BAB IV

IMPLEMENTASI, HASIL, DAN ANALISIS

1.1 Implementasi

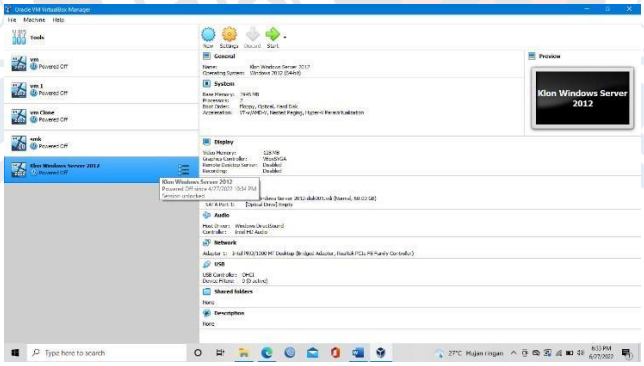
Implementasi merupakan penerapan maupun pelaksanaan dalam rancangan yang telah dibuat sebelumnya demi mendapatkan hasil melalui pelaksanaan tersebut. Di dalam proses implementasi ini dilakukan ketika penulis telah menyelesaikan proses untuk perancangan. Di dalam pengimplementasian mekanisme keamanan jaringan dengan widows server ini terlebih dahulu harus mengetahui kebutuhan apa saja yang akan dibutuhkan untuk pembuatan keamanan jaringan dengan windows server. Kebutuhan yang dibutuhkan meliputi kebutuhan *software* dan kebutuhan *hardware.*

Perancangan dan implementasi mekanisme keamanan jaringan dengan *windows server* akan dibuat berdasarkan dengan topologi yang telah dibuat. Dan dengan bantuan desain sistem yang telah dibuat akan dapat lebih memudahkan penulis dalam membuat perancangan menjadi lebih terstruktur dan pengimplementasian dapat berjalan sesuai dengan yang diharapkan. Dalam melakukan implementasi penelitian ini akan dijelaskan dari tahap awal dan hingga ke tahap akhir setelah tahap implementasi sukses dilakukan. Perancangan dan implementasi untuk proses yang pertama dimulai dari proses tahap persiapan dan penginstalan. Tahap persiapan yang dilakukan adalah dengan mempersiapkan perangkat apa saja yang akan dibutuhkan dalam pengimplementasi dan untuk tahap penginstalan akan dilakukan penginstalan untuk aplikasi yang berupa VM *VirtualBox* di dalam *device* dan ke dalam laptop yang digunakan. Setelah proses instalasi selesai kemudian akan berlanjut dengan tahap instalasi sistem operasi yang telah disiapkan sebelumnya, sistem operasi yang digunakan penulis dalam perancangan ini berupa *Windows Server* 2012 yang akan digunakan sebagai konfigurasi keamanan jaringan serta sebagai *server*. Setelah dilakukannya penginstalan, maka akan dilakukan

konfigurasi- konnfigurasi dasar yang berada di *Windows Server* dan yang akan terhubung langsung dengan *mikrotik.* Berikut merupakan proses perancangan maupun implementasi yang akan dijelaskan sebagai berikut:

1.1.1 Pengujian serta penerapan konfigurasi *Windows Server* di VM *VirtualBox*

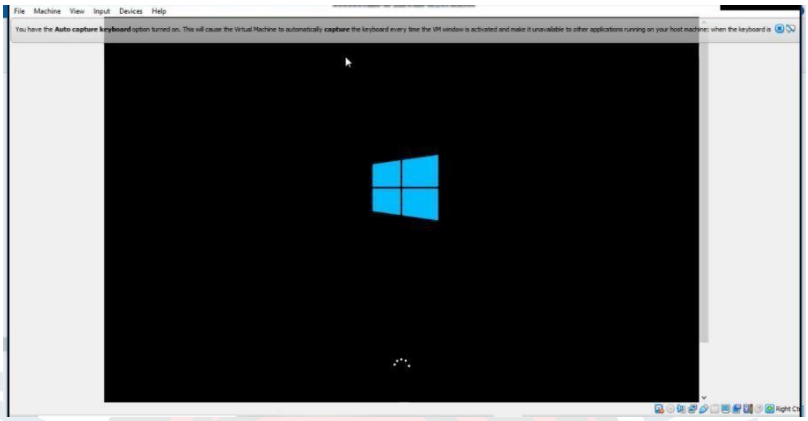
VM *VirtualBox* merupakan *software* dimana di dalam *software* ini memungkinkan pengguna untuk menjalankan sistem operasi di dalam *VirtualBox*. Di dalam proses instalasi *Windows Server* 2012 ini dilakukan sama halnya seperti instalasi *software* maupun aplikasi lainnya. Untuk tahap awal setelah VM *VirtualBox* berhasil terunduh, yang selanjutnya adalah dengan mmemasukkan file dari *windows server* yang telah diunduh sebelumnya. Sampai proses *Windows Server* dapat digunakan, kemudian penulis dapat melakukan konfigurasi- konfigurasi dasar seperti konfigurasi DNS, DHCP, ADDS, ADCS, dan untuk keamanannya adalah dengan konfigurasi NPS, *Radius Server* dan *Active Directory*.



Gambar 4.1 Tampilan VM VirtualBox

Gambar 4.1. merupakan tampilan dari *VirtualBox* yang akan dijadikan sebagai Perangkat Lunak dalam menjalankan sistem operasi yang akan digunakan dalam penelitian ini. Dalam melakukan instalasi VirtualBox ini terbilang cukup mudah dan pengoperasiaannya juga dapat lebih dimengerti oleh penulis. Fitur-

fitur didalam VirtualBox terbilang cukup banyak dan komplit sesuai dengan yang akan digunakan oleh peneliti.



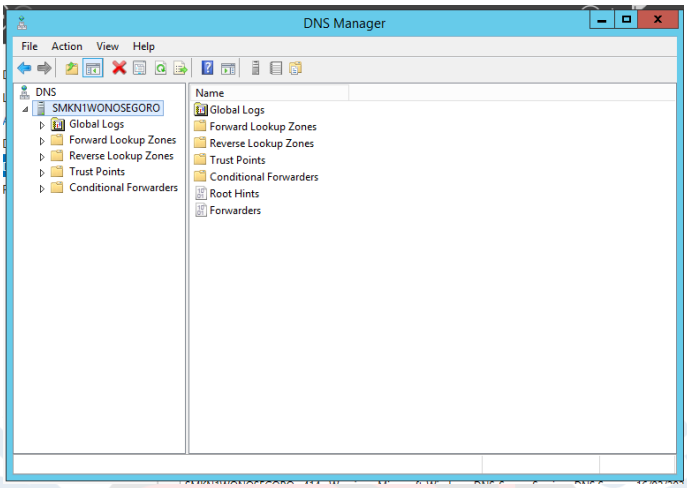
Gambar 4.2. Tampilan VirtualBox saat menjalankan OS

Gambar 4.2. menampilkan tampilan *VirtualBox* saat menjalanjan sistem operasi *windows server*. Dalam melakukan instalasi *windows server* penulis dapat menginstal terlebih dahulu *file iso* dari *Windows Server* 2012. Setelah dapat terinstal langkah yang harus dilakukan adalah dengan membuka aplikasi *VirtualBox,* kemudian klik menu *new* dalam membuat *file* baru penulis menuliskan *file iso* dengan nama instansi yang akan digunakan. Setelah berhasil, penulis dapat menentukan *type windows server* yang akan digunakan karena penulis akan menggunakan *type windows server* 2012 maka penulis akan menentukan *windows server* seperti yang akan dibutuhkan. Setelah berhasil menentukan *type* penulis dapat menentukan isi atau ukuran memori ram sesuai dengan spek dari laptop yang digunakan untuk membangun konfigurasi *windows server*. Setelah semua sudah dapat ditentukan sesuai dengan kebutuhan, *windows server* 2012 akan siap untuk digunakan sebagai sistem operasi guna mendukung penelitian ini.

