Konsep Konfigurasi Access List (ACL)

Posted by [emulanetwork](https://emulanetwork.wordpress.com/author/emulanetwork/) on [January 13, 2011](https://emulanetwork.wordpress.com/2011/01/13/konsep-konfigurasi-access-list-acl/)



Implementasi ACL

*RoadToCCNA  –*Bismillahirrahmaanirrahiim.. Akhirnya kita berjumpa lagi kawan

Pada bahasan sebelumnya kita membahas mengenai NAT yang sederhananya berfungsi mengoptimalkan pemakaian IP address public yang dipakai secara bersama dalam jaringan lokal. Tapi  selama *nyemplung*di blog Emulanetwork, pernah *ga* terbayang dalam benak kita untuk lebih mengoptimalkan jaringan komputer, baik LAN maupun WAN? Seperti paket mana yang diijinkan masuk ke dalam sebuah jaringan internal dan paket mana yang ditolak, atau paket mana saja yang akan dilepas ke jaringan eksternal (inside global) dan paket mana yang tidak di lepas, atau alamat-alamat mana saja yang diijinkan melakukan koneksi dengan alamat-alamat spesifik dan mana yang tidak boleh, atau layanan-layanan apa saja yang boleh digunakan oleh suatu alamat dan layanan-layanan apa saja yang tidak boleh, atau…. alamat-alamat mana saja yang boleh dan tidak boleh mengakses layanan-layanan khusus..?

Yup, benar sekali kawan… itulah beberapa fungsi sederhana dari Access List.

Dalam bahasa *wong djaringan*, sebernarnya access list merupakan sebuah daftar yang dirancang untuk menampung aturan-aturan yang digunakan untuk mengkontrol paket-paket yang lalu-lalang dalam sebuah jaringan, khususnya paket-paket datagram yang melewati sebuah router. Nah, sebelum terkena proses *access list,*paket-paket tersebut terlebih dahulu harus mendapat izin routing untuk melintas antar jaringan dari router-router yang terhubung, apabila izin routing (permit or deny) telah di dapat, maka proses *access list*diterapkan pada paket tersebut.

**Cara Kerja Sederhana Access List (ACL)**

Berdasarkan beberapa referensi yang saya pelajari, setidaknya ada tiga aturan yang berlaku bagi sebuah paket, jika access list di terapkan pada router, yaitu:

1.      Setiap paket akan dibandingkan dengan setiap baris aturan Access List secara urut.

2.      Jika menemukan kondisi yang sesuai maka paket terebut akan mengikuti aturan yang ada dalam Access List.

3.      Apabila paket tersebut tidak menemukan aturan yang sesuai maka paket tersebut tidak diperbolehkan lewat atau mengakses jaringan.

Penerapan access list itu sendiri terbagi menjadi dua macam, antara lain:

1.      **Standard Access List** –  yang akan melakukan penyeleksian paket berdasarkan alamat IP pengirim paket.

2.      **Extended Access List** –  yang akan menyeleksi sebuah paket berdasarkan alat IP pengirim dan penerima, protokol, dan jenis port paket yang dikirim.

Nah, ketika ACL dikonfigurasi pada sebuah router, maka ACL harus memiliki sebuah nomor identifikasi unik yang diberikan kepadanya. Nomor ini menandakan jenis access list yang dibuat dan harus berada pada range tertentu dari nomor yang valid untuk jenis daftar tersebut.

|  |  |
| --- | --- |
| **Jenis Access List** | **Range Nomor Pengenal** |
| **IP Standard** | 1-99 |
| **IP Extended** | 100-199 |
| **IPX Standard** | 800-899 |
| **IPX Extended** | 900-999 |
| **Apple Talk** | 600-699 |
| **IPX SAP Filter** | 1000-1099 |

**Konfigurasi Standar Acess List**

Berdasarkan tabel diatas, maka standar access list akan melakukan seleksi terhadap paket menggunakan alamat IP pengirim dengan range nomor pengenal yang dapat digunakan adalah nomor 1 sampai 99.

