

IMPLEMENTASI *ACCESS LIST* SEBAGAI *FILTER TRAFFIC* JARINGAN (STUDY KASUS PT. USAHA ENTERTAINMENT INDONESIA)

Agus Didi Purwanto¹, Mohammad Badrul²

Abstract—Cisco router are frequently used equipment on the network, primarily on a network of Wide Area Network (WAN). Cisco router has the function to forward a packet data to an addressing that is a far and being in a different computer network. Cisco router has one function that can be used as a traffic filtering that when implemented more then it would be firewall. With access list, cisco router can be used for later defended the network from some threat that will destroy the document and data that reside in an institution or a company. The result of this research are extended access list that is simulated in advance on packet tracer and then applied to the router 2600 series on a network that will help determine the source and destination address as well as the protocol and port number that you want. By using this type, access list can be more efficient in regulating user access allowed or not in a particular host and control the spread of the data packets that are useless in the network.

Intisari — Cisco router merupakan salah satu peralatan yang digunakan pada sebuah jaringan, terutama jaringan Wide Area Network (WAN). Cisco router memiliki fungsi untuk meneruskan paket data meski dengan jarak yang sangat jauh dan pada jaringan komputer yang berbeda. Cisco router memiliki satu fungsi yang dapat digunakan sebagai penyaring lalu lintas data yang ketika diimplementasikan akan seperti firewall. Dengan daftar akses, cisco router dapat digunakan sebagai keamanan jaringan dari yang akan menjaga dokumen dan data yang berada pada jaringan komputer institusi atau perusahaan. Hasil penelitian ini membahas tentang daftar akses yang disimulasikan dengan menggunakan aplikasi cisco packet tracer dan kemudian diterapkan pada router seri 2600 pada melalui interface yang ada pada router untuk menentukan sumber dan alamat tujuan serta protokol dan nomor port yang diinginkan. Dengan menggunakan daftar akses, router akan menentukan di perbolehkan atau tidak penyebaran paket pada suatu jaringan komputer.

Kata Kunci— Cisco, Router, Wide area network

I. PENDAHULUAN

Jaringan komputer menjadi pilihan yang tepat baik itu perusahaan maupun personal untuk menyediakan informasi dan menghubungkan Jaringan LAN ke internet. Karena Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus di tanggung adalah bagaimana jaminan sebuah keamanan bagi jaringan yang terhubung dengan Internet. Hal ini dapat dilihat dari penggunaan internet yang terus meningkat.

Dalam *Local Area Network* diketahui bahwa setiap sistem jaringan komputer yang terhubung tidak ada jaminan sebuah keamanan. Di dalam mengimplementasikan komponen dari sistem keamanan jaringan seperti firewall yang berfungsi untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak semua hubungan/kegiatan suatu segemen pada jaringan pribadi dengan jaringan luar yang bukan merupakan Segmen tersebut dapat berupa sebuah workstation, server, router, atau ruang lingkungannya. LAN (*Local Area Network*) [4].

Di suatu instansi atau perusahaan pastinya banyak sekelompok orang yang menghendaki pengambilan data secara illegal ataupun perusakan jaringan pada perusahaan tertentu. Oleh karena itu dibutuhkan suatu penangkal yang dapat melindungi data ataupun dokumen penting [8].

Keamanan jaringan komputer merupakan suatu hal yang dibutuhkan oleh setiap instansi atau perusahaan dalam menjalankan usaha dan bisnisnya. Bagaimana jika kewanaman jaringan ini tidak terpenuhi maka akan sangat merugikan. Apalagi jika berhubungan dengan data- data penting perusahaan. Jelas, kebutuhan akan keamanan jaringan komputer sudah menjadi suatu keharusan bagi setiap perusahaan.

PT. Usaha Entertainment Indonesia adalah salah satu perusahaan yang bergerak dibidang *Entertainment* dengan berkantor pusat di Jakarta dan saat ini sudah memiliki cabang di Bali. Dengan melihat topologi jaringan berjalan saat ini, lalu lintas data di jaringan tersebut sangat padat, dan dalam segi keamanan *filter* data, terlihat tidak adanya batas akses antara jaringan kantor pusat dan jaringan kantor cabang. Dalam hal ini tidak adanya *filter* data apakah data tersebut di perbolehkan masuk pada jaringan atau tidak. Hal inilah yang

¹Program Studi Teknik Informatika STMIK Nusa Mandiri Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan. Telp. (021) 78839513 Fax. (021) 78839421, e-mail: agus.didipurwanto@gmail.com;

² Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta, Jl. Damai No. 8 Warung Jati Barat (Margasatwa) Jakarta Selatan. Telp. (021) 78839513 Fax. (021) 78839421, e-mail: mohammad.mbl@nusamandiri.ac.id

akan menciptakan celah yang bisa menimbulkan ketidakamanan pada jaringan komputer.

Traffic filtering tidak lain merupakan sebuah teknik untuk mengontrol trafik-trafik yang diforward ke dan dari sebuah jaringan melintasi router. Fungsi ini melibatkan perancangan policy-policy keamanan. Pada implementasinya traffic filtering ini akan di rancang untuk membentuk environment firewall. Karena hal tersebut di atas penulis merasa pada PT. Usaha Entertainment Indonesia perlu membangun dan mengimplementasikan serta mengembangkan jaringan komputer dan mengusulkan suatu rancangan jaringan dengan implementasi *metode access control list*.

II. KAJIAN LITERATUR

Jaringan komputer adalah sebuah sistem yang terdiri dari atas komputer, *software* dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama [2]. Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*). Pihak yang meminta atau menerima layanan disebut pelayan klien (*client*) dan yang memberikan atau mengirim layanan disebut pelayan (server). Arsitektur ini disebut dengan sistem *client server*, dan digunakan pada hamper seluruh aplikasi jaringan komputer.

Jaringan terdiri dari komputer, *peripheral* dan peralatan penunjang lain yang saling berhubungan satu dengan yang lain untuk dapat digunakan secara bersama- sama atau dapat pula berdiri sendiri. Jumlah peralatan yang dihubungkan dapat bervariasi dari dua sampai beberapa ratus unit. Dimana setiap peralatan yang saling di hubungkan tersebut, didalam pengertian *Network* disebut *Node*.

Jika dilihat berdasarkan luas area yang dapat dijangkau atau dilayani jaringan Komputer terbagi menjadi 3 jenis yaitu LAN, MAN dan WAN.

A. Klasifikasi Jaringan Komputer

1. LAN

LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil, seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil [2]. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 *Ethernet* menggunakan perangkat *switch*, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s [9]. selain teknologi *Ethernet*, saat ini teknologi 802.11b (atau biasa disebut *Wifi*) juga sering digunakan untuk membentuk LAN dengan teknologi *Wifi* biasa disebut *hotspot*

2. MAN

MAN adalah sebuah jaringan komputer besar yang mencangkup sebuah kota atau sebuah kampus besar [3]. MAN biasanya merupakan gabungan dari LAN yang menggunakan teknologi *backbone* berkecepatan tinggi dan menyediakan layanan ke jaringan yang lebih besar seperti WAN dan *Internet*[9]. *Metropolitan Area Network* (MAN) suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya[2]. Jaringan MAN

adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antara 10 hingga 50 km, MAN ini merupakan jaringan yang tepat untuk membangun jaringan antara kantor-kantor dalam suatu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya, prinsip sama dengan LAN, hanya saja jarak lebih luas, yaitu 10-50 km.

