zenhadi@eepis-its.edu

MODUL 2
ACCESS CONTROL LIST

TUJUAN PEMBELAJARAN:

1. Mahasiswa mampu memahami aplikasi access-list.
2. Mahasiswa mampu mengkonfigurasi access-list dengan Cisco Router
3. Mahasiswa mampu menerapkan access-list pada suatu jaringan

DASAR TEORI

Standard IP Access List merupakan salah satu metode **Daftar Akses (Access List)** yang dipergunakan Cisco untuk **mengatur keluar masuknya traffic** ke dalam maupun keluar router. Metode ini biasa disebut dengan "**packet filtering**". Daftar akses (Access List) ini berfungsi untuk membandingkan atau mencocokkan setiap paket yang diterima atau di tolak dengan aturan atau daftar akses yang di terapkan pada router tersebut.

Access lists mengijinkan atau menolak pernyataan bahwa filter traffic dapat ke segmen jaringan dan dari segmen jaringan berdasarkan pada:

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

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.

Penggunaan access list yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan. 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 mengakses sumber daya WWW sementara yang lainnya ditolak. Dengan kombinasi access list yang benar, network manajer mempunyai kekuasaan untuk memaksa hampir semua kebijakan keamanan yang bisa mereka ciptakan.

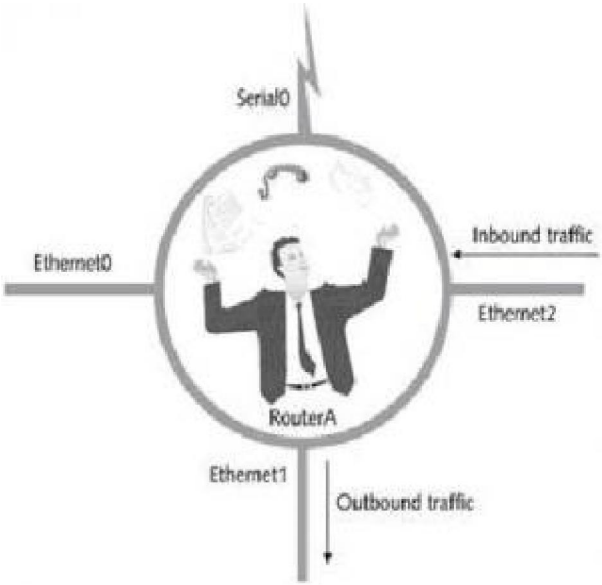
Access list juga bisa digunakan pada situasi lain yang tidak harus meliputi penolakan paket. Sebagai contoh access list digunakan untuk mengontrol network mana yang akan atau tidak dinyatakan oleh protocol dynamic routing. Konfigurasikan access list dengan cara yang sama. Perbedaannya disini hanyalah bagaimana menerapkannya ke protocol routing dan bukan ke interface. Kita juga bisa menggunakan access list untuk mengkategorikan paket atau antrian /layanan QOS, dan mengontrol tipe lalu lintas data nama yang akan mengaktifkan link ISDN.

Membuat access list sangat mirip dengan statement pada programming if – then jika sebuah kondisi terpenuhi maka aksi yang diberikan akan dijalankan/tidak terpenuhi, tidak ada yang terjadi dan statemen berikutnya akan dievaluasi. Statement ACL pada dasarnaya dalah paket filter dimana paket dibandingkan, dimana paket dikategorikan dan dimana suatu tindakan terhadap paket dilakukan.

List(daftar) yang telah dibuat bisa diterpakan baik kepada lalulintas inbound maupun outbound pada interface mana saja. Menerapkan ACL menyebabkan router menganalisa

setiap paket arah spesifik yang melalui interface tersebut dan mengmbil tindakan yang sesuai. Ketika paket dibandingkan dengan ACL, terdapat beberapa peraturan (rule) penting yang diikuti:

- Paket selalu dibandingkan dengan setiap baris dari ACL secara berurutan, sebagai contoh paket dibandingkan dengan baris pertama dari ACL, kemudian baris kedua, ketiga, dan seterusnya.
- Paket hanya dibandingkan baris-baris ACL sampai terjadi kecocokan. Ketika paket cocok dengan kondisi pada baris ACL, paket akan ditindaklanjuti dan tidak ada lagi kelanjutan perbandingan.
- Terdapat statement "tolak" yang tersembunyi (impilicit deny) pada setiap akhir baris ACL, ini artinya bila suatu paket tidak cocok dengan semua baris kondisi pada ACL, paket tersebut akan ditolak



Gambar 1. Inbound dan outbound trafik

Gambar 2. Standard dan Extended Access List

Gambar 3. Penempatan Standard dan Extended Access List

Jenis ACL

a. Standard ACL

Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.

b. Extended ACL

Extended ACL bisa mengevalusai banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi alamat IP sumber dan tujuan, field protocol pada header network layer dan nomor port pada header transport layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas.

