# IMPLEMENTASI DAN ANALISIS JARINGAN MPLS MENGGUNAKAN ALGORITMA SHA SEBAGAI KEAMANAN JARINGAN PADA KOMUNIKASI VOIP

## *MPLS Network Implementation And Analysis Using SHA Algorithm As A Network Security In Voip Communication*

**Marina Saraswati[1], Muhammad Iqbal, S.T., M.T [2], Dr. Indrarini Dyah Irawati, S.T., M.T [3]**
**Program Studi D3 Teknologi Telekomunikasi,Fakultas Ilmu Terapan, Universitas Telkom**
**Jl. Telekomunikasi No.1 Dayeuhkolot Bandung 40257 Indonesia**
**[1]marinasaraswati@student.telkomuniversity.ac.id, [2]miqbal@tass.telkomuniversity.ac.id,**
**[3]indrarini@tass.telkomuniversity.ac.id**

**Abstrak**

Seiring dengan perkembangan zaman teknologi informasi dan telekomunikasi maka semakin banyak kebutuhan akan kecepatan jaringan internet. Terutama untuk menghubungkan jaringan yang satu dengan jaringan yang lain, dimana kedua tempat jaringan tersebut letaknya saling berjauhan dan harus membutuhkan koneksi yang aman.

Dengan skalabilitas dan *traffic engineering* sebagai sisi keamanan *confidentiality* Teknologi MPLS memiliki kecepatan akses data yang cukup tinggi, selain itu juga dapat menghindari kemacetan dalam lalu lintas data di dalam suatu jaringan,

Dengan diterapkannya teknologi MPLS dengan menggunakan autentikasi pada routing protocol nya diharapkan dapat memperoleh suatu metode akses jaringan yang aman dan cepat dengan sistem keamanan data yang tinggi.

**Kata kunci : kata kunci : MPLS, *Routing Protocol Authentication***

***Abstract***

Along with the development of the age of information technology and telecommunications, the more the need for internet network speeds. Especially to connect one network to the other network, where the two network sites are located far apart and must require a secure connection.

With scalability and traffic engineering as the security side of confidentiality MPLS technology has a high enough data access speed, but it can also avoid congestion in data traffic on a network,

With the implementation of MPLS technology using authentication in the routing protocol it is expected to obtain a method of network access that is safe and fast with a high data security system.

.

**Keyword : MPLS,Routing Protocol Authentication**

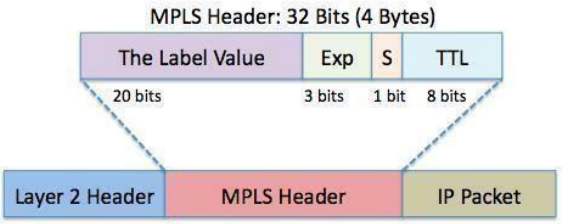
## 1. Pendahuluan

Seiring dengan perkembangan zaman teknologi informasi dan telekomunikasi maka semakin banyak kebutuhan akan kecepatan jaringan internet. Terutama untuk menghubungkan jaringan yang satu dengan jaringan yang lain, dimana kedua tempat jaringan tersebut letaknya saling berjauhan, maka untuk menghubungkan keduanya agar terjadi suatu koneksi yang lebih aman dan efisien maka dibutuhkan teknologi MPLS.Pada penelitian[9] VOIP dengan melakukan tunelling. Evaluasi dilakukan dengan mengukur kualitas layanan VOIP baik tanpa menggunakan MPLS maupun dengan menggunakan MPLSVPN Berdasarkan hasil penelitian dapat disimpulkan bahwa dengan penerapan VPN pada jaringan MPLS mampu meningkatkan Quality of Service (QoS) protokol routing OSPF pada jaringan VoIP tetapi

tidak ada konfigurasi autentikasi.Pada Penelitian [8] VoIP yang dilewatkan melalui jaringan MPLSVPN lebih baik performansi nya daripada trafik VoIP yang dilewatkan melalui jaringan IP biasa. Sehingga kualitas suara yang dihasilkan oleh jaringan VoIP over MPLS lebih baik daripada VoIP dengan jaringan IP biasa. Lalu pada penelitian [2] menganalisis mengenai keamanan VOIP pada jaringan MPLSVPN dengan mengimplementasikan tunnelling Ipsec namun metode yang digunakan membuat kinerja dari VOIP tersebut menurun.Sesuai pada permasalahan diatas pada tugas akhir ini akan melakukan perancangan jaringan MPLS autentikasi routing OSPF dengan menggunakan algoritma HMAC-SHA untuk membutktikan apakah algoritma enkripsi tersebut dapat menahan dari serangan *Injection Ipv4*, *Spoofing*, *Sniffing* dan juga tetap menghasilkan komunikasi VOIP yang aman dan baik.

## 2. Dasar Teori

### 2.1 Multi Protocol Label Switching (MPLS)




*Gambar 2.1 Header MPLS*

MPLS(Multi protocol label switching) metode meneruskan data dengan menggunakan label yang di lekatkan pada IP (forwarding ) melalui suatu jaringan backbone dengan berkecepatan tinggi dengan menggabungkan teknologi pada layer 2 dan routing pada layer 3. Mpls ini juga digunakan untuk mempercepat pengiriman paket dengan cara melakukan enkapsulasi pada paket IP dengan memasang header pada MPLS.

#### 2.1.1 MPLS Cloud

1. Label Edge Router (LER) : digunakan untuk menambahkan label ketika paket masuk atau informasi label pada router
2. Label Switch Router (LSR): label switch router yang digunakan untuk memforward ataumeneruskan paket yang telah di beri label dan terhubung juga dengan jaringan luar
3. MPLS Egress Node : MPLS node yang mengatur trafik saat meninggalkan MPLS domain
4. MPLS Ingress Node : MPLS node yang mengatur trafik saat memasuki MPLS domain
5. MPLS label : merupakan label yang di tempatkan sebagai MPLS header
6. MPLS Node : node yang menjalankan MPLS yang sebagai control protocol yang akan meneruskan paket berdasarkan label

Pada gambar MPLS cloud tersebut dapat di simpulkan bahwa paket yang masuk dari IP domain dan masuk ke dalam router LER dan selanjutnya akan diberi label dan akan di forward pada router LSR dan masih di beri label lalu masuk ke dalam router LER dan selanjutnya akan di lepas tanpalabel.

#### 2.1.2 Prinsip Kerja MPLS

Prinsip kerja jaringan mpls yaitu ketika customer mengirim paket maka router PE (LER) akan melekatkan label pada paket tersebut. Lalu selanjutnya pada router PE mengirim paket ke router P(LSR), label pada paket tersebut akan diganti dengan laber dari router P dan akan di kirim menuju ke router selanjutnya. Selanjutnya jika paket sudah sampai pada router PE paling pojok maka label pada paket tersebut akan di lepas dan paket di kirim menuju customer.

Keuntungan memakai teknik MPLS yaitu :

a. Tidak memerlukan routing look up, namun memaksimalkan LDP database
b. Mengurangi routing loops di core network
c. Mudah melakukan aplikasi failover dan loadbalance

Istilah pada label MPLS yaitu sebagai berikut :

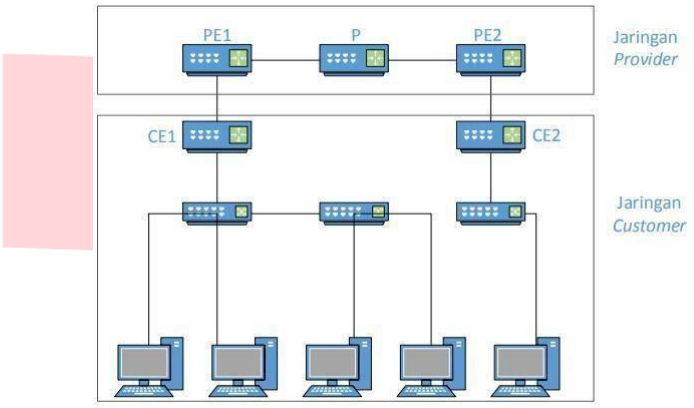
a. PUSH : yaitu memasangkan label pada paket
b. POP : melepaskan label paket lalu forwarding ke client/customer
c. SWAP : label awal di lepas lalu di ganti dengan label baru

d. Aggregate : label stack sudah di hilangkan
e. Untagged/No label : stack sudah di hilangkan dan paket di forward tanpa menggunakan label

## 2.2 VPN

Virtual Private Network (VPN) adalah sebuah jaringan komputer dimana koneksi antar perangkatnya (node) memanfaatkan jaringan publik sehingga yang diperlukan hanyalah koneksi internet di masing-masing site. Meskipun VPN menggunakan jaringan publik, keamanan dan kerahasiaan antar pengguna VPN dapat tetap terjaga karena VPN membentuk jalur virtual khusus yang hanya bisa diakses oleh pengguna VPN. MPLS VPN merupakan jaringan VPN berbasis MPLS dimana komunikasi antar pengguna menjadi lebih aman meskipun menggunakan jaringan publik.

