BAB II

LANDASAN TEORI

2.1. Tinjauan Pustaka

Penelitian yang dilakukan oleh (Firmansyah, 2018) di (STMIK Nusa Mandiri Jakarta dalam penelitiannya yang berjudul "*Analisis Perbandingan Kinerja Jaringan CISCO Virtual Router Redundancy Protocol (VRRP) Dan CISCO Hot Standby Router Protocol (HSRP*)". Setiap kegagalan dalam sistem jaringan komputer harus diminimalisir sedemikan mungkin. Kegagalan pada jaringan komputer terdiri dari kegagalan perangkat (*device*) yang digunakan, serta manajemen jaringan yang digunakan. Kegagalan pada sebuah perangkat jaringan akan mengakibatkan terjadinya kendala pada *Quality of Services* (QoS). Ada beberapa parameter yang sangat mempengaruhi QoS antara lain *packet lose*, *delay* dan *jitter* pada jaringan.

Untuk mengurangi dan meminimalisir kegagalan terhadap QoS pada suatu jaringan, kita dapat memanfaatkan sebuah fitur yang terdapat pada perangkat cisco dengan menggunakan *protocol redundancy*. Teknik optimalisasi jaringan ini digunakan untuk pengalihan koneksi yang terputus sehingga menghasilkan redundancy secara otomatis, teknik ini disebut dengan *Virtual Router Redundancy Proto*col (VRRP). VRRP bekerja dengan mengelompokan r*outer* secara bersamaan untuk menjadi satu *router virtual* dan menggunakan IP *Address* sendiri. VRRP merupakan protokol yang secara dinamis menunjukan satu atau lebih *virtual router* menjadi *gateway router* didalam jaringan LAN, yang memungkinkan beberapa *router* di *multiaccess link* untuk menggunakan *virtual ip address* yang sama. Protokol *routing redundancy* telah dikembangkan untuk menyediakan perlindungan terhadap *host* jika terjadi kegagalan pada *router*. VRRP merupakan sebuah protokol *multi vendor* yang banyak digunakan dalam jaringan LAN untuk melakukan antisipasi kegagalan dari *router* yang dijadikan sebagai *router* utama. VRRP pada dasarnya tidak mendukung fitur dari *load balancing*. Proses *failover* dari VRRP lebih *reliable*

ketimbang HSRP. Prioritas sangat mempengaruhi untuk menentukan *router master* dan *router backup*, dengan prioritas terbesar maka *router* tersebut dijadikan sebagai *router* master.

Dalam Penelitian yang dilakukan Rd.Amanda Yudiani, 2013. Universitas Telkom yang berjudul "Implemantasi dan Analisis *Virtual Router Redudandancy Protocol* (VRRP) dan *Hot Standby Router Protocol* (HRSP)", Bahwa VRRP dan HSRP merupakan *protokol redundancy*. Pada saat terjadi kegagalan pada *router* utama, VRRP dan HSRP memiliki mekanisme *recovery* masing-masing. HSRP merupakan *protokol redundancy* standar *Cisco* yang menetapkan sebuah *standby router* dan *active router* yang saling mengirimkan paket *hello* setiap 3s dan secara *otomatis standby router* dapat mengambil alih tugas *active router* yang mengalami gagal *link*. Sedangkan VRRP juga memiliki *backup router* yang bertugas sebagai *router* cadangan dan digunakan saat *master router* berhenti mengirimkan paket *advertise* yang dikirim setiap 1s yang menandakan *master router* berhenti bekerja.

Zulkarnain Wahyu Adi Saputra (2013), dalam sebuah penelitian dengan judul "Implementasi dan Analisis VRRP (*Virtual Router Redundancy Protocol*) dalam jaringan broardband nirkabel dengan studi kasus aplikasi FTP" bahwa beliau melakukan penelitian jaringan broadband nirkabel dengan menerapkan sebuah tehnik yang digunakan untuk mempertahankan link dengan menerapkan system cadangan yakni sebuah teknik VRRP Ketika sebuah *router* yang digunakan sebagai *router master* pada VRRP mati ataupun terganggu, jaringan akan dilewatkan pada *router* lain yang bertindak sebagai *router backup* sehingga data tetap akan terkirim sampai tujuan. Hal inilah merupakan sebuah solusi untuk menjamin *availabilitas* sambungan pada sebuah jaringan *client server* tentang penerapan VRRP pada jaringan dengan koneksi *broadband nirkabel*

Penelitian – penelitian tersebut diatas mengenai *reliability recovery* jaringan *stanby router* dan *active router* sebagai master merupakan *protocol*

redundancy cisco yang sangat efektif dalam sebuah jaringan yang secara automatis mengambil alih tugas jika mengalami kegagalan link oleh karena itu penulis tertarik untuk melakukan penelitian fungsi VRRP pada jaringan PT. TPPI Tuban dengan mengunakan simulasi jaringan *GNS3 IOS router cisco* dan switch cisco yang dijalankan secara *Virtualisasi* yang tidak merubah serta tidak mengurangi fitur seperti *device* aslinya sehingga fungsi *reability client server* bisa berjalan normal.

