

BAB III

METODOLOGI

Metodologi penelitian berfungsi sebagai penggambaran bagaimana langkah pengerjaan atau tahap yang dilakukan dalam penelitian. Langkah tersebut terbagi dalam beberapa bagian, yaitu:

3.1 Metode Pengumpulan Data

Dalam melakukan penelitian tugas akhir ini, penulis memerlukan data-data yang berkaitan dengan judul yaitu “*Autentikasi Hierarki di Radius LDAP*”. Proses pengumpulan data termasuk dalam tahap studi pustaka yaitu mencari dan mengumpulkan materi-materi yang berkaitan dengan penelitian untuk dijadikan referensi. Data bersumber dari buku, internet, laporan yang relevan serta materi dan bahan kuliah yang telah dipelajari.

3.2 Metode Perancangan dan Simulasi

a. Perencanaan

Pada tahap ini dilakukan identifikasi terhadap penelitian yang telah ada sebelumnya, definisi dan cakupan sistem yang telah diimplementasikan.

b. Analisis

Setelah proses perencanaan selesai, dilakukan analisa kebutuhan sistem dan studi kelayakan simulasi sistem baik mengenai struktur jaringan, perangkat lunak dan perangkat kerasnya, maupun sumber daya yang terlibat didalamnya.

c. Desain struktur

Autentikasi hierarki di radius LDAP ini diperlukan desain yang terstruktur, konfigurasi perangkat keras dan lunak, serta simulasi sistem jaringan.

d. Simulasi

Struktur jaringan yang telah didesain kemudian disimulasikan. Dimulai dari penyusunan rencana perangkat keras dan perangkat lunak yang akan digunakan, membuat mesin virtual untuk radius server sesuai dengan struktur desain topologi, melakukan konfigurasi jaringan, dan mememanajemennya melalui *web browser* serta dilakukan pengujian sistem oleh penulis terhadap simulasi autentikasi hierarki di Radius LDAP.

e. Pengujian Autentikasi Hierarki di Radius LDAP

Simulasi mulai diuji coba terhadap semua mesin virtual yang telah di konfigurasi dan terhubung ke GNS3. Pengujian ini harus berhasil ketika simulasi dilakukan dengan menggunakan *credentials user* di setiap universitas terhubung ke radius server. Pengujian dilakukan oleh penulis dan beberapa rekan terdekat yang juga memiliki *smartphone* dengan sistem operasi android berdasar pada perangkat *wireless*.

3.3 Skenario Autentikasi Hierarki

Ketika *user* dari universitas A ingin mendapatkan akses ke jaringan Wi-Fi di universitas B, dengan ini kedua universitas harus dalam satu radius server yang terhubung pada standar *wireless* 802.1X. Artinya, asosiasi *user* dengan *wireless access point* (AP) terhubung pada server *Remote Authentication Dial In Users Service* (RADIUS) lokal dalam rangka proses autentikasi *user*. *User* pengunjung memasuki *credentials* untuk *login*, yaitu berupa *username* (dalam bentuk format *username@domain*) dan *password*. Permintaan tersebut menuju ke radius server lokal yang kemudian diteruskan ke Radius Top Level. Setelah Radius Top Level mengidentifikasi bahwa *user* milik domain yang berbeda berdasarkan pada pengidentifikasian autentikasi ke database, jika *user* ditemukan dalam database permintaan diteruskan melalui hierarki radius ke server di universitas *user* berasal. Tetapi jika tidak ada dalam database maka permintaan tidak akan diteruskan, dan proses autentikasi berhenti di radius server lokal. Proses terakhir *user* dikonfirmasi dan tanggapan diarahkan kembali ke universitas B, dengan kondisi *access point*

yang berada di universitas B terhubung pada perangkat *user* dan *user* diberikan hak akses. Universitas dapat menggunakan salah satu metode autentikasi yang berbeda tergantung pada tingkat keamanan yang diperlukan.

3.4 Analisis

Penulis membagi aktifitas pada tahap analisis ini menjadi beberapa fase, yaitu:

3.4.1 Identify (Mengidentifikasi Masalah)

Permasalahan yang muncul dari mahasiswa pada umumnya ketika ingin berkunjung ke universitas yang diinginkan sulit untuk mendapatkan akses internet melalui Wi-Fi yang tersedia di universitas lokal. Untuk mendapatkan akses pun harus meminjam identitas dari mahasiswa lokal. Berdasarkan dari permasalahan tersebut, penulis melakukan penelitian berupa simulasi agar mahasiswa yang berkunjung tidak perlu meminjam identitas mahasiswa lokal, tetapi menggunakan identitas mahasiswa itu sendiri melalui *bandwidth* universitas asal. *Bandwidth* adalah besaran nilai yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam koneksi melalui sebuah *network*, atau lebar saluran data (pita) yang dapat dilewati secara bersama-sama oleh seluruh data yang di transfer.

3.4.2 Understand (Memahami Rumusan Masalah)

Hasil dari identifikasi masalah membutuhkan pemahaman yang baik agar dapat menghasilkan solusi yang tepat. Dengan studi pustaka yang telah dijelaskan pada subbab 3.1, hasilnya digunakan untuk merumuskan solusi yang efektif dalam menyelesaikan rumusan masalah. Dari pemahaman ini, penulis berusaha meneliti dan mensimulasikan sistem jaringan yang akan dibangun dengan memahami konsep dari jaringan Inherent dan penerapannya pada *hierarchical design model* serta metode maupun jenis keamanan yang digunakan. Diharapkan dengan adanya penelitian ini dapat membantu mengatasi masalah tersebut.

3.4.3 Analyze (Menganalisa Komponen Sistem)

Hasil dari analisis adalah penulis akan merancang sebuah jaringan hierarki yang disimulasikan melalui *software network emulator* GNS3 yang terintegrasi pada VirtualBox sebagai mesin virtual untuk radius server.

3.4.4 Report (Melaporkan Hasil Analisis)

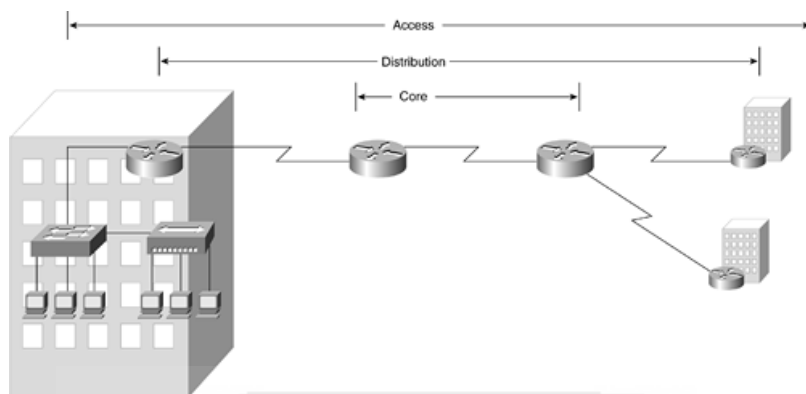
Proses akhir dari tahap analisis adalah pelaporan rincian dari berbagai komponen sistem yang dibutuhkan. Berpacu pada skenario autentikasi hierarki pada subbab 3.3, maka penulis menganalisa bahwa topologi jaringan yang akan digunakan yaitu topologi *hierarchical*. Topologi *hierarchical* atau topologi *tree* mempunyai susunan jaringan mirip dengan pohon yang bercabang. Pada topologi ini setiap *node* memiliki tingkat masing – masing, layaknya pohon yang memiliki cabang dan memiliki cabang lagi. *Node* yang memiliki tingkat tinggi diletakkan di atas sedangkan untuk *node* yang memiliki tingkat rendah diletakkan di bawah. Data yang dikirim oleh *node* tertentu harus melewati *central node* atau *node* pusat untuk sampai pada tujuan. Adapun kelebihan dan kekurangan dari topologi ini, antara lain:

Kelebihan :

- Topologi ini mudah dimanajemen karena adanya pusat *node* dalam tingkatan masing – masing.
- Bermanfaat untuk menjangkau jarak yang jauh dengan adanya sifat *repeater* dari *hub*.

Kekurangan :

- Jika ada *node* yang rusak di tingkat atas, maka *node* yang berada di bawahnya akan susah untuk mengirim *node* yang jauh atau tetangganya.
- Dalam membangun sebuah jaringan harus maksimal dalam mendesain topologi, karena kabel yang dibutuhkan banyak untuk membuat topologi ini.
- Sering terjadi tabrakan file data (*collision*).



Gambar 3.1 Desain Model Topologi Hierarki (Rifan, 2011)

Topologi hierarki membantu dalam mengembangkan topologi jaringan di lapisan yang terpisah. Setiap lapisan memiliki fungsi tertentu, memungkinkan penulis untuk memilih peralatan yang tepat guna merancang sistem jaringan pada simulasi autentikasi hierarki di radius LDAP. Sebagai contoh, pada **Gambar 3.1** *router* yang dimiliki setiap organisasi, posisinya berada di bawah *router* yang menghubungkan bangunan di setiap organisasi. *Switch* dan *hub* menghubungkan perangkat pengguna dan server dalam satu bangunan. Dari tiga lapisan yang dimiliki model topologi hierarki, pada lapisan akses menghubungkan pengguna melalui *hub*, *bridge*, *switch*, atau *router*.

Berbagai komponen yang dibutuhkan untuk penelitian ini mencakup;

a. Spesifikasi *Software*

No	<i>Software</i>	Keterangan
1.	Linux 32 bit	Sistem Operasi untuk radius server pada <i>Zeroshell</i>
2.	Windows 10 Pro	Sistem Operasi yang digunakan penulis dalam melakukan penelitian.
3.	Android	Sistem Operasi untuk <i>smartphone</i> guna menunjang pengujian sistem saat simulasi.
4.	Google Chrome	<i>Web Browser</i> untuk melakukan manajemen sistem
5.	VirtualBox	Versi 5.0.10 r104061, mesin virtual yang terdapat di VirtualBox digunakan untuk menginstalasi <i>zeroshell</i> sebagai radius server.

6.	GNS3	GNS3 versi 1.3.10, sistem yang telah dirancang akan di simulasikan melalui <i>Network Emulator</i> GNS3.
----	------	--

Tabel 3.1 Tabel Spesifikasi *Software*

b. Spesifikasi *Hardware*

No	Perangkat	Jumlah	Spesifikasi Unit
1.	Access Point	1	TP-LINK 3G/3.75 G Wireless Line N Router Model No: TL-MR3220
2.	Kabel LAN	1	Straight UTP
3.	Laptop Dell Inspiron 14 3000 series	1	Operasi Sistem: Windows 10 Pro 64-bit Processor: Intel Core i5-4210U 1.7GHz RAM: 4.00 GB VGA: NVIDIA GEFORCE
4.	Smartphone	Tidak terbatas	Sistem operasi berbasis android dan mendukung perangkat wireless.
5.	Router Cisco C3725 series	2	Router Internet memiliki 4 interface Fast Ethernet. Router R_UII memiliki 2 interface Fast Ethernet
6.	Ethernet Switch	1	3 port Fast Ethernet
7.	Radius Server	4	Sistem operasi: Linux 32 bit, open source yang digunakan adalah zeroshell

Tabel 3.2 Tabel Spesifikasi *Hardware*

3.5 Persiapan Tools

Beberapa *tools* yang perlu dijelaskan yaitu:

1. *Access Point*

Access point adalah sebuah perangkat jaringan yang berisi sebuah *transceiver* dan antena untuk transmisi dan menerima sinyal ke dan dari *clients remote*. Dengan *access points* (AP) *clients wireless* dapat dengan cepat dan mudah untuk terhubung ke jaringan LAN secara *wireless*. AP harus terhubung dengan adaptor karena merupakan sumber daya untuk *access point*.

2. Kabel LAN

Kabel LAN merupakan media transmisi *ethernet* yang menghubungkan piranti-piranti jaringan dalam jaringan komputer satu lokasi.

3. Laptop dan *Smartphone*

Diperlukan perangkat keras seperti laptop dan *smartphone* untuk menjalankan aplikasi yang telah ditentukan dalam penelitian ini dan membantu keberhasilan proses autentikasi *user* baik dalam konfigurasi maupun pengujian sistem.

4. *Software*

Software adalah program yang berisi instruksi/perintah sebagai perantara yang menghubungkan antara *hardware* dan *brainware* (perangkat manusia) sehingga dapat menghasilkan informasi yang diinginkan *brainware*.

3.6 Persiapan *Simulasi*

1. *Access Point*

Access point yang berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak *Client* dapat saling terhubung melalui jaringan (*Network*). Sebagai *Hub/Switch* yang bertindak untuk menghubungkan jaringan lokal dengan jaringan *wireless/nirkabel*, pada *access point* inilah koneksi data/internet dipancarkan atau dikirim melalui gelombang radio, ukuran kekuatan sinyal juga mempengaruhi area *coverage* yang akan dijangkau, semakin besar kekuatan sinyal (ukurannya dalam satuan dBm atau mW) semakin luas jangkauannya.

2. Kabel LAN

Kabel UTP yang digunakan sebagai kabel jaringan LAN (*Local Area Network*) pada sistem jaringan komputer. Dalam pemakaian sehari-hari, kabel UTP sudah sangat baik digunakan sebagai kabel jaringan komputer misalnya dalam kegunaan ruang kantor atau dalam sistem jaringan suatu perusahaan.

3. Laptop

Laptop adalah perangkat utama yang sangat bermanfaat untuk membantu penulis melakukan konfigurasi. Tanpa perangkat laptop, segala konfigurasi pada *software* yang telah ditentukan tidak akan dapat terlaksana.

4. Zeroshell

Zeroshell adalah salah satu distribusi Linux untuk server dan perangkat embedded ditujukan untuk memberikan layanan jaringan terutama LAN. *Zeroshell* tersedia dalam bentuk Live CD atau gambar *Compact Flash*, dan mesin VirtualBox. Tidak perlu menggunakan *shell* untuk mengelola dan mengkonfigurasinya, tetapi melalui tampilan *interface* web GUI di *web browser*.

Berikut adalah fitur utama dari distribusi *Linux Zeroshell* (Ricciardi, 2005) ;

- a. Radius Server mampu menyediakan autentikasi yang aman yaitu pada jaringan yang mendukung IEEE 802.1X dalam bentuk protokol EAP-TTLS dan *Wi - Fi Protected Access (WPA/WPA2)*.
- b. *Captive portal* untuk autentikasi jaringan *wireless* menggunakan *web browser Zeroshell* yang bertindak sebagai *gateway*. *Client* yang akan mengakses jaringan harus mengautentikasi sendiri melalui *web browser* menggunakan Kerberos 5 *username* dan *password*.
- c. *Firewall Packet Filter* dan *Stateful Packet Inspection (SPI)* dengan filter yang berlaku di kedua *routing* dan menjembatani pada semua jenis *interface* termasuk VPN dan VLAN;
- d. QoS (*Quality of Service*) manajemen dan membentuk lalu lintas untuk mengontrol lalu lintas jaringan yang padat dan beberapa jenis lalu lintas seperti VoIP dan *peer-to -peer*.
- e. VPN host-to-LAN dan LAN-to-LAN dengan protokol IPSec/L2TP dan OpenVPN.
- f. *Routing* dan *Bridging* memiliki kemampuan VLAN dengan berdasar pada protokol IEEE 802.1Q .
- g. Multizone DNS (*Domain Name System*) Server.
- h. Multi subnet DHCP Server .

- i. PPPoE *client* untuk koneksi ke WAN (*Wide Area Network*) melalui ADSL , DSL dan kabel baris.
- j. Updater DNS *client* dinamis untuk DynDNS.
- k. NTP (*Network Time Protocol*) *client* dan server.
- l. Syslog server untuk menerima dan katalogisasi sistem log yang dihasilkan oleh *remote host*.
- m. Kerberos 5 autentikasi.
- n. LDAP server.
- o. Otoritas sertifikasi X.509

5. VirtualBox

Merupakan sebuah perangkat lunak virtualisasi diciptakan oleh *Oracle Corporation*, yang dapat digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama". Fungsi ini sangat penting jika seseorang ingin melakukan uji coba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada atau kehilangan sistem utama. Sistem operasi yang dapat menjalankannya antara lain Linux, Mac OS X, Windows XP, Windows Vista, Windows 7, Windows 8, Solaris, dan OpenSolaris.