Ingat saja rumusnya kawan:

Router(config)# **access-list** [nomor pengenal] {permit/deny} [alamat pengirim] [wildcard-mask]

Misal: Router\_Pusat(config)#access-list 10 permit 172.25.0.0 0.0.255.255

Pada contoh tersebut [Router1] mengijinkan semua host atau paket yang berasal dari network ID 172.25.0.0 untuk melewati [Router\_Pusat]. Angka 0.0.255.255 (wildcard) digunakan untuk membandingkan paket, sehingga semua network ID yang di cek cukup 2 (dua) bagian terdepan yaitu 172.25. Apabila angka wildcard yang digunakan 0.0.0.255 maka network ID yang di cek adalah 3 (tiga) bagian terdepan, misalnya 172.25.82.

Ada beberapa tahap yang harus kita lakukan untuk mengkonfigurasi Standard Access List, yaitu:

1. Memberikan identitas (nama, alamat IP, subnet mask, dan gateway untuk komputer yang terhubung) ke router pusat.
2. Mengkonfigurasi routing antara 2 (dua) jaringan yang akan dikenakan Access List. Nah *routing*dilakukan agar kedua jaringan tersebut terhubung terlebih dahulu sebelum ada *Packet Filtering*.
3. Membuat Access List dan menerapkannya pada interface router.

Sebagai contoh kita akan simulasikan pada kasus dibawah ini, *lets learning by doing* kawan..



Ada dua buah jaringan lokal yang terhubung pada router dengan spesifikasi:

>> Router A,

IP Inside Global    : 200.100.10.1/30 (S0/0/0 DCE)

IP Inside Local      : 192.168.100.1/24 (F0/0)

>> Router B,

IP Inside Global : 200.100.10.2/30 (S0/0/0 DCE)

IP Inside Local   : 172.16.1.1/16 (F0/0)

Semua konfigurasi routing protokol dapat digunakan, kecuali RIP karena dalam simulasi ini kita menggunakan teknik subnetting pada ip publicnya, masih ingat kan alasannya kawan?

Nah pada simulasi kali ini kita akan mengijinkan semua host dari jaringan *inside local*Router B, 172.16.0.0/16 dapat mengakses jaringan *inside local*Router A, 192.168.100.0/24. Maka perintahnya adalah:

Router>en

Router#conf t

Router(config)#host Router\_A

Router\_A#int f0/0

Router\_A(config-if)#ip add 192.168.100.1 255.255.255.0

Router\_A(config-if)#int s0/0/0

Router\_A(config-if)#ip add 200.100.10.1 255.255.255.252

Router\_A(config-if)#exit

Router\_A(config)#router eigrp 100

Router\_A(config-router)#net 192.168.100.0

Router\_A(config-router)#net 200.100.10.0

Router\_A(config-router)#exit

//Konfigurasi Access List Pada Router A

Router\_A(config)#access-list 10 permit 172.16.0.0 0.0.255.255

Router\_A(config)#exit

//Selanjutnya kita dapat menerapkannya khusus pada interface f0/0 pada router A

Router\_A(config)#int f0/0

Router\_A(config-if)#ip access-group 10 out

Router\_A(config-if)#exit

//Opsi[out] pada bagian akhir perintah tersebut dimaksudkan untuk melewatkan paket keluar dari Router A tersebut.

//Untuk melihat konfigurasi access list

Router#show access-lists

Standard IP access list 10

permit 172.16.0.0 0.0.255.255 (2 match(es))

Nah, berikutnya adalah kita akan memberikan akses hanya pada satu host dari *inside local* pada Router B (PC B3) dengan alamat IP 172.16.0.3/16 agar dapat mengakses ke jaringan 192.168.100.0/16. Maka perintahnya adalah sebagai berikut:

//Konfigurasi Access List Pada Router A

Router\_A(config)#access-list 20 permit 172.16.0.3 0.0.0.0

Router\_A(config)#exit

//Selanjutnya kita dapat menerapkannya khusus pada interface f0/0 pada router A

Router\_A(config)#int f0/0

Router\_A(config-if)#ip access-group 20 out

Router\_A(config-if)#exit

//Opsi[out] pada bagian akhir perintah tersebut dimaksudkan untuk melewatkan paket keluar dari Router A tersebut.

//Untuk melihat konfigurasi access list

Router#show access-lists

Standard IP access list 10

permit 172.16.0.0 0.0.255.255 (5 match(es))

Standard IP access list 20

permit host 172.16.0.3 (4 match(es))

**Konfigurasi Extended Access List**

Untuk mengkonfigurasi Extended Access List sebenarnya tidak terlalu beda jauh dengan cara mengkonfigurasi Standard Access List. Perintah yang digunakan ada penambahan informasi tentang paket yang diijinkan atau ditolak.

