

IMPLEMENTASI *ACCESS LIST* PENGAMANAN JARINGAN SIKAD KAMPUS UNIVERSITAS GUNADARMA MENGUNAKAN *CISCO PACKET TRACER 6.0.1*

¹ Noftra Rolly
² Nurul Adhayanti

^{1,2}Jurusan Sistem Informasi, Fakultas Ilmu Komputer,
nofra93@gmail.com, nurul_a@staff.gunadarma.ac.id
Universitas Gunadarma

ABSTRAK

Pada era globalisasi ini, semakin berkembangnya teknologi diseluruh bidang, contohnya dibidang pendidikan internet juga sangat dibutuhkan seperti pada universitas gunadarma. Universitas Gunadarma juga memberikan fasilitas dan kemudahan kepada mahasiswa untuk bisa mengakses informasi melalui jaringan Internet seperti: Studentsite, BAAK Online dan Staffsite dengan system informasi akademik yang saling terintegrasi.

Penulis menggunakan Access Control List dan software Packet Tracer 6.0.1. agar jaringan yang menggunakan saling terintegrasi sehingga dapat dijaga keamanannya dan mengimplementasikannya pada jaringan sistem Informasi Akademik Kampus Universitas Gunadarma karena software ini bisa digunakan sebagai software simulasi pada perangkat seperti cisco switch, cisco router yang dapat dikonfigurasi, serta dapat juga diuji konektivitasnya seperti ketika menggunakan perangkat aslinya.

Kata Kunci : SIKAD, ACCESS CONTROL LIST, CISCO PACKET TRACER 6.0.1

I. PENDAHULUAN

Gunadarma pertama kali berdiri pada tanggal 7 Agustus 1981 dengan nama Program Pendidikan Ilmu Komputer (PPIK). Sejak saat itu, kegiatan belajar mengajar mengacu pada pendidikan ilmu Computer dan matematika. Setelah itu pada tanggal 10 Juli 1984, melalui Surat Keputusan Yayasan Pendidikan Gunadarma, secara resmi nama Gunadarma dikukuhkan ke dalam sekolah tinggi menjadi Sekolah Tinggi Komputer Gunadarma (STKG). setelah mengalami perkembangan dan berhasil membuat fakultas yang baru dan berdidikasi, Gunadarma berhasil dikukuhkan menjadi Universitas Gunadarma pada tanggal 3 April 1996. Pada saat itu era globalisasi belum bisa memberikan kemudahan- kemudahan bagi mahasiwa maupun dosen untuk bisamengaksesinformasi. Dan semakin berkembangnya teknologi di bidang komputer, universitas gunadarma memberikan fasilitas dan kemudahan kepada mahasiswa untuk bisa mengakses informasi melalui Internet seperti: *Studentsite* merupakan salah satu dari beberapa layanan yang disediakan oleh Universitas Gunadarma yang digunakan untuk memudahkan mahasiswa mencari informasi seputar kegiatan dan semua aktifitas yang ada di Gunadarma, *BAAK Online* merupakan tempat menangani segala sesuatu yang berkaitan dengan penyelenggaraan kegiatan belajar-mengajar di Universitas Gunadarma dan administrasi akademik bagi seluruh mahasiswa UniversitasGunadarma, *Staffsite* merupakan informasi berbasis web browser untuk mengunduh modul ajaran dan sekaligus melihat informasi lengkap tentang dosen tersebut.

Perusahaan ini didirikan pada tahun 1984, dengan mempekerjakan 51.480 pekerja yang bergerak dibidang jaringan dan telekomunikasi yaitu *Cisco System.Inc*. Kantornya bermarkas di San José, California, Amerika Serikat. Visi dari *Cisco System.Inc (Cisco)* yaitu “mengubah bagaimana cara hidup,bekerja,bermain dan belajar”,dan ada pun

slogannya lainnya adalah “ Selamat datang kedalam dunia Jaringan “ (*welcome to the human network*). Untuk jaringan, cisco juga memberikan kemudahan untuk saling terkoneksi dan saling terhubung dari jaringan satu dengan jaringan lainnya untuk berbagi sumber daya, berkomunikasi dan mengakses informasi. Setiap perangkat-perangkat yang terhubung ke dalam jaringan disebut node. Secara umum jaringan komputer dibagi atas 5 jenis, yaitu: 1. *Local Area Network (LAN)*, merupakan jaringan yang terdapat didalam gedung atau kampus yang berukuran sampai beberapa kilometer. 2. *Metropolitan Area Network (MAN)*, merupakan versi *LAN* yang berukuran lebih besar dan dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan, *MAN* dapat menunjang data dan suara, sehingga bisa terhubung dengan jaringan televisikabel. 3. *Wide Area Network (WAN)*, jangkauannya dapat mencakup sebuah negara bahkan benua. Terbentuknya jaringan yang menghubungkan antara komputer satu dengan komputer lainnya merupakan definisi dari topologi. Jenis topologi jaringan yang saat ini banyak digunakan adalah bus, token-ring, star dan peer-to-peer network.

OSI Model merupakan suatu dekripsi abstrak mengenai desain lapisan- lapisan komunikasi dan protokol jaringan komputer yang dikembangkan sebagai bagian dari inisiatif *Open Systems Interconnection (OSI)* atau sering disebut juga sebagai Standarisasi Internasional untuk Jaringan. Selain itu osi model juga:

- Sebagai proses komunikasi dibuat kedalam lapisan-lapisan yang membuatnya lebih sederhana.
- Sebagai perubahan pada suatu lapisan tidak mempengaruhi lapisan lainnya.
- Standar komunikasi dapat disamakan pada jenis perangkat yang berbeda vendor agar dapat berkomunikasi satu sama lain.

Osi sendiri memiliki 7 layer dan untuk melihat apa saja yang ada di dalam Osi layer lihat table di bawah ini.

Tabel 1.1 OSI Model.

| OSI # | OSI Layer Name | TCP/IP # | TCP/IP Layer Name | Encapsulation Units |
|-------|----------------|----------|-------------------|---------------------|
| 7 | Application | 4 | Application | data |
| 6 | Presentation | | | data |
| 5 | Session | | | data |
| 4 | Transport | 3 | Transport | segments |
| 3 | Network | 2 | Internet | packets |
| 2 | Data Link | 1 | Network Access | frames |
| 1 | Physical | | | bits |

Setelah melihat table *OSI* dan layernya, *Internet Protokol (IP)* termasuk dalam *Osi model* layer ke 3. *Internet Protokol* itu sendiri atau di singkat (*IP*). adalah protokol lapisan jaringan (*network layer* dalam *OSI Reference Model*) atau protokol lapisan internetwork yang digunakan oleh *protokol TCP/IP* untuk melakukan pengalamatan dan routing paket data antar host-host di jaringankomputer berbasis *TCP/IP* seperti table di bawah ini.

