BAB IV

HASIL PENELITIAN

4.1 Pendahuluan

Bab ini menjelaskan hasil dari implementasi infrastruktur jaringan pada gedung perusahaan travel agent berdasarkan desain dan konfigurasi yang telah dilakukan. Pembahasan mencakup pengujian koneksi antar perangkat, pembagian jalur provider, pengaturan akses WiFi untuk pegawai dan Guest, serta penerapan filter MAC address. Setiap pengujian yang dilakukan akan dijelaskan hasilnya untuk memastikan jaringan berjalan sesuai rancangan.

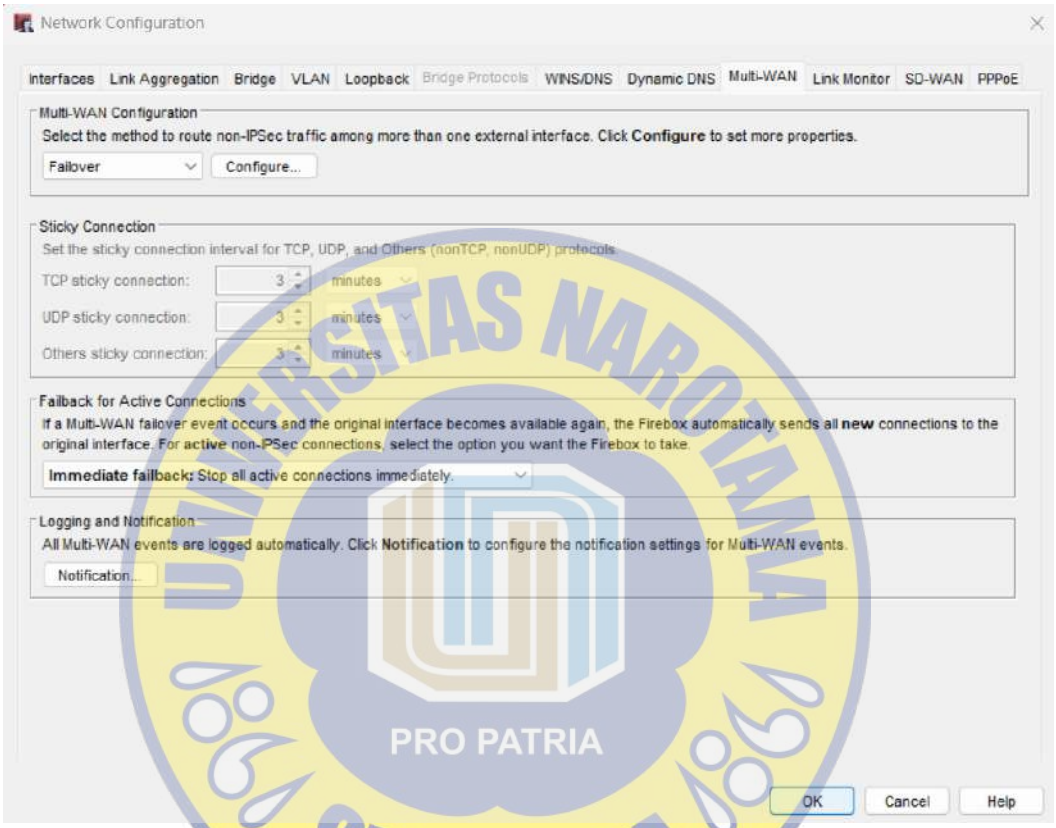
4.2 Hasil Implementasi Infrastruktur Jaringan

4.2.1 Konfigurasi ISP dan Distribusi Internet di WatchGuard

Gambar 4.1 Pembagian jalur ISP pada WatchGuard Firewall

WatchGuard Firewall diposisikan untuk melindungi jaringan dari ancaman eksternal dan untuk pembatasan akses browsing. Namun, konfigurasi spesifik firewall ini tidak termasuk dalam fokus penelitian ini. Fungsinya hanya dijelaskan sebagai bagian dari infrastruktur.

Untuk IP yang dipasang di WatchGuard yaitu ***10.0.3.1/24***, yang tersebut juga akan di pasang di list IP Address pada setiap lantai. Konfigurasi Multi-WAN "Failover" di WatchGuard bertujuan untuk membackup jaringan utama apabila downtime loss rate mendekati angka 25%.



Gambar 4.2 Konfigurasi Jaringan Multi-WAN WatchGuard

Berikut struktur ISP pada Gedung :

- ISP 1 (250 Mbps) :

  ISP 1 digunakan untuk kebutuhan jaringan lokal gedung. Digunakan untuk mendukung kebutuhan internal jaringan lokal gedung. ISP ini memiliki bandwidth hingga 250 Mbps yang didistribusikan ke seluruh lantai melalui MikroTik Distribusi.

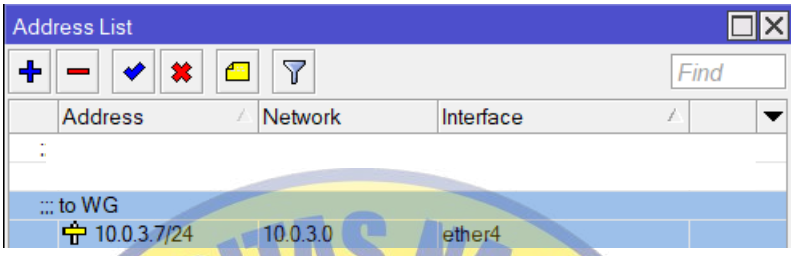
- ISP 2 (100 Mbps 1:1) :

  ISP 2 digunakan untuk akses ke server berbasis cloud, email, dan kebutuhan akses internet eksternal yang lebih kritis. Bandwidth 1:1 menjamin performa stabil tanpa fluktuasi.

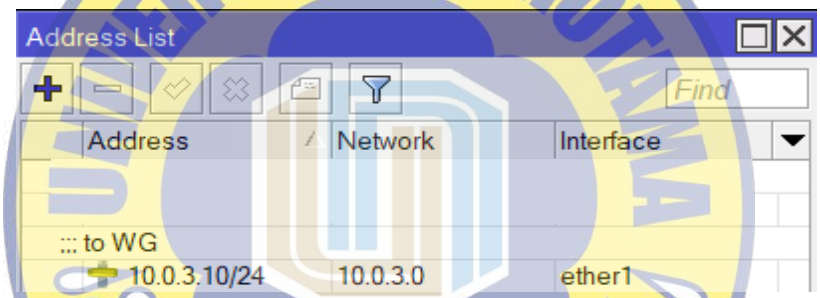
4.2.2 Konfigurasi Mikrotik per Lantai

4.2.2.1 Konfigurasi Routes ke WatchGuard

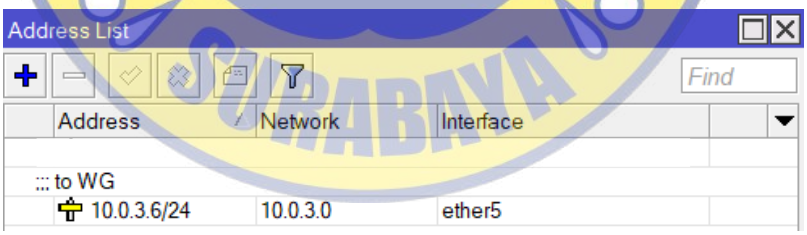
Seperti yang di jelaskan diatas sebelumnya, IP perangkat pada alat WatchGuard ialah 10.0.3.1/24. Maka dari itu perlu adanya tambahan IP Address dan IP Routes untuk mendapatkan akses internet di setiap mikrotik per lantai.



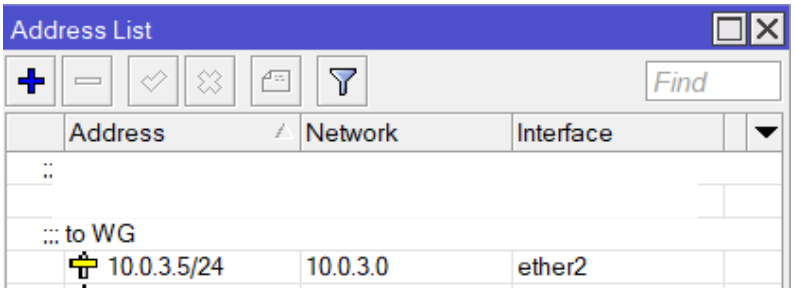
Gambar 4.3 IP Address List lt.1



Gambar 4.4 IP Address List lt.2



Gambar 4.5 IP Address List lt.3



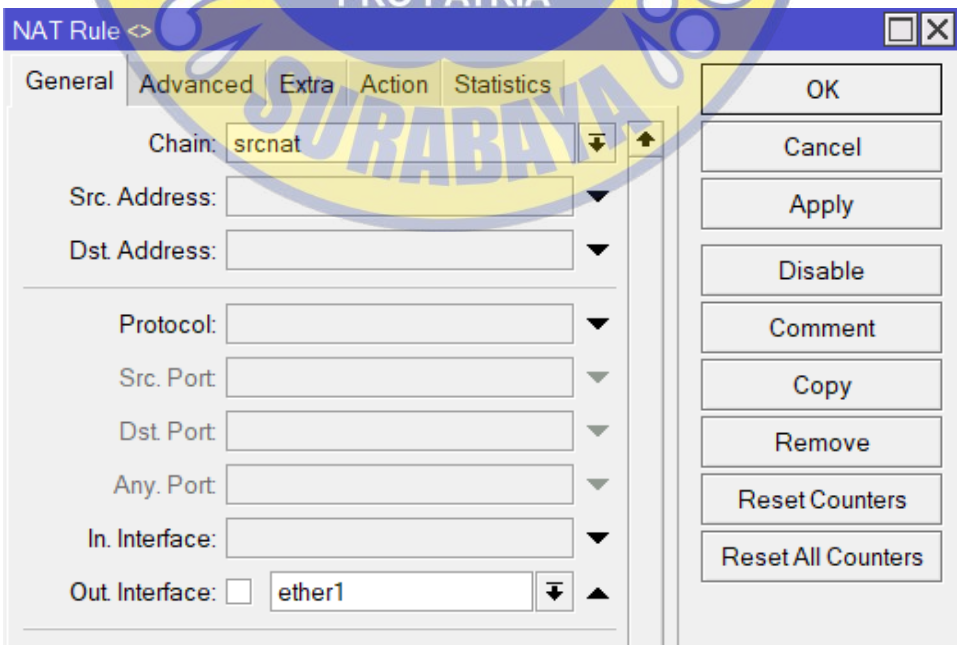
Gambar 4.6 IP Address List lt.4

Apabila IP Address sudah di tambahkan, maka pada IP Routes sudah otomatis tertambah dengan sendirinya dengan status “Reachable”.

