Paper

Analisis Keamanan Jaringan WAN Dengan Teknik Standart ACL dan Extended AC

Author: **Rizko Liza, Nur Wulan**

SNASTIKOM 10
Seminar Nasional Teknologi Informasi dan Komunikasi
UNIVERSITAS HARAPAN MEDAN 2012-2023
Program Studi Teknik Informatika
TEMA : DUNIA AKADEMIK DI ERA SOCIETY 5.0 : TANTANGAN DAN PELUANG
ISSN : 2964-1950

SNASTIKOM Ke 10 Tahun 2023
ISBN: 2964-1950

Analisis Keamanan Jaringan WAN Dengan Teknik Standart ACL dan Extended AC

Risko Liza[1*], Nur Wulan[2]
[1,2]Universitas Harapan Medan, Medan, Indonesia
[1] riskoliza@unhar.ac.id, [2] nurwulan@unhar.ac.id

[*)] riskoliza@unhar.ac.id

Abstrak

Access Control List (ACL) digunakan sebagai kontrol keamanan jaringan WAN fungsi dari ACL dalam penulisan ini adalah untuk mengatur hak akses dan menyaring lalu lintas data di suatu jaringan dengan mengontrol paket-paket. Karena banyak perusahaan atau kantor-kantor memiliki server sendiri untuk mengolah dan sebagai penyimpanan data perusahaan, dimana perusahaan-perusahaan sekarang mengunakan WAN (Wide Area Network), Jaringan WAN berfungsi untuk menghubungkan komunikasi antar cabang kecabang lainnya tetapi, Pada penulisan ini ACL memiliki 2 (dua) buah teknik yaitu teknik Standart ACL dan Extented ACL yang berfungsi untuk menjaga dan mengatur lalu lintas komunikasi yang padat dalam sebuah jaringan WAN. Karena dalam teknik Standart ACL dam Extended ACL memilik hak akses yang berbeda.

Kata Kunci: Sistem keamanan, Jaringan WAN, ACL, Standart ACL, Extended ACL.

Abstract

Access Control List (ACL) is used as a security control for WAN networks. The function of ACL in this paper is to regulate access rights and filter data traffic on a network by controlling packets. Because many companies or offices have their own servers to process and store company data, companies now use WAN (Wide Area Network). The WAN network functions to connect communications between branches and other branches, however, at this writing ACL has 2 (two) techniques, namely Standard ACL and Extended ACL techniques which function to maintain and manage heavy communication traffic in a WAN network. Because in the Standard ACL and Extended ACL techniques they have different access rights.

Keywords: Security system, WAN Network, ACL, Standard ACL, Extended ACL.

1. PENDAHULUAN

Pertumbuhan pengguna internet di dunia dan di Indonesia terus meningkat seiring dengan perkembangan teknologi Informasi serta perkembangan *website* di Indonesia juga sangat pesat. Perusahaan baik dalam skala besar maupun kecil membutuhkan jaringan komputer untuk melakukan komunikasi dan pertukaran data. Dengan bantuan teknologi komputer yang ada saat ini, perusahaan dapat berkomunikasi dan melakukan pertukaran data kepada divisi–divisi yang lain dalam jarak jauh. Implementasi jaringan ini dilakukan dengan cara menghubungkan komputer yang satu dengan komputer yang lain, dari divisi satu dengan divisi lain dalam jaringan luas disebut *Wide Area Network* (WAN). Jaringan WAN berfungsi agar antara cabang-cabang perusahaan dan pusat perusahaan dapat saling bertukar informasi yang dibutuhkan. Jika ingin dibangun jaringan WAN yang sesungguhnya maka pasti membutuhkan biaya yang cukup besar. Oleh karena itu *Cisco* sebagai perusahaan terkemuka di bidang jaringan meluncurkan sebuah aplikasi yang berfungsi untuk mensimulasikan jaringan komputer, yaitu *Cisco Packet Tracer. Cisco Packet Tracer* adalah sebuah *software* yang dapat digunakan untuk melakukan simulasi jaringan. Dalam metode *Access Control List* (ACL) digunakan sebagai kontrol keamanan jaringan WAN. Adapun referensi yang penulis buat terdapat pada jurnal-jurnal sebelumnya yang sudah pernah dibuat dengan judul "Analisis Penggunaan *Access Control List* (ACL) Dalam Jaringan Komputer Di Kawasan Batamindo Industrial Park Batam" [1] dan "*Extended Access List* untuk Mengendalikan Trafik Jaringan" [2]. *WAN* digunakan untuk menghubungkan jaringan area lokal yang

satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain. [3]. Untuk menjalankan operasi logika AND, tiap bit di dalam IP *Address* dibandingkan dengan bit *subnet mask*. [4]

Model *OSI* adalah suatu dekripsi abstrak mengenai desain lapisan komunikasi dan protokol jaringan komputer yang dikembangkan sebagai bagian dari inisiatif *Open Systems Interconnection* atau disingkat OSI. Model ini disebut dengan model Tujuh Lapisan OSI (OSI sevenlayer model), lapisan tersubut diantaranya: *physical layer*, *data link layer*, *network layer*, *transport layer*, session layer, *presentation layer*, dan *application layer*. [5]. Setiap kata *Router* dalam tulisan berikutnya akan diartikan sebagai *Cisco Router*. [6]. Serangan terhadap keamanan sistem informasi *(security attack)* akhir-akhir ini seringkali terjadi kejahatan komputer/*cybercrime* pada dunia maya seringkali di lakuka oleh kelompok orang yang ingin menembus suatu keaman sebuah sistem[7].

Router menguji semua paket data untuk menentukan apakah paket tersebut diijinkan untuk lewat atau tidak berdasarkan kriteria yang ditentukan di dalam *Access Control List (ACL)*. [8]. Pembuatan jaringan ini memakai 1 buah *server*, 1 buah *switch*, dan 1 buah *PC*. Semua sudah terdapat di dalam aplikasi *Cisco Packet Tracer* tersebut. Langsung saja, berikut langkah-langkahnya[9]

2. METODE PENELITIAN

2.1 Tahap Proses Perancangan

Tahap perancangan yang dilakukan adalah menyiapkan *software* aplikasi Simulasi Jaringan menggunakan *Cisco Packet Tracer 5.3.3* melakukan pembuatan sistem konfigurasi jaringan. Tahap perencanaan merupakan tahap pengumpulan beberapa bahan yang dapat disajikan sebagai landasan awal untuk pendefinisian permasalahan. Pada tahap ini semua permasalahan-permasalahan terkait keamanan jaringan komputer dapat di kumpulkan sehingga di temukan solusi untuk menyelesaikan masalah tersebut. Tahap perencanaan ini di fokuskan kepada kebutuhan-kebutuhan yang terkait pada solusi pemecahan masalah tersebut agar pelaksanaan tahap-tahap selanjutnya lebih terstruktur dan proporsional. Dalam perencanaan ini perencanaan dimulai dengan melakukan analisis. data yang diperoleh kemudian diolah untuk perancangan sistem analisis jaringan atau simulasi jaringan yang akan di buat.

2.2 Tahap Proses Analisis

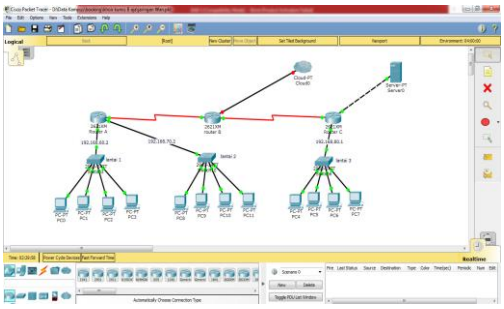
Tahap proses analisis merupakan tahap analisis pengumpulan data atau pendefinisian spesifikasi kebutuhan, fungsi yang akan dibuat difokuskan pada kebutuhan sistem yang akan disampaikan. Hal ini guna mempermudah dalam merancang jaringan WAN menggunakan *stadart acces list* dan *extended acces list* kemudian dianalisis keamanan dari jaringan tersebut

2.3 Identifikasi Masalah

Berdasarkan hasil identifikasi masalah jaringan komputer yang ada maka dilakukan analisis kebutuhan untuk merancang dan mengembangkan jaringan WAN. Maka dari permasalahan diatas itu, rancangan jaringan komputer menggunakan *standart acces list* dan *extended acces list*. dalam membangun sebuah sistem jaringan WAN diperlukan sebuah perangkat router yang berfungsi untuk menghubungkan beberapa *network* atau *device* yang berbeda segmen sehingga saling terhubung antara satu komputer dengan komputer lain.

