# ANALISIS KETAHANAN BGP DAN EIGRP TERHADAP ROUTE INJECTION DENGAN MITIGASI BASIC FILTERING MENGGUNAKAN PREFIX-LIST

## SKRIPSI

**Sahrul Apriandi 2207421012**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

**2026**

# ANALISIS KETAHANAN BGP DAN EIGRP TERHADAP ROUTE INJECTION DENGAN MITIGASI BASIC FILTERING MENGGUNAKAN PREFIX-LIST

# SKRIPSI

**Dibuat untuk Melengkapi Syarat – Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik**

**Sahrul Apriandi**

**2207421012**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

**2026**

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : Sahrul Apriandi |
| NIM | : 2207421012 |
| Jurusan/Program Studi | : Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan |
| Judul Skripsi | : Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list* |

Menyatakan dengan sebenarnya bahwa skripsi ini benar – benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri – ciri plagiat dan bentuk – bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok,

Yang membuat pernyataan

Sahrul Apriandi

NIM. 2207421012

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## LEMBAR PENGESAHAN

Skripsi diajukan oleh:

| | |
|---|---|
| Nama | : Sahrul Apriandi |
| NIM | : 2207421012 |
| Program Studi | : Teknik Multimedia dan Jaringan |
| Judul Skripsi | : Analisis Ketahanan BGP dan EIGRP terhadap Route Injection dengan Mitigasi Basic Filtering Menggunakan Prefix-list |

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 1, Bulan Juli, Tahun 2026 dan dinyatakan **LULUS**.

**Disahkan oleh:**

| | | |
|---|---|---|
| Pembimbing I | Defiana Arnaldy, S.Tp., M.Si.. | ( ) |
| Penguji I | Asep Kurniawan, S.Pd., M.Kom. | ( ) |
| Penguji II | Fachroni Arbi Murad, S.Kom., M.Kom. | ( ) |
| Penguji III | Iik Muhamad Malik Matin, S.Kom., M.T. | ( ) |

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas rahmat, karunia, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list*". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Diploma Empat pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta.

Dalam penyusunan skripsi ini, penulis menyadari bahwa selesainya skripsi ini tidak terlepas dari doa, dukungan, arahan, dan bantuan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT yang telah memberikan rahmat, kesehatan, kekuatan, dan kelancaran kepada penulis dalam menyelesaikan skripsi ini.
2. Bapak Defiana Arnaldy, S.Tp., M.Si., selaku dosen pembimbing yang telah memberikan arahan, bimbingan, masukan, serta waktu selama proses penyusunan skripsi ini.
3. Seluruh dosen dan staf Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta yang telah memberikan ilmu, bantuan, dan pelayanan akademik selama masa perkuliahan.
4. Almarhumah Ibu tercinta yang telah lebih dahulu tenang di sisi Allah SWT, atas kasih sayang, doa, dan pengorbanan yang menjadi kekuatan bagi penulis dalam menjalani proses pendidikan hingga tahap ini.
5. Ayah tercinta yang selalu berjuang, memberikan doa, dukungan, semangat, serta pengorbanan yang besar kepada penulis selama masa perkuliahan hingga penyusunan skripsi ini.
6. Saudara, om, dan tante yang telah memberikan doa, dukungan, motivasi, serta bantuan kepada penulis selama proses perkuliahan dan penyusunan skripsi.

7. Rekan-rekan Program Studi Teknik Multimedia dan Jaringan yang telah memberikan bantuan, dukungan, serta semangat selama masa perkuliahan hingga selesainya skripsi ini.
8. Syifa Chandra, Alvito, Jibran, Salsabila, Indah Dwi, Shabrina, Wibi, Abdan, Rizki dan Audi yang telah memberikan dukungan, semangat, bantuan, serta menjadi tempat berbagi cerita selama proses perkuliahan hingga penyusunan skripsi ini.
9. Seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah membantu dan memberikan dukungan kepada penulis dalam menyelesaikan skripsi ini.

Akhir kata, penulis berharap Allah SWT membalas segala kebaikan semua pihak yang telah membantu. Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan, sehingga kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca serta menjadi referensi dalam bidang keamanan *routing* dan jaringan komputer.

Depok, 9 Juni 2026

Sahrul Apriandi

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : Sahrul Apriandi |
| NIM | : 2207421012 |
| Jurusan/Program Studi | : Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan |

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

**Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok,

Yang menyatakan

Sahrul Apriandi

NIM. 2207421012

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

**Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list***

## ABSTRAK

*Keamanan routing merupakan aspek penting dalam menjaga stabilitas jaringan karena manipulasi informasi rute dapat menyebabkan perubahan jalur trafik dan gangguan konektivitas. Penelitian ini bertujuan menganalisis ketahanan Border Gateway Protocol (BGP) dan Enhanced Interior Gateway Routing Protocol (EIGRP) terhadap route injection, serta mengevaluasi efektivitas basic filtering menggunakan prefix-list sebagai mitigasi. Pengujian dilakukan pada simulasi Graphical Network Simulator 3 (GNS3) dengan tiga skenario, yaitu baseline, route injection, dan setelah mitigasi. Skenario route injection dilakukan oleh R4-ATTACKER dengan memasukkan rute tidak sah berupa prefix host /32 menuju PC1, PC2, dan PC3, yaitu 192.168.16.2/32, 192.168.17.2/32, dan 192.168.18.2/32. Pada BGP, rute tidak sah masuk sebagai prefix yang diiklankan oleh R4-ATTACKER, sedangkan pada EIGRP rute tidak sah masuk sebagai rute eksternal dengan kode D EX. Evaluasi dilakukan berdasarkan routing table, next-hop, ping, traceroute, Wireshark, waktu pemulihan, delay, throughput, dan packet loss. Hasil pengujian menunjukkan bahwa saat route injection, nilai packet loss rata-rata meningkat menjadi 66,67% pada BGP dan EIGRP. Nilai throughput BGP menurun dari 1,440 Kbps pada kondisi baseline menjadi 0,957 Kbps saat route injection, sedangkan EIGRP menurun dari 1,498 Kbps menjadi 0,967 Kbps. Setelah mitigasi diterapkan, rute tidak sah berhasil ditolak, packet loss kembali menjadi 0%, dan throughput meningkat menjadi 1,477 Kbps pada BGP serta 1,468 Kbps pada EIGRP. Dengan demikian, basic filtering menggunakan prefix-list efektif dalam membatasi dampak route injection pada BGP dan EIGRP.*

**Kata kunci:** basic filtering, BGP, EIGRP, prefix-list, Quality of Service, route injection.

POLITEKNIK NEGERI JAKARTA

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME ..... ii
LEMBAR PENGESAHAN ..... iii
KATA PENGANTAR ..... iv
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS ..... vi
ABSTRAK ..... vii
DAFTAR ISI ..... viii
DAFTAR TABEL ..... x
DAFTAR GAMBAR ..... xi
BAB I ..... 1
PENDAHULUAN ..... 1
1.1 Latar Belakang ..... 1
1.2 Perumusan Masalah ..... 4
1.3 Batasan Masalah ..... 5
1.4 Tujuan dan Manfaat ..... 7
1.5 Sistematika Penulisan ..... 8
BAB II ..... 9
TINJAUAN PUSTAKA ..... 9
2.1 Penelitian Terkait ..... 9
2.2 Konsep *Routing* dan *Control Plane* ..... 11
2.3 *Border Gateway Protocol* (BGP) dan *Autonomous System* ..... 12
2.4 *Enhanced Interior Gateway Routing Protocol* (EIGRP) ..... 13
2.5 *Route Injection* ..... 13
2.6 Mitigasi Basic Filtering Menggunakan Prefix-list ..... 14
2.7 Parameter Evaluasi dan *Quality of Service* (QoS) ..... 14
2.8 GNS3 ..... 17
2.9 Wireshark ..... 17
BAB III ..... 19
METODE PENELITIAN ..... 19
3.1 Rancangan Penelitian ..... 19
3.2 Tahapan Penelitian ..... 21
3.3 Objek Penelitian ..... 25
BAB IV ..... 27

HASIL DAN PEMBAHASAN ..... 27
4.1 Analisis Kebutuhan ..... 27
4.2 Perancangan Sistem ..... 29
4.2.1 Perancangan Topologi BGP ..... 30
4.2.2 Perancangan Topologi EIGRP ..... 32
4.2.3 Perancangan Pengalamatan IP ..... 34
4.2.4 Perancangan Mekanisme Route Injection ..... 36
4.2.5 Perancangan Mekanisme Mitigasi ..... 37
4.2.6 Perancangan Skenario Pengujian ..... 37
4.3 Implementasi Sistem ..... 39
4.3.1 Implementasi *Routing* BGP ..... 39
4.3.2 Implementasi *Routing EIGRP* ..... 43
4.3.3 Verifikasi Konektivitas Jaringan ..... 47
4.4 Pengujian ..... 50
4.4.1 Deskripsi Pengujian ..... 51
4.4.2 Prosedur Pengujian ..... 52
4.4.3 Data Hasil Pengujian ..... 54
4.4.4 Analisis Data / Evaluasi Pengujian ..... 85
BAB V ..... 107
PENUTUP ..... 107
5.1 Simpulan ..... 107
5.2 Saran ..... 108
DAFTAR PUSTAKA ..... 109
DAFTAR RIWAYAT HIDUP ..... 112
LAMPIRAN ..... 113

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## DAFTAR TABEL

Tabel 2.1 Penelitian Terkait ..... 9
Tabel 2. 2 Indeks Delay berdasarkan standar *TIPHON*..... 16
Tabel 2.3 Indeks *Packet loss* berdasarkan standar *TIPHON*..... 17
Tabel 4.1 Analisis Kebutuhan..... 27
Tabel 4.2 Kebutuhan Perangkat Penelitian..... 28
Tabel 4.3 Pembagian Autonomous System pada Topologi BGP..... 32
Tabel 4.4 Pembagian Router pada Topologi EIGRP ..... 34
Tabel 4.5 Pengalamatan IP..... 35
Tabel 4.6 Skenario Pengujian..... 38
Tabel 4.7 Hasil Pengujian QoS Baseline pada Topologi BGP ..... 57
Tabel 4.8 Hasil Pengujian QoS Baseline pada Topologi EIGRP ..... 59
Tabel 4.9 Target Route Injection ..... 60
Tabel 4.10 Hasil Pengujian QoS Saat Route Injection pada Topologi BGP ..... 65
Tabel 4.11 Hasil Pengujian QoS Saat Route Injection pada Topologi EIGRP..... 70
Tabel 4.12 Hasil Pengujian QoS Setelah Mitigasi pada Topologi BGP..... 76
Tabel 4.13 Hasil Pengujian QoS Setelah Mitigasi pada Topologi EIGRP ..... 80
Tabel 4.14 Hasil Pengujian QoS pada Topologi BGP ..... 88
Tabel 4.15 Hasil Pengujian QoS Saat Route Injection pada Topologi BGP ..... 88
Tabel 4.16 Hasil Pengujian QoS Setelah Mitigasi pada Topologi BGP..... 91
Tabel 4.17 Hasil Pengujian QoS Baseline pada Topologi EIGRP..... 93
Tabel 4.18 Hasil Pengujian QoS Saat *Route Injection* pada Topologi EIGRP..... 94
Tabel 4.19 Hasil Pengujian Waktu Konvergensi dan Pemulihan ..... 96
Tabel 4.20 Rekapitulasi Perbandingan Rata-rata QoS BGP dan EIGRP ..... 99
Tabel 4.21 Hasil Pengujian Waktu Serangan Masuk dan Pemulihan .....103
Tabel 4.22 Perbandingan Hasil Pengamatan GNS3 dan Wireshark .....105

POLITEKNIK NEGERI JAKARTA

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# DAFTAR GAMBAR

Gambar 3.1 Tahapan Penelitian ..... 21
Gambar 4.1 Topologi BGP pada GNS3 ..... 31
Gambar 4.2 Topologi EIGRP pada GNS3 ..... 33
Gambar 4.3 Hasil Verifikasi Neighbor BGP pada R1-KOMINFO ..... 42
Gambar 4.4 Verifikasi Neighbor EIGRP pada Router R1-KOMINFO ..... 46
Gambar 4.5 Pengujian Konektivitas pada Kondisi Baseline ..... 49
Gambar 4.6 Hasil Pengujian Ping Baseline pada Topologi BGP ..... 56
Gambar 4.7 Capture ICMP Baseline pada Topologi BGP ..... 56
Gambar 4.8 Hasil Pengujian Ping Baseline pada Topologi EIGRP ..... 58
Gambar 4.9 Capture ICMP Baseline pada Topologi EIGRP ..... 58
Gambar 4.10 Konfigurasi *Route Injection* pada R4-ATTACKER ..... 61
Gambar 4.11 Hasil Verifikasi Route Injection BGP Target PC1 ..... 62
Gambar 4.12 Hasil Verifikasi Route Injection BGP Target PC2 ..... 62
Gambar 4.13 Hasil Verifikasi Route Injection BGP Target PC3 ..... 62
Gambar 4.14 Hasil Pengujian *Ping* Saat *Route Injection* pada Topologi BGP .... 63
Gambar 4.15 Capture ICMP Saat Route Injection pada Topologi BGP ..... 64
Gambar 4.16 Konfigurasi *Route Injection* EIGRP pada R4-ATTACKER ..... 67
Gambar 4.17 Hasil Verifikasi Route Injection EIGRP Target PC1 ..... 67
Gambar 4.18 Hasil Verifikasi *Route Injection* EIGRP Target PC2 ..... 68
Gambar 4.19 Hasil Verifikasi Route Injection EIGRP Target PC3 ..... 68
Gambar 4.20 Hasil Pengujian *Ping* Saat *Route Injection* pada Topologi EIGRP . 69
Gambar 4.21 *Capture* ICMP Saat *Route Injection* pada Topologi EIGRP ..... 70
Gambar 4.22 Konfigurasi *Basic Filtering* BGP pada Router R1-KOMINFO ..... 73
Gambar 4.23 Tabel BGP R1-KOMINFO Setelah Mitigasi BGP ..... 73
Gambar 4.24 *Routing Table* R1-KOMINFO Setelah Mitigasi BGP ..... 74
Gambar 4.25 Pemulihan Konektivitas Setelah Mitigasi BGP ..... 75
Gambar 4.26 *Capture* ICMP Setelah Mitigasi BGP ..... 75
Gambar 4.27 Konfigurasi *Basic Filtering* EIGRP pada Router R1-KOMINFO .. 77
Gambar 4.28 *Routing Table* R1-KOMINFO Setelah Mitigasi EIGRP ..... 78
Gambar 4.29 Pemulihan Konektivitas Setelah Mitigasi EIGRP ..... 79
Gambar 4.30 *Capture* ICMP Setelah Mitigasi EIGRP ..... 80
Gambar 4.31 Hasil *Traceroute* pada Topologi BGP ..... 82
Gambar 4.32 Hasil *Traceroute* pada Topologi EIGRP ..... 84
Gambar 4.33 Grafik Perbandingan Packet Loss BGP dan EIGRP ..... 101
Gambar 4.34 Grafik Perbandingan Delay BGP dan EIGRP ..... 102
Gambar 4.35 Grafik Perbandingan Throughput BGP dan EIGRP ..... 102
Gambar 4.36 Grafik Perbandingan Waktu Serangan Masuk dan Pemulihan ..... 104

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah meningkatkan ketergantungan masyarakat terhadap jaringan komputer dan Internet dalam berbagai aktivitas. Jaringan komputer tidak hanya digunakan untuk pertukaran data, tetapi juga menjadi infrastruktur utama dalam mendukung layanan digital, komunikasi, dan operasional organisasi. (Kabir et al., 2021) menjelaskan bahwa komunikasi berbasis Internet telah menjadi bagian penting dalam kehidupan sehari-hari, sedangkan protokol *routing* berperan dalam menentukan jalur pengiriman data dari sumber menuju tujuan. Oleh karena itu, keandalan protokol *routing* menjadi faktor penting dalam menjaga ketersediaan dan kualitas layanan jaringan.

Dalam jaringan komputer, protokol *routing* digunakan untuk membangun dan memperbarui informasi rute agar paket data dapat dikirim melalui jalur yang sesuai. Protokol *routing* dinamis seperti *Border Gateway Protocol* (BGP) dan *Enhanced Interior Gateway Routing Protocol* (EIGRP) memungkinkan router bertukar informasi *routing* secara otomatis ketika terjadi perubahan kondisi jaringan. BGP banyak digunakan pada jaringan antar-*Autonomous System*, sedangkan EIGRP digunakan pada jaringan internal atau *enterprise*. Meskipun kedua protokol tersebut memiliki karakteristik berbeda, keduanya sama – sama bergantung pada validitas informasi *routing* yang diterima router dalam proses pemilihan jalur.

Keamanan *routing* menjadi penting karena kesalahan atau manipulasi informasi rute dapat menyebabkan router memilih jalur yang tidak semestinya. (OECD, 2022) menjelaskan bahwa sistem *routing* Internet masih menghadapi berbagai insiden seperti *route leak* dan *route hijacking* yang dapat mengganggu ketersediaan layanan serta mengalihkan trafik ke jalur yang tidak diinginkan. Pada BGP, salah satu serangan yang sering dibahas adalah *prefix hijacking*, yaitu kondisi ketika suatu *Autonomous System* mengiklankan prefix yang bukan miliknya. (Sermpezis et al., 2021)

menyatakan bahwa BGP prefix hijacking merupakan ancaman serius terhadap ketahanan dan keamanan komunikasi Internet karena dapat memengaruhi ketersediaan dan kerahasiaan komunikasi.

Insiden keamanan *routing* juga masih terjadi hingga saat ini. MANRS mencatat bahwa insiden *routing* seperti *route leak, route hijack*, dan IP *spoofing* dapat menyebabkan layanan Internet melambat, tidak dapat dijangkau, atau trafik dialihkan melalui jaringan yang tidak semestinya (Siddiqui, 2022). Selain itu (Labs, 2025) menjelaskan bahwa BGP *hijacking* masih menjadi ancaman karena BGP tidak memiliki mekanisme autentikasi bawaan yang kuat, sementara penerapan mekanisme keamanan seperti RPKI dan *Route Origin Validation* belum merata. Kondisi tersebut menunjukkan bahwa isu keamanan *routing* masih relevan untuk diteliti, khususnya pada skenario manipulasi informasi *routing*.

Selain BGP, jaringan internal yang menggunakan EIGRP juga perlu diperhatikan dari sisi ketahanan *routing*. EIGRP dikenal sebagai protokol *routing* dinamis yang mampu menentukan jalur terbaik dan beradaptasi terhadap perubahan topologi jaringan. (Kabir et al., 2021) menggunakan EIGRP sebagai salah satu protokol yang dianalisis berdasarkan *latency, throughput*, dan *convergence time* pada jaringan *enterprise* (Antoni Musril et al., 2021) juga menunjukkan bahwa EIGRP dapat diterapkan pada jaringan kampus dengan pengukuran *Quality of Service* (QoS) seperti *throughput, packet loss, latency,* dan *jitter*. Namun, kemampuan EIGRP dalam memilih rute dan melakukan konvergensi tidak berarti protokol tersebut bebas dari risiko manipulasi informasi *routing*, terutama apabila terdapat route injection atau informasi rute yang tidak sah masuk ke domain *routing* internal.

Dampak dari manipulasi informasi *routing* tidak hanya terlihat pada perubahan jalur, tetapi juga dapat memengaruhi kualitas layanan jaringan. Ketika router memilih rute yang salah atau tidak valid, paket data dapat mengalami gangguan berupa peningkatan *delay*, penurunan *throughput,*



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

atau *packet loss*. (Antoni Musril et al., 2021) menjelaskan bahwa QoS digunakan untuk mengukur kemampuan jaringan dalam memberikan layanan. (Nisa et al., 2024) juga menjelaskan bahwa pengujian QoS dapat dilakukan menggunakan parameter *throughput, delay, jitter*, dan *packet loss* untuk mengetahui kualitas kinerja jaringan. Dengan demikian, QoS dapat digunakan sebagai indikator untuk menilai dampak serangan *routing* dan efektivitas mitigasi yang diterapkan.

Berbagai mekanisme keamanan telah dikembangkan untuk mengurangi risiko manipulasi informasi *routing*, seperti *Internet Routing Registry* (IRR), *Resource Public Key Infrastructure* (RPKI), *Route Origin Validation* (ROV), dan BGPsec. Namun, (OECD, 2022) menjelaskan bahwa belum ada satu mekanisme yang dapat menyelesaikan seluruh permasalahan keamanan *routing* secara menyeluruh. Selain itu, beberapa mekanisme keamanan membutuhkan penerapan yang lebih kompleks dan belum selalu mudah diterapkan secara merata pada jaringan operasional. Oleh karena itu, mekanisme yang lebih sederhana dan mudah dikonfigurasi seperti *basic filtering* masih relevan untuk diuji sebagai langkah mitigasi.

*Basic filtering* dapat diterapkan dengan mengendalikan informasi *routing* yang masuk maupun keluar dari router. (McDaniel et al., 2021) menunjukkan bahwa mekanisme filtering dapat membatasi propagasi *route leak* secara signifikan pada BGP. Sementara itu, *distribute-list* dan *prefix-list* dapat digunakan untuk mengontrol *routing* update pada protokol *routing* dinamis agar informasi rute yang diterima atau diiklankan menjadi lebih terkontrol (Global, 2023). Dengan demikian, *basic filtering* menjadi mekanisme mitigasi yang praktis karena dapat diterapkan melalui konfigurasi router tanpa membutuhkan infrastruktur keamanan tambahan yang kompleks.

Berdasarkan penelitian sebelumnya, (Eko Kurniawanto, 2021) telah membahas implementasi BGP pada jaringan MAN dan melakukan pengujian kualitas layanan menggunakan parameter QoS. Namun,

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

penelitian tersebut belum membahas aspek keamanan *routing*, skenario serangan, mitigasi, maupun perbandingan dengan protokol EIGRP. Di sisi lain, penelitian terkait EIGRP seperti (Kabir et al., 2021) dan (Antoni Musril et al., 2021) lebih banyak berfokus pada performa *routing* dan QoS, bukan pada pengujian ketahanan terhadap manipulasi informasi *routing*. Oleh karena itu, masih diperlukan penelitian yang menguji dan membandingkan ketahanan BGP dan EIGRP terhadap manipulasi informasi *routing* serta mengevaluasi efektivitas *basic filtering* sebagai mekanisme mitigasi.

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk menganalisis perbandingan ketahanan protokol BGP dan EIGRP terhadap manipulasi informasi *routing*, dengan skenario route injection pada BGP dan EIGRP. Penelitian ini juga mengevaluasi efektivitas *basic filtering* dalam memitigasi serangan berdasarkan parameter QoS berupa *throughput, delay,* dan *packet loss*. Hasil penelitian diharapkan dapat memberikan bukti empiris mengenai dampak manipulasi *routing* terhadap kualitas layanan jaringan serta menjadi referensi bagi administrator jaringan dalam menerapkan mekanisme keamanan *routing* yang sederhana dan mudah diimplementasikan.

## 1.2 Perumusan Masalah

Berdasarkan latar belakang, masih terdapat sejumlah persoalan terkait kerentanan pertukaran informasi *routing* terhadap manipulasi *route advertisement*, khususnya melalui *route injection* pada BGP dan EIGRP. Selain itu, diperlukan evaluasi terhadap mekanisme mitigasi yang lebih ringan dan realistis seperti *basic filtering* pada protokol BGP dan EIGRP di lingkungan simulasi GNS3. Oleh karena itu, permasalahan dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana karakteristik *routing* dan *Quality of Service* (QoS) pada protokol BGP dan EIGRP dalam kondisi *baseline* sebelum terjadi manipulasi informasi *routing*?

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2. Bagaimana dampak *route injection* terhadap *routing* table, pemilihan jalur komunikasi, waktu konvergensi atau pemulihan, *delay, throughput*, dan *packet loss* pada protokol BGP dan EIGRP?
3. Bagaimana penerapan *basic filtering* berbasis *prefix-list* dalam menolak rute tidak sah yang berasal dari *router attacker* pada protokol BGP dan EIGRP?
4. Bagaimana efektivitas *basic filtering* dalam memitigasi manipulasi informasi *routing* pada BGP dan EIGRP berdasarkan perubahan *routing* table, konektivitas, dan parameter QoS?

## 1.3 Batasan Masalah

Berdasarkan latar belakang dan perumusan masalah yang telah diuraikan, ruang lingkup penelitian ini perlu dibatasi agar pembahasan lebih terarah dan tidak meluas ke aspek keamanan jaringan di luar fokus penelitian. Oleh karena itu, batasan masalah dalam penelitian ini dirumuskan sebagai berikut:

1. Penelitian ini dilakukan menggunakan simulasi jaringan pada GNS3, sehingga hasil pengujian merepresentasikan kondisi pada lingkungan simulasi dan tidak dimaksudkan sebagai representasi langsung jaringan produksi.
2. Protokol *routing* yang dianalisis dibatasi pada *Border Gateway Protocol* (BGP) dan *Enhanced Interior Gateway Routing Protocol* (EIGRP) dengan satu topologi fisik yang sama. Topologi penelitian terdiri dari PC-ATTACKER sebagai representasi sumber serangan dari Internet, R1-KOMINFO sebagai router utama dan *gateway* menuju Internet, R2-CAPIL, R3-SANGIR, R4-ATTACKER sebagai *compromised router, switch backbone*, serta tiga client pengujian yaitu PC1, PC2, dan PC3.
3. Skenario serangan dibatasi pada route injection, yaitu penyisipan route atau prefix tidak sah ke dalam proses *routing*. Pada BGP, *route injection* dilakukan melalui pengiklanan prefix tidak sah dari *router*

*attacker*, sedangkan pada EIGRP dilakukan melalui *static route* palsu yang di-*redistribute* ke proses EIGRP.

4. Penelitian ini tidak membahas proses eksploitasi, teknik peretasan, pencurian kredensial, maupun proses attacker memperoleh akses administratif ke router. Dalam penelitian ini, PC-ATTACKER ditempatkan pada sisi Internet sebagai representasi sumber serangan eksternal dan diasumsikan telah berhasil memperoleh akses kendali terhadap R4-ATTACKER. Router R4-ATTACKER kemudian berperan sebagai *compromised router* yang digunakan untuk melakukan *route injection*.
5. Mitigasi yang digunakan dibatasi pada *basic filtering* berbasis *prefix-list* untuk menolak *prefix* atau route tidak sah yang berasal dari *router attacker*. Pada BGP, *filtering* diterapkan pada router penerima *update* dari *neighbor attacker*, sedangkan pada EIGRP *filtering* diterapkan pada *router legitimate* yang menerima *update route* dari *attacker* dalam domain EIGRP.
6. Parameter pengujian dibatasi pada perubahan *routing table*, *next-hop* atau jalur terpilih, waktu konvergensi atau pemulihan, serta parameter *Quality of Service* (QoS) yang meliputi *delay, throughput*, dan *packet loss. Traffic* pengujian menggunakan ICMP ping dan dianalisis melalui hasil terminal serta capture Wireshark. Pengujian dilakukan terhadap tiga host tujuan, yaitu PC1 dengan alamat 192.168.16.2, PC2 dengan alamat 192.168.17.2, dan PC3 dengan alamat 192.168.18.2 pada kondisi *baseline, route injection*, dan setelah mitigasi.
7. Penelitian ini tidak membahas serangan data plane seperti ARP *spoofing, sniffing, Man-in-the-Middle, firewall bypass*, maupun enkripsi aplikasi, serta tidak membahas mekanisme keamanan *routing* lain seperti RPKI, BGPsec, autentikasi *routing*, *firewall-based access control*, atau *intrusion detection system* karena fokus mitigasi dibatasi pada *basic filtering*.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## 1.4 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang telah disusun, penelitian ini memiliki tujuan yang ingin dicapai serta manfaat yang diharapkan bagi pengembangan ilmu maupun praktik keamanan jaringan, khususnya pada aspek keamanan *routing* atau control plane. Oleh karena itu, pada bagian ini diuraikan tujuan dan manfaat penelitian sebagai berikut.

Tujuan penelitian ini adalah:

1. Menganalisis karakteristik kualitas layanan jaringan pada protokol BGP dan EIGRP pada kondisi normal berdasarkan parameter *throughput, delay,* dan *packet loss.*
2. Menganalisis pengaruh *route injection* terhadap *routing* table, jalur komunikasi, dan kualitas layanan jaringan pada protokol BGP dan EIGRP berdasarkan parameter *throughput, delay*, dan *packet loss*.
3. Membandingkan tingkat ketahanan protokol BGP dan EIGRP terhadap route injection berdasarkan perubahan *routing* table, waktu konvergensi atau pemulihan, *throughput, delay*, dan *packet loss* dari kondisi normal ke kondisi saat serangan.
4. Menganalisis efektivitas penerapan *basic filtering* berbasis *prefix-list* dalam memitigasi *route injection* pada protokol BGP dan EIGRP berdasarkan perubahan *routing* table, waktu pemulihan, *throughput, delay,* dan *packet loss*.

Secara umum, penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Memberikan informasi mengenai karakteristik kualitas layanan jaringan pada protokol BGP dan EIGRP pada kondisi normal maupun saat terjadi *route injection* berdasarkan parameter *throughput, delay*, dan *packet loss*.
2. Menjadi referensi dalam memahami perbedaan tingkat ketahanan protokol BGP dan EIGRP terhadap *route injection*.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

3. Memberikan gambaran mengenai efektivitas penerapan *basic filtering* berbasis *prefix-list* sebagai mekanisme mitigasi terhadap *route injection*.
4. Menjadi referensi bagi administrator jaringan dalam menerapkan mekanisme keamanan dasar untuk membatasi masuknya route atau prefix tidak sah ke dalam *routing* table.
5. Menambah referensi penelitian mengenai keamanan *routing*, khususnya terkait perbandingan ketahanan protokol BGP dan EIGRP terhadap *route injection* serta efektivitas *basic filtering* berdasarkan parameter *Quality of Service* (QoS).

## 1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam penelitian ini, yaitu sebagai berikut:

1. Bab I Pendahuluan
   Bab ini membahas latar belakang penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.
2. Bab II Tinjauan Pustaka
   Bab ini membahas teori yang mendukung penelitian, meliputi *routing*, *control plane*, BGP, EIGRP, *route injection*, *basic filtering*, *Quality of Service* (QoS), serta penelitian terdahulu yang relevan.
3. Bab III Metode Penelitian
   Bab ini menjelaskan rancangan penelitian, tahapan penelitian, objek penelitian, diagram alir sistem, skenario pengujian, serta metode pengambilan dan analisis data yang digunakan dalam penelitian.
4. Bab IV Hasil dan Pembahasan
   Bab ini menyajikan hasil implementasi, pengujian, dan analisis sistem, meliputi mekanisme *routing*, *route injection*, *basic filtering*, perubahan rute, waktu konvergensi, serta pengukuran *Quality of Service* (QoS).
5. Bab V Penutup
   Bab ini berisi kesimpulan penelitian berdasarkan hasil pengujian yang diperoleh serta saran untuk pengembangan penelitian selanjutnya.

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# BAB II
# TINJAUAN PUSTAKA

## 2.1 Penelitian Terkait

Penelitian terkait digunakan sebagai acuan untuk memahami pendekatan dan metode yang telah diterapkan pada penelitian-penelitian sebelumnya yang relevan dengan topik keamanan *routing* (BGP), serangan *Route Injection dan Prefix Hijacking*, serta mekanisme mitigasinya. Ringkasan penelitian terkait yang dijadikan acuan dalam penelitian ini disajikan pada Tabel 2.1.

Tabel 2.1 Penelitian Terkait

| No | Judul Penelitian | Hasil Penelitian | Perbedaan |
|---|---|---|---|
| 1 | *Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols (Kabir et al., 2021)* | Menganalisis performa RIP, EIGRP, dan OSPF berdasarkan latency, throughput, dan convergence time pada jaringan enterprise. | Penelitian tersebut berfokus pada performa *routing* protocol, sedangkan penelitian ini menguji route injection pada BGP dan EIGRP serta mitigasi prefix-list. |
| 2 | *Quality of Service EIGRP Routing Protocol on Campus Area Network (Musril et al., 2021)* | Menunjukkan bahwa EIGRP memiliki performa QoS yang baik berdasarkan throughput, packet loss, latency, dan jitter. | Penelitian tersebut hanya membahas QoS EIGRP pada kondisi normal, sedangkan penelitian ini menguji dampak route injection dan filtering pada EIGRP serta membandingkannya dengan BGP. |

POLITEKNIK NEGERI JAKARTA

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| No | Judul Penelitian | Hasil Penelitian | Perbedaan |
|---|---|---|---|
| 3 | *Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis* (McDaniel et al., 2021) | Menunjukkan bahwa filtering dapat membatasi penyebaran rute bermasalah pada BGP. | Penelitian tersebut berfokus pada route leak BGP, sedangkan penelitian ini menggunakan prefix-list untuk memitigasi route injection pada BGP dan EIGRP. |
| 4 | *Estimating the Impact of BGP Prefix Hijacking* (Sermpezis et al., 2021) | Menjelaskan bahwa manipulasi prefix pada BGP dapat berdampak pada keamanan dan ketersediaan komunikasi Internet. | Penelitian tersebut berfokus pada prefix hijacking BGP, sedangkan penelitian ini menguji route injection sebagai manipulasi informasi *routing* pada BGP dan EIGRP. |
| 5 | *Implementasi Routing Protokol Border Gateway Protocol (BGP) pada Router Mikrotik RB2011 di Kominfo Kabupaten Solok Selatan* (Putra & Patra, 2021) | Mengimplementasikan BGP pada jaringan MAN dan mengevaluasi kualitas layanan jaringan menggunakan parameter QoS. | Penelitian tersebut membahas implementasi BGP pada kondisi normal, sedangkan penelitian ini menambahkan skenario route injection, perbandingan dengan EIGRP, dan mitigasi prefix-list. |

Berdasarkan Tabel 2.1, penelitian terkait yang digunakan dalam penelitian ini menunjukkan bahwa kajian sebelumnya masih banyak berfokus pada performa *routing* protocol, pengukuran Quality of Service (QoS), dan keamanan *routing* pada BGP. Penelitian Kabir et al. (2021) membahas performa RIP, EIGRP, dan OSPF berdasarkan latency, throughput, dan convergence time pada jaringan enterprise. Penelitian Musril et al. (2021)

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

juga membahas EIGRP, tetapi fokusnya masih pada performa QoS dalam kondisi normal. Sementara itu, penelitian Putra dan Patra (2021) membahas implementasi BGP pada jaringan MAN dan mengevaluasi kualitas layanan jaringan menggunakan parameter QoS. Ketiga penelitian tersebut menunjukkan bahwa parameter QoS dapat digunakan untuk menilai performa *routing*, tetapi belum membahas dampak serangan terhadap *routing* table, konektivitas, maupun efektivitas mitigasi.