1.1.2 Instalasi dan Konfigurasi *Windows Server* DNS *Server*

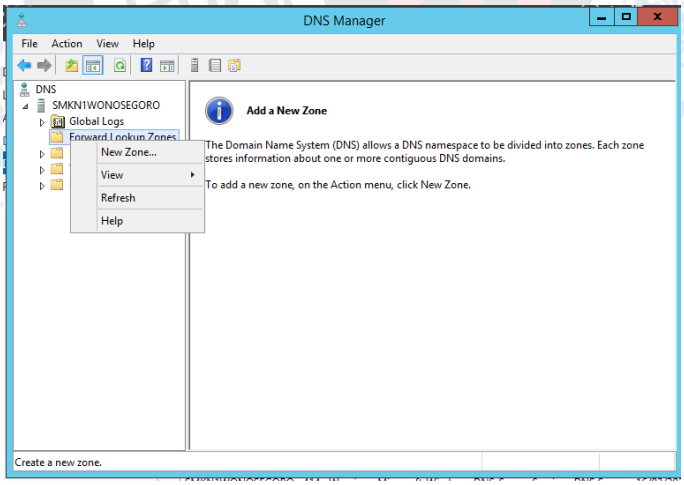
Setelah berhasil menjalankan Sistem Operasi di *Windows Server*, tahap selanjutnya yang akan dilakukan adalah melakukan Konfigurasi didalam *windows server*. Penulis dapat melakukan

konfigurasi yang berada di dalam *local server* terlebih dahulu lalu dapat mengganti *computer name* sesuai dengan yang dibutuhkan, kemudian penulis dapat mengganti *IP Address Ethernet*. *IP Address* yang digunakan adalah *IP Static* sehingga diharapkan nantinya tidak akan terjadi perubahan jika akan dikoneksikan dengan IP yang berada di *Mikrotik*. Jika kedua hal tersebut telah terselesaikan, langkah berikutnya adalah dengan menginstal DNS *Server* yang berada di dalam Sistem Operasi *Windows Server*. Fungsi dari penginstalan DNS *Server* (*Domain Name System*) adalah untuk mengubah alamat *IP Address* menjadi sebuah domain yang nantinya dapat memudahkan para pengguna jika saat akan terhubung ke jaringan Internet yang telah disediakan. Jika DNS *Server* (*Domain Name System*) sudah terinstal maka tahap selanjutnya akan dilakukan konfigurasi didalam DNS *Server*. Di dalam konfigurasi ini, penulis melakukan beberapa tahapan, pada tahap pertama dilakukan untuk pemilihan *Forward Lookup Zone* yang digunakan untuk membuat *New Zone* atau zona baru yang difungsikan sebagai permintaan klien untuk meminta sebuah alamat IP dengan memberikan nama *host* lalu setelah mengisi nama *host* dengan nama shakila.id. kemudian setelah mengisi nama *host*, penulis akan diarahkan pada menu dan memilih opsi *New Host* (A or AAA) untuk mengisi nama domain, dan *IP Address*. Kemudian setelah perintah terselesaikan, penulis akan diarahkan untuk memilih *Reverse Lookup Zone* yang dimaksudkan untuk menyelesaikan permintaan klien dimana klien meminta nama *host* dengan memberikan alamat *IP Address*. Setelah selesai menyelesaikan perintah, akan diarahkan untuk memilih *New Pointer* pada *Reverse Lookup Zone* yang digunakan untuk menunjukkan nama *host* untuk alamat *IP Address* yang telah ditentukan sebelumnya.



Gambar 4.3. Konfigurasi DNS Server

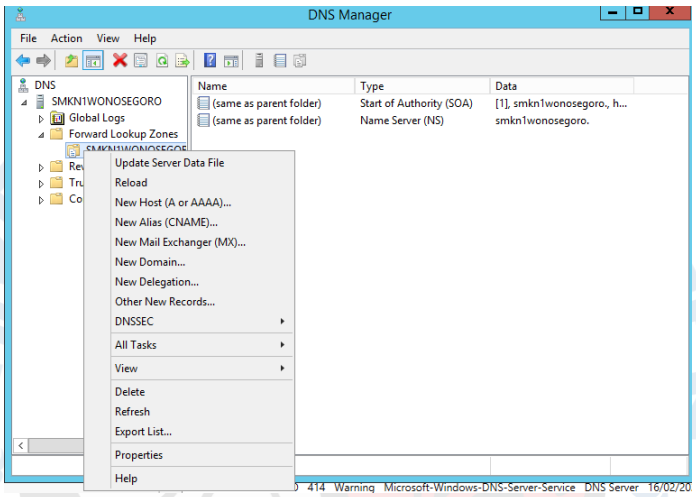
Gambar 4.3. menampilkan tampilan konfigurasi DNS Server yang dapat terlihat bahwa nama dns server telah berubah menjadi smkn 1 wonosegoro, sebagaimana yang telah ditentukan penulis diawal konfigurasi. Guna dari penggunaan nama ini adalah untuk memudahkan penulis dalam melakukan konfigurasi- konfigurasi lainnya.



Gambar 4.4 Tahap Konfigurasi Forward Lookup Zone

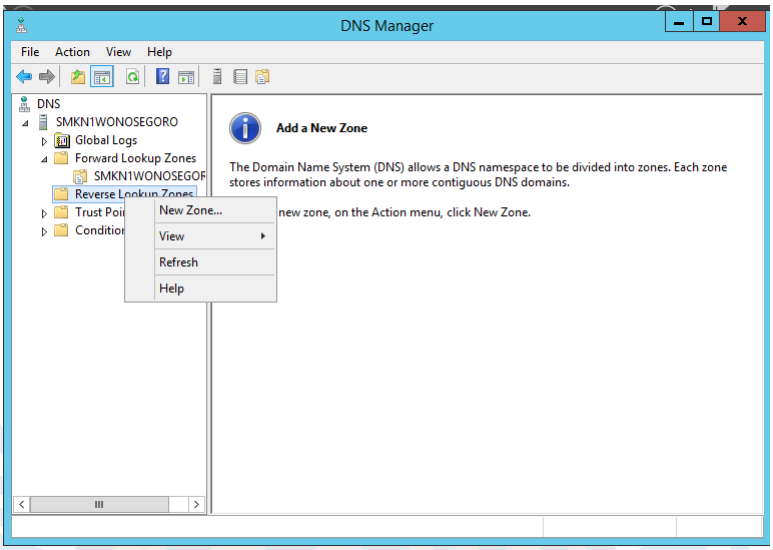
Gambar 4.4 menampilkan tampilan dari tahap konfigurasi dns *server*, setelah melakukan penginstalan dan penggantian nama. Penulis dapat memulai langkah awal konfigurasi dengan memilih *forward lookup zone*

yang difungsikan sebagai permintaan klien untuk meminta sebuah alamat IP dengan memberikan nama *host* lalu setelah mengisi nama *host*, penulis akan diarahkan pada menu dan memilih opsi *New Host* (A or AAA) untuk mengisi nama domain, dan *IP Address* yang telah ditentukan oleh penulis.



