JUMANJI | Vol. 3 | No. 1 | Halaman 74 - 83
ISSN (p): 2598-8050 April 2019
ISSN (e): 2598-8069

Implementasikan *Single Service Set Identifier* Menggunakan *Dynamic VLAN* Dan *Active Directory* Pada Perangkat Nirkabel

WAHYU WIDODO[1], DIAN DIDIK PURWANTO[2]

[1,2] Jurusan Teknik Informatika, STMIK El Rahma Yogyakarta
Email : wahyu@stmikelrahma.ac.id

ABSTRAK

Semakin banyak perangkat akses dan mobilitas pegawai memerlukan pengelolaan agar bisa perangkat akses yang ada dapat dimanfaatkan oleh banyak pengguna dari unit kerja yang berlainan dengan tidak mengurangi faktor keamanan. Perancangan jaringan nirkabel dengan satu buah nama jaringan dengan autentikasi berbasis data Active Directory diimplementasikan untuk mengatasi permasalahan yang ada. Penelitian ini merancang dan mengimplementasikan single service set identifier pada perangkat akses, keamanan akses berbasis layanan autentikasi Network Policy Server dengan data pengguna tersimpan pada layanan Active Directory Domain Services pada server Windows 2008R2.Hasil pengujian pada perangkat laptop dengan sistem operasi Windows 10, user dapat melakukan autentikasi dan mendapatkan ip address sesuai profile grup user.

Kata kunci: *active directory , jaringan nirkabel*, *single ssid*.

ABSTRACT

The more access and employee mobility devices require management so that existing access devices can be used by many users from different work units without reducing security factors. Designing a wireless network with one network name with Active Directory data-based authentication is implemented to overcome existing problems. This research designs and implements single service set identifier *on access devices, access security based authentication service Network Policy Server with user data stored on Active Directory Domain Services on Windows 2008R2 servers. The results of testing on laptop devices with Windows 10 operating system, users can authenticate and get ip address according to user group profile.*

Keywords*: active directory, single ssid, wirelles.*

COPYRIGHT © JUMANJI 2019

1. PENDAHULUAN

Pemerintah Kota Yogyakarta dituntut untuk dapat memanfaatkan teknologi informasi untuk pelayanan public dengan membangunan jaringan intranet mandiri yang menghubungkan 27 Organisasi Perangkat Daerah (OPD), 14 kecamatan, 45 kelurahan, 18 puskesmas dan 6 puskesmas pembantu dengan pusat koneksi di Balaikota Yogyakarta **(Suroatmojo, 2015).** Untuk semakin meningkatkan kecepatan pelayanan data bagi pelayanan masyarakat, Pemerintah Kota Yogyakarta tidak hanya mengembangkan jaringan data melalui kabel tetapi juga nirkabel (*wifi*). Bertambahnya penggunaan perangkat *All in one Computer, notebook, tablet dan smartphone* yang terkoneksi melalu media *wifi* membuat kebutuhan akses *wireless* semakin meningkat **(Sadikin, 2015)**. Dinas Komunkasi Informatika dan Persandian Kota Yogyakarta mengakomodir kebutuhan akses *wifi* melakukan penambahan jumlah perangkat *Access Point* sehingga jaringan *wifi* dapat diakses secara mudah oleh pegawai. Perangkat dipasang dengan memberikan nama *service set indentifier* (*ssid*) sesuai nama kantor dimana perangkat tersebut dipasang dan diamankan dengan kata kunci berbagi (*preshared-key*) tertentu.

Permasalahan yang terjadi di lapangan bahwa setiap karyawan Pemerintah Kota Yogyakarta berkeinginan untuk selalu terhubung dengan jaringan walaupun tidak dikantor asal tetapi terkendala banyaknya nama jaringan nirkabel yaitu *service set indentifier (ssid)* dan kata kunci berbagi (*preshared-key*) yang berbeda beda sehingga pegawai kesulitan untuk memilih jaringan mana untuk terkoneksi ke intranet Pemerintah Kota Yogyakarta. Pengamanan dengan kata kunci berbagi (*preshared-key*) menimbulkan kerentanan kebocoran akses maka diperlukan pengelolaan untuk mencegah penggunaan jaringan *wireless* oleh pihak yang tidak berkepentingan **(Omolokun, 2017)**. Kebutuhan pegawai untuk terkoneksi ke jaringan kantor asal melalui *Virtual LAN (Vlan)* agar tidak mengurangi ketersediaan *ip* di tempat pegawai terkoneksi. Maka dari itu diperlukan adanya sebuah sistem autentikasi jaringan yang baik.

