**LAPORAN PRAKTIKUM**

**INFRASTRUKTUR SISTEM INFORMASI**

(Access Control List)



Oleh :

|  |  |
| --- | --- |
| Nama | : Agung Sapto Margono Dh |
| NPM | : 15753003 |
| Program Studi | : Manajemen Informatika |

**JURUSAN EKONOMI DAN BISNIS**

**POLITEKNIK NEGERI LAMPUNG**

**BANDAR LAMPUNG**

**2017**

**BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang**

Dalam mempelajari ilmu jaringan dan komunikasi data, dibutuhkan kemampuan anasisis yang sangat baik. ACL adalah sebuah fitur yang mempunyai cara kerja seperti firewall sederhana. Dengan menggunakan ACL, kita dapat membatasi packet-packet apa saja yang dapat masuk dan keluar. Disini penulis menjelaskan bagaimana cara menyelesaikan studi kasus yang berhubungan dengan ACL. Dan dengan tulisan ini penulis berharap para pembaca dapat memahami bagaimana cara kerja dan cara menyelesaikan masalah yang ada.

* 1. **Rumusan Masalah**
* Apa itu ACL ?
* Bagaimana cara menyelesaikan studi kasus yang diberikan ?
  1. **Tujuan**
* Mahasiswa memahami apa itu ACL.
* Mahasiswa dapat menyelesaikan studi kasus yang diberikan.

**BAB II**

**LANDASAN TEORI**

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

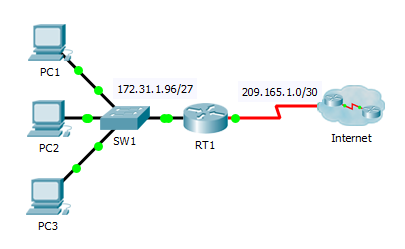
ACL (Access Control List) merupakan metode selektivitas terhadap packet data yang akan dikirimkan pada alamat yang dituju. Secara sederhana ACL dapat kita ilustrasikan seperti halnya sebuah standard keamanan. Hanya packet yang memiliki kriteria yang sesuai dengan aturan yang diperbolehkan melewati gerbang 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.

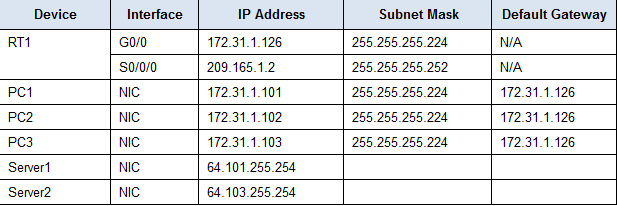
**BAB III**

**PEMBAHASAN**

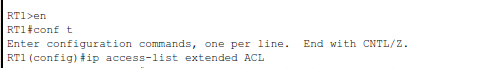
**3.1 Configure Standard IPv4 ACLs**

1. Topologi jaringan dan tabel IP Address yang akan di-config.

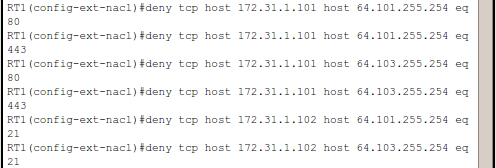




2. Buat access list extended dengan nama ACL



3. Block protokol tcp pada host 172.31.1.101 yang mengarah ke host 64.101.255.254 dengan port 80 dan 443, block protokol tcp pada host 172.31.1.101 yang mengarah ke host 64.103.255.254 dengan port 80 dan 443, block protokol tcp pada host 172.31.1.102 yang mengarah ke host 64.101.255.254 dan 64.103.255.254 host dengan 21



3. Block protokol icmp pada host 172.31.1.103 yang mengarah ke host 64.101.255.254 dan host 64.103.255.254

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\3.png

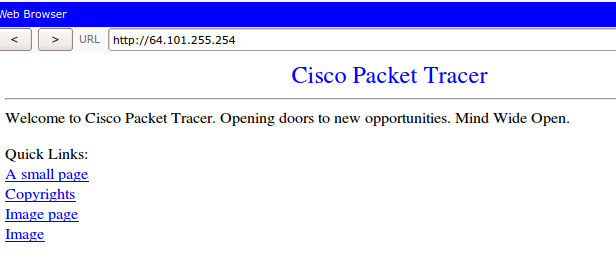
4. Perbolehkan semua paket agar semua paket yang melintas kecuali paket yang ditolak seperti rule diatas

