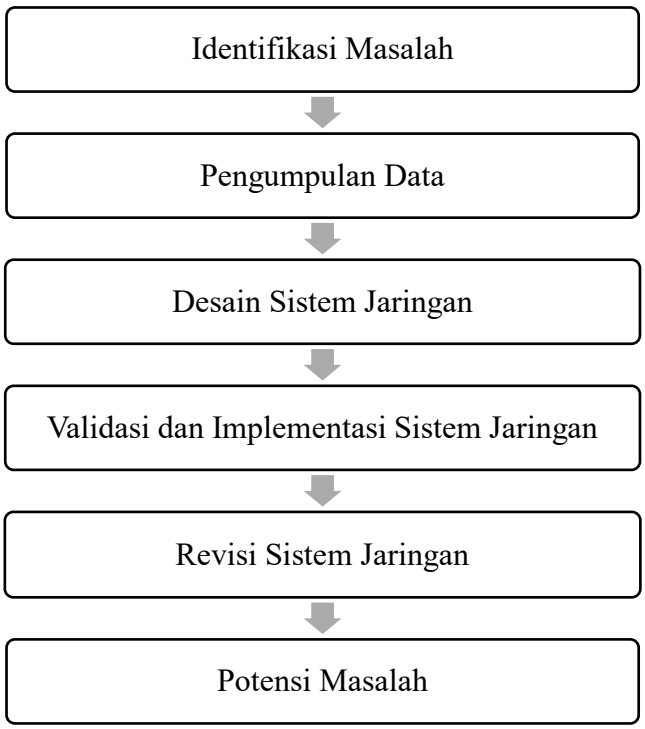
BAB III
METODE PENELITIAN

3.1 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode penelitian pengembangan *(Research and Development/R&D),* yang bertujuan untuk mengembangkan sistem keamanan jaringan berbasis Mikrotik melalui penerapan kombinasi teknik *Port Knocking* dan *Access Control List (ACL).* Penelitian ini dilaksanakan secara langsung pada lingkungan jaringan di Kantor Pengadilan Agama Rantauprapat Kelas I B, dengan fokus utama pada perancangan, implementasi, dan evaluasi sistem yang dibangun.

Model penelitian pengembangan yang digunakan dalam penelitian ini mengadaptasi model R&D dari *Borg and Gall*, yang disederhanakan menjadi enam tahapan inti agar lebih sesuai untuk ruang lingkup skripsi tingkat sarjana. Model ini menekankan pada proses yang sistematis mulai dari identifikasi masalah hingga uji coba produk atau sistem.



Adapun tahapan-tahapan dalam model pengembangan ini adalah sebagai berikut:

1. Identifikasi Masalah

   Identifikasi Masalah dilakukan untuk mengamati dan menemukan permasalahan yang terjadi pada sistem jaringan di Kantor Pengadilan Agama Rantauprapat. Proses identifikasi dilakukan melalui survei langsung ke lapangan, observasi konfigurasi jaringan yang sedang berjalan, serta wawancara dengan pihak pengelola IT.

2. Pengumpulan Data

   Mengumpulkan data melalui observasi, wawancara, dan studi literatur untuk memahami kebutuhan sistem.

3. Desain Sistem Jaringan

   Merancang sistem keamanan jaringan berbasis Mikrotik menggunakan metode *Port Knocking* dan ACL.

4. Validasi dan Implementasi Sistem Jaringan

   Membangun dan menerapkan sistem berdasarkan desain yang telah dibuat, serta melakukan pengujian awal.

5. Revisi Sistem Jaringan

   Melakukan perbaikan atau penyempurnaan sistem berdasarkan hasil uji awal dan analisis kelemahan.

6. Potensi dan Masalah

   Mengidentifikasi permasalahan keamanan jaringan yang terjadi di lingkungan instansi.

Melalui tahapan di atas, penelitian ini diharapkan dapat menghasilkan sistem keamanan jaringan yang tidak hanya efektif dan efisien, tetapi juga relevan dan aplikatif untuk digunakan di lingkungan nyata. Selain itu, pendekatan ini memungkinkan peneliti untuk melakukan perbaikan berkelanjutan terhadap sistem berdasarkan umpan balik dan hasil pengujian langsung di lapangan.

