

OTENTIKASI PENGGUNA JARINGAN MENGGUNAKAN RADIUS WINDOWS 2008 SERVER PADA PT PERTAMINA

Denda Aristiara¹, Cahyani Budihartanti²

¹ Jurusan Teknik Informatika, STMIK Nusa Mandiri, Jl. Kramat Raya No.25, Jakarta Pusat, 10420, Indonesia. t4ksh1d0@gmail.com

²Jurusan Sistem Informasi, STMIK Nusa Mandiri, Jl. Damai No.8, Warung Jati Barat (Margasatwa), Pasar Minggu, Jakarta, Indonesia.
cahyani.cbh@nusamandiri.ac.id

ABSTRAKSI

Sistem koneksi jaringan kabel pada PT Pertamina Marketing Operation Region III belum memiliki mekanisme keamanan yang dapat memastikan pengguna jaringan yang terhubung adalah pengguna yang memiliki hak akses kedalam jaringan perusahaan. Sistem otentikasi, otorisasi dan akunting akan sangat membantu dalam menjaga keamanan jaringan perusahaan, karena ketiga point tersebut berguna untuk memeriksa dan memastikan pengguna jaringan yang terkoneksi ke dalam jaringan perusahaan, sehingga berguna untuk meminimalisir kemungkinan tindak kejahatan dalam operasional teknologi informasi yang dimiliki perusahaan. RADIUS server adalah perangkat server yang menyediakan sistem otentikasi, otorisasi dan akunting bagi pengguna jaringan. Pemanfaatan RADIUS Windows 2008 Server yang dimiliki PT Pertamina Marketing Operation Region III untuk otentikasi pengguna jaringan diharapkan mampu meningkatkan sistem keamanan perusahaan.

Keywords: RADIUS Server, RADIUS Windows, Otentikasi Jaringan, Keamanan Jaringan.

ABSTRACT

Wired network connection system on PT Pertamina Marketing Operations Region III does not yet have a mechanism that can ensure the security of networks connected users are users who have the right of access to the corporate network . System authentication , authorization and accounting will be very helpful in maintaining the security of the corporate network , because the three points are useful to check and ensure the network users are connected to the corporate network , so it is useful to minimize the possibility of crime in the information technology operations of the company. RADIUS server is a server software system that provides authentication, authorization , and accounting for network users . Windows 2008 RADIUS Server Utilization owned PT Pertamina Marketing Operations Region III for authentication of network users is expected to increase the company's security system.

Keywords: RADIUS Server, RADIUS Windows, Network Authentication, Network Security.

PENDAHULUAN

Sebuah institusi dan instansi yang menjadikan teknologi informasi dan komunikasi sebagai media utama dalam operasional pekerjaannya, keamanan jaringan menjadi hal yang penting bagi pribadi maupun instansi dalam menjaga kerahasiaan dan keamanan data yang dimilikinya. Seorang administrator jaringan perlu memperhatikan dalam pemberian hak akses kepada user atau pengguna jaringan. Otorisasi penggunaan hak akses dapat memberikan nilai tambah dalam menjaga keamanan jaringan, sehingga pengguna jaringan yang tidak memiliki otoritas atau hak izin akses tidak dapat terhubung dengan jaringan yang dimiliki, dan seorang administrator jaringan juga dapat membatasi apa saja yang dapat diakses oleh pengguna jaringan. Sebuah radius server dapat memenuhi kebutuhan tersebut, radius server digunakan sebagai sistem otentikasi, otorisasi dan akunting untuk proses akses penggunaan jaringan.

Menurut (Sujarwo,2010) “Autentikasi adalah sebuah usaha pengecekan identitas seseorang pengguna sistem komunikasi pada proses login ke dalam sebuah sistem”.

Belum adanya proses otentikasi pengguna jaringan untuk meningkatkan sistem keamanan teknologi informasi dan komunikasi yang berjalan untuk mencegah dan mengurangi adanya tindak kejahatan, mengingat PT Pertamina merupakan perusahaan besar dengan teknologi informasi dan komunikasi menjadi fungsi penunjang yang vital dalam operasional pekerjaan. Berdasarkan latar belakang tersebut maka menarik minat peneliti untuk membahas tema tersebut dengan judul OTENTIKASI PENGGUNA

JARINGAN MENGGUNAKAN WINDOWS RADIUS 2008 SERVER PADA PT. PERTAMINA.

