ANALISIS PERBANDINGAN KINERJA QOS DENGAN METODE PPTP,L2TP, SSTP DAN IPSEC PADA JARINGAN VPN DENGAN MENGGUNAKAN MIKROTIK PADA KANTOR BADAN PERWAKILAN DAN KEPENDUDUKAN KELUARGA BERENCANA NASIONAL (BKKBN) PEKANBARU

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Teknik Pada Fakultas Teknik Universitas Islam Riau Pekanbaru

DISUSUN OLEH :

AGUS KARTIKO
163510263

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2022

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, serta kita hadiahkan shalawat kepada junjungan kita Nabi Muhammad SAW sehingga penulis dapat menyelesaikan laporan penelitian ini untuk menyelesaikan program studi strata 1 (S1) pada jurusan Teknik Informatika UNIVERSITAS ISLAM RIAU dengan judul "**Analisis Perbandingan Kinerja Quality Of Service (QOS) Dengan Menggunakan Pptp, L2tp, Sstp Dan Ipsec Pada Jaringan VPN Menggunakan Mikrotik Pada Kantor BKKBN Pekanbaru**".

Penulis menyadari bahwa dalam penelitian ini masih terdapat kesalahan dan kekurangan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran dari para pembaca sehingga pada penelitian yang akan datang akan lebih baik dari penelitian ini. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Prof, Dr. H. Syafrinaldi, S.H.,M.C.L selaku Rektor Universitas Islam Riau.
2. Bapak Dr. Eng Muslim, ST, MT selaku Dekan Fakultas Teknik Universitas Islam Riau
3. Ibu Dr. Mursyidah, M.Sc selaku Wakil Dekan I Fakultas Teknik
4. Bapak Dr. Anas Puri, ST., MT selaku Wakil Dekan II Fakultas Teknik

5. Bapak Akmar Efendi, S.Kom. M.Kom selaku Wakil Dekan III Fakultas Teknik sekaligus Pembimbing Akademik penulis yang selalu memberikan motivasi, serta arahan dan dukungan kepada penulis selama proses perkuliahan
6. Bapak Dr. Apri Siswanto, S.Kom., M.Kom selaku Ketua Program Studi Teknik Informatika Universitas Islam Riau
7. Bapak Yudhi Arta, ST., M.Kom selaku Pembimbing Skripsi yang selalu memberikan dukungan, motivasi dan memberikan arahan serta saran agar penulis dapat menyelesaikan skripsi dengan baik dan memberikan kelancaran bagi penulis untuk menyelesaikan skripsi ini.
8. Ibu Ana Yulianti, ST., M.Kom selaku Sekretaris Ketua Program Studi
9. Segenap Dosen Program Studi Teknik Informatika Universitas Islam Riau yang telah membrikan ilmu yang begitu berharga, membimbing, mendidik, dan membrikan kesempatan kepada penulis untuk dapat belajar
10. Segenap pengurus Tata Usaha Fakultas Teknik Universitas Islam Riau beserta Staff yang telah banyak membantu dalam berbagai urusan administrasi selama proses penyelesaian skripsi
11. Teruntuk yang teristimewah Orang Tua yang selalu memberikan dukungan, motivasi yang luar biasa, dan kasih sayang yang tak henti-hentinya diberikan kepada penulis untuk dapat menyelesaikan skripsi ini dengan baik. Terimakasih untuk do'a yang selalu di panjatkan disetiap shalat, terimakasih telah menjadi pendengar yang baik disaat penulis sedang merasa lelah, kehilangan arah, orang tua selalu menjadi alasan penulis untuk kembali semangat menyelesaikan skripsi ini.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

12. Terimakasih untuk seluruh keluarga besar yang selalu memberikan do'a dan kasih sayang kepada penulis
13. Untuk seluruh teman-teman yang tidak dapat disebutkan satu-persatu penulis ucapkan terimakasih karena telah bersama-sama belajar dibangku perkuliahan, memberikan canda tawa setiap harinya, semoga apa yang telah kita perjuangkan dapat membuahkan hasil yang baik. Skripsi ini mungkin masih banyak kekurangan dan jauh dari kata sempurna, semoga kekurangan dalam skripsi ini dapat menjadikan masukan dan pertimbangan bagi penulis lain agar dapat menjadi referensi penulis karya ilmiah selanjutnya.

Pekanbaru, Januari 2022

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

ABSTRAK

Hal ini sangat penting untuk dipertimbangkan saat ini. Kemudian meminta informasi. Untuk komunikasi itu perlu disimpan dan distabilkan. Penelitian dengan judul "Analisis Perbandingan Kinerja Quality Of Service (QOS) Dengan Menggunakan Pptp, L2tp, Sstp Dan Ipsec Pada Jaringan VPN Menggunakan Mikrotik Pada Kantor BKKBN Pekanbaru". Dalam penelitian ini terdapat masalah kualitas point-to-point tunneling (PPTP), Layer 2 tunneling protocol (L2TP), Secure Sockets Tunneling Protocol (SSTP), dan Internet Protocol Security (IPsec). Pengujian ini dilakukan dengan menggunakan dua skema kontrol bandwidth, yaitu skema Download dan Upload. Sebelum melakukan pengujian QoS (Quality Of Service) dengan aplikasi Wireshark, pengujian ini menggunakan bantuan situs Speedtest untuk menghitung nilai download dan upload sebelum melakukan pengujian QoS (Quality Of Service). Berdasarkan penelitian yang telah dilakukan analisis perbandingan QOS (Quality Of Service) semua client dengan menggunakan metode Point to Point Tunneling protocol (PPTP), Layer 2 Tunneling Protokol (L2TP), Secure Socket Tunneling protocol (SSTP) dan Internet Protokol Security (IPSec), maka dapat disimpulkan bahwa untuk pengujian Delay terbaik dihasilkan pada metode SSTP, Packet loss terbaik dihasilnya semua sama sama nol, maka dapat disimpulkan bahwa untuk pengujian Througput terbaik di hasilkan oleh metode L2TP dan IPSEC, Sedangkan Jitter maka terbaik dihasilkan pada metode PPTP dan SSTP.

Kata kunci : Mikrotik, Winbox, Wireshark, QoS(Quality of Service), SpeedTest, Delay, Paket Loss, Througput, Jitter.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

ABSTRACT

This is very important to consider at this time. Then ask for information. For communication it needs to be stored and stabilized. Research entitled "Comparative Analysis of Quality Of Service (QOS) Performance Using Pptp, L2tp, Sstp and Ipsec on VPN Networks Using Mikrotik at the Pekanbaru BKKBN Office". In this study there are quality problems of point-to-point tunneling (PPTP), Layer 2 tunneling protocol (L2TP), Secure Sockets Tunneling Protocol (SSTP), and Internet Protocol Security (IPsec). This test is carried out using two bandwidth control schemes, namely the Download and Upload schemes. Before doing the QoS (Quality Of Service) test with the Wireshark application, this test uses the help of the Speedtest site to calculate the download and upload values before doing the QoS (Quality Of Service) test. Based on research that has been carried out a comparative analysis of QOS (Quality Of Service) of all clients using the Point to Point Tunneling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Tunneling protocol (SSTP) and Internet Protocol Security (IPSec), it can be concluded that for the best delay test the result is the SSTP method, the best packet loss results are all equal to zero, it can be concluded that the best throughput test is produced by the L2TP and IPSEC methods, while the best Jitter is generated by the PPTP and SSTP methods.

Keywords : Mikrotik, Winbox, Wireshark, QoS(Quality of Service), SpeedTest, Delay, Packet Loss, Througput, Jitter.

DAFTAR ISI

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR GAMBAR

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan kemajuan teknologi modern dewasa ini kebutuhan masyarakat akan informasi semakin besar. Sehingga diperlukan media informasi yang cepat, tepat dan akurat dalam upaya memenuhi kebutuhan akan informasi tersebut. Namun permasalahan yang sering timbul adalah faktor keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Maka dibutuhkan suatu cara agar dapat memperoleh suatu informasi data, tukar menukar data, dilakukan dengan aman dan stabil.

Masalah keamanan, kemudahan dan kecepatan dalam transfer data (pertukan data) adalah salah satu aspek yang paling penting dalam suatu jaringan komunikasi terutama untuk perusahaan-perusahaan skala menengah keatas maupun kantor pemerintahan Badan Kependudukan dan Keluarga Berencana Nasional terutama sebagai jaringan komunikasi yang terbuka yang penggunanya dapat mengakses, berbagi dan menambah informasi semudah mungkin sehingga ditakutkan rentan terjadi jatuhnya informasi yang bersifat rahasia dari suatu perusahaan dan kantor pemerintah Badan Kependudukan dan Keluarga Berencana Nasional dan bisa menyebabkan kerugian bagi perusahaan dan kantor pemerintah Badan Kependudukan dan Keluarga Berencana Nasional tersebut. Virtual Private Network (*VPN*) adalah sebuah proses dimana jaringan umum (*public network* atau internet) 2 diamankan kemudian difungsikan menjadi sebuah jaringan privat (private network). Semuanya untuk mencapai satu tujuan yaitu mempermudah

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

kehidupan manusia, khususnya dalam mempermudah pertukaran data dan informasi, serta penyebarannya yang tidak terbatas lagi pada ruang dan waktu. Oleh karena itu kemajuan teknologi informasi harus terus di upayakan dan ditingkatkan kualitas dan kuantitasnya. Salah satu kemajuan teknologi informasi di bidang transmisi pada saat ini yang berkembang salain fiber optic ialah penggunaan perangkat wireless *LAN*.

VPN (Virtual Private Network) adalah sebuah teknologi komunikasi yang memungkinkan untuk terkoneksi ke jaringan *publik* dan menggunakanya untuk bergabung ke jaringan lokal, dengan cara tersebut maka akan diperoleh hak dan pengaturan yang sama seperti halnya berada didalam kantor atau jaringan itu sendiri, walaupun sebenarnya menggunakan jaringan public.

VPN merupakan suatu sistem yang menghubungkan antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan internet (publik). VPN adalah teknologi komunikasi yang memungkinkan seorang pegawai yang berada di dalam kantor terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama ketika pegawai berada di kantor Badan Kependudukan dan Keluarga Berencana Nasional (bkkbn). Kendala yang dihadapi pada kantor adalah waktu pengiriman. Tidak terbatas waktu pengiriman menjadi hambatan pengolahan file ketika lalu lintas padat. Jadwal penyelesaian pekerjaan menjadi mundur dan dapat berakibat komplain atas keterlambatan tesebut. Begitu juga saat file yang dikirim melalui email tidak dapat langsung diolah juga karena merupakan file konversi. Pengiriman file melalui email juga tidak sepenuhnya terjamin keamanannya, dan Rawan penyadapan. Untuk

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

mengatasi hal tersebut pada pegawai kantor Badan Kependudukan dan Keluarga Berencana Nasional (BKKBN) membutuhkan cara yang aman, efisien dan efektif. Permasalahan ini akan semakin kompleks apabila kantor tersebut mempunyai banyak kantor cabang yang tersebar di berbagai kota dengan jarak yang jauh. Sedangkan di lain pihak seluruh kantor tersebut memerlukan suatu metode untuk selalu berhubungan, misalnya untuk transfer dan sinkronisasi data.

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas dapat di identifikasi masalah yang muncul sebagai berikut:

1. Kendala yang dihadapi pada kantor adalah waktu pengiriman. Tidak terbatas waktu pengiriman menjadi hambatan pengolahan file ketika lalu lintas padat. Jadwal penyelesaian pekerjaan menjadi mundur dan dapat berakibat komplain atas keterlambatan tesebut.
2. Yang paling jadi masalah adalah performa Internet.
3. Bahaya dari *Vpn* yaitu Data dan Privasi yang hilang.
4. Adanya permasalahan koneksi yang lambat dapat disebabkan oleh banyaknya PC yang di sharing, dapat juga dikarenakan aktivitas client PC yang sedang mengunduh atau upload yang menghabiskan bandwidth tersebut.

1.3 Batasan Masalah

Batasan masalah yang terdapat pada penelitian dan pengembangan terakhir ini adalah:

1. Sistem manajemen bandwith menggunakan aplikasi winbox.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2. Monitoring traffic jaringan terdapat pada *Wireshark* dan *Router Os Winbox* tersebut
3. Aplikasi yang digunakan adalah *Wireshark* , untuk mengatur menggunakan bantuan dari situs Speedtest untuk mengukur besar nilai unduh dan unggah pengujian QOS.
4. Parameter yang digunakan untuk pengukuran pengaruh penggunaan IPSec di jaringan internet adalah latency dan Throughput

1.4 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat dirumuskan masalah sebagai berikut:

1. Bagaimanakah cara mengetahui peforma masing masing protocol *VPN*?
2. Bagaimana kinerja QoS (Quality of Service) mengatasi kemacetan yang terjadi pada jaringan?
3. Bagaimana menganalisa kualitas data atau trafik dalam jaringan VPN dengan protokol L2TP dan PPTP?
4. Bagaimana cara maksimalkan fitur protokol PPTP,L2TP,SSTP,dan IPSEC pada jaringan VPN dengan benar?

1.5 Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Meningkatkan efisiensi dan aktifitas jaringan di kantor BKKBN.
2. Memberikan masukan solusi untuk meningkatkan kinerja jaringan pada BKKBN agar lebih optimal.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. Memberikan gambaran tentang kelebihan dan kekurangan pada penerapan QoS.

1.6 Manfaat Penelitian

Adapun manfaat yang dapat diambil pada penelitian ini adalah:

1. Mengetahui kualitas performa protokol *PPTP* dan *L2TP*
2. Sebagai bahan referensi perancangan suatu jaringan VPN dengan menggunakan mikrotik agar dapat kualitas jaringan yang bagus
3. Memberikan data perbandingan tentang performa protokol *PPTP* dan *L2TP* sebagai dasar perancangan suatu jaringan VPN menggunakan mikrotik

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB II

LANDASAN TEORI

2.1 Studi Keputusan

Dengan Untuk menyusun proposal penelitian ini penulis juga melakukan studi kepustakaan yang merujuk kepada penelitian-penelitian sebelumnya yang berkaitan dengan penelitian yang penulis buat. Studi kepustakaan ini dilakukan sebagai bahan perbandingan dan referensi bagi penulis.

Studi kepustakaan pertama berdasarkan penelitian yang dilakukan oleh Menurut (Zamalia et al., 2018) Dengan melakukan penelitian tentang *Tunnel Point to Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Secure Socket Tunneling Protocol* (SSTP), dan *Internet Protocol Security* (IPsec) merupakan jenis VPN yang telah banyak didukung oleh protokol jaringan untuk dapat diterapkan pada banyak perangkat jaringan komputer. Keempat metode tersebut diterapkan secara bergantian pada mikrotik. Setiap metode yang diterapkan, selanjutnya akan dianalisis dengan menggunakan aplikasi *Wireshark* dengan parameter *Quality of Service* (QoS) yang terdiri dari *Packet Loss, Delay*, dan *Throughput*. Pengujian dilakukan terhadap 4 *client* yang terhubung ke *access point* dengan dua skenario jaringan, skenario pertama semua *client* mengakses web berbasis *download* dan skenario kedua semua *client* pada jaringan mengakses web *streaming* video. Hasil pengujian keamanan antara *tunnel PPTP, L2TP, SSTP*, dan *IPSec* menunjukan bahwa tingkat keamanan yang dibagun oleh *tunnel* IPsec lebih baik dari *tunnel PPTP, L2TP*, dan *SSTP*. Sedangkan untuk hasil pengujian terhadap

performa, keamanan serta temuan-temuan pengujian diperoleh bahwa *tunnel VPN IPsec* lebih baik dibandingkan *tunnel VPN,PPTP, L2TP*, dan *SSTP*.

Studi kepustakaan kedua adalah berdasarkan penelitian yang di lakukan oleh (Azhar & Romliyanto, n.d.) Dengan judul penelitian "Analisis Perbandingan Protokol *PPTP* dan *L2TP* Menggunakan Video Call Melalui Jaringan *Virtual Private Network* (VPN)", isi dari penelitiannya adalah user dapat melakukan koneksi ke private network dari manapun, apabila diperlukan. Pada jaringan VPN ini akan dilakukan perbandingan kualitas jaringan di mana jaringan nya tersebut menggunakan dua protocol yang berbeda, yaitu protocol *PPTP* dan *L2TP*. Dalam ha ini akan dilakukan pengujian untuk mengetahui perbedaannya dengan melakukan panggilan video call.

Studi kepustakaan ketiga adalah berdasarkan penelitian yang di lakukan oleh (Mukhlishah, 2020) . Dengan judul penelitian Analisis Perbandingan Kinerja Jaringan *Secure Socket Tunneling Protocol* (Sstp) Dan *Layer Two Tunneling Protocol* (L2tp) + *Internet Protocol Security* (Ipsec) Menggunakan Metode Quality Of Service (Qos). Isi dari penelitiannya adalah Dalam tahapan ini peneliti mencoba memahami topologi serta kinerja jaringan yang akan diterapkan, sehingga bisa menganalisa perbandingan kinerja *SSTP* dan *L2TP+IPSecurity* berdasarkan parameter yang digunakan yaitu Troughput, delay, packet loss dan jitter. Setelah diuji, selanjutnya yaitu membandingkan hasil pengujian dari dua metode tunneling untuk performa jaringan tersebut dengan menganalisis serta menyimpulkan hasil pengujian yang telah didapat.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Kesimpulan dari ketiga jurnal diatas yaitu : Untuk melakukan perbandingan performa jaringan ketika di terapkan metode SSTP dan L2TP+IPSec sehingga mengetahui performa jaringan mana yang lebih bagus dan cocok digunakan sesuai dengan kebutuhan pengguna.Dan membangun sistem jaringan *VPN* dengan memasang seluruh perangkat sesuai dengan rancangan jaringan menggunakan tiap langkah sehingga selesai menurut (Mukhlishah, 2020)

Langkah pertama kali pada proses implementasi adalah konfigurasi *SSTP* pada jaringan *VPN* sampai selesai kemudian mengecek konfigurasi *VPN* tersebut dengan perintah "ping" ke koneksi internet, selain itu juga bisa menggunakan tool "speedtest" untuk mengetahui kecepatan pada koneksi *VPN* tersebut.

Langkah berikutnya adalah konfigurasi *L2TP* yang dikombinasikan dengan IPSec sampai selesai kemudian cek konfigurasi dengan menguji koneksi ke internet dan cek kecepatan koneksi VPN tersebut.

Pengujian dilakukan untuk mengumpulkan data-data melalui wireshark yang akan digunakan untuk menganalisis nilai Troughput, Packet loss, Delay dan jitter. Pada pengujian nilai troughput yang akan di analisa yaitu jumlah total semua paket data yang berhasil diterima melalui media transmisi jaringan. Pada pengujian packet loss yang dianalisa yaitu jumlah total paket yang hilang selama melakukan transmisi data pada jaringan. Pada pengujian delay yang dianalisa yaitu waktu tunda yang dibutuhkan suatu paket data yang dikirim oleh sumber sampai tujuan. Dan pada pengujian jitter yang dianalisa yaitu perbedaan selang waktu antara paket pada jaringan.Menurut (Mukhlishah, 2020)

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Menurut (Azhar & Romliyanto, n.d.) yaitu : Kualitas QOS jaringan VPN yang menggunakan protocol L2TP lebih baik daripada jaringan VPN yang menggunakan protocol PPTP karena paket data yang diterima pada waktu yang sama lebih besar pada jaringan VPN L2TP sehingga sehingga nilai troughputnya lebih besar.

Menurut (Zamalia et al., 2018) yaitu : Berdasarkan hasil uji QoS dengan metode PPTP, L2TP, SSTP dan IPSec maka dapat dibuatkan tabel yang membandingkan nilai delay antara metode PPTP, L2TP, SSTP dan IPSec dari tiap-tiap kondisi download dan upload.

Dan terakhir menurut (Nasihin et al., 2015) yaitu : Permasalahan yang terjadi yaitu saat data-data tersebut harus selalu tersedia, otomatis akan membutuhkan jaringan yang selalu menyediakan akses pada distribusi data. Namun data yang ada hanya tersedia dalam lokal area jaringan instansi tersebut, sehingga untuk mengakses data dan memonitoring jaringan hanya dapat dilalukan secara local jaringan.