Jenis Lalu Lintas ACL

a. Inbound ACL

Ketika sebuah ACL diterapkan pada paket inbound di sebuah interface, paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan.

b. Outbond ACL

Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut di-route ke outbound interface dan diproses melalui ACL malalui antrian.

Panduan Umum ACL

Terdapat beberapa panduan umum ACL yang seharusnya diikuti ketika membuat dan mengimplementasikan ACL pada router :

- Hanya bisa menerapkan satu ACL untuk setiap interface, setiap protocol dan setiap arah. Artinya bahwa ketika membuat ACL IP, hanya bisa membuat sebuah inbound ACL dan satu Outbound ACL untuk setiap interface.
- Organisasikan ACL sehingga test yang lebih spesifik diletakkan pada bagian atas ACL
- Setiap kali terjadi penambahan entry baru pada ACL, entry tersebut akan diletakkan pada bagian bawah ACL. Sangat disarankan menggunakan text editor dalam menggunakan ACL

- Tidak bisa membuang satu baris dari ACL. Jika kita mencoba demikian, kita akan membuang seluruh ACL. Sangat baik untuk mengcopy ACL ke text editor sebelum mencoba mengubah list tersebut.

Wildcard Masking

Wildcard masking digunakan bersama ACL untuk menentukan host tunggal, sebuah jaringan atau range tertentu dari sebuah atau banyak network. Untuk mengerti tentang wildcard, kita perlu mengerti tentang blok size yang digunkan untuk menentukan range alamat. Beberapa blok size yang berbeda adalah 4, 8, 16, 32, 64.

Ketika kita perlu menentukan range alamat, kita memilih blok size selanjutnya yang terbesar sesuai kebutuhan. Sebagai contoh, jika kita perlu menentukan 34 network, kita memerlukan blok size 64. jika kita ingin menentukan 18 host, kita memerlukan blok size 32. jiak kita perlu menunjuk 2 network, maka blok size 4 bisa digunakan. Wildcard digunakan dengan alamat host atau network untuk memberitahukan kepada router untuk difilter. Untuk menentukan sebuah host, alamat akan tampak seperti berikut 172.16.30.5 0.0.0.0 keempat 0 mewakili setiap oktet pada alamat. Dimanapun terdapat 0, artinya oktet pada alamat tersebut harus persis sama. Untuk menentukan bahwa sebuah oktet bisa bernilai apa saja, angka yang digunakan adalah 255. sebagai contoh, berikut ini adalah subnet /24 dispesifikasikan dengan wildcard: 172.16.30.0 0.0.255 ini memberitahukan pada router untuk menentukan 3 oktet secara tepat, tapi oktet ke-4 bisa bernilai apa saja.

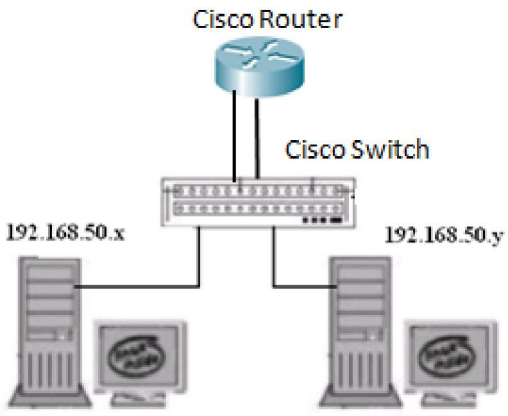
PERALATAN :
1. PC Client dengan sistem operasi Linux
2. Cisco Switch
3. Cisco Router

TUGAS PENDAHULUAN

1. Apa perbedaan antara LAN dan VLAN ?
2. Mengapa dalam VLAN diperlukan router ?

PERCOBAAN

Bangunlah jaringan sebagai berikut :