Table 1.2. IP Addresses

| Class | 1 st Octet Decimal Range | 1 st Octet High Order Bits | Network/Host ID (N=Network, H=Host) | Default Subnet Mask | Number of Networks | Hosts per Network (Usable Addresses) |
|-------|-------------------------------------|---------------------------------------|-------------------------------------|---------------------|----------------------------|--------------------------------------|
| A | 1–126* | 0 | N.H.H.H | 255.0.0.0 | 126 ($2^7 - 2$) | 16,777,214 ($2^{24} - 2$) |
| B | 128–191 | 10 | N.N.H.H | 255.255.0.0 | 16,382 ($2^{14} - 2$) | 65,534 ($2^{16} - 2$) |
| C | 192–223 | 110 | N.N.N.H | 255.255.255.0 | 2,097,150 ($2^{21} - 2$) | 254 ($2^8 - 2$) |
| D | 224–239 | 1110 | Reserved for Multicasting | | | |
| E | 240–254 | 1111 | Experimental; used for research | | | |

Tabel 1.3. Private IP Addresses

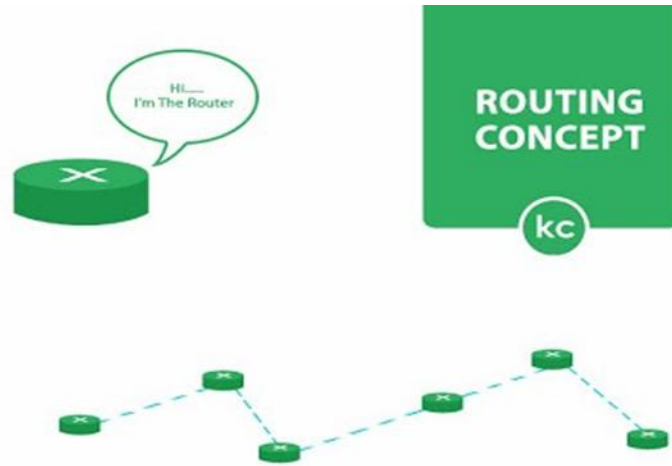
| Private IP Addresses | | | |
|----------------------|-------------------------|-------------|-------------------------------|
| Class | Private Networks | Subnet Mask | Address Range |
| A | 10.0.0.0 | 255.0.0.0 | 10.0.0.0 - 10.255.255.255 |
| B | 172.16.0.0 - 172.31.0.0 | 255.240.0.0 | 172.16.0.0 - 172.31.255.255 |
| C | 192.168.0.0 | 255.255.0.0 | 192.168.0.0 - 192.168.255.255 |

Subnet mask yang digunakan pada angka biner 32 bit dapat digunakan dalam membedakan antara *network* ID dan host ID, merupakan sebuah petunjuk suatu *host* terletak, yang terdapat pada jaringan lokal atau jaringan luar.

Tabel 1.4. Subnet Mask

| | | |
|-----|-----------------|-------|
| /16 | 255.255.0.0 | 65534 |
| /17 | 255.255.128.0 | 32766 |
| /18 | 255.255.192.0 | 16382 |
| /19 | 255.255.224.0 | 8190 |
| /20 | 255.255.240.0 | 4094 |
| /21 | 255.255.248.0 | 2046 |
| /22 | 255.255.252.0 | 1022 |
| /23 | 255.255.254.0 | 510 |
| /24 | 255.255.255.0 | 254 |
| /25 | 255.255.255.128 | 126 |
| /26 | 255.255.255.192 | 62 |
| /27 | 255.255.255.224 | 30 |
| /28 | 255.255.255.240 | 14 |
| /29 | 255.255.255.248 | 6 |
| /30 | 255.255.255.252 | 2 |

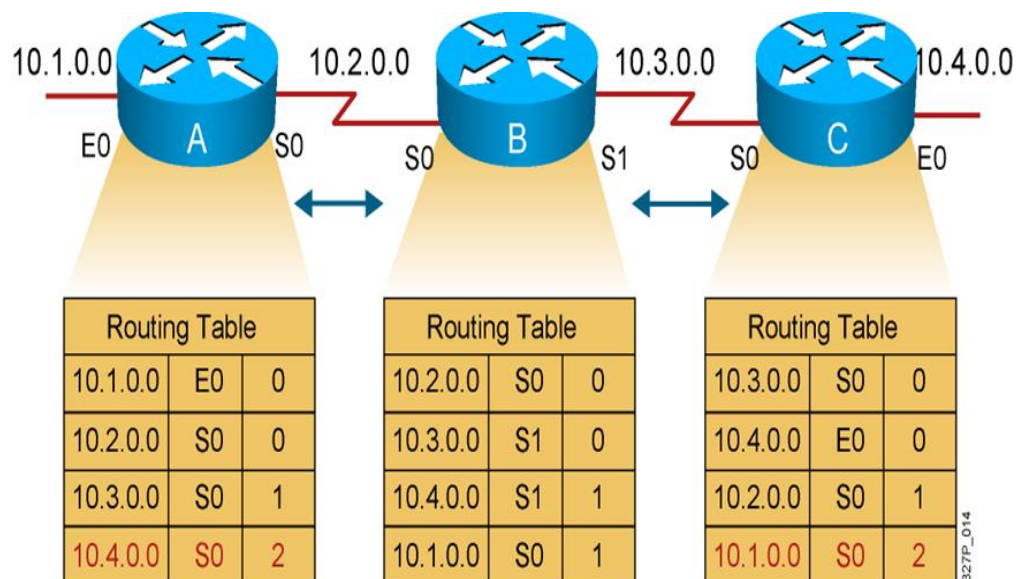
Alat jaringan komputer yang digunakan dalam mengirimkan paket data pada jaringan atau Internet menuju tujuannya yang kita kenal sebagai router.



Gambar 1.1. Router (Sumber Modul Cisco)

Dasar Routing, yaitu:

- Menentukan *Path* (jalur) sebuah paket melalui jaringan.
- Menentukan semua rute yang mungkin.
- Menentukan rute terbaik.
- *Maintenance* (memelihara) *table routing*.



Gambar 1.2. Routingtable (Sumber Modul Cisco)

Setelah mengetahui dasar routing dan mengetahui jalur mana yang harus dilalui oleh paket tersebut, setelah itu Routing akan melakukan perbandingan. Untuk pembagian Routing itu sendiri di bagi menjadi dua, yaitu *Router Static* dan *Router Dinamis*.

IP Routing yaitu proses dimana suatu router meneruskan paket dari satu network ke *network* yang lain menggunakan router. *Router* tersebut berkomunikasi menggunakan alamat logika atau *IP Address* untuk melakukan suatu proses routing. Agar router dapat melakukan proses routing ke jaringan yang dituju, maka dibutuhkan tabel routing. Tabel routing adalah tabel yang berisi informasi-informasi rute yang dapat dicapai oleh suatu router. Ketika *router* menggunakan routing dinamis, informasi ini dipelajari dari router yang lain. Ketika

menggunakan routing statis, maka seorang network administrator akan mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual. Ada beberapa routing dinamic untuk IP, yaitu: *Routing Information Protocol (RIP)*, *Interior Gateway Routing Protocol(IGRP)*, *Open Shortest Path First(OSPF)*, *Enhanced Interior Gateway Routing Protocol(EIGRP)*, *Exterior Gateway Protocol(EGP)*

Salah satu perangkat jaringan komputer dan terhubung dalam beberapa network segment disebut dengan Switch. Istilah lain pada switch yaitu multi-port network bridge (Jembatan jaringan multi-port) dalam memproses dan mengirimkan data pada layer 2 OSI atau 3 OSI (multi layer switch). Beberapa fungsi dari switch yaitu tidak mengganggu jalannya distribusi data lain yang sedang berjalan sehingga bisa membuat jalannya sendiri, terdapatnya bandwidth tersendiri yang bisa berjalan full duplex (kirim terima secara bersamaan). Hal ini berbeda pada switch yang menjalankan data half duplex (kirim-terima secara bergantian) yang bisa membagi semua bandwidth ke semua jalur sehingga menyebabkan terjadinya tabrakan data.

