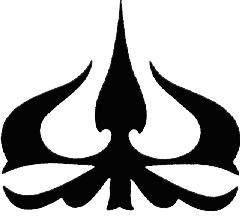
Makalah Sistem Pengendalian Akses

Akses Kontrol Pada RADIUS



**Nama : Vebry Dwiyana Risalni**

**NIM : 064.10.001 rrrrrrrrrr**

**Jurusan Teknik Informatika**

**Fakultas Teknologi Industri**

**Universitas Trisakti**

**RADIUS**

Remote Access Dial In User Service (RADIUS) adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan autentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan.

RADIUS dikembangkan dipertengahan tahun 1990 oleh Livingstone Enterprise (sekarang Lucent Technologies). Pada awalnya perkembangan RADIUS menggunakan port 1645 yang ternyata bentrok dengan layanan datametrics. Sekarang port yang dipakai RADIUS adalah port 1812 yang format standarnya ditetapakan pada Request for Command (RFC) 2138.

Server RADIUS menggunakan konsep AAA untuk mengatur akses jaringan dengan dua langkah yang dikenal sebagian “AAA transaction” dimana AAA tersebut memiliki kepanjangan Authentication, Authorization, dan Accounting. Autentikasi yaitu proses pengesahan identitas pengguna untuk mengakses jaringan, Autorisasi yaitu proses pengecekan wewenang pengguna, mana saja hak-hak akses yang diperbolehkan dan mana saja yang tidak sedangkan Accounting merupakan proses pengumpulan data dan informasi seputar berapa lama user melakukan koneksi dan billing time yang telah dilalui selama pemakaian.

Protokol RADIUS biasa digunakan oleh ISP dan perusahaan untuk mengatur akses ke internet atau jaringan internal, jaringan wireless, dan layanan e-mail terintegrasi.

**Karakteristik**

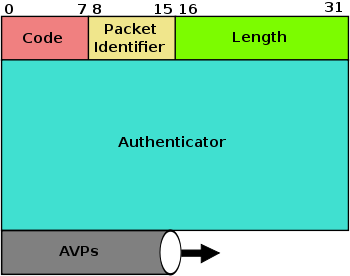
* Berbasis UDP Protocol (port 1812 untuk autentikasi dan 1813 untuk autorisasi)
* Bisa ditempatkan dimana saja di internet dan dapat membuat autentikasi (PPP, PAP, CHAP, MS-CHAP, EAP) antara Network Access Server (NAS) dan server itu sendiri
* RADIUS menggunakan Remote Access Server (RAS) Secure ID untuk membuat autentikasi yang kuat dalam pengontrolan akses

**Fungsi RADIUS**

* Mengautentikasi pengguna atau device sebelum memberikan akses ke sebuah jaringan.
* Mengautorisasi user dan device tersebut atas layanan-layanan jarungan tertentu
* Mencatat penggunaan layanan tersebut.

**Format Paket Data RADIUS**

Format paket RADIUS terdiri dari Code, Identifier, Length, Authenticator dan Attributes



**Code :** Memiliki panjang 1 byte (8 bit), digunakan untuk membedakan tipe pesan RADIUS yang dikirim. Tipe pesan RADIUS dapat berupa access request, access accept, access reject dan access challenge.

**Identifier :** Memiliki panjang 1 byte yang digunakan untuk menyesuaikan antara paket permintaan dan respon dari server RADIUS.

**Length :** Memiliki panjang 2 byte, memberikan informasi mengenai panjang paket. Jika paket kurang atau lebih dari yang diidentifikasikan pada length maka paket akan dibuang.

