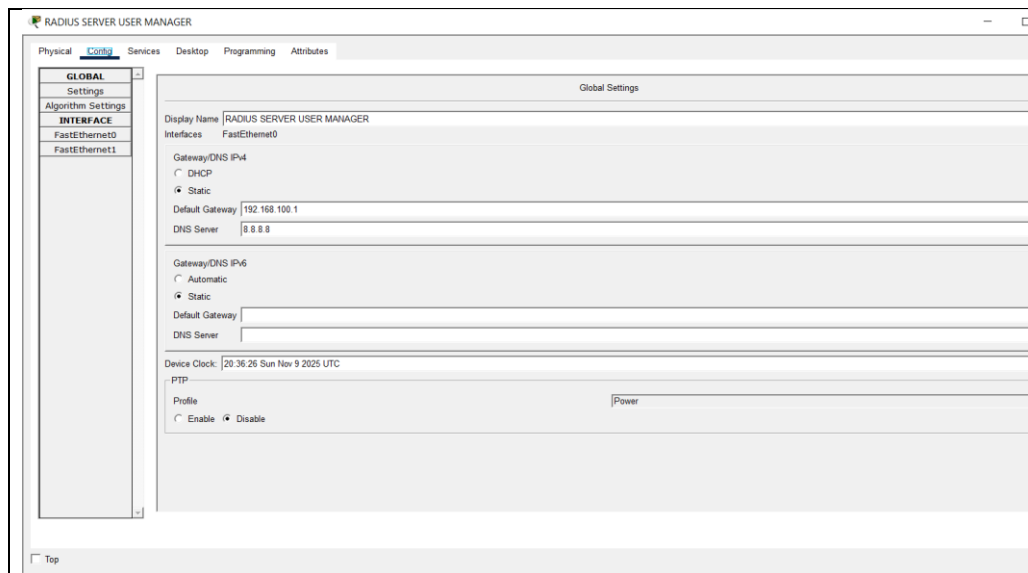
Sumber: Penulis, 2026

Gambar 5.4 FastEthernet 1/1

Gambar di atas menunjukkan konfigurasi *interface FastEthernet1/1* pada *router* di *cisco packet tracer* yang digunakan sebagai *gateway* jaringan ruang praktik ruang kantor. Pada konfigurasi tersebut, *interface FastEthernet1/1* diberikan alamat IP 192.168.30.1 dengan *subnet mask* 255.255.255.0. Alamat IP tersebut berfungsi sebagai *gateway* utama bagi seluruh perangkat *client* yang berada pada jaringan ruang kantor.

Dalam topologi jaringan ini, perangkat *client* akan memperoleh alamat IP secara otomatis menggunakan layanan DHCP yang telah dikonfigurasi pada *router*. Dengan adanya DHCP, *client* tidak perlu melakukan pengaturan alamat IP secara manual karena sistem akan memberikan alamat IP, *subnet mask*, dan *gateway* secara otomatis saat perangkat terhubung ke jaringan

5.2.5 Konfigurasi *Gateway Internet Server User manager*

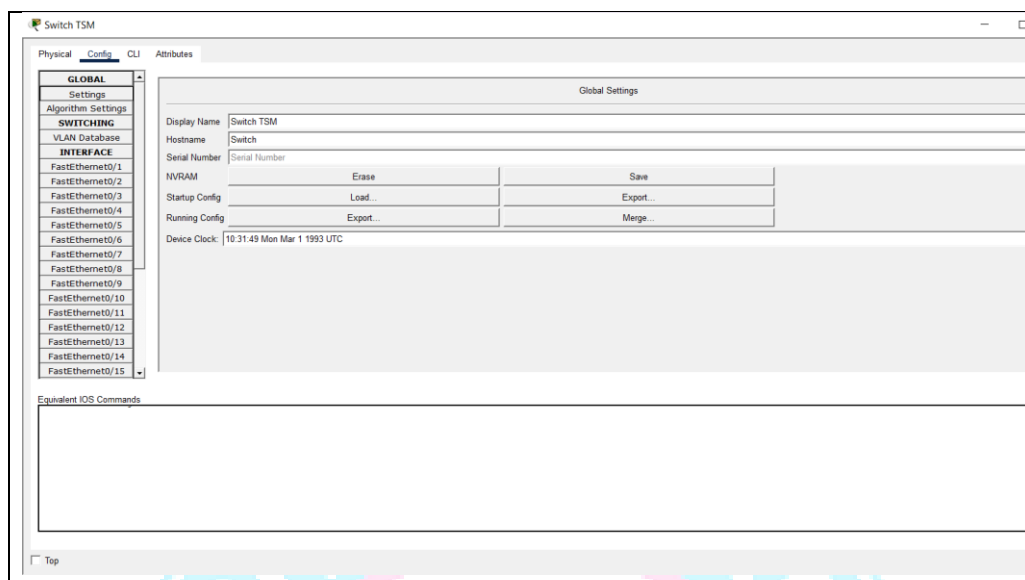


Sumber: Penulis, 2026

Gambar 5.5 *Default Gateway 192.168.100.1*

Gambar berikut menunjukkan konfigurasi *gateway* internet pada perangkat *user manager* melalui menu *config* → *settings*. Pada konfigurasi ini digunakan metode *static* IP dengan alamat 192.168.100.1 sebagai *default gateway*. Alamat IP tersebut berasal dari interface *FastEthernet 0/0* pada *router* yang berfungsi sebagai jalur koneksi internet. Pengaturan *gateway* ini bertujuan agar *user manager* dapat terhubung ke jaringan internet dan melakukan komunikasi data dengan perangkat lain pada jaringan. Selain itu, konfigurasi *DNS server* 8.8.8.8 digunakan untuk membantu proses penerjemahan alamat domain sehingga akses jaringan dapat berjalan dengan baik.

5.2.6 Switch TSM



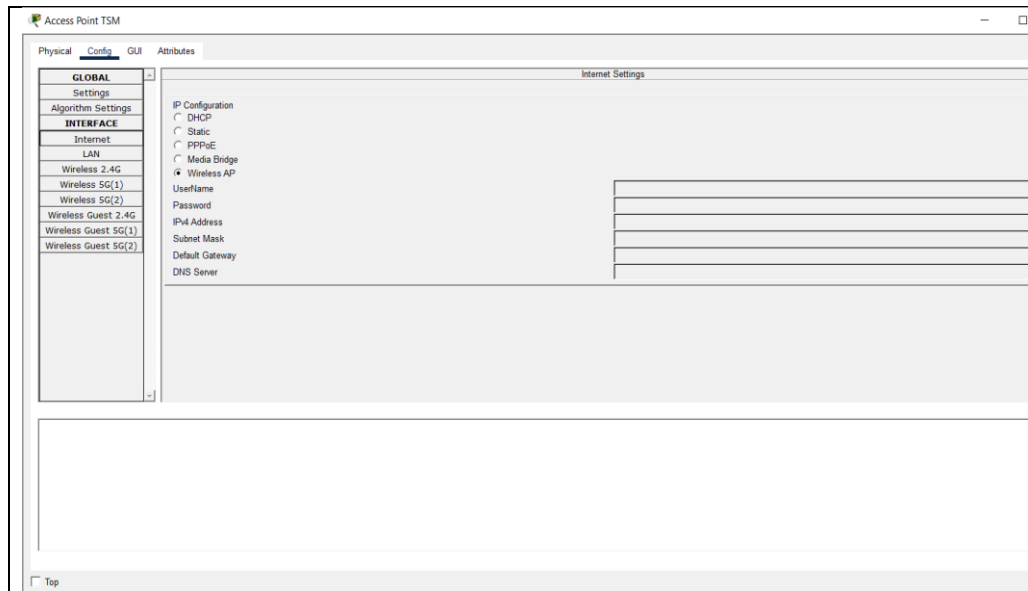
Sumber: Penulis, 2026

Gambar 5.6 Switch TSM

Gambar berikut menunjukkan konfigurasi pada perangkat *switch* TSM yang digunakan sebagai media penghubung jaringan antara *router* dan perangkat *client*. *Switch* berfungsi untuk mendistribusikan koneksi jaringan agar komunikasi data antar perangkat dapat berjalan dengan baik.

Pada jaringan ini, *switch* terhubung dengan *router* melalui *interface FastEthernet* 0/1 yang menggunakan alamat 192.168.10.1 sebagai *default gateway*. Melalui koneksi tersebut, perangkat *client* yang terhubung ke *switch* dapat memperoleh layanan DHCP dan akses jaringan dari *router* sehingga konektivitas jaringan dapat berjalan dengan optimal.

5.2.7 Access point TSM



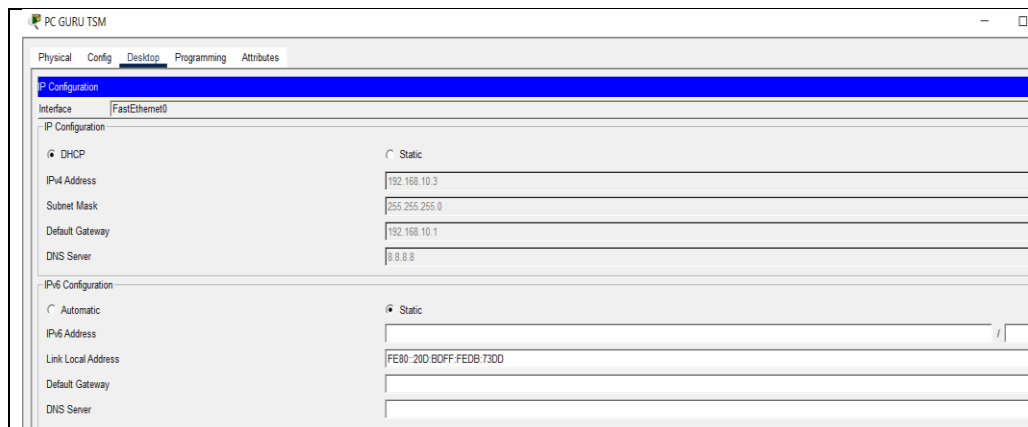
Sumber: Penulis, 2026

Gambar 5.7 Mematikan DHCP Access point TSM

Gambar berikut menunjukkan konfigurasi pada perangkat *access point* TSM dengan memilih mode *wireless AP* pada menu *config* → *internet*. Konfigurasi ini dilakukan untuk menonaktifkan fungsi *DHCP server* pada *access point* sehingga perangkat tidak membuat jaringan baru secara otomatis.

Pada implementasi jaringan ini, layanan *DHCP* dan *default gateway* sepenuhnya dikelola oleh *router* mikrotik dengan alamat *gateway* 192.168.10.1. *Access point* hanya berfungsi sebagai media penyebar jaringan *wireless* kepada perangkat *client* seperti laptop dan *smartphone*. Dengan mematikan *DHCP server* pada *access point*, seluruh perangkat *client* akan memperoleh alamat IP secara otomatis dari mikrotik sehingga semua perangkat berada dalam satu jaringan yang sama dan komunikasi data dapat berjalan dengan baik.

5.2.8 PC TSM



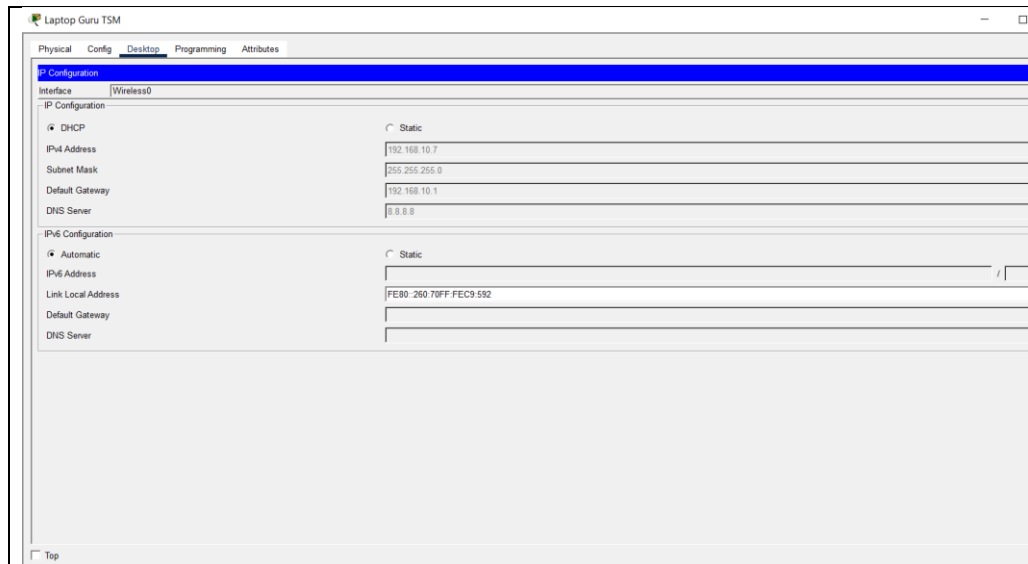
Sumber: Penulis, 2026

Gambar 5.8 PC TSM

Gambar berikut menunjukkan konfigurasi jaringan pada perangkat PC TSM yang digunakan sebagai *client* dalam jaringan. Konfigurasi dilakukan pada menu *desktop* → *IP configuration* dengan metode DHCP sehingga komputer memperoleh alamat IP secara otomatis dari *router*.

Pada konfigurasi ini, PC TSM memperoleh alamat IP 192.168.10.3 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga menggunakan *default gateway* 192.168.10.1 sebagai jalur utama menuju jaringan dan internet. DNS *server* yang digunakan adalah 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini mempermudah proses pengelolaan jaringan karena alamat IP dapat diberikan secara otomatis tanpa perlu melakukan pengaturan manual pada setiap perangkat *client*.

5.2.9 Laptop TSM



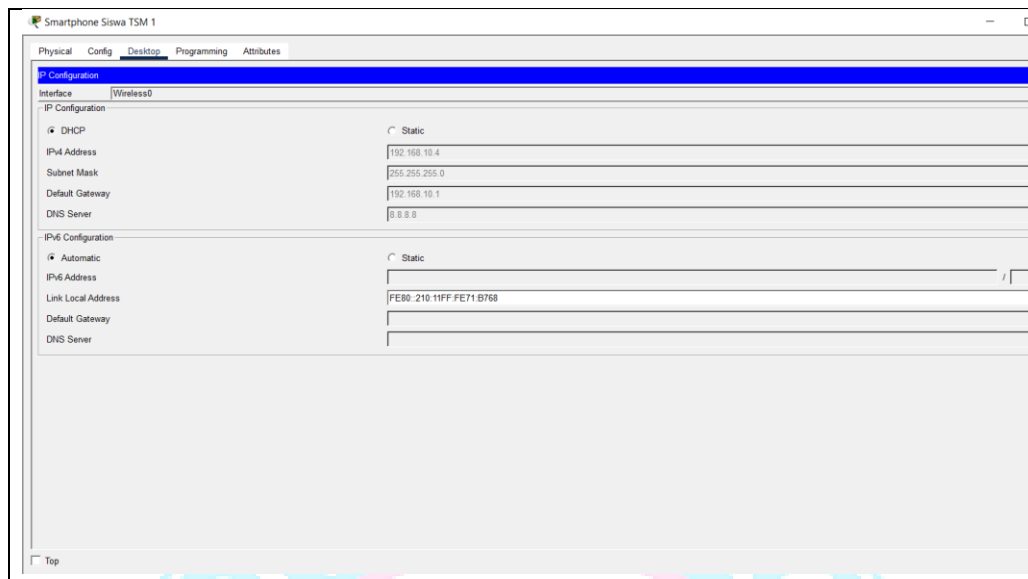
Sumber: Penulis, 2026

Gambar 5.9 Laptop TSM

Gambar berikut menunjukkan konfigurasi alamat IP pada perangkat laptop TSM melalui menu *desktop* → *IP configuration*. Pada konfigurasi ini digunakan metode DHCP sehingga laptop memperoleh alamat IP secara otomatis dari *router* mikrotik melalui *access point*.

Laptop menggunakan interface *wireless0* dan memperoleh alamat IP 192.168.10.7 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga memperoleh *default gateway* 192.168.10.1 sebagai jalur utama menuju jaringan dan internet, serta *DNS server* 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini menunjukkan bahwa *access point* telah berhasil mendistribusikan jaringan *wireless* dari mikrotik kepada perangkat *client* tanpa membuat jaringan baru. Dengan konfigurasi tersebut, laptop dapat terhubung ke jaringan *wireless* dan mengakses layanan jaringan.

5.2.10 Smartphone TSM



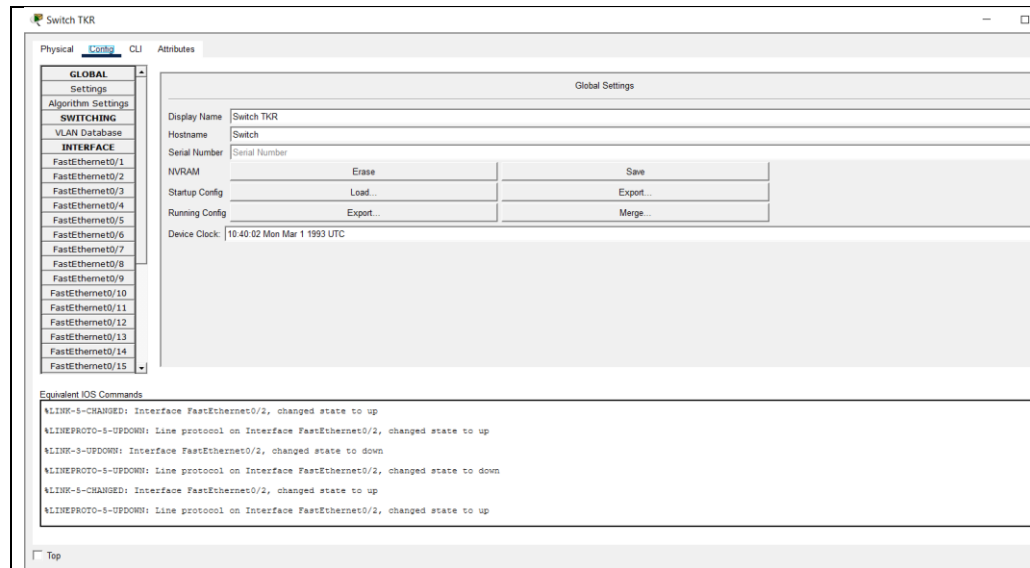
Sumber: Penulis, 2026

Gambar 5.10 Smartphone TSM

Gambar berikut menunjukkan konfigurasi alamat IP pada perangkat *smartphone* siswa TSM melalui menu *desktop* → *IP configuration*. Pada konfigurasi ini digunakan metode DHCP sehingga *smartphone* memperoleh alamat IP secara otomatis dari *router* mikrotik melalui *access point*.

Smartphone menggunakan *interface wireless0* dan memperoleh alamat IP 192.168.10.4 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga memperoleh *default gateway* 192.168.10.1 sebagai jalur utama menuju jaringan dan internet, serta *DNS server* 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini menunjukkan bahwa *smartphone* telah berhasil terhubung ke jaringan *wireless* yang didistribusikan oleh *access point* dan memperoleh layanan jaringan dari mikrotik. Dengan konfigurasi tersebut, *smartphone* dapat mengakses layanan jaringan dan internet dengan baik.

5.2.11 Switch TKR



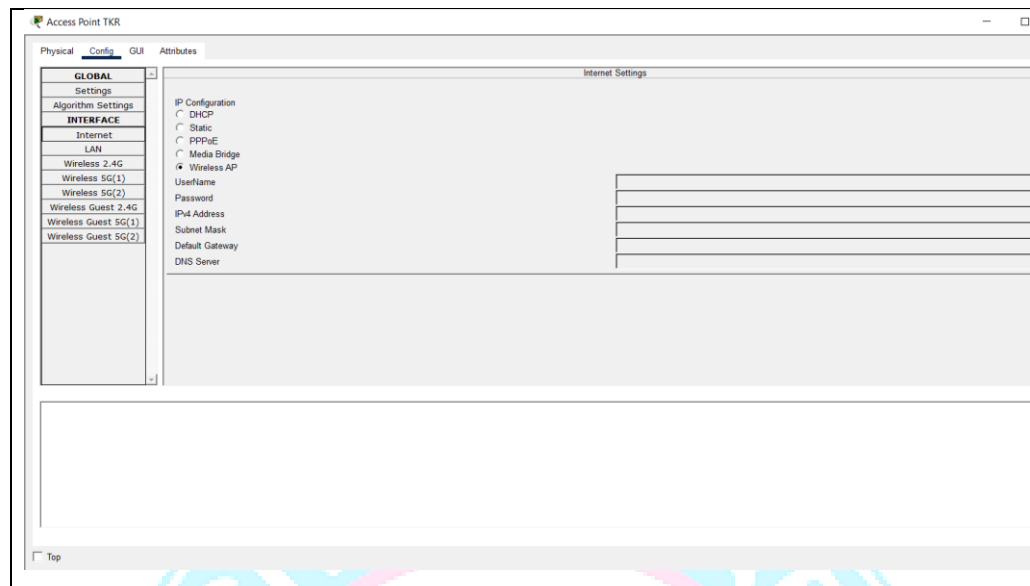
Sumber: Penulis, 2026

Gambar 5.11 Switch TKR

Gambar berikut menunjukkan konfigurasi pada perangkat *switch* TKR yang digunakan sebagai media penghubung jaringan antara *router* dan perangkat *client*. *Switch* berfungsi untuk mendistribusikan koneksi jaringan agar komunikasi data antar perangkat dapat berjalan dengan baik.

Pada jaringan ini, *switch* terhubung dengan *router* melalui *interface FastEthernet 1/0* yang menggunakan alamat 192.168.20.1 sebagai *default gateway*. Melalui koneksi tersebut, perangkat *client* yang terhubung ke *switch* dapat memperoleh layanan DHCP dan akses jaringan dari *router* sehingga konektivitas jaringan dapat berjalan dengan optimal.

5.2.12 Access point TKR



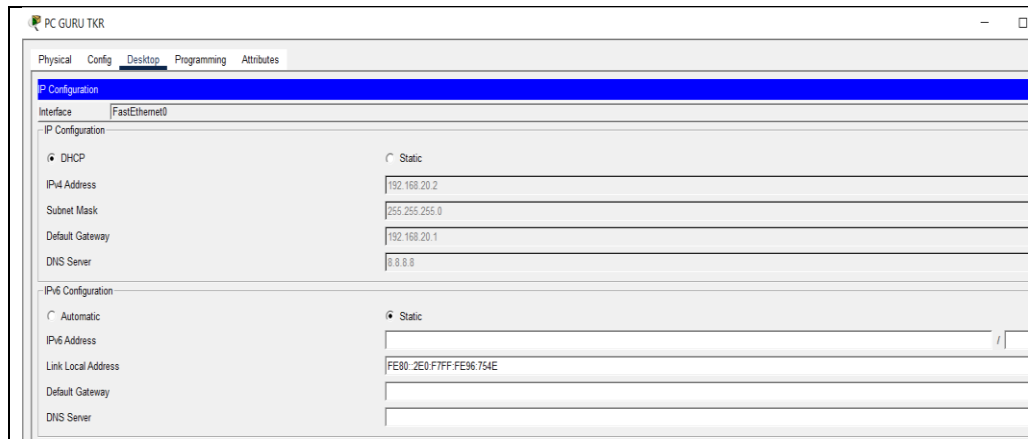
Sumber: Penulis, 2026

Gambar 5.12 Access point TKR

Gambar berikut menunjukkan konfigurasi pada perangkat *access point* TKR dengan memilih mode *wireless* AP pada menu config → internet. Konfigurasi ini dilakukan untuk menonaktifkan fungsi *DHCP server* pada *access point* sehingga perangkat tidak membuat jaringan baru secara otomatis.

Pada implementasi jaringan ini, layanan *DHCP* dan *default gateway* sepenuhnya dikelola oleh *router* mikrotik dengan alamat *gateway* 192.168.20.1. *Access point* hanya berfungsi sebagai media penyebar jaringan *wireless* kepada perangkat *client* seperti laptop dan *smartphone*. Dengan mematikan *DHCP server* pada *access point*, seluruh perangkat *client* akan memperoleh alamat IP secara otomatis dari mikrotik sehingga semua perangkat berada dalam satu jaringan yang sama dan komunikasi data dapat berjalan dengan baik.

5.2.13 PC TKR



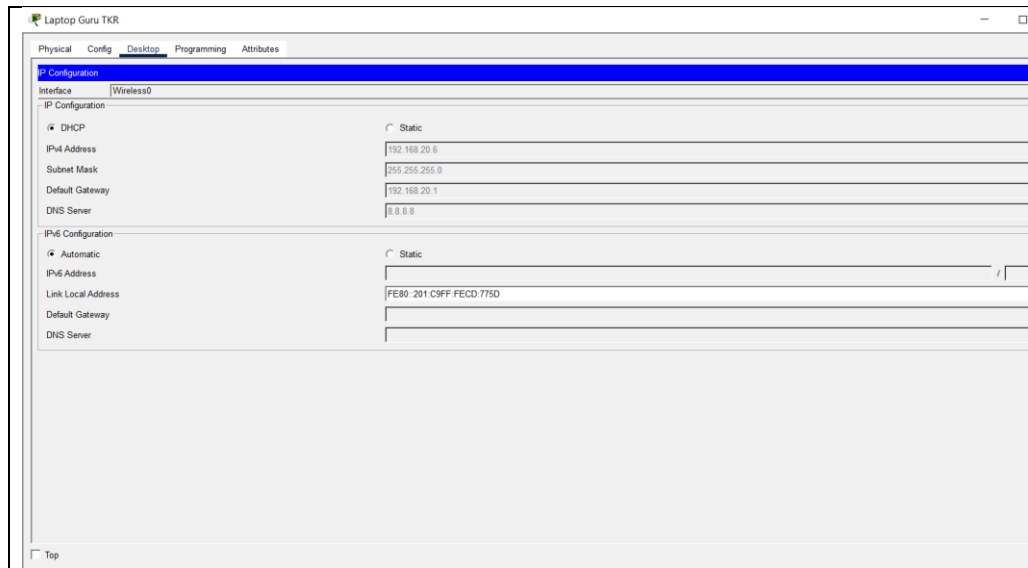
Sumber: Penulis, 2026

Gambar 5. 13 PC TKR

Gambar berikut menunjukkan konfigurasi jaringan pada perangkat PC TKR yang digunakan sebagai *client* dalam jaringan. Konfigurasi dilakukan pada menu *desktop* → IP configuration dengan metode DHCP sehingga komputer memperoleh alamat IP secara otomatis dari *router*.

Pada konfigurasi ini, PC TKR memperoleh alamat IP 192.168.20.2 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga menggunakan *default gateway* 192.168.20.1 sebagai jalur utama menuju jaringan dan internet. DNS *server* yang digunakan adalah 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini mempermudah proses pengelolaan jaringan karena alamat IP dapat diberikan secara otomatis tanpa perlu melakukan pengaturan manual pada setiap perangkat *client*.

5.2.14 Laptop TKR



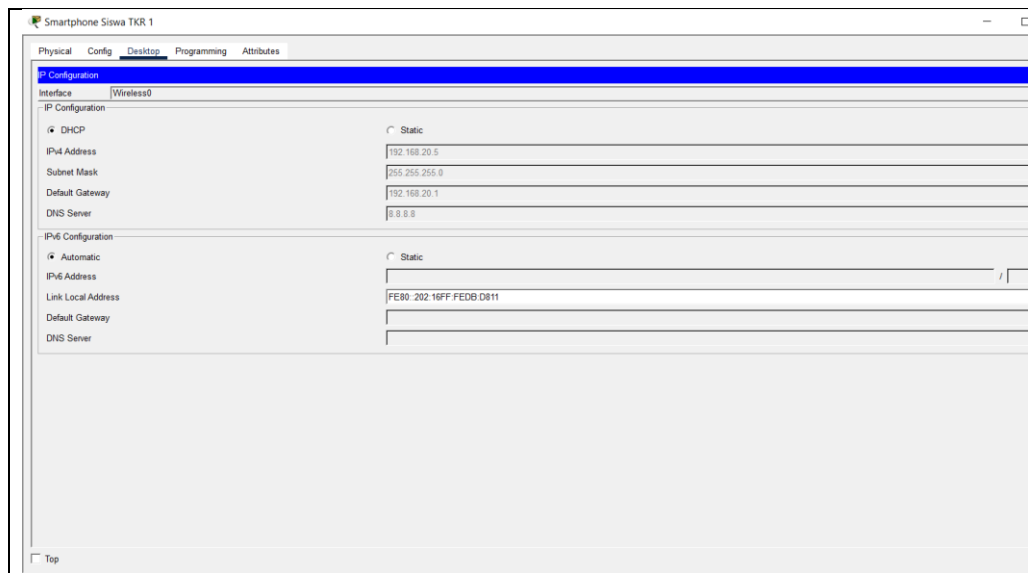
Sumber: Penulis, 2026

Gambar 5.14 Laptop TKR

Gambar berikut menunjukkan konfigurasi alamat IP pada perangkat laptop TKR melalui menu *desktop* → *IP configuration*. Pada konfigurasi ini digunakan metode DHCP sehingga laptop memperoleh alamat IP secara otomatis dari *router* mikrotik melalui *access point*.

Laptop menggunakan interface *wireless0* dan memperoleh alamat IP 192.168.20.6 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga memperoleh *default gateway* 192.168.20.1 sebagai jalur utama menuju jaringan dan internet, serta *DNS server* 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini menunjukkan bahwa *access point* telah berhasil mendistribusikan jaringan *wireless* dari mikrotik kepada perangkat *client* tanpa membuat jaringan baru. Dengan konfigurasi tersebut, laptop dapat terhubung ke jaringan *wireless* dan mengakses layanan jaringan.

5.2.15 Smartphone TKR



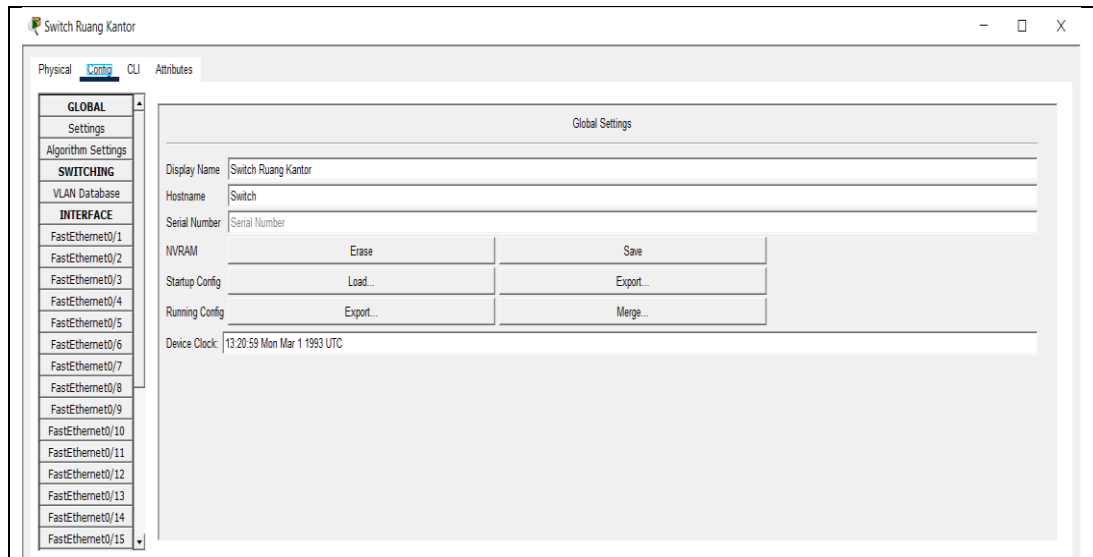
Sumber: Penulis, 2026

Gambar 5.15 Smartphone TKR

Gambar berikut menunjukkan konfigurasi alamat IP pada perangkat *smartphone* siswa TKR melalui menu *desktop* → *IP configuration*. Pada konfigurasi ini digunakan metode DHCP sehingga *smartphone* memperoleh alamat IP secara otomatis dari *router* mikrotik melalui *access point*.

Smartphone menggunakan *interface wireless0* dan memperoleh alamat IP 192.168.20.5 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga memperoleh *default gateway* 192.168.20.1 sebagai jalur utama menuju jaringan dan internet, serta *DNS server* 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini menunjukkan bahwa *smartphone* telah berhasil terhubung ke jaringan *wireless* yang didistribusikan oleh *access point* dan memperoleh layanan jaringan dari mikrotik. Dengan konfigurasi tersebut, *smartphone* dapat mengakses layanan jaringan dan internet dengan baik.

5.2.16 Switch Ruang Kantor



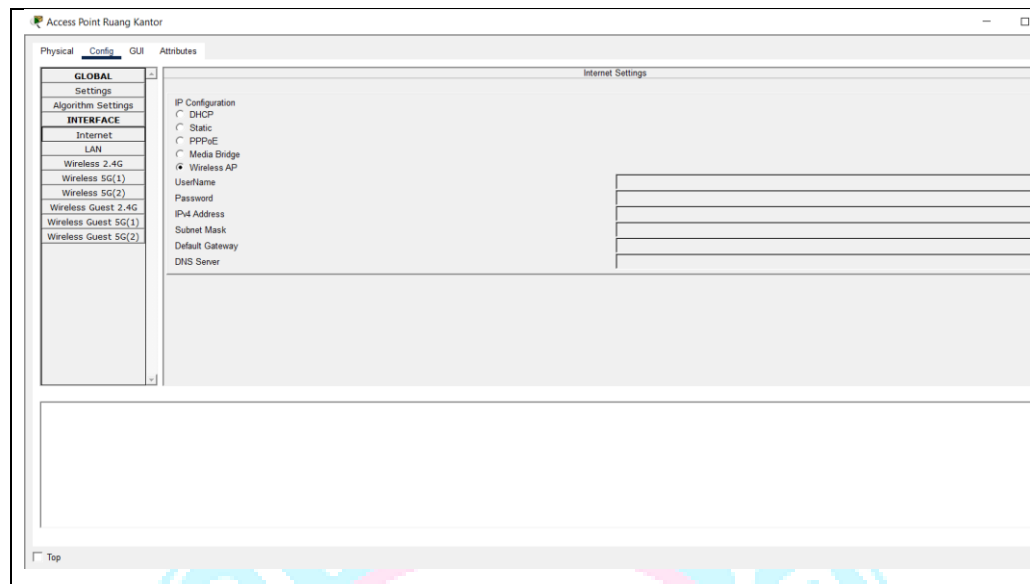
Sumber: Penulis, 2026

Gambar 5.16 Switch Ruang Kantor

Gambar berikut menunjukkan konfigurasi pada perangkat *switch* ruang kantor yang digunakan sebagai media penghubung jaringan antara *router* dan perangkat *client*. *Switch* berfungsi untuk mendistribusikan koneksi jaringan agar komunikasi data antar perangkat dapat berjalan dengan baik.

Pada jaringan ini, *switch* terhubung dengan *router* melalui *interface FastEthernet* 1/1 yang menggunakan alamat 192.168.30.1 sebagai *default gateway*. Melalui koneksi tersebut, perangkat *client* yang terhubung ke *switch* dapat memperoleh layanan DHCP dan akses jaringan dari *router* sehingga konektivitas jaringan dapat berjalan dengan optimal.

5.2.17 Access point Ruang Kantor



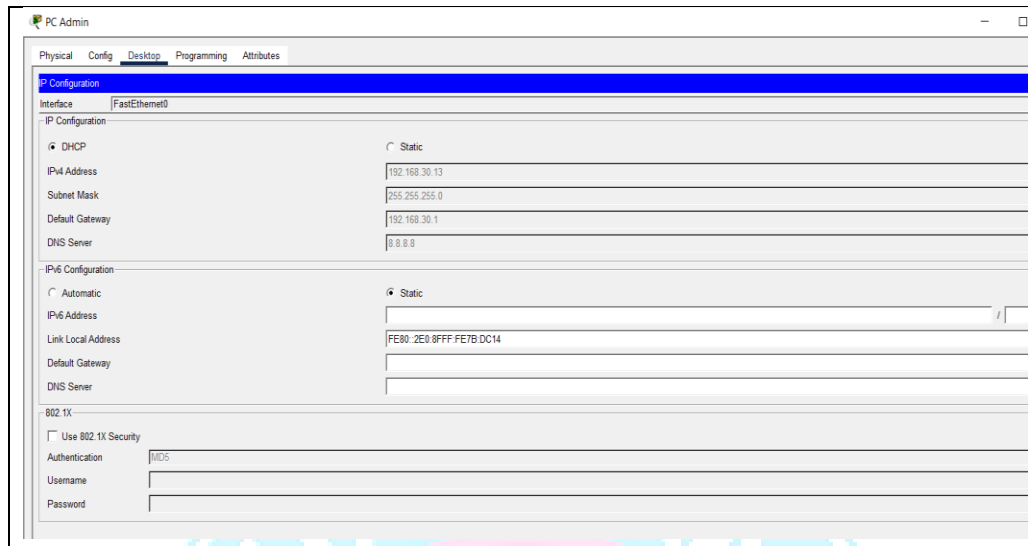
Sumber: Penulis, 2026

Gambar 5.17 Access point Ruang Kantor

Gambar berikut menunjukkan konfigurasi pada perangkat *access point* ruang kantor dengan memilih mode *wireless AP* pada menu config → internet. Konfigurasi ini dilakukan untuk menonaktifkan fungsi *DHCP server* pada *access point* sehingga perangkat tidak membuat jaringan baru secara otomatis.

Pada implementasi jaringan ini, layanan *DHCP* dan *default gateway* sepenuhnya dikelola oleh *router* mikrotik dengan alamat *gateway* 192.168.30.1. *Access point* hanya berfungsi sebagai media penyebar jaringan *wireless* kepada perangkat *client* seperti laptop dan *smartphone*. Dengan mematikan *DHCP server* pada *access point*, seluruh perangkat *client* akan memperoleh alamat IP secara otomatis dari mikrotik sehingga semua perangkat berada dalam satu jaringan yang sama dan komunikasi data dapat berjalan dengan baik.

5.2.18 PC Ruang Kantor



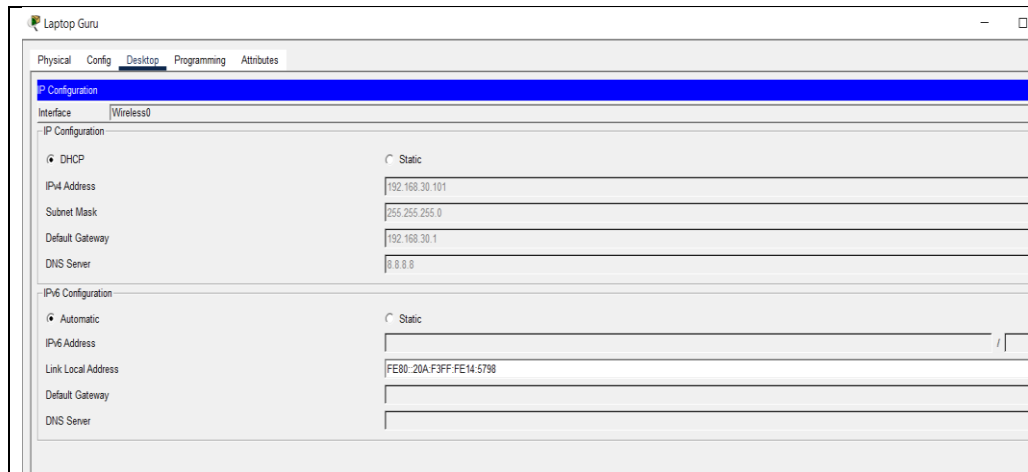
Sumber: Penulis, 2026

Gambar 5.18 PC Ruang Kantor

Gambar berikut menunjukkan konfigurasi jaringan pada perangkat PC ruang kantor yang digunakan sebagai *client* dalam jaringan. Konfigurasi dilakukan pada menu *desktop* → *IP configuration* dengan metode DHCP sehingga komputer memperoleh alamat IP secara otomatis dari *router*.

Pada konfigurasi ini, PC ruang kantor memperoleh alamat IP 192.168.30.13 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga menggunakan *default gateway* 192.168.30.1 sebagai jalur utama menuju jaringan dan internet. DNS *server* yang digunakan adalah 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini mempermudah proses pengelolaan jaringan karena alamat IP dapat diberikan secara otomatis tanpa perlu melakukan pengaturan manual pada setiap perangkat *client*.

5.2.19 Laptop Ruang Kantor



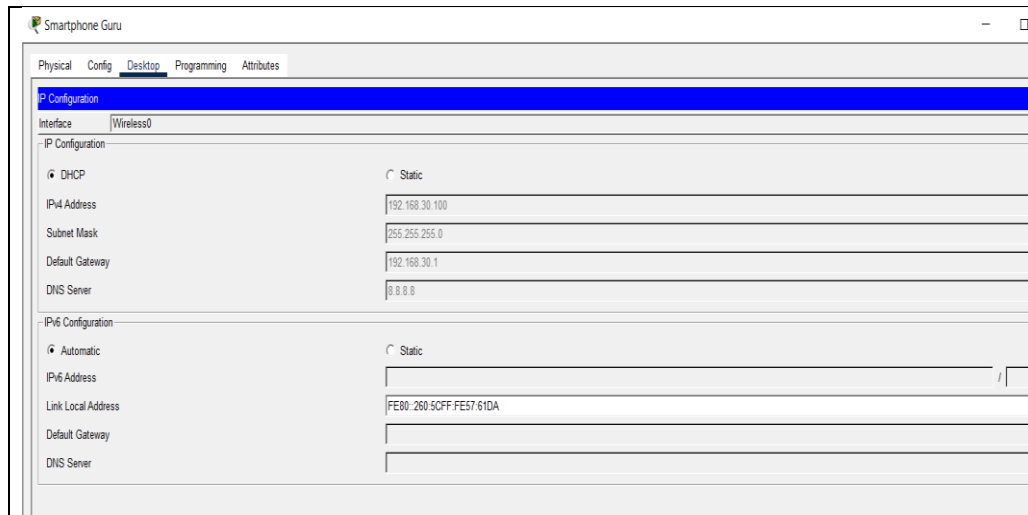
Sumber: Penulis, 2026

Gambar 5.19 Laptop Ruang Kantor

Gambar berikut menunjukkan konfigurasi alamat IP pada perangkat laptop ruang kantor melalui menu *desktop* → *IP configuration*. Pada konfigurasi ini digunakan metode DHCP sehingga laptop memperoleh alamat IP secara otomatis dari *router* mikrotik melalui *access point*.

Laptop menggunakan interface *wireless0* dan memperoleh alamat IP 192.168.30.101 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga memperoleh *default gateway* 192.168.30.1 sebagai jalur utama menuju jaringan dan internet, serta *DNS server* 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini menunjukkan bahwa *access point* telah berhasil mendistribusikan jaringan *wireless* dari mikrotik kepada perangkat *client* tanpa membuat jaringan baru. Dengan konfigurasi tersebut, laptop dapat terhubung ke jaringan *wireless* dan mengakses layanan jaringan.

5.2.20 *Smartphone Ruang Kantor*



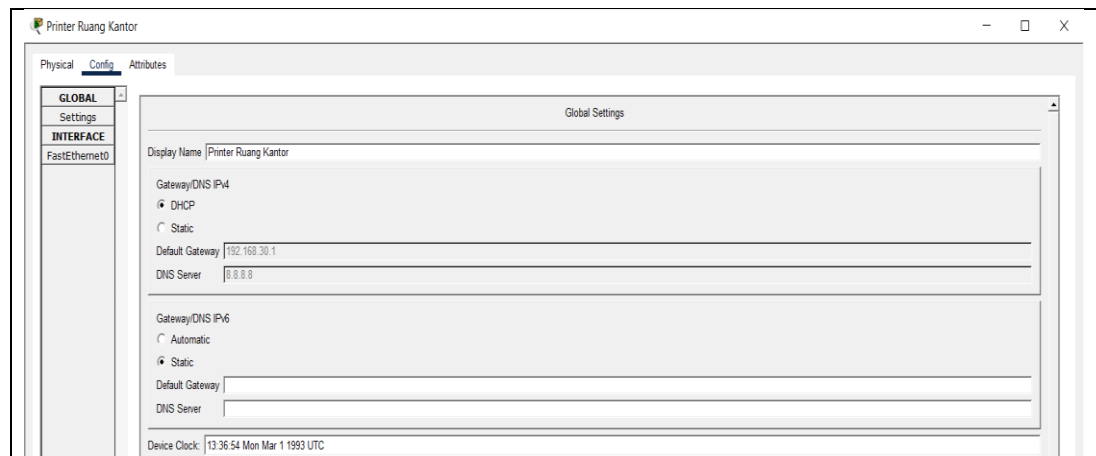
Sumber: Penulis, 2026

Gambar 5. 20 *Smartphone Ruang Kantor*

Gambar berikut menunjukkan konfigurasi alamat IP pada perangkat *smartphone* guru ruang kantor melalui menu *desktop* → *IP configuration*. Pada konfigurasi ini digunakan metode DHCP sehingga *smartphone* memperoleh alamat IP secara otomatis dari *router* mikrotik melalui *access point*.

Smartphone menggunakan *interface wireless0* dan memperoleh alamat IP 192.168.30.100 dengan *subnet mask* 255.255.255.0. Selain itu, perangkat juga memperoleh *default gateway* 192.168.30.1 sebagai jalur utama menuju jaringan dan internet, serta *DNS server* 8.8.8.8 untuk membantu proses penerjemahan alamat domain. Konfigurasi DHCP ini menunjukkan bahwa *smartphone* telah berhasil terhubung ke jaringan *wireless* yang didistribusikan oleh *access point* dan memperoleh layanan jaringan dari mikrotik. Dengan konfigurasi tersebut, *smartphone* dapat mengakses layanan jaringan dan internet dengan baik.

5.2.21 *Printer Ruang Kantor*



Sumber: Penulis, 2026

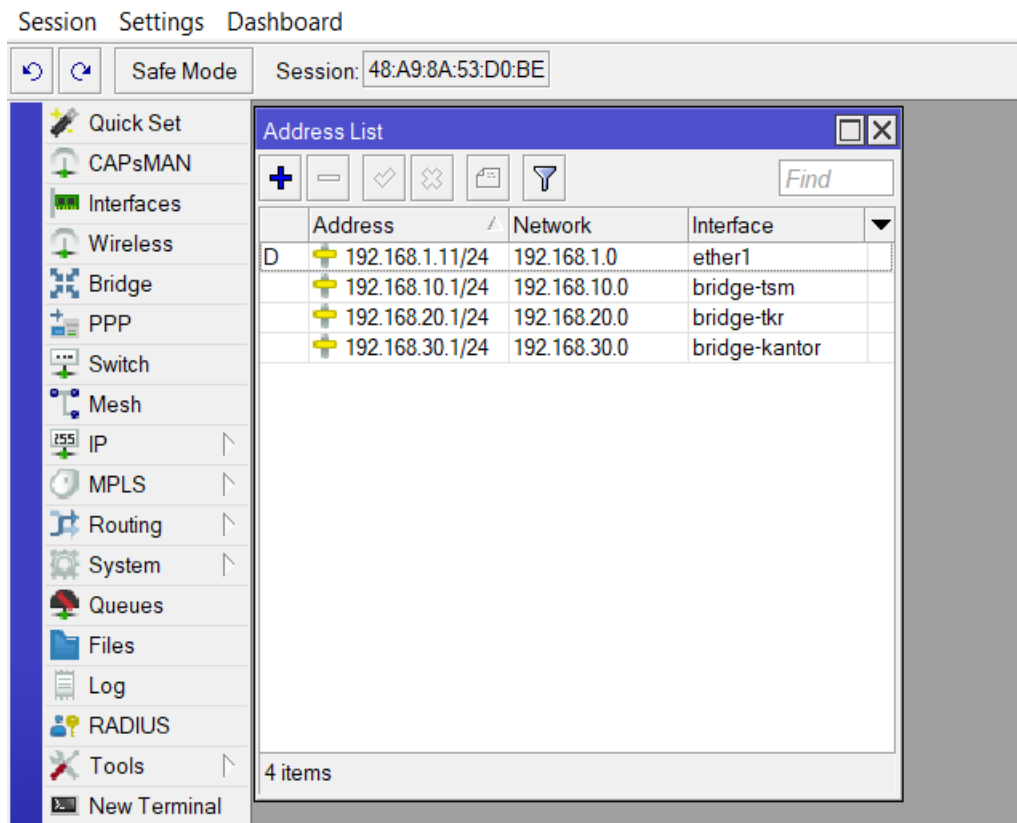
Gambar 5.21 *Printer Ruang Kantor*

Gambar berikut menunjukkan konfigurasi jaringan pada perangkat *printer* ruang kantor melalui menu *config* → *settings*. Pada konfigurasi ini digunakan metode DHCP sehingga *printer* memperoleh pengaturan jaringan secara otomatis dari *router* mikrotik.

Printer menggunakan *default gateway* 192.168.30.1 sebagai jalur utama menuju jaringan dan memperoleh DNS *server* 8.8.8.8 untuk membantu proses komunikasi jaringan. Konfigurasi DHCP ini mempermudah pengelolaan perangkat karena *printer* dapat terhubung ke jaringan tanpa perlu melakukan pengaturan alamat IP secara manual. Dengan konfigurasi tersebut, *printer* dapat terhubung ke jaringan ruang kantor sehingga dapat digunakan oleh perangkat lain dalam jaringan untuk proses pencetakan dokumen.

5.3 Konfigurasi Winbox

5.3.1 Konfigurasi IP Address



Sumber: Penulis, 2026

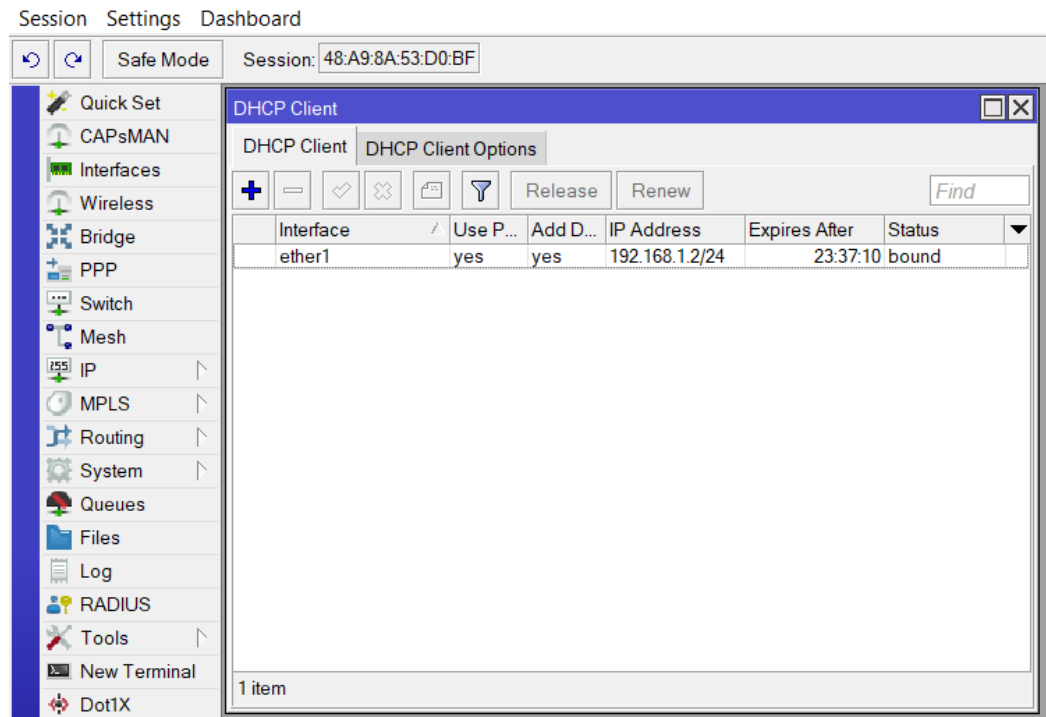
Gambar 5.22 Address List

Gambar berikut menunjukkan konfigurasi alamat IP pada *router* mikrotik menggunakan aplikasi winbox melalui menu IP → *addresses*. Konfigurasi ini dilakukan pada perangkat jaringan nyata (*real device*) untuk mengatur pembagian jaringan pada beberapa ruangan yang terhubung dalam sistem jaringan.

Pada konfigurasi tersebut, *interface ether1* digunakan sebagai jalur koneksi internet dan memperoleh alamat IP secara otomatis dari jaringan internet/provider, yaitu 192.168.1.11/24 pada network 192.168.1.0. Selain itu, *router* juga dikonfigurasi menggunakan beberapa *interface bridge* untuk memisahkan jaringan berdasarkan ruangan atau divisi. *Interface bridge-tsm* diberikan alamat IP 192.168.10.1/24 untuk jaringan ruang praktik TSM, *interface bridge-tnr* diberikan alamat IP 192.168.20.1/24 untuk jaringan TKR, dan *interface bridge-kantor* diberikan alamat IP 192.168.30.1/24 untuk jaringan kantor.

Konfigurasi alamat IP pada *router* mikrotik ini bertujuan agar perangkat dapat berfungsi sebagai *gateway* utama, penghubung antarjaringan lokal, serta mengatur distribusi koneksi internet kepada seluruh perangkat *client* pada masing-masing jaringan dalam implementasi jaringan nyata.