3. WAN

Suatu WAN meliputi area geografi yang lebih luas lagi, yang meliputi suatu negara atau dunia. Umumnya jaringan ditempatkan pada banyak lokasi yang berbeda [3]. WAN digunakan untuk menghubungkan banyak LAN yang secara geografis terpisah. WAN dibuat dengan cara menghubungkan LAN menggunakan layannan seperti Leased Line, dial-up, satelit atau layanan paket carrier [9]. Dengan WAN, sekolah yang ada di Yogyakarta dapat berkomunikasi dengan sekolah yang ada di Munchen Jerman dalam beberapa menit saja tanpa mengeluarkan biaya yang banyak. *Wide Area Network* (WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota, atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik [2]. WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer dilokasi yang lain

B. Jenis-Jenis Jaringan

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai *client* dan juga *server*. Tetapi ada jaringan yang memiliki komputer yang khusus didedikasikan sebagai *server* sedangkan yang lain sebagai *client*. Ada juga yang tidak memiliki komputer yang khusus berfungsi sebagai *server* saja. Karena itu berdasarkan fungsinya maka ada dua jenis jaringan komputer.

1. Client Server

Pada jaringan ini terdapat 1 atau beberapa komputer server maupun menjadi komputer client dan diubah-ubah melalui software jaringan pada protokolnya. Komputer client sebagai perantara untuk dapat mengakses data pada komputer server sedangkan komputer server menyediakan informasi yang diperlukan oleh komputer client [2]. Seiring dengan pertumbuhan jaringan, baik dari segi ukuran maupun trafik, lebih dari satu *server* dalam sebuah jaringan dapat saja digunakan *server-server* untuk sistem jaringan yang besar memiliki fungsi dan tugas masing- masing [9].

2. Peer to peer

Pada jaringan ini tidak ada komputer client maupun komputer server karena semua komputer dapat melakukan pengiriman maupun penerimaan informasi sehingga semua computer berfungsi sebagai *client* sekaligus *server* [2].

Komputer- komputer yang terdapat dalam jaringan *peer to peer* dapat bertindak sebagai *server* dan juga bertindak sebagai *client*. Jenis jaringan ini juga tidak memiliki *Administrator* yang bertanggungjawab terhadap seluruh jaringan. Masing- masing user bertindak sebagai *Administrator* pada komputer yang digunakannya [9]. *User*

masing- masing komputer dapat menentukan data mana yang diperbolehkan untuk diakses oleh *user* dari komputer lain.

Peer to peer juga dikenal dengan istilah *workgroup*. Jumlah pengguna dalam sebuah jaringan *peer to peer* biasanya kurang dari 10. Jenis jaringan ini relatif sederhana karena masing-masing komputer berfungsi sebagai *server* dan *client* sehingga tidak diperlukan sebuah komputer yang bertindak sebagai *server* pusat. Dari sisi biayanya jenis jaringan ini dapat lebih murah dibanding jenis jaringan *client server*.

C. Perangkat Keras Jaringan

Ada beberapa perangkat keras yang digunakan untuk penelitian ini antara lain:

1. Modem

Modem berasal dari singkatan Modulator Demodulator. Modulator merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan Demodulator adalah bagian yang memisahkan sinyal informasi (yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik [4]. Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah.

2. Router

Router sering digunakan untuk menghubungkan beberapa *network*. Baik *network* yang sama maupun berbeda dari segi teknologinya. *Router* juga digunakan untuk membagi *network* besar menjadi beberapa buah *subnet* (*network-network* kecil). Setiap *subnet* seolah-olah “terisolir” dari *network* lain. Hal ini dapat membagi-bagi *traffic* yang akan berdampak positif pada performa *network* [2]. Sebuah *router* memiliki kemampuan *routing*. Artinya *router* secara cerdas dapat mengetahui kemana rute perjalanan informasi (yang disebut *packet*) akan dilewatkan, apakah ditujukan untuk *host* lain yang satu *network* atau berbeda *network*.

3. Bridge

Bridge atau *transparent bridge* merupakan perangkat *network* yang digunakan untuk menghubungkan dua buah LAN (*Local Area Network*) atau membagi sebuah LAN menjadi dua buah segmen. Tujuannya adalah untuk mengurangi *traffic* sedemikian rupa sehingga dapat meningkatkan performa *network* [2].

4. Switch/Hub

Switch adalah *bridge* yang memiliki banyak port, sehingga disebut sebagai *multiport bridge*. *Switch* berfungsi sebagai sentral atau konsestrator pada sebuah *network*. *Switch* dapat mempelajari alamat *hardware* *host* tujuan, sehingga informasi berupa data bisa langsung dikirim ke *host* tujuan [2]. *hub* mirip dengan *switch*, namun *hub* tidak secerdas *switch*. Jika *switch* mengirim suatu informasi langsung dikirim ke *host* tujuan, kalau *hub* mengirim informasi tersebut kesemua *host*. Kondisi seperti ini menyebabkan beban *traffic* yang tinggi. Oleh sebab itu, *hub* biasanya digunakan pada *network* berskala kecil, seperti *network* di Lab.komputer sekolah, warnet dll.

5. Network Interface Card (Nic)

Network interface card (NIC) adalah expansion board yang digunakan supaya komputer dapat dihubungkan dengan jaringan. sebagian besar NIC dirancang untuk jaringan, protokol, dan media tertentu. NIC biasa disebut dengan LAN card (*Local Area Network Card*) [4].

D. IP Address

IP Address merupakan singkatan dari *Internet Protocol Address*, *IP Address* adalah identitas numeric yang diberikan kepada suatu alat seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protokol sebagai sarana komunikasi, *IP Address* memiliki dua fungsi yaitu[5] :

1. Sebagai alat identifikasi host atau antarmuka pada jaringan.
2. Sebagai alamat lokasi jaringan.

IP Address sendiri memakai system bilangan 32 bit, system ini dikenal dengan nama *Internet Protocol* version 4 atau IPv4. Saat ini IPv4 masih ramai digunakan, untuk memudahkan dalam pembagiannya maka *IP Address* dibagi ke dalam kelas-kelas yang berbeda, yaitu sebagai berikut [5]:

1. Kelas A

IP Address kelas A terdiri atas 8 bit untuk *network ID* dan sisanya 24 bit digunakan untuk *host ID*, sehingga *IP Address* kelas A digunakan untuk jaringan dengan jumlah *host* sangat besar. Pada bit pertama diberikan angka 0 sampai dengan 127 [5].

2. Kelas B

IP Address kelas B terdiri atas 16 bit untuk *network ID* dan sisanya 16 bit digunakan untuk *host ID*, sehingga *IP Address* kelas B digunakan untuk jaringan dengan jumlah *host* tidak terlalu besar. Pada 2 bit pertama, diberikan angka 10 [5].

3. Kelas C

IP Address kelas C terdiri atas 24 bit untuk *network ID* dan sisanya 8 bit digunakan untuk *host ID*, sehingga *IP Address* kelas C digunakan untuk jaringan berukuran kecil. Kelas C biasanya digunakan untuk jaringan *Local Area Network* atau LAN. Pada 3 bit pertama, diberikan angka 110 [5].

Kelas *IP Address* lainnya adalah D dan E, namun kelas IP D dan E tersebut tidak digunakan untuk alokasi IP secara normal tetapi digunakan untuk *IP multicasting* dan untuk eksperimental [5].

Nilai *subnet mask* berfungsi untuk memisahkan *network ID* dengan *host ID*. *Subnet mask* diperlukan oleh TCP/IP untuk menentukan, apakah jaringan yang dimaksud adalah jaringan lokal atau nonlokal. Untuk jaringan Nonlokal berarti TCP/IP harus mengirimkan paket data melalui sebuah *Router*. Dengan demikian, diperlukan *address mask* untuk menyaring *IP Address* dan paket data yang keluar masuk jaringan tersebut [5].