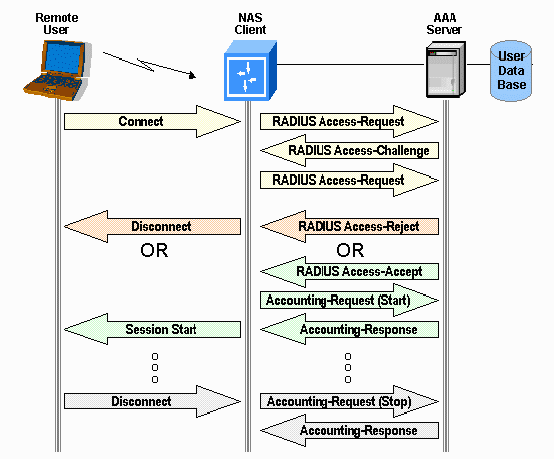
**Authenticator :** Memiliki panjang 16 byte yang digunakan untuk mengautentikasi tanggapan dari server RADIUS.

**Attributes** : Memiliki panjang yang tidak tetap, berisi autentikasi, autorisasi dan informasi. Contoh atribut RADIUS yaitu, username dan password.

Protokol RADIUS merupakan protokol connectionless berbasis UDP yang tidak menggunakan koneksi langsung. Satu paket RADIUS ditandai dengan field UDP yang menggunakan port 1812. Beberapa pertimbangan RADIUS menggunakan lapisan transport UDP yaitu:

1. Jika permintaan autentikasi pertama gagal, maka permintaan kedua harus dipertimbangkan.
2. Bersifat stateless yang menyederhanakan protokol pada penggunaan UDP.
3. UDP menyederhanakan implementasi dari sisi server.

**Prinsip Kerja RADIUS**



RADIUS merupakan protokol security yang bekerja menggunakan system client-server terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan pengguna yang tidak berhak. RADIUS melakukan autentikasi user melalui serangkain komunikasi antara client dan server. Bila user telah berhasil melakukan autentikasi, maka user tersebut dapat menggunakan layanan yang disediakan oleh jaringan.

Kelebihan yang diberikan oleh protokol RADIUS yaitu Menjalankan sistem administrasi terpusat. Protokol *connectionless* berbasis UDP yang tidak menggunakan koneksi langsung. Mendukung autentikasi Password Authentication Protocol (PAP) dan Challenge Handshake Authentication Protocol (CHAP) Password melalui PPP.

Pada protokol RADIUS masih ditemukan beberapa kelemahan yaitu tidak adanya autentikasi dan verifikasi terhadap access request dan tidak sesuai digunakan pada jaringan dengan skala yang besar.

**Mekanisme Akses RADIUS**

Lalu lintas pesan pada RADIUS menggunakan metode permintaan dan tanggapan (client/server) yang dapat dilihat pada gambar di bawah ini

* *Access Reject*

User ditolak aksesnya ke semua sumberdaya dalam jaringan. Penyebabnya bisa termasuk kegagalah untuk menyediakan indentifikasi yang tepat atau nama akun yang salah/tidak aktif

* *Access Challenge*

Permintaan informasi tambahan dari user, seperti password alteernatif, PIN, token atau kartu.

* *Access Accept*

User diberikan akses masuk. Begitu User ter-autentifikasi, server RADIUS akan sering mengecek agar User hanya menggunakan sumberdaya sesuai dengan yang diminta. Misalnya User hanya boleh mengakses fasilitas hotspot, dan tidak untuk menggunakan printer. Informasi tentang User dalam *database* bisa disimpan secara lokal dalam server RADIUS atau disimpan dalam tempat penyimpanan eksternal seperti LDAP atau *Active Directory*

**Proses Authentication**

Proses autentikasi diperlukan ketika pemilik mempunyai kebutuhan untuk membatasi siapa saja yang diperbolehkan masuk ke dalam jaringan remote accessnya. Untuk memenuhi kebutuhan tersebut, pengguna yang ingin mengakses sebuah jaringan secara remote harus diidentifikasi terlebih dahulu. Pengguna yang ingin masuk ke dalam jaringan pribadi tersebut perlu diketahui terlebih dahulu sebelum bebas mengakses jaringan tersebut. Pengenalan ini bertujuan untuk mengetahui apakah pengguna tersebut berhak atau tidak untuk mengakses jaringan.