6. GNS3

GNS3 adalah *network emulator* berbasis GUI yang mirip dengan Cisco Packet Tracer untuk membangun, mendesain, dan menguji sebuah jaringan telekomunikasi dari berbagai ukuran tanpa perlu *hardware*. Pada GNS3 memungkinkan simulasi jaringan yang lebih bagus daripada *network simulator* dari yang pernah ada karena menggunakan operasi sistem asli dari perangkat jaringan seperti cisco dan juniper, sehingga seperti berada dalam kondisi yang lebih nyata saat melakukan konfigurasi *router*. GNS3 sangat berbeda dengan *network simulator* Cisco Packet Tracer.

7. Smartphone

Dalam penelitian ini *smartphone* digunakan sebagai alat bantu untuk terhubung ke jaringan Wi-Fi dan memastikan bahwa proses autentikasi berhasil atau tidak.

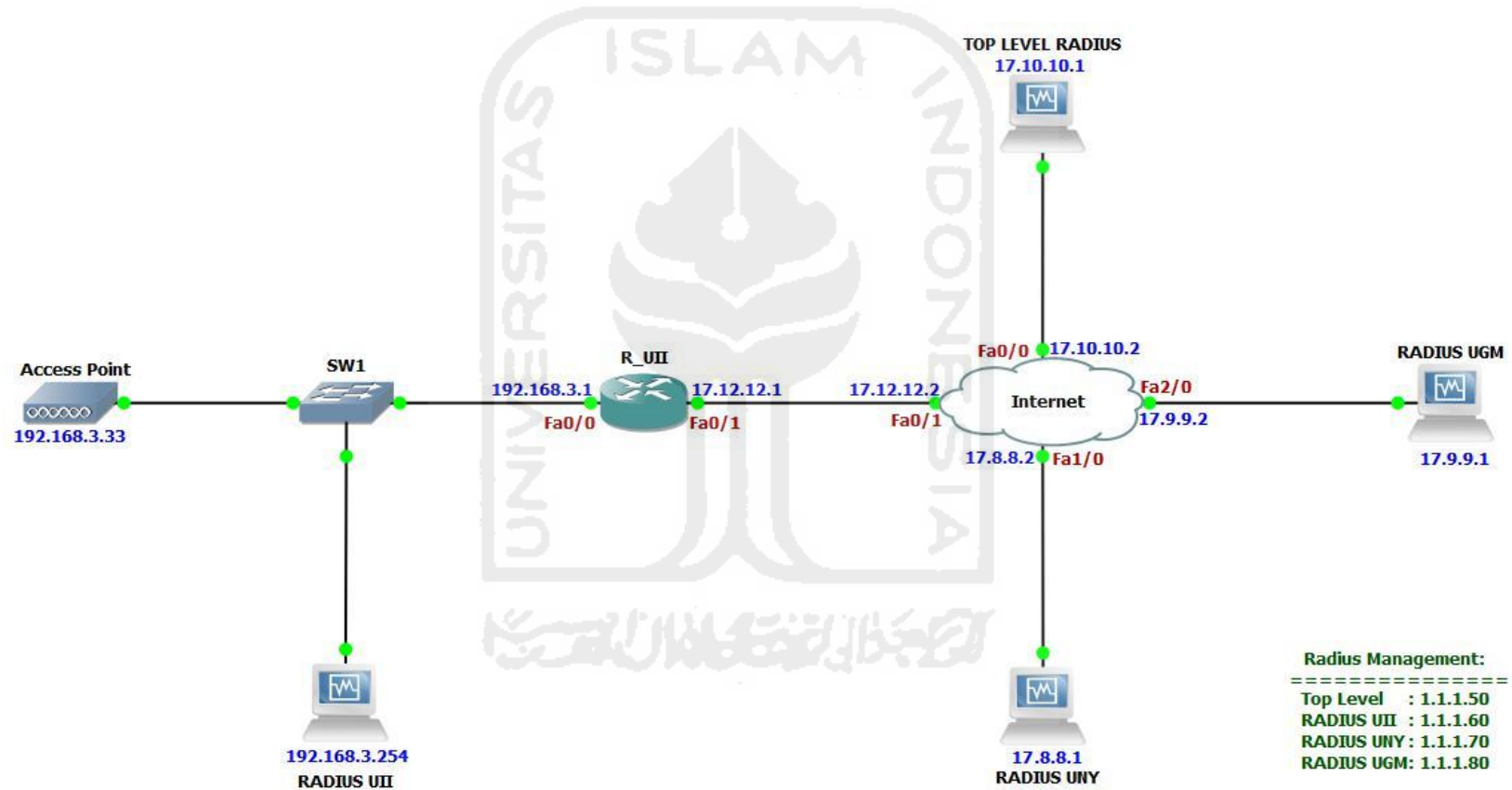
8. Browser

Merupakan aplikasi yang digunakan untuk mengoperasikan internet, terutama sebagai media untuk melakukan *browsing*, *surfing*, dan melakukan aktivitas di dunia maya lainnya. *Browser* adalah perangkat lunak yang berfungsi menampilkan dan melakukan interaksi dengan dokumen-dokumen yang disediakan oleh *server*.



3.7 Perancangan Topologi Menggunakan Network Emulator GNS3

3.7.1 Topologi



Gambar 3.2 Topologi

Pada tahap ini, penulis menentukan topologi untuk simulasi autentikasi hierarki di radius LDAP. Keterangan dari topologi pada **Gambar 3.2** adalah sebagai berikut:

1. Jenis topologi yang diterapkan adalah mode jaringan *wireless* infrastruktur.
2. Seluruh alamat IP radius server untuk *interface* adapter 2 (ETH01) menggunakan IP *address* kelas A, terkecuali Radius UII dan *access point* menggunakan alamat IP kelas C dengan *subnet mask* 255.255.255.0 atau /24 secara keseluruhan.
3. Pada segmen jaringan terdapat beberapa *device* yaitu 1 buah *access point*, 4 buah radius server (Radius UII, Radius UNY, Radius UGM, dan Radius Top Level), 2 buah *router* (Internet, R_UII), dan 1 buah *switch*.
4. Alamat IP pada radius manajemen menggunakan kelas A untuk *interface* adapter 1 (ETH00).

Berikut adalah tabel rancangan IP *address* untuk topologi jaringan pada **Gambar 3.2**:

No.	Nama	IP Address	SubnetMask	Gateway
1.	<i>Access Point</i>	192.168.3.3	255.255.255.0	-
IP Radius Server, Interface ETH01				
2.	Radius UII	192.168.3.254	255.255.255.0	192.168.3.1
3.	Radius UNY	17.8.8.1	255.255.255.0	17.8.8.2
4.	Radius Top Level	17.10.10.1	255.255.255.0	17.10.10.2
5.	Radius UGM	17.9.9.1	255.255.255.0	17.9.9.2
IP Radius Manajemen, Interface ETH00				
6.	Radius UNY	1.1.1.70	255.255.255.0	-
7.	Radius Top Level	1.1.1.50	255.255.255.0	-
8.	Radius UGM	1.1.1.80	255.255.255.0	-
9.	Radius UII	1.1.1.60	255.255.255.0	-

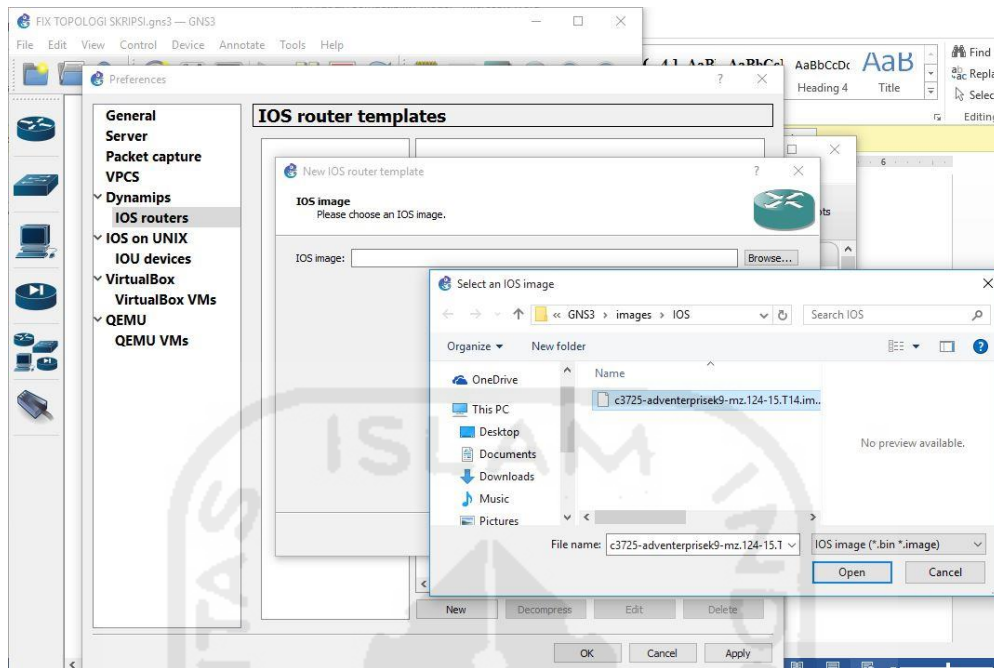
Tabel 3.3 Rancangan IP Address

Wireless access point dengan SSID “UII” berada pada satu *network* dengan Radius UII yaitu 192.168.3.0, karena posisi AP terletak di UII. Radius Top Level dalam hal ini adalah radius server yang berfungsi mengirimkan *credentials user* ke masing-masing radius server keorganisasiannya ketika *realm* telah terdefinisi.

Proses dari topologi simulasi ini yaitu ketika seorang *user* dari UNY maupun UGM menginginkan akses internet saat berkunjung ke UII mereka harus mencari signal Wi-Fi dengan SSID “UII”. Sebelum diijinkan untuk mengakses internet, mereka harus melalui proses autentikasi terlebih dahulu dengan memberikan informasi yaitu *username* dan *password* dengan syarat *username* harus menggunakan *realm* sesuai universitas asal. Saat login, server lokal akan mendeteksi *realm* yang dimasukkan oleh *user* misalnya *realm @ugm.ac.id* kemudian akan dikirimkan ke radius server Top Level. Tugas Top Level kemudian mengirim *credentials* tersebut ke server universitas yang telah terdeteksi *realm*-nya. Database LDAP yang terdapat pada masing-masing server radius bertugas mengecek apakah *credentials* dimasukkan dengan benar atau tidak, jika benar maka proses autentikasi berhasil. Proses selanjutnya dikirim kembali ke server lokal dan *user* diijinkan untuk mengakses internet. Namun sebaliknya jika *user* salah memasukkan *credentials*, maka proses autentikasi gagal *user* pun tidak diberikan hak akses internet.

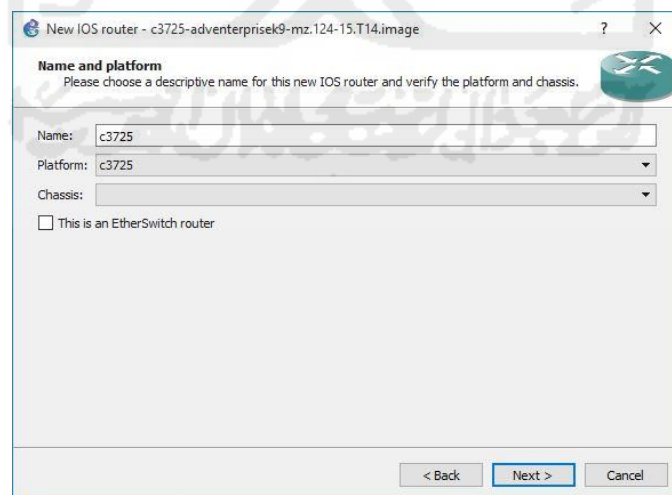
3.7.2 Perancangan Topologi

Aplikasi GNS3 yang telah di install akan digunakan untuk merancang topologi dalam penelitian ini. Beberapa *device* dari GNS3 akan ditambahkan sesuai skema jaringan pada **Gambar 3.2**. Langkah konfigurasi *device* yang akan ditambahkan pada halaman kerja GNS3 ditunjukkan pada **Gambar 3.3 - Gambar 3.7**, antara lain :

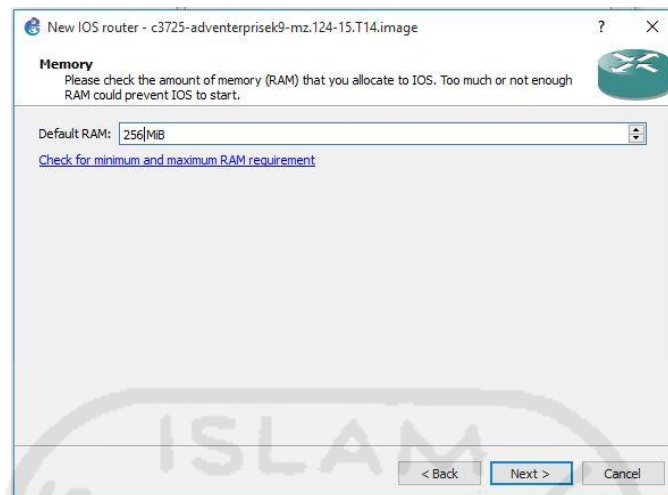


Gambar 3.3 Menambahkan Router di GNS3

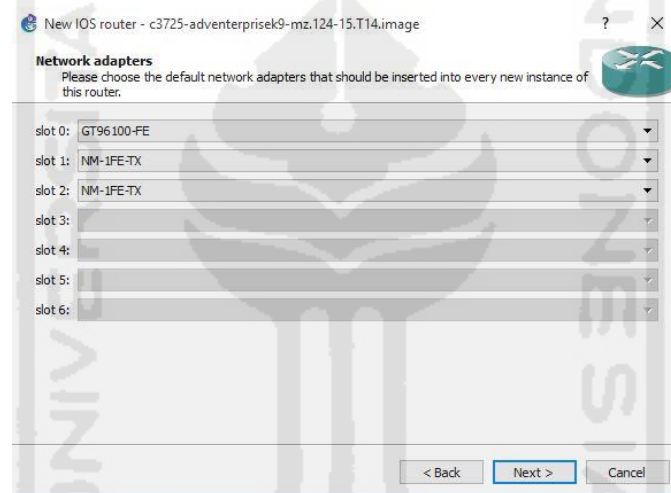
Kemudian untuk konfigurasi selanjutnya dapat dilihat pada **Gambar 3.4** sampai dengan **Gambar 3.8** yaitu memberi nama dan menentukan *platform* yang digunakan *router*, menentukan ukuran *default memory* RAM, *Network Adapter*, *default WIC* Modules, dan ukuran pada Idle-PC.