Pada sisi keamanan *routing*, penelitian McDaniel et al. (2021) menunjukkan bahwa mekanisme filtering dapat membatasi penyebaran rute bermasalah pada BGP, sedangkan Sermpezis et al. (2021) menjelaskan bahwa manipulasi prefix pada BGP dapat berdampak pada keamanan dan ketersediaan komunikasi Internet. Kedua penelitian tersebut relevan untuk memperkuat dasar bahwa manipulasi informasi *routing* dapat mengganggu jaringan dan bahwa filtering dapat digunakan sebagai salah satu mekanisme mitigasi. Namun, penelitian tersebut masih berfokus pada konteks BGP dan belum membandingkan dampaknya dengan protokol EIGRP.

Berdasarkan penelitian-penelitian tersebut, masih terdapat ruang penelitian pada pengujian route injection terhadap dua protokol *routing* yang berbeda, yaitu BGP sebagai protokol inter-domain dan EIGRP sebagai protokol intra-domain. Oleh karena itu, penelitian ini berfokus pada pengujian route injection pada BGP dan EIGRP serta penerapan basic filtering menggunakan prefix-list. Evaluasi dilakukan pada kondisi normal, saat serangan, dan setelah filtering diterapkan dengan indikator perubahan *routing* table, konektivitas, waktu konvergensi atau pemulihan, serta parameter QoS berupa delay, throughput, dan packet loss. Dengan demikian, penelitian ini tidak hanya membahas performa *routing* dalam kondisi normal, tetapi juga menguji dampak serangan dan efektivitas mitigasi terhadap stabilitas *routing* dan kualitas layanan jaringan.

## 2.2 Konsep *Routing* dan *Control Plane*

*Routing* merupakan proses penentuan jalur yang digunakan untuk mengirimkan paket data dari sumber menuju tujuan. Pada jaringan dinamis,

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

proses pemilihan jalur dilakukan dengan bantuan protokol *routing* agar router dapat bertukar informasi rute dan memperbarui *routing* table secara otomatis ketika terjadi perubahan topologi. (Kabir et al., 2021) menjelaskan bahwa protokol *routing* digunakan untuk menentukan jalur terbaik dalam proses pengiriman data pada jaringan enterprise.

Dalam sistem *routing*, control plane berperan dalam pertukaran informasi rute dan pembentukan keputusan *routing*. Apabila informasi pada control plane dimanipulasi, maka router dapat memilih jalur yang tidak semestinya meskipun koneksi fisik masih berjalan. Oleh karena itu, keamanan informasi *routing* menjadi penting karena validitas route advertisement sangat berpengaruh terhadap stabilitas jaringan dan ketersediaan layanan (OECD, 2022; Pranaya & Wellem, 2021).

## 2.3 *Border Gateway Protocol* (BGP) dan *Autonomous System*

*Border Gateway Protocol* (BGP) merupakan protokol *routing* yang digunakan untuk pertukaran informasi rute antar-*Autonomous System* (AS). BGP banyak digunakan pada jaringan *inter-domain* karena dapat menghubungkan jaringan yang memiliki kebijakan *routing* berbeda. (Eko Kurniawanto, 2021) menjelaskan bahwa BGP dapat digunakan untuk mendukung konektivitas jaringan berskala besar dan pertukaran rute antarjaringan.

Namun, BGP memiliki kelemahan karena masih bergantung pada kepercayaan terhadap *route advertisement* yang diterima dari *router* atau AS lain. (Saad et al., 2022) menjelaskan bahwa model kepercayaan pada BGP dapat dimanfaatkan oleh pihak tidak sah untuk mengiklankan *prefix* palsu dan mengalihkan jalur trafik. (Scott et al., 2024) juga menyatakan bahwa BGP masih menjadi protokol *inter-domain* yang rentan terhadap serangan *routing*. Dalam penelitian ini, konsep tersebut digunakan sebagai dasar untuk memahami *route injection* pada BGP, yaitu kondisi ketika *attacker* mengiklankan rute tidak sah sehingga memengaruhi proses pemilihan rute.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## 2.4 *Enhanced Interior Gateway Routing Protocol* (EIGRP)

*Enhanced Interior Gateway Routing Protocol* (EIGRP) merupakan protokol *routing* dinamis yang digunakan pada jaringan internal atau *intra-domain*. EIGRP berfungsi untuk menentukan jalur terbaik berdasarkan informasi *routing* yang dipertukarkan antar-*router*. (Kabir et al., 2021) menggunakan EIGRP sebagai salah satu protokol yang dianalisis berdasarkan *latency*, *throughput*, dan *convergence time*.

(Antoni Musril et al., 2021) menjelaskan bahwa EIGRP dapat diterapkan pada jaringan kampus dan dievaluasi menggunakan parameter *Quality of Service* (QoS), seperti *throughput*, *packet loss*, *latency*, dan *jitter*. (Vidananda Agastya et al., 2021) juga menunjukkan bahwa EIGRP dapat digunakan pada perancangan jaringan kampus dengan hasil pengujian *packet loss*, *throughput*, dan *delay* yang memenuhi kategori baik berdasarkan standar TIPHON. Meskipun demikian, EIGRP tetap bergantung pada validitas informasi *routing* yang diterima. Jika terdapat rute tidak sah yang masuk ke domain EIGRP, *routing table* dapat berubah dan menyebabkan jalur komunikasi tidak sesuai dengan kondisi normal.

## 2.5 *Route Injection*

*Route injection* merupakan bentuk manipulasi informasi *routing* ketika *attacker* mengiklankan atau memasukkan rute yang tidak sah ke dalam jaringan. Rute tersebut dapat diterima oleh *router* dan masuk ke *routing table*, sehingga *router* berpotensi memilih jalur yang tidak semestinya. Pada BGP, *route injection* dapat terjadi ketika *attacker* mengiklankan *prefix* tertentu agar *router* lain menganggap rute tersebut valid. Pada EIGRP, *route injection* dapat terjadi ketika rute eksternal masuk ke domain *routing* internal dan memengaruhi pemilihan jalur.

(Shapira & Shavitt, 2022) menjelaskan bahwa serangan pada BGP dapat mengubah jalur trafik dan mengalihkan komunikasi melalui jaringan penyerang. (Pranaya & Wellem, 2021) juga menjelaskan bahwa *route advertisement* yang tidak valid dapat mengganggu konektivitas antar-AS

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dan mengalihkan *routing* ke tujuan yang tidak semestinya. Dampak *route injection* dapat diamati melalui perubahan *routing table*, perubahan *next-hop*, gangguan konektivitas, peningkatan *delay*, penurunan *throughput*, serta *packet loss*.

## 2.6 Mitigasi Basic Filtering Menggunakan Prefix-list

*Basic filtering* merupakan mekanisme penyaringan rute yang digunakan untuk mengontrol informasi *routing* yang diterima atau diiklankan oleh *router*. Pada penelitian ini, mekanisme *basic filtering* dibatasi pada penggunaan *prefix-list*. *Prefix-list* digunakan untuk mengizinkan atau menolak *prefix* tertentu berdasarkan kebijakan *routing* yang telah ditentukan.

(McDaniel et al., 2021) menunjukkan bahwa mekanisme *filtering* dapat membantu membatasi penyebaran rute bermasalah pada BGP. Sementara itu, (Pranaya & Wellem, 2021) menunjukkan bahwa validasi terhadap *route advertisement* dapat mencegah penyebaran rute yang tidak sah. Penelitian ini tidak menerapkan mekanisme kriptografis seperti RPKI/ROA atau BGPsec, tetapi menggunakan *prefix-list* karena lebih sederhana, ringan, dan realistis diterapkan pada konfigurasi *router* di lingkungan simulasi.

## 2.7 Parameter Evaluasi dan *Quality of Service* (QoS)

Evaluasi pada penelitian ini tidak hanya menilai keberhasilan paket mencapai tujuan, tetapi juga mengamati perubahan informasi rute pada *control plane* saat serangan dan setelah mitigasi diterapkan. Perubahan tersebut diamati melalui entri pada *routing table*, perubahan jalur seperti *next-hop* dan *AS path* pada BGP, serta waktu konvergensi atau pemulihan jaringan. Dalam konteks keamanan BGP, iklan rute yang tidak sah dapat memengaruhi pemilihan jalur lintas-AS sehingga perubahan rute dan waktu konvergensi menjadi indikator penting untuk menggambarkan dampak serangan terhadap layanan (Scott et al., 2024).

Selain indikator *routing*, penelitian ini menggunakan parameter *Quality of Service* (QoS) untuk menggambarkan dampak perubahan rute pada *control*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*plane* terhadap komunikasi pada *data plane*. Parameter yang digunakan meliputi *delay*, *throughput*, dan *packet loss*. Ketiga parameter tersebut digunakan untuk mengukur waktu pengiriman paket, laju trafik yang berhasil diamati, serta persentase kehilangan paket selama transmisi (Auliya & Dian W. Chandra, 2025; Nugroho et al., 2024). Pengukuran dilakukan untuk membandingkan kondisi *baseline*, saat *route injection*, dan setelah *basic filtering* diterapkan pada BGP maupun EIGRP.

Pada penelitian ini, standar TIPHON digunakan untuk menginterpretasikan nilai *delay* dan *packet loss* berdasarkan kategori kualitas layanan (Nisa et al., 2024). Sementara itu, nilai *throughput* digunakan sebagai parameter perbandingan antar-skenario tanpa dikategorikan berdasarkan TIPHON. Hal ini karena trafik pengujian menggunakan paket ICMP berukuran kecil dengan interval pengiriman tertentu, sehingga nilai *throughput* yang diperoleh menunjukkan laju trafik ICMP yang diamati dan bukan kapasitas maksimum jaringan. Dengan demikian, interpretasi TIPHON digunakan untuk memperjelas perubahan *delay* dan *packet loss*, sedangkan *throughput* dianalisis berdasarkan perubahan nilainya pada setiap kondisi pengujian.

a. *Delay*

*Delay* adalah waktu tempuh yang diperlukan paket data untuk berpindah dari pengirim ke penerima. Nilai *delay* yang meningkat dapat menunjukkan adanya antrean (*queueing*), pemanjangan jalur, atau kemacetan (*congestion*) sehingga berpotensi menimbulkan jeda pada layanan *real-time* (Auliya & Dian W. Chandra, 2025; Nugroho et al., 2024). Dalam pengukuran, nilai rata-rata *delay* dapat dihitung dengan membagi total *delay* terhadap jumlah paket yang diterima pada interval pengamatan tertentu (Nisa et al., 2024), sebagaimana Persamaan (1).

Persamaan (1) Rata-rata *delay*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

$$\text{Rata-rata } delay = \frac{\text{total delay}}{(\text{jumlah paket diterima } -1)}$$

Parameter ini digunakan untuk menilai apakah perubahan rute dan proses konvergensi selama serangan maupun setelah mitigasi menyebabkan waktu tempuh paket meningkat dibandingkan kondisi normal.

Tabel 2. 2 Indeks Delay berdasarkan standar *TIPHON*

| Kategori | *Delay* | Indeks |
|---|---|---|
| Sangat Baik | < 150 ms | 4 |
| Baik | 150 - 300 ms | 3 |
| Cukup | 300 - 450 ms | 2 |
| Buruk | > 450 ms | 1 |

Sumber tabel *TIPHON*: (Nisa et al., 2024).

b. *Packet loss*

*Packet loss* adalah persentase paket data yang hilang selama proses pengiriman. Kehilangan paket dapat terjadi karena kepadatan jaringan (*congestion*), gangguan pada jalur, atau error pada *link*, dan peningkatannya berdampak pada retransmisi serta penurunan kualitas aplikasi (Auliya & Dian W. Chandra, 2025; Nugroho et al., 2024). Nilai *packet loss* dapat dihitung menggunakan persentase selisih paket terkirim dan paket diterima terhadap paket terkirim (Nisa et al., 2024), sebagaimana Persamaan (2).

Persamaan (2) *Packet loss*

$$Packet\ loss = \frac{(\text{paket terkirim} - \text{paket diterima})}{\text{paket diterima}} \times 100\%$$

Parameter ini digunakan untuk menilai apakah serangan manipulasi rute dan perubahan jalur meningkatkan kehilangan paket pada jaringan uji, baik pada *BGP* maupun *EIGRP*, serta apakah mitigasi

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*basic filtering* mampu menurunkan kembali nilai *packet loss* mendekati kondisi normal.

Tabel 2.3 Indeks *Packet loss* berdasarkan standar *TIPHON*

| Kategori | *Packet loss* | Indeks |
|---|---|---|
| Sangat Baik | 0 - 2% | 4 |
| Baik | 3 - 14% | 3 |
| Cukup | 15 - 24% | 2 |
| Buruk | > 25% | 1 |

Sumber tabel *TIPHON*: (Nisa et al., 2024).

## 2.8 GNS3

GNS3 (*Graphical Network Simulator-3*) merupakan aplikasi simulator jaringan yang digunakan untuk membangun topologi dan menjalankan perangkat jaringan secara virtual, sehingga skenario pengujian dapat direplikasi tanpa harus menggunakan perangkat fisik. Pada penelitian simulasi BGP dan RPKI/ROV, GNS3 digunakan untuk mengimplementasikan beberapa *router* virtual serta *routing server* BIRD, dan dapat dipadukan dengan VMware untuk menjalankan mesin virtual yang dibutuhkan oleh topologi (Pranaya & Wellem, 2021). Selain itu, pemanfaatan GNS3 juga umum digunakan pada simulasi pengujian kinerja dan *Quality of Service* (QoS) pada topologi BGP, di mana pengiriman trafik uji dan pengukuran parameter seperti *throughput*, *delay*, dan *packet loss* dapat dilakukan pada lingkungan simulasi (Sahal Nurhidayah et al., 2022). Pada penelitian ini, GNS3 digunakan sebagai media simulasi untuk membangun topologi BGP dan EIGRP, menjalankan skenario normal-serangan-mitigasi, serta memudahkan pengamatan perubahan rute dan parameter QoS secara terukur.

## 2.9 Wireshark

Wireshark merupakan aplikasi *network protocol analyzer* yang digunakan untuk menangkap dan menganalisis paket data pada jaringan. (Nisa et al., 2024) menggunakan Wireshark dalam proses pengukuran QoS dengan parameter *throughput*, *delay*, *jitter*, dan *packet loss*. (Auliya & Dian W.

Chandra, 2025) juga menggunakan Wireshark untuk pengukuran QoS pada layanan jaringan.

Pada penelitian ini, Wireshark digunakan untuk melakukan *capture traffic* ICMP pada kondisi *baseline*, saat terjadi *route injection*, dan setelah penerapan *basic filtering* menggunakan *prefix-list*. Data hasil *capture* digunakan untuk menghitung *delay*, *throughput*, dan *packet loss*, serta mengamati perubahan konektivitas antar-PC selama proses pengujian berlangsung.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# BAB III
# METODE PENELITIAN

## 3.1 Rancangan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian eksperimental komparatif. Pendekatan kuantitatif digunakan karena penelitian menghasilkan data numerik yang dapat diukur secara objektif, seperti parameter *Quality of Service* (QoS) yang meliputi *delay*, *throughput*, dan *packet loss*, serta indikator lain berupa perubahan *routing table* dan waktu konvergensi atau pemulihan jaringan.

Jenis penelitian eksperimental komparatif dipilih karena penelitian ini membandingkan kondisi jaringan pada beberapa skenario yang berbeda, yaitu kondisi normal atau *baseline*, kondisi saat terjadi *route injection*, dan kondisi setelah penerapan mitigasi. Selain itu, penelitian ini juga membandingkan dua protokol *routing* dengan karakteristik berbeda, yaitu *Border Gateway Protocol* (BGP) sebagai protokol *routing inter-domain* dan *Enhanced Interior Gateway Routing Protocol* (EIGRP) sebagai protokol *routing intra-domain*.

Perlakuan dalam penelitian ini berupa manipulasi informasi *routing* pada *control plane* melalui skenario *route injection*. *Route injection* dilakukan dengan mengiklankan atau memasukkan rute tidak sah ke dalam jaringan sehingga *router* berpotensi memilih jalur yang tidak semestinya. Pada protokol BGP, *route injection* diamati melalui masuknya *route advertisement* atau *prefix* tidak sah ke *routing table*. Pada protokol EIGRP, *route injection* diamati melalui masuknya rute eksternal ke dalam domain *routing* internal yang dapat memengaruhi pemilihan jalur komunikasi.

Pada rancangan penelitian ini, sumber serangan direpresentasikan oleh PC-ATTACKER yang ditempatkan pada sisi Internet. PC-ATTACKER tidak digunakan sebagai perangkat yang secara langsung melakukan *route injection* ke dalam protokol *routing*, melainkan sebagai representasi sumber

serangan eksternal. Penelitian ini mengasumsikan bahwa PC-ATTACKER telah berhasil memperoleh akses kendali terhadap R4-ATTACKER. Setelah dikompromikan, R4-ATTACKER berperan sebagai *compromised router* yang digunakan untuk mengiklankan atau memasukkan rute tidak sah ke dalam proses *routing* BGP dan EIGRP. Dengan demikian, fokus penelitian tidak berada pada proses eksploitasi *router*, tetapi pada dampak *route injection* terhadap *routing table*, jalur komunikasi, dan kualitas layanan jaringan.

Mitigasi yang digunakan dalam penelitian ini adalah *basic filtering* menggunakan *prefix-list*. *Prefix-list* diterapkan untuk membatasi atau menolak informasi rute yang tidak sah agar tidak memengaruhi *routing table* dan jalur komunikasi. Efektivitas mitigasi diamati dengan membandingkan kondisi jaringan sebelum serangan, saat *route injection*, dan setelah *prefix-list* diterapkan.

Penelitian dilakukan pada lingkungan simulasi jaringan menggunakan *Graphical Network Simulator 3* (GNS3). Penggunaan simulasi memungkinkan pengujian dilakukan secara terkontrol dan fleksibel tanpa memengaruhi jaringan produksi. Data yang digunakan terdiri dari data primer berupa hasil observasi langsung dari simulasi, seperti *routing table*, hasil *ping*, hasil *traceroute*, waktu konvergensi atau pemulihan, dan hasil *capture* Wireshark. Hasil *traceroute* digunakan sebagai data pendukung untuk melihat jalur komunikasi yang dilalui paket pada setiap skenario pengujian. Data sekunder berupa literatur digunakan untuk mendukung konsep *routing*, *route injection*, *prefix-list*, dan QoS.

Pengujian dilakukan terhadap tiga *host* tujuan, yaitu PC1 dengan alamat 192.168.16.2, PC2 dengan alamat 192.168.17.2, dan PC3 dengan alamat 192.168.18.2. Setiap *host* diuji pada tiga kondisi, yaitu kondisi *baseline*, kondisi saat *route injection*, dan kondisi setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan. Hasil pengujian dari ketiga *host*



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

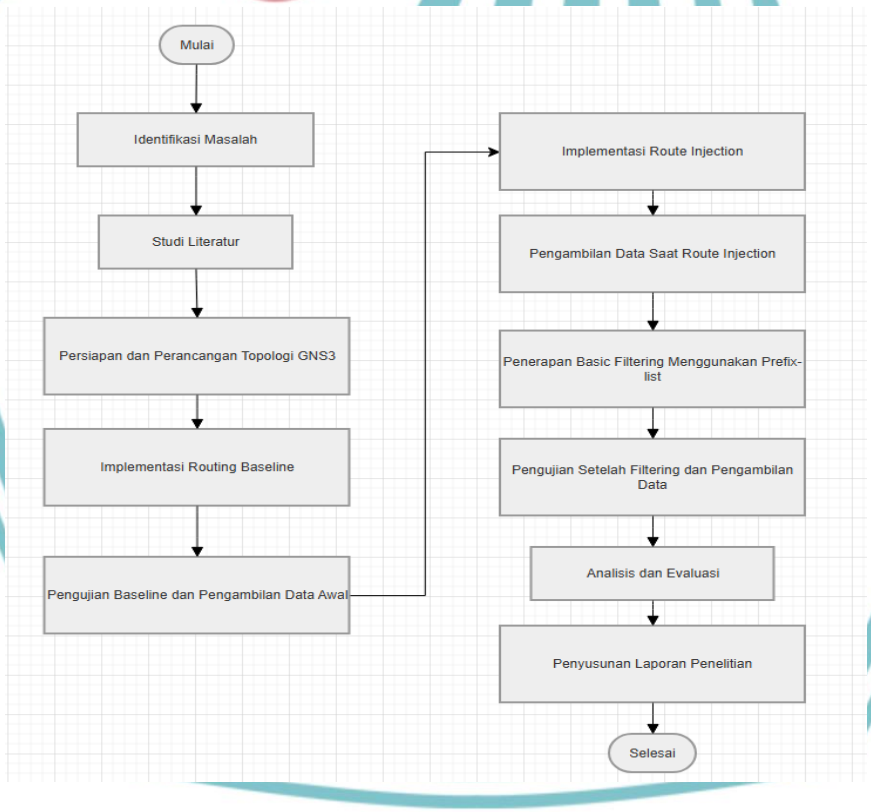
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

digunakan untuk membandingkan dampak *route injection* secara lebih menyeluruh, sehingga analisis tidak hanya berfokus pada satu *host* tujuan.

Dengan rancangan tersebut, penelitian ini berfokus pada pengujian ketahanan BGP dan EIGRP terhadap *route injection*, serta evaluasi efektivitas *basic filtering* menggunakan *prefix-list* dalam memulihkan stabilitas jaringan berdasarkan perubahan *routing table*, konektivitas, waktu pemulihan, dan parameter QoS

## 3.2 Tahapan Penelitian

Adapun tahapan yang dilakukan dalam penelitian ini, diantaranya:




Gambar 3.1 Tahapan Penelitian

Pada Gambar 3.1 menunjukkan tahapan yang dilakukan dalam penelitian ini melalui beberapa tahapan penyelesaian permasalahan yang diangkat, sebagai berikut:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1. Identifikasi Masalah

   Tahap identifikasi masalah dilakukan untuk memahami konteks penelitian dan menentukan fokus permasalahan yang dianalisis. Penelitian ini berfokus pada keamanan *routing*, khususnya manipulasi informasi *routing* pada protokol BGP dan EIGRP melalui skenario *route injection*. *Route injection* menjadi permasalahan karena rute tidak sah yang masuk ke *routing table* dapat menyebabkan *router* memilih jalur yang tidak semestinya. Berdasarkan analisis awal, gangguan pada informasi *routing* dapat memengaruhi stabilitas *routing*, konektivitas antar-*client*, serta kualitas layanan jaringan. Oleh karena itu, diperlukan pengujian untuk mengetahui dampak *route injection* terhadap BGP dan EIGRP, serta mengevaluasi efektivitas *basic filtering* menggunakan *prefix-list* sebagai mekanisme mitigasi.

2. Studi Literatur

   Tahap studi literatur dilakukan dengan mengumpulkan dan mempelajari referensi yang berkaitan dengan *routing*, *control plane*, BGP, EIGRP, *route injection*, *basic filtering*, *prefix-list*, QoS, GNS3, dan Wireshark. Referensi diperoleh dari jurnal ilmiah, artikel penelitian, dokumentasi teknis, serta sumber pendukung lain yang relevan. Hasil dari studi literatur digunakan sebagai dasar dalam menyusun batasan penelitian, menentukan skenario pengujian, memilih parameter evaluasi, serta memahami hubungan antara manipulasi informasi *routing* dan dampaknya terhadap kualitas layanan jaringan.

3. Persiapan dan Perancangan Topologi

   Tahap ini dilakukan untuk menyiapkan rancangan topologi jaringan yang akan digunakan pada lingkungan simulasi GNS3. Perancangan mencakup penentuan jumlah *router*, *client*, koneksi antarperangkat, pengalamatan IP, serta posisi sumber serangan eksternal. Topologi penelitian diperbaiki dengan menambahkan PC-ATTACKER pada sisi Internet sebagai representasi sumber serangan dari luar jaringan. R1-KOMINFO berperan sebagai *router* utama sekaligus *gateway* menuju Internet, sedangkan R4-ATTACKER berperan sebagai *compromised*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*router* yang diasumsikan telah berhasil dikendalikan oleh PC-ATTACKER. Topologi ini dirancang untuk mendukung pengujian dua protokol *routing*, yaitu BGP sebagai protokol *routing inter-domain* dan EIGRP sebagai protokol *routing intra-domain*. Selain itu, pada tahap ini juga ditentukan alur pengujian terhadap tiga *host*, yaitu PC1, PC2, dan PC3, dengan kondisi pengujian *baseline*, *route injection*, dan setelah *basic filtering* menggunakan *prefix-list* diterapkan.

4. Implementasi *Routing* Baseline

   Pada tahap ini dilakukan konfigurasi alamat IP dan protokol *routing* pada perangkat yang telah dirancang di GNS3. Konfigurasi *routing* dilakukan pada BGP dan EIGRP hingga jaringan mencapai kondisi stabil atau *converged*. Setelah konfigurasi selesai, dilakukan validasi *baseline* untuk memastikan seluruh perangkat dapat saling terhubung sesuai jalur normal. Validasi dilakukan dengan melihat *routing table* dan melakukan pengujian konektivitas menggunakan *ping* antar-*client*. Kondisi *baseline* digunakan sebagai acuan untuk membandingkan hasil pengujian pada tahap serangan dan setelah mitigasi.

5. Pengujian Baseline dan Pengambilan Data Awal

   Tahap ini dilakukan untuk memperoleh data awal sebelum *route injection* diterapkan. Pengujian *baseline* dilakukan pada PC1, PC2, dan PC3 untuk memastikan bahwa seluruh *host* dapat berkomunikasi melalui jalur *routing* yang valid. Data yang dikumpulkan meliputi *routing table*, jalur komunikasi, status konektivitas, waktu konvergensi, serta parameter QoS berupa *delay*, *throughput*, dan *packet loss*. Jalur komunikasi diamati menggunakan *traceroute* sebagai data pendukung untuk mengetahui rute yang dilalui paket pada kondisi normal. Pengambilan data QoS dilakukan menggunakan Wireshark dengan menangkap *traffic* ICMP selama proses pengujian konektivitas. Data *baseline* menjadi nilai pembanding untuk mengetahui perubahan yang terjadi ketika *route injection* diterapkan pada masing-masing *host* tujuan.

6. Implementasi Route Injection

   Pada tahap ini dilakukan penerapan skenario *route injection* melalui R4-ATTACKER yang berperan sebagai *compromised router*. PC-ATTACKER diasumsikan telah memperoleh akses kendali terhadap R4-ATTACKER, sehingga R4 dapat digunakan untuk mengiklankan atau memasukkan rute tidak sah ke dalam jaringan. Pada BGP, *route injection* dilakukan dengan mengiklankan *prefix host* /32 dari R4-ATTACKER ke R1-KOMINFO, sedangkan pada EIGRP *route injection* dilakukan dengan membuat *static route* palsu menuju Null0 pada R4-ATTACKER, kemudian *route* tersebut di-*redistribute* ke dalam proses EIGRP. *Route injection* dilakukan terhadap tiga target pengujian, yaitu PC1 dengan *prefix* 192.168.16.2/32, PC2 dengan *prefix* 192.168.17.2/32, dan PC3 dengan *prefix* 192.168.18.2/32. Dampak *route injection* diamati melalui perubahan *routing table*, perubahan *next-hop*, hasil *traceroute*, gangguan konektivitas, waktu konvergensi, serta perubahan parameter QoS berupa *delay*, *throughput*, dan *packet loss*.

7. Penerapan Basic Filtering Menggunakan Prefix-list

   Setelah dampak *route injection* diperoleh, tahap berikutnya adalah menerapkan *basic filtering* menggunakan *prefix-list*. *Prefix-list* digunakan untuk membatasi atau menolak rute tidak sah yang berasal dari *attacker*. Penerapan *prefix-list* dilakukan sebagai mekanisme mitigasi untuk mencegah rute tidak sah memengaruhi *routing table*. Setelah konfigurasi *filtering* diterapkan, dilakukan validasi ulang untuk memastikan rute yang tidak sah berhasil ditolak dan jalur komunikasi kembali menggunakan rute yang valid.

8. Pengujian Setelah Filtering dan Pengambilan Data

   Tahap ini dilakukan untuk memperoleh data setelah *basic filtering* menggunakan *prefix-list* diterapkan. Pengujian dilakukan kembali terhadap PC1, PC2, dan PC3 pada protokol BGP dan EIGRP. Data yang dikumpulkan meliputi *routing table*, jalur komunikasi berdasarkan *traceroute*, konektivitas, waktu pemulihan, *delay*, *throughput*, dan



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*packet loss*. Data pada tahap ini digunakan untuk melihat apakah penerapan *prefix-list* mampu menolak rute tidak sah dan mengembalikan kondisi jaringan mendekati kondisi *baseline*. Hasil pengujian kemudian disajikan dalam bentuk tabel dan grafik agar perubahan nilai *delay*, *throughput*, dan *packet loss* pada setiap kondisi dapat dibandingkan secara lebih jelas.

9. Analisis dan Evaluasi

   Pada tahap ini dilakukan analisis terhadap seluruh data yang diperoleh dari kondisi *baseline*, saat *route injection*, dan setelah *filtering*. Analisis dilakukan dengan membandingkan perubahan *routing table*, konektivitas, waktu konvergensi atau pemulihan, serta parameter QoS pada PC1, PC2, dan PC3. Evaluasi dilakukan untuk mengetahui dampak *route injection* terhadap BGP dan EIGRP, membandingkan kondisi setiap *host* yang diuji, serta menilai efektivitas *prefix-list* dalam memitigasi serangan. Hasil QoS berupa *delay*, *throughput*, dan *packet loss* disajikan dalam bentuk tabel dan grafik untuk memperjelas perubahan kualitas layanan jaringan pada setiap skenario pengujian.

10. Penyusunan Laporan Penelitian

    Tahap akhir penelitian adalah penyusunan laporan skripsi. Laporan berisi seluruh proses penelitian mulai dari latar belakang, tinjauan pustaka, metode penelitian, perancangan dan implementasi sistem, hasil pengujian, analisis, kesimpulan, serta saran. Laporan disusun berdasarkan hasil pengujian yang telah dilakukan pada lingkungan simulasi GNS3 dan data yang diperoleh dari *routing table*, pengujian konektivitas, *traceroute*, serta *capture* Wireshark.

## 3.3 Objek Penelitian

Objek penelitian merupakan hal yang menjadi sasaran dalam penelitian. Objek pada penelitian ini adalah protokol *routing Border Gateway Protocol* (BGP) dan *Enhanced Interior Gateway Routing Protocol* (EIGRP) yang diuji pada lingkungan simulasi jaringan menggunakan *Graphical Network Simulator 3* (GNS3). BGP digunakan untuk merepresentasikan pertukaran

informasi *routing* pada jaringan *inter-domain*, sedangkan EIGRP digunakan untuk merepresentasikan pertukaran informasi *routing* pada jaringan *intra-domain* atau jaringan internal.

Perangkat yang digunakan dalam penelitian terdiri dari R1-KOMINFO, R2-CAPIL, R3-SANGIR, R4-ATTACKER, PC-ATTACKER, PC1, PC2, dan PC3. PC-ATTACKER ditempatkan pada sisi Internet sebagai representasi sumber serangan eksternal, sedangkan R4-ATTACKER berperan sebagai *compromised router* yang diasumsikan telah dikendalikan oleh PC-ATTACKER untuk melakukan *route injection*.

Penelitian ini berfokus pada pengujian dampak *route injection* terhadap BGP dan EIGRP. *Route injection* dilakukan dengan mengiklankan atau memasukkan rute tidak sah ke dalam jaringan sehingga dapat memengaruhi *routing table* dan proses pemilihan jalur. Selain itu, penelitian ini juga menguji efektivitas *basic filtering* menggunakan *prefix-list* sebagai mekanisme mitigasi untuk membatasi atau menolak rute tidak sah.