2.2. Landasan Teori

Jaringan Komputer menurut Andi (2010:2), Dengan semakin berkembangnya kebutuhan pengolahan data dan informasi didalam sebuah perusahaan dibutuhkan beberapa komputer yang digunakan oleh banyak orang yang bekerja dalam sebuah tim.

Jenis – jenis jaringan Menurut Andi (2010:53) berdasarkan jangkauan area atau lokasi, dibedakan menjadi 3 jenis yaitu:

1. *Lokal Area Network* (LAN) merupakan jaringan yang menghubungkan sejumlah komputer yang ada dalam suatu lokasi dengan area yang terbatas seperti ruang atau gedung. LAN dapat menggunakan media komunikasi seperti kabel dan wireless.
2. *Wide Area Network* (WAN) merupakan jaringan antara LAN satu dengan LAN lain yang dipisahkan oleh lokasi yang cukup jauh. Contoh penggunaan WAN adalah hubungan antara kantor pusat dengan kantor cabang yang ada di daerah-daerah.
3. *Metropolitan Area Network* (MAN) merupakan jaringan yang lebih besar dari jaringan LAN tetapi lebih kecil dari jaringan WAN. Jaringan MAN dan jaringan WAN sama-sama menghubungkan beberapa LAN yang membedakan hanya lingkup areanya yang berbeda.

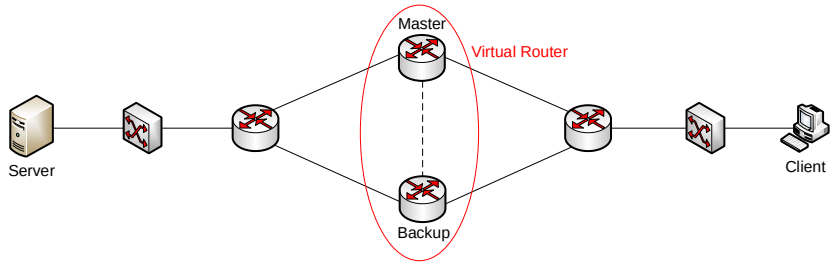
2.2.1. VRRP

Virtual Router Redundancy Protocol (VRRP) (R. Hinden, April,

2004) adalah *protocol* yang dikembangkan oleh IEEE ini memiliki tujuan yang sama yaitu *REDUNDANCY*. Fungsi VRRP itu sendiri adalah menyediakan *backup gateway*, sehingga apabila *primary gateway (master) failed traffic* akan dilewatkan ke *secondary gateway (backup)* (Hinden. Robert, 2004).

VRRP dirancang untuk digunakan di *multiaccess, multicast* maupun *broadcast* dengan menggunakan *ethernet LAN*. VRRP tidak dimaksudkan sebagai pengganti dari protokol dinamis yang ada. VRRP mendukung *Ethernet, Fastethernet, Bridge Group Virtual Interface* (BVI), *Gigabit Ethernet interfaces* dan pada *Multiprotocol Label Switching* (MPLS), *Virtual Private Networks* (VPNs).

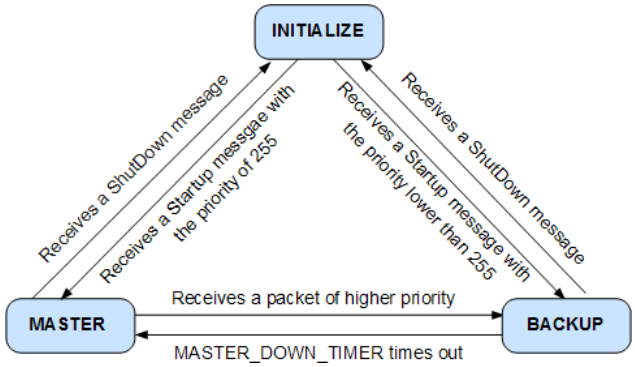
Mekanisme kerja dari protokol ini terimplemetasikan dalam sebuah *Virtual router* atau VRRP group. *Virtual router* merupakan sekumpulan *router* yang difungsikan untuk kebutuhan *redundancy*. Jumlah *router* yang dapat diaplikasikan bisa lebih dari satu untuk membentuk sebuah *virtual router* atau lebih. Pada VRRP akan ada sebuah *router* yang berperan sebagai master dan ada satu atau beberapa *router* yang berperan sebagai *backup*. *High Availability* sistem akan terjaga dengan aplikasi VRRP ini pada sebuah jaringan. Hal ini bisa terjadi karena ketika main-*link* mengalami down maka paket data masih tetap akan bisa dilewatkan melalui link lainnya.



Gambar 2.1 Topologi VRRP.

Gambar 2.1 merupakan topologi jaringan VRRP yang menjadi salah satu solusi redudansi perangkat jaringan dimana *router* 1 dan *router* 2 menjadi *virtual router* yang akan saling melakukan *backup*.

