BAB IV

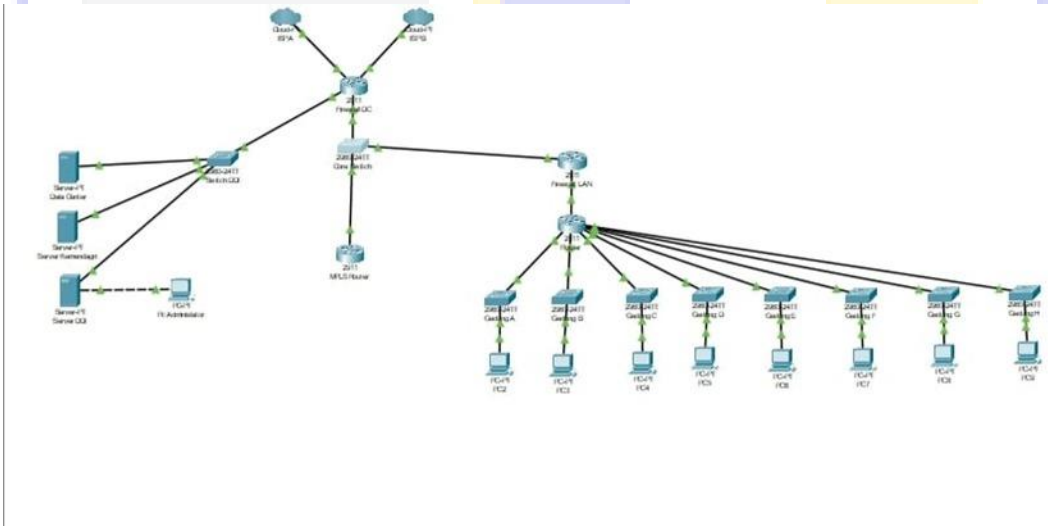
RANCANGAN JARINGAN USULAN

4.1 Jaringan Usulan

Jaringan usulan dirancang sebagai solusi untuk mengatasi berbagai kendala yang ditemukan pada jaringan berjalan. Perancangan ini meliputi perubahan topologi jaringan, penyusunan skema baru yang lebih efisien, serta optimalisasi infrastruktur teknologi informasi yang mencakup server, firewall, dan perangkat monitoring berbasis syslog. Selain itu, jaringan usulan juga menekankan pada penerapan dan penguatan sistem keamanan, mulai dari segmentasi VLAN hingga integrasi IDS/IPS, serta pengelolaan bandwidth yang lebih merata. Rincian dari rancangan ini akan dijelaskan lebih lanjut pada subbab berikutnya, meliputi aspek topologi jaringan, skema jaringan, keamanan jaringan, rancangan aplikasi, dan manajemen jaringan.

4.1.1 Topologi Jaringan

Sebagai bagian dari usulan sistem monitoring dan optimalisasi, dirancang topologi jaringan baru yang menambahkan mekanisme segmentasi VLAN, firewall, serta monitoring berbasis syslog. Topologi ini berfungsi sebagai rancangan utama jaringan usulan. Hal tersebut dapat dilihat pada Gambar IV.1



Sumber : Cisco Packet Tracer

Gambar **Error! No text of specified style in document.**.1 Topologi Jaringan Usulan

