|  |  |
| --- | --- |
| Laporan Ke | 7 |
| Tanggal Dikumpul | 17 November 2017 |
| Paraf Dosen/Teknisi |  |

**LAPORAN PRAKTIKUM**

**INFRASTRUKTUR SISTEM INFORMASI**

***(Configure Standard IPv4 ACLs and Configuring Extended ACLs)***



**OLEH :**

**ADE IRMA RILYANI**

**15753001**

**JURUSAN EKONOMI DAN BISNIS**

**POLITEKNIK NEGERI LAMPUNG**

**BANDAR LAMPUNG**

**2017**

**BAB I**

**PENDAHULUAN**

1.1.Latar Belakang

Salah satu keterampilan terpenting yang dibutuhkan administrator jaringan adalah penguasaan daftar kontrol akses (ACL). ACL menyediakan kemampuan packet filtering untuk mengendalikan arus lalu lintas. Perancang jaringan menggunakan firewall untuk melindungi jaringan dari penggunaan yang tidak sah. Firewall adalah solusi perangkat keras atau perangkat lunak yang memberlakukan kebijakan keamanan jaringan. Pertimbangkan kunci di pintu sebuah ruangan di dalam sebuah bangunan. Kunci hanya mengizinkan pengguna resmi dengan kunci atau kartu akses untuk melewati pintu. Demikian pula, firewall menyaring paket yang tidak sah atau berpotensi berbahaya untuk memasuki jaringan. Pada router Cisco, kita dapat mengkonfigurasi firewall sederhana yang menyediakan kemampuan penyaringan lalu lintas dasar menggunakan ACL. Administrator menggunakan ACL untuk memfilter lalu lintas, mengizinkan atau memblokir paket tertentu pada suatu jaringan.

1.2. Rumusan Masalah

1.2.1 Bagaimana cara mengkonfigurasi dan memverifikasi pengoperasian *Access Control List* (ACL)?

1.3. Tujuan

1.3.1 Mahasiswa diharapkan dapat mengkonfigurasi dan memverifikasi pengoperasian *Access Control List* (ACL).

**BAB II**

**LANDASAN TEORI**

**2.1 Pengertian Access Control List (ACL)**

ACL (Access Control List) merupakan metode selektivitas terhadap packet data yang akan dikirimkan pada alamat yang dituju. Secara sederhana ACL dapat kita ilustrasikan seperti halnya sebuah standard keamanan. Hanya packet yang memiliki kriteria yang sesuai dengan aturan yang diperbolehkan melewati gerbang keamanan, dan bagi packet yang tidak memiliki kriiteria yang sesuai dengan aturan yang diterapkan, maka paket tersebut akan ditolak. ACL dapat berisi daftar IP address, MAC Address, subnet, atau port yang diperbolehkan maupun ditolak untuk melewati jaringan.

**2.2 Jenis-jenis** **Access Control List (ACL)**

**2.2.1 Standard ACL**

Standard ACL merupakan jenis ACL yang paling sederhana. Standard 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. Standard ACL dapat diimplementasikan pada proses filtering protocol TCP, UDP atau pada nomor port yang digunakan. Meskipun demikian, Standard ACL hanya mampu mengijinkan atau menolak paket berdasarkan alamat sumbernya saja. Berikut ini adalah contoh konfigurasi dari Standard ACL.

|  |
| --- |
| Router(config)#access-list list list [nomor daftar akses IP standar] [permit / deny] [IP address] [wildcard mask] |

Pada konfigurasi di atas, nomor daftar akses IP adalah 1 – 99, kemudian permit / deny adalah sebuah parameter untuk mengizinkan atau menolak hak akses. IP address diisi dengan alamat pengirim atau alamat asal, kemudian wildcard mask adalah untuk menentukan jarak dari suatu subnet.

**2.2.2 Extended ACL**

Extended ACL merupakan jenis ACL yang mampu memberikan tingkat keamanan yang lebih baik ketimbang Standard ACL. Extended ACL mampu melakukan filtering pada alamat sumber (source) dan alamat tujuan (destination). Selain itu extended ACL memberikan keleluasaan kepada admin jaringan dalam melakukan proses filtering dengan tujuan yang lebih spesifik.

|  |
| --- |
| Router(config)#access-list [nomor daftar akses IP extended] [permit atau deny] [protokol] [source address] [wildcard mask] [destination address] [wildcard mask] [operator] [informasi port] |

Pada konfigurasi diatas, nomor daftar akses IP extended adalah 100 – 199, kemudian sama dengan standart ACL permit atau deny adalah sebuah parameter untuk mengizinkan atau menolak hak akses. Protokol dapat diisi dengan TCP, UDP, dsb. Destination address diisi dengan alamat yang akan dituju, wildcard mask untuk menentukan jarak subnet. Operator dapat diisi seperti eq

**2.3 Cara kerja Access Control List (ACL)**

Prinsip dasar cara kerja ACL adalah mencocokkan setiap packet yang akan dikirim dengan informasi yang telah dipetakan sebelumnya didalam daftar akses. Seandainya packet yang dikirim sesuai dengan kriteria yang didefinisikan didalam daftar akses, maka packet tersebut akan diijinkan (permit) untuk melawati router untuk kemudian diteruskan ke alamat yang dituju oleh packet. Tetapi, seandainya packet yang dikirim tidak sesuai dengan kriteria yang telah didefinisikan didalam daftar akses, maka packet yang akan dikirim tersebut langsung ditolak(deny).

