BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Terdapat beberapa penelitian yang sebelumnya sudah dilakukan kemudian digunakan sebagai acuan dalam penelitian ini.

Heri Cahyana (2013) mengimplementasikan *routing protocol* OSPF sebagai *dynamic routing*. Tiga buah Mikrotik RB750 dikonfigurasi dalam OSPF area 0 sebagai area *backbone*. Melalui penelitian tersebut didapatkan hasil ketiga *router* dapat saling terkoneksi dan bertukar tabel *routing* menggunakan *routing protocol* OSPF.

Wagito (2012) mengimplementasikan *internet exchange* menggunakan Mikrotik RB750 dengan tujuan memperpendek rute antar ISP. Implementasi tersebut awalnya disimulasikan pada aplikasi Packet Tracer kemudian dikonfigurasi pada RB750. Konsep *exchange* yang diterapkan menggunakan *static-route* tanpa menggunakan *check-gateway* atau *distance route*, sehingga membutuhkan *script* untuk mendeteksi apakah *link* IX mengalami gangguan. Melalui penelitian tersebut, IX dapat memperpendek rute transit ke ISP lain yang berada pada regional yang sama.

Yasir Arafat, dkk (2022) melakukan penelitian dan implementasi pembangunan jaringan Internet dan Intranet di Kabupaten Sambas, Kalimantan Barat. Pembangunan infrastruktur menggunakan topologi *star* dengan pusat data berada di balai desa Pemangkat Kota meliputi perangkat jaringan nirkabel *outdoor*

dan *web server* yang digunakan untuk aplikasi *website* administrasi desa dan *website* pembelajaran daring bagi SDN di area tersebut.

Hendra Kurniawan, dkk (2015) melakukan penelitian mengenai perancangan Intranet untuk mendukung proses pembelajaran di STMIK Pontianak. Penelitian ini menghasilkan *prototype* desain jaringan menggunakan topologi *star* yang menghubungkan satu *server web e-learning* dengan komputer di masing-masing ruang pembelajaran sehingga dosen tidak perlu membawa laptop ke ruangan.

Akhmad Fathurohman, dkk (2021) melakukan penelitian mengenai implementasi BGP pada jaringan publik Universitas Muhammadiyah Semarang. Penelitian tersebut menghasilkan konfigurasi implementasi BGP yang digunakan untuk terkoneksi ke 2 internet provider secara multihoming yang digunakan sebagai failover ketika provider utama down. Di dalam penelitian juga dibahas mengenai topologi jaringan intranet yang ada saat ini menggunakan gabungan topologi *star* dan *ring*.

Tabel 2.1 Tabel Perbandingan Penelitian

No	Penulis	Objek Penelitian	Metode/Teknologi	Keterangan
1	Heri Cahyana (2013)	Konfigurasi Routing Dinamik OSPF Pada Mikrotik RB750	Mikrotik, OSPF	Konfigurasi OSPF Pada Mikrotik
2	Wagito (2012)	Implementasi Internet Exchange Menggunakan Router RB750	Mikrotik, *static routing, ping script*	Membuat miniatur IX
3	Yasir Arafat, dkk (2022)	Rancang Bangun Jaringan Internet Dan Intranet Untuk Mendukung Layanan Administrasi Dan Informasi Masyarakat	Mikrotik, *web server, wireless*	Membuat jaringan Intranet untuk web admin desa dan *e-learning*

4	Hendra Kurniawan (2015)	Penerapan Network Development Life Cycle Dalam Perancangan Intranet Untuk Mendukung Proses Pembelajaran	web server, intranet	*prototype* jaringan Intranet untuk kampus
5	Akhmad Fathurohman, dkk (2021)	Implementasi BGP Pada Jaringan Publik Universitas Muhammadiyah Semarang	Mikrotik, BGP	Menerapkan BGP *multihoming* 2 ISP
6	Usulan Penulis (2022)	Implementasi BGP Menggunakan EoIP Over IPSec Pada RouterOS	Mikrotik, BGP, Tunnel EoIP + IPSec	BGP *dynamic routing* pada Intranet

2.2 Dasar Teori

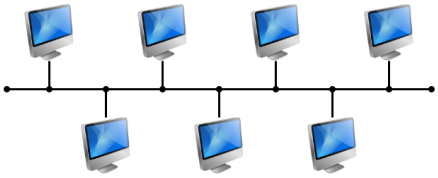
Dalam penelitian ini memanfaatkan beberapa dasar teori meliputi topologi jaringan, penyelenggaraan Intranet melalui Internet, Mikrotik, BGP, Eoip, IPSec.