Aspek yang diamati dalam penelitian ini meliputi perubahan *routing table*, perubahan jalur komunikasi atau *next-hop*, konektivitas antar-*client*, waktu konvergensi atau pemulihan jaringan, serta parameter *Quality of Service* (QoS) berupa *delay*, *throughput*, dan *packet loss*. Pengujian dilakukan terhadap tiga *host*, yaitu PC1 dengan alamat 192.168.16.2, PC2 dengan alamat 192.168.17.2, dan PC3 dengan alamat 192.168.18.2 pada kondisi *baseline*, *route injection*, dan setelah *basic filtering* menggunakan *prefix-list* diterapkan.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# BAB IV
# HASIL DAN PEMBAHASAN

## 4.1 Analisis Kebutuhan

Analisis kebutuhan dilakukan untuk menentukan aspek yang diperlukan dalam proses perancangan, implementasi, dan pengujian sistem. Kebutuhan pada penelitian ini mencakup protokol *routing*, perangkat lunak, skenario pengujian, metode serangan, metode mitigasi, serta parameter pengujian yang digunakan untuk mengevaluasi kondisi jaringan. Aspek kebutuhan yang digunakan dalam penelitian ini ditunjukkan pada Tabel 4.1.

Tabel 4.1 Analisis Kebutuhan

| No | Aspek | Detail |
|---|---|---|
| 1 | Protokol *routing* | BGP digunakan sebagai protokol *routing* inter-domain antar Autonomous System, sedangkan EIGRP digunakan sebagai protokol *routing* intra-domain pada jaringan internal. |
| 2 | Perangkat lunak | GNS3 digunakan untuk membangun simulasi jaringan. Wireshark digunakan untuk melakukan capture dan analisis paket. VPCS digunakan sebagai client untuk pengujian konektivitas. Cisco IOS image digunakan sebagai router virtual. |
| 3 | Skenario pengujian | Pengujian dilakukan pada tiga kondisi, yaitu kondisi normal atau baseline, kondisi saat route injection, dan kondisi setelah penerapan basic filtering menggunakan prefix-list. |
| 4 | Metode serangan | Serangan dilakukan menggunakan metode route injection dengan mengiklankan atau memasukkan rute tidak sah dari router attacker ke jaringan. |
| 5 | Metode mitigasi | Mitigasi dilakukan menggunakan basic filtering dengan menerapkan prefix-list untuk membatasi atau menolak rute tidak sah dari attacker. |
| 6 | Parameter pengujian | Parameter yang digunakan meliputi *routing* table, next-hop, konektivitas, waktu konvergensi atau pemulihan, delay, throughput, dan packet loss. |
| 7 | Data pengamatan | Data diperoleh dari hasil perintah show ip route, show ip bgp, pengujian ping, traceroute, serta hasil capture Wireshark. |

Berdasarkan Tabel 4.1, kebutuhan utama dalam penelitian ini berfokus pada pengujian ketahanan *routing* terhadap *route injection* dan penerapan mitigasi *basic filtering* menggunakan *prefix-list*. BGP digunakan untuk mengamati pertukaran informasi *routing* pada jaringan *inter-domain*, sedangkan EIGRP digunakan untuk mengamati pertukaran informasi

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*routing* pada jaringan internal. Parameter pengujian seperti *routing table*, *next-hop*, konektivitas, waktu konvergensi atau pemulihan, *delay*, *throughput*, dan *packet loss* digunakan untuk membandingkan kondisi jaringan sebelum serangan, saat *route injection*, dan setelah mitigasi diterapkan.

Selain aspek kebutuhan sistem, penelitian ini juga membutuhkan perangkat pendukung untuk menjalankan simulasi dan proses pengujian. Kebutuhan perangkat yang digunakan dalam penelitian ini ditunjukkan pada Tabel 4.2.

Tabel 4.2 Kebutuhan Perangkat Penelitian

| No | Perangkat / Komponen | Spesifikasi / Versi | Keterangan |
|---|---|---|---|
| 1 | Laptop/komputer | 11th Gen Intel(R) Core(TM) i5-11400H @ 2.70 GHz, RAM 24 GB, penyimpanan 477 GB, NVIDIA GeForce RTX 3050 Laptop GPU 4 GB | Digunakan sebagai perangkat utama untuk menjalankan simulasi GNS3, router virtual, VPCS, dan Wireshark. |
| 2 | GNS3 | Versi 2.2.58.1 | Digunakan untuk membangun topologi jaringan dan menjalankan simulasi. |
| 3 | Wireshark | Versi 4.6.5 | Digunakan untuk melakukan capture paket ICMP dan membantu pengukuran QoS. |
| 4 | VPCS | Bawaan GNS3 | Digunakan sebagai client untuk pengujian ping dan traceroute. |
| 5 | Cisco IOS image | c7200-adventerprisek9-mz.152-4.S6.image | Digunakan sebagai router virtual untuk menjalankan konfigurasi BGP, EIGRP, dan prefix-list. |
| 6 | Sistem operasi | Windows 11 64-bit | Digunakan sebagai sistem operasi utama untuk menjalankan aplikasi pendukung penelitian. |

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Tabel 4.2, perangkat utama yang digunakan dalam penelitian ini adalah laptop atau komputer yang menjalankan GNS3 sebagai media simulasi jaringan. GNS3 digunakan untuk membangun topologi dan menjalankan *router virtual*, sedangkan Wireshark digunakan untuk mengamati paket ICMP selama proses pengujian. VPCS digunakan sebagai *client* untuk melakukan pengujian *ping* dan *traceroute*, sementara *Cisco IOS image* digunakan untuk menjalankan konfigurasi BGP, EIGRP, dan *prefix-list*.

Dengan kebutuhan tersebut, sistem simulasi dapat digunakan untuk mengamati perubahan *routing table*, perubahan *next-hop*, masuknya rute tidak sah, gangguan konektivitas, serta dampaknya terhadap kualitas layanan jaringan. Kebutuhan ini menjadi dasar dalam proses perancangan sistem, implementasi konfigurasi, dan pengujian pada skenario *baseline*, *route injection*, dan setelah mitigasi.

## 4.2 Perancangan Sistem

Perancangan sistem pada penelitian ini dilakukan untuk membangun model simulasi jaringan yang sesuai dengan kebutuhan pengujian. Sistem dirancang menggunakan GNS3 dengan dua topologi pengujian, yaitu topologi BGP dan topologi EIGRP. Kedua topologi menggunakan struktur jaringan yang sama dan diadaptasi dari topologi pada penelitian Eko Kurniawanto (2021), yang membahas implementasi *routing* BGP pada jaringan MAN serta pengujian kualitas layanan jaringan.

Pada penelitian ini, topologi tersebut dimodifikasi sesuai kebutuhan pengujian dengan menambahkan PC-ATTACKER pada sisi Internet dan R4-ATTACKER sebagai *compromised router*. PC-ATTACKER digunakan untuk merepresentasikan sumber serangan eksternal dari luar jaringan, sedangkan R4-ATTACKER diasumsikan telah berhasil dikendalikan oleh PC-ATTACKER dan digunakan untuk melakukan *route injection*. Penambahan PC-ATTACKER dilakukan agar asal serangan terlihat berasal dari luar jaringan, bukan dari jaringan internal.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pada topologi BGP, *router* dikonfigurasi menggunakan AS yang berbeda untuk merepresentasikan pertukaran *routing* antar-*Autonomous System*. Sementara itu, pada topologi EIGRP, struktur perangkat yang sama digunakan untuk merepresentasikan jaringan internal dengan protokol *routing* EIGRP AS 100. Dengan rancangan tersebut, penelitian dapat membandingkan dampak *route injection* dan efektivitas *prefix-list* pada dua protokol *routing* yang berbeda menggunakan struktur topologi yang setara.

Kedua topologi digunakan untuk menguji dampak *route injection* terhadap *routing table*, konektivitas, waktu konvergensi atau pemulihan, serta parameter *Quality of Service* (QoS) berupa *delay*, *throughput*, dan *packet loss*. Pengujian dilakukan pada tiga *host* tujuan, yaitu PC1, PC2, dan PC3, dengan tiga kondisi pengujian, yaitu *baseline*, *route injection*, dan setelah penerapan *basic filtering* menggunakan *prefix-list*.

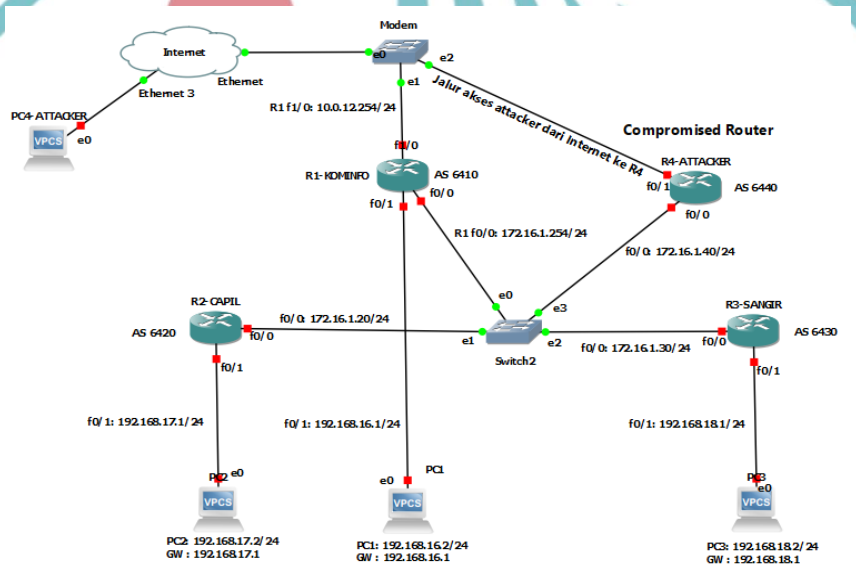
### 4.2.1 Perancangan Topologi BGP

Topologi BGP dirancang untuk merepresentasikan pertukaran informasi *routing* antar-*Autonomous System*. Pada topologi ini terdapat tiga *router* utama, yaitu R1-KOMINFO, R2-CAPIL, dan R3-SANGIR, serta satu *compromised router* yaitu R4-ATTACKER. R1-KOMINFO berada pada AS 6410, R2-CAPIL berada pada AS 6420, R3-SANGIR berada pada AS 6430, dan R4-ATTACKER berada pada AS 6440. *Router* tersebut saling terhubung melalui jaringan transit 172.16.1.0/24 menggunakan Switch2.

Pada topologi ini, PC4-ATTACKER ditempatkan pada sisi Internet sebagai representasi sumber serangan eksternal. PC4-ATTACKER terhubung ke jaringan melalui Internet dan modem. R1-KOMINFO berperan sebagai *router* utama sekaligus *gateway* menuju Internet, sedangkan R4-ATTACKER memiliki koneksi ke modem sebagai jalur akses dari sisi Internet dan koneksi ke Switch2 sebagai jalur *routing* internal. Dalam penelitian ini, R4-ATTACKER diasumsikan telah berhasil dikompromikan oleh PC4-ATTACKER,

sehingga R4 digunakan sebagai *compromised router* untuk melakukan *route injection* ke dalam jaringan BGP.

Sisi *client* terdiri dari PC1, PC2, dan PC3. PC1 berada pada jaringan 192.168.16.0/24, PC2 berada pada jaringan 192.168.17.0/24, dan PC3 berada pada jaringan 192.168.18.0/24. *Router* R4-ATTACKER digunakan untuk mensimulasikan *route injection* dengan mengiklankan rute tidak sah ke R1-KOMINFO. Susunan perangkat dan hubungan antar-*router* pada topologi BGP dapat dilihat pada Gambar 4.1.




Gambar 4.1 Topologi BGP pada GNS3

Berdasarkan Gambar 4.1, topologi BGP digunakan untuk mengamati bagaimana route advertisement yang tidak sah dari R4-ATTACKER dapat memengaruhi proses pemilihan rute pada router BGP. Dampak yang diamati meliputi perubahan *routing* table, perubahan next-hop, gangguan konektivitas antar-client, waktu konvergensi atau pemulihan, serta perubahan nilai delay, throughput, dan packet loss.

Agar peran setiap router pada topologi BGP lebih jelas, pembagian perangkat dan Autonomous System dijelaskan pada Tabel 4.3.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.3 Pembagian Autonomous System pada Topologi BGP

| Router | Peran | AS | Keterangan |
|---|---|---|---|
| R1-KOMINFO | Router utama | AS 6410 | Gateway PC1, gateway menuju Internet, dan terhubung ke jaringan transit |
| R2-CAPIL | Router utama | AS 6420 | Gateway PC2 |
| R3-SANGIR | Router utama | AS 6430 | Gateway PC3 |
| R4-ATTACKER | Compromised router | AS 6440 | Router yang diasumsikan telah dikompromikan dan digunakan untuk mengiklankan rute tidak sah |

Berdasarkan Tabel 4.3, setiap router pada topologi BGP ditempatkan pada AS yang berbeda. Pembagian AS tersebut digunakan untuk merepresentasikan hubungan antarjaringan yang saling bertukar informasi *routing* menggunakan BGP. R4-ATTACKER tidak digunakan sebagai router utama, melainkan sebagai compromised router untuk menguji apakah rute tidak sah yang diiklankan dapat memengaruhi *routing* table dan jalur komunikasi.

### 4.2.2 Perancangan Topologi EIGRP

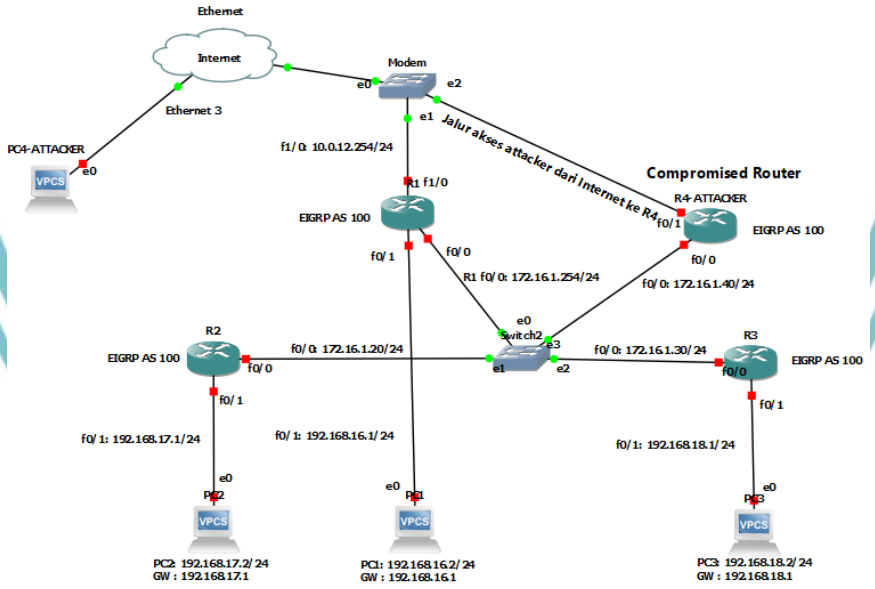
Topologi EIGRP menggunakan struktur jaringan yang sama dengan topologi BGP, tetapi protokol *routing* yang digunakan adalah EIGRP. Pada topologi ini, router R1, R2, R3, dan R4 menjalankan EIGRP AS 100. Router R1, R2, dan R3 berperan sebagai router utama, sedangkan R4 berperan sebagai compromised router yang digunakan untuk melakukan route injection. Seluruh router terhubung melalui jaringan transit 172.16.1.0/24 menggunakan Switch2. R1 berperan sebagai gateway untuk PC1, R2 berperan sebagai gateway untuk PC2, dan R3 berperan sebagai gateway untuk PC3.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pada topologi ini, PC4-ATTACKER ditempatkan pada sisi Internet sebagai representasi sumber serangan eksternal. PC4-ATTACKER terhubung ke jaringan melalui Internet dan modem. R4-ATTACKER memiliki koneksi ke modem sebagai jalur akses dari sisi Internet, serta koneksi ke Switch2 sebagai jalur *routing* internal. Dalam penelitian ini, R4-ATTACKER diasumsikan telah berhasil dikompromikan oleh PC4-ATTACKER, sehingga R4 digunakan untuk memasukkan rute tidak sah ke dalam domain EIGRP.

Route injection pada topologi EIGRP dilakukan dengan membuat static route palsu menuju Null0 pada R4-ATTACKER, kemudian route tersebut di-redistribute ke dalam proses EIGRP. Skenario ini digunakan untuk mengamati apakah rute tidak sah dapat masuk ke *routing* table router lain dan memengaruhi jalur komunikasi. Susunan perangkat pada topologi EIGRP dapat dilihat pada Gambar 4.2.




Gambar 4.2 Topologi EIGRP pada GNS3

Berdasarkan Gambar 4.2, topologi EIGRP digunakan untuk mengamati dampak route injection pada jaringan internal. Dampak

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

yang diamati meliputi perubahan *routing* table, perubahan next-hop, konektivitas antar-client, waktu konvergensi atau pemulihan, serta parameter QoS. Setelah mitigasi diterapkan, prefix-list digunakan untuk membatasi atau menolak rute tidak sah dari R4-ATTACKER.

Pembagian perangkat pada topologi EIGRP dijelaskan pada Tabel 4.4 agar fungsi setiap router dan perangkat pendukung lebih mudah dipahami.

Tabel 4.4 Pembagian Router pada Topologi EIGRP

| Router | Peran | *Routing* | Keterangan |
|---|---|---|---|
| R1 | Router utama | EIGRP AS 100 | Gateway PC1, gateway menuju Internet, dan terhubung ke jaringan transit |
| R2 | Router utama | EIGRP AS 100 | Gateway PC2 |
| R3 | Router utama | EIGRP AS 100 | Gateway PC3 |
| R4 | Compromised router | EIGRP AS 100 | Router yang diasumsikan telah dikompromikan dan digunakan untuk melakukan route injection |

Berdasarkan Tabel 4.4, router R1, R2, R3, dan R4 berada pada domain EIGRP AS 100. R1, R2, dan R3 digunakan sebagai router utama, sedangkan R4 tidak digunakan sebagai router utama, melainkan sebagai compromised router untuk menguji apakah rute tidak sah dapat memengaruhi *routing* table dan jalur komunikasi pada jaringan EIGRP.

### 4.2.3 Perancangan Pengalamatan IP

Pengalamatan IP dirancang agar setiap router dan client dapat saling terhubung sesuai dengan topologi pengujian. Jaringan transit antarrouter menggunakan network 172.16.1.0/24, sedangkan jaringan client menggunakan tiga network berbeda, yaitu 192.168.16.0/24, 192.168.17.0/24, dan 192.168.18.0/24. Selain itu,

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

terdapat jaringan akses menuju Internet yang digunakan untuk menghubungkan PC4-ATTACKER, modem, R1-KOMINFO, dan R4-ATTACKER. Rincian pengalamatan IP yang digunakan pada topologi ditampilkan pada Tabel 4.5.

Tabel 4.5 Pengalamatan IP

| Perangkat | Interface | IP Address | Keterangan |
|---|---|---|---|
| R1-KOMINFO | f1/0 | 10.0.12.254/24 | Terhubung ke modem |
| R1-KOMINFO | f0/0 | 172.16.1.254/24 | Terhubung ke jaringan transit |
| R1-KOMINFO | f0/1 | 192.168.16.1/24 | Gateway PC1 |
| R2-CAPIL | f0/0 | 172.16.1.20/24 | Terhubung ke jaringan transit |
| R2-CAPIL | f0/1 | 192.168.17.1/24 | Gateway PC2 |
| R3-SANGIR | f0/0 | 172.16.1.30/24 | Terhubung ke jaringan transit |
| R3-SANGIR | f0/1 | 192.168.18.1/24 | Gateway PC3 |
| R4-ATTACKER | f0/0 | 172.16.1.40/24 | Terhubung ke jaringan transit |
| PC1 | e0 | 192.168.16.2/24 | Gateway 192.168.16.1 |
| PC2 | e0 | 192.168.17.2/24 | Gateway 192.168.17.1 |
| PC3 | e0 | 192.168.18.2/24 | Gateway 192.168.18.1 |

Berdasarkan Tabel 4.5, setiap client berada pada network yang berbeda dan menggunakan router masing-masing sebagai default gateway. PC1 menggunakan gateway R1-KOMINFO, PC2 menggunakan gateway R2-CAPIL, dan PC3 menggunakan gateway R3-SANGIR. Jaringan 172.16.1.0/24 digunakan sebagai jalur transit antarrouter melalui Switch2, sedangkan interface R1-KOMINFO menuju modem digunakan untuk merepresentasikan koneksi

jaringan ke arah Internet. PC4-ATTACKER tidak dicantumkan dalam tabel pengalamatan IP karena perangkat tersebut hanya digunakan sebagai representasi sumber serangan eksternal dalam asumsi penelitian, bukan sebagai perangkat yang dikonfigurasi dalam proses *routing*. R4-ATTACKER tetap dikonfigurasi pada jaringan transit dan berperan sebagai compromised router yang digunakan untuk melakukan route injection..

### 4.2.4 Perancangan Mekanisme Route Injection

*Route injection* dirancang sebagai skenario serangan pada *control plane* dengan cara mengiklankan atau memasukkan rute tidak sah melalui R4-ATTACKER. Dalam penelitian ini, R4-ATTACKER berperan sebagai *compromised router* yang diasumsikan telah berhasil dikendalikan oleh PC-ATTACKER dari sisi Internet. PC-ATTACKER tidak melakukan *route injection* secara langsung, melainkan menjadi representasi sumber serangan eksternal yang memperoleh akses kendali terhadap R4-ATTACKER.

Pada topologi BGP, *route injection* dilakukan melalui *route advertisement* dari R4-ATTACKER ke R1-KOMINFO dengan mengiklankan *prefix host* /32 yang tidak sah. Pada topologi EIGRP, *route injection* dilakukan dengan membuat *static route* palsu menuju Null0 pada R4-ATTACKER, kemudian *route* tersebut di-*redistribute* ke dalam proses EIGRP sehingga dapat muncul pada *routing table router* lain. *Route injection* dilakukan terhadap tiga target pengujian, yaitu PC1 dengan *prefix* 192.168.16.2/32, PC2 dengan *prefix* 192.168.17.2/32, dan PC3 dengan *prefix* 192.168.18.2/32. Dampak *route injection* diamati melalui perubahan *routing table*, perubahan *next-hop*, hasil *traceroute*, gangguan konektivitas, waktu konvergensi, serta perubahan parameter QoS berupa *delay*, *throughput*, dan *packet loss*. Jika rute tidak sah diterima oleh *router*, maka jalur komunikasi dapat berubah dari



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

kondisi normal dan berpotensi menyebabkan *packet loss*, peningkatan *delay*, atau penurunan *throughput*.

### 4.2.5 Perancangan Mekanisme Mitigasi

Mitigasi yang digunakan pada penelitian ini adalah *basic filtering* menggunakan *prefix-list*. *Prefix-list* digunakan untuk membatasi atau menolak rute tidak sah yang berasal dari R4-ATTACKER agar rute tersebut tidak memengaruhi *routing table* dan proses pemilihan jalur pada *router* utama.

Pada topologi BGP, *prefix-list* diterapkan pada R1-KOMINFO untuk menolak *prefix host* /32 tidak sah yang diiklankan oleh R4-ATTACKER. *Filtering* diterapkan terhadap *update routing* yang berasal dari *neighbor* R4-ATTACKER, sehingga *prefix* tidak sah tidak masuk ke tabel BGP maupun *routing table* R1-KOMINFO.

Pada topologi EIGRP, *prefix-list* digunakan bersama *distribute-list* untuk membatasi masuknya rute tidak sah yang berasal dari R4-ATTACKER ke dalam domain EIGRP. Dengan mekanisme ini, rute eksternal hasil redistribusi *static route* dari R4-ATTACKER dapat ditolak sebelum digunakan dalam proses pemilihan jalur.

Setelah *prefix-list* diterapkan, dilakukan pengujian ulang terhadap PC1, PC2, dan PC3 untuk melihat apakah rute tidak sah berhasil ditolak dan apakah konektivitas kembali normal. Efektivitas mitigasi diamati berdasarkan perubahan *routing table*, konektivitas antar-*client*, waktu pemulihan, *delay*, *throughput*, dan *packet loss*.

### 4.2.6 Perancangan Skenario Pengujian

Pengujian dirancang dalam tiga kondisi utama, yaitu *baseline*, *route injection*, dan setelah *filtering*. Kondisi *baseline* digunakan untuk memperoleh gambaran kondisi normal jaringan sebelum adanya rute tidak sah. Kondisi *route injection* digunakan untuk mengetahui dampak masuknya *prefix* tidak sah terhadap *routing table*, jalur



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

komunikasi, dan kualitas layanan jaringan. Sementara itu, kondisi setelah *filtering* digunakan untuk mengevaluasi kemampuan *prefix-list* dalam menolak rute tidak sah dan mengembalikan kondisi jaringan mendekati *baseline*.

Pada penelitian ini, pengujian dilakukan terhadap tiga *host* tujuan, yaitu PC1, PC2, dan PC3. Setiap *host* diuji pada kondisi *baseline*, *route injection*, dan setelah *filtering*. Pembagian target ini dilakukan agar dampak *route injection* tidak hanya diamati pada satu *host*, tetapi juga dapat dibandingkan pada beberapa *network* berbeda. Ringkasan skenario pengujian ditampilkan pada Tabel 4.6.

Tabel 4.6 Skenario Pengujian

| No | Target | Prefix Route Injection | Kondisi Pengujian | Data yang Diamati |
|---|---|---|---|---|
| 1 | PC1 | 192.168.16.2/32 | Baseline, Route Injection, Setelah Filtering | *Routing* table, next-hop, konektivitas, traceroute, waktu pemulihan, delay, throughput, packet loss |
| 2 | PC2 | 192.168.17.2/32 | Baseline, Route Injection, Setelah Filtering | *Routing* table, next-hop, konektivitas, traceroute, waktu pemulihan, delay, throughput, packet loss |
| 3 | PC3 | 192.168.18.2/32 | Baseline, Route Injection, Setelah Filtering | *Routing* table, next-hop, konektivitas, traceroute, waktu pemulihan, delay, throughput, packet loss |

Berdasarkan Tabel 4.6, route injection dilakukan dengan menggunakan prefix host /32 pada masing-masing target pengujian. Pada topologi BGP, prefix tidak sah diiklankan oleh R4-



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

ATTACKER ke R1-KOMINFO. Pada topologi EIGRP, prefix tidak sah dimasukkan melalui static route pada R4-ATTACKER, kemudian di-redistribute ke dalam proses EIGRP. Data hasil pengujian dari setiap target digunakan untuk membandingkan perubahan kondisi jaringan pada saat baseline, saat route injection, dan setelah filtering diterapkan.

## 4.3 Implementasi Sistem

Implementasi sistem dilakukan dengan membangun topologi jaringan pada simulator GNS3 berdasarkan rancangan yang telah dijelaskan sebelumnya. Tahap ini mencakup konfigurasi alamat IP serta protokol *routing* BGP dan EIGRP pada perangkat yang digunakan dalam pengujian. Selanjutnya, dilakukan verifikasi hubungan *neighbor*, *routing table*, dan konektivitas antar-*client* untuk memastikan jaringan berada dalam kondisi *baseline* yang stabil sebelum pengujian *route injection* dan mitigasi menggunakan *prefix-list* dilakukan pada subbab berikutnya.

Pada implementasi ini, R4-ATTACKER dikonfigurasi sebagai perangkat yang terhubung ke jaringan *routing*, tetapi pada kondisi *baseline* belum mengiklankan atau menyebarkan rute tidak sah. PC4-ATTACKER tidak dikonfigurasi dalam proses *routing*, karena perangkat tersebut hanya digunakan sebagai representasi sumber serangan eksternal dari sisi Internet. Dalam skenario penelitian, R4-ATTACKER diasumsikan telah dikompromikan oleh PC4-ATTACKER dan digunakan sebagai *compromised router* untuk melakukan *route injection*.

### 4.3.1 Implementasi *Routing* BGP

Implementasi *routing* BGP dilakukan pada topologi BGP yang terdiri dari router R1-KOMINFO, R2-CAPIL, R3-SANGIR, dan R4-ATTACKER. R1-KOMINFO dikonfigurasi menggunakan AS 6410, R2-CAPIL menggunakan AS 6420, R3-SANGIR menggunakan AS 6430, dan R4-ATTACKER menggunakan AS 6440. Router R4-ATTACKER digunakan sebagai compromised router yang akan mengiklankan rute tidak sah pada skenario route

injection. Namun, pada kondisi baseline, R4-ATTACKER hanya dikonfigurasi sebagai neighbor BGP dengan R1-KOMINFO dan belum mengiklankan prefix apa pun.

Pada implementasi BGP ini, R1-KOMINFO berperan sebagai router utama yang membentuk hubungan neighbor dengan R2-CAPIL, R3-SANGIR, dan R4-ATTACKER. Sementara itu, R2-CAPIL dan R3-SANGIR hanya membentuk hubungan neighbor BGP dengan R1-KOMINFO. R4-ATTACKER juga hanya membentuk hubungan neighbor BGP dengan R1-KOMINFO. Pola ini digunakan agar proses masuknya rute tidak sah dari R4 dapat diamati melalui satu titik pengujian, yaitu R1-KOMINFO, sehingga proses mitigasi menggunakan prefix-list dapat diterapkan secara lebih terarah.

Konfigurasi BGP dilakukan dengan mendefinisikan nomor *Autonomous System*, *neighbor* BGP, serta *network* yang akan diiklankan. Contoh konfigurasi BGP pada router R1-KOMINFO adalah sebagai berikut:

```
router bgp 6410
bgp log-neighbor-changes
bgp router-id 192.168.16.1
neighbor 172.16.1.20 remote-as 6420
neighbor 172.16.1.30 remote-as 6430
neighbor 172.16.1.40 remote-as 6440
network 192.168.16.0 mask 255.255.255.0
```

Konfigurasi tersebut menunjukkan bahwa R1-KOMINFO menjalankan BGP pada AS 6410 dan membentuk hubungan *neighbor* dengan R2-CAPIL pada AS 6420, R3-SANGIR pada AS 6430, serta R4-ATTACKER pada AS 6440. Perintah network 192.168.16.0 mask 255.255.255.0 digunakan untuk mengiklankan jaringan PC1 ke dalam proses BGP.

Konfigurasi pada R2-CAPIL dilakukan dengan mendefinisikan AS 6420, *neighbor* menuju R1-KOMINFO, serta *network* jaringan PC2



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

yang akan diiklankan ke dalam BGP. Contoh konfigurasi pada R2-CAPIL adalah sebagai berikut:

```
router bgp 6420
bgp log-neighbor-changes
bgp router-id 192.168.17.1
neighbor 172.16.1.254 remote-as 6410
network 192.168.17.0 mask 255.255.255.0
```

Konfigurasi tersebut menunjukkan bahwa R2-CAPIL menjalankan BGP pada AS 6420 dan membentuk hubungan *neighbor* dengan R1-KOMINFO melalui alamat 172.16.1.254. Perintah network 192.168.17.0 mask 255.255.255.0 digunakan untuk mengiklankan jaringan PC2 ke dalam proses BGP.

Sedangkan konfigurasi pada R3-SANGIR dilakukan dengan mendefinisikan AS 6430, *neighbor* menuju R1-KOMINFO, serta *network* jaringan PC3. Contoh konfigurasi pada R3-SANGIR adalah sebagai berikut:

```
router bgp 6430
bgp log-neighbor-changes
bgp router-id 192.168.18.1
neighbor 172.16.1.254 remote-as 6410
network 192.168.18.0 mask 255.255.255.0
```

Konfigurasi tersebut menunjukkan bahwa R3-SANGIR menjalankan BGP pada AS 6430 dan membentuk hubungan *neighbor* dengan R1-KOMINFO melalui alamat 172.16.1.254. Perintah network 192.168.18.0 mask 255.255.255.0 digunakan untuk mengiklankan jaringan PC3 ke dalam proses BGP.

Pada router R4-ATTACKER, konfigurasi BGP dilakukan agar R4 dapat membentuk hubungan neighbor dengan R1-KOMINFO. Pada kondisi baseline, R4 belum diberikan konfigurasi network, sehingga R4 belum mengiklankan prefix apa pun ke dalam BGP. Contoh konfigurasi pada R4-ATTACKER adalah sebagai berikut:



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
router bgp 6440
bgp log-neighbor-changes
bgp router-id 4.4.4.4
neighbor 172.16.1.254 remote-as 6410
```

Konfigurasi tersebut menunjukkan bahwa R4-ATTACKER menjalankan BGP pada AS 6440 dan membentuk hubungan neighbor dengan R1-KOMINFO. Pada tahap baseline, R4-ATTACKER belum mengiklankan prefix tertentu. Hal ini dilakukan agar R4 hanya berada dalam kondisi siap sebagai neighbor BGP, sedangkan skenario route injection belum dijalankan.

Setelah konfigurasi BGP dilakukan, verifikasi dilakukan menggunakan perintah berikut:

show ip bgp summary

Perintah show ip bgp summary digunakan untuk melihat status *neighbor* BGP dan jumlah prefix yang diterima dari masing-masing *neighbor*. Selain itu, perintah show ip bgp dan show ip route juga digunakan untuk memastikan bahwa rute dari masing-masing jaringan telah masuk ke tabel BGP dan *routing table*. Hasil verifikasi *neighbor* BGP pada R1-KOMINFO ditunjukkan pada Gambar 4.3.