**BAB III**

**PEMBAHASAN**

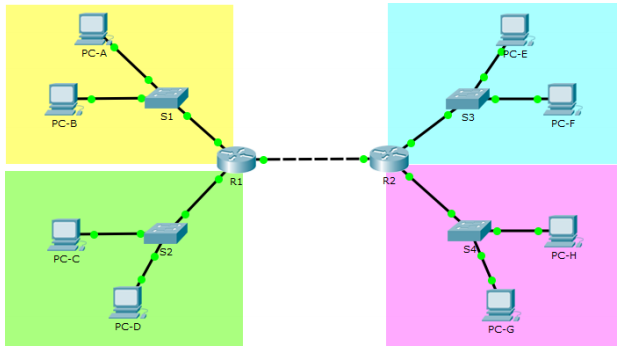
**4.1.3.5 Configure Standard IPv4 ACLs**

Organisasi baru-baru ini memutuskan untuk membatasi lalu lintas menggunakan ACL standar IPv4. Sebagai jaringan administrator, tugas Anda adalah mengkonfigurasi dua ACL standar IPv4 untuk membatasi lalu lintas ke LAN Pink dan LAN Biru (lihat Diagram Topologi PT). Anda juga harus mengkonfigurasi standar bernama IPv4 ACL untuk membatasi jarak jauh akses ke router R1. Interface router dan rute default / statis telah dikonfigurasi. Remote SSH akses juga telah diaktifkan pada router. Anda memerlukan informasi akses berikut untuk konsol, VTY, dan mode EXEC istimewa:

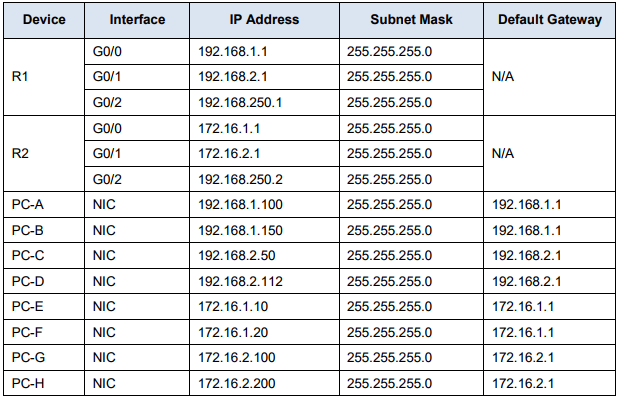
Nama pengguna: **admin01**

Password: **ciscoPA55**

Enable Secret: **secretPA55**



Gambar 1. Topology

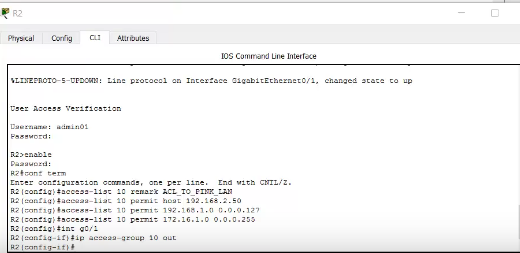


Gambar 2. *Addressing Table*

**Bagian 1: Mengkonfigurasi ACL Standar IPv4 untuk Membatasi akses ke LAN**

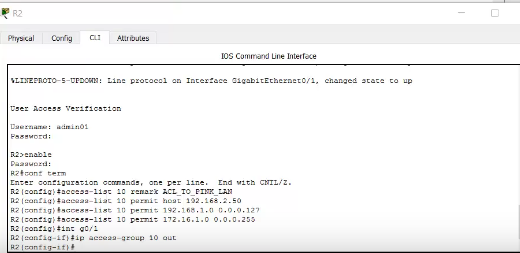
**Pink**

Pada Bagian 1, kita akan mengkonfigurasi dan menerapkan daftar akses 10 untuk membatasi akses ke LAN Pink. Lakukan konfigurasi seperti dibawah ini :



Gambar 3

Daftar akses 10 harus dikonfigurasi pada router yang benar, dan diterapkan pada inteface yang benar dan di sebelah kanan arah. Dengan mengetikkan perintah sebagai berikut :

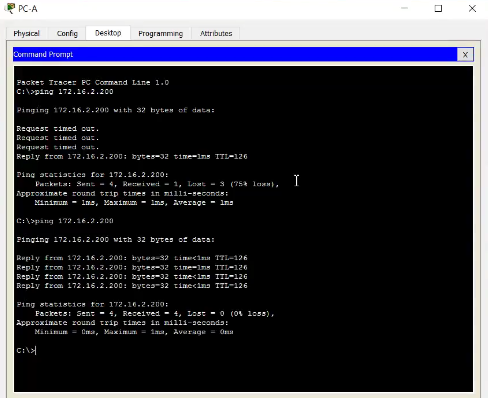


Gambar 4

Langkah selanjutnya yaitu buatlah kemudian terapkan, dan uji acces list 10. Setelah mengkonfigurasi dan menerapkan daftar akses 10, kita harus dapat melakukan tes jaringan berikut:

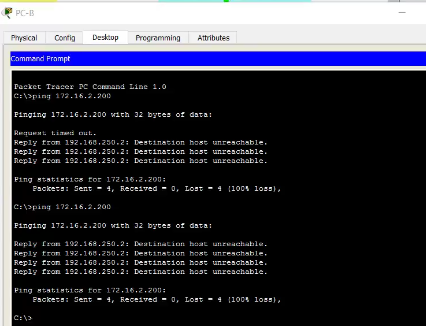
* Ping dari PC-A ke host di LAN Pink harus berhasil, tapi ping dari PC-B harus ditolak.

