IMPLEMENTASI *REMOTE AUTHENTICATION DIAL – IN USER SERVICE* PADA JARINGAN NIRKABEL DI UNIVERSITAS KRISTEN MARANATHA

Semuil Tjiharjadi
Jurusan Sistem Komputer
Universitas Kristen Maranatha
semuiltj@gmail.com

Adrian M. Sutantio
Jurusan Teknik Elektro
Universitas Kristen Maranatha

Abstrak -Saat ini, penggunaan teknologi nirkabel mulai banyak digunakan oleh banyak orang di Indonesia karena banyak sekali kemudahan yang tidak dimiliki oleh jaringan kabel biasa, misalnya mobilitas. Tetapi teknologi wireless jarang diimplementasikan dalam skala yang besar, karena sulit mengatur autentikasi, autorasi, akunting, auditing (AAAA) untuk user. Pada makalah ini telah dibuat perancangan server – server yang dapat digunakan untuk menangani permasalahan autentikasi, otorasi, akunting, auditing (AAAA), yang disimulasikan di dalam suatu teslab. Digunakan 1 access point sebagai perangkat untuk mengubah sinyal analog kabel menjadi sinyal radio, 1 komputer dengan sistem operasi Windows XP sebagai klien, 4 komputer dengan sistem operasi Windows 2003 server, masing – masing berfungsi sebagai Web Server, Active Directory, Server IAS, dan Server FirstSpot. Pada Active Directory dimasukkan nama – nama user yang akan melakukan simulasi, saat klien ingin terhubung dengan internet (pada testlab, internet akan diwakili satu web server yang sudah diinstall Microsoft IIS), klien tersebut akan terhadang captive portal (Server FirstSpot) yang akan meminta autentikasi klien. Sesudah klien memasukkan user name dan password, FirstSpot mengirim data tersebut ke Microsoft IAS. Bila data yang dikirimkan sesuai pada data yang ada di dalam Active Directory maka user tersebut diberi otorasi dan dapat terhubung dengan internet (Microsoft IIS). Selama user terhubung ke internet, Microsoft IAS melakukan auditing dan akunting yang kemudian hasilnya akan dilaporkan ke server FirstSpot.

Kata Kunci: wireless, hotspot, remote, authentication

I. PENDAHULUAN

Teknologi Internet nirkabel (hotspot) belakangan ini sudah sangat menjamur di Indonesia. Banyak dari universitas – universitas terkenal sudah mulai memasang hotspot di lingkungan kampus mereka. Teknologi hotspot ini menjadi sangat populer karena dapat memudahkan user untuk mendapat koneksi internet di mana saja dalam cakupan area hotspot tanpa harus dipusingkan oleh kabel – kabel yang bertebaran. Kelebihan lainnya adalah prosedur pemasangannya yang sangat mudah. Jaringan lama yang sudah dipasang juga tidak perlu dibongkar tetapi dapat digabungkan dengan perangkat hotspot baru, sehingga pemasangan teknologi ini tidak akan merusak infrastruktur yang telah ada.

Banyaknya jumlah serta karakter pengguna, lalu luasnya cakupan wilayah wireless yang akan diimplementasikan di Universitas Kristen Maranatha menjadikan penanganan menjadi rumit dan memerlukan implementasi dengan teknologi yang sesuai. Untuk itu dipilihlah teknologi *RADIUS SERVER* karena keunggulannya untuk memenuhi semua kriteria yang diperlukan dalam implementasi di UK. Maranatha. Penerapan *RADIUS SERVER* ini menggunakan microsoft IAS yang mampu mengontrol server dan proxy *RADIUS* (*Remote Authentication Dial – in User Service*). *RADIUS* sendiri adalah standar dari teknologi networking untuk melakukan Authentication, Authorization, Accounting dan Auditing (AAAA) terhadap user. *RADIUS* mempermudah administrator jaringan besar untuk mendata user – user yang tergabung di dalam jaringan.

