

# [Finalisasi Dokumentasi & Presentasi] - [Pekan 15]

---

## Anggota Kelompok dan Peran

- Muhammad Novri Aziztra (10231066) - Network Architect
- Zahwa Hanna Dwi Putri (10231092) - Network Engineer
- Indah Nur Fortuna (10231044) - Network Services Specialist
- Putri Rahmawati (10231074) - Security & Documentation Specialist

## Daftar Isi

1. Pendahuluan
2. Isi Laporan
3. Konfigurasi Perangkat
4. Screenshot dan Hasil Pengujian
5. Kendala dan Solusi
6. Kesimpulan

## Pendahuluan

### Latar Belakang

Dalam era transformasi digital saat ini, kebutuhan akan infrastruktur jaringan komputer yang handal, aman, dan terkelola dengan baik menjadi fondasi utama dalam mendukung kinerja organisasi, khususnya di sektor teknologi informasi. Kondisi ideal yang diharapkan adalah terciptanya sistem jaringan enterprise yang mampu mengakomodasi kebutuhan komunikasi data secara efisien antar departemen dan lokasi kerja, dengan pengelolaan lalu lintas yang terstruktur, penggunaan alamat IP yang tepat, serta layanan jaringan yang berjalan optimal. Selain itu, sebuah jaringan yang ideal juga mampu memberikan dukungan terhadap pertumbuhan organisasi, menjamin kecepatan akses informasi, serta mendukung mobilitas kerja lintas lokasi dengan tetap mempertahankan keamanan data internal. Dengan demikian, infrastruktur jaringan bukan hanya sebagai sarana pendukung, tetapi juga menjadi aset strategis yang menentukan keberlangsungan dan keunggulan kompetitif perusahaan.

Namun, dalam kenyataan di lapangan, banyak organisasi masih menghadapi kendala dalam membangun dan mengelola jaringan komputer yang memenuhi kriteria tersebut. Permasalahan seperti kurangnya segmentasi jaringan, konfigurasi IP yang tidak efisien, serta minimnya mekanisme keamanan antar divisi, menjadi penyebab utama turunnya performa sistem dan meningkatnya risiko gangguan. Salah satu contoh nyata dapat dilihat pada PT. Nusantara Network, sebuah perusahaan yang bergerak di bidang teknologi informasi dan memiliki dua lokasi operasional: kantor pusat dan kantor cabang. Di setiap lokasi, terdapat beberapa departemen dengan kebutuhan komunikasi data yang berbeda-beda. Belum adanya pemisahan VLAN antar departemen, belum diterapkannya layanan DHCP, DNS, serta tidak adanya sistem keamanan berbasis ACL, menjadi tantangan yang harus segera diatasi. Kondisi ini menunjukkan adanya kesenjangan antara harapan dan realitas yang mengharuskan adanya desain ulang jaringan yang menyeluruh dan sistematis.

Melihat kondisi tersebut, penyusunan proyek perancangan jaringan enterprise ini menjadi sangat penting untuk dilakukan sebagai bentuk upaya pengembangan solusi konkret atas permasalahan yang ada. Proyek ini juga merupakan bagian dari kegiatan praktikum Desain dan Manajemen Jaringan Komputer, yang bertujuan untuk mengintegrasikan seluruh konsep yang telah dipelajari selama perkuliahan ke dalam sebuah studi kasus nyata. Mahasiswa dituntut untuk mampu merancang topologi jaringan, melakukan subnetting, mengelola VLAN, menerapkan routing dinamis (OSPF), serta mengimplementasikan layanan DHCP, DNS, dan NAT, sekaligus menyusun kebijakan keamanan jaringan melalui Access Control List (ACL). Pendekatan ini tidak hanya melatih kemampuan teknis, tetapi juga meningkatkan keterampilan analisis, pemecahan masalah, dan kerja kolaboratif melalui metode Project Based Learning (PBL). Oleh karena itu, melalui makalah ini, diharapkan dapat tersusun sebuah rancangan jaringan enterprise yang optimal, aman, dan sesuai dengan kebutuhan operasional PT. Nusantara Network secara menyeluruh.

## Tujuan

Adapun tujuan dari proyek akhir ini adalah sebagai berikut:

1. Menerapkan konsep jaringan komputer secara menyeluruh dalam satu proyek komprehensif.
2. Merancang jaringan enterprise yang aman, efisien, dan sesuai kebutuhan organisasi.
3. Mengembangkan keterampilan teknis dalam konfigurasi perangkat jaringan seperti router dan switch.
4. Menerapkan layanan jaringan seperti DHCP, DNS, NAT, dan routing dinamis menggunakan OSPF.
5. Menyusun kebijakan keamanan menggunakan ACL untuk membatasi akses antar departemen.
6. Meningkatkan kemampuan bekerja dalam tim serta menyusun dokumentasi teknis yang baik.
7. Menyajikan hasil proyek melalui presentasi yang informatif dan profesional.

## Ruang Lingkup

Ruang lingkup proyek ini merupakan batasan hal-hal yang akan dikerjakan oleh penyusun dalam merancang dan mengimplementasikan jaringan enterprise untuk PT. Nusantara Network. Ruang lingkup ini bertujuan agar fokus pekerjaan tetap berada pada aspek-aspek penting yang relevan dengan tujuan proyek dan tidak meluas ke luar konteks permasalahan. Adapun ruang lingkup proyek meliputi:

1. Perancangan topologi jaringan fisik dan logis pada dua lokasi (kantor pusat dan kantor cabang).
2. Pembagian subnet dan pengalaman IP berdasarkan jumlah host pada tiap departemen.
3. Konfigurasi VLAN untuk pemisahan jaringan antar departemen.
4. Implementasi routing dinamis (OSPF) untuk konektivitas antar gedung.
5. Penerapan layanan jaringan, seperti DHCP, DNS, dan NAT.
6. Pengaturan keamanan jaringan menggunakan Access Control List (ACL) sesuai kebijakan akses.
7. Monitoring jaringan secara terpusat untuk mengawasi performa dan keamanan.
8. Dokumentasi dan presentasi hasil proyek sebagai bentuk pertanggungjawaban akhir.

## Isi Laporan

### [Perencanaan Proyek & Desain Awal] - [Pekan 9]

#### **Analisis Kebutuhan Jaringan**

PT. Nusantara Network memiliki dua lokasi yaitu Kantor Pusat (Gedung A) dengan Departemen IT, Keuangan, SDM, dan Server Farm, serta Kantor Cabang (Gedung B) dengan Departemen Marketing dan Operasional. Berikut rincian kebutuhan:

## **Struktur Organisasi dan Perangkat**

Kantor Pusat (Gedung A):

- Departemen IT:
  - PC: 30 unit
  - Switch: 2 unit (Cisco Switch 2960)
  - Router: 1 unit (Cisco Router 2911)
  - VLAN: 10 (192.168.10.0/26)
- Departemen Keuangan
  - PC: 25 unit
  - Switch: 2 unit (Cisco Switch 2960)
  - Router: 1 unit (Cisco Router 2911)
  - VLAN: 20 (192.168.20.0/27)
- Departemen SDM:
  - PC: 20 unit
  - Switch: 1 unit (Cisco Switch 2960)
  - Router: 1 unit (Cisco Router 2911)
  - VLAN: 30 (192.168.30.0/27)
- Server Farm:
  - Server: 10 unit (Generic Server)
  - Switch: 2 unit (Cisco Switch 2960)
  - Router: 1 unit (Cisco Router 1941)
  - Firewall: 2 unit (ASA 5505)
  - VLAN: 40 (192.168.40.0/28)

Kantor Cabang (Gedung B):

- Departemen Marketing:
  - PC: 30 unit
  - Switch: 2 unit (Cisco Switch 2960)
  - Router: 1 unit (Cisco Router 2911)
  - VLAN: 50 (192.168.50.0/26)
- Departemen Operasional:
  - PC: 35 unit
  - Switch: 3 unit (Cisco Switch 2960)
  - Router: 1 unit (Cisco Router 2911)
  - VLAN: 60 (192.168.60.0/26)

## **Jenis Kabel**

- Straight-Through Cable: Untuk koneksi antar perangkat berbeda (misalnya, PC ke switch, switch ke router).

- Cross-OVER Cable: Untuk koneksi antar perangkat sejenis (misalnya, switch ke switch, router ke router).

## Koneksi Antar Gedung

Koneksi antar Gedung A dan Gedung B menggunakan teknologi WAN dengan bandwidth terbatas. Prioritas diberikan pada trafik penting seperti data server dan komunikasi antar departemen.

## Routing Dinamis

Routing dinamis dengan OSPF digunakan untuk manajemen rute yang efisien, memungkinkan router mengenali VLAN secara otomatis dan menyesuaikan rute saat terjadi perubahan.

## Layanan Jaringan

- DHCP: Mengalokasikan IP secara otomatis untuk setiap VLAN.
- NAT: Memungkinkan perangkat internal mengakses internet menggunakan satu IP publik dari ISP.
- DNS: DNS internal untuk domain lokal, dengan forwarding ke DNS eksternal untuk akses internet.

## Keamanan

ACL diterapkan untuk membatasi akses antar departemen, misalnya:

- VLAN Keuangan tidak dapat mengakses VLAN IT.
- Server Farm hanya dapat diakses oleh VLAN IT.
- VLAN Operasional memiliki akses terbatas ke VLAN lain.

## Timeline Proyek

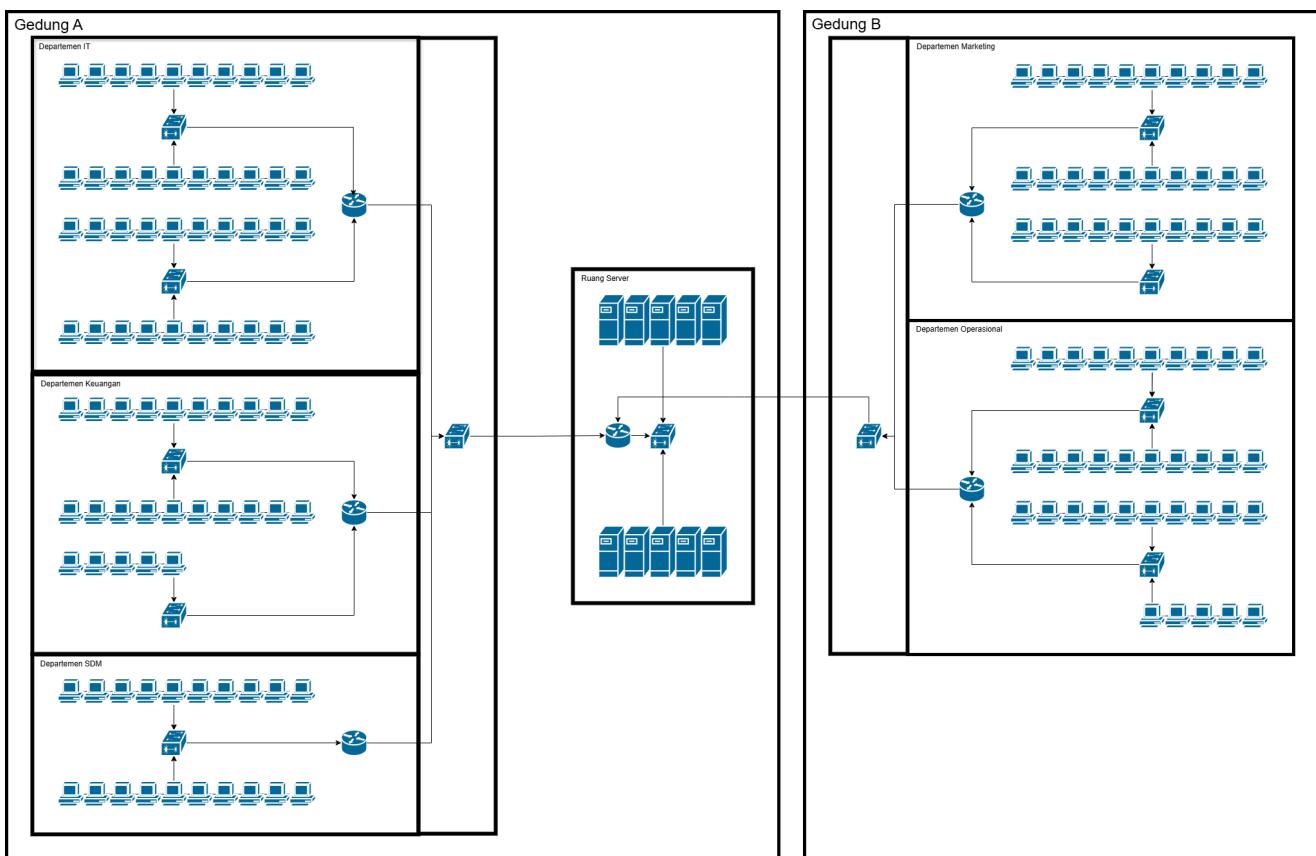
Pekan	Aktivitas	Tenggat Waktu
9	Perencanaan Proyek & Desain Awal	12 April 2025
10	Desain Topologi & Skema Pengalamatan	17 April 2025
11	Implementasi Topologi Dasar & VLAN	24 April 2025
12	Implementasi Routing & WAN	1 Mei 2025
13	Implementasi Layanan Jaringan	8 Mei 2025
14	Implementasi Keamanan & Pengujian	15 Mei 2025
15	Finalisasi Dokumentasi & Presentasi	22 Mei 2025

Timeline Proyek PT. Nusantara Network

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AX	AZ	BA	BC	BD
1																																																				
2	Pekan																																																			
3		Kegiatan																																																		
4																																																				
5	9	Perencanaan Projek & Desain Awal	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30																												
6	10	Desain Topologi & Skema Pengalaman																																																		
7	11	Implementasi Topologi Dasar & VLAN																																																		
8	12	Implementasi Routing & WAN																																																		
9	13	Implementasi Layanan Jaringan																																																		
10	14	Implementasi Keamanan & Pengujian																																																		
11	15	Finalisasi Dokumentasi & Presentasi																																																		
12	Keterangan																																																			
13		Deadline																																																		
14		Sudah Berproses																																																		
15		Diskusi Kelompok																																																		
16																																																				
17																																																				
18																																																				
19																																																				
20																																																				

[Link Spreadsheet Timeline Proyek](#)

## Sketsa Awal Desain Jaringan



## Penjelasan Sketsa

Sketsa awal menggambarkan infrastruktur jaringan PT. Nusantara Network dengan dua lokasi terpisah: Gedung A (Kantor Pusat) dan Gedung B (Kantor Cabang), yang dihubungkan melalui koneksi WAN.

### Gedung A (Kantor Pusat)

- Departemen IT (VLAN 10):
  - 30 PC terhubung ke 2 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 2911.
  - Subnet: 192.168.10.0/26.
- Departemen Keuangan (VLAN 20):
  - 30 PC terhubung ke 2 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 2911.
  - Subnet: 192.168.20.0/26.
- Departemen SDM (VLAN 30):
  - 30 PC terhubung ke 2 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 2911.
  - Subnet: 192.168.30.0/26.

- 25 PC terhubung ke 2 Cisco Switch 2960.
- Switch terhubung ke Cisco Router 2911.
- Subnet: 192.168.20.0/27.
- Departemen SDM (VLAN 30):
  - 20 PC terhubung ke 1 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 2911.
  - Subnet: 192.168.30.0/27.
- Server Farm (VLAN 40):
  - 10 Generic Server terhubung ke 2 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 1941.
  - Subnet: 192.168.40.0/28.

#### **Gedung B (Kantor Cabang)**

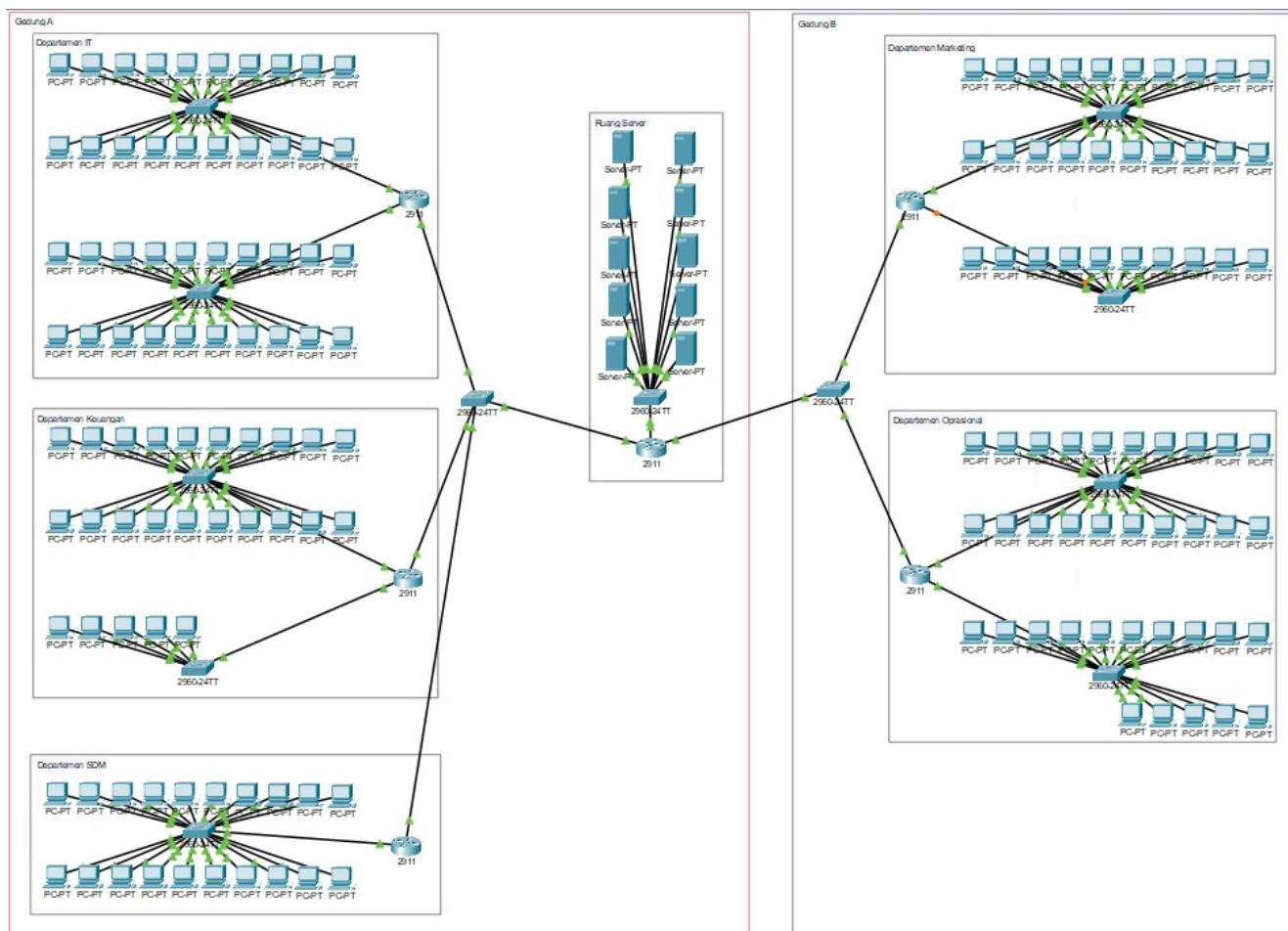
- Departemen Marketing (VLAN 50):
  - 30 PC terhubung ke 2 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 2911.
  - Subnet: 192.168.50.0/26.
- Departemen Operasional (VLAN 60):
  - 35 PC terhubung ke 3 Cisco Switch 2960.
  - Switch terhubung ke Cisco Router 2911.
  - Subnet: 192.168.60.0/26.

#### **Koneksi Antar Perangkat**

- Straight-Through Cable: Digunakan untuk menghubungkan PC ke switch dan switch ke router.
- Cross-Over Cable: Digunakan untuk menghubungkan switch ke switch atau router ke router.
- Koneksi WAN menghubungkan router di Gedung A dan Gedung B, dengan OSPF untuk routing dinamis.

 [Desain Topologi & Skema Pengalamatan] - [Pekan 10]

#### **Diagram Topologi Fisik dan Logis**



Gambar topologi logis jaringan PT. Nusantara Network menampilkan struktur jaringan yang tersegmentasi antara dua gedung, yaitu Gedung A dan Gedung B, yang terkoneksi ke pusat data (server center) melalui sebuah router utama. Pada Gedung A terdapat tiga departemen, yakni IT, Keuangan, dan SDM. Masing-masing departemen memiliki dua buah switch Cisco 2960 yang menghubungkan puluhan PC sebagai perangkat end-user. Switch-switch ini kemudian terkoneksi ke satu switch pusat (core switch) di Gedung A, yang selanjutnya terhubung ke router Cisco 2911 di tengah jaringan. Hal yang serupa juga diterapkan pada Gedung B, yang menaungi Departemen Marketing dan Operasional. Masing-masing departemen di Gedung B juga menggunakan dua switch access yang terhubung ke switch pusat Gedung B, lalu dilanjutkan ke router utama.

Di bagian tengah jaringan terdapat ruang server (server farm) yang berisi beberapa perangkat server yang terhubung ke switch khusus. Switch ini kemudian dihubungkan langsung ke router pusat yang juga menjadi simpul utama dalam proses routing antar VLAN. Setiap departemen dikelompokkan ke dalam VLAN yang berbeda untuk menjaga segmentasi dan keamanan data, seperti VLAN 10 untuk IT, VLAN 20 untuk Keuangan, VLAN 30 untuk SDM, VLAN 40 untuk Server Farm, VLAN 50 untuk Marketing, dan VLAN 60 untuk Operasional. Untuk komunikasi antar switch, digunakan VLAN 99 sebagai native VLAN pada port trunk. Seluruh koneksi antar switch dan router menggunakan konfigurasi trunk agar dapat membawa banyak lalu lintas VLAN secara bersamaan.

Secara keseluruhan, desain ini menerapkan model jaringan hirarkis yang terdiri dari tiga lapisan utama, yaitu access layer (yang menghubungkan PC ke switch), distribution layer (pengelompokan switch di setiap gedung), dan core layer (routing antar gedung dan server). Hubungan logis antar perangkat juga menunjukkan pemanfaatan inter-VLAN routing yang dilakukan oleh router utama melalui konfigurasi sub-interface, sehingga memungkinkan setiap departemen saling berkomunikasi meski berada di VLAN yang

berbeda. Desain ini tidak hanya menjamin efisiensi komunikasi internal, tetapi juga meningkatkan keamanan dan skalabilitas jaringan perusahaan.

**Tabel Pengalaman IP**

Departemen	Subnet	IP Range	Broadcast	Gateway	VLAN ID
IT	192.168.0.0/26	192.168.0.1 – 192.168.0.62	192.168.0.63	192.168.0.1	10
Keuangan	192.168.0.64/27	192.168.0.65 – 192.168.0.94	192.168.0.95	192.168.0.65	20
SDM	192.168.0.96/27	192.168.0.97 – 192.168.0.126	192.168.0.127	192.168.0.97	30
Server Farm	192.168.0.128/28	192.168.0.129 – 192.168.0.142	192.168.0.143	192.168.0.129	40
Marketing	192.168.0.144/26	192.168.0.145 – 192.168.0.206	192.168.0.207	192.168.0.145	50
Operasional	192.168.0.208/26	192.168.0.209 – 192.168.0.270	192.168.0.271	192.168.0.209	60
Antar Router	192.168.0.272/30	192.168.0.273 – 192.168.0.274	192.168.0.275	192.168.0.273	99

**Daftar Perangkat yang dibutuhkan**

Gedung	Departemen	PC	Switch (Jenis)	Router (Jenis)	Server (Jenis)	VLAN
Gedung A	IT	40	2 × Cisco Switch 2960	-	-	10
Gedung A	Keuangan	25	2 × Cisco Switch 2960	-	-	20
Gedung A	SDM	20	1 × Cisco Switch 2960	-	-	30
Gedung A	Server Farm	-	2 × Cisco Switch 2960	1 × Cisco Router 2911	10 × Generic Server	40
Gedung B	Marketing	30	2 × Cisco Switch 2960	-	-	50
Gedung B	Operasional	35	3 × Cisco Switch 2960	-	-	60

Jenis Kabel	Pengertian	Fungsi Utama
Straight-Through	Kabel dengan susunan ujung yang sama	Menghubungkan perangkat berbeda, seperti PC ke Switch atau Switch ke Router.
Cross-Over	Kabel dengan susunan ujung berbeda (T568A-T568B)	Menghubungkan perangkat sejenis, seperti PC ke PC atau Switch ke Switch.

### Rencana Penerapan VLAN

VLAN ID	Nama VLAN	Departemen/Fungsi	Tujuan/Deskripsi
10	VLAN_IT	Departemen IT (Gedung A)	Memisahkan jaringan IT agar memiliki akses yang lebih luas terhadap sistem & server.
20	VLAN_KEUANGAN	Departemen Keuangan (Gedung A)	Memberikan keamanan pada komunikasi data keuangan.
30	VLAN_SDM	Departemen SDM (Gedung A)	Melindungi data personal dan operasional terkait kepegawaian.
40	VLAN_SERVER	Server Farm (Gedung A)	Menjadi pusat layanan jaringan seperti DNS, DHCP, dsb.
50	VLAN_MARKETING	Departemen Marketing (Gedung B)	Mengatur lalu lintas divisi marketing yang mungkin mengakses data campaign & klien.
60	VLAN_OPERASIONAL	Departemen Operasional (Gedung B)	Mengelola koneksi untuk operasional harian kantor cabang.
99	VLAN_TRUNK	Antar-router/switch (trunk)	VLAN native/trunk untuk komunikasi antar perangkat jaringan (router-on-a-stick setup).

Untuk memungkinkan komunikasi antar VLAN pada jaringan PT. Nusantara Network, digunakan metode Router-on-a-Stick, yaitu satu router (atau Layer 3 switch) yang dikonfigurasi dengan beberapa sub-interface untuk masing-masing VLAN. Ini diperlukan karena secara default, perangkat dalam VLAN yang berbeda tidak bisa saling berkomunikasi tanpa perantara Layer 3.

#### 1. Konfigurasi Switch

Pada sisi switch, port yang mengarah ke router dikonfigurasi sebagai trunk port, sedangkan port ke perangkat pengguna dikonfigurasi sebagai access port dan ditetapkan ke VLAN tertentu. Contoh:

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport access vlan 10  
Switch(config)# interface fastEthernet 0/24  
Switch(config-if)# switchport mode trunk
```

## 2. Konfigurasi Router (Router-on-a-Stick)

Sebuah interface router (misalnya GigabitEthernet0/0) akan dibuat menjadi beberapa sub-interface, masing-masing mewakili satu VLAN dengan penetapan tag 802.1Q. Setiap sub-interface diberi IP address sebagai default gateway untuk VLAN tersebut.

```
Router(config)# interface GigabitEthernet0/0.10  
Router(config-subif)# encapsulation dot1Q 10  
Router(config-subif)# ip address 192.168.10.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.20  
Router(config-subif)# encapsulation dot1Q 20  
Router(config-subif)# ip address 192.168.20.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.30  
Router(config-subif)# encapsulation dot1Q 30  
Router(config-subif)# ip address 192.168.30.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.40  
Router(config-subif)# encapsulation dot1Q 40  
Router(config-subif)# ip address 192.168.40.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.50  
Router(config-subif)# encapsulation dot1Q 50  
Router(config-subif)# ip address 192.168.50.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.60  
Router(config-subif)# encapsulation dot1Q 60  
Router(config-subif)# ip address 192.168.60.1 255.255.255.0
```

Catatan: Tidak perlu sub-interface untuk VLAN 99 (trunk/native), karena itu hanya digunakan untuk tagging antar switch dan tidak memiliki IP gateway.

## 3. Routing Antar VLAN

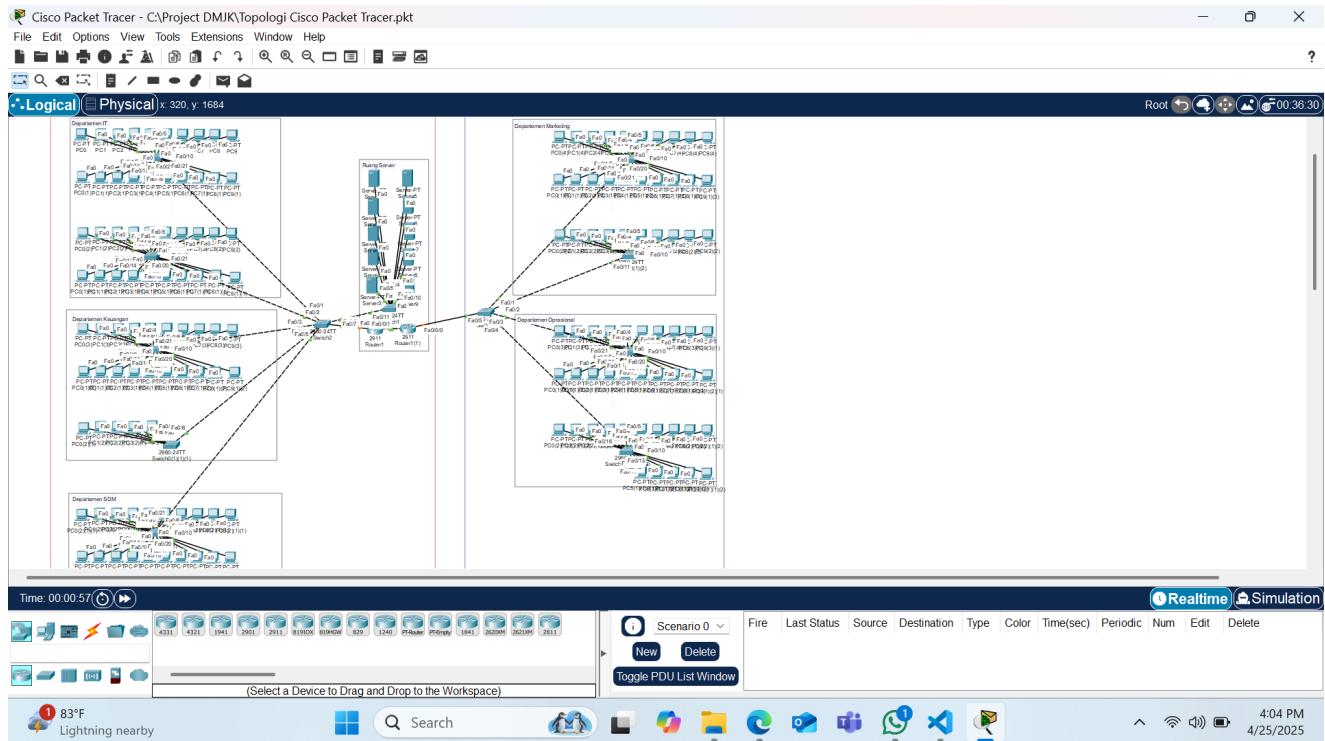
Setelah konfigurasi di atas, router secara otomatis akan mengenali semua VLAN sebagai subnet yang terhubung langsung, dan routing antar VLAN dapat berlangsung tanpa perlu konfigurasi routing tambahan.

## 4. Hasil Akhir

Dengan konfigurasi ini, komputer dalam VLAN IT (VLAN 10) dapat berkomunikasi dengan komputer di VLAN SDM (VLAN 30) atau mengakses server di VLAN 40, selama aturan keamanan (misalnya ACL atau firewall) mengizinkan.



## Topologi



Penjelasan : Topologi yang ditampilkan dalam gambar adalah diagram jaringan yang dibuat menggunakan Cisco Packet Tracer. Diagram ini menggambarkan struktur jaringan dalam sebuah organisasi, terdiri dari beberapa departemen atau area, seperti Departemen IT, Departemen Keuangan, Departemen SDM, Ruang Server, Departemen Marketing, dan Departemen Operasional.

Setiap departemen memiliki perangkat seperti PC, switch, dan terhubung secara hierarkis. Switch dalam masing-masing departemen dihubungkan ke router pusat (Router1) melalui port Fast Ethernet seperti Fa0/1, Fa0/2, dan sebagainya. Topologi ini menunjukkan bahwa router berperan sebagai pusat komunikasi antar departemen, memastikan koneksi antara berbagai segmen jaringan.

Di bagian Ruang Server, terdapat perangkat server yang dihubungkan langsung ke switch, memberikan layanan penting ke seluruh departemen. Selain itu, diagram ini memperlihatkan koneksi logis antara router dan switch, yang direpresentasikan oleh garis penghubung. Secara keseluruhan, topologi ini mencerminkan desain jaringan yang terstruktur untuk mendukung komunikasi dan kolaborasi antar berbagai area dalam organisasi. Desain ini mempermudah pengelolaan jaringan serta identifikasi masalah yang mungkin muncul.

## Konfigurasi VLAN dan Trunking

## Switch Departemen IT

The screenshot shows a window titled "Switch0" with tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area is labeled "IOS Command Line Interface". The CLI session output is as follows:

```
*LINK-5-CHANGED: Interface FastEthernet0/21, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN_IT
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface fa0/21
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

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

```
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN_IT
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface fa0/21
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

Top

Penjelasan : Gambar tersebut menunjukkan proses konfigurasi dua buah switch pada Cisco Packet Tracer melalui Command Line Interface (CLI). Pada kedua switch, administrator terlebih dahulu masuk ke mode konfigurasi dengan perintah enable dan conf t . Selanjutnya, dibuat dua VLAN, yaitu VLAN 10 dengan nama "VLAN\_IT" dan VLAN 99 dengan nama "VLAN\_NATIVE". Setelah itu, port FastEthernet dari 0/1 hingga 0/20 dikonfigurasi sebagai access port yang tergabung ke dalam VLAN 10. Sedangkan port FastEthernet 0/21 dikonfigurasi sebagai trunk port untuk menghubungkan antar switch. Pada konfigurasi trunk ini, VLAN 99 ditetapkan sebagai native VLAN. Terakhir, konfigurasi disimpan dengan perintah write memory. Notifikasi yang muncul seperti %LINK-5-CHANGED dan %LINEPROTO-5-UPDOWN menunjukkan adanya perubahan status pada port, menandakan koneksi antar switch mulai aktif. Konfigurasi ini penting untuk membentuk jaringan VLAN yang tersegmentasi namun tetap dapat saling berkomunikasi melalui trunking.

The screenshot shows a terminal window titled "Switch0(1)(1)" with the "CLI" tab selected. The window displays the following configuration commands:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN_KEUANGAN
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface fa0/1-20
^
* Invalid input detected at '^' marker.

Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface fa0/21
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

At the bottom right of the terminal window are "Copy" and "Paste" buttons. Below the terminal window is a toolbar with a "Top" button.

Switch0(1)(1)(1)

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN KEUANGAN
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

Top

Penjelasan : Konfigurasi pada kedua switch dilakukan untuk membuat jaringan VLAN yang tersegmentasi dan terhubung melalui trunking. Pertama, VLAN 20 dibuat dengan nama VLAN KEUANGAN dan VLAN 99 sebagai VLAN\_NATIVE. Di Switch 1, port fa0/1 sampai fa0/20 dikonfigurasi sebagai akses VLAN 20, sedangkan port fa0/21 digunakan sebagai trunk. Trunk tersebut diset menggunakan perintah switchport mode trunk dan switchport trunk native vlan 99, sehingga VLAN 99 berfungsi sebagai native VLAN untuk komunikasi antar switch.

Di Switch 2, konfigurasi serupa diterapkan dengan port fa0/1 sampai fa0/5 diset sebagai akses untuk VLAN 20 dan port fa0/6 sebagai trunk. Trunk juga dikonfigurasi dengan VLAN 99 sebagai native, memastikan kedua switch bisa bertukar data VLAN 20 dengan benar tanpa tag VLAN tambahan karena penggunaan native VLAN. Setelah konfigurasi selesai, perintah write memory digunakan untuk menyimpan semua pengaturan. Dengan konfigurasi ini, segmentasi jaringan berdasarkan departemen keuangan berjalan optimal dan komunikasi antar switch tetap terjaga melalui trunk yang efisien.

The screenshot shows the CLI interface for a Cisco switch. The title bar says "Switch0(1)(1)(1)(1)". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main window displays the following configuration script:

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN_SDM
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface fa0/21
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit%SPAN TREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on FastEthernet0/21 VLAN99.

%SPAN TREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/21 on VLAN099. Inconsistent local
vlan.

exit
^
* Invalid input detected at '^' marker.

Switch(config-if)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99),
with Switch FastEthernet0/5 (1).

Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]

```

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

Penjelasan : Pada Switch 1, dibuat dua VLAN yaitu VLAN 30 (VLAN\_SDM) untuk akses pengguna dan VLAN 99 (VLAN\_NATIVE) sebagai native VLAN. Port fa0/1-fa0/20 diset mode akses ke VLAN 30, sementara fa0/21 diset sebagai trunk dengan native VLAN 99 untuk koneksi antar switch. Konfigurasi disimpan dengan write memory.

Namun, muncul error Native VLAN mismatch dan BPDU error di fa0/21 karena VLAN native di Switch 1 (VLAN 99) tidak sama dengan VLAN native di Switch 2 (kemungkinan masih default VLAN 1). Akibatnya, port trunk diblokir oleh STP untuk mencegah loop. Solusinya, samakan VLAN native di kedua switch.

## Server Farm

The screenshot shows a terminal window titled "Switch1" with the "CLI" tab selected. The window displays the following configuration commands:

```
*LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 60
Switch(config-vlan)#name SERVER_FARM
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 60
Switch(config-if-range)#exit
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

At the bottom right of the terminal window are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

Penjelasan : Pada Switch 2, VLAN 60 (SERVER\_FARM) dibuat untuk akses pengguna dan VLAN 99 (VLAN\_NATIVE) untuk koneksi trunk. Port fa0/1-fa0/10 diset sebagai akses VLAN 60, sedangkan port fa0/11 diset sebagai trunk dengan native VLAN 99. Setelah konfigurasi disimpan, port trunk siap digunakan.

Dengan menyamakan native VLAN 99 pada kedua switch (Switch 1 dan Switch 2), masalah Native VLAN mismatch yang sebelumnya terjadi berhasil diatasi, sehingga koneksi trunk antar switch dapat berjalan normal tanpa konflik.

The screenshot shows a window titled "Switch0(2)" with tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area is labeled "IOS Command Line Interface". The CLI output is as follows:

```
*LINK-5-CHANGED: Interface FastEthernet0/21, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 40
Switch(config-vlan)#name VLAN_MARKETING
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#interface fa0/21
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

Below the CLI window are two buttons: "Copy" and "Paste".

 Top

Switch0(1)(2)

Physical    Config    **CLI**    Attributes

IOS Command Line Interface

```
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 40
Switch(config-vlan)#name VLAN_MARKETING
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/11 (99),
with Switch FastEthernet0/2 (1).
write memory
Building configuration...
[OK]
Switch#
```

Top

Penjelasan : Switch1 dikonfigurasi untuk departemen Server Farm dengan VLAN 60 yang dinamai SERVER\_FARM dan VLAN 99 sebagai VLAN\_NATIVE. Port Fa0/1 hingga Fa0/10 disetel sebagai akses VLAN 60, sedangkan Fa0/11 disetel sebagai trunk dengan native VLAN 99.

Switch2 dikonfigurasi untuk departemen Marketing dengan VLAN 40 yang dinamai VLAN\_MARKETING dan VLAN 99 sebagai VLAN\_NATIVE. Port Fa0/1 hingga Fa0/20 diatur sebagai akses VLAN 40, dan port Fa0/21 sebagai trunk dengan native VLAN 99.

Switch3 juga untuk departemen Marketing dengan konfigurasi serupa seperti Switch2. Namun, muncul peringatan Native VLAN mismatch karena terjadi perbedaan native VLAN antara Switch3 (VLAN 99) dan perangkat yang terhubung di Fa0/11 yang kemungkinan masih menggunakan VLAN default (VLAN 1).

The screenshot shows a window titled "Switch0(1)(1)(2)" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected, displaying the following command-line session:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name VLAN_OPERASIONAL
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range 0/1-20
^
% Invalid input detected at '^' marker.

Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#exit
Switch(config)#interface fa0/21
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
wrtie memory
^
% Invalid input detected at '^' marker.

Switch#
```

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

The screenshot shows a Cisco Switch CLI interface titled "Switch0(1)(1)(1)(2)". The tab "CLI" is selected. The command-line interface displays the following configuration script:

```
*LINK-5-CHANGED: Interface FastEthernet0/16, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name VLAN_OPERASIONAL
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#exit
Switch(config)#interface fa0/16
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
*SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
```

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

Penjelasan : Gambar pertama (switchoperasional1.jpg) menampilkan konfigurasi VLAN pada sebuah switch Cisco menggunakan antarmuka CLI. Pada gambar tersebut, administrator jaringan membuat dua VLAN, yaitu VLAN 50 dengan nama "VLAN\_OPERASIONAL" dan VLAN 99 dengan nama "VLAN\_NATIVE". Selanjutnya, port FastEthernet 0/1 hingga 0/20 dikonfigurasi sebagai mode access dan dimasukkan ke dalam VLAN 50. Port FastEthernet 0/21 dikonfigurasi sebagai mode trunk dengan VLAN native 99. Terjadi beberapa pesan status yang menunjukkan perubahan state pada port tersebut, seperti line protocol yang awalnya down kemudian up. Meskipun konfigurasi berhasil, terdapat pesan error saat mencoba perintah "write memory" yang menunjukkan ketidakvalidan input.

Gambar kedua (switchoperasional2.jpg) juga menampilkan konfigurasi VLAN pada switch Cisco dengan langkah-langkah serupa. VLAN 50 dan 99 dibuat dengan nama yang sama seperti pada gambar pertama. Namun, kali ini port FastEthernet 0/1 hingga 0/15 dikonfigurasi sebagai mode access dan dimasukkan ke dalam VLAN 50, sedangkan port FastEthernet 0/16 dikonfigurasi sebagai mode trunk dengan VLAN native 99. Pesan status juga muncul, menunjukkan perubahan state pada port tersebut. Berbeda dengan gambar

pertama, perintah "write memory" berhasil dieksekusi dengan pesan "[OK]", menandakan bahwa konfigurasi telah disimpan dengan sukses.

Kedua gambar tersebut menggambarkan proses konfigurasi VLAN dan trunking pada perangkat switch Cisco, dengan perbedaan pada range port yang dikonfigurasi serta keberhasilan penyimpanan konfigurasi.

#### Main Switch A

The screenshot shows a CLI interface for a Cisco switch named 'Switch2'. The window title is 'Switch2'. The tab bar at the top has four tabs: 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs is the text 'IOS Command Line Interface'. The main area contains the following configuration commands:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with
Switch FastEthernet0/21 (99).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/7 (1), with
Switch FastEthernet0/11 (99).

Switch(config-vlan)#vlan 10
Switch(config-vlan)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with
Switch FastEthernet0/6 (99).

Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 60
Switch(config-vlan)#vlan 60
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with
Switch FastEthernet0/21 (99).

Switch(config-vlan)#vlan 6
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/5 (1), with
Switch FastEthernet0/21
Switch(config-vlan)#vlan 99
Switch(config-vlan)#interface range fa0/1-5
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with
Switch FastEthernet0/21 (99).

Switch(config-if-range)#interface range fa0/1-5
Switch(config-if-range)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with
Switch FastEthernet0/21 (99).
```

At the bottom right of the command window are two buttons: 'Copy' and 'Paste'. At the bottom left is a 'Top' button.

The screenshot shows a Cisco Switch interface titled "Switch2". The "CLI" tab is selected. The command-line interface (CLI) window displays the following configuration script:

```
Switch(config-if-range)#switchport trunk native vlan 99
Switch(config-if-range)#exit
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

Penjelasan : Gambar mainswitcha1.jpg menampilkan konfigurasi VLAN pada sebuah switch Cisco, tetapi terdapat beberapa masalah terkait Native VLAN Mismatch yang terdeteksi melalui pesan error CDP (Cisco Discovery Protocol). Pesan tersebut menunjukkan ketidakcocokan VLAN native antara port-port tertentu (Fa0/1, Fa0/3, Fa0/5, dll.) dengan port trunk (Fa0/21 atau Fa0/11) yang memiliki VLAN native 99. Selama proses pembuatan VLAN (10, 20, 30, 40, 60, dan 99), pesan error terus muncul, mengindikasikan bahwa konfigurasi trunk belum sinkron antara switch yang terhubung.

Pada gambar mainswitcha2.jpg, administrator jaringan memperbaiki masalah tersebut dengan mengonfigurasi ulang port Fa0/6 sebagai trunk dan menetapkan VLAN native 99. Setelah konfigurasi, protokol pada port Fa0/6 sempat down kemudian up, menandakan proses negosiasi trunking berhasil. Konfigurasi disimpan dengan perintah write memory, dan pesan "[OK]" menunjukkan bahwa perubahan telah berhasil diterapkan. Gambar ini menggambarkan langkah perbaikan untuk menyelesaikan masalah Native VLAN Mismatch yang muncul sebelumnya.

#### Main Switch B

The screenshot shows a Cisco Switch interface titled "Switch3". The "CLI" tab is selected. The command-line interface (CLI) window displays the following configuration script:

```
* incomplete command
Switch(config)#vlan 50
Switch(config-vlan)#name VLAN_OPERASIONAL
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name VLAN_MARKETING
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_NATIVE
Switch(config-vlan)#exit
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with
Switch FastEthernet0/16 (99).
t
Switch(config)#exit
Switch#
```

The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a device named 'Switch3'. The window has tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. The main area displays the following CLI session:

```

Switch(config)#interface range fa0/1-4
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (1), with
Switch FastEthernet0/11 (99).

Switch(config-if-range)#s
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with
Switch FastEthernet0/21 (99).

* Ambiguous command: "s"
Switch(config-if-range)#
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan 99
Switch(config-if-range)#e%SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/3 on
VLAN0099. Port consistency restored.

%SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/3 on VLAN0001. Port
consistency restored.

xit%SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/2 on VLAN0099. Port
consistency restored.

%SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/2 on VLAN0001. Port
consistency restored.

Switch(config)#interface fa0/5
Switch(config-if)#switchport mode trunk

Switch(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99

```

At the bottom right of the CLI window are 'Copy' and 'Paste' buttons.

Top

Penjelasan : Gambar mainswitchb1.jpg menunjukkan konfigurasi VLAN pada Switch3 dengan pembuatan tiga VLAN: VLAN 50 (VLAN\_OPERASIONAL), VLAN 40 (VLAN\_MARKETING), dan VLAN 99 (VLAN\_NATIVE). Namun, muncul pesan error Native VLAN Mismatch pada port FastEthernet0/4 yang terhubung ke port FastEthernet0/16 switch lain, karena perbedaan VLAN native (1 vs 99). Pesan ini mengindikasikan ketidaksesuaian konfigurasi trunk antara kedua perangkat, yang dapat menyebabkan masalah komunikasi jaringan.

Pada gambar mainswitchb2.jpg, administrator berusaha memperbaiki masalah tersebut dengan mengonfigurasi port FastEthernet0/1 hingga 0/4 sebagai trunk dan menetapkan VLAN native 99. Selama proses, pesan error Native VLAN Mismatch masih muncul pada beberapa port (Fa0/2 dan Fa0/3), tetapi setelah konfigurasi ulang, sistem memulihkan konsistensi port dengan pesan UNBLOCK\_CONSIST\_PORT. Port FastEthernet0/5 juga dikonfigurasi sebagai trunk dengan VLAN native 99, yang sempat mengalami down-up pada protokolnya, menandakan proses negosiasi trunking yang berhasil. Gambar ini menggambarkan upaya perbaikan masalah VLAN mismatch melalui sinkronisasi konfigurasi trunk.

## Main Router A

The screenshot shows a window titled "Router1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected, displaying the IOS Command Line Interface. The configuration commands listed are:

```
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.10
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/1 (1),
with Switch FastEthernet0/6 (99).

Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/1 (1),
with Switch FastEthernet0/6 (99).

% 192.168.30.0 overlaps with GigabitEthernet0/0.30
Router(config-subif)#interface GigabitEthernet0/0.40
Router(config-subif)#no ip address
Router(config-subif)#no encapsulation dot1Q 40
Router(config-subif)#exit
Router(config)#%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/1 (1),
with Switch FastEthernet0/6 (99).

Router(config)#interface GigabitEthernet0/0.99
Router(config-subif)#encapsulation dot1Q 99 native
Router(config-subif)#ip address 192.168.99.1 255.255.255.0
```

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

Penjelasan : Pada jendela CLI, terdapat berbagai perintah konfigurasi untuk interface GigabitEthernet, seperti pengaturan jenis encapsulation, pemberian alamat IP, dan penanganan kesalahan VLAN. Salah satu perintah yang terlihat adalah penggunaan encapsulation dot1Q untuk menentukan VLAN tertentu, seperti VLAN 10, 20, 30, dan 40. Namun, terdapat beberapa kesalahan, termasuk "native VLAN mismatch" pada interface FastEthernet dan tumpang tindih jaringan IP pada interface GigabitEthernet0/0.30. Hal ini menunjukkan pentingnya pengelolaan VLAN dan alamat IP yang hati-hati dalam konfigurasi jaringan. Gambar ini relevan untuk administrator jaringan atau pelajar yang mempelajari cara mengkonfigurasi router dan menyelesaikan masalah jaringan.

## Main Router B

The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "Router1(1)". The window has tabs at the top: "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main area contains the following configuration commands:

```
Router(config)#interface GigabitEthernet 0/1.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/0 (1),
with Switch FastEthernet0/5 (99).

Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#EXIT
Router(config)#interface GigabitEthernet 0/1.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.1 255.255.255.0
Router(config-subif)#EXIT
Router(config)#interface GigabitEthernet 0/1.99
Router(config-subif)#interface GigabitEthernet 0/1.99
Router(config-subif)#encapsulation dot1Q 99 native
Router(config-subif)#ip address 192.168.99.2 255.255.255.0
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/0 (1),
with Switch FastEthernet0/5 (99).

Router(config-subif)#ip address 192.168.99.2 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#no shutdown

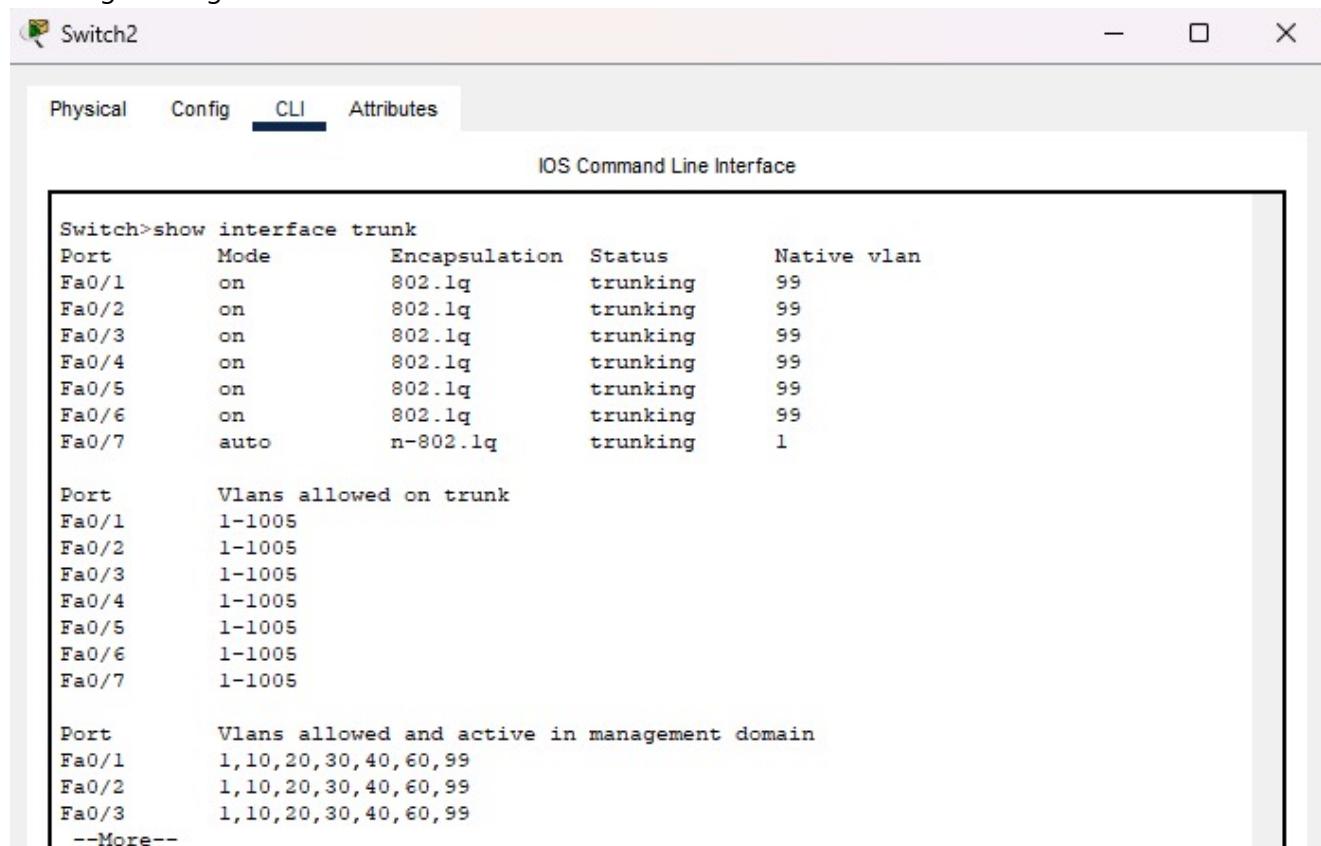
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.40, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.50, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up
exit
Router(config)#exit
Router#
&SYS-5-CONFIG-T: Configured from console by console
```

Below the command window are two buttons: "Copy" and "Paste".

Top

Penjelasan : Pada gambar diatas terdapat sejumlah perintah konfigurasi yang diterapkan pada beberapa interface GigabitEthernet, termasuk konfigurasi VLAN dengan encapsulation dot1Q dan pemberian alamat IP pada sub-interface seperti 0/1.40, 0/1.50, dan 0/1.99. Perintah seperti "no shutdown" digunakan untuk mengaktifkan interface, dan pesan log menunjukkan perubahan status interface, misalnya menjadi aktif ("state to up"). Gambar ini relevan untuk memahami konfigurasi jaringan berbasis VLAN dan manajemen interface pada router, yang penting bagi administrator jaringan atau pelajar dalam bidang jaringan komputer.

## Trunking Gedung A



The screenshot shows a terminal window titled "Switch2" with the "CLI" tab selected. The output of the "show interface trunk" command is displayed:

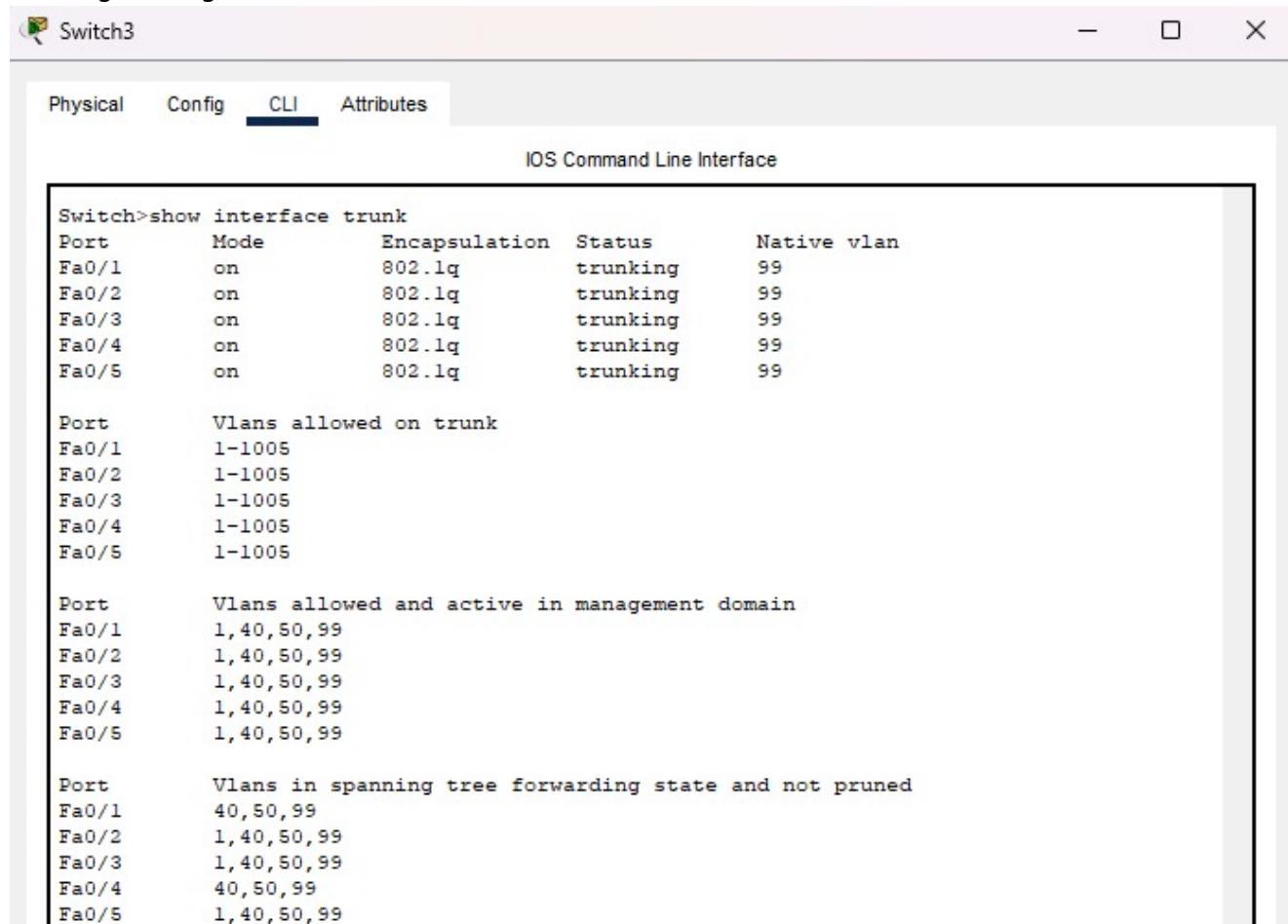
```
Switch>show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1    on        802.1q         trunking   99
Fa0/2    on        802.1q         trunking   99
Fa0/3    on        802.1q         trunking   99
Fa0/4    on        802.1q         trunking   99
Fa0/5    on        802.1q         trunking   99
Fa0/6    on        802.1q         trunking   99
Fa0/7    auto      n-802.1q       trunking   1

Port      Vlans allowed on trunk
Fa0/1    1-1005
Fa0/2    1-1005
Fa0/3    1-1005
Fa0/4    1-1005
Fa0/5    1-1005
Fa0/6    1-1005
Fa0/7    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,10,20,30,40,60,99
Fa0/2    1,10,20,30,40,60,99
Fa0/3    1,10,20,30,40,60,99
--More--
```

Penjelasan : Gambar diatas menunjukkan informasi mengenai konfigurasi trunk pada switch dengan menggunakan perintah show interface trunk. Perintah ini memberikan detail tentang port trunk yang aktif, termasuk mode trunk, tipe encapsulation, native VLAN, VLAN yang diizinkan, dan VLAN yang aktif. Sebagian besar port trunk, seperti FastEthernet0/1 hingga 0/6, berada dalam mode "on" dengan encapsulation 802.1q dan menggunakan native VLAN 99, sedangkan FastEthernet0/7 menggunakan mode "auto" dengan native VLAN 1. Semua port trunk mengizinkan lalu lintas untuk VLAN 1-1005, dan beberapa VLAN seperti 1, 10, 20, 30, 40, 60, dan 99 terdaftar sebagai VLAN aktif dalam domain. Informasi ini berguna bagi administrator jaringan untuk memastikan koneksi antar VLAN berjalan lancar serta untuk mengidentifikasi dan mengatasi potensi masalah dalam konfigurasi trunk. Adanya pesan "--More--" menunjukkan data tambahan yang belum terlihat dalam tampilan ini.

## Status Trunk



```

Switch>show interface trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1    on        802.1q        trunking   99
Fa0/2    on        802.1q        trunking   99
Fa0/3    on        802.1q        trunking   99
Fa0/4    on        802.1q        trunking   99
Fa0/5    on        802.1q        trunking   99

Port      Vlans allowed on trunk
Fa0/1    1-1005
Fa0/2    1-1005
Fa0/3    1-1005
Fa0/4    1-1005
Fa0/5    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,40,50,99
Fa0/2    1,40,50,99
Fa0/3    1,40,50,99
Fa0/4    1,40,50,99
Fa0/5    1,40,50,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    40,50,99
Fa0/2    1,40,50,99
Fa0/3    1,40,50,99
Fa0/4    40,50,99
Fa0/5    1,40,50,99

```

Penjelasan : Gambar diatas merupakan hasil dari perintah show interface trunk pada antarmuka CLI (Command Line Interface) sebuah switch. Output tersebut memberikan informasi terkait konfigurasi trunk pada beberapa port FastEthernet (Fa0/1 hingga Fa0/5).

Detail yang ditampilkan meliputi mode trunk yang diatur "on", tipe encapsulation yang menggunakan standar 802.1q, serta native VLAN yang disetel ke VLAN 99 untuk setiap port. Semua port mengizinkan lalu lintas dari VLAN 1 hingga 1005, dan VLAN yang aktif dalam domain manajemen mencakup VLAN 1, 40, 50, dan 99. Selain itu, VLAN yang berada dalam status forwarding pada spanning tree protocol (STP) juga sama, yaitu VLAN 1, 40, 50, dan 99.

Informasi ini penting bagi administrator jaringan untuk memastikan konfigurasi trunk yang benar pada switch, sehingga lalu lintas antar VLAN dapat dikelola dengan baik tanpa konflik. Output ini juga membantu dalam memvalidasi pengaturan spanning tree untuk memastikan kelancaran jaringan.

## **Uji Konektivitas**

## VLAN Gedung A

The screenshot shows a software window titled "Switch2" with tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main content displays the output of the command "Switch>show vlan brief".

VLAN Name	Status	Ports
1 default	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
40 VLAN0040	active	
60 VLAN0060	active	
99 VLAN0099	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Penjelasan : Gambar diatas menunjukkan hasil perintah show vlan brief pada sebuah switch, yang merangkum konfigurasi VLAN (Virtual Local Area Network). Informasi yang ditampilkan mencakup daftar VLAN, nama VLAN, status VLAN (semuanya aktif), dan port yang terhubung ke masing-masing VLAN. VLAN default (VLAN 1) memiliki banyak port aktif, sedangkan VLAN lain seperti VLAN 10, 20, 30, 40, 60, dan 99 juga terdaftar aktif tanpa port yang terhubung. Selain itu, VLAN sistem seperti 1002 hingga 1005 juga termasuk dalam daftar. Informasi ini berguna untuk memahami pengaturan segmentasi jaringan pada switch tersebut.

## VLAN Gedung B

The screenshot shows a software window titled "Switch3" with tabs for "Physical", "Config", "CLI" (selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main content displays the output of the command "Switch>show vlan brief".

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
40 VLAN_MARKETING	active	
50 VLAN_OPERASIONAL	active	
99 VLAN_NATIVE	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Penjelasan : Gambar diatas menunjukkan hasil dari perintah show vlan brief yang memberikan gambaran konfigurasi VLAN pada sebuah switch. Output ini mencantumkan beberapa VLAN yang terkonfigurasi, seperti VLAN 1 (default), VLAN 40, 50, dan 99, beserta VLAN sistem seperti 1002 hingga 1005. Informasi yang ditampilkan meliputi nama VLAN, status (semua aktif), dan port yang terhubung. VLAN default

memiliki banyak port yang digunakan, termasuk beberapa FastEthernet (Fa0/6 hingga Fa0/24) dan GigabitEthernet (Gi0/1 dan Gi0/2), sementara VLAN lainnya belum memiliki port yang terhubung. Output ini membantu administrator jaringan untuk memahami distribusi port dan pengelolaan VLAN pada perangkat jaringan.

## Konfigurasi Router

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	down
GigabitEthernet0/0.10	192.168.10.1	YES	manual	up	down
GigabitEthernet0/0.20	192.168.20.1	YES	manual	up	down
GigabitEthernet0/0.30	192.168.30.1	YES	manual	up	down
GigabitEthernet0/0.40	unassigned	YES	unset	up	down
GigabitEthernet0/0.59	192.168.59.1	YES	manual	up	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/0/0	unassigned	YES	unset	up	up
FastEthernet0/0/1	unassigned	YES	unset	up	up
FastEthernet0/0/2	unassigned	YES	unset	up	down
FastEthernet0/0/3	unassigned	YES	unset	up	down
FastEthernet0/1/0	unassigned	YES	unset	up	down
FastEthernet0/1/1	unassigned	YES	unset	up	down
FastEthernet0/1/2	unassigned	YES	unset	up	down
FastEthernet0/1/3	unassigned	YES	unset	up	down
FastEthernet0/2/0	unassigned	YES	unset	up	down
FastEthernet0/2/1	unassigned	YES	unset	up	down
FastEthernet0/2/2	unassigned	YES	unset	up	down
FastEthernet0/2/3	unassigned	YES	unset	up	down
FastEthernet0/3/0	unassigned	YES	unset	up	down
--More--					

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	up	down
GigabitEthernet0/1.40	192.168.40.1	YES	manual	up	down
GigabitEthernet0/1.50	192.168.50.1	YES	manual	up	down
GigabitEthernet0/1.59	192.168.59.2	YES	manual	up	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/0/0	unassigned	YES	unset	up	up
FastEthernet0/0/1	unassigned	YES	unset	up	up
FastEthernet0/0/2	unassigned	YES	unset	up	down
FastEthernet0/0/3	unassigned	YES	unset	up	down
FastEthernet0/1/0	unassigned	YES	unset	up	down
FastEthernet0/1/1	unassigned	YES	unset	up	down
FastEthernet0/1/2	unassigned	YES	unset	up	down
FastEthernet0/1/3	unassigned	YES	unset	up	down
FastEthernet0/2/0	unassigned	YES	unset	up	down
FastEthernet0/2/1	unassigned	YES	unset	up	down
FastEthernet0/2/2	unassigned	YES	unset	up	down
FastEthernet0/2/3	unassigned	YES	unset	up	down
FastEthernet0/3/0	unassigned	YES	unset	up	down
FastEthernet0/3/1	unassigned	YES	unset	up	down
FastEthernet0/3/2	unassigned	YES	unset	up	down
--More--					

Penjelasan : Gambar diatas merupakan hasil perintah show ip interface brief pada CLI router "Router1". Output ini menunjukkan informasi konfigurasi antarmuka jaringan, termasuk nama antarmuka, alamat IP, metode konfigurasi IP, serta status administratif dan protokol. Beberapa antarmuka seperti GigabitEthernet0/0 dan GigabitEthernet0/1 berada dalam kondisi "administratively down" tanpa alamat IP. Sub-antarmuka seperti GigabitEthernet0/1.50 dan GigabitEthernet0/1.51 memiliki alamat IP terkonfigurasi, tetapi protokolnya "down". Sementara itu, antarmuka FastEthernet0/0/0 terlihat aktif dengan status "up" baik secara administratif maupun protokolnya. Pesan "--More--" mengindikasikan adanya informasi tambahan yang belum ditampilkan. Output ini penting untuk memverifikasi koneksi jaringan dan mengidentifikasi masalah pada antarmuka.

Selain itu, informasi seperti alamat IP terkonfigurasi secara manual dan status protokol yang "down" pada sub-antarmuka menunjukkan adanya potensi kendala dalam koneksi jaringan. Status "administratively down" pada beberapa antarmuka utama juga mengindikasikan bahwa konfigurasi jaringan masih membutuhkan penyesuaian agar seluruh antarmuka dapat berfungsi secara optimal. Output ini menjadi alat penting bagi administrator untuk melakukan troubleshooting dan optimisasi konfigurasi jaringan pada router.

## Kendala dan Solusi

1. Kesusahan untuk mengkonfigurasi karena pada topologi sebelumnya ternyata terlalu tricky/sulit alurnya, jadi menyelesaikan kendala ini dengan menghapus router setiap departemen.
2. Kesalahan dalam penentuan Subnetting, sehingga pada saat konfigurasi terjadi invalid. Memperbaiki kendala ini adalah dengan menyesuaikan pada VLAN yang sudah ditentukan setiap departemennya

### Table Subnetting Terbaru

VLAN	Nama	Gedung	Subnet	Gateway IP (Router)
10	IT	Gedung A	192.168.10.0/24	192.168.10.1
20	Keuangan	Gedung A	192.168.20.0/24	192.168.20.1
30	SDM	Gedung A	192.168.30.0/24	192.168.30.1
60	Server	Gedung A	192.168.60.0/24	192.168.60.1
40	Marketing	Gedung B	192.168.40.0/24	192.168.40.1
50	Operasional	Gedung B	192.168.50.0/24	192.168.50.1
99	Native VLAN	Semua	-	-
-	Link Router A-B	Koneksi Antar Router	192.168.100.0/30	Router A: .1, Router B: .2

↳ [Implementasi Routing & WAN] - [Pekan 12]

🔗 [Link File Simulasi](#)

### Konfigurasi Routing Statis Pada Jaringan Intra-Gedung

Pada implementasi jaringan ini, routing statis tidak digunakan karena seluruh konektivitas antar-subnet dan antar-gedung telah dilakukan melalui routing dinamis menggunakan protokol OSPF. Setiap VLAN dalam satu gedung telah dikenali sebagai jaringan yang langsung terhubung oleh masing - masing router, sehingga tidak memerlukan konfigurasi rute statis tambahan. Dalam hal ini, semua VLAN dalam satu gedung sudah langsung terhubung ke router masing - masing, sehingga router otomatis mengenali jaringan-jaringan tersebut sebagai directly connected network. Karena itu, implementasi ini tidak menambahkan rute statis agar antar-VLAN bisa saling terhubung dalam gedung yang sama.

Sementara itu, untuk menghubungkan jaringan antar gedung, digunakan routing dinamis dengan OSPF. Protokol OSPF memungkinkan setiap router bertukar informasi secara otomatis tentang jaringan yang mereka ketahui. Hal ini membuat jalur komunikasi antar gedung dapat terbentuk tanpa perlu konfigurasi rute satu per satu. Selain itu, OSPF juga dapat menyesuaikan rute dengan cepat jika terjadi perubahan pada jaringan, seperti koneksi antar-router terputus atau ada perangkat baru yang ditambahkan.

### Implementasi Routing Dinamis (OSPF) Untuk Koneksi Antar-Gedung

## Konfigurasi IP Sub-Interface Untuk VLAN di Router A

```
Router# 
Physical Config CLI Attributes
IOS Command Line Interface

FastEthernet0/0/2 unassigned YES unest up down
FastEthernet0/0/3 unassigned YES unest up down
FastEthernet0/0/10 unassigned YES unest up down
FastEthernet0/0/11 unassigned YES unest up down
FastEthernet0/0/12 unassigned YES unest up down
FastEthernet0/0/13 unassigned YES unest up down
FastEthernet0/0/14 unassigned YES unest up down
FastEthernet0/0/15 unassigned YES unest up down
Vlan1 unassigned YES unest administratively down down

Router#enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gig0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gig0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gig0/0.60
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.60.1 255.255.255.0
Router(config-subif)#exit
```

Penjelasan : Pada jendela CLI, terdapat berbagai perintah konfigurasi untuk interface GigabitEthernet, seperti pengaturan jenis encapsulation, pemberian alamat IP, dan penanganan kesalahan VLAN. Salah satu perintah yang terlihat adalah penggunaan encapsulation dot1Q untuk menentukan VLAN tertentu, seperti VLAN 10, 20, dan 60. Sub-interface GigabitEthernet0/1.10 dikonfigurasi dengan alamat IP 192.168.10.1 dan subnet mask 255.255.255.0 untuk VLAN 10 (VLAN\_IT), GigabitEthernet0/1.20 dengan alamat IP 192.168.20.1 dan subnet mask 255.255.255.0 untuk VLAN 20 (VLAN KEUANGAN), serta GigabitEthernet0/1.60 dengan alamat IP 192.168.60.1 dan subnet mask 255.255.255.0 untuk VLAN 60 (VLAN SERVER). Namun, terdapat beberapa kesalahan, termasuk "native VLAN mismatch" pada interface FastEthernet dan tumpang tindih jaringan IP pada interface GigabitEthernet0/0.30.

## Konfigurasi IP Sub-Interface Untuk VLAN di Router B

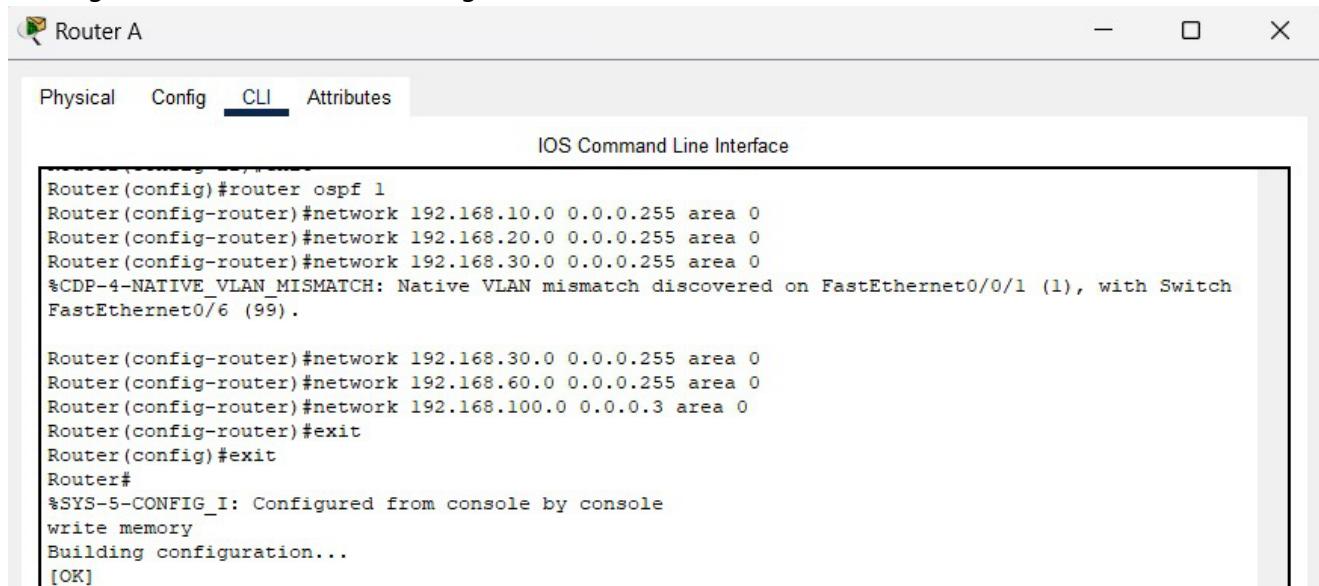
```
Router(1)#
Physical Config CLI Attributes
IOS Command Line Interface

FastEthernet0/0/0 unassigned YES unest up down
FastEthernet0/0/1 unassigned YES unest up down
FastEthernet0/0/2 unassigned YES unest up down
FastEthernet0/0/3 unassigned YES unest up down
FastEthernet0/0/10 unassigned YES unest up down
FastEthernet0/0/11 unassigned YES unest up down
FastEthernet0/0/12 unassigned YES unest up down
FastEthernet0/0/13 unassigned YES unest up down
FastEthernet0/0/14 unassigned YES unest up down
FastEthernet0/0/15 unassigned YES unest up down
Vlan1 unassigned YES unest administratively down down

Router#enable
Router(config)#interface gig0/0.10
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gig0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.1 255.255.255.0
Router(config-subif)#exit
```

Penjelasan : Pada jendela CLI, terdapat berbagai perintah konfigurasi untuk interface GigabitEthernet, seperti pengaturan jenis encapsulation, pemberian alamat IP, dan penanganan kesalahan VLAN. Salah satu perintah yang terlihat adalah penggunaan encapsulation dot1Q untuk menentukan VLAN tertentu, seperti VLAN 40 dan VLAN 50. Sub-interface GigabitEthernet0/1.50 dikonfigurasi dengan alamat IP 192.168.50.1 dan subnet mask 255.255.255.0 untuk VLAN 50 (VLAN\_OPERASIONAL), sedangkan sub-interface GigabitEthernet0/1.40 dikonfigurasi dengan alamat IP 192.168.40.1 dan subnet mask 255.255.255.0 untuk VLAN 40 (VLAN\_MARKETING). Namun, terdapat beberapa kesalahan, termasuk "native VLAN mismatch" pada interface FastEthernet dan tumpang tindih jaringan IP pada interface GigabitEthernet0/1.99.

## Routing Dinamis OSPF (Antar-Gedung) di Router A



The screenshot shows the CLI interface for Router A. The tab 'CLI' is selected. The command history displays the configuration of OSPF area 0 with networks 192.168.10.0, 192.168.20.0, and 192.168.30.0. A warning message '%CDP-4-NATIVE\_VLAN\_MISMATCH' is shown regarding a VLAN mismatch on FastEthernet0/0/1. The configuration concludes with writing memory and building the configuration.

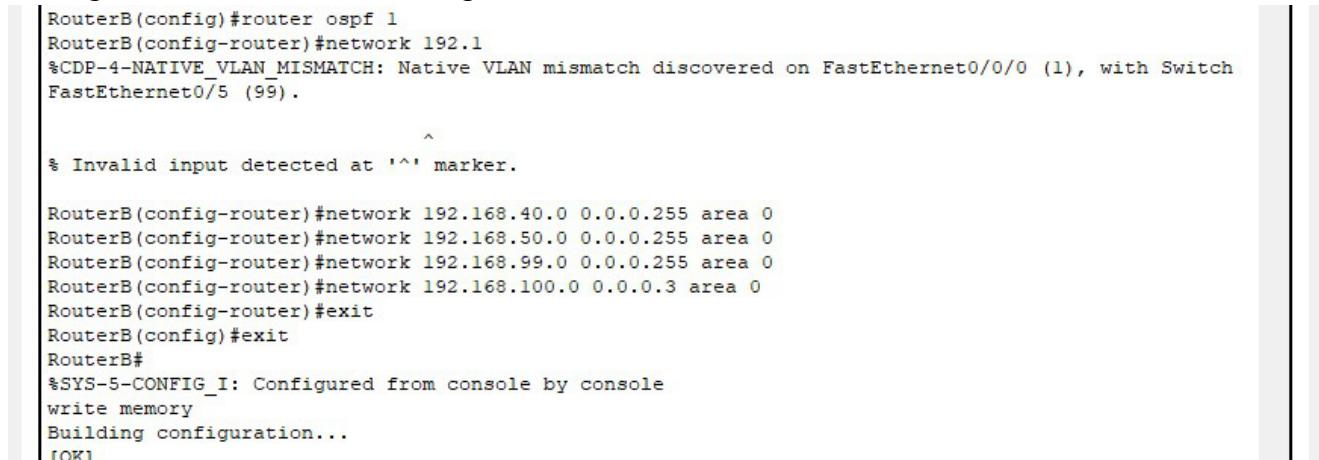
```
Router(config)#router ospf 1
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#network 192.168.30.0 0.0.0.255 area 0
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/1 (1), with Switch
FastEthernet0/6 (99).

Router(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router(config-router)#network 192.168.60.0 0.0.0.255 area 0
Router(config-router)#network 192.168.100.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

Penjelasan : Pada jendela CLI, terlihat konfigurasi routing dinamis menggunakan OSPF yang dilakukan pada Router A. Router ini dikonfigurasi dengan OSPF menggunakan perintah router ospf 1. Beberapa jaringan dimasukkan dalam konfigurasi OSPF, seperti network 192.168.10.0 0.0.0.255 area 0, network 192.168.30.0 0.0.0.255 area 0, dan network 192.168.100.0 0.0.0.3 area 0, yang masing - masing mengkonfigurasi jaringan untuk VLAN 10, VLAN 30, dan koneksi antar router.

Namun, muncul pesan peringatan %CDP-4-NATIVE\_VLAN\_MISMATCH, yang menunjukkan adanya ketidakcocokan antara native VLAN pada interface FastEthernet0/0/1 di Router A dan switch yang terhubung pada FastEthernet0/6. Hal ini dapat menyebabkan masalah dalam komunikasi trunk antar perangkat. Setelah konfigurasi selesai, perintah write memory digunakan untuk menyimpan konfigurasi yang telah diterapkan.

## Routing Dinamis OSPF (Antar-Gedung) di Router B



The screenshot shows the CLI interface for Router B. The configuration of OSPF area 0 with networks 192.168.40.0, 192.168.50.0, and 192.168.99.0 is shown. A warning message '%CDP-4-NATIVE\_VLAN\_MISMATCH' is displayed regarding a VLAN mismatch on FastEthernet0/0/0. The configuration concludes with writing memory and building the configuration.

```
RouterB(config)#router ospf 1
RouterB(config-router)#network 192.168.40.0 0.0.0.255 area 0
RouterB(config-router)#network 192.168.50.0 0.0.0.255 area 0
RouterB(config-router)#network 192.168.99.0 0.0.0.255 area 0
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/0/0 (1), with Switch
FastEthernet0/5 (99).

^
% Invalid input detected at '^' marker.

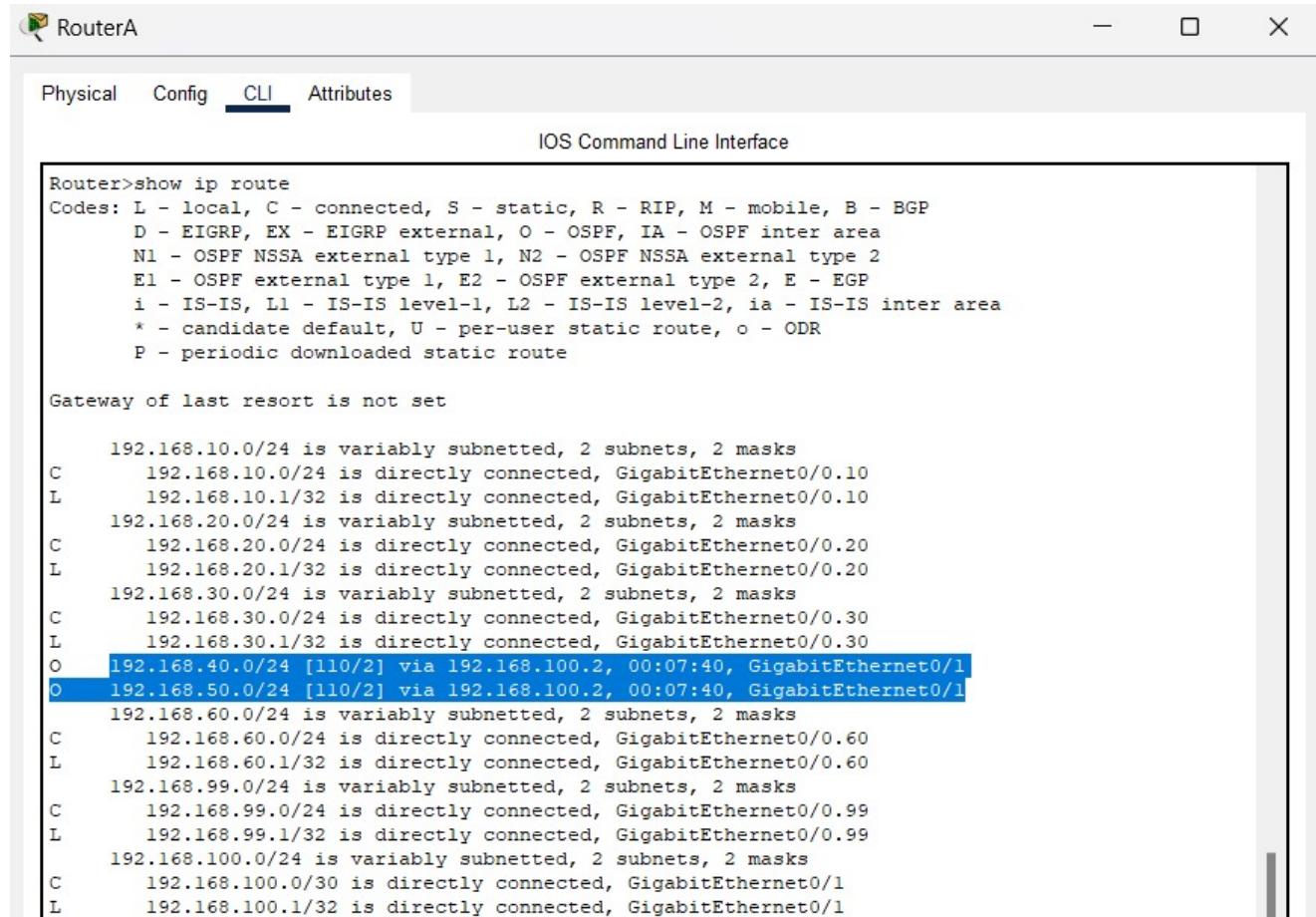
RouterB(config-router)#network 192.168.40.0 0.0.0.255 area 0
RouterB(config-router)#network 192.168.50.0 0.0.0.255 area 0
RouterB(config-router)#network 192.168.99.0 0.0.0.255 area 0
RouterB(config-router)#network 192.168.100.0 0.0.0.3 area 0
RouterB(config-router)#exit
RouterB(config)#exit
RouterB#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

Penjelasan : Pada jendela CLI, terlihat konfigurasi routing dinamis menggunakan OSPF yang dilakukan pada Router B. Router ini dikonfigurasi dengan OSPF menggunakan perintah router ospf 1. Beberapa jaringan dimasukkan dalam konfigurasi OSPF, seperti network 192.168.40.0 0.0.0.255 area 0, network 192.168.50.0 0.0.0.255 area 0, dan network 192.168.100.0 0.0.0.3 area 0, yang masing - masing mengkonfigurasi jaringan untuk VLAN 40, VLAN 50, dan koneksi antar router.

Namun, muncul pesan peringatan %CDP-4-NATIVE\_VLAN\_MISMATCH, yang menunjukkan adanya ketidakcocokan antara native VLAN pada interface FastEthernet0/0/0 di Router B dan switch yang

terhubung pada FastEthernet0/5. Hal ini dapat menyebabkan masalah dalam komunikasi trunk antar perangkat. Setelah konfigurasi selesai, perintah write memory digunakan untuk menyimpan konfigurasi yang telah diterapkan.

#### Hasil Perintah show ip route Pada Router A



The screenshot shows the CLI interface for RouterA. The 'CLI' tab is selected. The output of the 'show ip route' command is displayed:

```
Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
  192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
  192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
O     192.168.40.0/24 [110/2] via 192.168.100.2, 00:07:40, GigabitEthernet0/1
O     192.168.50.0/24 [110/2] via 192.168.100.2, 00:07:40, GigabitEthernet0/1
  192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, GigabitEthernet0/0.60
L       192.168.60.1/32 is directly connected, GigabitEthernet0/0.60
  192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.99.0/24 is directly connected, GigabitEthernet0/0.99
L       192.168.99.1/32 is directly connected, GigabitEthernet0/0.99
  192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.100.0/30 is directly connected, GigabitEthernet0/1
L       192.168.100.1/32 is directly connected, GigabitEthernet0/1
```

Penjelasan : Gambar di atas menunjukkan hasil perintah show ip route pada Router A. Tabel routing ini memberikan informasi tentang rute yang digunakan oleh router untuk mengirimkan lalu lintas antar jaringan.

Prefix O = route dari OSPF:

Rute dengan prefix O menunjukkan bahwa rute tersebut berasal dari protokol OSPF (Open Shortest Path First). Sebagai contoh, pada rute 192.168.40.0/24 [110/2] via 192.168.100.2, 00:07:40, GigabitEthernet0/1, terlihat bahwa jaringan 192.168.40.0/24 dapat dijangkau melalui OSPF dengan next hop IP 192.168.100.2, dan interface yang digunakan adalah GigabitEthernet0/1.

Prefix C = directly connected (VLAN lokal) :

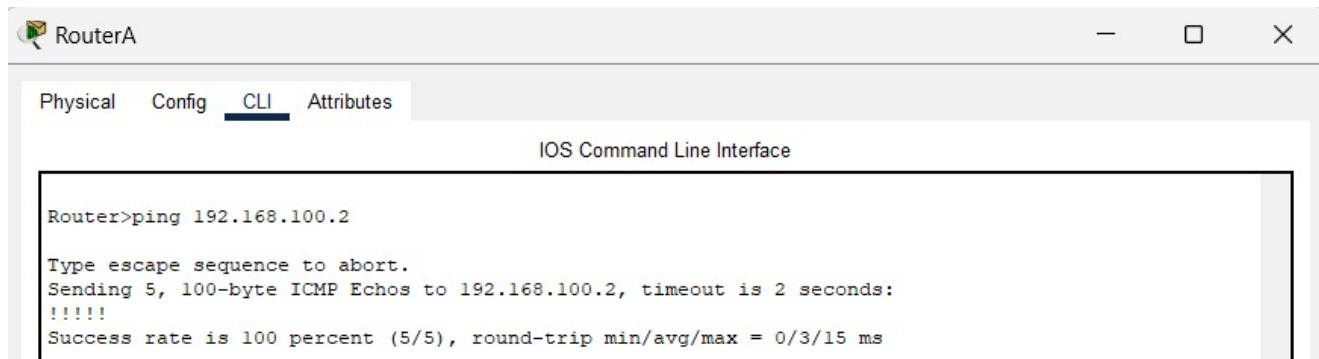
Rute dengan prefix C menunjukkan jaringan yang terhubung langsung (directly connected) ke router. Misalnya, 192.168.10.0/24 is directly connected, GigabitEthernet0/0.10 menunjukkan bahwa jaringan 192.168.10.0/24 terhubung langsung melalui interface GigabitEthernet0/0.10.

Via IP (Next-Hop) :

Pada setiap entri, Anda dapat melihat via IP, yang menunjukkan alamat IP tujuan selanjutnya (next-hop) yang harus ditempuh oleh paket untuk mencapai jaringan yang dituju. Contohnya, pada rute 192.168.40.0/24 [110/2] via 192.168.100.2, paket akan dikirimkan ke IP 192.168.100.2 sebagai next-hop.

## Simulasi Koneksi WAN Antar Gedung (Uji Konektivitas)

### WAN Test Dari Router A ke Router B



RouterA

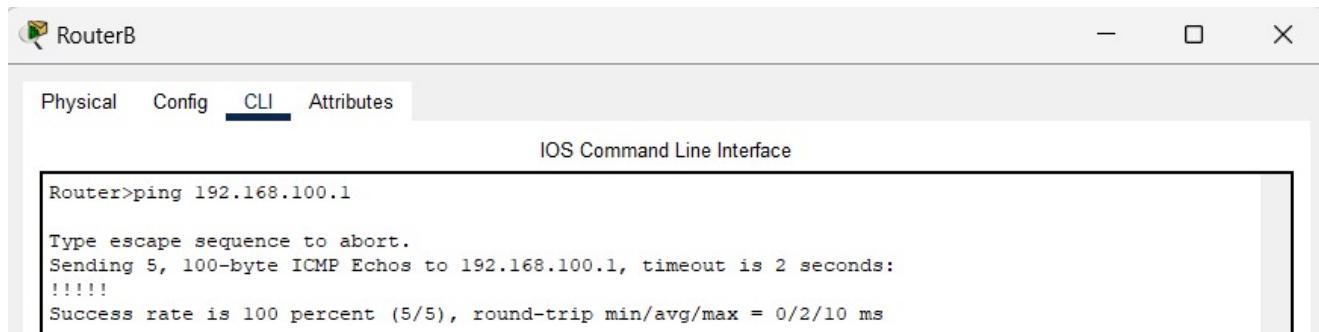
Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>ping 192.168.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/15 ms
```

Penjelasan : Pada jendela CLI, terlihat perintah ping yang digunakan untuk menguji konektivitas antar gedung (WAN Test) dari Router A ke Router B. Perintah ping 192.168.100.2 digunakan untuk mengirimkan 5 paket ICMP Echo Request dengan ukuran 100-byte ke alamat IP tujuan 192.168.100.2 yang terhubung ke Router B. Tanda "!!!!" menunjukkan bahwa semua paket yang dikirimkan berhasil menerima tanggapan (reply), menandakan bahwa jalur antara Router A dan Router B berjalan dengan baik. Success rate tercatat 100 percent (5/5) yang berarti semua paket yang dikirimkan berhasil diterima dengan baik tanpa ada paket yang hilang. Round-trip min/avg/max = 0/3/15 ms menunjukkan waktu perjalanan pulang-pergi paket, dengan waktu rata - rata 3 ms dan waktu maksimum 15 ms, yang mengindikasikan latensi yang sangat rendah. Ini menunjukkan konektivitas yang cepat dan stabil antar gedung A dan gedung B. Hasil uji konektivitas ini memastikan bahwa jalur WAN antar gedung berfungsi dengan baik dan dapat digunakan untuk komunikasi antara Gedung A dan Gedung B tanpa masalah.