2.2.1 Topologi Jaringan

Menurut Vikram Singh dan Jaspal Ramola (2014), istilah topologi mengacu kepada cara komputer dapat terhubung satu sama lain dan membentuk suatu jaringan komputer. Dalam membuat desain jaringan terdapat beberapa model yang bisa diterapkan tergantung dari kebutuhan dan kegunaan jaringan. Tentunya setiap model memiliki keunggulan dan kelemahan masing-masing. Topologi secara fisik dan topologi secara logika bisa saja berbeda. Dalam penerapan topologi secara logika biasanya bisa lebih dinamis menyesuaikan konfigurasi router dan switch yang digunakan, namun pengaturannya terbatas pada topologi fisik. Berikut adalah 5 topologi dasar pada jaringan komputer.

a. Topologi *Bus*

Merupakan cara menghubungkan beberapa komputer menggunakan 1 kabel *coaxial* sebagai *backbone* jaringan. Setiap percabangan menggunakan BNC *T connector*, sedangkan di ujung kabel menggunakan BNC *terminator* agar sinyal tidak memantul kembali ke jaringan. Biaya yang dikeluarkan dalam implementasi topologi ini tidaklah mahal karena tidak menggunakan perangkat aktif seperti *switch* atau *router*, namun apabila jumlah *node* bertambah banyak maka beban *bandwidth* akan semakin besar pada 1 kabel, dan mengganggu transmisi data ke *node* lainnya.



Gambar 2.1 Topologi Bus

b. Topologi *Ring*

Merupakan cara menghubungkan beberapa komputer menyerupai lingkaran, dimana setiap *node* akan terhubung ke 2 *node* lainnya. *Traffic* ditransmisikan melalui token yang bergerak dari satu *node* ke *node* lainnya searah jarum jam atau berlawanan arah jarum jam. Masing-masing *node* bertanggung jawab atas *traffic* seluruh jaringan. Jika salah satu *node* mati, maka token akan gagal ditransmisikan dan data tidak bisa sampai ke tujuan. Saat ini topologi *ring* mulai ditinggalkan karena dinilai tidak efisien dan sangat bergantung pada masing-masing *node* untuk mentransmisikan data mengitari jaringan.

Gambar 2.2 Topologi Ring

c. Topologi *Star*

Merupakan cara menghubungkan jaringan komputer secara terpusat pada satu perangkat, biasanya berupa *switch*. Topologi ini paling banyak digunakan oleh pengelola jaringan karena dinilai mudah implementasinya dan masing-masing *node* tidak membebani *node* lainnya. Biaya implementasi relatif lebih besar daripada topologi *bus* dan *ring* karena masing-masing *node* membutuhkan interkoneksi ke *switch*. Dalam topologi star proses identifikasi masalah juga lebih mudah karena jaringan sudah tersegmentasi, *traffic* dari suatu *node* langsung ke *switch* tanpa melalui *node* lainnya. Kelemahan topologi ini yaitu apabila *switch* atau kabel *backbone* bermasalah maka seluruh jaringan akan *down*.

Gambar 2.3 Topologi Star

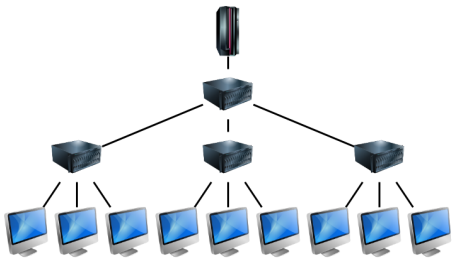
d. Topologi *Mesh*

Topologi ini terdiri dari *mesh fully connected* dan *partial connected*. Pada *partial connected*, tidak semua perangkat komputer terhubung satu sama lain. Kelebihan dari topologi *mesh* adalah jaringan komputer memiliki banyak ruang bagi lalu lintas data, namun topologi ini membutuhkan lebih banyak kabel dibanding topologi lainnya. Proses konfigurasi dan perawatannya juga lebih rumit karena perlu memastikan bahwa tidak terjadi *looping* pada jaringan.

Gambar 2.4 Topologi Mesh Fully Connected

e. Topologi *Tree*

Merupakan bentuk gabungan dari topologi *bus* dan topologi *star*, membentuk sistem hirarki dari jaringan pusat ke jaringan paling ujung. Pada umumnya topologi *bus* merupakan *backbone* utama dari topologi jaringan ini, sedangkan topologi *star* berada dari percabangan sampai hirarki paling ujung. Keuntungan dari topologi ini adalah pengembangan jaringan dapat dilakukan dengan mudah, cukup menambahkan cabang pada jalur utama. Kelemahan dari topologi ini adalah perlu adanya perhatian khusus pada jalur *backbone* karena semua *traffic* terkonsentrasi pada jalur *backbone*.