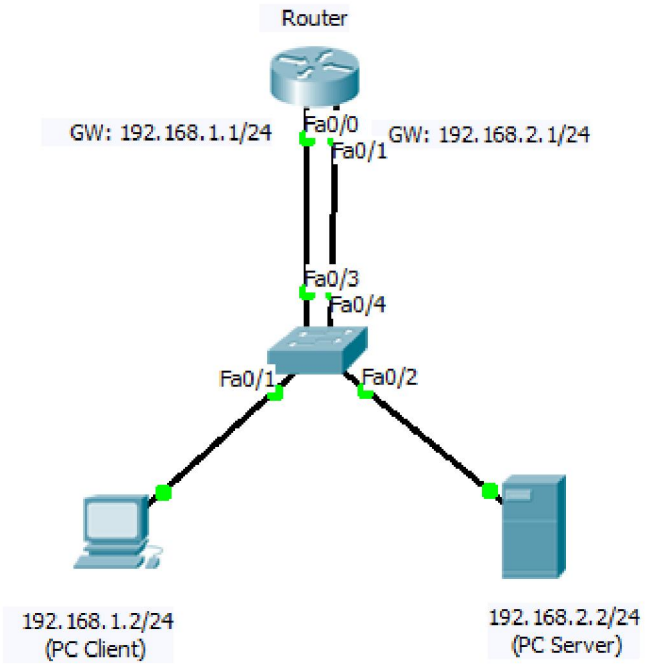


Gambar 4. Jaringan Percobaan

NB:
Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.
192.168.50.x & y : IP dari router.

A. Percobaan ACL dengan Standard Access-lisst

Sebelum setting pada jaringan sesungguhnya, buatlah dahulu simulasinya di packet tracer.



1. Rubah IP di PC dan tambahkan gateway di masing-masingnya.

   PC Client :

```
# ifconfig   eth0  192.168.1.2 netmask 255.255.255.0
# route  add -net default  gw  192.168.1.1
```

   PC Server :

```
# ifconfig   eth0  192.168.2.2 netmask 255.255.255.0
# route  add -net default  gw  192.168.2.1
```

   Lakukan tes koneksi (ping dan traceroute) antara PC Client dan PC Server, catat hasilnya.

   NB : Setting diatas pada kelompok 1; untuk kelompok 2, gunakan netID 192.168.11.0/24 dan 192.168.12.0/24, begitu seterusnya.

2. Setting IP di masing-masing interface Cisco Router
   a. Masuk ke configure mode untuk mulai konfigurasi

```
Router# configure terminal
Router(config)#
```

   b. Konfigurasi port fastethernet dan berikan ip address pada port tersebut

   Konfigurasi pada interface fastethernet 0/0

```
Router(config)# interface fastethernet 0/0
Router(config-if) # ip address 192.168.1.1 255.255.255.0
Router(config-if) # no shutdown     => untuk mengaktifkan interface
Router(config-if) # CTRL+Z          => utk kembali ke privileged mode
Router #
```

   Konfigurasi pada interface fastethernet 0/1

```
Router(config)# interface fastethernet 0/1
Router(config-if) # ip address 192.168.2.1 255.255.255.0
Router(config-if) # no shutdown     => untuk mengaktifkan interface
```

```
Router(config-if) # CTRL+Z          => utk kembali ke privileged mode
Router #
```

c. Jalankan perintah berikut dan catat hasilnya.

```
Router# show ip interface brief
Router# show ip route
```

3. Pada PC
   Tes koneksi dari PC Client ke PC Server. Gunakan ping dan traceroute, catat hasilnya. Bandingkan hasilnya dengan langkah 1.

4. Setting ACL pada Cisco Router
   a. Lakukan blocking koneksi dari jaringan 192.168.1.0/24 ke jaringan 192.168.2.0/24.

```
Router#conf t
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 10 permit any
```

   b. Terapkan acl pada interface yang dekat dengan destination packet

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group 10 out
Router(config-if)#^Z
Router#
```

   c. Lihat konfigurasi, dan catat hasilnya.

```
Router#show  access-lists
Router#show  run
```

5. Pada PC
   Tes koneksi dari PC Client ke PC Server. Gunakan ping dan traceroute, catat hasilnya. Bandingkan hasilnya dengan langkah 3.

B. Percobaan ACL dengan Extended Access-lisst

1. Setting di Cisco Router, hapus acl sebelumnya

```
Router#conf t
Router(config)#no access-list 10
Router(config)# interface fastEthernet 0/1
Router(config-if)# no ip access-group 10 out
```

2. Pada PC
   a. Lakukan instalasi aplikasi server pada PC Server (web server, ftp server, telnet dan ssh)

```
# apt-get install apache2 proftpd telnetd openssh-server
```

   b. Cek, apakah port pada aplikasi tersebut sudah terbuka, catat hasilnya.