Untuk mengatasi permasalahan dan memberikan solusi atas permasalahan tersebut, penulis bermaksud untuk mengimplementasikan *single ssid multiple profile* menggunakan *dynamic vlan* dan *active directory* pada jaringan nirkabel Pemerintah Kota Yogyakarta. Penggunaan satu nama jaringan atau *service set indentifier (ssid)* yang memungkinkan pengguna untuk terkoneksi ke jaringan lokal kantor asal dengan autentikasi yang tersimpan pada server *Active Directory* **(Cahyo, 2017)**. Sistem ini akan melakukan pengecekan identitas pengguna agar memastikan bahwa pengguna tersebut sah untuk mengakses jaringan internet dan terkoneksi dengan jaringan kantor asal.

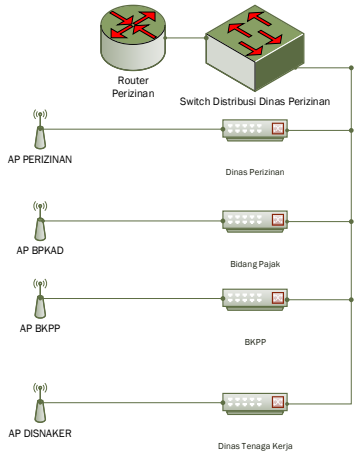
2. PEMBAHASAN

2.1. Metode Penelitian

Metode penelitian dengan melakukan observas jaringan wireles untuk mendapatkan data *ssid* yang terdapat pada pemerintah Kota Yogyakarta. Observasi dilakukan menggunakan Aplikasi *Wifi Analyser. Wifi Analyser* adalah perangkat pemindai nama *SSID* pada jaringan nirkabel yang diinstall pada perangkat telepon genggam berbasis android. Untuk mempermudah identifikasi jaringan Pemerintah Kota Yogyakarta, ditentukan *SSID* bernama "SEGOROAMARTO". Pemilihan kata SEGOROAMARTO dilatarbelakangi gerakan Segoro Amarto yang merupakan kepanjangan dari Semangat Gotong Royong Agawe Majune Ngayogyakarta atau semangat gotong royong menuju kemajuan Yogyakarta). Gerakan ini adalah ide Sri Sultan HB X **(Suroatmojo, 2015).**

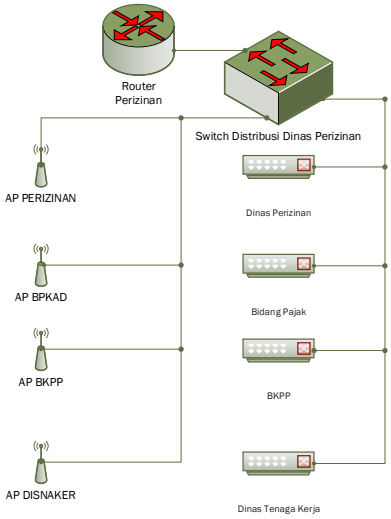
2.3. Perancangan Sistem

Berdasar Peraturan Daerah Kota Yogyakarta No 5 tahun 2016 tentang Pembentukan Dan Susunan Perangkat Daerah Kota Yogyakarta, maka jaringan komputer pada Organisasi Perangkat Daerah Kota Yogyakarta mempunyai alokasi ip seperti lampiran (2) dengan topologi setiap OPD adalah seperti Gambar 1.