Gambar 2.5 Topologi Tree

2.2.2 Intranet

Menurut Martin White (2017), konsep Intranet pertama kali digagas oleh Douglas Engelbart pada tahun 1951, kemudian direalisasikan pada tahun 1962 ketika Ia membuat prototipe NLS (*on-line system*) di Stanford Research Institute (SRI). Engelbart menunjukkan karyanya ke publik pada tahun 1968, pada tahun berikutnya tim riset Engelbart diundang bergabung dengan tim riset ARPANET untuk mengembangkan sistem yang kemudian disebut sebagai jaringan Internet. Perkembangan pesat Intranet terjadi pada saat teknologi *Ethernet* mulai dikembangkan oleh Xerox PARC pada tahun 1973-1974, selanjutnya IBM mulai mengembangkan teknologi *Token Ring* namun kemudahan proses instalasi dan perawatan teknologi *Ethernet* membuat perkembangan *Token Ring* ditinggalkan. Pada rentang tahun 1994-2002, Microsoft dan Netscape berlomba-lomba membuat *groupware*, suatu aplikasi yang memungkinkan anggota organisasi untuk berbagi informasi, dokumen, surel, sinkronisasi kalender, dan lain-lain. Intranet berkembang menjadi Ekstranet, dan kemudian terus berkembang menjadi Internet, dimana informasi bisa diakses dari seluruh penjuru dunia.

Dari awal perkembangannya sampai saat ini, Intranet digunakan oleh organisasi untuk mewujudkan kolaborasi dan pertukaran data secara internal

dalam organisasi secara tertutup. Selain membutuhkan jaringan komputer, Intranet juga membutuhkan *software* dan sistem *client-server* dalam operasionalnya sehingga data bisa diakses bersama-sama secara *real-time*. Bermula dari aplikasi yang diakses hanya menggunakan *browser*, Intranet dikembangkan menjadi sistem terintegrasi yang saling terkoneksi, bersamaan dengan perkembangan sistem *Lightweight Directory Access Protocol* (LDAP). LDAP merupakan sistem manajemen sumber daya pada organisasi yang mampu mengatur hak akses para anggota dalam satu kesatuan kontrol. Sampai saat ini konsep Intranet terus dikembangkan bahkan sampai ke jaringan Internet, namun dengan kontrol tersendiri sehingga informasi hanya bisa diakses oleh internal organisasi.

2.2.3 Internet

Menurut Leiner, dkk (1997), Bolt Beranek and Newman (BBN) mengaktifkan *node* pertama ARPANET di University of California, Los Angeles (UCLA) pada September 1969. Saat itu mesin komputasi yang digunakan adalah SDS Sigma 7 terkoneksi dengan *packet switch* yang disebut *Interface Message Processors* (IMP), hasil gagasan Leonard Kleinrock. Proyek “Augmentation of Human Intellect” milik Douglas Engelbart menggunakan mesin SDS 940 di Stanford Research Institute (SRI) menjadi *node* kedua yang terkoneksi ke ARPANET. UCLA difungsikan sebagai Network Measurement Center berperan untuk melakukan analisa jaringan ARPANET, sedangkan SRI sebagai Network Information Center berperan sebagai pemetaan alamat jaringan, perawatan tabel *hostname*, juga sebagai pencatatan *Request For Comments* (RFC).

Pada Oktober 1969, pesan host-to-host pertama di jaringan ARPANET dikirimkan dari UCLA ke SRI. Jaringan ARPANET kemudian menjadi 4 host setelah bergabungnya UC Santa Barbara (UCSB) dan University of Utah, yang berperan mencari cara merepresentasikan visual 3-dimensi pada mesin komputasi. Dalam perkembangan ARPANET, David Clark dan tim riset dari MIT memperkenalkan teknologi *Transmission Control Protocol* (TCP) sebagai protokol komunikasi untuk mengirim dan menerima data. Namun protokol tersebut dianggap terlalu berat bagi komputer standar rumahan dengan sumber daya yang terbatas. Lalu mereka mengimplementasikan hasil riset mereka pada Xerox Alto buatan Xerox PARC, IBM PC, dan lain-lain. Hasilnya TCP dapat diterima masyarakat luas sebagai protokol yang cukup reliabel dalam melakukan transmisi data. Protokol TCP dapat melakukan pengecekan keutuhan data dan melakukan transmisi ulang jika ada data-data yang mengalami *collision* ataupun *corrupt*.

