BAB IV

RANCANGAN JARINGAN USULAN

4.1 Jaringan Usulan

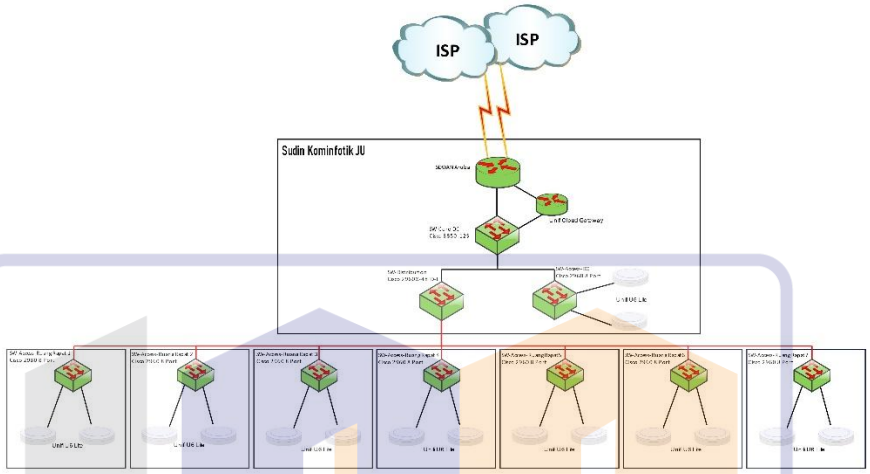
Hasil analisis terhadap jaringan yang berjalan menunjukkan beberapa kendala, antara lain penggunaan *access point* standalone yang tidak mendukung pengelolaan terpusat, belum diterapkannya *Quality of Service* (QoS), ketiadaan sistem *firewall*, serta koneksi yang kurang stabil saat trafik tinggi. Permasalahan ini menyebabkan pengelolaan jaringan menjadi kurang efisien dan rentan terhadap gangguan.

Sebagai solusi, penulis mengusulkan penerapan Unifi Cloud Gateway dan penggantian *access point* dengan Unifi AP yang terintegrasi dalam satu sistem manajemen berbasis cloud melalui *Unifi Site Manager*. Pendekatan ini bertujuan untuk memudahkan konfigurasi, meningkatkan keamanan jaringan, serta memastikan kualitas layanan tetap optimal. Selain itu, solusi ini juga diharapkan dapat mengoptimalkan pemanfaatan bandwidth ISP, sehingga jaringan menjadi lebih stabil dan terkelola dengan baik di seluruh lingkungan Kantor Walikota Administrasi Jakarta Utara.

4.1.1 Topologi Jaringan

Jaringan di Suku Dinas Kominfotik Jakarta Utara menggunakan topologi star yang secara umum telah berjalan dengan baik. Namun, perangkat yang digunakan, khususnya pada jaringan nirkabel, belum mendukung pengelolaan bandwidth secara optimal, sehingga memengaruhi efisiensi dan kestabilan koneksi di lingkungan kerja. Untuk mengatasi hal tersebut, penulis mengusulkan penerapan Unifi Cloud Gateway sebagai solusi manajemen jaringan terpusat, serta penggantian perangkat a*ccess point* TPlink Archer C60 dengan Unifi U6 Lite yang lebih mendukung integrasi sistem

berbasis *cloud* dan peningkatan performa jaringan nirkabel. Dengan langkah ini, diharapkan jaringan, khususnya konektivitas nirkabel, menjadi lebih stabil, aman dan mudah dikelola secara menyeluruh.



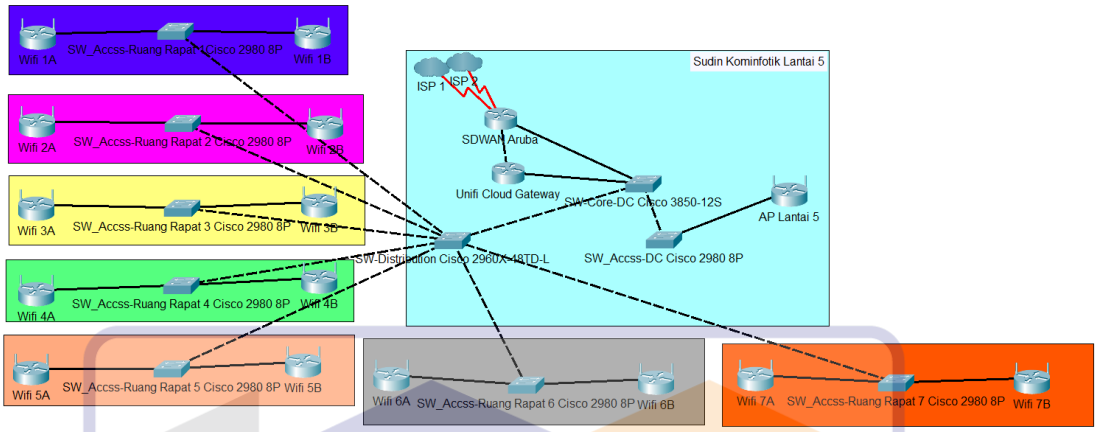
Sumber: [30]

Gambar IV. 1 Topologi Jaringan Usulan

4.1.2 Skema Jaringan

Untuk skema jaringan usulan yang dirancang oleh penulis ke Sudin Kominfotik Jakarta Utara ialah untuk topologi yaitu masih sama topologi star. Perbedaaan yang terdapat dalam skema yang dirancang oleh penulis yaitu topologi yang diusulkan dengan saat ini yaitu terdapat penambahan perangkat Unifi Cloud Gateway dan Unifi U6 Lite yang menggantikan TPLink Archer C60. Topologi yang diusulkan ini dianggap efektif dan dapat mendukung jaringan di Kantor Walikota Administrasi Jakarta Utara. Dalam skema jaringan yang diajukan ini, penulis menggunakan UniFi Dashboard untuk manajemen terpusat yang digunakan untuk memantau, mengelola dan mengoptimalkan infrastruktur jaringan nirkabel berbasis *access point* untuk mendapatkan kualitas dan kestabilan internet di Kantor Walikota Administrasi Jakarta Utara. Maka penulis membuat dan mengusulkan rancangan

topologi ini dengan harapan dapat diimplementasikan sebagai topologi jaringan yang baru.



Sumber: [30]

Gambar IV. 2 Skema Jaringan Usulan

4.1.3 Keamanan Jaringan

Dalam upaya meningkatkan keamanan jaringan pada segmen pengguna umum, penulis menerapkan mekanisme *Content Filtering* melalui submenu *Cybersecurity* pada Unifi Dashboard. Pengaturan ini diterapkan pada SSID KOMINFOTIK yang dikaitkan dengan VLAN 30, dengan tujuan membatasi akses terhadap konten-konten yang tidak sesuai dengan kebijakan penggunaan jaringan. Salah satu fitur yang diaktifkan adalah *SafeSearch*, yang memungkinkan penyaringan hasil pencarian dari mesin pencari seperti Google agar tidak menampilkan konten yang bersifat negatif atau tidak pantas.

Selain itu, penulis menambahkan sejumlah domain secara manual ke dalam Blocklist, sehingga akses ke situs-situs tertentu dapat diblokir secara spesifik. Jadwal pemblokiran disetel ke mode *Always*, yang memastikan filter berlaku secara permanen tanpa jeda waktu. Seluruh konfigurasi ini merupakan bagian dari implementasi firewall berbasis aplikasi, yang dirancang untuk menjaga kestabilan dan integritas

jaringan, serta memastikan bahwa penggunaan jaringan tetap berada dalam batasan yang aman dan terkendali.

4.1.4 Rancangan Aplikasi

UniFi Dashboard merupakan platform manajemen terpusat yang digunakan untuk memantau, mengelola dan mengoptimalkan infrastruktur jaringan nirkabel berbasis *access point*. Dalam rancangan aplikasi ini peningkatan kualitas jaringan di Kantor Walikota Administrasi Jakarta Utara, Unifi Dashboard menjadi alat penunjang utama karena kemampuannya dalam menyajikan data *real time* mengenai trafik jaringan, distribusi klien, kekuatan sinyal serta kestabilan koneksi antar titik akses.

4.1.5 Manajemen Jaringan

Gambar IV. 3 Dashboard UniFi Cloud Gateway

Dashboard UniFi Cloud Gateway yang ditampilkan pada Gambar IV. 3 merupakan sistem pemantauan dan manajemen jaringan terintegrasi yang digunakan untuk mengelola konektivitas nirkabel dan kabel pada jaringan institusi atau perusahaan. Sistem ini memperlihatkan tampilan antarmuka manajemen jaringan yang menjadi pusat pengaturan infrastruktur jaringan nirkabel. Dalam tampilan tersebut, penulis mengelola dua SSID, yaitu KOMINFOTIK dan KOMINFOTIK-AP, yang

masing-masing terhubung pada VLAN 30 dan VLAN 34 serta dipancarkan oleh dua Access Point (AP) pada frekuensi 2.4 GHz dan 5 GHz secara simultan.

Perbedaan utama antara kedua SSID tersebut terletak pada segmentasi pengguna. SSID KOMINFOTIK ditujukan untuk kebutuhan akses pengguna umum, sedangkan SSID KOMINFOTIK-AP diperuntukkan secara khusus bagi administrator jaringan. Segmentasi ini memberikan fleksibilitas dalam pengelolaan jaringan sekaligus mendukung penerapan kebijakan keamanan dan kualitas layanan (QoS) secara lebih spesifik.

Penulis menerapkan pembatasan bandwidth dan pemblokiran akses tertentu pada SSID KOMINFOTIK, mengingat SSID ini digunakan oleh publik sehingga memerlukan pengendalian untuk mencegah penggunaan sumber daya jaringan secara berlebihan dan menjaga kestabilan koneksi. Sementara itu, SSID KOMINFOTIK-AP diberikan akses penuh tanpa pembatasan untuk mendukung aktivitas pemantauan dan administrasi jaringan secara optimal oleh tim teknis.

Setelah dilakukan implementasi sistem berbasis Unifi Cloud Gateway yang mengacu pada lima pilar manajemen jaringan menurut standar FCAPS, diperoleh berbagai dampak positif yang signifikan terhadap kualitas dan efisiensi jaringan nirkabel di lingkungan Kantor Walikota Administrasi Jakarta Utara. Penerapan sistem ini tidak hanya meningkatkan stabilitas dan performa jaringan, tetapi juga menyederhanakan proses manajemen dan pemantauan perangkat secara real time, sekaligus memperkuat aspek keamanan melalui pengaturan akses dan pemanfaatan *firewall* yang terintegrasi. Seluruh proses konfigurasi, pelaporan, hingga pengendalian trafik kini dapat dilakukan secara terpusat dan lebih responsif terhadap dinamika kebutuhan jaringan institusi.

1. *Fault Management*

   Fungsi ini berfokus pada deteksi, isolasi dan penyelesaian gangguan jaringan secepat mungkin. Dalam konteks implementasi perangkat Unifi, sistem akan memberikan notifikasi otomatis apabila terjadi anomali, seperti *access point* yang tidak aktif, penurunan performa atau kehilangan konektivitas. Hal ini memungkinkan administrator jaringan merespon gangguan secara cepat sebelum berdampak luas pada pengguna.

2. *Configuration Management*

   Tugas dari konfigurasi adalah mengelola pengaturan perangkat jaringan termasuk *router, switch* dan *access point*. Penelitian ini menggunakan *Unifi Network Controller* sebagai antarmuka grafis yang mendukung konfigurasi terpusat. Seluruh *access point* yang terhubung ke Unifi Cloud Gateway dapat dikonfigurasi secara *remote*, termasuk penyesuaian SSID, segmentasi jaringan, hingga penerapan kebijakan *firewall* dan VLAN. Hal ini meningkatkan efisiensi dan konsistensi pengaturan jaringan di seluruh lokasi.

3. *Accounting Management*

   Fungsi ini berkaitan dengan pencatatan aktivitas pengguna dan pemanfaatan sumber daya jaringan. Dalam sistem Unifi, fitur statistik dan *insight* memungkinkan administrator memantau trafik, konsumsi *bandwidth* per perangkat, serta log aktivitas. Informasi ini berguna untuk melakukan alokasi *bandwidth* yang adil, audit keamanan, maupun evaluasi kinerja layanan jaringan.

4. *Performance Management*

   Fokusnya adalah menjaga performa jaringan tetap optimal dengan memantau kecepatan akses, latensi, utilisasi *bandwidth* dan beban perangkat. Penelitian

ini mengimplementasikan teknologi *Quality of Service* (QoS) untuk memastikan data penting mendapat prioritas jalur data. Dengan QoS, administrator dapat menghindari kemacetan trafik dan menjaga kualitas layanan utama tetap stabil.

5. *Security Management*

   Aspek ini meliputi pengamanan jaringan dari ancaman, baik eksternal maupun internal. Penelitian ini menggunakan fitur *firewall* yang tersedia pada Unifi Cloud Gateway untuk membatasi lalu lintas berdasarkan aturan tertentu, seperti pemblokiran port atau pembatasan *IP address*. Selain itu, dukungan terhadap sistem autentikasi pengguna, enkripsi trafik dan deteksi aktivitas ilegal memberikan lapisan proteksi tambahan dalam arsitektur jaringan.

Dalam arsitektur jaringan modern yang diangkat dalam penelitian ini, pengelolaan seluruh perangkat dilakukan secara terpusat melalui platform Unifi Cloud Gateway. Sistem ini memungkinkan monitoring perangkat *access point* secara *real time*, konfigurasi jarak jauh, serta logging aktivitas jaringan. Cloud Gateway juga mendukung integrasi langsung dengan fitur keamanan seperti *firewall* dan sistem QoS, menjadikan pengelolaan jaringan tidak hanya efisien tetapi juga aman dan responsif terhadap kebutuhan pengguna. Dengan penerapan manajemen jaringan berbasis FCAPS yang didukung oleh teknologi Cloud Gateway dan Unifi Network Controller, penelitian ini bertujuan membangun sistem jaringan nirkabel yang stabil, adaptif dan terkelola dengan baik sesuai kebutuhan institusi.

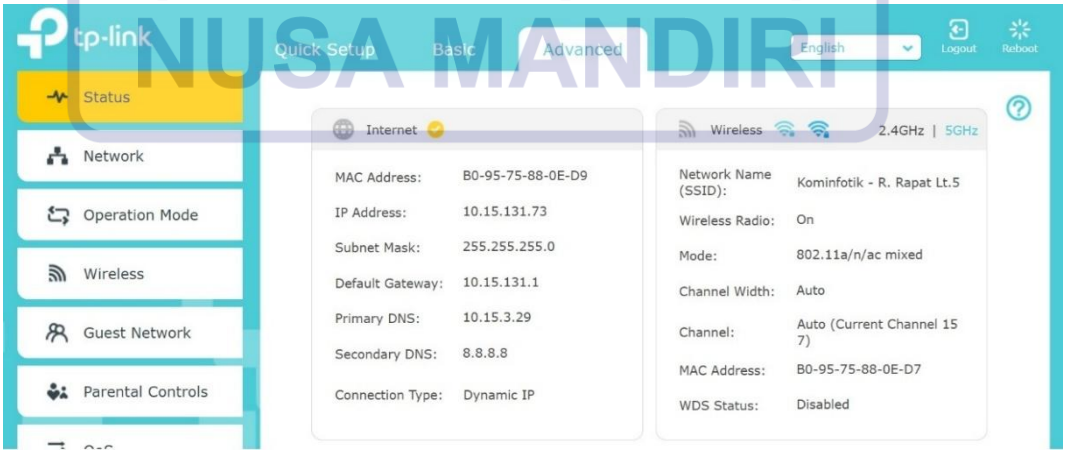
4.2 Pengujian Jaringan

4.2.1 Pengujian Jaringan Awal

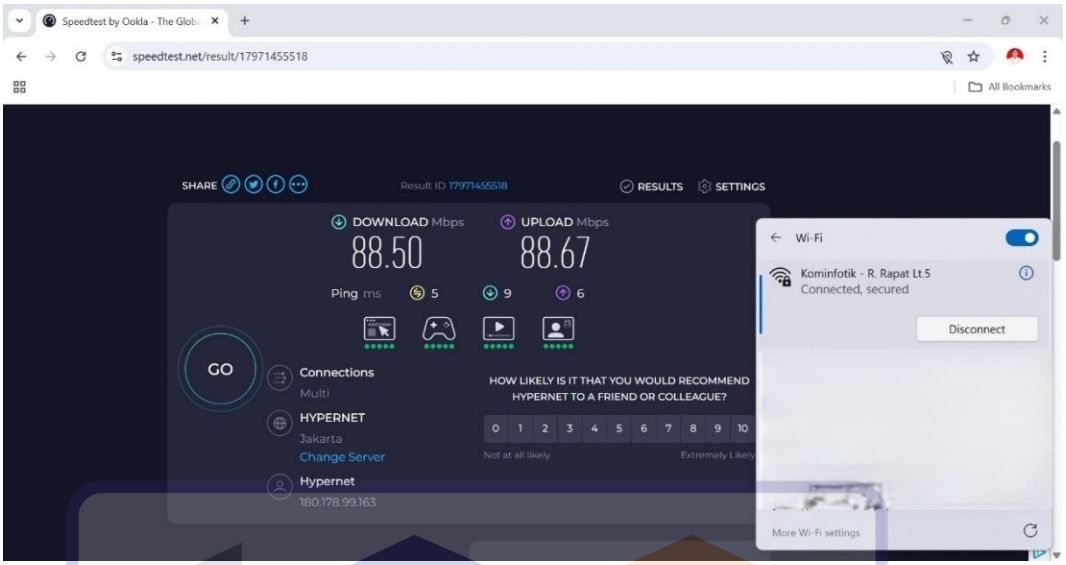
Berdasarkan hasil pengujian *bandwidth* di beberapa titik strategis dalam gedung Kantor Walikota Administrasi Jakarta Utara, diketahui bahwa kecepatan akses

internet yang diterima oleh pengguna tidak mencerminkan kapasitas penuh yang disediakan oleh ISP. Rata-rata kecepatan download hanya mencapai 24.5 Mbps, jauh di bawah bandwidth yang seharusnya dapat dimanfaatkan. Hal ini mengindikasikan adanya ketidak efisiensi dalam manajemen lalu lintas data.

Kondisi ini diperburuk dengan tidak adanya penerapan *Quality of Service* (QoS) dalam sistem jaringan. Seluruh trafik data, baik untuk keperluan administratif, *browsing*, *video streaming*, maupun pembaruan sistem, berjalan tanpa pembeda prioritas. Akibatnya, layanan yang seharusnya bersifat kritikal tidak mendapatkan alokasi bandwidth yang memadai, terutama saat jaringan berada pada kondisi padat. Selain itu, perangkat *access point* yang digunakan saat ini masih menggunakan TPLink Archer C60, yang merupakan perangkat dengan teknologi Wifi generasi lama. Keterbatasan spesifikasi perangkat ini, seperti kapasitas koneksi klien terbatas dan tidak adanya dukungan manajemen terpusat, turut menjadi faktor penghambat dalam optimalisasi performa jaringan. Dalam pengujian lapangan, perangkat ini tidak mampu mendistribusikan *bandwidth* secara maksimal, terutama ketika digunakan secara bersamaan oleh banyak pengguna.



Gambar IV. 4 Tampilan Setting Jaringan Nirkabel yang belum dioptimalisasikan



Gambar IV. 5 *Bandwidth* Jaringan Nirkabel yang belum dioptimalisasikan

Gambar di atas menunjukkan hasil pengujian kecepatan internet pada jaringan eksisting yang masih menggunakan perangkat *access point* TP-Link Archer C60. Berdasarkan pengujian tersebut, terlihat bahwa distribusi *bandwidth* tidak merata dan kecepatan akses internet tidak mencerminkan kapasitas maksimal yang disediakan oleh pihak ISP. Hal ini menandakan bahwa manajemen *bandwidth* belum berjalan secara efisien dan optimal. Salah satu penyebab utama ketidakefisienan ini adalah tidak adanya pengaturan pembagian *bandwidth* minimum dan maksimum untuk setiap pengguna. Ketika beberapa pengguna melakukan aktivitas berat seperti mengunduh file dalam waktu yang bersamaan, maka terjadi persaingan *bandwidth* yang menyebabkan pengguna lain mengalami penurunan kecepatan akses, meskipun mereka hanya melakukan aktivitas ringan seperti browsing atau mengakses aplikasi administratif.

Selain itu, ketiadaan fitur *Quality of Service* (QoS) dalam sistem jaringan saat ini menyebabkan seluruh jenis trafik diperlakukan sama, tanpa adanya prioritas untuk layanan penting. Akibatnya, performa jaringan menjadi tidak stabil, terutama pada jam kerja dengan beban tinggi.

4.2.2 Pengujian Jaringan Akhir

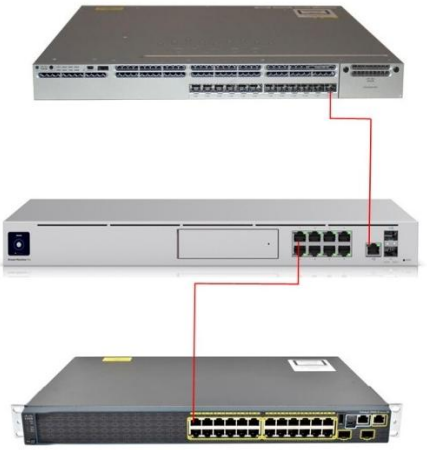
Manajemen *bandwidth* yang sebelumnya belum berjalan secara optimal kini telah ditingkatkan melalui penerapan perangkat baru, yaitu Unifi Cloud Gateway sebagai komponen utama dalam pengelolaan bandwidth dan penerapan *Quality of Service* (QoS), serta Unifi U6 Lite sebagai perangkat *access point* untuk mendukung performa jaringan nirkabel yang lebih stabil dan efisien.

Proses konfigurasi Unifi Cloud Gateway dilakukan melalui Unifi Dashboard, sebuah antarmuka manajemen berbasis web yang memungkinkan pengaturan jaringan dilakukan secara terpusat dan *real time*. Seluruh tahapan konfigurasi, mulai dari instalasi perangkat, pengaturan *bandwidth*, hingga penerapan QoS, dilaksanakan langsung oleh penulis sebagai bagian dari implementasi sistem.

Adapun hasil dari tahapan konfigurasi secara menyeluruh, mulai dari tahap awal hingga akhir, dijelaskan pada bagian berikut:

1. **Pemasangan Unifi Cloud Gateway**

   Gambar dibawah menunjukkan skema penempatan perangkat Unifi Cloud Gateway dalam infrastruktur jaringan yang telah dikonfigurasi. Perangkat ini ditempatkan setelah SDWAN Aruba, dengan koneksi dari port 4 pada SDWAN menuju port WAN pada Unifi Cloud Gateway. Selanjutnya, koneksi dari port LAN 1 pada Unifi Cloud Gateway diarahkan ke switch distribusi, yang berfungsi untuk mendistribusikan alamat IP VLAN kepada seluruh perangkat jaringan. Pengaturan VLAN ini telah dikonfigurasi sebelumnya melalui antarmuka Unifi Cloud Gateway.



Gambar IV. 6 Skema Pemasangan Unifi Cloud Gateway

2. Pemasangan Unifi U6 Lite

Gambar dibawah menunjukkan proses pemasangan perangkat *Access Point* Unifi U6 Lite dalam jaringan. Koneksi dilakukan dari switch distribusi menuju ke perangkat PoE (*Power over Ethernet*) *injector*, kemudian dilanjutkan dari PoE ke port pada *Access Point* Unifi U6 Lite.

Penggunaan PoE ini bertujuan untuk menyuplai daya listrik dan data internet melalui satu kabel Ethernet (UTP), sehingga tidak memerlukan adaptor listrik terpisah. Dengan demikian, pemasangan *Access Point* menjadi lebih praktis dan efisien, terutama pada area yang terbatas sumber listrik.

Gambar IV. 7 Skema Pemasangan Access Point Unifi U6 Lite

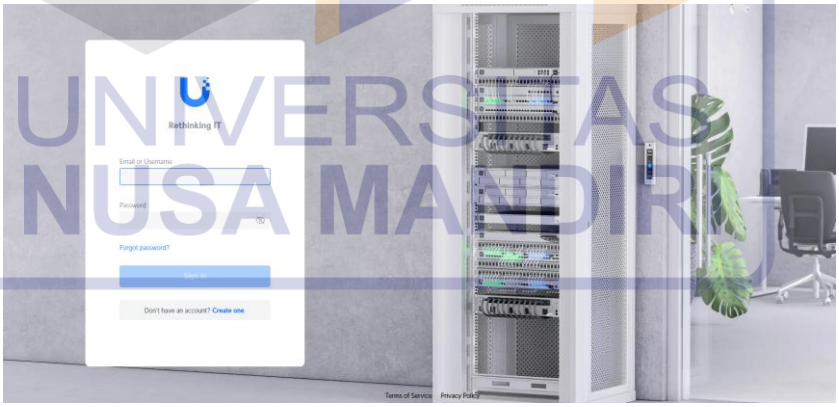
Setelah perangkat Unifi Cloud Gateway terhubung dengan jaringan melalui sambungan kabel, langkah pertama yang harus dipastikan adalah bahwa perangkat telah memperoleh koneksi internet secara stabil. Koneksi ini penting sebagai syarat utama agar perangkat dapat terhubung ke platform manajemen cloud milik Unifi.

Selanjutnya, proses konfigurasi dilakukan melalui Unifi Dashboard, yaitu antarmuka berbasis web yang dapat diakses menggunakan browser dengan membuka tautan resmi di alamat: https://unifi.ui.com. Melalui dashboard ini, administrator dapat melakukan proses setup awal dan manajemen jaringan secara terpusat.

Berikut adalah tahapan konfigurasi awal Unifi Cloud Gateway:

1) Akses Unifi Dashboard

Buka browser dan kunjungi laman https://unifi.ui.com. Login menggunakan akun Unifi yang telah terdaftar.



Gambar IV. 8 Dashboard Unifi

2) Setting Perangkat Unifi Cloud Gateway

Setelah masuk ke dashboard, dalam tahap konfigurasi jaringan yang dilakukan adalah menetapkan alamat IP statis pada port WAN pada port 9 di perangkat Unifi Cloud Gateway. Pemberian *IP Address* ini bertujuan agar perangkat dapat

terhubung langsung ke jaringan utama dan memperoleh akses ke internet. Konfigurasi ini dilakukan melalui Unifi Dashboard, dengan cara memilih antarmuka WAN dan memasukkan informasi *IP Address, subnet mask, gateway* dan *DNS* yang sesuai dengan skema jaringan instansi.

Setelah konektivitas internet berhasil dikonfigurasi melalui port WAN, langkah selanjutnya adalah melakukan pembuatan *Virtual Local Area Network* (VLAN). VLAN digunakan untuk memisahkan trafik jaringan berdasarkan fungsi atau unit kerja, sehingga meningkatkan efisiensi dan keamanan jaringan. Melalui antarmuka Unifi, dapat menentukan ID VLAN, nama VLAN, serta subnet IP yang digunakan.

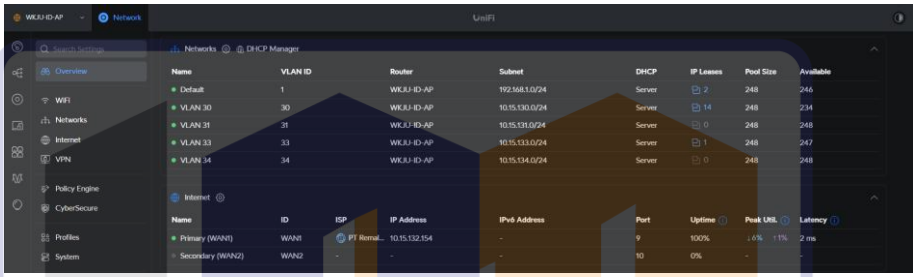
Berikut langkah-langkah untuk konfigurasi *IP Address* pada port WAN:

a. Masuk ke Menu Settings di Unifi Dashboard
b. Pilih Submenu Internet
c. Pilih Interface WAN pada port 9
d. Masukan Konfigurasi *IP Address* statis yang meliputi:
   1. *IP Address*
   2. Subnet Mask
   3. Default Gateway
   4. DNS Server
e. Simpan pengaturan untuk menerapkan konfigurasi.

Berikut langkah-langkah untuk menambahkan VLAN untuk *Access Point*:

a. Masuk ke menu setting
b. Pilih submenu network
c. Klik tombol *Create New Network*
d. Tentukan parameter VLAN, meliputi:

1. VLAN 30, VLAN, 31, VLAN 33 dan VLAN 34
2. I*P Address* dan *Subnet Range* yang sudah ditentukan
3. Atur DHCP range untuk Pengaturan rentang DHCP dilakukan untuk menentukan alokasi alamat IP secara otomatis kepada klien yang terhubung ke jaringan.
4. Simpan pengaturan untuk menerapkan konfigurasi.

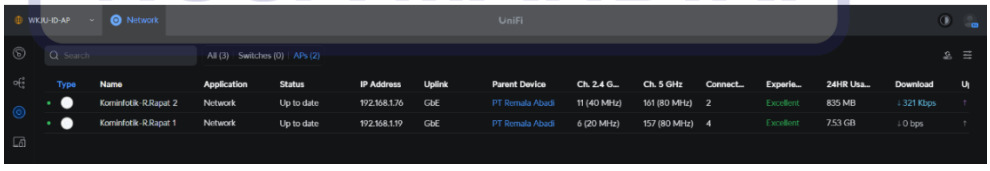


Gambar IV. 9 Dashboard Unifi Setting *IP Address* dan Setting VLAN

3) Adopsi dan Konfigurasi Perangkat Unifi U6 Lite

Proses adopsi perangkat untuk menghubungkan Cloud Gateway ke sistem manajemen Unifi. Pastikan perangkat memiliki status *Connected* setelah proses ini selesai.

Setelah adopsi perangkat selesai, lalu atur parameter dasar seperti zona waktu, lokasi jaringan, dan informasi perangkat.



Gambar IV. 10 Dashboard Unifi Adopsi Perangkat

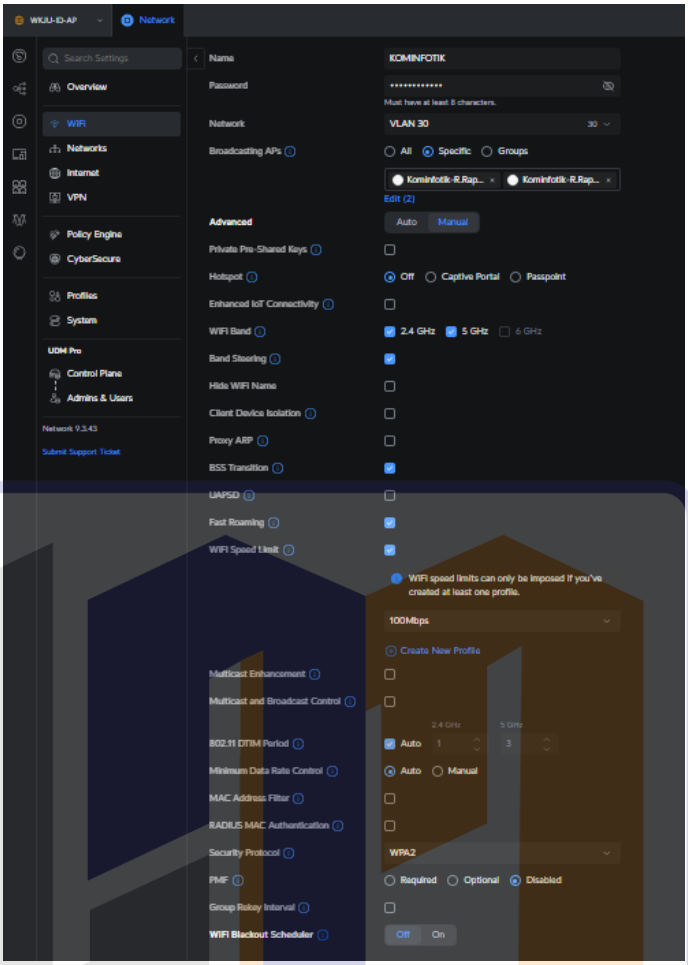
a. Pembuatan SSID (*Service Set Identifier*)

Pengaturan SSID dilakukan untuk menetapkan nama jaringan nirkabel yang akan digunakan oleh pengguna dalam mengakses jaringan. Dalam penelitian ini, penulis melakukan konfigurasi melalui Unifi Dashboard dengan membuat

dua SSID, yaitu KOMINFOTIK untuk klien umum dan KOMINFOTIK AP untuk administrator. Pemisahan SSID ini bertujuan untuk membedakan segmentasi akses jaringan sesuai kebutuhan pengguna. Selanjutnya, masing-masing SSID dikaitkan dengan VLAN berbeda, yakni VLAN 30 untuk klien umum dan VLAN 33 untuk klien admin, guna memisahkan trafik jaringan berdasarkan jenis pengguna dan mendukung pengelolaan akses serta keamanan yang lebih efektif.

Selain itu, penulis juga mengaktifkan fitur *Fast Roaming* yang tersedia pada submenu konfigurasi SSID. Fitur ini memungkinkan perangkat klien untuk berpindah antar *access point* secara cepat dan *seamless* tanpa kehilangan koneksi, sehingga sangat mendukung mobilitas pengguna di lingkungan kerja yang dinamis. Penulis juga menerapkan metode keamanan WPA2 dengan pengaturan kata sandi yang kuat sebagai bentuk perlindungan akses jaringan. Setelah seluruh konfigurasi selesai, pengaturan disimpan untuk diterapkan secara permanen ke sistem.

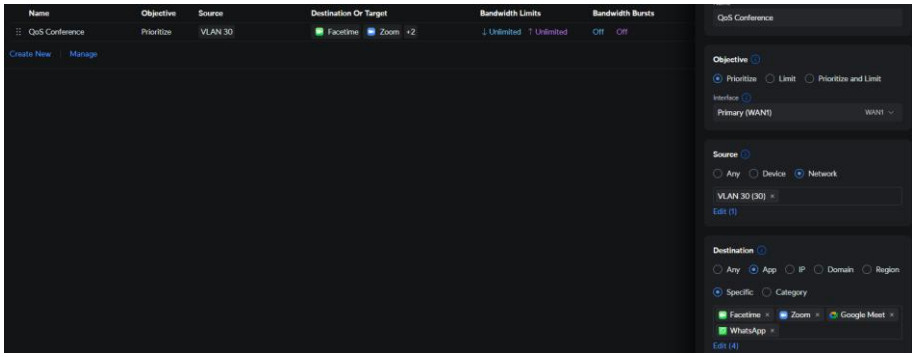
Gambar IV. 11 Dashboard Unifi Daftar SSID



Gambar IV. 12 Dashboard Unifi Daftar setting SSID

b. Konfigurasi *Quality of Service* (QoS)

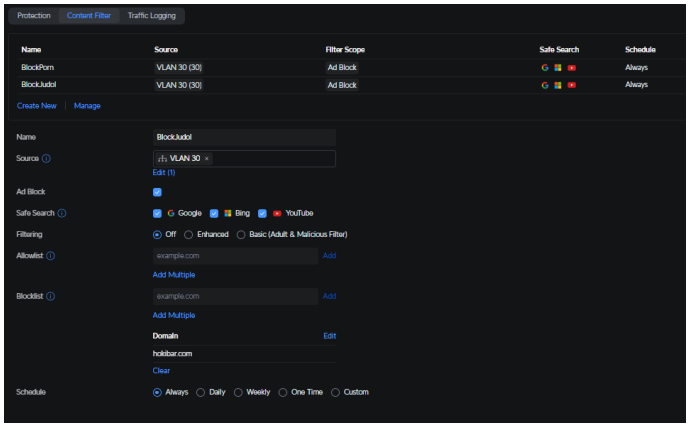
Penulis melakukan konfigurasi QoS pada jaringan VLAN 30 melalui antarmuka Unifi Dashboard sebagai upaya untuk meningkatkan kualitas koneksi khususnya pada aplikasi konferensi daring. Dalam konfigurasi ini, penulis menetapkan prioritas *bandwidth* untuk beberapa aplikasi penting seperti Zoom, Google Meet, Facetime, WhatsApp. Sebelumnya, jaringan Wifi yang digunakan oleh klien umum kerap mengalami *disconnect* mendadak, terutama saat terjadi kepadatan trafik. Dengan pengaturan QoS ini, trafik jaringan dapat dikendalikan secara lebih efisien, sehingga koneksi menjadi lebih stabil, responsif dan mendukung aktivitas komunikasi daring secara optimal.



Gambar IV. 13 Dashboard Unifi Daftar setting QoS

c. Block Situs

Penulis melakukan konfigurasi *Content Filtering* melalui submenu *Cybersecure* pada Unifi Dashboard sebagai bagian dari penguatan sistem *firewall* untuk membatasi akses konten pada jaringan klien umum, yaitu SSID KOMINFOTIK yang menggunakan VLAN 30. Pengaturan ini bertujuan untuk meningkatkan keamanan jaringan dengan mengendalikan akses terhadap situs-situs yang tidak sesuai dengan kebijakan penggunaan. Pada konfigurasi ini, fitur *SafeSearch* diaktifkan agar pencarian melalui mesin pencari seperti Google dapat difilter secara menyeluruh, sehingga mencegah munculnya konten yang tidak pantas. Selain itu, penulis menambahkan daftar domain secara manual melalui fitur *Blocklist* untuk memblokir situs tertentu secara spesifik. Pengaturan *schedule block* diset pada opsi *Always*, yang berarti pemblokiran akan diterapkan secara terus-menerus tanpa batas waktu tertentu. Seluruh pengaturan ini merupakan bagian dari penerapan *firewall* berbasis aplikasi yang bertujuan untuk menjaga jaringan tetap aman, terkendali dan selaras dengan kebijakan keamanan yang telah ditetapkan.