```
R1-KOMINFO#show ip bgp summary
BGP router identifier 192.168.16.1, local AS number 6410
BGP table version is 4, main routing table version 4
3 network entries using 432 bytes of memory
3 path entries using 240 bytes of memory
3/3 BGP path/bestpath attribute entries using 408 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1128 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.20     4         6420       8      10        4    0    0 00:04:08        1
172.16.1.30     4         6430       8      10        4    0    0 00:03:59        1
172.16.1.40     4         6440       7      10        4    0    0 00:03:54        0
```

Gambar 4.3 Hasil Verifikasi Neighbor BGP pada R1-KOMINFO

Berdasarkan Gambar 4.3, bagian yang diberi tanda menunjukkan informasi neighbor BGP pada router R1-KOMINFO. Kolom Neighbor menunjukkan alamat IP router tetangga yang membentuk sesi BGP dengan R1, yaitu 172.16.1.20 sebagai R2-CAPIL,

172.16.1.30 sebagai R3-SANGIR, dan 172.16.1.40 sebagai R4-ATTACKER. Kolom AS menunjukkan nomor Autonomous System dari masing-masing neighbor, yaitu AS 6420, AS 6430, dan AS 6440.

Kolom MsgRcvd dan MsgSent menunjukkan jumlah pesan BGP yang diterima dan dikirim selama sesi BGP berjalan. Kolom Up/Down menunjukkan lama waktu sesi BGP telah aktif. Sementara itu, kolom State/PfxRcd menunjukkan status sesi BGP atau jumlah prefix yang diterima dari neighbor. Pada neighbor R2-CAPIL dan R3-SANGIR, nilai State/PfxRcd bernilai 1, yang menunjukkan bahwa R1-KOMINFO menerima satu prefix dari masing-masing router tersebut. Prefix yang diterima dari R2-CAPIL adalah jaringan 192.168.17.0/24, sedangkan prefix yang diterima dari R3-SANGIR adalah jaringan 192.168.18.0/24.

Pada neighbor R4-ATTACKER, nilai State/PfxRcd bernilai 0. Kondisi tersebut menunjukkan bahwa sesi BGP antara R1-KOMINFO dan R4-ATTACKER telah terbentuk, tetapi R4 belum mengiklankan prefix apa pun. Dengan demikian, kondisi tersebut masih termasuk baseline karena skenario route injection belum dilakukan. Kondisi baseline ini kemudian digunakan sebagai acuan sebelum dilakukan pengujian route injection dan penerapan mitigasi menggunakan prefix-list.

### 4.3.2 Implementasi *Routing EIGRP*

Implementasi *routing* EIGRP dilakukan pada topologi EIGRP dengan menggunakan struktur perangkat yang sama, yaitu R1-KOMINFO, R2-CAPIL, R3-SANGIR, dan R4-ATTACKER. Pada topologi ini, seluruh router menjalankan EIGRP AS 100 untuk membangun hubungan *routing* pada jaringan internal. Sebelum konfigurasi EIGRP dilakukan, konfigurasi *routing* dan route serangan dari pengujian sebelumnya dibersihkan atau dinonaktifkan terlebih dahulu agar tidak memengaruhi hasil pengujian EIGRP.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Router R4-ATTACKER digunakan sebagai compromised router yang akan memasukkan rute tidak sah pada skenario route injection. Namun, pada kondisi baseline, R4-ATTACKER hanya dikonfigurasi sebagai neighbor EIGRP dan belum diberikan static route palsu maupun konfigurasi redistribution. Hal ini dilakukan agar kondisi baseline merepresentasikan jaringan normal sebelum route injection dilakukan.

Konfigurasi EIGRP dilakukan dengan mendefinisikan nomor AS dan network yang terhubung pada masing-masing router. Contoh konfigurasi EIGRP pada router R1-KOMINFO adalah sebagai berikut:

```
router eigrp 100
no auto-summary
network 172.16.1.0 0.0.0.255
network 192.168.16.0 0.0.0.255
```

Konfigurasi tersebut menunjukkan bahwa R1-KOMINFO menjalankan EIGRP AS 100. Perintah no auto-summary digunakan untuk menonaktifkan summarization otomatis. Network 172.16.1.0/24 digunakan sebagai jaringan transit antarrouter, sedangkan network 192.168.16.0/24 merupakan jaringan client PC1.

Konfigurasi pada R2-CAPIL dilakukan dengan menyesuaikan network transit dan network client PC2. Contoh konfigurasi pada R2-CAPIL adalah sebagai berikut:

```
router eigrp 100
no auto-summary
network 172.16.1.0 0.0.0.255
network 192.168.17.0 0.0.0.255
```



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Konfigurasi tersebut menunjukkan bahwa R2-CAPIL menjalankan EIGRP AS 100 dan mengiklankan jaringan transit serta jaringan PC2 ke dalam proses EIGRP.

Konfigurasi pada R3-SANGIR juga dilakukan dengan menyesuaikan network transit dan network client PC3. Contoh konfigurasi pada R3-SANGIR adalah sebagai berikut:

```
router eigrp 100
no auto-summary
network 172.16.1.0 0.0.0.255
network 192.168.18.0 0.0.0.255
```

Konfigurasi tersebut menunjukkan bahwa R3-SANGIR menjalankan EIGRP AS 100 dan mengiklankan jaringan transit serta jaringan PC3 ke dalam proses EIGRP.

Pada router R4-ATTACKER, konfigurasi EIGRP dilakukan agar R4 dapat membentuk hubungan neighbor dengan router lain melalui jaringan transit. Contoh konfigurasi pada R4-ATTACKER adalah sebagai berikut:

```
router eigrp 100
no auto-summary
network 172.16.1.0 0.0.0.255
```

Konfigurasi tersebut menunjukkan bahwa R4-ATTACKER menjalankan EIGRP AS 100 dan terhubung pada jaringan transit 172.16.1.0/24. Pada tahap baseline, R4-ATTACKER belum diberikan konfigurasi tambahan untuk melakukan route injection. Dengan demikian, R4 hanya berperan sebagai neighbor EIGRP, tetapi belum menyebarkan rute tidak sah ke router lain.

Setelah konfigurasi EIGRP dilakukan, verifikasi dilakukan menggunakan perintah berikut:

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
show ip eigrp neighbors
show ip route
```

Perintah show ip eigrp neighbors digunakan untuk memastikan hubungan neighbor EIGRP telah terbentuk antarrouter. Sementara itu, perintah show ip route digunakan untuk melihat rute yang diperoleh melalui EIGRP. Hasil verifikasi neighbor EIGRP ditunjukkan pada Gambar 4.4.

```
R1-KOMINFO#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   172.16.1.30             Fa0/0                    14 00:07:21   33   198  0  6
1   172.16.1.40             Fa0/0                    13 00:07:21   46   276  0  6
0   172.16.1.20             Fa0/0                    11 00:07:21   33   198  0  6
R1-KOMINFO#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.12.0/24 is directly connected, FastEthernet1/0
L        10.0.12.254/32 is directly connected, FastEthernet1/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, FastEthernet0/0
L        172.16.1.254/32 is directly connected, FastEthernet0/0
      192.168.16.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.16.0/24 is directly connected, FastEthernet0/1
L        192.168.16.1/32 is directly connected, FastEthernet0/1
D     192.168.17.0/24 [90/30720] via 172.16.1.20, 00:07:19, FastEthernet0/0
D     192.168.18.0/24 [90/30720] via 172.16.1.30, 00:07:19, FastEthernet0/0
```

Gambar 4.4 Verifikasi Neighbor EIGRP pada Router R1-KOMINFO

Berdasarkan Gambar 4.4, bagian atas yang diberi tanda menunjukkan hasil perintah show ip eigrp neighbors pada router R1-KOMINFO. Hasil tersebut menunjukkan bahwa R1-KOMINFO telah berhasil membentuk hubungan neighbor EIGRP dengan tiga router, yaitu 172.16.1.20 sebagai R2-CAPIL, 172.16.1.30 sebagai R3-SANGIR, dan 172.16.1.40 sebagai R4-ATTACKER. Seluruh neighbor tersebut terbentuk melalui interface FastEthernet0/0 yang terhubung pada jaringan transit 172.16.1.0/24.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Kolom Hold menunjukkan waktu tunggu sebelum neighbor dianggap tidak aktif apabila tidak ada paket hello yang diterima. Kolom Uptime menunjukkan lama hubungan neighbor EIGRP telah terbentuk. Kolom SRTT, RTO, Q Cnt, dan Seq Num menunjukkan informasi teknis terkait proses pertukaran paket EIGRP, seperti waktu respons, waktu retransmission, jumlah antrean paket, dan nomor urut update. Nilai-nilai tersebut menunjukkan status hubungan neighbor EIGRP, bukan jumlah prefix yang diterima.

Pada bagian bawah yang diberi tanda, terlihat hasil perintah show ip route yang digunakan untuk memverifikasi *routing* table pada R1-KOMINFO. *Routing* table tersebut menunjukkan adanya route connected yang ditandai dengan kode C, alamat local interface yang ditandai dengan kode L, serta route EIGRP internal yang ditandai dengan kode D.

Route menuju jaringan 192.168.17.0/24 diperoleh melalui next-hop 172.16.1.20, yaitu R2-CAPIL. Sementara itu, route menuju jaringan 192.168.18.0/24 diperoleh melalui next-hop 172.16.1.30, yaitu R3-SANGIR. Hal ini menunjukkan bahwa pada kondisi baseline, R1-KOMINFO telah menerima informasi *routing* EIGRP secara normal menuju jaringan client PC2 dan PC3.

Pada *routing* table tersebut belum terdapat route external EIGRP dengan kode D EX yang berasal dari R4-ATTACKER. Dengan demikian, kondisi pada Gambar 4.4 masih menunjukkan baseline EIGRP, karena R4-ATTACKER sudah menjadi neighbor EIGRP tetapi belum melakukan route injection.

### 4.3.3 Verifikasi Konektivitas Jaringan

Setelah konfigurasi *routing* BGP dan EIGRP selesai dilakukan, tahap selanjutnya adalah melakukan verifikasi konektivitas jaringan. Verifikasi ini bertujuan untuk memastikan bahwa setiap client dapat

saling berkomunikasi melalui jalur *routing* yang telah terbentuk pada kondisi baseline. Pada tahap ini, pengujian belum digunakan untuk menganalisis nilai Quality of Service (QoS) secara rinci, karena pembahasan data delay, throughput, dan packet loss disajikan pada subbab 4.4.

Pada penelitian ini, pengujian konektivitas dilakukan pada tiga client, yaitu PC1, PC2, dan PC3. PC1 menggunakan alamat IP 192.168.16.2/24 dengan default gateway 192.168.16.1, PC2 menggunakan alamat IP 192.168.17.2/24 dengan default gateway 192.168.17.1, dan PC3 menggunakan alamat IP 192.168.18.2/24 dengan default gateway 192.168.18.1. Pengujian dilakukan menggunakan perintah ping untuk memastikan komunikasi antar-client dapat berjalan sebelum skenario route injection diterapkan.

Contoh pengujian konektivitas dari PC1 menuju PC2 dan PC3 adalah sebagai berikut:

```
ping 192.168.17.2
ping 192.168.18.2
```

Pengujian tersebut dilakukan pada kondisi baseline, yaitu kondisi ketika *routing* telah berjalan normal dan belum terdapat pengiklanan rute tidak sah dari R4-ATTACKER. Pada kondisi ini, R4 hanya berperan sebagai router yang terhubung dalam topologi, sedangkan skenario route injection belum dijalankan.

Hasil pengujian konektivitas pada kondisi baseline ditunjukkan pada Gambar 4.5.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
PC1> ping 192.168.17.2
84 bytes from 192.168.17.2 icmp_seq=1 ttl=62 time=76.143 ms
84 bytes from 192.168.17.2 icmp_seq=2 ttl=62 time=61.945 ms
84 bytes from 192.168.17.2 icmp_seq=3 ttl=62 time=60.748 ms
84 bytes from 192.168.17.2 icmp_seq=4 ttl=62 time=60.518 ms
84 bytes from 192.168.17.2 icmp_seq=5 ttl=62 time=62.692 ms

PC1> ping 192.168.18.2
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=77.210 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.867 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=60.635 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=60.780 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=61.933 ms
```

Gambar 4.5 Pengujian Konektivitas pada Kondisi Baseline

Berdasarkan Gambar 4.5, pengujian konektivitas dilakukan dari PC1 menuju PC2 dengan alamat IP 192.168.17.2 dan dari PC1 menuju PC3 dengan alamat IP 192.168.18.2. Hasil pengujian menunjukkan bahwa kedua alamat tujuan memberikan balasan berupa reply. Hal ini ditunjukkan dengan munculnya keterangan 84 bytes from 192.168.17.2 dan 84 bytes from 192.168.18.2 pada hasil ping.

Nilai icmp_seq menunjukkan urutan paket ICMP yang dikirim, sedangkan ttl menunjukkan Time To Live atau batas jumlah hop yang dapat dilalui paket sebelum dibuang. Pada hasil pengujian, nilai ttl sebesar 62 menunjukkan bahwa paket berhasil melewati perangkat *routing* hingga sampai ke tujuan. Sementara itu, nilai time menunjukkan waktu tempuh paket dari PC1 menuju alamat tujuan dan kembali lagi ke PC1 dalam satuan milidetik.

Dengan adanya balasan dari PC2 dan PC3, dapat disimpulkan bahwa komunikasi antar-client pada kondisi baseline telah berjalan dengan baik. Kondisi ini menunjukkan bahwa rute antarjaringan sudah terbentuk sebelum dilakukan skenario route injection.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## 4.4 Pengujian

Pengujian dilakukan untuk mengetahui kondisi jaringan pada tiga skenario, yaitu *baseline*, *route injection*, dan setelah penerapan mitigasi *basic filtering* menggunakan *prefix-list*. Pengujian dilakukan pada dua topologi *routing*, yaitu BGP dan EIGRP. Pada kondisi *baseline*, seluruh router telah dikonfigurasi sesuai dengan protokol yang digunakan dan hubungan *neighbor* telah terbentuk. Pada topologi BGP, R1-KOMINFO telah membentuk hubungan *neighbor* dengan R2-CAPIL, R3-SANGIR, dan R4-ATTACKER. R2-CAPIL dan R3-SANGIR telah mengiklankan *prefix* valid, sedangkan R4-ATTACKER belum mengiklankan *prefix* apa pun. Pada topologi EIGRP, R4-ATTACKER juga telah membentuk hubungan *neighbor* EIGRP, tetapi belum menyebarkan rute tidak sah.

Pengujian ini bertujuan untuk mengamati perubahan informasi *routing*, dampak masuknya rute tidak sah terhadap konektivitas jaringan, serta efektivitas *prefix-list* dalam menolak rute tersebut agar komunikasi tetap menggunakan jalur yang valid. Ketiga skenario digunakan untuk mengamati perubahan jaringan secara bertahap, mulai dari kondisi normal, kondisi saat *route injection* terjadi, hingga kondisi setelah mitigasi diterapkan.

Aspek keamanan yang diuji berfokus pada keamanan *control plane routing*. Serangan *route injection* digunakan untuk menguji apakah *prefix* tidak sah yang diiklankan atau dimasukkan oleh R4-ATTACKER dapat diterima oleh router dan memengaruhi proses pemilihan jalur. *Prefix* yang diuji terdiri dari 192.168.16.2/32 untuk PC1, 192.168.17.2/32 untuk PC2, dan 192.168.18.2/32 untuk PC3. Apabila rute tersebut diterima, integritas informasi *routing* dapat terganggu dan dapat menyebabkan perubahan jalur komunikasi, *timeout*, *destination host unreachable*, atau *packet loss*.

Pengamatan dilakukan melalui perubahan *routing table* dan *next-hop*, konektivitas antar-client, hasil *ping* dan *traceroute*, waktu konvergensi atau pemulihan, serta parameter *Quality of Service* (QoS) yang meliputi *delay*, *throughput*, dan *packet loss*. Pada BGP, pengamatan dilakukan melalui

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

status *neighbor*, jumlah *prefix* yang diterima, serta perubahan jalur pada tabel BGP. Pada EIGRP, pengamatan dilakukan melalui hubungan *neighbor*, munculnya rute eksternal dengan kode D EX, serta perubahan jalur setelah rute tidak sah dimasukkan.

Data hasil pengujian kemudian dibandingkan antara kondisi *baseline*, saat *route injection*, dan setelah penerapan *prefix-list*. Perbandingan tersebut digunakan untuk menilai dampak *route injection* terhadap kestabilan jaringan serta efektivitas *basic filtering* dalam mencegah rute tidak sah memengaruhi proses *routing*.

### 4.4.1 Deskripsi Pengujian

Pengujian dilakukan menggunakan GNS3 pada dua topologi, yaitu BGP dan EIGRP. Pengujian terdiri dari tiga kondisi, yaitu *baseline*, *route injection*, dan setelah penerapan *basic filtering* menggunakan *prefix-list*. Ketiga kondisi tersebut digunakan untuk mengamati perubahan *routing table*, *next-hop*, konektivitas antar-client, waktu konvergensi atau pemulihan, serta parameter QoS berupa *delay*, *throughput*, dan *packet loss*.

Pada kondisi *baseline* BGP, R1-KOMINFO telah membentuk hubungan *neighbor* dengan R2-CAPIL, R3-SANGIR, dan R4-ATTACKER. R2-CAPIL dan R3-SANGIR telah mengiklankan *prefix* valid, sedangkan R4-ATTACKER belum mengiklankan *prefix* apa pun. Pada kondisi *baseline* EIGRP, R4-ATTACKER juga telah menjadi *neighbor* dalam EIGRP AS 100, tetapi belum memasukkan rute tidak sah. Kondisi *baseline* digunakan sebagai acuan untuk membandingkan perubahan yang terjadi saat *route injection* dan setelah *filtering* diterapkan.

Serangan dilakukan dengan membuat R4-ATTACKER mengiklankan atau memasukkan *prefix host* /32 yang tidak sah. *Prefix* yang digunakan dalam pengujian adalah 192.168.16.2/32 untuk PC1, 192.168.17.2/32 untuk PC2, dan 192.168.18.2/32 untuk PC3. Pada BGP, *prefix* tidak sah diiklankan melalui sesi *neighbor*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

antara R4-ATTACKER dan R1-KOMINFO. Pada EIGRP, *prefix* tidak sah dimasukkan ke dalam proses EIGRP sehingga dapat dipelajari oleh router lain sebagai rute eksternal dengan kode D EX.

Penggunaan *prefix* /32 dilakukan karena rute *host* lebih spesifik dibandingkan rute *network* /24 yang valid. Berdasarkan mekanisme *longest prefix match*, router dapat memilih rute /32 apabila rute tersebut masuk ke *routing table*. Kondisi ini dapat menyebabkan perubahan *next-hop* dan jalur komunikasi menuju target yang diuji.

R4-ATTACKER diasumsikan mengetahui alamat target karena penelitian dilakukan dalam lingkungan simulasi terkontrol. Penelitian ini tidak membahas proses pencarian informasi atau *reconnaissance*, tetapi berfokus pada dampak setelah rute tidak sah diiklankan atau dimasukkan ke dalam protokol *routing*. Rute dari R4 dapat diterima secara teknis karena dikirim melalui mekanisme pertukaran informasi *routing* yang sah. Namun, rute tersebut tidak sah dari sisi keamanan karena R4 bukan pemilik jaringan tujuan.

Setelah dampak serangan diperoleh, mitigasi diterapkan menggunakan *prefix-list*. Pada BGP, *prefix-list* diterapkan secara *inbound* pada *neighbor* R4-ATTACKER. Pada EIGRP, *prefix-list* diterapkan melalui *distribute-list* pada antarmuka jaringan transit. Pengujian kemudian diulang untuk memastikan *prefix* tidak sah ditolak dan komunikasi kembali menggunakan rute valid.

### 4.4.2 Prosedur Pengujian

Prosedur pengujian dilakukan untuk mengevaluasi dampak *route injection* dan efektivitas *basic filtering* menggunakan *prefix-list* pada protokol BGP dan EIGRP. Pengujian membandingkan kondisi sebelum serangan, saat serangan, dan setelah mitigasi. Perbandingan dilakukan berdasarkan perubahan *routing table*, konektivitas antar-client, waktu konvergensi atau pemulihan, serta parameter QoS berupa *delay*, *throughput*, dan *packet loss*.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tahapan pengujian yang dilakukan adalah sebagai berikut:

1. Penyusunan Skenario Pengujian

   Skenario pengujian disusun berdasarkan tiga kondisi, yaitu *baseline*, *route injection*, dan setelah penerapan *prefix-list*. Skenario yang sama diterapkan pada topologi BGP dan EIGRP agar dampak serangan serta hasil mitigasi pada kedua protokol dapat dibandingkan. Pengujian dilakukan terhadap tiga *host* tujuan, yaitu PC1, PC2, dan PC3.
2. Pengujian Baseline

   Pada topologi BGP, R1-KOMINFO telah membentuk hubungan *neighbor* dengan R2-CAPIL, R3-SANGIR, dan R4-ATTACKER. R2-CAPIL dan R3-SANGIR telah mengiklankan *prefix* valid, sedangkan R4-ATTACKER belum mengiklankan *prefix* apa pun. Pada topologi EIGRP, R4-ATTACKER juga telah menjadi *neighbor* dalam EIGRP AS 100, tetapi belum memasukkan rute tidak sah. Pengujian dilakukan dengan memeriksa *routing table*, menjalankan *ping* dan *traceroute* antar-client, serta melakukan *capture* paket menggunakan Wireshark.
3. Pengujian Route Injection

   Pada tahap ini, R4-ATTACKER mengiklankan atau memasukkan *prefix* tidak sah terhadap masing-masing target pengujian. *Prefix* yang digunakan adalah 192.168.16.2/32 untuk PC1, 192.168.17.2/32 untuk PC2, dan 192.168.18.2/32 untuk PC3. Pada BGP, *prefix* tersebut diiklankan melalui sesi *neighbor* R4-ATTACKER dengan R1-KOMINFO. Pada EIGRP, *prefix* tersebut dimasukkan ke dalam proses EIGRP sehingga dapat dipelajari sebagai rute eksternal dengan kode D EX. Setelah serangan dijalankan, dilakukan pengamatan terhadap *routing table*, *next-hop*, hasil *ping* dan *traceroute*, waktu konvergensi, serta hasil *capture* Wireshark.

4. Pengujian Setelah Filtering

   Setelah dampak *route injection* diamati, mitigasi diterapkan menggunakan *prefix-list* untuk menolak *prefix* tidak sah dari R4-ATTACKER. Pada BGP, *prefix-list* diterapkan secara *inbound* pada *neighbor* R4-ATTACKER. Pada EIGRP, *prefix-list* diterapkan melalui *distribute-list* pada antarmuka jaringan transit. Pengujian kemudian diulang untuk mengamati *routing table*, konektivitas, waktu pemulihan, dan parameter QoS.

5. Analisis Hasil Pengujian

   Hasil kondisi *baseline*, saat *route injection*, dan setelah *filtering* dibandingkan pada masing-masing protokol. Analisis dilakukan berdasarkan perubahan *routing table*, konektivitas, waktu konvergensi atau pemulihan, serta nilai *delay*, *throughput*, dan *packet loss*.

### 4.4.3 Data Hasil Pengujian

Data hasil pengujian disajikan berdasarkan urutan kondisi jaringan, yaitu kondisi *baseline*, kondisi saat terjadi *route injection*, kondisi setelah penerapan mitigasi *basic filtering* menggunakan *prefix-list*, serta hasil pengujian *traceroute*. Penyajian data dilakukan secara berurutan agar perubahan kondisi jaringan dapat diamati dengan jelas, mulai dari kondisi normal, kondisi saat rute tidak sah masuk ke proses *routing*, hingga kondisi jaringan kembali pulih setelah mitigasi diterapkan.

#### 4.4.3.1 Hasil Pengujian Kondisi Baseline

Data hasil pengujian disajikan berdasarkan urutan kondisi jaringan, yaitu kondisi *baseline*, kondisi saat terjadi *route injection*, kondisi setelah penerapan mitigasi *basic filtering* menggunakan *prefix-list*, serta hasil pengujian *traceroute*. Penyajian data dilakukan secara berurutan agar perubahan kondisi jaringan dapat diamati dengan jelas, mulai dari kondisi normal, kondisi saat rute tidak sah masuk ke proses *routing*,



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

hingga kondisi jaringan kembali pulih setelah mitigasi diterapkan.

Kondisi *baseline* digunakan sebagai acuan awal sebelum skenario *route injection* diterapkan. Pada kondisi ini, router telah dikonfigurasi sesuai dengan protokol *routing* yang digunakan dan konektivitas antar-*client* diuji menggunakan perintah *ping*. Pengujian dilakukan pada dua topologi, yaitu topologi BGP dan topologi EIGRP, untuk memastikan bahwa masing-masing jaringan berada dalam kondisi normal sebelum rute tidak sah dimasukkan oleh R4-ATTACKER.

Pada kondisi *baseline*, pengujian dilakukan pada jalur komunikasi antar-*client*, yaitu PC1 ke PC2, PC1 ke PC3, dan PC2 ke PC3. Selain pengujian menggunakan *ping*, pengamatan juga dilakukan menggunakan Wireshark untuk memastikan adanya paket ICMP *Echo Request* dan *Echo Reply*. Hasil pengujian pada kondisi *baseline* disajikan secara terpisah berdasarkan topologi BGP dan EIGRP.

a. Hasil Pengujian Baseline pada Topologi BGP

Pengujian *baseline* pada topologi BGP dilakukan untuk memastikan bahwa komunikasi antar-*client* dapat berjalan melalui jalur *routing* BGP yang telah terbentuk. Pada tahap ini, belum terdapat rute tidak sah dari R4-ATTACKER yang digunakan dalam proses *routing*. Pengujian dilakukan dengan mengirim paket ICMP dari PC1 ke PC2, PC1 ke PC3, dan PC2 ke PC3. Hasil pengujian *ping* pada topologi BGP ditunjukkan pada Gambar 4.6.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

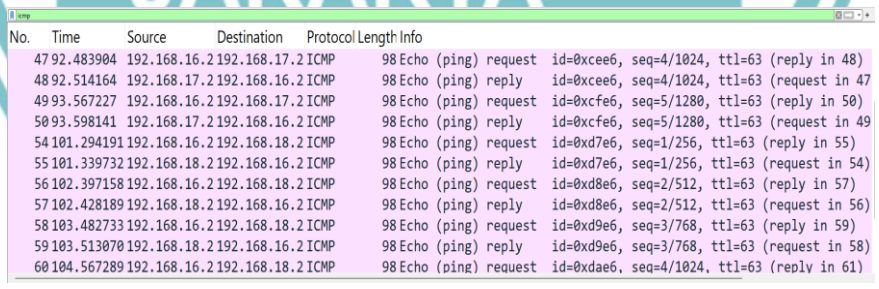
```
PC1> ping 192.168.17.2
84 bytes from 192.168.17.2 icmp_seq=1 ttl=62 time=77.497 ms
84 bytes from 192.168.17.2 icmp_seq=2 ttl=62 time=60.258 ms
84 bytes from 192.168.17.2 icmp_seq=3 ttl=62 time=60.603 ms
84 bytes from 192.168.17.2 icmp_seq=4 ttl=62 time=60.334 ms
84 bytes from 192.168.17.2 icmp_seq=5 ttl=62 time=61.335 ms

PC1> ping 192.168.18.2
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=77.224 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=63.480 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.892 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=62.512 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=60.692 ms
```

Gambar 4.6 Hasil Pengujian Ping Baseline pada Topologi BGP

Berdasarkan Gambar 4.6, bagian yang diberi tanda menunjukkan bahwa setiap *client* memperoleh balasan berupa *reply* dari alamat tujuan. Hal ini menunjukkan bahwa jalur komunikasi antar-*client* pada topologi BGP telah berjalan dengan baik. Dengan demikian, topologi BGP berada pada kondisi normal sebelum skenario *route injection* diterapkan.

Selain menggunakan *ping*, pengamatan paket juga dilakukan menggunakan Wireshark. Pengamatan ini bertujuan untuk memastikan bahwa komunikasi ICMP benar-benar terjadi secara dua arah melalui paket *Echo Request* dan *Echo Reply*. Hasil *capture* ICMP pada topologi BGP ditunjukkan pada Gambar 4.7.




Gambar 4.7 Capture ICMP Baseline pada Topologi BGP

Berdasarkan Gambar 4.7, bagian yang diberi tanda terlihat adanya paket ICMP *Echo Request* yang dikirim oleh *client*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

sumber dan paket ICMP *Echo Reply* yang diterima dari *client* tujuan. Adanya pasangan paket tersebut menunjukkan bahwa komunikasi dua arah pada topologi BGP berhasil dilakukan pada kondisi *baseline*. Hasil pengukuran QoS pada kondisi *baseline* topologi BGP ditunjukkan pada Tabel 4.7.

Tabel 4.7 Hasil Pengujian QoS Baseline pada Topologi BGP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Baseline | PC1 ke PC2 | 30 | 30 | 0 | 0% | 164,41 ms | 1,413 Kbps |
| Baseline | PC1 ke PC3 | 30 | 30 | 0 | 0% | 31,12 ms | 1,495 Kbps |
| Baseline | PC2 ke PC3 | 30 | 30 | 0 | 0% | 164,89 ms | 1,413 Kbps |
| Rata-rata | - | 30 | 30 | 0 | 0% | 120,14 ms | 1,440 Kbps |

Berdasarkan Tabel 4.7, seluruh alur komunikasi pada topologi BGP berhasil menerima 30 paket dari total 30 paket yang dikirim. Nilai *packet loss* pada seluruh alur sebesar 0%, sehingga dapat disimpulkan bahwa tidak terdapat kehilangan paket pada kondisi *baseline*. Nilai rata-rata *delay* pada kondisi ini adalah 120,14 ms, sedangkan rata-rata *throughput* sebesar 1,440 Kbps. Kondisi ini menunjukkan bahwa sebelum *route injection* dilakukan, komunikasi antar-*client* pada topologi BGP berada dalam keadaan normal dan stabil.

b. Hasil Pengujian Baseline pada Topologi EIGRP

Pengujian *baseline* pada topologi EIGRP dilakukan dengan metode yang sama, yaitu menggunakan perintah *ping* antar-*client*. Pengujian ini bertujuan untuk memastikan bahwa proses pertukaran informasi *routing* pada EIGRP telah berjalan dan jalur komunikasi antar-*client* berada dalam kondisi normal sebelum skenario *route injection* diterapkan. Hasil pengujian *ping* pada topologi EIGRP ditunjukkan pada Gambar 4.8.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
PC1> ping 192.168.17.2
84 bytes from 192.168.17.2 icmp_seq=1 ttl=62 time=62.659 ms
84 bytes from 192.168.17.2 icmp_seq=2 ttl=62 time=60.545 ms
84 bytes from 192.168.17.2 icmp_seq=3 ttl=62 time=61.054 ms
84 bytes from 192.168.17.2 icmp_seq=4 ttl=62 time=60.247 ms
84 bytes from 192.168.17.2 icmp_seq=5 ttl=62 time=62.265 ms

PC1> ping 192.168.18.2
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=61.259 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.870 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.196 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=61.059 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=62.070 ms
```

Gambar 4.8 Hasil Pengujian Ping Baseline pada Topologi EIGRP

Berdasarkan Gambar 4.8, bagian yang diberi tanda menunjukkan bahwa setiap *client* pada topologi EIGRP memperoleh balasan berupa *reply* dari alamat tujuan. Kondisi ini menunjukkan bahwa jalur komunikasi antar-*client* telah terbentuk dengan baik melalui protokol EIGRP. Dengan demikian, topologi EIGRP juga berada pada kondisi normal sebelum rute tidak sah dari R4-ATTACKER diiklankan.

Selanjutnya, Wireshark digunakan untuk mengamati paket ICMP selama proses pengujian konektivitas berlangsung. Hasil *capture* ICMP pada topologi EIGRP ditunjukkan pada Gambar 4.9.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 617 | 580.901892 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x96e4, seq=5/1280, ttl=63 (request in 616 |
| 623 | 586.135767 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x9be4, seq=1/256, ttl=63 (reply in 624) |
| 624 | 586.166703 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x9be4, seq=1/256, ttl=63 (request in 623) |
| 628 | 587.222286 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x9ce4, seq=2/512, ttl=63 (reply in 629) |
| 629 | 587.252823 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x9ce4, seq=2/512, ttl=63 (request in 628) |
| 632 | 588.306076 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x9de4, seq=3/768, ttl=63 (reply in 633) |
| 633 | 588.336534 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x9de4, seq=3/768, ttl=63 (request in 632) |
| 634 | 589.391405 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x9ee4, seq=4/1024, ttl=63 (reply in 635) |
| 635 | 589.422671 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x9ee4, seq=4/1024, ttl=63 (request in 634 |
| 637 | 590.475190 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x9fe4, seq=5/1280, ttl=63 (reply in 639) |
| 639 | 590.506217 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x9fe4, seq=5/1280, ttl=63 (request in 637 |

Gambar 4.9 Capture ICMP Baseline pada Topologi EIGRP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Gambar 4.9, bagian yang diberi tanda terlihat adanya paket ICMP *Echo Request* dan *Echo Reply* pada komunikasi antar-*client*. Hal ini membuktikan bahwa komunikasi dua arah pada topologi EIGRP berhasil dilakukan pada kondisi *baseline*. Hasil pengukuran QoS pada kondisi *baseline* topologi EIGRP ditunjukkan pada Tabel 4.8.