Ping dari PC-A :



Gambar 5

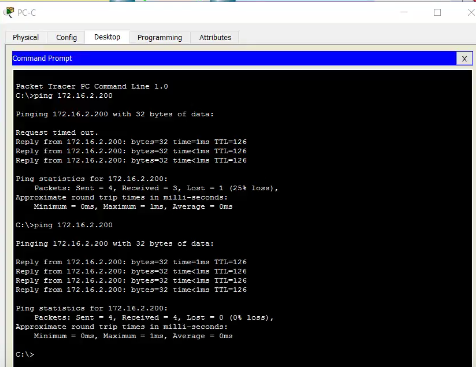
Ping dari PC-B :



Gambar 6

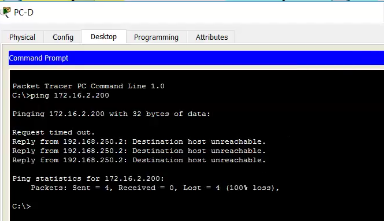
* Ping dari PC-C ke host di LAN Pink harus berhasil, tapi ping dari PC-D harus ditolak.

Ping dari PC-C :



Gambar 7

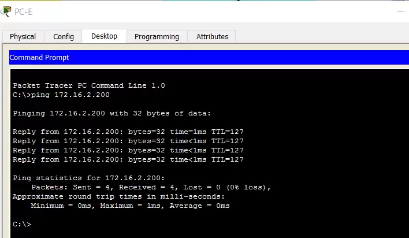
Ping dari PC-D :



Gambar 8

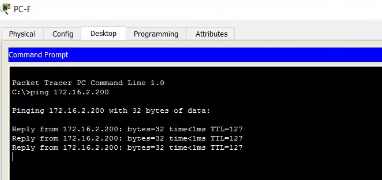
* Ping dari host di LAN Biru ke host di LAN Pink harus berhasil.

Ping dari PC-E :



Gambar 9

Ping dari PC-F :

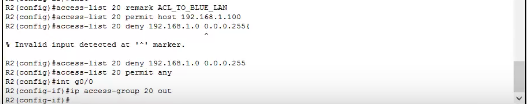


Gambar 10

**Bagian 2 : Mengkonfigurasi Standar IPv4 ACL untuk Membatasi Akses ke LAN Biru**

Pada Bagian 2 ini, kita akan mengkonfigurasi dan menerapkan daftar akses 20 untuk membatasi akses ke LAN Biru.

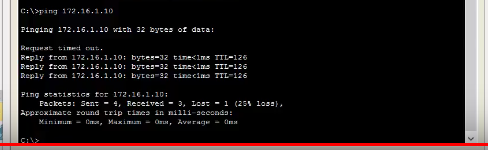
Langkah pertama dalam bagian ini yaitu buat garis besar apa yang ingin kita capai dengan access list 20. Kemudian access list 20 harus dikonfigurasi pada router yang benar, dan diterapkan pada interfaces yang benar dan ke arah yang benar. Dengan mengetikan perintah seperti pada gambar berikut :



Gambar 11

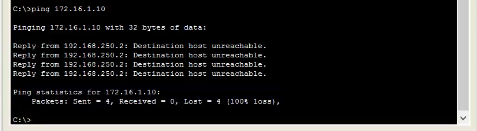
Langkah kedua yang harus dilakukan yaitu buatlah kemudian terapkan, dan uji access list 20. Setelah mengkonfigurasi dan menerapkan access list 20 Anda harus dapat melakukan tes jaringan berikut:

* Hanya PC-A di LAN Kuning yang berhasil melakukan ping ke LAN Biru.



Gambar 12

* Ping dari host di Yellow LAN ke Blue LAN harus gagal.



Gambar 13

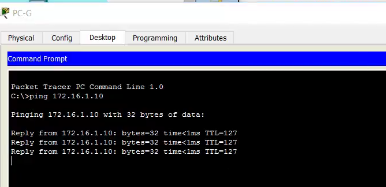
* Ping dari host di LAN Hijau dan Pink ke LAN Biru harus berhasil.