Perangkat VRRP membagi tanggung jawab untuk meneruskan paket seolah-olah mereka memiliki alamat IP yang sesuai dengan *default gateway* yang dikonfigurasi pada *host.* Salah satu perangkat akan bertindak sebagai *master* dan perangkat lainnya bertindak sebagai *backup*. Jika peragkat *master* gagal, perangkat *backup* akan menjadi *master*. Dengan cara ini redundansi perangkat akan selalu tersedia, sehingga lalu lintas di jaringan akan dialihkan tanpa bergantung pada satu perangkat.



Gambar 2.2 Cara Kerja VRRP.

Pada cara kerja VRRP (R. Hinden, April, 2004) terdapat 3 states yaitu *Initialize state, Master state* dan *Backup state* yang digambarkan pada Gambar 2.2. *Initialize state* mengirimkan *Startup* message ke 2 perangkat switch dengan prioritas 255 untuk *Master state* dan prioritas dibawah 255 untuk *Backup state.* Hal tersebut dilakukan karena untuk memberikan pemberitahuan bahwa perangkat tersebut merupakan *Master* atau *Backup*. Kemudian *Master* dan *Backup* mengirimkan pesan kepada *Initialize state* mengenai statusnya mati atau hidup. Untuk penjelasan yang lebih mendalam mengenai ketiga state tersebut akan diuraikan dibawah ini.

Tabel 2.1 *Initialize state, Master state* dan *Backup state.*

State	Deskripsi
Initialize	Jika VRRP tidak tersedia, perangkat *router* di *Initialize State* tidak bisa meneruskan proses paket VRRP. Ketika perangkat *router* berfungsi atau mendeteksi kesalahan, masuk pada fase

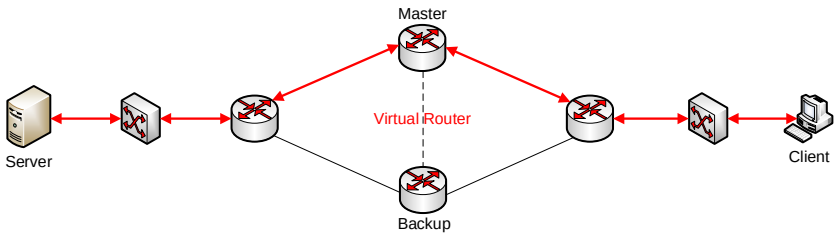
	Initialize State.
Master	Pada perangkat *router* yang menggunakan VRRP ketika memasuki *Master State,* akan melakukan operasi berikut: 1. Mengirim paket VRRP *Advertisement* disetiap *interval* waktu. 2. Menggunakan *virtual MAC address* untuk merespon paket ARP yang ditujukan kepada *virtual IP Address*. 3. Meneruskan paket IP yang ditujukan ke *virtual MAC Address.* 4. Memproses paket IP yang ditujukan untuk *virtual IP Address*.
Backup	Pada perangkat *router* yang menggunakan VRRP ketika memasuki *Backup State,* akan melakukan operasi berikut: 1. Menerima paket VRRP *Advertisement* dari *Router Master* dan menentukan apakah *Router Master* bekerja dengan baik. 2. Tidak akan merespon permintaan paket ARP yang ditujukan untuk alamat *IP virtual.* 3. Menyingkirkan paket IP yang ditujukan ke *virtual MAC address dan virtual IP address.* 4. Menyingkirkan paket yang membawa prioritas yang lebih rendah dari perangkat dan tidak akan mereset waktu *Master Down Timer.* Jika kondisi *Master_Down_ Timer* direset akan membandingkan alamat IP yang diterima dengan membawa prioritas yang sama dengan perangkat arti nya *master down time* sama dengan *skewtime*, dengan rumus :

	$Skewtime = \frac{256-priority}{256}$ …….... (2.1) Sedangkan *master down interval* dengan rumus : (3 x *advertisement interval*) + *skewtime* …… (2.2)

a. Mekanisme VRRP

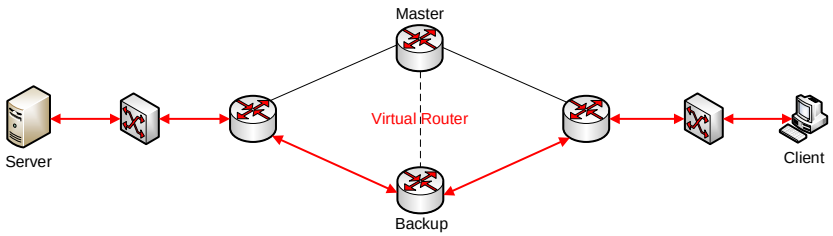
Pada protokol redudansi VRRP memungkinkan dua atau lebih *router* dapat secara otomatis memilih satu *router* untuk bertindak sebagai *master* dan satu atau lebih *router* lain bertindak sebagai *router backup* untuk melayani *router* master. Pada implementasinya protokol *redundancy* VRRP tidak dapat menentukan sendiri *router master* dan *router backup*, oleh karena itu hal pertama yang dilakukan adalah dengan mengkonfigurasi dan menentukan secara manual *router* mana yang akan bertindak sebagai *master* dan *backup*. Setelah melakukan konfigurasi lalu yang dilakukan oleh *router* master adalah mengirimkan paket *advertisements* kepada *master* lain selama *router* lain berfungsi normal. Pada dasarnya *router master* akan menyebarkan alamat IPnya sendiri bahwa alamat IP tersebut adalah miliknya.

