Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)
Edisi 1 Volume 1, Agustus 2014 ISSN :2089-9033

Pembangunan *Network Access Control* untuk Autentikasi dan *Security* dengan Menggunakan *802.1X Authentication*

Asep M Taufik[1]

[1] Teknik Informatika – Universitas Komputer Indonesia
Jl. Dipatiukur 112-114 Bandung
Email : aseps.mt@gmail.com[1]

ABSTRAK

UPT TI merupakan pengelola teknologi informasi di Unpad. Permasalahan yang dihadapi UPT TI pada saat ini, adalah bertambahnya jumlah pengguna yang dapat dengan mudah mengakses jaringan Unpad, sehingga menyebabkan sulitnya sistem dalam memvalidasi dan mengontrol akses *user* dan perangkat-perangkat yang masuk atau terkoneksi ke jaringan Unpad. Pemanfaatan mekanisme *network access control* (NAC) dengan standar protocol IEEE 802.1x menjadi salah satu solusi yang berdasarkan pada *mac address* perangkat pengguna. Dengan mekanisme ini, *user* yang terkoneksi ke jaringan Unpad akan menjadi terkontrol dan lebih aman, selain itu akan memudahkan bagi *network administrator* dalam melakukan monitoring, serta investigasi ketika terjadi hal-hal yang tidak wajar yang diakibatkan oleh perangkat *user*.

Kata Kunci : Unpad, *Network Access Control* (NAC), IEEE 802.1x, *mac address.*

1. PENDAHULUAN

UPT TI Unpad terus meningkatkan pelayanan dan pengembangan fasilitas teknologi informasi untuk menunjang setiap kegiatan di lingkungan Unpad.
Namun seiring pertambahan *node-node* jaringan tersebut, kontrol dan pengidentifikasian terhadap pengguna, perangkat dan aktivitas yang ada di dalam jaringan menjadi sulit dilakukan oleh *network administrator*. Sehingga tidak menutup kemungkinan aktivitas - aktivitas lainnya yang dapat mengganggu, mengambil, bahkan merusak data dan infrastruktur jaringan Unpad mengingat akses ke jaringan Unpad sangat mudah, disamping adanya kelemahan-kelemahan pada aplikasi atau *software*. Selain itu juga, metode dan teknologi yang digunakan untuk aktivitas – aktivitas ilegal dalam teknologi informasi atau jaringan komunikasi terus berkembang dan adanya kebiasaan-kebiasaan yang yang salah dilakukan *user* seperti tidak meng*update* antivirus, membuka *attachment* yang berbahaya dan lain sebagainya.
Maka dibutuhkan suatu mekanisme manajemen kontrol di jaringan Unpad agar jaringan lebih optimal dan aman. Salah satunya dengan pengimplementasian autentikasi pada jaringan (*network access control*) yang berjalan pada layer media-access (layer 2 OSI) mengg*unakan IEEE 802.1x authentication* dengan *mac address*. Mekanisme ini akan memvalidasi perangkat-perangkat seperti leptop, ponsel dan perangkat lainnya yang digunakan oleh *user*. *User* yang terkoneksi ke jaringan Unpad akan menjadi terkontrol dan lebih aman, selain itu akan memudahkan bagi *network administrator* dalam melakukan monitoring, serta investigasi ketika terjadi hal-hal yang tidak wajar yang diakibatkan oleh perangkat *user*.

1.1 Network Access Controll

Network Access Control adalah sebuah jalan untuk keamanan jaringan komputer yang mencoba menyatukan teknologi keamanan *endpoint* (seperti antivirus, *host intrusion prevention*, dan *vulnaberity assessment*).

Network Access Control adalah solusi jaringan komputer yang menggunakan suatu kumpulan protokol untuk mendefinisikan dan mengimplementasikan sebuah kebijakan yang menjelaskan cara untuk mengamankan akses ke suatu node jaringan oleh suatu perangkat ketika mereka mencoba untuk pertama kalinya. NAC mungkin saja menghubungkan proses *automatic remediation* (memperbaiki *node non-compliant* sebelum memperbolehkan untuk mengaskes) kedalam sistem jaringan, memperbolehkan infrastruktur jaringan seperti *router, switch* dan *firewall* untuk bekerja bersama dengan s*e*rver *back office* dan komputer *end user* untuk memastikan sistem informasi berjalan dengan aman sebelum kerja sama kedua sistem diperbolehkan.