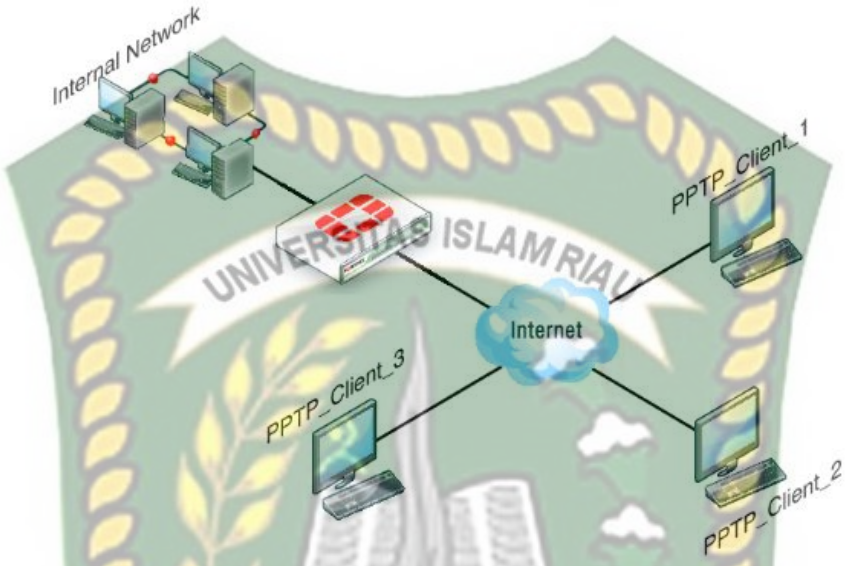
2.2 Point to Point Tunneling Protocol (PPTP)

PPTP merupakan protocol jaringan yang memungkingkan pengamanan transfer data dari *remote client* (client yang berada jauh dari server) ke server pribadi perusahaan dengan membuat sebuah VPN melalui *TCP/IP* menurut (Watmah, 2020).

Seluruh komunikasi data antar jaringan pribadi akan melalui tunnel ini, sehingga orang atau user dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Di dalam tunneling terdapat proses enkapsulasi, (Pérez et al., 2017)

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

transmisi dan dekapsulasi paket yang di komunikasikan. Topologi PPTP Client pada kantor bkkbn.

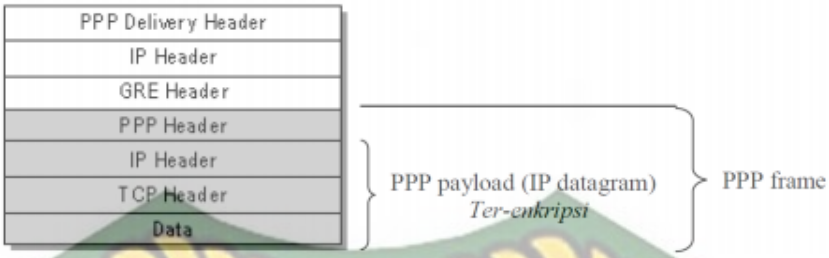


Gambar 2 1 Topologi PPTP

Teknologi tunneling dikelompokkan secara garis besar berdasarkan protokol tunneling layer 2 (*Data Link Layer*) dan layer 3 (*Network Layer*) model OSI layer. Yang termasuk ke dalam tunneling layer 2 adalah *L2F*, *PPTP*, dan *L2TP*. Sedangkan yang termasuk layer 3 adalah *IPSec*, *VTP, dan ATMP*. Setelah *PPTP* tunnel terbentuk, data dari user ditransmisikan antara *PPTP client* dan *PPTP server*. Data yang ditransmisikan dalam bentuk IP datagram yang berisi *PPP paket*.

IP datagram dibuat dengan menggunakan versi protokol *Generic Routing Encapsulation (GRE)* internet yang telah dimodifikasi. Struktur paket data yang dikirimkan melalui *PPTP* dapat digambarkan sebagai berikut:

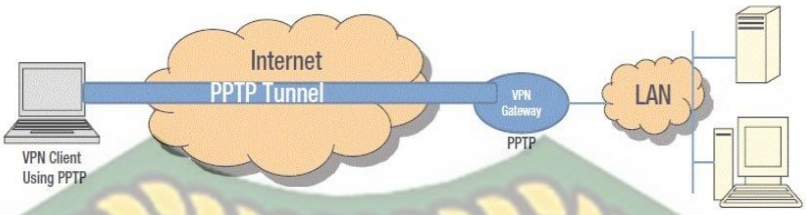
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 2 2 Paket Data PPTP

Menurut (Ikhwan & Amalina, 2017) Cara kerja *PPTP* dimulai dari sebuah remote atau *PPTP client mobile* yang membutuhkan akses ke sebuah LAN private dari sebuah perusahaan. Pengaksesan dilakukan dengan menggunakan *ISP lokal*. *Client* (yang menggunakan *Windows NT Server* versi 4.0 atau *Windows NT Workstation versi 4.0*) menggunakan DialUp networking dan *protokol remote access PPP* untuk terhubung ke sebuah ISP. Client terhubung ke *Network Access Server (NAS)* pada fasilitas ISP. NAS di sini bisa berupa prosesor front-end, server dial-in atau server *Point-of-Presence* (POP). Begitu terhubung, client bisa mengirim dan menerima paket data melalui internet. NAS menggunakan *protocol TCP/IP* untuk semua trafik yang melalui internet Setelah client membuat koneksi PPP ke ISP, panggilan Dial-Up Networking yang kedua dibuat melalui koneksi PPP yang sudah ada. Data dikirimkan menggunakan koneksi yang kedua ini dalam bentuk IP datagram yang berisi paket PPP yang telah ter-enkapsulasi. Panggilan yang kedua tersebut selanjutnya menciptakan koneksi *VPN* ke server *PPTP* pada LAN private perusahaan. Koneksi inilah (melalui panggilan kedua) yang di-istilahkan sebagai tunnel (lorong). Berikut ini gambar yang menjelaskan proses tersebut :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 2.3 Tunelling PPTP

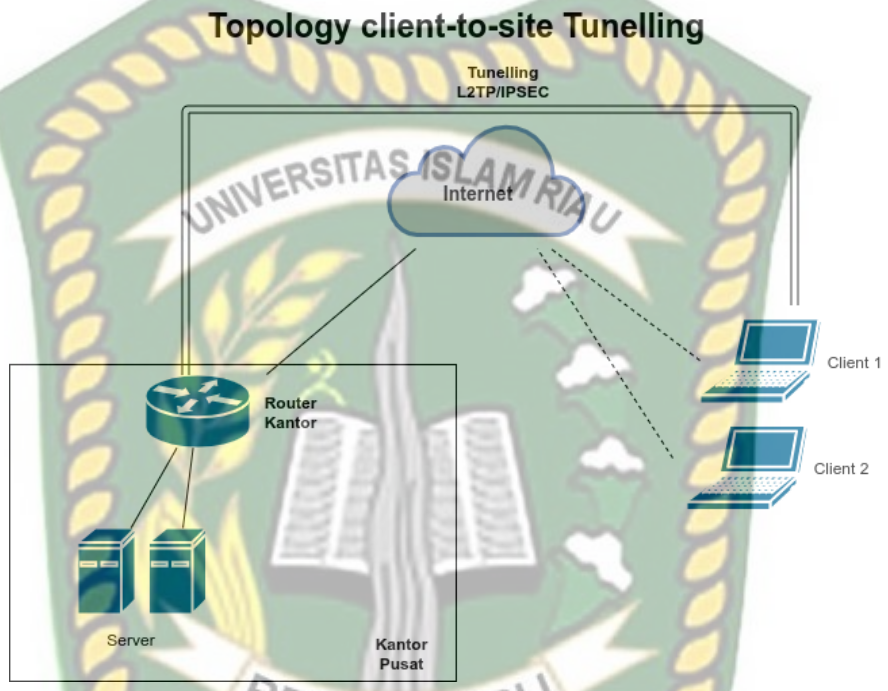
Menurut (Watmah, 2020)Tunneling pada gambar diatas adalah sebuah proses pengiriman paket data ke sebuah komputer pada jaringan privat dengan me-routing paket data tersebut melalui beberapa jaringan yang lain, misalnya Internet. Router-router jaringan yang lain tidak bisa mengakses komputer yang berada pada jaringan privat.

2.3 Layer 2 Tunneling Protocol (L2TP)

Menurut (Zamalia et al., 2018) L2TP merupakan tunneling protocol yang memadukan dua buah tunneling protokol yaitu Layer 2 Forwarding milik Cisco dan PPTP yang dimiliki Microsoft. L2TP umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang dapat membawa semua jenis protokol komunikasi di dalamnya dan biasanya menggunakan port 1702 dengan protokol UDP. Terdapat dua model tunnel yang dikenal, yaitu compulsory dan voluntary. Perbedaan utama keduanya terletak pada endpoint tunnel-nya. Pada compulsory tunnel, ujung tunnel berada pada ISP, sedangkan pada voluntary ujung tunnel berada pada client remote.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Layer 2 Tunneling Protocol (L2TP) merupakan hasil penggabungan dari spesifikasi *PPTP dan L2F*, dimana dapat mengenkapsulasi *PPP frames* dan mengantarkan data ke jaringan bersama (public).

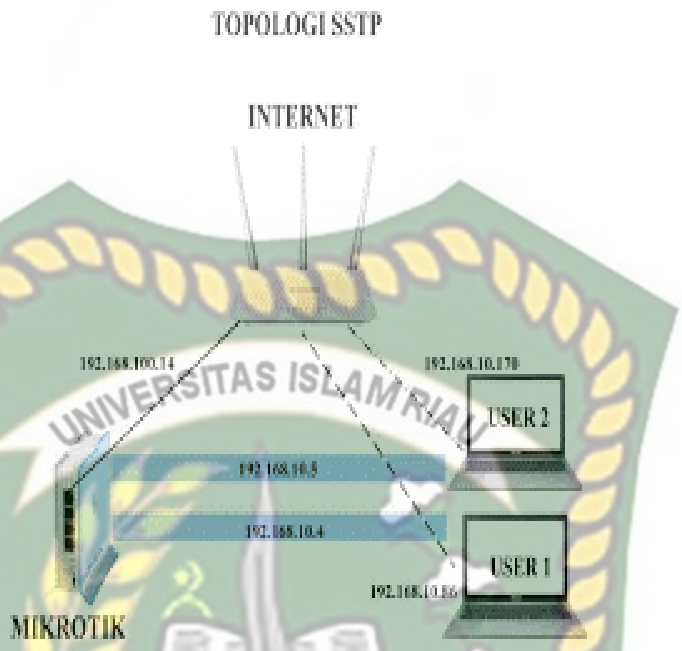


Gambar 2.4 Tunnelling L2TP

2.4 Secure Socket Tunneling Protokol (SSTP)

Secure Socket Tunneling Protokol adalah tembusan protokol yang tersedia pada *platform* Microsoft. Protokol ini berbasis pada kombinasi kedua teknologi, *SSL dan TCP*. enkripsi terkuatlah yang diaktifkan. Sejak sesi *SSTP*, dalam kenyataannya, sebuah sesi *HTTPS*, *SSTP* mungkin bisa digunakan melalui *firewall* atau ISP *throttling*. Di sisi lain, sejak *SSTP* beroperasi melalui *TCP*, dalam beberapa kasus akan dikendalikan IKEv2 atau protokol berbasis *UDP* lainnya. Secara keseluruhan, *SSTP* adalah pilihan terbaik dan dapat membantu menyelesaikan masalah konektivitas ataupun masalah kecepatan yang dimiliki.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 2.5 Topologi SSTP

Diperkenalkan oleh *Microsoft Corporation* dalam *Windows Vista Service Package 1* (SP1), kanalisasi soket aman yang sekarang tersedia untuk *SEIL, Linux dan RouterOS*, namun masih diutamakan untuk *platform* Windows. Oleh karena protokol ini memakai SSL v3, sehingga memberikan keunggulan yang sama dengan *OpenVPN*, seperti kemampuan untuk mencegah masalah *firewall* NAT.

SSTP adalah protokol *VPN* yang stabil dan mudah digunakan, terutama disebabkan integrasinya ke dalam Windows. SSTP (*Secure Socket Tunneling protocol*) adalah bentuk VPN *tunnel* yang menyediakan mekanisme untuk mengirimkan *traffic* PPP atau *L2TP* melalui sebuah saluran SSL 3.0. SSL menyediakan *transport-level security* dengan *key-negotiation*, enkripsi dan *traffic integrity checking*. Penggunaan SSL melalui *port* TCP 443 mengizinkan *SSTP* untuk melewati secara virtual semua *firewall* dan *proxy server* kecuali untuk otentikasi web *proxy*.

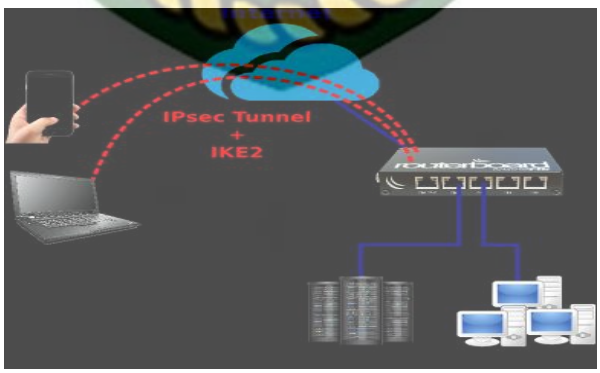
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

SSTP *server* harus diotentikasi selama fase *SSL*. *SSTP client* dapat secara opsional diotentikasi selama fase SSL, dan harus diotentikasi selama fase PPP. Penggunaan PPP mendukung metode otentikasi secara umum seperti *EAP-TLS* dan *MS-CHAP*. SSTP dapat diterapkan di *linux, BSD, dan Windows*. Mikrotik *router* OS juga mengizinkan SSTP *client* dan *server*.

Salah satu fitur VPN yang ada di MikroTik adalah SSTP (*Secure Socket Tunneling protocol*). SSTP merupakan sebuah *PPP Tunnel* dengan *TLS 1.0 Channel*. Fitur ini berjalan pada protokol TCP dan *Port* 443. Supaya dapat memanfaatkan SSTP secara optimal dengan keamanan yang baik. Maka diharuskan menambahkan sertifikat SSL untuk koneksi antara *server* dan *client*.

Sertifikat Teknologi SSL menjaminkan tingkat keamanan transportasi dan integritas lalu lintas. SSL pada *server* dikonfigurasikan sedemikian rupa sehingga hanya metode SSL itu bias didapatkan dengan membeli melalui vendor-vendor yang ada atau bisa dibuat sendiri menggunakan *Open SSL*.

2.5 Internet Protokol Security (IPSec)

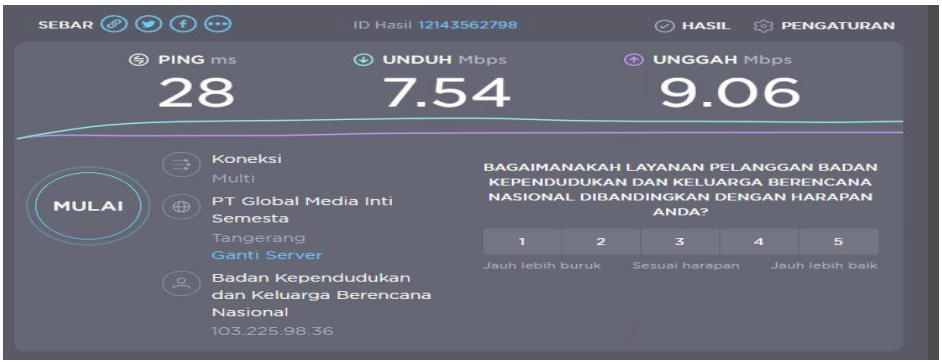


Gambar 2.6 Topologi IPSEC

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

IPSec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan system untuk memilih *protocol* keamanan yang diperlukan, algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec bekerja dengan tiga cara yaitu: *Network-to-network, Host-to-network dan Host-to-host*.IPSec adalah pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya. Pada dasarnya paket IP tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditransmisikan oleh si pengirim paket. Paket IP yang tidak memiliki keamanan atau *security*, sangat mudah untuk diketahui isinya dan alamat IP itu sendiri. Menurut (Sari & Kemala, 2020) IPsec adalah metode yang bertujuan untuk menjaga keamanan IP datagram ketika paket diransmisikan pada *traffic*. Sehingga IPsec menjadi suatu mekanisme yang diimplementasikan pada VPN. IPSec berada pada *layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada di atasnya.

2.6 Quality Of Service (QOS)



Gambar 2 7 Quality Of Service

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Dari segi *networking*, QoS mengacu kepada kemampuan memberikan pelayanan berbeda kepada lalu lintas jaringan dengan kelas-kelas yang berbeda. Menurut (Iryani et al., 2020) Tujuan akhir dari QoS adalah memberikan *network service* yang lebih baik dan terencana dengan *dedicated bandwidth*, *jitter* dan *latency* yang terkontrol dan meningkatkan *loss* karakteristik. Berikut adalah penjelasan mengenai parameterparameter yang digunakan dalam penilaian QoS yang baik:

1. Delay

Menurut (Zamalia et al., 2018) *Delay* adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Besarnya *delay* dapat diklasifikasikan seperti yang ditunjukkan pada Tabel 2.1 dibawah ini.

Tabel 2 1 Delay

Kategori Latensi	Besar *Delay*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	>450 ms	1

Untuk mengukur persamaan *delay*

$$\boldsymbol{Delay} = \frac{\boldsymbol{Total\ delay}}{\boldsymbol{Total\ paket\ yang\ di\ terima}} \quad \textbf{(2,1) } \boldsymbol{Tabel\ Delay}$$

2. Packet Loss

Menurut (Mukhlishah, 2020) *Packet Loss* merupakan parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang,

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efesiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima. Nilai *packet loss* sesuai dengan versi TIPHON ditunjukkan pada Tabel 2. 2 dibawah ini.

Tabel 2 2 Packet Loss

Kategori Degredasi	*Packet Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	1

Untuk mengukur *packet loss* digunakan Persamaan *Packet Loss.*

$$\mathbf{PL} = \frac{PTT-PT}{PTT} \times 100\ \%\ \ \textbf{(2,2) } \textit{Tabel Packet Loss}$$

Ket : PL = Packet Loss

PTT = Paket Total Tercapture

PT = Packet Terkirim

3.Throughput

Menurut (Nasihin et al., 2015) *Throughput* yaitu kecepatan (*rate*) transfer data yang efektif yang diukur dalam bps. *Throughtput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu.dibagi oleh durasi interval waktu tersebut.Untuk mengukur *throughput* digunakan Persamaan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Tabel 2 3 Throughput

Kategori Jitter	Kualitas	Indeks
Sangat Bagus	100%	4
Bagus	75%	3
Sedang	50%	2
Jelek	<25%	1

$$T = \frac{JDK}{LP}$$ **(2,3) Tabel Througput**

Ket :

T = Throughput
JDK = Jumlah Data yang di Kirim
LP = Lama Pengamatan

Total kedatangan paket IP berhasil yang ditinjau di lokasi pengukuran pada destination ketika interval waktu tertentu dibagi oleh durasi interval waktu tersebut (Sama dengan, jumlah pengiriman paket IP berhasil per service-second). Throughput lebih pada memvisualkan bandwidth yang asli pada waktu tertentu serta ketika keadaan serta jaringan internet tertentu yang dipakai untuk men-download sesuatu file yang berukuran tertentu.

4.Jitter

Jitter adalah variasi dalam panjang antrian, dalam waktu pengolahan data dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan.