Network ID dan *host ID* didalam *IP Address* dibedakan oleh penggunaan *subnet mask*. Masing-masing *subnet mask* menggunakan pola nomor 32-bit yang merupakan *bit groups* dari semua satu (1) yang menunjukkan *network ID* dan semua nol (0) menunjukkan *host ID* dari porsi *IP Address*[5].

E. Access Control List

Metode Packet Filtering Based merupakan konsep dasar dari paket *filtering* router[10]. Kita dapat membuat suatu aturan untuk meneruskan atau menolak akses dari dalam dan luar jaringan. Sedangkan menurut Rafiudin menyimpulkan bahwa "*Traffic Filtering* merupakan teknik untuk mengontrol trafik- trafik yang di *forward* ke dan dari sebuah jaringan melintasi *router*"[11]. *Access List* mengijinkan atau menolak pernyataan bahwa *filter traffic* dapat ke segmen jaringan dan dari segi segmen jaringan berdasarkan pada alamat sumber, alamat tujuan, tipe protokol dan nomor *port* dari paket.

Penggunaan *access list* yang paling umum digunakan adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan. Sebagai contoh yaitu mengatur *access list* untuk membuat keputusan yang sangat spesifik tentang peraturan pola lalu lintas sehingga *access list* hanya memperbolehkan *host* tertentu untuk mengakses sumber daya WWW sementara yang lainnya di tolak. *List* atau daftar yang telah dibuat pada *access list* bisa diterapkan baik kepada lalu lintas *inbound* maupun *outbound* pada *interface* mana saja. Menerapkan *ACLs* menyebabkan *router* menganalisa setiap paket arah spesifik yang melalui *interface* tersebut dan mengambil tindakan yang sesuai.

Urutan *statement access list* sangatlah penting. Saat *router* memutuskan apakah perlu mem-*forward* atau memblokir sebuah paket, *software cisco IOS* mengetes paket tersebut untuk setiap statemen kriteria dalam urutan yang sesuai saat mereka dibuat. Setelah tidak ada lagi statemen yang dicek. Jadi, saat kita membuat sebuah statemen kriteria yang secara pasti membuka/ mengizinkan semua trafik maka statemen- statemen berikutnya yang ditambahkan tidak lagi akan di cek. Ada dua tipe *access list* yaitu :

1. Standard Access List

Standard access list hanya digunakan untuk *filtering address* sumber *IP/ IPX*. *Standard access list* merupakan bentuk sederhana dari *traffic filtering*. Kita dapat menggunakan untuk memfilter paket- paket berdasarkan *IP Address* sumber (*source address*) paket. Berikut adalah *sintaks* dasar *standard access list* : *access-list[list number] [permit| deny] [ip address] [wildcard mask][log]*.

2. Extended Access List

Extended access list digunakan untuk *filtering* lebih kompleks, seperti *filtering* berdasarkan jenis protokol, *address* sumber dan tujuan, *port- port (TCP/ UDP)* sumber dan tujuan dan tipe- tipe pesan (*ICMP/ IGMP*). *Extended access list* mampu menjawab keterbatasan *standard access list*. *Sintaks extended access list* adalah sebagai berikut: *Access-list [list number] [permit | deny] [protocol] [source specification] [destination specification] [protocol qualification]*

III. METODE PENELITIAN

Dalam memudahkan pembuatan dan pengumpulan data-data yang diperlukan dalam penelitian ini, maka peneliti menggunakan metode penelitian sebagai berikut :

1. Teknik Pengumpulan Data

Teknik yang dilakukan untuk pengumpulan data adalah sebagai berikut :

a. Observasi

Penulis melakukan pengamatan langsung mengadakan kunjungan dan menganalisa jaringan komputer yang ada di PT. Usaha Entertainment Indonesia.

b. Wawancara

Untuk mendapatkan informasi atau data yang diperlukan dalam penulisan skripsi ini penulis melakukan wawancara dengan *General Manajer* PT. Usaha Entertainment Indonesia dan *Staff Network Administrator*.

c. Studi Pustaka

Metode ini merupakan cara untuk mendapatkan data-data secara teoritis sebagai bahan penunjang dalam penyusunan penelitian dengan cara mempelajari, meneliti dan menelaah berbagai literatur-literatur dari perpustakaan maupun dari buku-buku referensinya lainnya, juga dari situs-situs internet yang berkaitan dengan topik penelitian.

2. Analisa Penelitian

Dalam melakukan penelitian, penulis melakukan riset di kantor pusat yang berada di SCBD Sudirman Jakarta, dalam melakukan pengujian dan implementasi penulis menggunakan *software cisco packet tracer 6.0.1* sebagai sarana untuk simulasi. Analisa penelitian yang dilakukan terdiri dari :

a. Analisa Kebutuhan

Jaringan PT. Usaha Entertainment Indonesia termasuk dalam Jaringan *Wide Area Network*. Dimana, Infrastruktur jaringan kantor pusat dan kantor cabang tertata dengan baik. Dalam melakukan penelitian ini, penulis perlu memahami spesifikasi dari perangkat keras yang digunakan antara lain: *Router, Switch, Access Point* dan *software cisco packet tracer 6.0.1* untuk simulasi agar kebutuhan tentang penelitian berjalan dengan lancar.

b. Desain

Design yang akan penulis gunakan adalah sesuai dengan Jaringan komputer PT. Usaha Entertainment Indonesia baik kantor pusat dan kantor cabang. Topologi jaringan komputer di kantor pusat dan kantor cabang menggunakan topologi jaringan *Star*.

c. Testing

Testing sangatlah dibutuhkan untuk melihat apakah konfigurasinya sudah benar atau masih ada kesalahan, untuk itu testing di lakukan pada aplikasi *cisco packet tracer 6.0.1*, yaitu dengan cara memberikan pesan dari jaringan kantor pusat ke jaringan kantor cabang di Bali.

d. Implementasi

Dalam melakukan implementasi, PT. Usaha Entertainment Indonesia akan membutuhkan peran serta dari *Internet*

Service Provider (ISP) sebagai penyedia jaringan *Virtual Privat Network (VPN)* untuk kebutuhan jaringan *internet* dari kantor pusat dan cabang. Namun untuk menghubungkan jaringan kantor pusat dan kantor cabang tetap menggunakan aplikasi *cisco packet tracer 6.0.1*.

