BAB II

TINJAUAN PUSTAKA

2.1 Penilitian Sebelumnya

Meskipun penelitian mengenai deteksi dan mitigasi serangan DDoS pada arsitektur Software-Defined Networking (SDN) telah berkembang pesat, sebagian besar pendekatan yang diusulkan masih berfokus pada pemanfaatan teknik machine learning dan deep learning. Seperti pada jurnal yang berjudul *An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers* yang ditulis oleh James Dzisi Gadze, Akua Acheampomaa Bamfo-Asante, Justice Owusu Agyemang, Henry Nunoo-Mensah, dan Kwasi Adu-Boahen Opare (Technologies 2021, 9, 14) [23] misalnya, meneliti efektivitas model deep learning seperti LSTM dan CNN dalam mendeteksi serta mengklasifikasikan trafik DDoS yang mengancam controller SDN. Hasil penelitian menunjukkan bahwa pendekatan berbasis deep learning mampu meningkatkan akurasi deteksi serangan DDoS dibandingkan dengan model machine learning konvensional. Namun, solusi yang diusulkan dalam jurnal ini masih terbatas pada aspek deteksi dan belum secara spesifik membahas mekanisme mitigasi yang dapat diimplementasikan di tingkat infrastruktur jaringan yang lebih luas, seperti melalui manipulasi Border Gateway Protocol (BGP) Community.

Padahal, dalam praktik di jaringan global, mitigasi DDoS tidak hanya membutuhkan deteksi dini, tetapi juga aksi respons yang cepat dan terkoordinasi untuk mengalihkan, memblokir, atau mengurangi dampak trafik berbahaya. Salah satu mekanisme yang telah banyak digunakan oleh operator jaringan adalah BGP Community, yang memungkinkan pengalihan trafik (misal: blackholing atau sinkholing) melalui pengaturan kebijakan routing antar Autonomous System (AS). Sayangnya, baik dalam jurnal ini maupun dalam sebagian besar literatur yang direview, integrasi antara deteksi otomatis berbasis AI/ML dan aksi mitigasi berbasis BGP Community masih sangat minim dibahas.

Dengan kata lain, terdapat kekosongan penelitian (research gap) pada aspek integrasi antara sistem deteksi DDoS berbasis deep learning dengan mekanisme mitigasi otomatis yang memanfaatkan BGP Community. Belum ada framework yang menghubungkan hasil klasifikasi trafik DDoS secara real-time dengan kebijakan routing BGP Community, sehingga aksi pengalihan atau pemblokiran trafik dapat dilakukan secara otomatis dan efisien. Selain itu, efektivitas dan potensi risiko dari penerapan BGP Community dalam mitigasi DDoS pada lingkungan SDN juga belum banyak dianalisis, baik dari sisi performa jaringan maupun kualitas layanan yang diterima pengguna akhir.

Oleh karena itu, penelitian lebih lanjut sangat diperlukan untuk mengembangkan solusi yang mengintegrasikan deteksi serangan DDoS berbasis AI/ML dengan mitigasi berbasis BGP Community. Penelitian tersebut diharapkan mampu menghadirkan sistem yang tidak hanya mampu mendeteksi serangan secara akurat, namun juga dapat merespons dengan cepat melalui pengaturan routing di level BGP, serta memberikan evaluasi yang komprehensif terhadap dampaknya pada performa dan keamanan jaringan secara keseluruhan.

2.2 Kajian Teoritis

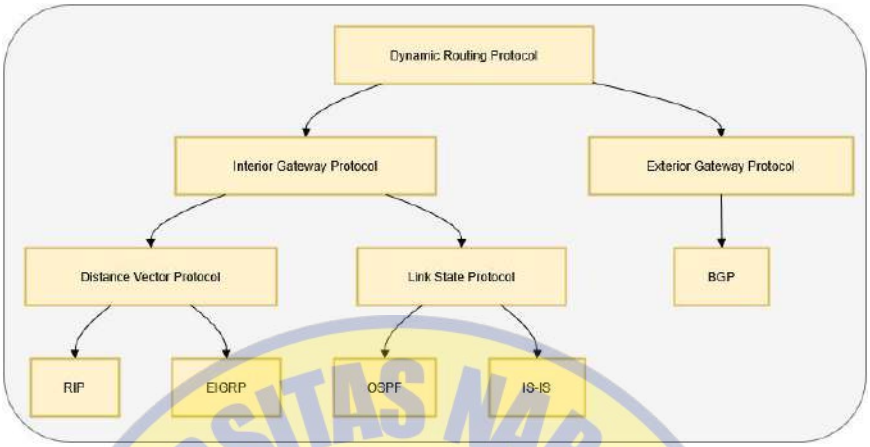
Kajian teoritis dalam penelitian ini mencakup pembahasan mengenai konsep routing, BGP, GNS3, route reflector, dan sebagai dasar dalam memahami dan mengembangkan penelitian ini.

2.2.1 Jenis Routing Dinamis

Routing protocol adalah protokol yang terdapat pada routing dinamik (dynamic routing). Routing protocol bertugas untuk menentukan jalur terbaik yang akan dilewati oleh data serta memperbarui informasi tabel routing apabila terjadi perubahan jaringan.Terdapat macam-macam routing protocol yang dapat digunakan untuk melakukan routing dinamik. Setiap protokol memiliki kelebihan dan kekurangan masing-masing.

Beberapa routing protocol juga menggunakan sebuah algoritma yang bertugas untuk melakukan kalkulasi untuk mendapatkan jalur terbaik (best

path). Jadi dynamic routing protocol itu terbagi menjadi 2, yakni Interior Gateway Protocol (IGP) dan Exterior Gateway Protocol (EGP).