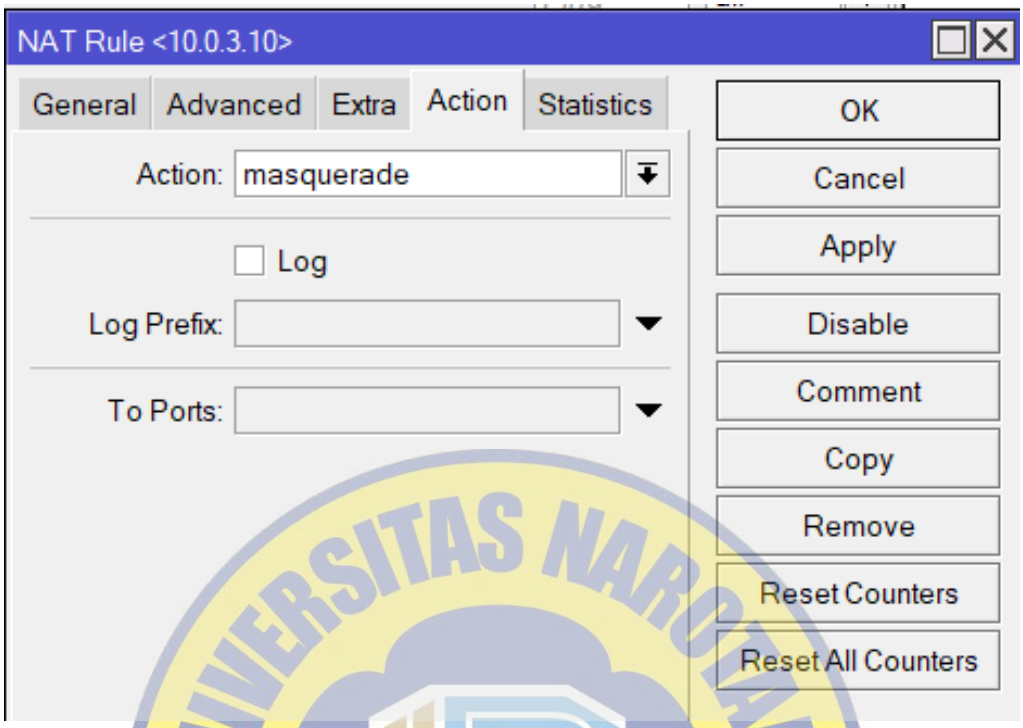
Gambar 4.7 IP Routes List lt.1

4.2.2.2 Konfigurasi Firewall NAT pada mikrotik

Penggunaan NAT pada mikrotik bertujuan untuk mengubah sumber IP yang keluar dari Jaringan Local menjadi internet.



Gambar 4.8 NAT Rule General



Gambar 4.9 NAT Rule Action

Penjelasan:

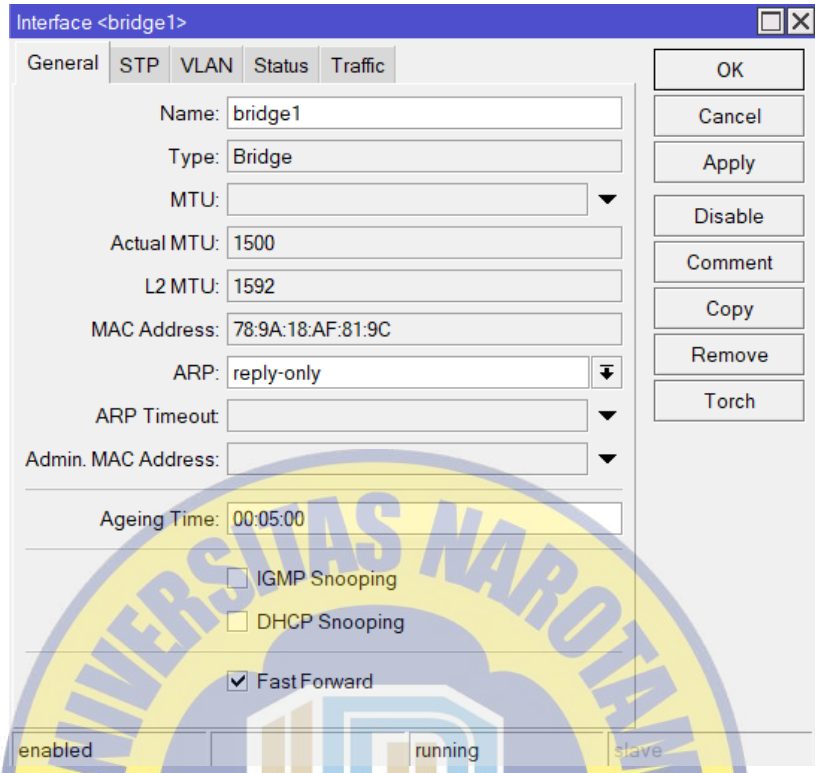
- Chain = srcnat: Menentukan bahwa aturan NAT ini berlaku untuk paket dengan alamat IP sumber.
- Action = masquerade: Menggunakan IP publik yang ada pada antarmuka ether1 untuk mengakses internet.
- out-interface = ether1: Menentukan yang terhubung ke ISP

4.2.2.3 Konfigurasi Bridge

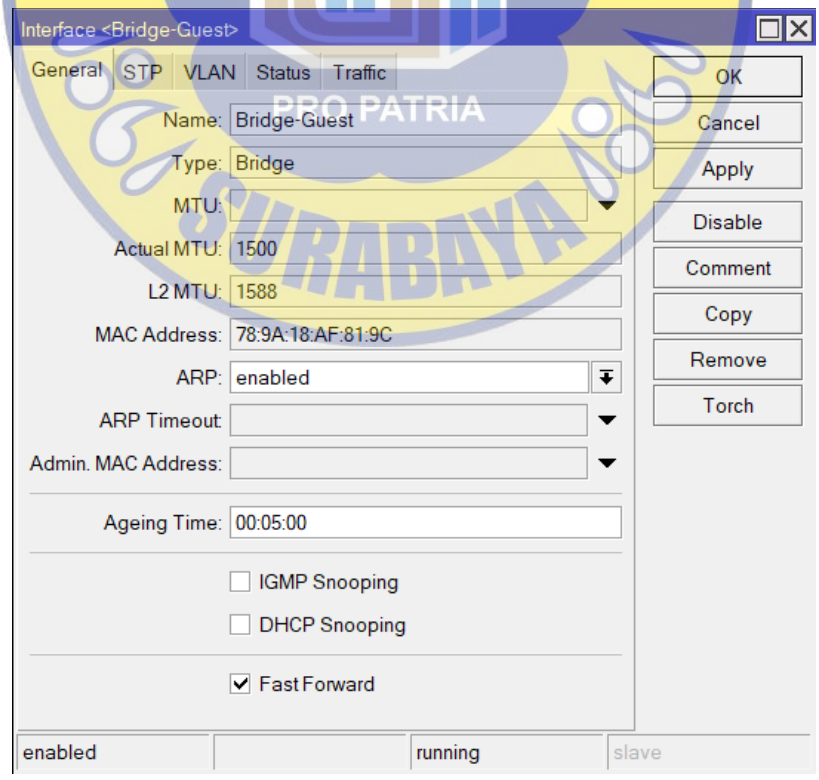
Bridge di siapkan untuk pengelolaan jaringan pemisah antara Wi-Fi Karyawan dengan Guest, dan untuk penerapan MAC Address Filtering. Konfigurasi ini diterapkan pada Mikrotik lt.1, lt.2, lt.3 dan lt.4. Sebagai contoh Konfigurasi, saya menggunakan mikrotik dari lt.2.

a. Konfigurasi bridge sebagai pemisah antara Wi-Fi Karyawan dan Guest.

   Terdapat perbedaan konfigurasi bridge untuk mengamankan ip dhcp, perbedaan tersebut dapat di lihat pada gambar dibawah serta di penjelasan di bawah :



Gambar 4.10 Bridge Wi-Fi Karyawan

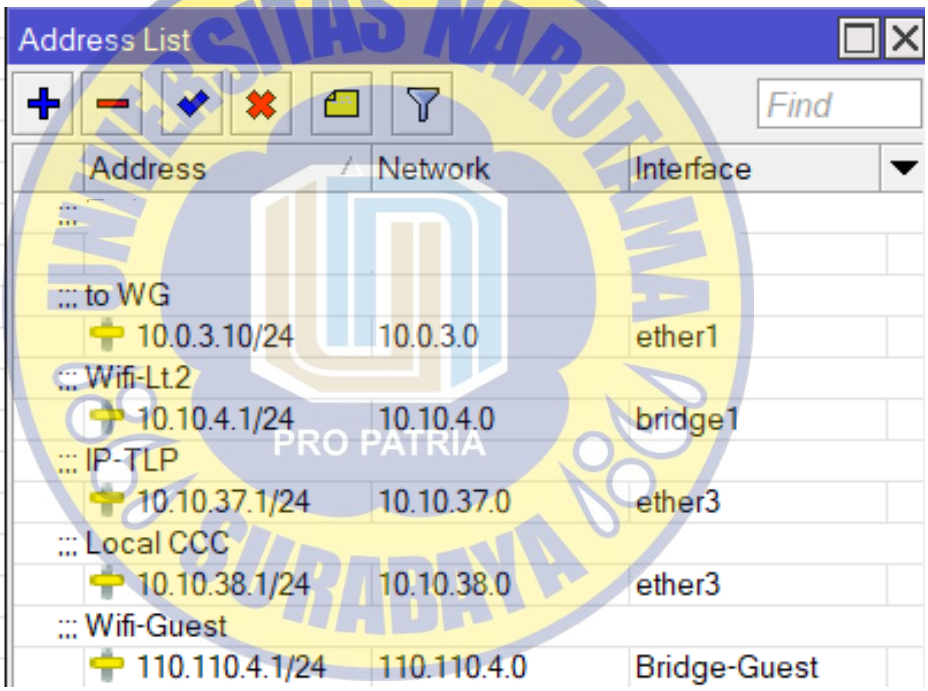


Gambar 4.11 Bridge Wi-Fi Guest

Penjelasan :

- ARP : Enabled diatas akan membuat mengijinkan interkoneksi client yang mendapatkan ip address dari proses DHCP.
- ARP : Reply-Only diatas akan membuat router hanya mengijinkan interkoneksi client yang mendapatkan ip address dari proses DHCP. User yang melakukan setting ip address manual justru tidak bisa interkoneksi ke router.

b. Penambahan IP Address untuk bridge



Gambar 4.12 IP Address bridge

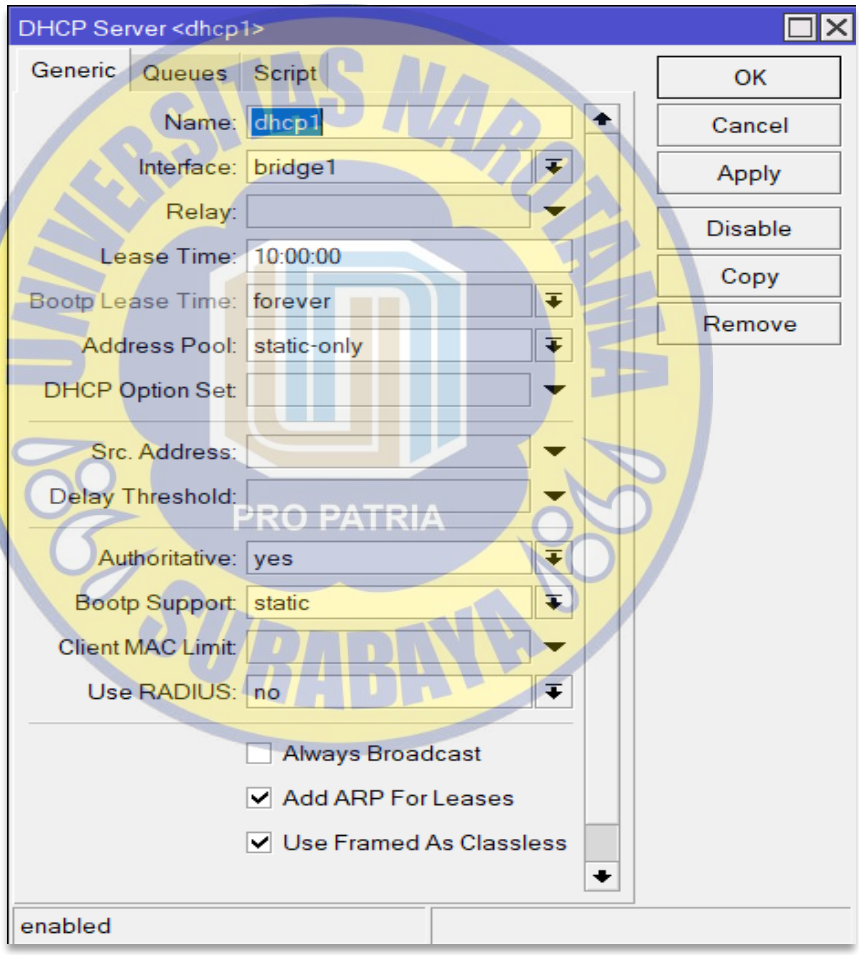
Penjelasan :

- IP Wi-Fi lt.2 dengan IP Wi-Fi Guest berbeda dikarenakan untuk memudahkan deteksi IP yang tertera pada DHCP Lease di mikrotik.
- Untuk IP Local CCC digunakan untuk PC dan Printer yang terkoneksi dengan LAN.
- IP Tlp digunakan untuk pemberian IP yang di setup pada perangkat telp Yealink.

c. Konfigurasi bridge dan DHCP Server sebagai MAC Address Filtering.