IV. HASIL DAN PEMBAHASAN

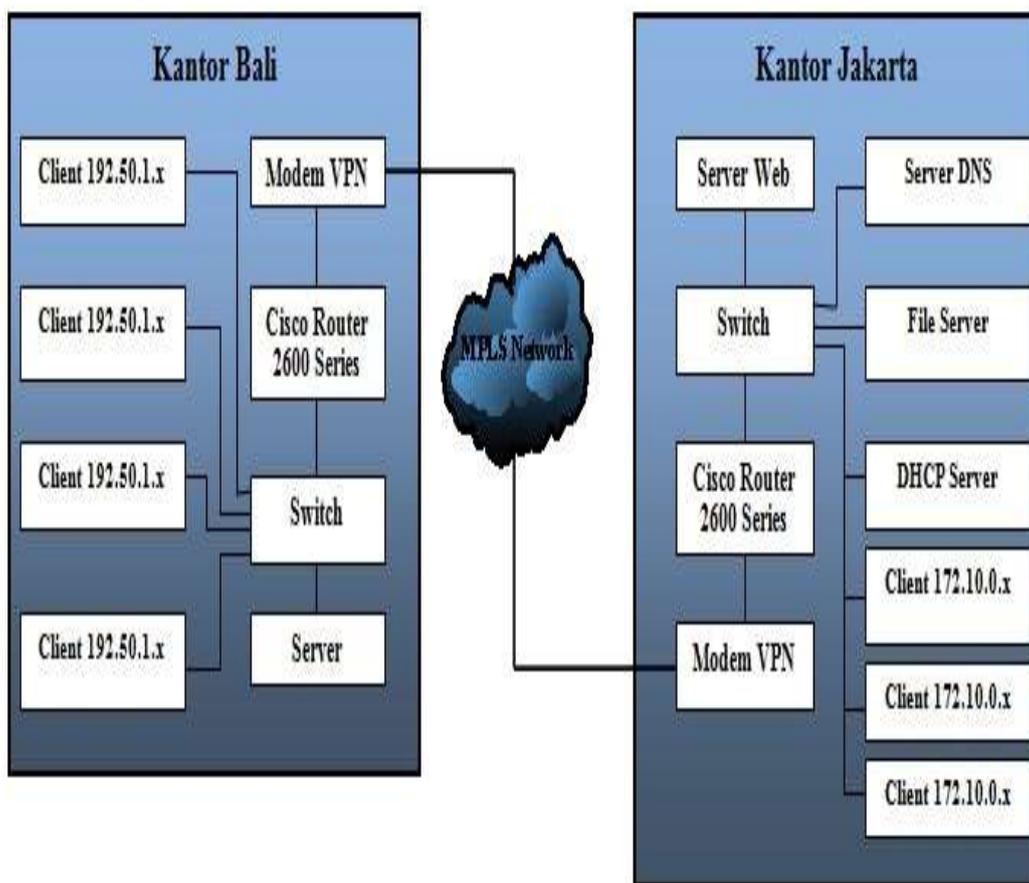
Dalam pembahasan ini peneliti membahas tentang jaringan yang sedang diterapkan di perusahaan dan usulan jaringan yang penulis usulkan.

A. Jaringan yang sedang diterapkan

Pembahasan ini peneliti akan membahas tentang topologi jaringan, arsitektur jaringan, skema jaringan dan keamanan jaringan.

1. Topologi jaringan

Topologi jaringan merupakan sebuah pola rancang bangun untuk membentuk sebuah arsitektur jaringan. Topologi yang digunakan dalam WAN PT. Usaha Entertainment Indonesia di kantor pusat Jakarta maupun di kantor cabang Bali adalah topologi star. Karena topologi star merupakan topologi yang paling bagus digunakan untuk *client server*. Setiap komponen dihubungkan langsung ke switch pusat sehingga pengelolaan semakin mudah dan jika terjadi kegagalan komunikasi mudah untuk ditelusuri. Jika terjadi kegagalan pada satu komponen atau terminal tidak mempengaruhi komunikasi terminal lainnya. Selain itu, kontrol terpusat sehingga memudahkan dalam deteksi dan isolasi kesalahan serta memudahkan pengelolaan jaringan.



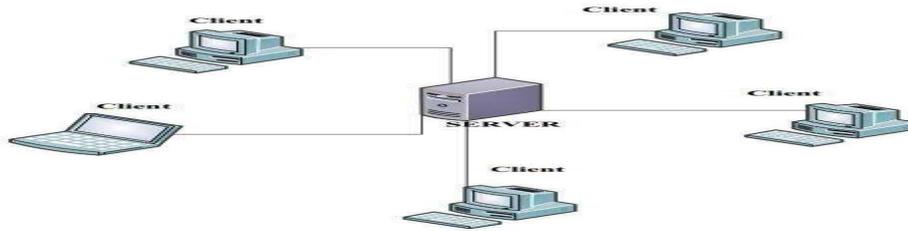
Sumber : Divisi IT PT. Usaha Entertainment Indonesia (2015)

Gambar 1. Topologi Jaringan PT. Usaha Entertainment Indonesia

2. Arsitektur Jaringan

Pada jaringan LAN PT. Usaha Entertainment Indonesia (Dstorm KTV) masing- masing kantor menggunakan jaringan

client server dengan topologi *star*. Topologi star merupakan topologi yang paling banyak digunakan oleh perusahaan-perusahaan dalam memenuhi kebutuhan jaringan komputer.



Sumber : Divisi IT PT. Usaha Entertainment Indonesia (2015)

Gambar 2. Arsitektur Jaringan PT. Usaha Entertainment Indonesia

Pada jaringan komputer kantor Jakarta PT. Usaha Entertainment menggunakan IP Address kelas B dengan gateway 172.10.0.1 dan memiliki empat server antara lain:

a. Web Server

Web server PT. Usaha Entertainment Indonesia yaitu www.dstormktv.com yang nantinya bisa di akses oleh seluruh pengguna jaringan internet. Web server ini menggunakan alamat IP 172.10.0.2.

b. DNS Server

DNS Server merupakan server yang dimiliki PT. Usaha Entertainment Indonesia untuk sinkronisasi dengan web hosting. Dengan adanya DNS server ini seluruh pengguna internet bisa mengakses website www.dstormktv.com, akan sangat sulit jika mengakses dengan alamat IP Address web server.

c. DHCP Server

DHCP Server dengan alamat IP Address 172.10.0.4 merupakan server yang bertugas untuk memberikan IP Dynamic kepada seluruh pengguna mobile user. Dengan adanya DHCP server ini client akan mendapatkan IP address dari server sesuai dengan range yang telah di

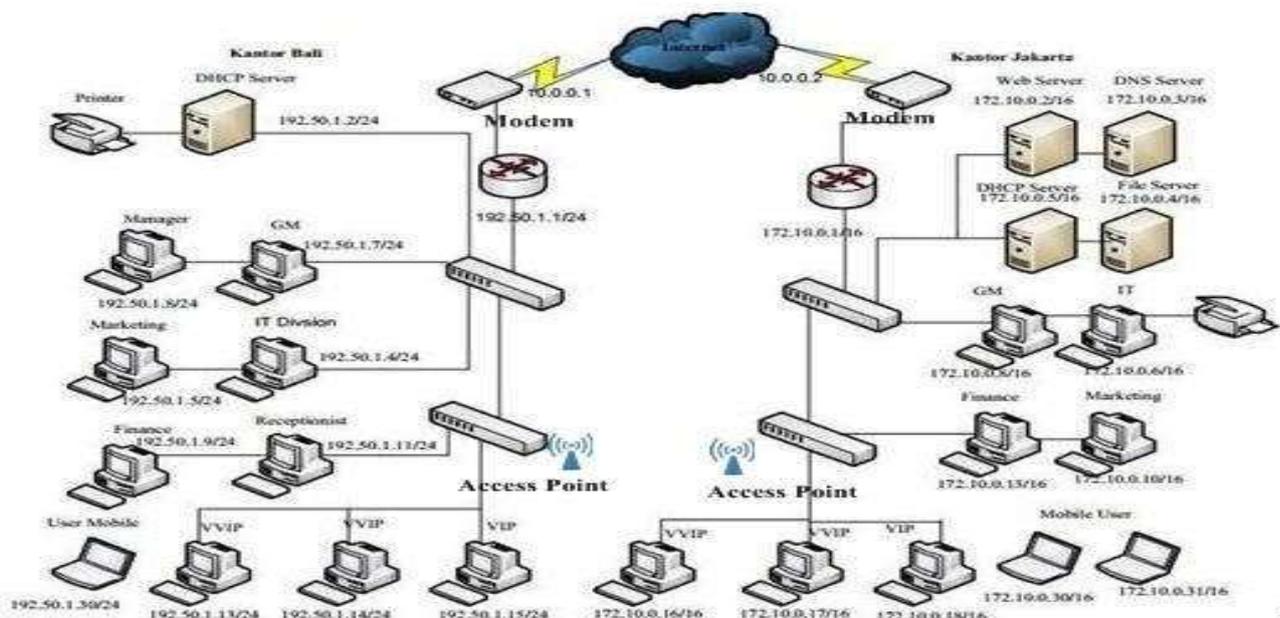
tentukan oleh IT Network. Pada jaringan wireless kantor Jakarta ini IT Network membuat range dimulai dari IP Address 172.10.0.30.

