

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

### **Anggota Kelompok dan Peran**

- Meiske Handayani (10231052) - Network Architect
- Muhammad Ariel Rayhan (10231058) - Network Engineer
- Nilam Ayu Nandastari Romdoni (10231070) - Network service Specialist
- Ranaya Chintya Mahitsa (10231078) - Security & Documentation Specialist

### **Daftar Isi**

#### **1. Pendahuluan**

##### **1.1 Latar Belakang**

##### **1.2 Tujuan**

##### **1.3 Ruang Lingkup**

#### **2. Isi Laporan**

##### **2.1 Perencanaan Proyek & Desain Awal (Minggu 9)**

Pembentukan Kelompok dan Pembagian Peran  
Analisis Kebutuhan PT. Nusantara Network  
Segmentasi Jaringan (VLAN)  
Koneksi Antar Gedung (WAN)  
Akses Internet (NAT)  
Alokasi IP (DHCP)  
Resolusi Nama (DNS)  
Kontrol Akses (ACL)  
Routing Dinamis (OSPF)  
Monitoring & Manajemen Terpusat  
Brainstorming Desain Jaringan Awal

##### **2.2 Desain Topologi & Skema Pengalamatan (Minggu 10)**

Finansial Desain Topologi Jaringan  
Detail Topologi untuk Gedung A dan Gedung B  
Perencanaan Skema Pengalamatan IP (Subnetting)  
Penentuan Perangkat yang Dibutuhkan

##### **2.3 Implementasi Topologi Dasar & VLAN (Minggu 11)**

Pembangunan Topologi Dasar di Cisco Packet Tracer/GNS3  
Konfigurasi VLAN dan Trunking  
Konfigurasi Router Gedung A, Gedung B, dan Router Utama  
Implementasi Routing Antar-VLAN

##### **2.4 Implementasi Routing & WAN (Minggu 12)**

Konfigurasi Routing Statis pada Jaringan Intra-Gedung  
Implementasi Routing Dinamis (OSPF) untuk Koneksi Antar-Gedung  
Simulasi Koneksi WAN Antar Gedung

##### **2.5 Implementasi Layanan Jaringan (Minggu 13)**

Konfigurasi DHCP Server untuk Setiap Departemen

- Konfigurasi IP Helper-Address
- Pengujian Alokasi IP Dinamis
- Implementasi DNS Server untuk Resolusi Nama Internal
- Konfigurasi NAT untuk Akses Internet

## **2.6 Implementasi Keamanan & Pengujian (Minggu 14)**

- Implementasi Access Control List (ACL) Sesuai Kebijakan Keamanan
- Pengujian Menyeluruh Semua Fitur Jaringan
- Matriks Pengujian Fitur ACL
- Troubleshooting dan Perbaikan Masalah

## **3. Kendala dan Solusi**

- Dokumentasi Masalah yang Dihadapi
- Langkah-Langkah Penyelesaian

## **4. Kesimpulan**

## **1. Pendahuluan**

### **1.1 Latar Belakang**

PT. Nusantara Network merupakan sebuah perusahaan yang bergerak di bidang teknologi informasi, dengan fokus utama pada penyediaan solusi digital dan layanan teknologi untuk mendukung transformasi digital di berbagai sektor industri. Kantor pusat perusahaan ini terletak di Gedung A, yang menjadi pusat koordinasi dan pengelolaan berbagai aktivitas strategis dan operasional. Selain itu, perusahaan juga memiliki kantor cabang yang berlokasi di Gedung B, yang berfungsi sebagai perluasan operasional untuk mendukung kebutuhan bisnis yang terus berkembang.

Di kantor pusat, terdapat empat departemen utama yang masing-masing memiliki fungsi krusial dalam menunjang keberlangsungan operasional perusahaan. Departemen Teknologi Informasi (IT) menjadi tulang punggung dalam pengelolaan sistem dan jaringan internal, dilengkapi dengan 40 unit komputer yang digunakan oleh tim teknis untuk pengembangan perangkat lunak, pemeliharaan infrastruktur, serta dukungan teknis harian. Departemen Keuangan memiliki 25 unit komputer yang digunakan untuk aktivitas akuntansi, perencanaan anggaran, dan laporan keuangan, sehingga membutuhkan tingkat keamanan data yang sangat tinggi. Sementara itu, Departemen Sumber Daya Manusia (SDM) yang terdiri dari 20 komputer bertanggung jawab dalam pengelolaan data karyawan, perekrutan, pelatihan, serta pengembangan organisasi. Tidak kalah penting, Server Farm yang terdapat di kantor pusat mencakup 10 unit server yang berfungsi untuk menangani berbagai layanan penting seperti penyimpanan data, pengelolaan basis data, layanan email, serta sistem internal perusahaan lainnya.

Sementara itu, kantor cabang yang terletak di Gedung B terdiri dari dua departemen utama, yaitu Departemen Marketing dengan 30 komputer yang digunakan untuk kegiatan promosi, riset pasar, dan pengelolaan kampanye digital, serta Departemen Operasional yang memiliki 35 komputer untuk menunjang aktivitas logistik, distribusi, dan dukungan layanan pelanggan. Dengan total keseluruhan 160 perangkat yang tersebar di dua lokasi fisik, perusahaan menghadapi tantangan dalam membangun dan mengelola infrastruktur jaringan yang tidak hanya andal dan efisien, tetapi juga aman dan mudah dikendalikan dari pusat.

Tantangan utama yang dihadapi PT. Nusantara Network mencakup kompleksitas arsitektur jaringan yang timbul akibat adanya pemisahan geografis antara kantor pusat dan cabang, yang memerlukan koneksi yang stabil dan aman. Selain itu, perlindungan data menjadi prioritas utama, khususnya pada Departemen Keuangan dan Server Farm, yang menyimpan informasi sensitif dan bersifat strategis. Oleh karena itu, dibutuhkan sistem keamanan jaringan yang canggih seperti firewall, VPN, dan sistem deteksi intrusi (IDS). Di samping itu, kebutuhan akan sistem manajemen jaringan yang terpusat dan bersifat scalable menjadi sangat penting, agar perusahaan dapat dengan mudah

memantau, mengelola, dan memperluas infrastruktur teknologi seiring dengan pertumbuhan bisnis dan peningkatan volume data di masa mendatang.

## **1.2 Tujuan**

Proyek ini bertujuan untuk merancang dan mengimplementasikan infrastruktur jaringan terpadu yang andal, aman, dan berkinerja tinggi guna mendukung operasional PT. Nusantara Network secara optimal. Tujuan utama meliputi:

### **1.2.1 Membangun Jaringan yang Stabil dan Aman**

- Segmentasi Jaringan : Menerapkan VLAN untuk mengisolasi traffic antar-departemen (IT, Keuangan, SDM, Marketing, Operasional) guna mencegah gangguan silang dan meningkatkan keamanan data, terutama untuk informasi sensitif di Departemen Keuangan dan Server Farm.
- Proteksi Data : Mengimplementasikan enkripsi end-to-end melalui VPN untuk komunikasi antar-gedung (Gedung A dan B) serta mengamankan akses remote dengan autentikasi multifaktor.
- Lapisan Keamanan Berlapis : Memasang firewall next-generation (NGFW) dengan fitur Unified Threat Management (UTM) dan sistem IDS/IPS untuk memantau serta memblokir serangan siber secara real-time.

### **1.2.2 Meningkatkan Efisiensi Operasional**

- Manajemen Terpusat : Mengadopsi solusi Software-Defined Networking (SDN) atau platform manajemen berbasis cloud (seperti Cisco DNA Center atau Aruba Central) untuk memudahkan konfigurasi, monitoring, dan troubleshooting jaringan secara terpusat dari kantor pusat.
- Optimalisasi Kinerja : Menerapkan load balancing pada Server Farm untuk mendistribusikan beban traffic secara merata, memastikan ketersediaan layanan kritikal (seperti database, ERP, dan aplikasi internal) tanpa downtime.
- Quality of Service (QoS) : Memprioritaskan traffic penting (VoIP, video conference, dan akses server) untuk menjaga produktivitas karyawan.

### **1.2.3 Mendukung Skalabilitas Jangka Panjang**

- Infrastruktur dirancang untuk mendukung pertumbuhan perusahaan, seperti penambahan cabang, perangkat IoT, atau ekspansi cloud dengan fleksibilitas dalam penambahan node jaringan dan bandwidth.

Dengan pencapaian tujuan-tujuan di atas, PT. Nusantara Network akan memiliki infrastruktur jaringan yang tidak hanya memenuhi kebutuhan saat ini tetapi juga siap menghadapi tantangan digital di masa depan.

### 1.3 Ruang Lingkup

Ruang lingkup proyek perancangan dan implementasi infrastruktur jaringan PT. Nusantara Network mencakup seluruh aspek teknis dan operasional yang diperlukan untuk membangun sistem jaringan yang andal, aman, efisien, dan scalable. Lingkup ini terbagi menjadi beberapa bagian utama yang menjelaskan batasan dan cakupan kerja sebagai berikut:

#### 1.3.1 Cakupan Wilayah Implementasi

- **Kantor Pusat (Gedung A)** : Mencakup jaringan untuk Departemen IT, Keuangan, SDM, serta Server Farm dengan total 95 perangkat.
- **Kantor Cabang (Gedung B)** : Meliputi jaringan untuk Departemen Marketing dan Operasional dengan total 65 perangkat.
- **Koneksi Antar-Gedung** : Pengadaan dan konfigurasi koneksi dedicated (fiber optic) serta failover berbasis 4G/LTE atau microwave antara Gedung A dan Gedung B.

#### 1.3.2 Desain dan Topologi Jaringan

- **Topologi Jaringan** : Perancangan arsitektur jaringan dengan pendekatan hierarki tiga lapis (Core, Distribution, Access Layer) di kantor pusat.
- **Segmentasi VLAN** : Penerapan Virtual LAN untuk pemisahan trafik antar departemen guna meningkatkan keamanan dan efisiensi.
- **High Availability (HA)** : Konfigurasi protokol seperti HSRP/VRRP untuk menjaga ketersediaan layanan.

#### 1.3.3. Keamanan Jaringan

- **Perlindungan Data** : Implementasi enkripsi end-to-end melalui VPN untuk komunikasi antar-gedung dan autentikasi multifaktor untuk akses remote.
- **Kontrol Akses** : Pembatasan akses berbasis peran (role-based access control) di lingkungan jaringan internal.