### 2.2.1 Arsitektur MPLS-VPN




Keterangan :

a. Perangkat Customer : yaitu perangkat pada jaringan yang berhubungan langsung dengan pengguna jaringan.
b. Perangkat Customer Edge (CE) : yaitu perangkat yang terletak di paling luar jaringan customer yang berhubungan langsung dengan perangkat Provider Edge (PE) untuk meneruskan setiap paket yang dikirim untuk customer.
c. Perangkat Provider Edge (PE) : yaitu perangkat yang terletak di paling luar jaringan provider. Perangkat PE berfungsi untuk melakukan pemberian label paket, pertukaran informasi antar protokol routing, dan sebagai pembatas antara protokol routing pada customer dan provider.
d. Perangkat Provider : yaitu perangkat yang terletak di pusat jaringan provider yang berfungsi untuk melakukan proses switching dan meneruskan paket MPLS menuju perangkat PE tujuan.

### 2.2.2 Tipe MPLS-VPN

Terdapat dua tipe MPLS-VPN, yaitu :

**a. BGP/MPLS VPNs (Layer 3 VPNs)**

Tipe ini menggunakan perluasan dari protokol routing yang sudah ada dari internet (BGP-4), untuk membangun komunikasi antar lokasi yang berjauhan. Tipe ini dikategorikan dalam RFC 2547bis VPNs.

**b. Layer 2 MPLS VPNs**

Tipe ini memperluas konektivitas customer Layer 2 melalui infrastruktur MPLS. Untuk VPN tipe ini biasa disebut Martini VPNs. Perluasan dari Layer 2 VPNs juga mendukung Virtual Private LAN Services (VPLS)

## 2.3 Komponen MPLS-VPN

Komponen pada konfigurasi jaringan MPLSVPN-L3 adalah dipelukan beberapa komponen seperti VRF, Routing Distinguisher, Route Target dan sebagaiannya.

### 2.3.1 VRF ( Virtual Routing Forwarding )

VRF merupakan sebuah routing and forwarding untuk sekumpulan site dengan kebutuhan konektivitas yang sama. VRF table digunakan untuk menyimpan rute dari local router CE (IPv4) maupun remote CE segera setelah update terjadi.Struktur data yang berkaitan dengan sebuah VRF adalah table IP routing, table CEF, routing protocol context, dan daftar beberap interface yang menggunakan VRF. Atribut MPLS VPN yang juga berkatian dengan VRF adalah RD dan RT (import maupun export). Routing context adalah routing protocol yang berjalan di sebuah VRF. Routing context diperkenalkan di Cisco IOS utnuk mendukung salinan routing protocol VPN yang terpisah dan terisolasi satu dengan lainnya. Routing context didukung oleh beberapa routing protocol yang mengenali VPN, yaitu EIGRP, OSPF, RIPv2, dan rute statis. Table VRF yang berisi tentang rute-rute yang tersedia untuk kumpulan site tertentu. Per VRF forwarding table dibangun atas per VRF routing table. Table ini digunakan untuk meneruskan paket yang diterima dari interface yang mendukung VRF[13].

### 2.3.2 Routing Distinguisher

Route distinguisher membuat alamat IPv4 terdiri dari 32 bit menjadi 96 bit unique address. Format route distinguisher adalah autonomous sistem number:arbitrary number atau IP address:arbitrary number. Sebagai contoh, alamat IP tujuan adalah 192.168.10.0 dengan nomor autonomous sistem 100 dan jalur VPN 1. Setelah ditambahkan route distinguisher, alamat IP tujuan akan dikenali oleh jaringan sebagai 100:1 atau 192.168.10.0:1. Paket IP yang telah ditambahkan route distinguisher akan menjadi paket VPN-IPv4. Alamat VPN-IPv4 ini yang akan digunakan oleh MP BGP untuk meneruskan paket melalui MPLS.

### 2.3.3 Route Target

RT merupakan atribut tambahan yang dimuat ke dalam rute BGP VPNv4 untuk menunjukkan keanggotaan VPN. RT terdiri dari dua jenis, yaitu:

a. Export RT : digunakan untuk mengidentifikasikan keanggotaan VPN dan ditambahkan ke dalam rute pelanggan ketika diubah ke dalam rute VPNv4. Export RT mengidentifikasikan sekumpulan VPN dimana site berasosiasi dengan virtual routing table yang semestinya.
b. Import RT : berkaitan dengan setiap virtual routing table dan memilih rute untuk dimasukkan ke dalam virtual routing table. Setiap VRF di sebuah router PE bisa memiliki sejumlah Import RT yang mengidentifikasikan sekumpulan VPN dari mana VRF menerima rute.Pendekatan VRF-ke-VRF adalah metode yang paling sederhana untuk memungkinkan penyedia layanan MPLS VPN untuk bertukar informasi routing VPN untuk situs CE dalam domain MPLS berbeda.

## 2.4 Routing Protocol

### 2.4.1 Jenis Routing Protocol

a. Routing Protocol OSPF

Open Shortest Path First (OSPF) adalah protokol perutean link-state yang dikembangkan sebagai pengganti untuk vektor jarak Routing Information Protocol (RIP). OSPF menentukanjalur terpendeknya berdasarkan denganmetricyang digunakan OSPF,diantaranya cost untuk round trip time,network throughput dari link yang digunakan,link availability dan reability. OSPF menggunakan IP datagram dengan port 89 sebagai transport protocol-nya untuk mengirimrouting data,dan paket OSPF bersifat multicast sehingga paket OSPF tersebar ke seluruh jaringan. OSPF termasuk routing protocol yang unggul dengan kemampuan cepatnya konvergensi,error detection dan error correction yang baik[14]

b. Routing Protocol EIGRP

EIGRP adalah routing protocol buatan cisco menggantikan IGRP.Termasuk dalam Distance Vector routing protocol Dengan menggunakan algoritma DUAL yang memberikan efisiensi dan membantu mencegah terjadinya penghitungan error saat menentukan jalur. Metric yang digunakan EIGRP diantarnya bandwidth ,load ,delay, MTU(maximum transmission unit),hopcount,

reliability. EIGRP menggunakan RTP sebagai transport protocol untuk routing data yang membawa update information dan neighbor information dengan port 88 dan mendukung multicast[14]

c. Routing Protocol BGP

Border Gateway Protocol (BGP) merupakan salah satu jenis routing protokol yang digunakan untuk koneksi antar Autonomous System (AS), dan salah satu jenis routing protokol yang banyak digunakan di ISP besar (Telkomsel) ataupun perbankan. BGP termasuk dalam kategori routing protokol jenis Exterior Gateway Protokol (EGP).Dengan adanya EGP, router dapat melakukan pertukaran rute dari dan ke luar jaringan lokal Auotonomous System (AS). BGP mempunyai skalabilitas yang tinggi karena dapat melayani pertukaran routing pada beberapa organisasi besar. Oleh karena itu BGP dikenal dengan routing protokol yang sangat rumit dan kompleks[14].

## 2.5 Aspek Keamanan Jaringan

a. Authentication, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.
b. Integrity, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.
c. Non-repudiation, merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
d. Authority, informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
e. Confidentiality, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
f. Privacy, lebih ke arah data-data yang bersifat pribadi.
g. Availability, aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
h. Access Control, aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password* ataupun dengan mekanisme lain[14]

## 2.6 Routing Protocol Authentication

Apa itu HASH? Hash atau algoritma hashing merupakan bentuk fungsi matematika yang melakukan pengcodean data dan mengubah ke bentuk tetap. Sebagai contoh kalimat "SSL Indonesia, Penyedia Sertifikat SSL Termurah" ketika kita menggunakan algoritma hashing kita akan mendapatkan code "070765bbb4". Hasil ini dikenal sebagai hasil hash atau nilai hash. Terkadang hashing disebut sebagai enkripsi satu arah. Algoritma hashing digunakan dalam berbagai hal biasanya digunakan sebagai sandi pada komputer, beberapa dioptimalkan untuk kecepatan dan keamanan. Salah satu sifat algoritma hashing adalah determinisme.Kali ini yang akan kita bahas adalah algoritma SHA. SHA (Secure Hashing Algorithm) ini berfungsi sebagai keamanan kriptografi. Jika kita kaitkan dengan sertifikat SSL ini akan berkaitan dengan Rantai penerbitan sertifikat SSL. Sertifikat SSL memfasilitasi koneksi internet menggunakan enkripsi asimetris, dimana public key dimiliki oleh penyedia otoritas sertifikat SSL dan private key dimiliki oleh klien. Setiap sertifikat SSL memiliki public key yang dapat digunakan oleh klien untuk mengenkripsi data, dan pemilik sertifikat SSL memiliki private key pada server dan digunakan untuk mendekripsi data. Secara sederhana tujuan utama enkripsi asimetris adalah pertukaran kunci untuk meningkatkan keamanan penyebaran data[5].