Tabel 2 4 Jitter

Kategori Jitter	Peak Jitter	Indeks
Sangat Bagus	0 ms	4
Bagus	0 s/d 75 ms	3
Sedang	75 s/d 125	2
Jelek	125 s/d 225	1

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Persamaan perhitungan Jitter

$$\frac{Total\ variasi\ delay}{Total\ paket\ yang\ di\ terima} \quad (2,4)$$ ***Tabel Jitter***

2.7 Parameter QUALITY OF SERVICE (QOS)

Tabel 2 5 Parameter Quality Of Service

Parameter QoS	Scenario	*Workload (byte)*	Average results	*TIPHON Standart*
Delay (ms)	1 (3 nodes)	2000	3.53	Very Good
		2500	4.76	Very Good
		3000	4.49	Very Good
	2 (4 nodes)	2000	3.77	Very Good
		2500	4.63	Very Good
		3000	6.53	Very Good
	3 (5 nodes)	2000	3.83	Very Good
		2500	4.93	Very Good
		3000	10.63	Very Good
Jitter (ms)	1 (3 node)	2000	4.67	Good
		2500	5.06	Good
		3000	6.43	Good
	2 (4 nodes)	2000	4.70	Good
		2500	5.06	Good
		3000	6.50	Good
	3 (5 nodes)	2000	6.67	Good
		2500	13.10	Good
		3000	20.28	Good
Packet loss (%)	1 (3 node)	2000	3.85	Good
		2500	13.86	Good
		3000	25.39	Bad
	2 (4 nodes)	2000	7.95	Good
		2500	35.14	Bad
		3000	45.40	Bad
	3 (5 nodes)	2000	35.25	Bad
		2500	66.60	Bad
		3000	74.05	Bad
Throughput (%)	1 (3 nodes)	2000	80.58	Good
		2500	60.88	Medium
		3000	50.28	Medium
	2 (4 nodes)	2000	47.66	Bad
		2500	59.16	Good
		3000	79.98	Good
	3 (5 nodes)	2000	56.38	Good
		2500	39.28	Bad
		3000	35.32	Bad

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Hasil perbandingan yang ditunjukkan pada Tabel 1 adalah protokol routing Babel QoS pada Mobile Ad-hoc Jaringan dengan standar TIPHON. Hasilnya adalah sebagai berikut:

Pada skenario 3, 4, dan 5 node dengan beban 2000 byte, 2500 byte, dan 3000 byte, delay termasuk dalam kategori sangat baik.

Pada skenario 3, 4, dan 5 node dengan beban 2000 byte, 2500 byte, dan 3000 byte, jitter adalah termasuk dalam kategori baik.

Dalam skenario 3 node dengan beban 2000 byte dan 2500 byte, packet loss termasuk dalam kategori baik. Dalam skenario 3 node dengan beban 3000 byte, packet loss disertakan dalam kategori jelek. Dalam skenario 4 node dengan beban 2000 byte, packet loss disertakan dalam kategori baik. Pada skenario 4 node dengan beban 2500 byte dan 3000 byte, packet loss termasuk dalam kategori jelek. Dalam skenario 5 node dengan beban 2000 byte, 2500 byte, dan 3000 byte, packet loss termasuk dalam kategori jelek.

Pada skenario 3 node dengan beban 2000 byte, throughput termasuk dalam kategori baik. Dalam skenario 3 node dengan beban 2500 byte dan 3000 byte, throughput termasuk dalam kategori sedang. Dalam skenario 4 node dengan beban 2000 byte, throughput disertakan dalam kategori jelek. Dalam skenario 4 node dengan beban 2500 byte dan 3000 byte, throughput termasuk dalam kategori baik. Dalam skenario 5 node dengan beban 2000 bytes, throughput termasuk dalam kategori baik. Dalam skenario 5 node dengan beban 2500 byte dan 3000 byte, throughput termasuk dalam kategori jelek.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB III

METODOLOGI PENELITIAN

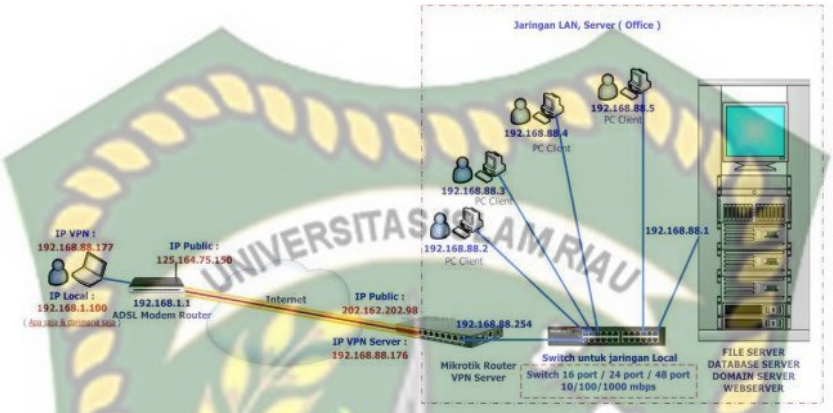
3.1 Definisi Masalah dan Analisis Skenario Jaringan Kantor BKKBN

Pada penelitian ini terdapat beberapa masalah mengenai quality of service pada *Tunnel Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Tunneling Protocol (SSTP), dan Internet Protocol Security (IPsec)* yaitu:

1. *SSTP dan L2TP+IPSec* merupakan protokol jaringan yang dapat melindungi jaringan dari ancaman luar seperti konflik IP, MAC dan DHCP server jahat, serta membuat performa jaringan lebih baik, dengan metode penggunaan jalur tersendiri yang di lalui atau dilewati.
2. Kinerja jaringan yang buruk tentu akan berdampak buruk bagi oleh perkantoran berubah menjadi lambat.
3. Metode *SSTP dan L2TP+IPSec* sehingga mengetahui performa jaringan mana yang lebih bagus dan cocok digunakan sesuai dengan kebutuhan pengguna.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

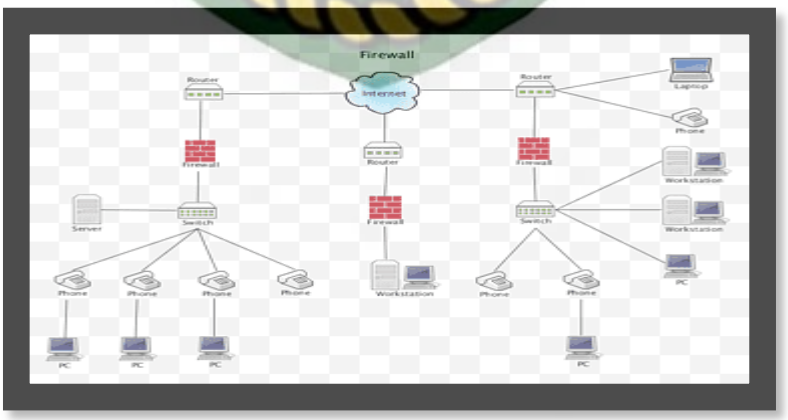
3.1.1 Analisis Skenario Jaringan Kantor BKKBN



Gambar 3. 1 Skenario Jaringan Kantor Bkkbn Pekanbaru

Pc client ke Local Area Network (LAN) saling komunikasi Virtual Private Network (VPN) yang menghubungkan sebuah PC atau Laptop Client ke jaringan LAN via internet. Sehingga kita dapat mengakses semua resource yang ada dalam jaringan atau server di kantor. Sehingga dengan VPN ini seolah-olah PC / Laptop Client berada dalam 1 tempat atau 1 jaringan LAN tersebut.

3.1.2 Blok Diagram Jaringan

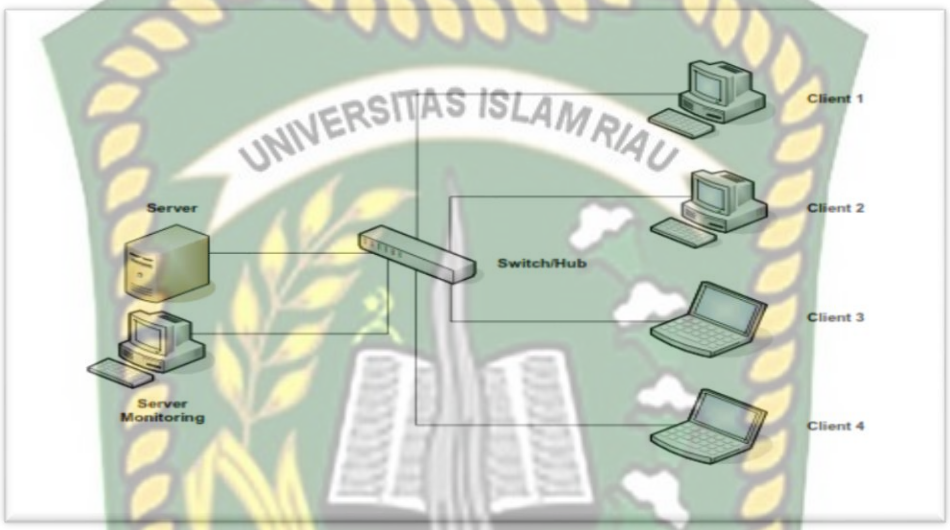


Gambar 3. 2 Blok Diagram Jaringan Kantor Bkkbn

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Gambar diatas terdapat alat jaringan berupa internet , router , switch , firewall dan perangkat keras yaitu Pc , Laptop dan Hp atau telephone.

3.1.3 Diagram Jaringan Kantor Bkkbn Pekanbaru



Gambar 3. 3 Diagram Jaringan Kantor Bkkbn Pekanbaru

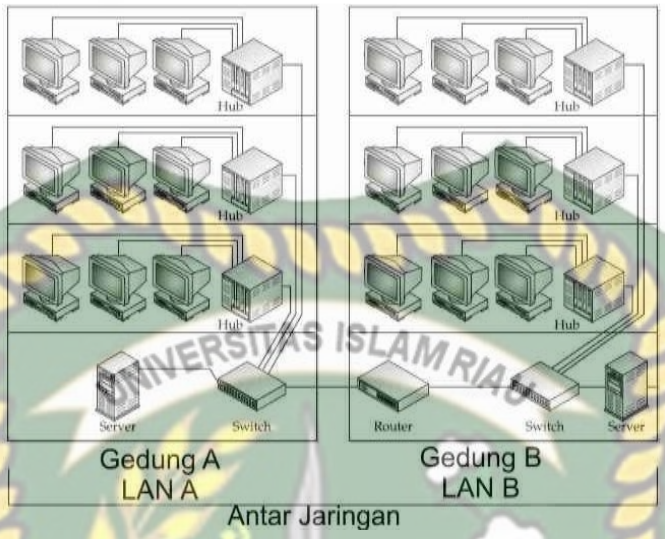
Kantor Bkkbn dengan menggunakan ***Local Area Network*** (*LAN*) . Jaringan yang di batasi oleh area yang relative kecil. Pada umumnya di batasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung.

3.1.4 Skema Jaringan Kantor Bkkbn

Skema jaringan internal penulis melihat beberapa permasalahan yang harus dibenahi sehingga nantinya untuk jaringan internal akan dibuat skema jaringan yang memenuhi kualitas standar jaringan komputer.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Skema topologi jaringan komputer pada gedung A dan gedung B :



Gambar 3. 4 Gambar Skema Jaringan

3.2 Alat dan Bahan Penelitian Yang Digunakan

Peralatan yang digunakan dalam perancangan ini terdiri dari perangkat keras dan perangkat lunak.Daftar peralatan yang digunakan adalah:

3.2.1 Perangkat keras (*Hardware*) :

1. Cisco router 2801: 3 buah yang digunakan untuk:
   a. 1 buah sebagai router ISP A
   b. 1 buah sebagai router ISP B
   c. 1 buah sebagai router Network Client
   d. 1 buah switch
2. Personal Computer : 3 buah yang digunakan adalah :
   a. 1 buah sebagai PC Server
   b. 1 buah sebagai PC Client
   c. 1 buah PC sebagai router mikrotik untuk L2TP/PPTP Server

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.2.2 Perangkat Lunak (*Software*) :

1. *Mikrotik*
2. *Cisco Paket Tracer*
3. *Virtualbox Dan Winbox*
4. *Cmd (Command Promt)*
5. *Wireshark Network*

3.2.3 Bahan Penelitian

Berikut ini adalah beberapa bahan yang di gunakan untuk penelitan yaitu berupa perangkat lunak atau *software*. Untuk dapat melakukan analisis sebuah penelitian tentu saja *software* sangat penting untuk melancarkan proses analisis yang sesuai dengan kebutuhan. Dan *software* yang digunakan dalam penelitian ini adalah berupa sebagai berikut.

a. Sistem Operasi Windows 10

Sistem Operasi di gunakan untuk mengendalikan sumber daya Laptop yang Penulis gunakan untuk penelitian.

b. Cisco Packet Tracer 7.1

Aplikasi yang di gunakan untuk membuat arsitektur dan topologi jaringan yang terhubung ke internet.

c. Qos Pada Mikrotik

QoS (kualitas layanan) adalah metode untuk menjaga kualitas layanan tetap **pada** batas minimal yang ditentukan. ***QoS*** juga bisa digunakan untuk mengatur prioritas berdasarkan parameter-parameter yang

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

diberikan dan menghindari terjadinya monopoli sebuah traffic terhadap seluruh bandwidth yang tersedia.

d. Winbox

Utility yang digunakan untuk konektivitas dan konfigurasi MikroTik menggunakan MAC Address atau protokol IP. Dengan winbox kita dapat melakukan konfigurasi MikroTik RouterOS dan RouterBoard menggunakan mode GUI dengan cepat dan sederhana.

e. WireShark

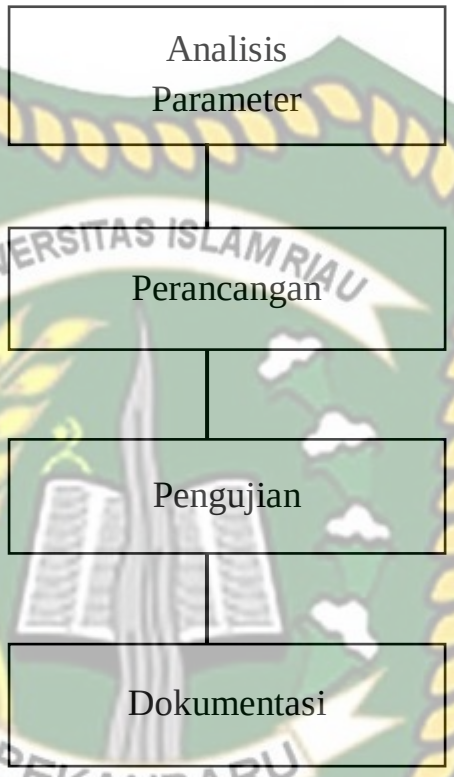
Sangat berguna untuk profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Hal ini karena Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer.

f. Command Prompt

Tools ini di gunakan untuk menulis script untuk mencari IP Address target untuk membuat IP bayangan yang akan di arahkan ke IP pembajak.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.3 Prosedur Penelitian



Gambar 3. 5 Skema Prosedur Penelitian

Dalam proses pengumpulan data untuk mendapatkan data yang benar dan menyakinkan agar hasil yang dicapai agar tidak menyimpang dari tujuan telah diterapkan sebelumnya,penulis melakukan dengan langkah-langkah penelitian sebagai berikut :

1. Analisis Parameter

Di dalam tahapan ini akan di rancang sebuah proses pengiriman data atau halaman web dari server menuju client, sehingga dapat di ketahui parameter

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

parameter *quality of service* antara lain Delay, Packet Loss, dan Througput. Sehingga kesimpulan akan di ambil dari hasil perbandingan yang sudah diperoleh.

2. Perancangan

Tahap ini akan merancang analisa *quality of service*. Spesifikasi kebutuhan yang telah di dapat ke dalam bentuk arsitektural perangkat lunak dengan menggunakan *Speedtest*.

3. Pengujian

Dalam pengujian kinerja quality of service pada *Point to point tunnelling protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Tunneling Protokol (SSTP), Internet Protocol Security (IPSEC)* dilakukan dengan cara menggunakan aplikasi wireshark dan mikrotik untuk mendapatkan hasil dari pengujian yang berjalan.

4. Dokumentasi

Pada proses dokumentasi, penulis juga melakukan studi pustaka, membaca dan mempelajari dokumen dokumen, buku-buku acuan, serta sumber lainnnya yang berkaitan dengan penelitian untuk dijadikan referensi.

3.4 Perhitungan Data

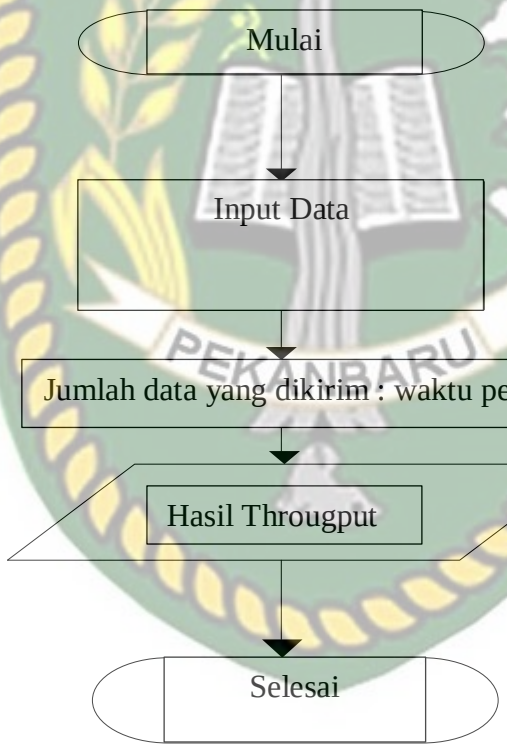
Perhitungan data berdasarkan pada parameter QoS (Quality of Service), dikarenakan QoS merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

servis. QoS didesain untuk membantu network administrator memastikan bahwa user mendapatkan kinerja yang handal dan memuaskan.

Komponen-komponen dari QoS adalah Throughput, Delay, Loss packet dan dalam pengujian kali ini saya menambahkan utilisasi bandwidth dalam menentukan QoS. Berikut ini yang dilakukan untuk menetukan parameter-parameter tersebut.

3.4.1 Menghitung Througput PPTP (Point to Point Tunneling Protocol)

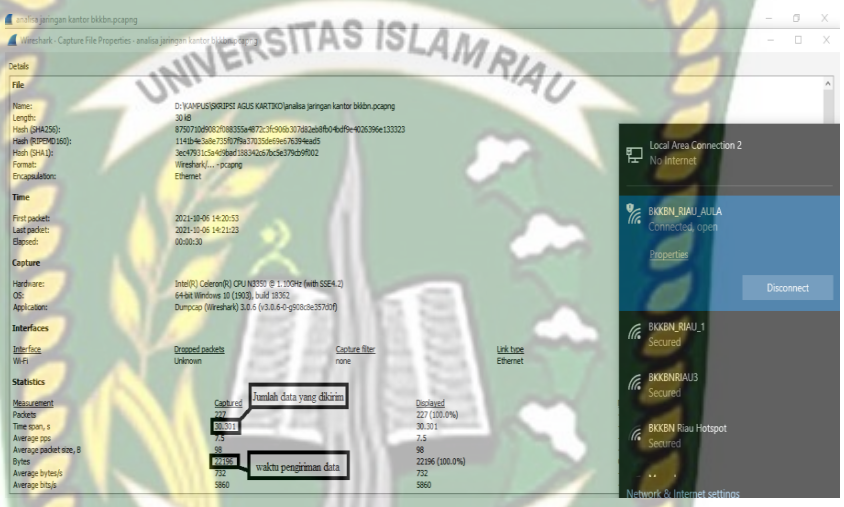


Gambar 3. 6 *Flowchart* Perhitungan *Throughput*

Langkah yang dilakukan untuk perhitungan *Throughput* menggunkan apliksi *wireshark* ini adalah input data, yang mana itu adalah hasil capture

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

jaringan melalui *wireshark*. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu jumlah data yang dikirim/waktu pengiriman data. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.