Tabel 4.8 Hasil Pengujian QoS Baseline pada Topologi EIGRP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Baseline | PC2 ke PC1 | 30 | 30 | 0 | 0% | 30,51 ms | 1,497 Kbps |
| Baseline | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,52 ms | 1,499 Kbps |
| Baseline | PC2 ke PC3 | 30 | 30 | 0 | 0% | 31,04 ms | 1,499 Kbps |
| Rata-rata | - | 30 | 30 | 0 | 0% | 30,69 ms | 1,498 Kbps |

Berdasarkan Tabel 4.8, seluruh alur komunikasi pada topologi EIGRP berhasil memperoleh balasan *Echo Reply*. Dari 30 paket yang dikirim pada setiap alur, seluruh paket berhasil diterima kembali sehingga nilai *packet loss* sebesar 0%. Nilai rata-rata *delay* pada kondisi *baseline* EIGRP adalah 30,69 ms, sedangkan rata-rata *throughput* sebesar 1,498 Kbps. Hal ini menunjukkan bahwa sebelum *route injection* diterapkan, proses *routing* EIGRP berjalan normal dan komunikasi antar-*client* berada dalam kondisi stabil.

Berdasarkan hasil pengujian pada topologi BGP dan EIGRP, seluruh *client* dapat saling berkomunikasi pada kondisi *baseline*. Hasil *ping* menunjukkan adanya balasan dari alamat tujuan, sedangkan hasil *capture* Wireshark menunjukkan adanya paket ICMP *Echo Request* dan *Echo Reply*. Dengan demikian, kedua topologi dinyatakan berada dalam kondisi normal dan dapat

digunakan sebagai pembanding terhadap kondisi saat *route injection* dan setelah penerapan mitigasi menggunakan *prefix-list*.

#### 4.4.3.2 Hasil Pengujian Kondisi *Route Injection*

Setelah kondisi *baseline* berhasil diverifikasi, tahap berikutnya adalah menjalankan skenario *route injection*. Pada tahap ini, R4-ATTACKER digunakan sebagai *compromised router* untuk mengiklankan atau memasukkan rute tidak sah ke dalam jaringan. Pengujian dilakukan untuk mengetahui apakah rute tidak sah dari R4-ATTACKER dapat diterima oleh router lain, masuk ke dalam *routing table*, memengaruhi proses pemilihan jalur, serta berdampak terhadap konektivitas antar-*client*.

Pada pengujian ini, *route injection* dilakukan terhadap tiga target host, yaitu PC1 dengan alamat 192.168.16.2, PC2 dengan alamat 192.168.17.2, dan PC3 dengan alamat 192.168.18.2. Setiap target diiklankan atau dimasukkan dalam bentuk *prefix host* /32. Penggunaan *prefix* /32 dilakukan karena rute tersebut lebih spesifik dibandingkan rute jaringan asli /24. Dengan demikian, apabila rute /32 tersebut masuk ke *routing table*, router dapat memilih rute tidak sah tersebut berdasarkan prinsip *longest prefix match*.

Ringkasan target *route injection* ditunjukkan pada Tabel 4.9.

Tabel 4.9 Target Route Injection

| No | Target | Alamat Host | Prefix Route Injection | Keterangan |
|---|---|---|---|---|
| 1 | PC1 | 192.168.16.2 | 192.168.16.2/32 | Rute tidak sah menuju host PC1 |
| 2 | PC2 | 192.168.17.2 | 192.168.17.2/32 | Rute tidak sah menuju host PC2 |
| 3 | PC3 | 192.168.18.2 | 192.168.18.2/32 | Rute tidak sah menuju host PC3 |



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Tabel 4.9, seluruh target serangan menggunakan *prefix host* /32. *Prefix* tersebut digunakan untuk menguji apakah rute tidak sah yang lebih spesifik dapat memengaruhi pemilihan jalur pada protokol BGP dan EIGRP.

a. Hasil Pengujian *Route Injection* pada Topologi BGP

Pada topologi BGP, R4-ATTACKER telah terhubung sebagai *neighbor* BGP pada kondisi *baseline*, tetapi belum mengiklankan rute tidak sah. Skenario *route injection* dilakukan dengan mengiklankan *prefix host* /32 dari R4-ATTACKER menuju R1-KOMINFO. Pada pengujian ini, *prefix* yang diuji adalah 192.168.16.2/32, 192.168.17.2/32, dan 192.168.18.2/32.

Agar *prefix* /32 dapat diiklankan melalui BGP, R4-ATTACKER terlebih dahulu dikonfigurasi dengan rute statis menuju Null0. Rute statis tersebut digunakan agar *prefix* tersedia pada *routing table* R4 dan dapat dimasukkan ke dalam proses BGP menggunakan perintah `network`. Konfigurasi *route injection* BGP pada R4-ATTACKER ditunjukkan pada Gambar 4.10.

```
R4-ATTACKER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-ATTACKER(config)#ip route 192.168.17.2 255.255.255.255 Null0
R4-ATTACKER(config)#router bgp 6440
R4-ATTACKER(config-router)# network 192.168.17.2 mask 255.255.255.255
R4-ATTACKER(config-router)#end
R4-ATTACKER#
```

Gambar 4.10 Konfigurasi *Route Injection* pada R4-ATTACKER

Berdasarkan Gambar 4.10, R4-ATTACKER dikonfigurasi dengan rute statis menuju Null0 untuk masing-masing target. Selanjutnya, *prefix* tersebut diiklankan melalui proses BGP AS 6440 menggunakan perintah network dengan *subnet mask* 255.255.255.255. *Prefix* tersebut dianggap tidak sah karena alamat PC1, PC2, dan PC3 bukan merupakan jaringan milik R4-ATTACKER.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Setelah konfigurasi dilakukan pada R4-ATTACKER, verifikasi dilakukan pada R1-KOMINFO untuk memastikan apakah *prefix* tidak sah berhasil diterima melalui BGP. Verifikasi dilakukan menggunakan perintah show ip bgp dan show ip route terhadap masing-masing alamat target. Hasil verifikasi *route injection* BGP ditunjukkan pada Gambar 4.11 sampai Gambar 4.13.

```
R1-KOMINFO#show ip bgp 192.168.16.2
BGP routing table entry for 192.168.16.2/32, version 15
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 10
  6440
    172.16.1.40 from 172.16.1.40 (4.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
R1-KOMINFO#show ip route 192.168.16.2
Routing entry for 192.168.16.2/32
  Known via "bgp 6410", distance 20, metric 0
  Tag 6440, type external
  Last update from 172.16.1.40 00:00:21 ago
  Routing Descriptor Blocks:
  * 172.16.1.40, from 172.16.1.40, 00:00:21 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6440
      MPLS label: none
```

Gambar 4.11 Hasil Verifikasi Route Injection BGP Target PC1

```
R1-KOMINFO#show ip bgp
BGP table version is 5, local router ID is 192.168.16.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  192.168.16.0     0.0.0.0                  0         32768 i
 *>  192.168.17.0     172.16.1.20              0             0 6420 i
 *>  192.168.17.2/32  172.16.1.40              0             0 6440 i
 *>  192.168.18.0     172.16.1.30              0             0 6430 i
R1-KOMINFO#
```

Gambar 4.12 Hasil Verifikasi Route Injection BGP Target PC2

```
R1-KOMINFO#show ip bgp 192.168.18.2
BGP routing table entry for 192.168.18.2/32, version 17
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 14
  6440
    172.16.1.40 from 172.16.1.40 (4.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
R1-KOMINFO#show ip route 192.168.18.2
Routing entry for 192.168.18.2/32
  Known via "bgp 6410", distance 20, metric 0
  Tag 6440, type external
  Last update from 172.16.1.40 00:42:49 ago
  Routing Descriptor Blocks:
  * 172.16.1.40, from 172.16.1.40, 00:42:49 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6440
      MPLS label: none
```

Gambar 4.13 Hasil Verifikasi Route Injection BGP Target PC3

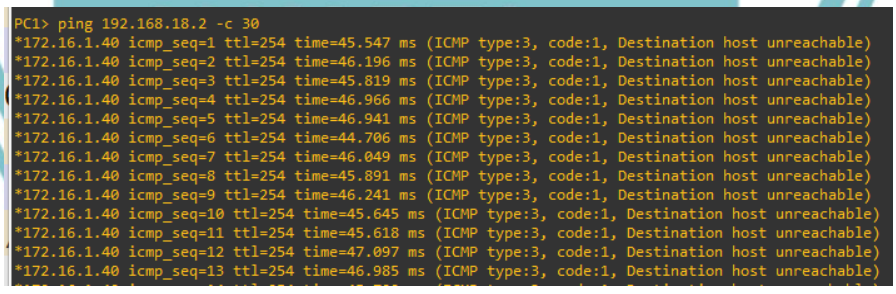
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Gambar 4.11 sampai Gambar 4.13, *prefix* tidak sah berhasil diterima oleh R1-KOMINFO melalui *next-hop* 172.16.1.40, yaitu alamat R4-ATTACKER. Pada tabel BGP, rute yang diterima dari R4 ditandai sebagai rute valid dan dapat dipilih sebagai *best path*. Selain itu, hasil verifikasi pada *routing table* menunjukkan bahwa *prefix host* /32 masuk sebagai rute menuju target yang diuji.

Walaupun rute asli menuju jaringan PC1, PC2, dan PC3 masih tersedia dalam bentuk *prefix* /24, rute tidak sah /32 dari R4-ATTACKER lebih spesifik. Oleh karena itu, trafik menuju host target dapat diarahkan ke R4-ATTACKER berdasarkan prinsip *longest prefix match*. Hal ini menunjukkan bahwa *route injection* pada BGP tidak hanya masuk ke tabel BGP, tetapi juga dapat memengaruhi jalur pengiriman paket.

Setelah perubahan rute teridentifikasi, pengujian dilanjutkan dari sisi *client* untuk mengetahui dampak *route injection* terhadap konektivitas jaringan. Pengujian dilakukan menggunakan perintah *ping* pada alur komunikasi yang melibatkan target serangan. Hasil pengujian *ping* saat *route injection* BGP ditunjukkan pada Gambar 4.14

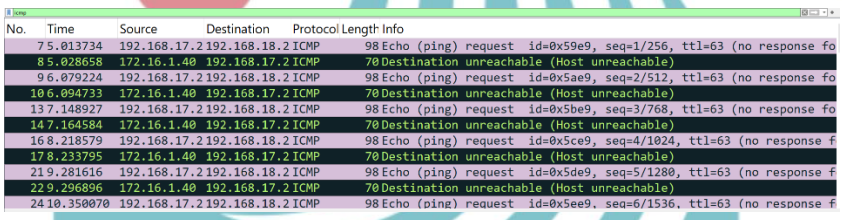



Gambar 4.14 Hasil Pengujian *Ping* Saat *Route Injection* pada Topologi BGP

Berdasarkan Gambar 4.14, terdapat gangguan konektivitas pada alur komunikasi yang menuju target *route injection*. Gangguan tersebut ditunjukkan dengan tidak diterimanya balasan *reply*,

munculnya *request timeout*, atau pesan *destination host unreachable*. Kondisi ini terjadi karena trafik menuju target diarahkan ke R4-ATTACKER melalui rute tidak sah /32, kemudian paket tidak diteruskan ke tujuan sebenarnya karena rute pada R4 diarahkan ke Null0.

Untuk memperkuat hasil pengujian *ping*, dilakukan pengamatan paket menggunakan Wireshark. Pengamatan ini bertujuan untuk melihat apakah paket ICMP yang dikirim oleh *client* memperoleh balasan dari alamat tujuan atau tidak. Hasil *capture* ICMP pada kondisi *route injection* BGP ditunjukkan pada Gambar 4.15.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 7 | 5.013734 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x59e9, seq=1/256, ttl=63 (no response fo |
| 8 | 5.028658 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 9 | 6.079224 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5ae9, seq=2/512, ttl=63 (no response fo |
| 10 | 6.094733 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 13 | 7.148927 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5be9, seq=3/768, ttl=63 (no response fo |
| 14 | 7.164584 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 16 | 8.218579 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5ce9, seq=4/1024, ttl=63 (no response f |
| 17 | 8.233795 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 21 | 9.281616 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5de9, seq=5/1280, ttl=63 (no response f |
| 22 | 9.296896 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 24 | 10.350070 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5ee9, seq=6/1536, ttl=63 (no response f |

Gambar 4.15 Capture ICMP Saat Route Injection pada Topologi BGP

Berdasarkan Gambar 4.15, terlihat adanya paket ICMP *Echo Request* yang dikirim menuju alamat tujuan. Namun, pada alur yang terdampak, paket tersebut tidak memperoleh balasan *Echo Reply* dari target. Pada beberapa pengujian juga muncul pesan *Destination host unreachable* dari alamat 172.16.1.40, yaitu R4-ATTACKER. Hasil ini memperkuat bahwa komunikasi dua arah terganggu setelah rute tidak sah dari R4-ATTACKER masuk ke proses *routing* BGP.

Hasil pengukuran QoS pada kondisi *route injection* BGP ditunjukkan pada Tabel 4.10.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.10 Hasil Pengujian QoS Saat Route Injection pada Topologi BGP

| Target Serangan | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| PC1 | PC2 ke PC1 | 30 | 0 | 30 | 100% | Tidak terukur | 1,300 Kbps |
| PC1 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0,402 Kbps |
| PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,60 ms | 1,493 Kbps |
| PC2 | PC1 ke PC2 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 164,79 ms | 1,415 Kbps |
| PC2 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,63 ms | 1,411 Kbps |
| PC3 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,295 Kbps |
| PC3 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,60 ms | 1,493 Kbps |

Berdasarkan Tabel 4.10, *route injection* pada topologi BGP menyebabkan gangguan pada alur komunikasi yang menuju target serangan. Pada target PC1, komunikasi PC2 menuju PC1 mengalami *packet loss* sebesar 100%. Pada target PC2, alur PC1 menuju PC2 dan PC2 menuju PC3 mengalami *packet loss* sebesar 100%. Pada target PC3, alur PC1 menuju PC3 mengalami *packet loss* sebesar 100%, sedangkan alur lain yang tidak langsung terdampak masih memperoleh balasan.

Nilai *delay* pada alur yang mengalami *packet loss* 100% dinyatakan tidak terukur karena tidak terdapat paket *Echo Reply* yang diterima dari alamat tujuan. Dengan demikian, dampak utama *route injection* pada BGP terlihat dari meningkatnya nilai

*packet loss*, tidak adanya balasan dari target, serta perubahan jalur menuju R4-ATTACKER sebagai *next-hop* tidak sah.

Berdasarkan hasil pengujian pada topologi BGP, *route injection* berhasil dilakukan oleh R4-ATTACKER dengan mengiklankan *prefix host* /32 ke dalam jaringan. *Prefix* tersebut diterima oleh R1-KOMINFO melalui *next-hop* 172.16.1.40 dan digunakan dalam proses pemilihan jalur. Karena *prefix* /32 lebih spesifik dibandingkan rute asli /24, trafik menuju target dapat diarahkan ke R4-ATTACKER. Kondisi ini menunjukkan bahwa integritas informasi *control plane routing* pada BGP terganggu dan berdampak pada ketersediaan komunikasi antar-*client*.

b. Hasil Pengujian *Route Injection* pada Topologi EIGRP

Pada topologi EIGRP, R4-ATTACKER telah berada pada jaringan transit yang sama dan telah membentuk hubungan *neighbor* EIGRP pada kondisi *baseline*. Namun, pada kondisi *baseline*, R4-ATTACKER belum menyebarkan rute tidak sah. Skenario *route injection* dilakukan dengan memasukkan rute tidak sah menuju host target melalui R4-ATTACKER.

Berbeda dengan BGP, *route injection* pada EIGRP dilakukan dengan membuat rute statis menuju Null0 pada R4-ATTACKER, kemudian rute statis tersebut di-*redistribute* ke dalam proses EIGRP AS 100. Pada pengujian ini, *prefix* yang diuji adalah 192.168.16.2/32, 192.168.17.2/32, dan 192.168.18.2/32. Konfigurasi *route injection* EIGRP pada R4-ATTACKER ditunjukkan pada Gambar 4.16.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip route 192.168.17.2 255.255.255.255 Null0
R4(config)#
R4(config)#router eigrp 100
R4(config-router)# redistribute static metric 10000 100 255 1 1500
R4(config-router)#end
R4#
```

Gambar 4.16 Konfigurasi *Route Injection* EIGRP pada R4-ATTACKER

Berdasarkan Gambar 4.16, R4-ATTACKER dikonfigurasi dengan rute statis menuju Null0 untuk alamat target. Rute tersebut kemudian didistribusikan ke dalam EIGRP menggunakan perintah redistribute static metric 10000 100 255 1 1500. Konfigurasi ini menyebabkan R4-ATTACKER mengiklankan rute tidak sah sebagai rute eksternal ke dalam domain EIGRP AS 100.

Setelah konfigurasi dilakukan pada R4-ATTACKER, verifikasi dilakukan pada router utama untuk memastikan apakah rute tidak sah berhasil diterima melalui EIGRP. Verifikasi dilakukan menggunakan perintah show ip route terhadap alamat target. Hasil verifikasi *route injection* EIGRP ditunjukkan pada Gambar 4.17 sampai Gambar 4.19.

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.16.0/24 is variably subnetted, 3 subnets, 2 masks
D EX     192.168.16.2/32
           [170/284160] via 172.16.1.40, 00:22:35, FastEthernet0/0
D     192.168.17.0/24 [90/30720] via 172.16.1.20, 00:56:20, FastEthernet0/0
D     192.168.18.0/24 [90/30720] via 172.16.1.30, 00:56:20, FastEthernet0/0
```

Gambar 4.17 Hasil Verifikasi Route Injection EIGRP Target PC1

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
R1-KOMINFO#show ip route 192.168.17.2
Routing entry for 192.168.17.2/32
  Known via "eigrp 100", distance 170, metric 284160, type external
  Redistributing via eigrp 100
  Last update from 172.16.1.40 on FastEthernet0/0, 00:05:14 ago
  Routing Descriptor Blocks:
  * 172.16.1.40, from 172.16.1.40, 00:05:14 ago, via FastEthernet0/0
      Route metric is 284160, traffic share count is 1
      Total delay is 1100 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Gambar 4.18 Hasil Verifikasi *Route Injection* EIGRP Target PC2

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.17.0/24 [90/30720] via 172.16.1.20, 03:26:02, FastEthernet0/0
      192.168.18.0/24 is variably subnetted, 2 subnets, 2 masks
D        192.168.18.0/24 [90/30720] via 172.16.1.30, 03:26:02, FastEthernet0/0
D EX     192.168.18.2/32
           [170/284160] via 172.16.1.40, 00:00:02, FastEthernet0/0
```

Gambar 4.19 Hasil Verifikasi Route Injection EIGRP Target PC3

Berdasarkan Gambar 4.17 sampai Gambar 4.19, rute tidak sah menuju target berhasil masuk ke *routing table* router melalui protokol EIGRP. Rute tersebut ditandai dengan kode D EX, yang menunjukkan bahwa rute berasal dari EIGRP eksternal hasil redistribusi. Selain itu, rute diterima melalui *next-hop* 172.16.1.40, yaitu alamat R4-ATTACKER. Kondisi ini menunjukkan bahwa R4-ATTACKER berhasil memasukkan rute tidak sah ke dalam domain EIGRP.

Walaupun rute asli menuju jaringan PC1, PC2, dan PC3 masih tersedia dalam bentuk *prefix* /24, rute tidak sah /32 dari R4-ATTACKER lebih spesifik. Oleh karena itu, trafik menuju host target dapat diarahkan ke R4-ATTACKER berdasarkan prinsip *longest prefix match*. Hal ini membuktikan bahwa *route injection*

pada EIGRP dapat memengaruhi proses pemilihan jalur pada router.

Setelah perubahan *routing table* teridentifikasi, pengujian dilanjutkan dari sisi *client* untuk mengetahui dampaknya terhadap konektivitas jaringan. Pengujian dilakukan menggunakan perintah *ping* pada alur komunikasi yang menuju atau melibatkan target serangan. Hasil pengujian *ping* saat *route injection* EIGRP ditunjukkan pada Gambar 4.20.

```
PC1> ping 192.168.17.2 -c 30
*172.16.1.40 icmp_seq=1 ttl=254 time=46.260 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=2 ttl=254 time=46.763 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=3 ttl=254 time=46.452 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=4 ttl=254 time=45.457 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=5 ttl=254 time=44.950 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=6 ttl=254 time=45.904 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=7 ttl=254 time=45.421 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=8 ttl=254 time=46.586 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=9 ttl=254 time=45.027 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=10 ttl=254 time=46.355 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=11 ttl=254 time=46.909 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=12 ttl=254 time=46.358 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=13 ttl=254 time=45.267 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=14 ttl=254 time=44.618 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=15 ttl=254 time=45.735 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=16 ttl=254 time=45.665 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=17 ttl=254 time=45.915 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=18 ttl=254 time=45.956 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=19 ttl=254 time=46.312 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=20 ttl=254 time=47.158 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=21 ttl=254 time=46.871 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=22 ttl=254 time=46.553 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=23 ttl=254 time=45.281 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=24 ttl=254 time=44.911 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=25 ttl=254 time=45.277 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=26 ttl=254 time=45.944 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=27 ttl=254 time=45.541 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=28 ttl=254 time=47.107 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=29 ttl=254 time=45.630 ms (ICMP type:3, code:1, Destination host unreachable)
*172.16.1.40 icmp_seq=30 ttl=254 time=46.376 ms (ICMP type:3, code:1, Destination host unreachable)
```

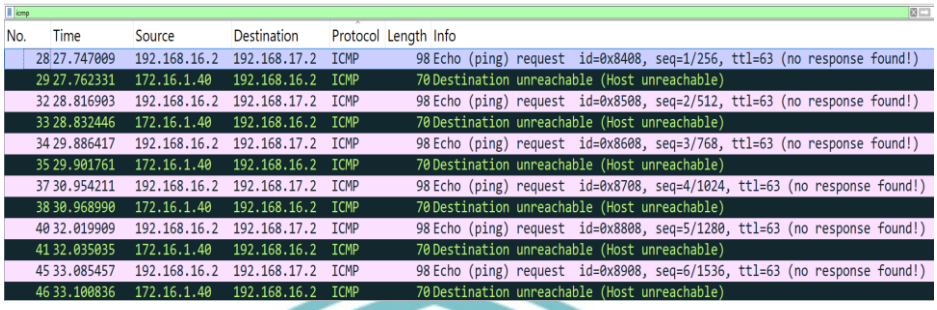
Gambar 4.20 Hasil Pengujian *Ping* Saat *Route Injection* pada Topologi EIGRP

Berdasarkan Gambar 4.20, hasil pengujian *ping* menunjukkan adanya gangguan konektivitas setelah *route injection* diterapkan. Gangguan tersebut ditunjukkan dengan tidak diterimanya balasan *reply*, munculnya *destination host unreachable*, atau keterangan *no response*. Kondisi ini terjadi karena trafik menuju target diarahkan ke R4-ATTACKER melalui rute /32, kemudian paket dibuang karena rute pada R4 diarahkan ke Null0.

Untuk memperkuat hasil pengujian *ping*, dilakukan pengamatan paket menggunakan Wireshark. Hasil *capture* ICMP pada kondisi *route injection* EIGRP ditunjukkan pada Gambar 4.21.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 28 | 27.747009 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x8408, seq=1/256, ttl=63 (no response found!) |
| 29 | 27.762331 | 172.16.1.40 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 32 | 28.816903 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x8508, seq=2/512, ttl=63 (no response found!) |
| 33 | 28.832446 | 172.16.1.40 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 34 | 29.886417 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x8608, seq=3/768, ttl=63 (no response found!) |
| 35 | 29.901761 | 172.16.1.40 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 37 | 30.954211 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x8708, seq=4/1024, ttl=63 (no response found!) |
| 38 | 30.968990 | 172.16.1.40 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 40 | 32.019909 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x8808, seq=5/1280, ttl=63 (no response found!) |
| 41 | 32.035035 | 172.16.1.40 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 45 | 33.085457 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x8908, seq=6/1536, ttl=63 (no response found!) |
| 46 | 33.100836 | 172.16.1.40 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |

Gambar 4.21 *Capture* ICMP Saat *Route Injection* pada Topologi EIGRP

Berdasarkan Gambar 4.21, terlihat adanya paket ICMP *Echo Request* yang dikirim menuju alamat tujuan. Namun, pada alur yang terdampak, paket tersebut tidak memperoleh balasan *Echo Reply* dari target. Pada beberapa pengujian juga muncul pesan *Destination host unreachable* dari alamat 172.16.1.40. Hal ini menunjukkan bahwa komunikasi dua arah antar-*client* terganggu setelah rute tidak sah dari R4-ATTACKER masuk ke proses *routing* EIGRP.

Hasil pengukuran QoS pada kondisi *route injection* EIGRP ditunjukkan pada Tabel 4.11.

Tabel 4.11 Hasil Pengujian QoS Saat Route Injection pada Topologi EIGRP

| Target Serangan | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| PC1 | PC2 ke PC1 | 30 | 0 | 30 | 100% | Tidak terukur | 1,303 Kbps |
| PC1 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0,402 Kbps |
| PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,61 ms | 1,496 Kbps |
| PC2 | PC1 ke PC2 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 166,05 ms | 1,404 Kbps |



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| Target Serangan | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| PC2 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,70 ms | 1,496 Kbps |
| PC3 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,299 Kbps |
| PC3 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,301 Kbps |

Berdasarkan Tabel 4.11, *route injection* pada topologi EIGRP menyebabkan gangguan pada alur komunikasi yang menuju atau melibatkan target serangan. Pada target PC1, alur PC2 menuju PC1 dan PC1 menuju PC3 mengalami *packet loss* sebesar 100%. Pada target PC2, alur PC1 menuju PC2 dan PC2 menuju PC3 mengalami *packet loss* sebesar 100%. Pada target PC3, alur PC1 menuju PC3 dan PC2 menuju PC3 mengalami *packet loss* sebesar 100%.

Nilai *delay* pada alur yang mengalami kegagalan tidak dapat dihitung karena tidak terdapat paket *Echo Reply* dari alamat tujuan. Pada alur yang masih memperoleh balasan, nilai *delay* tetap dapat dihitung karena komunikasi dua arah masih berhasil dilakukan. Hasil ini menunjukkan bahwa *route injection* pada EIGRP dapat menyebabkan gangguan konektivitas sesuai dengan target *prefix* tidak sah yang dimasukkan oleh R4-ATTACKER.

Berdasarkan hasil pengujian pada topologi EIGRP, *route injection* berhasil dilakukan oleh R4-ATTACKER dengan memasukkan *prefix host* /32 ke dalam domain EIGRP AS 100. Rute tersebut diterima sebagai rute eksternal EIGRP dengan kode D EX melalui *next-hop* 172.16.1.40. Karena *prefix* /32 lebih spesifik dibandingkan rute asli /24, trafik menuju target diarahkan ke R4-ATTACKER. Kondisi ini menunjukkan bahwa integritas



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

informasi *control plane routing* pada EIGRP terganggu dan berdampak terhadap ketersediaan komunikasi antar-*client*.

#### 4.4.3.3 Hasil Pengujian Setelah Mitigasi Basic Filtering

Setelah dampak *route injection* berhasil diamati pada kondisi sebelumnya, tahap berikutnya adalah menerapkan mitigasi *basic filtering* menggunakan *prefix-list*. Pengujian setelah mitigasi dilakukan untuk mengetahui apakah *prefix-list* mampu menolak rute tidak sah yang berasal dari R4-ATTACKER dan mengembalikan jalur komunikasi ke rute yang valid.

Pengujian dilakukan secara terpisah pada topologi BGP dan EIGRP karena kedua protokol memiliki mekanisme penerimaan dan penyaringan rute yang berbeda. Pada topologi BGP, *prefix-list* diterapkan secara *inbound* pada *neighbor* R4-ATTACKER. Sementara itu, pada topologi EIGRP, *prefix-list* diterapkan melalui *distribute-list* untuk menyaring rute yang masuk ke proses EIGRP.

a. Hasil Pengujian Setelah Mitigasi pada Topologi BGP

Mitigasi pada topologi BGP dilakukan pada router R1-KOMINFO. Router R1-KOMINFO dipilih sebagai titik penerapan mitigasi karena pada skenario *route injection*, R1 menerima *route advertisement* tidak sah dari R4-ATTACKER. Rute tidak sah yang sebelumnya diiklankan oleh R4 berupa *prefix host* /32 menuju PC1, PC2, dan PC3.

Untuk menolak *prefix* tersebut, diterapkan *prefix-list* pada router R1-KOMINFO. *Prefix-list* digunakan untuk menolak *prefix* 192.168.16.2/32, 192.168.17.2/32, dan 192.168.18.2/32, serta tetap mengizinkan *prefix* lainnya agar proses pertukaran rute BGP yang valid tetap berjalan. Pada draf lama, mitigasi BGP

dijelaskan diterapkan di R1-KOMINFO untuk menolak *prefix* tidak sah dari R4-ATTACKER.

```
R1-KOMINFO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-KOMINFO(config)#$ist FILTER-INVALID-BGP seq 5 deny 192.168.17.2/32
R1-KOMINFO(config)#$ist FILTER-INVALID-BGP seq 100 permit 0.0.0.0/0 le 32
R1-KOMINFO(config)#
R1-KOMINFO(config)#router bgp 6410
R1-KOMINFO(config-router)#$72.16.1.40 prefix-list FILTER-INVALID-BGP in
R1-KOMINFO(config-router)#end
R1-KOMINFO#clear ip bgp 172.16.1.40 soft in
R1-KOMINFO#
```

Gambar 4.22 Konfigurasi *Basic Filtering* BGP pada Router R1-KOMINFO

Berdasarkan Gambar 4.22, *prefix-list* FILTER-INVALID-BGP digunakan untuk menolak *prefix* tidak sah yang berasal dari R4-ATTACKER. Aturan permit 0.0.0.0/0 le 32 tetap digunakan agar *prefix* valid lainnya masih dapat diterima oleh R1-KOMINFO. *Prefix-list* tersebut diterapkan secara *inbound* pada *neighbor* 172.16.1.40, yaitu R4-ATTACKER. Dengan konfigurasi tersebut, setiap *route advertisement* dari R4 akan diperiksa terlebih dahulu sebelum diterima oleh R1-KOMINFO.

Setelah konfigurasi *prefix-list* diterapkan, dilakukan verifikasi pada tabel BGP R1-KOMINFO. Verifikasi ini bertujuan untuk memastikan apakah *prefix* tidak sah yang sebelumnya diterima dari R4-ATTACKER masih muncul atau sudah berhasil ditolak.

```
R1-KOMINFO#show ip bgp
BGP table version is 6, local router ID is 192.168.16.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  192.168.16.0     0.0.0.0                  0         32768 i
 *>  192.168.17.0     172.16.1.20              0             0 6420 i
 *>  192.168.18.0     172.16.1.30              0             0 6430 i
```

Gambar 4.23 Tabel BGP R1-KOMINFO Setelah Mitigasi BGP

Berdasarkan Gambar 4.23, *prefix host* /32 yang sebelumnya berasal dari R4-ATTACKER sudah tidak digunakan sebagai jalur



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

utama. Rute yang tersedia kembali mengarah ke *prefix* valid masing-masing jaringan, seperti 192.168.16.0/24, 192.168.17.0/24, dan 192.168.18.0/24. Kondisi ini menunjukkan bahwa *prefix-list* berhasil menolak rute tidak sah yang sebelumnya diiklankan oleh R4-ATTACKER.

Untuk memastikan rute yang digunakan dalam proses pengiriman paket, dilakukan verifikasi lanjutan menggunakan perintah show ip route terhadap alamat target. Hasil verifikasi *routing table* setelah mitigasi BGP ditunjukkan pada Gambar 4.24.