Gambar 2.1 Jenis Routing Dinamis

Sumber: Dokumen Pribadi

Seperti pada gambar 2.1 jenis routing terbagi dalam 2 jenis yaitu Interior Gateway Protocol (IGP) yang terdiri dari routing RIP, EIGRP, OSPF dan Exterior Gateway Protocol (EGP) yang terdiri dari routing BGP. Berikut penjelasan dari masing routing tersebut:

1. RIP (Routing Information Protocol)

Routing Information Protocol (RIP) termasuk dalam kategori protokol routing berbasis distance vector, yang menentukan jalur berdasarkan jumlah lompatan (hop) dari satu router ke router tujuan. Istilah *hop count* mengacu pada jumlah router yang dilalui untuk mencapai tujuan, sedangkan *hop* adalah jarak antar router. RIP memiliki dua versi, yaitu versi 1 dan versi 2.

RIPv2 merupakan pengembangan dari versi sebelumnya. Salah satu keunggulan RIPv2 dibandingkan RIP versi 1 adalah kemampuannya dalam mendukung Variable Length Subnet Mask (VLSM), fitur yang tidak tersedia di RIP versi pertama. Namun, RIPv2 hanya dapat bertukar informasi routing dengan router lain yang juga menggunakan RIPv2, sementara versi pertama mampu menerima pembaruan rute dari kedua versi.

Keduanya merupakan protokol open standard, sehingga dapat digunakan pada perangkat dari berbagai vendor. RIP umumnya lebih cocok diterapkan pada jaringan berskala kecil hingga menengah karena batas maksimal hop yang didukung hanya 15. Jika rute menuju tujuan memerlukan lebih dari 15 hop, maka paket data tidak akan dikirim dan akan dibuang. Keterbatasan inilah yang membuat RIP kurang ideal untuk jaringan berskala besar.

Kelebihan :

- Versi 2 mendukung VLSM dan CIDR.
- Konfigurasinya cukup sederhana.
- Tidak rumit dalam implementasi.
- Auto-summary dapat dinonaktifkan (pada RIPv2).
- Mendukung fitur autentikasi.

Kekurangan :

- Versi 1 tidak mendukung VLSM dan CID
- Jumlah *hop* maksimal hanya 15.
- RIPv2 tidak bisa menerima update dari RIPv1.
- Konvergensi lambat.
- Update routing dilakukan terus-menerus, menambah beban trafik.

2. EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP merupakan protokol routing yang dikembangkan oleh Cisco dan hanya bisa digunakan pada perangkat Cisco. Meski berbasis *distance vector*, EIGRP tidak hanya mengandalkan jumlah *hop* untuk menentukan rute. Protokol ini menggunakan kombinasi parameter seperti *bandwidth*, *load*, *delay*, dan *reliability*, yang dihitung untuk memilih jalur terbaik. EIGRP menggunakan algoritma DUAL (Diffusing Update Algorithm) untuk menentukan dan memelihara rute utama dan jalur alternatif (*Feasible Successor*) jika rute utama gagal. Dalam pengoperasiannya, EIGRP

menggunakan tiga jenis tabel: *routing table*, *neighbor table*, dan *topology table*.

Kelebihan :

- Mendukung CIDR dan VLSM.
- Jumlah *hop* maksimal mencapai 224.
- Proses konvergensi sangat cepat.
- Cakupan jaringan lebih luas dibandingkan RIP

Kekurangan :

- Bersifat proprietary Cisco, tidak bisa digunakan di perangkat non-Cisco.
- Update routing dilakukan secara berkala.
- Memerlukan lebih banyak sumber daya dari router.

3. OSPF (Open Shortest Path First)

OSPF merupakan salah satu protokol routing yang termasuk dalam kategori *link-state*. Pemilihan jalur terbaik dalam OSPF tidak hanya mengandalkan jumlah *hop*, melainkan berdasarkan nilai *cost* yang diberikan pada setiap link jaringan. Nilai *cost* ini dihitung dari berbagai faktor, seperti bandwidth, dan semakin rendah nilainya, maka semakin besar kemungkinan link tersebut dipilih sebagai rute utama..

Dalam menentukan jalur tercepat dan paling efisien, OSPF memanfaatkan algoritma **Dijkstra** yang akan menghitung rute optimal berdasarkan peta topologi jaringan yang dimiliki. Dengan kata lain, OSPF memiliki kemampuan untuk memetakan seluruh struktur jaringan secara menyeluruh dan memilih rute terbaik secara otomatis.

Untuk mengatur skalabilitas dan efisiensi dalam pertukaran informasi, OSPF membagi jaringan menjadi beberapa *area*. Setiap konfigurasi OSPF wajib memiliki satu area pusat bernama **area 0**, yang dikenal juga sebagai *backbone area*. Area ini menjadi poros utama dan penghubung dari area-area lainnya. Administrator jaringan dapat membuat area tambahan seperti area 1, area 15, atau area lainnya sesuai kebutuhan,

namun area-area tersebut wajib terhubung dengan *backbone* agar dapat saling bertukar informasi routing.

Agar komunikasi antar area dapat dilakukan, OSPF menggunakan jenis router khusus yang disebut ABR (Area Border Router), yakni router yang memiliki interface di lebih dari satu area dan bertugas menjembatani pertukaran data antar area. Selain ABR, terdapat beberapa jenis peran router dalam OSPF:

- Internal Router: Router yang seluruh interfacenya berada dalam satu area tunggal.
- Backbone Router: Router yang memiliki setidaknya satu interface yang terletak di area backbone (area 0).
- ASBR (Autonomous System Boundary Router): Router yang terhubung ke jaringan luar yang menggunakan protokol routing berbeda dari OSPF, dan digunakan untuk pertukaran rute antar protokol.

    - Internal Router, adalah router yang keseluruhan interface/linknya terletak dalam satu area.
    - Backbone Router, adalah router yang salah satu link atau seluruhnya terletak di area backbone
    - Autonomous System Boundary Router, adalah router yang salah satu interface/linknya mengarah ke jaringan yang menggunakan routing protocol selain OSPF.

Kelebihan :

- Ideal untuk jaringan besar dan kompleks..
- Mendukung penggunaan VLSM dan CIDR, memungkinkan pengalamatan IP yang lebih fleksibel.
- Tidak memiliki batas maksimal jumlah *hop*, berbeda dengan RIP.Merupakan *open standart protocol* sehingga bisa digunakan pada vendor yang berbeda

- Bersifat *open standard*, sehingga dapat digunakan di berbagai perangkat dari vendor yang berbeda.
- Proses *convergence* berlangsung cepat saat terjadi perubahan dalam jaringan.
- Hanya melakukan update ketika terjadi perubahan jaringan
- Mendukung mekanisme autentikasi untuk keamanan pertukaran informasi routing.
- Tidak mengirimkan pembaruan routing secara terus-menerus, melainkan hanya saat ada perubahan topologi.