#### 1.3.4. Manajemen dan Monitoring Terpusat

- **Manajemen Jaringan** : Penggunaan solusi berbasis cloud seperti Cisco DNA Center atau Aruba Central untuk konfigurasi, pemantauan, dan troubleshooting jaringan secara terpusat.
- **Monitoring Trafik dan Log Aktivitas** : Integrasi tools pemantauan real-time serta pencatatan log aktivitas jaringan untuk audit dan deteksi dini terhadap anomali.

### 1.3.5. Optimisasi dan Kinerja

- **Load Balancing:** Penerapan mekanisme distribusi beban trafik pada Server Farm untuk memastikan ketersediaan layanan penting tanpa downtime.
- **Quality of Service (QoS):** Konfigurasi prioritas trafik untuk aplikasi penting seperti VoIP, video conference, dan akses ke server internal.

### 1.3.6. Redundansi dan Failover

- **Koneksi Redundan :** Penyediaan jalur internet cadangan dan konfigurasi failover otomatis untuk menjaga kontinuitas layanan.
- **Perangkat Redundan :** Penggunaan perangkat jaringan cadangan (redundant switches, routers, dan firewall) untuk menghindari single point of failure.

### 1.3.8. Batasan Proyek

- Tidak mencakup integrasi aplikasi bisnis spesifik (ERP, CRM, dsb.), kecuali dalam konteks akses jaringan.
- Implementasi hanya berlaku pada dua lokasi fisik perusahaan (Gedung A dan B).
- Tidak termasuk pelatihan SDM kecuali dalam bentuk dokumentasi dan sesi handover teknis.

## 2. Isi Laporan

### 2.1 Perencanaan Proyek & Desain Awal - (Minggu 9)

#### A. Pembentukan kelompok dan pembagian peran

Meiske Handayani (10231052) - Network Architect, yang bertanggung jawab merancang arsitektur jaringan secara menyeluruh.

Muhammad Ariel Rayhan (10231058) - Network Engineer, yang akan mengimplementasikan dan mengkonfigurasi perangkat jaringan.

Nilam Ayu Nandastari Romdoni (10231070) - Network service Specialist, bertugas mengelola layanan jaringan dan optimasi kinerja.

Ranaya Chintya Mahitsa (10231078) - Security & Documentation Specialist, yang fokus pada keamanan jaringan dan penyusunan dokumentasi proyek.

#### B. Analisis kebutuhan PT. Nusantara Network.

### **1. Segmentasi Jaringan (VLAN)**

Kebutuhan : Setiap departemen harus berada di VLAN terpisah.

Tujuan :

- Isolasi antar departemen untuk mencegah akses tidak sah.
- Pengelolaan trafik jaringan yang lebih baik.

### **2. Koneksi Antar Gedung (WAN)**

Kebutuhan : Koneksi antara Gedung A (kantor pusat) dan Gedung B (kantor cabang) melalui teknologi WAN dengan bandwidth terbatas.

Tujuan :

- Menghubungkan jaringan antar lokasi.
- Pengaturan bandwidth efisien karena keterbatasan koneksi.

### **3. Akses Internet (NAT)**

Kebutuhan : Implementasi NAT (Network Address Translation).

Tujuan :

- Mengizinkan perangkat internal mengakses internet menggunakan IP publik yang terbatas.
- Menjaga keamanan jaringan internal.

### **4. Alokasi IP (DHCP)**

Kebutuhan : DHCP Server untuk setiap departemen.

Tujuan :

- Otomatisasi pemberian IP address.
- Mengurangi konfigurasi manual.

### **5. Resolusi Nama (DNS)**

Kebutuhan : Layanan DNS internal dan eksternal.

Tujuan :

- Memudahkan komunikasi antar perangkat dengan nama.
- Mendukung layanan internal dan akses ke internet.

### **6. Kontrol Akses (ACL)**

Kebutuhan : Access Control List.

Tujuan :

- Membatasi akses antar VLAN/departemen sesuai kebijakan.
- Menambah lapisan keamanan jaringan.

### **7. Routing Dinamis (OSPF)**

Kebutuhan : Routing OSPF antar gedung.

Tujuan :

- Otomatisasi pengelolaan rute antar jaringan.
- Adaptif terhadap perubahan topologi jaringan.

## **8. Monitoring & Manajemen Terpusat**

Kebutuhan : Sistem monitoring dan manajemen jaringan.

Tujuan :

- Deteksi dini masalah jaringan.
- Sentralisasi kontrol untuk efisiensi pengelolaan

### **C. Brainstorming desain jaringan awal.**

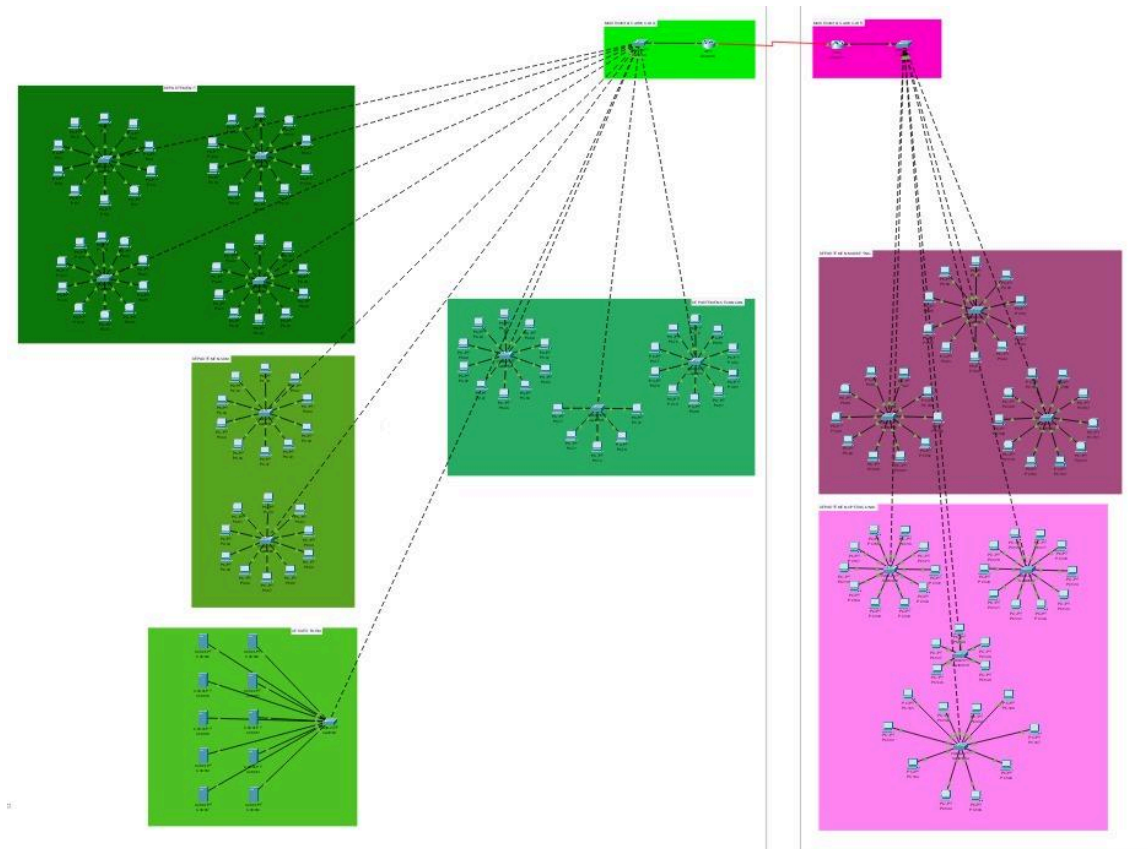
- Terdapat komponen Internet yang berfungsi sebagai gateway utama bagi seluruh perangkat di jaringan internal
- Komponen Router Utama berfungsi untuk pengelolaan traffic antar VLAN dan koneksi ke gedung cabang (WAN). Juga menjalankan OSPF sebagai routing dinamis.
- Komponen Layer 3 Switch yang nantinya akan ada di masing-masing departemen yang dipisah menggunakan VLAN. pada Gedung A (VLAN 10, departemen IT, 40 komputer. VLAN 20 Departemen Keuangan, 25 Komputer. VLAN 30, Departemen SDM, 20 Komputer)
- Pada Gedung B (VLAN 40 pada departemen Marketing dengan jumlah 30 komputer dan VLAN 50 pada departemen Operasional dengan 35 komputer)

## **2.2 Desain Topologi & Skema Pengalamatan - (Minggu 10)**

### **A. Finansial desain topologi jaringan**

Berikut merupakan finansial desain topologi jaringan yang telah kami rancang :





Pada gambar tersebut merupakan desain topologi jaringan untuk dua gedung, yaitu Gedung A (Kantor Pusat) dan Gedung B (Kantor Cabang). Dengan detail topologi sebagai berikut :

- Kantor Pusat Gedung A
  - Departemen IT
    - 40 Pc
    - 4 Switch
  - Departemen Keuangan
    - 25 Pc
    - 3 Switch
  - Departemen SDM
    - 20 Pc
    - 2 Switch
  - Server Farm yang berisikan 10 server untuk berbagai layanan dan 1 switch.
- Kantor Cabang Gedung B
  - Departemen Marketing

- 30 Pc
- 3 Switch

→ Departemen Operasional

- 35 Pc
- 4 Switch

## B. Perencanaan skema pengalamatan IP (subnetting)

Berikut adalah tabel perencanaan yang telah kami buat untuk skema pengalamatan IP (subnetting) :

Tabel Pengalamatan IP (subnet, VLAN ID, gateway, range, dsb):

Subnet	VLAN ID	Nama	Gateway	Range	Jumlah Host	Deskripsi
192.168.10.0/24	10	IT_DEPT	192.168.10.1	192.168.10.2 – 192.168.10.254	40	Departemen IT (Gedung A)
192.168.20.0/24	20	KEU_DEPT	192.168.20.1	192.168.20.2 – 192.168.20.254	25	Departemen Keuangan (Gedung A)
192.168.30.0/24	30	SDM_DEPT	192.168.30.1	192.168.30.2 – 192.168.30.254	20	Departemen SDM (Gedung A)
192.168.40.0/24	40	SERVER_FARM	192.168.40.1	192.168.40.2 – 192.168.40.254	10	Server Farm (Gedung A)
192.168.50.0/24	50	MKT_DEPT	192.168.50.1	192.168.50.2 – 192.168.50.254	30	Departemen Marketing (Gedung B)
192.168.60.0/24	60	OPS_DEPT	192.168.60.1	192.168.60.2 – 192.168.60.254	35	Departemen Operasional (Gedung B)
172.16.0.0/30	-	WAN_LINK	-	172.16.0.1 - 172.16.0.2	2	Koneksi WAN antar gedung
203.0.113.0/30	-	ISP_LINK	-	203.0.113.1 - 203.0.113.2	2	Koneksi ke ISP
192.168.1.0/24	1	MANAGEMENT	192.168.1.1	192.168.1.2 - 192.168.1.254	254	Management perangkat jaringan.