3.2 Tempat dan Waktu Penelitian

3.2.1 Tempat Penelitian

Tempat penelitian dilaksanakan di Kantor Pengadilan Agama Rantauprapat Kelas I B yang beralamat di Jln. S.M.Raja, Komplek Asrama Haji No.04 Kelurahan Ujung Bandar, Kecamatan Rantau Selatan, Kabupaten Labuhanbatu.

Gambar 3. 1 Kantor Pengadilan Agama Rantauprapat Kelas I B

3.2.2 Waktu Penelitian

Waktu Penelitian dimulai pada saat penulis mengajukan riset untuk penelitian yaitu pada bulan April 2025. Dengan melakukan survey tempat dan melakukan pengamatan terhadap objek yang akan diteliti. Dan berlanjut hingga bulan Juni untuk langkah pembuatan laporan skripsi. Berikut *table* waktu pengerjaan penelitian sebagai berikut :

Tabel 3. 1 Jadwal Penelitian

No	Tahapan Kegiatan	Tahun 2025															
		April				Mei				Juni				Juli			
		Minggu Ke															
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Uji Coba Sistem Jaringan																
2	Pengumpulan Data																
3	Desain Sistem Jaringan																

4	Validasi dan Implementasi Sistem Jaringan																
5	Revisi Sistem Jaringan																
6	Potensi masalah																

3.3 Metode Pengembangan

Pengembangan sistem keamanan jaringan pada penelitian ini dilakukan dengan menerapkan dua metode utama, yaitu *Port Knocking* dan *Access Control List (ACL).* Kedua metode ini digunakan secara bersamaan untuk menciptakan sistem autentikasi berlapis yang mampu membatasi dan mengendalikan akses ke jaringan.

3.3.1 *Port Knocking*

Port knocking adalah suatu metode keamanan jaringan yang digunakan untuk menyembunyikan *port* penting dari akses langsung, terutama *port* manajemen seperti *Winbox* (*port* 8291), SSH *(port* 22), dan HTTP (*port* 80) pada perangkat Mikrotik. Teknik ini bekerja berdasarkan konsep *"security by obscurity",* di mana *port* akan tampak tertutup *(filtered/stealth)* bagi siapa pun yang mencoba mengaksesnya secara langsung. Adapun fungsi *Port Knocking* dalam Sistem Ini

1. Menyembunyikan *Port* Manajemen

   Dengan *Port Knocking*, *port* seperti *Winbox* atau SSH tidak akan merespons permintaan dari luar secara *default*. Ini membuat *port* tersebut tidak terlihat saat dilakukan *port scanning* oleh pihak tidak bertanggung jawab.

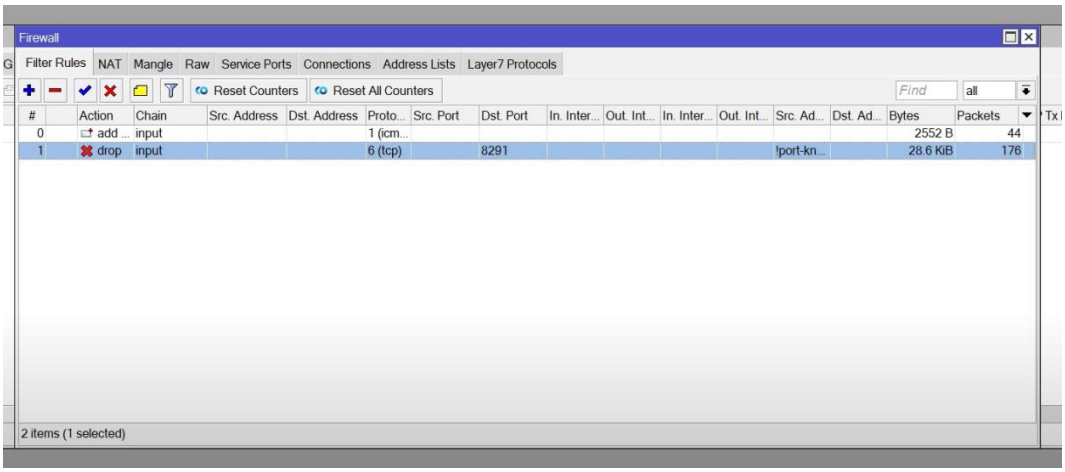
2. Autentikasi Awal

   Port Knocking berperan sebagai gerbang autentikasi pertama. Hanya pengguna yang mengetahui dan mengirimkan urutan *knock* (misalnya, permintaan ke port 1000 → 2000 → 3000 dalam urutan tertentu) yang akan diberikan akses ke *port* manajemen.