Selama ini terdapat kelebihan teknologi *Wireles,* yang dikenal dengan istilah *CAMP*, yaitu: *Convenience, Affordability, Mobility, Productivity*. Melalui daerah cakupan yang fleksibel serta dapat menjalankan koneksi jaringan tanpa harus dibatasi oleh kabel, maka jaringan nirkabel memiliki kesempatan lebih baik untuk menghindari bertahan dari gangguan luar. Misalnya, pada jaringan kabel, rawan akan gangguan tikus, kabel terbelit, atau kerusakan infrastruktur lainnya.

RADIUS sendiri merupakan singkatan dari *Remote Authentication Dial-In User Service* adalah standar umum yang dikembangkan secara luas untuk menyediakan *authentication, authorization, auditing dan accounting* yang terpusat untuk *dial-up*, *virtual private network*, dan biasanya digunakan untuk *wireless network access*. *Authentication* adalah proses verifikasi data dari pengguna yang berusaha untuk terkoneksi dengan jaringan. *Authorization* adalah proses untuk menentukan apakah user memiliki ijin terhubung dengan jaringan dan kondisi apa yang telah disetujui. *Accounting* adalah pilihan untuk tetap menyimpan data sukses atau tidaknya permintaan koneksi.

Awalnya, teknologi *RADIUS* ini dikembangkan untuk *dial-up remote access*, sampai *saat* ini, *RADIUS* telah mendukung perangkat jaringan lain seperti *server Virtual Private Network* (VPN), *wireless access point*s, *authenticating ethernet switches,* akses *Digital Subscriber Line* (DSL), dan banyak tipe akses jaringan yang lain. Standar *RADIUS* dijabarkan pada RFC 2856 "Remote Authentication Dial-in User Service (*RADIUS*)," (IETF Draft Standard) dan RFC 2866 "*RADIUS* Accounting" (Informational).

II. METODOLOGI PENELITIAN

Makalah ini sebenarnya lebih memaparkan implementasi penggunaan teknologi *RADIUS SERVER* dalam memenuhi masalah serta kebutuhan teknologi wireless yang terjadi di UK. Maranatha. Pengujian serta pengumpulan data dilakukan melalui uji coba (*trial and error*) dan selanjutnya dilakukan pengamatan melalui data log yang ada di server mengenai keberhasilan dari penerapan serta perancangan teknologi *RADIUS SERVER* ini.

III. HASIL DAN PEMBAHASAN

Sebuah klien *RADIUS* (biasanya berupa *server* akses seperti *dial-up server*, VPN *server* atau *wireless access point*) mengirim identitas user dan informasi parameter koneksi dalam bentuk pesan *RADIUS* kepada sebuah *RADIUS SERVER*. *RADIUS SERVER* akan melakukan autentikasi dan autorasi permintaan klien *RADIUS*, dan mengirimkan kembali respon pesan *RADIUS*. Klien *RADIUS* juga mengirimkan pesan akunting *RADIUS* kepada *RADIUS SERVER*.

Pada umumnya, standar *RADIUS* mendukung penggunaan *proxy RADIUS*. *Proxy RADIUS* adalah sebuah komputer yang melanjutkan pesan *RADIUS* antara klien *RADIUS*, *server RADIUS* dan *RADIUS proxy* lainnya. Pesan *RADIUS* tidak pernah dikirimkan diantara klien akses dan *server* akses.

Pesan *RADIUS* dikirimkan sebagai pesan User Datagram Protocol (UDP). Port UDP yaitu 1812 digunakan untuk pesan autentikasi *RADIUS* dan *port* UDP 1813 digunakan untuk pesan akunting *RADIUS*. Beberapa *server* akses mungkin juga menggunakan port UDP 1645 untuk pesan autentikasi *RADIUS*. [1]

Sebuah pesan *RADIUS* mengandung header dan atribut *RADIUS*. Setiap atribut *RADIUS* mendefinisikan sepotong informasi tentang *permintaan* koneksi. Sebagai contoh, ada atribut *RADIUS* untuk nama user, password, tipe koneksi yang dikehendaki user, dan alamat IP dari *server* akses.

