

TUGAS AKHIR DMJK - 6

Desain Manajemen Jaringan Komputer



ANGGOTA



Az-Zahra Atikah N
10231022



Chintya
10221078



Djaky Abyyu Fauzan T
10231032

STUDI KASUS

PT. Nusantara Network adalah perusahaan yang bergerak di bidang teknologi informasi dengan 4 departemen utama dan memiliki cabang di 2 lokasi berbeda. Perusahaan ini membutuhkan infrastruktur jaringan yang aman, efisien, dan mudah dikelola.

DETAIL ORGANISASI

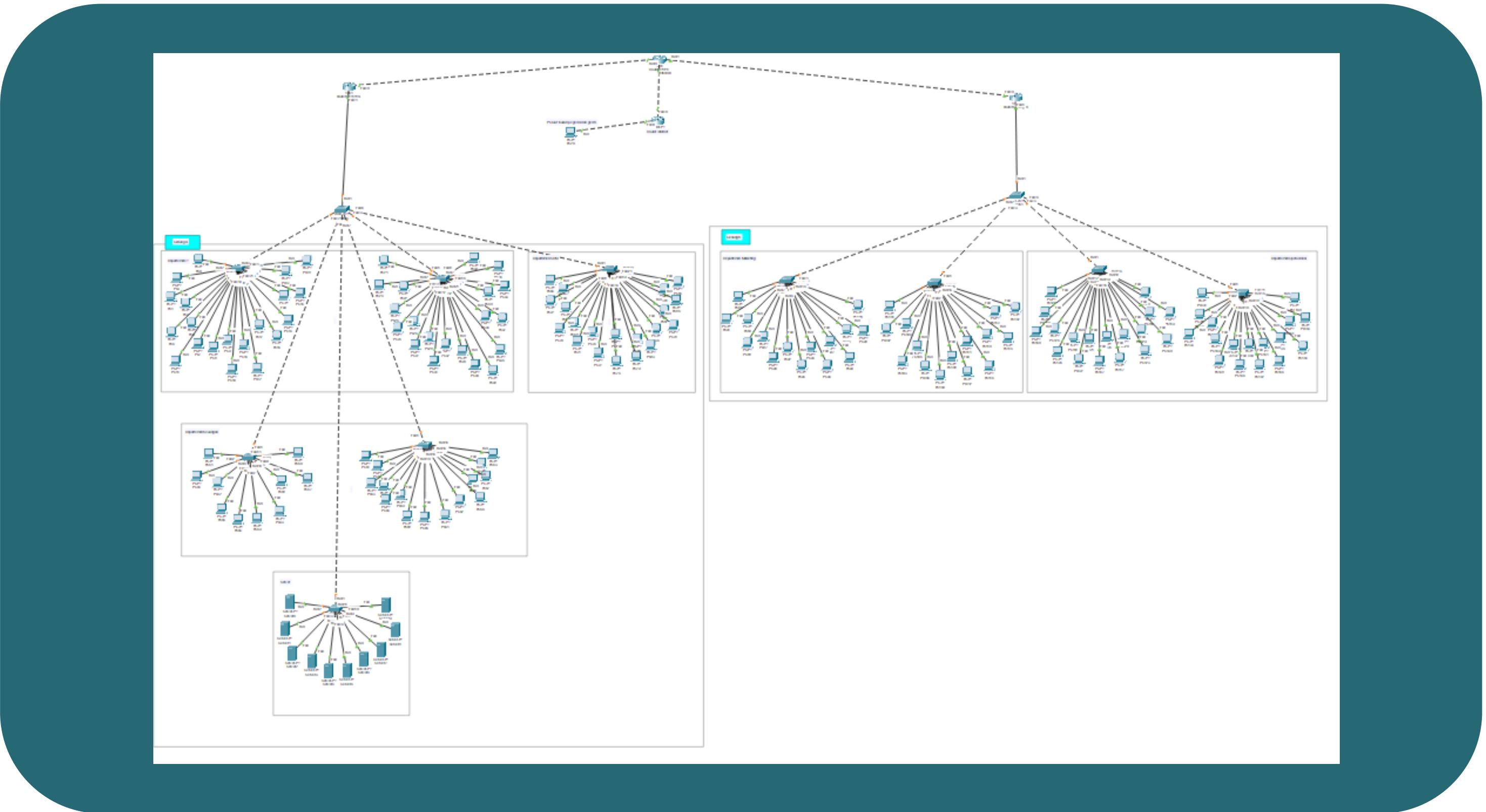
Kantor Pusat (Gedung A)