3. Pencegahan *Port Scanning & Brute Force*

Karena *port* manajemen tidak terbuka secara *default*, serangan seperti *port scanning* dan *brute force* tidak dapat dilakukan. Sistem hanya "membuka diri" ketika *knocking* yang sah terdeteksi.

- Cara Kerja *Port Knocking*
  1. *Firewall* Mikrotik dikonfigurasi agar semua port manajemen tertutup.
  2. Pengguna yang sah mengirimkan *knock* ke serangkaian *port* dalam urutan yang telah ditentukan (misal: 7000 → 8000 → 9000).
  3. Mikrotik mendeteksi urutan *knock* tersebut menggunakan *rule firewall* berbasis *connection state* dan *timeout.*
  4. Jika urutannya benar, Mikrotik secara otomatis membuka akses ke port tertentu (misal *port Winbox*) selama jangka waktu tertentu (misal 15–30 detik).
  5. Setelah waktu habis, *port* kembali tertutup secara otomatis.



Gambar 3. 2 Konfigurasi *Port Knocking*

Dalam penelitian ini, *Port Knocking* berperan sebagai lapisan keamanan awal yang melindungi *port* manajemen Mikrotik dari akses sembarangan. Fungsinya sangat penting dalam konteks kantor seperti Pengadilan Agama Rantauprapat, di mana akses jaringan harus dikontrol secara ketat, tetapi tetap memungkinkan untuk diakses oleh *administrator* jaringan dari perangkat tertentu. Dengan menerapkan *Port Knocking*:

1. Administrator bisa tetap mengakses router dari perangkat tertentu,

2. Pengguna tidak sah akan kesulitan mengetahui *port* yang terbuka karena hasil *port scanning* akan selalu tampak seolah semua *port* tertutup,
3. Sistem menjadi lebih aman tanpa mempersulit akses bagi pihak internal.

Port Knocking hanya memastikan bahwa *port* yang diminta dibuka sementara, namun tidak menjamin perangkat yang membuka *port* adalah perangkat yang sah. Oleh karena itu, setelah *knocking* berhasil, sistem akan melanjutkan proses *autentikasi* ke tahap ACL, di mana identitas perangkat akan diperiksa (*MAC Address* dan *IP Address*).

3.3.2 *Access Control List (ACL)*

Access Control List (ACL) digunakan untuk menyaring dan membatasi perangkat yang diizinkan untuk mengakses jaringan, dengan dasar identitas seperti *MAC Address* dan *IP Address*. Penerapan ACL menjadi lapisan keamanan kedua setelah proses *Port Knocking* berhasil dilakukan, artinya meskipun sebuah perangkat berhasil membuka *port* manajemen *router* melalui urutan *knock* yang tepat, akses tetap akan dibatasi jika identitas perangkat tidak sesuai dengan daftar yang telah ditentukan.

ACL bekerja dengan memverifikasi setiap koneksi masuk berdasarkan alamat MAC atau IP perangkat. Jika perangkat tidak termasuk dalam *whitelist* (daftar yang diizinkan), maka koneksi akan ditolak, dibatasi, atau bahkan diputus secara otomatis oleh *router*. Hal ini memastikan bahwa hanya perangkat yang sah dan telah terdaftar sebelumnya yang bisa mengakses jaringan secara penuh, sehingga mengurangi risiko penyusupan oleh perangkat asing.

Dalam konteks penelitian ini, ACL berfungsi sebagai sistem *filtering* dan kontrol akses lanjutan, dengan cara:

1. Memastikan hanya perangkat internal (seperti laptop admin atau komputer staf tetap) yang bisa terhubung,
2. Mencegah perangkat tidak dikenal meskipun mereka berhasil melakukan *Port Knocking,*
3. Mengatur hak akses berdasarkan *level* pengguna, IP *statis*, dan *interface* jaringan.

Dengan adanya ACL, sistem keamanan menjadi berlapis dan selektif, menjamin hanya pengguna dan perangkat yang benar-benar dikenal yang diberi akses terhadap jaringan dan layanan internal.