Hal tersebut bertujuan untuk menginformasikan kepada *router* yang lain bahwa *router* master masih normal dan belum mengalami kegagalan. Ketika *router backup* menerima paket *Advertisement* dari *router master*, maka waktu dari *master_down_timer* akan *reset* dan menunggu paket *Advertisement* selanjutnya. Jika paket *Advertisement* tidak diterima oleh *router backup* sebelum waktu *master_down_timer* berakhir, maka *router backup* akan memilih *router master* baru yang kemudian akan bertanggung jawab untuk merespon *ARP requests, fowarding packet,* dan lain lain yang berhubungan dengan satu atau lebih alamat *virtual IP* yang terkait dengan *router master* sebelumnya.



Gambar 2.3 *Paket Data melalui router master*

Pada Gambar 2.3 terlihat garis merah yang menandakan paket data dialirkan melalui *router master* karena memiliki prioritas yang tinggi dan ketika *router master* tersebut bermasalah karena mati / *down* atau koneksi terputus maka secara otomatis aliran paket data akan berpindah melalui *router backup*. Gambar 2.4 menunjukkan bahwa aliran data sudah berpindah ke *router backup*.



Gambar 2.4 *Paket data melalui router backup*

Ketika *router master* sudah terkoneksi kembali maka aliran paket data dari *router backup* akan berpindah secara otomatis ke *router master* karena prioritas *router master* lebih besar dibandingkan *router backup*.

b. Keuntungan dari VRRP

1. *Redundancy* : VRRP memungkinkan untuk mengkonfigurasi beberapa *router* sebagai default gateway *router*, yang mengurangi kemungkinan satu titik kegagalan dalam sebuah jaringan
2. *Load Sharing* : VRRP dapat dikonfigurasi sedemikian rupa sehingga lalu lintas ke dan dari klien LAN dapat digunakan bersama oleh beberapa *router*, sehingga dapat membagi beban lalu lintas yang tersedia secara lebih merata di antara *router*.

3. *Multiple Virtual Router* : VRRP mendukung hingga 255 *virtual router* (VRRP *group*) pada sebuah *router physical interface*. Beberapa dukungan *router virtual* memungkinkan untuk melaksanakan redudancy dan *load sharing* dalam topologi LAN.
4. *Multiple IP Addresses* : *Virtual Router* dapat mengelola beberapa IP *address*, termasuk *secondary* ip *address*. Oleh karena itu, jika memiliki beberapa *subnet* yang dikonfigurasi pada *Ethernet interface*, VRRP dapat dikonfigurasikan pada setiap *subnet.*
5. *Preemption* : Skema *redundancy* dari VRRP memungkinkan untuk membuat terlebih dahulu *virtual router* cadangan yang telah mengambil alih *virtual router master* yang gagal dengan prioritas yang lebih tinggi dari *virtual router* cadangan yang tersedia.
6. *Authentication* : Pesan VRRP *digest* 5 (MD5) algoritma otentikasi melindungi VRRP-*spoofing* terhadap perangkat lunak dan menggunakan standar industri *algoritma* MD5 untuk meningkatkan kehandalan dan keamanan.
7. *Advertisement Protokol* : VRRP menggunakan *Internet Assigned Numbers Authority (*IANA) dengan *standard multicast address*-nya (224.0.0.18). Skema pengalamatan ini meminimalkan jumlah *router* yang harus melayani multicasts dan memungkinkan peralatan tes untuk mengidentifikasi secara akurat paket VRRP pada segmen.
8. VRRP *Object Tracking* : VRRP *Object Tracking* menyediakan cara untuk memastikan *router virtual master* terbaik dari *router* VRRP untuk VRRP group dengan mengubah prioritas ke status *Object Tracking* seperti *interface* atau *IP route states*

c. Istilah dalam VRRP

Jaringan VRRP memerlukan beberapa komponen untuk melakukan mekanisme kerjanya. Komponen ini harus dikonfigurasi secara manual oleh seorang admin jaringan. Adapun komponen VRRP

adalah sebagai berikut :

1. *Virtual Router* (VR).