BAHAN DAN METODE

Konsep Dasar Jaringan

Menurut (Tim Wahana Komputer,2013) ”Jaringan komputer merupakan sebuah sistem yang terdiri dari komputer – komputer yang didesain untuk dapat saling berbagi baik sumberdaya, data maupun akses“.

Jaringan komputer kini telah berkembang dan menjadi suatu kebutuhan di segala aspek, baik dalam bidang industri maupun pendidikan, karena jaringan komputer mempunyai beberapa manfaat, yaitu :

1. *Sharing Resource*
2. *Integrasi Data*
3. Pengembangan dan pemeliharaan
4. Keamanan Data
5. *Network Access*

Untuk konektifitas jaringan komputer secara garis besar dapat dibedakan menjadi 2 model, yaitu :

1. *Peer To Peer*

Menurut (Tim Wahana Komputer,2009) “Secara prinsip, hubungan peer to peer ini adalah bahwa setiap komputer dapat berfungsi server (penyedia layanan) dan client”.

2. *Client Server*

(TimWahanaKomputer ,2009)“Client Server merupakan arsitektur jaringan komputer yang memisahkan client dengan server, jaringan tipe ini merupakan jaringan yang termasuk sering ditemui di jaringan computer”.

Jaringan komputer jika ditinjau dari luas jangkauannya, terbagi atas:

1. *Local Are Network (LAN)*

Menurut (Tim Wahana Komputer,2009) “LAN adalah

jaringan komputer yang hanya mencakup area tertentu yang berukuran kecil, misalnya rumah, kantor, atau gedung. LAN zaman sekarang umumnya menggunakan teknologi ethernet sebagai infrastruktur“

2. Metropolitan Area Network (MAN)

Menurut (Tim Wahana Komputer,2009)

“Metropolitan Area Network merupakan jaringan komputer yang menghubungkan dua atau lebih Local Area Network atau Campus Area Network namun tidak melewati batas kota, atau area metropolitan tertentu“.

3. Wide Area Network (WAN)

Menurut (Tim Wahana Komputer,2009)

“WAN adalah jaringan komunikasi data yang mencakup area geografis yang luas. Misalnya antara satu negara dengan negara lainnya. Sebuah WAN biasanya menggunakan fasilitas yang disediakan oleh perusahaan telekomunikasi”.

IP Address

Menurut Sukmaaji dkk (2008:61) ”IP Address merupakan pengalaman dengan panjang 32 bit yang terbagi dalam dua bagian yaitu identitas jaringan dan identitas host. Format pengalaman yang digunakan dikenal dengan istilah *dotted-decimal notation*, yang masing-masing bagian terdiri dari 8 bit”.

Setiap node yang terhubung pada sebuah jaringan yang berbasis protocol TCP/IP haruslah memiliki sebuah alamat IP (*IP Address*) yang unik, artinya dalam satu jaringan tidak boleh ada node yang memiliki

alamat yang sama persis.

Ip address terdiri dari deret empat angka di mana tiap angka besarnya antara 0 sampai 255. Jika diuraikan dalam bilangan biner, maka akan menjadi 32 bit. Seperti terlihat pada tabel berikut :

Tabel 1 *IP address*

Dec	10	103	7	1
Bin	00001 010	011001 11	000001 11	000000 01

Pembagian IP dilakukan berdasarkan kelas-kelas yang diatur oleh sebuah badan internasional yang menangani IP dan DNS, yaitu *Internic*. Maksud pembagian kelas ini adalah agar alokasi IP dapat disesuaikan dengan permintaannya. Bila permintaan itu bermaksud mengadakan/menjadi provider jaringan internasional dengan *backbone* yang memiliki *bandwidth* raksasa antar benua, maka ia akan diberi IP kelas yang tinggi misalnya kelas A. Sedangkan jika ia hanya mendaftar untuk jaringan kecil misalnya untuk kantor biasa, maka ia akan diberi IP dengan kelas C. IP dibagi menjadi beberapa kelas berdasarkan pada pembagian *Network ID* dan *Host ID*, diantaranya :

Tabel 2 Perbandingan Kelas *Ip address*

Kelas	Network Bit	Jumlah Host Jaringan	Oktat Pertama	Subnet Mask
A	8	16.777.214	0 – 127	255.0.0.0
B	16	65.534	128 – 191	255.255.0.0
C	24	254	192 – 223	255.225.255.0

Sumber: www.ilmukomputer.com

Perangkat Jaringan

Perangkat keras yang dibutuhkan untuk membangun sebuah jaringan komputer diantaranya :*server, client, Network Interface Card (NIC): kabel, bridges, switch,*

hub, modem, repeater, router dan lainnya yang dibutuhkan untuk proses transformasi data di dalam jaringan komputer.