Pada umumnya, perangkat remote access telah dilengkapi dengan sebuah daftar yang berisikan siapa-siapa saja yang berhak masuk ke jaringan di belakangnya. Metode yang paling umum digunakan untuk mengenali pengakses jaringan adalah dialog Login dan Password. Metode ini juga didukung oleh banyak komponen lainnya, seperti metode *challenge* dan *response*, *messaging support*, dan enkripsi, tergantung pada protokol sekuriti apa yang Anda gunakan.

**Proses Authorization**

Proses authorization merupakan langkah selanjutnya setelah proses autentikasi berhasil. Ketika pengguna yang ingin mengakses jaringan pemilik telah dikenali dan termasuk dalam daftar yang diperbolehkan membuka akses, langkah berikutnya Anda harus memberikan batasan hak-hak apa saja yang akan diterima oleh pengguna tersebut.

Untuk membatasi masing-masing pengguna biasanya adalah dengan menggunakan seperangkat atribut khusus yang dirangkai-rangkai untuk menghasilkan *policy* tentang hak-hak apa saja yang dapat dilakukan si pengguna. Atribut-atribut ini kemudian dibandingkan dengan apa yang dicatat di dalam *database*.

Setelah dibandingkan dengan informasi yang ada di database, hasilnya akan dikembalikan lagi kepada fasilitas AAA yang berjalan pada perangkat tersebut. Berdasarkan hasil ini, perangkat *remote access* akan memberikan apa yang menjadi hak dari si pengguna tersebut. Apa saja yang bisa dilakukannya dan apa saja yang dilarang sudah berlaku dalam tahap ini.

*Database* yang berfungsi untuk menampung semua informasi ini dapat dibuat secara lokal di dalam perangkat *remote access* atau router maupun dalam perangkat khusus yang biasanya disebut dengan istilah server sekuriti. Di dalam server sekuriti ini biasanya tidak hanya informasi profil penggunanya saja yang ditampung, protokol sekuriti juga harus berjalan di sini untuk dapat melayani permintaan informasi profil dari perangkat-perangkat yang berperan sebagai kliennya. Pada perangkat inilah nantinya *attribute-value* (AV) dari pengguna yang ingin bergabung diterima dan diproses untuk kemudian dikembalikan lagi menjadi sebuah peraturan oleh fasilitas AAA tersebut.

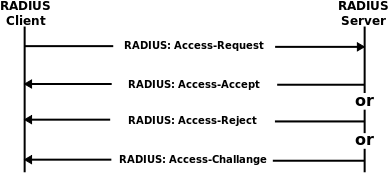
Metode authorization biasanya dilakukan dalam banyak cara. Bisa dilakukan dengan cara *one-time authorization* yang memberikan seluruh hak dari si pengguna hanya dengan satu kali proses *authorization*. Atau bisa juga dilakukan per *service authorization* yang membuat pengguna harus diotorisasi berkali-kali ketika ingin menggunakan layanan tertentu. *Authorization* juga bisa dibuat per pengguna berdasarkan daftar yang ada di server sekuriti, atau kalau protokolnya mendukung otorisasi bisa diberlakukan per group pengguna. Selain itu, jika keamanan server memungkinkan, pemilik dapat memberlakukan aturan-aturan otorisasi berdasarkan sistem pengalamatan *IP*, *IPX*, dan banyak lagi

**Proses Accounting**  
 Proses accounting dalam layanan koneksi remote access amat sangat penting, apalagi jika pemilik membuat jaringan ini untuk kepentingan komersial. Dalam proses accounting ini, perangkat remote access atau server sekuriti akan mengumpulkan informasi seputar berapa lama si pengguna sudah terkoneksi, billing time (waktu start dan waktu stop) yang telah dilaluinya selama pemakaian, sampai berapa besar data yang sudah dilewatkan dalam transaksi komunikasi tersebut.