5.3.2 DHCP Client



Sumber: Penulis, 2026

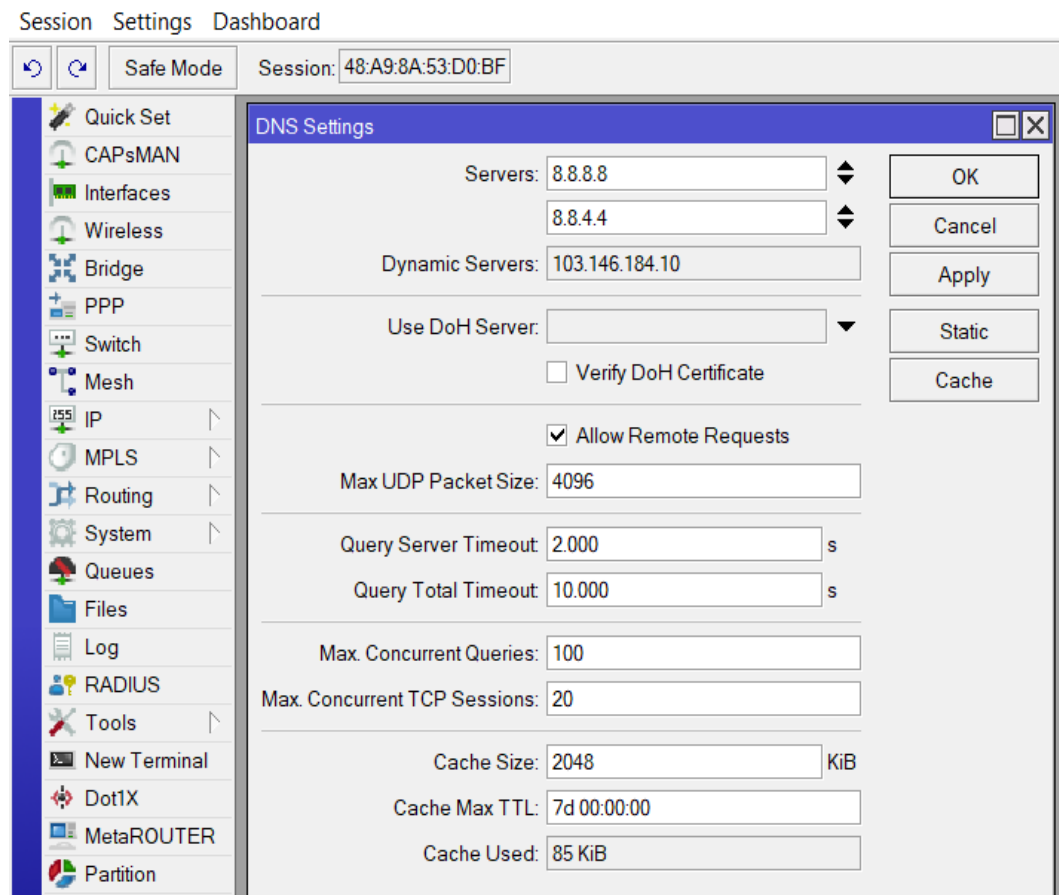
Gambar 5.23 DHCP Client

Gambar berikut menunjukkan konfigurasi DHCP *client* pada *router* mikrotik menggunakan aplikasi winbox melalui menu IP → DHCP *client*. Konfigurasi ini dilakukan pada perangkat jaringan nyata (*real device*) untuk memperoleh alamat IP secara otomatis dari sumber internet.

Pada konfigurasi tersebut, *interface ether1* digunakan sebagai jalur koneksi internet dan memperoleh alamat IP 192.168.1.2/24 dengan status *bound*, yang menandakan bahwa *router* mikrotik telah berhasil menerima alamat IP dari jaringan internet melalui layanan DHCP.

Konfigurasi DHCP *client* ini bertujuan agar *router* mikrotik dapat terhubung dengan jaringan internet secara otomatis tanpa perlu melakukan pengaturan IP

5.3.4 DNS Setting



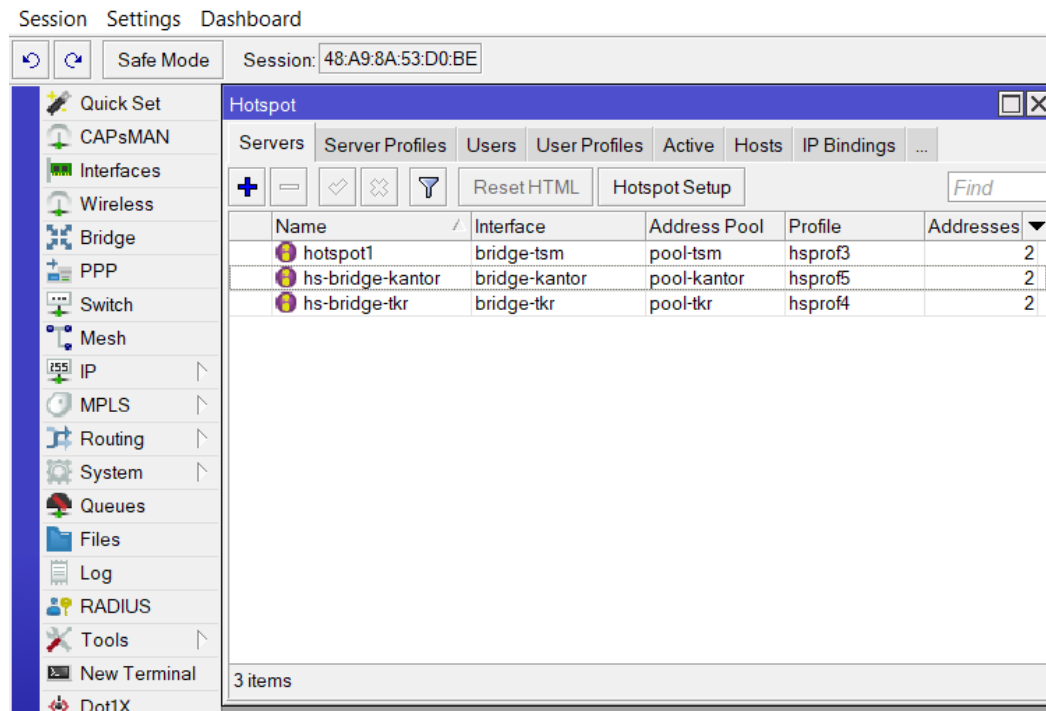
Sumber: Penulis, 2026

Gambar 5.25 DNS Setiing

Gambar berikut menunjukkan konfigurasi *Domain Name System* (DNS) pada *router* mikrotik menggunakan aplikasi winbox melalui menu IP → DNS. Konfigurasi DNS ini dilakukan agar *router* mikrotik dapat menerjemahkan alamat domain menjadi alamat IP sehingga perangkat *client* dapat mengakses internet dengan baik.

Pada konfigurasi tersebut digunakan DNS *server* 8.8.8.8 dan 8.8.4.4 yang merupakan layanan DNS publik dari *Google*. Selain itu, opsi *allow remote requests* diaktifkan agar *router* mikrotik dapat melayani permintaan DNS dari seluruh perangkat *client* yang terhubung pada jaringan lokal. Konfigurasi DNS ini bertujuan untuk mendukung proses komunikasi jaringan dan mempercepat akses internet pada seluruh perangkat yang terhubung ke *router* mikrotik.

5.3.5 Hotspot Server



Sumber: Penulis, 2026

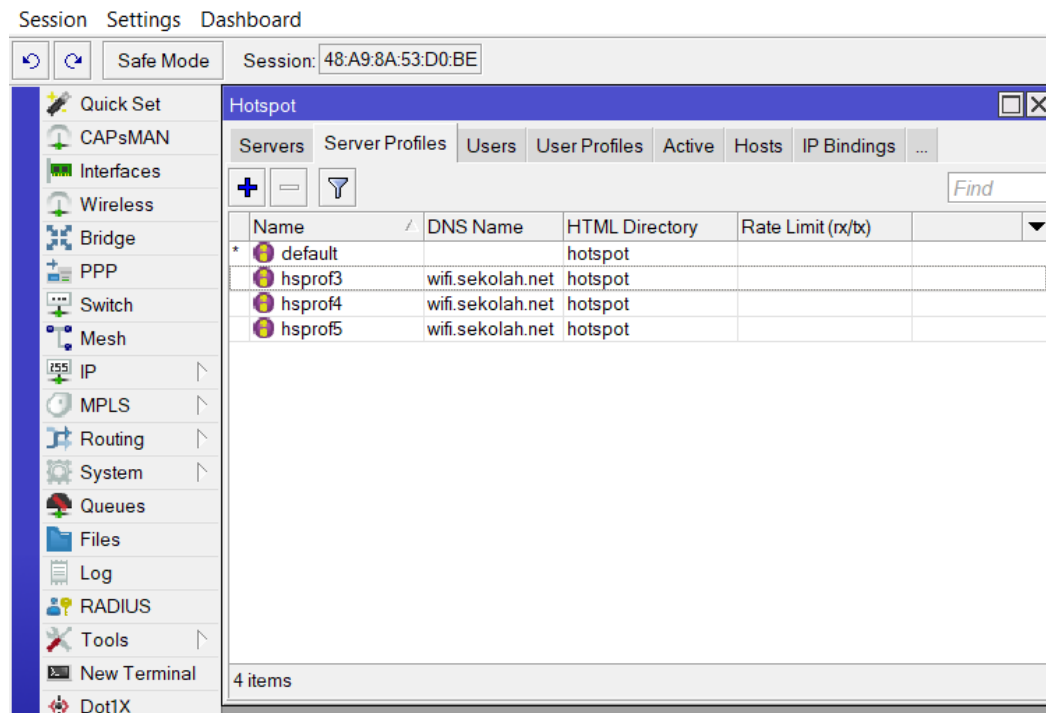
Gambar 5. 26 Hotspot Server

Konfigurasi *hotspot server* pada mikrotik dilakukan untuk mengelola autentikasi pengguna sebelum dapat mengakses jaringan internet. Pada konfigurasi ini, terdapat tiga *hotspot server* yang digunakan untuk masing-masing jaringan ruangan, yaitu jaringan TSM, TKR, dan kantor.

Hotspot server pertama dengan nama *hotspot1* menggunakan *interface bridge-tsm* sebagai jalur jaringan ruang praktik TSM dengan *address pool pool-tsm* dan *profile hsprof3*. Selanjutnya, *hotspot server hs-bridge-kantor* menggunakan *interface bridge-kantor* dengan *address pool pool-kantor* dan *profile hsprof5* untuk jaringan kantor. Sedangkan *hotspot server hs-bridge-tnr* menggunakan *interface bridge-tnr* dengan *address pool pool-tnr* dan *profile hsprof4* untuk jaringan TKR.

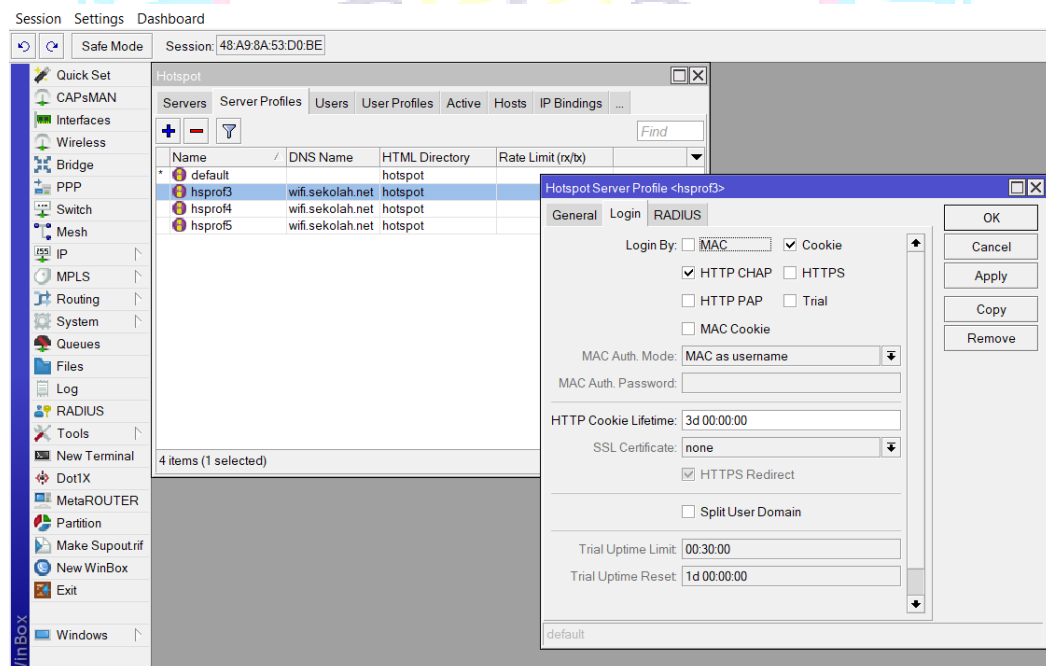
Dengan konfigurasi tersebut, setiap perangkat *client* yang terhubung ke jaringan akan memperoleh alamat IP dari *address pool* yang telah ditentukan, kemudian diarahkan ke halaman *login hotspot* untuk melakukan autentikasi menggunakan *username* dan *password* sebelum mendapatkan akses internet. Konfigurasi ini bertujuan untuk mempermudah pengelolaan pengguna serta meningkatkan keamanan dan kontrol akses jaringan pada masing-masing ruangan.

5.3.6 Server Profile Hotspot



Sumber: Penulis, 2026

Gambar 5.27 Server Profile Hotspot



Sumber: Penulis, 2026

Gambar 5.28 Login by HTTP CHAP

Konfigurasi *hotspot server profile* pada mikrotik dilakukan untuk mengatur metode autentikasi dan pengelolaan layanan *hotspot* pada setiap jaringan yang digunakan. Pada konfigurasi ini terdapat beberapa *profile hotspot*, yaitu *hsprof3*, *hsprof4*, dan *hsprof5*, yang masing-masing digunakan pada jaringan TSM, TKR, dan kantor. Seluruh *profile* menggunakan DNS *name wifi.sekolah.net* dengan direktori halaman *login* berada pada folder *hotspot* sebagai tempat penyimpanan file autentikasi *hotspot* mikrotik.

Pada tab *login*, metode autentikasi dikonfigurasi dengan mengaktifkan fitur HTTP CHAP pada seluruh *profile hotspot*. Penggunaan metode HTTP CHAP bertujuan untuk meningkatkan keamanan proses *login* karena *username* dan *password* pengguna tidak dikirim dalam bentuk teks biasa, melainkan menggunakan metode autentikasi terenkripsi.

Dengan konfigurasi tersebut, setiap pengguna yang terhubung ke jaringan *hotspot* akan diarahkan ke halaman *login* menggunakan alamat DNS yang telah ditentukan dan diwajibkan melakukan autentikasi menggunakan *username* dan *password* sebelum memperoleh akses internet. Konfigurasi ini membantu meningkatkan keamanan serta mempermudah pengelolaan akses pengguna pada sistem jaringan sekolah.

5.3.7 Users Hotspot

Server	Name	Address	MAC Address	Profile	Uptime
all	Achmad Sukri, S.Pd, M.Si Ruang Kantor			Guru_Kantor	02:36:29
all	Erwansah Bustomi, B.I Ruang Kantor			Guru_Kantor	00:12:13
all	Agus Syahputra TSM			Siswa_TSM	00:48:12
all	Febisa Zumel, S.E Ruang Kantor			Guru_Kantor	00:00:00
all	Selvi Puranda, S.Kom Ruang Kantor			Guru_Kantor	00:00:00
all	Henny Purwati, S.Pd Ruang Kantor			Guru_Kantor	00:00:00
all	Indri Susanti, S.Pd Ruang Kantor			Guru_Kantor	00:00:00
all	Tri Muhi Haryani, M.Pd Ruang Kantor			Guru_Kantor	00:00:00
all	Arifina Yanna Indah, S.T Ruang Kantor			Guru_Kantor	00:00:00
all	Dedi Saputra, S.Pd Ruang Kantor			Guru_Kantor	00:00:00
all	Dr. Lutfi, S.Ag, MM Ruang Kantor			Guru_Kantor	00:00:00
all	Ryan Aziz, S.Pd Ruang Kantor			Guru_Kantor	00:00:00
all	Andri Hermawan, S.P, M.Si Ruang Kantor			Guru_Kantor	00:00:00
all	Saddam Muslim, S.Si Ruang Kantor			Guru_Kantor	00:00:00
all	Hanny Sunarya, S.T Ruang Kantor			Guru_Kantor	00:00:00
all	Rahmi Widia Pratiwi, S.T Ruang Kantor			Guru_Kantor	00:00:00
all	Finilia, S.Pd Ruang Kantor			Guru_Kantor	00:00:00
all	Dita Ratna Sari, S.Pd Ruang Kantor			Guru_Kantor	00:00:00

Sumber: Penulis, 2026

Gambar 5. 29 Users Hotspot

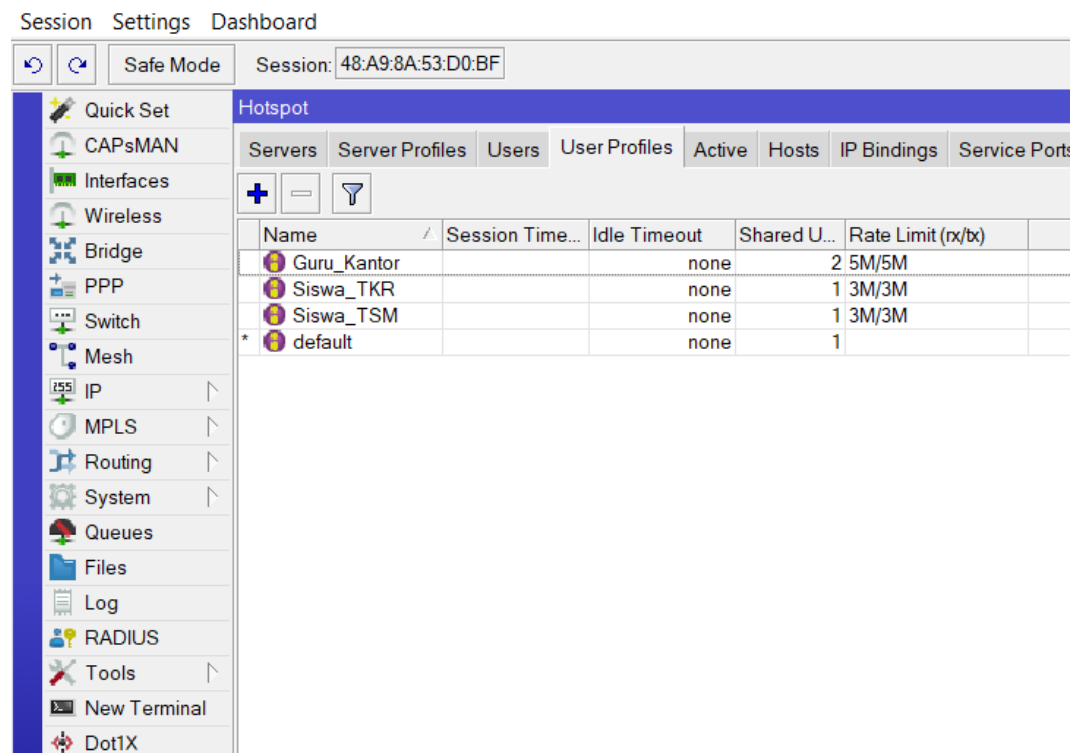
Konfigurasi *user hotspot* pada mikrotik dilakukan melalui menu *hotspot* → *users* untuk mengelola akun pengguna yang dapat mengakses jaringan internet sekolah. Pada konfigurasi ini, setiap pengguna diberikan *username* sesuai identitas masing-masing dan dikelompokkan berdasarkan *profile* akses yang telah ditentukan. Pengguna dengan *profile* *guru_kantor* digunakan untuk guru dan staf di ruang kantor, *profile* *siswa_TSM* digunakan untuk siswa ruang praktik Teknik Sepeda Motor (TSM), sedangkan *profile* *siswa_TKR* digunakan untuk siswa ruang praktik Teknik Kendaraan Ringan (TKR).

Setiap akun *hotspot* dibuat secara terpisah agar proses autentikasi dapat dilakukan menggunakan *username* dan *password* masing-masing pengguna sebelum memperoleh akses internet. Penerapan autentikasi ini bertujuan meningkatkan keamanan jaringan, mencegah penggunaan internet oleh pengguna yang tidak terdaftar, serta memudahkan administrator dalam memantau aktivitas pengguna pada jaringan sekolah.

Konfigurasi *user hotspot* juga mendukung penerapan pembagian *bandwidth* dan pengaturan hak akses berdasarkan kelompok pengguna. Guru dan staf ruang kantor memperoleh *profile* akses *guru_kantor*, sedangkan siswa memperoleh *profile*

sesuai jurusan masing-masing, yaitu siswa_TSM dan siswa_TKR. Pengelompokan tersebut membantu administrator jaringan dalam melakukan pengelolaan akses internet agar lebih terstruktur dan merata sesuai kebutuhan setiap ruangan. Penerapan *user hotspot* pada penelitian ini merupakan bagian dari implementasi metode autentikasi *user manager* untuk optimalisasi keamanan mikrotik dan pemerataan akses internet.

5.3.8 Users Profile



Sumber: Penulis, 2026

Gambar 5.30 Users Profile

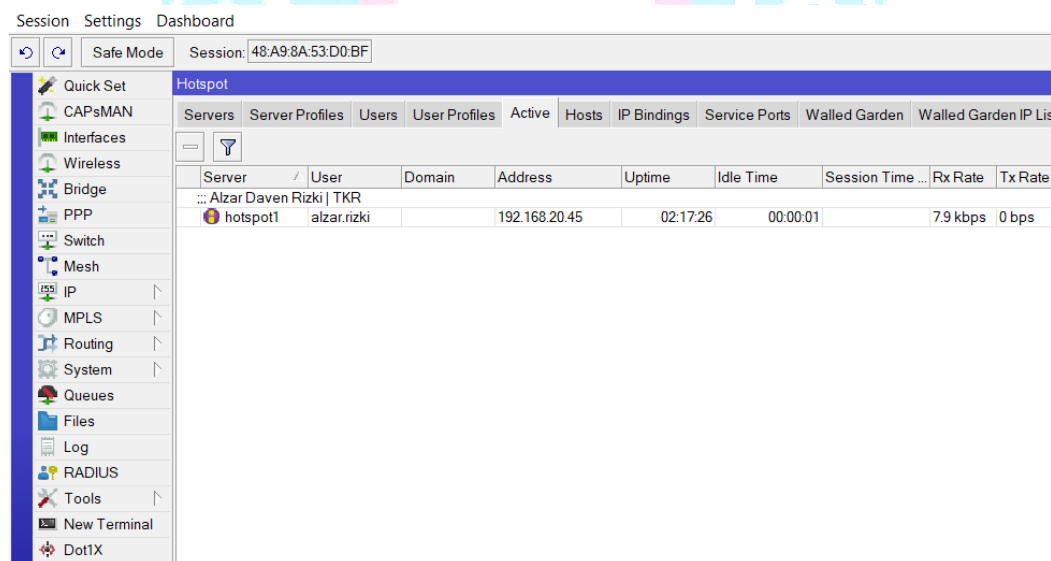
Konfigurasi *user profile* pada mikrotik dilakukan melalui menu *hotspot* → *user profiles* untuk mengatur hak akses dan pembagian *bandwidth* bagi setiap kelompok pengguna jaringan *hotspot*. Pada konfigurasi ini dibuat beberapa *profile* pengguna, yaitu guru_kantor, siswa_TKR, dan siswa_TSM. Setiap *profile* memiliki pengaturan *bandwidth* yang berbeda sesuai kebutuhan pengguna pada masing-masing ruangan dan jurusan.

Profile guru_kantor diberikan batas *bandwidth* sebesar 5M/5M karena digunakan oleh guru dan staf ruang kantor yang membutuhkan akses internet lebih

stabil untuk kegiatan administrasi dan pembelajaran. *Profile* siswa_TKR dan siswa_TSM masing-masing diberikan *bandwidth* sebesar 3M/3M untuk mendukung aktivitas belajar siswa pada ruang praktik Teknik Kendaraan Ringan (TKR) dan Teknik Sepeda Motor (TSM).

Penerapan *user profile* ini bertujuan untuk melakukan pemerataan penggunaan *bandwidth* agar koneksi internet tetap stabil dan tidak digunakan secara berlebihan oleh pengguna tertentu. Dengan adanya pembagian *profile* tersebut, administrator jaringan dapat mengelola kualitas layanan internet sesuai kebutuhan pengguna serta meningkatkan efisiensi penggunaan jaringan di lingkungan sekolah.

5.3.9 Users Active



Server	User	Domain	Address	Uptime	Idle Time	Session Time	Rx Rate	Tx Rate
hotspot1	alzar.rizki		192.168.20.45	02:17:26	00:00:01		7.9 kbps	0 bps

Sumber: Penulis, 2026

Gambar 5.31 Users Active

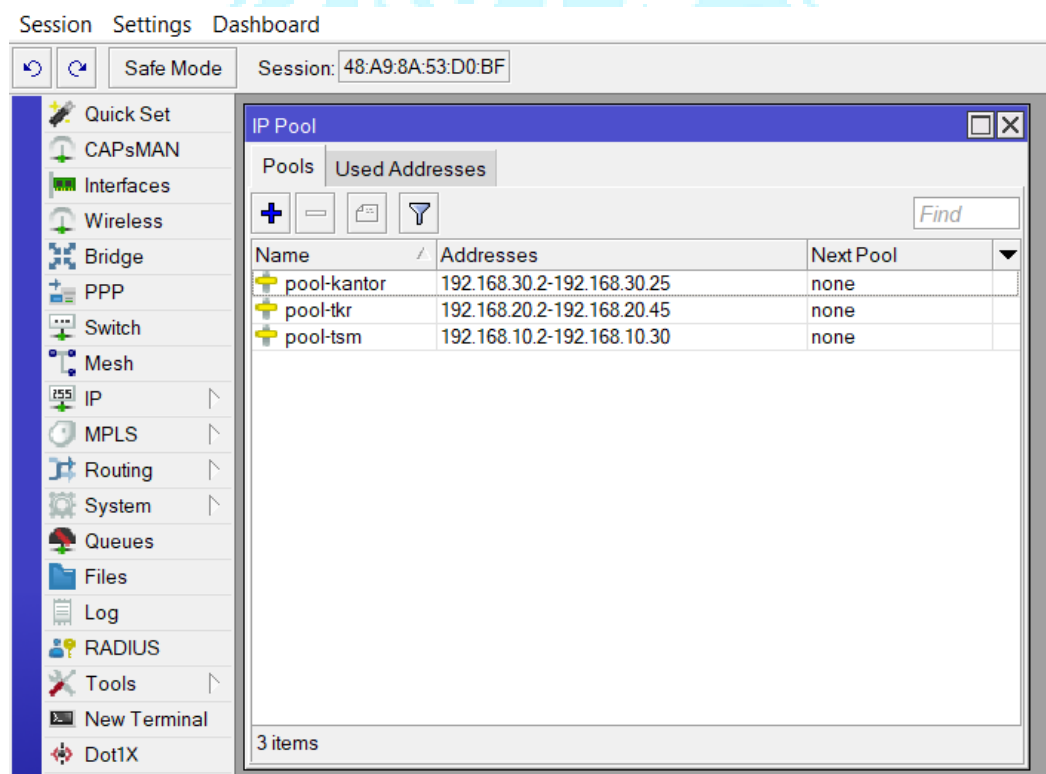
Menu *active users* pada mikrotik digunakan untuk menampilkan pengguna *hotspot* yang sedang aktif terhubung ke jaringan internet. Pada konfigurasi ini terlihat bahwa pengguna dengan *username* alzar.rizki dari kelompok TKR sedang berhasil *login* ke *hotspot server hotspot1* dan memperoleh alamat IP 192.168.20.45.

Informasi yang ditampilkan pada menu *active users* meliputi *username* pengguna, alamat IP yang digunakan, waktu koneksi (*uptime*), waktu tidak aktif (*idle time*), serta kecepatan *transfer* data (*Rx Rate* dan *Tx Rate*). Data tersebut

membantu administrator jaringan dalam memantau aktivitas pengguna yang sedang menggunakan jaringan *hotspot* secara *real-time*.

Penerapan fitur *active users* bertujuan untuk memudahkan proses monitoring pengguna jaringan, mengetahui pengguna yang sedang aktif mengakses internet, serta membantu administrator dalam melakukan pengawasan penggunaan *bandwidth* pada jaringan sekolah. Dengan adanya monitoring ini, keamanan dan kestabilan jaringan dapat lebih terjaga karena setiap pengguna yang terhubung dapat teridentifikasi dengan jelas berdasarkan akun *hotspot* masing-masing.

5.3.10 IP Pool



Sumber: Penulis, 2026

Gambar 5.32 IP Pool

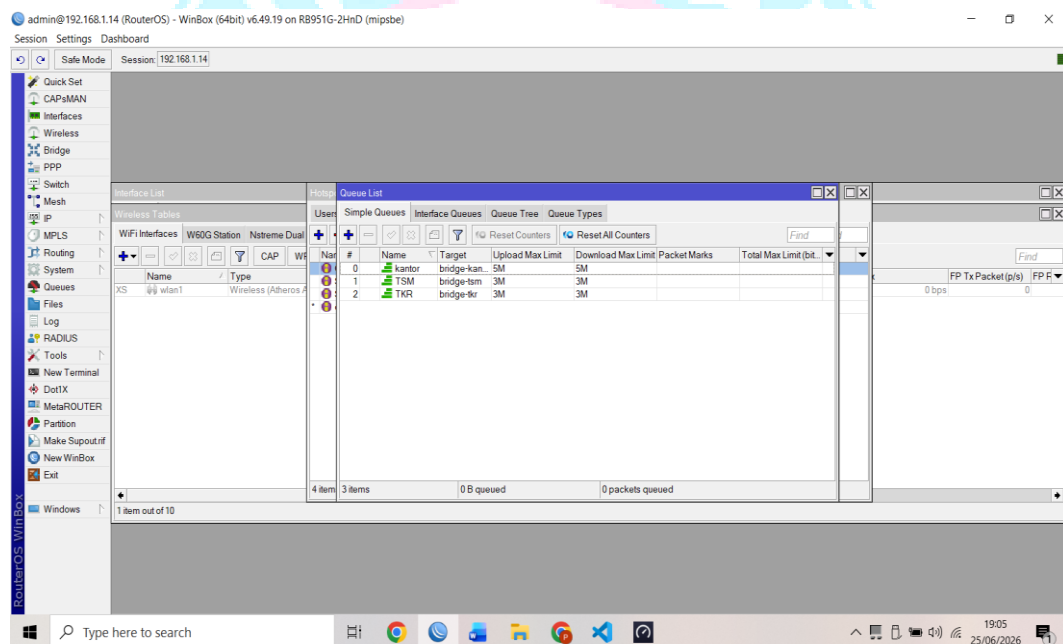
Menu *IP Pool* pada mikrotik digunakan untuk menentukan rentang alamat IP yang akan dibagikan kepada pengguna jaringan secara otomatis. Pada konfigurasi ini terdapat tiga buah *IP Pool* yang digunakan untuk membedakan jaringan berdasarkan lokasi dan pengguna, yaitu *pool-kantor*, *pool-tnr*, dan *pool-tsm*.

Pool pool-kantor menggunakan rentang alamat IP 192.168.30.2 – 192.168.30.25 yang digunakan untuk perangkat pada jaringan ruang kantor. *Pool*

pool-tkr menggunakan rentang alamat IP 192.168.20.2 – 192.168.20.45 yang digunakan pada jaringan ruang praktik TKR. *Pool pool*-tsm menggunakan rentang alamat IP 192.168.10.2 – 192.168.10.30 yang digunakan pada jaringan ruang praktik TSM.

Konfigurasi IP *Pool* bertujuan untuk mempermudah pengelolaan alamat IP pada masing-masing jaringan sehingga pembagian IP menjadi lebih teratur dan mengurangi kemungkinan terjadinya konflik alamat IP antar perangkat. Dengan pemisahan *pool* berdasarkan ruangan atau jurusan, administrator jaringan juga lebih mudah melakukan monitoring dan manajemen pengguna jaringan *hotspot*.

5.3.11 Simple Queue



Sumber: Penulis, 2026

Gambar 5.33 Simple Queue

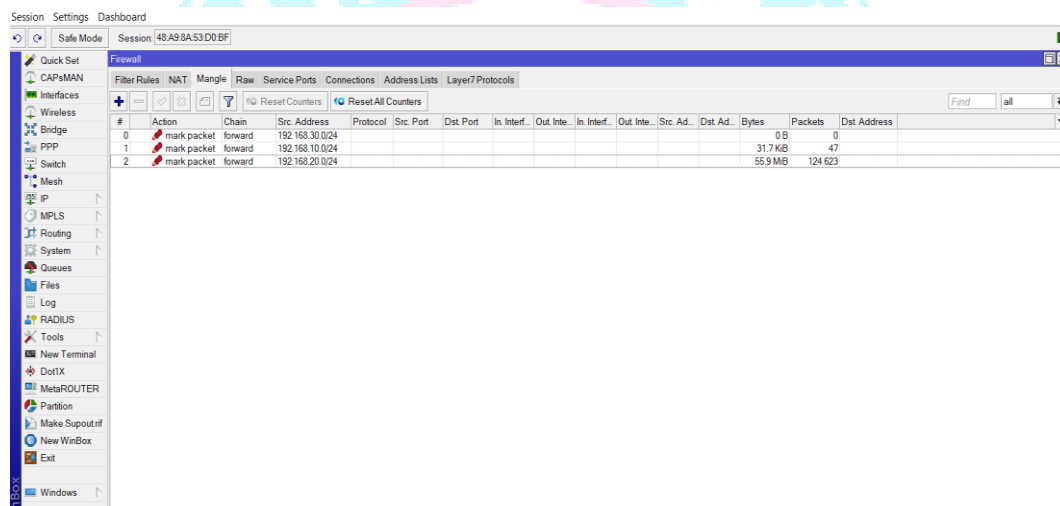
Menu *Simple Queue* pada mikrotik digunakan untuk melakukan pengaturan dan pembatasan *bandwidth* pada setiap segmen jaringan yang terhubung ke *router*. Pada konfigurasi ini terdapat tiga buah *simple queue* yaitu Kantor, TKR, dan TSM yang digunakan untuk mengatur alokasi *bandwidth* pada masing-masing jaringan di lingkungan sekolah.

Simple queue kantor digunakan untuk mengatur *bandwidth* jaringan ruang kantor dengan batas maksimum sebesar 5 Mbps. *Simple queue* TKR digunakan

untuk mengatur *bandwidth* jaringan TKR dengan batas maksimum sebesar 3 Mbps. Sedangkan *simple queue* TSM digunakan untuk mengatur *bandwidth* jaringan TSM dengan batas maksimum sebesar 3 Mbps.

Penerapan *simple queue* dilakukan agar penggunaan *bandwidth* internet pada setiap jaringan dapat terkontrol sesuai kebutuhan masing-masing bagian. Dengan adanya pembatasan *bandwidth* tersebut, penggunaan internet menjadi lebih stabil dan merata karena setiap jaringan memperoleh alokasi *bandwidth* yang telah ditentukan sehingga dapat mengurangi terjadinya penggunaan *bandwidth* secara berlebihan pada salah satu jaringan.

5.3.12 Mangle



Sumber: Penulis, 2026

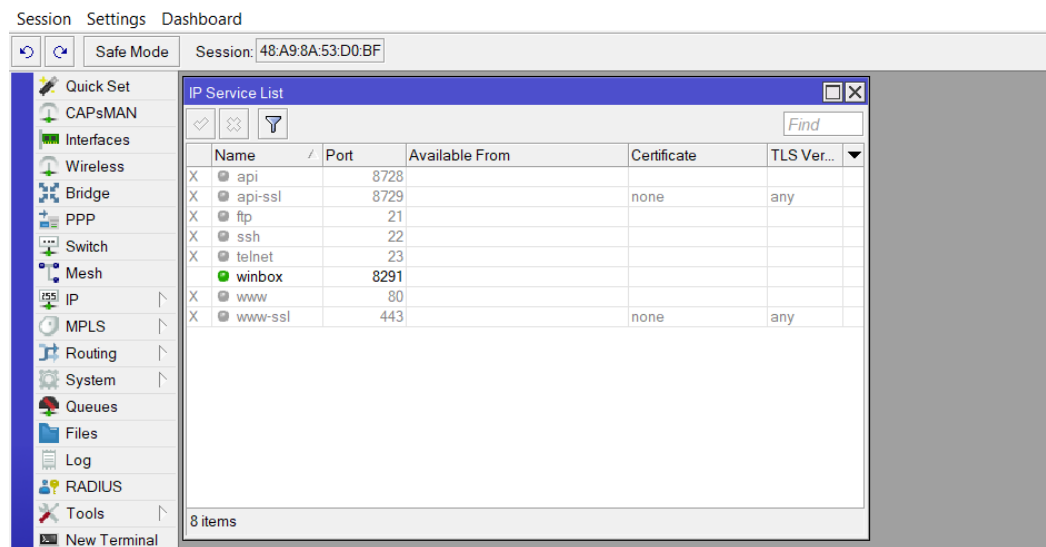
Gambar 5.34 Mangle

Menu *mangle* pada mikrotik digunakan untuk melakukan penandaan (*mark packet*) terhadap paket data yang melewati jaringan. Penandaan paket ini bertujuan untuk membedakan trafik jaringan berdasarkan sumber alamat IP sehingga dapat digunakan dalam proses manajemen *bandwidth* menggunakan *queue tree*.

Pada konfigurasi ini terdapat tiga aturan *mark packet* pada *chain forward*. Aturan pertama digunakan untuk menandai paket data yang berasal dari jaringan 192.168.30.0/24 sebagai jaringan ruang kantor. Aturan kedua digunakan untuk menandai paket data dari jaringan 192.168.10.0/24 sebagai jaringan Teknik Sepeda Motor (TSM). Aturan ketiga digunakan untuk menandai paket data dari jaringan 192.168.20.0/24 sebagai jaringan Teknik Kendaraan Ringan (TKR).

Penerapan konfigurasi *mangle* dilakukan agar setiap trafik jaringan dapat dikenali dan dipisahkan sesuai kelompok pengguna. Penandaan paket tersebut kemudian digunakan sebagai acuan dalam pengaturan *bandwidth* pada *queue tree*, sehingga pembagian *bandwidth* internet dapat berjalan lebih teratur, stabil, dan sesuai dengan kebutuhan masing-masing jaringan.

5.3.13 Blok Akses Konfigurasi



Sumber: Penulis, 2026

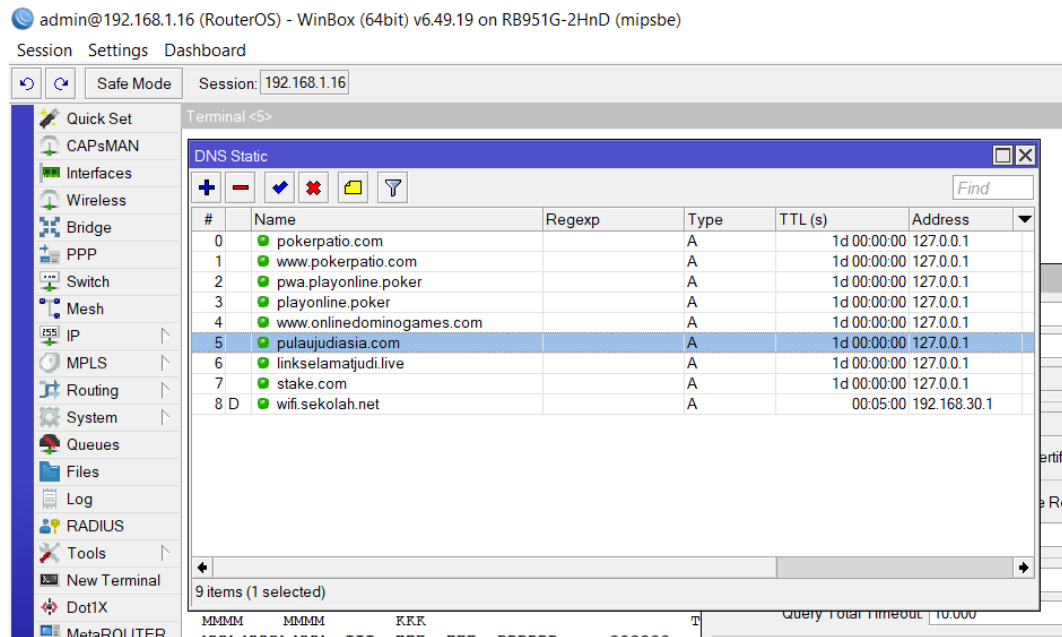
Gambar 5.35 Blok Akses Konfigurasi

Menu *IP service list* pada mikrotik digunakan untuk mengatur layanan akses yang diperbolehkan pada *router*. Pada konfigurasi ini hanya layanan *winbox* yang diaktifkan, sedangkan layanan lainnya seperti *api*, *api-ssl*, *ftp*, *ssh*, *telnet*, *www*, dan *www-ssl* dinonaktifkan.

Layanan *winbox* berjalan pada *port* 8291 dan digunakan oleh administrator jaringan untuk melakukan konfigurasi serta pengelolaan *router* mikrotik. Sementara itu layanan *www* dan *www-ssl* yang digunakan untuk akses *webfig* melalui browser dinonaktifkan guna meningkatkan keamanan perangkat jaringan.

Penerapan konfigurasi ini bertujuan untuk membatasi akses administrasi *router* agar hanya dapat dilakukan menggunakan aplikasi *winbox*. Dengan menonaktifkan layanan yang tidak digunakan, risiko akses tidak sah terhadap *router* dapat diminimalkan sehingga keamanan jaringan menjadi lebih terjaga.

5.3.14 Pengamanan Jaringan dengan Pemblokiran *Website*



Sumber: Penulis, 2026

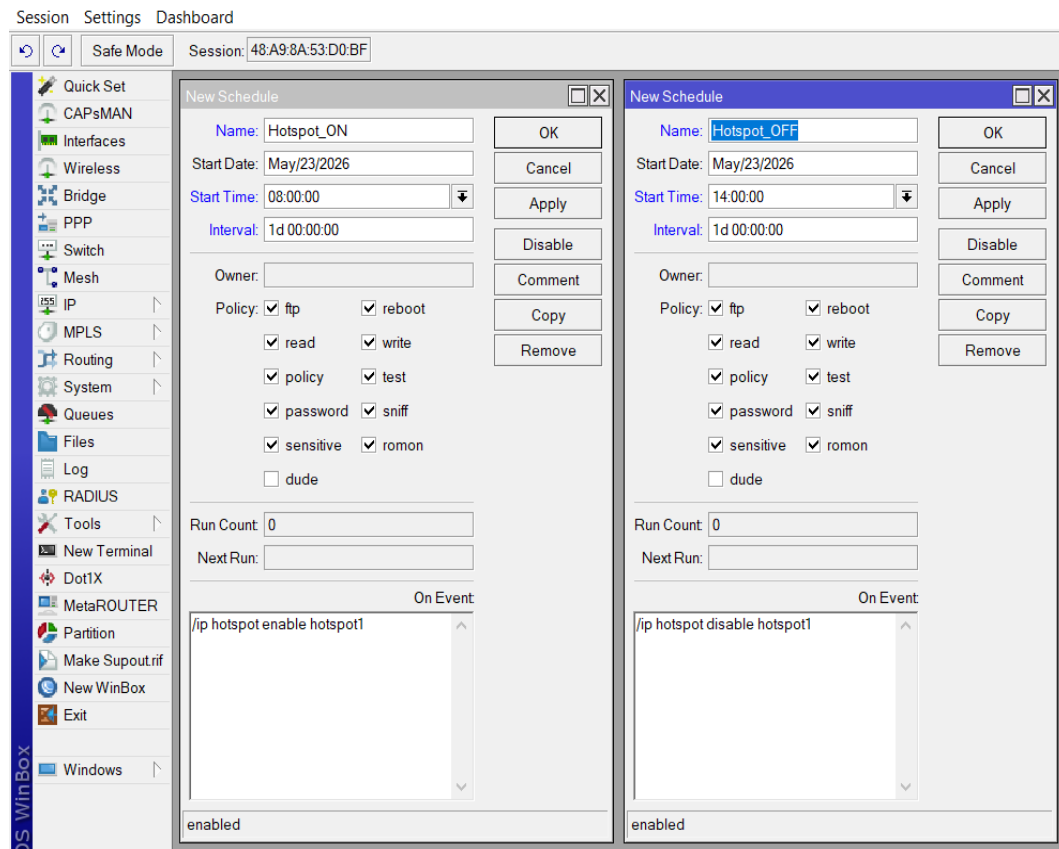
Gambar 5.36 Blok *Website*

Menu DNS *static* pada mikrotik digunakan untuk melakukan pengaturan resolusi nama domain ke alamat IP tertentu. Pada konfigurasi yang ditunjukkan pada gambar, beberapa domain yang dikategorikan sebagai situs yang tidak mendukung kegiatan pendidikan dikonfigurasi untuk diarahkan ke alamat IP 127.0.0.1. Dengan metode ini, ketika pengguna mencoba mengakses domain yang telah ditentukan, proses resolusi DNS akan mengarah ke alamat lokal sehingga halaman *website* tidak dapat ditampilkan.

Konfigurasi DNS *static* tersebut diterapkan sebagai salah satu mekanisme penyaringan akses internet pada jaringan sekolah. Melalui pengaturan ini, administrator jaringan dapat membatasi akses ke konten yang tidak sesuai dengan lingkungan pendidikan, sehingga penggunaan internet oleh siswa dan pengguna jaringan lainnya dapat lebih terkontrol.

Selain berfungsi sebagai media pemblokiran akses, DNS *static* juga dapat digunakan untuk mengarahkan nama domain tertentu ke layanan yang berada di dalam jaringan lokal. Penerapan konfigurasi ini membantu mempermudah pengelolaan akses jaringan sekaligus meningkatkan keamanan dan efektivitas penggunaan internet di lingkungan sekolah.

5.3.15 Schedule



Sumber: Penulis, 2026

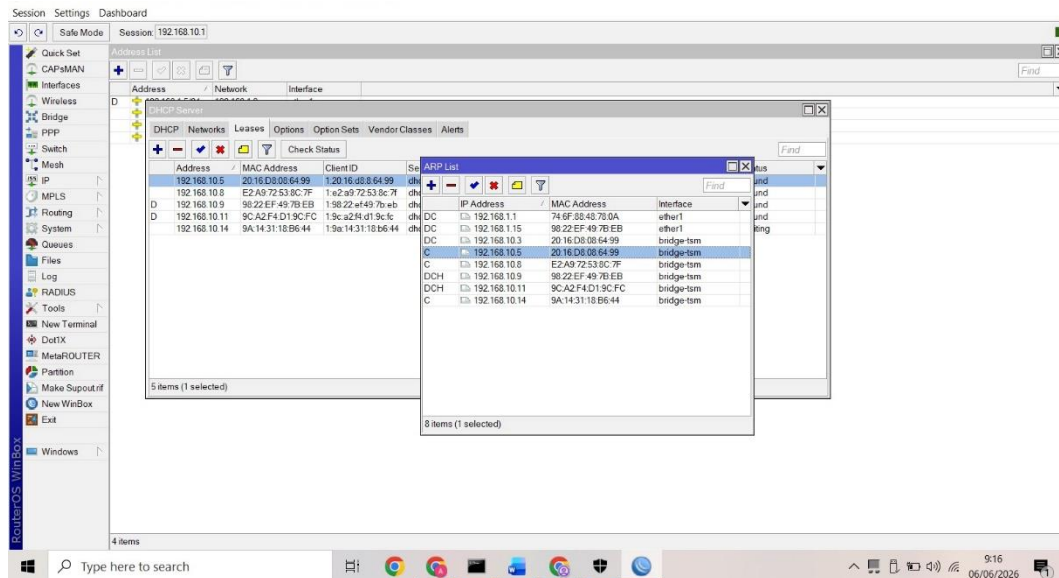
Gambar 5.37 Schedule

Pada konfigurasi tersebut terdapat dua buah *scheduler*, yaitu *hotspot_ON* dan *hotspot_OFF*. *Scheduler hotspot_ON* dijalankan setiap hari pada pukul 08:00:00 dengan perintah `/ip hotspot enable hotspot1` untuk mengaktifkan layanan *hotspot* secara otomatis. Sedangkan *scheduler hotspot_OFF* dijalankan setiap hari pada pukul 14:00:00 dengan perintah `/ip hotspot disable hotspot1` untuk menonaktifkan.

Pengaturan *interval* 1d 00:00:00 menunjukkan bahwa *scheduler* akan berjalan otomatis setiap satu hari sekali sesuai waktu yang telah ditentukan. Dengan konfigurasi ini jaringan *hotspot* hanya dapat digunakan pada jam operasional sekolah, sedangkan di luar jam tersebut pengguna tidak dapat terhubung ke layanan *hotspot* meskipun jaringan *wi-fi* masih aktif dan terlihat pada perangkat pengguna. Penerapan fitur *scheduler* bertujuan untuk mengontrol penggunaan internet agar lebih teratur, meningkatkan keamanan jaringan, serta mengurangi penyalahgunaan akses internet di luar jam kegiatan belajar mengajar.

5.3.16 Konfigurasi *Firewall Client*

a. TSM

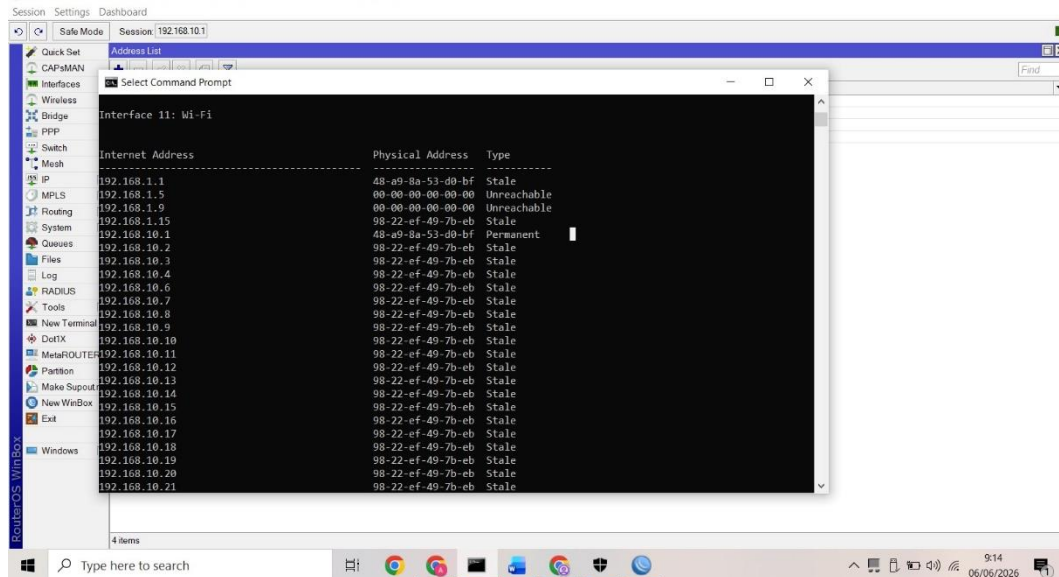


Sumber: Penulis, 2026

Gambar 5.38 Konfigurasi *Firewall Client* TSM

Pada konfigurasi sistem keamanan jaringan ini, pengelolaan tabel IP-to-MAC address dilakukan secara terpusat melalui fitur *DHCP server leases* dan *ARP list* pada mikrotik. Berdasarkan implementasi di lapangan, perangkat klien yang valid (seperti laptop pengujian) diikat secara permanen menggunakan metode *Static Binding*. Hal ini terlihat pada menu *DHCP Leases* di mana IP Address 192.168.10.5 telah diikat secara statis dengan MAC address 20:16:D8:08:64:99.

Pengikatan statis tersebut secara otomatis akan tersinkronisasi ke dalam tabel *ARP list* dengan tanda *flag C (complete / static)*, seperti yang ditunjukkan pada entri IP 192.168.10.5 pada *interface bridge-tsm*. Sementara itu, perangkat penyerang atau pengguna asing yang mencoba masuk tanpa izin akan terdeteksi dengan *flag DCH (dynamic, DHCP, active hotspot)* atau *DC*, seperti pada IP 192.168.10.9 dengan MAC address 98:22:EF:49:7B:EB.