d. File Server

File server dengan alamat IP Address 172.10.0.5 merupakan server yang akan melayani semua fasilitas multimedia. PT. Usaha Entertainment Indonesia adalah salah satu perusahaan yang bergerak di bidang entertainment dengan usahanya adalah karaoke dan meeting room. File server ini berisi data lagu dan seluruh transaksi yang digunakan pada aplikasi.

3. Skema Jaringan

Jaringan yang baik tidaklah identik dengan kecepatan akses saja. Banyak faktor yang mempengaruhi kualitas suatu jaringan. Adapun penjelasan secara menyeluruh dari sistem jaringan yang sedang berjalan, maka penulis mencoba menggambarkan keadaan jaringan komputer yang ada di kantor cabang maupun di kantor pusat PT. Usaha Entertainment Indonesia dengan beberapa perangkat lainnya yang digunakan.



Sumber : Divisi IT PT. Usaha Entertainment Indonesia

Gambar 3. skema Jaringan PT. Usaha Entertainment Indonesia

4. Keamanan Jaringan

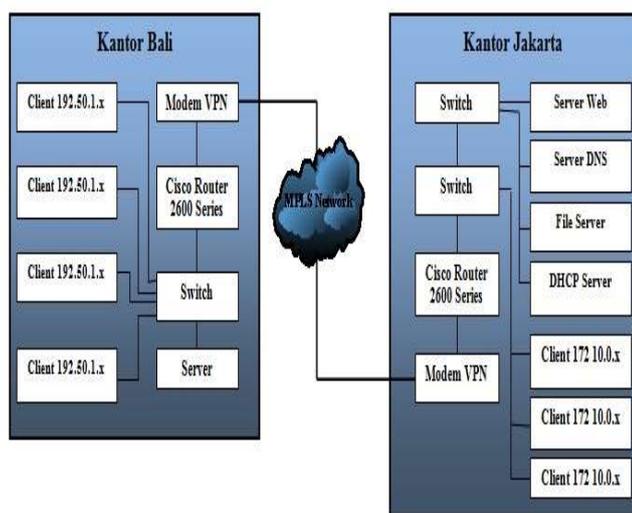
Seiring dengan semakin meningkatnya penggunaan *internet*, hal tersebut memberikan celah keamanan pada jaringan WAN PT. Usaha Entertainment Indonesia. Untuk mengatasi hal tersebut *Staff Network Administrator* hanya mengimplementasikan *antivirus* guna menghindari adanya *virus yang bersifat free* yang masuk pada jaringan dan menggunakan *authentication* pada semua perangkat *mobile*. Selain itu, tidak ada *firewall* yang mampu menangkal serangan dari luar dan juga tidak adanya manajemen *user* seperti *access list*.

B. Jaringan Usulan

Pembahasan ini penulis akan membahas tentang topologi jaringan berjalan, arsitektur jaringan, skema jaringan dan keamanan jaringan, Rancangan Aplikasi, Manajemen Jaringan, keamanan jaringan, Pengujian Jaringan Awal, Pengujian Jaringan Akhir yang penulis usulkan pada PT. Usaha Entertainment Indonesia.

1. Topologi Jaringan usulan

Berdasarkan analisa yang ada pada jaringan PT. Usaha Entertainment Indonesia penulis memberikan usulan agar semua komputer *server* yang ada di Kantor Jakarta di pisahkan sendiri dalam satu *switch*, artinya penambahan satu infrastruktur berupa *switch* agar mempermudah dalam upaya *maintenance* dan kemungkinan jika perusahaan menginginkan teknologi lain misalnya adalah *Virtual Local Area Network (VLAN)*. Dengan adanya penggunaan VLAN ini, jaringan perusahaan akan lebih efisien karena mampu menghindari adanya *collusion* atau tabrakan data. Sedangkan pada kantor Bali, penulis tidak memberikan usulan topologi apapun karena masih mampu untuk mengatasi dan dilihat dari segi kebutuhan masih bisa mampu mengakomodir kebutuhan jaringan yang ada.

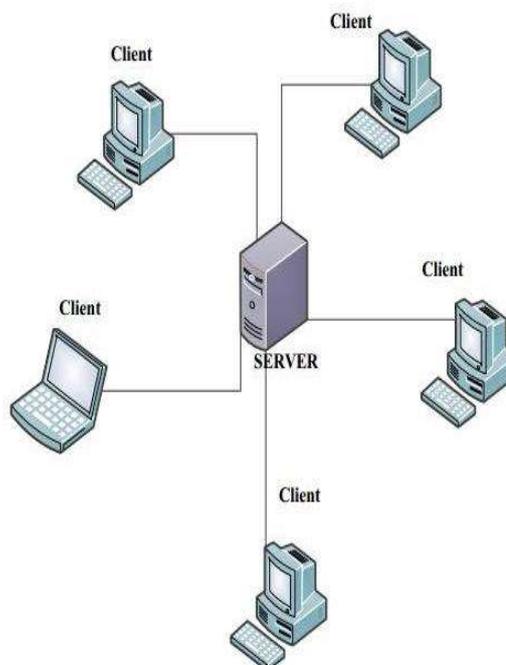


Sumber : Hasil Penelitian (2015)

Gambar 4. Topologi Usulan Kantor Jakarta

2. Arsitektur Jaringan Usulan

Pada jaringan LAN PT. Usaha Entertainment Indonesia (Dstorm KTV) masing- masing kantor menggunakan jaringan *client server* dengan topologi *star*. Topologi star merupakan topologi yang paling banyak digunakan oleh perusahaan-perusahaan dalam memenuhi kebutuhan jaringan komputer.