Pada Konfigurasi Bridge Karyawan, dapat dilihat sebelumnya bahwa terdapat perbedaan ARP pada bridge-Guest dengan bridge1. Dikarenakan Router hanya akan meresponse request client dengan kombinasi IP Address dan MAC Address yang sesuai dengan tabel ARP tanpa menambahkan entri ARP secara otomatis.

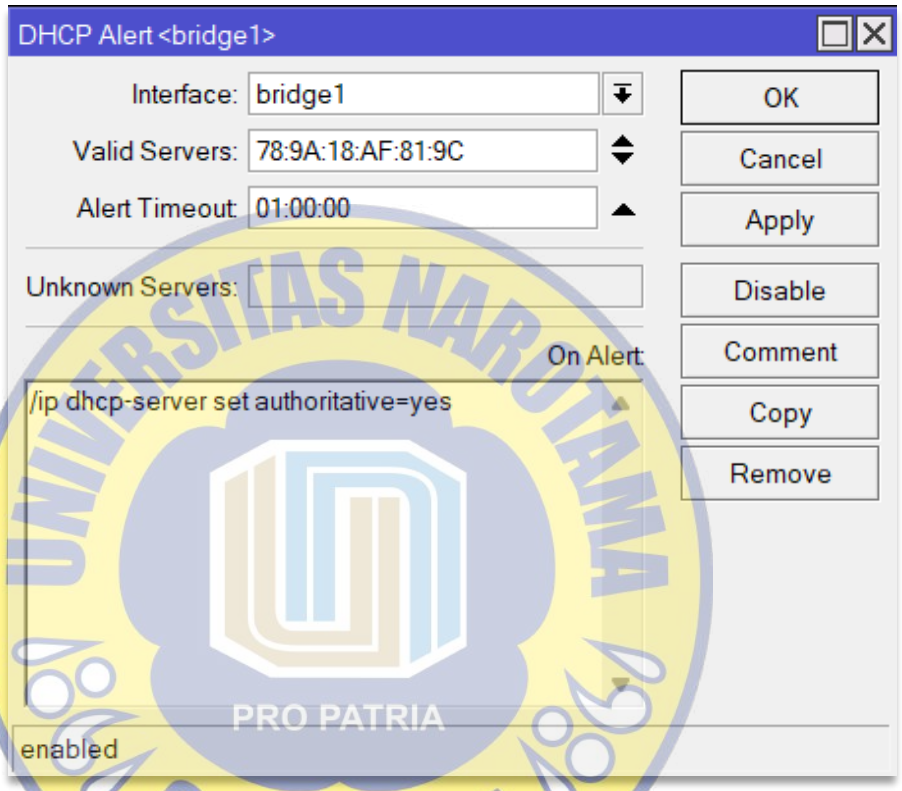
Pada tab DHCP Server, ubah Address Pool menjadi static-only dan centang Add ARP for Leases.



Gambar 4.13 DHCP Server General

Selanjutnya juga bisa membatasi lagi perangkat yang terkoneksi via DHCP Server hanya perangkat yang sudah kita tentukan saja. Untuk kebutuhan tersebut bisa mengatur parameter pada DHCP Server yaitu Address Pool dengan di-set ke opsi 'Static-Only'.

Masih pada tab DHCP Server, pada tab Alert terdapat perubahan interface, penambahan MAC Address bridge1, dan penambahan script */ip dhcp-server set authoritative=yes*, yang digunakan untuk mendeteksi adanya multiple dhcp server pada satu jaringan yang sama.

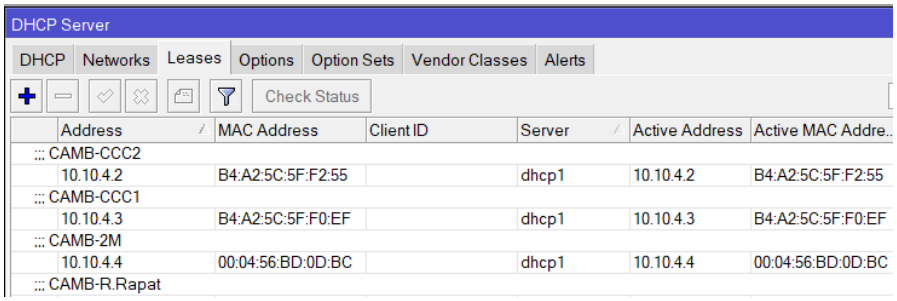


Gambar 4.14 DHCP Alert

d. Penambahan MAC Address Karyawan.

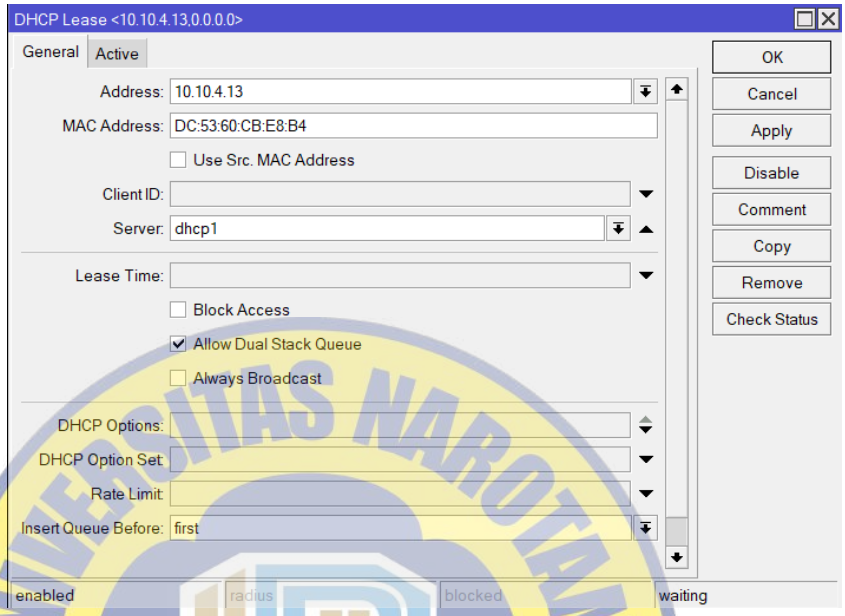
Penambahan MAC Address bisa di lakukan secara manual maupun dengan script.

Berikut contoh penambahan dilakukan secara manual :



Gambar 4.15 DHCP Lease

Pada DHCP Lease, Klik (+) maka akan muncul tab pada gambar dibawah



Gambar 4.16 DHCP Lease

Isi IP Address dengan segment ip yang sudah di tentukan sebelumnya, isi MAC Address yang sesuai dengan laptop, dan pastikan server sesuai dengan yang di konfigurasi DHCP sebelumnya. Berikan comment apabila ingin menambahkan nama, lalu OK.

Berikut contoh penambahan dilakukan dengan script:

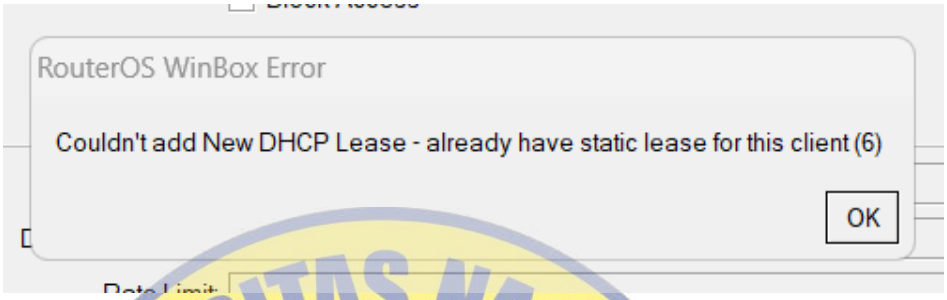
```
/ip dhcp-server lease add address=10.10.4.16 mac-address=28:C6:3F:C0:97:07
server=dhcp1 comment="MOCH. AMRI ADHIMATIEN"
```

Gambar 4.17 DHCP Lease Script

Buat dengan notepad dengan isi script */ip dhcp-server lease add address=10.10.4.16 mac-address=28:C6:3F:C0:97:07 server=dhcp1 comment="MOCH. AMRI ADHIMATIEN"* lalu save dengan format .rsc

Apabila sudah di save, import file .rsc ke Files di Mikrotik, apabila script sukses maka akan keluar message *script file loaded and executed successfully.*

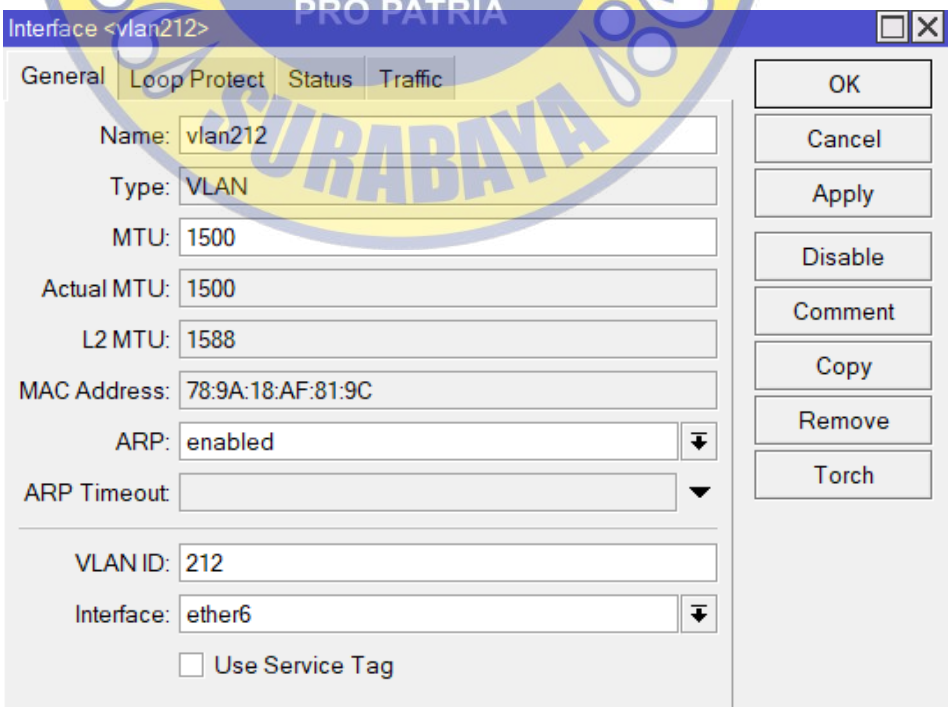
Untuk memastikan script sebelumnya berjalan, saya mencoba menambahkan dengan IP Address yang berbeda namun dengan MAC yang sama, hasilnya akan keluar notifikasi warning karena terdapat double MAC Address.