VLAN (Virtual Local Area Network) adalah sebuah LAN sebagai kelompok device terdapat dalam konfigurasi (menggunakan software manajemen) sehingga saling berkomunikasi yang seolah-olah terhubung dengan jaringan yang sama walaupun secara fisik mereka berada pada segmen dalam LAN yang berbeda. *VLAN* dibuat lebih pada koneksi logikal yang lebih fleksibel dan dapat membagi jaringan ke dalam beberapa subnetwork serta mengijinkan banyak subnet dalam jaringan yang menggunakan switch yang sama. *VLAN* merupakan fungsi logik dari sebuah switch yang berfungsi membagi jaringan LAN ke dalam beberapa jaringan virtual. Dapat memudahkan administrator jaringan saat membagi secara logik group workstation secara fungsional yang tidak dibatasi oleh batasan lokasi merupakan Implementasi *VLAN* dalam jaringan. Kecepatan dalam pengiriman data sangat dibutuhkan dalam sebuah organisasi, salah satu bentuk kontribusi dengan menggunakan *VLAN* adalah meningkatkan kinerja jaringan dengan kemampuan membagi sebuah broadcast domain yang besar menjadi beberapa broadcast domain yang lebih kecil. Dengan adanya *VLAN*, kita dapat melakukan segmentasi jaringan switch pada departemen dengan kebutuhan masing-masing instansi sesuai dengan fungsinya sehingga para pekerja/pengguna dapat mengakses jaringan yang sama walaupun berada dalam lokasi yang berbeda.

Dari segi keamanan data pada setiap jaringan dibuat tersendiri, dengan adanya segmennya bisa terpisah secara logik, yang dapat mengurangi kesempatan data yang terganggu. *VLAN* dapat menciptakan kelompok *broadcast* sesuai dengan kebutuhan jaringan, sehingga jaringan dapat dipecah atau dibagi lebih kecil agar dapat membatasi akses-akses yang tidak diijinkan. Adanya kontrol pada setiap port dan user yang ada oleh Administrator. *Level MAC address*, protokol-protokol dapat mengatur keamanan atau tergantung kebutuhan. Seperti mengontrol paket mana yang bias di access dan paket mana yang tidak boleh di access. Karena tujuan *access list* sendiri untuk pengamanan jaringan dan sekaligus mengontrol paket data seperti di bawah ini.

Access Control List(ACL).

Access list merupakan 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. Penggunaan *access list* yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan. Sebagai contoh kita dapat mengatur *access list* untuk membuat keputusan yang sangat spesifik tentang

peraturan pola lalu lintas sehingga access list hanya memperbolehkan host tertentu untuk mengakses data tersebut, sementara yang lainnya ditolak.

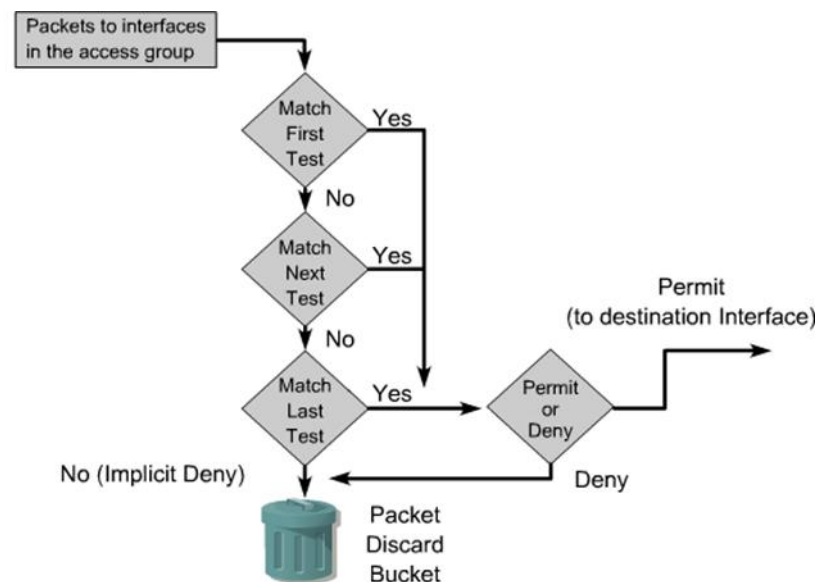
Selain itu kita juga bisa menggunakan access list untuk mengkategorikan paket antrian layanan data, pengidentifikasian jaringan yang dapat mengontrol tipe lalu lintas data berdasarkan pada:

- Alamat tujuan
- Tipe protocol
- Dan nomor port dari paket.

Selain itu agar paket data yang di kirim atau data yang ingin di akses harus mengetahui aturan aturan di access list tersebut seperti di bawah iniseperti:

- Paket akan dibandingkan setiap baris *Access List* secara berurutan
- Paket dibandingkan setiap baris hanya hingga terjadi *Match* (menemukan yang pas) Setelah ditemukan (*MATCH*) dan ditindak lanjuti maka tidak ada lagi perbandingan berikutnya
- Secara *implicit* (tersirat) pada akhir dari *akseslist* ada perintah “*deny*” Jika tidak ada yang *Match* maka paket akan di*Discard*

Untuk mengetahui bagaimana cara kerja ACL lihat gambar di bawah ini :



Gambar 1.3. Cara Kerja ACL

Tipe dari *ACL*, yaitu: *Standard ACL* dan *Extended ACL*

Dua metode digunakan untuk identifikasi *Standard* dan *Extended ACL*:

- *Numbered ACL*: Menggunakan sebuah nomor sebagai identifikasi
- *Named ACL*: Menggunakan deskripsi nama atau nomor untuk identifikasi.

Untuk penerapan *ACL* di bagi menjadi 2 yaitu:

- *Inbound ACL*
- *Outbound ACL*

Identifikasi *ACL*

- Nomor *Standard ACL IPv4* (1-99) dengan Range Tambahan (1300- 1999)
- Nomor *Extended ACL IPv4* (100-199) dengan Range Tambahan (2000- 2699)

Named ACL bisa digunakan untuk identifikasi *IP Standard dan Extended ACL* dengan sebuah alpha numeric string (nama)

Tabel 1.5. IPv4 ACL

| IPv4 ACL Type | Number Range/Identifier |
|-------------------------------|-------------------------|
| Numbered Standard | 1–99, 1300–1999 |
| Numbered Extended | 100–199, 2000–2699 |
| Named (Standard and Extended) | Name |

327P_515

Tata Cara Konfigurasi ACL

- *Standard* atau *Extended* mengindikasikan jenis *Access List* yang digunakan.
- Hanya ada satu *ACL per interface, per protocol*, dan per *Direction* yang diperbolehkan.
- Informasi lebih spesifik berada pada baris bagian atas *ACL*.
- Sebuah list baru akan ditempatkan pada akhir *ACL*.
- Penghapusan *ACL* secara individual tidak diperbolehkan.
- Akhir *ACL* sebaiknya diterapkan perintah permintanya.
- Buat *ACL* dan terapkan pada *interface (inbound atau outbound)*.
- *ACL* tidak melakukan filter jika trafik berasal dari *Router* itu sendiri.
- Letakkan *Standard ACL* dekat dengan *destination*.
- Letakkan *Extended ACL* dekat dengan *Source*.