Sumber : Hasil Penelitian (2015)

Gambar 5. Arsitektur Jaringan

Pada jaringan komputer kantor Jakarta PT. Usaha Entertainment menggunakan *IP Address* kelas B dengan gateway 172.10.0.1 dan memiliki empat *server* antara lain:

a. Web Server

Web server PT. Usaha Entertainment Indonesia yaitu www.dstormktv.com yang nantinya bisa di akses oleh seluruh pengguna jaringan *internet*. *Web server* ini menggunakan alamat IP 172.10.0.2.

b. DNS Server

DNS Server merupakan *server* yang dimiliki PT. Usaha Entertainment Indonesia untuk sinkronisasi dengan *web hosting*. Dengan adanya *DNS server* ini seluruh pengguna *internet* bisa mengakses *website* www.dstormktv.com, akan sangat sulit jika mengakses dengan alamat *IP Address* *web server*.

c. DHCP Server

DHCP Server dengan alamat *IP Address* 172.10.0.4 merupakan *server* yang bertugas untuk memberikan *IP Dynamic* kepada seluruh pengguna *mobile user*. Dengan adanya *DHCP server* ini *client* akan mendapatkan *IP address* dari *server* sesuai dengan *range* yang telah di tentukan oleh *IT Network*. Pada jaringan *wireless* kantor

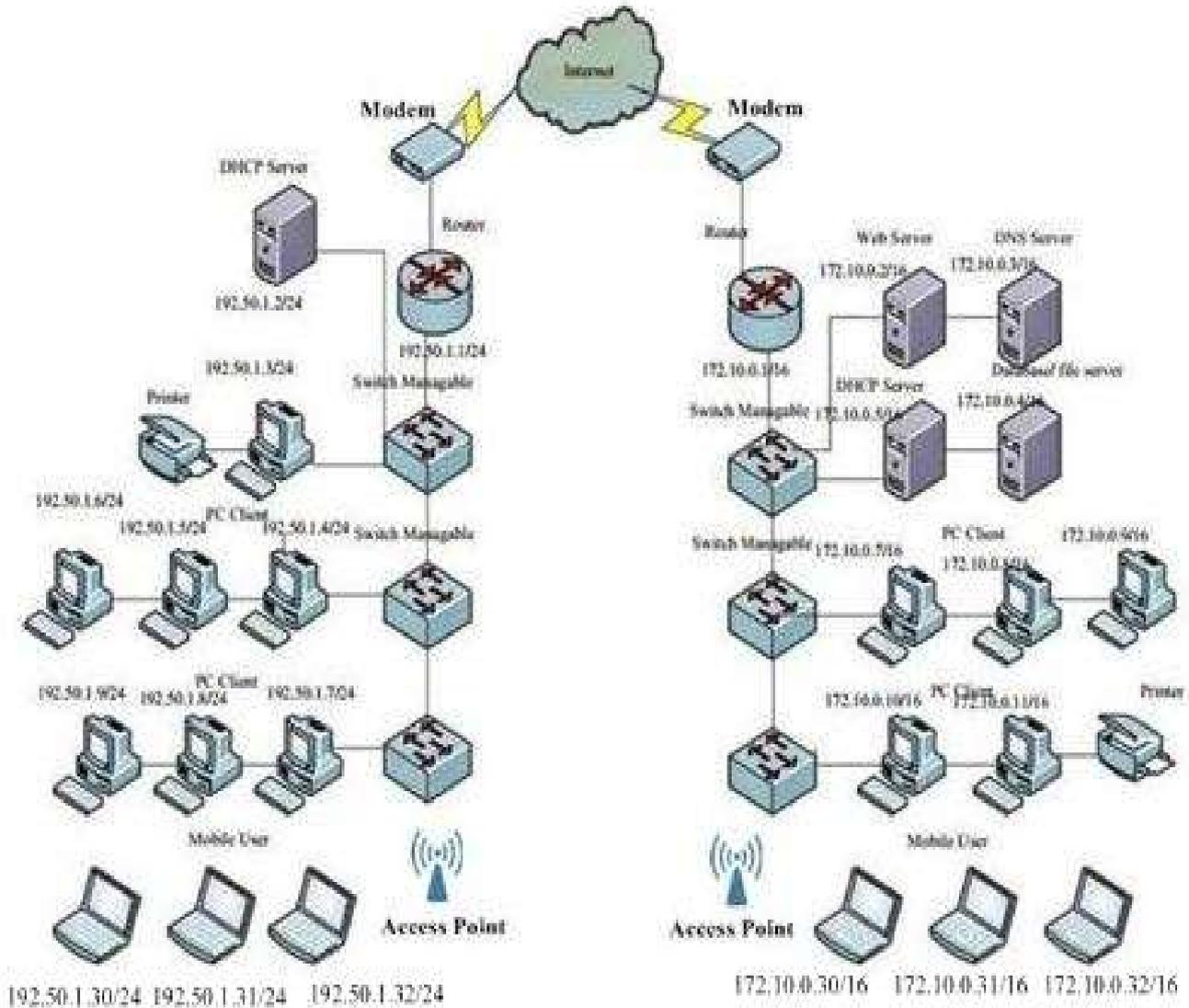
Jakarta ini *IT Network* membuat *range* dimulai dari IP Address 172.10.0.30.

d. File Server

File server dengan alamat *IP Address* 172.10.0.5 merupakan *server* yang akan melayani semua fasilitas multimedia. PT .Usaha Entertainment Indonesia adalah salah satu perusahaan yang bergerak di bidang *entertainment* dengan usahanya adalah karaoke dan *meeting room*. *File server* ini berisi data lagu dan seluruh transaksi yang digunakan pada aplikasi.

3. Skema Jaringan Usulan

Pada usulan jaringan *Wide Area Network (WAN)* PT. Usaha Entertainment Indonesia, penulis menambahkan satu infrastruktur *switch manageable* yang bisa digunakan jika ke depannya perusahaan menginginkan teknologi *virtual* sehingga dapat mempermudah untuk segmentasi. dapat dilihat pada gambar 6:



Sumber : Hasil Penelitian (2015)

Gambar 6. Skema jaringan usulan



4. Manajemen Jaringan

Manajemen jaringan merupakan sebuah fungsi pengawasan terhadap kinerja jaringan dan mengambil tindakan untuk mengendalikan aliran trafik agar kapasitas pengoperasian pada sebuah jaringan dapat dilakukan secara maksimal. Protokol yang sering digunakan dalam implementasi manajemen jaringan adalah *Simple Network Management Protocol (SNMP)*. *SNMP* adalah sebuah protokol yang dirancang untuk memberikan kemampuan untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Jenis *Simple Network Management Protocol (SNMP)* yang paling banyak digunakan adalah *Network Management Station (NMS)* yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan. Peralatan yang dimanage menjalankan *SNMP agent*, yaitu proses *background* yang memonitor peralatan tersebut dan mengkomunikasikannya ke *network management station*. *Cisco ruter* sudah memiliki peralatan yang memiliki *SNMP agent*, sedangkan untuk pencatatan data dapat menggunakan aplikasi *Multi Router Traffic Grapher (MRTG)*. Pengolahan *Simple Network Management Protocol (SNMP)* dijalankan dengan mengumpulkan data dan melakukan penetapan terhadap variabel- variabel dalam elemen jaringan yang di kelola. Keamanan Jaringan.

5. Kemananan Jaringan

Berdasarkan penelitian yang dilakukan penulis, keamanan jaringan di PT. Usaha Entertainment Indonesia masih kurang mencukupi, oleh karena itu penulis memberikan solusi agar keamanan jaringan komputer di PT. Usaha Entertainment Indonesia menjadi lebih aman. Adapun yang menjadi usulan penulis antara lain:

1. Firewall

Network firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya di jumpai dalam dua bentuk yakni sebuah perangkat terdedikasi atau sebuah perangkat lunak yang diinstalasikan dalam sebuah *server*. Contoh *firewall* yang penulis rekomendasikan adalah *Microsoft Internet Security and Acceleration Server (ISA)*.

2. Metode Access Control list

Metode access control list pada dasarnya adalah memfilter *permit* atau *deny* suatu paket data yang akan keluar dari jaringan maupun yang akan masuk pada suatu jaringan komputer. Untuk itu penulis membuat rules atau aturan yang harus di konfigurasi.

