

**LAPORAN TUGAS PROJECT**

**Mata Kuliah : Proyek Jaringan Komputer**

**Judul Tugas : Optimalisasi Jaringan Perusahaan**

**dengan VPN Tunnel Multi-Site.**

**Pertemuan :**

**Dosen Pengampu : Boy Yuliadi S.Kom**

**Nama Mahasiswa : Kenedi Peres**

**NIM : 411221012**

# **PERNYATAAN KEASLIAN TUGAS**

Saya yang bertanda tangan di bawah ini menyatakan bahwa tugas ini dibuat dengan usaha sendiri dan berdasarkan referensi yang valid. Saya juga menyatakan bahwa saya (tidak menggunakan) Chat GPT atau AI lainnya dalam pembuatan tugas ini. Jika menggunakan AI, saya memastikan bahwa saya telah melakukan verifikasi terhadap kebenaran dan keakuratan informasi yang dihasilkan.

Nama : Kenedi Peres

NIM : 411221012

Program Studi : Teknik Informatika

Tanggal : 25 April 2025

Tanda Tangan :

# 

# **KATA PENGANTAR**

Puji syukur kehadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan Proyek Jaringan Komputer ini dengan judul ***“Optimalisasi Jaringan Perusahaan dengan VPN Tunnel Multi-Site.”***.

Laporan ini disusun sebagai bagian dari upaya mengidentifikasi dan memberikan solusi terhadap tantangan teknis yang dihadapi perusahaan, khususnya dalam pengelolaan infrastruktur jaringan komputer. Pesatnya ekspansi operasional dan tingginya ketergantungan pada teknologi informasi mendorong perlunya evaluasi menyeluruh terhadap keamanan data, segmentasi jaringan, penyimpanan terpusat, serta komunikasi antar kantor. Penulis mengucapkan terima kasih kepada:

1. PT. Citra Mandiri Negara atas kesempatan dan dukungan data selama penelitian.
2. Pembimbing dan Tim IT perusahaan yang telah memberikan masukan berharga.
3. Rekan-rekan tim yang turut berkontribusi dalam diskusi dan pengembangan solusi.

Laporan ini mencakup analisis kebutuhan, desain solusi, hingga evaluasi implementasi dengan harapan dapat menjadi referensi bagi peningkatan infrastruktur TI perusahaan. Penulis menyadari masih terdapat keterbatasan dalam laporan ini, sehingga saran dan kritik konstruktif sangat diharapkan untuk penyempurnaan di masa mendatang.

**Jakarta, 13 Maret 2025**

**Kenedi Peres**

**411221012**

# 

# **ABSTRAK**

Laporan ini membahas optimalisasi jaringan perusahaan PT. Citra Mandiri Negara dengan implementasi VPN Tunnel Multi-Site untuk meningkatkan efisiensi, keamanan, dan skalabilitas jaringan. Melalui segmentasi VLAN, trunking, OSPF, dan VPN Tunnel, solusi yang dirancang berhasil mengatasi tantangan komunikasi antar divisi dan kantor cabang. Hasil pengujian menunjukkan keberhasilan komunikasi antar VLAN yang diizinkan, seperti VLAN 15 dengan VLAN 45, 50, 55, 70, dan 100 ataupun sebaliknya, serta isolasi VLAN tertentu untuk keamanan. Implementasi *Access Control List*, DHCP, dan *EtherChannel* juga turut memperkuat manajemen jaringan. Laporan ini menyimpulkan bahwa solusi yang diterapkan mampu mendukung pertumbuhan perusahaan di masa depan dengan infrastruktur yang lebih andal dan terintegrasi.

**Kata Kunci:** VLAN, Trunking, VPN Tunnel, OSPF, Keamanan Jaringan, Skalabilitas Jaringan, Efisiensi Jaringan

# **DAFTAR ISI**

[**PERNYATAAN KEASLIAN TUGAS 2**](#_heading=h.hcafhpj14kyc)

[**KATA PENGANTAR 3**](#_heading=h.wj8qilghfpg5)

[**ABSTRAK 4**](#_heading=h.vf8inmout8ip)

[**DAFTAR ISI 5**](#_heading=h.vy9v69ckndyt)

[**BAB I PENDAHULUAN 7**](#_heading=h.i299wgaamq4v)

[1.1 Latar Belakang 7](#_heading=h.cqzltrel3ife)

[**1.2 Rumusan Masalah 7**](#_heading=)

[1.3 Tujuan dan Manfaat Penelitian 7](#_heading=h.b5jif6fipmsg)

[**BAB II TINJAUAN PUSTAKA 9**](#_heading=)

[2.1 VLAN (Virtual Local Area Network) 9](#_heading=h.t9lr2cvh6ujy)

[2.2 Trunking 9](#_heading=h.1wfar6hxr9jh)

[2.3 Access Control List (ACL) 10](#_heading=h.lxljkmqjutap)

[2.4 Etherchannel 10](#_heading=h.1zro8hjx4m1)

[2.5 DHCP (Dynamic Host Configuration Protocol) 10](#_heading=h.tw8sk0l7g8e4)

[2.6 Open Shortest Path First (OSPF) 10](#_heading=h.n0j0bl20heha)

[2.7 VPN Tunnel 11](#_heading=h.4ggennk17kq3)

[**BAB III METODOLOGI PENELITIAN 12**](#_heading=h.1owu6bw75zqo)

[3.1 Jenis Penelitian 12](#_heading=h.5jpep91rugp1)

[3.2 Pengumpulan Data 12](#_heading=h.6ml8q4cabxgx)

[3.3 Analisis Kebutuhan 12](#_heading=h.lp9zlnkx7or7)

[3.4 Perancangan Topologi 13](#_heading=h.59i2m2bdqpvn)

[3.5 Timeline 13](#_heading=h.y37cczwv26px)

[**BAB IV HASIL PEMBAHASAN 15**](#_heading=h.pzgkxesua8te)

[4.1 Analisis Jaringan Eksisting 15](#_heading=h.vfhdqrd053qh)

[4.2 Rekomendasi Desain Topologi 15](#_heading=h.l2vyctjghyu3)

[4.3 Konfigurasi VLAN dan Trunking 16](#_heading=h.l9p3l7okoasv)

[4.4 Implementasi Routing OSPF 17](#_heading=h.61kq6ym2w8mg)

[4.5 Penerapan Keamanan LAN 18](#_heading=h.t6ekekmb31ia)

[4.6 Implementasi DHCP dan EtherChannel 18](#_heading=h.gkwsxcqjs2yo)

[4.7 Konfigurasi End Device 18](#_heading=h.27f8ahhceqdl)

[4.7 Hasil Pengujian Simulasi Jaringan 59](#_heading=h.ds988qdnjhzj)

[**BAB V PENUTUP 75**](#_heading=h.qyy0rqsiw9al)

[5.1 Kesimpulan 75](#_heading=h.iwo513djvp71)

[5.2 Saran 75](#_heading=h.c69oc5awcxwi)

[**DAFTAR PUSTAKA 76**](#_heading=h.bur3lrjit7tz)

[**LAMPIRAN DATA PUBLIKASI DOSEN TEKNIK INFORMATIKA 80**](#_heading=h.m8dngyxy06md)

[Mencari Publikasi di Sinta 80](#_heading=h.r8s92m1sf7in)

# 

# **BAB I PENDAHULUAN**

## **1.1 Latar Belakang**

Perkembangan teknologi informasi yang sangat pesat membuat kebutuhan masyarakat dunia akan akses internet semakin tinggi. Perkembangan tersebut mengharuskan sebuah perusahaan dapat memiliki hak akses pada jaringan Publik /layanan internet. Dengan internet perusahaan dapat saling terhubung satu dengan lainnya dengan jaringan komputer berbasi WAN (*Wide Area Network*) (Wahyudi & Firmansyah, 2021).

Ekspansi operasional PT. Citra Mandiri Negara yang berlangsung pesat, disertai dengan meningkatnya kebutuhan akan teknologi informasi, telah menciptakan tantangan dalam hal transfer dan komunikasi data antara kantor pusat dan cabang. Tingginya pertumbuhan jumlah perangkat dan pengguna mengakibatkan kompleksitas jaringan yang semakin tinggi, termasuk kebutuhan komunikasi real-time, dan keandalan koneksi, dalam pertukaran data yang belum sepenuhnya terpenuhi.

Oleh karena itu, redesain infrastruktur jaringan komputer menjadi solusi untuk meningkatkan efisiensi komunikasi, dan skalabilitas jaringan sejalan dengan perkembangan perusahaan. Salah satu aspek utama yang perlu diperbaiki adalah optimasi *Local Area Network* (LAN) sebagai tulang punggung komunikasi internal maupun eksternal, termasuk penerapan protokol jaringan yang lebih efisien dan terintegrasi guna mendukung aliran data yang stabil antara kantor pusat dan seluruh cabang. Dengan demikian, perusahaan dapat memastikan kelancaran operasional, dan peningkatan produktivitas.

## **1.2 Rumusan Masalah**

1. Bagaimana meningkatkan keandalan dan kecepatan transfer data antara kantor pusat dan cabang mengingat tingginya pertumbuhan pengguna dan perangkat yang membutuhkan komunikasi intensif?
2. Bagaimana mengoptimalkan protokol jaringan untuk mendukung pertukaran data yang efisien, stabil, dan aman antar-lokasi?
3. Bagaimana merancang infrastruktur jaringan yang *scalable* agar mampu menyesuaikan dengan perkembangan perusahaan di masa depan?

## **1.3 Tujuan dan Manfaat Penelitian**

**1.3.1 Tujuan Penelitian**  
Adapun Tujuan yang dapat diperoleh dari perancangan ini antara lain:

1. Meningkatkan Keandalan dan Kecepatan Transfer Data

Merancang infrastruktur jaringan yang mampu menangani pertumbuhan pengguna dan perangkat dengan komunikasi intensif antara kantor pusat dan cabang.

1. Meningkatkan Keamanan

Melalui segmentasi VLAN, VPN *Tunnel* dan penerapan *Access Control List* (ACL) untuk membatasi dan mengisolasi VLAN.