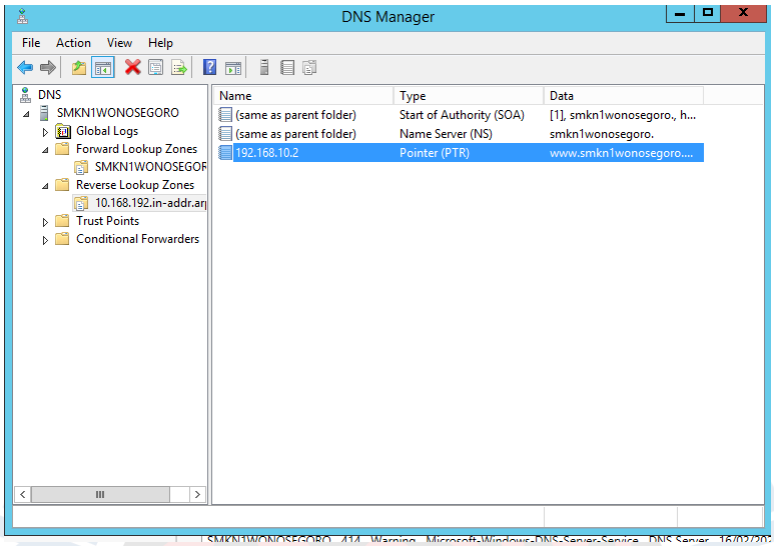
Gambar 4.5 Konfigurasi New Host (A or AAA)

Gambar 4.5. menampilkan konfigurasi *new host* (A or AAA) yang konfigurasinya dilakukan setelah membuat *forward lookup zone*. Jika langkan *forward lookup zone* telah dilakukan penulis dapat membuat *host name*, dengan menambahkan dibagian *new host* (A or AAA)



Gambar 4.6 Konfigurasi Reverse Lookup Zone

Gambar 4.6 menampilkan konfigurasi *reverse lookup zone* yang dilakukan setelah mengkonfigurasi *forward lookup zone*. Fungsi dari konfigurasi *reverse lookup zone* adalah untuk mengubah *IP Address* menjadi nama *server* yang akan digunakan. Hal yang akan ditampilkan setelah melakukan konfigurasi ini adalah dapat memudahkan komputer atau *user* dalam mengidentifikasi alamat *web* dan dapat melayani permintaan *IP Address* dari *host.*



Gambar 4.7 Konfigurasi New Pointer

Gambar 4.7 menampilkan tampilan konfigurasi *new pointer* (PTR). Fungsi dari dibentuknya *new* PTR adalah untuk memetakan sebuah nama *host* ke nama kanonik untuk *host* yang telah dibuat. Dalam melakukan pembuatan PTR untuk sebuah nama *host* di dalam *domain* yang dapat mewakili sebuah alamat *IP Address* menerapkan pencarian balik ke *reverse lookup zone* untuk alamat yang telah ditentukan.

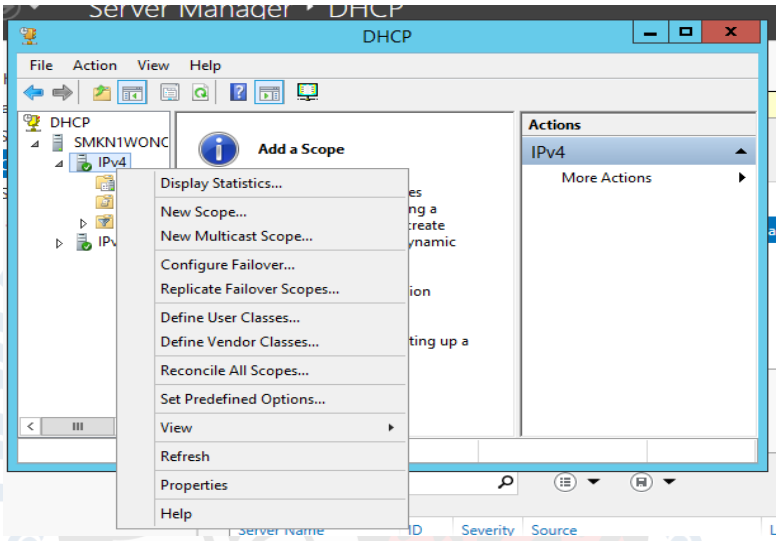
Pada tahap ini penulis akan diminta untuk beberapa tahapan lanjutan, tahapan selanjutnya dalam Konfigurasi *Forward Lookup Zone* di DNS *Server* yaitu dengan membuat *New Zone* > *Primary Zone* > Beri Nama *Zone* yang akan dibuat dan dalam kasus ini penulis memberi nama dengan smk.edu.dns > *next* > *zone name* akan otomatis muncul sesuai dengan yang sudah diisi sebelumnya menjadi smk.edu > kemudian klik *finish* pada *button* yang telah disediakan. Di dalam tahapan ini penulis berhasil membuat sebuah *zone* baru dengan nama smk.edu. Setelah langkah konfigurasi dalam membuat zona baru selesai, maka *zone name* baru di dalam folder *Forward Lookup Zone* akan muncul nama dengan smk.edu. Langkah selanjutnya yang akan dilakukan

penulis adalah dengan memilih smk.edu > klik kanan > pilih *New Host* (A or AAA) > akan muncul seperti form dan penulis diminta untuk mengisi *New Host* dan *IP Address* > lalu *add host*. Setelah konfigurasi di *Forward Lookup Zone* selesai, penulis akan melakukan konfigurasi di bagian *Reverse Lookup Zone* dengan langkah klik kanan pada *Reverse Lookup Zone* > pilih *new zone* > *primary zone* > masukkan tiga okted pertama IP untuk DNS Server > setelah itu klik *finish*. Setelah selesai dalam tahap awal di *Reverse Lookup Zone*, di dalam folder *Reverse Lookup Zone* akan muncul IP yang telah diisi sebelumnya langkah selanjutnya adalah > klik kanan pada IP > klik kanan > pilih *New Pointer* (PTR) > klik *browser* untuk memasukkan host yang sudah dibuat pada *Forward Lookup Zone* > lalu klik ok. Setelah berhasil melakukan konfigurasi seperti tahapan diatas, penulis dapat melihat hasil dari konfigurasi di CMD (*Command Prompt*).