Gambar 1 Topologi Jaringan yang Sudah Ada

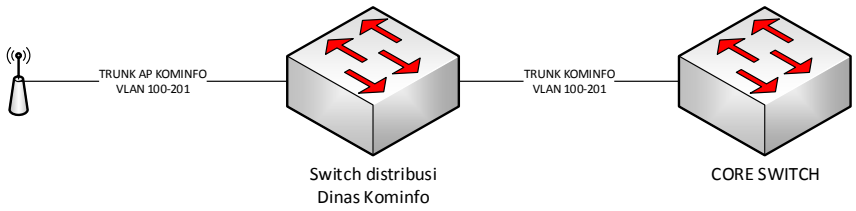
Topologi diatas memiliki kelemahan, yaitu setiap Access Point hanya dapat melewatkan vlan OPD saja. Untuk merancang sebuah jaringan wireless single ssid multiple vlan dengan active directory diperlukan modifikasi topologi seperti Gambar 2.



Gambar 2 Rancangan Topologi Baru

Dengan topologi seperti Gambar 2 di atas, semua switch terhubung secara link trunk pada switch distribusi, sehingga memungkinkan untuk melewatkan semua vlan yang terdaftar pada switch distribusi. Konfigunasi *switch* pada perancangan jaringan sesuai pada Gambar 2 dimana terdapat *switch* distribusi Dinas Kominfo sebagai penghubung antara *Access Point* dengan core *switch* seperti pada Gambar 3.

COPYRIGHT © JUMANJI 2019



Gambar 3 Rancangan Konfigurasi Switch

Untuk dapat menghantarkan *vlan* opd dari *userwireless*, setiap *switch* harus dapat mengakses *vlan opd* yang diizinkan. Kumpulan *vlan-vlan* yang diizinkan untuk dapat diakses melaui *SSID* SEGOROAMARTO kemudian dikoneksikan dengan *Access Point* dengan mode *link tunk* seperti pada Gambar 4.

```
SW-KOMINFO-L2-PANEL#show interfaces status | include  connected
Gi1/0/6                   connected    21         a-full  a-100 10/100/1000BaseTX
Gi1/0/10  UNIFI-SMART-CITY  connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/11  UNIFI-RISET       connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/12  UNIFI-APLIKASI    connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/13  UNIFI-KABIDTI     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/15  UNIFI-PKIT        connected    trunk      a-full  a-100 10/100/1000BaseTX
Gi1/0/19  UNIFI-NOC         connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/26  SW-HARDWARE       connected    21         a-full  a-100 10/100/1000BaseTX
Gi1/0/40                    connected    21         a-full  a-100 10/100/1000BaseTX
Gi1/0/46                    connected    21         a-full  a-100 10/100/1000BaseTX
Gi1/0/47  PC-DIDIK          connected    250        a-full a-1000 10/100/1000BaseTX
Gi1/0/48  SW-UNIFI          connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/52  TO-NOC-SW-Lt2-Port connected    trunk      a-full a-1000 1000BaseLX SFP
SW-KOMINFO-L2-PANEL#
```

Gambar 4 Interface Switch Distribusi Dinas Kominfo

Setiap *port* pada *switch* yang terkoneksi ke *Access Point* dikonfigurasi hingga dapat melalukan semua *vlan* OPD. Pada tabel 1 adalah contoh konfigurasi *switch* untuk port no 15.

Table 1 Konfigurasi Switch

```
SW-KOMINFO-L2-PANEL#show running-config interface gi1/0/15
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet1/0/15
 description UNIFI-PKIT
 switchport trunk native vlan 250
 switchport trunk allowed vlan 10-256
 switchport mode trunk
end

SW-KOMINFO-L2-PANEL#
```

Perancangan memanfaatkan fasilitas aplikasi layanan *Windows* Server 2008R2 antara lain *Active Directory Domain Services*, *Active DirectoryCertificate Services*, dan *NetworkPolicy services.* Untuk memanfaatkan layanan *Active Directory Domain Services,* administrator harus melakukan konfigurasi terlebih dahulu dengan cara diketikkan perintah dcpromo, windows server akan mengecek instalasi *Active Directory* **(Amin, 2017)**.