Gambar 3. 7 *Summary Troughput (Ringkasan Troughput)*

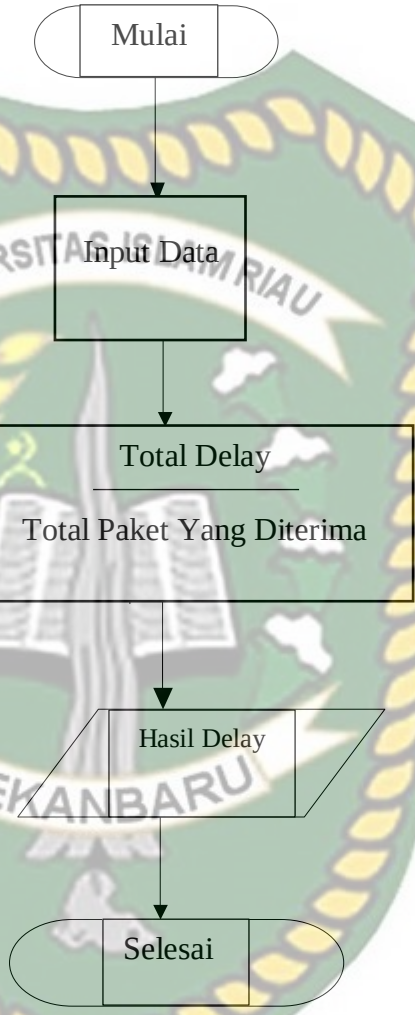
Dari percobaan diatas Troughput yang dihasilkan 0,0109212471 Kbps dilihat pada table TIPHON nilai Troughput ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Jumlah data yang dikirim (30.301) dibagi dengan waktu pengiriman data (22196) sama dengan hasilnya (5860 Kbps).

$$\frac{Jumlah\ data\ yang\ dikirim}{waktu\ pengiriman\ data}$$

$$\frac{30.301}{22196} = \frac{1{,}365155883 Kbps}{125} = 0{,}0109212471 \text{ kbps}$$

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

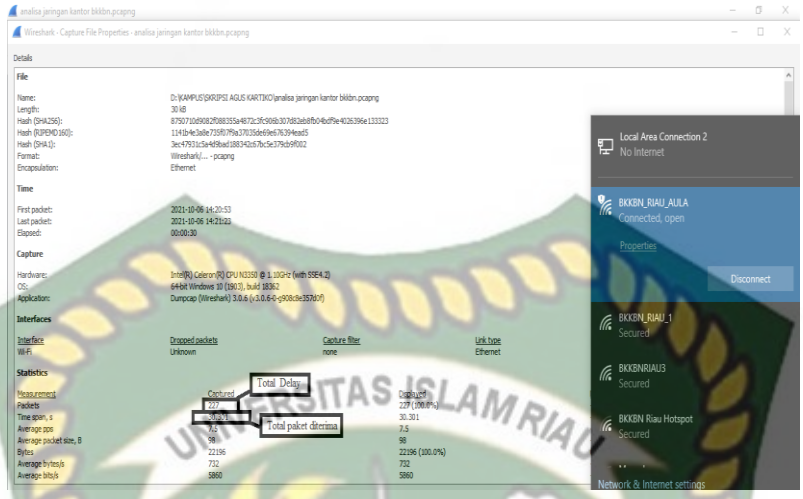
3.4.2 Menghitung *Delay PPTP (*Point to Point Tunneling Protocol)



Gambar 3. 8 *Flowchart* Perhitungan *Delay*

Langkah yang dilakukan untuk perhitungan Delay menggunkan apliksi wireshark ini adalah input data, yang mana itu adalah hasil capture jaringan melalui wireshark. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu jumlah Delay/jumlah packet receive. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 3. 9 *Summary delay (Ringkasan Delay)*

$$\frac{total\ paket\ yang\ di\ terima}{total\ delay}$$

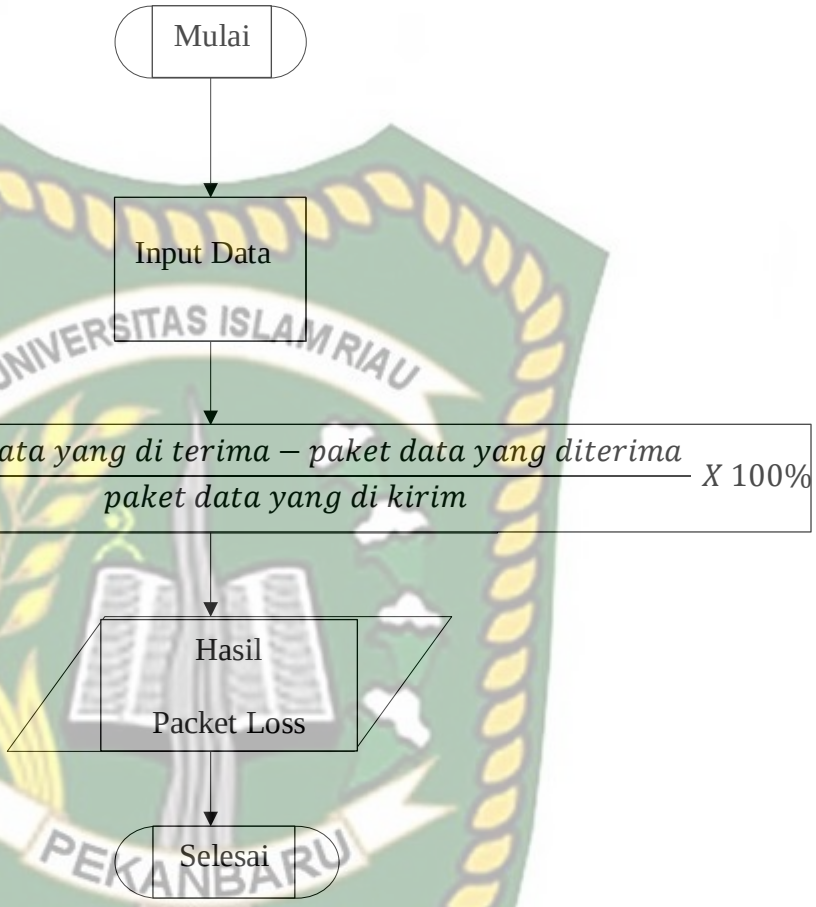
$$\frac{30.301}{227} = 133{,}4845814977974 \text{ ms}$$

=133,4845814977974 ms .

Dari percobaan diatas delay yang dihasilkan 133,4845814977974 ms dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Total paket diterima (30.301) dibagi dengan total delay (227) sama dengan hasilnya (133,4845814977974 ms).

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

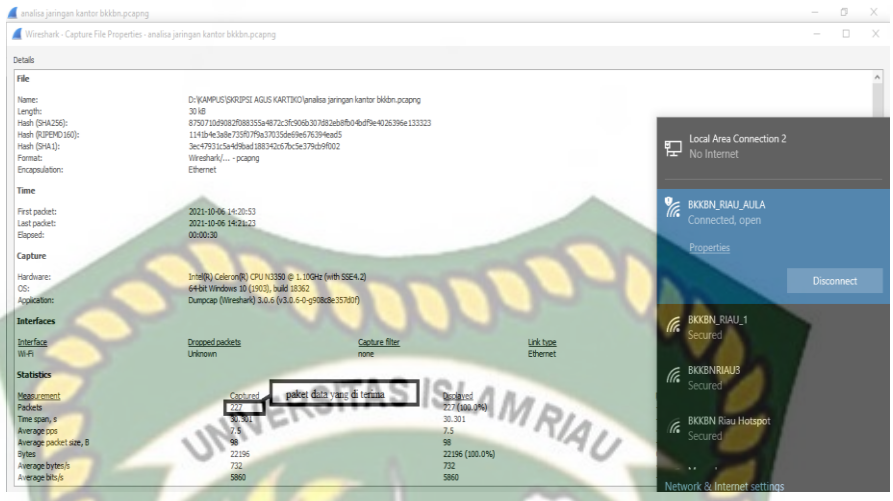
3.4.3 Menghitung *Packet Loss PPTP (*Point to Point Tunneling Protocol)



Gambar 3. 10 *Flowchart* Perhitungan *Packet Loss*

Langkah yang dilakukan untuk perhitungan *packet Loss* menggunkan apliksi *wireshark* ini adalah input data, yang mana itu adalah hasil capture jaringan melalui *wireshark*. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu (data dikirim-data diterima)/data dikirim X 100%. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 3. 11 *Summary* Paket Loss

$$\frac{(paket\ data\ yang\ dikirim - paket\ data\ yang\ deterima)}{paket\ data\ yang\ dikirim} \times 100\%$$

= (227) x 100% : 227

= 0 / Tidak ada paket yang hilang

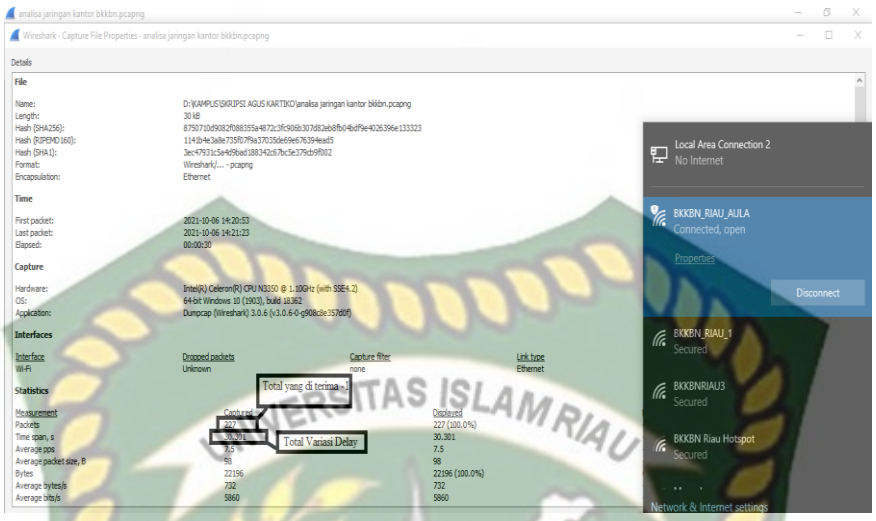
Dari percobaan diatas packet loss yang dihasilkan 0 . dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Paket data di kirim (**227**) dibagi dengan total paket yang di kirim (**227**) sama dengan hasilnya (0) karena tidak ada paket yang hilang.

3.4.4 Menghitung Jitter PPTP (Point to Point Tunneling Protocol)

Rumus Jitter, yaitu:

$$total\ variasi\ delay / total\ paket\ yang\ di\ terima - 1$$

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



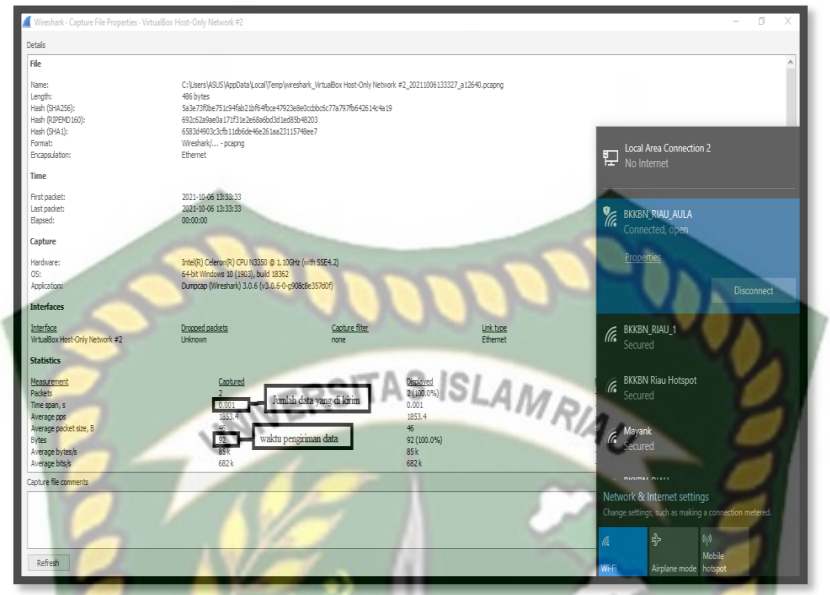
Gambar 3. 12 Menghitung Jitter

Dari percobaan diatas JITTER yang dihasilkan 134,0752212389381. dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Total variasi delay (**30.301**) dibagi dengan total paket yang di terima -1 **(227-1 menjadi 226)** sama dengan hasilnya (134,0752212389381) karena termasuk kategori jitter yaitu jelek.

3.4.5 Menghitung Througput L2TP (Layer 2 Tunneling Protocol)

Langkah yang dilakukan untuk perhitungan *Throughput* menggunkan apliksi *wireshark* ini adalah input data, yang mana itu adalah hasil capture jaringan melalui *wireshark*. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu jumlah data yang dikirim/waktu pengiriman data. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 3. 13 Througput L2TP (Layer 2 Tunneling Protocol)

Dari percobaan diatas Troughput yang dihasilkan 0,0109212471 Kbps dilihat pada table TIPHON nilai Troughput ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Jumlah data yang dikirim (0,001) dibagi dengan waktu pengiriman data (92) , Di bagi dengan 125 . sama dengan hasilnya (869.565216 Kbps).

$$\frac{Jumlah\ data\ yang\ dikirim}{waktu\ pengiriman\ data}$$

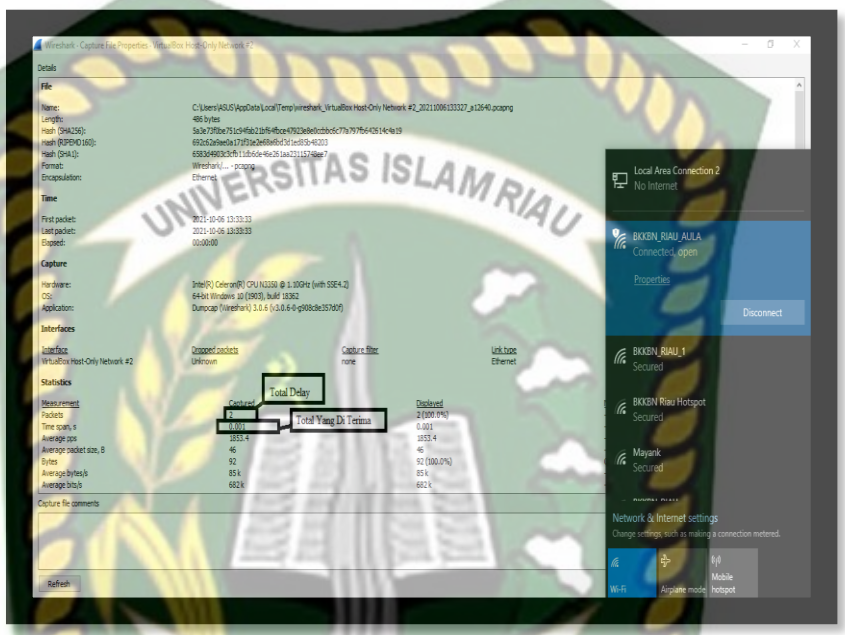
$$\frac{0.001}{92} = \frac{1{,}08695652Kbps}{125} = 869.565216 \text{ kbps}$$

3.4.6 Menghitung *Delay L2TP (*Layer 2 Tunneling Protocol)

Langkah yang dilakukan untuk perhitungan Delay menggunkan apliksi wireshark ini adalah input data, yang mana itu adalah hasil capture jaringan melalui wireshark. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

keperluan data yang diminta agar bisa dimasukan pada rumus yaitu jumlah Delay/jumlah packet receive. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.



Gambar 3. 14 Delay L2TP (Layer 2 Tunneling Protocol)

$$\frac{total\ paket\ yang\ di\ terima}{total\ delay}$$

$$\frac{0.001}{2} = 0.0005 \text{ ms}$$

Dari percobaan diatas delay yang dihasilkan 0.0005 ms dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Total paket diterima (0.001) dibagi dengan total delay (2) sama dengan hasilnya (0.0005 ms).

3.4.7 Menghitung *Packet Loss L2TP (layer 2 Tunneling Protocol)*

Langkah yang dilakukan untuk perhitungan *packet Loss* menggunkan apliksi *wireshark* ini adalah input data, yang mana itu adalah hasil capture

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

jaringan melalui *wireshark*. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu (data dikirim-data diterima)/data dikirim X 100%. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.

Gambar 3. 15 Paket Loss L2TP (Layer 2 Tunneling Protocol)

$$\frac{(paket\ data\ yang\ dikirim - paket\ data\ yang\ deterima)}{paket\ data\ yang\ dikirim} \times 100\%$$

= (2) x 100% : 2

= 0 / Tidak ada paket yang hilang

Dari percobaan diatas packet loss yang dihasilkan 0 . dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Paket data di kirim (**2**) dibagi dengan total paket yang di kirim (**2**) sama dengan hasilnya (0) karena tidak ada paket yang hilang.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.4.8 Menghitung Jitter L2TP (Layer 2 Tunneling Protocol)

Rumus Jitter, yaitu:

$$total\ variasi\ delay / total\ paket\ yang\ di\ terima - 1$$

Gambar 3. 16 Jitter L2TP

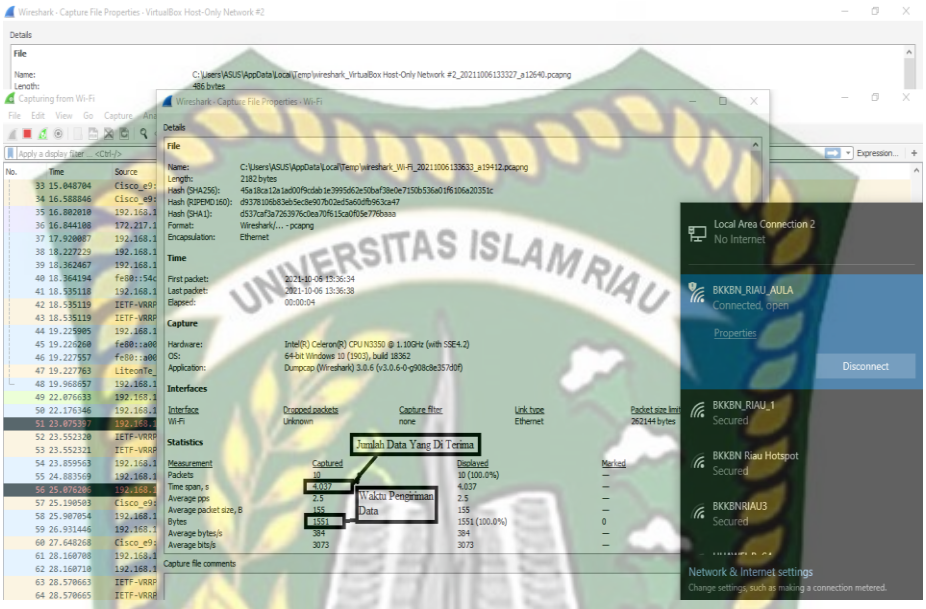
Dari percobaan diatas JITTER yang dihasilkan 0.001. dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Total variasi delay (**0.001**) dibagi dengan total paket yang di terima -1 (**2-1 menjadi 1**) sama dengan hasilnya (0.001).

3.4.9 Menghitung Througput SSTP (Secure Socket Tunneling Protokol)

Langkah yang dilakukan untuk perhitungan *Throughput* menggunkan apliksi *wireshark* ini adalah input data, yang mana itu adalah hasil capture jaringan melalui *wireshark*. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu jumlah data yang dikirim/waktu pengiriman data. Setelah hasil didapatkan lalu hasil akan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.



Gambar 3. 17 Througput SSTP (Secure Socket Tunneling Protokol)

Dari percobaan diatas Troughput yang dihasilkan 0.020822695 Kbps dilihat pada table TIPHON nilai Troughput ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Jumlah data yang dikirim (4,037) dibagi dengan waktu pengiriman data (1551) , Di bagi dengan 125 . sama dengan hasilnya (0.020822695 Kbps).

$$\frac{Jumlah\ data\ yang\ dikirim}{waktu\ pengiriman\ data}$$

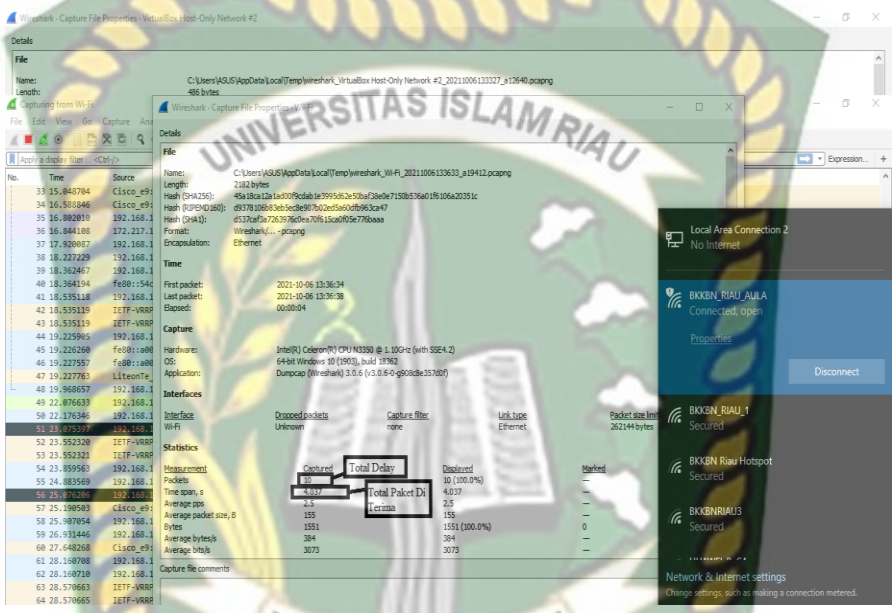
$$\frac{4{,}037}{1551} = \frac{2{,}60283688\ Kbps}{125} = 0.020822695\ \text{kbps}$$

3.10 Menghitung *Delay* SSTP (Secure Socket Tunneling Protokol)

Langkah yang dilakukan untuk perhitungan Delay menggunkan apliksi wireshark ini adalah input data, yang mana itu adalah hasil capture jaringan melalui

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

wireshark. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu jumlah Delay/jumlah packet receive. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.



