



MODUL PRAKTIKUM SISTEM OPERASI DAN JARINGAN KOMPUTER

10. ACL & DHCP

Access Control List (ACL)

A. Pengenalan

ACL adalah singkatan dari Access Control List, yang merupakan daftar yang digunakan untuk mengontrol hak akses ke sumber daya atau objek tertentu dalam sistem komputer atau jaringan. ACL digunakan untuk mengatur izin akses, pembatasan, atau pengaturan keamanan pada berbagai jenis sumber daya, seperti berkas, direktori, perangkat jaringan, atau objek lainnya. Secara umum, dalam ACL terdapat entri yang mencakup identitas pengguna atau grup pengguna tertentu dan hak akses yang diberikan kepada mereka. Contoh hak akses yang dapat diatur dalam ACL meliputi hak akses membaca, menulis, mengeksekusi, mengedit, menghapus, dan lain sebagainya.

1. Keamanan: Mencegah akses yang tidak sah.
2. Efisiensi: Mengatur hak akses secara sistematis berdasarkan kebijakan organisasi.
3. Fleksibilitas: Dapat digunakan di berbagai perangkat dan sistem, seperti server atau perangkat jaringan.

B. Jenis Lalu Lintas ACL

- Outbound

Outbound ACL digunakan untuk mengontrol apa yang diperbolehkan dan apa yang diblokir ketika lalu lintas meninggalkan jaringan. Ini dapat mencakup lalu lintas yang dihasilkan oleh pengguna, server, atau perangkat dalam jaringan yang akan menghubungi sumber daya di luar jaringan. Outbound ACL umumnya digunakan untuk memberikan perlindungan dan mengendalikan lalu lintas keluar dari jaringan, memastikan kepatuhan dengan kebijakan keamanan jaringan, serta melindungi sumber daya internal dari ancaman eksternal. Ini juga dapat digunakan untuk mengendalikan lalu lintas yang keluar menuju jaringan

yang mungkin memiliki batasan atau aturan tertentu.

- **Inbound**

Inbound ACL mengontrol lalu lintas yang mencoba memasuki jaringan Anda. Ini mencakup lalu lintas yang berasal dari sumber eksternal, seperti internet atau jaringan lainnya, dan menuju ke sumber daya di dalam jaringan. Inbound ACL digunakan untuk memberikan perlindungan jaringan dari lalu lintas yang tidak diinginkan, potensial berbahaya, atau yang tidak sesuai dengan kebijakan keamanan jaringan. Hal ini membantu mencegah serangan dari luar, seperti serangan DDoS (Distributed Denial of Service), serangan malware, atau upaya penetrasi ilegal.

C. Jenis ACL

- **Standard ACL**

Standard Access Control Lists (Standard ACL) adalah jenis Access Control List (ACL) dalam jaringan yang digunakan untuk mengontrol akses ke sumber daya jaringan berdasarkan alamat IP pengirim. Standard ACL memungkinkan Anda mengatur lalu lintas jaringan dengan cara yang lebih sederhana dibandingkan dengan jenis ACL lainnya, seperti Extended ACL. Fokus utama Standard ACL adalah pada alamat IP pengirim, dan karena itu, hanya dapat mengizinkan atau memblokir lalu lintas berdasarkan alamat IP tersebut. Untuk ACL Standar, biasanya digunakan rentang nomor ACL dari 1 hingga 99.

Kelebihan dari Standard ACL adalah kesederhanaannya dan efisiensinya dalam mengizinkan atau memblokir seluruh subnet jaringan atau host tertentu. Namun, keterbatasannya terletak pada kurangnya fleksibilitas. Anda tidak dapat mengatur lalu lintas berdasarkan alamat IP tujuan, nomor port, protokol, atau parameter lainnya. Oleh karena itu,

Standard ACL lebih sesuai untuk situasi yang memerlukan pengontrolan lalu lintas yang sangat sederhana, seperti mengizinkan atau memblokir seluruh subnet jaringan atau host tertentu.

- **Extended ACL**

Extended Access Control Lists (Extended ACL) adalah jenis Access Control List (ACL) yang digunakan dalam jaringan komputer untuk mengontrol lalu lintas jaringan secara rinci dan canggih. Dalam Extended ACL, Anda dapat menentukan aturan berdasarkan beberapa parameter, termasuk alamat IP pengirim dan tujuan, nomor port, protokol, dan opsi lainnya. Kelebihan utama dari Extended ACL adalah kemampuannya untuk memberikan kontrol yang sangat terperinci atas lalu lintas jaringan, yang membuatnya ideal untuk mengatur kebijakan keamanan jaringan yang kompleks. Extended ACL digunakan untuk mengizinkan atau memblokir akses ke layanan atau sumber daya jaringan tertentu, mengelola lalu lintas menuju server aplikasi, serta melindungi jaringan dari ancaman jaringan dengan lebih rinci dan tepat. Ini menjadikannya pilihan yang lebih kuat dibandingkan dengan Standard ACL yang hanya memungkinkan pengontrolan berdasarkan alamat IP pengirim. Konfigurasi Extended ACL biasanya melibatkan penentuan alamat IP sumber dan tujuan, protokol, nomor port, dan tindakan yang harus diambil terhadap lalu lintas yang cocok dengan aturan tersebut. Untuk ACL Ekstensif, biasanya digunakan rentang nomor ACL dari 100 hingga 199.

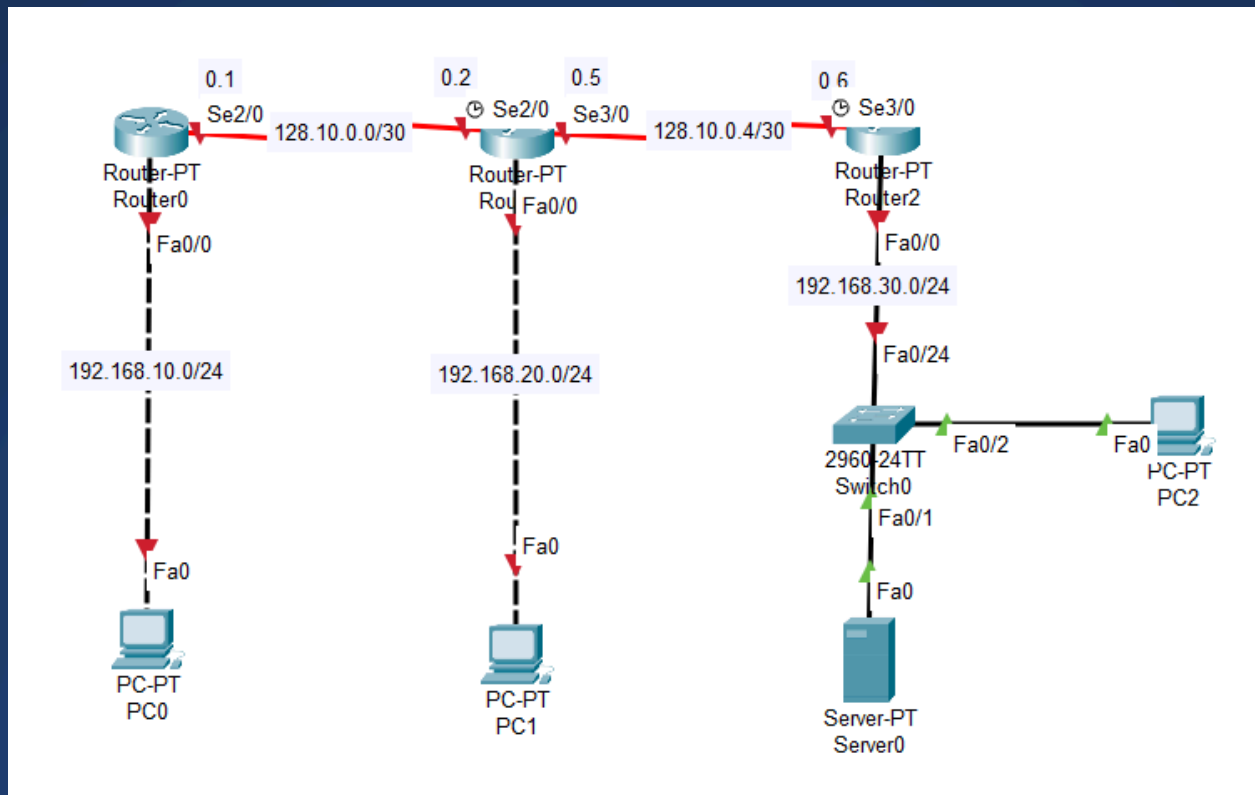
- Kelebihan : Kontrol yang lebih rinci.
- Kekurangan : Konfigurasi lebih kompleks.
- Contoh Penggunaan : Memblokir akses ke layanan tertentu (HTTP, FTP) untuk alamat IP tertentu

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) adalah protokol jaringan yang digunakan untuk otomatisasi konfigurasi alamat IP dan parameter jaringan lainnya kepada perangkat yang terhubung ke jaringan. DHCP memungkinkan perangkat seperti komputer, ponsel, atau perangkat jaringan lainnya untuk mendapatkan konfigurasi jaringan secara dinamis tanpa perlu konfigurasi manual. Dalam jaringan yang menggunakan DHCP, ketika sebuah perangkat terhubung ke jaringan, ia akan secara otomatis meminta konfigurasi jaringan dari server DHCP. Server DHCP kemudian memberikan alamat IP yang unik, bersama dengan informasi seperti subnet mask, gateway, dan DNS server kepada perangkat tersebut.

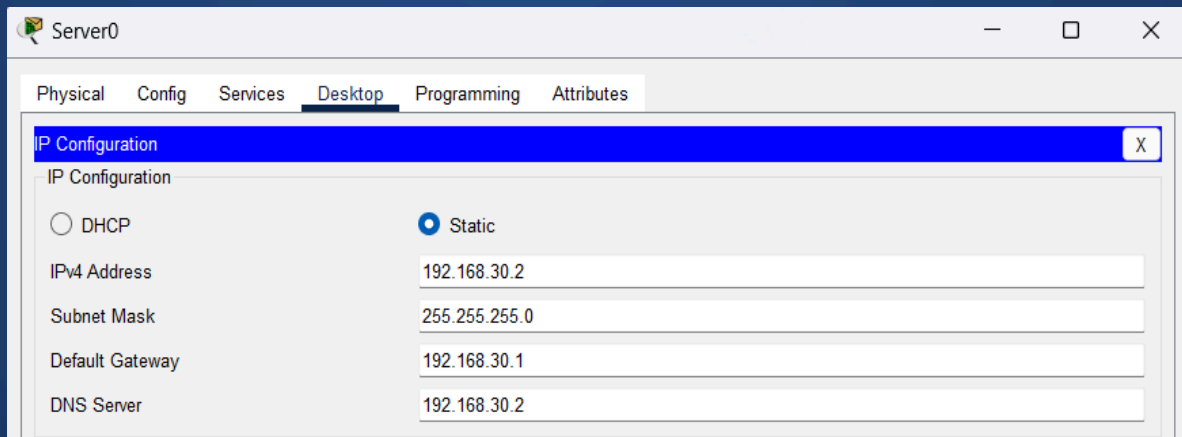
Dynamic Host Configuration Protocol (DHCP) berfungsi sebagai mekanisme otomatis yang memfasilitasi konfigurasi perangkat yang terhubung ke jaringan. Ketika perangkat baru terhubung, ia mengirimkan permintaan DHCP Discover yang diterima oleh server-server DHCP di jaringan. Server-server tersebut merespons dengan tawaran konfigurasi dalam bentuk pesan DHCP Offer. Klien memilih tawaran yang paling sesuai dan mengirimkan pesan DHCP Request untuk mengkonfirmasi tawaran tersebut. Setelah menerima pesan Request, server DHCP mengirimkan pesan DHCP Acknowledgment (ACK) yang berisi konfirmasi. Klien mengkonfigurasi dirinya sendiri sesuai dengan konfigurasi yang diterima, termasuk alamat IP, subnet mask, gateway, dan informasi jaringan lainnya. Perangkat perlu secara berkala memperbarui sewa alamat IP melalui proses yang dikenal sebagai lease renewal. Apabila perangkat tidak lagi memerlukan alamat IP, ia dapat mengembalikan alamat tersebut ke pool DHCP dengan mengirim pesan DHCP Release. Proses ini memungkinkan perangkat untuk secara otomatis dan efisien mendapatkan konfigurasi jaringan tanpa konfigurasi manual yang rumit.

KONFIGURASI STANDARD ACCESS LIST

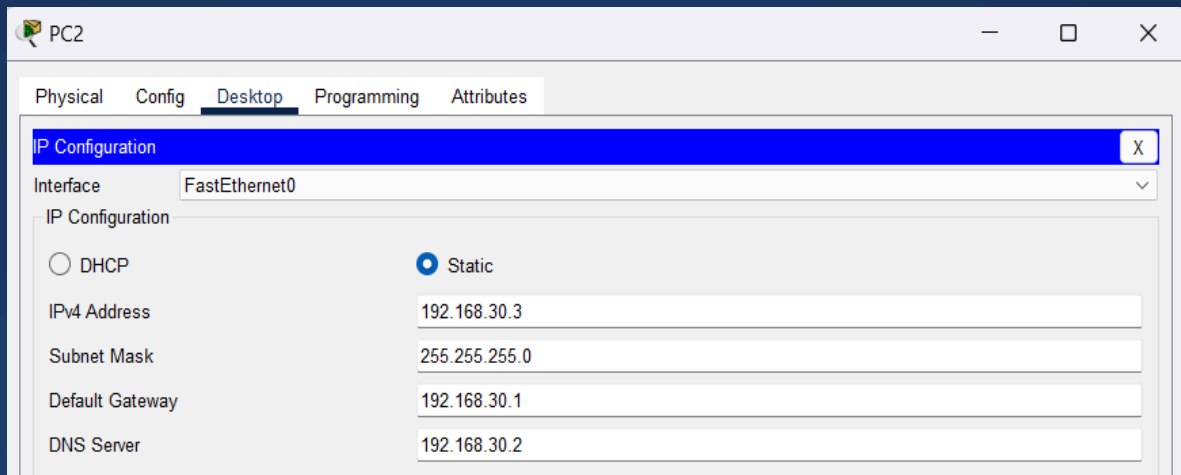


Buatlah topologi seperti yang di atas ini:

a. Konfigurasi untuk Server



b. Konfigurasi untuk PC2



c. Konfigurasi untuk Router0

```
Router>en
```

```
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#int fa0/0
```

```
Router(config-if)#no sh
```

```
Router(config-if)#
```

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

```
Router(config-if)#ip add 192.168.10.1 255.255.255.0
```

```
Router(config-if)#ex
```

```
Router(config)#int se2/0
```

```
Router(config-if)#no sh
```

%LINK-5-CHANGED: Interface Serial2/0, changed state to down

```
Router(config-if)#
```

```
Router(config-if)#ip add 128.10.0.1 255.255.255.252
```

```
Router(config-if)#ex
```

```
Router(config)#service dhcp
```

```
Router(config)#ip dhcp pool jarkom
Router(dhcp-config)#net 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 192.168.30.2
Router(dhcp-config)#ex
Router(config)#ip dhcp excluded-address 192.168.10.1
```

```
Router(config)#router eigrp 10
Router(config-router)#net 128.10.0.0
Router(config-router)#net 192.168.10.0
Router(config-router)#ex
```

d. Konfigurasi untuk Router1

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Router(config-if)#ip add 192.168.20.1 255.255.255.0
Router(config-if)#ex
Router(config)#int se2/0
Router(config-if)#ip add 128.10.0.2 255.255.255.252
Router(config-if)#no sh
```


Router(config-if)#

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router(config-if)#ex

Router(config)#int se3/0

Router(config-if)#ip add 128.10.0.5 255.255.255.252

Router(config-if)#no sh

%LINK-5-CHANGED: Interface Serial3/0, changed state to down

Router(config-if)#ex

Router(config)#service dhcp

Router(config)#ip dhcp pool prak

Router(dhcp-config)#net 192.168.20.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.20.1

Router(dhcp-config)#dns-server 192.168.30.2

Router(dhcp-config)#ex

Router(config)#ip dhcp excluded-address 192.168.20.1

Router(config)#router eigrp 10

Router(config-router)#net 128.10.0.0

Router(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 128.10.0.1 (Serial2/0) is up: new adjacency

Router(config-router)#net 128.10.0.4

Router(config-router)#net 192.168.20.0

Router(config-router)#ex

Router(config)#

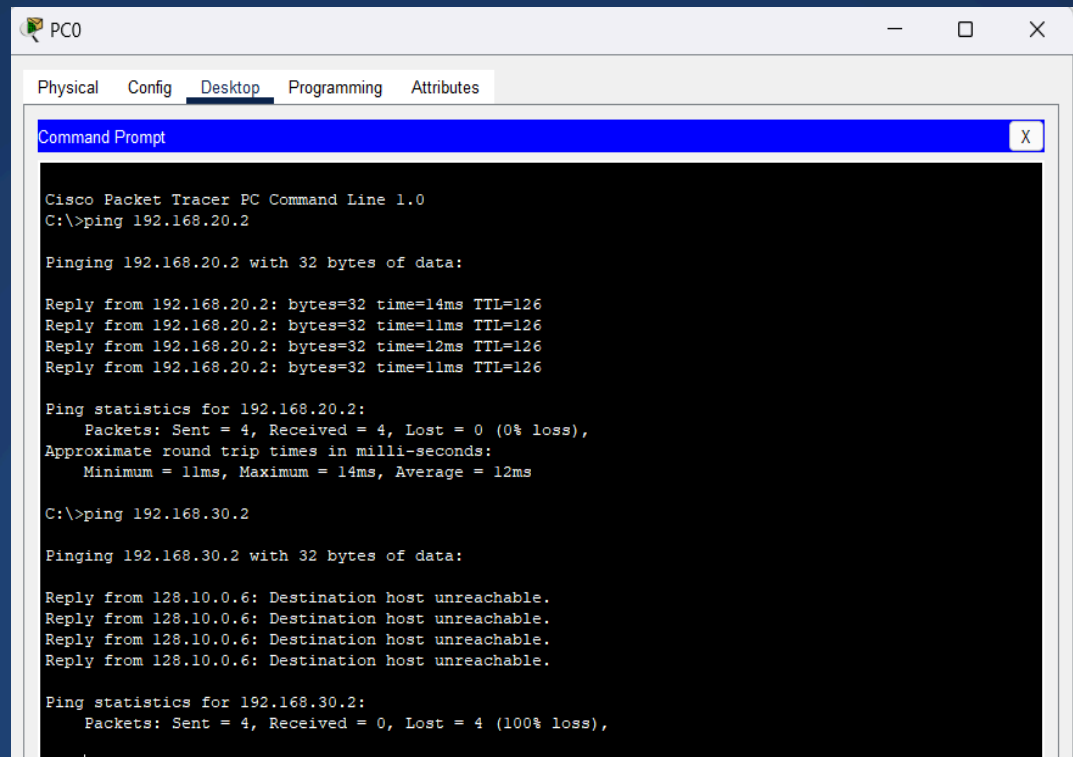
e. Konfigurasi untuk Router2

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#no sh
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
Router(config-if)#ip add 192.168.30.1 255.255.255.0
Router(config-if)#ex
Router(config)#int se3/0
Router(config-if)#ip add 128.10.0.6 255.255.255.252
Router(config-if)#no sh
Router(config-if)#
%LINK-5-CHANGED: Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed
state to up
Router(config-if)#ex
Router(config)#router eigrp 10
Router(config-router)#net 128.10.0.4
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 128.10.0.5 (Serial3/0) is
up: new adjacency
Router(config-router)#net 192.168.30.0
Router(config-router)#ex

Router(config)#access-list 1 deny host 192.168.10.2
Router(config)#access-list 1 permit any
Router(config)#int fa0/0
```

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

Router(config-if)#



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=14ms TTL=126
Reply from 192.168.20.2: bytes=32 time=11ms TTL=126
Reply from 192.168.20.2: bytes=32 time=12ms TTL=126
Reply from 192.168.20.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 12ms

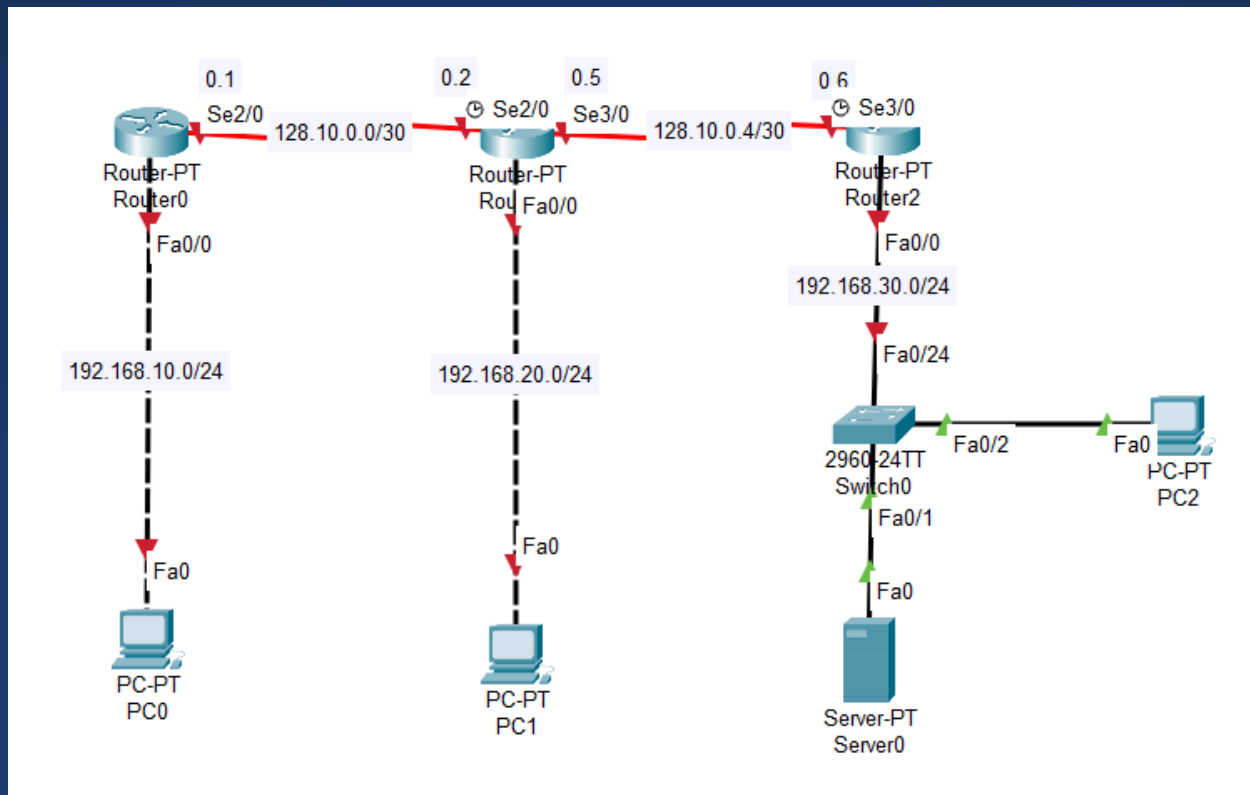
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 128.10.0.6: Destination host unreachable.
Reply from 128.10.0.6: Destination host unreachable.
Reply from 128.10.0.6: Destination host unreachable.
Reply from 128.10.0.6: Destination host unreachable.

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

KONFIGURASI EXTENDED ACCESS LIST



Buatlah topologi seperti yang di atas ini:

a. Konfigurasi Server

Lakukan hal yang sama seperti sebelumnya

b. Konfigurasi untuk PC 2

Lakukan hal yang sama seperti sebelumnya

c. Konfigurasi untuk Router3

Lakukan hal yang sama, namun kali ini tambahkan ACL

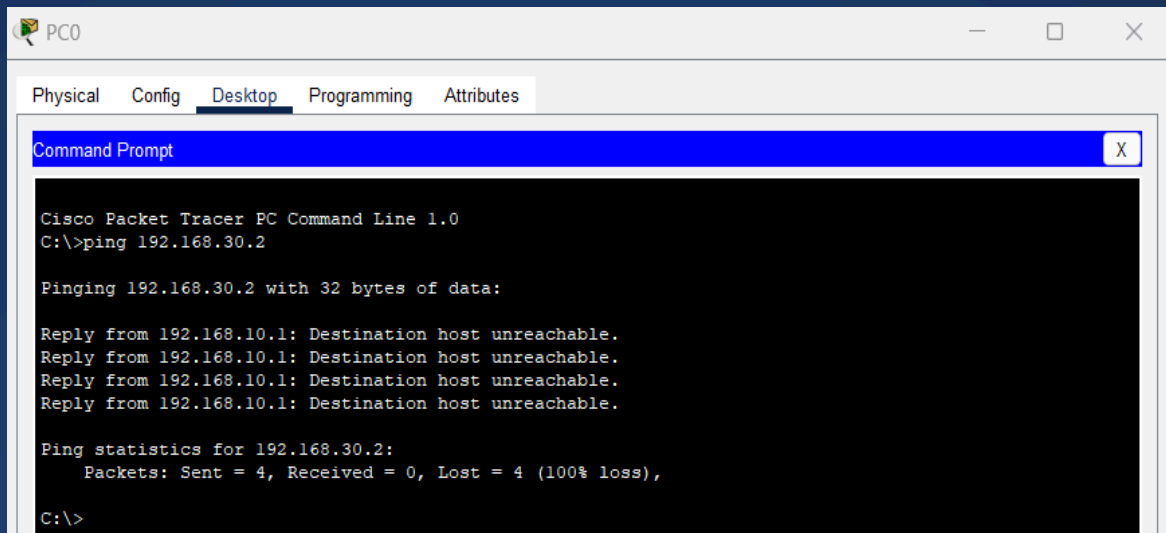
```
Router(config)#ip access-list extended block
```

```
Router(config-ext-nacl)#deny icmp host 192.168.10.2 host 192.168.30.2
```