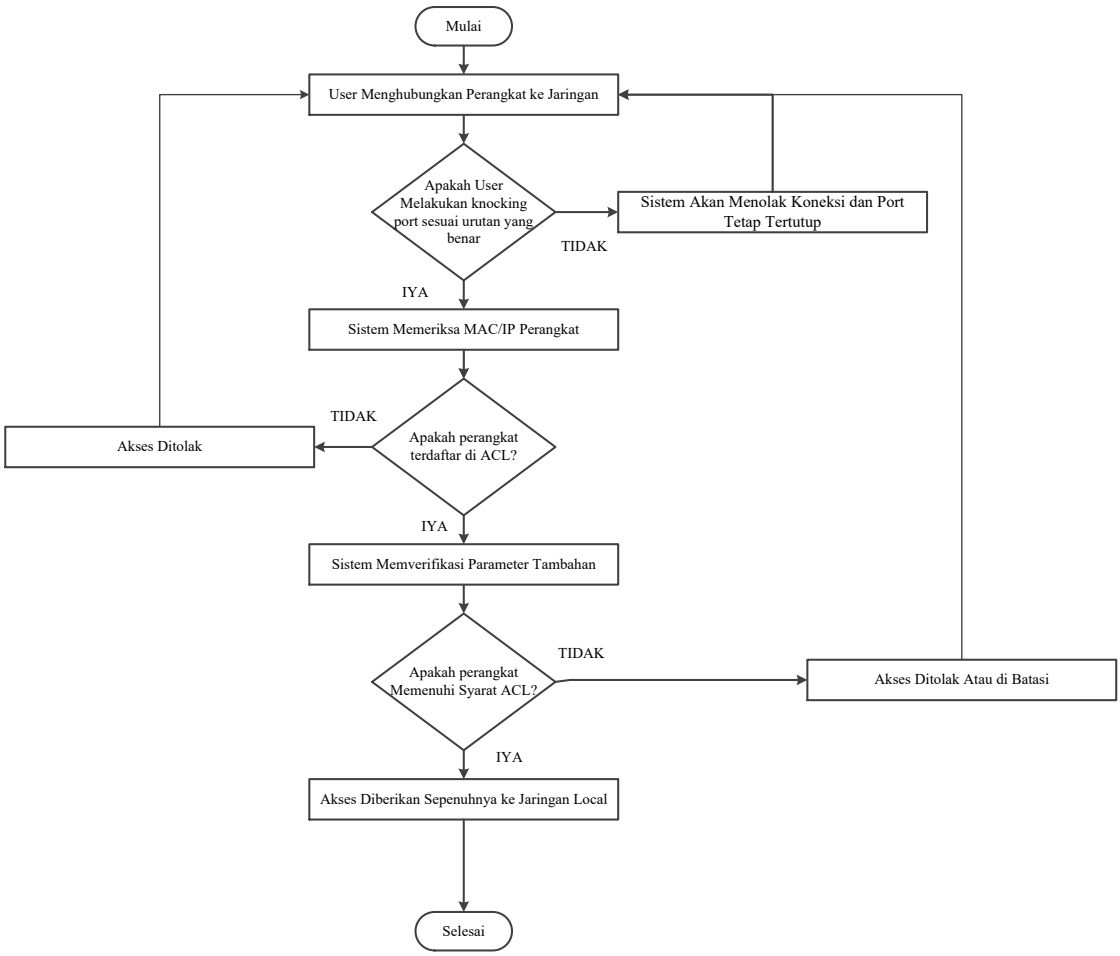
Setelah metode ditentukan, sistem dirancang menggunakan topologi bus, di mana Mikrotik hAP lite RB941-2nD berperan sebagai pengendali utama jaringan. Sistem dirancang sedemikian rupa sehingga alur autentikasi dilakukan secara berlapis:

1. Pengguna melakukan *knocking* (akses ke *port* tersembunyi),
2. Jika urutan *knock* sesuai, *port* manajemen terbuka sementara,
3. Mikrotik kemudian memverifikasi identitas perangkat melalui ACL,
4. Jika sesuai, akses diberikan; jika tidak, koneksi ditolak.

Dengan rancangan ini, sistem keamanan jaringan tidak hanya mengandalkan satu lapisan pengamanan, tetapi memiliki mekanisme kontrol yang bertingkat untuk mengurangi risiko akses tidak sah dari luar jaringan.