Kekurangan :

- Membutuhkan sumber daya perangkat yang lebih besar karena menyimpan dan memproses informasi topologi lengkap.
- Perlu perencanaan yang cermat dalam desain dan implementasinya, terutama pada jaringan besar dengan banyak area.

4. BGP

Border Gateway Protocol atau BGP adalah protokol *routing* untuk mengarahkan lalu lintas data antara sistem otonom. Fungsi utamanya akan menentukan rute terbaik bagi lalu lintas data berdasarkan informasi topologi jaringan dan kebijakan *routing*.

Dalam jaringan internet global, protokol ini memainkan peran kunci dalam mengarahkan lalu lintas data dari satu titik ke titik lainnya. Hasilnya, data dapat sampai ke tujuan dengan lebih cepat dan aman.

Pada dasarnya, cara kerja *Border Gateway Protocol* dimulai dengan pertukaran informasi *routing* di antara *router* dalam sistem otonom yang berbeda. *Router* BGP akan bertukar pesan dengan *router* tetangga untuk menyampaikan informasi tentang jaringan yang mereka kenal.

Setiap *router* akan mempertimbangkan berbagai faktor seperti jarak fisik, kecepatan, dan keandalan koneksi saat memilih rute terbaik untuk

mengirimkan data. *Router* akan menggunakan informasi ini untuk memutuskan rute terbaik untuk mencapai tujuan akhir lalu lintas data.
Karena melalui rute yang paling cepat untuk transmisi data, maka lalu lintas data pun dapat berjalan dengan lebih efisien. Berikut manfaat penggunaan BGP:

a. Menemukan Rute Terbaik

Salah satu manfaat utama BGP adalah kemampuannya untuk menemukan rute terbaik bagi lalu lintas data di jaringan internet. Dengan menggunakan informasi topologi jaringan dan kebijakan *routing*, protokol ini dapat menentukan jalur yang paling efisien untuk mengirimkan data.

b. Melacak Perubahan Jaringan

Manfaat yang kedua adalah untuk melacak perubahan dalam topologi jaringan dan mengambil tindakan yang sesuai. Seperti penjelasan cara kerja *Border Gateway Protocol* sebelumnya, *router* akan secara teratur bertukar pesan dengan *router* tetangga untuk memperbarui informasi *routing* mereka.
Jika terjadi perubahan dalam jaringan, seperti penambahan atau penghapusan jalur, maka BGP akan secara otomatis memperbarui tabel *routing*. Kemudian, lalu lintas data akan diarahkan melalui rute tercepat yang statusnya masih aktif.

c. Mengatur Kebijakan Jaringan

Manfaat ketiga BGP adalah memberikan fleksibilitas kepada administrator jaringan untuk mengatur kebijakan *routing* sesuai dengan kebutuhan bisnis. Anda dapat menentukan preferensi rute, memprioritaskan atau memblokir lalu lintas jaringan tertentu, hingga mengatur jalur cadangan untuk menghindari gangguan.

d. Menambah Lapisan Keamanan

Manfaat yang terakhir adalah untuk menambah lapisan keamanan dalam jaringan internet. Anda dapat mengatur konfigurasi untuk

mengenali dan memblokir lalu lintas yang mencurigakan atau berbahaya, seperti serangan DDoS atau *phishing*.

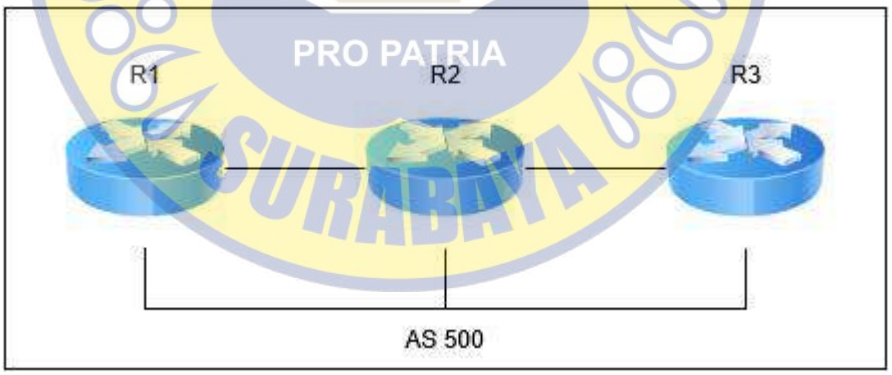
Dengan memantau dan mengatur lalu lintas dengan hati-hati, BGP membantu melindungi jaringan dari serangan siber yang dapat mengganggu operasi bisnis. Data Anda pun menjadi lebih aman berkat rute transmisi yang bebas dari potensi serangan siber.

2.2.2 Jenis Routing BGP

Ada dua jenis utama BGP yang perlu dipahami: eBGP (External Border Gateway Protocol) dan iBGP (Internal Border Gateway Protocol).

1. iBGP

iBGP, di sisi lain, digunakan untuk pertukaran informasi routing dalam AS yang sama. Dalam sebuah AS, ada banyak router yang terhubung satu sama lain dan menjalankan BGP. iBGP memastikan bahwa semua router di AS tersebut memiliki informasi routing yang sama. Dengan demikian, lalu lintas data dapat dikelola secara efisien di dalam AS.



