SAIN TEKOM
ISSN 2088-1770 (Print)
ISSN 2503-3247 (Online)
Vol. 15 No. 2 (2025) 208-221

JURNAL
SAINTEKOM
Sains, Teknologi, Komputer, dan Manajemen

Integrasi Penyimpanan Data dan Keamanan Jaringan Kantor KEMENAG Menggunakan Metode PPDIOO

*Abdul Hadi[1], Herkules[2], Siti Maryamah[3]
[1,2,3)]Teknik Informatika, STMIK Palangkaraya
Jl. G. Obos No.114, Menteng, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah
Email: [1]abdulhadi@stmikplk.ac.id, [2]herkules@stmikplk.ac.id, [3]sitikemag@gmail.com

ABSTRACT

Poor network design can lead to various issues, such as limited performance, increased operational costs, higher security risks, and difficulties in managing and monitoring network infrastructure. The KEMENAG XYZ office currently operates a local network with multiple wireless modem devices that are not interconnected, resulting in inefficiencies and security challenges in organizational data management.This study aims to implement centralized data storage and network device hardening to support the revitalization program for the use of information and communication technology as well as the optimization of public information transparency at the KEMENAG XYZ city office. The research adopts the Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) methodology by leveraging both hardware and software network technologies.The expected outcomes include a new network infrastructure topology design, more structured data management, and the implementation of enhanced security measures for network devices.

Keywords : network topology; data centralization; data security; PPDIOO

ABSTRAK

Perancangan jaringan yang tidak optimal dapat mengakibatkan berbagai masalah seperti keterbatasan kinerja, peningkatan biaya operasional, risiko keamanan yang lebih tinggi, kesulitan dalam mengelola dan monitoring infrastruktur jaringan. Kantor KEMENAG xyz saat ini mempunyai jaringan lokal dengan banyak perangkat modem wireless yang tidak terhubung antara perangkat jaringan yang satu dengan yang lain yang berdampak pada efisiensi dan keamanan pengelolaan data organisasi. Penelitian ini bertujuan untuk mengimplementasikan sentralisasi penyimpanan data dan hardening perangkat jaringan sehingga menunjang program revitalisasi pemanfaatan teknologi komunikasi dan informasi serta optimalisasi keterbukaan informasi publik pada Kantor KEMENAG kota xyz dengan menggunakan metode *Prepare*, *Plan*, *Design*, *Implement*, *Operate*, dan *Optimize* (PPDIOO) dengan mengoptimalkan teknologi perangkat keras maupun perangkat lunak jaringan. Hasil luaran yang dihasilkan berupa desain topologi infrastruktur jaringan yang baru, pengelolaan data yang lebih terstruktur, dan implementasi keamanan pada perangkat jaringan.

Kata kunci : topologi jaringan; sentralisasi data; keamanan data; PPDIOO

Diterima Redaksi: 18-8-2025 | Selesai Revisi: 05-9-2025 | Diterbitkan Online: 30-9-2025

1. PENDAHULUAN

Peran manajemen data dan informasi diera industri 4.0 yang ditandai dengan konektivitas tinggi dan ketergantungan terhadap teknologi informasi, jaringan komputer memegang peran sentral dalam menunjang komunikasi, pertukaran data, serta akses informasi yang cepat dan efisien. Organisasi pemerintahan, seperti Kementerian Agama (KEMENAG), juga dituntut untuk memiliki infrastruktur jaringan yang andal guna mendukung pelayanan publik yang responsif dan aman (Tjut Adek et al., 2022). Seiring dengan meningkatnya volume dan kompleksitas data, tantangan dalam optimalisasi infrastruktur jaringan pun semakin nyata.

Hasil wawancara penulis dengan pegawai di Kantor KEMENAG Kota XYZ menunjukkan bahwa beberapa bidang masih menyimpan data secara lokal di komputer masing-masing, dan menggunakan layanan cloud gratis melalui akun pribadi. Praktik ini tidak hanya menyulitkan manajemen akun dan kontrol data, tetapi juga meningkatkan risiko kehilangan atau penyalahgunaan informasi akibat kurangnya integrasi dan pengamanan sistem (Vansuri et al., 2023). Ketidakterpaduan dalam penyimpanan data menghambat kolaborasi antarbidang serta memperlambat aliran informasi yang seharusnya mendukung kinerja organisasi secara menyeluruh (Halim, 2019).

Perancangan jaringan yang tidak dioptimalkan dapat mengakibatkan berbagai masalah, termasuk keterbatasan kinerja, peningkatan biaya operasional, risiko keamanan yang lebih tinggi, dan kesulitan dalam mengelola infrastruktur jaringan (Rahayu et al., 2021; Wahyudiono & Lestiono, 2020). Oleh karena itu, penting bagi organisasi untuk memahami betapa vitalnya peran optimalisasi perancangan jaringan guna menjaga efisiensi, keandalan, dan keamanan dalam operasional sehari-hari (Indrayani, 2019). Dalam hal peningkatan kinerja jaringan, beberapa faktor perlu dipertimbangkan adalah perancangan topologi jaringan yang sesuai dapat memberikan manfaat besar dalam mengoptimalkan kinerja dalam jangka waktu yang panjang (Anwar & Nurhaida, 2019).