Enkripsi PEAP dengan EAP-MS-CHAP v2 memvalidasi server RADIUS berdasarkan sertifikat yang ada di server. Selain itu, sertifikat server harus dikeluarkan oleh *CA* publik yang dipercaya oleh komputer *klien*. Artinya, sertifikat *CA* publik sudah ada di folder Otoritas Sertifikasi Root Tepercaya di toko/tempat daftar penyimpanan sertifikat komputer *klien*. Untuk mengkonfigurasi Microsoft *Windows* Server versi 2008 R2 sebagai server *CA* yang

COPYRIGHT © JUMANJI 2019

mengeluarkan sertifikat ke *NPS*, server perlu menambah *role* pada server windows **(Utama, 2013)**.

Network Policy Services (*NPS*) digunakan sebagai fungsi *radius* untuk mengautentikasi *klien* nirkabel. Instalasi *NPS* dimulai dengan menambahkan server roles sebagai *Network* Policy dan Access Services. Langkah selanjutnya adalah membuat WLAN *group* baru. WLAN Grup baru dibuat untuk mempermudah manajemen pemilihan profil hingga pada suatu saat profil dapat dengan mudah diganti dan dengan cepat dikembalikan lagi.

Konfigurasi pada *Access Point* dilakukan untuk mengatur single *SSID* dan mempermudah *user* untuk menghubungunkan perangkat. AP pada penelitian ini menggunakan perangkat UniFi. Produsen perangkat menyediakan aplikasi UniFi Controller untuk melakukan seting pada perangkat Unifi **(Geier,2005)**. Konfigurasi *Access Point* dimulai dengan memilih *site* yang akan dikonfigurasi, *site* dapat berupa sekumpulan *Access Point* yang mempunyai konfigurasi yang sama atau mewakili area tertentu untuk mempermudah pengelolaan.

Setiap pengguna jaringan yang terhubung melalui *wifi* dirancang agar terhubung kejaringan OPD asal. Untuk itu perlu pembuatan profil kantor berupa *group* pada *Active Directory*. Pembuatan profil *group* ini dapat dimulai dengan membuka *Active Directory* seperti pada Gambar 5.

Gambar 5 Menu Active Directoy

Setiap *user* yang akan terkoneksi akan diautentikasi terlebih dahulu oleh *Network Policy Server (NPS)*. Apabila akses berhasil diautentikasi, NPS akan menentukan profil mana yang berlaku menurut policies yang berlaku adalah setiap *user* akan terkoneksi dengan *vlan* OPD asal. Untuk membuat profil koneksi sesuai OPD masing masing user, perlu dilakukan pengaturan policies pada *NPS*.

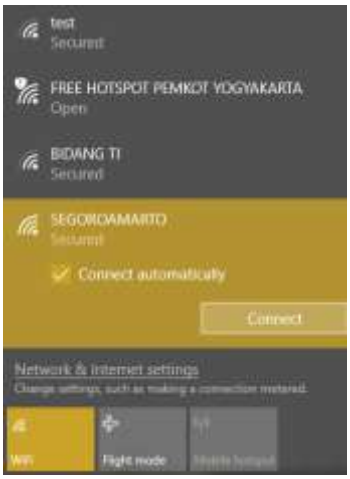
3. HASIL DAN PEMBAHASAN

Akses jaringan *wireless* merupakan perangkat jaringan komputer tanpa kabel dalan media komunikasinya jadi yang digunakan yaitu menggunakan media frekuensi dalam penelitian ini menggunakan frekuensi 2,4GHz dan 5,8Hgz. Sedangkan yang dimaksud Single *SSID* adalah menggunakan satu buah *SSID* bermana SEGOROAMARTO. Multiple *VLAN* artinya pada *SSID* yang diakses dapat memberikan *vlan* dan ip sesuai dengan data pengguna. Data pengguna dan *group* OPD disimpan pada *Active Directory*. Sedangkan yang dimaksud *roaming* dalam penelitian ini adalah perpindahan *user* pengguna *wifi* dari lokasi satu ke lokasi lain dan dari *wifi* satu ke *wifi* yang lain tanpa mengalami putus koneksi **(Suyatno, 2015)**.