1. Mendesain Jaringan yang Scalable

Membangun infrastruktur yang dapat menyesuaikan dengan perkembangan perusahaan di masa depan.

**1.3.1 Manfaat Penelitian**  
Adapun manfaat yang dapat diharapkan dari perancangan ini antara lain:

1. Mempercepat proses produksi dengan mengurangi hambatan transfer data antar-divisi dan kantor cabang.
2. Mengurangi ketergantungan pada layanan vendor atau pihak ketiga untuk transfer file besar.
3. Penyederhanaan manajemen jaringan dengan DHCP dan konfigurasi terpusat.
4. Infrastruktur yang dirancang mampu mendukung ekspansi perusahaan di masa depan tanpa perlu perubahan besar.

# **BAB II TINJAUAN PUSTAKA**

## **2.1 VLAN *(Virtual Local Area Network)***

*Virtual Local Area Network* (VLAN) adalah sebuah metode untuk mengelompokkan perangkat-perangkat jaringan secara virtual. Pengelompokan ini memungkinkan lalu lintas jaringan antar kelompok dapat diatur dan dikendalikan dengan lebih efektif (Rifandi, 2023). VLAN umumnya dikonfigurasi berdasarkan kebijakan yang ditentukan oleh administrator jaringan, seperti lokasi fisik, departemen, atau fungsi perangkat (Rifandi, 2023).

Sebagai sebuah teknik jaringan, VLAN mengelola sekelompok pengguna dalam satu basis data VLAN, di mana kelompok atau grup VLAN ini disusun berdasarkan *switchport* yang ada pada sebuah *switch* (Saputra et al., 2023). Lebih lanjut, VLAN dapat didefinisikan sebagai kumpulan perangkat di satu atau lebih jaringan LAN yang dikonfigurasikan melalui perangkat lunak (Ismail et al., 2021). Beberapa tipe koneksi VLAN meliputi *Trunk Link*, *Access Link*, dan *Hybrid Link* (Ismail et al., 2021). Jaringan LAN sendiri sering digunakan untuk menghubungkan komputer pribadi dan *workstation* dalam suatu kantor atau pabrik guna berbagi sumber daya, seperti *printer*, dan bertukar informasi (Suryantoro et al., 2021).

## **2.2 Trunking**

Semua tautan harus melewati pusat yang menyalurkan data ke semua simpul atau *client* yang dipilih. Jaringan tersebut dibangun dengan bantuan *Switch* yang secara standar *(default)* membuat jaringan tunggal dengan *domain broadcast* yang besar, dan ini terus bertambah jumlahnya sesuai kebutuhan di jaringan LAN (Ismail et al., 2021). Dengan adanya infrastruktur jaringan *Virtual Local Area Network* (VLAN) menggunakan metode *VLAN Trunking Protocol* (VTP), diharapkan Jaringan *Local Area Network* (LAN) menjadi lebih fleksibel dan meningkatkan kinerja jaringan dengan cara memecah jaringan ke segmen-segmen yang lebih kecil, sehingga akan mengurangi *traffic* pada saat pertukaran data. Selain itu, VLAN juga dapat membatasi hak akses setiap pengguna dengan cara mengelompokkan IP setiap segmen (Ar Rasyid et al., 2024).

## **2.3 Access Control List (ACL)**

Salah satu cara untuk melakukan packet filtering adalah dengan menggunakan *Access Control List* (ACL). ACL memberi *network administrator* kemampuan untuk mengontrol paket-paket yang dapat diakses melalui *proxy server.* Dalam aplikasi Winbox, ACL dapat digabungkan dengan perintah *http\_access* untuk menentukan apakah paket-paket akan ditolak atau diterima masuk ke sistem. Daftar kontrol akses merupakan dasar *filtering* untuk aplikasi Winbox (Amar et al., 2022).

## **2.4 Etherchannel**

*Etherchannel* adalah protokol yang memungkinkan penggabungan dua atau lebih *physical port* pada perangkat switch atau *router interface* menjadi satu grup logis (Amal, 2021). Umumnya, *Etherchannel* dimanfaatkan untuk meningkatkan kapasitas *bandwidth,* mengoptimalkan kinerja, dan meningkatkan keandalan jaringan, dengan cara menggabungkan beberapa jalur fisik menjadi satu jalur logis (Rifandi, 2023).

## **2.5 DHCP *(Dynamic Host Configuration Protocol)***

DHCP membantu menghemat penggunaan alamat IP karena tidak harus menetapkan alamat IP secara permanen ke setiap komputer klien. Server DHCP adalah perangkat jaringan yang dapat memberikan alamat IP kepada komputer *client* yang tersambung ke jaringan agar komputer tersebut dapat berkomunikasi (Maneka dan Kahewu 2021).

## **2.6 Open Shortest Path First (OSPF)**

*Open Shortest Path First* (OSPF) mendistribusikan informasi *router* yang tergabung dalam autonomous system (AS), yang kemudian disebarkan dalam beberapa *link-state advertisement* (LSA) dan disimpan dalam *link-state database* (LSDB). Untuk membentuk tabel *routing*, dilakukan perhitungan *Shortest Path First* dari *link-state database*. Apabila terjadi perubahan topologi jaringan, perhitungan ulang akan dilakukan. OSPF juga merupakan protokol *routing* yang dapat mempelajari berbagai rute dan memilih lebih dari satu rute untuk mencapai tujuan (Tama et al., 2023).

## **2.7 VPN Tunnel**

*Virtual Private Network* (VPN) adalah teknologi yang dirancang untuk menyediakan koneksi komunikasi aman melalui jaringan publik. VPN bekerja dengan mengenkripsi data dan memastikan keamanan komunikasi antara pengguna dan jaringan tujuan. Di era digital ini, VPN telah menjadi kebutuhan utama di berbagai sektor termasuk bisnis, pendidikan, organisasi pemerintahan untuk melindungi informasi sensitif dari ancaman pihak ketiga, (Ariyadi & Prabowo, 2021).

# **BAB III METODOLOGI PENELITIAN**

## **3.1 Jenis Penelitian**

Penelitian ini tergolong sebagai penelitian terapan *(applied research)* dengan pendekatan pengembangan sistem. Hal ini dikarenakan penelitian ini bertujuan untuk merancang ulang dan mengembangkan infrastruktur jaringan pada PT. Citra Mandiri Negara guna mengatasi permasalahan yang teridentifikasi, serta meningkatkan efisiensi, keamanan, dan skalabilitas jaringan secara keseluruhan.

## **3.2 Pengumpulan Data**

Pengumpulan data merupakan tahapan krusial dalam penelitian ini untuk memperoleh informasi yang akurat dan relevan terkait infrastruktur jaringan PT. Citra Mandiri Negara. Metode yang digunakan meliputi:

1. Observasi Topologi Eksisting  
   Observasi dilakukan secara langsung terhadap infrastruktur jaringan yang saat ini beroperasi di kantor pusat yaitu PT. Citra Mandiri Negara dan kantor cabang PT. Citra Print Indonesia (CPI) serta PT. Citra Factory Indonesia (CFI). Fokus observasi meliputi identifikasi perangkat keras jaringan, konfigurasi alamat IP, pembagian subnet, serta analisis alur lalu lintas data yang ada. Tujuan dari observasi ini adalah untuk memahami secara mendalam struktur jaringan dan mengidentifikasi potensi sumber masalah seperti broadcast storm dan segmentasi yang kurang efisien.
2. Studi Literatur  
   Studi literatur dilakukan untuk mengumpulkan teori, konsep, dan penelitian terdahulu yang relevan dengan perancangan jaringan komputer, khususnya mengenai *Virtual Local Area Network* (VLAN), *Trunking* *(protocol 802.1Q)*, *Virtual private network* (VPN) *tunnel*, *Access Control List* (ACL), *EtherChannel,* dan *Dynamic Host Configuration Protocol* (DHCP). Informasi dari studi literatur ini menjadi dasar dalam perancangan solusi dan pengembangan kerangka berpikir penelitian.

## **3.3 Analisis Kebutuhan**

Analisis kebutuhan dalam penelitian ini merupakan langkah krusial untuk memastikan bahwa perancangan ulang infrastruktur jaringan dapat secara efektif menjawab tantangan dan kebutuhan operasional PT. Citra Mandiri Negara. Kebutuhan utama yang diidentifikasi meliputi.

1. Peningkatan efisiensi jaringan melalui optimalisasi routing dan segmentasi VLAN.
2. Penguatan keamanan dengan kontrol akses dan LAN Security.
3. Peningkatan skalabilitas jaringan
4. Penyederhanaan manajemen alamat IP.

## **3.4 Perancangan Topologi**

Bagian perancangan topologi jaringan akan menguraikan konfigurasi jaringan yang mengusulkan hal-hal sebagai berikut,

1. Segmentasi Jaringan  
   Pembagian jaringan ke dalam *Virtual Local Area Network* (VLAN) berdasarkan divisi atau fungsi, seperti VLAN Prepress & Desainer dan VLAN CTP, untuk meningkatkan segmentasi dan isolasi lalu lintas.
2. Koneksi Aman Antar-Site dengan VPN Tunnel

Penerapan VPN Tunnel untuk menghubungkan kantor pusat dan cabang secara aman melalui jaringan publik. VPN Tunnel menggunakan enkripsi data guna memastikan kerahasiaan dan integritas komunikasi antar-site.

1. Konektivitas Antar-VLAN  
   Implementasi teknologi *Trunking* (protokol 802.1Q) melalui satu jalur fisik untuk efisiensi konektivitas antar-VLAN, khususnya antar switch dan router.
2. Skema Pengalamatan IP  
   Perencanaan skema pengalamatan IP yang efisien untuk setiap VLAN dan subnet yang akan digunakan, serta penyederhanaan pengelolaan alamat IP melalui protokol DHCP.