   Sebuah *virtual router* (VR) terdiri dari sebuah *router owner* atau *router master* dan satu atau lebih *router backup*. Keduanya akan berada di dalam satu jaringan yang sama dan terkonfigurasi dengan parameter di bawah ini :

   1. Memiliki VRID *(Virtual Router ID)* yang sama
   2. Memiliki konfigurasi *virtual* IP yang sama untuk tiap-tiap *router*
   3. *Router* owner dan *router backup* terkoneksi dalam sebuah VR yang sama

2. *Virtual MAC address*

   Karena sifat VRRP adalah *virtual* maka MAC *address*-nya pun juga *virtual*. RFC2338 menstandarisasi penggunaan MAC *address* untuk VRRP adalah 00:00:5E:00:01. Oktet terakhir dari MAC *address* tersebut adalah nilai *integer* VRID, sehingga apabila VRID sebuah sistem VRRP adalah 49 maka MAC *address virtual*nya akan menjadi 00:00:5E:00:31. Alamat MAC *virtual* ini tidak bisa dirubah secara manual karena telah menjadi standar *internasional.*

3. *Virtual IP address*

   Virtual IP yang berada dalam jaringan VRRP harus sama. Pada *router* master alamat IP *virtual* harus sama degan alamat IP fisik. Sebagai contoh alamat IP *virtual* dan fisik pada *router* master adalah 192.168.26.2, sedangkan pada *router backup* alamat IP *virtual* adalah 10.10.1.2 tetapi alamat IP fisiknya adalah 192.168.28.2.

4. ARP (*Address Resolution Protocol*)

   ARP adalah protokol yang digunakan untuk pemetaan alamat MAC menuju alamat IP. ARP bertanggung jawab terhadap letak sebuah node VRRP pada jaringan. ARP berhubungan

langsung dengan alamat *virtual* MAC dalam jaringan dan proses ARP request ini semuanya dilakukan oleh *router master*.

5. *Owner*

Owner dalam jaringan VRRP adalah sebuah *router master* yang bekerja di bawah sebuah *virtual router*. *Owner* harus diset *priority*-nya dengan nilai 255. *Router* master adalah komponen utama yang bekerja kita jaringan VRRP berfungsi. *Router master* atau *owner* ini memberikan paket *advertisement* terus menerus kepada *router backup* untuk menjaga stabilitas koneksinya. Paket *advertisement* ini dikirim melalui alamat IP *multicast* yang sudah distandarisasi dalam RFC-2338 yaitu 224.0.0.18 dan melalui protokol nomor 112.

6. *Backup*

Sebuah sistem VRRP sekurang-kurangnya harus terdiri dari sebuah *router backup*. *Router backup* harus dikonfigurasi dengan alamat IP *virtual* yang sama dengan *router* master. Nilai *default* dari priority *router backup* adalah 100. Ketika *router* master mengalami kegagalan, maka *router backup* dengan nilai *priority* tertinggilah yang akan mengambil-alih tugas dari *router master*.

2.2.2. Kualitas *Reliability* Jaringan

Quality of service atau QoS adalah kemampuan dari suatu Jaringan IP untuk memberikan layanan lebih bagus untuk suatu tipe data/traffic tertentu (biasanya yang penting), tentu saja dengan mengorbankan layanan untuk tipe data/traffic yang tidak terlalu penting.

QoS didesain untuk membantu *end user* (*client*) menjadi lebih *produktif* dengan memastikan bahwa *user* mendapatkan performansi yang handal dari aplikasi berbasis jaringan. *QoS* mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. *QoS* merupakan suatu tantangan yang besar dalam jaringan berbasis IP dan

internet secara keseluruhan. Tujuan dari *QoS* adalah untuk memenuhi kebutuhan-kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. *QoS* menawarkan kemampuan untuk mendefinisikan atribut layanan yang disediakan, baik secara *kualitatif* maupun *kuantitatif.*

a. Parameter QoS

Performansi mengacu ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. Performansi merupakan kumpulan dari beberapa parameter besaran teknis, yaitu :

1. *Throughput*

   Kecepatan (*rate*) transfer data efektif, yang diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang sukses dari sebuah *channel* komunikasi (Bradner, S,1991). Proses penghitungan parameter *throughput* menggunakan rumus sebagai berikut (Constantine, Mei, 2011) (1.1):

$$\textbf{\textit{Throughput}} = \frac{\textbf{\textit{Paket data yang diterima}}}{\textbf{\textit{Lama Pengalatan}}} \quad \text{..... (2.3)}$$

Tabel 2.2 *Qos Throughput*

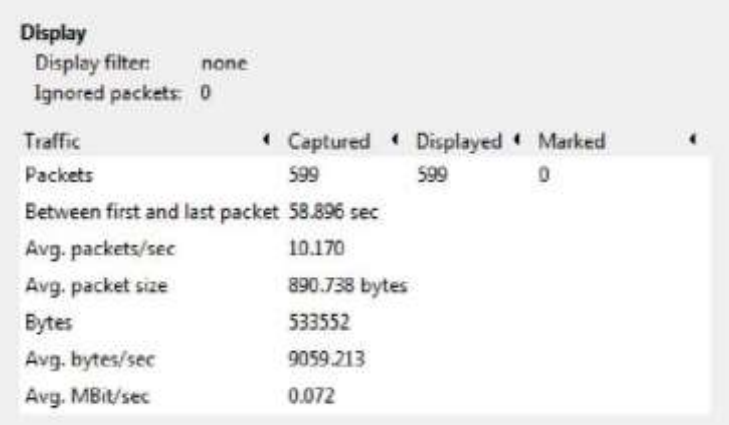
Kategori Throughput	Throughput	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	< 25	1

(*Sumber : Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) General aspects of Quality of Service DTR/TIPHON-05006.1999)*

Tabel berikut menunjukan hasil penelitian sebelumnya dengan perhitungan throughput dari capture data yang telah dilakukan.