1.1.3 Instalasi dan Konfigurasi Windows Server DHCP Pool (*Dynamic Host Configuration Protocol*)

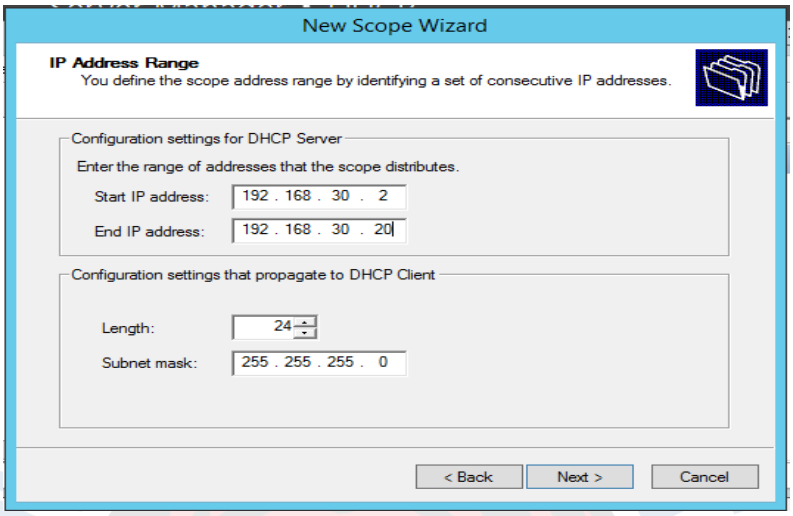
Setelah melakukan tahap instal dan konfigurasi DNS Server (*Domain Name System)*. Maka tahap selanjutnya, penulis akan melakukan instalasi dan konfigurasi DHCP Pool *(Dynamic Host Configuration Protocol).* Konfigurasi DHCP Pool berfungsi sebagai pendistribusian alamat *IP Address* secara otomatis kepada perangkat client yang ingin terhubung dengan jaringan internet. Dalam melakukan konfigurasi DHCP Pool penulis melakukan beberapa tahapan. Untuk tahap awal penulis melakukan tahap untuk memberikan nama scope pada pilihan *new scope*. Kemudian penulis akan diarahkan untuk mengisi nama *scope* yang akan digunakan kemudian memasukkan alamat *IP Address* yang memungkinkan *users* mana yang akan mendapatkan *IP Address* awal yang sudah ditentukan, kemudian diarahkan untuk mengisi *IP Address* akhir untuk *users* yang dapat tersambung dengan jaringan yang telah tersedia nanti. Kemudian akan diarahkan untuk mengisi IP *Gateway* dan IP DNS yang sudah dibuat sebelumnya

untuk menghubungkan satu antar lainnya agar tidak terjadi suatu masalah pada jaringan.



Gambar 4.8 Tahap Konfigurasi DHCP Pool

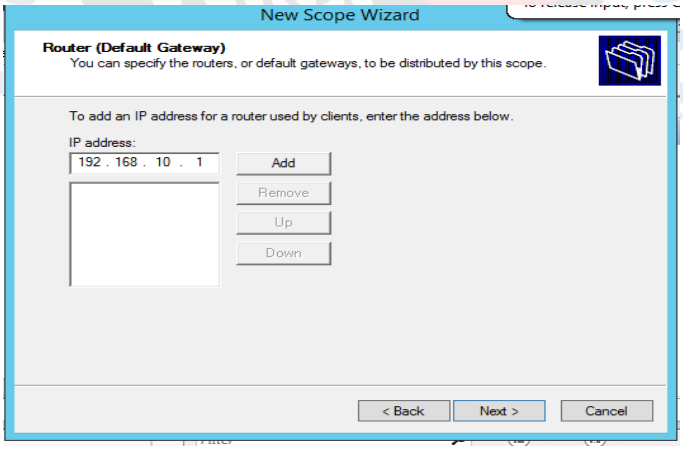
Pada tahap awal konfigurasi DHCP Pool yang perlu dilakukan adalah dengan klik kanan pada *tabs* DHCP > klik kanan > pilih Ipv4 > *New Scope* > Beri nama *scope*, penulis memberi nama *scope* Ruang TU > Masukkan *IP Range* dengan *start IP* > Masukkan *Lease Time IP* > Masukkan *IP Gateway* > Masukkan IP DNS Server > Masukkan IP Windows Server > lalu klik *Finish*.



Gambar 4.9 Start dan End IP Addres

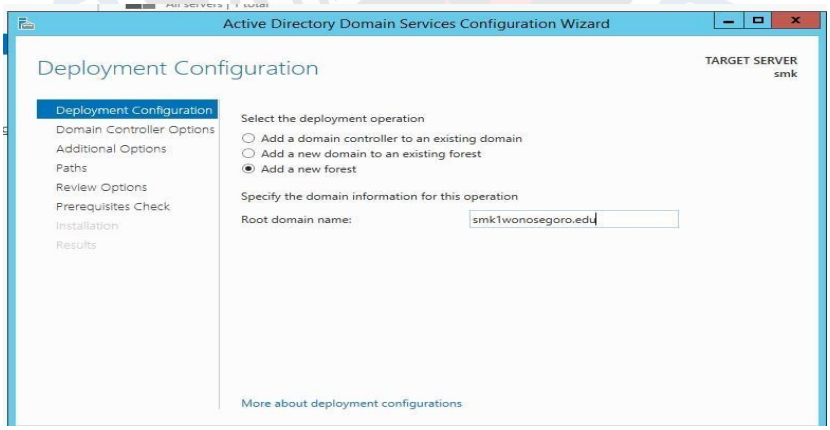
start IP Address berarti adalah IP awal yang nantinya dapat terhubung dengan jaringan yang sudah tersedia dan kegunaan *End IP Address* adalah untuk membatasi IP yang dapat terhubung dengan jaringan internet.

1.1.4 Instalasi dan Konfigurasi ADDS



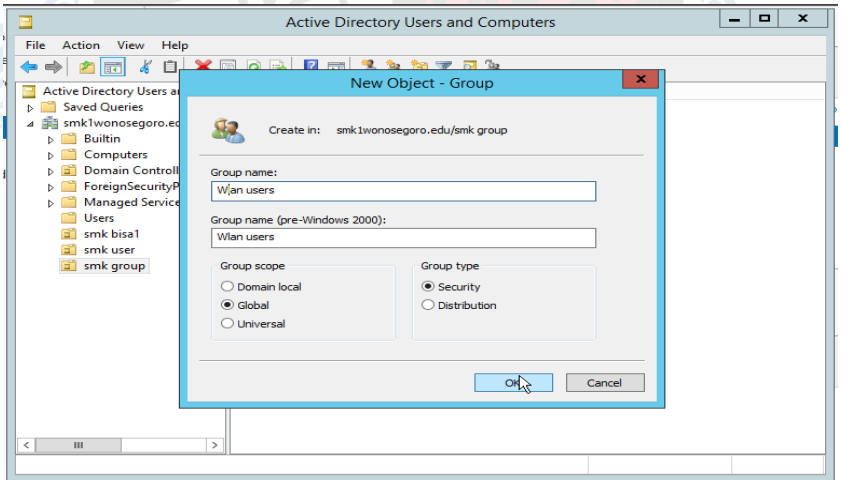
Gambar 4.10 Instalasi dan Konfigurasi ADDS