## **3.5 Timeline**

Berikut adalah tahapan pelaksanaan penelitian yang telah direncanakan:

*Tabel 1. Timeline Proyek*

| **Minggu** | **Kegiatan** | **Prioritas** | **Deskripsi Kegiatan** | **Durasi** | **Bukti Dokumentasi Kegiatan** |
| --- | --- | --- | --- | --- | --- |
| **Ke-1** | **Pengenalan Perusahaan dan Orientasi** | **Tinggi** | Menyusun jadwal orientasi perusahaan dan pengenalan sistem. Mempelajari struktur organisasi dan prosedur kerja. | 7 hari | [***Data Gambar***](https://drive.google.com/drive/folders/1BZne88TBw2Z5YW39PWpdNybg24hpj8Up?usp=drive_link) |
| **Ke-2** | **Perencanaan dan Analisis** | **Tinggi** | Pengumpulan kebutuhan, analisis jaringan saat ini, penentuan tujuan VLAN. | 7 hari | [Data Gambar](https://drive.google.com/drive/folders/1BZne88TBw2Z5YW39PWpdNybg24hpj8Up?usp=drive_link) |
| **Ke-3** | **Perancangan Topologi Jaringan** | **Tinggi** | Perancangan topologi VLAN, pengalamatan IP, konfigurasi trunking. | 21 hari | [Data Gambar](https://drive.google.com/drive/folders/1BZne88TBw2Z5YW39PWpdNybg24hpj8Up?usp=drive_link) |
| **Ke-4** | **Konfigurasi** | **Sedang** | Konfigurasi perangkat jaringan (switch dan router), implementasi VLAN, trunking, dan VPN Tunnel. | 28 hari | File |
| **Ke-5** | **Testing & Optimasi** | **Sedang** | Pengujian fungsionalitas VLAN, trunking, dan VPN Tunnel. Validasi kinerja jaringan. | 21 Hari | File |
| **Ke-6** | **Dokumentasi dan Laporan akhir** | **Tinggi** | Pembuatan dokumentasi lengkap (topologi, konfigurasi, hasil pengujian) | 7 Hari | File |

### 

**Keterangan:**

1. **Prioritas Tinggi (Tinggi)**: Tugas yang sangat penting dan harus diselesaikan terlebih dahulu karena mempengaruhi kelancaran proses pekerjaan dan keberhasilan proyek.
2. **Prioritas Sedang (Sedang)**: Tugas yang penting, namun bisa dilakukan setelah tugas-tugas prioritas tinggi diselesaikan. Tugas ini mendukung keberhasilan keseluruhan pekerjaan namun tidak kritikal.

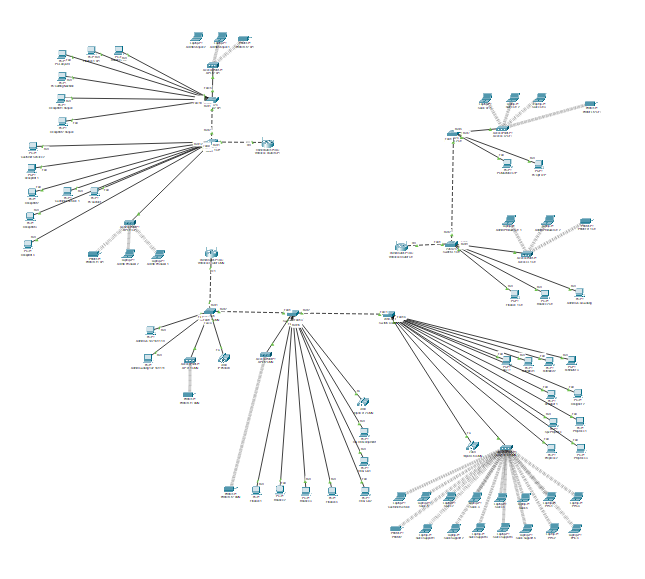
## 

# **BAB IV HASIL PEMBAHASAN**

## **4.1 Analisis Jaringan Eksisting**

Berikut adalah gambaran topologi jaringan saat ini, yang terdiri dari kantor pusat PT. Citra Mandiri Negara (CMN), serta dua kantor cabang, yaitu PT. Citra Print Indonesia (CPI) dan PT. Citra Factory Indonesia (CFI).

1. Bahwa komunikasi antar divisi, spesifiknya antara divisi Prepress & Desainer dengan divisi CTP *(Computer to Plate),* tidak dapat dilakukan. Kondisi ini menyebabkan transfer file harus menggunakan aplikasi pihak ketiga.
2. Setiap kantor cabang dan pusat tidak dapat berkomunikasi.
3. Penyimpanan file masih dilakukan di PC client masing-masing dan juga aplikasi pihak ketiga.

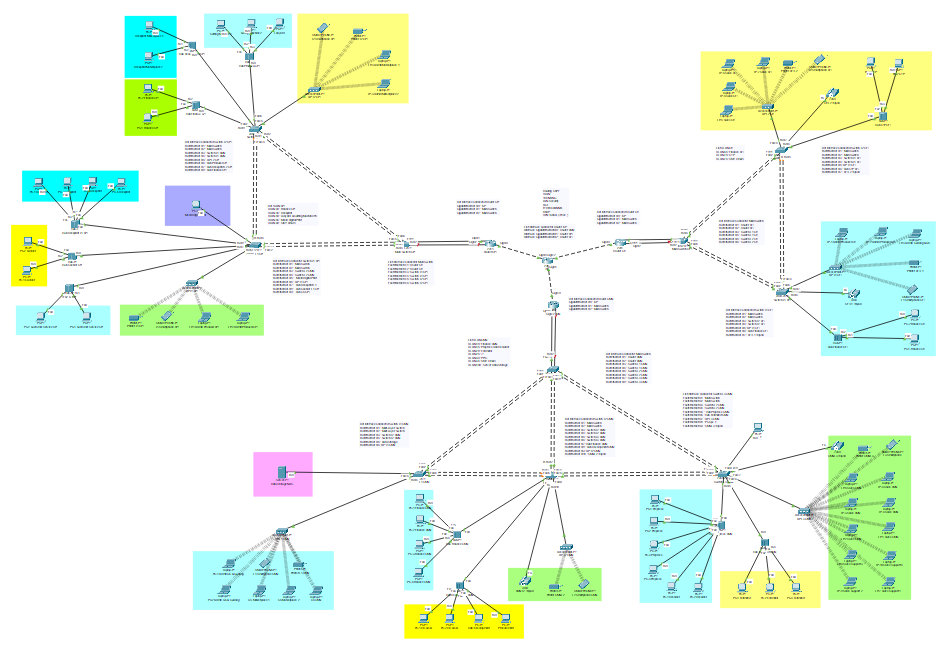


*Gambar Topologi Jaringan Citra Group*

## **4.2 Rekomendasi Desain Topologi**

Berikut adalah gambaran topologi jaringan yang direkomendasikan, yang terdiri dari kantor pusat PT. Citra Mandiri Negara (CMN), serta dua kantor cabang, yaitu PT. Citra Print Indonesia (CPI) sebagai, dan PT. Citra Factory Indonesia (CFI).

Berdasarkan analisis kebutuhan jaringan, direkomendasikan desain topologi berbasis VLAN dan VPN Tunnel untuk mencapai transfering file yang efisien.



*Gambar Rekomendasi Topologi Jaringan*

## **4.3 Konfigurasi VLAN dan Trunking**

Pada tahap ini, dilakukan konfigurasi *Virtual Local Area Network* (VLAN) dan *Trunking* sebagai solusi untuk mengatasi permasalahan segmentasi jaringan yang kurang efisien yang terjadi pada infrastruktur jaringan PT. Citra Mandiri Negara. Implementasi VLAN bertujuan untuk mengelompokkan perangkat-perangkat jaringan secara logis berdasarkan divisi atau fungsi, seperti VLAN Prepress & Desainer dan VLAN CTP. Sementara itu, konfigurasi *Trunking* dengan protokol 802.1Q memastikan efisiensi konektivitas antar-VLAN melalui satu jalur fisik, sehingga mengurangi *traffic* dan meningkatkan kinerja jaringan secara keseluruhan.

*Table 2 Skema Subnetting PT. Citra Mandiri Negara*

| **VLAN ID** | **Nama VLAN** | **Subnet/IP Address** | **Gateway Default** |
| --- | --- | --- | --- |
| 10 | Finance CMN | 192.168.10.0/24 | 192.168.10.1 |
| 15 | Prepress, Desain | 192.168.15.0/24 | 192.168.15.1 |
| 20 | Estimator | 192.168.20.0/24 | 192.168.20.1 |
| 25 | Spv IT | 192.168.25.0/24 | 192.168.25.1 |
| 30 | PPIC | 192.168.30.0/24 | 192.168.30.1 |
| 35 | Staf Umum | 192.168.35.0/24 | 192.168.35.1 |
| 100 | Data Storage | 192.168.100.0/24 | 192.168.100.1 |

*Table 3 Skema Subnetting PT. Citra Print Indonesia*

| **VLAN ID** | **Nama VLAN** | **Subnet/IP Address** | **Gateway Default** |
| --- | --- | --- | --- |
| 40 | Finance CPI | 192.168.40.0/24 | 192.168.40.1 |
| 45 | Deskprint | 192.168.45.0/24 | 192.168.45.1 |
| 50 | *Lanyard & Mesin Cutting* | 192.168.50.0/24 | 192.168.50.1 |
| 55 | Mesin Digital Print | 192.168.55.0/24 | 192.168.55.1 |
| 60 | Staff Umum | 192.168.60.0/24 | 192.168.60.1 |

*Table 4 Skema Subnetting PT. Citra Factory Indonesia*

| **VLAN ID** | **Nama VLAN** | **Subnet/IP Address** | **Gateway Default** |
| --- | --- | --- | --- |
| 65 | Finance CFI | 192.168.65.0/24 | 192.168.65.1 |
| 70 | Mesin CTP | 192.168.70.0/24 | 192.168.70.1 |
| 75 | Staff Umum | 192.168.75.0/24 | 192.168.75.1 |

## **4.4 Implementasi Routing OSPF**

Implementasi protokol *routing Open Shortest Path First* (OSPF) sangat penting dalam perancangan ini untuk memungkinkan komunikasi yang dinamis dan efisien antar-VLAN yang berbeda melalui *router.* OSPF dipilih karena kemampuannya dalam mendistribusikan informasi router yang tergabung dalam suatu *autonomous system* (AS) dan mengoptimalkan pemilihan jalur terbaik berdasarkan perhitungan *Shortest Path First.* Dengan OSPF, jaringan dapat secara otomatis menyesuaikan rute apabila terjadi perubahan topologi, menjamin ketersediaan komunikasi dan efisiensi lalu lintas data di PT. Citra Mandiri Negara.

## **4.5 Penerapan Keamanan LAN**

Untuk memperkuat keamanan jaringan secara keseluruhan, beberapa protokol dan fitur keamanan diimplementasikan:

1. *Access Control List* (ACL)  
   ACL dikonfigurasi pada router dan untuk melakukan packet filtering. ACL memungkinkan administrator jaringan mengontrol paket-paket yang dapat diakses atau melewati perangkat, dengan menentukan apakah paket akan ditolak atau diterima masuk ke sistem. Penerapan ACL ini berfungsi untuk membatasi akses antar-VLAN yang berbeda, misalnya, untuk mencegah akses tidak sah dari VLAN tertentu ke server data yang sensitif, atau memfilter jenis lalu lintas tertentu yang dianggap berisiko.
2. *LAN Security*  
   Selain ACL, fitur keamanan LAN lainnya juga dipertimbangkan dan diimplementasikan untuk meningkatkan proteksi. Ini dapat mencakup *Port Security* pada *switch* untuk mencegah perangkat tidak dikenal terhubung ke jaringan, Implementasi fitur-fitur ini secara kolektif memastikan segmentasi yang efektif dan kontrol akses yang ketat, serta jalur komunikasi data yang aman.
3. VPN Tunnel untuk Koneksi Antar-Site

Dikonfigurasikan untuk mengisolasi lalu lintas antar-site dari jaringan publik, sekaligus memungkinkan komunikasi yang aman antara VLAN yang diizinkan.

## **4.6 Implementasi DHCP dan EtherChannel**

Penyederhanaan manajemen jaringan dan peningkatan performa merupakan manfaat langsung dari implementasi DHCP dan *EtherChannel.* Dengan DHCP, beban administratif yang berkaitan dengan pengelolaan alamat IP secara manual dapat diminimalisir, sehingga sumber daya IT dapat dialokasikan untuk tugas-tugas yang lebih strategis. Di sisi lain, *EtherChannel* berperan penting dalam mengatasi potensi *bottleneck bandwidth* pada jalur-jalur kritis. Penggabungan beberapa jalur fisik menjadi satu jalur logis tidak hanya meningkatkan kapasitas *throughput* tetapi juga menyediakan *mekanisme failover* otomatis, yang secara signifikan meningkatkan ketersediaan dan redundansi jaringan, selaras dengan tujuan efisiensi dan skalabilitas jaringan.

## **4.7 Konfigurasi End Device**

Berikut adalah susunan konfigurasi yang diterapkan disemua perangkat keras jaringan.

1. **ISP**

Router ISP

enable

configure terminal

hostname ISP

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name isp.local

crypto key generate rsa general-keys modulus 2048

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

interface GigabitEthernet0/0

ip address 203.0.113.1 255.255.255.252

no shutdown

exit

interface GigabitEthernet0/1

ip address 198.51.100.1 255.255.255.252

no shutdown

exit

interface GigabitEthernet0/2

ip address 192.0.2.1 255.255.255.252

no shutdown

exit

ip routing

ip route 192.168.0.0 255.255.0.0 203.0.113.2

ip route 192.168.0.0 255.255.0.0 198.51.100.2

ip route 192.168.0.0 255.255.0.0 192.0.2.2

end

write memory

1. **Kantor Pusat ( PT. Citra Mandiri Negara ).**  
   1. Router CMN

enable

configure terminal

hostname Router-CMN

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cmn.local

crypto key generate rsa general-keys modulus 2048

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 101 permit ip 192.168.45.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 101 permit ip 192.168.45.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 101 permit ip 192.168.45.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 101 permit ip 192.168.55.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 101 permit ip 192.168.55.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 101 permit ip 192.168.55.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 deny ip any any

access-list 102 permit ip 192.168.15.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 102 permit ip 192.168.25.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 102 permit ip 192.168.100.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 102 deny ip any any

crypto isakmp policy 10

encr aes 256

hash sha

authentication pre-share

group 5

lifetime 86400

exit

crypto isakmp key CitraNetwork2025 address 172.16.1.1

crypto isakmp key CitraNetwork2025 address 172.16.1.10

crypto ipsec transform-set TS\_CMN esp-aes 256 esp-sha-hmac

crypto map CM\_CMN\_CPI 10 ipsec-isakmp

set peer 172.16.1.1

set transform-set TS\_CMN

match address 101

set pfs group5

exit

crypto map CM\_CMN\_CFI 20 ipsec-isakmp

set peer 172.16.1.10

set transform-set TS\_CMN

match address 102

set pfs group5

exit

interface GigabitEthernet0/0

ip address 198.51.100.2 255.255.255.0

no shutdown

exit

interface GigabitEthernet0/1

ip address 172.16.1.2 255.255.255.252

crypto map CM\_CMN\_CPI

crypto map CM\_CMN\_CFI

no shutdown

exit

interface GigabitEthernet0/2

shutdown

exit

interface GigabitEthernet0/1.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.10.1 192.168.10.10

ip dhcp pool VLAN10

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

exit

interface GigabitEthernet0/1.15

encapsulation dot1Q 15

ip address 192.168.15.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.15.1 192.168.15.10

ip dhcp pool VLAN15

network 192.168.15.0 255.255.255.0

default-router 192.168.15.1

exit

interface GigabitEthernet0/1.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.20.1 192.168.20.10

ip dhcp pool VLAN20

network 192.168.20.0 255.255.255.0

default-router 192.168.20.1

exit

interface GigabitEthernet0/1.25

encapsulation dot1Q 25

ip address 192.168.25.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.25.1 192.168.25.10

ip dhcp pool VLAN25

network 192.168.25.0 255.255.255.0

default-router 192.168.25.1

exit

interface GigabitEthernet0/1.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.30.1 192.168.30.10

ip dhcp pool VLAN30

network 192.168.30.0 255.255.255.0

default-router 192.168.30.1

exit

interface GigabitEthernet0/1.35

encapsulation dot1Q 35

ip address 192.168.35.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.35.1 192.168.35.10

ip dhcp pool VLAN35

network 192.168.35.0 255.255.255.0

default-router 192.168.35.1

exit

interface GigabitEthernet0/1.100

encapsulation dot1Q 100

ip address 192.168.100.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.100.1 192.168.100.10

ip dhcp pool VLAN100

network 192.168.100.0 255.255.255.0

default-router 192.168.100.1

exit

ip route 0.0.0.0 0.0.0.0 198.51.100.1

router ospf 1

router-id 5.5.5.5

network 172.16.0.4 0.0.0.3 area 0

network 192.168.15.0 0.0.0.255 area 0

network 192.168.25.0 0.0.0.255 area 0

network 192.168.100.0 0.0.0.255 area 0

exit

access-list 100 permit udp any eq 68 any eq 67

access-list 100 permit udp any eq 67 any eq 68

access-list 100 deny ip 192.168.10.0 0.0.0.255 any

access-list 100 deny ip 192.168.20.0 0.0.0.255 any

access-list 100 deny ip 192.168.30.0 0.0.0.255 any

access-list 100 deny ip 192.168.35.0 0.0.0.255 any

access-list 100 deny ip any 192.168.10.0 0.0.0.255

access-list 100 deny ip any 192.168.20.0 0.0.0.255

access-list 100 deny ip any 192.168.30.0 0.0.0.255

access-list 100 deny ip any 192.168.35.0 0.0.0.255

access-list 100 permit ip any any

end

write memory

2. Main Switch CMN

enable

configure terminal

hostname SW-MAIN-CMN

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cmn.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 10

name Finance

exit

vlan 15

name Prepress

exit

vlan 20

name Estimator

exit

vlan 25

name Spv\_IT

exit

vlan 30

name PPIC

exit

vlan 35

name Staff\_Umum

exit

vlan 100

name Data\_Storage

exit

interface FastEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface FastEthernet0/2

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

shutdown

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/3-4

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/5-6

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface Port-channel3

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/7-8

channel-group 3 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface range FastEthernet0/9-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,10,15,20,25,30,35,100 priority 4096

end

write memory

3. Switch Lantai CMN ( SW-L1-CMN )

enable

configure terminal

hostname SW-L1-CMN

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cmn.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 10

name Finance

exit

vlan 15

name Prepress

exit

vlan 20

name Estimator

exit

vlan 25

name Spv\_IT

exit

vlan 30

name PPIC

exit

vlan 35

name Staff\_Umum

exit

vlan 100

name Data\_Storage

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/3-4

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface FastEthernet0/5

switchport mode access

switchport access vlan 100

switchport port-security maximum 1

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/6

switchport mode access

switchport access vlan 35

switchport port-security maximum 20

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface range FastEthernet0/7-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,10,15,20,25,30,35,100 priority 8192

end

write memory

4. Switch Lantai 2 CMN ( SW-L2-CMN )

enable

configure terminal

hostname SW-L2-CMN

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cmn.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 10

name Finance

exit

vlan 15

name Prepress

exit

vlan 20

name Estimator

exit

vlan 25

name Spv\_IT

exit

vlan 30

name PPIC

exit

vlan 35

name Staff\_Umum

exit

vlan 100

name Data\_Storage

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/3-4

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface Port-channel3

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/5-6

channel-group 3 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface FastEthernet0/7

switchport mode access

switchport access vlan 10

switchport port-security maximum 4

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/8

switchport mode access

switchport access vlan 35

switchport port-security maximum 4

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/9

switchport mode access

switchport access vlan 35

switchport port-security maximum 20

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/10

switchport mode access

switchport access vlan 35

switchport port-security maximum 1

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface range FastEthernet0/11-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,10,15,20,25,30,35,100 priority 12288

end

write memory

4. Switch Lantai 3 CMN ( SW-L3-CMN )

enable

configure terminal

hostname SW-L3-CMN

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cmn.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 10

name Finance

exit

vlan 15

name Prepress

exit

vlan 20

name Estimator

exit

vlan 25

name Spv\_IT

exit

vlan 30

name PPIC

exit

vlan 35

name Staff\_Umum

exit

vlan 100

name Data\_Storage

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100,200

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

exit

interface range FastEthernet0/3-4

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 10,15,20,25,30,35,100

no shutdown

exit

interface FastEthernet0/5

switchport mode access

switchport access vlan 15

switchport port-security maximum 6

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/6

switchport mode access

switchport access vlan 20

switchport port-security maximum 3

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/7

switchport mode access

switchport access vlan 35

switchport port-security maximum 20

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/8

switchport mode access

switchport access vlan 25

switchport port-security maximum 1

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/9

switchport mode access

switchport access vlan 35

switchport port-security maximum 1

switchport port-security

switchport port-security violation shutdown

no shutdown

exit

interface range FastEthernet0/10-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,10,15,20,25,30,35,100,200 priority 16384

end

write memory

1. **Kantor Cabang ( PT. Citra Print Indonesia ) Area 1.**  
   1. Router CPI

enable

configure terminal

hostname Router-CPI

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cpi.local

crypto key generate rsa general-keys modulus 2048

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

access-list 101 permit ip 192.168.45.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 101 permit ip 192.168.45.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 101 permit ip 192.168.45.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 101 permit ip 192.168.55.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 101 permit ip 192.168.55.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 101 permit ip 192.168.55.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 101 deny ip any any

access-list 102 permit ip 192.168.45.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 102 permit ip 192.168.50.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 102 permit ip 192.168.55.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 102 deny ip any any

crypto isakmp policy 10

encr aes 256

hash sha

authentication pre-share

group 5

lifetime 86400

exit

crypto isakmp key CitraNetwork2025 address 172.16.1.2

crypto isakmp key CitraNetwork2025 address 172.16.1.6

crypto ipsec transform-set TS\_CPI esp-aes 256 esp-sha-hmac

crypto map CM\_CPI\_CMN 10 ipsec-isakmp

set peer 172.16.1.2

set transform-set TS\_CPI

match address 101

set pfs group5

exit

crypto map CM\_CPI\_CFI 20 ipsec-isakmp

set peer 172.16.1.6

set transform-set TS\_CPI

match address 102

set pfs group5

exit

interface GigabitEthernet0/0

ip address 203.0.113.2 255.255.255.0

no shutdown

exit

interface GigabitEthernet0/1

ip address 172.16.1.6 255.255.255.252

crypto map CM\_CFI\_CPI

crypto map CM\_CFI\_CMN

no shutdown

exit

interface GigabitEthernet0/2

shutdown

exit

interface GigabitEthernet0/1.40

encapsulation dot1Q 40

ip address 192.168.40.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.40.1 192.168.40.10

ip dhcp pool VLAN40

network 192.168.40.0 255.255.255.0

default-router 192.168.40.1

exit

interface GigabitEthernet0/1.45

encapsulation dot1Q 45

ip address 192.168.45.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.45.1 192.168.45.10

ip dhcp pool VLAN45

network 192.168.45.0 255.255.255.0

default-router 192.168.45.1

exit

interface GigabitEthernet0/1.50

encapsulation dot1Q 50

ip address 192.168.50.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.50.1 192.168.50.10

ip dhcp pool VLAN50

network 192.168.50.0 255.255.255.0

default-router 192.168.50.1

exit

interface GigabitEthernet0/1.55

encapsulation dot1Q 55

ip address 192.168.55.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.55.1 192.168.55.10

ip dhcp pool VLAN55

network 192.168.55.0 255.255.255.0

default-router 192.168.55.1

exit

interface GigabitEthernet0/1.60

encapsulation dot1Q 60

ip address 192.168.60.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.60.1 192.168.60.10

ip dhcp pool VLAN60

network 192.168.60.0 255.255.255.0

default-router 192.168.60.1

exit

ip route 0.0.0.0 0.0.0.0 203.0.113.1

router ospf 1

router-id 4.4.4.4

network 172.16.0.0 0.0.0.3 area 0

network 192.168.45.0 0.0.0.255 area 0

network 192.168.50.0 0.0.0.255 area 0

network 192.168.55.0 0.0.0.255 area 0

exit

access-list 100 permit udp any eq 68 any eq 67

access-list 100 permit udp any eq 67 any eq 68

access-list 100 deny ip 192.168.40.0 0.0.0.255 any

access-list 100 deny ip any 192.168.40.0 0.0.0.255

access-list 100 deny ip 192.168.60.0 0.0.0.255 any

access-list 100 deny ip any 192.168.60.0 0.0.0.255

access-list 100 deny ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255

access-list 100 deny ip 192.168.60.0 0.0.0.255 192.168.40.0 0.0.0.255

access-list 100 permit ip any any

end

write memory

2. Switch Utama CPI ( SW-MAIN-CPI )

enable

configure terminal

hostname SW-MAIN-CPI

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cpi.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 40

name Finance\_cpi

exit

vlan 45

name Deskprint

exit

vlan 50

name Cutting\_lanyard

exit

vlan 55

name Mesin\_Digital

exit

vlan 60

name Staff\_umum

exit

interface FastEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface FastEthernet0/2

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

shutdown

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

exit

interface range FastEthernet0/3-4

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

exit

interface range FastEthernet0/5-6

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface range FastEthernet0/7-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,40,45,50,55,60 priority 4096

end

write memory

3. Switch Lantai 1 CPI ( SW-L1-CPI )

enable

configure terminal

hostname SW-L1-CPI

! Banner MOTD

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cpi.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 40

name Finance\_cpi

exit

vlan 45

name Deskprint

exit

vlan 50

name Cutting\_lanyard

exit

vlan 55

name Mesin\_Digital

exit

vlan 60

name Staff\_umum

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

exit

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

exit

interface range FastEthernet0/3-4

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface FastEthernet0/5

switchport mode access

switchport access vlan 55

switchport port-security

switchport port-security maximum 1

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/6

switchport mode access

switchport access vlan 60

switchport port-security

switchport port-security maximum 20

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/7

switchport mode access

switchport access vlan 45

switchport port-security

switchport port-security maximum 4

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/8

switchport mode access

switchport access vlan 40

switchport port-security

switchport port-security maximum 2

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/9

switchport mode access

switchport access vlan 60

switchport port-security

switchport port-security maximum 4

switchport port-security violation shutdown

no shutdown

exit

interface range FastEthernet0/10-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,40,45,50,55,60 priority 8192

end

write memory

4. Switch Lantai 2 CPI ( SW-L2-CPI )

enable

configure terminal

hostname SW-L2-CPI

! Banner MOTD

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cpi.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 40

name Finance\_cpi

exit

vlan 45

name Deskprint

exit

vlan 50

name Cutting\_lanyard

exit

vlan 55

name Mesin\_Digital

exit

vlan 60

name Staff\_umum

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

exit

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

exit

interface range FastEthernet0/3-4

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 40,45,50,55,60

no shutdown

exit

interface FastEthernet0/5

switchport mode access

switchport access vlan 60

switchport port-security

switchport port-security maximum 20

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/6

switchport mode access

switchport access vlan 50

switchport port-security

switchport port-security maximum 3

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/7

switchport mode access

switchport access vlan 45

switchport port-security

switchport port-security maximum 2

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/8

switchport mode access

switchport access vlan 40

switchport port-security

switchport port-security maximum 2

switchport port-security violation shutdown

no shutdown

exit

interface range FastEthernet0/9-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,40,45,50,55,60 priority 12288

end

write memory

1. **Kantor Cabang ( PT. Citra Factory Indonesia ) Area 2.**  
   1. Router CFI

enable

configure terminal

hostname Router-CFI

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cfi.local

crypto key generate rsa general-keys modulus 2048

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.15.0 0.0.0.255

access-list 101 permit ip 192.168.15.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.25.0 0.0.0.255

access-list 101 permit ip 192.168.25.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.100.0 0.0.0.255

access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 101 deny ip any any

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.45.0 0.0.0.255

access-list 102 permit ip 192.168.45.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.50.0 0.0.0.255

access-list 102 permit ip 192.168.50.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.55.0 0.0.0.255

access-list 102 permit ip 192.168.55.0 0.0.0.255 192.168.70.0 0.0.0.255

access-list 102 deny ip any any

crypto isakmp policy 10

encr aes 256

hash sha

authentication pre-share

group 5

lifetime 86400

exit

crypto isakmp key CitraNetwork2025 address 172.16.1.1

crypto isakmp key CitraNetwork2025 address 172.16.1.10

crypto ipsec transform-set TS\_CFI esp-aes 256 esp-sha-hmac

crypto map CM\_CFI\_CPI 10 ipsec-isakmp

set peer 172.16.1.1

set transform-set TS\_CFI

match address 102

set pfs group5

exit

crypto map CM\_CFI\_CMN 20 ipsec-isakmp

set peer 172.16.1.10

set transform-set TS\_CFI

match address 101

set pfs group5

exit

interface GigabitEthernet0/0

ip address 192.0.2.2 255.255.255.0

no shutdown

exit

interface GigabitEthernet0/1

ip address 172.16.1.6 255.255.255.252

crypto map CM\_CFI\_CPI

crypto map CM\_CFI\_CMN

no shutdown

exit

interface GigabitEthernet0/2

shutdown

exit

interface GigabitEthernet0/1.65

encapsulation dot1Q 65

ip address 192.168.65.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.65.1 192.168.65.10

ip dhcp pool VLAN65

network 192.168.65.0 255.255.255.0

default-router 192.168.65.1

exit

interface GigabitEthernet0/1.70

encapsulation dot1Q 70

ip address 192.168.70.1 255.255.255.0

no shutdown

exit

ip dhcp excluded-address 192.168.70.1 192.168.70.10

ip dhcp pool VLAN70

network 192.168.70.0 255.255.255.0

default-router 192.168.70.1

exit

interface GigabitEthernet0/1.75

encapsulation dot1Q 75

ip address 192.168.75.1 255.255.255.0

ip access-group 100 in

no shutdown

exit

ip dhcp excluded-address 192.168.75.1 192.168.75.10

ip dhcp pool VLAN75

network 192.168.75.0 255.255.255.0

default-router 192.168.75.1

exit

ip route 0.0.0.0 0.0.0.0 192.0.2.1

router ospf 1

router-id 6.6.6.6

network 172.16.0.8 0.0.0.3 area 0

network 192.168.70.0 0.0.0.255 area 0

exit

access-list 100 permit udp any eq 68 any eq 67

access-list 100 permit udp any eq 67 any eq 68

access-list 100 deny ip 192.168.65.0 0.0.0.255 any

access-list 100 deny ip any 192.168.65.0 0.0.0.255

access-list 100 deny ip 192.168.75.0 0.0.0.255 any

access-list 100 deny ip any 192.168.75.0 0.0.0.255

access-list 100 deny ip 192.168.65.0 0.0.0.255 192.168.75.0 0.0.0.255

access-list 100 deny ip 192.168.75.0 0.0.0.255 192.168.65.0 0.0.0.255

access-list 100 permit ip any any

end

write memory

2. Switch Utama CFI ( SW-MAIN-CFI )

enable

configure terminal

hostname SW-MAIN-CFI

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cfi.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 65

name Finance\_cfi

exit

vlan 70

name Mesin\_ctp

exit

vlan 75

name Staff\_umum

exit

interface FastEthernet0/1

switchport mode trunk

switchport trunk allowed vlan 65,70,75

no shutdown

exit

interface FastEthernet0/2

switchport mode trunk

switchport trunk allowed vlan 65,70,75

shutdown

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 65,70,75

exit

interface range FastEthernet0/3-4

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 65,70,75

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 65,70,75

exit

interface range FastEthernet0/5-6

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 65,70,75

no shutdown

exit

interface range FastEthernet0/7-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,65,70,75 priority 4096

end

write memory

3. Switch Lantai 2 CFI ( SW-L2-CFI )  
enable

configure terminal

hostname SW-L2-CFI

banner motd #

Designed and Configured by

411221012 - Kenedi Peres

#

enable secret nitesane98

service password-encryption

username admin secret nitesane98

ip domain-name cfi.local

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

line console 0

password nitesane98

login

exit

line vty 0 15

transport input ssh

login local

exit

vlan 65

name Finance\_cfi

exit

vlan 70

name Mesin\_ctp

exit

vlan 75

name Staff\_umum

exit

interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 65,70,75

exit

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 65,70,75

no shutdown

exit

interface Port-channel2

switchport mode trunk

switchport trunk allowed vlan 65,70,75

exit

interface range FastEthernet0/3-4

channel-group 2 mode active

switchport mode trunk

switchport trunk allowed vlan 65,70,75

no shutdown

exit

interface FastEthernet0/5

switchport mode access

switchport access vlan 75

switchport port-security

switchport port-security maximum 20

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/6

switchport mode access

switchport access vlan 70

switchport port-security

switchport port-security maximum 2

switchport port-security violation shutdown

no shutdown

exit

interface FastEthernet0/7

switchport mode access

switchport access vlan 75

switchport port-security

switchport port-security maximum 1

switchport port-security violation shutdown

no shutdown

exit

interface range FastEthernet0/8-24

shutdown

exit

interface range GigabitEthernet0/1-2

shutdown

exit

spanning-tree mode rapid-pvst

spanning-tree vlan 1,65,70,75 priority 12288

end

write memory

## **4.7 Hasil Pengujian Simulasi Jaringan**

Berikut adalah gambaran topologi jaringan saat ini, yang terdiri dari kantor pusat PT. Citra Mandiri Negara (CMN), serta dua kantor cabang, yaitu PT. Citra Print Indonesia (CPI) dan PT. Citra Factory Indonesia (CFI). Adapun Skenario-nya adalah sebagai berikut :

1. VLAN 15 bisa berkomunikasi dengan VLAN 45, VLAN 50, VLAN 55, VLAN 70 dan VLAN 100 dalam area jaringan WAN.

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.45.11*

*Pinging 192.168.45.11 with 32 bytes of data:*

*Reply from 192.168.45.11: bytes=32 time=18ms TTL=126*

*Reply from 192.168.45.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.45.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.45.11: bytes=32 time=12ms TTL=126*

*Ping statistics for 192.168.45.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 1ms, Maximum = 18ms, Average = 8ms*

*C:\>ping 192.168.50.11*

*Pinging 192.168.50.11 with 32 bytes of data:*

*Reply from 192.168.50.11: bytes=32 time=3ms TTL=126*

*Reply from 192.168.50.11: bytes=32 time=2ms TTL=126*

*Reply from 192.168.50.11: bytes=32 time=3ms TTL=126*

*Reply from 192.168.50.11: bytes=32 time=2ms TTL=126*

*Ping statistics for 192.168.50.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 2ms, Maximum = 3ms, Average = 2ms*

*C:\>ping 192.168.55.11*

*Pinging 192.168.55.11 with 32 bytes of data:*

*Reply from 192.168.55.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.55.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.55.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.55.11: bytes=32 time=1ms TTL=126*

*Ping statistics for 192.168.55.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 1ms, Maximum = 1ms, Average = 1ms*

*C:\>ping 192.168.70.11*

*Pinging 192.168.70.11 with 32 bytes of data:*

*Reply from 192.168.70.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.70.11: bytes=32 time=12ms TTL=126*

*Reply from 192.168.70.11: bytes=32 time=10ms TTL=126*

*Reply from192.168.70.11: bytes=32 time=22ms TTL=126*

*Ping statistics for 192.168.70.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 1ms, Maximum = 22ms, Average = 11ms*

*C:\>ping 192.168.100.11*

*Pinging 192.168.100.11 with 32 bytes of data:*

*Reply from 192.168.100.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.100.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.100.11: bytes=32 time=10ms TTL=127*

*Reply from 192.168.100.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.100.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 10ms, Average = 2ms*

*C:\>*

1. Dalam area LAN CPI, VLAN 45 dapat berkomunikasi dengan VLAN 50, dan juga VLAN 55.
2. VLAN 40

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.45.11*

*Pinging 192.168.45.11 with 32 bytes of data:*

*Reply from 192.168.45.11: Destination host unreachable.*

*Reply from 192.168.45.11: Destination host unreachable.*

*Reply from 192.168.45.11: Destination host unreachable.*

*Reply from 192.168.45.11: Destination host unreachable.*

*Ping statistics for 192.168.45.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.50.11*

*Pinging 192.168.50.11 with 32 bytes of data:*

*Request timed out.*

*Reply from 192.168.50.11: Destination host unreachable.*

*Reply from 192.168.50.11: Destination host unreachable.*

*Reply from 192.168.50.11: Destination host unreachable.*

*Ping statistics for 192.168.50.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.55.11*

*Pinging 192.168.55.11 with 32 bytes of data:*

*Reply from 192.168.55.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Ping statistics for 192.168.55.11:*

*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: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Ping statistics for 192.168.60.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>*

1. VLAN 45

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.40.11*

*Pinging 192.168.40.11 with 32 bytes of data:*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Ping statistics for 192.168.40.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.50.11*

*Pinging 192.168.50.11 with 32 bytes of data:*

*Request timed out.*

*Reply from 192.168.50.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.50.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.50.11: bytes=32 time=2ms TTL=127*

*Ping statistics for 192.168.50.11:*

*Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 2ms, Average = 0ms*

*C:\>ping 192.168.55.11*

*Pinging 192.168.55.11 with 32 bytes of data:*

*Reply from 192.168.55.11: bytes=32 time=1ms TTL=127*

*Reply from 192.168.55.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.55.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.55.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.55.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 1ms, Average = 0ms*

*C:\>ping 192.168.60.11*

*Pinging 192.168.60.11 with 32 bytes of data:*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Ping statistics for 192.168.60.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.70.11*

*Pinging 192.168.70.11 with 32 bytes of data:*

*Request timed out.*

*Reply from 192.168.70.11: bytes=32 time=4ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=25ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=2ms TTL=125*

*Ping statistics for 192.168.70.11:*

*Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 2ms, Maximum = 25ms, Average = 10ms*

*C:\>ping 192.168.100.11*

*Pinging 192.168.100.11 with 32 bytes of data:*

*Request timed out.*

*Reply from 192.168.100.11: bytes=32 time=3ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=2ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=3ms TTL=126*

*Ping statistics for 192.168.100.11:*

*Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 2ms, Maximum = 3ms, Average = 2ms*

*C:\>*

1. VLAN 50

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.40.11*

*Pinging 192.168.40.11 with 32 bytes of data:*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Ping statistics for 192.168.40.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.45.11*

*Pinging 192.168.45.11 with 32 bytes of data:*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.45.11: bytes=32 time=4ms TTL=127*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.45.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 4ms, Average = 1ms*

*C:\>ping 192.168.55.11*

*Pinging 192.168.55.11 with 32 bytes of data:*

*Reply from 192.168.55.11: bytes=32 time=1ms TTL=127*

*Reply from 192.168.55.11: bytes=32 time=12ms TTL=127*

*Reply from 192.168.55.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.55.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.55.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 12ms, Average = 3ms*

*C:\>ping 192.168.60.11*

*Pinging 192.168.60.11 with 32 bytes of data:*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Ping statistics for 192.168.60.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.70.11*

*Pinging 192.168.70.11 with 32 bytes of data:*

*Reply from 192.168.70.11: bytes=32 time=4ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=5ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=4ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=3ms TTL=125*

*Ping statistics for 192.168.70.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 3ms, Maximum = 5ms, Average = 4ms*