User pengguna *wifi* juga harus autentik, dengan maksud *user* dan *password* harus sesuai dengan data yang telah disimpan didalam *Active Directory*. *Network* Policy Server berperan untuk melakukan autentikasi dan authorisasi *user* dan *password* pengguna *wifi*, selain itu akan melakukan pengecekan jika *user* yang dipanggil ada dalam database maka *radius* akan memberikan ijin terhadap *user* tersebut **(Muskitta,2016).** Pada implementasi digunakan pengujian *username* yaitu :

a. Menggunakan data *user* name dan *password* yang sesuai pada *Active Directory*
b. *User*name dan atau *password* tidak sesuai dengan data pada *Active directory*

Proses koneksi dengan enkripsi PEAP hanya perlu dilakukan sekali saja untuk jangka waktu aktif sertifikat atau selama *password* pada *Active Directory* sama. Proses koneksi ke ssid SEGOROAMARTO dilakukan dengan cara memilih *ssid* SEGOROAMARTO seperti pada Gambar 6.



Gambar 6 Memilih SSID Segoroamarto

Ketika *user*melakukan autentikasi, maka *NPS* akan melakukan autentikasi. Ketika berhasil, maka terdapat keterangan *Network Policy Server granted access to a user* seperti pada Gambar 7

Gambar 7 Event Properties

Data lengkap dari koneksi diatas seperti pada tabel 2 berikut ini.

Table 2 Contoh Data Event Properties

Data Event Viewer
Log Name : Security
Source : Microsoft-*Windows*-Security-Auditing
Date : 5/29/2018 9:45:41 AM
Event ID : 6272
Task Category : *Network* Policy Server
Level : Information
Keywords : Audit Success
User : N/A
Computer : actor.jogjakota.go.id
Description:
Network Policy Server granted access to a *user*.

User:
Security ID: JOGJAKOTA\didik
Account Name: didik
Account Domain: JOGJAKOTA
Fully Qualified Account Name: JOGJAKOTA\didik

Client Machine:
Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -
OS-Version: -
Called Station Identifier: 80-2A-A8-D4-46-E7:SEGOROAMARTO
Calling Station Identifier: 70-1C-E7-C4-AF-C7

NAS:
NAS IPv4 Address: -
NAS IPv6 Address: -
NAS Identifier: 802aa8d346e7
NAS Port-Type: *Wireless* - IEEE 802.11
NAS Port: 0

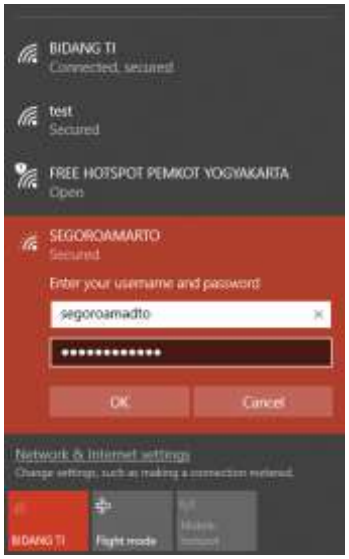
RADIUS Client:
Client Friendly Name: Unifi-Kominfo-xxx
Client IP Address: 192.168.8.175

Authentication Details:
Connection Request Policy Name: SEGOROAMARTO
Network Policy Name: kominfo
Authentication Provider: *Windows*
Authentication Server: actor.jogjakota.go.id
Authentication Type: PEAP
EAP Type: Microsoft: Secured *password* (EAP-MSCHAP v2)
Account Session Identifier: -
Logging Results: Accounting information was written to the local log file.