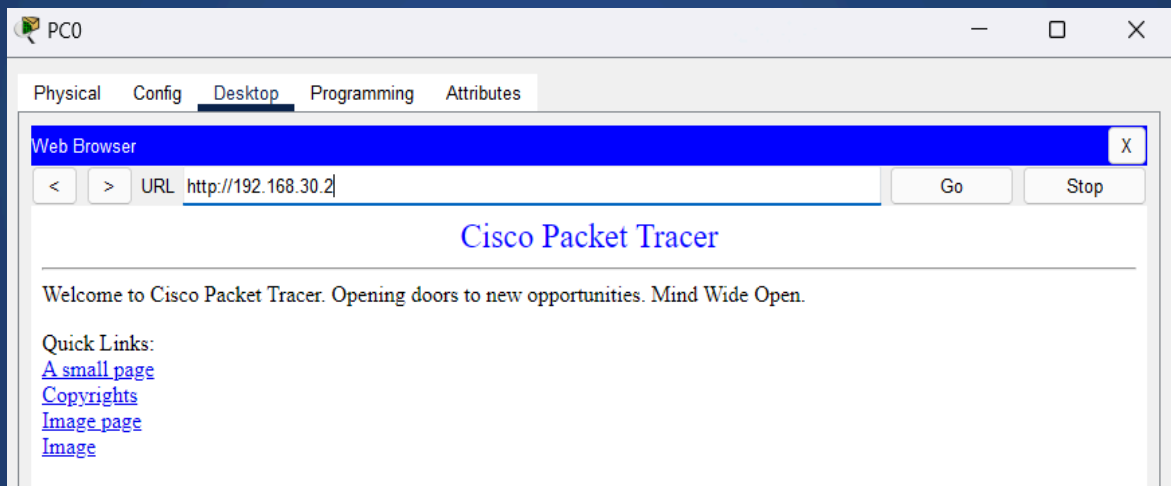
```
Router(config-ext-nacl)#permit ip any any
```

```
Router(config-ext-nacl)#int fa0/0
```

```
Router(config-if)#ip access-group block in
```



Namun Web Server nya masih bisa diakses



d. Router4

Lakukan hal yang sama, namun kali ini tambahkan ACL

```
Router(config)#ip access-list extended block
```

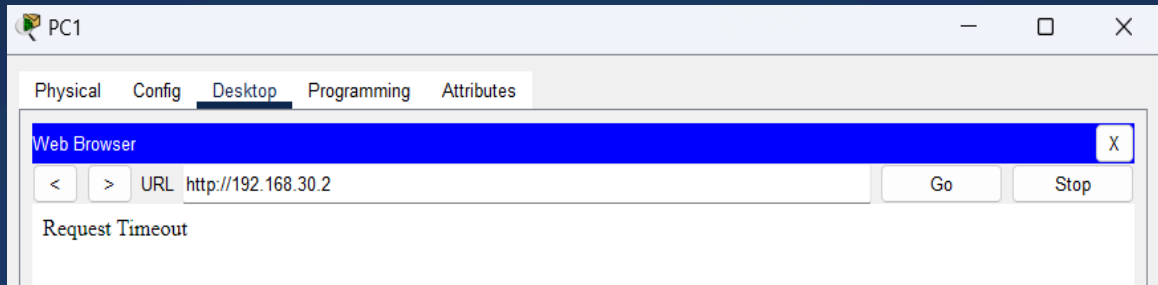
```
Router(config-ext-nacl)#deny tcp host 192.168.20.2 host 192.168.30.2 eq www
```

```
Router(config-ext-nacl)#permit ip any any
```

```
Router(config-ext-nacl)#int fa0/0
```

```
Router(config-if)#ip access-group block in
```

```
Router(config-if)#
```



e. Router5

Lakukan hal yang sama sebelumnya