Konsekuensi yang didapat karena adanya serangan ini adalah:

1.Mengarahkan *Traffic* peroutingan yang mengakibatkan *routing loops*

2. Mengarahkan *Traffic* peroutingan sehingga dapat dimonitor pada *link* yang tidak aman.

3.Mengarahkan *Traffic* untuk membuang informasi peroutingan

## 2.7 VOIP

VOIP(Voice Over Internet Protocol) merupakan teknologi berkomunikasi jarak jauh melalui media internet. Dengan menggunakan internet , maka data suara akan diubah menjadi kode digital dan kemudian diteruskan hingga menjadi paket-paket data yang ada di dalam jaringan. Jadi, data tersebut tidak akan melalui analog seperti cara kerja telepon pada umumnya. Intinya, VoIP merupakan teknologi suara yang dikirim dengan memanfaatkan media berupa Internet Protocol atau IP.

## 2.8 Jenis – Jenis Serangan

a. SPOOFING

Spoofing adalah suatu teknik serangan yang tidak sah dan tidak legal untuk mengakses sebuah computer ataupun sebuah informasi. dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya. Hal ini biasanya dilakukan oleh seorang hacker/ cracker.

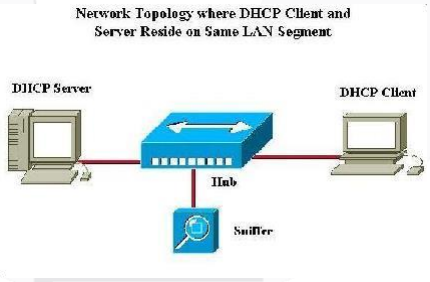
Macam – macam Spoofing adalah sebagai berikut :

1. IP Spoofing : adalah serangan dengan memalsukan IP Address yang sebenarnya
2. DNS Spoofing : adalah serangan yang terjadi pada DNS server sehingga DNS dan IP address akan di alihkan kepada penyerang
3. IP Address Spoofing : adalah teknik serangan yang digunakan untuk membuat paket IP dengan source IP palsu

b. SNIFFING

Sniffing merupakan teknik serangan yang terjadi pada paket data atau penyadapan data dengan cara memonitoring dan menganalisis setiap paket data yang di transmisikan dari server ke client.

Sniffer merupakan suatu tools aplikasi yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC(*Request for Comments*) atau spesifikasi yang lain.




Gambar 2.4 Gambaran sniffer

Sumber : (https://alfaridzi.wordpress.com/)

c. BRUTEFORCE

Suatu teknik serangan untuk bisa meretas sistem dengan cara mencoba kata sandi yang tepat dan sampai bisa berhasil masuk ke dalam sistem tersebut. waktu yang dibutuhkan untuk bisa menemukan kata sandi yang tepat juga tidak bisa ditentukan. Jika *users* atau target serangan menggunakan kata sandi yang cukup panjang dan kompleks, maka perlu beberapa hari, bulan, atau bahkan bertahun-tahun untuk memecahkan kata sandi. Pada penelitian ini akan menggunakan LOKI. *Attack tool* ini juga dapat melakukan cracking dengan cara *bruteforce* dari paket protocol yang tertangkap

## 2.9 QOS

QoS ( Quality Of Service ) atau bisa disebut juga dengan kualitas layanan yang didalamnya terdapat beberapa parameter yang digunakan untuk mengukur seberapa baik suatu jaringan dengan menetapkan prioritas untuk tipe data tertentu pada jaringan. Organisasi menggunakan QoS untuk memenuhi persyaratan lalu lintas dari aplikasi sensitif, seperti suara dan video real-time, dan untuk mencegah penurunan kualitas yang disebabkan oleh packet loss, penundaan dan jitter.

Beberapa parameter QoS dan standarisasi terbaik menurut TIPHON adalah sebagai berikut :

a. Throughput

Throughput yaitu kecepatan (rate) transferdata efektif, yang diukur dalam bps (bit per second). Throughput adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

$$\textbf{Throughput :} \quad \frac{Packed\ received\ (kb)}{Time\ transmitted\ (s)}$$

| Kategori *Throughput* | *Throughput* | Indeks |
|---|---|---|
| *Bad* | 0 – 338 kbps | 0 |
| *Poor* | 338 – 700 kbps | 1 |
| *Fair* | 700 – 1200 kbps | 2 |
| *Good* | 1200 kbps – 2,1 Mbps | 3 |
| *Excelent* | >2,1 Mbps | 4 |

Gambar 2.5 Standarisasi Troughput TIPHON

b. Packet Loss

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang dapat terjadi karena *collision* dan *congestion* pada jaringan

$$\textbf{Packet loss} = \frac{(Packet\ transmitted - Packet\ received)}{Packet\ transmitted} \ X\ 100\%$$

| Kategori *Packet Loss* | *Packet Loss* | Indeks |
|---|---|---|
| *Poor* | >25% | 1 |
| *Medium* | 12 – 24% | 2 |
| *Good* | 3 – 14% | 3 |
| *Perfect* | 0 – 2% | 4 |

Gambar 2.6 Standarisasi Packet Loss TIPHON

c. Jitter atau Variasi Kedatangan Paket

Jitter diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan jitter Jitter lazimnya disebut variasi delay, berhubungan erat dengan latency, yang menunjukkan banyaknya variasi delay pada transmisi data di jaringan.

| Kategori *Jitter* | *Jitter* | Indeks |
|---|---|---|
| *Poor* | 125 – 225 ms | 1 |
| *Medium* | 75 – 125 ms | 2 |
| *Good* | 0 – 75 ms | 3 |
| *Perfect* | 0 ms | 4 |

Gambar 2.7 Standarisasi JITTER TIPHON

d. Delay (Latency)

Delay (Latency) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama.

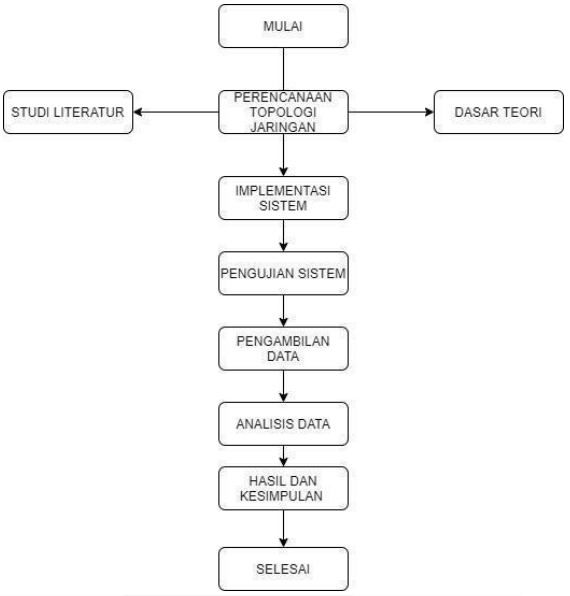
| Kategori Latency | Latency | Indeks |
|---|---|---|
| *Poor* | > 450 s | 1 |
| *Medium* | 300 – 450 s | 2 |
| *Good* | 150 – 300 s | 3 |
| *Perfect* | < 150 s | 4 |

Gambar 2.8 Standarisasi Troughput TIPHON

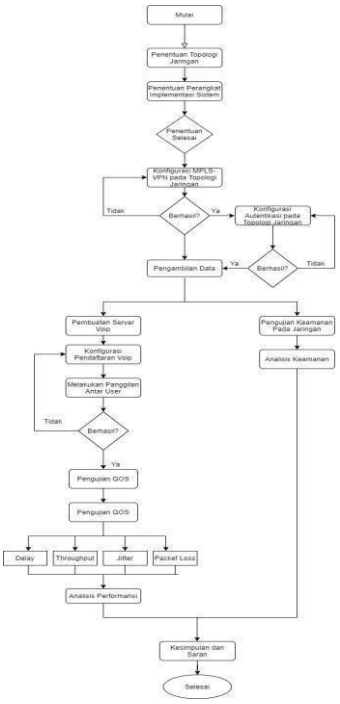
## 3. PENELITIAN DAN PERANCANGAN

### 3.1 Blok Diagram Perencanaan

Pada bab ini akan di bahas mengenai proses perancangan dan penelitian serta proses implementasi sistem yang akan dibangun pada tugas akhir ini, untuk membangun suatu jaringan backbone yang sederhana dibutuhkan skenario yang terstruktur dan baik. Dengan tujuan proses pengimplementasian akhir yang sesuai dengan penulis yaitu mampu membangun suatu jaringan yang di rencanakan dan menganalisis performansi dan keamanan jaringan yang telah dibangun