### WAN Test Dari Router B ke Router A



RouterB

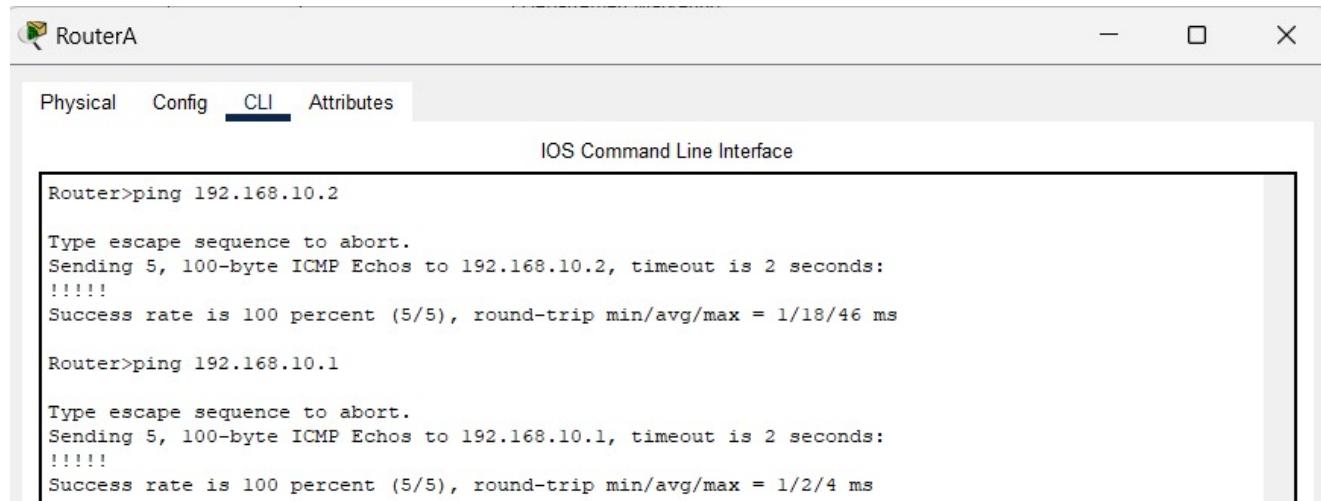
Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```

Penjelasan : Pada jendela CLI, terlihat perintah ping yang digunakan untuk menguji konektivitas antar gedung (WAN Test) dari Router B ke Router A. Perintah ping 192.168.100.1 digunakan untuk mengirimkan 5 paket ICMP Echo Request dengan ukuran 100-byte ke alamat IP tujuan 192.168.100.1, yang terhubung ke Router A. Tanda "!!!!" menunjukkan bahwa semua paket yang dikirimkan berhasil menerima tanggapan (reply), menandakan bahwa jalur antara Router B dan Router A berjalan dengan baik. Success rate tercatat 100 percent (5/5) yang berarti semua paket yang dikirimkan berhasil diterima dengan baik tanpa ada paket yang hilang. Round-trip min/avg/max = 0/2/10 ms menunjukkan waktu perjalanan pulang-pergi paket, dengan waktu rata - rata 2 ms dan waktu maksimum 10 ms, yang mengindikasikan latensi yang sangat rendah. Ini menunjukkan konektivitas yang cepat dan stabil antar Gedung B dan Gedung A. Hasil uji konektivitas ini memastikan bahwa jalur WAN antar gedung berfungsi dengan baik dan dapat digunakan untuk komunikasi antara Gedung B dan Gedung A tanpa masalah.

## Wan Test Router A ke Vlan 10



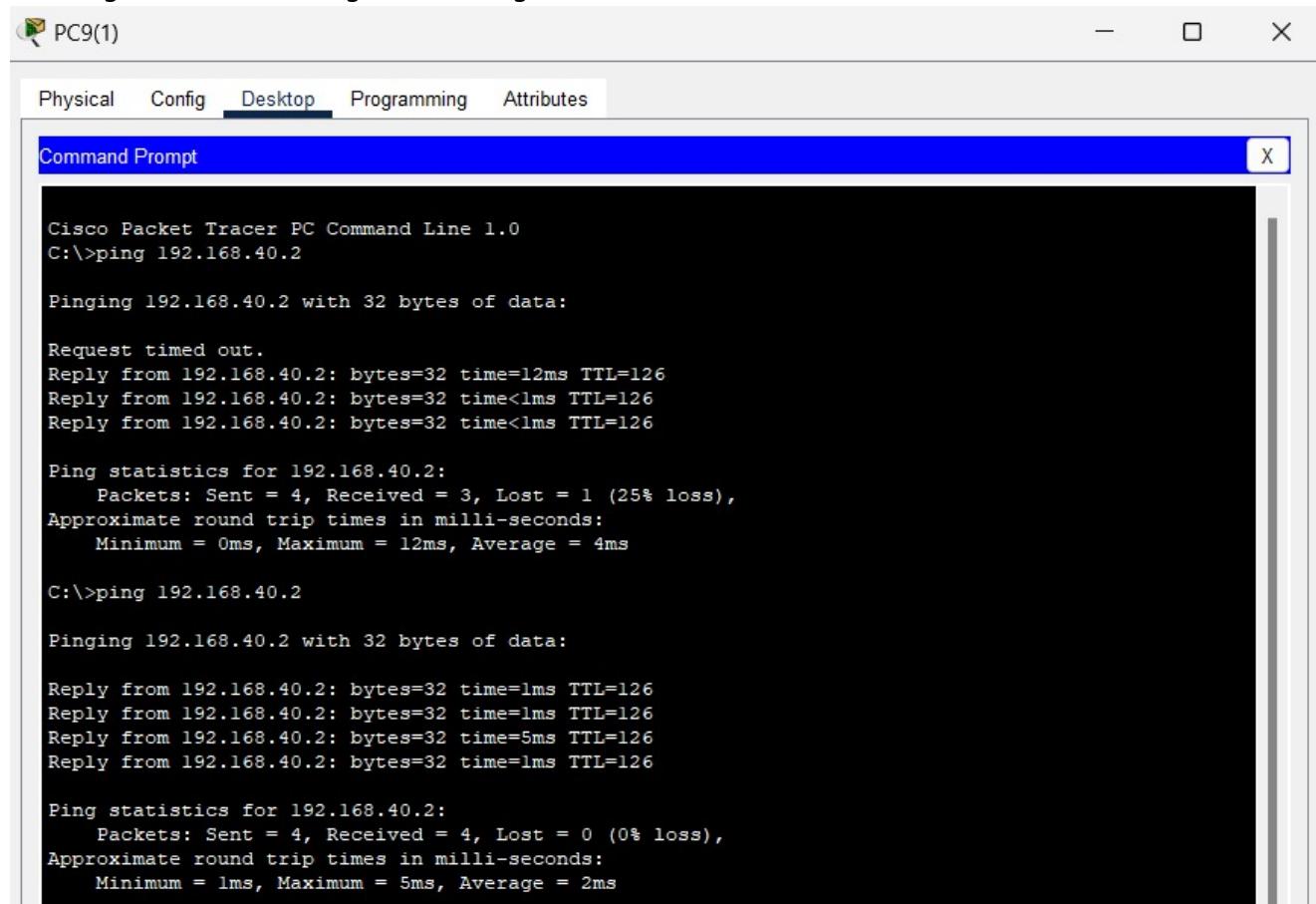
```
Router>ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/18/46 ms

Router>ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Penjelasan : Pada jendela CLI, terlihat perintah ping yang digunakan untuk menguji koneksi antar VLAN lokal di Gedung A. Perintah ping 192.168.10.2 digunakan untuk mengirimkan 5 paket ICMP Echo Request ke alamat IP 192.168.10.2, yang merupakan alamat IP di VLAN 10 di Gedung A. Tanda "!!!!" menunjukkan bahwa semua paket yang dikirimkan berhasil mendapatkan tanggapan (reply), yang berarti jalur komunikasi antar VLAN di Gedung A berfungsi dengan baik. Success rate tercatat 100 percent (5/5) yang berarti tidak ada paket yang hilang. Round-trip min/avg/max = 1/18/46 ms menunjukkan waktu perjalanan pulang-pergi paket, dengan waktu rata - rata 18 ms dan waktu maksimum 46 ms, yang menunjukkan latensi yang relatif rendah.

Kemudian, perintah ping 192.168.10.1 digunakan untuk mengirimkan 5 paket ICMP Echo Request ke alamat IP 192.168.10.1, yang juga terhubung dengan VLAN 10 di Gedung A. Hasilnya sama, yaitu 100 percent (5/5) berhasil, dengan round-trip min/avg/max = 1/2/4 ms, yang menunjukkan latensi yang sangat rendah antara perangkat dalam VLAN yang sama. Secara keseluruhan, hasil uji ping ini menunjukkan bahwa komunikasi antar perangkat di dalam VLAN 10 di Gedung A berjalan lancar tanpa masalah, dengan latensi yang sangat baik.

## Test Ping Antar Vlan Gedung A ke Gedung B (Pc Vlan 10 ke Pc Vlan 40)



The screenshot shows a Cisco Packet Tracer interface with a 'Command Prompt' window open. The window title is 'Command Prompt'. The content of the window is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.2: bytes=32 time=12ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 4ms

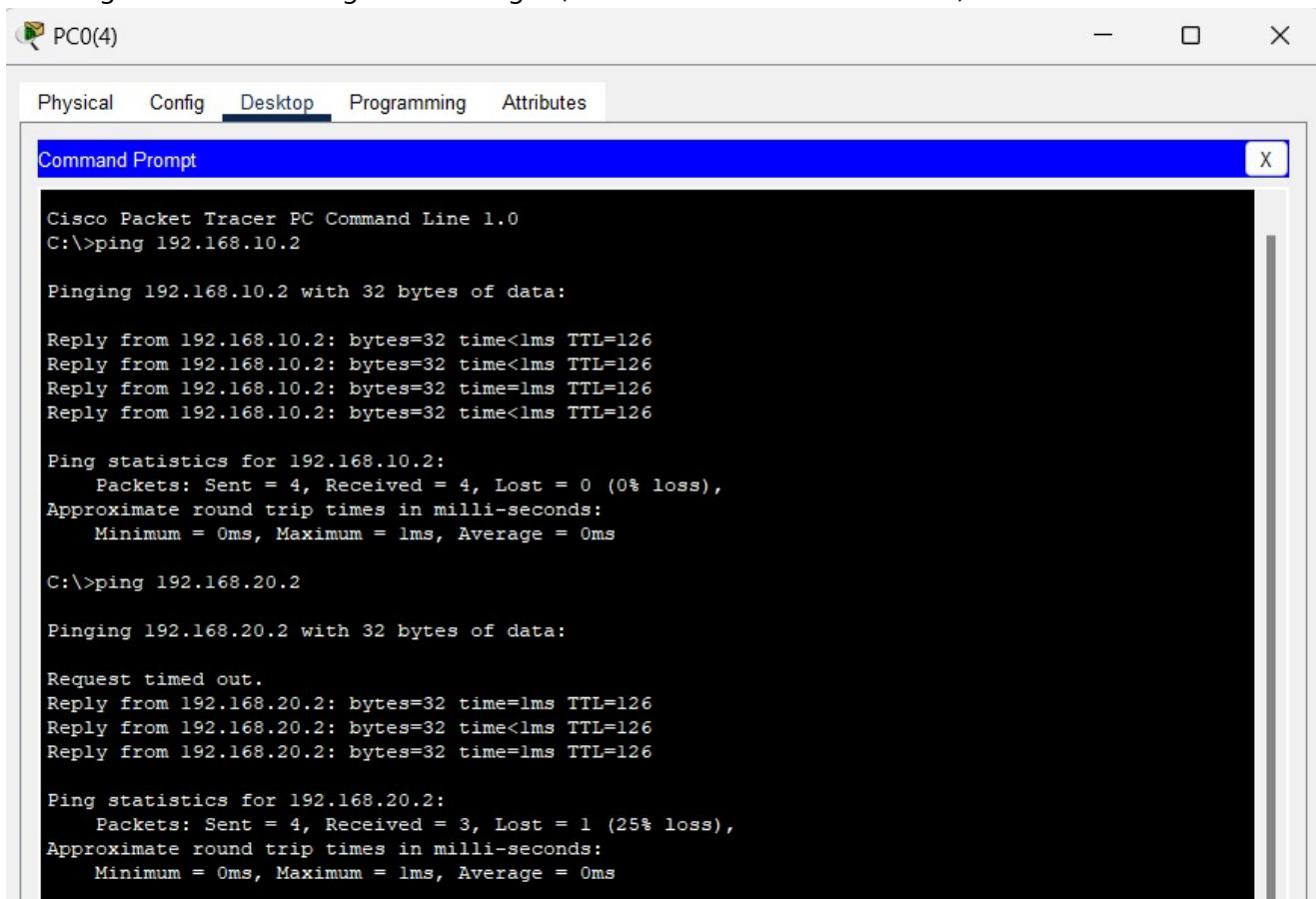
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.40.2: bytes=32 time=1ms TTL=126
Reply from 192.168.40.2: bytes=32 time=1ms TTL=126
Reply from 192.168.40.2: bytes=32 time=5ms TTL=126
Reply from 192.168.40.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

Penjelasan : Pada gambar di atas, terlihat hasil perintah ping yang digunakan untuk menguji koneksi antar VLAN di dua gedung yang berbeda, yaitu dari PC di VLAN 10 di Gedung A ke PC di VLAN 40 di Gedung B. Perintah ping 192.168.40.2 digunakan untuk mengirimkan 5 paket ICMP Echo Request ke alamat IP 192.168.40.2 di Gedung B. Pada percobaan pertama, hasilnya menunjukkan 1 paket yang hilang (25% loss), yang berarti hanya 3 dari 4 paket yang berhasil mendapatkan respons. Round-trip min/avg/max = 0ms/4ms/12ms menunjukkan bahwa waktu perjalanan pulang-pergi paket rata - rata adalah 4ms, dengan waktu maksimum 12ms, yang menunjukkan adanya latensi yang masih wajar meskipun ada sedikit kehilangan paket. Pada percobaan kedua, hasilnya menunjukkan 0% packet loss, yang berarti semua paket yang dikirim berhasil mendapatkan respons, dengan round-trip min/avg/max = 1ms/2ms/5ms, yang menunjukkan latensi yang lebih rendah dan sangat baik antara kedua perangkat. Hasil uji ping ini mengindikasikan bahwa meskipun ada sedikit gangguan pada percobaan pertama, koneksi antar VLAN di dua gedung (Gedung A dan Gedung B) sudah stabil dan dapat berjalan dengan baik pada percobaan kedua.



The screenshot shows a window titled "Command Prompt" from Cisco Packet Tracer. It displays two ping operations. The first operation is "ping 192.168.10.2" which shows four successful replies with TTL=126 and round-trip times between 0ms and 1ms. The second operation is "ping 192.168.20.2" which shows three successful replies and one lost packet (25% loss) with round-trip times between 0ms and 5ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time<1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Penjelasan : Pada gambar di atas, terlihat hasil perintah ping yang digunakan untuk menguji koneksi antar VLAN di dua gedung yang berbeda, yaitu dari PC di VLAN 40 di Gedung B ke PC di VLAN 10 dan 20 di Gedung A. Perintah ping 192.168.10.2 digunakan untuk mengirimkan 4 paket ICMP Echo Request ke alamat IP 192.168.10.2 yang berada di Gedung A (VLAN 10). Hasilnya menunjukkan bahwa semua paket berhasil diterima tanpa kehilangan paket (0% loss), dengan round-trip min/avg/max = 0ms/1ms/1ms, yang menunjukkan latensi yang sangat rendah dan koneksi yang stabil antara PC di Gedung B dan PC di VLAN 10 di Gedung A.

Selanjutnya, perintah ping 192.168.20.2 digunakan untuk mengirimkan 4 paket ICMP Echo Request ke alamat IP 192.168.20.2 yang berada di VLAN 20 Gedung A. Pada percobaan ini, terlihat bahwa 1 paket hilang (25% loss), yang berarti hanya 3 dari 4 paket berhasil mendapatkan respons. Round-trip min/avg/max = 0ms/1ms/5ms menunjukkan waktu perjalanan pulang-pergi paket dengan waktu maksimum 5ms, yang masih tergolong baik meskipun ada sedikit kehilangan paket. Secara keseluruhan, hasil uji ping ini menunjukkan bahwa koneksi antar VLAN di Gedung A dan Gedung B berjalan dengan baik, meskipun ada sedikit gangguan pada komunikasi dengan VLAN 20 di Gedung A.

### Perbedaan Routing Statis dan Dinamis

Routing statis dan routing dinamis punya perbedaan yang cukup besar dalam cara kerjanya. Routing statis artinya kita harus menentukan jalur ke setiap jaringan secara manual. Ini cocok untuk jaringan kecil yang tidak sering berubah, karena lebih sederhana dan tidak membebani kerja router. Tapi, kalau ada perubahan di jaringan, kita harus mengubah konfigurasinya sendiri. Jadi kurang fleksibel dan cukup merepotkan kalau jaringannya besar atau sering berubah.

Sebaliknya, routing dinamis seperti OSPF ini lebih pintar karena bisa menyesuaikan jalur secara otomatis. Kalau ada perubahan seperti kabel putus atau ada router baru, OSPF bisa mencari jalur bary sendiri tanpa perlu diatur ulang. Ini sangat membantu di jaringan besar atau antar-gedung seperti pada tugas ini. Kekurangannya, routing dinamis sedikit lebh berat untuk router karena memerlukan lebih banyak proses. Tapi secara umum, untuk jaringan yang kompleks dan butuh fleksibilitas, routing dinamis jauh lebih praktis dan efisien dibanding routing statis.

☛ [Implementasi Layanan Jaringan] - [Pekan 13]

☛ [Link File Simulasi Topologi Cisco Packet Tracer](#)

### Konfigurasi CLI untuk DHCP dan DNS

Departemen IT (192.168.10.0/24)

```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp pool IT_POOL
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 192.168.10.254
exit
```

Departemen Keuangan (192.168.20.0/24)

```
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp pool KEUANGAN_POOL
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 192.168.20.254
exit
```

Departemen SDM (192.168.30.0/24)

```
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool SDM_POOL
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 192.168.30.254
exit
```

Server (192.168.60.0/24)

```
ip dhcp excluded-address 192.168.60.1 192.168.60.10
ip dhcp pool SERVER_POOL
```

```
network 192.168.60.0 255.255.255.0
default-router 192.168.60.1
dns-server 192.168.60.254
exit
```

#### Departemen Marketing (192.168.40.0/24)

```
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp pool MARKETING_POOL
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 192.168.40.254
exit
```

#### Departemen Operasional (192.168.50.0/24)

```
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp pool OPERASIONAL_POOL
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 192.168.50.254
exit
```

## Hasil Konfigurasi DHCP dan DNS Router A

The screenshot shows the CLI interface for RouterA. At the top, there are tabs for Physical, Config, CLI (which is selected), and Attributes. Below the tabs, it says "IOS Command Line Interface". A message "Press RETURN to get started." is displayed. The main area contains the output of the "show ip route" command. It starts with a legend for route codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP, i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area, \* - candidate default, U - per-user static route, o - ODR, P - periodic downloaded static route. It then lists routes: Gateway of last resort is 8.8.8.8 to network 0.0.0.0. Routes include: 8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks (C 8.0.0.0/8 is directly connected, GigabitEthernet0/2; L 8.8.8.7/32 is directly connected, GigabitEthernet0/2); 192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks (C 192.168.10.0/24 is directly connected, GigabitEthernet0/0.10; L 192.168.10.1/32 is directly connected, GigabitEthernet0/0.10); 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks (C 192.168.20.0/24 is directly connected, GigabitEthernet0/0.20; L 192.168.20.1/32 is directly connected, GigabitEthernet0/0.20); 192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks (C 192.168.30.0/24 is directly connected, GigabitEthernet0/0.30; L 192.168.30.1/32 is directly connected, GigabitEthernet0/0.30). A "More--" prompt is at the bottom. At the bottom right are "Copy" and "Paste" buttons. At the bottom left is a "Top" button.

```
Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 8.8.8.8 to network 0.0.0.0

 8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     8.0.0.0/8 is directly connected, GigabitEthernet0/2
L     8.8.8.7/32 is directly connected, GigabitEthernet0/2
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L     192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L     192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L     192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
--More--
```

Top

### Penjelasan:

Gambar ini menunjukkan hasil perintah show ip route pada Router A. Pada tampilan ini, seluruh rute yang muncul adalah jaringan yang langsung terhubung (C) dan alamat lokal (L), seperti 192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, dan 8.8.8.0/23. Tidak terlihat adanya rute dinamis seperti OSPF ("O"), sehingga kemungkinan besar Router A belum melakukan konfigurasi OSPF atau belum menerima update OSPF dari router lain. Tampilan juga menunjukkan bahwa beberapa interface seperti GigabitEthernet0/2 dan GigabitEthernet0/20 digunakan untuk koneksi langsung ke beberapa subnet.

## Hasil Konfigurasi DHCP dan DNS Router B

```
IOS Command Line Interface

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 GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.50, changed state to up
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.1 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done

Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 192.168.100.1 to network 0.0.0.0

O  192.168.10.0/24 [110/2] via 192.168.100.1, 00:40:00, GigabitEthernet0/0
O  192.168.20.0/24 [110/2] via 192.168.100.1, 00:40:00, GigabitEthernet0/0
O  192.168.30.0/24 [110/2] via 192.168.100.1, 00:40:00, GigabitEthernet0/0
    192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.40.0/24 is directly connected, GigabitEthernet0/1.40
L    192.168.40.1/32 is directly connected, GigabitEthernet0/1.40
    192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.50.0/24 is directly connected, GigabitEthernet0/1.50
L    192.168.50.1/32 is directly connected, GigabitEthernet0/1.50
O  192.168.60.0/24 [110/2] via 192.168.100.1, 00:40:00, GigabitEthernet0/0
    192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.100.0/30 is directly connected, GigabitEthernet0/0
--More--
```

Top

### Penjelasan:

Gambar ini menampilkan hasil perintah show ip route pada Router B. Terlihat bahwa Router B telah berhasil membentuk koneksi OSPF (ditandai dengan log OSPF yang berhasil mencapai status FULL) dan menerima beberapa rute dari protokol OSPF, seperti jaringan 192.168.10.0/24, 192.168.30.0/24, dan 192.168.60.0/24, yang diterima melalui gateway 192.168.100.1. Ini dibuktikan dengan adanya label "O" di awal baris rute tersebut, menandakan bahwa rute tersebut dipelajari melalui OSPF. Selain itu, terdapat beberapa jaringan lokal (L) dan yang terhubung langsung (C), seperti 192.168.50.0/24 dan 192.168.100.0/30. Artinya, Router B sudah memiliki konfigurasi routing dinamis yang baik dan dapat mengenali jaringan di luar koneksi langsungnya.

### Konfigurasi CLI untuk NAT

```

! Konfigurasi NAT Overload (PAT) Lengkap
! Langkah 1: Buat Access-List untuk menentukan IP lokal yang di-NAT
access-list 100 permit ip 192.168.0.0 0.0.255.255 any

! Langkah 2: Terapkan NAT Overload menggunakan interface publik
ip nat inside source list 100 interface GigabitEthernet0/1 overload

! Langkah 3: Tentukan interface mana yang 'inside' dan 'outside'
interface GigabitEthernet0/0    ! Interface ke jaringan lokal (Gedung A/B)
ip address 192.168.1.1 255.255.0.0
ip nat inside
no shutdown
exit

interface GigabitEthernet0/1    ! Interface ke ISP
ip address dhcp
ip nat outside
no shutdown
exit

```

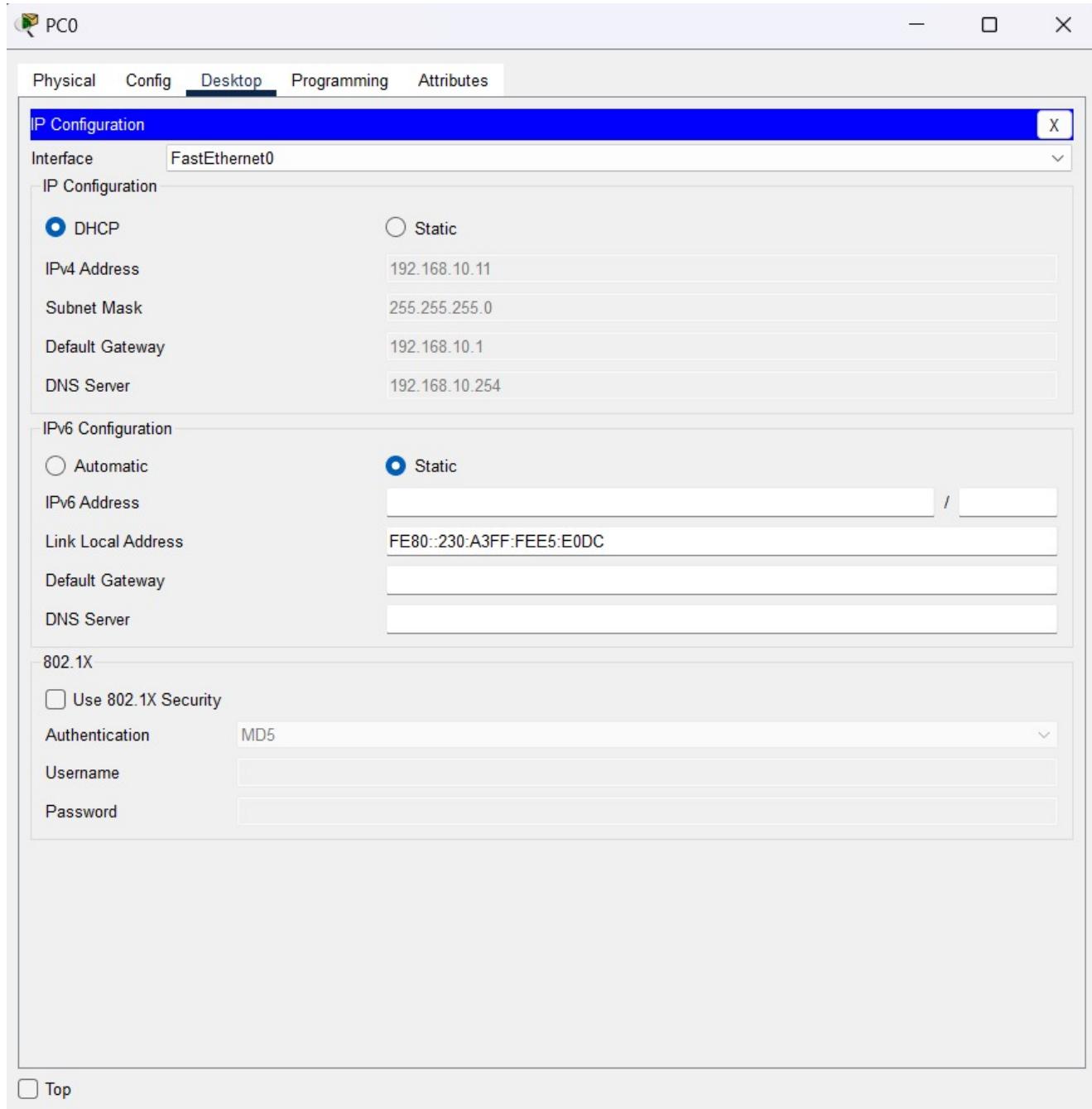
Konfigurasi di atas merupakan langkah-langkah lengkap untuk menerapkan *NAT Overload (PAT)* pada perangkat router Cisco. Pada langkah pertama, dibuat access-list dengan nomor 100 yang memberikan izin untuk seluruh alamat IP dalam rentang 192.168.0.0/16 agar dapat diteruskan ke jaringan luar. Langkah ini bertujuan untuk mendefinisikan alamat-alamat IP lokal (private) yang akan dikonversi menggunakan NAT.

Selanjutnya, pada langkah kedua, konfigurasi NAT Overload dilakukan dengan perintah `ip nat inside source list 100 interface GigabitEthernet0/1 overload`. Perintah ini menginstruksikan router untuk menggunakan IP publik dari interface GigabitEthernet0/1 (yang terhubung ke ISP) sebagai alamat asal, dan memungkinkan banyak perangkat internal menggunakan satu alamat IP publik tersebut melalui teknik port address translation.

Pada langkah ketiga, ditentukan arah lalu lintas NAT dengan menandai interface GigabitEthernet0/0 sebagai `ip nat inside`, karena terhubung ke jaringan lokal (misalnya Gedung A atau B), dan memberikan alamat IP statis 192.168.1.1/16. Sedangkan interface GigabitEthernet0/1 yang mengarah ke ISP diberi perintah `ip nat outside` serta dikonfigurasi untuk menerima alamat IP publik secara otomatis melalui DHCP. Perintah `no shutdown` pada kedua interface memastikan bahwa koneksi aktif. Dengan konfigurasi ini, router dapat meneruskan lalu lintas dari jaringan lokal ke internet dengan efisien menggunakan satu IP publik.

### **Pengujian Alokasi IP Dinamis**

Pengujian dilakukan dengan mengaktifkan DHCP pada perangkat client, sehingga perangkat dapat memperoleh alamat IP secara otomatis dari DHCP Server yang telah dikonfigurasi.



Berikut adalah detail parameter yang diperoleh melalui DHCP:

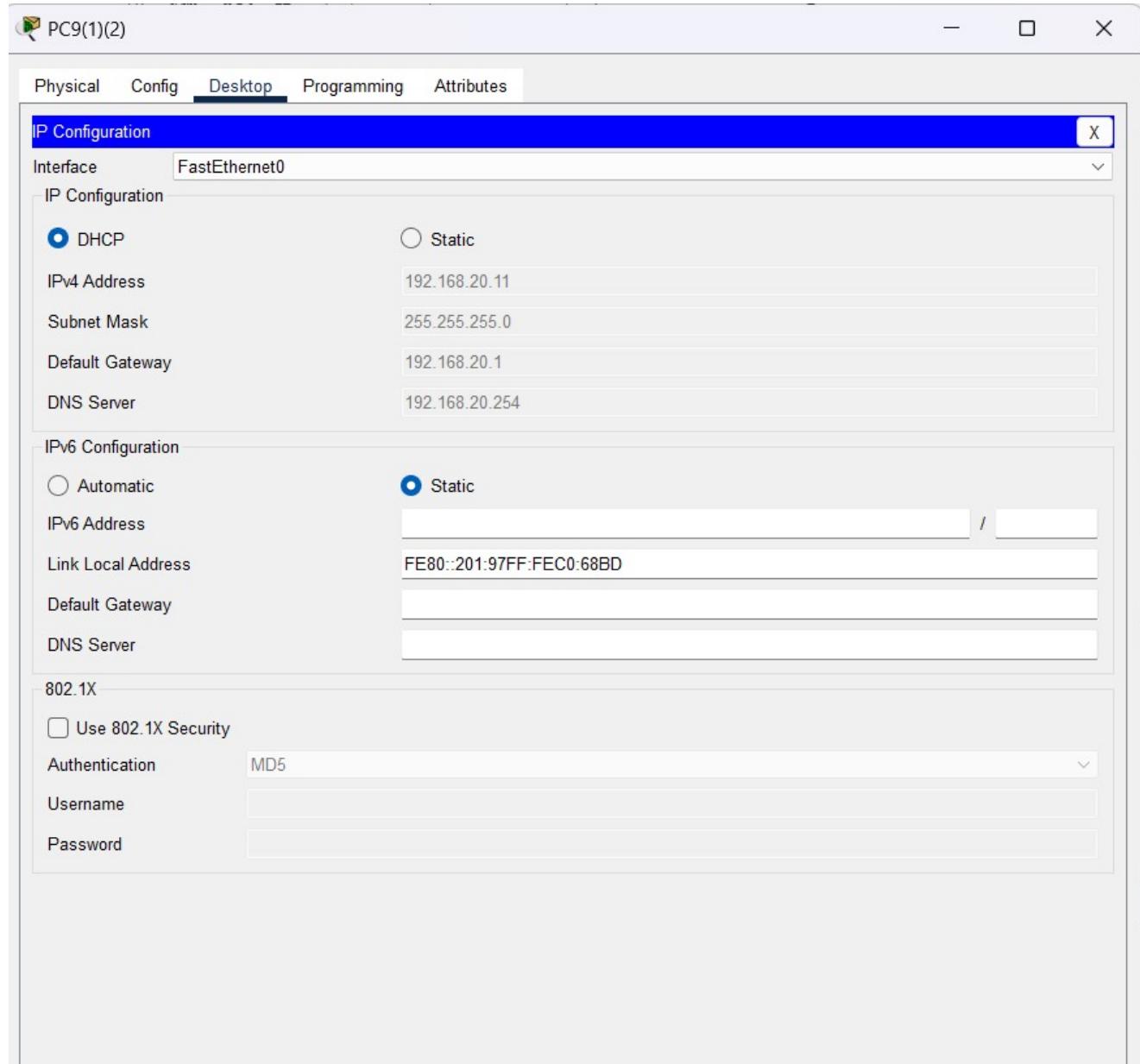
- Alamat IP yang diterima: 192.168.10.11
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.1
- DNS Server: 192.168.10.254
- Status DHCP Request: Berhasil

Hasil konfigurasi DHCP menunjukkan bahwa perangkat klien berhasil memperoleh parameter jaringan secara otomatis dari DHCP Server yang dikelola oleh *Departemen IT*. Perangkat menerima alamat IP 192.168.10.11 dengan subnet mask 255.255.255.0, yang menunjukkan bahwa klien berada dalam jaringan dengan rentang IP 192.168.10.0/24. Default gateway yang diterima adalah 192.168.10.1, yang digunakan sebagai jalur utama untuk komunikasi keluar dari jaringan lokal. Selain itu, DNS Server yang diberikan

adalah 192.168.10.254, yang berperan dalam menerjemahkan nama domain menjadi alamat IP untuk akses layanan internet atau internal.

Status DHCP Request yang ditampilkan adalah berhasil, menandakan bahwa proses pemberian alamat IP berjalan dengan baik tanpa kendala. Hal ini menunjukkan bahwa DHCP Server berfungsi optimal dalam mendistribusikan konfigurasi IP secara otomatis, mengurangi kebutuhan konfigurasi manual pada perangkat klien, serta memastikan efisiensi dan konsistensi konfigurasi jaringan internal.

## Departemen Keuangan



Berikut adalah detail parameter yang diperoleh melalui DHCP:

- Alamat IP yang diterima: 192.168.20.11
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.20.1
- DNS Server: 192.168.20.254
- Status DHCP Request: Berhasil

DHCP Server di *Departemen Keuangan* telah berfungsi secara optimal dalam mendistribusikan konfigurasi jaringan kepada perangkat klien. Berdasarkan hasil yang diperoleh, perangkat berhasil menerima alamat IP

192.168.20.11 dengan subnet mask 255.255.255.0, yang menandakan perangkat berada dalam jaringan 192.168.20.0/24. Default gateway yang diberikan adalah 192.168.20.1, memungkinkan perangkat melakukan komunikasi antar jaringan, khususnya akses keluar dari jaringan lokal. Selain itu, DNS Server yang diterima adalah 192.168.20.254, yang berperan penting dalam proses penerjemahan nama domain ke alamat IP.

Status permintaan DHCP tercatat berhasil, menunjukkan bahwa proses pemberian alamat IP berjalan dengan lancar tanpa kendala. Dengan konfigurasi ini, perangkat di Departemen Keuangan dapat langsung terhubung ke jaringan tanpa memerlukan pengaturan manual, sehingga efisiensi dan konsistensi pengelolaan jaringan dapat terjaga. Seluruh parameter yang diberikan sesuai dengan desain jaringan yang telah dirancang khusus untuk departemen ini.

## Departemen SDM

The screenshot shows a software interface for managing network configurations. The title bar says "PC4(2)(1)(1)". The top menu has tabs: Physical, Config, Desktop (which is selected), Programming, and Attributes. The main area is titled "IP Configuration". Under "IP Configuration", there is a section for "FastEthernet0". The "Interface" dropdown is set to "FastEthernet0". The "IP Configuration" section contains fields for IPv4 Address (192.168.30.12), Subnet Mask (255.255.255.0), Default Gateway (192.168.30.1), and DNS Server (192.168.30.254). Below this is an "IPv6 Configuration" section with fields for IPv6 Address (FE80::2E0:8FFF:FE5:4574), Link Local Address, Default Gateway, and DNS Server. At the bottom is a "802.1X" section with a checkbox for "Use 802.1X Security" (unchecked), Authentication (MD5), Username, and Password fields. A "Top" button is at the bottom left.

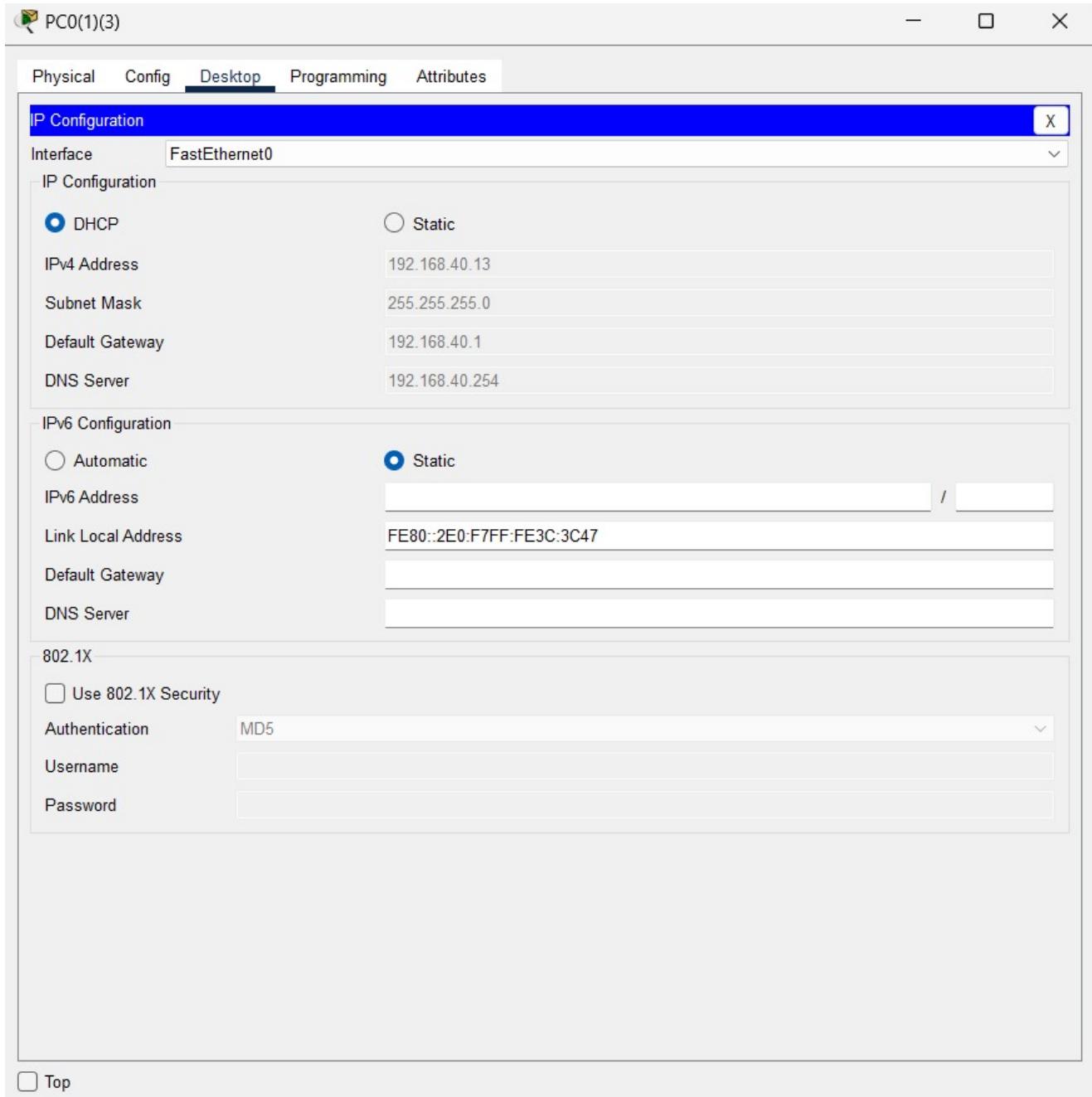
Berikut adalah detail parameter yang diperoleh melalui DHCP:

- Alamat IP yang diterima: 192.168.30.12

- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.30.1
- DNS Server: 192.168.30.254
- Status DHCP Request: Berhasil

Implementasi DHCP di *Departemen Marketing* menunjukkan kinerja yang efektif dalam mendistribusikan konfigurasi jaringan secara otomatis kepada perangkat klien. Perangkat berhasil memperoleh alamat IP 192.168.30.12 dengan subnet mask 255.255.255.0, yang menandakan bahwa perangkat berada di dalam jaringan 192.168.30.0/24. Default gateway yang diberikan, yaitu 192.168.30.1, memungkinkan perangkat melakukan komunikasi ke luar jaringan lokal. Selain itu, perangkat menerima DNS Server 192.168.30.254, yang bertugas menerjemahkan nama domain ke alamat IP untuk mendukung akses ke layanan internet maupun sumber daya internal.

Status DHCP Request: Berhasil menunjukkan bahwa proses permintaan konfigurasi berjalan lancar dan DHCP Server mampu merespons dengan baik. Seluruh parameter yang diterima sudah sesuai dengan rancangan topologi jaringan untuk departemen ini, sehingga menjamin konektivitas internal yang stabil dan efisien tanpa perlu konfigurasi manual pada setiap perangkat. Dengan demikian, DHCP Server berperan penting dalam mendukung kelancaran operasional jaringan di Departemen Marketing.



Berikut adalah detail parameter yang diperoleh melalui DHCP:

- Alamat IP yang diterima: 192.168.40.13
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.40.1
- DNS Server: 192.168.40.254
- Status DHCP Request: Berhasil

Pengujian DHCP di *Departemen Marketing* menunjukkan bahwa server DHCP berhasil mendistribusikan konfigurasi jaringan secara otomatis kepada perangkat klien. Perangkat menerima alamat IP 192.168.40.13 dengan subnet mask 255.255.255.0, yang menunjukkan bahwa perangkat berada dalam jaringan 192.168.40.0/24. Default gateway yang diberikan adalah 192.168.40.1, memungkinkan perangkat menjalin komunikasi antar jaringan, sementara DNS Server 192.168.40.254 digunakan untuk proses resolusi nama domain ke alamat IP.

Status DHCP Request: Berhasil menandakan bahwa proses alokasi IP berjalan tanpa kendala. Seluruh parameter yang diberikan telah sesuai dengan skema jaringan yang dirancang untuk Departemen Marketing, mendukung konektivitas internal yang stabil dan efisien tanpa perlu konfigurasi manual. Konfigurasi ini juga memungkinkan perangkat untuk berkomunikasi dengan layanan eksternal secara lancar.

## Departemen Operasional

The screenshot shows a software interface for managing network configurations. At the top, there are tabs: Physical, Config, Desktop (which is selected), Programming, and Attributes. Below the tabs, the title bar says "IP Configuration". Under "IP Configuration", the interface is set to "FastEthernet0". There are two radio button options: "DHCP" (selected) and "Static". For "DHCP", there are fields for IPv4 Address (192.168.50.11), Subnet Mask (255.255.255.0), Default Gateway (192.168.50.1), and DNS Server (192.168.50.254). For "Static", there are fields for IPv6 Address (FE80::260:47FF:FE33:565E), Link Local Address, Default Gateway, and DNS Server. In the "802.1X" section, there is a checkbox for "Use 802.1X Security" which is unchecked. The "Authentication" method is set to MD5, and there are fields for "Username" and "Password". At the bottom left, there is a "Top" button.

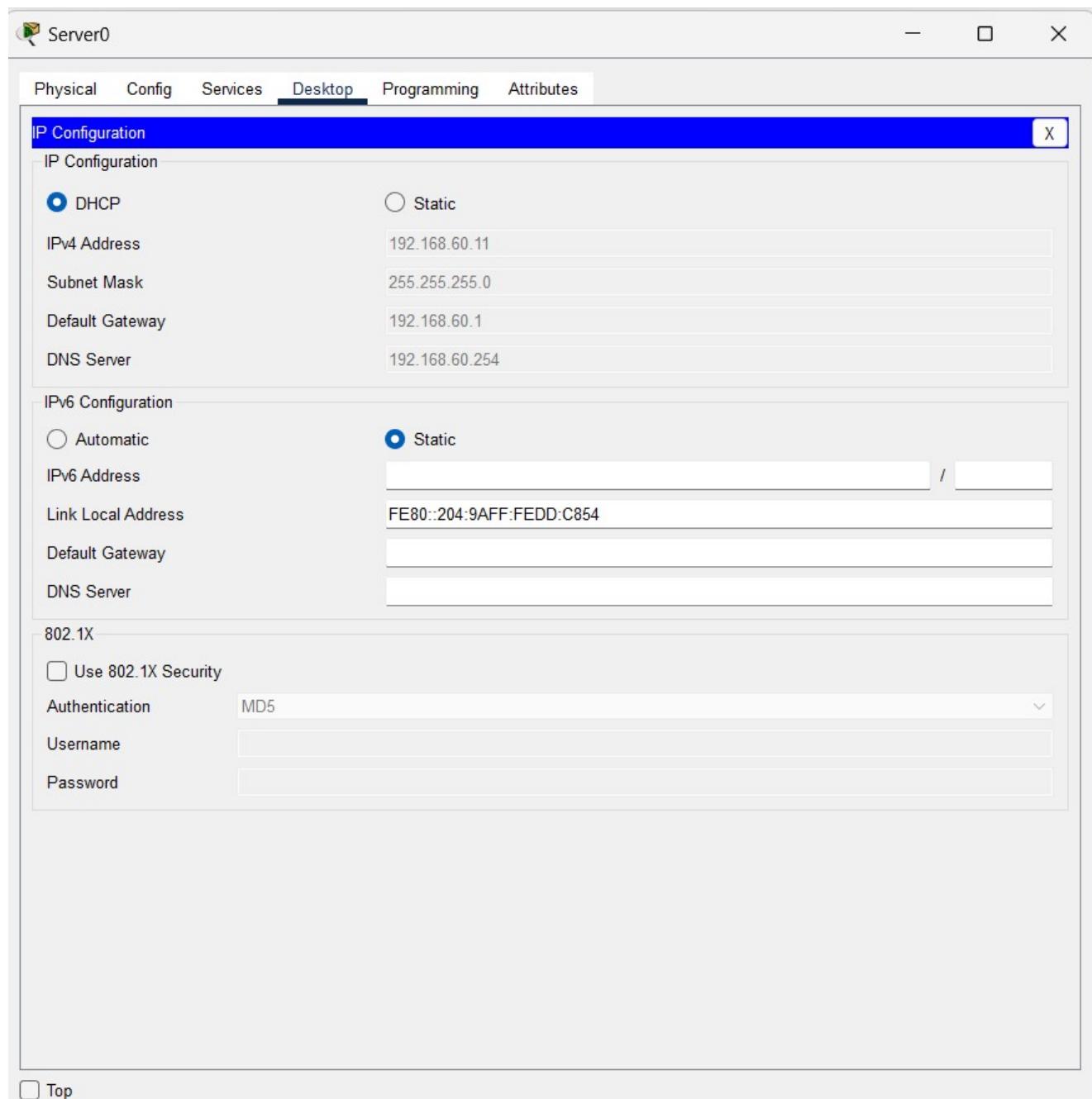
Berikut adalah detail parameter yang diperoleh melalui DHCP:

- Alamat IP yang diterima: 192.168.50.11
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.50.1
- DNS Server: 192.168.50.254
- Status DHCP Request: Berhasil

Pengujian DHCP pada perangkat PC di *Departemen Operasional* menunjukkan hasil yang optimal, di mana perangkat berhasil memperoleh konfigurasi jaringan secara otomatis dari DHCP Server. Perangkat menerima alamat IP 192.168.50.11, dengan subnet mask 255.255.255.0, yang mengindikasikan bahwa perangkat berada dalam jaringan 192.168.50.0/24. Selain itu, default gateway 192.168.50.1 telah diterapkan, berperan sebagai jalur keluar menuju jaringan lain di luar subnet lokal.

DNS Server yang diterima adalah 192.168.50.254, yang memungkinkan perangkat untuk melakukan resolusi nama domain. Status DHCP Request: Berhasil menandakan bahwa proses permintaan dan penerimaan konfigurasi jaringan telah dilakukan tanpa hambatan. Dengan konfigurasi ini, perangkat di Departemen Operasional dapat terhubung secara efisien ke jaringan internal, serta dapat mengakses layanan eksternal dengan bantuan DNS publik jika dikonfigurasi lebih lanjut.

## Server



The screenshot shows a window titled "Server0" with a tab bar at the top: Physical, Config, Services, Desktop, Programming, Attributes. The "Desktop" tab is selected. Below the tabs, there is a section titled "IP Configuration". Under "IP Configuration", there are two options: "DHCP" (selected) and "Static". For "DHCP", the "IPv4 Address" is 192.168.60.11, "Subnet Mask" is 255.255.255.0, "Default Gateway" is 192.168.60.1, and "DNS Server" is 192.168.60.254. Under "IPv6 Configuration", there are two options: "Automatic" (selected) and "Static". For "Static", the "IPv6 Address" field contains "FE80::204:9AFF:FEED:C854". Below these sections is a "802.1X" section with a checkbox for "Use 802.1X Security" which is unchecked. The "Authentication" dropdown is set to "MD5". There are also fields for "Username" and "Password". At the bottom left of the window, there is a "Top" button.

Berikut adalah detail parameter yang diperoleh melalui DHCP:

- Alamat IP yang diterima: 192.168.60.11

- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.60.1
- DNS Server: 192.168.60.254
- Status DHCP Request: Berhasil

Berdasarkan pengujian DHCP, Server0 berhasil menerima konfigurasi jaringan secara otomatis tanpa perlu pengaturan manual. Alamat IP yang diberikan adalah 192.168.60.11, yang menunjukkan bahwa server berada di dalam jaringan 192.168.60.0/24, dengan subnet mask 255.255.255.0, yang menandakan bahwa server dapat berkomunikasi dengan perangkat lain dalam jaringan lokal yang sama. Default gateway 192.168.60.1 berfungsi sebagai jalur keluar dari jaringan lokal menuju jaringan lainnya, termasuk akses ke internet. DNS Server 192.168.60.254 bertugas untuk memfasilitasi proses resolusi nama domain.

Status DHCP Request: Berhasil menandakan bahwa perangkat telah berhasil memperoleh pengaturan jaringan secara otomatis dan siap digunakan dalam lingkungan jaringan tersebut. Server ini siap untuk berkomunikasi dengan perangkat lainnya di jaringan internal maupun mengakses layanan eksternal dengan lancar.

### **Perbaikan Trunk**

The screenshot shows a CLI session on a Cisco switch. The user is configuring the interface FastEthernet0/5 to switchport mode access, setting the native VLAN to 30. They then configure the interface FastEthernet0/21 to switchport mode access, setting the native VLAN to 99. Both configurations result in a warning message: "%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch FastEthernet0/5 (30)." After exiting configuration mode, the user sees a message indicating 'Switch con0 is now available' and is prompted to press RETURN to start.

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch FastEthernet0/5 (30).

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/21
Switch(config-if)#switchport mode access
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#exit
Switch(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch
FastEthernet0/5 (30).

Switch con0 is now available

Press RETURN to get started.
```

[Copy](#)

[Paste](#)

[Top](#)

Gambar di atas menunjukkan proses konfigurasi trunk pada switch jaringan melalui antarmuka baris perintah (CLI). Dalam proses ini, dilakukan sejumlah langkah untuk memastikan koneksi trunk berfungsi dengan baik dan bebas dari gangguan. Pada tahap awal, muncul peringatan terkait ketidaksesuaian VLAN native antara dua switch yang terhubung, yang berpotensi menyebabkan gangguan komunikasi antar perangkat.