Instalasi ADDS *(Active Directory Domain Server)* dilakukan di dalam *Windows Server* yang nantinya ketika saat penginstalan kita akan diminta untuk menambahkan *forest* atau sekumpulan domain yang artinya domain yang akan penulis buat akan menjadi domain *controller* untuk domain yang akan dibuat. Setelah berhasil melakukan instalasi ADDS, penulis akan melakukan konfigurasi di dalam ADDS (*Active Directory Domain Services*) yang digunakan untuk menyimpan *directory* data dan mengelola komunikasi antara *users* dan *domain*. Yang akan dilakukan penulis adalah untuk proses *user logon*, dan authentikasi *users*. Untuk tahap konfigurasi ADDS (*Active Directory Domain Server*) penulis membuat sebuah organisasi unit sesuai nama perusahaan yang akan diinginkan. Kemudian akan diarahkan untuk membuat grup yang fungsinya sebagai pengecualian untuk *users* yang akan terhubung. Nama grup yang akan ditentukan di dalam penelitian ini adalah dengan pengecualian menurut dengan divisi yang berada di lingkup kerja tersebut. Setelah menentukan grup sesuai yang dibutuhkan, peneliti akan membuat *users* yang nantinya akan digunakan sebagai identitas *users* yang akan terhubung dengan memberikan *password* yang telah ditentukan oleh peneliti. Setelah berhasil dengan beberapa *step* diatas akan di tampilkan beberapa hasil terhadap apa yang sudah dikonfigurasi sebelumnya.



Gambar 4.11 Tahap Konfigurasi ADDS

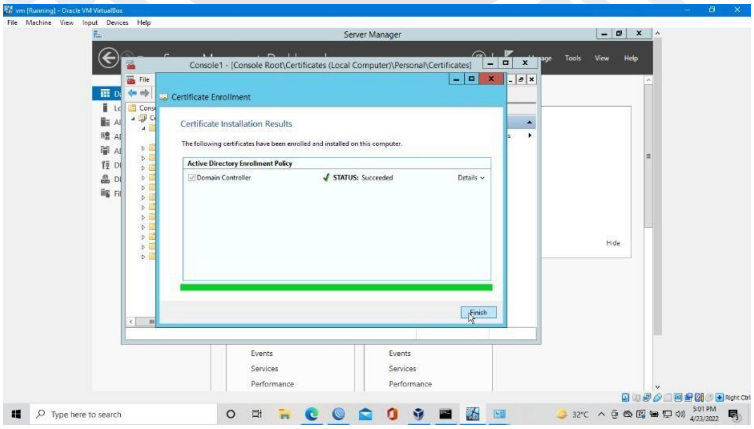
Tahap awal dalam konfigurasi ADDS di dalam *windows server* adalah dengan melakukan beberapa langkah klik kanan pada ADDS > Pilih *Active Directory Users* and *Computers* > klik kanan pada nama *host* yang telah dibuat di DNS yaitu smk.edu > pilih *new* > *organization unit* > beri nama pada *organization* yang akan dibuat penulis memberinya nama dengan Wlan *Users* > setelah unit terbuat, akan diarahkan untuk membuat grup > masukkan nama grup > setelah grup sudah terbuat, akan diarahkan kembali untuk membuat *user* pada unit > klik kanan pada unit *Wlan Users* > pilih *new* > *user* > masukkan nama *profile user*, penulis membuat nama dengan smk bisa1 > masukkan *password* dan *ceklist* di bagian *user cannot change password* dan *password never expired* > *finish*. Setelah *user* telah berhasil dibuat, klik pada *user* yang telah dibuat atau smk bisa1 > pilih pada *member of* lalu ditambahkan ke grup yang sudah dibuat sebelumnya > pilih grup > lalu tambahkan. Ulangi langkah sesuai dengan kebutuhan grup yang akan dibuat



Gambar 4.12 user dalam grup

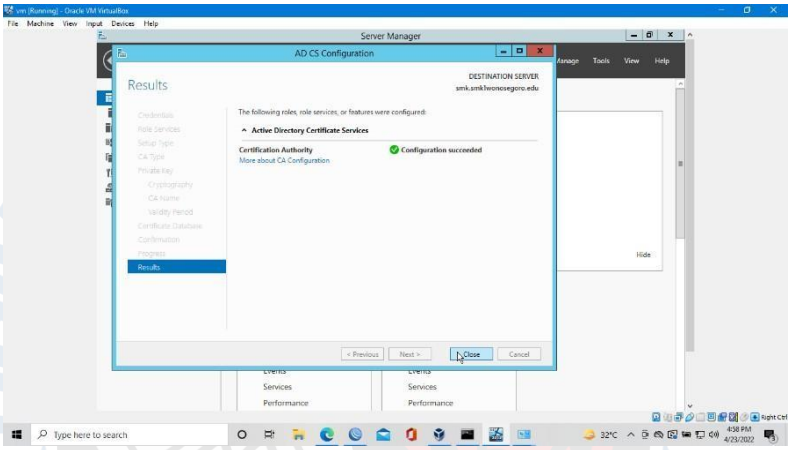
1.1.5 Instalasi dan Konfigurasi ADCS (*Active Directory Sertivicates Services*)

Instalasi dan konfigurasi ADCS (*Active Directory Sertificates Services*) dapat berfungsi sebagai peningkatan suatu keamanan, integritas data, dan otentikasi. Dengan konfigurasi ADCS (*Active Directory Sertivicates Services*) diharapkan dapat membuat Insfrastrktur Kunci Publik, hierarki otoritas sertifikasi (CA). Sertifikat ini dapat mengikat identiras seseorang, perangkat, atau layanan ke kunci publik pribadi yang sesuai. tahapan yang diperlukan dalam konfigurasi ADCS (*Active Directory Sertificates Services*) adalah dengan memilih *Certificate Authority* yang digunakan untuk memvalidasi identitas entitas seperti situs *web*, alamat *email*, perusahaan, atau orang perseorangan. Kemudian peneliti dapat memilih *Enterprise CA*, setelah melakukan kedua hal tersebut, peneliti diminta untuk *root CA*, lalu pilih *Create a new privat key*, lalu peneliti akan diminta untuk memasukkan nama sertifikat yang akan dibuat dengan nama yg sudah ada pada konfigurasi sebelumnya, kemudian akan diminta untuk menentukan durasi atau periode yang dibutuhkan untuk masa sertifikatnya. Dan konfigurasi telah berhasil dilakukan setelah adanya tampilan yang menunjukkan apa saja yang telah di konfig sebelumnya.



Gambar 4.12 Konfigurasi Complete ADCS

Gambar 4.12 menampilkan tampilan gambar telah suksesnya konfigurasi *active directory sertificate service* di *windows server*. Setelah melakukan *complete* konfigurasi, peneliti telah dapat membuat sertifikat untuk penelitian ini.