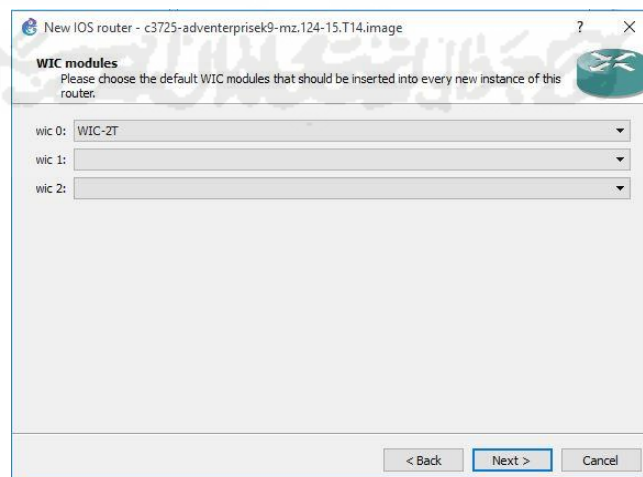
Gambar 3.4 Name dan Platform Router



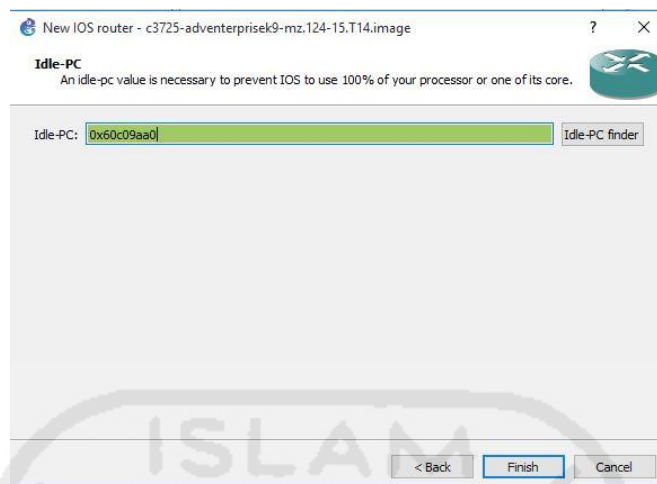
Gambar 3.5 Menentukan *Default RAM*



Gambar 3.6 Menentukan Network Adapter *Router C3725*



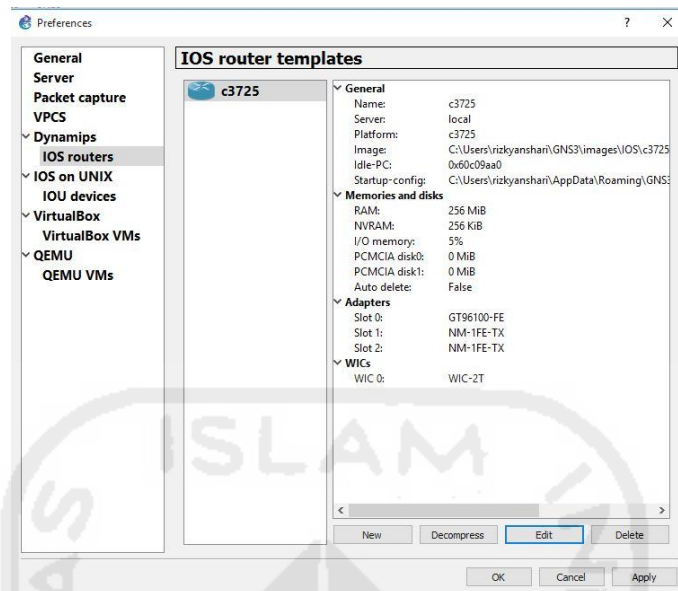
Gambar 3.7 Menentukan WIC Modules Pada *Router C3725*



Gambar 3.8 Idle-PC Untuk *Router* Cisco

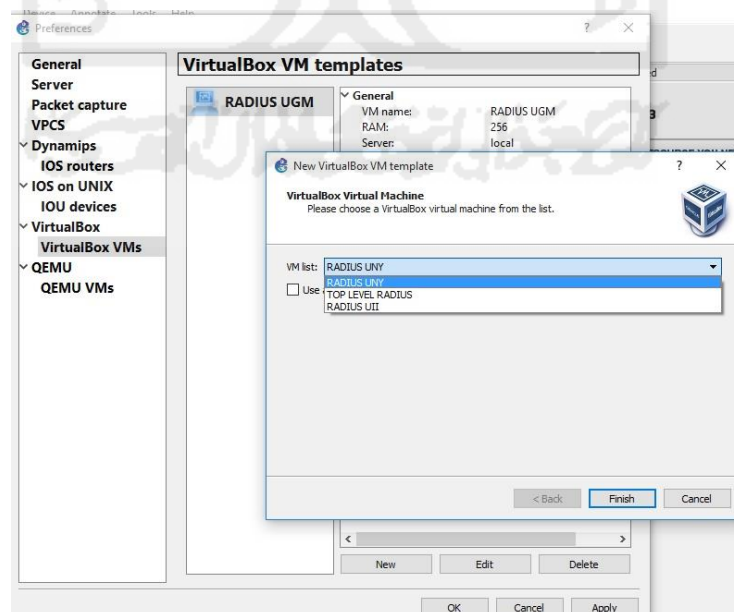
Untuk menambahkan *router* cisco *download* terlebih dahulu salah satu IOS Cisco yaitu IOS *Image* c3725-adventerprise9-mz.124-15.T14.image. Registrasikan *image* tersebut pada menu Edit->Preferences->Dynamips->IOS *router*->New untuk menambahkan IOS *image* yang disesuaikan dengan *platform router* IOS-nya. Kali ini yang digunakan pada topologi yaitu *Router* C3725 menggunakan *platform* C3725 *series*.

Selanjutnya, perlu ditentukan ukuran RAM seperti pada **Gambar 3.5** sebesar 256 MiB. Kemudian slot pada *router* untuk jenis *interface* diatur dengan *Ethernet*, *FastEthernet*, maupun *serial*. **Gambar 3.8** adalah menentukan ukuran Idle-PC untuk *router* karena ketika IOS berjalan, proses yang terjadi menggunakan CPU bisa mencapai 100%. Hal ini akan sangat memberatkan laptop apabila jaringan yang akan disimulasikan lebih banyak. Oleh karena itu, GNS3 menyediakan fitur Idle-PC yang akan mengurangi pemrosesan di laptop dengan konsep membuat *router* menjadi *sleep/hibernate* kemudian akan aktif bila dilakukan konfigurasi. Setelah selesai sebagaimana ditunjukkan pada **Gambar 3.9** terdapat informasi lengkap *router* Cisco yang baru saja ditambahkan.

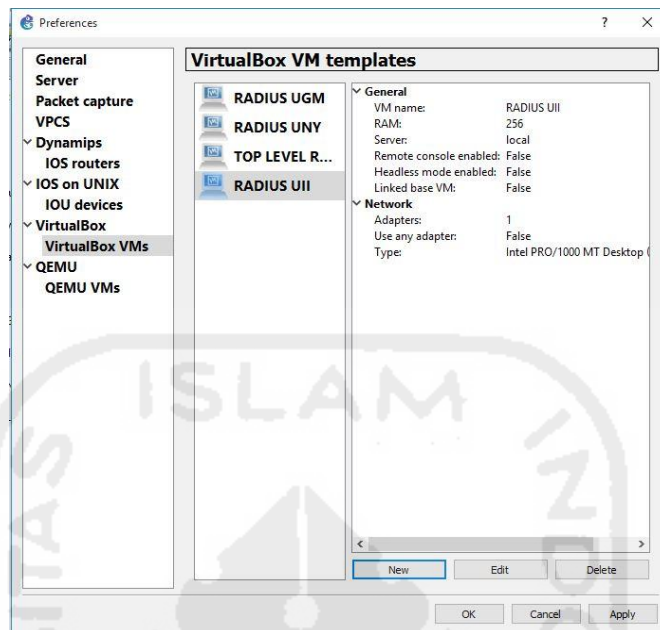


Gambar 3.9 Informasi Lengkap Router Cisco yang Ditambahkan

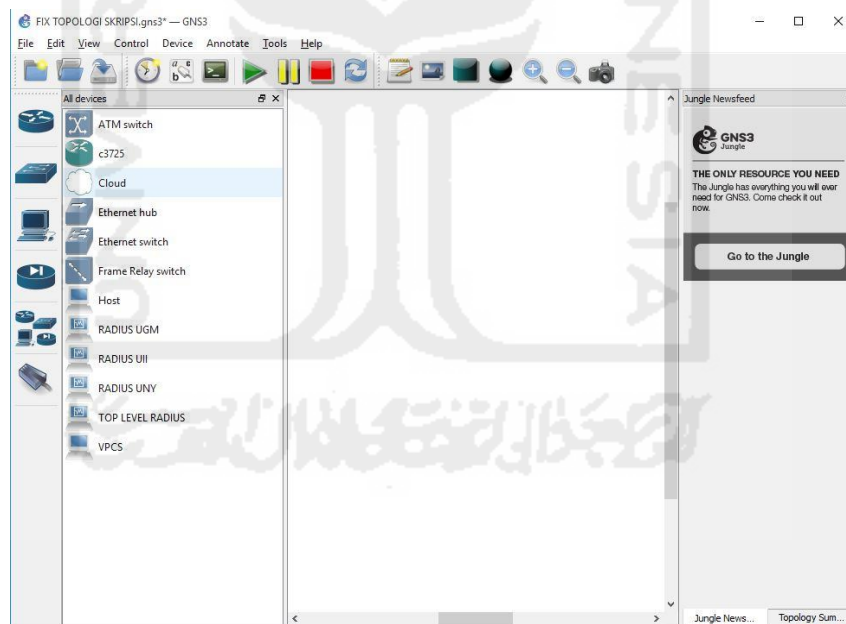
Gambar 3.10 - Gambar 3.11 mengintegrasikan mesin virtual yang telah dibuat di VirtualBox dengan GNS3 pada menu Edit->Preferences->VirtualBox VMs -> New, dan integrasikan semua radius server di Virtualbox pada kolom VM List. Hasil penjelasan terhadap **Gambar 3.10** adalah semua mesin virtual yang ada di dalam VirtualBox terdeteksi pada kolom “VM List”, setelah keempat radius server ditambahkan maka seluruhnya akan tampil di “VirtualBox VM Templates” yang terdapat pada menu VirtualBox->Virtual VMs.



Gambar 3.10 Mengintegrasikan Mesin Virtual di VirtualBox dengan GNS3

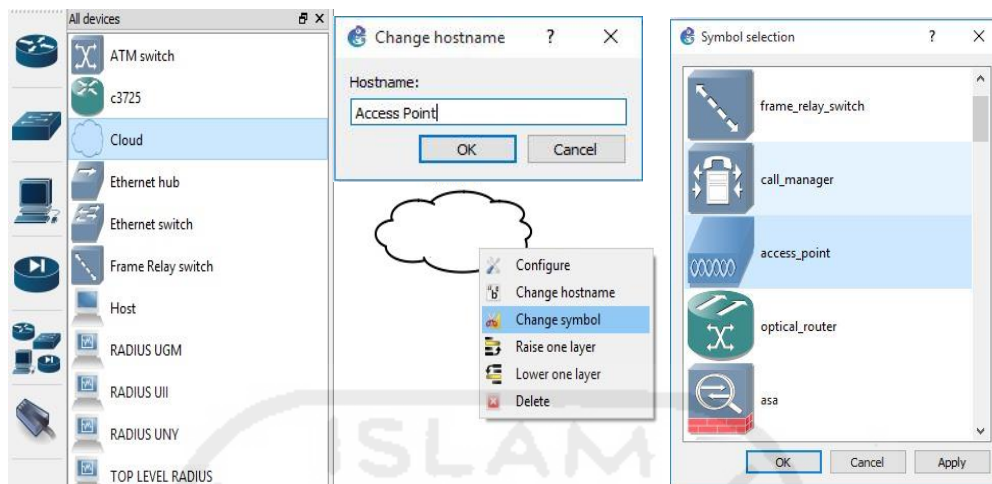


Gambar 3.11 Keempat *Guest* Radius Server di GNS3



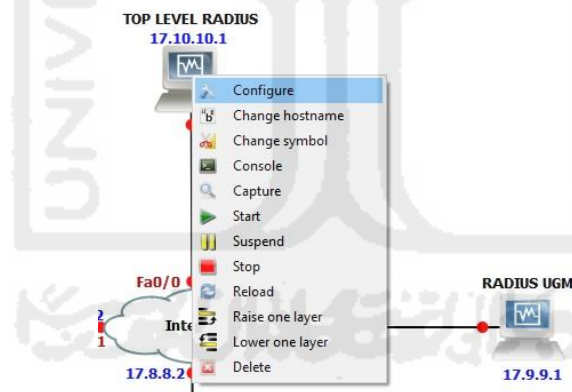
Gambar 3.12 Toolbar *All Devices* yang Telah Ditambahkan

Setelah semua *device* telah ditambahkan seperti pada **Gambar 3.12** selanjutnya simulasikan dengan mendrag *device* yang dibutuhkan sesuai topologi ke dalam halaman kerja GNS3.



Gambar 3.13 *Change symbol device*

Gambar 3.13 menunjukkan *device* “cloud” yang ingin dirubah simbolnya menjadi *access point*. Merubah simbol pada *object cloud* dengan memilih opsi “*change symbol*” lalu pilih *access point*. Opsi “*change hostname*” berfungsi untuk merubah nama *device* sesuai skema jaringan yang telah dibuat.

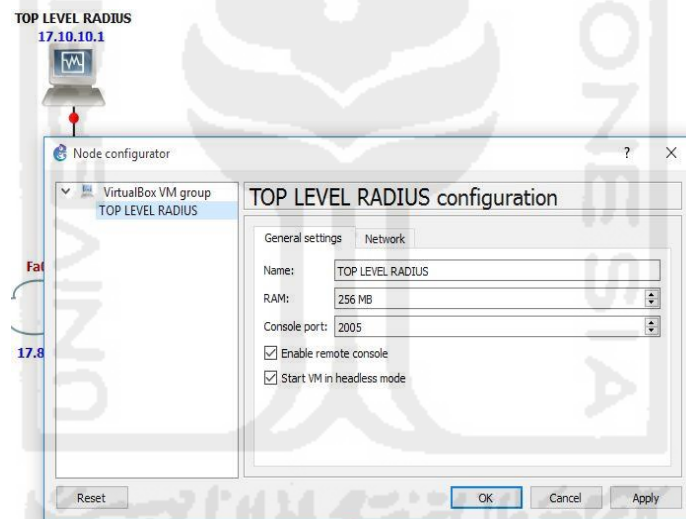


Gambar 3.14 *Konfigurasi Device*

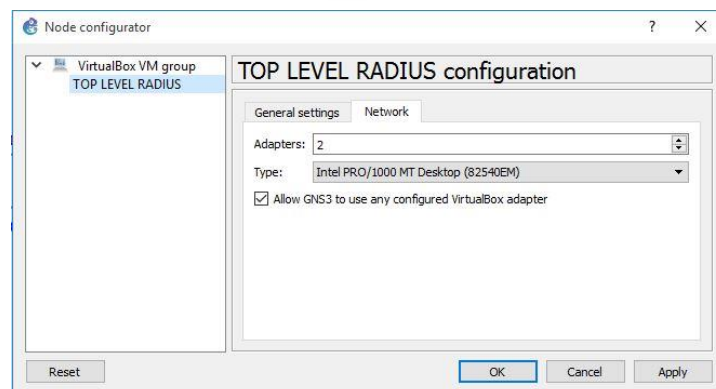
Hubungkan semua *device* yang telah diletakkan di halaman kerja GNS3 untuk dikoneksikan satu sama lain dengan menggunakan toolbar “*Add a link*”. Pada saat awal semua *device* terhubung, simbol sambungan kabel masih berwarna merah. Setelah simbol *start/play* diklik pada menu toolbar GNS3, semua *device* yang terhubung akan aktif dan sambungan kabel berubah warna menjadi hijau.

Khusus untuk *guest* VirtualBox sebelum menghubungkan antar radius server menggunakan *link* sebelumnya tentukan terlebih dahulu jumlah *interface* (NIC) untuk masing-masing mesin virtual. Dengan memilih opsi “*configure*” seperti **Gambar 3.14** di masing-masing *guest* VirtualBox, kemudian atur jumlah *interface* yang akan digunakan di kolom “*Adapters*” pada sub menu “*network*” kemudian pilih “2” untuk 2 buah *interface FastEthernet*.

Pastikan “*Enable remote console, Start VM in headless mode, dan Allow GNS3 to use any configured virtualbox adapters*” dalam keadaan aktif seperti pada **Gambar 3.15** dan **Gambar 3.16**, agar *console* di setiap *device* dapat berjalan dan memungkinkan GNS3 menggunakan semua konfigurasi adapter pada VirtualBox serta mengaktifkan semua mesin virtual secara otomatis tanpa membuka aplikasi VirtualBox.