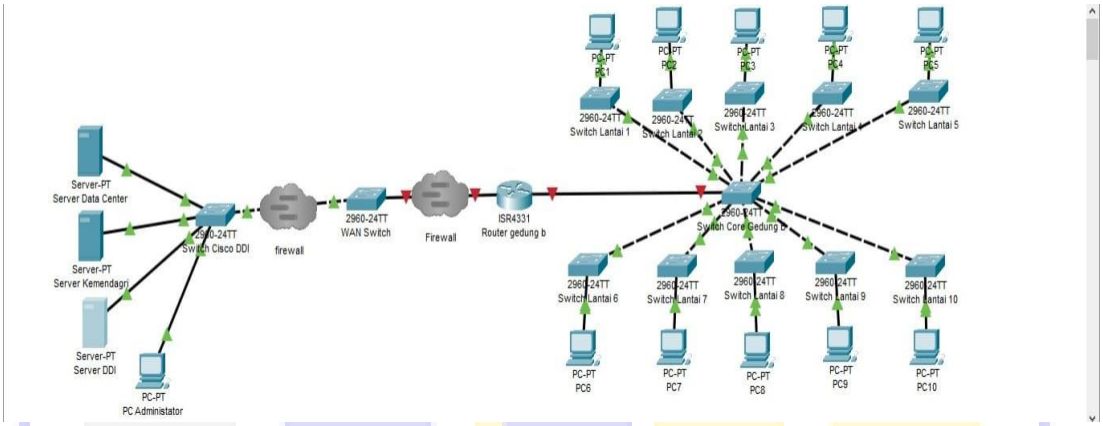
Topologi jaringan usulan pada penelitian ini dirancang untuk mendukung implementasi sistem monitoring dan optimalisasi jaringan pada website DDI di Kementerian Dalam Negeri. Skema jaringan terdiri dari beberapa komponen utama, yaitu data center, server aplikasi, router pusat, multilayer switch, serta perangkat client yang tersebar pada masing-masing lantai gedung. Pada sisi data center, terdapat beberapa server yang berfungsi untuk menyimpan database, menjalankan aplikasi, serta mengelola layanan website DDI. Seluruh server ini terhubung ke switch utama yang berfungsi sebagai penghubung menuju router pusat. Router pusat mengatur konektivitas jaringan internal dengan jaringan eksternal, termasuk koneksi ke cloud server dan branch office.

Dari router pusat, jalur koneksi diteruskan menuju multilayer switch yang berfungsi melakukan segmentasi jaringan berdasarkan VLAN serta mendistribusikan trafik ke berbagai perangkat jaringan. Multilayer switch ini kemudian menghubungkan firewall LAN untuk memberikan keamanan tambahan sebelum data diteruskan ke distribution switch yang membagi koneksi ke setiap client di tiap lantai gedung. Setiap lantai diilustrasikan dengan client PC yang terkoneksi melalui access switch, sehingga alokasi bandwidth dan pengaturan IP dapat dilakukan secara lebih terstruktur.

Selain itu, topologi ini juga didukung dengan perangkat monitoring berbasis syslog yang terhubung ke server administrator. Perangkat ini berperan dalam mencatat seluruh aktivitas jaringan, baik dari sisi client maupun server, sehingga administrator dapat melakukan analisis trafik, deteksi permasalahan, dan optimisasi jaringan secara real time. Dengan rancangan ini, sistem monitoring dapat berjalan terpusat melalui data center, sementara optimisasi jaringan dilakukan melalui pengaturan VLAN, alokasi IP, serta manajemen bandwidth yang dikontrol dari multilayer switch. Hal ini sesuai dengan pendekatan NDLC yang digunakan, yaitu dengan melalui tahap analisis, perancangan, implementasi, monitoring, dan optimisasi jaringan secara menyeluruh.

4.1.2 Skema Jaringan

Rancangan skema jaringan usulan menampilkan hubungan antar server, firewall, router, dan switch pada tiap lantai gedung. Skema ini menekankan distribusi koneksi secara tersegmentasi dengan dukungan monitoring real-time. Hal tersebut dapat dilihat pada Gambar IV.2



Sumber : Cisco Packet Tracer

Gambar **Error! No text of specified style in document.**.2 Skema Jaringan Usulan

Skema jaringan usulan di lingkungan Kemendagri bertujuan untuk mendukung penerapan sistem monitoring serta optimalisasi jaringan melalui pendekatan NDLC. Struktur jaringan ini terdapat tiga server utama yaitu Server Data Center, Server Kemendagri, dan Server DDI yang menjadi pusat layanan dan penyimpanan data. Ketiga server ini terhubung ke Switch Cisco DDI dan dapat diakses langsung oleh PC Administrator. Seluruh lalu lintas dari server diarahkan melalui firewall untuk memastikan keamanan data, sebelum diteruskan ke WAN Switch dan Router. Router berperan sebagai penghubung antara jaringan pusat dengan jaringan internal gedung.

Dari router, koneksi diteruskan ke Switch Core Gedung, yang kemudian mendistribusikan koneksi ke switch akses di setiap lantai. Setiap lantai (lantai 1–10) memiliki switch yang bertugas menghubungkan perangkat pengguna (PC1 hingga PC10). Dengan struktur ini, setiap lantai memiliki segmentasi jaringan tersendiri, sehingga apabila terjadi gangguan pada satu lantai, tidak akan memengaruhi kinerja jaringan pada lantai lainnya. Rancangan jaringan ini juga memperhatikan aspek keamanan dan monitoring. Firewall yang ditempatkan di antara server dan router menjadi lapisan perlindungan utama terhadap ancaman internal maupun eksternal. Administrator juga dapat memanfaatkan sistem monitoring berbasis syslog dan

dashboard untuk mengawasi aktivitas jaringan secara real-time, seperti status perangkat, lalu lintas DHCP, serta penggunaan bandwidth pada tiap lantai. Dengan demikian, troubleshooting dapat dilakukan dengan cepat, sekaligus mendukung penerapan load balancing dan optimalisasi performa jaringan.

4.1.3 Keamanan Jaringan

Sistem keamanan jaringan dalam studi ini menerapkan metode pendekatan Network Development Life Cycle (NDLC) dalam proses perancangannya, yang mencakup lima tahapan utama: analisis, perancangan, implementasi, pengujian, dan pemeliharaan sistem keamanan secara menyeluruh. Pada tahap analisis, dilakukan pengkajian terhadap kebutuhan keamanan jaringan di lingkungan Kementerian Dalam Negeri, dengan fokus pada layanan website milik Direktorat Data dan Informasi (DDI).

Tahapan perancangan difokuskan pada integrasi berbagai komponen proteksi, seperti penggunaan firewall sebagai penghalang utama terhadap akses tidak sah, serta penerapan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) untuk mengidentifikasi dan menangkal aktivitas mencurigakan secara langsung. Selain itu, protokol enkripsi SSL/TLS diterapkan guna mengamankan lalu lintas data, khususnya komunikasi antara server DDI dan pengguna, sehingga kerahasiaan dan integritas data tetap terjaga.

Pada tahap implementasi, sistem dilengkapi dengan autentikasi dua faktor (2FA) untuk membatasi akses hanya kepada personel yang memiliki izin resmi. Selanjutnya, tahap pengujian dilakukan guna mengevaluasi ketahanan sistem terhadap berbagai jenis ancaman, termasuk simulasi serangan seperti unauthorized access, brute force attack, serta pemantauan aktivitas melalui sistem logging berbasis syslog.

Tahap pemeliharaan dilakukan secara berkala dengan dukungan sistem pemantauan jaringan waktu nyata, yang memungkinkan tim IT mendeteksi potensi kerentanan secara proaktif serta melakukan perbaikan tanpa mengganggu jalannya operasional layanan. Melalui penerapan metode NDLC, sistem keamanan yang dibangun bersifat tidak hanya reaktif terhadap gangguan, tetapi juga fleksibel dan dapat dikembangkan sesuai dengan kebutuhan operasional yang terus berkembang di lingkungan Kementerian Dalam Negeri.

4.1.4 Rancangan Aplikasi

Perancangan pada sistem aplikasi ini diawali dengan tahap analisis kebutuhan jaringan, yang mencakup identifikasi berbagai permasalahan seperti distribusi bandwidth yang tidak merata, ketiadaan sistem penyaringan konten, serta kebutuhan akan pemantauan lalu lintas jaringan dan peningkatan efisiensi akses data. Pada fase perancangan, akan dibuat representasi topologi jaringan interkoneksi, termasuk posisi server monitoring, firewall, serta susunan perangkat utama guna memastikan integrasi sistem berjalan secara optimal.

Tahapan selanjutnya adalah pembuatan prototipe dan simulasi jaringan menggunakan alat virtualisasi seperti VirtualBox. Proses simulasi ini mencakup pengujian konektivitas internet, penyaringan konten, pengelolaan bandwidth, serta pengujian sistem keamanan melalui konfigurasi firewall dan VPN. Saat implementasi, server berbasis Linux yang akan digunakan sebagai gerbang utama (gateway), sistem firewall, serta pusat kendali untuk pemantauan lalu lintas dan manajemen bandwidth jaringan. Pengaturan keamanan, pemfilteran IP, dan kontrol akses pengguna akan dikelola secara terpusat melalui antarmuka administrator yang mudah digunakan.

Setelah tahap implementasi, sistem memasuki fase monitoring. Pada tahap ini, seluruh aktivitas jaringan termasuk pemakaian bandwidth, akses situs web, hingga potensi ancaman akan diawasi secara real time. Dengan sistem pemantauan yang terintegrasi, administrator dapat mendeteksi serta mengatasi gangguan atau aktivitas mencurigakan dengan cepat dan efisien. Terakhir, tahap manajemen akan memastikan bahwa kebijakan akses, keamanan, serta prosedur operasional jaringan diterapkan secara konsisten, didukung dengan dokumentasi berkala dan penyesuaian strategi sesuai dengan perkembangan kebutuhan organisasi.

4.1.5 Manajemen Jaringan

Manajemen jaringan yang dirancang untuk Kementerian Dalam Negeri difokuskan pada integrasi dan pemantauan infrastruktur jaringan secara waktu nyata guna menjamin kelancaran akses serta pelayanan website DDI. Pendekatan yang digunakan mengikuti siklus pengembangan jaringan atau Network Development Life Cycle (NDLC), yang mencakup tahapan mulai dari analisis kebutuhan, perancangan arsitektur jaringan yang efisien dan mudah dikembangkan, hingga tahap implementasi yang menitikberatkan pada kestabilan koneksi dan aspek keamanan. Sistem

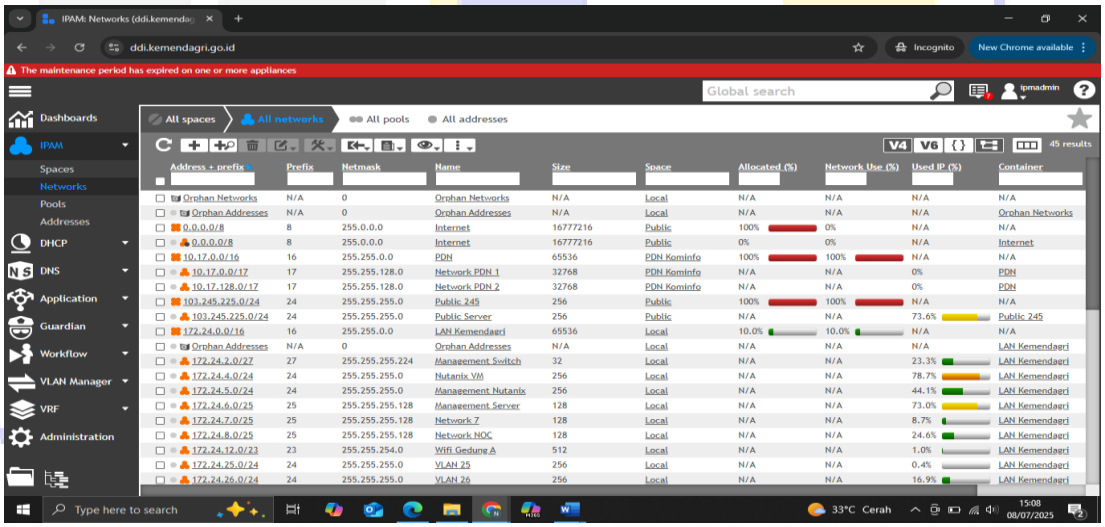
pemantauan jaringan akan diterapkan menggunakan metode yang mampu mendeteksi gangguan secara dini melalui pemberitahuan waktu nyata, sehingga proses perawatan dan perbaikan dapat dilaksanakan secara preventif. Proses optimalisasi juga mencakup pengelolaan bandwidth secara efektif, penerapan sistem penyaringan keamanan, serta penempatan titik akses di lokasi-lokasi strategis agar kecepatan dan kestabilan akses terhadap website DDI tetap terjaga. Dengan penerapan manajemen jaringan yang terstruktur ini, diharapkan performa website DDI dapat meningkat secara signifikan dan mendukung pelaksanaan tugas-tugas administrasi internal secara maksimal.