### 3.2 Tahap Proses Perancangan



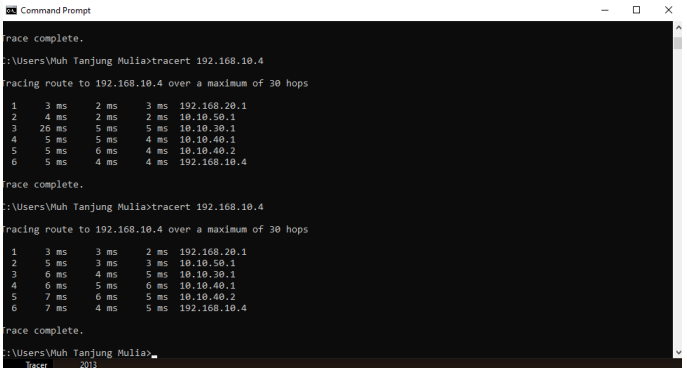

### 3.3 Skenario Pengujian

Adapun berbagai macam skenario yang akan dilakukan adalah sebagai berikut:

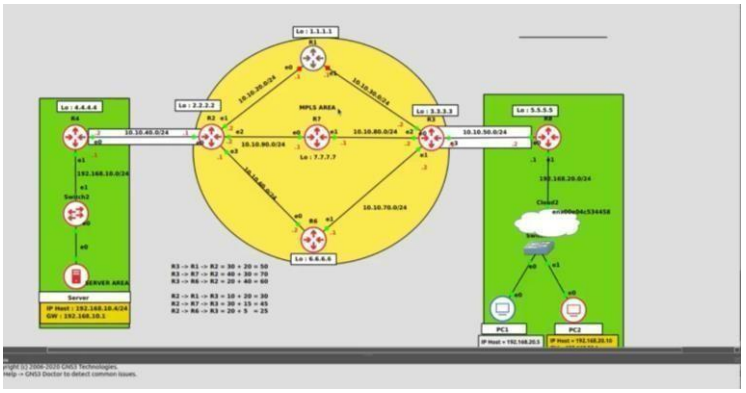
a. Pemutusan jalur utama ketika komunikasi antara server ke pc1 sedang berkomunikasi
b. Melakukan serangan spoofing dengan cracking di sisi CE-P menggunakan autentikasialgoritma SHA
c. Melakukan serangan spoofing dengan menggunakan injection ipv4 di sisi PE-P tanpamenggunakan autentikasi SHA
d. Melakukan pengujian sniffing komunikasi voip dengan autentikasi SHA
e. Melakukan uji coba konvergen router apabila core jaringan di matikan pada saatkomunikasi berlangsung dibutuhkan up time berapa lama
f. Melakukan komunikasi voip pada jalur utama dan back up dengan autentikasi
g. Melakukan komunikasi voip pada jalur utama dan back up tanpa autentikasi

## 4. HASIL PENELITIAN/HASIL PENGUKURAN, ANALISIS, DAN PEMBAHASAN

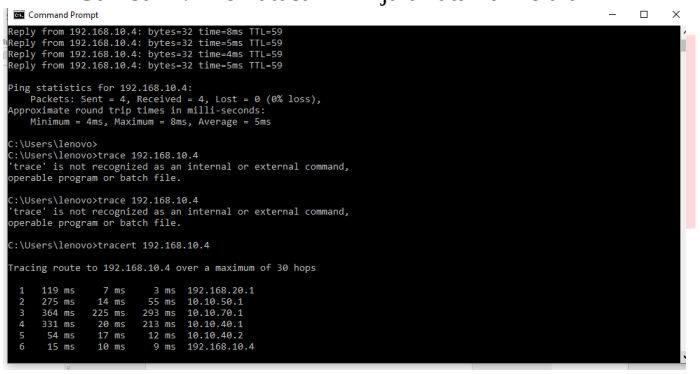
### 4.1 Pengujian Jalur Utama




Setelah melakukan konfigurasi pada semua router dan melakukan percobaan untuk ping dari server menuju client 1. Maka dihasilkan jalur terbaik yang di lalui adalah melalui atas yaitu server 1 menuju pc 1 kemudian lanjut menuju R2 yaitu Provider Edge dan pada di router ini lah ditentukan dimana jalur terbaik yang akan dilewati dengan berdasarkan beberapa cost yang terdapat pada peroutingan OSPF. Lalu selanjutnya melewati router Provider atas di R1 lalu menuju Provider Edge 3 dan diteruskzan ke Customer Edge di R5 dan jika berhasil akan terjadi request dan replay pada proses tersebut. Alasannya karna berdasarkan cost yang sudah ditentukan, jika cost paling rendah maka yang di pilih untuk menjadi jalur utama



Gambar 4.2 Pemutusan link jalur utama melalui R1

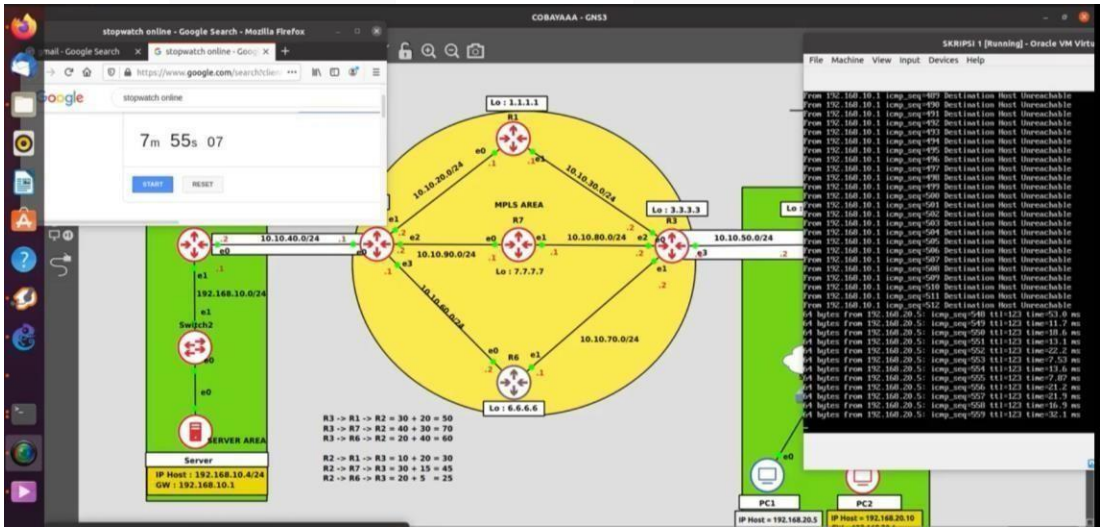



4.3 Trace Jalur Backup

Dan selanjutnya akan dilakukan pemutusan jalur utama, pada area MPLS yaitu router 1 pada jalur utama yang melalui jalur atas. Pada skenario kedua dilakukan pemutusan jalur utama disaat komunikasi dari server ke client sedang berlangsung maka jalur backup yang menggantikan yaitu melalui jalur bawah yang memiliki metric cost terendah kedua. sehingga dapat di verifikasi bahwa jalur backup ini secara otomatis akan menggantikan posisi jalur utama sehingga komunikasi dari server menuju client akan tetap berjalan

## 4.2 Pengujian Uptime Router

5.

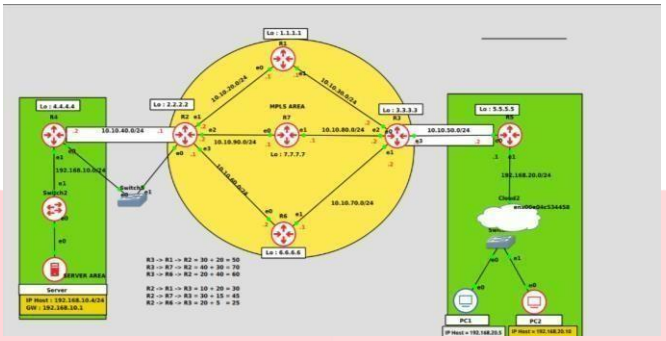



Gambar 4.4 Pengujian Uptime Router

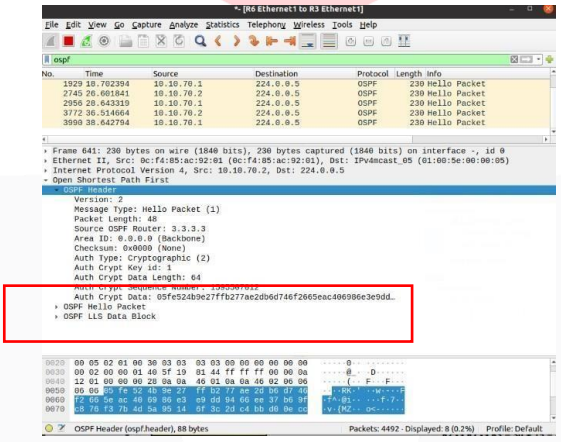
Pada saat pengujian uptime router ,ketika area mpls dimatikan maka informasi ping dari server menuju pc akan putus.Pada saat melakukan pengujian menggunakan stopwatch untuk menunggu konvergensi jaringan, maka di dapatkan waktu 7menit 55detik untuk bisa konvergensi kembali. Dikarenakan spefikasi laptop yang digunakan untuk jaringan utama MPLS dan Server yang dibuat virtual memiliki spesifikasi processor AMD Ryzen 3 dengan ram 8gb.