Access List selain memiliki fungsi untuk memblokir paket data dan mengontrol paket data. *Access list* juga memiliki keuntungan dan kerugian seperti di bawah ini:

1. Keuntungan *Access-list*.
 - Menggunakan teknik routing sehingga dapat diatur jalur komunikasi jaringan.
 - Pada komputer atau server dapat dijaga keamanannya.
 - Dapat terdefinisi jalur komunikasinya.
2. Kerugian *Access-list*.
 - Komunikasi untuk setiap komputer terbatas.
 - Struktur komunikasi Router Cisco membutuhkan waktu lama dalam proses Implementasi.

Layanan yang dapat memberikan secara otomatis nomor IP kepada komputer yang memintanya disebut dengan *DHCP (Dynamic Host Configuration Protocol)*. Sedangkan Komputer yang memberikan nomor IP disebut sebagai *DHCP server*, 4 tahapan proses yang terdapat pada DHCP untuk memberikan konfigurasi nomor IP, antara lain:

1. IP Lease Request

Client meminta nomor IP ke server (Broadcast mencari DHCPserver).

2. IP Lease Offer

DHCP server dapat memberikan penawaran no IP ke client (bisa satu atau lebih server jika memang ada).

3. IP Lease Selection

Dengan *message* menyetujui peminjaman kepada *DHCP Server*, *Client* dapat memilih penawaran *DHCP Server* yang pertama diterima dan kembali melakukan *broadcast*.

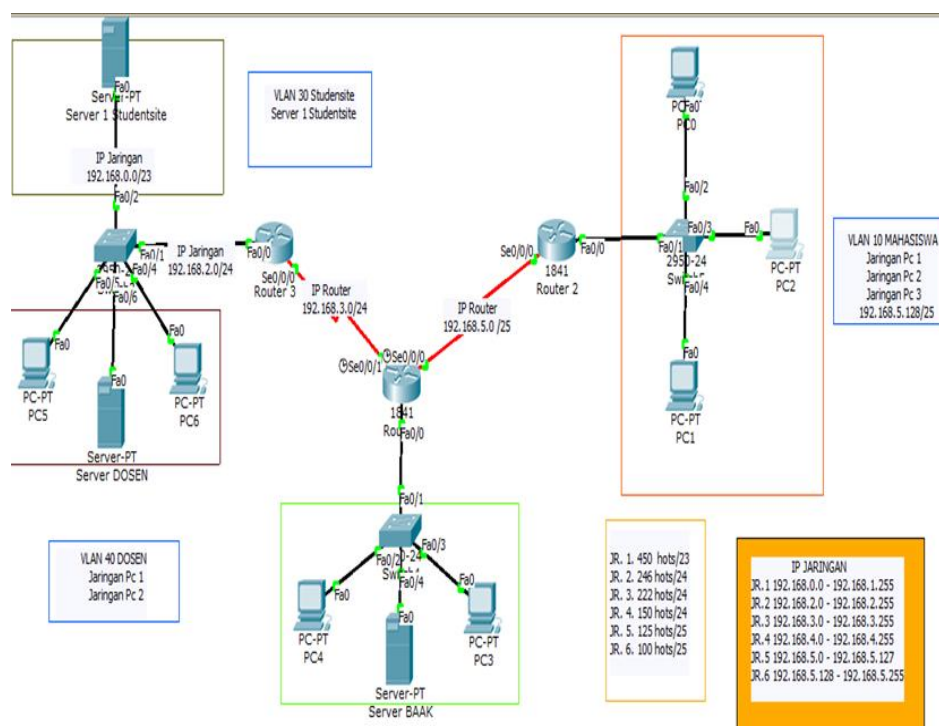
4. IP Lease Acknowledge

Client dapat melakukan inisialisasi dengan mengikat nomor IP dan langsung bisa mempergunakan jaringan tersebut. Setelah client mendapatkan jawaban pesan dari *DHCP Server* yang menang berupa konfirmasi no IP dan informasi sebuah *ACKnowledgment*. Sedangkan *DHCP Server* yang lain menarik tawarannya kembali.

II. METODE PENELITIAN

Secara garis besar pada bab ini membahas pembangunan *ACL (Access Control List)* dan bagaimana cara memblock jaringan yang tidak boleh di akses, serta mengamankan paket data secara spesifik. Untuk konfigurasi *Routing*, menggunakan *routing OSPF* simulasi pada *Packet Tracer*.

Topologi jaringan yang digunakan untuk gambaran umum dalam pengujian routing protocolnya. penulis akan menggunakan 3 buah *router*, 7 buah *PC* dan 3 buah *server* pada jaringan IPv4. Topologi ditunjukkan pada Gambar 2.1:



Gambar 2.1 Topologi Jaringan Bus

Berdasarkan topologi di atas menggambarkan tiga *router Cisco* yang berada di area jaringan yang berbeda. Kemudian digunakan kabel serial untuk menghubungkan ketiga *router cisco* tersebut sehingga bisa saling terhubung antara client di masing-masing jaringan. Agar biasa saling terkoneksi maka setiap perangkat dalam jaringan itu harus diberi alamat (*address*). Melalui pengalamatan inilah maka setiap perangkat dapat terhubung ke internet dan keberadaannya diketahui dari identitas alamatnya. Tanpa alamat atau identitas itu maka setiap perangkat dalam jaringan tidak akan dapat melakukan koneksi dan pertukaran informasi. Alamat dimaksud adalah *Internet Protocol (IP) address*.

Pada tahun 1981 IP versi 4 (IPv4) dibuat dan diperkenalkan diseluruh dunia. IPv4 sebagian besar sudah digunakan pada berbagai perangkat jaringan antara lain terdapat dalam *Server, Router, Bandwidth Management, Access Point/HotSpot, Switch/Hub*, atau perangkat lain yang menggunakannya seperti *Komputer, Laptop, Hand Phone*, dan lain sebagainya.

Deretan angka biner antar 32-bit sampai 128-bit yang terdapat dalam alamat IP dapat dipakai sebagai alamat identifikasi pada tiap komputer *host* di jaringan Internet. Pengalamatan pada IPv4 yang terdapat angka biner 32 bit dapat dikelompokkan menjadi 4 segmen, dimana setiap segmennya terdiri 8 bit dan dibatasi oleh notasi titik. Misalnya IPv4 yaitu 192.168.1.1. yang terdiri atas 32 bit

maka total jumlahnya adalah 24 atau sebanyak 2 pangkat 32 (232), yaitu sekitar 4.294.967.296 *host* alamat IP yang dihasilkan di seluruh dunia.