Quarantine Information:
Result: Full Access
Session Identifier:

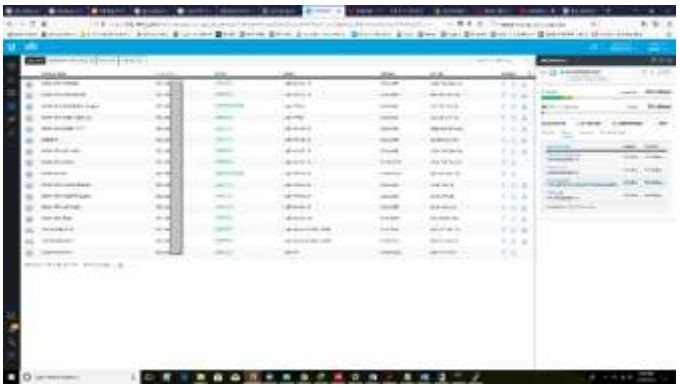
Dari data diatas dapat diambil informasi bahwa pada tanggal 29 Mei 2018 komputer actor.jogjakota.go.id berhasil melakukan autentikasi dan mengizinkan *user* didik untuk terkoneksi dengan jaringan. *klien* dan terhubung melalui ssid SEGOROAMARTO dengan *mac addresswireless* 80-2A-A8-D4-46-E7 menggunakan perangkat *wireless* dengan mac address 70-1C-E7-C4-AF-C7.

Koneksi tersebut sesuai dengan *connection request policy* SEGOROAMARTO dan *network* policy name kominfo sehingga akan mendapatkan *vlan* sesuai pengaturan *policy* pada kominfo. Autentikasi dilakukan oleh actor.jogjakota.go.id dengan tipe autentikasi *PEAP* dan type *EAP EAP-MSCHAPv2*. Ketika penguna hendak terkoneksi dengan ssid SEGOROAMARTO namun memasukkan *user* dan *password* yang tidak sesuai dengan daftar yang ada pada active directory maka *Network* Policy Server melarang akses dari *user*. Pada contoh gambar 8, pengguna memasukkan *user* yang tidak tersimpan pada *Active Directory.*



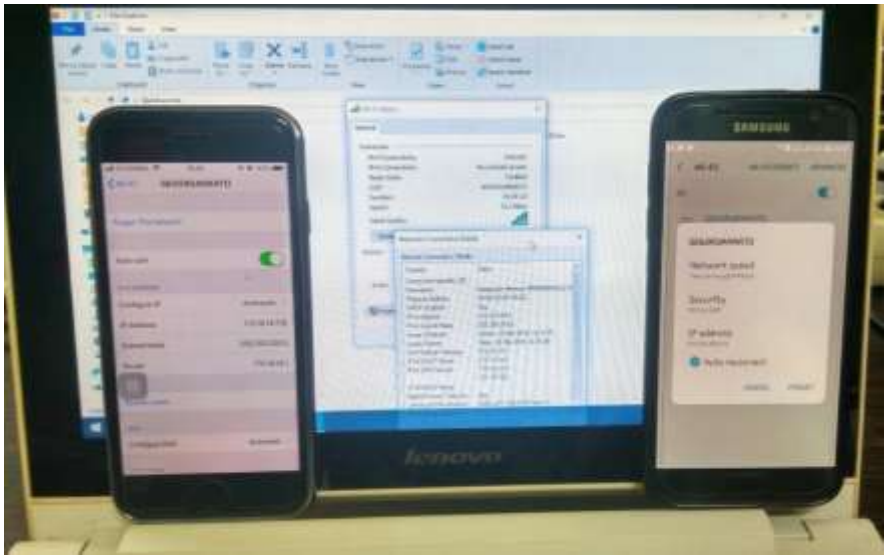
Gambar 8 User tidak sesuai

Akses pengguna yang tidak berhasil diautentikasi dapat dilihat pengelola melalui aplikasi Event Viewer diperoleh keterangan bahwa *Network* Policy Server denied access to a *user* dengan *account* name segoroamarto. Perangkat yang sudah melakukan autentikasi dapat terkoneksi secara otomatis jika terkoneksi dengan ssid SEGOROAMARTO tidak perlu mengisikan *user* dan *password* kembali *user* dan *password* sudah tersimpan pada profil jaringan. Dengan menggunakan software unifi controller, dapat diketahui perangkat apa saja yang terkoneksi pada sebuah *Access Point* seperti pada Gambar 9.