### 4.3 Melakukan spoofing pada sisi CE-PE menggunakan Cracking Tools LOKI

Untuk penyerangan Man In The Middle Attack pada topologi ini telah ter autentikasi menggunakan hash algotitma SHA yang digunakan untuk enkripsi. Lalu akan dilakukan penyerangan pada router sisi PE dan CE, dikarenakan area tersebut yang menjadi jalur untuk keluar masuknya jalur paket yang di lewati atau Engress dan Ingress Label Router

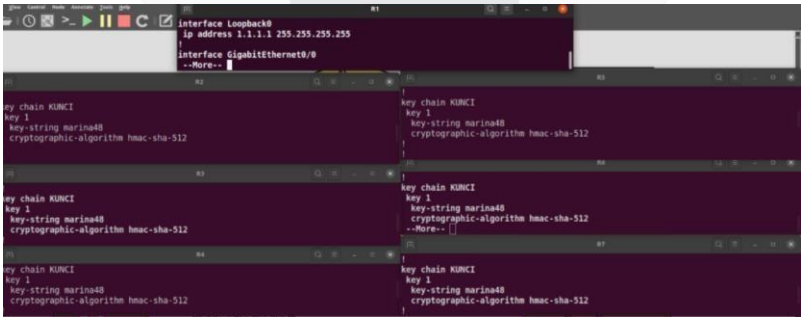



Gambar 4.5 Skenario Spoofing MPLSVPN pada CE-PE




Gambar 4.6 Informasi routing ospf dengan autentikasi yang sudah di aktifkan

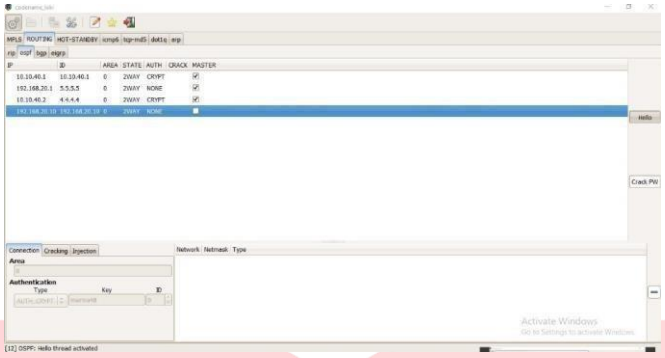
Dengan menggunakan routing protocol autentikasi yang sudah di konfigurasi di setiap interface router di core jaringan mpls vpn maka penyerang yang menangkap paket informasi data routing tersebut tidak akan langsung memodifikasi paket yang datang dengan mudah, dikarenakan paket yang datang harus terlebih dahulu di cracking sehingga dapat diketahui key yang digunakan untuk melakukan enkripsi tersebut.




Gambar 4.7 Konfigurasi autentikasi jaringan

Untuk penelitian ini,digunakan keychain nya yaitu ‘KUNCI’ dan key string nya yaitu marina48, dan algoritma yang dgunakan untuk enkripsi nya yaitu di tingkat paling tinggi yaitu di HMAC SHA 512.

Untuk membuktikan ke akuratan hash yang digunakan pada penelitian kali ini sudah cukup bagus atau tidak terhadap serangan bruteforce yang diberikan. Pada penelitian ini digunakan tools LOKI untuk melakukan bruteforce pada router di sisi CE dan PE menggunakan wordlist yang sudah di atur di dalan tools nya.

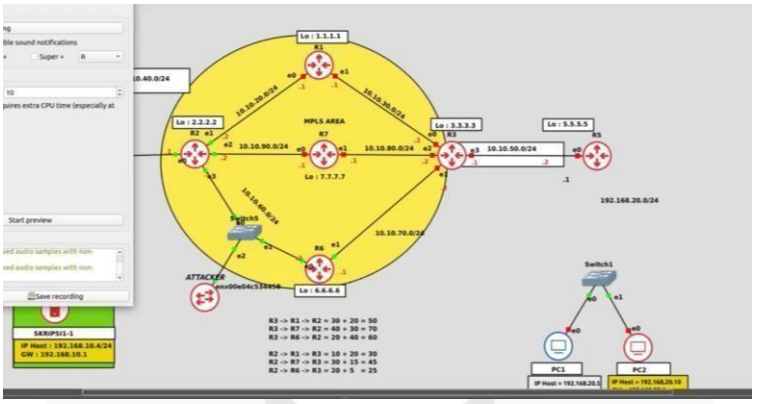


Gambar 4.8 Tampilan LOKI saat bruteforce dilakukan

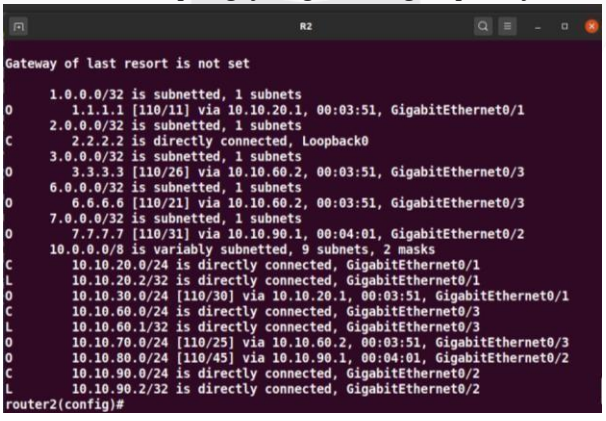
Pada tampilan tersebut muncul ip loopback 5.5.5.5 yang merupakan ip loopback pada router 5 atau router Customer Edge dan ip loopback 4.4.4.4 yang merupakan router 4 atau router Provider.

### 4.4 Melakukan spoofing pada sisi PE-P menggunakan injection ipv4

Pada sub bab ini, penulis akan menguji jaringan mpls tanpa autentikasi dengan melakukan serangan ipv4 injection pada sisi router Provider dan Provider Edge dengan memasangkan switch di tengah antara jalur R6 menuju R2.