Network Access Control memiliki tujuan yang sama dengan namanya yaitu mengkontrol akses ke jaringan dengan beberapa kebijakan, termasuk pemeriksaan sebelum dan *pasca* masuk untuk *endpoint*, dimana *user* dan perangkatnya dapat pergi ke suatu jaringan dan apa yang dapat mereka lakukan dalam jaringan tersebut.

Dengan kata lain ketika suatu komputer terhubung, komputer tersebut tidak diijinkan untuk

mengakses apapun kecuali komputer tersebut mengikuti kebijakan yang telah didefinisikan; termasuk perlindungan anti-virus, *update* sistem, dan konfigurasi. Ketika komputer sedang dicek oleh *pre-installed software agent*, komputer hanya dapat mengakses sumber yang dapat memulihkan (memecahkan atau meng*update*) berbagai *issues*/masalah. Ketika kebijakan terpenuhi, komputer dapat mengakses sumber jaringan dan internet, dengan kebijakan yang telah ditentukan oleh NAC.

Banyak sekali solusi yang menawarkan NAC baik yang berupa *appliance* maupun berupa aplikasi yang diinstalkan pada server. Selain itu juga, ada yang berbayar ataupun yang gratis. Beberapa solusi NAC diantaranya adalah :

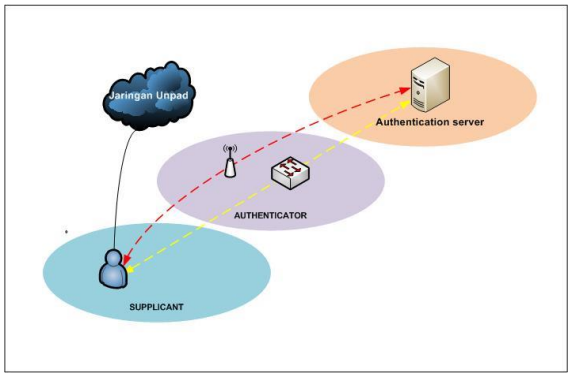
1. Cisco NAC Appliance.
2. ForeScout
3. Symantec NAC for security
4. McAfee NAC Appliance, Modul and Software
5. Extreme Network NAC Solution
6. Trustwave Network Access Control
7. Packetfence

Selain yang disebutkan diatas banyak lagi yang menawarkan solusi-solusi untuk *network access control* ini.

1.2 IEEE 802.1X

IEEE 802.1x merupakan protokol kontrol akses jaringan berbasis port yang memanfaatkan karakteristik infrastruktur LAN IEEE 802 untuk menyediakan media autentikasi dan autorisasi perangkat yang terhubung pada port LAN yang memiliki karakteristik koneksi *point to point*, dan mencegah akses jika autentikasi dan autorisasi gagal. Tujuan penggunaan standar ini IEEE 802.1x ini adalah untuk menghasilkan kontrol akses dan autentikasi terhadap perangkat user yang akan masuk ke jaringan Unpad.

IEEE 802.1x ini terdiri dari tiga bagian, yaitu pengguna atau user (mahasiswa, staff dan dosen Unpad) yang akan diauthentikasi atau yang disebut *supplicant*, server yang akan melakukan autentikasi yang disebut *Network Access Server* (*NAS*) *authentication server* yang digunakan adalah Remote Authentication Dial-In User Service (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses wireless ataupun jaringan kabel. Yang ketiga adalah *authenticator* yang menghubungkan kedua bagian tersebut dalam hal ini switch manageable.