Daftar perangkat yang dibutuhkan (router, switch, server, dsb). Daftar Perangkat yang dibutuhkan dalam komponen ini adalah sebagai berikut :

### A. Gedung A

#### 1. Departemen IT

- 40 Pc
- 4 Switch
- Kabel Cross Over

#### 2. Departemen SDM

- 20 Pc
- 2 Switch
- Kabel Cross Over

#### 3. Departemen Keuangan

- 25 Pc
  - 3 Switch
  - Kabel Cross Over
4. Server Farm
    - 10 Server
    - 1 Switch
    - Kabel Straight Through
  5. 1 Main Router dan 1 Main Switch di Gedung A

#### B. Gedung B

1. Departemen Marketing
  - 30 Pc
  - 3 Switch
  - Kabel Cross Over
2. Departemen Operasional
  - 35 Pc
  - 4 Switch
  - Kabel Cross Over
  - 1 Main Router dan 1 Main Switch di Gedung B

Untuk kedua gedung memiliki 1 router utama yang menjadi ibu dari kedua main router di masing-masing gedung.

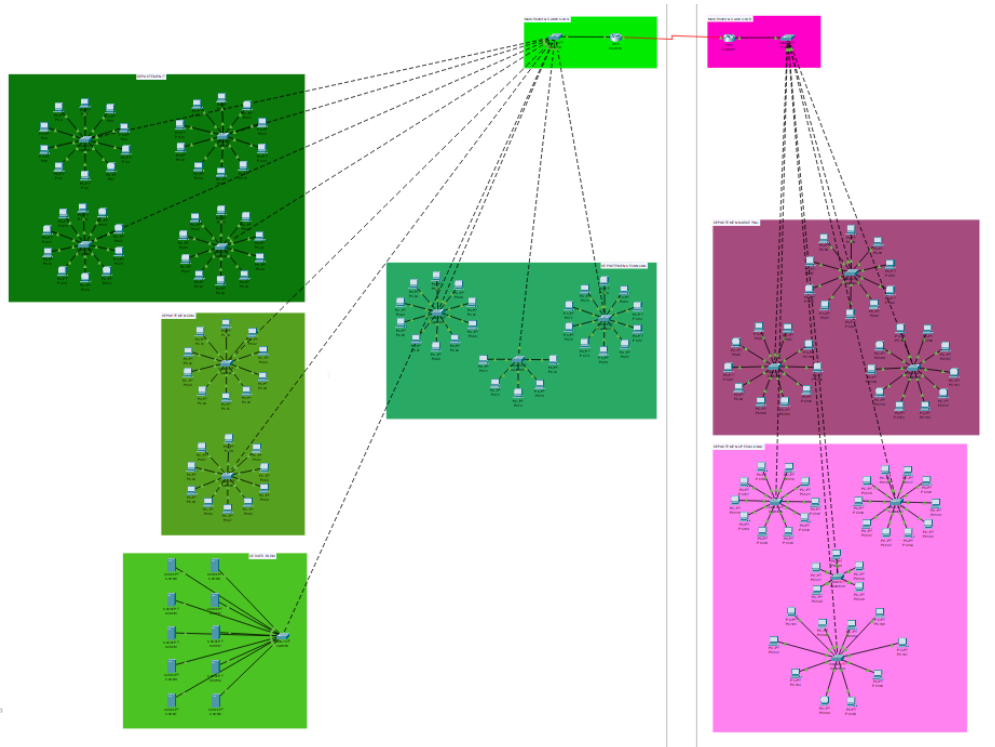
#### C. Penentuan Perangkat yang dibutuhkan

Rencana Penerapan VLAN :

VLAN ID	Nama	Subnet	Tujuan
1	MANAGEMENT	192.168.1.0/24	Manajemen dan administrasi perangkat jaringan
10	IT_DEPT	192.168.10.0/24	Segmentasi untuk Departemen IT dengan akses ke semua departemen dan server farm
20	KEU_DEPT	192.168.20.0/24	Segmentasi untuk Departemen Keuangan dengan akses terbatas ke server farm
30	SDM_DEPT	192.168.30.0/24	Segmentasi untuk Departemen SDM dengan akses ke semua departemen untuk koordinasi
40	SERVER_FARM	192.168.40.0/24	Segmentasi untuk Server Farm dengan keamanan tinggi untuk layanan perusahaan
50	MKT_DEPT	192.168.50.0/24	Segmentasi untuk Departemen Marketing dengan akses terbatas ke server farm
60	OPS_DEPT	192.168.60.0/24	Segmentasi untuk Departemen Operasional dengan akses terbatas ke server farm
99	NATIVE	-	VLAN native untuk trunk links (tidak digunakan untuk endpoint)

## 2.3 Implementasi Topologi Dasar & VLAN - (Minggu 11)

A. Pembangunan topologi dasar di Cisco Packet Tracer/GNS3.



## → Gedung A (Kantor Pusat)

Diagram sebelah kiri menggambarkan jaringan di **kantor pusat**, yang terdiri dari beberapa VLAN untuk tiap departemen:

### 1. Departemen IT

- Terdapat **4 kelompok subnet**, masing-masing terdiri dari 10 komputer.
- Semua terhubung ke **switch masing-masing**, yang kemudian terhubung ke switch utama departemen.
- Kemungkinan menggunakan VLAN untuk segmentasi trafik.

### 2. Departemen Keuangan

- Terdiri dari 3 kelompok subnet dengan masing-masing 8 komputer.
- Fokus pada **keamanan dan isolasi data** terlihat dari struktur yang tidak digabung dengan departemen lain.

### 3. Departemen SDM

- Menyediakan jaringan untuk sekitar 20 komputer.
- Struktur topologinya serupa, menggunakan switch untuk koneksi antar perangkat.

### 4. Server Farm

- Menampilkan koneksi langsung dari **server-server utama** ke switch core jaringan yang berfungsi untuk penyimpanan data, email, ERP, database, dll.

### 5. Switch Core Gedung A

- **Titik pusat distribusi VLAN** dari seluruh departemen.
- Tersambung ke gedung B melalui **koneksi garis merah (kemungkinan fiber optic dedicated line)**.

## → Gedung B (Kantor Cabang)

Diagram kanan menggambarkan struktur jaringan di **kantor cabang**:

### 1. Departemen Marketing

- Terdiri dari beberapa kelompok subnet (sekitar 30 komputer).
- Menggunakan switch masing-masing dan koneksi konsisten ke switch utama cabang.

### 2. Departemen Operasional

- Serupa dengan Marketing: terbagi menjadi beberapa kelompok PC yang terhubung ke switch, kemudian ke switch utama.

### 3. Switch Core Gedung B

- Menjadi pusat koneksi dari semua departemen di Gedung B.
- Terhubung ke switch utama di Gedung A melalui jalur merah dan jalur VPN (putus-putus hitam).

#### → Koneksi Antar Gedung

- **Garis Merah** menghubungkan core switch Gedung A ke core switch Gedung B — ini adalah **koneksi utama**, kemungkinan **dedicated fiber optic**.
- **Garis Putus-Putus Hitam** adalah jalur **redundan atau backup (VPN, LTE, atau microwave)**.
- Jalur ini juga menghubungkan VLAN antar departemen dari Gedung A ke B.

### B. Konfigurasi VLAN dan trunking

#### → Switch Gedung A

...

```
Switch>enable
Switch configure terminal
Switch (config)#vlan 10
Switch (config-vlan) name IT DEPT
Switch (config-vlan) #vlan 20
Switch (config-vlan)# name KEU DEPT
Switch(config-vlan)#vlan 30
```

```

Switch(config-vlan) name SDM DEPT
Switch (config-vlan)#vlan 40
Switch(config-vlan)# name SERVER FARM
Switch (config-vlan)#vlan 99
Switch (config-vlan)# name MANAGEMENT
Switch (config-vlan)#interface range fa0/110
Switch(config-if-range) #switchport mode access
Switch (config-if-range) #switchport access vlan 10
Switch (config-if-range) #interface range fa0/11-15
Switch (config-if-range) #switchport mode access
Switch (config-if-range) #switchport access vlan 20
Switch (config-if-range) #interface range fa0/16 20
Switch (config-if-range) #switchport mode access
Switch(config-if-range) #switchport access vlan 30
Switch (config-if-range) #interface range fa0/21 22
Switch (config-if-range) #switchport mode access
Switch (config-if-range)#switchport access vlan 40
Switch (config-if-range) #interface gi0/1
Switch (config-if)#switchport mode trunk Switch (config-if)#switchport trunk native vlan 99
...

```

Konfigurasi ini bertujuan untuk membuat beberapa VLAN (Virtual LAN) di sebuah switch dan mengalokasikan port tertentu ke masing-masing VLAN. VLAN 10, 20, 30, 40, dan 99 masing-masing dinamai sesuai dengan departemen seperti IT, Keuangan, SDM, Server Farm, dan Manajemen. Port FastEthernet (fa0/1, fa0/11-15, fa0/16 dan fa0/20, fa0/21-22) dikonfigurasi sebagai access port dan ditugaskan ke VLAN yang sesuai. Terakhir, port GigabitEthernet gi0/1 dikonfigurasi sebagai trunk port untuk mentransmisikan beberapa VLAN antar switch, dengan VLAN 99 diset sebagai native VLAN, yaitu VLAN default untuk lalu lintas yang tidak diberi tag.

#### → Router Gedung A

...

```

Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet0/0.10
Router (config-subif)#encapsulation dot10 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router (config-subif)#interface gigabitEthernet0/0.20
Router(config-subif)#encapsulation dot10 20
Router (config-subif)#ip address 192.168.20.1 255.255.255.0
Router (config-subif)#interface gigabitEthernet0/0.30
Router(config-subif)#encapsulation dot10 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#interface gigabitEthernet0/0.40
Router(config-subif)#encapsulation dot10 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0

```

```

Router(config-subif)#interface gigabitEthernet0/0.99
Router(config-subif)#encapsulation dot10 99
Router(config-subif)#ip address 192.168.1.2 255.255.255.0
Router(config-subif)#interface gigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#interface gigabitEthernet0/1
Router (config-if)#ip address 172.16.0.1 255.255.255.252
Router(config-if)#no shutdown
LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up
LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up
...