Atribut *RADIUS* digunakan untuk menyampaikan informasi antara klien *RADIUS*, *proxy – proxy RADIUS*, dan *server RADIUS*. Sebagai contoh, daftar dari atribut dalam pesan permintaan akses termasuk informasi mengenai data user dan parameter dari permintaan koneksi, sedangkan daftar dari atribut dalam pesan persetujuan akses termasuk informasi tentang tipe koneksi yang dibuat, pembatasan koneksi dan atribut khusus yang dibutuhkan vendor tertentu (*vendor-specific attributes (VSAs).*

Atribut *RADIUS* dijabarkan pada RFCs 2865, 2866, 2867, 2868, 2869, dan 3162. RFC *dan* rancangan Internet untuk VSA mendefinisikan atribut *RADIUS* yang umum.

Untuk autentikasi Point-to-Point Protocol (PPP) seperti Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (*CHAP*), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), dan MS-CHAP versi 2 (MS-CHAP v2), hasil dari negosiasi autentikasi akan diteruskan kepada *server RADIUS* untuk verifikasi.

Untuk menyediakan keamanan untuk pesan *RADIUS*, klien *RADIUS* dan *server RADIUS* dikonfigurasi dengan sebuah common shared secret. *Shared* secret digunakan untuk mengamankan jalur *RADIUS* dan biasanya dikonfigurasi sebagai text string pada keduanya, klien *RADIUS* dan *server*.

Sebagai bagian dari implementasikan *RADIUS* maka digunakan Microsoft IAS (*Internet Authentication Service*) yang merupakan implementasi Microsoft dalam bidang *server* dan

proxy Remote Authentication Dial-in User Service (*RADIUS*). Sebagai *server RADIUS*, IAS melakukan tugas sebagai pusat koneksi autentikasi, otorasi, akunting, dan akunting (AAAA) untuk banyak tipe jaringan termasuk jaringan nirkabel, authenticating switch, remote *access dial-up* dan virtual private network (VPN) connections. Sebagai *proxy RADIUS*, IAS menyediakan routing pesan *RADIUS* diantara klien *RADIUS* (*server* akses), *proxy RADIUS*, dan *server RADIUS* yang menjalankan AAAA untuk permintaan koneksi. Ketika digunakan sebagai *proxy RADIUS*, IAS adalah pusat dari poin switching atau routing melewati jalur di mana akses *RADIUS* dan pesan akunting berjalan. Dengan IAS, AAAA dapat dengan mudah di atur untuk berbagai jenis komunitas, termasuk bisnis kecil, organisasi sedang, organisasi berskala besar, dan Internet Service Providers (ISPs). IAS memberikan kemampuan untuk mengamankan dan mengatur akses jaringan lewat berbagai skenario jaringan seperti berikut : [2]

- Karyawan terkoneksi dengan jaringan perusahaan lewat dial – up, VPN, nirkabel, dan koneksi berkabel, menggunakan berbagai peralatan seperti personal computer, personal digitall assistant, dan komputer member di luar domain, seperti komputer milik karyawan
- Karyawan terhubung dengan jaringan lain, termasuk internet dan patner jaringan bisnis dan internet
- Patner bisnis yang ingin tehubung ke dalam jaringan internal perusahaan

IAS memungkinkan penggunaan berbagai macam koneksi nirkabel, switch, remote *access*, atau perangkat VPN. IAS juga mendukung penggunaan basis sertifikat atau basis password untuk protokol autentikasinya dan menyediakan kemampuan untuk menghubungkan kebutuhan databasenya dengan *server* Structured Query Language (SQL).

Ketika *server* IAS adalah anggota dari domain Active Directory, IAS menggunakan layananan direktori Microsoft Active Directory sebagai database user dan bagian dari solusi sign – on. Dengan sebuah single sign-on, user hanya perlu memasukkan satu kali data pada saat proses autentikasi dan otorasi. Data ini kemudian digunakan untuk masuk ke dalam domain active directory dan digunakan juga untuk akses kontrol ke dalam jaringan.

Ketika peraturan remote IAS dikonfigurasi menggunakan Protected Extensible Authentication Protocol (PEAP) dan tipe PEAP untuk metode autentikasinya adalah untuk hubungan nirkabel, PEAP dengan cepat memperbolehkan pengguna untuk masuk ke dalam jaringan tanpa harus memasukkan kembali data setiap perangkat nirkabel bergabung di dalam *access point* satu dengan yang lainnya. [3]

Pada window *server* 2003, edisi standar, IAS dapat mengkonfigurasi maksimum 50 klien *RADIUS* dan maksimum 2 grup remote *RADIUS SERVER*. Klien *RADIUS* tidak dapat didefinisikan menggunakan domain name atau alamat IP. Jika domain name dari klien *RADIUS* mendapat banyak permintaan IP, IAS menggunakan IP pertama yang dikeluarkan oleh *server* DNS.