Tabel 6. memperlihatkan alokasi IP yang dipakai, baik pada topologi jaringan IPv4 yaitu sebagai berikut:

Tabel 2.1. IP Address

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|----------------|-----------|---------------|-----------------|-----------------|
| R1 | Se0/0/0 | 192.168.5.2 | 255.255.255.128 | N/A |
| | Se0/0/1 | 192.168.3.2 | 255.255.255.0 | N/A |
| | Fa0/0 | 192.168.4.1 | 255.255.255.0 | N/A |
| R2 | Se0/0/0 | 192.168.5.1 | 255.255.255.128 | N/A |
| | Fa0/0 | 192.168.5.129 | 255.255.255.128 | N/A |
| R3 | Se0/0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| | Fa0/0 | 192.168.3.2 | 255.255.255.0 | N/A |
| PC0 | Fa0/2 | 192.168.5.130 | 255.255.255.128 | 192.168.5.129 |
| PC1 | Fa0/3 | 192.168.5.131 | 255.255.255.128 | 192.168.5.129 |
| PC2 | Fa0/4 | 192.168.5.132 | 255.255.255.128 | 192.168.5.129 |
| PC3 | Fa0/3 | 192.168.4.3 | 255.255.255.0 | 192.168.4.1 |
| PC4 | Fa0/2 | 192.168.4.2 | 255.255.255.0 | 192.168.4.1 |
| S. BAAK | Fa0/4 | 192.168.4.4 | 255.255.255.0 | 192.168.4.1 |
| S. Studentsite | Fa0/3 | 192.168.0.2 | 255.255.254.0 | 192.168.0.1 |
| PC5 | Fa0/5 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| PC6 | Fa0/4 | 192.168.2.4 | 255.255.255.0 | 192.168.2.1 |
| S. Stafsite | Fa0/6 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 |

Setelah melakukan pengalamatan untuk jaringan agar saling berkomunikasi harus di hubungkan dengan *Router*.

Sebelum jaringan saling terkoneksi dan saling terhubung dari jaringan satu ke jaringan lainnya, yang harus di lakukan adalah mengkonfigurasi router 2 untuk mengenalkan setiap interface di jaringan mahasiswa. Seperti gambar 2.2. di bawah ini :

```
Router>en
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.5.129 255.255.255.128
Router(config-if)#no sh
Router(config-if)#ex
Router(config-if)#exit
Router(config)#int se0/0/0
Router(config-if)#ip add 192.168.5.1 255.255.255.128
Router(config-if)#no sh
```

Gambar 2.2. *Configurasi Interface*

Sebelum jaringan saling terkoneksi dan saling terhubung dari jaringan satu ke jaringan lainnya, yang harus dilakukan adalah mengkonfigurasi router 2 untuk mengenalkan setiap interface di jaringan mahasiswa. Seperti gambar 2.3. di bawah ini :

```
Router>en
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.5.129 255.255.255.128
Router(config-if)#no sh
Router(config-if)#ex
Router(config-if)#exit
Router(config)#int se0/0/0
Router(config-if)#ip add 192.168.5.1 255.255.255.128
Router(config-if)#no sh
```

Gambar 2.3. *Configurasi Interface*

Setelah melakukan pengenalan interface kepada *router* maka selanjutnya melakukan pengenalan *VLAN* untuk membagi jaringan sekecil mungkin.

Pengaturan keamanan juga dapat dilakukan pada level *MAC address*, protokol-protokol, atau tergantung kebutuhan. Untuk *configurasi VLAN* di jaringan mahasiswa lihat pada gambar 2.4.

```
Switch#en
Switch#enable
Switch#conf t
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name MAHASISWA
Switch(config-vlan)#ex
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#|
```

Gambar 2.4. *Config Vlan di jaringan Mahasiswa*

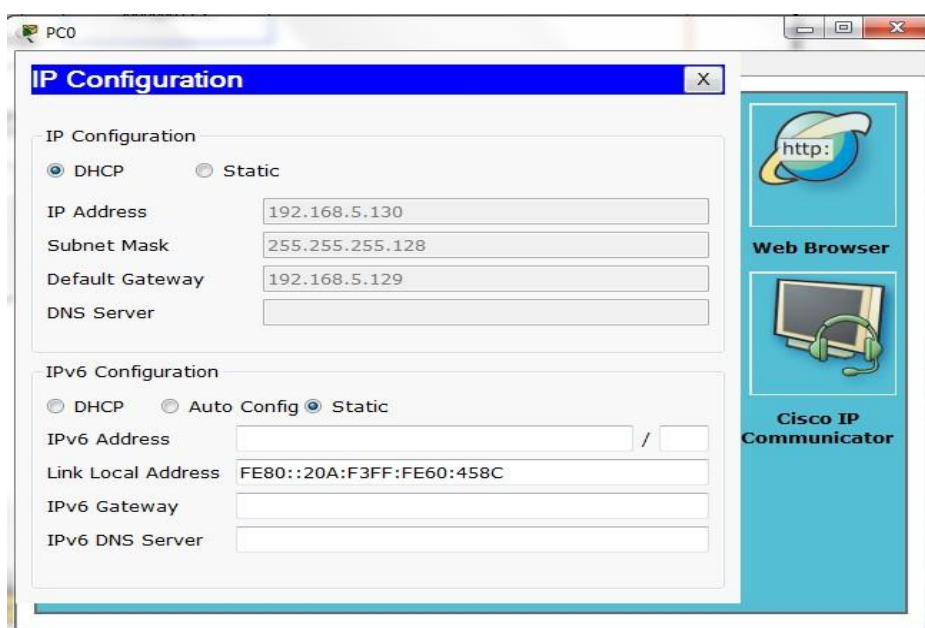
Setelah mengkonfigurasi *Vlan* selanjutnya memberi IP kepada setiap jaringan. Untuk proses pemberian IP Penulis menggunakan konfigurasi *DHCP*.

Untuk konfigurasi *DHCP* di jaringan Dosen bisa di lihat pada gambar 2.5 dan gambar 2.6.

```
Router>en
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp po
Router(config)#ip dhcp pool VLAN- Mahasiswa
Router(dhcp-config)#net 192.168.5.128 255.255.255.128
Router(dhcp-config)#def
Router(dhcp-config)#default-router 192.168.5.129
Router(dhcp-config)#ex
Router(config)#
```

Gambar 2.5. *Configurasi DHCP jaringan dosen*

Setelah di konfigurasi bisa di lihat di PC atau Server tersebut pada gambar 2.6.