- Departemen IT (40 komputer)
- Departemen Keuangan (25 komputer)
- Departemen SDM (20 komputer)
- Server Farm (10 server untuk berbagai layanan)

Kantor Cabang (Gedung B):

- Departemen Marketing (30 komputer)
- Departemen Operasional (35 komputer)

DESAIN TOPOLOGI JARINGAN



VLAN DAN TRUNKING

01

Implementasi VLAN

Pembagian VLAN Berdasarkan Departemen Gedung A

- VLAN 10: Departemen IT
- VLAN 20: Departemen Keuangan
- VLAN 30: Departemen SDM
- VLAN 40: Server Farm

Gedung B

- VLAN 50: Departemen Marketing
- VLAN 60: Departemen Operasional

02

Trunking

Port yang sama kemudian diubah menjadi mode trunk, yang berfungsi untuk membawa lalu lintas dari beberapa VLAN. Penggunaan mode access dan trunk secara bersamaan pada satu port tidak disarankan karena dapat menyebabkan konflik konfigurasi. Oleh karena itu, perlu dipastikan setiap port memiliki fungsi yang jelas, apakah sebagai akses atau trunk, sesuai kebutuhan jaringan.

ROUTING & WAN



Routing Statis

```
ip route 192.168.40.0 255.255.255.0 10.10.10.2
```

```
ip route 192.168.50.0 255.255.255.0 10.10.10.2
```

Kedua perintah ini digunakan untuk membuat router mengetahui ke mana harus mengirim paket jika tujuannya ke jaringan 192.168.40.0 atau 192.168.50.0.

Routing Dinamis OSPF Antar-Gedung

Routing antar-gedung dilakukan menggunakan protokol dinamis OSPF (Open Shortest Path First) untuk mempermudah manajemen dan otomatisasi rute.



Simulasi WAN

Pengujian dilakukan dari PC menggunakan perintah `ping` ke beberapa IP tujuan:

10.10.10.2 → Router tetangga

10.10.20.1 → Router antar-gedung

192.168.40.2 → Host dari gedung lain



DHCP, DNS & NAT

Pada konfigurasi DHCP, DNS setiap departemen memiliki subnet jaringan sendiri, default gateway yang spesifik, serta domain name internal masing-masing. Server DNS yang digunakan adalah publik (8.8.8.8) untuk menyederhanakan proses

Konfigurasi NAT digunakan agar perangkat dengan IP private di jaringan lokal dapat berkomunikasi ke jaringan publik (misalnya internet) dengan menerjemahkan alamat IP mereka.



KEAMANAN & PENGUJIAN

Access Control List (ACL) yang diterapkan berhasil meningkatkan keamanan jaringan dengan cara membatasi komunikasi antar subnet tertentu berdasarkan IP.

Pengujian dilakukan secara menyeluruh untuk memastikan semua fitur jaringan berjalan dengan baik, termasuk koneksi antar departemen dan implementasi kebijakan keamanan menggunakan ACL.

KESIMPULAN PRESENTASI

Seluruh fitur jaringan berhasil diimplementasikan sesuai rencana: VLAN, routing static & dinamis, DHCP, DNS, NAT, dan keamanan ACL. Hasil pengujian mendukung bahwa jaringan dapat berjalan optimal dan sesuai kebijakan keamanan serta tugas besar ini membantu kami belajar pentingnya perencanaan topologi, pembagian subnet, koordinasi tim, dan troubleshooting konfigurasi nyata di jaringan. Proyek ini membantu kami memahami keterkaitan antar layanan jaringan serta pentingnya dokumentasi yang baik.

TERIMA KASIH