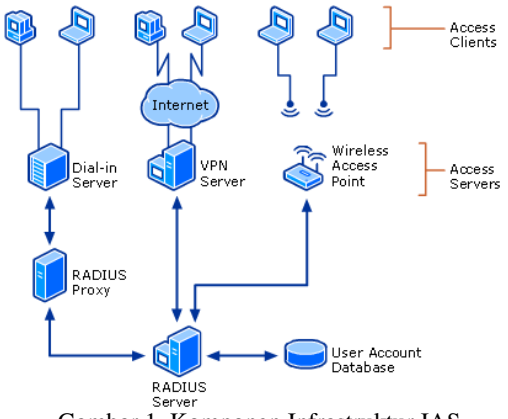
Pada windows *server* 2003, edisi Enterprise dan windows *server* 2003, edisi datacentre, dapat mengatur jumlah klien dan *RADIUS SERVER* sampai tidak berhingga, sebagai tambahan, OS ini dapat juga mengatur klien *RADIUS* dengan menjabarkan range alamat IP.

Komponen dari IAS sebagai *server RADIUS* terdiri dari 5 bagian yaitu *access clients*, *access server*s (klien *RADIUS*), IAS *server*s (*server RADIUS*), IAS *proxies* (*proxy RADIUS*), and user account database.

Access client adalah perangkat yang memerlukan beberapa akses level ke jaringan yang lebih besar. Contoh dari *access* client adalah klien dial – up atau klien VPN, klien *wireless* atau klien LAN yang terhubung lewat switch authenticating.

Access Servers Yang Berfungsi Sebagai *RADIUS Clients*

Access server adalah peralatan yang menyediakan akses ke jaringan yang lebih luas. Sebuah *access server* menggunakan infrastruktur *RADIUS* juga merupakan klien *RADIUS*, mengirimkan permintaan koneksi dan pesan akunting kepada *server RADIUS*.

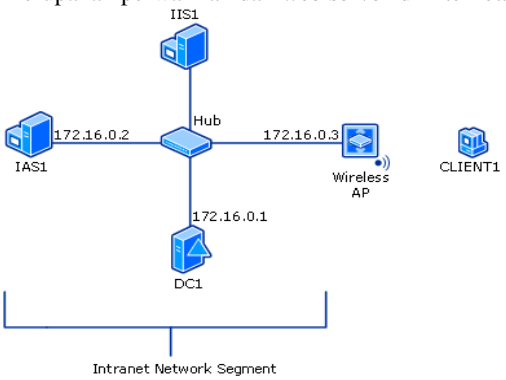


Gambar 1. Komponen Infrastruktur IAS

Jika accounts user untuk autentikasi berada pada database yang berbeda tipe IAS dapat dikonfigurasi sebagai *proxy RADIUS* untuk meneruskan permintaan autentikasi ke *server RADIUS* yang memang memiliki akses ke user

accountnya. Databases yang berbeda untuk Active Directory termasuk untrusted forests, untrusted domains, atau one-way trusted domains. [6]

Untuk testlab ini, tidak ada koneksi internet untuk mempermudah perancangan, sebagai gantinya, digunakan Microsoft IIS yang merupakan perwakilan dari *web server* di internet.



Gambar 2. Perancangan Awal Testlab

Operating sistem Window *Server* 2003 dengan SP1 pada tiap *server* di dalam Lab dan Windows *Firewall* (terintegrasi di dalam OS, dalam keadaan default akan nonaktif). Setelah *server* IAS dan IIS dikonfigurasi, Window *Firewall* dapat dinyalakan kembali dan akan dilakukan konfigurasi untuk pengecualian *(exception)* yang memperbolehkan komunikasi antar komputer dalam jaringan. Pada Domain Controller, Windows *Firewall* harus selalu dalam keadaan mati. Pada setiap komputer klien, Windows *Firewall* menyala secara otomatis ketika windows XP diinstal (OS yang dibutuhkan untuk klien adalah Windows XP Professional dengan SP2). Windows *Firewall* akan dibiarkan menyala untuk setiap komputer klien.