Penelitian lain menekankan pentingnya topologi jaringan dalam

DOI: https://doi.org/10.33020/saintekom.v15i2.968

mengurangi latensi dan meningkatkan kinerja sistem. Temuan ini mendukung urgensi optimalisasi infrastruktur jaringan (Younus & Sayidmarie, 2020). Namun, aspek keamanan berbasis prinsip *Confidentiality, Integrity,* dan *Availability* (CIA) belum tergarap secara menyeluruh. Penelitian ini memperluas cakupan dengan mengintegrasikan sentralisasi data dan hardening perangkat jaringan untuk meningkatkan kinerja sekaligus keamanan jaringan di Kantor KEMENAG.

Penelitian lain juga menyoroti pentingnya integrasi konsep keamanan untuk membangun jaringan yang tangguh terhadap serangan siber (Aji, 2023; Wahyudiono & Lestiono, 2020). Namun, penelitian tersebut belum mengkaji secara teknis penerapan konsep CIA dalam infrastruktur nyata. Penelitian ini mengisi gap tersebut dengan merancang jaringan yang mengintegrasikan CIA melalui sentralisasi data dan hardening perangkat, khususnya pada lingkungan kerja pemerintahan seperti KEMENAG. Lebih lanjut, penelitian lain fokus pada optimalisasi alokasi *bandwidth* secara adaptif berdasarkan pola lalu lintas jaringan (Nurbahri, 2021; Putra et al., 2020), dan terbukti meningkatkan kinerja jaringan. Namun, penelitian tersebut belum menyentuh aspek penguatan keamanan perangkat maupun efisiensi penyimpanan data. Penelitian ini mengisi celah tersebut dengan menggabungkan pendekatan optimalisasi infrastruktur melalui sentralisasi penyimpanan data dan hardening perangkat jaringan, khususnya dalam konteks kantor pemerintahan seperti KEMENAG.

Berdasar kebutuhan dan latar belakang diatas, akan dibuat topologi jaringan baru dengan mengutamakan efisiensi dan keamanan sistem informasi, diikuti dengan implementasi sentralisasi data dan hardening perangkat jaringan.

2. METODE

Pendekatan implementasi sentralisasi data dan hardening perangkat jaringan menggunakan metode *Prepare, Plan, Design, Implement, Operate, and Optimize* (PPDIOO). Metode ini dipilih karena menyediakan kerangka kerja yang sistematis dan berkelanjutan untuk membangun infrastruktur jaringan yang efisien, aman, dan terstruktur.

DOI: https://doi.org/10.33020/saintekom.v15i2.968

(Octaviyana & Soewito, 2023; Prabowo et al., 2019; Sitompul et al., 2021)

2.1. Prepare (Persiapan)

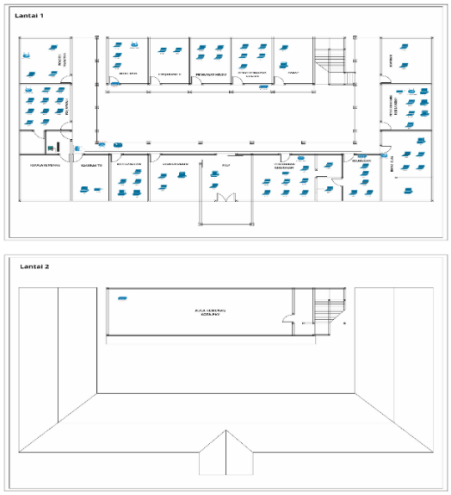
Proyek dimulai dengan fase persiapan. Di tahap ini, Kantor KEMENAG melakukan identifikasi kebutuhan dan memastikan semua sumber daya, baik perangkat keras, perangkat lunak. Kebutuhan jaringan yang ada dievaluasi, dan tujuan proyek ditentukan secara jelas. Setelah persiapan dilakukan, organisasi memasuki fase perencanaan. Pada tahap ini, langkah-langkah praktis untuk pelaksanaan proyek mulai dirumuskan.

2.2. Plan (Perencanaan)

Perencanaan meliputi pembuatan jadwal waktu, alokasi anggaran, serta pembuatan kebijakan keamanan dan prosedur penyimpanan data yang terpusat.

2.3. Design (Perancangan)

Setelah perencanaan, masuk ke fase desain, tahap ini melibatkan pembuatan rancangan jaringan yang terperinci berdasarkan pada perencanaan yang telah dibuat. Desain jaringan mencakup pemetaan topologi existing dan desain topologi baru, pemilihan perangkat keras dan perangkat lunak, serta usulan konfigurasi jaringan. Berdasarkan hasil observasi terjadapat tujuh perangkat modem wireless dengan layanan bandwidth yang berbeda-beda, dua perangkat acces point, satu perangkat router mikrotik yang tidak terpakai, 57 perangkat end device berupa laptop dan 11 berupa komputer desktop, berikut Gambar 1 desain infrastruktur jaringan *existing* kantor KEMENAG xyz.