Internet berkembang pesat sejak saat TCP/IP diimplementasikan, karena TCP/IP menjadi standar konektivitas Internet sehingga perangkat-perangkat yang dibuat oleh vendor yang berbeda-beda tetap dapat saling berkomunikasi dan bertukar informasi. Seiring juga dengan perkembangan komputer, perangkat jaringan yang diciptakan mulai beragam, mulai dari *desktop*, *laptop*, *tablet*, *smartphone*, IoT, dan lain-lain. Saat ini konektivitas Internet menjadi salah satu penunjang kebutuhan hidup.

2.2.4 RouterOS

MikroTik berawal dari sebuah perusahaan penyedia layanan Internet (ISP) di Latvia, dengan proyek pertama di negara Moldova pada tahun 1996. Pada tahun 1997, MikroTik mengembangkan sebuah sistem operasi bagi perangkat *router* yaitu RouterOS dengan fitur-fitur yang didesain sedemikian rupa bagi kebutuhan administrasi jaringan. Pada waktu itu MikroTik masih menggunakan perangkat keras PC (*personal computer*) standar dengan tambahan *interface* nirkabel. RouterOS dikembangkan dari Linux Kernel 2.2 dengan 5-15 tim R&D (*Research And Development*).

RouterOS menggunakan sistem lisensi *perpetual* dengan 6 *level* berbeda. Masing-masing *level* memiliki batasan fitur tersendiri. Secara *default*, RouterOS menggunakan lisensi *level* 0 (*trial mode*) dengan masa aktif selama 24 jam. Setelah masa *trial* berakhir, *router* akan *restart* dan kembali ke setelan awal. RouterOS pada arsitektur CHR (*cloud hosted router*) memiliki tingkatan yang berbeda. Pada CHR hanya terdapat 4 tingkatan lisensi, masing-masing tingkat membatasi besar *traffic* yang di-*forward* oleh *router*. Berbeda dengan arsitektur lainnya, lisensi gratis pada arsitektur CHR dapat digunakan tanpa batasan fitur. Pada CHR, lisensi dapat dipindahkan dari satu sistem ke sistem lain asalkan RouterOS dapat terkoneksi ke *server* Mikrotik. Masa *trial* pada arsitektur CHR adalah 60 hari, hal ini berlaku apabila hendak melakukan *upgrade* dari lisensi *free* ke tingkatan di atasnya. Jika sampai masa *trial* berakhir belum melakukan *update* lisensi, instalasi CHR akan dikunci dan tidak dapat melakukan *update firmware*, maka sistem harus diinstall ulang.

Untuk bersaing dengan produk lainnya, Mikrotik mulai mengembangkan perangkat keras sendiri pada tahun 2002. Berawal dari DOM (*disk on module*), RouterOS dapat diinstall pada PC standar dengan DOM sebagai pengganti *harddisk*. Untuk membuat sistem yang lebih efisien, Mikrotik mulai membuat SOC (*system on a chip*) dengan *brand* RouterBoard. Dengan kebutuhan sumber daya yang jauh lebih kecil, RouterBoard tetap dapat menjalankan sebagian besar fungsi *router* dan *firewall* dengan baik. Dengan perkembangan perangkat lunak RouterOS dan perkembangan perangkat keras RouterBoard, Mikrotik menjadi solusi lengkap bagi kebutuhan perangkat jaringan.

2.2.5 BGP

BGP (*Border Gateway Protocol*) merupakan protokol *routing* standar internasional. BGP merupakan protokol *routing* dengan klasifikasi *path vector*, menggunakan algoritma pemilihan jalur berdasarkan jarak menuju AS (*Autonomous System*) tujuan. AS merupakan domain otonomi suatu organisasi ditandai dengan AS *number* sebagai identitas masing-masing organisasi ataupun suborganisasi.

Pada umumnya interkoneksi BGP dalam suatu organisasi menggunakan IGP (*Interior Gateway Protocol*) seperti OSPF (*Open Shortest Path First*), digunakan apabila dalam suatu organisasi memiliki banyak *router* dan perlu saling bertukar tabel *routing*. Namun penggunaan OSPF kurang efektif digunakan pada

jaringan yang berada pada letak geografis yang berbeda karena perubahan *state* jaringan yang tidak stabil akan berimbas *flapping* pada jaringan.