Gambar 9 perangkat terkoneksi melalui controller Unifi

Dari keterangan gambar diatas didapat keterangan bahwa ada tiga *klien* yang menggunakan *ssid* SEGOROAMARTO yaitu sebuah *handphone* S7Masdidi, sebuah handphone iPhone-MD dan sebuah pc DESKTOP-P74JIU5 yang sama sama terkoneksi ke jaringan seperti pada Gambar 10.



Gambar 10 perangkat terkoneksi

4. KESIMPULAN DAN SARAN

Untuk membuat sebuah jaringan yang mudah diketahui sebagai *ssid* resmi Pemerintah Kota Yogyakarta adalah dengan membuat hanya ada satu *ssid / single ssid* yang dipancarkan oleh setiap *Access Point* milik Pemerintah Kota Yogyakarta. Dalam hal ini *ssid* akan diberi nama SEGOROAMARTO.Dengan menggunakan *Active Directory*, maka autentikasi dilakukan oleh *service NPS* (*Network Policy Server)* dengan cara menanyakan *user* dan *password* pada setiap perangkat yang pertama kali akan terkoneksi. Apabila autentikasi berhasil, Komputer akan menyimpan data koneksi. Apabila perangkat akan terkoneksi kembali cukup dengan membaca data yang tersimpan pada *known wireless network* dan akan otomatis terkoneksi, tanpa perlu menanyakan *user* dan *password* kembali. Agar setiap pengguna *wireless* SEGOROAMARTO dapat terhubung dengan jaringan OPD asal, perlu dilakukan langkah langkah :

a. Membuat *vlan* untuk setiap OPD
b. Pengelompokan *user* pada sebuah *usergroup* sesuai nama OPD
c. Pengalokasian *vlan* sesuai *usergroup*

Penelitian selanjutnya dapat dikembangkan lebih komplek lagi, diantara melakukan pembatasan kemampuan *user* pada sisi *Network Policy Server* dengan jumlah perangkat yang dapat login, waktu dan limitasi kuota. Selain itu perlu adanya sistem backup apabila server *Active Directory* utama mengalami kegagalan.

COPYRIGHT © JUMANJI 2019

DAFTAR RUJUKAN

Armin, A., Abrar, A., & Sorongan, E. (2017). Sentralisasi Otentikasi Pengguna Dan Pengelolaan Sumber Daya Jaringan Komputer Politeknik Negeri Balikpapan Dengan Menggunakan, (Politeknik Negeri Balikpapan).

Cahyo, A. D. (2017). Implementasi Metode Aaa (Authentication, Authorization,Accounting) Dalam Management User Pada Access Point (Studi Kasus : Laboratorium Sistem Informasi Dan Programming), (Fakultas Teknik, Universitas Halu Oleo).

Geier, J. (2005). *Wireless Networks first-step*. Yogyakarta: Andi.

Microsoft. (n.d.). Network Policy Server (NPS). Retrieved May 10, 2018, from https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

Muskitta, Y. J., Yohanes, B. W., & Wardana, H. K. (2016). Implementasi Protected Extensible Authentication Protocol (PEAP) menggunakan Remote Access Dial In User Service (RADIUS), (Universitas Kristen Satya Wacana, Salatiga).

Omolokun, T. (2017). Wireless Single SSID. Retrieved August 10, 2018, from https://mum.mikrotik.com/presentations/NG17/presentation_4854_1512134649.pdf

Sadikin, N. (2015). Implementasi Keamanan Jaringan Wireless Enterprise Menggunakan Remote Authentication. *Seminar Nasional Teknologi Informasi Dan Multimedia*, (Teknik Informatika Universitas Islam Attahiriyah Jakarta).

Suroatmojo, W. (2015). Analisis Program Segoro Amarto sebagai Wujud Pelaksanaan Good Governance Pemerintah Kota Yogyakarta, (Magister Ilmu Pemerintahan, Universitas Muhammadiyah Yogyakarta).

Suyatno, T. (2015). Wifi Roaming Menggunakan Captiv Portal Dengan Authotentifikasi Radius Server, (Teknik Informatika STMIK El Rahma).

Utama, I. (2013). *Active Directory & Jaringan Windows Server 2008*. Jakarta: Elex Media Komputindo.