4.2 Pengujian Jaringan

Di fase ini, sebelum dilakukan melaksanakan pengujian awal dan akhir terhadap jaringan komputer di instansi Kementerian Dalam Negeri. Pengujian ini bertujuan untuk mengevaluasi sejauh mana sistem keamanan jaringan telah berjalan secara optimal sesuai dengan harapan dan standar yang ditetapkan.

4.2.1 Pengujian Jaringan Awal

Pengujian awal jaringan dilakukan melalui antarmuka IP Address Management (IPAM) untuk melihat distribusi alamat IP dan pemakaian subnet. Hasil pengujian ini digambarkan secara detail dalam tampilan dashboard. Hal tersebut dapat dilihat pada Gambar IV.3



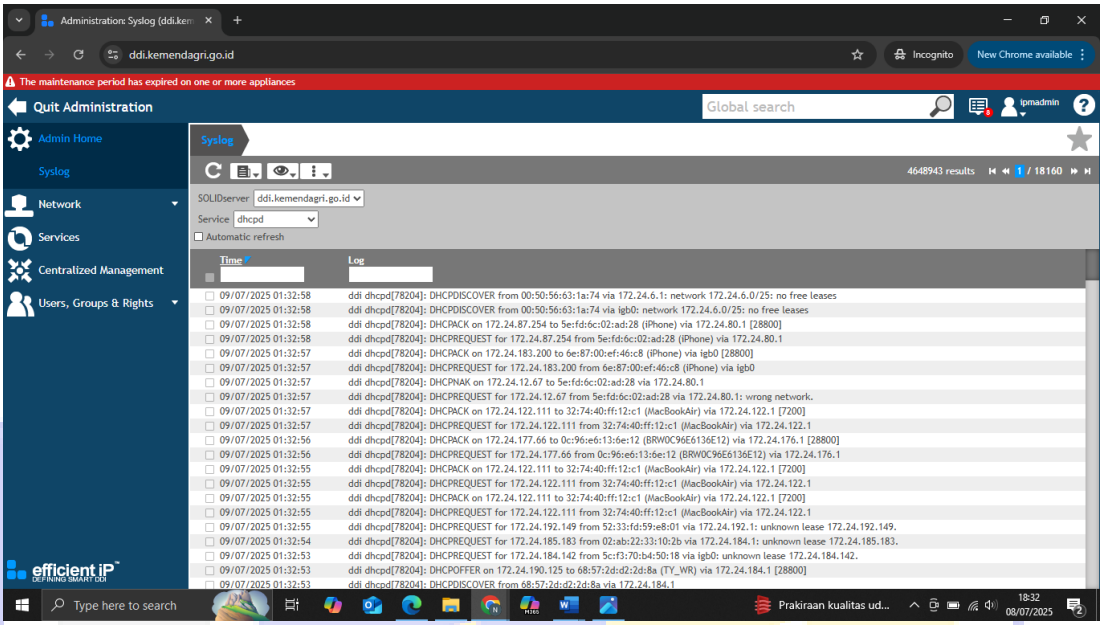
Sumber : Pusdatin

Gambar **Error! No text of specified style in document.**.3 Data Jaringan yang masuk di Kemendagri

Pengujian awal terhadap jaringan menunjukkan keberadaan antarmuka manajemen IP Address Management (IPAM) yang berfungsi dalam proses pemantauan serta pengelolaan alamat IP dan jaringan dalam suatu lingkungan teknologi informasi. Pada antarmuka tersebut ditampilkan berbagai jaringan dengan konfigurasi alamat IP dan subnet mask yang mencakup jaringan publik hingga jaringan lokal (LAN) di lingkungan Kementerian Dalam Negeri. Proses pengujian ini meliputi pengecekan status alokasi IP, tingkat pemanfaatan alamat IP dalam setiap subnet, serta pengelompokan jaringan berdasarkan kategori ruang atau space, seperti jaringan lokal dan publik. Tujuan utama dari proses ini adalah untuk menjamin distribusi alamat IP berlangsung secara efisien dan mencegah terjadinya konflik IP. Sebagai contoh, subnet publik 0.0.0.0/8 dengan prefix 8 memperlihatkan tingkat pemakaian sebesar 100%, yang menandakan bahwa seluruh alamat dalam subnet tersebut telah digunakan sepenuhnya. Sebaliknya, subnet lokal seperti 172.24.0.0/16 menunjukkan tingkat pemakaian yang rendah, yakni sekitar 10%, sehingga masih memungkinkan adanya penambahan perangkat jaringan di masa mendatang. Memonitoring ini sangat penting pada tahap awal pengujian, karena memastikan bahwa jaringan telah terhubung dengan benar, distribusi alamat IP telah sesuai, dan tidak terdapat gangguan pada koneksi sebelum tahap implementasi sistem jaringan lanjutan dilakukan. Dengan dukungan IPAM, administrator jaringan dapat melakukan pemantauan dan perencanaan sumber daya jaringan secara lebih terstruktur dan efisien.

4.2.2 Pengujian Jaringan Akhir

Pengujian akhir sistem monitoring menggunakan fitur syslog untuk merekam aktivitas DHCP secara detail, mulai dari DHCPDISCOVER hingga DHCPACK. Catatan log ini membantu administrator dalam mendeteksi permasalahan secara cepat. Hal tersebut dapat dilihat pada Gambar IV.4



Sumber : Pusdatin

Gambar **Error! No text of specified style in document.**.4 Syslog Wesbite DDI

Pengujian akhir terhadap jaringan, administrator memanfaatkan fitur syslog untuk melihat secara detail setiap permintaan dan distribusi alamat IP yang terjadi pada jaringan, seperti DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, dan DHCPACK. Monitoring ini dilakukan melalui dashboard EfficientIP yang menampilkan log aktivitas DHCP secara kronologis, lengkap dengan waktu, alamat IP, MAC address, dan status permintaan IP.

1. DHCPDISCOVER merupakan pesan siaran (broadcast) yang dikirimkan oleh klien DHCP sebagai upaya awal dalam menemukan server DHCP yang aktif pada jaringan lokal. Pada tahap ini, klien mengirimkan sinyal bahwa ia sedang mencari konfigurasi jaringan yang dapat diberikan oleh server DHCP untuk memperoleh alamat IP secara otomatis.
2. DHCPOFFER merupakan respons dari server DHCP terhadap pesan DHCPDISCOVER yang diterima. Dalam tahap ini, server mengirimkan tawaran kepada klien berupa alamat IP beserta informasi konfigurasi jaringan lainnya. Apabila terdapat lebih dari satu server DHCP yang merespons, klien berpotensi menerima beberapa DHCPOFFER dan kemudian memilih salah satu tawaran yang dianggap paling sesuai.

3. DHCPREQUEST merupakan pesan yang dikirim oleh klien sebagai tanggapan atas tawaran alamat IP dari server DHCP melalui DHCPOFFER. Dalam pesan ini, klien menyatakan persetujuannya terhadap salah satu tawaran yang diterima. Selain itu, pesan ini juga berfungsi sebagai pemberitahuan kepada server DHCP lainnya untuk membatalkan tawaran yang sebelumnya telah dikirimkan.
4. DHCPACK merupakan bentuk konfirmasi dari server DHCP yang menyetujui permintaan klien melalui pesan DHCPREQUEST. Pada tahap ini, server memberikan persetujuan dengan mengirimkan DHCPACK yang berisi alamat IP beserta parameter konfigurasi jaringan lainnya, yang berlaku untuk jangka waktu tertentu. Setelah pesan ini diterima, klien dapat mulai menggunakan alamat IP yang telah dialokasikan oleh server.