```
# nmap localhost

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-10-08
19:18 WIT
Interesting ports on localhost (127.0.0.1):
Not shown: 1670 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
```

```
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
```

c. Lakukan akses dari PC Client, dan pastikan semua aplikasi di atas dapat diakses dari client. Catat semua hasilnya.

```
# telnet <ip_server>
# ssh <ip_server>
# ftp <ip_server>
# ping <ip_server>
Web dari iceweasel.
```

3. Setting di Cisco Router
   a. Buat suatu rule di router sebagai berikut :
   Tolak akses telnet, ftp dan ping dari PC Client.
   Ijinkan akses web dan ssh dari PC Client.

```
Router#conf t
Router(config)#access-list 110 deny tcp host 192.168.1.2 host 192.168.2.2 eq 23
Router(config)#access-list 110 deny tcp host 192.168.1.2 host 192.168.2.2 eq 21
Router(config)#access-list 110 deny icmp host 192.168.1.2 host 192.168.2.2
Router(config)#access-list 110 permit ip any any
```

   b. Terapkan acl tersebut pada interface yang dekat dengan source yang paketnya ditolak

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 110 in
Router(config-if)#^Z
Router#
```

   c. Lihat konfigurasi, dan catat hasilnya.

```
Router#show access-lists
Router#show run
Router#show ip interface
```