Gambar 4.18 Error Double MAC Address / IP Address

4.2.2.4 Konfigurasi VLAN untuk Pemisahan SSID WiFi Karyawan dan Guest

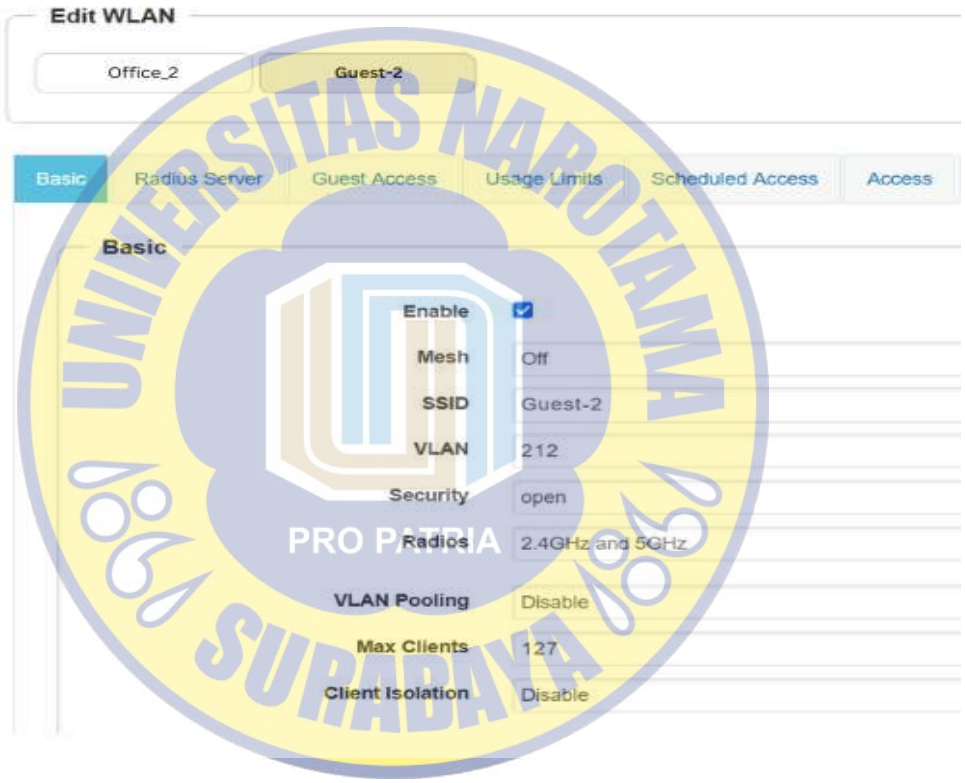
Untuk meningkatkan keamanan dan efisiensi penggunaan jaringan, diterapkan Virtual Local Area Network (VLAN) sebagai metode pemisahan antara WiFi Karyawan dan WiFi Guest. Dengan pemisahan ini, jaringan karyawan dan Guest memiliki segmen jaringan yang terisolasi, mencegah akses tidak sah ke sumber daya internal perusahaan.



Gambar 4.19 Vlan Setup

Pada Konfigurasi Wi-Fi Karyawan dan Guest, port yang digunakan untuk Access Point masing-masing lantai menjadi 1, hanya dipisah dengan penggunaan VLAN untuk Guest. VLAN WiFi Guest diberikan ID VLAN 212, di sesuaikan dengan masing-masing lantai dengan akses terbatas untuk internet, tanpa dapat mengakses jaringan internal.

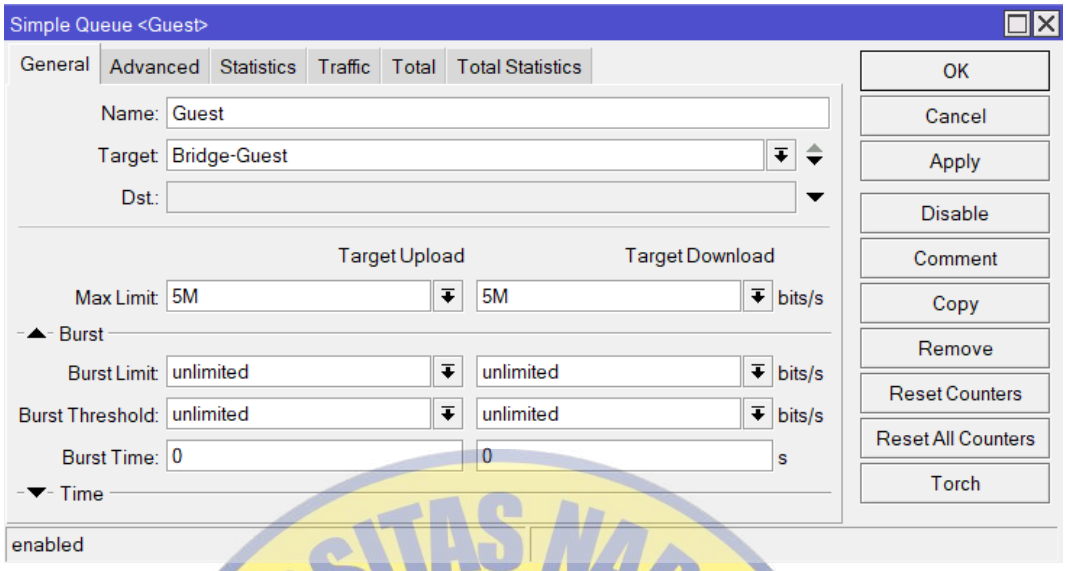
VLAN id tersebut kemudia akan di konfigurasikan pada perangkat Access Point Cambium.



Gambar 4.20 Cambium Guest-2

4.2.2.5 Konfigurasi Bandwidth Wi-Fi Guest

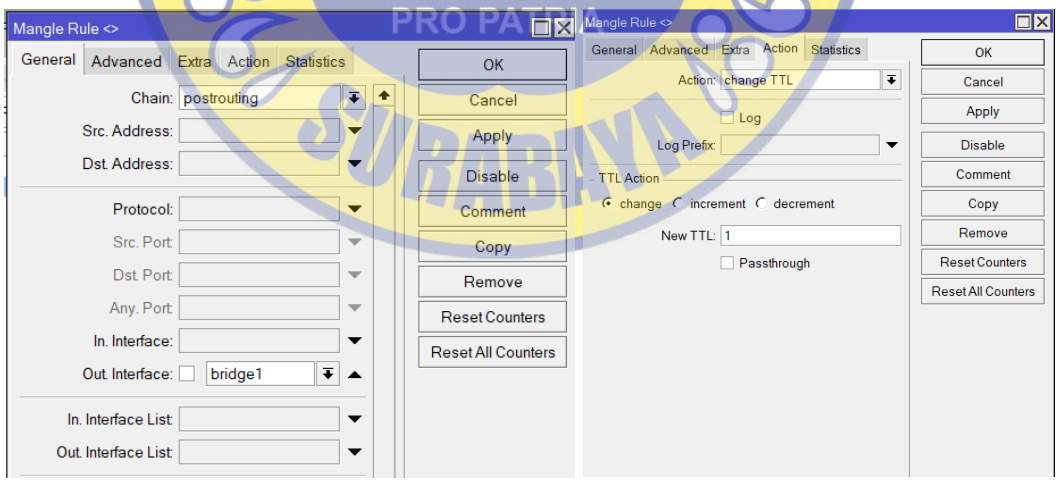
WiFi Guest yang memiliki bridge terpisah memiliki batasan bandwidth pada mikrotik untuk menjaga performa jaringan utama tetap stabil. Pembatasan MAC Address pada Wi-Fi Guest di terapkan di Queue pada Mikrotik dengan Limit upload serta download di 5Mbps.



Gambar 4.21 Queues bridge Guest

4.2.2.6 Konfigurasi pembatasan sharing koneksi

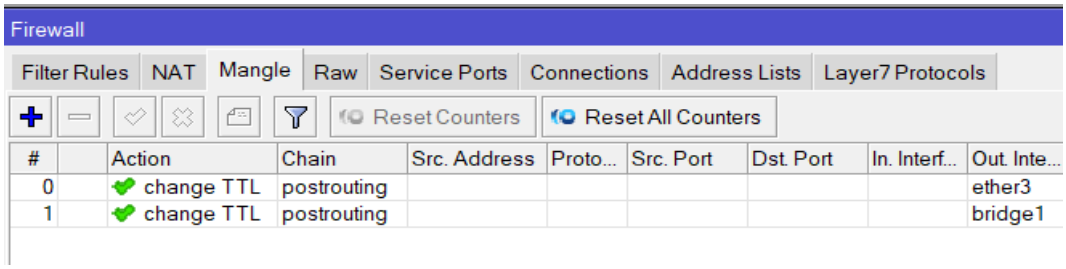
Konfigurasi ini digunakan untuk membatasi sharing koneksi wireless pada fitur Hotspot pada laptop dan PC. Hal ini dimaksudkan supaya koneksi hanya bisa digunakan oleh perangkat yang sudah terdaftar langsung ke mikrotik, dan tidak bisa di sharing lagi oleh perangkat dari client.



Gambar 4.22 Change TTL

Garis besar dari konfigurasinya adalah mengubah nilai TTL (Time To Live) dari packet download yang menuju ke client. Disini diubah menjadi nilai '1'. Untuk di Mikrotik sendiri kita bisa melakukan konfigurasi tersebut pada menu Firewall

Mangle. Konfigurasi ini berlaku untuk perangkat kantor yang terhubung dengan Wi-Fi maupun dengan LAN.



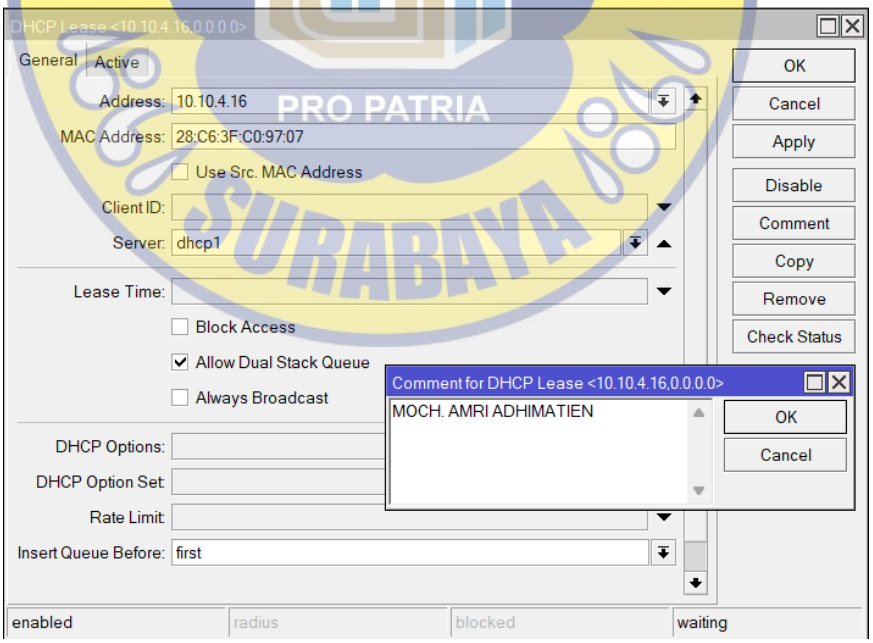
Gambar 4.23 Firewall Mangle

4.3 Pengujian Jaringan

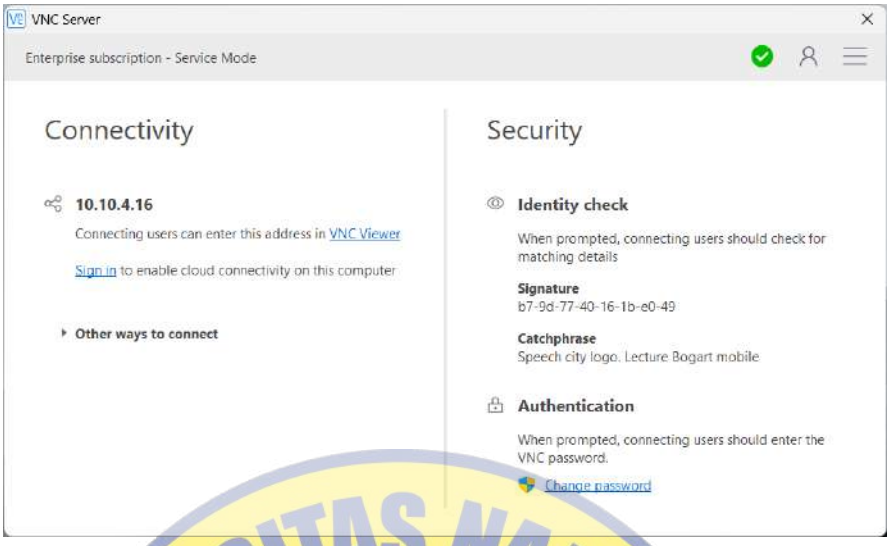
4.3.1 Pengujian Wi-Fi

1. Wi-Fi Karyawan :

Perangkat yang terdaftar pada daftar MAC address dapat terhubung ke WiFi Karyawan. IP yang di dapatkan pada Wi-Fi Karyawan sudah di buat secara static di mikrotik. Dengan hasil dari VNC menunjukkan bahwa Laptop yang terdaftar sudah berhasil terkoneksi dengan internet.



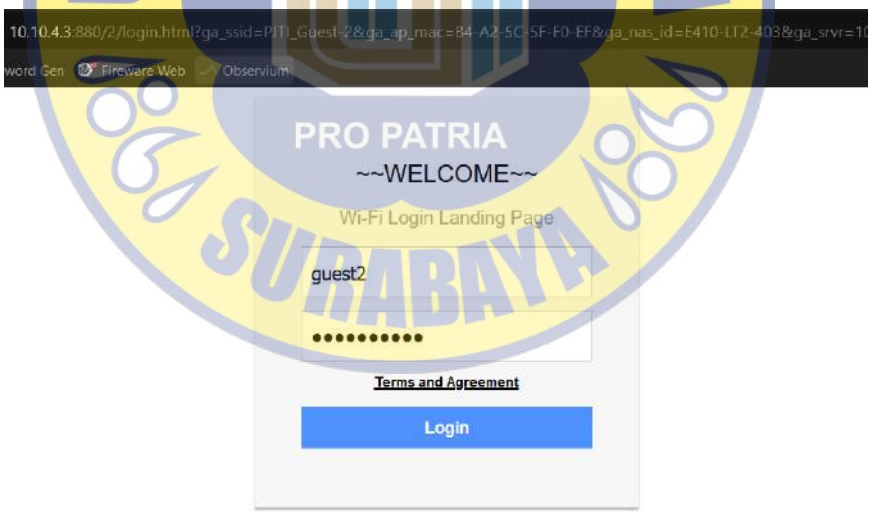
Gambar 4.24 Daftar IP dan Mac Address



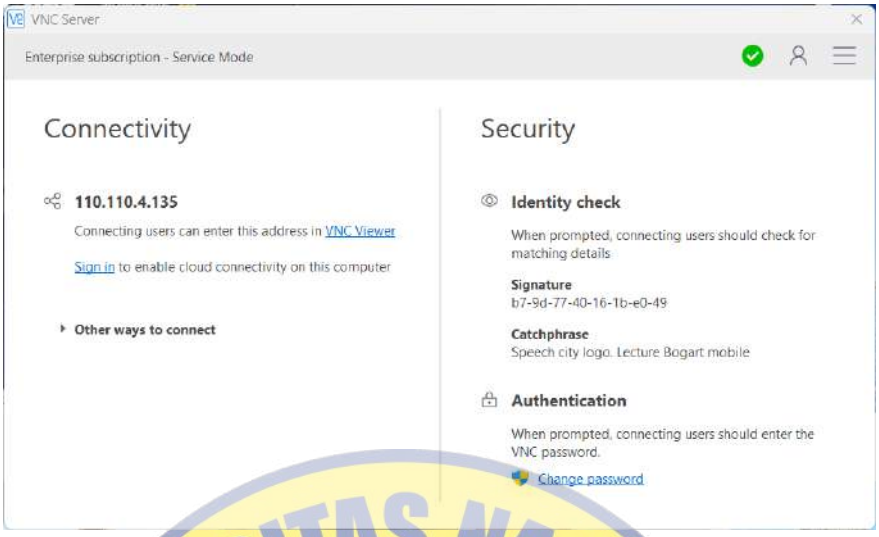
Gambar 4.25 IP Wi-Fi Karyawan dari VNC Server

2. WiFi Guest :

Guest dapat terhubung dengan mudah menggunakan password yang sudah di setup pada Cambium. Penggunaan landing page sebagai Langkah awal untuk masuk ke jaringan internet sebagai Guest.



Gambar 4.26 Landing Page login Wi-Fi Guest



Gambar 4.27 IP Wi-Fi Guest dari VNC Server

VNC mendeteksi bahwa IP Laptop yang telah terkoneksi dengan Wi-Fi Guest mendapatkan IP yang berbeda dengan IP Karyawan. Dengan kata lain, perbedaan IP antara Wi-Fi Guest dengan Karyawan sudah berhasil.

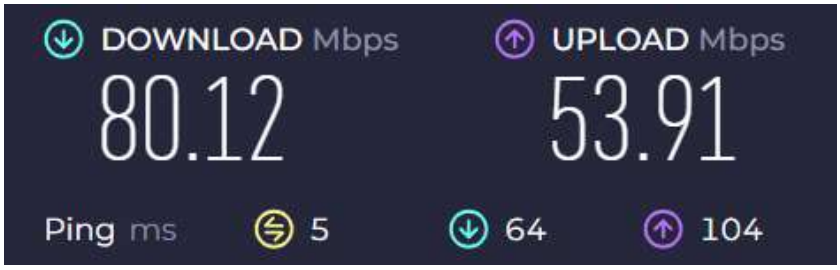
4.3.2 Analisis Performa Jaringan

Untuk mengukur efektivitas implementasi jaringan, dilakukan pengujian terhadap beberapa aspek seperti kecepatan, latensi, stabilitas koneksi, dan keamanan. Pengujian dilakukan dengan aplikasi speedtest.net untuk mengevaluasi bandwidth yang diterima oleh pengguna di setiap lantai, baik untuk Wi-Fi Karyawan dan Wi-Fi Guest.

4.3.2.1 Pengujian Speed Test Per Lantai

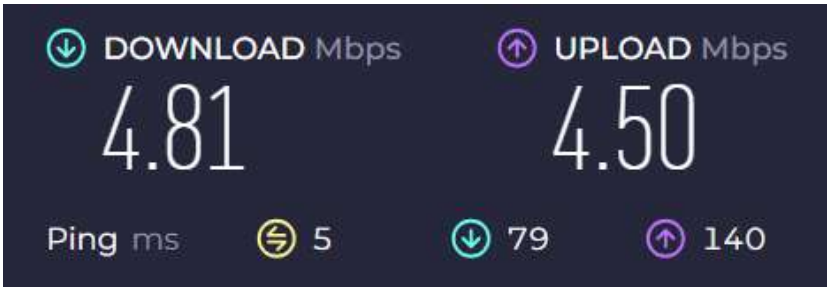
1. Lantai 1

- Pengujian Speedtest Wi-Fi Karyawan



Gambar 4.28 Speedtest Wi-Fi Karyawan lt.1

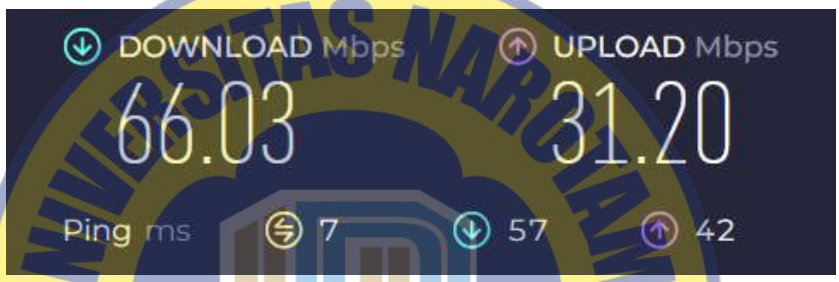
- Pengujian Speedtest Wi-Fi Guest



Gambar 4.29 Speedtest Wi-Fi Guest lt.1

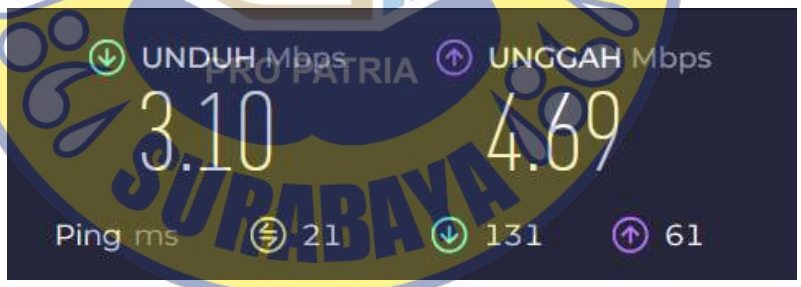
2. Lantai 2

- Pengujian Speedtest Wi-Fi Karyawan



Gambar 4.30 Speedtest Wi-Fi Karyawan lt.2

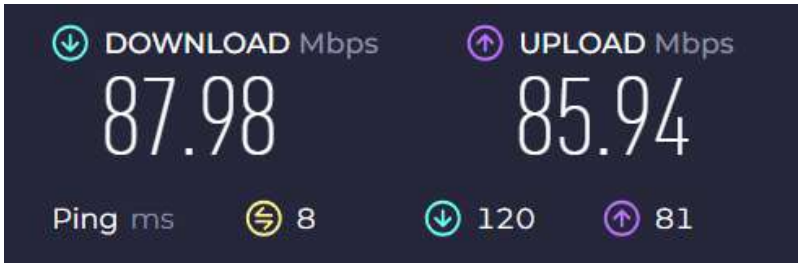
- Pengujian Speedtest Wi-Fi Guest



Gambar 4.31 Speedtest Wi-Fi Guest lt.2

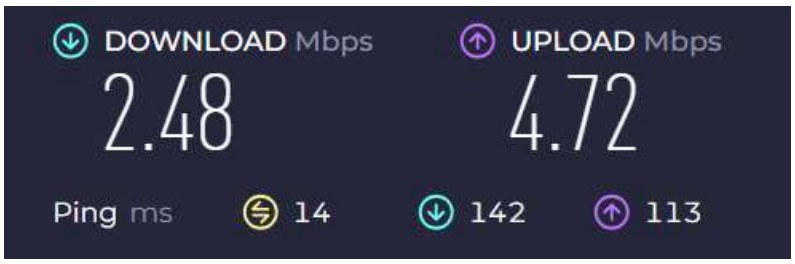
3. Lantai 3

- Pengujian Speedtest Wi-Fi Karyawan



Gambar 4.32 Speedtest Wi-Fi Karyawan lt.3

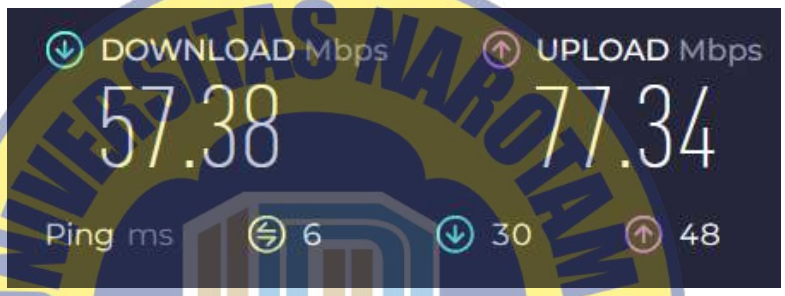
- Pengujian Speedtest Wi-Fi Guest



Gambar 4.33 Speedtest Wi-Fi Guest lt.3

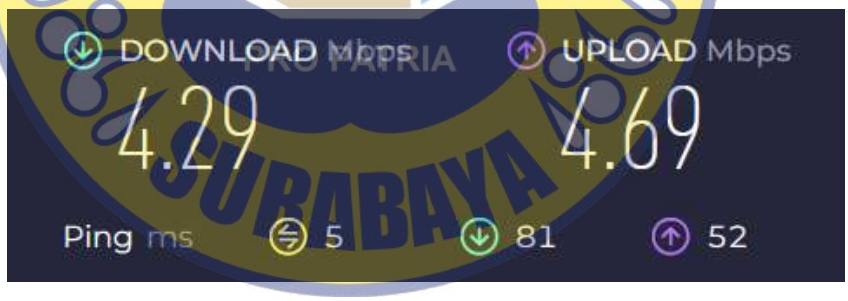
4. Lantai 4

- Pengujian Speedtest Wi-Fi Karyawan



Gambar 4.34 Speedtest Wi-Fi Karyawan lt.4

- Pengujian Speedtest Wi-Fi Guest



Gambar 4.35 Speedtest Wi-Fi Guest lt.4

Keterangan :

1. Uji Kecepatan WiFi Karyawan

Pengujian dilakukan menggunakan Speedtest untuk mengukur kecepatan unduh (download) dan unggah (upload) pada jaringan WiFi Karyawan. Hasil pengujian menunjukkan bahwa kecepatan yang diperoleh sesuai dengan alokasi bandwidth yang telah dikonfigurasi. Dengan jaringan yang lebih stabil, pengguna WiFi Karyawan dapat mengakses layanan cloud, sistem internal, dan aplikasi perusahaan tanpa gangguan yang signifikan.

2. Uji Kecepatan WiFi Guest

Pengujian Speedtest juga dilakukan pada jaringan WiFi Guest, yang telah dibatasi dengan maksimum kecepatan unggah dan unduh sebesar 5 Mbps. Hasil pengujian menunjukkan bahwa batasan ini diterapkan dengan baik oleh mikrotik, memastikan bahwa penggunaan bandwidth oleh Guest tidak mengganggu performa jaringan utama. Dengan pembatasan ini, WiFi Guest tetap dapat digunakan untuk aktivitas dasar seperti browsing dan komunikasi tanpa membebani sumber daya jaringan perusahaan.

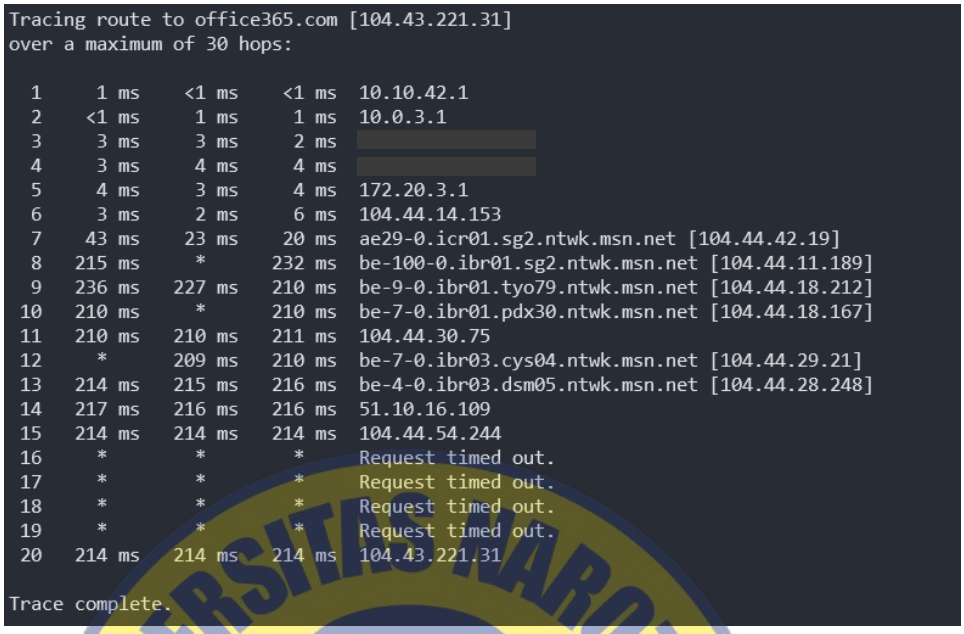
4.3.2.2 Pengujian Traceroute (tracert) untuk Analisis Pemisahan Jalur Koneksi Internet

Untuk memastikan bahwa pembagian jalur koneksi internet pada jaringan telah berjalan sesuai konfigurasi, dilakukan pengujian menggunakan Traceroute (tracert). Pengujian ini bertujuan untuk melihat jalur yang ditempuh paket data dari perangkat pengguna menuju internet melalui ISP yang telah dipisahkan.

Pemisahan jalur internet bisa dilihat pada gambar 4.38 dibawah, yang sudah di setup pada WatchGuard Firewall.

Gambar 4.36 WatchGuard Firewall

Dapat di lihat pada Gambar 4.48 diatas, bahwa ISP 2 di setup untuk koneksi eksternal seperti Zoom, Perbankan, Microsoft, Airlines dll. Beberapa pengetesan tracert bisa di lihat pada beberapa gambar di bawah ini :



Gambar 4.37 Tracert Office365.com

Analisis hasil tracert ke office365.com

1. Hop 1 & 2 (10.10.42.1 & 10.0.3.1)

   Menunjukkan bahwa ini gateway local dari router internal

2. Hop 3 & 4

   Ini adalah gateway ISP yang menghubungkan jaringan lokal ke jaringan penyedia layanan internet (ISP).

3. Hop 5 - 6 (172.20.3.1 & 104.44.14.153)

   Jalur ISP ke backbone internet.

4. Hop 7 - 15 (104.44.12.153 hingga 51.10.16.109)

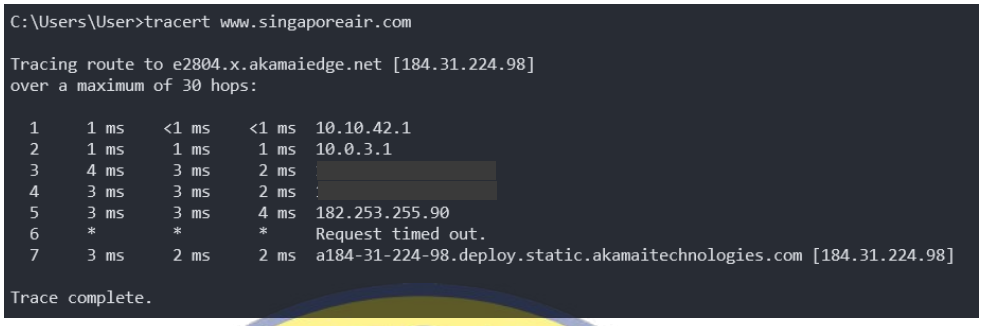
   Ini menunjukkan jalur yang masuk ke Microsoft Network (MSN.NET), yang merupakan infrastruktur global Microsoft untuk layanan seperti Office 365, Azure, dan lainnya. Latensi meningkat secara bertahap, terutama saat masuk ke server di Singapura (SG2), Tokyo (TYO79), Portland (PDX30), dan Dallas (DSM05).

5. Hop 16 - 19 (Request timed out)

   Ini berarti beberapa hop dalam jalur tidak mengizinkan ICMP traceroute, tetapi paket masih diteruskan ke tujuan akhir, biasanya terjadi pada jaringan yang memiliki firewall ketat atau load balancer untuk alasan keamanan.

6. Hop 20 (104.43.221.31)

   Ini adalah IP tujuan akhir (server Office 365). Latency stabil di sekitar 214 ms, yang masih dalam batas wajar untuk koneksi antar-benua.



Gambar 4.38 tracert Singaporeair.com

Analisis hasil tracert ke www.singaporeair.com

1. Hop 1 & 2 (10.10.42.1 & 10.0.3.1)

   Menunjukkan bahwa ini gateway local dari router internal

2. Hop 3 & 4

   Ini adalah gateway ISP yang menghubungkan jaringan lokal ke jaringan penyedia layanan internet (ISP).

3. Hop 5 (182.253.255.90)

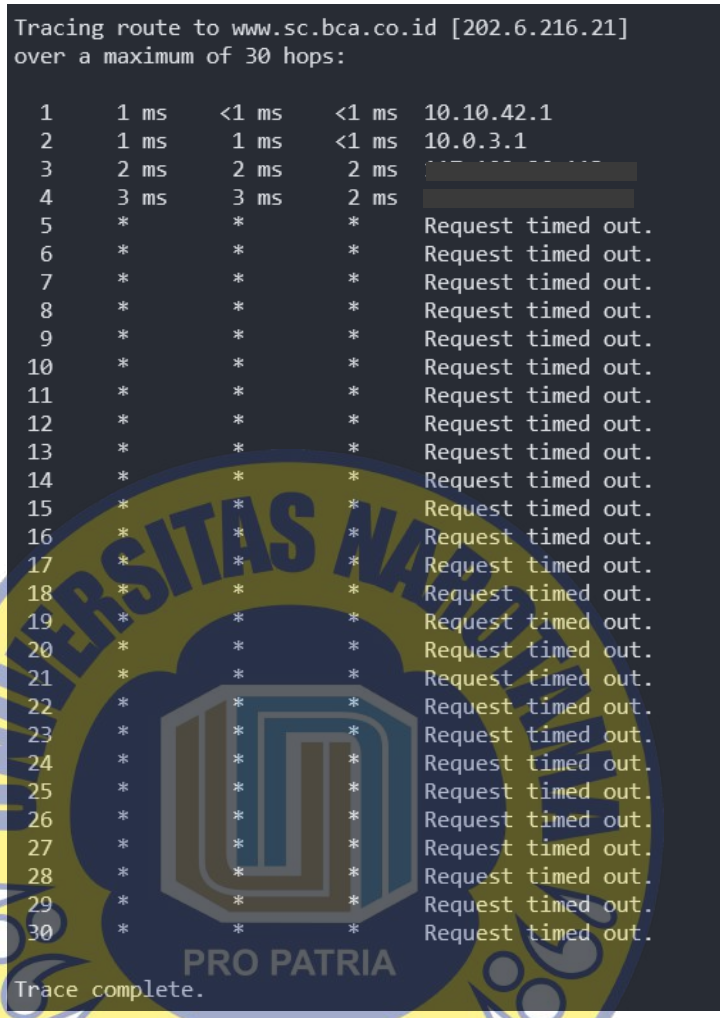
   Jalur ISP ke backbone internet,

4. Hop 6 (Request timed out)

   Timeout ini bisa terjadi karena firewall atau kebijakan jaringan yang memblokir ICMP TTL Exceeded.

5. Hop 7 (184.31.224.98 - Akamai Technologies)

   Ini adalah server tujuan atau CDN (Content Delivery Network) dari Singapore Airlines yang di-host oleh Akamai. Koneksi berhasil mencapai server akhir dengan latensi rendah (2-3ms).



Gambar 4.39 tracert www.bca.co.id

Analisis hasil tracert ke www.bca.co.id

1. Hop 1 & 2 (10.10.42.1 & 10.0.3.1)

   Menunjukkan bahwa ini gateway local dari router internal

2. Hop 3 & 4

   Menunjukkan IP Public dan gateway ISP ke backbone internet

3. Hop 5-30 (Request timed out)

   Tidak ada respons dari jalur selanjutnya, yang bisa disebabkan oleh beberapa factor, Firewall BCA memblokir ICMP Traceroute demi alasan keamanan, Server tujuan tidak mengizinkan traceroute untuk menghindari eksploitasi jaringan, Paket tetap sampai ke tujuan tetapi tidak memberikan respons kepada traceroute.

Kesimpulan dari pengetesan tracert diatas :

1. Jalur internet berfungsi dengan baik ke semua tujuan, meskipun ada beberapa hop yang mengalami Request Timed Out karena firewall atau kebijakan jaringan.
2. Traceroute ke Office 365 menunjukkan latensi yang lebih tinggi, yang wajar untuk koneksi internasional.
3. Traceroute ke BCA sepenuhnya diblokir setelah hop ke-4, tetapi ini tidak berarti koneksi gagal—hanya saja BCA membatasi traceroute untuk alasan keamanan.
4. Tidak ada pemutusan koneksi atau packet loss yang signifikan, menandakan jaringan stabil secara keseluruhan.

4.4. Analisis Performa Jaringan

Untuk mengukur efektivitas implementasi jaringan, dilakukan pengujian terhadap beberapa aspek seperti kecepatan, latensi, stabilitas koneksi, dan keamanan. Berikut adalah perbandingan kondisi jaringan sebelum dan sesudah implementasi:

4.4.1. Tabel Perbandingan Sebelum dan Sesudah Implementasi

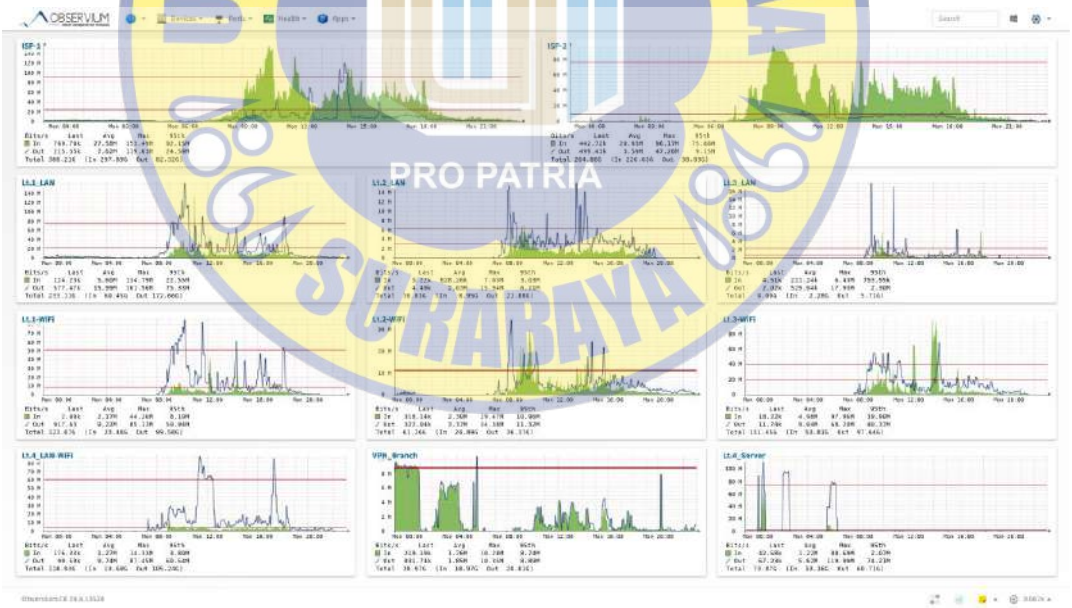
Tabel 4.1 Perbandingan Analisis Performa Jaringan

No	Parameter	Sebelum Implementasi	Sesudah Implementasi
1	Kecepatan Internet	Tidak stabil, sering terjadi fluktuasi kecepatan	Lebih stabil dengan pembagian bandwidth yang optimal
2	Latensi	Latensi tinggi, sering terjadi delay saat akses server eksternal	Latensi lebih rendah dan koneksi lebih responsif
3	Keamanan Jaringan	Hanya menggunakan password Wi-Fi (WPA2)	Menggunakan MAC Address Filtering untuk mengontrol perangkat yang bisa mengakses jaringan

4	Monitoring Jaringan	Tidak ada sistem monitoring real-time	Menggunakan Observium untuk monitoring performa jaringan
5	Keamanan dari Perangkat Tidak Terdaftar	Semua perangkat dapat terhubung dengan hanya mengetahui password	Hanya perangkat terdaftar dengan MAC Address Filtering yang bisa terhubung

4.5. Monitoring Jaringan dengan Observium

Untuk memastikan performa jaringan setelah implementasi, dilakukan monitoring menggunakan Observium, yaitu sebuah sistem pemantauan jaringan berbasis SNMP yang menyediakan tampilan visual mengenai trafik jaringan, penggunaan bandwidth, serta status perangkat jaringan



Gambar 4.40 Observium

4.5.1. Pengenalan Observium dalam Monitoring Jaringan

Pada penggunaanya, observium digunakan untuk :

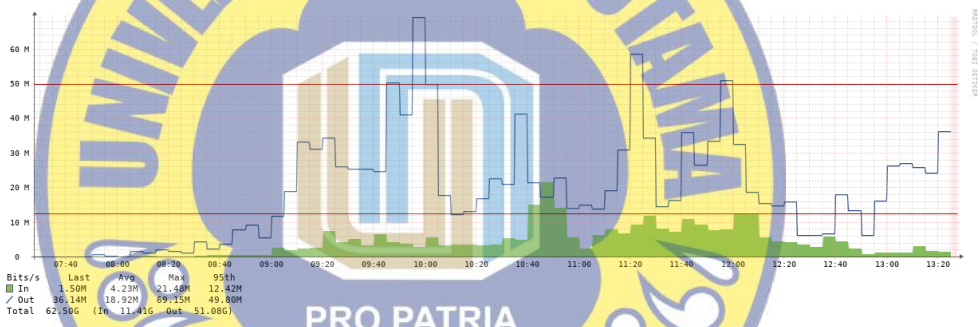
1. Melihat penggunaan bandwidth per perangkat dan interface.

2. Memantau kesehatan perangkat jaringan (CPU, RAM, dan suhu perangkat).
3. Menganalisis pola lalu lintas jaringan internet.
4. Mendeteksi anomali lalu lintas jaringan, seperti lonjakan penggunaan yang tidak wajar atau potensi serangan.

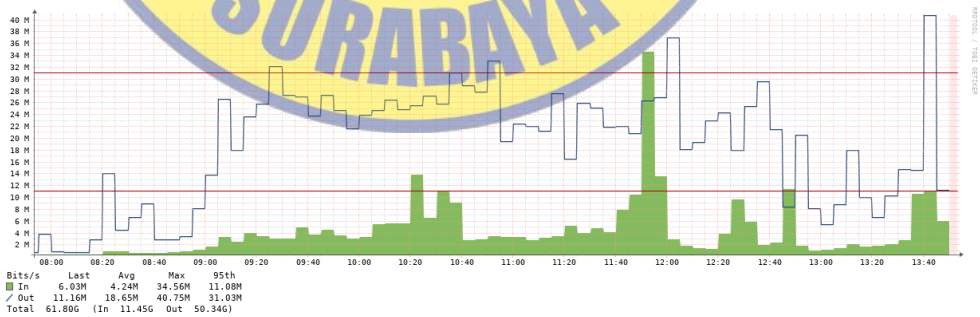
4.5.2. Hasil Monitoring Trafik Jaringan

Setelah implementasi VLAN untuk pemisahan jaringan WiFi Karyawan dan WiFi Guest, hasil monitoring menunjukkan perubahan signifikan pada pola penggunaan bandwidth:

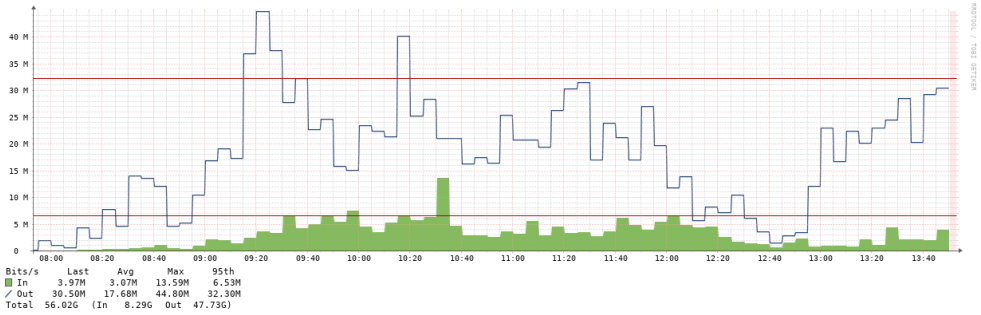
1. WiFi Karyawan memiliki pola penggunaan yang lebih stabil. Penggunaan bisa di lihat pada gambar dibawah ini.