Gambar 2.2 Jenis topologi iBGP

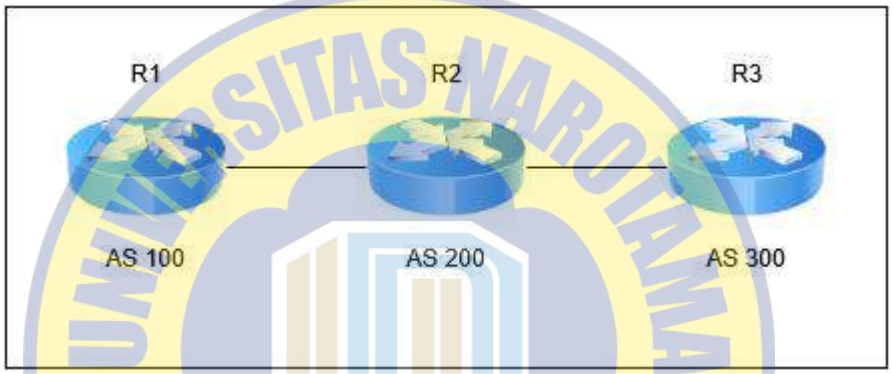
Sumber: Dokumentasi Pribadi

Seperti pada gambar 2.2 menunjukkan topologi jaringan yang terdiri dari tiga router yaitu R1, R2, dan R3 yang tergabung dalam satu Autonomous

System (AS) dengan nomor AS 500. Setiap router saling terhubung secara berurutan, di mana R1 terhubung ke R2, dan R2 terhubung ke R3.

2. eBGP

eBGP digunakan untuk pertukaran informasi routing antara AS yang berbeda. Biasanya, eBGP digunakan oleh penyedia layanan internet (ISP) untuk menghubungkan AS mereka dengan AS lain di internet. Informasi routing yang diterima melalui eBGP dapat digunakan untuk memutuskan jalur terbaik menuju tujuan.

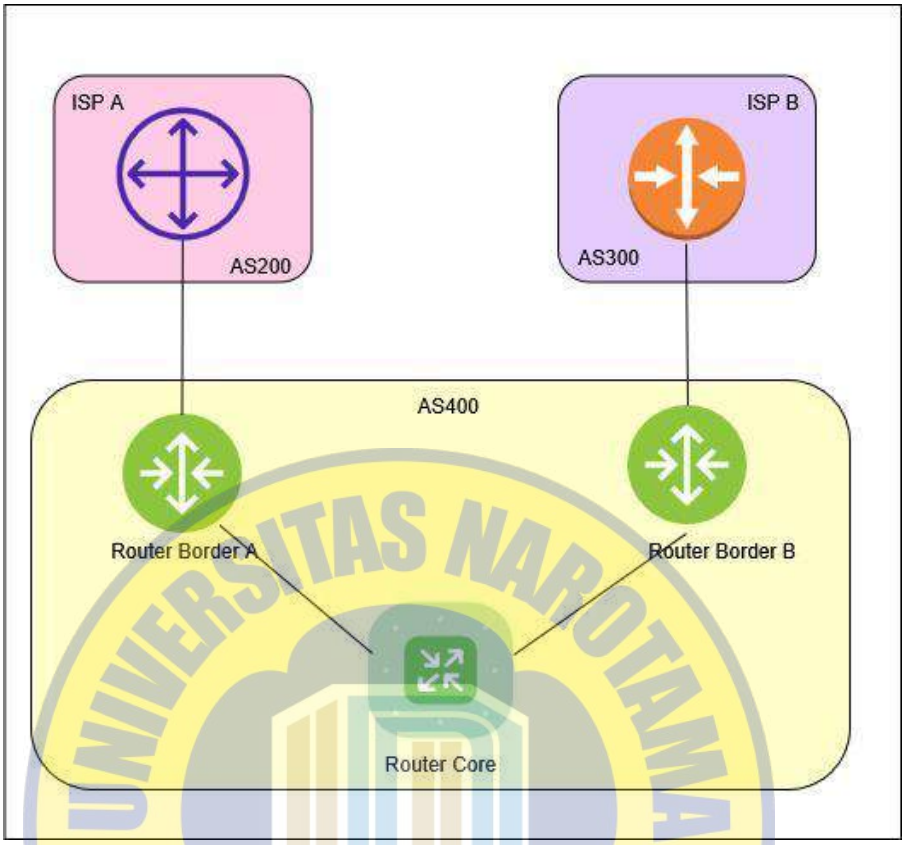


. Gambar 2.3 Jenis topologi eBGP

Sumber : Dokemen Pribadi

Seperti pada gambar 2.3 memperlihatkan sebuah topologi jaringan yang terdiri dari tiga router, masing-masing berada dalam Autonomous System (AS) yang berbeda. Router R1 berada dalam AS 100, R2 dalam AS 200, karena setiap router berada di AS yang berbeda, komunikasi antar router ini memerlukan penggunaan External BGP (eBGP), yaitu protokol routing antar-AS yang umum digunakan di jaringan backbone internet atau antarlembaga besar.

Dalam implementasi di lapangan kedua routing BGP tersebut dapat digunakan bersamaan dengan topologi seperti dibawah ini.