Sebagai tambahan, harus dipastikan juga terdapat *Wireless Access Point* yang menyediakan koneksi ke jaringan intranet kabel. *Firewall* untuk *Wireless Access point* biasanya dikontrol oleh software bawaan *Wireless Access point* tersebut. Untuk simulasi pada test lab, *firewall* AP akan dimatikan untuk menjaga hubungan yang lancar dengan software Windows. [4]

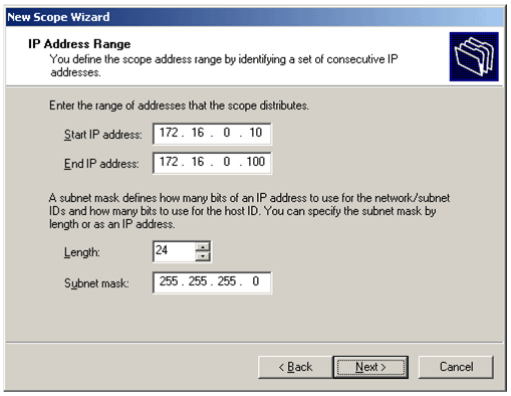
Test lab *wireless* ini mewakili bagian jaringan dalam intranet perusahaan. Semua Computer dalam intranet perusahaan termasuk *Wireless Access point* dikoneksikan menggunakan sebuah hub atau switch. Alamat *private* 172.16.0.0/24 digunakan pada bagian jaringan intranet. IIS1 dan CLIENT1 mendapat alamat IP address menggunakan DHCP. Dalam testlab, rata – rata komputer yang akan digunakan sudah memiliki spesifikasi pentium 4 di atas 1 GHZ, memory DDR2 256 MB, harddisk 40 GB, dengan NIC (Network Interface Card) 10/100.

DC1 adalah sebuah komputer dengan OS Windows *Server* 2003 dengan SP1, Enterprise *Edition.* Untuk alamat IP-nya, sebelum diinstall domain controller, harus disetting menjadi 172.16.0.1 dan subnet mask 255.255.255.0. Di dalam DC1, akan dikonfigurasi protokol sebagai berikut :

Domain controller adalah komputer / *server* pada jaringan windows yang bertanggung jawab untuk mengatur user yang ingin mendapat hak akses dalam jaringan. Di dalam domain controller sendiri terdapat active directory yang menyimpan semua informasi account, user yang telah diautentikasi, dan menerapkan kebijakan keamanan pada jaringan. Domain yang akan dibuat dalam testlab diberi nama example.com. Pembuatan DC ini sendiri memerlukan CD Windows karena instalasi standar Windows 2003 server tidak mencakup software Active Directory.

Sebuah DNS *server* untuk domain DNS example.com. DNS (Domain Name System) berfungsi untuk menterjemahkan nama komputer ke alamat IP pada jaringan testlab, misalnya, nama domain example.com akan diterjemahkan menjadi 172.16.0.1. DNS biasanya disetting sekaligus pada saat DHCP diinstall. Pada testlab scope (range) yang akan digunakan untuk DHCP adalah IP 172.16.0.10 sampai 172.16.0.100, dan peralatan yang akan mendapat IP dari DHCP adalah IIS1 dan CLIENT1.

IAS1 adalah sebuah komputer dengan OS Windows *Server* 2003 SP1, Standard Edition, yang menyediakan *RADIUS* authentication and authorization untuk AP *wireless*. Untuk koneksi intranet lokal, harus diatur terlebih dahulu protocol TCP/IP dengan alamat IP 172.16.0.2, subnet mask 255.255.255.0, dan alamat IP DNS *server* 172.16.0.1, karena IAS menggunakan IP statis pada jaringan.