3.3.3 *Flowchart* Sistem Jaringan

Flowchart sistem menggambarkan alur proses autentikasi yang harus dilalui oleh pengguna sebelum memperoleh akses ke jaringan internal. Sistem keamanan ini dirancang untuk membatasi akses hanya kepada perangkat yang lolos verifikasi ganda, yaitu melalui Port Knocking dan *Access Control List (ACL)*. Dengan penggabungan dua metode ini, sistem memberikan perlindungan berlapis terhadap potensi akses tidak sah atau penyusupan ke dalam jaringan.



Gambar 3. 3 *Flowchart* Sistem

Adapun alur kerja sistem dari sisi pengguna pada Gambar 3.3 dapat dijelaskan sebagai berikut:

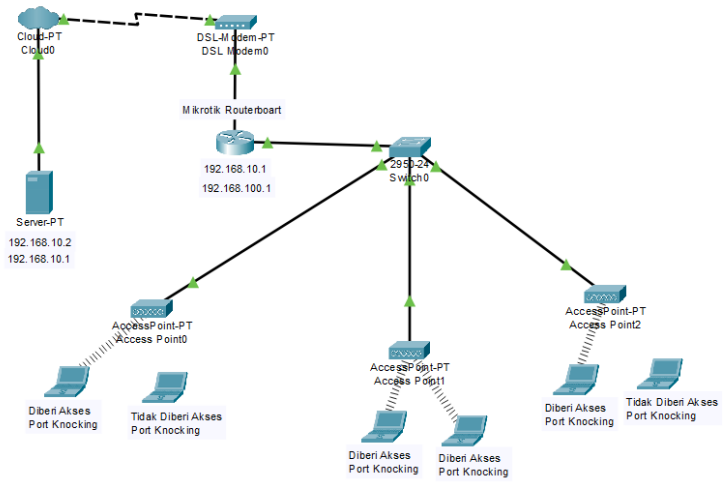
1. Pengguna mencoba mengakses jaringan, baik melalui koneksi kabel *(LAN)* maupun nirkabel *(WiFi)*.
2. Sistem mendeteksi permintaan koneksi dan menunggu urutan *knocking* dilakukan ke *port-port* tertentu.
3. Apabila urutan *knocking* salah atau tidak dilakukan, sistem akan menolak koneksi dan *port* tetap tertutup.
4. Jika urutan *knocking* benar, maka sistem membuka *port* manajemen (misalnya *port Winbox*) secara sementara.
5. Setelah akses ke *port* terbuka, sistem melakukan verifikasi terhadap identitas perangkat berdasarkan *MAC address* atau *IP address.*
6. Jika MAC/IP tidak terdaftar dalam ACL, akses tetap akan ditolak meskipun *knocking* berhasil.

7. Jika MAC/IP terdaftar dalam ACL, sistem akan memverifikasi parameter tambahan, seperti kekuatan sinyal, durasi waktu akses, dan batasan *bandwidth.*
8. Jika semua kriteria lolos, maka akses diberikan sepenuhnya ke jaringan lokal.

3.3.4 Perancangan Sistem Jaringan

Perancangan sistem jaringan dalam penelitian ini bertujuan untuk menerapkan metode keamanan berlapis menggunakan Port Knocking *dan Access Control List (ACL)* pada perangkat Mikrotik. Sistem dirancang agar mampu menyaring akses berdasarkan urutan autentikasi dan identitas perangkat, serta memberikan perlindungan ganda terhadap upaya penyusupan ke jaringan internal. Sistem ini diimplementasikan pada jaringan yang telah dirancang khusus untuk mengakomodasi kebutuhan segmentasi dan *filtering*.

Topologi yang digunakan adalah topologi bus, di mana seluruh perangkat terhubung dalam satu jalur utama dengan Mikrotik hAP lite RB941-2nDsebagai pusat kontrol. Topologi ini dipilih karena sederhana dan efektif dalam skala jaringan lokal kantor. Topologi jaringan secara keseluruhan dapat dilihat pada gambar berikut:



Gambar 3. 4 Topologi Jaringan

Topologi jaringan menunjukkan perangkat Mikrotik *RouterBoard* sebagai pusat jaringan, terhubung dengan tiga *access point* yang melayani perangkat client

berupa laptop yang mengatur berjalannya akses jaringan yang diberi izin masuk dan mengakses *server.* Jaringan juga terhubung dengan internet melalui *modem DSL.* Perancangan ini memungkinkan pembagian segmentasi jaringan dan pengendalian akses berdasarkan pengaturan *Port Knocking* dan ACL.