Gambar 2.4 Topologi eBGP dan iBGP

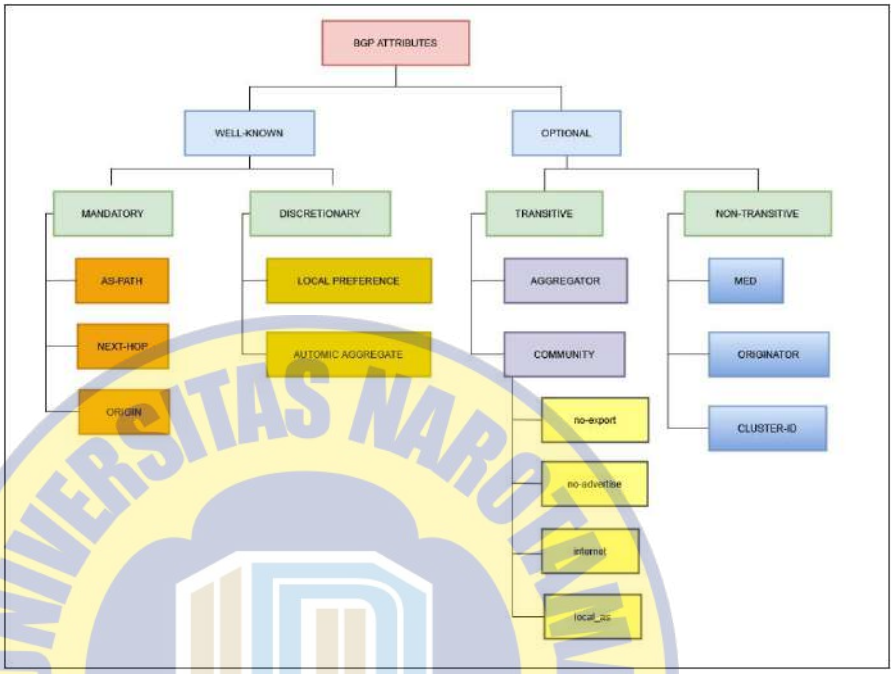
Sumber: Dokumen Pribadi

Dalam Gambar 2.4 kedua jenis routing BGP yaitu eBGP dan iBGP dapat diterapkan dimana biasanya eBGP bertindak untuk routing upstream dan iBGP sebagai routing internal

2.2.2 Atribut BGP

"Atribut BGP Community telah berkembang menjadi alat penting dalam pengelolaan routing antar domain. Dengan menandai rute menggunakan nilai komunitas, operator jaringan dapat menyampaikan informasi kebijakan routing secara efisien kepada mitra BGP mereka. Salah satu inovasi dalam hal ini adalah pengenalan atribut *ACCEPT_OWN*, yang memungkinkan router menerima kembali rute yang sebelumnya ditolak karena berasal dari dirinya sendiri, terutama dalam konteks VPN MPLS. Hal ini meningkatkan fleksibilitas dalam

pengelolaan rute dan mendukung konfigurasi jaringan yang lebih kompleks. John Uttaro, Pradosh Mohapatra, David Smith, 2015).



Gambar 2.5 Jenis BGP Atribut

Sumber: Dokumen Pribadi

Pada Gambar 2.5 tersebut menggambarkan klasifikasi atribut-atribut dalam BGP (Border Gateway Protocol) yang digunakan untuk pengambilan keputusan routing antar Autonomous System (AS). Atribut BGP diklasifikasikan menjadi dua kelompok besar, yaitu Well-Known dan Optional. Atribut Well-Known adalah atribut yang harus dikenali oleh semua router BGP, sedangkan atribut Optional tidak wajib dikenali, dan bisa bervariasi tergantung pada implementasi vendor atau kebijakan jaringan. BGP memiliki sejumlah atribut yang digunakan untuk mengatur dan menginformasikan karakteristik suatu route. Atribut ini dikelompokkan menjadi dua kategori besar: *Well-Known* dan *Optional.*

1. *Well-Known Attributes*

Atribut ini bersifat standar dan dikenali oleh seluruh perangkat jaringan yang mendukung BGP, tanpa memandang merek atau vendor. Well-known attributes dibagi menjadi dua jenis:

a. Mandatory

Jenis ini selalu ada setiap kali sebuah router menjalankan BGP. Contohnya:

1. AS-Path – Menyimpan informasi urutan Autonomous System (AS) yang dilewati oleh sebuah route.
2. Next-Hop – Menunjukkan alamat IP gateway yang digunakan untuk mencapai route tersebut.
3. Origin – Mengindikasikan sumber route, apakah berasal dari BGP secara langsung atau hasil redistribusi dari protokol IGP.

b. Discretionary

Atribut ini hanya akan muncul jika dikonfigurasi secara khusus. Jika tidak diaktifkan, atribut ini tidak akan dibawa dalam proses pertukaran BGP. Contohnya:

1. Local Preference – Menentukan jalur upstream yang diutamakan.
2. Atomic Aggregate – Menandakan bahwa suatu route merupakan hasil summarization (penggabungan prefix).

2. Optional Attributes

Atribut ini tidak selalu ada pada semua perangkat, karena sifatnya tergantung dukungan vendor. Optional attributes terbagi menjadi dua jenis:

a. Transitive

Jika perangkat penerima tidak mengenali atribut ini, atribut tetap diteruskan ke perangkat berikutnya. Contohnya:

- Aggregator – Router yang melakukan summarization.
- Community – Label yang digunakan untuk pengelompokan route, dengan beberapa tipe:
    1. No-Export – Route hanya disebarkan ke internal BGP, tidak keluar ke eBGP.
    2. No-Advertise – Route tidak didistribusikan ke manapun, baik internal maupun eksternal.
    3. Internet – Route dapat diiklankan ke semua peer BGP.

4. Local-AS – Digunakan pada BGP Confederation, route hanya dibagikan dalam sub-AS yang sama.

b. Non-Transitive

Jika perangkat tidak mengenali atribut ini, atribut tersebut akan dibuang (tidak diteruskan). Contohnya:

1. MED (Multi-Exit Discriminator) – Mengarahkan pilihan jalur untuk lalu lintas masuk dari AS tetangga.
2. Originator ID – Menunjukkan router asli yang membuat route dalam skenario Route Reflector.
3. Cluster ID – Identitas cluster dalam konfigurasi Route Reflector. redundant route reflector.

Untuk pemilihan best-path BGP menggunakan urutan attributnya sebagai berikut dengan prioritaskan jalur dengan WEIGHT tertinggi

1. Prioritaskan jalur dengan LOCAL PREFERENCE tertinggi
2. Prioritaskan jalur yang dihasilkan secara lokal melalui perintah *network* atau *redistribute* dibandingkan perintah *aggregate-address*
3. Prioritaskan jalur dengan AS PATH terpendek yang dihasilkan via perintah *network* atau *redistribute* dibandingkan perintah *aggregate-address*
4. Prioritaskan jalur dengan tipe ORIGIN paling rendah (IGP > EGP > Incomplete)
5. Prioritaskan jalur dengan nilai MULTI-EXIT DISCRIMINATOR (MED) terendah
6. Prioritaskan koneksi eBGP dibandingkan iBGP
7. Prioritaskan jalur dengan metrik IGP terendah menuju next-hop BGP
8. Jika kedua jalur bersifat eksternal (eBGP), prioritaskan yang pertama kali diterima
9. Prioritaskan rute yang berasal dari router BGP dengan Router ID terendah
10. Jika originator atau Router ID sama untuk beberapa jalur, prioritaskan dengan panjang cluster list terpendek