2.4 Rancangan Topology

Dari analisa kebutuhan perusahaan, maka akan dirancang *topology* yang dapat memenuhi kebutuhan perusahaan.



Gambar 2.1 Rancangan Topologi Jaringan WAN

Gambar 2.1 adalah gambar rancangan topologi logikal yang paling tepat untuk diterapkan. Dari gambar di atas dapat di lihat bahwa jaringan wan menggunakan sebuah router yang berfungsi untuk menghubungkan beberapa *network* atau *device* yang berbeda segmen sehingga saling terhubung antara satu komputer dengan komputer lain. Switch yang terdapat pada setiap lantai akan terhubung ke *switch* lainnya. Hal ini dimaksudkan agar jaringan ini memiliki *redundancy*, dalam membangun jaringan WAN diterapkannya *acces list*. *Access list* adalah pengelompokan paket berdasarkan kategori. *Access list* bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas *network. access list* menjadi *tool* pilihan untuk pengambilan keputusan pada situasi ini.

Berikut rincian pembagian IP *address*:

Tabel 2.1 Tabel Pembagian IP *Addres*

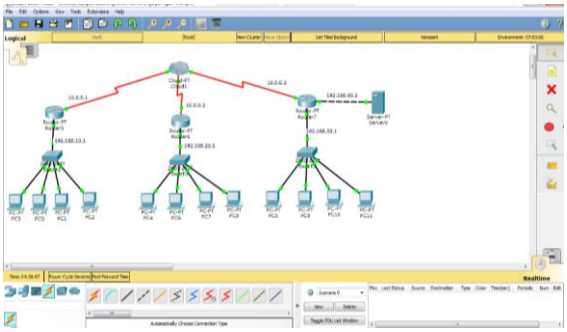
Subnet	IP ADDRES
Lantai 1	192.168.60.0/24
Lantai 2	192.168.70.0/24
Lantai 3	192.168.80.0/24

3. HASIL DAN PEMBAHASAN

Implementasi dari jaringan wan menerapkan teknologi ACL Standart dan Extended memakai perangkat untuk menerapkan keamanan pada suatu jaringan wan, penulis menggunakan simulator *cisco paket tracer* untuk dapat mengimplementasikan jaringan wan tersebut, adapun perangkat keras yang digunakan seperti berikut.

3.1 Tampilan Arsitektur Jaringan WAN

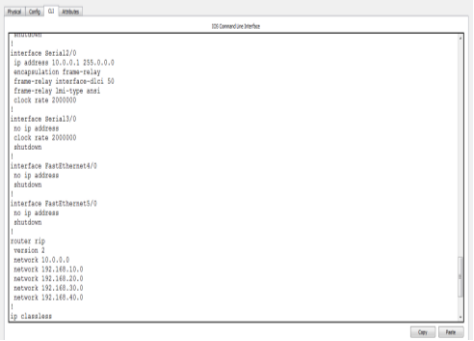
Pada tampilan arsitektur jaringan WAN menggunakan menggunakan *ACL Standart* dan *Extended* yang terdiri dari 3 *switch* yang masing masing terdiri dari 4 komputer dan terdapat *cloud WAN* yang menggunakan *frame-relay* untuk menghubungkan masing masing *router* seperti pada gambar:



Gambar 3.1 Tampilan Jaringan WAN

3.2 Tampilan Show Run Pada Router Gedung A

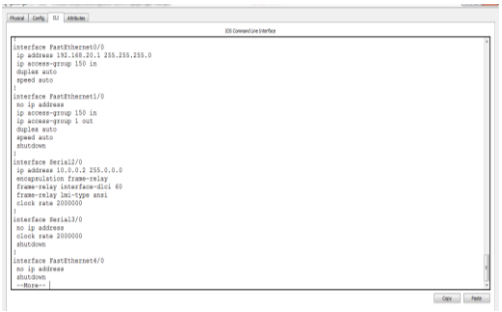
Tampilan *show run* merupakan tampilan yang menampilkan langsung aktifitas yang ada pada jaringan yang dibangun seperti pada perangkat *router*, pada tampilan tersebut terlihat konfigurasi berada di port keberapa beserta *ip address*, lihat gambar:



Gambar 3.2 Tampilan show run

3.3. Tampilan show run pada Router gedung B

Tampilan *show run* merupakan tampilan yang menampilkan langsung aktifitas yang ada pada jaringan yang dibangun seperti pada perangkat router, pada tampilan tersebut terlihat konfigurasi berada di port keberapa beserta *ip address*, lihat gambar:



Gambar 3.3 Tampilan Show Run Pada Router Gedung B

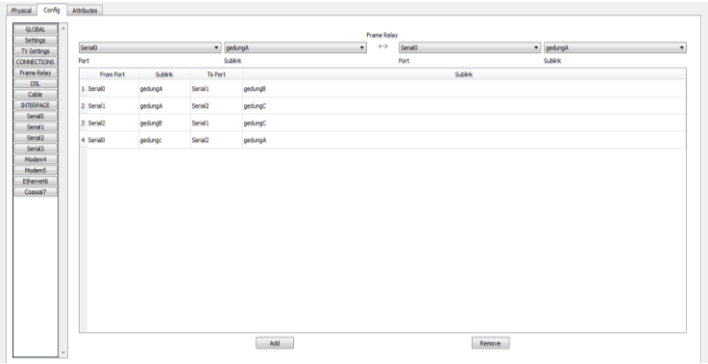
3.4. Tampilan Show Run Pada Router Gedung C

Tampilan *show run* merupakan tampilan yang menampilkan langsung aktifitas yang ada pada jaringan yang dibangun seperti pada perangkat router, pada tampilan tersebut terlihat konfigurasi berada di port keberapa beserta *ip address*, lihat gambar:

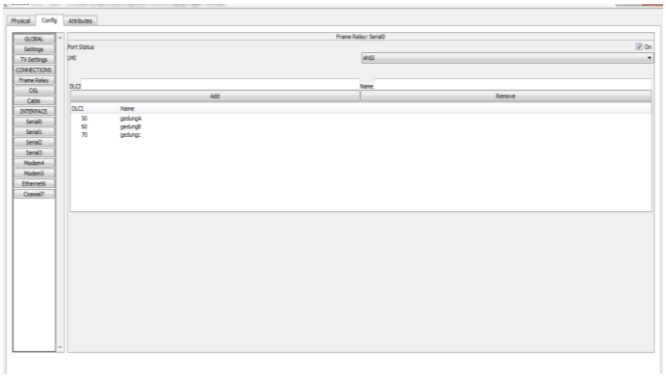
Gambar 3.4 Tampilan Show Run Pada Router Gedung B

3.5 Tampilan Konfigurasi Frame Relay Pada Cloud WAN

Tampilan konfigurasi frame relay merupakan tampilan yang ada pada perangkat cloud yang berfungsi untuk menghubungkan 3 router yang berbeda lokasi, pada port serial 0 terdapat kabel yang dihubungkan menuju port cloud, lihat gambar:



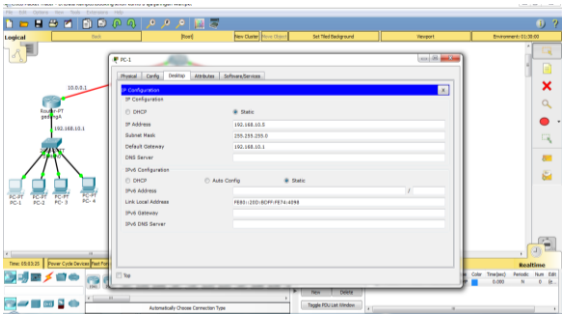
Gambar 3.5 Tampilan Konfigurasi Frame Relay