Router(config)#**access-list** [acl number] {permit|deny} {protocol . .} ?

[/source]

[wild-card source net/host add] [destination net/host add] [wildcard dest net/host add] ?

// gunakan ‘?’ untuk melihat opsi selanjutnya

Contohnya:

Router\_A(config)#access-list 100 permit tcp    172.16.0.0     0.0.255.255   192.168.100.3    0.0.0.0   eq   telnet

Pada contoh perintah diatas, kita mengijinkan (permit) **paket telnet** dari semua host yang ada di jaringan 172.16.0.0 ke host 192.168.100.3. Angka [100] setelah perintah [access-list] merupakan pengenal bagi Extended Access List. Cara menerapkan Access List tersebut ke interface router juga tidak berbeda dengan penerapan Standard Access List.  Cara menerapkan Access List tersebut ke interface router juga tidak berbeda dengan penerapan Standard Access List.

Router\_A(config)#int f0/0

Router\_A(config)#ip access-group 100 {out|in}

**Kesimpulan**

Berdasarkan simulasi standar dan extended ACL tersebut, setidaknya kita bisa menarik kesimpulan sederhana kawan. Pada standard ACL hanya menggunakan alamat source IP address dalam paket IP sebagai kondisi yang di test, sehingga ACL tidak dapat membedakan tipe dari traffic IP seperti WWW, UDP, dan telnet. Sedangkan pada Extended ACL, selain bisa mengevaluasi source address dan destination address extended ACL juga dapat mengevaluasi header layer 3 dan 4 pada paket IP.  Nah, berikut adalah tugas besar dari ACL, baik jenis standar maupun extended, diantaranya:

* Membatasi lalulintas jaringan dan menambah performa jaringan. Sebagai contoh, ACL yang membatasi lalulintas video dapat dengan baik mengurangi beban jaringan dan menambah performa jaringan.
* Menyediakan kontrol aliran lalulintas. ACL dapat membatasi pengiriman update routing. Jika update tidak diperlukan disebabkan kondisi-kondisi jaringan, akanmenghemat bandwidth.
* Menyediakan sebuah level dasar keamanan untuk akses jaringan. ACL dapat mengijinkan satu host untuk mengakses sebuah bagian dari jaringan dan mencegah host lain untuk mengakses area yang sama. Sebagai contoh, Host A diperbolehkan untuk mengakses jaringan Sumberdaya Manusia dan Host B dicegah untuk mengaksesnya.
* Memutuskan jenis lalulintas yang dilewatkan atau diblok pada interface-interface router. ACL dapat mengijinkan pe-rute-an lalulintas e-mail, tapi mem-blok semua lalulintas telnet.
* Mengontrol wilayah sebuah client mana yang dapat mengakses pada sebuah jaringan
* Menyaring host-host untuk diperbolehkan atau ditolak mengakses ke sebuah segment jaringan. ACL dapat digunakan untuk memperbolehkan atau menolak seorang user untuk mengakses jenis-jenis file seperti FTP atau HTTP.

Terakhir sebagai penutup, jika ACL tidak dikonfigurasi pada router, semua paket-paket yang melewati router akan diperbolehkan untuk mengakses keseluruhan jaringan. Sudah tentu hal ini membahayakan jaringan internal apabila terkoneksi dengan jaringan internet.

### Simulasi ACL Standard di Cisco Packet Tracer



Hai Teman ?? Kali ini saya akan memberikan penjelasan tentang cara Konfigurasi ACL Standard pada Cisco Packet Tracer.Pada kesempatan sebelumnya saya juga telah melakukan konfigurasi Port Security pada Switch yang dapat dilihat disini. Ngomong-omong apa sih ACL Standart itu? Yuk simak penjelasan lebih lengkapnya pada artikel dibawah ini.

### A. Pengertian

     Access Control List (ACL) merupakan daftar kondisi yang dirancang sedemikian rupa oleh administrator jaringan untuk mengontrol akses-akses ke dan dari interface-interface router, mencegah trafik-trafik tertentu untuk masuk ke jaringan atau sebaliknya, mencegah trafik-trafik untuk keluar dari jaringan. Access list dapat mengizinkan host-host tertentu mengakses bagian tertentu dalam jaringan, dan mencegah host lainnya mengakses area yang sama.