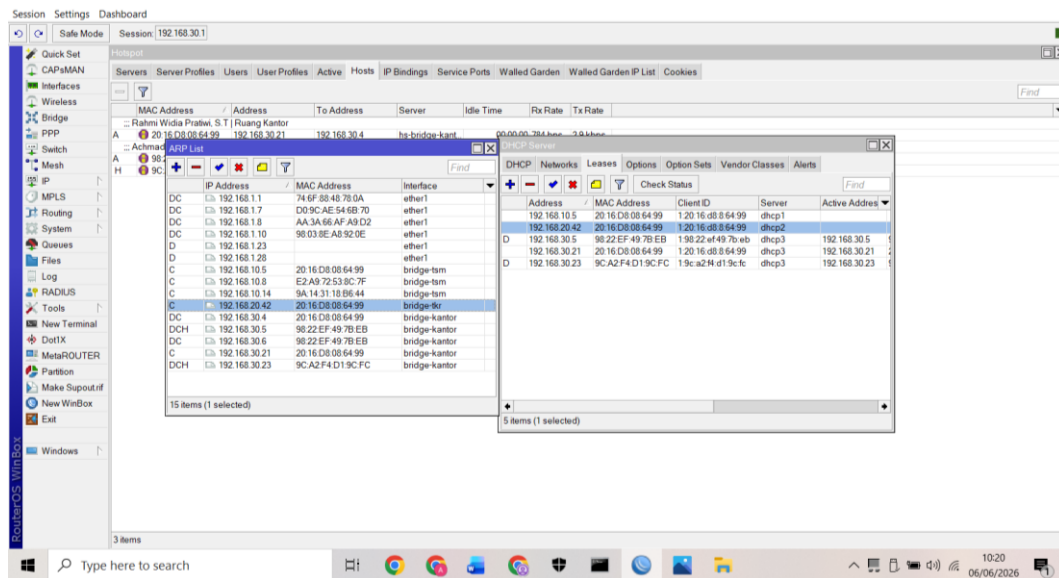


Sumber: Penulis, 2026

Gambar 5.39 Konfigurasi *Firewall* Tambahan *Client* TSM

Gambar tersebut secara jelas menunjukkan visualisasi penambahan konfigurasi keamanan mandiri yang dilakukan langsung pada sisi perangkat klien menggunakan utilitas *command prompt* khusus untuk area jaringan TSM. Melalui eksekusi perintah pengikatan statis (*static neighbor binding*), jalur komunikasi menuju IP *gateway* utama jaringan TSM yaitu 192.168.10.1 berhasil dikunci secara permanen yang ditandai dengan munculnya status *permanent* pada tabel sistem. Langkah ini sengaja diterapkan sebagai benteng pertahanan terakhir di tingkat pengguna guna mengantisipasi serangan manipulasi data lokal dari pihak-pihak yang tidak bertanggung jawab di dalam jaringan lokal TSM tersebut.

b. TKR

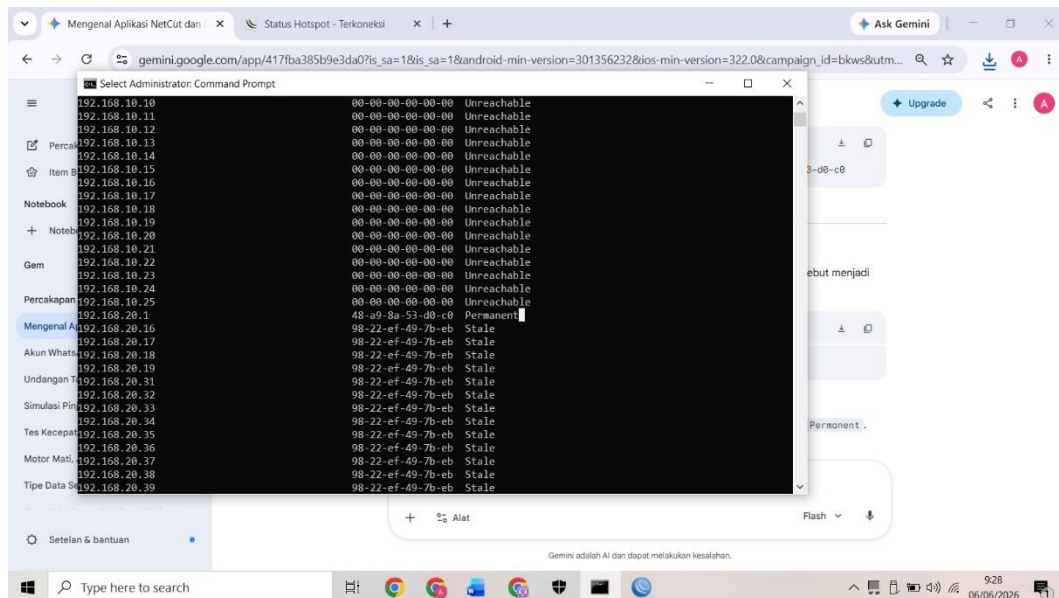


Sumber: Penulis, 2026

Gambar 5.40 Konfigurasi *Firewall Client* TKR

Pada konfigurasi sistem keamanan jaringan ini, pengelolaan tabel IP-to-MAC address dilakukan secara terpusat melalui fitur *DHCP server leases* dan *ARP list* pada mikrotik. Berdasarkan implementasi di lapangan, perangkat klien yang valid (seperti laptop pengujian) diikat secara permanen menggunakan metode *static binding*. Hal ini terlihat pada menu *DHCP leases* di mana IP address 192.168.20.42 telah diikat secara statis dengan MAC address 20:16:D8:08:64:99 pada server dhcp2.

Pengikatan statis tersebut secara otomatis akan tersinkronisasi ke dalam tabel *ARP list* dengan tanda flag C (*complete / static*), seperti yang ditunjukkan pada entri IP 192.168.20.42 pada interface *bridge-kr*. Sementara itu, perangkat penyerang atau pengguna asing yang mencoba masuk tanpa izin akan terdeteksi dengan flag DCH (*dynamic, DHCP, active hotspot*) atau DC, seperti pada IP 192.168.20.45 dengan MAC address 98:22:EF:49:7B:EB pada interface *bridge-kr*.

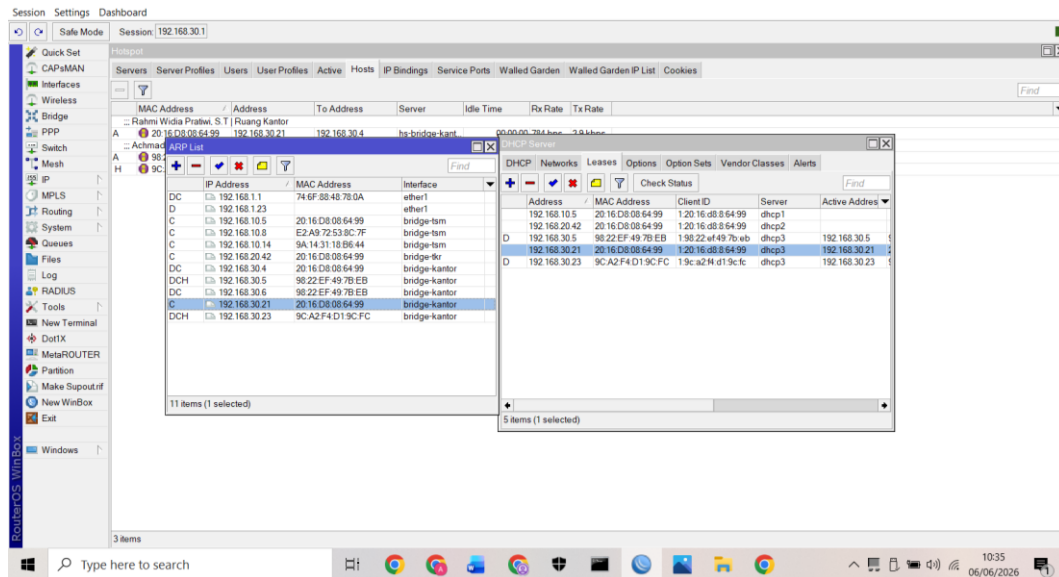


Sumber: Penulis, 2026

Gambar 5.41 Konfigurasi *Firewall* Tambahan *Client* TKR

Gambar tersebut secara jelas menunjukkan visualisasi penambahan konfigurasi keamanan mandiri yang dilakukan langsung pada sisi perangkat klien menggunakan utilitas *command prompt* khusus untuk area jaringan TKR. Melalui eksekusi perintah pengikatan statis (*static neighbor binding*), jalur komunikasi menuju IP *gateway* utama jaringan TSM yaitu 192.168.20.1 berhasil dikunci secara permanen yang ditandai dengan munculnya status permanent pada tabel sistem. Langkah ini sengaja diterapkan sebagai benteng pertahanan terakhir di tingkat pengguna guna mengantisipasi serangan manipulasi data lokal dari pihak-pihak yang tidak bertanggung jawab di dalam jaringan lokal TKR tersebut.

c. Ruang Kantor

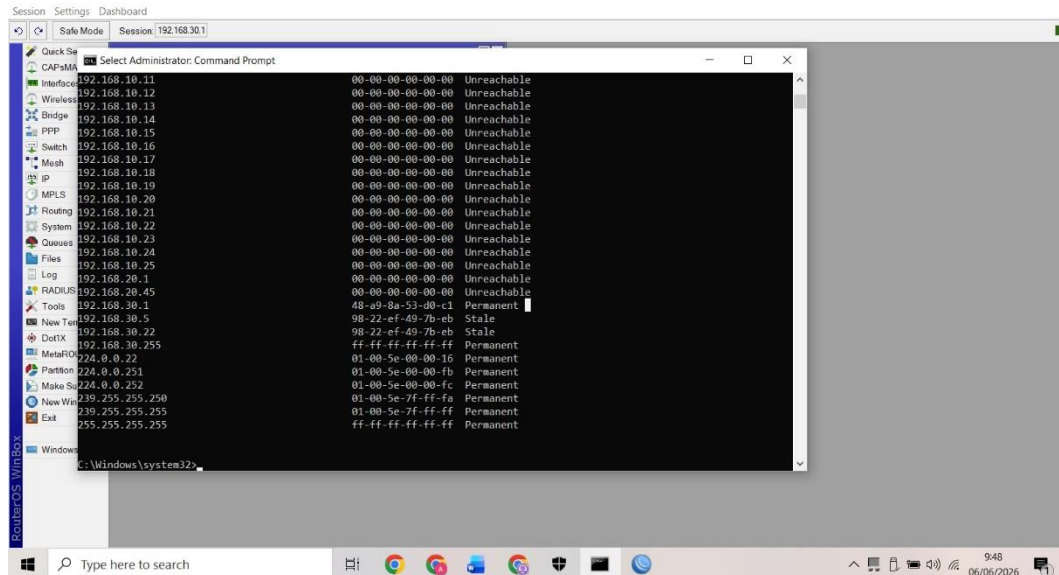


Sumber: Penulis, 2026

Gambar 5.42 Konfigurasi *Firewall Client* Kantor

Pada konfigurasi sistem keamanan jaringan ini, pengelolaan tabel IP-to-MAC address dilakukan secara terpusat melalui fitur *DHCP server leases* dan *ARP list* pada mikrotik. Berdasarkan implementasi di lapangan, perangkat klien yang valid (seperti laptop pengujian) diikat secara permanen menggunakan metode *static binding*. Hal ini terlihat pada menu *DHCP leases* di mana IP address 192.168.20.42 telah diikat secara statis dengan MAC address 20:16:D8:08:64:99 pada server dhcp2.

Pengikatan statis tersebut secara otomatis akan tersinkronisasi ke dalam tabel *ARP list* dengan tanda *flag C* (*complete / static*), seperti yang ditunjukkan pada entri IP 192.168.20.42 pada interface *bridge-kr*. Sementara itu, perangkat penyerang atau pengguna asing yang mencoba masuk tanpa izin akan terdeteksi dengan flag *DCH* (*dynamic, DHCP, active hotspot*) atau *DC*, seperti pada IP 192.168.30.5 dengan MAC address 98:22:EF:49:7B:EB pada interface *bridge-kantor*.



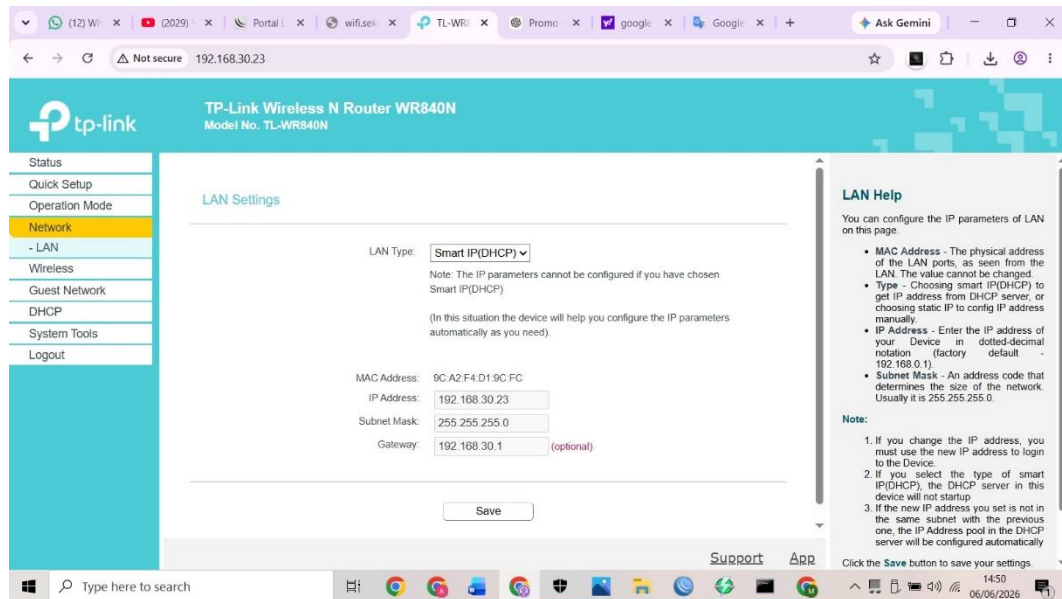
Sumber: Penulis, 2026

Gambar 5.43 Konfigurasi *Firewall* Tambahan *Client* Kantor

Gambar tersebut secara jelas menunjukkan visualisasi penambahan konfigurasi keamanan mandiri yang dilakukan langsung pada sisi perangkat klien menggunakan utilitas *command prompt* khusus untuk area jaringan TKR. Melalui eksekusi perintah pengikatan statis (*static neighbor binding*), jalur komunikasi menuju IP *gateway* utama jaringan TSM yaitu 192.168.20.1 berhasil dikunci secara permanen yang ditandai dengan munculnya status permanent pada tabel sistem. Langkah ini sengaja diterapkan sebagai benteng pertahanan terakhir di tingkat pengguna guna mengantisipasi serangan manipulasi data lokal dari pihak-pihak yang tidak bertanggung jawab di dalam jaringan lokal TKR tersebut.

5.4 Konfigurasi *Access point*

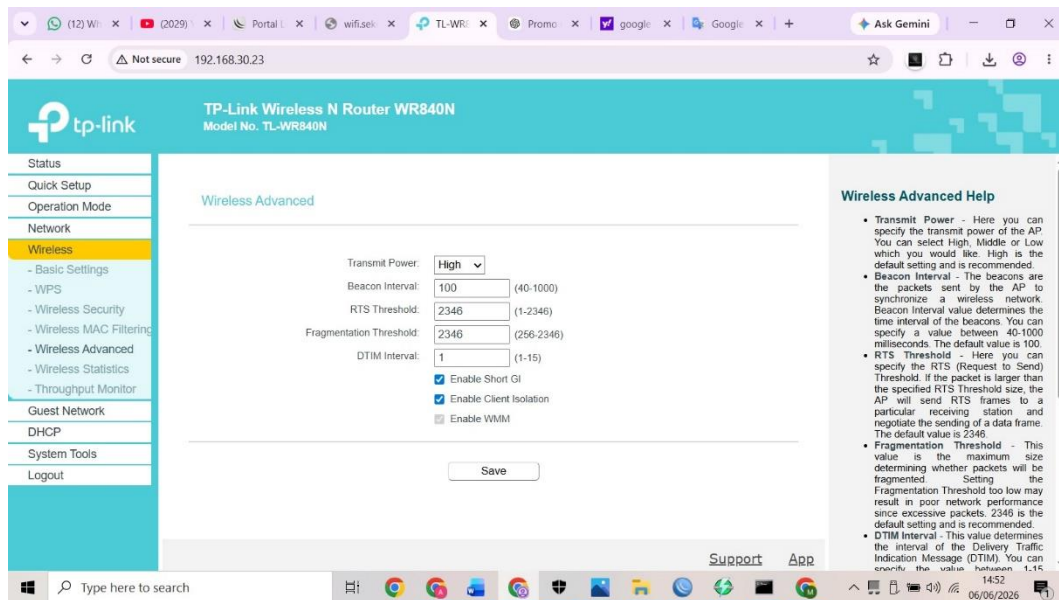
5.4.1 Konfigurasi AP Kantor



Sumber: Penulis, 2026

Gambar 5.44 DHCP AP Kantor

Tahap pengamanan dilanjutkan dengan melakukan konfigurasi langsung pada perangkat keras *access point* (AP) TP-Link TL-WR840N yang bertugas memancarkan sinyal di area kantor. Langkah awal dilakukan dengan menyelaraskan parameter jaringan pada menu *network* LAN. Jenis LAN diatur menggunakan mode *smart* IP (DHCP) dengan perolehan IP *address* statis eksternal pada 192.168.30.23 yang menginduk langsung ke *gateway* utama *router* (192.168.30.1). Penyetelan ini bertujuan agar manajemen perangkat AP kantor tetap berada dalam satu segmen kontrol yang valid.

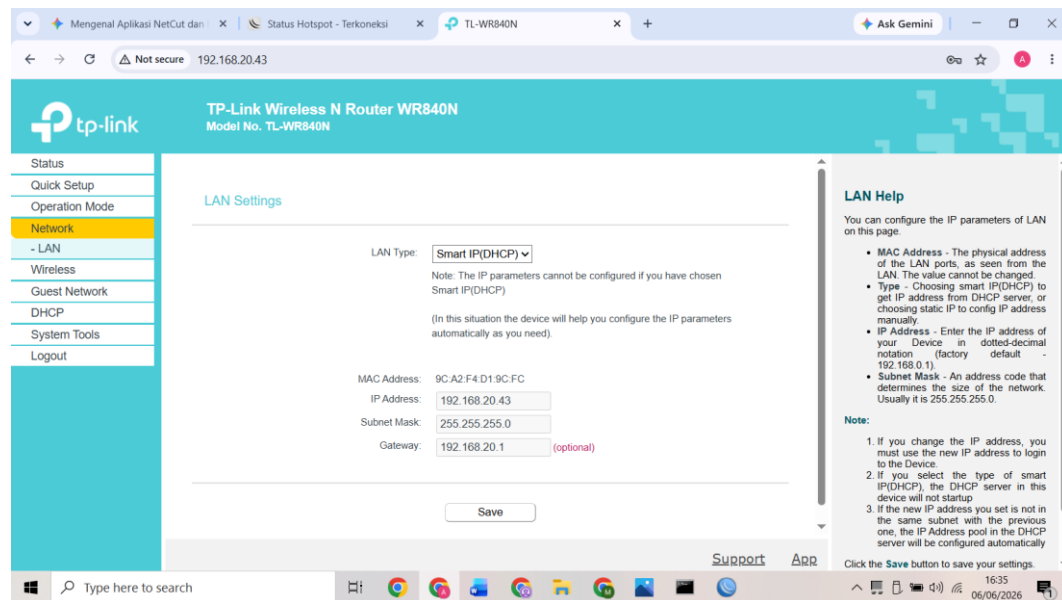


Sumber: Penulis, 2026

Gambar 5.45 *Enable Client Isolation Kantor*

Sebagai inti dari pertahanan lokal di level udara (*layer 2*), konfigurasi dilanjutkan ke menu *wireless* berikutnya *wireless advanced*. Pada halaman ini, dilakukan tindakan *preventif* dengan memberikan tanda centang aktif pada opsi *enable client isolation*. Pengaktifan fitur ini secara instan memutus hak komunikasi horizontal antar perangkat nirkabel yang terhubung ke AP kantor. Efeknya, setiap klien dipaksa bergerak secara vertikal hanya menuju internet, sehingga menutup celah aksi pemindaian maupun eksekusi pemutusan koneksi sepihak oleh sesama pengguna *hotspot*.

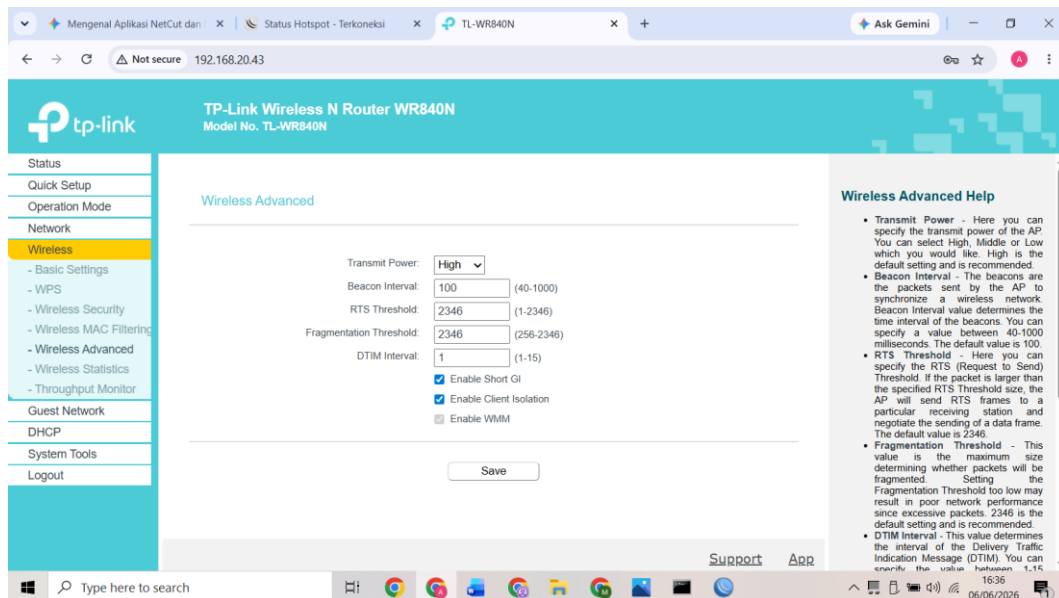
5.4.2 Konfigurasi AP TKR



Sumber: Penulis, 2026

Gambar 5.46 DHCP AP TKR

Tahap pengamanan dilanjutkan dengan melakukan konfigurasi langsung pada perangkat keras *access point* (AP) TP-Link TL-WR840N yang bertugas memancarkan sinyal di area TKR. Langkah awal dilakukan dengan menyelaraskan parameter jaringan pada menu *network* LAN. Jenis LAN diatur menggunakan mode *smart* IP (DHCP) dengan perolehan IP *address* statis eksternal pada 192.168.20.43 yang menginduk langsung ke *gateway* utama *router* (192.168.20.1). Penyetelan ini bertujuan agar manajemen perangkat AP TKR tetap berada dalam satu segmen kontrol yang valid.

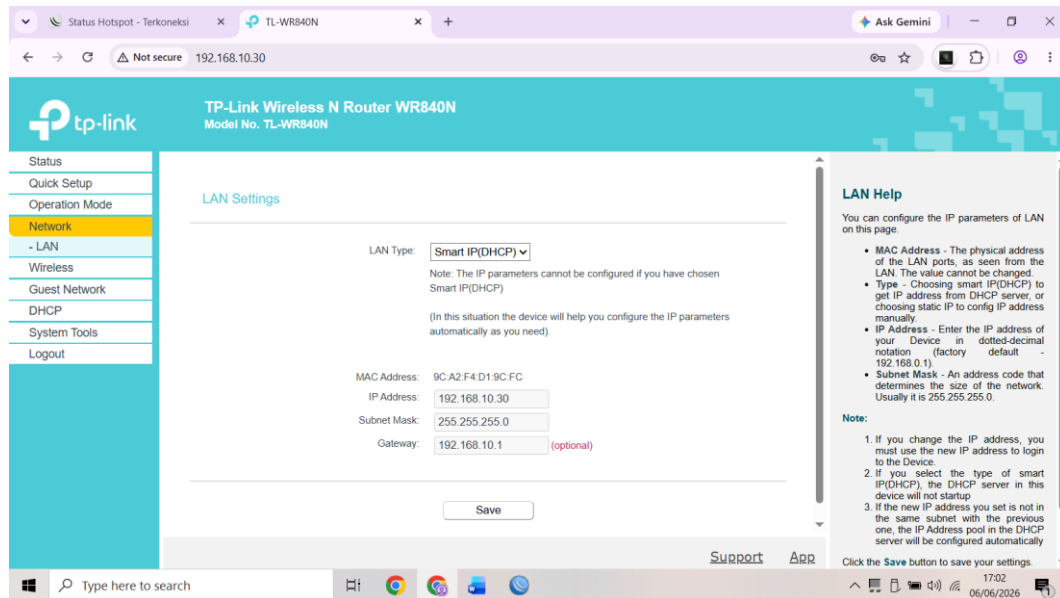


Sumber: Penulis, 2026

Gambar 5.47 Enable Client Isolation TKR

Sebagai inti dari pertahanan lokal di level udara (*layer 2*), konfigurasi dilanjutkan ke menu *wireless* berikutnya *wireless advanced*. Pada halaman ini, dilakukan tindakan *preventif* dengan memberikan tanda centang aktif pada opsi *enable client isolation*. Pengaktifan fitur ini secara instan memutus hak komunikasi horizontal antar perangkat nirkabel yang terhubung ke AP TKR. Efeknya, setiap klien dipaksa bergerak secara vertikal hanya menuju internet, sehingga menutup celah aksi pemindaian maupun eksekusi pemutusan koneksi sepihak oleh sesama pengguna *hotspot*.

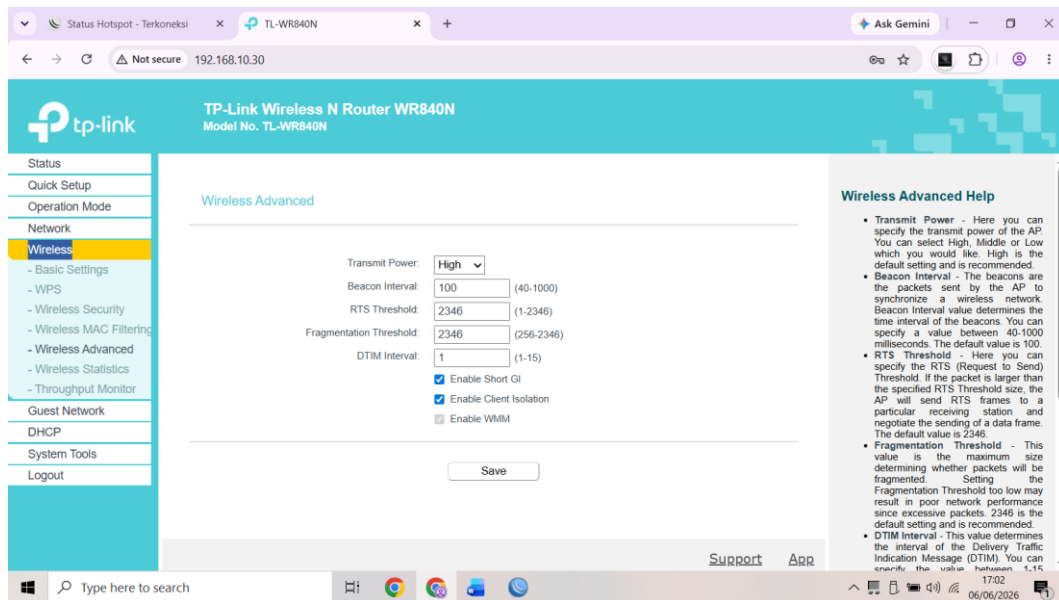
5.4.3 Konfigurasi AP TSM



Sumber: Penulis, 2026

Gambar 5.48 DHCP AP TSM

Tahap pengamanan dilanjutkan dengan melakukan konfigurasi langsung pada perangkat keras *access point* (AP) TP-Link TL-WR840N yang bertugas memancarkan sinyal di area TSM. Langkah awal dilakukan dengan menyelaraskan parameter jaringan pada menu *network* LAN. Jenis LAN diatur menggunakan mode *smart* IP (DHCP) dengan perolehan IP *address* statis eksternal pada 192.168.10.30 yang menginduk langsung ke *gateway* utama *router* (192.168.10.1). Penyetelan ini bertujuan agar manajemen perangkat AP TSM tetap berada dalam satu segmen kontrol yang valid.



Sumber: Penulis, 2026

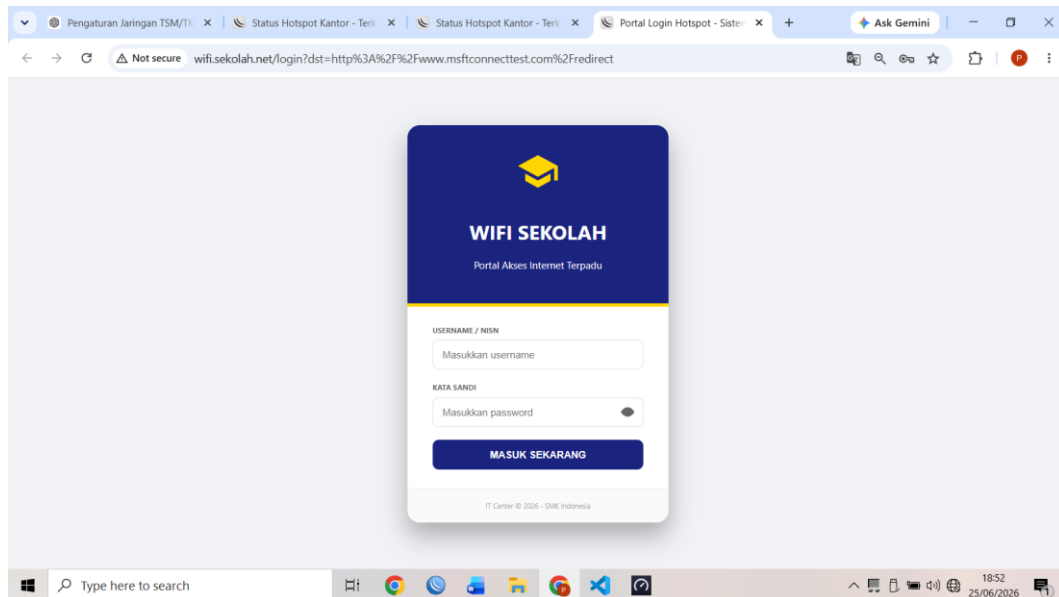
Gambar 5.49 Enable Client Isolation TSM

Sebagai inti dari pertahanan lokal di level udara (*layer 2*), konfigurasi dilanjutkan ke menu *wireless* berikutnya *wireless advanced*. Pada halaman ini, dilakukan tindakan *preventif* dengan memberikan tanda centang aktif pada opsi *enable client isolation*. Pengaktifan fitur ini secara instan memutus hak komunikasi horizontal antar perangkat nirkabel yang terhubung ke AP TSM. Efeknya, setiap klien dipaksa bergerak secara vertikal hanya menuju internet, sehingga menutup celah aksi pemindaian maupun eksekusi pemutusan koneksi sepihak oleh sesama pengguna *hotspot*.

5.5 Pengujian Jaringan

5.5.1 Pengujian Menggunakan *Web Browser / Chrome*

1. *Captive Portal Form Login*



Sumber: Penulis, 2026

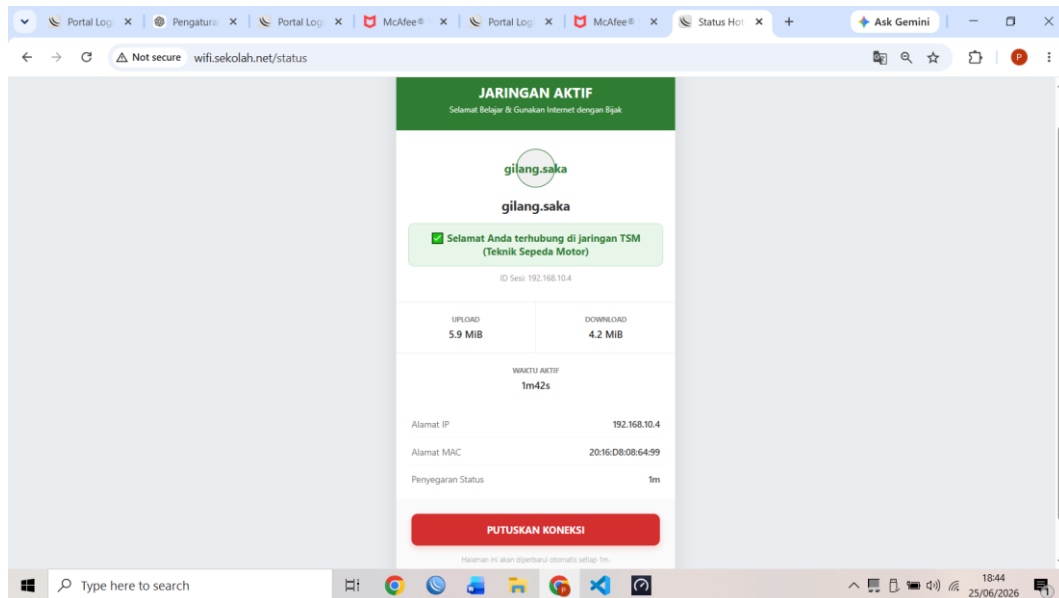
Gambar 5.50 *Captive Portal Form Login*

Pengujian jaringan dilakukan menggunakan *website google chrome* untuk memastikan layanan *hotspot* dapat berjalan dengan baik pada perangkat pengguna. Pada tahap pengujian ini, perangkat pengguna terlebih dahulu dihubungkan ke jaringan *wi-fi* sekolah yang telah dikonfigurasi pada mikrotik.

Setelah perangkat berhasil terhubung ke jaringan *wi-fi*, sistem secara otomatis mengarahkan pengguna menuju halaman *captive portal login hotspot* dengan alamat domain *wifi.sekolah.net*. Halaman *login* tersebut digunakan sebagai media autentikasi pengguna sebelum dapat mengakses layanan internet. Pada halaman *login* tersedia *form username* dan *password* yang harus diisi sesuai akun *hotspot* yang telah dibuat sebelumnya pada mikrotik.

Tampilan *captive portal* dirancang menggunakan antarmuka sederhana dan responsif sehingga dapat digunakan dengan mudah oleh pengguna baik melalui laptop maupun *smartphone*. Pengujian ini bertujuan untuk memastikan bahwa fitur *hotspot*, *DNS redirect*, serta autentikasi pengguna berjalan sesuai konfigurasi yang telah diterapkan pada jaringan sekolah.

2. Captive Portal Form Status



Sumber: Penulis, 2026

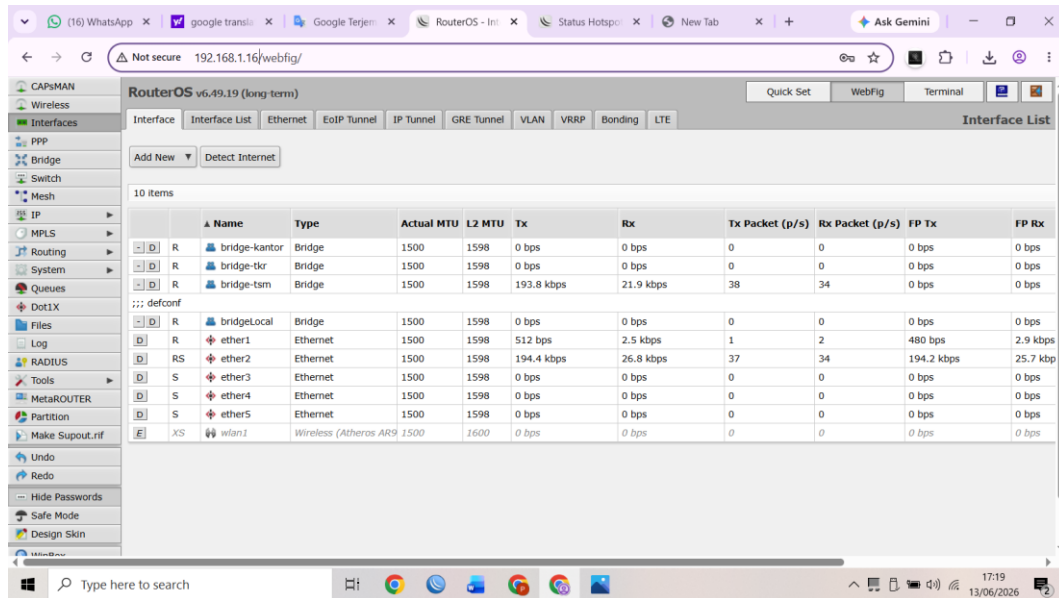
Gambar 5.51 Captive Portal Form Status

Setelah pengguna berhasil melakukan *login* pada halaman *captive portal*, sistem *hotspot* mikrotik akan menampilkan halaman status koneksi jaringan. Halaman ini digunakan untuk memberikan informasi mengenai status akses internet pengguna yang sedang aktif pada jaringan *hotspot* sekolah.

Pada halaman status tersebut ditampilkan beberapa informasi seperti *username* pengguna, alamat IP yang diperoleh perangkat, alamat MAC perangkat, jumlah data *upload* dan *download*, serta lama waktu koneksi pengguna pada jaringan *hotspot*. Selain itu tersedia tombol *putuskan koneksi* yang digunakan untuk menghentikan sesi koneksi *hotspot* secara manual.

Berdasarkan hasil pengujian, pengguna dengan *username* *gilang.saka* berhasil melakukan autentikasi dan memperoleh alamat IP 192.168.10.4 dari jaringan *hotspot* TSM. Hal ini menunjukkan bahwa konfigurasi *hotspot*, DHCP, autentikasi pengguna, serta pengalokasian IP *address* pada mikrotik telah berjalan dengan baik sesuai rancangan sistem jaringan yang diterapkan.

3. Pengujian Pemblokiran Akses *WebFig*

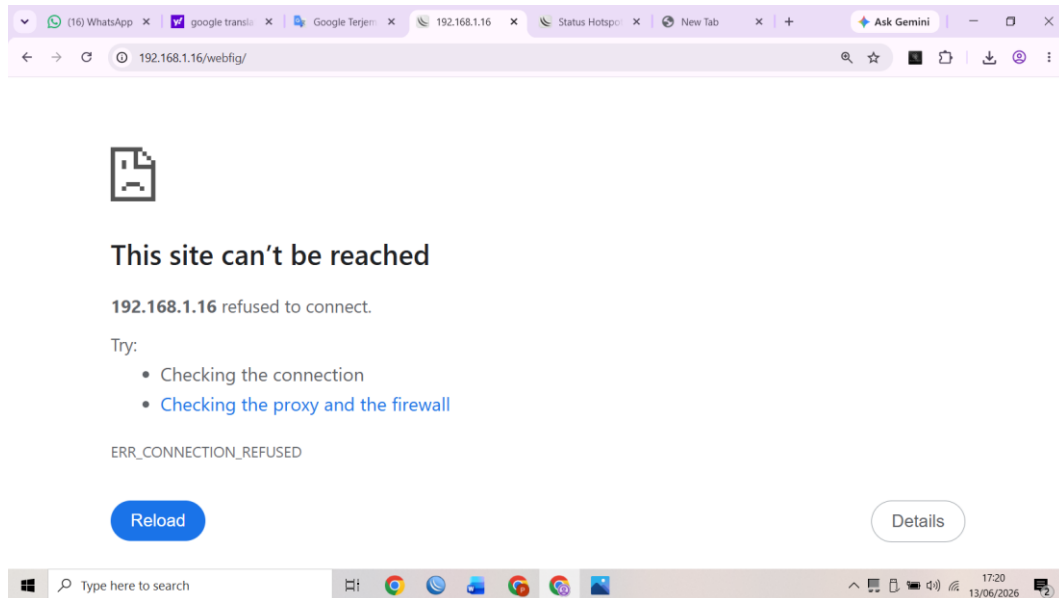


Sumber: Penulis, 2026

Gambar 5.52 Sebelum di *Block* Akses *WebFig*

Pengujian akses *webfig* dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa layanan manajemen *router mikrotik* melalui antarmuka *webfig* dapat diakses dengan baik sebelum dilakukan pembatasan akses. Pada pengujian ini dilakukan percobaan mengakses alamat *192.168.1.16/webfig/*.

Hasil pengujian menunjukkan bahwa halaman *webfig* berhasil ditampilkan dan pengguna dapat melihat antarmuka manajemen *RouterOS*. Pada halaman tersebut ditampilkan berbagai menu konfigurasi seperti *interfaces*, *bridge*, *ip*, *routing*, dan menu administrasi lainnya yang dapat digunakan untuk melakukan pengelolaan jaringan. Kondisi ini menunjukkan bahwa layanan *webfig* dapat diakses dengan normal melalui jaringan yang digunakan.



Sumber: Penulis, 2026

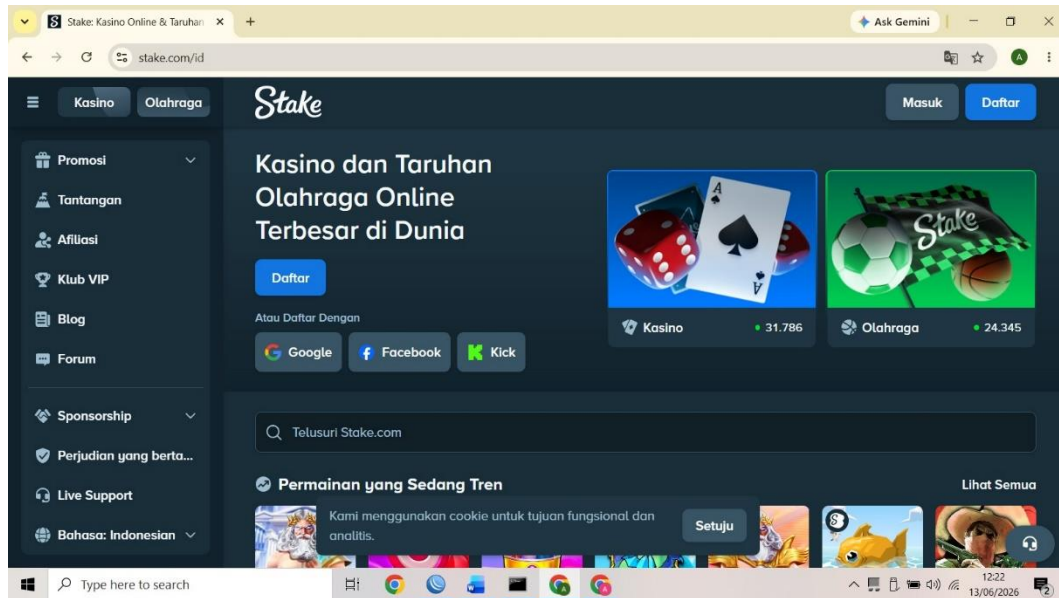
Gambar 5.53 Sudah di *Block* Akses *WebFig*

Setelah konfigurasi pembatasan akses diterapkan pada *router mikrotik*, dilakukan pengujian ulang terhadap layanan *webfig* melalui alamat *192.168.1.16/webfig/*. Pengujian ini bertujuan untuk memastikan bahwa akses ke halaman administrasi *router* telah berhasil dibatasi sesuai dengan kebijakan keamanan jaringan yang diterapkan.

Hasil pengujian menunjukkan bahwa halaman *webfig* tidak dapat diakses. Website menampilkan pesan “*This site can't be reached*”, “*192.168.1.16 refused to connect*”, serta kode kesalahan “*ERR_CONNECTION_REFUSED*”. Pesan tersebut menunjukkan bahwa koneksi menuju layanan *webfig* telah ditolak sehingga halaman administrasi *router* tidak dapat ditampilkan.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pembatasan akses terhadap *webfig* berhasil diterapkan. Dengan adanya pembatasan ini, hanya pengguna atau administrator yang memiliki hak akses tertentu yang dapat melakukan pengelolaan *router mikrotik*, sehingga keamanan jaringan sekolah dapat lebih terjaga dan risiko akses tidak sah dapat diminimalkan.

4. Pengujian Pemblokiran *Website Judi Online stake.com*

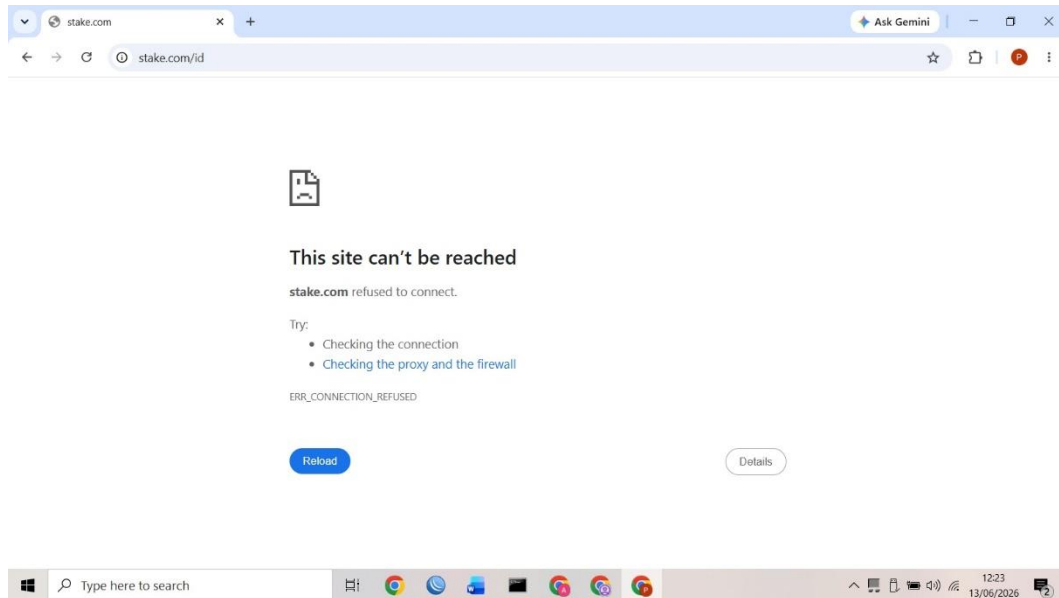


Sumber: Penulis, 2026

Gambar 5.54 Sebelum di *Block Website* <https://stake.com/>

Pengujian akses website dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk mengetahui kondisi akses *website* sebelum diterapkannya konfigurasi pemblokiran pada *router* mikrotik. Pada pengujian ini dilakukan percobaan mengakses *website* perjudian online stake.com.

Hasil pengujian menunjukkan bahwa *website* dapat diakses dengan normal dan seluruh halaman utama berhasil ditampilkan pada *website*. Halaman yang ditampilkan berisi berbagai menu dan layanan yang disediakan oleh *website* tersebut, sehingga pengguna jaringan masih dapat mengakses konten perjudian online tanpa adanya pembatasan. Kondisi ini menunjukkan bahwa sebelum konfigurasi DNS *static* diterapkan, *website* tersebut masih dapat dijangkau melalui jaringan *hotspot* sekolah.



Sumber: Penulis, 2026

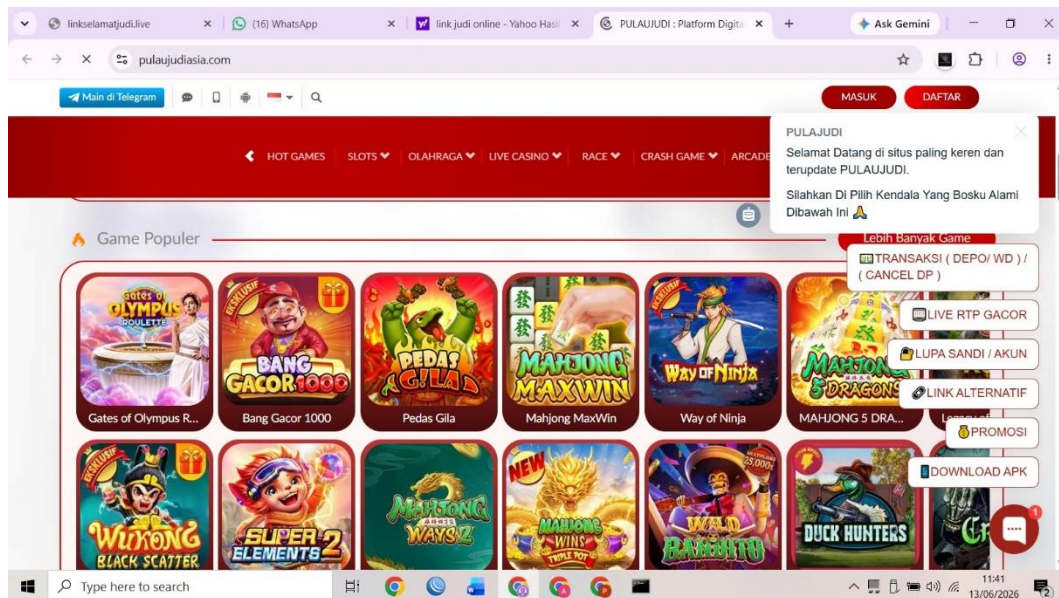
Gambar 5.55 Sudah di Block Website <https://stake.com/>

Setelah konfigurasi pemblokiran *website* diterapkan pada *router* mikrotik menggunakan fitur DNS *static*, dilakukan pengujian ulang terhadap *website* yang sama melalui jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa aturan pemblokiran telah berjalan sesuai dengan konfigurasi yang dibuat.

Hasil pengujian menunjukkan bahwa *website* stake.com tidak dapat diakses oleh pengguna jaringan. *Website* menampilkan pesan “*This site can't be reached*”, “*stake.com refused to connect*”, serta kode kesalahan “*ERR_CONNECTION_REFUSED*”. Pesan tersebut menunjukkan bahwa permintaan akses ke *website* telah ditolak sehingga halaman *website* gagal ditampilkan.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pemblokiran *website* pada *router* mikrotik berhasil diterapkan. Dengan demikian, akses ke *website* yang mengandung unsur perjudian dapat dibatasi sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman dan sesuai dengan tujuan pembelajaran.

5. Pengujian Pemblokiran Website Judi Online *pulaujudiasia.com*

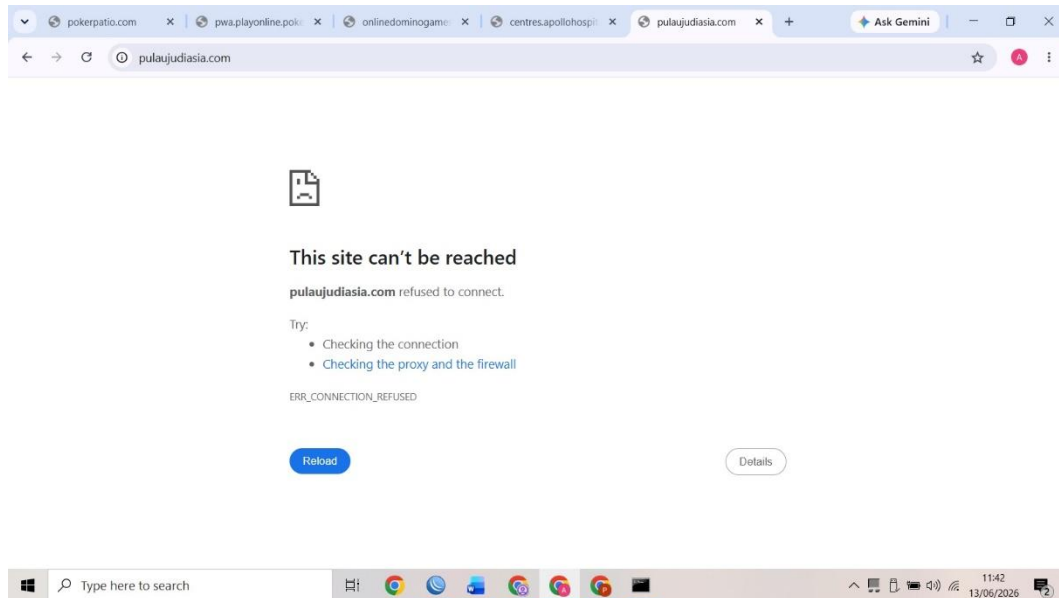


Sumber: Penulis, 2026

Gambar 5.56 Sebelum di Block Website <https://pulaujudiasia.com/>

Pengujian akses *website* dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk mengetahui kondisi akses *website* sebelum diterapkannya konfigurasi pemblokiran pada *router* mikrotik. Pada pengujian ini dilakukan percobaan mengakses salah satu *website* perjudian online melalui alamat domain yang telah ditentukan.

Hasil pengujian menunjukkan bahwa *website* dapat diakses dengan normal dan seluruh halaman utama berhasil ditampilkan pada *website*. Pengguna dapat melihat berbagai menu, permainan, serta layanan yang tersedia pada *website* tersebut tanpa mengalami kendala akses. Kondisi ini menunjukkan bahwa sebelum diterapkannya aturan pemblokiran, *website* masih dapat diakses oleh pengguna jaringan *hotspot* sekolah sehingga berpotensi digunakan untuk aktivitas yang tidak mendukung kegiatan pembelajaran.



Sumber: Penulis, 2026

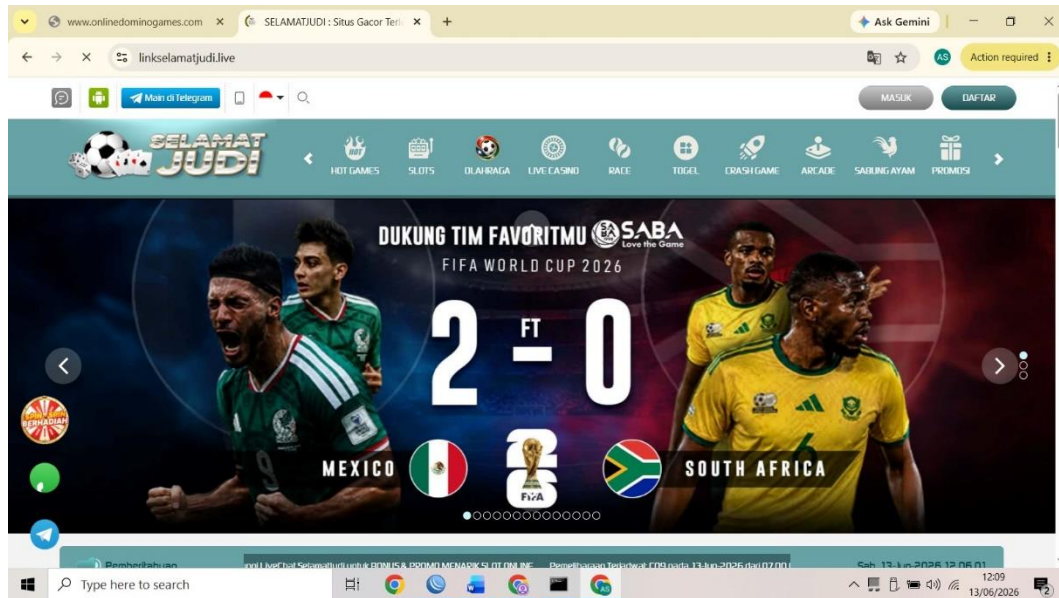
Gambar 5.57 Sudah di Block Website <https://pulaujudiasia.com/>

Setelah konfigurasi pemblokiran *website* diterapkan pada *router* mikrotik menggunakan fitur DNS *static*, dilakukan pengujian ulang terhadap *website* yang sama melalui jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa aturan pemblokiran telah berjalan sesuai dengan konfigurasi yang telah dibuat.

Hasil pengujian menunjukkan bahwa *website* tidak dapat diakses oleh pengguna jaringan. *Website* menampilkan pesan “*This site can't be reached*”, “*refused to connect*”, serta kode kesalahan “*ERR_CONNECTION_REFUSED*”. Pesan tersebut menunjukkan bahwa permintaan akses menuju *website* telah ditolak sehingga halaman *website* gagal ditampilkan pada *website*.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pemblokiran *website* pada *router* mikrotik berhasil diterapkan dengan baik. Dengan adanya mekanisme pemblokiran ini, akses ke *website* yang mengandung unsur perjudian dapat dibatasi sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman, terkontrol, dan sesuai dengan tujuan pendidikan.