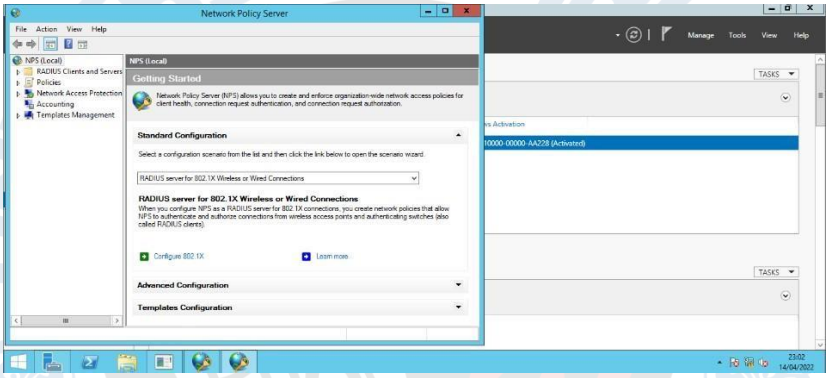
Gambar 4.13 Tampilan Akhir Konfigurasi ADCS

Gambar 4.13 menampilkan tampilan akhir setelah dilakukannya konfigurasi *active directory certificate services* di*windows server*. Dilakukannya konfigurasi ini adalah untuk dapat mengidentifikasi siapa saja yang nantinya akan meminta sertifikat dan berbagai masalah untuk *user*.

1.1.6 Instalasi dan Konfigurasi NPAS (*Network Policy and Acces Services*)

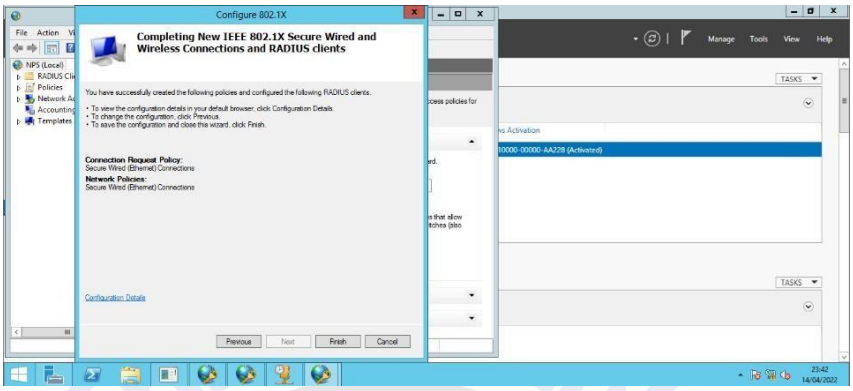
Instalasi dan Konfigurasi NPAS (*Network Policy and Acces Services*) difungsikan sebagai penerus permintaan koneksi NPS atau *Radius Server* sehingga nantinya akan dapat memuat permintaan koneksi dan meneruskannya ke *domain* yang telah ditentukan sebelumnya untuk authentikasi dan autorisasi. Tahapan untuk konfigurasi NPAS akan dilakukan setelah penginstalan terselesaikan. Ketika penginstalan sudah terselesaikan peneliti dapat masuk ke menu NPAS, kmeudian akan ada beberapa opsi atau perintah untuk menentukan *standard configuration*. Peneliti

pemilih opsi untuk *Radius server for* 802.1x *Wireless or Wizard Connections*, lalu peneliti dapat menentukan untuk jenis koneksi yang dibutuhkan, dalam kasus ini peneliti memilih *Secure Wires (Ethernet) Connections*. Kemudian peneliti akan diminta untuk memasukkan IP *Radius Client* yang akan dibutuhkan beserta *password* untuk authentikasi, dan peneliti akan diminta untuk menentukan pilihan metode dalam authentikasi yang akan dilanjutkan dengan permintaan authentikasi dan konfigurasi telah terselesaikan.



Gambar 4.14 Konfigurasi NPAS

Gambar 4.14 menampilkan tampilan pada konfigurasi NPAS. Peneliti akan menentukan sistem keamanan yang akan digunakan untuk proyek ini. Penentuan ini dapat disesuaikan dengan kebutuhan dari proyek. Dalam penelitian ini penulis melakukan konfigurasi pada *Radius Server* 802.1x *windows or wired connections* lalu pilih *configure* 802.1x.



Gambar 4.15 Konfigurasi NPAS tahap akhir

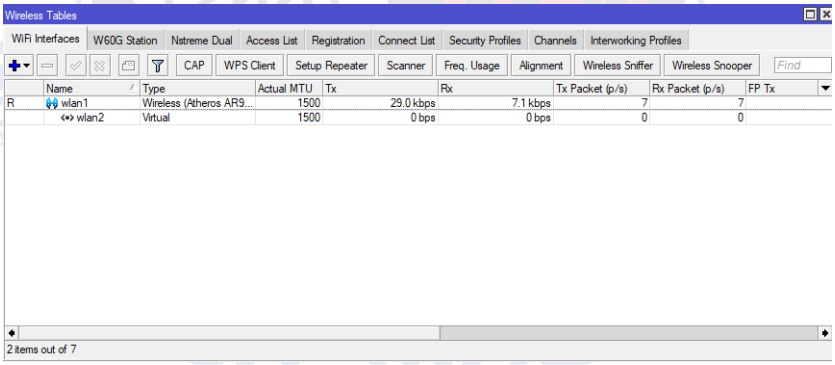
Gambar 4.15 menampilkan tampilan pada tahap akhir dalam konfigurasi NPAS di*windows server*. Beberapa langkah sebelumnya yang telah dilakukan adalah dengan menambahkan *radius client* > kemudian dengan menambahkan *IP Radius Client* dan *Verify* > tambahkan *password* untuk memudahkan penulis *password* akan diisi sama seperti dengan konfigurasi sebelumnya > setelah terdaftar klik *next* > pilih *microsoft : secure password (EAP-MSCHAP v2)* lalu pilih *configure* > penulis dapat menentukan berapa kali authentikasi dapat diulang > tambahkan *group* yang telah dibuat pada konfigurasi ADDS, *group* tersebut yang nantinya akan menjalankan *policy* tersebut > *configure* > dan *finish.*

1.1.7 Konfigurasi *Router*

Router atau *mikrotik* adalah sistem operasi dan perangkat lunak yang digunakan untuk mengubah suatu perangkat komputer menjadi sebuah jaringan. Untuk menjalankan router digunakan sebuah *software* yaitu *Winbox*, yang kegunaannya adalah untuk memudahkan konfigurasi router mikrotik karena sudah dilengkapi dengan GUI (*Graphical User Interface*).

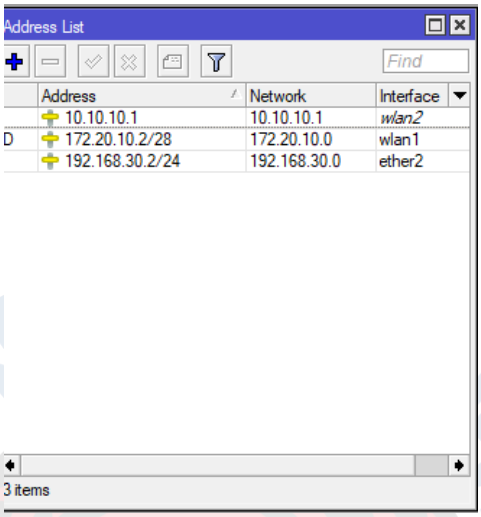
Konfigurasi *wireless* di dalam *winbox* sangat dibutuhkan karena nantinya akan digunakan sebagai sumber internet bagi *users* yang akan terhubung ke jaringan internet yang sudah disediakan sebelumnya. Sehingga fungsi *router* disini adalah untuk menyebarkan penyebaran sumber internet. Setelah melakukan

konfigurasi di *tab wireless*, akan dilakukan konfigurasi di *IP Address* yang nantinya akan digunakan sebagai penjembatan dalam berkomunikasi antar *devices*. Setelah dapat mengkonfigurasi *IP Address* peneliti diharapkan untuk mengkonfigurasi DHCP *Relay* yang fungsinya dalam penelitian ini adalah untuk pengganti DHCP *Server*, karena menggunakan Windows Server nantinya *user* akan akan mendapatkan IP, IP DNS, dan IP *Gateway* dari windows server yang telah dikonfigurasi sebelumnya. Untuk tahap akhir dalam konfigurasi di *Winbox* adalah dengan melakukan konfigurasi *Radius Server* yang digunakan untuk authentikasi *users* saat akan masuk kejaringan, hal ini berhubungan dengan konfigurasi yang ada di*Windows Server* karena authentikasi untuk masuk ke jaringan menggunakan *radius server* pada *windows server* yang mengatur *enkripsi*, dan data pengguna.