Tabel 2.3 *Hasil perhitungan throughput*

Parameter yang dihitung	Nilai yang didapat
Paket data yang diterima	533552 bytes (*diubah ke bps, dikalikan 8*) = 4.268.416
Lama pengamatan	58,896 s
throughput	72,4737 kbps



Display

Display filter: none

Ignored packets: 0

Traffic	Captured	Displayed	Marked
Packets	599	599	0
Between first and last packet	58.896 sec		
Avg. packets/sec	10.170		
Avg. packet size	890.738 bytes		
Bytes	533552		
Avg. bytes/sec	9059.213		
Avg. MBit/sec	0.072		

Gambar 2.5 Contoh summary hasil *cupture wireshark*

Troughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Jika kondisi throughput nya buruk maka ada beberapa paket yang tidak dapat diamati untuk destination tertentu.

2. *Delay.*

Waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari suatu titik ke titik lain yang menjadi tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama (G. Almes, S. Kalidindi, S. M. Zekauskas, 1999). Perhitungan delay menggunakan persamaan berikut (Anjik. Rianto, 2008) (1.2):

$$\boldsymbol{Rata - rata\ Delay} = \frac{\boldsymbol{Total\ Delay}}{\boldsymbol{Total\ Paket\ yang\ di\ terima}} \quad \ldots\ldots\ldots (2.4)$$

Tabel 2.4 ***QoS Delay***

Kategori *Delay*	Besar *Delay*	Indeks
Sangat Bagus	<150 ms	4
Bagus	<250 ms	3
Jelek	<350 ms	2
Sangat Jelek	>450 ms	1

(Sumber : *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) General aspects of Quality of Service DTR/TIPHON-05006.1999*)

Tabel berikut menunjukan hasil penelitian sebelumnya dengan perhitungan rata-rata delay dari capture data yang telah dilakukan Gambar 2.5

Tabel 2.5 *Hasil perhitungan rata-rata delay*

Parameter yang dihitung	Nilai yang didapat
Total packet yang diterima	599 packet
Total Delay	58,896068 s
Rata-rata Delay	98,32 ms

3. Jitter

Jitter merupakan variasi kedatangan paket, hal ini diakibatkan oleh variasi- variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan *jitter*. *Jitter* lazimnya disebut variasi *delay* , yang menunjukkan banyaknya variasi *delay* pada taransmisi data di jaringan (Demichelis. C, 2002). Cara perhitungan *jitter* dapat menggunakan rumus berikut : (Clark, Alan.2003) 1.3 :

$$\boldsymbol{Jitter} = \frac{\textbf{Total Variasi } \boldsymbol{delay}}{\boldsymbol{Total\ Paket\ yang\ di\ terima - 1}} \qquad \text{..... (2.5)}$$

Total variasi *delay* diperoleh penjumlahan :

(delay 2 – delay 1) + (delay 3 – delay 2) + ... (delay n – delay (n-1))

Keterangan :

n = paket

Kategori kinerja jaringan berbasis IP dalam *jitter* versi TIPHON (*Telecomunications and internet protocol harmonization over networks*), mengelompokkan menjadi empat kategori penurunan kinerja jaringan berdasarkan nilai jitter seperti berikut :

Tabel 2.6 ***QoS Jitter***

Kategori Jitter	Besar Jitter	Indeks
Sangat Bagus	0 ms	4
Bagus	75 ms	3
Sedang	125 ms	2
Jelek	225 ms	1

(Sumber : *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) General aspects of Quality of Service DTR/TIPHON-05006.1999)*

Tabel berikut menunjukan hasil penelitian sebelumnya dengan perhitungan jitter dari capture data yang telah dilakukan gambar 2.5

Tabel 2.7 *Hasil perhitungan jitter*

Parameter yang dihitung	Nilai yang didapat
Total *packet* yang diterima	599 *packet*
Total varisi *delay*	99,253674 s
Jitter	165,98 ms

Berdasarkan tabel tersebut, kategori *jitter* dari jaringan ini ‘jelek’, karena ***adanya delay*** antrian pada ***router*** dan ***switch***.

Besarnya nilai *jitter* akan sangat dipengaruhi oleh variasi

beban trafik dan besarnya tumbukan antar *packet* (*congestion*) yang ada dalam jaringan tersebut. Semakin besar beban trafik di dalam jaringan akan menyebabkan semakin besar pula peluang terjadinya *congestion*, dengan demikian nilai *jitter*-nya akan semakin besar. Semakin besar nilai jitter akan menyebabkan nilai QoS semakin turun.