Gambar 1 Mekanisme *IEEE 802.1x*

1.3 Protokol AAA

Menurut Jonathan Hassel (2002) konsep kerja *server* autentikasi dikenal dengan AAA *(authentication*, *authorization*, and *accounting).* Yang terdiri dari otentikasi, otorisasi, dan pendaftaran akun pengguna. Konsep AAA mempunyai fungsi yang berfokus pada tiga aspek dalam kontrol akses *user*, yaitu :

1. *Authentication*

Otentikasi adalah proses verifikasi untuk menyatakan suatu identitas. Bentuk umum yang biasa digunakan untuk melakukan otentikasi menggunakan kombinasi *login ID/username* dan *password*. jika kombinasi kedua nya benar maka *client* dapat mengakses ke sumber daya jaringan tertentu. Proses otentikasi dapat dianalogikan seperti seorang tamu yang datang ke rumah anda, sebelum tamu tersebut diperbolehkan masuk, tentu anda harus mengetahui tamu itu terlebih dahulu, jika anda kenal dengan tamu tersebut, maka tamu tersebut pastinya akan anda persilahkan masuk dan sebaliknya.

2. *Authorization*

Otorisasi melibatkan penggunaan seperangkat aturan - aturan yang berlaku untuk memutuskan aktifitas apa saja yang dizinkan dalam sistem atau sumber daya jaringan tertentu untuk pengguna yang terotentikasi. Proses Authorization merupakan lanjutan dari proses Authentication. Proses Authorization dapat dianalogikan sebagai berikut: jika anda sudah mengizinkan tamu untuk masuk kerumah anda, tentu anda mempunyai aturan – aturan yang ditempel di dinding rumah anda, misalnya tamu hanya boleh masuk sampai dengan ruang tamu. Dengan aturan seperti ini tentu akan memudahkan seseorang untuk melakukan kontrol terhadap sumber daya jaringan tertentu.

3. *Accounting*

Proses *accounting* merupakan proses dimana terdapat proses pencatatan berapa lama seorang pengguna sudah terkoneksi (waktu mulai / waktu stop) yang telah dilakukan selama pemakaian. Data dan informasi ini sangat berguna baik untuk pengguna maupun administrator, biasanya laporan

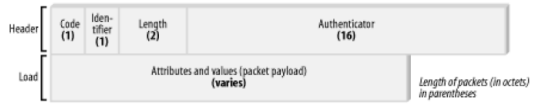
ini digunakan untuk melakukan *auditing*, membuat laporan pemakaian, membaca karakteristik jaringan, dan pembuatan *billing* tagihan. Jadi pada intinya proses *accounting* berguna untuk mengetahui apa saja yang dilakukan oleh *client* dan *service* apa saja yang dilakukan oleh *client*. Analogi sederhananya adalah mesin absensi di kantor, ia akan mencatat waktu datang dan waktu pulang, dengan demikian petugas dapat memonitoring karyawan dengan mudah.

1.3.1 RADIUS

RADIUS merupakan singkatan dari *Remote Authentication Dial-In User Service*. Pertama kali dikembangkan oleh Livingston Enterprises. Merupakan *network* protokol keamanan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar. RADIUS didefinisikan dalam RFC 2865 dan RFC 2866. RADIUS biasa digunakan oleh perusahaan untuk mengatur akses ke internet bagi *client*.
RADIUS melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses sumber daya jaringan. Sehingga memastikan bahwa pengguna yang mengakses jaringan adalah pengguna yang sah. RADIUS berstandar IEEE 802.1x. Sering disebut "*port authentication based*". RADIUS merupakan protokol *client – server* yang berada pada layer aplikasi pada OSI layer. Dengan protokol *transport* UDP.(Jonathan Hassel, 2002).