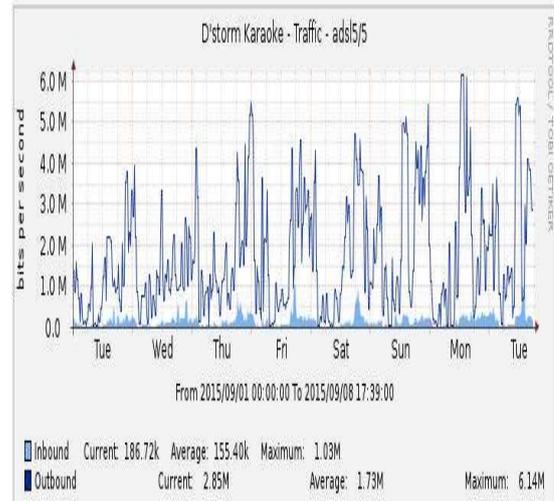
6. Pengujian

Dalam hal pengujian keamanan jaringan penulis menggunakan pengujian keamanan jaringan menggunakan dua langkah pengujian yaitu:

1. Pengujian jaringan Awal

a. Pada pengujian keamanan jaringan awal ini penulis mencoba Pengujian traffic menggunakan *MRTG (Multi Router Traffic Grapher)*, pengujian ini dilakukan dengan menggunakan aplikasi yang telah diberikan oleh pihak

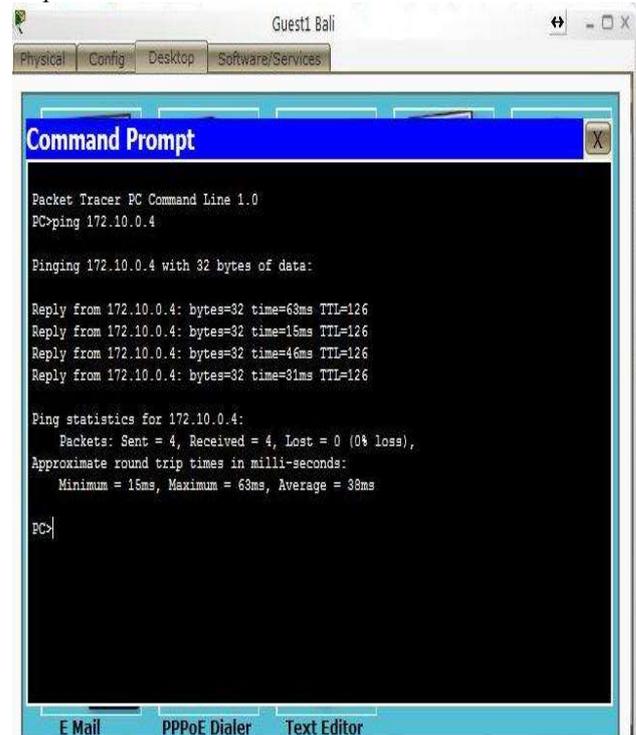
ISP (Internet Services Provider) melalui link dalam bentuk html dan bisa dikases dengan internet.



Sumber : Hasil Penelitian (2015)

Gambar 7. Multi Router Traffic Grapher

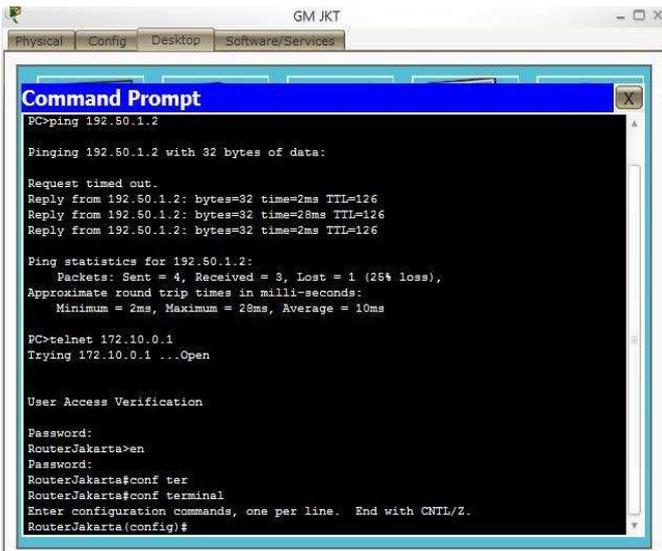
b. Pengujian jaringan kantor Jakarta dengan kantor bali melalui simulasi *cisco packet tracer*, melalui tes *protocol ICMP* antara user Jakarta.



Sumber : Hasil Penelitian (2015)

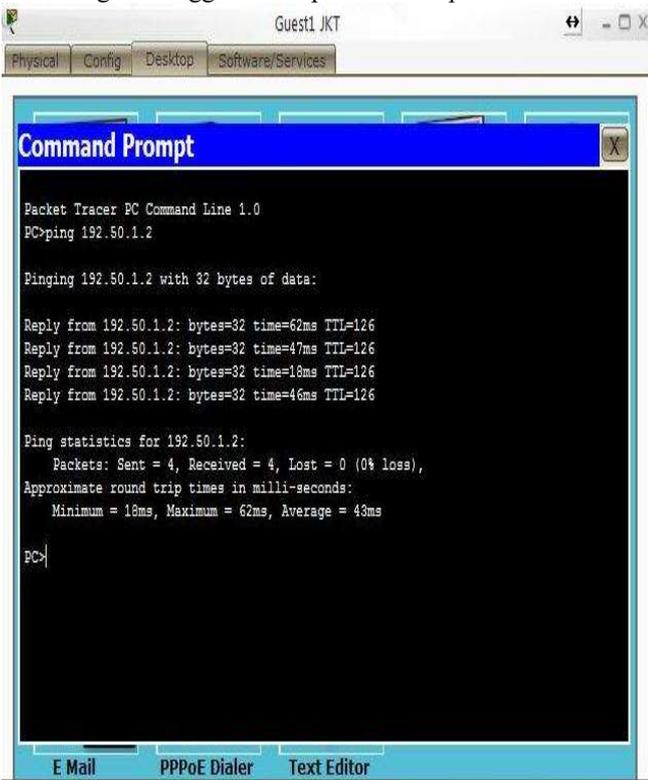
Gambar 8. Guest1 Bali permit ICMP user Jakarta

c. Pengujian jaringan kantor Jakarta user *General Manager* melakukan *Telnet router* Jakarta dengan menggunakan aplikasi *cisco packet tracer*.



Sumber : Hasil Penelitian (2015)
Gambar 9. General Manager Jakarta Permit Telnet

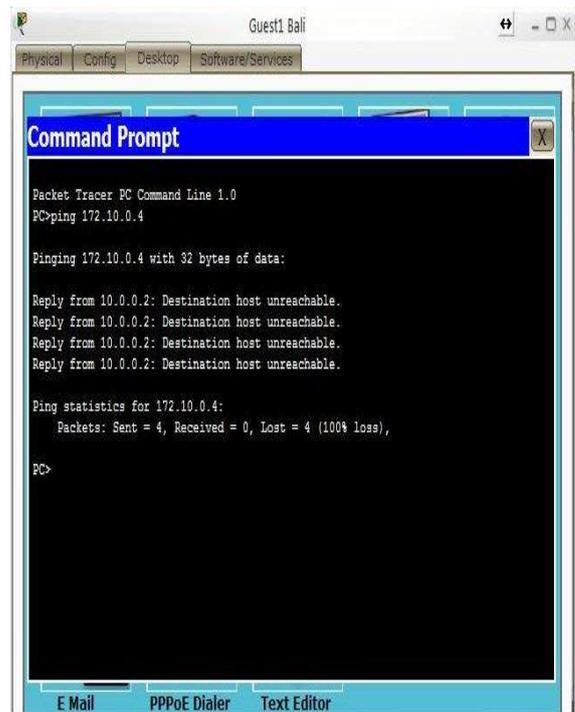
- d. Pengujian *Guest1* Jakarta *permit ICMP user network* Bali dengan menggunakan aplikasi *cisco packet tracer*.