```

Kodingan tersebut merupakan konfigurasi sub-interface pada router Cisco untuk implementasi Inter-VLAN Routing menggunakan Router-on-a-Stick, di mana satu interface fisik (GigabitEthernet0/0) dibagi menjadi beberapa sub-interface (0/0.10, 0/0.20, dst.) masing-masing untuk VLAN yang berbeda menggunakan perintah encapsulation dot1Q. Setiap sub-interface diberi alamat IP sesuai dengan subnet VLAN-nya untuk menghubungkan antar VLAN, sementara interface GigabitEthernet0/1 dikonfigurasi dengan IP point-to-point. Perintah no shutdown di akhir memastikan semua interface aktif.

#### → **Router Gedung B**

...

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet0/0.50 Router(config-subif)#encapsulation dot10 50
Router (config-subif)#ip address 192.168.50.1 255.255.255.0
Router(config-subif)#interface gigabitEthernet0/0.60
Router (config-subif)#encapsulation dot10 60
Router(config-subif)#ip address 192.168.60.1 255.255.255.0
Router(config-subif)#interface gigabitEthernet0/0.99
Router (config-subif)#ip address 192.168.1.3 255.255.255.0
Router (config-subif)#encapsulation dot10 99
Router (config-subif)#interface gigabitEthernet0/0
Router (config-if)#no shutdown
Router (config-if)#interface gigabitEthernet0/1
Router (config-if)#ip address 172.16.0.2 255.255.255.252
Router (config-if)#no shutdown
LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
BLINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

```



LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

SLINK-5-CHANGED: Interface GigabitEthernet0/0.60, changed state to up

SLINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed state to up

SLINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up

SLINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.99, changed state to up

...

Konfigurasi ini digunakan untuk mengatur subinterface pada router Cisco dengan metode Inter-VLAN Routing menggunakan router-on-a-stick. Subinterface GigabitEthernet0/0 dibagi menjadi tiga VLAN: VLAN 50 (192.168.50.1), VLAN 60 (192.168.60.1), dan VLAN 99 (192.168.1.3) dengan masing-masing perintah encapsulation dot1Q untuk menetapkan ID VLAN. Interface utama GigabitEthernet0/0 dan GigabitEthernet0/1 diaktifkan menggunakan no shutdown, serta interface GigabitEthernet0/1 dikonfigurasi dengan IP 172.16.0.2/30 sebagai jalur antar-router. Pesan status menunjukkan bahwa semua interface berhasil aktif dan berfungsi.

#### → **Router Utama**

...

Router>enable

Router configure terminal

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

Router (config)#interface gigabitEthernet0/0

Router (config-if)#ip address 172.16.0.10 255.255.255.252

Router (config-if)#no shutdown

Router(config-if)#interface gigabitEthernet0/1

Router(config-if)#ip address 172.16.0.11 255.255.255.252

Bad mask /30 for address 172.16.0.11

Router(config-if)#no shutdown

LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#

LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Router (config-if)#ip route 192.168.10.0 255.255.255.0 172.16.0.1

Router (config)#ip route 192.168.20.0 255.255.255.0 172.16.0.1

Router (config)#ip route 192.168.30.0 255.255.255.0 172.16.0.1

Router (config)#ip route 192.168.40.0 255.255.255.0 172.16.0.1

Router (config)#

Router (config)#ip route 192.168.50.0 255.255.255.0 172.16.0.2

Router (config)#ip route 192.168.60.0 255.255.255.0 172.16.0.2

Router (config)#

...

Konfigurasi di atas merupakan pengaturan dasar pada router Cisco yang meliputi pemberian alamat IP pada dua antarmuka (GigabitEthernet0/0 dan 0/1) dengan subnet mask /30 (255.255.255.252), meskipun terjadi kesalahan saat mengatur IP pada interface 0/1. Setelah itu, kedua interface diaktifkan dengan perintah `no shutdown`, dan status koneksi berubah menjadi aktif (up). Selanjutnya, router dikonfigurasi dengan beberapa static route untuk mengarahkan lalu lintas ke jaringan 192.168.x.x melalui gateway 172.16.0.1 dan 172.16.0.2, memungkinkan komunikasi antar jaringan melalui jalur yang telah ditentukan secara manual.

### C. Implementasi routing antar-VLAN.

...

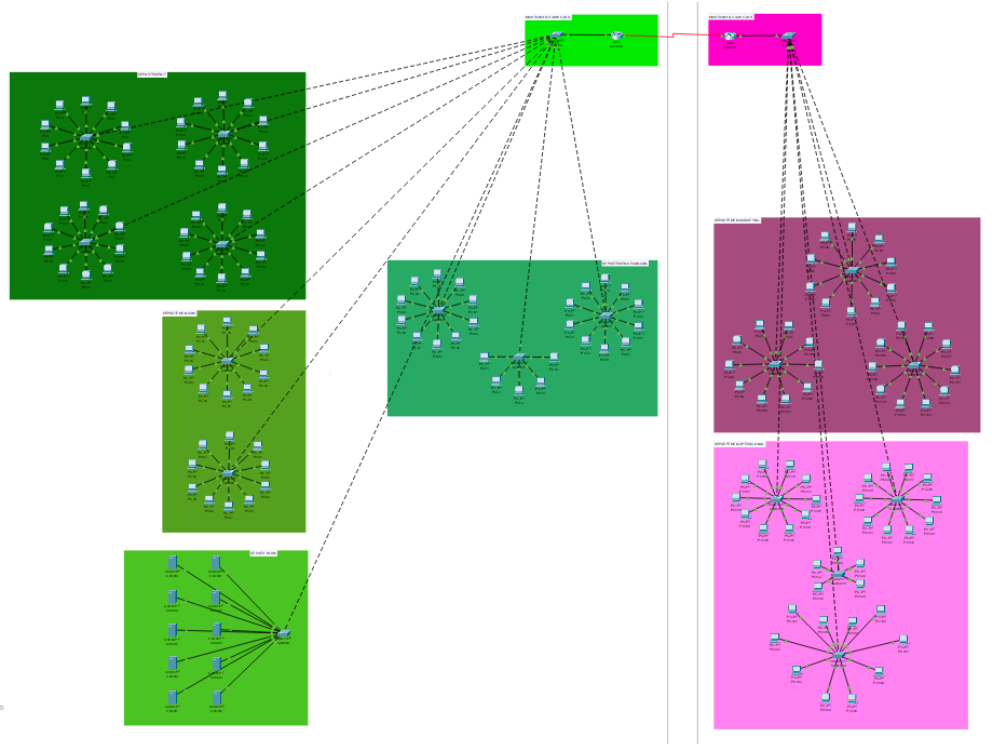
```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 50
Switch (config-vlan)# name MKT DEPT
Switch (config-vlan)#vlan 60
Switch (config-vlan)# name OPS DEPT
Switch (config-vlan)#vlan 99
Switch(config-vlan)# name MANAGEMENT name
Switch (config-vlan)#interface range fa0/1 15
Switch(config-if-range) #switchport mode access
Switch (config-if-range) #switchport access vlan 50
Switch (config-if-range) finterface range fa0/16 30
interface range not validated command rejected
Switch (config)#switchport mode access
Invalid input detected at marker.
Switch (config)#switchport access vlan 60
Invalid input detected at marker.
Switch (config)#interface gi0/1
Switch (config-if)#switchport mode trunk
Switch (config-if)#switchport trunk native vlan 95
```

...

Kode konfigurasi tersebut digunakan untuk mengatur VLAN pada sebuah switch Cisco. Pertama, mode konfigurasi diaktifkan, kemudian dibuat tiga VLAN: VLAN 50 dengan nama "MKT DEPT", VLAN 60 dengan nama "OPS DEPT", dan VLAN 99 dengan nama "MANAGEMENT". Selanjutnya, interface FastEthernet dari fa0/1 hingga fa0/15 dikonfigurasi sebagai access mode dan ditetapkan ke VLAN 50. Terdapat kesalahan saat mencoba mengonfigurasi fa0/16 hingga fa0/30 karena penulisan perintah yang salah. Kesalahan lain juga muncul saat mencoba mengatur mode access dan VLAN di luar konteks interface. Terakhir, interface GigabitEthernet 0/1 dikonfigurasi sebagai trunk dan diatur VLAN native-nya ke VLAN 95.

## 2.4 Implementasi Routing & WAN - (Minggu 12)

### A. Konfigurasi routing statis pada jaringan intra-gedung.



Routing statis adalah metode mengatur rute jaringan secara manual oleh administrator jaringan, di mana jalur antar jaringan (subnet) sudah ditentukan dan tidak berubah-ubah kecuali diedit secara manual. Jika diterapkan dalam jaringan intra-gedung (jaringan lokal di dalam satu gedung), maka konfigurasi routing statis bertujuan untuk mengatur komunikasi antar VLAN, subnet, atau departemen tanpa menggunakan protokol routing dinamis seperti OSPF atau RIP.

### Router Gedung A

```
Router(config-if)#
Router(config-if)#! Routing OSPF
Router(config-if)#router ospf 1
Router(config-router)# router-id 1.1.1.1
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
Router(config-router)# network 192.168.40.0 0.0.0.255 area 0
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 172.16.0.0 0.0.0.3 area 0
Router(config-router)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

00:02:12: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet0/0.99 from LOADING to FULL, Loading Done

Router(config-router)#
Router#
%SYS-5-CONFIG I: Configured from console by console
```

```bash

Router (config-if)#

Router (config-if)#! Routing OSPF

```
Router (config-if)#router ospf 1
Router (config-router)# router-id 1.1.1.1
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
Router (config-router)# network 192.168.40.0 0.0.0.255 area 0
Router (config-router)# network 192.168.1.0 0.0.0.255 area 0
Router (config-router)# network 172.16.0.0 0.0.0.3 area 0
Router (config-router)#
LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

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

```
00:02:12: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet0/0.99 from
LOADING to FULL, Loading Done
Router (config-router)#
Router#
%SYS-5-CONFIG I: Configured from console by console
'''
```

Router ini dikonfigurasi dengan OSPF proses ID 1. Router ID diset ke 1.1.1.1. Router mengiklankan beberapa network ke area OSPF 0:

```
192.168.10.0/24
192.168.20.0/24
192.168.30.0/24
192.168.40.0/24
192.168.1.0/24
172.16.0.0/30
```

Terlihat bahwa interface GigabitEthernet0/1 telah aktif (state to up). Router ini berhasil membentuk OSPF adjacency dengan router lain yang memiliki Router ID 2.2.2.2 pada interface GigabitEthernet0/0.

## 1. Fundamental Konfigurasi OSPF

Router ini menggunakan OSPF dengan parameter inti:

- Process ID: 1 (nilai lokal, tidak perlu match dengan router lain)
- Router ID: 1.1.1.1 (harus unik dalam domain OSPF)
- Area 0: Backbone area wajib untuk semua router OSPF

## 2. Network Advertisement (Penyebaran Jaringan)

Perintah network mengontrol:

Interface mana yang berpartisipasi dalam OSPF

Network mana yang diiklankan ke router lain

etail Network yang Diiklankan:

Network, Wildcard Mask, Keterangan :

192.168.10.0 0.0.0.255 Subnet /24 (Gedung A LAN)

192.168.20.0 0.0.0.255 Subnet /24 (Gedung A LAN)

172.16.0.0 0.0.0.3 Link /30 (ke Router Utama)

Mekanisme Wildcard Mask:

- 0.0.0.255 = 24 bit pertama harus match (subnet /24)

- 0.0.0.3 = 30 bit pertama match (subnet /30)

Router Gedung B

```
Router(config-if)#
Router(config-if)#! Routing OSPF
Router(config-if)#router ospf 1
Router(config-router)# router-id 2.2.2.2
Router(config-router)# network 192.168.50.0 0.0.0.255 area 0
Router(config-router)# network 192.168.60.0 0.0.0.255 area 0
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 172.16.0.4 0.0.0.3 area 0
Router(config-router)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

00:02:12: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet0/0.99 from LOADING to FULL,
Loading Done

Router#
%SYS-5-CONFIG_I: Configured from console by console
```

```bash

Router (config-if)#

Router (config-if)#! Routing OSPF

Router (config-if)#router ospf 1

Router (config-router)# router-id 2.2.2.2

Router(config-router)# network 192.168.50.0 0.0.0.255 area 0

Router (config-router)# network 192.168.60.0 0.0.0.255 area 0

Router (config-router)# network 192.168.1.0 0.0.0.255 area 0

Router (config-router)# network 172.16.0.4 0.0.0.3 area 0

Router (config-router)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

00:02:12: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet0/0.99 from LOADING to FULL,

Loading Done

Router#

%SYS-5-CONFIG I: Configured from console by console

```

Router ini juga menggunakan OSPF dengan proses ID 1. Router ID diset ke 2.2.2.2.  
Mengiklankan network:

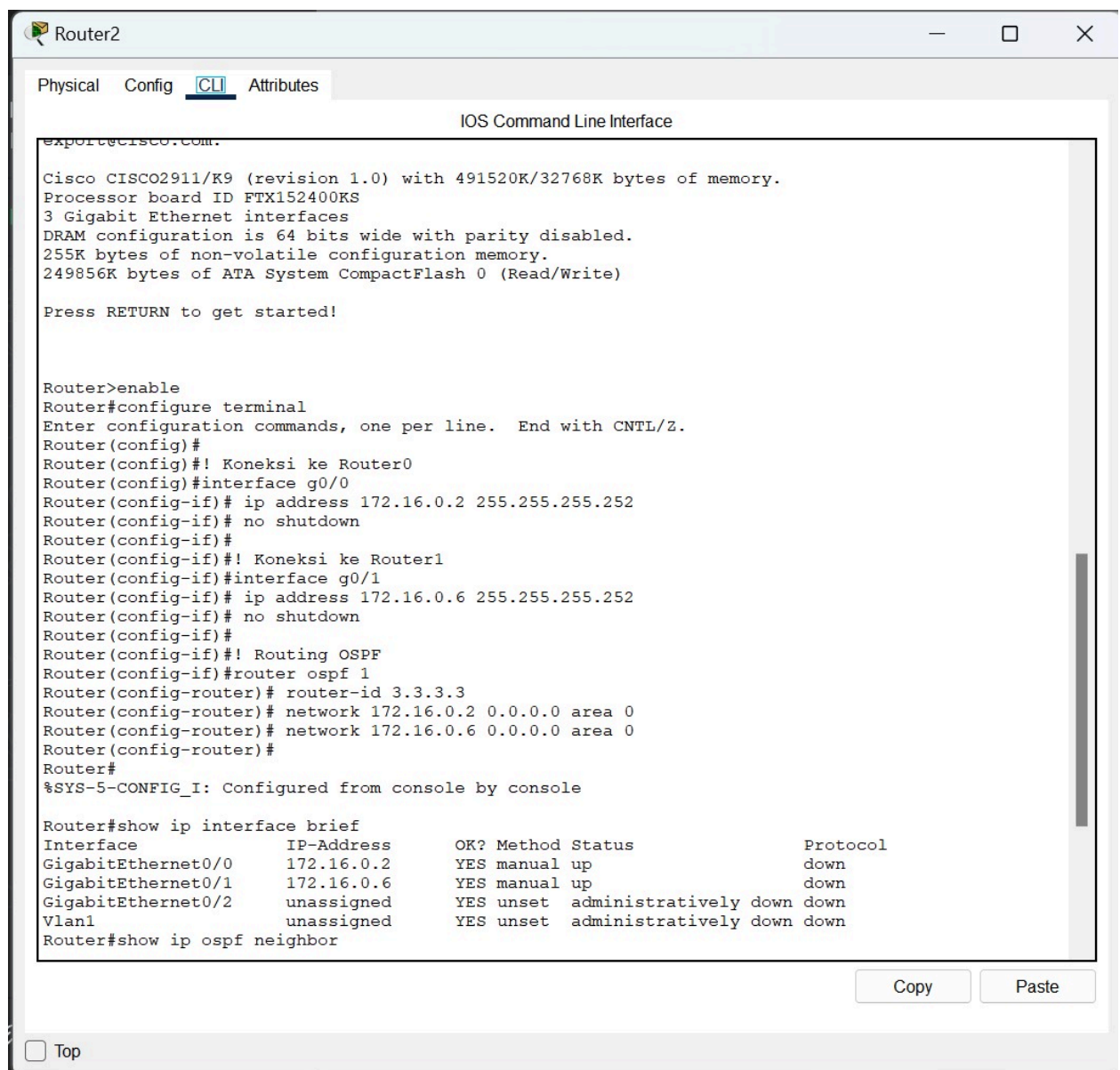
192.168.50.0/24

192.168.60.0/24

192.168.1.0/24

172.16.0.4/30

Sama seperti router sebelumnya, interface GigabitEthernet0/1 diaktifkan. Router ini juga berhasil membentuk adjacency OSPF dengan router 1.1.1.1. Router ini merupakan router tetangga dari RouterGedA, dan mereka saling bertukar informasi OSPF.



```
Router2
Physical Config CLI Attributes
IOS Command Line Interface
export@cisco.com:

Cisco CISC02911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#! Koneksi ke Router0
Router(config)#interface g0/0
Router(config-if)# ip address 172.16.0.2 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)#
Router(config-if)#! Koneksi ke Router1
Router(config-if)#interface g0/1
Router(config-if)# ip address 172.16.0.6 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)#
Router(config-if)#! Routing OSPF
Router(config-if)#router ospf 1
Router(config-router)# router-id 3.3.3.3
Router(config-router)# network 172.16.0.2 0.0.0.0 area 0
Router(config-router)# network 172.16.0.6 0.0.0.0 area 0
Router(config-router)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       172.16.0.2      YES manual  up          down
GigabitEthernet0/1       172.16.0.6      YES manual  up          down
GigabitEthernet0/2       unassigned      YES unset   administratively down down
Vlan1                    unassigned      YES unset   administratively down down
Router#show ip ospf neighbor
```

☐ Top

Copy Paste

```bash

Router>enable

Router#configure terminal

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

```
Router (config)#  
Router (config)#! Koneksi ke Router0  
Router (config)#interface g0/0  
Router(config-if)# ip address 172.16.0.2 255.255.255.252  
Router(config-if)# no shutdown  
Router (config-if)#  
Router(config-if)#! Koneksi ke Router1  
Router (config-if)#interface g0/1  
Router (config-if)# ip address 172.16.0.6 255.255.255.252  
Router (config-if)# no shutdown  
Router(config-if)#  
Router(config-if)#! Routing OSPF  
Router (config-if)#router ospf 1  
Router(config-router) router-id 3.3.3.3  
Router (config-router)# network 172.16.0.2 0.0.0.0 area 0  
Router(config-router)# network 172.16.0.6 0.0.0.0 area 0  
Router(config-router)#  
Router#
```

SYS-5-CONFIG\_I: Configured from console by console

```
Router#show ip interface brief  
Interface  
GigabitEthernet0/0  
GigabitEthernet0/1  
GigabitEthernet0/2  
IP-Address  
OK? Method Status  
Protocol  
172.16.0.2  
YES manual up  
down  
172.16.0.6  
YES manual up  
down  
unassigned  
YES unset  
administratively down down  
Vlan1  
unassigned  
YES unset administratively down down  
Router#show ip ospf neighbor  
...
```

Ini merupakan router utama yang terhubung ke dua router lainnya (Router0 dan Router1) melalui:

GigabitEthernet0/0 ke 172.16.0.2/30

GigabitEthernet0/1 ke 172.16.0.6/30

Router ID diset ke 3.3.3.3.

Network OSPF yang dikonfigurasi:

172.16.0.2/30

172.16.0.6/30

Perintah show ip interface brief menunjukkan bahwa interface sudah UP, tapi: Protokol down, yang artinya belum ada konektivitas OSPF pada layer 3. Perintah show ip ospf neighbor tidak menunjukkan neighbor, artinya belum ada tetangga OSPF terbentuk. Router ini belum berhasil membentuk hubungan OSPF dengan router-router lain. Masalah kemungkinan ada pada kabel, IP address, atau OSPF belum berjalan di router tetangga.

Routing statis adalah metode routing yang dikonfigurasi secara manual oleh administrator jaringan, cocok untuk jaringan kecil yang topologinya tidak sering berubah karena lebih aman, ringan, dan tidak menggunakan bandwidth tambahan. Sebaliknya, routing dinamis seperti OSPF dan EIGRP lebih cocok untuk jaringan besar dan kompleks karena dapat menyesuaikan secara otomatis terhadap perubahan topologi, mempercepat proses failover, serta mengurangi beban konfigurasi manual. Meskipun routing dinamis membutuhkan lebih banyak sumber daya CPU dan bandwidth untuk bertukar informasi antar-router, fleksibilitas dan skalabilitasnya menjadikannya pilihan utama di lingkungan jaringan yang dinamis dan terus berkembang.