Gambar IV. 14 Dashboard Unifi Content Filter BlockJudol

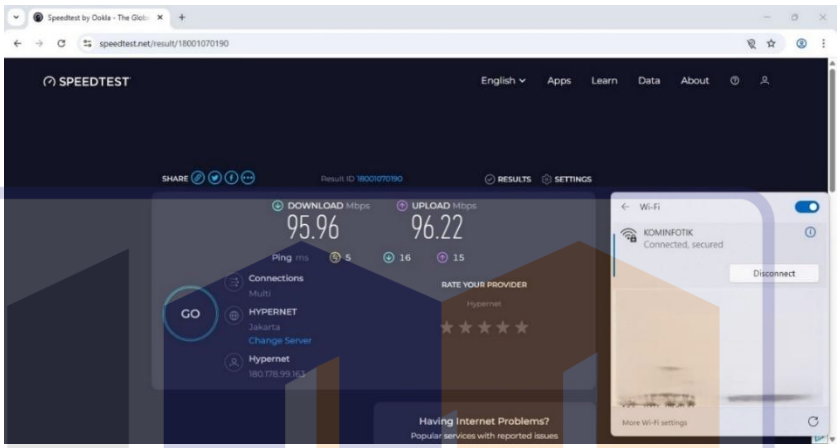
Gambar IV. 15 Dashboard Unifi Content Filter BlockPorn

3. Pengujian Jaringan

1) Management *Bandwidth*

Penulis membedakan konfigurasi SSID berdasarkan kategori pengguna sebagai bagian dari strategi manajemen *bandwidth* yang optimal. SSID KOMINFOTIK, yang ditujukan untuk klien umum, dikonfigurasi dengan batas kecepatan internet sebesar 100 Mbps guna menjaga kestabilan dan efisiensi distribusi bandwidth di lingkungan jaringan. Sementara itu, SSID KOMINFOTIK AP yang diperuntukkan bagi administrator diberikan akses tanpa batasan kecepatan hingga 350 Mbps, untuk memastikan kelancaran dalam melakukan pemantauan, konfigurasi dan pengelolaan sistem jaringan

secara menyeluruh. Hasil implementasi ini menunjukkan bahwa pengaturan QoS menggunakan Unifi Cloud Gateway mampu membagi prioritas akses jaringan secara tepat sesuai dengan peran dan kebutuhan masing-masing pengguna.



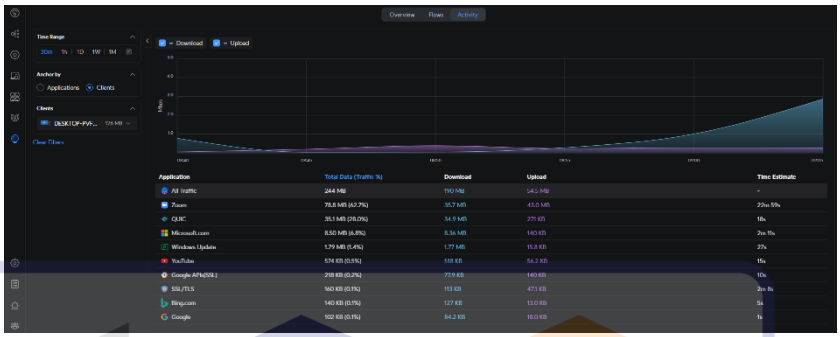
Gambar IV. 16 *Bandwidth* untuk Klien Umum

Gambar IV. 17 *Bandwidth* untuk Administrator

2) Prioritas *video conference*

Penulis dapat memantau lalu lintas data secara *real time* dan mengevaluasi efektivitas kebijakan QoS yang diterapkan. Dari data yang ditampilkan, terlihat bahwa aplikasi *video conference* mendominasi penggunaan *bandwidth* dengan konsumsi mencapai 78,8 MB dengan persentase 62,7% dari total trafik klien. Hal ini menunjukkan bahwa kebijakan QoS berhasil mengalokasikan prioritas

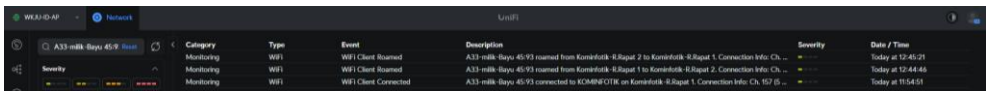
bandwidth dengan tepat untuk aplikasi yang membutuhkan koneksi stabil dan *real time*, seperti Zoom, yang umumnya digunakan untuk keperluan komunikasi video dan rapat daring.



Gambar IV. 18 Prioritas *video conference*

3) Fitur *Roaming*

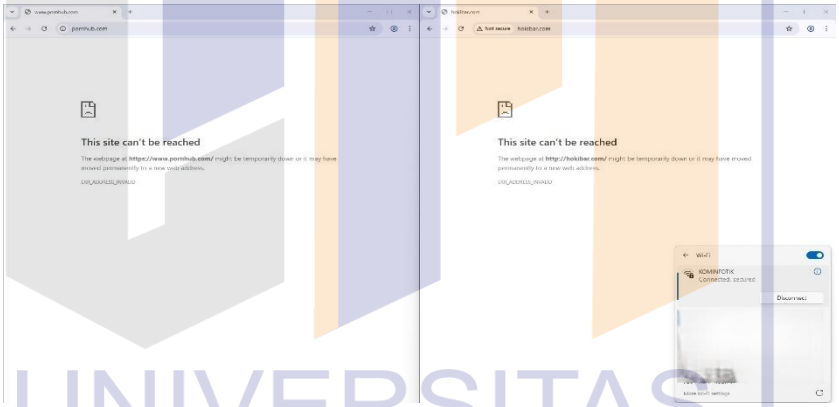
Untuk fitur *fast roaming* pada sistem jaringan nirkabel telah berjalan dengan baik. Hal ini ditunjukkan oleh adanya catatan peristiwa *Wifi Client Roamed* yang merekam perpindahan perangkat klien secara otomatis dari satu AP ke AP lainnya. Fitur *roaming* ini terjadi tanpa adanya gangguan koneksi atau pemutusan akses, yang menandakan bahwa proses transisi antar AP berlangsung mulus dan responsif. Fitur ini sangat penting untuk memastikan konektivitas tetap stabil terutama bagi pengguna yang berpindah tempat di dalam area jangkauan jaringan, seperti saat melakukan panggilan video atau aktivitas penting lainnya. Dengan demikian, penerapan *fast roaming* memberikan dampak positif terhadap kualitas layanan jaringan nirkabel secara keseluruhan, sekaligus mendukung efisiensi mobilitas pengguna di lingkungan kerja.



Gambar IV. 19 Fitur Roaming

4) Block Konten Terlarang

Sebagai bagian dari implementasi penguatan keamanan jaringan, penulis melakukan konfigurasi pemblokiran terhadap situs-situs yang dikategorikan sebagai konten terlarang melalui fitur *Content Filtering* pada Unifi Dashboard. Dalam konfigurasi ini, penulis secara khusus menambahkan domain situs judi online yang saat ini marak diakses, serta situs-situs dengan konten dewasa yang dinilai tidak sesuai dengan kebijakan penggunaan jaringan. Pemblokiran ini diterapkan pada VLAN 30 yang digunakan oleh klien umum dengan SSID KOMINFOTIK, tujuannya untuk menjaga integritas jaringan serta menciptakan lingkungan digital yang aman.



Gambar IV. 20 Block Konten Terlarang

4. Hasil Parameter QoS menggunakan Wireshark

File

Name:	C:\Users\Lenovo\AppData\Local\Temp\wireshark_Wi-FiE95LD3.pcapng
Length:	2365 kB
Hash (SHA256):	310d3c6c9ce52de4d577dcad103641518cc76c9a00f0d1543476705c8b52dafb
Hash (SHA1):	54013dd8508bb7ed671ab27dfe1d0ab13f6ee9c8
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2025-10-02 14:27:17
Last packet:	2025-10-02 14:28:41
Elapsed:	00:01:24

Capture

Hardware:	13th Gen Intel(R) Core(TM) i5-13420H (with SSE4.2)
OS:	64-bit Windows 11 (24H2), build 26100
Application:	Dumpcap (Wireshark) 4.4.9 (v4.4.9-0-g57bf67214076)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	8117	8117 (100.0%)	—
Time span, s	84.173	84.173	—
Average pps	96.4	96.4	—
Average packet size, B	258	258	—
Bytes	2094870	2094870 (100.0%)	0
Average bytes/s	24 k	24 k	—
Average bits/s	199 k	199 k	—

Gambar IV. 21 Hasil Test Wireshark Access Point Lama

File

Name:	C:\Users\Lenovo\AppData\Local\Temp\wireshark_Wi-FiLOTPD3.pcapng
Length:	148 kB
Hash (SHA256):	19e1a08f5ba377f956c172e790d78e397dceab6b871cdf4669a4d8bc0898a64d
Hash (SHA1):	53111164d21f4d2df0e69240b46eb0ef2f6482e2
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2025-10-01 11:31:13
Last packet:	2025-10-01 11:33:07
Elapsed:	00:01:53

Capture

Hardware:	13th Gen Intel(R) Core(TM) i5-13420H (with SSE4.2)
OS:	64-bit Windows 11 (24H2), build 26100
Application:	Dumpcap (Wireshark) 4.4.9 (v4.4.9-0-g57bf67214076)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	633	633 (100.0%)	—
Time span, s	113.723	113.723	—
Average pps	5.6	5.6	—
Average packet size, B	200	200	—
Bytes	126699	126699 (100.0%)	0
Average bytes/s	1114	1114	—
Average bits/s	8912	8912	—

Gambar IV. 22 Hasil Test Wireshark Access Point Baru

Dari hasil pengukuran kualitas jaringan nirkabel di Kantor Walikota Administrasi Jakarta Utara, terlihat adanya perbedaan signifikan antara perangkat TP-Link Archer C60 yang digunakan sebelum instalasi dengan UniFi U6 Lite setelah dilakukan pergantian access point. Parameter QoS

seperti *throughput, delay, jitter*, dan *packet loss* menunjukkan bahwa UniFi U6 Lite memberikan kinerja yang lebih stabil dan optimal dibandingkan dengan TP-Link Archer C60. Hal ini menunjukkan bahwa pergantian perangkat access point berpengaruh terhadap peningkatan kualitas layanan jaringan nirkabel. Berikut hasil yang ditunjukan pada Tabel IV. 1 dan Tabel IV. 2

Tabel IV. 1 Parameter QoS Access Point Sebelum Implementasi

Parameter QoS	Hasil Pengukuran	Standar TIPHON
Throughput	199 kb/s	0
Packet Loss	0,02 %	4
Jitter	0.03 ms	3
Delay	10.369 ms	3

Tabel IV. 2 Parameter QoS Access Point Setelah Implementasi

Parameter QoS	Hasil Pengukuran	Standar TIPHON
Throughput	8,912	4
Packet Loss	0,2 %	4
Jitter	1.67 ms	3
Delay	179.657035 ms	3

Berdasarkan hasil perhitungan yang ditunjukan pada Tabel IV. 1 dan Tabel IV. 2 yang dilakukan terhadap analisis jaringan nirkabel di Kantor Walikota Administrasi Jakarta Utara menggunakan aplikasi Wireshark, diperoleh nilai *throughput* sebesar 8,912 kb/s atau 8,9 Mb/s. Mengacu pada standar TIPHON, nilai tersebut dikategorikan sangat baik karena berada di atas 2,1 Mb/s. Selanjutnya, hasil perhitungan *packet loss* menunjukkan nilai sebesar 0,2%. Berdasarkan standar TIPHON, nilai ini juga termasuk dalam kategori sangat baik karena berada di bawah ambang batas 2%. Untuk parameter *delay*, diperoleh hasil sebesar 179,65 ms yang menurut standar TIPHON masuk dalam kategori baik. Sementara itu, hasil perhitungan *jitter*

menunjukkan nilai sebesar 1,67 ms dan dapat dikategorikan baik sesuai dengan standar TIPHON.

Pergantian access point dari TP-Link Archer C60 ke UniFi U6 Lite terbukti berhasil meningkatkan kualitas layanan jaringan nirkabel. Peningkatan ini terlihat dari kestabilan *throughput*, rendahnya nilai *packet loss*, serta perbaikan pada parameter *delay* dan *jitter*. Secara keseluruhan, implementasi perangkat UniFi U6 Lite memberikan pengalaman jaringan yang lebih responsif, stabil dan andal dibandingkan penggunaan perangkat sebelumnya.