Ping dari PC-D :

D:\ADE IRMA RILYANI\SEMESTER 5\INFRA SI\PERBAGIAN\4135\Screenshot_2017-11-10_10-28-53.png PING PC D SUCCS.png

Gambar 14

Ping dari PC-G :

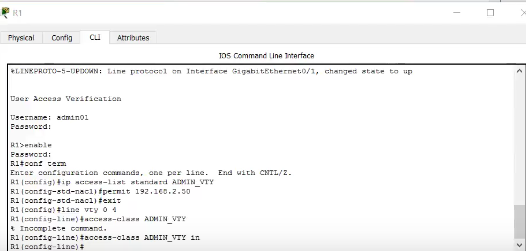


Gambar 15

**Bagian 3: Mengkonfigurasi Standar Bernama IPv4 ACL**

Pada Bagian 3, kita akan mengkonfigurasi dan menerapkan standar bernama IPv4 ACL untuk membatasi akses jarak jauh ke router R1.

Langkah pertama dalam bagian ini yaitu buat garis besar apa yang ingin kita capai dengan ACL Standard.

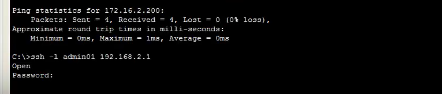


Gambar 16

Langkah selanjutnya yaitu Uji access list ADMIN\_VTY.

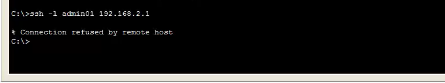
Setelah mengkonfigurasi dan menerapkan access list ADMIN\_VTY, Anda harus dapat melakukan tes jaringan berikut:

1. Sambungan SSH dari host PC-C ke R1 harus berhasil.



Gambar 17

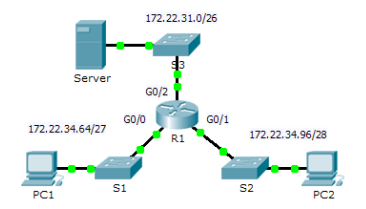
1. Sambungan SSH dari semua host lainnya harus gagal.



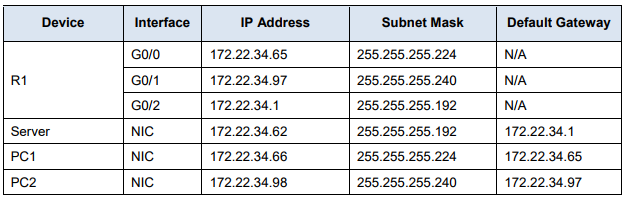
Gambar 18

**4.2.2.10 Configuring Extended ACLs - Scenario 1**

Dua karyawan membutuhkan akses ke layanan yang diberikan oleh server. PC1 hanya membutuhkan akses FTP sementara PC2 saja membutuhkan akses web Kedua komputer tersebut bisa melakukan ping ke server, tapi tidak saling berhubungan satu sama lain.



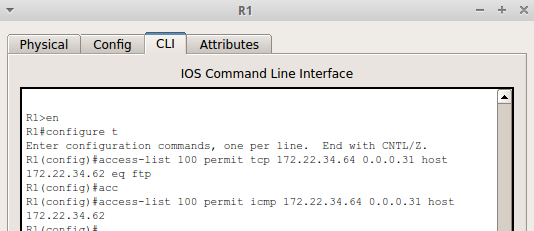
Gambar 1. Topology



Gambar 2. *Addressing Table*

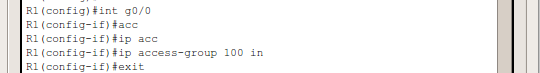
**Bagian 1 : Mengkonfigurasi, Menerapkan dan Verifikasi sebuah Extended Numbered ACL.**

Langkah pertama yang harus dilakukan yaitu Mengkonfigurasi ACL untuk mengizinkan FTP dan ICMP. Dengan mengetikan perintah seperti dibawah ini :



Gambar 3

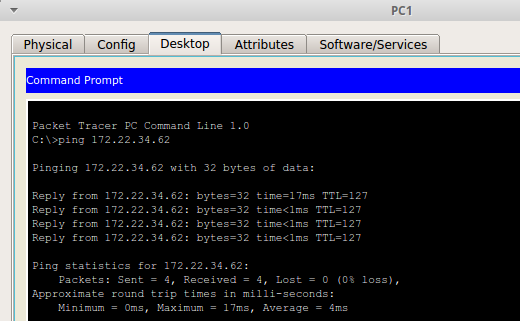
Langkah kedua yang harus dilakukan yaitu terapkan ACL pada interface yang benar untuk menyaring traffic. Dari perspektif R1, lalu lintas yang digunakan ACL 100 adalah inbound dari jaringan yang terhubung ke interface Gigabit Ethernet 0/0. Masukkan mode konfigurasi antarmuka dan pasang ACL. Seperti pada gambar berikut:



Gambar 4

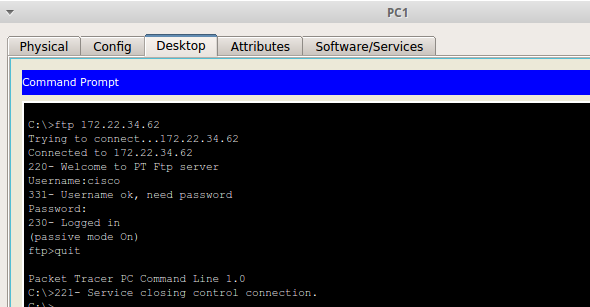
Langkah selanjutnya yaitu lakukan verifikasi implementasi ACL.