6. Pengujian Pemblokiran Website Judi Online *linkselamatjudi.live*

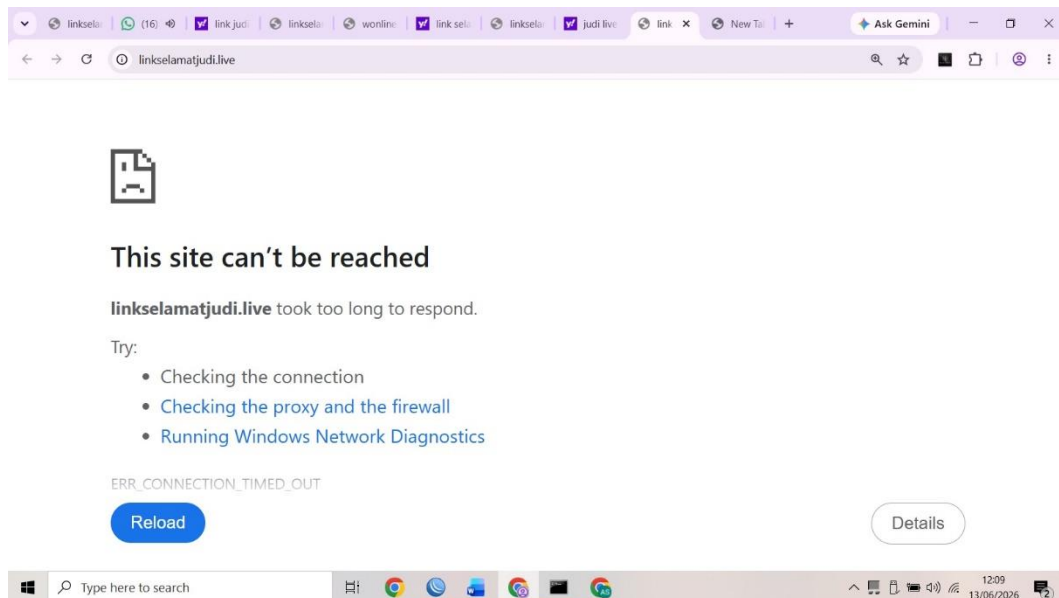


Sumber: Penulis, 2026

Gambar 5.58 Sebelum di Block Website <https://linkselamatjudi.live/>

Pengujian akses *website* dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk mengetahui kondisi akses *website* sebelum diterapkannya konfigurasi pemblokiran pada *router* mikrotik. pada pengujian ini dilakukan percobaan mengakses salah satu *website* perjudian online melalui domain yang telah ditentukan.

Hasil pengujian menunjukkan bahwa *website* dapat diakses dengan normal dan seluruh halaman utama berhasil ditampilkan pada *website*. Pengguna dapat melihat berbagai menu layanan seperti permainan *slot*, olahraga, *live casino*, dan fitur lainnya yang tersedia pada *website* tersebut. Hal ini menunjukkan bahwa sebelum penerapan kebijakan pemblokiran, *website* masih dapat diakses secara bebas oleh pengguna jaringan *hotspot* sekolah.



Sumber: Penulis, 2026

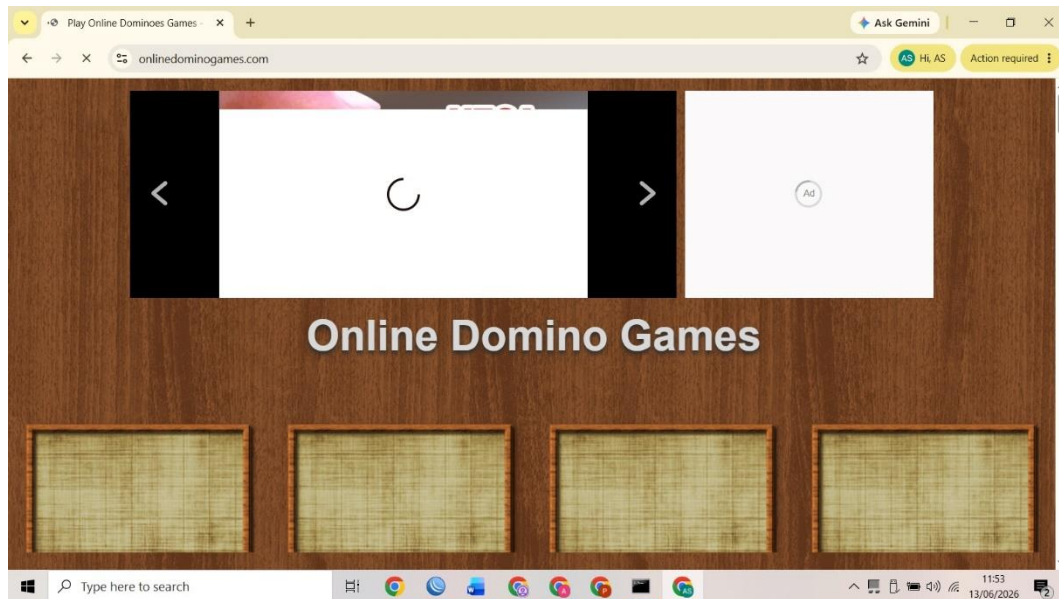
Gambar 5.59 Sudah di *Block Website* <https://linkselamatjudi.live/>

Setelah konfigurasi pemblokiran *website* diterapkan pada *router* mikrotik menggunakan fitur DNS *static*, dilakukan pengujian ulang terhadap domain yang sama melalui jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa aturan pemblokiran telah berjalan sesuai dengan konfigurasi yang telah dibuat.

Hasil pengujian menunjukkan bahwa *website* tidak dapat diakses oleh pengguna jaringan. *Website* menampilkan pesan “*This site can't be reached*”, “*took too long to respond*”, serta kode kesalahan “*ERR_CONNECTION_TIMED_OUT*”. Pesan tersebut menunjukkan bahwa *website* gagal memperoleh respons dari *website* tujuan sehingga halaman tidak dapat dimuat.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pemblokiran *website* pada *router* mikrotik berhasil diterapkan. Dengan adanya mekanisme pemblokiran ini, akses ke *website* yang mengandung unsur perjudian dapat dibatasi sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman, terkontrol, dan sesuai dengan tujuan pendidikan.

7. Pengujian Pemblokiran Website Judi Online *www.onlinedominogames.com*

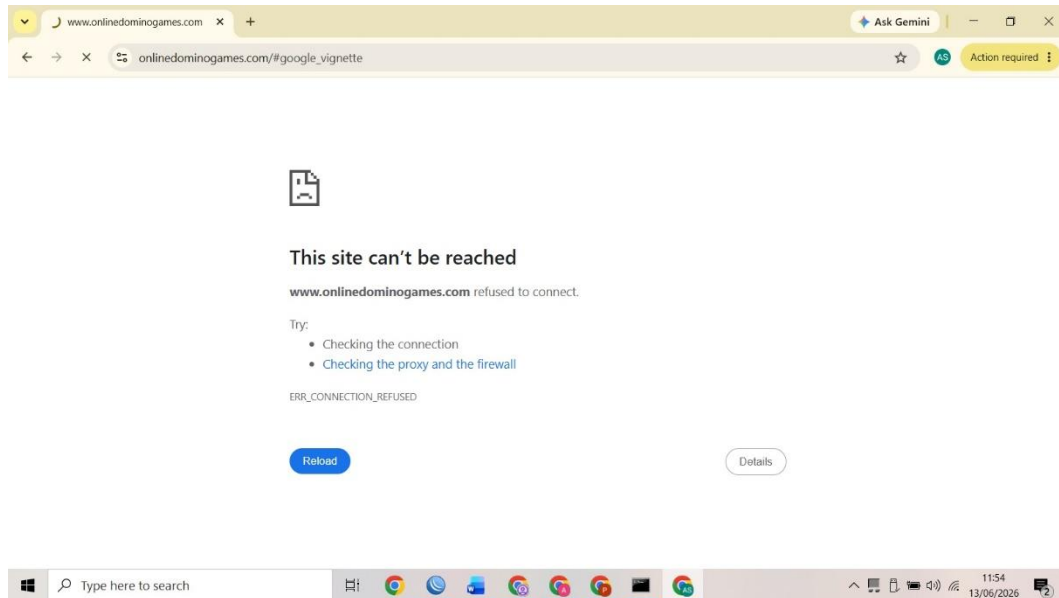


Sumber: Penulis, 2026

Gambar 5.60 Sebelum di Block Website [https:// www.onlinedominogames.com/](https://www.onlinedominogames.com/)

Pengujian akses *website* dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk mengetahui kondisi akses *website* sebelum diterapkannya konfigurasi pemblokiran pada *router mikrotik*. Pada pengujian ini dilakukan percobaan mengakses *website* permainan domino online melalui domain www.onlinedominogames.com.

Hasil pengujian menunjukkan bahwa *website* dapat diakses dengan normal dan halaman utama berhasil ditampilkan pada browser. Pengguna masih dapat melihat tampilan *website* beserta konten yang tersedia di dalamnya tanpa mengalami kendala akses. Kondisi ini menunjukkan bahwa sebelum penerapan kebijakan pemblokiran, *website* tersebut masih dapat diakses oleh pengguna jaringan *hotspot* sekolah.



Sumber: Penulis, 2026

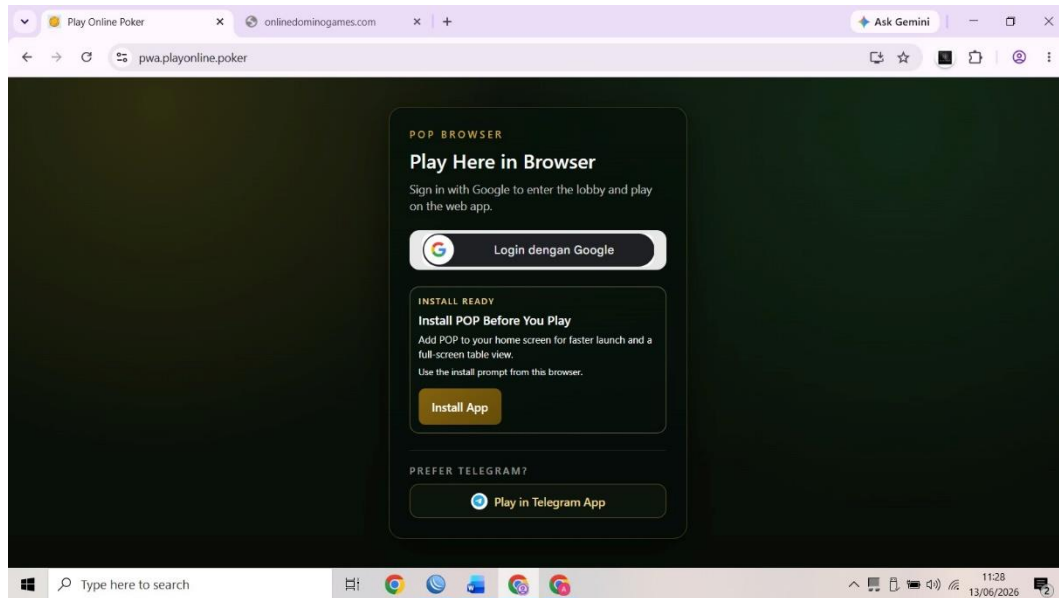
Gambar 5.61 Sudah di *Block Website* [https:// www.onlinedominogames.com/](https://www.onlinedominogames.com/)

Setelah konfigurasi pemblokiran *website* diterapkan pada *router mikrotik* menggunakan fitur *DNS static*, dilakukan pengujian ulang terhadap domain [onlinedominogames.com](https://www.onlinedominogames.com) melalui jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa aturan pemblokiran telah berjalan sesuai dengan konfigurasi yang telah dibuat.

Hasil pengujian menunjukkan bahwa *website* tidak dapat diakses oleh pengguna jaringan. *Website* menampilkan pesan “*This site can't be reached*”, “*www.onlinedominogames.com refused to connect*”, serta kode kesalahan “*ERR_CONNECTION_REFUSED*”. Pesan tersebut menunjukkan bahwa koneksi menuju *website* telah ditolak sehingga halaman tidak dapat ditampilkan pada *website*.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pemblokiran *website* pada *router mikrotik* berhasil diterapkan. Dengan adanya mekanisme pemblokiran ini, akses ke *website* yang mengandung unsur perjudian dan permainan daring yang tidak sesuai dengan lingkungan pendidikan dapat dibatasi, sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman, terkontrol, dan mendukung kegiatan pembelajaran.

8. Pengujian Pemblokiran Website Judi Online *pwa.playonline.poker*

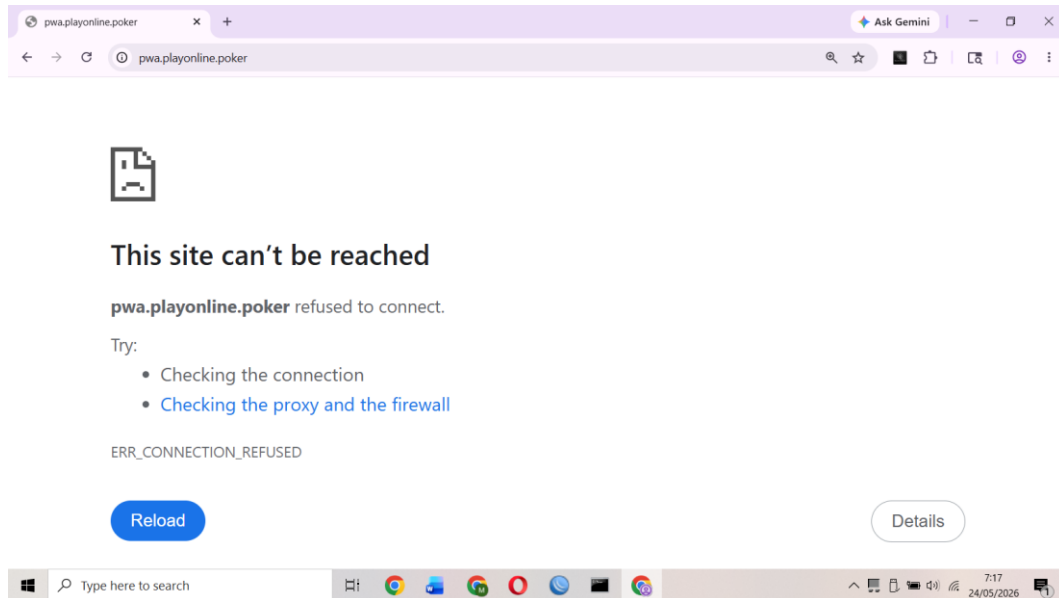


Sumber: Penulis, 2026

Gambar 5.62 Sebelum di Block Website *https://pwa.playonline.poker/*

Pengujian akses *website* dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk mengetahui kondisi akses *website* sebelum diterapkannya konfigurasi pemblokiran pada *router mikrotik*. Pada pengujian ini dilakukan percobaan mengakses *website* permainan poker online melalui domain *pwa.playonline.poker*.

Hasil pengujian menunjukkan bahwa *website* dapat diakses dengan normal dan halaman utama berhasil ditampilkan. Pengguna masih dapat melihat halaman masuk (*login*), menu akses permainan, serta berbagai layanan yang tersedia pada *website* tersebut tanpa mengalami kendala. Kondisi ini menunjukkan bahwa sebelum penerapan kebijakan pemblokiran, *website* masih dapat diakses oleh pengguna jaringan *hotspot* sekolah.



Sumber: Penulis, 2026

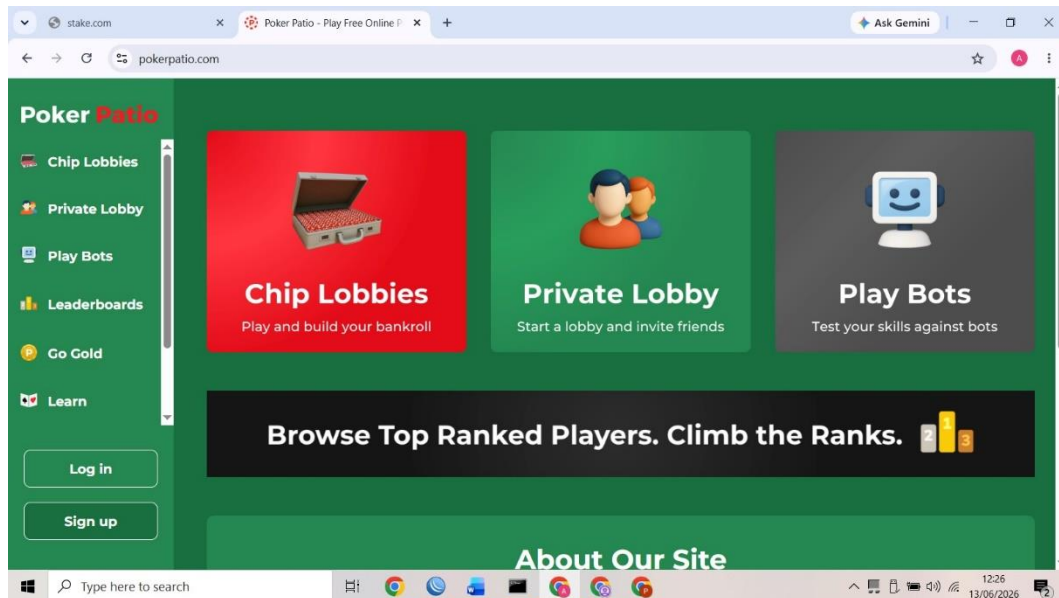
Gambar 5.63 Sudah di Block Website <https://pwa.playonline.poker/>

Setelah konfigurasi pemblokiran *website* diterapkan pada *router mikrotik* menggunakan fitur *DNS static*, dilakukan pengujian ulang terhadap domain *pwa.playonline.poker* melalui jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa aturan pemblokiran telah berjalan sesuai dengan konfigurasi yang telah dibuat.

Hasil pengujian menunjukkan bahwa *website* tidak dapat diakses oleh pengguna jaringan. *Website* menampilkan pesan “*This site can't be reached*”, “*pwa.playonline.poker refused to connect*”, serta kode kesalahan “*ERR_CONNECTION_REFUSED*”. Pesan tersebut menunjukkan bahwa koneksi menuju *website* telah ditolak sehingga halaman tidak dapat ditampilkan.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pemblokiran *website* pada *router mikrotik* berhasil diterapkan. Dengan adanya mekanisme pemblokiran ini, akses ke *website* yang mengandung unsur perjudian dapat dibatasi sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman, terkontrol, dan sesuai dengan tujuan pendidikan.

9. Pengujian Pemblokiran Website Judi Online *pokerpatio.com*

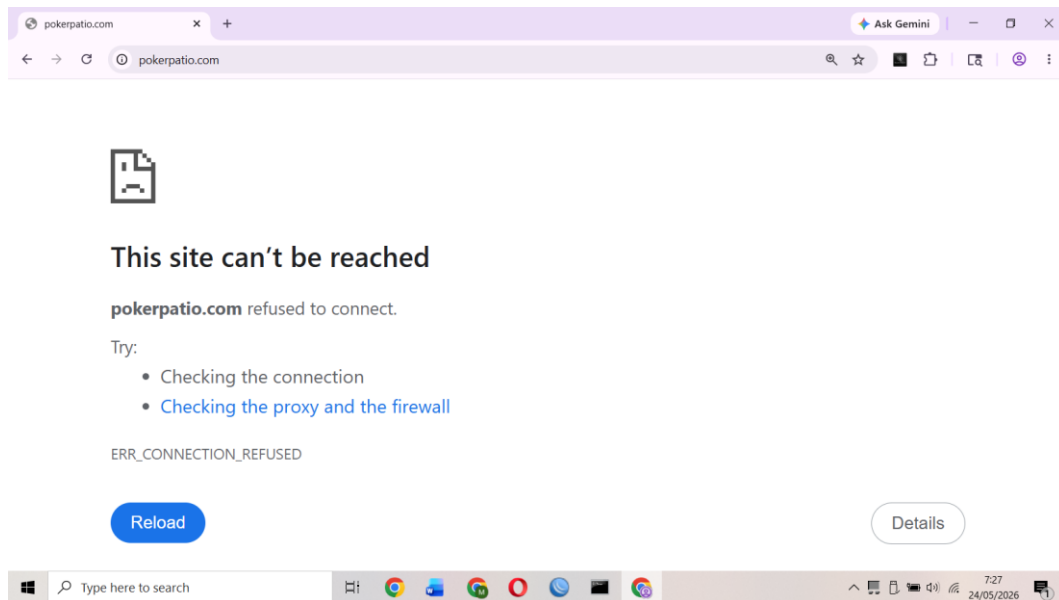


Sumber: Penulis, 2026

Gambar 5.64 Sebelum di Block Website <https://pokerpatio.com/>

Pengujian akses *website* dilakukan menggunakan *website google chrome* yang terhubung ke jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk mengetahui kondisi akses *website* sebelum diterapkannya konfigurasi pemblokiran pada *router mikrotik*. Pada pengujian ini dilakukan percobaan mengakses *website* permainan poker online melalui domain *pokerpatio.com*.

Hasil pengujian menunjukkan bahwa *website* dapat diakses dengan normal dan halaman utama berhasil ditampilkan. Pengguna masih dapat melihat berbagai menu layanan yang tersedia, seperti *chip lobbies*, *private lobby*, dan *play bots*, serta informasi lain yang disediakan pada *website* tersebut. Kondisi ini menunjukkan bahwa sebelum penerapan kebijakan pemblokiran, *website* masih dapat diakses secara bebas oleh pengguna jaringan *hotspot* sekolah.



Sumber: Penulis, 2026

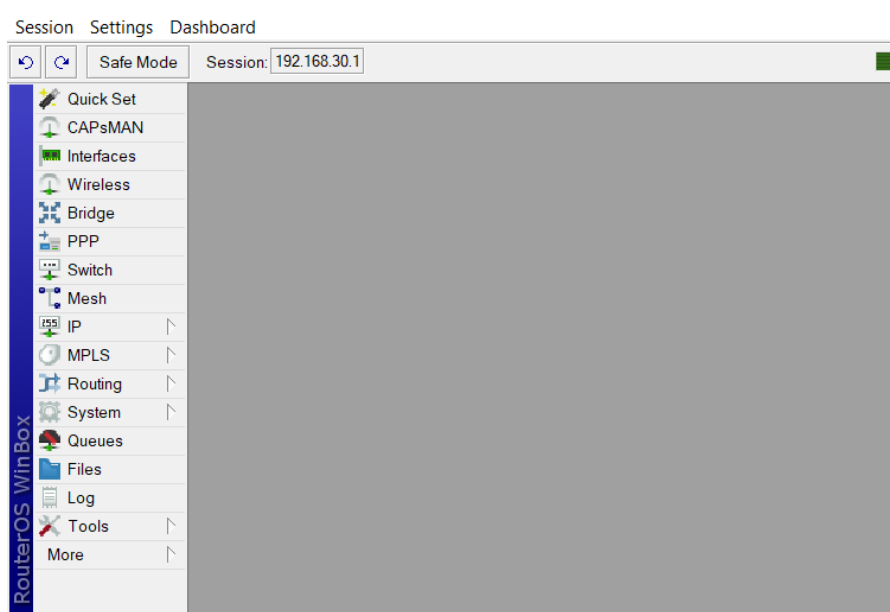
Gambar 5.65 Sudah di Block Website <https://pokerpatio.com/>

Setelah konfigurasi pemblokiran *website* diterapkan pada *router mikrotik* menggunakan fitur *DNS static*, dilakukan pengujian ulang terhadap domain *pokerpatio.com* melalui jaringan *hotspot* sekolah. Pengujian ini bertujuan untuk memastikan bahwa aturan pemblokiran telah berjalan sesuai dengan konfigurasi yang telah dibuat.

Hasil pengujian menunjukkan bahwa *website* tidak dapat diakses oleh pengguna jaringan. *Website* menampilkan pesan “*This site can't be reached*”, “*pokerpatio.com refused to connect*”, serta kode kesalahan “*ERR_CONNECTION_REFUSED*”. Pesan tersebut menunjukkan bahwa koneksi menuju *website* telah ditolak sehingga halaman tidak dapat ditampilkan.

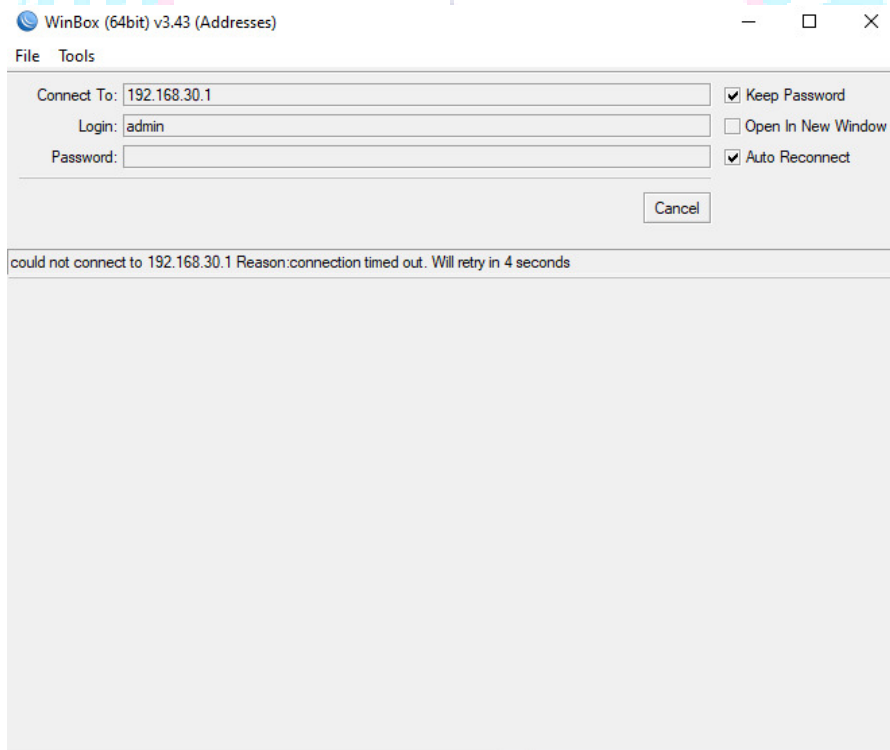
Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pemblokiran *website* pada *router mikrotik* berhasil diterapkan. Dengan adanya mekanisme pemblokiran ini, akses ke *website* yang mengandung unsur perjudian dapat dibatasi sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman, terkontrol, dan sesuai dengan tujuan pendidikan.

10. Pengujian Blok Akses Sesuai dengan MAC Address



Sumber: Penulis, 2026

Gambar 5.66 Pengujian MAC Address Admin



Sumber: Penulis, 2026

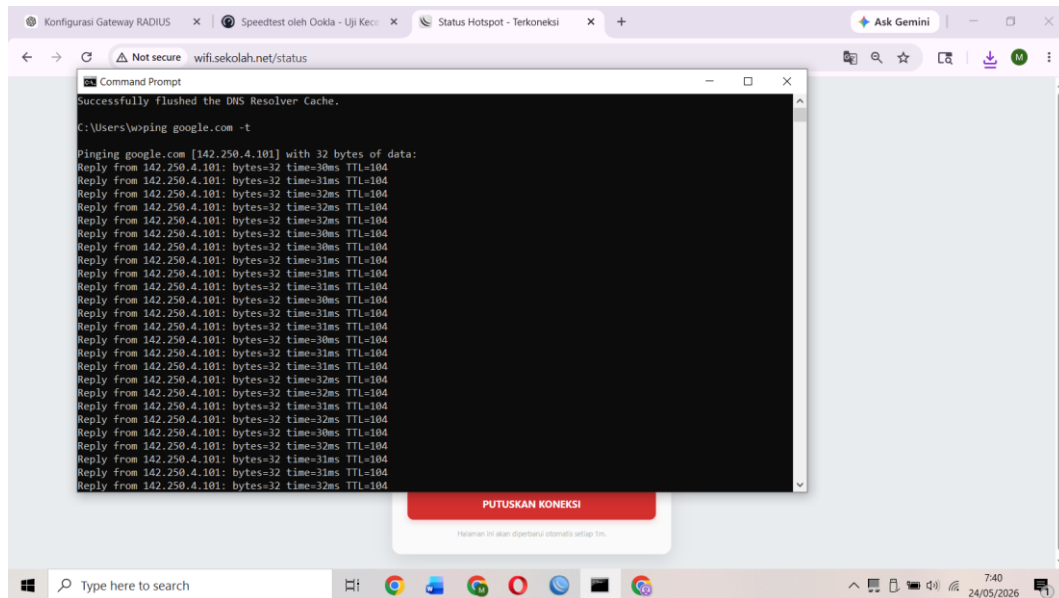
Gambar 5.67 Akses Konfigurasi Perangkat Client

Pengujian fungsionalitas sistem keamanan jaringan dilakukan untuk memvalidasi konfigurasi *firewall filter rules* dalam membatasi hak akses kontrol (*access control*) ke menu konfigurasi *router* mikrotik. Skenario pengujian ini diterapkan dengan membuat aturan *whitelist* (daftar putih) berbasis *MAC address*, di mana sistem hanya mengizinkan autentikasi masuk ke winbox jika berasal dari *MAC address* laptop administrator yang telah ditentukan, dan memblokir seluruh *MAC address* lain yang tidak terdaftar.

Berdasarkan hasil pengujian pada Gambar 5.66, ketika perangkat laptop administrator yang *MAC address*-nya telah didaftarkan melakukan *login*, sistem berhasil mengenali identitas perangkat tersebut dan memberikan hak akses penuh untuk masuk ke dalam menu utama winbox. Hal ini membuktikan bahwa aturan *filter* pada *firewall* telah bekerja secara akurat dalam mengenali perangkat yang sah (*authorized device*).

Sebaliknya, pada Gambar 5.67 menunjukkan kondisi ketika perangkat lain dengan *MAC address* yang berbeda mencoba melakukan koneksi ke winbox. Perangkat tersebut secara otomatis ditolak oleh aturan *firewall filter rules router*, yang ditandai dengan munculnya status *connection timed out* pada aplikasi winbox. Dengan demikian, dapat disimpulkan bahwa pengujian fitur keamanan kendali akses berbasis *MAC address* ini berhasil diimplementasikan dengan sempurna dan mampu mengamankan *router* dari akses ilegal perangkat asing.

5.5.2 Pengujian Menggunakan *Command Prompt*



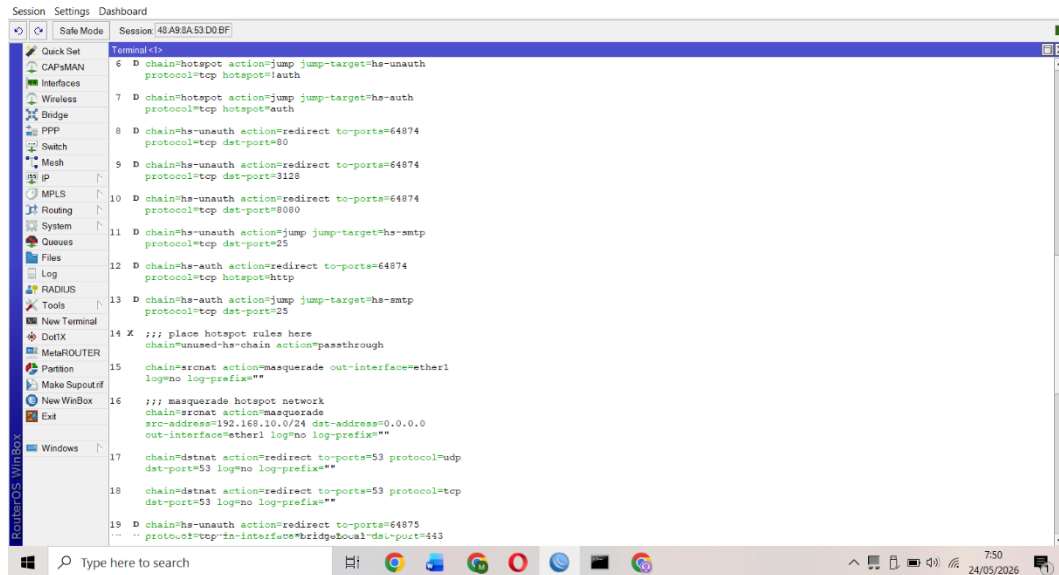
Sumber: Penulis, 2026

Gambar 5.68 Pengujian *Command Prompt*

Pengujian jaringan menggunakan CMD (*Command Prompt*) dilakukan dengan menjalankan perintah `ping google.com -t` untuk mengetahui kualitas koneksi internet pada jaringan *hotspot* sekolah. Berdasarkan hasil pengujian pada Gambar 5.68, perangkat berhasil menerima *reply* dari *server* tujuan dengan nilai waktu (*time*) berkisar antara 30 ms hingga 32 ms. Hasil tersebut menunjukkan bahwa koneksi internet pada jaringan *hotspot* sekolah berjalan dengan baik dan stabil.

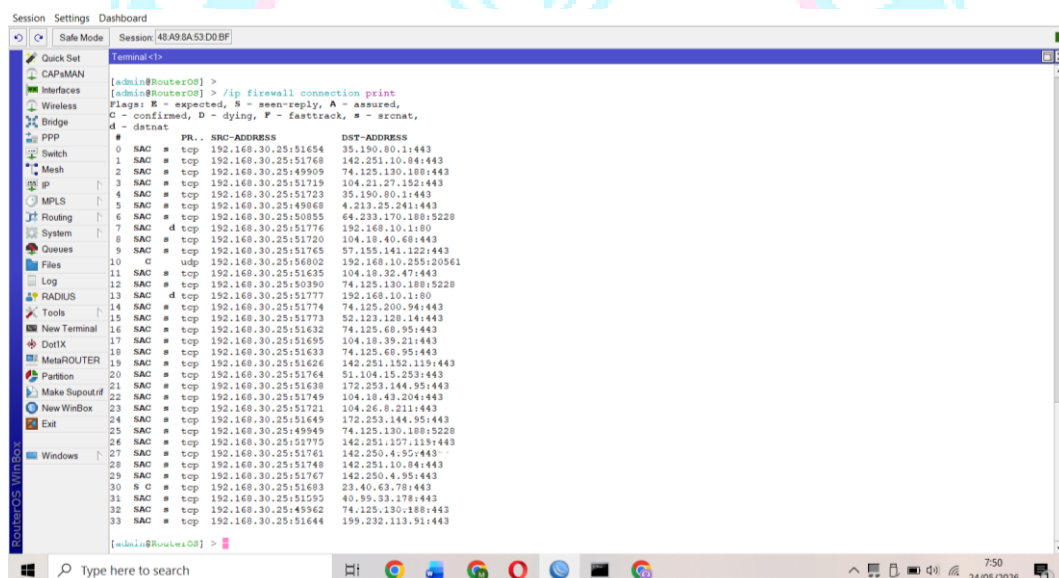
Hasil pengujian juga menunjukkan bahwa seluruh paket data berhasil terkirim tanpa adanya pesan *request timed out*, sehingga nilai *packet loss* pada jaringan sebesar 0%. Selain itu, perbedaan nilai *delay* yang tidak terlalu jauh menunjukkan bahwa tingkat *jitter* pada jaringan tergolong stabil. Dengan demikian, konfigurasi jaringan *hotspot* pada *router* mikrotik telah berjalan dengan baik dan mampu mendukung aktivitas akses internet di lingkungan sekolah secara optimal.

5.5.3 Pengujian Menggunakan CLI Router Mikrotik



Sumber: Penulis, 2026

Gambar 5.69 NAT (Network Address Translation)



Sumber: Penulis, 2026

Gambar 5.70 Perangkat *Client* yang terhubung

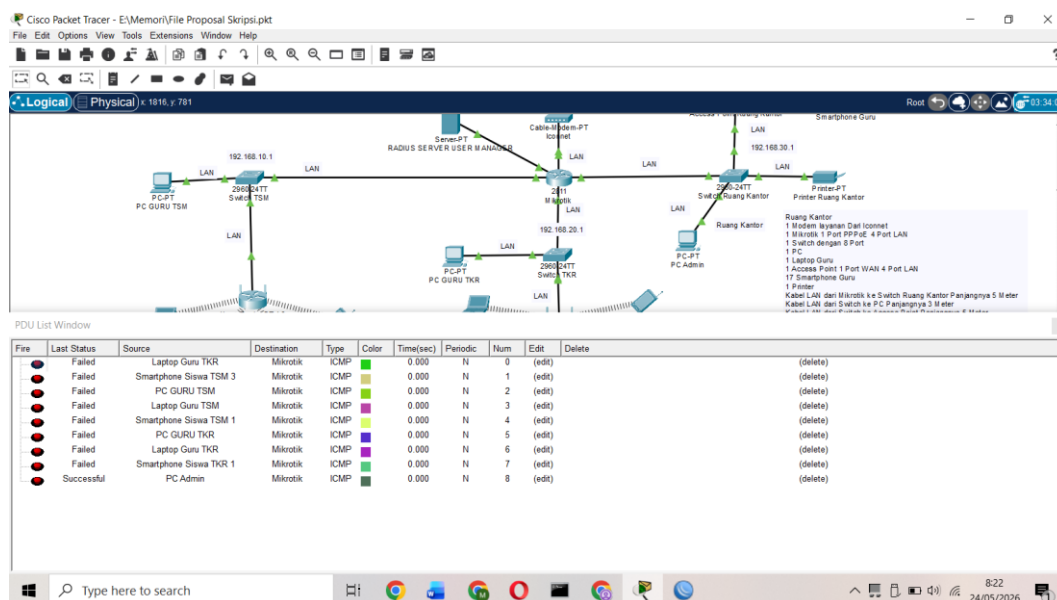
Pengujian CLI dilakukan menggunakan fitur terminal pada *router* mikrotik untuk memastikan koneksi jaringan dan proses translasi IP (*Network Address Translation*/NAT) berjalan dengan baik. Pengujian dilakukan dengan mengetik perintah `/ip firewall connection print` untuk menampilkan daftar koneksi aktif pada *router* mikrotik. Hasil pengujian menunjukkan bahwa perangkat *client* dengan IP lokal 192.168.30.25 berhasil terhubung ke berbagai alamat IP internet

menggunakan protokol TCP pada *port* HTTPS (443). Hal tersebut menunjukkan bahwa perangkat *client* telah berhasil melakukan komunikasi data melalui jaringan internet menggunakan *router* mikrotik sebagai *gateway* utama jaringan *hotspot*.

Selain itu, dilakukan pengecekan konfigurasi NAT menggunakan aturan *chain=srcnat action=masquerade* pada *firewall* NAT *router* mikrotik. NAT (*network address translation*) merupakan proses penerjemahan alamat IP lokal menjadi alamat IP publik agar perangkat pada jaringan lokal dapat mengakses internet. Pada konfigurasi ini, fitur *srcnat masquerade* berfungsi untuk mengubah alamat IP *private* milik *client* menjadi alamat IP publik milik *router* saat mengirimkan data ke internet. Dengan adanya konfigurasi tersebut, seluruh perangkat pada jaringan *hotspot* dapat menggunakan koneksi internet melalui satu jalur koneksi internet yang tersedia pada *router* mikrotik.

Hasil pengujian menunjukkan bahwa proses translasi IP berhasil diterapkan dengan baik, ditandai dengan munculnya koneksi aktif dari IP lokal menuju berbagai alamat IP internet pada terminal *router* mikrotik. Berdasarkan hasil tersebut dapat disimpulkan bahwa koneksi jaringan, proses NAT, dan akses internet pada *hotspot* telah berjalan sesuai konfigurasi yang diterapkan sehingga perangkat *client* dapat terhubung ke internet dengan normal melalui *router* mikrotik.

5.5.4 Pengujian Menggunakan *Simple PDU*



Sumber: Penulis, 2026

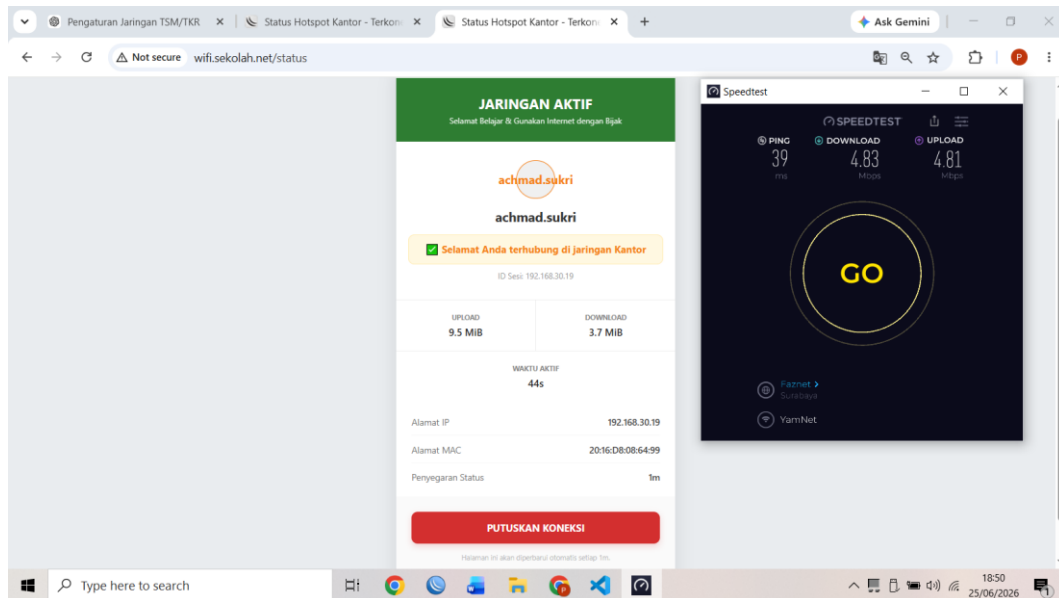
Gambar 5.71 Pengujian *Simple PDU*

Pengujian simulasi jaringan dilakukan menggunakan aplikasi *cisco packet tracer* dengan memanfaatkan fitur *Simple PDU* untuk menguji pembatasan akses terhadap *router* mikrotik. Pengujian dilakukan dengan mengirimkan paket ICMP (*ping*) dari beberapa perangkat *client* menuju *router* mikrotik. Pada pengujian ini perangkat admin berhasil mengirimkan paket ke *router* dengan status *successful*. Hasil tersebut menunjukkan bahwa perangkat admin memiliki hak akses untuk melakukan komunikasi langsung dengan *router*.

Selain itu, pengujian juga dilakukan dari beberapa perangkat pengguna lain seperti PC guru, laptop guru, dan *smartphone* siswa menuju *router* mikrotik. Hasil pengujian menunjukkan status *failed* pada perangkat non-admin. Kondisi tersebut menandakan bahwa *router* mikrotik berhasil membatasi akses ping dari pengguna selain admin sesuai konfigurasi keamanan jaringan yang diterapkan.

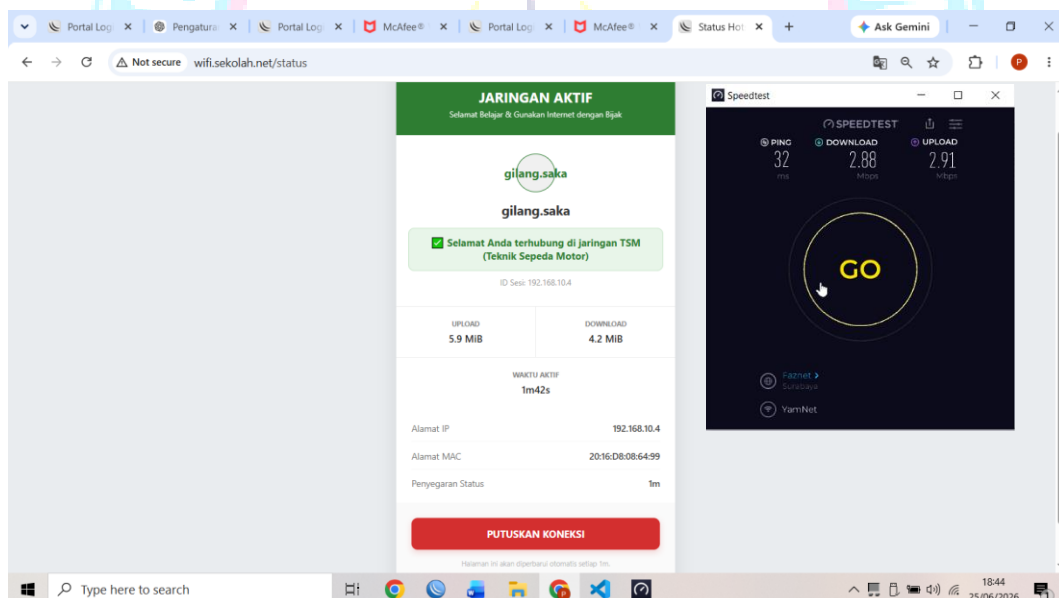
Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi pembatasan akses pada jaringan *hotspot* sekolah telah berjalan dengan baik. Hanya perangkat admin yang diizinkan melakukan akses langsung ke *router*, sedangkan perangkat pengguna lain tidak dapat melakukan komunikasi ICMP (*ping*) ke *router* mikrotik.

5.5.5 Pengujian Menggunakan *Speedtest*



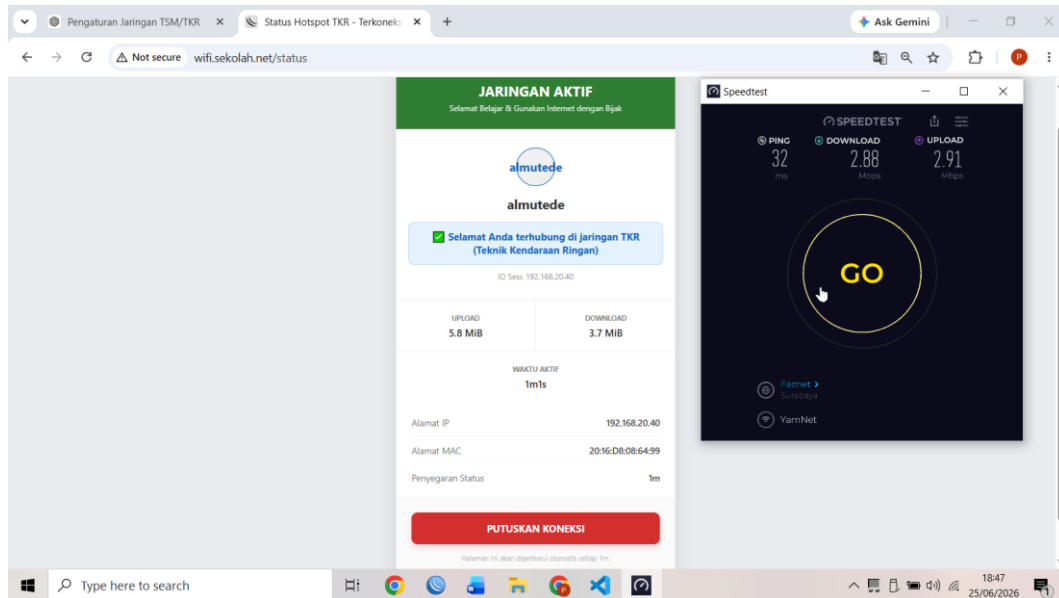
Sumber: Penulis, 2026

Gambar 5.72 *Speedtest* Guru



Sumber: Penulis, 2026

Gambar 5.73 *Speedtest* Siswa TSM



Sumber: Penulis, 2026

Gambar 5.74 Speedtest Siswa TKR

Pengujian *bandwidth* dilakukan menggunakan aplikasi *Speedtest by Ookla* pada jaringan *hotspot* sekolah untuk memastikan pembagian *bandwidth* antara pengguna berjalan sesuai konfigurasi yang telah diterapkan pada *router* mikrotik. Pengujian dilakukan terhadap beberapa akun pengguna *hotspot* yang berbeda dengan melakukan pengukuran kecepatan *download* dan *upload* setelah pengguna berhasil *login* ke jaringan *hotspot* sekolah.

Hasil pengujian pertama pada akun *achmad.sukri* sebagai guru menunjukkan kecepatan *download* sebesar 4.83 Mbps dan *upload* sebesar 4.81 Mbps. Hasil tersebut menunjukkan bahwa pengguna berhasil memperoleh akses internet sesuai pembagian *bandwidth* yang telah dikonfigurasi pada *router* mikrotik.

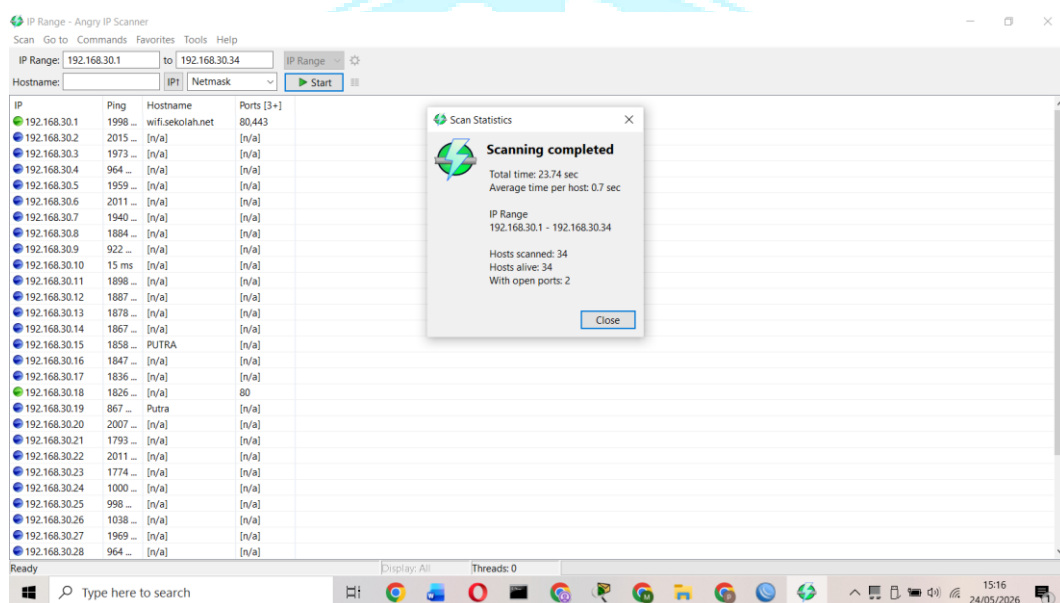
Hasil pengujian kedua pada akun *gilang.saka* sebagai siswa TSM menunjukkan kecepatan *download* sebesar 2.88 Mbps dan *upload* sebesar 2.91 Mbps. Kecepatan yang diperoleh berbeda dengan pengguna sebelumnya karena pembagian *bandwidth* dilakukan berdasarkan aturan yang diterapkan pada masing-masing pengguna atau kelompok pengguna.

Hasil pengujian ketiga pada akun *almutede* sebagai siswa TKR menunjukkan kecepatan *download* sebesar 2.88 Mbps dan *upload* sebesar 2.91 Mbps. Hasil tersebut menunjukkan bahwa pembatasan *bandwidth* berjalan dengan baik sehingga

setiap pengguna memperoleh kecepatan internet sesuai kebijakan yang telah ditentukan.

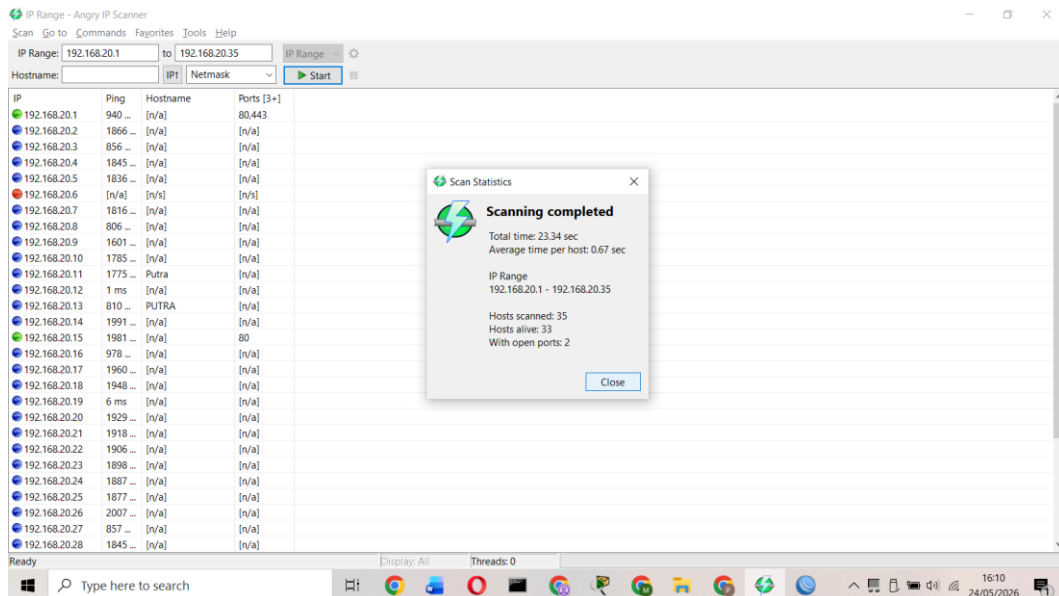
Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi manajemen *bandwidth* pada *router* mikrotik telah berjalan dengan baik. Setiap pengguna *hotspot* memperoleh *bandwidth* yang stabil dan sesuai dengan konfigurasi yang diterapkan sehingga penggunaan jaringan internet pada lingkungan sekolah dapat lebih terkontrol dan merata.