   Atau lebih mudahnya ACL (Access Control List) adalah  firewall pada Router/switch Cisco untuk mem-filter (men-deny atau meng-allow) packet yang masuk ataupun keluar.

**Karakterisik ACL secara umum**

* Menentukan tipe traffic yang akan di control

* Menentukan karakteristrik traffic

* Mengidentifikasi traffic dengan permit atau deny

* Dapat men-deny traffic spesifik atau secara keseluruhan

* Terdapat implisit deny any pada akhir baris access list secara default

* Masing-masing baris hanya untuk satu protokol spesifik

* masing protocol, satu incoming traffic dan satu outgoing trafficMasing-masing interface router maksimal hanya punya dua access list untuk masing-

* Ketika access list di assign untuk interface, tentukan apakah untuk incoming atau outgoing

* Access list sifatnya global di router, tapi filter traffic hanya berlaku di interface yang di assign access list

* Masing-masing access list dapat di assign ke beberapa interface

* Akan tetapi tiap interface hanya boleh satu incoming dan satu outgoing

* Access list dapat digunakan untuk nge-log traffic yang match dengan access list statement

* Access list yang di applied ke inbound traffic dilakukan sebelum routing decision
* Access list yang di applied ke outbound traffic dilakukan setelah routing decision

* Ketikkan rule access list secara berurutan, dengan statement paling restrictive berada di atas

**ACL Standard**

1. Nomor ACL : 1- 99
2. Digunakan untuk filter source IP address
3. Permit / Deny semua protocol suite TCP/IP
4. Tips : assign pada router yang terdekat dengan destination (close to the destination Router)

**Konfigurasi ACL**

     Untuk melakukan setting ACL di router, pertama setting rule ACL terlebih dahulu di mode global router, kemudian langkah kedua assign rule ACL tersebut di interface.

Router(config)# access-list 1 permit/deny source hostname/ip/network

Router(config)# access-list 1 permit/deny any
Router(config)# interface fa0/0
Router(config)# ip access-group 1 in/out

**Untuk menyatakan match sebuah host bisa menggunakan 2 cara :**

* Dengan wildcard mask “0.0.0.0”, misal 192.168.1.1 0.0.0.0
* Dengan keyword “host”, misal host 192.168.1.1

**Untuk menyatakan match semua host bisa menggunakan 2 cara :**

* Dengan wildcard mask “255.255.255.255”, misal 0.0.0.0 255.255.255.255
* Dengan keyword “any”, misal any source atau destination

### B. Latar Belakang

### C. Alat dan Bahan

- Seperangkat PC / Laptop

- Cisco Packet Tracer

### D. Maksud dan Tujuan

### E. Tahap Pelaksanaan

1. Pertama - tama buat dulu topologinya seperti dibawah ini



2. Selanjutnya buat Rule/Aturan dari ACL Standard yang akan dibuat.Misal seperti dibawah ini.

***1. Deny host 192.168.1.1 berkomunikasi dengan network 192.168.2.0
2. Deny network 1.1.1.1 berkomunikasi dengan network 192.168.2.0
3. Permit semua trafik lainnya***

3. Kemudian atur IP address dari kedua PC pada Topologi tsb.

 PC 0



 PC 1



4. Selanjutnya atur juga IP dari setiap interface pada setiap Router di Topologi diatas.
**Router 1**

Router>en

Router#conf t

Router(config)#int lo 0

Router(config-if)#ip add 1.1.1.1 255.255.255.255

Router(config-if)#ex

Router(config)#int fa0/0

Router(config-if)#ip add 192.168.1.254 255.255.255.0

Router(config-if)#no sh

Router(config-if)#ex

Router(config)#int fa0/1

Router(config-if)#ip add 12.12.12.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#ex