4. Pada PC
   Tes koneksi dari PC Client ke PC Server. Ulangi langkah 2.c dan bandingkan hasilnya.

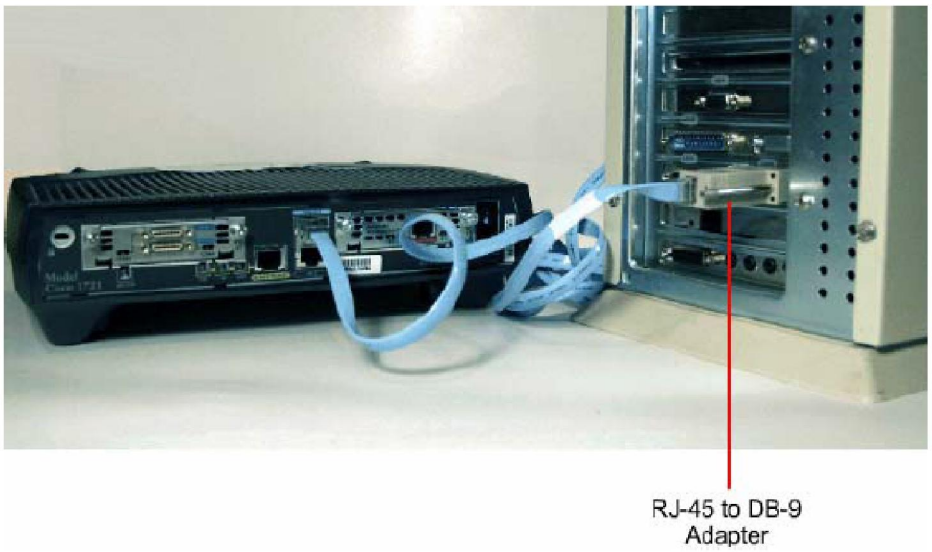
LAPORAN RESMI

Daftar Pertanyaan

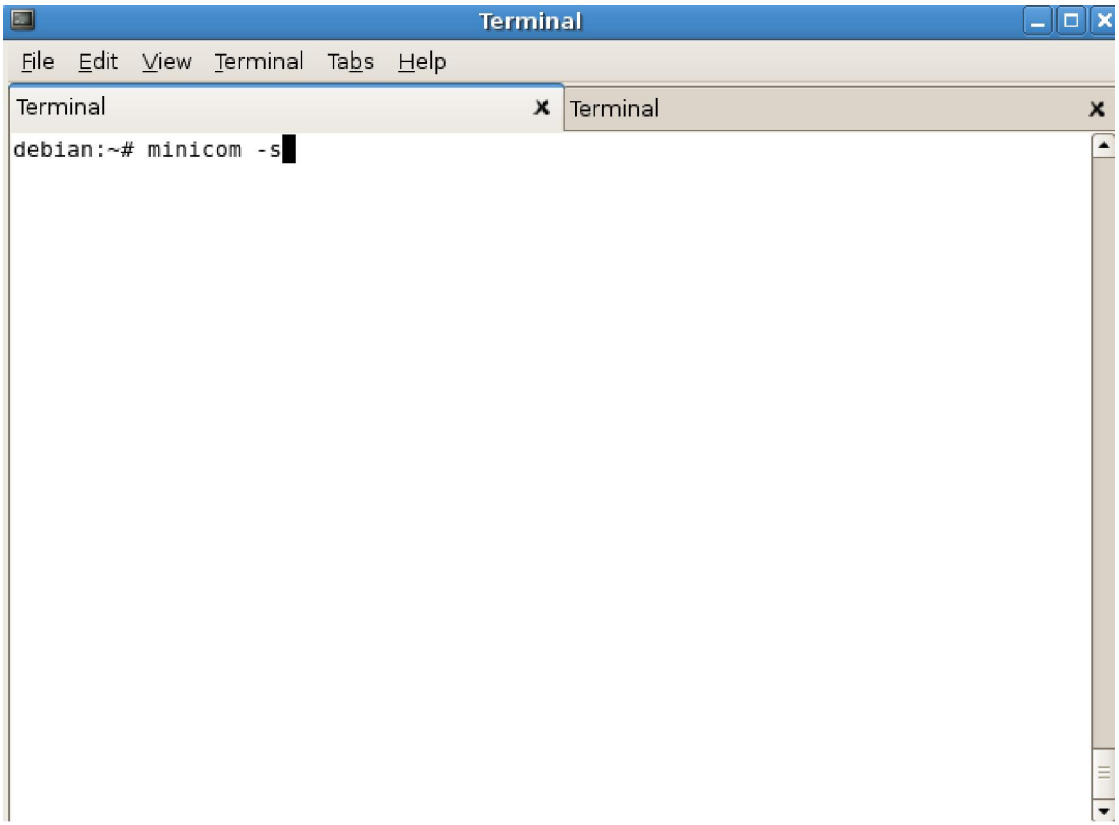
1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Tugas akan diberikan oleh dosen waktu praktikum

LAMPIRAN

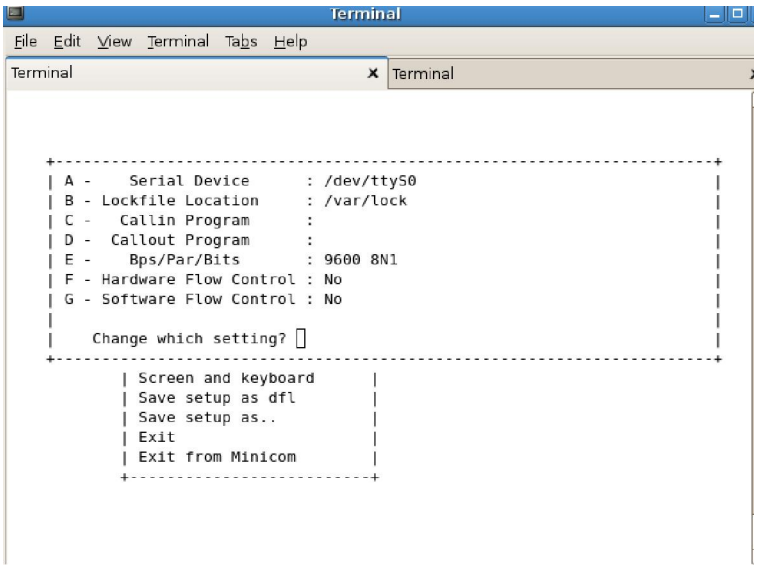
SETTING SWITCH DAN ROUTER DARI PC MENGGUNAKAN LINUX



1. Hubungkan kedua PC pada serial port dengan Router pada interface “console” menggunakan kabel console.
2. Nyalakan PC
3. Jalankan aplikasi Minicom



4. Pilih Serial Port pada menu. Ganti nilai “Current 38400 8N1” menjadi “9600 8N1” dengan menekan tombol “E”, atur juga Hardware Flow Control dan Software Flow Control menjadi “No”.



12. Melakukan komunikasi ke perangkat switch atau router.