Gambar 2.6. hasil konfigurasi DHCP

Setelah melakukan semua konfigurasi agar bisa saling terhubung dari jaringan satu ke jaringan lainnya yaitu yang terakhir mengkonfigurasi *Router 3*. Untuk mengenalkan jaringan *Studentsite* dengan jaringan Dosen. Untuk konfigurasi *Routing menggunakan Routing OSPF* dapat dilihat pada dibawah ini.



```

Router#en
Router#enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 100
Router(config-router)#net 192.168.3.0 0.0.0.255
% Incomplete command.
Router(config-router)#net 192.168.0.0 0.0.0.255
% Incomplete command.
Router(config-router)#net 192.168.2.0 0.0.0.255
% Incomplete command.
Router(config-router)#net 192.168.3.0 0.0.0.255 a 10
Router(config-router)#
00:40:35: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.5.2 on Serial0/0/0 from LOADI
NG to FULL, Loading Done
Router(config-router)#net 192.168.2.0 0.0.0.255 a 10
Router(config-router)#net 192.168.0.0 0.0.0.255 a 10
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

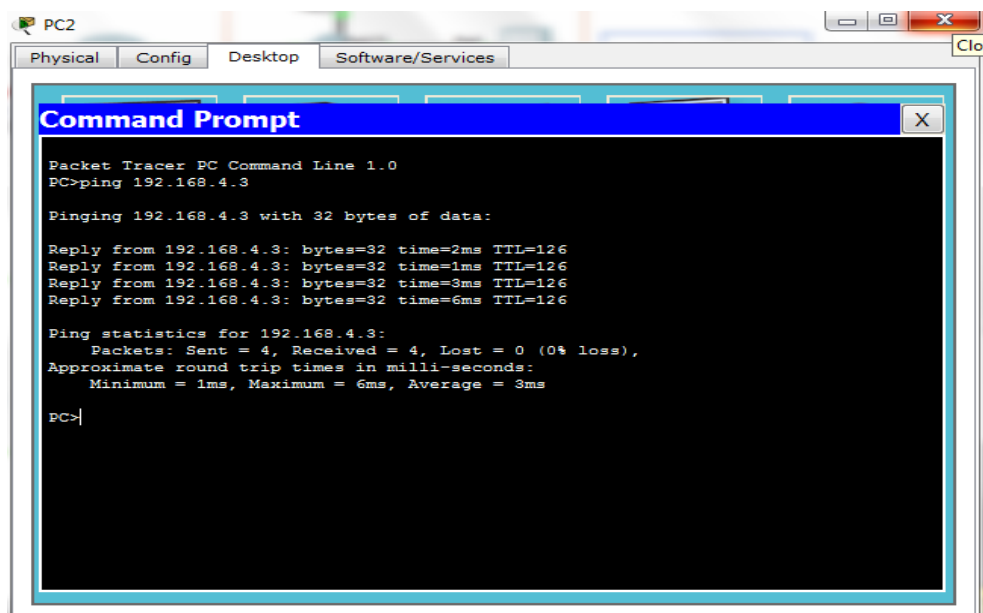
```

Gambar 2.7. Routing OSPF

Setelah semua *Router* dikonfigurasi, dan untuk melihat hasil pengujiannya saya akan mencoba *ngeping* menggunakan *Realtime* dan *Comand Prompt* dari *PC 2* dengan IP 192.168.5.132 ke *PC 4* dengan IP 192.168.4.3 lihat gambar 2.8.

| Fire | Last Status | Source | Destination | Type | Color | Time (sec) | Periodic | Num |
|---|-------------|--------|-------------|------|---|------------|----------|-----|
|  | Successful | PC2 | PC4 | ICMP |  | 0.000 | N | 0 |

Gambar 2.8. Ping real Time



```

PC2
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.4.3

Pinging 192.168.4.3 with 32 bytes of data:

Reply from 192.168.4.3: bytes=32 time=2ms TTL=126
Reply from 192.168.4.3: bytes=32 time=1ms TTL=126
Reply from 192.168.4.3: bytes=32 time=3ms TTL=126
Reply from 192.168.4.3: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.4.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 3ms

PC>

```

Gambar 2.9. Ping command Prompt

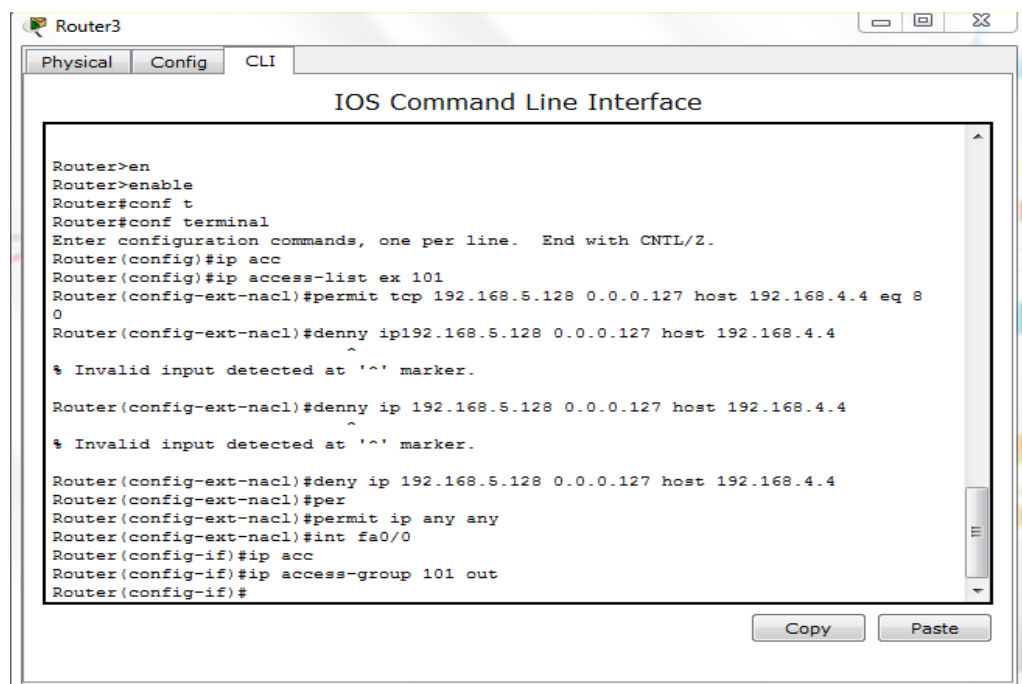
Setelah melakukan pengujian dan berhasil semua sekarang menentukan pemblokiran jaringan . yaitu hanya jaringan tertentu yang bisa mengakses jaringan yang di inginkan dengan metode *Access List Web Browser*.

Untuk *ACL* yang di terapkan kali ini menggunakan *ACL Standard* dan *ACL HTTP* (menggunkan *Web Browser*). Dan *Access Control List* ini penulis membagi jaringan tertentu yang bisa di *Acces* seperti:

1. Jaringan Mahasiswa (*I-lounge*) hanya bisa *Acces* fia *Http* ke server BAAK.
2. Jaringan Mahasiswa hanya bisa *aces* melalui *Http* ke Server *Studentsite*
3. Jaringan Mahasiswa di tolak ke jaringan Dosen

konfigurasi yang pertama yaitu:

1. Jaringan Mahasiswa (*I-lounge*) hanya bisa *Acces* melalui *Http* ke server BAAK. Dengan cara mengkonfigurasi *access list* pada router 2 dari jaringan mahasiswa untuk mengakses jaringan BAAK *Online di Router 1*. Untuk cara mengkonfigurasinya bisa di lihat pada gambar 2.10.