4. *Packet Loss*

Didefinisikan sebagai kegagalan transmisi paket IP mencapai tujuannya. Kegagalan paket tersebut mencapai tujuan, dapat disebabkan oleh beberapa hal yaitu terjadinya *overload* trafik di dalam jaringan, tabrakan (*congestion*) dalam jaringan, error yang terjadi pada media fisik (Almes, G. Kalidindi, S. Zekauskas, M, 1999). Penghitungan *packet loss* didapatkan dengan menggunakan fungsi yang sudah ada pada aplikasi *wireshark* yaitu dengan menggunakan command "*tcp.analysis.flags && !tcp.analysis.window_update*" jika terdapat paket *tcp* yang jelek atau rusak seperti paket "*TCP retransmission"* maka packet tersebut lah yang kemudian dijumlahkan kemudian di rata – rata kan.

$$\boldsymbol{Paket\ loss} = \frac{\boldsymbol{Paket\ yang\ dikirim - paket\ yang\ diterima}}{\boldsymbol{Paket\ yang\ di\ kirim}} \boldsymbol{x}\ \mathbf{100}\ \% \quad (2.6)$$

Tabel 2.8 *Packet Loss*

Kategori *Degradasi*	*Packet loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Jelek	25 %	2

(Sumber : *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) General aspects of Quality of Service DTR/TIPHON-05006.1999)*

Tabel berikut menunjukan hasil penelitian sebelumnya dengan

perhitungan Packet loss dari capture data yang telah dilakukan gambar 2.5

Tabel 2.9 *Hasil perhitungan Packet loss*

Parameter yang dihitung	Nilai yang didapat
Paket data yang dikirim	599
Paket data yang diterima	599
Packet Loss	0 %

Jika kategori loss nya tidak 0%, maka ada beberapa total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena *retransmisi* akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut.

b. Parameter *Downtime*

Adapun perhitungan parameter *downtime* dengan rumus :

$$\text{MTBF} = \frac{Jumlah\ Operation\ Availability - Downtime}{Number\ of\ Repair} \quad \ldots\ldots\ldots\ldots\ldots\ldots (2.7)$$

Keterangan :

MTBF = *Maen time between failures*

Kemudian nilai MTBF dapat dilakukan menghitung nilai MTTR dengan perhitungan rumus :

$$\text{MTTR} = \frac{Total\ maintenance\ time}{Number\ of\ repair} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.8)$$

Keterangan :

MTTR = *Maen time to repair*

Dari hasil perhitungan MTBF dan MTTR dapat di lakukan perhitungan *availability* sistem dengan rumus :

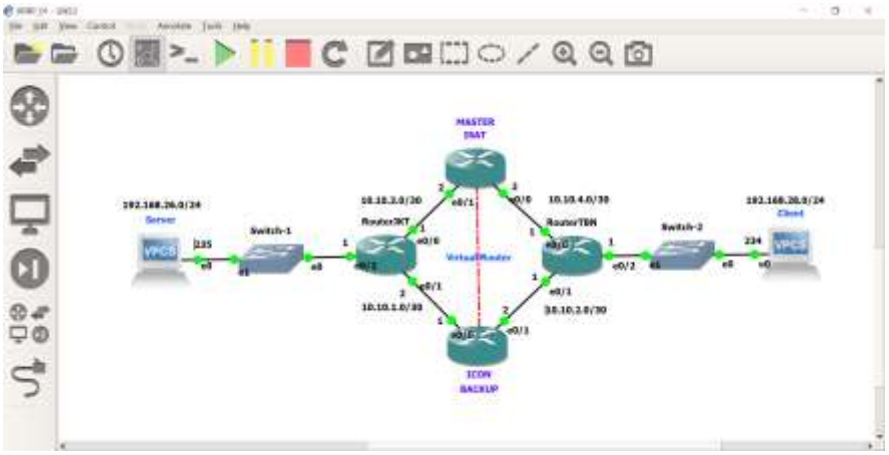
$$Availability = \frac{MTBF}{MTBF+MTTR} \times 100 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.9)$$

2.2.3. Tools Software Jaringan

Dalam penelitian ini khususnya dalam bidang jaringan komputer penulis mempelajari berbagai metode yang digunakan pada jaringan komputer tersebut, untuk mempermudah penerapannya dilapangan tanpa harus merubah topologi jaringan yang sudah fix dan stabil tentu nya memerlukan *tools* untuk bisa menerapkan metode / teori yang penulis pelajari tanpa harus merubah sistem jaringan yang ada, dan *tools* tersebut dipakai untuk mempermudah dalam analisa suatu metode jaringan, berikut adalah beberapa *tools* yang digunakan dalam penelitian ini.

a. ***Graphic Network Simulator 3*** (GNS3)