Data dan informasi ini akan berguna sekali untuk pengguna maupun administratornya. Biasanya informasi ini akan digunakan dalam melakukan proses auditing, membuat laporan pemakaian, penganalisisan karakteristik jaringan, pembuatan billing tagihan, dan banyak lagi. Fasilitas accounting pada jaringan remote access umumnya juga memungkinkan Anda untuk melakukan monitoring terhadap layanan apa saja yang digunakan oleh pengguna. Dengan demikian, fasilitas accounting dapat mengetahui seberapa besar *resource* jaringan yang pemilik gunakan.

Ketika fasilitas AAA diaktifkan pada sebuah perangkat jaringan *remote access*, perangkat tersebut akan melaporkan setiap transaksi tersebut ke keamanan server. Mekanisme pelaporan dapat berbeda-beda tergantung pada protokol yang dipergunakan oleh pemilik. Setiap *record accounting* akan mempengaruhi nilai-nilai atribut dari proses AAA yang lain seperti authentication dan authorization. Semua informasi yang saling terkait ini kemudian disimpan di dalam *database* server sekuriti atau jika memang diperlukan, kumpulan informasi ini dapat disimpan di server khusus tersendiri. Biasanya server khusus *billing* diperlukan jika penggunanya sudah berjumlah sangat banyak.

Berikut ini adalah contoh cara kerja RADIUS:



* 1. Sebuah *Wireless Node* (WN) / *Supplicant* dengan alamat IP 192.168.10.30 dan IP yang telah terdaftar dalam pemfilteran MAC ADDRESS meminta akses ke *wireless network* atau *Access Point* (AP).
  2. *Access Point* (AP) akan menanyakan identitas *Supplicant*. Tidak ada trafik data selain *Client* yang diperbolehkan sebelum *Supplicant* terautentikasi. Dalam hal ini,*Access point* bukanlah sebuah autentikator, tetapi *access point* berisi autentikator.
  3. Setelah nama-pengguna dan password dikirim, proses autentikasi dimulai. Autentikator mengenkapsulasi kembali pesan ke dalam format RADIUS, dan mengirimnya ke RADIUS server. Selama proses autentikasi, autentikator hanya menyampaikan paket antara Supplicant dan RADIUS server. Setelah proses autentikasi selesai, RADIUS server mengirimkan pesan sukses (atau gagal, apabila proses autentikasinya gagal.) Apabila proses autentikasi sukses, *Supplicant* diperbolehkan untuk mengakses wireless LAN dan/atau internet.
  4. Jika nama *Supplicant* tidak terautentifikasi, maka radius server akan mengirim pesan gagal. Dan proses authentifikasi tidak berjalan atau gagal.

**Contoh Implementasi**

RADIUS umumnya digunakan oleh ISP (*Internet Service Provider*) atau penyedia layanan internet untuk melakukan *Authentication* (pembuktian keaslian pengguna), *Authorize* (mengatur pemberian hak /otoritas) dan *Accounting* (mencatat penggunaan layanan yang digunakan).

RADIUS menjalankan sistem administrasi pengguna yang terpusat. Sistem ini akan mempermudah tugas administrator. Dapat kita bayangkan berapa banyak jumlah pelanggan yang dimiliki oleh sebuah ISP, dan ditambah lagi dengan penambahan pelanggan baru dan penghapusan pelanggan yang sudah tidak berlangganan lagi. Apabila tidak ada suatu sistem administrasi yang terpusat, maka akan merepotkan administrator dan tidak menutup kemungkinan ISP akan merugi atau pendapatannya berkurang. Dengan sistem ini pengguna dapat menggunakan *hotspot* di tempat yang berbeda-beda dengan melakukan autentikasi ke sebuah RADIUS server.