Gambar 3.6 Tampilan Konfigurasi Port

3.6 Tampilan Setting IP Address Komputer Gedung A

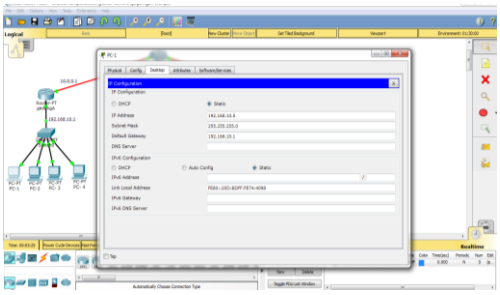
Tampilan setting IP address untuk memberikan alamat ip kepada masing masing komputer atau pc pada komputer yang berada di gedung A yang berfungsi agar dapat terhubung ke jaringan WAN dalam satu jaringan, lihat gambar:



Gambar 3.7 Tampilan Setting Ip Address Komputer Gedung A

3.7 Tampilan Setting IP Address Gedung B

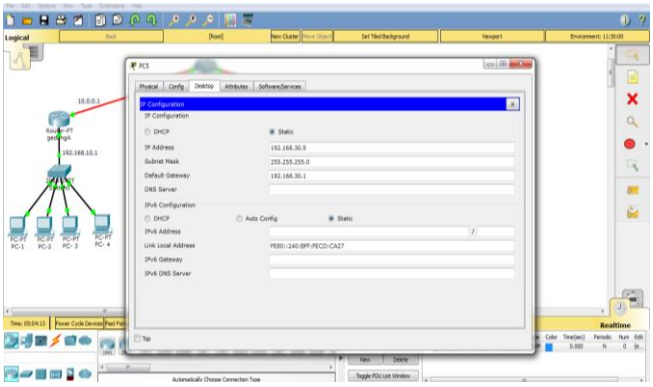
Tampilan setting IP address untuk memberikan alamat ip kepada masing masing komputer atau pc yang berada pada gedung B berfungsi agar dapat terhubung ke jaringaan WAN dalam satu jaringan, lihat gambar:



Gambar 3.8 Tampilan Setting IP Address Gedung B

3.8 Tampilan Setting IP Address Gedung C

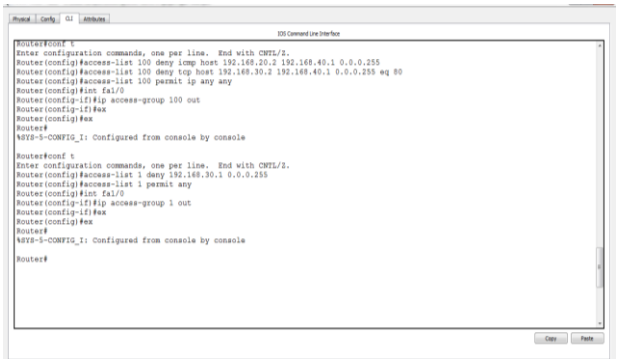
Tampilan setting IP address untuk memberikan alamat ip kepada masing masing komputer atau pc pada gedung C yang berfungsi agar dapat terhubung ke jaringan WAN dalam saru jaringan, lihat gambar:



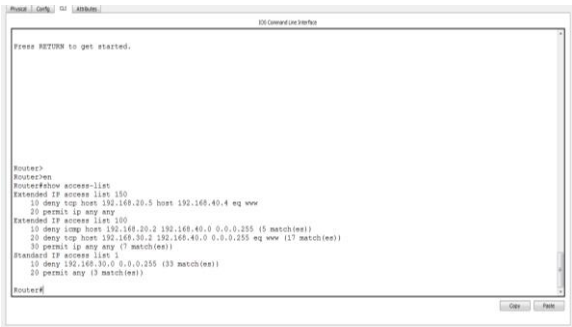
Gambar 3.9 Tampilan setting ip address gedung C