1. *Server*

Server komputer yang memberikan suatu layanan bagi komputer lain dalam jaringan.

2. *Client (Workstation)*

Workstation adalah perangkat keras yang digunakan untuk meminta dan menerima layanan dari server dalam suatu jaringan”.

3. *Network Interface(NIC)*

Network Interface Card atau merupakan sebuah hardware komputer yang didesain guna memungkinkan komputer berkomunikasi menggunakan jaringan. NIC memungkinkan adanya akses fisik ke media jaringan dan juga menyediakan sistem addressing *low-level* melalui penggunaan *mac-address*.”

4. Kabel Jaringan

Kabel merupakan media transmisi yang umum digunakan. Berikut beberapa jenis kabel jaringan yang umum digunakan:

- a. *Twisted Pair*
- b. Koaksial
- c. Fiber Optik

5. Modem

Modem singkatan dari modulator/demodulator yang merupakan sebuah piranti yang digunakan untuk mengkonversikan data digital menjadi sinyal analog (atau gelombang) untuk transmisi melalui jaringan analog, seperti telepon (PSTN).

6. Hub

Menurut (Wahana Komputer ,2005)”*Hub* adalah alat yang berfungsi sebagai tempat untuk

menerima data dan meneruskannya menuju tempat yang lain.“ Hub mengirimkan paket ke semua port yang ada.”

7. *Switch*

Menurut (Wahana Komputer ,2005)”*Switch* atau *switch hub* pada dasarnya adalah *hub* juga. Switch memiliki kemampuan mentransfer data hanya pada port yang dituju saja, berbeda dengan hub yang mem-broadcast data yang datang ke semua *port* yang dimiliki termasuk *port* tempat data tersebut berasal“.

8. *Router*

Menurut (Tim Wahana Komputer ,2009) ”Router adalah peranti jaringan yang bertugas untuk memecah atau memperluas jaringan dengan memforward paket data sepanjang jaringan menggunakan header dan tabel forwarding sehingga bisa menentukan rute terbaik untuk transportasi data“.

9. *Repeater*

Menurut (Tim Wahana Komputer ,2009) ”Repeater merupakan piranti elektronik yang bertugas menerima sinyal kemudian meneruskannya pada level yang lebih tinggi atau dengan daya yang lebih besar.“

Sistem Keamanan Jaringan

Berikut ini adalah teori pendukung yang berkaitan dengan keamanan jaringan yang peneliti dapat dari hasil penelitian pada jaringan perusahaan PT Pertamina *Marketing Operation Region III*.

1. Proxy

Menurut (Tim Wahana Komputer ,2005) “Proxy adalah perangkat atau suatu aplikasi yang berfungsi untuk menyaring permintaan pada suatu server”. Proxy berfungsi untuk meningkatkan kinerja dari

suatu jaringan dan berfungsi untuk menyaring akses internet yang diperbolehkan”.

2. *Wireless Captive Portal*

Menurut (Supriyono,2013) “*Captive Portal* adalah suatu teknik autentikasi dan pengamanan data yang lewat dari network internal ke network eksternal”.

3. *Port Security*

Port Security berfungsi untuk membatasi jumlah *MAC address* yang diizinkan terhubung dengan tiap port dan juga dapat membatasi *MAC address* mana saja yang diizinkan

4. Antivirus

Antivirus berfungsi untuk mencegah penyebaran virus yang datang dari *client* agar tidak menyebar ke *client* lain yang saling terhubung ke satu jaringan.

5. Radius

Menurut (Febyatmoko,2006) “RADIUS adalah singkatan dari Remote Authentication Dial-in User Service yang berfungsi untuk menyediakan mekanisme keamanan dan manajemen user pada jaringan computer”.

Metode Penelitian

Metode penelitian yang peneliti lakukan dalam penelitian ini peneliti melakukan riset di PT Pertamina kantor Marketing Operation Region III adalah:

Analisa Penelitian.

a. Analisa kebutuhan

Berisi tentang semua kebutuhan yang diperlukan dalam merancang otentikasi pengguna jaringan menggunakan sebuah radius server yang terintegritas dengan perangkat switch cisco.

b. Desain

Mendesain sistem yang dapat menyelesaikan masalah yang

dihadapi perusahaan yang diperoleh dari pemilihan alternatif sistem keamanan jaringan. Kegiatan dalam tahap ini antara lain, menggambar skema dan topologi jaringan.

c. Testing

Membangun rancangan otentikasi pengguna jaringan dengan menggunakan Windows Radius 2008 Server, switch cisco dan beberapa komputer.

d. Implementasi

Jaringan yang telah disimulasikan kemudian diuji untuk dilihat kinerjanya dan mengevaluasinya.