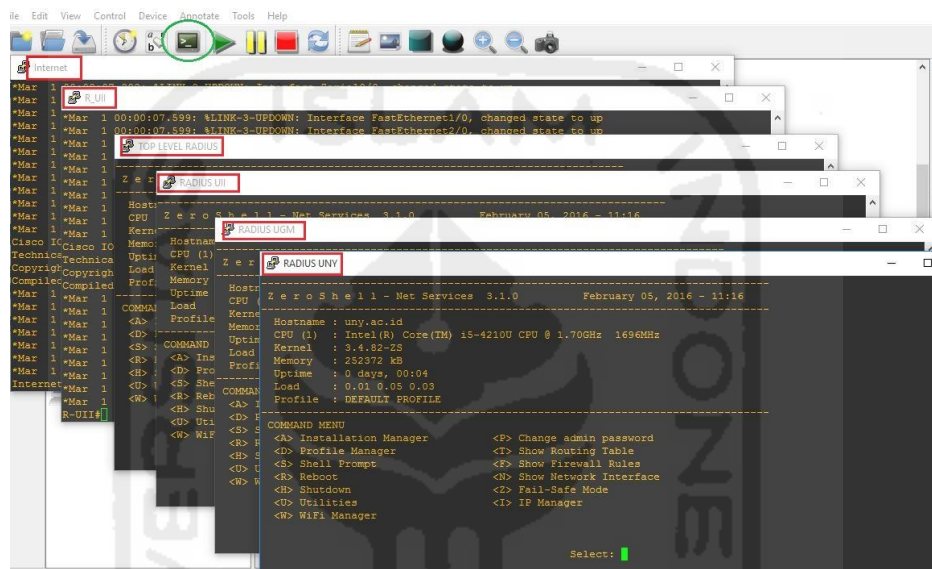


Gambar 3.15 Konfigurasi *Device* Radius Top Level



Gambar 3.16 Konfigurasi *Network* Adapter Radius Top Level

Simbol *console* (tanda *elips* berwarna hijau) pada toolbar GNS3 akan memunculkan terminal/*console* berupa CLI (*Comman Line Interface*) yaitu *text interface* setiap *device* yang telah ditambahkan di halaman kerja GNS3 berupa dua buah router dan empat radius server seperti **Gambar 3.17**. Namun sebelum menjalankan *console*, pastikan terlebih dahulu mengaktifkan semua *device* dan kabel tersambung dengan baik.



Gambar 3.17 Console All Device

```

R1#
R1#conf t 1
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hos
R1(config)#hostname Internet 2
Internet(config)#int f0/0
Internet(config-if)#ip address 17.10.10.2 255.255.255.0 3
Internet(config-if)#no sh 4
Internet(config-if)#
*Mar 1 00:01:44.015: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:01:45.015: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Internet(config-if)#int f0/1 5
Internet(config-if)#ip address 17.12.12.2 255.255.255.0 6
Internet(config-if)#no sh 7
Internet(config-if)#
*Mar 1 00:02:13.239: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 00:02:14.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Internet(config-if)#int f1/0 8
Internet(config-if)#ip address 17.9.9.2 255.255.255.0 9
Internet(config-if)#no sh 10
Internet(config-if)#int
*Mar 1 00:03:33.851: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 1 00:03:34.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
Internet(config-if)#int f2/0 11
Internet(config-if)#ip address 17.8.8.2 255.255.255.0 12
Internet(config-if)#no sh 13
Internet(config-if)#
*Mar 1 00:04:51.207: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Mar 1 00:04:52.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
Internet(config-if)#exit 14
Internet(config)#ip for
Internet(config)#ip forward-protocol n
Internet(config)#ip forward-protocol nd 15
Internet(config)#ip route 0.0.0.0 0.0.0.0 17.12.12.1 16
Internet(config)#exit 17
Internet#
*Mar 1 00:09:53.635: %SYS-5-CONFIG_I: Configured from console by console
Internet#copy run
Internet#copy running-config st
Internet#copy running-config startup-config 18
Destination filename [startup-config]? enter
Building configuration...
[OK]
Internet#

```

Gambar 3.18 Konfigurasi Interface "Internet"

Gambar 3.18 menunjukkan *console* untuk melakukan konfigurasi pada *device* Internet. R1# berada pada modus *privilege EXEC*, maka untuk beralih ke modus *global configuration* diperlukan perintah seperti berikut ini;

a. R1#Conf t atau

R1#Config terminal

Beberapa konfigurasi dasar yang harus dilakukan;

b. R1(config)#hostname Internet

Konfigurasi FastEthernet

c. Internet(config)#interface f0/0

d. Internet(config-if)#ip address 17.10.10.2 255.255.255.0

e. Internet(config-if)#no shutdown

f. Internet(config)#interface f0/1

g. Internet(config-if)#ip address 17.12.12.2 255.255.255.0

h. Internet(config-if)#no shutdown

i. Internet(config)#interface f1/0

j. Internet(config-if)#ip address 17.8.8.2 255.255.255.0

k. Internet(config-if)#no shutdown

l. Internet(config)#interface f2/0

m. Internet(config-if)#ip address 17.9.9.2 255.255.255.0

n. Internet(config-if)#no shutdown

o. Internet(config)#exit

p. Internet(config)#ip forward protocol nd

q. Internet(config)#ip route 0.0.0.0 0.0.0.0 17.12.12.1

r. Internet(config)#exit

s. Internet(config)#copy running-config startup-config

Tekan enter untuk menyimpan konfigurasi.

```

R2
*Mar 1 00:00:11.363: %LINK-5-CHANGED: Interface FastEthernet2/0, changed state to administratively down
R2#conf t 1
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R_UII 2
R_UII(config)#int f0/0 3
R_UII(config-if)#ip address 192.168.3.1 255.255.255.0 4
R_UII(config-if)#no sh 5
R_UII(config-if)#
*Mar 1 00:01:57.895: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:01:58.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to u
R_UII(config-if)#int f0/1 6
R_UII(config-if)#ip address 17.12.12.1 255.255.255.0 7
R_UII(config-if)#no sh 8
R_UII(config-if)#
*Mar 1 00:02:39.491: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 00:02:40.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to u
R_UII(config-if)#exit 9
R_UII(config)#ip for
R_UII(config)#ip forward-protocol nd 10
R_UII(config)#ip route 0.0.0.0 0.0.0.0 17.12.12.2 11
R_UII(config)#exit 12
R_UII#
*Mar 1 00:03:22.307: %SYS-5-CONFIG_I: Configured from console by console
R_UII#cop
R_UII#copy run
R_UII#copy running-config st
R_UII#copy running-config startup-config 13
Destination filename [startup-config]? enter
Building configuration...
[OK]
R_UII#

```

Gambar 3.19 Konfigurasi *Interface* Router “R_UII”

Konfigurasi *console* pada Router “R_UII” langkahnya sama saja dengan konfigurasi *console* Internet, hanya saja menyesuaikan *interface* yang digunakannya. Berikut rincian konfigurasi dari **Gambar 3.19** ;

1. R1#Conf t atau
R1#Config terminal
2. R1(config)#hostname R_UII

Konfigurasi *FastEthernet*

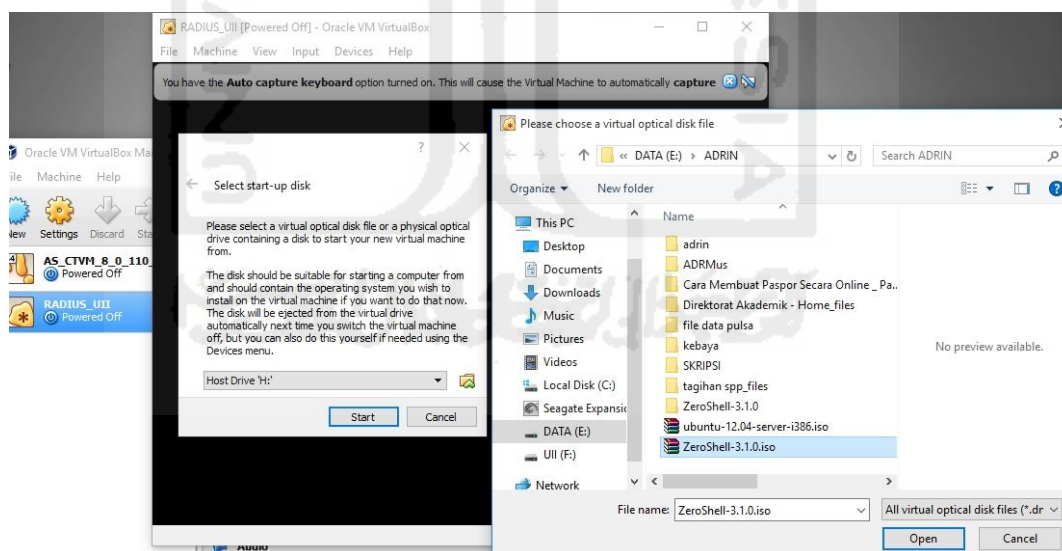
3. R_UII(config)#interface f0/0
4. R_UII(config-if)#ip address 192.168.3.1 255.255.255.0
5. R_UII(config-if)#no shutdown
6. R_UII(config)#interface f0/1
7. R_UII(config-if)#ip address 17.12.12.1 255.255.255.0
8. R_UII(config-if)#no shutdown
9. R_UII(config)#exit
10. R_UII(config)#ip forward protocol nd
11. R_UII(config)#ip route 0.0.0.0 0.0.0.0 17.12.12.2
12. R_UII(config)#exit
13. R_UII(config)#copy running-config startup-config

Tekan enter untuk menyimpan konfigurasi.

3.8 Membuat Virtual Mesin untuk Instalasi Zeroshell

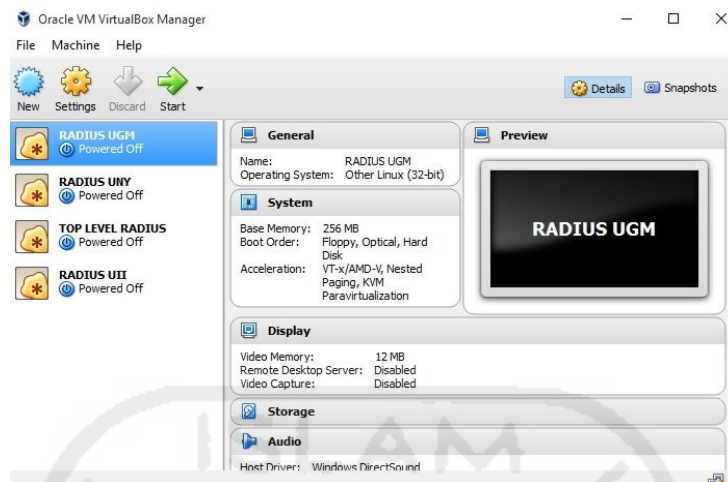
Aplikasi VirtualBox yang di install akan digunakan untuk menambahkan Mesin Virtual (VM). Pada menu *New*->beri nama VM yang baru dan menentukan operasi sistem yang akan diinstall. Selanjutnya ditentukan ukuran *memory* RAM sebesar 256 MB. Ukuran ini sudah cukup untuk menjalankan berbagai macam aktifitas. Untuk membuat mesin virtual ini diperlukan *Virtual hard disk* baru “*Create a virtual hard disk now*” dan VDI adalah format *default* untuk *virtual hard disk*.

Secara *default* *Dynamically allocated* merupakan ukuran *file harddisk* yang tercipta di dalam komputer secara otomatis akan bertambah ketika data yang digunakan bertambah. Jenis *Fixed* akan menciptakan sebuah *file* dengan ukuran maksimum dan tidak akan berubah ukurannya sekalipun tidak menggunakan kapasitas *hard disk* di dalam virtual mesin, namun jenis *virtual hard disk* ini biasanya lebih cepat. Dalam hal ini ukuran alokasi *harddisk* untuk VM Radius UII sebesar 6 GB. Tahap terakhir yaitu menginstall Zeroshell menggunakan *file ISO* Zeroshell 3.1.0.



Gambar 3.20 Instalasi Zeroshell pada Radius UII

Langkah di atas merupakan proses membuat virtual mesin (VM) untuk instalasi Zeroshell sebagai radius server pada Radius UII. Selanjutnya, membuat virtual mesin untuk Radius UGM, Radius UNY, dan Radius Top Level dilakukan dengan langkah yang serupa pada Radius UII.

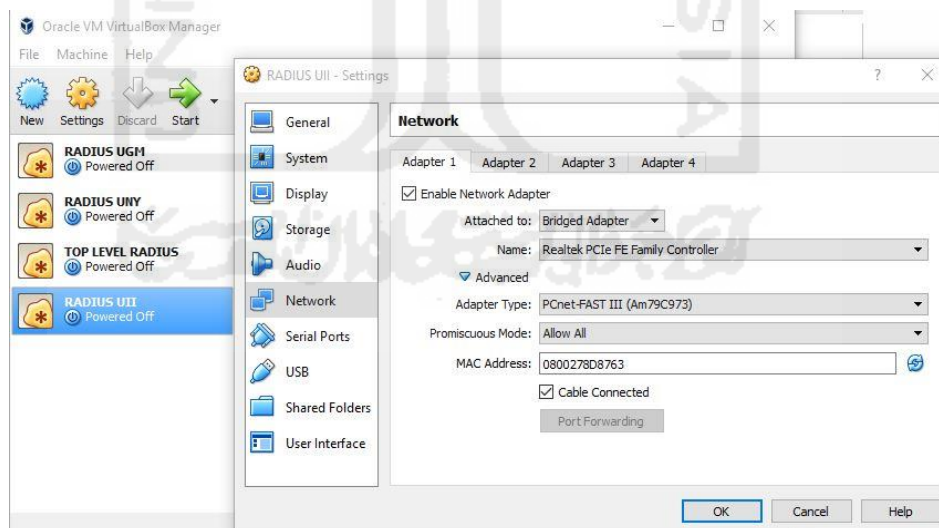


Gambar 3.21 *Virtual Machine Radius Server*

Gambar 3.21 menunjukkan 4 mesin virtual Radius Server yang sudah siap disimulasikan menggunakan GNS3 untuk proses autentikasi secara hierarki.

3.9 Konfigurasi *Interface* Pada Mesin Virtual

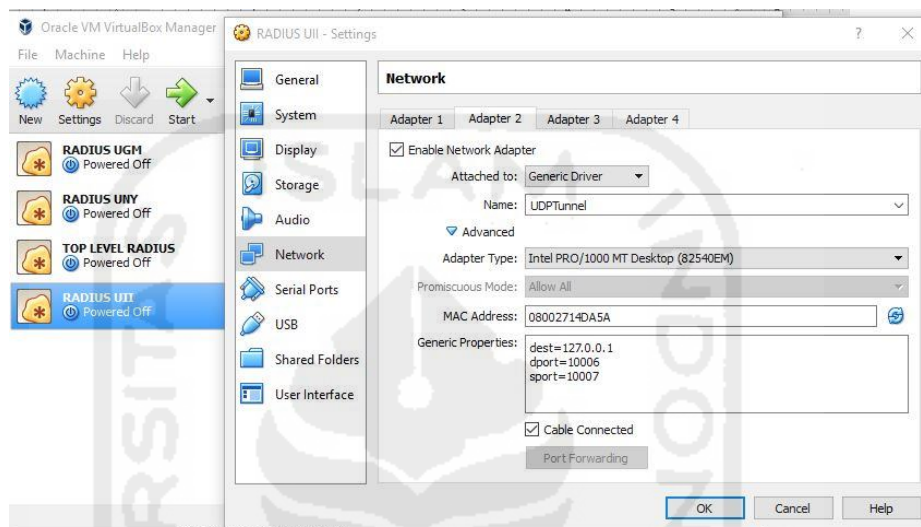
Konfigurasi *interface* untuk setiap mesin virtual pada VirtualBox terletak di bagian *settings* -> *network*. Seperti terlihat pada **Gambar 3.22**.