Hasil dari simulasi yang dilakukan diatas adalah :

- OSPF berhasil diimplementasikan antara Router Gedung A dan B, tetapi gagal di Router Utama karena kesalahan konfigurasi network statement.
- Routing static bisa digunakan sebagai fallback jika OSPF gagal, tetapi kurang skalabel

## **2.5 Implementasi Layanan Jaringan - (Minggu 13)**

### **A. Konfigurasi DHCP Server untuk setiap departemen.**

#### **1. Konfigurasi DHCP Server pada Router Utama**

Konfigurasi DHCP server pada router yang bertujuan untuk memberikan alamat IP secara otomatis kepada perangkat di berbagai VLAN. VLAN 10 (IT - Gedung A) menggunakan subnet 192.168.10.0/24 dengan default gateway dan DNS server di 192.168.10.1, VLAN 20 (Finance - Gedung A) menggunakan 192.168.20.0/24 dengan gateway 192.168.20.1, VLAN 30 (HR - Gedung A) menggunakan 192.168.30.0/24 dengan gateway 192.168.30.1, VLAN 50 (Marketing - Gedung B) menggunakan 192.168.50.0/24 dengan gateway



192.168.50.1, dan VLAN 60 (Operations - Gedung A) menggunakan 192.168.60.0/24 dengan gateway 192.168.60.1.

**DHCP Pool untuk VLAN 10 (IT - Gedung A)**

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool IT_DEPARTEMENT
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 192.168.10.1
Router(dhcp-config)#exit
```

**DHCP Pool untuk VLAN 20 (FINANCE - Gedung A)**

```
Router(config)#ip dhcp pool FINANCE_DEPARTMENT
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 192.168.20.1
Router(dhcp-config)#exit
```

**DHCP Pool untuk VLAN 30 (HR - Gedung A)**

```
Router(config)#ip dhcp pool HR_DEPARTMENT
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#dns-server 192.168.30.1
Router(dhcp-config)#exit
```

**DHCP Pool untuk VLAN 50 (MARKETING - Gedung B)**

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool MARKETING_DEPARTMENT
Router(dhcp-config)#network 192.168.50.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.50.1
Router(dhcp-config)#dns-server 192.168.50.1
Router(dhcp-config)#exit
```

**DHCP Pool untuk VLAN 60 (OPERATIONS - Gedung A)**

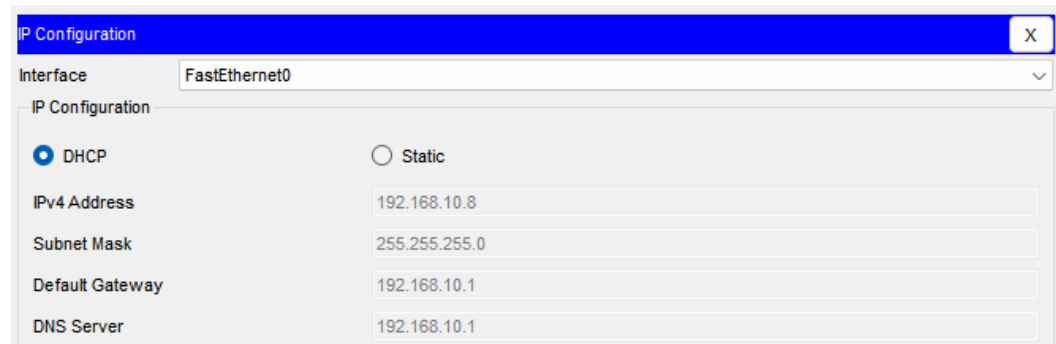
```
Router(config)#ip dhcp pool OPERATIONS_DEPARTMENT
Router(dhcp-config)#network 192.168.60.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.60.1
Router(dhcp-config)#dns-server 192.168.60.1
Router(dhcp-config)#exit
```

2. Pengujian Alokasi IP Dinamis

Setelah konfigurasi, lakukan pengujian dengan mengubah konfigurasi IP pada PC klien di setiap VLAN menjadi DHCP. Dilakukan dengan :

- Membuka PC di VLAN
- Masuk ke IP Configuration, pilih DHCP.
- Verifikasi IP address, subnet mask, default gateway, dan DNS server yang diterima. harus sesuai dengan pool.

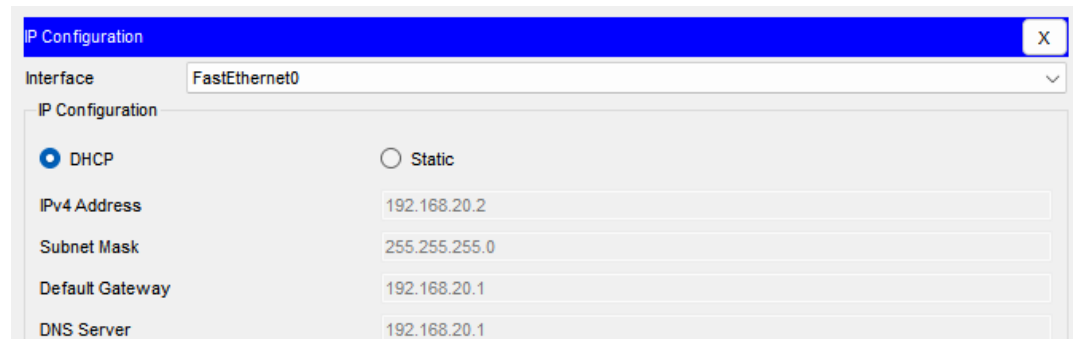
### Pengujian Client di VLAN 10



| IP Configuration                      |                              |
|---------------------------------------|------------------------------|
| Interface                             | FastEthernet0                |
| IP Configuration                      |                              |
| <input checked="" type="radio"/> DHCP | <input type="radio"/> Static |
| IPv4 Address                          | 192.168.10.8                 |
| Subnet Mask                           | 255.255.255.0                |
| Default Gateway                       | 192.168.10.1                 |
| DNS Server                            | 192.168.10.1                 |

Pada gambar tersebut menunjukkan PC12 di Departemen IT (VLAN 10) Gedung A berhasil mendapatkan konfigurasi IP secara otomatis dari DHCP Server di Router Utama. Alamat IP yang diterima adalah 192.168.10.8, Subnet Mask 255.255.255.0, Default Gateway 192.168.10.1, dan DNS Server 192.168.10.1 dan telah sesuai dengan konfigurasi DHCP Pool IT\_DEPARTEMENT.

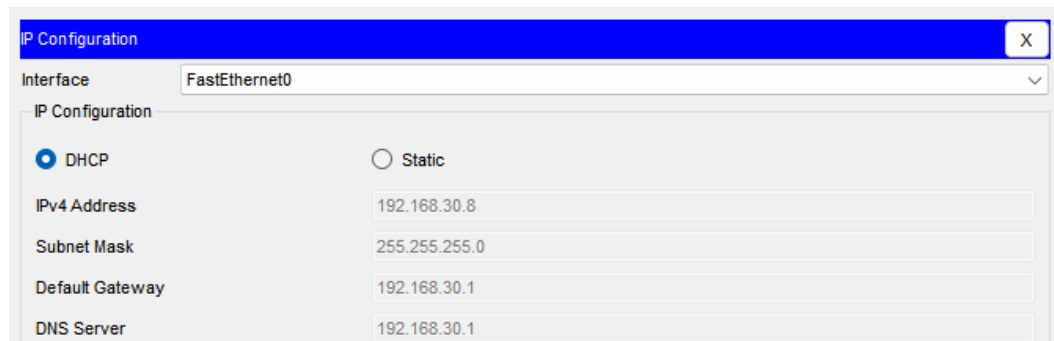
### Pengujian Client di VLAN 20



| IP Configuration                      |                              |
|---------------------------------------|------------------------------|
| Interface                             | FastEthernet0                |
| IP Configuration                      |                              |
| <input checked="" type="radio"/> DHCP | <input type="radio"/> Static |
| IPv4 Address                          | 192.168.20.2                 |
| Subnet Mask                           | 255.255.255.0                |
| Default Gateway                       | 192.168.20.1                 |
| DNS Server                            | 192.168.20.1                 |

Pada gambar tersebut menunjukkan PC64 di Departemen FINANCE (VLAN 20) Gedung A berhasil mendapatkan konfigurasi IP secara otomatis dari DHCP Server di Router Utama. Alamat IP yang diterima adalah 192.168.20.2, Subnet Mask 255.255.255.0, Default Gateway 192.168.20.1, dan DNS Server 192.168.20.1 dan telah sesuai dengan konfigurasi DHCP Pool FINANCE\_DEPARTEMENT.

### Pengujian Client di VLAN 30

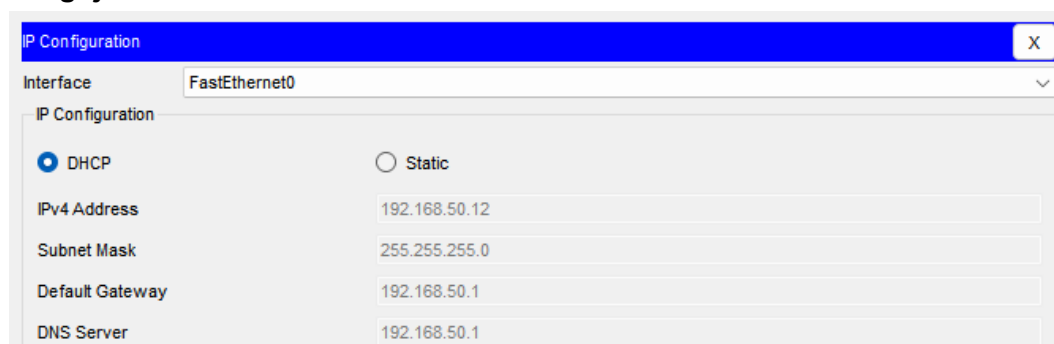


The screenshot shows the 'IP Configuration' window for the 'FastEthernet0' interface. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IP Address, Subnet Mask, Default Gateway, and DNS Server are populated with the following values:

| Field           | Value         |
|-----------------|---------------|
| IPv4 Address    | 192.168.30.8  |
| Subnet Mask     | 255.255.255.0 |
| Default Gateway | 192.168.30.1  |
| DNS Server      | 192.168.30.1  |

Pada gambar tersebut menunjukkan PC39 di Departemen HR (VLAN 30) Gedung A berhasil mendapatkan konfigurasi IP secara otomatis dari DHCP Server di Router Utama. Alamat IP yang diterima adalah 192.168.30.8, Subnet Mask 255.255.255.0, Default Gateway 192.168.30.1, dan DNS Server 192.168.30.1 dan telah sesuai dengan konfigurasi DHCP Pool HR\_DEPARTEMENT.

### Pengujian Client di VLAN 50

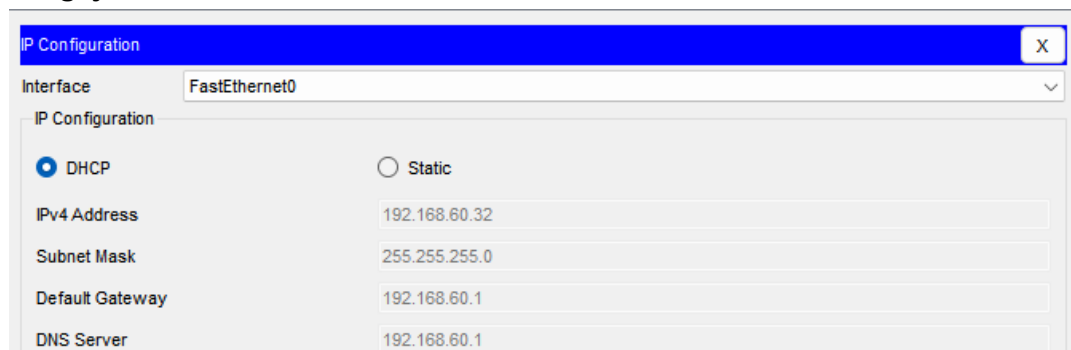


The screenshot shows the 'IP Configuration' window for the 'FastEthernet0' interface. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IP Address, Subnet Mask, Default Gateway, and DNS Server are populated with the following values:

| Field           | Value         |
|-----------------|---------------|
| IPv4 Address    | 192.168.50.12 |
| Subnet Mask     | 255.255.255.0 |
| Default Gateway | 192.168.50.1  |
| DNS Server      | 192.168.50.1  |

Pada gambar tersebut menunjukkan PC86 di Departemen MARKETING (VLAN 50) Gedung B berhasil mendapatkan konfigurasi IP secara otomatis dari DHCP Server di Router Utama. Alamat IP yang diterima adalah 192.168.50.12, Subnet Mask 255.255.255.0, Default Gateway 192.168.50.1, dan DNS Server 192.168.50.1 dan telah sesuai dengan konfigurasi DHCP Pool HR\_DEPARTEMENT.

## Pengujian Client di VLAN 60

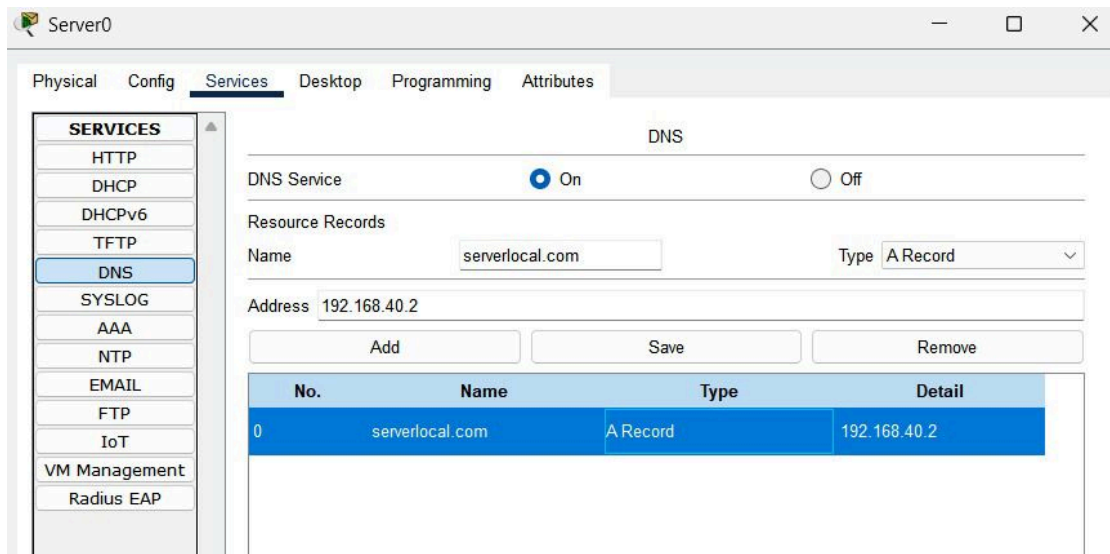


The screenshot shows the 'IP Configuration' window for the 'FastEthernet0' interface. The 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IP Address, Subnet Mask, Default Gateway, and DNS Server are all populated with the following values:

| Field           | Value         |
|-----------------|---------------|
| IPv4 Address    | 192.168.60.32 |
| Subnet Mask     | 255.255.255.0 |
| Default Gateway | 192.168.60.1  |
| DNS Server      | 192.168.60.1  |

Pada gambar tersebut menunjukkan PC115 di Departemen OPERASIONS (VLAN 60) Gedung B berhasil mendapatkan konfigurasi IP secara otomatis dari DHCP Server di Router Utama. Alamat IP yang diterima adalah 192.168.60.32, Subnet Mask 255.255.255.0, Default Gateway 192.168.60.1, dan DNS Server 192.168.60.1 dan telah sesuai dengan konfigurasi DHCP Pool OPERASIONS\_DEPARTEMENT.

### B. Implementasi DNS Server untuk resolusi nama internal.



The screenshot shows the 'Server0' configuration window with the 'Services' tab selected. The 'DNS' service is enabled (On). The 'Resource Records' section shows an 'A Record' for the domain 'serverlocal.com' with the IP address '192.168.40.2'. The table below summarizes the DNS record:

| No. | Name            | Type     | Detail       |
|-----|-----------------|----------|--------------|
| 0   | serverlocal.com | A Record | 192.168.40.2 |

Gambar tersebut menggambarkan konfigurasi layanan DNS (Domain Name System) yang aktif pada sebuah server di aplikasi simulasi jaringan seperti Cisco Packet Tracer. Layanan DNS yang diaktifkan memungkinkan server untuk menerima permintaan dari klien dan menerjemahkan nama domain ke alamat IP. Konfigurasi mencakup entri A Record dengan nama domain *serverlocal.com* yang mengarah ke alamat IP *192.168.40.2*. Dengan adanya entri ini, klien dalam jaringan yang menggunakan server DNS ini dapat mengakses server dengan mengetikkan nama domain *serverlocal.com*, yang mempermudah akses tanpa perlu mengingat alamat IP. Tabel menunjukkan bahwa satu DNS record telah tersimpan, menghubungkan nama domain tersebut ke IP yang relevan.

### C. Konfigurasi NAT untuk akses internet.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 192.168.40.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface gig0/1 overload
Router(config)#exit
Router#
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 192.168.40.0 0.0.0.255
Router(config)#ip nat inside source list i interface gig0/1 overload
Router(config)#exit
Router#
```

```
Router#
Router#show ip nat tr
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 8.8.8.7:50         192.168.40.1:50   192.168.1.2:50     192.168.1.2:50
icmp 8.8.8.7:51         192.168.40.1:51   192.168.1.2:51     192.168.1.2:51
icmp 8.8.8.7:52         192.168.40.1:52   192.168.1.2:52     192.168.1.2:52
icmp 8.8.8.7:53         192.168.40.1:53   192.168.1.2:53     192.168.1.2:53
Router#
```

---

```
Router#
Router#show ip nat tr
Router#show ip nat translations
```

| Pro  | Inside global | Inside Local    | Outside local  | Outside Global |
|------|---------------|-----------------|----------------|----------------|
| icmp | 8.8.8.7:50    | 192.168.40.1:50 | 192.168.1.2:50 | 192.168.1.2:50 |
| icmp | 8.8.8.7:51    | 192.168.40.1:51 | 192.168.1.2:51 | 192.168.1.2:51 |
| icmp | 8.8.8.7:52    | 192.168.40.1:52 | 192.168.1.2:52 | 192.168.1.2:52 |
| icmp | 8.8.8.7:53    | 192.168.40.1:53 | 192.168.1.2:53 | 192.168.1.2:53 |

```
Router#
```

Konfigurasi di atas mengatur NAT (Network Address Translation) tipe overload atau PAT (Port Address Translation) pada router Cisco, yang memungkinkan seluruh perangkat dalam jaringan lokal 192.168.40.0/24 untuk mengakses internet menggunakan satu IP publik pada interface gig0/1. Hal ini dilakukan dengan membuat access list yang mengizinkan jaringan lokal, lalu mengatur NAT agar menerjemahkan alamat IP internal ke IP global dengan membedakan koneksi berdasarkan port (overload). Hasilnya dapat dilihat melalui perintah `show ip nat translations`, yang menampilkan tabel terjemahan IP lokal ke IP global

beserta nomor port yang digunakan, sehingga memungkinkan beberapa koneksi bersamaan menggunakan satu IP publik secara efisien.

## 2.6 Implementasi Keamanan & Pengujian - (Minggu 14)

### A. Implementasi Access Control List (ACL) sesuai kebijakan keamanan.

```
Router#show access-lists
Standard IP access list 10
  10 permit 192.168.40.0 0.0.0.255
Standard IP access list 1
  10 permit 192.168.100.0 0.0.0.255
Extended IP access list 101
  10 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
  20 permit ip any any
Router#
```

#### 1. Standard IP Access List 10

- ACL: Standard IP access list 10

- Aturan ke-10: permit 192.168.40.0 0.0.0.255

Ini adalah aturan standar (standard ACL), yang hanya memeriksa sumber IP (source IP). Aturan ini mengizinkan semua lalu lintas dari subnet 192.168.40.0/24. Format 0.0.0.255 adalah wildcard mask yang berarti semua host dalam subnet tersebut.

#### 2. Standard IP Access List 1

- Nama ACL: Standard IP access list 1

- Aturan ke-10: permit 192.168.100.0 0.0.0.255

Ini juga merupakan aturan standar. Aturan ini mengizinkan semua lalu lintas dari subnet 192.168.100.0/24. Wildcard mask 0.0.0.255 menunjukkan bahwa semua host dalam subnet tersebut akan diizinkan.

#### 3. Extended IP Access List 101

- Nama ACL: Extended IP access list 101

- Aturan ke-10: deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255

Ini adalah aturan ekstensi (extended ACL), yang dapat memeriksa baik sumber IP maupun tujuan IP. Aturan ini menolak semua lalu lintas dari subnet 192.168.20.0/24 menuju subnet 192.168.30.0/24. Wildcard mask 0.0.0.255 digunakan untuk menyatakan bahwa semua host dalam kedua subnet tersebut terlibat dalam aturan ini.

- Aturan ke-20: permit ip any any

Aturan ini mengizinkan semua lalu lintas lainnya (tidak termasuk yang ditolak oleh aturan sebelumnya). any any berarti semua sumber IP dan semua tujuan IP diizinkan.