Pengumpulan Data

a. Metode Observasi

Observasi adalah mengamati langsung terhadap kegiatan yang terjadi, untuk mendapatkan data-data yang lengkap dan akurat. Pada metode observasi ini peneliti melakukan pengamatan langsung di PT Pertamina kantor *Marketing Operation Region III* yang beralamatkan di Jl. Kramat Raya No.59 Jakarta Pusat untuk mendapatkan data skema jaringan, topologi, dan sistem yang berjalan pada jaringan disana.

b. Metode Wawancara

Wawancara dilakukan dengan menanyakan langsung kepada Bapak Lucky Alpha Darmawan selaku Asisten Operasi dan Komunikasi divisi IT M & T Jakarta selama penelitian dari tanggal 13 November 2013 sampai dengan 29 November 2013 untuk memperoleh informasi yang lengkap dan akurat.

c. Metode Kepustakaan

Metode ini membantu peneliti dalam hal membuat laporan yang ditunjang dengan buku-

buku, jurnal dan referensi yang berhubungan dengan analisa dan implementasi Otentikasi pengguna jaringan menggunakan Windows Radius Server yang dimuat dalam penyusunan penelitian ini .

HASIL DAN PEMBAHASAN

Hasil analisa jaringan PT Pertamina *Marketing Operation Region III* permasalahan yang ada pada sistem yang berjalan yaitu :belum adanya mekanisme otentikasi bagi pengguna jaringan kabel, sebagai proses pengesahan identitas pengguna untuk mengakses jaringan.

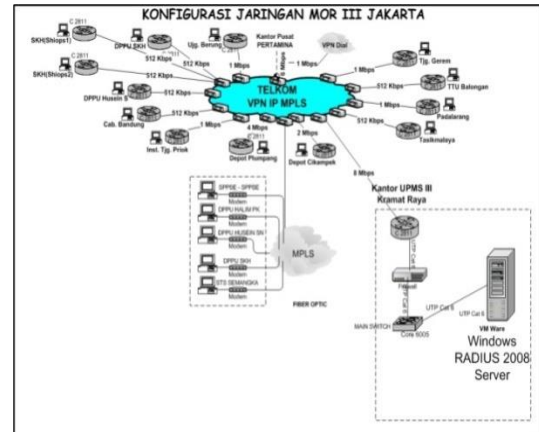
Untuk mengatasi permasalahan yang dihadapi oleh perusahaan, maka dibutuhkan solusi yang dapat membantu meningkatkan sistem keamanan jaringan yang dimiliki perusahaan. Penggunaan RADIUS Server untuk sistem otentikasi dan otorisasi bagi pengguna jaringan kabel menjadi alternatif peneliti untuk mengatasi masalah yang ada. Sistem yang diusulkan menggunakan Windows Radius Server 2008 yang diintegrasikan dengan perangkat switch cisco yang dimiliki oleh PT Pertamina *Marketing Operation Region III*.

Topologi Jaringan Usulan

Topologi jaringan yang diterapkan pada PT Pertamina *Marketing Operation Region (MOR) III* beserta kantor unit dan cabang yaitu menggunakan topologi star karena seluruh perangkat jaringan terpusat dengan switch, karena lebih memudahkan pada saat proses instalasi dan pengaturan perangkat jaringan. Untuk topologi WAN memiliki jaringan VPN IP dengan vendor PT TELKOM.

Peneliti mengusulkan untuk menggunakan topologi dan

infrastruktur jaringan yang sudah ada pada PT Pertamina *Marketing Operation Region III* hanya menambahkan fungsi dari RADIUS server yang telah ada untuk otentikasi pengguna jaringan kabel.