```
R1-KOMINFO#show ip route 192.168.17.2
Routing entry for 192.168.17.0/24
  Known via "bgp 6410", distance 20, metric 0
  Tag 6420, type external
  Last update from 172.16.1.20 00:44:02 ago
  Routing Descriptor Blocks:
  * 172.16.1.20, from 172.16.1.20, 00:44:02 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6420
      MPLS label: none
```

Gambar 4.24 *Routing Table* R1-KOMINFO Setelah Mitigasi BGP

Berdasarkan Gambar 4.24, R1-KOMINFO kembali menggunakan rute valid menuju jaringan tujuan. Rute host /32 dari R4-ATTACKER tidak lagi digunakan sebagai jalur pengiriman paket. Dengan demikian, jalur komunikasi menuju PC1, PC2, dan PC3 kembali menggunakan router utama yang sesuai.

Setelah verifikasi tabel BGP dan *routing table* menunjukkan bahwa rute tidak sah telah ditolak, pengujian dilanjutkan dari sisi *client*. Pengujian dilakukan menggunakan perintah *ping* untuk memastikan apakah konektivitas jaringan kembali normal setelah mitigasi diterapkan.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
PC2> ping 192.168.16.2 -c 30
84 bytes from 192.168.16.2 icmp_seq=1 ttl=62 time=60.029 ms
84 bytes from 192.168.16.2 icmp_seq=2 ttl=62 time=61.859 ms
84 bytes from 192.168.16.2 icmp_seq=3 ttl=62 time=61.724 ms
84 bytes from 192.168.16.2 icmp_seq=4 ttl=62 time=62.118 ms
84 bytes from 192.168.16.2 icmp_seq=5 ttl=62 time=61.699 ms
84 bytes from 192.168.16.2 icmp_seq=6 ttl=62 time=62.235 ms
84 bytes from 192.168.16.2 icmp_seq=7 ttl=62 time=61.055 ms
84 bytes from 192.168.16.2 icmp_seq=8 ttl=62 time=61.953 ms
84 bytes from 192.168.16.2 icmp_seq=9 ttl=62 time=61.760 ms
84 bytes from 192.168.16.2 icmp_seq=10 ttl=62 time=60.287 ms
84 bytes from 192.168.16.2 icmp_seq=11 ttl=62 time=61.561 ms
84 bytes from 192.168.16.2 icmp_seq=12 ttl=62 time=62.688 ms
84 bytes from 192.168.16.2 icmp_seq=13 ttl=62 time=61.361 ms
84 bytes from 192.168.16.2 icmp_seq=14 ttl=62 time=61.126 ms
84 bytes from 192.168.16.2 icmp_seq=15 ttl=62 time=60.846 ms
84 bytes from 192.168.16.2 icmp_seq=16 ttl=62 time=56.702 ms
84 bytes from 192.168.16.2 icmp_seq=17 ttl=62 time=46.875 ms
84 bytes from 192.168.16.2 icmp_seq=18 ttl=62 time=62.166 ms
84 bytes from 192.168.16.2 icmp_seq=19 ttl=62 time=61.429 ms
84 bytes from 192.168.16.2 icmp_seq=20 ttl=62 time=61.631 ms
84 bytes from 192.168.16.2 icmp_seq=21 ttl=62 time=60.744 ms
84 bytes from 192.168.16.2 icmp_seq=22 ttl=62 time=61.734 ms
84 bytes from 192.168.16.2 icmp_seq=23 ttl=62 time=59.740 ms
84 bytes from 192.168.16.2 icmp_seq=24 ttl=62 time=61.882 ms
84 bytes from 192.168.16.2 icmp_seq=25 ttl=62 time=61.047 ms
84 bytes from 192.168.16.2 icmp_seq=26 ttl=62 time=62.057 ms
84 bytes from 192.168.16.2 icmp_seq=27 ttl=62 time=62.079 ms
84 bytes from 192.168.16.2 icmp_seq=28 ttl=62 time=61.800 ms
84 bytes from 192.168.16.2 icmp_seq=29 ttl=62 time=61.264 ms
84 bytes from 192.168.16.2 icmp_seq=30 ttl=62 time=61.692 ms
```

Gambar 4.25 Pemulihan Konektivitas Setelah Mitigasi BGP

Berdasarkan Gambar 4.25, paket ICMP kembali memperoleh balasan berupa *reply* dari alamat tujuan. Tidak adanya *request timeout* maupun *destination host unreachable* menunjukkan bahwa konektivitas antar-*client* berhasil dipulihkan setelah *basic filtering* diterapkan.

Untuk memperkuat hasil pengujian konektivitas, dilakukan pengamatan ulang menggunakan Wireshark. Pengamatan ini bertujuan untuk memastikan bahwa komunikasi ICMP kembali berlangsung secara dua arah setelah mitigasi diterapkan.

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 2 | 3.738306 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc321, seq=1/256, ttl=63 (reply in 3) |
| 3 | 3.769362 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc321, seq=1/256, ttl=63 (request in 2) |
| 4 | 4.827182 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc521, seq=2/512, ttl=63 (reply in 5) |
| 5 | 4.856946 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc521, seq=2/512, ttl=63 (request in 4) |
| 6 | 5.912484 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc621, seq=3/768, ttl=63 (reply in 7) |
| 7 | 5.942565 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc621, seq=3/768, ttl=63 (request in 6) |
| 8 | 6.990648 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc721, seq=4/1024, ttl=63 (reply in 9) |
| 9 | 7.021202 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc721, seq=4/1024, ttl=63 (request in 8) |
| 10 | 8.077892 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc821, seq=5/1280, ttl=63 (reply in 11) |
| 11 | 8.109430 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc821, seq=5/1280, ttl=63 (request in 10 |
| 12 | 9.160396 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc921, seq=6/1536, ttl=63 (reply in 13) |

Gambar 4.26 *Capture* ICMP Setelah Mitigasi BGP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Gambar 4.26, terlihat adanya paket ICMP *Echo Request* dan *Echo Reply* pada komunikasi antar-*client*. Adanya pasangan paket *request* dan *reply* menunjukkan bahwa komunikasi dua arah berhasil dipulihkan setelah *prefix* tidak sah ditolak oleh mekanisme *basic filtering*.

Hasil pengukuran QoS setelah mitigasi pada topologi BGP ditunjukkan pada Tabel 4.12.

Tabel 4.12 Hasil Pengujian QoS Setelah Mitigasi pada Topologi BGP

| Target Mitigasi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| PC1 | PC2 ke PC1 | 30 | 30 | 0 | 0% | 30,59 ms | 1,497 Kbps |
| PC1 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,50 ms | 1,498 Kbps |
| PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 31,16 ms | 1,494 Kbps |
| PC2 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,54 ms | 1,495 Kbps |
| PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,50 ms | 1,498 Kbps |
| PC2 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 164,83 ms | 1,412 Kbps |
| PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,63 ms | 1,411 Kbps |
| PC3 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,32 ms | 1,495 Kbps |
| PC3 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 31,16 ms | 1,494 Kbps |

Berdasarkan Tabel 4.12, seluruh alur yang diuji setelah mitigasi BGP berhasil memperoleh balasan *Echo Reply*. Nilai *packet loss* pada seluruh alur menjadi 0%. Kondisi ini menunjukkan bahwa penerapan *prefix-list* pada R1-KOMINFO berhasil menolak rute tidak sah dari R4-ATTACKER dan mengembalikan komunikasi menuju jalur yang valid.

b. Hasil Pengujian Setelah Mitigasi pada Topologi EIGRP

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pada topologi EIGRP, mitigasi tetap dilakukan menggunakan *prefix-list*. Namun, karena EIGRP tidak menerapkan *prefix-list* secara langsung pada *neighbor* seperti BGP, maka *prefix-list* diterapkan ke proses EIGRP melalui perintah *distribute-list*. Dengan demikian, *distribute-list* pada penelitian ini digunakan sebagai mekanisme penerapan *prefix-list* agar rute tidak sah dapat disaring pada proses *routing* EIGRP.

Pada skenario *route injection* EIGRP, R4-ATTACKER mengiklankan rute tidak sah menuju PC1, PC2, dan PC3 melalui proses EIGRP AS 100. Rute tersebut berpotensi diterima oleh router-router utama yang berada pada jaringan transit yang sama, yaitu R1-KOMINFO, R2-CAPIL, dan R3-SANGIR. Oleh karena itu, mitigasi diterapkan pada ketiga router utama tersebut. Pada draf lama, bagian EIGRP juga sudah menjelaskan bahwa mitigasi dilakukan menggunakan *prefix-list* melalui *distribute-list* dan diterapkan pada router utama.

```
R1-KOMINFO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-KOMINFO(config)#$ist FILTER-INVALID-EIGRP seq 5 deny 192.168.17.2/32
R1-KOMINFO(config)#$ist FILTER-INVALID-EIGRP seq 100 permit 0.0.0.0/0 le 32
R1-KOMINFO(config)#
R1-KOMINFO(config)#router eigrp 100
R1-KOMINFO(config-router)#$ix FILTER-INVALID-EIGRP in FastEthernet0/0
R1-KOMINFO(config-router)#end
R1-KOMINFO#clear ip eigrp neighbors
```

Gambar 4.27 Konfigurasi *Basic Filtering* EIGRP pada Router R1-KOMINFO

Berdasarkan Gambar 4.27, *prefix-list* FILTER-INVALID-EIGRP digunakan untuk menolak *prefix* tidak sah yang berasal dari R4-ATTACKER. Selanjutnya, *prefix-list* tersebut diterapkan ke proses EIGRP menggunakan perintah *distribute-list* secara *inbound* pada interface FastEthernet0/0 yang terhubung ke jaringan transit 172.16.1.0/24. Konfigurasi yang sama diterapkan pada R1-KOMINFO, R2-CAPIL, dan R3-SANGIR.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Setelah konfigurasi mitigasi diterapkan, dilakukan verifikasi pada *routing table* untuk memastikan apakah rute tidak sah dari R4-ATTACKER masih digunakan atau telah berhasil ditolak.

```
R1-KOMINFO#show ip route 192.168.17.2
Routing entry for 192.168.17.0/24
  Known via "eigrp 100", distance 90, metric 30720, type internal
  Redistributing via eigrp 100
  Last update from 172.16.1.20 on FastEthernet0/0, 00:00:18 ago
  Routing Descriptor Blocks:
  * 172.16.1.20, from 172.16.1.20, 00:00:18 ago, via FastEthernet0/0
      Route metric is 30720, traffic share count is 1
      Total delay is 200 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Gambar 4.28 *Routing Table* R1-KOMINFO Setelah Mitigasi EIGRP

Berdasarkan Gambar 4.28, rute tidak sah dengan kode D EX yang sebelumnya berasal dari R4-ATTACKER sudah tidak digunakan oleh router utama. Router kembali menggunakan rute valid menuju jaringan tujuan melalui router utama yang sesuai. Kondisi ini menunjukkan bahwa *prefix-list* yang diterapkan melalui *distribute-list* berhasil menolak rute tidak sah pada topologi EIGRP.

Setelah rute tidak sah berhasil ditolak, pengujian konektivitas dilakukan kembali menggunakan perintah *ping*. Pengujian ini bertujuan untuk memastikan bahwa mitigasi yang diterapkan tidak hanya berhasil pada level *routing table*, tetapi juga mampu memulihkan konektivitas antar-*client*. Hasil pengujian ping setelah mitigasi EIGRP ditunjukkan pada Gambar 4.29.

© Hak Cipta milik Politeknik Negeri Jakarta

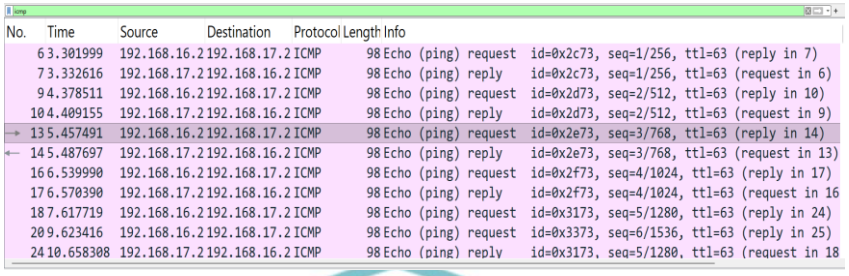
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
PC1> ping 192.168.17.2 -c 30
84 bytes from 192.168.17.2 icmp_seq=1 ttl=62 time=60.267 ms
84 bytes from 192.168.17.2 icmp_seq=2 ttl=62 time=61.492 ms
84 bytes from 192.168.17.2 icmp_seq=3 ttl=62 time=60.638 ms
84 bytes from 192.168.17.2 icmp_seq=4 ttl=62 time=61.092 ms
84 bytes from 192.168.17.2 icmp_seq=5 ttl=62 time=61.221 ms
84 bytes from 192.168.17.2 icmp_seq=6 ttl=62 time=60.794 ms
84 bytes from 192.168.17.2 icmp_seq=7 ttl=62 time=60.401 ms
84 bytes from 192.168.17.2 icmp_seq=8 ttl=62 time=60.762 ms
84 bytes from 192.168.17.2 icmp_seq=9 ttl=62 time=60.807 ms
84 bytes from 192.168.17.2 icmp_seq=10 ttl=62 time=60.602 ms
84 bytes from 192.168.17.2 icmp_seq=11 ttl=62 time=61.793 ms
84 bytes from 192.168.17.2 icmp_seq=12 ttl=62 time=60.830 ms
84 bytes from 192.168.17.2 icmp_seq=13 ttl=62 time=61.265 ms
84 bytes from 192.168.17.2 icmp_seq=14 ttl=62 time=61.207 ms
84 bytes from 192.168.17.2 icmp_seq=15 ttl=62 time=61.196 ms
84 bytes from 192.168.17.2 icmp_seq=16 ttl=62 time=60.875 ms
84 bytes from 192.168.17.2 icmp_seq=17 ttl=62 time=60.759 ms
84 bytes from 192.168.17.2 icmp_seq=18 ttl=62 time=61.656 ms
84 bytes from 192.168.17.2 icmp_seq=19 ttl=62 time=60.447 ms
84 bytes from 192.168.17.2 icmp_seq=20 ttl=62 time=61.850 ms
84 bytes from 192.168.17.2 icmp_seq=21 ttl=62 time=61.044 ms
84 bytes from 192.168.17.2 icmp_seq=22 ttl=62 time=60.843 ms
84 bytes from 192.168.17.2 icmp_seq=23 ttl=62 time=61.064 ms
84 bytes from 192.168.17.2 icmp_seq=24 ttl=62 time=61.038 ms
84 bytes from 192.168.17.2 icmp_seq=25 ttl=62 time=61.123 ms
84 bytes from 192.168.17.2 icmp_seq=26 ttl=62 time=61.264 ms
84 bytes from 192.168.17.2 icmp_seq=27 ttl=62 time=60.992 ms
84 bytes from 192.168.17.2 icmp_seq=28 ttl=62 time=61.298 ms
84 bytes from 192.168.17.2 icmp_seq=29 ttl=62 time=61.146 ms
84 bytes from 192.168.17.2 icmp_seq=30 ttl=62 time=60.813 ms
```

Gambar 4.29 Pemulihan Konektivitas Setelah Mitigasi EIGRP

Berdasarkan Gambar 4.29, hasil pengujian *ping* menunjukkan bahwa komunikasi antar-*client* kembali memperoleh balasan berupa *reply*. Tidak adanya *request timeout* maupun *destination host unreachable* menunjukkan bahwa jalur komunikasi kembali berjalan normal setelah rute tidak sah ditolak menggunakan *prefix-list* dan *distribute-list*.

Selain pengujian menggunakan *ping*, dilakukan juga pengamatan paket menggunakan Wireshark. Pengamatan ini digunakan untuk memastikan bahwa paket ICMP kembali memperoleh balasan dari alamat tujuan setelah mitigasi diterapkan.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6 | 3.301999 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x2c73, seq=1/256, ttl=63 (reply in 7) |
| 7 | 3.332616 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x2c73, seq=1/256, ttl=63 (request in 6) |
| 9 | 4.378511 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x2d73, seq=2/512, ttl=63 (reply in 10) |
| 10 | 4.409155 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x2d73, seq=2/512, ttl=63 (request in 9) |
| 13 | 5.457491 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x2e73, seq=3/768, ttl=63 (reply in 14) |
| 14 | 5.487697 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x2e73, seq=3/768, ttl=63 (request in 13) |
| 16 | 6.539990 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x2f73, seq=4/1024, ttl=63 (reply in 17) |
| 17 | 6.570390 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x2f73, seq=4/1024, ttl=63 (request in 16 |
| 18 | 7.617719 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x3173, seq=5/1280, ttl=63 (reply in 24) |
| 20 | 9.623416 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0x3373, seq=6/1536, ttl=63 (reply in 25) |
| 24 | 10.658308 | 192.168.17.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0x3173, seq=5/1280, ttl=63 (request in 18 |

Gambar 4.30 *Capture* ICMP Setelah Mitigasi EIGRP

Berdasarkan Gambar 4.30, terlihat adanya paket ICMP *Echo Request* dan *Echo Reply* selama pengujian konektivitas. Adanya pasangan paket tersebut menunjukkan bahwa komunikasi dua arah antar-*client* berhasil dipulihkan setelah *filtering* diterapkan pada topologi EIGRP.

Hasil pengukuran QoS setelah mitigasi pada topologi EIGRP ditunjukkan pada Tabel 4.13.

Tabel 4.13 Hasil Pengujian QoS Setelah Mitigasi pada Topologi EIGRP

| Target Mitigasi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| PC1 | PC2 ke PC1 | 30 | 30 | 0 | 0% | 30,61 ms | 1,414 Kbps |
| PC1 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 31,41 ms | 1,496 Kbps |
| PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,65 ms | 1,496 Kbps |
| PC2 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 165,57 ms | 1,407 Kbps |
| PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 164,77 ms | 1,414 Kbps |
| PC2 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 32,32 ms | 1,497 Kbps |
| PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 31,32 ms | 1,496 Kbps |



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| Target Mitigasi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| PC3 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,47 ms | 1,494 Kbps |
| PC3 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,68 ms | 1,496 Kbps |

Berdasarkan Tabel 4.13, seluruh alur pengujian pada topologi EIGRP berhasil memperoleh balasan *Echo Reply* setelah mitigasi diterapkan. Nilai *packet loss* pada seluruh alur menjadi 0%. Hasil ini menunjukkan bahwa penerapan *prefix-list* melalui *distribute-list* berhasil menolak rute tidak sah dari R4-ATTACKER dan memulihkan komunikasi antar-*client*.

Berdasarkan keseluruhan hasil pengujian setelah mitigasi, *basic filtering* menggunakan *prefix-list* mampu menolak rute tidak sah pada kedua protokol, baik BGP maupun EIGRP. Pada BGP, *prefix-list* diterapkan secara *inbound* pada *neighbor* R4-ATTACKER. Sedangkan pada EIGRP, *prefix-list* diterapkan melalui *distribute-list*. Meskipun mekanisme penerapannya berbeda, keduanya menunjukkan hasil yang sama, yaitu rute tidak sah berhasil ditolak dan konektivitas antar-*client* dapat dipulihkan.

#### 4.4.3.4 Hasil Pengujian Traceroute

Selain pengujian menggunakan *ping* dan pengamatan paket melalui Wireshark, penelitian ini juga melakukan pengujian *traceroute* sebagai data pendukung. Pengujian ini digunakan untuk melihat jalur komunikasi yang dilalui paket pada kondisi *baseline*, kondisi saat terjadi *route injection*, dan kondisi setelah penerapan mitigasi *basic filtering* menggunakan *prefix-list*. Hasil *traceroute* tidak digunakan sebagai parameter utama QoS, melainkan sebagai data pendukung untuk memperkuat analisis perubahan jalur *routing*.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian *traceroute* difokuskan pada komunikasi dari PC1 menuju PC2 dengan alamat tujuan 192.168.17.2. Pemilihan jalur ini dilakukan karena *prefix* yang digunakan pada salah satu skenario *route injection* adalah 192.168.17.2/32, yaitu rute *host* menuju PC2. Dengan demikian, perubahan jalur yang terjadi akibat masuknya rute tidak sah dari R4-ATTACKER dapat diamati secara langsung melalui hasil *traceroute*.

a. Hasil Pengujian *Traceroute* pada Topologi BGP

Pada topologi BGP, pengujian *traceroute* dilakukan pada tiga kondisi, yaitu kondisi *baseline*, kondisi saat terjadi *route injection*, dan kondisi setelah mitigasi *basic filtering* diterapkan. Pengujian dilakukan dari PC1 menuju PC2 untuk melihat apakah jalur komunikasi masih melewati rute valid atau mengalami perubahan akibat masuknya *prefix* tidak sah dari R4-ATTACKER. Hasil pengujian *traceroute* pada topologi BGP ditunjukkan pada Gambar 4.31.

```
PC1> trace 192.168.17.2
trace to 192.168.17.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   15.092 ms  14.820 ms  15.152 ms
 2   172.16.1.20   45.818 ms  46.173 ms  45.791 ms
 3   *192.168.17.2   61.531 ms (ICMP type:3, code:3, Destination port unreachable)

PC1> trace 192.168.17.2
trace to 192.168.17.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   15.857 ms  14.866 ms  15.865 ms
 2   172.16.1.40   45.974 ms  45.823 ms  45.503 ms
 3   *172.16.1.40   46.374 ms (ICMP type:3, code:1, Destination host unreachable)

PC1> trace 192.168.17.2
trace to 192.168.17.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   15.400 ms  15.144 ms  15.463 ms
 2   172.16.1.20   46.045 ms  45.758 ms  45.539 ms
 3   *192.168.17.2   60.117 ms (ICMP type:3, code:3, Destination port unreachable)
```

Gambar 4.31 Hasil *Traceroute* pada Topologi BGP

Berdasarkan Gambar 4.31, pada kondisi *baseline*, hasil *traceroute* dari PC1 menuju PC2 menunjukkan bahwa paket melewati *gateway* PC1, yaitu 192.168.16.1 pada *hop* pertama. Selanjutnya, paket diteruskan menuju R2-CAPIL melalui alamat 172.16.1.20 pada *hop* kedua, kemudian mencapai PC2 dengan

alamat 192.168.17.2 pada *hop* ketiga. Munculnya pesan *destination port unreachable* pada alamat 192.168.17.2 menunjukkan bahwa paket *traceroute* telah sampai ke alamat tujuan.

Saat *route injection* diterapkan, jalur komunikasi mengalami perubahan. Pada kondisi ini, *hop* pertama masih melewati *gateway* 192.168.16.1, tetapi *hop* kedua berubah menjadi 172.16.1.40, yaitu alamat R4-ATTACKER. Selanjutnya, muncul pesan *destination host unreachable* dari 172.16.1.40. Kondisi ini menunjukkan bahwa paket dari PC1 menuju PC2 tidak lagi diteruskan melalui R2-CAPIL, melainkan diarahkan ke R4-ATTACKER.

Perubahan jalur tersebut terjadi karena R1-KOMINFO menerima rute tidak sah 192.168.17.2/32 dari R4-ATTACKER. Rute /32 tersebut lebih spesifik dibandingkan rute valid 192.168.17.0/24, sehingga router memilih rute tidak sah tersebut berdasarkan prinsip *longest prefix match*. Akibatnya, paket menuju PC2 diarahkan ke R4-ATTACKER dan tidak dapat mencapai tujuan sebenarnya karena rute pada R4 diarahkan ke Null0.

Setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan, hasil *traceroute* kembali menunjukkan jalur yang valid. Paket dari PC1 menuju PC2 kembali melewati *gateway* 192.168.16.1 pada *hop* pertama, kemudian diteruskan melalui R2-CAPIL dengan alamat 172.16.1.20 pada *hop* kedua, dan mencapai PC2 dengan alamat 192.168.17.2 pada *hop* ketiga. Munculnya kembali pesan *destination port unreachable* dari 192.168.17.2 menunjukkan bahwa paket telah sampai ke tujuan. Hal ini membuktikan bahwa *prefix-list* berhasil menolak *prefix* tidak sah dari R4-ATTACKER, sehingga jalur BGP kembali menggunakan rute valid menuju PC2.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

b. Hasil Pengujian *Traceroute* pada Topologi EIGRP

Pada topologi EIGRP, pengujian *traceroute* juga dilakukan pada tiga kondisi, yaitu kondisi *baseline*, kondisi saat terjadi *route injection*, dan kondisi setelah mitigasi diterapkan. Pengujian dilakukan dari PC1 menuju PC2 untuk melihat dampak masuknya rute eksternal EIGRP tidak sah yang berasal dari R4-ATTACKER. Hasil pengujian *traceroute* pada topologi EIGRP ditunjukkan pada Gambar 4.32.

```
PC1> trace 192.168.17.2
trace to 192.168.17.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   15.009 ms  15.058 ms  15.167 ms
 2   172.16.1.20   46.437 ms  45.436 ms  45.457 ms
 3   *192.168.17.2   60.954 ms (ICMP type:3, code:3, Destination port unreachable)

PC1> trace 192.168.17.2
trace to 192.168.17.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   14.165 ms  15.164 ms  15.077 ms
 2   172.16.1.40   45.325 ms  45.765 ms  46.546 ms
 3   *172.16.1.40   45.527 ms (ICMP type:3, code:1, Destination host unreachable)

PC1> trace 192.168.17.2
trace to 192.168.17.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   15.161 ms  14.981 ms  15.393 ms
 2   172.16.1.20   46.178 ms  46.152 ms  45.708 ms
 3   *192.168.17.2   61.131 ms (ICMP type:3, code:3, Destination port unreachable)
```

Gambar 4.32 Hasil *Traceroute* pada Topologi EIGRP

Berdasarkan Gambar 4.32, pada kondisi *baseline*, hasil *traceroute* dari PC1 menuju PC2 menunjukkan bahwa paket melewati *gateway* PC1, yaitu 192.168.16.1 pada *hop* pertama. Selanjutnya, paket diteruskan menuju R2-CAPIL melalui alamat 172.16.1.20 pada *hop* kedua, kemudian mencapai PC2 dengan alamat 192.168.17.2 pada *hop* ketiga. Munculnya pesan *destination port unreachable* pada alamat 192.168.17.2 menunjukkan bahwa paket *traceroute* telah sampai ke alamat tujuan.

Saat *route injection* diterapkan, jalur komunikasi mengalami perubahan. Pada kondisi ini, *hop* pertama tetap melewati *gateway* 192.168.16.1, tetapi *hop* kedua berubah menjadi 172.16.1.40, yaitu alamat R4-ATTACKER. Selanjutnya, muncul pesan

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*destination host unreachable* dari 172.16.1.40. Kondisi ini menunjukkan bahwa paket dari PC1 menuju PC2 tidak lagi diteruskan melalui R2-CAPIL, melainkan diarahkan ke R4-ATTACKER.

Perubahan jalur tersebut terjadi karena rute tidak sah 192.168.17.2/32 masuk ke dalam domain EIGRP sebagai rute eksternal dengan kode D EX. Rute /32 tersebut lebih spesifik dibandingkan rute valid 192.168.17.0/24, sehingga router memilih rute tidak sah tersebut berdasarkan prinsip *longest prefix match*. Akibatnya, paket menuju PC2 diarahkan ke R4-ATTACKER dan tidak dapat mencapai tujuan sebenarnya karena rute pada R4 diarahkan ke Null0.

Setelah *prefix-list* diterapkan melalui *distribute-list*, hasil *traceroute* kembali menunjukkan jalur yang valid. Paket dari PC1 menuju PC2 kembali melewati *gateway* 192.168.16.1 pada *hop* pertama, kemudian diteruskan melalui R2-CAPIL dengan alamat 172.16.1.20 pada *hop* kedua, dan mencapai PC2 dengan alamat 192.168.17.2 pada *hop* ketiga. Munculnya kembali pesan *destination port unreachable* dari 192.168.17.2 menunjukkan bahwa paket telah sampai ke tujuan. Kondisi ini membuktikan bahwa rute tidak sah dari R4-ATTACKER berhasil ditolak, sehingga jalur EIGRP kembali menggunakan R2-CAPIL sebagai jalur komunikasi yang valid.

### 4.4.4 Analisis Data / Evaluasi Pengujian

Analisis data dilakukan untuk mengevaluasi perubahan kondisi jaringan pada tiga skenario, yaitu kondisi *baseline*, kondisi saat terjadi *route injection*, dan kondisi setelah penerapan mitigasi *basic filtering* menggunakan *prefix-list*. Evaluasi dilakukan berdasarkan perubahan *routing table*, *next-hop*, konektivitas antar-*client*, hasil

*traceroute*, parameter *Quality of Service* (QoS), serta waktu serangan masuk dan waktu pemulihan jaringan.

Pada penelitian ini, skenario *route injection* dilakukan terhadap tiga target, yaitu PC1 dengan alamat 192.168.16.2, PC2 dengan alamat 192.168.17.2, dan PC3 dengan alamat 192.168.18.2. Setiap target dimasukkan sebagai *prefix host* /32. Pada topologi BGP, R4-ATTACKER mengiklankan *prefix* tidak sah tersebut melalui sesi *neighbor* BGP dengan R1-KOMINFO. Pada topologi EIGRP, R4-ATTACKER membuat rute statis menuju Null0, kemudian rute tersebut di-*redistribute* ke dalam EIGRP AS 100 sehingga diterima sebagai rute eksternal.

Pada kondisi *baseline*, komunikasi antar-*client* masih menggunakan rute valid menuju jaringan masing-masing. Setelah *route injection* diterapkan, router menerima rute tidak sah /32 dari R4-ATTACKER. Rute /32 tersebut lebih spesifik dibandingkan rute valid /24, sehingga router dapat memilih rute tidak sah berdasarkan prinsip *longest prefix match*. Kondisi ini menyebabkan *next-hop* menuju target berubah ke 172.16.1.40, yaitu R4-ATTACKER.

Pada topologi BGP, rute tidak sah masuk sebagai *prefix* BGP yang diiklankan oleh R4-ATTACKER. Pada topologi EIGRP, rute tidak sah masuk sebagai rute eksternal dengan kode D EX. Dampaknya terlihat pada perubahan jalur komunikasi, gangguan konektivitas, peningkatan *packet loss*, serta penurunan *throughput* pada alur yang terdampak.

Hasil *traceroute* juga memperkuat perubahan jalur tersebut. Pada kondisi *baseline*, jalur dari PC1 menuju PC2 melewati R2-CAPIL dengan alamat 172.16.1.20. Saat *route injection* diterapkan, *hop* kedua berubah menjadi 172.16.1.40, yaitu R4-ATTACKER. Setelah mitigasi diterapkan, jalur kembali melewati R2-CAPIL. Dengan demikian, hasil *traceroute* menunjukkan bahwa *route injection*



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

menyebabkan perubahan *next-hop*, sedangkan *prefix-list* mampu mengembalikan jalur ke rute yang valid.

Untuk mengukur dampak serangan terhadap kualitas komunikasi, dilakukan pengujian QoS dengan mengirimkan 30 paket ICMP pada setiap alur antar-*client*. Nilai *packet loss* dihitung berdasarkan perbandingan jumlah paket yang dikirim dan diterima. Nilai *delay* diperoleh dari rata-rata waktu respons paket yang memperoleh balasan, sedangkan *throughput* dihitung berdasarkan lalu lintas paket ICMP yang diamati menggunakan Wireshark. Pada kondisi serangan, nilai *delay* hanya dihitung dari alur yang masih memperoleh balasan, sehingga tidak mewakili keseluruhan kondisi jaringan.

a. Analisis QoS pada Topologi BGP

Analisis QoS pada topologi BGP dilakukan untuk mengetahui perubahan kualitas komunikasi jaringan pada kondisi *baseline*, saat terjadi *route injection*, dan setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan. Parameter yang diamati meliputi jumlah paket yang dikirim, jumlah paket yang diterima, jumlah paket hilang, *packet loss*, rata-rata *delay*, dan *throughput*. Pengujian dilakukan menggunakan paket ICMP sebanyak 30 paket pada setiap alur komunikasi.

Pada topologi BGP, kondisi *baseline* digunakan sebagai acuan awal sebelum rute tidak sah dari R4-ATTACKER diiklankan ke dalam jaringan. Pada kondisi ini, seluruh komunikasi antar-*client* masih menggunakan jalur valid sesuai *routing table* BGP yang telah terbentuk. Hasil pengujian QoS pada kondisi *baseline* topologi BGP ditunjukkan pada Tabel 4.14.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.14 Hasil Pengujian QoS pada Topologi BGP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Baseline | PC1 ke PC2 | 30 | 30 | 0 | 0% | 164,41 ms | 1,413 Kbps |
| Baseline | PC1 ke PC3 | 30 | 30 | 0 | 0% | 31,12 ms | 1,495 Kbps |
| Baseline | PC2 ke PC3 | 30 | 30 | 0 | 0% | 164,89 ms | 1,413 Kbps |
| Rata-rata Baseline | - | 30 | 30 | 0 | 0% | 120,14 ms | 1,440 Kbps |

Berdasarkan Tabel 4.14, seluruh alur komunikasi pada kondisi *baseline* berhasil memperoleh balasan *Echo Reply*. Pada alur PC1 ke PC2, PC1 ke PC3, dan PC2 ke PC3, seluruh 30 paket yang dikirim berhasil diterima kembali sehingga nilai *packet loss* sebesar 0%. Nilai rata-rata *delay* pada kondisi *baseline* adalah 120,14 ms, sedangkan rata-rata *throughput* sebesar 1,440 Kbps. Kondisi ini menunjukkan bahwa sebelum *route injection* dilakukan, topologi BGP berada dalam keadaan normal dan komunikasi antar-*client* berjalan stabil.

Selanjutnya, pengujian dilakukan pada kondisi *route injection*. Pada kondisi ini, R4-ATTACKER mengiklankan *prefix host* /32 menuju PC1, PC2, dan PC3 secara bergantian. Rute /32 tersebut lebih spesifik dibandingkan rute jaringan valid /24, sehingga dapat memengaruhi proses pemilihan jalur pada router. Hasil pengujian QoS saat *route injection* pada topologi BGP ditunjukkan pada Tabel 4.15.