1.3.2 Format Paket RADIUS

Protokol RADIUS menggunakan paket UDP untuk melewati transmisi antara *client* dan *server*. Protokol tersebut akan berkomunikasi pada *port* 1812. Berikut struktur paket RADIUS :



Gambar 2.1 Format Paket RADIUS

Format paket data RADIUS pada Gambar 2.19 terdiri dari 5 (lima) bagian, yaitu:

1. *Code* : memiliki panjang satu oktet, digunakan untuk membedakan tipe pesan RADIUS yang dikirimkan pada paket. Kode-kode tersebut (dalam desimal) dapat dilihat pada Tabel 2.2

Tabel 1 Kode Tipe Pesan RADIUS

Kode	Tipe pesan RADIUS
1	*Access-Request*
2	*Access-Accept*
3	*Access-Reject*
4	*Accounting-Request*
5	*Accounting-Response*
11	*Access-Challenge*
12	*Status-Server (experimental)*
13	*Status-Client (experimental)*
255	*Reserved*

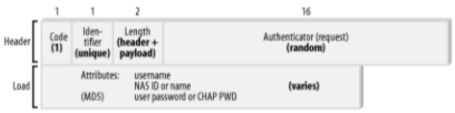
2. *Identifier* : Memiliki panjang satu oktet, bertujuan untuk mencocokkan permintaan.
3. *Length* : Memiliki panjang dua oktet, memberikan informasi mengenai panjang paket.
4. *Authenticator* : Memiliki panjang 16 oktet, digunakan untuk membuktikan balasan dari RADIUS *server*, selain itu digunakan juga untuk algoritma *password*.

Attributes : Berisikan informasi yang dibawa pesan RADIUS, setiap pesan dapat membawa satu atau lebih atribut. Contoh atribut RADIUS: nama pengguna, *password*, alamat IP *access point* (AP), pesan balasan. Tujuan standar 802.1x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk *wireless* LAN. Standar ini berdasarkan pada *Internet Engineering Task Force* (IETF), *Extensible Authentication Protocol* (EAP), yang ditetapkan dalam RFC 2284.

1.3.3 Tipe Pesan RADIUS

Ada 4 (empat) jenis paket pesan RADIUS yang relevan dengan otentikasi dan otorisasi pada fase transaksi AAA yaitu :

1. *Access-Request*
   Paket *Access-Request* digunakan oleh layanan konsumen ketika meminta layanan tertentu dari jaringan. *Client* mengirimkan paket *request* ke RADIUS *server* dengan daftar layanan yang diminta. Faktor kunci dalam transmisi ini adalah kolom kode pada *header* paket, dimana *header* paket tersebut harus di-*set* dengan nilai 1, yang merupakan nilai unik pada paket permintaan. RFC menyatakan bahwa balasan harus dikirimkan ke semua paket permintaan yang *valid*, apakah jawabannya adalah otorisasi atau penolakan.



Gambar 2. Paket *Access-Request*

Tabel 2 Paket *Access-Request*

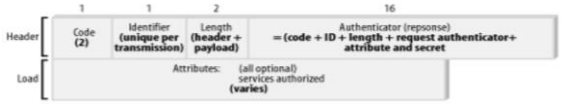
Identifier	Unique per request
Length	Panjang header ditambah semua atribut data tambahan
Authenticator	Request

Attribute Data	2 atau lebih

2. Access-Accept

Paket *Access-Accept* dikirim oleh RADIUS *server* kepada *client* untuk mengakui bahwa permintaan *client* diberikan. Jika semua permintaan Access-Request dapat diterima, maka server RADIUS harus mengatur paket respon dengan nilai 2 pada sisi *client*, setelah paket tersebut diterima, paket tersebut di cek apakah sama atau benar paket tersebut adalah paket respon dari RADIUS *server* dengan menggunakan *identifier field*. Jika terdapat paket yang tidak mengikuti standar ini maka paket tersebut akan dibuang.

Paket *Access-Accept* dapat berisi banyak atau sedikit atribut informasi yang perlu untuk dimasukkan. Kemungkinan besar atribut informasi pada paket ini akan menjelaskan jenis layanan apa saja yang telah dikonfirmasi dan resmi sehingga *client* dapat menggunakan layanan tersebut. Namun, jika tidak ada atribut informasi yang disertakan, maka *client* menganggap bahwa layanan yang diminta adalah yang diberikan.