5.5.6 Pengujian Menggunakan *Angry IP Scanner*



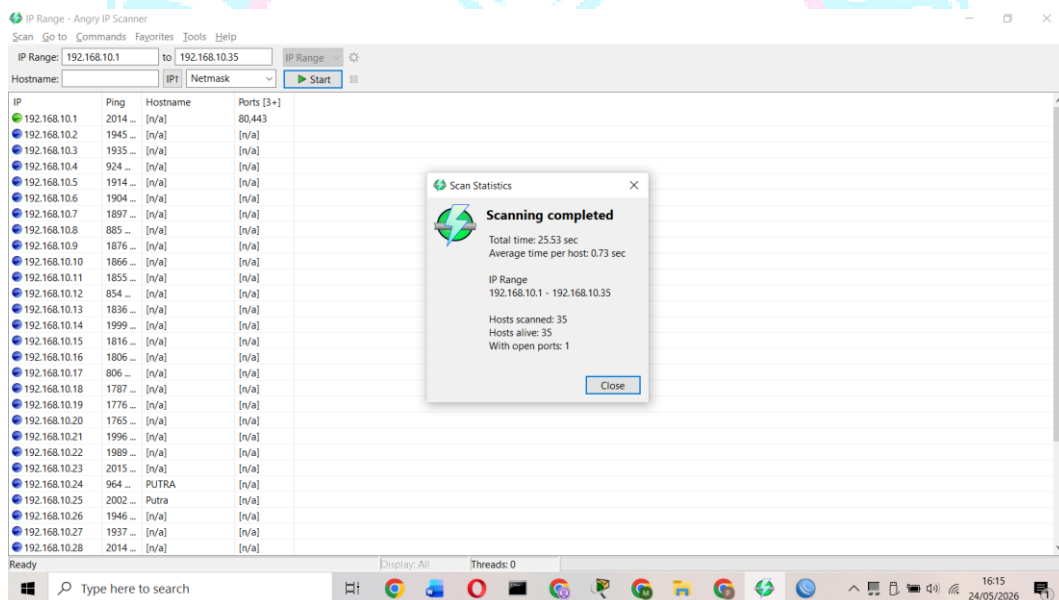
Sumber: Penulis, 2026

Gambar 5.75 Scanning 192.168.30.1



Sumber: Penulis, 2026

Gambar 5.76 Scanning 192.168.20.1



Sumber: Penulis, 2026

Gambar 5.77 Scanning 192.168.10.1

Pengujian koneksi jaringan dilakukan dengan mencoba perpindahan kabel *access point* pada setiap *port ethernet* mikrotik yang telah dikonfigurasi sebagai jaringan berbeda, yaitu *ether* dengan *gateway* 192.168.10.1, 192.168.20.1, dan 192.168.30.1. Pada saat *access point* dipindahkan ke masing-masing *port ethernet*, laptop yang terhubung ke *hotspot* secara otomatis memperoleh alamat IP sesuai

dengan *gateway* pada *ethernet* tersebut melalui layanan DHCP yang telah dikonfigurasi pada mikrotik.

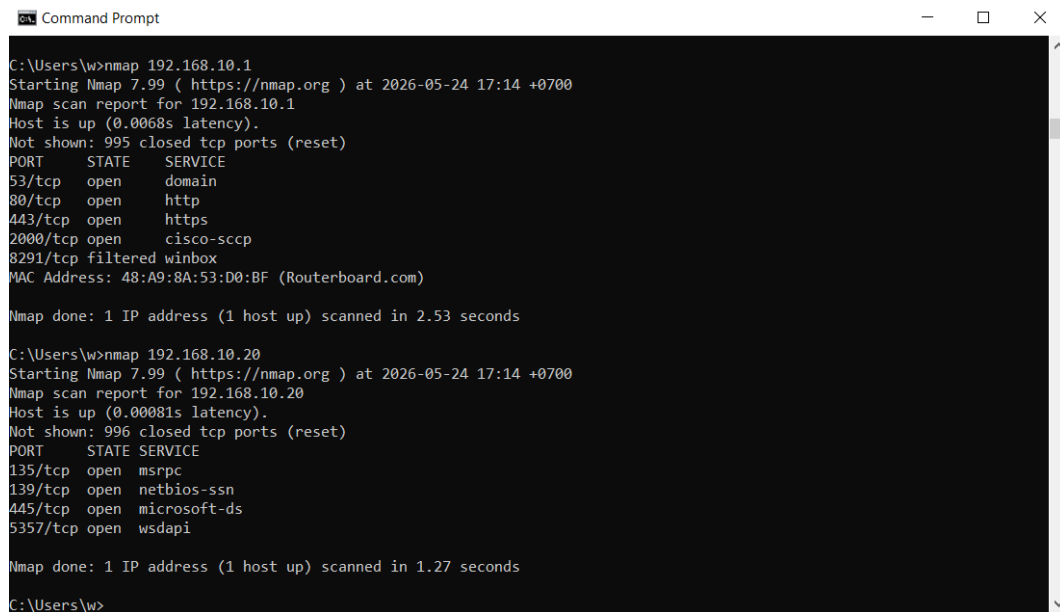
Hasil pengujian menunjukkan bahwa ketika *access point* terhubung ke *ethernet* dengan *gateway* 192.168.10.1, laptop memperoleh alamat IP pada jaringan 192.168.10.x. Saat *access point* dipindahkan ke *ethernet* dengan *gateway* 192.168.20.1, laptop memperoleh alamat IP pada jaringan 192.168.20.x. Selanjutnya ketika *access point* dipindahkan ke *ethernet* dengan *gateway* 192.168.30.1, laptop memperoleh alamat IP pada jaringan 192.168.30.x. Hal ini menunjukkan bahwa konfigurasi DHCP dan *hotspot* pada masing-masing *ethernet* telah berjalan sesuai dengan jaringan yang digunakan.

Pengujian kemudian dilanjutkan menggunakan aplikasi *angry IP scanner* untuk melakukan pemindaian pada setiap jaringan. Berdasarkan hasil *scanning*, alamat IP laptop yang digunakan dalam pengujian berhasil terdeteksi pada masing-masing jaringan sesuai dengan *ethernet* yang sedang digunakan. Pada jaringan 192.168.10.x, 192.168.20.x, dan 192.168.30.x, perangkat laptop muncul sebagai *host* aktif pada hasil pemindaian jaringan. Hasil tersebut membuktikan bahwa perangkat *client* berhasil terhubung ke jaringan *hotspot* dan dapat dikenali oleh sistem jaringan mikrotik.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa konfigurasi *hotspot* dan DHCP *server* pada mikrotik berhasil berjalan dengan baik. Perpindahan *access point* ke *ethernet* yang berbeda dapat membuat perangkat *client* memperoleh alamat IP otomatis sesuai jaringan masing-masing, serta perangkat berhasil terdeteksi pada proses *scanning* jaringan.

5.5.7 Pengujian Menggunakan Nmap

1. Scanning IP 192.168.10.1



```

C:\Users\w>nmap 192.168.10.1
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-24 17:14 +0700
Nmap scan report for 192.168.10.1
Host is up (0.0068s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
2000/tcp  open  cisco-sccp
8291/tcp  filtered winbox
MAC Address: 48:A9:8A:53:D0:BF (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 2.53 seconds

C:\Users\w>nmap 192.168.10.20
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-24 17:14 +0700
Nmap scan report for 192.168.10.20
Host is up (0.00081s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds

C:\Users\w>
  
```

Sumber: Penulis, 2026

Gambar 5.78 Nmap 192.168.10.1

Pada pengujian pertama dilakukan *scanning* terhadap IP *gateway* mikrotik yaitu 192.168.10.1. Hasil *scanning* menunjukkan beberapa *port* penting berada dalam kondisi *open*, yaitu *port* 53/tcp (DNS), 80/tcp (HTTP), 443/tcp (HTTPS), dan 2000/tcp (Cisco SCCP). Selain itu, *port* 8291/tcp berada pada status *filtered* yang menandakan akses winbox dilindungi oleh *firewall* mikrotik. Hasil tersebut menunjukkan bahwa perangkat *gateway* mikrotik aktif dan menjalankan layanan jaringan *hotspot* dengan baik.

Sedangkan pada pengujian kedua dilakukan *scanning* terhadap IP laptop *client* yaitu 192.168.10.20. Hasil *scanning* menunjukkan *port* 135/tcp (MSRPC), 139/tcp (NetBIOS-SSN), 445/tcp (Microsoft-DS), dan 5357/tcp (WSDAPI) berada dalam kondisi *open*. *Port-port* tersebut merupakan layanan bawaan sistem operasi *windows* yang aktif pada perangkat *client*. Hasil ini menunjukkan bahwa laptop *client* berhasil terhubung ke jaringan *hotspot* dan dapat terdeteksi pada jaringan saat proses *scanning* dilakukan.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa Nmap berhasil digunakan untuk menganalisis perangkat *gateway* maupun perangkat *client* pada jaringan *hotspot*. Pengujian ini membuktikan bahwa layanan jaringan pada

mikrotik berjalan dengan baik dan perangkat *client* berhasil memperoleh koneksi jaringan sesuai konfigurasi *hotspot* yang telah diterapkan.

2. Scanning IP 192.168.20.1

```

C:\Users\w>nmap 192.168.20.1
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-24 16:49 +0700
Nmap scan report for 192.168.20.1
Host is up (0.0031s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
2000/tcp   open  cisco-sccp
8291/tcp   filtered winbox
MAC Address: 48:A9:8A:53:D0:C0 (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds

C:\Users\w>nmap 192.168.20.17
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-24 16:51 +0700
Nmap scan report for 192.168.20.17
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
C:\Users\w>

```

Sumber: Penulis, 2026

Gambar 5. 79 Nmap 192.168.20.1

Pada pengujian pertama dilakukan *scanning* terhadap IP *gateway* mikrotik yaitu 192.168.20.1. Hasil *scanning* menunjukkan beberapa *port* penting berada dalam kondisi *open*, yaitu *port* 53/tcp (DNS), 80/tcp (HTTP), 443/tcp (HTTPS), dan 2000/tcp (Cisco SCCP). Selain itu, *port* 8291/tcp berada pada status *filtered* yang menandakan akses winbox dilindungi oleh *firewall* mikrotik. Hasil tersebut menunjukkan bahwa perangkat *gateway* mikrotik aktif dan menjalankan layanan jaringan *hotspot* dengan baik.

Sedangkan pada pengujian kedua dilakukan *scanning* terhadap IP laptop *client* yaitu 192.168.20.17. Hasil *scanning* menunjukkan *port* 135/tcp (MSRPC), 139/tcp (NetBIOS-SSN), 445/tcp (Microsoft-DS), dan 5357/tcp (WSDAPI) berada dalam kondisi *open*. *Port-port* tersebut merupakan layanan bawaan sistem operasi *windows* yang aktif pada perangkat *client*. Hasil ini menunjukkan bahwa laptop *client* berhasil terhubung ke jaringan *hotspot* dan dapat terdeteksi pada jaringan saat proses *scanning* dilakukan.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa Nmap berhasil digunakan untuk menganalisis perangkat *gateway* maupun perangkat *client* pada jaringan *hotspot*. Pengujian ini membuktikan bahwa layanan jaringan pada mikrotik berjalan dengan baik dan perangkat *client* berhasil memperoleh koneksi jaringan sesuai konfigurasi *hotspot* yang telah diterapkan.

3. Scanning IP 192.168.30.1

```

C:\Users\w>nmap 192.168.30.1
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-24 17:05 +0700
Nmap scan report for wifi.sekolah.net (192.168.30.1)
Host is up (0.0035s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
2000/tcp   open  cisco-sccp
8291/tcp   filtered winbox
MAC Address: 48:A9:8A:53:D0:C1 (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 2.02 seconds

C:\Users\w>nmap 192.168.30.10
Starting Nmap 7.99 ( https://nmap.org ) at 2026-05-24 17:06 +0700
Nmap scan report for 192.168.30.10
Host is up (0.00075s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
C:\Users\w>
  
```

Sumber: Penulis, 2026

Gambar 5.80 Nmap 192.168.30.1

Pengujian pertama dilakukan pada IP *gateway* mikrotik yaitu 192.168.30.1. Hasil *scanning* menunjukkan bahwa *host* dalam kondisi aktif dengan *latency* sebesar 0.0035 detik. Dari hasil *scanning* ditemukan beberapa *port* dalam kondisi *open*, yaitu *port* 53/tcp sebagai layanan DNS, *port* 80/tcp sebagai layanan HTTP, *port* 443/tcp sebagai layanan HTTPS, serta *port* 2000/tcp untuk layanan Cisco SCCP. Selain itu, *port* 8291/tcp berada dalam kondisi *filtered* yang menunjukkan akses winbox pada mikrotik dibatasi atau dilindungi oleh *firewall*. Hasil ini menunjukkan bahwa *gateway hotspot* berjalan dengan baik dan layanan jaringan aktif pada perangkat mikrotik.

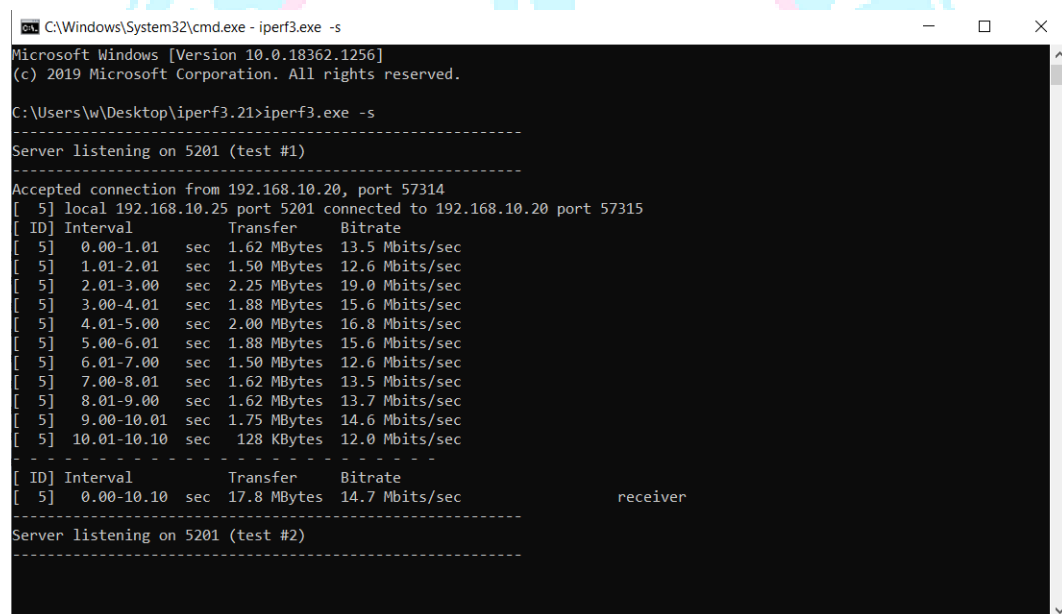
Selanjutnya dilakukan *scanning* terhadap perangkat *client* dengan IP 192.168.30.10 yang terhubung ke jaringan *hotspot*. Hasil *scanning* menunjukkan bahwa *host* aktif dengan *latency* sebesar 0.00075 detik. Pada perangkat *client*

ditemukan beberapa *port* terbuka, yaitu *port* 135/tcp (MSRPC), *port* 139/tcp (NetBIOS-SSN), *port* 445/tcp (Microsoft-DS), dan *port* 5357/tcp (WSDAPI). *Port-port* tersebut merupakan layanan bawaan sistem operasi *windows* yang aktif pada perangkat *client* saat terhubung ke jaringan.

Berdasarkan hasil pengujian tersebut dapat disimpulkan bahwa proses *scanning* menggunakan Nmap berhasil dilakukan pada *gateway* maupun perangkat *client*. Pengujian ini membuktikan bahwa jaringan *hotspot* berjalan dengan baik, perangkat *client* berhasil terhubung ke jaringan, serta layanan jaringan pada masing-masing perangkat dapat terdeteksi melalui proses *scanning port* menggunakan Nmap.

5.5.8 Pengujian Menggunakan Iperf3

1. Pengujian iperf3 di Jaringan 192.168.10.1



```

C:\Windows\System32\cmd.exe - iperf3.exe -s
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\w\Desktop\iperf3.21>iperf3.exe -s

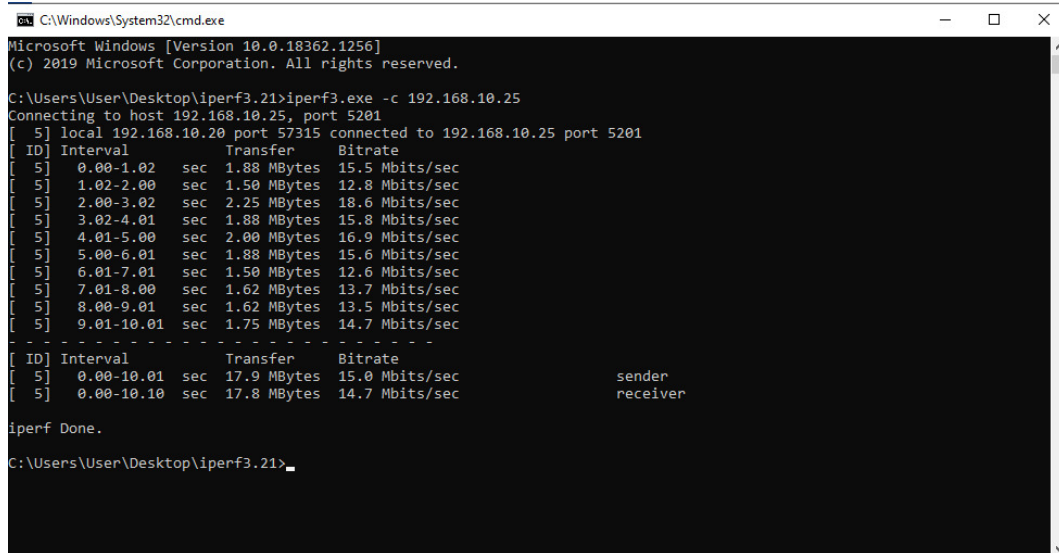
Server listening on 5201 (test #1)

Accepted connection from 192.168.10.20, port 57314
[ 5] local 192.168.10.25 port 5201 connected to 192.168.10.20 port 57315
[ ID] Interval      Transfer    Bitrate
[ 5] 0.00-1.01 sec  1.62 MBytes 13.5 Mbits/sec
[ 5] 1.01-2.01 sec  1.50 MBytes 12.6 Mbits/sec
[ 5] 2.01-3.00 sec  2.25 MBytes 19.0 Mbits/sec
[ 5] 3.00-4.01 sec  1.88 MBytes 15.6 Mbits/sec
[ 5] 4.01-5.00 sec  2.00 MBytes 16.8 Mbits/sec
[ 5] 5.00-6.01 sec  1.88 MBytes 15.6 Mbits/sec
[ 5] 6.01-7.00 sec  1.50 MBytes 12.6 Mbits/sec
[ 5] 7.00-8.01 sec  1.62 MBytes 13.5 Mbits/sec
[ 5] 8.01-9.00 sec  1.62 MBytes 13.7 Mbits/sec
[ 5] 9.00-10.01 sec 1.75 MBytes 14.6 Mbits/sec
[ 5] 10.01-10.10 sec 128 KBytes 12.0 Mbits/sec
-----
[ ID] Interval      Transfer    Bitrate
[ 5] 0.00-10.10 sec 17.8 MBytes 14.7 Mbits/sec
-----
Server listening on 5201 (test #2)

```

Sumber: Penulis, 2026

Gambar 5.81 Sebagai *Server* dengan IP 192.168.10.25



```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User\Desktop\iperf3.21>iperf3.exe -c 192.168.10.25
Connecting to host 192.168.10.25, port 5201
[ 5] local 192.168.10.20 port 57315 connected to 192.168.10.25 port 5201
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-1.02 sec  1.88 MBytes  15.5 Mbits/sec
[ 5] 1.02-2.00 sec  1.50 MBytes  12.8 Mbits/sec
[ 5] 2.00-3.02 sec  2.25 MBytes  18.6 Mbits/sec
[ 5] 3.02-4.01 sec  1.88 MBytes  15.8 Mbits/sec
[ 5] 4.01-5.00 sec  2.00 MBytes  16.9 Mbits/sec
[ 5] 5.00-6.01 sec  1.88 MBytes  15.6 Mbits/sec
[ 5] 6.01-7.01 sec  1.50 MBytes  12.6 Mbits/sec
[ 5] 7.01-8.00 sec  1.62 MBytes  13.7 Mbits/sec
[ 5] 8.00-9.01 sec  1.62 MBytes  13.5 Mbits/sec
[ 5] 9.01-10.01 sec 1.75 MBytes  14.7 Mbits/sec
-----
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-10.01 sec 17.9 MBytes  15.0 Mbits/sec
[ 5] 0.00-10.10 sec 17.8 MBytes  14.7 Mbits/sec

iperf Done.

C:\Users\User\Desktop\iperf3.21>

```

Sumber: Penulis, 2026

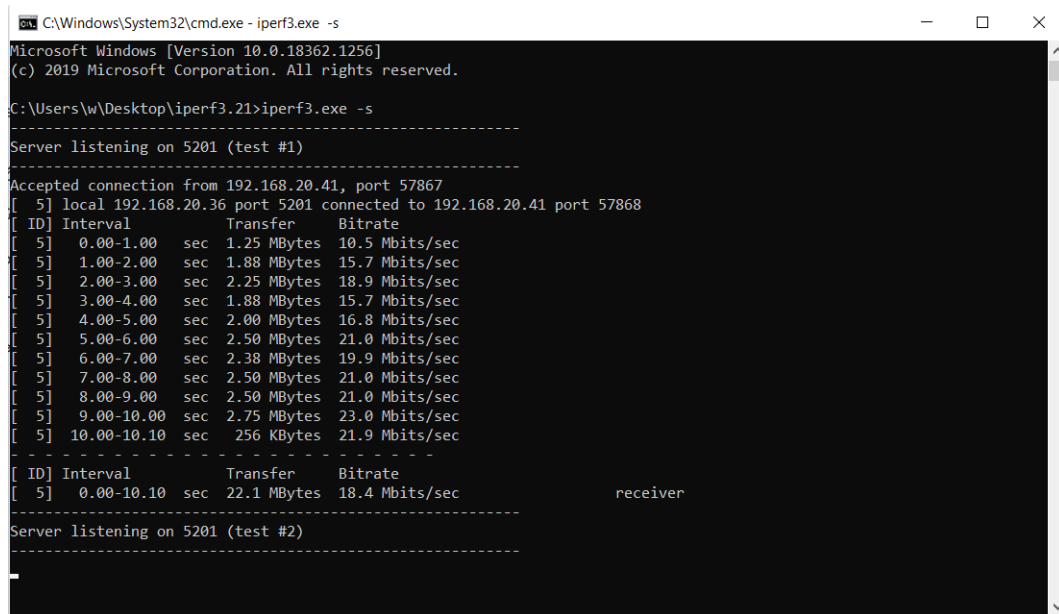
Gambar 5.82 Sebagai *Client* dengan IP 192.168.10.20

Hasil pengujian menggunakan iperf3 menunjukkan bahwa proses komunikasi antara perangkat *server* dan *client* berhasil dilakukan dengan baik. Pengujian dilakukan menggunakan dua perangkat laptop yang terhubung pada jaringan nirkabel (*wi-fi*) yang sama, di mana perangkat *server* memiliki alamat IP 192.168.10.25 dan perangkat *client* memiliki alamat IP 192.168.10.20.

Pada saat pengujian berlangsung, perangkat *client* berhasil terhubung ke *server* melalui port 5201 dengan status koneksi berhasil diterima (*accepted connection*). Hasil pengujian menampilkan proses *transfer* data sebesar 17.9 MBytes pada sisi *sender* dan 17.8 MBytes pada sisi *receiver*, serta nilai *throughput* jaringan secara *realtime* hingga pengujian selesai dilakukan.

Berdasarkan hasil pengujian tersebut, diperoleh nilai *throughput* rata-rata sebesar 14.7 Mbits/sec. Nilai tersebut menunjukkan bahwa jaringan nirkabel mampu melakukan proses pertukaran data antar perangkat dengan baik dan stabil mengikuti kapasitas maksimal dari media transmisi yang digunakan. Dengan demikian, dapat disimpulkan bahwa pengujian *throughput* jaringan menggunakan iperf3 berhasil dilakukan sesuai dengan kondisi jaringan yang telah diterapkan.

2. Pengujian iperf3 di Jaringan 192.168.20.1



```

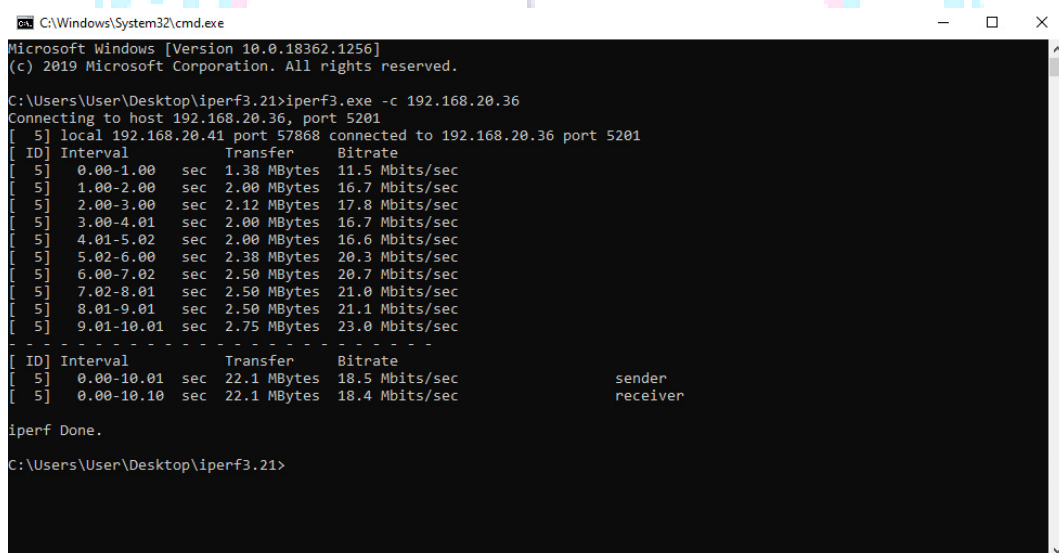
C:\Windows\System32\cmd.exe - iperf3.exe -s
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\w\Desktop\iperf3.21>iperf3.exe -s
-----
Server listening on 5201 (test #1)
-----
Accepted connection from 192.168.20.41, port 57867
[ 5] local 192.168.20.36 port 5201 connected to 192.168.20.41 port 57868
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-1.00    sec  1.25 MBytes  10.5 Mbits/sec
[ 5] 1.00-2.00    sec  1.88 MBytes  15.7 Mbits/sec
[ 5] 2.00-3.00    sec  2.25 MBytes  18.9 Mbits/sec
[ 5] 3.00-4.00    sec  1.88 MBytes  15.7 Mbits/sec
[ 5] 4.00-5.00    sec  2.00 MBytes  16.8 Mbits/sec
[ 5] 5.00-6.00    sec  2.50 MBytes  21.0 Mbits/sec
[ 5] 6.00-7.00    sec  2.38 MBytes  19.9 Mbits/sec
[ 5] 7.00-8.00    sec  2.50 MBytes  21.0 Mbits/sec
[ 5] 8.00-9.00    sec  2.50 MBytes  21.0 Mbits/sec
[ 5] 9.00-10.00   sec  2.75 MBytes  23.0 Mbits/sec
[ 5] 10.00-10.10  sec   256 KBytes  21.9 Mbits/sec
-----
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-10.10   sec  22.1 MBytes  18.4 Mbits/sec
-----
Server listening on 5201 (test #2)
-----

```

Sumber: Penulis, 2026

Gambar 5.83 Sebagai *Server* dengan IP 192.168.20.36



```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User\Desktop\iperf3.21>iperf3.exe -c 192.168.20.36
Connecting to host 192.168.20.36, port 5201
[ 5] local 192.168.20.41 port 57868 connected to 192.168.20.36 port 5201
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-1.00    sec  1.38 MBytes  11.5 Mbits/sec
[ 5] 1.00-2.00    sec  2.00 MBytes  16.7 Mbits/sec
[ 5] 2.00-3.00    sec  2.12 MBytes  17.8 Mbits/sec
[ 5] 3.00-4.01    sec  2.00 MBytes  16.7 Mbits/sec
[ 5] 4.01-5.02    sec  2.00 MBytes  16.6 Mbits/sec
[ 5] 5.02-6.00    sec  2.38 MBytes  20.3 Mbits/sec
[ 5] 6.00-7.02    sec  2.50 MBytes  20.7 Mbits/sec
[ 5] 7.02-8.01    sec  2.50 MBytes  21.0 Mbits/sec
[ 5] 8.01-9.01    sec  2.50 MBytes  21.1 Mbits/sec
[ 5] 9.01-10.01   sec  2.75 MBytes  23.0 Mbits/sec
-----
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-10.01   sec  22.1 MBytes  18.5 Mbits/sec
[ 5] 0.00-10.10   sec  22.1 MBytes  18.4 Mbits/sec
-----
iperf Done.

C:\Users\User\Desktop\iperf3.21>

```

Sumber: Penulis, 2026

Gambar 5.84 Sebagai *Client* dengan IP 192.168.20.41

Hasil pengujian menggunakan iperf3 menunjukkan bahwa proses komunikasi antara perangkat *server* dan *client* berhasil dilakukan dengan baik. Pengujian dilakukan menggunakan dua perangkat laptop yang terhubung pada jaringan nirkabel (*wi-fi*) yang sama, di mana perangkat *server* memiliki alamat IP 192.168.20.36 dan perangkat *client* memiliki alamat IP 192.168.20.41.

Pada saat pengujian berlangsung, perangkat *client* berhasil terhubung ke *server* melalui *port* 5201 dengan status koneksi berhasil diterima (*accepted connection*). Hasil pengujian menampilkan proses transfer data sebesar 22.1 MBytes pada sisi *sender* dan 22.1 MBytes pada sisi *receiver*, serta nilai *throughput* jaringan secara *realtime* hingga pengujian selesai dilakukan.

Berdasarkan hasil pengujian tersebut, diperoleh nilai *throughput* rata-rata sebesar 18.4 Mbits/sec. Nilai tersebut menunjukkan bahwa jaringan nirkabel mampu melakukan proses pertukaran data antar perangkat dengan baik dan stabil mengikuti kapasitas maksimal dari media transmisi yang digunakan. Dengan demikian, dapat disimpulkan bahwa pengujian *throughput* jaringan menggunakan *iperf3* berhasil dilakukan sesuai dengan kondisi jaringan yang telah diterapkan.

3. Pengujian *iperf3* di Jaringan 192.168.30.1

```

C:\Windows\System32\cmd.exe - iperf3.exe -s
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\w\Desktop\iperf3.21>iperf3.exe -s

Server listening on 5201 (test #1)
-----
Accepted connection from 192.168.30.24, port 58367
[ 5] local 192.168.30.23 port 5201 connected to 192.168.30.24 port 58368
[ ID] Interval      Transfer    Bitrate
[ 5] 0.00-1.00    sec 1.75 MBytes 14.7 Mbits/sec
[ 5] 1.00-2.00    sec 1.75 MBytes 14.7 Mbits/sec
[ 5] 2.00-3.00    sec 1.75 MBytes 14.7 Mbits/sec
[ 5] 3.00-4.00    sec 1.88 MBytes 15.7 Mbits/sec
[ 5] 4.00-5.00    sec 2.00 MBytes 16.8 Mbits/sec
[ 5] 5.00-6.00    sec 1.88 MBytes 15.7 Mbits/sec
[ 5] 6.00-7.00    sec 1.88 MBytes 15.7 Mbits/sec
[ 5] 7.00-8.00    sec 2.00 MBytes 16.8 Mbits/sec
[ 5] 8.00-9.00    sec 2.00 MBytes 16.8 Mbits/sec
[ 5] 9.00-10.00   sec 2.25 MBytes 18.9 Mbits/sec
[ 5] 10.00-10.08  sec 128 KBytes 14.0 Mbits/sec
-----
[ ID] Interval      Transfer    Bitrate
[ 5] 0.00-10.08   sec 19.2 MBytes 16.0 Mbits/sec
-----
Server listening on 5201 (test #2)
-----
receiver

```

Sumber: Penulis, 2026

Gambar 5.85 Sebagai *Server* dengan IP 192.168.30.23

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User\Desktop\iperf3.21>iperf3.exe -c 192.168.30.23
Connecting to host 192.168.30.23, port 5201
[ 5] local 192.168.30.24 port 58368 connected to 192.168.30.23 port 5201
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-1.01    sec  1.88 MBytes  15.6 Mbits/sec
[ 5] 1.01-2.00    sec  1.88 MBytes  15.8 Mbits/sec
[ 5] 2.00-3.01    sec  1.75 MBytes  14.5 Mbits/sec
[ 5] 3.01-4.01    sec  2.00 MBytes  16.9 Mbits/sec
[ 5] 4.01-5.01    sec  1.88 MBytes  15.6 Mbits/sec
[ 5] 5.01-6.01    sec  1.75 MBytes  14.7 Mbits/sec
[ 5] 6.01-7.00    sec  2.00 MBytes  17.0 Mbits/sec
[ 5] 7.00-8.01    sec  2.00 MBytes  16.7 Mbits/sec
[ 5] 8.01-9.01    sec  2.00 MBytes  16.8 Mbits/sec
[ 5] 9.01-10.01   sec  2.25 MBytes  18.8 Mbits/sec
-----
[ ID] Interval      Transfer      Bitrate
[ 5] 0.00-10.01   sec  19.4 MBytes  16.2 Mbits/sec
[ 5] 0.00-10.08   sec  19.2 MBytes  16.0 Mbits/sec

iperf Done.