Tabel 4.15 Hasil Pengujian QoS Saat Route Injection pada Topologi BGP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Route Injection | PC2 ke PC1 | 30 | 0 | 30 | 100% | Tidak terukur | 1,300 Kbps |

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Target PC1 | | | | | | | |
| Route Injection Target PC1 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0,402 Kbps |
| Route Injection Target PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,60 ms | 1,493 Kbps |
| Rata-rata Target PC1 | - | 30 | 10 | 20 | 66,67% | 30,60 ms | 1,065 Kbps |
| Route Injection Target PC2 | PC1 ke PC2 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| Route Injection Target PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 164,79 ms | 1,415 Kbps |
| Route Injection Target PC2 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| Rata-rata Target PC2 | - | 30 | 10 | 20 | 66,67% | 164,79 ms | 0,472 Kbps |
| Route Injection Target PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,63 ms | 1,411 Kbps |
| Route Injection Target PC3 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,295 Kbps |
| Route Injection Target PC3 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,301 Kbps |
| Rata-rata Target PC3 | - | 30 | 10 | 20 | 66,67% | 30,63 ms | 1,336 Kbps |

Berdasarkan Tabel 4.15, *route injection* menyebabkan gangguan pada alur komunikasi yang menuju atau melibatkan target serangan. Pada target PC1, alur PC2 ke PC1 dan PC1 ke PC3 mengalami *packet loss* sebesar 100%, sedangkan alur PC2 ke PC3 tetap berjalan

normal. Nilai rata-rata *packet loss* pada target PC1 menjadi 66,67%. Hal ini menunjukkan bahwa rute tidak sah 192.168.16.2/32 memengaruhi komunikasi yang menuju PC1 maupun jalur balasan yang melibatkan PC1.

Pada target PC2, alur PC1 ke PC2 dan PC2 ke PC3 mengalami *packet loss* sebesar 100%, sedangkan alur PC1 ke PC3 masih berjalan normal. Nilai rata-rata *packet loss* pada target PC2 juga sebesar 66,67%. Gangguan ini terjadi karena trafik yang menuju alamat 192.168.17.2 diarahkan ke R4-ATTACKER melalui rute tidak sah 192.168.17.2/32. Selain itu, komunikasi PC2 ke PC3 ikut terganggu karena paket balasan menuju PC2 juga mengikuti rute tidak sah tersebut.

Pada target PC3, alur PC1 ke PC3 dan PC2 ke PC3 mengalami *packet loss* sebesar 100%, sedangkan alur PC1 ke PC2 tetap berjalan normal. Nilai rata-rata *packet loss* pada target PC3 menjadi 66,67%. Kondisi ini menunjukkan bahwa setiap trafik yang menuju alamat 192.168.18.2 diarahkan ke R4-ATTACKER akibat masuknya rute tidak sah 192.168.18.2/32.

Nilai *delay* pada kondisi *route injection* hanya dapat dihitung pada alur yang masih memperoleh balasan *Echo Reply*. Pada alur yang mengalami *packet loss* sebesar 100%, nilai *delay* dinyatakan tidak terukur karena tidak terdapat paket balasan dari alamat tujuan. Oleh karena itu, indikator utama dampak *route injection* pada topologi BGP adalah peningkatan *packet loss* dan penurunan *throughput* pada alur yang terdampak.

Setelah dampak serangan diamati, mitigasi *basic filtering* menggunakan *prefix-list* diterapkan pada R1-KOMINFO. *Prefix-list* digunakan untuk menolak *prefix* tidak sah yang berasal dari R4-ATTACKER agar rute tersebut tidak lagi masuk dan digunakan



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dalam proses pemilihan jalur. Hasil pengujian QoS setelah mitigasi pada topologi BGP ditunjukkan pada Tabel 4.16.

Tabel 4.16 Hasil Pengujian QoS Setelah Mitigasi pada Topologi BGP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Setelah Mitigasi Target PC1 | PC2 ke PC1 | 30 | 30 | 0 | 0% | 30,59 ms | 1,497 Kbps |
| Setelah Mitigasi Target PC1 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,50 ms | 1,498 Kbps |
| Setelah Mitigasi Target PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 31,16 ms | 1,494 Kbps |
| Rata-rata Target PC1 | - | 30 | 30 | 0 | 0% | 30,75 ms | 1,496 Kbps |
| Setelah Mitigasi Target PC2 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,54 ms | 1,495 Kbps |
| Setelah Mitigasi Target PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,50 ms | 1,498 Kbps |
| Setelah Mitigasi Target PC2 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 164,83 ms | 1,412 Kbps |
| Rata-rata Target PC2 | - | 30 | 30 | 0 | 0% | 75,29 ms | 1,468 Kbps |
| Setelah Mitigasi Target PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,63 ms | 1,411 Kbps |
| Setelah Mitigasi Target PC3 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,32 ms | 1,495 Kbps |
| Setelah Mitigasi Target PC3 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 31,16 ms | 1,494 Kbps |

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Rata-rata Target PC3 | - | 30 | 30 | 0 | 0% | 30,70 ms | 1,467 Kbps |

Berdasarkan Tabel 4.16, seluruh alur komunikasi pada target PC1, PC2, dan PC3 kembali memperoleh balasan *Echo Reply* setelah mitigasi diterapkan. Nilai *packet loss* pada seluruh alur menjadi 0%. Pada target PC1, rata-rata *delay* setelah mitigasi sebesar 30,75 ms dengan rata-rata *throughput* sebesar 1,496 Kbps. Pada target PC2, rata-rata *delay* sebesar 75,29 ms dengan rata-rata *throughput* sebesar 1,468 Kbps. Sementara itu, pada target PC3, rata-rata *delay* sebesar 30,70 ms dengan rata-rata *throughput* sebesar 1,467 Kbps.

Hasil tersebut menunjukkan bahwa penerapan *prefix-list* berhasil menolak rute tidak sah dari R4-ATTACKER dan mengembalikan komunikasi ke jalur yang valid. Hal ini terlihat dari hilangnya *packet loss* pada seluruh alur setelah mitigasi diterapkan. Dengan demikian, *basic filtering* menggunakan *prefix-list* pada topologi BGP terbukti mampu memulihkan konektivitas jaringan setelah terjadi *route injection*.

Secara keseluruhan, hasil analisis QoS pada topologi BGP menunjukkan bahwa kondisi *baseline* berjalan normal dengan *packet loss* 0%. Saat *route injection* diterapkan, gangguan muncul pada alur komunikasi yang menuju atau melibatkan target serangan, dengan rata-rata *packet loss* sebesar 66,67% pada setiap target. Setelah mitigasi diterapkan, seluruh alur kembali normal dengan *packet loss* 0%. Hal ini membuktikan bahwa *route injection* berdampak terhadap kualitas komunikasi jaringan, sedangkan

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*prefix-list* efektif dalam menolak rute tidak sah dan memulihkan komunikasi antar-*client*.

b. Analisis QoS pada Topologi EIGRP

Analisis QoS pada topologi EIGRP dilakukan untuk mengetahui perubahan kualitas komunikasi jaringan pada kondisi *baseline*, saat terjadi *route injection*, dan setelah mitigasi *basic filtering* menggunakan *prefix-list* melalui *distribute-list* diterapkan. Parameter yang diamati meliputi jumlah paket yang dikirim, jumlah paket yang diterima, jumlah paket hilang, *packet loss*, rata-rata *delay*, dan *throughput*. Sama seperti pada topologi BGP, pengujian dilakukan menggunakan paket ICMP sebanyak 30 paket pada setiap alur komunikasi.

Pada topologi EIGRP, kondisi *baseline* digunakan sebagai acuan awal sebelum R4-ATTACKER memasukkan rute tidak sah ke dalam domain EIGRP. Pada kondisi ini, seluruh komunikasi antar-*client* masih menggunakan rute valid yang diperoleh melalui proses *routing* EIGRP AS 100. Hasil pengujian QoS pada kondisi *baseline* topologi EIGRP ditunjukkan pada Tabel 4.17.

Tabel 4.17 Hasil Pengujian QoS Baseline pada Topologi EIGRP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Baseline | PC2 ke PC1 | 30 | 30 | 0 | 0% | 30,51 ms | 1,497 Kbps |
| Baseline | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,52 ms | 1,499 Kbps |
| Baseline | PC2 ke PC3 | 30 | 30 | 0 | 0% | 31,04 ms | 1,499 Kbps |
| Rata-rata Baseline | - | 30 | 30 | 0 | 0% | 30,69 ms | 1,498 Kbps |

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Tabel 4.17, seluruh alur komunikasi pada kondisi *baseline* EIGRP berhasil memperoleh balasan *Echo Reply*. Pada alur PC2 ke PC1, PC1 ke PC3, dan PC2 ke PC3, seluruh 30 paket yang dikirim berhasil diterima kembali sehingga nilai *packet loss* sebesar 0%. Nilai rata-rata *delay* pada kondisi *baseline* adalah 30,69 ms, sedangkan rata-rata *throughput* sebesar 1,498 Kbps. Kondisi ini menunjukkan bahwa sebelum *route injection* diterapkan, proses *routing* EIGRP berjalan normal dan komunikasi antar-*client* berada dalam kondisi stabil.

Selanjutnya, pengujian dilakukan pada kondisi *route injection*. Pada kondisi ini, R4-ATTACKER membuat rute statis menuju Null0 untuk *prefix host* /32, kemudian rute tersebut di-*redistribute* ke dalam EIGRP AS 100. Rute tidak sah tersebut dapat masuk ke *routing table* sebagai rute eksternal EIGRP dengan kode D EX. Hasil pengujian QoS saat *route injection* pada topologi EIGRP ditunjukkan pada Tabel 4.18.

Tabel 4.18 Hasil Pengujian QoS Saat *Route Injection* pada Topologi EIGRP

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Route Injection Target PC1 | PC2 ke PC1 | 30 | 0 | 30 | 100% | Tidak terukur | 1,303 Kbps |
| Route Injection Target PC1 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0,402 Kbps |
| Route Injection Target PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,61 ms | 1,496 Kbps |
| Rata-rata Target PC1 | - | 30 | 10 | 20 | 66,67% | 30,61 ms | 1,067 Kbps |
| Route Injection | PC1 ke PC2 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Target PC2 | | | | | | | |
| Route Injection Target PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 166,05 ms | 1,404 Kbps |
| Route Injection Target PC2 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 0 Kbps |
| Rata-rata Target PC2 | - | 30 | 10 | 20 | 66,67% | 166,05 ms | 0,468 Kbps |
| Route Injection Target PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 30,70 ms | 1,496 Kbps |
| Route Injection Target PC3 | PC1 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,299 Kbps |
| Route Injection Target PC3 | PC2 ke PC3 | 30 | 0 | 30 | 100% | Tidak terukur | 1,301 Kbps |
| Rata-rata Target PC3 | - | 30 | 10 | 20 | 66,67% | 30,70 ms | 1,365 Kbps |

Berdasarkan Tabel 4.18, *route injection* pada topologi EIGRP menyebabkan gangguan pada alur komunikasi yang menuju atau melibatkan target serangan. Pada target PC1, alur PC2 ke PC1 dan PC1 ke PC3 mengalami *packet loss* sebesar 100%, sedangkan alur PC2 ke PC3 tetap berjalan normal. Nilai rata-rata *packet loss* pada target PC1 menjadi 66,67%. Gangguan ini terjadi karena rute tidak sah 192.168.16.2/32 masuk ke dalam domain EIGRP sebagai rute eksternal dan mengarahkan trafik menuju R4-ATTACKER.

Pada target PC2, alur PC1 ke PC2 dan PC2 ke PC3 mengalami *packet loss* sebesar 100%, sedangkan alur PC1 ke PC3 tetap berjalan normal. Nilai rata-rata *packet loss* pada target PC2 juga sebesar 66,67%. Kondisi ini menunjukkan bahwa rute tidak sah

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

192.168.17.2/32 menyebabkan trafik menuju PC2 diarahkan ke R4-ATTACKER. Selain itu, komunikasi PC2 ke PC3 ikut terganggu karena paket balasan menuju PC2 mengikuti rute tidak sah tersebut.

Pada target PC3, alur PC1 ke PC3 dan PC2 ke PC3 mengalami *packet loss* sebesar 100%, sedangkan alur PC1 ke PC2 tetap berjalan normal. Nilai rata-rata *packet loss* pada target PC3 menjadi 66,67%. Hal ini menunjukkan bahwa trafik menuju alamat PC3, yaitu 192.168.18.2, diarahkan ke R4-ATTACKER akibat masuknya rute tidak sah 192.168.18.2/32.

Nilai *delay* pada kondisi *route injection* hanya dapat dihitung pada alur yang masih memperoleh balasan *Echo Reply*. Pada alur yang mengalami *packet loss* sebesar 100%, nilai *delay* dinyatakan tidak terukur karena tidak terdapat paket balasan dari alamat tujuan. Oleh karena itu, indikator utama dampak *route injection* pada topologi EIGRP adalah peningkatan *packet loss* dan penurunan *throughput* pada alur yang terdampak.

Setelah dampak *route injection* diamati, mitigasi diterapkan menggunakan *prefix-list* melalui *distribute-list*. Mekanisme ini digunakan untuk menolak rute tidak sah yang berasal dari R4-ATTACKER agar rute tersebut tidak digunakan dalam proses pemilihan jalur EIGRP. Hasil pengujian QoS setelah mitigasi pada topologi EIGRP ditunjukkan pada Tabel 4.19.

Tabel 4.19 Hasil Pengujian Waktu Konvergensi dan Pemulihan

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Setelah Mitigasi Target PC1 | PC2 ke PC1 | 30 | 30 | 0 | 0% | 30,61 ms | 1,414 Kbps |
| Setelah Mitigasi Target PC1 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 31,41 ms | 1,496 Kbps |

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

| Kondisi | Alur | Sent | Received | Lost | Packet Loss | Avg Delay | Throughput |
|---|---|---|---|---|---|---|---|
| Setelah Mitigasi Target PC1 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,65 ms | 1,496 Kbps |
| Rata-rata Target PC1 | - | 30 | 30 | 0 | 0% | 30,89 ms | 1,469 Kbps |
| Setelah Mitigasi Target PC2 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 165,57 ms | 1,407 Kbps |
| Setelah Mitigasi Target PC2 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 164,77 ms | 1,414 Kbps |
| Setelah Mitigasi Target PC2 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 32,32 ms | 1,497 Kbps |
| Rata-rata Target PC2 | - | 30 | 30 | 0 | 0% | 120,89 ms | 1,439 Kbps |
| Setelah Mitigasi Target PC3 | PC1 ke PC2 | 30 | 30 | 0 | 0% | 31,32 ms | 1,496 Kbps |
| Setelah Mitigasi Target PC3 | PC1 ke PC3 | 30 | 30 | 0 | 0% | 30,47 ms | 1,494 Kbps |
| Setelah Mitigasi Target PC3 | PC2 ke PC3 | 30 | 30 | 0 | 0% | 30,68 ms | 1,496 Kbps |
| Rata-rata Target PC3 | - | 30 | 30 | 0 | 0% | 30,82 ms | 1,495 Kbps |

Berdasarkan Tabel 4.19, seluruh alur komunikasi pada target PC1, PC2, dan PC3 kembali memperoleh balasan *Echo Reply* setelah mitigasi diterapkan. Nilai *packet loss* pada seluruh alur menjadi 0%. Pada target PC1, rata-rata *delay* setelah mitigasi sebesar 30,89 ms dengan rata-rata *throughput* sebesar 1,469 Kbps. Pada target PC2, rata-rata *delay* sebesar 120,89 ms dengan rata-rata *throughput*

sebesar 1,439 Kbps. Sementara itu, pada target PC3, rata-rata *delay* sebesar 30,82 ms dengan rata-rata *throughput* sebesar 1,495 Kbps.

Hasil tersebut menunjukkan bahwa penerapan *prefix-list* melalui *distribute-list* berhasil menolak rute tidak sah dari R4-ATTACKER. Setelah rute tidak sah ditolak, jalur komunikasi kembali menggunakan rute valid menuju jaringan masing-masing *client*. Hal ini terlihat dari pulihnya konektivitas pada seluruh alur dan nilai *packet loss* yang kembali menjadi 0%.

Secara keseluruhan, hasil analisis QoS pada topologi EIGRP menunjukkan bahwa kondisi *baseline* berjalan normal dengan *packet loss* 0%. Saat *route injection* diterapkan, gangguan muncul pada alur komunikasi yang menuju atau melibatkan target serangan, dengan rata-rata *packet loss* sebesar 66,67% pada setiap target. Setelah mitigasi diterapkan, seluruh alur kembali normal dengan *packet loss* 0%. Dengan demikian, *basic filtering* menggunakan *prefix-list* melalui *distribute-list* terbukti mampu menolak rute tidak sah dan memulihkan komunikasi pada topologi EIGRP.

c. Perbandingan QoS BGP dan EIGRP

Setelah hasil pengujian QoS pada topologi BGP dan EIGRP dianalisis secara terpisah, tahap berikutnya adalah membandingkan nilai rata-rata dari kedua protokol. Perbandingan ini dilakukan untuk melihat perbedaan kondisi jaringan pada saat *baseline*, saat terjadi *route injection*, dan setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan. Parameter yang dibandingkan meliputi *packet loss*, *delay*, dan *throughput*.

Rekapitulasi perbandingan rata-rata QoS antara BGP dan EIGRP ditunjukkan pada Tabel 4.20.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.20 Rekapitulasi Perbandingan Rata-rata QoS BGP dan EIGRP

| Protokol | Kondisi | Delay Terukur | Kategori Delay | Packet Loss | Kategori Packet Loss | Throughput | Protokol |
|---|---|---|---|---|---|---|---|
| BGP | Baseline | 120,14 ms | Sangat Baik | 0% | Sangat Baik | 1,440 Kbps | BGP |
| BGP | Route Injection | 75,34 ms* | Sangat Baik* | 66,67 % | Buruk | 0,957 Kbps | BGP |
| BGP | Setelah Mitigasi | 45,58 ms | Sangat Baik | 0% | Sangat Baik | 1,477 Kbps | BGP |
| EIGRP | Baseline | 30,69 ms | Sangat Baik | 0% | Sangat Baik | 1,498 Kbps | EIGRP |
| EIGRP | Route Injection | 75,79 ms* | Sangat Baik* | 66,67 % | Buruk | 0,967 Kbps | EIGRP |
| EIGRP | Setelah Mitigasi | 60,87 ms | Sangat Baik | 0% | Sangat Baik | 1,468 Kbps | EIGRP |

Keterangan: tanda (*) menunjukkan bahwa nilai *delay* pada kondisi *route injection* hanya dihitung dari alur yang masih memperoleh balasan *Echo Reply*, sehingga tidak mewakili keseluruhan kondisi jaringan.

Berdasarkan Tabel 4.20, pada kondisi *baseline* kedua protokol menunjukkan nilai *packet loss* sebesar 0%. Hal ini menunjukkan bahwa sebelum *route injection* diterapkan, komunikasi antar-*client* pada topologi BGP dan EIGRP berjalan normal. Pada kondisi ini, BGP memiliki nilai *delay* rata-rata sebesar 120,14 ms dengan *throughput* sebesar 1,440 Kbps, sedangkan EIGRP memiliki nilai *delay* rata-rata sebesar 30,69 ms dengan *throughput* sebesar 1,498 Kbps.

Saat *route injection* diterapkan, nilai *packet loss* pada kedua protokol meningkat menjadi 66,67%. Nilai tersebut menunjukkan bahwa sebagian besar alur komunikasi yang menuju atau melibatkan target serangan mengalami kegagalan. Berdasarkan kategori *packet loss,* kondisi ini termasuk kategori buruk. Dengan demikian, *route*

*injection* terbukti memberikan dampak signifikan terhadap kualitas komunikasi pada topologi BGP maupun EIGRP.

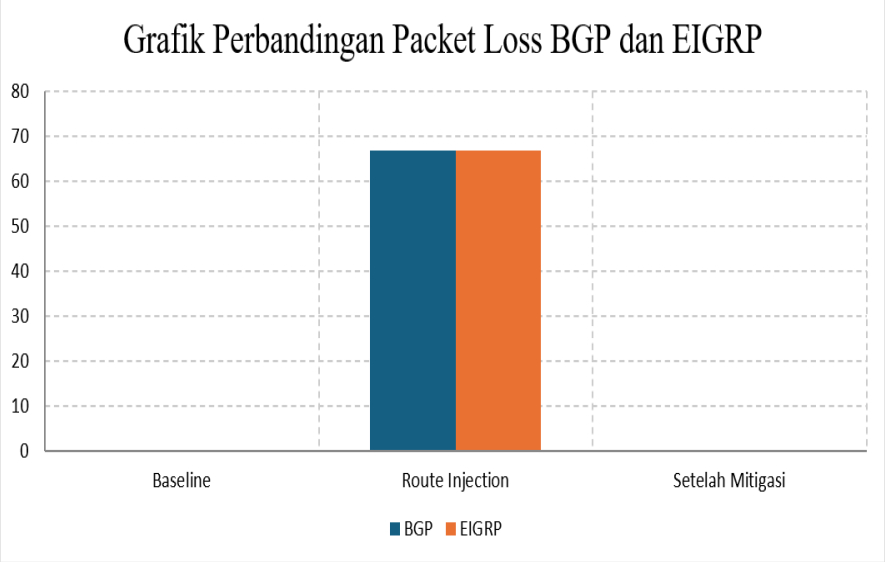
Nilai *delay* pada kondisi *route injection* tidak dapat dijadikan indikator utama dalam menilai kualitas jaringan secara keseluruhan. Hal ini disebabkan karena nilai *delay* hanya dihitung dari alur yang masih memperoleh balasan *Echo Reply*. Sementara itu, alur yang mengalami *packet loss* sebesar 100% tidak memiliki nilai *delay* terukur karena tidak terdapat paket balasan dari alamat tujuan. Oleh karena itu, dampak utama serangan lebih jelas terlihat dari peningkatan *packet loss* dan penurunan *throughput*.

Pada kondisi setelah mitigasi, nilai *packet loss* pada BGP dan EIGRP kembali menjadi 0%. Hal ini menunjukkan bahwa *basic filtering* menggunakan *prefix-list* berhasil menolak rute tidak sah dari R4-ATTACKER. Pada BGP, nilai *throughput* meningkat menjadi 1,477 Kbps, sedangkan pada EIGRP meningkat menjadi 1,468 Kbps. Kondisi ini menunjukkan bahwa komunikasi antar-*client* kembali berjalan normal setelah rute tidak sah ditolak.

Secara umum, BGP dan EIGRP menunjukkan pola perubahan yang sama. Pada kondisi *baseline*, kedua protokol berjalan normal. Saat *route injection* diterapkan, kedua protokol mengalami peningkatan *packet loss* dan penurunan *throughput*. Setelah mitigasi diterapkan, konektivitas kembali pulih dengan nilai *packet loss* 0%. Dengan demikian, penerapan *basic filtering* menggunakan *prefix-list* terbukti efektif dalam memitigasi *route injection* pada kedua protokol.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

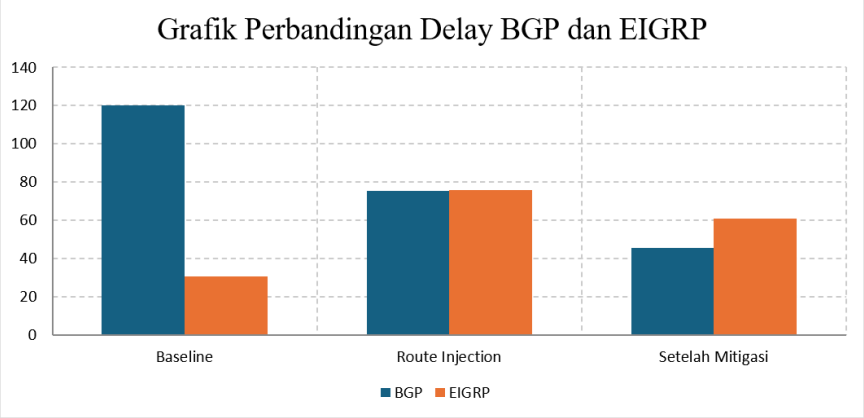



Gambar 4.33 Grafik Perbandingan Packet Loss BGP dan EIGRP

Berdasarkan Gambar 4.33, nilai *packet loss* pada kondisi *baseline* untuk BGP dan EIGRP sama-sama sebesar 0%. Hal ini menunjukkan bahwa sebelum *route injection* diterapkan, kedua protokol mampu menjalankan komunikasi antar-*client* secara normal tanpa kehilangan paket. Saat *route injection* diterapkan, nilai *packet loss* pada BGP dan EIGRP meningkat menjadi 66,67%. Peningkatan ini menunjukkan bahwa rute tidak sah yang berasal dari R4-ATTACKER berdampak terhadap kegagalan komunikasi pada alur yang menuju atau melibatkan target serangan. Setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan, nilai *packet loss* pada kedua protokol kembali menjadi 0%. Kondisi ini membuktikan bahwa mekanisme *filtering* berhasil menolak rute tidak sah dan memulihkan konektivitas jaringan.

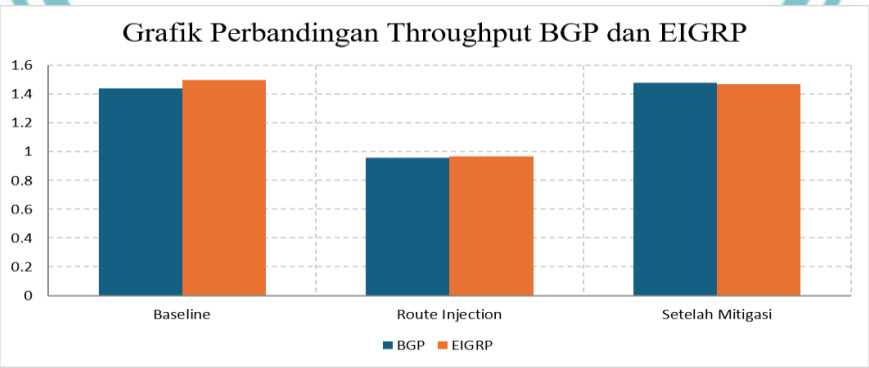
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta




Gambar 4.34 Grafik Perbandingan Delay BGP dan EIGRP

Berdasarkan Gambar 4.34, nilai *delay* pada kondisi *baseline* BGP sebesar 120,14 ms, sedangkan EIGRP sebesar 30,69 ms. Pada kondisi *route injection*, nilai *delay* terukur pada BGP sebesar 75,34 ms dan EIGRP sebesar 75,79 ms. Nilai tersebut hanya berasal dari alur komunikasi yang masih memperoleh balasan *Echo Reply*, sehingga tidak mewakili keseluruhan kondisi jaringan saat serangan terjadi. Hal ini disebabkan karena alur yang mengalami *packet loss* 100% tidak memiliki nilai *delay* yang dapat dihitung. Setelah mitigasi diterapkan, nilai *delay* BGP menjadi 45,58 ms, sedangkan EIGRP menjadi 60,87 ms. Secara umum, grafik ini menunjukkan bahwa nilai *delay* tetap berada pada kategori sangat baik, tetapi pada kondisi serangan parameter *delay* tidak dapat dijadikan indikator utama karena sebagian alur tidak memperoleh balasan.




Gambar 4.35 Grafik Perbandingan Throughput BGP dan EIGRP



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Gambar 4.35, pada kondisi *baseline* nilai *throughput* BGP sebesar 1,440 Kbps, sedangkan EIGRP sebesar 1,498 Kbps. Saat *route injection* diterapkan, nilai *throughput* BGP menurun menjadi 0,957 Kbps dan EIGRP menurun menjadi 0,967 Kbps. Penurunan ini terjadi karena sebagian alur komunikasi mengalami kegagalan akibat trafik diarahkan ke R4-ATTACKER melalui rute tidak sah. Setelah mitigasi diterapkan, nilai *throughput* kembali meningkat, yaitu BGP sebesar 1,477 Kbps dan EIGRP sebesar 1,468 Kbps. Hal ini menunjukkan bahwa setelah rute tidak sah ditolak, komunikasi antar-*client* kembali berjalan normal dan jumlah trafik ICMP yang berhasil diamati meningkat dibandingkan saat serangan.

Berdasarkan ketiga grafik tersebut, dapat disimpulkan bahwa BGP dan EIGRP memiliki pola perubahan yang serupa. Pada kondisi *baseline*, kedua protokol berjalan normal. Saat *route injection* diterapkan, terjadi peningkatan *packet loss* dan penurunan *throughput*. Setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan, nilai *packet loss* kembali menjadi 0% dan *throughput* kembali meningkat. Dengan demikian, grafik QoS memperkuat hasil tabel bahwa *prefix-list* efektif dalam menolak rute tidak sah pada BGP maupun EIGRP.

Tabel 4.21 Hasil Pengujian Waktu Serangan Masuk dan Pemulihan

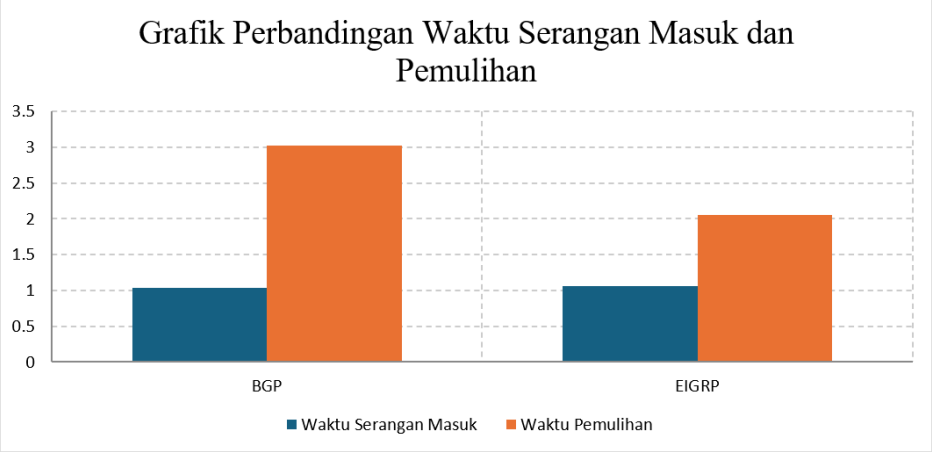
| Protokol | Target | Alur Pengujian | Waktu Serangan Masuk | Waktu Pemulihan |
|---|---|---|---|---|
| BGP | PC1 | PC2 ke PC1 | ± 1,05 detik | ± 1,05 detik |
| BGP | PC2 | PC1 ke PC2 | ± 1,00 detik | ± 6,00 detik |
| BGP | PC2 | PC2 ke PC3 | ± 1,00 detik | ± 4,00 detik |
| BGP | PC3 | PC1 ke PC3 | ± 1,05 detik | ± 1,06 detik |
| EIGRP | PC1 | PC2 ke PC1 | ± 1,06 detik | ± 1,05 detik |
| EIGRP | PC2 | PC1 ke PC2 | ± 1,07 detik | ± 4,09 detik |
| EIGRP | PC2 | PC2 ke PC3 | ± 1,06 detik | ± 2,05 detik |
| EIGRP | PC3 | PC1 ke PC3 | ± 1,06 detik | ± 1,06 detik |

Berdasarkan Tabel 4.21, waktu serangan masuk pada BGP dan EIGRP berada pada kisaran sekitar satu detik. Pada BGP, waktu serangan masuk berada pada rentang ±1,00 sampai ±1,05 detik. Pada

EIGRP, waktu serangan masuk berada pada rentang ±1,06 sampai ±1,07 detik. Hal ini menunjukkan bahwa rute tidak sah yang masuk ke proses *routing* dapat memengaruhi jalur komunikasi dalam waktu relatif cepat.

Waktu pemulihan setelah mitigasi menunjukkan nilai yang bervariasi pada setiap protokol dan alur pengujian. Pada BGP, waktu pemulihan berada pada rentang ±1,05 sampai ±6,00 detik. Pada EIGRP, waktu pemulihan berada pada rentang ±1,05 sampai ±4,09 detik. Perbedaan waktu pemulihan ini dapat terjadi karena proses pembaruan informasi *routing*, penerapan *filtering*, serta kondisi simulasi pada GNS3.

Secara umum, hasil pengujian waktu menunjukkan bahwa dampak *route injection* dapat terjadi dengan cepat setelah rute tidak sah diterima oleh router. Namun, setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan, jalur komunikasi dapat kembali pulih. Pemulihan tersebut ditandai dengan paket ICMP yang kembali memperoleh balasan *Echo Reply* setelah sebelumnya mengalami *timeout* atau *destination host unreachable*.




Gambar 4.36 Grafik Perbandingan Waktu Serangan Masuk dan Pemulihan

e. Perbandingan Hasil Pengamatan GNS3 dan Wireshark



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Selain berdasarkan nilai QoS, grafik perbandingan, dan waktu pemulihan, hasil pengujian juga dianalisis melalui perbandingan hasil pengamatan menggunakan GNS3 dan Wireshark. GNS3 digunakan sebagai lingkungan simulasi untuk membangun topologi, mengonfigurasi *routing*, melakukan pengujian *ping* dan *traceroute*, serta mengamati perubahan *routing table*. Sementara itu, Wireshark digunakan untuk melihat paket ICMP yang ter-*capture*, pasangan *Echo Request* dan *Echo Reply*, serta nilai *throughput*.

