**MODUL V**

**ACCESS CONTROL LISTS (ACL)**

1. **TUJUAN**
2. Mahasiswa mampu memahami konsep *access control lists*.
3. Mahasiswa mampu melakukan konfigurasi *standard access list* dan *extended access list* menggunakan Cisco *Router*.
4. Mahasiswa mampu menerapkan *access list* pada suatu jaringan.
5. **DASAR TEORI**
   * 1. *Access Control List*

*Access control list* merupakan metode daftar akses yang digunakan *cisco* untuk mengatur keluar masuknya *traffic* ke dalam maupun ke luar *router.*[1] ACL biasa disebut “paket *filtering*”. ACL diimplementasikan di *router*. ACL dapat mengendalikan keluar masuknya paket berdasarkan IP *address* asal atau tujuan.

*Access list* bekerja menyaring lalu-lintas data suatu *network* dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan pada alat penghubung (*interface*) *router*. *Router* menguji semua paket data untuk menentukan apakah paket tersebut diizinkan untuk lewat atau tidak berdasarkan kriteria yang ditentukan di dalam *access list*.

Contoh penggunaan ACL:

Dengan menggunakan *access list* maka dapat membuat keputusan yang sangat spesifik tentang peraturan pola lalu lintas, misalnya:

1. Hanya memperbolehkan *host* tertentu mengakses sumber daya WWW, sementara *host* yang lainnya ditolak.
2. Mengontrol *network* mana yang akan atau tidak ditanyakan oleh *protocol dynamic routing*.
3. Mengkategorikan paket atau QoS[8].

*Acces Control List* memiliki beberapa fungsi yang diantaranya :

* + - * 1. Membatasi jaringan dan meningkatkan untuk kerja jaringan, misal ACL memblok *traffic* video sehingga dapat menurunkan beban jaringan dan meningkatkan untuk kerja jaringan.
        2. ACL mampu memblok *update routing*, jika *update* tidak dibutuhkan karena kondisi jaringan maka *bandwidth* dapat dihemat.
        3. Mampu memberikan keamanan untuk akses jaringan.
        4. Mengontrol daerah-daerah dimana *client* dapat mengakses jaringan.
        5. Mengatur aliran *traffic*.
        6. Mampu memberikan dasar keamanan untuk akses ke jaringan. Misalnya, *host* A tidak diijinkan akses ke jaringan HRD dan *host* B diijinkan.
        7. Memutuskan jenis *traffic* mana yang dilewatkan atau diblok melalui *interface router*. Misalnya, *traffic email* dilayani, *trafiic* telnet diblok.
        8. Memilih *host-host* yang diijinkan atau diblok akses ke segmen jaringan. Misalnya, ACL mengijinkan atau memblok FTP atau HTTP.
    1. Macam-macam *Access Control List*

1. *Standard* ACL

*Standard* ACL hanya dapat digunakan untuk mengizinkan (*permit*) atau melarang (*deny*) *traffic* dari IP *address* tertentu. *Standard* ACL hanya menyeleksi *source* IP dari paket-paket yang datang. *Standard* ACL tidak dapat mem-*filter* IP *destination* dan *port* (*service*)[7]. Semua keputusan dibuat berdasarkan alamat IP sumber. Pada dasarnya *standard* ACL melewatkan atau menolak seluruh paket *protocol*.

Daftar akses *standard* (*standard access list*) mempergunakan alamat pengiriman paket dalam pembuatan daftar akses. Untuk membuat daftar akses *standard* dari *global configuration mode* adalah:

|  |
| --- |
| Router(config)#acccess-list <nomor daftar IP standard> <permit atau deny> <IP address> <wildcard masuk> |

Keterangan:

1. Nomor daftar akses IP *standard* adalah 1 sampai 99.
2. *Permit* atau *deny* adalah parameter untuk mengijinkan atau menolak.
3. IP *address* adalah alamat pengirim atau asal.
4. *Wildcard mask* adalah untuk menentukan jarak dari suatu *subnet*[8].
5. *Extended* ACL

*Extended* ACL digunakan untuk mengatur *traffic* berdasarkan *source* atau *destination* IP *address* dan *port*. Pada *extended* ACL dapat menentukan berbagai *protocol* seperti ICMP, TCP dan UDP. *Extended* ACL mampu membuat keputusan lebih spesifik ketika mengontrol lalu lintas. *Extended* ACL juga mampu menangani berbagai kondisi *firewall*. Secara umum pada *extended* ACL dapat membuat 99 buah *extended* IP ACL yang diberi nomor 100 sampai dengan 199[8].

*Extended* ACL bisa mengevaluasi 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.

Daftar akses *extended* (*extended access list*) adalah daftar akses lanjutan yang memiliki lebih banyak parameter yang dapat diukur, antara lain alamat (*source address*), alamat penerima (*destination address*), nomor *port* dan *protocol* seperti pada contoh berikut:

|  |
| --- |
| Router(config)#access-list <nomor daftar akses IP extended> <permit atau deny> <protocol> <source address> <wildcard mask> <destination address> <wildcard mask> <operator> <information port> |

Keterangan:

* + - * 1. Nomor daftar akses IP *extended* adalah 100 sampai 199.
        2. Permit atau *deny* adalah parameter untuk mengujinkan atau menolak.
        3. Protocoladalah seperti TCP, UDP, ICMP dan lain-lain.
        4. Source *address* adalah alamat pengirim atau asal.
        5. Destination *address* adalah alamat penerima atau yang dituju.
        6. Wildcard *mask* adalah untuk menentukan jarak dari suatu *subnet*.
        7. Operator adalah seperti eq (*equal*), lt (*langer than*), gt (*greater than*).
        8. Informasi *port* beripa nomor *port*, DNS, FTP, WWW, *telnet*, smtp dan lain-lain.[2]
    1. Macam-macam Lalu Lintas Pada ACL
       - 1. *Inbound*

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

* + - * 1. *Outbound*

Ketika sebuah ACL diterapkan pada paket *outbound* pada sebuah *interface router*, paket tersebut di-*route* ke *outbound interface* dan diproses melalui ACL[1].

* + 1. Cara Kerja *Access Control List*

1. *Access Control Lists* membandingkan atau mencocokkan setiap paket yang diterima atau ditolak dengan ukuran atau daftar akses yang diterapkan pada *router* tersebut.
2. *Access Control Lists* mengizinkan atau menolak ke segmen jaringan dan dari segmen berdasarkan pada:
3. Alamat sumber
4. Alamat tujuan
5. Tipe *protocol*
6. Nomor *port* dari paket[7].
   * 1. Cara Membuat *Access Control List*
        + 1. Masuk ke mode *global* *config* kemudian memberikan perintah *acces list* dan diikuti dengan parameter-parameter.
          2. Menentukan ACL ke *interface* yang ditentukan.

Langkah-langkah dalam membuat ACL pada *router* sebagai berikut :

* + - * 1. Menghubungkan *peripheral* sesuai dengan topologi
        2. Melakukan *setting* *interface* pada masing-masing *router*.
        3. Melakukan *setting* IP *addres* pada masing-masing PC.
        4. Membuat tabel *routing* pada setiap *router*.
        5. Melakukan *test* koneksi antar PC.
        6. Membuat *access* *list* dimana ditentukan ACL ke *interface* yang ditentukan[7].

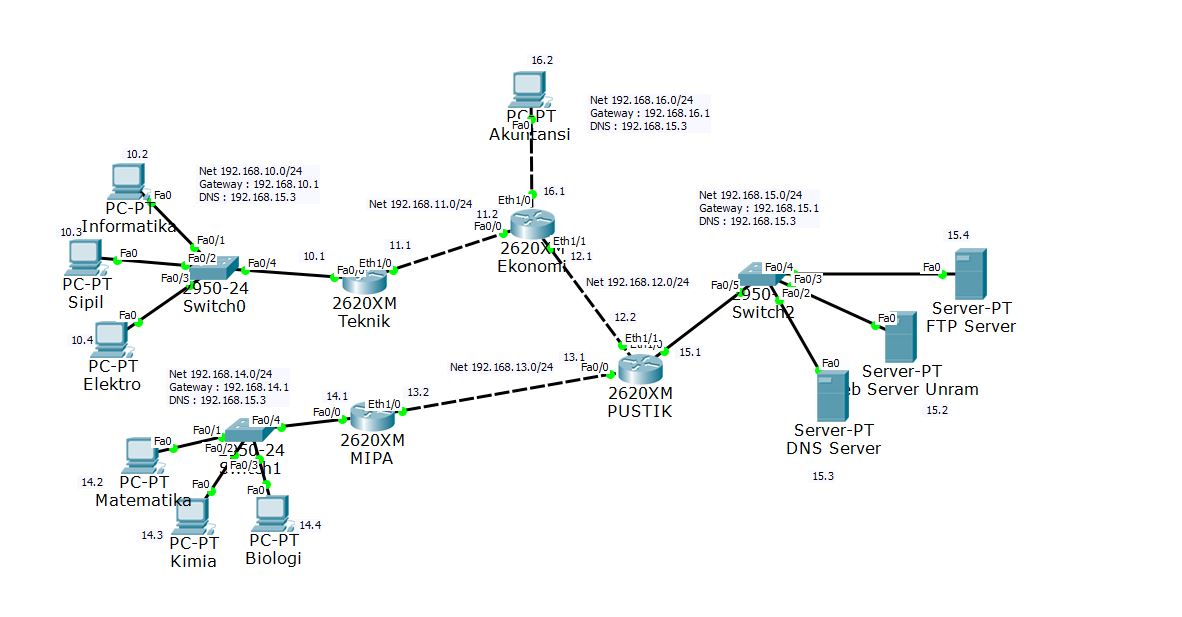
1. **ALAT DAN BAHAN**
2. *Laptop*/PC
3. *Software* Cisco Packet Tracer
4. **PERMASALAHAN**
   1. Melakukan konfigurasi *Access Control List* pada *Router* dengan aturan sebagai berikut :
      1. Sipil Tidak Boleh mengakses *Service* FTP *Server*
      2. Elektro Tidak Boleh mengakses *Service* FTP *Server*
      3. Sipil Tidak Boleh mengakses Kimia
      4. Elektro Tidak Boleh mengakses Kimia
      5. Sipil Tidak Boleh mengakses Biologi
      6. Elektro Tidak Boleh mengakses Biologi
      7. Sipil Tidak Boleh mengakses Matematika
      8. Elektro Tidak Boleh mengakses Matematika
      9. Sipil Tidak Boleh mengakses Akuntansi
      10. Elektro Tidak Boleh mengakses Akuntansi
      11. Sipil Boleh mengakses Web dan DNS *Server*
      12. Elektro Boleh mengakses Web dan DNS *Server*
      13. Informatika Boleh mengakses semua *Server*
      14. Informatika Boleh mengakses Matematika
      15. Informatika Boleh mengakses Akuntansi
      16. Matematika Tidak Boleh mengakses *Service* FTP *Server*
      17. Kimia Tidak Boleh mengakses *Service* FTP *Server*
      18. Biologi Tidak Boleh mengakses *Service* FTP *Server*
      19. Matematika Boleh mengakses Web dan DNS *Server* Unram
      20. Kimia Boleh mengakses Web dan DNS *Server* Unram
      21. Biologi Boleh mengakses Web dan DNS *Server* Unram
      22. LAN Ekonomi Tidak Boleh mengakses LAN Pustik
      23. LAN Ekonomi Boleh mengakses LAN MIPA
   2. Melakukan uji koneksi berdasarkan aturan yang telah diberikan, analisa dan *screenshot* hasilnya.
5. **LANGKAH PERCOBAAN**

Langkah 1:

Buka aplikasi Cisco Packet Tracer, gunakan kembali topologi jaringan yang telah Anda buat pada modul 4.

Tambahkan 1 buah *Switch* ke *Router*PUSTIK dan 3 buah *Server* seperti yang tampak pada **Gambar 5.1**. Tambahkan 1 buah PC pada *Router*Ekonomi. Lihat Langkah 2 untuk mengetahui cara menambah *port* pada *Router*.

Ubah label dan *hostname* pada masing-masing *Router*, PC, dan *Server*.

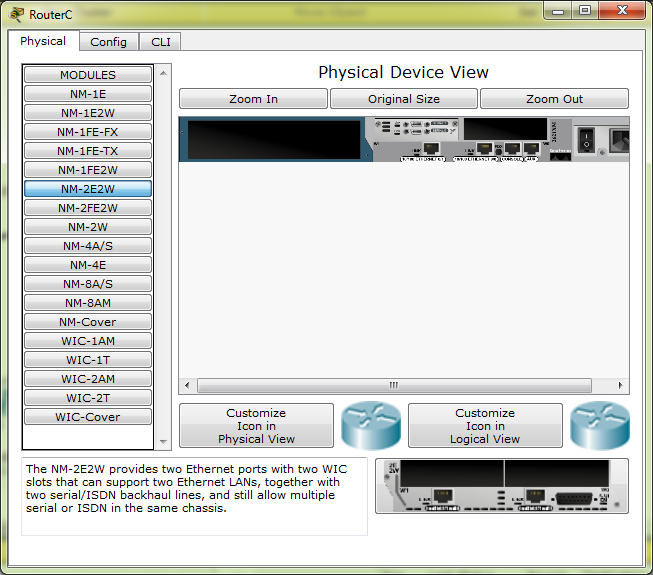
****

**Gambar 5.1** Topologi Jaringan

Langkah 2:

Untuk *Router*PUSTIK dan *Router*Ekonomi, tambahkan 1 buah *interface* *Ethernet* (NM-2E2W) seperti yang tampak pada **Gambar 5.2**, dengan cara sebagai berikut:

1. Klik *Router*, setelah itu akan muncul jendela baru.
2. Pilih *tab* *Physical*.
3. Matikan *Router* dengan menekan tombol *power*.
4. Pada bagian MODULES, pilih NM-2E2W lalu *drag* & *drop* *network* *module* tersebut ke slot yang kosong pada *Router*.
5. Setelah *network* *module* NM-2E2W terpasang, nyalakan *Router* dengan menekan tombol *power*.



Tombol Power

Network Module

NM-2E2W

Slot Kosong

**Gambar 5.2** Tampilan jendela pada perangkat *router*

Langkah 3:

1. Menghubungkan DNS *Server* – *Switch*, Web *Server* – *Switch*,dan FTP *Server* – *Switch* menggunakan kabel *Straight*-*Through* melalui *port* yang telah ditentukan seperti pada **Gambar 5.1**.
2. Menghubungkan Switch – *Router*PUSTIKmenggunakan kabel *Straight*-*Through* melalui *port* Eth1/0 yang telah ditentukan pada **Gambar 5.1**.
3. Menghubungkan PC Akuntansi menggunakan kabel *Cross*-*Over* ke *Router*Ekonomi melalui *port* Eth1/0 seperti pada **Gambar 5.1**.

Langkah 4:

1. Lakukan tambahan konfigurasi IP *Address* dan *Netmask* pada *Router*PUSTIK dan *Router*Ekonomi.

**Router PUSTIK**

RouterPUSTIK(config)#interface Eth1/0

RouterPUSTIK(config-if)#ip address 192.168.15.1 255.255.255.0

RouterPUSTIK(config-if)#no shutdown

RouterPUSTIK(config-if)#exit

**Router Ekonomi**

RouterEkonomi(config)#interface Eth1/0

RouterEkonomi(config-if)#ip address 192.168.16.1 255.255.255.0

RouterEkonomi(config-if)#no shutdown

RouterEkonomi(config-if)#exit

1. Jika menggunakan *Static* *Routing*, tambahkan *rute* untuk *Router* yang belum memiliki jalur menuju *network* 192.168.15.0/24 dan *network* 192.168.16.0/24.

**Router Teknik**

RouterTeknik(config)# ip route 192.168.15.0 255.255.255.0 192.168.11.2

RouterTeknik(config)# ip route 192.168.16.0 255.255.255.0 192.168.11.2

**Router Ekonomi**

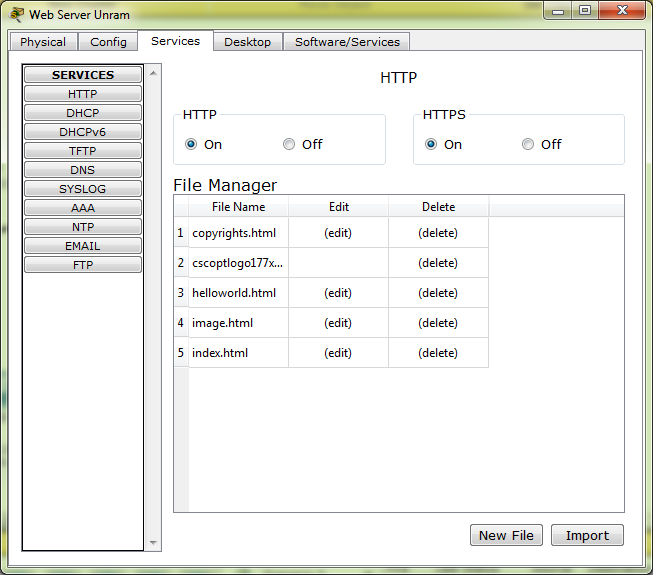
RouterEkonomi(config)# ip route 192.168.15.0 255.255.255.0 192.168.12.2

**Router MIPA**

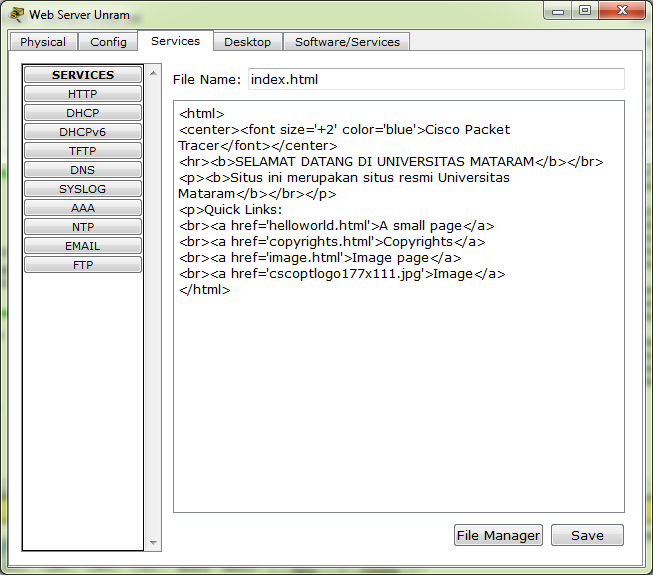
RouterMIPA(config)#ip route 192.168.15.0 255.255.255.0 192.168.13.1

RouterMIPA(config)#ip route 192.168.16.0 255.255.255.0 192.168.13.1

1. Lakukan konfigurasi IP *Address*, *Gateway*, *DNS*, dan *Netmask* pada Web *Server*, FTP *Server*, DNS *Server*, dan PC Akuntansi.
2. Aktifkan *Services* HTTP dan HTTPS pada Web *Server*, pilih *On*, seperti yang terlihat pada **Gambar 5.3**. Pada File *Manager*, klik edit untuk file *index*, ubah isi halaman *index* seperti yang terlihat pada **Gambar 5.4**.

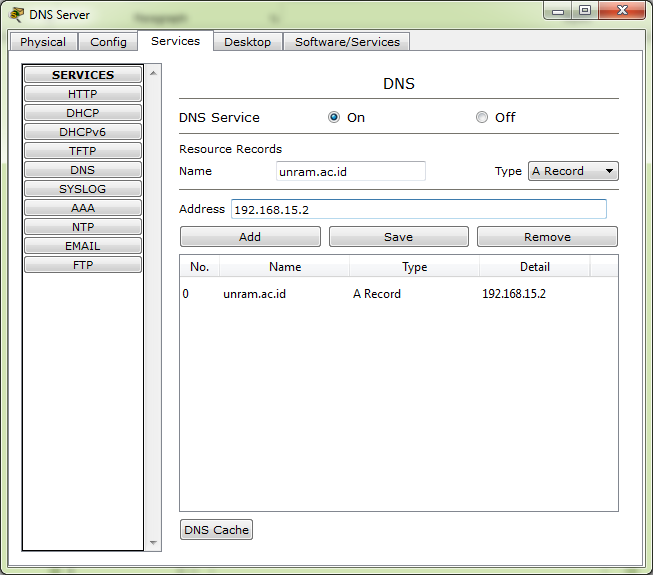


**Gambar 5.3** Jendela dialog HTTP pada web *server*



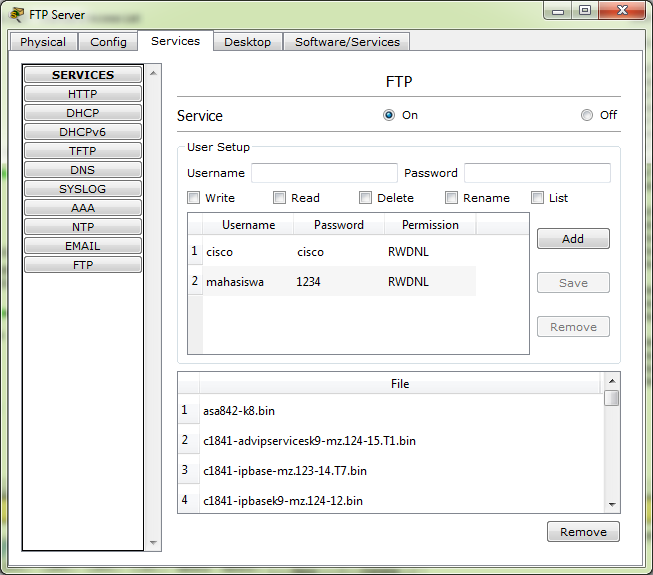
**Gambar 5.4** Jendela dialog *index* pada web *server*

1. Aktifkan *Services* DNS pada DNS *Server*, pilih On. Lalu isi *Name* dengan unram.ac.id, *Address* dengan 192.168.15.2, klik *add* seperti pada **Gambar 5.5**.



**Gambar 5.5** Jendela dialog *service* pada DNS *server*

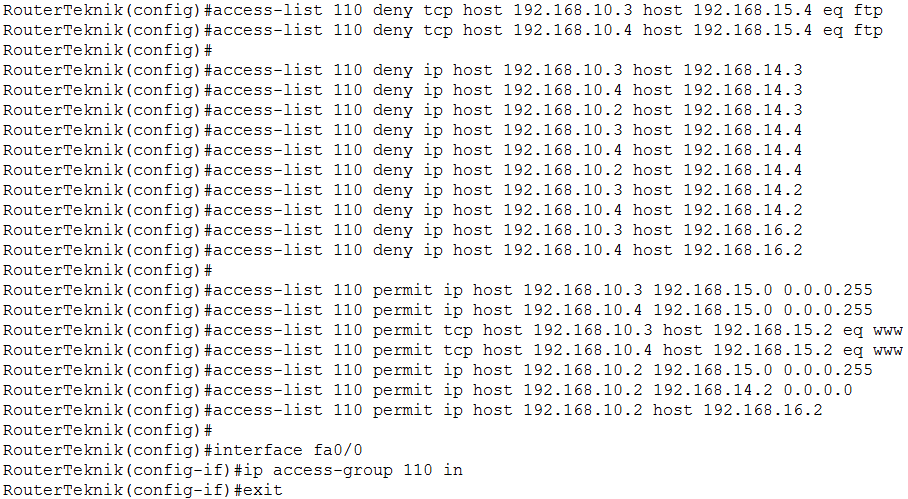
1. Aktifkan *Services* FTP pada FTP *Server*, pilih *On*. Pada *textbox* *username* isikan mahasiswa, *password* 1234, lalu centang *Write,* *Read,* *Delete,* *Rename,* *List*, kemudian klik tombol *Add* seperti yang tampak pada **Gambar 5.6**.



**Gambar 5.6** Jendela dialog *service* pada FTP *server*

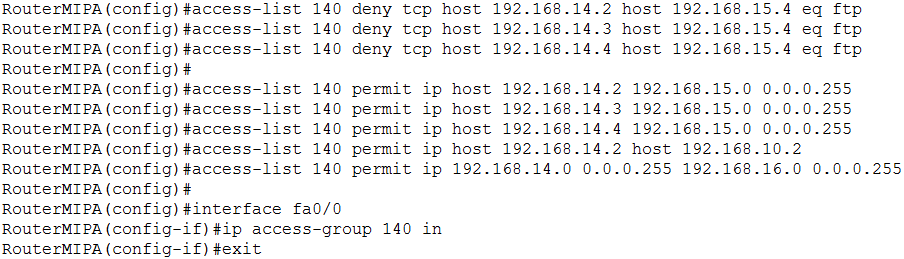
Langkah 5:

Membuat *Access Control List* (ACL)

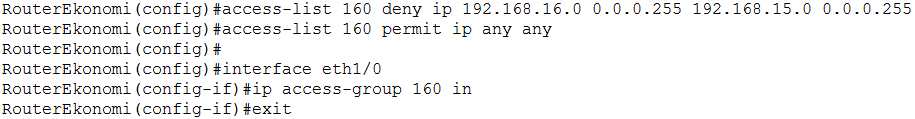
**Router Teknik**



**Router MIPA**

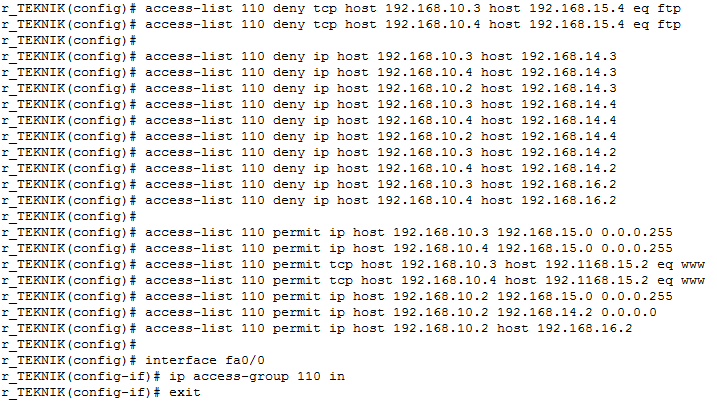




**Router Ekonomi**



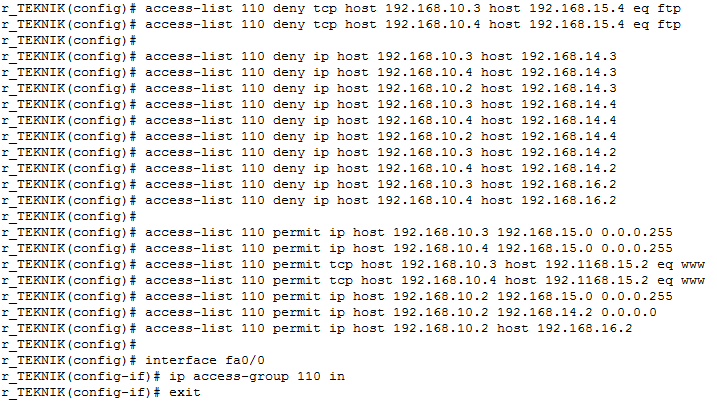
1. **HASIL DAN PEMBAHASAN**
   * + 1. Hasil Konfigurasi *Access* *Control* *List* pada *Router* dengan aturan-aturan yang telah diberikan.
2. *Router*Teknik



**Gambar 5.7** Konfigurasi ACL pada *Router* Teknik

*Script* “access-list 110 deny tcp host 192.168.10.3 host 192.168.15.4 eq ftp”, digunakan untuk memblokir akses *servise* PC sipil ke FTP *server* baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses *service* dari FTP *server* karena terdapat perintah “deny” pada *script.*

*Script* “access-list 110 deny tcp host 192.168.10.4 host 192.168.15.4 eq ftp”, digunakan untuk memblokir akses *servise* PC elektro ke FTP *server* baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses *service* dari FTP *server* karena terdapat perintah “deny” pada *script*.



**Gambar 5.8** Konfigurasi ACL pada *Router* Teknik

*Script* “access-list 110 deny ip host 192.168.10.3 host 192.168.14.3”, digunakan untuk memblokir akses *service* PC sipil ke PC kimia, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.4 host 192.168.14.3”, digunakan untuk memblokir akses PC elektro ke PC kimia, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.2 host 192.168.14.3”, digunakan untuk memblokir akses PC informatika ke PC kimia, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.3 host 192.168.14.4”, digunakan untuk memblokir akses PC sipil ke PC biologi, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.4 host 192.168.14.4”, digunakan untuk memblokir akses PC elektro ke PC biologi, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

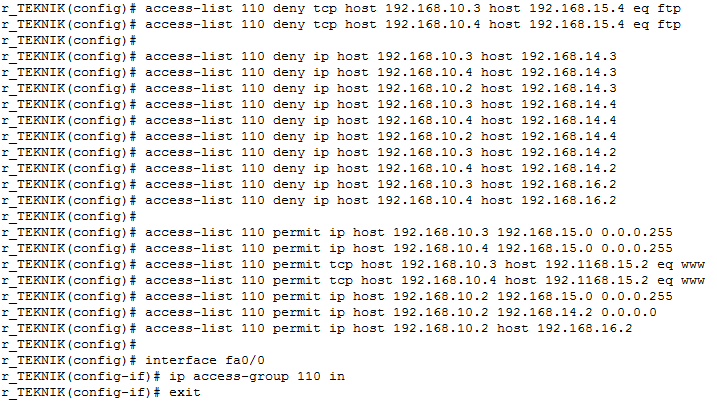
*Script* “access-list 110 deny ip host 192.168.10.2 host 192.168.14.4”, digunakan untuk memblokir akses PC informatika ke PC biologi, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.3 host 192.168.14.2”, digunakan untuk memblokir akses PC sipil ke PC matematika, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.4 host 192.168.14.2”, digunakan untuk memblokir akses PC elekro ke PC matematika, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

*Script* “access-list 110 deny ip host 192.168.10.3 host 192.168.16.2”, digunakan untuk memblokir akses PC sipil ke PC akuntansi, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.

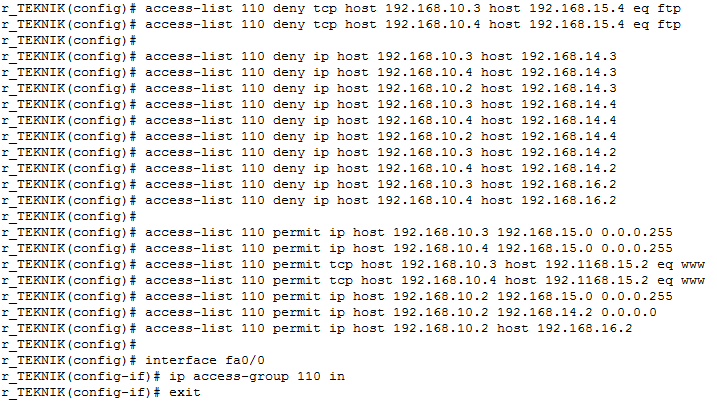
*Script* “access-list 110 deny ip host 192.168.10.4 host 192.168.16.2”, digunakan untuk memblokir akses PC elektro ke PC akuntansi, baik itu mengirim data sampai mengambil data atau tidak dibolehkan mengakses karena terdapat perintah “deny” pada *script*.



**Gambar 5.9** Konfigurasi ACL pada *Router* Teknik

*Script* “access-list 110 permit ip host 192.168.10.3 192.168.15.0 0.0.0.255”, digunakan untuk mengijinkan akses PC sipil ke *network* “192.168.15.0” karena terdapat perintah “permit” pada *script*.

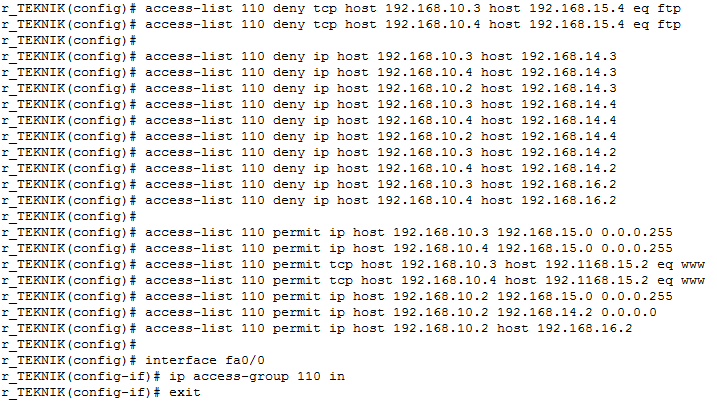
*Script* “access-list 110 permit ip host 192.168.10.4 192.168.15.0 0.0.0.255”, digunakan untuk mengijinkan akses PC elektro ke *network* “192.168.15.0” karena terdapat perintah “permit” pada *script*.



**Gambar 5.10** Konfigurasi ACL pada *Router* Teknik

*Script* “access-list 110 permit tcp host 192.168.10.3 host 192.168.15.2 eq www”, digunakan untuk mengijinkan akses PC sipil ke “192.168.15.2” yaitu ke *web server* karena terdapat perintah “permit” pada *script*.

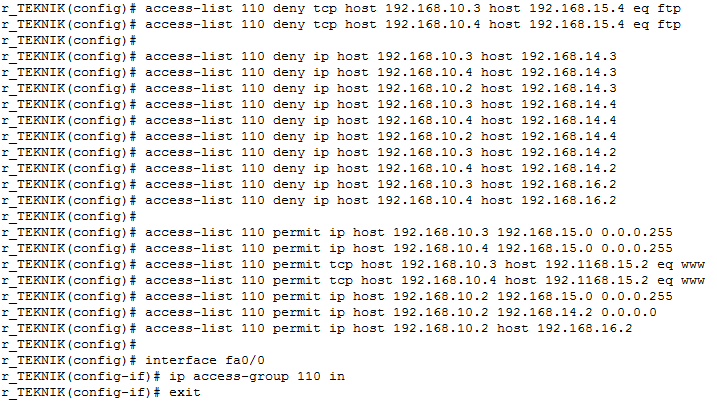
*Script* “access-list 110 permit tcp host 192.168.10.4 host 192.168.15.2 eq www”, digunakan untuk mengijinkan akses PC elektro ke “192.168.15.2” yaitu ke *web server* karena terdapat perintah “permit” pada *script*.



**Gambar 5.11** Konfigurasi ACL pada *Router* Teknik

*Script* “access-list 110 permit ip host 192.168.10.2 192.168.15.0 0.0.0.255”, digunakan untuk mengijinkan akses PC informatika ke *network* “192.168.15.0” karena terdapat perintah “permit” pada *script*.

*Script* “access-list 110 permit ip host 192.168.10.2 192.168.15.0 0.0.0.255”, digunakan untuk mengijinkan akses PC informatika ke *network* “192.168.15.0” karena terdapat perintah “permit” pada *script*.



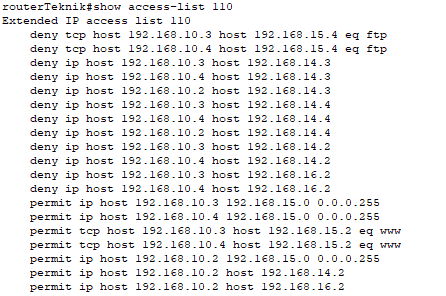
**Gambar 5.12** Konfigurasi ACL pada *Router* Teknik

“access-list 110 permit ip host 192.168.10.2 hot 192.168.16.2”, berarti bahwa PC “Informatika” diperbolehkan untuk mengakses“Akuntansi”.

Terakhir dilakukan *setting* *interface router* untuk menerapkan ACL. “fa0/0” dipilih sebagai tempat untuk menerapkan ACL karena konfigurasi ACL yang digunakan pada *router*Teknik adalah *extended* ACL. *Interface* yang digunakan oleh *extended* ACL adalah *interface* yang paling dekat dengan *source.*

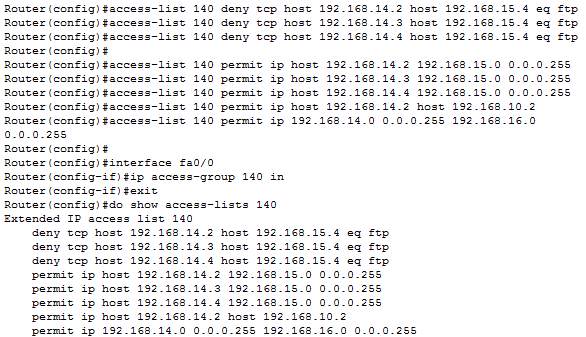
ACL yang sudah dikonfigurasi dapat dilihat statusnya pada *router* Teknik dengan menggunakan perintah “show access-list 110”. Balasan dari perintah tersebut dapat dilihat pada

Adapun hasil konfigurasi ACL yang telah dilakuakan pada *Router*Teknik adalah sebagai berikut:



**Gambar 5.13** Hasil konfigurasi ACL pada *Router* Teknik

1. *Router*MIPA

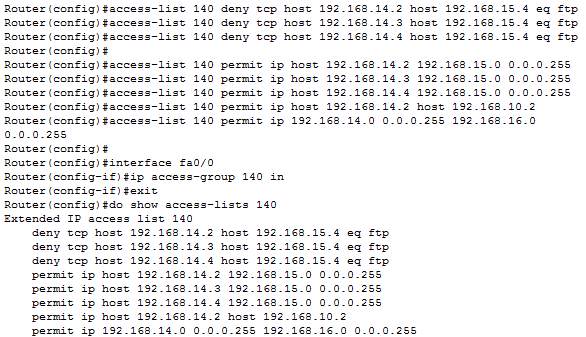


**Gambar 5.14** Hasil konfigurasi ACL pada *Router* MIPA

“access-list 140 deny tcp host 192.168.14.2 host 192.168.15.4 eq ftp”, berarti bahwa PC “Matematika” tidak diperbolehkan untuk mengakses *service* dari FTP *server* mulai dari mengirim data sampai mengambil data.

“access-list 140 deny tcp host 192.168.14.3 host 192.168.15.4 eq ftp”, berarti bahwa PC “Sipil” tidak diperbolehkan untuk mengakses *service* dari FTP *server* mulai dari mengirim data sampai mengambil data.

“access-list 140 deny tcp host 192.168.14.4 host 192.168.15.4 eq ftp”, berarti bahwa PC “Biologi” tidak diperbolehkan untuk mengakses *service* dari FTP *server* mulai dari mengirim data sampai mengambil data.

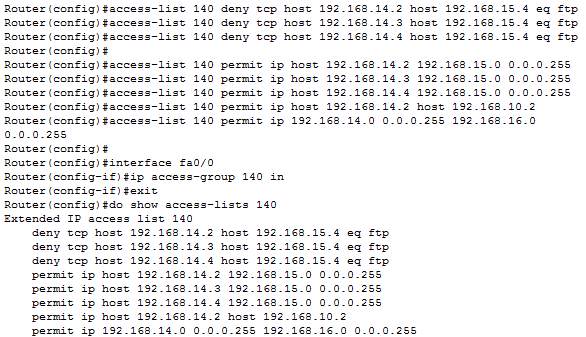


**Gambar 5.15** Hasil konfigurasi ACL pada *Router* MIPA

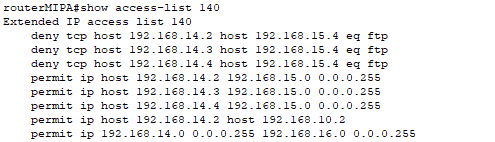
“access-list 140 permit ip host 192.168.14.2 192.168.15.0 0.0.0.255”, berarti bahwa PC “Matematika” diperbolehkan untuk mengakses *network* “192.168.15.0”.

“access-list 140 permit ip host 192.168.14.3 192.168.15.0 0.0.0.255”, berarti bahwa PC “Kimia” diperbolehkan untuk mengakses *network* “192.168.15.0”.

“access-list 140 permit ip host 192.168.14.4 192.168.15.0 0.0.0.255”, berarti bahwa PC “Biologi” diperbolehkan untuk mengakses *network* “192.168.15.0”.

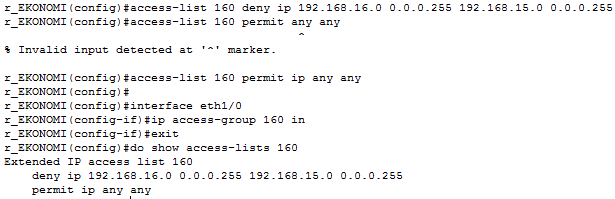


**Gambar 5.16** Konfigurasi ACL pada *Router* MIPA



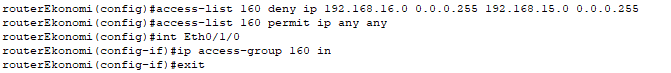
**Gambar 5.17** Hasil konfigurasi ACL pada *router*MIPA

1. *Router*Ekonomi



**Gambar 5.18** Hasil konfigurasi ACL pada *Router*Ekonomi

“access-list 160 deny ip host 192.168.16.0 0.0.0.255 192.168.15.0 0.0.0.0.255”, berarti bahwa *network* “192.168.16.0” tidak diperbolehkan untuk mengakses *network* “192.168.15.0”.



**Gambar 5.19** Konfigurasi ACL pada *Router*Ekonomi

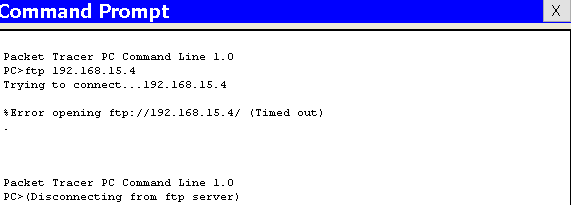
“access-list 160 permit any any”, berarti bahwa selain IP atau *network* yang di-*deny* maka semua IP atau *network* bisa saling terhubung.

Adapun hasil konfigurasi ACL yang telah dilakuakan pada *router* Ekonomi adalah sebagai berikut:



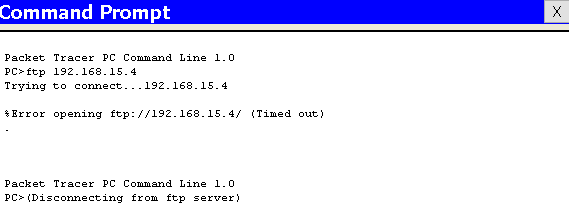
**Gambar 5.20** Hasil konfigurasi ACL pada *Router*Ekonomi

* + - 1. Hasil uji koneksi berdasarkan aturan yang telah diberikan beserta analisanya.

1. Sipil Tidak Boleh mengakses *Service* FTP *server*

**Gambar 5.21** Uji koneksi PC Sipil ke FTP *server*

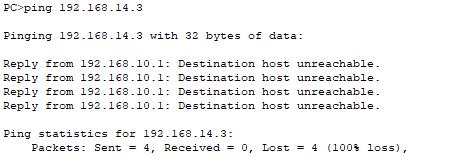
Pada **Gambar 5.21** merupakan hasil uji koneksi antara PC Sipil dengan FTP *server* yang memiliki IP *address* 192.168.15.4. Ketika diuji, hasilnya adalah “Request Timeout” yang artinya PC Sipil sudah tidak dapat mengakses FTP *server* karena saat di konfigurasi *access control list* dengan perintah “Deny” PC Sipil telah dibatasi atau diblok untuk tidak dapat mengakses FTP *server.*

1. Elektro Tidak Boleh mengakses *Service* FTP *Server*

**Gambar 5.22** Uji koneksi PC Elektro ke FTP *server*

Pada **Gambar 5.22** merupakan hasil uji koneksi antara PC Elektro dengan FTP *server* yang memiliki IP *address* 192.168.15.4. Ketika diuji, hasilnya adalah “Request Timeout” yang artinya PC Elektro sudah tidak dapat mengakses FTP *server* karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC elektro telah dibatasi atau diblok untuk tidak dapat mengakses FTP *server.*

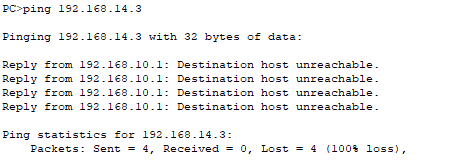
1. Sipil Tidak Boleh mengakses Kimia



**Gambar 5.23** Uji koneksi PC Sipil ke PC Kimia

Pada **Gambar 5.23** merupakan hasil uji koneksi antara PC Sipil dengan PC Kimiayang memiliki IP *address* 192.168.14.3. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC Sipil yang artinya PC Sipil sudah tidak dapat mengakses PC Kimia karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Sipil telah dibatasi atau diblok untuk tidak dapat mengakses PC Kimia*.*

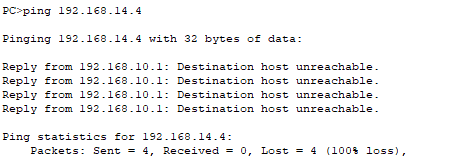
1. Elektro Tidak Boleh mengakses Kimia



**Gambar 5.24** Uji koneksi PC Elektro ke PC Kimia

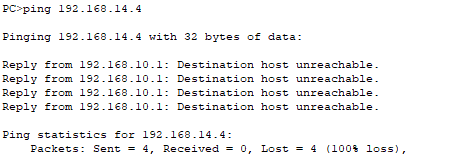
Pada **Gambar 5.24** merupakan hasil uji koneksi antara PC Elektro dengan PC Kimiayang memiliki IP *address* 192.168.14.3. Ketika diuji, hasilnya adalah “*host unreachable*” atau *host* tidak dapat terjangkau oleh PC Elektro yang artinya PC elektro sudah tidak dapat mengakses PC Kimia karena saat dikonfigurasi *access control list* dengan perintah “*deny*” PC Elektro telah dibatasi atau diblok untuk tidak dapat mengakses PC Kimia*.*

1. Sipil Tidak Boleh mengakses Biologi



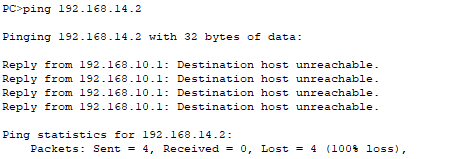
**Gambar 5.25** Uji koneksi PC Sipil ke PC Biologi

Pada **Gambar 5.25** merupakan hasil uji koneksi antara PC Sipil dengan PC Biologiyang memiliki IP *address* 192.168.14.4. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC sipil yang artinya PC Sipil sudah tidak dapat mengakses PC Biologi karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Sipil telah dibatasi atau diblok untuk tidak dapat mengakses PC Biologi.

1. Elektro Tidak Boleh mengakses Biologi

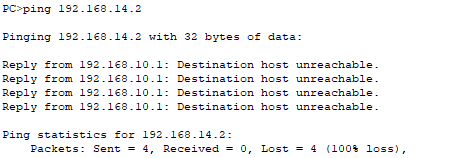
**Gambar 5.26** Uji koneksi PC Elektro ke PC Biologi

Pada **Gambar 5.26** merupakan hasil uji koneksi antara PC Sipil dengan PC Biologiyang memiliki IP *address* 192.168.14.4. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC Elektro yang artinya PC Elektro sudah tidak dapat mengakses PC Biologi karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Elektro telah dibatasi atau diblok untuk tidak dapat mengakses PC Biologi*.*

1. Sipil Tidak Boleh mengakses Matematika

**Gambar 5.27** Uji koneksi PC Sipil ke PC Matematika

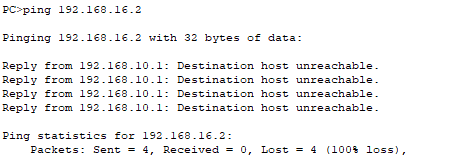
Pada **Gambar 5.27** merupakan hasil uji koneksi antara PC Sipil dengan PC Matematikayang memiliki IP *address* 192.168.14.2. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC sipil yang artinya PC Sipil sudah tidak dapat mengakses PC Matematika karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Sipil telah dibatasi atau diblok untuk tidak dapat mengakses PC Matematika*.*

1. Elektro Tidak Boleh mengakses Matematika

**Gambar 5.28** Uji koneksi PC Elektro ke PC Matematika

Pada **Gambar 5.28** merupakan hasil uji koneksi antara PC Elektro dengan PC Matematikayang memiliki IP *address* 192.168.14.2. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC Elektro yang artinya PC Elektro sudah tidak dapat mengakses PC Matematika karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Elektro telah dibatasi atau diblok untuk tidak dapat mengakses PC Matematika*.*

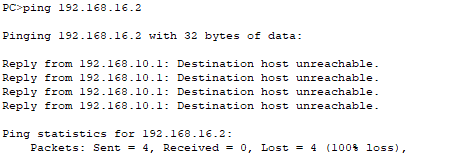
1. Sipil Tidak Boleh mengakses Akuntansi



**Gambar 5.29** Uji koneksi PC Sipil ke PC Akuntansi

Pada **Gambar 5.29** merupakan hasil uji koneksi antara PC Sipil dengan PC Akuntansiyang memiliki IP *address* 192.168.16.2. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC Sipil yang artinya PC Sipil sudah tidak dapat mengakses PC Akuntansi karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Sipil telah dibatasi atau diblok untuk tidak dapat mengakses PC Akuntansi*.*

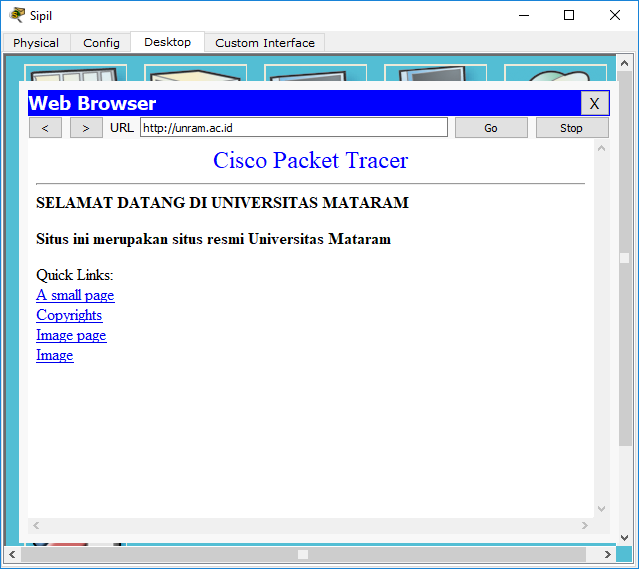
1. Elektro Tidak Boleh mengakses Akuntansi



**Gambar 5.30** Uji koneksi PC Elektro ke PC Akuntansi

Pada **Gambar 5.30** merupakan hasil uji koneksi antara PC Elektro dengan PC Akuntansiyang memiliki IP *address* 192.168.16.2. Ketika diuji, hasilnya adalah “host unreachable” atau *host* tidak dapat terjangkau oleh PC Elektro yang artinya PC Elektro sudah tidak dapat mengakses PC Akuntansi karena saat dikonfigurasi *access control list* dengan perintah “Deny” PC Sipil telah dibatasi atau diblok untuk tidak dapat mengakses PC Akuntansi*.*

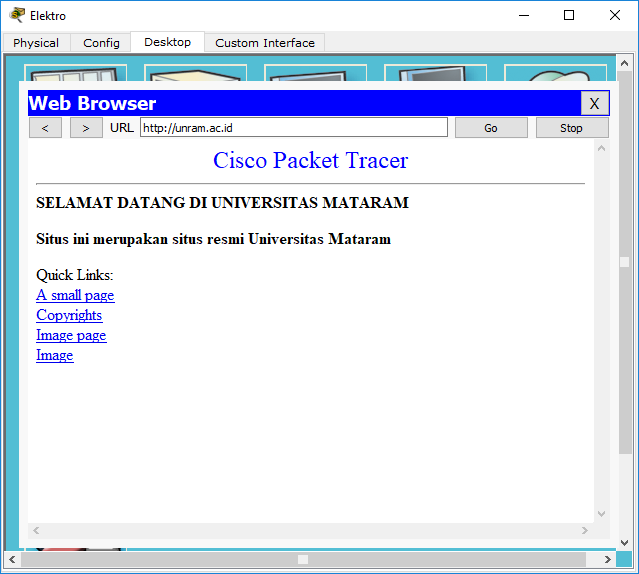
1. Sipil Boleh mengakses Web dan DNS *Server*



**Gambar 5.31** Uji koneksi PC Sipil ke Web dan DNS *server*

Pada **Gambar 5.31** merupakan hasil uji koneksi antara PC Sipil dengan Web dan DNS *server* yang memiliki URL *unram.ac.id* dan DNS *Address* 192.168.15.2. Ketika diuji, hasilnya web UNRAM dapat dibuka karena telah diberikan *access* “permit”.

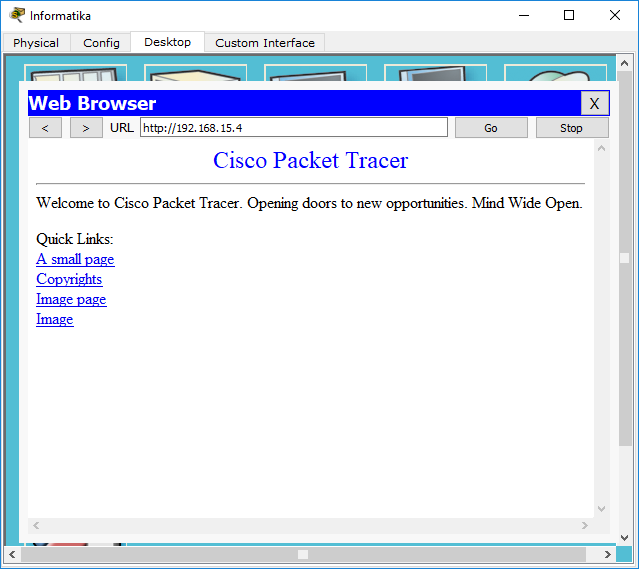
1. Elektro Boleh mengakses Web dan DNS *Server*



**Gambar 5.32** Uji koneksi PC Elektro ke Web dan DNS *server*

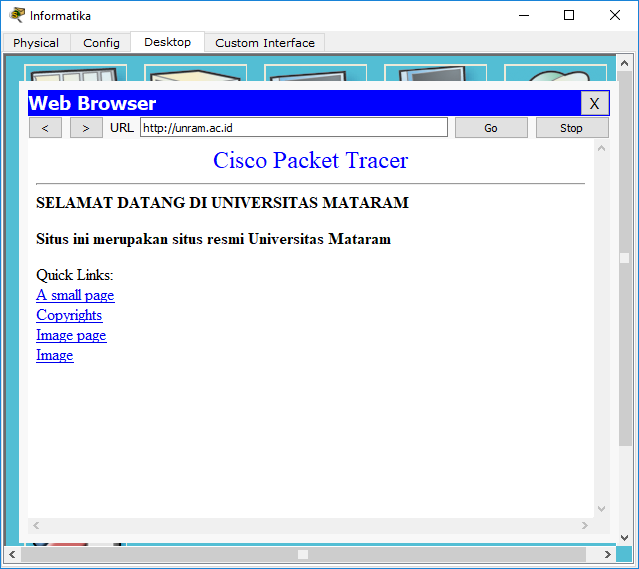
Pada **Gambar 5.32** merupakan hasil uji koneksi antara PC Elektro dengan Web dan DNS *server* yang memiliki URL *unram.ac.id* dan DNS *Address* 192.168.15.2. Ketika diuji, hasilnya web UNRAM dapat dibuka karena telah diberikan *access* “permit”.

1. Informatika Boleh mengakses semua *Server*



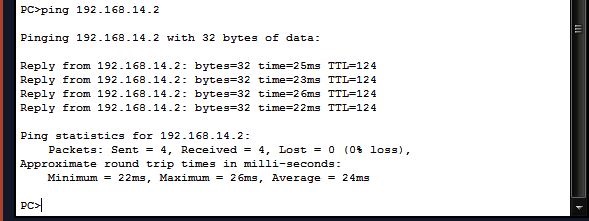
**Gambar 5.33** Uji koneksi PC Informatika ke FTP *server*

Pada **Gambar 5.33** merupakan hasil uji koneksi antara PC Informatika dengan FTP *server* yang memiliki yang memiliki IP *address* 192.168.15.4. Ketika diuji, hasilnya web dapat dibuka karena telah diberikan *access* “permit”agar dapat terhubung dengan FTP *server.*



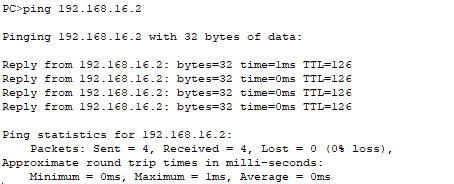
**Gambar 5.34** Uji koneksi PC Informatika ke Web dan DNS *server*

Pada **Gambar 5.34** merupakan hasil uji koneksi antara PC Informatika dengan Web dan DNS *server* yang memiliki URL *unram.ac.id*. Ketika diuji, hasilnya web UNRAM dapat dibuka karena telah diberikan *access* “permit”untuk dapat terhubung dengan web *server* UNRAM.

1. ****Informatika Boleh mengakses Matematika

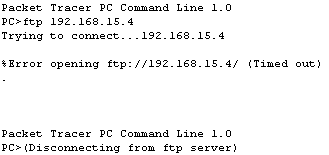
**Gambar 5.35** Uji koneksi PC Informatika ke PC Matematika

Pada **Gambar 5.35** dilakukan tes koneksi antar PC informatika ke PC matematikayang memiliki IP *address* 192.168.14.2. PC informatika akan mendapatkan hasil dari PC tujuan berupa paket yang dikirimkan berhasil diterima tanpa kehilangan data. Maka dapat dikatakan aturan ini telah berhasil ditetapkan.

1. Informatika Boleh mengakses Akuntansi

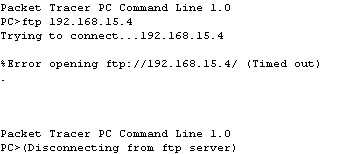
**Gambar 5.36** Uji koneksi PC Informatika ke PC Akuntansi

Pada **Gambar 5.36** dilakukan tes koneksi antar PC informatika ke PC akuntansiyang memiliki IP *address* 192.168.16.2. PC informatika akan mendapatkan hasil dari PC tujuan berupa paket yang dikirimkan berhasil diterima tanpa kehilangan data. Maka dapat dikatakan aturan ini telah berhasil ditetapkan.

1. Matematika Tidak Boleh mengakses *Service* FTP *Server*

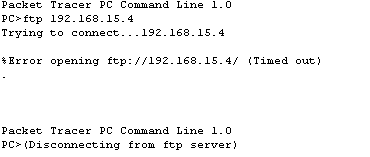
**Gambar 5.37** Uji koneksi PC Matematika ke FTP *server*

Pada **Gambar 5.37** merupakan hasil uji koneksi antara PC Matematika dengan FTP *server* yang memiliki IP *address* 192.168.15.4. Ketika diuji, hasilnya adalah “Request Timeout” yang artinya PC Matematika sudah tidak dapat mengakses FTP *server* karena saat dikonfigurasi *access control list* dengan perintah “deny” PC Matematika telah dibatasi atau diblok untuk tidak dapat mengakses FTP *server.*

1. Kimia Tidak Boleh mengakses *Service* FTP *Server*

**Gambar 5.38** Uji koneksi PC Kimia ke FTP *server*

Pada **Gambar 5.38** merupakan hasil uji koneksi antara PC Kimia dengan FTP *server* yang memiliki IP *address* 192.168.15.4. Ketika diuji, hasilnya adalah “Request Timeout” yang artinya PC Kimia sudah tidak dapat mengakses FTP *server* karena saat dikonfigurasi *access control list* dengan perintah “deny” PC Kimia telah dibatasi atau diblok untuk tidak dapat mengakses FTP *server.*

1. Biologi Tidak Boleh mengakses *Service* FTP *Server*

**Gambar 5.39** Uji koneksi PC Biologi ke FTP *server*

Pada **Gambar 5.39** merupakan hasil uji koneksi antara PC Biologi dengan FTP *server* yang memiliki IP *address* 192.168.15.4. Ketika diuji, hasilnya adalah “Request Timeout” yang artinya PC Biologi sudah tidak dapat mengakses FTP *server* karena saat dikonfigurasi *access control list* dengan perintah “deny” PC Biologi telah diblok untuk tidak dapat mengakses FTP *server.*

1. Matematika Boleh mengakses Web dan DNS *Server* Unram

****

**Gambar 5.40** Uji koneksi PC Matematika ke Web dan DNS *server*

Pada **Gambar 5.40** merupakan hasil uji koneksi antara PC Matematika dengan Web dan DNS *server* yang memiliki URL unram.ac.id dan DNS *Address* 192.168.15.2. Ketika diuji, hasilnya web UNRAM dapat dibuka karena telah diberikan *access* “permit” untuk dapat terhubung dengan web *server* UNRAM.

1. Kimia Boleh mengakses Web dan DNS *Server* Unram

****

**Gambar 5.41** Uji koneksi PC Kimia ke Web dan DNS *server*

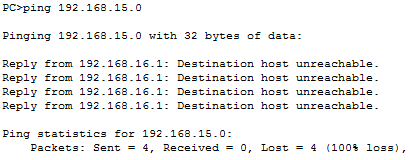
Pada **Gambar 5.41** merupakan hasil uji koneksi antara PC Kimia dengan Web dan DNS *server* yang memiliki URL unram.ac.id dan DNS *Address* 192.168.15.2. Ketika diuji, hasilnya web UNRAM dapat dibuka karena telah diberikan *access* “permit” untuk dapat terhubung dengan web *server* UNRAM.

1. ****Biologi Boleh mengakses Web dan DNS *Server* Unram

**Gambar 5.42** Uji koneksi PC Biologi ke Web dan DNS *server*

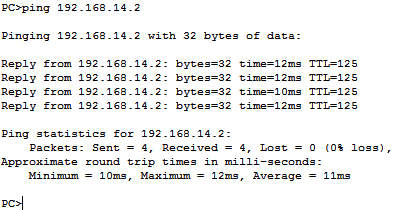
Pada **Gambar 5.42** merupakan hasil uji koneksi antara PC Biologi dengan Web dan DNS *server* yang memiliki URL unram.ac.id dan DNS *Address* 192.168.15.2. Ketika diuji, hasilnya web UNRAM dapat dibuka karena telah diberikan *access* “permit”untuk dapat terhubung dengan web *server* UNRAM.

1. LAN Ekonomi Tidak Boleh mengakses LAN Pustik



**Gambar 5.43** Uji koneksi PC Akuntansi di LAN Ekonomi ke Web *server* di LAN Pustik

Pada **Gambar 5.43** merupakan hasil uji koneksi antara PC Akuntansi yang berada pada LAN Ekonomi dengan Web dan DNS *server* yang berada pada LAN Pustik*.* Web dan DNS *server* memiliki URL unram.ac.id. Ketika diuji, hasilnya web UNRAM tidak dapat dibuka karena telah diberikan *access* “Deny”untuk tidak dapat terhubung dengan web *server* UNRAM.

1. ****LAN Ekonomi Boleh mengakses LAN MIPA

**Gambar 5.44** Uji koneksi PC Akuntansi di LAN Ekonomi ke PC Matematika di LAN MIPA

Pada **Gambar 5.44** dilakukan tes koneksi antar PC Akuntansi yang ada pada LAN Ekonomi ke PC Matematika yang berada pada LAN MIPAyang memiliki IP *address* 192.168.14.2. PC Akuntansi akan mendapatkan hasil dari PC tujuan berupa paket yang dikirimkan berhasil diterima tanpa kehilangan data.

1. **KESIMPULAN**

Berdasarkan pratikum yang telah dilakukan, didapatkan kesimpulan sebagai berikut:

1. ACL adalah daftar urutan pernyataan penerimaan atau penolakan yang dijalankan untuk pengalamatan atau protokol *layer* atas. Tujuan dari penggunaan ACL adalah untuk mengatur jalur trafik masuk ataupun keluarnya akses jaringan, dalam hal ini dapat menentukan akses tersebut dapat dilewatkan atau diblok.
2. Dalam melakukan pengujian koneksi didapatkan hasil jika dikonfigurasi dengan perintah “*Deny*” akan menghasilkan “*Request Timeout*” dan “*Destination host unreachable*” yang berarti penolakan akses ke *server*. Dan jika dikonfigurasi dengan perintah “*Permit*” maka akan dapat mengakses *web* Unram pada *server.*
3. Lalu lintas ACL dibagi menjadi 2 macam, *inbound* dan *outbound*. *Inbound* ACL diterapkan pada paket yang masuk pada suatu *interface* sedangkan *outbound* diterapkan pada paket yang keluar pada suatu *interface* dan diproses melalui antrian