Gambar 1. Topologi Jaringan PT Pertamina MOR III

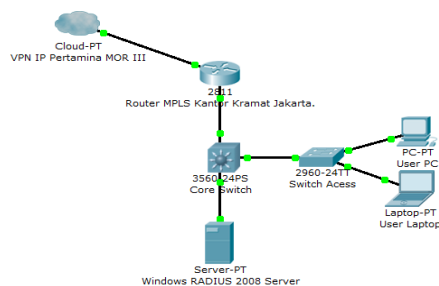
Skema Jaringan Usulan

Pada rancangan jaringan usulan, perlu dilakukan beberapa penambahan dan perubahan sistem pada jaringan PT Pertamina *Marketing Operation Region III*. Adanya penambahan yaitu pada fungsi dan konfigurasi RADIUS Server, dengan menambahkan protokol 802.1x untuk jaringan kabel. Penambahan konfigurasi juga dilakukan pada switch cisco yang dimiliki PT Pertamina *Marketing Operation Region III* agar dapat terintegrasi dengan Windows RADIUS 2008 server.

Pada penelitian ini peneliti melakukan simulasi menggunakan perangkat yang sudah ada pada PT Pertamina *Marketing Operation Region (MOR) III*. Menggunakan Windows RADIUS 2008 server, kemudian mensimulasikan dengan salah satu switch cisco yang ada, dan menggunakan satu unit perangkat komputer untuk tes hasil sistem yang sudah dibuat.

Untuk skala jaringan WAN PT Pertamina MOR III, maka administrator perlu menambahkan IP *Address switch* cisco lokasi mana saja yang akan didaftarkan pada Windows RADIUS 2008 server, dan juga menambahkan konfigurasi 802.1x pada masing-masing switch cisco.

Pengguna jaringan PT Pertamina MOR III umumnya menggunakan sistem operasi windows 7, untuk menjalankan sistem keamanan ini maka protokol 802.1x pada sistem operasi pengguna jaringan perlu diaktifkan. Secara default protokol 802.1x pada sistem operasi windows 7 tidak aktif, oleh karena itu administrator jaringan perlu mengaktifkan service Wired AutoConfig pada sistem operasi windows 7.



Gambar 2. Skema Jaringan Usulan

Keamanan Jaringan

Windows RADIUS 2008 Server yang dimiliki PT Pertamina MOR III dapat dioptimalisasikan fungsinya untuk keperluan otentikasi pengguna jaringan kabel, RADIUS server yang memiliki protokol 802.1x memiliki beberapa fungsi yang dapat menambah tingkah keamanan dari suatu jaringan.

Protokol 802.1x menyediakan layanan untuk *authentication*, *authorization*, dan *accounting* dalam sebuah sistem jaringan.

1. Otentikasi

Metode otentikasi yang digunakan akan berguna untuk mencocokkan identitas *username* dan *password* yang dimiliki pengguna jaringan dengan data yang ada di *database server*, *database server* yang digunakan oleh peneliti dalam penelitian ini menggunakan *database* yang ada pada *domain controller*.

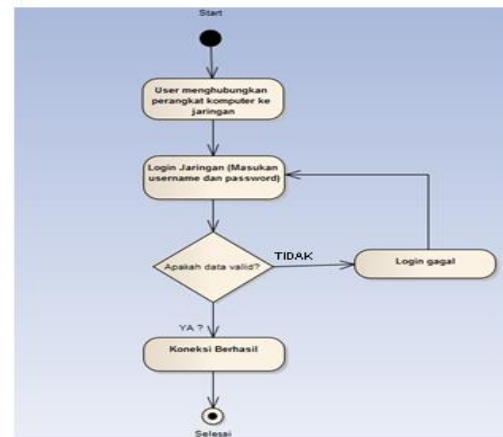
2. Otorisasi

Metode otorisasi berfungsi ketika data yang dimasukkan oleh pengguna jaringan adalah data yang valid, maka sistem akan mengizinkan pengguna jaringan untuk terkoneksi dengan jaringan.

3. Akunting

Setelah pengguna jaringan melalui tahap otentikasi dan otorisasi maka proses pencatatan semua aktifitas pengguna jaringan akan dilakukan.