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\4.png

5. Masuk ke interface g0/0 lalu daftarkan access group dengan access list ACL untuk paket data masuk

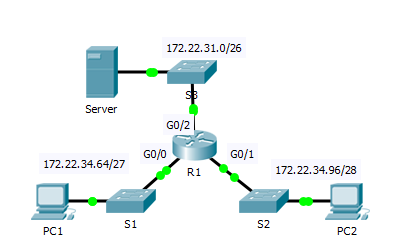
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\5.png

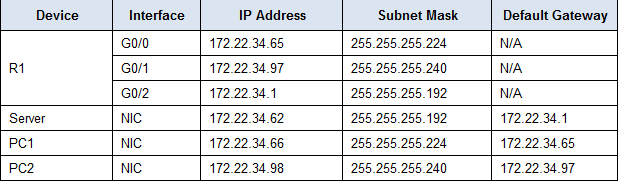
6. Test web browser dari PC 2 ke alamat http://64.101.255.254



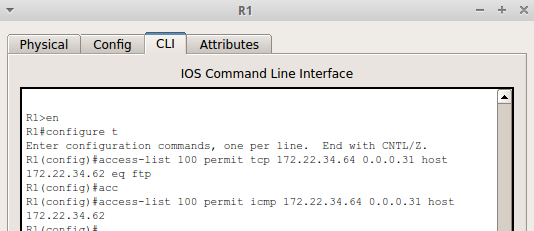
**3.2 Configuring Extended ACLs Scenario 1**

1. Topologi jaringan dan tabel IP Address yang akan di-config.

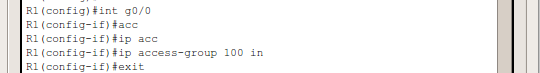




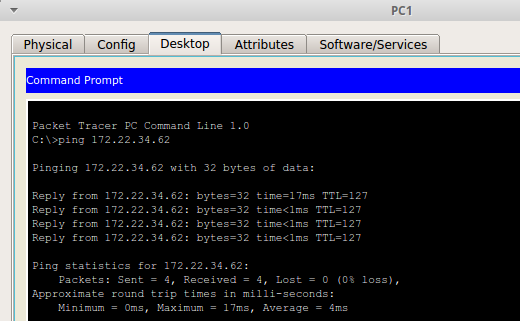
2. Pada access list dengan id 100, izinkan packet tcp dari host 172.22.34.64 dengan wild card 0.0.0.31 ke host 172.22.34.62 dengan port ftp dan packet icmp dari host 172.22.34.64 dengan wild card 0.0.0.31 ke host 172.22.34.62



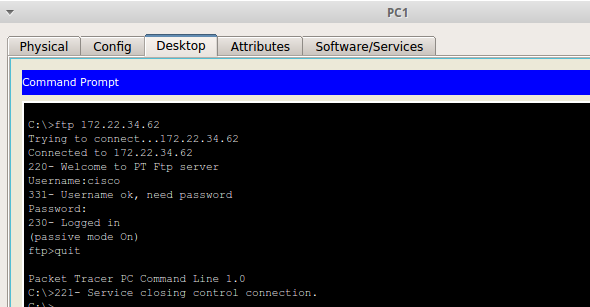
3. Masuk ke interface g0/0 dan daftarkan access group dengan access list yang ber id 100 untuk packet data masuk



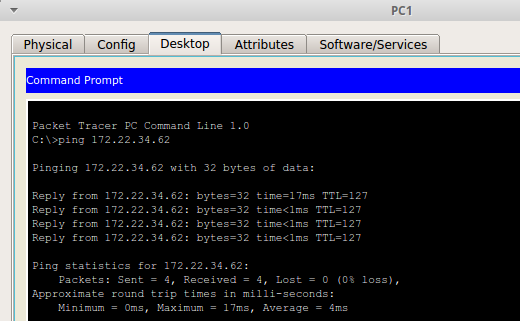
4. Test ping dari PC1 ke 172.22.34.62



5. Test ftp dari PC1 ke 172.22.34.

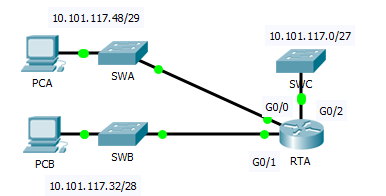


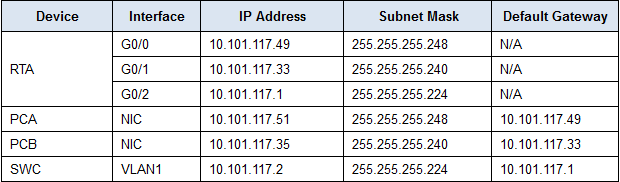
6. Test ping dari PC1 ke 172.22.34.62



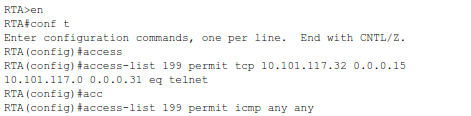
**3.3 Configuring Extended ACLs Scenario 2**

1. Topologi jaringan dan tabel IP Address yang akan di-config.

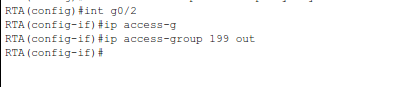




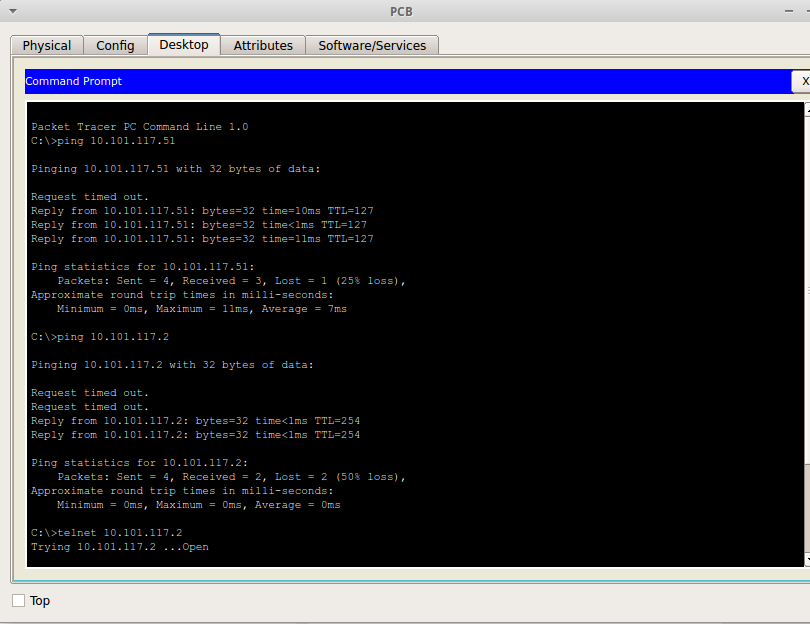
2. Buat access list dengan id 199, izinkan packet tcp dari host 10.101.117.32 dengan wild card 0.0.0.15 ke host 10.101.117.0 dengan wild card 0.0.0.31 dengan port telnet dan izinkan semua packet icmp.



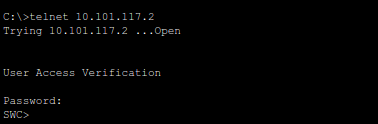
3. Masuk ke interface g0/2 lalu daftarkan access group dengan access list dengan id 199 untuk paket data keluar



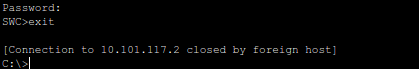
4. Test ping dari PCB ke host 10.101.117.51 dan ke host 10.101.117.2.



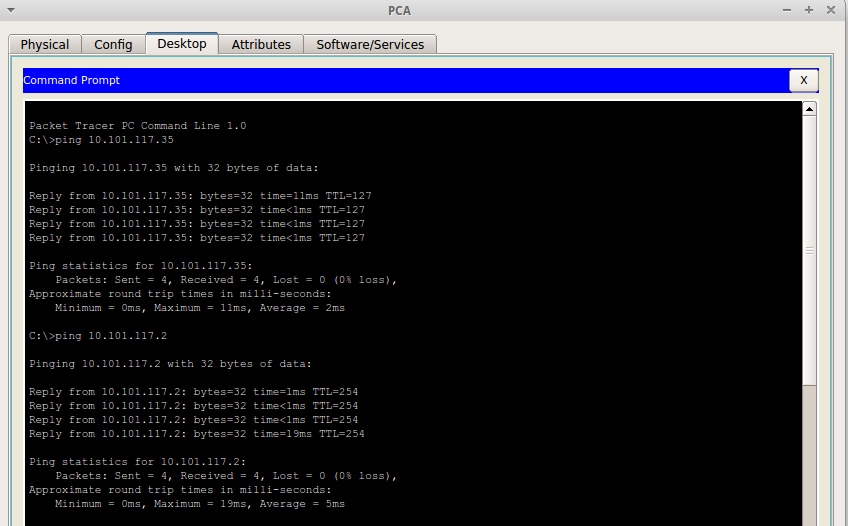
5. Test telnet dari PCB ke host 10.101.117.2