Gambar 3. 18 Delay STTP (Secure Socket Tunneling Protokol)

$$\frac{total\ paket\ yang\ di\ terima}{total\ delay}$$

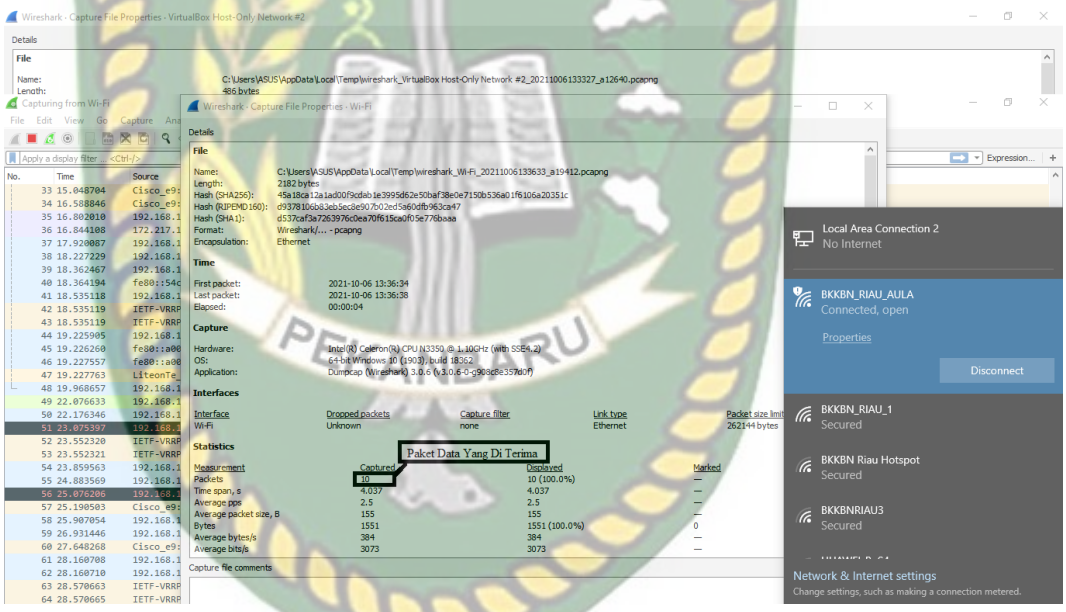
$$\frac{4.037}{10} = 403{,}7\ \text{ms}$$

Dari percobaan diatas delay yang dihasilkan 0.0005 ms dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Total paket diterima (4.037) dibagi dengan total delay (10) sama dengan hasilnya (403,7 ms).

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.11 Menghitung *Packet Loss SSTP (*Secure Socket Tunneling Protokol*)*

Langkah yang dilakukan untuk perhitungan *packet Loss* menggunkan apliksi *wireshark* ini adalah input data, yang mana itu adalah hasil capture jaringan melalui *wireshark*. Selanjutnya dilakukan filtering dari hasil tersebut untuk mendapatkan keperluan data yang diminta agar bisa dimasukan pada rumus yaitu (data dikirim-data diterima)/data dikirim X 100%. Setelah hasil didapatkan lalu hasil akan dikonversikan kedalam bentuk grafik agar mempermudah dalam proses analisis jaringan.



Gambar 3. 19 Packet Loss SSTP (Secure Socket Tunneling Protokol)

$$\frac{(paket\ data\ yang\ dikirim - paket\ data\ yang\ deterima)}{paket\ data\ yang\ dikirim} \times 100\%$$

= (10) x 100% : 10

= 0 / Tidak ada paket yang hilang

Dari percobaan diatas packet loss yang dihasilkan 0 . dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total

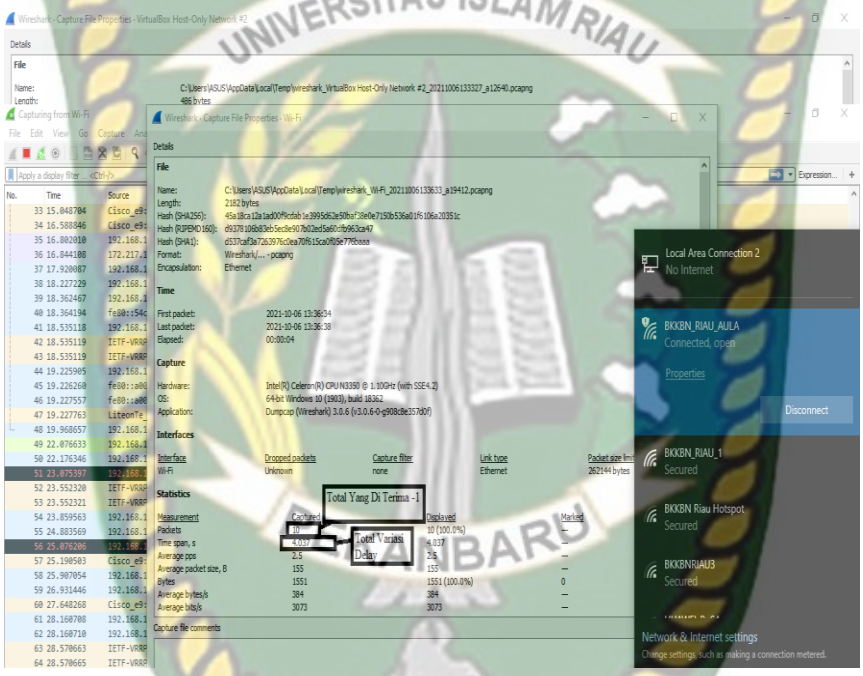
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

bandwith yang oleh ISP. Paket data di kirim (**10**) dibagi dengan total paket yang di kirim (**10**) sama dengan hasilnya (0) karena tidak ada paket yang hilang.

3.12 Menghitung Jitter *SSTP (*Secure Socket Tunneling Protokol*)*

Rumus Jitter, yaitu:

$$total\ variasi\ delay / total\ paket\ yang\ di\ terima - 1$$

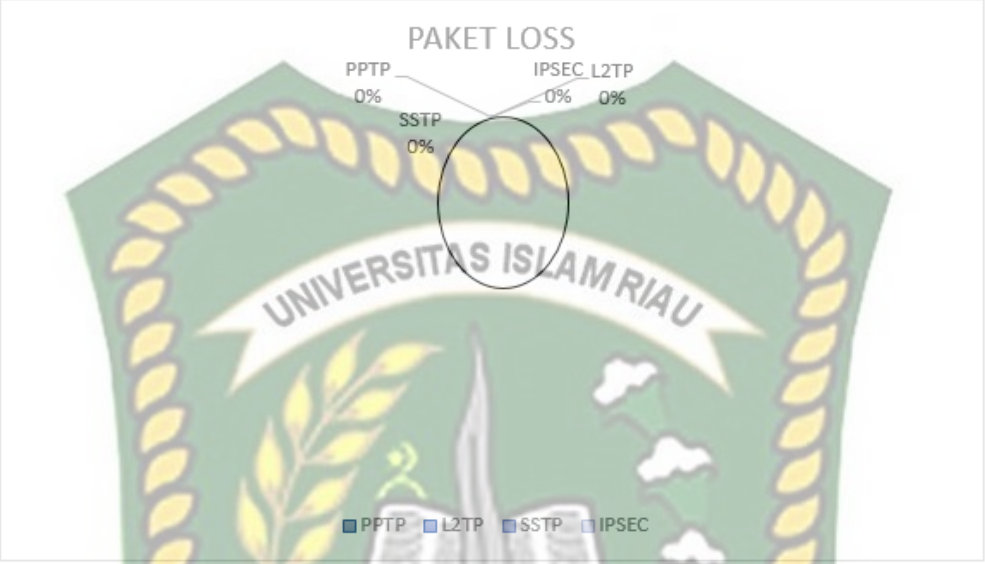


Gambar 3. 20 Jitter SSTP (Secure Socket Tunneling Protokol)

Dari percobaan diatas JITTER yang dihasilkan 478,555556 . dilihat pada table TIPHON nilai delay ikut dalam kategori sangat bagus karena 100% dari total bandwith yang oleh ISP. Total variasi delay (**4.307**) dibagi dengan total paket yang di terima -1 (**10-1 menjadi 9**) sama dengan hasilnya (478,555556).

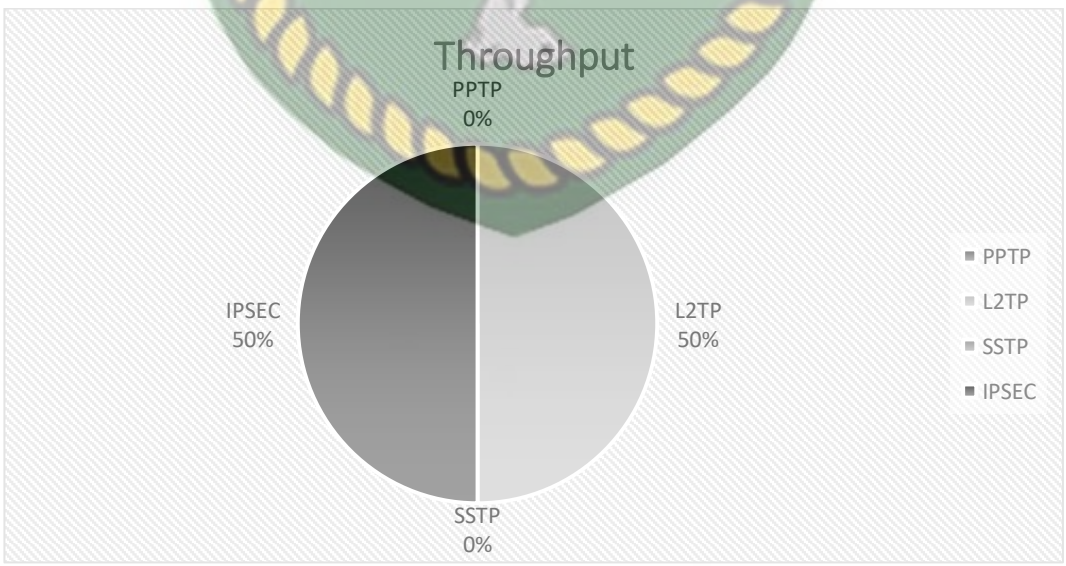
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.5 Statistik Pengaruh Jaringan VPN



Gambar 3. 21 Pengaruh Virtual Private Network (VPN)Paket Loss

Terdapat Gambar 3.21 di atas yaitu karena tidak ada paket yang hilang. Hasilnya sama sama (0% PPTP),(0%L2TP),(0%SSTP),(0% IPSEC).



Gambar 3. 22 Pengaruh VPN Throughput

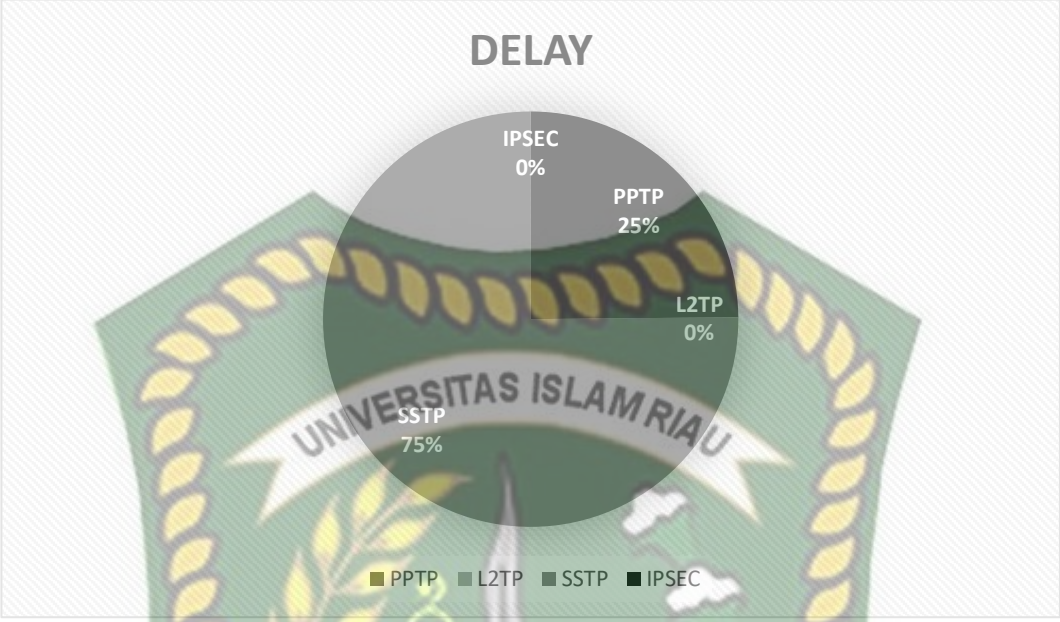
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Terdapat Gambar 3.22 di atas yaitu (PPTP 0%) , (L2TP 50%), (SSTP 0%), (IPSEC 50%). Dari hasil pengukuran dan analisis menunjukkan bahwa kualitas jaringan dipengaruhi karena adanya interferensi. interaksi antar gelombang di dalam suatu daerah. Interferensi dapat bersifat membangun dan merusak.

Gambar 3. 23 Pengaruh VPN JITTER

Terdapat Gambar 3.23 di atas yaitu (PPTP 74%) , (L2TP 0%), (SSTP 26%), (IPSEC 0%). Dari hasil pengukuran dan analisis menunjukkan bahwa kualitas jaringan dipengaruhi karena adanya interferensi. interaksi antar gelombang di dalam suatu daerah. Interferensi dapat bersifat membangun dan merusak.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 3. 24 Pengaruh VPN Delay

Terdapat Gambar 3.24 di atas yaitu (PPTP 25%) , (L2TP 0%), (SSTP 75%), (IPSEC 0%). Dari hasil pengukuran dan analisis menunjukkan bahwa kualitas jaringan dipengaruhi karena adanya interferensi. interaksi antar gelombang di dalam suatu daerah. Interferensi dapat bersifat membangun dan merusak.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

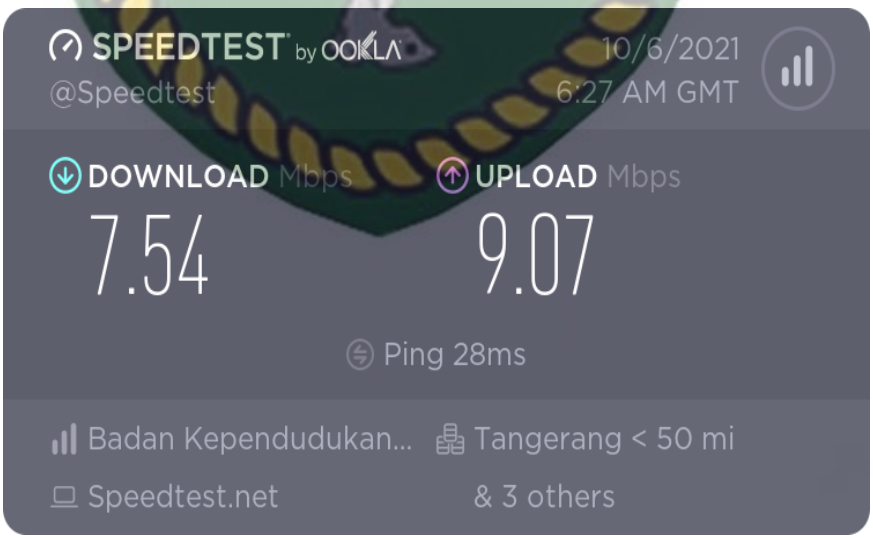
BAB IV

HASIL DAN PEMBAHASAN

4.1 Pengujian

Pada penelitian ini di mulai dari menyambungkan kabel LAN di port 1 Router Board Mikrotik dan kemudian melakukan konfigurasi hostpot untuk melakukan pengujian. Pengujian ini dilakukan menggunakan management bandwidth dengan dua skema yaitu, skema Download dan Upload.

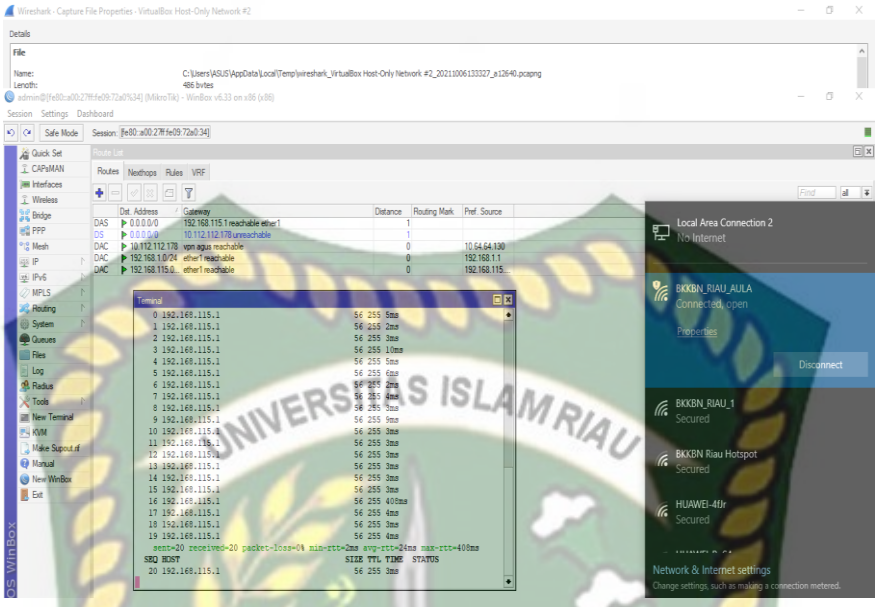
Sebelum melakukan uji QoS dengan aplikasi Wireshark, pengujian ini menggunakan bantuan dari situs Speedtest untuk mengukur besar nilai unduh dan unggah sesaat sebelum melakukan uji QoS. Data QoS diambil pada setiap PC client yang terhubung pada server yang sudah diinstalkan aplikasi wireshark. Adapun hasil dari Speed Test dapat dilihat pada Gambar 4.1



Gambar 4 1 Hasil SpeedTes Di Kantor BKKBN PEKANBARU

Jumlah perangkat yang terhubung pada access point ditunjukkan oleh Gambar 4.2.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4 2 Jumlah IP Address Perangkat Terhubung pada Access Point

1. Perhitungan Delay PPTP

Perhitungan delay PPTP berdasarkan persamaan dari pengujian data QoS yang dilakukan pada PC 1 yaitu :

$$\frac{30.301}{227} = 133{,}4845814977974 \text{ ms}$$

Summary Data QoS pada PC 1 *ditunjukkan* oleh Gambar 4.3

Gambar 4 3 *Summary* Data QoS pada PC 1

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

2. Perhitungan *Packet Loss*

Berdasarkan Gambar 4.3, perhitungan *packet loss* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari *PPTP* PC 1 yaitu :