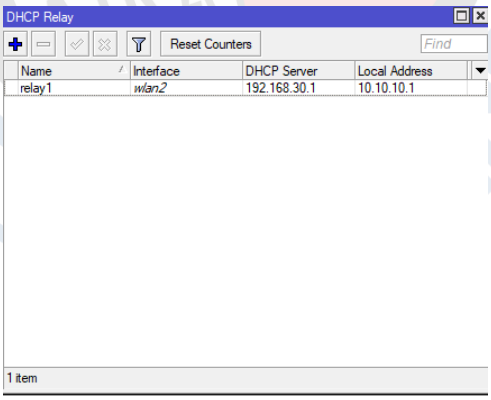
Gambar 4.16 Konfigurasi Tabs Wireless

Gambar 4.16 menampilkan konfigurasi winbox pada tabs tabs wireless. Pada tahap ini penulis melakukan konfigurasi untuk menentukan jaringan yang akan disebarkan melalui *router mikrotik.*



Gambar 4.17 Konfigurasi IP Address

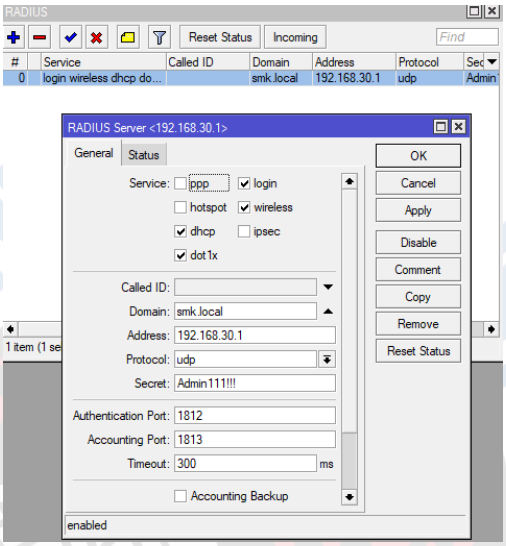
Gambar 4.17 menampilkan tampilan konfigurasi *IP Address* yang telah ditentukan. IP berupa IP yang telah dilakukan konfigurasi di*windows server*. Sehingga dengan diisinya IP tersebut nantinya akan dapat saling terhubung dan membentuk jaringan serta konfigurasi keamanan sesuai dengan keinginan penulis.



Gambar 4.18 Konfigurasi DHCP Relay

Gambar 4.18 menampilkan konfigurasi *DHCP Relay*. Dalam konfigurasi ini digunakan untuk mengirimkan *IP Address* ke perangkat *client* dari *DHCP Server* yang terpusat pada sebuah

router sehingga *router* lain hanya menjadi *DHCP Relay* yang bertugas meneruskan *DHCP Request* atau melanjutkan permintaan dari perangkat *client* ke *DHCP Server*.



Gambar 4.19 Konfigurasi Radius Server di Router

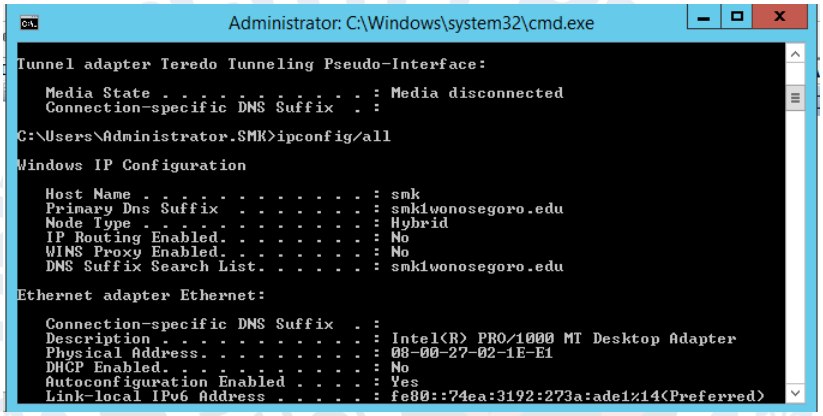
Gambar 4.19 menampilkan konfigurasi *radius server* di*router mikrotik*. Dalam konfigurasi *Radius Server* ini yang nantinya akan digunakan untuk authentikasi *users* saat akan masuk kejaringan, hal ini berhubungan dengan konfigurasi yang ada di Windows Server karena authentikasi untuk masuk ke jaringan menggunakan *radius server* pada *windows server* yang mengatur *enkripsi*, dan data pengguna.

1.2 Hasil

Output berupa hasil implementasi dan uji coba yang telah dilakukan peneliti telah melakukan beberapa rangkaian proses evaluasi, meliputi pengujian konektivitas antara *router* dan windows server dan pengujian authentikasi *radius server* yang berada di *mikrotik* dan windows server.

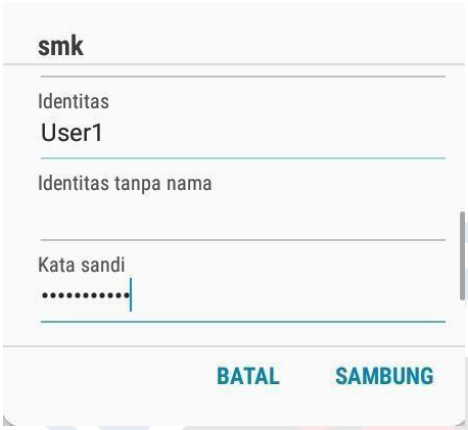
1.2.1 Pengujian DNS Server

Hasil dari pengujian DNS *Server* dapat dilihat pada aplikasi CMD (*Command Prompt*) dengan mengisikan *IP Address* yang telah dibuat, maka setelah kita memilih tombol *enter* akan muncul beberapa *point* seperti yang ada digambar. Penulis berhasil melakukan konfigurasi DNS dengan hasil dapat dilihat seperti *host name*, dan DNS *Suffix* nya.



