

Optimalisasi Jaringan Nirkabel Menggunakan Mekanisme *Authentication, Authorization, Dan Accounting (Aaa)* Pada Router Mikrotik Rb951 Di Pt Xon Indonesia

Wireless Network Optimization Using Authentication, Authorization, And Accounting (Aaa) Mechanism On Mikrotik Rb951 Router At Pt Xon Indonesia

Yusuf Muhyidin^{1*}, Ari Supriatna¹, Dayan Singasatia¹, Rani Sri Wahyuni¹
Korespondensi Email : yusufmuhyidin@wastukancana.ac.id

¹Program Studi Teknik Informatika, STT Wastukancana, Purwakarta 41151, Indonesia

Abstrak. Internet merupakan jaringan global yang memungkinkan perangkat dari berbagai sistem saling terhubung. Dalam operasional data center, jaringan yang stabil dan aman sangat dibutuhkan. PT XON Indonesia menggunakan jaringan wireless untuk mendukung aktivitas kerja. Namun, lonjakan jumlah pengguna di lantai 2 memunculkan beberapa kendala, seperti belum adanya pemisahan jaringan antar pengguna, sistem autentikasi, kontrol pemakaian *bandwidth*. Masalah ini berisiko menurunkan kualitas koneksi dan keamanan jaringan. Untuk mengatasinya, studi ini mempunyai solusi berupa pengelolaan jaringan menggunakan VLAN untuk segmentasi, portal login untuk autentikasi pengguna, pengaturan *bandwidth* agar lebih merata melalui perangkat MikroTik. Langkah ini diharapkan dapat meningkatkan keamanan, kestabilan, dan kenyamanan dalam penggunaan jaringan di lingkungan kerja.

Kata kunci: Wireless Network, Mikrotik, AAA;

Abstract. The internet is a global network that allows devices from various systems to connect to each other. In data centre operations, a stable and secure network is needed. PT XON Indonesia uses a wireless network to support work activities. However, the surge in the number of users on the 2nd floor raises several obstacles, such as the absence of network separation between users, authentication systems, bandwidth usage control. This problem risks reducing connection quality and network security. To overcome this, this study has a solution in the form of network management using VLANs for segmentation, login portals for user authentication, bandwidth management to be more evenly distributed through MikroTik devices. This step is expected to improve security, stability, and comfort in using the network in the work environment

Keywords: Wireless Network, Mikrotik, AAA;

* Penulis korespondensi: yusufmuhyidin@wastukancana.ac.id

1. Pendahuluan

Internet merupakan jaringan komputer global yang memungkinkan pertukaran data antar perangkat tanpa memandang jenis sistem operasi maupun perangkat keras yang digunakan[1]. Jaringan komputer, khususnya jaringan *wireless*, telah menjadi teknologi umum dalam mendukung kebutuhan akses informasi secara cepat dan fleksibel tanpa koneksi fisik langsung. Namun, dengan meningkatnya kebutuhan dan kompleksitas pengguna, muncul tantangan dalam menjaga keamanan, efisiensi, dan stabilitas jaringan.

Dalam dunia industri data center, jaringan komputer memiliki peranan penting dalam mendukung layanan penyimpanan dan distribusi data dalam skala besar. PT XON Indonesia CGK4 adalah salah satu perusahaan yang menyediakan layanan tersebut, sekaligus menyediakan *working area* dengan jaringan *wireless* sebagai salah satu fasilitas utama. Seiring bertambahnya aktivitas di lantai 2, terutama dari pengguna internal dan customer, muncul berbagai permasalahan, seperti tidak adanya segmentasi jaringan antar pengguna, belum tersedianya autentikasi saat mengakses jaringan, penggunaan *bandwidth* yang tidak terkendali. Masalah-masalah tersebut berdampak pada berkurangnya kualitas layanan jaringan serta meningkatkan potensi ancaman terhadap sistem. Beberapa penelitian sebelumnya telah membuktikan bahwa jaringan *wireless* tanpa sistem autentikasi dan manajemen terpusat rentan terhadap serangan seperti *DDoS*, *packet sniffing*, dan akses tidak sah. Sebagai contoh [2] menjelaskan bahwa penerapan protokol RADIUS dapat mencegah serangan hingga 98%, sedangkan penelitian menunjukkan bahwa jaringan tanpa enkripsi dan segmentasi sangat rentan dibobol[2].

Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan pengembangan sistem jaringan *wireless* melalui penerapan *Virtual Local Area Network* (VLAN) guna membagi jaringan sesuai kategori pengguna, penggunaan portal login untuk autentikasi melalui protokol *Remote Authentication Dial-In User Service* (RADIUS), pengaturan manajemen *bandwidth* agar penggunaan jaringan lebih merata.

Optimalisasi ini diharapkan mampu meningkatkan aspek keamanan, efisiensi, dan stabilitas jaringan *wireless* di lingkungan kerja PT XON Indonesia CGK4. Seluruh sistem dirancang mengacu pada konsep *Authentication, Authorization, and Accounting* (AAA) guna memastikan bahwa setiap pengguna yang terhubung ke jaringan dapat terverifikasi, terkontrol, dan tercatat dengan baik. Proses permintaan akses juga dilakukan secara sistematis melalui tim *Network Operation Center* (NOC), dimulai dari permohonan via email, verifikasi formulir kunjungan, hingga pemberian kredensial dan nomor tiket akses. Langkah ini merupakan bagian dari kebijakan perusahaan untuk menjamin pengelolaan akses jaringan yang aman dan tertib. PT XON Indonesia CGK4 adalah salah satu perusahaan yang menyediakan layanan tersebut, sekaligus menyediakan *working area* dengan jaringan *wireless* sebagai salah satu fasilitas utama. Seiring bertambahnya aktivitas di lantai 2, terutama dari pengguna internal dan customer, muncul berbagai permasalahan, seperti tidak adanya segmentasi jaringan antar pengguna, belum tersedianya autentikasi saat mengakses jaringan, penggunaan *bandwidth* yang tidak terkendali.

2. Metode

2.1 Network Development Life Cycle

Dalam penelitian ini menggunakan metode NDLC (*Network Development Life Cycle*), NDLC merupakan sebuah metode yang bergantung pada proses pembangun sebelumnya seperti perancangan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data Metode ini baik digunakan dalam perancangan jaringan [3].



Gambar 1. Metode NDLC

Pada gambar 1 merupakan alur penelitian NDLC dimana dilakukan proses Analisis yang dimana melalui tahap observasi atau pengecekan kelengkapan dan melakukan wawancara apa yang menjadi kebutuhannya dan Penelitian ini menggunakan model penelitian kualitatif [3].

1. Analisis

Pada tahap Analisis, dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan *user*, dan analisa topologi atau jaringan yang sudah ada saat ini[3].

2. Desain

Pada tahap Desain, dibuat interkoneksi desain topologi jaringan yang akan dibangun. Dengan desain ini, diharapkan dapat memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain mencakup struktur topologi, desain akses data, desain tata *layout* perkabelan, dan elemen lain yang memberikan gambaran jelas tentang proyek yang akan dibangun[3].

3. *Prototyping*

Pada tahap Simulasi *Prototyping*, beberapa networkers membuat simulasi menggunakan tools khusus di bidang jaringan, seperti *BOSON*, *Packet Tracer*, atau *PNETLAB*. Simulasi ini bertujuan untuk melihat kinerja awal jaringan yang akan dibangun dan menjadi bahan presentasi serta diskusi dengan tim. Namun, karena keterbatasan perangkat lunak, beberapa *networkers* hanya menggunakan alat bantu seperti *VISIO* untuk membuat desain topologi yang akan dibangun[3].

4. Implementasi

Tahap Implementasi membutuhkan waktu yang lebih lama dibandingkan tahap sebelumnya. Pada tahap ini, networkers menerapkan semua yang telah dirancang dan didesain. Implementasi adalah tahapan yang sangat menentukan keberhasilan atau kegagalan proyek yang sedang dibangun[3].

5. *Monitoring*

Tahap *Monitoring* dilakukan untuk memastikan jaringan komputer dan komunikasi berjalan sesuai keinginan serta tujuan awal dari pengguna pada tahap analisis. *Monitoring* diperlukan agar potensi masalah dapat diidentifikasi dan diselesaikan lebih awal[3].

6. Manajemen

Tahap Manajemen, perhatian utama diberikan pada kebijakan (*policy*). Kebijakan ini dirancang untuk menjaga agar sistem yang telah dibangun dapat berjalan dengan baik dan berkelanjutan. [3].

2.2 RADIUS (Remote Authentication Dial in User Service)

Remote Authentication Dial In User Service (RADIUS) adalah protokol jaringan yang menyediakan manajemen *Authentication*, *Authorization*, dan *Accounting* (AAA) secara terpusat bagi

pengguna layanan jaringan[4].

2.3 Authentication, Authorization and Accounting (AAA)

1. Authentication

Authentication Merupakan suatu proses untuk memverifikasi identitas yang digunakan oleh user untuk masuk pada jaringan komputer. Menggunakan kombinasi dari *user* dan *password* untuk memasuki suatu jaringan komputer[5].

2. Authorization

Authorization merupakan proses yang memutuskan apakah user dapat mengakses jaringan tersebut atau tidak. Sebagai contoh, dalam perusahaan yang bergerak pada penyedia layanan internet atau ISP, ISP berhak memutuskan apakah akan memberikan alamat *IP Static* atau alamat *IP DHCP*.

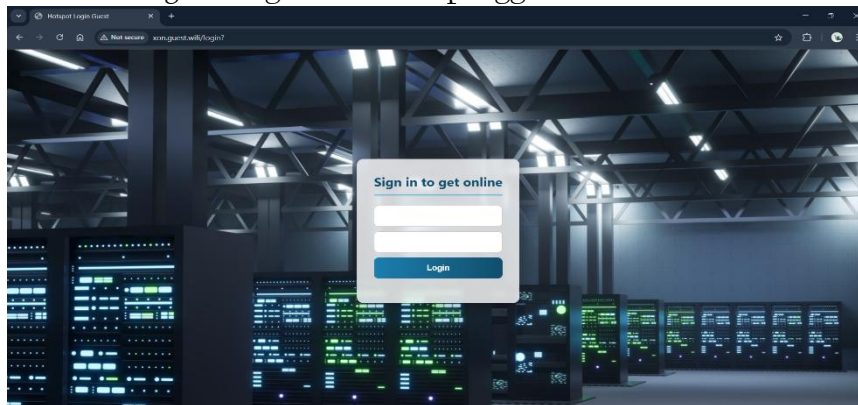
3. Accounting

Accounting Merupakan bagian akhir dari kerangka kerja AAA, *accounting* dapat mengukur dan mencatat sumber daya yang telah digunakan, termasuk jumlah waktu atau jumlah data yang dikirim dan atau diterima selama pelanggan tersebut memanfaatkan sumber daya tersebut[5].

3. Hasil dan Pembahasan

3.1 Implementasi Login Hotspot

Sistem *login hotspot* telah berhasil diimplementasikan untuk tiga SSID, yaitu *Xon_Guest*, *Xon_NOC* dan *Xon_Employee*, Masing masing SSID terhubung ke server Mikrotik yang telah di konfigurasi oleh *User Manager* sebagai otentikasi pengguna.



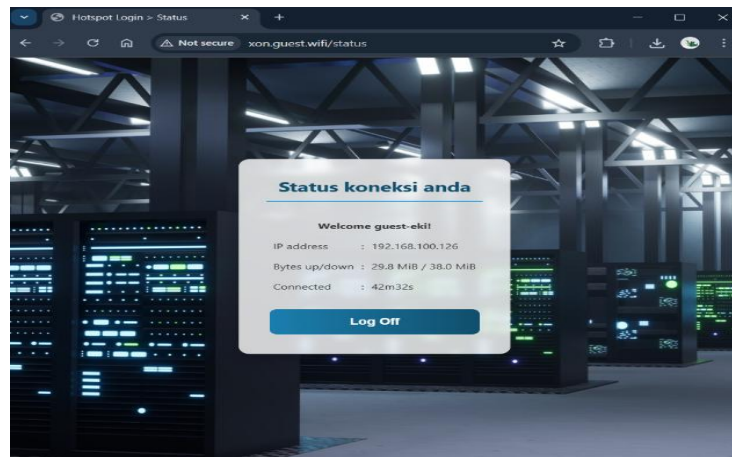
Gambar 2. Login

3.2 Hasil Pengujian Login

Pengujian dilakukan dengan beberapa akun pengguna yang telah dibuat di user manager. Hasilnya menunjukkan bahwa masing masing akun hanya dapat *login* pada SSID yang sudah ditentukan. Sebagai contoh, akun untuk pengguna NOC Login gagal pada SSID *Xon_Guest* ataupun *Xon_Employee* begitupun sebaliknya. Hal ini menunjukkan segmentasi pengguna berdasarkan SSID berjalan dengan baik

3.3 Pengujian VLAN

Ketiga SSID telah dipisahkan menggunakan konfigurasi VLAN dengan *ip address*. Pengujian dilakukan menggunakan perintah *ping* dari SSID *Xon_guest* ke SSID *Xon_noc*