= (227) x 100% : 227

= 0 / Tidak ada paket yang hilang

3. Perhitungan *Throughput*

Berdasarkan Gambar 4.3, perhitungan *throughput* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC1 yaitu :

$$\frac{30.301}{22196} = \frac{1{,}365155883 Kbps}{125} = 0{,}0109212471 \text{ kbps}$$

4. Perhitungan Jitter

Berdasarkan Gambar 4.3, perhitungan *Jitter* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC1 yaitu :

$$\frac{30.301}{226} = 134{,}0752212389381$$

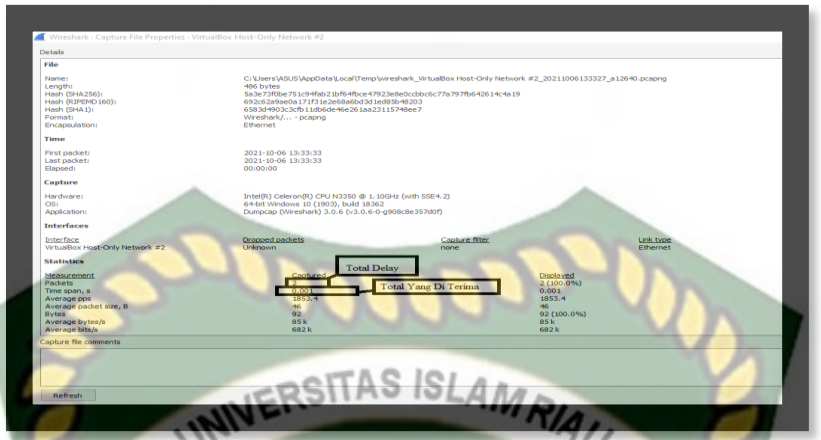
5. Perhitungan Delay L2TP

Perhitungan delay L2TP berdasarkan persamaan dari pengujian data QoS yang dilakukan pada PC 2 yaitu :

$$\frac{0.001}{2} = 0.0005 \text{ ms}$$

Summary Data QoS pada PC 1 *ditunjukkan* oleh Gambar 4.4

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4 4 *Summary* Data QoS pada PC 2

6. Perhitungan *Packet Loss*

Berdasarkan Gambar 4.4, perhitungan *packet loss* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari *PPTP* PC 2 yaitu :

= (2) x 100% : 2

= 0 / Tidak ada paket yang hilang

7. Perhitungan *Throughput*

Berdasarkan Gambar 4.4, perhitungan *throughput* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC 2 yaitu :

$$\frac{0.001}{92} = \frac{1{,}086956525Kbps}{125} = 869.565216 \text{ kbps}$$

8. Perhitungan Jitter

Berdasarkan Gambar 4.4, perhitungan *Jitter* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC 2 yaitu :

$$\frac{0.001}{1} = 0.001 \text{ MS}$$

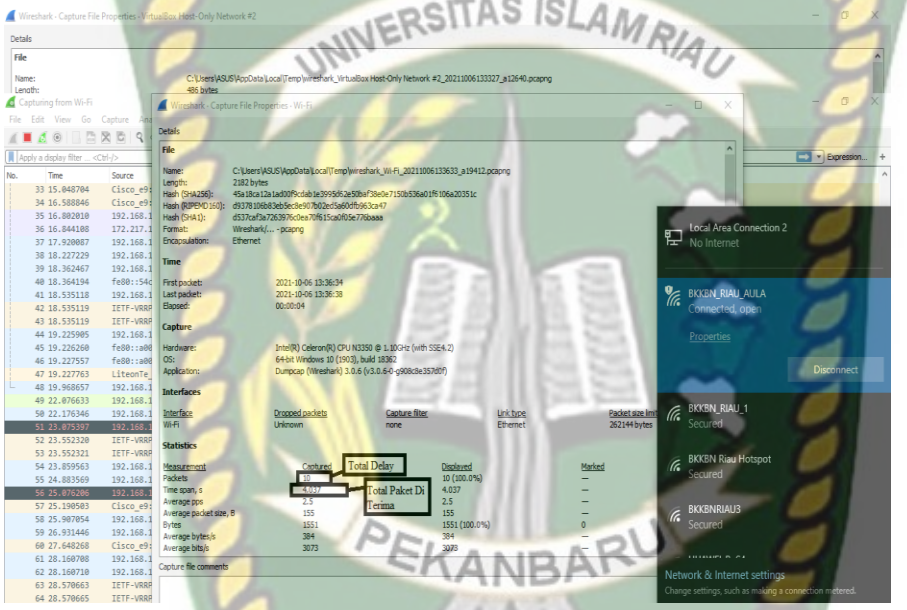
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

9. Perhitungan Delay SSTP

Perhitungan delay SSTP berdasarkan persamaan dari pengujian data QoS yang dilakukan pada PC 3 yaitu :

$$\frac{4.037}{10} = 403{,}7 \text{ ms}$$

Summary Data QoS pada PC 3 *ditunjukkan* oleh Gambar 4.5



Gambar 4 5 Sumary Delay QOS PC 3

10. Perhitungan *Packet Loss*

Berdasarkan Gambar 4.5, perhitungan *packet loss* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari *SSTP* PC 3 yaitu :

= (10) x 100% : 10

= 0 / Tidak ada paket yang hilang

11. Perhitungan *Throughput*

Berdasarkan Gambar 4.5, perhitungan *throughput* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC 3 yaitu :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

$$\frac{4{,}037}{1551} = \frac{2{,}60283688\ Kbps}{125} = 0.020822695 \text{ kbps}$$

12. Perhitungan Jitter

Berdasarkan Gambar 4.5, perhitungan *Jitter* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC 3 yaitu :

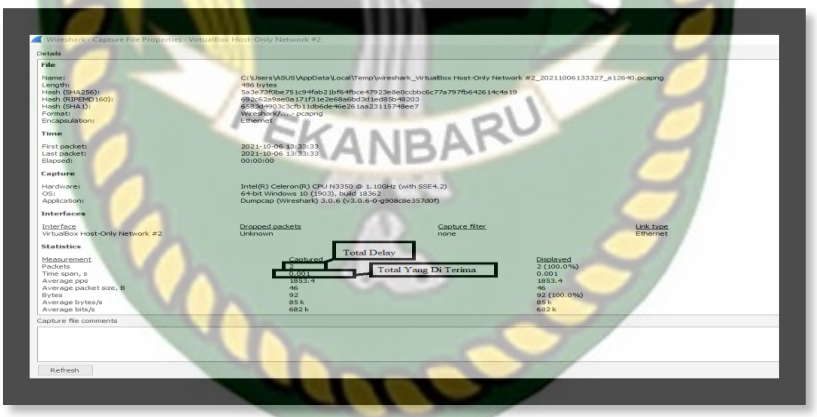
$$\frac{4.307}{9} = 478{,}555556 \text{ ms}$$

13.Perhitungan Delay IPSEC

Perhitungan delay L2TP berdasarkan persamaan dari pengujian data QoS yang dilakukan pada PC 2 yaitu :

$$\frac{0.001}{2} = 0.0005 \text{ ms}$$

Summary Data QoS pada PC 1 *ditunjukkan* oleh Gambar 4.6



Gambar 4 6 *Summary* Data QoS pada PC 4

14. Perhitungan *Packet Loss*

Berdasarkan Gambar 4.6, perhitungan *packet loss* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari *PPTP* PC 2 yaitu :

= (2) x 100% : 2

= 0 / Tidak ada paket yang hilang

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

15. Perhitungan *Throughput*

Berdasarkan Gambar 4.6, perhitungan *throughput* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC 4 yaitu :

$$\frac{0.001}{92} = \frac{1{,}08695652 Kbps}{125} = 869.565216 \text{ kbps}$$

16. Perhitungan Jitter

Berdasarkan Gambar 4.6, perhitungan *Jitter* berdasarkan Persamaan dari pengujian data QoS yang dilakukan yang diambil dari PC 4 yaitu :

$$\frac{0.001}{1} = 0.001 \text{ ms}$$

4.2 Hasil Pengujian

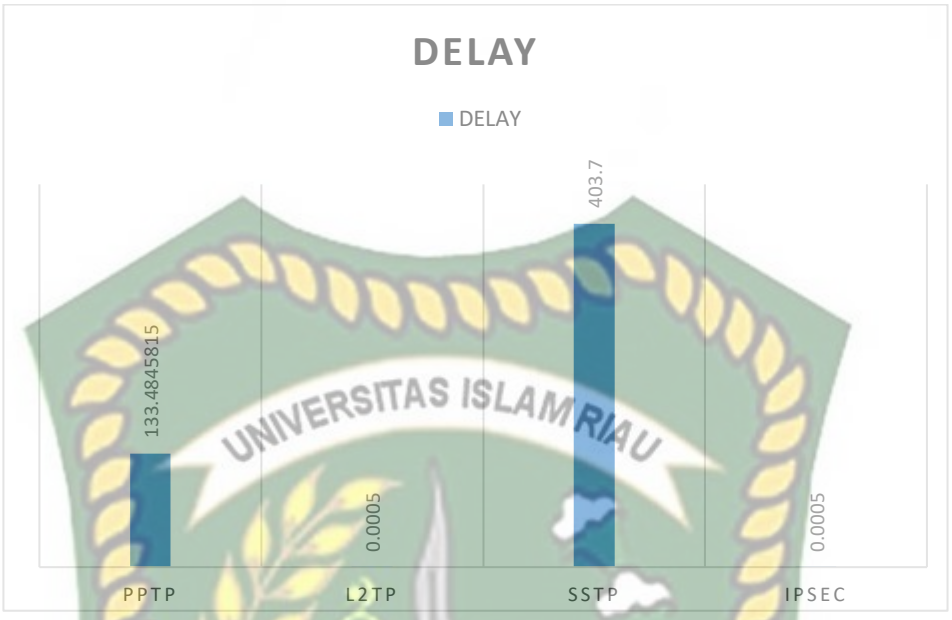
Metode Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protokol (L2TP), Secure Socket Tunneling Protocol (SSTP) dan Internet Protokol Security (IPSec)

Berdasarkan hasil uji QoS dengan metode PPTP, L2TP, SSTP dan IPSec maka dapat dibuatkan tabel yang membandingkan nilai delay antara metode PPTP, L2TP, SSTP dan IPSec dari tiap-tiap kondisi.

Tabel 4.1 Rata-Rata Nilai *Delay* Metode PPTP,L2TP, SSTP dan IPSec

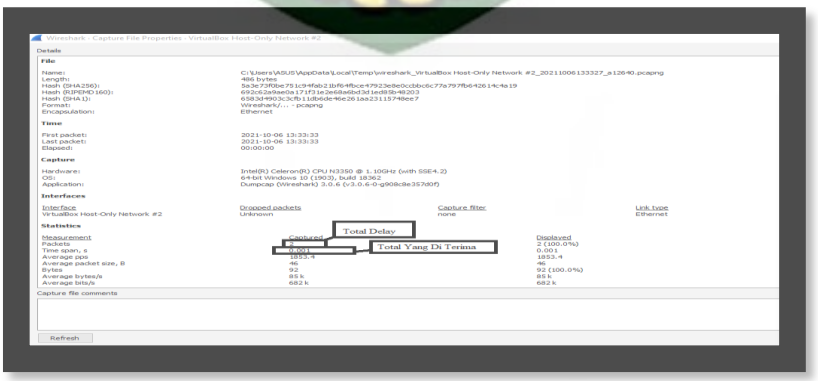
METODE	DELAY
PPTP	**133,4845814977974**
L2TP	**0,0005**
SSTP	**403,7**
IPSEC	**0,0005**

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



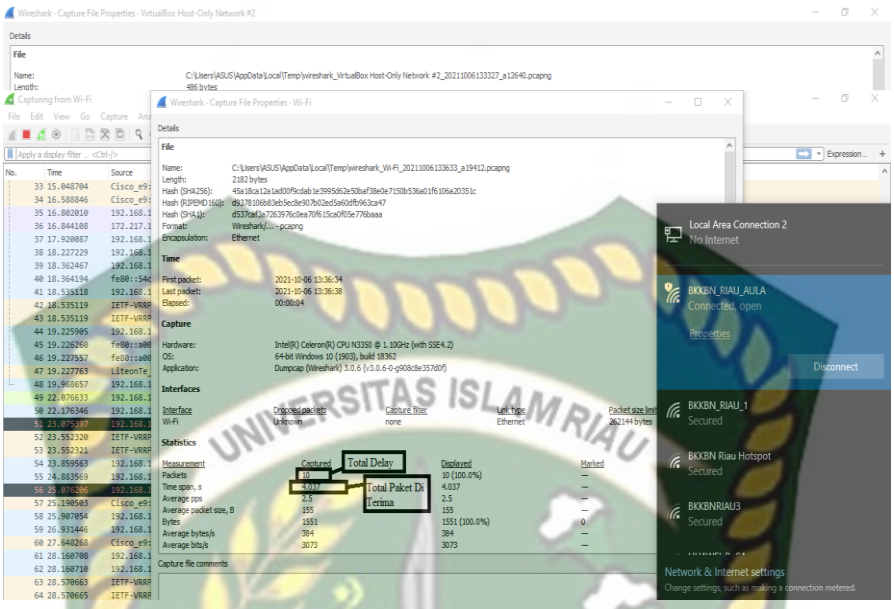
Gambar 4 7 Grafik Rata-Rata Nilai Delay Metode PPTP, L2TP, SSTP dan IPSec

Gambar 4 8 Capture Wireshark Delay PPTP

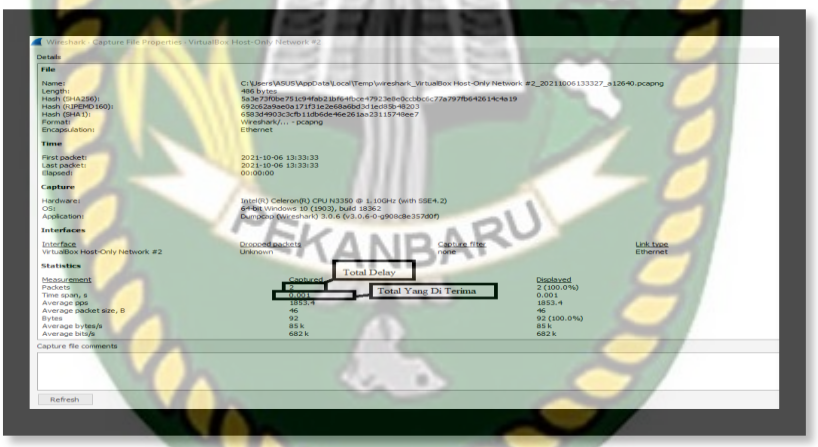


Gambar 4 9 Capture Wireshark Delay L2TP

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4 10 Capture Wireshark Delay SSTP



Gambar 4 11 Capture Wireshark Delay IPSEC

Berdasarkan Tabel 4.1 dan Gambar 4.4 menunjukkan perbandingan QoS dari parameter delay pada empat kondisi pengujian, dimana delay pada 4 metode dengan kondisi menunjukkan perbedaan yang cukup signifikan yakni pada metode PPTP dan SSTP lebih baik dibandingkan dari metode L2TP dan IPSEC.

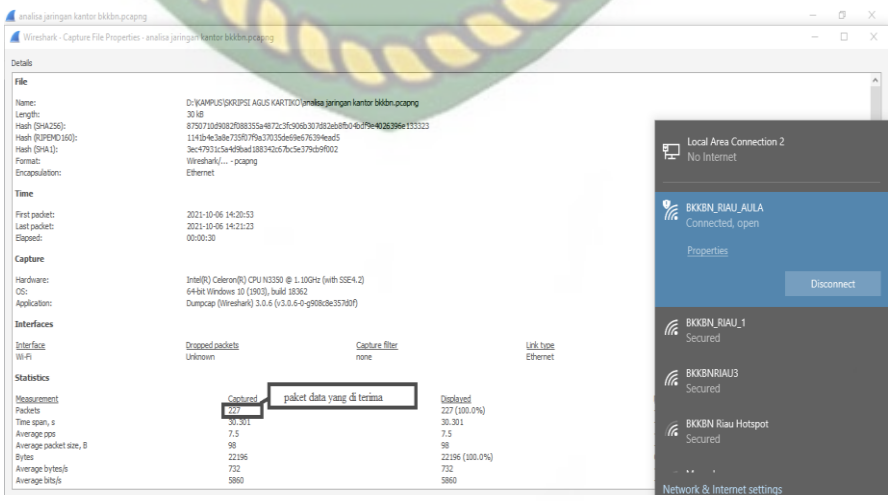
Grafik dan Tabel Rata-Rata Nilai Paket Loss Metode PPTP, L2TP, SSTP dan IPSec secara bertutut-turut ditunjukkan oleh Gambar 4.5 dan Tabel 4.2

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Gambar 4 12 Grafik Rata-Rata Nilai Paket Loss Metode PPTP, L2TP, SSTP dan IPSec

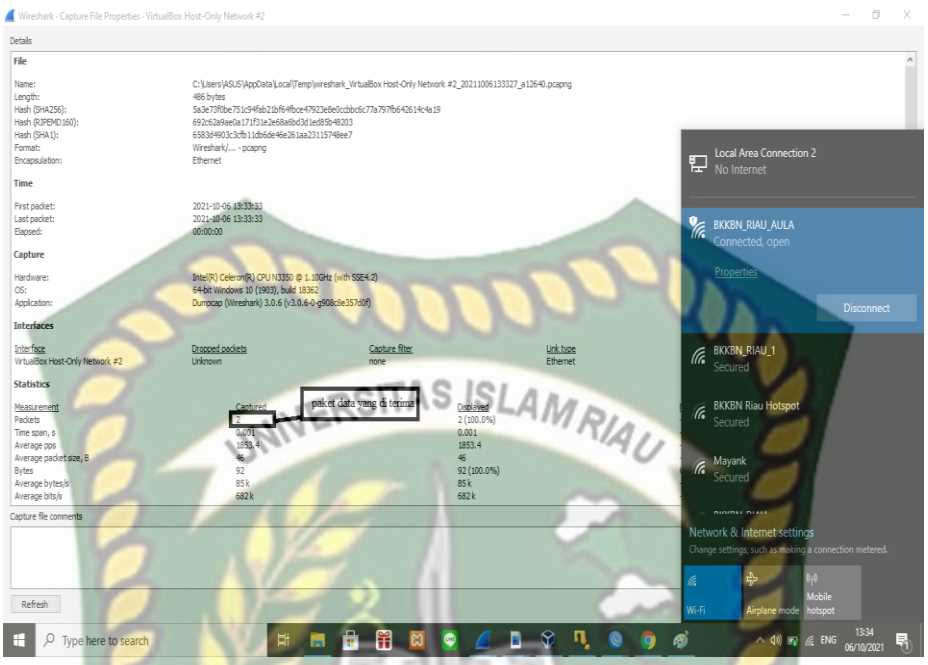
Tabel 4.2 Rata-Rata Nilai Paket Loss Metode PPTP, L2TP, SSTP dan IPSec