Untuk mengatasi permasalahan tersebut, dilakukan pengaturan ulang pada interface FastEthernet, termasuk penetapan mode akses dan trunk, serta pengaturan VLAN yang diizinkan melalui trunk. Selain itu, VLAN native pada port trunk diperbarui menjadi VLAN 99 untuk memastikan kompatibilitas konfigurasi antar perangkat.

Meskipun pesan peringatan masih muncul setelah konfigurasi diperbarui, langkah-langkah ini bertujuan untuk meningkatkan kestabilan koneksi trunk serta memastikan pengelolaan lalu lintas data antar VLAN dapat berjalan secara optimal. Konfigurasi ini merupakan bagian penting dalam menjaga efisiensi dan

stabilitas jaringan secara keseluruhan. Jika diperlukan, analisis tambahan dapat disertakan dalam laporan untuk menjelaskan dampak dari perubahan konfigurasi terhadap kinerja jaringan.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/5 (30), with Switch
FastEthernet0/21 (99).

% Incomplete command.
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

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

Switch(config-if)#switchport trunk allowed
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/7 (1), with Switch
FastEthernet0/11 (99).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (10), with Switch
FastEthernet0/21 (1).

% Incomplete command.
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#ex
Switch(config)#interface FastEthernet0/24
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (10), with Switch
FastEthernet0/21 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (20), with Switch
FastEthernet0/21 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (20), with Switch
FastEthernet0/6 (1).

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#ex
```

[Top](#)

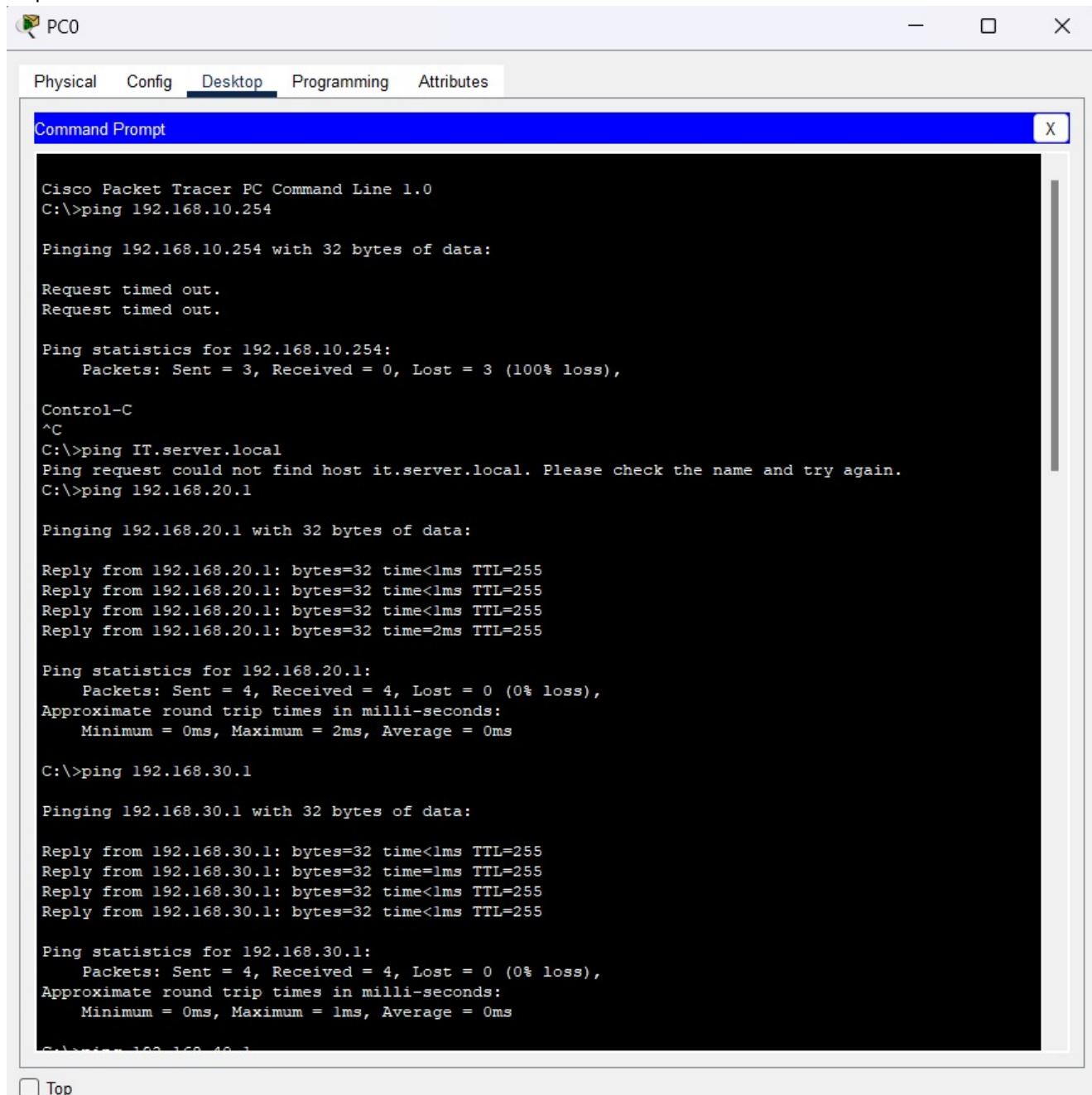
Gambar ini menampilkan proses konfigurasi trunk pada switch jaringan menggunakan antarmuka baris perintah (CLI). Dalam gambar tersebut terlihat sejumlah perintah yang digunakan untuk mengatur VLAN serta koneksi antar perangkat dalam jaringan. Salah satu pesan peringatan yang muncul adalah ketidaksesuaian VLAN native pada port FastEthernet0/21, yang dapat menyebabkan gangguan komunikasi antar switch.

Untuk mengatasi permasalahan tersebut, dilakukan konfigurasi dengan mengubah mode switchport menjadi trunk, menentukan daftar VLAN yang diizinkan, serta menetapkan VLAN native ke VLAN 99. Meskipun setelah konfigurasi dilakukan peringatan VLAN mismatch masih muncul, langkah-langkah ini ditujukan untuk memastikan koneksi trunk dapat berfungsi secara optimal sehingga lalu lintas data antar VLAN berjalan dengan baik.

Laporan ini dapat diperluas dengan analisis tambahan mengenai dampak konfigurasi terhadap performa jaringan serta solusi lebih lanjut yang dapat diterapkan guna meningkatkan stabilitas dan kompatibilitas antar perangkat jaringan.

## Konektivitas ke Jaringan Eksternal melalui NAT

Departemen IT



The screenshot shows a Windows-style application window titled "PC0". The tab bar at the top has tabs for "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". Below the tabs is a "Command Prompt" window with the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 192.168.10.254:
  Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\>ping IT.server.local
Ping request could not find host it.server.local. Please check the name and try again.
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

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
Reply from 192.168.20.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.20.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time=1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

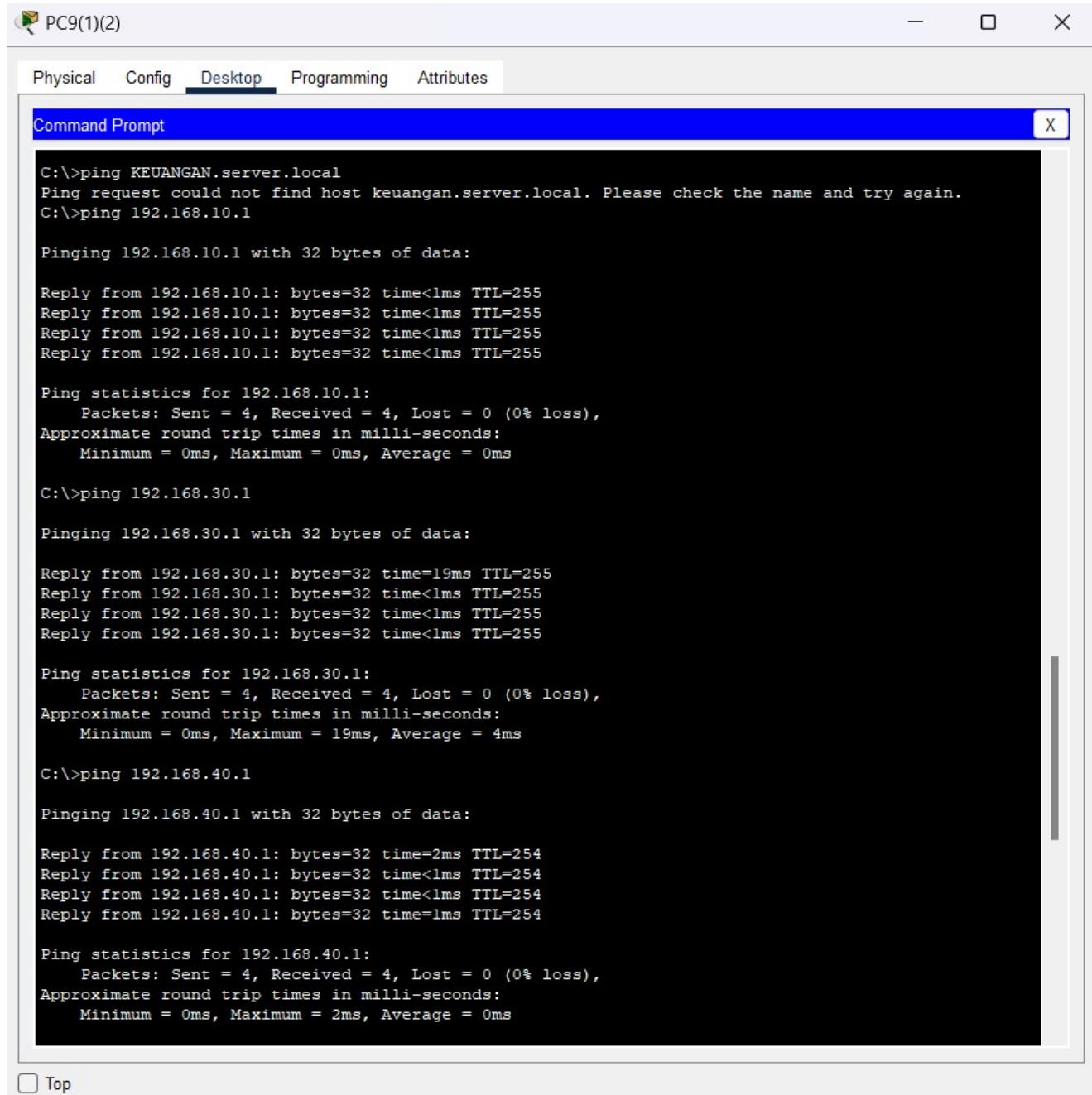
Ping statistics for 192.168.30.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Top

Pada gambar yang ditampilkan, dilakukan pengujian konektivitas jaringan menggunakan perintah ping di Cisco Packet Tracer. Pengujian pertama dilakukan dengan melakukan ping ke alamat IP 192.168.10.254, namun hasilnya menunjukkan bahwa permintaan ping mengalami "Request timed out" yang mengindikasikan tidak ada respons dari perangkat dengan IP tersebut. Statistik ping menunjukkan bahwa dari 4 paket yang dikirim, 3 di antaranya hilang, dengan tingkat kehilangan paket mencapai 100%. Selanjutnya, dilakukan ping ke IT.server.local, namun perintah ini gagal karena nama host IT.server.local tidak dapat ditemukan, dengan pesan kesalahan "Ping request could not find host", yang kemungkinan disebabkan oleh kesalahan konfigurasi DNS atau penulisan nama host yang tidak tepat.

Kemudian, dilakukan ping ke alamat IP 192.168.20.1 dan 192.168.30.1, yang keduanya berhasil dengan baik. Semua 4 paket yang dikirimkan ke masing-masing alamat IP menerima respons tanpa adanya kehilangan paket, serta waktu respons yang sangat cepat, berkisar antara 1 ms hingga 2 ms. Dengan demikian, dapat disimpulkan bahwa koneksi jaringan ke perangkat dengan IP 192.168.20.1 dan 192.168.30.1 berjalan lancar, sementara masalah terjadi pada koneksi ke 192.168.10.254 dan dalam pencarian nama host IT.server.local. Masalah tersebut perlu ditindaklanjuti untuk memperbaiki koneksi jaringan yang tidak stabil pada perangkat tersebut.

## Departemen Keuangan



The screenshot shows a Cisco Packet Tracer interface. At the top, there's a toolbar with icons for PC9(1)(2), Minimize, Maximize, and Close. Below the toolbar, a menu bar has tabs: Physical, Config, Desktop (which is selected and highlighted in blue), Programming, and Attributes. A sub-menu titled 'Command Prompt' is open, showing a black terminal window with white text. The terminal output displays several ping commands and their results:

```
C:\>ping KEUANGAN.server.local
Ping request could not find host keuangan.server.local. Please check the name and try again.

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=19ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 4ms

C:\>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:

Reply from 192.168.40.1: bytes=32 time=2ms TTL=254
Reply from 192.168.40.1: bytes=32 time<1ms TTL=254
Reply from 192.168.40.1: bytes=32 time<1ms TTL=254
Reply from 192.168.40.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

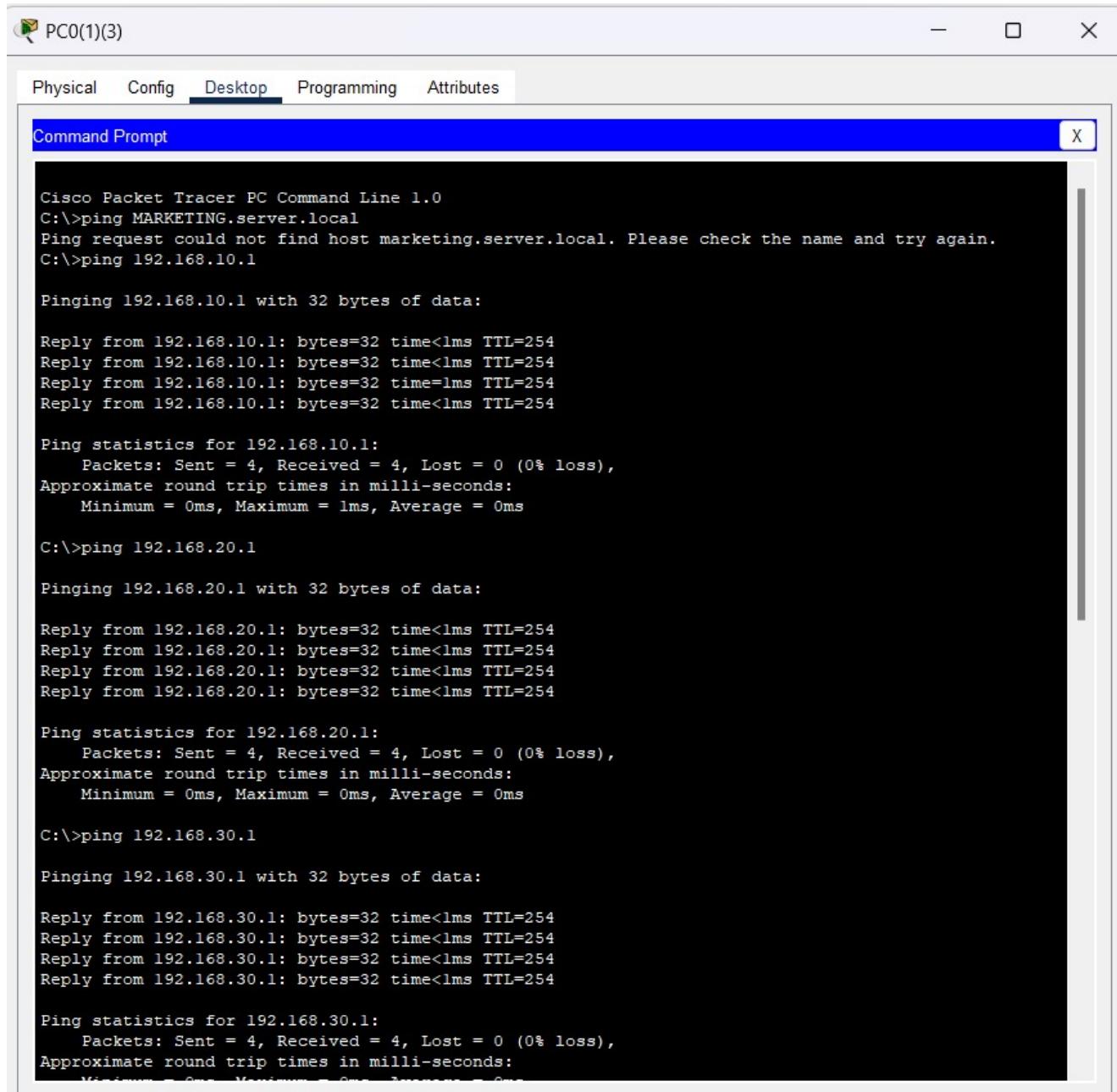
Top

Pada gambar yang ditampilkan, dilakukan pengujian koneksi jaringan menggunakan perintah ping di Cisco Packet Tracer. Pengujian pertama dilakukan dengan melakukan ping ke alamat KEUANGAN.server.local, namun hasilnya menunjukkan pesan kesalahan "Ping request could not find host", yang mengindikasikan bahwa perangkat tidak dapat menemukan host dengan nama KEUANGAN.server.local. Hal ini kemungkinan disebabkan oleh kesalahan konfigurasi DNS atau penulisan nama host yang tidak tepat.

Selanjutnya, dilakukan ping ke alamat 192.168.10.1, dan pengujian ini berhasil dengan baik. Semua 4 paket yang dikirimkan menerima respons tanpa adanya kehilangan paket, serta waktu respons yang sangat cepat (kurang dari 1ms). Kemudian, dilakukan ping ke 192.168.30.1, yang juga berhasil. Semua paket yang dikirimkan diterima kembali tanpa ada yang hilang, dengan waktu respons berkisar antara 19ms hingga kurang dari 1ms.

Terakhir, dilakukan ping ke 192.168.40.1, yang juga berhasil dengan baik. Semua paket yang dikirimkan mendapatkan respons tanpa ada kehilangan paket, dengan waktu respons sekitar 2ms. Dengan demikian, dapat disimpulkan bahwa koneksi jaringan ke perangkat dengan alamat IP 192.168.10.1, 192.168.30.1, dan 192.168.40.1 berjalan dengan lancar tanpa masalah. Namun, terdapat masalah dalam pencarian host KEUANGAN.server.local, yang perlu ditindaklanjuti untuk memastikan konfigurasi DNS atau nama host sudah benar.

## Departemen Marketing



The screenshot shows a Windows-style desktop environment with a taskbar at the top. A window titled "Command Prompt" is open, displaying a series of ping commands and their results. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with "Desktop" currently selected. The command prompt output is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping MARKETING.server.local
Ping request could not find host marketing.server.local. Please check the name and try again.
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=254
Reply from 192.168.10.1: bytes=32 time<1ms TTL=254
Reply from 192.168.10.1: bytes=32 time=1ms TTL=254
Reply from 192.168.10.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=254

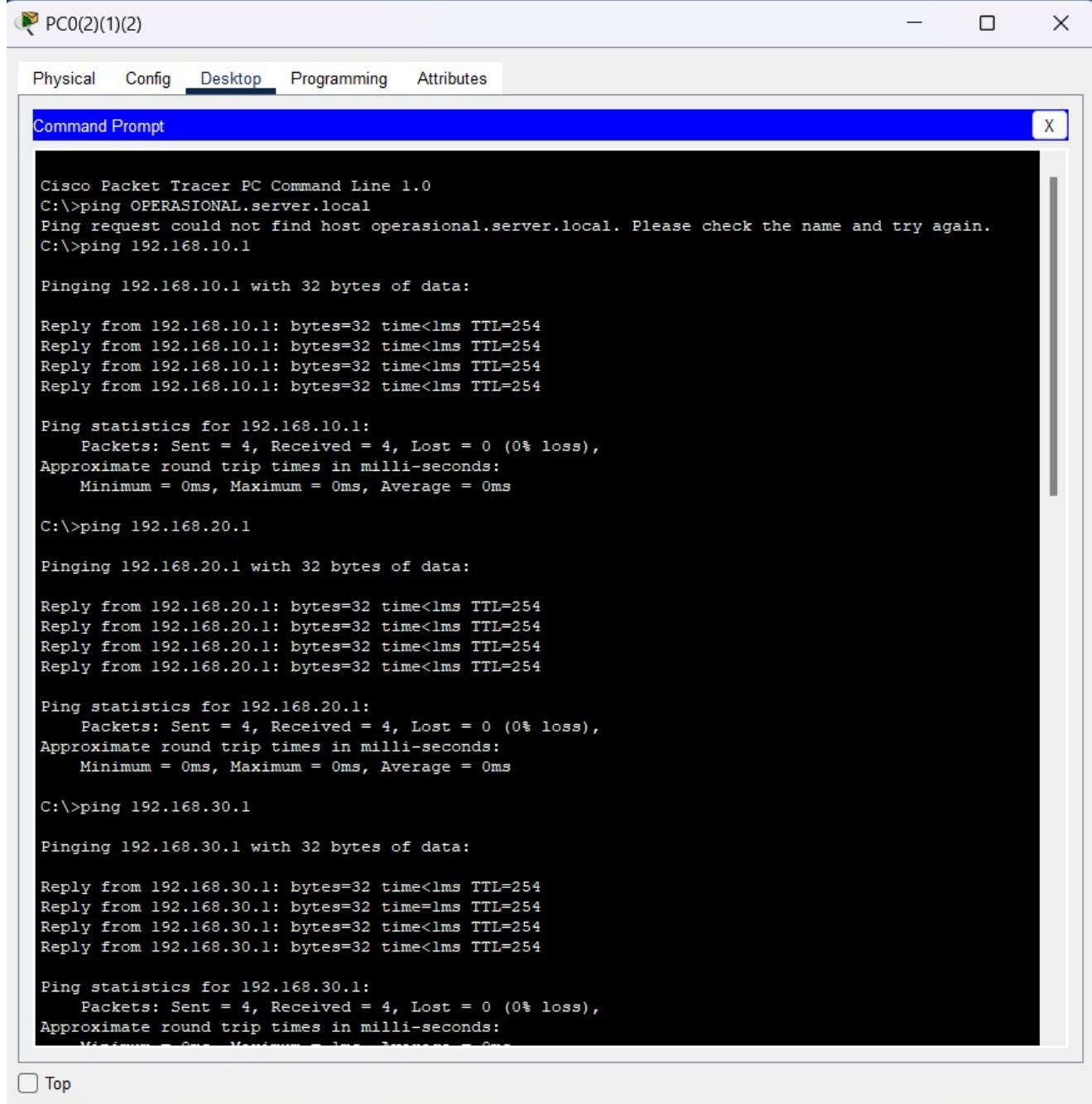
Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pada gambar yang ditampilkan, dilakukan pengujian konektivitas jaringan menggunakan perintah ping di Cisco Packet Tracer. Pengujian pertama dilakukan dengan melakukan ping ke alamat

MARKETING.server.local, namun hasilnya menunjukkan pesan kesalahan "Ping request could not find host", yang mengindikasikan bahwa perangkat tidak dapat menemukan host dengan nama MARKETING.server.local. Hal ini kemungkinan disebabkan oleh kesalahan konfigurasi DNS atau penulisan nama host yang tidak tepat.

Selanjutnya, dilakukan ping ke alamat 192.168.10.1, dan pengujian ini berhasil dengan baik. Semua 4 paket yang dikirimkan menerima respons tanpa adanya kehilangan paket, serta waktu respons yang sangat cepat (kurang dari 1ms). Kemudian, dilakukan ping ke 192.168.20.1, yang juga berhasil. Semua paket yang dikirimkan diterima kembali tanpa ada yang hilang, dengan waktu respons yang sangat cepat (kurang dari 1ms).

Terakhir, dilakukan ping ke 192.168.30.1, yang juga berhasil dengan baik. Semua paket yang dikirimkan mendapatkan respons tanpa ada kehilangan paket, dengan waktu respons yang sangat cepat (kurang dari 1ms). Dengan demikian, dapat disimpulkan bahwa koneksi jaringan ke perangkat dengan alamat IP 192.168.10.1, 192.168.20.1, dan 192.168.30.1 berjalan dengan lancar tanpa masalah. Namun, terdapat masalah dalam pencarian host MARKETING.server.local, yang perlu ditindaklanjuti untuk memastikan konfigurasi DNS atau nama host sudah benar.



The screenshot shows a window titled "Cisco Packet Tracer PC Command Line 1.0". The tabs at the top are "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Programming" being the active tab. Below the tabs is a title bar "Command Prompt" with a close button "X". The main area contains the following command-line output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping OPERASIONAL.server.local
Ping request could not find host operasional.server.local. Please check the name and try again.

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
Reply from 192.168.30.1: bytes=32 time<1ms TTL=254
Reply from 192.168.30.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

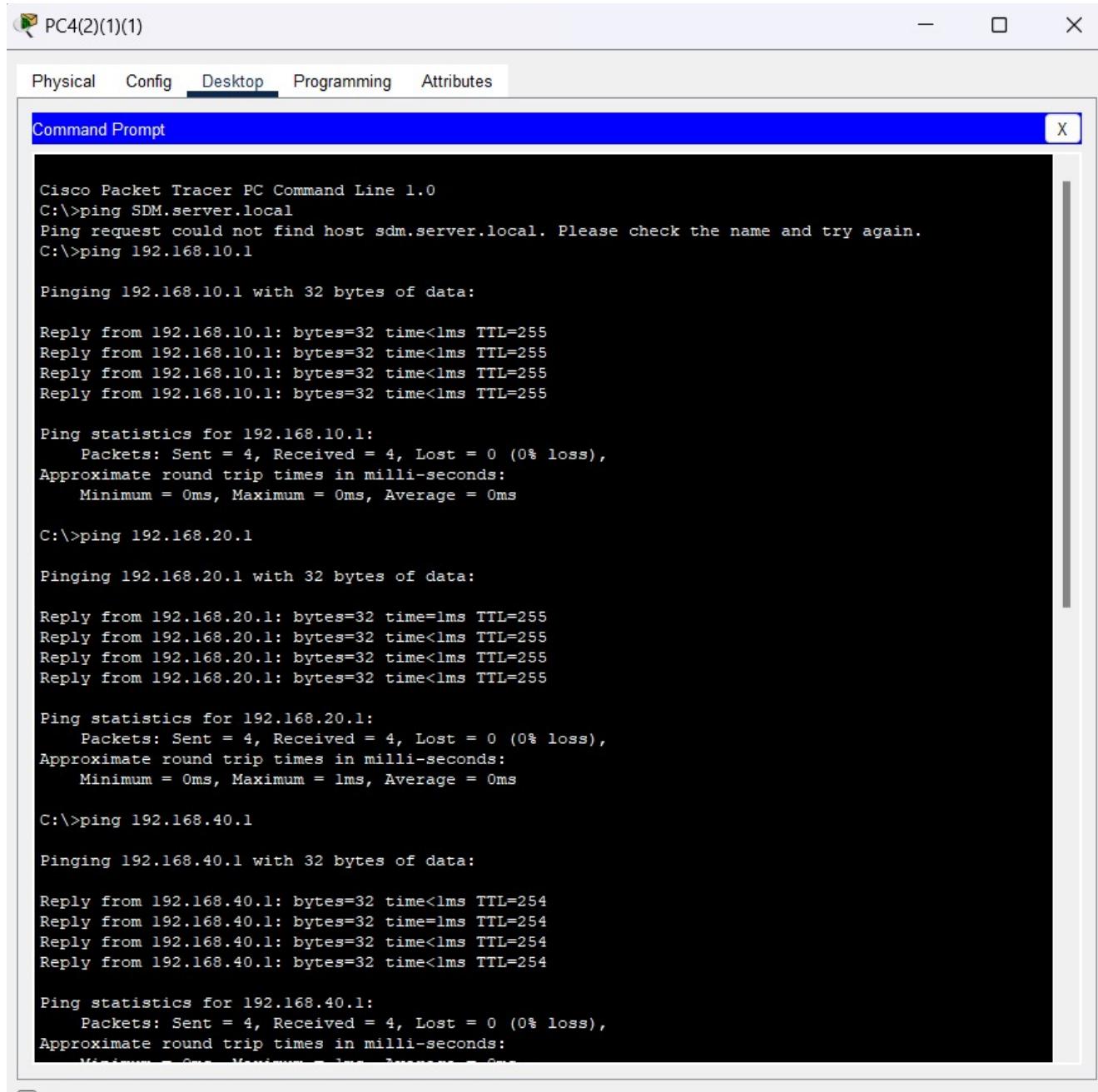
Top

Pada gambar yang ditampilkan, dilakukan pengujian koneksi jaringan menggunakan perintah ping di Cisco Packet Tracer. Pengujian pertama dilakukan dengan melakukan ping ke alamat OPERASIONAL.server.local, namun hasilnya menunjukkan pesan kesalahan "Ping request could not find host", yang mengindikasikan bahwa perangkat tidak dapat menemukan host dengan nama OPERASIONAL.server.local. Hal ini kemungkinan disebabkan oleh kesalahan konfigurasi DNS atau penulisan nama host yang tidak tepat.

Selanjutnya, dilakukan ping ke alamat 192.168.10.1, dan pengujian ini berhasil dengan baik. Semua 4 paket yang dikirimkan menerima respons tanpa adanya kehilangan paket, serta waktu respons yang sangat cepat (kurang dari 1ms). Kemudian, dilakukan ping ke 192.168.20.1, yang juga berhasil. Semua paket yang dikirimkan diterima kembali tanpa ada yang hilang, dengan waktu respons yang sangat cepat (kurang dari 1ms).

Terakhir, dilakukan ping ke 192.168.30.1, yang juga berhasil dengan baik. Semua paket yang dikirimkan mendapatkan respons tanpa ada kehilangan paket, dengan waktu respons yang sangat cepat (kurang dari 1ms). Dengan demikian, dapat disimpulkan bahwa koneksi jaringan ke perangkat dengan alamat IP 192.168.10.1, 192.168.20.1, dan 192.168.30.1 berjalan dengan lancar tanpa masalah. Namun, terdapat masalah dalam pencarian host OPERASIONAL.server.local, yang perlu ditindaklanjuti untuk memastikan konfigurasi DNS atau nama host sudah benar.

## Departemen SDM



The screenshot shows a Windows-style window titled "PC4(2)(1)(1)" with a tab bar containing "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". Below the tabs is a "Command Prompt" window. The command prompt output is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping SDM.server.local
Ping request could not find host sdm.server.local. Please check the name and try again.
C:>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

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

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:

Reply from 192.168.40.1: bytes=32 time<1ms TTL=254
Reply from 192.168.40.1: bytes=32 time=1ms TTL=254
Reply from 192.168.40.1: bytes=32 time<1ms TTL=254
Reply from 192.168.40.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

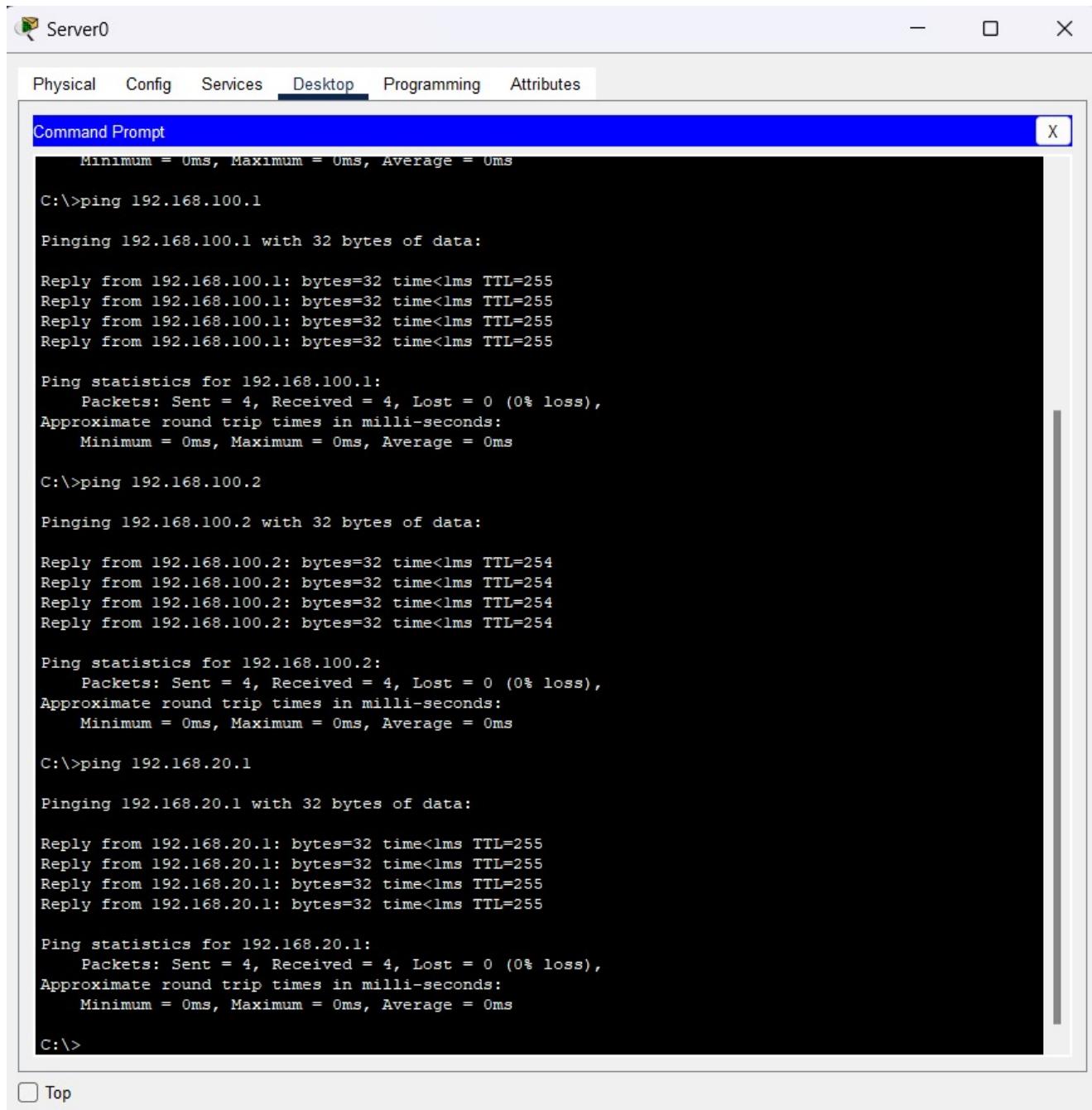
Pada gambar yang ditampilkan, dilakukan pengujian konektivitas jaringan menggunakan perintah ping di Cisco Packet Tracer. Pengujian pertama dilakukan dengan melakukan ping ke alamat SDM.server.local, namun hasilnya menunjukkan pesan kesalahan "Ping request could not find host", yang mengindikasikan bahwa perangkat tidak dapat menemukan host dengan nama SDM.server.local. Masalah ini kemungkinan disebabkan oleh kesalahan konfigurasi DNS atau penulisan nama host yang tidak tepat.

Selanjutnya, dilakukan ping ke alamat 192.168.10.1, dan pengujian ini berhasil dengan baik. Semua 4 paket yang dikirimkan menerima respons tanpa adanya kehilangan paket, serta waktu respons yang

sangat cepat (kurang dari 1ms). Pengujian yang sama juga dilakukan untuk alamat IP 192.168.20.1 dan 192.168.40.1, yang keduanya berhasil dengan hasil yang sama: tidak ada kehilangan paket dan waktu respons yang cepat, berkisar antara kurang dari 1ms.

Dengan demikian, dapat disimpulkan bahwa koneksi jaringan ke perangkat dengan alamat IP 192.168.10.1, 192.168.20.1, dan 192.168.40.1 berjalan dengan lancar tanpa adanya masalah. Namun, terdapat masalah dalam pencarian host SDM.server.local, yang perlu ditindaklanjuti untuk memastikan konfigurasi DNS atau nama host sudah benar.

## Server



The screenshot shows a Windows Server interface titled "Server0". The "Desktop" tab is selected in the top navigation bar. A Command Prompt window is open, displaying the results of several ping commands. The output shows successful pings to 192.168.100.1, 192.168.100.2, and 192.168.20.1 with minimum, maximum, and average latencies near 0ms.

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.100.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

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

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pada gambar yang ditampilkan, dilakukan pengujian koneksi jaringan menggunakan perintah ping di Server0. Pengujian pertama dilakukan dengan melakukan ping ke alamat 192.168.100.1, dan pengujian ini berhasil dengan baik. Semua 4 paket yang dikirimkan menerima respons tanpa adanya kehilangan paket, serta waktu respons yang sangat cepat (kurang dari 1ms).

Selanjutnya, dilakukan ping ke alamat 192.168.100.2, yang juga berhasil dengan baik. Semua paket yang dikirimkan diterima kembali tanpa ada yang hilang, dengan waktu respons yang sangat cepat (kurang dari 1ms). Kemudian, dilakukan ping ke 192.168.20.1, yang juga berhasil. Semua paket yang dikirimkan diterima kembali tanpa ada yang hilang, dengan waktu respons yang sangat cepat (kurang dari 1ms).

Dengan demikian, dapat disimpulkan bahwa koneksi jaringan ke perangkat dengan alamat IP 192.168.100.1, 192.168.100.2, dan 192.168.20.1 berjalan dengan lancar tanpa masalah. Semua pengujian menunjukkan 0% packet loss dan waktu respons yang sangat cepat, menandakan tidak adanya masalah dalam konektivitas jaringan antara perangkat-perangkat tersebut.

### **Kendala**

1. Terjadi kesulitan dalam mengkonfigurasi CLI untuk DHCP di Departemen SDM akibat kesalahan pada konfigurasi trunk sebelumnya, yang mengakibatkan kegagalan pada pengaturan DHCP. Hal ini mempengaruhi alokasi alamat IP otomatis di jaringan tersebut.
2. Saat dilakukan pengujian ping ke DNS untuk server internal, pengujian gagal dan perangkat tidak dapat terhubung ke DNS server, yang menunjukkan adanya masalah dalam resolusi nama domain untuk server internal.

RouterA

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Press RETURN to get started.

Router>show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 8.8.8.8

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags     Age Type   Address(es)
Router>ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router>enable
Router#ping google.com
Translating "google.com"...domain server (8.8.8.8)
% Unrecognized host or address or protocol not running.

Router#
```

Top

RouterB

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 8.8.8.8

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags     Age Type   Address(es)
Router#ping google.com
Translating "google.com"...domain server (8.8.8.8)
% Unrecognized host or address or protocol not running.
```

3. Perintah show ip nat berhasil dieksekusi, namun hasil yang ditampilkan tidak sesuai dengan yang diharapkan. Tidak ada informasi yang relevan atau hasil yang lengkap mengenai status NAT yang seharusnya tersedia.

#### ↳ [Implementasi Keamanan & Pengujian] - [Pekan 14]

## Dokumentasi Konfigurasi ACL

### Konfigurasi ACL GEDUNG A (Router A)

```
Router> enable
Router# configure terminal

!ACL 101 - Departemen Keuangan!
access-list 101 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255      !
Blokir ke Marketing
access-list 101 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255      !
Blokir ke Operasional
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255      !
Boleh ke SDM
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255      !
Boleh ke Server Farm
access-list 101 permit ip any any

!ACL 102 - Departemen SDM!
access-list 102 deny ip 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255
! Blokir ke semua Server
access-list 102 permit ip 192.168.30.0 0.0.0.255 host 192.168.60.20
! Kecuali ke server SDM
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
! Ke IT
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
! Ke Keuangan
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
! Ke Marketing
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
! Ke Operasional
access-list 102 permit ip any any

!Terapkan ACL di Router A !
interface GigabitEthernet0/0.20
  ip access-group 101 in
exit

interface GigabitEthernet0/0.30
  ip access-group 102 in
exit

end
write memory
```

### Konfigurasi ACL GEDUNG B (Router B)

```
Router> enable
Router# configure terminal

!ACL 103 - Departemen Marketing & Operasional !
access-list 103 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255      !
Marketing ke Keuangan
access-list 103 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255      !
Operasional ke Keuangan
access-list 103 permit ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255      !
Marketing ke Server Farm
access-list 103 permit ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255      !
Operasional ke Server Farm
access-list 103 permit ip any any

! Terapkan ACL di Router B !
interface GigabitEthernet0/1.40
  ip access-group 103 in
exit

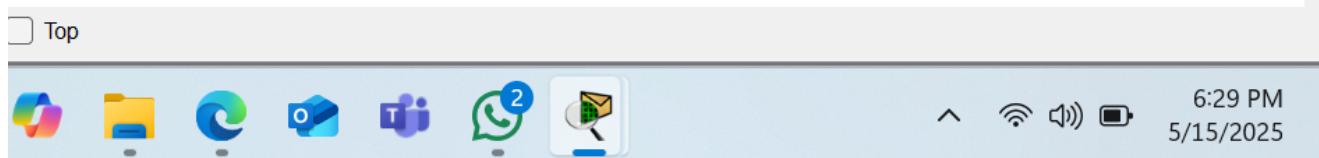
interface GigabitEthernet0/1.50
  ip access-group 103 in
exit

end
write memory
```

## Konfigurasi ACL di CLI Router A

Pada gambar Router A terlihat konfigurasi router utama jaringan perusahaan. Kode konfigurasi kemungkinan mencakup implementasi routing protokol seperti OSPF atau EIGRP untuk routing dinamis, konfigurasi NAT/PAT untuk translasi alamat jaringan, dan implementasi kebijakan QoS untuk klasifikasi dan prioritas lalu lintas. Tujuannya adalah menyediakan routing efisien dan aman antar segment jaringan perusahaan. Hasilnya adalah koneksi yang mulus antara departemen dengan latensi minimal, traffic management yang optimal untuk berbagai jenis aplikasi, dan kemampuan untuk menyesuaikan secara dinamis dengan perubahan topologi jaringan.

## Konfigurasi ACL di CLI Router B



```
RouterB Physical Config CLI Attributes
IOS Command Line Interface

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)

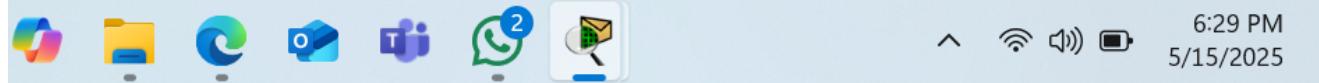
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.50, changed state to up

00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.1 on GigabitEthernet0/0 from
LOADING to FULL, Loading Done

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/z.
Router(config)#access-list 103 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 103 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config)#access-list 103 permit ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255
Router(config)#access-list 103 permit ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255
Router(config)#access-list 103 permit ip any any
Router(config)#interface GigabitEthernet0/1.40
Router(config-subif)#ip access-group 103 in
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/1.50
Router(config-subif)#ip access-group 103 in
Router(config-subif)#exit
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Router#
```

Copy Paste



6:29 PM  
5/15/2025

Pada gambar Router B terlihat konfigurasi router sekunder atau backup. Kode konfigurasi mungkin mencakup implementasi HSRP (Hot Standby Router Protocol) atau GLBP (Gateway Load Balancing Protocol) untuk redundansi gateway, konfigurasi BGP untuk koneksi multi-homing ke penyedia internet, dan implementasi IPv6 dual-stack untuk transisi jaringan yang mulus. Tujuannya adalah memastikan ketersediaan koneksi internet yang konstan dan distribusi beban yang optimal. Hasilnya adalah infrastruktur routing yang tangguh dan skalabel dengan kemampuan untuk menangani kegagalan perangkat tanpa gangguan layanan, manajemen bandwidth yang efisien, dan persiapan untuk adopsi teknologi networking masa depan.