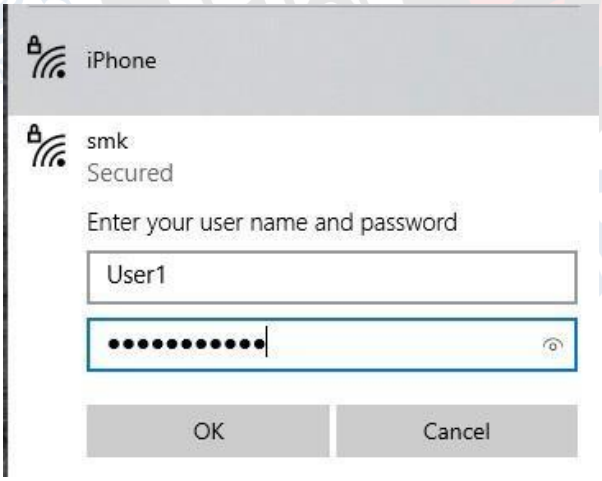
Gambar 4.20 Pengujian authentikasi Radius Server

Setelah dilakukannya implementasi, penulis memiliki hasil atas apa yang sudah diimplementasikan dengan adanya authentikasi pengguna jaringan saat akan terbuhung ke jaringan internet. *User* diminta untuk memasukkan *username* dan *password* yang telah ditentukan oleh penulis pada saat melakukan konfigurasi di windows server. *Username* yang dapat dimasukkan oleh *user* adalah *user1* dan *password* yang dapat dimasukkan oleh *user* adalah “esemkabisa1”. Di dalam tahap hasil uji coba ini, penulis menyantumkan 3 *user* yang berhasil untuk mendapatkan authentikasi saat akan terhubung ke jaringan.



Gambar 4.21 Gambar authentikasi user 1

Gambar 4.21 menampilkan tampilan pada saat *user* melakukan authentikasi dengan mengisi *username* serta *password* yang telah dikonfigurasi oleh penulis.



Gambar 4.22 authentikasi user 2

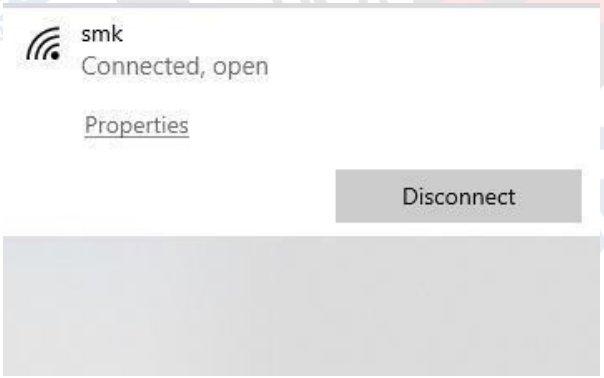
Gambar 4.22 menampilkan tampilan pada saat *user* kedua melakukan authentikasi dengan mengisi *username* dan *password* saat akan menyambungkan perangkat ke jaringan internet.

4.2.3 Pengujian Konektivitas Antara *Router* dan Windows Server

Dalam sebuah pengujian yang telah dilakukan penulis, dapat disimpulkan bahwa beberapa *user* dapat terhubung jaringan yang sudah dilakukan konfigurasi keamanan jaringan.

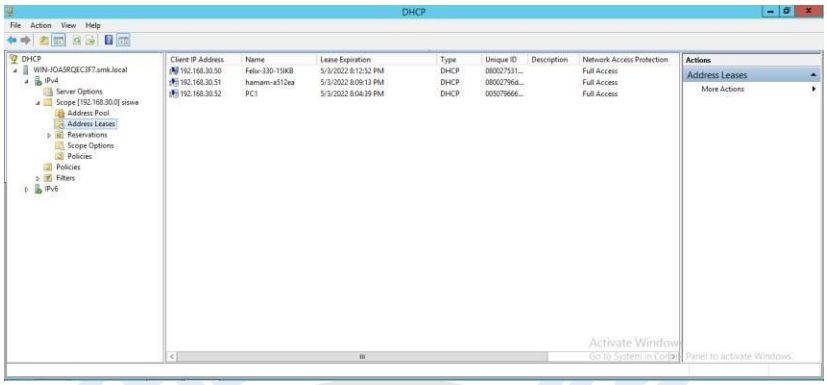
Gambar 4.23 Status Konektivitas user 1

Gambar 4.23 menampilkan tampilan perangkat dari *user* yang telah berhasil melakukan authentikasi dengan memasukkan *username* dan *password*.



Gambar 4.24 konektivitas user 2

Gambar 4.23 menampilkan tampilan perangkat dari *user* kedua yang telah berhasil melakukan authentikasi dengan memasukkan *username* dan *password*.



Gambar 4.25 User yang terdeteksi di Windows Server

Users yang sudah terhubung ke jaringan internet akan memasukkan datanya ke dalam *windows server*, sehingga *server* dapat memantau aktivitas dari siapa saja yang telah terhubung ke jaringan internet smk.

1.3 Analisis

Perancangan dan Implementasi Keamanan Jaringan dengan *Windows Server* telah berhasil dilakukan sesuai dengan rancangan yang telah dibuat sebelumnya berdasarkan topologi. Dalam hal implementasi yang meliputi instalasi, dan konfigurasi terdapat beberapa masalah yang disebabkan karena adanya konfigurasi yang belum sesuai sehingga proyek tidak bisa dijalankan, dan adanya masalah dari ekstenal seperti masalah laptop dan kebutuhan *router*nya. Dalam beberapa kasus tersebut penyelesaian yang dilakukan penulis adalah dengan melakukan konfigurasi ulang dan menelusuri terkait apa saja yang nantinya akan menyebabkan masalah agar nantinya tidak menyebabkan masalah yang terus berulang. Dan terkait masalah yang disebabkan karna laptop, dalam hal antisipasi, penulis melakukan beberapa tahap uji coba terkait *software* dan sistem operasi yang digunakan agar dapat menyesuaikan dengan laptop yang diharapkan untuk kedepannya tidak akan terjadi kendala dalam tahap konfigurasi dan implementasi. Versi dalam *windows server* sangat berpengaruh terhadap perfoma laptop, sehingga untuk kalancaran sebuah

proyek penulis dapat menentukan dan melakukan tahap instalasi *windows server* agar penulis dapat mengetahui versi *windows server* yang cocok untuk laptop yang akan digunakan sebagai perangkat. Setelah melewati beberapa kasus, penulis dapat menyelesaikan proyek dengan sangat baik. Tahap selanjutnya setelah perancangan adalah tahap implementasi, dimana seharusnya penulis akan mengimplementasikan proyek ini di SMK N 1 Wonosegoro. Namun terjadi kendala yang dikarenakan pihak sekolah yang belum memiliki waktu untuk dapat menginjinkan penulis untuk tahap implementasi. Sehingga karena saran dari pembimbing untuk dapat memiliki opsi tempat kedua dalam implementasi disaat- saat terakhir, penulis memutuskan untuk memilih tempat yang kurang lebih sama dengan tempat sebelumnya. Dimana akan ada *user* yang akan terhubung, dan dapat menjadi pelengkap dalam pengimplementasian proyek ini. Kekurangan dari proyek ini adalah dalam tahap pengimplementasian, pada konfigurasi masih mencantumkan nama instansi lokasi yang akan menjadi tempat implementasi sebelumnya. Diluar hal tersebut perancangan dan pengimplementasian ini dapat berjalan sesuai yang diharapkan oleh penulis, walaupun melaui proses yang membutuhkan banyak pembelajaran.