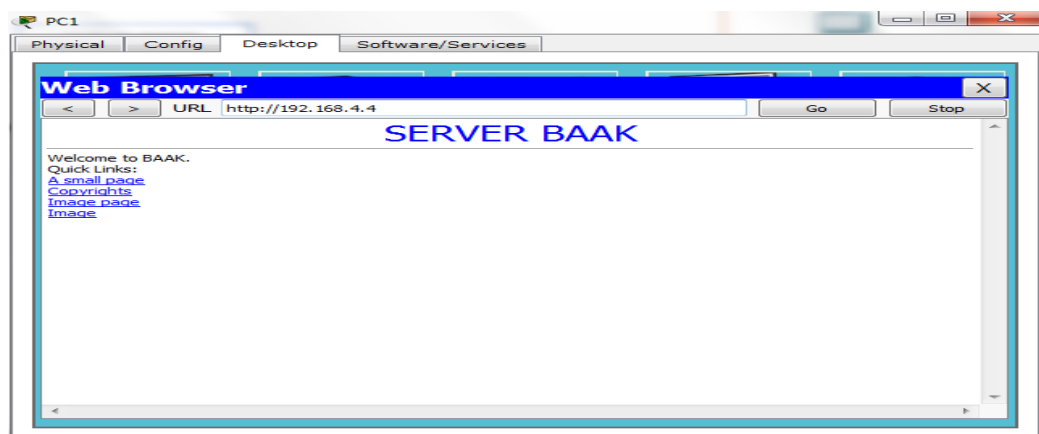
```

Router3
Physical Config CLI
IOS Command Line Interface

Router>en
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list ex 101
Router(config-ext-nacl)#permit tcp 192.168.5.128 0.0.0.127 host 192.168.4.4 eq 80
Router(config-ext-nacl)#deny ip 192.168.5.128 0.0.0.127 host 192.168.4.4
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#deny ip 192.168.5.128 0.0.0.127 host 192.168.4.4
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#deny ip 192.168.5.128 0.0.0.127 host 192.168.4.4
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#int fa0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 101 out
Router(config-if)#
  
```

Gambar 2.10. konfigurasi *Acl* ke jaringan *BAAK Online* menggunakan *Web browser*

Setelah di konfigurasi, sekarang kita coba dari PC 1 dari jaringan mahasiswa, lalu kita coba menghubungkan lewat HTTP dengan memasukan IP nya yaitu 192.168.4.4 dan hasilnya bisa di lihat pada gambar 2.11 di bawah ini.

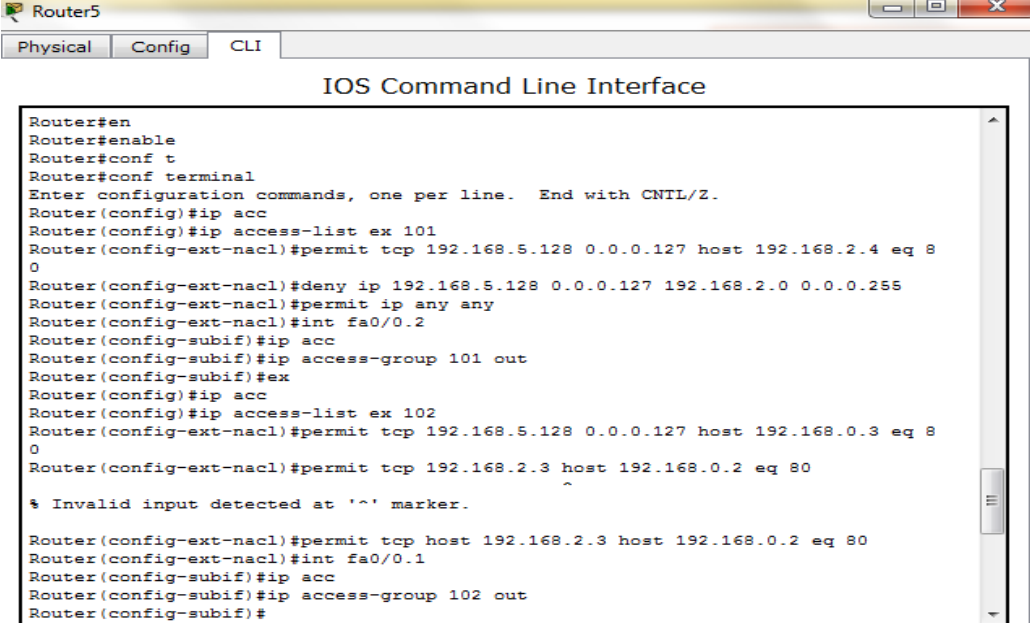


Gambar 2.11. hasil *connected* menggunakan *web rowser*

Konfigurasi yang ke dua.

2 Jaringan Mahasiswa hanya bisa *aces* lewat *Http* ke *Server Studentsite*.

Yaitu mengkonfigurasi dari router 2 di jaringan mahasiswa, lalu memasukan IP jaringan Router 3 di jaringan *Studentsite*. Untuk cara mengkonfigurasinya bisa di lihat di 2.12.

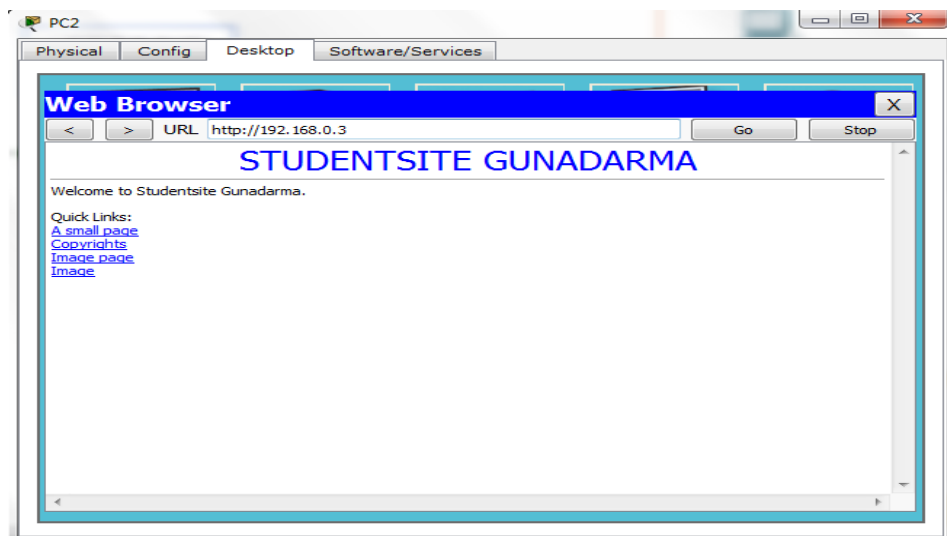


```

Router5
Physical Config CLI
IOS Command Line Interface
Router#en
Router#enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip acc
Router(config)#ip access-list ex 101
Router(config-ext-nacl)#permit tcp 192.168.5.128 0.0.0.127 host 192.168.2.4 eq 8
0
Router(config-ext-nacl)#deny ip 192.168.5.128 0.0.0.127 192.168.2.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#int fa0/0.2
Router(config-subif)#ip acc
Router(config-subif)#ip access-group 101 out
Router(config-subif)#ex
Router(config)#ip acc
Router(config)#ip access-list ex 102
Router(config-ext-nacl)#permit tcp 192.168.5.128 0.0.0.127 host 192.168.0.3 eq 8
0
Router(config-ext-nacl)#permit tcp 192.168.2.3 host 192.168.0.2 eq 80
% Invalid input detected at '^' marker.
Router(config-ext-nacl)#permit tcp host 192.168.2.3 host 192.168.0.2 eq 80
Router(config-ext-nacl)#int fa0/0.1
Router(config-subif)#ip acc
Router(config-subif)#ip access-group 102 out
Router(config-subif)#
  
```

Gambar 2.12. Konfigurasi Acl ke jaringan *Studentsite* menggunakan *Web browser*

Setelah di konfigurasi, sekarang kita coba menyambungkan dari PC 2 dengan memasukan IP Jaringan *Studentsite* yaitu 192.168.0.3 dan hasilnya bisa di lihat pada gambar 2.13.