### Matriks Pengujian ACL (Hasil Pengujian ACL Berdasarkan IP)

Sumber: Departemen IT – 192.168.10.14

No	Tujuan	Hasil Ping	Keterangan
1	Keuangan (192.168.20.15)	Reply from 192.168.20.15	<input checked="" type="checkbox"/> Diizinkan (akses penuh)
2	SDM (192.168.30.11)	Reply from 192.168.30.11	<input checked="" type="checkbox"/> Diizinkan
3	Marketing (192.168.40.12)	Reply from 192.168.40.12	<input checked="" type="checkbox"/> Diizinkan
4	Operasional (192.168.50.12)	Reply from 192.168.50.12	<input checked="" type="checkbox"/> Diizinkan
5	Server Farm (192.168.60.11)	Reply from 192.168.60.11	<input checked="" type="checkbox"/> Diizinkan

Sumber: Departemen Keuangan – 192.168.20.15

No	Tujuan	Hasil Ping	Keterangan
1	IT (192.168.10.14)	Reply from 192.168.10.14	<input checked="" type="checkbox"/> Diizinkan
2	SDM (192.168.30.11)	Reply from 192.168.30.11	<input checked="" type="checkbox"/> Diizinkan
3	Marketing (192.168.40.12)	Destination host unreachable	<input checked="" type="checkbox"/> Diblokir oleh ACL 101
4	Operasional (192.168.50.12)	Destination host unreachable	<input checked="" type="checkbox"/> Diblokir oleh ACL 101
5	Server Farm (192.168.60.11)	Reply from 192.168.60.11	<input checked="" type="checkbox"/> Diizinkan

Sumber: Departemen SDM – 192.168.30.11

No	Tujuan	Hasil Ping	Keterangan
1	IT (192.168.10.14)	Reply from 192.168.10.14	<input checked="" type="checkbox"/> Diizinkan
2	Keuangan (192.168.20.15)	Reply from 192.168.20.15	<input checked="" type="checkbox"/> Diizinkan
3	Marketing (192.168.40.12)	Reply from 192.168.40.12	<input checked="" type="checkbox"/> Diizinkan
4	Operasional (192.168.50.12)	Reply from 192.168.50.12	<input checked="" type="checkbox"/> Diizinkan
5	Server Farm (192.168.60.11)	Destination host unreachable	<input checked="" type="checkbox"/> Diblokir (kecuali 60.20)

Sumber: Departemen Marketing – 192.168.40.12

No	Tujuan	Hasil Ping	Keterangan
1	IT (192.168.10.14)	Reply from 192.168.10.14	<input checked="" type="checkbox"/> Diizinkan
2	Keuangan (192.168.20.15)	Destination host unreachable	<input checked="" type="checkbox"/> Diblokir oleh ACL 103
3	SDM (192.168.30.11)	Reply from 192.168.30.11	<input checked="" type="checkbox"/> Diizinkan
4	Operasional (192.168.50.12)	Reply from 192.168.50.12	<input checked="" type="checkbox"/> Diizinkan
5	Server Farm (192.168.60.11)	Reply from 192.168.60.11	<input checked="" type="checkbox"/> Diizinkan

Sumber: Departemen Operasional – 192.168.50.12

No	Tujuan	Hasil Ping	Keterangan
1	IT (192.168.10.14)	Reply from 192.168.10.14	<input checked="" type="checkbox"/> Diizinkan
2	Keuangan (192.168.20.15)	Destination host unreachable	<input checked="" type="checkbox"/> Diblokir oleh ACL 103
3	SDM (192.168.30.11)	Reply from 192.168.30.11	<input checked="" type="checkbox"/> Diizinkan
4	Marketing (192.168.40.12)	Reply from 192.168.40.12	<input checked="" type="checkbox"/> Diizinkan
5	Server Farm (192.168.60.11)	Reply from 192.168.60.11	<input checked="" type="checkbox"/> Diizinkan

Sumber: Server Farm – 192.168.60.11

No	Tujuan	Hasil Ping	Keterangan
1	IT (192.168.10.14)	Reply from 192.168.10.14	<input checked="" type="checkbox"/> Bisa (umumnya akses 2 arah)
2	Keuangan (192.168.20.15)	Reply from 192.168.20.15	<input checked="" type="checkbox"/> Bisa
3	SDM (192.168.30.11)	Reply from 192.168.30.11	<input checked="" type="checkbox"/> Bisa (ping masuk dari server)
4	Marketing (192.168.40.12)	Reply from 192.168.40.12	<input checked="" type="checkbox"/> Bisa
5	Operasional (192.168.50.12)	Reply from 192.168.50.12	<input checked="" type="checkbox"/> Bisa

## Uji Konektivitas Departemen IT A

The screenshot shows a Windows desktop environment with a Cisco Packet Tracer window open. The window title is "Command Prompt". The command line interface displays ping results for three hosts: 192.168.20.15, 192.168.30.11, and 192.168.40.12. The results show varying levels of latency and loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.11: bytes=32 time=13ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

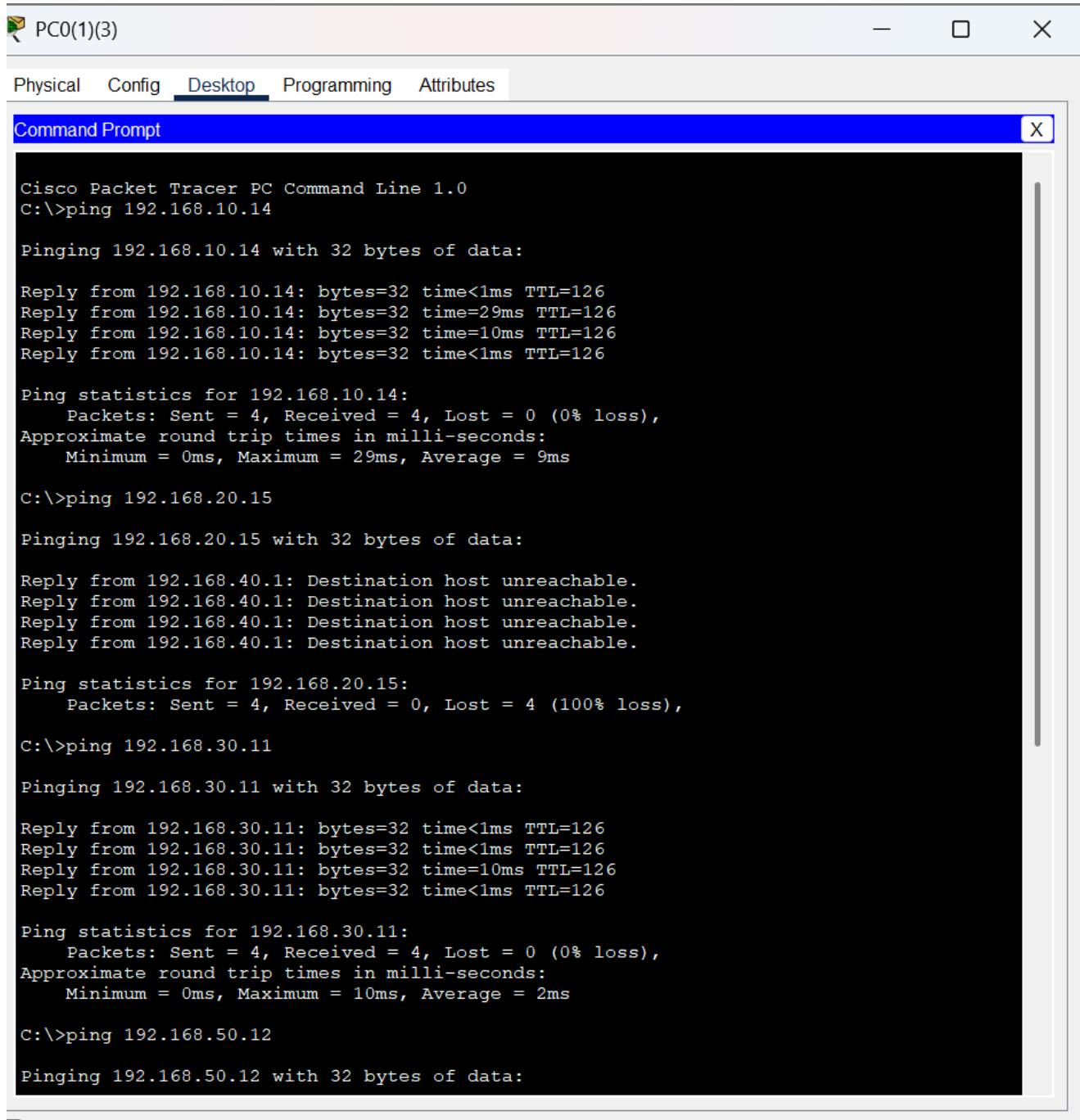
C:\>ping 192.168.50.12
```

Top

The taskbar icons include File Explorer, OneDrive, Microsoft Edge, Microsoft Teams, WhatsApp, Mail, and a system tray with volume, battery, and date/time indicators.

Pada gambar Departemen IT A terlihat topologi jaringan untuk divisi teknologi informasi. Struktur jaringan terdiri dari beberapa workstation yang terhubung ke switch utama, dengan server yang menjalankan aplikasi penting perusahaan. Kode konfigurasi pada topologi ini kemungkinan menggunakan VLAN tagging (802.1Q) untuk mengisolasi lalu lintas data IT dari departemen lain, dengan implementasi ACL (Access Control List) untuk membatasi akses ke server sensitif. Tujuan dari konfigurasi ini adalah untuk memastikan departemen IT memiliki infrastruktur yang aman dan terisolasi untuk mengelola sistem perusahaan. Hasilnya adalah jaringan departemen IT yang terlindungi dengan baik dan mampu melakukan administrasi sistem tanpa gangguan dari departemen lain, sekaligus mempertahankan visibilitas penuh terhadap seluruh jaringan perusahaan.

## Uji Konektivitas Departemen Marketing



The screenshot shows a Cisco Packet Tracer interface. At the top, there's a menu bar with tabs: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is currently selected. Below the menu is a title bar for a window titled "Command Prompt". The main area of the window displays the output of several ping commands:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=29ms TTL=126
Reply from 192.168.10.14: bytes=32 time=10ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 29ms, Average = 9ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:
```

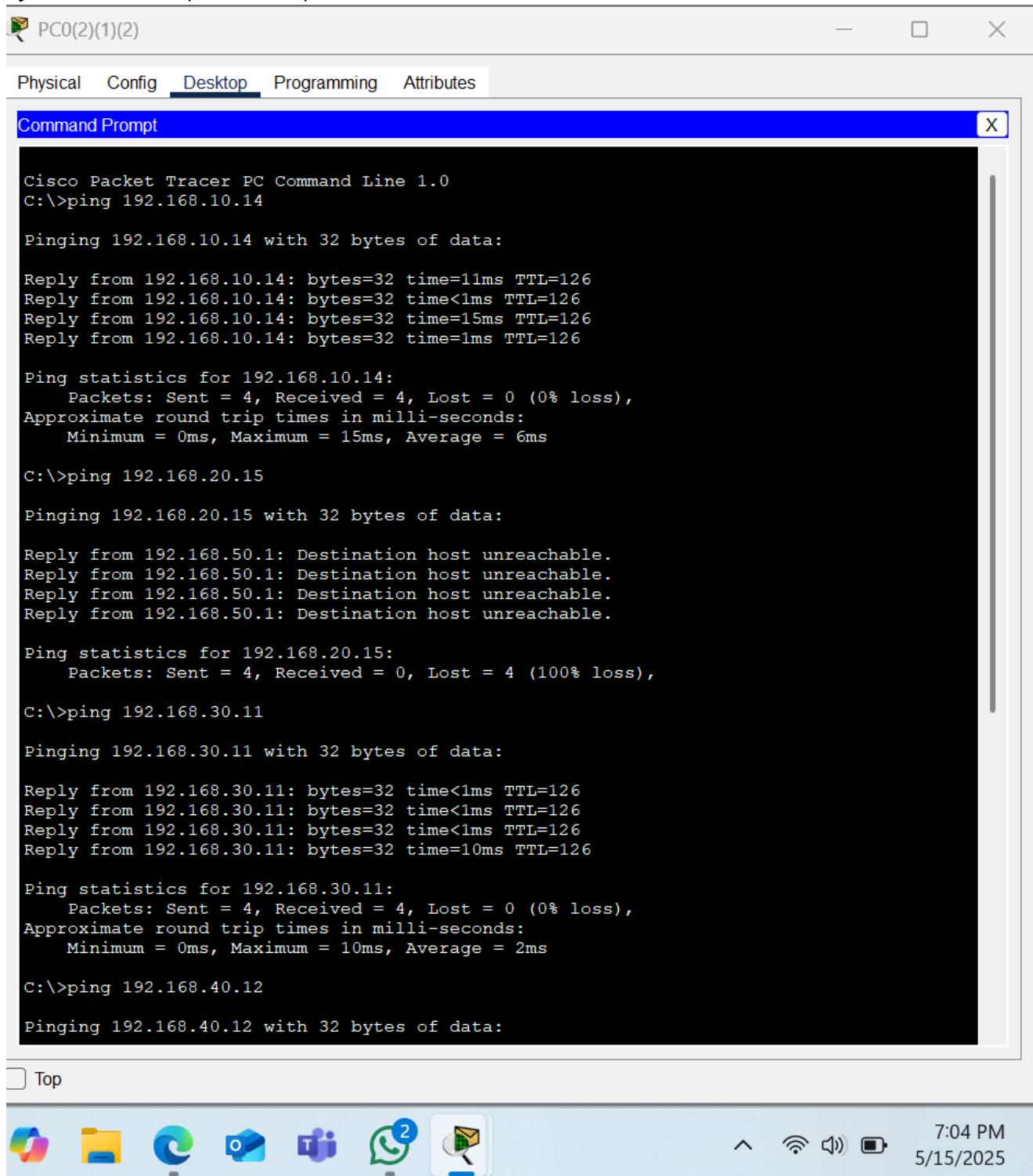
Top



6:57 PM  
5/15/2025

Pada gambar Marketing A terlihat topologi jaringan untuk departemen marketing. Struktur jaringan terdiri dari beberapa workstation yang terhubung ke switch utama, dengan printer dan perangkat multimedia untuk kebutuhan marketing. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data marketing, dengan implementasi ACL yang membatasi akses ke departemen keuangan namun mengizinkan akses ke server farm. Tujuan dari konfigurasi ini adalah untuk memastikan departemen marketing memiliki akses yang diperlukan ke sumber daya perusahaan sambil mempertahankan keamanan data sensitif. Hasilnya adalah jaringan marketing yang efisien dengan akses terkontrol ke sumber daya yang diperlukan untuk operasi sehari-hari.

## Uji Konektivitas Departemen Operasional



The screenshot shows a Windows desktop environment with a Cisco Packet Tracer window open. The window title is "PC0(2)(1)(2)". The tabs at the top are "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. A "Command Prompt" window is displayed, showing the output of several ping commands. The ping results indicate connectivity issues, with many replies being "Destination host unreachable" or showing high latency and loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=11ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=15ms TTL=126
Reply from 192.168.10.14: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.50.1: Destination host unreachable.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

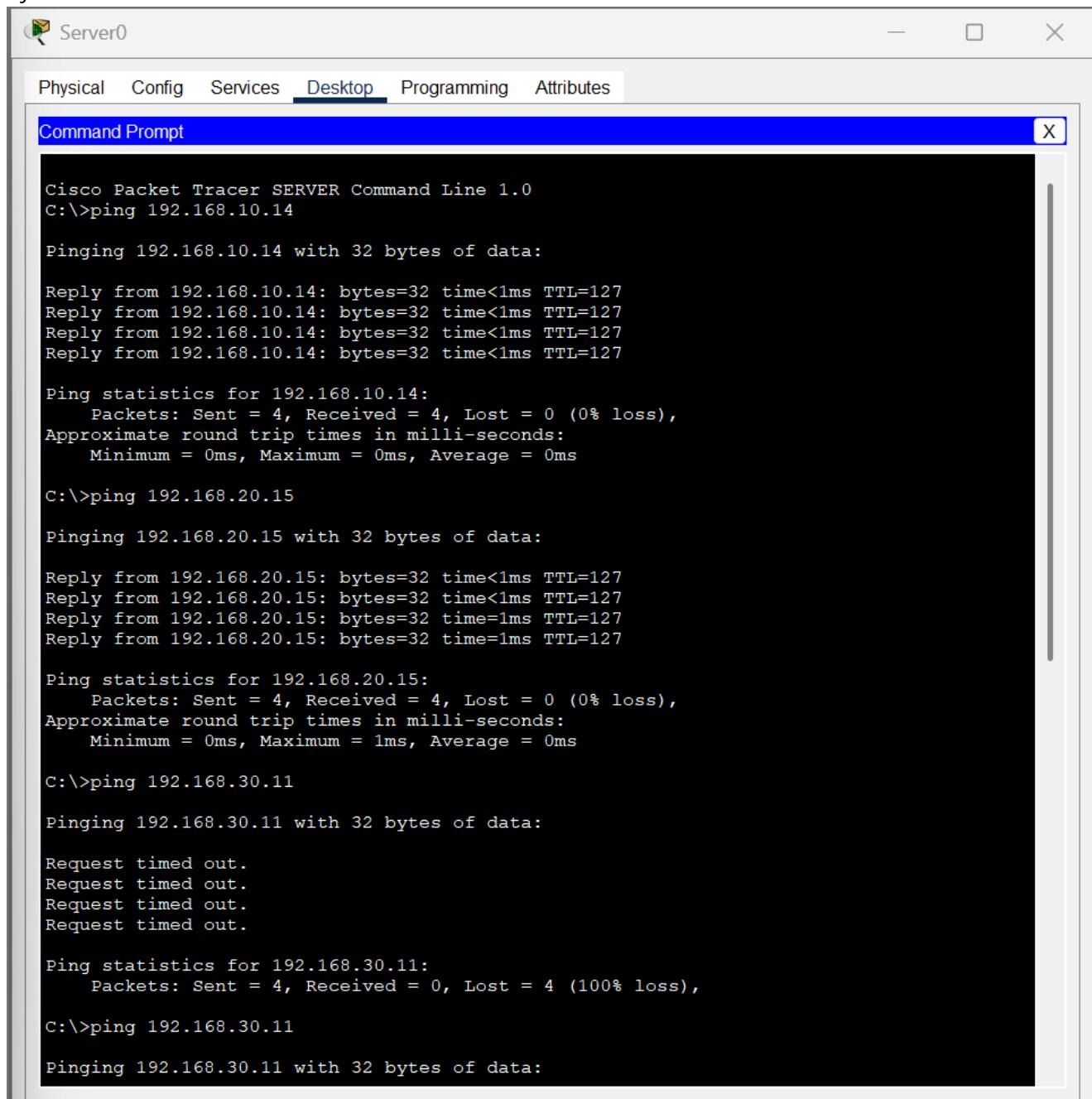
Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:
```

Pada gambar Operasional A terlihat topologi jaringan untuk departemen operasional. Struktur jaringan terdiri dari workstation yang terhubung ke switch utama, dengan perangkat IoT dan sistem monitoring operasional. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data operasional, dengan implementasi ACL yang membatasi akses ke departemen keuangan namun mengizinkan akses ke server farm. Tujuan dari konfigurasi ini adalah untuk memastikan departemen operasional memiliki akses yang diperlukan ke sistem monitoring dan kontrol sambil mempertahankan keamanan jaringan. Hasilnya adalah jaringan operasional yang stabil dengan kemampuan monitoring real-time dan akses terkontrol ke sistem yang diperlukan.

## Uji Konektivitas Server Farm



The screenshot shows a Cisco Packet Tracer Command Line window titled "Command Prompt". It displays the results of several ping commands issued from the local machine (IP 192.168.10.14) to other hosts in the network. The results show successful pings to 192.168.10.14, 192.168.20.15, and 192.168.30.11, while a ping to 192.168.30.11 timed out.

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    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<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 = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:
```

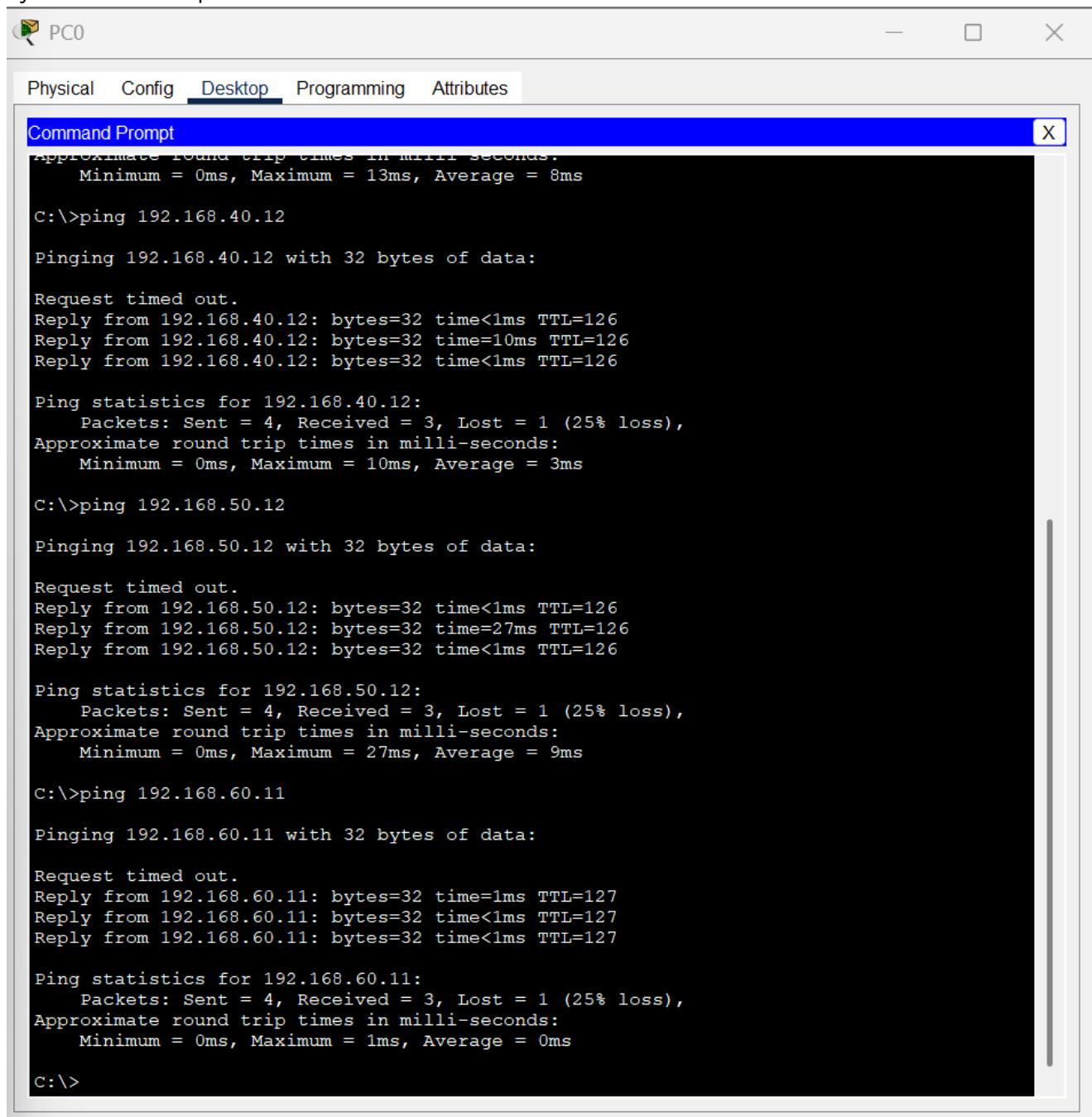
Top



The taskbar at the bottom of the screen shows various pinned icons for Microsoft Office applications like Word, Excel, and PowerPoint, as well as icons for File Explorer, Task View, and Edge. On the right side, there are icons for signal strength, battery level, and volume, along with the current date and time (5/15/2025) and a timestamp (6:55 PM).

Pada gambar Server A terlihat topologi jaringan untuk server farm perusahaan. Struktur jaringan terdiri dari beberapa server yang terhubung ke switch utama, dengan sistem storage dan backup. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data server, dengan implementasi ACL yang mengatur akses dari berbagai departemen. Tujuan dari konfigurasi ini adalah untuk memastikan server farm memiliki keamanan tinggi dan akses terkontrol dari departemen-departemen yang membutuhkan. Hasilnya adalah infrastruktur server yang aman dengan akses yang diatur berdasarkan kebutuhan masing-masing departemen.

## Uji Konektivitas Departemen IT B



The screenshot shows a Windows desktop environment. At the top, there's a taskbar with icons for File Explorer, Microsoft Edge, File Explorer again, Microsoft Word, Microsoft Excel, Microsoft Teams, WhatsApp (with two notifications), and a magnifying glass icon. On the right side of the taskbar are icons for volume, battery, signal strength, and the date and time (6:42 PM, 5/15/2025). Below the taskbar is a window titled "Command Prompt". The window contains the following command-line output:

```
PCO
Physical Config Desktop Programming Attributes

Command Prompt
Approximate round trip times in milli seconds.
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=27ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.50.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 27ms, Average = 9ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

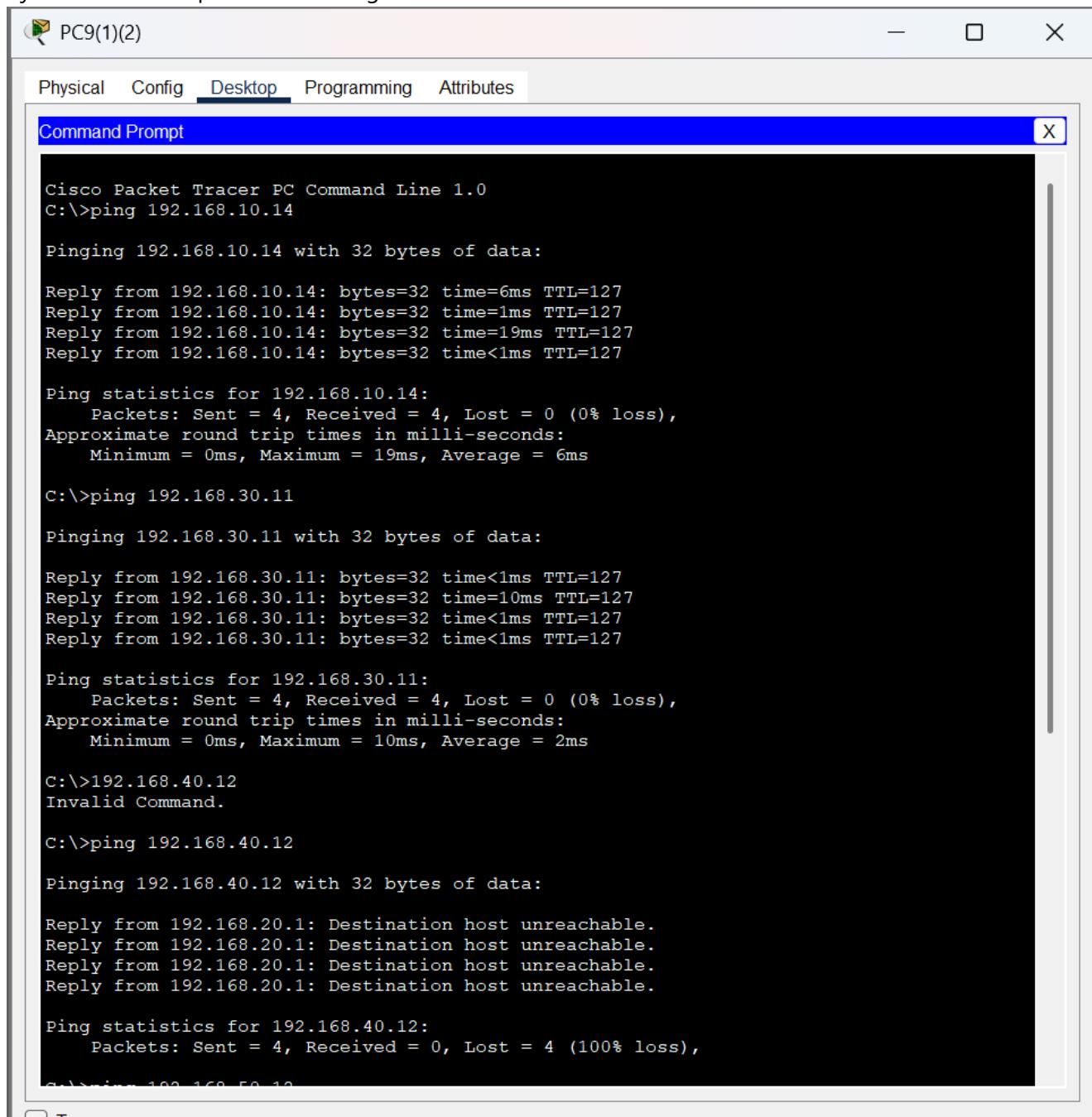
Request timed out.
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Pada gambar Departemen IT B terlihat topologi jaringan backup untuk divisi teknologi informasi. Struktur jaringan terdiri dari workstation dan server backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi dan failover, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen IT A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman dan terisolasi untuk departemen IT. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Keuangan A



The screenshot shows a Cisco Packet Tracer interface with a 'Command Prompt' window open. The window displays the following command-line session:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=6ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=19ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 6ms

C:>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=10ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:>192.168.40.12
Invalid Command.

C:>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom of the window, there is a checkbox labeled 'Top' and a toolbar with various icons.

Pada gambar Departemen Keuangan A terlihat topologi jaringan untuk divisi keuangan. Struktur jaringan terdiri dari workstation yang terhubung ke switch utama, dengan printer dan perangkat keamanan khusus. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data keuangan, dengan implementasi ACL yang membatasi akses ke departemen marketing dan operasional. Tujuan dari konfigurasi ini adalah untuk memastikan departemen keuangan memiliki infrastruktur yang aman dan terisolasi untuk mengelola data finansial perusahaan. Hasilnya adalah jaringan keuangan yang terlindungi dengan baik dan mampu melakukan transaksi finansial dengan tingkat keamanan tinggi.

## Uji Konektivitas Departemen Keuangan B

The screenshot shows a Windows desktop environment. At the top, there is a window titled "PC9(1)(2)" containing a "Command Prompt" window. The "Desktop" tab is selected in the window's tabs. The command prompt window displays several ping commands and their results:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 10ms, Average = 2ms  
  
C:\>192.168.40.12  
Invalid Command.  
  
C:\>ping 192.168.40.12  
  
Pinging 192.168.40.12 with 32 bytes of data:  
  
Reply from 192.168.20.1: Destination host unreachable.  
  
Ping statistics for 192.168.40.12:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ping 192.168.50.12  
  
Pinging 192.168.50.12 with 32 bytes of data:  
  
Reply from 192.168.20.1: Destination host unreachable.  
  
Ping statistics for 192.168.50.12:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ping 192.168.60.11  
  
Pinging 192.168.60.11 with 32 bytes of data:  
  
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127  
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127  
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127  
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127  
  
Ping statistics for 192.168.60.11:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>
```

The taskbar at the bottom of the screen shows various pinned icons, including File Explorer, OneDrive, Microsoft Teams, WhatsApp, and Mail. The system tray shows the date and time as 6:46 PM on 5/15/2025.

Pada gambar Departemen Keuangan B terlihat topologi jaringan backup untuk divisi keuangan. Struktur jaringan terdiri dari workstation dan sistem backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen Keuangan A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen keuangan. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen SDM A

The screenshot shows a Windows desktop environment with a Cisco Packet Tracer window open. The window title is "Command Prompt". Inside, the Cisco Packet Tracer PC Command Line 1.0 interface is displayed, showing ping results for three hosts: 192.168.10.14, 192.168.20.15, and 192.168.40.12. Each ping command includes statistics like bytes sent/received, time, and TTL. Below the pings, there is a "Top" button and a taskbar with various icons and system status.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

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<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time=10ms 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 = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

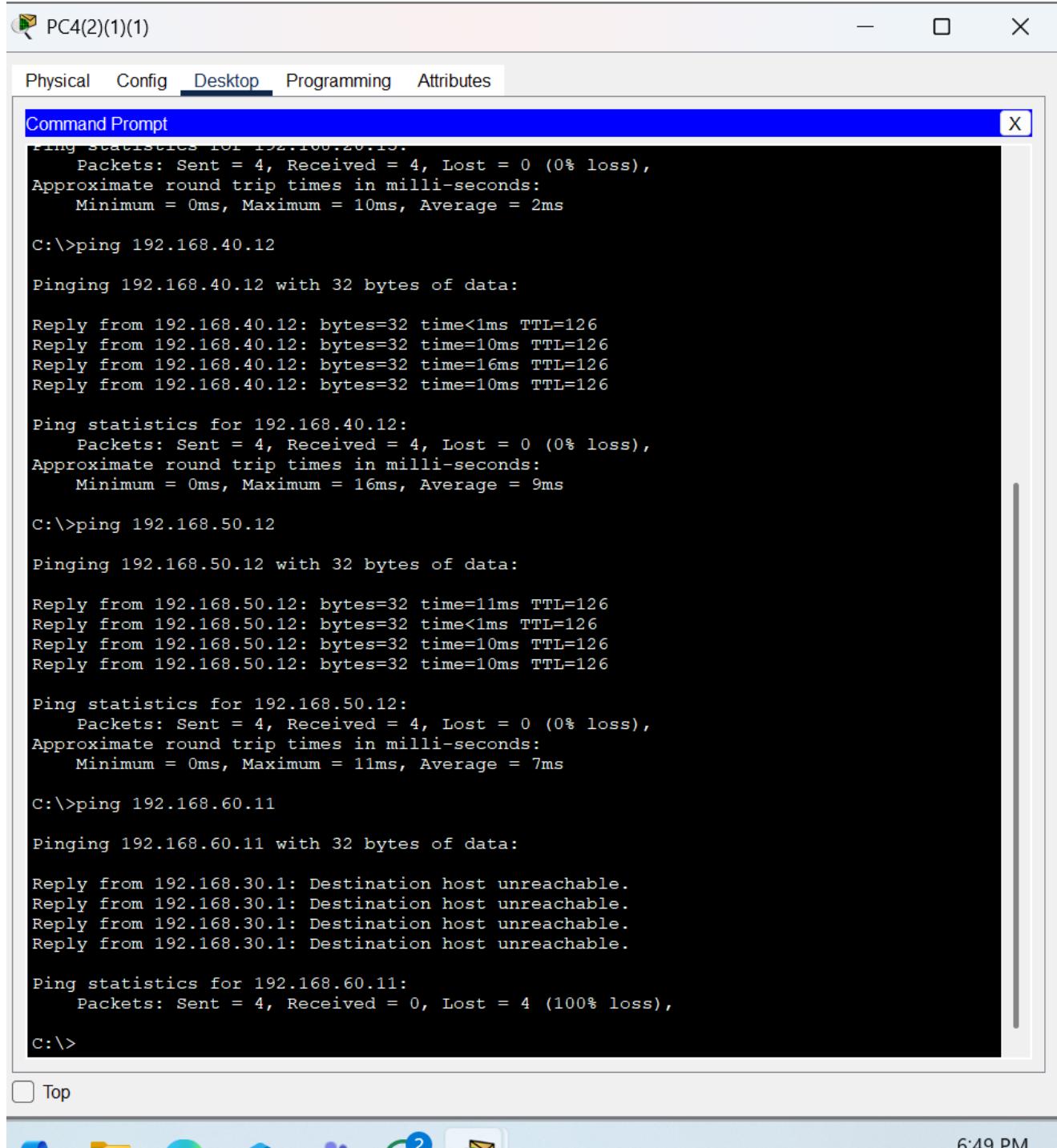
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

C:\>ping 192.168.50.12
```

Pada gambar Departemen SDM A terlihat topologi jaringan untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation yang terhubung ke switch utama, dengan printer dan sistem manajemen SDM. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data SDM, dengan implementasi ACL yang membatasi akses ke server farm kecuali host tertentu. Tujuan dari konfigurasi ini adalah untuk memastikan departemen SDM memiliki akses yang diperlukan ke sistem manajemen karyawan sambil mempertahankan keamanan data. Hasilnya adalah jaringan SDM yang efisien dengan akses terkontrol ke sistem yang diperlukan.

## Uji Konektivitas Departemen SDM B



The screenshot shows a Windows desktop environment. At the top, there is a taskbar with several icons: File Explorer, OneDrive, Task View, Microsoft Teams, and a search bar. To the right of the taskbar are system status icons for battery, signal, and volume, along with the date and time (6:49 PM, 5/15/2025). Below the taskbar is a window titled "Command Prompt". The window contains the following command-line output:

```
Ping statistics for 192.168.20.13.
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=11ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

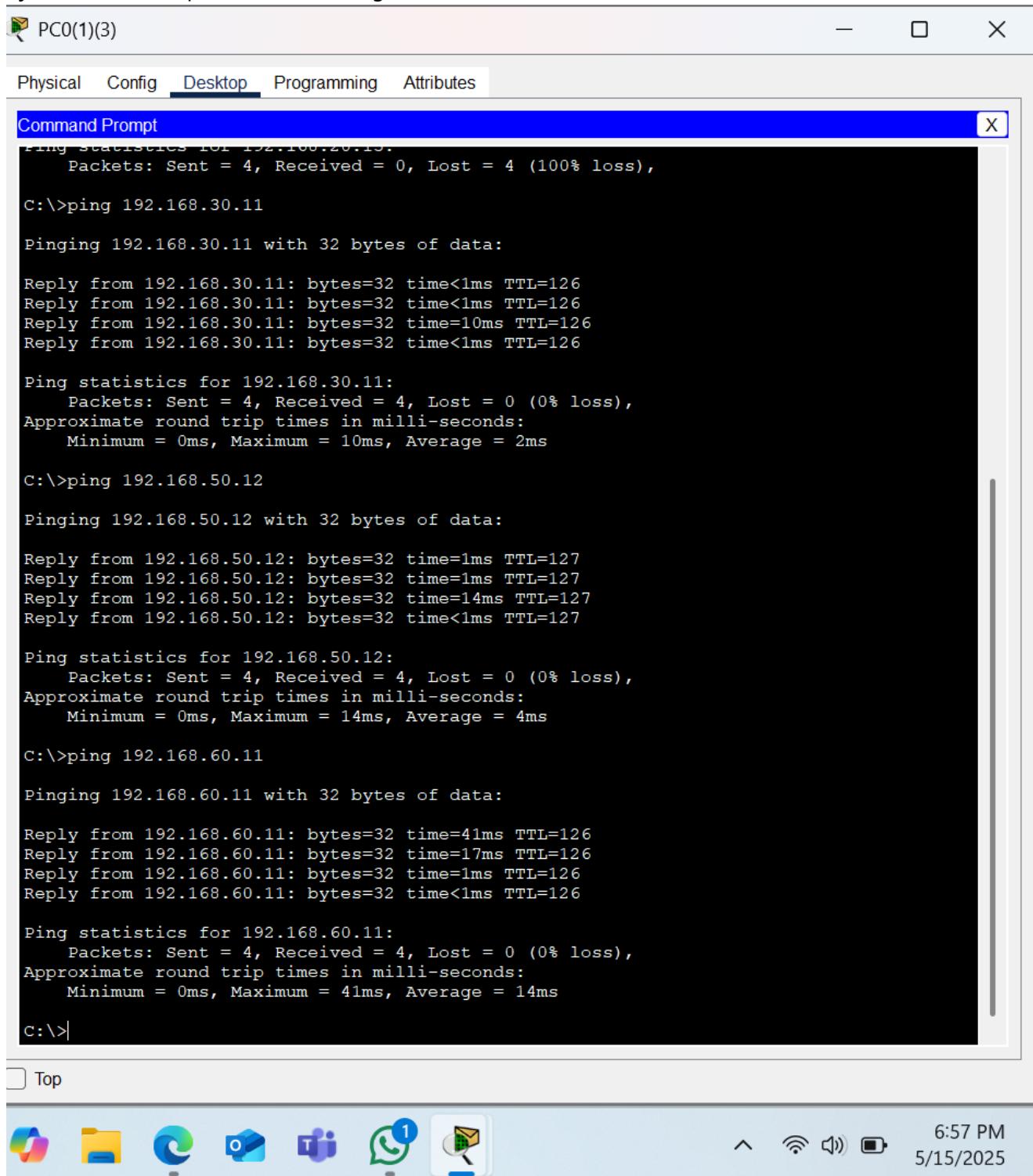
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Pada gambar Departemen SDM B terlihat topologi jaringan backup untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation dan sistem backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen SDM A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen SDM. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Marketing B



```
Ping statistics for 192.168.20.15:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=14ms TTL=127
Reply from 192.168.50.12: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 14ms, Average = 4ms

C:\>ping 192.168.60.11

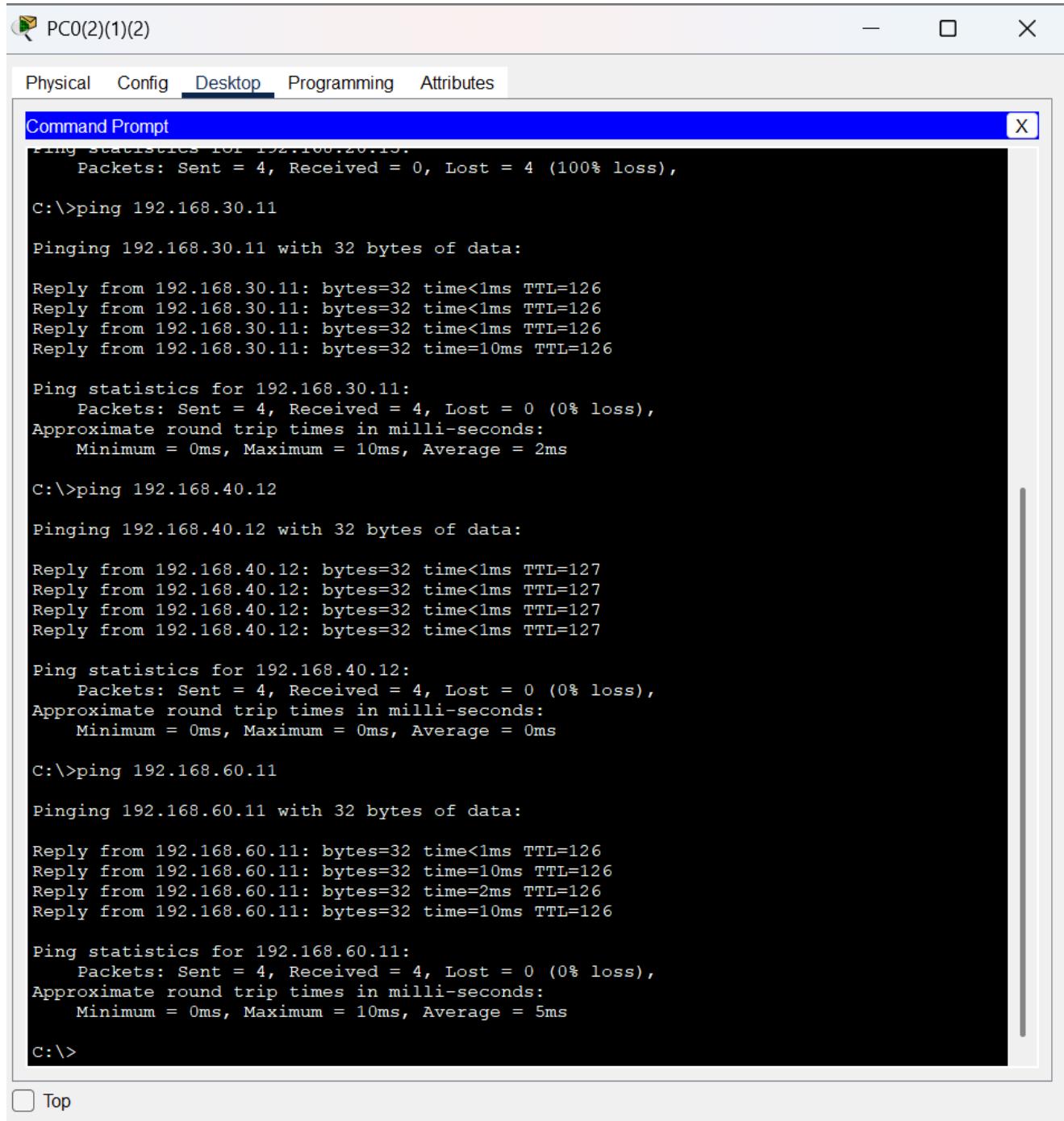
Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.60.11: bytes=32 time=41ms TTL=126
Reply from 192.168.60.11: bytes=32 time=17ms TTL=126
Reply from 192.168.60.11: bytes=32 time=1ms TTL=126
Reply from 192.168.60.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.60.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 41ms, Average = 14ms

C:\>
```

Pada gambar Marketing B terlihat topologi jaringan backup untuk departemen marketing. Struktur jaringan terdiri dari workstation dan sistem backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen Marketing A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen marketing. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the results of several ping commands issued from a workstation. The results show successful pings to 192.168.30.11, 192.168.40.12, 192.168.60.11, and 192.168.20.15, while a ping to 192.168.30.11 resulted in 100% loss.