* Ping dari PC1 ke Server. Jika ping tidak berhasil, verifikasi alamat IP sebelum melanjutkan



Gambar 5

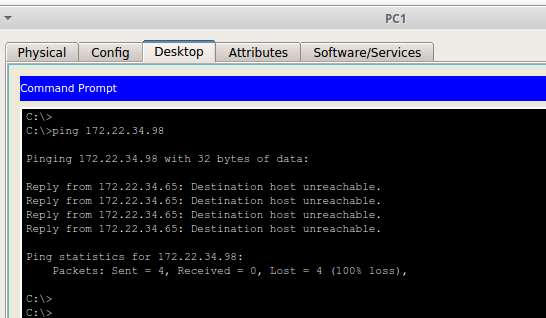
* FTP dari PC1 ke Server Username dan password keduanya cisco. Seperti dgambar dibawah ini :



Gambar 6

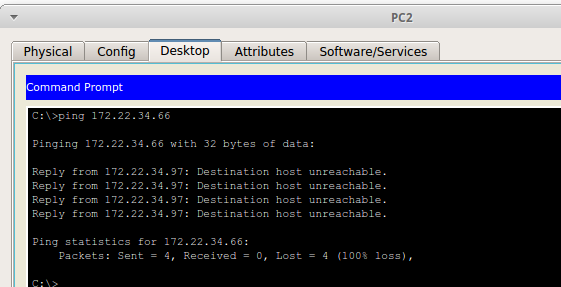
Ping dari PC1 ke PC2. Host tujuan harus tidak terjangkau, karena traffic tidak diizinkan secara eksplisit.

PC 1 :



Gambar 7

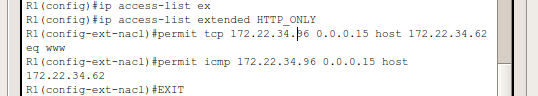
PC 2 :



Gambar 8

**Bagian 2 : Mengkonfigurasi, Menerapkan dan Verifikasi Extended Named ACL.**

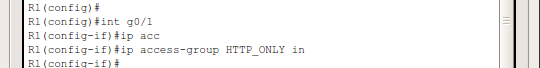
Langkah pertama yang dilakukan pada tahap ini adalah Mengkonfigurasi ACL untuk mengizinkan akses HTTP dan ICMP.



Gambar 9

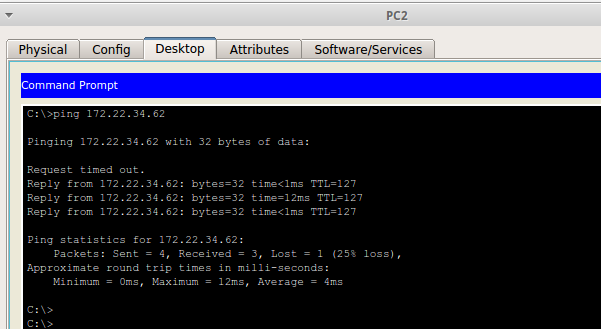
Langkah selanjutnya yaitu terapkan ACL pada interface yang benar untuk menyaring traffic.

Dari perspektif R1, traffic yang mengakses daftar HTTP\_ONLY berlaku untuk masuk dari jaringan yang terhubung ke interface Gigabit Ethernet 0/1. Masukkan mode konfigurasi interface dan pasang ACL.



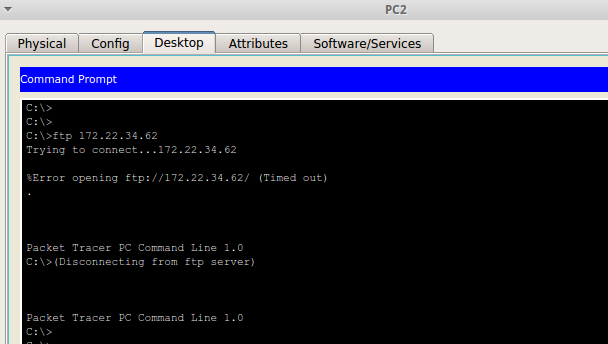
Gambar 10

Langkah yang terakhir yaitu Verifikasi implementasi ACL. Dengan meakukan pengujian seperti dibawah ini :

* Ping dari PC2 ke Server. Jika ping tidak berhasil, verifikasi alamat IP sebelum melanjutkan.

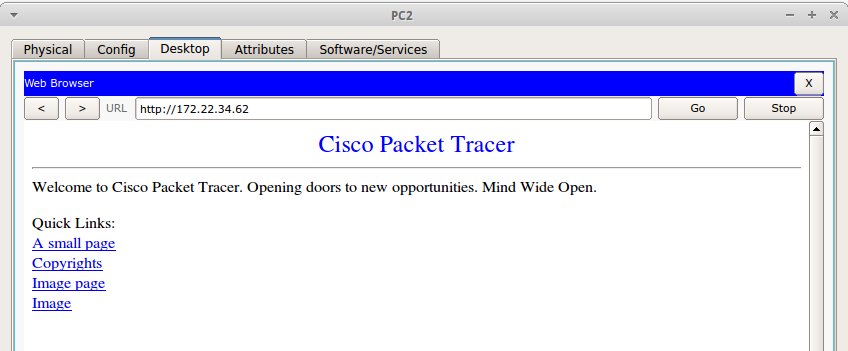
Gambar 11

* FTP dari PC2 ke Server Sambungannya harus gagal.