3.9 Tampilan Konfigurasi ACL Standart

Tampilan konfigurasi ACL sebagai konfigurasi yang dilakukan pada perangkat router yang berfungsi melakukan block terhadap ip yang berada pada gedung C menuju ip server. Berikut ini konfigurasi ACL standart seperti pada gambar:



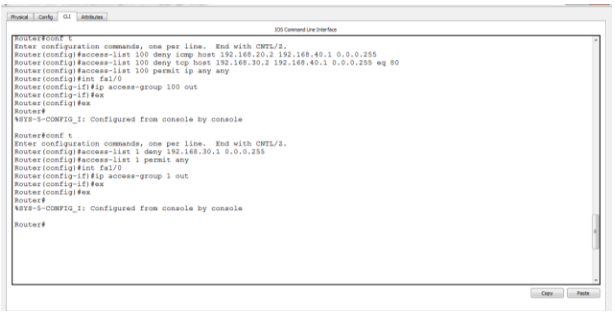
Gambar 3.10 Tampilan konfigurasi ACL Standart



Gambar 3.11 Tampilan konfigurasi show access-list ACL

3.10 Tampilan Konfigurasi ACL Extended

Tampilan konfigurasi ACL sebagai konfigurasi yang dilakukan pada perangkat router yang berfungsi melakukan block terhadap ip yang berada pada gedung A menuju ip yang berada pada gedung B. Berikut ini konfigurasi ACL standart seperti pada gambar:



Gambar 3.12 Tampilan konfigurasi ACL Extended

Gambar 3.13 Tampilan konfigurasi show access-list ACL

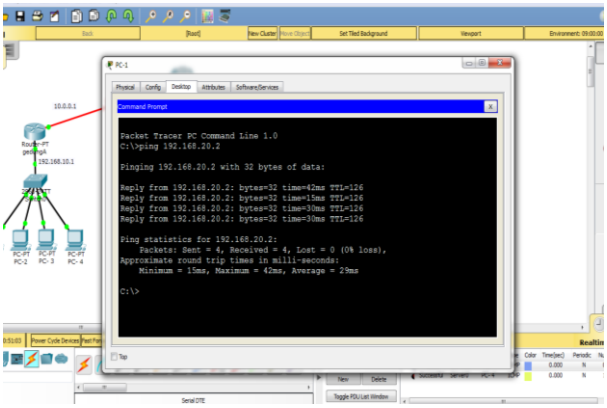
3.11 Tampilan Konfigurasi Router

Tampilan konfigurasi router sebagai konfigurasi yang dilakukan pada perangkat router yang akan akan menghubungkan setiap komputer didalam jaringan.berikut ini konfigurasi router seperti pada gambar:

Gambar 3.14 Tampilan Konfigurasi Router

3.12 Tampilan Tes Koneksi Antara Gedung A Dengan Gedung B

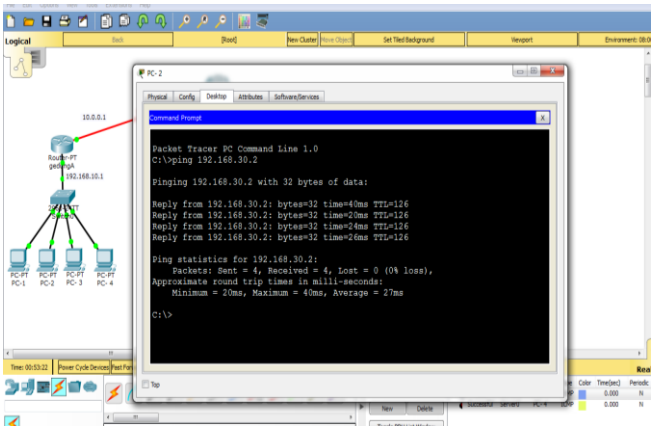
Tampilan ping untuk membuktikan bahwa gedung A dan B terhubung maka dilakukan pengetesan ping dari gedung A menuju Gedung B, seperti pada gambar berikut:



Gambar 3.15 Tampilan Tes Koneksi Antara Gedung A dengan Gedung B

3.13 Tampilan Tes Koneksi Antara Gedung B Dan Gedung C

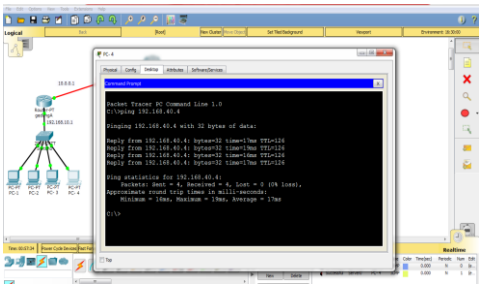
Tampilan ping untuk membuktikan bahwa gedung B dan Gedung C terhubung maka dilakukan pengetesan ping dari gedung B menuju Gedung C, seperti pada gambar berikut:



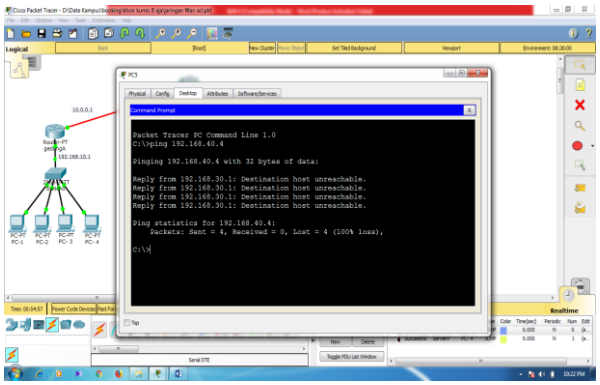
Gambar 3.16 Tampilan Tes Koneksi Antara Gedung B Dan Gedung C

3.14 Tampilan Tes Koneksi Menggunakan Standart ACL

Tampilan ping untuk membuktikan bahwa dalam melakukan penerapan standart ACL perlu dilakukan tes koneksi agar dapat diketahui standart ACL sudah berjalan atau belum, seperti pada gambar berikut:



Gambar 3.17 Tampilan Tes Koneksi Antara Gedung C Dan Server Sebelum Diterapkan Standart ACL

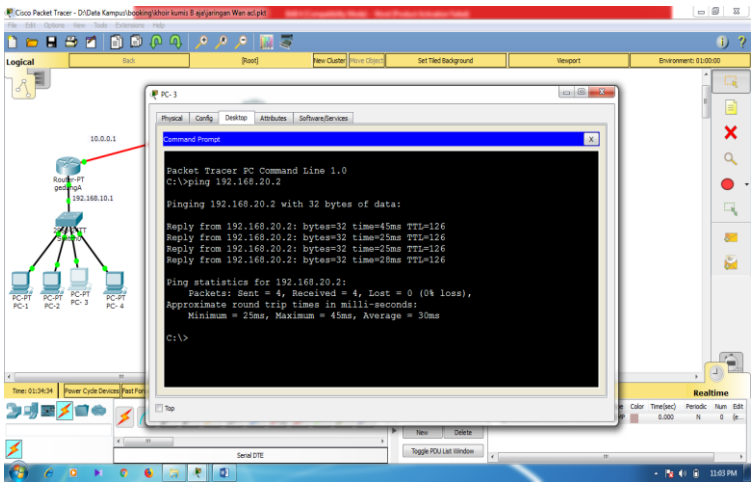


Gambar 4.18 Tampilan Tes Koneksi Antara Gedung C Dan Server Setelah Diterapkan Standart ACL

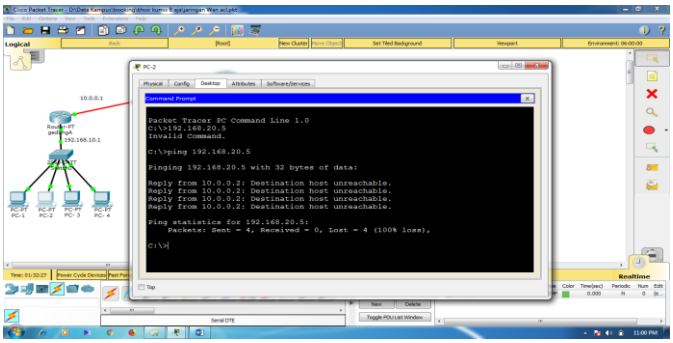
Pada gambar diatas terbukti sebelum melakukan penerapan standart ACL tes koneksi antara gedung C dan server masih terhubung, setelah dilakukan penerapan ACL standart tidak bisa lagi melakukan tes ping karena standart acl menutup akses IP gedung C.