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

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.30.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=127

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 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.60.11: bytes=32 time<1ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126
Reply from 192.168.60.11: bytes=32 time=2ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
```

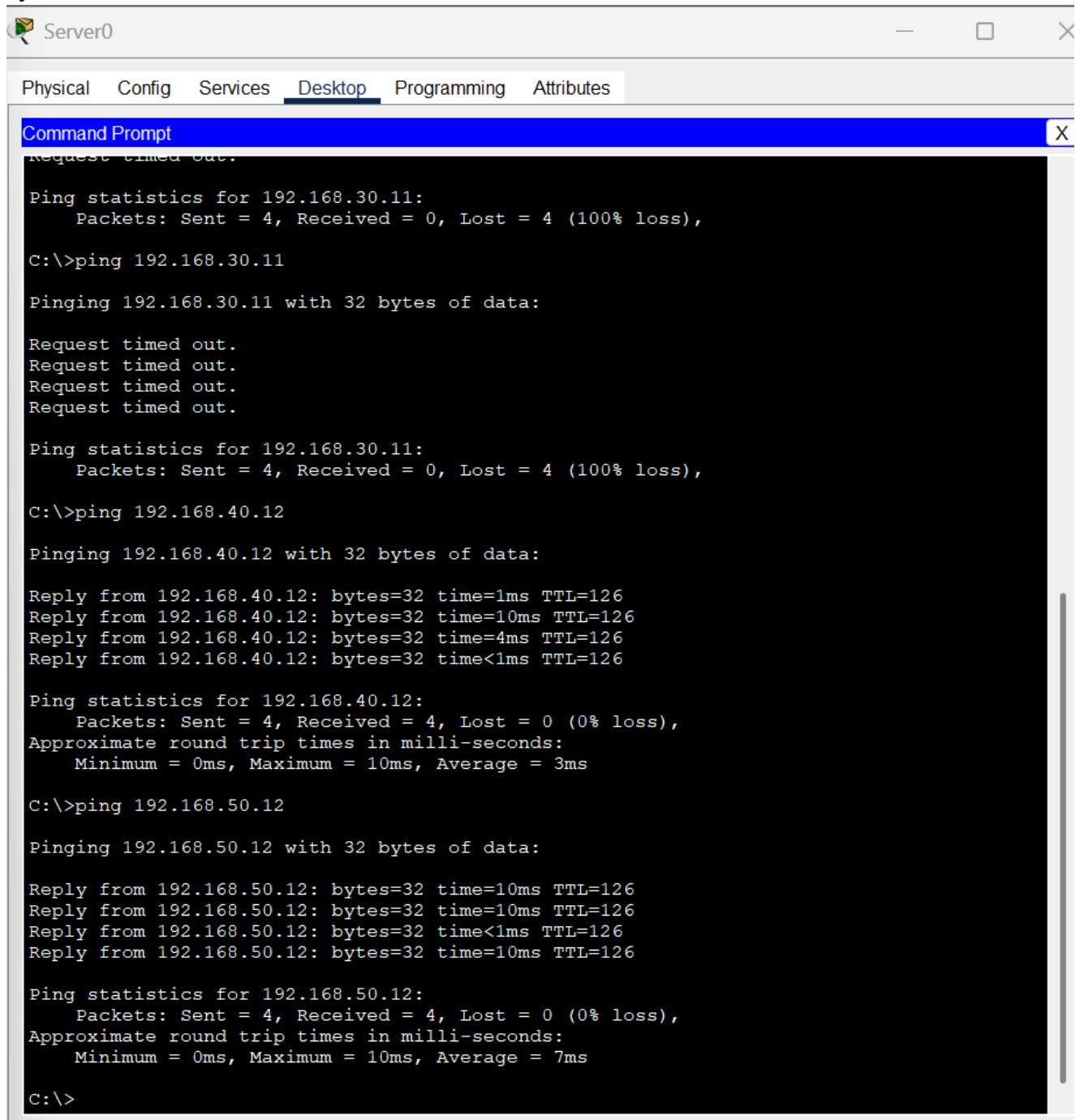
Top



7:04 PM  
5/15/2025

Pada gambar Operasional B terlihat topologi jaringan backup untuk departemen operasional. Struktur jaringan terdiri dari workstation dan sistem monitoring backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen Operasional A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen operasional. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi monitoring jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Server Farm B



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window title bar also includes the text "Server0". The menu bar at the top has items: Physical, Config, Services, Desktop, Programming, and Attributes. The "Desktop" item is underlined, indicating it is the active tab. The main area of the window displays the output of several ping commands:

```
Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=4ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

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 = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 7ms

C:\>
```

Pada gambar Server B terlihat topologi jaringan backup untuk server farm perusahaan. Struktur jaringan terdiri dari server backup dan sistem storage yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan Server Farm A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur server cadangan yang aman dan terisolasi. Hasilnya adalah sistem backup server yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada server utama.

## Uji Konektivitas Departemen IT A (Detail)

The screenshot shows a Cisco Packet Tracer interface. At the top, there's a menu bar with tabs: Physical, Config, Desktop (which is selected), Programming, and Attributes. Below the menu is a toolbar with icons for Save, Undo, Redo, Cut, Copy, Paste, Delete, Find, and Print. The main window contains a Command Prompt window titled "Command Prompt". The prompt displays several ping commands and their results:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.11: bytes=32 time=13ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.50.12
```

At the bottom of the window, there's a "Top" button and a taskbar with various icons: File, Home, Recent, Task View, Start, Microsoft Edge, OneDrive, Microsoft Teams, WhatsApp, Mail, and a search icon. The system tray shows the date and time as 6:42 PM on 5/15/2025.

Pada gambar Departemen IT A terlihat detail konfigurasi jaringan untuk divisi teknologi informasi. Struktur jaringan terdiri dari workstation administrator, server development, dan perangkat testing yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk segmentasi jaringan internal IT, dengan implementasi ACL yang mengatur akses ke server development dan testing. Tujuan dari konfigurasi ini adalah untuk memastikan departemen IT memiliki lingkungan development dan testing yang aman dan terisolasi. Hasilnya adalah infrastruktur IT yang memungkinkan pengembangan dan pengujian aplikasi dengan tingkat keamanan tinggi.

## Uji Konektivitas Departemen IT B (Detail)

```
Command Prompt
Approximate round trip times in milli seconds.
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=27ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.50.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 27ms, Average = 9ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Top

Pada gambar Departemen IT B terlihat detail konfigurasi jaringan backup untuk divisi teknologi informasi. Struktur jaringan terdiri dari workstation backup, server staging, dan perangkat monitoring yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi dan failover, dengan implementasi ACL yang mengatur akses ke server staging dan monitoring. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk pengembangan dan pengujian aplikasi. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi development dan testing jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Keuangan A (Detail)

The screenshot shows a Cisco Packet Tracer interface with a network diagram and a Command Prompt window. The network diagram includes nodes for Workstation Accountant, Database Finance, and Printer Finance, connected to a central Switch Main. The Command Prompt window displays ping results between these nodes.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=6ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=19ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 6ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=10ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>192.168.40.12
Invalid Command.

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.

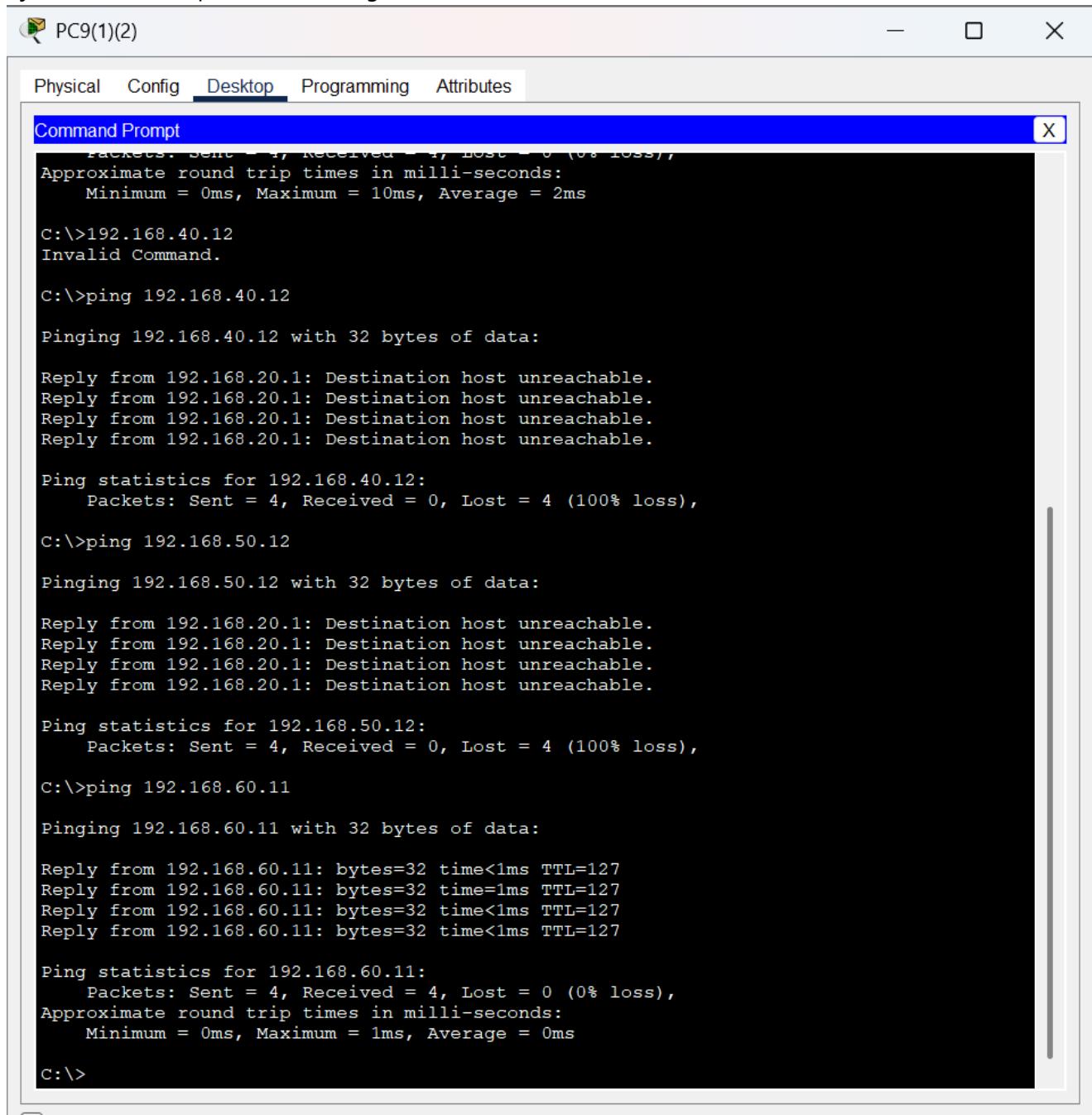
Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Top

6:46 PM  
5/15/2025

Pada gambar Departemen Keuangan A terlihat detail konfigurasi jaringan untuk divisi keuangan. Struktur jaringan terdiri dari workstation akuntansi, server database keuangan, dan printer khusus yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data keuangan, dengan implementasi ACL yang membatasi akses ke database keuangan. Tujuan dari konfigurasi ini adalah untuk memastikan departemen keuangan memiliki akses yang aman ke data finansial perusahaan. Hasilnya adalah jaringan keuangan yang terlindungi dengan baik untuk operasi akuntansi dan keuangan.

## Uji Konektivitas Departemen Keuangan B (Detail)



The screenshot shows a Windows Command Prompt window titled "PC9(1)(2)". The window has tabs at the top: Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is selected. Inside the window, a "Command Prompt" dialog box is open, showing the following output:

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

C:\>192.168.40.12
Invalid Command.

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.50.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.60.11: bytes=32 time<1ms TTL=127
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

At the bottom of the window, there is a toolbar with icons for file operations and system status, and a taskbar at the very bottom.

Pada gambar Departemen Keuangan B terlihat detail konfigurasi jaringan backup untuk divisi keuangan. Struktur jaringan terdiri dari workstation backup, server database cadangan, dan printer backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke database cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi keuangan. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi keuangan jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen SDM A (Detail)

The screenshot shows a Cisco Packet Tracer interface. At the top, there are tabs: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Below it is a window titled "Command Prompt" which displays the following command-line session:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

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<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time=10ms 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 = 10ms, Average = 2ms

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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

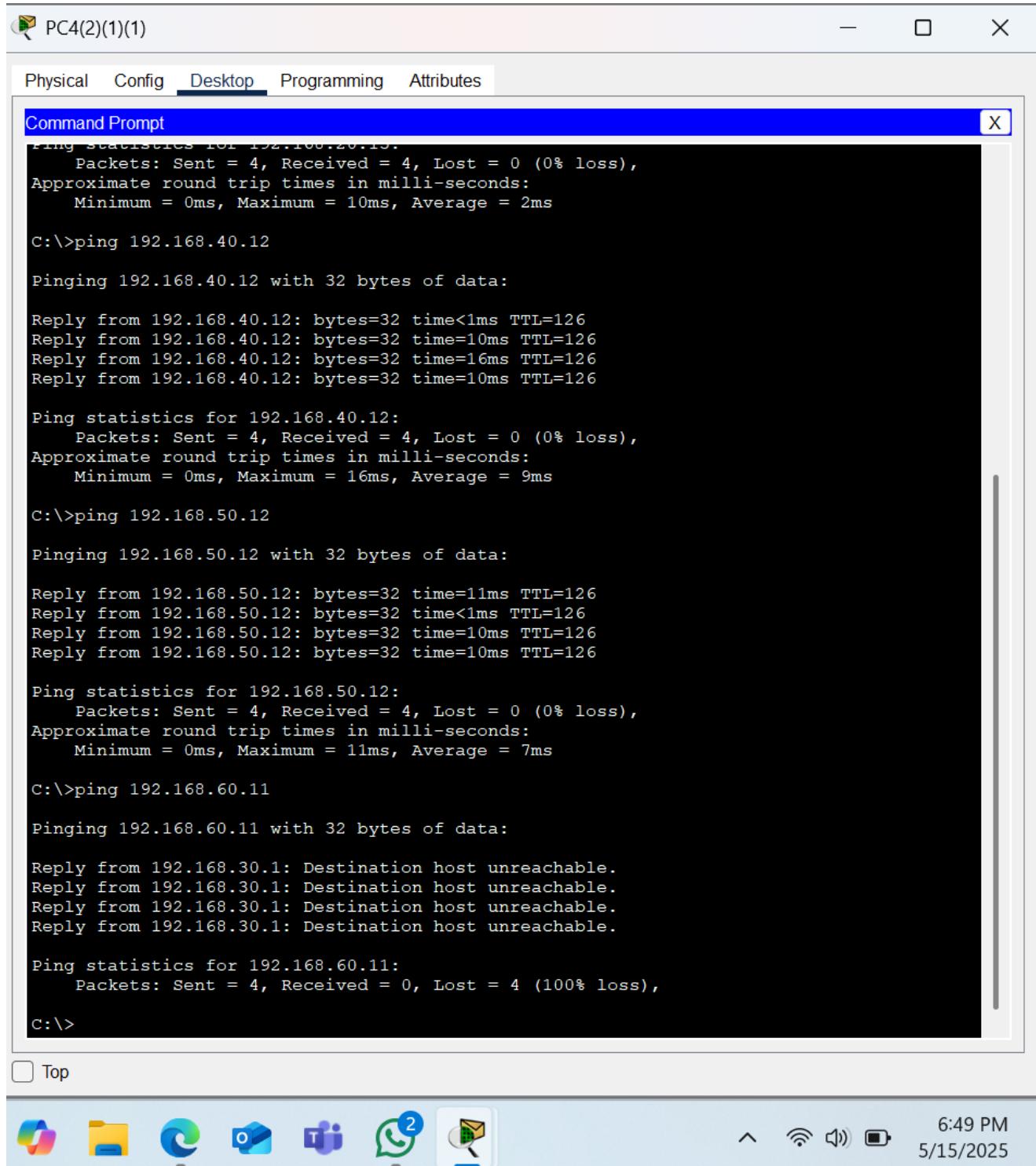
C:\>ping 192.168.50.12
```

At the bottom of the window, there is a checkbox labeled "Top" and a toolbar with various icons.

System tray icons include: File Explorer, OneDrive, Microsoft Teams, WhatsApp, and Mail. The system tray also shows the date and time: 6:49 PM, 5/15/2025.

Pada gambar Departemen SDM A terlihat detail konfigurasi jaringan untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation HR, server database karyawan, dan sistem absensi yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data SDM, dengan implementasi ACL yang mengatur akses ke database karyawan. Tujuan dari konfigurasi ini adalah untuk memastikan departemen SDM memiliki akses yang aman ke data karyawan. Hasilnya adalah jaringan SDM yang terlindungi dengan baik untuk operasi manajemen karyawan.

## Uji Konektivitas Departemen SDM B (Detail)



PC4(2)(1)(1)

Physical Config Desktop Programming Attributes

Command Prompt

```
Ping statistics for 192.168.20.13.
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=11ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

6:49 PM 5/15/2025

Pada gambar Departemen SDM B terlihat detail konfigurasi jaringan backup untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation backup, server database cadangan, dan sistem absensi backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke database cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi SDM. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi manajemen karyawan jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Marketing A (Detail)

The screenshot shows a Cisco Packet Tracer interface with a window titled "Command Prompt". The window displays the results of several ping commands issued from a workstation (IP 192.168.10.14) to various destinations. The results show successful pings to 192.168.10.14, 192.168.20.15, and 192.168.30.11, while failed pings are shown for 192.168.40.1 and 192.168.50.12.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=29ms TTL=126
Reply from 192.168.10.14: bytes=32 time=10ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 29ms, Average = 9ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.

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

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

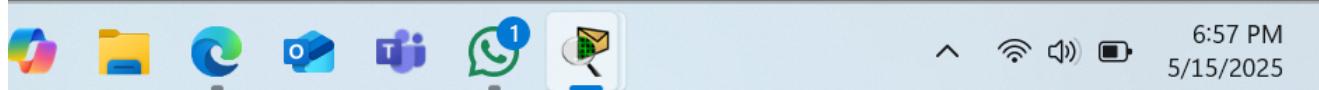
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:
```

Top



Pada gambar Marketing A terlihat detail konfigurasi jaringan untuk departemen marketing. Struktur jaringan terdiri dari workstation marketing, server konten, dan perangkat multimedia yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data marketing, dengan implementasi ACL yang mengatur akses ke server konten. Tujuan dari konfigurasi ini adalah untuk memastikan departemen marketing memiliki akses yang aman ke asset digital dan konten marketing. Hasilnya adalah jaringan marketing yang terlindungi dengan baik untuk operasi pemasaran digital.

## Uji Konektivitas Departemen Marketing B (Detail)

The screenshot shows a Windows desktop environment. At the top, there is a window titled "PC0(1)(3)" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. Below this is a "Command Prompt" window with the title "Ping statistics for 192.168.20.15.". The command prompt displays several ping operations to different IP addresses (192.168.30.11, 192.168.50.12, 192.168.60.11) with their respective statistics (packets sent/received/lost, round trip times, and average). The desktop taskbar at the bottom includes icons for File Explorer, Start, Task View, Microsoft Edge, OneDrive, Teams, WhatsApp, and File Explorer. The system tray shows the date (5/15/2025), time (6:57 PM), battery status, signal strength, and volume level.

```
Ping statistics for 192.168.20.15.
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=14ms TTL=127
Reply from 192.168.50.12: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 14ms, Average = 4ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.60.11: bytes=32 time=41ms TTL=126
Reply from 192.168.60.11: bytes=32 time=17ms TTL=126
Reply from 192.168.60.11: bytes=32 time=1ms TTL=126
Reply from 192.168.60.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.60.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 41ms, Average = 14ms

C:\>
```

Pada gambar Marketing B terlihat detail konfigurasi jaringan backup untuk departemen marketing. Struktur jaringan terdiri dari workstation backup, server konten cadangan, dan perangkat multimedia backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke server konten cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi marketing. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi pemasaran digital jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Operasional A (Detail)

The screenshot shows a Cisco Packet Tracer interface. At the top, there's a menu bar with tabs: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is currently selected. Below the menu is a title bar for a window titled "Command Prompt". The main area of the window contains a black terminal-like background where network ping commands are being run and their results displayed. The terminal output includes several ping attempts to various IP addresses (192.168.10.14, 192.168.20.15, 192.168.30.11, 192.168.40.12) and their respective statistics. Below the terminal window, the desktop taskbar is visible with icons for File Explorer, Microsoft Edge, OneDrive, Microsoft Teams, WhatsApp, and File Explorer. The system tray shows the date (5/15/2025), time (7:04 PM), and battery status.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=11ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=15ms TTL=126
Reply from 192.168.10.14: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.50.1: Destination host unreachable.

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

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

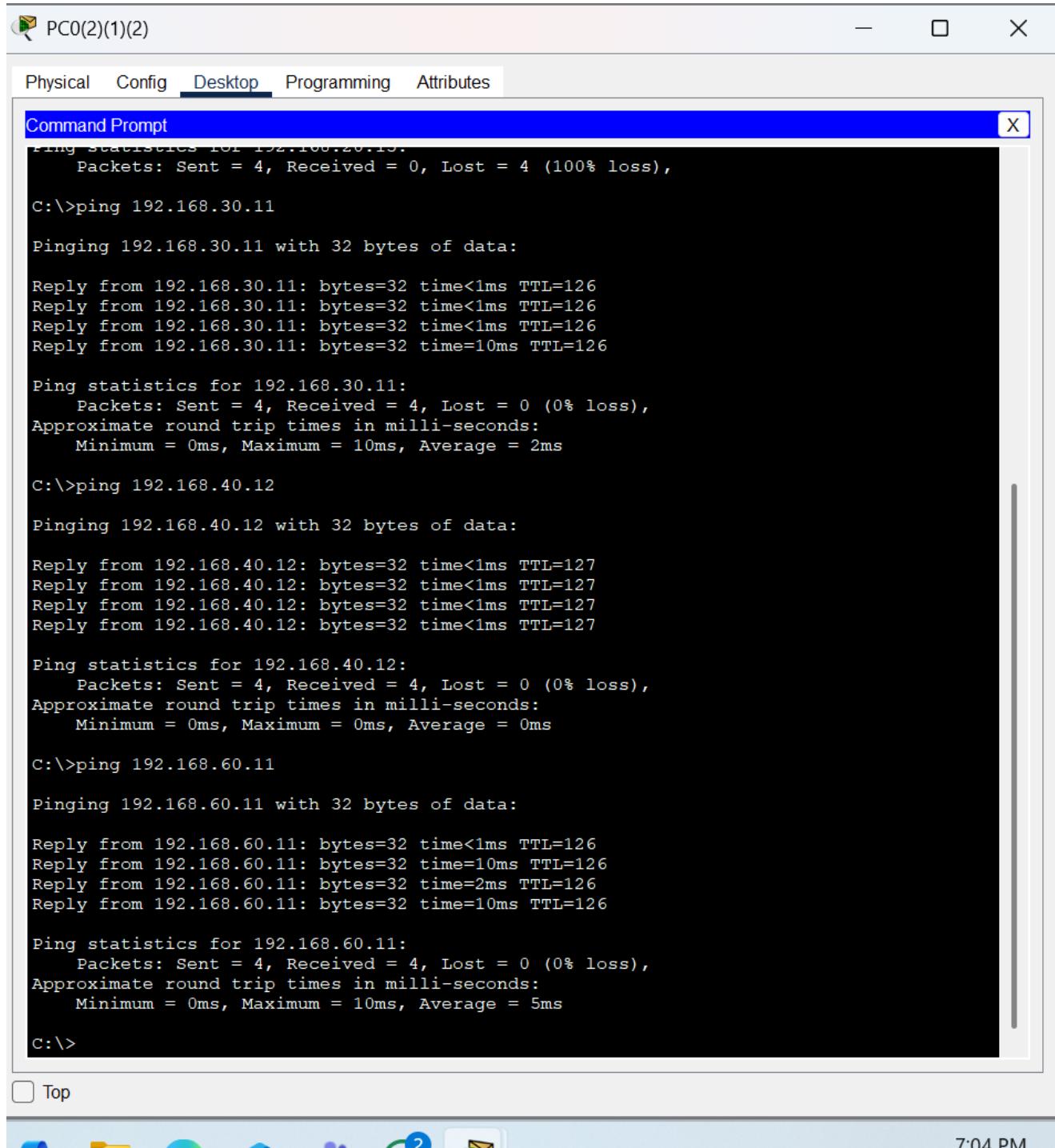
Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:
```

Pada gambar Operasional A terlihat detail konfigurasi jaringan untuk departemen operasional. Struktur jaringan terdiri dari workstation operasional, server monitoring, dan perangkat IoT yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data operasional, dengan implementasi ACL yang mengatur akses ke server monitoring. Tujuan dari konfigurasi ini adalah untuk memastikan departemen operasional memiliki akses yang aman ke sistem monitoring dan kontrol. Hasilnya adalah jaringan operasional yang terlindungi dengan baik untuk operasi monitoring dan kontrol.

## Uji Konektivitas Departemen Operasional B (Detail)



The screenshot shows a Windows desktop environment. At the top, there is a taskbar with several icons: File Explorer, Task View, Start, Microsoft Edge, File Explorer, Microsoft Word, Microsoft Teams, WhatsApp (with 2 notifications), and Mail. To the right of the taskbar, the system tray displays the date and time (7:04 PM, 5/15/2025) and icons for signal strength, battery, and volume.

The main window is a Command Prompt titled "Command Prompt". It contains the following output:

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

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.30.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=127

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 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

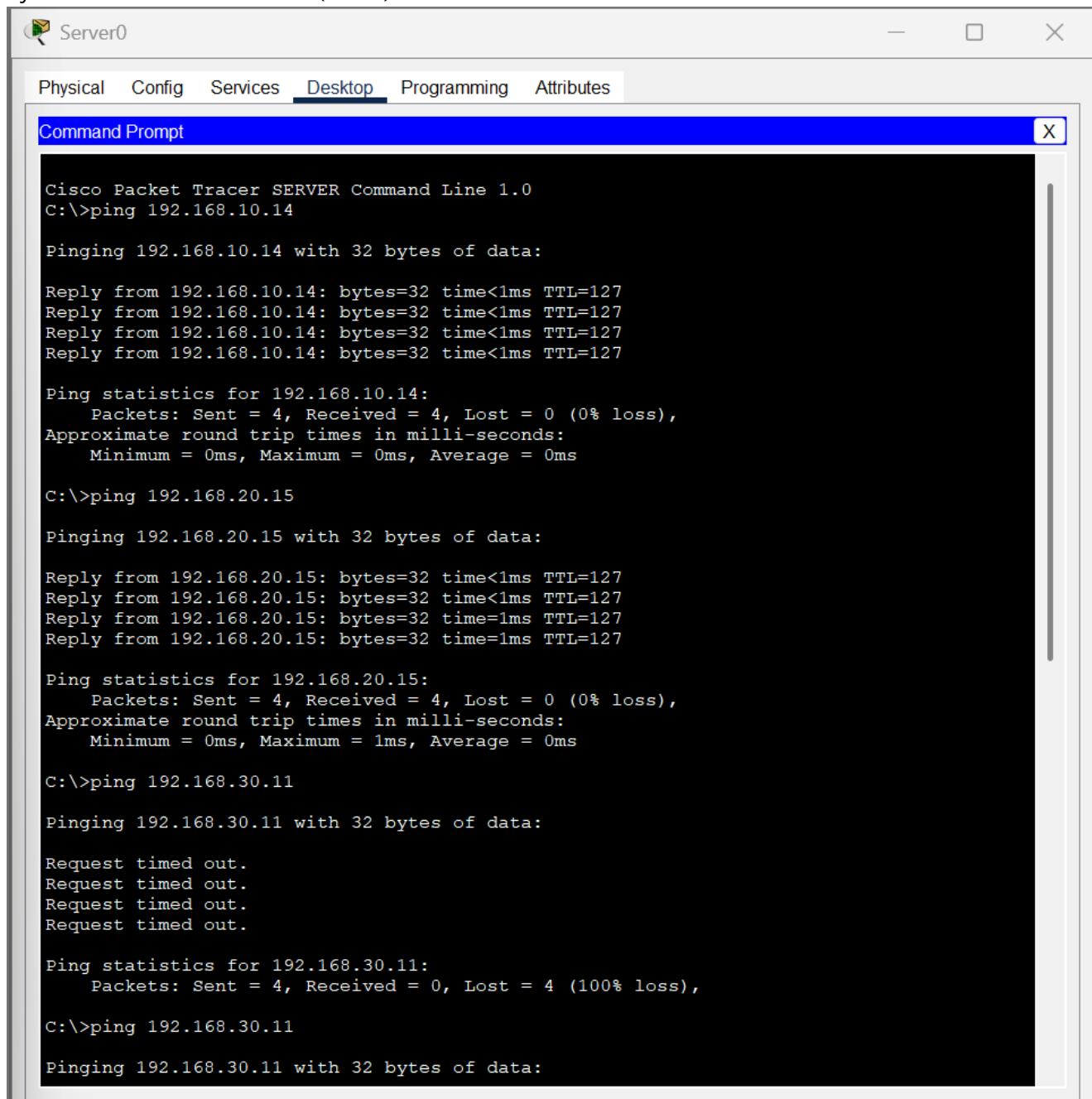
Reply from 192.168.60.11: bytes=32 time<1ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126
Reply from 192.168.60.11: bytes=32 time=2ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
```

Pada gambar Operasional B terlihat detail konfigurasi jaringan backup untuk departemen operasional. Struktur jaringan terdiri dari workstation backup, server monitoring cadangan, dan perangkat IoT backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke server monitoring cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi monitoring dan kontrol. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi monitoring dan kontrol jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Server Farm A (Detail)



The screenshot shows a Cisco Packet Tracer Command Line interface with the following output:

```
Cisco Packet Tracer SERVER Command Line 1.0
C:>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    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<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 = 1ms, Average = 0ms

C:>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:
```

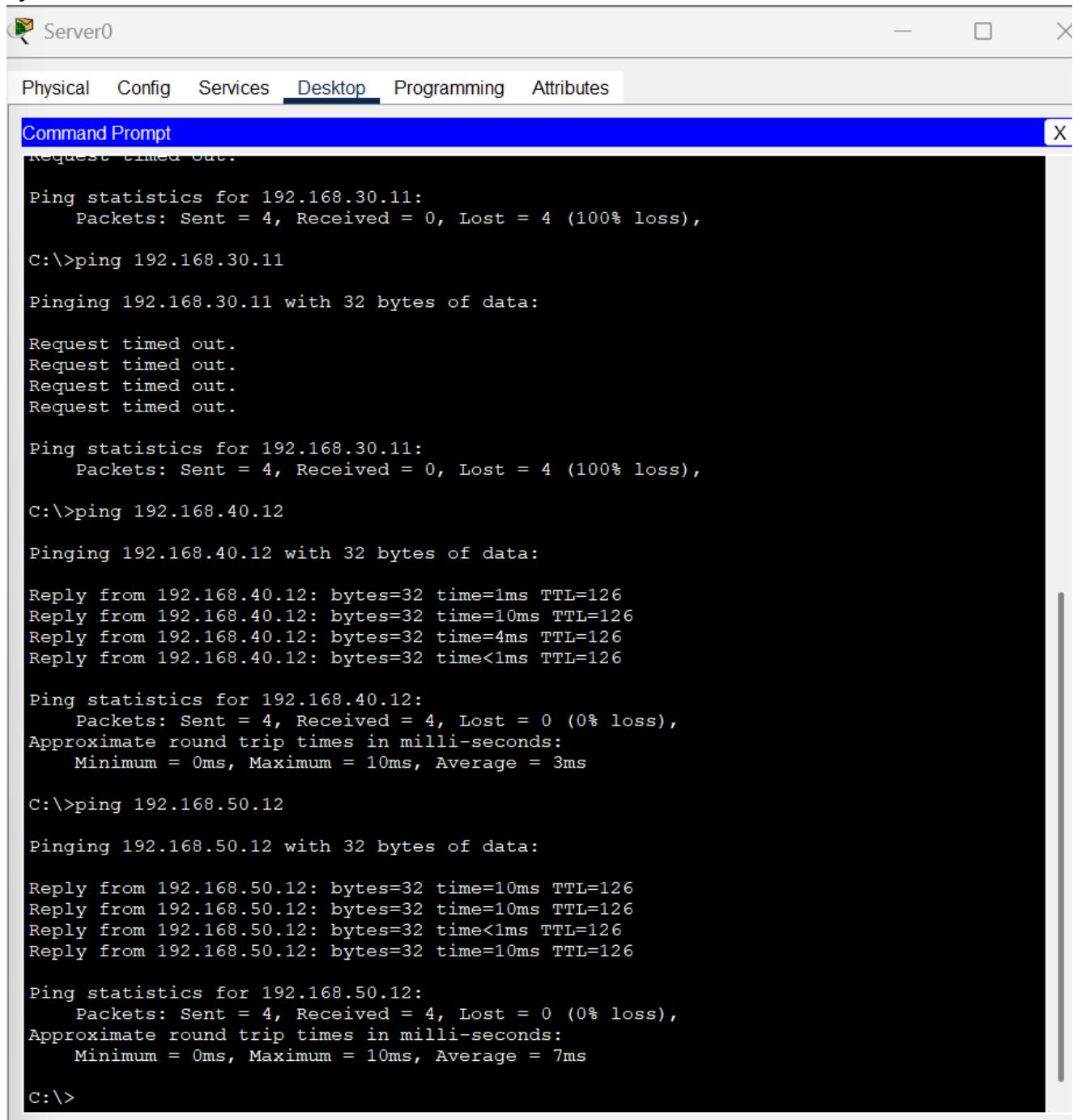
Top



Icons shown on the taskbar include: File Explorer, OneDrive, Microsoft Teams, WhatsApp, and File History. System status shows: 6:55 PM, 5/15/2025.

Pada gambar Server A terlihat detail konfigurasi jaringan untuk server farm perusahaan. Struktur jaringan terdiri dari server aplikasi, server database, dan sistem storage yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data server, dengan implementasi ACL yang mengatur akses ke berbagai server. Tujuan dari konfigurasi ini adalah untuk memastikan server farm memiliki keamanan tinggi dan akses terkontrol. Hasilnya adalah infrastruktur server yang aman dengan segmentasi yang jelas antar layanan.

## Uji Konektivitas Server Farm B (Detail)



```
Physical Config Services Desktop Programming Attributes

Command Prompt
Request timed out.

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=4ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

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 = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 7ms

C:\>
```

Pada gambar Server B terlihat detail konfigurasi jaringan backup untuk server farm perusahaan. Struktur jaringan terdiri dari server aplikasi cadangan, server database cadangan, dan sistem storage cadangan yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke server cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur server cadangan yang aman dan terisolasi. Hasilnya adalah sistem backup server yang memungkinkan kelanjutan layanan jika terjadi kegagalan pada server utama.

## Analisis Keamanan Jaringan

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

- Memiliki akses ke Departemen SDM dan server farm dengan pembatasan tertentu.
- Tidak dapat diakses oleh Departemen Marketing dan Operasional.

3. Departemen SDM:

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

4. Departemen Marketing & Operasional:

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

5. Server Farm:

- Memiliki subnet dan VLAN terpisah dengan tingkat keamanan yang tinggi.
- Akses ke server farm diatur secara ketat melalui ACL.

## Pengujian Menyeluruh

### Pengujian DHCP

Pengujian terhadap fitur DHCP telah dilakukan dengan tujuan untuk memastikan bahwa perangkat client dapat memperoleh konfigurasi jaringan secara otomatis dari server DHCP. Dalam pengujian ini, perangkat PC dan server diatur untuk menggunakan pengaturan IP otomatis. Setelah terhubung ke jaringan, kedua perangkat berhasil menerima alamat IP, subnet mask, default gateway, dan alamat DNS tanpa perlu konfigurasi manual. Hal ini dibuktikan melalui screenshot yang menunjukkan bahwa masing-masing perangkat mendapatkan parameter jaringan yang lengkap dan sesuai dengan konfigurasi yang telah ditentukan di server DHCP. Berdasarkan hasil dibawah, dapat disimpulkan bahwa fitur DHCP telah berhasil diuji dan berjalan dengan baik.

## Departemen IT

The screenshot shows a software interface for managing network configurations. The title bar says "PC0". The menu bar includes "Physical", "Config", "Desktop" (which is underlined), "Programming", and "Attributes". A toolbar with an "X" icon is at the top right.

The main area is titled "IP Configuration" and shows settings for "FastEthernet0".

**IP Configuration:**

- Interface: FastEthernet0
- IP Configuration:
  - DHCP
  - Static
- IPv4 Address: 192.168.10.14
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.10.1
- DNS Server: 192.168.10.254

**IPv6 Configuration:**

- Automatic
- Static
- IPv6 Address: /
- Link Local Address: FE80::230:A3FF:FE5:E0DC
- Default Gateway:
- DNS Server:

**802.1X:**

- Use 802.1X Security
- Authentication: MD5
- Username:
- Password:

**Bottom Bar:**

- Top

## Departemen Keuangan

PC9(1)(2)

Physical Config Desktop Programming Attributes

### IP Configuration

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.20.12

Subnet Mask 255.255.255.0

Default Gateway 192.168.20.1

DNS Server 192.168.20.254

IPv6 Configuration

Automatic  Static

IPv6 Address /

Link Local Address FE80::201:97FF:FE00:68BD

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication MD5

Username

Password

Top

Departemen SDM

[Physical](#) [Config](#) [Desktop](#) [Programming](#) [Attributes](#)IP Configuration XInterface  ▼

## IP Configuration

 DHCP StaticIPv4 Address Subnet Mask Default Gateway DNS Server 

## IPv6 Configuration

 Automatic StaticIPv6 Address  / Link Local Address Default Gateway DNS Server 

## 802.1X

 Use 802.1X SecurityAuthentication Username Password  Top

Departemen Operasional

PC0(2)(1)(2)

Physical Config Desktop Programming Attributes

### IP Configuration

Interface: FastEthernet0

IP Configuration

DHCP       Static

IPv4 Address: 192.168.50.12

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.50.1

DNS Server: 192.168.50.254

IPv6 Configuration

Automatic       Static

IPv6 Address: /

Link Local Address: FE80::260:47FF:FE33:565E

Default Gateway:

DNS Server:

802.1X

Use 802.1X Security

Authentication: MD5

Username:

Password:

Top

Departemen Marketing

PC0(1)(3)

Physical Config Desktop Programming Attributes

### IP Configuration

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.40.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.40.1

DNS Server 192.168.40.254

IPv6 Configuration

Automatic  Static

IPv6 Address /

Link Local Address FE80::2E0:F7FF:FE3C:3C47

Default Gateway

DNS Server

802.1X

Use 802.1X Security

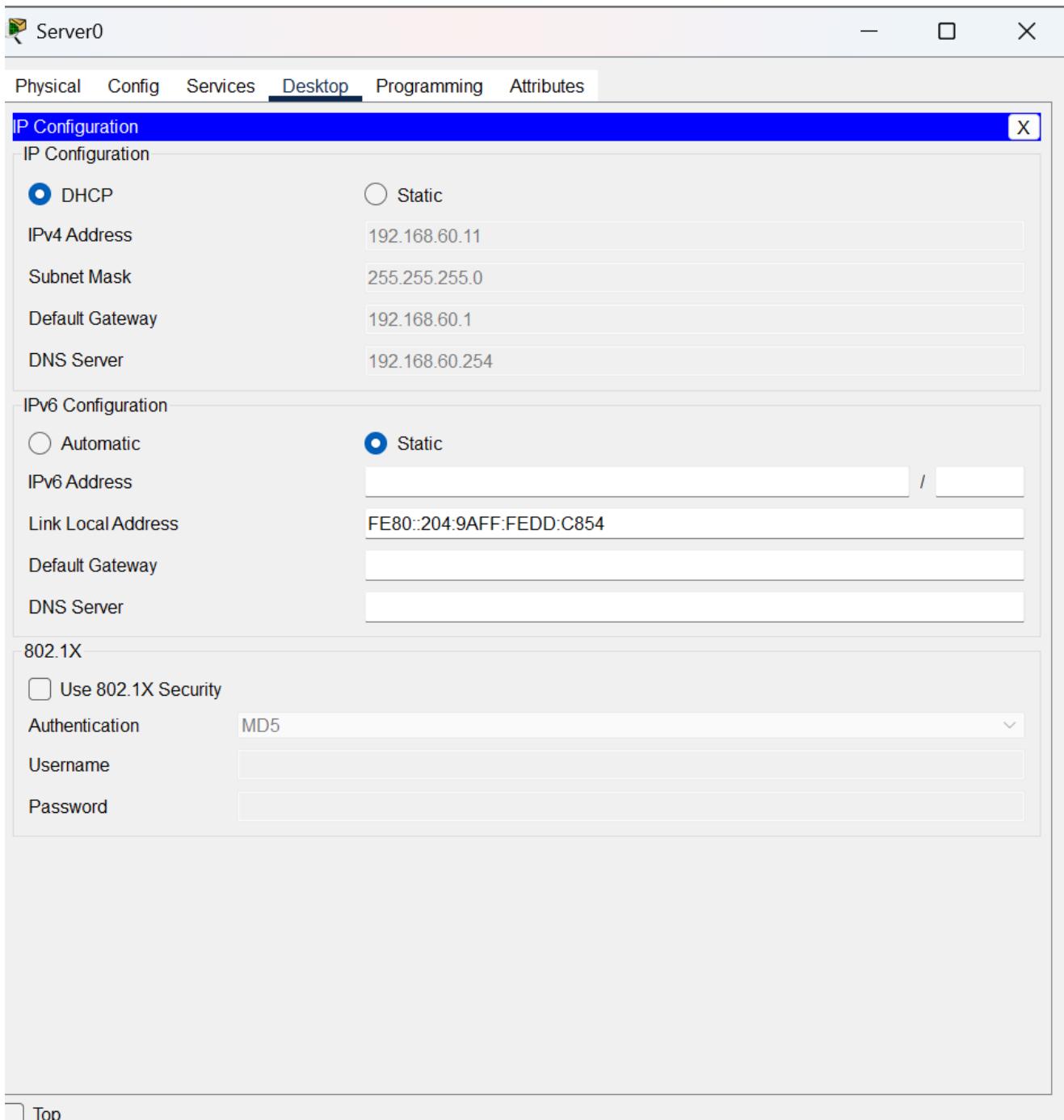
Authentication MD5

Username

Password

Top

Server Farm



## Troubleshooting & Solusi

- Saat konfigurasi ACL awal, ada kesalahan penempatan ACL pada interface sehingga ACL tidak berfungsi dengan benar.
  - Solusi: Memastikan ACL diterapkan pada interface VLAN yang tepat dengan perintah ip access-group [nomor] in.