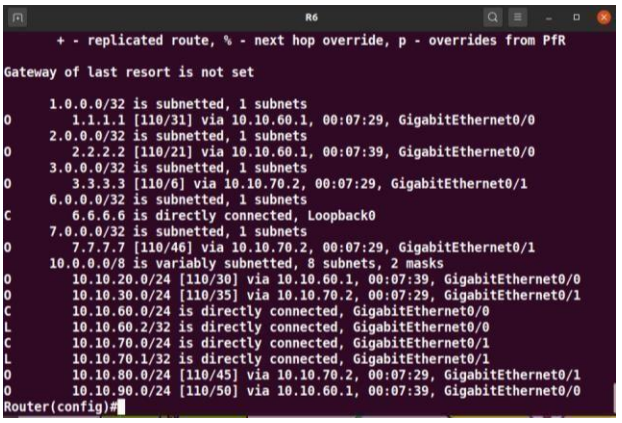



Gambar 4.9 Topologi jaringan serangan ipv4 injection



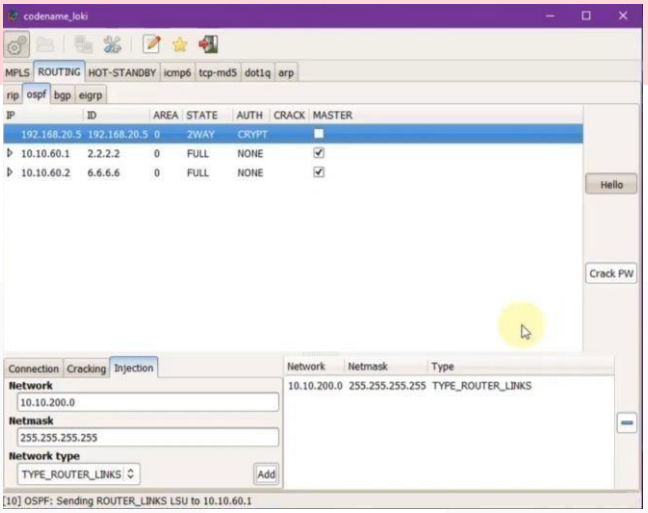
```
R2

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/11] via 10.10.20.1, 00:03:51, GigabitEthernet0/1
      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/26] via 10.10.60.2, 00:03:51, GigabitEthernet0/3
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/21] via 10.10.60.2, 00:03:51, GigabitEthernet0/3
      7.0.0.0/32 is subnetted, 1 subnets
O        7.7.7.7 [110/31] via 10.10.90.1, 00:04:01, GigabitEthernet0/2
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        10.10.20.0/24 is directly connected, GigabitEthernet0/1
L        10.10.20.2/32 is directly connected, GigabitEthernet0/1
O        10.10.30.0/24 [110/30] via 10.10.20.1, 00:03:51, GigabitEthernet0/1
C        10.10.60.0/24 is directly connected, GigabitEthernet0/3
L        10.10.60.1/32 is directly connected, GigabitEthernet0/3
O        10.10.70.0/24 [110/25] via 10.10.60.2, 00:03:51, GigabitEthernet0/3
O        10.10.80.0/24 [110/45] via 10.10.90.1, 00:04:01, GigabitEthernet0/2
C        10.10.90.0/24 is directly connected, GigabitEthernet0/2
L        10.10.90.2/32 is directly connected, GigabitEthernet0/2
router2(config)#
```

Gambar 4.10 Tabel routing sisi PE sebelum dilakukan ipv4 injection



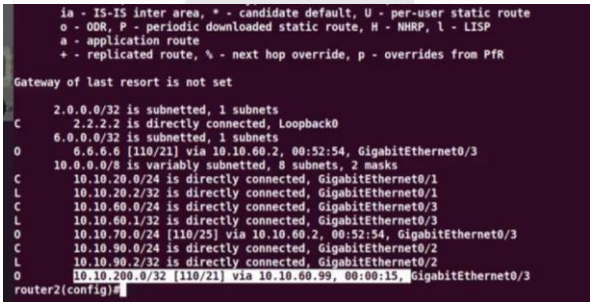

Gambar 4.11 Tabel routing sisi CE sebelum dilakukan ipv4 injection

Selanjutnya untuk melakukan ipv4 injection digunakan juga tools LOKI untuk memasukan ip injeksi ke dalam router yang sudah ditentukan.

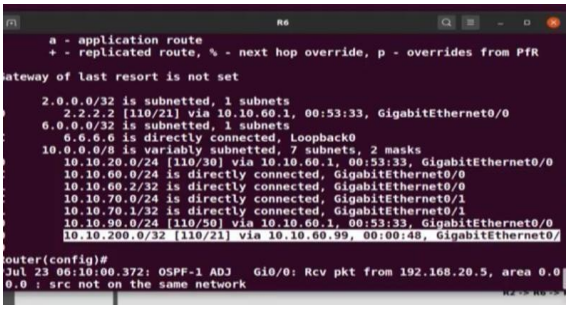



Gambar 4.11 Tampilan Injection ipv4 di sisi P-PE

Untuk melakukan injeksi, terlebih dahulu untuk mengirim ‘hello message’pada router yang akan di injeksi. Setelah melakukan hello message, maka status nya akan menjadi ‘FULL’ yang artinya sudah dapat di berikan IP injeksi terhadap router yang ingin di serang. Untuk network dan netmask nya bebas ditentukan. Lalu setelah mengirimkan ip injeksi , lihat lagi tabel routing pada sisi PE dan P yang sudah dilakukan serangan ipv4 injection



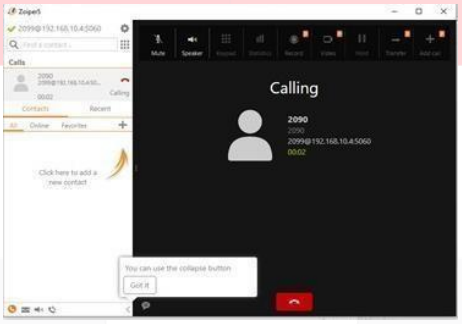

Gambar 4.12 Tabel routing sisi PE setelah ipv4 injection tanpa autentikasi



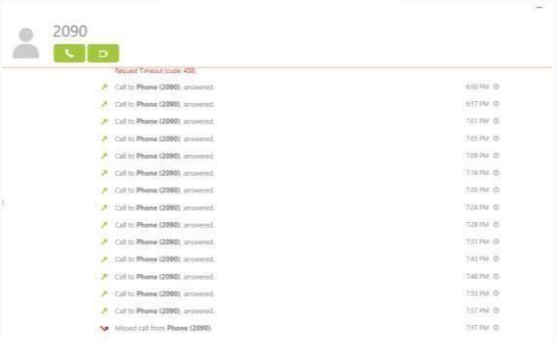

Gambar 4.13 Tabel routing sisi P setelah ipv4 injection tanpa autentikasi

Pada tabel routing tersebut terjadi penambahan jalur routing pada routing tabel di router R2 dan R6 , yaitu dengan ip address 10.10.200.0/32 via 10.10.60.99 yang dimana ip tersebut merupakan ip host attacker. Dan hal ini menyebabkan router membuang paket dengan tujuan ip networkr 10.10.200.0, dikarenakan hal ini disebabkan sebenarnya jaringan 10.10.200.0 tidak ada dan akan otomatis terbuang, untuk melakukan ipv4 injection tersebut sudah terligat hasilnya kurang dari 2 menit untuk melakukan injection ipv4.

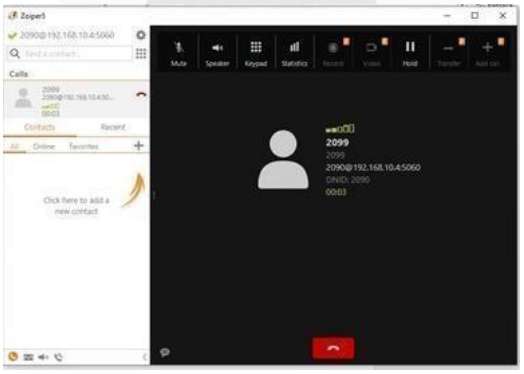
## 4.5 Melakukan komunikasi VOIP



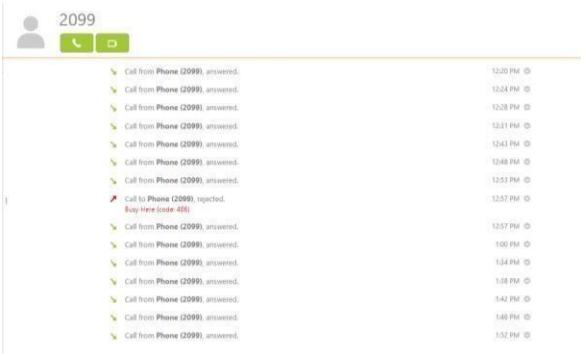

Gambar 4.14 Tampilan Komunikasi Voip Client 1




Gambar 4.15 Log History Call Voip Client 1



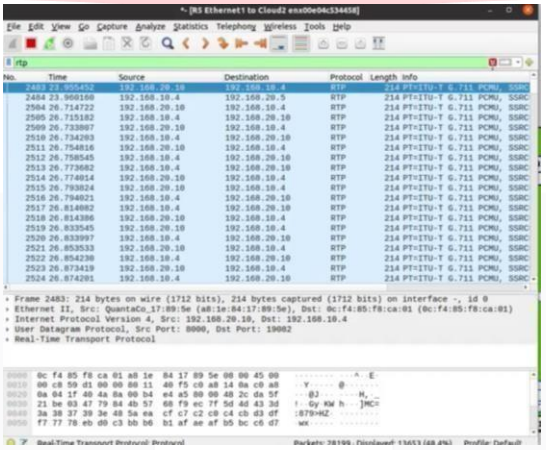

Gambar 4.16 Tampilan Komunikasi Voip Client 2




Gambar 4.17 Log History Call Voip client 2

Pengujian layanan komunikasi voip pada penelitian ini adalah dengan menggunakan jaringan MPLS menggunakan autentikasi dan tanpa autentikasi dengan di masing-masing didalam jaringan tersebut akan dilakukan pengujian di jalur utama dan jalur backup untuk menguji kinerja jaringan pada saat komunikasi voip tersebut berjalan.