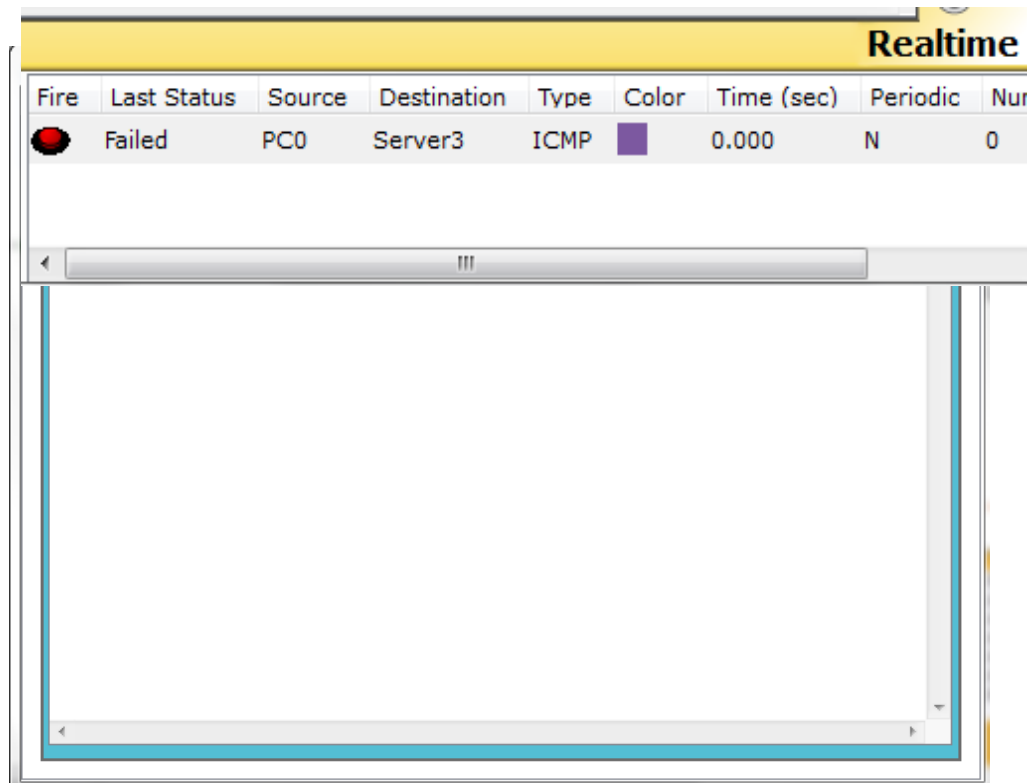


Gambar 2.13. hasil *connected* menggunakan *web browser*

Dan yang terakhir.

3. Jaringan Mahasiswa di tolak ke jaringan Dosen

Yaitu dengan mengkonfigurasi *Router 2* di jaringan mahasiswa ke jaringan dosen di *Router 1*. maka setelah di konfigurasi, sekarang kita coba menyambungkan dari PC 1, dan hasilnya bisa di lihat pada gambar 2.13. dan gambar 2.14 di bawah ini.



Gambar 2.14 hasil *connected* menggunakan *web browser*

III. SIMPULAN dan SARAN

Simpulan

Sistem jaringan komputer yang dibutuhkan pada setiap instansi berbeda- beda serta fungsi dan kegunaannya juga berbeda-beda antara *BAAK Online*, *Studentsite* dan *Staffsite*. Tujuan perbedaan setiap instansi ini memudahkan mahasiswa untuk mencari informasi perkuliahan, ataupun tentang nilai akademik. Agar lebih memudahkan mahasiswa setiap Instansi dapat di akses melalui jaringan internet, namun untuk pengimplementasi jaringan ini penulis menambahkan serta *ACL (Access Control List)* tujuannya untuk mengamankan jaringan dari orang-orang yang tidak bertanggung jawab serta mengatur lalu lintas data. Misalkan jaringan Mahasiswa hanya bisa mengakses jaringan *Staffsite* melalui *Web browser (Internet)* tapi tidak bisa untuk mengunduh file di *Staffsite*. Begitu juga jaringan yang lainnya, jaringan mahasiswa hanya bisa akses ke jaringan *BAAK Online* melalui *Web browser (Internet)* tapi tidak bisa *ping realtime* atau *ping comant prompt* menggunakan simulator *Packet Tracer*.

Saran

Dalam melakukan desain jaringan ini terdapat kesalahan-kesalahan serta kekurangan yang harusnya disempurnakan lebih lanjut, adapun beberapa saran dari penulis yaitu :

1. Topologi jaringan dibuat lebih mendetail, hingga bagian-bagian yang lebih kecil, seperti memperkecil jaringan di jaringan mahasiswa.
2. Pengaman jaringan harus di perluas lagi Terutama di jaringan BAAK *Online*, *Staffsite* dan *Studentsite* agar lebih aman dan lebih terkontrol perlu penambahan keaman seperti *FireWall*, *FTP Server*, *Mail Server* dan *Remote Desktop*.
3. Selanjutnya disarankan ada perbandingan antara *routing protocol* yang lain. Contoh: *Protocol IS-IS*, *EIGRP*, *BGP*, *RIP*, *EGP* dan lain-lain. Dari segi perangkat dan perancangan disain topologi, untuk mengetahui *routing* apa yang lebih efisien.

DAFTAR PUSTAKA

- [1] Ali Warman Tarihoran, Modul CCNA Bootcamp, Training Partner, Jakarta, 2006.
- [2] Anonim, Modul Panduan Jaringan Komputer Dasar, Universitas Gunadarma, Depok, 2013.
- [3] Iwan Sofana, CISCO CCNA & JARINGAN KOMPUTER, Informatika, Bandung, 2012.
- [4] Dasar Jaringan Local Area Network
<http://robby.c.staff.gunadarma.ac.id/Downloads/files/4563/LAN.doc>
- [5] Model Jaringan OSI Layer.
<http://irianto.staff.gunadarma.ac.id/Downloads/files/16422/MODEL+JARINGAN+7+OSI+LAYER.pdf>
- [6] Modul CCNP URL: <http://www.routecloud.net/files/htp-student/>
- [7] URL: http://id.wikipedia.org/wiki/Penghala#Jenis-jenis_router
- [8] <http://studentsite.gunadarma.ac.id/>
- [9] <http://staff.gunadarma.ac.id/>
- [10] <http://baak.gunadarma.ac.id/>