Sumber : Hasil Penelitian (2015)
Gambar 10. *Guest1* Jakarta *permit ICMP User* Bali

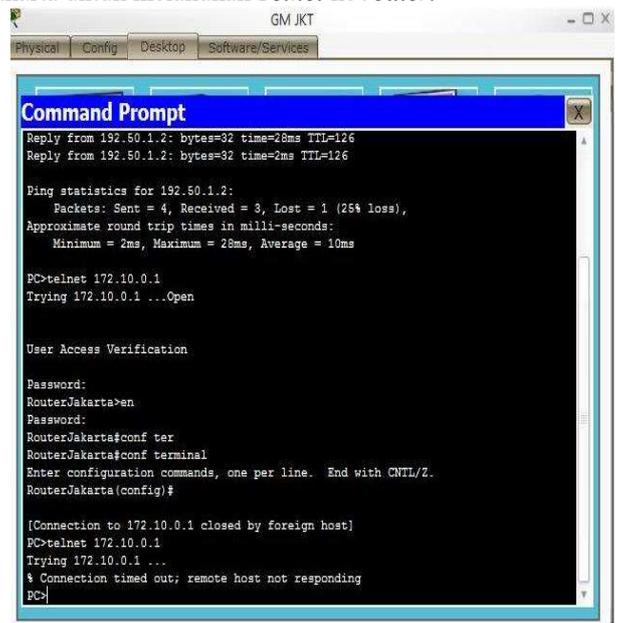
2. Pengujian Jaringan Akhir

- a. Melakukan penolakan (*deny*) terhadap paket dari *user* kantor Bali ke *user* kantor Jakarta melalui *protocol ICMP*.



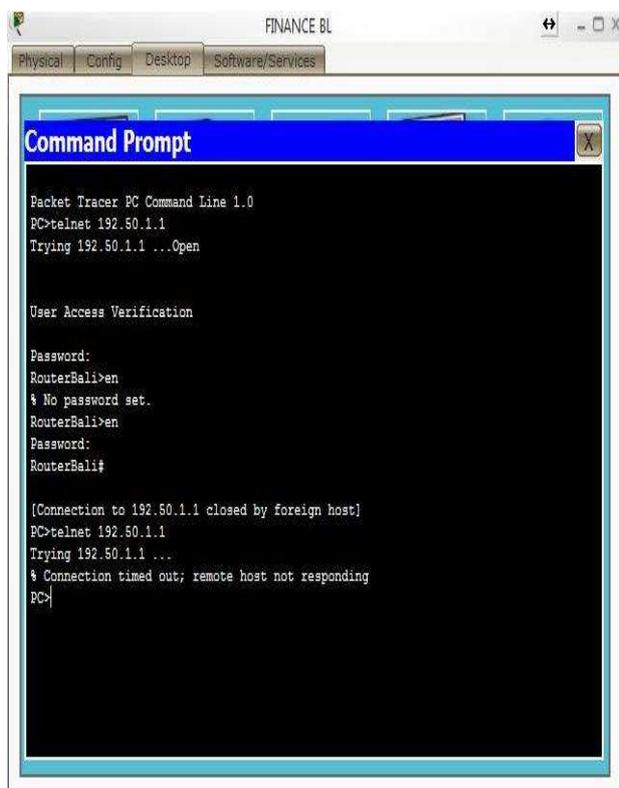
Sumber : Hasil Penelitian (2015)
Gambar 11. *Guest1* Bali deny ICMP to Netwok Jakarta

- b. Melakukan penolakan (*deny*) terhadap General Manager Jakarta untuk melakukan *Telnet* ke *router*.



Sumber : Hasil Penelitian (2015)
Gambar 12. *Host General Manager* Jakarta deny telnet router

- c. Melakukan penolakan (*deny*) terhadap *user finance* kantor bali untuk melakukan *terlnet* router bali.



Sumber : Hasil Penelitian (2015)

Gambar 13. Deny user finance bali telnet router bali

V. KESIMPULAN

Selama melakukan penelitian, penulis banyak menemukan kendala baik dalam instalasi serta konfigurasi jaringan komputer dan juga konfigurasi perangkat-perangkat jaringan seperti *router* dan peran serta *Internet Service Provider (ISP)* sebagai penyedia layanan *Virtual Private Network (VPN)* untuk *internet*. Tentunya kendala ini menjadi pengalaman yang sangat berguna pada waktu dan kesempatan yang lain khususnya dalam perancangan jaringan *Wide Area Network (WAN)* bagi penulis. Dari penelitian yang dilakukan penulis, maka dapat ditarik kesimpulan bahwa:

1. Dengan *access control list*, lalu lintas (*traffic*) data di jaringan *Wide Area Network* PT. Usaha Entertainment Indonesia lebih efisien.
2. *Access control list* bisa menghindari adanya akses data yang tidak di perlukan dalam jaringan.
3. Dengan *access control list* serta penambahan *firewall* akan sangat meningkatkan kemampuan dalam hal kewanaman jaringan komputer.

REFERENSI

- [1] Rochim, Adian Fatchur, Andrian Satria Martiyanto. Desain dan Implementasi Web Proxy dan VPN ISSN: 2087-4685.

Semarang: Jurnal Sistem Komputer - Vol. 1 No. 1 Tahun 2011. 2011.

- [2] Aditya, A. Mahir Membuat Jaringan Komputer. Jakarta: Dunia Komputer. 2011
- [3] Wagito. Jaringan Komputer, Teori dan Implementasi Berbasis Linux. Yogyakarta: Gava Media, 2005.
- [4] Paulus, Y. J. "Computer Networking, Pengaturan Jaringan, Keamanan Jaringan, Koneksi dan sharing, Troubleshooting Jaringan", Yogyakarta: Andi. 2012.
- [5] Winarto, E., Zaki, A., & Community, S. , Membuat Sendiri Jaringan Komputer. Semarang: PT. Elex Media Komputindo, 2013.
- [6] Madcom. Sistem Jaringan Komputer untuk Pemula. Madiun: Andi. 2010.
- [7] Feilner, Markus. OpenVPN, Building and Integrating Virtual Private Networks. Birmingham: Packt Publishing Ltd. 2006.
- [8] Alfin Hikmaturokhan , Adnan Purwanto, Rendy Munadi, Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan Cisco Router. 2010.
- [9] Arifin, Zaenal. Langkah Mudah Membangun Jaringan Komputer. Yogyakarta: Andi Offset. 2005.
- [10] Stiawan, Deris. Sistem Keamanan Komputer. Jakarta: Elex Media Komputindo. 2005.
- [11] Rafiudin, Rahmat. Membangun Firewall dan Traffic Filtering Berbasis Cisco. Jogjakarta: Andi Offset. 2006.



Agus Didi Purwanto, S.Kom. Tahun 2015 lulus dari Program Strata Satu (S1) Program Studi Teknik Informatika STMIK Nusa Mandiri Jakarta. Saat ini bekerja di PT. Usaha Entertainment Indonesia.



Mohammad Badrul. M.Kom. Tahun 2009 lulus dari Program Strata Satu (S1) Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta. Tahun 2012 lulus dari Program Strata Dua (S2) Magister Ilmu Komputer STMIK Nusa Mandiri Jakarta Saat ini mengajar di STMIK Nusa Mandiri Jakarta dengan jabatan fungsional akademik Asisten Ahli dan pada Tahun 2015 telah tersertifikasi dosen.