Rancangan Aplikasi



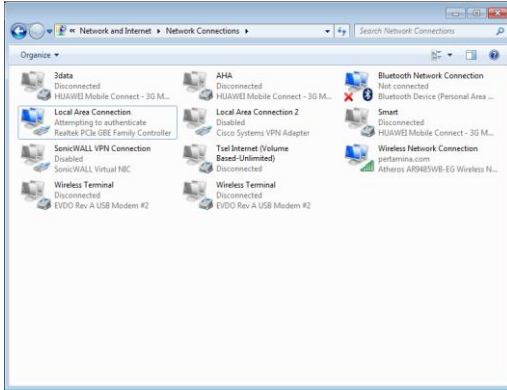
Gambar 3. Rancangan Aplikasi

Pengujian Jaringan

A. Pengujian Jaringan Awal

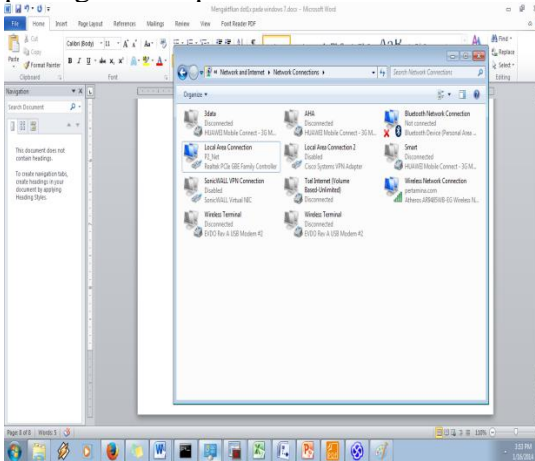
Sebelum adanya perubahan pada jaringan PT Pertamina MOR III, pengguna jaringan kabel dapat terkoneksi dengan jaringan perusahaan tanpa adanya mekanisme keamanan otentikasi, setelah user menghubungkan perangkat

komputernya dengan kabel jaringan yang disediakan maka user akan terhubung dan terkoneksi dengan jaringan.



Gambar 4 Koneksi jaringan awal.

Pada jaringan awal yang berjalan, pengguna jaringan tidak diberlakukan sistem otentikasi jaringan saat akan terhubung ke jaringan, sehingga bisa langsung terkoneksi saat kabel jaringan perusahaan dihubungkan ke perangkat komputer.



Gambar 5 Koneksi jaringan awal bagian dua.

B. Pengujian Jaringan Akhir

1) Langkah pertama dalam pengujian jaringan adalah mengkonfigurasi Windows RADIUS 2008 server, berikut langkah-langkahnya:

A. Membuat Radius Client

1. Klik Start, Pilih

Administrative Tools, kemudian pilih Network Policy Server.

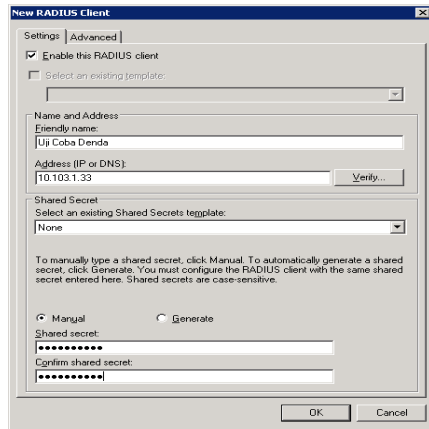
2. Pada menu RADIUS Client and Server, klik kanan RADIUS Client, pilih New.
3. Tampil kotak dialog New RADIUS Client, pada tab setting, isi kolom Friendly name dengan nama RADIUS yang diinginkan, pada kolom Address (IP or DNS) isi dengan alamat ip radius klien, pilih manual shared secret dan ketik password shared secret yang diinginkan. Kata kunci shared secret harus diisi sama dengan RADIUS klien. Klik OK.

B. Mengkonfigurasi dot.1x untuk pengguna jaringan kabel.

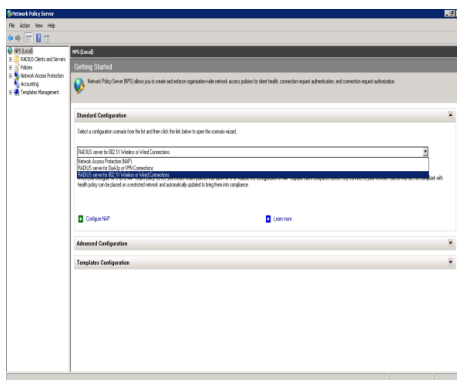
1. Klik menu NPS (*local*), pilih list konfigurasi *RADIUS server for 802.1x Wireless or Wired Connection*.
2. Tampil kotak dialog *Configure 802.1x*, kemudian pilih tipe koneksi *802.1x Secure Wired (Ethernet) Connections*.
3. Klik *RADIUS Client* yang telah dibuat atau yang diinginkan, kemudian klik *Next*.
4. Pilih metode otentikasi *Microsoft Protected EAP (PEAP)* pada daftar list yang ada, kemudian klik *Next*.
5. Tampil kotak dialog *specify user group*, pilih *group user* yang akan didaftarkan untuk otentikasi 802.1x. Disini saya mencoba mendaftarkan group email Groups UPms III. Kemudian klik Ok dan klik *Next*.
6. Tampil kotak dialog *Traffic*

Controls, langsung saja klik *Next*.