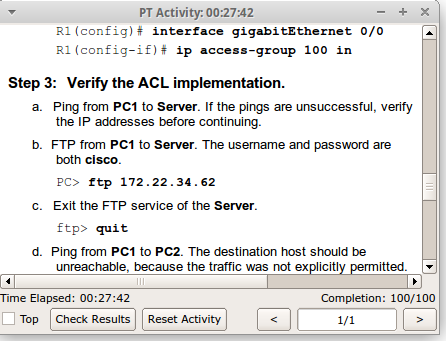
Gambar 12

* Buka web browser di PC2 dan masukkan alamat IP Server sebagai URL. Sambungannya harus berhasil.



Hambar 13

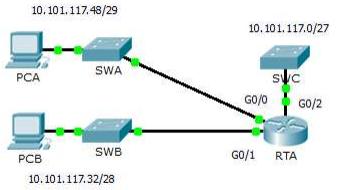
Cek Aktivity Result, jika konfigurasi sudah benar dan lengkap maka skor akan tampil 100/100 seperti pada gambar berikut :



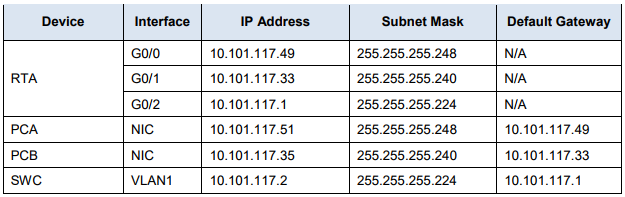
Gambar 14

**4.2.2.11 Configuring Extended ACLs - Scenario 2**

Dalam skenario ini, perangkat pada satu LAN diizinkan untuk mengakses perangkat dari jarak jauh di LAN lain menggunakan Telnet protokol. Selain ICMP, semua lalu lintas dari jaringan lain ditolak.



Gambar 1. Topology



Gambar 2. *Addressing Table*

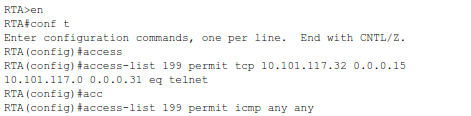
**Bagian 1 : Mengkonfigurasi, Menerapkan dan Verifikasi sebuah Extended Numbered ACL**

Langkah pertama yg perlu diperhatikan adalah :

* Lalu lintas Telnet dari perangkat pada jaringan 10.101.117.32/28 diizinkan untuk perangkat di 10.101.117.0/27 jaringan.
* Lalu lintas ICMP diperbolehkan dari sumber manapun ke tujuan manapun.
* Semua lalu lintas lainnya ke 10.101.117.0/27 diblokir.

**Langah 1. Mengkonfigurasi ACL yang diperpanjang.**

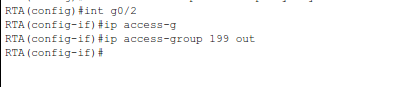
Ketikanlah perintah seperti dibawah ini :



Gambar 3

**Langkah 2. Menerapkan ACL yang diperpanjang.**

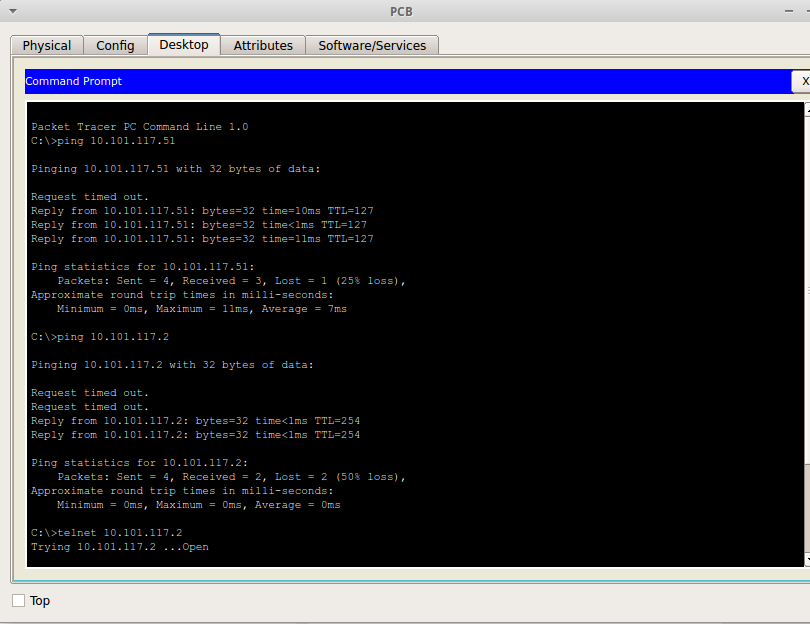
Karena daftar akses 199 mempengaruhi lalu lintas yang berasal dari kedua jaringan 10.101.117.48/29 dan 10.101.117.32/28, penempatan terbaik untuk ACL ini mungkin di antarmuka Gigabit Ethernet 0/2 dalam arah keluar. Ketikan perintah seperti di bawah ini :