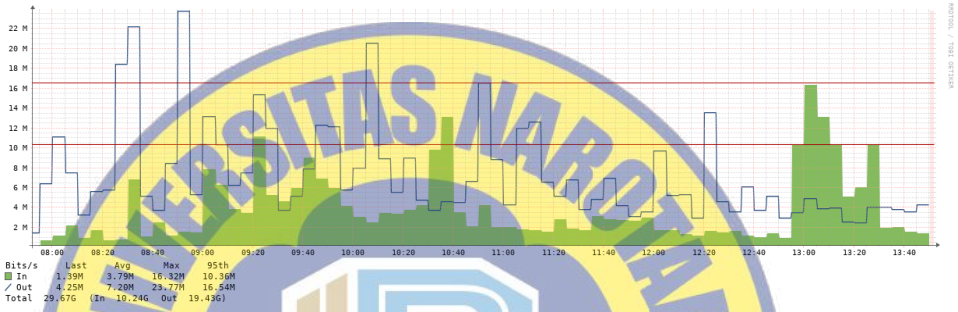
Gambar 4.41 traffic penggunaan Wi-Fi Karyawan lt.1



Gambar 4.42 traffic penggunaan Wi-Fi Karyawan lt.2

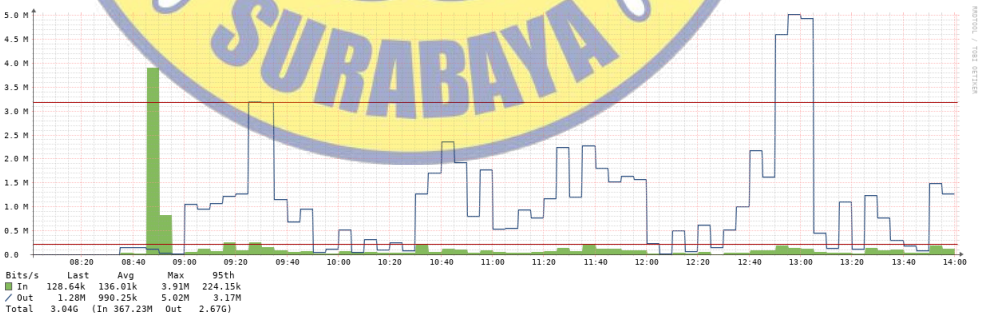


Gambar 4.43 traffic penggunaan Wi-Fi Karyawan lt.3

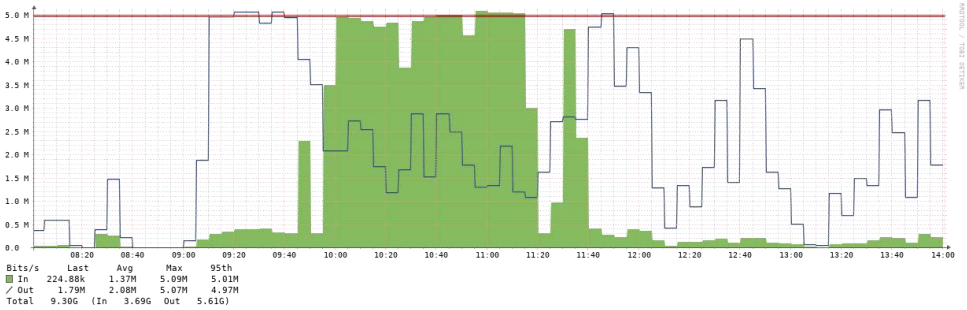


Gambar 4.44 traffic penggunaan Wi-Fi Karyawan lt.4

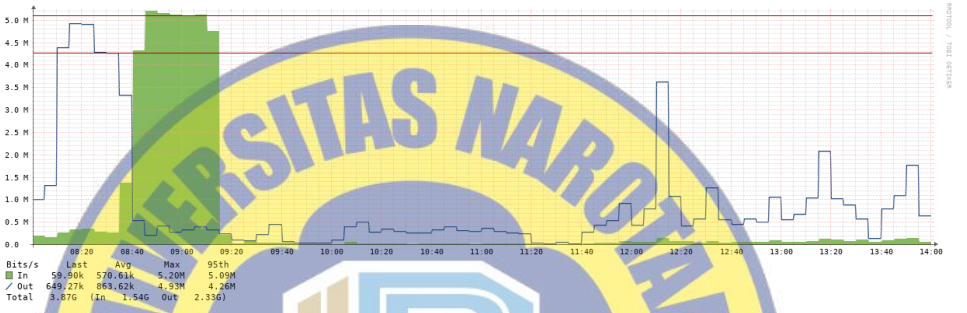
2. WiFi Guest mengalami lonjakan akses pada jam kerja, namun tetap berada dalam batas maksimal 5mbps yang ditetapkan, sehingga tidak mengganggu jaringan internal perusahaan.



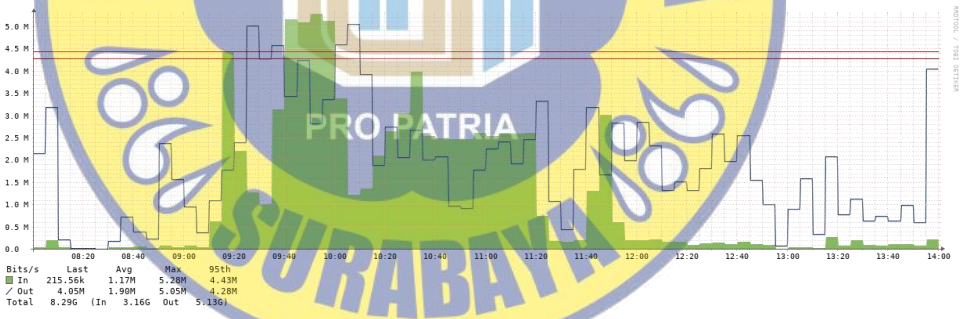
Gambar 4.45 traffic penggunaan Wi-Fi Guest lt.1



Gambar 4.46 traffic penggunaan Wi-Fi Guest lt.2



Gambar 4.47 traffic penggunaan Wi-Fi Guest lt.3



Gambar 4.48 traffic penggunaan Wi-Fi Guest lt.4

4.5.3. Analisis Hasil Monitoring

Dari hasil observasi menggunakan Observium, dapat disimpulkan bahwa:

1. Pemisahan VLAN berhasil mengisolasi trafik WiFi Guest dan WiFi Karyawan, sehingga tidak terjadi interferensi antar jaringan.
2. Pembatasan bandwidth efektif dalam menjaga kualitas koneksi, terutama bagi pengguna internal yang membutuhkan akses stabil ke aplikasi bisnis.

3. Monitoring dengan Observium mempermudah analisis performa jaringan secara real-time, memungkinkan admin jaringan untuk segera melakukan troubleshooting jika terjadi anomali.

4.6. Studi Kasus Penggunaan Jaringan di Beberapa Divisi

Implementasi jaringan tidak hanya diuji secara teknis, tetapi juga dievaluasi berdasarkan pengalaman pengguna dari beberapa divisi dalam perusahaan travel agent ini. Berikut adalah studi kasus penggunaan jaringan pada beberapa divisi utama:

4.6.1. Divisi Marketing

- Kebutuhan Jaringan: Akses cepat ke internet untuk riset pasar, mengunggah konten ke media sosial, dan mengelola iklan digital.
- Kendala Sebelum Implementasi: Sering terjadi keterlambatan akses karena bandwidth terbagi tanpa kontrol.
- Perubahan Setelah Implementasi: Dengan pembagian bandwidth yang lebih baik, akses ke platform digital lebih stabil dan cepat.

4.6.2. Divisi Finance

- Kebutuhan Jaringan: Koneksi aman dan stabil untuk mengakses sistem keuangan berbasis cloud dan melakukan transaksi online.
- Kendala Sebelum Implementasi: Sering terjadi lag saat mengakses sistem keuangan, terutama pada jam kerja sibuk.
- Perubahan Setelah Implementasi: Dengan prioritas bandwidth yang lebih tinggi, akses ke sistem keuangan menjadi lebih cepat dan minim gangguan.

4.6.3. Divisi IT Support

- Kebutuhan Jaringan: Monitoring real-time, troubleshooting jaringan, serta mengelola server dan firewall.
- Kendala Sebelum Implementasi: Tidak ada sistem monitoring yang jelas sehingga sulit mendeteksi permasalahan jaringan.
- Perubahan Setelah Implementasi: Dengan Observium, IT Support dapat segera mengidentifikasi dan menyelesaikan masalah jaringan.

4.6.4. Divisi Customer Service, Travel Consultant

- Kebutuhan Jaringan: Akses cepat ke website Airlines dan Travelport untuk melayani pelanggan dengan respons cepat.
- Kendala Sebelum Implementasi: Sering terjadi disconnect saat melayani customer untuk pembelian ticket.
- Perubahan Setelah Implementasi: Dengan konfigurasi jaringan yang lebih baik, akses ke Airlines dan Travelport menjadi lancar.

4.7. Pembahasan

Hasil implementasi menunjukkan bahwa desain infrastruktur jaringan yang telah direncanakan berhasil memenuhi kebutuhan operasional gedung perusahaan. Beberapa poin penting yang dapat diambil adalah:

1. Efektivitas Desain Topologi Jaringan
   - Kombinasi penggunaan WatchGuard Firewall, Switch Core, dan MikroTik memberikan distribusi jaringan yang efisien.
   - VLAN memisahkan jaringan karyawan dan Guest tanpa mengurangi kualitas layanan.
   - Struktur jaringan yang modular memudahkan pengelolaan dan troubleshooting jika terjadi gangguan.
2. Keamanan Jaringan yang Optimal
   - MAC Address Filtering meningkatkan keamanan jaringan dengan memastikan hanya perangkat terdaftar yang dapat terhubung.
   - NAT dan firewall pada MikroTik membantu melindungi jaringan dari ancaman eksternal.
   - Pemisahan VLAN mengurangi risiko penyebaran serangan dari tamu yang menggunakan Wi-Fi Guest.
   - Dengan fitur logging pada MikroTik, aktivitas jaringan dapat dimonitor untuk mendeteksi potensi ancaman keamanan.
3. Efisiensi Penggunaan Bandwidth
   - Pembagian bandwidth antara karyawan dan Guest berjalan sesuai kebutuhan.

- Pembatasan bandwidth pada Wi-Fi Guest menjaga stabilitas jaringan karyawan.
- Hasil pengujian menunjukkan bahwa WiFi Karyawan mendapatkan prioritas lebih tinggi sehingga aplikasi bisnis berjalan lebih lancar.
- Dengan konfigurasi Queue Tree di MikroTik, penggunaan bandwidth dapat dikontrol dan dimonitor secara optimal.

4. Ketersediaan dan Stabilitas Jaringan
    - Fitur failover memastikan konektivitas tetap berjalan meskipun ISP utama mengalami gangguan.
    - Monitoring melalui Observium memberikan visibilitas penuh terhadap performa jaringan.
    - Dengan monitoring real-time, deteksi dini terhadap lonjakan trafik atau penggunaan tidak wajar dapat dilakukan untuk mencegah gangguan layanan.
    - Hasil observasi menunjukkan bahwa sebelum implementasi, jaringan mengalami fluktuasi kecepatan pada jam sibuk. Setelah optimasi, kestabilan jaringan meningkat dengan rata-rata latensi yang lebih rendah
5. Evaluasi Kinerja Sebelum dan Sesudah Implementasi
    - Hasil traceroute menunjukkan bahwa jalur internet untuk WiFi Karyawan dan WiFi Guest telah terpisah dengan baik, mengonfirmasi efektivitas pengaturan routing dan VLAN.
    - Dari data Observium, penggunaan bandwidth lebih merata dengan penurunan beban pada jam-jam sibuk dibandingkan sebelum VLAN diterapkan.
6. Dampak Implementasi terhadap Operasional Perusahaan
    - Dengan jaringan yang lebih stabil dan aman, produktivitas karyawan meningkat karena tidak ada gangguan koneksi dalam mengakses aplikasi bisnis.
    - Feedback dari pengguna menunjukkan bahwa WiFi Guest tetap nyaman digunakan tanpa mengganggu jaringan utama karyawan.

- Administrator jaringan lebih mudah melakukan troubleshooting dan pengelolaan perangkat berkat pemantauan yang lebih transparan.

Dengan semua faktor ini, implementasi infrastruktur jaringan berbasis MikroTik dengan VLAN, MAC Address Filtering, dan sistem monitoring telah memberikan hasil yang efektif, aman, dan efisien, mendukung kebutuhan operasional perusahaan secara optimal.