METODE	PAKET LOSS
PPTP	0
L2TP	0
SSTP	0
IPSEC	0

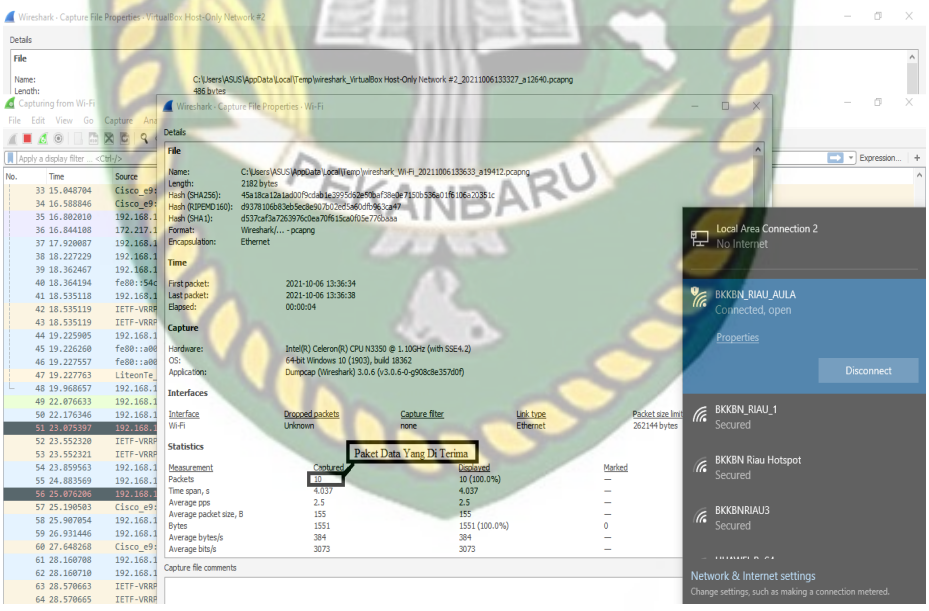


Gambar 4 13 Capture Wireshark Packet Loss PPTP

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

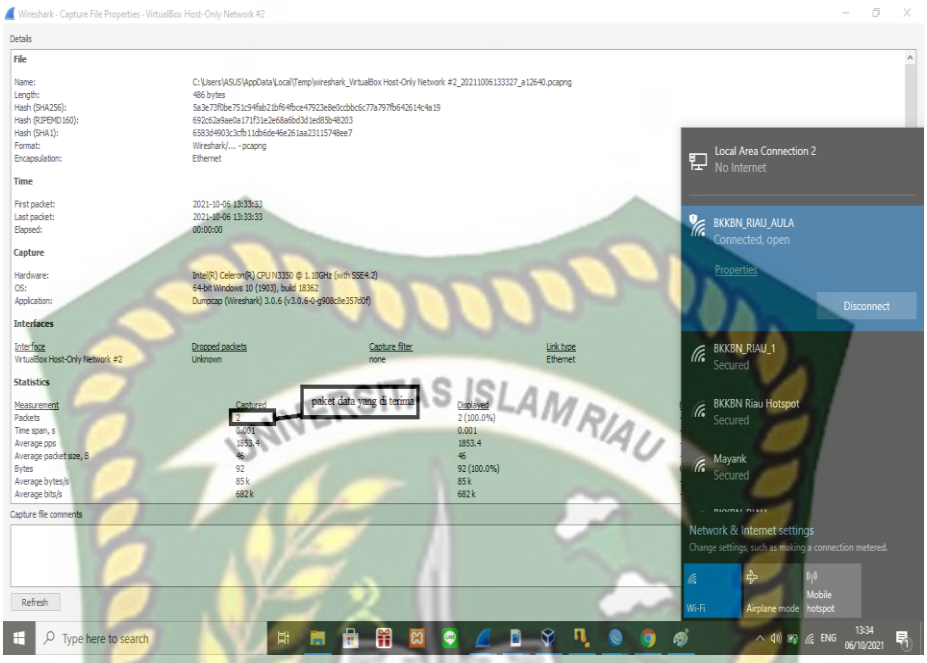


Gambar 4 14 Capture Wireshark Packet Loss L2TP



Gambar 4 15 Capture Wireshark Packet Loss SSTP

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4 16 Capture Wireshark Packet Loss IPSEC

Berdasarkan Tabel 4.2 dan Gambar 4.5 menunjukkan pebandingan QoS dari parameter paket loss pada empat kondisi pengujian, dimana paket loss pada 4 metode dengan kondisi menunjukkan hasilnya sama sama 0 yakni metode PPTP,L2TP,SSTP,IPSEC .

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

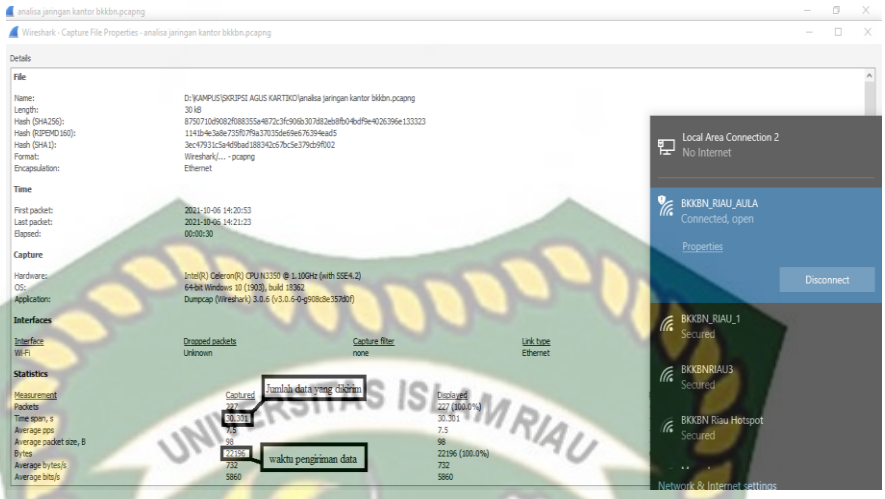
Tabel dan Grafik Rata-Rata Nilai Throughput Metode PPTP, L2TP, SSTP dan IPSec secara bertutut-turut ditunjukkan oleh Tabel 4.3 dan Gambar 4.6.

Gambar 4 17 Grafik Rata-Rata Nilai Throughput Metode PPTP, L2TP, SSTP dan IPSec

Tabel 4.3 Rata-Rata Nilai Throughput Metode PPTP, L2TP, SSTP dan IPSec

METODE	THROUGPUT
PPTP	0,0109212471
L2TP	869,565216
SSTP	0,020822695
IPSEC	869,565216

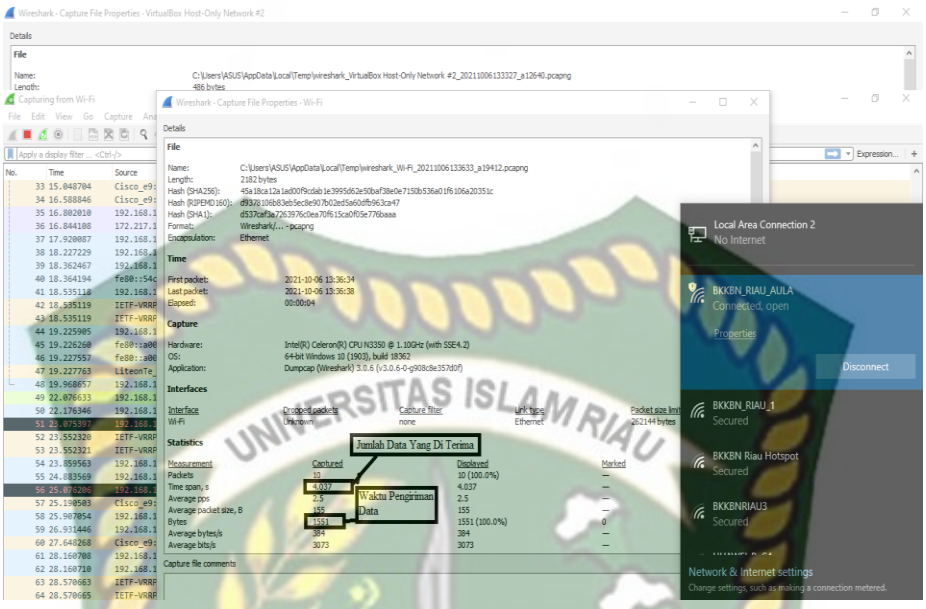
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



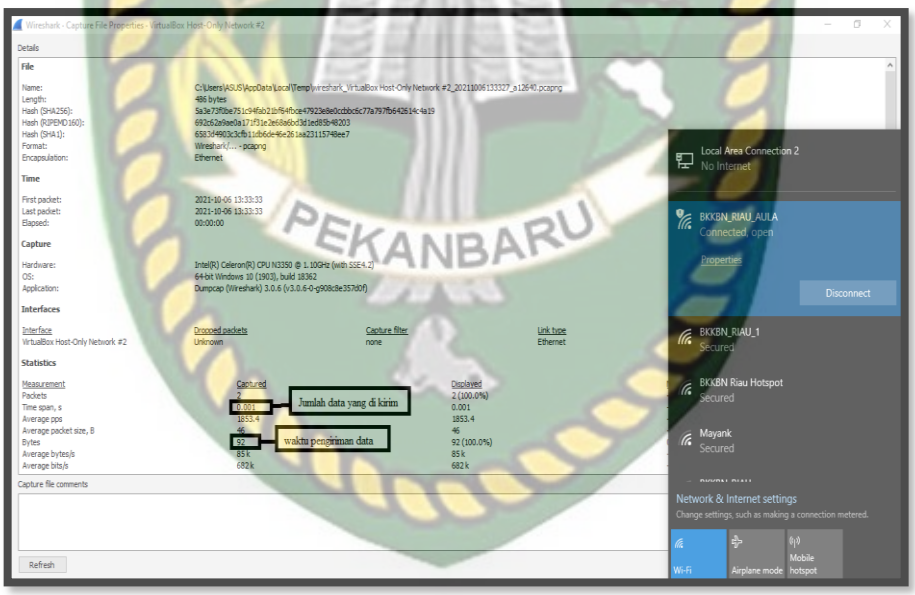
Gambar 4 18 Capture Wireshark Througphut PPTP

Gambar 4 19 Capture Wireshark Througphut L2TP

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4 20 Capture Wireshark Througphut SSTP

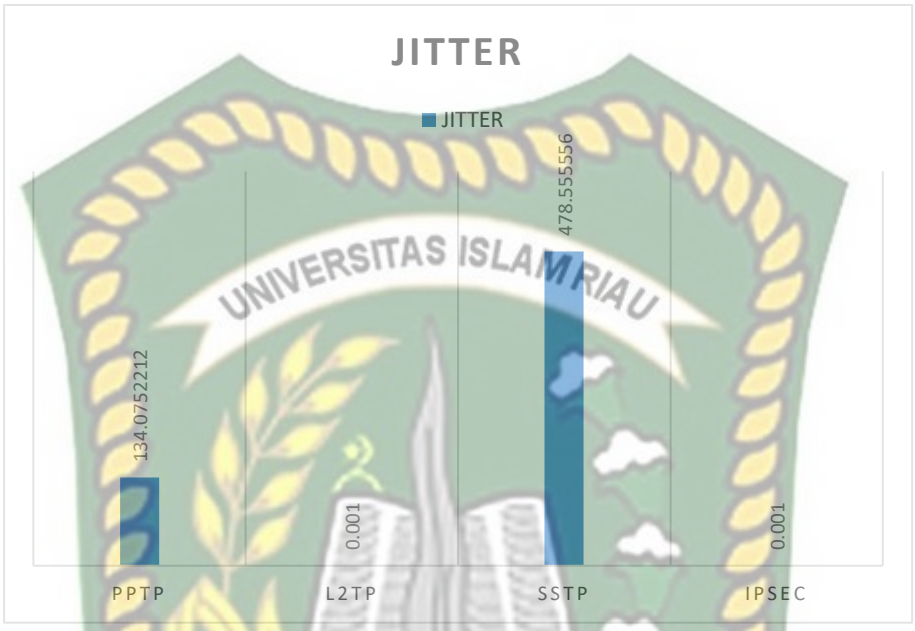


Gambar 4 21 Capture Wireshark Througphut IPSEC

Dari Tabel 4.3 dan Gambar 4.6 menunjukkan perbandingan QoS dari parameter throughput pada empat kondisi pengujian, dimana throughput pada 4 metode dengan kondisi menunjukan perbedaan yang cukup signifikan yakni pada metode L2TP dan IPSEC , lebih baik dibandingkan dari metode PPTP dan SSTP.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

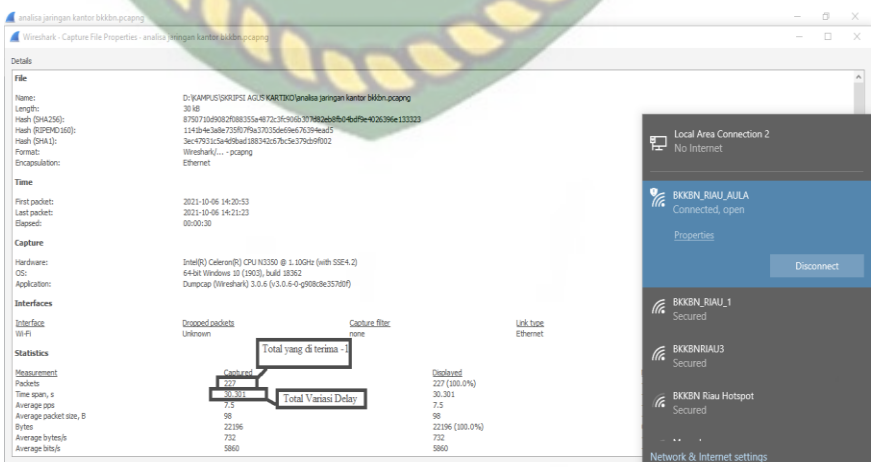
Tabel dan Grafik Rata-Rata Nilai Jitter Metode PPTP, L2TP, SSTP dan IPSec secara bertutut-turut ditunjukkan oleh Tabel 4.4 dan Gambar 4.7.



Gambar 4 22 Grafik Rata rata Jitter Metode PPTP,L2TP,SSTP,IPSEC

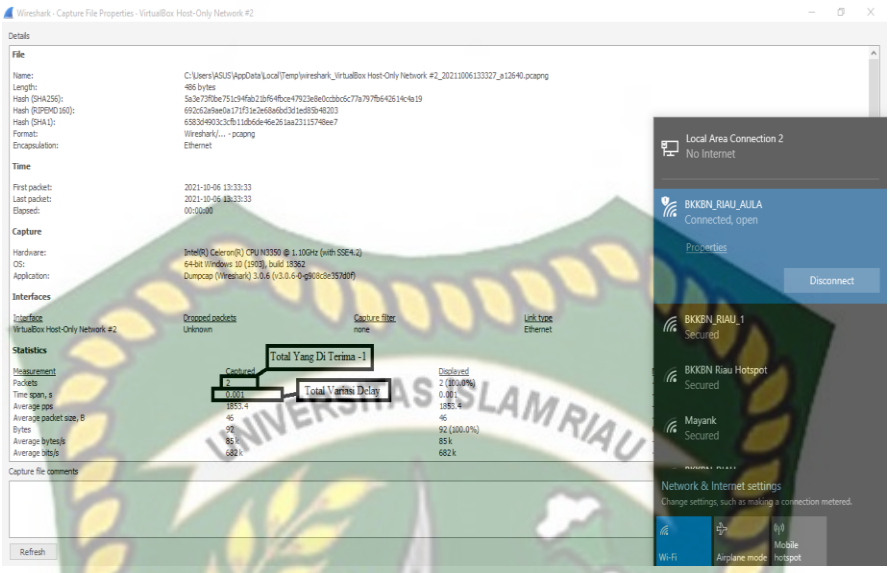
Tabel 4.4 Rata-Rata Nilai Throughput Metode PPTP, L2TP, SSTP dan IPSec

METODE	JITTER
PPTP	134,075221238981
L2TP	0,001
SSTP	478,555556
IPSEC	0,001

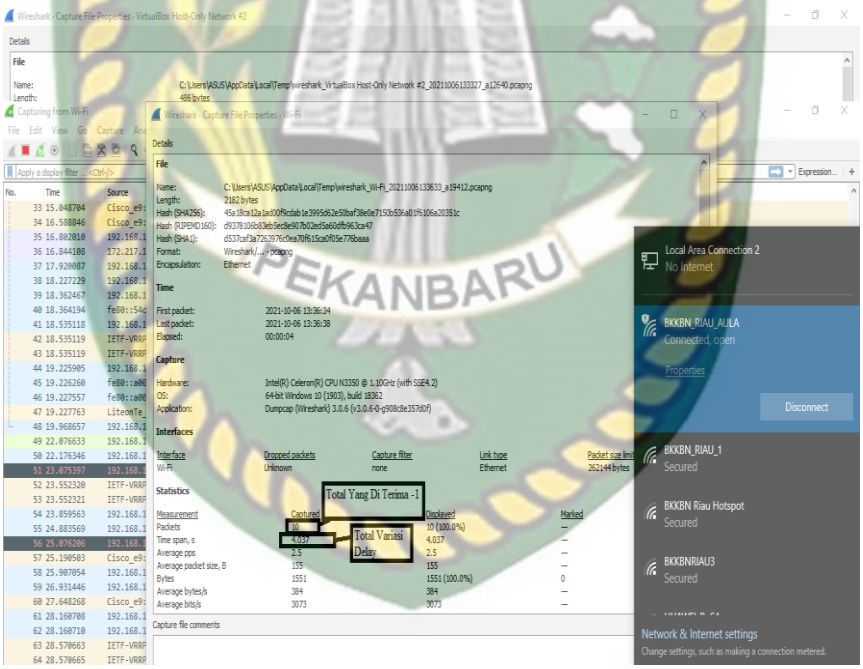


Gambar 4 23 Capture Wireshark Jitter PPTP

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

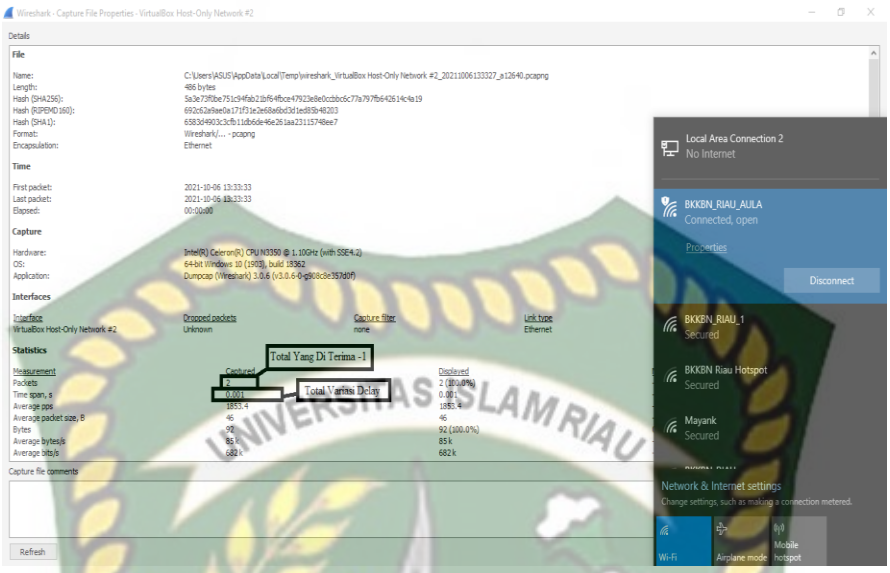


Gambar 4 24 Capture Wireshark Jitter L2TP



Gambar 4 25 Capture Wireshark Jitter SSTP

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



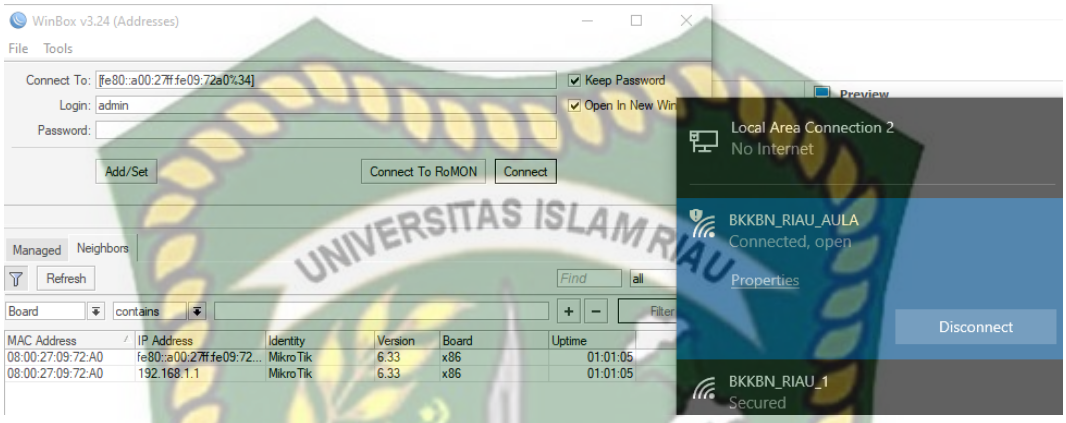
Gambar 4 26 Capture Wireshark Jitter IPSEC