Gambar 3.22 *Interface Radius UII Adapter 1*

Gambar 3.22 menunjukkan konfigurasi Adapter 1. Opsi “*Bridged Adapter*” dipilih pada kolom *Attached to* dan “*Realtek PCIe FE Family Controller*” adalah

nama adapter fisik yang terdeteksi saat LAN tertanam di Laptop. Kolom *Promiscuous Mode* ditentukan pada opsi “*Allow All*”, kemudian centang “*Enable Network Adapter*” dan “*Cable Connected*” agar adapter 1 tetap aktif. *Bridged adapter* artinya menghubungkan Zeroshell pada mesin virtual dengan adapter fisik yang tertanam pada laptop.



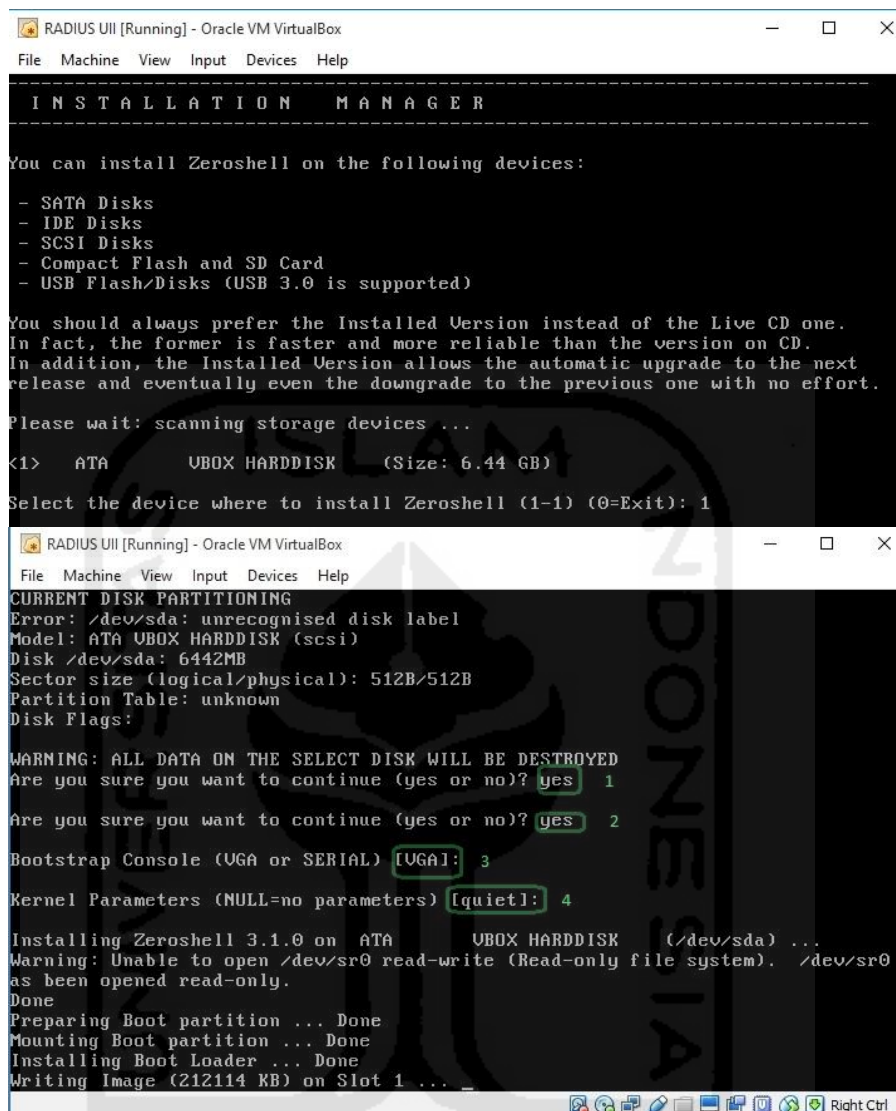
Gambar 3.23 Interface Radius UII Adapter 2

Pada **Gambar 3.23** centang “*Enable Network Adapter*” dan “*Cable Connected*” agar adapter 2 tetap aktif. Ketika VirtualBox dan GNS3 telah terintegrasi maka konfigurasi Adapter 2 secara otomatis akan menyesuaikan.

3.10 Instalasi Zeroshell Sebagai Radius Server

3.10.1 Radius UII

Mesin virtual yang telah dibuat sebelumnya seperti langkah pada bab 4.4, akan dilakukan tahap konfigurasi berikutnya untuk proses autentikasi secara hierarki. Selanjutnya menjelaskan proses instalasi Zeroshell pada Radius UII. Tampilan installasi terlihat seperti **Gambar 3.24 - Gambar 3.27**;



Gambar 3.24 Langkah Instalasi Zeroshell Pada Radius UII (1)

Pada **Gambar 3.24** menampilkan langkah awal instalasi Zeroshell untuk Radius UII. Terlihat dari gambar diberikan pilihan untuk memilih 1 yaitu ATA VBOX HADRDISK (Size 6.44 GB), atau 0 yaitu exit. Dalam hal ini untuk menginstal pilih “1” kemudian langkah berikutnya seperti yang diberi tanda *elips* berwarna hijau, yaitu untuk proses instalasi no.1 sampai no.6 lakukan hal yang serupa di setiap radius server.

```

RADIUS UII [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Preparing Boot partition ... Done
Mounting Boot partition ... Done
Installing Boot Loader ... Done
Writing Image (212114 KB) on Slot 1 ... Done
Preparing Profile Partition ... Done
Do you want to create a configuration profile? [yes]: 5
Profile Description [DEFAULT PROFILE]: 6
Hostname [zeroshell.example.com]: uui.ac.id
Admin Password [zeroshell]: 12345
LDAP Base [dc=example,dc=com]: dc=uui,dc=ac,dc=id
Kerberos 5 REALM [EXAMPLE.COM]: uui.ac.id

<1> ETH00 - Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (rev 40)

Management Interface [1]
IP Address to assign to ETH00 [192.168.0.75]: 1.1.1.60
Netmask [255.0.0.0]:
Default Gateway:

Creating the new Profile ... Done ✓
Activating the Profile (DEFAULT PROFILE) ... Done ✓
Installation process terminated
Press any key to return to the Command Menu...

```

Gambar 3.25 Langkah Instalasi Zeroshell pada Radius UII (2)

Gambar 3.25 adalah langkah selanjutnya untuk melakukan instalasi *Zeroshell*. Tanda *elips* berwarna hijau dan kuning menunjukkan perintah yang harus diketik saat membuat sebuah konfigurasi di dalam *Zeroshell*. Untuk memulai membuat sebuah profil konfigurasi ketik “yes”, kemudian “Default Profile” untuk deskripsi profil. *Hostname* untuk Radius UII adalah “uui.ac.id” dan *password*-nya “12345”. Lalu konfigurasi pada database LDAP yaitu “dc=uui,dc=ac,dc=id” dan konfigurasi untuk *realm*-nya adalah “uui.ac.id”. *Realm* ini harus dibuat karena sangat penting dalam proses autentikasi ketika *user* ingin *login* mendapatkan akses internet. Tanda centang, menandakan konfigurasi instalasi *Zeroshell* untuk Radius UII telah selesai dan *Default Profile* telah diaktifkan.

```

-----
Z e r o S h e l l - N e t S e r v i c e s   3.1.0           September 14, 2015 - 05:12
-----
Hostname : uii.ac.id
CPU (1)  : Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz  1696MHz
Kernel   : 3.4.02-ZS
Memory   : 252372 kB
Uptime   : 0 days, 00:27
Load     : 0.00 0.01 0.05
Profile  : DEFAULT PROFILE
-----

COMMAND MENU
<A> Installation Manager      <P> Change admin password
<D> Profile Manager          <T> Show Routing Table
<S> Shell Prompt             <F> Show Firewall Rules
<R> Reboot                   <N> Show Network Interface
<H> Shutdown                 <Z> Fail-Safe Mode
<U> Utilities                 <I> IP Manager
<W> WiFi Manager
Press Ctrl+C to logout.

Select: _

```

Gambar 3.26 Tampilan Utama pada Zeroshell untuk Radius UII

Setelah konfigurasi instalasi berhasil, tunggu sampai *booting* Zeroshell selesai lalu keluar tampilan seperti **Gambar 3.26** yaitu tampilan awal saat memulai mesin virtual pada Radius UII. *Command Menu* menampilkan pilihan dari banyak menu pada Zeroshell, setiap menu pun masing-masing memiliki fungsi tersendiri. Menu “Profile Manager” adalah untuk melihat informasi profil dari konfigurasi radius server.

```

-----
P R O F I L E   M A N A G E R
-----

<C> Create Profile
<A> Activate Profile
<D> Deactivate Profile
<Q> Quit
>> a

Please wait: scanning storage devices ...

Disk: ATA UBOX HARDDISK
<1> DEFAULT PROFILE (ACTIVE)

Select a profile from the list (1-1): 1

PROFILE INFO
Description      : DEFAULT PROFILE
Last Activation  : Already Active
Hostname         : uii.ac.id
Kerberos 5 Realm : UII.AC.ID
LDAP Base        : dc=uii,dc=ac,dc=id
Last Backup      : Never

NETWORK CONFIGURATION
ETH00 1.1.1.60/255.0.0.0
ETH01 192.168.3.254/255.255.255.0
UPN99 192.168.250.254/255.255.255.0
Default Gateway 192.168.3.1

WARNING: The profile is already active!!!

Press any key to return to the main menu._

```

Gambar 3.27 Profil Manager Radius UII

Gambar 3.27 menampilkan pilihan menu “<A> Activate Profile” yaitu profil konfigurasi yang telah diaktifkan. Setelah itu terdapat menu “*Default Profile*” yang berisi informasi tentang Radius UII dan konfigurasi jaringan di dalamnya.

Tahap instalasi Zeroshell untuk Radius UGM, Radius UNY, dan Radius Top Level dilakukan dengan serupa seperti dijelaskan pada subbab 4.6.1. Namun konfigurasi untuk *Hostname*, *Realm*, *LDAP Base*, dan *network configuration* berbeda di setiap radius server. Oleh karena itu, konfigurasi disesuaikan dengan radius server yang ingin dibuat.

3.10.2 Radius UNY



```

RADIUS UNY [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Please wait: scanning storage devices ...
Disk: ATA UBOX HARDDISK
<1> DEFAULT PROFILE (ACTIVE)

Select a profile from the list (1-1): 1

PROFILE INFO
Description      : DEFAULT PROFILE
Last Activation  : Already Active
Hostname         : uny.ac.id
Kerberos 5 Realm: UNY.AC.ID
LDAP Base        : dc=uny,dc=ac,dc=id
Last Backup      : Never

NETWORK CONFIGURATION
ETH00 1.1.1.70/255.0.0.0
ETH00 vlan 20 not configured
ETH01 17.8.8.1/255.255.255.0
UPN99 192.168.250.254/255.255.255.0
Default Gateway 17.8.8.2

WARNING: The profile is already active!!!
Press any key to return to the main menu.
  
```

Gambar 3.28 Informasi Profil dan Konfigurasi Jaringan Radius UNY

Gambar 3.28 menunjukkan informasi profil dan konfigurasi jaringan dari Radius UNY, dengan rincian sebagai berikut;

```

Hostname           : uny.ac.id
Realm              : UNY.AC.ID
Database LDAP      : dc=uny, dc=ac, dc=id
ETH00              : 1.1.1.70 subnet-mask 255.255.255.0 atau /24
ETH01              : 17.8.8.1 subnet-mask 255.255.255.0 atau /24
Default Gateway    : 17.8.8.2
  
```

3.10.3 Radius UGM

```

RADIUS UGM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
>> a
Please wait: scanning storage devices ...
Disk: ATA UBOX HARDDISK
<1> DEFAULT PROFILE (ACTIVE)
Select a profile from the list (1-1): 1
PROFILE INFO
Description      : DEFAULT PROFILE
Last Activation  : Already Active
Hostname        : ugm.ac.id
Kerberos 5 Realm : UGM.AC.ID
LDAP Base       : dc=ugm,dc=ac,dc=id
Last Backup     : Never
NETWORK CONFIGURATION
ETH00 1.1.1.80/255.0.0.0
ETH01 17.9.9.1/255.255.255.0
UPN99 192.168.250.254/255.255.255.0
Default Gateway 17.9.9.2
WARNING: The profile is already active!!!
Press any key to return to the main menu...

```

Gambar 3.29 Informasi Profil dan Konfigurasi Jaringan Radius UGM

Gambar 3.29 menunjukkan informasi profil dan konfigurasi jaringan Radius UGM, dengan rincian sebagai berikut;

Hostname	: ugm.ac.id
Realm	: UGM.AC.ID
Database LDAP	: dc=ugm, dc=ac, dc=id
ETH00	: 1.1.1.80 subnet-mask 255.255.255.0 atau /24
ETH01	: 17.9.9.1 subnet-mask 255.255.255.0 atau /24
Default Gateway	: 17.9.9.2

3.10.4 Radius Top Level

```

TOP LEVEL RADIUS [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
>> a
Please wait: scanning storage devices ...
Disk: ATA UBOX HARDDISK
<1> DEFAULT PROFILE (ACTIVE)
Select a profile from the list (1-1): 1
PROFILE INFO
Description      : DEFAULT PROFILE
Last Activation  : Already Active
Hostname        : topLevel.ac.id
Kerberos 5 Realm : TOPLEVEL.AC.ID
LDAP Base       : dc=toplevel,dc=ac,dc=id
Last Backup     : Never
NETWORK CONFIGURATION
ETH00 1.1.1.50/255.0.0.0
ETH01 17.10.10.1/255.255.255.0
UPN99 192.168.250.254/255.255.255.0
Default Gateway 17.10.10.2
WARNING: The profile is already active!!!
Press any key to return to the main menu...

```

Gambar 3.30 Informasi Profil dan Konfigurasi Jaringan Radius Top Level

Rincian dari **Gambar 3.30** yaitu Informasi Profil dan Konfigurasi Jaringan Radius Top Level adalah sebagai berikut;

```

Hostname       : toplevel.ac.id
Realm         : TOPLEVEL.AC.ID
Database LDAP  : dc=toplevel, dc=ac, dc=id
ETH00         : 1.1.1.50 subnet-mask 255.255.255.0 atau /24
ETH01         : 17.10.10.1 subnet-mask 255.255.255.0 atau /24
Default Gateway : 17.10.10.2

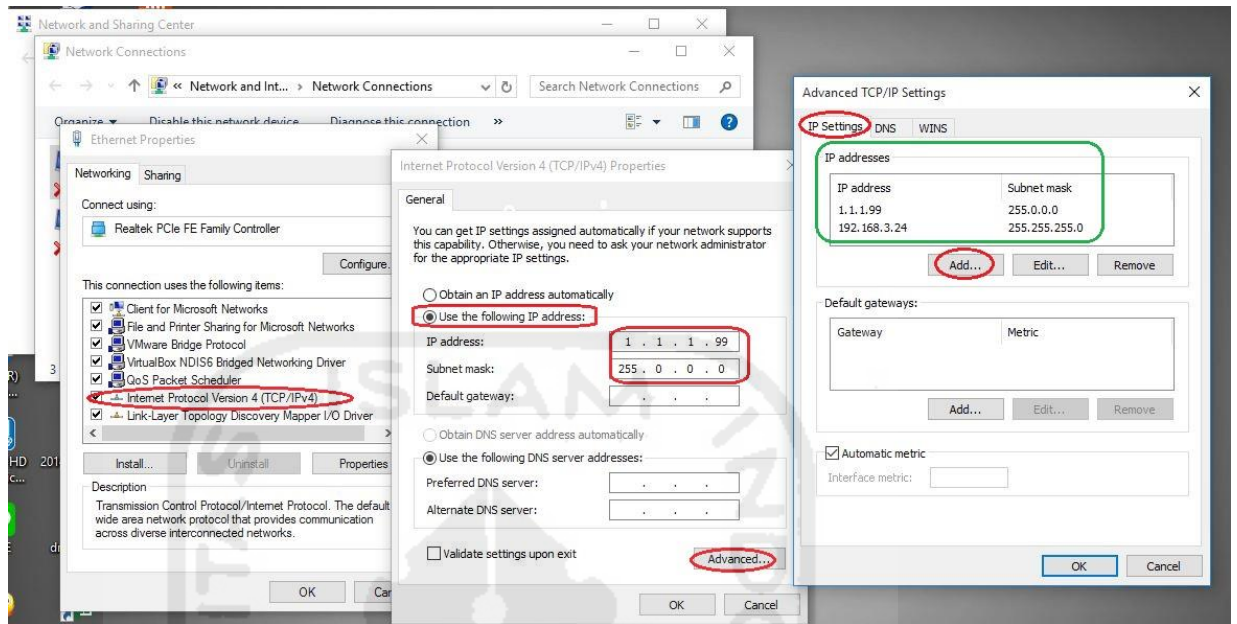
```

3.11 Manajemen Melalui Web Browser

Setelah tahap instalasi selesai, tahap selanjutnya adalah melakukan manajemen radius server melalui web *Interface* dengan mengarahkan web *browser* ke alamat *network* yang digunakan pada *interface* adapter 1 (ETH00) yaitu 1.1.1.0 dan *access point* menggunakan *network* 192.168.3.0. Namun, sebelumnya harus mencocokkan kedua *network* tersebut pada adapter fisik yang tersambung di laptop karena IP nya harus dalam satu *network*.