Tabel 4.22 Perbandingan Hasil Pengamatan GNS3 dan Wireshark

| Kondisi | Hasil pada GNS3 | Hasil pada Wireshark | Keterangan |
|---|---|---|---|
| Baseline | *Routing* table menggunakan rute valid, ping berhasil, dan traceroute melewati jalur normal | Paket ICMP menampilkan pasangan Echo Request dan Echo Reply | Jaringan berjalan normal |
| Route Injection | Terjadi perubahan rute menuju R4-ATTACKER, ping mengalami timeout atau destination host unreachable, dan traceroute berubah menuju R4 | Paket ICMP pada alur terdampak tidak memperoleh balasan normal dan nilai throughput menurun | Jaringan terganggu akibat rute tidak sah |
| Setelah Mitigasi | Rute tidak sah tidak lagi digunakan, ping kembali memperoleh reply, dan traceroute kembali menuju jalur valid | Paket ICMP kembali menampilkan pasangan Echo Request dan Echo Reply, serta nilai throughput meningkat | Jaringan pulih setelah basic filtering diterapkan |

Berdasarkan Tabel 4.22, hasil pengamatan menggunakan GNS3 dan Wireshark menunjukkan pola yang saling mendukung pada setiap kondisi pengujian. Pada kondisi *baseline*, GNS3 menunjukkan bahwa *routing table* masih menggunakan rute valid dan konektivitas antar-*client* berjalan normal. Hal ini diperkuat oleh hasil pengamatan Wireshark yang menampilkan adanya pasangan paket ICMP *Echo Request* dan *Echo Reply*. Kondisi tersebut menunjukkan bahwa sebelum *route injection* diterapkan, komunikasi dua arah antar-*client* dapat berjalan dengan baik.

Pada kondisi *route injection*, GNS3 menunjukkan adanya perubahan informasi *routing* menuju R4-ATTACKER. Perubahan tersebut

terlihat dari masuknya rute tidak sah ke *routing table*, perubahan *next-hop* menjadi 172.16.1.40, hasil *ping* yang mengalami *timeout* atau *destination host unreachable*, serta hasil *traceroute* yang mengarah ke R4-ATTACKER. Sementara itu, Wireshark menunjukkan bahwa paket ICMP pada alur yang terdampak tidak memperoleh balasan normal dari alamat tujuan. Hal ini membuktikan bahwa perubahan informasi pada *control plane routing* berdampak langsung terhadap komunikasi pada *data plane*.

Setelah mitigasi *basic filtering* menggunakan *prefix-list* diterapkan, rute tidak sah tidak lagi digunakan dalam proses pemilihan jalur. Hasil *ping* kembali memperoleh *reply*, hasil *traceroute* kembali melewati jalur valid, dan Wireshark kembali menampilkan pasangan paket ICMP *Echo Request* dan *Echo Reply*. Kondisi ini menunjukkan bahwa *prefix-list* berhasil menolak rute tidak sah dari R4-ATTACKER dan memulihkan komunikasi antar-*client*.

Secara keseluruhan, *route injection* terbukti dapat memengaruhi pemilihan jalur pada BGP dan EIGRP. Dampaknya terlihat dari perubahan *next-hop*, gangguan konektivitas, peningkatan *packet loss*, dan penurunan *throughput*. Setelah mitigasi diterapkan, rute tidak sah berhasil ditolak, konektivitas kembali normal, dan nilai *packet loss* kembali menjadi 0%. Dengan demikian, *basic filtering* menggunakan *prefix-list* dapat dinyatakan efektif dalam membatasi dampak *route injection* pada topologi BGP maupun EIGRP.



© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

# BAB V
# PENUTUP

## 5.1 Simpulan

Berdasarkan hasil perancangan, implementasi, pengujian, dan analisis yang telah dilakukan, diperoleh beberapa simpulan sebagai berikut:

1. Pada kondisi *baseline*, simulasi jaringan pada GNS3 berhasil merepresentasikan pengujian keamanan *routing* pada dua protokol, yaitu BGP sebagai protokol *routing* antar-*Autonomous System* dan EIGRP sebagai protokol *routing* internal. Kondisi *baseline* menunjukkan bahwa hubungan *neighbor* berhasil terbentuk, *routing table* menggunakan rute valid, konektivitas antar-*client* berjalan normal, dan nilai *packet loss* pada topologi BGP maupun EIGRP sebesar 0%. Hal ini menunjukkan bahwa sebelum *route injection* diterapkan, kedua topologi berada dalam kondisi stabil.
2. Skenario *route injection* berhasil memengaruhi proses pemilihan jalur pada BGP dan EIGRP. Pada BGP, R4-ATTACKER mengiklankan *prefix host* /32 tidak sah menuju PC1, PC2, dan PC3 melalui sesi *neighbor* BGP. Pada EIGRP, R4-ATTACKER memasukkan rute statis menuju Null0, kemudian rute tersebut di-*redistribute* ke dalam EIGRP sehingga muncul sebagai rute eksternal dengan kode D EX. Karena *prefix* /32 lebih spesifik dibandingkan rute valid /24, *router* memilih rute tidak sah tersebut berdasarkan prinsip *longest prefix match*. Kondisi ini menyebabkan perubahan *next-hop* menuju R4-ATTACKER dan mengganggu jalur komunikasi yang menuju atau melibatkan target serangan.
3. Dampak *route injection* terlihat pada perubahan kualitas layanan jaringan. Pada kondisi serangan, nilai *packet loss* rata-rata meningkat menjadi 66,67% pada BGP dan EIGRP. Nilai *throughput* BGP menurun dari 1,440 Kbps pada kondisi *baseline* menjadi 0,957 Kbps saat *route injection*, sedangkan EIGRP menurun dari 1,498 Kbps menjadi 0,967 Kbps. Hasil ini menunjukkan bahwa *route*

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

*injection* tidak hanya memengaruhi informasi *routing* pada *control plane*, tetapi juga berdampak terhadap komunikasi pada *data plane*, terutama pada alur yang menuju atau melibatkan target serangan.

4. Penerapan mitigasi *basic filtering* menggunakan *prefix-list* berhasil menolak rute tidak sah dari R4-ATTACKER pada BGP dan EIGRP. Pada BGP, *prefix-list* diterapkan secara *inbound* pada *neighbor* R4-ATTACKER. Pada EIGRP, *prefix-list* diterapkan melalui *distribute-list* pada antarmuka jaringan transit. Setelah mitigasi diterapkan, rute tidak sah tidak lagi digunakan, konektivitas antar-*client* kembali normal, nilai *packet loss* kembali menjadi 0%, dan *throughput* meningkat menjadi 1,477 Kbps pada BGP serta 1,468 Kbps pada EIGRP. Dengan demikian, *basic filtering* menggunakan *prefix-list* terbukti efektif dalam membatasi dampak *route injection* pada *control plane routing* BGP maupun EIGRP.

## 5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran untuk pengembangan penelitian selanjutnya, yaitu sebagai berikut:

1. Penelitian selanjutnya dapat menguji variasi serangan routing lain, seperti route leak, manipulasi AS path, atau serangan terhadap pembentukan neighbor.
2. Mitigasi dapat dikembangkan dengan membandingkan prefix-list dengan metode lain, seperti RPKI/ROV, BGPsec, autentikasi EIGRP, atau kebijakan filtering tambahan.
3. Pengujian selanjutnya dapat menggunakan topologi yang lebih kompleks, jumlah router dan client yang lebih banyak, serta trafik selain ICMP, seperti TCP atau UDP.
4. Pada jaringan nyata, administrator disarankan menerapkan kebijakan filtering dan validasi prefix agar rute tidak sah tidak mudah masuk ke proses routing..

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## DAFTAR PUSTAKA

Antoni Musril, H., Sri Artika, F., Derta, S., Darmawati, G., & Okra, R. (2021). Quality of Service EIGRP *Routing* Protocol on Campus Area Network. *Journal of Physics: Conference Series*, *1779*(1). https://doi.org/10.1088/1742-6596/1779/1/012005

Auliya, K. X., & Dian W. Chandra. (2025). Analisis hubungan antara kualitas layanan jaringan dan pengalaman pengguna pada layanan video streaming youtube. *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi*, *4*(3), 272–281. https://doi.org/10.24246/itexplore.v4i3.2025.pp272-281

Eko Kurniawanto, S. P. (2021). Implementasi *Routing* Protokol Border Gateway Protocol (Bgp) Pada Router Mikrotik Rb 2011 Di Kominfo Kabupaten Solok Selatan. *Jurnal Teknoif Teknik Informatika Institut Teknologi Padang*, *9*(2), 97–103. https://doi.org/10.21063/jtif.2021.v9.2.97-103

Global, P. (2023). *Everything You Need to Know About Distribute and Prefix Lists*. https://info.pivitglobal.com/resources/distribute-and-prefix-lists?utm_source

Kabir, M. H., Kabir, M. A., Islam, M. S., Mortuza, M. G., & Mohiuddin, M. (2021). Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF *Routing* Protocols. *Engineering Proceedings*, *10*(1). https://doi.org/10.3390/ecsa-8-11285

Labs, Q. (2025). *Understanding BGP hijacking: risks, real-world examples, and how to protect your network in 2025*. https://qrator.net/blog/details/why-bgp-hijacking-still-threatens-global-networks/

McDaniel, T., Smith, J. M., & Schuchard, M. (2021). Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis. *28th Annual Network and Distributed System Security Symposium, NDSS 2021*, 1–16. https://doi.org/10.14722/ndss.2021.23080

Nisa, I. S. N., Rahmat Miyarno Saputro, Tegar Fatwa Nugroho, & Alfirna Rizqi Lahitani. (2024). Analisis Quality of Service (QoS) Menggunakan Standar

Parameter Tiphon pada Jaringan Internet Berbasis Wi-Fi Kampus 1 Unjaya. *Teknomatika: Jurnal Informatika Dan Komputer*, *17*(1), 1–9. https://doi.org/10.30989/teknomatika.v17i1.1307

Nugroho, H. A. S. A., Sonhaji, & Prasetyo, A. C. (2024). Evaluasi Kinerja Jaringan WiFi Mahasiswa: Analisis Throughput, Delay, Jitter, dan Packet loss. *Jurnal BATIRSI*, *8*(1), 23–27.

OECD. (2022). *Routing security: BGP incidents, mitigation techniques and policy actions*. (330). https://www.oecd-ilibrary.org/science-and-technology/*routing*-security_40be69c8-en%0Afiles/11282/OECD - 2022 - *Routing* security BGP incidents, mitigation techni.pdf

Pranaya, V. B., & Wellem, T. (2021). Implementasi BGP dan Resource Public Key Infrastructure menggunakan BIRD untuk Keamanan *Routing*. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(6), 1161–1170. https://doi.org/10.29207/resti.v5i6.3631

Saad, M., Anwar, A., Ahmad, A., Alasmary, H., Yuksel, M., & Mohaisen, D. (2022). RouteChain: Towards Blockchain-based secure and efficient BGP *routing*. *Computer Networks*, *217*(September). https://doi.org/10.1016/j.comnet.2022.109362

Sahal Nurhidayah, M., Pranindito, D., & Dyah Wahyuningrum, R. (2022). Analisis dan Simulasi *Routing* Border Gateway Protocol (BGP) Antar Autonomous System menggunakan Free Range *Routing* (FRR). *Jurnal Litek : Jurnal Listrik Telekomunikasi Elektronika*, *19*(2), 48–56. https://doi.org/10.30811/litek.v19i2.11

Scott, B. A., Johnstone, M. N., & Szewczyk, P. (2024). A Survey of Advanced Border Gateway Protocol Attack Detection Techniques. *Sensors*, *24*(19), 6414. https://doi.org/10.3390/s24196414

Sermpezis, P., Kotronis, V., Arakadakis, K., & Vakali, A. (2021). Estimating the Impact of BGP Prefix Hijacking. *2021 IFIP Networking Conference, IFIP Networking 2021*. https://doi.org/10.23919/IFIPNetworking52078.2021.9472813



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Shapira, T., & Shavitt, Y. (2022). AP2Vec: An Unsupervised Approach for BGP Hijacking Detection. *IEEE Transactions on Network and Service Management*, *19*(3), 2255–2268. https://doi.org/10.1109/TNSM.2022.3166450

Siddiqui, A. (2022). *BGP Security in 2021 - MANRS*. https://manrs.org/2022/02/bgp-security-in-2021/?utm_source

Vidananda Agastya, I. B., Wiharta, D. M., & Putra Sastra, N. (2021). Perancangan Jaringan Dengan Protokol Eigrp Di Universitas Udayana. *Jurnal SPEKTRUM*, *8*(2), 61. https://doi.org/10.24843/spektrum.2021.v08.i02.p8

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## DAFTAR RIWAYAT HIDUP

Sahrul Apriandi lahir di Banyumas pada tanggal 27 April 2004. Penulis menyelesaikan pendidikan dasar di SDN Sepanjang Jaya 1 Kota Bekasi pada tahun 2016. Setelah itu, penulis melanjutkan pendidikan ke SMPN 16 Kota Bekasi dan lulus pada tahun 2019.

Pada tahun 2022, penulis menyelesaikan pendidikan menengah kejuruan di SMKN 3 Kota Bekasi. Setelah menyelesaikan pendidikan menengah kejuruan, penulis melanjutkan pendidikan tinggi di Politeknik Negeri Jakarta, Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan Jaringan.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

## LAMPIRAN

Bukti Konfigurasi Route Injection melalui Redistribusi Static Route pada EIGRP

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip route 192.168.17.2 255.255.255.255 Null0
R4(config)#
R4(config)#router eigrp 100
R4(config-router)# redistribute static metric 10000 100 255 1 1500
R4(config-router)#end
R4#
```

Konfigurasi Route Injection melalui Pengiklanan Prefix BGP pada R4-ATTACKER

```
R4-ATTACKER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-ATTACKER(config)#ip route 192.168.17.2 255.255.255.255 Null0
R4-ATTACKER(config)#
R4-ATTACKER(config)#router bgp 6440
R4-ATTACKER(config-router)# network 192.168.17.2 mask 255.255.255.255
R4-ATTACKER(config-router)#
R4-ATTACKER(config-router)#end
R4-ATTACKER#clear ip bgp * soft
```

Hasil Verifikasi Rute Tidak Sah EIGRP Saat *Route Injection*

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.17.0/24 is variably subnetted, 2 subnets, 2 masks
D        192.168.17.0/24 [90/30720] via 172.16.1.20, 00:26:07, FastEthernet0/0
D EX     192.168.17.2/32
           [170/284160] via 172.16.1.40, 00:00:56, FastEthernet0/0
D     192.168.18.0/24 [90/30720] via 172.16.1.30, 00:26:07, FastEthernet0/0
```

Hasil Verifikasi *Routing* EIGRP Setelah Mitigasi *Basic Filtering*

Lanjutan

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.17.0/24 [90/30720] via 172.16.1.20, 00:29:16, FastEthernet0/0
D     192.168.18.0/24 [90/30720] via 172.16.1.30, 00:29:16, FastEthernet0/0
```

Rute Tidak Sah 192.168.17.2/32 pada *Routing* Table R1-KOMINFO

```
R1-KOMINFO#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.17.0/24 is variably subnetted, 2 subnets, 2 masks
B        192.168.17.0/24 [20/0] via 172.16.1.20, 00:03:40
B        192.168.17.2/32 [20/0] via 172.16.1.40, 00:00:31
B     192.168.18.0/24 [20/0] via 172.16.1.30, 00:03:40
```

Status Neighbor BGP dan Penerimaan Prefix dari R4-ATTACKER saat Route Injection

```
R1-KOMINFO#show ip bgp summary
BGP router identifier 192.168.16.1, local AS number 6410
BGP table version is 5, main routing table version 5
4 network entries using 576 bytes of memory
4 path entries using 320 bytes of memory
4/4 BGP path/bestpath attribute entries using 544 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1512 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.20     4         6420      10      11        5    0    0 00:05:34        1
172.16.1.30     4         6430      10      11        5    0    0 00:05:33        1
172.16.1.40     4         6440      13      18        5    0    0 00:05:35        1
R1-KOMINFO#
```

Verifikasi Prefix-list dan Tabel BGP Setelah Mitigasi pada R1-KOMINFO



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lanjutan

```
R1-KOMINFO#show ip prefix-list FILTER-INVALID-BGP
ip prefix-list FILTER-INVALID-BGP: 2 entries
   seq 5 deny 192.168.17.2/32
   seq 100 permit 0.0.0.0/0 le 32
R1-KOMINFO#show ip bgp
BGP table version is 6, local router ID is 192.168.16.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  192.168.16.0     0.0.0.0                  0         32768 i
 *>  192.168.17.0     172.16.1.20              0             0 6420 i
 *>  192.168.18.0     172.16.1.30              0             0 6430 i
```

Capture ICMP Saat *Route Injection* pada BGP

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 3.333528 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0xef4b, seq=1/256, ttl=63 (no response found!) |
| 4 | 3.348729 | 172.16.1.30 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 5 | 4.399099 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0xf04b, seq=2/512, ttl=63 (no response found!) |
| 6 | 4.414310 | 172.16.1.30 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 7 | 5.466356 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0xf14b, seq=3/768, ttl=63 (no response found!) |
| 8 | 5.481888 | 172.16.1.30 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 11 | 6.536318 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0xf24b, seq=4/1024, ttl=63 (no response found!) |
| 12 | 6.552054 | 172.16.1.30 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 13 | 7.613546 | 192.168.16.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) request id=0xf34b, seq=5/1280, ttl=63 (no response found!) |
| 14 | 7.629228 | 172.16.1.30 | 192.168.16.2 | ICMP | 70 | Destination unreachable (Host unreachable) |

Capture ICMP Setelah Mitigasi pada EIGRP

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6 | 16.850927 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x1c40, seq=1/256, ttl=63 (reply in 8) |
| 7 | 18.862717 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x1e40, seq=2/512, ttl=63 (reply in 9) |
| 8 | 19.902807 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x1c40, seq=1/256, ttl=63 (request in 6) |
| 9 | 19.902807 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x1e40, seq=2/512, ttl=63 (request in 7) |
| 11 | 20.876392 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2040, seq=3/768, ttl=63 (reply in 12) |
| 12 | 20.906334 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2040, seq=3/768, ttl=63 (request in 11) |
| 13 | 21.960099 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2140, seq=4/1024, ttl=63 (reply in 14) |
| 14 | 21.989872 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2140, seq=4/1024, ttl=63 (request in 13) |
| 15 | 23.040136 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2340, seq=5/1280, ttl=63 (reply in 16) |
| 16 | 23.069696 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2340, seq=5/1280, ttl=63 (request in 15) |
| 17 | 24.126601 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2440, seq=6/1536, ttl=63 (reply in 18) |
| 18 | 24.157347 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2440, seq=6/1536, ttl=63 (request in 17) |
| 20 | 25.207331 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2540, seq=7/1792, ttl=63 (reply in 21) |
| 21 | 25.238368 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2540, seq=7/1792, ttl=63 (request in 20) |
| 23 | 26.272704 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2640, seq=8/2048, ttl=63 (reply in 24) |
| 24 | 26.302591 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2640, seq=8/2048, ttl=63 (request in 23) |
| 25 | 27.356620 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2740, seq=9/2304, ttl=63 (reply in 26) |



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lanjutan

Hasil Pengujian Ping 30 Paket dari PC1 menuju PC3

```
PC1> ping 192.168.18.2 -c 30
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=75.734 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.855 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=60.173 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=62.182 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=62.237 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=60.599 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=61.792 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=60.989 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=60.292 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=60.700 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=60.866 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=60.560 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=62.326 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=61.338 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=60.603 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=60.539 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=61.965 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=62.191 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=61.950 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=60.574 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=59.555 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=63.033 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=62.534 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=61.174 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=60.295 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=61.760 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=59.746 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=61.232 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=61.792 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=62.192 ms
```

Hasil Pengujian Ping 30 Paket dari PC2 menuju PC3

```
PC2> ping 192.168.18.2 -c 30
192.168.18.2 icmp_seq=1 timeout
192.168.18.2 icmp_seq=2 timeout
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.373 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=60.352 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=60.278 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=61.195 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=62.133 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=60.521 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=60.307 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=62.680 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=60.829 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=63.102 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=60.958 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=57.655 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=62.169 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=61.014 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=59.982 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=61.288 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=61.382 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=59.996 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=61.597 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=61.396 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=62.370 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=62.043 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=60.039 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=61.665 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=61.929 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=60.937 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=61.808 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=61.800 ms
```

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lanjutan

Hasil Verifikasi Rute BGP pada Router R1-KOMINFO

```
R1-KOMINFO#show ip route 192.168.18.2
Routing entry for 192.168.18.0/24
  Known via "bgp 6410", distance 20, metric 0
  Tag 6430, type external
  Last update from 172.16.1.30 02:06:39 ago
  Routing Descriptor Blocks:
  * 172.16.1.30, from 172.16.1.30, 02:06:39 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6430
      MPLS label: none
```

Hasil Pengujian Ping 30 Paket dari PC2 Menuju Jaringan 192.168.16.2

```
PC2> ping 192.168.16.2 -c 30
84 bytes from 192.168.16.2 icmp_seq=1 ttl=62 time=61.207 ms
84 bytes from 192.168.16.2 icmp_seq=2 ttl=62 time=62.888 ms
84 bytes from 192.168.16.2 icmp_seq=3 ttl=62 time=61.519 ms
84 bytes from 192.168.16.2 icmp_seq=4 ttl=62 time=60.462 ms
84 bytes from 192.168.16.2 icmp_seq=5 ttl=62 time=61.166 ms
84 bytes from 192.168.16.2 icmp_seq=6 ttl=62 time=60.823 ms
84 bytes from 192.168.16.2 icmp_seq=7 ttl=62 time=60.224 ms
84 bytes from 192.168.16.2 icmp_seq=8 ttl=62 time=67.869 ms
84 bytes from 192.168.16.2 icmp_seq=9 ttl=62 time=61.070 ms
84 bytes from 192.168.16.2 icmp_seq=10 ttl=62 time=61.156 ms
84 bytes from 192.168.16.2 icmp_seq=11 ttl=62 time=62.458 ms
84 bytes from 192.168.16.2 icmp_seq=12 ttl=62 time=72.276 ms
84 bytes from 192.168.16.2 icmp_seq=13 ttl=62 time=62.381 ms
84 bytes from 192.168.16.2 icmp_seq=14 ttl=62 time=61.355 ms
84 bytes from 192.168.16.2 icmp_seq=15 ttl=62 time=62.558 ms
84 bytes from 192.168.16.2 icmp_seq=16 ttl=62 time=61.420 ms
84 bytes from 192.168.16.2 icmp_seq=17 ttl=62 time=62.121 ms
84 bytes from 192.168.16.2 icmp_seq=18 ttl=62 time=62.589 ms
84 bytes from 192.168.16.2 icmp_seq=19 ttl=62 time=61.370 ms
84 bytes from 192.168.16.2 icmp_seq=20 ttl=62 time=60.964 ms
84 bytes from 192.168.16.2 icmp_seq=21 ttl=62 time=60.417 ms
84 bytes from 192.168.16.2 icmp_seq=22 ttl=62 time=61.394 ms
84 bytes from 192.168.16.2 icmp_seq=23 ttl=62 time=61.289 ms
84 bytes from 192.168.16.2 icmp_seq=24 ttl=62 time=63.642 ms
84 bytes from 192.168.16.2 icmp_seq=25 ttl=62 time=62.905 ms
84 bytes from 192.168.16.2 icmp_seq=26 ttl=62 time=74.522 ms
84 bytes from 192.168.16.2 icmp_seq=27 ttl=62 time=48.258 ms
84 bytes from 192.168.16.2 icmp_seq=28 ttl=62 time=56.000 ms
84 bytes from 192.168.16.2 icmp_seq=29 ttl=62 time=59.326 ms
84 bytes from 192.168.16.2 icmp_seq=30 ttl=62 time=61.835 ms
```

Capture Paket ICMP Selama Pengujian Konektivitas

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 2 | 3.738306 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc321, seq=1/256, ttl=63 (reply in 3) |
| 3 | 3.769362 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc321, seq=1/256, ttl=63 (request in 2) |
| 4 | 4.827182 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc521, seq=2/512, ttl=63 (reply in 5) |
| 5 | 4.856946 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc521, seq=2/512, ttl=63 (request in 4) |
| 6 | 5.912484 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc621, seq=3/768, ttl=63 (reply in 7) |
| 7 | 5.942565 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc621, seq=3/768, ttl=63 (request in 6) |
| 8 | 6.990648 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc721, seq=4/1024, ttl=63 (reply in 9) |
| 9 | 7.021202 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc721, seq=4/1024, ttl=63 (request in 8) |
| 10 | 8.077892 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc821, seq=5/1280, ttl=63 (reply in 11) |
| 11 | 8.109430 | 192.168.18.2 | 192.168.16.2 | ICMP | 98 | Echo (ping) reply id=0xc821, seq=5/1280, ttl=63 (request in 10 |
| 12 | 9.160396 | 192.168.16.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0xc921, seq=6/1536, ttl=63 (reply in 13) |



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lanjutan

Hasil Verifikasi Rute BGP pada Router R1-KOMINFO

```
R1-KOMINFO#show ip bgp 192.168.18.2
BGP routing table entry for 192.168.18.2/32, version 17
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 14
  6440
    172.16.1.40 from 172.16.1.40 (4.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
R1-KOMINFO#show ip route 192.168.18.2
Routing entry for 192.168.18.2/32
  Known via "bgp 6410", distance 20, metric 0
  Tag 6440, type external
  Last update from 172.16.1.40 00:42:49 ago
  Routing Descriptor Blocks:
  * 172.16.1.40, from 172.16.1.40, 00:42:49 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6440
      MPLS label: none
```

Hasil Konfigurasi *Route Injection* pada Router Attacker

```
R4-ATTACKER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-ATTACKER(config)#ip route 192.168.18.2 255.255.255.255 Null0
R4-ATTACKER(config)#
R4-ATTACKER(config)#router bgp 6440
R4-ATTACKER(config-router)# network 192.168.18.2 mask 255.255.255.255
R4-ATTACKER(config-router)#end
```

Hasil Konfigurasi *Basic Filtering* pada Router R1-KOMINFO

```
R1-KOMINFO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-KOMINFO(config)#$ist FILTER-INVALID-BGP seq 5 deny 192.168.18.2/32
%Insertion failed - seq # exists with different policy: 5
R1-KOMINFO(config)#$ist FILTER-INVALID-BGP seq 10 permit 0.0.0.0/0 le 32
R1-KOMINFO(config)#
R1-KOMINFO(config)#router bgp 6410
R1-KOMINFO(config-router)#$72.16.1.40 prefix-list FILTER-INVALID-BGP in
R1-KOMINFO(config-router)#end
```

Hasil Pengujian *Traceroute* Menuju Jaringan 192.168.18.2

```
PC1> trace 192.168.18.2
trace to 192.168.18.2, 8 hops max, press Ctrl+C to stop
 1   192.168.16.1   15.658 ms  14.193 ms  15.079 ms
 2   172.16.1.40   45.362 ms  45.876 ms  45.781 ms
 3   *172.16.1.40   45.859 ms (ICMP type:3, code:1, Destination host unreachable)
```

Capture Paket ICMP Setelah Mitigasi pada EIGRP

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 83 | 31.458956 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x29ee, seq=25/6400, ttl=63 (request in 8 |
| 84 | 32.512750 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2aee, seq=26/6656, ttl=63 (reply in 85) |
| 85 | 32.542511 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2aee, seq=26/6656, ttl=63 (request in 8 |
| 88 | 33.594640 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2bee, seq=27/6912, ttl=63 (reply in 89) |
| 89 | 33.625410 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2bee, seq=27/6912, ttl=63 (request in 8 |
| 93 | 34.677765 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2cee, seq=28/7168, ttl=63 (reply in 94) |
| 94 | 34.707670 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2cee, seq=28/7168, ttl=63 (request in 9 |
| 95 | 35.760221 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2dee, seq=29/7424, ttl=63 (reply in 96) |
| 96 | 35.791025 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2dee, seq=29/7424, ttl=63 (request in 9 |
| 97 | 36.849156 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x2eee, seq=30/7680, ttl=63 (reply in 98) |
| 98 | 36.880175 | 192.168.18.2 | 192.168.17.2 | ICMP | 98 | Echo (ping) reply id=0x2eee, seq=30/7680, ttl=63 (request in 9 |

Lanjutan

Hasil Verifikasi Tabel *Routing* EIGRP Setelah Mitigasi

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.17.0/24 [90/30720] via 172.16.1.20, 03:26:02, FastEthernet0/0
      192.168.18.0/24 is variably subnetted, 2 subnets, 2 masks
D        192.168.18.0/24 [90/30720] via 172.16.1.30, 03:26:02, FastEthernet0/0
D EX     192.168.18.2/32
           [170/284160] via 172.16.1.40, 00:00:02, FastEthernet0/0
```

Hasil Pengujian *Ping* 30 Paket dari PC1 Menuju Jaringan 192.168.18.2

```
PC1> ping 192.168.18.2 -c 30
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=61.191 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.042 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.830 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=60.109 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=62.294 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=61.270 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=61.368 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=61.380 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=61.125 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=62.149 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=61.125 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=60.874 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=61.476 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=61.751 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=61.592 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=62.227 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=61.176 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=61.692 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=60.526 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=62.179 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=61.552 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=61.679 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=60.613 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=63.482 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=54.771 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=64.642 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=60.830 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=60.187 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=62.232 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=61.278 ms
```

Capture Paket ICMP Sebelum Mitigasi pada EIGRP

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 7 | 5.013734 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x59e9, seq=1/256, ttl=63 (no response fo |
| 8 | 5.028658 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 9 | 6.079224 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5ae9, seq=2/512, ttl=63 (no response fo |
| 10 | 6.094733 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 13 | 7.148927 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5be9, seq=3/768, ttl=63 (no response fo |
| 14 | 7.164584 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 16 | 8.218579 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5ce9, seq=4/1024, ttl=63 (no response f |
| 17 | 8.233795 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 21 | 9.281616 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5de9, seq=5/1280, ttl=63 (no response f |
| 22 | 9.296896 | 172.16.1.40 | 192.168.17.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 24 | 10.350070 | 192.168.17.2 | 192.168.18.2 | ICMP | 98 | Echo (ping) request id=0x5ee9, seq=6/1536, ttl=63 (no response f |

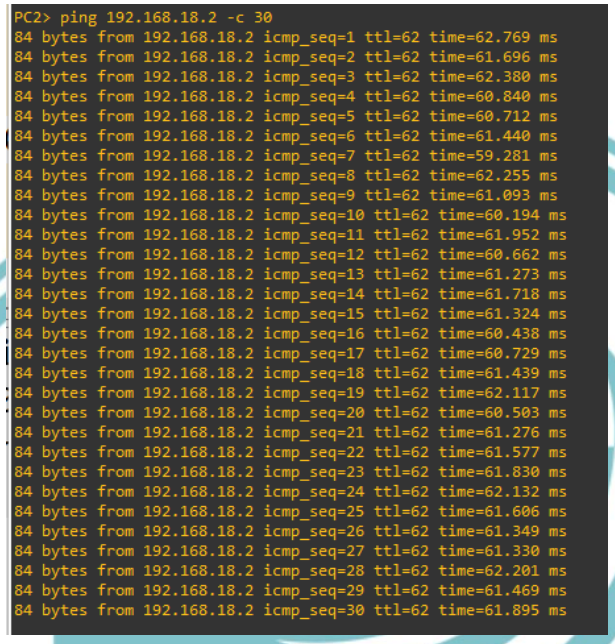


© Hak Cipta milik Politeknik Negeri Jakarta

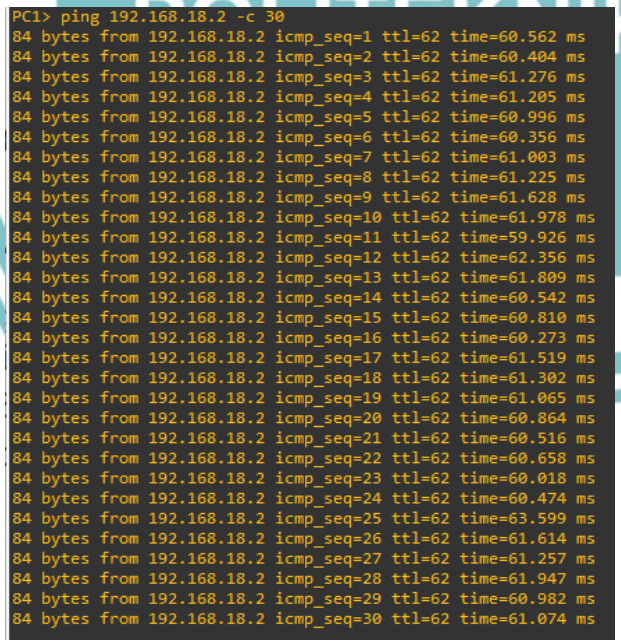
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lanjutan

Hasil Pengujian *Ping* 30 Paket dari PC2 Menuju Jaringan 192.168.18.2 Setelah Mitigasi




Hasil Pengujian *Ping* 30 Paket dari PC1 Menuju Jaringan 192.168.18.2 Setelah Mitigasi






© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta