

## Tugas Kelompok 4 [Pekan 14]

### Anggota Kelompok dan Peran:

- Muhammad Ayash Az dzikri 10231060 - Network Engineer
- Cintya Widhi Astuti 10231026 - Security & Documentation Specialist
- Riqqah Khaldi Karina 10231082 - Network Architect
- Verina Rahma Dinah 10231090 - Network Services Specialist

### Tugas Kelompok:

1. Implementasi Access Control List (ACL) sesuai kebijakan keamanan.
2. Pengujian menyeluruh semua fitur jaringan.
3. Troubleshooting dan perbaikan masalah.

### Deliverable (Format Markdown):

- **Laporan Implementasi Tahap 4**, berisi:
- Link file simulasi final.
- **WAJIB:** Dokumentasi konfigurasi CLI lengkap untuk implementasi ACL:

```
### ACL Configuration
```bash
Router> enable
Router# configure terminal
Router(config)# access-list 101 deny ip 192.168.20.0 0.0.0.255 192.168.30.0
0.0.0.255
```

- Matriks pengujian yang menunjukkan semua fitur telah diuji dengan screenshot hasil dan penjel
- Hasil troubleshooting (jika ada) dan solusinya dengan penjelasan detail langkah-langkah yang
- Analisis keamanan jaringan yang telah diimplementasikan.

### Pendahuluan

#### Latar Belakang

PT. Nusantara Network merupakan perusahaan teknologi informasi yang sedang berkembang dengan struktur organisasi yang terdiri dari 5 departemen utama yang tersebar di 2 gedung yang berbeda, yaitu kantor pusat (Gedung A) dan kantor cabang (Gedung B). Seiring dengan perkembangan bisnis dan kompleksitas operasional perusahaan, kebutuhan akan infrastruktur jaringan yang mudah dikelola, aman, dan efisien menjadi semakin krusial.

Infrastruktur jaringan yang digunakan saat ini belum sepenuhnya mampu memenuhi kebutuhan tersebut, khususnya dalam hal keamanan data, manajemen traffic, serta kemudahan pengelolaan jaringan secara terpusat. Selain itu, belum adanya pengaturan pembagian akses antar departemen secara optimal menimbulkan potensi celah keamanan dan inefisiensi dalam komunikasi data antar unit kerja. Oleh karena itu, diperlukan perancangan ulang infrastruktur jaringan yang dapat mengakomodasi kebutuhan perusahaan secara menyeluruh.

## Tujuan

Perancangan jaringan ini bertujuan untuk:

- Membangun jaringan yang aman dan efisien melalui segmentasi VLAN.
- Menyediakan konektivitas antar gedung menggunakan teknologi WAN.
- Mengatur akses internet dengan implementasi NAT.
- Menyediakan layanan DHCP dan DNS untuk pengelolaan IP dan resolusi nama.
- Menerapkan ACL untuk pembatasan akses antar departemen.
- Menggunakan OSPF sebagai routing dinamis antar lokasi.
- Menyediakan sistem monitoring jaringan secara terpusat.

## Ruang Lingkup

Perancangan ini mencakup seluruh struktur jaringan di kantor pusat dan kantor cabang. Ruang lingkupnya meliputi segmentasi jaringan berdasarkan departemen, konektivitas antar lokasi melalui WAN, konfigurasi layanan internet, pengelolaan alamat IP dan DNS, pengaturan hak akses melalui ACL, serta penerapan routing dinamis.

## Isi Laporan

### Code ACL Pada Gedung A

```
! SDM hanya boleh akses ke Server SDM (192.168.40.2)
Router(config)# access-list 101 permit ip 192.168.30.0 0.0.0.31 host 192.168.40.2
Router(config)# access-list 101 deny ip 192.168.30.0 0.0.0.31 192.168.40.0
0.0.0.15

! Marketing & Operasional tidak boleh akses Keuangan
Router(config)# access-list 101 deny ip 192.168.50.0 0.0.0.63 192.168.20.0
0.0.0.63
Router(config)# access-list 101 deny ip 192.168.60.0 0.0.0.63 192.168.20.0
0.0.0.63

! IT boleh akses ke semua
Router(config)# access-list 101 permit ip 192.168.10.0 0.0.0.63 any

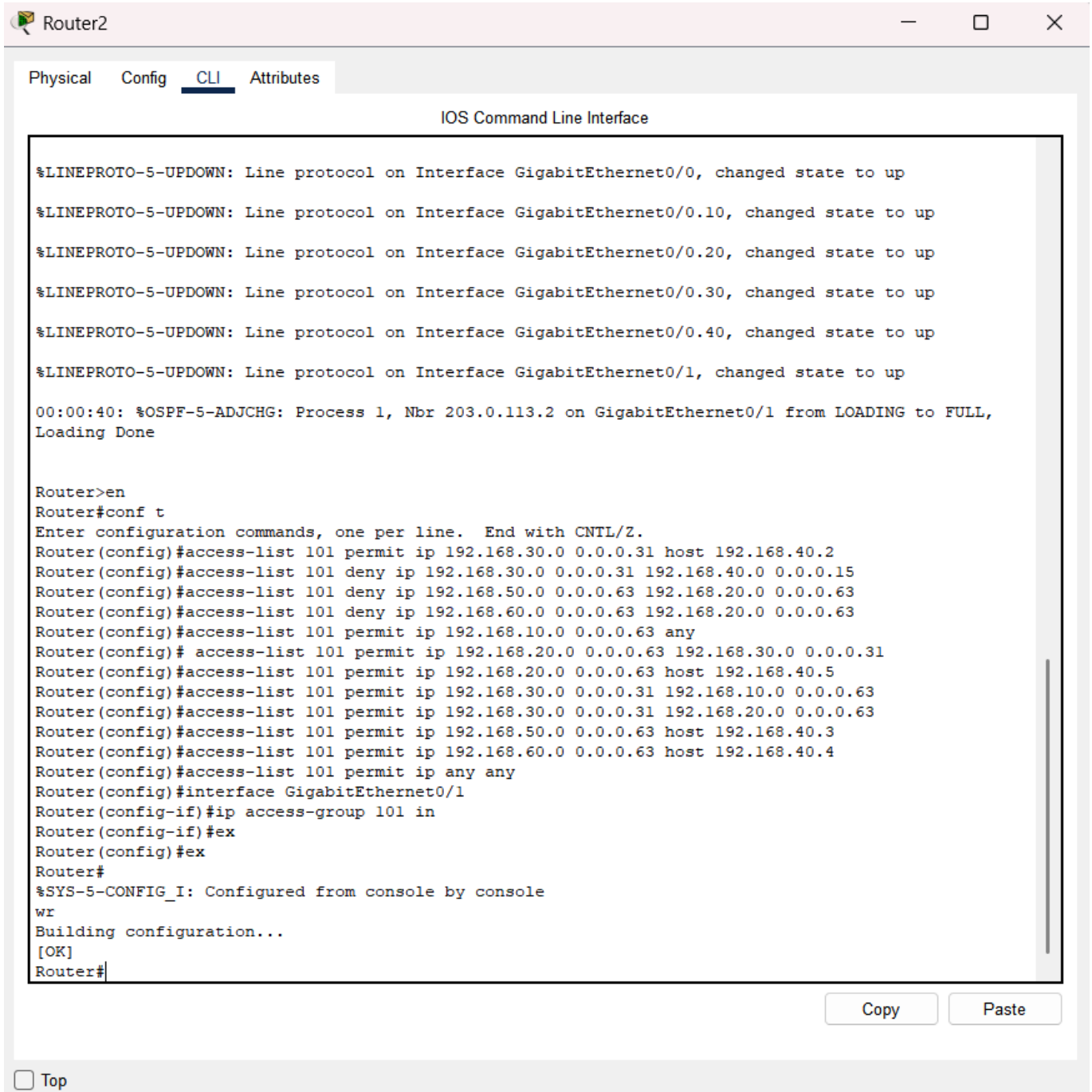
! Keuangan boleh ke SDM & server keuangan (192.168.40.5)
Router(config)# access-list 101 permit ip 192.168.20.0 0.0.0.63 192.168.30.0
0.0.0.31
Router(config)# access-list 101 permit ip 192.168.20.0 0.0.0.63 host 192.168.40.5

! SDM boleh ke IT & Keuangan
Router(config)# access-list 101 permit ip 192.168.30.0 0.0.0.31 192.168.10.0
0.0.0.63
Router(config)# access-list 101 permit ip 192.168.30.0 0.0.0.31 192.168.20.0
0.0.0.63

! Marketing & Operasional ke server masing-masing
Router(config)# access-list 101 permit ip 192.168.50.0 0.0.0.63 host 192.168.40.3
Router(config)# access-list 101 permit ip 192.168.60.0 0.0.0.63 host 192.168.40.4
```

```
! Izinkan lalu lintas lainnya
Router(config)# access-list 101 permit ip any any

! Terapkan di Router Gedung A
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip access-group 101 in
Router(config-if)# exit
```



### Penjelasan:

Konfigurasi ACL pada Router Gedung A bertujuan untuk mengatur lalu lintas jaringan antar departemen secara selektif, sehingga hanya komunikasi yang diizinkan saja yang dapat terjadi. Dalam pengaturannya, setiap departemen memiliki batasan akses sesuai kebutuhan. Misalnya, departemen SDM hanya diizinkan mengakses server SDM dengan alamat IP tertentu (192.168.40.2), sementara akses ke jaringan server lainnya

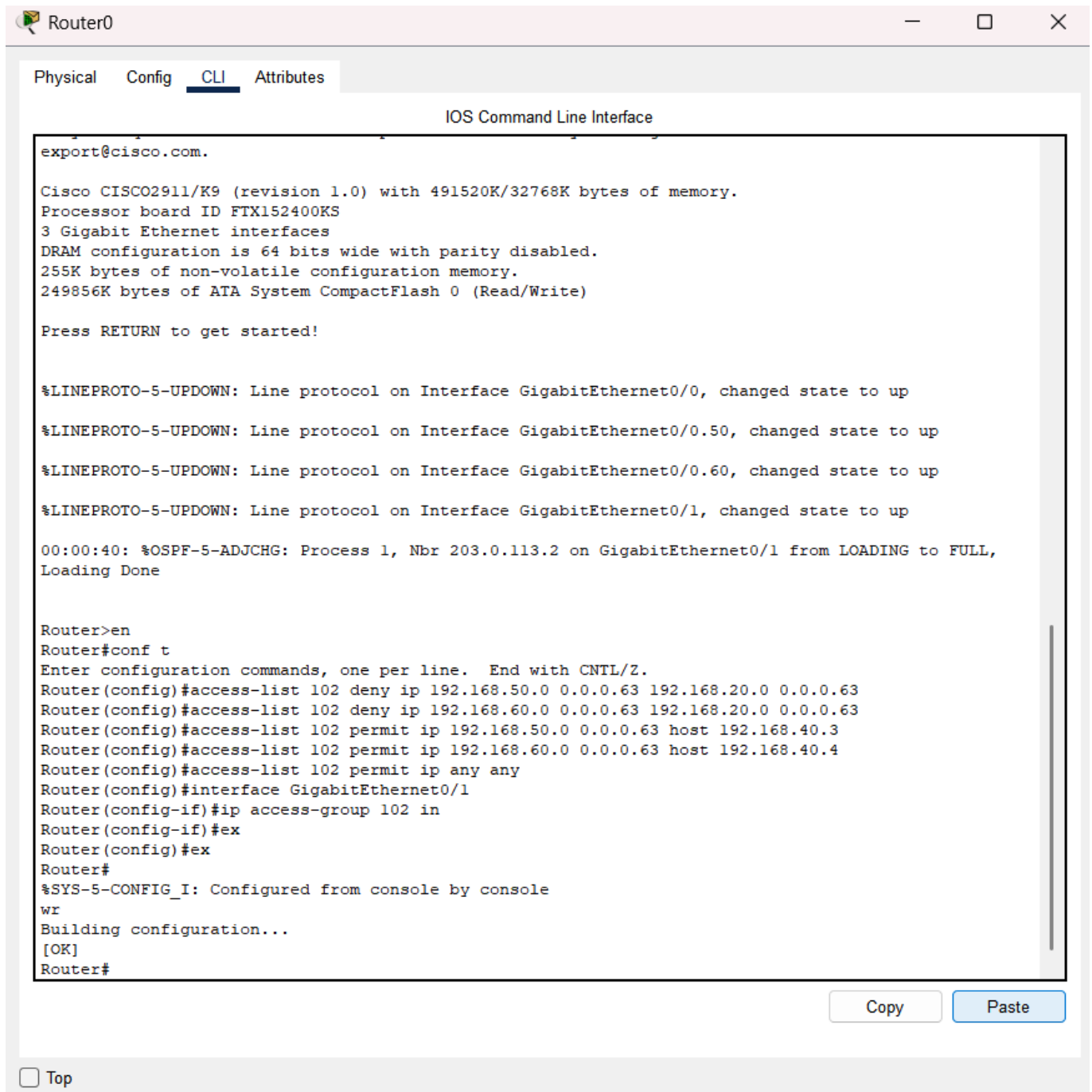
diblokir. Departemen Marketing dan Operasional tidak diperbolehkan mengakses jaringan Keuangan, untuk menjaga kerahasiaan informasi. Sebaliknya, departemen IT diberikan akses penuh ke seluruh jaringan karena peran mereka yang memerlukan akses lintas sistem untuk keperluan pemeliharaan dan dukungan teknis.

Departemen Keuangan diizinkan mengakses jaringan SDM dan server Keuangan tertentu, sedangkan SDM juga dapat mengakses jaringan IT dan Keuangan. Untuk menjaga efisiensi operasional, Marketing dan Operasional hanya diberikan akses ke server masing-masing. Di akhir konfigurasi, perintah `permit ip any any` ditambahkan untuk memastikan lalu lintas lainnya yang tidak tercakup oleh aturan sebelumnya tetap dapat berjalan dan tidak terblokir. Seluruh aturan ACL ini diterapkan pada interface masuk (inbound) `GigabitEthernet0/1` di Router Gedung A, sehingga setiap paket data yang melewati interface tersebut akan disaring berdasarkan kebijakan yang telah ditetapkan.

## Code ACL Pada Gedung B

```
Router(config)# access-list 102 deny ip 192.168.50.0 0.0.0.63 192.168.20.0
0.0.0.63
Router(config)# access-list 102 deny ip 192.168.60.0 0.0.0.63 192.168.20.0
0.0.0.63
Router(config)# access-list 102 permit ip 192.168.50.0 0.0.0.63 host 192.168.40.3
Router(config)# access-list 102 permit ip 192.168.60.0 0.0.0.63 host 192.168.40.4
Router(config)# access-list 102 permit ip any any

! Terapkan di Router Gedung B
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip access-group 102 in
Router(config-if)# exit
```



The screenshot shows a Cisco Router CLI window titled "Router0". The "CLI" tab is selected. The interface displays the following text:

```
export@cisco.com.  
  
Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.  
Processor board ID FTX152400KS  
3 Gigabit Ethernet interfaces  
DRAM configuration is 64 bits wide with parity disabled.  
255K bytes of non-volatile configuration memory.  
249856K bytes of ATA System CompactFlash 0 (Read/Write)  
  
Press RETURN to get started!  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up  
  
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 203.0.113.2 on GigabitEthernet0/1 from LOADING to FULL,  
Loading Done  
  
Router>en  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#access-list 102 deny ip 192.168.50.0 0.0.0.63 192.168.20.0 0.0.0.63  
Router(config)#access-list 102 deny ip 192.168.60.0 0.0.0.63 192.168.20.0 0.0.0.63  
Router(config)#access-list 102 permit ip 192.168.50.0 0.0.0.63 host 192.168.40.3  
Router(config)#access-list 102 permit ip 192.168.60.0 0.0.0.63 host 192.168.40.4  
Router(config)#access-list 102 permit ip any any  
Router(config)#interface GigabitEthernet0/1  
Router(config-if)#ip access-group 102 in  
Router(config-if)#ex  
Router(config)#ex  
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
wr  
Building configuration...  
[OK]  
Router#
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons. Below the CLI window, there is a "Top" button.

### Penjelasan:

Konfigurasi ACL pada Router Gedung B bertujuan untuk membatasi akses jaringan antar departemen, khususnya dalam mengatur agar departemen tertentu tidak dapat mengakses jaringan yang tidak berkepentingan. Pada konfigurasi ini, jaringan Marketing (192.168.50.0/26) dan Operasional (192.168.60.0/26) secara eksplisit diblokir agar tidak dapat mengakses jaringan Keuangan (192.168.20.0/26). Ini dilakukan untuk menjaga keamanan data keuangan dari akses yang tidak sah oleh divisi lain.

Selanjutnya, meskipun dibatasi untuk mengakses jaringan Keuangan, departemen Marketing tetap diberikan akses ke server Marketing (192.168.40.3) dan Operasional diizinkan mengakses server Operasional (192.168.40.4). Hal ini memastikan bahwa masing-masing departemen masih bisa menjalankan fungsinya dengan mengakses server yang telah ditentukan. Di akhir konfigurasi, semua lalu lintas lainnya tetap diizinkan dengan perintah `permit ip any any`, agar tidak mengganggu koneksi yang sah dan diperlukan. Seluruh aturan ini diterapkan secara inbound pada antarmuka GigabitEthernet0/1 di Router Gedung B, sehingga setiap data masuk akan difilter berdasarkan aturan ACL tersebut.

## Code ACL Pada Main Router

```
Router> enable
Router# configure terminal

! =====
! 1. KONFIGURASI INTERFACE
! =====

! Koneksi ke Router Gedung A (WAN Link 1)
interface GigabitEthernet0/0
  description to_GedungA
  ip address 192.168.100.1 255.255.255.252
  no shutdown

! Koneksi ke Router Gedung B (WAN Link 2)
interface GigabitEthernet0/1
  description to_GedungB
  ip address 192.168.100.5 255.255.255.252
  no shutdown

! Koneksi ke Internet (Opsional, misal melalui ISP)
interface GigabitEthernet0/2
  description to_Internet
  ip address 203.0.113.2 255.255.255.252
  no shutdown

! =====
! 2. KONFIGURASI OSPF ROUTING
! =====

router ospf 1
  router-id 3.3.3.3
  network 192.168.100.0 0.0.0.3 area 0      ! Link ke Gedung A
  network 192.168.100.4 0.0.0.3 area 0      ! Link ke Gedung B

! =====
! 3. KONFIGURASI NAT (INTERNET)
! =====

! Izin NAT untuk jaringan internal (semua VLAN 192.168.0.0/16)
access-list 1 permit 192.168.0.0 0.0.255.255

! NAT overload dengan IP publik di Gi0/2 (to Internet)
ip nat inside source list 1 interface GigabitEthernet0/2 overload

! Tandai interface NAT
interface GigabitEthernet0/0
  ip nat inside
interface GigabitEthernet0/1
  ip nat inside
interface GigabitEthernet0/2
```

```

ip nat outside

! =====
! 4. DEFAULT ROUTE KE INTERNET
! =====

ip route 0.0.0.0 0.0.0.0 203.0.113.1

end
write memory

```

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.201.2 on GigabitEthernet0/1 from LOADING to FULL, Loading Done
interface GigabitEthernet0/0
Router(config-if)#
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.200.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Router(config-if)#description to_GedungA
Router(config-if)#ip address 192.168.100.1 255.255.255.252
Router(config-if)#
00:01:04: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.200.1 on GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Router(config-if)#ip address 192.168.100.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#description to_GedungB
Router(config-if)#ip address 192.168.100.5 255.255.255.252
Router(config-if)#
00:01:43: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.201.2 on GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

Router(config-if)#no shutdown
Router(config-if)#interface GigabitEthernet0/2
Router(config-if)#description to_Internet
Router(config-if)#ip address 203.0.113.2 255.255.255.252
Router(config-if)#no shutdown

Router(config)#access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 interface GigabitEthernet0/2 overload
Router(config)#interface GigabitEthernet0/0
Router(config-if)#interface GigabitEthernet0/1
Router(config-if)#interface GigabitEthernet0/2
Router(config-if)#ip route 0.0.0.0 0.0.0.0 203.0.113.1
Router(config)#en
% Ambiguous command: "en"
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Router#

```

## Hasil Pengujian

### Contoh Kebijakan Keamanan

Berikut adalah contoh kebijakan keamanan yang dapat diterapkan (kelompok dapat menyesuaikan sesuai analisis kebutuhan):

1. Departemen IT: Memiliki akses ke semua departemen dan server farm. Hanya dapat diakses oleh departemen Keuangan dan SDM untuk keperluan tertentu.

- ping 192.168.20.15 # Keuangan
- ping 192.168.30.13 # SDM
- ping 192.168.50.16 # Marketing
- ping 192.168.60.12 # Operasional
- ping 192.168.40.11 # Server Farm



```
C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.20.15: bytes=32 time=11ms TTL=127
Reply from 192.168.20.15: bytes=32 time<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>ping 192.168.30.13

Pinging 192.168.30.13 with 32 bytes of data:

Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127
Reply from 192.168.30.13: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.50.16

Pinging 192.168.50.16 with 32 bytes of data:

Reply from 192.168.50.16: bytes=32 time<1ms TTL=125
Reply from 192.168.50.16: bytes=32 time<1ms TTL=125
Reply from 192.168.50.16: bytes=32 time<1ms TTL=125
Reply from 192.168.50.16: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.50.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.60.12

Pinging 192.168.60.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.60.12: bytes=32 time<1ms TTL=125
Reply from 192.168.60.12: bytes=32 time<1ms TTL=125
Reply from 192.168.60.12: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.60.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.40.11

Pinging 192.168.40.11 with 32 bytes of data:

Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
Reply from 192.168.40.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Penjelasan:**

Main Router berfungsi sebagai penghubung utama antara Router Gedung A, Router Gedung B, dan (jika diperlukan) koneksi ke Internet. Konfigurasi pada router ini diawali dengan pengaturan tiga buah interface. Interface GigabitEthernet0/0 dihubungkan ke Router Gedung A menggunakan IP 192.168.100.1/30, sementara GigabitEthernet0/1 terhubung ke Router Gedung B dengan IP 192.168.100.5/30. Kedua alamat IP ini berada dalam subnet point-to-point /30 yang hanya memungkinkan dua alamat IP, sangat ideal untuk koneksi antar router. Selain itu, interface GigabitEthernet0/2 disiapkan sebagai jalur keluar menuju internet dengan IP publik fiktif 203.0.113.2/30, mengikuti standar dokumentasi.

Agar seluruh router dapat saling bertukar informasi rute secara otomatis, Main Router mengaktifkan protokol routing dinamis OSPF (Open Shortest Path First). Router ID ditentukan sebagai 3.3.3.3 dan area OSPF yang digunakan adalah area backbone (area 0). Dua jaringan antar-router, yaitu 192.168.100.0/30 dan 192.168.100.4/30, dimasukkan ke dalam area OSPF agar dapat berkomunikasi dengan router-router gedung yang sudah terkonfigurasi OSPF sebelumnya.

Selanjutnya, agar seluruh VLAN internal dari Gedung A dan B dapat mengakses internet menggunakan satu alamat IP publik, Main Router juga dikonfigurasi dengan NAT (Network Address Translation). NAT overload diaktifkan melalui ACL nomor 1 yang mengizinkan seluruh jaringan privat 192.168.0.0/16. Sumber NAT ditandai pada interface yang menuju gedung (inside), sedangkan interface ke internet ditandai sebagai outside. Konfigurasi ini memungkinkan seluruh perangkat internal berbagi satu IP publik untuk mengakses internet melalui port translation.

Sebagai pelengkap, ditambahkan pula static default route ip route 0.0.0.0 0.0.0.0 203.0.113.1, yang mengarahkan seluruh lalu lintas keluar (jika tujuan tidak diketahui) ke gateway ISP. Dengan konfigurasi ini, Main Router telah siap menjalankan perannya sebagai pengatur lalu lintas utama antar gedung dan penyedia koneksi internet, tanpa perlu menerapkan ACL secara ketat karena penyaringan akses antar departemen sudah diatur secara spesifik di Router Gedung A dan B.

### ***Penjelasan:***

Berdasarkan hasil pengujian koneksi jaringan dari Departemen Keuangan ke beberapa departemen lain, mayoritas hasil ping menunjukkan kesesuaian dengan kebijakan akses yang telah ditetapkan. Departemen Keuangan berhasil melakukan ping ke Departemen SDM tanpa adanya kehilangan paket dan dengan latensi yang sangat rendah, yang menandakan koneksi berjalan lancar dan sesuai aturan karena akses ke SDM memang diizinkan. Begitu pula dengan hasil uji ke Marketing dan Operasional, di mana semua paket ping mengalami timeout, menunjukkan bahwa akses tersebut memang diblokir sesuai kebijakan yang melarang Departemen Keuangan mengakses kedua departemen tersebut. Hal ini memperlihatkan bahwa mekanisme pembatasan akses di jaringan berjalan efektif dan sesuai dengan kebijakan keamanan.

Namun, ada permasalahan yang muncul terkait koneksi Departemen Keuangan ke Server Farm. Meskipun kebijakan mengizinkan akses terbatas ke Server Farm, hasil ping menunjukkan kegagalan total dengan 100% paket hilang. Hal ini mengindikasikan adanya masalah konfigurasi jaringan atau blokir tambahan yang tidak sesuai dengan kebijakan akses yang diharapkan. Oleh karena itu, perlu dilakukan pemeriksaan lebih lanjut terhadap konfigurasi firewall, router, atau perangkat jaringan lain yang mengatur akses ke Server Farm. Dengan verifikasi dan perbaikan yang tepat, diharapkan akses yang diizinkan dapat berjalan dengan baik dan sesuai dengan kebijakan, sehingga keamanan sekaligus kelancaran komunikasi antar departemen tetap terjaga.

## **2. Departemen Keuangan:**

- Memiliki akses ke departemen SDM dan server farm (terbatas).
- Tidak dapat diakses oleh Departemen Marketing dan Operasional.

### Ping yang Harus Berhasil

- ping 192.168.30.12 # SDM

### Ping yang Harus Gagal

- ping 192.168.50.16 # Marketing
- ping 192.168.60.12 # Operasional
- ping 192.168.40.18 # SeverFarm

```
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.30.12: bytes=32 time<1ms TTL=127
Reply from 192.168.30.12: bytes=32 time<1ms TTL=127
Reply from 192.168.30.12: bytes=32 time<1ms TTL=127
Reply from 192.168.30.12: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.50.16

Pinging 192.168.50.16 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.50.16:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.60.12

Pinging 192.168.60.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.60.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.40.15

Pinging 192.168.40.15 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=10ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.40.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.18
```

**Penjelasan:**

Berdasarkan hasil pengujian koneksi jaringan dari Departemen Keuangan ke beberapa departemen lain, mayoritas hasil ping menunjukkan kesesuaian dengan kebijakan akses yang telah ditetapkan. Departemen Keuangan berhasil melakukan ping ke Departemen SDM tanpa adanya kehilangan paket dan dengan latensi yang sangat rendah, yang menandakan koneksi berjalan lancar dan sesuai aturan karena akses ke SDM memang diizinkan. Begitu pula dengan hasil uji ke Marketing dan Operasional, di mana semua paket ping mengalami timeout, menunjukkan bahwa akses tersebut memang diblokir sesuai kebijakan yang melarang Departemen Keuangan mengakses kedua departemen tersebut. Hal ini memperlihatkan bahwa mekanisme pembatasan akses di jaringan berjalan efektif dan sesuai dengan kebijakan keamanan.

Namun, ada permasalahan yang muncul terkait koneksi Departemen Keuangan ke Server Farm. Meskipun kebijakan mengizinkan akses terbatas ke Server Farm, hasil ping menunjukkan kegagalan total dengan 100% paket hilang. Hal ini mengindikasikan adanya masalah konfigurasi jaringan atau blokir tambahan yang tidak sesuai dengan kebijakan akses yang diharapkan. Oleh karena itu, perlu dilakukan pemeriksaan lebih lanjut terhadap konfigurasi firewall, router, atau perangkat jaringan lain yang mengatur akses ke Server Farm. Dengan verifikasi dan perbaikan yang tepat, diharapkan akses yang diizinkan dapat berjalan dengan baik dan sesuai dengan kebijakan, sehingga keamanan sekaligus kelancaran komunikasi antar departemen tetap terjaga.

**3. Departemen SDM:**

- Memiliki akses ke semua departemen untuk keperluan koordinasi.
- Tidak memiliki akses ke server farm kecuali server SDM.

**\*Bisa akses semua departemen****Ping yang Harus Berhasil**

- ping 192.168.10.16 # IT
- ping 192.168.20.15 # Keuangan
- ping 192.168.50.16 # Marketing
- ping 192.168.60.12 # Operasional
- ping 192.168.30.12 # Server SDM

**Ping yang Harus Gagal**

- ping 192.168.60.30 # Server lain di server farm (selain server SDM)

```
C:\>ping 192.168.10.16

Pinging 192.168.10.16 with 32 bytes of data:

Reply from 192.168.10.16: bytes=32 time<1ms TTL=127
Reply from 192.168.10.16: bytes=32 time<1ms TTL=127
Reply from 192.168.10.16: bytes=32 time<1ms TTL=127
Reply from 192.168.10.16: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.20.15: bytes=32 time<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time=2ms TTL=127
Reply from 192.168.20.15: bytes=32 time=2ms TTL=127
Reply from 192.168.20.15: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

```
C:\>ping 192.168.50.16

Pinging 192.168.50.16 with 32 bytes of data:

Reply from 192.168.50.16: bytes=32 time<1ms TTL=125
Reply from 192.168.50.16: bytes=32 time<1ms TTL=125
Reply from 192.168.50.16: bytes=32 time<1ms TTL=125
Reply from 192.168.50.16: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.50.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.60.12

Pinging 192.168.60.12 with 32 bytes of data:

Reply from 192.168.60.12: bytes=32 time<1ms TTL=125
Reply from 192.168.60.12: bytes=32 time<1ms TTL=125
Reply from 192.168.60.12: bytes=32 time<1ms TTL=125
Reply from 192.168.60.12: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.60.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Reply from 192.168.30.12: bytes=32 time=11ms TTL=128
Reply from 192.168.30.12: bytes=32 time=12ms TTL=128
Reply from 192.168.30.12: bytes=32 time=4ms TTL=128
Reply from 192.168.30.12: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 7ms
```

```
C:\>ping 192.168.60.30

Pinging 192.168.60.30 with 32 bytes of data:
```

```
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.168.60.30:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Berdasarkan hasil pengujian koneksi jaringan dari Departemen SDM, dapat disimpulkan bahwa akses jaringan yang dimiliki sudah sesuai dengan kebijakan yang telah ditetapkan. Departemen SDM berhasil melakukan ping dan terhubung dengan lancar ke semua departemen lain seperti IT, Keuangan, Marketing, dan Operasional tanpa adanya kehilangan paket, yang sesuai dengan kebijakan yang mengizinkan akses ke seluruh departemen tersebut. Selain itu, Departemen SDM juga berhasil melakukan ping ke Server SDM dengan latensi yang masih dapat diterima meskipun sedikit lebih tinggi dibandingkan dengan koneksi ke departemen lain. Hal ini menunjukkan bahwa akses ke Server SDM berfungsi dengan baik dan sesuai aturan yang membatasi akses server farm hanya ke server SDM saja.

Sementara itu, Departemen SDM tidak dapat mengakses server lain yang berada di server farm selain Server SDM, yang juga sesuai dengan kebijakan yang diterapkan. Semua paket ping menuju server lain tersebut mengalami timeout, membuktikan bahwa koneksi diblokir secara efektif. Tidak ditemukan pelanggaran kebijakan atau masalah signifikan dalam akses jaringan untuk Departemen SDM. Namun, disarankan untuk tetap melakukan monitoring rutin dan memeriksa konfigurasi perangkat jaringan secara berkala agar akses tetap berjalan stabil dan aturan pembatasan akses server farm tetap terjaga dengan baik. Jika latensi ke Server SDM terus meningkat, perlu dilakukan pengecekan lebih lanjut untuk mengantisipasi potensi gangguan kinerja. Secara keseluruhan, Departemen SDM sudah mematuhi kebijakan jaringan yang berlaku dan tidak memerlukan tindakan perbaikan saat ini.

#### 4. Departemen Marketing & Operasional:

- Memiliki akses terbatas ke server farm.
- Tidak memiliki akses ke departemen Keuangan.