Gambar 4. Koneksi ke Wifi Xon_Guest

```

C:\WINDOWS\system32\cmd. X + v

Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c6b5:a090:30b0:6c95%20
IPv4 Address. . . . . : 192.168.100.126
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 192.168.100.1

C:\Users\ivana>ping 192.168.150.11

Pinging 192.168.150.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.150.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ivana>

```

Gambar 5. Hasil tes ping wifi xon_guest

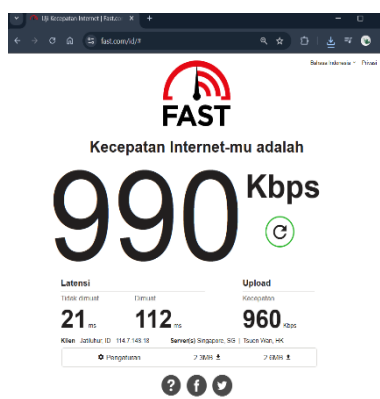
Hasilnya menunjukkan tes ping tidak bisa komunikasi antar VLAN sudah berhasil dibatasi sesuai preencanaan.

3.4 Pengujian Bandwidth

Pengujian kecepatan akses internet dilakukan menggunakan situs '*fast.com*' sebagai alat bantu uji kecepatan yang sederhana namun akurat. Pengujian ini bertujuan untuk memastikan bahwa konfigurasi pembatasan *bandwidth* pada masing-masing SSID berjalan sesuai dengan pengaturan yang telah diterapkan pada perangkat Mikrotik.

Tabel 1. Manajemen *Bandwidth*

No	SSID	Bandwidth
1	Xon_Guest	1 Mbps
2	Xon_NOC	1.5 Mbps
3	Xon_Employee	2 Mbps



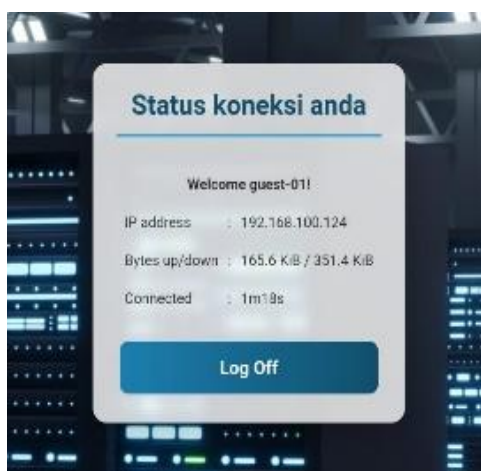
Gambar 6. Tes Speed/ bandwidth

3.5 Pengujian Batas Pengguna Akun

Pengujian ini dilakukan untuk memastikan bahwa setiap pengguna hanya dapat login dari maksimal dua perangkat secara bersamaan, Konfigurasi ini dilakukan pada *User Manager* dengan mengatur nilai shared user = 2 untuk setiap akun.

Tabel 2. Hasil Pengujian

No	Username	Jumlah Perangkat Dicoba	Status Login
1	guest-01	1	Berhas
2	guest-01	2	Berhasil
3	guest-01	3	Gagal



Gambar 7. Pengujian Login

Hasil pengujian menunjukkan bahwa ketika satu akun *login* dari dua perangkat, akses berhasil. Namun, saat perangkat ketiga mencoba login menggunakan akun yang sama, akses ditolak oleh sistem dan terdapat notif '*simultaneous session limit reached*'.

Hal ini membuktikan bahwa pengaturan pembatasan jumlah perangkat per pengguna berjalan sesuai dengan yang diharapkan, sehingga dapat mencegah penyalahgunaan akun dan menjaga stabilitas jaringan.

3.6 Alokasi IP Address

Setiap *SSID* yang digunakan dalam sistem telah dikonfigurasi menggunakan *VLAN* yang berbeda beda dan di alokasikan ke *IP Address* tersendiri, Hal ini bertujuan untuk memisahkan lalu lintas jaringan serta memudahkan proses manajemen dan pembatasan akses.

Tabel berikut menunjukkan alokasi IP berdasarkan SSID dan VLAN :

Tabel 3. Alokasi Ip Address

No	SSID	VLAN	Network	Gateway IP
1	Xon_Guest	100	192.168.100.0/25	192.168.100.1
2	Xon_NOC	150	192.168.150.0/28	192.168.150.1
3	Xon_Employee	200	192.168.200.0/27	192.168.200.1

3.7 Penerapan Konsep AAA Dalam Sistem

Sistem login yang dibangun menerapkan prinsip AAA (Authentication, authorization, Accounting) melalui integrasi Mikrotik Usermanager sebagai *server Radius*.

1. *Authentication* dilakukan saat pengguna mencoba login dengan memasukkan *username* dan *password*. Sistem akan memverifikasi data tersebut ke *server RADIUS* melalui Mikrotik *User Manager*. Jika informasi login sesuai, maka pengguna diizinkan untuk mengakses jaringan.
2. *Authorization* akan menentukan hak akses pengguna berdasarkan kategori akun yang digunakan. Misalnya, pengguna dengan akun kategori *guest* hanya diizinkan mengakses jaringan VLAN 100 dengan *bandwidth* terbatas 1 Mbps, sedangkan akun *employee* akan diarahkan ke VLAN 200 dengan *bandwidth* lebih tinggi. Ini memastikan bahwa setiap pengguna hanya memperoleh akses sesuai kebutuhannya.
3. *Accounting* berfungsi mencatat aktivitas pengguna selama terkoneksi ke jaringan. Informasi seperti durasi koneksi, jumlah perangkat yang digunakan (dibatasi maksimal dua perangkat per *user*), dan volume data yang dikonsumsi akan direkam oleh *User Manager*. Data ini berguna bagi *administrator* untuk monitoring penggunaan jaringan, evaluasi kebijakan akses, serta pelaporan bila diperlukan.

4. Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, sistem hotspot yang dibangun berhasil berjalan sesuai dengan tujuan. Sistem berhasil membuat segmentasi jaringan menjadi tiga SSID, yaitu *Xon_Guest*, *Xon_NOC*, dan *Xon_Employee*, yang masing-masing dipisahkan menggunakan VLAN dan dialokasikan ke IP Address yang berbeda. Pengujian menunjukkan bahwa segmentasi jaringan berjalan sesuai rencana, di mana masing-masing kategori pengguna tidak dapat saling berkomunikasi atau ping antar VLAN. Proses login pengguna juga berfungsi sebagaimana mestinya. Setiap akun hanya dapat digunakan untuk login pada SSID yang sesuai, dan sistem berhasil membatasi akses login agar maksimal hanya dua perangkat yang dapat terhubung menggunakan satu akun. Selain itu, pengujian terhadap pembatasan *bandwidth* menggunakan situs *fast.com* menunjukkan bahwa kecepatan internet yang diterima oleh pengguna sesuai dengan konfigurasi masing-masing SSID, yaitu 1 Mbps untuk *Guest*, 1.5 Mbps untuk *NOC*, dan 2 Mbps untuk *Employee*. Secara keseluruhan, sistem telah mampu mengatur segmentasi jaringan, otentikasi pengguna, pembatasan jumlah perangkat, dan pengelolaan *bandwidth* sesuai kategori pengguna.

DAFTAR PUSTAKA

- [1] Rahayu, S. P., Gusti, I., Putra, L., & Prisma, E. (2022). Implementasi Monitoring Manajemen Jaringan Dengan Software The Dude Berbasis Telegram Messenger. *Journal of Informatics and Computer Science*, 04.
- [2] Muhamad Malik Matin, I., Ramadhan, F., Hutasoit, G. S., Aurellia Hapsari, A., Teknik Informatika dan Komputer Politeknik Negeri Jakarta Jl GA Siwabessy, D. D., Beji, K., Depok, K., & Barat, J. (2024). Analisis Kerentanan Jaringan pada Fasilitas Internet Nirkabel pada Serangan Packet Sniffing. 4(1), 28.
- [3] Zulkarnaen, I., & Aliyah, J. (2021a). Perancangan Jaringan Menggunakan Router Switch Cisco Packet Tracer Pada Kantor Diskominfotik Provinsi Nusa Tenggara Barat (Vol. 5, Issue 2).
- [4] Syarif Aziz, A., Studi Ilmu Komputer, P., Sains, F., Ilmu Kesehatan, dan, Bina Bangsa Getsempena, U., Tanggul Krueng Lamnyong No, J., Kec Syiah Kuala, R., & Banda Aceh, K. (2021). Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius Design And Security Analysis On Freeradius Centralized Authentication System. *Journal of Informatics and Computer Science*, 7(2). <http://www.mikrotik.com>.

- [5] Fauzi, A., Dedy Irawan, J., & Vendyansyah, N. (2020). Rancang Bangun Sistem Manajemen User Aaa (Authentication, Authorization, Accounting) Dan Monitoring Jaringan Hotspot Berbasis Web. In Jurnal Mahasiswa Teknik Informatika (Vol. 4, Issue 1)