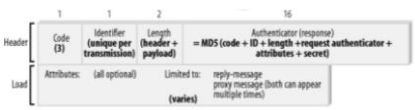
Gambar 3 *Paket Access-Accept*

Tabel 2.1 Paket *Access-Accept*

Packet Type	Response
Code	2
Identifier	Identical to Access-Request per
Length	Header length plus all additional attribute
Authenticator	Response
Attribute Data	0 or more

3. Access-Reject

RADIUS server dapat pula mengirimkan paket *Access-Reject* kembali ke *client* jika harus menolak salah satu layanan yang diminta *client* dalam paket *Access-Request*. Penolakan tersebut dapat didasarkan pada kebijakan sistem, hak istimewa yang tidak cukup, atau kriteria lain. *Access-Reject* dapat dikirim setiap saat selama waktu koneksi. Nilai yang diberikan untuk kode pada paket ini adalah 3.



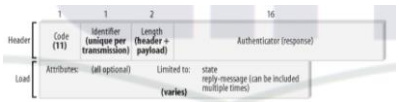
Gambar 4 Paket *Access-Reject*

Tabel 3 Paket *Access- Reject*

Packet Type	Response
Code	3
Identifier	Identical to Access-Request
Length	Header length plus all additional attribute
Authenticator	Response
Attribute Data	0 or more

4.Access-Challenge

Apabila *server* menerima informasi yang bertentangan dari *user*, atau membutuhkan informasi lebih lanjut, atau hanya ingin mengurangi risiko otentikasi palsu, *server* dapat menerbitkan paket *Access-Challenge* untuk *client*. Setelah client menerima paket *Access-Challenge* memberikan paket *Access-Request* yang baru disertai atribut informasi yang diminta *server*. Nilai yang diberikan pada *header* paket ini adalah 11.



Gambar 5 Paket *Access- Challenge*

Tabel 4 Paket *Access-Challenge*

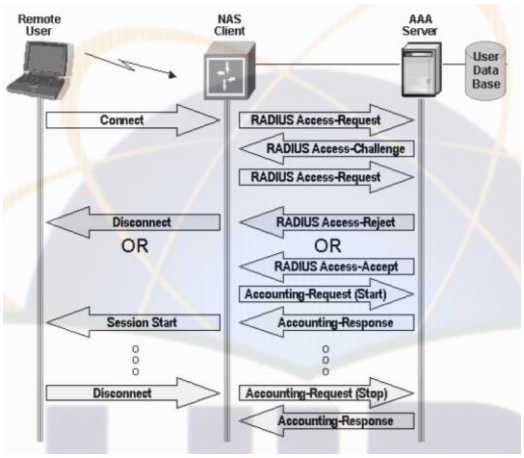
Packet Type	Response
Code	11
Identifier	Identical to Access-Request
Length	Header length plus all additional attribute
Authenticator	Response
Attribute Data	0 or more

1.3.4 Tahapan Pembentukan RADIUS

Penggunaan RADIUS terhadap usaha pembentukan koneksi jaringan dapat dilakukan dengan melalui tahapan tahapan berikut:

1. *Access server*, *access point* menerima permintaan koneksi dari *access client*.
2. *Access server* dikonfigurasi agar dapat menggunakan RADIUS sebagai protokol yang melakukan proses otentikasi, otorisasi dan *accounting*, membuat sebuah pesan *access request* dan mengirimkannya ke *server* RADIUS.