7. Setelah komplit klik *Finish*.



Gambar 6. Membuat Radius Client



Gambar 7. Membuat dot.1x pengguna jaringan kabel.

2) Langkah kedua mengkonfigurasi 802.1x pada cisco switch yang akan dijadikan *radius client*.

1. `aaa new-model` (Untuk mengaktifkan AAA).
2. `aaa authentication login default none` (Menggunakan AAA hanya untuk 802.1x, secara optimal)
3. `aaa authentication dot1x default group radius`
`aaa authorization network default group radius` (Memberikan hak akses

VLAN secara dinamik pada network group radius)

4. `radius-server host 192.168.21.240` (Mengkonfigurasi IP untuk RADIUS server).
5. `radius-server key rad123` (Key untuk RADIUS server).
6. `dot1x system-auth-control` (Untuk mengaktifkan 802.1x).
7. `interface Fa0/1`
`switchport mode access`
`dot1x port-control auto` (Mengaktifkan 802.1x pada interface switch)

3) Langkah ketiga adalah mendaftarkan RADIUS Windows 2008 Server ke aktif direktori:

- a) Masuk ke dalam NPS Server, dengan klik Start - Administrative Tools - Network Policy Server.
- b) Klik kanan NPS Server, Pilih Register in Active Directory.
- c) Tampil kotak dialog Register Network Policy Server in Active Directory, kemudian klik OK.

4) Langkah berikutnya yaitu dengan mengaktifkan protokol 802.1x pada sistem operasi perangkat pengguna jaringan, yang digunakan adalah sistem operasi windows 7.

- a. Secara default services protokol 802.1x untuk konfigurasi adapter LAN pada windows 7 tidak diaktifkan, cara mengaktifkannya dengan masuk ke menu services windows dengan masuk ke menu run (tekan tombol windows + r), ketika services.msc kemudian enter.
- b. Pada menu services,

cari services Wired AutoConfig kemudian klik kanan pilih start.

c. Selanjutnya klik *Start*, pilih *Control Panel*, klik *Network and Sharing Center*, klik *Change adapter settings*, klik kanan *Local Area Connection* pilih *properties*.

d. Pada menu *Local Area Connection*, pilih tab *Authentication*, berikan tanda ceklist pada *Enable IEEE 802.1x authentication*, pilih metode otentikasi *Microsoft Protected EAP (PEAP)*.

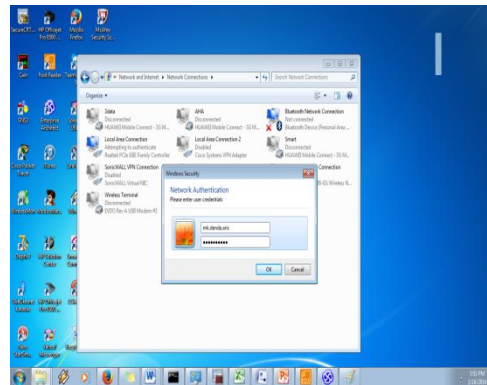
e. Selanjutnya klik *button Additional Settings*, tampil menu *additional settings*, beri tanda *ceklistspecify authentication mode* kemudian pilih *User Authentication*, klik *OK*.

f. Klik *button settings*, tampil kotak dialog *Protected EAP Properties* hapus tanda *ceklist validate server certificate*, pilih metode otentikasi *Secure password (EAP-MSCHAP v2)*.

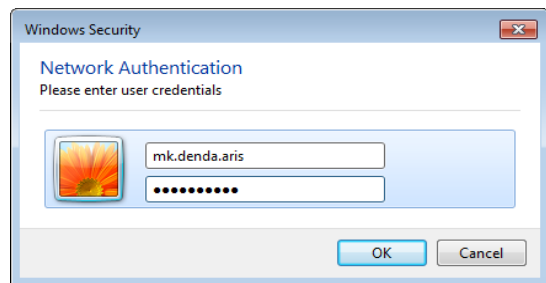
g. Klik *button Configure*, hapus tanda *ceklist Automatically use my windows logon name and password (and domain if any)*. Klik *Ok* semua kotak dialog.