Router(config)#

**Router 2**

Router>en

Router#conf t

Router(config)#int lo 0

Router(config-if)#ip add 2.2.2.2 255.255.255.255

Router(config-if)#ex

Router(config)#int fa0/0

Router(config-if)#ip add 192.168.2.254 255.255.255.0

Router(config-if)#no sh

Router(config-if)#ex

Router(config)#int fa0/1

Router(config-if)#ip add 12.12.12.2 255.255.255.0

Router(config-if)#no sh

Router(config-if)#ex

Router(config)#

 5. Kemudian lakukan Routing OSPF area 0 pada topologi diatas.berikut konfigurasinya :

**Router 1**

Router(config)#router ospf 10

Router(config-router)#network 1.1.1.1 0.0.0.0 area 0

Router(config-router)#network 192.168.1.0 0.0.0.255 area 0

Router(config-router)#network 12.12.12.0 0.0.0.255 area 0

Router(config-router)#ex

Router(config)#

**Router 2**

Router(config)#router ospf 10

Router(config-router)#network 2.2.2.2 0.0.0.0 area 0

Router(config-router)#network 192.168.2.0 0.0.0.255 area 0

Router(config-router)#network 12.12.12.0 0.0.0.255 area 0

Router(config-router)#ex

Router(config)#

6. Selanjutnya coba tes koneksi dengan melakukan ping dari PC 0 (192.168.1.1) ke PC 1 (192.168.2.1)



7. Kemudian kita coba setting ACL standartnya di Router 2, mengapa kok di Router 2 ?? karena agar rule yang kita buat tadi bisa berjalan normal,maka kita taruh di router yang terdekat dgn tujuan.Ingat ya prinsip ACL Standard yaitu **"assign pada router yang terdekat dengan destination"**

Router(config)#access-list 1 deny 192.168.1.1 0.0.0.0

Router(config)#access-list 1 deny 1.1.1.1 0.0.0.0

Router(config)#access-list 1 permit any

8. Selanjutnya tempatkan ACL tersebut di interface outgoing menuju network 192.168.2.0, agar ACL bisa bekerja efektif.
**Apply ACL Interface di fa0/0 Router 2**

Router(config)#int fa0/0

Router(config-if)#ip access-group 1 out

9. Lalu coba tampilkan Acces List Standard yang sudah dibuat di Router 2
ketikkan "show access-list"



**Pengujian**
10. Kemudian coba test lagi, lakukan ping lagi dari PC0 ke PC1.Dan hasilnya tidak berhasil,hal ini menandakan konfigurasi ACL Standard pada Rule nomor 1 sudah berhasil.Host 192.168.1.1 tidak diperbolehkan untuk berkomunikasi dengan network 192.168.2.1



 12. Selanjutnya kita akan coba test ping ke 192.168.2.1 menggunakan IP selain 192.168.1.1.Ubah IP Address PC 0 menjadi 192.168.1.3



13. Coba lakukan ping ke PC1 dan berhasil. Rule ACL nomor 1 sudah benar-benar berhasil mem-filter host 192.168.1.1 saat mengakses network 192.168.2.1.



14. Test ping dari Loopback 0 (1.1.1.1) R1 ke PC1 (192.168.2.1)

Router>en

Router#ping

Protocol [ip]:*enter*

Target IP address: 192.168.2.1

Repeat count [5]: *enter*

Datagram size [100]: *enter*

Timeout in seconds [2]: *enter*

Extended commands [n]: y

Source address or interface: loopback0

Type of service [0]: *enter*

Set DF bit in IP header? [no]: *enter*

Validate reply data? [no]: *enter*

Data pattern [0xABCD]: *enter*

Loose, Strict, Record, Timestamp, Verbose[none]: *enter*

Sweep range of sizes [n]: *enter*

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

**UUUUU**

**Success rate is 0 percent (0/5)**

Router#



Tes Ping dari Loopback1 ke Laptop2 hasilnya 0 percent dan ditampilkan kode U (unreachable).Berarti rule ACL baris ke-2 sudah berhasil.

15. Untuk verifikasi rule ACL baris ke-3 yaitu permit semua trafik lainnya, kita akan mencoba menambahkan Host baru dengan IP selain 192.168.1.1 seperti gambar dibawah



Beri IP Laptop : 192.168.1.2/24



16. Lalu coba test ping ke 192.168.2.1 dan hasilnya berhasil,Rule nomor 3 sudah sukses.



### F. Referensi

Ebook CCNA Lab Guide Nixtrain\_1st Edition\_Full Version.pdf

<http://myconfigure.blogspot.co.id/2014/03/konfigurasi-access-control-list-di.html>

### G. Hasil dan Kesimpulan