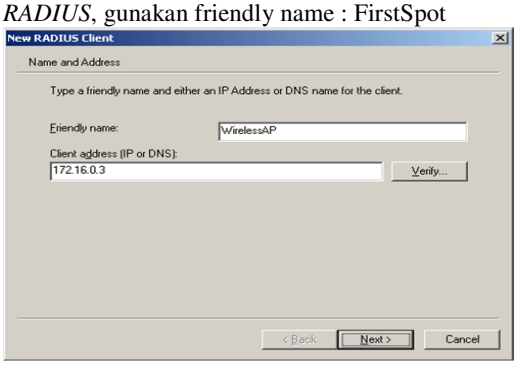
Gambar 3. Tampilan New Scope Wizard

Install Microsoft IAS lewat Add or Remove Program dari control panel. IAS juga dapat dikonfigurasi ketika sedang menginstall Windows 2003 *server*.

Perlu diperhatikan, ketika akan menentukan shared secret untuk Microsoft IAS karena shared secret ini akan terus digunakan agar peralatan lain atau software lain dapat mengakses data *RADIUS*.

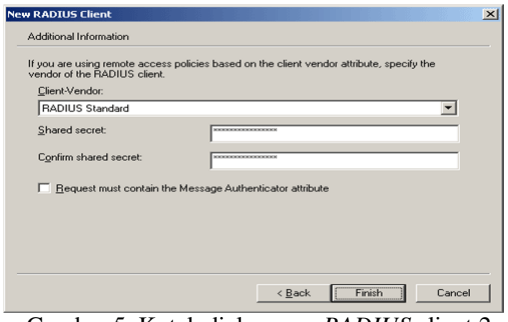
Setelah selesai menginstall IAS, dalam folder **Administrative Tools**, buka snap – in Internet Authentication Service. Klik kanan **Internet Authentication Service**, dan kemudian klik **Register *Server* in Active Directory**. Ketika dialog boks **Register Internet Authentication *Server* in Active Directory** muncul, klik **OK.** Register ke Active Directory bertujuan agar *server* IAS dikenali dan mengakses data dalam domain.

Wireless AP dimasukkan ke dalam klien *RADIUS* agar dapat dikonfigurasi ketika user meminta autentikasi ke *server* utama (active directory). Bila perancangan telah diubah (gambar III.6) tanpa *Access Point* yang mendukung *RADIUS*, gunakan friendly name : FirstSpot



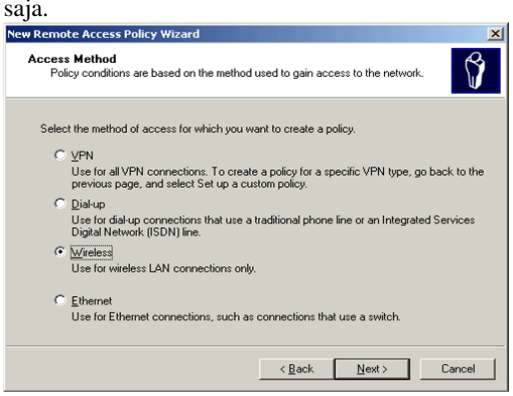
Gambar 4. Kotak Dialog New *RADIUS* Client 1

Ketika diminta untuk memasukkan shared secret, masukkan shared secret yang sama dengan shared secret ketika menginstall Microsoft IAS.



Gambar 5. Kotak dialog new *RADIUS* client 2

Langkah terakhir yang harus dikonfigurasi adalah Remote Access Policy. Remote Access Policy adalah kebijakan yang dibuat untuk semua klien yang melakukan koneksi secara remote (tidak langsung terhubung dengan Active Directory). Untuk teslab ini, Remote Access Policy digunakan untuk mengkonfigurasi klien yang terhubung ke Active Directory menggunakan koneksi *wireless* saja.



Gambar 6. Pengaturan Policy Remote Access

Ketika menginstall Windows 2003, Windows *Firewall* non aktif secara default, untuk keamanan, Windows *Firewall* sebaiknya dinyalakan tetapi dengan memasukkan pot 1812 dan 1813 UDP sebagai pengecualian agar Microsoft IAS dapat bekerja dengan lancar tanpa terhalangi oleh *Firewall*.

Pengaturan *policy* pada IAS yang menggunakan skenario 2 (gambar 7) agak berbeda dengan pengaturan skenario 1, karena pada skenario 2 akan digunakan custom policy, bukan menggunakan wizard. Cara mengatur *policy* skenario 2 akan dijelaskan pada lampiran C.