Seperti tercantum pada RFC 4271, terdapat IBGP (*Internal Border Gateway Protocol*) dan EBGP (*External Border Gateway Protocol*). IBGP memungkinkan *router-router* yang berada pada *Autonomous System* yang sama untuk bertukar informasi tabel *routing*, sedangkan EBGP digunakan untuk bertukar tabel *routing* pada *Autonomous System* yang berbeda. Walaupun bisa diimplementasikan sebagai IGP, seperti OSPF, *internal* BGP mengharuskan seluruh *node* terkoneksi secara *full mesh* untuk mencegah terjadinya *routing loop*. Imbasnya adalah ketika hendak menambah *node* baru pada jaringan, perlu dilakukan *setup* interkoneksi BGP di internal AS. Untuk mengatasi hal tersebut, dibuatlah BGP *Route Reflector* (RFC 4456) sebagai solusi alternatif dari *full mesh* IBGP.

Dalam interkoneksi *external* BGP terdapat beberapa metode *load sharing* untuk menghubungkan suatu organisasi ke Internet, antara lain:

a. Single Homed

Merupakan metode interkoneksi BGP dari suatu *Autonomous System* menggunakan satu jalur ke ISP (*Internet Service Provider*). Kelebihan dari metode ini adalah biaya instalasi lebih terjangkau, proses perawatan juga lebih mudah. Kelemahan dari metode ini adalah tidak adanya jalur cadangan jika jalur utama bermasalah.

b. Dual Homed

Merupakan metode interkoneksi BGP yang menghubungkan suatu *Autonomous System* ke ISP menggunakan lebih dari satu jalur. Masing-masing jalur dapat diterminasi pada satu *router* atau lebih. Kelebihan dari metode ini adalah terdapat jalur cadangan ke ISP, namun apabila ada kendala di sisi ISP maka koneksi Internet akan terputus.

c. Single Multi-homed

Merupakan metode interkoneksi BGP dari suatu *Autonomous System* ke lebih dari satu ISP, namun masih menggunakan satu jalur interkoneksi di masing-masing ISP. Metode ini mampu menjaga interkoneksi ke Internet apabila salah satu ISP mengalami gangguan.

d. Dual Multi-homed

Merupakan metode interkoneksi BGP dari suatu *Autonomous System* ke lebih dari satu ISP menggunakan lebih dari satu jalur interkoneksi. Metode ini dinilai lebih aman dari gangguan, namun membutuhkan biaya yang lebih tinggi serta perawatan jaringan yang lebih rumit.

Sama seperti pada alamat IP, *Autonomous System Number* (ASN) juga memiliki alokasi bagi penggunaan privat. *Private ASN* dialokasikan pada rentang 64512 – 65534, dapat digunakan untuk interkoneksi EBGP dalam satu organisasi.

2.2.6 EoIP Over IPSec

Ethernet over Internet Protocol (EoIP) merupakan protokol *tunnel proprietary* milik MikroTik yang berjalan di atas protokol GRE (*Generic Routing Encapsulation*). EoIP membutuhkan konfigurasi IP statik dan parameter *tunnel id* di kedua sisi agar *tunnel* bisa terbentuk. Setelah EoIP terbentuk, *interface* EoIP bisa dipasang pada *bridge* dengan *ethernet* fisik *router*, maka *broadcast domain* akan diteruskan ke ujung *tunnel* sehingga *layer 2* di masing-masing *router* bisa saling bertukar data.

Secara *default* EoIP tidak memiliki enkripsi sehingga data yang ditransmisikan pada jaringan publik bisa disadap. Untuk mengatasi hal tersebut dapat dilakukan beberapa cara. *Tunnel* EoIP bisa dibuat di atas interkoneksi PPP seperti PPTP, SSTP, OpenVPN, dan lain-lain. Atau bisa juga mengaktifkan fitur enkripsi dari IPSec dengan cara menambahkan IPSec *secret* pada *interface tunnel*.

Dharma dan Suharjito (2020) melakukan penelitian mengenai kondisi ketika *tunnel* EoIP tanpa IPSec menggunakan aplikasi Wireshark. Dari hasil penelitian tersebut ditemukan bahwa peneliti dapat melakukan *sniffing* terhadap *traffic* yang melewati jalur *tunnel* EoIP, menampilkan data sensitif yang dikirimkan oleh satu *node* ke *node* yang lain. Ketika IPSec pada EoIP diaktifkan, RouterOS melakukan enkripsi data terlebih dahulu sebelum mengirimkan data ke node lain. Hal tersebut membuktikan bahwa IPSec dapat mengamankan transmisi EoIP pada jalur Internet.