C:\Users\User\Desktop\iperf3.21>

```

Sumber: Penulis, 2026

Gambar 5.86 Sebagai *Client* dengan IP 192.168.30.24

Hasil pengujian menggunakan iperf3 menunjukkan bahwa proses komunikasi antara perangkat *server* dan *client* berhasil dilakukan dengan baik. Pengujian dilakukan menggunakan dua perangkat laptop yang terhubung pada jaringan nirkabel (*wi-fi*) yang sama, di mana perangkat *server* memiliki alamat IP 192.168.30.23 dan perangkat *client* memiliki alamat IP 192.168.30.24.

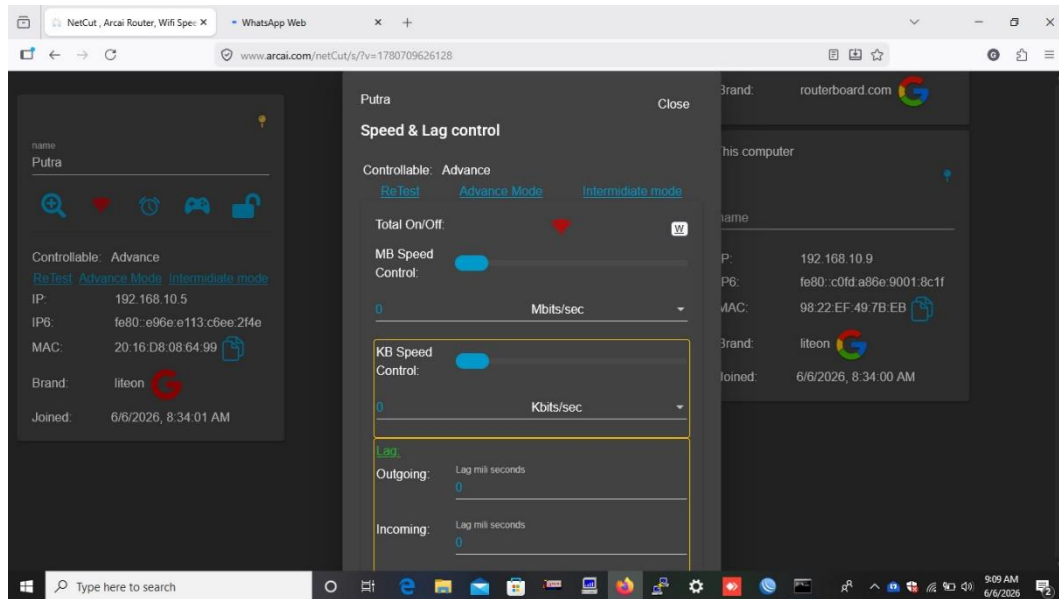
Pada saat pengujian berlangsung, perangkat *client* berhasil terhubung ke *server* melalui *port* 5201 dengan status koneksi berhasil diterima (*accepted connection*). Hasil pengujian menampilkan proses transfer data sebesar 19.4 MBytes pada sisi *sender* dan 19.2 MBytes pada sisi *receiver*, serta nilai *throughput* jaringan secara *realtime* hingga pengujian selesai dilakukan.

Berdasarkan hasil pengujian tersebut, diperoleh nilai *throughput* rata-rata sebesar 16.0 Mbits/sec. Nilai tersebut menunjukkan bahwa jaringan nirkabel mampu melakukan proses pertukaran data antar perangkat dengan baik dan stabil mengikuti kapasitas maksimal dari media transmisi yang digunakan. Dengan demikian, dapat disimpulkan bahwa pengujian *throughput* jaringan menggunakan iperf3 berhasil dilakukan sesuai dengan kondisi jaringan yang telah diterapkan.

5.5.9 Pengujian Menggunakan Aplikasi Pihak Ketiga

1. Netcut

a. TSM

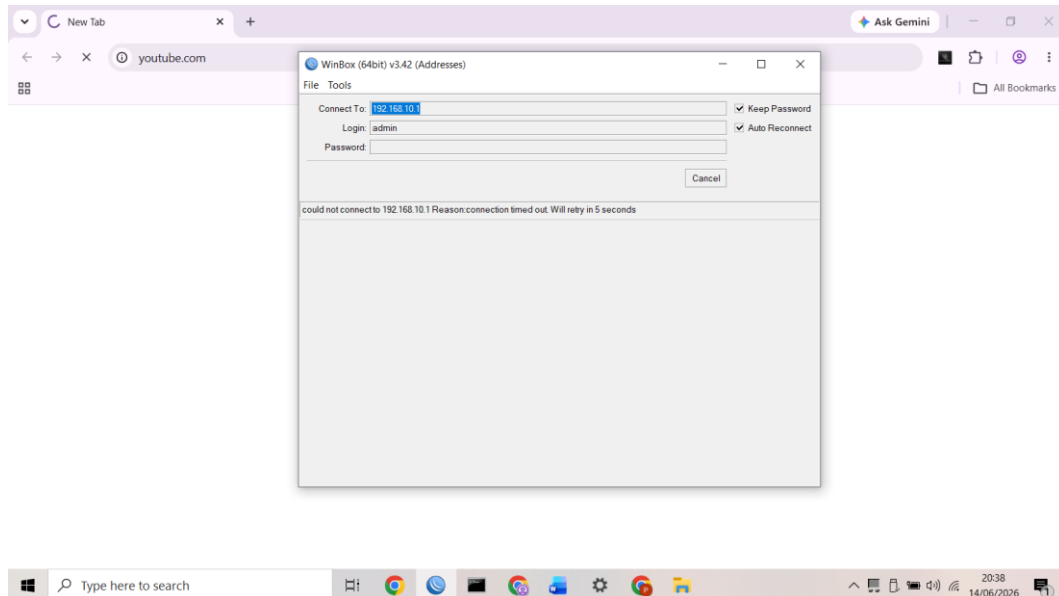


Sumber: Penulis, 2026

Gambar 5.87 Netcut sisi TSM

Gambar diatas secara jelas menunjukkan visualisasi pengujian penetrasi jaringan menggunakan aplikasi *NetCut* dari sisi perangkat penyerang dengan identitas IP address 192.168.10.9 dan MAC address 98:22:EF:49:7B:EB. Melalui fitur *speed* dan *lag control* yang diaktifkan oleh pihak yang tidak bertanggung jawab tersebut, terlihat upaya manipulasi *bandwidth* secara agresif yang diarahkan kepada target bernama "Putra" dengan IP address 192.168.10.5 dan MAC address 20:16:D8:08:64:99.

Penyerang menggeser parameter *MB Speed Control* dan *KB Speed Control* hingga menyentuh nilai minimal atau angka nol guna memotong arus data lokal dan melumpuhkan koneksi internet pada perangkat target. Eksekusi serangan sepihak ini sengaja dilakukan sebagai parameter pengujian untuk melihat sejauh mana ketahanan sistem pertahanan mandiri pada perangkat *endpoint* klien ketika berhadapan langsung dengan pemutusan jaringan lokal di udara.

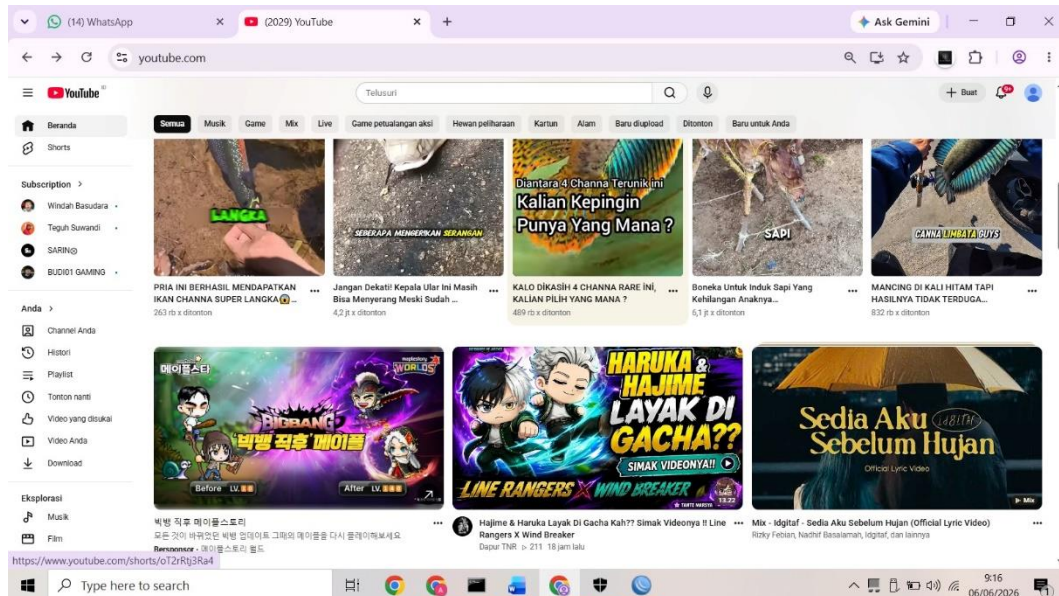


Sumber: Penulis, 2026

Gambar 5. 88 Sebelum di Aktifkan di Sisi TSM

Gambar di atas menunjukkan hasil pengujian ketersediaan layanan internet (*availability*) pada perangkat klien di dalam jaringan TSM sebelum diterapkannya konfigurasi *client isolation* pada *access point*. Pengujian dilakukan dengan mensimulasikan serangan pemutusan koneksi menggunakan aplikasi *netcut* dari perangkat penyerang yang berada pada jaringan yang sama.

Berdasarkan hasil pengujian, perangkat klien tidak dapat terhubung ke *router* mikrotik melalui aplikasi winbox yang ditandai dengan munculnya pesan "*could not connect to 192.168.10.1 (Reason: connection timed out)*". Kondisi ini menunjukkan bahwa serangan yang dilakukan berhasil mengganggu komunikasi jaringan sehingga akses pengguna terhadap layanan jaringan menjadi terputus. Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, perangkat klien masih rentan terhadap serangan pemutusan koneksi pada jaringan lokal.



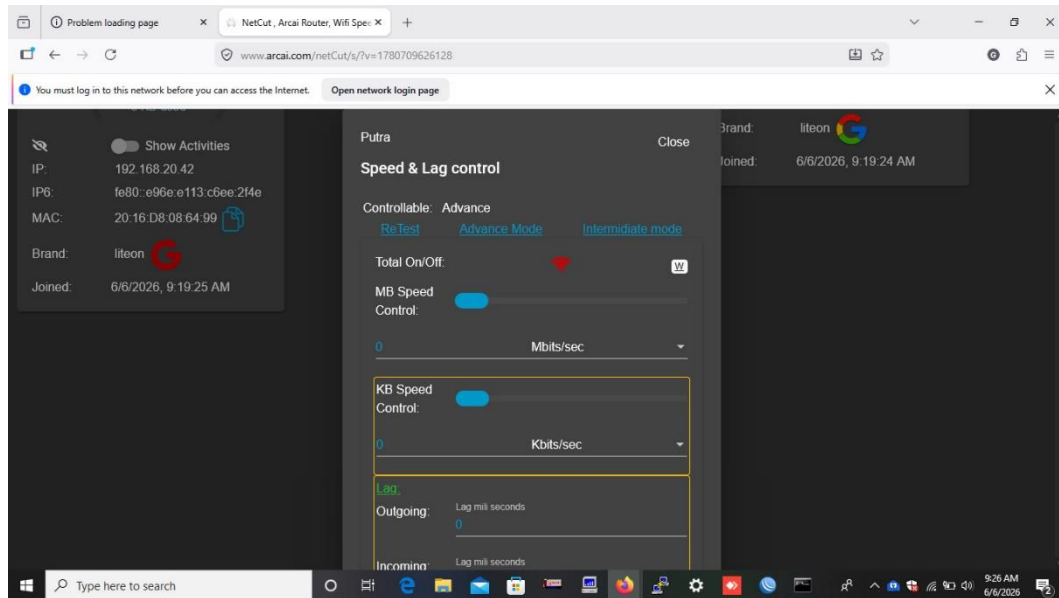
Sumber: Penulis, 2026

Gambar 5.89 Sudah di Aktifkan di Sisi TSM

Gambar diatas menunjukkan visualisasi pengujian ketersediaan layanan internet (*availability*) pada perangkat klien di dalam jaringan TSM setelah konfigurasi *client isolation* pada *access point* berhasil diaktifkan. Berdasarkan pembuktian hasil di lapangan, meskipun perangkat penyerang yang tidak bertanggung jawab telah memanipulasi parameter kecepatan hingga ke nilai minimal melalui panel *netcut* guna melumpuhkan target, mekanisme isolasi antar klien terbukti berhasil dan tetap tidak dapat ditembus.

Hal ini ditunjukkan secara nyata melalui kemampuan laptop pengujian yang masih dapat mengakses, memuat, serta memutar halaman video youtube secara lancar, responsif, dan *real-time* tanpa mengalami gejala pemutusan koneksi ataupun *request timeout*. Hasil ini memberikan kesimpulan krusial bahwa penerapan konfigurasi *client isolation* pada *access point* sukses memberikan perlindungan penuh, mematahkan upaya intervensi penyerang di jaringan TSM, dan memastikan ketersediaan akses internet pengguna tetap berjalan aman serta stabil.

b. TKR

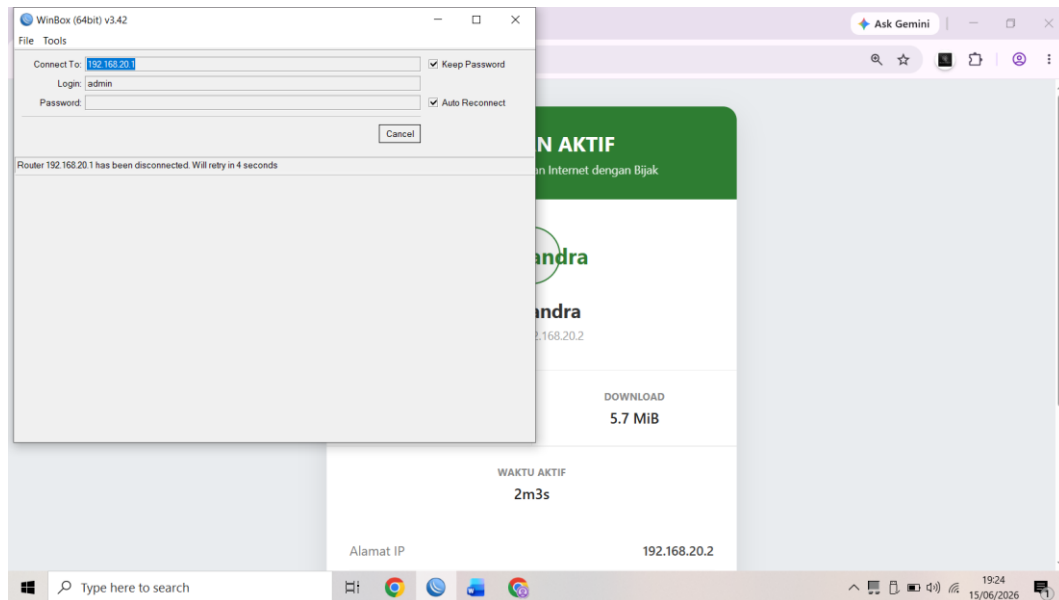


Sumber: Penulis, 2026

Gambar 5.90 Netcut sisi TKR

Gambar diatas secara jelas menunjukkan visualisasi pengujian penetrasi jaringan menggunakan aplikasi *netcut* dari sisi perangkat penyerang dengan identitas IP address 192.168.20.45 dan MAC address 98:22:EF:49:7B:EB. Melalui fitur *speed* dan *lag control* yang diaktifkan oleh pihak yang tidak bertanggung jawab tersebut, terlihat upaya manipulasi *bandwidth* secara agresif yang diarahkan kepada target bernama "Putra" dengan IP address 192.168.20.42 dan MAC address 20:16:D8:08:64:99.

Penyerang menggeser parameter *MB speed control* dan *KB speed control* hingga menyentuh nilai minimal atau angka nol guna memotong arus data lokal dan melumpuhkan koneksi internet pada perangkat target. Eksekusi serangan sepihak ini sengaja dilakukan sebagai parameter pengujian untuk melihat sejauh mana ketahanan sistem pertahanan mandiri pada perangkat *endpoint* klien ketika berhadapan langsung dengan pemutusan jaringan lokal di udara.

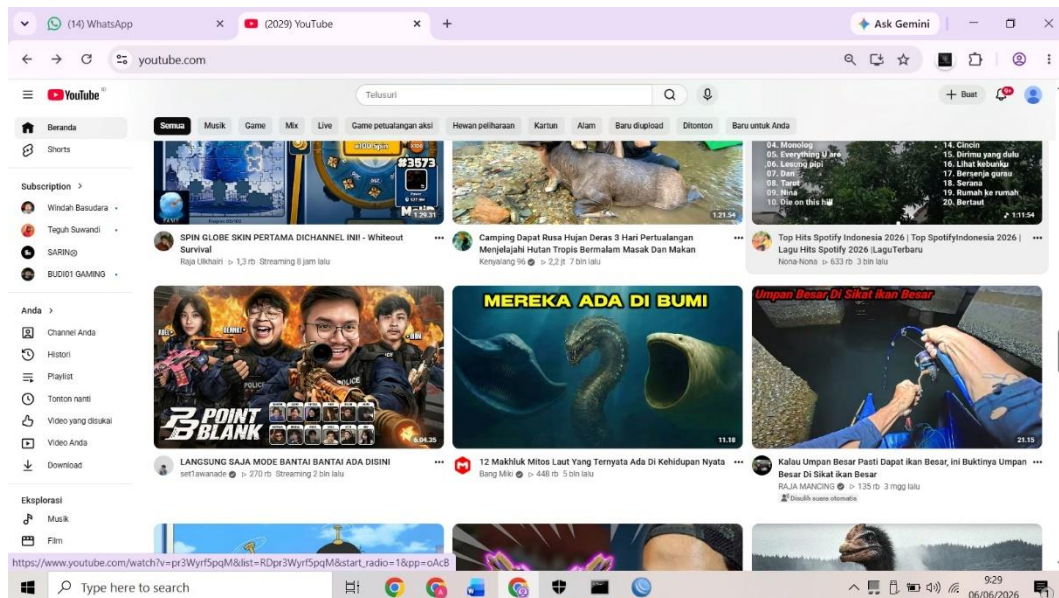


Sumber: Penulis, 2026

Gambar 5.91 Sebelum di Aktifkan di Sisi TKR

Gambar diatas menunjukkan visualisasi pengujian ketersediaan layanan internet (*availability*) pada perangkat klien di dalam jaringan TKR sebelum konfigurasi *client isolation* pada *access point* diterapkan. Pengujian dilakukan dengan mensimulasikan serangan menggunakan aplikasi *netcut* dari perangkat lain yang berada pada jaringan yang sama untuk mengganggu konektivitas perangkat target.

Berdasarkan hasil pengujian, perangkat klien mengalami gangguan koneksi yang ditandai dengan terputusnya akses ke *router* mikrotik melalui aplikasi winbox. Hal ini terlihat dari munculnya pesan bahwa koneksi ke *router* telah terputus (*disconnected*), yang menunjukkan bahwa serangan berhasil memengaruhi komunikasi jaringan pada perangkat target. Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, perangkat klien masih rentan terhadap serangan pemutusan koneksi yang dilakukan melalui jaringan lokal.



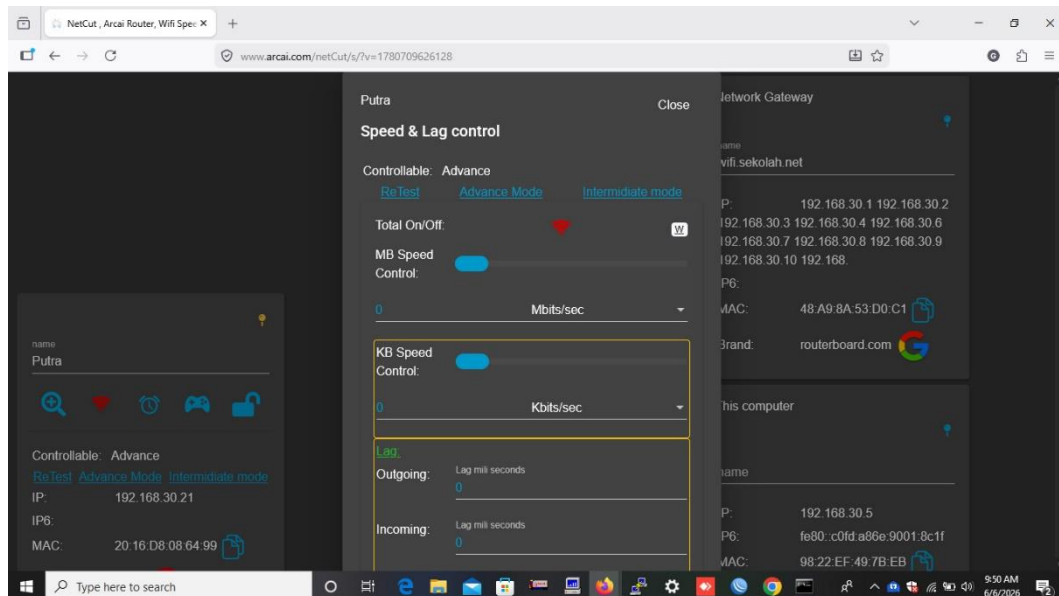
Sumber: Penulis, 2026

Gambar 5.92 Sudah di Aktifkan di Sisi TKR

Gambar diatas menunjukkan visualisasi pengujian ketersediaan layanan internet (*availability*) pada perangkat klien di dalam jaringan TKR setelah konfigurasi *client isolation* pada *access point* berhasil diaktifkan. Berdasarkan pembuktian hasil di lapangan, meskipun perangkat penyerang telah melakukan upaya manipulasi koneksi melalui aplikasi *netcut* guna melumpuhkan target, mekanisme isolasi antar klien terbukti berhasil mencegah terjadinya gangguan komunikasi pada perangkat yang diuji.

Hal ini ditunjukkan secara nyata melalui kemampuan laptop pengujian yang masih dapat mengakses, memuat, serta menampilkan halaman *website* youtube secara lancar, responsif, dan *real-time* tanpa mengalami gejala pemutusan koneksi ataupun *request timeout*. Hasil ini memberikan kesimpulan bahwa penerapan konfigurasi *client isolation* pada *access point* berhasil meningkatkan keamanan jaringan, mematahkan upaya intervensi penyerang di jaringan TKR, serta memastikan ketersediaan akses internet pengguna tetap berjalan aman dan stabil.

c. Kantor

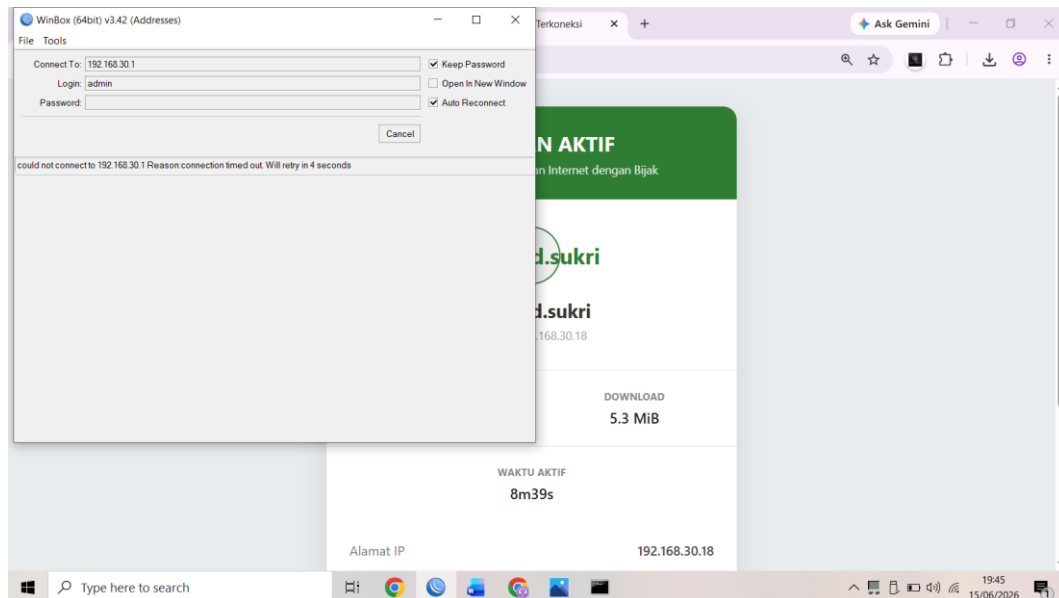


Sumber: Penulis, 2026

Gambar 5.93 Netcut sisi Kantor

Gambar diatas secara jelas menunjukkan visualisasi pengujian penetrasi jaringan menggunakan aplikasi *NetCut* dari sisi perangkat penyerang dengan identitas IP address 192.168.30.23 dan MAC address 98:22:EF:49:7B:EB. Melalui fitur *speed* dan *lag control* yang diaktifkan oleh pihak yang tidak bertanggung jawab tersebut, terlihat upaya manipulasi *bandwidth* secara agresif yang diarahkan kepada target bernama "Putra" dengan IP address 192.168.30.21 dan MAC address 20:16:D8:08:64:99.

Penyerang menggeser parameter *MB Speed Control* dan *KB Speed Control* hingga menyentuh nilai minimal atau angka nol guna memotong arus data lokal dan melumpuhkan koneksi internet pada perangkat target. Eksekusi serangan sepihak ini sengaja dilakukan sebagai parameter pengujian untuk melihat sejauh mana ketahanan sistem pertahanan mandiri pada perangkat *endpoint* klien ketika berhadapan langsung dengan pemutusan jaringan lokal di udara.

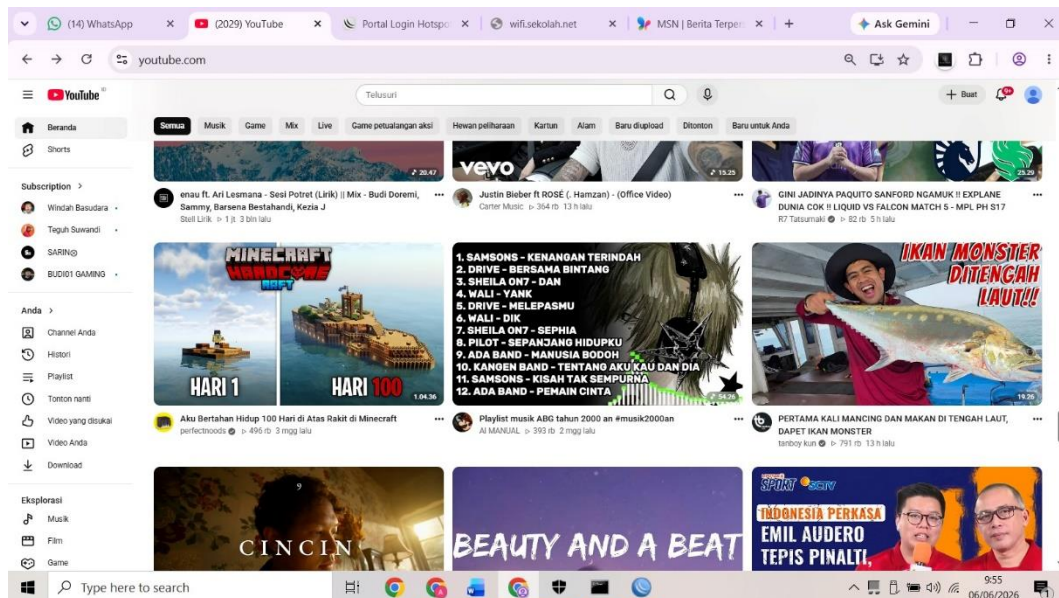


Sumber: Penulis, 2026

Gambar 5.94 Sebelum di Aktifkan di Sisi Kantor

Gambar diatas menunjukkan visualisasi pengujian ketersediaan layanan internet (*availability*) pada perangkat klien di dalam jaringan kantor sebelum konfigurasi *client isolation* pada *access point* diterapkan. Pengujian dilakukan dengan mensimulasikan serangan menggunakan aplikasi *netcut* dari perangkat lain yang berada pada jaringan yang sama untuk mengganggu konektivitas perangkat target.

Berdasarkan hasil pengujian, perangkat klien mengalami gangguan koneksi yang ditandai dengan ketidakmampuan mengakses *router* mikrotik melalui aplikasi winbox. Hal ini terlihat dari munculnya pesan "*could not connect to 192.168.30.1 Reason: connection timed out*", yang menunjukkan bahwa komunikasi jaringan antara perangkat klien dan *gateway* telah terganggu akibat serangan yang dilakukan. Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, perangkat klien masih rentan terhadap serangan pemutusan koneksi pada jaringan lokal.



Sumber: Penulis, 2026

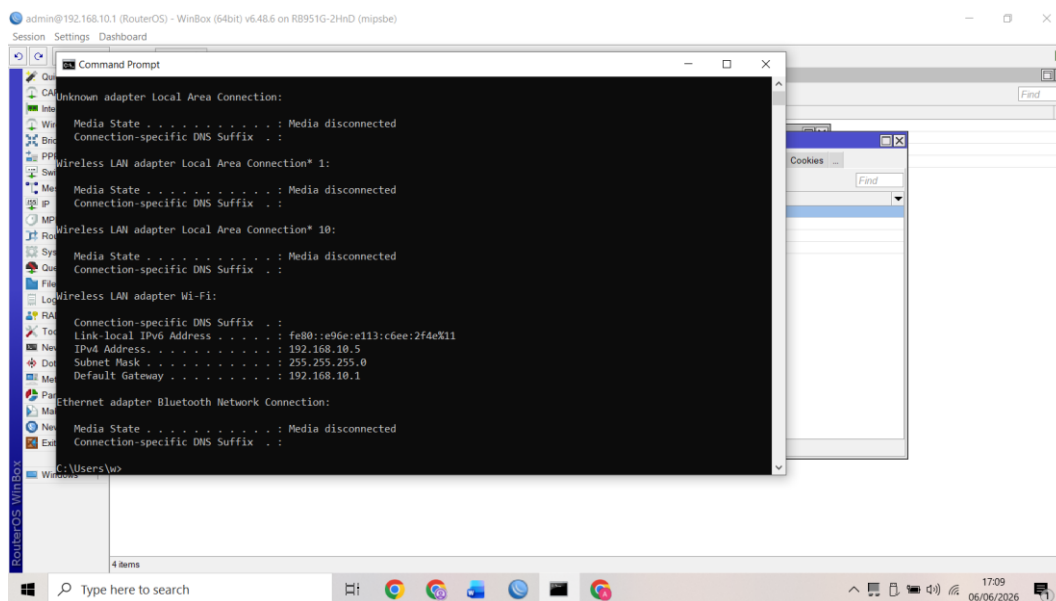
Gambar 5.95 Sudah di Aktifkan di Sisi Kantor

Gambar diatas menunjukkan visualisasi pengujian ketersediaan layanan internet (*availability*) pada perangkat klien di dalam jaringan kantor setelah konfigurasi *client isolation* pada *access point* berhasil diaktifkan. Berdasarkan pembuktian hasil di lapangan, meskipun perangkat penyerang telah melakukan upaya manipulasi koneksi melalui aplikasi *netcut* guna melumpuhkan target, mekanisme isolasi antar klien terbukti berhasil mencegah gangguan komunikasi pada perangkat yang diuji.

Hal ini ditunjukkan secara nyata melalui kemampuan laptop pengujian yang masih dapat mengakses, memuat, serta memutar halaman video youtube secara lancar, responsif, dan *real-time* tanpa mengalami gejala pemutusan koneksi ataupun *request timeout*. Hasil ini memberikan kesimpulan krusial bahwa penerapan konfigurasi *client isolation* pada *access point* berhasil memberikan perlindungan terhadap upaya intervensi penyerang di jaringan kantor serta memastikan ketersediaan akses internet pengguna tetap berjalan aman dan stabil.

2. CMD (*Command Prompt*)

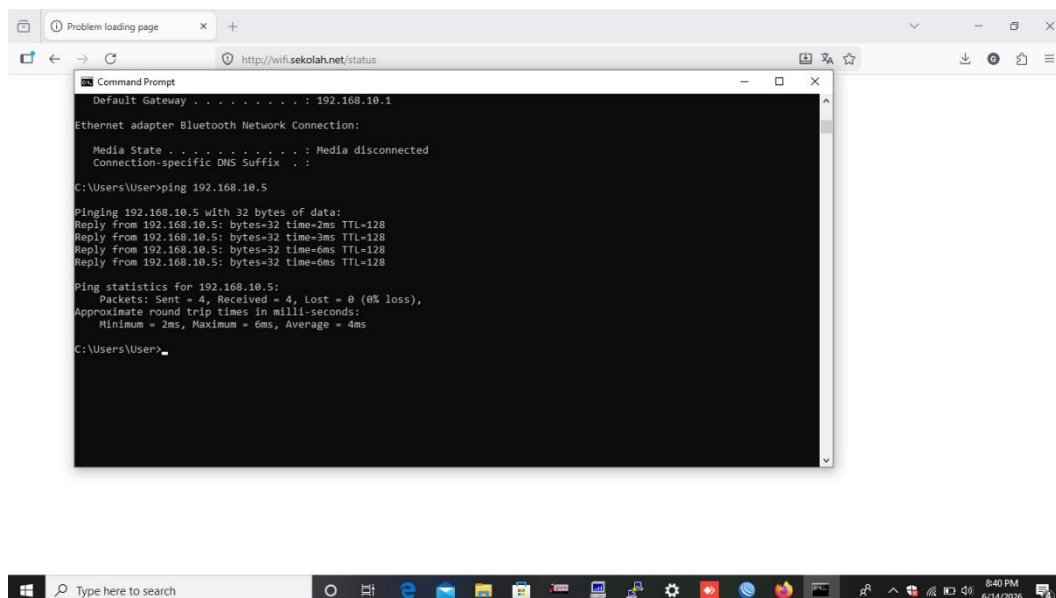
a. TSM



Sumber: Penulis, 2026

Gambar 5.96 Laptop Korban TSM

Pada pengujian validasi keamanan di sisi perangkat korban, dilakukan pengecekan konfigurasi parameter jaringan nirkabel *hotspot* menggunakan *command prompt*. Berdasarkan hasil eksekusi perintah *ipconfig*, diketahui perangkat korban telah terhubung secara sah pada segmen jaringan lokal yang dikelola oleh *routerOS* mikrotik (*hs-bridge*) dengan kepemilikan alamat IPv4 192.168.10.5 dan *default gateway* 192.168.10.1. Kondisi ini menandakan bahwa perangkat korban berada dalam status aktif dan siap menerima maupun mengirimkan lalu lintas data di dalam jaringan tersebut.

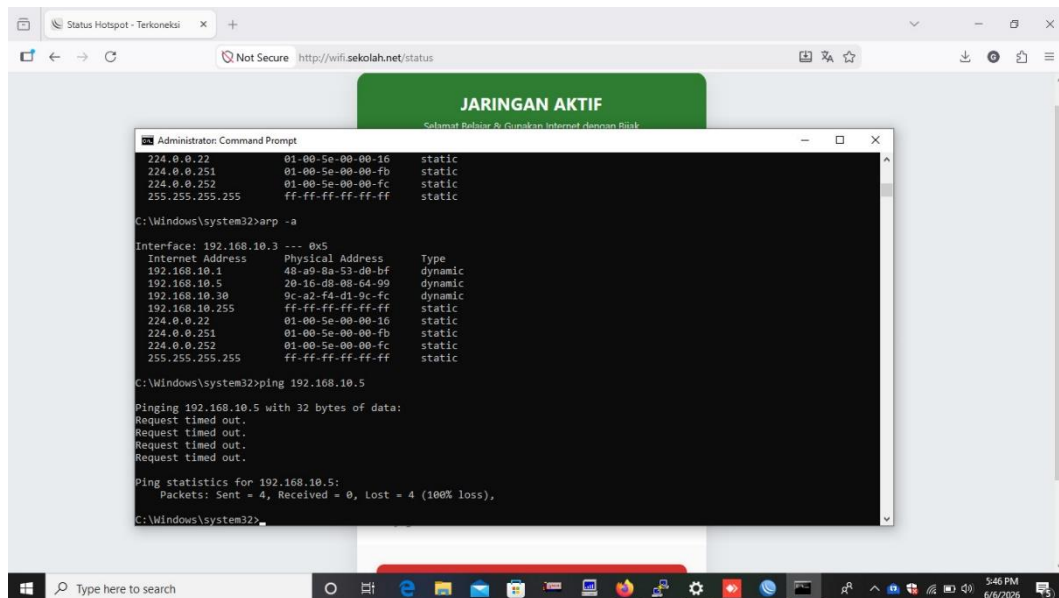


Sumber: Penulis, 2026

Gambar 5.97 Hasil Sebelum Diterapkan *Client Isolation* TSM

Untuk gambar sebelum *client isolation* diterapkan, terlihat bahwa perangkat penyerang masih dapat berkomunikasi langsung dengan perangkat korban. Hal ini dibuktikan melalui hasil perintah *ping* 192.168.10.5 yang memperoleh balasan (*reply*) secara berurutan dengan tingkat keberhasilan 100% dan tanpa kehilangan paket (0% *packet loss*). Kondisi tersebut menunjukkan bahwa perangkat penyerang dan perangkat korban masih berada dalam jalur komunikasi yang sama sehingga lalu lintas data antar-klien dapat berlangsung tanpa pembatasan.

Pengujian ini membuktikan bahwa sebelum penerapan fitur *client isolation* pada *access point*, komunikasi horizontal antar pengguna *wi-fi* masih terbuka. Dengan kondisi tersebut, perangkat penyerang masih memiliki visibilitas terhadap perangkat lain yang berada pada segmen jaringan yang sama dan berpotensi melakukan berbagai aktivitas seperti pemindaian jaringan, pengumpulan informasi perangkat, hingga serangan berbasis *ARP spoofing*. Hasil pengujian ini menjadi dasar perlunya penerapan *client isolation* untuk membatasi komunikasi langsung antar klien dan meningkatkan keamanan jaringan dari ancaman yang berasal dari pengguna dalam jaringan lokal.



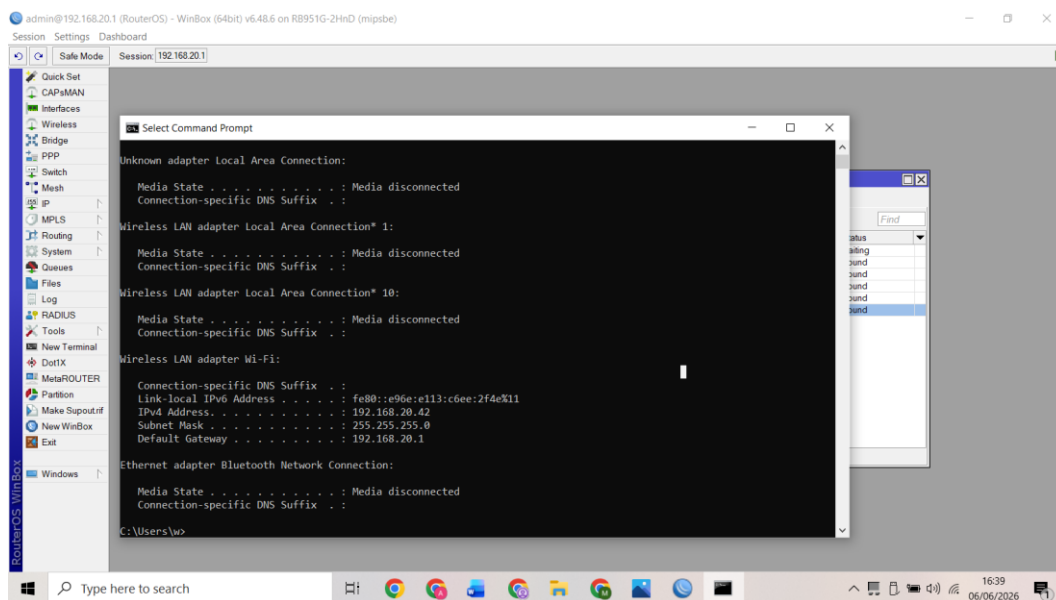
Sumber: Penulis, 2026

Gambar 5.98 Hasil Sudah Diterapkan *Client Isolation* TSM

Pengujian dari sudut pandang perangkat penyerang dilakukan untuk melihat sejauh mana ancaman interaksi lokal dapat terjadi di dalam segmen jaringan yang sama. Melalui perintah `arp -a`, laptop penyerang (yang menggunakan IP 192.168.10.3) awalnya mendeteksi keberadaan IP korban 192.168.10.5 di dalam tabel pemetaan ARP lokalnya. Namun, ketika penyerang mencoba meluncurkan eksploitasi langsung atau interaksi horizontal ke perangkat target dengan mengirimkan paket ICMP *echo request* melalui perintah `ping 192.168.10.5`, sistem *command prompt* secara konsisten menghasilkan status *request timed out* (RTO) dengan tingkat kegagalan paket (*packet loss*) mencapai 100%.

Kegagalan pengiriman data dari penyerang ke korban yang ditunjukkan oleh status RTO tersebut menjadi bukti valid dan konkrit bahwa fitur *client isolation* yang diterapkan pada *access point* telah berfungsi dengan sempurna. Kebijakan keamanan ini berhasil mengunci dan memutus jalur komunikasi horizontal antar-pengguna *wi-fi* secara permanen. Dampaknya, meskipun penyerang mencoba menggunakan berbagai macam pemindaian jaringan TSM, penyerang akan kehilangan visibilitas penuh untuk mengeksekusi serangan berbahaya seperti *ARP spoofing*, ataupun upaya penyusupan lainnya terhadap perangkat korban.

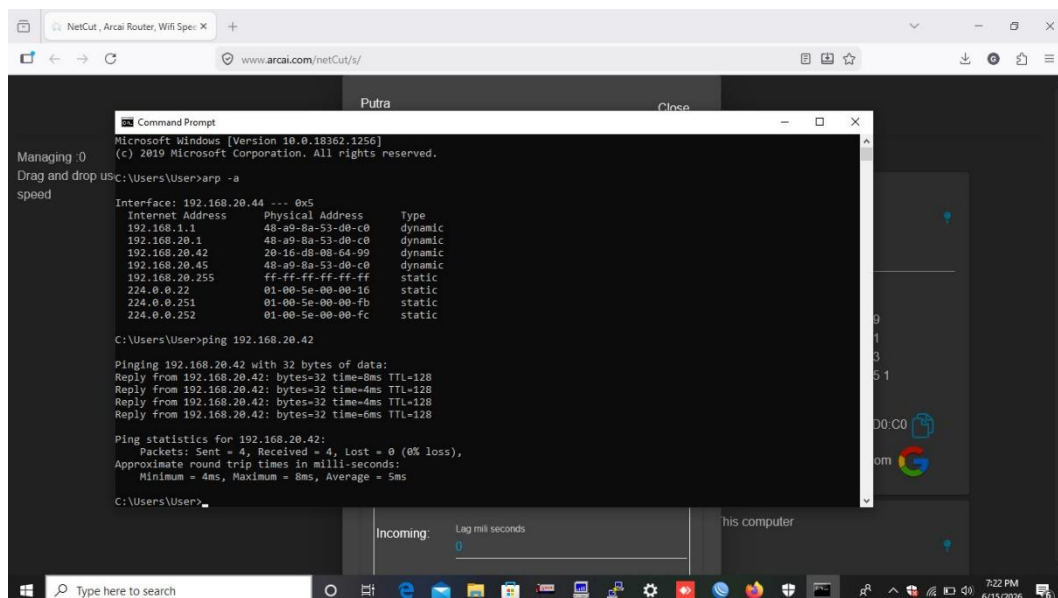
b. TKR



Sumber: Penulis, 2026

Gambar 5.99 Laptop Korban TKR

Pada pengujian validasi keamanan di sisi perangkat korban, dilakukan pengecekan konfigurasi parameter jaringan nirkabel *hotspot* menggunakan *command prompt*. Berdasarkan hasil eksekusi perintah *ipconfig*, diketahui perangkat korban telah terhubung secara sah pada segmen jaringan lokal yang dikelola oleh *routerOS* mikrotik (*hs-bridge*) dengan kepemilikan alamat IPv4 192.168.20.42 dan *default gateway* 192.168.20.1. Kondisi ini menandakan bahwa perangkat korban berada dalam status aktif dan siap menerima maupun mengirimkan lalu lintas data di dalam jaringan tersebut.



Sumber: Penulis, 2026

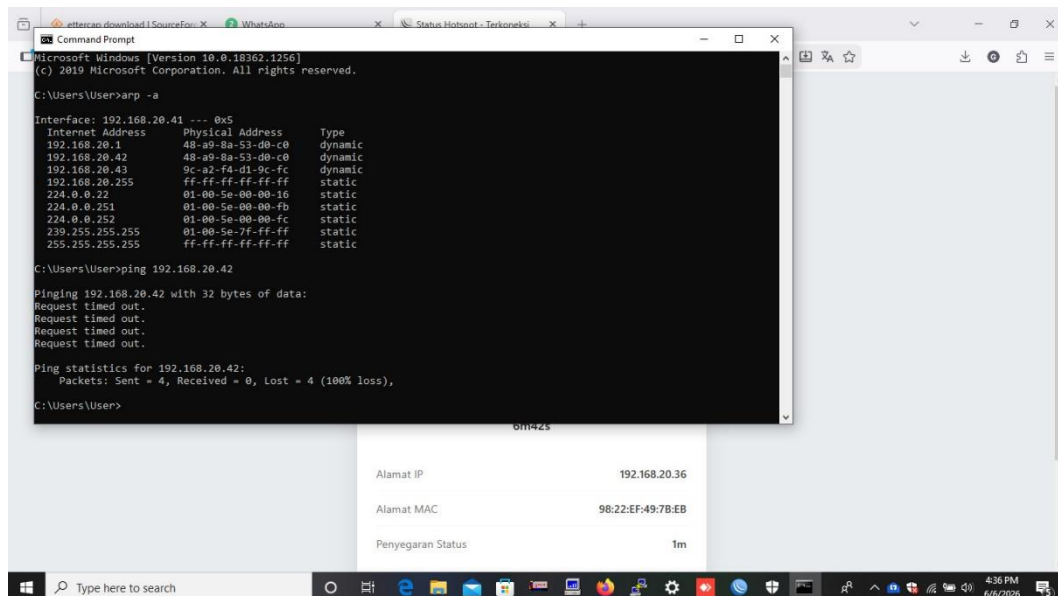
Gambar 5.100 Hasil Sebelum Diterapkan *Client Isolation* TKR

Pengujian dari sudut pandang perangkat penyerang dilakukan untuk melihat sejauh mana interaksi antar perangkat dapat terjadi di dalam segmen jaringan TKR yang sama. Melalui perintah `arp -a`, laptop penyerang yang menggunakan IP 192.168.20.44 berhasil mendeteksi keberadaan perangkat target dengan IP 192.168.20.42 pada tabel ARP lokal. Selanjutnya, pengujian konektivitas dilakukan menggunakan perintah `ping 192.168.20.42` untuk mengetahui apakah komunikasi langsung antar perangkat masih dapat berlangsung.

Berdasarkan hasil pengujian, seluruh paket *ICMP echo request* yang dikirimkan oleh perangkat penyerang memperoleh balasan (*reply*) dari perangkat target dengan tingkat keberhasilan 100% dan tanpa kehilangan paket (0% *packet loss*). Hasil tersebut menunjukkan bahwa komunikasi horizontal antar pengguna *wi-fi* masih terbuka dan tidak terdapat mekanisme pembatasan akses antar klien pada jaringan TKR.

Kondisi ini membuktikan bahwa sebelum penerapan fitur *client isolation* pada *access point*, perangkat penyerang masih dapat mendeteksi serta berkomunikasi langsung dengan perangkat lain yang berada dalam jaringan yang sama. Dengan adanya akses tersebut, berbagai aktivitas seperti pemindaian jaringan, pengumpulan informasi perangkat, maupun serangan berbasis ARP

spoofing berpotensi dilakukan oleh pihak yang tidak bertanggung jawab terhadap perangkat korban.



Sumber: Penulis, 2026

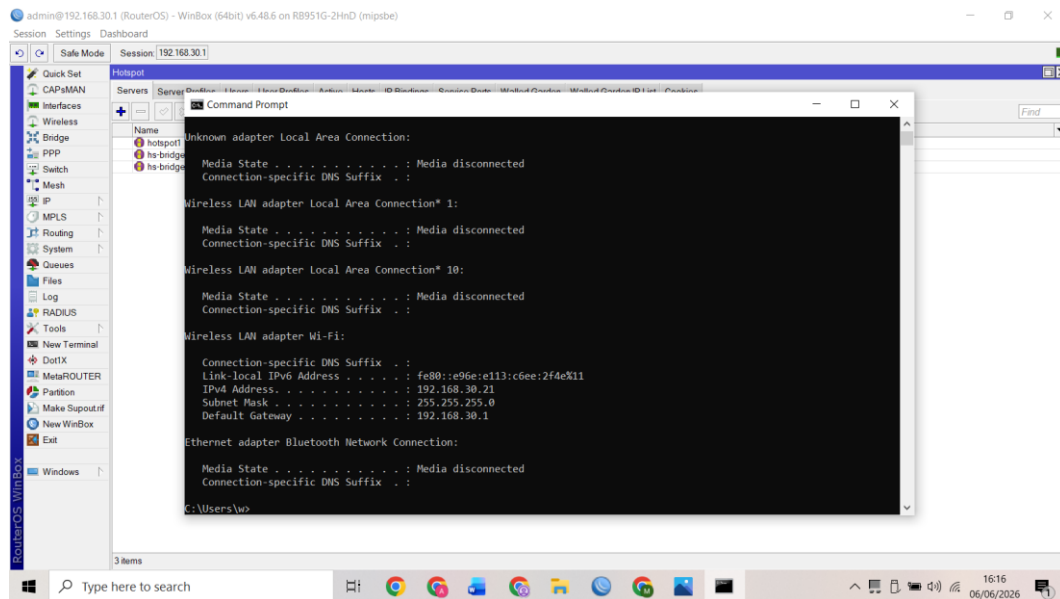
Gambar 5.101 Hasil Sudah Diterapkan *Client Isolation* TKR

Pengujian dari sudut pandang perangkat penyerang dilakukan untuk melihat sejauh mana ancaman interaksi lokal dapat terjadi di dalam segmen jaringan yang sama. Melalui perintah `arp -a`, laptop penyerang (yang menggunakan IP 192.168.20.41) awalnya mendeteksi keberadaan IP korban 192.168.20.42 di dalam tabel pemetaan ARP lokalnya. Namun, ketika penyerang mencoba meluncurkan eksploitasi langsung atau interaksi horizontal ke perangkat target dengan mengirimkan paket ICMP *echo request* melalui perintah `ping 192.168.20.42`, sistem *command prompt* secara konsisten menghasilkan status *request timed out* (RTO) dengan tingkat kegagalan paket (*packet loss*) mencapai 100%.

Kegagalan pengiriman data dari penyerang ke korban yang ditunjukkan oleh status RTO tersebut menjadi bukti valid dan konkrit bahwa fitur *client isolation* yang diterapkan pada *access point* telah berfungsi dengan sempurna. Kebijakan keamanan ini berhasil mengunci dan memutus jalur komunikasi horizontal antar-pengguna *wi-fi* secara permanen. Dampaknya, meskipun penyerang mencoba menggunakan berbagai macam pemindaian jaringan TKR, penyerang akan

kehilangan visibilitas penuh untuk mengeksekusi serangan berbahaya seperti ARP *spoofing*, ataupun upaya penyusupan lainnya terhadap perangkat korban.

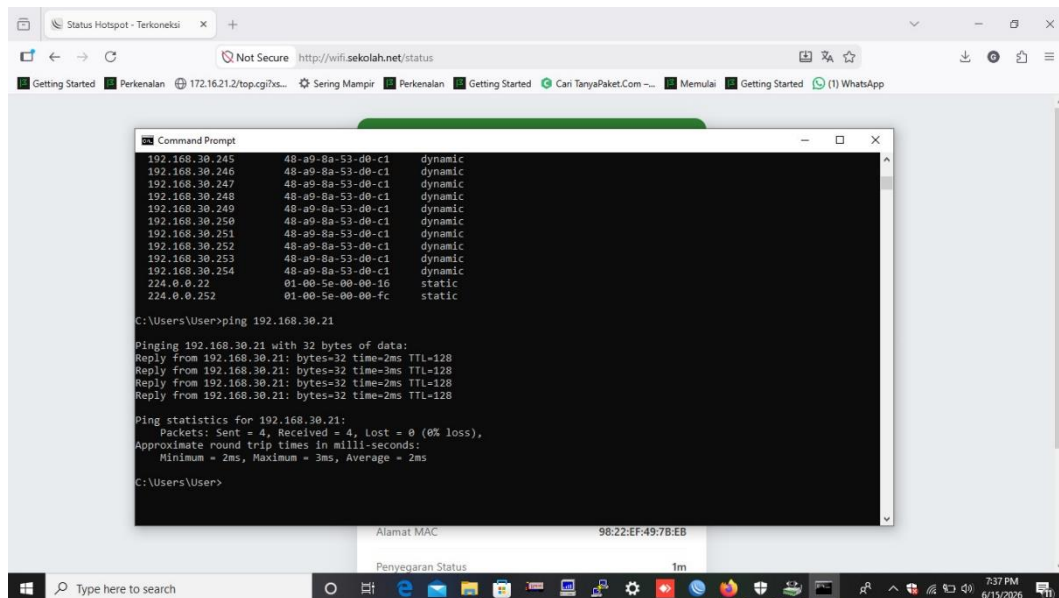
c. Kantor



Sumber: Penulis, 2026

Gambar 5.102 Laptop Korban Kantor

Pada pengujian validasi keamanan di sisi perangkat korban, dilakukan pengecekan konfigurasi parameter jaringan nirkabel *hotspot* menggunakan *command prompt*. Berdasarkan hasil eksekusi perintah *ipconfig*, diketahui perangkat korban telah terhubung secara sah pada segmen jaringan lokal yang dikelola oleh *routerOS* mikrotik (*hs-bridge*) dengan kepemilikan alamat IPv4 192.168.30.21 dan *default gateway* 192.168.30.1. Kondisi ini menandakan bahwa perangkat korban berada dalam status aktif dan siap menerima maupun mengirimkan lalu lintas data di dalam jaringan tersebut.



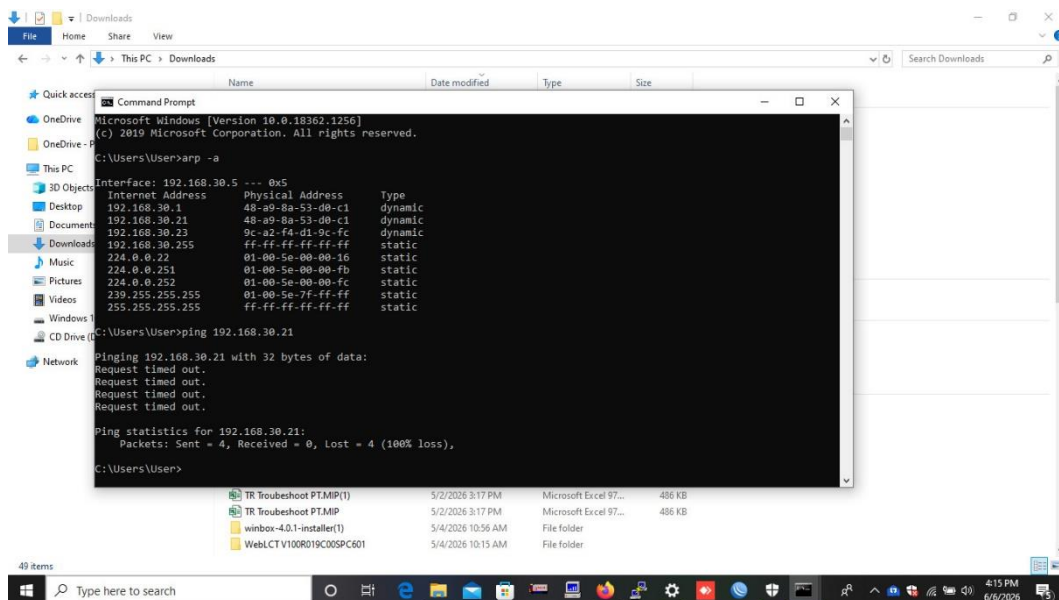
Sumber: Penulis, 2026

Gambar 5.103 Hasil Sebelum Diterapkan *Client Isolation* Kantor

Pengujian dari sudut pandang perangkat penyerang dilakukan untuk mengetahui tingkat keterhubungan antar perangkat dalam jaringan kantor sebelum penerapan fitur *client isolation*. Melalui tabel ARP yang ditampilkan menggunakan perintah `arp -a`, perangkat penyerang masih dapat mendeteksi keberadaan perangkat target yang berada pada segmen jaringan yang sama. Selanjutnya dilakukan pengujian konektivitas menggunakan perintah `ping 192.168.30.21` untuk memastikan apakah komunikasi langsung antar perangkat masih dapat dilakukan.

Berdasarkan hasil pengujian, seluruh paket ICMP *echo request* yang dikirimkan berhasil memperoleh balasan (*reply*) dari perangkat target dengan tingkat keberhasilan 100% dan tanpa kehilangan paket (0% *packet loss*). Nilai waktu respons yang rendah menunjukkan bahwa komunikasi antar perangkat berlangsung secara normal tanpa adanya pembatasan akses pada jaringan lokal.

Hasil pengujian ini membuktikan bahwa sebelum penerapan *client isolation* pada *access point*, perangkat penyerang masih dapat mendeteksi dan berkomunikasi secara langsung dengan perangkat lain yang terhubung pada jaringan kantor. Kondisi tersebut menunjukkan bahwa komunikasi horizontal antar pengguna *wi-fi* masih terbuka sehingga berpotensi dimanfaatkan untuk melakukan pemindaian jaringan, pengumpulan informasi perangkat, maupun serangan berbasis ARP *spoofing* terhadap perangkat lain dalam jaringan yang sama.



Sumber: Penulis, 2026

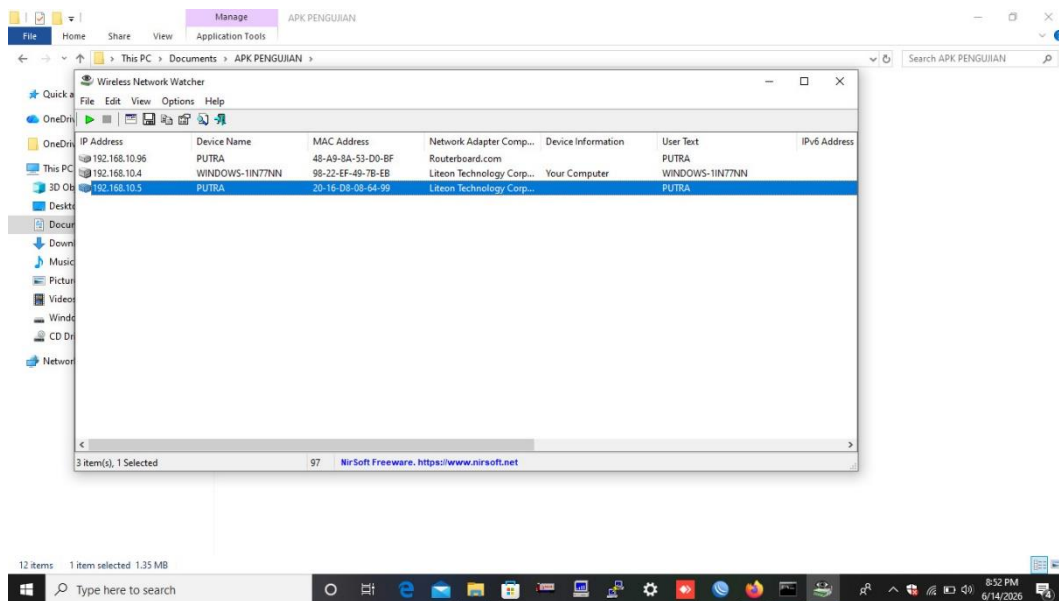
Gambar 5.104 Hasil Sudah Diterapkan *Client Isolation* Kantor

Pengujian dari sudut pandang perangkat penyerang dilakukan untuk melihat sejauh mana ancaman interaksi lokal dapat terjadi di dalam segmen jaringan yang sama. Melalui perintah `arp -a`, laptop penyerang (yang menggunakan IP 192.168.30.5) awalnya mendeteksi keberadaan IP korban 192.168.30.21 di dalam tabel pemetaan ARP lokalnya. Namun, ketika penyerang mencoba melancarkan eksploitasi langsung atau interaksi horizontal ke perangkat target dengan mengirimkan paket ICMP *echo request* melalui perintah `ping 192.168.30.21`, sistem *command prompt* secara konsisten menghasilkan status *request timed out* (RTO) dengan tingkat kegagalan paket (*packet loss*) mencapai 100%.

Kegagalan pengiriman data dari penyerang ke korban yang ditunjukkan oleh status RTO tersebut menjadi bukti valid dan konkrit bahwa fitur *client isolation* yang diterapkan pada *access point* telah berfungsi dengan sempurna. Kebijakan keamanan ini berhasil mengunci dan memutus jalur komunikasi horizontal antar-pengguna *wi-fi* secara permanen. Dampaknya, meskipun penyerang mencoba menggunakan berbagai macam pemindaian jaringan kantor, penyerang akan kehilangan visibilitas penuh untuk mengeksekusi serangan berbahaya seperti *ARP spoofing*, ataupun upaya penyusupan lainnya terhadap perangkat korban.

3. *Wireless Network Watcher*

a. TSM

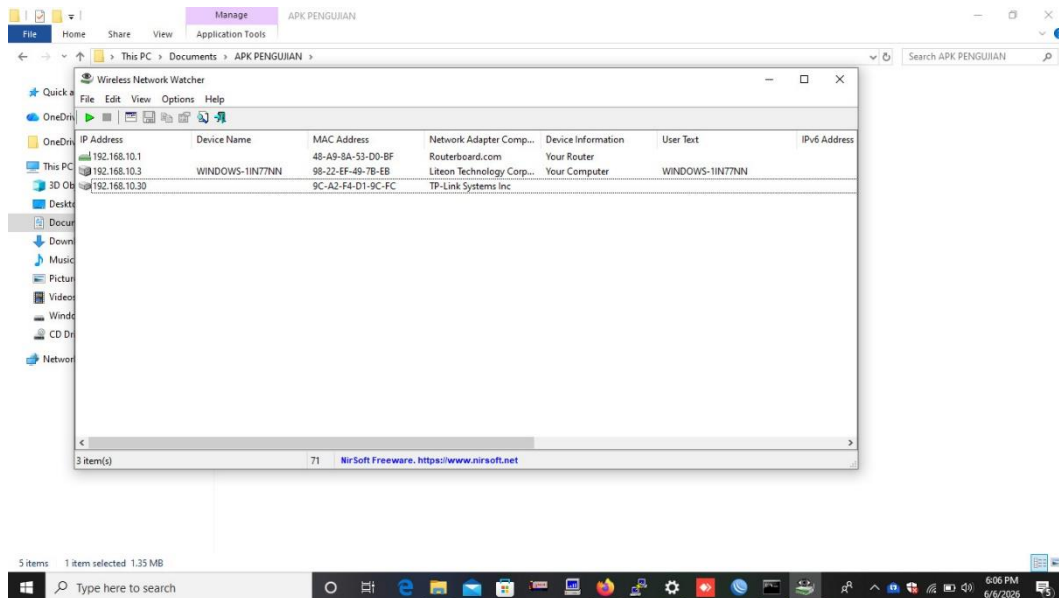


Sumber: Penulis, 2026

Gambar 5.105 Pengujian Sebelum Penerapan *Client Isolation* TSM

Pengujian menggunakan aplikasi *wireless network watcher* dilakukan dari sisi perangkat penyerang untuk mengetahui apakah perangkat lain yang berada pada jaringan TSM masih dapat dideteksi sebelum penerapan fitur *client isolation*. Hasil pemindaian menunjukkan bahwa perangkat penyerang berhasil menemukan beberapa *host* yang aktif pada jaringan, termasuk perangkat target dengan alamat IP 192.168.10.5. Selain itu, informasi perangkat seperti alamat MAC, nama perangkat, serta identitas pengguna juga masih dapat ditampilkan oleh aplikasi.

Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, visibilitas antar pengguna dalam jaringan TSM masih terbuka. Kondisi ini memungkinkan perangkat penyerang untuk melakukan identifikasi perangkat lain yang terhubung ke jaringan, sehingga berpotensi dimanfaatkan untuk aktivitas pemindaian jaringan, pengumpulan informasi perangkat, maupun serangan lanjutan terhadap pengguna lain yang berada dalam segmen jaringan yang sama.



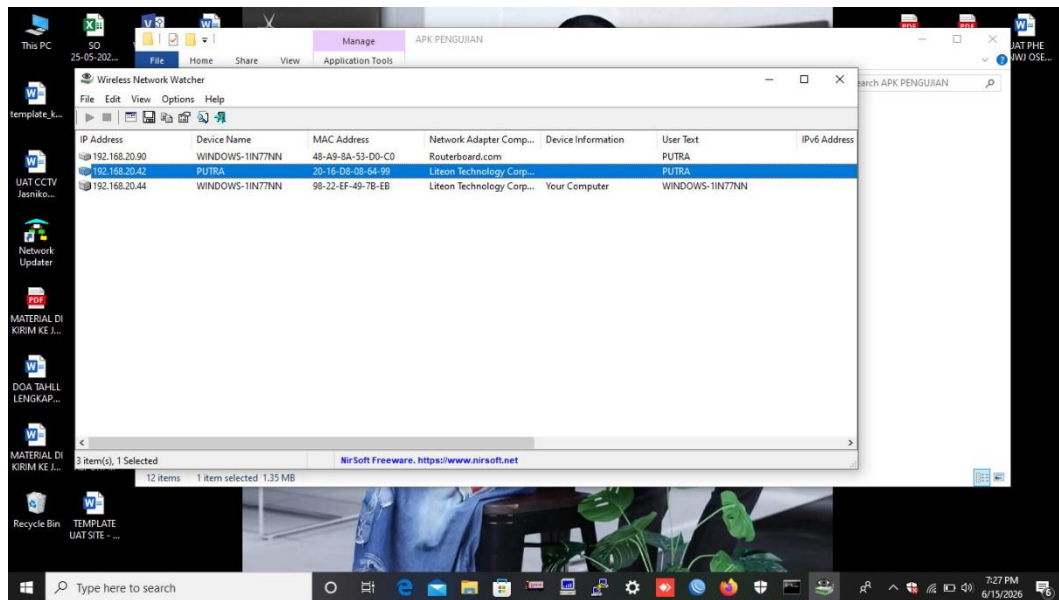
Sumber: Penulis, 2026

Gambar 5.106 Pengujian Sudah Penerapan *Client Isolation* TSM

Pengujian menggunakan aplikasi *wireless network watcher* kembali dilakukan setelah fitur *client isolation* pada *access point* diaktifkan. Berdasarkan hasil pemindaian, perangkat penyerang tidak lagi dapat mendeteksi perangkat target yang sebelumnya terhubung pada jaringan TSM. Daftar perangkat yang ditampilkan hanya menunjukkan perangkat penyerang, *router*, dan perangkat jaringan yang diizinkan untuk berkomunikasi, sementara perangkat klien lain tidak lagi terlihat pada hasil pemindaian.

Kondisi tersebut menunjukkan bahwa fitur *client isolation* berhasil membatasi visibilitas antar pengguna dalam jaringan nirkabel. Dengan terputusnya akses deteksi antar klien, perangkat penyerang kehilangan kemampuan untuk mengidentifikasi keberadaan perangkat lain yang terhubung pada jaringan TSM. Hasil ini membuktikan bahwa *client isolation* efektif dalam mengurangi risiko pemindaian jaringan, pengumpulan informasi perangkat, serta berbagai serangan yang memerlukan komunikasi langsung antar pengguna dalam satu segmen jaringan.

b. TKR

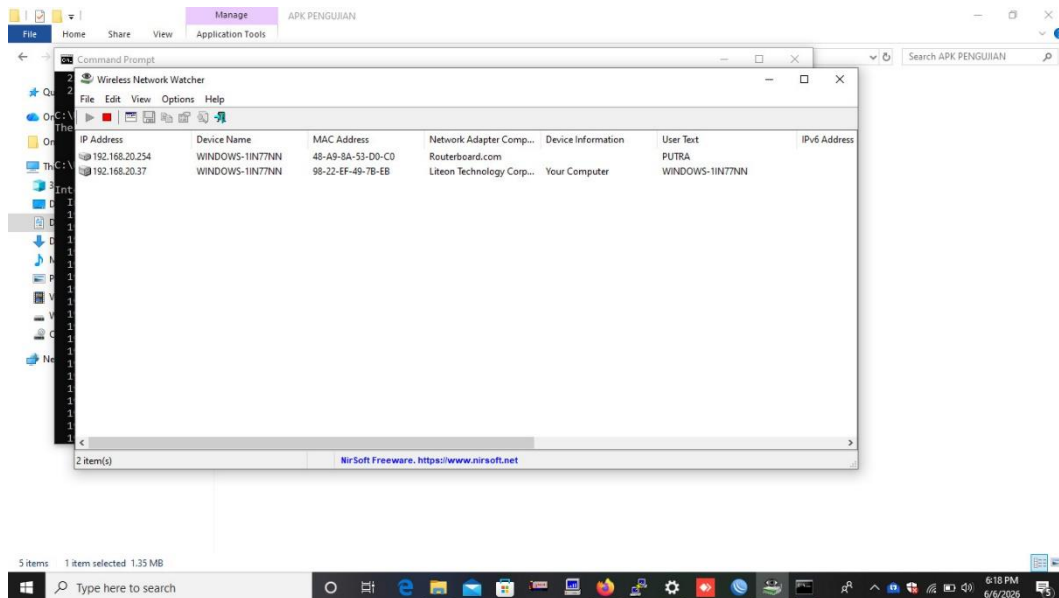


Sumber: Penulis, 2026

Gambar 5.107 Pengujian Sebelum Penerapan *Client Isolation* TKR

Pengujian menggunakan aplikasi *wireless network watcher* dilakukan dari sisi perangkat penyerang untuk mengetahui apakah perangkat lain yang berada pada jaringan TKR masih dapat dideteksi sebelum penerapan fitur *client isolation*. Hasil pemindaian menunjukkan bahwa perangkat penyerang berhasil menemukan beberapa *host* yang aktif pada jaringan, termasuk perangkat target dengan alamat IP 192.168.20.42. Selain itu, informasi perangkat seperti alamat MAC, nama perangkat, serta identitas pengguna juga masih dapat ditampilkan oleh aplikasi.

Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, visibilitas antar pengguna dalam jaringan TKR masih terbuka. Kondisi ini memungkinkan perangkat penyerang untuk melakukan identifikasi perangkat lain yang terhubung ke jaringan, sehingga berpotensi dimanfaatkan untuk aktivitas pemindaian jaringan, pengumpulan informasi perangkat, maupun serangan lanjutan terhadap pengguna lain yang berada dalam segmen jaringan yang sama.



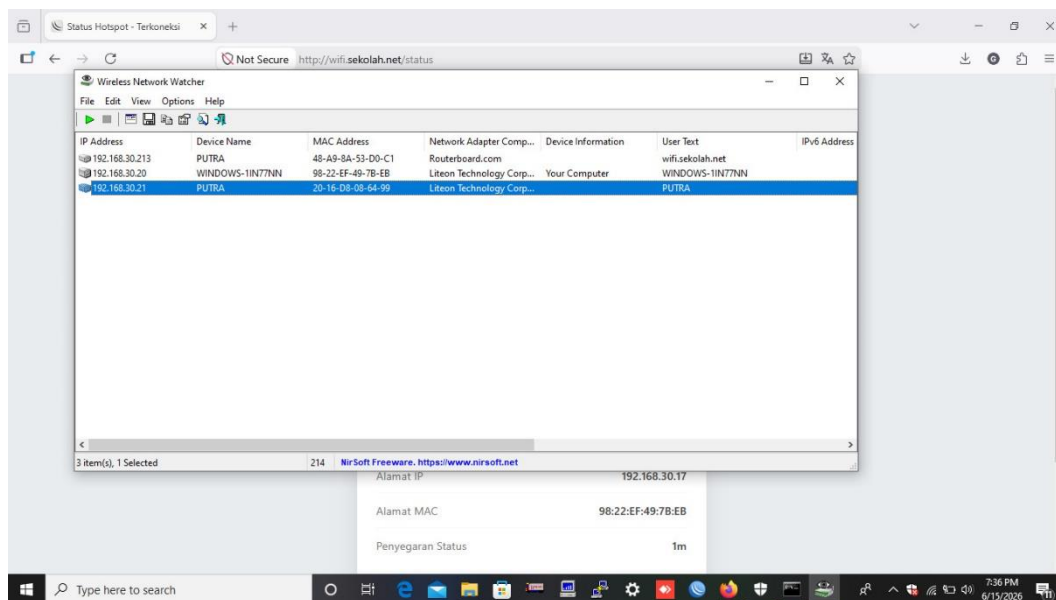
Sumber: Penulis, 2026

Gambar 5.108 Pengujian Sudah Penerapan *Client Isolation* TKR

Pengujian menggunakan aplikasi *wireless network watcher* kembali dilakukan setelah fitur *client isolation* pada *access point* diaktifkan. Berdasarkan hasil pemindaian, perangkat penyerang tidak lagi dapat mendeteksi perangkat target yang sebelumnya terhubung pada jaringan TKR. Daftar perangkat yang ditampilkan hanya menunjukkan perangkat penyerang, *router*, dan perangkat jaringan yang diizinkan untuk berkomunikasi, sementara perangkat klien lain tidak lagi terlihat pada hasil pemindaian.

Kondisi tersebut menunjukkan bahwa fitur *client isolation* berhasil membatasi visibilitas antar pengguna dalam jaringan nirkabel. Dengan terputusnya akses deteksi antar klien, perangkat penyerang kehilangan kemampuan untuk mengidentifikasi keberadaan perangkat lain yang terhubung pada jaringan TKR. Hasil ini membuktikan bahwa *client isolation* efektif dalam mengurangi risiko pemindaian jaringan, pengumpulan informasi perangkat, serta berbagai serangan yang memerlukan komunikasi langsung antar pengguna dalam satu segmen jaringan.

c. Kantor

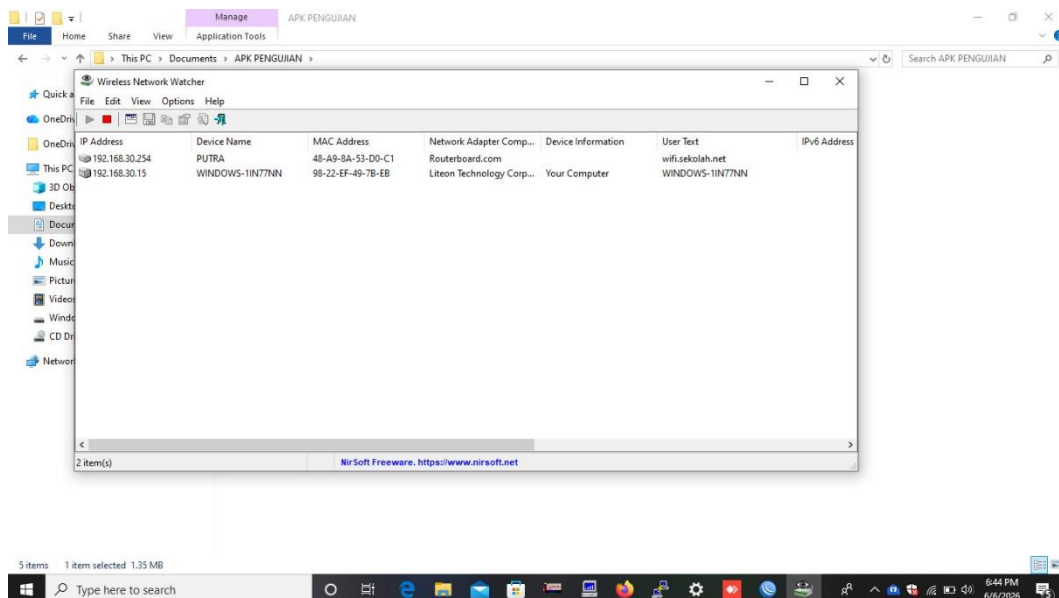


Sumber: Penulis, 2026

Gambar 5.109 Pengujian Sebelum Penerapan *Client Isolation* Kantor

Pengujian menggunakan aplikasi *wireless network watcher* dilakukan dari sisi perangkat penyerang untuk mengetahui apakah perangkat lain yang berada pada jaringan kantor masih dapat dideteksi sebelum penerapan fitur *client isolation*. Hasil pemindaian menunjukkan bahwa perangkat penyerang berhasil menemukan beberapa *host* yang aktif pada jaringan, termasuk perangkat target dengan alamat IP 192.168.30.21. Selain itu, informasi perangkat seperti alamat MAC, nama perangkat, serta identitas pengguna juga masih dapat ditampilkan oleh aplikasi.

Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, visibilitas antar pengguna dalam jaringan kantor masih terbuka. Kondisi ini memungkinkan perangkat penyerang untuk melakukan identifikasi perangkat lain yang terhubung ke jaringan, sehingga berpotensi dimanfaatkan untuk aktivitas pemindaian jaringan, pengumpulan informasi perangkat, maupun serangan lanjutan terhadap pengguna lain yang berada dalam segmen jaringan yang sama.



Sumber: Penulis, 2026

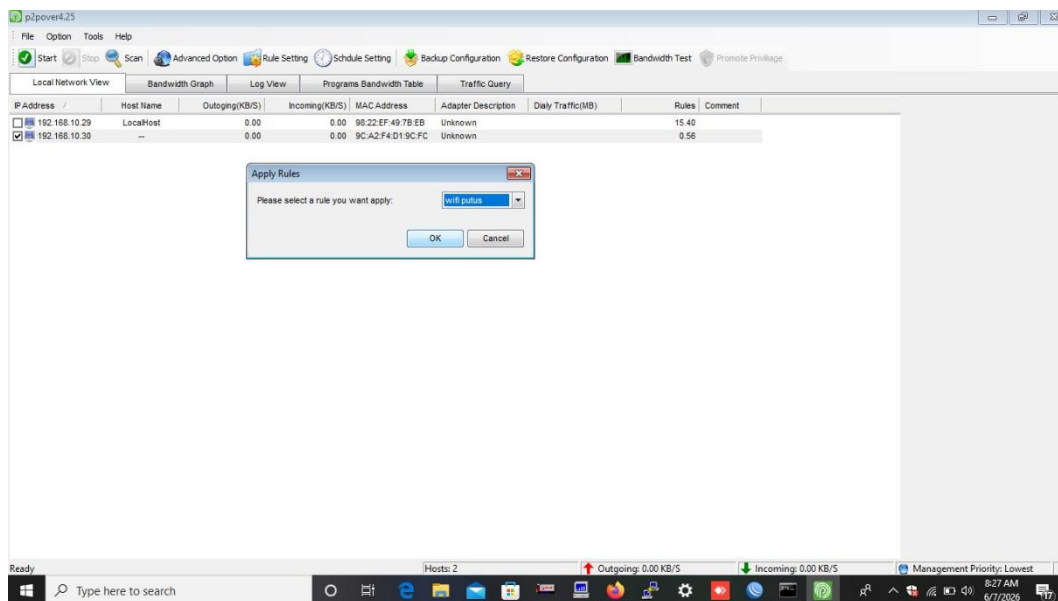
Gambar 5.110 Pengujian Sebelum Penerapan *Client Isolation* Kantor

Pengujian menggunakan aplikasi *wireless network watcher* kembali dilakukan setelah fitur *client isolation* pada *access point* diaktifkan. Berdasarkan hasil pemindaian, perangkat penyerang tidak lagi dapat mendeteksi perangkat target yang sebelumnya terhubung pada jaringan kantor. Daftar perangkat yang ditampilkan hanya menunjukkan perangkat penyerang, *router*, dan perangkat jaringan yang diizinkan untuk berkomunikasi, sementara perangkat klien lain tidak lagi terlihat pada hasil pemindaian.

Kondisi tersebut menunjukkan bahwa fitur *client isolation* berhasil membatasi visibilitas antar pengguna dalam jaringan nirkabel. Dengan terputusnya akses deteksi antar klien, perangkat penyerang kehilangan kemampuan untuk mengidentifikasi keberadaan perangkat lain yang terhubung pada jaringan kantor. Hasil ini membuktikan bahwa *client isolation* efektif dalam mengurangi risiko pemindaian jaringan, pengumpulan informasi perangkat, serta berbagai serangan yang memerlukan komunikasi langsung antar pengguna dalam satu segmen jaringan.

4. P2pover

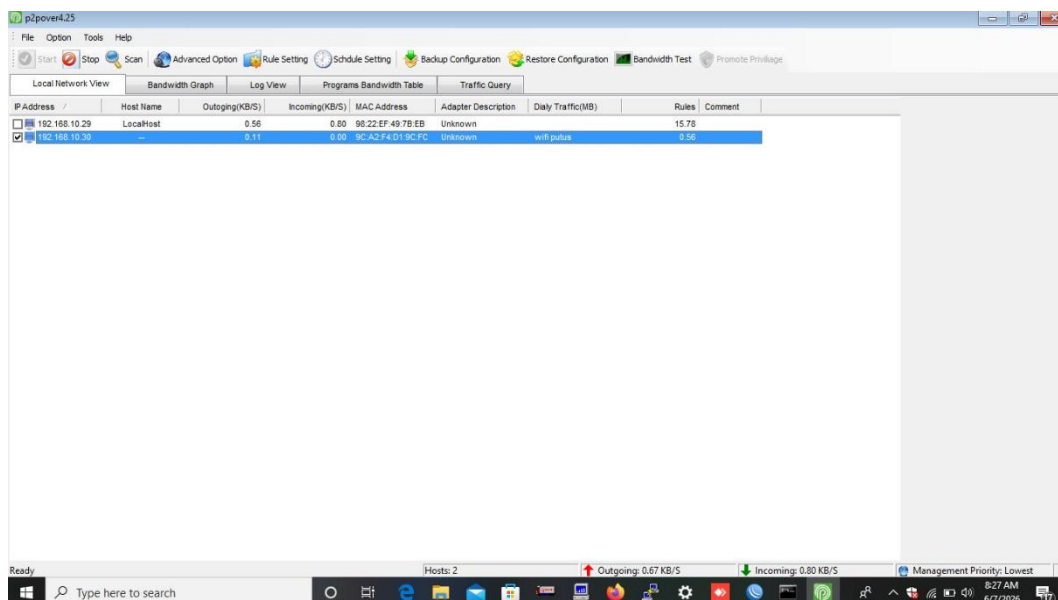
a. TSM



Sumber: Penulis, 2026

Gambar 5.111 Rules Wi-Fi Putus TSM

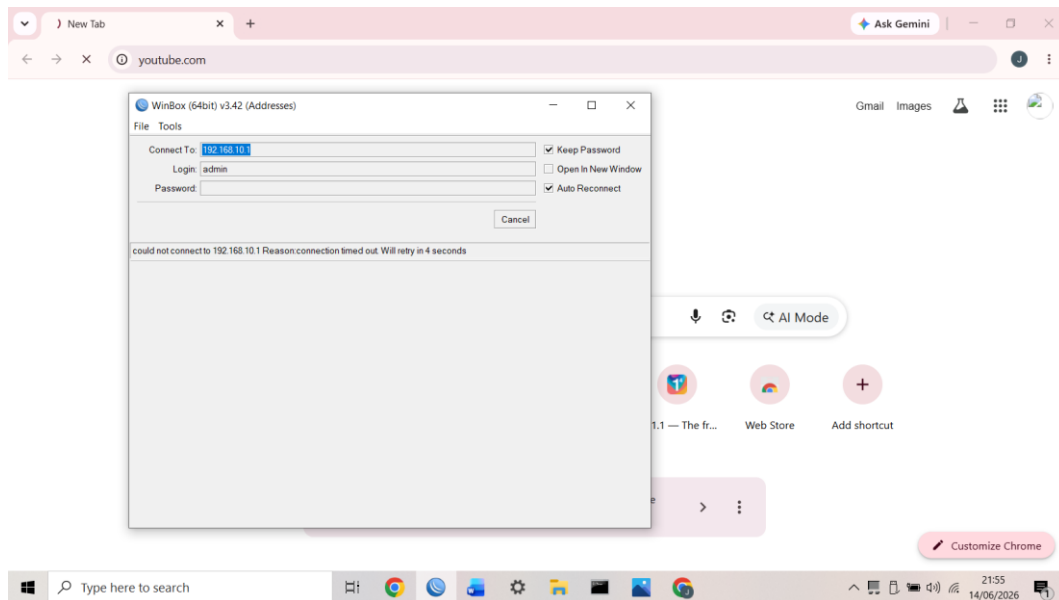
Fase eksekusi serangan pada perangkat lunak P2Pover v4.25 dimulai dengan melakukan pemetaan aturan (*rule binding*) pada menu utama. Berdasarkan gambar tersebut, aturan kustom bernama *wifi putus* yang di dalamnya telah mengonstruksikan batasan *bandwidth* terendah sebesar 10 KB/S beserta pemblokiran total pada protokol *WWW*, *P2P*, dan *instant messaging* diimplementasikan secara langsung pada *host* target dengan alamat IP 192.168.10.30. Proses pengikatan ini menandai bahwa parameter manipulasi jaringan telah siap dilepaskan menuju *MAC address* target melalui *interface* nirkabel yang digunakan oleh penyerang.



Sumber: Penulis, 2026

Gambar 5.112 Start Putus TSM Sesuai Rules

Setelah kebijakan pembatasan berhasil diikatkan pada host sasaran, penguji mengaktifkan tombol eksekusi utama (*start*) untuk memulai proses manipulasi tabel ARP di jaringan lokal. Jendela *local network view* menunjukkan status sistem telah beralih menjadi aktif (*running*), di mana aturan '*wifi putus*' secara resmi berjalan pada host 192.168.10.30. Pada fase ini, komputer penyerang mulai menyebarkan paket penipuan (*ARP reply spoofing*) secara konstan yang bertujuan untuk mengarahkan seluruh lalu lintas gerbang data internet milik target agar melewati *interface* penyerang terlebih dahulu sebelum diteruskan ke *gateway* utama.

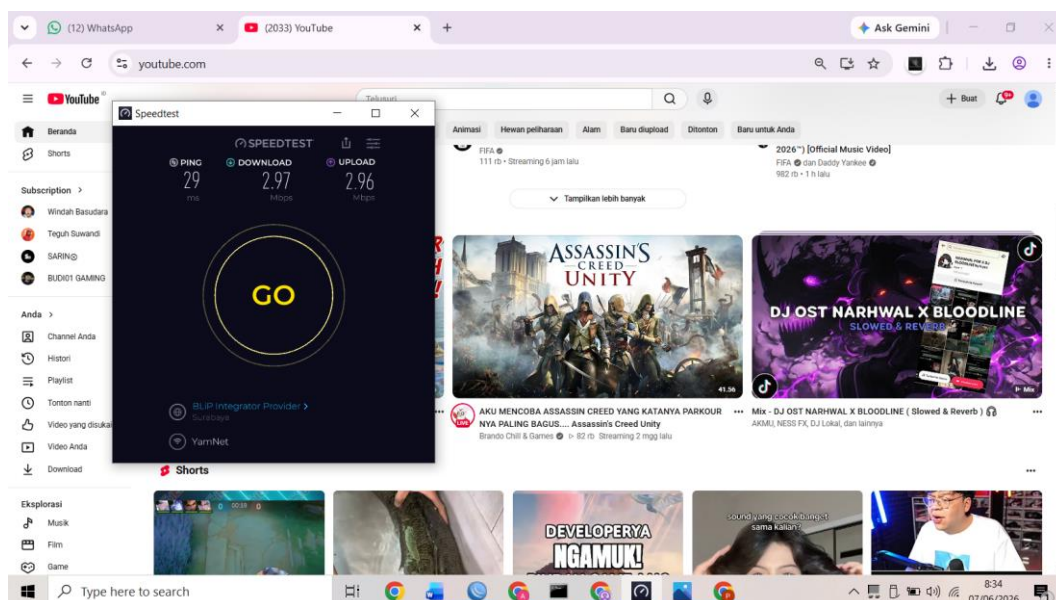


Sumber: Penulis, 2026

Gambar 5.113 Hasil P2Pover Sebelum Diterapkan *Client Isolation* TSM

Gambar diatas menunjukkan hasil pengujian menggunakan aplikasi P2Pover pada jaringan TSM sebelum fitur *client isolation* diterapkan pada *access point*. Pengujian dilakukan untuk mengetahui apakah perangkat penyerang masih dapat melakukan serangan ARP *spoofing* terhadap perangkat korban yang berada dalam jaringan yang sama.

Berdasarkan hasil pengujian, serangan ARP *spoofing* berhasil dilakukan sehingga koneksi perangkat korban ke *router* mikrotik melalui aplikasi winbox terputus dan menampilkan pesan *connection timed out*. Kondisi ini menunjukkan bahwa komunikasi antar klien masih terbuka dan dapat dimanfaatkan oleh penyerang untuk mengganggu konektivitas perangkat lain. Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, jaringan TSM masih rentan terhadap serangan ARP *spoofing* yang dapat menyebabkan terganggunya ketersediaan layanan jaringan bagi pengguna.



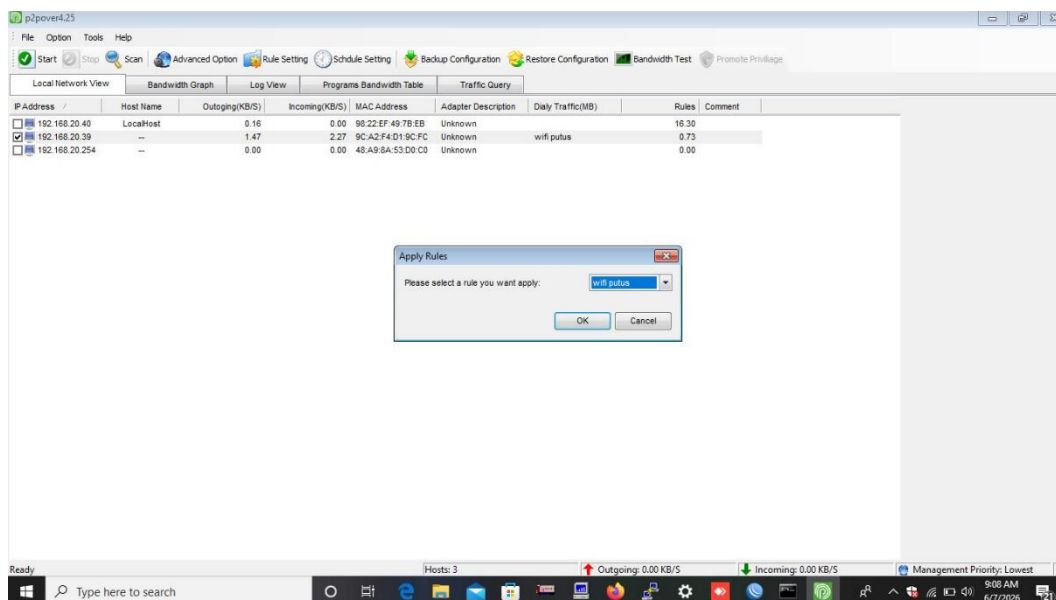
Sumber: Penulis, 2026

Gambar 5.114 Hasil P2Pover Sudah Diterapkan *Client Isolation* TSM

Tahap krusial dari eksperimen ini ditunjukkan melalui verifikasi empiris pada sisi perangkat korban (192.168.10.30) saat serangan sedang berlangsung aktif. Berdasarkan hasil pengukuran parameter performa jaringan menggunakan instrumen *speedtest*, didapatkan fakta bahwa laptop korban sama sekali tidak mengalami pemutusan koneksi ataupun degradasi performa."

Perangkat target mampu mempertahankan latensi rendah sebesar 29 ms dengan *throughput* unduh mencapai 2.97 Mbps dan unggah sebesar 2.96 Mbps, serta tetap dapat melakukan aktivitas streaming pada platform youtube secara lancar. Fenomena kegagalan serangan P2Pover ini menjadi bukti konkret bahwa arsitektur keamanan *client isolation* yang diaktifkan bertindak secara efektif sebagai perisai layer data *link*. Karena setiap paket data antar klien nirkabel disekat dan diisolasi secara ketat, paket manipulasi ARP dari laptop penyerang diredam total di udara dan tidak pernah sampai meracuni tabel ARP pada korban.

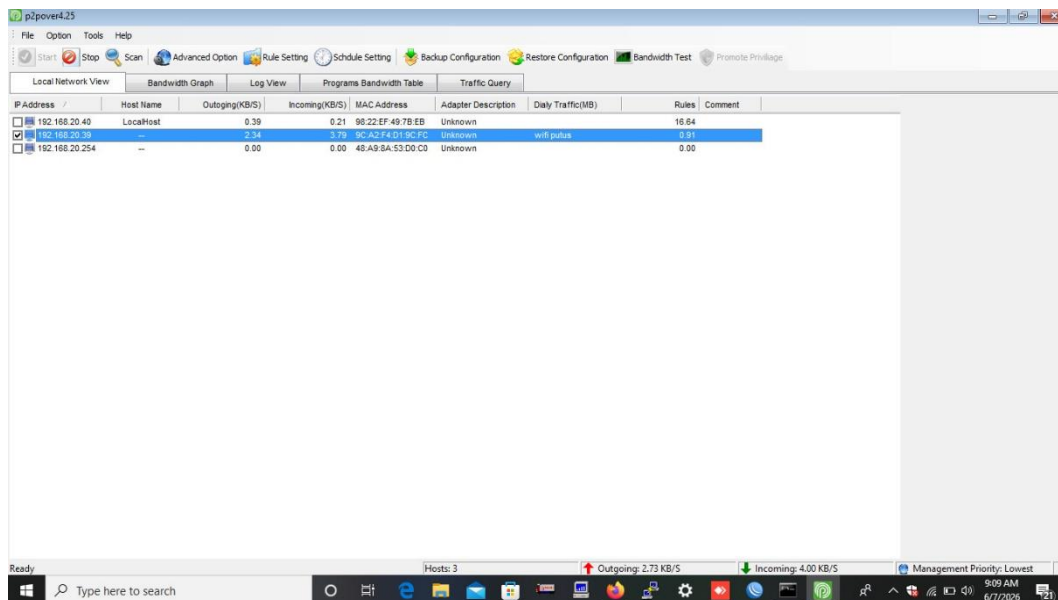
b. TKR



Sumber: Penulis, 2026

Gambar 5.115 Rules Wi-Fi Putus TKR

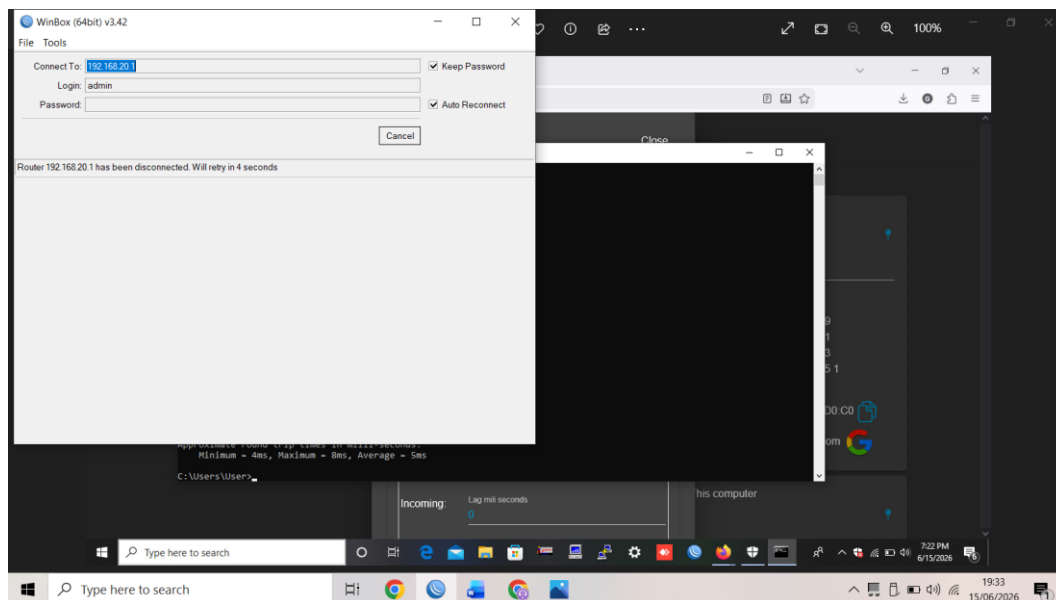
Fase eksekusi serangan pada perangkat lunak P2Pover v4.25 dimulai dengan melakukan pemetaan aturan (*rule binding*) pada menu utama. Berdasarkan gambar tersebut, aturan kustom bernama *wifi putus* yang di dalamnya telah mengonstruksikan batasan *bandwidth* terendah sebesar 10 KB/S beserta pemblokiran total pada protokol WWW, P2P, dan *instant messaging* diimplementasikan secara langsung pada *host* target dengan alamat IP 192.168.20.39. Proses pengikatan ini menandai bahwa parameter manipulasi jaringan telah siap dilepaskan menuju *MAC address* target melalui *interface* nirkabel yang digunakan oleh penyerang.



Sumber: Penulis, 2026

Gambar 5.116 Start Putus TKR Sesuai Rules

Setelah kebijakan pembatasan berhasil diikatkan pada host sasaran, penguji mengaktifkan tombol eksekusi utama (*start*) untuk memulai proses manipulasi tabel ARP di jaringan lokal. Jendela *local network view* menunjukkan status sistem telah beralih menjadi aktif (*running*), di mana aturan '*wifi putus*' secara resmi berjalan pada host 192.168.20.39. Pada fase ini, komputer penyerang mulai menyebarkan paket penipuan (*ARP reply spoofing*) secara konstan yang bertujuan untuk mengarahkan seluruh lalu lintas gerbang data internet milik target agar melewati *interface* penyerang terlebih dahulu sebelum diteruskan ke *gateway* utama.

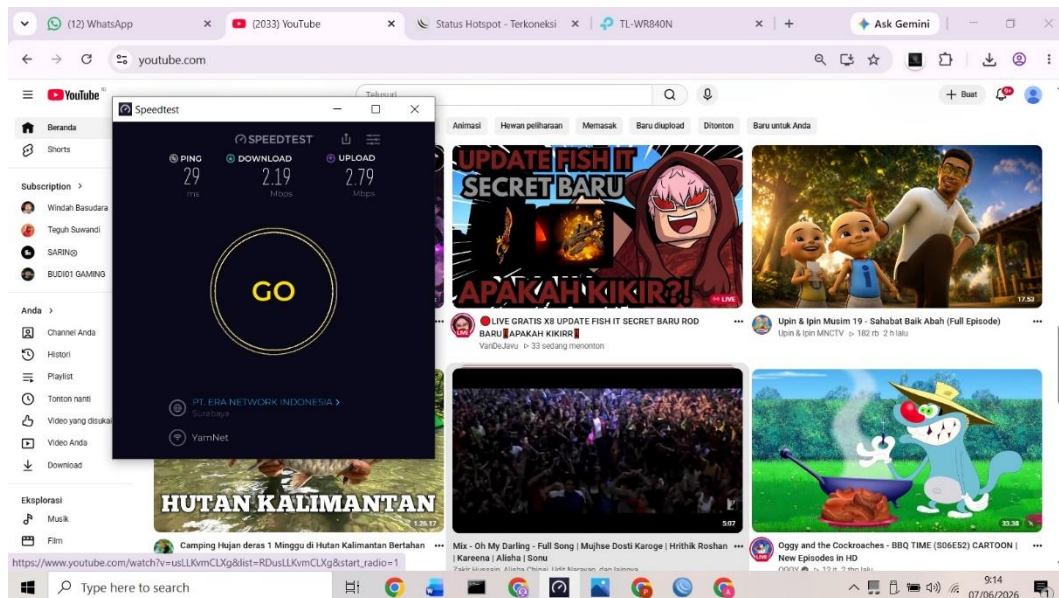


Sumber: Penulis, 2026

Gambar 5. 117 Hasil P2Pover Sebelum Diterapkan *Client Isolation* TKR

Gambar diatas menunjukkan hasil pengujian menggunakan aplikasi P2Pover pada jaringan TKR sebelum fitur *client isolation* diterapkan pada *access point*. Pengujian dilakukan untuk mengetahui apakah perangkat penyerang masih dapat melakukan serangan ARP *spoofing* terhadap perangkat korban yang berada dalam jaringan yang sama.

Berdasarkan hasil pengujian, serangan ARP *spoofing* berhasil dilakukan sehingga koneksi perangkat korban ke *router* mikrotik melalui aplikasi winbox terputus dan menampilkan pesan *connection timed out*. Kondisi ini menunjukkan bahwa komunikasi antar klien masih terbuka dan dapat dimanfaatkan oleh penyerang untuk mengganggu konektivitas perangkat lain. Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, jaringan TKR masih rentan terhadap serangan ARP *spoofing* yang dapat menyebabkan terganggunya ketersediaan layanan jaringan bagi pengguna.



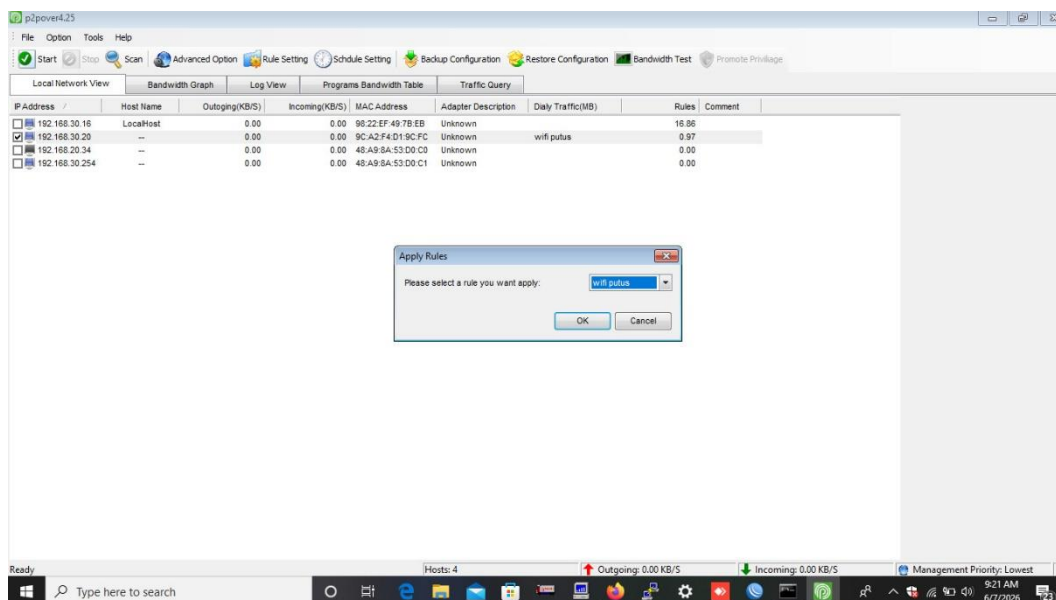
Sumber: Penulis, 2026

Gambar 5.118 Hasil P2Pover Sudah Diterapkan *Client Isolation* TKR

Tahap krusial dari eksperimen ini ditunjukkan melalui verifikasi empiris pada sisi perangkat korban (192.168.20.39) saat serangan sedang berlangsung aktif. Berdasarkan hasil pengukuran parameter performa jaringan menggunakan instrumen *speedtest*, didapatkan fakta bahwa laptop korban sama sekali tidak mengalami pemutusan koneksi ataupun degradasi performa."

Perangkat target mampu mempertahankan latensi rendah sebesar 29 ms dengan *throughput* unduh mencapai 2.19 Mbps dan unggah sebesar 2.79 Mbps, serta tetap dapat melakukan aktivitas streaming pada platform youtube secara lancar. Fenomena kegagalan serangan P2Pover ini menjadi bukti konkret bahwa arsitektur keamanan *client isolation* yang diaktifkan bertindak secara efektif sebagai perisai layer data *link*. Karena setiap paket data antar klien nirkabel disekat dan diisolasi secara ketat, paket manipulasi ARP dari laptop penyerang diredam total di udara dan tidak pernah sampai meracuni tabel ARP pada korban.

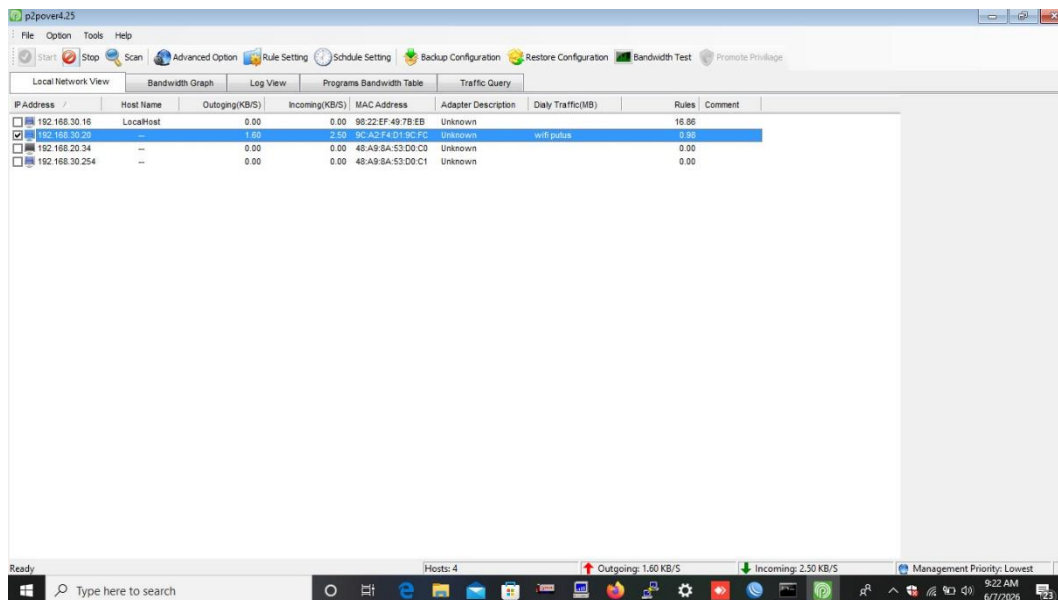
c. Kantor



Sumber: Penulis, 2026

Gambar 5.119 Rules Wi-Fi Putus Kantor

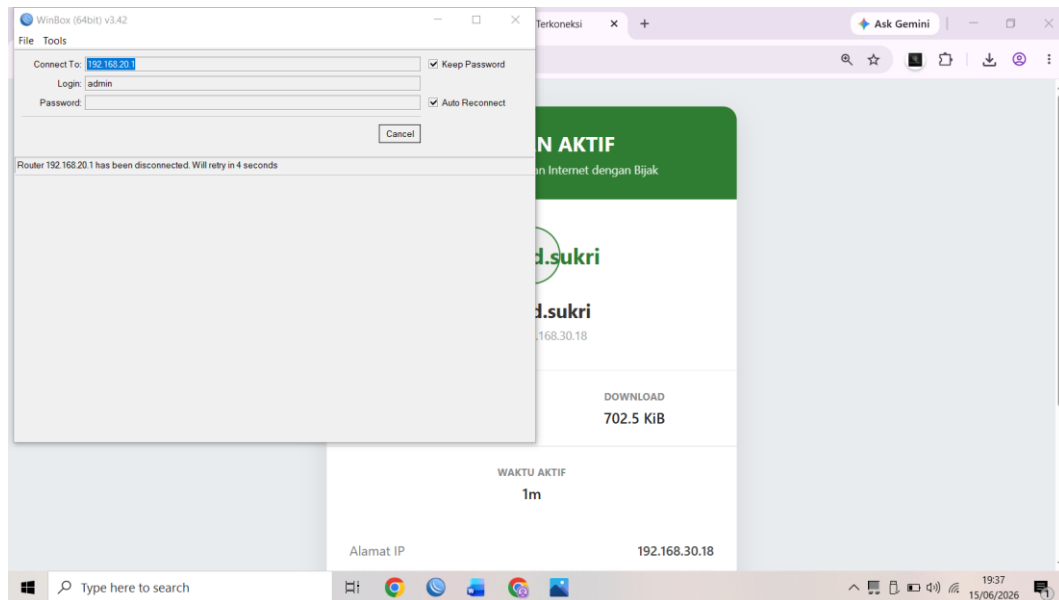
Fase eksekusi serangan pada perangkat lunak P2Pover v4.25 dimulai dengan melakukan pemetaan aturan (*rule binding*) pada menu utama. Berdasarkan gambar tersebut, aturan kustom bernama *wifi putus* yang di dalamnya telah mengonstruksikan batasan *bandwidth* terendah sebesar 10 KB/S beserta pemblokiran total pada protokol WWW, P2P, dan *instant messaging* diimplementasikan secara langsung pada *host* target dengan alamat IP 192.168.30.20. Proses pengikatan ini menandai bahwa parameter manipulasi jaringan telah siap dilepaskan menuju *MAC address* target melalui *interface* nirkabel yang digunakan oleh penyerang.



Sumber: Penulis, 2026

Gambar 5.120 Start Putus Kantor Sesuai Rules

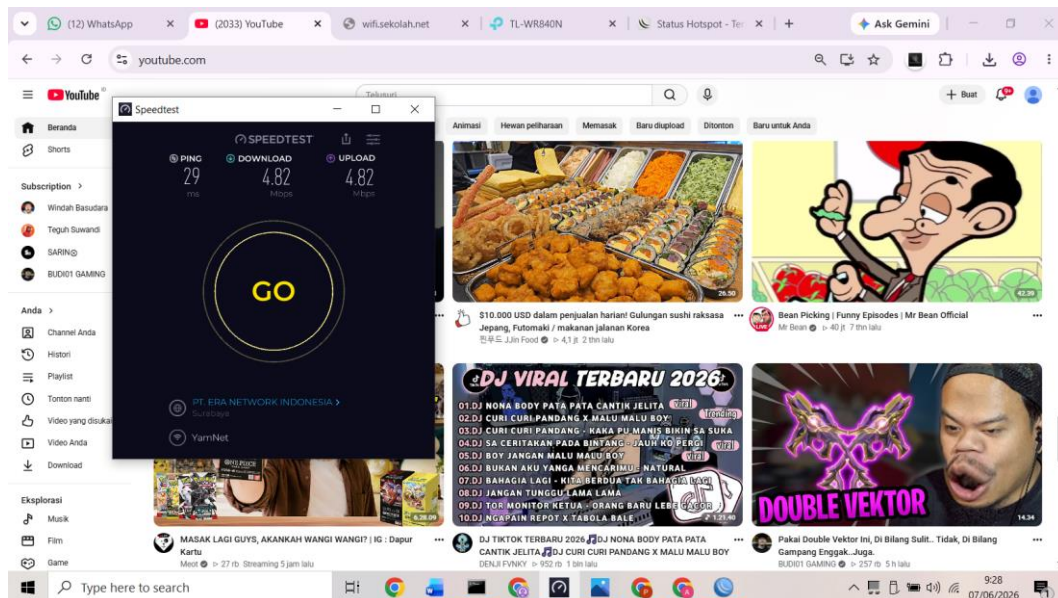
Setelah kebijakan pembatasan berhasil diikatkan pada host sasaran, penguji mengaktifkan tombol eksekusi utama (*start*) untuk memulai proses manipulasi tabel ARP di jaringan lokal. Jendela *local network view* menunjukkan status sistem telah beralih menjadi aktif (*running*), di mana aturan '*wifi putus*' secara resmi berjalan pada host 192.168.30.20. Pada fase ini, komputer penyerang mulai menyebarkan paket penipuan (ARP *reply spoofing*) secara konstan yang bertujuan untuk mengarahkan seluruh lalu lintas gerbang data internet milik target agar melewati *interface* penyerang terlebih dahulu sebelum diteruskan ke *gateway* utama.



Gambar 5.121 Hasil P2Pover Sebelum Diterapkan *Client Isolation* Kantor

Gambar diatas menunjukkan hasil pengujian menggunakan aplikasi P2Pover pada jaringan kantor sebelum fitur *client isolation* diterapkan pada *access point*. Pengujian dilakukan untuk mengetahui apakah perangkat penyerang masih dapat melakukan serangan *ARP spoofing* terhadap perangkat korban yang berada dalam jaringan yang sama.

Berdasarkan hasil pengujian, serangan *ARP spoofing* berhasil dilakukan sehingga koneksi perangkat korban ke *router* mikrotik melalui aplikasi winbox terputus dan menampilkan pesan *connection timed out*. Kondisi ini menunjukkan bahwa komunikasi antar klien masih terbuka dan dapat dimanfaatkan oleh penyerang untuk mengganggu konektivitas perangkat lain. Hasil tersebut membuktikan bahwa sebelum penerapan *client isolation*, jaringan kantor masih rentan terhadap serangan *ARP spoofing* yang dapat menyebabkan terganggunya ketersediaan layanan jaringan bagi pengguna.



Sumber: Penulis, 2026

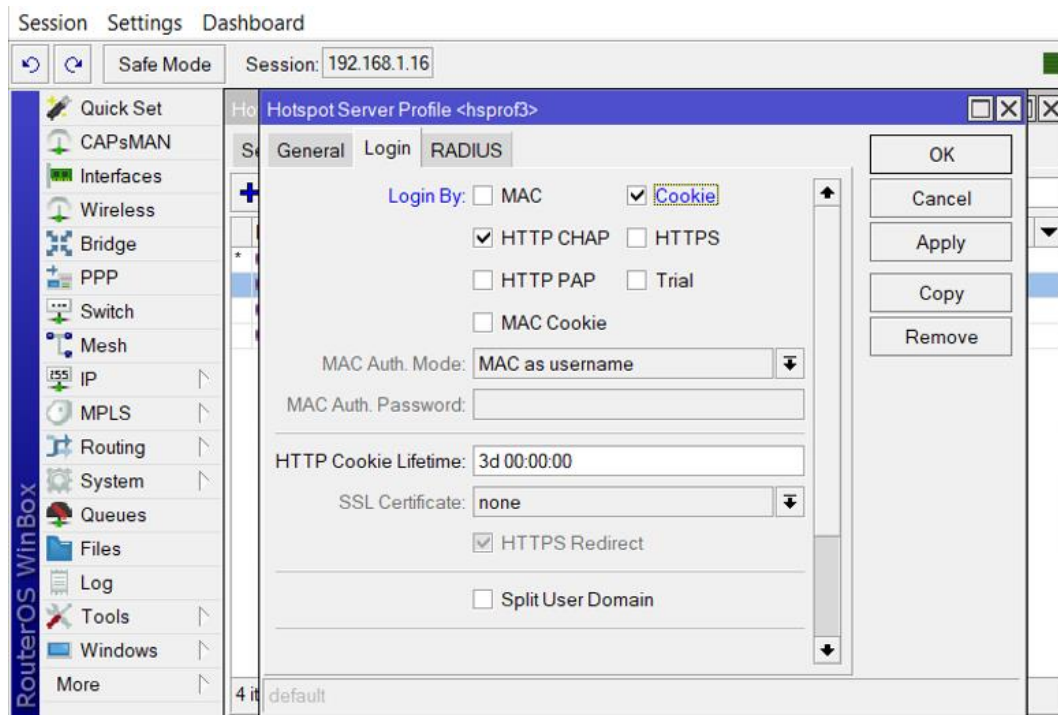
Gambar 5.122 Hasil P2Pover Sudah Diterapkan *Client Isolation* Kantor

Tahap krusial dari eksperimen ini ditunjukkan melalui verifikasi empiris pada sisi perangkat korban (192.168.30.20) saat serangan sedang berlangsung aktif. Berdasarkan hasil pengukuran parameter performa jaringan menggunakan instrumen *speedtest*, didapatkan fakta bahwa laptop korban sama sekali tidak mengalami pemutusan koneksi ataupun degradasi performa."

Perangkat target mampu mempertahankan latensi rendah sebesar 29 ms dengan *throughput* unduh mencapai 4.82 Mbps dan unggah sebesar 4.82 Mbps, serta tetap dapat melakukan aktivitas streaming pada platform youtube secara lancar. Fenomena kegagalan serangan P2Pover ini menjadi bukti konkret bahwa arsitektur keamanan *client isolation* yang diaktifkan bertindak secara efektif sebagai perisai layer data *link*. Karena setiap paket data antar klien nirkabel disekat dan diisolasi secara ketat, paket manipulasi ARP dari laptop penyerang diredam total di udara dan tidak pernah sampai meracuni tabel ARP pada korban.

5. TMAC

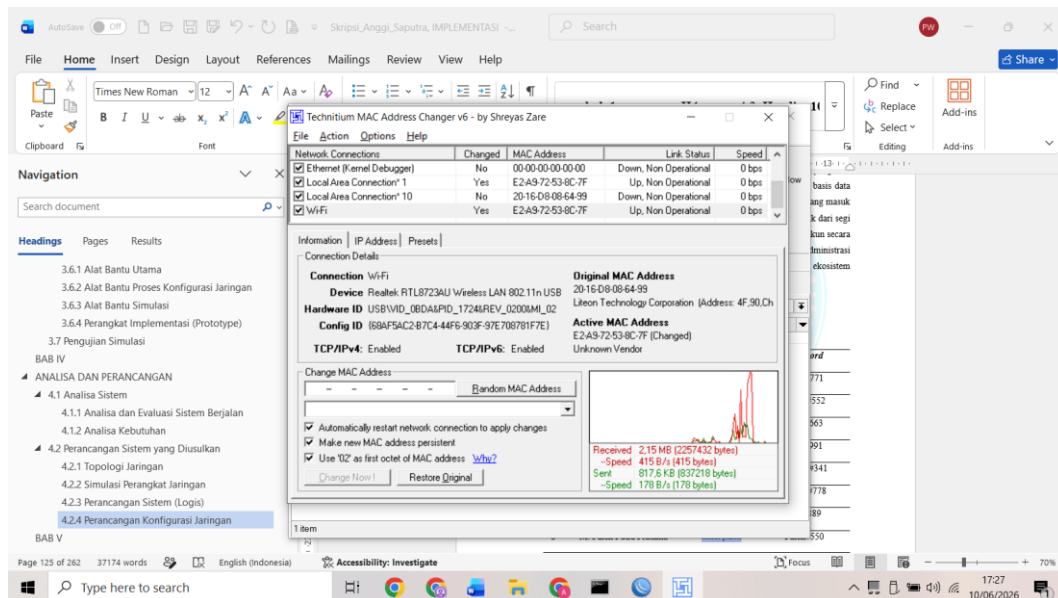
a. Sebelum *Cookie* Dimatikan



Sumber: Penulis, 2026

Gambar 5.123 *Cookie* Dalam Keadaan *Default* / Tercentang

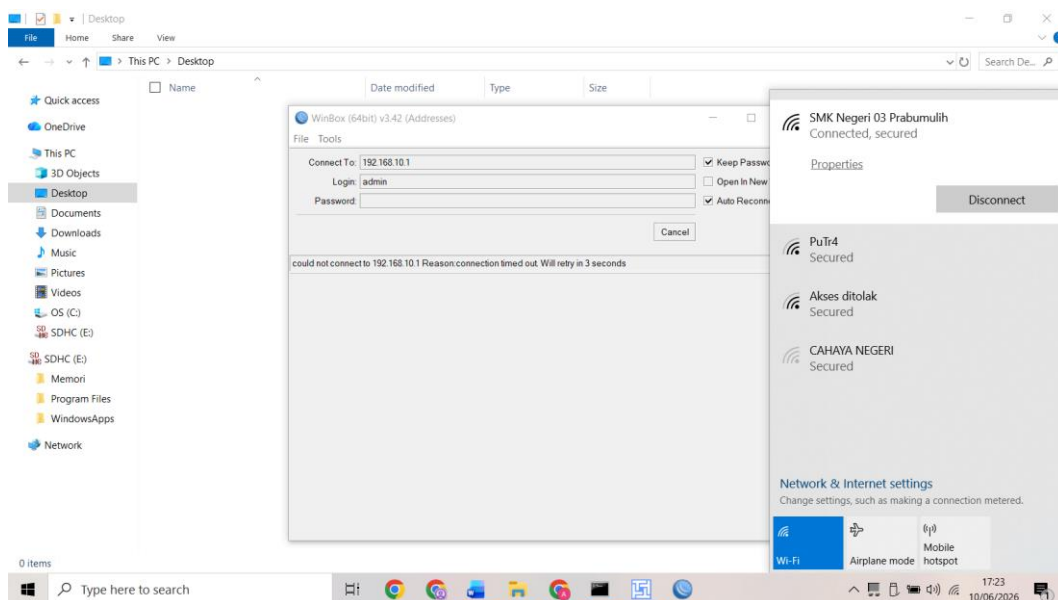
Pada gambar di atas ditunjukkan konfigurasi *login hotspot* mikrotik yang masih menggunakan fitur *cookie*. Pada konfigurasi tersebut metode *login* yang digunakan adalah HTTP CHAP dan *cookie*, sedangkan fitur MAC *login* dan MAC *cookie* tidak diaktifkan. Kondisi ini menyebabkan sesi autentikasi tetap tersimpan pada sistem *hotspot* sehingga berpotensi dimanfaatkan oleh pihak yang tidak berwenang apabila berhasil memperoleh identitas perangkat yang sedang aktif.



Sumber: Penulis, 2026

Gambar 5.124 Menyamar Menjadi MAC Korban

Gambar di atas menunjukkan proses perubahan alamat MAC address menggunakan aplikasi *technitium mac address changer* (TMAC). Pada tahap ini alamat MAC address perangkat korban yang telah berhasil login ke *hotspot* disalin dan diterapkan pada perangkat pengujian. Setelah perubahan dilakukan, perangkat pengujian memiliki identitas MAC address yang sama dengan perangkat korban. Pengujian ini bertujuan untuk mengetahui apakah sistem *hotspot* mampu membedakan perangkat asli dengan perangkat yang melakukan penyamaran identitas menggunakan teknik *MAC address spoofing*.

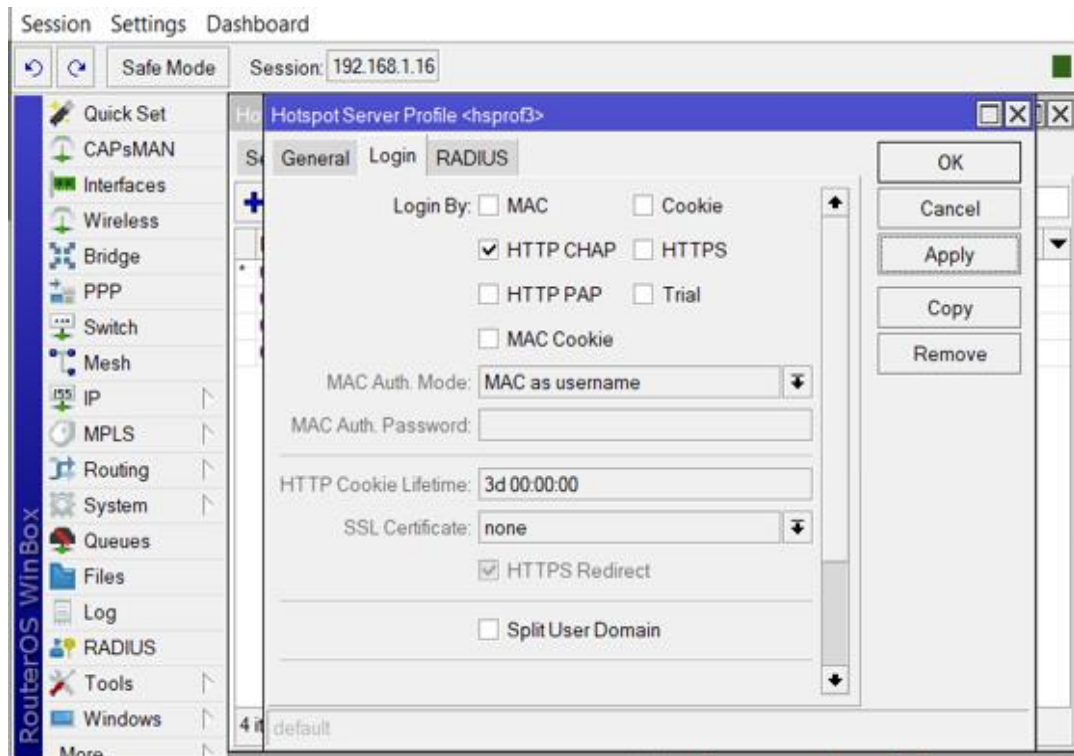


Sumber: Penulis, 2026

Gambar 5.125 Hasil Tidak Dihapus Ceklis *Cookie*

Setelah proses perubahan MAC *address* berhasil dilakukan, perangkat penguji terhubung kembali ke jaringan nirkabel sekolah. Pada tahap ini perangkat berhasil melakukan koneksi ke *access point* tanpa mengalami kendala. Meskipun menggunakan perangkat yang berbeda, jaringan mengenali perangkat penguji sebagai perangkat yang sama dengan korban karena menggunakan MAC *address* yang identik. Hal ini menunjukkan bahwa mekanisme autentikasi pada *hotspot* masih mengandalkan identitas perangkat yang telah tersimpan sebelumnya.

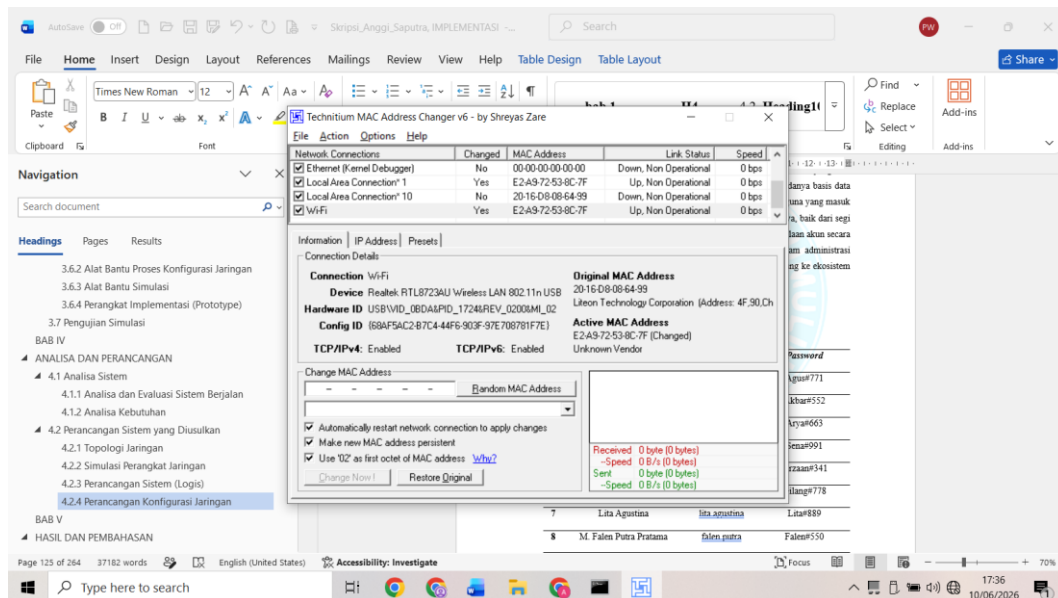
b. Setelah *Cookie* Dimatikan



Sumber: Penulis, 2026

Gambar 5.126 *Cookie* Dalam Keadaan Tidak Tercentang

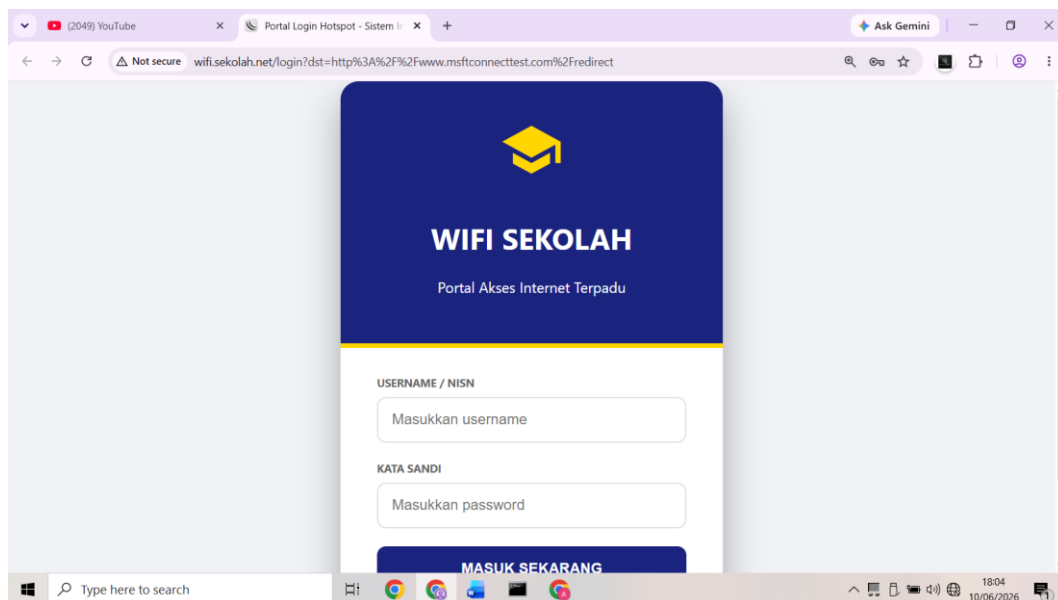
Pada gambar di atas ditunjukkan konfigurasi *login hotspot* mikrotik setelah fitur *cookie* dinonaktifkan. Pada konfigurasi ini hanya metode autentikasi HTTP CHAP yang digunakan, sedangkan fitur *cookie*, MAC *login*, dan MAC *cookie* tidak diaktifkan. Dengan dinonaktifkannya fitur *cookie*, sistem tidak lagi menyimpan sesi autentikasi pengguna pada perangkat *client*. Akibatnya setiap perangkat yang ingin mengakses internet harus melakukan proses *login* menggunakan *username* dan *password* yang valid. Konfigurasi ini diterapkan untuk mengurangi risiko penyalahgunaan sesi *login* yang sebelumnya masih tersimpan pada perangkat pengguna.



Sumber: Penulis, 2026

Gambar 5.127 Menyamar Menjadi MAC Korban

Gambar di atas menunjukkan proses pengujian menggunakan aplikasi *technitium MAC address changer* (TMAC). Pada tahap ini alamat *MAC address* perangkat korban yang telah terhubung ke jaringan *hotspot* disalin dan diterapkan pada perangkat penguji. Tujuan pengujian ini adalah untuk mengetahui apakah perangkat yang melakukan penyamaran identitas *MAC address* masih dapat memperoleh akses internet setelah fitur *cookie* dinonaktifkan pada *hotspot* mikrotik.



Sumber: Penulis, 2026

Gambar 5.128 Hasil Dihapus Ceklis *Cookie*

Berdasarkan hasil pengujian yang ditunjukkan pada gambar di atas, perangkat penguji yang telah melakukan penyamaran *MAC address* tidak langsung memperoleh akses internet. Saat perangkat mencoba mengakses internet, sistem *hotspot* secara otomatis mengarahkan pengguna ke halaman *portal login hotspot*. Hal ini menunjukkan bahwa sesi autentikasi pengguna tidak lagi tersimpan pada perangkat sebagaimana saat fitur *cookie* masih aktif. Dengan demikian, meskipun penyerang berhasil menyalin *MAC address* perangkat korban, akses internet tidak dapat diperoleh secara langsung tanpa melakukan proses autentikasi ulang menggunakan *username* dan *password* yang valid.

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil penelitian, perancangan, simulasi, implementasi terbatas, serta pengujian jaringan yang telah dilakukan pada penelitian “Implementasi Metode Autentikasi *User manager* untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet”, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Implementasi autentikasi *user manager* berbasis *hotspot* pada *router* mikrotik berhasil diterapkan untuk meningkatkan keamanan jaringan internet di lingkungan sekolah. Sistem autentikasi melalui halaman *login* mampu membedakan akses pengguna guru dan siswa sehingga penggunaan jaringan menjadi lebih terkontrol.
2. Penerapan manajemen *bandwidth* menggunakan fitur *simple queue* pada mikrotik berhasil membagi kapasitas jaringan internet antara ruang kantor, ruang praktik TSM, dan ruang praktik TKR sesuai kebutuhan masing-masing pengguna. Hasil pengujian menunjukkan pembagian *bandwidth* berjalan sesuai konfigurasi yang telah ditentukan.
3. Penambahan *access point* dan perancangan topologi jaringan berhasil memperluas jangkauan jaringan internet dari ruang kantor menuju ruang praktik TSM dan TKR.
4. Konfigurasi keamanan jaringan seperti penerapan pembatasan akses *router* hanya untuk administrator, pemblokiran akses terhadap alamat situs yang tidak sesuai dengan lingkungan pendidikan, serta mekanisme pengamanan untuk melindungi perangkat dari gangguan antar pengguna dalam jaringan berhasil diterapkan sehingga dapat meningkatkan keamanan jaringan sekolah.
5. Pengujian jaringan menggunakan *ping*, *packet data unit* (PDU), *angry IP scanner*, Nmap, dan *iperf3*, *netcut*, *command prompt*, *wireless network watcher*, *p2pover*, TMAC menunjukkan bahwa seluruh perangkat dapat

saling terhubung dengan baik, layanan *hotspot* berjalan sesuai rancangan, serta konektivitas jaringan berhasil divalidasi baik melalui simulasi maupun implementasi terbatas menggunakan perangkat nyata.

6.2 Saran

Meskipun implementasi autentikasi *user manager*, manajemen *bandwidth*, serta keamanan jaringan pada mikrotik telah berhasil dirancang dan diterapkan sesuai dengan kebutuhan penelitian, masih terdapat beberapa hal yang dapat dikembangkan untuk meningkatkan kualitas jaringan dan performa sistem di masa mendatang. Oleh karena itu, beberapa saran yang dapat diberikan untuk pengembangan selanjutnya adalah sebagai berikut:

1. Penelitian selanjutnya disarankan untuk melakukan implementasi jaringan secara langsung di lingkungan sekolah secara menyeluruh, sehingga hasil konfigurasi, autentikasi *user manager*, manajemen *bandwidth*, serta keamanan jaringan dapat diterapkan dan diuji pada kondisi jaringan yang sebenarnya.
2. Pengembangan jaringan dapat dilakukan dengan menambahkan sistem keamanan yang lebih lanjut seperti enkripsi data, serta sistem deteksi serangan jaringan agar keamanan jaringan menjadi lebih optimal.
3. Implementasi jaringan dapat diperluas tidak hanya pada ruang kantor, ruang praktik TSM, dan ruang praktik TKR, tetapi juga pada seluruh area sekolah agar pemerataan akses internet menjadi lebih maksimal.
4. Pihak sekolah disarankan untuk melakukan pemeliharaan jaringan secara berkala, seperti pengecekan perangkat mikrotik, *access point*, kabel jaringan, dan konfigurasi *hotspot* agar kualitas jaringan tetap terjaga.
5. Sistem keamanan jaringan dapat dikembangkan lebih lanjut dengan menambahkan lebih banyak pemblokiran terhadap situs-situs yang tidak pantas diakses oleh guru maupun siswa, seperti situs perjudian, pornografi, media ilegal, dan konten negatif lainnya sehingga penggunaan internet di lingkungan sekolah menjadi lebih aman, terkontrol, dan sesuai dengan lingkungan pendidikan.

DAFTAR PUSTAKA

- Abdillah Hasibuan, F., & Subhiyanto. (2021). Jaringan Komputer Berbasis Radius Server untuk Meningkatkan Pemanfaatan Internet di Madrasah Aliyah Al-Azhaar Ummu Suwanah. *Jurnal Teknik Informatika Stmik Antar Bangsa*, 7, 30–39. <https://doi.org/10.51998/jti.v7i1.349>
- Aditama Purba, J., & Nurhayati, A. (2024). Implementasi Mikrotik Untuk Sistem *Billing Voucher Hotspot*. *Infotek: Jurnal Informatika Dan Teknologi*, 4(2), 312–322. <https://doi.org/10.29408/jit.v4i2.3734>
- Al Khoiri, A., & Kuswandi. (2024). Implementasi Manajemen Jaringan *Bandwidth* Mikrotik Dengan *Simple Queue* Pada Balai Pelatihan Teknik Perkeretaanpian Sofyan Hadi Bekasi. *Jakarta Gedung Sentra Kramat Jalan Kramat Raya*, 9.
- Allo, A. K., & Widiyari, I. R. (2024). Analisis Keamanan *Website* SIASAT Menggunakan Teknik Footprinting dan Vulnerability Scanning. *Jurnal Teknologi Informasi Dan Komunikasi*, 8(2), 2024. <https://doi.org/10.35870/jti>
- Anamatalu, D., Hariadi, F., & Malo, R. M. I. (2023). Manajemen *User* Dan *Bandwidth* Pada Jaringan *Hotspot* Menggunakan Mikrotik Di Sekolah Menengah Kejuruan Negeri 5 Waingapu. *Jurnal Teknik Informatika, Sains Dan Ilmu Komunikasi*, 2(1), 01–08. <https://doi.org/10.59841/saber.v2i1.603>
- Ananda Khairunnisa, P., Anissa, N., Yukandri, & Parhusip, J. (2024). Perancangan Sistem Keamanan Jaringan Berbasis *Cybersecurity* untuk Mitigasi Ancaman *Siber* pada Infrastruktur TI: Studi Kasus di Indonesia. *Jurnal Ilmu Teknik Dan Informatika*, 4, 9–16. <https://doi.org/10.51903/teknik>
- Aprilian, Y., & Afriansyah, D. (2024). Rancang Bangun Aplikasi *Learning Management System* Berbasis *Moodle* Untuk Mendukung Pembelajaran *Blended Learning* Menggunakan Platform Cloud VPS Linux Ubuntu. *Jurnal Teknologi Dan Informatika (JEDA)*, 5(2), 2745–8911.
- Arbi Murad, F., Kurniawan, A., Yusuf Bagus, M., & Rasyiidin. (2025). *Port Knocking* Pada Mikrotik Untuk Meningkatkan Keamanan *Wifi* Di Era Industri 4.0. *Review Pendidikan Dan Pengajaran*, 8.
- Ariyadi, T., Dali Purwanto, T., & Fajar, M. M. (2023). Implementasi *Desain* Jaringan *Hotspot* Berbasis Mikrotik Dengan Metode NDLC (*Network*

- Development Life Cycle*) Pada PT Kirana Permata. *Jurnal Ilmiah Informatika*, 11, 189–195. <https://doi.org/10.33884/jif.v11i02.8032>
- Ariyadi, T., & Jordi, R. (2024). Perancangan Jaringan Lan Di Sekolah Menggunakan *Cisco Packet Tracer* Dan *Protocol Routing Ospf*. *Jurnal Ilmiah Teknik Dan Ilmu Komputer*, 3.
- Asrin, F., Ismarmiaty, Putra, S. A. S., Setyoningrum, N. G., Yuliana, A., Juwari, Ernawati, T., Harsapranata, A. I., Nofarita, E., Ekawati, N., Alia, P. A., Fitri, N. A., & Saleh, A. (2024). *Keamanan Sistem Informasi*.
- Ayman, R., Suparlan, & Wahyudi, J. (2024). *Design of Video Transmission with Wi-Fi on Runway Inspection using Jetson Nano and Data Synchronization*. *Indonesian Journal of Education & Mathematical Science*, 5(1), 1–11. <https://doi.org/10.30596/ijems.v5i1.16154>
- Cahya, B., Rizki Adi Sutiyo, F., El Saputra, Y., & Elfarizi, M. (2023). Implementasi *Firewall* Pada Mikrotik Untuk Keamanan Jaringan. *Jurnal JOCOTIS-Journal Science Informatica and Robotics E*, 1(2), 63–80. <https://jurnal.ittc.web.id/index.php/jct/>
- Carlos, Y., Rino, & Edy. (2024). Implementasi Sistem Monitoring Jaringan Berbasis Web Menggunakan Mikrotik. *Jurnal Algor*, 5. <https://jurnal.buddhidharma.ac.id/index.php/algor/index>
- Colanus Rally Drajana, I., & Bode, A. (2021). Simulasi Jaringan Menggunakan Cisco Packet Tracer. *Jurnal Sistem Informasi Dan Teknik Komputer*, 6.
- Dian Candra Wirlaksana, R., Sumaedi, A., Huda, N., Fitri, & Ucup. (2024). Implementasi Sistem *Hotspot* Mikrotik Sebagai Upaya Pemerataan Jaringan Internet Di Pedesaan. *Pengabdian Kepada Masyarakat*, 2(5).
- Fadila, F., Safriani, Eliana, & Khaddafi, M. (2025). *Pengumpulan Data Dalam Penelitian Kualitatif: Wawancara Data Collection In Qualitative Research: Interviews*. <https://jicnusanantara.com/index.php/jiic>
- Fattah Nasution, A. (2023). *Metode Penelitian Kualitatif* (M. Albina, Zulfa, & Nita, Eds.).
- Fauzan Fitriani, J., & Sujadi, H. (2023). *Implementasi Hotspot Dengan Pengelolaan User manager Dan Bandwidth Menggunakan Mikrotik RB941-2nd (Studi Kasus Smk Kesehatan Bhakti Kencana Jatiwangi)*. 1(1).

- Fauzi, A., Ficky Duskarnaen, M., & Ajie, H. (n.d.). *Desain Dan Implementasi Management Bandwidth Pada Hotspot Mikrotik Di Smk Mutiara 17 Agustus Bekasi*.
- Fitrian, J. F., & Sujadi, H. (2023). *Mikrotik RB941-2nd (Studi Kasus Smk Kesehatan Bhakti Kencana Jatiwangi)*. 1(1).
- Frederic P. Sitanggang, Y., Meilano, R., & Hadi Saputra, M. (2025). *Optimalisasi Manajemen Bandwidth Pada Jaringan Internet Menggunakan Metode Ppdioo Di Politeknik Jambi*. 7(1), 43. <https://ojs.politeknikjambi.ac.id/elti>
- Hariani. (2021). Eksplorasi Web Browser Dalam Pencarian Bukti Digital Menggunakan Sqlite. *Jurnal Informatika Sain Dan Teknologi*, 6(1), 66–74. <https://doi.org/https://doi.org/10.24252/instek.v6i1.18638>
- Hasanah, H., Haya Salsabila, K., Enggal Gemintang, R., Hafizh Fadillah, M., Hatta Ramadhan, M., Juhdahu, B., & Hidayat, R. (2025). *Manajemen Bandwidth Dan Kontrol Akses Jaringan Menggunakan Mikrotik Pada Lembaga Paud*. 5(1). <https://doi.org/10.46880/tamika.Vol5No1.pp67-75>
- Hasibuan, A. (2025). *Buku Ajar Teknologi Jaringan Nirkabel*.
- Henrayanto Denny Yulizar, V., & Haris, A. (2025). Pemanfaatan *Cisco Packet Tracer* dalam Simulasi Jaringan pada Pembelajaran Siswa SMK Muhammadiyah 2 Tangerang. *Journal Of Management and Business*, 19–39.
- Ichsansyah, A., Syahroni, M., & Nasri. (2024). *Analisis Perbandingan Manajemen Bandwidth Menggunakan Router Mikrotik RB951Ui-2hnd Dengan Metode Queue Tree Dan Hierarchical Token Bucket* (Vol. 21, Number 2).
- Khair, H., M Saragih, J. D., & H Pardede, A. M. (2021). *Pengamanan Data Teks Menggunakan Algoritma Modular Multiplication Based Block Chiper*.
- Khairi Faldi, R., & Hadi, R. (2023). *Laporan Komunikasi Data Dan Jaringan Pengenalan Fitur Pada Cisco Packet Tracer*.
- Kriswantoro, M. C., & Ayatullah, A. H. (2023). *Manajemen Bandwidth Pada Jaringan Pemerintah Kota Surabaya Menggunakan Metode Queue Tree*. *AICOMS 2023*, 2(2), 1–8. <https://jurnal.politap.ac.id/index.php/aicoms>
- Kurniasari, E., Reyhandera, R. N., Oktaviani, & Kembaren, S. B. (2025). *Penerapan Metode Design Thinking Dalam Perancangan UI/UX Aplikasi*

- Tafsir Mimpi Menggunakan Figma. *Jurnal Minfo Polgan*, 13(2), 2212–2221.
<https://doi.org/10.33395/jmp.v13i2.14415>
- Made Adi Surya Permana, I., Gede Putu Krisna Juliharta, I., & Gede Juliana Eka Putra, I. (2025). Analisis Keamanan Sistem Informasi Menggunakan Metode *Vulnerability Assesment* pada Aplikasi Web Karangasem.go.id. *Remik: Riset Dan E-Jurnal Manajemen Informatika Komputer*, 9(2).
<https://doi.org/10.33395/remik.v9i2.14561>
- Mafakhiri, J. (2021). *Analisis Kinerja Internet Hotspot dengan Menerapkan Bandwidth Management Menggunakan Mikrotik User manager di Kedai KARMILA*. 6(4), 2622–4615. <https://doi.org/10.32493/informatika.v6i4.12566>
- Mardatillah, N. A., & Murhayati, S. (2025). *Data dan Fakta Penelitian Kualitatif*.