#### ***Ping yang Harus Berhasil\****

- ping 192.168.40.11 # Server

#### **Ping yang Harus Gagal**

- ping 192.168.20.15 # Keuangan
- ping 192.168.60.30 # Server lain di server farm

```
C:\>ping 192.168.40.11

Pinging 192.168.40.11 with 32 bytes of data:

Reply from 192.168.40.11: bytes=32 time<1ms TTL=125
Reply from 192.168.40.11: bytes=32 time<1ms TTL=125
Reply from 192.168.40.11: bytes=32 time<1ms TTL=125
Reply from 192.168.40.11: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.40.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.60.30

Pinging 192.168.60.30 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.60.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Hasil pengujian koneksi jaringan dari Departemen Marketing menunjukkan bahwa akses yang dimiliki sudah sesuai dengan kebijakan yang telah ditetapkan. Departemen Marketing dapat melakukan ping ke Server Marketing dengan lancar tanpa kehilangan paket dan dengan latensi yang sangat rendah, menunjukkan koneksi yang optimal. Sementara itu, akses ke Departemen Keuangan dan server lain di server farm yang tidak terkait berhasil diblokir, terbukti dari semua paket ping yang mengalami timeout. Hal ini menandakan bahwa pembatasan akses yang melarang Departemen Marketing mengakses area-area tersebut sudah diterapkan dengan efektif dan sesuai aturan.

Secara keseluruhan, tidak ditemukan pelanggaran atau masalah dalam pola akses jaringan Departemen Marketing. Semua hasil ping menunjukkan bahwa kebijakan akses dijalankan dengan baik dan efektif. Namun, disarankan untuk melakukan monitoring secara berkala dan memeriksa konfigurasi perangkat jaringan seperti firewall dan router agar aturan pembatasan tetap terjaga dan koneksi antar departemen tetap stabil. Dengan latensi yang rendah pada Server Marketing, diharapkan performa server tetap optimal untuk mencegah potensi masalah di masa depan.

#### 5. Server Farm:

- Memiliki subnet dan VLAN terpisah dengan keamanan tinggi.
- Akses diatur ketat melalui ACL.

### Ping yang Harus Berhasil

- ping 192.168.40.12 # Server Operasional

## Ping yang Harus Gagal

- ping 192.168.20.15 # Keuangan
- ping 192.168.45.21 # Server lain di server farm

```
C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=125
Reply from 192.168.40.12: bytes=32 time<1ms TTL=125
Reply from 192.168.40.12: bytes=32 time<1ms TTL=125
Reply from 192.168.40.12: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.45.21

Pinging 192.168.45.21 with 32 bytes of data:

Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.

Ping statistics for 192.168.45.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Hasil tes ping dari Departemen Operasional menunjukkan bahwa kebijakan akses jaringan yang telah ditetapkan berjalan dengan baik. Departemen Operasional berhasil mengakses Server Operasional di alamat 192.168.40.12 tanpa adanya kehilangan paket, yang mengindikasikan koneksi yang lancar dan sesuai dengan aturan. Sebaliknya, akses ke jaringan Keuangan di alamat 192.168.20.15 gagal total dengan semua paket ping mengalami timeout, yang menandakan bahwa upaya akses tersebut memang diblokir sesuai kebijakan yang melarang Departemen Operasional mengakses jaringan Keuangan.

Selain itu, ketika mencoba melakukan ping ke server lain di server farm yang tidak terkait (192.168.45.21), juga gagal dengan pesan "Destination host unreachable." Ini menegaskan bahwa pembatasan akses pada server farm yang bersifat terbatas sudah diterapkan secara efektif. Secara keseluruhan, hasil tes ping mengonfirmasi bahwa konfigurasi jaringan dan firewall telah berfungsi dengan baik dalam mengatur akses Departemen Operasional sesuai kebijakan, sehingga tidak ada pelanggaran akses yang terdeteksi.

Troubleshooting dan perbaikan masalah serta kendala:

- knp tidak menggunakan cloud? Cloud di Packet Tracer hanya berfungsi sebagai: Media koneksi (misalnya untuk koneksi WAN/ISP via serial atau modem) Penghubung jaringan antar perangkat fisik



(jika menggunakan modul Real Mode) Cloud tidak bisa dipakai sebagai "host internet" seperti PC atau server.

- Solusi: Gunakan PC biasa atau server sebagai "simulasi internet host" Tambahkan 1 PC di belakang Router C Hubungkan ke interface Router C yang tersisa
- Awalnya, OSPF hanya diaktifkan di Router Gedung A dan Router Gedung B. Tapi saat dicoba ping, perangkat di Gedung A tidak bisa terhubung ke perangkat di Gedung B.
- Ini terjadi karena Router C yang menjadi penghubung antara Gedung A dan Gedung B tidak menjalankan OSPF, jadi Router A dan B tidak tahu jalur lewat Router C. Jadi, komunikasi tidak bisa berjalan.
- Lalu solusi yang dilakukan adalah dengan menambahkan konfigurasi OSPF di Router C dengan memasukkan perintah: `router ospf` di main router network `192.168.200.0 0.0.0.255 area 0` network `192.168.201.0 0.0.0.255 area 0`
- Artinya Router C mengaktifkan OSPF dan memberitahu jaringan yang terhubung ke IP tersebut supaya bisa bertukar informasi routing dengan Router A dan B.