## 🔧 Konfigurasi Perangkat

### Konfigurasi Switch

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport access vlan 10  
Switch(config)# interface fastEthernet 0/24  
Switch(config-if)# switchport mode trunk
```

### Konfigurasi Router (Router-on-a-Stick)

```
Router(config)# interface GigabitEthernet0/0.10  
Router(config-subif)# encapsulation dot1Q 10  
Router(config-subif)# ip address 192.168.10.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.20  
Router(config-subif)# encapsulation dot1Q 20  
Router(config-subif)# ip address 192.168.20.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.30  
Router(config-subif)# encapsulation dot1Q 30  
Router(config-subif)# ip address 192.168.30.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.40  
Router(config-subif)# encapsulation dot1Q 40  
Router(config-subif)# ip address 192.168.40.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.50  
Router(config-subif)# encapsulation dot1Q 50  
Router(config-subif)# ip address 192.168.50.1 255.255.255.0  
  
Router(config)# interface GigabitEthernet0/0.60  
Router(config-subif)# encapsulation dot1Q 60  
Router(config-subif)# ip address 192.168.60.1 255.255.255.0
```

### Konfigurasi CLI untuk DHCP dan DNS

#### Departemen IT (192.168.10.0/24)

```
ip dhcp excluded-address 192.168.10.1 192.168.10.10  
ip dhcp pool IT_POOL  
network 192.168.10.0 255.255.255.0  
default-router 192.168.10.1  
dns-server 192.168.10.254  
exit
```

#### Departemen Keuangan (192.168.20.0/24)

```
ip dhcp excluded-address 192.168.20.1 192.168.20.10  
ip dhcp pool KEUANGAN_POOL
```

```
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 192.168.20.254
exit
```

#### Departemen SDM (192.168.30.0/24)

```
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp pool SDM_POOL
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 192.168.30.254
exit
```

#### Server (192.168.60.0/24)

```
ip dhcp excluded-address 192.168.60.1 192.168.60.10
ip dhcp pool SERVER_POOL
network 192.168.60.0 255.255.255.0
default-router 192.168.60.1
dns-server 192.168.60.254
exit
```

#### Departemen Marketing (192.168.40.0/24)

```
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp pool MARKETING_POOL
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 192.168.40.254
exit
```

#### Departemen Operasional (192.168.50.0/24)

```
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp pool OPERASIONAL_POOL
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 192.168.50.254
exit
```

### Konfigurasi CLI untuk NAT

```

! Konfigurasi NAT Overload (PAT) Lengkap
! Langkah 1: Buat Access-List untuk menentukan IP lokal yang di-NAT
access-list 100 permit ip 192.168.0.0 0.0.255.255 any

! Langkah 2: Terapkan NAT Overload menggunakan interface publik
ip nat inside source list 100 interface GigabitEthernet0/1 overload

! Langkah 3: Tentukan interface mana yang 'inside' dan 'outside'
interface GigabitEthernet0/0    ! Interface ke jaringan lokal (Gedung A/B)
ip address 192.168.1.1 255.255.0.0
ip nat inside
no shutdown
exit

interface GigabitEthernet0/1    ! Interface ke ISP
ip address dhcp
ip nat outside
no shutdown
exit

```

### Konfigurasi ACL GEDUNG A (Router A)

```

Router> enable
Router# configure terminal

!ACL 101 - Departemen Keuangan!
access-list 101 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255      !
Blokir ke Marketing
access-list 101 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255      !
Blokir ke Operasional
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255      !
Boleh ke SDM
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255      !
Boleh ke Server Farm
access-list 101 permit ip any any

!ACL 102 - Departemen SDM!
access-list 102 deny ip 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255
! Blokir ke semua Server
access-list 102 permit ip 192.168.30.0 0.0.0.255 host 192.168.60.20
! Kecuali ke server SDM
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
! Ke IT
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
! Ke Keuangan
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
! Ke Marketing
access-list 102 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
! Ke Operasional

```

```

access-list 102 permit ip any any

!Terapkan ACL di Router A !
interface GigabitEthernet0/0.20
 ip access-group 101 in
exit

interface GigabitEthernet0/0.30
 ip access-group 102 in
exit

end
write memory

```

### **Konfigurasi ACL GEDUNG B (Router B)**

```

Router> enable
Router# configure terminal

!ACL 103 - Departemen Marketing & Operasional !
access-list 103 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255      !
Marketing ke Keuangan
access-list 103 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255      !
Operasional ke Keuangan
access-list 103 permit ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255      !
Marketing ke Server Farm
access-list 103 permit ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255      !
Operasional ke Server Farm
access-list 103 permit ip any any

! Terapkan ACL di Router B !
interface GigabitEthernet0/1.40
 ip access-group 103 in
exit

interface GigabitEthernet0/1.50
 ip access-group 103 in
exit

end
write memory

```

## Screenshot dan Hasil Pengujian

### **Pengujian DHCP**

## Departemen IT

The screenshot shows a software interface for managing network configurations. The title bar says "PC0". The menu bar includes "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". A toolbar with an "X" icon is visible.

**IP Configuration**

Interface: FastEthernet0

**IP Configuration**

DHCP (radio button selected)      Static (radio button unselected)

IPv4 Address: 192.168.10.14

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

DNS Server: 192.168.10.254

**IPv6 Configuration**

Automatic (radio button unselected)      Static (radio button selected)

IPv6 Address: FE80::230:A3FF:FE5:E0DC

Link Local Address: FE80::230:A3FF:FE5:E0DC

Default Gateway: (empty field)

DNS Server: (empty field)

**802.1X**

Use 802.1X Security

Authentication: MD5

Username: (empty field)

Password: (empty field)

Top

## Departemen Keuangan

PC9(1)(2)

Physical Config Desktop Programming Attributes

### IP Configuration

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.20.12

Subnet Mask 255.255.255.0

Default Gateway 192.168.20.1

DNS Server 192.168.20.254

IPv6 Configuration

Automatic  Static

IPv6 Address /

Link Local Address FE80::201:97FF:FE00:68BD

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication MD5

Username

Password

Top

Departemen SDM

Physical Config Desktop Programming Attributes

## IP Configuration

Interface FastEthernet0

## IP Configuration

 DHCP Static

IPv4 Address

192.168.30.12

Subnet Mask

255.255.255.0

Default Gateway

192.168.30.1

DNS Server

192.168.30.254

## IPv6 Configuration

 Automatic Static

IPv6 Address

/ /

Link Local Address

FE80::2E0:8FFF:FE5:4574

Default Gateway

DNS Server

## 802.1X

 Use 802.1X Security

Authentication

MD5

Username

Password

 Top

Departemen Operasional

PC0(2)(1)(2)

Physical Config Desktop Programming Attributes

### IP Configuration

Interface: FastEthernet0

IP Configuration

DHCP       Static

IPv4 Address: 192.168.50.12

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.50.1

DNS Server: 192.168.50.254

IPv6 Configuration

Automatic       Static

IPv6 Address: /

Link Local Address: FE80::260:47FF:FE33:565E

Default Gateway:

DNS Server:

802.1X

Use 802.1X Security

Authentication: MD5

Username:

Password:

Top

Departemen Marketing

PC0(1)(3)

Physical Config Desktop Programming Attributes

### IP Configuration

Interface FastEthernet0

IP Configuration

DHCP  Static

IPv4 Address 192.168.40.11

Subnet Mask 255.255.255.0

Default Gateway 192.168.40.1

DNS Server 192.168.40.254

IPv6 Configuration

Automatic  Static

IPv6 Address /

Link Local Address FE80::2E0:F7FF:FE3C:3C47

Default Gateway

DNS Server

802.1X

Use 802.1X Security

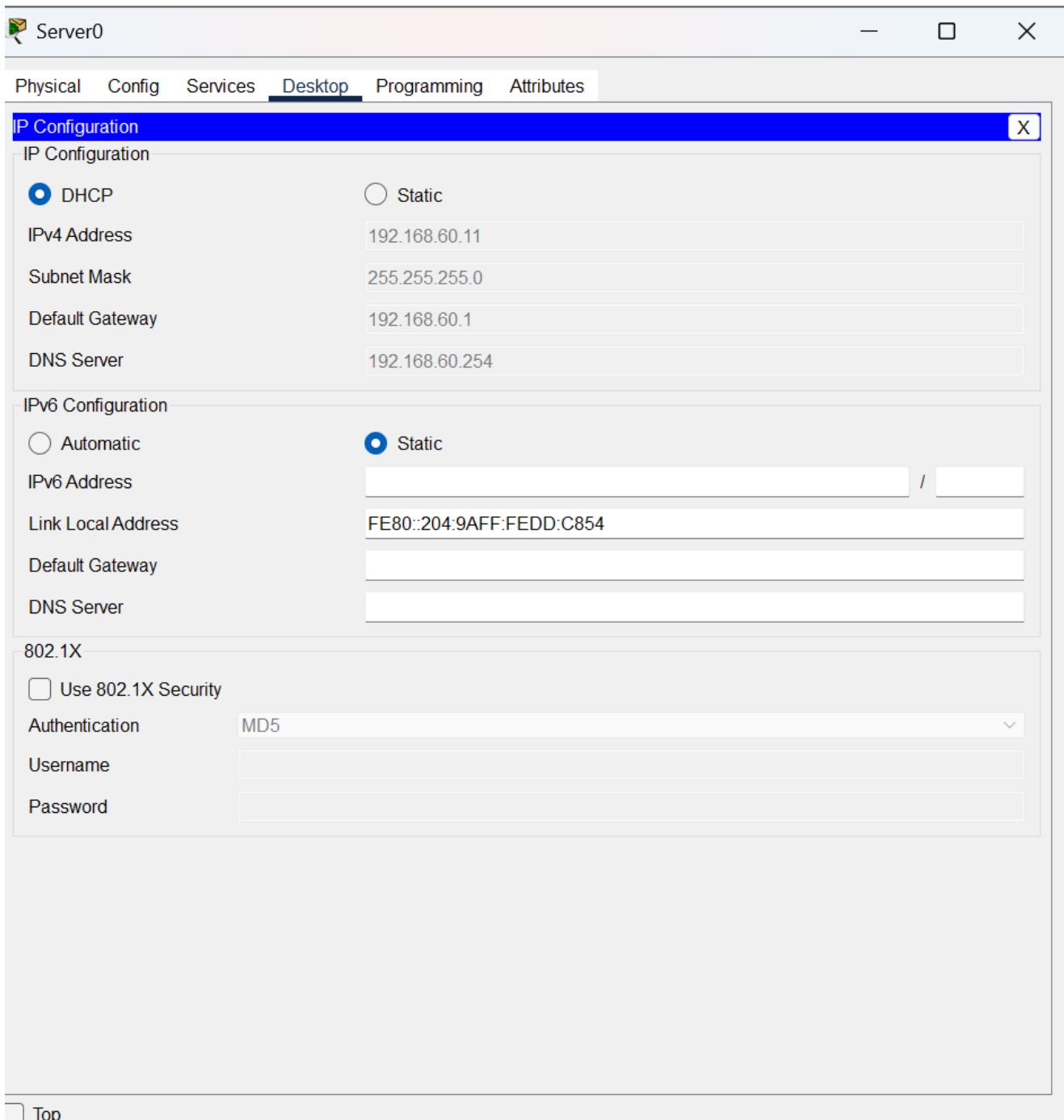
Authentication MD5

Username

Password

Top

Server Farm



Penjelasan : Pengujian terhadap fitur DHCP telah dilakukan dengan tujuan untuk memastikan bahwa perangkat client dapat memperoleh konfigurasi jaringan secara otomatis dari server DHCP. Dalam pengujian ini, perangkat PC dan server diatur untuk menggunakan pengaturan IP otomatis. Setelah terhubung ke jaringan, kedua perangkat berhasil menerima alamat IP, subnet mask, default gateway, dan alamat DNS tanpa perlu konfigurasi manual. Hal ini dibuktikan melalui screenshot yang menunjukkan bahwa masing-masing perangkat mendapatkan parameter jaringan yang lengkap dan sesuai dengan konfigurasi yang telah ditentukan di server DHCP. Berdasarkan hasil dibawah, dapat disimpulkan bahwa fitur DHCP telah berhasil diuji dan berjalan dengan baik.

### Matriks Pengujian ACL (Hasil Pengujian ACL Berdasarkan IP)

## Uji Konektivitas Departemen IT A

The screenshot shows a Windows desktop environment with a Cisco Packet Tracer application window open. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. A Command Prompt window is embedded within the Cisco application, showing the output of several ping commands. The ping results indicate connectivity issues, with many requests timing out or failing to receive replies.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.11: bytes=32 time=13ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

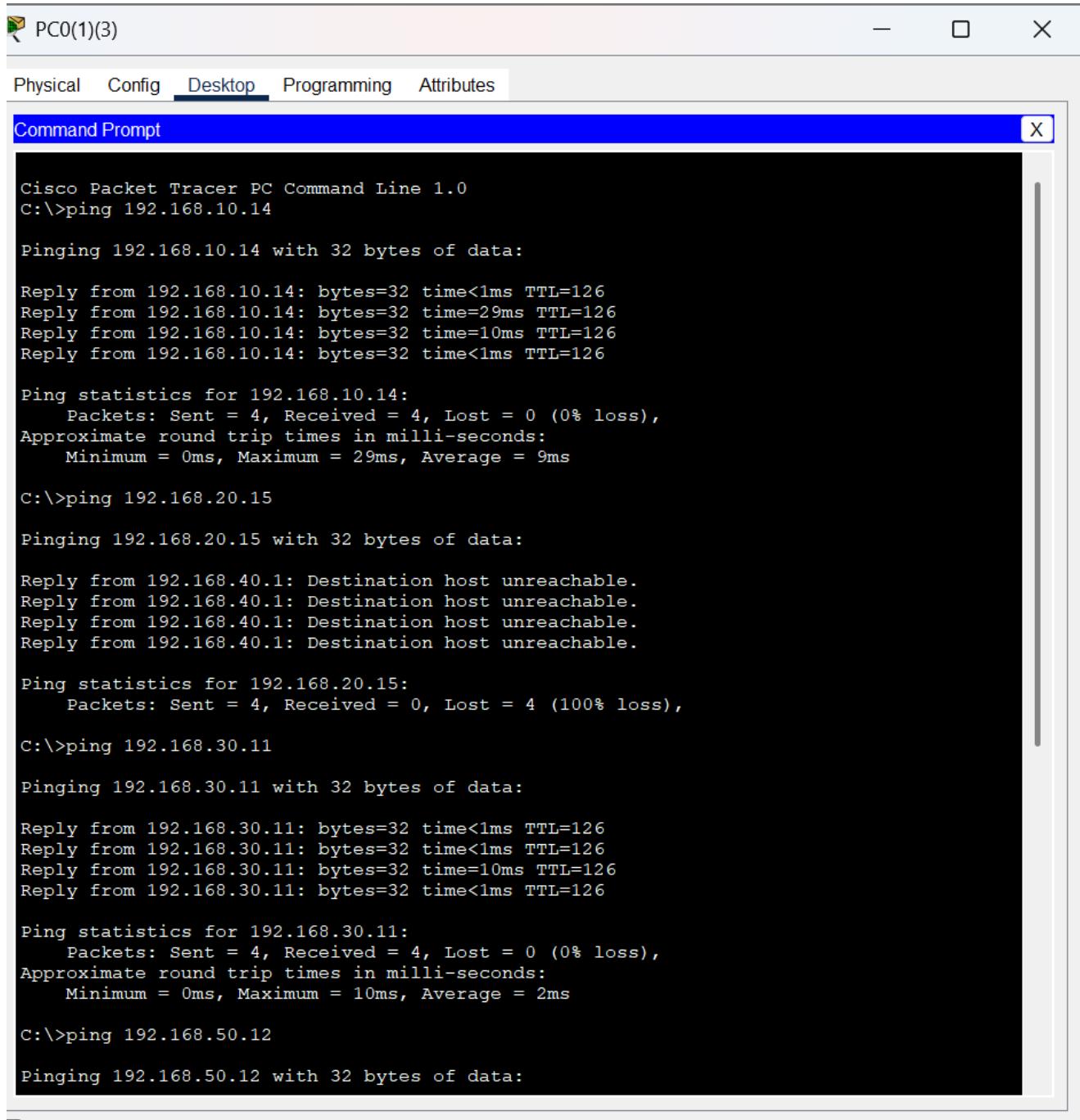
C:\>ping 192.168.50.12
```

Top

The taskbar shows various pinned icons for Microsoft Office applications like OneDrive, File Explorer, and Microsoft Teams. The system tray displays the date and time (6:42 PM, 5/15/2025), battery level, signal strength, and volume controls.

Pada gambar Departemen IT A terlihat topologi jaringan untuk divisi teknologi informasi. Struktur jaringan terdiri dari beberapa workstation yang terhubung ke switch utama, dengan server yang menjalankan aplikasi penting perusahaan. Kode konfigurasi pada topologi ini kemungkinan menggunakan VLAN tagging (802.1Q) untuk mengisolasi lalu lintas data IT dari departemen lain, dengan implementasi ACL (Access Control List) untuk membatasi akses ke server sensitif. Tujuan dari konfigurasi ini adalah untuk memastikan departemen IT memiliki infrastruktur yang aman dan terisolasi untuk mengelola sistem perusahaan. Hasilnya adalah jaringan departemen IT yang terlindungi dengan baik dan mampu melakukan administrasi sistem tanpa gangguan dari departemen lain, sekaligus mempertahankan visibilitas penuh terhadap seluruh jaringan perusahaan.

## Uji Konektivitas Departemen Marketing



The screenshot shows a Cisco Packet Tracer interface with a window titled "Command Prompt". The window displays the output of several ping commands from a PC0(1)(3) workstation. The results show successful pings to 192.168.10.14 and 192.168.30.11, while attempts to ping 192.168.20.15 and 192.168.50.12 resulted in destination host unreachable errors due to 100% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=29ms TTL=126
Reply from 192.168.10.14: bytes=32 time=10ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 29ms, Average = 9ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:
```

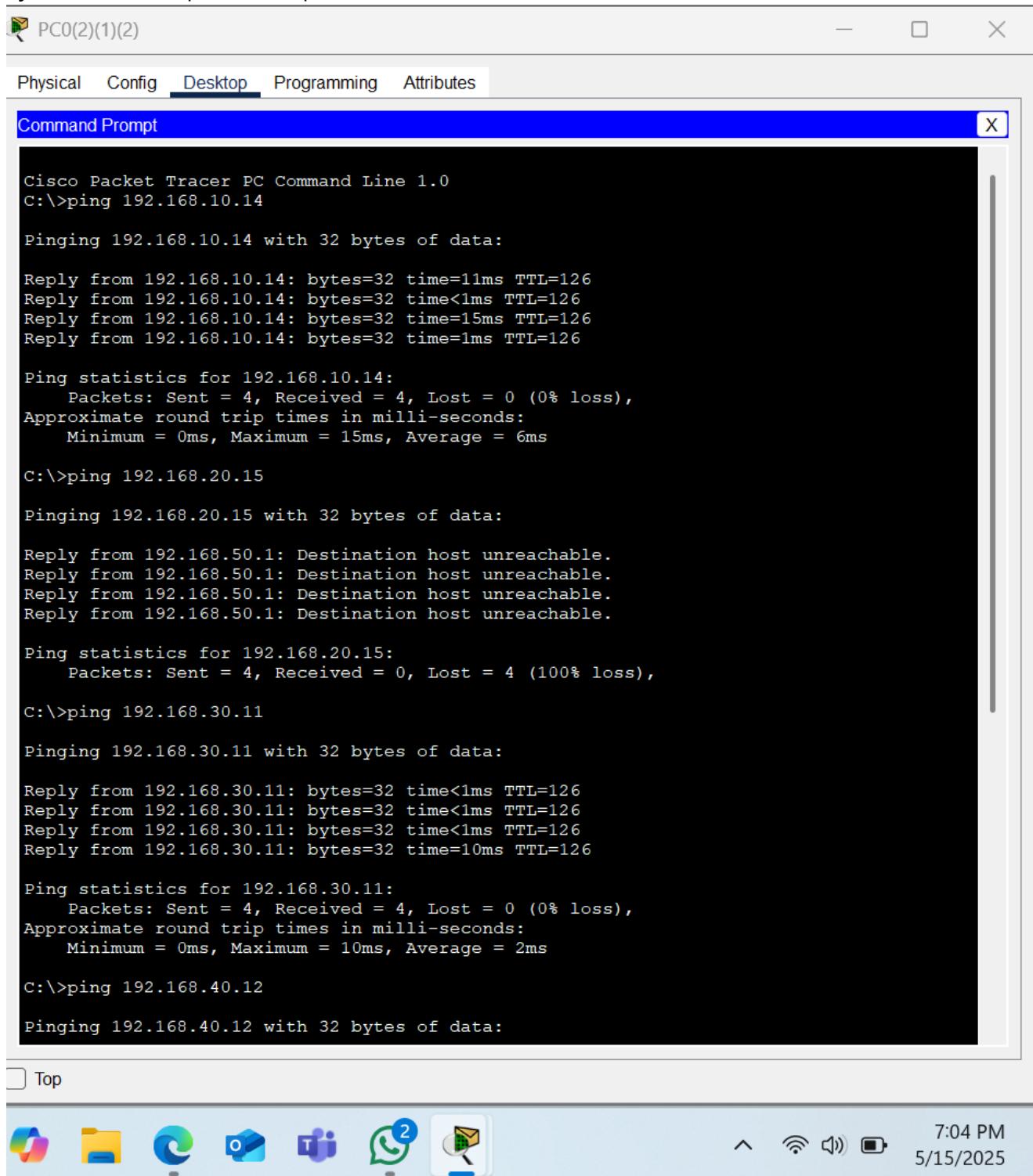
Top



6:57 PM  
5/15/2025

Pada gambar Marketing A terlihat topologi jaringan untuk departemen marketing. Struktur jaringan terdiri dari beberapa workstation yang terhubung ke switch utama, dengan printer dan perangkat multimedia untuk kebutuhan marketing. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data marketing, dengan implementasi ACL yang membatasi akses ke departemen keuangan namun mengizinkan akses ke server farm. Tujuan dari konfigurasi ini adalah untuk memastikan departemen marketing memiliki akses yang diperlukan ke sumber daya perusahaan sambil mempertahankan keamanan data sensitif. Hasilnya adalah jaringan marketing yang efisien dengan akses terkontrol ke sumber daya yang diperlukan untuk operasi sehari-hari.

## Uji Konektivitas Departemen Operasional



The screenshot shows a Windows desktop environment with a Cisco Packet Tracer window open. The window title is "PC0(2)(1)(2)". The tabs at the top are "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. A "Command Prompt" window is displayed, showing the results of several ping commands. The output includes:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=11ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=15ms TTL=126
Reply from 192.168.10.14: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.50.1: Destination host unreachable.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

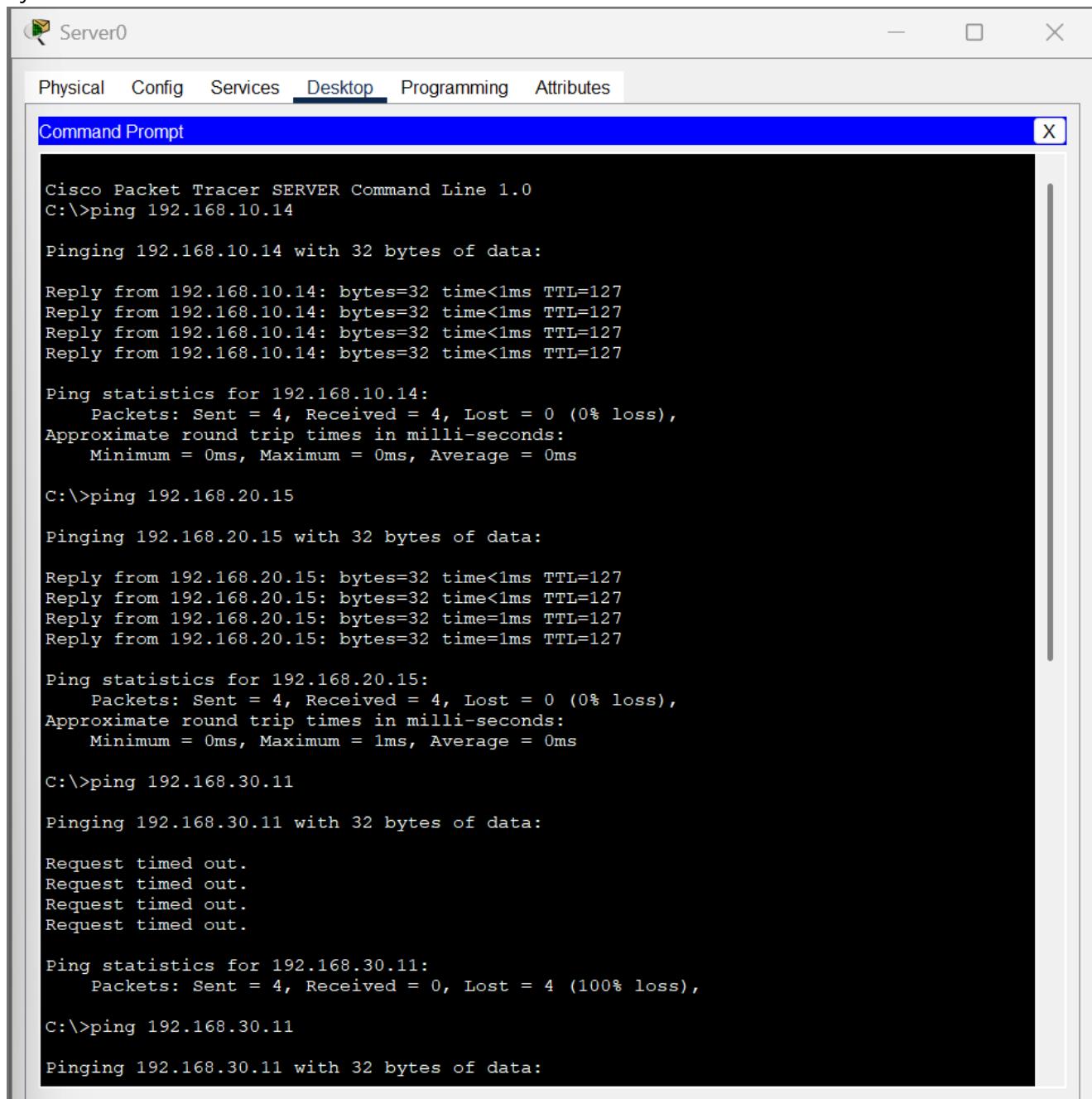
Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:
```

Pada gambar Operasional A terlihat topologi jaringan untuk departemen operasional. Struktur jaringan terdiri dari workstation yang terhubung ke switch utama, dengan perangkat IoT dan sistem monitoring operasional. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data operasional, dengan implementasi ACL yang membatasi akses ke departemen keuangan namun mengizinkan akses ke server farm. Tujuan dari konfigurasi ini adalah untuk memastikan departemen operasional memiliki akses yang diperlukan ke sistem monitoring dan kontrol sambil mempertahankan keamanan jaringan. Hasilnya adalah jaringan operasional yang stabil dengan kemampuan monitoring real-time dan akses terkontrol ke sistem yang diperlukan.

## Uji Konektivitas Server Farm



The screenshot shows a Cisco Packet Tracer Command Line window titled "Command Prompt". It displays the results of several ping commands issued from the command line. The results show successful pings to 192.168.10.14, 192.168.20.15, and 192.168.30.11, with 0% loss and low round-trip times. However, there is a request timed out for 192.168.30.11. The ping to 192.168.30.11 shows 100% loss.

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    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<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 = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:
```

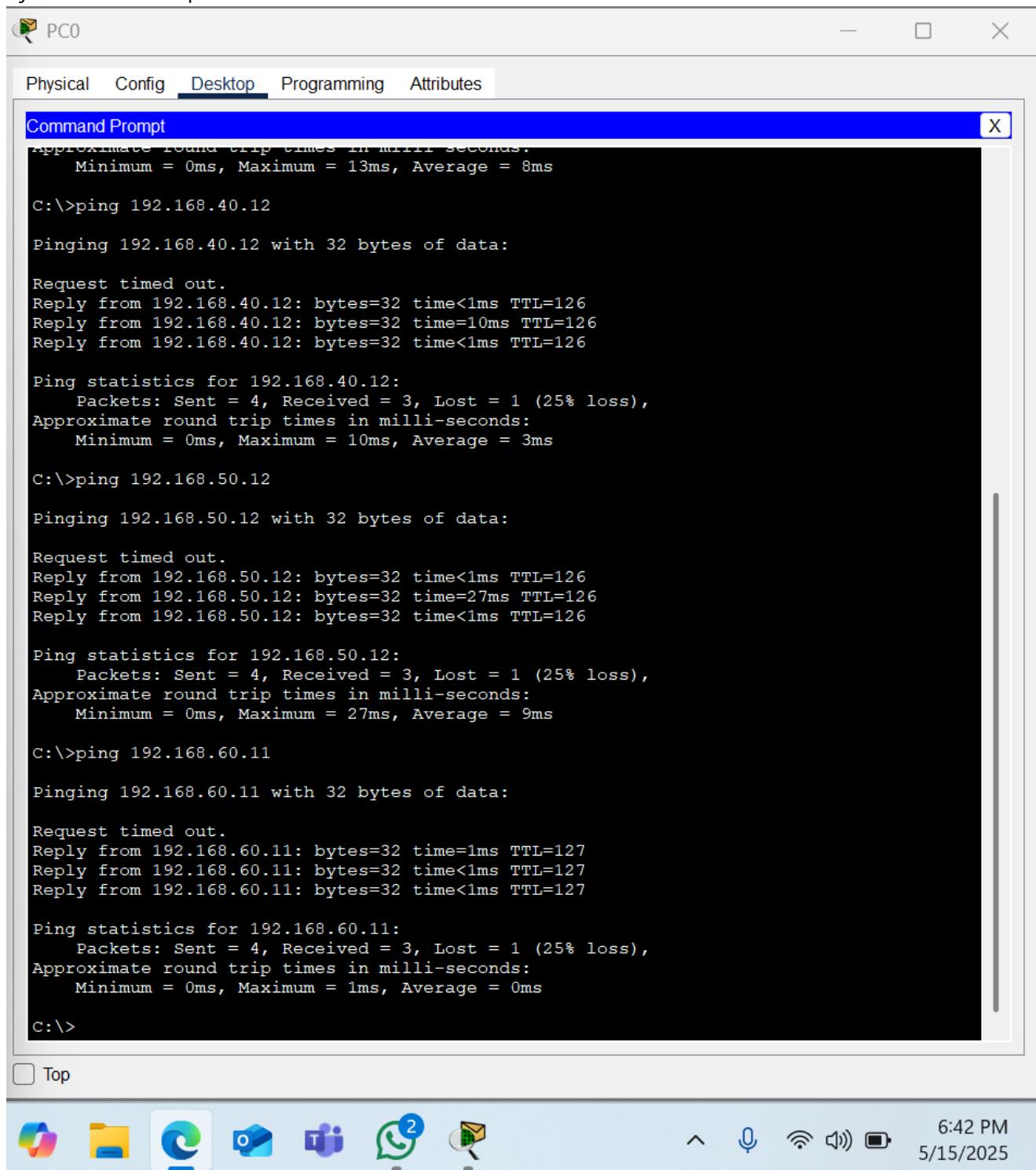
Top



The taskbar at the bottom of the screen shows various icons for Microsoft Office applications (Word, Excel, PowerPoint, OneDrive, and Teams). On the right side, it displays the date (5/15/2025), time (6:55 PM), and battery status.

Pada gambar Server A terlihat topologi jaringan untuk server farm perusahaan. Struktur jaringan terdiri dari beberapa server yang terhubung ke switch utama, dengan sistem storage dan backup. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data server, dengan implementasi ACL yang mengatur akses dari berbagai departemen. Tujuan dari konfigurasi ini adalah untuk memastikan server farm memiliki keamanan tinggi dan akses terkontrol dari departemen-departemen yang membutuhkan. Hasilnya adalah infrastruktur server yang aman dengan akses yang diatur berdasarkan kebutuhan masing-masing departemen.

## Uji Konektivitas Departemen IT B



```
PCO
Physical Config Desktop Programming Attributes

Command Prompt
Approximate round trip times in milli seconds.
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=27ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.50.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 27ms, Average = 9ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

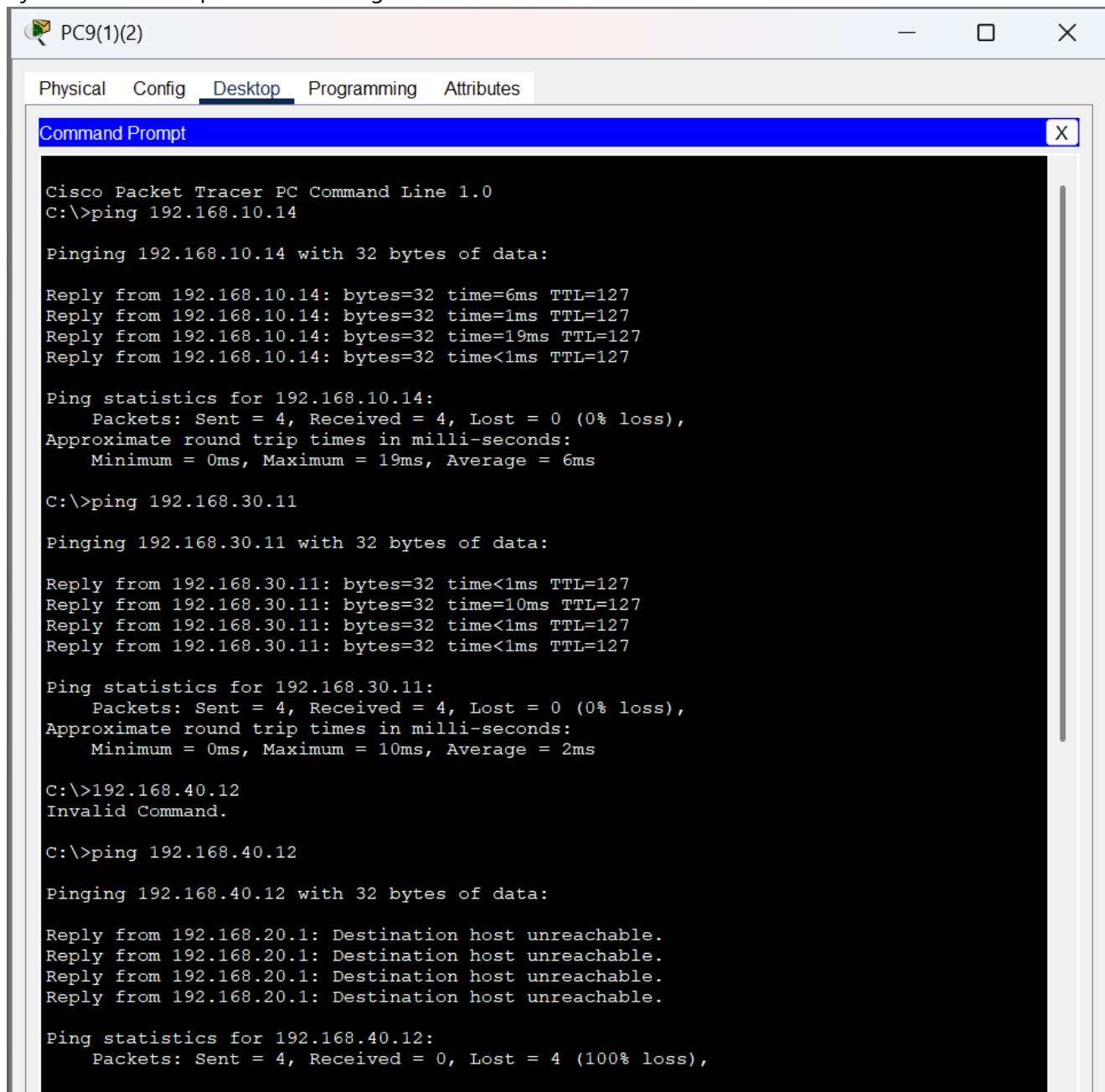
Request timed out.
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Pada gambar Departemen IT B terlihat topologi jaringan backup untuk divisi teknologi informasi. Struktur jaringan terdiri dari workstation dan server backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi dan failover, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen IT A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman dan terisolasi untuk departemen IT. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Keuangan A



The screenshot shows a Cisco Packet Tracer interface with a 'Command Prompt' window open. The window displays the following command-line session:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=6ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=19ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 6ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=10ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>192.168.40.12
Invalid Command.

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Top



6:46 PM  
5/15/2025

Pada gambar Departemen Keuangan A terlihat topologi jaringan untuk divisi keuangan. Struktur jaringan terdiri dari workstation yang terhubung ke switch utama, dengan printer dan perangkat keamanan khusus. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data keuangan, dengan implementasi ACL yang membatasi akses ke departemen marketing dan operasional. Tujuan dari konfigurasi ini adalah untuk memastikan departemen keuangan memiliki infrastruktur yang aman dan terisolasi untuk mengelola data finansial perusahaan. Hasilnya adalah jaringan keuangan yang terlindungi dengan baik dan mampu melakukan transaksi finansial dengan tingkat keamanan tinggi.

## Uji Konektivitas Departemen Keuangan B

The screenshot shows a Windows desktop environment. At the top, there is a window titled "PC9(1)(2)" containing a "Command Prompt" window. The "Desktop" tab is selected in the window's tabs. The command prompt window displays several ping commands and their results:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 10ms, Average = 2ms  
  
C:\>192.168.40.12  
Invalid Command.  
  
C:\>ping 192.168.40.12  
  
Pinging 192.168.40.12 with 32 bytes of data:  
  
Reply from 192.168.20.1: Destination host unreachable.  
  
Ping statistics for 192.168.40.12:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ping 192.168.50.12  
  
Pinging 192.168.50.12 with 32 bytes of data:  
  
Reply from 192.168.20.1: Destination host unreachable.  
  
Ping statistics for 192.168.50.12:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ping 192.168.60.11  
  
Pinging 192.168.60.11 with 32 bytes of data:  
  
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127  
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127  
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127  
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127  
  
Ping statistics for 192.168.60.11:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>
```

At the bottom of the screen, the taskbar is visible with various icons and the system tray showing the date and time.

Pada gambar Departemen Keuangan B terlihat topologi jaringan backup untuk divisi keuangan. Struktur jaringan terdiri dari workstation dan sistem backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen Keuangan A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen keuangan. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen SDM A

The screenshot shows a Cisco Packet Tracer interface. At the top, there are tabs: Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Below it is a window titled "Command Prompt" with the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

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<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time=10ms 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 = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

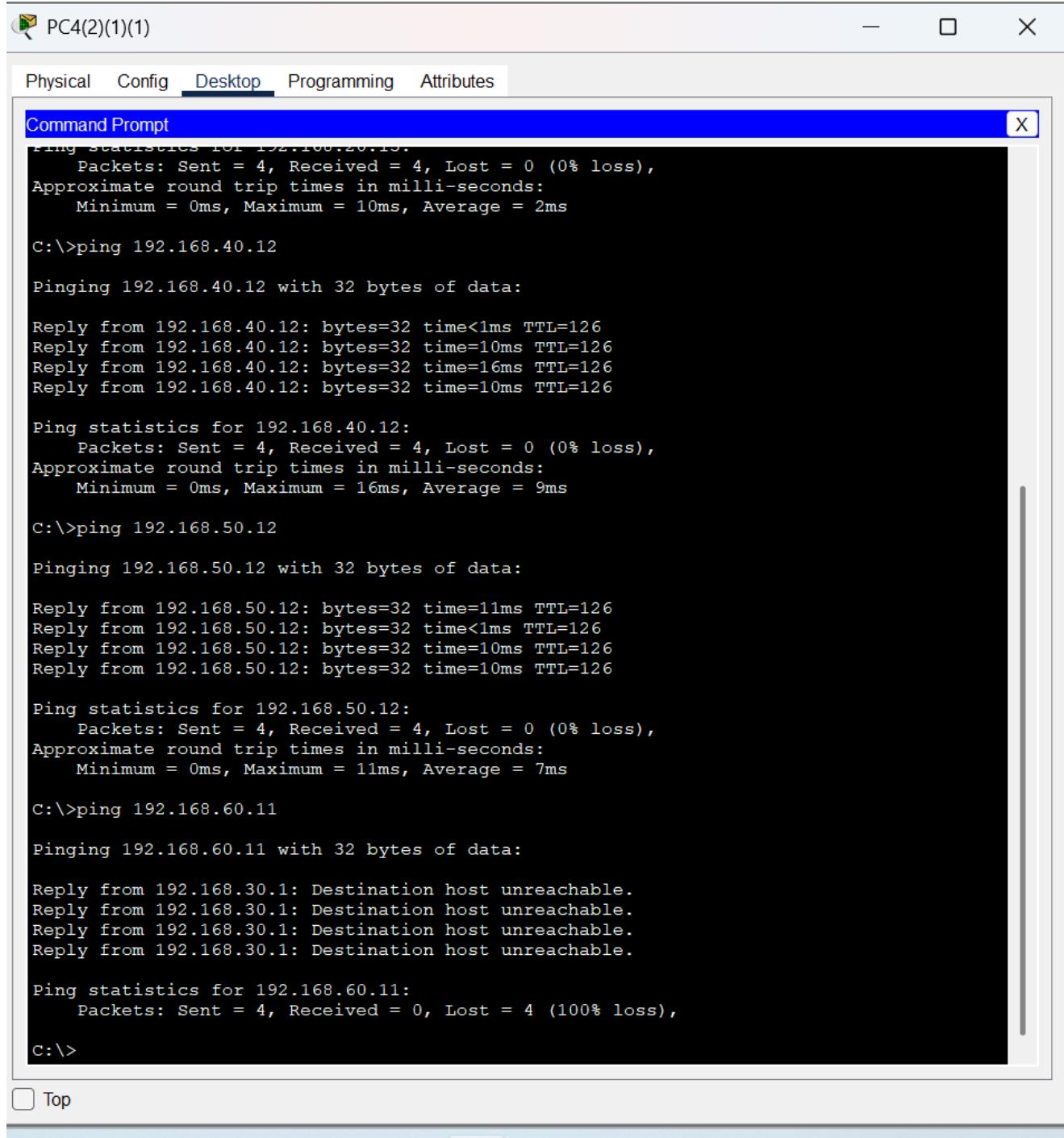
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

C:\>ping 192.168.50.12
```

At the bottom of the window, there is a checkbox labeled "Top" and a toolbar with various icons.

Pada gambar Departemen SDM A terlihat topologi jaringan untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation yang terhubung ke switch utama, dengan printer dan sistem manajemen SDM. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data SDM, dengan implementasi ACL yang membatasi akses ke server farm kecuali host tertentu. Tujuan dari konfigurasi ini adalah untuk memastikan departemen SDM memiliki akses yang diperlukan ke sistem manajemen karyawan sambil mempertahankan keamanan data. Hasilnya adalah jaringan SDM yang efisien dengan akses terkontrol ke sistem yang diperlukan.



The screenshot shows a Windows desktop environment. At the top, there is a taskbar with several pinned icons: File Explorer, Microsoft Edge, File History, Microsoft Teams, WhatsApp, and Mail. To the right of the taskbar, the system tray displays the date (5/15/2025), time (6:49 PM), battery status, signal strength, and volume level. Below the taskbar is a window titled "Command Prompt". The window contains the following command-line output:

```
Ping statistics for 192.168.20.13.
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=11ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Pada gambar Departemen SDM B terlihat topologi jaringan backup untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation dan sistem backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen SDM A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen SDM. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Marketing B

```
Ping statistics for 192.168.20.15:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=14ms TTL=127
Reply from 192.168.50.12: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 14ms, Average = 4ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

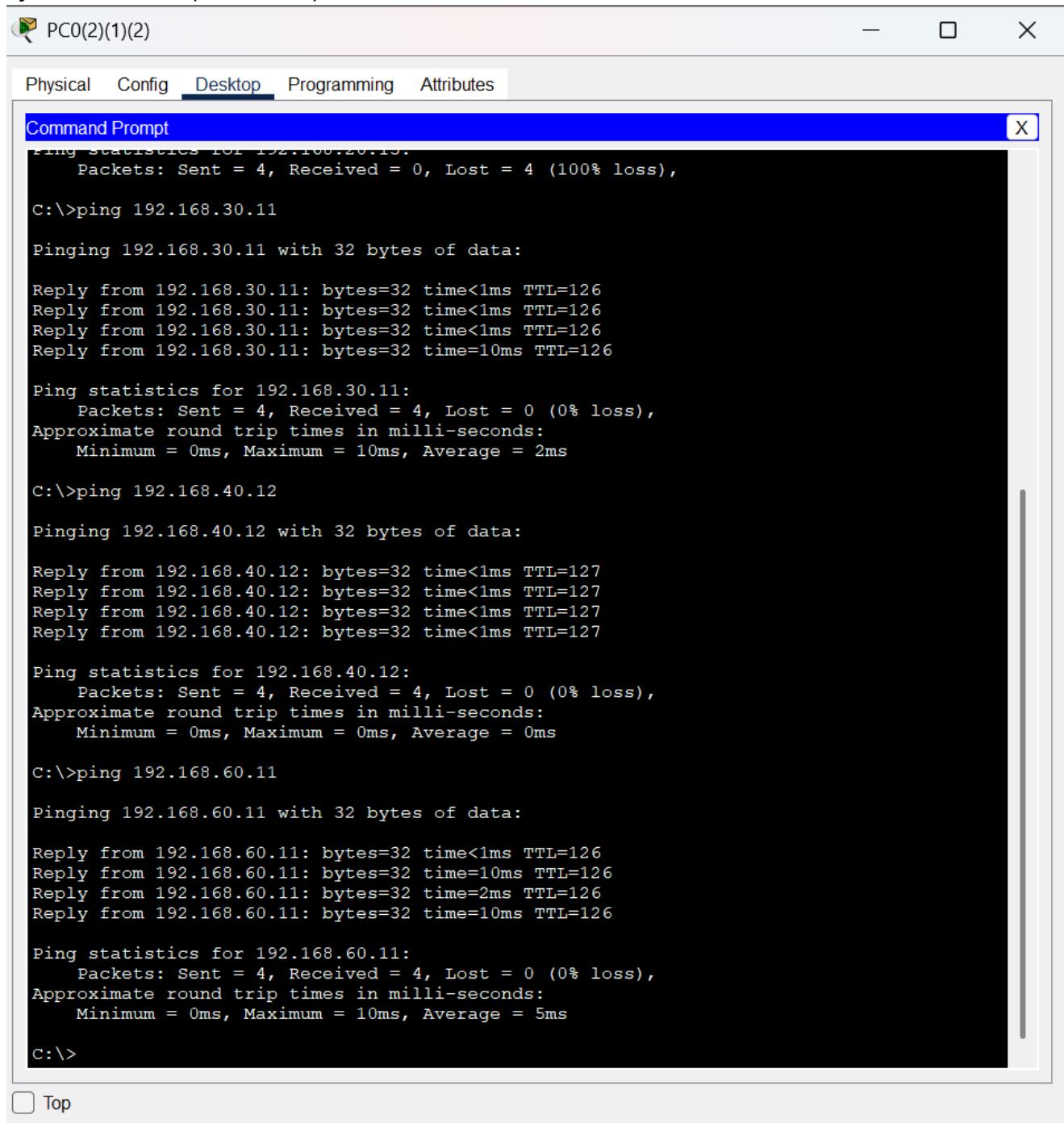
Reply from 192.168.60.11: bytes=32 time=41ms TTL=126
Reply from 192.168.60.11: bytes=32 time=17ms TTL=126
Reply from 192.168.60.11: bytes=32 time=1ms TTL=126
Reply from 192.168.60.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.60.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 41ms, Average = 14ms

C:\>
```

Pada gambar Marketing B terlihat topologi jaringan backup untuk departemen marketing. Struktur jaringan terdiri dari workstation dan sistem backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen Marketing A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen marketing. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Operasional B



```
PC0(2)(1)(2)
Physical Config Desktop Programming Attributes

Command Prompt
X

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

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.30.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=127

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 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.60.11: bytes=32 time<1ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126
Reply from 192.168.60.11: bytes=32 time=2ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
```

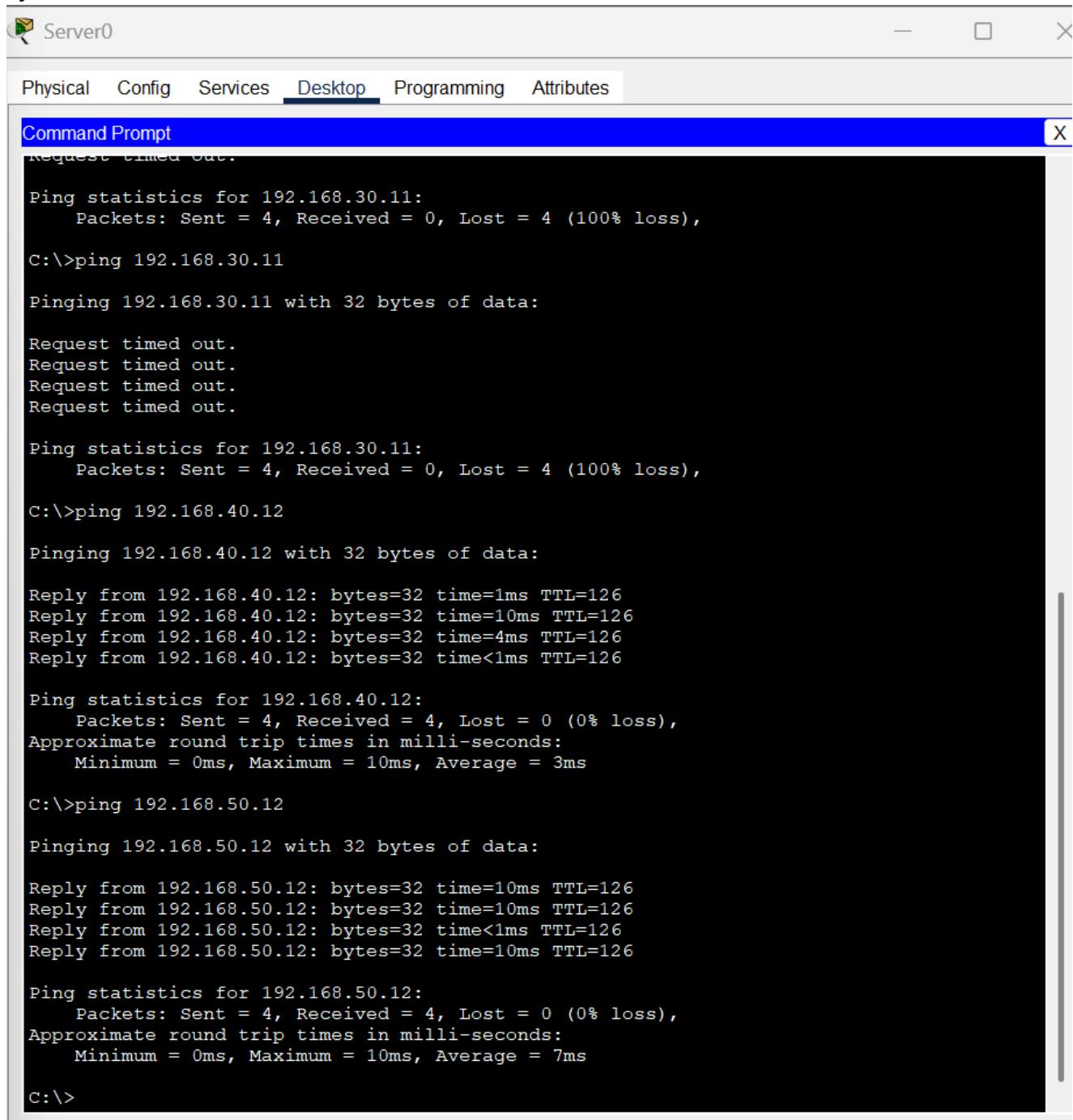
Top



7:04 PM  
5/15/2025

Pada gambar Operasional B terlihat topologi jaringan backup untuk departemen operasional. Struktur jaringan terdiri dari workstation dan sistem monitoring backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan departemen Operasional A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk departemen operasional. Hasilnya adalah sistem backup yang terlindungi dengan baik dan mampu mengambil alih operasi monitoring jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Server Farm B



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window title bar also includes the text "Server0". The menu bar at the top has items: Physical, Config, Services, Desktop, Programming, and Attributes. The "Desktop" item is underlined, indicating it is the active tab. The main area of the window displays the output of several ping commands:

```
Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=4ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

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 = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 7ms

C:\>
```

Pada gambar Server B terlihat topologi jaringan backup untuk server farm perusahaan. Struktur jaringan terdiri dari server backup dan sistem storage yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mencerminkan kebijakan keamanan Server Farm A. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur server cadangan yang aman dan terisolasi. Hasilnya adalah sistem backup server yang terlindungi dengan baik dan mampu mengambil alih operasi jika terjadi kegagalan pada server utama.

## Uji Konektivitas Departemen IT A (Detail)

The screenshot shows a Cisco Packet Tracer interface. At the top, there's a menu bar with 'Physical', 'Config', 'Desktop' (which is selected), 'Programming', and 'Attributes'. Below the menu is a toolbar with icons for 'File', 'Edit', 'View', 'Tools', 'Help', and a search bar. The main window contains a terminal window titled 'Command Prompt' with the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.11: bytes=32 time=13ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.50.12
```

At the bottom of the window, there's a 'Top' button and a taskbar with various icons: File, Copy, Paste, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneDrive, Microsoft Teams, WhatsApp, and Mail. The taskbar also shows the date and time: 6:42 PM, 5/15/2025.