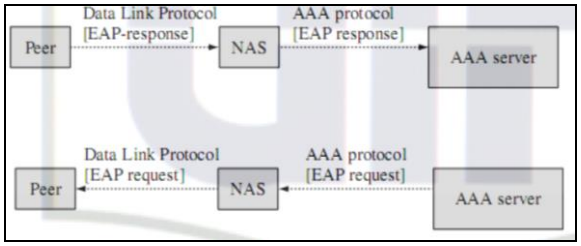
3. Server RADIUS melakukan evaluasi pesan *access request*
4. Jika dibutuhkan, server RADIUS mengirimkan pesan *access challenge* ke *access server*. Jawaban terhadap pesan tersebut dikirimkan dalam bentuk *access request* ke *server* RADIUS.
5. Surat kepercayaan dan otorisasi dari usaha pembentukan koneksi diverifikasi.
6. Jika usaha pembentukan koneksi dan diotorisasi, server RADIUS mengirimkan sebuah pesan *access accept* ke *access server*. Sebaliknya jika usaha tersebut ditolak maka server RADIUS mengirimkan sebuah pesan *access reject* ke *access server*.
7. Selama menerima pesan *access accept*, *access server* melengkapi proses koneksi dengan *access client* dan mengirimkan sebuah pesan *accounting request* ke server radius.
8. Setelah pesan *accounting request* diproses, *server* RADIUS mengirimkan sebuah pesan *accounting response*. (Zaenal Arifin, 2008).



Gambar 6 Proses Pembentukan Koneksi Protokol RADIUS

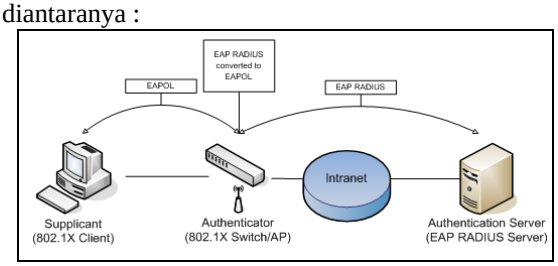
1.4 EAP

EAP atau *Extensible Authentication Protocol* adalah suatu *framework* otentikasi yang menyediakan layanan *transport* dan penggunaan *key* material dan parameter yang dihasilkan oleh EAP pada awalnya dikembangkan untuk koneksi *Point-to-Point* atau PPP. Namun, saat ini EAP juga diimplementasikan dan banyak digunakan untuk otentikasi penggunaan pada jaringan nirkabel. EAP digunakan pada *three-tier authentication*, maka pada proses komunikasinya EAP akan menggunakan *transport* protokol yang berbeda. Pertama, pada komunikasi antara *supplicant* dan *authenticator*, EAP akan menggunakan data *link* protokol seperti PPP, Ethernet atau WLAN. Kedua, pada komunikasi mengunakan *application layer* protokol seperti RADIUS atau Diameter.



Gambar 7 Proses Komunikasi Protokol EAP antara *Supplicant*, NAS dan *Authentication Server*

Dalam EAP terdapat beberapa komponen diantaranya :

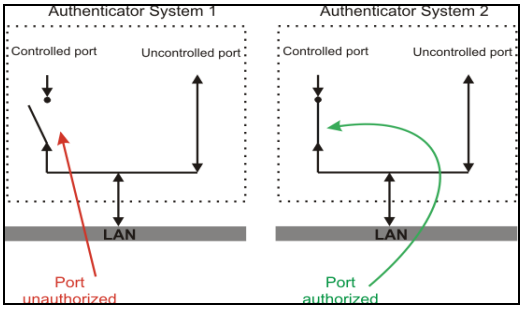


Gambar 8 Komponen EAP

1. *Supplicant*

   Merupakan *wireless node* yang ingin mengakses jaringan disebut *supplicant*.
2. *Authenticator*

   Merupakan perangkat yang memberikan akses menuju *server*. *Authenticator* merupakan *device* yang memproses apakah suatu *supplicant* dapat mengakses jaringan atau tidak. *Authenticator* mengontrol dua jenis *port* yaitu yang disebut dengan *controlled ports* dan yang disebut dengan *uncontrolled ports*. Kedua jenis *port* tersebut merupakan logikal *port* dan menggunakan koneksi fisikal yang sama. Sebelum otentikasi berhasil, hanya *port* dengan jenis *uncontrolled* yang dibuka. Trafik yang diperbolehkan hanyalah EAPOL atau EAPOW. Setelah *supplicant* melakukan autentifikasi dan berhasil, *port* jenis *controlled* dibuka sehingga *supplicant* dapat mengakses LAN secara biasa. IEEE 802.1x mempunyai peranan penting dari standar 802.11i.