### 4.6 Sniffing Paket Pada Sisi Client pada saat komunikasi berlangsung



Gambar 4.18 Sniffing Komunikasi Voip

Pada komunikasi antara 2 client dan server tersebut menggunakan protocol UDP ( User Datagram Protocol ). Kemudai dalam komunikasi VOIP juga terdapat dua protocol yang difungsikan untuk membangun infrastrukturnya, terdapat protokol SIP ( Session Initation Protocol ) berfungsi untuk memodifikasi dan mengakhiri, suatu sesi multimedia yang melibatkan satu user atau lebih. Atau seperti sebuah wadah pada saat akan melakukan komunikasi. Kemudian memerlukan protokol lain untuk memberikan layanan transfer data secara realtime,dengan menggunakan protocol RTP ( Realtime Transport Protocol)

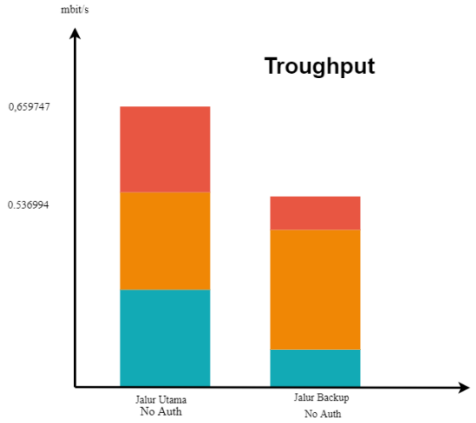
### 4.7 Hasil Pengukuran QoS komunikasi VOIP pada jalur utama dan back up tanpa autentikasi.

Pada pengujian komunikasi voip ( voice over internet protocol ) dilakukan dengan skenario jalur utama dan jalur back up. Untuk komunikasi berlangsung selama 2 menit di tiap percobaan lalu akan di hitung dan di analisa hasil pengukuran nya dengan menggunakan parameter dibawah ini :

a. Pengukuran Troughput

Tabel 4.1 Pengukuran Troughput No Authentication

| NO | Jalur Utama No Auth | Jalur Backup No Auth |
|---|---|---|
| 1 | 0.250137 | 0.700259 |
| 2 | 0.713958 | 0.639603 |
| 3 | 0.528685 | 0.643223 |
| 4 | 0.451996 | 0.656826 |
| 5 | 0.740198 | 0.658826 |
| rata- rata | 0.536994 mbit/s | 0.536994 mbit/s |

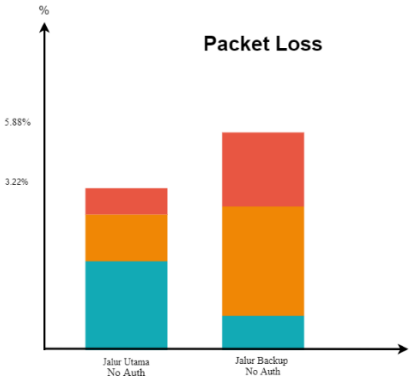



Berdasarkan pengujian yang sudah di lakukan , didapatkan hasil untuk nilai troughout di jalur utama menjadi 0.536994 mbit/s dan pada jalur backup didapatkan 0.536994 mbit/s dan itu membuktikan bahwa sangat bagus menurut standarisasi TIPHON.

b.Packet Loss

Tabel 4.2 Pengukuran Packet Loss No Authentication

| NO | Jalur Utama No Auth | Jalur Backup No Auth |
|---|---|---|
| 1 | 2.734% | 4.140% |
| 2 | 4.116% | 4.965% |
| 3 | 3.550% | 7.960% |
| 4 | 2.644% | 7.158% |
| 5 | 3.054% | 4.918% |
| rata- rata | 3.22% | 5.82% |

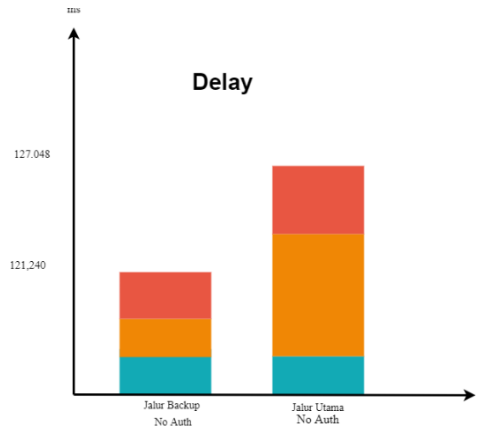



Setelah dilakukan pengujian komunikasi terdapat loss sebesar 3.22% pada jalur utama dan 5.82% pada jalur backup. Itu berarti bagus menurut kategori TIPHON

a. Delay

Tabel 4.3 Pengukuran Delay No Authentication

| NO | Jalur Utama No Auth | Jalur Backup No Auth |
|---|---|---|
| 1 | 120.458 | 121.767 |
| 2 | 140.926 | 121.809 |
| 3 | 123.934 | 118.697 |
| 4 | 128.546 | 123.565 |
| 5 | 121.376 | 120.362 |
| rata- rata | 127.048 ms | 121,240 ms |

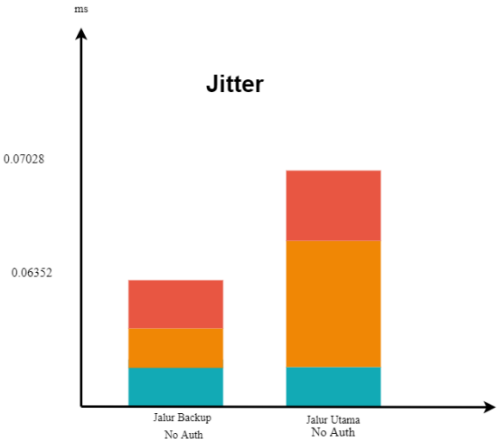



Berdasarkan standarisasi TIPHON delay yang didapatkan pada jalur utama sebesar termasuk 127.048 ms.Dan untuk jalur back up sebesar 121,240 ms dan termasuk ke dalam kategori bagus

d. Jitter

Tabel 4.4 Pengukuran Jitter No Authentication

| NO | Jalur Utama No Auth | Jalur Backup No Auth |
|---|---|---|
| 1 | 0.04416 | 0.08165 |
| 2 | 0.03678 | 0.02359 |
| 3 | 0.05211 | 0.09451 |
| 4 | 0.12398 | 0.06114 |
| 5 | 0.09441 | 0.05677 |
| rata- rata | 0.07028 ms | 0.06352 ms |



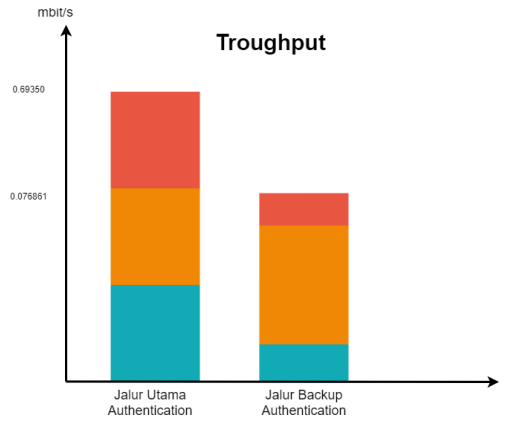

Setelah pengujian yang dilakukan didapatkan hasil jitter pada jalur utama sebesar 0.07028 ms dan pada jalur back sebesar 0.06352 ms yang berarti buruk

**4.11 Hasil Pengukuran QoS komunikasi VOIP pada jalur utama dan back up autentikasi**

a. Pengukuran Troughput

Tabel 4.5 Pengukuran Troughput Authentication

| NO | Jalur Utama Auth | Jalur Backup Auth |
|---|---|---|
| 1 | 0.853096 | 0.717632 |
| 2 | 0.628057 | 0.731962 |
| 3 | 0.670316 | 0.943536 |
| 4 | 0.612732 | 0.705464 |
| 5 | 0.703311 | 0.744462 |
| rata- rata | 0.69350 mbit/s | 0.076861mbit/s |

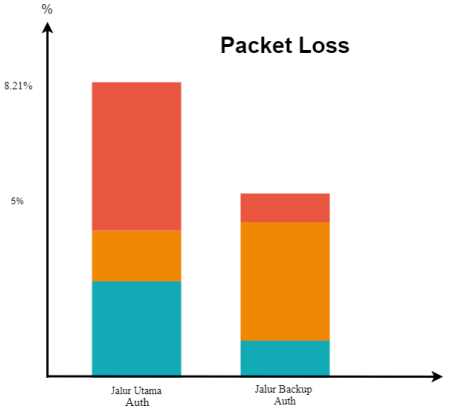



Setelah dilakukan pengujian, hasil troughput di jalur utama yaitu sebesar 0.69350 mbit/s dan jalur backup sebesar 0.076861mbit/s yang menandakan bagus menurut standarisasi TIPHON

b. Packet loss

Tabel 4.6 Pengukuran Packet Loss Authentication

| NO | Jalur Utama Auth | Jalur Backup Auth |
|---|---|---|
| 1 | 8.491% | 5.326% |
| 2 | 8.501% | 4.552% |
| 3 | 7.610% | 4.920% |
| 4 | 8.201% | 5.550% |
| 5 | 8.288% | 4.651% |
| rata- rata | 8.22% | 5% |