Gambar 1. Desain existing kantor KEMENAG xyz

DOI: https://doi.org/10.33020/saintekom.v15i2.968

Sebelum membangun sentralisasi data beserta keamanannya, Penulis bekerja sama dengan pihak divisi yang berkepentingan untuk mendefinisikan kebutuhan-kebutuhan (spesifikasi ruang, power, perangkat keras, perangkat lunak) dan batasan-batasan keamanan data yang akan dibangun. Adapun peralatan yang dibutuhkan untuk implementasi jaringan baru berupa satu buah router mikrotik, lima buah perangkat Access Point (AP), satu roll kabel UTP cat 6, satu buah switch PoE Manage untuk perangkat AP, satu buath switch hub gigabit untuk perangkat komputasi, konektor rj45, perangkat NAS synology DS723+ beserta aksesorisnya, dan UPS sebagai backup peralatan jaringan.

2.4. Implement (Implementasi)

Kemudian, desain yang sudah dirumuskan dieksekusi dalam fase implementasi. Pada fase ini, perangkat keras seperti server penyimpanan terpusat dipasang, dan perangkat lunak yang dibutuhkan dikonfigurasi. Sistem penyimpanan data mulai terintegrasi dengan jaringan yang ada, sementara langkah-langkah pengamanan, seperti hardening perangkat jaringan dan pengaturan firewall juga diimplementasikan.

2.5. Operate (Operasional)

Setelah implementasi selesai, proyek masuk ke tahap operasional. Sistem mulai dioperasikan dan dimonitor secara rutin untuk memastikan semuanya berjalan lancar. Pemeliharaan berkelanjutan dilakukan untuk menjaga performa sistem, termasuk monitoring jaringan, pengelolaan akses, dan backup data secara berkala. Jika terdapat masalah dalam operasional, tim IT dapat segera melakukan perbaikan.

2.6. Optimize (Optimasi)

Fase terakhir adalah optimasi, di mana performa sistem dievaluasi dan penyempurnaan dilakukan secara berkelanjutan. Dalam tahap ini, tim mengevaluasi log jaringan dan feedback dari pengguna untuk mencari area yang bisa ditingkatkan, baik dari sisi performa, kapasitas penyimpanan, maupun keamanan. Pembaruan perangkat lunak dan optimasi perangkat keras diterapkan untuk memastikan bahwa sistem tetap bekerja dengan efisien dan aman seiring berjalannya waktu.

Dengan menggunakan metode PPDIOO, dapat dipastikan bahwa implementasi sentralisasi penyimpanan data dan hardening perangkat jaringan

DOI: https://doi.org/10.33020/saintekom.v15i2.968

dilakukan secara sistematis, terukur, dan berkelanjutan, sehingga menghasilkan sistem yang optimal dan aman (Hadi et al., 2021).

3. HASIL DAN PEMBAHASAN

Sebelum dilakukan perubahan desain, kondisi jaringan di Kantor KEMENAG xyz belum terintegrasi dengan baik antarbidang sehingga mengakibatkan keterbatasan dalam konektivitas dan manajemen jaringan. Untuk mengatasi permasalahan tersebut, dilakukan perancangan ulang topologi jaringan fisikal yang tidak hanya menghubungkan seluruh perangkat, tetapi juga memperhatikan aspek keamanan, ketersediaan, dan efisiensi pengelolaan jaringan.

3.1. Perubahan Desain Topologi Fisikal

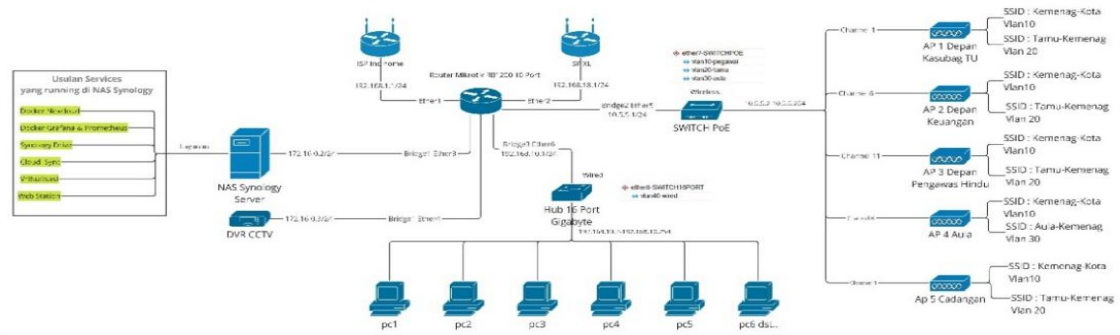
Sebelum implementasi jaringan infrastruktur dapat dilihat seperti pada Gambar 1, terlihat jaringan tidak terhubung antar bidang (ruangan). Perubahan desain topologi akan diterapkan untuk menghubungkan perangkat router, switch, access point dan end device agar bisa saling terhubung secara fisikal. Semua perangkat jaringan ditempatkan di ruangan umum karena lokasi tersebut area yang terjangkau dengan titik pemasangan kabel, dan juga pengelola jaringan ditugaskan pada seksi urusan umum. Aspek keamanan yang diusulkan pada sebagai berikut yaitu :

1. Pembagian subnetting yang berbeda antara peralatan komputasi dan jaringan client menggunakan Virtual LAN (VLAN).
2. Dua layanan Internet Service Provider (ISP) yang akan dijadikan load balance dan failover untuk mengakomodir availability jaringan internet.
3. Router difungsikan untuk limitasi bandwidth, dan akses firewall.
4. Perangkat Synology digunakan untuk sentralisasi data dan juga disematkan aplikasi network monitoring jaringan dan beberapa aplikasi web server untuk kebutuhan layanan web publik.
5. Jaringan wireless dibagi sesuai pengguna menggunakan beberapa SSID dengan pembagian subnetting sesuai VLAN masing-masing.

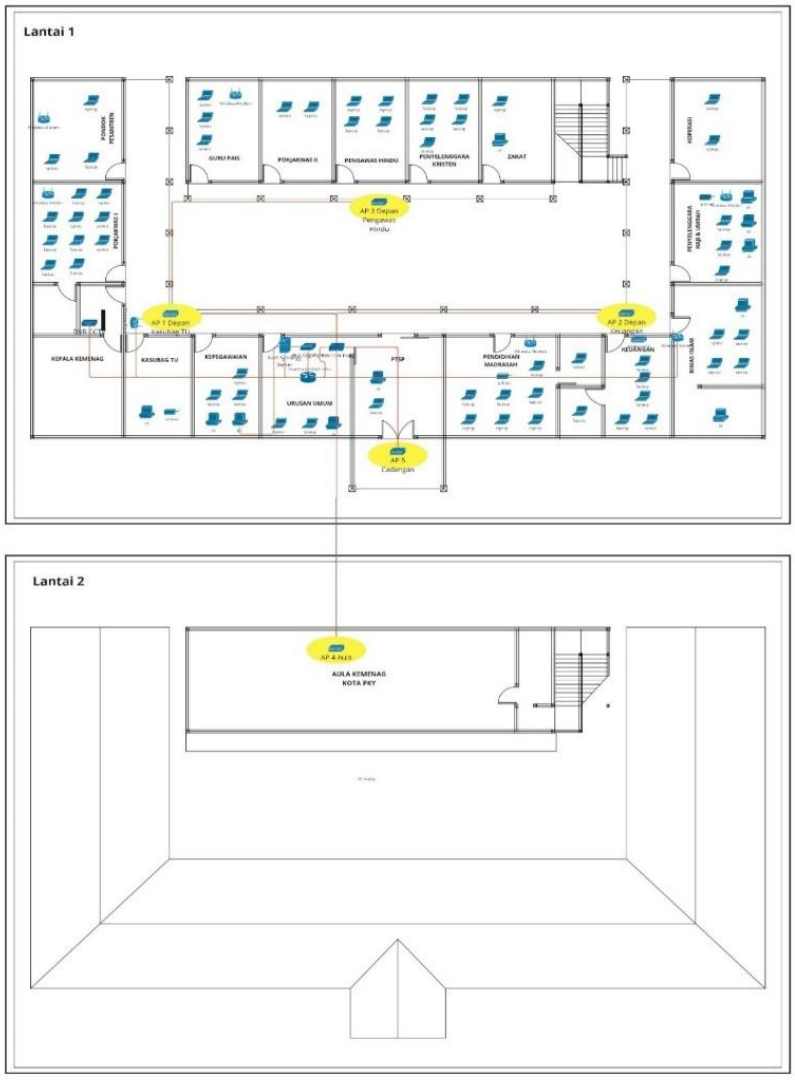
Sedangkan aspek sentralisasi data menggunakan NAS Synology dengan membagi limitasi kapasitas, dan fitur yang akan dipakai yaitu synology

DOI: https://doi.org/10.33020/saintekom.v15i2.968

drive sehingga semua perangkat yang terinstal synology drive client selalu melakukan sinkronasi ke perangkat NAS. Berikut Gambar 2 topologi fisikal dan Gambar 3 denah peletakan perangkat jaringan.



Gambar 2. Topologi fisikal



Gambar 3. Denah peletakan perangkat jaringan

DOI: https://doi.org/10.33020/saintekom.v15i2.968

3.2. Topologi Logical dan *Services*

Sebelum implementasi, perangkat end device mendapatkan IP address dari modem yang terpasang dibeberapa ruangan. Pada topologi logical baru semua perangkat end device akan mendapatkan IP address dari DHCP server router mikrotik, berikut Tabel 1 Topologi *logical* baru.

Tabel 1. Topologi *logical*

No.	Nama Perangkat	Interface	IP Address	Gateway
1	Modem Indihome	1	192.168.1.1/24	192.168.1.1/24
2	Modem XL	1	192.168.18.1/24	192.168.18.1/24
3	Mikrotik	1	192.168.1.2/24	192.168.1.1/24
		2	192.168.18./24	192.168.18.1/24
		3 (Bridge1) NAS Synology	172.16.10.1/24	172.16.10.1/24
		4 (Bridge1) DVR CCTV	172.16.10.1/24	172.16.10.1/24
		5 (Bridge2) Acces Point	10.5.10.1/24	10.5.10.1/254
		6 (Bridge3) Switch hub PC	192.168.10.1/24	192.168.10.1/24
		7	-	-
		8	-	-
		9	-	-
		10	-	-
4	NAS Synology	1	172.16.10.2/24	172.16.10.1/24
5	DVR CCTV	2	172.16.10.3/24	172.16.10.1/24
6	AP 1	1	10.5.10.2/24	10.5.10.1/24
7	AP 2	2	10.5.10.3/24	10.5.10.1/24
8	AP 3	3	10.5.10.4/24	10.5.10.1/24
9	AP 4	4	10.5.10.5/24	10.5.10.1/24
10	AP 5	5	10.5.10.6/24	10.5.10.1/24

Services atau layanan merujuk pada berbagai fungsi dan kemampuan yang disediakan oleh infrastruktur jaringan untuk memungkinkan komunikasi, pertukaran data, dan interaksi antar perangkat atau pengguna. Berikut beberapa jenis layanan yang akan diimplementasikan yaitu: Firewall, DHCP server, load balance, failover, login hotspot, bridge, VLAN SSID.

3.3. Impelementasi Sentralisasi Penyimpanan Data

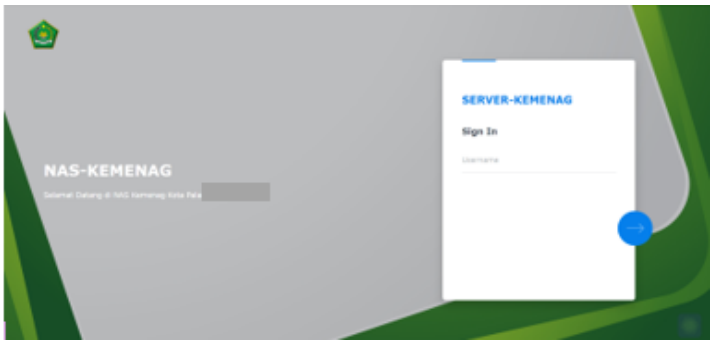
Implementasi sentralisasi penyimpanan data pada kantor kemenag xyz menggunakan perangkat Synology DS723+, prosesnya akan melibatkan beberapa langkah teknis untuk memastikan bahwa data dari berbagai departemen dan pengguna dapat dikelola dengan aman, terpusat, dan

DOI: https://doi.org/10.33020/saintekom.v15i2.968

mudah diakses sesuai dengan kebutuhan kantor.

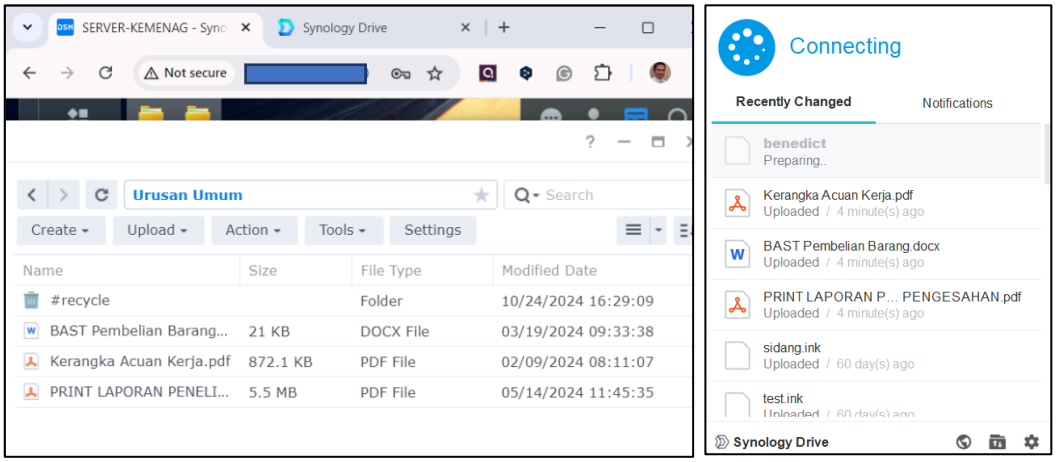
Proses dimulai dengan penyiapan perangkat Synology NAS (Network Attached Storage), yang akan menjadi pusat dari sistem penyimpanan data terpusat. Perangkat ini dipilih karena kemampuannya untuk menyediakan penyimpanan data yang efisien, mudah diakses, serta dilengkapi dengan berbagai fitur keamanan. Synology NAS akan ditempatkan di pusat data kantor atau di lokasi yang memiliki akses jaringan yang kuat. Dalam hal ini, teknisi memastikan bahwa kapasitas penyimpanan NAS cukup untuk menampung seluruh data yang akan dipusatkan, serta mempertimbangkan kemampuan perangkat untuk diperluas jika di masa depan kebutuhan penyimpanan meningkat.

Setelah perangkat Synology terpasang secara fisik dan terhubung ke jaringan lokal Kantor KEMENAG XYZ, langkah berikutnya adalah konfigurasi dasar. Konfigurasi ini mencakup pengaturan awal perangkat, seperti alamat IP statis agar Synology NAS dapat diakses oleh semua pengguna dalam jaringan kantor. Teknis lain yang dilakukan adalah menentukan struktur folder atau direktori di dalam perangkat sesuai dengan kebutuhan organisasi. Misalnya, folder dapat dibagi berdasarkan departemen seperti "Bagian Urusan Umum", "Bidang pendidikan agama dan keagamaan Islam", "bidang penyelenggaraan haji dan umrah ", dan lainnya, sehingga data dari setiap departemen tersimpan dengan rapi dan terorganisir. Berikut Gambar 4 tampilan login synology yang sudah disesuaikan, dan Gambar 5 proses singkronasi data dari komputer ke synology drive.



Gambar 4. Tampilan Login Synology

DOI: https://doi.org/10.33020/saintekom.v15i2.968



Gambar 5. Tampilan sinkronasi data dari komputer ke synology drive

Kemudian, kontrol akses merupakan bagian penting dalam sentralisasi penyimpanan data. Pada Synology NAS, administrator akan mengatur hak akses bagi setiap pengguna atau grup pengguna. Di Kantor KEMENAG XYZ, ini berarti hanya pegawai tertentu yang dapat mengakses folder tertentu, sesuai dengan kebijakan keamanan data.

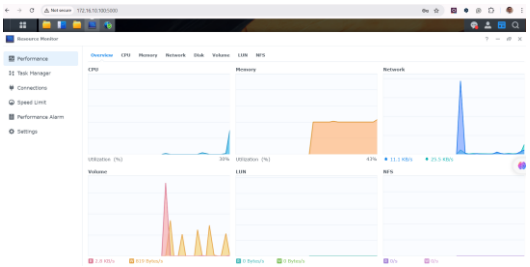
Untuk melindungi data dari kemungkinan kegagalan perangkat atau kehilangan data, mekanisme backup menjadi bagian penting dalam konfigurasi Synology NAS. Sistem *Redundant Array of Independent Disks* (RAID) diaktifkan untuk memastikan data disalin secara otomatis ke beberapa disk, sehingga jika salah satu disk mengalami kerusakan, data tidak hilang. Selain itu, Synology juga memungkinkan konfigurasi backup secara otomatis ke lokasi lain, baik melalui jaringan lokal maupun ke cloud. Kantor KEMENAG XYZ dapat memilih untuk menyimpan cadangan data di server lain di kantor, atau menggunakan solusi cloud yang disediakan oleh Synology untuk menjaga data tetap aman meski terjadi bencana fisik.

Setelah konfigurasi selesai, sinkronisasi data dilakukan. Data dari berbagai komputer dan server di Kantor KEMENAG dipindahkan atau disinkronkan ke dalam Synology NAS. Synology memiliki aplikasi Cloud Sync yang mempermudah pengguna dalam sinkronisasi data dari berbagai perangkat ke NAS secara otomatis. Hal ini memungkinkan pegawai di berbagai departemen untuk memiliki akses yang

DOI: https://doi.org/10.33020/saintekom.v15i2.968

sama terhadap dokumen dan file penting dari mana saja selama mereka memiliki izin akses yang sesuai.

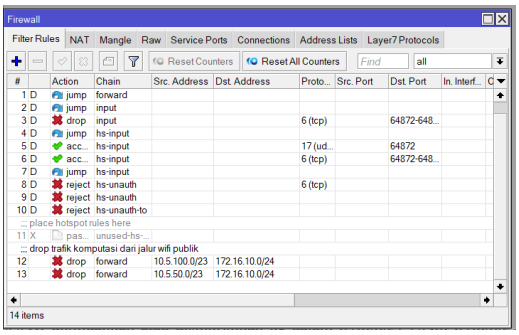
Selanjutnya, monitoring dan pemeliharaan menjadi aspek yang tidak kalah penting. Synology menyediakan fitur DSM (DiskStation Manager), sebuah antarmuka yang mudah digunakan untuk mengelola dan memonitor sistem. Administrator jaringan di Kantor KEMENAG dapat menggunakan DSM untuk memantau penggunaan penyimpanan, kinerja jaringan, serta melakukan audit terhadap akses data. Laporan berkala juga dapat dihasilkan untuk mengetahui seberapa sering data diakses atau apakah ada ancaman keamanan yang perlu diatasi, berikut Gambar 6 tampilan menu resource monitor.