3.11.1 Konfigurasi Interface Adapter Fisik

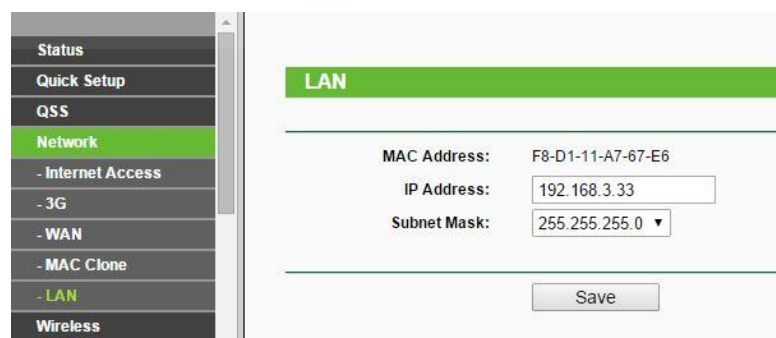
Hubungkan laptop dengan kabel *Ethernet* ke port LAN TP-Link *Access Point*. Lalu tetapkan IP *address* menjadi IP *static* pada laptop yang akan digunakan. Merubah IP *address* laptop menjadi satu *network* dengan alamat IP manajemen radius dan IP pada *access point*. Dengan masuk ke menu *Network and Sharing Center* (ada pada logo komputer di pojok kanan bawah layar)->“*Open Network and Sharing Center*”->“*Ethernet*”->“*Properties*”->“*Internet Protocol Version 4(TCP/IPv4)*”->merubah IP menjadi 1.1.1.99 (IP *host* tidak boleh sama dengan IP radius manajemen). Untuk menambahkan IP yang satu *network* dengan IP *access point*, terdapat pada menu “*advanced*”->“*IP settings*”->“*add*” diisi dengan alamat IP 192.168.3.24 dan *subnet mask* 255.255.255.0”.



Gambar 3.31 Merubah IP Address Interface Adapter Fisik

3.11.2 Access Point

Secara *default*, IP untuk jenis TP-LINK ini adalah 192.168.1.1 dan *netmask* 255.255.255.0. Untuk masuk ke *wireless Router* TP-LINK melalui *web browser* menggunakan alamat IP *default* dari *access point* tersebut, namun pada penelitian ini alamat IP telah dirubah menjadi “192.168.3.3”. Setelah alamat tersebut diketik pada kolom URL, lalu akan muncul sebuah kotak dialog *Authentication Required*. Kotak dialog tersebut menyediakan kolom Nama Pengguna diisi dengan “admin”, dan *password*-nya “admin”.



Gambar 3.32 Merubah Alamat IP Access Point

Gambar 3.32 menunjukkan halaman web *access point* untuk merubah alamat IP *default* yang terdapat pada menu *Network->LAN*. Halaman tersebut menyediakan kolom yang diisi dengan alamat IP yang diinginkan beserta *subnet mask*.

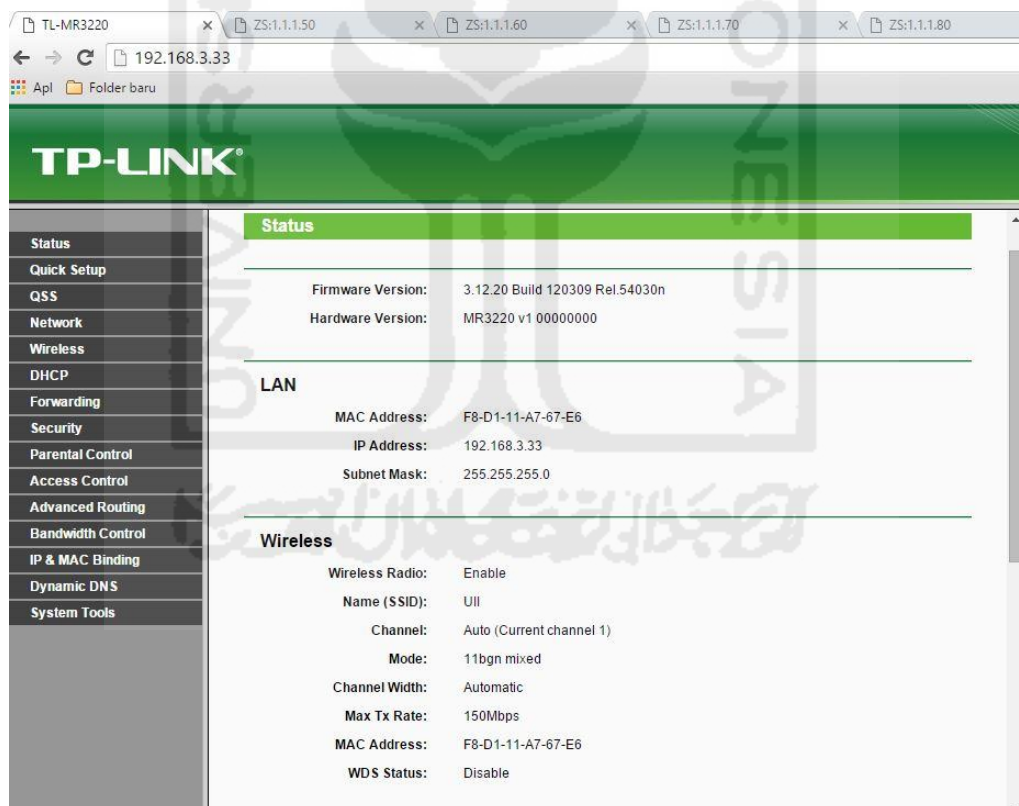
Gambar 3.33 *Wireless Settings*

Pengaturan *wireless* terdapat pada menu *wireless->>wireless settings*. Kolom *wireless network name* diisi dengan “UII” yang akan berfungsi sebagai SSID. *Region* dipilih sesuai lokasi, dan “Auto” untuk *channel*.

Gambar 3.34 *Wireless Security*

Kemudian untuk mengatur keamanan yang akan digunakan autentikasi hierarki di Radius LDAP terdapat pada menu *wireless->wireless security*. Jenis keamanan yang digunakan adalah *version->WPA2 enterprise*, *Encryption->AES*. Kemudian konfigurasi selanjutnya Radius Server IP ->192.168.3.254 (Alamat IP Radius UII), Radius *Port->1812*, Radius *Password->1234567890*, dan *Group Key Update Period->0*.

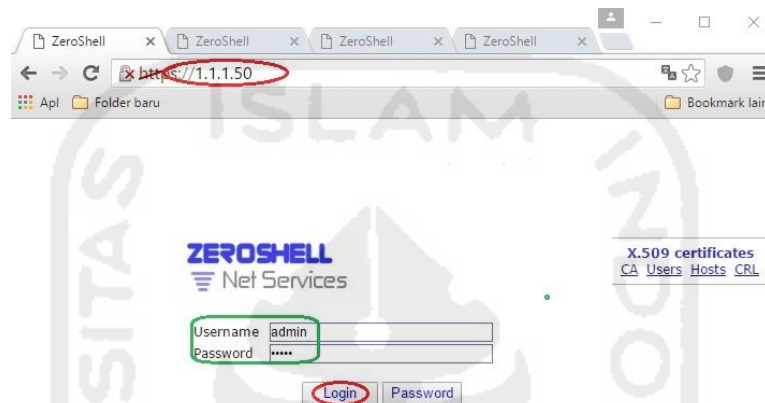
Dalam *access point* pada penelitian ini fungsi DHCP dinonaktifkan karena DHCP akan dikonfigurasi di dalam manajemen radius server. Jika pengaturan *access point* semua telah selesai dikonfigurasi, *reboot system* pada menu *system tools->Reboot*, lalu tunggu sampai *restarting* selesai. Konfigurasi yang telah berhasil akan tampil seperti pada **Gambar 3.35** menu “Status”.



Gambar 3.35 Status konfigurasi *Access Point*

3.11.3 Halaman Login

Memajemen radius server harus masuk ke *web browser* dengan menetik alamat IP manajemen radius server di kolom URL. Pada Radius Top Level alamat IP nya adalah “1.1.1.50”, Radius UII “1.1.1.60”, Radius UNY “1.1.1.70”, dan Radius UGM “1.1.1.80”. Kemudian yang dimasukkan pada kolom *Username* yaitu “admin” dan *password*-nya “12345”.



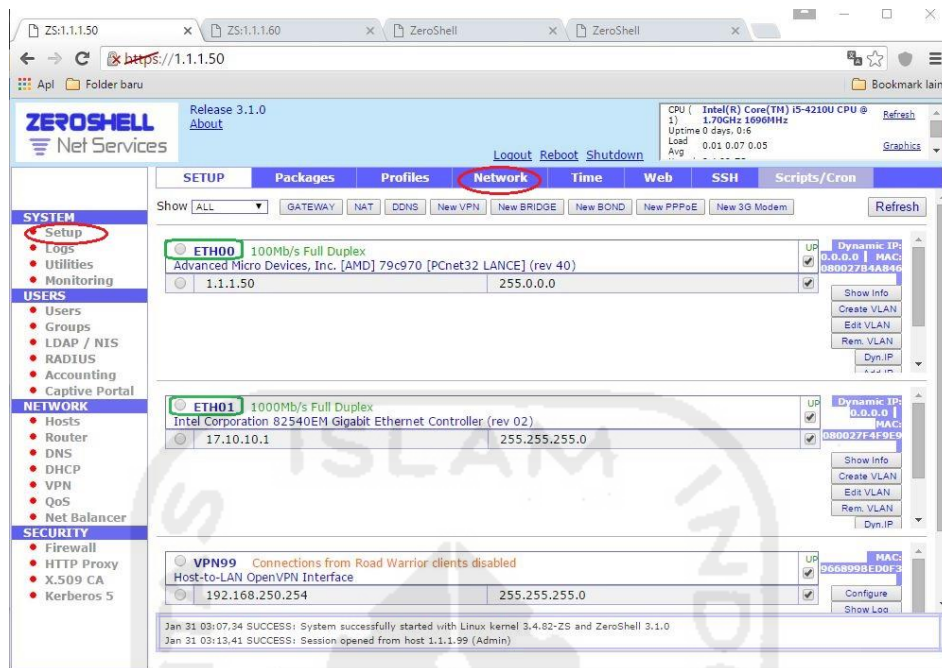
Gambar 3.36 Halaman Login Radius Top Level

3.11.4 Network Radius Server

Setelah masuk halaman login, *browser* akan menampilkan tampilan web *interface* pada ZeroShell. Kemudian pada menu setup->network (tanda *elips* berwarna merah) untuk mengatur jaringan di dalam radius server dan tanda *elips* berwarna hijau merupakan informasi alamat IP kedua *interface* ETH00 dan ETH01. Untuk mengatur alamat IP terdapat pada menu “add ip” dari salah satu *interface*. Namun dahulukan dulu *interface* ETH01 lalu ETH00 karena setelah merubah IP pada ETH00 *browser* akan *disconnect*, sebab *interface* tersebut digunakan untuk manajemen IP radius server.

a. Radius Top Level

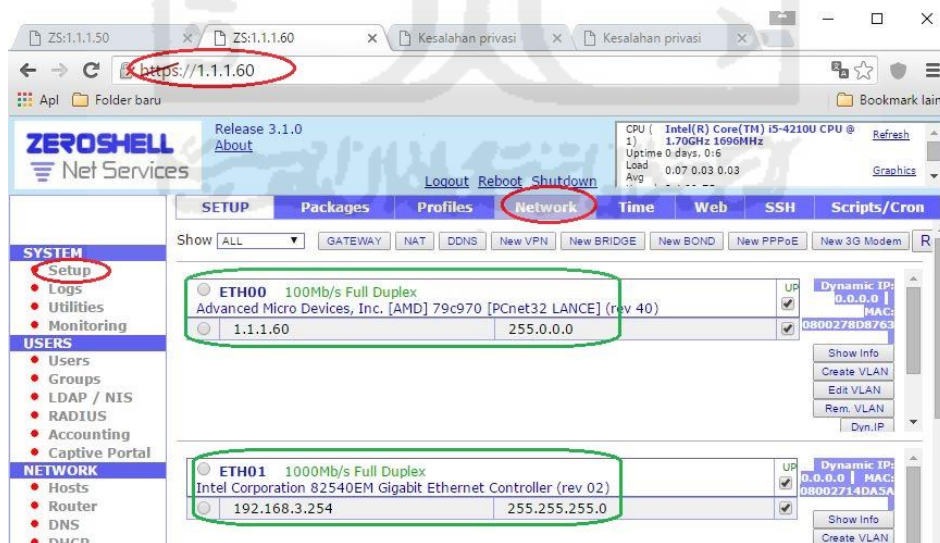
Tanda *elips* berwarna hijau adalah dua *interface* yang digunakan pada Radius Top Level yaitu ETH00 “1.1.1.50/24” dan ETH01 “17.10.10.1/24”.



Gambar 3.37 Konfigurasi Jaringan Radius Top Level

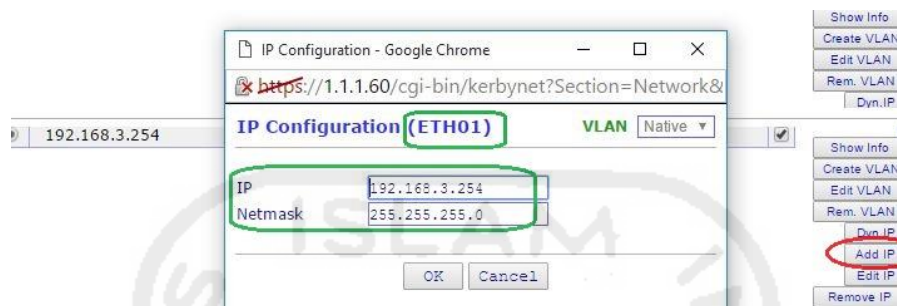
b. Radius UII

Tanda *elips* berwarna hijau adalah dua *interface* yang digunakan pada Radius UII yaitu ETH00 “1.1.1.60/24” dan ETH01 “192.168.3.254/24”.