Gambar 4

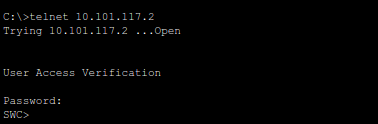
**Langkah 3. Verifikasi penerapan ACL yang diperpanjang.**

1. Ping dari PCB ke semua alamat IP lainnya di jaringan. Jika ping tidak berhasil, verifikasi IP alamat sebelum melanjutkan. Seperti gambar berikut :



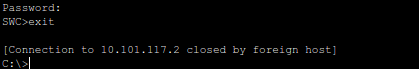
Gambar 5

1. Telnet dari PCB ke SWC. Kata sandinya adalah cisco.



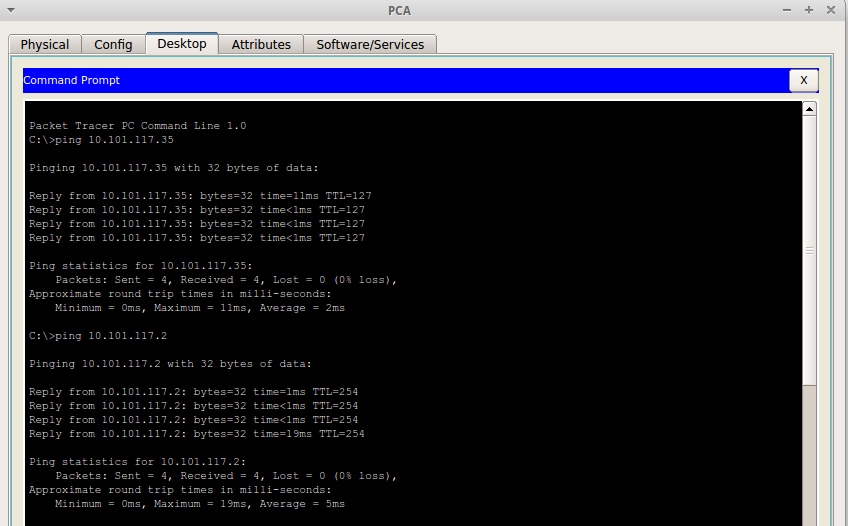
Gambar 6

1. Keluar dari layanan Telnet dari UKSW.



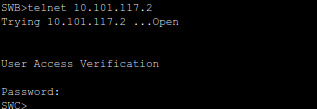
Gambar 7

1. Ping dari PCA ke semua alamat IP lainnya di jaringan. Jika ping tidak berhasil, verifikasi IP alamat sebelum melanjutkan. Seperti gambar berikut :

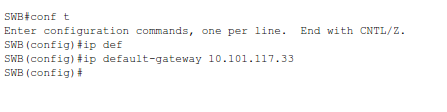


Gambar 8

1. Telnet dari PCA ke SWC. Daftar akses menyebabkan router menolak koneksi.

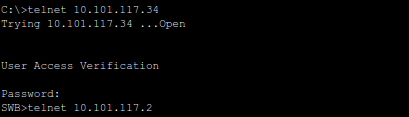


Gambar 9



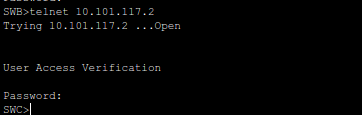
Gambar 10. Untuk memperbaiki kesalahan di atas maka lakukan konfigurasi ulang pada ip default gateway di SWB.

1. Telnet dari PCA ke SWB. Daftar akses ditempatkan pada G0 / 2 dan tidak mempengaruhi koneksi ini. Setelah masuk ke SWB, jangan log out.



Gambar 11

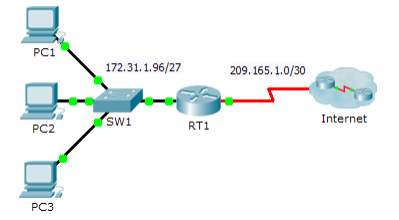
1. Setelah masuk ke SWB, jangan log out. Telnet ke SWC.



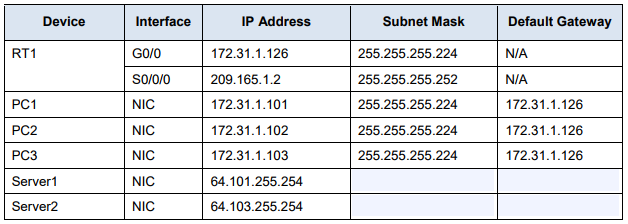
Gambar 12

**4.2.2.12 Configuring Extended ACLs - Scenario 3**

Dalam skenario ini, perangkat tertentu di LAN diizinkan untuk berbagai layanan pada server yang terletak di Internet.



Gambar 1. Topology



Gambar 2. *Addressing Table*

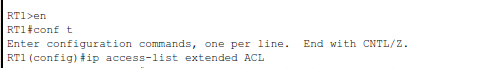
**Bagian 1: Mengkonfigurasi ACL Bernama yang Ditunjuk**

Gunakan satu nama ACL untuk menerapkan kebijakan berikut:

* Blok akses HTTP dan HTTPS dari PC1 ke Server1 dan Server2. Server berada di dalam awan dan Anda hanya tahu alamat IP mereka.
* Blok akses FTP dari PC2 ke Server1 dan Server2.
* Blokir akses ICMP dari PC3 ke Server1 dan Server2.