- Martani, A., Sukirman, & Junaedy. (2024). *Jaringan Komputer – dengan Mikrotik*.
- Muhajir, F., & Utami, E. (2026). Analisis Performa *WireGuard* dan *OpenVPN* pada VPN Perbankan Berbasis MikroTik menggunakan ICMP, iPerf3, dan *Mann-Whitney*. *Jurnal Riset Komputer*, 13(1), 2407–389.
<https://doi.org/10.30865/jurikom.v13i1.9438>
- Ngatono, Dwiyatno, S., Dedi Jubaedi, A., Ferdiansyah, Y., Krinaningsih, E., & Rahmat. (2024). *Implementasi User manager Mikrotik Dalam Authentication Login Pada Hotspot*.
- Ningsih, S., Satra, R., & Widya Mufila Gaffar, A. (2025). Analisis Penempatan *Access point* Pada Jaringan *Wireless LAN* Fakultas Agama UMI. *Jurnal Minfo Polgan*, 13(2), 2463–2472. <https://doi.org/10.33395/jmp.v13i2.14510>
- Ningsy Guncya, R. (2024). Rancang Bangun Sistem Autentikasi *Hotspot* Berbasis Radius Server Menggunakan Mikrotik Pada Sekolah Menengah Kejuruan Negeri 5 Luwu. *Mars: Jurnal Teknik Mesin, Industri, Elektro Dan Ilmu Komputer*, 2(3), 138–152. <https://doi.org/10.61132/mars.v2i3.150>
- Novi Syahputri, C., Anggraini, C., Fawi Anugerah, H., Zufria, I., & Iqbal Nahwi, M. (2023). *Penerapan Kinerja Filter Rule dengan Metode Raw dan Layer 7 Protocol di Router Mikrotik*. 05(2).
- Nur Iman, A., & Sholeh, M. (2024). *Analisis Keamanan Jaringan Wifi di MI Inwanul Huda*.

- Nurfanis, Zaenudin, & Masjun Efendi, M. (2024). *Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Di Smk Bangun Negeri Hu'u*.
- Nurhayati, Sedubun, S., Rumapea, E. L. B., & Ahmad. (2024). *Inovasi Pendidikan di Era Digital: Tantangan dan Solusi*. <https://mediapenerbitindonesia.com>
- Pratama, P. A. E., Andreyana, P. V., & Nurjana, P. R. (2024). Pengujian High Availability pada Asynchronous DNS Berbasis Restknot menggunakan Algoritma Round Robin. *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi*, 5(1), 1019–1032. <https://doi.org/10.35870/jimik.v5i1.582>
- Putri, H. J., & Murhayati, S. (2025). *Metode Pengumpulan Data Kualitatif*.
- Rahmadan, M., & Eri Gunawan, C. (2024). *Perancangan Data Flow Diagram Aplikasi Tabungan Sampah Pt Pusri Palembang*. 3(1), 1–9.
- Rahman, M., Budi Handwika, R., & Izzatus Zahro, A. (2023). Penerapan Model Network Development Life Cycle (NDLC) Pada Infrastruktur Jaringan Internet Kantor Desa Kemiri. *Jurnal Publikasi Teknik Informatika*, 2(3), 37–47. <https://doi.org/10.55606/jupti.v2i3.1790>
- Rahmat, D., Afwa, N. N., & Febrianti, M. (2024). Infrastruktur Jaringan Komputer Berbasis Cisco Packet Tracer Di Labkom E-18 Universitas Muhammadiyah Sukabumi. *Infotech Journal*, 10(2), 252–256. <https://doi.org/10.31949/infotech.v10i2.10920>
- Rahmayanty, D., Raja Guk Guk, R., Dwi Indah Cahya, B., & Regilsa Muhammad. (2023). *Peran Orang Tua Dalam Mengaplikasikan Internet Sebagai Media Pendidikan Bagi Anak*. 5.
- Ramadanti, M., Hidayat, A., & Mustika. (2025). *Implementasi Sistem Autentikasi Dan Pengamanan Jaringan Wireless Berbasis Captive Portal Di Pkbm Alsuroya Metro*. 6(1), 55–66.
- Ramadhani, S., & Hidayati, R. (2025). Analisis Kepuasan Mahasiswa terhadap Penggunaan Aplikasi Figma dalam Desain UI/UX dengan Pendekatan *End-User Computing Satisfaction* (EUCS). *Digital Transformation Technology*, 4(2), 1132–1139. <https://doi.org/10.47709/digitech.v4i2.5292>

- Ramadona Wijaya, F., Alya Rahmi Lubis, F., Najib Sihab Siregar, M., & Ayu Fauziah Batubara, A. (2025). Sumber Data, Subjek Penelitian, dan Isu Terkait. *Jurnal Edukatif*, 271–276.
- Ramayanti, D., & Saputra, V. (2025). Optimasi Infrastruktur *Wi-Fi* dan Manajemen *Bandwidth* di Sekolah Menengah Menggunakan Teknologi Mikrotik. *Arcitech: Journal of Computer Science and Artificial Intelligence*, 5(1), 1–17. <https://doi.org/10.29240/arcitech.v5i1.12408>
- Rifka Khairyansyah, S., Saskia Amalia, D., Aditya, S., Sah, A., & Aribowo, D. (2024). Teknologi *WI-FI* Menggunakan Topologi Star. *Mars: Jurnal Teknik Mesin, Industri, Elektro Dan Ilmu Komputer*, 2(2), 27–33. <https://doi.org/10.61132/mars.v2i2.89>
- Risa, M. (2021). *Metode Penelitian* (A. Pratomo, Ed.). Poliban Press.
- Rizky, M. A. H., Solehudin, A., & Nurkifli, E. H. (2024). Optimalisasi *Bandwidth* Pada Jaringan Internet Menggunakan Metode *Simple Queue* Dan *Peer Connection Queue* (Studi Kasus: Pt. Paragon Pratama Teknologi). *Jurnal Mahasiswa Teknik Informatika*, 8(4).
- Rizqillah, M. R., Eka Suryana, M., & Irzal, M. (2023). Improvisasi Crawling pada Peta Web Menggunakan Algoritma Terdistribusi dengan Model Koordinasi Berbasis *Socket Programming*. *J-KOMA*, 49–62.
- Romdona, S., Senja Junista, S., & Gunawan, A. (2025). Teknik Pengumpulan Data: Observasi, Wawancara Dan Kuesioner. *Jisosepol: Jurnal Ilmu Sosial Ekonomi Dan Politik*, 3(1), 39–47. <https://samudrapublisher.com/index.php/JISOSEPOL>
- Rosnelly, R., & Wira Yudha, S. (2023). Jurnal Ilmu Sosial Ekonomi Dan Politik Perancangan Aplikasi Otomatisasi Deteksi Xss Berbasis Cli Dengan Bahasa Pemrograman Go. *Journal of Information System*, 8(2), 11–20. <https://fe.ekasakti.org/index.php/UJIS/article/view/37>
- Safila Dewi, S., & Syaripudin, A. (2024). Rancangan Dan Implementasi Jaringan *Hotspot* Dengan Menggunakan Metode *Queue Tree* Pada Mikrotik Sebagai Penunjang Pembelajaran Online Di Desa Pasilian. *OKTAL: Jurnal Ilmu Komputer Dan Science*, 3(4), 998–1009. <https://journal.mediapublikasi.id/index.php/oktal/article/view/2642>

- Sar'an, Andrayani, D., Nurainum, & Aslmiah Nasution, S. (2025). Pembelajaran Kuis Sebagai Strategi Meningkatkan Motivasi Belajar Siswa. *Alkarim : Jurnal Pendidikan, Psikologi Dan Studi Islam*, 10(1), 29–35.
<https://jurnal.staiyaptip.ac.id/index.php/alkarim/article/view/498>
- Sianhar, Y., & Marhalim. (2025). Penerapan *Firewall* Berbasis Mikrotik Dalam Optimalisasi. *Jurnal Informatika Teknologi Dan Sains*, 7(2), 868–877.
<https://doi.org/https://doi.org/10.51401/jinteks.v7i2.5774>
- Siswanto, E. (2023). Perancangan Dan Implementasi Jaringan Lokal Dan *Hotspot* Smk Muhammadiyah Kedungtuban Dengan Mikrotik Dan Konfigurasi Winbox. *Jurnal Ilmiah Sains Dan Teknologi*, 2.
<https://jurnal.usahidsolo.ac.id/index.php/jimstek/article/view/1525>
- Siswanto, E., Dianta, I. A., & Danang. (2021). Captive Portal Dan Implementasi *Bandwidth* Management Di Stikes St. Elisabeth Semarang. *Jurnal Ilmiah Manajemen Dan Kewirausahaan*, 1(1), 1–16.
<https://doi.org/https://doi.org/10.51903/imk.v1i1.55>
- Sulung, U., & Muspawi, M. (2024). Memahami Sumber Data Penelitian Primer, Sekunder, Dan Tersier. *Jurnal Edu Research Indonesian Institute For Corporate Learning And Studies*, 5(3), 110–116.
<https://iicls.org/index.php/jer/article/download/238/195/>
- Sundara, K. A., Aspriyono, H., & Supardi, R. (2022). Perancangan Manajemen *Bandwidth* Menggunakan Mikrotik *Router Wireless* Pada Sekolah Menengah Kejuruan Negeri 4 Kota Bengkulu. *Jurnal Media Infotama*, 18(2), 279–290.
<https://doi.org/https://doi.org/10.37676/jmi.v18i2.2747>
- Syahindra, W. (2022). Perancangan dan Implementasi *Router* Mikrotik Pada Infrastruktur Jaringan Komputer Internet dengan Media *Transmisi Wired* dan Nirkabel (Studi Kasus: IAIN Curup). *Arcitech: Journal of Computer Science and Artificial Intelligence*, 2(1), 63–76.
<https://doi.org/https://doi.org/10.29240/arcitech.v2i1.7974>
- Tsalil Amri, I., & Selamat, R. (2025). *Implementasi Manajemen Bandwidth Router Mikrotik Menggunakan Metode Hierarchical Token Bucket (Htb) Di Smk Dharma Bhakti 4 Jambi*. 8(1), 13–18.

- Wahyuni, S., & Tamrin, H. (2024). *Code-Switching in the Daily Conversations of Female Students at Pondok Pesantren Nuruttauhid Bulukumba, South Sulawesi: A Sociolinguistic Study*. <https://doi.org/10.15408/ltr.v3i2>
- Wijoyo, A., Rosadi, A., Is Hakim, F., Hanafi, M., & Sidik, R. (2023). *Keamanan Jaringan Melindungi Sistem dari Serangan Luar*. <https://journal.mediapublikasi.id/index.php/jriin>
- Wisnu Prio Pamungkas, R., Ashkiyyah, K., Rayhan, M., & Sunaryo, H. (2024). Membangun Tampilan Sistem Transaksi Online (Nana&Co) Menggunakan Figma. *Nusantara Journal of Multidisciplinary Science*, 1(11). <https://jurnal.intekom.id/index.php/njms>
- Yunita, Maulana, I., Gilang Hermawan, A., Veranda Deanda, G., Yusuf Habibi, M., & Aribowo, D. (2024). Simulasi Komunikasi Data Dengan Menggunakan Model Referensi OSI Pada *Cisco Packet Tracer*. *Venus: Jurnal Publikasi Rumpun Ilmu Teknik*, 2(2), 179–187. <https://doi.org/10.61132/venus.v2i2.271>
- Zulkarnaen. (2021). Implementasi *User manager* Sebagai *Radius Server* Pada *Router Board Mikrotik Rb750gr3*. *Teknimedia*, 2, 56–63.

LAMPIRAN

Lampiran 1 Surat Permohonan Penelitian


FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH

Prabumulih, 03 November 2025

Nomor : 025 /FASILKOM/UNPRA/Inf-S1/XI/2025
Lampiran : -
Perihal : Permohonan Penelitian dan Pengambilan Data

Kepada Yth,
Kepala Sekolah SMK Negeri 3 Prabumulih
Di
Tempat

Dalam rangka pelaksanaan skripsi mahasiswa Program Studi Informatika Fakultas Ilmu Komputer Universitas Prabumulih, maka kami harapkan bantuan dari Bpk/Ibu kiranya mengizinkan mahasiswa:

1. Nama : Anggi Saputra
Nim : 2022230007
Program Studi : Informatika

Untuk melaksanakan penelitian dan pengambilan data ditempat Bpk/Ibu Pimpin guna menyelesaikan skripsi. Atas bantuan dan kerjasamanya kami ucapkan terima kasih.


Ketua Program Studi,
Informatika,
Lyda Setiawan, S.Kom., M.Kom.
NIDN.0209129101

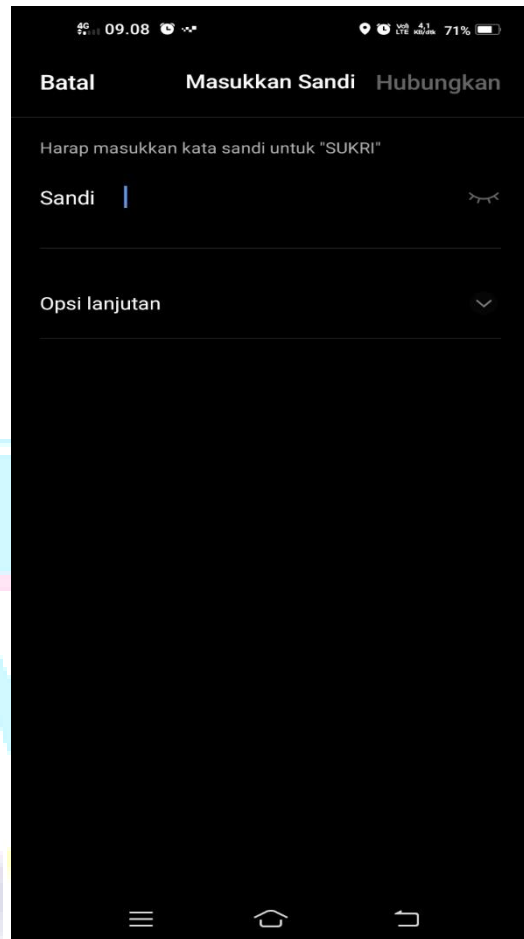
Jalan Patra No.50 RT.01 RW.03 Kelurahan Sukaraja Kecamatan Prabumulih Selatan
Kota Prabumulih Sumatera Selatan Indonesia Telpn 0713-3224417 Fax 0713-322418
e-mail : mail@unpra.ac.id

Lampiran 2 Surat Balasan Permohonan Penelitian

	PEMERINTAH PROVINSI SUMATERA SELATAN DINAS PENDIDIKAN SMK NEGERI 3 PRABUMULIH TERAKREDITASI "A" Jalan Sungai Medang Kelurahan Sungai Medang Kecamatan Cambai Kota Prabumulih Provinsi Sumatera Selatan ,Kode Pos 31145 Email : officialsmknegeri3pbm@gmail.com	
SURAT KETERANGAN		
Nomor	: 421.5 / 925 / SMKN 3. PBM / Dikif. SS / XII / 2025	
Perihal	: Balasan Permohonan Izin Penelitian	
 Kepada Yth. Ketua Program Studi Informatika, Fakultas Ilmu Komputer Universitas Prabumulih Di Tempat		
 Dengan hormat, Menindak lanjuti Surat Permohonan Izin Penelitian dan Pengambilan Data nomor 025/FASILKOM/UNPRA/Inf-S1/XI/2025 perihal untuk penyusunan Tugas Akhir Kepala Sekolah SMK Negeri 3 Prabumulih, memberitahukan bahwa:		
Nama	: Anggi Saputra	
Nim	: 2022230007	
Program Studi	: Informatika	
 Diizinkan untuk mengadakan penelitian Tugas Akhir dengan judul "Implementasi Metode Autentikasi User Manager Untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet (Studi Kasus : SMK Negeri 3 Prabumulih)".		
Demikian surat izin penelitian ini agar dapat dipergunakan sebagaimana mestinya.		
 Prabumulih, 01 Desember 2025 Kepala SMK Negeri 3 Kota Prabumulih  Kehmad Sekh, S.Pd., M.Si NIP. 197005211994121002		

Lampiran 3 Dokumentasi Wawancara & Observasi







ABSEN PRAKTEK KELAS XI TKR

Mapel : Konsentrasi Keahlian Teknik Kendaraan Ringan

No	N A M A	Tgl	Tgl	Tgl	Tgl	Tgl	Tgl
		Materi	Materi	Materi	Materi	Materi	Materi
		06-8-25	07-8-25	13-8-25	14-8-25		
		Elektrikal	Elektrikal	Elektrikal	Elektrikal		
		Body	Body	Body	Body		
1	Adi Ariski	✓	✓	✓	✓		
2	Adil Pratama	✓	✓	✓	✓		
3	Al Juansyah	✓	✓	✓	✓		
4	Aldi Alfian	✓	✓	✓	✓		
5	Almutede Ansyah	✓	✓	✓	✓		
6	Alzar Daven Rizki	✓	✓	✓	✓		
7	Andes Ramadhan	✓	✓	✓	✓		
8	Angga Saputra	✓	✓	✓	✓		
9	April Ramza	✓	✓	✓	✓		
10	Arjuna Raga Pratama	✓	✓	✓	✓		
11	Awansyah	✓	✓	✓	✓		
12	Bayu Anggara	✓	✓	✓	✓		
13	Denis	✓	✓	✓	✓		
14	Dika Pernandes	✓	✓	✓	✓		
15	Diki Candra	✓	✓	✓	✓		
16	El Abib Anandi	✓	✓	✓	✓		
17	Hози	✓	✓	✓	✓		
18	Marsel Saputra	✓	✓	✓	✓		
19	Muhammad Iqbal Fahriansyah	✓	✓	✓	✓		
20	Muhammad Rafli	✓	✓	✓	✓		
21	Nando Perdana	✓	✓	✓	✓		
22	Nauval Irwansyah	✓	✓	✓	✓		
23	Paril Adiya	✓	✓	✓	✓		
24	Pedro Jeri Handaka	✓	✓	✓	✓		
25	Radev Priyanka	✓	✓	✓	✓		
26	Raya Andaka	✓	✓	✓	✓		
27	Restu Singgi	✓	✓	✓	✓		
28	Rudi Ansah	✓	✓	✓	✓		
29	Taufik Hidayat	✓	✓	✓	✓		
30	Yayan Sanjaya	✓	✓	✓	✓		
31	Yolan Saputra	✓	✓	✓	✓		
32	Zaki Tri Prasetyo	✓	✓	✓	✓		

Guru Mata Pelajaran


 Harry Sunarya, ST

Lampiran 4 Daftar Pertanyaan Wawancara

Draft Wawancara

Nama Narasumber : Harry Sunarya, S.T
Jabatan : Ketua Kompetensi TKRO
Tempat Wawancara : SMK Negeri 3 Prabumulih
Tanggal Wawancara : 1 Desember 2025
Pewawancara : Anggi Saputra

No	Pertanyaan	Jawaban
1	Boleh dijelaskan mengenai posisi dan tanggung jawab Bapak sebagai Ketua Kompetensi Teknik Kendaraan Ringan Otomotif dalam pelaksanaan pendidikan di sekolah?	Sebagai Ketua Kompetensi TKRO, saya bertanggung jawab mengoordinasikan proses pembelajaran praktik dan teori otomotif, memastikan kurikulum kejuruan berjalan sesuai standar, serta mengelola kesiapan sarana bengkel dan peralatan praktik. Tugas saya juga memastikan kegiatan pembelajaran mengikuti perkembangan teknologi, termasuk penggunaan sumber belajar berbasis digital dalam kegiatan praktik siswa.
2	Bagaimana kondisi akses internet di ruang praktik TKR, termasuk kekuatan sinyal, jangkauan, dan kendala koneksi yang sering menghambat kegiatan pembelajaran?	Kondisi internet di ruang praktik TKR masih lemah kadang jaringannya hanya mencapai satu batang saja dan sinyal sering terputus. Hal ini menyebabkan pembelajaran digital tidak berjalan maksimal, terutama ketika membuka materi online atau video.
3	Apakah keterbatasan jaringan tersebut berdampak pada pelaksanaan pembelajaran berbasis digital, seperti penggunaan aplikasi, konten multimedia, atau instruksi praktik yang membutuhkan akses online?	Ya, keterbatasan jaringan sangat berdampak. Ruang praktik TKR sering mengalami kesulitan dalam mengakses materi visual sistem kendaraan, aplikasi pembelajaran, diagram teknik online, maupun referensi digital lainnya. Pembelajaran yang seharusnya berlangsung lebih interaktif menjadi terhambat karena koneksi yang lambat dan tidak stabil, sehingga penggunaan sumber belajar berbasis internet di ruang praktik TKR tidak dapat dimaksimalkan.
4	Apakah Bapak bersedia menerima masukan terkait pengembangan jaringan dan perluasan akses internet agar ruang praktik TKR dapat lebih optimal dalam kegiatan pembelajaran?	Ya, tentu saya bersedia. Selama masukan tersebut dapat membantu memperbaiki kualitas jaringan dan mendukung proses pembelajaran praktik, saya sangat terbuka agar akses internet di ruang TKR bisa lebih baik.
5	Apa harapan Bapak terhadap peningkatan sistem jaringan internet di sekolah ke depannya, khususnya dalam mendukung kompetensi keahlian TKR?	Saya berharap sekolah dapat memperluas jangkauan jaringan hingga ruang praktik TKR, dan menyediakan sinyal yang stabil. Dengan peningkatan tersebut, pembelajaran berbasis digital di kompetensi TKRO akan jauh lebih efektif dan sesuai kebutuhan perkembangan teknologi otomotif.

Narasumber



Harry Sunarya, S.T

NIPPPK. 19711128202321002

Prabumulih, 1 Desember 2025

Pewawancara



Anggi Saputra

Draft Wawancara

Nama Narasumber : Rahmi WidiaPratiwi, S.T
 Jabatan : Ketua Kompetensi TBSM
 Tempat Wawancara : SMK Negeri 3 Prabumulih
 Tanggal Wawancara : 1 Desember 2025
 Pewawancara : Anggi Saputra

No	Pertanyaan	Jawaban
1	Dapatkah Ibu menjelaskan secara singkat mengenai SMK Negeri 3 Prabumulih?	SMK Negeri 3 Prabumulih adalah sekolah kejuruan yang fokus menyiapkan siswa agar siap kerja melalui praktik langsung dan pembelajaran berbasis industri. Sekolah ini memiliki beberapa kompetensi keahlian dan terus berupaya meningkatkan kualitas fasilitas serta proses belajar.
2	Boleh dijelaskan mengenai posisi dan tanggung jawab Ibu sebagai Ketua Kompetensi Teknik dan Bisnis Sepeda Motor dalam pelaksanaan pendidikan di sekolah?	Sebagai Ketua Kompetensi TBSM, saya bertanggung jawab dalam mengatur pelaksanaan pembelajaran produktif, memastikan kesiapan fasilitas praktik, koordinasi dengan guru bidang kejuruan, serta memastikan kompetensi yang diajarkan sesuai standar industri otomotif. Saya juga memastikan proses pembelajaran dapat mengikuti perkembangan teknologi, termasuk penggunaan media digital dalam kegiatan praktik.
3	Apa visi dan misi SMK Negeri 3 Prabumulih menurut dokumen resmi sekolah?	Visi sekolah adalah menciptakan lulusan yang kompeten, berkarakter, dan mampu bersaing di dunia kerja. Misinya mencakup peningkatan kualitas pembelajaran, penerapan teknologi informasi dalam pendidikan, serta penguatan kompetensi peserta didik melalui praktik kejuruan dan kemitraan dengan dunia industri. Saya menyarankan untuk melihat langsung melalui dokumen resmi dari pihak sekolah terkait visi dan misi nya.
4	Bagaimana struktur umum organisasi di SMK Negeri 3 Prabumulih berdasarkan pembagian bidang dan kompetensi keahlian?	Struktur organisasi sekolah terdiri dari Kepala Sekolah yang dibantu Wakil Kepala Sekolah dalam bidang kurikulum, kesiswaan, sarana prasarana, dan hubungan industri. Di bawahnya terdapat ketua program keahlian, ketua kompetensi keahlian seperti TBSM dan TKRO, guru produktif, serta unit pendukung seperti Tata Usaha dan Bimbingan Konseling. Untuk mengetahui lebih lanjut struktur organisasi nya bisa lihat saja dokumen struktur organisasi nya.
5	Bagaimana kondisi akses internet di ruang praktik TSM, termasuk kekuatan sinyal, jangkauan, serta kendala koneksi yang mempengaruhi kegiatan praktik siswa?	Kondisi internet di ruang praktik TSM masih lemah kadang jaringannya hanya mencapai satu batang saja dan sinyal sering terputus. Hal ini menyebabkan pembelajaran digital tidak berjalan maksimal, terutama ketika membuka materi online atau video teknik perbaikan sepeda motor.

6	Apakah di sekolah ini ada akses internet utama, Bu? Kalau ada, menggunakan layanan apa?	Ya, ada. Akses internet utama di sekolah menggunakan layanan Iconnet.
7	Apakah Ibu bisa memberitahu saya di mana letak akses internet utama sekolah saat ini ditempatkan?	Akses internet utama berada di ruang kantor pusat administrasi. Dari sana jaringan menyebar, tetapi belum ada distribusi khusus yang diarahkan ke ruang praktik TSM sehingga jangkauannya masih sangat terbatas.
8	Apakah benar sistem keamanan jaringan dari penyedia layanan internet (ISP) di sekolah masih menggunakan password Wi-Fi biasa dan belum menggunakan autentikasi pengguna seperti username dan password per pengguna?	Ya, benar. Saat ini akses internet masih menggunakan satu password Wi-Fi tanpa sistem autentikasi khusus. Jadi siapa saja yang mengetahui kata sandi bisa langsung terhubung, dan ini sering menyebabkan password bocor dan dipakai secara bebas.
9	Apakah keterbatasan jaringan tersebut berdampak pada pelaksanaan pembelajaran berbasis digital, seperti penggunaan aplikasi, simulasi servis, katalog online, atau bahan ajar multimedia?	Tentu berdampak. Kondisi keterbatasan jaringan di ruang TKR menyebabkan akses terhadap materi digital, katalog komponen, maupun video pembelajaran menjadi terhambat. Pemanfaatan media pembelajaran berbasis internet juga tidak dapat berjalan optimal karena koneksi yang lambat dan tidak stabil, sehingga aktivitas praktik dan penyampaian informasi teknis berbasis digital di ruang TKR sering terganggu.
10	Apakah Ibu bersedia menerima masukan terkait pengembangan jaringan dan perluasan akses internet agar ruang praktik TSM lebih optimal dalam mendukung pembelajaran?	Tentu saya bersedia. Jika ada solusi yang bisa membantu memperluas jaringan, meningkatkan keamanan, dan memastikan internet lebih menyebar, itu akan sangat bermanfaat bagi pembelajaran praktik TSM.
11	Apa harapan Ibu terhadap peningkatan sistem jaringan internet di sekolah ke depannya, khususnya dalam mendukung kompetensi keahlian TSM?	Saya berharap akses internet utama tidak hanya berada di ruang kantor saja, tetapi dapat disebar sampai ke ruang praktik agar kegiatan pembelajaran berbasis digital bisa berjalan lebih lancar dan maksimal.

Narasumber

Rahmi WidiaPratiwi, S.T

Prabumulih, 1 Desember 2025

Pewawancara

Anggi Saputra



**FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH**

**KESEDIAAN SEBAGAI PEMBIMBING SKRIPSI
PROGRAM STUDI INFORMATIKA**

Yang bertanda tangan di bawah ini:

Nama : Iwan Setiawan, S.Kom., M.Kom.
NUPTK : 1541769670130303
Program Studi : Informatika
Fakultas : Ilmu Komputer

Bersedia menjadi pembimbing I Skripsi, dan

Nama : Hermizahadiwidastra, S.Kom., M.Kom.
NUPTK : 2863762663130192
Program Studi : Informatika
Fakultas : Ilmu Komputer

Bersedia menjadi pembimbing II Skripsi

Dari mahasiswa Program Studi Informatika Fakultas Ilmu Komputer Universitas Prabumulih di bawah ini:

Nama : Anggi Saputra
NIM : 2022230007
Judul Skripsi : Implementasi Metode *Autentikasi User Manager* untuk Optimalisasi Keamanan Mikrotik dan Pemerataan Akses Internet

Demikian surat kesediaan membimbing ini kami buat, atas perhatiannya kami ucapkan terima kasih.

Prabumulih,

Juni 2026

Dosen Pembimbing I

(Iwan Setiawan, S.Kom., M.Kom.)
NUPTK. 1541769670130303

Dosen Pembimbing II

(Hermizahadiwidastra, S.Kom., M.Kom.)
NUPTK. 2863762663130192



FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH

KARTU BIMBINGAN SKRIPSI

NAMA : ANGGI SAPUTRA
NIM : 2022230007
PROGRAM STUDI : INFORMATIKA
NAMA PEMBIMBING I : IWAN SETIAWAN, S.Kom., M.Kom
JUDUL : IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER*
UNTUK OPTIMALISASI KEAMANAN MIKTOTIK DAN
PEMERATAAN AKSES INTERNET

NO	TGL KONSULTASI	TOPIK POKOK YANG DIBICARAKAN	TANDA TANGAN PEMB. I	TGL MENGHADAP KEMBALI
1	6-2-2026	BAB I ACC	<i>[Signature]</i>	
		BAB II ACC	<i>[Signature]</i>	
		BAB III ACC	<i>[Signature]</i>	
2	22-4-2026	BAB IV a. Evaluasi sistem jaringan, b. Bahasa asing c. Perancangan d. Struktur kurik e. Gambar f. Topologi Jaringan	<i>[Signature]</i>	

Mulai Bimbingan : 6-2-2026

Batas Akhir Bimbingan :

Mengetahui Kaprodi Informatika

PERHATIAN !
TIDAK BOLEH HILANG
SETIAP BIMBINGAN HARUS DIBAWA

[Signature]
IWAN SETIAWAN, S.Kom.M.Kom.



FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH

KARTU BIMBINGAN SKRIPSI

NAMA : ANGGI SAPUTRA
NIM : 2022230007
PROGRAM STUDI : INFORMATIKA
NAMA PEMBIMBING I : IWAN SETIAWAN, S.Kom., M.Kom
JUDUL : IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER*
UNTUK OPTIMALISASI KEAMANAN MIKTOTIK DAN
PEMERATAAN AKSES INTERNET

NO	TGL. KONSULTASI	TOPIK POKOK YANG DIBICARAKAN	TANDA TANGAN PEMB. I	TGL MENGHADAP KEMBALI
3.	6/5/2026	BAB IV a. gambar		
4.	15/5/2026	BAB IV ACC		
5.	25/5/2026	BAB V a. Hardware		
6.	29/5/2026	BAB V ACC		
7.	9/6/2026	BAB VI ACC		
8.	10/6/2026	keengkapan, ACC SAP JHE UJI		

Mulai Bimbingan :

Mengetahui Kaprodi Informatika

Batas Akhir Bimbingan :

PERHATIAN !
TIDAK BOLEH HILANG
SETIAP BIMBINGAN HARUS DIBAWA

IWAN SETIAWAN, S.Kom.M.Kom.



FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH

KARTU BIMBINGAN SKRIPSI

NAMA : ANGGI SAPUTRA
NIM : 2022230007
PROGRAM STUDI : INFORMATIKA
NAMA PEMBIMBING II : HERMIZAHADIWIDASTRA, S.Kom., M.Kom
JUDUL : IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER*
UNTUK OPTIMALISASI KEAMANAN MIKROTIK DAN
PEMERATAAN AKSES INTERNET

NO	TGL. KONSULTASI	TOPIK POKOK YANG DIBICARAKAN	TANDA TANGAN PEMB. II	TGL MENGHADAP KEMBALI
1	12/02 2026	BAB I. 1.5 tambahkan manfaat prolektis & TEORIS. ✓ BAB II 2.8. Di bawah tabelnya. ✓ 1. Silakan baca paragraf terakhir,		
2	12/02 2026	BAB I ACC BAB II ACC lanjut BAB III		
3	13/02 2026	BAB III. 3.1.4. berikan tabel ✓ Isi dengan asy. ✓ 3.7 tambahkan poin 2 penjelasan Tools yg digunakan format angka. ✓		
4	7/04 2026	Tool dalam Jarkom 7 + penjelasan & penyesuaian & kesimpulan		

Mulai Bimbingan : Mengetahui Kaprodi Informatika
Batas Akhir Bimbingan :

PERHATIAN !
TIDAK BOLEH HILANG
SETIAP BIMBINGAN HARUS DIBAWA

IWAN SETIAWAN, S.Kom.M.Kom.



FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH

KARTU BIMBINGAN SKRIPSI

NAMA : ANGGI SAPUTRA
NIM : 2022230007
PROGRAM STUDI : INFORMATIKA
NAMA PEMBIMBING II : HERMIZAHADIWIDASTRA, S.Kom., M.Kom
JUDUL : IMPLEMENTASI METODE AUTENTIKASI USER MANAGER
UNTUK OPTIMALISASI KEAMANAN MIKROTIK DAN
PEMERATAAN AKSES INTERNET

NO	TGL. KONSULTASI	TOPIK POKOK YANG DIBICARAKAN	TANDA TANGAN PEMB. II	TGL MENGHADAP KEMBALI
5	9/04 2026	ACC BAB IV lanjut BAB IV	[Signature]	
6	19/05 2026	4.2.2.1 perangkat keras. lebih detail lagi 4.2.1. Topologi jaringan yg. Detail rtr gbr tsb. l 4.3. tambahkan Network Diagram 4. form Logru. Desaint upk 5. " " Desaint upk Tabel 4.1, 4.2	[Signature]	
7	03/06 2026	ACC BAB IV lanjut BAB V	[Signature]	

Mulai Bimbingan :

Mengetahui Kaprodi Informatika

Batas Akhir Bimbingan :

PERHATIAN !
TIDAK BOLEH HILANG
SETIAP BIMBINGAN HARUS DIBAWA

IWAN SETIAWAN, S.Kom.M.Kom.



FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH

KARTU BIMBINGAN SKRIPSI

NAMA : ANGGI SAPUTRA
NIM : 2022230007
PROGRAM STUDI : INFORMATIKA
NAMA PEMBIMBING II : HERMIZAHADIWIDASTRA, S.Kom., M.Kom
JUDUL : IMPLEMENTASI METODE AUTENTIKASI *USER MANAGER*
UNTUK OPTIMALISASI KEAMANAN MIKROTIK DAN
PEMERATAAN AKSES INTERNET

NO	TGL. KONSULTASI	TOPIK POKOK YANG DIBICARAKAN	TANDA TANGAN PEMB. II	TGL MENGHADAP KEMBALI
8.	07/06 2026	Kasus V. - permasalahan bhs asing. - Tambahkan lg alat bantu tools untuk uji coba konfigurasi keamanan jaringan.		
9	10/06 2026	- Hasil pengujian sebelum & sesudah menggunakan aplikasi Tools pengujian • Hasil pengujian Raza telah web portal. web portal hasil dari alat tools yg digunakan.		
10	17/06 2026	ACC Kasus V #1 ACC Kasus VI #2 Siap Uji #3		

Mulai Bimbingan :
Batas Akhir Bimbingan :

Mengetahui Kaprodi Informatika

PERHATIAN !
TIDAK BOLEH HILANG
SETIAP BIMBINGAN HARUS DIBAWA

IWAN SETIAWAN, S.Kom.M.Kom.



**FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH**

PENILAIAN REVIEW SKRIPSI

Nama : Anggi Saputra
NIM : 2022230007
Judul Skripsi : Implementasi Metode *Autentikasi User Manager* untuk Optimalisasi
Keamanan Mikrotik dan Pemerataan Akses Internet
Hari/Tanggal : SENIN / 22-6-2026

Saran dan masukan :

IKUTI DRAFT PENGUJI DENGAN KONSULTASI
KE PEMBIMPIING DAHULU

ACC SIAP DILID

14/1/2026

Rekomendasi*:

- a. Dilanjutkan tanpa perbaikan
- ☒ b. Dilanjutkan dengan perbaikan
- c. Ditolak

Prabumulih, 22-6-2026
Ketua Sidang

(Iwan Setiawan, S.Kom., M.Kom)
NUPTK. 1541769670130303

*pilih salah satu



**FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH**

PENILAIAN REVIEW SKRIPSI

Nama : Anggi Saputra
NIM : 2022230007
Judul Skripsi : Implementasi Metode Autentikasi User Manager untuk Optimalisasi
Keamanan Mikrotik dan Pemerataan Akses Internet
Hari/Tanggal : Senin 22 Mei 2026
Saran dan masukan :

- Pastikan dahulu den: Dosen penguji
perhatikan setiap revisi catatan, catatan
lipatan kertas pd Modul yg diberikan
Kpd dosen - dosen Dosen penguji
lakukan segera perbaikan.

Prof. M. A. H. 14/ Mei 2026

Rekomendasi*:

- a. Dilanjutkan tanpa perbaikan
- ☒ b. Dilanjutkan dengan perbaikan
- c. Ditolak

Prabumulih, 22 Mei 2026
Penguji I

(Hermizahadiwidastra, S.Kom., M.Kom)
NUPTK. 2863762663130192

*pilih salah satu



**FAKULTAS ILMU KOMPUTER
UNIVERSITAS PRABUMULIH**

PENILAIAN REVIEW SKRIPSI

Nama : Anggi Saputra
NIM : 2022230007
Judul Skripsi : Implementasi Metode *Autentikasi User Manager* untuk Optimalisasi
Keamanan Mikrotik dan Pemerataan Akses Internet
Hari/Tanggal : Senin, 22 Juni 2026
Saran dan masukan :

- Sempurnakan metode queue
- perbaiki metode konfigurasi
- tambahkan informasi apakah jaringan sudah
dimana mana
- perbaiki layout tulisan
Fit Jula 06/7 2026

Rekomendasi*:

- Dilanjutkan tanpa perbaikan
- Dilanjutkan dengan perbaikan
- Ditolak

Prabumulih, Juli 2026
Penguji II

(Jepri Yandi, S.Kom., M.Kom)
NUPTK. 3948771672130302

*pilih salah satu