Gambar 3.38 Konfigurasi Jaringan Radius UII

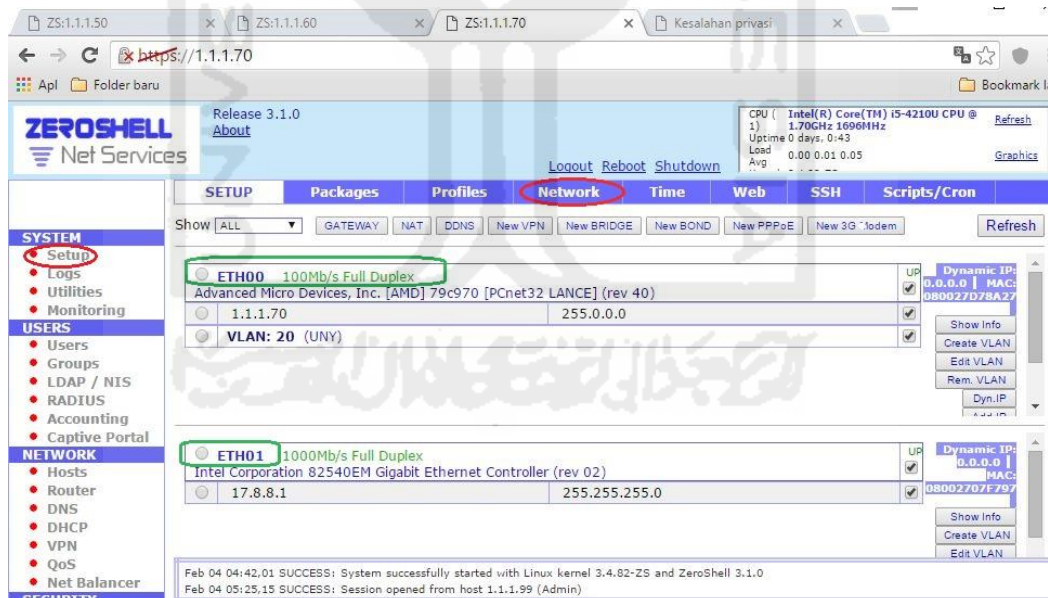
Gambar 3.39 menunjukkan “IP Configuration” interface ETH01 yang terdapat pada menu “Add IP” dari salah satu interface. Alamat IP address dan netmask yang belum ditambahkan pada interface adapter saat instalasi Zeroshell, dapat menggunakan menu ini untuk konfigurasi IP.



Gambar 3.39 Menambahkan IP Konfigurasi Pada Interface

c. Radius UNY

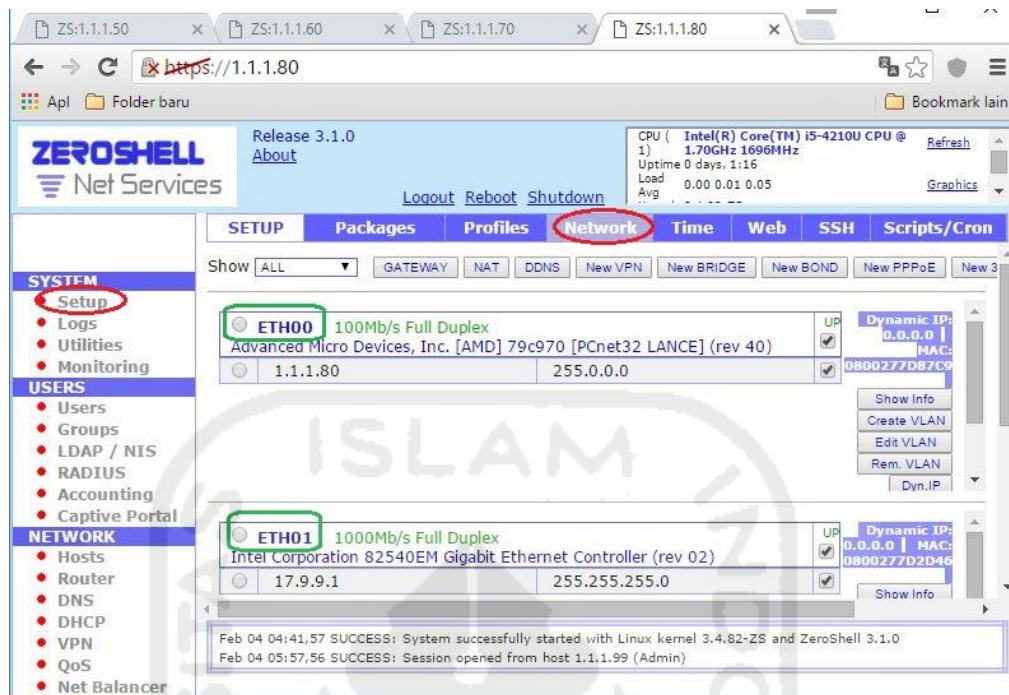
Tanda *elips* berwarna hijau adalah dua interface yang digunakan pada Radius UNY yaitu ETH00 “1.1.1.70/24” dan ETH01 “17.8.8.1/24”.



Gambar 3.40 Konfigurasi Network Radius UNY

d. Radius UGM

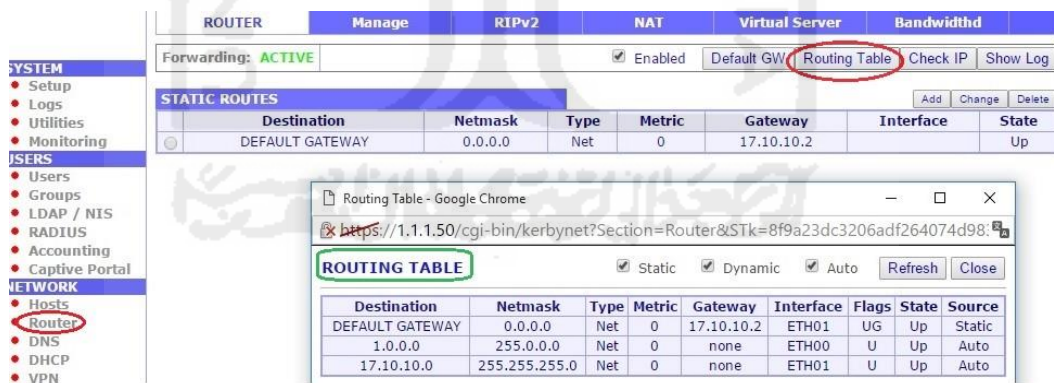
Tanda *elips* berwarna hijau adalah dua interface yang digunakan pada Radius UGM yaitu ETH00 “1.1.1.80/24” dan ETH01 “17.9.9.1/24”.



Gambar 3.41 Network Radius UGM

3.11.5 Routing Table Radius Server

Untuk melihat informasi *default Gateway* dan *routing table* terdapat pada menu *Network->Router->Default GW* atau *Routing Table*.



Gambar 3.42 Routing Table Radius Top Level

Gambar 3.42 menunjukkan *Routing table* pada Radius Top Level yaitu *default gateway* dengan alamat IP "17.10.10.2" menggunakan *interface* ETH01 dan tujuan *network* "1.0.0.0" *netmask* "255.0.0.0" pada *interface* ETH00 dan "17.10.10.0/24" menggunakan *interface* ETH01.

Destination	Netmask	Type	Metric	Gateway	Interface	Flags	State	Source
DEFAULT GATEWAY	0.0.0.0	Net	0	192.168.3.1	ETH01	UG	Up	Static
1.0.0.0	255.0.0.0	Net	0	none	ETH00	U	Up	Auto
192.168.3.0	255.255.255.0	Net	0	none	ETH01	U	Up	Auto

Gambar 3.43 Routing Table Radius UII

Gambar 3.43 menunjukkan *Routing table* pada Radius UII yaitu *default gateway* dengan alamat IP "192.168.3.1" yang menggunakan *interface* ETH01, tujuan *network*-nya adalah "1.0.0.0" *netmask* "255.0.0.0" pada *interface* ETH00 dan "192.168.3.0/24" pada *interface* ETH01.

Destination	Netmask	Type	Metric	Gateway	Interface	Flags	State	Source
DEFAULT GATEWAY	0.0.0.0	Net	0	17.8.8.2	ETH01	UG	Up	Static
1.0.0.0	255.0.0.0	Net	0	none	ETH00	U	Up	Auto
17.8.8.0	255.255.255.0	Net	0	none	ETH01	U	Up	Auto

Gambar 3.44 Routing Table Radius UNY

Gambar 3.44 menunjukkan *Routing table* pada Radius UNY yaitu *default gateway* dengan alamat IP "17.8.8.2" yang menggunakan *interface* ETH01, tujuan *network*-nya adalah "1.0.0.0" *netmask* "255.0.0.0" pada *interface* ETH00 dan "17.8.8.0/24" pada *interface* ETH01.

ROUTING TABLE

Destination	Netmask	Type	Metric	Gateway	Interface	Flags	State	Source
DEFAULT GATEWAY	0.0.0.0	Net	0	17.9.9.2	ETH01	UG	Up	Static
1.0.0.0	255.0.0.0	Net	0	none	ETH00	U	Up	Auto
17.9.9.0	255.255.255.0	Net	0	none	ETH01	U	Up	Auto

Gambar 3.45 Routing Table Radius UGM

Gambar 3.45 menunjukkan *routing table* pada Radius UGM yaitu *default gateway* dengan alamat IP "17.9.9.2" yang menggunakan *interface* ETH01, tujuan *network*-nya yaitu "1.0.0.0" *netmask* "255.0.0.0" pada *interface* ETH00 dan "17.9.9.0/24" pada *interface* ETH01.

3.11.6 Radius Aktif

Pastikan semua radius server dalam keadaan aktif dengan memastikan tanda "enabled" telah dicentang agar dapat mengaktifkan fungsi AAA.

RADIUS Server for Wireless and Identity Based Networking Services

Status: ACTIVE Enabled Show Requests 802.1x

802.1x Configuration Save Cancel

X.509 Host Certificate
Local CA OU=Hosts, CN=uny.ac.id View Status: OK Check CRL Imported Trusted CAs

Feb 04 04:42:01 SUCCESS: System successfully started with Linux kernel 3.4.82-ZS and ZeroShell 3.1.0
Feb 04 05:25:15 SUCCESS: Session opened from host 1.1.1.99 (Admin)

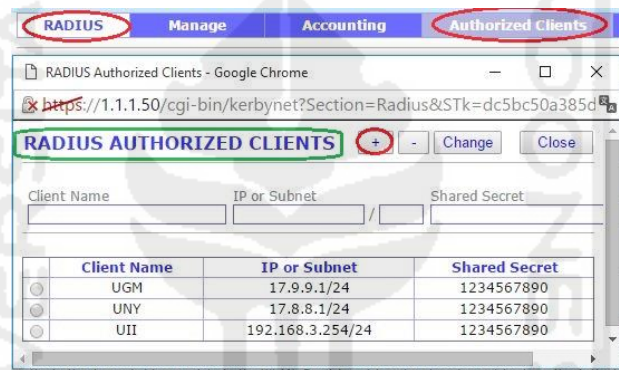
Gambar 3.46 Radius UNY Aktif

3.11.7 Authorized Client

Authorized Client merupakan konfigurasi radius server untuk mengatur radius server mana saja yang diijinkan untuk umelakukan proses autentikasi *user*. Konfigurasi di setiap radius server akan dijelaskan, sebagai berikut :

1. Radius Top Level

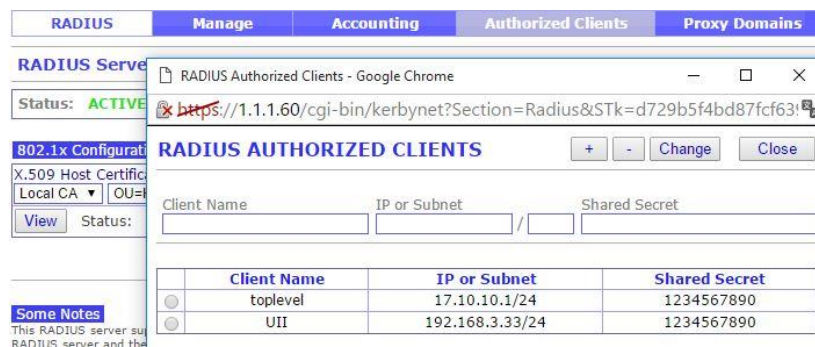
Pada menu *Authorized Client*, tab “+” untuk mengisi kolom “*Client Name, IP or Subnet*, dan *Shared Secret*”. Untuk menghapus kolom “-” dan mengganti isi kolom terdapat pada tombol “*change*”. *Client Name* pada Radius Top Level diisi dengan Radius “UGM, UNY, UII” dan untuk alamat IP nya disesuaikan dengan alamat IP radius tersebut menggunakan *interface* ETH01.



Gambar 3.47 *Authorized Client* Radius Top Level

2. Radius UII

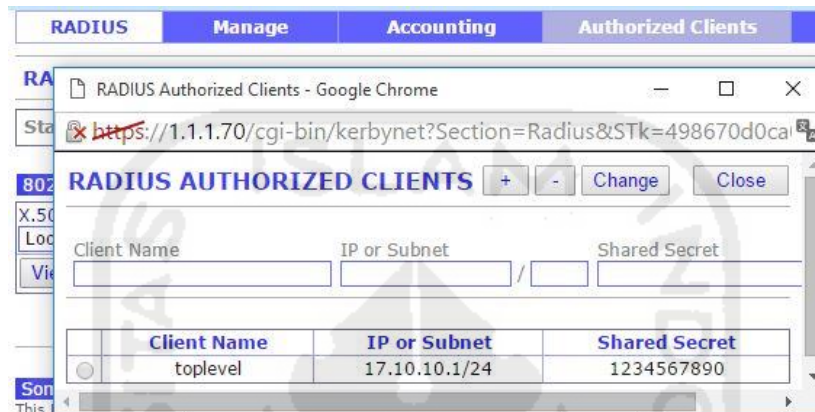
Pada Radius UII *Client Name* diisi dengan Top level dan alamat IP pada *interface* ETH01 yaitu “17.10.10.1/24”, UII menggunakan alamat IP *access point* karena sesuai dengan skema *access point* berada di UII. Tab “*change*” berfungsi untuk mengganti kolom yang telah terisi.



Gambar 3.48 *Authorized Client* Radius UII

3. Radius UNY dan Radius UGM

Pada **Gambar 3.49** menunjukkan *Authorized Client* untuk Radius UNY, kolom *Client Name* diisi dengan “Top level” dan alamat IP pada *interface* ETH01 yaitu “17.10.10.1/24”. Dalam hal ini *Authorized Client* berlaku juga untuk Radius UGM.



Gambar 3.49 *Authorized Client* Radius UNY

3.11.8 Proxy Domain

Setelah melakukan konfigurasi pada *Authorized Client*, diperlukan juga konfigurasi pada *Proxy Domain* yang berfungsi untuk mengenali domain atau *realm* mana saja yang akan dikenali oleh setiap radius server ketika proses autentikasi terjadi. Konfigurasi terdapat pada menu *User->Radius->Proxy Domains*, yang harus didaftarkan ke dalam kolom *Realm* adalah *realm* yang ingin dikenali oleh masing-masing radius server. Kemudian isi kolom *proxy server* disesuaikan dengan alamat IP radius menggunakan *interface* ETH01, kolom *Auth Port* “1812”, dan *shared secret* “1234567890”.



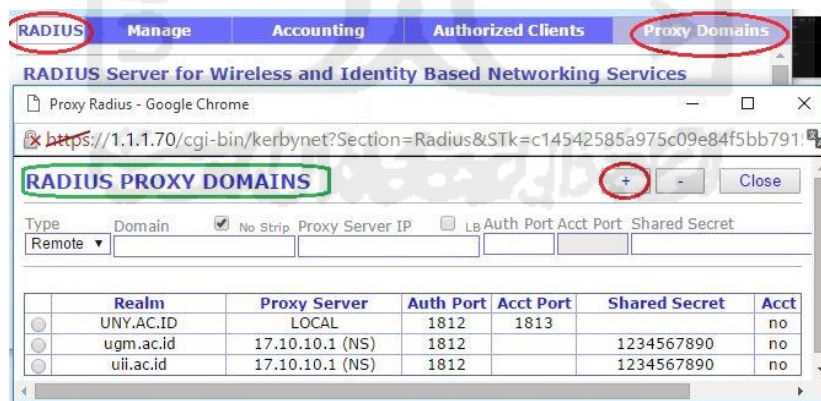
Gambar 3.50 Proxy Domain Radius Top Level

Gambar 3.50 menunjukkan halaman web Zeroshell pada menu *Proxy Domain Radius Top Level*. *Realm* yang akan dikenali oleh Radius Top Level adalah “ugm.ac.id, uii.ac.id, dan uny.ac.id”. Kolom “*Proxy Server*” diisi dengan alamat IP radius server yang menggunakan *interface* ETH01 yaitu 17.9.9.1 untuk Radius UGM, 192.168.3.254 untuk Radius UII, 17.8.8.1 untuk Radius UNY.