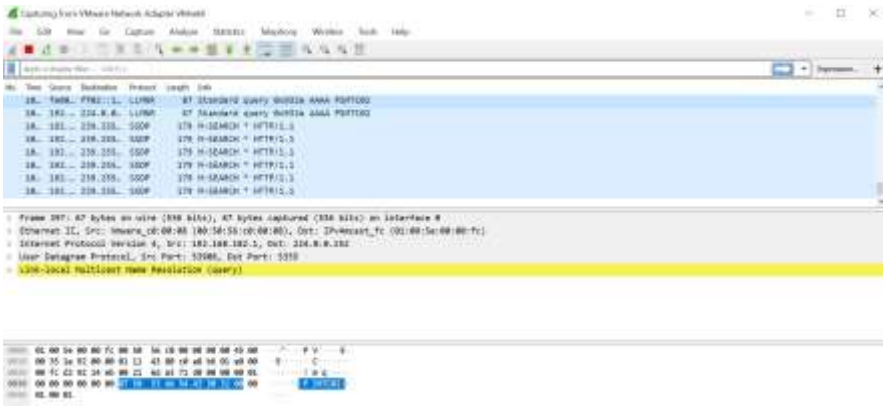
Graphic Network Simulator 3 (GNS3) merupakan sebuah simulator yang dapat melakukan emulasi jaringan yang komplek. Simulator ini dapat mensimulasikan suatu rancangan jaringan sebelum diimplementasikan pada kondisi *real* di lapangan, simulasi menggunakan GNS3 bekerja tanpa harus memiliki perangkat jaringan seperti *router* dan *switch* (http://www.gns3.com). Tools GNS3 menggunakan *Sistem Operasi* (OS) yang sebenarnya, misalnya IOS pada *router* / switch cisco dan *Router* OS pada perangkat cisco.



Gambar 2.5 GNS3

b. Wireshark

Wireshark adalah penganalisis paket jaringan, *Wireshark* mampu menangkap paket-paket data/informasi pada paket yang berada di jaringan, aplikasi tersebut akan mencoba untuk menangkap paket jaringan dan menampilkan data yang ada didalam paket secara detail [https://www.wireshark.org].

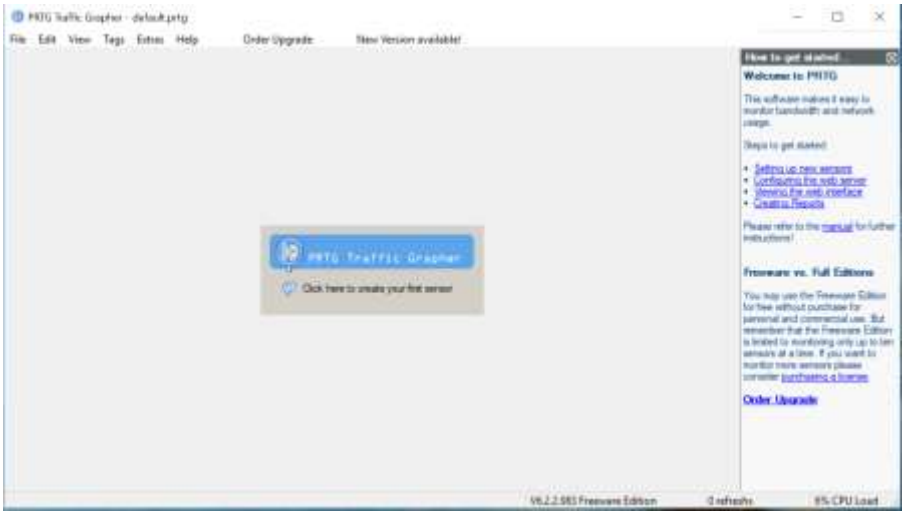


Gambar 2.6 Wireshark

c. PRTG Trafic Grapher

PRTG (*Paessler Router Traffic Grapher*) adalah perangkat lunak yang mudah digunakan untuk memantau penggunaan *bandwidth* dan banyak parameter jaringan lain melalui *SNMP, Packet Sniffing,* atau *Cisco NetFlow* yang memungkinkan untuk pengukuran *traffic* berdasarkan alamat IP dan atau protokol. Pengukuran berbasis SNMP hanya berbasis pada *port. Software* ini juga memungkinkan untuk secara cepat mempersiapkan dan menjalankan sebuah proses pemantauan untuk sebuah jaringan tertentu. Dengan PRTG ini maka dengan mudah dapat mengetahui sejumlah data yang mengalir melalui perangkat seperti *router* dan memantau penggunaan PC serta menganalisa traffic yang dapat dikategorikan ke dalam beberapa jenis protokol. *PRTG Traffic Grapher* berjalan pada mesin Windows di dalam jaringan selama 24 jam setiap hari dan terus-menerus mencatat penggunaan parameter jaringan. Dengan *PRTG Traffic Grapher* ini dapat memonitor semua aspek jenis protokol mulai dari

jenis jaringan protokol *FTP, HTTP, HTTPS, SMTP, ICMP,DNS, POP3, SNMP* dan lainnya . disini dapat dilihat seberapa banyak penggunaan *bandwith* pada masing-masing protokol yang telah ada.



Gambar 2.7 PRTG *Trafic Grapher*