Gambar 9 Skema *Port Based Authentication*

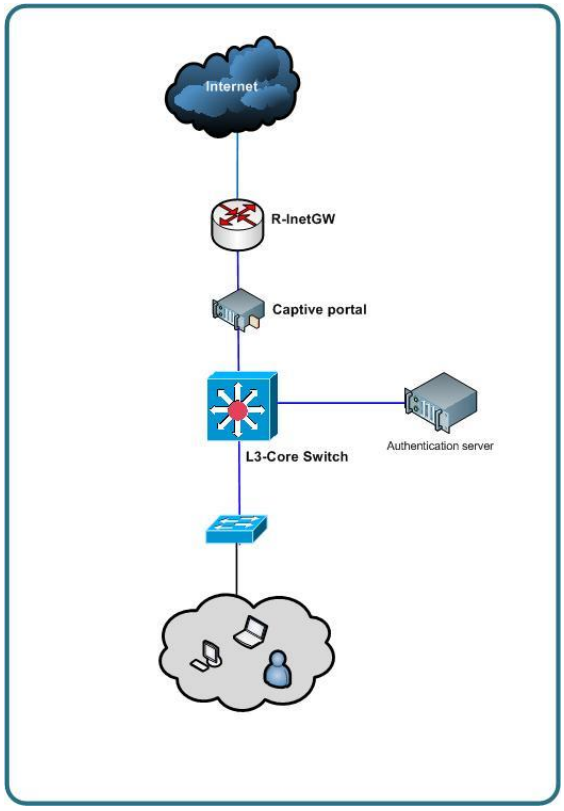
3. *Authentication Server* / RADIUS

Authentication Server / RADIUS adalah *server* yang menentukan apakah suatu *supplicant valid* atau tidak. *Authentication server* adalah berupa RADIUS *server* [RFC2865].

2 ISI PENELITIAN

2.1 Implementasi

Untuk mengimplementasikan network access control di Unpad. Berikut adalah arsitektur yang akan digunakan dalam menggambarkan sistem dari kinerja ATM :



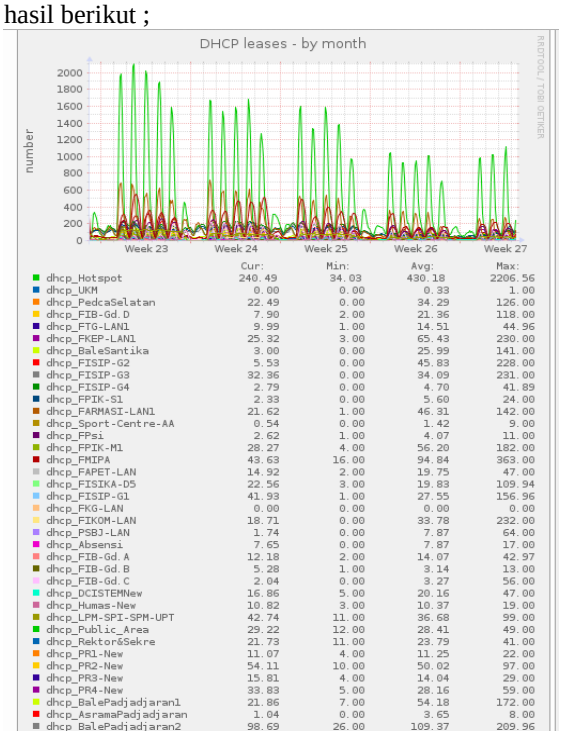
Gambar 10 Arsitektur Pengujian NAC

Perancangan pengalamatan ip ini disesuaikan berdasarkan arsitektur yang dibuat. Pengalamatan ip address ini sangat penting untuk memperlancar proses instalasi dan konfigurasi server atau switch. Subnetting alamat IP yang dialokasikan adalah 10.32.254.0/24 untuk *management*, 10.0.10.0/24 untuk *isolation*, 10.0.8.0/24 untuk *registration*, 10.0.0.0/24 untuk switch dan 10.32.0.0/24 untuk alamat network user. Network address yang dialokasikan adalah sebanyak tiga kelas C atau 254 host