*C:\>ping 192.168.100.11*

*Pinging 192.168.100.11 with 32 bytes of data:*

*Reply from 192.168.100.11: bytes=32 time=10ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=10ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=1ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=1ms TTL=126*

*Ping statistics for 192.168.100.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 1ms, Maximum = 10ms, Average = 5ms*

*C:\>ping 192.168.15.11*

*Pinging 192.168.15.11 with 32 bytes of data:*

*Reply from 192.168.15.11: bytes=32 time=11ms TTL=126*

*Reply from 192.168.15.11: bytes=32 time=10ms TTL=126*

*Reply from 192.168.15.11: bytes=32 time=8ms TTL=126*

*Reply from 192.168.15.11: bytes=32 time=9ms TTL=126*

*Ping statistics for 192.168.15.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 8ms, Maximum = 11ms, Average = 9ms*

*C:\>*

1. VLAN 55

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.40.11*

*Pinging 192.168.40.11 with 32 bytes of data:*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Ping statistics for 192.168.40.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.45.11*

*Pinging 192.168.45.11 with 32 bytes of data:*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.45.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.45.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 0ms, Average = 0ms*

*C:\>ping 192.168.50.11*

*Pinging 192.168.50.11 with 32 bytes of data:*

*Reply from 192.168.50.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.50.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.50.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.50.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.50.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 0ms, Average = 0ms*

*C:\>ping 192.168.60.11*

*Pinging 192.168.60.11 with 32 bytes of data:*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Reply from 192.168.60.11: Destination host unreachable.*

*Ping statistics for 192.168.60.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.70.11*

*Pinging 192.168.70.11 with 32 bytes of data:*

*Reply from 192.168.70.11: bytes=32 time=15ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=5ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=17ms TTL=125*

*Reply from 192.168.70.11: bytes=32 time=4ms TTL=125*

*Ping statistics for 192.168.70.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 4ms, Maximum = 17ms, Average = 10ms*

*C:\>ping 192.168.100.11*

*Pinging 192.168.100.11 with 32 bytes of data:*

*Reply from 192.168.100.11: bytes=32 time=2ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=19ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=2ms TTL=126*

*Reply from 192.168.100.11: bytes=32 time=21ms TTL=126*

*Ping statistics for 192.168.100.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 2ms, Maximum = 21ms, Average = 11ms*

*C:\>ping 192.168.15.11*

*Pinging 192.168.15.11 with 32 bytes of data:*

*Reply from 192.168.15.11: bytes=32 time=11ms TTL=126*

*Reply from 192.168.15.11: bytes=32 time=26ms TTL=126*

*Reply from 192.168.15.11: bytes=32 time=9ms TTL=126*

*Reply from 192.168.15.11: bytes=32 time=15ms TTL=126*

*Ping statistics for 192.168.15.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 9ms, Maximum = 26ms, Average = 15ms*

*C:\>*

1. VLAN 60

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.40.11*

*Pinging 192.168.40.11 with 32 bytes of data:*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Reply from 192.168.40.11: Destination host unreachable.*

*Ping statistics for 192.168.40.2:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.45.11*

*Pinging 192.168.45.11 with 32 bytes of data:*

*Reply from 192.168.45.11: Destination host unreachable.*

*Reply from 192.168.45.11: Destination host unreachable.*

*Reply from 192.168.45.11: Destination host unreachable.*

*Reply from 192.168.45.11: Destination host unreachable.*

*Ping statistics for 192.168.45.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.50.11*

*Pinging 192.168.50.11 with 32 bytes of data:*

*Reply from 192.168.50.11: Destination host unreachable.*

*Reply from 192.168.50.11: Destination host unreachable.*

*Reply from 192.168.50.11: Destination host unreachable.*

*Reply from 192.168.50.11: Destination host unreachable.*

*Ping statistics for 192.168.50.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.55.11*

*Pinging 192.168.55.11 with 32 bytes of data:*

*Reply from 192.168.55.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Reply from 192.168.55.11: Destination host unreachable.*

*Ping statistics for 192.168.55.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.100.11*

*Pinging 192.168.100.11 with 32 bytes of data:*

*Reply from 192.168.100.11: Destination host unreachable.*

*Reply from 192.168.100.11: Destination host unreachable.*

*Reply from 192.168.100.11: Destination host unreachable.*

*Reply from 192.168.100.11: Destination host unreachable.*

*Ping statistics for 192.168.100.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.70.11*

*Pinging 192.168.70.11 with 32 bytes of data:*

*Reply from 192.168.70.11: Destination host unreachable.*

*Reply from 192.168.70.11: Destination host unreachable.*

*Reply from 192.168.70.11: Destination host unreachable.*

*Reply from 192.168.70.11: Destination host unreachable.*

*Ping statistics for 192.168.70.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>*

1. Dalam area LAN CMN, Semua VLAN terisolasi, akan tetapi VLAN 15, dapat berkomunikasi dengan VLAN 100, hasil outputnya sebagai berikut.

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.10.11*

*Pinging 192.168.10.11 with 32 bytes of data:*

*Reply from 192.168.10.11: Destination host unreachable.*

*Reply from 192.168.10.11: Destination host unreachable.*

*Reply from 192.168.10.11: Destination host unreachable.*

*Reply from 192.168.10.11: Destination host unreachable.*

*Ping statistics for 192.168.10.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.20.11*

*Pinging 192.168.25.11 with 32 bytes of data:*

*Reply from 192.168.25.11: Destination host unreachable.*

*Reply from 192.168.25.11: Destination host unreachable.*

*Reply from 192.168.25.11: Destination host unreachable.*

*Reply from 192.168.25.11: Destination host unreachable.*

*Ping statistics for 192.168.25.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.25.11*

*Pinging 192.168.25.11 with 32 bytes of data:*

*Reply from 192.168.25.11: Destination host unreachable.*

*Reply from 192.168.25.11: Destination host unreachable.*

*Reply from 192.168.25.11: Destination host unreachable.*

*Reply from 192.168.25.11: Destination host unreachable.*

*Ping statistics for 192.168.25.2:*

*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: Destination host unreachable.*

*Reply from 192.168.30.11: Destination host unreachable.*

*Reply from 192.168.30.11: Destination host unreachable.*

*Reply from 192.168.30.11: Destination host unreachable.*

*Ping statistics for 192.168.30.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.35.11*

*Pinging 192.168.35.11 with 32 bytes of data:*

*Reply from 192.168.35.11: Destination host unreachable.*

*Reply from 192.168.35.11: Destination host unreachable.*

*Reply from 192.168.35.11: Destination host unreachable.*

*Reply from 192.168.35.11: Destination host unreachable.*

*Ping statistics for 192.168.35.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.100.11*

*Pinging 192.168.100.11 with 32 bytes of data:*

*Reply from 192.168.100.11: bytes=32 time=1ms TTL=127*

*Reply from 192.168.100.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.100.11: bytes=32 time<1ms TTL=127*

*Reply from 192.168.100.11: bytes=32 time<1ms TTL=127*

*Ping statistics for 192.168.100.11:*

*Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 0ms, Maximum = 1ms, Average = 0ms*

*C:\>*

1. Dalam area LAN CFI, Semua VLAN terisolasi.  
   Hasil output sebagai berikut.

*Cisco Packet Tracer PC Command Line 1.0*

*C:\>ping 192.168.65.11*

*Pinging 192.168.65.11 with 32 bytes of data:*

*Reply from 192.168.65.11: Destination host unreachable.*

*Reply from 192.168.65.11: Destination host unreachable.*

*Reply from 192.168.65.11: Destination host unreachable.*

*Reply from 192.168.65.11: Destination host unreachable.*

*Ping statistics for 192.168.65.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>ping 192.168.75.11*

*Pinging 192.168.75.11 with 32 bytes of data:*

*Reply from 192.168.75.11: Destination host unreachable.*

*Reply from 192.168.75.11: Destination host unreachable.*

*Reply from 192.168.75.11: Destination host unreachable.*

*Reply from 192.168.75.11: Destination host unreachable.*

*Ping statistics for 192.168.75.11:*

*Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

*C:\>*

# **BAB V PENUTUP**

## **5.1 Kesimpulan**

Berdasarkan hasil analisis, perancangan, serta implementasi sistem jaringan berbasis VLAN, trunking, OSPF, dan VPN Tunnel di PT. Citra Mandiri Negara, dapat disimpulkan bahwa solusi yang diterapkan mampu meningkatkan efisiensi, keamanan, serta skalabilitas jaringan antar kantor pusat dan cabang. Segmentasi VLAN berhasil mengisolasi lalu lintas berdasarkan fungsi divisi, protokol OSPF memastikan komunikasi dinamis antar subnet, dan konfigurasi IPsec VPN mendukung koneksi aman antar lokasi. Selain itu, penerapan ACL, DHCP, dan EtherChannel semakin memperkuat manajemen akses, pengalamatan otomatis, serta performa jaringan secara keseluruhan.

Hasil pengujian simulasi dihalaman. 59–74 membuktikan keberhasilan komunikasi antar VLAN,

1. VLAN 15 dapat mengakses VLAN 45, 50, 55, 70, dan 100
2. Mengisolasi VLAN tertentu, seperti VLAN 40 dan VLAN 60.

## **5.2 Saran**

Berdasarkan hasil penelitian dan implementasi jaringan yang telah dilakukan, berikut beberapa saran untuk pengembangan Infrastruktur Jaringan.

1. Peningkatan Infrastruktur Jaringan

Penambahan perangkat jaringan seperti switch dan router untuk mendukung skalabilitas dan redundansi, terutama jika perusahaan melakukan ekspansi ke cabang baru.

1. Pengembangan Penyimpanan Terpusat

Implementasi *Network-Attached Storage* (NAS) untuk mengoptimalkan manajemen data, terutama untuk file berukuran besar yang sering dipertukarkan antar divisi.

# **DAFTAR PUSTAKA**

Pasaribu, F. I. (2021). Analisa kontrol pengamanan mikrotik router pada jaringan komputer

dan PC cloning. *Jurnal Elektro dan Telekomunikasi,* 5(2), 9–19.

Suryantoro, H., Sopian, A., & Dartono. (2021). Penerapan teknologi Fortigate dalam

pembangunan jaringan VPN-IP berbasis IPSEC. *Jurnal Elektro dan Informatika*

*Swadharma,* 1(1), 21–25.

Pradana, D. A., & Budiman, A. S. (2021). The DHCP snooping and DHCP alert method in

securing DHCP server from DHCP rogue attack. *IJID (International Journal of*

*Informatics Development),* 10(1), 38–46. <https://doi.org/10.14421/ijid.2021.2287>

Laksono, A. T., & Nasution, M. A. H. (2020). Implementasi keamanan jaringan komputer

Local Area Network menggunakan Access Control List pada Perusahaan X. *Jurnal*

*Sistem Komputer dan Informatika (JSON),* 1(2), 83.

<https://doi.org/10.30865/json.v1i2.1920>

Manafe, R. E., Belutowe, Y. S., & Katemba, P. (2022). Perancangan jaringan Virtual Local

Area Network (VLAN) untuk menunjang transaksi data antar jaringan. *Jurnal*

*Teknologi Informasi,* 6(1), 102-111.

Noviriandini, A., Bachtiar, D., & Indriyani, L. (2023). Perancangan jaringan Virtual Local

Area Network menggunakan Cisco Packet Tracer pada SMK Islam Assa'adatul

Abadiyah. *JUKI: Jurnal Komputer dan Informatika,* 5(2), 255-260.

Rahman, T., Zaini, T. R., & Chrisnawati, G. (2020). Perancangan jaringan Virtual Local Area

Network (VLAN) & DHCP pada PT. Navicom Indonesia Bekasi. *JIKA (Jurnal*

*Informatika),* 4(1), 36-41.

C. C. Wijaya and A. S. Budiman,“Perancangan Keamanan Jaringan Komputer Pada Router

Dengan Metode ACL Pada PT. Aruna Sinar Jaya Jakarta,” *J. Zetroem,* vol. 5, no. 2,

pp. 180–186, 2023, doi: 10.36526/ztr.v5i2.3077.

A. T. Laksono and M. A. H. Nasution, “Implementasi Keamanan Jaringan Komputer Local

Area Network Menggunakan Access Control List pada Perusahaan X,” *J. Sist.*

*Komput. dan Inform.,* vol. 1, no. 2, p. 83, 2020, doi: 10.30865/json.v1i2.1920.

Amar, M. R., Anwar, S., & Nurdiawan, O. (2022). Optimalisasi menggunakan access control

list berbasis mikrotik pada Amami Event Organizer. *MEANS (Media Informasi*

*Analisis dan Sistem),* 7(1), 117–123. <https://doi.org/10.54367/means.v7i1.1800>

Essah, R., Atta Senior, I. A., & Anand, D. (2021). Assessing the Performance Analysis of

OSPFV3 and EIGRP in Applications in IPV6 Analysis for Articles Published in

Scopus between 2016 and 2021. *Asian Journal of Research in Computer Science,*

12(2), 40–56. <https://doi.org/10.9734/ajrcos/2021/v12i230280>

Amal, I., Fiade, A., Nanang, H., & Arini. (2022). Performance measurement of first hop

redundancy protocol with Etherchannel for file transfer services. *2022 10th*

*International Conference on Cyber and IT Service Management (CITSM 2022),* 1–7.

<https://doi.org/10.1109/CITSM56380.2022.9935955>

Cisco. (2022b). Understand and Use the Enhanced Interior Gateway Routing Protocol. *Cisco*

*Systems, Inc.*

[https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-pro](https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html)

[tocol-eigrp/16406-eigrp-toc.html](https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html)

Cisco. (2022c). Understand Open Shortest Path First (OSPF) - *Design Guide. Cisco Systems, Inc.*

Cisco. (2022d). *Understand the Hot Standby Router Protocol Features and Functionality.*

Cisco Systems, Inc.

[https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234](https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html)

[-hsrpguidetoc.html](https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html)

Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route

Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols.

*Computer Standards and Interfaces,* 68, 103391.

<https://doi.org/10.1016/j.csi.2019.103391>

Mudhoep, D. I., Linawati, & Oka Saputra. (2021). Combination of Routing Protocol OSPF

and BGP Using VRRP, HSRP, and GLBP. *Jurnal Nasional Teknik Elektro Dan*

*Teknologi Informasi,* 10(1), 1-10. <https://doi.org/10.22146/jnteti.v10i1.942>

Syahputra, R., Rahmadi Kurnia, & Rian Ferdian. (2020). Analysis of FHRP Design and

Implementation in RIPv2 and OSPF Routing Protocols. *Jurnal RESTI (Rekayasa*

*Sistem Dan Teknologi Informasi),* 4(1), 102 - 108.

<https://doi.org/10.29207/resti.v4i1.1490>

Maneka, R., & Kahewu, D. I. (2021). Analisis perancangan server DHCP menggunakan

Ubuntu Server 18.04 LTS pada jaringan komputer. *Jurnal Teknik Informatika (JTI),*

16(2), 173–178. <https://doi.org/10.35793/jti.16.2.2021.36531>

Amal, S. (2021). Konfigurasi Etherchannel menggunakan protocol LACP pada Cisco Packet

Tracer. *Jurnal Sistem Komputer dan Informatika (JSON),* 3(1), 64–67.

<https://doi.org/10.30864/json.v3i1.341>

Rifandi. (2023). Analisis kinerja jaringan menggunakan teknologi Etherchannel pada

topologi lingkar dengan metode LACP. *Jurnal Ilmiah Komputasi, Teknologi*

*Informasi, dan Komunikasi (KOMTEKINFO),* 1(1), 23–30.

<https://jurnal.komtekinfo.com/index.php/komtekinfo/article/view/3>

Amar, F., Nurulhadi, A., & Hermawan, A. E. (2022). Optimalisasi keamanan jaringan

menggunakan firewall dan proxy server berbasis Mikrotik RouterOS. *Jurnal Ilmiah*

*Komputer dan Informatika (JIKOMIKA),* 2(2), 23–29.

<https://doi.org/10.33486/jikomika.v2i2.3387>

Ismail, Y. O., Dwilaksono, F., & Agussalim. (2021). Analisis dan desain jaringan VLAN pada

SMKN 1 Surabaya. Jurnal Ekonomi, Informasi dan Sistem (JEIS), 2(2), 64–72.

<https://ejurnal.swadharma.ac.id/index.php/jeis/article/download/422/345>

Ar-Rasyid, H., Broto, S., & Artika, W. (2024). Optimasi infrastruktur jaringan VLAN

Trunking Protocol menggunakan simulasi Packet Tracer pada PT. Rukun Sejahtera

Teknik. *JEIS Jurnal Elektro dan Informatika Swadharma* 4(1): 39-46 DOI:

10.56486/jeis.vol4no1.422

# **LAMPIRAN DATA PUBLIKASI DOSEN TEKNIK INFORMATIKA**

| **No** | **Nama** | **Google Scholar** | **Sinta Kemdikbud** |
| --- | --- | --- | --- |
| 1 | Desi Ramayanti, S.Kom., M.T | <https://scholar.google.com/citations?hl=id&user=5Bj7BbsAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6101423> |
| 2 | Henri Septanto, S.Kom., M.Kom | <https://scholar.google.com/citations?hl=id&user=ORsUaXAAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/5983737> |
| 3 | Sri Dianing, S.T., M.Kom. | <https://scholar.google.com/citations?hl=id&user=X-QJtRkAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6664233> |
| 4 | Boy Yuliadi, S.Kom, M.Kom | <https://scholar.google.com/citations?hl=id&user=IjkjpWoAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6675379> |
| 5 | Uus Rusmawan, S.Pd. M.Kom | <https://scholar.google.com/citations?hl=id&user=O-yvO64AAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6766795> |
| 6 | Giri Purnama, S.Pd, M.Kom | <https://scholar.google.com/citations?hl=id&user=fSe1F_IAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6683093> |
| 7 | Eri Dariato, ST., MTI | <https://scholar.google.com/citations?hl=id&user=cu9JmTAAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6818944> |
| 8 | Lionie, S.Kom., MMSI |  | <https://sinta.kemdikbud.go.id/authors/profile/6818955> |
| 9 | Kenneth Mohammad Albany Hakim, ST, MMSI | <https://scholar.google.com/citations?hl=id&user=x5WaD3sAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6818942> |
| 10 | Muhammad Patria, ST, MT | <https://scholar.google.com/citations?hl=id&user=xhrySzUAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6818924> |
| 11 | Arum Kusuma Wardani, ST, MMSI | <https://scholar.google.com/citations?hl=id&user=5MCXlrYAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6818937> |
| 12 | Ekky Bayu Pratama, ST, MMSI |  | <https://sinta.kemdikbud.go.id/authors/profile/6818935> |
| 13 | Fakhria Nur Sabrina, ST, MMSI | <https://scholar.google.com/citations?hl=id&user=83JBi4cAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6818938> |
| 14 | Nur Farida Irmawati, ST, MMSI | <https://scholar.google.com/citations?hl=id&user=RgKqfB4AAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6818933> |
| 15 | Dwi Andrian Susanto, S.Kom., M.Kom |  | <https://sinta.kemdikbud.go.id/authors/profile/6818928> |
| 16 | Ari Hidayatullah, S.Kom., M.Kom | <https://scholar.google.com/citations?hl=id&user=2j2-buEAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6767436> |
| 17 | Imam Mulya, SKom., M.M.S.I | <https://scholar.google.com/citations?hl=id&user=SA-5ZMQAAAAJ> | <https://sinta.kemdikbud.go.id/authors/profile/6796897> |
| 18 | Bias Yulisa Geni, S.Kom., M.Kom. | <https://scholar.google.com/citations?user=b8AVcvYAAAAJ&hl=id> |  |

## Mencari Publikasi di Sinta

1. Klik Link pada Dosen yang akan dicari , kemudian di klik pilihan mulai dari **scopus, Web of Science, Garuda, Google Scholar, Rama.**