11. Prioritaskan jalur yang berasal dari alamat neighbor terendah

2.2.3 Cara Kerja BGP Community

Setiap nilai BGP Community terdiri dari 32 bit, yang umumnya ditulis dalam format ASN:Value, di mana:

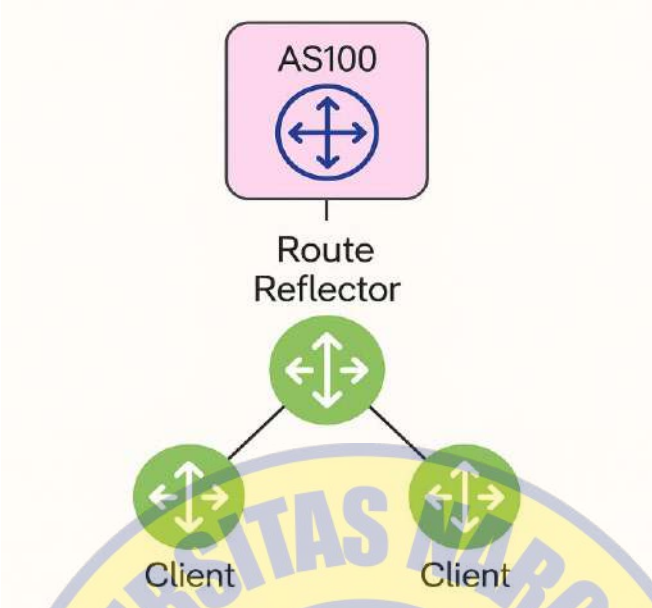
- ASN (Autonomous System Number) adalah nomor sistem otonom yang menetapkan komunitas tersebut.
- Value adalah angka yang menunjukkan tindakan atau kebijakan tertentu yang diinginkan.

Ketika sebuah rute ditandai dengan nilai community tertentu, router penerima dapat menerapkan kebijakan berdasarkan nilai tersebut. Misalnya, sebuah ISP dapat menetapkan bahwa rute dengan community 65000:100 harus diberikan preferensi lokal yang lebih tinggi, atau rute dengan community 65000:200 tidak boleh diumumkan ke peer tertentu.

Atribut ini bersifat transitive, artinya nilai community dapat diteruskan ke AS berikutnya, kecuali jika dikonfigurasi untuk dihapus. Namun, karena tidak semua AS memahami atau menghormati nilai community yang tidak mereka kenal, efektivitasnya bergantung pada kesepakatan dan dokumentasi antara operator jaringan

2.2.4 Route Reflector

Route Reflector (RR) adalah mekanisme dalam protokol BGP (Border Gateway Protocol) yang dirancang untuk mengatasi masalah skalabilitas dalam konfigurasi IBGP (Internal BGP). Dalam topologi IBGP tradisional, setiap router harus membentuk sesi BGP dengan semua router lainnya dalam Autonomous System (AS), yang dikenal sebagai full mesh. Namun, pendekatan ini tidak efisien dan sulit dikelola seiring pertumbuhan jumlah router. Seperti yang terdapat dalam Gambar 2.6 router yang pada AS 100 bertugas sebgai router reflector dan dua router lainnya yang terhubung bertugas sebagai client.



Gambar 2.6 Skema Route Reflector

Sumber: Dokumen Pribadi

Ketika router reflector menerima rute dari salah satu client, ia akan memantulkan (reflect) rute tersebut ke semua Client lainnya dan Non-Client. Sebaliknya, jika router reflector menerima rute dari Non-Client, ia hanya memantulkannya ke semua Client. Dengan demikian, Client tidak perlu membentuk sesi IBGP langsung dengan router lain, cukup dengan router reflector saja.

2.2.5 Autonomous System

Autonomous System (AS) adalah sekumpulan jaringan IP beserta router yang dikelola oleh satu organisasi atau otoritas tunggal, serta menerapkan kebijakan routing yang seragam. Setiap AS memiliki identitas unik berupa Autonomous System Number (ASN) yang digunakan oleh Border Gateway Protocol (BGP) untuk pertukaran informasi routing antar-AS..

Dalam konteks BGP, AS berfungsi sebagai unit administratif yang mengelola routing lalu lintas internet. Router di dalam AS menggunakan protokol routing internal seperti OSPF atau IS-IS untuk menentukan jalur

terbaik dalam AS tersebut. Untuk komunikasi antar AS, BGP digunakan untuk bertukar informasi routing. Setiap AS mengumumkan prefiks IP yang dapat dijangkau melalui jaringan mereka kepada AS tetangga, memungkinkan pembentukan jalur routing global yang efisien. Berikut fungsi Autonomous System dalam Internet Backbone:

1. Routing dan Pengelolaan Jaringan

AS berfungsi mengarahkan data di internet dengan memanfaatkan ASN dan protokol seperti BGP untuk menentukan jalur paling efisien antar-jaringan. Hal ini memastikan perpindahan data dari satu lokasi ke lokasi lain berlangsung tanpa hambatan..

2. Konektivitas dan Interoperabilitas

AS memungkinkan berbagai jaringan saling terhubung dan bertukar data, membentuk infrastruktur internet global yang terintegrasi. Dengan adanya AS, penyedia layanan internet (ISP) maupun penyedia layanan cloud dapat memberikan konektivitas yang stabil dan luas jangkauannya.

3. Kebijakan Routing

Penerapan Kebijakan Routing Setiap AS mengatur kebijakan routing sesuai keputusan operator jaringannya. Kebijakan ini mengatur arah dan pengelolaan lalu lintas data baik di dalam jaringan maupun antar-jaringan, dengan tujuan mengoptimalkan performa, mengelola beban trafik, serta menjaga keamanan.