Dari Tabel 4.4 dan Gambar 4.7 menunjukkan perbandingan QoS dari parameter throughput pada empat kondisi pengujian, dimana throughput pada 4 metode dengan kondisi menunjukan perbedaan yang cukup signifikan yakni pada metode SSTP, lebih baik dibandingkan dari metode PPTP,L2TP,dan IPSEC.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4.3 Hasil Analisis Mikrotik Di Kantor BKKBN

4.3.1 Winbox Mikrotik Kantor BKKBN



Gambar 4 27 Mikrotik Di Kantor BKKBN PEKANBARU

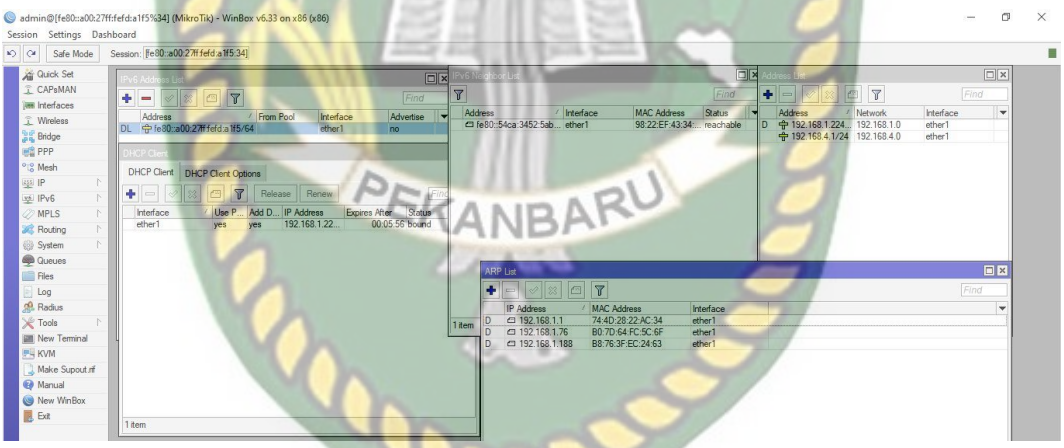
MikroTik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless, cocok digunakan oleh ISP, provider hotspot, & warnet.Menurut (Ardhitya, 2017)Pengertian dan Penjelasan Mikrotik. *Ilmu Komputer.Com*, *1*(1), 1–4. sistem operasi yang berbasis perangkat lunak (software) yang dipergunakan untuk menjadikan komputer sebagai router sebuah jaringan. Mikrotik juga menggunakan sistem operasi berbasis Linux dan menjadi dasar network router. Sistem operasi (OS) ini sangat cocok untuk membangun administrasi jaringan komputer yang berskala kecil hingga besar.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4.3.2 WiFi Kantor BKKBN Pekanbaru

Gambar 4 28 WiFi Di Kantor BKKBN Pekanbaru

4.3.3 ARP (Address Resolution Protocol) Di Mikrotik



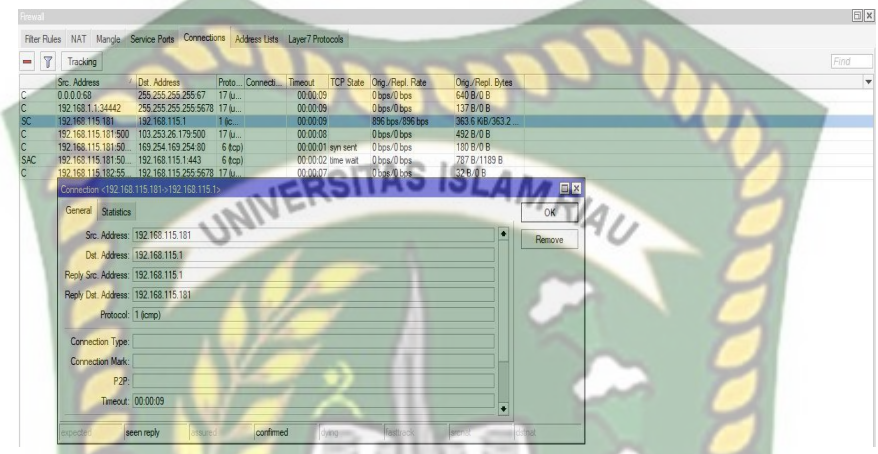
Gambar 4 29 ARP Mikrotik

Sebuah protokol dalam TCP/IP Protocol Suite yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address). menggabungkan 2 buah layer yakni layer 2 (Mac Address) dan layer 3 (IP Address) pada masing-masing client yang akses ke jaringan komputer milik kita dengan maksud untuk mencocokan kedua layer tersebut, jika ada 1 buah layer ada yang tidak sesuai maka client tersebut tidak akan bisa terhubung ke jaringan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

tersebut. mencocokan IP Address dan MAC Address pada setiap client yang terhubung ke jaringan, jika salah satu nya tidak sesuai maka client tersebut .

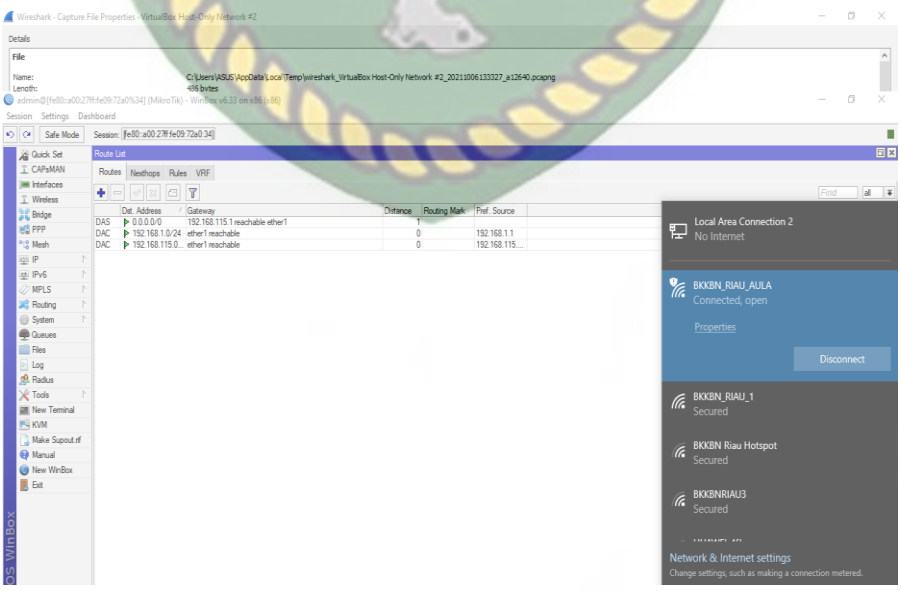
4.3.4 Firewall Di Mikrotik



Gambar 4 30 Firewall Di Mikrotik

Untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan menentukan apakah paket data bisa masuk dan keluar dari suatu jaringan.Menurut (Santoso, 2020).

4.3.5 Route List



Gambar 4 31 Route List

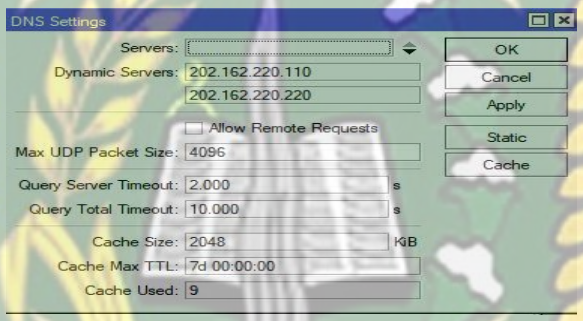
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Penulis akan menjelaskan pada gambar diatas terdapat DAS dan DAC sebagai berikut :

DAS: Dynamic Active Static, suatu routing bersifat static yang dibuat secara dynamic atau otomatis .

DAC: Dynamic Active Connect, konfigurasi terhubung yang dibuat secara otomatis.

4.3.6 DNS (Domain Name System)

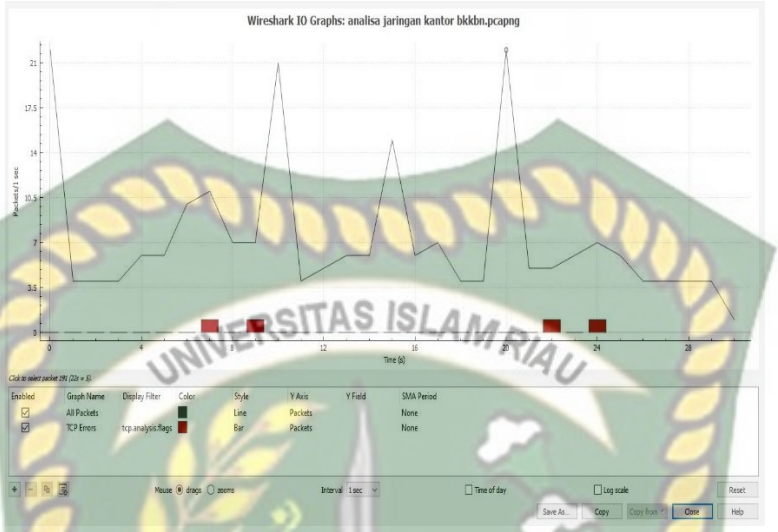


Gambar 4 32 DNS

Sebuah sistem yang bertugas menyimpan semua informasi data domain dalam jaringan. Dengan menurut (Rahman & Nurdin, 2020) adanya **DNS**, domain atau hostname yang ada akan ditranslate dan diterjemahkan dalam alamat **IP** sehingga dapat diakses.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4.3.7 Wireshark Grafik



Gambar 4 33 Wireshark Grafik

Grafik disimpan di profil saat ini.menurut (Rosa, 2018) Dibagi menjadi interval waktu, yang dapat diatur seperti yang dijelaskan di bawah ini. Mengklik pada grafik akan membawa Anda ke paket terkait dalam daftar paket. Grafik individu dapat dikonfigurasi menggunakan opsi berikut:

Enabled : Gambar atau jangan gambar grafik ini.

Graph Name : Nama grafik ini.

Display Filter : Membatasi grafik ke paket yang cocok dengan filter ini.

Color : Warna yang digunakan untuk memplot garis, batang, atau titik grafik.

Style : Cara merepresentasikan data grafik secara visual, misalnya dengan menggambar garis, batang, lingkaran.

Sumbu Y : Nilai yang akan digunakan untuk sumbu Y grafik. Dapat menjadi salah satu dari: **Paket, Byte, atau Bit :** Jumlah total paket, byte paket, atau bit paket

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

yang cocok dengan filter tampilan grafik per interval. Nilai nol dihilangkan dalam beberapa kasus.

SUM(Bidang Y) : Jumlah nilai bidang yang ditentukan dalam "Bidang Y" per interval.

JUMLAH BINGKAI (Bidang Y): Jumlah bingkai yang berisi bidang yang ditentukan dalam "Bidang Y" per interval. Tidak seperti grafik "Paket" biasa, grafik ini selalu menampilkan nilai nol .

JUMLAH BIDANG (Bidang Y): Jumlah instance bidang yang ditentukan dalam "Bidang Y" per interval. Beberapa bidang, seperti dns.resp.name , dapat muncul beberapa kali dalam sebuah paket.

MAX(Bidang Y), MIN(Bidang Y), AVG(Bidang Y) : Nilai rata-rata maksimum, minimum, dan aritmatika dari "Bidang Y" yang ditentukan per interval. Untuk nilai MAX dan MIN, mengarahkan dan mengklik grafik akan menampilkan dan membawa Anda ke paket dengan nilai MAX atau MIN dalam interval alih-alih paket terbaru.

BEBAN (Bidang Y): Jika "Bidang Y" adalah nilai waktu relatif, ini adalah jumlah dari nilai "Bidang Y" dibagi dengan waktu interval. Ini dapat berguna untuk melacak waktu respons.

Bidang Y: Bidang filter tampilan tempat mengekstrak nilai untuk penghitungan sumbu Y yang tercantum di atas.

Masa SMA : Tampilkan rata-rata nilai selama periode interval tertentu.

Mouse drags / zooms : Saat menggunakan mouse di dalam area grafik, seret konten grafik atau pilih area zoom.

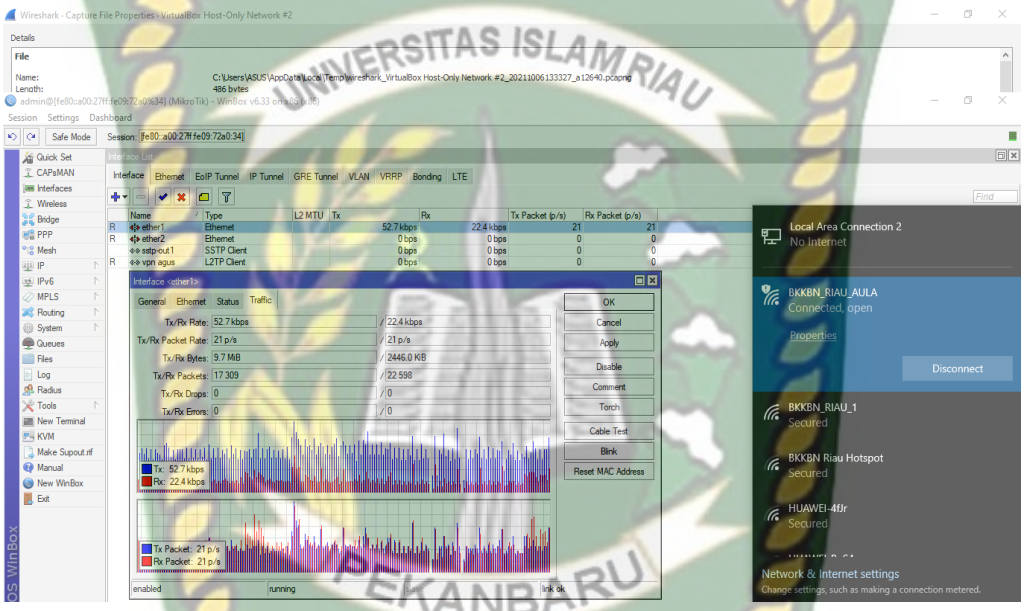
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Interval : Tetapkan periode interval untuk grafik.

Time of day (Waktu hari) : Beralih antara menampilkan waktu absolut dalam sehari atau waktu relatif dari awal pengambilan di sumbu X.

Log scale (Skala log) : Beralih di antara sumbu Y logaritmik atau linier.

4.3.8 Traffik Di Winbox Mikrotik



Gambar 4 34 Data Traffik Mikrotik

Traffic monitor ini dapat digunakan untuk memonitoring traffic yang berjalan di sebuah interface pada router. Di dalamnya dapat menentukan sebuah nilai ambang batas traffic. Jika traffic sudah mencapai ambang batas yang ditentukan, maka Traffic Monitor dapat mengeksekusi sebuah script. Dengan demikian sebenarnya kita dapat menggunakan fitur ini untuk berbagai kebutuhan, yakni dengan menentukan script apa yang akan dieksekusi menurut (Supendar & Handrianto, 2017)

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan analisis perbandingan *QOS (Quality Of Service)* semua client dengan menggunakan metode Point to Point Tunneling protocol (PPTP), Layer 2 Tunneling Protokol (L2TP), Secure Socket Tunneling protocol (SSTP) dan Internet Protokol Security (IPSec), maka dapat disimpulkan bahwa untuk pengujian Delay terbaik dihasilkan pada metode SSTP, Packet loss terbaik dihasilnya semua sama sama nol, maka dapat disimpulkan bahwa untuk pengujian Througput terbaik di hasilkan oleh metode *L2TP* dan *IPSEC*, Sedangkan Jitter maka terbaik dihasilkan pada metode PPTP dan SSTP.

5.2 Saran

Hasil penelitian ini, Penulis berharap dapat dijadikan suatu patokan untuk lebih mengembangkan performansi jaringan VPN. Masih banyak yang perlu dianalisa dalam jaringan VPN khusunya metode PPTP, L2TP, SSTP dan IPSec, baik dari sisi keamanan keempat metode tersebut, banyaknya client yang melakukan proses transmisi data, dan lain sebagainya yang mempengaruhi performansi jaringan VPN.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR PUSTAKA

Ardhitya, A. I. (2017). Pengertian dan Penjelasan Mikrotik. *Ilmu Komputer.Com*, *1*(1), 1–4.

Azhar, R., & Romliyanto, E. (n.d.). *Analisa Perbandingan Protokol Pptp Dan L2Tp Menggunakan Video Call Melalui Jaringan Virtual Private Network (Vpn) Comparative Analysis Pptp Protocol and L2Tp Using Video Call Through Virtual Private Network (Vpn)*. 13–21.

Ikhwan, S., & Amalina, A. (2017). Analisis Jaringan VPN Menggunakan PPTP dan L2TP. *Jurnal Infotel*, *9*(3), 1–7. https://doi.org/10.20895/infotel.v9i3.274

Iryani, N., Dwi, A., & Masykuroh, K. (2020). Analisa Performansi QoS Aplikasi Pembelajaran Daring pada Jam Kerja. *JTERA (Jurnal Teknologi Rekayasa)*, *5*(2), 201. https://doi.org/10.31544/jtera.v5.i2.2020.201-206

Mukhlishah, A. (2020). *Analisis Perbandingan Kinerja Jaringan Secure Socket Tunneling Protocol (Sstp) Dan Layer Two Tunneling Protocol (L2tp) + Internet Protocol Security (Ipsec) Menggunakan Metode Quality Of Service (Qos)*. *XV*, 16–25.

Nasihin, F. Z., Negara, A. B. P., & Irwansyah, A. (2015). Studi Perbandingan Performa QoS (Quality of Service) Tunneling Protocol PPTP Dan L2TP Pada Jaringan VPN Menggunakan MikroTik. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *4*(1), 39–44. http://jurnal.untan.ac.id/index.php/justin/article/view/12214

Pérez, A., Santamaria, E. K., Operario, D., Tarkang, E. E., Zotor, F. B., Cardoso, S.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

R. de S. N., Autor, S. E. U., De, I., Dos, A., Vendas, O. D. E., Empresas, D. A. S., Atividades, P. O., Artigo, N., Gest, G. N. R. M. D. E., Para, D. E. F., Miranda, S. F. da R., Ferreira, F. A. A., Oliver, J., Dario, M., … Volk, J. E. (2017). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *BMC Public Health*, *5*(1), 1–8. https://ejournal.poltektegal.ac.id/index.php/siklus/article/view/298%0Ahttp://repositorio.unan.edu.ni/2986/1/5624.pdf%0Ahttp://dx.doi.org/10.1016/j.jana.2015.10.005%0Ahttp://www.biomedcentral.com/1471-2458/12/58%0Ahttp://ovidsp.ovid.com/ovidweb.cgi?T=JS&P

Rahman, T., & Nurdin, H. (2020). Abdul Hamid No.77, RT.8/RW.4, Cawang, Kramat Jati, Jakarta Timur 13630 1 Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri. *Jl. Raya Jatiwaringin*, *5*(1), 23.

Rosa, S. L. (2018). Pendeteksian Anomali Penggunaan Internet di LAN Universitas Islam Riau Indonesia. *It Journal Research and Development*, *3*(1), 72–83. https://doi.org/10.25299/itjrd.2018.vol3(1).1994

Santoso, J. D. (2020). Analisis Perbandingan Metode Queue Pada Mikrotik. *Pseudocode*, *7*(1), 1–7. https://doi.org/10.33369/pseudocode.7.1.1-7

Sari, A. P., & Kemala, N. (2020). *Perancangan Jaringan Virtual Private Network Berbasis Ip Security Menggunakan Router Mikrotik*. *7*(2), 150–164.

Supendar, H., & Handrianto, Y. (2017). Simple Queue dalam Menyelesaikan Masalah Manajemen Bandwidth pada Mikrotik Bridge. *Bina Insani ICT Journal*, *4*(1), 21–30.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Watmah, S. (2020). Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang. *INSANtek – Jurnal Inovasi Dan Sains Teknik Elektro ISSN: 2722-574X*, *1*(1), 6–12.

Zamalia, W. O., Aksara, L. M. F., Yamin, M., Informatika, J. T., Teknik, F., & Oleo, U. H. (2018). *ANALISIS PERBANDINGAN PERFORMA QoS, PPTP , L2TP , SSTP DAN IPSEC PADA JARINGAN VPN MENGGUNAKAN MIKROTIK*. *4*(2), 29–36.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :