

IMPLEMENTASI NETWORK ACCESS CONTROL PADA JARINGAN LOCAL AREA NETWORK MENGGUNAKAN MIKROTIK

Putri Oktaviani¹

Prodi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu¹

Putriov910@gmail.com^{1*}

Abstract

This study aims to build a LAN network infrastructure with authentication before connecting to the network and to implement a network security system using Network Access Control (NAC) based on the IEEE 802.1x standard with Mikrotik. This research uses the Network Development Life Cycle (NDLC) method. By using the NDLC research method, it is hoped that it can define the design or development process cycle of a computer network system, especially in the process of implementing Network Access Control (NAC) on a LAN network using a Mikrotik router. The results of this study indicate that the 802.11x protocol can be applied to Network Access Control (NAC) on a computer network using a Mikrotik router, where Mikrotik is used as an authenticator and authentication server (Radius Server) using a user manager. The quality of service with the Quality Of Service (QOS) method for LAN network performance with the application of Network Access Control (NAC) is categorized as Good based on the tests that have been carried out with the results of a delay of 1.92 ms, jitter of 33.3 ms, packet loss of 0%, and throughput of 548 kb. Mikrotik routers can still monitor (monitoring) active hostnames after implementing Network Access Control (NAC) on Local Area Network networks using the 802.11x protocol

Keywords: 802.1x, NAC, LAN, Radius, Mikrotik

Abstrak

Penelitian ini bertujuan untuk membangun infrastruktur jaringan LAN dengan otentikasi sebelum terhubung ke dalam jaringan serta menerapkan sistem keamanan jaringan menggunakan Network Access Control (NAC) berdasarkan standar IEEE 802.1x dengan Mikrotik. Penelitian ini menggunakan metode metode Network Development Life Cycle (NDLC). Dengan menggunakan metode penelitian NDLC ini diharapkan dapat mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer terutama dalam proses implementasi Network Access Control (NAC) pada jaringan LAN menggunakan router Mikrotik. Hasil dari penelitian ini menunjukkan bahwa Protokol 802.11x dapat diterapkan untuk Network Access Control (NAC) pada jaringan komputer dengan menggunakan router Mikrotik, dimana mikrotik dijadikan sebagai authenticator serta authentication server (Radius Server) menggunakan user manager. Kualitas layanan dengan metode Quality Of Service (QOS) untuk performansi jaringan LAN dengan penerapan Network Access Control (NAC) dikategorikan Baik berdasarkan pengujian yang sudah dilakukan dengan hasil delay sebesar 1.92 ms, jitter sebesar 33.3 ms, packet loss sebesar 0%, dan throughput sebesar 548 kb. Router mikrotik masih dapat memantau (monitoring) active hostname setelah penerapan Network Access Control (NAC) pada jaringan Local Area Network menggunakan protokol 802.11x.

Kata Kunci : 802.1x, NAC, LAN, Radius, Mikrotik.

1. Pendahuluan

Dalam proses perkembangan teknologi informasi, jaringan komputer merupakan salah satu teknologi yang juga menjadi bagian penting, sebab jaringan komputer merupakan pondasi dari pemanfaatan teknologi informasi tersebut. Dengan menggunakan jaringan komputer pengguna teknologi informasi dapat saling terhubung satu sama lainnya. Dalam penggunaan jaringan komputer ini dapat dilakukan baik menggunakan media kabel ataupun nirkabel

Jaringan komputer yang menggunakan media kabel ini biasanya disebut dengan jaringan *Local Area Network* (LAN) atau jaringan yang terhubung menggunakan kabel dalam cakupan lokal saja misalnya di kantor. Penggunaan jaringan LAN ini biasanya diperuntukkan untuk keperluan administrasi sebuah kantor yang efisien dan tidak bergantung dengan sinyal seperti menggunakan jaringan tanpa kabel (*wireless*). Dalam penggunaan jaringan LAN ini akan lebih mudah terhubung kedalam jaringan jika menggunakan IP address yang sifatnya dinamis atau didapatkan secara langsung

ketika terhubung kedalam jaringan, akan tetapi hal ini akan menyebabkan tidak adanya pembatasan dalam penggunaan jaringan yang menyebabkan pengguna manapun bebas untuk terhubung. Oleh sebab itulah dibutuhkan sebuah sistem otentikasi terhadap jaringan LAN untuk menghindari akses masuk ke jaringan secara bebas dalam upaya mengamankan koneksi pada jaringan LAN.

Terdapat banyak cara yang dapat diterapkan untuk melakukan otentikasi pada jaringan LAN, seperti *Network Access Control (NAC)*, dimana NAC ini merupakan solusi dalam mengamankan jaringan komputer dengan menggunakan beberapa protokol untuk mendefinisikan dan mengimplementasikan sebuah rule ataupun aturan dengan mendeskripsikan cara ataupun teknik untuk mengamankan akses untuk terhubung ke dalam suatu jaringan. Dengan adanya *Network Access Control (NAC)* ini, maka setiap komputer ataupun perangkat yang terhubung memerlukan otentikasi terlebih dahulu.

Penerapan *Network Access Control (NAC)* pada koneksi LAN dapat diterapkan dengan menggunakan standar IEEE 802.1x, dimana standar ini merupakan standar dalam memberikan otentikasi sekaligus otoritas terhadap perangkat yang terhubung melalui *port* LAN secara fisik. Dalam penerapannya setiap perangkat yang terkoneksi dengan standar IEEE 802.1X akan dibagi kedalam beberapa istilah, yaitu *supplicant*, *authenticator*, *authentication server*. Salah satu perangkat yang mendukung standar IEEE 802.1x ini adalah Router Mikrotik. Saat ini Mikrotik mendukung untuk fungsi sebagai *Supplicant* ataupun *Authenticator*, selain itu juga Router Mikrotik menawarkan *server* otentikasi (*authentication server*) yang disebut dengan *User Manager (Userman)*, sehingga Mikrotik dapat menerapkan *Network Access Control (NAC)* dengan standar IEEE 802.1x baik sebagai *supplicant*, *authenticator*, maupun *authentication server*.

2. Tinjauan Pustaka

Menurut IETF Working Group Institute of Electrical and Electronics Engineers (IEEE) 802.1X merupakan standar yang digunakan untuk memberikan autentikasi dan otorisasi ke perangkat yang telah terhubung melalui port Local Area Network (LAN) secara fisik untuk menetapkan autentikasi point-to-point. Sehingga keamanan jaringan berbasis kabel dalam perusahaan atau organisasi dapat ditingkatkan.

Menurut Damara, IEEE 802.1x merupakan standar *port* jaringan berbasis kontrol akses. 802.1x yang memanfaatkan Protokol *Authentication* dengan varian yang diperluas untuk mengotentikasi akun pengguna atau terhadap otentikasi sistem eksternal melalui jaringan kabel. Otentikasi 802.1X melibatkan tiga pihak yaitu *supplicant*, *authenticator*, dan *authentication server* seperti yang terlihat pada Gambar 1 berikut.



Gambar 1 Skema Standar 802.1x

Dari Gambar 1 Skema Standar 802.1x diatas, dapat dijelaskan fungsi dari masing – masing pihak yang terlibat dalam standar IEEE 802.1x seperti berikut ini (Wikipedia, 2021).

1. *Supplicant* (Pemohon)

Supplicant atau pemohon adalah *client* perangkat (seperti laptop) yang ingin menempel pada LAN / WLAN. Istilah *supplicant* atau pemohon juga digunakan secara bergantian untuk merujuk pada perangkat lunak yang berjalan pada *client* yang memberikan kredensial kepada pengautentikasi.

2. *Authenticator* (Pengautentikasi)

Authenticator atau pengautentikasi adalah perangkat jaringan yang menyediakan *link* data antara *client* dan jaringan dan dapat mengizinkan atau memblokir lalu lintas jaringan antara dua perangkat jaringan, seperti *Ethernet switch* atau titik akses nirkabel.

3. Authentication Server (Server Otentikasi)

Authentication server atau *server* otentikasi biasanya merupakan *server* tepercaya yang dapat menerima dan menanggapi permintaan untuk akses jaringan, dan dapat memberi tahu pengautentikasi jika koneksi diizinkan, dan berbagai pengaturan yang harus diterapkan ke koneksi atau pengaturan *client* tersebut. *Server* otentikasi biasanya menjalankan perangkat lunak yang mendukung protokol RADIUS dan EAP. Dalam beberapa kasus, perangkat lunak *server* otentikasi mungkin berjalan pada perangkat keras otentikasi.

Pengautentikasi bertindak seperti penjaga keamanan untuk jaringan yang dilindungi. Pemohon (yaitu, perangkat *client*) tidak diizinkan mengakses melalui pengautentikasi ke sisi jaringan yang dilindungi sampai identitas pemohon telah divalidasi dan diotorisasi. Dengan otentikasi berbasis *port* 802.1X, pemohon pada awalnya harus memberikan kredensial yang diperlukan kepada pengautentikasi - ini akan ditentukan sebelumnya oleh administrator jaringan dan dapat menyertakan nama pengguna / kata sandi atau sertifikat digital yang diizinkan. Pengautentikasi meneruskan kredensial ini ke *server* otentikasi untuk memutuskan apakah akses akan diberikan. Jika *server* otentikasi menentukan bahwa kredensial itu valid, ia memberi tahu pengautentikasi, yang pada gilirannya memungkinkan pemohon (perangkat *client*) untuk mengakses sumber daya yang terletak di sisi jaringan yang dilindungi.

3. Network Access Control (NAC)

Menurut Damara, Shesia Rizki. 2020. Network Access Control (NAC) adalah sebuah solusi dalam keamanan jaringan komputer yang menggunakan beberapa protokol untuk mendefinisikan dan mengimplementasikan sebuah aturan yang mendeskripsikan cara untuk mengamankan sebuah akses ke dalam sebuah jaringan ketika sebuah alat mencoba untuk tersambung dalam suatu jaringan.

Menurut Damara), *Network Access Control* (NAC) merupakan solusi untuk keamanan jaringan komputer dengan beberapa kebijakan, termasuk pemeriksaan sebelum dan pasca masuk untuk *endpoint*. Dimana *user* dan perangkatnya dapat mengakses ke suatu jaringan dan apa saja yang dapat diakses pada jaringan tersebut. NAC dimulai dengan memeriksa apakah suatu perangkat diizinkan untuk terhubung ke jaringan. melalui teknologi yang dikenal sebagai 802.1X, yang menyediakan tiga fungsi penting yang disebut *Authentication*, *Authorization*, dan *Accounting*

Dengan adanya *Network Access Control* ini, maka setiap perangkat (*supplicant*) yang akan terkoneksi memerlukan autentikasi terlebih dahulu. Analoginya sama seperti ketika kita akan terkoneksi ke *wireless access point* dan harus memasukkan otentikasi sebelum terkoneksi. Adapun secara teknis ada beberapa proses/tahap untuk melakukan otentikasi diantaranya *Initialization*, *Initiation*, *Negotiation*, dan *Authentication* (Citraweb, 2020). Untuk lebih jelasnya dapat dilihat pada Gambar 2 berikut.



Gambar 2. Tahapan Otentikasi NAC

4. Mikrotik

Menurut Towidjojo (2012:1), *router* MikroTik dikenal sebagai *router* yang irit *hardware*, memiliki banyak fitur, mudah dikonfigurasi (*user friendly*) dan dapat diinstal pada PC (Personal Computer). Selain itu, *router* MikroTik dikenal karena fitur-fitur yang lengkap, murah dan

kemampuannya yang sangat tinggi. *Router* Mikrotik bisa diterapkan pada berbagai skenario jaringan dari yang sederhana sampai yang rumit.

Menurut Whitten dalam Putra dan Bugis (2019:59), Mikrotik adalah sistem operasi dan perangkat lunak yang bisa dipakai dengan tujuan menjadikan computer biasa menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk IP *network* dan jaringan *wireless*.

Dot1X merupakan implementasi dari standard IEEE 802.1X di MikroTik RouterOS. Pada Mikrotik fitur Dot1X (IEEE 802.1X) baru ditambahkan pada RouterOS versi 6.45.1. Saat ini Mikrotik mendukung untuk fungsi sebagai Supplicant ataupun Authenticator. Dan tipe EAP yang disupport ketika sebagai supplicant seperti EAP-TLS, EAP-TTLS, EAP-MSCHAPv2 dan PEAP (Citraweb, 2020).

5. Remote Access Dial In User Service (Radius)

Menurut Amarudin dan Yuliansyah (2018:62), RADIUS merupakan suatu protokol yang dikembangkan untuk proses AAA (*authentication, authorization, and accounting*). *Remote Access Dial- in User Service* (RADIUS), merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentifikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme autentifikasi yang sudah banyak digunakan sebelumnya, yaitu menggunakan metode *challenge/response*. RADIUS menjalankan sistem administrasi pengguna yang terpusat. Sistem ini tentunya akan mempermudah tugas seorang administrator. Dengan sistem ini pengguna dapat menggunakan hotspot di tempat yang berbeda-beda dengan melakukan autentifikasi ke *server* RADIUS.

Menurut Vivanda dan Susanti (2019:247), *Remote Access Dial In User Service* (Radius) merupakan *protokol connectionless* berbasis UDP yang tidak menggunakan koneksi langsung dan ditandai dengan *field* UDP yang menggunakan port 1812. Radius *server* sendiri merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentifikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme autentifikasi dengan menggunakan metode *challenge/ response*.

6. User Manager

Menurut Putra and Bugis (2019:59), *User manager* adalah suatu aplikasi manajemen system di dalam mikrotik yang juga berfungsi sebagai radius server yang bisa dipakai untuk *HotSpot users*, PPP (PPtp/PPPoE), DHCP *users*, LAN atau WLAN *users*, dan *Router users*. *User Manager* memudahkan dalam membuat layanan jaringan yang didistribusikan secara luas, misal hotspot di cafe, mall, hotel dan sebagainya.

7. Jaringan Komputer

Menurut Madcoms, Jaringan komputer merupakan kumpulan dari beberapa komputer dan peralatan penunjang lainnya yang terhubung dalam satu kesatuan dan saling terkoneksi.

Menurut Foruzen, Jaringan komputer merupakan hasil dari koneksi (hubungan) dari sejumlah perangkat atau komputer yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (komputer desktop, komputer jinjing, smartphone, PC tablet) dan perangkat penghubung (*router, switch, modem, wireless access point*).

Pada sebuah jaringan komputer minimal terdapat dua buah komputer atau perangkat yang saling terhubung satu sama lain. Dalam sebuah jaringan yang lebih luas, akan terdapat beragam perangkat komputer dan perangkat penghubung lainnya yang saling terhubung serta terjadi proses komunikasi dan transfer paket data di dalamnya.

8. Metode Penelitian

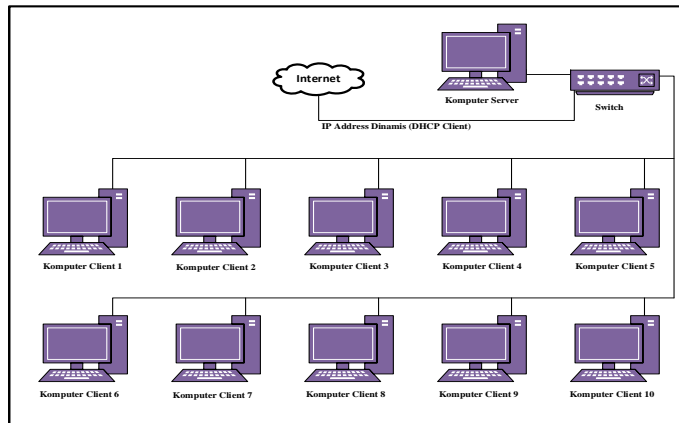
Metode penelitian yang digunakan adalah metode *Network Development Life Cycle* (NDLC). Dengan menggunakan metode penelitian NDLC ini diharapkan penulis dapat mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer terutama dalam proses implementasi *Network Access Control* (NAC) pada jaringan LAN menggunakan router Mikrotik. Berikut merupakan gambar dan tahapan dari metode penelitian NDLC, yaitu:



Gambar 3. NDLC Model

Dari Gambar 3. NDLC Model, dapat dijelaskan tahapan yang akan dilakukan seperti berikut ini:

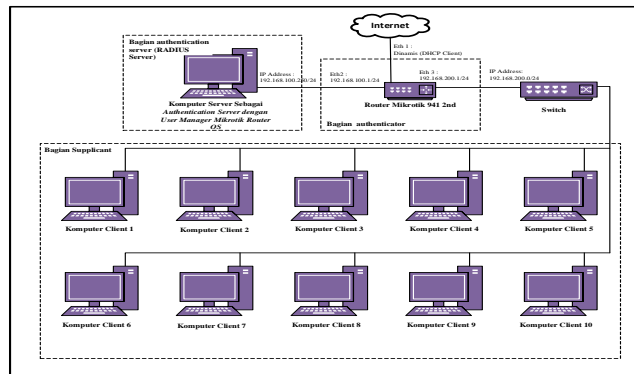
1. Tahap *Analysis* (Analisis)
Tahapan analisis merupakan tahapan awal yang dilakukan dalam menganalisis kebutuhan, analisis permasalahan yang ada, analisis keinginan *user*, dan analisa topologi jaringan yang sudah ada, bisa dibidang tahapan ini adalah tahapan pengumpulan data yang dibutuhkan untuk perumusan masalah dalam menyelesaikan kendala yang ada. Dengan mengidentifikasi sistem yang sedang berjalan lalu mencoba untuk menganalisis suatu pengembangan sistem seperti apa yang akan diterapkan pada jaringan LAN dengan menerapkan *Network Access Control* (NAC) untuk melakukan otentikasi sebelum terhubung ke jaringan.
2. Tahap *Design*
Pada tahapan ini, penulis akan membuat desain gambar topologi jaringan yang akan dibangun, desain akses data dan sebagainya dalam upaya implementasi *Network Access Control* (NAC) pada jaringan LAN menggunakan Mikrotik.
3. Tahap *Simulation Prototype*
Pada tahapan ini, dilakukan simulasi pengembangan jaringan LAN dengan menerapkan *Network Access Control* (NAC) sebelum diimplementasikan pada jaringan LAN. Hal ini dimaksudkan untuk melihat kinerja dari jaringan yang akan dibangun dan menjadi bahan presentasi dan *sharing* dengan pengembangan sistem jaringan.
4. Tahap *Implementation*
Pada tahapan ini, merupakan tahapan dimana implementasi *Network Access Control* (NAC) pada jaringan LAN menggunakan Mikrotik. Pada tahapan ini juga akan terlihat bagaimana pengembangan yang akan dibangun serta apakah jaringan tersebut akan memberikan pengaruh terhadap sistem yang ada.
5. Tahap *Monitoring*
Tahapan *monitoring* merupakan tahapan penting agar jaringan dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan penulis pada tahap awal analisis. Penulis akan menggunakan *tools* yang ada di Mikrotik yang berfungsi untuk memonitor lalu lintas jaringan.
6. Tahap *Management*
Pada tahap manajemen ini akan dilakukan beberapa langkah pengelolaan agar sistem yang telah dibangun dapat berjalan sesuai dengan yang diharapkan.
 - a. **Diagram Blok Sistem Lama**
Berdasarkan dari data yang penulis peroleh dari studi observasi yang dilakukan pada laboratorium komputer UPT. Puskom, saat ini tidak ada sistem otentikasi yang diterapkan untuk melakukan kontrol terhadap akses jaringan LAN. Adapun skema diagram blok sistem yang ada saat ini adalah sebagai berikut.



Gambar 4. Diagram Blok Sistem Lama

b. Diagram Blok Sistem Baru

Pada penelitian ini akan dilakukan pengembangan terhadap arsitektur yang sudah ada dengan menerapkan *Network Access Control (NAC)* pada jaringan LAN menggunakan Mikrotik dalam melakukan otentikasi sebelum *client* dapat terhubung ke dalam jaringan. Adapun topologi yang akan digunakan adalah sebagai berikut.

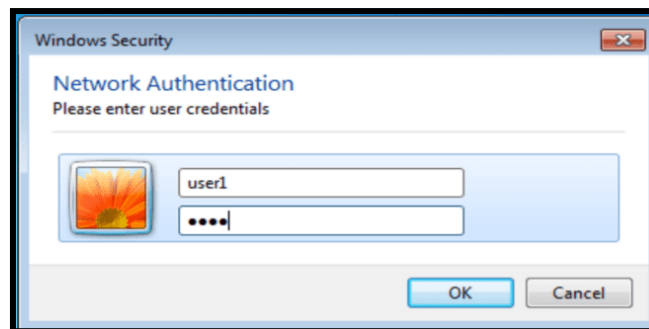


Gambar 5. Diagram Blok Sistem Baru

Pada Gambar 5 tersebut dapat dilihat bahwa terdapat tambahan radius *server* sebagai *authentication server* menggunakan *user manager* pada Mikrotik RouterOS yang di *Install* secara virtual dengan aplikasi virtualbox pada komputer *server*, selanjutnya terdapat juga Mikrotik Router Board RB941-2nd yang akan digunakan sebagai *authenticator*, serta komputer *client* akan menjadi *supplicant* atau perangkat yang menerima trafik jaringan dari *authenticator*, dimana untuk terhubung harus mendapatkan otentikasi dari *authentication server*.

9. Hasil dan pembahasan

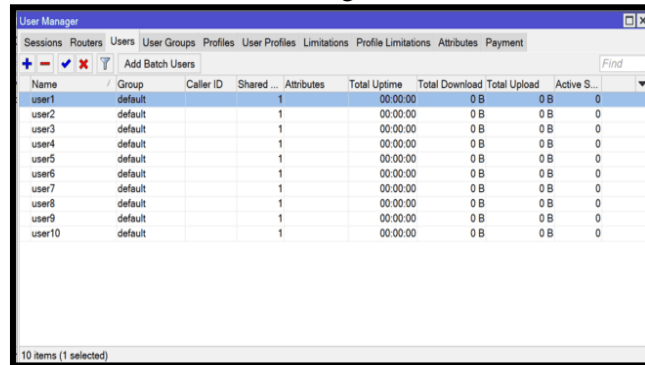
Pada bab ini akan menjelaskan hasil dari penelitian yang telah dilakukan, dari implementasi *Network Access Control (NAC)* pada jaringan *Local Area Network (LAN)* menggunakan mikrotik adalah sebagai berikut.



Gambar 6. Tampilan Network Authentication pada Client

Pada Gambar 6. diatas, dapat dilihat bahwa untuk dapat terhubung ke jaringan Local Area Network (LAN) membutuhkan autentikasi terhadap jaringan, dimana untuk terhubung ke *network*

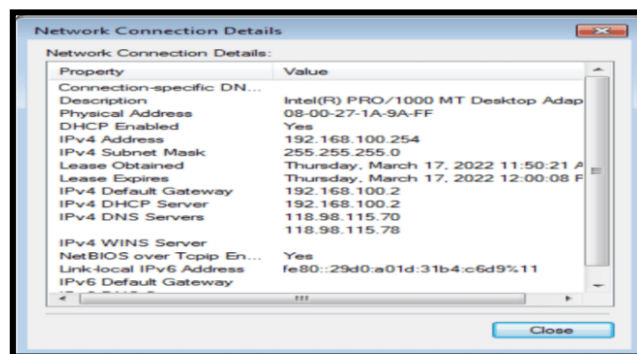
otentikasi ini harus memasukkan *username* dan *password* yang sudah dibuat pada *server* autentikasi (*authentication server*) yang dalam penelitian ini menggunakan *user manager* pada Mikrotik seperti yang terlihat pada Gambar 7. user autentikasi user manager berikut.



Name	Group	Caller ID	Shared	Attributes	Total Uptime	Total Download	Total Upload	Active S...
user1	default		1		00:00:00	0 B	0 B	0
user2	default		1		00:00:00	0 B	0 B	0
user3	default		1		00:00:00	0 B	0 B	0
user4	default		1		00:00:00	0 B	0 B	0
user5	default		1		00:00:00	0 B	0 B	0
user6	default		1		00:00:00	0 B	0 B	0
user7	default		1		00:00:00	0 B	0 B	0
user8	default		1		00:00:00	0 B	0 B	0
user9	default		1		00:00:00	0 B	0 B	0
user10	default		1		00:00:00	0 B	0 B	0

Gambar 7. User Autentikasi User Manager

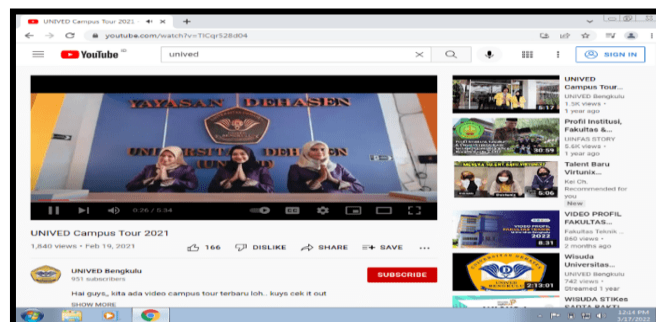
Pada Gambar 7. diatas, dapat dilihat *user* yang sudah dibuat pada autentikasi *server* yang dalam penelitian ini menggunakan aplikasi user manager dari mikrotik dan diteruskan oleh *authenticator* menggunakan protokol 802.11x atau dot1x yang terdapat pada router gateway dalam jaringan. Setelah *client* atau *supplicant* berhasil di autentikasi oleh autentikasi *server*, maka *client* atau *supplicant* akan mendapatkan alokasi IP *address* yang sudah dibuat sebelumnya pada *router gateway*. Adapun alokasi IP *address* yang didapatkan oleh client dapat dilihat pada Gambar 8 Alokasi IP Address Client seperti berikut ini.



Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Desktop Adap
Physical Address	08-00-27-1A-9A-FF
DHCP Enabled	Yes
IPv4 Address	192.168.100.254
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Thursday, March 17, 2022 11:50:21 A
Lease Expires	Thursday, March 17, 2022 12:00:08 P
IPv4 Default Gateway	192.168.100.2
IPv4 DHCP Server	192.168.100.2
IPv4 DNS Servers	118.98.115.70 118.98.115.78
IPv4 WINS Server	
NetBIOS over Tcpi En...	Yes
Link-local IPv6 Address	fe80::29d0:a01d:31b4:c6d9%11
IPv6 Default Gateway	

Gambar 8 Alokasi IP Address Client

Setelah client atau supplicat dapat terhubung ke jaringan, maka client juga akan dapat mengakses koneksi internet yang ada pada jaringan komputer seperti yang terlihat pada Gambar 4.4 Akses Internet oleh Client seperti berikut ini.



Gambar 9. Akses Internet oleh Client

Pada sub bab pembahasan ini akan dibahas bagaimana cara membangun dan mengimplementasikan *Network Access Control (NAC)* pada jaringan *Local Area Network (LAN)* menggunakan mikrotik. Adapun pembahasan yang akan dilakukan dapat dilihat seperti berikut ini.

A. Persiapan Alat dan Bahan

Dalam melakukan penelitian ini, alat dan bahan yang digunakan meliputi perangkat lunak dan perangkat keras.

1. Perangkat Lunak (Software)

Adapun perangkat lunak (software) yang digunakan dalam penelitian ini dapat dilihat seperti berikut.

- a. Sistem Operasi Windows 7
- b. Winbox

2. Perangkat Keras (Hardware)

Adapun perangkat Keras (hardware) yang digunakan dalam penelitian ini dapat dilihat seperti berikut.

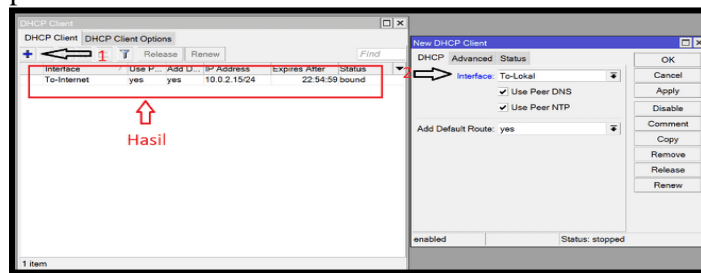
- a. 1 unit Laptop Asus sebagai server
- b. 1 unit RouterBoard RB 951
- c. 10 unit Laptop Lenovo, Dell, dan Asus sebagai client
- d. Mikrotik RouterOS

B. Konfigurasi Router Mikrotik

Agar dapat digunakan sebagai Router, Mikrotik Router Board harus di konfigurasi terlebih dahulu untuk menyesuaikan penggunaan jaringan. Adapun beberapa konfigurasi yang perlu dilakukan adalah sebagai berikut.

1. Konfigurasi DHCP Client

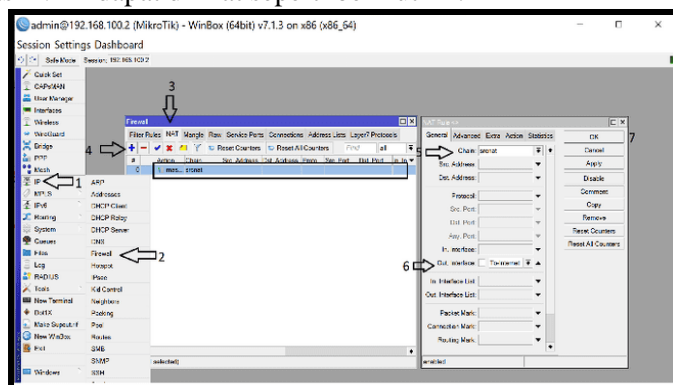
DHCP client digunakan untuk menghubungkan router Mikrotik dengan Modem agar dapat terkoneksi ke jaringan internet. Untuk melakukan konfigurasi ini dapat dilakukan menggunakan aplikasi winbox dan login menggunakan username dan password dari router mikrotik, selanjutnya masuk ke menu IP dan klik DHCP client kemudian tambahkan interface yang akan digunakan. Adapun hasil dari konfigurasi DHCP client dapat dilihat seperti berikut.



Gambar 10. Hasil Konfigurasi DHCP Client

2. Konfigurasi Firewall NAT

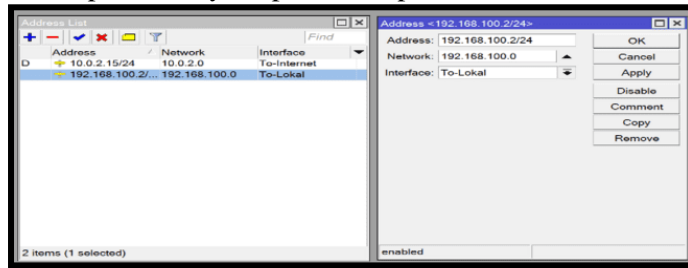
NAT digunakan oleh router agar dapat mentranslasikan domain menjadi IP address sehingga client yang terhubung dapat mengakses situs – situs yang sudah menggunakan domain. NAT juga bisa sebagai media untuk mentranslasikan alamat IP public sehingga dapat diakses oleh jaringan lokal. Untuk melakukan konfigurasi NAT dapat dilakukan melalui menu IP dan pilih firewall, selanjutnya klik tab NAT, kemudian tambahkan NAT dengan pengaturan Chain diisi dengan srcnat, out interface diisi dengan ethernet yang menuju modem (to-internet) dan action di isi dengan masquerade. Klik OK untuk menyimpan perubahan. Adapun hasil dari konfigurasi NAT dapat dilihat seperti berikut ini.



Gambar 11. Konfigurasi NAT

3. Konfigurasi IP address Lokal

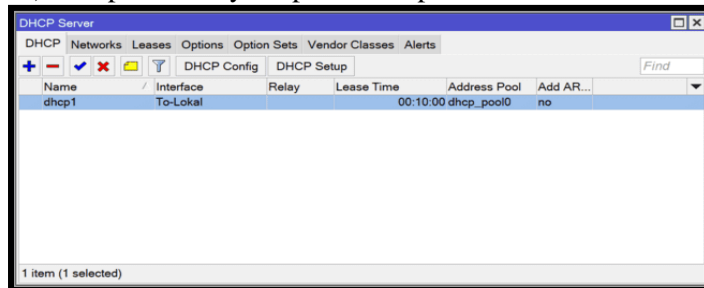
Untuk menambahkan IP *address* yang akan digunakan pada jaringan LAN, dapat dilakukan dengan caraklik menu IP dan pilih address kemudian tambahkan IP address 192.168.100.2/24. Adapun hasilnya dapat dilihat pada Gambar berikut.



Gambar 12 Hasil Konfigurasi IP Address Lokal

4. Konfigurasi DHCP Server

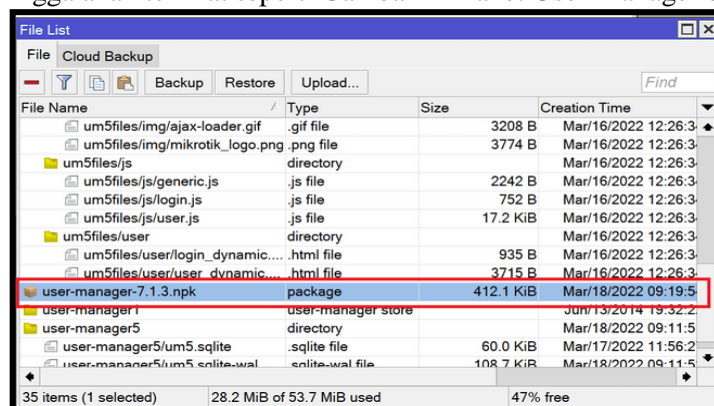
Untuk menambahkan DHCP *Server* yang akan digunakan pada jaringan LAN, dapat dilakukan dengan cara klik menu IP dan pilih DHCP Server kemudian tambahkan DHCP server melalui menu DHCP setup dan sesuaikan port ethernet yang akan digunakan yaitu ether 2 (To-Lokal). Adapun hasilnya dapat dilihat pada Gambar berikut.



Gambar 13 Hasil Konfigurasi DHCP Server

C. Konfigurasi User Manager

User manager akan menjadi aplikasi yang akan digunakan untuk menerapkan *authentication server* yang merupakan salah satu komponen untuk mendukung *Network Access Control (NAC)* di jaringan *Local Area Network (LAN)*. Untuk menerapkan user manager ini pada router mikrotik, sebelumnya kita harus menyiapkan paket install untuk router mikrotik sesuai dengan versi router OS yang digunakan, dimana dalam penelitian ini menggunakan router OS V7.1.3, setelah paket install user manager berhasil di download selanjutnya upload paket tersebut ke router mikrotik sehingga akan terlihat seperti Gambar 14 Paket User Manager berikut.



Gambar 14 Paket User Manager

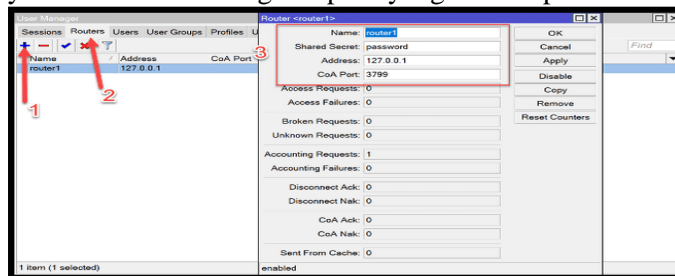
Setelah paket user manager sudah di upload, *reboot router* untuk menambahkannya ke sistem dari *router* mikrotik. Berikutnya setelah selesai reboot sistem maka user manager akan ada [ada sistem router mikrotik dan dapat langsung di konfigurasi untuk diterapkan pada *Network Access Control (NAC)* sebagai *authentication server* pada jaringan LAN. Adapun beberapa konfigurasi yang perlu dilakukan adalah sebagai berikut.