3.15 Tampilan Tes Koneksi Menggunakan Extended ACL

Tampilan ping untuk membuktikan bahwa dalam melakukan penerapan Extended ACL perlu dilakukan tes koneksi agar dapat diketahui extended ACL sudah berjalan atau belum, ketika extended ACL berhasil dilakukan gedung A dengan client 2 menuju gedung B client 1 tidak berhasil dilakukan ping. Seperti pada gambar berikut:



Gambar 4.19 Tampilan Tes Koneksi Antara Gedung A Client 1 Dan Gedung B Clien 1 Sebelum Diterapkan Extended ACL



Gambar 4.20 Tampilan Tes Koneksi Antara Gedung A Client 1dan Gedung B Client 1 Setelah Diterapkan Extended ACL

Pada gambar diatas terbukti sebelum melakukan penerapan standart ACL tes koneksi antara gedung A client 1 dan gedung B client 1 masih terhubung, setelah dilakukan penerapan ACL Extended tidak bisa lagi melakukan tes ping karena extended ACL menutup akses antara client digedung A menuju client digedung B.

4. KESIMPULAN

Dalam uraian rangkaian mulai dari proses implementasi Standart ACL dan Extended ACL, Untuk *Standart ACL* hanya melakukan *filtering* pada alamat sumber *(Source)* dari paket yang dikirimkan. Alamat sumber yang dimaksud dapat berupa alamat sumber dari jaringan *(Network Address)* atau alamat sumber dari *host*. Sebagai yang telah diterapkan pada gedung B dengan *IP address* 192.168.168.20.5 untuk *IP* tersebut hanya dapat berinteraksi atau berkomunikasi dengan server dan *host-host* yang lain seperti pada gedung A, gedung B, dan gedung C. Tapi tidak dapat mengakses web server. Sedangkan untuk *Extended ACL* mampu melakukan *filtering* pada alamat sumber *(source)* dan alamat tujuan *(destination)*. Seperti yang juga sudah diterapkan pada gedung C terhadap seluruh *host* atau *client* yang ada tidak dapat berinteraksi atau berkomunikasi dengan server juga tidak dapat mengakses *web server*. Dan hanya diberikan akses untuk saling berkomunikasi kepada jaringan *(Network Address)* lainnya seperti gedung A, gedung B, dan gedung C.

DAFTAR PUSTAKA

ISBN: 2964-1950

[1] Pastima Simanjuntak, dkk. 2017. Analisis Penggunaan *Access Control List* (ACL) Dalam Jaringan Komputer Di Kawasan Batamindo Industrial Park Batam. Vol 2 No.2 Batam.
[2]. Hari Antoni Musril. 2016. *Extended Access List* untuk Mengendalikan Trafik Jaringan. Vol 2. Bukit Tinggi.
[3]. Budi Sutedjo. 2004. Komputer dan jaringan. Konsep dan perancangan jaringan komputer: bangunan satu lantai, gedung bertingkat & kawasan. Yogyakarta.
[4]. Efendi. 2016. *Networking*. Belajar dan mengenal *IP Address, Subnetting, DNS.* Jakarta.
[5]. Sora Niko. 2018. *Gateway*. Pengertian dasar *gateway.* Jakarta.
[6]. Alinazar. 2003. Router, Routing. Defenisi router dan routing dalam jaringan komputer. Palembang.
[7]. Hardiansyah. 2002. Kemanan jaringan. Sistem pengamanan jaringan *WAN.* Yogyakarta.
[8]. Suharyanto, dkk. 2007. ACL (*Access Control List*). Analisis penggunaan ACL (*Acces Control List*) dalam jaringan komputer. Bandung.
[9]. Mufadhol. 2012. Cisco packet tracer. Simulasi jaringan komputer menggunakan *cisco packet tracer.* Jakarta.