4. Keamanan dan Kontrol

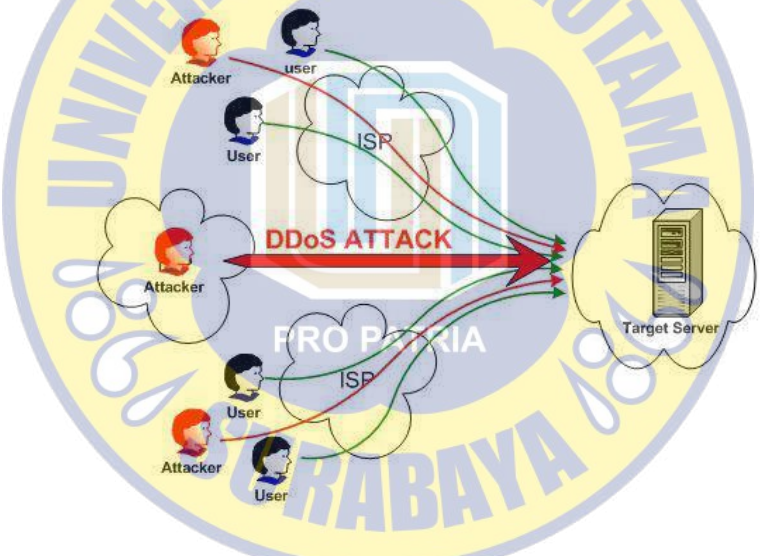
Keamanan dan Pengendalian Jaringan Melalui AS, operator memiliki kendali penuh atas keamanan dan pengaturan arus data. Mereka dapat menerapkan langkah-langkah keamanan khusus serta memantau aktivitas jaringan untuk mencegah ancaman dan serangan, sekaligus memastikan layanan tetap tersedia dengan performa optimal.

.

2.2.6 DDOS

DDoS merupakan singkatan dari *Distributed Denial of Service*, di mana jenis serangan ini berusaha membuat seluruh lalu lintas jaringan internet tidak lagi dapat digunakan. DDoS tidak hanya melumpuhkan *server* tetapi juga sistem sekaligus jaringan internet yang digunakan oleh *user*.

Serangan siber ini berusaha membuat seluruh lalu lintas server lumpuh dengan mengirimkan banyak permintaan (*request*) transaksi data yang besar secara terus-menerus. Semakin besar transaksi data, semakin besar juga dampak kelumpuhan lalu lintas jaringan yang diakibatkan. Jika kapasitas *bandwidth* besar tentu serangan DDoS tidak akan berpengaruh banyak. Tetapi biasanya para *hacker* menggunakan beberapa komputer *host* sekaligus.



Gambar 2.7 ilustrasi serangan ddos volum traffic

Sumber: www.jetorbit.com

Gambar 2.7 di atas menggambarkan serangan Distributed Denial of Service (DDoS) yang mengarah ke sebuah *Target Server*. Berikut penjelasan detailnya:

1. Pelaku (Attacker)
    - Beberapa *attacker* (dilabeli "Attacker") mengirim permintaan palsu secara masif. Mereka biasanya menggunakan *botnet*

(jaringan perangkat terinfeksi malware) untuk melancarkan serangan.

2. Korban (User)
    - Pengguna asli (*User*) yang mencoba mengakses server terhalang karena lalu lintas jaringan dipenuhi oleh permintaan palsu dari *attacker*.
3. Peran ISP (Internet Service Provider)
    - *ISP* (penyedia layanan internet) menjadi titik transit traffic serangan. Tanpa mitigasi, bandwidth ISP akan kewalahan, memengaruhi pengguna lain.
4. Target Server
    - Server tujuan (misal: website/aplikasi) tidak bisa membedakan traffic normal dan serangan. Akibatnya, server *overload*

2.2.7 GNS3

GNS3 (Graphical Network Simulator-3) adalah sebuah aplikasi simulasi jaringan berbasis antarmuka grafis (GUI) yang pertama kali dirilis pada tahun 2008. Aplikasi ini memungkinkan pengguna untuk membuat simulasi perangkat jaringan nyata dengan bantuan emulator maupun teknologi virtualisasi. Salah satu emulator yang digunakan dalam GNS3 adalah Dynamips, yang berfungsi untuk menjalankan IOS milik perangkat Cisco. Di masa lalu, pengguna harus menginstal Dynamips secara manual pada sistem operasi seperti Windows, Linux, FreeBSD, atau MacOS untuk mensimulasikan router Cisco. Namun kini, GNS3 telah mengintegrasikan semua kebutuhan tersebut dalam satu paket lengkap dengan antarmuka grafis yang user-friendly, sehingga jauh lebih praktis dan mudah digunakan.

Manfaat yang bisa kita dapatkan dari GNS3 :

1. Gratis dan Open Source – GNS3 dapat digunakan tanpa biaya dan bersifat open source, yang berarti pengguna bebas memodifikasi dan bahkan turut berkontribusi dalam pengembangan fitur melalui platform

seperti GitHub.Oleh karena itu GNS3 menjadi tools simulasi network yang terfavorit hingga kini. Penggunanya banyak, komunitasnya banyak. Supportnya mudah didapat.

2. Popularitas dan Dukungan Komunitas – Karena bersifat terbuka dan gratis, GNS3 menjadi salah satu simulator jaringan paling populer hingga saat ini, dengan komunitas pengguna yang luas serta dukungan yang mudah ditemukan.
3. Fitur yang Sangat Luas – Jika dibandingkan dengan aplikasi sejenis, GNS3 menawarkan fitur yang sangat beragam dan fleksibel, menjadikannya alat simulasi jaringan yang sangat powerful.

Kemudahan Dalam Penggunaan GNS3

GNS3 bekerja dengan cara menggabungkan berbagai komponen emulator dan virtualisasi untuk membuat lingkungan simulasi jaringan. Meskipun platform ini hanya menyediakan alat untuk menjalankan emulasi atau virtualisasi, konten atau perangkat jaringan seperti router, switch, firewall, dan server perlu disiapkan sendiri oleh pengguna. Beberapa perangkat dasar seperti virtual switch, hub, dan cloud sudah tersedia sebagai bagian dari GNS3, namun peran mereka lebih sebagai pelengkap daripada perangkat utama.