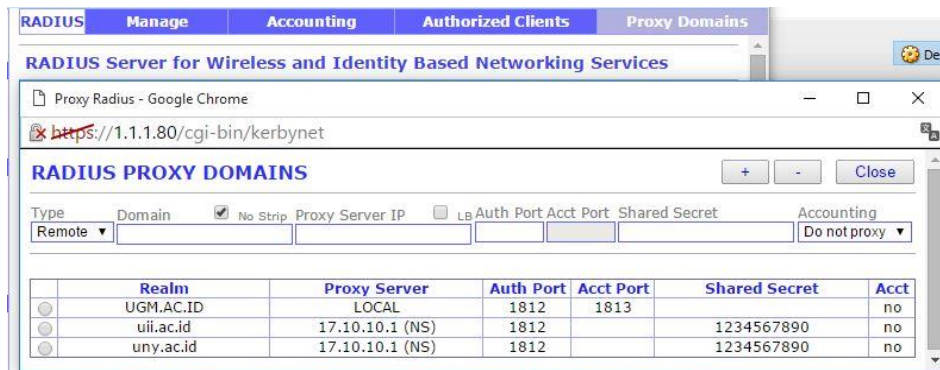
Gambar 3.51 Proxy Domain Radius UII

Proxy Domain pada Radius UII adalah *realm* yang dikenali oleh Radius UII yaitu ugm.ac.id dan uny.ac.id. Kolom *Proxy Server* berisi alamat IP Radius Top Level menggunakan *interface* ETH01 yaitu 17.10.10.1 yang berfungsi untuk mengirimkan kembali *credentials user* ke radius server sesuai *realm* yang terdefinisi.



Gambar 3.52 Proxy Domain Radius UNY

Proxy Domain pada Radius UNY adalah *realm* yang dikenali oleh Radius UNY yaitu ugm.ac.id dan uii.ac.id. Kolom “*Proxy Server*” berisi alamat IP Radius Top Level menggunakan *interface* ETH01 yaitu 17.10.10.1.

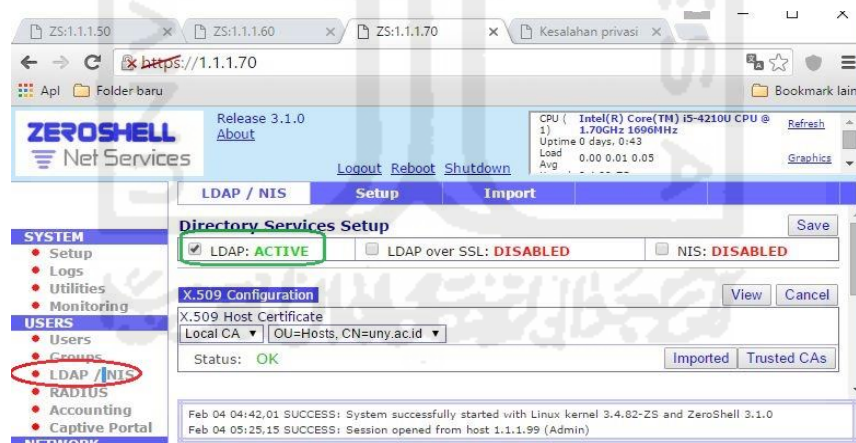


Gambar 3.53 Proxy Domain Radius UGM

Proxy Domain pada Radius UGM adalah *realm* yang dikenali oleh radius UGM yaitu *uii.ac.id* dan *uny.ac.id*. Kolom “*Proxy Server*” berisi alamat IP radius Top Level pada *interface* ETH01 yaitu 17.10.10.1.

3.11.9 LDAP

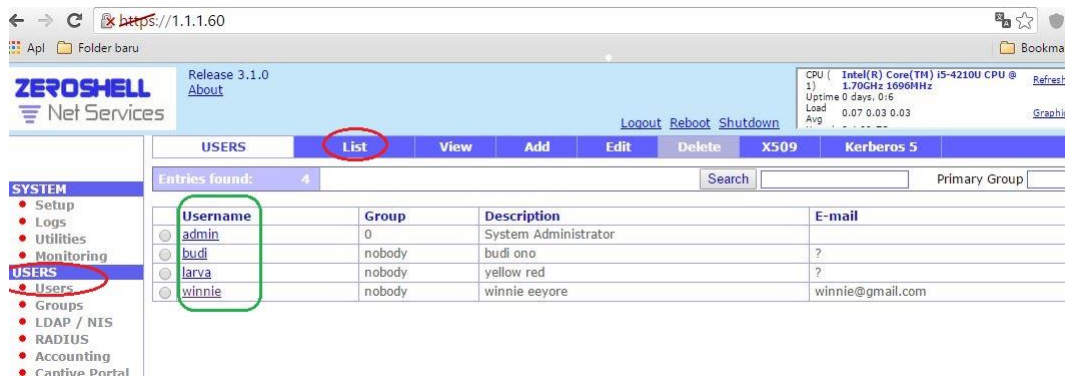
Pastikan database LDAP di setiap radius server telah aktif seperti yang ditunjukkan **Gambar 3.54**, karena hal ini akan membantu keberhasilan proses autentikasi *user*.



Gambar 3.54 LDAP Radius UNY Aktif

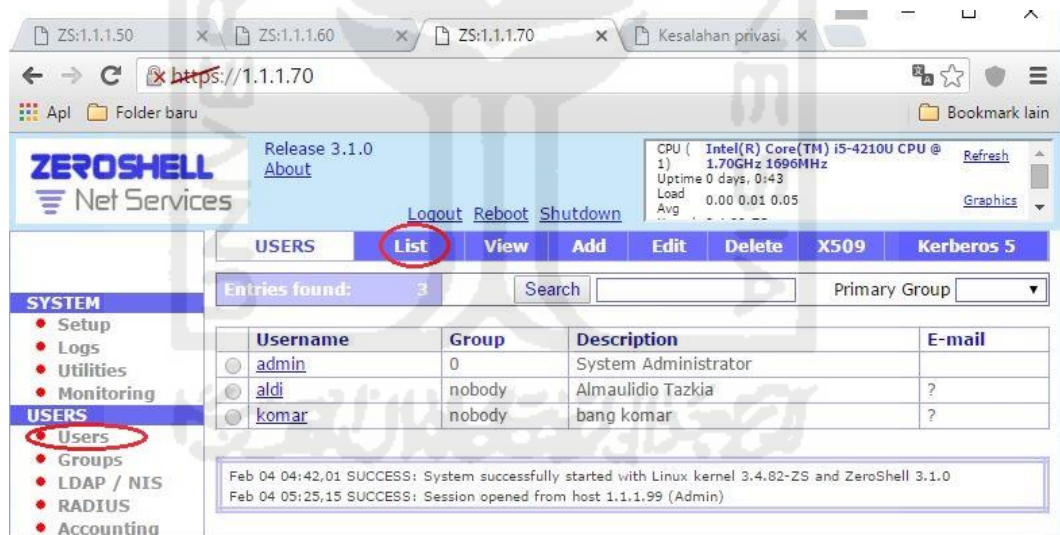
3.11.10 User

Untuk manajemen *user* pada radius server, terdapat pada menu *Users->Users* di setiap halaman web *ZeroShell*.



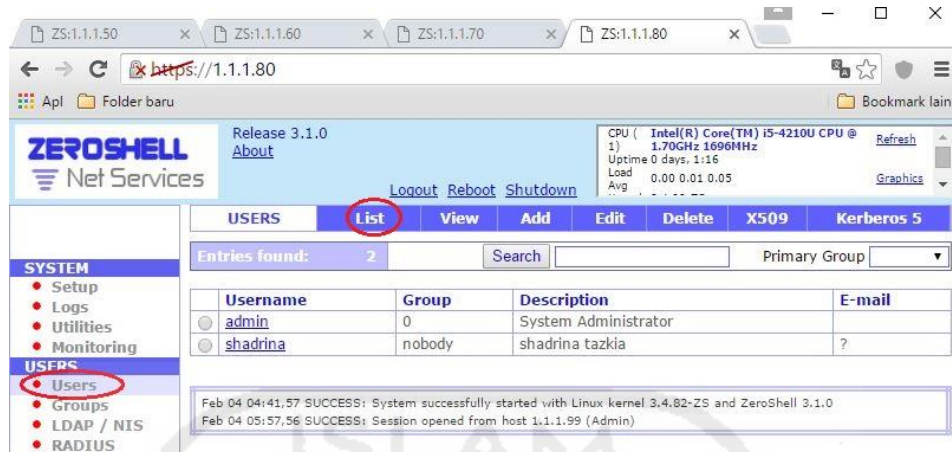
Gambar 3.55 List User Radius UII

Gambar 3.55 menunjukkan *list user* dari Radius UII yang telah berhasil diregistrasikan. Halaman *List user* terdapat pada menu *Users->Users->List*. *User* Radius UII yang berhasil ditambahkan adalah *username* budi, larva, dan Winnie Eeyore”.



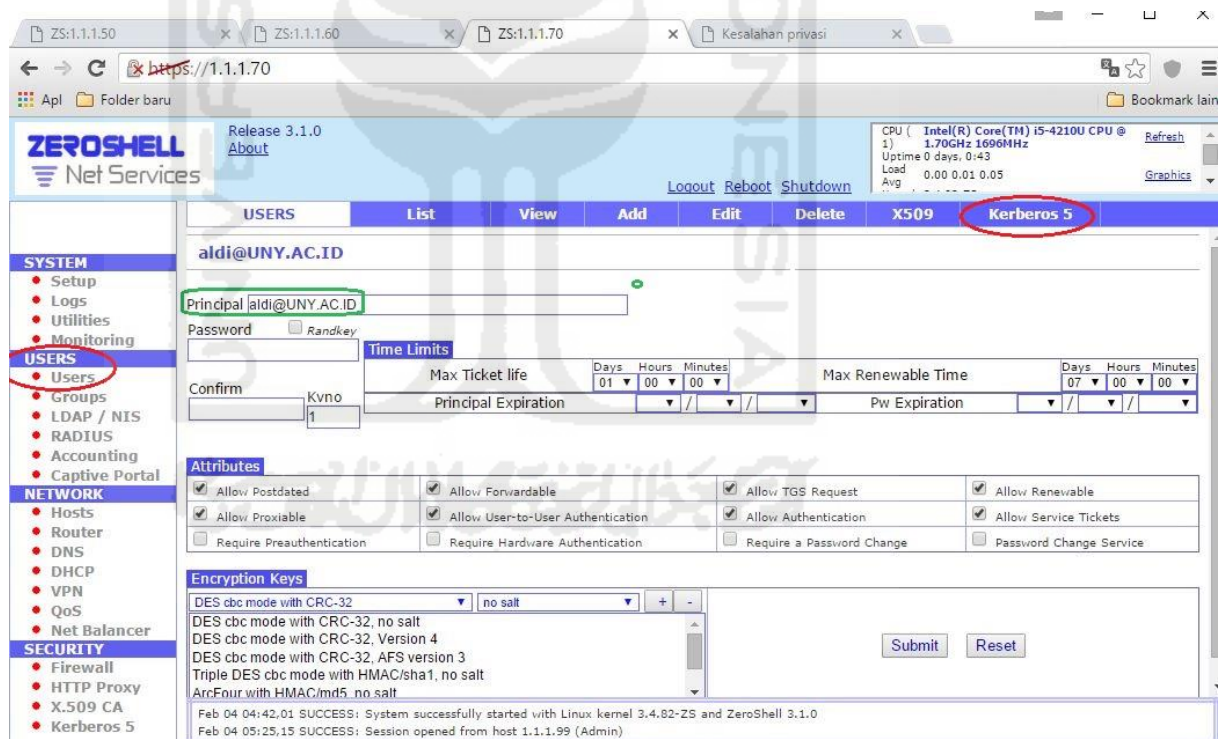
Gambar 3.56 List User Radius UNY

Gambar 3.56 menunjukkan *list user* dari Radius UNY yang telah berhasil diregistrasikan. *User* Radius UNY yang berhasil ditambahkan adalah *username* aldi, dan komar dengan nama lengkap secara terurut yaitu “Almaulidio Tazkia dan bang komar”.



Gambar 3.57 List User Radius UGM

Gambar 3.57 menunjukkan *list user* dari Radius UGM yang telah berhasil diregistrasikan. *Username* shadrina dengan nama lengkap “shadrina tazkia” adalah *user* yang telah berhasil ditambahkan pada Radius UGM.

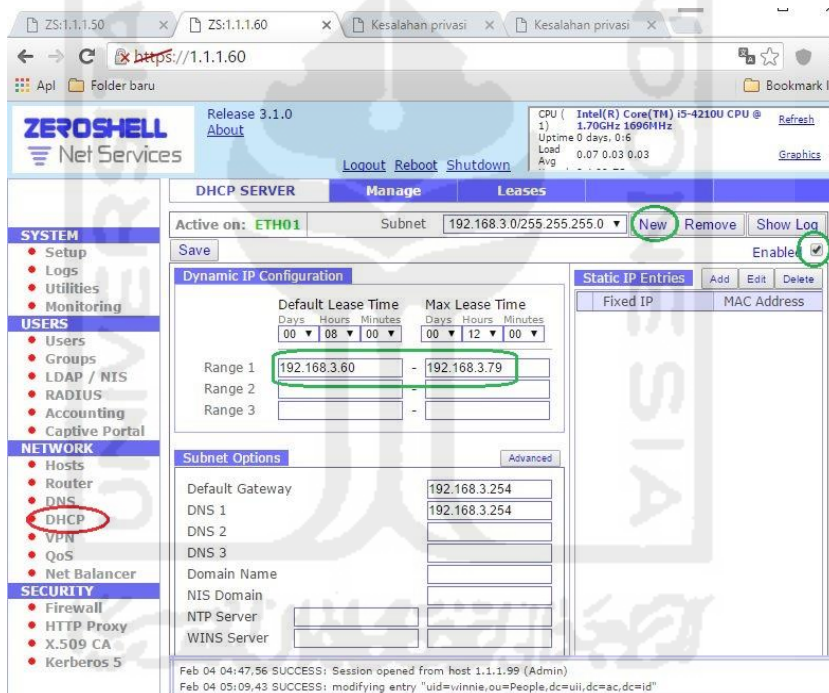


Gambar 3.58 Realm User Radius UNY

Gambar 3.58 menampilkan halaman menu “Kerberos 5” yaitu menu untuk melihat informasi dari salah satu *user* yang berhasil ditambahkan. Tanda *elips* berwarna hijau menunjukkan *principal* yang artinya *username* saat masuk ke halaman *login*.

3.11.11 DHCP

DHCP (*Dynamic Host Control Protocol*) berfungsi untuk memberikan IP kepada *user* yang telah berhasil *login*. Untuk autentikasi hierarki di radius LDAP ini, DHCP dikonfigurasi pada Radius UII. *Network->DHCP->Manage* adalah urutan menu untuk masuk ke halaman pengaturan DHCP seperti yang ditunjukkan pada **Gambar 3.59**. Tab “New” untuk menambahkan *interface* yang *network*-nya akan diberikan IP DHCP. Dalam penelitian ini *interface* yang digunakan untuk DHCP server adalah *network* ETH01 Radius UII. Pada *Dynamic IP Configuration*, kolom *Range* 1 diisi dengan alamat IP 192.168.3.60 – 192.168.3.79. DHCP harus dalam keadaan aktif dengan memastikan “*enabled*” telah dicentang.



Gambar 3.59 DHCP diatur dalam Radius UII