Gambar 6. Tampilan *resousce monitor* DSM

3.4 Daftar Hardening Perangkat Jaringan

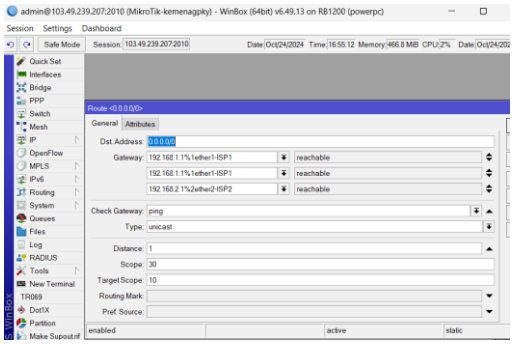
Proses hardening dimulai dengan memperketat akses ke router MikroTik melalui konfigurasi firewall dan limitasi bandwidth. Firewall diatur untuk memfilter lalu lintas jaringan, hanya mengizinkan port dan protokol yang benar-benar diperlukan, serta membatasi akses dari alamat IP yang tidak dikenal atau mencurigakan untuk mengakses perangkat komputasi sehingga aspek keamanan CIA pada bagian confidentiality dan integrity terlindungi. Sedangkan manajemen bandwidth pada MikroTik memungkinkan pengaturan alokasi penggunaan internet untuk setiap pengguna atau perangkat dalam jaringan, guna memastikan distribusi koneksi yang adil dan optimal. Dengan fitur seperti Simple Queue. Manajemen ini juga memungkinkan pengendalian penggunaan data serta memastikan akses internet yang stabil dan efisien bagi seluruh pengguna, berikut Gambar 7 beberapa konfigurasi firewall untuk membatasi akases keperangkat komputasi.



Gambar 7. Filter rules mikrotik

DOI: https://doi.org/10.33020/saintekom.v15i2.968

Penerapan load balancing menggunakan metode Equal-Cost Multiple Path (ECMP) dengan membagi beban trafik internet sesuai kebutuhan, sehingga mempercepat konektivitas dan mencegah satu ISP menjadi terlalu terbebani. Sementara itu, failover berfungsi sebagai cadangan jika satu ISP mengalami gangguan atau kegagalan, secara otomatis trafik akan dialihkan ke ISP kedua, memastikan aspek keamanan CIA bagian availability tetap terjaga. Kombinasi kedua mekanisme ini menjamin stabilitas dan kontinuitas akses internet bagi pengguna. Berikut Gambar 8 konfigurasi load balancing dan failover.



Gambar 8. *Load Balancing* menggunakan ECMP dan failover

Adapun kata sandi yang kuat dan kompleks juga menjadi bagian penting dalam hardening perangkat MikroTik di kantor KEMENAG. Administrator memastikan bahwa semua akun pengguna memiliki kata sandi yang kuat dengan kombinasi karakter yang sulit ditebak, yang mencegah serangan brute force atau akses tidak sah. Selain itu, untuk menjaga performa jaringan yang optimal dan adil, administrator menerapkan limitasi bandwidth per pengguna menggunakan metode Simple *Per Connection Queue* (PCQ) pada MikroTik. Pengaturan ini membatasi alokasi bandwidth tiap pengguna sehingga penggunaan jaringan tetap efisien dan tidak terganggu oleh pemakaian berlebih.

3.5. Pengujian

Pengujian dalam penelitian ini bertujuan untuk memastikan bahwa sistem yang diterapkan, termasuk sentralisasi penyimpanan data dan hardening perangkat jaringan berjalan sesuai dengan spesifikasi yang ditentukan.

Pengujian dilakukan untuk mengevaluasi kinerja, keamanan, dan stabilitas sistem, mulai dari pengaturan perangkat keras hingga integrasi jaringan. Berikut Tabel 3 hasil perbandingan sebelum dan sesudah konfigurasi.

DOI: https://doi.org/10.33020/saintekom.v15i2.968

Tabel 3. Perbedaan sebelum dan sesudah implementasi konfigurasi

Perubahan	Sebelum	Sesudah
Pembagian *subnetting* yang berbeda antara peralatan komputasi dan jaringan client	Tidak ada pembagian subnet antara perangkat komputasi dan client luar	Implementasi subnet menggunakan VLAN pada perangkat komputasi dan client luar dengan menggunakan VLAN ID : 10, 20, 30
Efisiensi langganan modem dan implementasi *load balance* dan *failover* untuk mengakomodir *availability* jaringan internet	Berlangganan lima ISP yang sama tanpa manajemen load balancing dan failover	Layanan ISP efisien dengan dua vendor berbeda yang di-upgrade ke 100 Mbps, dikelola satu router menggunakan load balance dan failover untuk menjaga ketersediaan koneksi.
Manajemen Jaringan menggunakan router	Belum dikelola menggunakan router sehingga antar jaringan dalam ruangan tidak bisa terkoneksi secara *phsyical* dan *logical*	Jaringan dikelola menggunakan router mikrotik RB1200 dengan konfigurasi limitasi bandwidth seperti pada Tabel 2, load balance, failover, VLAN, *hardening* keamanan mikrotik (firewall, limitasi akses)
Sentralisasi penyimpanan data	Data tersimpan di lokal komputer dan beberapa akun google drive	Data disimpan di NAS Synology dan disinkronkan secara realtime dari perangkat lokal melalui aplikasi Synology Drive.
Pengaturan SSID	SSID dibuat sesuai nama ruangan dengan frekuensi yang acak sehingga berakibat interferensi pada frekuensi yang sama	SSID disesuaikan dengan pembagian VLAN ID (Gambar 2), menggunakan frekuensi statis yang dikelola oleh AI pada access point Ruijie.

4. KESIMPULAN

Berdasarkan implementasi metode PPDIOO, perubahan desain topologi jaringan fisikal, serta penerapan sentralisasi penyimpanan data dan hardening perangkat jaringan di Kantor KEMENAG Kota xyz berhasil dilakukan secara sistematis dan terukur. Hasil implementasi ini memungkinkan seluruh perangkat jaringan terhubung dengan baik, meningkatkan keamanan melalui pembagian VLAN, pengaturan firewall, dan manajemen akses, sekaligus mendukung ketersediaan layanan dengan konfigurasi *load balance* dan *failover* pada dua ISP. Sentralisasi data dengan NAS Synology juga mendorong kolaborasi yang lebih aman dan efisien, sekaligus memperkuat fondasi layanan digital ke depan.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

DOI: https://doi.org/10.33020/saintekom.v15i2.968

Anwar, M. K., & Nurhaida, I. (2019). Implementasi Load Balancing Menggunakan Metode Equal Cost Multi Path (ECMP) Pada Interkoneksi Jaringan. *Jurnal Telekomunikasi dan Komputer*, *9*(1), 39. https://doi.org/10.22441/incomtech.v9i1.5003

Hadi, A., Herkules, H., & Norhayati, N. (2021). Perencanaan Layout Data Center Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah. *Jurnal Sains Komputer dan Teknologi Informasi*, *4*(1), 9–16. https://doi.org/10.33084/jsakti.v4i1.2275

Halim, R. M. N. (2019). Penerapan Network Attached Storage (NAS) berbasis Raspberry Pi di LP3SDM AZRA Palembang. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *6*(3), 309. https://doi.org/10.25126/jtiik.2019631416

Indrayani, N. (2019). *Evaluasi Pendekatan Tersentral dalam Penerapan IT Governance dari Perspektif Kantor Cabang Perusahaan*.

Nurbahri, R. (2021). Perancangan dan Implementasi Virtual Local Area Network (Vlan) untuk Optimalisasi Bandwidth Jaringan. *Vol .*, *1*.

Octaviyana, R. A., & Soewito, B. (2023). *Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja PPDIOO*.

Prabowo, A. A., Bidoyono, A., & Almaarif, A. (2019). *Analisis Dan Perancangan Telecommunication Cabling Infrastructure Data Center Di Pt. Xyz Dengan Standar Tia-942 Dan Metode Ppdioo Life-Cycle Approach*.

Putra, Y. S., Indriastuti, M. T., & Mukti, F. S. (2020). Optimalisasi Nilai Throughput Jaringan Laboratorium Menggunakan Metode Hierarchical Token Bucket (Studi Kasus: Stmik Asia Malang). *Network Engineering Research Operation*, *5*(2), 83. https://doi.org/10.21107/nero.v5i2.161

Rahayu, S. K., Ruqoyah, S., Berliana, S., Pratiwi, S. B., & Saputra, H. (2021). Cybercrime dan dampaknya pada teknologi e-commerce. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(3), 632. https://doi.org/10.52362/jisamar.v5i3.478

Sitompul, D. R. H., Harmaja, O. J., & Indra, E. (2021). *Perancangan Pengembangan Desain Arsitektur Jaringan Menggunakan Metode PPDIOO*. *4*(2).

Tjut Adek, R., Yunizar, Z., Maha, D. T. P., & Fajriana, F. (2022). Perancangan Desain Jaringan Fiber Optik Dengan Teknologi Gigabit Passive Optical Network Di Universitas Malikussaleh. *Jurnal Saintekom*, *12*(2), 168–175. https://doi.org/10.33020/saintekom.v12i2.305

Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Restu, A. M., & Firmansyah, R. R. (2023). *Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi*. *2*(1).

Wahyudiono & Lestiono. (2020). Konsep Penerapan Keamanan Jaringan Publik Di Lingkungan Kampus Stmik Bina Patria. *Transformasi*, *16*(1). https://doi.org/10.56357/jt.v16i1.220

Younus, K. M., & Sayidmarie, K. H. (2020). *A Tri-Band Frequency Reconfigurable Slot Antenna for Wireless Applications*. *35*(2).

DOI: https://doi.org/10.33020/saintekom.v15i2.968