IIS1 adalah komputer yang berjalan pada komputer yang memiliki OS Windows *Server* 2003 SP1, standard edition, dan Internet Information Services (IIS). IIS menyediakan pelayanan Web dan File *Server* untuk klien intranet. Dalam testlab, *server* IIS disimulasikan seolah – olah merupakan web *server* yang ada di jaringan internet dunia karena pada testlab ini tidak ada jaringan internet real.

Wireless AP biasanya dapat diatur dari komputer mana saja di dalam jaringan. Ketik IP address dari AP, dan lakukan setting : Nama jaringan (SSID) yaitu **WIR_TST_LAB**.

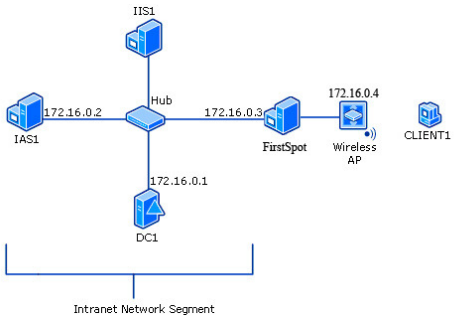
Untuk alamat IP Interface Ethernet, gunakan IP address 172.16.0.3 dengan subnet mask 255.255.255.0.

Untuk security, gunakan autentikasi IEEE 802.1X dengan **WEP**.

Untuk setting *RADIUS SERVER* utama : alamat IP **172.16.0.2**, Port UDP **1812**, dan shared secret, yang harus sama dengan shared secret sebelumnya yang dimasukkan saat mengatur IAS *server*.

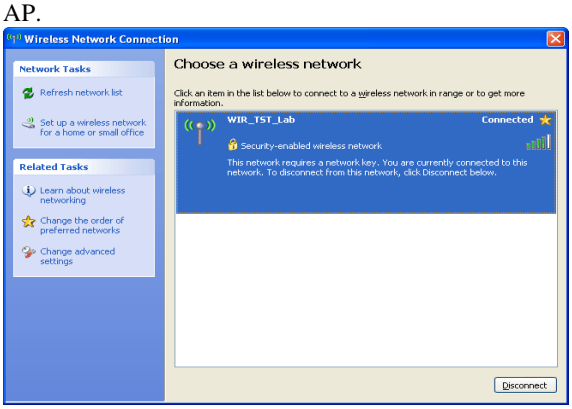
Tetapi karena sulit untuk mencari akses point yang mendukung *RADIUS*, maka dibuat alternatif lain yaitu dengan menambahkan sebuah server yang memiliki fungsi utama sebagai sebuah

router yang memiliki kemampuan untuk mendukung *RADIUS* diantara jaringan intranet dan *wireless access point*. Server yang akan digunakan pada teslab ini adalah server dengan OS Microsoft 2003 standard edition yang telah terintegrasi dengan software FirstSpot, sehingga perancangan awal berubah menjadi seperti gambar 7.



Gambar 7. Perancangan Akhir Menggunakan Server Firstspot

Client1 adalah sebuah komputer yang berjalan pada Windows XP Professional dengan SP2 yang berlaku sebagai klien *wireless* dan mematuhi akses ke jaringan intranet lewat *wireless* AP.



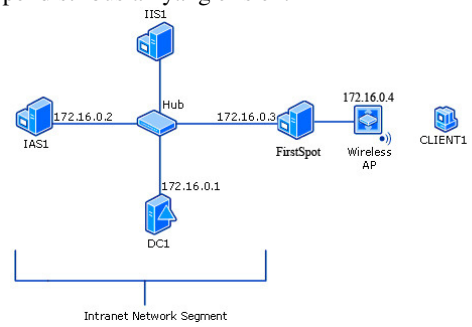
Gambar 10.Kotak Dialog Wireless Connection pada Windows XP

Setelah authentication berjalan dengan sukses, cek pengaturan TCP/IP untuk wireless adapter lewat pengaturan Network Connections. Seharusnya sudah didapat IP diantara alamat 172.16.0.10-172.16.0.100 dari scope DHCP.
Untuk mencoba hubungan ke Web *server* antara CLIENT1 dan IIS1 lewat hubungan *wireless*, jalankan Internet Explorer pada CLIENT1.
Jika diminta oleh Internet Connection Wizard, atur IE untuk koneksi LAN. Pada Address, ketik http://IIS1/iisstart.htm. Seharusnya halaman web Login FirstSpot akan tampil.