3.3.6 Implementasi Sistem

Pada tahap ini, sistem keamanan jaringan mulai diterapkan secara langsung dengan memanfaatkan perangkat Mikrotik *RouterBoard* hAP lite. Implementasi difokuskan pada konfigurasi metode *Port Knocking* dan *Access Control List (ACL)* yang saling terintegrasi untuk meningkatkan segmentasi dan kontrol akses jaringan. Langkah-langkah implementasi dilakukan sebagai berikut:

1. Konfigurasi *Port Knocking*

   Pengaturan dimulai dengan menutup semua *port* penting pada Mikrotik seperti *Winbox*, SSH, dan HTTP. *Port* hanya akan terbuka jika pengguna melakukan *knocking* atau permintaan koneksi ke beberapa *port* secara berurutan dalam urutan yang telah ditentukan.

   - Konfigurasi dilakukan melalui aplikasi *Winbox.*
   - *Firewall* disetting agar mengenali urutan *knock* sebagai "sinyal masuk" yang sah.
   - Hanya pengguna yang berhasil melakukan *knocking* dengan urutan benar yang akan diberikan akses ke *port* manajemen.

2. Konfigurasi *Access Control List (ACL)*

   Setelah *Port Knocking* berhasil dilakukan, pengguna masih harus melewati penyaringan ACL untuk dapat mengakses jaringan.

   - Konfigurasi ACL dilakukan dengan membatasi akses berdasarkan *MAC address* dan *IP address.*
   - Hanya perangkat yang telah didaftarkan dalam daftar ACL yang dapat terhubung ke jaringan *WiFi* dan mengakses jaringan lokal.
   - ACL juga digunakan untuk membatasi kekuatan sinyal (*signal strength*), waktu koneksi, dan kecepatan akses.

3. Integrasi dan Pengujian Awal

Sistem diuji secara bertahap, mulai dari satu perangkat *client* yang sah hingga mencoba koneksi dari perangkat asing.

- Jika *knock sequence* salah atau MAC tidak dikenali, akses akan ditolak.
- Jika keduanya berhasil, maka akses diberikan secara terbatas sesuai profil pada ACL.

Implementasi ini bertujuan agar hanya pengguna yang melewati dua lapis otentikasi (*Port Knocking* dan ACL) yang dapat terhubung ke jaringan, sehingga risiko dari serangan eksternal maupun internal dapat diminimalisir secara signifikan.

3.4 Alat dan Bahan Penelitian

Dalam penelitian ini, pengembangan sistem keamanan jaringan dilakukan secara langsung melalui proses perancangan dan implementasi perangkat jaringan menggunakan metode *Port Knocking* dan *Access Control List (ACL).* Oleh karena itu, dibutuhkan beberapa alat dan bahan pendukung, baik berupa perangkat keras *(hardware)* maupun perangkat lunak *(software)* untuk menunjang keberhasilan proses penelitian.

Tabel 3. 2 *Hardware* yang Digunakan

No	Nama Perangkat	Fungsi
1	Mikrotik hAP lite RB941-2nD	*Router* utama yang digunakan untuk konfigurasi sistem keamanan jaringan
2	Modem DSL	Sumber koneksi internet untuk kebutuhan pengujian akses
3	*Access Point*	Media koneksi nirkabel untuk perangkat *client*
4	Laptop	Untuk konfigurasi, dokumentasi, dan pengujian sistem
5	Laptop *Client*	Digunakan untuk menguji autentikasi *client* terhadap sistem
6	Kabel LAN	Menghubungkan antar perangkat jaringan

Tabel 3. 3 *Software* yang Digunakan

No	Nama Software	Fungsi
1	*Winbox*	Aplikasi konfigurasi dan monitoring Mikrotik RouterBoard
2	*Advanced IP Scanner*	Untuk memantau perangkat yang aktif dalam jaringan
3	*Cisco Packet Tracer*	Untuk mendesain topologi dan memvisualisasikan sistem jaringan
4	*Microsoft Word*	Untuk penyusunan laporan dan dokumentasi skripsi