1. Mengaktifkan session pada user manager dengan memberikan tanda centang pada menu setting user manager.



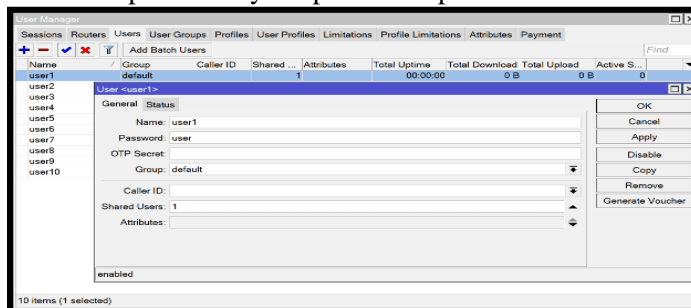
Gambar 15. Mengaktifkan Sessions User Manager

2. Menambahkan router yang akan dilayani oleh user manager, dimana untuk menambahkan router ini dapat dilakukan pada menu routers dan tambahkan router yang akan digunakan sebagai penerima layanan dari user manager seperti yang terlihat pada Gambar berikut.



Gambar 16. Menambahkan Router di User Manager

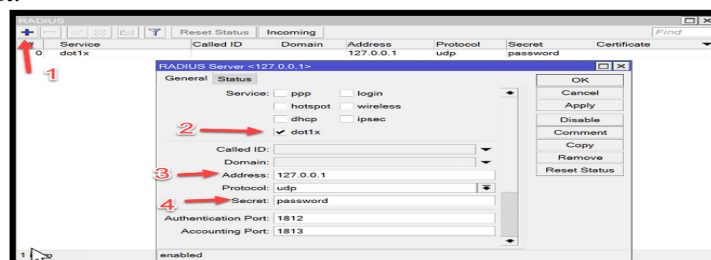
3. Menambahkan *user* untuk autentikasi oleh *client* atau *supplicant* pada jaringan LAN, dimana untuk menambahkan user ini dapat dilakukan pada menu user dan mengklik tombol tambah ataupun add batch users. Adapun hasilnya dapat dilihat pada Gambar berikut.



Gambar 17. Menambahkan User di User Manager

D. Mengaktifkan Radius Server

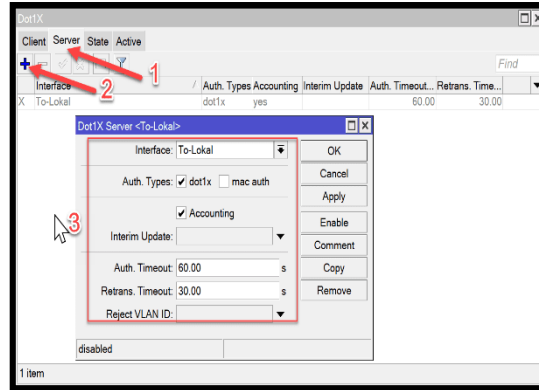
Radius server akan digunakan untuk melayani *service Authentication* yang sudah dibuat sebelumnya di *User Manager*, dimana untuk mengaktifkan RADIUS ini dapat dilakukan dengan masuk ke menu RADIUS pada *router* mikrotik dan tambahkan *Radius Server* seperti yang terlihat pada Gambar berikut.



Gambar 18. Mengaktifkan Radius Server

E. Konfigurasi Protokol 802.11x (dot1x) di Mikrotik

Protokol 802.11x ini merupakan salah satu protokol yang mendukung penerapan Network Access Control (NAC) pada Jaringan Local Area Network (LAN). Untuk menerapkan protokol dot1x dapat dilakukan dengan masuk ke menu Dot1x kemudian masuk ke tab Server dan tambahkan pengaturan seperti Gambar berikut.

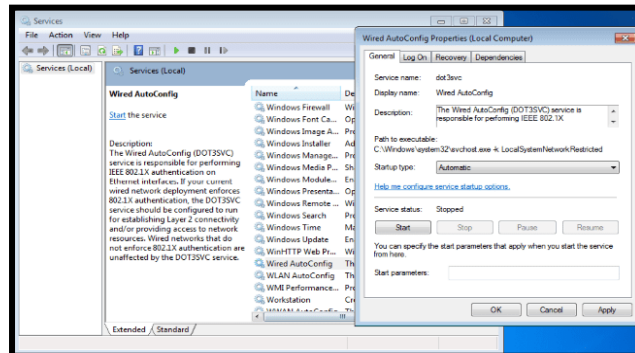


Gambar 19. Hasil Konfigurasi Protokol Dot1x

F. Konfigurasi Penggunaan NAC pada Client

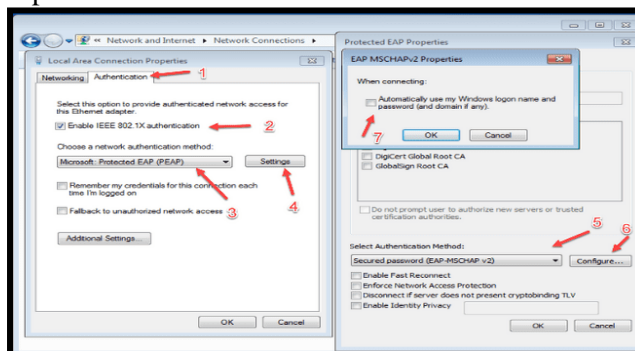
Untuk menggunakan layanan dari NAC pada client yang dalam penelitian ini menggunakan sistem operasi windows 7, maka ada beberapa konfigurasi yang harus dilakukan, adapun konfigurasi yang perlu dilakukan adalah sebagai berikut.

1. Mengaktifkan otomatis *wired auto config* dari menu service pada windows untuk merespon layanan protokol 802.11x (dot1x) yang sudah diterapkan pada *router gateway*. Berikut hasil konfigurasi yang sudah dilakukan.



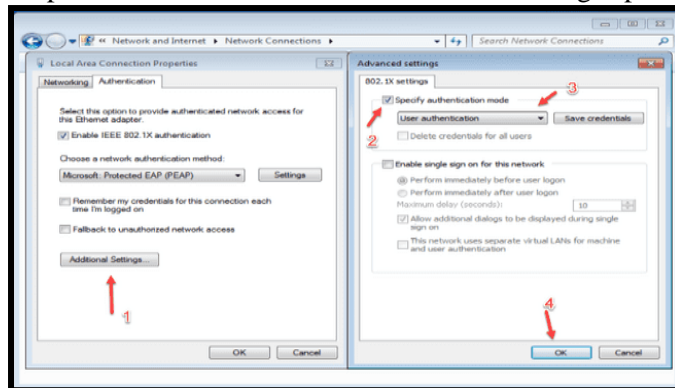
Gambar 20. Hasil Konfigurasi Wired Auto Config

2. Konfigurasi metode autentikasi yang akan digunakan, dimana dalam penelitian ini menggunakan metode autentikasi *Protected Extensible Authentication Protocol (PEAP)* yang meruokan metode standar dari penerapan protokol 802.11x. adapun konfigurasi yang perlu dilakukan dapat dilihat pada Gambar berikut.



Gambar 21. Hasil Konfigurasi Metode Autentikasi

3. Merubah autentikasi mode, hal ini dilakukan agar windows tidak secara otomatis melakukan koneksi ke dot1x server, sebab autentikasinya membutuhkan username dan password dari autentikasi server user manager. Adapun konfigurasi untuk merubah autentikasi mode dapat dilakukan melalui menu Additional setting seperti berikut.



Gambar 22. Hasil Konfigurasi Mode Autentikasi

10. Hasil Pengujian

Berikut ini merupakan hasil pengujian dengan menggunakan metode *blackbox*.

Tabel 1 Hasil Pengujian Metode Blackbox

No	Jenis Pengujian	Kriteria	Hasil	Keterangan
1.	Pengujian Akses Jaringan LAN	Dengan Otentikasi yang benar	Client atau Supplicant dapat terhubung dan mendapatkan alokasi IP address secara otomatis	Sesuai dengan Rencana
		Dengan Otentikasi yang salah	Client atau Supplicant tidak dapat terhubung dengan pesan Authentication Failed.	
2.	Pengujian Kualitas Layanan dengan <i>Network Access Control (NAC)</i>	Delay	1.92 ms	Dikategorikan BAIK sesuai dengan standar <i>Quality Of Service (QOS)</i>
		Jitter	33.3 ms	
		Throughput	548 kb	
		Packet loss	0%	
3.	Pengujian Active Hostname	Pengujian dilakukan dengan memperhatikan Active hostname yang terhubung.	Dapat menampilkan active hostname yang terhubung dalam Jaringan LAN	Dapat dipantau melalui Router Gateway.

11. Kesimpulan

Berdasarkan penelitian yang sudah penulis lakukan, maka dapat disimpulkan bahwa:

- a) Protokol 802.11x dapat diterapkan untuk *Network Access Control (NAC)* pada jaringan komputer dengan menggunakan *router* Mikrotik, dimana mikrotik dijadikan sebagai *authenticator* serta *authentication server (Radius Server)* menggunakan user manager.
- b) Kualitas layanan dengan metode *Quality Of Service (QOS)* untuk performansi jaringan LAN dengan penerapan *Network Access Control (NAC)* dikategorikan Baik berdasarkan pengujian yang sudah dilakukan dengan hasil delay sebesar 1.92 ms, *jitter* sebesar 33.3 ms, *packet loss* sebesar 0%, dan *throughput* sebesar 548 kb.

- c) *Router mikrotik* masih dapat memantau (monitoring) *active hostname* setelah penerapan *Network Access Control (NAC)* pada jaringan *Local Area Network* menggunakan protokol 802.11x.

Limitasi dan studi lanjutan

1. Protokol 802.11x ini dapat membantu pengamanan jaringan lokal menggunakan media kabel di instansi pemerintahan. Akan tetapi untuk memaksimalkan penggunaannya lebih baik dipisahkan antara router gateway dengan authentication server.
2. Penggunaan protokol 802.11x ini akan membantu proses pengamanan jaringan LAN, tetapi akan menyulitkan saat ada perangkat baru yang akan terpasang, sebaiknya penggunaan *Network Access Control (NAC)* hanya digunakan pada perangkat – perang penting saja.

REFERENSI

1. Damara, Shesia Rizki. 2020. “Analisis Dan Implementasi Kontrol Akses Jaringan Dan Kebijakan Pada PT. Asuransi Jiwa Sinarmas MSIG Tbk Menggunakan Sistem Genian NAC.” *Jurnal Ilmiah KOMPUTASI*.
2. IETF Working Group. “Forwarding and Control Element Separation (Forces) Framework,” IETF Working Group, [Online], <http://www.Ietf.org/html.charters/forcescharter.html/> diakses pada 19 Juni 2017.
3. I. Chaidir and R. R. Wirawan, “Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List,” *J. Tek. Komput. AMIK BSI*, vol. 4, no. 1, pp. 212–216, 2018.
4. Sinaga, Andre Rizal, Rakhmadhany Primananda, and Primantara Hari Trisnawan. 2018. “Implementasi Autentikasi Mode Multi-Auth Pada Jaringan Local Area Network Berbasis Kabel Menggunakan Protokol IEEE 802 . 1X Dan Radius Server.” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* 2(10): 3307–14.
5. P. Simanjuntak et al., “Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan,” *J. Teknol. Inf. Politek. Telkom*, vol. 1, no. 1, pp. 1–35, 2019.
6. Syahrudin. 2019. *Implementasi Kebijakan Publik: Konsep Teori Dan Studi Kasus*. Bandung: Nusa Media.
7. Towidjojo Rendra, 2012. *Mikrotik Kunfu Kitab 1*. Jasakom, Yogyakarta.
8. Vivanda, Tabita Wahyu Eka, and Aria Indah Susanti. 2019. “Rancang Bangun Sistem Jaringan Hotspot Berbasis Manajemen User Dengan Menggunakan Userman Dan Radius Server Pada Mikrotik Routerboard Di SMK Negeri 1 Kemlagi.” *JURNAL TECNOSCIENZA; Vol 3 No 2 (2019): TECNOSCIENZA*.