FirstSpot Adalah sebuah server dengan OS Windows Server 2003, yang telah diinstall software FirstSpot dari Patronsoft. Untuk percobaan di testlab, setting standar FirstSpot tidak diubah sama sekali.
Ketika melakukan login (klik start, program files, FirstSpot, Configuration Manager) password standar adalah :
User name : firstspot Password : password
Setelah berhasil login, ubah authetication mode (Categories, Authentication Server) menjadi *RADIUS*, dengan *RADIUS SERVER* IP 172.16.0.2 dan *RADIUS* shared secret sesuai dengan shared secred Microsoft IAS.

Firstspot sendiri adalah sebuah software yang mengatur manajemen pembuatan hotspot terutama billing kepada user. Software ini dipilih karena berbasis windows murni dan mendukung penuh teknologi *RADIUS*. Dengan berbasis pada teknologi captive portal, software ini mampu mensentralisasi segala pengaturan hotspot dengan mudah lewat web browser.

Berdasarkan implementasi yang dilakukan didapatkan bahwa Pengaturan dan login berbasis web, tidak diperlukan software instalasi tambahan. Terdapat fasilitas billing untuk penggunaan yang lebih lanjut. Serta memiliki Log yang sangat lengkap untuk auditing, termasuk waktu, banyak data yang dikirim, klien yang mendapat IP dari DHCP, dan URL tracking (melihat website yang dikunjungi). Juga terdapat pengaturan *bandwidth* agar dapat terjadi pendistribusian yang efisien.



Gambar 11. Perancangan Akhir Menggunakan Server Firstspot 2

FirstSpot akan berfungsi sebagai jembatan antara *Wireless* AP dan Jaringan Intranet lainnya. Pemasangan *server* FirstSpot pada titik seperti pada gambar, memberikan keuntungan lain, yaitu tidak perlu menggunakan *Wireless* AP yang mendukung *RADIUS* karena masih sangat jarang dan mahal. *Wireless* AP yang digunakan cukup AP biasa misalnya DLINK Airplus DWL-2100 yang banyak tersedia di pasaran. [5]

Untuk membuka web untuk mengatur server, ketikkan localhost:5787 pada browser atau dengan klik pada Configuration Manager di start menu.

IV. KESIMPULAN

Simulasi jaringan *hotspot* yang ter-integrasi dengan *RADIUS SERVER* telah berjalan dengan baik, sehingga tidak akan sulit untuk diimplementasikan ke dalam keadaan sebenarnya.

Software FirstSpot berfungsi sebagai jembatan antara Microsoft IAS dan *Wireless Access Point*, sehingga *Authentication, Authorization, Accounting* dan *Auditing* (AAAA) terhadap user dapat dilakukan dan diperoleh keunggulan lain yaitu fasilitas billing.

Untuk pengembangan lebih lanjut diusulkan penelaahan untuk implementasi lebih lanjut pada setiap jaringan *hotspot* diberbagai unit maupun departemen yang dapat dikelola secara terpusat untuk memudahkan administrasi dan peningkatan keamanan yang lebih baik.

REFERENSI

[1] "RADIUS", http://en.wikipedia.org/wiki/ RADIUS.

[2] "How to use the Microsoft Radius server IAS in a wireless or/and VPN deployment", http://www.microsoft.com/technet/community/chats/trans/isa/isa0316.mspx.

[3] "Wireless Networking with Microsoft IAS Server", http://www.microsoft.com/technet/ community/chats/trans/network/net1216.mspx

[4] "Securing Wireless LANs with Certificate Services", http://www.microsoft.com/ technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx?mfr=true

[5] "FirstSpot® v7", http://www.patronsoft.com/ firstspot/

[6] "Using RADIUS For WLAN Authentication, Part I", http://www.wi-fiplanet.com/ tutorials/ article.php/ 3114511