Tabel 5 Daftar IP Address Perangkat

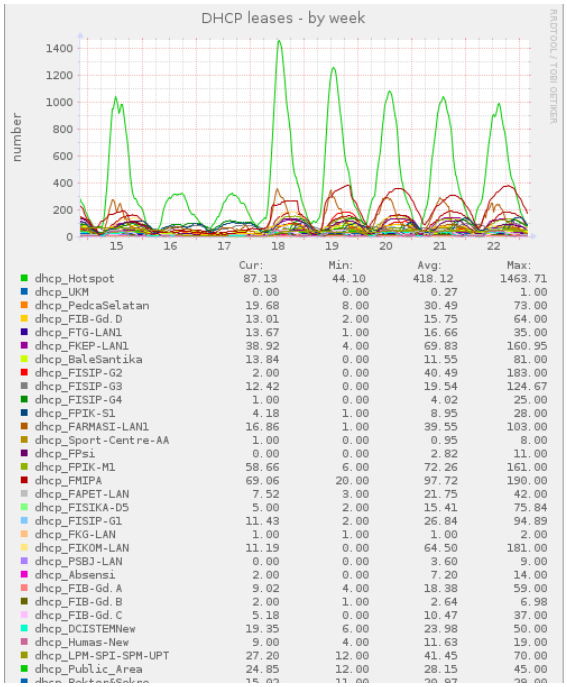
Type	Vlan id	IP Address
Management Server	1	10.32.254.10/24
Registration point server	51	10.0.8.10/24
Isolation point server	52	10.0.10.10/24
MAC detection	53	-
L3 Core Switch	1	10.32.254.1/24
Akses Switch	1	10.32.254.2/24
Client node	60	10.32.253.10/24 – 10.32.253.254/24

Setelah dirancanng kemudian konfigurasi masing masing perangkat mulai dari server sampai switch. Kemudian setelah dilakukan implementasi selanjutnya adalah dilakukan proses pengujian dengan tools monitoring munin., sehingga diperoleh hasil berikut ;



Gambar 11 Monitoring sebelum implementasi NAC

Terdapat perbedaan dengan hasil pengujian yang dilakuan selama satu minggu :



Gambar 11 Monitoring setelah implementasi NAC

Tabel Hasil Pengujian

Jenis Pengujian	Data Sebelum Implementasi	Data Sesudah Implementasi
Monitoring Munin Perangkat yang terkoneksi	Max 2000	Max 1400

5. KESIMPULAN

Berdasarkan analisa, perancangan, implementasi dan pengujian yang telah dilakukan, maka dapat ditarik kesimpulan yaitu dengan penerapan mekanisme NAC seorang network administrator dapat dengan mudah memonitor dan mengkontrol siapa saja yang terkoneksi juga mengontrol aktivitas yang ada dalam jaringan Unpad guna kepentingan keamanan informasi, data dan infrastruktur. Sehingga ketika terjadi suatu hal seorang network administrator dapat dengan mudah menanggulangi s*ecurity issue* di jaringan Unpad.

6. DAFTAR PUSTAKA

[1] Sociaty. IEEE Standards, Port-Based Network Access Controll, New York: The Institute of Electrical and Electronics Engineers, Inc., 2001.

[2] Czarny. Benny, Network Access Control Technologies, California: Opswat, 2008.

[3] Carlson. Tom, Information Security Management : Understanding ISO 1779,New Jersey: Lucent technologies World Services, 2001.

[4] Strand, L.802.1X Port-Based Authentication HOWTO.http://tldp.org/HOWTO/html_single/8021X-HOWTO/. Januari 2011

[5] Rigney, C., S. Willens, A. Rubens, and W.Simpson. 2000.Remote Authentication Dial In UserService (RADIUS). IETF RFC 2865.

[6] IEEE Std 802.1X . 2001.IEEE Standard for Local and Metropolitan area networks–Port-Based Network Access Control. IEEE.