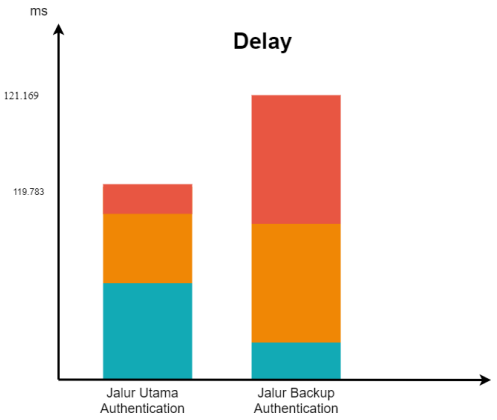



Berdasarkan pengukuran yang telah dilakukan besar packet loss yang di hasilkan pada jalur utama 8.22% dan pada jalur backup sebesar 5% yang berarti bagus.

c. Delay

d. Tabel 4.7 Pengukuran Delay Authentication

| NO | Jalur Utama Auth | Jalur Backup Auth |
|---|---|---|
| 1 | 122.578 | 121.217 |
| 2 | 120.901 | 121.155 |
| 3 | 111.329 | 122.172 |
| 4 | 122.665 | 121.775 |
| 5 | 121.446 | 119.520 |
| rata- rata | 119,783 ms | 121.169 ms |

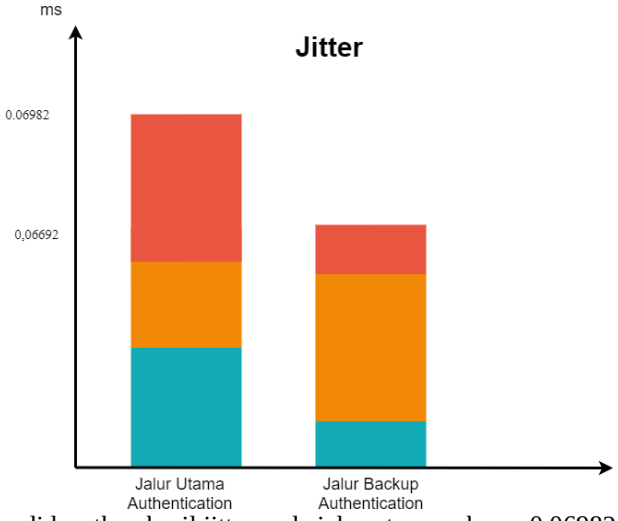



Pada parameter qos delay, didapatkan pada jalur utama yaitu 119,783 ms dan untuk jalur backup sebesar 121.169 ms yang berarti bagus karna lebih dari 150-200 ms menurut standarisasi TIPHON

e. Jitter

Tabel 4.8 Pengukuran Jitter Authentication

| NO | Jalur Utama Auth | Jalur Backup Auth |
|---|---|---|
| 1 | 0.014545 | 0.081633 |
| 2 | 0.121051 | 0.040533 |
| 3 | 0.020456 | 0.094518 |
| 4 | 0.079786 | 0.061144 |
| 5 | 0.113272 | 0.056775 |
| rata- rata | 0.06982 ms | 0,06692 ms |




Setelah pengujian yang dilakukan didapatkan hasil jitter pada jalur utama sebesar 0.06982 ms dan pada jalur back sebesar 0,06692 ms yang berarti bagus

## 5. KESIMPULAN

### 5.1 Kesimpulan

1. Berhasil melakukan perancangan jaringan mpls-vpn l3 menggunakan 3 jalur dengan menggunakan autentikasi pada routing protocol OSPF yang digunakan untuk pengujian.
2. Berhasil melakukan injection ipv4 pada jaringan mpls-vpn tanpa menggunakan autentikasi dengan menggunakan tools LOKI .
3. Algoritma SHA (Secure Hash Algorithm) tidak dapat berhasil meng-cracking key-string yang sudah di konfigurasi karena memiliki tingkat keamanan yang bagus.
4. Berhasil melakukan komunikasi layanan VOIP dengan menggunakan virtual server pada jaringan MPLS-VPN L3
5. Implementasi routing protocol autentikasi tidak memebebani kinerja jaringan di buktikan setelah di simpulkan hasil pengukuran pada parameter Q.o.S VOP.

### 5.2 Saran

1. Melakukan filtering jaringan untuk melindungi integrity dari jaringan
2. Lebih mencari tools yang banyak untuk melakukan simulasi serangan yang mengarah pada integrity
3. Perlu dicoba fungsi hash algoritma lain seperti blowfish untuk mencoba attack bagian integrity

## DAFTAR PUSTAKA

[1] Agustino, M. Feryanto and D. Malik, Sistem Evaluasi Control of Service pada Jaringan Multiprotokol Label Switching, Jakarta: Universitas Bina Nusantara, 2007.

[2] Andi Taufik Saputra. 2010. Implementasi dan Analisa Unjuk Kerja Secure VOIP Pada Jaringan VPN Berbasis MPLS Dengan Menggunakan Tunneling IPSEC [SKRIPSI]. Depok (ID): Universitas Indonesia.

[2] Anonim, "IP Routing EIGRP Configuration Guide, Cisco IOS Release 15SY," Chapter: EIGRP/SAF HMAC-SHA-256 Authentication, [Online]. Available: https://www.cisco.com. [Accessed 3 July 2020].

[3] Anonim, "IP Routing: EIGRP Configuration Guide, Cisco IOS Release 15M&T," EIGRP/SAF HMAC-SHA-256 Authentication, [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15- mt/ire-15-mt-book/ire-sha-256.pdf. [Accessed 3 July 2020].

[4] Anonim, "Media Neliti," Metodologi Pengujian Keamanan Jaringan VoIP, [Online]. Available: https://media.neliti.com/media/publications/234344-metodologi- pengujian-keamanan-jaringan-v-8f71a007.pdf. [Accessed 3 July 2020].

[5] Anonim, "Network Lesson," EIGRP SHA Authentication, [Online]. Available: https://networklessons.com/cisco/ccie-routing-switching-written/eigrp-sha- authentication. [Accessed 3 July 2020].

[6] Anonim. [Online]. Available: https://c0decafe.de/. [Accessed 3 July 2020].

[7] B. Euginia and T. Ghozali, "Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router MIKROTIK," *T E S L A*, vol. 20, no. 2, pp. 109-117, 2018.

[8] C. M. Shabirin, Analisis Implementasi Routing Protocol Authentication Pada Jaringan MPLSVPN-L3VPN, Bandung: Universitas Telkom, 2014.

[9] D. Wijanarko and . B. M. Susanto "Performa Protokol Routing VOIP Pada Jaringan MPLS VPN dengan Tunelling Open VPN" in Seminar Nasional Hasil Penelitian 2017, Jember, 2017

[10] I. Arif, "Santekno," BGP (Border Gateway Protocol), 28 December 2019. [Online]. Available: https://santekno.com. [Accessed 3 July 2020].

[11] O. Sulaiman and M. Ihwani, "Analisis Perbandingan Penggunaan Metric Cost dan Bandwidth Pada Routing Protocol OSPF," *Sinkron: Jurnal dan Penelitian Teknik Informatika,* vol. 5, no. 1, pp. 1-7, 2017.

[12] R. Wulandari, "Analisis QOS (Quality Of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon –Lipi)," *Jurnal Teknik Informatika dan Sistem Informasi* , vol. 2, no. 2, pp. 162-172, 2016.

[13] S. Chairunnisa, Analisis Performansi Qos Inter Autonomous System Mpls-Vpn Back- To-Back VRF Pada Layanan IMS, Bandung: Universitas Telkom, 2018.

[14] S. Merchant, "Networkology," Routing Protocol Authentication – RIP, OSPF, EIGRP and BGP (CCIE Notes), 1 January 2014. [Online]. Available: https://networkology.net/2014/01/01/routing-protocol-authentication-rip-ospf-eigrp- and-bgp-ccie-notes/. [Accessed 3 July 2020].

[15] S. Syamsu, "Routing," in *Modul Jaringan Komputer*, Makasar, STMIK AKBA, 2015, pp. 1-23.

[16] S. Wilkins, "Cisco Press," Routing Protocol Authentication Concepts and Configuration, 13 July 2012. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=1728836. [Accessed 3 July 2020].

[17] M. F. Adriant and . I. Mardianto , "Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan," in Seminar Nasional Cendekiawan 2015, Jakarta,2015.