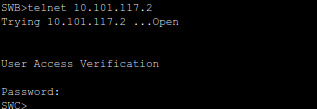
6. Login telnet dari PCB ke host 10.101.117.2



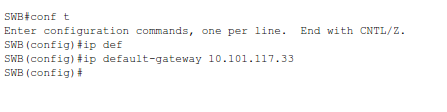
7. Test ping dari PCA ke host 10.101.117.35 dan ke host 10.101.117.2



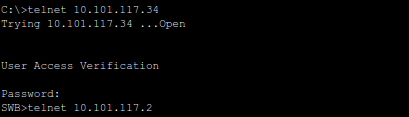
8. Test telnet dari PCA ke host 10.101.117.2



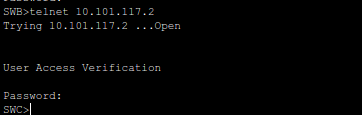
9. Atur default gateway pada switch SWB dengan host 10.101.117.33



10. Test telnet dari PCA ke host 10.101.117.34

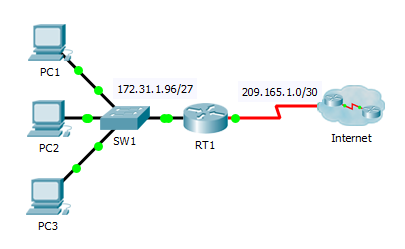


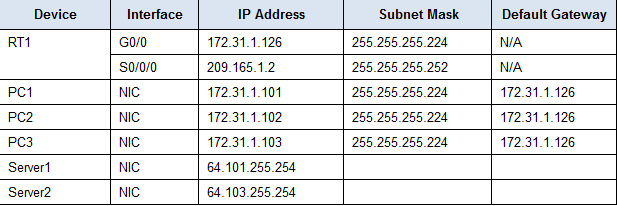
11. Test telnet dari PCA ke host 10.101.117.2



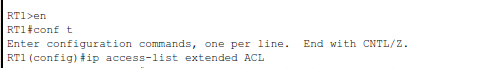
**3.4 Configuring Extended ACLs Scenario 3**

1. Topologi jaringan dan tabel IP Address yang akan di-config.

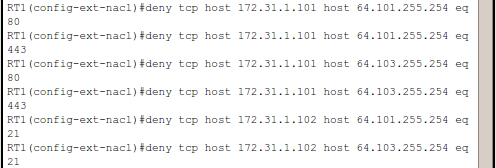




2. Buat access list extended dengan nama ACL



3. Block protokol tcp pada host 172.31.1.101 yang mengarah ke host 64.101.255.254 dengan port 80 dan 443, block protokol tcp pada host 172.31.1.101 yang mengarah ke host 64.103.255.254 dengan port 80 dan 443, block protokol tcp pada host 172.31.1.102 yang mengarah ke host 64.101.255.254 dan 64.103.255.254 host dengan 21



4. Block protokol icmp pada host 172.31.1.103 yang mengarah ke host 64.101.255.254 dan host 64.103.255.254

3

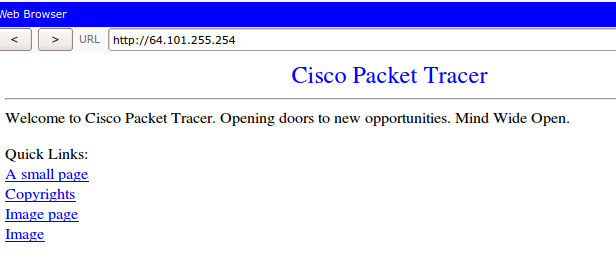
5. Perbolehkan semua paket agar semua paket yang melintas kecuali paket yang ditolak seperti rule diatas

4

6. Masuk ke interface g0/0 lalu daftarkan access group dengan access list ACL untuk paket data masuk

5

7. Test web browser dari PC 2 ke alamat http://64.101.255.254



**BAB IV**

**PENUTUP**

1. **Kesimpulan**

ACL adalah salah satu kemampuan yang wajib dimiliki oleh mahasiswa yang menekuni dibidang jaringan. Bisa dikatakan bahwa ACL adalah firewall dengan versi sederhana. Dengan mengaplikasikan ACL dalam sebuah topologi jaringan, maka jaringan akan lebih aman karena tidak sembarang packet dapat berlalu lintas didalam topologi jaringan tersebut.