Langkah 1: Deny PC1 mengakses HTTP dan layanan HTTPS pada Server1 dan Server2.

1. Buat daftar akses IP diperpanjang bernama ACL yang akan menolak akses PC1 ke layanan HTTP dan HTTPS Server1 dan Server2. Karena tidak mungkin untuk langsung mengamati subnet server di Internet, dibutuhkan empat aturan.



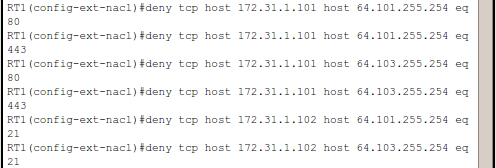
Gambar 3

b. Catatlah pernyataan yang menolak akses dari PC1 ke Server1, hanya untuk HTTP (port 80).

c. Catatlah pernyataan yang menolak akses dari PC1 ke Server1, hanya untuk HTTPS (port 443).

d. Catatlah pernyataan yang menolak akses dari PC1 ke Server2, hanya untuk HTTP.

e. Catatlah pernyataan yang menolak akses dari PC1 ke Server2, hanya untuk HTTPS.

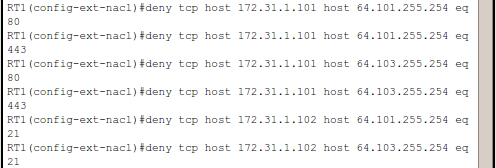


Gambar 4

Langkah 2: Deny PC2 untuk mengakses layanan FTP pada Server1 dan Server2.

1. Catatlah pernyataan yang menolak akses dari PC2 ke Server1, hanya untuk FTP (hanya port 21).

b. Catatlah pernyataan yang menolak akses dari PC2 ke Server2, hanya untuk FTP (hanya port 21).



Gambar 5

Langkah 3: Deny PC3 untuk ping Server1 dan Server2.

1. Catatlah pernyataan yang menolak akses ICMP dari PC3 ke Server1.

b. Catatlah pernyataan yang menolak akses ICMP dari PC3 ke Server2.

D:\ADE IRMA RILYANI\SEMESTER 5\INFRA SI\PERBAGIAN\4.2.2.12\4.2.2.12\3.png

Gambar 6

Langkah 4: Izinkan semua lalu lintas IP lainnya.

D:\ADE IRMA RILYANI\SEMESTER 5\INFRA SI\PERBAGIAN\4.2.2.12\4.2.2.12\4.png

Gambar 7

**Bagian 2: Menerapkan dan Verifikasi Extended ACL**

Lalu lintas yang akan disaring berasal dari network 172.31.1.96/27 dan ditujukan untuk network jarak jauh.

Langkah 1: Terapkan ACL ke interface yang benar dan ke arah yang benar.

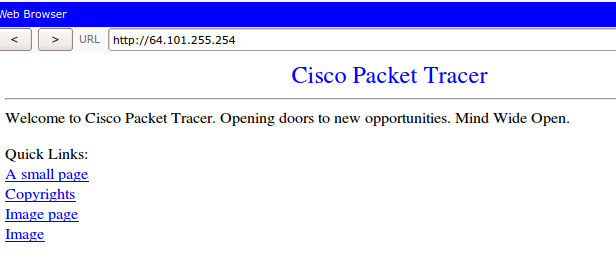
1. Perintah untuk menerapkan ACL ke interface yang benar dan arah yang benar?

D:\ADE IRMA RILYANI\SEMESTER 5\INFRA SI\PERBAGIAN\4.2.2.12\4.2.2.12\5.png

Gambar 8

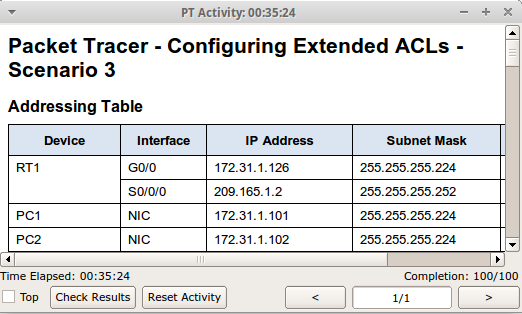
Langkah 2: Uji akses untuk setiap PC.

1. Akses situs web Server1 dan Server2 menggunakan Browser Web PC1 dan menggunakan protokol HTTP dan HTTPS.



Gambar 9

Cek Aktivity Result, jika konfigurasi benar dan lengkap maka skor akan tampil 100/100 seperti pada gambar berikut :



Gambar 10

**BAB IV**

**PENUTUP**

**4.1 Kesimpulan**

Berdasarkan praktikum yang telah kita laksanakan tersebut, kita dapat menyimpulkan bahwa dengan mengetahui dan memahami bagaimana cara langkah-langkah konfigurasi standar IPV4 dan Extend pada ACL, maka kita dapat membuat konfigurasi dan verifikasi ACL sendiri agar memudahkan kita dalam mengendalikan arus lalu lintas dan penguasaan daftar control akses pada suatu jaringan.