5) Langkah terakhir pengujian koneksi jaringan, ketika kabel di *plugin* ke perangkat komputer dan tampil *notification*, klik *notification* tersebut maka akan tampil menu *login* untuk otentikasi, masukan *username* dan *password*.

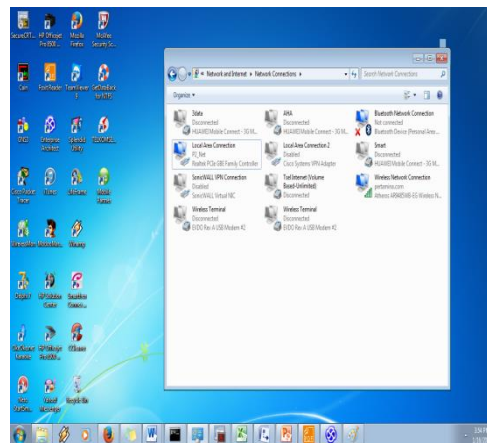
Gambar 8. Notifikasi untuk otentikasi



Gambar 9. Tampilan otentikasi jaringan



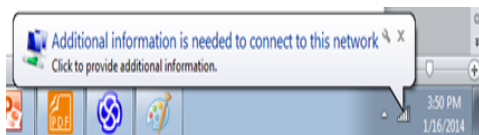
Gambar 10. Kotak dialog login



Gambar 11. Koneksi berhasil setelah login.

KESIMPULAN

Setelah peneliti mempelajari dan menganalisa sistem jaringan yang berjalan pada PT Pertamina Marketing Operation Region III maka peneliti dapat mengambil kesimpulan bahwa:



- a. Penggunaan RADIUS Windows 2008 Server untuk membuat sistem otentikasi pengguna jaringan berhasil dengan baik, sehingga mekanisme keamanan untuk koneksi pengguna jaringan kabel kini telah tersedia.
- b. Adanya sistem otentikasi dan otorisasi untuk pengguna jaringan kabel, membuat akses pengguna jaringan menjadi lebih aman, sehingga tidak sembarang orang dapat menggunakan jaringan kabel untuk akses ke sistem jaringan perusahaan.

DAFTAR PUSTAKA

- Febyatmoko, Gesit Singgih, Taufik Hidayat dan Mukhammad Andri S. 2006. Sistem Otentikasi, Otorisasi dan Pelaporan Koneksi User pada Jaringan Wireless Menggunakan Chillispot dan Server RADIUS. ISSN: 0854-4743. Yogyakarta. Media Informatika, Vol 4, No.1, Juni 2006: 67-69. Diambil dari: <http://journal.uii.ac.id/index.php/media-informatika/article/viewFile/122/83>. (26 September 2013).
- Sofana, Iwan. 2012. Cisco CCNP dan Jaringan Komputer. Bandung: Informatika Bandung.
- Sujarwo, Ari. 2010. Implementasi Network Storage dan Internet Gateway Menggunakan Autentikasi OPENLDAP. ISSN: 1907-5022. Yogyakarta. Diambil dari: <http://journal.uii.ac.id/index.php/Snati/article/viewFile/1968/1742>. (31 Oktober 2013).
- Sukamaaji, Anjik dan Rianto. 2008. Jaringan Komputer Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan. Yogyakarta: Andi.
- Supriyono, Agus dan Imam Riadi. 2013. Rancang Bangun Sistem Hotspot Menggunakan Captive Portal. ISSN: 2338-5197. Yogyakarta. Jurnal Sarjana Teknik Informatika. Vol 1, No.1, Juni 2013. Diambil dari: <http://journal.uad.ac.id/index.php/JSTIF/article/download/1743/1048>. (20 Januari 2014).
- Tim Wahana Komputer. 2005. Seri Buku Pintar Menjadi Administrator Jaringan Komputer. Yogyakarta: Andi.
- Tim Wahana Komputer. 2013. Konsep dan Implementasi Jaringan menggunakan Windows Server 2012. Yogyakarta: Andi.
- Yuliansyah, Herman. 2011. Optimalisasi RADIUS Server sebagai Sistem Otentikasi dan Otorisasi untuk Proses Login Multi Aplikasi Web Berbasis PHP. ISSN: 1979-2328. Yogyakarta. Diambil dari: <http://repository.upnyk.ac.id/634/1/C-4.pdf>. (31 Oktober 2013)