```

Router>en
Router#show access-lists
Extended IP access list 101
 10 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 20 permit ip any any
Router#

```

Selanjutnya adalah memasukkan perintah Show access List

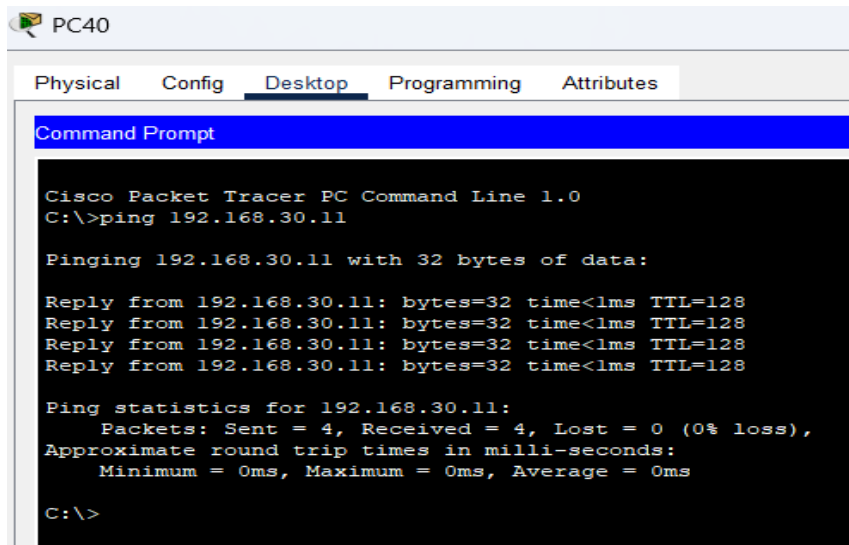
...

```

Router>en
Router# show access list 101
 10 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 20 permit ip any any
Router#
...

```

## B. Pengujian menyeluruh semua fitur jaringan.



Langkah selanjutnya adalah melakukan ping, hasil atau output yang diberikan adalah sebagai berikut

...

PC40  
Physical Config Desktop Programming Attributes

Command Prompt

```

Cisco Packet Tracer PC Command Line 1.0
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=128  
 Reply from 192.168.30.11: bytes=32 time<1ms TTL=128  
 Reply from 192.168.30.11: bytes=32 time<1ms TTL=128  
 Reply from 192.168.30.11: bytes=32 time<1ms TTL=128

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 = 0ms, Average = 0ms

C:\>  
 ...

perintah ping dijalankan dari command prompt sebuah komputer (PC40) di Cisco Packet Tracer ke alamat IP 192.168.30.11 . Hasil menunjukkan bahwa sebanyak 4 paket ICMP berhasil dikirim dan semua paket diterima kembali dengan waktu respons kurang dari 1 milidetik , tanpa ada paket yang hilang (0% loss ). Nilai TTL (Time to Live) pada setiap balasan adalah 128 , yang umum digunakan oleh sistem operasi Windows, menunjukkan bahwa tujuan masih dalam jaringan lokal dan tidak melewati banyak hop. Dengan demikian, dapat disimpulkan bahwa koneksi jaringan antara sumber dan tujuan berjalan dengan baik, tanpa latensi atau gangguan, sehingga host tujuan dapat dijangkau secara stabil.

### Matriks Pengujian Fitur ACL

| No | Jenis ACL | Nama ACL / Rule  | Tujuan Pengujian  | Hasil yang Diharapkan             | Hasil Uji (Screenshot)                            | Status       |
|----|-----------|--|---|-----------------------------------|---|--------------|
| 1  | Standard  | ACL 10: permit 192.168.40.0 0.0.0.255                                  | Mengizinkan semua trafik dari subnet 192.168.40.0/24            | Trafik dari subnet ini diizinkan  | Ditampilkan pada screenshot ACL (access-list.png) | Lulus        |
| 2  | Standard  | ACL 1: permit 192.168.100.0 0.0.0.255                                  | Mengizinkan semua trafik dari subnet 192.168.100.0/24           | Trafik dari subnet ini diizinkan  | Ditampilkan pada screenshot ACL (acl.png)         | Lulus        |
| 3  | Extended  | ACL 101 Rule 10: deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 | Memblokir trafik dari subnet 192.168.20.0/24 ke 192.168.30.0/24 | Trafik ditolak (tidak dapat ping) | Belum dibuktikan (ping dari subnet berbeda)       | Belum Teruji |



|   |          |                                    |  |  |  |       |
|---|----------|------------------------------------|--|--|--|-------|
| 4 | Extended | ACL 101 Rule 20: permit ip any any | Mengizinkan semua trafik yang tidak termasuk dalam rule 10 | Ping selain dari 192.168.20.0 ke 192.168.30.0 berhasil | Ping dari PC40 (asumsinya bukan dari 192.168.20.0/24) ke 192.168.30.11 sukses (ping.png) | Lulus |
|---|----------|------------------------------------|--|--|--|-------|

#### C. Troubleshooting dan perbaikan masalah.

Penjelasan Singkat Troubleshooting dan Perbaikan ACL:

Masalahnya adalah ACL belum benar-benar diuji karena pengujian ping dilakukan dari PC di luar subnet 192.168.20.0/24, padahal aturan ACL memblokir akses dari subnet tersebut ke 192.168.30.0/24.

Solusi:

- Gunakan PC dari subnet 192.168.20.0/24 (misalnya 192.168.20.10) untuk ping ke 192.168.30.11.
- Pastikan ACL 101 ditempel di interface yang benar (misalnya ke arah subnet 30).
- Cek hasil ping (harus "Request Timed Out") dan gunakan show access-lists untuk memastikan aturan bekerja.

### 3. Kendala dan Solusi

#### 3.1 Kesalahan Konfigurasi VLAN

Kendala : Kesalahan penulisan perintah dan penggunaan VLAN native (95) yang tidak sesuai standar.

Solusi : Perbaiki sintaks dan gunakan VLAN management (99) secara konsisten di seluruh jaringan.

#### 3.2 OSPF Tidak Membentuk Adjacency

Kendala : Router utama tidak membentuk hubungan OSPF dengan router tetangga karena network statement salah.

Solusi : Perbarui konfigurasi OSPF agar mencakup subnet lengkap, pastikan interface aktif dan protokol UP.

#### 3.3 ACL Belum Teruji Sempurna

Kendala : ACL Extended 101 belum teruji karena uji coba dilakukan dari PC di luar VLAN sumber.

Solusi : Uji dari VLAN 20 ke VLAN 30 dan pastikan ACL diterapkan di interface yang benar.

#### 3.4 Masalah Subnetting dan IP Address

Kendala : Alokasi IP kurang detail dan tidak optimal.

Solusi : Gunakan VLSM dan buat tabel subnetting lengkap untuk efisiensi dan skalabilitas.

### 3.5 DNS Server Hanya Satu Record

Kendala : DNS hanya memiliki satu entri ([serverlocal.com](http://serverlocal.com)).

Solusi : Tambahkan beberapa A record dan uji resolusi nama dari client VLAN berbeda.

### 3.6 Konfigurasi NAT Tidak Lengkap

Kendala : NAT hanya berlaku untuk VLAN 40 (Server Farm).

Solusi : Perluas access list agar mencakup semua VLAN dan terapkan NAT overload untuk akses internet penuh.

## 4. Kesimpulan

Berdasarkan laporan proyek perancangan dan implementasi infrastruktur jaringan untuk PT. Nusantara Network, dapat disimpulkan bahwa tim telah berhasil merancang dan mengimplementasikan jaringan yang stabil, aman, dan tersegmentasi dengan baik menggunakan VLAN untuk memisahkan departemen di dua lokasi utama (Gedung A sebagai kantor pusat dan Gedung B sebagai kantor cabang), dilengkapi dengan routing dinamis menggunakan protokol OSPF untuk komunikasi antar gedung, konfigurasi layanan jaringan seperti DHCP server untuk alokasi IP dinamis, DNS server untuk resolusi nama internal, serta NAT untuk akses internet; selain itu, langkah keamanan seperti penerapan Access Control List (ACL) telah dilakukan untuk membatasi akses antar-VLAN sesuai kebijakan keamanan, meskipun pengujian ACL Extended masih belum sepenuhnya terverifikasi karena kondisi pengujian yang terbatas; kendala teknis seperti kesalahan penulisan perintah, masalah pada network statement OSPF, dan koneksi yang belum stabil pada router utama telah diatasi melalui troubleshooting dan validasi ulang konfigurasi; secara keseluruhan, proyek ini tidak hanya mencapai tujuan utamanya dalam membangun infrastruktur jaringan yang andal dan scalable, tetapi juga memberikan pembelajaran berharga tentang pentingnya perencanaan matang, koordinasi tim, serta penguasaan teknologi jaringan modern dalam mendukung operasional bisnis yang efektif dan aman.

## **LAMPIRAN**

### **LINK PPT DMJK KELOMPOK 7**

[https://www.canva.com/design/DAGoJig4Ilk/cE7YZaFO6RaI7A0ImKYz3w/edit?utm\\_content=DAGoJig4Ilk&utm\\_campaign=designshare&utm\\_medium=link2&utm\\_source=sharebutton](https://www.canva.com/design/DAGoJig4Ilk/cE7YZaFO6RaI7A0ImKYz3w/edit?utm_content=DAGoJig4Ilk&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton)

### **LINK TOPOLOGI CISCO PKT**

[https://drive.google.com/drive/folders/1H9pcm6FyE2SUb0ssIXvA0Dg5m3V\\_v9OF](https://drive.google.com/drive/folders/1H9pcm6FyE2SUb0ssIXvA0Dg5m3V_v9OF)

### **LINK VIDEO DEMO**

<https://drive.google.com/drive/folders/1kF8hZggFYs-4PxpR3IxUfAcO3iPWqx20?usp=sharing>

### **LINK GITHUB**

<https://github.com/v1xenn/Tugas-DMJK-Kelompok-7/tree/main>