2.2.8 Mikrotik

Mikrotik adalah sistem operasi yang berbasis perangkat lunak (*software*) yang dipergunakan untuk menjadikan komputer sebagai router sebuah jaringan. Sistem operasi (OS) tersebut juga menggunakan sistem operasi berbasis Linux dan menjadi dasar *network router*. OS ini sangat cocok untuk membangun administrasi jaringan komputer yang berskala kecil hingga besar.

Fitur dalam MikroTik

Dalam pengoperasian sistem ini, berbagai fitur yang tersedia pada MikroTik memiliki peranan penting untuk dimanfaatkan. Beberapa di antaranya yaitu:

- **Address List** berfungsi untuk mengelompokkan alamat IP berdasarkan penamaan tertentu.
- **Asynchronous** digunakan sebagai pendukung koneksi serial PPP, baik untuk dial-in maupun dial-out.
- **Bonding** memungkinkan penggabungan beberapa interface ethernet menjadi satu jalur terpadu.
- **Bridge** menyediakan dukungan untuk fungsi spinning tree, multiple bridge interface, serta firewall pada bridge.
- **Data Rate Management** mendukung pengaturan kecepatan data menggunakan metode seperti burst, PCQ, RED, SFQ, FIFO, queue, CIR, MIR, hingga pembatasan koneksi peer-to-peer.
- **Firewall dan NAT** dapat digunakan untuk memfilter koneksi peer-to-peer, menerapkan source NAT, maupun destination NAT.
- **Hotspot** memiliki dukungan untuk pembatasan data, penggunaan SSL, dan protokol HTTPS.
- **M3P** berfungsi pada koneksi wireless maupun ethernet.
- **Proxy** mendukung protokol SOCKS, parent proxy, dan DNS statis.
- **WinBox** adalah aplikasi yang digunakan untuk melakukan konfigurasi dan mengelola sistem MikroTik dari jarak jauh.
- **Routing** menyediakan opsi routing statis maupun dinamis.

2.3 Profil Institusi

Gambar 2.6 Kantor Dinas Kominfo Jatim

Sumber: Diskominfo Jatim

Kantor Dinas Komunikasi dan Informatika Provinsi Jawa Timur yang beralamat di Jl. Ahmad Yani No. 242-244 Surabayan memiliki 4 Lantai dengan terdapat aula yang sering digunakan unutk pertemuan antar Dinas ataupun rapat besar, kondisi gedung kantor seperti pada gambar 2.6.

1. Nama Organisasi

   Dinas Komunikasi dan Informatika Provinsi Jawa Timur

2. Visi dan Misi

   Visi : Mewujudkan Jawa Timur sebagai provinsi yang maju dan sejahtera melalui penerapan teknologi informasi dan komunikasi yang inovatif, efektif, dan efisien.

   a. Meningkatkan akses dan kualitas layanan informasi publik.

b. Mengembangkan infrastruktur teknologi informasi dan komunikasi yang handal.
c. Mendorong partisipasi masyarakat dalam pembangunan melalui pemanfaatan teknologi informasi.
d. Meningkatkan kapasitas sumber daya manusia di bidang komunikasi dan informatika.
e. Mengembangkan sistem pemerintahan berbasis elektronik untuk mendukung tata kelola pemerintahan yang baik.

3. Tugas Pokok dan Fungsi

Tugas Pokok: Melaksanakan urusan pemerintahan daerah di bidang komunikasi dan informatika, statistik, serta persandian sesuai dengan ketentuan peraturan perundang-undangan.

Fungsi:

a. Perumusan kebijakan teknis di bidang komunikasi, informatika, statistik, dan persandian.
b. Pelaksanaan kebijakan di bidang komunikasi, informatika, statistik, dan persandian.
c. Penyusunan rencana strategis dan operasional di bidang komunikasi dan informatika
d. Pengelolaan infrastruktur teknologi informasi dan komunikasi pemerintah daerah.
e. Pengelolaan sistem informasi dan layanan informasi publik.
f. Pembinaan dan pengawasan terhadap pelaksanaan tugas di bidang komunikasi dan informatika di tingkat kabupaten/kota.

4. Nama Organisasi

Dinas Komunikasi dan Informatika Provinsi Jawa Timur terdiri dari beberapa bidang yang masing-masing dipimpin oleh kepala bidang, yaitu:

a. Bidang Informasi Komunikasi Publik : Bertanggung jawab atas pengelolaan informasi publik dan media komunikasi.
b. Bidang Aplikasi Informatika: Mengelola pembangunan dan

pemeliharaan infrastruktur teknologi informasi.

c. Bidang Statistik: Mengelola data dan statistik yang diperlukan untuk perencanaan pembangunan.
d. Bidang Persandian dan Keamanan Informasi: Mengelola keamanan informasi dan persandian untuk melindungi data pemerintah.

5. Program Kerja dan Kegiatan

Beberapa program dan kegiatan utama yang dilaksanakan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur meliputi:

a. Pengembangan E-Govt:
b. Peningkatan Literasi Digital: Program pelatihan dan sosialisasi untuk meningkatkan literasi digital masyarakat.
c. Penyediaan Layanan Informasi Publik: Mengelola portal informasi publik dan layanan pengaduan masyarakat.
d. Penguatan Infrastruktur TIK: Pembangunan dan pemeliharaan jaringan komunikasi dan data untuk mendukung operasional pemerintahan.
e. Keamanan Informasi dan Persandian: Implementasi sistem keamanan informasi untuk melindungi data pemerintah dari ancaman siber.

6. Alamat dan Kontak

Alamat Kantor: Jl. Ahmad Yani No.242-244, Gayungan, Kota Surabaya, Jawa Timur 60235, Indonesia.

7. Komitmen Terhadap Inovasi dan Pelayanan

Dinas Komunikasi dan Informatika Provinsi Jawa Timur berkomitmen untuk terus berinovasi dalam memberikan layanan terbaik kepada masyarakat. Dengan memanfaatkan teknologi

informasi yang maju, dinas ini bertujuan untuk menciptakan pemerintahan yang lebih terbuka, responsif, dan akuntabel.