Pada gambar Departemen IT A terlihat detail konfigurasi jaringan untuk divisi teknologi informasi. Struktur jaringan terdiri dari workstation administrator, server development, dan perangkat testing yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk segmentasi jaringan internal IT, dengan implementasi ACL yang mengatur akses ke server development dan testing. Tujuan dari konfigurasi ini adalah untuk memastikan departemen IT memiliki lingkungan development dan testing yang aman dan terisolasi. Hasilnya adalah infrastruktur IT yang memungkinkan pengembangan dan pengujian aplikasi dengan tingkat keamanan tinggi.

## Uji Konektivitas Departemen IT B (Detail)

```
PC0
Physical Config Desktop Programming Attributes

Command Prompt
Approximate round trip times in milli seconds.
    Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=27ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.50.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 27ms, Average = 9ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.60.11: bytes=32 time=1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127
Reply from 192.168.60.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Top

Pada gambar Departemen IT B terlihat detail konfigurasi jaringan backup untuk divisi teknologi informasi. Struktur jaringan terdiri dari workstation backup, server staging, dan perangkat monitoring yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi dan failover, dengan implementasi ACL yang mengatur akses ke server staging dan monitoring. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk pengembangan dan pengujian aplikasi. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi development dan testing jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Keuangan A (Detail)

The screenshot shows a Cisco Packet Tracer interface with a network diagram and configuration details for the Finance department. The configuration window displays the following command-line output:

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=6ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=19ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 6ms

C:>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time=10ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127
Reply from 192.168.30.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:>192.168.40.12
Invalid Command.

C:>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

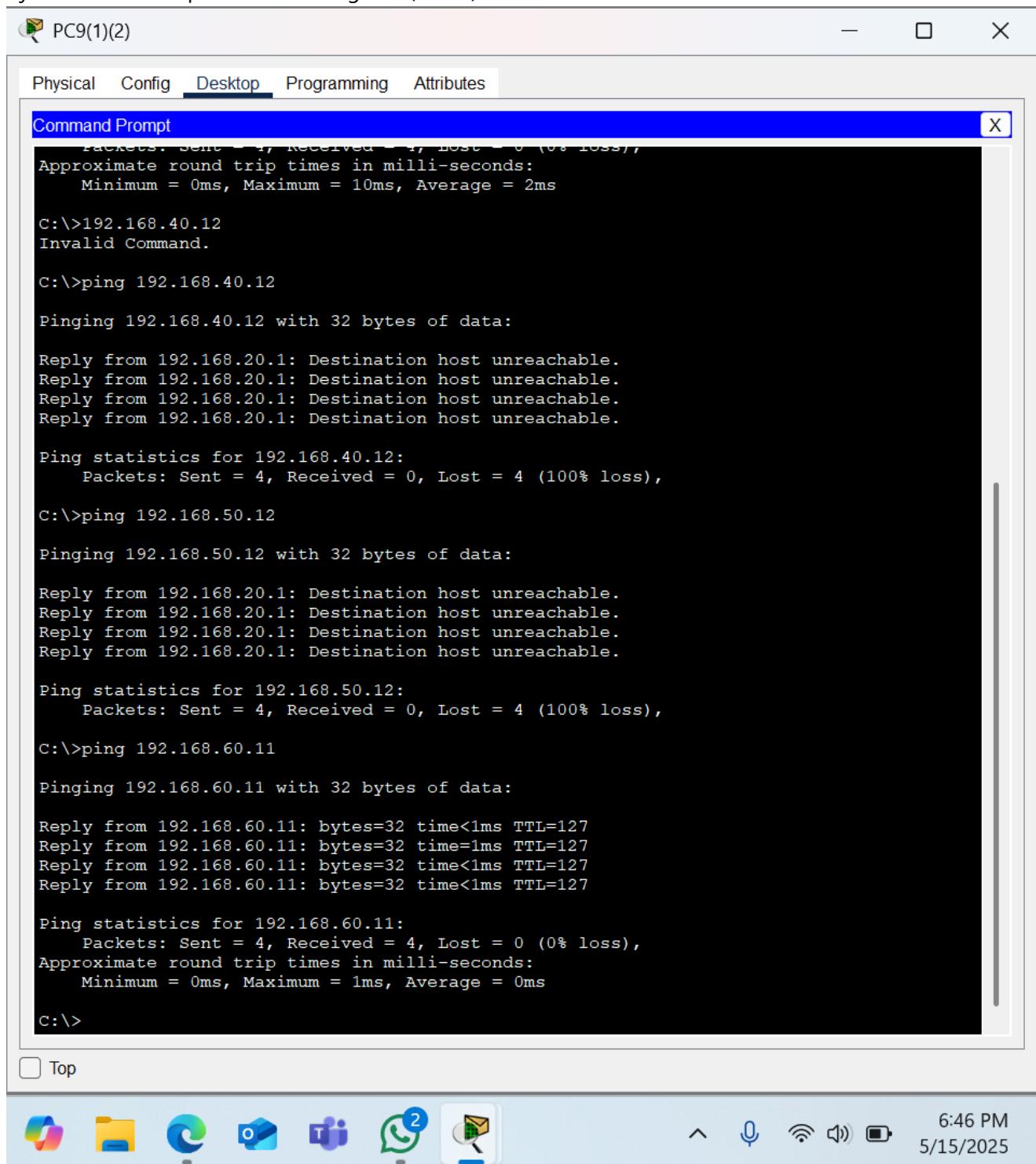
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom of the window, there is a toolbar with icons for file operations and a status bar showing the date and time.

Pada gambar Departemen Keuangan A terlihat detail konfigurasi jaringan untuk divisi keuangan. Struktur jaringan terdiri dari workstation akuntansi, server database keuangan, dan printer khusus yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data keuangan, dengan implementasi ACL yang membatasi akses ke database keuangan. Tujuan dari konfigurasi ini adalah untuk memastikan departemen keuangan memiliki akses yang aman ke data finansial perusahaan. Hasilnya adalah jaringan keuangan yang terlindungi dengan baik untuk operasi akuntansi dan keuangan.

## Uji Konektivitas Departemen Keuangan B (Detail)



Pada gambar Departemen Keuangan B terlihat detail konfigurasi jaringan backup untuk divisi keuangan. Struktur jaringan terdiri dari workstation backup, server database cadangan, dan printer backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke database cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi keuangan. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi keuangan jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen SDM A (Detail)

The screenshot shows a Windows desktop environment with a Cisco Packet Tracer window open. The window title is "Command Prompt". The content of the window displays the results of several ping commands issued from the command line. The results show successful connections to hosts at 192.168.10.14, 192.168.20.15, 192.168.40.12, and 192.168.50.12, with low ping times and 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=1ms TTL=127
Reply from 192.168.10.14: bytes=32 time<1ms TTL=127
Reply from 192.168.10.14: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

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<1ms TTL=127
Reply from 192.168.20.15: bytes=32 time=10ms 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 = 10ms, Average = 2ms

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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

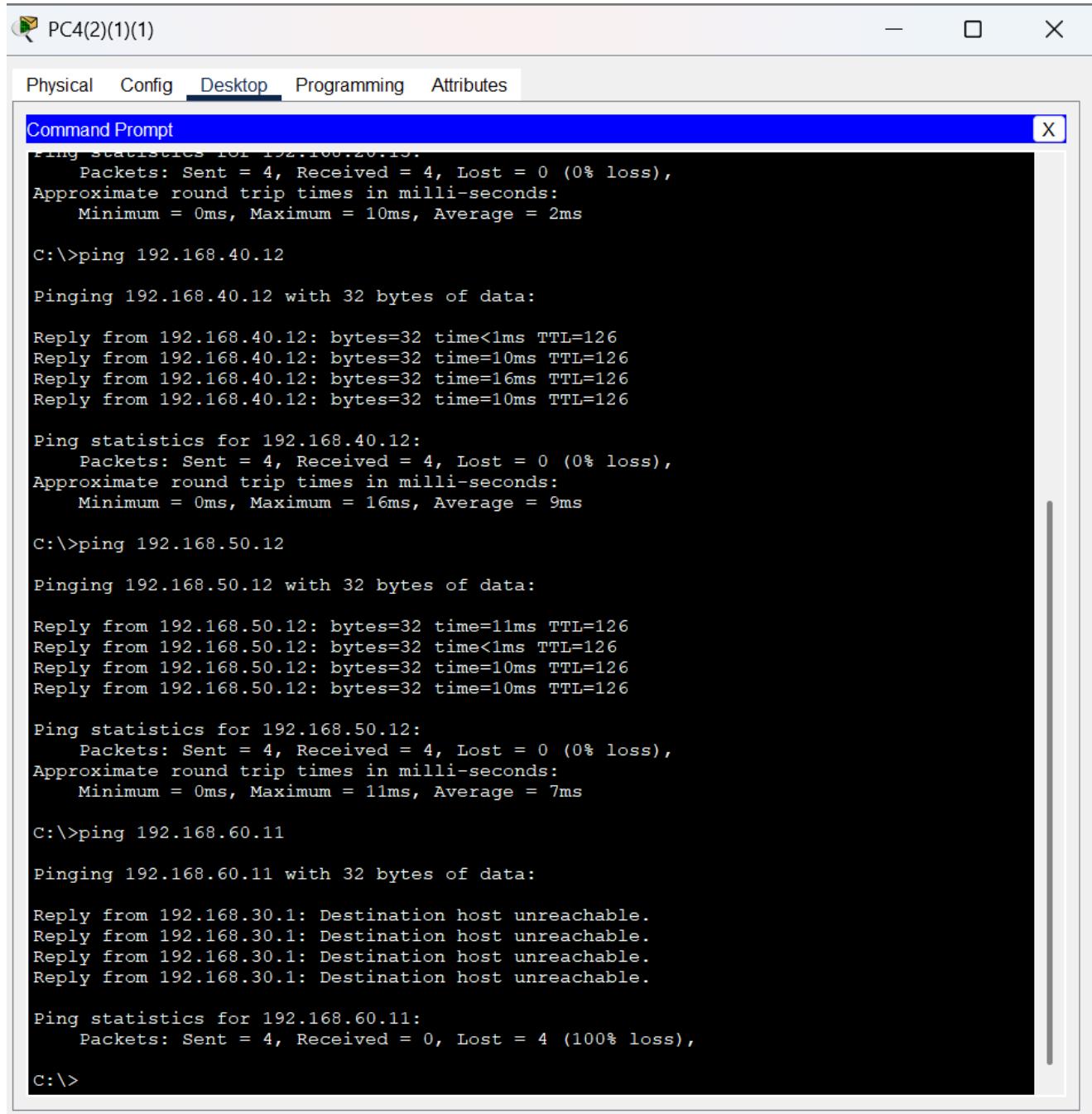
C:\>ping 192.168.50.12
```

Top

The taskbar at the bottom of the screen shows various pinned icons for Microsoft Word, File Explorer, OneDrive, Microsoft Teams, WhatsApp, and Edge browser. On the right side of the taskbar, there are icons for signal strength, battery level, and the date and time (6:49 PM, 5/15/2025).

Pada gambar Departemen SDM A terlihat detail konfigurasi jaringan untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation HR, server database karyawan, dan sistem absensi yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data SDM, dengan implementasi ACL yang mengatur akses ke database karyawan. Tujuan dari konfigurasi ini adalah untuk memastikan departemen SDM memiliki akses yang aman ke data karyawan. Hasilnya adalah jaringan SDM yang terlindungi dengan baik untuk operasi manajemen karyawan.

## Uji Konektivitas Departemen SDM B (Detail)



The screenshot shows a Windows desktop environment. At the top, there is a taskbar with several pinned icons: File Explorer, OneDrive, Edge browser, Microsoft Teams, WhatsApp, and Mail. The system tray shows the date (5/15/2025), time (6:49 PM), battery status, signal strength, and volume level. Below the taskbar is a window titled "Command Prompt". The window contains the following command-line output:

```
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 = 10ms, Average = 2ms

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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=16ms TTL=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126

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 = 16ms, Average = 9ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=11ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.50.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Pada gambar Departemen SDM B terlihat detail konfigurasi jaringan backup untuk divisi sumber daya manusia. Struktur jaringan terdiri dari workstation backup, server database cadangan, dan sistem absensi backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke database cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi SDM. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi manajemen karyawan jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Marketing A (Detail)

The screenshot shows a Cisco Packet Tracer interface with a window titled "Command Prompt". The window displays the results of several ping commands issued from a workstation (PC0(1)(3)) to various hosts in the network. The results show successful pings to 192.168.10.14 and 192.168.20.15, while pings to 192.168.40.1 and 192.168.30.11 result in destination host unreachable errors. Pings to 192.168.50.12 also fail. Below the command prompt window, the taskbar shows icons for file, folder, start, and search, along with system status indicators like battery level and date/time (6:57 PM, 5/15/2025).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=29ms TTL=126
Reply from 192.168.10.14: bytes=32 time=10ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 29ms, Average = 9ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.

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

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:
```

Pada gambar Marketing A terlihat detail konfigurasi jaringan untuk departemen marketing. Struktur jaringan terdiri dari workstation marketing, server konten, dan perangkat multimedia yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data marketing, dengan implementasi ACL yang mengatur akses ke server konten. Tujuan dari konfigurasi ini adalah untuk memastikan departemen marketing memiliki akses yang aman ke asset digital dan konten marketing. Hasilnya adalah jaringan marketing yang terlindungi dengan baik untuk operasi pemasaran digital.

## Uji Konektivitas Departemen Marketing B (Detail)

The screenshot shows a Windows desktop environment. At the top, there is a window titled "PC0(1)(3)" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. Below this is a "Command Prompt" window with the title "Ping statistics for 192.168.20.15.". The command prompt displays several ping operations to different IP addresses (192.168.30.11, 192.168.50.12, 192.168.60.11) with their respective statistics (packets sent/received/lost, round trip times, and average). The taskbar at the bottom includes icons for File Explorer, Microsoft Edge, OneDrive, Teams, WhatsApp, and File Explorer again. The system tray shows the date (5/15/2025), time (6:57 PM), and battery status.

```
Ping statistics for 192.168.20.15.
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=1ms TTL=127
Reply from 192.168.50.12: bytes=32 time=14ms TTL=127
Reply from 192.168.50.12: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 14ms, Average = 4ms

C:\>ping 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

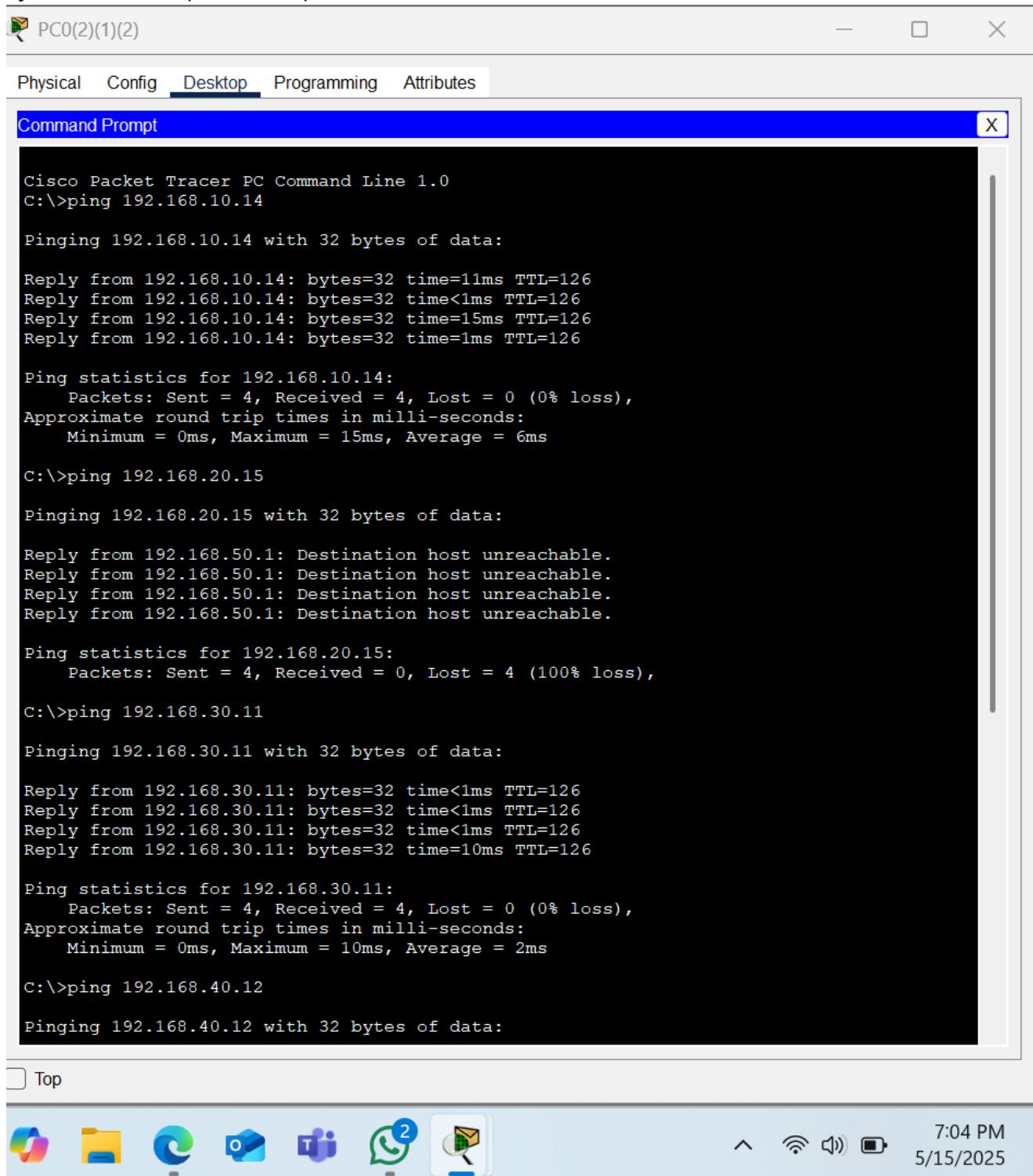
Reply from 192.168.60.11: bytes=32 time=41ms TTL=126
Reply from 192.168.60.11: bytes=32 time=17ms TTL=126
Reply from 192.168.60.11: bytes=32 time=1ms TTL=126
Reply from 192.168.60.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.60.11:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 41ms, Average = 14ms

C:\>
```

Pada gambar Marketing B terlihat detail konfigurasi jaringan backup untuk departemen marketing. Struktur jaringan terdiri dari workstation backup, server konten cadangan, dan perangkat multimedia backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke server konten cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi marketing. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi pemasaran digital jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Departemen Operasional A (Detail)



The screenshot shows a window titled "PC0(2)(1)(2)" containing a "Command Prompt" window. The Command Prompt displays ping results for various IP addresses (192.168.10.14, 192.168.20.15, 192.168.30.11, 192.168.40.12) from a Cisco Packet Tracer PC Command Line 1.0 environment. The results show varying levels of connectivity and latency.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time=11ms TTL=126
Reply from 192.168.10.14: bytes=32 time<1ms TTL=126
Reply from 192.168.10.14: bytes=32 time=15ms TTL=126
Reply from 192.168.10.14: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms

C:\>ping 192.168.20.15

Pinging 192.168.20.15 with 32 bytes of data:

Reply from 192.168.50.1: Destination host unreachable.

Ping statistics for 192.168.20.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

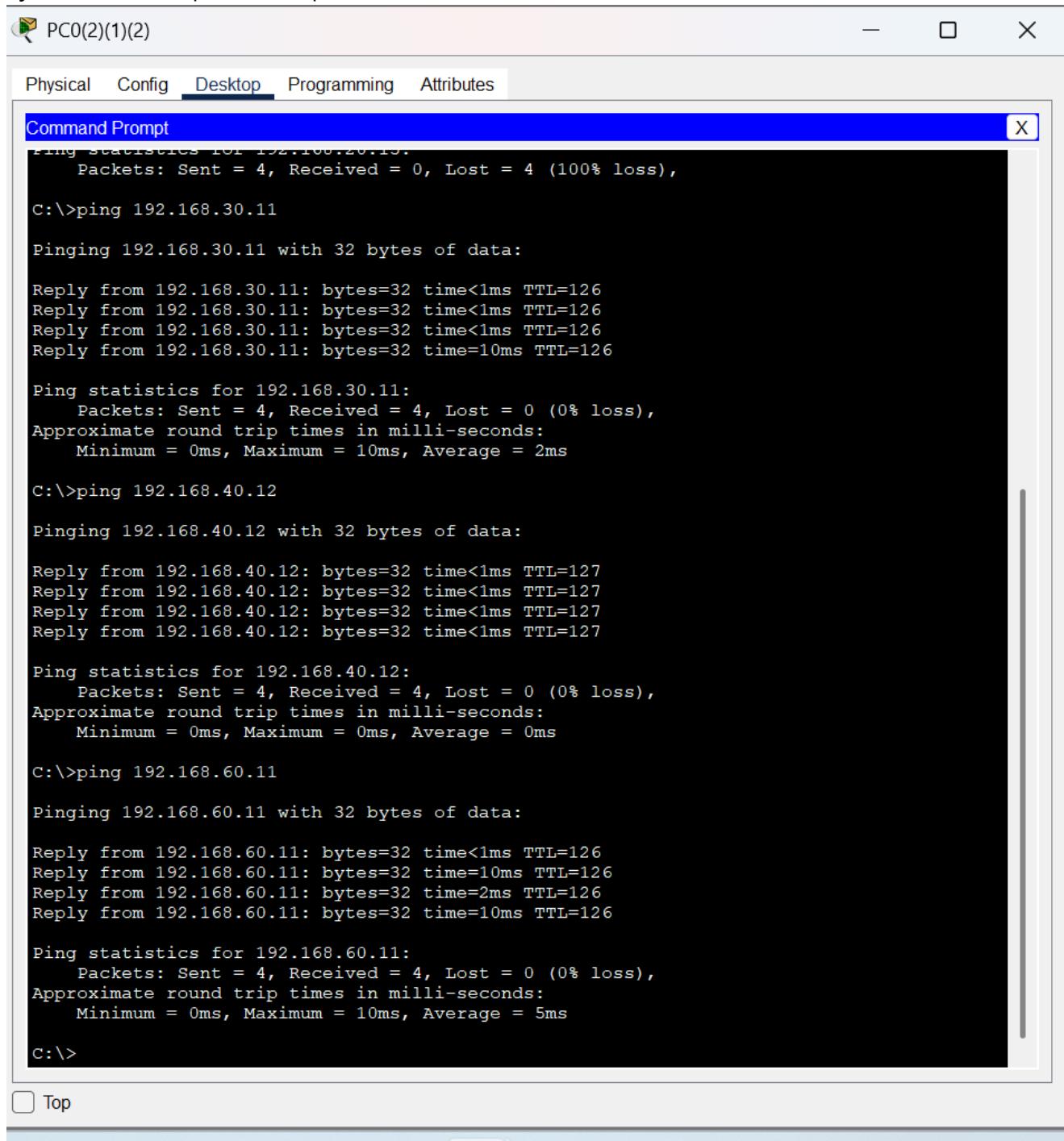
Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:
```

Pada gambar Operasional A terlihat detail konfigurasi jaringan untuk departemen operasional. Struktur jaringan terdiri dari workstation operasional, server monitoring, dan perangkat IoT yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data operasional, dengan implementasi ACL yang mengatur akses ke server monitoring. Tujuan dari konfigurasi ini adalah untuk memastikan departemen operasional memiliki akses yang aman ke sistem monitoring dan kontrol. Hasilnya adalah jaringan operasional yang terlindungi dengan baik untuk operasi monitoring dan kontrol.

## Uji Konektivitas Departemen Operasional B (Detail)



```
PC0(2)(1)(2) Physical Config Desktop Programming Attributes

Command Prompt
ping statistics for 192.168.20.15.
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time<1ms TTL=126
Reply from 192.168.30.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.30.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.40.12

Pinging 192.168.40.12 with 32 bytes of data:

Reply from 192.168.40.12: bytes=32 time<1ms TTL=127

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 192.168.60.11

Pinging 192.168.60.11 with 32 bytes of data:

Reply from 192.168.60.11: bytes=32 time<1ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126
Reply from 192.168.60.11: bytes=32 time=2ms TTL=126
Reply from 192.168.60.11: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.60.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
```

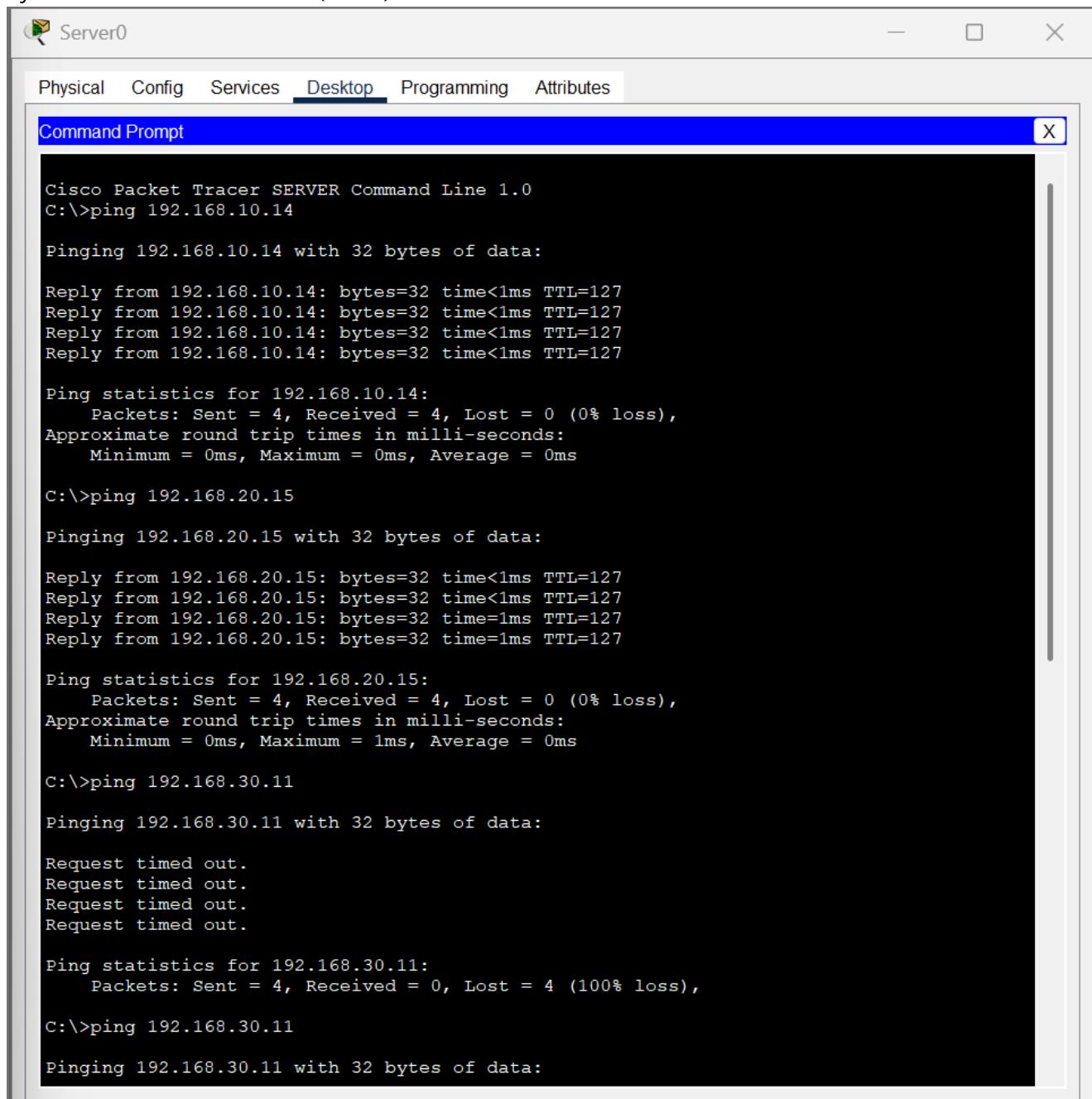
Top



7:04 PM  
5/15/2025

Pada gambar Operasional B terlihat detail konfigurasi jaringan backup untuk departemen operasional. Struktur jaringan terdiri dari workstation backup, server monitoring cadangan, dan perangkat IoT backup yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke server monitoring cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur cadangan yang aman untuk operasi monitoring dan kontrol. Hasilnya adalah sistem backup yang memungkinkan kelanjutan operasi monitoring dan kontrol jika terjadi kegagalan pada sistem utama.

## Uji Konektivitas Server Farm A (Detail)



The screenshot shows a Cisco Packet Tracer Command Line interface with the title bar "Command Prompt". The window contains the following command-line output:

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.14

Pinging 192.168.10.14 with 32 bytes of data:

Reply from 192.168.10.14: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.14:
    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<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 = 1ms, Average = 0ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:
```

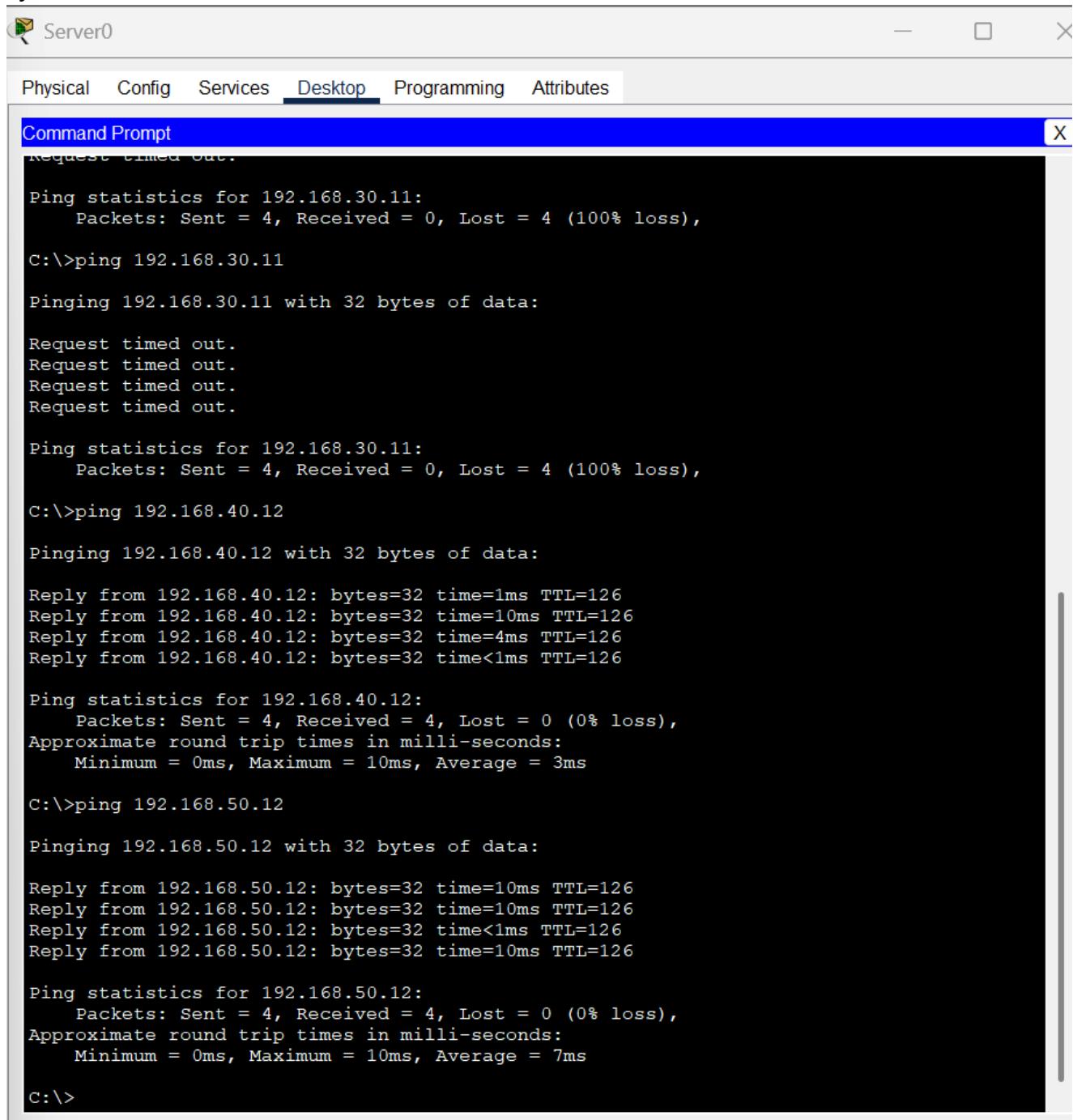
Top



The taskbar icons include File Explorer, OneDrive, Microsoft Edge, Teams, WhatsApp, and File Explorer. The system tray shows the date and time as 6:55 PM on 5/15/2025.

Pada gambar Server A terlihat detail konfigurasi jaringan untuk server farm perusahaan. Struktur jaringan terdiri dari server aplikasi, server database, dan sistem storage yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk mengisolasi lalu lintas data server, dengan implementasi ACL yang mengatur akses ke berbagai server. Tujuan dari konfigurasi ini adalah untuk memastikan server farm memiliki keamanan tinggi dan akses terkontrol. Hasilnya adalah infrastruktur server yang aman dengan segmentasi yang jelas antar layanan.

## Uji Konektivitas Server Farm B (Detail)



```
Physical Config Services Desktop Programming Attributes

Command Prompt
Request timed out.

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

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

Ping statistics for 192.168.30.11:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=126
Reply from 192.168.40.12: bytes=32 time=10ms TTL=126
Reply from 192.168.40.12: bytes=32 time=4ms TTL=126
Reply from 192.168.40.12: bytes=32 time<1ms TTL=126

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 = 10ms, Average = 3ms

C:\>ping 192.168.50.12

Pinging 192.168.50.12 with 32 bytes of data:

Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126
Reply from 192.168.50.12: bytes=32 time<1ms TTL=126
Reply from 192.168.50.12: bytes=32 time=10ms TTL=126

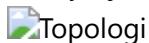
Ping statistics for 192.168.50.12:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 7ms

C:\>
```

Pada gambar Server B terlihat detail konfigurasi jaringan backup untuk server farm perusahaan. Struktur jaringan terdiri dari server aplikasi cadangan, server database cadangan, dan sistem storage cadangan yang terhubung ke switch utama. Kode konfigurasi pada topologi ini menggunakan VLAN tagging untuk redundansi, dengan implementasi ACL yang mengatur akses ke server cadangan. Tujuan dari konfigurasi ini adalah untuk menyediakan infrastruktur server cadangan yang aman dan terisolasi. Hasilnya adalah sistem backup server yang memungkinkan kelanjutan layanan jika terjadi kegagalan pada server utama.

## ⚠ Kendala dan Solusi

1. Kesusahan untuk mengkonfigurasi karena pada topologi sebelumnya ternyata terlalu tricky/sulit alurnya, jadi menyelesaikan kendala ini dengan menghapus router setiap departemen.



2. Kesalahan dalam penentuan Subnetting, sehingga pada saat konfigurasi terjadi invalid.

Memperbaiki kendala ini adalah dengan menyesuaikan pada VLAN yang sudah ditentukan setiap departemennya

Table Subnetting Terbaru

VLAN	Nama	Gedung	Subnet	Gateway IP (Router)
10	IT	Gedung A	192.168.10.0/24	192.168.10.1
20	Keuangan	Gedung A	192.168.20.0/24	192.168.20.1
30	SDM	Gedung A	192.168.30.0/24	192.168.30.1
60	Server	Gedung A	192.168.60.0/24	192.168.60.1
40	Marketing	Gedung B	192.168.40.0/24	192.168.40.1
50	Operasional	Gedung B	192.168.50.0/24	192.168.50.1
99	Native VLAN	Semua	-	-
-	Link Router A-B	Koneksi Antar Router	192.168.100.0/30	Router A: .1, Router B: .2

3. Terjadi kesulitan dalam konfigurasi DHCP di Departemen SDM akibat kesalahan pada pengaturan trunk sebelumnya. Hal ini menyebabkan perangkat tidak mendapat IP secara otomatis. Oleh karena itu, perlu dilakukan perbaikan trunk agar komunikasi dengan DHCP server berjalan lancar.

Switch0(1)(1)(1)(1)

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch
FastEthernet0/5 (30).

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#ex
Switch(config)#interface FastEthernet0/21
Switch(config-if)#switchport mode access
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#ex
Switch(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/21 (99), with Switch
FastEthernet0/5 (30).

Switch con0 is now available

Press RETURN to get started.
```

Top

[Copy](#) [Paste](#)

## IOS Command Line Interface

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/5 (30), with Switch
FastEthernet0/21 (99).

% Incomplete command.
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

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

Switch(config-if)#switchport trunk allowed
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/7 (1), with Switch
FastEthernet0/11 (99).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (10), with Switch
FastEthernet0/21 (1).

% Incomplete command.
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#ex
Switch(config)#interface FastEthernet0/24
Switch(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (10), with Switch
FastEthernet0/21 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (20), with Switch
FastEthernet0/21 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (20), with Switch
FastEthernet0/6 (1).

Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#ex
```

 Top

4. Saat dilakukan pengujian ping ke DNS untuk server internal, pengujian gagal dan perangkat tidak dapat terhubung ke DNS server, yang menunjukkan adanya masalah dalam resolusi nama domain untuk server internal.

RouterA

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Press RETURN to get started.

Router>show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 8.8.8.8

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags     Age Type   Address(es)
Router>ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router>enable
Router#ping google.com
Translating "google.com"...domain server (8.8.8.8)
% Unrecognized host or address or protocol not running.

Router#
```

Top

RouterB

Physical Config **CLI** Attributes

IOS Command Line Interface

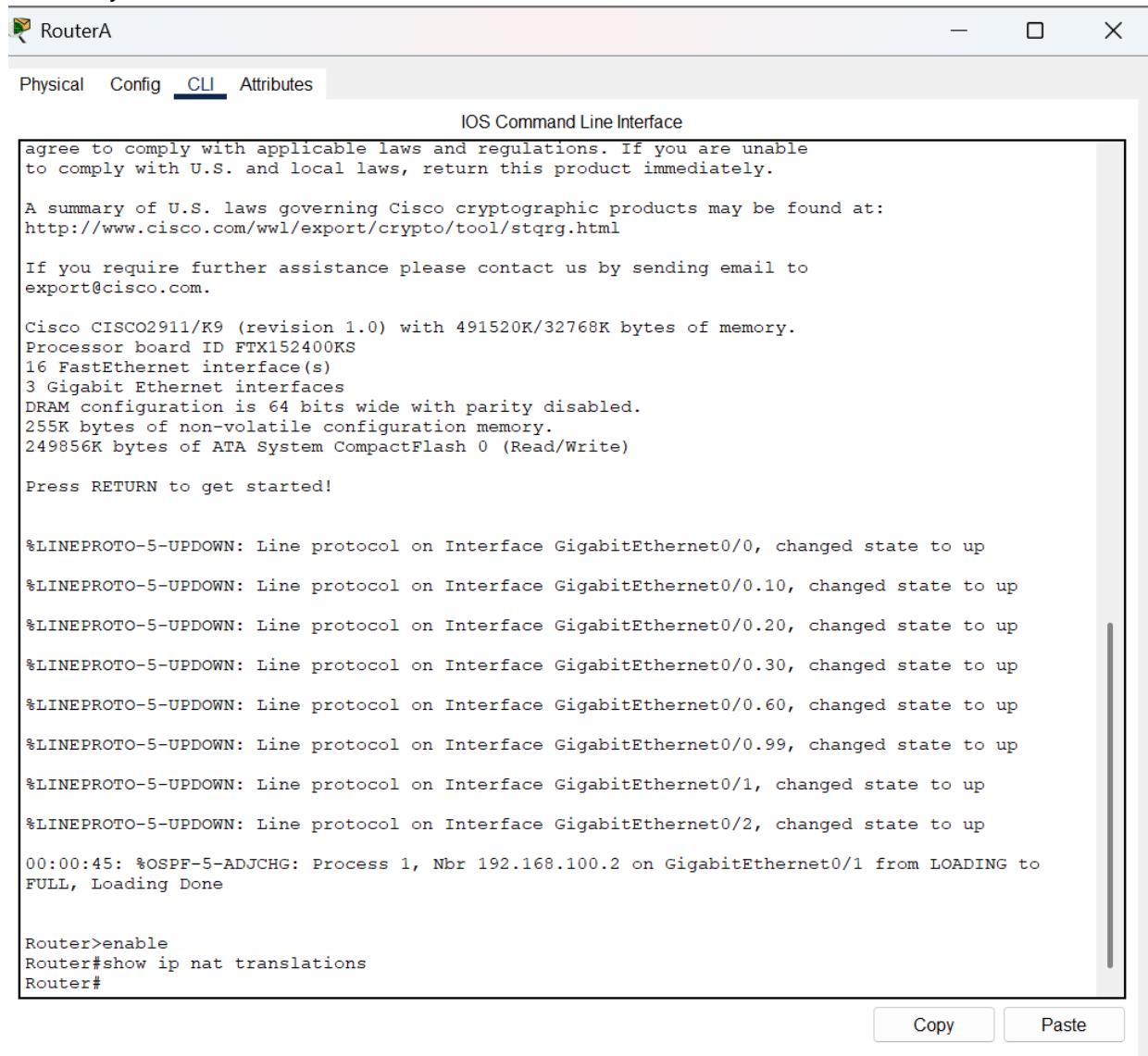
```
Router#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 8.8.8.8

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags     Age Type   Address(es)
Router#ping google.com
Translating "google.com"...domain server (8.8.8.8)
% Unrecognized host or address or protocol not running.
```

5. Perintah show ip nat berhasil dieksekusi, namun hasil yang ditampilkan tidak sesuai dengan yang diharapkan. Tidak ada informasi yang relevan atau hasil yang lengkap mengenai status NAT yang

seharusnya tersedia.



The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a router named 'RouterA'. The 'CLI' tab is selected. The screen displays various system information and logs. At the top, there is a note about legal compliance and product return. Below that, a summary of U.S. laws governing Cisco cryptographic products is provided. The system then lists its hardware configuration, including memory, processor board ID, and interface details. A message encourages pressing RETURN to start. Following this, a series of log entries show the line protocol status changing from down to up for multiple interfaces (GigabitEthernet0/0, 0/0.10, 0/0.20, 0/0.30, 0/0.60, 0/0.99, 0/1, 0/2). A specific log entry at 00:00:45 indicates an OSPF adjacency change from 'LOADING' to 'FULL'. Finally, the user enters 'enable' mode and runs a command to show IP NAT translations. At the bottom right of the window are 'Copy' and 'Paste' buttons.

```
IOS Command Line Interface
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wat/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
16 FastEthernet interface(s)
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 GigabitEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, 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 GigabitEthernet0/0.99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.2 on GigabitEthernet0/1 from LOADING to
FULL, Loading Done

Router>enable
Router#show ip nat translations
Router#
```

Copy      Paste

6. Saat melakukan konfigurasi ACL awal, terjadi kesalahan dalam penempatan ACL pada interface sehingga menyebabkan ACL tidak berfungsi dengan benar. Hal ini membuat aturan yang seharusnya membatasi atau mengatur lalu lintas jaringan tidak berjalan sesuai harapan. Untuk mengatasi masalah tersebut, perlu memastikan bahwa ACL diterapkan pada interface VLAN yang tepat dengan menggunakan perintah `ip access-group [nomor] in`, sehingga aturan ACL dapat bekerja secara efektif sesuai dengan tujuan konfigurasi.

## Kesimpulan

Proyek perancangan jaringan enterprise untuk PT. Nusantara Network berhasil mencapai tujuan utama dalam membangun infrastruktur jaringan yang efisien, aman, dan mendukung kebutuhan operasional perusahaan. Hasil yang dicapai meliputi:

### 1. Desain dan Implementasi Jaringan

Topologi jaringan hierarkis berhasil dirancang dengan segmentasi VLAN untuk masing-masing departemen (IT, Keuangan, SDM, Marketing, Operasional, dan Server Farm) di dua lokasi (Gedung A dan Gedung B). Konfigurasi VLAN, trunking, dan routing dinamis menggunakan OSPF memastikan koneksi antar-departemen dan antar-gedung berjalan lancar.

## 2. Layanan Jaringan

Implementasi DHCP memungkinkan alokasi IP otomatis yang sukses untuk semua perangkat, sementara NAT memfasilitasi akses internet menggunakan satu IP publik. DNS internal mendukung resolusi nama domain lokal, meskipun terdapat kendala dalam pengujian DNS server internal.

## 3. Keamanan Jaringan

Access Control List (ACL) diterapkan untuk mengatur akses antar-departemen sesuai kebijakan, seperti membatasi akses Departemen Marketing dan Operasional ke Keuangan, serta mengamankan Server Farm. Pengujian ACL menunjukkan aturan keamanan berfungsi dengan baik setelah perbaikan konfigurasi.

## 4. Pengujian dan Konektivitas

Pengujian menyeluruh, termasuk ping antar-router dan uji DHCP, menunjukkan koneksi jaringan stabil. Sistem backup untuk setiap departemen dan Server Farm berhasil dikonfigurasi untuk mendukung redundansi dan failover.

## 5. Pemecahan Masalah

Kendala seperti Native VLAN mismatch, kesalahan subnetting, dan konfigurasi ACL yang salah berhasil diatasi melalui penyesuaian trunk, revisi skema pengalaman IP, dan penerapan ACL pada interface yang tepat.

Pembelajaran yang Didapatkan:

1. Proyek ini meningkatkan pemahaman tentang konfigurasi perangkat jaringan (switch, router), implementasi VLAN, routing dinamis (OSPF), serta layanan DHCP, DNS, dan NAT. Penggunaan Cisco Packet Tracer memberikan pengalaman praktis dalam simulasi jaringan.
2. Mengatasi kendala seperti kesalahan konfigurasi trunk dan ACL mengasah kemampuan analisis dan troubleshooting, menekankan pentingnya ketelitian dalam konfigurasi jaringan.
3. Pendekatan Project Based Learning (PBL) melatih kerja tim, pembagian tugas, dan komunikasi efektif antar anggota kelompok dengan peran berbeda (Network Architect, Engineer, Services Specialist, dan Security Specialist).
4. Penyusunan dokumentasi teknis yang rapi dan presentasi hasil proyek meningkatkan kemampuan komunikasi teknis dan profesionalisme dalam menyampaikan solusi jaringan.
5. Proyek ini menunjukkan pentingnya segmentasi jaringan dan kebijakan keamanan untuk melindungi data sensitif, serta desain jaringan yang skalabel untuk mendukung pertumbuhan organisasi.

Secara keseluruhan, proyek ini tidak hanya menghasilkan rancangan jaringan yang fungsional dan aman untuk PT. Nusantara Network, tetapi juga memberikan pembelajaran berharga tentang desain, implementasi, dan pengelolaan jaringan enterprise yang dapat diterapkan dalam konteks nyata.

## Video Demo/Tutorial

[Link Video Demo](#)

## Slide Presentasi

[Link Drive Presentasi](#)